管理ポータル

25.11

パートナー管理者ガイド

リビジョン: 2025/12/15

目次

このドキュメントについて

この文書は、 Cyber Protect Cloudを使用してクライアントにサービスを提供するパートナー管理者を対象としています。

この文書では、管理ポータルを使用して Cyber Protect Cloudで利用できるサービスを設定・管理する方法について説明します。

Cyber Protect Cloudのバージョン情報

Cyber Protect Cloudは、サービスプロバイダー、リセラー、ディストリビュータがパートナーやカスタマーにデータ保護サービスを提供するためのクラウドプラットフォームです。

サービスは、パートナーレベル、カスタマーレベルおよびエンドユーザーレベルにそれぞれ提供されます。

クラウドサービス管理は、**サービスコンソール**と呼ばれるWebアプリケーションから利用できます。テナントとユーザーアカウントの管理は、**管理ポータル**と呼ばれるWebアプリケーションから利用できます。

管理ポータル管理者は、以下のことが可能になります。

- サービスとテナントの制限値（クォータ）の設定
- テナントの管理
- ユーザーアカウントの管理
- ストレージの管理
- カスタマイズの管理
- サービスの使用状況のモニタリングとサービスコンソールへのアクセス
- サービス使用状況レポートの生成

ライセンスモード

ライセンスモードはサービスとその機能を使用する際の会計処理や課金用のスキームです。ライセンスモードでは、価格を計算する際のベースとして使用される単位を決定します。ライセンスモードは、パートナーが子パートナーまたはカスタマーテナントに対して設定できます。

注意
すべてのライセンスモードはパートナーテナントで有効にできますが、カスタマー テナントでは 1 つのライセンスモードのみを有効にできます。

組み込みのライセンスエンジンは、テナントで有効になっているサービス、各サービスで使用可能なクォータ、保護計画で要求される機能に応じて、テナントが使用する提供項目を自動的に取得します。ユーザーは、保護計画をカスタマイズすることで、保護レベルとコストを最適化できます。

保護サービスのライセンスモード

保護サービスは、ソリューションベースのライセンスモードとサービスベースのライセンスモードを提供します。

ソリューションベースのライセンス（ワークロードごと）

ソリューションベースのライセンスは、サイバープロテクションで最も一般的に使用されるサービスに対応した使いやすいサービスパッケージを求める中小規模のマネージドサービスプロバイダー（MSP）を対象としています。

- セキュリティとRMM
- バックアップとDisaster Recovery
- 究極の保護

請求書発行は、ワークロードごとに行われます。該当する場合は、クラウドストレージの使用は別途請求されます。パートナーポータルのライセンスガイドを参照してください。

サービスベースのライセンス（ワークロード/ギガバイトあたり）

両方のサービスベースのライセンスモードの機能セットは同一であり、請求書発行に使用される単位のみが異なります。

- ワークロードごとのライセンスでは、請求書発行は保護対象のワークロードの数に基づいて行われます。使用したクラウドストレージには追加料金がかかる場合があります。
- ギガバイト単位のライセンスモードでは、請求書発行は使用されているクラウドストレージとローカルストレージに基づいて行われます。

どちらのモードの保護サービスにも、ほぼすべてのサイバーセキュリティリスクに対応した標準保護機能が付属します。ユーザーはそれらの機能を追加料金なしで使用できます。標準機能の使用は記録されますが、請求の対象とはなりません。課金モードに含まれ、請求の対象となる提供項目の全リストは、"標準および追加の保護サービス"（42ページ）で確認できます。

追加サービスがカスタマーに対して有効になっている時、請求書発行が開始されるのは、カスタマーが保護計画に含まれているサービスの機能を使用し始めた後になります。保護計画内に追加サービス機能が適用されると、ライセンスエンジンにより自動で、必要なライセンスが保護対象のワークロードごとに割り当てられます。

追加サービスの利用を停止すると、ライセンスは取り消され、請求も停止されます。ライセンスエンジンは、サービスの実際の使用状況をふまえて、自動的にライセンスを割り当てます。

標準Cyber Protectサービス機能に対してのみ、ライセンスを割り当てることができます。追加サービスは使用状況に基づいて課金され、ライセンスを手動で変更することはできません。これらのライセンスの割り当ておよび割り当て解除は、ライセンスエンジンによって自動で行われます。ワークロードのライセンス種類を手動で変更することはできますが、変更が再度割り当てられるのは、そのワークロードの保護計画がユーザーに変更されたときになります。

File Sync & Shareのライセンスモード

File Sync & Shareには、次のライセンスモードがあります:

- ユーザーあたり
- ギガバイトあたり

どちらのモードでも、Notarization and eSignatureを追加サービスとして提供しています。

注意
Notarization and eSignatureに対する課金は、機能を有効にした時点では開始されません。課金が開始されるのは、カスタマーが機能の使用を開始した後になります。サービスが有効になると、記録が行われ使用状況レポートに含められますが、機能が使用されない限り課金対象とはなりません。

物理データ配送の課金

物理データ配送の課金は、使用量に応じた支払いモデルになります。

保護サービスのライセンスモードの切り替え

管理ポータル では、テナントのライセンスモードを切り替えることができます。

切り替え処理は、バックグラウンドで次の手順で実行されます。

1. 元の提供項目で利用できた機能に一致するように、新しいサービス（提供項目）をカスタマーテナントにプロビジョニングします（提供項目を有効にしてクォータを設定します）。
2. 未使用の提供項目の割り当てを解除し、保護計画で使用される機能に応じて提供項目をワークロードに割り当てる（使用状況の調整）。

次の表は、すべてのサポートされているシナリオでのライセンスモードの切り替えの結果を示します。

切り替え前	切り替え後	切り替えの結果		
		提供アイテム	制限値（クォータ）	使用状況
サービスベース（ワークロードまたはギガバイトあたり）	ソリューションベース（ワークロードあたり）	ソリューションベースのライセンスモードで親テナントが利用できるすべてのサービスが有効になっています。	すべての利用可能なクォータが「無制限」に設定されています。	提供項目は、ワークロードに割り当てられた保護計画で使用される機能に応じて、ワークロードに再割り当てされます。
ソリューションベース（ワークロードあたり）	サービスベース（ワークロードあたりまたはギガバイトあたり）	サービスベースのライセンスモードで親テナントで利用可能なすべてのサービスが有効になっています。	すべての利用可能なクォータが「無制限」に設定されています	
サービスベース（ワークロードあたりまたはギガバイトあたり）	サービスベース（ワークロードあたりまたはワークロードあたり）	元のモードで有効にされていたサービスは、変更後のモードでも有効になります。	クォータは、元のサービスから変更後のサービスに「そのまま」レプリケーションされます。	

注意

スイッチの種類にかかわらず、すべての保護計画は中断することなく機能し、すべての登録済みのワークロードとそのバックアップは保持され、履歴の使用状況統計は保持されます。

例: サービスベース（ワークロードごと）からソリューションベース（ワークロードごと）への切り替え

このシナリオでは、カスタマーのテナントに、8台のワークステーションで使用されているサービスベース（ワークロードごと）の標準保護があり、クォータは10台のワークステーションに設定されています。3台のワークステーションでは、保護計画でソフトウェアのインベントリとパッチ管理（RMMサービスの一部）が使用されており、2台のワークステーションでは、保護計画でURLフィルタリング（Detection and Responseサービスの一部）が有効になっており、1台のマシンでは、継続的データ保護（Advanced Backupサービスの一部）が使用されています。次の表は、ソリューションベースのライセンスモードの下での使用状況の提供項目への変換を示します。

切り替え元提供項目 - 使用数/クォータ	切り替え先提供項目 - 使用数/クォータ

• 標準保護
  ◦ ワークステーション - 8/10
• 検知と応答 - 2/10
• Advanced Backupワークステーション - 1/10
• RMM - 3/10
	• 究極の保護
	  ◦ ワークステーション - 8/無制限

切り替え時には、次の手順が実施されました:

1. 元の請求書発行構成で使用可能だった機能をカバーする提供項目「究極の保護」が自動的に有効化されました。
2. クォータは「無制限」に設定されていました。
3. 保護計画での実際の使用状況に従って使用状況が調整されました。8台のワークステーションが究極の保護提供製品の機能を使用しています。

例: ソリューションベースからサービスベース（ワークロードごと）の請求

この例では、カスタマーは、ワークロードに複数のソリューションベースの提供項目を割り当てています。各ワークロードには、1 つのライセンスモード (ソリューションベースまたはサービスベース (ワークロードまたはギガバイト単位)) のみを割り当てることができます。

ソリューションベースの提供項目 - 使用量/クォータ	サービスベースの提供項目 - 使用量/クォータ

• セキュリティとRMM
  ◦ Microsoft 365 シート - 2/12 (保護計画におけるセキュリティ状況管理)
  ◦ エンドポイント - 4/12 (保護計画にマルウェア対策保護が含まれるワークステーション4台)
	• 標準保護
	  ◦ ワークステーション - 4/無制限
	• RMM
	  ◦ Microsoft 365 シート数 - 2/無制限

• バックアップおよびDisaster Recovery
  ◦ ワークステーション 2/10（保護計画にバックアップのみ含まれる）
  ◦ サーバー 3/10（保護計画にバックアップとディザスタリカバリが含まれる）
	• 標準保護
	  ◦ ワークステーション - 2/無制限
	  ◦ サーバー - 3/無制限
	• Disaster Recovery - 3/無制限

• 究極の保護 2/10
  ◦ 仮想マシン 2/10（保護計画にバックアップとマルウェア対策保護が含まれる）
	• Standard Protection
	  ◦ 仮想マシン - 2/無制限

切り替え時には、次の手順が実施されました:

1. 切り替え元のエディションで利用できたすべての機能をカバーする提供項目が自動的に有効になりました。課金モードでは、複数の提供項目を必要に応じてワークロードに割り当てることができます。
2. クォータがまとめて複製されました。

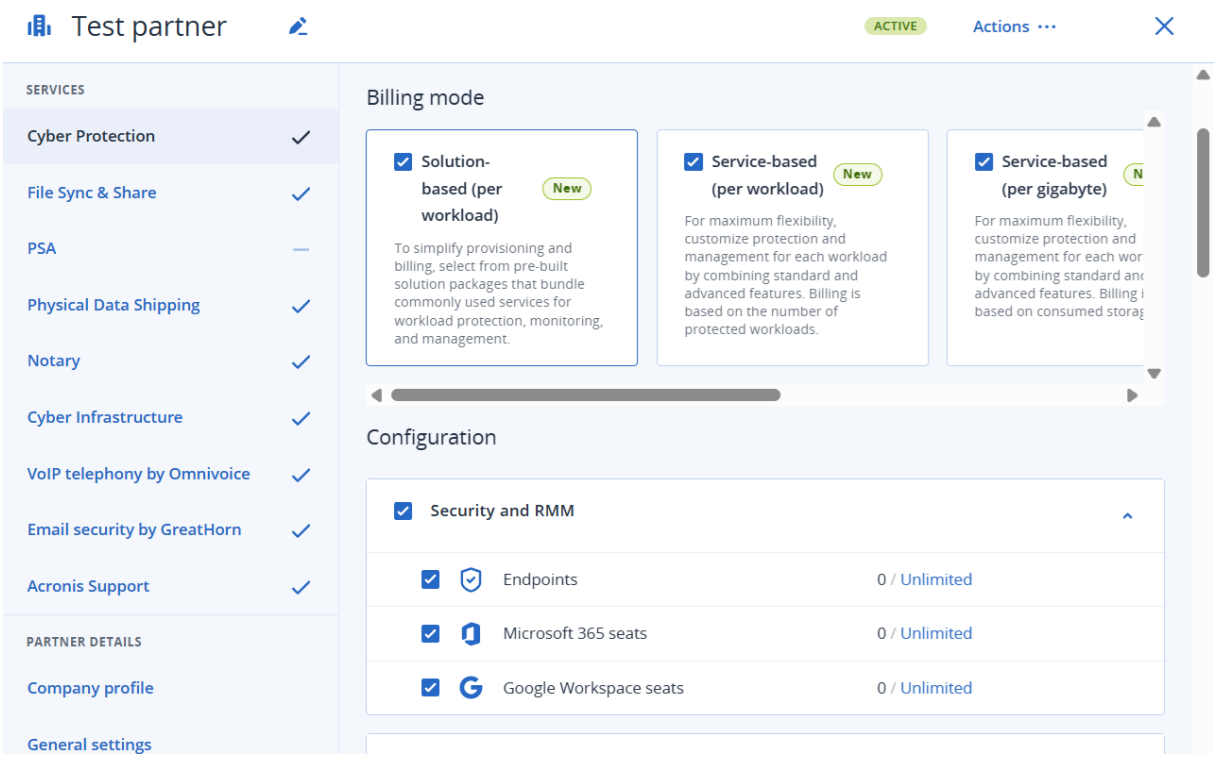
3. 使用数が保護計画に応じて調整されました。
4. すべての提供項目が有効になり、クォータが「無制限」にリセットされます。

提供項目および制限値（クォータ）

提供アイテム

提供項目は、サービス内の機能セットであり、特定のワークロードタイプまたは機能ごとにグループ化されています。例えば、ストレージ、ディザスタリカバリインフラストラクチャなどです。

管理ポータルでは、提供項目は、UI のサービス構成セクションのチェックボックスに対応します。



個別の提供項目を有効にすることで、保護対象ワークロードの内容、クォータの設定による保護対象ワークロードの数、追加の保護プロセスの有効/無効によるパートナー、カスタマー、エンドユーザーの利用可能な保護レベルを決定します。

有効でない機能は、アップセルシナリオを構成しない限り、カスタマーやユーザーには表示されません。アップセルシナリオの詳細については、「"アップセルカスタマー向けのアップセル施策を構成"（165ページ）」を参照してください。

機能の使用状況はサービスから収集され、提供項目に反映され、レポートや請求のために使用されます。

制限値（クォータ）

制限値（クォータ）はテナントによるサービスの使用を制限できます。"ソフトおよびハード制限値（クォータ）"（17ページ）を参照してください。

提供アイテムの有効化/無効化

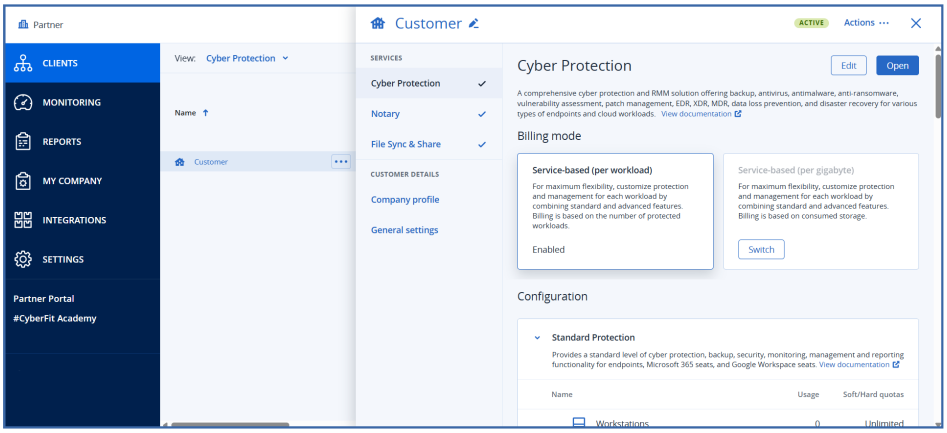
ソリューションベースまたはサービスベースの構成で提供項目を有効化および無効化できます。

提供項目の有効化/無効化

1. 管理ポータルで、**クライアント**に移動します。
2. カスタマーの行をクリックします。

   注意
   カスタマー名をクリックしないでください。

   省略記号アイコン（...）をクリックして、**[設定]** をクリックします。
3. ネットワークセクションで、編集するインターフェースを選択します。
   例えば、**サイバープロテクション**。
4. **[編集]** をクリックします。



5. 提供項目の有効化/無効化。

   注意
   サービスの提供項目をすべて無効にしても、サービスが自動的に無効になることはありません。

6. **[保存]** をクリックします。

下の表に示す提供項目を無効にする場合には、制限事項がいくつかあります。

提供アイテム	無効化	結果
バックアップストレージ	使用状況がゼロの場合、無効にすることができます。	クラウドストレージは顧客テナント内のバックアップ先として利用できなくなります。
ローカルバックアップ	使用状況がゼロの場合、無効にすることができます。	ローカルストレージは、カスタマーテナント内のバックアップ先として使用できなくなります。ローカルバックアップのクォータ

		を無効にすると、S3互換、Azure、AWS、Wasabi、Impossible Cloudなどのローカルディスク、ネットワーク共有、パブリッククラウドへのバックアップが無効になります。
データソース（Microsoft 365およびGoogle Workspaceを含む）*	使用状況がゼロの場合、無効にすることができます。	データソース（Microsoft 365およびGoogle Workspaceを含む）の保護はカスタマーテナント内で利用できなくなります。以下のカスタマーテナント:
すべてのDisaster Recovery提供アイテム	使用状況がゼロを上回る場合、無効にすることができます。	詳細については、「ソフトおよびハード制限値（クォータ）」をご覧ください。
すべてのNotary提供アイテム	使用状況がゼロの場合、無効にすることができます。	顧客テナント内でのNotaryサービスは無効になります。
すべてのFile Sync & Share提供アイテム	提供アイテムは個別に有効または無効にできません。	顧客テナント内で、File Sync & Shareサービスは利用できなくなります。
すべての物理データ配送提供アイテム	使用状況がゼロの場合、無効にすることができます。	顧客テナント内での物理データ配送サービスは無効になります。

*提供項目は、Cyber Protectコンソールで追加できるワークロードに関するものです。 以下の表は、管理ポータルで提供項目、提供項目の組み合わせ、または追加サービスが有効にされていない場合に、利用できないワークロードタイプをまとめたものです。

使用状況がゼロを上回る際に無効にできない提供アイテムについては、手動で使用量を削除してから、対応する提供アイテムを無効にすることができます。

これらの提供項目または追加の保護サービスを無効にした場合	これらのタイプのワークロードを追加することはできません
以下の組み合わせ: • Microsoft 365シート • Microsoft 365 SharePoint online • Microsoft 365 Teams	Microsoft 365 Business
以下の組み合わせ: • Google Workspace • Google Workspace共有ドライブ	Google Workspace
以下の組み合わせ: • サーバー	• Microsoft SQL Server • Microsoft Exchange Server

これらの提供項目または追加の保護サービスを無効にした場合	これらのタイプのワークロードを追加することはできません
• 仮想コンピュータ	• Microsoft Active Directory
以下の提供項目: • NAS	Synology
以下の提供項目: • Mobile	• iOSデバイス • Androidデバイス
以下のアドバンスドパック: • Advanced Backup	Oracleデータベース
以下の組み合わせ: • Eメールアーカイブのシート • アーカイブストレージ	メールサーバー

ソフトおよびハード制限値（クォータ）

クォータでテナントによるサービスの使用を制限できます。クォータを設定するには、**[顧客]** タブで顧客を選択し、サービスタブを選択し、**[編集]** をクリックします。

指定した容量を超過すると、ユーザーの電子メールアドレスに通知が送信されます。追加制限値（クォータ）を設定していない場合は、制限値（クォータ）は「**ソフト**」と見なされます。これは、Cyber Protectionサービスの使用に関する制限が適用されていないことを表します。

クォータの追加を指定すると、クォータは「**ハード**」とみなされます。**追加容量**により、ユーザーは指定された値の分だけ制限値（クォータ）を超過することができます。追加容量を超過すると、サービスの使用に関する制限が適用されます。

例

ソフト制限値（クォータ）:ワークステーションに、20台の制限値（クォータ）を設定しました。カスタマーの保護済みワークステーションが20台に達すると、Eメールによる通知がカスタマーに送られますが、Cyber Protectionサービスは引き続き利用可能です。

ハード制限値（クォータ）:ワークステーションの制限値（クォータ）を20台に設定し、追加分を5台にする場合、保護済みワークステーションの数が20台に達したときにEメールによる通知がカスタマーに送られます。さらに25台に達するとCyber Protectionサービスが無効化されます。

ハードクォータに到達すると、サービスが制限されます（別のワークロードを保護したり、より多くのストレージを使用したりすることができなくなります）。指定したハードクォータを超過すると、ユーザーのEメールアドレスに通知が送信されます。

注意
Microsoft 365 のシートと Google Workspace のシートのクォータは常にソフトクォータです。というのも、使用状況の制限はベンダー側でサポートされていないからです。

制限値（クォータ）を定義できるレベル

制限値（クォータ）は下の表に示すレベルで設定できます。

テナント/ユーザー	ソフト制限値（クォータ）（クォータのみ）	ハード制限値（クォータ）（クォータと追加量）
パートナー	はい	いいえ
フォルダ	はい	いいえ
顧客	はい	はい
ユニット	いいえ	いいえ
ユーザー	はい	はい

ソフト制限値（クォータ）はパートナーとフォルダレベルで設定できます。部署レベルでは制限値（クォータ）を設定できません。ハード制限値（クォータ）は顧客とユーザーレベルで設定できます。

ユーザーレベルで設定したハード制限値（クォータ）の合計量が、関係する顧客ハード制限値（クォータ）を超えることはできません。

ソフトおよびハードクォータの設定

子テナントにクォータを設定するには

1. 管理ポータルで **[クライアント]** へ進みます。
2. クォータを設定するテナントの名前の横にある三つの点をクリックし、**[設定]**をクリックします。
3. 設定するサービスを選択し、**[編集]** をクリックします。
4. 設定するクォータのタイプを選択します。たとえば、**ワークステーション**や**サーバー**を選択できます。
5. 右側の**[無制限]**リンクをクリックして、**クォータの編集**ウィンドウを開きます。
   - クォータについてクライアントに通知し、クライアントのサービス利用を制限したくない場合は、**[ソフトクォータ]** フィールドにクォータ値を設定します。
     クォータに到達すると、クライアントに通知Eメールが届きますが、Cyber Protectionサービスは引き続き利用できます。
   - クライアントのサービス利用を制限したい場合は、**[ハードクォータ]** を選択し、**ハードクォータ**の以下のフィールドにクォータの値を設定します。
     クォータに到達すると、クライアントに通知Eメールが届き、Cyber Protectionサービスは無効化されます。
6. **[クォータの編集]**ウィンドウで、**[適用]**をクリックし、**[保存]**をクリックします。

重要
製品のUIに表示されるストレージ使用量の値は、バイナリバイト単位（メビバイト（MiB）、ギビバイト（GiB）、テビバイト（TiB））ですが、ラベルにはそれぞれMB、GB、TBが表示されます。たとえば、実際の使用量が3105886629888バイトの場合、UIに表示される値は2.82と正しく表示されますが、ラベルはTiBではなくTBになります。

Backup制限値（クォータ）

クラウドストレージの制限値（クォータ）、ローカルバックアップの制限値（クォータ）、ユーザーが保護できるマシン/デバイス/Webサイトの最大数を指定できます。以下の制限値（クォータ）を利用できます。

デバイスの制限値（クォータ）

- **ワークステーション**
- **サーバー**
- **仮想コンピュータ**
- **モバイル デバイス**
- **Webホスティングサーバー**（Plesk、cPanel、DirectAdmin、VirtualMin、またはISPManagerのコントロールパネルを実行しているLinuxベースの物理サーバーまたは仮想サーバー）
- **Web サイト**

マシン/デバイス/Webサイトは、少なくとも1つの保護計画が適用されていれば、保護されているとみなされます。 モバイルデバイスは、最初のバックアップが実行された後に、保護されます。

複数のデバイスで超過が発生すると、ユーザーは保護計画をそれ以外のデバイスに適用できなくなります。

クラウドデータソースの制限値（クォータ）

- **Microsoft 365シート**
  このクォータは、サービスプロバイダーによって企業全体に適用されます。会社の管理者は、管理ポータルでクォータとその使用状況を表示できます。ハードクォータを超過すると、バックアップ計画を新しいシートに適用できなくなります。
  このクォータの課金は、Cyber Protectionに選択した課金モードに応じて異なります。
  - **[ギガバイト単位]** 課金モードでは、課金はストレージ使用状況のみに基づいて行われ、シートはカウントされません。
  - **[ワークロード単位]** 課金モードでは、Microsoft 365の保護されたシートの数に基づいて課金が行われます。ストレージの使用状況については、保護されていないシートのみが課金されます。
    次の表は、**ワークロード単位**の課金モードをまとめたものです。

	バックアップロケーション	
	アクロニスホステッドストレージ* パートナーホステッドストレージ	**Microsoft Azure Storage Googleストレージ**
保護されたシート	課金は、保護されたシートの数に基づいて行われます。 保護されたシートのバックアップに使用されるストレージスペースには課金されません。	保護されたシートと使用されたストレージの両方が課金されます。
保護されていないシート	保護されていないシートには課金されません。 保護されていないシートのバックアップに使用されるストレージスペースには課金されます。	保護されていないシートには課金されません。 保護されていないシートのバックアップに使用されるストレージスペースには課金されます。

* Acronisストレージの公正使用ポリシーが適用されます。利用規約は、https://www.acronis.com/ja-jp/company/licensing/#cyber-cloud-fair-usageでご確認いただけます。

Microsoft 365ユーザーが次のいずれかを所有している場合、シートは保護されているものと見なされます。

- バックアップ計画が適用されるメールボックス
- バックアップ計画が適用されるOneDrive
- Microsoft 365 SharePoint OnlineサイトやMicrosoft 365 Teamsなどの企業レベルの保護対象リソースにアクセスします。

  Microsoft 365 SharePointまたはTeamsサイトのメンバー数を確認する方法については、こちらのナレッジベースの記事を参照してください。

シートは、次の場合に保護されなくなります。

- ユーザーのMicrosoft 365 SharePoint OnlineサイトやMicrosoft 365 Teamsなどの企業レベルの保護対象リソースへのアクセスが取り消された。
- ユーザーのメールボックスまたはOneDriveからすべてのバックアップ計画が取り消されている。
- Microsoft 365組織でユーザーが削除されました。

以下のMicrosoft 365リソースは課金対象外であり、シート単位のライセンスは必要ありません。

- 共有メールボックス
- ルームと備品
- バックアップされたSharePointサイトまたMicrosoft Teamsにアクセスできる外部ユーザー。

注意

ブロック対象のMicrosoft 365ユーザーで、保護された個人用メールボックスやOneDriveを所有せず、共有リソース（共有メールボックス、SharePointサイト、Microsoft Teams）にのみアクセスできる場合、このユーザーは課金対象外となります。ブロック対象のユーザーとは、有効なログインアカウントを所有しておらず、Microsoft 365サービスにアクセスできないユーザーのことです。
Microsoft 365 組織内に存在するすべてのライセンス対象外のユーザーをブロックする方法については、"ライセンス対象外のMicrosoft 365ユーザーのサインインを防止する"（24ページ）を参照してください。

重要

ローカルエージェントとクラウドエージェントは別個のクォータを消費します。両方のエージェントを使用して同じワークロードをバックアップした場合、二重に課金されます。以下に例を示します。

- ローカルエージェントを使用して120人のユーザーのメールボックスをバックアップし、クラウドエージェントを使用して同じユーザーのOneDriveファイルをバックアップする場合、Microsoft 365の240シート分が課金されます。
- ローカルエージェントを使用して120人のユーザーのメールボックスをバックアップし、クラウドエージェントを使用して同じメールボックスをバックアップする場合、Microsoft 365の240シート分が課金されます。

Microsoft 365シートのライセンスに関するよくあるご質問（FAQ）については、「Cyber Protect Cloud: Microsoft 365（GB単位のライセンス）」および「Cyber Protect Cloud: Microsoft 365のライセンスと価格の変更」を参照してください。

- **Microsoft 365 SharePoint Online**

  このクォータは、サービスプロバイダーによって企業全体に適用されます。このクォータにより、SharePoint Onlineサイトの保護が可能になり、保護できるサイトコレクションとグループサイトの最大数が設定されます。

  企業管理者は管理ポータルでクォータを表示できます。また、企業管理者は使用状況レポート内でクォータとともにSharePoint Onlineバックアップで使用されているストレージ容量を表示できます。

- **Microsoft 365 Teams**

  この制限値（クォータ）は、サービスプロバイダーによって企業全体に適用されます。この制限値（クォータ）により、Microsoft 365 Teamsの保護機能を有効または無効にします。また、保護できるチーム数の上限を設定します。1つのチームを保護するには、そのメンバーまたはチャネルの数に関係なく、1つのクォータが必要です。企業管理者は管理ポータルで制限値（クォータ）と使用状況を表示できます。

- **Microsoft 365 Eメールアーカイブ用シート**

  Microsoft 365 Eメールアーカイブ用シートのクォータは、 Microsoft 365 メールサーバーのEメールアーカイブを作成する機能を有効または無効にし、アーカイブに追加できるメールボックスの最大数を設定します。

- **Eメールアーカイブ用シート（廃止）**

  このクォータは非推奨であり、管理ポータルで新しいテナントを作成する際に有効にすることはできません。

既存のテナントでは、クォータがすでに有効になっている場合にのみ無効にできますが、再度有効にすることはできません。

重要
新しいカスタマーテナントを作成する場合は、**Microsoft 365 アーカイブ用シート**のクォータを使用します。
既存のカスタマーの場合、**Eメールアーカイブ用シート（廃止）**のクォータは自動的に**Microsoft 365アーカイブ用シート**のクォータに置き換えられます。既存の**Eメールアーカイブ用シート（廃止）**の下での使用は、**Microsoft 365アーカイブ用シート**に転送されます。

Google Workspaceシート
この制限値（クォータ）は、サービスプロバイダーによって企業全体に適用されます。企業は**Gmail**メールボックス（カレンダーと連絡先を含む）と**Google ドライブ**ファイル、またはその両方を保護できます。企業管理者は管理ポータルで制限値（クォータ）と使用状況を表示できます。
Google Workspaceシートは、1つ以上のバックアップ計画がユーザーのメールボックスまたはGoogleドライブに適用されていれば、保護されているとみなされます。
ハードクォータが超過していると、企業管理者はバックアップ計画を新しいシートに適用できなくなります。

- **Google Workspace共有ドライブ**
  この制限値（クォータ）は、サービスプロバイダーによって企業全体に適用されます。この制限値（クォータ）は、Google Workspace共有ドライブを保護する機能を有効または無効にします。制限値（クォータ）が有効になっている場合、共有ドライブをいくつでも保護できます。企業管理者は管理ポータルで制限値（クォータ）を表示できませんが、使用状況レポート内で、共有ドライブバックアップで使用されているストレージ容量を表示できます。
  余分なGoogle Workspaceのシートクォータを1つまたは複数所有しているカスタマーに限り、Google Workspace共有ドライブのバックアップを利用できます。このクォータは検証のみで、利用されません。

ストレージの制限値（クォータ）

重要
製品のUIに表示されるストレージ使用量の値は、バイナリバイト単位（メビバイト（MiB）、ギビバイト（GiB）、テビバイト（TiB））ですが、ラベルにはそれぞれMB、GB、TBが表示されます。たとえば、実際の使用量が3105886629888バイトの場合、UIに表示される値は2.82と正しく表示されますが、ラベルはTiBではなくTBになります。

- **クラウドリソース**
  - **バックアップストレージ**
    - **バックアップストレージ**
      このクォータは、クラウドストレージにあるバックアップの合計サイズを制限します。バックアップストレージのハードクォータを超過していると、バックアップ操作は開始されません。
      ワークロードごとの請求書発行モードでは、このクォータはMicrosoft 365およびGoogle Workspaceとは異なるワークロードのバックアップにのみ適用されます。

Microsoft 365 および Google Workspace のワークロードのバックアップストレージは無制限です*。**Microsoft 365 のシート** や **Google Workspace のシート** などのシートクォータがワークロードから削除されると、バックアップストレージは無制限のままですが、その使用量には料金が発生します。

[ギガバイト単位] 課金モードでは、このクォータは、Microsoft 365ワークロードおよびGoogle Workspaceワークロードを含む、あらゆるバックアップに適用されます。

* Acronisストレージの公正使用ポリシーが適用されます。利用規約は、https://www.acronis.com/ja-jp/company/licensing/#cyber-cloud-fair-usageでご確認いただけます。

- **アーカイブストレージ**

  このクォータにより、クラウドインフラのEメールアーカイブの合計サイズを制限します。

- **Advanced Disaster Recovery**

  このセクションには、ディザスタリカバリに関連するクォータが含まれています。

- **ローカルリソース**
  - **ローカルバックアップ**

    ローカルバックアップのクォータは、S3互換、Azure、AWS、Wasabi、Impossible Cloudなどのローカルディスク、ネットワーク共有、パブリッククラウドへのバックアップの合計サイズを制限します。

    - この制限値（クォータ）には追加容量を設定できません。
    - ローカルバックアップにはハードクォータを適用できません。

    注意
    ローカルバックアップのクォータを無効にすると、ローカルバックアップ、ネットワーク共有へのバックアップが無効になり、パブリッククラウドにバックアップを作成します。

バックアップストレージのクォータ超過

バックアップストレージのクォータを超えることはできません。プロテクションエージェント証明書には、テナントのバックアップクォータに相当する技術クォータが指定されています。またそれとは別に追加容量があります。クォータを超過すると、バックアップが開始できません。バックアップ作成中に証明書のクォータに達しても、追加容量に達していなければ、バックアップは正常に完了します。バックアップ作成中に追加容量に達した場合、バックアップは失敗します。

例:

ユーザーテナントのクォータの空き領域が1TBで、このユーザー向けに構成されている追加容量が5TBとします。ユーザーがバックアップを開始します。作成されたバックアップのサイズがたとえば3TBの場合、追加容量を超えていないため、バックアップは正常に完了します。作成されたバックアップのサイズが6TBよりも大きい場合、追加容量を超過した時点でバックアップが失敗します。

重要
製品のUIに表示されるストレージ使用量の値は、バイナリバイト単位（メビバイト（MiB）、ギビバイト（GiB）、テビバイト（TiB））ですが、ラベルにはそれぞれMB、GB、TBが表示されます。たとえば、実際の使用量が3105886629888バイトの場合、UIに表示される値は2.82と正しく表示されますが、ラベルはTiBではなくTBになります。

バックアップ制限値（クォータ）変換

一般的に、バックアップ制限値（クォータ）はこのように取得され、リソースタイプへの提供アイテムマッピングはこのように機能します。システムは利用可能な提供アイテムとリソースタイプを比較し、一致した提供アイテムの制限値（クォータ）を取得します。

リソースタイプと完全に一致していなくても別の提供項目制限値（クォータ）を割り当てる機能もあります。これを**バックアップ制限値（クォータ）変換**といいます。一致する提供アイテムがない場合、システムはリソースタイプに対してより高コストの適切な制限値（クォータ）を見つけようとします（自動バックアップ制限値（クォータ）変換）。適切なものが何も見つからない場合、Cyber Protectコンソールでリソースタイプにサービス制限値（クォータ）を手動で割り当てることができます。

例

仮想マシンをバックアップしようとしています（ワークステーション、エージェントベース）。

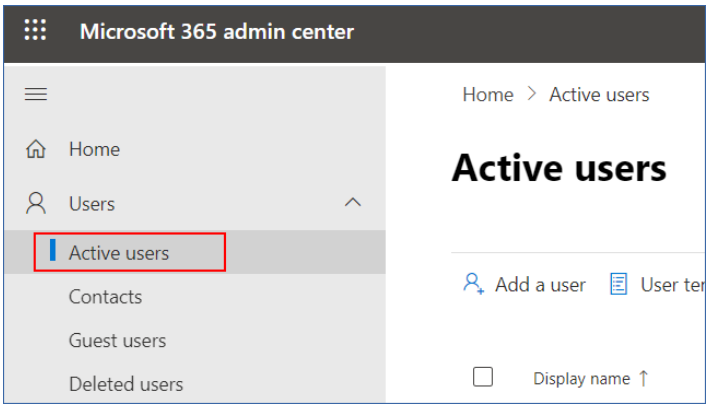
最初に、システムは割り当てられた**仮想マシン**制限値（クォータ）があるかどうかをチェックします。それが見つからない場合、システムは自動的に**ワークステーション**制限値（クォータ）の取得を試みます。それも見つからない場合、他の制限値（クォータ）は自動的に取得されません。**仮想マシン**制限値（クォータ）よりも高コストの制限値（クォータ）が十分にあり、それが仮想マシンに適用可能な場合、Cyber Protectコンソールにログインし、手動で**サーバー**制限値（クォータ）を割り当てることができます。

ライセンス対象外のMicrosoft 365ユーザーのサインインを防止する

サインインステータスを編集することで、Microsoft 365組織内に存在するライセンス対象外のユーザーすべてがサインインできないように設定できます。

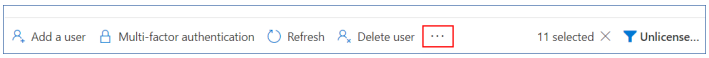
ライセンス対象外のユーザーのサインインを防止するには

1. Microsoft 365 管理センター（https://admin.microsoft.com）にグローバル管理者としてログインします。
2. ナビゲーションメニューで、**[ユーザー]** > **[アクティブユーザー]** に進みます。



3. [**フィルタ**] をクリックしてから、[**ライセンス対象外のユーザー**] を選択します。

4. ユーザー名の横にあるチェックボックスを選択してから、省略記号（...）のアイコンをクリックします。



5. メニューから、[**サインインステータスを編集**] を選択します。
6. [**ユーザーのサインインをブロック**] チェックボックスを選択してから、[**保存**] をクリックします。

アーカイブストレージクォータ

アーカイブストレージクォータは、カスタマーテナント向けにコスト効率の良いS3互換のオブジェクトストレージを可能にします。

クォータが有効になると、**アーカイブストレージ**タブがCyber Protectコンソールの**バックアップストレージ**の下に表示されます。

アーカイブストレージはソフトクォータモデルで運用され、厳格な上限を強制しません。使用量が設定されたクォータを超えても、サービスは利用可能で中断されません。

アーカイブストレージクォータ

アーカイブストレージクォータは、カスタマーテナント向けにコスト効率の良いS3互換のオブジェクトストレージを可能にします。

クォータが有効になると、**アーカイブストレージ**タブがCyber Protectコンソールの**バックアップストレージ**の下に表示されます。

アーカイブストレージはソフトクォータモデルで運用され、厳格な上限を強制しません。使用量が設定されたクォータを超えても、サービスは利用可能で中断されません。

Disaster Recovery制限値（クォータ）

注意
Disaster Recovery提供項目は、Disaster Recoveryサービスでのみ使用可能です。

これらの制限値（クォータ）は、サービスプロバイダーによって企業全体に適用されます。企業管理者は管理ポータルで制限値（クォータ）と使用状況を表示できますが、ユーザーの制限値（クォータ）は設定できません。

Microsoft Azure への Disaster Recovery では、次の提供項目が利用できます。

- **Azure への DR と直接バックアップ**
  Advanced Disaster Recovery とカスタマーの Azure サブスクリプションへの直接バックアップを有効にします。保護された各ワークロードに 1 つのクォータが割り当てられます。

Disaster Recovery から Cyber Protect Cloud まで、次の提供項目が利用可能です。

- **ディザスタリカバリストレージ**
  ディザスタリカバリストレージは、ディザスタリカバリで保護されているサーバーのバックアップストレージのサイズを示しています。ディザスタリカバリストレージの使用量は、ディザスタリカバリサーバーで保護されているワークロードのバックアップストレージの使用量と同じになります。このストレージサイズは、サーバーが現在稼働しているかどうかにかかわらず、復元サーバーが作成された時点から計算されます。このクォータの追加容量に達した場合、プライマリサーバーと復元サーバーの作成や、既存プライマリサーバーのディスクの追加/拡張は実行できなくなります。このクォータの追加容量を超過した場合、フェールオーバーの開始、または停止したサーバーの起動が実行できなくなります。実行中のサーバーは引き続き実行されます。
- **コンピュートポイント**
  この制限値（クォータ）は、請求期間中にプライマリおよびリカバリサーバーによって消費される CPU および RAM リソースを制限します。この制限値（クォータ）の追加容量に達した場合、すべてのプライマリおよびリカバリサーバーがシャットダウンされます。次の請求期間の開始までこれらのサーバーを使用することはできません。デフォルトの請求期間は完全な暦月です。
  制限値（クォータ）が無効に設定されている場合、請求期間に関係なくサーバーを使用することはできません。
- **パブリック IP アドレス**
  この制限値（クォータ）は、プライマリサーバーと復元サーバーに割り当てることができるパブリックIPアドレスの数を制限します。この制限値（クォータ）の追加容量に達した場合、それ以上サーバーにパブリックIPアドレスを有効にできなくなります。サーバー設定で **[パブリック IP アドレス]** チェックボックスをオフにすると、サーバーがパブリック IP アドレスを使用できないようにすることができます。その後、別のサーバーにパブリック IP アドレスを使用させることができます。パブリック IP アドレスは通常同じものではありません。
  制限値（クォータ）が無効にされている場合、すべてのサーバーがパブリックIPアドレスの使用を停止し、インターネットから到達できなくなります。
- **クラウドサーバー**
  この制限値（クォータ）はプライマリサーバーとリカバリサーバーの総数を制限します。この制限値（クォータ）の追加容量に達した場合、プライマリサーバーや復元サーバーを作成することはできません。
  制限値（クォータ）が無効になっている場合、サーバーはCyber Protectコンソールに表示されますが、利用できる操作は **[削除]** のみです。
- **インターネットアクセス**

この制限値（クォータ）は、プライマリサーバーと復元サーバーからのインターネットアクセスを有効または無効にします。

制限値（クォータ）が無効になると、プライマリサーバーと復元サーバーはインターネットへの接続を確立できません。

File Sync & Share制限値（クォータ）

テナントに対して以下のFile Sync & Shareクォータを定義できます:

- **ユーザー**

  File Sync & Shareのユーザー数の制限を定義します。

  注意
  UserおよびUser + Administratorのユーザーロールのみがこのクォータにカウントされます。
  AdministratorおよびGuestのユーザーロールはこのクォータから除外されます。

- **クラウドストレージ**

  テナントに割り当てられるクラウドストレージの上限を定義します。

Physical Data Shipping制限値（クォータ）

Physical Data Shippingサービスの制限値（クォータ）は、ドライブごとに消費されます。複数のマシンの最初のバックアップを、1台のハードドライブに保存できます。

テナントのために、以下のPhysical Data Shipping制限値（クォータ）を定義できます。

- **クラウドへ**

  初期バックアップをハードディスクドライブを使用してクラウドデータセンターに配送することを許可します。この制限値（クォータ）は、クラウドデータセンターへ移動されるドライブの最大数を定義します。

Notary制限値（クォータ）

テナントのために、以下のNotary制限値（クォータ）を定義できます。

- **Notaryのストレージ**

  公証済ファイル、署名済みファイル、および公証または署名が進行中のファイルの最大クラウドストレージスペースを定義します。

  このクォータの使用量を減らすには、既に公証済または署名済みのファイルを公証ストレージから削除します。

- **ノータリゼーション**

  公証サービスを使用して公証済にできる、最大のファイル数を定義します。

  ファイルは、公証ストレージにアップロードされるとすぐに公証済と見なされ、公証ステータスが **[実行中]** に変更されます。

  同じファイルが複数回ノータライズ（公証）されると、各ノータリゼーションは新しいノータリゼーションとしてカウントされます。

- **電子署名**
  デジタル電子署名の最大数を定義します。

ワークロードのサービスクォータの変更

ワークロードの保護レベルは、適用されるサービスクォータによって定義されます。サービスクォータは、ワークロードが登録されているテナントで利用可能な提供項目に関連します。

サービスクォータは、保護計画が最初にワークロードに適用されるときに、自動的に割り当てられます。

保護されているワークロードの種類、オペレーティングシステム、必要な保護レベル、クォータの可用性に応じて、もっとも適切なクォータが割り当てられます。組織内でもっとも適切なクォータが利用できない場合、次善に適切なクォータが割り当てられます。例えば、もっとも適切なクォータが**Webホスティングサーバー**であるものの、それが利用できない場合、**サーバー**のクォータが割り当てられます。

クォータ割り当ての例:

- Windows ServerまたはLinuxオペレーティングシステムを実行する物理マシンには、**サーバー**クォータが割り当てられます。
- Windowsのデスクトップオペレーティングシステムを実行する物理マシンには、**ワークステーション**クォータが割り当てられます。
- Hyper-Vロールが有効化されたWindows 10を実行する物理マシンには、**ワークステーション**クォータが割り当てられます。
- 仮想デスクトップインフラストラクチャ上で実行され、ゲスト オペレーティングシステム内にプロテクション エージェント（エージェントfor Windowsなど）がインストールされているデスクトップマシンには、**仮想マシン**クォータが割り当てられます。このタイプのマシンは、**仮想マシン**クォータが使用できない場合に**ワークステーション**クォータを使用することもできます。
- 仮想デスクトップインフラ上で動作し、エージェントレスモード（VMwareエージェントまたはHyper-Vエージェントなど）でバックアップされるデスクトップマシンには、**仮想マシン**クォータが割り当てられます。
- Hyper-VまたはvSphereサーバーには、**サーバー**クォータが割り当てられます。
- cPanelまたはPleskが動作するサーバーには、**Webホスティングサーバー**クォータが割り当てられます。また、**Webホスティングサーバー**クォータが使用できない場合、Webサーバーが実行されているマシンのタイプに応じて、**仮想マシン**または**サーバー**クォータを使用することもできます。
- アプリケーション認識型バックアップの場合、ワークステーションであっても**サーバー**クォータが必要です。

元の割り当ては後から手動で変更できます。たとえば、同じワークロードにさらに高度な保護計画を適用するには、ワークロードのサービスクォータをアップグレードする必要が生じる場合があります。その保護計画で必要となる機能が、現在割り当てられているサービスクォータでサポートされていない場合、保護計画は失敗します。

また、クォータの割り当てが行われた後に、より適切なクォータを購入した場合は、サービスクォータを変更できます。例えば、仮想マシンに**ワークステーション**クォータが割り当てられている場合がこれ

に相当します。**仮想マシン**クォータを購入した後、元の**ワークステーション**クォータではなく、購入したクォータをワークロードに手動で割り当てることができます。

また、現在割り当てられているサービスクォータを解放して、それを別のワークロードに割り当てることもできます。

個別ワークロードまたはワークロードのグループのサービスクォータを変更できます。

個別ワークロードのサービスクォータを変更するには

1. Cyber Protectコンソールで **[デバイス]** に進みます。
2. ワークロードを選択して、**詳細**をクリックします。
3. **[サービスクォータ]** セクションで、**[変更]** をクリックします。
4. **[クォータの変更]** ウィンドウで、サービスクォータまたは **[クォータなし]** を選択し、**[変更]** をクリックします。

ワークロードのグループのサービスクォータを変更するには

1. Cyber Protectコンソールで **[デバイス]** に進みます。
2. 複数のマシンを選択し、**[クォータの割り当て]** をクリックします。
3. **[クォータの変更]** ウィンドウで、サービスクォータまたは **[クォータなし]** を選択し、**[変更]** をクリックします。

ソリューションベースのライセンスにおけるMicrosoft 365シートの使用量計算の例

Microsoft 365およびGoogle Workspaceシートの最高レベルの保護を提供するために、アクロニスは、Microsoft 365のセキュリティ態勢管理を提供するOctigaや、Eメールセキュリティおよびコラボレーションアプリセキュリティサービスを提供するFortinetなどのトップレベルのサードパーティベンダーと提携しました。アクロニスのプラットフォームとベンダー側の会計およびレポートメカニズムは異なるため、二重計上が発生する可能性があります。

Cyber Protect Cloud プラットフォームでは、保護されている各シートに ID が割り当てられ、その ID に対して使用されるクォータが計上されます。シートがアクロニスの機能のみを使用している場合、使用状況のデータはシート ID ごとに報告され、計上されます。シートがベンダーの機能を使用している場合、ベンダーはこのシートを ID にマッピングせずに単位（数値）として報告します。各ソリューションには、アクロニスとベンダー提供の機能の両方が含まれており、外部サービスによって報告されるシートを明示的に識別することはできないため、二重計上を回避するためにプラットフォーム側で追加の計算が実行されます。この記事では、これらの計算ロジックについて説明し、Microsoft 365 シート保護における最も一般的なユースケースの例を示します。Google Workspace の使用状況を計算する際にも、同じロジックが使用されます。

ソリューションベースのライセンスにおける主要および二次的提供項目

以下の例をよりよく理解できるよう、このセクションの情報をお読みください。

ソリューションベースのライセンスでは、各ソリューションに、Microsoft 365シートと Google Workspaceシートの保護を制御する以下の主要な提供項目が含まれています。子テナントに対してソリューションを有効にする際に、管理ポータルでこれらの項目を選択し、ソフトクォータを設定できます。デフォルトでは、クォータは**[無制限]**に設定されています。

- セキュリティとRMM
  - Microsoft 365シート
  - Google Workspaceシート
- バックアップとDisaster Recovery
  - Microsoft 365シート
  - Google Workspaceシート
- 究極の 保護
  - Microsoft 365シート
  - Google Workspaceシート

各主要提供項目 (OI) には、より詳細なアカウント管理とレポート作成に使用される二次提供項目があります。二次提供項目 (OI) はテナント構成 UI では表示されず、個別に制御することはできませんが、透明性を確保するために使用状況レポートで利用できます。二次提供項目は、その親にあたる提供項目 (OI) が有効になったときに自動的に有効になり、その親 OI が無効になったときに自動的に無効になります。二次提供項目のクォータは常に無制限に設定されます。主要提供項目のクォータはデフォルトで無制限であり、必要に応じて変更できます。

注意
Microsoft 365 のシートと Google Workspace のシートのクォータは常にソフトクォータです。というのも、使用状況の制限はベンダー側でサポートされていないからです。

アクロニス独自のサービスは、提供されたシート ID で二次提供項目のシート数ごとの使用状況をレポートします。これにより、保護されたシートを明確に特定でき、二重計上を防止できます。

Octiga と Fortinet は、シート ID を提供せずに二次提供項目のシート数ごとのサービスの使用状況をレポートします。これにより、シートの二重計上が発生する可能性があります。たとえば、究極の保護の Microsoft 365シートのアーカイブと Microsoft 365 用のセキュリティ態勢管理のように、ソリューション内で 2 つ以上のサービスを使用するシートは、各サービスごとにレポートされます (2 ユニットとして)。

二重計上を避けるために、プラットフォームは、各ソリューション内の主要提供項目に集約するために、二次提供項目の使用状況を計算します。二重計上を避けるために適用されるメカニズムは、有効化されて使用されているソリューションによって異なります。「使用」とは、少なくとも 1 つの二次提供項目が保護されたシートによって使用されていることを意味します。

注意
次の例では、二次提供項目 (OI) が統合とのマッピングを容易にするために API 名で表示されます。主要提供項目 (OI) は、UI に表示される名前と API 名の両方で表示されます。

計算の例

例 1: すべてのソリューションが使用されている場合の使用状況の計算

すべてのソリューションが有効化されて使用されている場合、次のロジックが適用されます。

1. 各ソリューションの二次提供項目から最高の使用数を見つけます。
   この機能は、サービスベースのライセンスの標準保護機能に含まれ、ソリューションベースのライセンスのセキュリティとRMMまたは究極の保護ライセンスにも含まれます。たとえば、セキュリティとRMMが 50 の「セキュリティ」シートと 60 の「管理」シートを示す場合、60 を取得します。

   注意
   一部の二次提供項目は無料で利用でき、その値は計算から除外されます。

2. 究極の保護ソリューションをベースとして考慮します。
   なぜ「究極の保護」をベースとして考慮するのか？「究極の保護」の主要な提供項目である**Microsoft 365シート**には、セキュリティとRMMとBackup and Disaster Recoveryソリューションの両方の二次提供項目が含まれています。保護されたシートがセキュリティおよびRMMとBackup and Disaster Recoveryソリューションの両方のサービスを使用する場合、可能であれば自動的に「究極の保護」に切り替わります。「究極の保護」のユニット数は常に両方のサービスを使用するライセンス数を示し、この数はセキュリティとRMMまたはBackup and Disaster Recoveryのみを使用するライセンス数から引かれます。
3. 究極の保護の使用数を他のソリューション（セキュリティおよびRMM、Backup and Disaster Recovery）の使用数から引き算し、重複するライセンスに対しては請求書発行を1回にします。
   結果が負の値の場合は、0に変換します。
4. 主要提供項目の計算結果を表示します。

セキュリティとRMM		バックアップとDisaster Recovery		究極の保護	
提供項目名	使用状況	提供項目名	使用状況	提供項目名	使用状況
Microsoft 365シート bndl_secrmm_m365_seats	**30**	**Microsoft 365シート** bndl_bdr_m365_seats	**15**	**Microsoft 365シート** bndl_ult_m365_seats	**30**
bndl_secondary_m365_seats_security	50				
bndl_secondary_m365_seats_management	60				
bndl_secondary_m365_seats_management_freeexcluded	90				
		bndl_bdr_secondary_m365_	30		

セキュリティとRMM		バックアップとDisaster Recovery		究極の保護	
		seats_backup			
		bndl_bdr_secondary_m365_seats_sharedexcluded	60		
		bndl_secondary_m365_sharepoint_sitesexcluded	2		
		bndl_secondary_m365_teamsexcluded	4		
		bndl_secondary_gworkspace_team_driveexcluded	10		
		bndl_secondary_m365_seats_archiving	45		
				bndl_ult_secondary_m365_seats_backup	0
				bndl_ult_secondary_m365_seats_shared	5
				bndl_ult_secondary_m365_seats_backup_advanced	30
				bndl_secondary_m365_seats_collaboration_apps	10
使用状況の計算手順					
各ソリューションの二次提供項目の中から最大使用量を見つけます。 無料で利用できる提供項目は考慮しません。	60		45		30
2. 究極の保護の最大値から他の2	60		45		使用

セキュリティとRMM		バックアップとDisaster Recovery		究極の保護	
つのソリューションの最大値を引きます	引く 30		引く 30		不可
結果	30		15		30

例2: 「究極の保護」のみが有効な場合の使用量の計算

究極の保護のみが有効な場合、二次提供項目の使用量の中で最も高い数値が実際の使用量として計上されます。

究極の保護	
提供項目名（API）	使用状況
究極の保護 bndl_ult_m365_seats	**60**
bndl_secondary_m365_seats_security	50
bndl_secondary_m365_seats_management	60
bndl_secondary_m365_seats_management_freeexcluded	90
bndl_ult_secondary_m365_seats_backup	30
bndl_ult_secondary_m365_seats_shared	5
bndl_secondary_m365_sharepoint_sitesexcluded	2
bndl_secondary_m365_teamsexcluded	4
bndl_secondary_gworkspace_team_driveexcluded	10
bndl_secondary_m365_seats_archiving	45
bndl_ult_secondary_m365_seats_backup_advanced	30
bndl_secondary_m365_seats_collaboration_apps	10
使用状況の計算手順	
1. 二次提供項目の中から最大使用量を見つけます。 無料で利用できる提供項目は計算しません。	60
結果	60

例3: セキュリティとRMMおよび究極の保護が有効な場合の使用量の計算

セキュリティとRMMおよび究極の保護ソリューションが有効で使用されている場合、次のロジックが適用されます。

1. 両方のソリューションの二次提供項目から最高の使用量を見つけます。

   注意
   一部の二次提供項目は無料で利用できるため、その値は計算から除外されます。

2. Ultimate Protectionの使用量をSecurityおよびRMMの使用量から引き算し、重複するライセンスは1回のみ請求されるようにします。
   結果が負の値の場合は、0に変換します。
3. 主要提供項目の計算結果を表示します。

セキュリティとRMM		**究極の保護**		
提供項目名（API）	使用状況	提供項目名（API）	使用状況	
Microsoft 365シート bndl_secrmm_m365_seats	**15**	**Microsoft 365シート** bndl_ult_m365_seats	**45**	
bndl_secondary_m365_seats_security	50			
bndl_secondary_m365_seats_management	60			
bndl_secondary_m365_seats_management_freeexcluded	90			
		bndl_ult_secondary_m365_seats_backup	30	
		bndl_ult_secondary_m365_seats_shared	5	
		bndl_secondary_m365_sharepoint_sitesexcluded	2	
		bndl_secondary_m365_teamsexcluded	4	
		bndl_secondary_gworkspace_team_driveexcluded	10	
		bndl_secondary_m365_seats_archiving	45	
		bndl_ult_secondary_m365_seats_backup_advanced	30	
		bndl_secondary_m365_seats_collaboration_apps	10	
使用状況の計算手順				

セキュリティとRMM		究極の保護	
1. セキュリティとRMMと究極の保護ソリューションの二次OIの中から最大の使用量を見つけます。 無料で利用できる提供項目は計算しません。	60		45
2. 究極の保護の最大使用量をセキュリティとRMMの最大使用量から引き算します。	60-45		-
結果	**15**		**45**

例4: Backup and Disaster Recoveryおよび究極の保護が有効な場合の使用量の計算

Backup and Disaster Recoveryおよび究極の保護ソリューションが有効な場合、次のロジックが適用されます。

1. 両方のソリューションの二次提供項目から最高の使用量を見つけます。

   注意
   一部の二次提供項目は無料で利用できるため、その値は計算から除外されます。

2. 究極の保護の使用量からBackup and Disaster Recoveryの使用量を引き、重複するシートが1回だけ請求されるようにします。
   結果が負の値の場合は、0に変換します。
3. 主要提供項目の計算結果を表示します。

バックアップとDisaster Recovery		究極の保護	
提供項目名（API）	使用状況	提供項目名（API）	使用状況
Microsoft 365シート bndl_bdr_m365_seats	**0**	**Microsoft 365シート** bndl_ult_m365_seats	**60**
bndl_bdr_secondary_m365_seats_backup	30		
bndl_bdr_secondary_m365_seats_sharedexcluded	60		
bndl_secondary_m365_sharepoint_sitesexcluded	2		
bndl_secondary_m365_teamsexcluded	4		
bndl_secondary_gworkspace_team_driveexcluded	10		
bndl_secondary_m365_seats_archiving	45		
		bndl_secondary_m365_seats_security	50
		bndl_secondary_m365_seats_management	60

バックアップとDisaster Recovery		究極の保護	
		bndl_secondary_m365_seats_management_freeexcluded	90
		bndl_ult_secondary_m365_seats_backup	0
		bndl_ult_secondary_m365_seats_shared	5
		bndl_ult_secondary_m365_seats_backup_advanced	30
		bndl_secondary_m365_seats_collaboration_apps	10
使用状況の計算手順			
1. Backup and Disaster Recoveryおよび究極の保護ソリューションの二次提供項目の中で最大の使用量を見つけます。 無料で利用できる提供項目は計算しません。	45		60
2. 究極の保護の最大使用量をBackup and Disaster Recoveryの最大使用量から引きます。 結果が負の値の場合は、0に変換します。	45 引く 60 は -15		
結果	**0**		**60**

例5: セキュリティとRMMおよびBackup and Disaster Recoveryの両方が使用されている場合の使用量の計算

セキュリティとRMMおよびBackup and Disaster Recoveryソリューションが有効になっている場合、次のロジックが適用されます。

1. 両方のソリューションの二次提供項目から最高の使用量を見つけます。

> **注意**
> 一部の二次提供項目は無料で利用できるため、その値は計算から除外されます。

2. 各主要提供項目の結果を表示します。

セキュリティとRMM		バックアップとDisaster Recovery	
提供項目名（API）	使用状況	提供項目名（API）	使用状況

セキュリティとRMM		バックアップとDisaster Recovery	
Microsoft 365シート bndl_secrmm_m365_seats	**60**	**Microsoft 365シート** bndl_bdr_m365_seats	**45**
bndl_secondary_m365_seats_security	50		
bndl_secondary_m365_seats_management	60		
bndl_secondary_m365_seats_management_freeexcluded	90		
		bndl_bdr_secondary_m365_seats_backup	30
		bndl_bdr_secondary_m365_seats_sharedexcluded	60
		bndl_secondary_m365_sharepoint_sitesexcluded	2
		bndl_secondary_m365_teamsexcluded	4
		bndl_secondary_gworkspace_team_driveexcluded	10
		bndl_secondary_m365_seats_archiving	45
使用状況の計算手順			
1. セキュリティとRMM、Backup and Disaster Recoveryソリューションの二次提供項目の中で最大使用値を見つけます。 無料で利用できる提供項目は計算しません。	60		45
結果	**60**		**45**

例6: セキュリティとRMMのみを使用している場合の使用量の計算

1. セキュリティと RMM > **Microsoft 365シート**提供項目の二次提供項目から最も高い使用数を見つけます。

   注意
   一部の二次提供項目は無料で利用できるため、その値は計算から除外されます。

2. 主要提供項目の計算結果を表示します。

セキュリティとRMM	
提供項目名（API）	使用状況
Microsoft 365シート bndl_secrmm_m365_seats	**60**
bndl_secondary_m365_seats_security	50
bndl_secondary_m365_seats_management	60
bndl_secondary_m365_seats_management_freeexcluded	90
使用状況の計算手順	
1. セキュリティと RMM > **Microsoft 365シート**提供項目で、二次提供項目の最大使用値を見つけます。 無料で利用できる提供項目は計算しません。	60
結果	**60**

例 7: Backup and Disaster Recoveryのみを使用した場合の使用量の計算

1. バックアップとDisaster Recovery > **Microsoft 365** OI のセカンダリ提供項目から最も高い使用数を見つけます。

   注意
   一部の二次提供項目は無料で利用できるため、その値は計算から除外されます。

2. 主要提供項目の計算結果を表示します。

バックアップとDisaster Recovery	
提供項目名（API）	使用状況
Microsoft 365シート bndl_bdr_m365_seats	**45**
bndl_bdr_secondary_m365_seats_backup	30
bndl_bdr_secondary_m365_seats_sharedexcluded	60
bndl_secondary_m365_sharepoint_sitesexcluded	2
bndl_secondary_m365_teamsexcluded	4
bndl_secondary_gworkspace_team_driveexcluded	10
bndl_secondary_m365_seats_archiving	45
使用状況の計算手順	

バックアップとDisaster Recovery	
1. Backup and Disaster Recovery ソリューションの二次提供項目の中から、最大の使用量の値を見つけます。 無料で利用できる提供項目は計算しません。	45
結果	**45**

ストレージ計算の例

バックアップ用の空き容量は、一部の提供項目に含まれています。詳細については、パートナーポータルのライセンスガイドを参照してください。

このトピックでは、 クラウドのストレージスペースの使用と請求書の計算の例を示します。

重要
以下の例は、正確な請求書情報ではありません。ストレージ使用量の計算に適用される原則を例示する目的で使用されています。

例: 使用済みストレージが含まれているストレージよりも少ない

含まれているストレージは、単一のストレージプールに集約されます。テナントのすべてのワークロードは、まず、このストレージがいっぱいになるまで使用します。

ワークロードライセンス	含まれるストレージ	使用済みストレージ
サーバー x 3	3 x 3TB = 9TB	10 TB
仮想マシン x 2	2 x 2TB = 4TB	2 TB
ワークステーション x 5	500GB x 5 = 1.5TB	2 TB
保護対象のワークロード合計 = 10	含まれるストレージ合計 = 14.5TB	使用済みストレージ合計 = 21TB
		請求対象のストレージ = 0

例: 使用済みストレージは含まれるストレージと等しい

含まれているストレージは 1 つのストレージプールに集約され、すべてのワークロードがそれを消費しますが、上限を超えることはありません。

ワークロードライセンス	含まれるストレージ	使用済みストレージ
サーバー x 3	3 x 3TB = 9TB	12 TB

ワークロードライセンス	含まれるストレージ	使用済みストレージ
仮想マシン x 2	2 x 2TB = 4TB	1 TB
ワークステーション x 5	500GB x 5 = 1.5TB	1.5 TB
保護対象のワークロード合計 = 10	含まれるストレージ合計 = 14.5TB	使用済みストレージ合計 = 14.5TB
		請求対象のストレージ = 0

例: 使用済みストレージが含まれているストレージを超えている

含まれるストレージは 1 つのストレージプールに集約され、すべてのワークロードがそれを消費します。含まれるストレージが超過すると、使用済みストレージが含まれるストレージから差し引かれ、差額が請求書発行されます。

ワークロードライセンス	含まれるストレージ	使用済みストレージ
サーバー x 3	3 x 3TB = 9TB	15 TB
仮想マシン x 2	2 x 2TB = 4TB	5 TB
ワークステーション x 5	500GB x 5 = 1.5TB	1 TB
保護対象のワークロード合計 = 10	含まれるストレージ合計 = 14.5TB	使用済みストレージ合計 = 21TB
		請求対象のストレージ = 6.5TB

注意
ストレージの価格は、選択したライセンスモードによって異なる場合があります。価格表を確認してください。

同様に、テナントの子テナントの使用量は共通のプルに集約され、親テナントには超過使用分のみが請求書発行されます。

Cyber Protect Cloud のサービス

クラウドサービスは、パートナーによって、またはエンドカスタマーのプライベートクラウドでホストされる機能を組み合わせたものです。通常は、サービスはサブスクリプションか従量課金ベースで販売されます。

Cyber Protect Cloud はサイバーセキュリティ、データ保護、管理を統合し、サイバーセキュリティの脅威からエンドポイント、システム、データを保護します。 いくつかのサービスで構成されています: 保護、File Sync & Share、物理データ配送、サイバーインフラストラクチャです。これらの一部は、追加のサービスを有効にすることで拡張できます。

- **保護** - 基礎製品に含まれるセキュリティおよび管理機能、ディザスタリカバリ、バックアップと復元、自動化、Eメールセキュリティを従量課金制の機能として利用できる、完全なサイバープロテクション。サービスには迅速かつ簡単なライセンス管理のためのソリューションベースと、より柔軟できめ細かいサービス制御のためのサービスベース（ワークロードごと、ギガバイトごと）の2つのライセンスモードがあります。各ライセンスモードは、標準の提供項目のセットで構成されており、追加の保護サービスで拡張できます（追加料金が発生します）。
  パートナーポータルの "ライセンスモード"（9ページ） およびライセンスガイドを参照してください。
- **File Sync & Share** - いつでも、どこでも、どのデバイスからでも企業のコンテンツを安全に共有するためのソリューション。共有されたコンテンツの真正性は、ブロックチェーン技術により保証されます。
- **物理データ配送** - ハードドライブで最初のバックアップデータをクラウドデータセンターへ転送することで、時間とネットワークトラフィックを節約できるソリューション。
- **Cyber Infrastructure** - プロダクトキーの代わりに Cyber InfrastructureのService Provider License Agreement（SPLA）を使用できます。

パートナーテナントとして、管理ポータルのどのサービスを子テナントで利用可能にするか選択できます。構成はテナントごとに行われ、テナントの編集またはプロビジョニング時に行われます（テナントの作成を参照）。

標準および追加の保護サービス

利用可能な標準サービスと追加サービスは、選択したライセンスモードによって異なります。

追加のサービスは、選択したライセンスに含まれるサービスの上に有効にすることができます。追加のサービスは、標準のライセンスに含まれる機能と重複しない独自の機能を提供します。クライアントは、1つまたは複数の追加サービスを使用して、ワークロードを保護できます。追加のサービスは、サービスベースのライセンス（ワークロード単位およびギガバイト単位）と、ソリューションベースのライセンスの両方で利用できます。

重要

- カスタマーテナントに対しては、ソリューションベースまたはサービスベースのいずれかのライセンスモードを 1 つだけ有効にできます。
- すべてのライセンスモードとすべての提供項目をパートナーまたはフォルダテナントに対して有効にできます。

ソリューションベースのライセンスにおける標準サービス

次の表には、ワークロードの種類ごとに利用可能な機能に関する情報が含まれています。

ワークロード	セキュリティとRMM	バックアップとDR1	究極の保護1
エンドポイント （ワークステーション、サーバー、仮想マシン、Web ホスティングサーバー）	• Active protection • アンチマルウェア保護 • Endpoint Detection and Response （EDR） • Extended Detection and Response（XDR） • リモート管理および監視（RMM）	なし	なし
サーバー	サーバーのセキュリティとRMMは、"エンドポイント"（42ページ）提供項目を介して有効化されます。	• バックアップ • Disaster Recovery	• バックアップ • Advanced Backup • Disaster Recovery • Active protection • アンチマルウェア保護 • Endpoint Detection and Response （EDR）

ワークロード	セキュリティとRMM	バックアップとDR1	究極の保護1
			• Extended Detection and Response（XDR） • リモート管理および監視（RMM） • データ漏洩防止
仮想コンピュータ	"エンドポイント"（42ページ）提供項目に含まれています。	• バックアップ • アクロニスまたはパートナーがホストする環境へのDisaster Recovery • AzureへのDisaster Recovery	• バックアップ • Advanced Backup • Disaster Recovery • Active protection • アンチマルウェア保護 • Endpoint Detection and Response（EDR） • Extended Detection and Response（XDR） • リモート管理および監視（RMM） • データ漏洩防止
ワークステーション	"エンドポイント"（42ページ）提供項目に含まれています。	• バックアップ • AzureへのDisaster Recovery	• バックアップ • Azureへの Disaster Recovery • Advanced Backup • Active protection • アンチマルウェア保護 • Endpoint Detection and

ワークロード	セキュリティとRMM	バックアップとDR[1]	究極の保護[1]
			Response（EDR） • Extended Detection and Response（XDR） • リモート管理および監視（RMM） • データ漏洩防止
モバイルデバイス	なし	• バックアップ	なし
Web サイト	なし	• バックアップ	なし
Microsoft 365	• Eメールセキュリティ • セキュリティ体制の管理	• バックアップ • Eメールアーカイブ	• バックアップ • Advanced Backup • Eメールアーカイブ • Eメールセキュリティ • Collaboration Security • セキュリティ体制の管理
Google Workspace	• Eメールセキュリティ	• バックアップ	• バックアップ • Direct Backup to Public Cloud • Eメールセキュリティ

1 このソリューションの各提供項目には、一定量の無料ストレージが含まれています。パートナーポータルのライセンスガイドを確認してください。

重要
同じワークロードに複数の提供項目を組み合わせることはできません。たとえば、同じワークステーションにセキュリティとRMM、バックアップとDRの両方を適用することはできません。代わりに、究極の保護を使用する必要があります。両方のソリューションの機能が保護計画に含まれている場合、保護されたワークロードのライセンスは自動的に究極の保護に切り替わります。

ソリューションベースのライセンスを使用すると、次の追加サービスを有効にできます。

- マネージド検知と応答
  セキュリティとRMMのエンドポイントおよび究極の保護のサーバー、仮想マシン、ワークステーションと互換性があります。
- セキュリティ意識向上トレーニング
- ホステッドクラウドストレージ（超過用）
- ジオレプリケーション
- Disaster Recoveryインフラストラクチャ

Notarization and eSignatureサービスは、File Sync & Shareサービスで有効にできます。ユーザー単位とギガバイト単位の両方の請求書発行モードで利用できます。

サービスベースのライセンスにおける標準機能と追加サービス

保護サービスの両方のサービスベースのライセンスモードの機能は同じです。

次の表は、標準保護の提供項目と追加サービスで利用できる機能をまとめたものです。

注意
追加サービスは、拡張するサービスが有効になっている場合にのみ使用できます。標準サービスの機能が無効になっている場合、ユーザーは追加サービスを使用できません。たとえば、保護機能が無効の場合、ユーザーはAdvanced Backupサービスの機能を使用できません。

保護 サービスの標準機能と追加サービス

[保護] の下で [標準保護] サービスを有効にすると、デフォルトで含まれている多くの機能が有効になります。さらに、追加のサービスを有効にすることもできます。

次の表には、Cyber Protect サービス機能と追加サービスの概要が示されています。提供製品の完全なリストについては、パートナーポータルの「ライセンスガイド」を参照してください。

保護サービスの標準および追加サービス

機能グループ	標準保護	追加サービス
Detection and Responseライセンス	• #CyberFit スコア • 脆弱性診断 • ウイルス対策およびマルウェア対策保護:クラウド署名ベースファイル検出（リアルタイム保護ではなく、スケジュールスキャンのみ）* • ウイルス対策およびマルウェア対策保護:実行前AIベースファイル分析ツール、ふるまいベースCyber Engine • Microsoft Defender管理 *ゼロデイ攻撃の検出には、Cyber Protect	Detection and Responseサービスには、XDR、Endpoint Detection and Response（EDR）、Managed Detection and Response（MDR）が含まれます。 • Advanced Email Security、Microsoft 365コラボレーションアプリケーション、Microsoft Entra IDなどのサードパーティ製品との統合 • 集中管理されたインシデントページでインシデントを管理 • インシデントのスコープと影響を可視

機能グループ	標準保護	追加サービス
	がヒューリスティックスキャンルールと悪意のあるコマンドを探すアルゴリズムを使用します。	化 • 推奨事項と修復手順 • 脅威フィードを使用して、一般に公開されている、ワークロードに対する攻撃を確認 • セキュリティイベントを180日間保存 • Managed Detection and Response（MDR） • ランサムウェア対策保護:Active Protection • ローカル署名ベースの検出によるウイルス対策およびマルウェア対策保護（リアルタイム保護） • エクスプロイト防御 • URLフィルタ処理 • エンドポイントファイアウォールの管理 • フォレンジックバックアップ、マルウェアに対応するバックアップスキャン、安全な復元、社内許可リスト • スマート保護計画（CPOCアラートとの統合） • マルウェアに対応する集中管理バックアップスキャン • リモートワイプ • Microsoft Defender Antivirus • Microsoft Security Essentials • Microsoft 365メールボックスのマルウェアのバックアップスキャン XDRサービスを有効にする方法については、"XDRの有効化"（51ページ）を参照してください。
データ漏洩防止	• デバイス制御	データ損失防止（DLP）サービス: • 周辺デバイスやネットワーク通信を介したワークロードのデータ漏洩をコンテンツ認識方式で防止 • 個人を特定できる情報（PII）、保護された医療情報（PHI）、PCI DSS（Payment Card Industry Data Security Standard、決済カード業界データセキュリティ基準）データ、お

機能グループ	標準保護	追加サービス
		よび「機密扱い」カテゴリの文書を事前に自動検出 • データ漏洩防止ポリシーの自動作成（オプションでエンドユーザーアシスタンス付き） • 自動学習ベースのポリシー調整による適応型のデータ漏洩防止措置 • クラウドベースの集中管理監査ログ、アラート、エンドユーザー通知
RMM	エンドポイントの場合: • グループ管理 • 保護計画の集中管理 • ハードウェアインベントリ • リモート制御 • リモート操作 • 技術者1人あたりの同時接続数 • リモート接続プロトコル: RDP • 4個のモニタ • しきい値ベースの監視 • 最終ログインユーザーの表示 • WindowsとmacOSの脆弱性診断	RMM サービスには、次の機能が含まれます。 エンドポイントの場合: • パッチ管理 • ディスク状態 • ソフトウェアインベントリ • Windowsオペレーティングシステムのサードパーティ製品の脆弱性診断 • フェールセーフパッチ • サイバースクリプト処理 • リモートアシスタンス • ファイル転送と共有 • 接続するセッションを選択 • マルチビューでワークロードを観察 • 接続モード: 制御、表示のみ、カーテン • クイックアシストアプリケーションによる接続 • リモート接続プロトコル:NEARとApple Screen Sharing • NEAR接続のセッション記録 • スクリーンショット送信 • セッション履歴リモート • 24個のモニタ • しきい値ベースの監視 • アノマリベースの監視 • DeployPilotによるリモートソフトウェア配置 • サードパーティのWindowsアプリケーションの脆弱性診断 • 位置情報トラッキング • ヘルプデスクチャット Microsoft 365シートの場合:

機能グループ	標準保護	追加サービス
		• Microsoft 365セキュリティポスチャをベストプラクティスのベースラインで監査し、ベースラインの逸脱を自動および手動で修正し、ユーザー管理、オンボーディング、およびオフボーディングを行います。
Eメールセキュリティ	なし	Microsoft 365やGmailのメールボックスのリアルタイム保護: • マルウェア対策、スパム対策 • Eメール内のURLスキャン • DMARC分析 • フィッシング対策 • なりすまし防止 • 添付ファイルのスキャン • コンテンツの対処と再構築 • 信頼性の可視化 「構成ガイド」を参照してください。
セキュリティ意識向上トレーニング		• セキュリティ意識向上トレーニング • コンプライアンストレーニング • フィッシングシミュレーション • ポリシー確認管理
Disaster Recovery	Demo Disaster Recovery標準機能を使用して、ワークロードのDisaster Recoveryシナリオをテストできます。 利用可能なDisaster Recovery標準機能と、その制限事項にご注意ください: • 隔離されたネットワーク環境でフェールオーバーをテスト。1か月あたりの計算ポイントを32に制限、同時テストフェールオーバー操作最大5回。 • 復元サーバーの構成:1基のCPUおよび2GBのRAM、1基のCPUおよび4GBのRAM、2基のCPUおよび8GBのRAM。 • フェールオーバーに利用できる復元ポイントの数: バックアップ直後に利用できる直近の復元ポイントのみ。 • 利用可能な接続モード:クラウド限定およびポイントツーサイト。 • VPNゲートウェイのアベイラビリティー:直近のテストフェールオーバー	Disaster Recoveryサービスを有効にして、すべてのDisaster Recovery機能を使用してワークロードを保護できます。 • 本番フェールオーバー • 隔離されたネットワーク環境でフェールオーバーをテスト。 • フェールオーバーに利用できる復元ポイントの数: 復元サーバーの作成後に利用可能なすべての復元ポイント。 • プライマリサーバー • 復元/プライマリサーバー構成:制限なし • 利用可能な接続モード:クラウド限定、ポイントツーサイト、サイト間Open VPN、マルチサイトIPsec VPN。 • VPNゲートウェイのアベイラビリティー: 常に利用可能。 • クラウドネットワークの数:23。 • パブリック IP アドレス • インターネットアクセス

機能グループ	標準保護	追加サービス
	の完了後4時間アクティブでない場合、VPNゲートウェイは一時停止し、テストフェールオーバーの開始時に再度配置されます。 • クラウドネットワークの数:1. • インターネットアクセス • ランブックの操作: 作成と編集。	• ランブックの操作: 作成、編集、実行。

追加サービスが有効になっている場合、その機能は保護計画に表示され、追加サービスアイコン でマークされます。ユーザーが保護計画で機能を有効にすると、追加の請求書発行が適用される旨の警告が表示されます。

追加サービスが有効化されておらず、アップセルがオンになっている場合、追加サービス機能は保護計画に表示されますが、使用することはできません。管理者に連絡して必要な追加サービスを有効にするように求めるメッセージが、ユーザーに表示されます。

追加サービスが有効ではなく、アップセルがオフになっている場合、カスタマーの保護計画には追加機能が表示されません。

保護サービスの従量課金と追加サービス

保護サービスの従量課金と追加サービス

機能グループ	従量課金制機能	追加サービス
バックアップ	• ファイルのバックアップ • イメージバックアップ • アプリケーションバックアップ • ネットワーク共有バックアップ • クラウドストレージへのバックアップ • ローカルストレージへのバックアップ • ワンクリック復元 • 継続的データ保護 • Microsoft SQL Serverクラスターおよびマイクロソフト Exchangeクラスターのバックアップをサポート - Always On Availability Groups（AAG）およびデータベース可用性グループ（DAG） • MariaDB、MySQL、Oracle DB、SAP HANAのバックアップをサポート • データ保護マップおよびコンプライアンスレポート • オフホストのデータ処理 • Microsoft 365およびGoogle	Direct Backup to Public Cloud

機能グループ	従量課金制機能	追加サービス
	Workspaceワークロードのバックアップ間隔 • ブータブルメディアのリモート操作 **注意** クラウドストレージの使用状況に応じた料金が適用可能です。	
File Sync & Share	• 暗号化済みファイルベースのコンテンツを保存 • すべての専用デバイス間でファイルを同期 • 専属ユーザーおよび専用システムとフォルダやファイルを共有	Notarization and eSignature サービス: • 公証と電子署名 • 文書テンプレート* *同期および共有ファイルのバックアップ
物理データ配送	物理データ配送機能	なし

注意
追加保護サービスを有効にするには、該当の拡張に対応する標準保護機能を有効にする必要があります。機能を無効にすると、その追加サービスは自動的に無効になり、そのパックを使用する保護計画も自動的に取り消されます。たとえば、保護機能を無効にすると、そのサービスが自動的に無効になり、そのパックを使用するすべての計画が取り消されます。

ユーザーは、標準保護なしで追加サービスを使用することはできませんが、特定のワークロードで追加サービスと一緒に標準保護のみを使用できます。

請求書発行とライセンスに関する情報については、パートナーポータルの「ライセンスガイド」を参照してください。

データ漏洩防止

Data Loss Prevention (DLP) モジュールは、実行モードで、ローカルおよびネットワークチャネルを介して転送されるデータのコンテンツを検査し、組織固有のデータフローポリシールールを適用することにより、ワークステーション、サーバー、仮想マシンから機密情報が漏洩することを防止します。

Data Loss Preventionモジュールの使用を開始する前に、『基本ガイド』に記載されている Data Loss Prevention管理の基本概念と論理構造を読み、理解していることを確認します。

また、『技術仕様』文書も参照してください。

Data Loss Preventionサービスの有効化

デフォルトでは、Data Loss Prevention は、究極の保護ライセンスまたは両方のサービスベースのライセンスを持つ新しいテナントの構成で有効になっています。テナント作成プロセス中に機能が無効になっている場合、パートナー管理者は後で機能を有効にできます。

Advanced Data Loss Preventionを有効化するには

1. 管理ポータルで **[クライアント]** へ進みます。
2. パートナーまたはカスタマーを編集のために開きます。
3. バックアップを有効にする:
   a. [サービスベースのライセンスの場合] **設定**セクションで、適用する請求書発行モードの下で**Data Loss Prevention**を選択し、保護するワークロードのクォータを構成します。
   b. [ソリューションベースのライセンスの場合] **究極の保護**ライセンスを有効にし、保護するエンドポイントを選択してから、クォータを構成します。

   デフォルトでは、クォータはすべてのエンドポイントで無制限に設定されています。
4. 設定を保存します。

XDR

XDR（Extended Detection and Response）サービスは、MSP向けに目的に沿って設計された、完全でネイティブに統合された、高度に効率的なソリューションを提供します。すべてのマルウェアの脅威からワークロードを継続的に保護します。XDRサービスは、Extended Detection and Response（XDR）、Endpoint Detection and Response（EDR）、および"Managed Detection and Response（MDR）"（60ページ）で構成されています。

XDRを使用して、次のことを行います。

- エンドポイント、Eメール、Microsoft Entra ID、Microsoft 365アプリケーション（SharePoint、OneDrive、Teams）に対応する包括的な可視性により、クライアント環境の保護を脆弱性のある対象領域の全体に拡張し、高度な脅威から確実に保護します。
- サイバーセキュリティ、データ保護、エンドポイント管理をネイティブに統合します。XDRは、ビジネス継続性を実現するために、脆弱な攻撃対象を保護するように設計されています。
- セキュリティサービスの起動、管理、拡張、および提供を簡単に行うことができるため、効率が向上します。また、XDRには、AIベースのインシデント分析、調査を簡単に実行できるワンクリックの応答、すべてのサービスに対応する単一のエージェントとコンソール、追加ツールをテクノロジースタックに統合するためのカスタマイズ可能なプラットフォームが含まれています。

XDRの有効化

パートナー管理者は、XDR保護サービスを有効にすることで、クライアントの保護計画に Extended Detection and Response（XDR）機能を提供することができます。

注意
保護対象とするすべてのワークロードの保護計画で、Endpoint Detection and Response（EDR）も有効にする必要があります。詳細については、EDR の有効化を参照してください。

XDRサービスを有効にするには

1. 管理ポータルにログインします。

   注意
   プロンプトが表示されたら、XDRサービスを適用するクライアントを選択し、**[有効化]** をクリックします。

2. 左側のナビゲーションペインで、**[クライアント]** をクリックします。
3. Cyber Protect以下の、**[保護]** タブをクリックします。
   プロテクションサービスをサブスクライブしている既存のクライアントの一覧が表示されます。
4. XDRパックを追加するクライアントをクリックします。
   [設定] タブで、**[保護]**セクションの下にある **[XDR]** チェックボックスが選択されていることを確認します。

XDRとサードパーティプラットフォームの統合

XDRは、次の統合をサポートします。

- Perception Point
- Microsoft 365サービス
- Fortinet

統合にアクセスするには、管理ポータルで **[統合]** に移動します。

注意
この機能は、管理者ロールを割り当てられたユーザーのみが使用できます。

Perception Pointとの統合

このトピックでは、Perception Pointと XDRの統合方法について説明します。

この統合により、Eメールセキュリティとコラボレーションアプリでmicrosoft 365を使用するカスタマーに対し、XDR（Extended Detection and Response）ソリューションを提供できます。XDR統合により、Perception Pointを使用する既存のEDR（Endpoint Detection and Response）ソリューションの機能が強化されます。

Perception PointをXDRと統合する主な手順は、以下のとおり3つあります。

1. 必要な保護サービスを有効にします。
2. Perception Pointで、Eメールセキュリティやコラボレーションアプリチャネルを設定し、APIキーを抽出する。
3. カスタマーのPerception Point XDR統合を有効にする。

必要な保護サービスを有効にするには

1. 管理ポータルで、統合を有効にするカスタマーにアクセスします。
2. ライセンスモードに依存するサービスを有効にします。

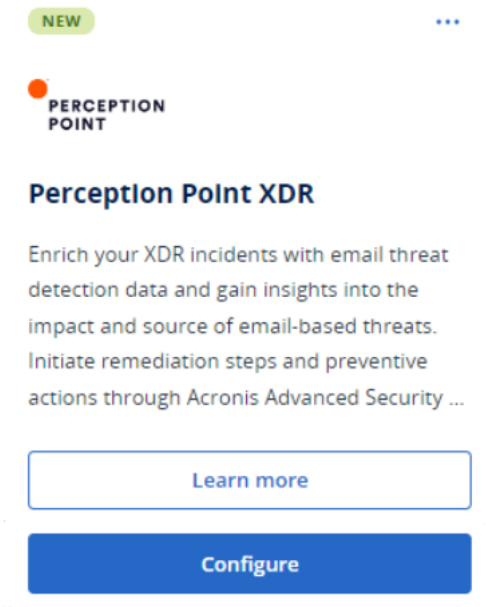
- ソリューションベースのモード: **セキュリティとRMM**または**究極の保護**を有効にします。
- サービスベースのモード: **Detection and Response**、**Detection and Response**サービス、および**Email and Collaboration Security**サービスを有効にします。詳細については、"標準および追加の保護サービス"（42ページ）を参照してください。

Perception Pointで、Eメールセキュリティやコラボレーションアプリチャネルを設定し、APIキーを抽出するには

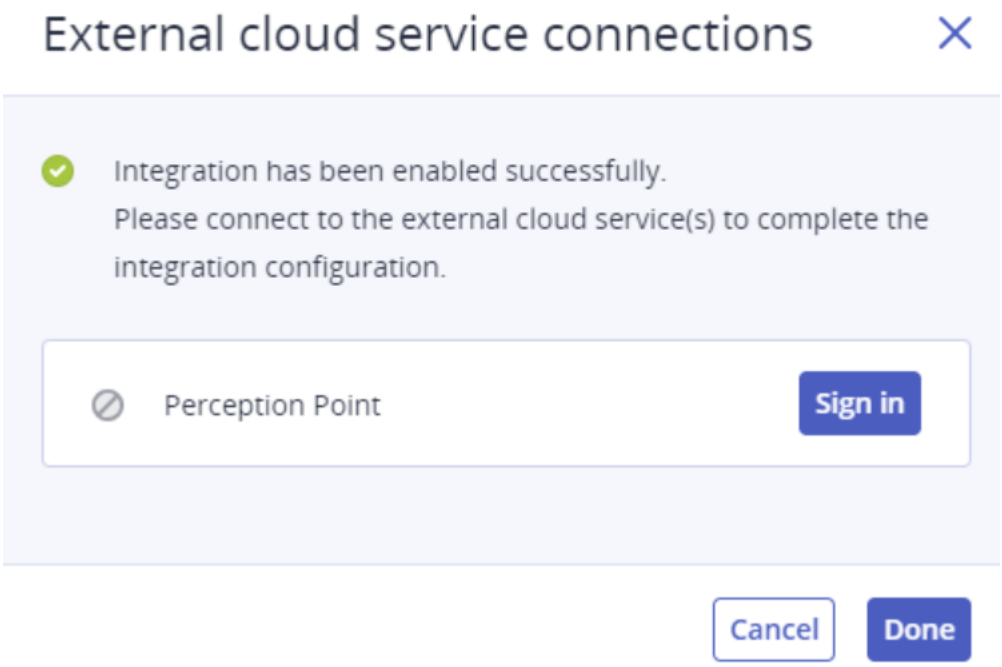
1. 管理ポータルで、統合を有効にするカスタマーにアクセスし、**[サービス管理]** をクリックしてCyber Protectコンソールを開きます。
2. **[Eメールセキュリティ]** に移動し、**[Eメールセキュリティのコンソールに移動]** をクリックして、Perception Pointを開きます。
3. 該当するEメールセキュリティやコラボレーションアプリチャネルをPerception Pointに作成します。詳細については、Perception Pointのドキュメントを参照してください。
4. 左側のナビゲーションメニューで、**[プロフィール]** をクリックします。
5. **[セキュリティ]** セクションで、APIキーの横にあるコピーのアイコンをクリックします。このキーは、次の手順にある説明のとおり、XDR統合を有効にするために使用されます。

カスタマーのPerception Point XDR統合を有効にするには

1. 管理ポータルで **[統合]** へ進みます。
2. **Perception Point XDR**統合を検索し、表示されたタイルの **[設定]** をクリックします。



3. **[カスタマー管理]** タブをクリックし、XDR統合を有効にするカスタマーを選択して、**[有効化]**をクリックします。
4. 表示されたダイアログで、**[サインイン]** をクリックします。



5. 前の手順でコピーしたPerception Point APIキーを入力し、**[完了]** をクリックします。
6. 統合が稼働していることを確認するには、**[有効化状態]** 列が **[有効]** と表示され、**[サービス接続]** 列が **[1/1]**（接続が実行中）と表示されていることを確認します。

Microsoft 365サービスとの統合

このトピックでは、Microsoft 365サービスとAdvanced Security + XDRを統合する方法について説明します。

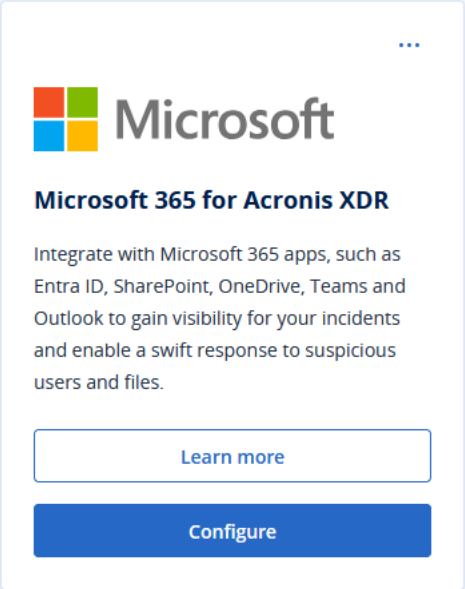
この統合により、コラボレーションアプリケーションにMicrosoft 365を使用しているエンドカスタマー向けに、強化されたメタデータがEDR（Endpoint Detection and Response）およびXDR（Extended Detection and Response）インシデントに対して提供されます。この統合により、インシデントの影響を受けた認証済みユーザーの詳細も提供されます。また、ユーザーアカウントのアクセスをブロックまたは制限するなどの対応アクションを実行することもできます。

重要
統合を正しく機能させるには、次のいずれかのライセンスが必要です。

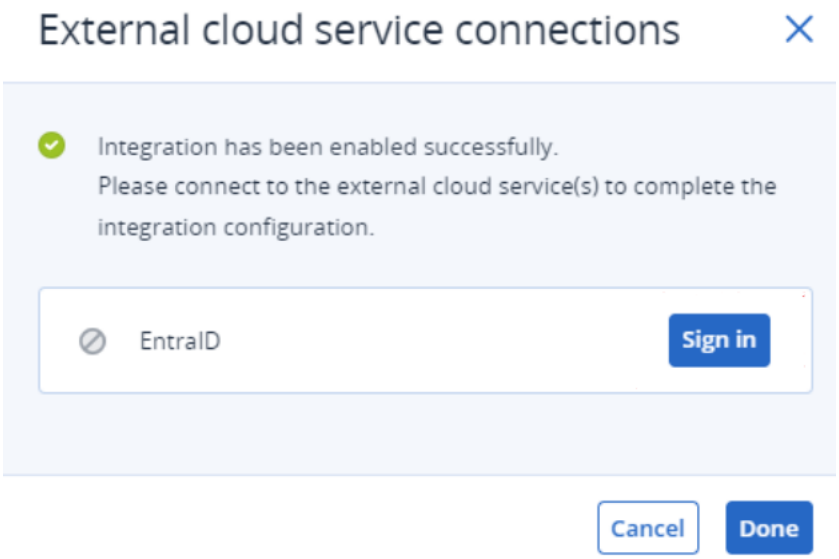
- Microsoft 365 Business Standard
- Microsoft 365 Business Premium
- Office 365 E1
- Office 365 E3
- Microsoft 365 E3
- Microsoft 365 E5

Microsoft 365サービスとの統合を行うには

1. Microsoft Azureポータルに移動し、カスタマーのテナントとしてログインします。
2. 画面の指示に従って、新しいアプリケーションを作成し、新しいアプリケーションに必要なロールを割り当てます。Microsoft 365 APIアクセスの構成についての詳細は、このナレッジベースの記事を参照してください。
3. Advanced Security + XDRパックの管理ポータルで、該当するカスタマーテナントの**[Workpack]**オプションが有効になっていることを確認します。
4. **[統合]** に移動し、**[Microsoft 365 XDR]** 統合を検索します。
5. **[Microsoft 365 for XDR]** カタログのタイルで、**[設定]** をクリックしてから **[有効化]** をクリックします。



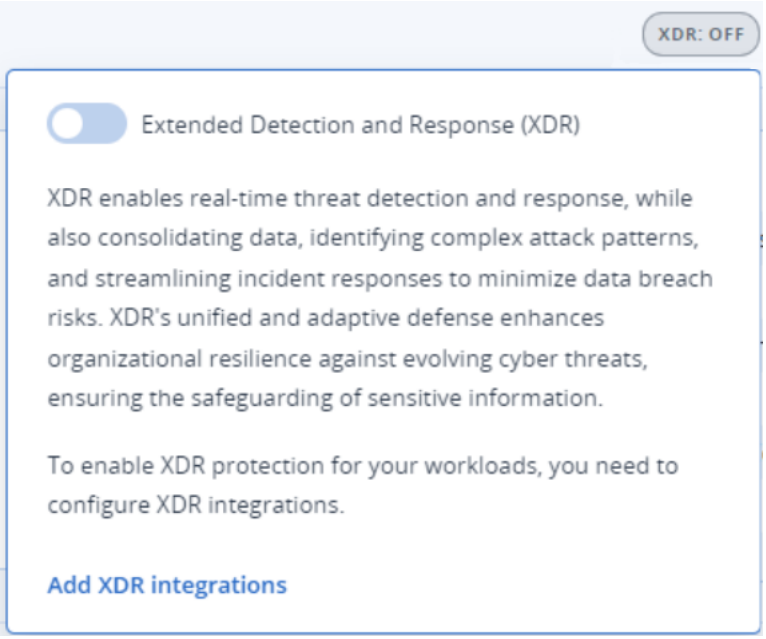
6. **[カスタマー管理]**タブをクリックし、統合を有効にするカスタマーテナントを選択して、**[有効化]**をクリックします。
7. 以下を定義します。
   - **カスタムドメイン**: カスタマーがMicrosoft 365でカスタムドメインを使用している場合は、ここに入力します。カスタムドメインを使用していない場合は、このフィールドを空白のままにします。
   - **リージョン**: ドロップダウンリストからMicrosoft 365テナントに関連するリージョンを選択します。
8. **[有効化]** をクリックします。表示されたダイアログで、**[サインイン]** をクリックします。



9. 次のとおり入力します。
   - **ID**: 手順2で作成したアプリケーションのオブジェクトID。

     注意
     Microsoft 365の [**アプリ登録**] > [**概要**] ページで、[**ローカルディレクトリ内のマネージドアプリケーション**] フィールドにあるアプリ名のリンクをクリックしてコピーし、表示されるページでオブジェクトIDを選択します。メインの [**アプリ登録**] > [**概要**] ページに表示されるオブジェクトIDはコピーしないでください。

   - **シークレット**: アプリケーションに作成されたAPIクライアントのシークレット。
   - **テナントID**: Microsoft 365のテナント。
10. [**サインイン**] をクリックして、[**完了**] をクリックします。
    正常に接続できるようにするには、[**サービスの接続**] 列が [**1/1**]（接続が実行中）と表示されていることを確認します。
11. [**クライアント**] に移動し、XDRを有効にするカスタマーを選択して、[**サービスの管理**] をクリックします。
    Cyber Protectコンソールが表示されます。
12. [**保護**] に移動し、[**XDR: オフ**] をクリックします。
13. 表示されたポップアップでトグルスイッチをクリックして、XDRを有効にします。



これで、Microsoft 365に登録されたワークロードを含むインシデントに、このユーザーに対するエンリッチ化されたXDR情報と対応アクションが含まれます。

Fortinetとの統合

このトピックでは、FortinetとXDRの統合方法について説明します。

この統合では、Fortinetのセキュリティソフトウェアとアプライアンスからイベントを取り込み、対象のインシデントと関連付けて、Endpoint Detection and Response（EDR）とExtended Detection and Response（XDR）インシデントに豊富なメタデータを提供します。

重要
統合を正しく機能させるためには、カスタマーが、該当するネットワークのFortiGate Cloud Serviceライセンスを所有している必要があります。

Fortinetと XDRを統合するには、以下に示す3つの主な手順を実行する必要があります。

- XDRのクォータを有効にする。
- Fortinetとアクロニスが連携するように設定します。
- 管理ポータルで統合を有効にします。

XDRのクォータを有効にするには

1. 管理ポータルで、統合を有効にする、該当のカスタマーにアクセスします。
2. XDRのクォータが有効であることを確認してください。
   - ソリューションベースのライセンスでは、XDRは**セキュリティとRMM**または**究極の保護**ライセンスで利用可能です
   - サービスベースのライセンスでは、XDRは**Detection and Response**提供項目で利用可能です。

   詳細については、"標準および追加の保護サービス"（42ページ）を参照してください。

アクロニスと連携するようにFortinetを構成するには

1. FortiGateまたはFortiGate Cloud Serviceアカウントにログインします。
2. URLまたはIPアドレスをブロックする対応アクションの場合:
   a. **[セキュリティプロファイル]** > **[Webフィルタ]** に移動して、**[アクロニスWebフィルタ]** という名前のフィルタを定義します。次に、**[静的URLフィルタ]** セクションで、**[URLフィルタ]** スイッチをクリックして、有効にして、1つ以上のURLをリストに追加します。

      注意
      フィルタリングするURLが含まれていない場合、Webフィルタは自動的に無効になります。Webフィルタを有効にしたままにするには、一時的にダミーのURLを定義できます。

   b. **[ポリシーとオブジェクト]** > **[ファイアウォールポリシー]** に移動し、関連するポリシー（**[セキュリティプロファイル]** セクション）に、**[アクロニスWebフィルタ]** が追加されていることを確認します。

   対応アクションが開始されると、Webフィルタおよびファイアウォールポリシーが定義されていなくても、Fortinetからレピュテーション情報が送信されます。Webフィルタを追加すると、URLまたはIPアドレスをブロックできます。

   注意
   アクロニスWebフィルタが定義されていないか、ロケーションが指定されていない場合、XDRグラフにはブロック対応アクションが表示されません。

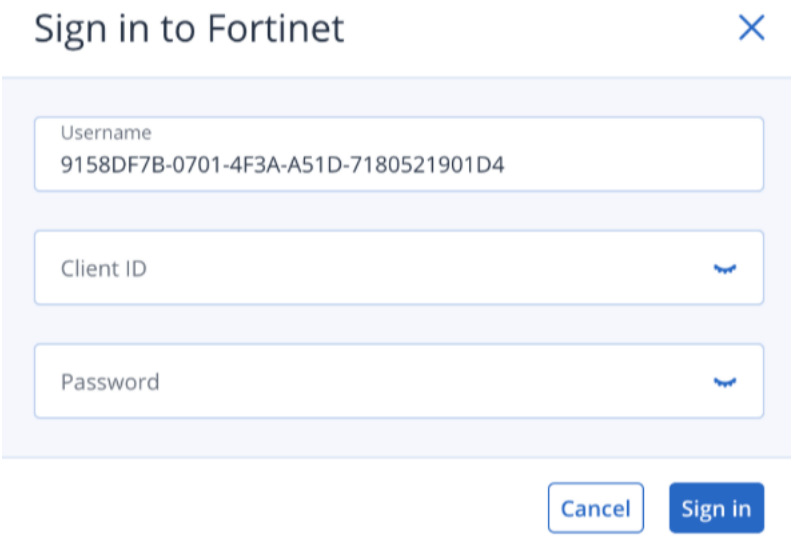
3. エンドポイントを分離するには:
   - **[ポリシーとオブジェクト]** > **[ファイアウォールポリシー]** に移動して、送信接続のブロックと許可のための2つのポリシー（アクロニスドメイン用およびIPアドレス用）を定義します。
   - **[ポリシーとオブジェクト]** > **[アドレス]** に移動し、**[アドレスグループ]** タブで、次のように定義します。
     - **アクロニスアイソレーテッドグループ**では、ブロックされたアドレスが自動的に保存されます。 **アクロニスアイソレーテッドグループ**は、**Group**タイプであり、ブロックポリシーにリンクする必要があります。
     - **Acronis Allowed Hosts**グループでは、許可されたアドレスとドメインが保存されます。**Acronis Allowed Hosts**は、**Group**タイプであり、送信接続を許可するポリシーにリンクする必要があります。例えば、**アクロニスアイソレーテッドグループ**をポリシーの**Source**フィールドに追加し、**Acronis Allowed Hosts**グループを**Destination**フィールドに追加します。

       注意
       アクロニスエージェントの動作に必要なアクロニスデータセンターのアドレスとポートは、こちらに一覧表示されています。

カスタマーのFortinet XDR統合を有効にするには

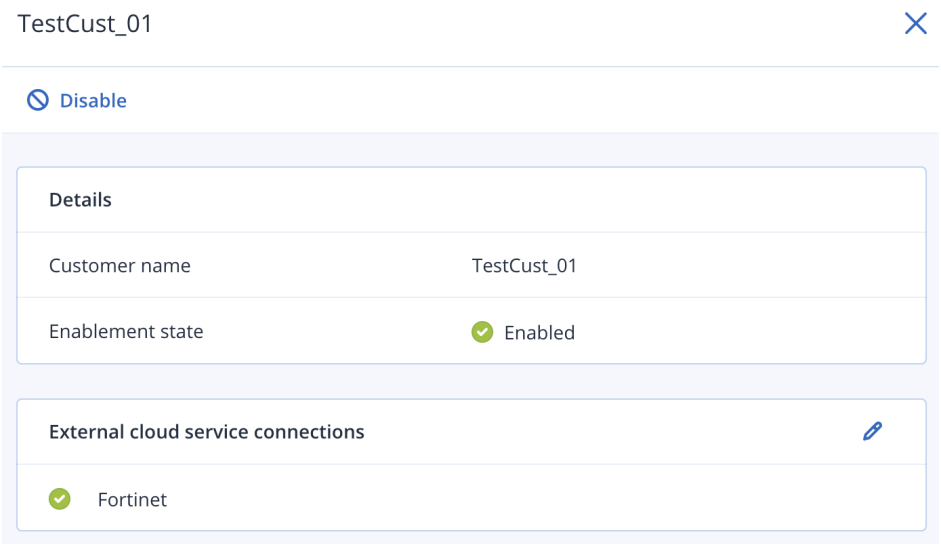
1. 管理ポータルで **[統合]** へ進みます。
2. **Fortinet XDR**統合を検索し、表示されたタイルの **[構成]** をクリックします。
3. **[カスタマー管理]** タブをクリックし、XDR統合を有効にするカスタマーを選択して、 **[有効化]** をクリックします。

4. ダイアログボックスに、関連するFortinetユーザー名、クライアントID、パスワードを入力します。



注意
Fortinetの資格情報は、IAM APIユーザーを作成し、FortiGateクラウドの管理者許可を設定したときに生成されます。詳細については、FortiGateクラウドの文書を参照してください。また、Fortinetのクライアントであり、開発ネットワークページにアクセスできる場合は、こちらの文書を参照してください。

5. **[サインイン]**をクリックします。
6. 統合が正常に動作していることを確認するには、関連するカスタマー行をクリックして、**[有効化状態]** フィールドが **[有効]** になっていることを確認します。



7. （オプション） Fortinetのユーザー名、クライアントID、パスワードをアップデートするには、**[外部クラウドサービスの接続]** セクションの鉛筆アイコンをクリックします。

Fortinet XDRの統合を無効にするには

1. 管理ポータルで **[統合]** へ進みます。
2. **Fortinet XDR**統合を検索し、表示されたタイルの **[構成]** をクリックします。
3. **[カスタマー管理]** タブをクリックし、XDR統合を無効にするカスタマーを選択して、 **[無効化]**をクリックします。

Managed Detection and Response（MDR）

MDRは、社内にセキュリティの専門技術がないMSPや、Endpoint Detection and Response（EDR）、また Extended Detection and Response（XDR）によって検出されたセキュリティインシデントの調査や対応に補助的サポートを必要とするMSP向けに、24時間365日のサービスを提供します。

MDR機能は、管理ポータルの「Detection and Response」サービス（サービスベースのライセンスモードの場合）および「セキュリティとRMM」または「究極の保護」（ソリューションベースのライセンスモードの場合）で有効化され、MDRサービスは外部のMDRベンダーによって提供されます。MDRが特定のカスタマーに対して有効化されている場合、MDRベンダーは、そのクライアントに属する保護計画でEDRまたはXDRが有効になっているワークロードについて、Cyber Protect Cloudプラットフォームからインシデントデータを受信します。その後、MDRベンダーは、利用可能な応答アクションを使用してインシデントをトリアージするために、さまざまなレベルのサービスを実行します。詳細については、"Managed Detection and Response (MDR) とは"（60ページ）を参照してください。

XDRとの連携の詳細については、「Extended Detection and Response（XDR）」を参照してください。

EDRとの連携の詳細については、EDR（Endpoint Detection and Response）を参照してください。

Managed Detection and Response (MDR) とは

MDRとは、サードパーティベンダーが提供するサービスで、熟練したアナリスト、統合ツール、脅威インテリジェンス、およびベンダーとアクロニスの両方のテクノロジーを組み合わせながら、潜在的なセキュリティ脅威や侵害を監視して対応します。

管理ポータルでMDRがカスタマーに対して有効になっている場合、アクロニスは、MDRベンダーがこれらのインシデントの調査と対応操作を実施できるように、インシデントのテレメトリを転送します。自動的に緩和されないインシデントのみがMDRベンダーに転送されることにご注意ください。

MDRの主要コンポーネント

MDRは、次の3つの主要コンポーネントで構成されています。

- 監視
- 分離
- 対応と修復

監視

MDRベンダーは、カスタマーのエンドポイントから検出されたセキュリティアラートや通知を監視します。ベンダーは、次に、分析、セキュリティオーケストレーション、および応答を使用して、これらの

アラートを一般的な脅威、脅威インテリジェンス、およびサードパーティの脅威インテリジェンスと関連付けて優先順位を付けます。その結果、ベンダーはアラートや通知が漏洩か侵害かを判断できます。

潜在的なセキュリティ脅威をもたらす可能性があるとMDR ベンダーが判断したセキュリティイベントはすべて、カスタマーが直面するセキュリティインシデントとしてエスカレーションされ、Cyber Protectコンソールに表示されます。そのベンダーは、脅威の深刻度と推奨される改善策（すでに実施された操作など）のコンテキストを提供します。

分離

MDR ベンダーのアナリストは、事前に定義されたプレイブックを活用してエンドポイント分離のための対応にあたります。MDR ベンダーによる対応操作はすべて、該当するセキュリティインシデントで反映されます。エンドポイントを分離するかどうかの判断は、エンドポイントからのデータを利用して、脅威インテリジェンスや脅威調査による詳細情報も得て行われます。

対応と修復

対応と修復の操作は、最初の監視と分離の操作が完了した後に行われます。セキュリティインシデントが検出されると、MDRベンダーはセキュリティインシデントに応じた対応にあたります。対応と修復の操作には次のようなものがあります。

- 提供されたデータ、インテリジェンス、勧告に基づき、セキュリティインシデントを軽減、阻止、防止する方法に関するガイダンス。
- セキュリティ事象を分析・調査し、侵害の根本原因と範囲を特定する。
- ワークロードの分離、脅威の隔離、または脅威の完全な修復を行うために、承認済みワークフローを実行すること（MDRベンダーの対応プレイブックに定義されているとおり）。
- サービスプロバイダーに、カスタマーが直面するセキュリティインシデント、脅威インテリジェンス、勧告を引用した、より詳細なセキュリティエスカレーションを提供する。
- 全面的にカスタマーからの連絡先情報を介して、セキュリティインシデントの作成、Eメールによる通知、電話など、さまざまなチャネルを通じてインシデントをエスカレーションする。
- 脅威が修正されるまでカスタマーとの連絡を保ち、新しい情報が発生した場合はタイムリーに最新情報を提供する。
- 対応操作がMDRサービスの範囲外である場合、MDRベンダーは、集中すべき領域に関する推奨事項を提供する（インシデント対応などの追加サービスの推奨も含む）。

責任マトリックス: 誰が何をするのか?

MDRを最大限に活用するには、プロセスに関与するすべての関係者の責任を明確に分担し、理解することが重要です。以下は、MDRベンダーとマネージドサービスプロバイダー（MSP）のプロセスにおけるロールを定義するために使用できるRACI表の例です。R（Responsible: 実行責任）、A（Accountable: 説明責任）、C（Consulted: 相談先）、I（Informed: 報告先）。

アクション	MDRベンダー	MSP
エンドポイントへのエージェント配置（登録を含む）		R、A

アクション	MDRベンダー	MSP
保護計画の構成 (EDR 用)	I	R、A
新しいアラートまたはアップデートされたアラートの24時間年中無休の監視	R、A	I
インシデントの調査と隔離	R、A	I
根本原因分析レポートの生成	R、A	I
インシデントのアップデート	R、A	I
異なる通信チャネルを通じた最初の評価応答	R、A	I
インシデントの推奨事項の生成	R、A	I
インシデントに関する推奨事項の適用（ロールバックおよびバックアップからの復元を含む）	標準: C 高度: R, A	標準: R、A 高度: C、I
月次レポートの生成	R、A	I
オンデマンドインシデント調査	A、C	R、C

Managed Detection and Response (MDR) の有効化

選択したカスタマーのMDRを有効にするには、次の 2 つのステップを実行します。

- ステップ1: カスタマーのMDR提供項目を有効にする。
- ステップ2: MDRベンダーのアプリとの統合を設定する。

注意
セルフマネージドのカスタマーはMDRを有効にできません。セルフマネージドのカスタマーの構成情報に関する詳細については、"カスタマープロファイルの自己管理を構成する"（121ページ）を参照してください。

さらに、カスタマーごとに1つのMDRベンダーのみを選択できますが、必要に応じて選択したMDRベンダーを変更できます。また、異なるカスタマーに異なるMDRベンダーを使用することもできます。

特定のカスタマーのMDRを有効にするには

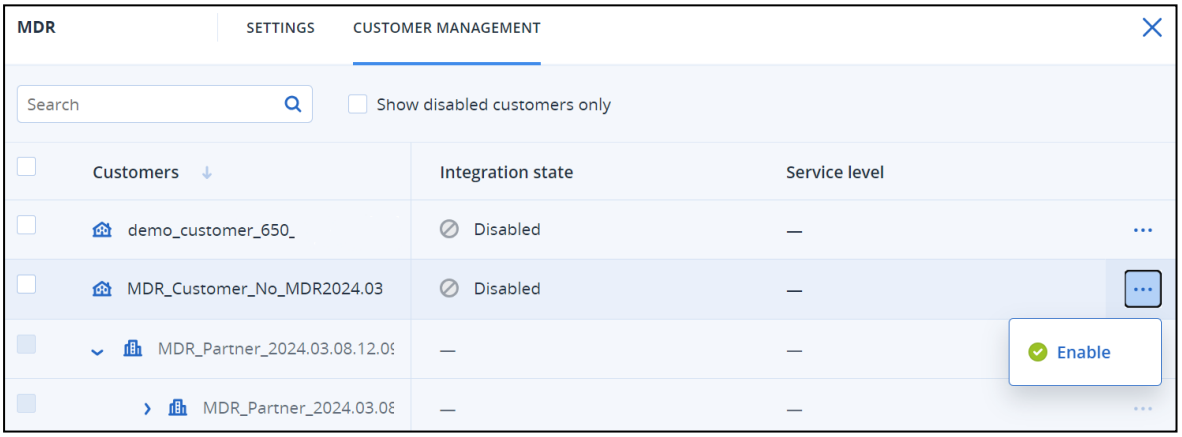
1. 管理ポータルで **[クライアント]** へ進みます。
2. 該当のカスタマー名の横にある省略記号アイコン（...）をクリックし、**[設定]** を選択します。
3. **[保護]** タブで **[編集]** をクリックします。
4. [ソリューションベースのライセンスモードの場合] 2 つの **Managed Detection and Response** チェックボックスが選択されていることを確認します。
5. [サービスベースのライセンスモードの場合] **Detection and Response** セクションで、**エンドポイント** および **Managed Detections and Response** のチェックボックスが選択されていることを確認

します。

6. **[保存]**をクリックして、変更を適用します。

MDRベンダーのアプリとの統合を設定するには

1. 管理ポータルで **統合**へ進みます。
2. 検索バーを使ってMDRベンダーのアプリを探します。
3. 表示されたMDRカタログカードで、**[設定]** クリックします。
4. **[設定]**タブで、鉛筆のアイコンをクリックし、少なくとも 1 つのパートナーの連絡先情報を入力します。この連絡先に、セキュリティイベントが検出された際、MDRベンダーから連絡が入ります。連絡先情報は、最大3件まで登録できます。入力が完了したら、**[有効化]** をクリックします。
   セキュリティイベントが検出されると、ベンダーは次の連絡先に移る前に、各連絡先に6 回電話をかけます。電話連絡の後、または連絡が取れなかった場合、ベンダーはすべての連絡先に、エスカレーションとインシデントの概要を説明するEメールを送信します。
5. **[カスタマー管理]**タブで、該当する顧客の右端の列にある省略記号アイコン（...）をクリックし、次に **[有効化]** をクリックします。



   複数のカスタマーを無効にするには、該当するカスタマーの左横にあるチェックボックスを選択し、**[カスタマー管理]**タブの左上にある **[有効化]** を選択します。
6. 表示されたダイアログの **[サービスレベル]** ドロップダウンリストから、選択したカスタマーに適用するMDRサービスのレベルを選択します。
   - **標準**: 24時間365日のカスタマーエンドポイントの監視による攻撃検知、AIを活用したイベントのトリアージと優先順位付け、脅威の封じ込めと影響を受けたエンドポイントの隔離、優先順位付けされたインシデントリストに対するリアルタイムのコンソール内の可視化が含まれます。
   - **アドバンス**: このレベルでは、**[標準]** に含まれる機能に加えて、攻撃のロールバック、復元、セキュリティギャップの解消を含む完全な修復が可能です。
7. **[有効化]** をクリックして、MDRの統合を完了します。
   IP許可リスト機能が有効になっている場合（"Webインターフェイスへのアクセス制限"（105ページ）を参照）、MDRベンダーのIPを許可リストに追加するよう求められます。これにより、ベンダーが該当するワークロードを監視できるようになります。**[有効化]** をクリックして確定します。
   これで、MDRが有効になり、セキュリティインシデントがMDRベンダーに転送され、調査と対応のアクティビティが実施されます。MDRサービスの詳細については、"Managed Detection and Response (MDR) とは"（60ページ）を参照してください

Managed Detection and Response (MDR) の無効化

提供項目レベルでMDRを無効化できます。また、MDRベンダーの統合アプリで、個々のカスタマーのMDRを無効にすることもできます。

MDRの提供項目を無効化するには

1. 管理ポータルで **[クライアント]** へ進みます。
2. 該当のカスタマー名の横にある省略記号アイコン（...）をクリックし、**[設定]** を選択します。
3. **[保護]** タブで **[編集]** をクリックします。
4. **[Advanced Security + EDR]** セクションで、**[ワークロード]** および **[Managed Detection and Response]** チェックボックスが選択されていないことを確認します。次に、**[保存]** をクリックして変更を適用します。
   また、**[設定]** タブで **[Advanced Security + EDR]** サービスを無効にでき、それで自動的にMDRが無効になります。

MDRベンダーの統合アプリで個々のカスタマーのMDRを無効にするには

1. 管理ポータルで **[統合]** へ進みます。
2. 該当するMDRベンダーアプリを検索します。
3. 表示されたMDRカタログカードで、**[設定]** クリックします。
4. **[カスタマー管理]**タブで、該当する顧客の右端の列にある省略記号アイコン（...）をクリックし、**[無効化]** を選択します。
   複数のカスタマーを無効にするには、各カスタマーの左側にあるチェックボックスを選択し、**[カスタマー管理]**タブの左上にある **[無効化]** を選択します。

Managed Detection and Response (MDR) で利用可能な対応操作

MDRには、インシデントレベルで適用できる数多くの対応操作が含まれています。

対応操作はMDRセキュリティアナリストによって実行され、Cyber Protectコンソールにアクセスするか、APIコールを実行することで、該当するアクションを適用します。このアナリストは、**セキュリティアナリスト**ロールでCyber Protectコンソールにログインします。

すべての対応操作は **[アクティビティ]** リストに記録されます。カスタマーは、実行された対応アクションアクティビティのリストと、これらのアクティビティのステータス（処理中/成功/失敗）を表示できます。**[開始ユーザー]** 列には、パートナーユーザー、カスタマーユーザー、MDRセキュリティアナリストのいずれでも、アクションを開始したユーザーが表示されます。

注意
以下の表に記載されている対応操作には、EDR（Endpoint Detection and Response）ドキュメントの関連セクションへの参照が含まれています。

対応操作	追加情報
調査ステータスを変更	ステータスは以下のいずれかに設定できま

対応操作	追加情報
	す。 • **調査中** • **終了** • **誤検知** 調査ステータスの変更の詳細については、サイバーキルチェーンでインシデントを調査する方法を参照してください。
ネットワーク分離	MDRのセキュリティアナリストは以下の操作ができます。 • ワークロードの分離 • ワークロード分離の解除 • 分離ステータスの確認 ワークロード分離の詳細については、「ワークロードのネットワーク分離を管理する」を参照してください。
コメントの付加	MDRセキュリティアナリストは、インシデントのサイバーキルチェーンで **[コメントを投稿]** をクリックして、インシデントにコメントを付加できます。このコメントは、特定のインシデントの **[アクティビティ]** タブに表示されます。詳細については、「インシデントを軽減するために実行される操作を理解する」を参照してください。
プロセス/プロセスツリーの停止	このアクションはインシデント全体に適用できます。応答アクションは、インシデントのプロセスがすでに停止している場合でも起動できます。 非同期対応は、対応操作が処理された後に送られます。対応は以下のいずれかになります。 • 成功: すべてのプロセスが正常に停止。 • 警告を伴い正常に完了: いくつかのプロセスが正常に停止されたか、停止するプロセスがない（またはMDRの外部で停止された）。 • エラー: プロセスが停止されなかった。 プロセスまたはプロセスツリーの停止に関する詳細については、「不審なプロセスに対する対応操作を定義する」を参照してくださ

対応操作	追加情報
	い。
検疫	このアクションはインシデント全体に適用できます。応答アクションは、インシデントのファイルまたはプロセスがすでに隔離されている場合でも起動できます。 非同期対応は、対応操作が処理された後に送られます。対応は以下のいずれかになります。 • 成功: すべてのファイルとプロセスが正常に隔離された。 • 警告を伴い正常に完了: 一部のファイルおよびプロセスが正常に隔離されたか、隔離するファイル またはプロセスがない (またはMDR の外部で隔離された)。 • エラー: ファイルまたはプロセスが隔離されなかった。 プロセスの隔離の詳細については、「不審なプロセスに対する対応操作を定義する」を参照してください。ファイルの隔離の詳細については、「不審なファイルに対する対応操作を定義する」を参照してください。
ファイルを削除	このアクションはインシデント全体に適用できます。応答アクションは、インシデントのファイルがすでに削除されている場合でも起動できます。 非同期対応は、対応操作が処理された後に送られます。対応は以下のいずれかになります。 • 成功: すべてのファイルが正常に削除された。 • 警告を伴い正常に完了: いくつかのファイルが正常に削除されたか、削除するファイルがない（またはMDRの外部で削除された）。 • エラー: ファイルは削除されなかった。 ファイル削除の詳細については、「不審なファイルに対する対応操作を定義する」を参照してください。
ワークロードを再起動	ワークロードを再起動するまでの時間間隔または即座の再起動の設定が有効になります。

対応操作	追加情報
	ワークロードの再起動の詳細については、「ワークロードを再起動」を参照してください。
URL、ファイル、プロセスを許可リスト/ブロックリストに追加する	デフォルト計画（ワークロードに現在割り当てられているプラン）の許可リスト/ブロックリストに、URL、ファイル、またはプロセスを追加します。 非同期対応は、対応操作が処理された後に送られます。対応は以下のいずれかになります。 • 成功: すべてのURL、ファイル、プロセスが正常に追加された。 • 警告を伴い正常に完了: いくつかのURL、ファイル、プロセスは正常に追加されたが、いくつか追加されなかったものがある（すでに許可リストに含まれている場合など）。 • エラー: アクションが失敗した。 URL、ファイル、またはプロセスを許可リストやブロックリストに追加する方法の詳細については、「プロセス、ファイル、ネットワークを保護計画のブロックリストまたは許可リストに追加する」を参照してください。

Eメールセキュリティ

Email Securityサービスは、Microsoft 365、Google Workspace、Open-Xchangeのメールボックスをリアルタイムで保護します。

- マルウェア対策およびスパム対策
- Eメール内のURLスキャン
- DMARC分析
- フィッシング対策
- なりすまし防止
- 添付ファイルのスキャン
- コンテンツの対処と再構築
- 信頼性の可視化
- メールボックスの所有者による、隔離されたスパムのセルフサービスによる解放

また、Microsoft 365コラボレーションアプリシートを有効にすることで、コンテンツを介するセキュリティ脅威からMicrosoft 365クラウドコラボレーションアプリケーションを保護することができます。これらのアプリケーションには、OneDrive、SharePoint、Teamsが含まれる。

Email Securityは、ワークロード単位またはギガバイト単位で有効にすることができ、ライセンスモデルに影響します。

Email Securityの詳細については、「Advanced Email Securityデータシート」を参照してください。

設定手順については、Email Securityのドキュメントを参照してください。

Disaster Recovery

Disaster Recovery を有効にすると、すべての Disaster Recovery 機能を使用してワークロードを保護できます。

以下のDisaster Recovery機能を利用できます。

- 本番フェールオーバー
- AI スクリーンショット検証による自動化されたテストフェールオーバー
- ダウンタイムがほとんどない状態での仮想マシンと物理マシンへの自動増分フェールバック
- ポイントインタイムリカバリ：100の復元ポイントが利用可能
- 再感染を回避するためにマルウェアのないポイントにフェールオーバーする
- ランブックの自動化
- RPO準拠のトラッキングを使用したリアルタイムDRダッシュボード
- 複数のネットワーク接続オプション：クラウド限定、ポイントツーサイト、サイト間Open VPN、マルチサイトIPsec VPN（Cyber Protect CloudへのDisaster Recovery）
- クラウドネットワークの数Cyber Protect Cloud: 23
- 複数のネットワーク接続オプション: Azure IPsec VPN、Azure ExpressRoute （Microsoft Azure への Disaster Recovery）
- Microsoft Azure の最大クラウドネットワーク数: Microsoft Azure サブスクリプション ポリシーによって制限されます。
- カスタマーは、Azure ネットワーキングと接続性を完全に制御でき、ネイティブの Azure プラットフォーム機能を活用するか、独自のカスタムソリューション (Microsoft Azure) を持ち込むかを選択できます。

Direct Backup to Public Cloud

Direct Backup to Public Cloudは、Azure、AmazonS3、およびS3互換クラウドストレージへのバックアップを可能にする追加のサービスです。

注意
このサービスは、Microsoft 365シートおよびGoogle Workspaceシートには利用できません。

セキュリティ意識向上トレーニング

パートナーは、カスタマーテナントのセキュリティ意識向上トレーニングサービスを有効にして、組織のユーザーが保護コンソールからセキュリティ意識向上トレーニング資料にアクセスできるようにすることができます。

Cyber Protectionクラウドコンソールからセキュリティ意識向上トレーニングに直接アクセスできることから、組織内のユーザーがより身につけやすく、範囲が広がるので、カスタマーはコンプライアンス（PCI、HIPPA、FedRamd、Soc 2）、ベンダーリスク管理、サイバー保険などの要件を満たすのに役立ちます。また、トレーニングにより、人為的ミスのリスクを低減することで、カスタマーはサイバーセキュリティを向上させることができます。

このサービスは、サードパーティの学習管理システムであるWizerによって提供され、次に示す機能がサポートされています。

- マルチテナント: Wizer管理者パネルでは、パートナー管理者は、セキュリティ意識向上トレーニングに登録されているすべてのカスタマーおよび直接のユーザーを表示できます。ただし、パートナーは子パートナーおよびその子テナントを表示できないため、プラットフォームは多階層ビューをサポートしていません。顧客の管理者は、組織内のユーザーのみを表示できます。
- テナントと管理者ユーザーの自動プロビジョニング: 初めてCyber Protect Cloudコンソールでサービスが有効になると、統合によって、統合を有効にした管理者用にWizerで新しいテナントが自動的に作成されます。その後、管理者は、Wizer管理者パネルにアクセスして、ユーザーを手動で追加するか、SSOを設定します（ユーザーの追加方法を参照）。
- トレーニングを楽しくする魅力的な内容
- 操作が簡単
- 月額サブスクリプション

Wizerの詳細については、https://www.wizer-training.com/を参照してください。

セキュリティ意識向上トレーニングサービスの有効化

セキュリティ意識向上トレーニングは、サードパーティベンダーであるWizerによって、Cyber Protect Cloudコンソールでの統合機能として提供されます。パートナーは、カスタマーに対してサービスを有効にする前に、自社のテナントに対してこの統合機能を有効にする必要があります。

サービスの有効化は、以下の高レベルの手順で行います。

1. クラウド管理コンソールで、パートナー管理者がカスタマーのセキュリティ意識向上トレーニングサービスを有効にします（カスタマーごとに1回）。
2. Cyber Protect Cloudコンソールで、管理者が組織内でのWizerとの統合を有効にします（組織ごとに1回）。
3. 管理者ユーザーは、Wizer管理コンソールに移動し、トレーニングプラットフォームにユーザーを登録します。

注意
サービスには、部署管理者とフォルダ管理者はアクセスできません。

カスタマーテナントに対し、セキュリティ意識向上トレーニングサービスを有効にするには

必要なロール: パートナー管理者

1. クラウド管理コンソールで、**[クライアント]** をクリックして、サービスを有効にするカスタマーを見つけます。

2. コンテキストメニューで **[設定]** をクリックします。
3. サービスの一覧で、**セキュリティ意識向上トレーニング**のチェックボックスを選択し、必要に応じてユーザー数のクォータを定義します。

組織のWizerとの統合を有効にするには

必要なロール: パートナー管理者、 カスタマー管理者、保護管理者、またはサイバー管理者。

注意
この初期設定は1回だけ実行されます。

1. Cyber Protect Cloudコンソールにログインします。
2. ナビゲーションメニューで、**[セキュリティ意識向上トレーニング]** > **[意識向上ダッシュボード]** の順にクリックします。
3. **[統合を有効にする]** をクリックします。
4. **[有効化]** をクリックして確定します。

統合が有効になると、Wizerプラットフォームに組織の新しいテナントがプロビジョニングされます。Wizerにアカウントが既にある場合に、新しいテナントの代わりにそのアカウントを使用するには、サービスプロバイダーに連絡してください。

CSVファイルをインポートするか、Active Directory、Octa、Google、または別のIDプロバイダーでSSOを設定することで、Wizer管理者パネルにアクセスし、手動でユーザーを追加できます（ユーザーの追加方法を参照）。

RMM

RMMは、エンドポイントとMicrosoft 365のシートに対して高度な監視と管理を提供する機能のコレクションです。詳細については、こちらをご覧ください。

各機能のソフトウェア要件を確認するには、Cyber Protect Cloud ユーザーガイドの該当するセクションを参照してください。

- エンドポイントについては、 RMMは次の機能を提供します。
  - **ソフトウェアインベントリ** - クライアントが使用するソフトウェアの一覧を表示し、アップデートの準備、計画、追跡の時間を節約し労力を省けます。
  - **DeployPilotによるリモートソフトウェア配置** - 管理対象のワークロードにソフトウェアをリモートで配置します。ソフトウェアの配置計画を使用してソフトウェア配置プロセスを自動化することで、ソフトウェア配布をワークロード全体で一貫して行えます。
  - **自動パッチ管理** - 脆弱性がエクスプロイトされる前に修復します。
  - **フェールセーフパッチの適用** - パッチを適用する前にシステムの自動バックアップを実行することで、パッチの適用が失敗した場合に、ワークロードを迅速かつ容易にリカバリします。
  - **機械学習に基づく監視とスマートアラート** - 予測監視とアラートにより、運用リスクを軽減し、監視作業を最適化します。
  - **特別な設定なしで使用できるサイバースクリプティング** - ルーチンのタスクを自動化し、効率化します。

  - **ドライブのヘルス状態の監視** - 予測監視とアラートにより事前に対応して、ドライブの故障によるダウンタイムの軽減を図ります。
  - **リモートデスクトップおよびリモートアシスタンス** - リモートワークロードにアクセスし、技術的な問題を迅速に解決します。帯域幅が限られている場合でも、時間を節約し、優れたパフォーマンスで信頼性の高いサポートを提供します。この機能には、より幅広いプラットフォームのサポート（Windows、macOS、Linux）、およびセッションの記録、リモート操作、ファイル転送、監視、レポート作成、マルチビューでのワークロード観察のための拡張機能が含まれます。
  - **サードパーティのWindowsアプリケーションの脆弱性診断** - 内部で管理されているデータベースがサポートする、314の重要なアプリケーションの脆弱性を検出し、管理することで、Windowsのサードパーティ アプリケーションのセキュリティ体制を強化します。

    サードパーティのWindowsアプリケーションの脆弱性診断は、RMMパックに移行されており、追加費用が発生する場合があります。これらのアプリケーションの保護を停止して機能を無効にするか、既存の複数の計画で機能を有効にする場合は、"Windowsサードパーティアプリケーションの脆弱性診断の一括無効化と一括有効化"（71ページ）を参照してください。
  - **位置情報トラッキング** - 管理対象のワークロードのリアルタイムの物理的ロケーションを表示します。
  - **ヘルプデスクチャット** - 管理対象のWindowsおよびmacOSワークロードの技術者とリモートユーザー間でリアルタイムでコミュニケーションを行うツールを使用して、問題の解決を迅速化し、カスタマーサービスを向上させます。
- Microsoft 365のシートに対して、 RMMはMicrosoft 365のセキュリティポスチャの継続的な監査を提供し、ベストプラクティスのベースライン、セキュリティポスチャベースラインの逸脱の自動修正、そしてユーザーのオンボーディングとオフボーディングを行います。

Windowsサードパーティアプリケーションの脆弱性診断の一括無効化と一括有効化

複数のカスタマーテナントで複数の管理対象ワークロードの Windowsサードパーティアプリケーションに脆弱性診断を無効化または有効化すると、時間がかかる面倒なタスクになる可能性があります。そのため、この機能を一括で無効化や有効化するユーティリティを作成しました。詳細については、以下に示すナレッジベースの記事を参照してください。

- 保護計画でサードパーティのWindowsアプリケーションの脆弱性診断を設定したが、カスタマーのテナントでRMMパックが有効になっていない場合、影響を受けるすべての計画でサードパーティのWindowsアプリケーションの脆弱性診断を無効にし、他のすべての脆弱性診断コンポーネントを保持するには、このユーティリティを使用します: https://care.acronis.com/s/article/Acronis-Cyber-Protect-Disabling-Vulnerability-Assessment-of-Third-Party-Windows-Applications-when-RMM-is-not-enabled-for-the-tenant。
- 一般的な脆弱性診断ポリシーが既に有効で、対応するテナントでRMMパックが有効になっている保護計画全体で、サードパーティのWindowsアプリケーションについて脆弱性診断を有効にする必要がある場合は、https://care.acronis.com/s/article/Acronis-Cyber-Protect-Enabling-Vulnerability-Assessment-for-Windows-Third-Party-Applications-when-Vulnerability-Assessment-module-is-enabled-in-Protection-plansのユーティリティを使用してサブポリシーを一括で有効にします。

機能統合

この章では、統合を検索してアクティベートするために必要な情報を記載しています。

統合により、サードパーティ製のサイバープロテクション、エンドポイント管理、カスタマー管理、監視、分析などを、標準のCyber Protectコンソール製品と同様に提供し、サードパーティ製のソフトウェアプラットフォームを通じて当社のソリューションを提供します。現在、200以上の統合により、パートナーとそのカスタマーの日常業務ルーチンを自動化し、効率化が図られています。

統合は、統合カタログに一覧表示されます。

注意
一部の統合では、アプリケーションプログラミングインターフェイス（API）クライアントにアクセスするためにAPIクライアントが必要です。

統合カタログ

次の統合カタログに利用可能な統合が一覧表示されます。

- アプリケーションカタログ:
  このカタログは一般に公開されています。このカタログから統合を有効化することはできません。顧客が使用したい統合を見つけた場合、その顧客は、貴社に連絡して有効化を依頼する必要があります。
- データセンター（DC）のカタログ:
  このカタログは、データセンター固有のものです。このカタログから統合を有効化できます。
  パートナーレベルの管理ポータル管理者は、以下の操作ができます。
  - データセンターに配置されているすべての統合を表示する。
  - データセンターに配置されたすべての統合を、自社向けまたはカスタマー向けに有効化する。

  カスタマーレベルの管理ポータル管理者は、以下の操作ができます。
  - 統合開発者がカスタマー向けに明示的に表示されるように設定した統合の表示のみを行う。
  - 統合開発者によりカスタマーが明示的に有効化を許可された統合の有効化のみを行う。

  注意
  カスタマーレベルの管理ポータル管理者によって有効化する前に、パートナーレベルの管理ポータル管理者が、パートナーレベルで統合を有効化する必要があります。

カタログエントリ

カタログエントリは、次の2つの部分で構成されます。

- カタログカードには、統合の概要が表示されます。
- カタログの詳細ページには、機能の詳細説明、スクリーンショット、ビデオ、機能一覧、連絡先情報、統合リソースへのリンクなど、さまざまな情報が表示されます。

データセンター統合カタログを開く

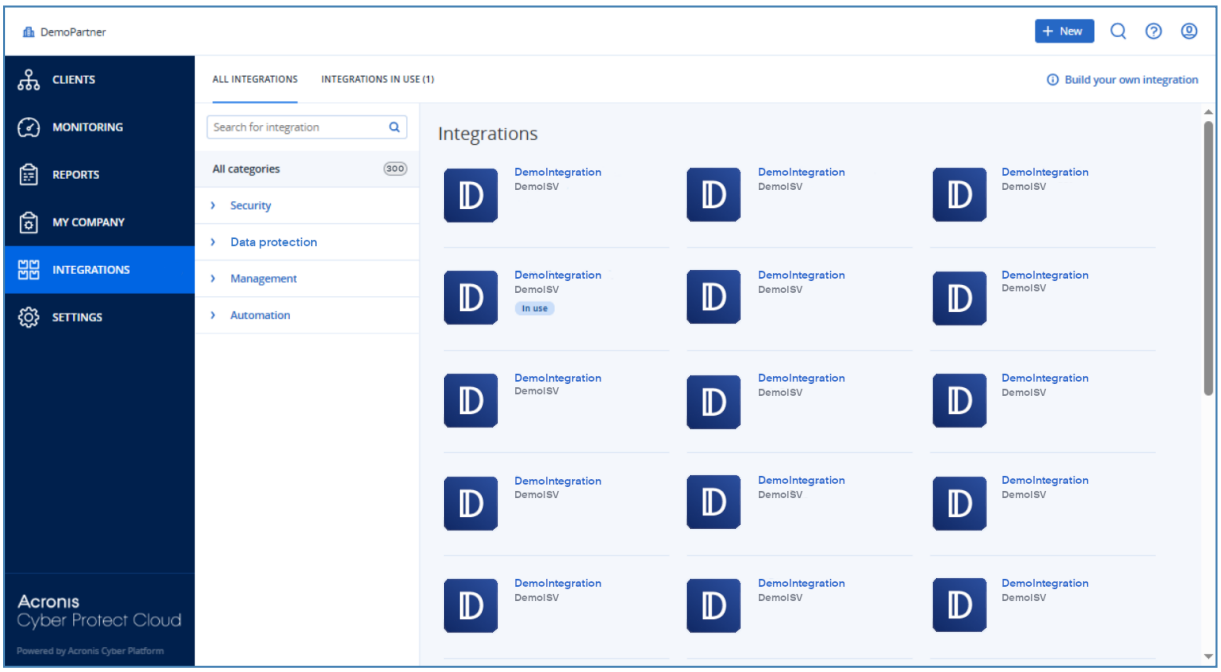
データセンター（DC）統合カタログでは、カタログカードにホバーすると、製品の簡単な説明、**構成**ボタン、および**詳細を表示**リンクが表示されます。

- **詳細情報**リンク
  統合カタログエントリごとに、機能の詳細説明、スクリーンショット、ビデオ、機能一覧、連絡先情報、統合リソースへのリンクなど、統合の詳細が記載されたページがあります。
  このリンクをクリックすると、統合の詳細ページが開きます。
- **設定**ボタン
  統合を有効化するには、このボタンをクリックします。

注意
非アクティブな統合を表すカタログカードは、グレー表示され、無効になっています。

DC統合カタログを開くには

1. 管理ポータルを開きます。
2. メインメニューから **[統合]** を選択します。
   デフォルトでは、**[すべての統合]** タブが開きます。 これにより、現在DCで利用可能な統合のカタログカードが表示されます。
3. （オプション） カテゴリを選択し、検索フィールドにテキストを入力して、カタログカードをフィルタリングします。

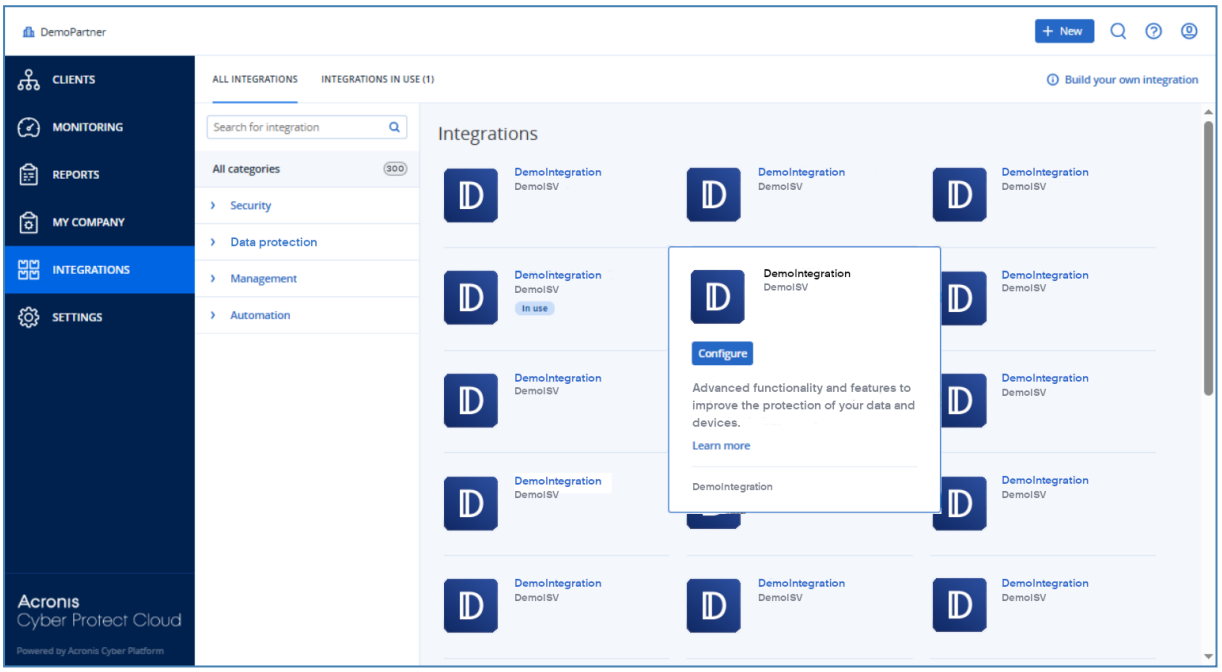


統合の詳細ページを開く

統合の詳細ページを開くには

1. データセンターで統合カタログを開きます。
2. 統合のカタログカードを見つけます。
3. カタログカードの上にホバーします。
4. **[詳細を確認]**をクリックします。

統合の詳細ページが開きます。

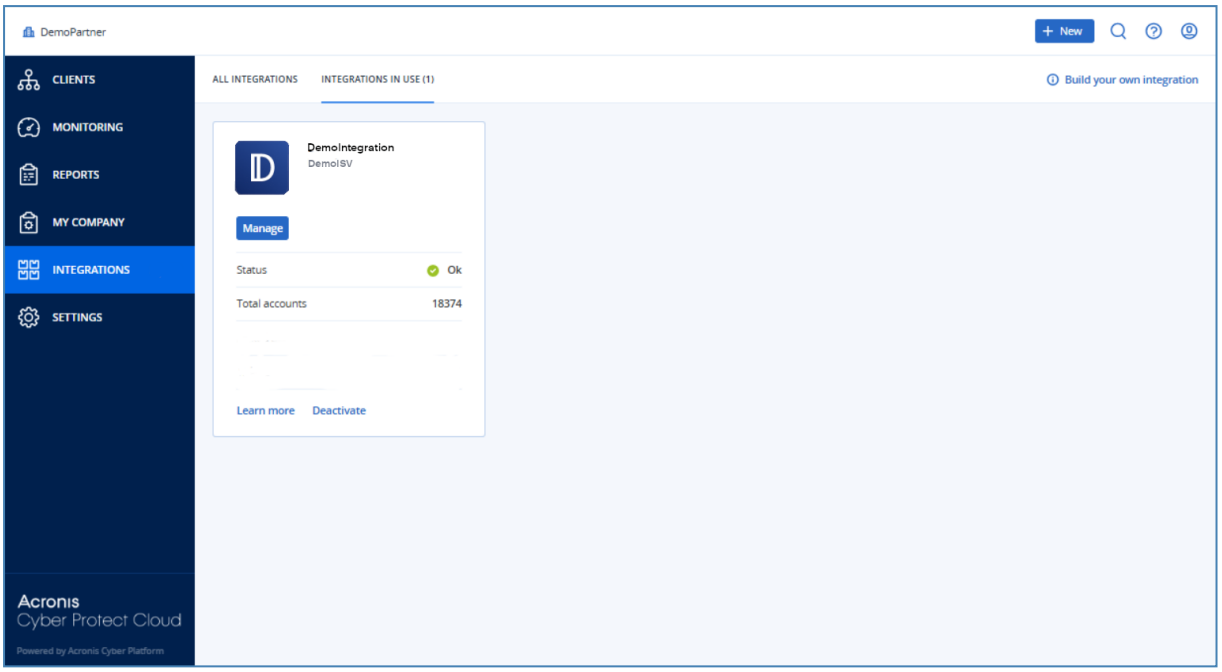


有効化された統合の表示

統合カタログの **[使用中の統合]** タブには、有効化した統合ごとにカードが表示されます。

有効化された統合を表示するには

1. データセンターで統合カタログを開きます。
2. **[使用中の統合]** タブを選択します。



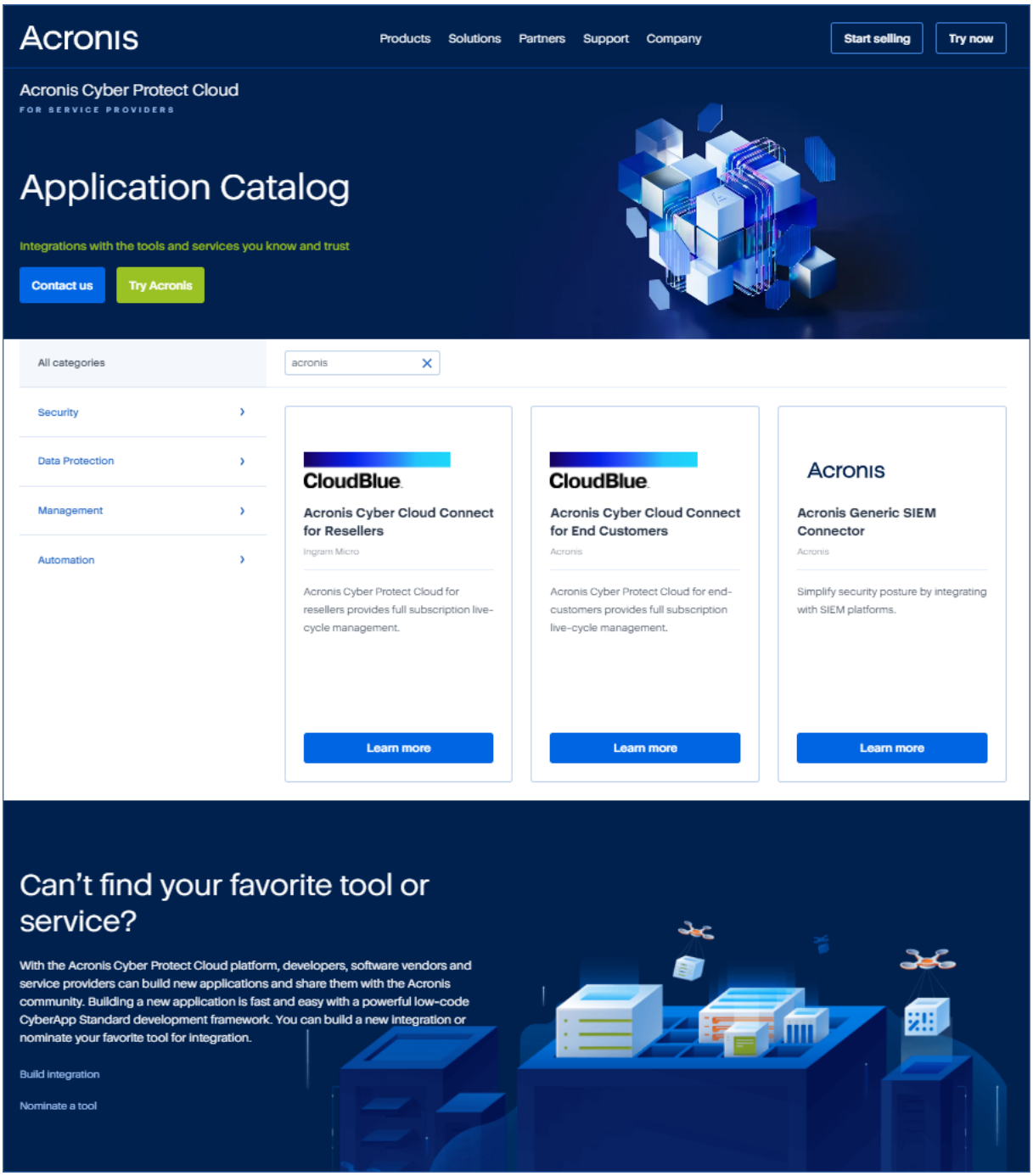
アプリケーションカタログを開く

アプリケーションカタログには、すべてのCyber Protect Cloud統合が一覧表示されています。

注意
アプリケーションカタログは参照専用です。このカタログから統合の有効化はできません。
統合は、管理ポータルのデータセンター統合カタログから有効化できます。

アプリケーションカタログを開くには

1. solutions.acronis.comをご覧ください。
   初期画面では、すべてのカタログカードのグリッドが表示されます。
2. （オプション） カテゴリを選択し、検索フィールドにテキストを入力して、カタログカードをフィルタリングします。



統合の詳細ページを開く

カタログエントリごとに、機能の詳細説明、スクリーンショット、ビデオ、機能一覧、連絡先情報、統合リソースへのリンクなどの統合の詳細が記載されたページもあります。

統合の詳細ページを開くには

1. solutions.acronis.comをご覧ください。
2. 関心のある統合のカタログカードを見つけます。
3. カタログカードの **[詳細]** をクリックします。

SOME FEATURES MIGHT NOT BE AVAILABLE IN YOUR DATA CENTER YET.

Acronis

Products Solutions Partners Support Company

Start selling Try now

Acronis Cyber Protect Cloud

FOR SERVICE PROVIDERS

Application Catalog

Integrations with the tools and services you know and trust

Contact us Try Acronis

← Back to integrations

Have a question or need help?

Acronis

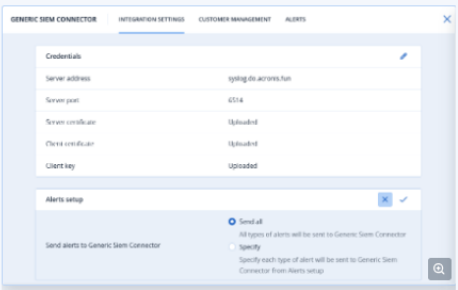
Integration: Acronis Generic SIEM Connector
Category: SIEM
Company: Acronis

Website

Acronis Generic SIEM Connector

SIEM (Security Information and Event Management) platforms are used by many MSPs for security incident investigation and remediation, threat hunting, and compliance. Acronis Generic SIEM Connector allows MSPs to forward Acronis Cyber Protect Cloud alerts to any SIEM system that supports the CEF event format over SYSLOG for further correlation and analysis to reveal patterns of activity that may indicate an attempt of intrusion.

Integration Overview



Simplify security posture by integrating with SIEM platforms.

SIEMs empower MSPs security specialists to identify attack rout across the network and get visibility into compromised files. Now with Acronis Generic SIEM connector, MSPs will gain extra visibility into customers networks, will be able to search for threats across all managed workloads, and correlate events from both security and data protection applications, and run response actions.

Features

Support of core event format
Acronis supports core event format - CEF (Common Event Format), enabling MSPs to work with any SIEM that supports CEF format out of the box. Alerts are transferred to SIEM via syslog server.

Threat hunting across all managed companies
Integration allows MSPs to select which customer tenants in Acronis should send alerts to SIEM. Since alerts are sent to the same SIEM instance, it's possible to run correlation, threat hunting and perform investigation for all customers in the same console. It also empowers MSPs to search for threats, that were discovered on one workload in one customer tenant, in other customers environments.

Simple integration enablement
It's very easy to enable the integration by obtaining server and client certificates, establishing connection to the server and specifying the server port.

Select data you want to see
It is possible to select which alerts should be sent to SIEM. With this functionality, MSPs benefit from reducing the amount of sent to SIEM data and, therefore, lower SIEM invoice. MSPs can select and work only with the data that is necessary.

Acronis

Acronis Generic SIEM Connector

Need help or support with an integration?

Contact Support

Can't find your favorite tool or service?

With the Acronis Cyber Protect Cloud platform, developers, software vendors and service providers can build new applications and share them with the Acronis community. Building a new application is fast and easy with a powerful low-code CyberApp Standard development framework. You can build a new integration or nominate your favorite tool for integration.

Build integration

Nominate a tool

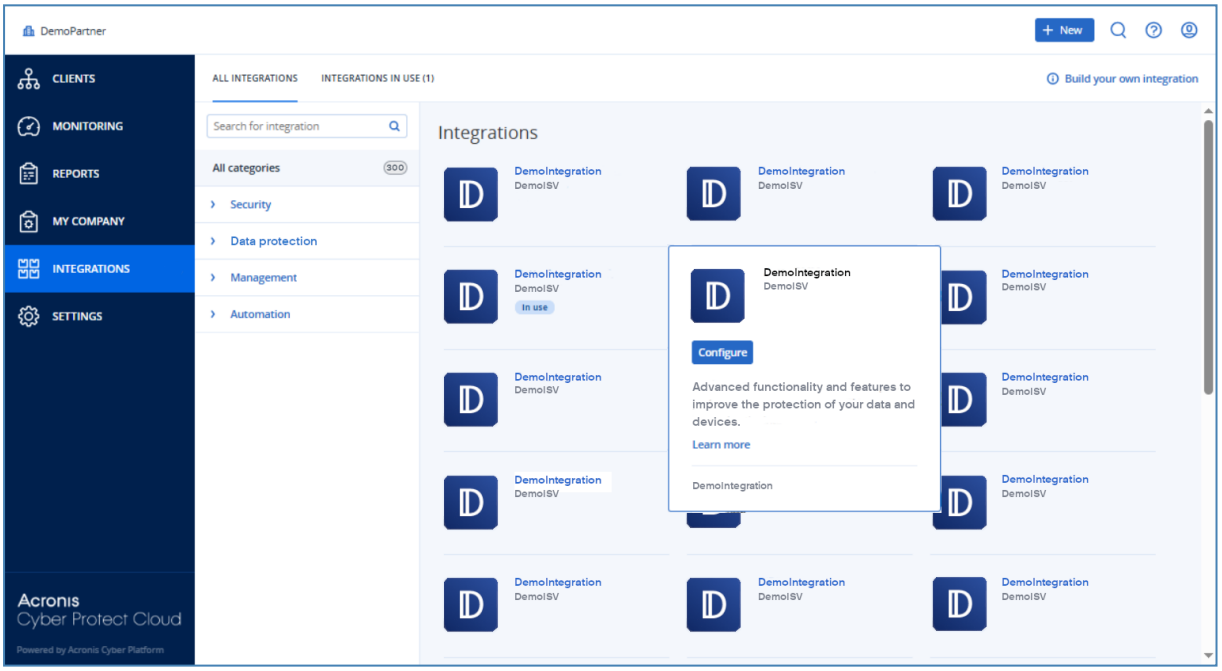
Engage with Acronis

Acronis © 2003–2024 Acronis International GmbH. Legal information | Privacy policy

統合の有効化

統合を有効化するには

1. データセンターで統合カタログを開きます。
2. 有効化する統合のカタログカードを見つけます。
   統合をフィルタリングするには:
   - （オプション） カテゴリを選択します。
   - （オプション） 検索フィールドに文字列を入力します。
3. カタログカードの上にホバーします。
4. **[設定]** をクリックします。
5. 画面の指示に従います。

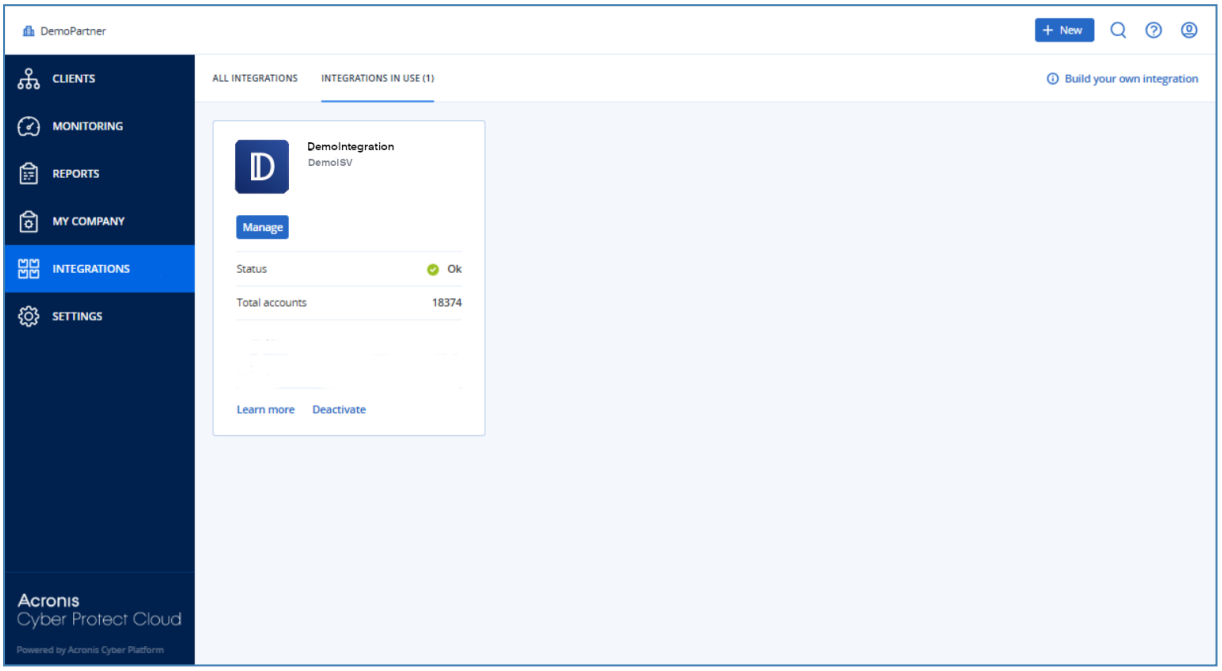


有効な統合の構成

有効な統合を構成するには

1. データセンターで統合カタログを開きます。
2. **[使用中の統合]** タブを選択します。
3. 構成する統合のカタログカードを見つけます。
4. **[管理]** をクリックします。
   統合構成画面が開きます。
5. 画面の指示に従うか、統合の文書を参照してください。

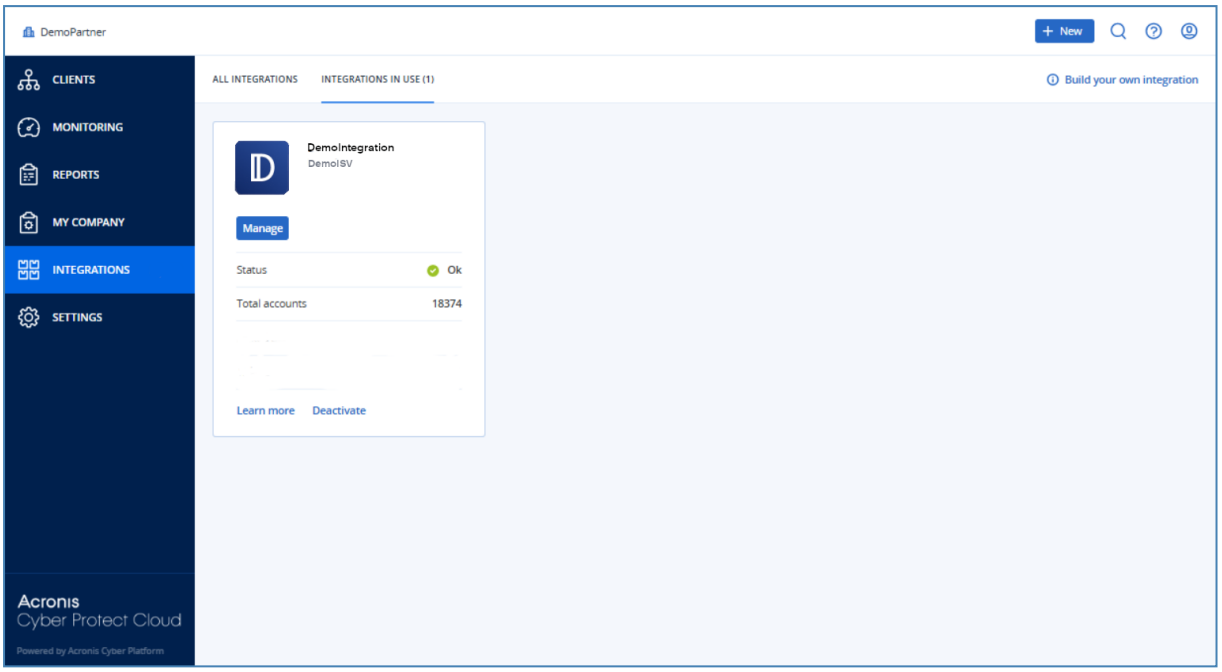
注意
文書は通常、カタログの詳細ページで入手できます。詳細については、統合の詳細ページを開くを参照してください。



有効な統合の無効化

統合を無効にするには

1. データセンターで統合カタログを開きます。
2. **[使用中の統合]** タブを選択します。
3. 無効にする統合のカタログカードを見つけます。
4. **[無効化]** をクリックします。
5. **[削除]** をクリックします。



APIクライアント

サードパーティシステム統合では、アプリケーションプログラミングインターフェイス（API）を使用できます。APIクライアントによりAPIへのアクセスが有効になり、これがプラットフォームのOAuth 2.0認証フレームワークの重要な部分となります。

APIクライアントは、プラットフォームデータおよびサービスデータにアクセスするために認証および承認する必要があるサードパーティシステムを表す特別なプラットフォームアカウントです。APIクライアントのアクセスは、管理ポータル管理者がクライアントを作成したテナントとそのサブテナントに限定されます。

注意
APIクライアントは、管理者アカウントのサービスロールを継承し、そのロールは後で変更することはできません。管理者アカウントのロールを変更したり、管理者アカウントを無効にしたりしても、クライアントには影響しません。

APIクライアントの資格情報

APIクライアントの資格情報は、一意の識別子（ID）とシークレット値で構成されます。この資格情報は、期限に定めがなく、管理ポータルや他のサービスコンソールへのログインに使用することはできません。

注意
このクライアントで二要素認証を有効にすることはできません。

APIクライアントのフロー

1. 管理ポータル管理者が、APIクライアントを作成します。
2. 管理者がサードパーティシステムでOAuth 2.0クライアント資格情報フローを有効にします。
3. APIでテナントやサービスにアクセスできるようになる前に、システムがこのフローに沿って、まず認証APIを使用してAPIクライアントの資格情報をプラットフォームに送信します。
4. プラットフォームがセキュリティトークン（そのクライアントに割り当てる固有の暗号文字列）を生成して送り返します。
5. その後、サードパーティシステムが、そのトークンをすべてのAPI要求に追加します。

注意
セキュリティトークンがあれば、API要求でクライアントの資格情報を渡す必要はありません。
セキュリティを強化するために、セキュリティトークンは2時間で期限切れになります。
この時間が経過すると、期限切れのトークンを使用したすべてのAPI要求は失敗し、システムはプラットフォームから新しいトークンを要求することになります。

APIクライアントの作成

APIクライアントを作成するには

1. 管理ポータルにログインします。
2. **[設定]** > **[APIクライアント]** > **[APIクライアントの作成]** をクリックします。
3. APIクライアントの名前を入力します。
4. **[次へ]** をクリックします。
   APIクライアントが作成され、デフォルトで **[アクティブ]** ステータスになります。
5. APIクライアントのIDとシークレット値とデータセンターのURLをコピーして保存します。サードパーティシステムでOAuth 2.0クライアント資格情報フローを有効にするときに、その情報が必要になります。

   重要
   セキュリティ上の理由で、シークレット値は1回しか表示されません。その値がわからなくなった場合、取得する方法はありません。リセットは可能です。

6. **[完了]** をクリックします。

APIクライアントのシークレット値のリセット

APIクライアントのシークレット値を失われた場合は、新しい値を生成できます。クライアントIDとデータセンターのURLは変更されません。

重要
このシークレット値をリセットすると、そのクライアントに割り当てられていたすべてのセキュリティトークンがすぐに期限切れになり、そのトークンが追加されていたAPI要求は失敗します。

APIクライアントのシークレット値をリセットするには

1. 管理ポータルにログインします。
2. **[設定]** > **[APIクライアント]** をクリックします。
3. リストで対象のクライアントを見つけます。
4. をクリックして、**[シークレットをリセット]** をクリックします。
5. **[次へ]** をクリックして、操作を確定します。
6. 新しいAPIクライアントシークレット値をコピーして保存します。

> **注意**
> セキュリティ上の理由で、シークレット値は1回しか表示されません。その値がわからなくなった場合、取得する方法はありません。手順を繰り返すことにより、リセットが可能です。

7. **[完了]** をクリックします。

APIクライアントの無効化

APIクライアントを無効にすることができます。無効にすると、クライアントに割り当てられているセキュリティトークンを使用したAPI要求は失敗しますが、トークン自体がすぐに期限切れになることはありません。

> **注意**
> クライアントを無効にしても、トークンの有効期限に影響はありません。

いつでもAPIクライアントを再度有効化できます。

APIクライアントを無効にするには

1. 管理ポータルにログインします。
2. **[設定]** > **[APIクライアント]** をクリックします。
3. リストで対象のクライアントを見つけます。
4. をクリックして、**[無効化]** をクリックします。
5. 操作を確定します。

無効にしたAPIクライアントの有効化

以前に無効にしたAPIクライアントを有効にすると、クライアントに割り当てられたセキュリティトークンを使用したAPI要求は、**トークンの有効期限が切れていなければ**成功します。

無効にされたAPIクライアントを有効にするには

1. 管理ポータルにログインします。
2. **[設定]** > **[APIクライアント]** をクリックします。
3. リストで対象のクライアントを見つけます。

4. をクリックして、**[有効]** をクリックします。
   APIクライアントのステータスが **[アクティブ]** に変わります。

APIクライアントの削除

APIクライアントを削除すると、そのクライアントに割り当てられていたすべてのセキュリティトークンがすぐに期限切れになり、そのトークンが追加されていたAPI要求は失敗します。

重要
削除したクライアントを復元する方法はありません。

APIクライアントを削除するには

1. 管理ポータルにログインします。
2. **[設定]** > **[APIクライアント]** をクリックします。
3. リストで対象のクライアントを見つけます。
4. をクリックして、**[削除]** をクリックします。
5. 操作を確定します。

統合の作成

Cyber Protect Cloudと統合するデータやサービスがある場合は、ベンダーポータルを使用してネイティブのCyberAppを作成するか、 API呼び出しを使用することができます。

CyberApp

ベンダーポータルは、サードパーティ製のソフトウェアベンダーが、CyberApp Standardのベストプラクティスに従って、Cyber Protect Cloud内で製品とサービスをネイティブに統合できるオンラインプラットフォームです。ベンダーポータルの統合は、CyberAppと呼ばれます。

注意
CyberAppとベンダーポータルの詳細については、統合ガイドを参照してください。

API統合

統合用の豊富なAPIスイートがあります。

注意
APIに関する詳細については、統合ガイドのプラットフォームAPIの章を参照してください。

Cyber Protect CloudとVMware Cloud Directorの統合

サービスプロバイダーは、VMware Cloud Director（旧称: VMware vCloud Director）とCyber Protect Cloudを統合し、すぐに使用可能な仮想マシンのバックアップソリューションをカスタマーに提供することができます。

統合には、次の手順が含まれます。

1. RabbitMQメッセージブローカーをVMware Cloud Director環境に設定します。
   RabbitMQはシングルサインオン（SSO）機能を提供しており、VMware Cloud Director資格情報を使用してCyber Protectコンソールにログインできます。
   Cyber Protect Cloudバージョン23.05（2023年5月リリース）以前では、VMware Cloud Director環境の変更をCyber Protect Cloudに同期させるためにRabbitMQも使用されます。
2. 管理エージェントを配置する。
   管理エージェントの配置時に、VMware Cloud Directorのプラグインもインストールされます。このプラグインにより、 Cyber ProtectionをVMware Cloud Directorのユーザーインターフェイスに追加します。
   管理エージェントは、VMware Cloud Director組織をCyber Protect Cloudのカスタマーテナントに、組織管理者をカスタマーテナントの管理者に、それぞれマッピングします。組織の詳細については、VMwareナレッジベースの「VMware Cloud Directorで組織を作成する」を参照してください。
   カスタマーのテナントは、VMware Cloud Directorの統合が構成されているパートナーのテナント内に作成されます。これら新規のカスタマーテナントは**ロック**モードになっており、パートナー管理者がCyber Protect Cloud内で管理することはできません。

   注意
   VMware Cloud Directorで一意のEメールアドレスを利用できる組織管理者のみが、 Cyber Protect Cloudにマッピングされます。

3. 1つまたは複数のバックアップエージェントを配置する。
   バックアップエージェントは、VMware Cloud Director環境で仮想マシンのバックアップおよび復元機能を提供します。

VMware Cloud DirectorとCyber Protect Cloudの統合を無効化したい場合は、テクニカルサポートにお問い合わせください。

制限事項

- VMware Cloud Directorとの統合は、**[サービスプロバイダーによる管理対象]** 管理モードのパートナーテナントで、その親テナントが **[サービスプロバイダーによる管理対象]** 管理モードを使用している場合に限り可能です。テナントの種類とそれぞれの管理モードについては、「"テナントの作成"（109ページ）」を参照してください。
  既存の直接パートナーはすべて、VMware Cloud Directorとの統合を構成できます。パートナー管理者は、子パートナーテナントの作成時に **[パートナー独自のVMware Cloud Directorインフラ]** チェックボックスを選択することで、サブテナントに対してもこのオプションを有効にできます。
- テナントで二要素認証が有効になっている場合、サービスアカウントとして設定されたパートナー管理者アカウントを使用する必要があります。それ以外の場合、エージェントはCyber Protect Cloudに対して認証できませません。
  エージェント用に専用アカウントを使用することをお勧めします。サービス アカウントの作成方法の詳細については、"ユーザーアカウントをサービスアカウントに変換するには"（128ページ）を参照してください。
- 複数のVMware Cloud Director組織で組織管理者ロールを割り当てられている管理者は、Cyber Protectionのいずれかのカスタマーテナントに対するバックアップと復元のみを管理できます。
- 新しいタブでCyber Protectコンソールが開きます。

ソフトウェア要件

サポートされるVMware Cloud Directorのバージョン

- VMware Cloud Director 10.4, 10.5, 10.6

VMware Cloud Director 10.4 および 10.5 では RabbitMQ メッセージブローカーが必要です。詳細については "RabbitMQメッセージブローカーの構成"（86ページ） を参照してください。VMware Cloud Director 10.6 にアップグレードする場合は、管理エージェントとバックアップエージェントを最新バージョンにアップデートする必要があります。詳細については "エージェントのアップデート"（94ページ） を参照してください。

推奨 Web ブラウザ

- Google Chrome 109以降
- Mozilla Firefox 115以降
- Opera 95 以降 (Chromium 109)
- Microsoft Edge 109以降
- Apple Safari（Mac OS X 用）16 以降、macOS および iOS オペレーティングシステムで実行

他のWebブラウザ（他のオペレーティングシステムで稼働するSafariブラウザなど）では、ユーザーインターフェースが正しく表示されないか、一部の機能が使用できない場合があります。

モバイルブラウザはサポートされていません。

RabbitMQメッセージブローカーの構成

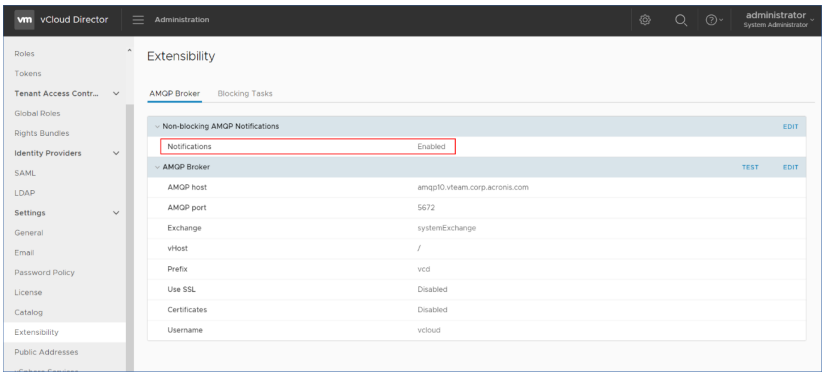
使用する場合 VMware Cloud Director 10.5 以前の場合は、RabbitMQ メッセージブローカーを構成する必要があります。

この手順はCyber Protect Cloudのバージョンによって異なります。バージョン23.06（2023年6月リリース）以降では、シンプルになった手順が使用されます。

RabbitMQを構成するには

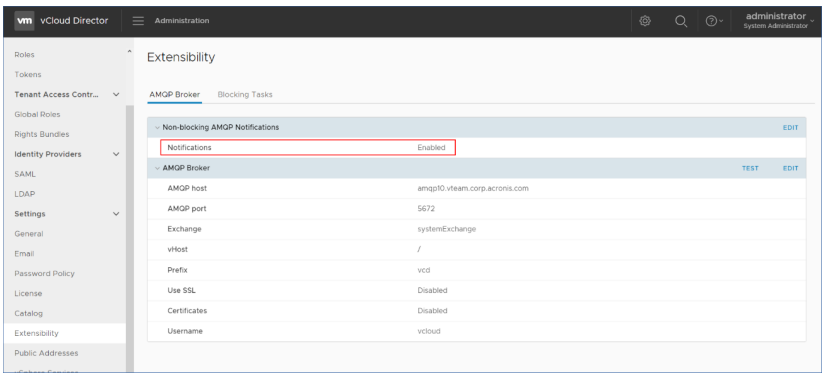
バージョン23.06以降

1. VMware Cloud Director環境に応じて、RabbitMQ AMQPブローカーをインストールします。
   RabbitMQのインストール方法の詳細については、VMwareのドキュメントを参照してください。
   RabbitMQのAMQPブローカーをインストールして構成します。
2. システム管理者としてVMware Cloud Directorプロバイダーポータルにログインします。
3. **[管理]** > **[拡張]** にアクセスし、**[ブロック対象でないAMQP通知]** で **[通知]** が有効になっていることを確認します。

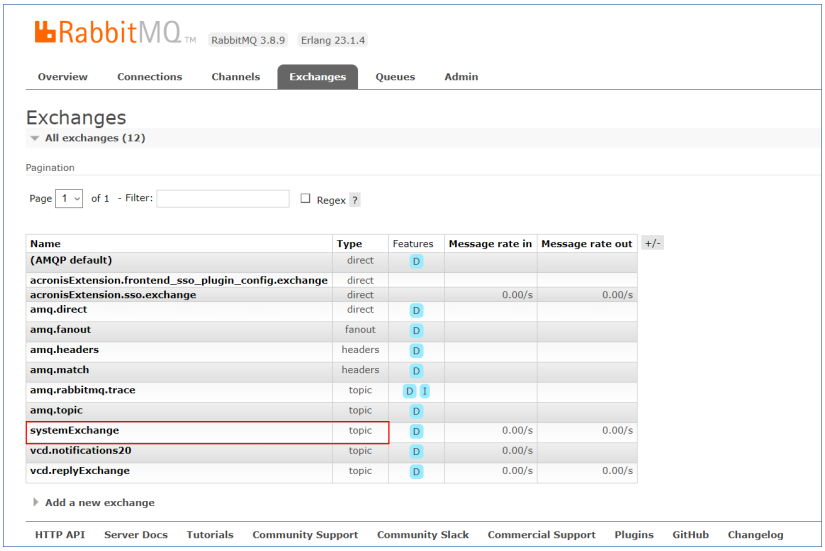


バージョン23.05以前

1. VMware Cloud Director環境に応じて、RabbitMQ AMQPブローカーをインストールします。
   RabbitMQのインストール方法の詳細については、VMwareのドキュメントを参照してください。
   RabbitMQのAMQPブローカーをインストールして構成します。
2. システム管理者としてVMware Cloud Directorプロバイダーポータルにログインします。
3. **[管理]** > **[拡張]** にアクセスし、**[ブロック対象でないAMQP通知]** で **[通知]** が有効になっていることを確認します。



4. RabbitMQ管理コンソールに管理者としてログインします。
5. **[Exchange]** タブで、Exchange（デフォルトでは**SystemExchange**という名前以下）が作成され、その種類が**トピック**であることを確認します。



VMware Cloud Directorのプラグインのインストールと公開

管理エージェントをインストールすると、VMware Cloud Directorのプラグインが自動的にインストールされます。

ただし、Cyber Protectionを利用するテナントには、手動でプラグインを公開する必要があります。

VMware Cloud Directorのプラグインを公開するには

1. システム管理者としてVMware Cloud Directorプロバイダーポータルにログインします。
2. ナビゲーションメニューから **[ポータルのカスタマイズ]** を選択します。
3. **[プラグイン]** タブで**Cyber Protection**プラグインを選択し、続いて **[公開]** をクリックします。
4. 公開のスコープを構成します。
   a. **[スコープ]** セクションでは、**[テナント]** チェックボックスのみを選択します。
   b. 既存および将来のすべてのテナントに対してプラグインを有効にする場合は **[公開]** セクションで、**[すべてのテナント]** を選択します。またプラグインを有効にする個別のテナントを選択することもできます。
5. **[保存]** をクリックします。
6. **[信頼]** をクリックします。

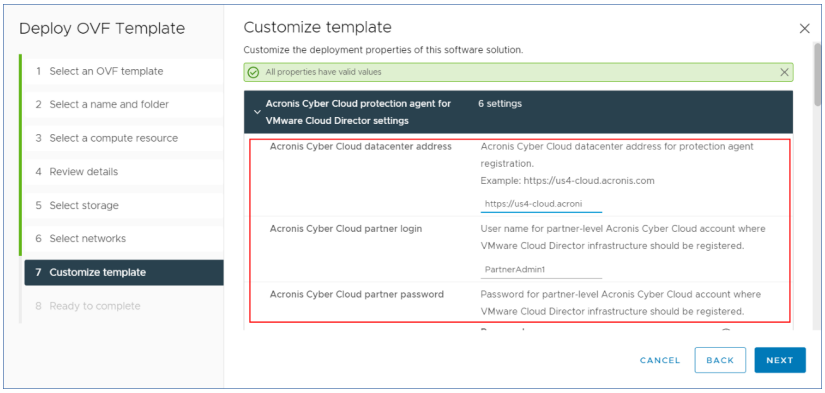
管理エージェントをインストールする

1. パートナー管理者としてCyber Protect Cloud管理ポータルにログインします。
2. **[設定]** > **[ロケーション]** に移動し、**[VMware Cloud Directorを追加]** をクリックします。

3. **[チャネルをリリース]** ドロップダウンリストで、エージェントのバージョンを選択します。次から選択できます。
   - **最新版** - 利用可能な最新バージョンです。
   - **以前の安定版** - プロテクション エージェントの以前のリリースにおける最新の安定版です。
4. **管理エージェント**のリンクをクリックして、ZIPファイルをダウンロードします。
5. 管理エージェントテンプレートファイル（`vCDManagementAgent.ovf`）と、仮想ハードディスクファイル（`vCDManagementAgent-disk1.vmdk`）を展開します。
6. vSphereクライアントで、VMware Cloud Directorにより管理されているvCenterインスタンス以下のESXiホストに、管理エージェントのOVFテンプレートを配置します。

重要
VMware Cloud Director環境ごとに、1つの管理エージェントのみをインストールできます。

7. 管理エージェントを構成するために、**[OVFテンプレートの配置]** ウィザードで、



   a. Cyber Protect Cloudデータセンターの URLを設定します。たとえば、`https://us5-cloud.example.com`です。
   b. パートナー管理者のログイン名とパスワード。

   注意
   テナントで二要素認証が有効になっている場合、サービスアカウントとして設定されたパートナー管理者アカウントを使用する必要があります。それ以外の場合、エージェントはCyber Protect Cloudに対して認証できませません。
   エージェント用に専用アカウントを使用することをお勧めします。サービス アカウントの作成方法の詳細については、"ユーザーアカウントをサービスアカウントに変換するには"（128ページ）を参照してください。

   c. VMware Cloud Director環境にある仮想マシンのバックアップストレージID。このバックアップストレージは、パートナーのみが所有できます。 ストレージの詳細については、「"ロケーションとストレージの管理"（167ページ）」を参照してください。
   IDを確認するには、管理ポータルで **[設定]** > **[ロケーション]** へ進み、任意のストレージを選択します。URLの**uuid**=の後にIDが表示されています。
   d. Cyber Protect Cloud課金モード: **ギガバイト単位**または**ワークロード単位**。

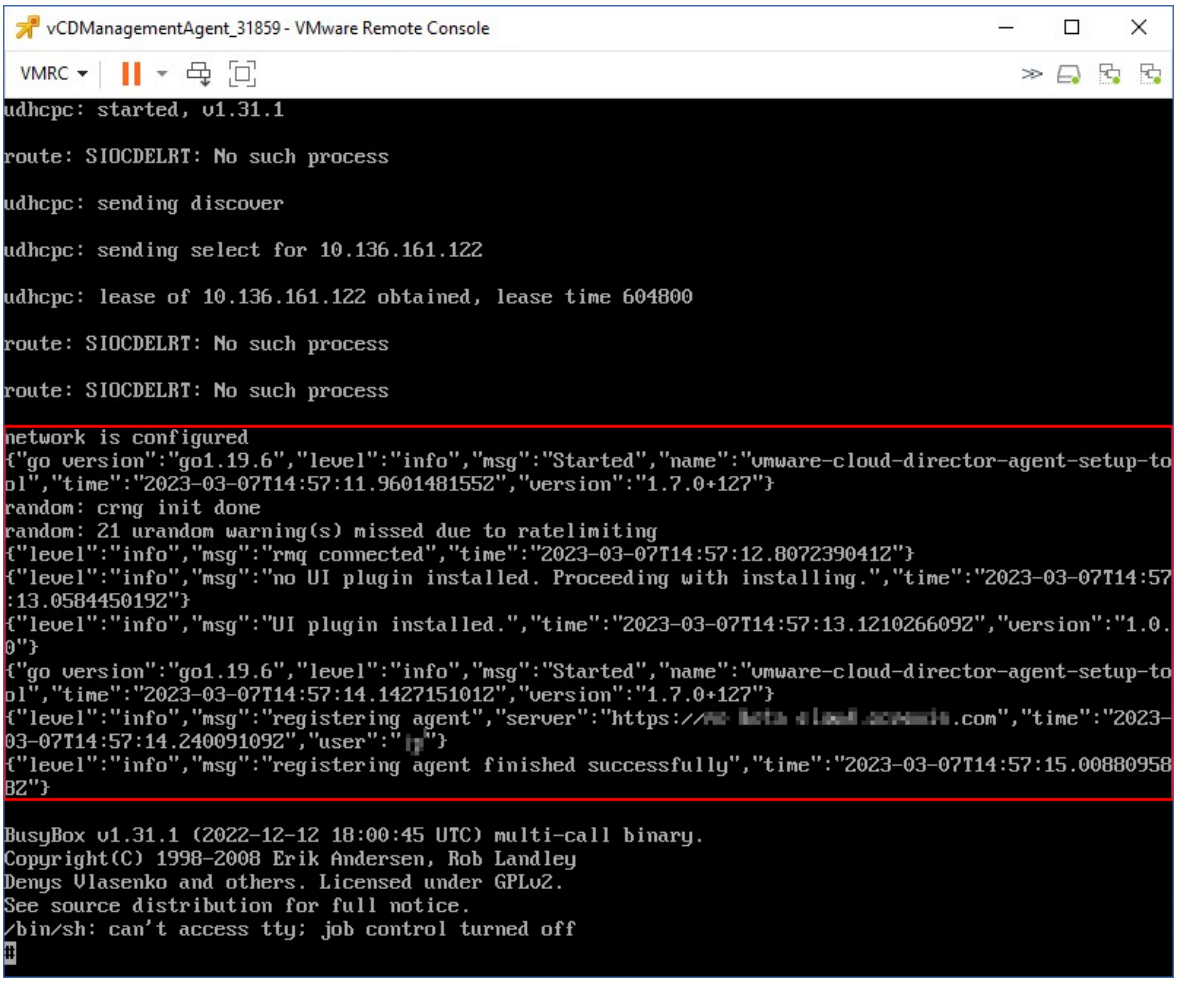
注意
選択された課金モードは、新しく作成されるすべてのカスタマーテナントに適用されます。

e. VMware Cloud Directorパラメータ: インフラストラクチャアドレス、システム管理者のログイン情報、パスワード。
f. [VMware Cloud Director 10.5 以前を使用している場合] RabbitMQ パラメータ: 管理者のログインとパスワード。
g. エージェントを含む仮想マシン上のrootユーザーのパスワード。
h. ネットワークパラメータ:IPアドレス、サブネットマスク、デフォルトゲートウェイ、DNS、DNSサフィックス。
   デフォルトでは、1つのネットワークインターフェースのみが有効化されています。2番目のネットワークインターフェースを有効にするには、**[eth1を有効化]** の隣にあるチェックボックスを選択します。

注意
ネットワーク設定で、管理エージェントがVMware Cloud Director環境とCyber Protect Cloudデータセンターの両方にアクセスできることを確認します。

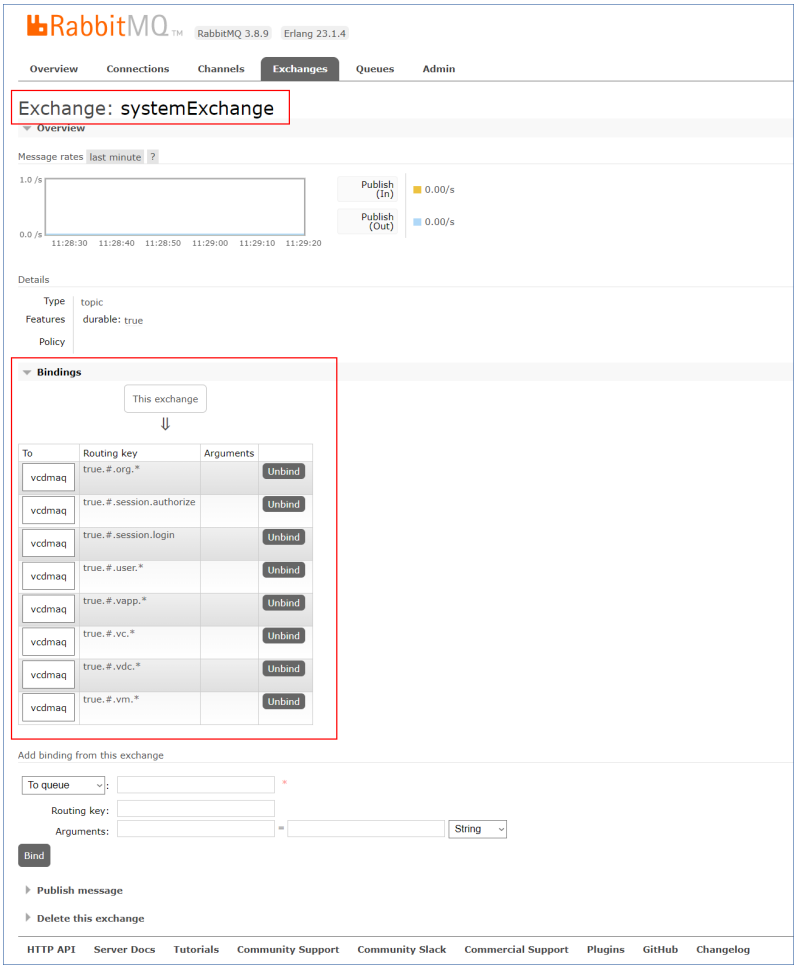
また初期配置後に、管理エージェントの設定を構成することもできます。vSphereクライアントで、管理エージェントを含む仮想マシンの電源をオフにして、**[設定]** > **[設定]** > **[vAppオプション]** をクリックします。任意の設定を適用してから、管理エージェント含む仮想マシンの電源をオンにします。

8. （オプション） vSphereクライアントで、管理エージェントを含む仮想マシンのコンソールを開き、セットアップを確認します。



9. [VMware Cloud Director 10.5 以前を使用している場合] RabbitMQ 接続を確認します。
   a. RabbitMQ管理コンソールに管理者としてログインします。
   b. **[Exchange]** タブで、RabbitMQのインストール時に設定したExchangeを選択します。デフォルトでは、**systemExchange**という名前になっています。

c. **vcdmaq**キューへの拘束力があることを確認します。



次に行うこと

エージェントのビルドが24.12.39185以降で、環境がVMware vSphere 8.x以降の場合、FIPS準拠モードを有効にできます。 "VMware Cloud DirectorのFIPS準拠モードの有効化"（93ページ）を参照してください。

バックアップエージェントをインストールする

1. パートナー管理者として管理ポータルにログインします。
2. **[設定]** > **[ロケーション]** に移動し、**[VMware Cloud Directorを追加]** をクリックします。
3. **[チャネルをリリース]** ドロップダウンリストで、エージェントのバージョンを選択します。次から選択できます。
   - **最新版** - 利用可能な最新バージョンです。
   - **以前の安定版** - プロテクション エージェントの以前のリリースにおける最新の安定版です。
4. **バックアップエージェント**のリンクをクリックして、ZIPファイルをダウンロードします。
5. バックアップエージェントテンプレートファイル（`vCDCyberProtectAgent.ovf`）と、仮想ハードディスクファイル（`vCDCyberProtectAgent-disk1.vmdk`）を展開します。

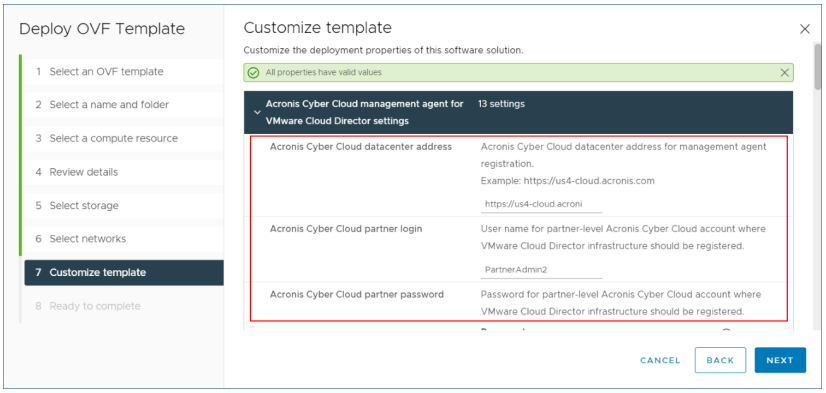
6. vSphereクライアントで、バックアップエージェントテンプレートを任意のESXiホストに配置します。

   ホストごとに、少なくとも1つのバックアップエージェントが必要です。デフォルトでは、バックアップエージェントに8GBのRAMと2つのCPUが割り当てられており、最大で5件のバックアップまたは復元タスクを同時に処理することができます。

   より多くのタスクを処理したり、バックアップや復元のトラフィックを分散させたりするには、同じホストに追加のエージェントを配置します。また、メモリの不足に関連する障害を回避するため、既存のエージェントに16GBのRAMと4個のvCPUを割り当てることをお勧めします。

   注意
   バックアップエージェントがインストールされていないESXiホスト上における仮想マシンのバックアップが、「タスクがタイムアウトしました」というエラーで失敗することがありました。

7. バックアップエージェントを構成するために、**[OVFテンプレートの配置]** ウィザードで、



   a. Cyber Protect CloudデータセンターのURLを設定します。たとえば、`https://us5-cloud.example.com`です。

   b. パートナー管理者のログイン名とパスワード。

      テナントで二要素認証が有効になっている場合、サービスアカウントとして設定されたパートナー管理者アカウントを使用する必要があります。それ以外の場合、エージェントはCyber Protect Cloudに対して認証できませません。

      エージェント用に専用アカウントを使用することをお勧めします。サービス アカウントの作成方法の詳細については、"ユーザーアカウントをサービスアカウントに変換するには"（128ページ）を参照してください。

   c. VMware vCenterのパラメータ: サーバーアドレス、ログイン名、パスワード。

      エージェントでは、これらの資格情報を使用してvCenter Serverへの接続が行われます。**管理者**ロールが割り当てられたアカウントを使用することをお勧めします。そうしない場合は、vCenter Server上で必要な権限を持つアカウントを指定します。

   d. エージェントを含む仮想マシン上の`root`ユーザーのパスワード。

   e. ネットワークパラメータ:IPアドレス、サブネットマスク、デフォルトゲートウェイ、DNS、DNSサフィックス。

デフォルトでは、単一のネットワークインターフェイスが有効化されています。2つ目のネットワークインターフェイスを有効化するには、**[eth1を有効化]** の横にあるチェックボックスを選択してください。

注意
ネットワーク設定で、バックアップエージェントがvCenter Serverと Cyber Protect Cloudデータセンターの両方にアクセスできることを確認します。

f. ダウンロード制限:最大ダウンロード速度です（単位: Kbps）。復元操作時のバックアップアーカイブの読み取り速度を定義します。デフォルト値は0（制限なし）です。
g. アップロード制限:最大アップロード速度です（単位: Kbps）。バックアップ操作時のバックアップアーカイブの書き込み速度を定義します。デフォルト値は0（制限なし）です。

また初期配置後に、バックアップエージェントの設定パラメータを構成することもできます。vSphereクライアントで、バックアップエージェントを含む仮想マシンの電源をオフにして、**[設定]** > **[設定]** > **[vAppオプション]** をクリックします。任意の設定を適用してから、バックアップエージェント含む仮想マシンの電源をオンにします。

8. vSphereクライアントで、バックアップエージェントを含む仮想マシンの**ホスト**と**Storage vMotion**が無効になっていることを確認します。

次に行うこと

エージェントのビルドが24.12.39185以降で、環境がVMware vSphere 8.x以降の場合、FIPS準拠モードを有効にできます。 "VMware Cloud DirectorのFIPS準拠モードの有効化"（93ページ）を参照してください。

VMware Cloud DirectorのFIPS準拠モードの有効化

FIPS準拠モードは、VMware vSphere 8.x以降における、エージェントビルド24.12.39185以降で有効にできます。このモードでは、バックアップエージェントは、すべての暗号化処理でFIPS 140-2準拠の暗号化ライブラリを使用します。詳細については、「FIPS準拠モード」を参照してください。

重要
FIPSモードを正常に動作させるには、管理エージェントとバックアップエージェントの両方でFIPSモードを有効にする必要があります。

クラウドディレクターインスタンスのCyber Protectエージェントで FIPS準拠モードを有効にするには

1. vSphere クライアントで、vCD管理エージェント仮想マシンを探し、リモートコンソールを開いて、次のコマンドを実行します。

```
fips-mode-setup --enable
```

2. vSphereクライアントに戻り、FIPS準拠モードを有効にするvCD Cyber Protectエージェント仮想マシンを探してから、リモートコンソールを開いて、次のコマンドを実行します。

```
fips-mode-setup --enable
```

3. FIPS準拠モードを有効にする他のすべてのvCD Cyber Protectエージェント仮想マシンでコマンドを実行します。

エージェントのアップデート

管理エージェントをアップデートするには

1. パートナー管理者として Cyber Protect Cloud管理ポータルにログインします。
2. **[設定]** > **[ロケーション]** に移動し、**[VMware Cloud Directorを追加]** をクリックします。
3. **管理エージェント**のリンクをクリックして、最新のエージェントを含むZIPファイルをダウンロードします。
4. 管理エージェントテンプレートファイル（vCDManagementAgent.ovf）と、仮想ハードディスクファイル（vCDManagementAgent-disk1.vmdk）を展開します。
5. vSphereクライアントで、現在の管理エージェント含む仮想マシンの電源をオフにします。
6. 最新のvCDManagementAgent.ovfおよびvCDManagementAgent-disk1.vmdkファイルを使用して、新規の管理エージェントを含む仮想マシンを配置します。
7. 以前のバージョンと同じ設定で、管理エージェントを構成します。
8. （オプション） 以前の管理エージェントを含む仮想マシンを削除します。

重要
各VMware Cloud Director環境に配置できるアクティブな管理エージェントは、1つのみです。

バックアップエージェントをアップデートするには

1. パートナー管理者として Cyber Protect Cloud管理ポータルにログインします。
2. **[設定]** > **[ロケーション]** に移動し、**[VMware Cloud Directorを追加]** をクリックします。
3. **バックアップエージェント**のリンクをクリックして、最新のエージェントを含むZIPファイルをダウンロードします。
4. 管理エージェントテンプレートファイルvCDCyberProtectAgent.ovfと、仮想ハードディスクファイルvCDCyberProtectAgent-disk1.vmdkを展開します。
5. vSphereクライアントで、現在のバックアップエージェント含む仮想マシンの電源をオフにします。現在実行中のバックアップタスクならびに復元タスクはすべて失敗します。タスクが実行されているかどうかを確認するには、vSphereクライアントで、バックアップエージェントを含む仮想マシンのコンソールを開き、コマンド「ps | grep esx_worker」を実行します。アクティブなesx_workerプロセスが存在しないことを確認します。
6. 最新のvCDCyberProtectAgent.ovfおよびvCDCyberProtectAgent-disk1.vmdkファイルを使用して、新規のバックアップエージェントを含む仮想マシンを配置します。
7. 以前のバージョンと同じ設定で、バックアップエージェントを構成します。
8. 以前のバックアップエージェントを含む仮想マシンを削除します。

バックアップ管理者の作成

組織管理者は、特別に割り当てられたバックアップ管理者にバックアップの管理を委任できます。

バックアップ管理者を作成するには

1. VMware Cloud Directorテナントポータルで、**[管理]** > **[ロール]** > **[新規]** をクリックします。
2. **[ロールを追加]** ウィンドウで、新しいロールの名前と説明を指定します。
3. 権限リストを下にスクロールして、**[その他]** 以下にある、**[セルフサービスのVMバックアップオペレーター]** を選択します。

   注意
   VMware Cloud Directorのプラグインをインストールすると、**[セルフサービスのVMバックアップオペレーター]** の許可が利用できるようになります。その方法については、「"VMware Cloud Directorのプラグインのインストールと公開"（87ページ）」を参照してください

4. VMware Cloud Directorテナントポータルで、**[ユーザー]** をクリックします。
5. ユーザーを選択して、**[編集]** をクリックします。
6. 作成した新しいロールをこのユーザーに割り当てます。

その結果、選択したユーザーは、この組織において仮想マシンのバックアップを管理できるようになります。

注意
VMware Cloud Director環境のシステム管理者は、**[セルフサービスのVMバックアップオペレーター]** の権限を有効にした汎用ロールを定義し、このロールをテナントに公開することができます。この場合、組織管理者に求められるのは、ユーザーにロールを割り当てることだけです。

システムレポート、ログファイル、構成ファイル

トラブルシューティングの際に、`sysinfo`ツールを使ってシステムレポートを作成したり、エージェントを使って仮想マシンのログファイルや構成ファイルを確認したりする必要が生じる場合があります。

仮想マシンには、vSphereクライアントのコンソールから直接アクセスしたり、SSHクライアントを使用してリモートでアクセスしたりできます。SSHクライアントで仮想マシンにアクセスするには、まず、対象のマシンへのSSH接続を有効にする必要があります。

仮想マシンに対するSSH接続を有効にするには

1. vSphereクライアントで、エージェントを含む仮想マシンのコンソールを開きます。
2. コマンドプロンプトでコマンド「`/bin/sshd`」を実行して、SSHデーモンを起動します。

これで、WinSCPなどのSSHクライアントを使って、この仮想マシンに接続できるようになります。

`sysinfo`ツールを実行するには

1. エージェントを含む仮想マシンにアクセスします。
   - 直接アクセスするには、vSphereクライアントで仮想マシンのコンソールを開きます。
   - リモートでアクセスするには、SSHクライアントで仮想マシンに接続します。
     デフォルトのログイン名とパスワードの組み合わせは、root:rootです。
2. /binディレクトリに移動して、sysinfoツールを実行します。

   ```
   # cd /bin/
   # ./sysinfo
   ```

   これにより、システムレポートのファイルがデフォルトのディレクトリ（/var/lib/Acronis/sysinfo）に保存されます。
   別のディレクトリを指定する場合は、--target_dirオプションを付けてsysinfoツールを実行します。

   ```
   ./sysinfo --target_dir path/to/report/dir
   ```

3. SSHクライアントを使って、生成されたシステムレポートをダウンロードします。

ログファイルまたは構成ファイルにアクセスするには

1. SSHクライアントで仮想マシンに接続します。
   デフォルトのログイン名とパスワードの組み合わせは、root:rootです。
2. 任意のファイルをダウンロードします。
   ログファイルは以下のロケーションにあります:
   - バックアップエージェント: /opt/acronis/var/log/vmware-cloud-director-backup-service/log.log
   - 管理エージェント: /opt/acronis/var/log/vmware-cloud-director-management-agent/log.log

   構成ファイルは以下のロケーションにあります:
   - バックアップエージェント: /opt/acronis/etc/vmware-cloud-director-backup-service/config.yml
   - 管理エージェント: /opt/acronis/etc/vmware-cloud-director-management-agent/config.yaml

Cyber Protectコンソールへのアクセス

VMware Cloud Director組織では、次のタイプの管理者が仮想マシンのバックアップを管理できます。

- 組織管理者
- 特別に割り当てられたバックアップ管理者
  このタイプの管理者を作成する方法については、「"バックアップ管理者の作成"（95ページ）」を参照してください。

管理者は、VMware Cloud Directorテナントポータルのナビゲーションメニューにある **[サイバープロテクション]** をクリックすることで、 カスタムCyber Protectコンソールにアクセスできます。

注意
シングルサインオンは組織管理者のみが利用できます。システム管理者によるVMware Cloud Director テナントポータルの利用はサポートされていません。

管理者はCyber Protectコンソールで、自分が所有するVMware Cloud Director組織要素（仮想データセンター、vApps、個別仮想マシン）にのみアクセスできます。VMware Cloud Director組織リソースのバックアップと復元を管理できます。

パートナー管理者は、カスタマーテナントのCyber Protectコンソールにアクセスし、カスタマーに代わってバックアップと復元を管理できます。

バックアップと復元の実行

保護計画の作成

バックアップ設定を構成するには、保護計画を作成する必要があります。

保護計画は複数のマシンに適用できます。また、同じマシンに複数の保護計画を適用することもできます。

制限事項

- マシン全体のバックアップのみがサポートされます。個々のディスクやボリュームをバックアップすることはできません。
- ファイルフィルタ（包含/除外）はサポートされていません。
- クラウドストレージが唯一の利用可能なバックアップロケーションです。ストレージは管理エージェント設定内で構成され、ユーザーが保護計画内で変更することはできません。
- 次のバックアップスキームがサポートされています:**常に増分（単一ファイル）**、**常に完全、日単位で増分バックアップ、週単位で完全バックアップ**。
- バックアップ後のクリーンアップもサポートされています。

保護計画を作成するには

1. Cyber Protectコンソールで **[デバイス]** > **[VMware Cloud Director]** に移動します。
2. 保護するマシンを選択して、**[保護]** をクリックします。
3. （すでに適用済みの計画の場合）**[計画を追加]** をクリックします。
4. **[計画の作成]** をクリックします。
5. **[暗号化]** で暗号化設定を行います。
6. （オプション） 保護計画の名前を変更するには、鉛筆のアイコンをクリックし、新しい名前を入力します。
7. （オプション） バックアップスキームまたはスケジュールを変更するには、**[スケジュール]** をクリックして設定を行います。
8. （オプション） 保持ルールを変更するには、**[保持する数]** をクリックして設定を行います。

9. （オプション） バックアップ・オプションを変更するには、**[バックアップオプション]** をクリックして設定を行います。
10. **[適用]** をクリックします。

マシンの復元

バックアップは元の仮想マシンにも別の仮想マシンにも復元できます。

制限事項

- ファイルレベルの復元はサポートされていません。
- VMware Cloud Director 10.4以降で別の仮想マシンにバックアップを復元できます。
  別の仮想マシンにバックアップを復元するには、エージェントバージョン24.02以降でバックアップを作成する必要があります。エージェントのバージョンは、エージェントのある仮想マシンの`/etc`ディレクトリにある`ProductVersion.conf`ファイルで確認できます。
- 別のマシンにバックアップを復元すると、別のマシンは**[デバイス]** > **[VMware Cloud Director]** > [組織] > [仮想データセンター] > **[スタンドアロンVM]** に表示されます。特定のvAppを復元 ターゲットとして選択することはできません。

マシンをリカバリするには

元のマシンに復元

1. Cyber Protect コンソールで、以下のいずれかの方法で復元ポイントを選択します。
   - **[デバイス]** > **[VMware Cloud Director]** に移動し、バックアップしたマシンを選択し、**[復元]** をクリックして、復元ポイントを選択します。
   - **[デバイス]** > **[VMware Cloud Director]** に移動し、バックアップアーカイブを選択し、**[バックアップの表示]** をクリックして、復元ポイントを選択します。
2. **[マシンを復元]** をクリックします。
3. **[復元を開始]** をクリックします。

別のマシンに復元

1. Cyber Protect コンソールで、以下のいずれかの方法で復元ポイントを選択します。
   - **[デバイス]** > **[VMware Cloud Director]** に移動し、バックアップしたマシンを選択し、**[復元]** をクリックして、復元ポイントを選択します。
   - **[デバイス]** > **[VMware Cloud Director]** に移動し、バックアップアーカイブを選択し、**[バックアップの表示]** をクリックして、復元ポイントを選択します。
2. **[マシンを復元]** をクリックします。
3. **[ターゲットマシン]** をクリックして **[新しいマシン]** を選択します。
4. その別のマシンの仮想データセンターを選択します。
5. 新しいマシンの名前を指定します。
   デフォルトでは、元のマシンの名前が表示されます。
6. **[OK]** をクリックします。

7. （オプション）**[VM設定]** をクリックして新しいマシンの以下の設定を変更し、**[OK]** をクリックします。
   - RAMのサイズ
   - 仮想プロセッサの数
   - ソケットあたりのコア数
   - ストレージのプロファイル
   - ネットワークアダプタと割り当てられたネットワーク
8. （オプション）**[ディスクマッピング]** をクリックしてディスクのディスクマッピングまたはストレージプ ロファイルを変更し、**[OK]** をクリックします。
9. **[復元を開始]** をクリックします。

VMware Cloud Directorとの統合を解除する

構成を元に戻し、Cyber Protect CloudからVMware Cloud Directorインスタンスの登録を解除するには、複雑な手順を実行する必要があります。サポート担当者にお問い合わせください。

管理ポータルの使用

次の手順では、管理ポータルの基本的な使い方について説明します。

推奨 Web ブラウザ

Webインターフェイスは、次のWebブラウザに対応しています。

- Google Chrome 109以降
- Mozilla Firefox 115以降
- Opera 95 以降 (Chromium 109)
- Microsoft Edge 109以降
- Apple Safari（Mac OS X 用）16 以降、macOS および iOS オペレーティングシステムで実行

他のWebブラウザ（他のオペレーティングシステムで稼働するSafariブラウザなど）では、ユーザーインターフェースが正しく表示されないか、一部の機能が使用できない場合があります。

モバイルブラウザはサポートされていません。

管理者アカウントの有効化

パートナーシップ契約を結ぶと、次の情報が含まれたメールメッセージが送信されます:

- **ログイン。**これは、ログインに使用するユーザー名です。ログイン情報は、アカウントのアクティベーションページにも表示されます。
- **[アカウントを有効化]**ボタン。ボタンをクリックして、アカウントのパスワードを設定します。パスワードは9文字以上にしてください。パスワードの詳細情報については、"パスワード要件"（100ページ）を参照してください。

パスワード要件

ユーザー登録時にパスワードの複雑さがチェックされ、次のいずれかに分類されます。

- 弱
- 中
- 強

パスワードの長さが十分でも、脆弱性のあるパスワードは保存できません。ユーザー名、ログイン名、ユーザーのEメールアドレス、またはユーザーアカウントが属するテナント名が繰り返し出現するパスワードは、いずれの場合でも脆弱であると見なされます。頻繁に使用されるパスワードも脆弱であると見なされます。

注意
パスワード要件は変更される場合があります。

パスワードの強度を高めるには、文字数を増やします。数字、大文字、小文字、記号など、さまざまな種類の文字を使用することは必須ではありませんが、これらを組み合わせることで、より強力で短いパスワードを作成できます。

管理ポータルのアクセス

管理者アカウントを有効化した後は、ログインと設定したパスワードを使用して管理ポータルにログインできます。

管理ポータルに初めてアクセスするには

1. サービスログインページに移動します。
   ログインページのアドレスは、受信したアクティベーションEメールに記載されています。
2. ログイン情報を入力して **[次へ]** をクリックします。
3. パスワード入力してから **[次へ]** をクリックします。

> **注意**
> ブルートフォース攻撃から Cyber Protect Cloudを保護するために、ログイン試行が10回失敗すると、ポータルはユーザーをロックアウトします。ロックアウト時間は5分です。ログインの試行に失敗した回数は、15分後にリセットされます。

4. オンボーディング調査を完了します。
   オンボーディング調査の詳細については、"オンボーディング調査"（101ページ）を参照してください。
5. 右側のメニューを使用して、[管理ポータル]に移動します。

管理ポータルのタイムアウト時間は、有効セッションに対しては24時間、アイドルセッションに対しては1時間です。

一部のサービスには、サービスコンソールから管理ポータルに切り替える機能が含まれています。

オンボーディング調査

オンボーディング調査は、テナントの最初のパートナー管理者が管理ポータルに初めてログインした際に完了する必要があります。このアンケートは、保護の優先分野、ビジネスモデル、企業規模に関する管理者の回答に基づいて動的に調整されます。オンボーディングエクスペリエンスをビジネスのニーズと関心に合わせて調整することで、プロセスの関連性と効率性が向上します。

この調査はスキップしたり閉じたりすることはできません。すべての質問に回答する必要があります。

企業プロファイルウィザードで連絡先を構成する

管理ポータルに初めてログインする際に、企業プロファイルウィザードのガイドに従って、会社の基本情報や任意の連絡先を入力できます。

ウィザードで会社の連絡先情報を設定し、必要に応じて後で変更できます。ご提供いただいた連絡先には、プラットフォームの新機能やその他の重要な変更に関する最新情報が送信されます。

Cyber Protectプラットフォームに存在するユーザーから連絡先を作成したり、サービスへのアクセス権を持たないユーザーの連絡先情報を追加したりできます。

注意
次の手順は、管理ポータルに初めてログインしたときのみ適用されます。後で会社の詳細や連絡先を変更するには、**[会社概要]** > **[企業プロファイル]**に移動します。会社の連絡先を設定するを参照してください。

企業プロファイルウィザードで企業の連絡先を構成するには

1. ウィザードの**会社情報**セクションで、所属会社に関する以下の詳細情報を提供します。
   - **法的な会社名**
   - **会社の登記上の所在地（本社住所）**
     - **国**
     - **郵便番号**
2. **[次へ]** をクリックします。
3. **会社の連絡先**で、次の用途で使用する連絡先を設定します。
   - **請求連絡先** - プラットフォームの使用状況レポートで、重要な変更に関するアップデートをお伝えするための連絡先です。
   - **業務連絡先** - プラットフォームにおける業務関連の重要な変更について、アップデートをお伝えするための連絡先です。
   - **技術連絡先** - プラットフォームにおける技術関連の重要な変更について、アップデートをお伝えするための連絡先です。

   連絡先は、複数の用途で使用できます。
   連絡先を作成するオプションを選択します。
   - **既存のユーザーから作成。**ドロップダウンリストからユーザーを選択します。
   - **新しい連絡先を作成。**以下の連絡先情報を提供してください。
     - **氏名（名）** - 連絡先となる担当者の名前です。このフィールドは必須です。
     - **氏名（姓）** - 連絡先となる担当者の姓です。このフィールドは必須です。
     - **業務用Eメールアドレス** - 連絡先となる担当者のEメールアドレスです。このフィールドは必須です。
     - **業務用電話番号** - このフィールドはオプションです。
     - **役職** - このフィールドはオプションです。
4. 請求書発行の連絡先を業務連絡先または技術連絡先としても使用する場合は、**請求のお問い合わせ**セクションで対応するフラグを選択します。
   - **業務関連の連絡先と同じ連絡先を使用してください**
   - **技術関連の連絡先と同じ連絡先を使用してください**
5. **[完了]** をクリックします。
   これにより、連絡先が作成されます。管理コンソールの **[会社概要]** > [企業プロファイル]セクションで情報を編集し、他の連絡先を設定できます。会社の連絡先を設定するを参照してください。

管理ポータルからCyber Protectコンソールへのアクセス

1. 管理ポータルで **監視** > **使用状況**へ進みます。
2. **[Cyber Protect]** の下で **[保護]** を選択してから、**[サービスを管理]** をクリックします。
   または、**[クライアント]** の下でカスタマーを選択してから、**[サービスの管理]** をクリックします。

これにより、Cyber Protectコンソールにリダイレクトされます。

重要
カスタマーの管理モードが**セルフサービス**の場合、代わりにサービスを管理することはできません。カスタマーモードを**サービスプロバイダーによる管理対象**に変更し、サービスを管理できるのはカスタマー管理者のみです。

管理ポータルのナビゲーション

管理ポータルを使用しているときは、常にテナントのコンテキスト内で操作しています。このテナントの名前は、アプリケーションの左上隅に表示されます。

管理ポータルにログインする際、デフォルトでは、使用可能な最上位の階層レベルが選択されています。リスト内のテナント名をクリックすると、階層を下にたどることができます。上位層に戻るには、左上隅の名前をクリックします。

ユーザーインターフェースでは、現在操作しているテナントのみが表示され、設定の範囲になります。例:

- **[クライアント]** タブには、現在作業しているテナントの直接の子オブジェクトのみが表示されます。**[表示]** ドロップダウンリストを使用して、テナントで有効になっているサービスの使用状況に関する統計を確認できます。
- **[監視]** タブには、現在作業しているテナントの直接の子オブジェクトの使用状況と操作に関する情報が表示されます。

  注意
  サブスクライブしているサービスによっては、このタブにその他のオプションが表示される場合があります。

- **[レポート]** タブでは、テナントおよびすべての子テナントのサービスとストレージの使用状況に関するレポートが表示されます。

  注意
  子テナントの管理モードによっては、パートナーとして、子パートナーテナントの下にある個々のカスタマーおよびそのユーザーに関する情報を表示できない場合があります。

- **[My Company（自分の会社）]** タブには、企業プロファイルと、現在操作しているテナントに存在するユーザーアカウントが表示されます。

[新規] ボタンを使用すると、テナントまたは新規ユーザーアカウントを現在操作しているテナントでのみ作成できます。

注意
サブスクライブしているサービスによっては、このメニューにその他のオプションが表示される場合があります。

受信トレイ

受信トレイページは、アプリケーション内でのコミュニケーションを効率化できるように設計されています。このガイドに従って、メッセージを効果的に管理し、整理して、生産性を向上させることができます。製品の受信トレイは、アプリケーション内でのコミュニケーションの受信と管理の中心的なハブです。重要なアップデート、メッセージ、およびアラートに関するワークフロー内の情報を常に把握できます。

概要

[受信トレイ] タブには、未読の通知の数を表示する通知カウンタがあります。このカウンタをクリックすると、未読の通知が表示されるため、保留中のアイテムを簡単に追跡できます。また、各フィルタ（カテゴリ、重要度、アクション）の横には、特定のフィルタで利用可能な通知の数を表示するカウンタがあり、各カテゴリにどのくらいの通知があるのか把握できます。

受信トレイには、アカウント設定とコンテキストに基づいて、機能のお知らせ、新しいトレーニングの案内、イベントやウェビナーの招待状、証明書の有効期限切れの通知、プロモーション、メンテナンス通知、アンケートなど、さまざまな通知が届きます。

通知の確認

通知セクションの確認

1. Cyber Protect Cloudコンソールにサインインします。
2. ナビゲーションペインで、**[受信トレイ]** メニュー項目を選択します。

受信トレイの検索

未読メッセージを検索するには

1. **[受信トレイ]** メニュー項目をクリックします。
2. 右上隅の **[未読のみ表示]** トグルを切り替えます。

受信トレイ内の重要な情報を検索するには

1. Cyber Protect Cloudダッシュボードから **[受信トレイ]** にアクセスします。
2. 受信トレイビューで、上部にある **[検索]** バーを見つけます。
3. 目的のキーワードや送信者名を入力して、メッセージをフィルタリングします。
4. **Enter** キーを押して検索結果を表示します。

検索条件に一致する通知がすべて表示されます。

管理ポータルの新機能

Cyber Protect Cloudの新しい機能がリリースされた場合、管理ポータルにログインすると、これらの機能について簡単な説明が記載されたポップアップウィンドウが表示されます。

また、管理ポータルのメインウィンドウの左下にある「**新機能**」のリンクをクリックすると、新機能の説明を確認できます。

Webインターフェイスへのアクセス制限

管理者は、テナントのメンバーがログインできるIPアドレスのリストを指定することにより、Webインターフェースへのアクセスを制限できます。

重要
ログイン制御を有効にすると、未登録のブータブルメディアを使用してクラウド ストレージから復元することができなくなります。詳細については、このKB記事を参照してください。

注意
- この制限事項は、API経由での管理ポータルへのアクセスにも適用されます。
- この制限は設定されたレベルでのみ適用されます。子テナントのメンバーには適用されません。

Webインターフェイスへのアクセスを制限する手順

1. 管理ポータルにログインします。
2. アクセスを制限したいテナントにナビゲートします。
3. **[設定]** > **[セキュリティ]** の順にクリックします。
4. **[ログイン管理]** スイッチを有効にします。
5. **[許可されたIPアドレス]** で、許可されたIPアドレスを指定します。
   次のいずれかのパラメータを、セミコロンで区切って入力できます。
   - IPアドレスの例:192.0.2.0
   - IPアドレス範囲の例:192.0.2.0-192.0.2.255
   - サブネットの例:192.0.2.0/24
6. **[保存]** をクリックします。

注意
サイバーインフラを利用するサービスプロバイダー向け（ハイブリッドモデル）:

管理ポータルの **[設定]** > **[セキュリティ]** で、**[ログイン管理]** スイッチが有効になっている場合は、**[許可されたIPアドレス]** リストにサイバーインフラストラクチャノードの外部パブリックIPアドレス（1つまたは複数）を追加してください。

7日間の履歴バー

クライアント画面では、**7日間の履歴**バーに、過去7日間の各カスタマーテナントにおけるワークロードのバックアップステータスが表示されます。このバーは168本の色付き線で表示されます。各線が1時間の間隔を表し、対応する1時間の間隔内で、もっとも悪いバックアップステータスを表示します。

線の各色が表す意味については、次の表を参照してください。

色	説明
赤	1時間の間に少なくとも1回のバックアップが失敗している
オレンジ	1時間の間に少なくとも1回のバックアップが警告をともない完了しているが、バックアップエラーは発生していない
緑	1時間の間に少なくとも1回のバックアップが成功しており、バックアップエラーや警告が発生していない
グレイ	1時間の間に完了したバックアップは存在しない

対応する統計情報の収集が行われるまで、**7日間の履歴**バーには、「バックアップなし」と表示されます。

パートナーテナントの場合、集計された統計情報がサポートされていないため、**7日間の履歴**バーは空白になります。

ユーザーアカウントとテナント

ユーザーアカウントには、管理者アカウントとユーザーアカウントの2つの種類があります。

- **管理者**は管理ポータルにアクセスできます。管理者は、すべてのサービスで管理者権限を持ちます。
- **ユーザー**は管理ポータルにアクセスできません。サービスへのアクセスとサービスにおけるその権限は、管理者が定義します。

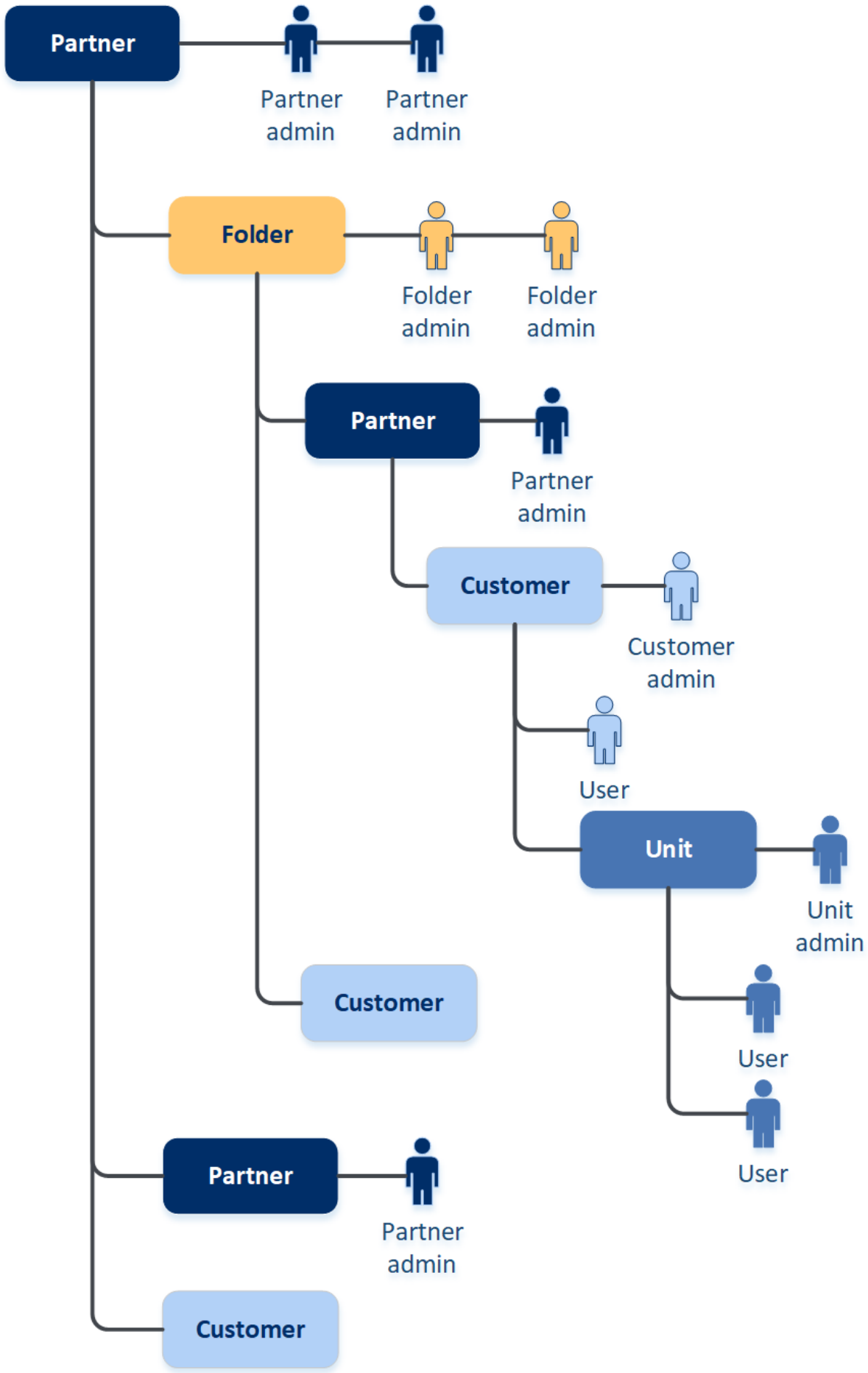
それぞれのアカウントはテナントに属しています。テナントは、パートナーや顧客専用の管理ポータルリソース（ユーザーアカウントや子テナントなど）とサービス提供（有効なサービスとその中のソリューションアイテム）の一部です。テナント階層は、サービスユーザーとプロバイダーの間のクライアント/ベンダーの関係と一致させる必要があります。

- **パートナー**のテナント種別は通常、サービスを再販するサービスプロバイダーに適用します。
- **フォルダ**のテナント種別は通常、パートナー管理者がパートナーと顧客をグループ化して、別々のソリューションや異なるカスタマイズ設定を構成するために使用する補助的なテナントです。
- **顧客**のテナント種別は通常、サービスを使用する組織に適用します。
- **部署**のテナント種別は通常、組織の部署や部門に適用します。

管理者は、階層における管理者のレベル以下のテナント、管理者アカウント、ユーザーアカウントを作成および管理できます。

管理モードが [**サービスプロバイダーによる管理対象**] になっている**顧客**または**パートナー**タイプのテナントでは、**パートナー**タイプの親テナント管理者が、下層管理者として行動することができます。それで、パートナーレベルの管理者は、たとえば、ユーザーアカウントとサービスを管理したり、子テナントのバックアップやその他のリソースにアクセスしたりできます。ただし、下位レベルの管理者は、上位レベルの管理者に対して、自分のテナントへのアクセスを制限できます。

次の図は、パートナー、フォルダ、顧客、および部署テナントの階層の例を示しています。


Partner
Partner admin
Partner admin
Folder
Folder admin
Folder admin
Partner
Partner admin
Customer
Customer admin
User
Unit
Unit admin
User
User
Customer
Partner
Partner admin
Customer

管理者とエンドユーザーによるバックアップアカウントの操作権限は以下のとおりです。

操作	ユーザー	カスタマーおよび部署の管理者	パートナーおよびフォルダの管理者
テナントの作成	いいえ	はい	はい
アカウントの作成	いいえ	はい	はい
ソフトウェアのダウンロードとインストール	はい	はい	いいえ*
サービスの管理	はい	はい	はい
使用状況レポートの作成	いいえ	はい	はい
カスタマイズの設定	いいえ	いいえ	はい

注意

- ユーザーはどのタイプのテナントからでも作成できます。ユーザーを作成する際は、最も大きい権限を付与されているテナントから、権限が最も小さなテナントまで、共有のEメールアドレスを指定することができます。例えば、パートナーテナントではフォルダ、カスタマー、ユニットテナントを作成できますが、カスタマーテナントではフォルダテナントを作成できません。
- ユニットの管理者は、Disaster Recovery保護計画を作成、変更、適用することはできません。

テナントの管理

Cyber Protectで利用できるテナントは次のとおりです:

- **パートナー**テナントは通常、パートナー契約を結んでいるパートナーごとに作成されます。
- **フォルダ** テナントは、通常、同じ提供項目を有効にしたり、共通のブランディング設定を構成したりするパートナーとカスタマーをグループ化するために作成されます。
- **顧客**テナントは通常、サービス契約を結んでいる組織ごとに作成されます。
- **[部署]**テナントは、新しい組織単位（OU）でサービスを管理するために、カスタマーのテナント内に作成されます。

テナントの作成および構成の手順は作成するテナントにより異なりますが、通常は次のようなプロセスとなります:

1. テナントを作成します。
2. テナントのサービスを有効にします。
3. テナントのサービスのクォータを設定します。

テナントの作成

パートナーテナントとして、次のテナントタイプを作成できます。

- **パートナー**テナントは通常、パートナー契約を結んでいるパートナーごとに作成されます。
- **フォルダ** テナントは、通常、同じ提供項目を有効にしたり、共通のブランディング設定を構成したりするパートナーとカスタマーをグループ化するために作成されます。
- **顧客**テナントは通常、サービス契約を結んでいる組織ごとに作成されます。
- **[部署]**テナントは、新しい組織単位（OU）でサービスを管理するために、カスタマーのテナント内に作成されます。

パートナー

パートナーテナントを作成するには

1. 管理ポータルにログインします。
   クライアントのリストがデフォルトで開きます。
2. [複数の子テナントがある場合] パートナーテナントを作成するパートナーテナントに移動します。
3. 右上にある **[新規]** > **[パートナー]** をクリックします。
4. **[パートナー名]** で、新しいテナントの名前を指定します。
5. （オプション）**[言語]** で、このテナントで使用される通知、レポート、およびソフトウェアインターフェイスのデフォルト言語を変更します。
6. **正式（法的）会社名**（必須）と**VAT番号、税務IDまたは会社登録番号**（任意）を入力します。
7. **詳細設定**の下で、テナントへのアクセスを管理するモードを選択します。
   - **フルアクセス** – このモードでは、親テナントの管理者に対してテナントへのフルアクセス権限が付与されます。つまり、パートナーのクォータ、ユーザー、プロパティを管理し、パートナーのカスタマーにアクセスし、パートナーとそのカスタマーの使用状況レポートを取得できます。このモードはデフォルトでオンになっています。
   - **制限アクセス** – このモードでは、親テナントの管理者は、このパートナーテナントへのアクセスが制限されます。つまり、テナントのプロパティとクォータのみを変更でき、パートナーおよびパートナーのカスタマーの使用状況レポートを取得できますが、パートナーのリソース（テナント、ユーザー、サービス、バックアップなど）を管理することはできません。また、パートナーのカスタマーの使用状況レポートを取得することもできません。

     注意
     [制限アクセス] を選択した場合、テナントの管理者のみが管理モードを変更できます。このため、管理者は、**[設定]** > **[セキュリティ]** に移動して、**[サポートにアクセス]**スイッチを有効にする必要があります。

   [クライアント] タブで、子テナントに対して選択された管理モードを確認できます。

注意

二要素認証（2FA）は、すべてのパートナーテナント（直接および間接）の本番モードでデフォルトで有効になっており、無効にすることはできません。テナントのすべてのユーザーは、よりセキュアなアクセスのために、アカウントの二要素認証を構成する必要があります。詳細については、二要素認証の設定を参照してください。

トライアルモードのパートナーの場合、アカウントが本番モードに切り替えられると、二要素認証が自動的に有効になります。

8. **[次へ]** をクリックします。
9. **[管理者を作成]**セクションで、管理者アカウントを構成します。

注意

管理モードが**[限定]**に設定されているパートナー テナントでは、管理者の作成が必須です。

a. 管理者アカウントのEメールアドレスを入力します。このEメールアドレスがログイン情報としても使用されます。
b. （オプション） Eメールアドレスとは異なるログイン情報を使用したい場合は、**[Eメールとは異なるログイン情報を使用する]** チェックボックスを選択し、管理者アカウントのログイン情報とEメールアドレスを入力します。

   残りのフィールドはオプションですが、管理者に連絡する必要がある場合に備えて、より多くの通信チャネルを提供しておくことができます。
c. （オプション） 言語を選択します。

   言語を選択しない場合、デフォルトでは英語が使用されます。
d. （オプション） **[連絡先の詳細]**の下で、追加の会社の連絡先を入力します。
   - **課金** - プラットフォームの使用状況レポートで、重要な変更に関するアップデートをお伝えするための連絡先です。
   - **技術** - プラットフォームにおける技術関連の重要な変更について、アップデートをお伝えするための連絡先です。
   - **業務** - プラットフォームにおける業務関連の重要な変更について、アップデートをお伝えするための連絡先です。

   注意

   単一のユーザーに1件または複数の会社の連絡先を割り当てることができます。

10. （オプション） **[言語]** で、このテナントで使用される通知、レポート、およびソフトウェアのデフォルト言語を変更します。
11. 次のいずれかを実行します。
    - テナントの作成を完了するには、**[作成]**をクリックします。

      この場合、すべての該当するライセンスとサービスはテナントに対して有効になります。
    - テナントで有効にするサービスを選択するには、**サービスのカスタマイズ (オプション)**をクリックします。

      "テナントのサービス、提供項目、クォータの構成"（115ページ）を参照してください。

フォルダ

フォルダを作成するには

1. 管理ポータルにログインします。
   クライアントのリストがデフォルトで開きます。
2. [子テナントが複数ある場合] フォルダテナントを作成するパートナーテナントに移動します。

   注意
   フォルダテナントは、パートナー テナントの下にのみ作成できます。

3. 右上にある **[新規]** > **[フォルダ]** をクリックします。
4. **[フォルダ名]** フィールドで、新しいテナントの名前を指定します。
5. （オプション）**[言語]** で、このテナントで使用される通知、レポート、およびソフトウェアインターフェイスのデフォルト言語を変更します。
6. **[次へ]** をクリックします。
7. **[管理者を作成]** で、管理者アカウントを作成します。
   a. 管理者アカウントのEメールアドレスを入力します。
      このEメールアドレスがログイン情報としても使用されます。
   b. Eメールアドレスとは異なるログイン情報を使用したい場合は、**[Eメールとは異なるログイン情報を使用する]**チェックボックスを選択し、管理者アカウントの姓名を入力します。
      残りのフィールドはオプションですが、管理者に連絡する必要がある場合に備えて、より多くの通信チャネルを提供しておくことができます。
      - **連絡先の詳細**の下で、電話番号、役職を入力し、会社の連絡先を指定します。
        - **課金** - プラットフォームの使用状況レポートで、重要な変更に関するアップデートをお伝えするための連絡先です。
        - **技術** - プラットフォームにおける技術関連の重要な変更について、アップデートをお伝えするための連絡先です。
        - **業務** - プラットフォームにおける業務関連の重要な変更について、アップデートをお伝えするための連絡先です。

        注意
        単一のユーザーに1件または複数の会社の連絡先を割り当てることができます。

8. 次のいずれかを実行します。
   - テナントの作成を完了するには、**[作成]**をクリックします。
     この場合、すべての該当するライセンスとサービスはテナントに対して有効になります。
   - テナントで有効にするサービスを選択するには、**サービスのカスタマイズ (オプション)**をクリックします。
     "テナントのサービス、提供項目、クォータの構成"（115ページ）を参照してください。

顧客

カスタマーテナントを作成するには

1. 管理ポータルにログインします。
   クライアントのリストがデフォルトで開きます。
2. [子テナントが複数ある場合] カスタマーテナントを作成するテナントに移動します。
3. 右上隅の **[新規]** をクリックし、**[カスタマー]** を選択します。
4. **[カスタマー名]** で、新しいテナントの名前を指定します。
5. （オプション） **[言語]** で、このテナントで使用される通知、レポート、およびソフトウェアのデフォルト言語を変更します。
6. （オプション） **[国/地域]**および**[業界]**フィールドにデータを入力します。
7. **処理モード**で、テナントが**トライアル:30日間の評価**モードでサービスを使用しているか、**製品版/本番** モードでサービスを使用しているかを選択します。
   月次サービス使用状況レポートには、両方のモードのテナントの使用状況データが含まれます。

   重要
   トライアルモードでは、30日間の評価期間が有効になり、製品に完全にアクセスできます。カスタマーが本番モードに切り替わると、その使用量は自動的に直近の請求サイクルに含まれることにご注意ください。
   いつでも製品版/本番 モードに切り替えることができます。ただし、製品版/本番モードからトライアルモードへの切り替えはできません。
   カスタマーのトライアルをキャンセルする場合、対応するカスタマーテナントを削除する必要もあります。そうしないと、30日間の試用期間が終了した時点で、そのカスタマーは自動的に本番モードに切り替わり、直近の請求サイクルでそれに応じた使用量が含まれることになります。詳細については、このナレッジベースの記事を参照してください。

8. **詳細設定**で、カスタマーテナントの管理モードを選択します。
   - **サービスプロバイダーによる管理** - このモードでは、親テナントの管理者にカスタマーへのフルアクセス（プロパティの変更、テナント、ユーザー、サービスの管理、バックアップやその他のリソースへのアクセス）を許可します。このモードはデフォルトで選択されています。
   - **カスタマーによる管理対象** - このモードでは、親テナントの管理者によるこのテナントへのアクセスを制限します。管理者は、テナントのプロパティを変更することはできますが、テナント内部（テナント、ユーザー、ユニット、サービス、バックアップ、その他のリソースなど）にアクセスしたり管理したりすることはできません。

     注意
     [カスタマーによる管理対象]を選択した場合、カスタマーテナントの管理者のみが管理モードを変更できます。このため、カスタマーの管理者は、**[設定]** > **[セキュリティ]** に移動して、**[サポートにアクセス]** スイッチを有効にする必要があります。

   [クライアント] タブで、子テナントに対して選択された管理モードを確認できます。
9. テナントの二要素認証 (2FA) を有効または無効にします。
   二要素認証が有効になっている場合、このテナントのすべてのユーザーは、よりセキュアなアクセスのためにアカウントの二要素認証を構成する必要があります。ユーザーは、二要素目のデバイスに認

証アプリケーションをインストールし、従来のログインとパスワードとともに、生成された一度のみ有効のTOTPコードを使用して、Cyber Protect Cloudコンソールにログインする必要があります。

詳細については、「二要素認証の設定」を参照してください。

カスタマーの二要素認証のステータスを確認するには、**[クライアント]** に移動します。

10. （オプション）**[コンプライアンスモード]** チェックボックスを選択します。

    このモードでは、暗号化されたバックアップのみが許可されます。暗号化パスワードは保護対象のデバイス上で設定する必要があります。暗号化パスワードがない場合、バックアップの作成は失敗します。クラウドサービスに対して、暗号化パスワードを提供する必要があるすべての操作は、利用できません。詳細については、"コンプライアンスモード"（118ページ）を参照してください。

    重要
    テナントの作成後にコンプライアンスモードを無効にすることはできません。

11. **[次へ]** をクリックします。
12. **[管理者を作成]**セクションで、管理者アカウントを構成します。

    注意
    管理モードが**セルフサービス**に設定されたカスタマーテナントの場合、管理者の作成が必須となります。

    a. 管理者アカウントのEメールアドレスを入力します。このEメールアドレスがログイン情報としても使用されます。
    b. Eメールアドレスとは異なるログイン情報を使用したい場合は、**[Eメールとは異なるログイン情報を使用する]**チェックボックスを選択し、管理者アカウントの姓名を入力します。

       残りのフィールドはオプションですが、管理者に連絡する必要がある場合に備えて、より多くの通信チャネルを提供しておくことができます。
    c. （オプション） 言語を選択します。

       言語を選択しない場合、デフォルトでは英語が使用されます。
    d. （オプション） 会社の連絡先を指定します。
       - **課金** - プラットフォームの使用状況レポートで、重要な変更に関するアップデートをお伝えするための連絡先です。
       - **技術** - プラットフォームにおける技術関連の重要な変更について、アップデートをお伝えするための連絡先です。
       - **業務** - プラットフォームにおける業務関連の重要な変更について、アップデートをお伝えするための連絡先です。

       注意
       単一のユーザーに1件または複数の会社の連絡先を割り当てることができます。

13. 次のいずれかを実行します。
    - テナントの作成を完了するには、**[作成]**をクリックします。

      この場合、すべての該当するライセンスとサービスはテナントに対して有効になります。

- テナントで有効にするサービスを選択するには、**サービスのカスタマイズ (オプション)**をクリックします。

  "テナントのサービス、提供項目、クォータの構成"（115ページ）を参照してください。

ユニット

部署を作成するには

1. 管理ポータルにログインします。

   クライアントのリストがデフォルトで開きます。
2. [子テナントが複数ある場合] 部署を作成するカスタマーテナントに移動します。

   注意
   部署テナントは、カスタマーテナントの下にのみ作成できます。
3. 右上にある **[新規]** > **[部署]** をクリックします。
4. **[部署名]** で、新しいテナントの名前を指定します。
5. （オプション） **[言語]** で、このテナントで使用される通知、レポート、およびソフトウェアのデフォルト言語を変更します。
6. （オプション） **[次へ]** をクリックします。
7. **[管理者を作成]** で、管理者アカウントを構成します。
   a. 管理者アカウントのEメールアドレスを入力します。このEメールアドレスがログイン情報としても使用されます。
   b. Eメールアドレスとは異なるログイン情報を使用したい場合は、**[Eメールとは異なるログイン情報を使用する]** チェックボックスを選択し、管理者アカウントの姓名を入力します。

      残りのフィールドはオプションですが、管理者に連絡する必要がある場合に備えて、より多くの通信チャネルを提供しておくことができます。
   c. （オプション） **[連絡先の詳細]**の下で、言語を選択します。

      言語を選択しない場合、デフォルトでは英語が使用されます。
8. 次のいずれかを実行します。
   - テナントの作成を完了するには、**[作成]**をクリックします。

     この場合、すべてのサービスと請求書発行がテナントに対して有効になります。
   - テナントのサービスを選択するには、**[カスタマイズサービス(オプション)]** をクリックします。

     "テナントのサービス、提供項目、クォータの構成"（115ページ）を参照してください。

テナントのサービス、提供項目、クォータの構成

デフォルトで有効になっているサービスは、作成するテナントの種類によって異なります。部署テナントの場合、親カスタマーテナントで有効になっているすべてのサービスがデフォルトで有効になります。

デフォルトではサービスは有効になっています

サービス	パートナーテナント	フォルダ	カスタマーテナント
保護	はい	はい	はい
物理データ配送	はい	はい	いいえ
Cyber Infrastructure	はい	はい	なし
アクロニスサポート	はい	なし	なし
File Sync & Share	はい	なし	いいえ

新しいテナントを作成すると、選択されたサービスのすべての提供項目が有効になります。テナント内のユーザーとその子テナントで利用できる提供項目を選択し、それらにクォータを設定できます。この手順はすべて任意です。

ライセンス、請求書発行、提供項目に関する詳細については、パートナーポータルの "ライセンスモード"（9ページ）、"標準および追加の保護サービス"（42ページ）、および「ライセンスガイド」を参照してください。

テナントの提供項目とクォータを設定するには

1. テナント作成ダイアログの下部で**サービスのカスタマイズ（オプション）**をクリックします。
2. [パートナー、フォルダ、またはカスタマーテナントを作成する場合] **[保護]** サービスページで、ライセンスモードを選択します。
   - **ソリューションベース（ワークロードごと）** - ワークロードごとに請求され、セキュリティとRMM、バックアップとDisaster Recovery、究極の保護（セキュリティ、RMM、バックアップ、DRなどを含む）など、保護サービスの最も一般的なニーズに対応するサービスバンドルを通じてライセンスが簡素化されます。追加サービスでバンドルを拡張できます。
   - **サービスベース（ワークロードごと）** - ワークロードごとに請求され、保護対象のワークロードで利用可能な提供項目のより詳細な制御を可能にします。ライセンスは、追加の保護サービスで拡張できる標準保護サービスで構成されています。使用されたクラウドストレージは別途請求されます。
   - **サービスベース（ギガバイト単位）** - 使用したクラウドおよびローカルストレージに基づいて請求され、ワークロードライセンスと同じ機能セットを提供します。

   注意
   カスタマーテナントでは、同時に有効にできるライセンスモードは 1 つだけです。パートナーテナントとフォルダテナントでは、すべてのライセンスモードを同時に有効にできます。

3. テナントで有効にする提供項目を制御するには、チェックボックスを使用します。

   注意
   使用可能な提供項目は、選択したライセンスによって異なります。

- 無効にする提供項目のチェックボックスをオフにします。
  テナントとその子テナント内のユーザーは、無効になっているソリューションアイテムに対応する機能を利用できません。
- 有効にする提供項目のチェックボックスを選択します。

4. 提供項目のクォータを指定するには、隣にある**[無制限]** リンクをクリックし、クォータを入力します。

   注意
   パートナーテナントを作成する場合、クォータはソフトクォータであり、平均を設定することはできず、サービスの使用を制限することもできません。クォータを超過した場合、テナントの管理者と親テナントの管理者にEメール通知が送信されます。

5. [カスタマーテナントを作成している場合] クォータの超過分を指定します。
   追加容量により、顧客テナントは指定された値の分だけ容量を超過できます。追加容量を超過すると、対応するサービスの使用に関する制限が適用されます。
6. テナントが使用できるストレージリソースを選択します。
   ストレージリソースはロケーション別にグループ化されています。このリストには、テナントで使用可能なストレージロケーションとリソースが含まれています。
   - パートナー/フォルダテナントを作成する際には、各サービスに対して複数のロケーションとストレージインスタンスを選択できます。
   - カスタマーテナントを作成するときは、1つのロケーションを選択し、このロケーション内でサービスごとに1つのストレージを選択する必要があります。カスタマーに割り当てられたストレージリソースは後から変更できますが、それは使用量が0 GBのときに限られます。つまり、カスタマーがストレージを使い始める前か、ストレージからすべてのバックアップを削除した後ということです。

     注意
     ストレージスペースの使用状況に関する情報はリアルタイムでアップデートされません。情報がアップデートされるまで最大24時間かかる場合があります。「ロケーションとストレージの管理」を参照してください。

7. **次のサービス**をクリックして、File Sync & Share、Cyber Infrastructure、物理データ配送など、すべての利用可能なサービスと提供項目を構成します。
8. 変更を保存します
   - 新しいテナントを作成する場合は、**[作成]**をクリックします。
   - テナントを編集している場合は、**[保存]**をクリックします。

管理コンソールの **[クライアント]** タブに、新しく作成されたテナントが表示されます。

テナント設定を編集したり、管理者を変更したりする場合は、**[クライアント]** タブでテナントを選択して、変更したいセクションで**[編集]**をクリックします。

既存のテナントのサービスを変更するには

"提供アイテムの有効化/無効化"（15ページ）を参照してください。

コンプライアンスモード

コンプライアンスモードは、より高いセキュリティが要求されるクライアント向けに設計されています。このモードでは、すべてのバックアップに暗号化を必須とし、ローカルで設定された暗号化パスワードのみを許可します。

コンプライアンスモードでは、顧客テナントとそのユニットで作成されたすべてのバックアップは、AESアルゴリズムと256ビットのキーで自動的に暗号化されます。ユーザーが暗号化パスワードを設定できるのは、保護対象デバイスのみであり、保護計画には設定できません。

重要
パートナー管理者は、新しい顧客テナントを作成するときにのみコンプライアンスモードを有効にでき、後でこのモードを無効にできません。既存のテナントにはコンプライアンスモードを有効にできません。

制限事項

- コンプライアンスモードは、バージョンが15.0.26390以上のエージェントとのみ互換性があります。
- コンプライアンスモードは、Red Hat Enterprise Linux 4.x、5.x、およびそれらの派生OSを実行しているデバイスでは利用できません。
- クラウドサービスでは暗号化パスワードにアクセスできません。この制限のため、コンプライアンスモードのテナントでは、一部の機能を利用できません。

サポートされない機能

コンプライアンスモードのテナントでは、以下の機能を利用できません。

- Cyber Protectコンソールを介した復元
- Cyber Protectコンソールを介したバックアップのファイルレベルの参照
- Web Restoreコンソールへのアクセス
- クラウドからクラウドへのバックアップ
- Webサイトバックアップ
- アプリケーションのバックアップ
- モバイルデバイスのバックアップ
- バックアップのマルウェア対策スキャン
- 安全な復元
- 社内ホワイトリストの自動作成
- データ保護マップ
- 災害復旧
- 利用できない機能に関連するレポートとダッシュボード

カスタマーテナントのコンプライアンスモードが有効かどうかを確認するには

必要なロール: パートナー管理者

1. 管理ポータルに移動します。
2. クライアントリストで、ステータスを確認したいテナントをクリックします。
   テナントに関する情報が右側に表示されます。
3. **[一般設定]**をクリックし、**[一般情報]**の下で、**[コンプライアンスモード]**のステータスを確認します。

複数のテナントへのサービス提供を有効化する

複数のテナントに対して、サービスおよび提供項目を一括で有効化することができます（1セッションにつき最大100テナントまで）。

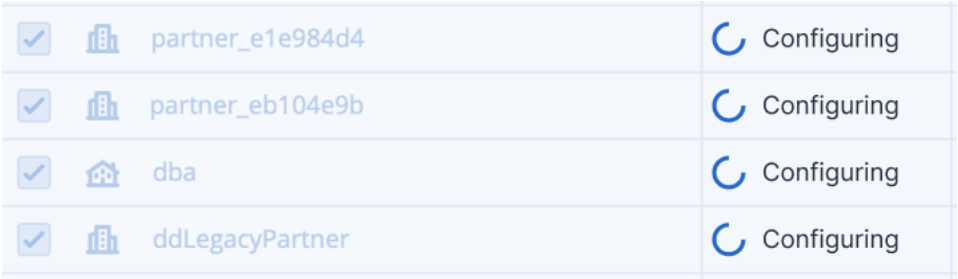
この手順は、パートナー、フォルダ、およびカスタマーテナントに適用されます。これらのタイプのテナントを同時に選択できます。

複数テナントのサービスを有効化するには

1. 管理ポータルで、**[クライアント]** に移動します。
2. 右上にある **[サービスを構成]** をクリックします。
3. 構成するテナントのチェックボックスを選択し、**[次へ]**をクリックします。
4. **[サービスを選択]** セクションで、選択したすべてのテナントに適用するサービスを選択し、**[次へ]** をクリックします。

   注意
   この画面では、以前に有効化したサービスを無効化することはできません。この手順を開始する前に選択されていたすべてのサービスと提供項目は、有効な状態が維持されます。

5. **[サービスを設定]** セクションで、選択したテナントに対して有効にしたいサービス機能および提供項目を選択し、**[次へ]** をクリックします。
6. **[サマリー]** セクションで、選択したテナントに適用される変更を確認します。
   [すべて展開] をクリックすると、すべてのテナントに適用するよう選択したサービスや提供項目が表示されます。
   また、各テナントを展開すると、そのテナントに固有のサービスや提供項目を表示できます。
7. **[変更を適用]** をクリックします。各テナントに対してサービスを構成している間、テナントは無効となり、**[テナントステータス]** 列には現在構成中のサービスおよび提供項目が表示されます（下図参照）。



選択したテナントに対してサービスや提供項目の設定が正常に適用されると、確認メッセージが表示されます。

何らかの理由でサービスや提供項目がテナントに適用されなかった場合、**[テナントステータス]** 列には「**未適用**」と表示されます。**[再試行]** をクリックすると、選択したテナントの設定を確認できます。

メンテナンスに関する通知を有効にする

パートナー管理者は、子テナント（パートナーおよびカスタマー）が、Cyber Protectデータセンターから直接メンテナンス通知のEメールを受信するように設定できます。また、製品メンテナンスの通知については管理ポータルサイトで受信するようにできます。これにより、メンテナンス関連のサポートコールを削減できます。

注意

- メンテナンス通知のEメールでは、データセンターのブランドが使用されます。これらの通知では、カスタマイズされたブランディングはサポートされていません。
- メンテナンス通知は、VMware Cloud Director ユーザーではサポートされていません。

子パートナー/カスタマーへのメンテナンス通知を有効にするには

1. パートナーユーザーとして管理ポータルにログインし、**[クライアント]** をクリックします。それから、メンテナンス通知を有効にするパートナーまたはカスタマーテナントの名前をクリックします。
2. **[設定]** をクリックします。
3. **[全般設定]** タブの **[メンテナンス通知]** オプションを有効にします。
   [メンテナンス通知] のオプションが表示されない場合は、サービスプロバイダーにお問い合わせください。

注意

メンテナンス通知の設定は有効化されますが、選択したテナントの側でユーザー通知が有効にされるか、このオプションが子パートナーまたはカスタマーに伝播してユーザーへの通知が有効になるまで、通知が送信されることはありません。

ユーザーへのメンテナンス通知を有効にするには

1. パートナーユーザーまたは企業管理者として、管理ポータルにログインします。
   パートナーは、管理しているすべてのテナントのユーザーにアクセスできます。
2. **[My Company（自分の会社）]** > **[ユーザー]** を選択し、メンテナンス通知を有効にするユーザーの名前をクリックします。
3. **[サービス]** タブの **[設定]** セクションで、鉛筆アイコンをクリックしてオプションを編集します。
4. **[メンテナンス通知]** チェックボックスを選択して、**[完了]** をクリックします。

選択されたユーザーに、データセンターの今後のメンテナンスアクティビティを通知するEメールが送信されるようになります。

検出されたデバイスに関する通知の有効化

新たに検出されたデバイスに関する通知を、次のロールのいずれかが割り当てられた、パートナーおよびカスタマーのユーザーアカウントで有効にできます。

- 管理ポータルの管理者。
- 保護コンソールの管理者またはサイバー管理者。

この場合、月曜日と木曜日に、次の情報が含まれたEメール通知が送信されます。

- 顧客の管理者の場合: 前回のチェック後に新しく検出されたデバイスの数（デバイスの種類別）。
- パートナー管理者の場合: 新しく検出されたデバイスのカスタマーごとの数。

検出されたデバイスの通知を有効にするには

1. パートナーユーザーまたは社内管理者として、管理ポータルにログインします。
2. **[企業管理]** > **[ユーザー]** を選択し、通知を有効にするユーザーの名前をクリックします。
3. **[サービス]** タブの **[設定]** セクションで、鉛筆アイコンをクリックします。
4. **[新たに検出されたデバイスに関する通知]** を選択して、**[完了]**をクリックします。

選択されたユーザーは、その企業ネットワークで新たに検出されたデバイスに関するEメール通知を受信します。

カスタマープロファイルの自己管理を構成する

パートナーが管理するテナントについて、自己管理型のカスタマープロファイルを設定できます。このオプションにより、テナントのプロファイルや連絡先情報をカスタマーごとに可視化できます。

カスタマープロファイルの自己管理を構成するには

1. 管理ポータルで **[クライアント]** へ進みます。
2. 自己管理型のカスタマープロファイルを構成したいクライアントを選択します。
3. **[設定]** タブを選択し、**[全般設定]** タブを選択します。
4. **[カスタマープロファイルの自己管理を有効化]** スイッチを有効または無効にします。

自己管理型のカスタマープロファイルを有効にすると、該当するクライアントのナビゲーションメニューには、**[企業プロファイル]** セクションと、ユーザー作成ウィザードの連絡先関連フィールド（**業務用電話番号**、**会社の連絡先**、**役職**）が表示されるようになります。

自己管理型のカスタマープロファイルを無効にすると、ナビゲーションメニューの **[企業プロファイル]** セクションと、ユーザー作成ウィザードの連絡先関連フィールドが非表示になります。

テナントの使用状況データをリフレッシュ

デフォルトでは、使用状況データは一定の間隔でリフレッシュされます。テナントの使用状況データは、手動でリフレッシュできます。

1. 管理コンソールで **[クライアント]** へ進みます。
2. テナントをクリックし、テナント行の省略記号をクリックします。
3. **[使用状況をリフレッシュ]** を選択します。

> **注意**
> データの取得には最大で10分かかります。

4. ページをリロードして、アップデートされたデータを表示します。

テナントを無効化または有効化

テナントを一時的に無効にする必要があるかもしれません。たとえば、テナントにサービスを利用するための負債がある場合です。

テナントを無効にするには

1. 管理ポータルで **[クライアント]** へ進みます。
2. 無効にするテナントを選択し、省略記号アイコン > **[無効化]** の順にクリックします。
3. **[無効化]** をクリックして操作を確認します。

以下のような結果になります。

- テナントとそのすべてのサブテナントが無効になり、サービスが停止します。
- テナントとそのサブテナントのデータは保持され、 Cyber Protect Cloudに保存されるので、課金は継続されます。
- テナントとそのサブテナントのすべてのAPIクライアントが無効になり、そのクライアントを使用したすべての統合が機能しなくなります。

テナントを有効化するには、クライアント一覧で選択してから、省略記号アイコン > **[有効化]** の順にクリックします。

テナントを別のテナントに移動

管理ポータルでは、テナントをある親テナントから別の親テナントに移動することができます。これは、あるパートナーから別のパートナーに顧客を転送する場合や、クライアントを編成するためのフォルダテナントを作成し、その一部を新しく作成したフォルダテナントに移動する場合に役立ちます。

移動可能なテナントの種類

テナントの種類	移動可能	ターゲットテナント
パートナー	はい	パートナーまたはフォルダ
フォルダ	はい	パートナーまたはフォルダ
顧客	はい	パートナーまたはフォルダ
ユニット	いいえ	なし

要件と制限事項

- テナントは、ターゲットの親テナントに元の親テナントと同じかより大きなサービスセットが存在し、元のテナントと同じ提供項目がある場合にのみ移動できます。
- 顧客テナントを移動する場合、元の親テナント内の顧客テナントに割り当てられたすべてのストレージが、ターゲットの親テナントに存在していなければなりません。これは、顧客サービス関連のデータを元のストレージから別のストレージに移動できないため必要となります。
- サービスプロバイダーが管理するカスタマーテナントでは、サービスプロバイダーレベルからカスタマーのワークロードに適用される計画（例えば、スクリプト計画）が使用される場合があります。このようなカスタマーのテナントを移動する場合、サービスプロバイダーの計画はカスタマーのワークロードから取り消され、これらの計画に関連するすべてのサービスは、このカスタマーに対して機能しなくなります。
- パートナーアカウントの階層内でテナントを移動できます。また、一部のカスタマーテナントをパートナーアカウント階層外のターゲットテナントに移動させることも可能です。この処理が可能かどうかについては、アカウントマネージャーにお問い合わせください。
- 管理者（管理ポータルの管理者または会社の管理者など）のみが、テナントを別の親テナントに移動させることができます。

テナントを移動する方法

1. 管理ポータルにログインします。
2. テナントを移動するターゲットパートナーまたはフォルダテナントの**内部ID**を検索してコピーします。以下の手順を実行します。
   a. **[クライアント]** タブで、移動先のテナントを選択します。
   b. テナントのプロパティパネルで三本線アイコンをクリックし、**[ID を表示]** をクリックします。
   c. **[内部ID]** フィールドに表示されているテキスト文字列をコピーし、**[キャンセル]** をクリックします。
3. 移動したいテナントを選択し、ターゲットのパートナー/フォルダに移動します。以下の手順を実行します。
   a. **[クライアント]** タブで、移動するテナントを選択します。
   b. テナントのプロパティパネルで三本線アイコンをクリックし、**[移動]** をクリックします。
   c. 移動先のテナントの内部IDを貼り付けて、**[移動]** をクリックします。

この処理はすぐに開始され、最大で10分間かかる場合があります。

移動先のテナントに子テナントがある場合（例えば、パートナーまたはフォルダテナントの中にカスタマーテナントがある場合）、テナントのサブツリー全体がターゲットテナントに移動されます。

パートナーテナントをフォルダテナントに変換（逆も同様）

管理ポータルを使用すると、パートナーテナントをフォルダテナントに変換できます。

これは、グループ化目的でパートナーテナントを使用し、テナントインフラストラクチャを適切に整理したい場合に役立ちます。これは、[オプションダッシュボード] にテナントに関する集約情報を含める場合にも便利です。

また、フォルダテナントをパートナーテナントに変換することもできます。

注意
変換は安全な操作であり、テナント内のユーザーおよびサービス関連のデータには影響しません。

テナントを変換します

1. 管理ポータルにログインします。
2. **[クライアント]** タブで、変換するテナントを選択します。
3. 次のいずれかを実行します。
   - テナント名の横にある省略記号アイコンをクリックします。
   - テナントを選択し、テナントのプロパティパネルの省略記号アイコンをクリックします。
4. **[フォルダへの変換]** または **[パートナーへの変換]** をクリックします。
5. 操作を確定します。

テナントへのアクセス制限

カスタマーレベル以上の管理者は、上位層の管理者に対して、自分のテナントへのアクセスを制限できます。

テナントへのアクセスが制限されていない場合、親テナントの管理者はテナントに制限なくアクセスできます。次の処理を実行できます。

- テナントのプロパティを変更する。
- テナント、ユーザー、およびテナントのサービスを管理する。
- テナント内のバックアップやその他のリソースにアクセスする。
- テナント、子テナント、すべてのカスタマーの使用状況レポートを取得する。

テナントへのアクセスが制限されている場合、親テナントの管理者は次の処理を実行できます。

- テナントのプロパティを変更する
- テナント、子テナント、およびすべてのカスタマーの使用状況レポートを取得します。

テナントに対する、上位レベルの管理者のアクセスを制限するには

1. 管理ポータルにログインします。
2. **[設定]** > **[セキュリティ]** へ進みます。
3. **[サポートアクセス]** スイッチを無効にします。

テナントの削除

リソースを解放するためのテナントを削除する必要が生じる場合もあります。使用状況の統計は、削除後1日以内に更新されます。大きなテナントの場合は、もっと長くかかることもあります。

テナントを削除するには、まず無効化することが必要です。無効化の詳しい方法については、テナントの無効化と有効化を参照してください。

注意
Cyber Protectはテナントをリカバリする機会を提供しますが、File Sync & Shareサービスの復元はサポートされていないことに注意してください。

テナントを削除するには

1. 管理ポータルで **[クライアント]** へ進みます。
2. 削除する無効テナントを選択し、省略記号アイコン > **[削除]** をクリックします。
3. この操作を確認するには、ログイン情報を入力し **[削除]** をクリックします。

作成が完了すると以下のようになります。

- テナントとサブテナントが削除されます。
- テナントとサブテナントで有効になっていたすべてのサービスが停止します。
- テナントとサブテナントのすべてのユーザーが削除されます。
- テナントとサブテナントのすべてのマシンの登録が解除されます。
- テナントとサブテナントのすべてのサービス関連データ（バックアップや同期ファイルなど）が削除されます。
- テナントとそのサブテナントのすべてのAPIクライアントが削除され、そのクライアントを使用したすべての統合が機能しなくなります。
- **テナントステータス**に **[削除済み]** と表示されます。**[削除済み]** のステータスにカーソルをホバーすると、テナントが削除された日付が表示されます。

注意
この削除日から30日以内であれば、関連するすべてのデータおよび設定を復元できます。

テナントをリカバリする

テナントが誤って削除された場合、Cyber Protectでは、30日間の間テナントをリカバリできます。

例えば、以下のような場合にテナントをリカバリする必要があるかもしれません:

- パートナーが意図せずにテナントを削除してしまった。
- パートナー開発チームが、統合のテスト中にテナント階層の一部、あるいは全体を誤って削除してしまった。
- パートナー統合で、新しいエディションに切り替える代わりに誤ってアプリケーションのプロビジョニングを解除してしまったため、データを復元する必要がある。
- パートナーが新しいライセンスに切り替える際にアプリケーションを誤って無効にしてしまったため、無効になったアプリケーションのデータを復元する必要がある。

テナントをリカバリするには

1. 管理ポータルで **[クライアント]** へ進みます。
2. **[Cyber Protect]** タブで、リカバリするテナントを見つけます。ステータスは**削除**と表示されます。
3. テナントをホバーし、省略記号アイコンをクリックします。
4. **[復元]** をクリックします。
   削除される前と同じステータスでテナントがリカバリされ、デフォルトで無効になることを確認するウィンドウが表示されます。
5. （オプション）テナントを有効にする必要がある場合は、**[テナントを有効にする]** チェックボックスを選択します。テナントは、後からいつでも有効化できます。
6. **[復元]** をクリックします。

作成が完了すると以下のようになります。

- テナントとサブテナントがリカバリされます。
- テナントとサブテナントで有効になっていたすべてのサービスが再起動します。

注意
File Sync & Shareサービスの復元はサポートされていません。

- テナントとサブテナントのすべてのユーザーがリカバリされます。
- テナントとサブテナントのすべてのマシンが再登録されます。
- テナントとサブテナントのすべてのサービス関連データ（バックアップなど）がリカバリされます。
- テナントとそのサブテナントのすべてのAPIクライアントがリカバリされ、そのクライアントを使用したすべての統合が再度開始されます。
- テナントが有効になっている場合、**テナントステータス**が**アクティブ**として表示されます。テナントがまだ有効になっていない場合は、**無効**として表示されます。

ユーザーの管理

パートナー管理者、カスタマー管理者、ユニット管理者は、自分がアクセスできるテナントのユーザーアカウントを設定および管理できます。

ユーザーアカウントの作成

次の場合、追加のアカウントを作成することができます:

- パートナー/フォルダ管理者アカウント - サービス管理業務を他の人と共有する場合
- カスタマー/見込み客 - 対応するカスタマー/見込み客へのアクセス許可が厳密に制限される他のユーザーに、サービス管理を委任する場合
- 顧客内のユーザーアカウントまたは部署テナント - ユーザーがサービスのサブセットのみにアクセスできるようにする場合

既存のアカウントをテナント間で移動することはできません。まず、テナントを作成して、そこにアカウントを作成する必要があります。

ユーザーアカウントを作成するには

1. 管理ポータルにログインします。
2. ユーザーアカウントを作成するテナントを指定します。["管理ポータルのナビゲーション"（103ページ）]をご覧ください。
3. 右上にある **[新規]** > **[ユーザー]** をクリックします。
   または、**[My Company（自分の会社）]** > **[ユーザー]** で、**[+新規]** をクリックします。
4. アカウントの次の連絡先情報を指定します:
   - **Email** - このEメールアドレスがログイン情報としても使用されます。 Eメールアドレスとは異なるログイン情報を使用したい場合は、**[Eメールとは異なるログイン情報を使用する]** チェックボックスを選択し、**ログイン情報**と**Eメールアドレス**を入力します。

     重要
     各アカウントで、一意のログインIDが必要になります。

   - **名**— このフィールドは、ユーザーアカウントの作成およびフォルダ内のユーザーの作成に必要です。
   - **姓**— このフィールドは、ユーザーアカウントの作成およびフォルダ内のユーザーの作成に必要です。
   - （オプション） **業務用電話**

     注意
     親パートナーがカスタマーテナントの **[カスタマープロファイルの自己管理を有効化]** オプションを有効にした場合のみ、ユーザー作成ウィザードに **[業務用電話]**、**[役職]**、**[会社の連絡先]** などのフィールドが表示されます。そうでない場合、これらのフィールドは表示されません。

   - （オプション）**役職**
   - **[言語]** フィールドで、このアカウントで使用される通知、レポート、およびソフトウェアのデフォルト言語を変更します。
5. （オプション）会社の連絡先を選択します。
   - **課金** - プラットフォームの使用状況レポートで、重要な変更に関するアップデートをお伝えするための連絡先です。
   - **技術** - プラットフォームにおける技術関連の重要な変更について、アップデートをお伝えするための連絡先です。
   - **業務** - プラットフォームにおける業務関連の重要な変更について、アップデートをお伝えするための連絡先です。

     注意
     単一のユーザーに1件または複数の会社の連絡先を割り当てることができます。

[ユーザー]リストの **[会社の連絡先]** 列で、ユーザーに割り当てられた会社の連絡先を表示し、必要に応じてユーザーアカウントを編集して会社の連絡先を変更できます。

6. [パートナー/フォルダテナントでアカウントを作成する場合は使用できません] ユーザーがアクセスするサービスと各サービスのロールを選択します。

   使用可能なサービスは、ユーザーアカウントが作成されたテナントで有効になっているサービスによって異なります。

   - **[企業管理者]** チェックボックスをオンにすると、ユーザーは現在テナントに対して有効になっているすべてのサービスの管理ポータルと管理者権限にアクセスできます。ユーザーは将来、テナントに対して有効になるすべてのサービスの管理者権限を持つことになります。
   - **[部署管理者]** チェックボックスをオンにすると、ユーザーは管理ポータルにアクセスできますが、サービスに応じてサービス管理者ロールを持つ場合と持たない場合があります。
   - チェックボックスをオンにしない場合、ユーザーはそのユーザーに対して有効にするサービスで割り当てるロールを持ちます。
7. **[作成]** をクリックします。

新しく作成されたユーザーアカウントが、**[My Company（自分の会社）]** 以下の **[ユーザー]** タブに表示されます。

ユーザー設定を編集する、またはユーザーの通知設定とバックアップ容量（パートナー/フォルダ管理者には使用できません）を指定する場合は、**[ユーザー]** タブでユーザーを選択して、編集するセクションの鉛筆アイコンをクリックします。

ユーザーのパスワードをリセットするには

1. 管理ポータルで **[My Company（自分の会社）]** > **[ユーザー]** へ進みます。
2. パスワードを無効にするユーザーを選択し、省略記号アイコン > **[パスワードをリセット]** を選択します。
3. **[リセット]** をクリックして操作を確認します。

これで、ユーザーはEメールで受信した手順に従い、リセット処理を完了させることができます。

二要素認証をサポートしていないサービス（ Cyber Infrastructureでの登録など）では、場合によってはユーザーアカウントをサービスアカウント（二要素認証を必要としないアカウント）に変換する必要があります。

ユーザーアカウントをサービスアカウントに変換するには

1. 管理ポータルで **[My Company（自分の会社）]** > **[ユーザー]** へ進みます。
2. サービスアカウントタイプに変換するアカウントのユーザーを選択し、省略記号アイコン > **[サービスアカウントとしてマーク]** をクリックします。
3. 確認画面で二要素認証のコードを入力し、操作を確定します。

二要素認証がサポートされていないサービスでも、このアカウントを利用できるようになりました。

各サービスで利用可能なユーザーのロール

1 人のユーザーには複数のロールを割り当てることができますが、サービスごとに 1 つのロールのみを割り当てることができます。サービスごとに、ユーザーにどのロールを割り当てるかを定義できます。

注意
利用可能なサービスは、サービスプロバイダーによって設定されます。

サービス	ロール	説明
使用不可	企業管理者	このロールにより、管理者にすべてのサービスに対する完全な権限が付与されます。 このロールでは、企業の許可リストへのアクセスが許可されます。社内保護サービスで Disaster Recovery アドオンが有効になっている場合、このロールでは、ディザスタリカバリ機能へのアクセスも許可されます。
	部署管理者 ユニットレベル	このロールは、ユニット内のすべての適用可能なサービスに対して、可能な限り高い許可を付与します。このロールは、ディザスタリカバリ機能へのアクセスを提供しません。
管理ポータル	管理者	このロールは 管理ポータル へのアクセスを許可します。管理者は、管理ポータルで組織全体のユーザーを管理できます。 関連項目: "Disaster Recoveryロール"（137ページ）。
	読み取り専用管理者 パートナーレベル	このロールは、パートナーの 管理ポータル と、このパートナーの全カスタマーの 管理ポータル 内のすべてのオブジェクトへの読み取り専用アクセスを提供します。"読み取り専用管理者ロール"（136ページ） を参照してください。
	読み取り専用管理者 カスタマーレベル	このロールでは、会社全体の 管理ポータル に存在するすべてのオブジェクトに対する読み取り専用アクセスが提供されます。"読み取り専用管理者ロール"（136ページ）を参照してください。
	読み取り専用管理者 ユニットレベル	このロールでは、企業ユニットおよびサブユニットの管理ポータルに存在するすべてのオブジェクトに対する読み取り専用アクセスが提供されます。"読み取り専用管理者ロール"（136ページ）を参照してください。
ベンダーポータル	開発者	このロールには、ベンダーポータルへの完全なアクセス権が付与されます。開発者は、CyberApps、CyberApp Descriptions、CyberApp Versionsを作成および管理できます。また、配置リクエストを提出したり、CyberAppの

		メトリクスを監視したりすることもできます。
	ユーザー	このロールでユーザーは、CyberApp Descriptionsの作成、管理、および承認のリクエストを行うことができます。
	読み取り専用ユーザー	このロールには、ベンダーポータルに対する読み取り専用のアクセス権が付与されます。

保護	

	管理者	このロールにより、カスタマーのプロテクションサービスの設定と管理が可能になります。 このロールは、以下の目的で必要です。 • Disaster Recovery機能の設定と管理。 • 企業全体の許可リストの設定と管理。 • デバイスの自動検出の実行。 • DeployPilotを使用してソフトウェアの配置に関連するすべてのアクションを実行する（ソフトウェア配置計画、ソフトウェアリポジトリ、ソフトウェアのパッケージ、クイック配置アクションの実行と連携）。
	サイバー管理者	このロールでは、管理者ロールの権限に加えて、プロテクションサービスの構成と管理、およびサイバースクリプト処理におけるアクションの承認が可能になります。 サイバー管理者ロールは、RMMパックを有効にしたテナントでのみ利用可能です。
	読み取り専用管理者	このロールでは、プロテクションサービスにおけるすべてのオブジェクトへの読み取り専用アクセスが提供されます。"読み取り専用管理者ロール"（136ページ）を参照してください。
	ユーザー	このロールにより、管理者特権なしでプロテクションサービスを使用することが可能になります。このロールが割り当てられたユーザーは、Endpoint Detection and Response などの機能が利用できるようになりますが、組織内の他のユーザーのデータにアクセスすることはできません。
	演算子を復元	Microsoft 365およびGoogle Workspaceの組織に適用されるこのロールは、バックアップへのアクセスを提供し、バックアップ内の機密コンテンツへのアクセスを制限しながら、バックアップの復元を許可します。詳細については、"復元オペレータロール"（137ページ）を参照してください。
	セキュリティ分析	このロールは、Detection and Responseが有効になっているカスタマーテナントでのみ割り当てることができます。このロールにより、サイバープロテクションコンソールにアクセスできるようになり、ユーザーはEDRインシデントの管理と対応アクションの実行が可能になります。
	DRサポートの演算子	このロールでは、組織内における保護サービスのすべてのオブジェクトに対する読み取り専用アクセスと、Disaster Recovery環境へのアクセスが提供され、高度なトラブルシューティングを実行できます。 関連項目:

		"Disaster Recoveryロール"（137ページ）。
	RMMオペレーター	このロールは、 サービスのリモート管理と監視機能へのアクセスのみを提供します。このロールを使用すると、以下を実行できます： • ワークロード資格情報管理にアクセスせずに、リモートデスクトップ接続（NEAR、RDP、Apple Screen Sharing、またはWebクライアント経由）を開始する。 • ワークロードを管理する（再起動、シャットダウン、スリープ状態にする、ごみ箱を空にする、またはリモートユーザーをログアウトする）。 • デバイスの詳細、ソフトウェアおよびハードウェアのインベントリ、監視データを閲覧する。 • 承認された組み込みスクリプトをオンデマンドで実行する。 • **マイパッケージ** リポジトリからオンデマンドでソフトウェアパッケージをインストールする。 • 承認されたパッチを受け入れられたEULAでオンデマンドでインストールする。 • アラートおよびアクティビティを参照する。 このロールは、読み取り専用管理者ロールとして、保護サービスの他のオブジェクトへの読み取り専用アクセスを持っています。
File Sync & Share	管理者	このロールにより、ユーザーのFile Sync & Shareの設定と管理が可能になります。
Cyber Infrastructure	管理者	このロールにより、ユーザーのCyber Infrastructureの設定と管理が可能になります。
パートナーポータル	パートナーポータルのユーザーに割り当てることができる複数のロールがあります。詳細については、"パートナーポータルのロール"（241ページ）を参照してください。	
Notary	管理者	このロールにより、ユーザーのNotaryの設定と管理が可能になります。
	ユーザー	このロールにより、管理者権限がなくともNotaryサービスが使用できるようになります。このロールを割り当てられたユーザーは、組織の他のユーザーのデータにはアクセスできません。

注意

ベンダーポータルは、2023年10月4日以降にアクロニステクノロジーエコシステムWeb サイトに登録したテクノロジーパートナーが利用できます。

統合の構築を検討し、ベンダーポータルと専用のサンドボックスへのアクセスを必要としている場合は、統合の章を参照してください。

アカウントとロールに関連する変更は、次の詳細とともに [**アクティビティ**]タブに表示されます。

- 変更点
- 変更者
- 変更日時

ユーザーロールとサイバースクリプトの権限

スクリプトとスクリプト計画で実行できる操作は、スクリプトのステータスとユーザーのロールによって異なります。

管理者は、次の制限のもとで、自分のテナントおよびその子テナント内の計画やワークロードなどのオブジェクトを管理できます。

- カスタマーのテナントは、パートナーの管理者のアクセスを制限できます。
- 親テナントのカスタマー管理者とパートナー管理者は、常にユニットにアクセスできます。

管理者は、自分のテナントおよび子テナント内の計画やワークロードなどのオブジェクトを管理できます。部署は常に顧客の管理者によってアクセス可能です。

管理者は、自分のテナントより上のレベルのオブジェクトを表示したりアクセスしたりすることはできません。

高レベルの管理者が自分のワークロードに適用したスクリプト計画の場合、低レベルの管理者に付与されるのは読み取り専用のアクセス権のみです。

以下のロールには、サイバースクリプトに関する権限が付与されます。

- **社内管理者**
  このロールにより、管理者に対しすべてのサービスに対する完全な権限が付与されます。サイバースクリプトに関しては、サイバー管理者ロールと同じ権限が付与されます。
- **サイバー管理者**
  このロールには、テナントで使用できるスクリプトの承認や、**テスト**ステータスでスクリプトを実行する機能など、完全な許可が付与されます。
- **管理者**
  このロールには、承認されたスクリプトを実行したり、そのスクリプトを使用するスクリプト計画を作成/実行したりするための、限定的な許可が付与されます。
- **読み取り専用管理者**
  このロールには、テナントで使用されるスクリプトと保護計画を表示することができる、限定的な許可が付与されます。
- **ユーザー**
  このロールには、承認されたスクリプトを実行したり、そのスクリプトを使用するスクリプト計画を作成/実行したりするための、限定的な許可が付与されます。この操作は、ユーザーのマシン上でのみ実行できます。

スクリプトのステータスとユーザーロールに応じて実行できるすべての操作を次の表にまとめました。

ロール	目的	スクリプトのステータス		
		下書き	テスト中	承認済み
サイバー管理者 **社内管理者**	スクリプト計画	編集（計画からドラフトのスクリプトを削除） 削除 取り消し 無効にする 停止	作成 編集 適用 有効にする 実行 削除 取り消し 無効にする 停止	作成 編集 適用 有効にする 実行 削除 取り消し 無効にする 停止
	スクリプト	作成 編集 ステータスを変更 クローンを作成 削除 実行をキャンセル	作成 編集 ステータスを変更 実行 クローンを作成 削除 実行をキャンセル	作成 編集 ステータスを変更 実行 クローンを作成 削除 実行をキャンセル
管理者 **ユーザー**（それぞれが所有するワークロード）	スクリプト計画	表示 編集 取り消し 無効にする 停止	表示 実行をキャンセル	作成 編集 適用 有効にする 実行 削除 取り消し 無効にする 停止
	スクリプト	作成 編集 クローンを作成 削除	表示 クローンを作成 実行をキャンセル	実行 クローンを作成 実行をキャンセル

		実行をキャンセル		
読み取り専用管理者	スクリプト計画	表示	表示	表示
	スクリプト	表示	表示	表示

読み取り専用管理者ロール

このロールを割り当てられたアカウントは、Cyber Protectコンソールへの読み取り専用アクセス権を付与されていて、次の操作を実行できます。

- システムレポートなどの診断用データの収集。
- バックアップの復元ポイントを確認できますが、バックアップコンテンツにドリルダウンしたり、ファイル、フォルダ、またはEメールを表示したりすることはできません。
- Advanced Security + XDRが有効になっている場合、読み取り専用の管理者はEDRインシデント画面の [対応アクション] タブにアクセスできますが、アクションを実行することはできません。
- 読み取り専用モードで、組織に属する他のユーザーのデータにアクセスします。

読み取り専用の管理者は、次の操作を実行できません。

- 任意のタスクを開始または停止する。
  たとえば読み取り専用の管理者は、復元を開始したり、実行中のバックアップを停止したりすることはできません。
- Disaster Recovery機能や企業全体の許可リストの構成と管理を実行します。また、ソフトウェア配置計画、ソフトウェアリポジトリ、およびソフトウェアパッケージに対して読み取り専用アクセス権を有します。
- ソースマシンまたはターゲットマシンのファイルシステムにアクセスする。
  たとえば、読み取り専用の管理者は、バックアップされたマシン上のファイル、フォルダ、またはEメールを表示できません。
- 任意の設定を変更する。
  たとえば、読み取り専用の管理者は、保護計画を作成したり、その設定を任意に変更したりすることはできません。
- データを作成、アップデート、または削除する。
  たとえば、読み取り専用の管理者は、バックアップを削除したり、クラウドツークラウドバックアップの検索インデックスを削除、アップデート、再構築したりすることはできません。

注意
管理ポータルでは、読み取り専用管理者はデモンストレーション目的で新しい子テナントの作成を開始し、そのすべてのプロパティを構成できますが、それらを保存することはできません。自分のテナントやユーザーのクォータを変更することはできません。

- スクリプト計画、監視計画、またはエージェント計画の変更を保存します。

保護計画のデフォルト設定を除いて、読み取り専用の管理者がアクセスできないすべてのUIオブジェクトは非表示になります。これらの設定は表示されますが、**[保存]** ボタンはアクティブではありません。

関連項目: "Disaster Recoveryロール"（137ページ）。

復元オペレータロール

注意
このロールは、プロテクションサービスにおいて、Microsoft 365とGoogle Workspaceのバックアップを行う場合に限り利用可能です。

復元オペレータは次の操作を行えます。

- アラートおよびアクティビティを表示する。
- バックアップのリストを表示および更新する。
- 復元ポイントのリストを表示する。
- バックアップの内容にアクセスせずに、バックアップを参照する。

  注意
  復元オペレータは、バックアップされたファイルの名前と、バックアップされたEメールの件名と送信者を確認できます。

- バックアップを検索する（フルテキスト検索はサポート対象外）。
- 元のMicrosoft 365組織またはGoogle Workspace組織内で、クラウドツークラウドバックアップのバックアップを元のロケーションにのみリカバリする。

復元オペレータは次の操作を行うことはできません。

- アラートを削除する。
- Microsoft 365組織またはGoogle Workspace組織を追加または削除する。
- バックアップロケーションの追加、削除、名前の変更を行う。
- バックアップの削除や名前の変更を行う。
- バックアップをリカバリするときに、フォルダを作成、削除、または名前を変更する。
- バックアップ計画の適用やバックアップの実行。
- バックアップ済みのファイルやEメールコンテンツにアクセスする。
- バックアップ済みのファイルやEメールの添付ファイルをダウンロードする。
- Eメールやカレンダーアイテムなど、バックアップ済みのクラウドリソースをメールで送信する。
- Microsoft 365 Teamsの会話を表示またはリカバリする。
- クラウドツークラウドバックアップを別のメールボックス、OneDrive、Google Drive、Microsoft 365 Teamなど、オリジナルでないロケーションにリカバリできます。

Disaster Recoveryロール

Disaster Recovery（DR）を有効化（する）と、管理ポータルレベルのすべての管理者と読み取り専用管理者に自動的にDisaster Recovery機能へのアクセス権が付与されます。アカウント作成プロセス中に、関連するロールを各ユーザーに割り当てることができます。

また、Disaster Recovery には、DR 特有のロールである DR サポートオペレーターも含まれています。このロールは必要に応じて保護レベルでユーザーに割り当てることができます。

注意
DRは、これらすべてのロールがユニットレベルではなく、会社レベルで利用できます。

以下の表では、利用可能な各ロールと、Disaster Recoveryで各ロールに割り当てられた権限を説明しています。

コンテキスト	機能領域	機能	管理者	読み取り専用管理者	DRサポートの演算子
サーバー	共通	すべてのアクティビティを表示	はい	はい	はい

コンテキスト	機能領域	機能	管理者	読み取り専用管理者	DRサポートの演算子
		ステータス別のアクティビティの表示: すべてのステータス / 実行中 / 成功 / 失敗	はい	はい	はい
	ディザスタリカバリロケーション （AzureへのDR に該当）	構成（保護計画から、DRセクションから）	はい	はい	はい
		サイトロケーションの選択	はい	はい	はい
		Azure サブスクリプション - 新規追加	はい	いいえ	いいえ
		Azure サブスクリプション - 既存のサブスクリプションを選択	はい	はい	はい
		Azureリージョンを選択	はい	いいえ	いいえ
		復元ネットワーク - 基本に切り替え	はい	はい	はい
		復元ネットワーク - 高度な設定に切り替え	はい	はい	はい
		復元ネットワーク - 追加	はい	いいえ	いいえ
		VNet、サブネットの一覧	はい	いいえ	いいえ
		設定	はい	いいえ	いいえ

コンテキスト	機能領域	機能	管理者	読み取り専用管理者	DRサポートの演算子
	リカバリサーバー	復元ポイントのリストを表示する	はい	はい	はい

コンテキスト	機能領域	機能	管理者	読み取り専用管理者	DRサポートの演算子
		復元サーバーの一覧を名前/ステータス/状態/RPO準拠/VM状態で並べ替え	はい	はい	はい
		復元サーバーの一覧で情報列を表示/非表示	はい	はい	はい
		復元サーバーの一覧を検索する	はい	はい	はい
		復元サーバーのリストで複数の項目を選択する	はい	はい	はい
		復元サーバーのプロパティを表示する	はい	はい	はい
		復元サーバーの計画を表示する	はい	はい	はい
		本番環境から復元サーバーへのフェールオーバーを開始/停止	はい	いいえ	いいえ
		復元サーバーへのテストフェールオーバーを開始/停止	はい	いいえ	はい
		今すぐ実行（バックアップ計画を実行）	はい	いいえ	いいえ
		復元サーバーのアクティビティを表示する	はい	はい	はい
		復元サーバーのフェールオーバーをキャンセル	はい	いいえ	いいえ
		VMへのフェールバック: データ転送の開始	はい	いいえ	いいえ
		フェールバックの切り替え	はい	いいえ	いいえ
		フェールバックを検証	はい	いいえ	いいえ
		フェールバックの表示ステータスと進行	はい	はい	はい
		フェールバックのキャンセル	はい	いいえ	いいえ
		フェールバック: 確認	はい	いいえ	いいえ
		物理マシンへのフェールバック: 開始	はい	いいえ	いいえ
		物理マシンへのフェールバック: 切り替え	はい	いいえ	いいえ
		物理マシンへのフェールバック: （マシンが復元されたことを）確認	はい	いいえ	いいえ
		復元サーバーの復元	はい	いいえ	いいえ
		復元サーバーの電源オン/オフ	はい	いいえ	はい
		コンソール	はい	いいえ	はい
		復元サーバーの設定を編集	はい	いいえ	いいえ

コンテキスト	機能領域	機能	管理者	読み取り専用管理者	DRサポートの演算子
		復元サーバーの設定を表示	はい	いいえ	はい
		復元サーバーを削除	はい	いいえ	いいえ
		復元サーバーの作成（デバイス - 一致しないデバイス - 保護）	はい	いいえ	いいえ
		接続 (Microsoft Azure ロケーション)	はい	いいえ	いいえ
		VM サイズ/ディスクの種類を一覧化	はい	はい	はい
	プライマリサーバー	プライマリサーバーのリストを表示	はい	はい	はい
		プライマリサーバーのリストを名前/ステータス/状態/RPO 準拠/VM 状態で並べ替え	はい	はい	はい
		プライマリサーバーのリストで情報列を表示/非表示	はい	はい	はい
		プライマリサーバーのリストを検索	はい	はい	はい
		プライマリサーバーのリストから複数の項目を選択	はい	はい	はい
		新しいプライマリサーバーの作成	はい	いいえ	いいえ
		プライマリサーバーのプロパティを表示	はい	はい	はい
		プライマリサーバーの計画の表示	はい	はい	はい
		プライマリサーバーの計画を編集	はい	いいえ	いいえ
		今すぐ実行	はい	いいえ	いいえ
		プライマリ サーバーのアクティビティを表示	はい	はい	はい
		プライマリ サーバーの復元	はい	いいえ	いいえ
		プライマリサーバーの電源をオン/オフ	はい	いいえ	はい
		コンソール	はい	いいえ	はい
		プライマリサーバーの設定を編集	はい	いいえ	いいえ
		プライマリサーバーの設定を表示	はい	いいえ	はい
		プライマリサーバーを削除	はい	いいえ	いいえ
接続	概要	すべての接続のステータスを表示（ローカルサイト - VPN トンネル - クラウドサイトのポイントツーサイト、サイトツーサイト、IPSec）	はい	はい	はい

コンテキスト	機能領域	機能	管理者	読み取り専用管理者	DRサポートの演算子
		VPNゲートウェイを再インストール	はい	いいえ	はい

コンテキスト	機能領域	機能	管理者	読み取り専用管理者	DRサポートの演算子
		ネットワークパケットをキャプチャ	はい	いいえ	はい

コンテキスト	機能領域	機能	管理者	読み取り専用管理者	DRサポートの演算子
		VPN アプライアンスに関する情報の表示	はい	はい	はい

コンテキスト	機能領域	機能	管理者	読み取り専用管理者	DRサポートの演算子
		VPNアプライアンスのダウンロードログ	はい	はい	はい

コンテキスト	機能領域	機能	管理者	読み取り専用管理者	DRサポートの演算子
		VPN アプライアンスの登録を解除	はい	いいえ	いいえ

コンテキスト	機能領域	機能	管理者	読み取り専用管理者	DRサポートの演算子
		VPN ゲートウェイに関する情報の表示	はい	はい	はい

コンテキスト	機能領域	機能	管理者	読み取り専用管理者	DRサポートの演算子
		VPN ゲートウェイのダウンロードログ	はい	はい	はい
		VPN ゲートウェイで tcpdump 収集をリクエスト	はい	はい	はい
		VPN アプライアンスで tcpdump 収集をリクエスト	はい	はい	はい
		ローカルサーバーのリストを表示	はい	はい	はい
		アクティブなポイントツーサイト接続の一覧を表示	はい	はい	はい
		すべてのクラウドサーバーのリストを表示して並べ替える	はい	はい	はい
		すべてのクラウドサーバーの一覧からサーバーに移動する	はい	はい	はい
		ネットワーク情報の表示	はい	はい	はい
		クラウドネットワークを追加/編集	はい	いいえ	いいえ
		サーバーを別のネットワークに大規模移動	はい	いいえ	いいえ
		IPSec 接続: ネットワークポリシーの表示	はい	はい	はい
		IPSec接続: IPSec/IKEセキュリティ設定の表示	はい	はい	はい
		IPSec接続: 事前共有鍵の変更	はい	いいえ	いいえ
		IPsec接続: 接続を無効化/有効化	はい	いいえ	はい
	プロパティ	プロパティの表示/非表示	はい	はい	はい
		サイトツーサイト接続をオン/オフ	はい	いいえ	はい
		サイトツーサイト: VPNアプライアンスのダウンロード	はい	はい	はい
		サイトツーサイト: ローカルルーティングの表示	はい	はい	はい
		サイトツーサイト: ローカルルーティングの編集	はい	いいえ	いいえ
		サイトツーサイト: IPsec 構成とログをダウンロード	はい	はい	はい
		ローカルサイトへのVPNアクセスをオン/オフ	はい	いいえ	はい
		ポイントツーサイト: 設定ファイルを再生成	はい	いいえ	はい
		ポイントツーサイト: OpenVPNの構成をダウンロード	はい	いいえ	はい
		ポイントツーサイト: 接続方法に関する情報の表示	はい	はい	はい
		サーバーのIPを再割り当て	はい	いいえ	いいえ
		DHCP:MACアドレスの一覧をダウンロード	はい	いいえ	はい

コンテキスト	機能領域	機能	管理者	読み取り専用管理者	DRサポートの演算子
ランブック		ランブックを作成	はい	いいえ	いいえ
		本番環境のフェールオーバーでのランブックの開始/停止	はい	いいえ	いいえ
		テストフェールオーバーでのランブックの開始/停止	はい	いいえ	はい
		ランブックを編集	はい	いいえ	いいえ
		実行履歴の表示	はい	はい	はい
		ランブックの表示	はい	はい	はい
		ランブックの実行の表示	はい	はい	はい
		ランブックの手動アクティビティで「完了」を押す	はい	いいえ	いいえ

ユーザー向け通知設定の変更

ユーザーが作成されたテナントで Cyber Protection サービスが有効になっている場合、ユーザーが受信する通知をEメールで受信するかどうかを構成できます。

ユーザーへの通知を構成するには

1. **My Company（自分の会社）** > **ユーザー** に移動します。
2. 通知を構成するユーザーをクリックし、**サービス**タブの**Eメール通知**セクションで鉛筆アイコンをクリックします。
3. 有効にするEメール通知のチェックボックスを選択します。

通知	説明
メンテナンスに関する通知	パートナーユーザー、子テナント（パートナー、カスタマー）、および個人ユーザーへの、Cyber Protectデータセンターで予定されているメンテナンスアクティビティに関する通知です。この通知は、パートナーユーザーが子テナントに対して、またパートナーユーザーまたは企業管理者が組織内の個人ユーザーに対して有効にすることができます。 次のロールは、メンテナンス通知を有効化および管理できます： • 企業管理者 • 管理ポータルの管理者 • サイバープロテクション管理者 **注意** 読み取り専用管理者ロールは、メンテナンス通知設定へのアクセス権を持っていません。
クォータ	クォータの超過に関する通知です。

通知	説明
の超過に関する通知	
定期使用状況レポート	毎月の最初の日に送信される、使用状況レポートです。
URLブランディング通知	Cyber Protect CloudサービスのカスタムURLに使用されている証明書の有効期限が近づいていることを通知します。この通知は、選択したテナントの全管理者に、証明書有効期限の30日前、15日前、7日前、3日前、1日前に送信されます。
本番切り替えまでのカウントダウン通知	トライアルの有効期限が切れる10日前と3日前に送信されるカスタマーのトライアルの有効期限切れに関する通知です。
本番モードのアクティベーション通知	本番モードのアクティベーションに関する通知です。
失敗に関する通知	検証を含む保護計画の実行結果と、各デバイスのディザスタリカバリ操作の結果に関する通知。
警告通知	検証を含む保護計画の実行結果と、各デバイスのディザスタリカバリ操作の結果に関する通知。
成功の通知	検証を含む保護計画の実行結果と、各デバイスのディザスタリカバリ操作の結果に関する通知。
アクティブアラートの日次概要	日時概要は、概要の生成時にCyber Protectコンソールに表示されるアクティブアラートのリストに基づいて生成されます。この概要は1日1回、10:00から23:59（UTC）の間に生成され、送信されます。 レポートが生成されて送信される時刻は、データセンターのワークロードによって異なります。当該時刻の時点でアクティブアラートがない場合、概要は送信されません。概要には、有効でない過去のアラートに関する情報は含まれません。たとえば、ユーザーがバックアップの失敗に気づいてアラートを消去した場合や、バックアップを再試行して概要が生成される前に成功した場合には、アラートは表示されず概要にも含まれません。
デバイス制御通知	デバイス制御モジュールを有効にした保護計画において、制限対象の周辺デバイスやポートの使用が試行されたことに関する通知です。
新たに検出されたデバイス	新しく検出されたデバイスに関する通知です。これらの通知は毎週月曜日と木曜日に送信されます。

通知	説明
に関する通知	
復元通知	次のリソースに対する復元アクションの通知: ユーザーのEメールメッセージとメールボックス全体、パブリックフォルダ、OneDrive/GoogleDrive（OneDrive全体とファイルまたはフォルダ）、SharePointファイル、Teams（チャネル、チーム全体、Eメールメッセージ、チームサイト）。 これらの通知に関連する処理では、次のアクションが復元アクションとみなされます: Eメールとして送信、ダウンロード、または復元操作の開始。
データ漏洩防止通知	ネットワーク上のこのユーザーのアクティビティに関連するデータ漏洩防止アラートの通知です。
セキュリティインシデントの通知	アクセス時、実行時、およびオンデマンドのスキャンで検出されたマルウェアや、振る舞い検知エンジンおよびURLフィルタリングエンジンからの検出結果を通知します。 **[軽減済み]** オプションと **[軽減されていない]** オプションの2種類があります。これらのオプションは、Endpoint Detection and Response（EDR）インシデントアラート、脅威フィードからのEDRアラート、個別アラート（EDRが有効になっていないワークロードの場合）に適しています。 EDRアラートが作成されると、関連するユーザーにEメールが送信されます。インシデントの脅威ステータスが変更されると、新しいEメールが送信されます。Eメールにはアクションボタンが含まれており、ユーザーがインシデントの詳細（軽減された場合）を表示したり、インシデントを調査および修正したり（軽減されなかった場合）できるようになっています。
インフラの通知	Disaster Recoveryインフラの問題に関する通知: Disaster Recoveryインフラが利用できない場合、またはVPNトンネルが利用できない場合。

注意

VMware Cloud Director ユーザーは、クォータの超過通知、スケジュールされた使用状況レポート（そのようなレポートが組織に対して設定されている場合）、およびアクティブアラートに関する日次要約を受信できます。

通知タイプとユーザーロールごとのデフォルトの通知設定を有効化

デフォルトで有効または無効になる通知は、通知タイプとユーザーロールによって異なります。

通知タイプ¥ユーザーロール	パートナー、フォルダ管理者	カスタマー、ユニット管理者（セルフサービス）	カスタマー、ユニット管理者（サービスプロバイダーによる管理）
メンテナンスに関する通知	はい （ダイレクトパートナーのユー	いいえ	いいえ

	ザーはデフォルトで有効、ダイレクトパートナー以外は無効)		
クォータの超過に関する通知	はい	はい	いいえ
定期使用状況レポート通知	はい	はい	いいえ
URLブランディング通知	いいえ	いいえ	いいえ
失敗に関する通知	いいえ	いいえ	いいえ
警告通知	いいえ	いいえ	いいえ
成功の通知	いいえ	いいえ	いいえ
アクティブアラートの日次概要	いいえ	はい	いいえ
デバイス制御通知	いいえ	いいえ	いいえ
復元通知	いいえ	いいえ	いいえ
データ漏洩防止通知	いいえ	いいえ	いいえ
セキュリティインシデント通知: 軽減済み	いいえ	いいえ	いいえ
セキュリティインシデント通知: 軽減されていない	いいえ	いいえ	いいえ
インフラストラクチャの通知	いいえ	いいえ	いいえ

デバイスタイプとユーザーロールごとにデフォルトで有効になっている通知

デバイスの種類¥ユーザーロール	ユーザー	カスタマーおよび部署の管理者	パートナーおよびフォルダの管理者
自身のデバイスに関する通知	はい	はい	使用不可*
子テナントのすべてのデバイスに関する通知	使用不可	はい	はい
Microsoft 365、Google Workspace、およびその他のクラウドベースのバックアップに関する通知	使用不可	はい	はい

*パートナー管理者は自身のデバイスは登録できませんが、自分用のカスタマー管理者アカウントを作成し、そのアカウントを使用して自身のデバイスを登録できます。ユーザーアカウントとテナントを参照してください。

ユーザーアカウントの無効化と有効化

クラウドプラットフォームへのアクセスを一時的に制限する必要がある場合は、対象のユーザーアカウントを無効にできます。

ユーザーアカウントを無効にするには

1. 管理ポータルで **[ユーザー]** へ進みます。
2. 無効にするユーザーアカウントを選択し、省略記号アイコン > **[無効化]** をクリックします。
3. **[無効化]** をクリックして操作を確認します。

そのユーザーは、クラウドプラットフォームを使用したり、通知を受け取ったりできなくなります。

注意
無効化されたユーザーに関連付けられているすべてのデバイスは、クォータが適用されないため、保護されなくなります。これらのデバイスの保護を継続するには、アクティブなユーザーに再割り当てします。

無効にされたAPIクライアントを有効にするには

1. 管理ポータルで **[ユーザー]** へ進みます。
2. ユーザーの一覧から無効なユーザーを選択し、次に省略記号アイコン > **有効化**をクリックします。

ユーザーアカウントの削除

リソース（記憶域スペースやライセンスなど）を解放するために、ユーザーアカウントを完全に削除することが必要になる場合もあります。使用状況の統計は、削除後1日以内に更新されます。大量のデータが存在するアカウントの場合は、もっと長くかかることもあります。

注意
ユーザーを削除した後は、削除したユーザーのログインアカウントを再利用できます。

ユーザーアカウントを削除するには、まず無効化する必要があります。無効化の詳しい方法については、ユーザーアカウントの無効化と有効化を参照してください。

ユーザーアカウントを削除するには

1. 管理ポータルで **[ユーザー]** へ進みます。
2. 無効になっているユーザーアカウントを選択し、省略記号アイコン > **[削除]** をクリックします。
3. この操作を確認するには、ログイン情報を入力し **[削除]** をクリックします。

作成が完了すると以下のようになります。

- このアカウントに対して設定された通知はすべて無効になります。
- そのユーザーアカウントに属していたすべてのデータが削除されます。
- 管理者は管理ポータルにアクセスできなくなります。
- このユーザーと関連付けられたワークロードのすべてのバックアップが削除されます。
- そのユーザーアカウントに関連していたすべてのマシンの登録が解除されます。
- このユーザーと関連付けられたすべてのワークロードから保護計画が取り消されます。
- このユーザーに属するすべてのFile Sync & Shareデータ（ファイルやフォルダなど）が削除されます。
- このユーザーに属するノータリーデータ（例: 公証済みファイル、電子署名されたファイル）が削除されます。
- ユーザーの**ステータス**には、**削除**と表示されます。**削除**ステータスをホバーすると、ユーザーが削除された日付と、この削除日から30日以内であれば関連するすべてのユーザーデータと設定をリカバリできるという注意が表示されます。

ユーザーアカウントをリカバリする

ユーザーアカウントは誤って削除される可能性があるため、Cyber Protectionではユーザーアカウントをリカバリする機会が提供されています。

ユーザーアカウントをリカバリする必要がある場合の例としては、企業管理者が退社したユーザーを削除したものの、そのユーザーに登録されているリソースがまだ必要な状況などがあります。

ユーザーアカウントをリカバリするには

1. 管理ポータルで **[My Company（自分の会社）]** > **[ユーザー]** へ進みます。
2. **[ユーザー]** タブで、リカバリするユーザーアカウントを見つけます。ステータスは**削除**と表示されます。
3. ユーザーアカウントをホバーし、省略記号アイコンをクリックします。
4. **[復元]** をクリックします。
   削除される前と同じステータスでユーザーアカウントがリカバリされ、デフォルトで無効になることを確認するウィンドウが表示されます。
5. （オプション）ユーザーアカウントを有効にする必要がある場合は、**[ユーザーを有効にする]** チェックボックスを選択します。ユーザーアカウントは、後からいつでも有効化できます。
6. **[復元]** をクリックします。

作成が完了すると以下のようになります。

- このユーザーアカウントがリカバリされます。
- そのユーザーアカウントに属していたすべてのデータがリカバリされます。
- そのユーザーアカウントに関連していたすべてのマシンが再登録されます。
- ユーザーアカウントが有効になっている場合、ユーザーステータスが**アクティブ**として表示されます。ユーザーアカウントがまだ有効になっていない場合は、**無効**として表示されます。

ユーザーアカウントの所有権の移転

制限がかかっているユーザーのデータへのアクセスを維持するために、ユーザーアカウントの所有権の移転が必要になる場合もあります。

重要
削除したアカウントのコンテンツの再割り当てはできません。

ユーザーアカウントの所有権を移転するには:

1. 管理ポータルで **[ユーザー]** へ進みます。
2. 所有権を移転するユーザーアカウントを選択し、**[一般情報]** セクションで鉛筆のアイコンをクリックします。
3. 既存のEメールを新しいアカウント所有者のEメールに置き換え、**[完了]** をクリックします。
4. **[はい]** をクリックしてこの操作を確認します。
5. 新しいアカウント所有者にEメールアドレスを確認してもらいます（そのための手順は、そのアドレスに送信されます）。
6. 所有権を移転するユーザーアカウントを選択し、省略記号アイコン > **[パスワードのリセット]** をクリックします。
7. **[リセット]** をクリックして操作を確認します。
8. 新しいアカウント所有者にパスワードをリセットしてもらいます（そのための手順は、そのEメールアドレスに送信されます）。

新しい所有者がそのアカウントにアクセスできるようになります。

二要素認証の管理

二要素認証（2FA）は複数の要素による認証の一種で、2つの要素の組み合わせを利用してユーザーのIDをチェックします。

- ユーザーが知っている何か（PINコードまたはパスワード）
- ユーザーが持っている何か（トークン）
- ユーザー自身の何か（生体情報）

二要素認証はアカウントへの不正アクセスに対して追加の保護を提供します。

Cyber Protect Cloudプラットフォームは、**タイムベースのワンタイムパスワード（TOTP）**認証をサポートしています。システムでTOTP認証が有効の場合、システムにアクセスするために、ユーザーは従来のパスワードとワンタイムTOTPコードを入力する必要があります。つまり、ユーザーはパスワード（第1要素）とTOTPコード（第2要素）を提供します。TOTPコードは、現在時刻とプラットフォームによって提供されるシークレット（QRコードまたは英数字コード）に基づいて、ユーザー第2要素デバイス上の認証アプリケーション内に生成されます。

注意
本番モードのパートナーテナントの場合、デフォルトで二要素認証が有効であり、無効にはできません。

カスタマーテナントの場合、二要素認証はオプションであり、無効にできます。

統合で使用されるパートナー管理者アカウントは、サービスアカウントに変換する必要があります。変換しないと、統合がCyber Protect Cloudに対して認証できなくなります。たとえば、VMware Cloud Directorの統合で使用されるアカウントは、管理エージェントとバックアップエージェントのアカウントです。サービスアカウントの作成方法の詳細については、"ユーザーアカウントをサービスアカウントに変換するには"（128ページ）を参照してください。

仕組み

1. カスタマー管理者は、組織レベルで二要素認証を有効にします。
2. 組織の全ユーザーは各自の第2要素デバイス（携帯電話、ノートPC、デスクトップPC、またはタブレット）に認証アプリケーションをインストールする必要があります。このアプリケーションはワンタイムTOTPコードを生成するために使用します。
   推奨される認証アプリ:
   - Google Authenticator
     iOSアプリバージョン（https://apps.apple.com/app/google-authenticator/id388497605）
     Androidバージョン
     （https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2）
   - Microsoft Authenticator
     iOSアプリバージョン（https://apps.apple.com/app/microsoft-authenticator/id983156458）
     Androidバージョン
     （https://play.google.com/store/apps/details?id=com.azure.authenticator）

   重要
   ユーザーは認証アプリケーションがインストールされるデバイスの時刻が正しく設定されており、実際の現在時刻を反映していることを確認する必要があります。
3. 組織ユーザーはシステムに再ログインする必要があります。
4. ログインIDとパスワードを入力後、ユーザーは、ユーザーアカウントのための二要素認証を設定するよう促されます。
5. ユーザーは認証アプリケーションを使用してQRコードをスキャンする必要があります。QRコードをスキャンできない場合、QRコードの下に表示される32桁のコードを使用し、認証アプリケーションへ手動で追加できます。

重要
QR コードを保存することを強くお勧めします。QR コードを印刷するか、32 桁のコードを書き留めるか、または QR コードのバックアップをクラウドに保存するアプリケーションを使用してください。二要素認証の 2 番目の要素のデバイスが紛失した場合に、QR コードまたは 32 桁のコードが必要になります。

一時ワンタイムパスワード（TOTP）コードは認証アプリケーション内に生成されます。30秒間隔で自動的に再生成されます。

6. ユーザーは、パスワードの入力後に**二要素認証を設定**画面上でTOTPコードを入力する必要があります。
7. 結果として、ユーザー用の二要素認証が設定されます。

ユーザーがシステムにログインする際、ログインIDとパスワードの入力が求められ、ワンタイムTOTPコードが認証アプリケーション内に生成されます。

ユーザーは、システムログイン時にブラウザを信頼済みとしてマークでき、そうするとそのブラウザ経由の以降のログインではTOTPコードは要求されません。

新しいデバイスで二要素認証を設定するには

1. 以前設定した認証アプリにアクセスできることを確認します。
2. 新しいデバイスに認証アプリをインストールします。
3. 新しいデバイスで認証アプリを設定します。
   - デバイスで二要素認証を構成した際に保存したPDFファイルを使用します。
     このファイルには、認証アプリをアクロニス アカウントに再度リンクする際に新しいデバイスの認証アプリに入力する必要がある、32桁のコードが含まれています。

     重要
     コードが正しいにもかかわらず動作しない場合は、認証モバイルアプリの時刻を同期してください。

   - セットアップ中にPDFファイルを保存していなかった場合:
     a. **[二要素認証をリセット]** をクリックして、モバイル認証アプリに表示されているワンタイムパスワードを入力します。
     b. 画面の指示に従います。

TOTP デバイスを紛失した場合の二要素認証の復元

- 保管されたPDFファイルにあるQRコードを使用して、新しいデバイスをリンクします。
- 認証アプリがバックアップをサポートしている場合は、バックアップコードからアカウントへのアクセスを復元します。
- 認証アプリがこれをサポートしている場合は、別のモバイルデバイスから同じアカウントでアプリを開きます。

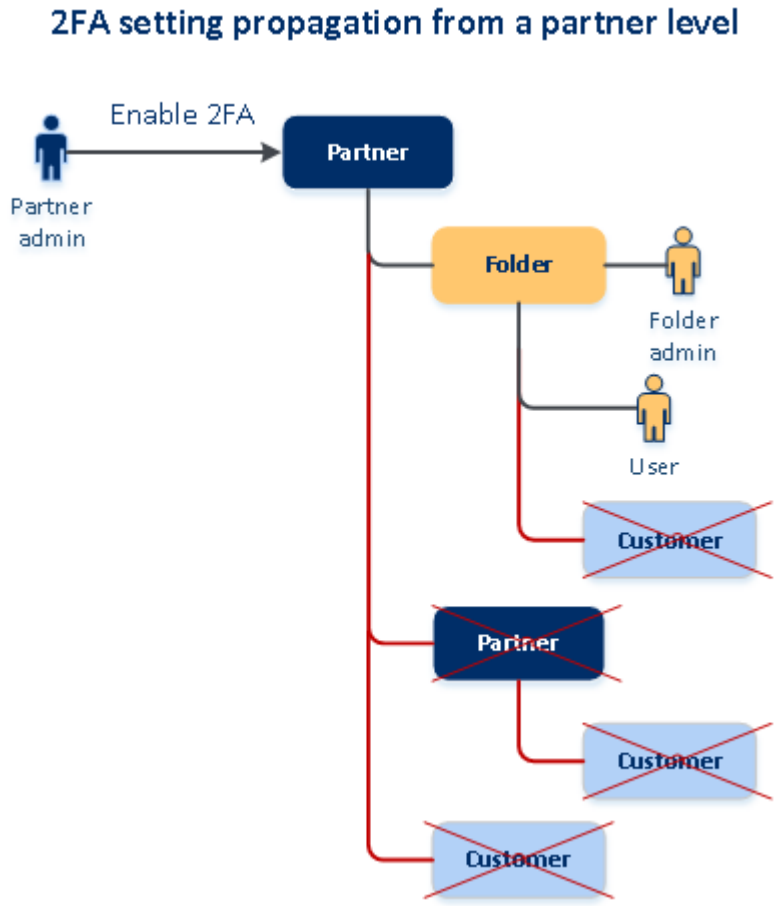
二要素設定のテナントレベル内での伝達

二要素認証は**組織レベル**で設定されます。二要素認証は以下のように有効または無効にすることができます。

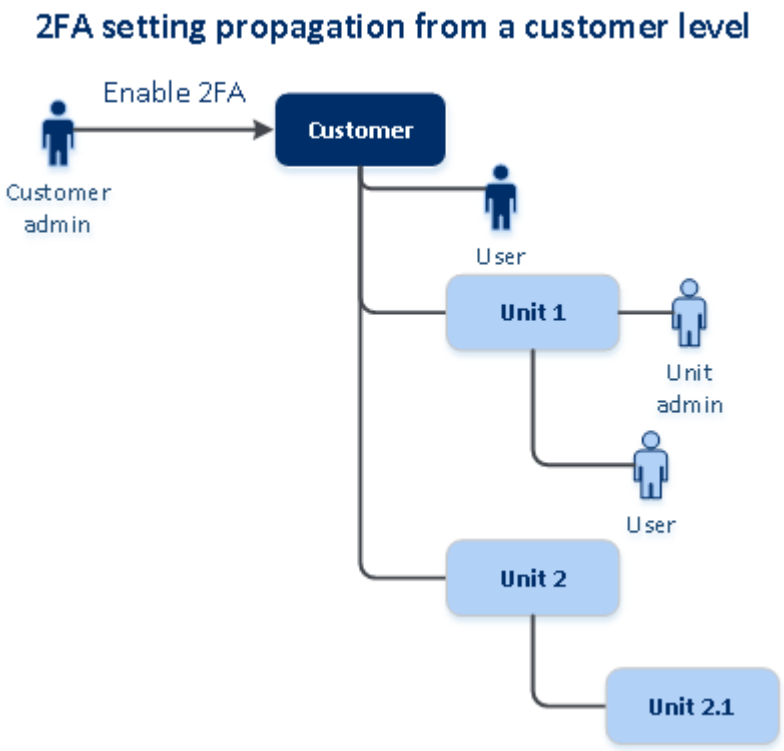
- 自分の組織について。
- 子テナントについて（**サポートアクセス**オプションがその子テナント内で有効になっている場合のみ）。

二要素認証設定はテナントレベル内で以下のように伝達されます。

- フォルダは二要素認証設定をパートナー組織から自動的に継承します。以下のスキームでは、赤い線は二要素認証設定の伝達が不可能であることを意味します。



- 各部署は二要素認証設定を顧客組織から自動的に継承します。



注意

1. **サポートアクセス**オプションがその子テナント内で有効になっている場合のみ、子組織の二要素認証を有効または無効にすることができます。
2. **サポートアクセス**オプションがその子テナント内で有効になっている場合のみ、子組織のユーザーの二要素認証設定を管理することができます。
3. フォルダまたは部署レベルの二要素認証を設定することはできません。
4. 親組織でこの設定が有効でない場合でも、二要素認証設定を設定できます。

テナントの二要素認証の設定

24.09リリースから、本番モードのすべてのパートナーテナント（直接、間接）では、デフォルトで二要素認証（2FA）が有効になり、無効にすることはできません。

トライアルパートナーは、アカウントが本番モードに切り替えられるとはじめて2FAが自動で有効になります。

サービスアカウント（2FAが無効になっているユーザー）のサポートは継続します。パートナー管理者は、ユーザーをサービスアカウントに変換することで、引き続き一時的に2FAを無効にできます。既存のサービスアカウントには影響がありません。これは、基本認証を使用するカスタム統合には2FAと互換性がないので重要です。このような統合の推奨解決策は、APIクライアントに統合を移行することです。

カスタマーテナントに対して2FAが強制されるわけではありませんが、組織で2FAを有効にすることを強くお勧めします。パートナー管理者としてカスタマー管理者に偽装して、自分が管理するカスタマーに対して2FAを有効にできます。

二要素認証を有効にするには

必要なロール: パートナー管理者またはカスタマー管理者

1. 管理ポータルにログインします。
2. **[クライアント]** に移動し、二要素認証を有効にするカスタマーテナントを選択します。
3. **[設定]** > **[セキュリティ]** へ進みます。
4. **[二要素認証]**のトグルをスライドし、**[有効化]** をクリックします。

組織のすべてのユーザーは、各自のアカウントに二要素認証を設定する必要があります。次回サインインしようとしたとき、または現在のセッションが期限切れになったときに、二要素認証が求められます。

アカウントに二要素認証を設定したユーザーの数が、トグルの下の進行状況バーに表示されます。アカウントを構成しているユーザーを確認するには、**[My Company（自分の会社）]** > **[ユーザー]** タブに移動し、**[2FAステータス]** 列を確認します。アカウントに二要素認証をまだ構成していないユーザーの2FAステータスは、**[セットアップが必要]** です。

二要素認証の構成が正常に完了すると、ユーザーはサービスコンソールへの毎回のログイン時に、ログイン情報、パスワード、およびTOTPコードの入力を求められるようになります。

二要素認証を無効にするには

注意
この手順は、カスタマーテナントのコンテキストでのみ適用されます。本番環境のパートナーテナントは、アカウントと子パートナーの二要素認証を無効にすることはできません。

必要なロール: パートナー管理者

1. 管理ポータルにログインします。
2. **[クライアント]** に移動し、二要素認証を無効にするカスタマーテナントを選択します。
3. **[設定]** > **[セキュリティ]** へ進みます。
4. 二要素認証を無効にするには、トグルをオフにして、**[無効化]** をクリックします。
5. （少なくとも 1 人のユーザーが組織内で二要素認証を設定している場合）モバイルデバイス上の認証アプリケーション内に生成された TOTP コードを入力します。

これで、組織の二要素認証が無効になり、すべてのシークレットが削除され、すべての信頼できるブラウザが無効になります。すべてのユーザーは、各自のログインIDとパスワードのみを使用してシステムにログインすることになります。**[My Company（自分の会社）]** > **[ユーザー]** タブの **[2FAステータス]** 列は非表示になります。

ユーザーの二要素認証を管理する

マネージドサービスプロバイダーとして、管理しているテナント内のすべてのユーザーの二要素認証設定を監視し、管理ポータルの**[会社概要]** > **[ユーザー]**タブで設定をリセットできます。

監視

管理ポータルの **[My Company（自分の会社）]** > **[ユーザー]** 以下に、組織内の全ユーザーのリストが表示されます。**2FAステータス**には、ユーザーの二要素設定が設定されているかどうかが表示されます。

ユーザーの二要素認証をリセットするには

1. 管理ポータルで **[My Company（自分の会社）]** > **[ユーザー]** へ進みます。
2. **[ユーザー]** タブで、設定を変更するユーザーを探し、省略記号アイコンをクリックします。
3. **[二要素認証をリセット]** をクリックします。
4. 第2要素デバイス上の認証アプリケーション内に生成されたTOTPコードを入力し、**[リセット]** をクリックします。

> **注意**
> ユーザーの二要素認証をリセットする場合は、ユーザーのデバイスではなく、自分の二要素目のデバイスからの時間ベースのワンタイムパスワード (TOTP) を入力する必要があります。これは、リセットを実行するログイン中のユーザーとして、二要素認証の資格情報を使用してアクションを確認ステップとして認証する必要があることを意味します。

結果として、ユーザーは二要素認証を再び設定できるようになります。

ユーザーの信頼済みブラウザをリセットするには

1. 管理ポータルで **[My Company（自分の会社）]** > **[ユーザー]** へ進みます。
2. **[ユーザー]** タブで、設定を変更するユーザーを探し、省略記号アイコンをクリックします。
3. **[信頼できるブラウザをすべてリセット]** をクリックします。
4. 第2要素デバイス上の認証アプリケーション内に生成されたTOTPコードを入力し、その後 **[リセット]** をクリックします。

> **注意**
> ユーザーの二要素認証をリセットする場合は、ユーザーのデバイスではなく、自分の二要素目のデバイスからの時間ベースのワンタイムパスワード (TOTP) を入力する必要があります。これは、リセットを実行するログイン中のユーザーとして、二要素認証の資格情報を使用してアクションを確認ステップとして認証する必要があることを意味します。

すべての信頼済みブラウザをリセットされたユーザーは、次のログイン時にTOTPコードを入力する必要があります。

ユーザーは手動ですべての信頼済みブラウザおよび二要素認証設定をリセットできます。これは、ユーザーがシステムにログインする際に、それぞれのリンクをクリックし、TOTP コードを入力して操作を確認することにより実行できます。

ユーザーの二要素認証を無効にするには

二要素認証を無効にすると、テナントのセキュリティが低下する可能性があるため、お勧めしません。

例外として、あるユーザーの二要素認証を無効にしておいて、テナントに属する他のすべてのユーザーについては二要素認証を維持する場合があります。この回避策は、クラウドとの統合が構成されているテナント内で二要素認証が有効になっており、この統合機能により、ユーザーアカウント（ログインパスワード）を介して、プラットフォームに対する認証が行われる場合に使用されます。統合を継続して利用する場合の一時的な解決策として、ユーザーを二要素認証が適用されないサービスアカウントに変更できます。

重要
二要素認証を無効にする目的で、一般ユーザーをサービスユーザーに切り替えることは、テナントのセキュリティにリスクをもたらすため、推奨されません。

テナントの二要素認証を無効にすることなく、クラウドとの統合を使用できるようにする安全なソリューションとしては、APIクライアントを作成した上で、クラウド統合をそれらと連携させる構成が推奨されます。

1. 管理ポータルで **[My Company（自分の会社）]** > **[ユーザー]** へ進みます。
2. **[ユーザー]** タブで、設定を変更するユーザーを探し、省略記号アイコンをクリックします。
3. **[サービスアカウントとしてマーク]** をクリックします。結果として、ユーザーは**サービスアカウント**と呼ばれる特別な二要素認証ステータスを獲得します。
4. （少なくともテナント内の1人のユーザーが二要素認証を設定している場合）無効化を確認するため、自分の第2要素デバイス上の認証アプリケーション内に生成されたTOTPコードを入力します。

注意
ユーザーの二要素認証をリセットする場合は、ユーザーのデバイスではなく、自分の二要素目のデバイスからの時間ベースのワンタイムパスワード (TOTP) を入力する必要があります。これは、リセットを実行するログイン中のユーザーとして、二要素認証の資格情報を使用してアクションを確認ステップとして認証する必要があることを意味します。

ユーザーの二要素認証を有効にするには

管理者は、以前に無効化した特定のユーザーの二要素認証を有効にする必要が生じるかもしれません。

1. 管理ポータルで **[My Company（自分の会社）]** > **[ユーザー]** へ進みます。
2. **[ユーザー]** タブで、設定を変更するユーザーを探し、省略記号アイコンをクリックします。
3. **[標準アカウントとしてマーク]** をクリックします。結果として、ユーザーはシステムに入る際に二要素認証を設定するか、TOTPコードを入力する必要が生じます。

第2要素デバイスを紛失した場合の二要素認証のリセット

第2要素デバイスの紛失時にアカウントへのアクセスをリセットするには、推奨アプローチの1つに従ってください。

- TOTPシークレット（QRコードまたは英数字コード）をバックアップから復元します。
  他の第2要素デバイスを使用し、このデバイスにインストールされている認証アプリケーションに保存されているTOTPシークレットを追加します。
- 管理者に二要素認証設定のリセットを依頼します。

総当たり攻撃に対する保護

総当たり攻撃とは、侵入者が正しいパスワードを推測しつつ大量のパスワードを送信してシステムへのアクセスを取得しようとする攻撃です。

プラットフォームの総当たり攻撃に対する保護メカニズムは、デバイス Cookie に基づいています。

プラットフォームで使用される総当たり攻撃に対する保護の設定は、あらかじめ定義されています。

パラメータ	パスワードの入力	TOTP コードの入力
試行上限	10	5
試行上限期間（上限はタイムアウトの後にリセットされます）	15 分（900 秒）	15 分（900 秒）
ロックアウト発生のタイミング	試行上限 +1（11 回目の試行時）	試行上限
ロックアウト期間	5 分（300 秒）	5 分（300 秒）

二要素認証が有効化されている場合、両方の要素（パスワードと TOTP コード）を用いた認証が成功した後に限り、デバイス Cookie がクライアント（ブラウザ）に発行されます。

信頼済みブラウザに対しては、1 つの要素（パスワード）のみを用いた認証が成功した後にデバイス Cookie が発行されます。

TOTP コードの入力の試行は、デバイスごとにではなくユーザーごとに登録されます。それで、ユーザーが別のデバイスを使用して TOTP コードを入力しようとしても、ブロックされます。

アップセルカスタマー向けのアップセル施策を構成

アップセルは、カスタマーに他の機能を購入してもらうための手法の1つです。

基本Cyber Protectエディションを利用している既存のカスタマーに対して、さらに高度な機能をお勧めしたいとお考えかもしれません。

カスタマーごとにアップセル機能を有効または無効にできます。デフォルトでは、アップセルオプションは有効になっています。カスタマーには、購入するまで使用できない追加機能が表示されます。この追加機能は、お勧めのアドバンスドパックの名前またはアイコンがすべて緑色でハイライト表示したラベルで表示されます。カスタマーでアップセルポイントをクリックすると、ダイアログに必要なアドバンスドパックを有効にするように促すメッセージが表示されます。カスタマーが **[必要なアドバンスドパックを有効にする]** リンクをクリックすると、確認ダイアログが表示されます。パートナーレベルで購入URLが構成されている場合、カスタマーが **[有効]** ボタンをクリックすると、そのURLにカスタマーがリダイレクトされます。

購入リンクを構成するには

パートナー管理者は、**[有効]** ボタンのリンクを構成でき、そのリンクでカスタマーは高度なサービスを購入するパートナーWeb サイトにリダイレクトされます。

1. 管理ポータルのナビゲーションメニューで、**[設定]** > **[ブランディング]** を選択します。
2. **[アップセル]** セクションで、**[購入URL]** 文字列の値を編集します。

注意
カスタマイズはパートナーとフォルダレベルで設定できます。カスタマイズは、カスタマイズが設定されているテナントのすべての直接および間接の子パートナー/フォルダおよび顧客に適用されます。

カスタマーごとにアップセル機能を無効化するには

1. 管理ポータルで **[クライアント]** へ進みます。
2. カスタマーを選択し、右ペインに移動して、**[設定]** タブをクリックしてから、**[全般設定]** をクリックします。
3. **[アップセル]** セクションで、**[高度な機能オプションの昇格]** を無効にして、選択したカスタマーのアップセル シナリオをオフにします。

アップセル要素がカスタマーに表示されます

ホワイトリスト

[ホワイトリスト] メニューが **[保護]** > **[マルウェア対策]** に追加されます。

企業の特定のアプリケーションがウイルス対策ソリューションで偽陽性の判定に基づいて検出される場合、信頼できるアプリケーションとしてホワイトリストに追加する作業を手動で行うと、非常に時間がかかってしまうことがあります。ホワイトリストにより、そのようなアプリケーションを許可リストに追加するプロセスを自動化できます。ウイルスおよびマルウェア対策保護モジュールでバックアップをスキャンし、スキャンしたデータを分析して、適切なアプリケーションを許可リストに追加し、偽陽性の判定に基づく検出を防ぎます。

このアップセルポイントは、Advanced Securityパックの販売促進を行います。

保護計画の作成または編集

次の各パックのさまざまな高度機能は、カスタマーが保護計画を作成または編集する際に表示されます。

- Direct Backup to Public Cloud
- RMM
- データ漏洩防止
- ウイルスおよびマルウェア対策保護
- Security + XDR

データ漏洩防止

[データ損失防止] アップセルポイントは、Cyber Protectionコンソールの **[保護]** メニュー項目の下にあります。

このアップセルポイントは、Data Loss Preventionサービスの販売促進を行います。

ロケーションとストレージの管理

[設定] > **[ロケーション]** セクションでは、**Cyber Protection**と**File Sync & Share**サービスをパートナーやカスタマーに提供するために使用できるクラウドストレージおよびディザスタリカバリインフラストラクチャが表示されます。

他のサービス用に設定されたストレージは、今後のリリースで **[ロケーション]** セクションに表示されます。

ロケーション

ロケーションは、クラウドストレージとディザスタリカバリインフラストラクチャを都合よくグループ化できるコンテナです。特定のデータセンターまたはインフラストラクチャコンポーネントの地理的なロケーションなど、任意に選択したものを表すことができます。

ロケーションはいくつでも作成して、バックアップストレージ、ディザスタリカバリインフラストラクチャ、および**File Sync & Share**ストレージを追加できます。1つのロケーションは、複数のクラウドストレージを含むことができますが、ディザスタリカバリインフラストラクチャは1つのみです。

ストレージの処理に関する情報については、"ストレージの管理"（168ページ）を参照してください。

パートナーと顧客向けのロケーションの選択

パートナー/フォルダテナントを作成するときは、複数のロケーションを選択し、この中で新しいテナントで使用できるサービスごとに複数のストレージを選択できます。

顧客テナントを作成するときは、1つのロケーションを選択し、このロケーション内でサービスごとに1つのストレージを選択する必要があります。顧客に割り当てられたストレージは後から変更できますが、それは使用量が0 GBのときに限られます。つまり、顧客がストレージを使い始める前か、ストレージからすべてのバックアップを削除した後ということです。

テナントが **[クライアント]** タブで選択されると、顧客テナントに割り当てられたストレージに関する情報がテナントの詳細パネルに表示されます。記憶域スペースの使用状況に関する情報はリアルタイムで更新されません。情報が更新されるまで最大24時間かかることがあります。

地理的冗長性については、"地理的冗長性ストレージ"（174ページ）を参照してください。

ロケーションの操作

新しいロケーションを作成するには、**[ロケーションの追加]** をクリックし、ロケーション名を指定します。

ストレージまたはディザスタリカバリインフラストラクチャを別のロケーションに移動するには、ストレージまたはインフラストラクチャを選択し、**ロケーション**フィールドで鉛筆アイコンをクリックし、ターゲットロケーションを選択します。

ロケーションの名前を変更するには、ロケーション名の横にある省略記号アイコンをクリックし、**[名前を変更]** をクリックしてから、新しいロケーション名を指定します。

ロケーションを削除するには、ロケーション名の横にある省略記号アイコンをクリックし、**[削除]** をクリックしてから、操作を確定します。空のロケーションのみ削除できます。

ストレージの管理

新しいストレージの追加

- **Cyber Protection**サービス:
  - デフォルトでは、バックアップされたデータは のデータセンター上のストレージサーバーに転送される仕組みですが、
  - 上位の管理者がパートナーテナントに対して **[パートナーが所有するバックアップストレージ]** 提供項目を有効にしている場合、パートナー管理者は、 Cyber Infrastructureソフトウェアを使用してパートナーが所有するデータセンターにストレージを編成できます。**[ロケーション]** セクションの **[バックアップストレージの追加]** をクリックすると、独自のデータセンターにおけるバックアップストレージの構成についての情報が表示されます。
  - 上位の管理者がパートナーテナントに対して **[パートナーが所有するディザスタリカバリインフラストラクチャ]** 提供項目を有効にしている場合、パートナー管理者はパートナーが所有するデータセンターにディザスタリカバリインフラストラクチャを編成できます。ディザスタリカバリインフラストラクチャの追加についての情報は、テクニカルサポートにお問い合わせください。

注意
データセンターにより使用されている、Amazon S3、Microsoft Azure、Google Cloud Storage、Wasabiなどのパブリッククラウドオブジェクトストレージでは、バックアップを検証することができません。 パートナーにより使用されている、パブリッククラウドオブジェクトストレージでは、バックアップを検証できます。ただし、検証処理によってこれらのパブリックオブジェクトストレージからの出力トラフィックが増加し、コストが大幅に増大する場合があります。そのため、これを有効にすることは推奨されていません。

- 他のサービスで使用されるストレージの追加についての情報は、テクニカルサポートにお問い合わせください。

ストレージの削除

お客様またはお客様の子テナントによって追加されたストレージを削除することができます。

ストレージが顧客テナントに割り当てられている場合、ストレージを削除する前に、すべての顧客テナントにストレージを使用するサービスを無効にしなければなりません。使用量がゼロになったときにストレージを削除できます。

ストレージの削除

1. 管理ポータルにログインします。
2. ストレージが追加されたテナントに移動します。
3. **[設定]** > **[ロケーション]** の順にクリックします。
4. 削除するストレージを選択します。
5. ストレージのプロパティパネルで三本線アイコンをクリックし、**[ストレージの削除]** をクリックします。
6. 操作を確定します。

不変ストレージ

不変ストレージは、ランサムウェア、誤操作による削除、内部の脅威からバックアップを保護し、不正または意図しない変更に対する防御策を提供します。バックアップが保持期間中に変更、暗号化、または削除されるのを防ぎ、本番システムや管理者アカウントが侵害された場合でも、改ざん防止および回復可能な状態を保証します。

不変ストレージは、サポートされているクラウドストレージインスタンスに保管されたすべてのクラウドバックアップで利用可能です。"サポートされるストレージとエージェント"（170ページ） を参照してください。

不変性ストレージを使用すると、指定した保持期間中に削除されたバックアップにアクセスできます。これらのバックアップから内容を復元できますが、変更、移動、または削除することはできません。保持期間が終了すると、削除されたバックアップは完全に削除されます。

不変ストレージには以下のバックアップが含まれています。

- 手動で削除されたバックアップ。
- 保護計画の **[保持する期間]** セクションまたはクリーンアップ計画の **[保持ルール]** セクションの設定に従って自動的に削除されるバックアップ。

削除されたバックアップは不変ストレージに保存され、ストレージスペースを消費します。また消費量に応じて課金が発生します。

削除されたテナントは、不変ストレージを含め、ストレージの利用料はかかりません。

不変ストレージモード

パートナーテナントの場合、不変ストレージモードを選択することはできません。パートナーは、別のパートナーまたはカスタマーテナントの不変ストレージを無効にしたり、再度有効にしたり、保持期間を設定したりできます。

顧客の管理者は、不変ストレージの無効化と再有効化、モードと保持期間の変更を実行できます。

不変ストレージは以下のモードで利用できます。

- **ガバナンスモード**
  不変ストレージを無効にしたり、再度有効にしたりできます。保持期間の変更や、コンプライアンスモードへの切り替えもできます。

注意
2024年9月から、パートナーテナントとカスタマーテナントのすべてのAcronis Hosted Storageで、14日間の保持期間を設定した不変ストレージのガバナンスモードがデフォルトで有効になります。詳細については、このナレッジベースの記事を参照してください。

- **コンプライアンスモード**

警告
一度コンプライアンスモードを選択すると、元に戻せなくなります。

不変ストレージを無効にすることはできません。保持期間を変更したり、ガバナンスモードに戻したりすることはできません。

サポートされるストレージとエージェント

- 不変ストレージはクラウドストレージのみでサポートされます。
  - 不変ストレージは、 Cyber Infrastructureバージョン4.7.1以降を利用する、Acronisまたはパートナーがホストするクラウドストレージストレージで使用できます。
  - Cyber Infrastructure ストレージ、Amazon S3 および EC2 ストレージ、Microsoft Azure ストレージなど、 Cyber Infrastructure Backup Gatewayで使用できるすべてのストレージがサポートされています。
  - 不変ストレージでは、 Cyber Infrastructure のバックアップゲートウェイサービス用にTCPポート40440が開放されている必要があります。バージョン4.7.1以降では、TCPポート40440は、**[バックアップ（ABGW）パブリック]** トラフィックタイプで自動的に開放されます。トラフィックタイプの詳細については、Acronis Cyber Infrastructureの文書を参照してください。
- 不変ストレージには、プロテクションエージェントバージョン21.12（ビルド15.0.28532）以降が必要です。
- TIBX（バージョン12）バックアップのみがサポートされています。

不変ストレージの構成

2024年9月以降、すべてのパートナーテナントとカスタマーテナントに対して、14日間の保持期間で、ガバナンスモードの不変ストレージがデフォルトで有効になります。

注意
削除されたバックアップへのアクセスを許可するには、受信接続用にバックアップストレージのポート40440を開く必要があります。

不変ストレージを構築するには

パートナーテナントで

1. 管理ポータルに管理者としてログインしてから、**[設定]** > **[セキュリティ]** へ移動します。
2. **[不変ストレージ]** スイッチがオンになっていることを確認します。
3. 14～3650日の範囲で保持期間を指定します。

デフォルトの保持期間は14日間です。保持期間が長くなると、ストレージの使用量が増える可能性があります。

4. **[保存]** をクリックします。

カスタマーテナントで

1. 管理ポータルに管理者としてログインしてから、**[クライアント]** に移動します。
2. カスタマーテナントの設定を編集するには、テナント名をクリックします。
3. ナビゲーションメニューで、**[設定]** > **[セキュリティ]** に進みます。
4. **[不変ストレージ]** スイッチがオンになっていることを確認します。
5. 14～3650日の範囲で保持期間を指定します。

   デフォルトの保持期間は14日間です。保持期間が長くなると、ストレージの使用量が増える可能性があります。
6. 不変ストレージモードを選択し、プロンプトが表示されたら選択を確定します。
   - **ガバナンスモード**

     このモードでは、すべてのバックアップが、指定した保持期間の間、不変ストレージに保持されるため、ランサムウェアや悪意のある相手がバックアップデータを改ざんしたり消去したりすることはできません。また、ディザスタリカバリにとって重要なバックアップデータの整合性も保証されます。

     このモードでは、不変ストレージの無効化と再度の有効化や、保持期間の変更、コンプライアンスモードへの切り替えができます。
   - **コンプライアンスモード**

     コンプライアンスモードは、ガバナンスモードの機能に加えて、データの改ざんを防ぐことで、組織がデータの保持とセキュリティの規制要件を順守するのに役立ちます。

     警告

     コンプライアンスモードを選択すると、元に戻すことはできません。このモードを選択した後は、不変のストレージを無効にしたり、保持期間を変更したり、ガバナンスモードに戻したりすることはできません。
7. **[保存]** をクリックします。
8. 既存のアーカイブを不変ストレージに追加するには、対応する保護計画を手動で実行するか、スケジュールに従って実行して、そのアーカイブに新しいバックアップを作成します。

   警告

   アーカイブを不変ストレージに登録されていない状態でバックアップを削除すると、バックアップは完全に削除されます。

不変ストレージを無効化するには

パートナーテナントで

- ヘルプについては、サポートチームまでお問い合わせください。

重要

この変更は、不変ストレージがデフォルトで有効になっていない子テナントで、カスタマーレベルでその不変ストレージの設定が変更されなかった場合にのみ継承されます。

24.09リリースから、カスタマーテナントでは、デフォルトで不変性ストレージが有効になります。データセンターごとのイネーブルメント状況を確認するには、このナレッジベースの記事を参照してください。パートナーレベルで不変ストレージを無効にしても、カスタマーテナントには影響しません。不変ストレージを無効にするには、カスタマーテナントに移動します。

注意

不変ストレージを無効にした後、削除したバックアップは永久に削除されます。不変ストレージにすでに保管されているバックアップは、最長14日間（336時間）、または保持期間が短い場合はその期間中利用可能です。

例:

不変ストレージに削除されたバックアップが2つあります：

- 保持期間が7日のバックアップA。
- 保持期間が1年のバックアップB。

不変ストレージを無効化するには。

- 今バックアップを削除すると、永久に削除されます。
- 7日目に、バックアップAは元の保持期間に従って永久に削除されます。
- 14日目に、バックアップBは不変ストレージの猶予期間に従って永久に削除されます（元の保持期間が14日を超えるため）。

カスタマーテナントで

- ヘルプについては、サポートチームまでお問い合わせください。

注意

ガバナンスモードでのみ、不変ストレージを無効にできます。

注意

不変ストレージを無効にした後、削除したバックアップは永久に削除されます。不変ストレージにすでに保管されているバックアップは、最長14日間（336時間）、または保持期間が短い場合はその期間中利用可能です。

例:

不変ストレージに削除されたバックアップが2つあります：

- 保持期間が7日のバックアップA。
- 保持期間が1年のバックアップB。

不変ストレージを無効化するには。

- 今バックアップを削除すると、永久に削除されます。
- 7日目に、バックアップAは元の保持期間に従って永久に削除されます。
- 14日目に、バックアップBは不変ストレージの猶予期間に従って永久に削除されます（元の保持期間が14日を超えるため）。

不変ストレージの使用状況の表示

Cyber Protectコンソール、または管理ポータルで生成できる**現在の使用状況**レポートで、不変ストレージがどのくらいのスペースを使用しているかを表示できます。

制限事項

- レポートの値には、ストレージ内のすべての削除されたバックアップの合計サイズとバックアップアーカイブのメタデータが含まれます。メタデータは、レポートの値の最大10%に達する場合があります。
- 値は最大24時間前の使用状況データを示します。
- 実際の使用量が0.01GB未満の場合、0.0GBと表示されます。

不変ストレージの使用状況を表示するには

Cyber Protectコンソールで

1. Cyber Protectコンソールにログインします。
2. **[バックアップ ストレージ]** > **[バックアップ]**に移動し、不変ストレージをサポートするクラウド ストレージの場所を選択します。
3. **不変ストレージとメタデータ** 列を確認します。

現在の使用状況レポート

1. 管理者として管理ポータルにログインします。
2. **[レポート]** > **[使用状況]** に移動します。
3. **[アドホック]** を選択します。
4. **[現在の使用状況]**を選択し、**[生成して送信]** をクリックします。
   Eメールアドレスに、CSV形式およびHTML形式のレポートが送信されます。
   HTMLファイルはZIPアーカイブに含まれています。

5. レポートの [**メトリクス名**] 列を確認します。
   不変ストレージの使用状況は、**クラウド ストレージ - 不変**行で確認できます。

不変ストレージの課金例

以下の例では、削除されたバックアップがデフォルトの保持期間である14日間、不変ストレージに保管されます。この期間、削除されたバックアップではストレージスペースが使用されます。保持期間が終了すると、削除済みバックアップは恒久的に削除され、ストレージ使用量は減少します。ストレージの使用量に応じて毎月課金されます。

日付	バックアップ	ストレージの使用状況	課金
4月1日	バックアップA（10GB）が作成される バックアップB（1GB）が作成される	10GB + 1GB = 11GB	
4月20日	バックアップBは削除され、不変ストレージに移動される（保持期間14日）	10GB + 1GB = 11GB	
4月30日			4月は11GBの使用量に対して課金される
5月4日	保持期間が終了したため、バックアップBが永久に削除される	11GB - 1GB = 10GB	
5月31日			5月は10GBの使用量に対して課金される

地理的冗長性ストレージ

地理的冗長性ストレージを使用すると、バックアップデータは、プライマリバックアップロケーションから地理的に離れたレプリケーションのロケーションに非同期でコピーされます。これにより、プライマリロケーションが利用できなくなった場合でも、データには耐障害性が確保され、アクセシビリティが維持されます。

レプリケーションされたデータは、元のデータと同じ容量のストレージスペースを使用します。

制限事項

- 地理的冗長性ストレージは、すべてのデータセンターで利用できるわけではありません。
- 地理的冗長性は、クラウド ストレージでのみサポートされています。パートナーホステッドストレージやパブリッククラウド ストレージなどのサードパーティストレージではサポートされていません。
- レプリケーションされたデータのロケーションは、データセンターによって異なります。詳細については、こちらのナレッジベースの記事を参照してください。
- 地理的冗長性ストレージをDisaster Recoveryと共に使用する場合は、追加の制限が適用されます。詳細については、Cyber Protect Cloudの文書を参照してください。

地理的冗長性ストレージをプロビジョニングする

地理的冗長性ストレージは、管理ポータルで該当のカスタマーテナントのプロビジョニングが行われた後に、このテナントで使用できるようになります。

地理的冗長性ストレージをプロビジョニングするには

1. 管理者として管理ポータルにログインします。
2. **[クライアント]** で、テナント名の横にある省略記号ボタン（…）> **[設定]** をクリックします。
3. **[保護]** タブで **[編集]** をクリックします。
4. **[クラウドリソース]** で、地理的冗長性を有効にするストレージを見つけます。
5. **[地理的冗長性]** の横にある **[有効化]** をクリックします。
6. **[保存]** をクリックします。

その結果、このカスタマーテナントで地理的冗長性クラウド ストレージが使用できるようになりますが、これは自動的には有効になりません。地理的冗長性ストレージを使用するには、Cyber Protectコンソールから有効化します。詳細については、"地理的冗長性ストレージを有効化する"（175ページ）を参照してください。

複数のテナントにおける地理的冗長性ストレージのプロビジョニングの詳細については、"複数のテナントへのサービス提供を有効化する"（119ページ）を参照してください。

地理的冗長性ストレージを有効化する

前提条件

- 地理的冗長性をサポートするストレージがカスタマーテナントに割り当てられます。 "パートナーと顧客向けのロケーションの選択"（167ページ）を参照してください。
- 管理ポータルでカスタマーテナント用に地理的冗長性ストレージがプロビジョニングされます。 "地理的冗長性ストレージをプロビジョニングする"（175ページ）を参照してください。
  互換性のないストレージ（たとえば、パートナーがホストするストレージ）が割り当てられている場合、地理的冗長性ストレージはプロビジョニングできません。

地理的冗長性ストレージは、Cyber Protectコンソールのメイン画面または **[設定]** タブで有効にできます。どちらの手順でも結果は同じです。

地理的冗長性ストレージを有効にするには

メイン画面での操作

1. 管理者としてCyber Protectコンソールにログインします。
   警告メッセージがCyber Protectコンソールの上部に表示されます。
2. 警告メッセージで、**[地理的冗長性クラウド ストレージを有効にする]** をクリックします。
3. レプリケーションのロケーションと料金について理解したことを確認するには、チェックボックスを選択します。
4. 選択を確定するには、 **[有効化]** をクリックします。

その結果、地理的冗長性ストレージが有効になり、バックアップデータがレプリケーションのロケーションにコピーされます。

[設定] タブでの操作

1. 管理者としてCyber Protectコンソールにログインします。
2. **[設定]** > **[システム設定]** に移動します。
3. デフォルトのバックアップオプションのリストを折りたたみ、**[地理的冗長性クラウドストレージ]** をクリックします。
4. **[地理的冗長性クラウドストレージ]** スイッチを有効にします。
5. **[保存]** をクリックします。
6. レプリケーションのロケーションと料金について理解したことを確認するには、チェックボックスを選択します。
7. 選択を確定するには、**[有効化]** をクリックします。

その結果、地理的冗長性ストレージが有効になり、バックアップデータがレプリケーションのロケーションにコピーされます。

地理的冗長性ストレージを無効化する

地理的冗長性ストレージは、Cyber Protectコンソールから無効にするか、管理ポータルでプロビジョニングを解除できます。

地理的冗長性ストレージを無効にするには

1. 管理者としてCyber Protectコンソールにログインします。
2. **[設定]** > **[システム設定]** に移動します。
3. デフォルトのバックアップオプションのリストを折りたたみ、**[地理的冗長性クラウドストレージ]** をクリックします。
4. **[地理的冗長性クラウドストレージ]** スイッチを無効にします。
5. **[保存]** をクリックします。
6. 選択を確認するには、**無効化**と入力して、**[無効化]** をクリックします。

その結果、地理的冗長性ストレージが無効になります。レプリケーションされたデータは1日以内に削除されます。

地理的冗長性ストレージのプロビジョニングを解除するには

1. 管理者として管理ポータルにログインします。
2. **[クライアント]** で、カスタマーテナントの名前の横にある省略記号ボタン（…）> **[設定]** の順にクリックします。
3. **[保護]** タブで **[編集]** をクリックします。
4. **[クラウドリソース]** で、必要なストレージ名の下の **[地理的冗長性]** チェックボックスをオフにします。
5. **[保存]** をクリックします。

その結果、カスタマーテナントの地理的冗長性ストレージが無効になり、Cyber Protectコンソールで有効にすることはできなくなります。レプリケーションされたデータは1日以内に削除されます。

ジオレプリケーションのステータスの表示

ジオレプリケーションのステータスは、プライマリバックアップロケーションからレプリケーションのロケーションにデータがコピーされているかどうかを示します。

以下のステータスがあります:

- **同期済み** - データがレプリケーションのロケーションにコピーされた。
- **同期実行中** - データをレプリケーションのロケーションにコピーしている。この操作にかかる時間は、データのサイズによって異なります。
- **保留中** - データレプリケーションが一時的に停止している。
- **無効** - データのレプリケーションが無効になっている。

レプリケーションステータスを確認するには

1. Cyber Protectコンソールにログインします。
2. [**バックアップストレージ**] タブでバックアップロケーションを選択し、バックアップアーカイブを選択します。
3. [**詳細**] をクリックし、[**ジオレプリケーションのステータス**] セクションでステータスを確認します。

アーカイブストレージ

アーカイブストレージは、長期データ保持のためのセキュリティ、スケーラブル、コスト効率の高いオブジェクトストレージです。コンプライアンス要件を満たす必要があるデータや、アクセス頻度が低いが保持しなければならないデータに使用できます。

注意
アーカイブストレージを保護計画やクラウドツークラウドバックアップ計画のバックアップ先として使用することはできません。

アーカイブストレージを使用するには、Cyber Protect コンソールで1つ以上のバケットを作成する必要があります。バケットにアクセスし、その内容を表示および管理したり、データを転送するには、S3互換のクライアントを使用する必要があります。

アーカイブストレージを使用するには、**アーカイブストレージ**クォータが管理ポータルで有効になっている必要があります。

アーカイブストレージの有効化

アーカイブストレージは、新しいカスタマーテナントに対してデフォルトで有効になっています。

既存のカスタマーテナントに対しても有効にすることができます。

不変ストレージを有効化するには

1. 管理ポータルで、**クライアント**に移動します。
2. カスタマーテナント名の横にある省略記号のアイコン（...）をクリックして、**[設定]**をクリックします。
3. **[編集]** をクリックします。
4. **[サービス]**で、**[サイバープロテクション]**をクリックします。
5. **[アーカイブストレージ]**で、**[アーカイブストレージ]**のチェックボックスを選択します。
6. **[保存]** をクリックします。

アーカイブストレージの無効化

重要
使用済みストレージスペースがゼロの場合にのみ、アーカイブストレージを無効にすることができます。

アーカイブストレージを無効化するには

1. 管理ポータルで、**クライアント**に移動します。
2. カスタマーテナント名の横にある省略記号のアイコン（...）をクリックして、**[設定]**をクリックします。
3. **[編集]** をクリックします。
4. **[サービス]**で、**[サイバープロテクション]**をクリックします。
5. **[アーカイブストレージ]**で、**[アーカイブストレージ]**のチェックボックスをクリアします。
6. **[保存]** をクリックします。

アーカイブストレージ使用量の監視

アーカイブストレージ使用量は、**[監視]** > **[使用状況]**の下 管理ポータル で監視できます。

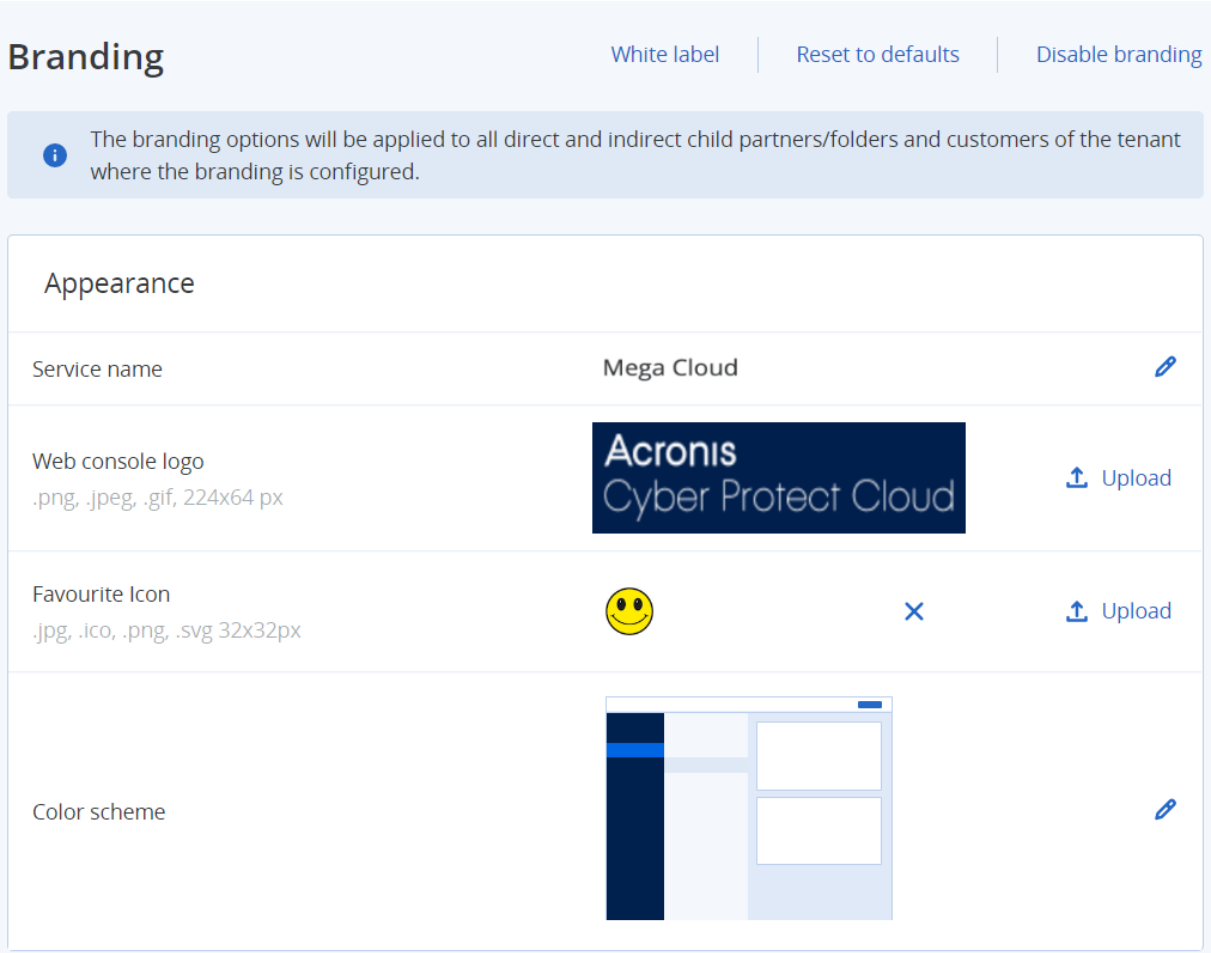
実際の使用量と請求可能な使用量の両方が表示されます。請求可能な使用量は最も近い整数テラバイトに切り上げられます。

アーカイブストレージは、オブジェクトごとに6か月の最小請求期間を適用します。この期間が終了する前にオブジェクトを削除した場合でも、6か月分の料金が適用されます。

カスタマイズとホワイトラベルの構成

[設定] > **[ブランディング]** セクションでは、パートナー管理者が管理ポータルと子テナントの**Cyber Protection**サービスのユーザーインターフェイスをカスタマイズして、上位層のパートナーとの関連付けを削除できます。

注意
ブランディング設定は、すべての子テナント（直接的または間接的に）に適用されます。自分のテナントのブランディング設定は、サービスプロバイダーによって構成されます。



カスタマイズはパートナーとフォルダレベルで設定できます。カスタマイズは、カスタマイズが設定されているテナントのすべての直接および間接の子パートナー/フォルダおよび顧客に適用されます。

他のサービスでは、それぞれのサービスコンソールで個別のカスタマイズ機能を提供しています。詳細については、対応するサービスの『ユーザーガイド』をご参照ください。

カスタマイズアイテム

外観

- **サービス名**。この名前は、管理ポータルとクラウドサービスから送信されるすべてのメールメッセージ（アカウントの有効化メール、サービス通知メール）、初回ログイン後の **[ようこそ]** 画面、および管理ポータルブラウザタブ名として使用されます。
- **Webコンソールのロゴ**。管理ポータルとサービスにロゴが表示されます。**[アップロード]** をクリックして、イメージファイルをアップロードします。
- **お気に入りアイコン**（カスタムURLを構成している場合に限り利用可能）。ファビコンは、ブラウザのタブでページタイトルの横に表示されます。**[アップロード]** をクリックして、イメージファイルをアップロードします。
- **配色**。配色は、すべてのユーザーインターフェースに使用される色の組み合わせを定義します。

注意
新しいタブで [プレビュースキーム] をクリックすると、子テナントへのインターフェースの表示状態をプレビューできます。カスタマイズは、**[配色の選択]** パネルの **[完了]** をクリックするまで適用されません。

エージェントとインストーラのカスタマイズ

WindowsエージェントとmacOSエージェントのインストールファイルおよびトレイモニタのブランディングをカスタマイズできます。

注意
このカスタマイズ機能を有効にするには、Cyber Protectionエージェントをバージョン 15.0.28816（リリース 22.01）以降にアップデートする必要があります。

- **エージェントインストーラのファイル名。**保護対象のワークロードでダウンロードされるインストールファイルの名前。
- **エージェントインストーラのロゴ。**エージェントのインストール時にセットアップウィザードに表示されるロゴです。**[アップロード]** をクリックして、イメージファイルをアップロードします。
- **エージェント名。**エージェントのインストール時にセットアップウィザードに表示される名前です。
- **トレイモニタ名。**トレイモニタウィンドウの上部に表示される名前です。

マニュアルおよびサポート

- **メインページのURL。**このページは、ユーザーが **[バージョン情報]** パネルで会社名をクリックすると開きます。
- **サポートページのURL。**このページは、ユーザーが **[バージョン情報]** パネルの **[サポートの連絡]** リンクまたは管理ポータルから送信されたメールメッセージをクリックすると開きます。
- **サポート窓口の電話。**この電話番号は **[バージョン情報]** パネルに表示されます。
- **ナレッジベースのURL。**このページは、ユーザーがエラーメッセージの **[ナレッジベース]** リンクをクリックすると開きます。
- **管理ポータル管理者ガイド。**ユーザーがこのページを開くには、管理ポータルのユーザーインターフェースの右上にある「?」アイコンをクリックしてから、**[バージョン情報]** > **[管理者ガイド]** をクリックします。
- **管理ポータル管理者ヘルプ。**ユーザーがこのページを開くには、管理ポータルのユーザーインターフェースの右上にある「?」アイコンをクリックしてから、**[ヘルプ]** をクリックします。

Cyber Protect CloudサービスのURL

カスタムドメインからCyber Protect Cloudのサービスを利用できるようになります。カスタムURLの初回設定時は **[設定]** をクリックします。既存の設定を変更する場合は **[再構成]** をクリックします。デフォルトのURL（https://cloud.acronis.com）を使用するには、**[デフォルトにリセット]** をクリックします。カスタムURLの詳細については、「カスタムWebインターフェースのURLを構成する」を参照してください。

法律文書設定

- **エンドユーザーライセンス契約（EULA）URL**。このページは、ユーザーが最初にログインした後、**[バージョン情報]** パネルまたは **[ようこそ]** 画面の**エンドユーザーライセンス契約**リンクをクリックすると開きます。またFile Sync & Shareアップロードリクエストのランディングページにも掲載されています。
- **プラットフォーム利用規約ページのURL**。このページは、パートナー管理者が最初にログインした後、**[バージョン情報]** パネルまたは **[ようこそ]** 画面の **[プラットフォーム利用規約]** リンクをクリックすると開きます。
- **個人情報保護方針URL**。このページは、ユーザーが最初にログインした後、**[ようこそ]** 画面の**プライバシーステートメント**リンクをクリックすると開きます。またFile Sync & Shareアップロードリクエストのランディングページにも掲載されています。

重要
ようこそ画面に文書を表示したくない場合は、その文書のURLを入力しないでください。

注意
File Sync & Shareアップロードリクエストの詳細については、Cyber Files Cloudユーザーズガイドを参照してください。

アップセル

- **購入URL**。このページは、ユーザーが **[今すぐ購入]** をクリックして、Cyber Protectionサービスのより上位のエディションにアップグレードする場合に開きます。カスタマー向けのアップセル施策の詳細については、「カスタマー向けアップセル施策の構成」を参照してください。

モバイルアプリ

- **App Store**。このページは、ユーザーが**Cyber Protection**サービスの **[追加]** > **[iOS]** をクリックすると開きます。
- **Google Play**。このページは、ユーザーが**Cyber Protection**サービスの **[追加]** > **[Android]** をクリックすると開きます。

メールサーバー設定

管理ポータルとサービスからメール通知を送信するために使用するカスタムのメールサーバーを指定できます。カスタムメールサーバーを指定するには、**[カスタマイズ]** をクリックしてから、次の設定を指定します。

- **[差出人]**で、メール通知の **[差出人]** フィールドに表示される名前を入力します。
- **[SMTP]** に送信メール サーバー（SMTP）の名前を入力します。
- **[ポート番号]** で、送信メールサーバーのポート番号を入力します。デフォルトでは、ポートは 25 に設定されます。

- **[暗号化]** で、SSL または TLS 暗号化を使用するかどうかを選択します。暗号化を無効にするには **[なし]** を選択してください。
- **[ユーザー名]** および **[パスワード]** で、メッセージを送信するために使用するアカウントの資格情報を指定します。

カスタマイズの設定

1. 管理ポータルにログインします。
2. カスタマイズを設定するテナントを指定します。
3. **[設定]** > **[カスタマイズ]** をクリックします。
4. （カスタマイズがまだ有効になっていない場合）**[カスタマイズを有効化]** をクリックします。
5. 上記のカスタマイズアイテムを設定します。

カスタマイズの設定をデフォルトに戻す

すべてのカスタマイズ項目をデフォルト値にリセットできます。

1. 管理ポータルにログインします。
2. カスタマイズをリセットするテナントに移動します。
3. **[設定]** > **[カスタマイズ]** をクリックします。
4. 右上の **[デフォルトの復元]** をクリックします。

カスタマイズの無効化

自分のアカウントとすべての子テナントのカスタマイズを無効にできます。

1. 管理ポータルにログインします。
2. カスタマイズを無効にするテナントに移動します。
3. **[設定]** > **[カスタマイズ]** をクリックします。
4. 右上の **[カスタマイズを無効化]** をクリックします。

ホワイトラベル

すべての子パートナーと子カスタマーについて、（Windows、macOS、およびLinuxの）Cyber Protectionエージェント、（Windows、macOS、およびLinuxの）Cyber Protection Monitor、およびConnect Clientをブランド化するか、またはホワイトラベル化するかを制御できます。このオプションを有効にすると、エージェント、Connect Client、およびトレイモニタがホワイトラベル化されます。またこの設定は、インストーラとCyber Protection Monitor で使用される名前とロゴに影響します。

ホワイトラベルの適用

1. 管理ポータルにログインします。
2. ホワイトラベルを適用するテナントに移動します。
3. **[設定]** > **[カスタマイズ]** をクリックします。

4. ウィンドウの上端で、[**ホワイトラベル**] をクリックして、[**サービス名**]、[**エンドユーザーライセンス契約（EULA）URL**]、[**管理ポータル管理者ガイド**]、[**管理ポータル管理者ヘルプ**]、および [**メールサーバー設定**] を除くすべてのカスタマイズ項目を消去します。

企業プロファイルを編集する

会社の詳細や連絡先は、管理ポータルの [**会社概要**] > [**企業プロファイル**]で変更できます。

このページでは、会社情報、法的住所、第1連絡先、請求先住所、第1請求書発行先連絡先、およびその他の連絡先を変更できます。

デフォルトでは、請求先住所と第1請求書発行連絡先フィールドは空です。請求先住所と請求書発行連絡先を異なるものにする場合は、次のように設定する必要があります。

注意
テナントごとに第1連絡先と第1請求書発行連絡先をそれぞれ1つだけ持つことができ、削除することはできません。

会社の請求先住所と第1請求書発行連絡先を構成するには

1. 管理コンソールで、[**会社概要**] > [**企業プロファイル**]に移動し、[**編集**]をクリックします。
2. [**請求先住所**]セクションで、請求書発行先の住所を入力します。
3. [**請求関連の連絡先を追加**]セクションで、請求書発行の第1連絡先の名、姓、会社のEメールを入力します。
   オプションで、電話番号を入力できます。
4. [**保存**] をクリックします。

また、[**会社の法的情報と同じ**]チェックボックスを選択することで、法務担当者を請求書発行の第1連絡先として使用することもできます。

会社の連絡先の構成

パートナーとして、自社および自社が管理するテナントの連絡先情報を設定できます。

ユーザーのロールに応じて、複数の連絡先を追加し、会社の連絡先を割り当てることができます。Cyber Protectプラットフォームに存在するユーザーから連絡先を作成したり、サービスへのアクセス権を持たないユーザーの連絡先情報を追加したりできます。

このリストの連絡先には、新機能やプラットフォームの重要な変更に関するアップデートが送信されます。

社内の連絡先を構成するには

1. 管理コンソールで、[**My Company（自分の会社）**] > [**企業プロファイル**] に移動します。
2. **連絡先**セクションで [+] をクリックします。
3. 連絡先を作成するオプションを選択します。

- **既存のユーザーから作成**
  - ドロップダウンリストからユーザーを選択します。
  - 会社の連絡先を選択します。
    - **課金** - プラットフォームの使用状況レポートで、重要な変更に関するアップデートをお伝えするための連絡先です。
    - **技術** - プラットフォームにおける技術関連の重要な変更について、アップデートをお伝えするための連絡先です。
    - **業務** - プラットフォームにおける業務関連の重要な変更について、アップデートをお伝えするための連絡先です。

    注意
    単一のユーザーに1件または複数の会社の連絡先を割り当てることができます。

    企業プロファイルの連絡先リストからユーザーに関連付けられている連絡先を削除しても、そのユーザーは削除されません。システムにより、ユーザーに関連付けられた会社の連絡先の割り当てがすべて解除されるため、これらの情報は、**ユーザー**リストの **[会社の連絡先]** 列に表示されなくなります。
    ユーザーに関連付けられている連絡先のEメールアドレスを変更する場合、システムから新しく定義したアドレスを確認するよう求められます。このアドレスにメールが送信され、ユーザーは変更を確認する必要があります。
- **新しい連絡先を作成**
  - 連絡先情報を指定します。
    - **氏名（名）**—連絡先となる担当者の名前です。このフィールドは必須です。
    - **氏名（姓）**—連絡先となる担当者の姓です。このフィールドは必須です。
    - **業務用Eメールアドレス**—連絡先となる担当者のEメールアドレスです。このフィールドは必須です。
    - **業務用電話番号** - このフィールドはオプションです。
    - **役職** - このフィールドはオプションです。
  - **[会社の連絡先]** を選択します。
    - **課金** - プラットフォームの使用状況レポートで、重要な変更に関するアップデートをお伝えするための連絡先です。
    - **技術** - プラットフォームにおける技術関連の重要な変更について、アップデートをお伝えするための連絡先です。
    - **業務** - プラットフォームにおける業務関連の重要な変更について、アップデートをお伝えするための連絡先です。

    注意
    単一のユーザーに1件または複数の会社の連絡先を割り当てることができます。

4. **[追加]** をクリックします。

テナントの連絡先を構成するには

注意
子テナントの連絡先情報を変更すると、変更内容がテナントに表示されます。

1. 管理ポータルで **[クライアント]** へ進みます。
2. テナントをクリックして、**[設定]** をクリックします。
3. **連絡先**セクションで [+] をクリックします。
4. 連絡先を作成するオプションを選択します。
   - **既存のユーザーから作成**
     - ドロップダウンリストからユーザーを選択します。
     - 会社の連絡先を選択します。
       - **課金** - プラットフォームの使用状況レポートで、重要な変更に関するアップデートをお伝えするための連絡先です。
       - **技術** - プラットフォームにおける技術関連の重要な変更について、アップデートをお伝えするための連絡先です。
       - **業務** - プラットフォームにおける業務関連の重要な変更について、アップデートをお伝えするための連絡先です。

       注意
       単一のユーザーに1件または複数の会社の連絡先を割り当てることができます。

       企業プロファイルの連絡先リストからユーザーに関連付けられている連絡先を削除しても、そのユーザーは削除されません。システムにより、ユーザーに関連付けられた会社の連絡先の割り当てがすべて解除されるため、これらの情報は、**ユーザー**リストの **[会社の連絡先]** 列に表示されなくなります。
       ユーザーに関連付けられている連絡先のEメールアドレスを変更する場合、システムから新しく定義したアドレスを確認するよう求められます。このアドレスにメールが送信され、ユーザーは変更を確認する必要があります。
   - **新しい連絡先を作成**
     - 連絡先情報を指定します。
       - **氏名（名）**—連絡先となる担当者の名前です。このフィールドは必須です。
       - **氏名（姓）**—連絡先となる担当者の姓です。このフィールドは必須です。
       - **業務用Eメールアドレス**—連絡先となる担当者のEメールアドレスです。このフィールドは必須です。
       - **業務用電話番号** - このフィールドはオプションです。
       - **役職** - このフィールドはオプションです。
     - **[会社の連絡先]** を選択します。
       - **課金** - プラットフォームの使用状況レポートで、重要な変更に関するアップデートをお伝えするための連絡先です。
       - **技術** - プラットフォームにおける技術関連の重要な変更について、アップデートをお伝えするための連絡先です。

- **業務** - プラットフォームにおける業務関連の重要な変更について、アップデートをお伝えするための連絡先です。

注意
単一のユーザーに1件または複数の会社の連絡先を割り当てることができます。

5. **[追加]** をクリックします。

カスタムWebインターフェースの構成

注意
カスタマイズされたURLは、デフォルトのURLとは異なるIPアドレスを指します。ファイアウォールポリシーを設定する際には、この点に留意してください。

Cyber Protect CloudサービスのWebインターフェースURLを構成するには

1. 管理ポータルで **[設定]** > **[ブランディング]** をクリックします。
2. **Cyber Protect CloudサービスのURL**セクションで次の操作を実行します。
   - カスタムURLの初回設定時は **[設定]** をクリックします。
   - 既存の設定を変更する場合は **[再構成]** をクリックします。
3. **ドメイン設定**の手順で、ドメインとCNAMEレコードを準備します。
   カスタムURLを使用するには、アクティブなドメイン名と、アカウントが存在するデータセンターを指すように設定されたCNAMEレコードが必要です。CNAMEレコードの構成は、DNSレジストラによって行われ、伝搬に最大で48時間かかる場合があります。
   データセンターのドメイン名を検索し、CNAMEレコードの構成をリクエストするには、「Acronis Cyber Protect Cloud: CNAMEレコードの定義方法」の記事を参照してください。
4. **URLを確認**の手順で、カスタムURLにアクセスできること、またCNAMEレコードが正しく構成されていることを確認します。これを実行するには、メインURL名を入力し、**[確認]** をクリックします。ワイルドカードSSL証明書を使用する場合、最大10個の代替ドメイン名を追加できます。Let's Encrypt証明書を使用する場合、代替ドメイン名は無視されます。
5. **SSL証明書**の手順で、次のいずれかを実行します。
   - 「Let's Encrypt」証明書を作成する。これを実行するには、**[「Let's Encrypt」による無料のSSL証明書]**をクリックします。このオプションは、第三者機関が発行した「Let's Encrypt」証明書を使用します。サービスプロバイダーは、これら無料の証明書を使用した結果として生じるいかなる問題にも責任を負いません。
     Let's Encryptの証明書の有効期限が切れると、自動的に更新されるため、追加の操作は必要ありません。 "Let's Encrypt 証明書の自動更新"（187ページ）を参照してください。
   - ワイルドカードの証明書をアップロードする。これを実行するには、**[ワイルドカード証明書のアップロード]** をクリックし、ワイルドカード証明書と秘密キーを提供します。

注意
証明書の検証エラーが発生し、エラーメッセージが表示される場合があります:「証明書を確認できませんでした: x509: 不明な認証局によって署名された証明書」。通常、これは中間証明書が見つからないことを意味します。証明書チェーンリゾルバを使用して証明書の構造を修正し、完全な証明書チェーンをアップロードします。

6. **[送信]** をクリックして変更を適用します。

Let's Encrypt 証明書の自動更新

Let's Encrypt証明書の有効期限とアップデートのタイミングは、次のロジックを使用して管理されます。

デフォルトでは、証明書の有効期間は90日間で、有効期間の2/3で更新されます。更新間隔（`renewBefore`）と証明書のライフサイクル（`duration`）が明示的に設定されていない場合、証明書は90日間の有効期間の2/3、つまり有効期限の約30日前に更新されます。

カスタムURLをデフォルトに戻すには

1. 管理ポータルで **[設定]** > **[ブランディング]** をクリックします。
2. **Acronis Cyber Protect CloudサービスのURL**セクションで、**[デフォルトにリセット]** をクリックしてデフォルトURL（https://cloud.acronis.com）を使用するようにします。

Cyber Protectionエージェントのアップデートを構成する

重要
保護サービスが有効になっている場合、エージェントのアップデート管理機能にアクセスできます。

この手順は、以下のCyber Protectionエージェントのアップデートに適用されます。Windowsエージェント、Linuxエージェント、Macエージェント、File Sync & Share Cyber Files Cloudエージェント。

Cyber Files Cloudには、WindowsバージョンとMacOSバージョンのデスクトップFile Sync & Shareエージェントがあります。これにより、マシンとユーザーのFile Sync & Shareクラウドストレージの間でファイルやフォルダの同期を行い、オフラインワークや、WFH（在宅勤務）やBYOD（Bring Your Own Device）のワークスタイルを促進することができます。

複数のワークロードを簡単に管理できるよう、すべてのマシンまたは個別マシンの全エージェントに対して、手動または自動の無人アップデートを構成できます。

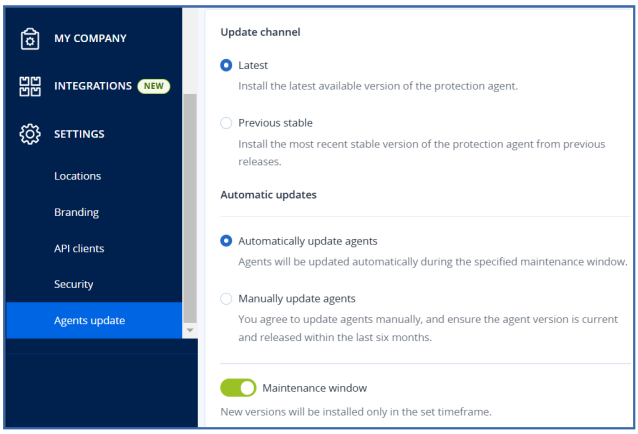
注意
個別マシン上のエージェントを管理し、Cyber Protectコンソールから自動アップデート設定をカスタマイズするには、Cyber Protectユーザーガイドでエージェントのアップデートのセクションを参照してください。

自動更新

注意
プロテクションサービスが有効になっていないパートナーおよびカスタマーは、サービスプロバイダーからFile Sync & Shareエージェントの自動アップデートの設定を継承します。

管理ポータルでエージェントの自動アップデートのデフォルト設定を構成するには

1. **[設定]** > **[エージェントのアップデート]** の順に選択します。



2. **[チャネルをアップデート]** で、自動アップデートに使用するバージョンを選択します。

オプション	説明
最新（デフォルト選択）	公開されている最新なバージョンのCyber Protectionエージェントをインストールします。
以前の安定版	Cyber Protectionエージェントの以前のリリースでの最新の安定版をインストールします。

3. **エージェントの自動アップデート]** オプションがオンになっていることを確認します。

注意
自動アップデートは、次のエージェントでのみ利用できます。
- Cyber Protectエージェント、バージョン26986（2021年5月リリース）以降。
- File Sync & Shareデスクトップエージェント、バージョン15.0.30370以降。

以前のエージェントは、自動アップデートを有効にする前に、まず手動で最新バージョンにアップデートする必要があります。

4. （オプション） メンテナンス期間を設定します。
デフォルトの期間は、エージェントがインストールされているマシンの時間で、毎日23:00から08:00までの間です。

注意
エージェントのアップデートは高速かつシームレスに実行されますが、ユーザー側で自動アップデートを拒否したり延期したりすることはできないため、ユーザーへの影響が最小限に抑えられる時間帯を選択することをお勧めします。

5. **[保存]** をクリックします。

手動アップデート

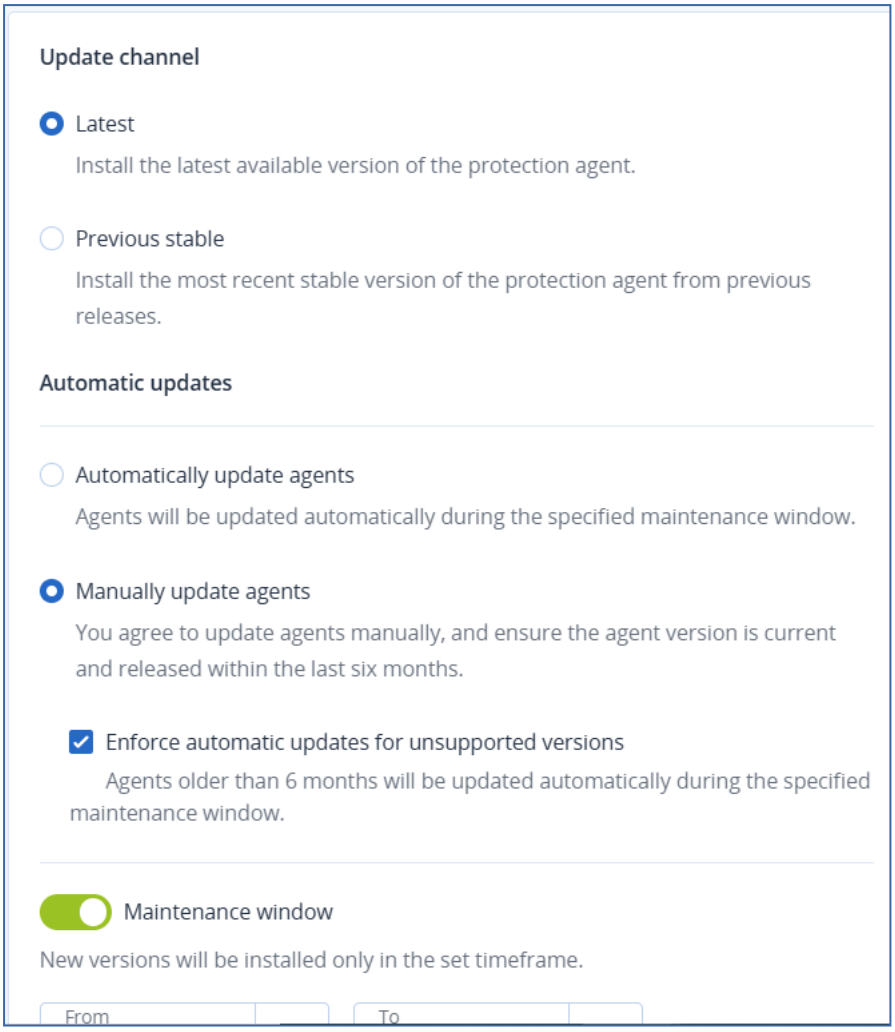
重要
エージェントの自動アップデートを有効にしておくことを強くお勧めします。定期的なアップデートにより、エージェントを最新の状態に保ち、パフォーマンスを向上させ、バグを修正し、保護およびセキュリティ機能を強化できます。

管理ポータルでエージェントの手動アップデートのデフォルト設定を構成するには

1. **設定** > **エージェントのアップデート** に移動します。
2. **[チャネルをアップデート]** で、自動アップデートに使用するバージョンを選択します。

オプション	説明
最新（デフォルト選択）	公開されている最新なバージョンのCyber Protectionエージェントをインストールします。
以前の安定版	Cyber Protectionエージェントの以前のリリースでの最新の安定版をインストールします。

3. **[エージェントの手動アップデート]** を選択します。



4. （オプション） セキュリティリスクを防ぎ、最新の機能へのアクセスを確保し、6か月以上前のエージェントによって引き起こされる技術的な問題を最小限に抑えるために、6か月以上前のエージェントの自動アップデートを有効にします。
   a. **[サポートされていないバージョンの自動アップデートを強制的に実行する]** を選択します。

      重要
      C25.02リリースでエージェントの自動アップデートを有効にしていない場合、このオプションは環境内のすべてのテナントに対して自動的に有効になります。

   b. （オプション） メンテナンス期間を設定します。
      デフォルトのメンテナンス期間は、エージェントがインストールされているマシンの時間で、毎日23:00から08:00までの間です。

      注意
      エージェントのアップデートは高速かつシームレスに実行されますが、ユーザー側で自動アップデートを拒否したり延期したりすることはできないため、ユーザーへの影響が最小限に抑えられる時間帯を選択することをお勧めします。

5. **[保存]** をクリックします。

エージェントのアップデートの監視

重要
エージェントアップデートの監視は、プロテクションモジュールを有効化しているパートナーおよびカスタマーの管理者のみが実行できます。

エージェントのアップデートを監視するには、Cyber Protectユーザーガイドのアラートおよびアクティビティの各セクションを参照してください。

監視

サービスの使用状況や操作に関する情報にアクセスするには、**[監視]** をクリックします。

使用状況

[使用状況] タブには、サービスの使用状況の概要が表示され、操作中のテナント内のサービスにアクセスすることができます。

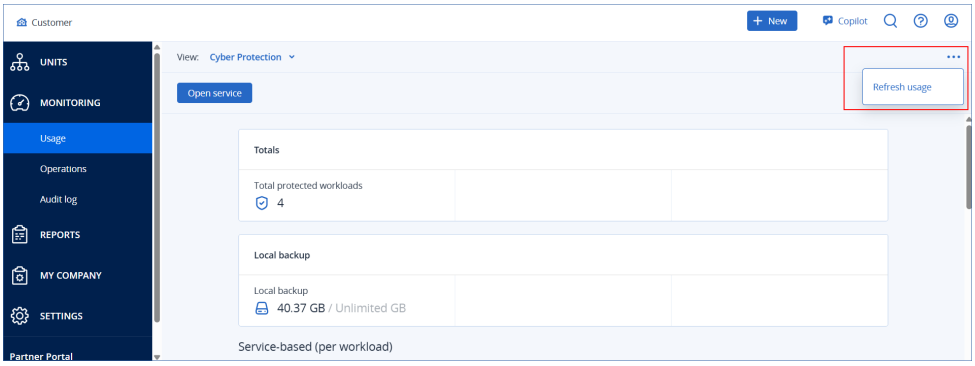
使用状況データには、標準機能と高度な機能の両方が含まれています。

重要
製品のUIに表示されるストレージ使用量の値は、バイナリバイト単位（メビバイト（MiB）、ギビバイト（GiB）、テビバイト（TiB））ですが、ラベルにはそれぞれMB、GB、TBが表示されます。たとえば、実際の使用量が3105886629888バイトの場合、UIに表示される値は2.82と正しく表示されますが、ラベルはTiBではなくTBになります。

Microsoft 365およびGoogle Workspaceワークロードのストレージ使用状況は、一般的なバックアップストレージとは別にレポートされ、**[Microsoft 365およびGoogle Workspaceのバックアップ]** セクションに表示されます。

タブに表示されている使用状況データをリフレッシュするには、画面の右上にある省略記号アイコン（...）をクリックして、**[使用状況をリフレッシュ]** を選択します。

注意
データの取得には最大で10分かかります。ページをリロードして、アップデートされたデータを表示します。



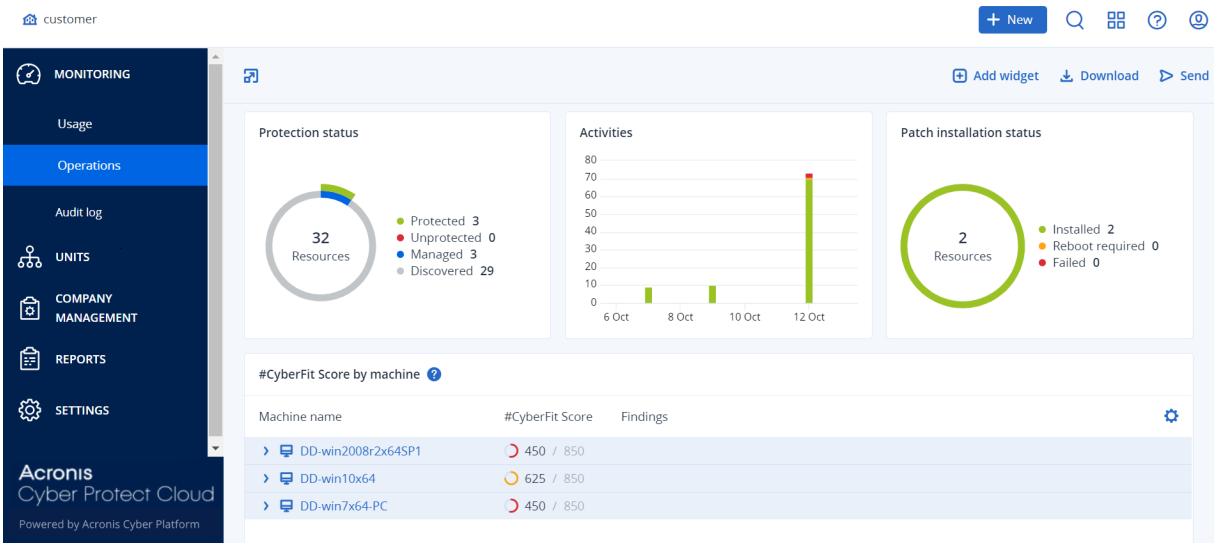
処理

[操作] ダッシュボードには、Cyber Protectionサービスに関連する操作の概要を示すカスタマイズ可能なウィジェットが多数用意されています。他のサービスのウィジェットは、将来のリリースで利用可能になります。

デフォルトでは、データは操作しているテナントに表示されます。表示されたテナントは、ウィジェットごとに個別に編集して変更することができます。選択したテナントの直接子顧客テナントに関する集約情報も表示されます（フォルダ内にあるテナントを含みます）。ダッシュボードでは、子パートナーとその子テナントに関する情報を表示しません。ダッシュボードを表示するには特定のパートナーにドリルダウンする必要があります。ただし、子パートナーのテナントをフォルダテナントに変更すると、このテナントの子顧客に関する情報が親テナントのダッシュボードに表示されます。

ウィジェットは、2 分間隔でアップデートされます。ウィジェットには、クリックすることによって、問題を調査し、トラブルシューティングを実行できる要素が含まれています。ダッシュボードの現在の状態は、.pdf または/および .xlsx 形式でダウンロードできる他、外部の受信者を含む任意のアドレスに電子メールで送信するようにも設定できます。

表、円グラフ、棒グラフ、一覧表、ツリー図として表示されるさまざまなウィジェットから選択できます。異なるテナントに異なるフィルタを使用して、同じタイプのウィジェットを複数追加することができます。



ダッシュボード上のウィジェットを再配置します

名前をクリックしてウィジェットをドラッグアンドドロップします。

ウィジェットを編集します

ウィジェット名の横にある鉛筆アイコンをクリックします。ウィジェットを編集すると、名前を変更したり、時間範囲を変更したり、データが表示されるテナントを選択したり、フィルタを設定することができます。

ウィジェットを追加します

[ウィジェットの追加] をクリックし、次のいずれかの操作を行います。

- 追加するウィジェットをクリックします。ウィジェットはデフォルト設定に追加されます。
- ウィジェットを追加する前に編集するには、ウィジェットが選択されているときにギアアイコンをクリックします。ウィジェットを編集したら、[**完了**] をクリックします。

ウィジェットを削除します

ウィジェット名の横にある X 記号をクリックします。

保護ステータス

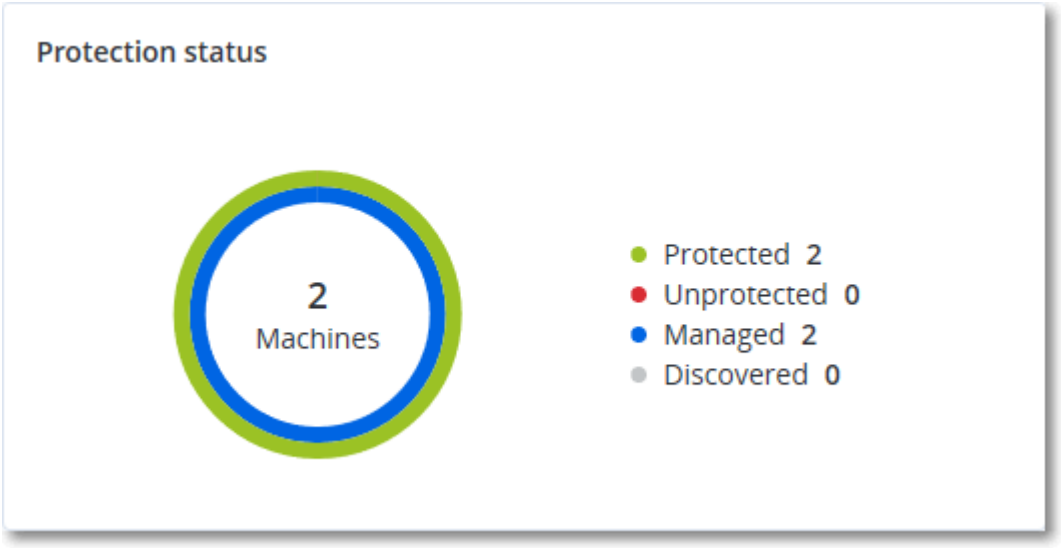
保護ステータス

このウィジェットはすべてのマシンについて現在の保護ステータスを表示します。

マシンは次のいずれかのステータスになります。

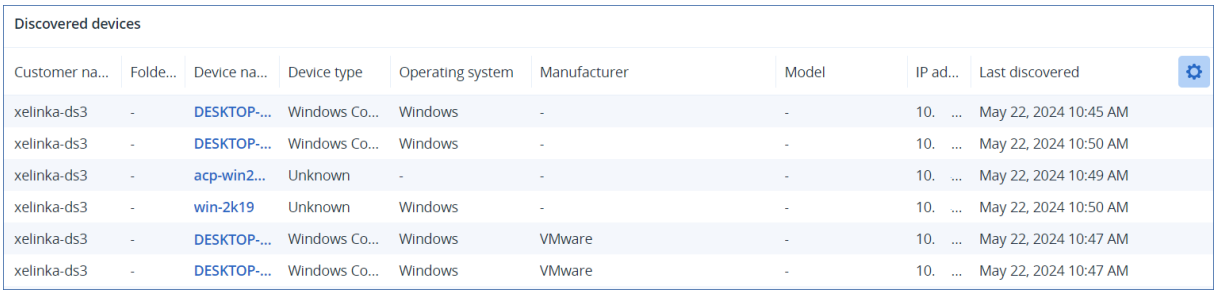
- **保護対象** - 保護計画が適用されているマシン。
- **保護対象外** - 保護計画が適用されていないマシン。これらには、保護計画が適用されていない検出済みマシンと管理対象のマシンの両方が含まれます。
- **管理対象** - プロテクションエージェントをインストール済みのマシン。
- **検出済み** - プロテクションエージェントを未インストールのマシン。

マシンのステータスをクリックすると、ステータスの詳細情報を含むマシンのリストにリダイレクトされます。



検出されたデバイス

このウィジェットには、カスタマーのネットワークで検出されたデバイスに関する詳細情報が表示されます。情報には、デバイスの種類、製造元、オペレーティングシステム、IPアドレス、MACアドレス、検出日などが含まれます。


Discovered devices

Customer na...	Folde...	Device na...	Device type	Operating system	Manufacturer	Model	IP ad...	Last discovered
xelinka-ds3	-	DESKTOP-...	Windows Co...	Windows	-	-	10. ...	May 22, 2024 10:45 AM
xelinka-ds3	-	DESKTOP-...	Windows Co...	Windows	-	-	10. ...	May 22, 2024 10:50 AM
xelinka-ds3	-	acp-win2...	Unknown	-	-	-	10. ...	May 22, 2024 10:49 AM
xelinka-ds3	-	win-2k19	Unknown	Windows	-	-	10. ...	May 22, 2024 10:50 AM
xelinka-ds3	-	DESKTOP-...	Windows Co...	Windows	VMware	-	10. ...	May 22, 2024 10:47 AM
xelinka-ds3	-	DESKTOP-...	Windows Co...	Windows	VMware	-	10. ...	May 22, 2024 10:47 AM

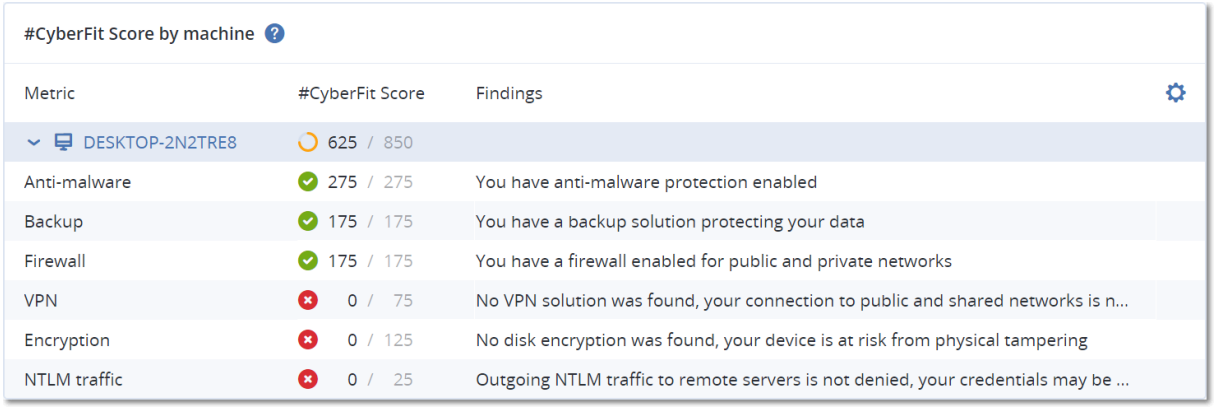
マシンごとの #CyberFit スコア

このウィジェットは、各マシンの合計#CyberFitスコア、その複合スコア、および次の各メトリクスに関する評価結果を示します。

- マルウェア対策
- バックアップ
- ファイアウォール
- VPN
- 暗号化
- NTLMトラフィック

各メトリクスのスコアを改善するには、レポートに記載された推奨事項を確認します。

#CyberFitスコアの詳細については、「マシンの#CyberFitスコア」を参照してください。


#CyberFit Score by machine

Metric	#CyberFit Score	Findings
DESKTOP-2N2TRE8	625 / 850	
Anti-malware	275 / 275	You have anti-malware protection enabled
Backup	175 / 175	You have a backup solution protecting your data
Firewall	175 / 175	You have a firewall enabled for public and private networks
VPN	0 / 75	No VPN solution was found, your connection to public and shared networks is n...
Encryption	0 / 125	No disk encryption was found, your device is at risk from physical tampering
NTLM traffic	0 / 25	Outgoing NTLM traffic to remote servers is not denied, your credentials may be ...

Endpoint Detection and Response（EDR）ウィジェット

Endpoint Detection and Response（EDR）には多くのウィジェットが含まれており、これらは**操作**ダッシュボードからアクセスできます。

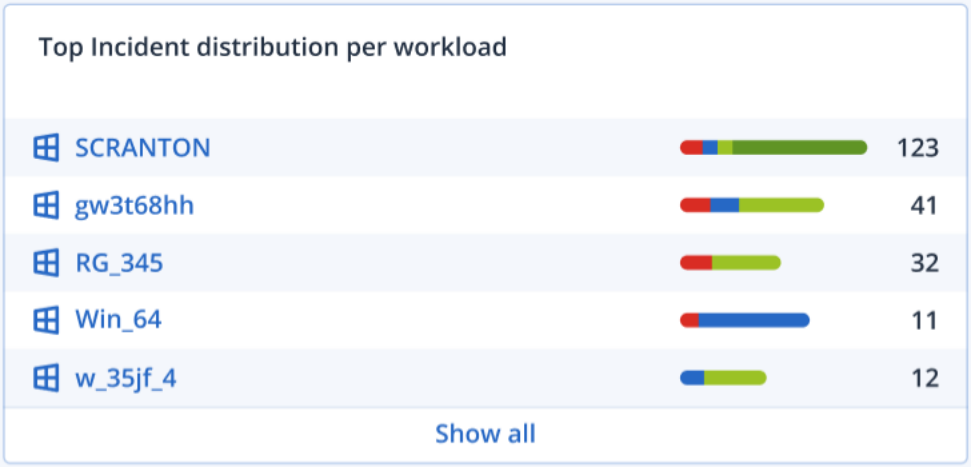
次のウィジェットが利用可能です。

- ワークロードごとの上位インシデントディストリビューション
- インシデントMTTR
- セキュリティインシデントのバーンダウン
- ワークロードのネットワークステータス

ワークロードごとの上位インシデントディストリビューション

このウィジェットには、インシデントの数が多い、上位5つのワークロードが表示されます（[**すべて表示**] をクリックすると、ウィジェットの設定に応じてフィルタリングされたインシデントのリストにリダイレクトされます）。

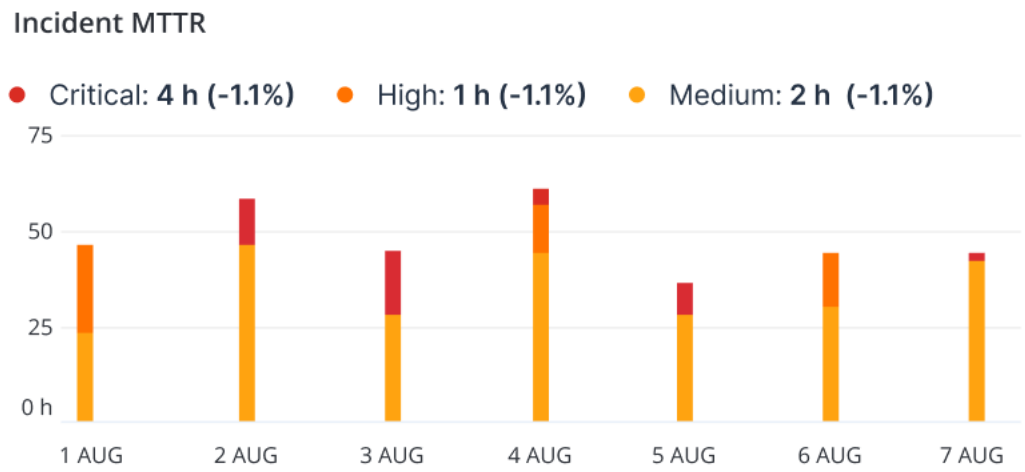
ワークロード行にホバーすると、インシデントに関する現在の調査ステータスの内訳が表示されます。調査ステータスは、**開始前**、**調査中**、**閉鎖済み**、**偽陽性**の順に表示されます。続いて、詳細に分析したいワークロードをクリックし、表示されたポップアップで関連するカスタマーを選択すると、ウィジェットの設定に応じてインシデントのリストがリフレッシュされます。



インシデントMTTR

このウィジェットでは、セキュリティインシデントの平均解決時間を表示します。これは、インシデントの調査や解決のスピードを示しています。

列をクリックすると、重要度（**重大**、**高**、**中**）別のインシデントの内訳と、重要度レベル別の解決に要した時間が表示されます。括弧内の%数値により、前期比での増減が表わされます。

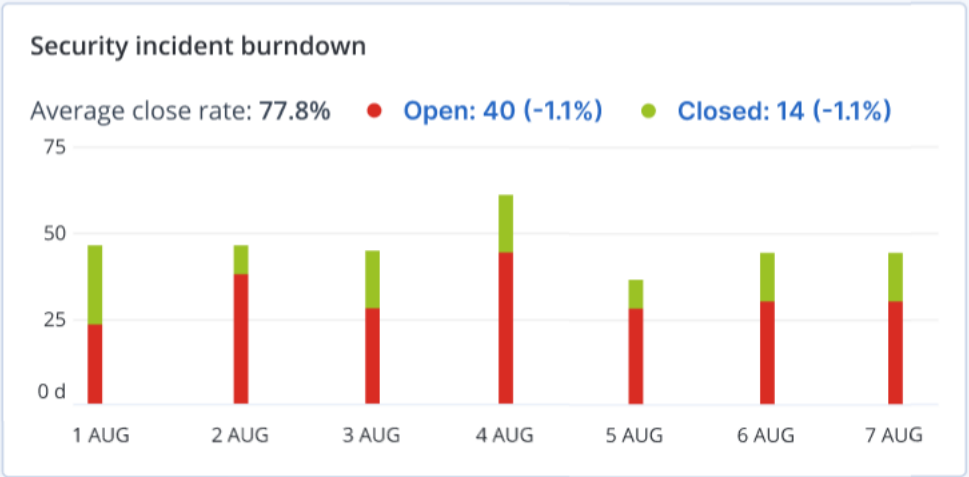


セキュリティインシデントのバーンダウン

このウィジェットでは、インシデントがクローズ状態になるまでの効率性が表示されます。この効率性は、オープン状態のインシデントの数と、一定期間内にクローズされたインシデントの数の比較により表わされます。

列をホバーすると、選択した日付におけるクローズ状態およびオープン状態のインシデントの内訳が表示されます。[オープン] の値をクリックするとポップアップが表示され、関連するテナントを選択できます。選択したテナントについて、現在オープンな状態のインシデント（**調査中**または**開始前**のステータス）を表示するフィルターが適用されたインシデントリストが表示されます。[クローズ] の値をクリックすると選択したテナントについて、現在オープンな状態ではないインシデント（**閉鎖済み**または**偽陽性**のステータス）を表示するフィルターが適用されたインシデントリストが表示されます。

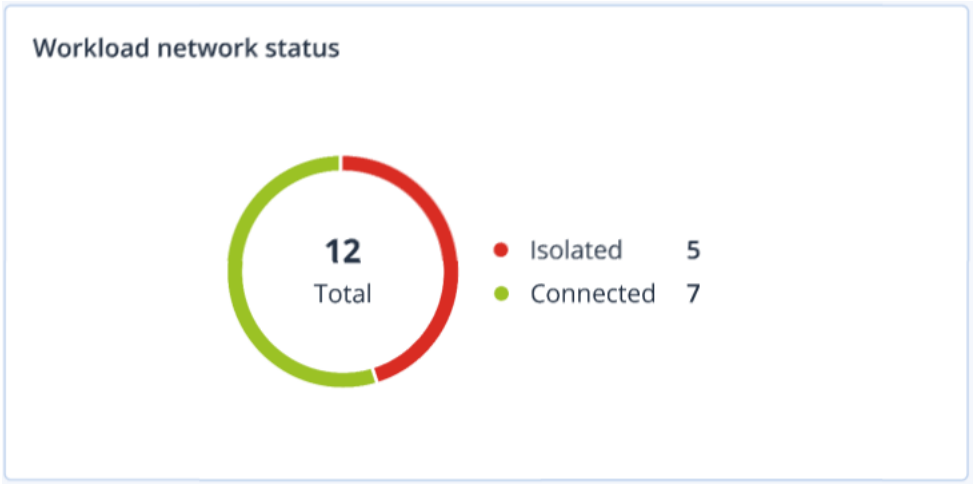
括弧内の%数値により、前期比での増減が表わされます。



ワークロードのネットワークステータス

このウィジェットでは、ワークロードの現在のネットワーク状態が表示され、分離されているワークロードの数と接続済みのワークロードの数が示されます。

[分離] の値をクリックすると、ポップアップが表示されるので、関連するテナントを選択します。表示されるワークロードビューではフィルターが適用され、分離されたワークロードが表示されます。[接続済み] の値をクリックすると、接続済みのワークロード（選択したテナントの）を表示するフィルターが適用されたエージェントリストとワークロードが表示されます。



ディスク状態監視

ディスク状態の監視は、現在のディスク状態のステータスに関する情報と予測情報を提供し、ディスク障害に関連して発生する可能性のあるデータ損失を防ぐことができます。HDDおよびSSDディスクがサポートされています。

制限事項

- ディスク状態の予測はWindowsを実行するマシンのみをサポートします。
- 物理マシンのディスクのみを監視します。仮想マシンのディスクは監視対象ではなく、ディスク状態ウィジェットに表示されません。
- RAID構成はサポートされていません。ディスク状態ウィジェットには、RAIDが実装されたマシンに関する情報は含まれていません。
- NVMe SSDはサポートされていません。
- 外付けストレージデバイスはサポートされていません。

ディスク状態は、次のいずれかのステータスで示されます。

- **OK**
  ディスク状態が70～100%です。
- **警告**
  ディスク状態が30～70%です。
- **重大**
  ディスク状態が0～30%です。
- **ディスクデータの計算中**
  現在のディスク状態と予測を計算中です。

仕組み

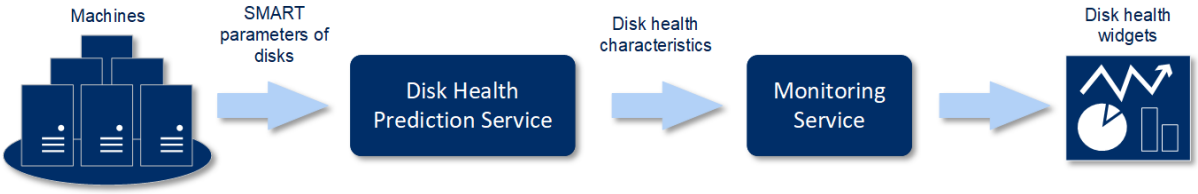
ディスク状態予測サービスは、AI ベースの予測モデルです。

1. プロテクションエージェントがディスクのSMARTパラメータを収集して、このデータをディスク状態予測サービスに渡します。

- SMART 5 - リアロケートされたセクタの数です。
- SMART 9 - 通電時間です。
- SMART 187 - 報告された未修正エラーです。
- SMART 188 - コマンドタイムアウトです。
- SMART 197 - 現在保留されているセクタの数です。
- SMART 198 - オフラインの未修正セクタの数です。
- SMART 200 - 書き込みエラー発生率です。

2. ディスク状態予測サービスは、受信したSMARTパラメータを処理して予測を実行し、次のようにディスク状態の特性を提供します:
   - ディスク状態の現在のステータス:OK、警告、重大。
   - ディスク状態の予測: 陰性、安定、陽性。
   - ディスク状態の予測は百分率で示されます。

   予測期間は1か月間です。
3. 監視サービスはこれらの特性情報を受信し、Cyber Protectコンソールのディスク状態ウィジェットに関連情報を表示します。



ディスク状態ウィジェット

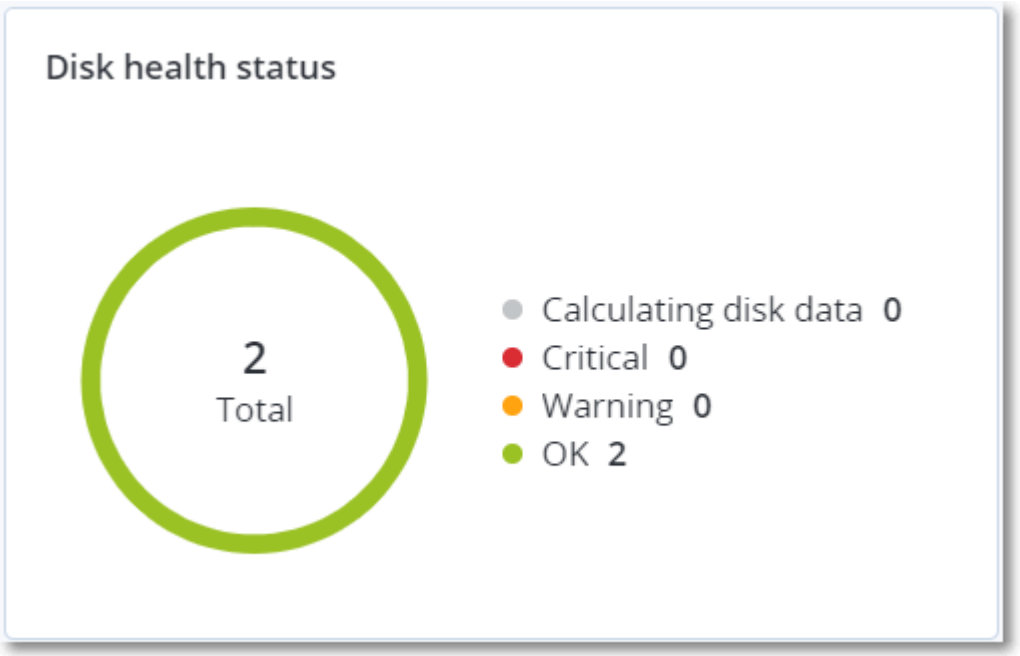
ディスク状態の監視結果は、Cyber Protectコンソールで利用できる以下のウィジェットに表示されます。

- **ディスク状態の概要**は、階層の詳細情報を含むツリー図ウィジェットです。階層は、ツリーをたどるようにして切り替えることができます。
  - マシンレベル
    選択したカスタマーのマシンに関する、ディスク状態ステータスの要約情報を表示します。最も重大なディスクステータスのみが表示されます。他のステータスは、該当するブロックにマウスを移動（ホバー）することでツールの先端に表示されます。マシンのブロックサイズは、該当するマシンの全ディスクの合計サイズによって異なります。マシンのブロックの色は、見つかったもっとも重大なディスクステータスによって異なります。

- ディスクレベル
  選択済みのマシンに現在搭載されている全ディスクのディスク状態ステータスを表示します。各ディスクブロックには、以下のいずれかのディスク状態予測とその確率がパーセンテージで表示されます。
  - 低下傾向
  - 安定傾向

- 改善傾向

- **ディスク状態ステータス**は、円グラフウィジェットで各ステータス別にディスクの数を示します。



ディスク状態アラート

30分間隔でディスク状態のチェックが実行されるとともに、対応するアラートが1日に1回生成されます。ディスク状態が**警告**から**重大**に変化する場合、必ずアラートが生成されます。

アラート名	重大度	ディスク状態ステータス	説明
ディスク障害が生じる可能性があります	警告	(30 – 70)	このマシン上の<disk name>ディスクは、今後故障する可能性があります。できるだけ早くこのディスクのフルイメージバックアップを実行し、新しいディスクに交換してからイメージをリカバリしてください。
ディスク障害が差し迫っています	重大	(0 – 30)	このマシンの<disk name>ディスクは、故障が差し迫った重大な状態にあります。ストレスが加わるとディスクが故障する可能性があるため、現時点ではこのディスクのイメージバックアップは推奨できません。今すぐこのディスクの最も重要なファイルをすべてバックアップして、交換してください。

データ保護マップ

データ保護マップ機能により、重要なすべてのデータを確認できます。また拡大縮小できるツリー形式のビューで、すべての重要なファイルについて数量、サイズ、ロケーション、保護ステータスの詳細を確認できます。

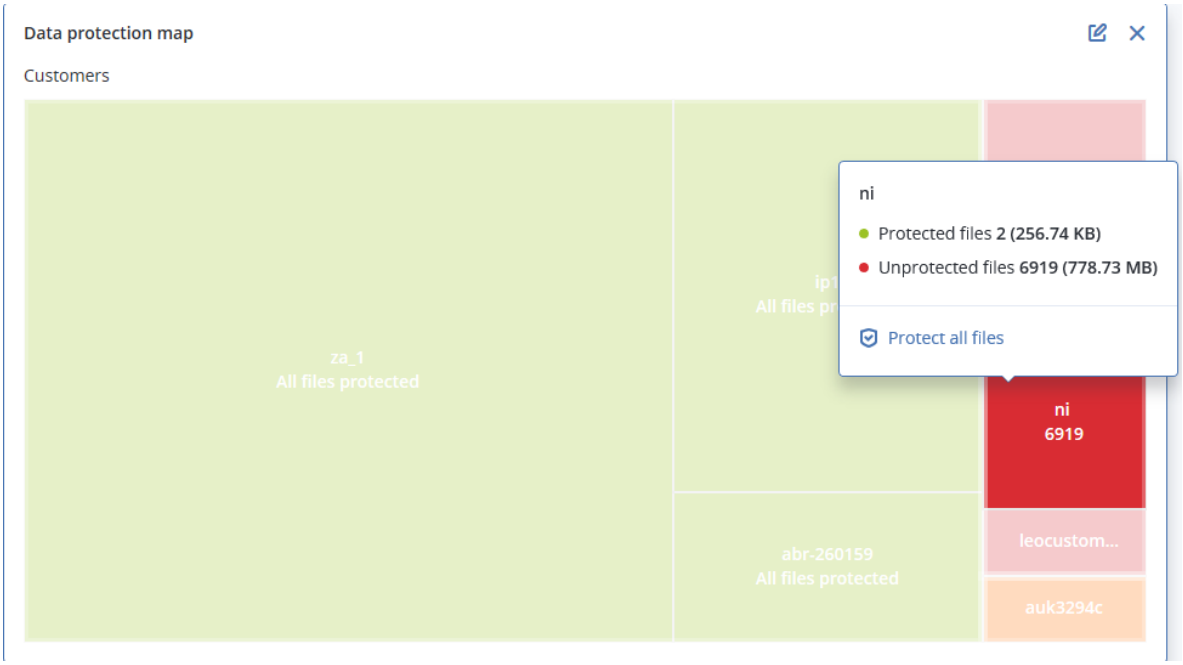
各ブロックのサイズは、カスタマー/マシンに属する重要なすべてのファイルの合計数/サイズによって異なります。

ファイルは次のいずれかの保護ステータスになります。

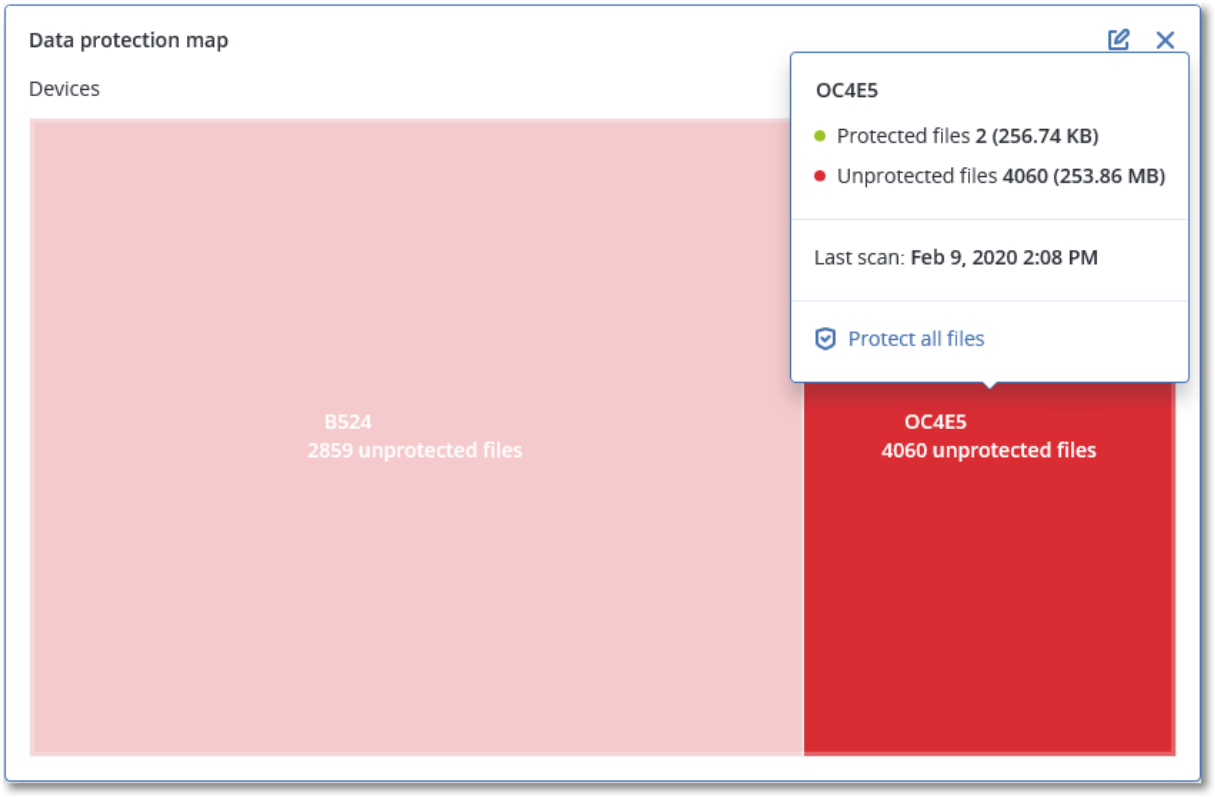
- **重大** - 選択済みカスタマーのテナント/マシン/ロケーションで、バックアップ対象に指定されていない拡張子を持つ保護非対象のファイルが、51～100%存在します。
- **低** - 選択済みカスタマーのテナント/マシン/ロケーションで、バックアップ対象に指定されていない拡張子を持つ保護非対象のファイルが、21～50%存在します。
- **中** - 選択済みカスタマーのテナント/マシン/ロケーションで、バックアップ対象に指定されていない拡張子を持つ保護非対象のファイルが、1～20%存在します。
- **高** - 選択済みカスタマーのテナント/マシン/ロケーションで、すべてのファイルが保護（バックアップ）対象に指定された拡張子を有しています。

データ保護確認の結果は、データ保護マップウィジェットのダッシュボードで確認できます。これは2階層のツリー図ウィジェットで、ツリーをたどるようにして表示を切り替えることができます。

- カスタマーテナントレベル - 選択済みのカスタマーごとに重要なファイルの保護ステータスに関する要約情報を表示します。



- マシンレベル - 選択済みのカスタマーのマシンごとに重要なファイルの保護ステータスに関する情報を表示します。



保護されていないファイルを保護するには、ブロックにマウスを移動（ホバー）して、**[すべてのファイルを保護]** をクリックします。ダイアログウィンドウで、保護されていないファイルの数とそのロケーションについての情報を見つけることができます。それらを保護するには、**[すべてのファイルを保護]** をクリックします。

CSV形式で詳細レポートをダウンロードすることもできます。

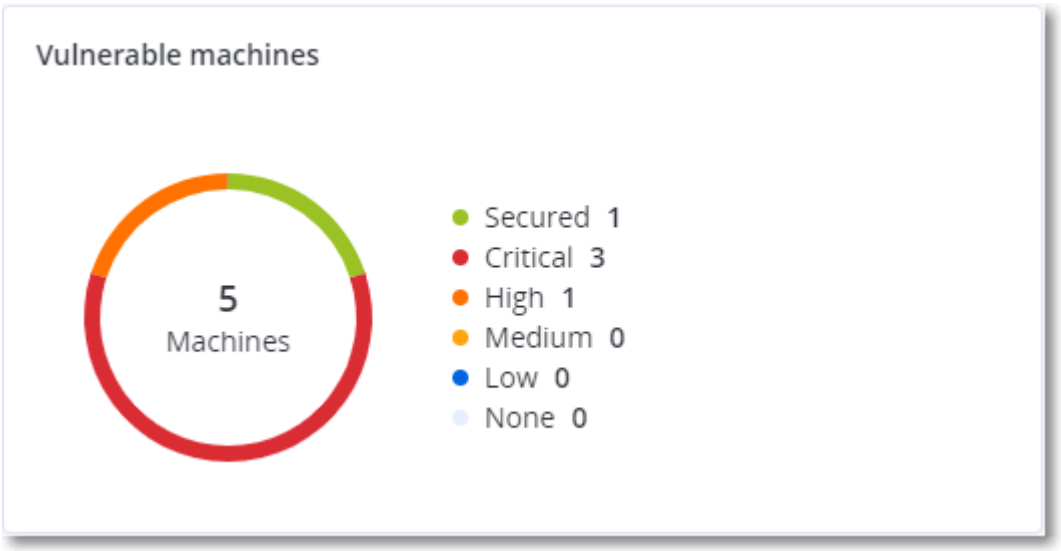
脆弱性診断ウィジェット

脆弱性のあるマシン

このウィジェットは脆弱性の重大度別に脆弱なマシンを表示します。

見つかった脆弱性は、共通脆弱性評価システム（CVSS）v3.0に従って、次の重大度レベルのいずれかで示されます。

- セキュア: 脆弱性が見つからない
- 重大:9.0 - 10.0 CVSS
- 高:7.0 - 8.9 CVSS
- 中:4.0 - 6.9 CVSS
- 低:0.1 - 3.9 CVSS
- なし:0.0 CVSS



既存の脆弱性

このウィジェットは、マシンに現時点で存在する脆弱性を表示します。**[既存の脆弱性]** ウィジェットには、タイムスタンプが表示される2つの列があります。

- **最初の検出** - マシンで最初に脆弱性が検出された日時。
- **最後の検出** - マシンで最後に脆弱性が検出された日時。

Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

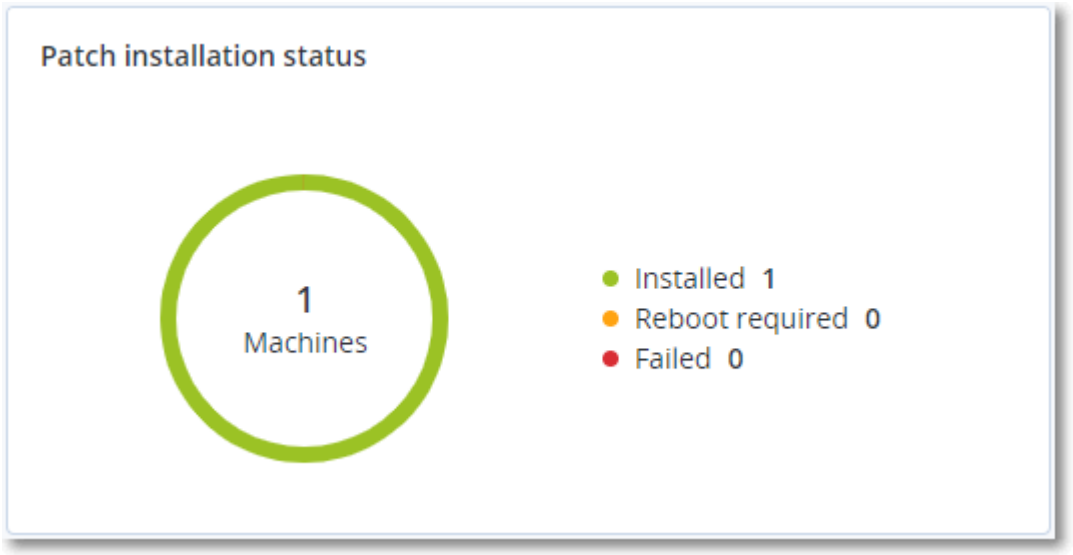
パッチインストールウィジェット

パッチの管理機能に関連する4種類のウィジェットがあります。

パッチインストールステータス

このウィジェットは、パッチインストールステータスでグループ化したマシンの数を表示します。

- **インストール済み** - 利用可能なすべてのパッチがマシンにインストール済み
- **再起動が必要** - パッチのインストール後にマシンの再起動が必要
- **失敗** - マシンでパッチインストールが失敗



パッチインストール概要

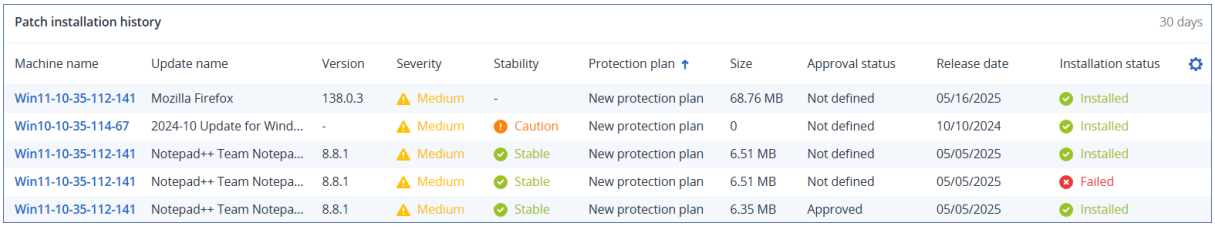
このウィジェットは、パッチインストールステータスによるマシンのパッチの概要を表示します。

Patch installation summary

Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
Installed	1	2	1	1	2	0	0

パッチインストール履歴

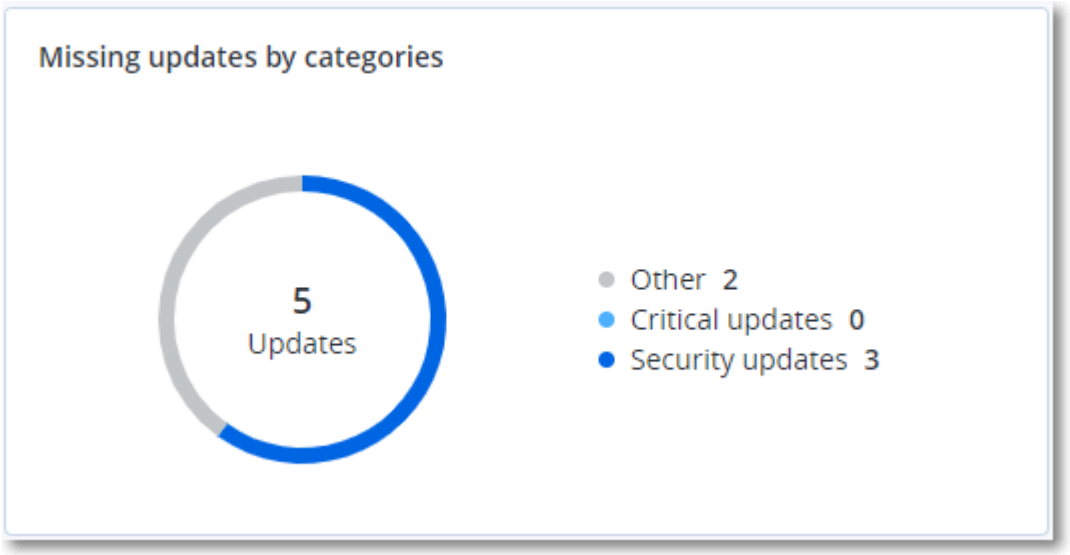
このウィジェットは、マシンのパッチに関する詳細を表示します。



カテゴリ別の未適用アップデート

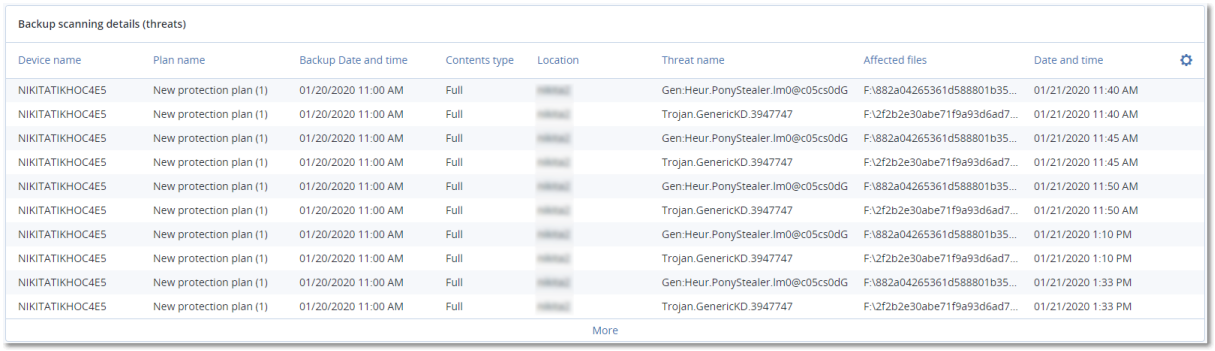
このウィジェットは、見つからないアップデートの数をカテゴリ別に表示します。次のカテゴリで表示されます。

- セキュリティアップデート
- 重要なアップデート
- その他



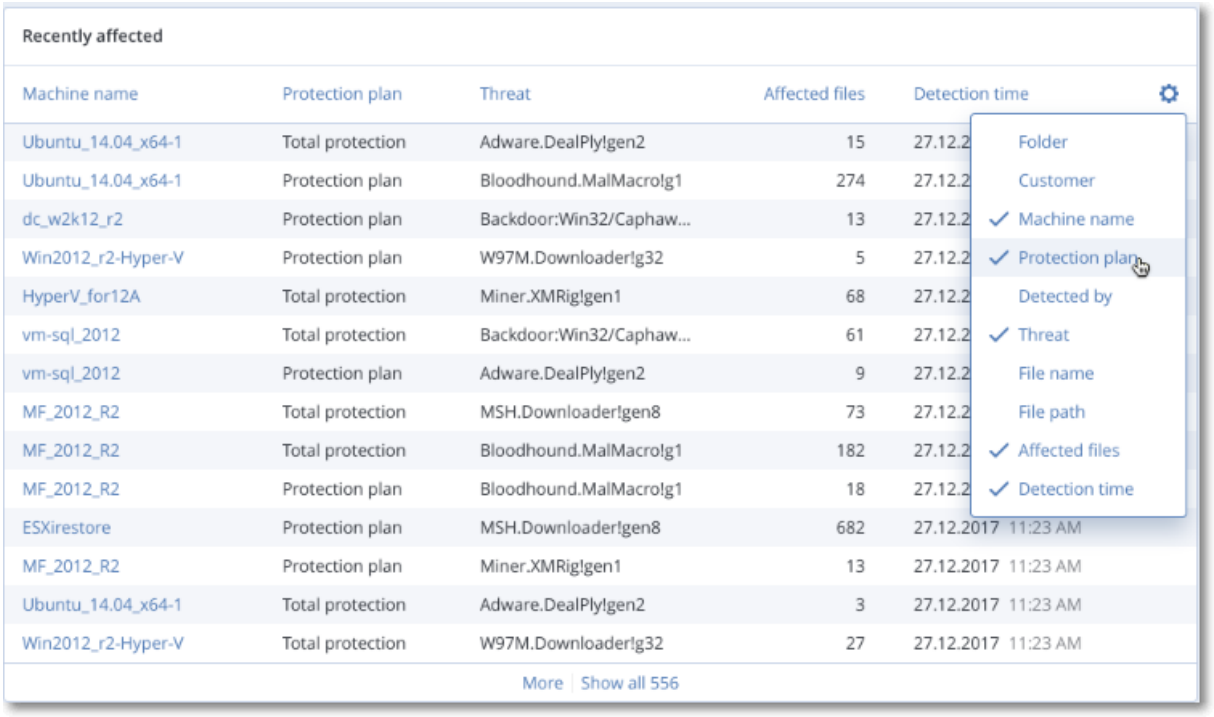
バックアップスキャンの詳細

このウィジェットは、バックアップで検出された脅威に関する詳細を表示します。



最近影響を受けたもの

このウィジェットには、ウイルス、マルウェア、ランサムウェアなどの脅威の影響にさらされているワークロードの詳細情報が表示されます。検出された脅威の情報、脅威が検出された時間、影響を受けたファイルの数などを確認できます。



最近影響を受けたワークロードのデータをダウンロードする

最近影響を受けたワークロードのデータをダウンロードし、CSVファイルを生成して、指定した受信者に送信できます。

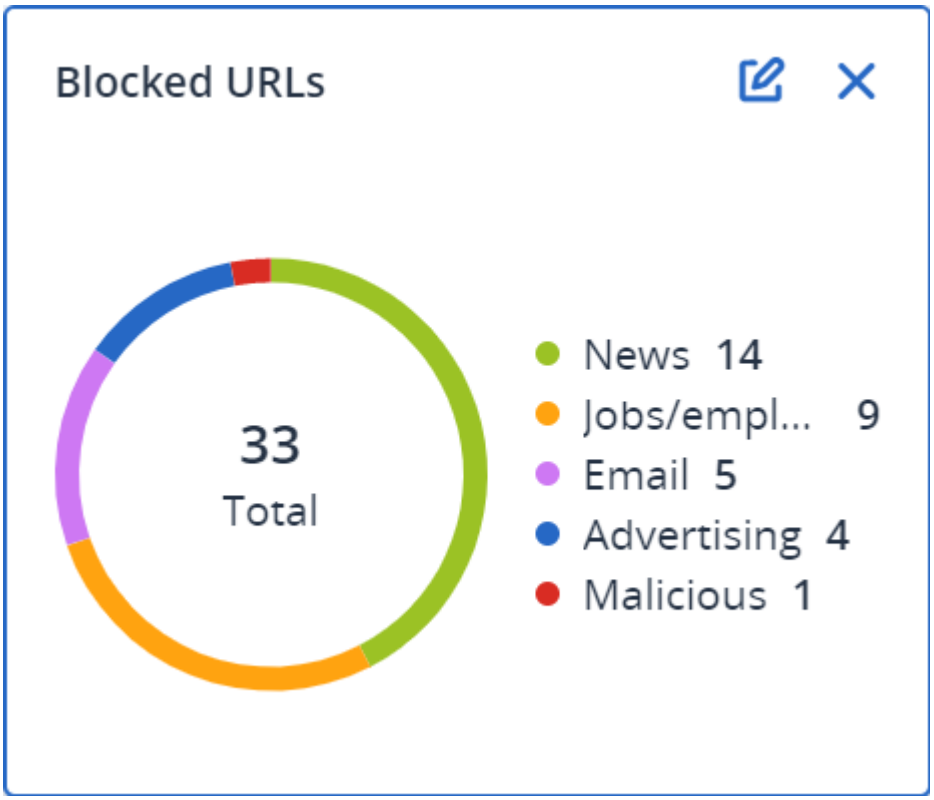
最近影響を受けたワークロードのデータをダウンロードするには

1. **[最近影響を受けたもの]** ウィジェットで、**[データをダウンロード]** をクリックします。
2. **[対象期間]** フィールドに、データをダウンロードする日数を入力します。入力可能な最大日数は200日です。
3. **[受信者]** フィールドに、すべての受信者のEメールアドレスを入力します。Eメールには、CSVファイルをダウンロードするためのリンクが記載されます。
4. **[ダウンロード]** をクリックします。

   システムにより、指定した期間に影響を受けたワークロードのデータを含む、CSVファイルの作成が開始されます。CSVファイルの作成が完了すると、システムにより受信者にEメールが送信されます。各受信者はその後、CSVファイルをダウンロードできるようになります。

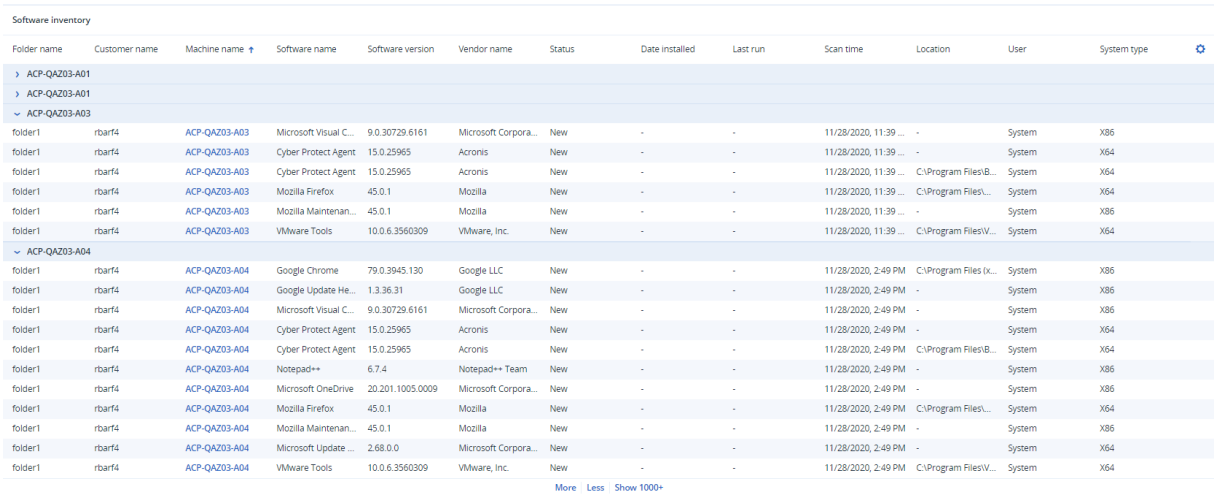
ブロックされたURL

ウィジェットには、ブロックされたURLの統計がカテゴリごとに表示されます。URLフィルタリングとカテゴリの詳細については、『サイバープロテクションユーザーガイド』を参照してください。



ソフトウェアインベントリウィジェット

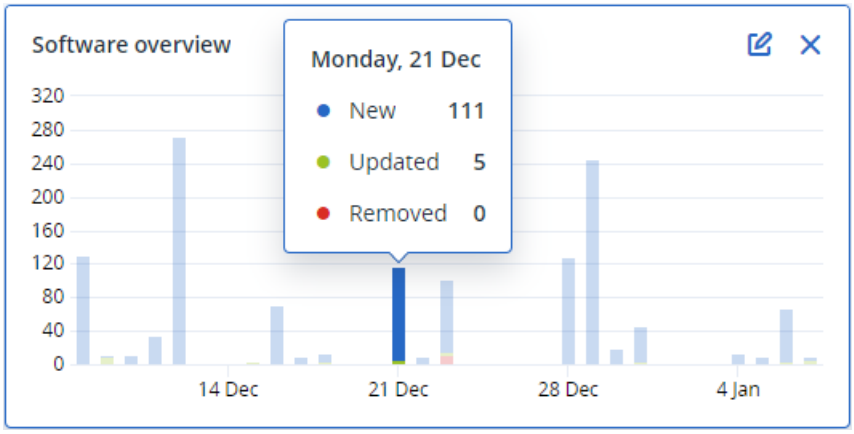
ソフトウェアインベントリテーブルウィジェットには、クライアントの組織内のWindowsおよびmacOSデバイスにインストールされている、すべてのソフトウェアに関する詳細情報が表示されます。



ウィジェット内の情報は、マシン名、ソフトウェア名、ベンダー名、ステータスでフィルタリングできます。

注意
マシン名、**ソフトウェア名**、**ベンダー名**フィルタでは、最大20個の値を選択できます。

ソフトウェアの概要ウィジェットには、指定した期間（7日、30日、または当月）にクライアントの組織内のWindowsおよびmacOSデバイスで新規導入、アップデート、および削除されたアプリケーションの数が表示されます。



チャートの特定のバーにホバーすると、次の情報を含むツールチップが表示されます。

新規 - 新しくインストールされたアプリケーションの数です。

アップデート済み - アップデートされたアプリケーションの数です。

削除済み -削除されたアプリケーションの数です。

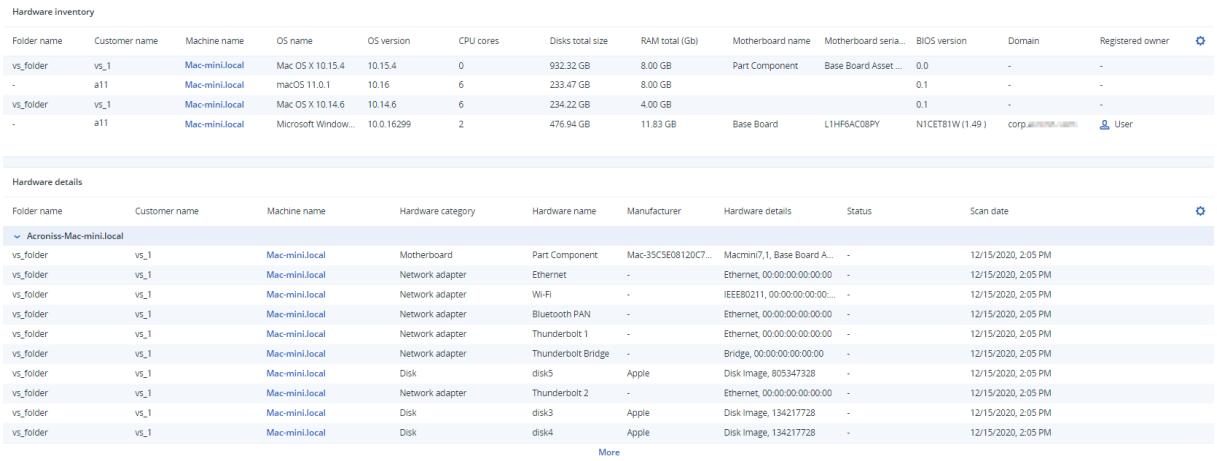
バーの特定のステータスに対応する部分をクリックすると、ポップアップウィンドウが読み込まれます。選択した日付およびステータスのアプリケーションを含むデバイスを所有している、すべてのカスタマーが一覧表示されます。リストからカスタマーを選択して、**[カスタマーへ移動]** をクリックすると、カスタマーのCyber Protectコンソールの、**[ソフトウェア管理]** -> **[ソフトウェアインベントリ]** ページにリダイレクトされます。ページ内の情報は、対応する日付とステータスでフィルタリングされます。

デバイス名でウィジェット内の情報をフィルタリングできます。

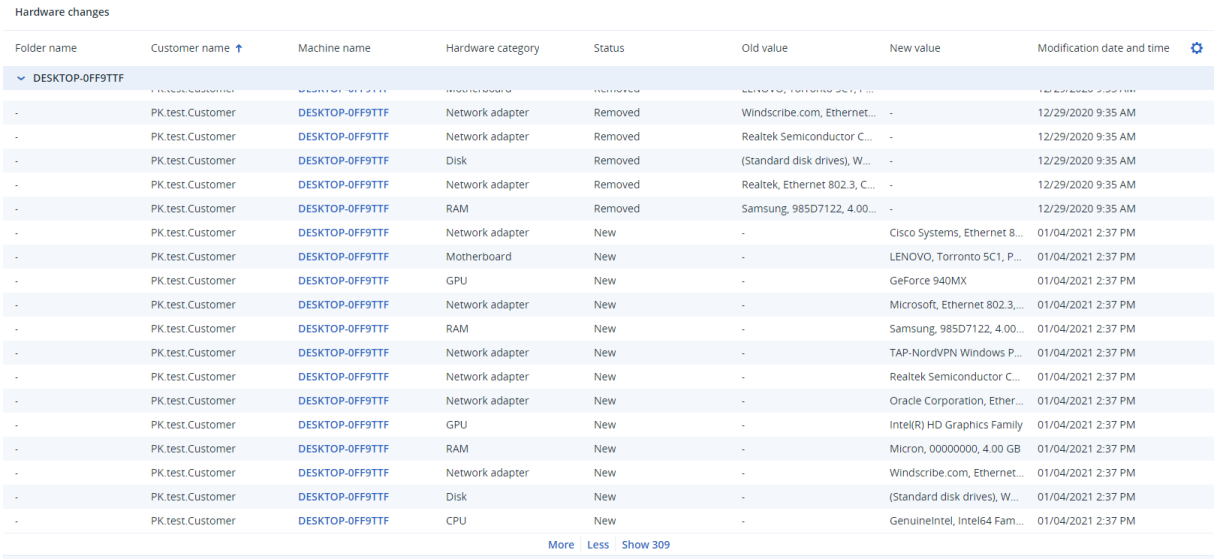
注意
デバイス名フィルタでは、最大20個の値を選択できます。

ハードウェアインベントリウィジェット

ハードウェアインベントリおよび**ハードウェアの詳細**テーブルウィジェットには、クライアントの組織内の物理的および仮想的なWindowsまたはmacOSデバイスにインストールされているすべてのハードウェアに関する情報が表示されます。



ハードウェアの変更テーブルウィジェットには、指定した期間（7日、30日、または当月）にクライアントの組織内の物理的および仮想的なWindowsまたmacOSデバイスで追加、削除、および変更されたハードウェアに関する情報が表示されます。



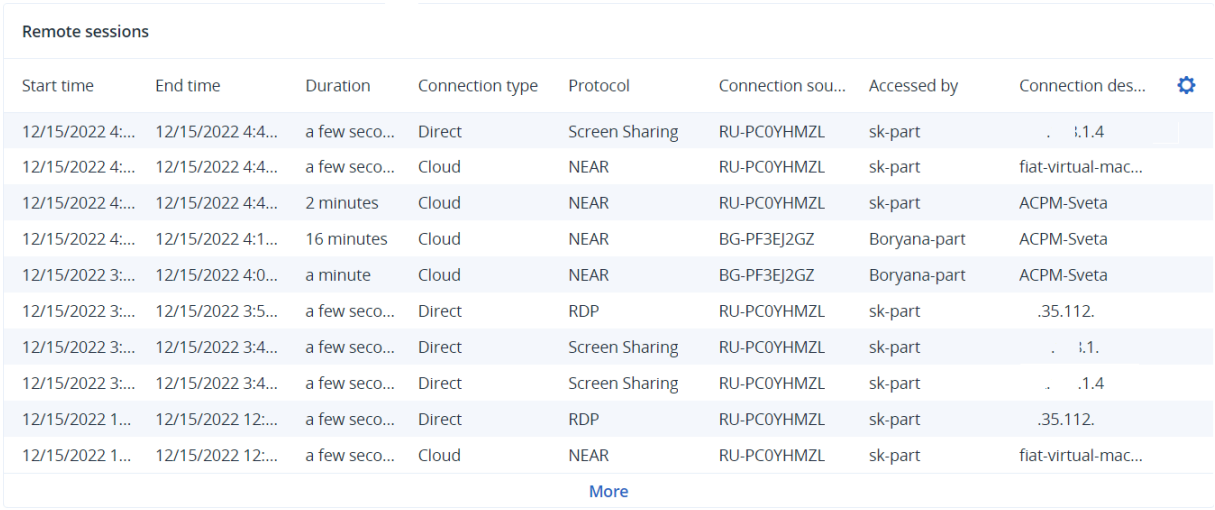
ハードウェアインベントリウィジェットに表示される結果をフィルタリングできます。

注意

マシン名フィルタでは、最大20個の値を選択できます。

セッション履歴

このウィジェットでは、指定された期間にクライアントの組織で実行された、リモートデスクトップとファイル転送セッションの詳細を表示します。



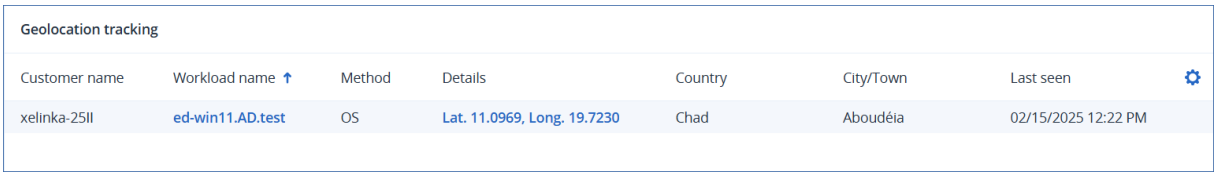
Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

More

位置情報トラッキングウィジェット

位置情報トラッキングウィジェットでは、クライアント組織内のワークロードのロケーションに関する詳細情報（国、都市または町、座標、最終確認時刻、位置情報トラッキング方法など）を確認できます。

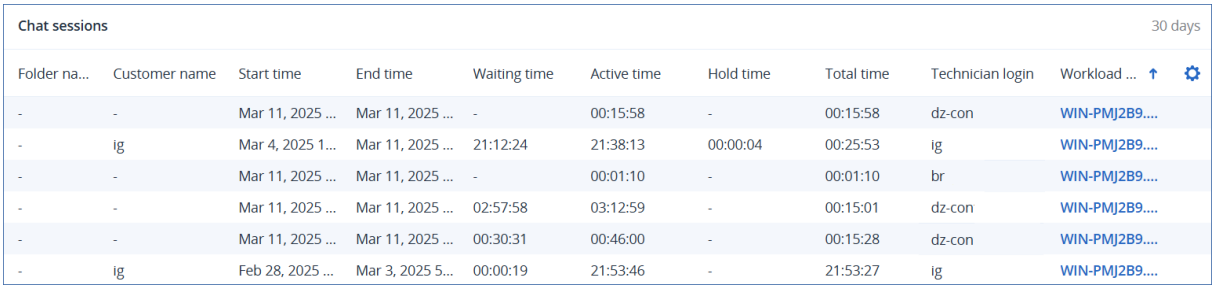


Geolocation tracking

Customer name	Workload name	Method	Details	Country	City/Town	Last seen
xelinka-25II	ed-win11.AD.test	OS	Lat. 11.0969, Long. 19.7230	Chad	Aboudéia	02/15/2025 12:22 PM

チャットセッションウィジェット

チャットセッションウィジェットでは、指定した期間におけるクライアントの組織内のリモートチャットセッションの詳細を表示できます。

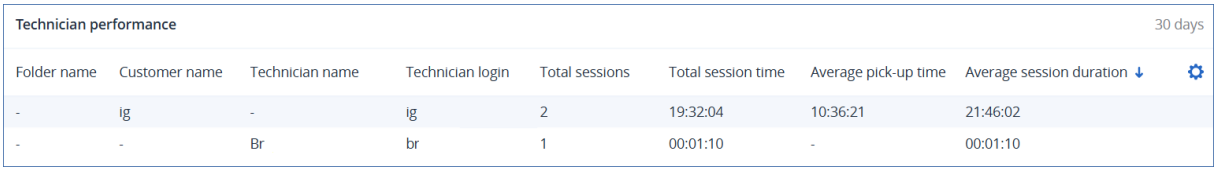


Chat sessions — 30 days

Folder na...	Customer name	Start time	End time	Waiting time	Active time	Hold time	Total time	Technician login	Workload ...
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	-	00:15:58	-	00:15:58	dz-con	WIN-PMJ2B9....
-	ig	Mar 4, 2025 1...	Mar 11, 2025 ...	21:12:24	21:38:13	00:00:04	00:25:53	ig	WIN-PMJ2B9....
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	-	00:01:10	-	00:01:10	br	WIN-PMJ2B9....
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	02:57:58	03:12:59	-	00:15:01	dz-con	WIN-PMJ2B9....
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	00:30:31	00:46:00	-	00:15:28	dz-con	WIN-PMJ2B9....
-	ig	Feb 28, 2025 ...	Mar 3, 2025 5...	00:00:19	21:53:46	-	21:53:27	ig	WIN-PMJ2B9....

技術者パフォーマンスウィジェット

技術者のパフォーマンスウィジェットでは、指定した期間におけるクライアントの組織内の各技術者のパフォーマンスの詳細を表示できます。



Technician performance — 30 days

Folder name	Customer name	Technician name	Technician login	Total sessions	Total session time	Average pick-up time	Average session duration
-	ig	-	ig	2	19:32:04	10:36:21	21:46:02
-	-	Br	br	1	00:01:10	-	00:01:10

監査ログ

監査ログには、次のイベントの情報が年代順に表示されます。

- 管理ポータル内でユーザーによって実行される処理
- Cyber Protectコンソールでユーザーが実行する、クラウドツークラウドのリソースを使った処理
- Cyber Protectコンソールで、ユーザーによって実行されるサイバースクリプト処理
- Eメールアーカイブに関連する操作
- 到達したクォータとその使用状況についてのシステムメッセージ

このログには、現在操作しているテナントおよびその直下のテナントのイベントが表示されます。イベントをクリックするとその詳細を表示できます。

監査ログはデータセンターに保管されているため、エンドユーザーのマシンで問題が発生しても、そのログの可用性は影響を受けません。

ログは毎日クリーンアップされます。イベントは180日後に削除されます。

監査ログのフィールド

イベントごとに、ログには以下の内容が表示されます。

- **イベント**
  イベントの短い説明です。例えば、**テナントが作成されました**、**テナントが削除されました**、**ユーザーが作成されました**、**ユーザーが削除されました**、**クォータに達しました**、**バックアップコンテンツが参照されました**、**スクリプトが変更されました**、などです。
- **重大度**
  次のいずれかが表示されます。
  - **エラー**
    エラーを示します。
  - **警告**
    悪影響を及ぼす可能性のあるアクションを示します。たとえば、**テナントが削除されました**、**ユーザーが削除されました**、**クォータに達しました**などです。
  - **通知**
    注意が必要になる可能性のあるイベントを示します。たとえば、**テナントがアップデートされました**、**ユーザーがアップデートされました**などです。
  - **情報**
    中立的な情報提供の変更または操作を示します。例えば、**テナントが作成されました**、**ユーザーが作成されました**、**クォータがアップデートされました**、**スクリプト計画が削除されました**、などです。
- **日付**
  イベントが発生した日付と時刻です。
- **オブジェクト名**

操作が実行されたオブジェクトです。たとえば、**ユーザーがアップデートされました**イベントのオブジェクトは、プロパティが変更されたユーザーです。クォータに関連するイベントの場合、クォータがオブジェクトです。

- **テナント**
  オブジェクトが属するテナントの名前です。
- **イニシエータ**
  イベントを開始したユーザーのログインです。システムメッセージおよび上位の管理者によって開始されたイベントの場合、イニシエータには**システム**と表示されます。
- **イニシエータのテナント**
  イニシエータが属するテナントの名前です。システムメッセージおよび上位の管理者によって開始されたイベントの場合、このフィールドは空白です。
- **方法**
  イベントが、Webインターフェース経由またはAPI経由のどちらで開始されたかを示します。
- **IP**
  イベントが開始されたマシンのIPアドレスです。

フィルタ処理と検索

イベントは、タイプ、重要度、または日付でフィルタリングできます。また、名前、オブジェクト、テナント、イニシエータ、およびイニシエータのテナントで検索することもできます。

Cyber Protectionエージェントのパフォーマンスデータの収集

環境内の保護されている Windows マシンについては、パフォーマンスログを手動で収集するか、システムパフォーマンスが工場出荷時に定義されたしきい値を下回った場合に診断データの自動収集を有効にできます。詳細については、"ETLデータ収集のパフォーマンスしきい値"（214ページ）を参照してください。

収集されたログは、ベンダーへの分析送信前に匿名化されます。すべてのログ、メッセージ、アラート、エラーメッセージからは、次のデータが削除されます。

- ユーザーアカウント
- 会社名
- 保護されているワークロードの名前

パートナー管理者として、子テナント内のランダムに選択されたエージェントのログの自動収集を有効にしたり、管理している組織内の特定のエージェントのログの自動収集を有効にしたりできます。

会社の管理者として、ランダムに選択されたエージェントまたは組織内の特定のエージェントのログの自動収集を有効にできます。

注意

- 個々のワークロードの自動データ収集は、Cyber Protection Windows バージョン 24.4.37758 以降用エージェントでサポートされています。
- テナントレベルでのパフォーマンスデータ収集は、Cyber ProtectionWindows バージョン 25.03.XXXXX 以降用エージェントでサポートされています。

サポートの推奨事項が十分に情報に基づいたものであることを保証するために、環境内のエージェントの約10%からデータを収集して分析します。

これは、個々のワークロードの設定を上書きするものではありません。たとえば、特定のワークロードで自動データ収集が無効になっている場合、そのワークロードは一括データ収集に含まれません。

複数のエージェントの自動収集

テナント内の複数のエージェントのパフォーマンスデータの自動収集を有効にするには

必要なロール: パートナー管理者、 カスタマー管理者

1. Cyber Protect Cloudコンソールで **[設定]** > **[エージェント]** に移動します。
2. 右側の **アクション** メニューで、**パフォーマンス モニタの設定を編集** をクリックします。
3. **パフォーマンスモニタ**セクションで、トグル**パフォーマンスログの自動収集とアップロード**を有効にします。

自動的に収集されたデータは、保護されているマシンのローカルディスクのフォルダ `C:\ProgramData\Acronis\ETLTool\ETL\` に保存され、匿名化されて、サービスプロバイダーに送信されて分析されます。

注意

ETL ログをクラウドに送信する回数の制限は、24 時間あたり 3 回です。

単一エージェントの自動収集

特定のエージェントのパフォーマンスデータの自動収集を有効にするには

1. 会社レベルの Cyber Protect Cloud コンソールで、**設定** > **エージェント** に移動します。
2. **[エージェント]** リストで、パフォーマンスモニタを有効にするエージェントを選択します。
3. 右側の **アクション** メニューで **詳細** をクリックします。
4. **パフォーマンスモニタ** セクションまでスクロールし、**このエージェントがパフォーマンスログを自動的に収集することを許可する** トグルを有効にします。

自動的に収集されたデータは、保護されているマシンのローカルディスクのフォルダ `C:\ProgramData\Acronis\ETLTool\ETL\` に保存されます。

手動収集

パフォーマンスデータを手動で収集するには

必要に応じてパフォーマンスデータを収集できます。この場合、パフォーマンスモニタとパフォーマンスデータの自動収集を有効にする必要はありません。

1. 保護されているマシンに管理者ユーザーとしてログインします。
2. コマンドプロンプトで、次のいずれかのコマンドを実行します。
   - `"C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o`
     ETLトレースの収集は、キーボードのSキーが押されるまで、または、最大時間制限の3600秒が経過するまで実行されます。
   - `"C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o -i X`
     Xはデータ収集の制限時間（秒）で、最大値は3600です。収集は、キーボードのSキーを押すことでいつでも停止できます。

手動で収集されたデータは、保護されているマシンのローカル ディスクのフォルダ`C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\`に保存されます。

パフォーマンスログを収集するには

1. 保護されているマシンに管理者ユーザーとしてログインします。
2. 必要とするデータを見つけます。
   - 自動的に収集されたパフォーマンスデータは、フォルダ`C:\ProgramData\Acronis\ETLTool\ETL\`にあります。
   - 手動で収集されたパフォーマンスデータは、フォルダ`C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\`にあります。

ETLトレースは、`sysinfo`パッケージにも含まれています。

ETLデータ収集のパフォーマンスしきい値

環境内の保護されているWindowsマシンに対してパフォーマンス データの自動収集を有効にできます。監視機能は、Cyber Protect Cloudコンソールでエージェントごとに構成され、システムパフォーマンスが事前に定義されたしきい値を下回ると、診断データの自動収集が有効になります。

しきい値のいずれかを超えると、自動データ収集が開始されます。

ETL データ収集のデフォルトのしきい値

次の表は、ETL データの自動収集をトリガーするしきい値について説明します。

パラメータ	説明	デフォルト値
"process-memory-consumption"	メモリの過剰使用のしきい値	
"allocated-memory-percent"		15
"minimum-allocated-memory-duration-seconds"		10
"allocated-memory-free-limit-seconds"		300
"process-disk-io"	高I/O使用率のしきい値	
"maximum-operations-number"		10000

パラメータ	説明	デフォルト値
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-file-io"	高ファイルI/O使用率のしきい値	
"maximum-operations-number"		30000
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-cpu-usage"	高CPU消費率のしきい値	
"cpu-percent"		15
"estimation-period-seconds"		10
"acronis-component-thresholds"	プロテクションエージェントのコンポーネントのパフォーマンス	
"behavioral-engine"	振る舞い検知エンジンのしきい値	
"average-system-utilization-percent"		50
"be-stats-event-number"		10
"avc-scan"	ウイルス対策およびマルウェア対策保護コンポーネントのしきい値	
"average-scan-duration-seconds"	最大平均スキャン時間	3
"estimation-period-seconds"		10
"maximum-scan-duration-seconds"	単一のスキャンの最大スキャン時間	5

レポート

サービスの使用状況や操作に関するレポートを作成するには、[**レポート**] をクリックします。

使用状況レポート

使用状況レポートは、サービスの使用に関する履歴データを提供します。使用状況レポートは、CSV形式とHTML形式の両方で利用できます。

重要
製品のUIに表示されるストレージ使用量の値は、バイナリバイト単位（メビバイト（MiB）、ギビバイト（GiB）、テビバイト（TiB））ですが、ラベルにはそれぞれMB、GB、TBが表示されます。たとえば、実際の使用量が3105886629888バイトの場合、UIに表示される値は2.82と正しく表示されますが、ラベルはTiBではなくTBになります。

レポートの種類

次のいずれかのレポートの種類を選択できます:

- **現在の使用状況**
  レポートには、現在のサービス使用状況のメトリクスが含まれます。
  使用状況のメトリクスメトリクスは、それぞれの子テナントの請求期間内に計算されます。レポートに含まれるテナントの請求期間が異なる場合、親テナントの使用状況は子テナントの使用状況の合計と異なる場合があります。
- **現在の使用状況の分布**
  このレポートは、外部プロビジョニングシステムによって管理されているパートナーテナントでのみ使用できます。このレポートは、子テナントの請求期間が親テナントの請求期間と一致しない場合に役立ちます。このレポートには、親テナントの現在の請求期間内に計算された、子テナントのサービス使用状況のメトリクスが含まれています。親テナントの使用状況は、子テナントの使用状況の合計と一致することが保証されています。
- **期間の概要**
  レポートには、指定期間の終了時のサービス使用状況のメトリクスと、指定期間の開始時と終了時のメトリクスの差が含まれます。

  注意
  ローカルストレージの使用状況データは、部署レベルとカスタマーテナントレベルでのみレポートが表示されます。サマリレポートでは、ローカルストレージの使用状況に関する情報はユーザーに提供されません。

- **期間の日別**
  レポートには、サービス使用状況のメトリクスと、指定された期間の毎日の変化が含まれます。

レポート範囲

レポートの対象範囲を次の値から選択できます。

- **直接の顧客およびパートナー**
  このレポートには、操作しているテナントの直下の子テナントのサービス使用状況メトリクスのみが含まれます。
- **すべての顧客およびパートナー**
  このレポートには、操作しているテナントのすべての子テナントのサービス使用状況メトリクスが含まれます。
- **すべてのカスタマーおよびパートナー（ユーザーの詳細を含む）**
  このレポートには、操作しているテナントのすべての子テナント、およびテナント内のすべてのユーザーのサービス使用状況メトリクスが含まれます。

使用量がゼロのメトリクス

使用量がゼロではないメトリクスに関する情報を表示し、使用量がゼロのメトリクス関する情報を非表示にすることで、レポートの行数を減らすことができます。

スケジュール済み使用状況レポートの構成

定期レポートには、前月のサービス使用状況メトリクスが含まれます。レポートは月初日の23:59:59（UTC時間）に生成され、翌日に送信されます。レポートは、ユーザー設定で **[定期使用状況レポート]** チェックボックスをオンにしている、テナントのすべての管理者に送信されます。

注意
日付によるフィルタリングは、アクティビティが開始または完了した時間ではなく、イベントがクラウドに送信されたタイムスタンプによって実行されます。つまり、サーバーへの接続が中断された場合、日次レポートには1日分を越えるデータが含まれる場合があります。

定期レポートを有効または無効にするには

1. 管理ポータルにログインします。
2. 利用可能な最上位のテナントで操作していることを確認してください。
3. **[レポート]** > **[使用状況]**をクリックします。
4. **[定期]** をクリックします。
5. **[月次サマリレポートを送信]** チェックボックスをオンまたはオフにします。
6. **[詳細レベル]** で、レポートのスコープを選択します。
7. （オプション） 使用量がゼロのメトリクスをレポートから除外する場合は、**[使用量がゼロのメトリクスを非表示]** を選択します。

カスタム使用状況レポートの構成

このレポートは手動でのみ生成され、レポートするタイミングをスケジュールすることはできません。レポートは、作成者の電子メールアドレスに送信されます。

カスタムレポートを生成するには

1. 管理ポータルにログインします。
2. レポートを作成するテナントを指定します。

3. **[レポート]** > **[使用状況]**をクリックします。
4. **[カスタム]** タブを選択します。
5. **[種類]** で、前述の説明に従ってレポートの種類を選択します。
6. [**現在の使用状況**レポートの種類では使用できません] **[期間]** でレポート期間を選択します:
   - **今月**
   - **前月**
   - **カスタム**
7. [**現在の使用状況**レポートの種類では使用できません] カスタムレポート期間を指定する場合は、開始日と終了日を選択します。それ以外の場合は、この手順をスキップします。
8. **[詳細レベル]** で、前述の説明に従ってレポートの範囲を選択します。
9. （オプション） 使用量がゼロのメトリクスをレポートから除外する場合は、**[使用量がゼロのメトリクスを非表示]** を選択します。
10. レポートを生成するには、**[生成して送信]** をクリックします。

操作レポート

操作に関するレポートには、**[操作]** ダッシュボードウィジェットの任意のセットを含めることができます。デフォルトでは、すべてのウィジェットに操作中のテナントのサマリ情報が表示されます。ウィジェットを編集するか、レポート設定のすべてのウィジェットに対して個別に変更することができます。

ウィジェットのタイプに応じ、レポートには時間範囲のデータ、または参照時やレポート生成時のデータが含まれます。"ウィジェットの種類に応じたレポートのデータ"（235ページ）をご覧ください。

すべての履歴ウィジェットで、同じ時間範囲のデータが表示されます。この範囲はレポート設定で変更できます。

デフォルトのレポートを使用したり、カスタムレポートを作成したりできます。

レポートをダウンロードできます。またXLSX（Excel）またはPDF形式によりEメールで送信することもできます。

デフォルトのレポートの一覧は次のとおりです。

レポート名	説明
マシンごとの #CyberFit スコア	各マシンのセキュリティメトリクスと構成の評価に基づき、#CyberFit スコアと、改善するための提案が表示されます。
アラート	指定された期間に発生したアラートを表示します。
バックアップスキャンの詳細	バックアップ内に検出された脅威に関する詳細を表示します。
日次のアクティビティ	指定された期間中に実行されたアクティビティの概要を表示します。
データ保護マップ	マシン上にあるすべての重要なファイルの数、サイズ、ロケーション、保護ステータスの詳細を表示します。
検出された脅威	影響を受けたマシンの詳細情報として、ブロックされた脅威の数、お

	よび正常なマシンと脆弱なマシンの数を表示します。
検出されたデバイス	クライアントのネットワークで検出されたすべてのデバイスを表示します。
ディスク状態の予測	HDD/SSDが故障するタイミングの予測と現在のディスクのステータスを示します。
既存の脆弱性	組織内のOSとアプリケーションの既存の脆弱性を一覧表示します。このレポートには、一覧にある各製品について、ネットワーク内で影響を受けたマシンの詳細情報が表示されます。
パッチ管理概要	未適用のパッチ、インストール済みのパッチ、適用可能なパッチの一覧を表示します。レポートを掘り下げることで、未適用/インストール済みパッチの情報およびシステム全体の詳細情報が得られます。
概要	指定された期間に保護されたデバイスの概要を表示します。
週単位のアクティビティ	指定された期間中に実行されたアクティビティの概要を表示します。
ソフトウェアインベントリ	クライアントの組織内のWindowsおよびmacOSマシンにインストールされている、すべてのソフトウェアに関する詳細情報を表示します。 **注意** レポートには、一度に最大20のワークロードを含めることができます。
ハードウェアインベントリ	クライアントの組織内の物理的および仮想的なWindowsまたはmacOSマシンで使用可能なすべてのハードウェアに関する詳細情報を表示します。 **注意** レポートには、一度に最大20のワークロードを含めることができます。
リモートセッション	指定された期間にクライアントの組織で実行された、リモートデスクトップとファイル転送セッションの詳細を表示します。

レポートの操作

追加

新しいレポートを追加するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. 使用可能なレポートのリスト以下で、**[レポートを追加]** をクリックします。
3. （定義済みレポートを追加するには）定義済みレポートの名前をクリックします。
4. （カスタムレポートを追加するには）**[カスタム]** をクリックしてから、レポートにウィジェットを追加します。
5. （オプション） ウィジェットをドラッグアンドドロップして並べ替えます。

表示

レポートを表示するには

- レポートを表示するには、その名前をクリックします。

編集

レポートを編集するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストで、編集するレポートを選択します。
3. 画面の右上隅にある **[設定]** をクリックします。
4. レポートを編集してから、**[保存]** をクリックします。

削除

レポートを削除するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストで、削除するレポートを選択します。
3. 画面の右上隅にある省略記号アイコン（...）をクリックして、**[レポートを削除]** をクリックします。
4. 確認ウィンドウで **[削除]** をクリックします。

スケジュール

レポートのスケジュールを設定するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストで、スケジュール設定するレポートを選択します。
3. 画面の右上隅にある **[設定]** をクリックします。
4. **[スケジュール]**の横にあるスイッチを有効にします。
   - 受信者のEメールアドレスを指定します。
   - レポートの形式を選択します。

   - **注意**
     PDFファイルには最大1,000件、XLSXファイルには最大10,000件の項目をエクスポートできます。PDFおよびXLSXファイルのタイムスタンプには、マシンのローカル時刻が使用されます。

   - レポートの言語を選択します。
   - スケジュールを構成します。
5. **[保存]** をクリックします。

ダウンロード

レポートをダウンロードするには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストでレポートを選択します。

3. 画面の右上隅にある **[ダウンロード]** をクリックします。
4. レポートの形式を選択します。

これにより、選択した形式のファイルがマシンにダウンロードされます。

[ExcelとPDF] を選択した場合、ZIPファイルがマシンにダウンロードされます。

送信する

レポートを送信するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストでレポートを選択します。
3. 画面の右上隅にある **[送信]** をクリックします。
4. 受信者のEメールアドレスを指定します。
5. レポートの形式を選択します。
6. **[送信する]** をクリックします。

構造のエクスポート

レポート構造をエクスポートするには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストでレポートを選択します。
3. 画面の右上隅にある省略記号アイコン（...）をクリックして、**[エクスポート]** をクリックします。

これにより、レポート構造はJSONファイルとしてマシンに保存されます。

データをダンプ

レポートデータをダンプするには

カスタム期間のデータをすべてフィルタリングせずにCSVファイルにエクスポートし、そのCSVファイルをEメールの受信者に送信できます。CSVファイルには、レポートに含まれるウィジェットのデータのみが含まれます。

注意
CSVファイルには、最大150,000件の項目をエクスポートできます。CSVファイルのタイムスタンプには、協定世界時（UTC）が使用されます。

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストで、データをダンプするレポートを選択します。
3. 画面の右上隅にある省略記号アイコン（...）をクリックして、**[データをダンプ]** をクリックします。
4. 受信者のEメールアドレスを指定します。
5. **[時間範囲]** で、データをダンプするカスタムの期間を指定します。

   注意
   長期間を対象とするCSVファイルの準備には、時間を要する場合があります。

6. **[送信する]** をクリックします。

エクゼクティブサマリ

エグゼクティブサマリレポートでは、指定した期間におけるカスタマー環境と保護されたデバイスに関する保護ステータスの概要が提供されます。

エグゼクティブサマリレポートには、クライアントの次に示すクラウドサービスの利用に関連する主要なパフォーマンスメトリクスを示す、動的ウィジェットのセクションが含まれています。バックアップ、マルウェア対策保護、脆弱性診断、パッチ管理、データ漏洩防止、ノータリー、Disaster Recovery、File Sync & Share。

レポートをカスタマイズするためのいくつかの方法があります。

- セクションを追加または削除します。
- セクションの順序を変更します。
- セクション名を変更します。
- セクション間でウィジェットを移動します。
- 各セクションのウィジェットの順序を変更します。
- ウィジェットを追加または削除します。
- ウィジェットをカスタマイズします。

PDFやExcel形式のエグゼクティブサマリレポートを作成し、カスタマー組織の利害関係者や所有者に送付することで、提供されたサービスの技術的/ビジネス的価値を容易に確認することができます。

パートナー管理者は、エグゼクティブサマリレポートを作成し、直接のカスタマーにのみ送信することができます。サブパートナーを含む複雑なテナント階層の場合は、サブパートナーがレポートを作成する必要があります。

エクゼクティブサマリウィジェット

エグゼクティブサマリレポートにセクションやウィジェットを追加また削除することができます。これにより、どのような情報を含めるかを制御できます。

ワークロードの概要ウィジェット

次の表に、**ワークロードの概要**セクションのウィジェットについての詳細を示します。

ウィジェット	説明
クラウドワークロードの保護ステータス	このウィジェットには、レポート生成時点における保護されたクラウドワークロードと保護されていないクラウドワークロードの数が種類別に表示されます。保護されたクラウドワークロードとは、少なくとも1つのバックアップ計画が適用されているクラウドワークロードのことです。保護されていないクラウドワークロードとは、バックアップ計画が適用されていないクラウドワークロードのことです。チャートには、以下のクラウドワークロードのタイプが示されています（AからZまでのアルファベット順）。 • Google Workspaceドライブ • Google Workspace Gmail

ウィジェット	説明
	• Google Workspace共有ドライブ • ホスト済み Exchange メールボックス • Microsoft 365メールボックス • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Web サイト 一部のワークロードタイプでは、以下のワークロードグループが使用されます。 • Microsoft 365:ユーザー、グループ、パブリックフォルダ、Teams、サイトコレクション • Google Workspace:ユーザー、共有ドライブ • Hosted Exchange:ユーザー 1つのワークロードグループに10,000を超えるワークロードがある場合、ウィジェットには対応するワークロードのデータが表示されません。 たとえば、カスタマーが10,000個のメールボックスと500ユーザーのOneDriveサービスを含むMicrosoft 365アカウントを所有している場合、それらはすべてユーザーワークロードグループに属することになります。これらのワークロードの合計は10,500になり、ワークロードグループの制限である10,000を超過します。そのため、ウィジェットでは対応する次のワークロードタイプが非表示になります:Microsoft 365メールボックス、およびMicrosoft 365 OneDrive。
サイバープロテクションのサマリ	ウィジェットには、指定した期間におけるサイバープロテクションのパフォーマンスに関する主要なメトリクスが表示されます。 **バックアップされたデータ** - クラウドとローカルのストレージに作成されたアーカイブの合計サイズです。 **軽減された脅威** - すべてのデバイスでブロックされたマルウェアの合計数です。 **ブロックされた悪意のあるURL** - すべてのデバイスでブロックされたURLの合計数です。 **パッチ適用済みの脆弱性** - すべてのデバイスでソフトウェアパッチをインストールすることで修正された脆弱性の合計数です。 **インストール済みパッチ** - すべてのデバイスでインストールされているパッチの合計数です。 **DRで保護されたサーバー** - Disaster Recoveryによって保護されているサーバーの合計数です。 **File Sync & Shareユーザー** - Cyber Filesを利用しているエンドユーザーとゲストユーザーの合計数です。 **公証済ファイル** - 公証済ファイルの合計数です。 **電子署名済み文書** - 電子署名済み文書の合計数です。

ウィジェット	説明
	ブロックされた周辺機器 - ブロックされた周辺デバイスの合計数です。
ワークロードのネットワークステータス	このウィジェットでは、分離されているワークロードの数と接続済みのワークロード（通常状態のワークロード）の数が示されます。 関連するカスタマーを選択します。表示されるワークロードビューではフィルターが適用され、分離されたワークロードが表示されます。[接続済み] の値をクリックすると、接続済みのワークロード（選択したカスタマー）を表示するフィルターが適用されたエージェントリストとワークロードが表示されます。
ワークロードの保護ステータス	ウィジェットには、レポート作成時点で保護されているワークロードと保護されていないワークロードが種類別に表示されます。保護されたワークロードとは、少なくとも1つの保護計画またはバックアップ計画が適用されているワークロードのことです。保護されていないワークロードとは、保護計画またはバックアップ計画が適用されていないワークロードのことです。以下のワークロードがカウントされます。 **サーバー** - 物理サーバー、およびドメインコントローラーサーバーです。 **ワークステーション** - 物理ワークステーションです。 **仮想マシン** - エージェントベースおよびエージェントレス両方の仮想マシンです。 **Webホスティングサーバー** - cPanelまたはPleskでインストールされた仮想サーバーまたは物理サーバーです。 **モバイルデバイス** - 物理モバイルデバイスです。 1つのワークロードが複数のカテゴリに属することもあります。たとえば、Webホスティングサーバーは、**サーバー**と**Webホスティングサーバー**の2つのカテゴリに分類されます。
検出されたデバイス	ウィジェットには、指定した期間にカスタマーのネットワークで検出されたデバイスに関する次の情報が表示されます。 **カスタマー名** **フォルダ名** **デバイス名** **デバイスの種類** **オペレーティングシステム** **製造元** **モデル** **IPアドレス** ウィジェットを編集し、表示される情報を、テナント、組織単位（OU）、デバイスタイプ、検出の種類、最初に検出された日付、最後に検出された日付、IPアドレス、MACアドレス、および検出の種類でフィルタリングできます。

マルウェア対策保護ウィジェット

次の表に、**脅威の防御**セクションのウィジェットについての詳細を示します。

ウィジェット	説明
ファイルのマルウェア対策スキャン	ウィジェットには、指定した日付範囲にデバイスに対して実行された、オンデマンドのマルウェア対策スキャンの結果が表示されます。 **ファイル** - スキャンされたファイルの合計数 **クリーン** - クリーンなファイルの合計数 **検出済み、隔離済み** - 隔離された感染ファイルの合計数 **検出済み、未隔離** - 未隔離の感染ファイルの合計数 **保護されているデバイス** - マルウェア対策保護ポリシーが適用されているデバイスの合計数 **登録済みデバイスの合計数** - レポート生成時に登録されたデバイスの合計数
バックアップのマルウェア対策スキャン	ウィジェットには、指定した日付範囲にバックアップに対して実行された、マルウェア対策スキャンの結果が表示されます。次のメトリクスが使用されます。 • スキャンされた復元ポイントの合計数 • クリーンな復元ポイントの数 • サポートされていないパーティションにおけるクリーンな復元ポイントの数 • 感染した復元ポイントの数サポートされていないパーティションにおけるクリーンな復元ポイントの数。
ブロックされたURL	指定した日付範囲で、Webサイトのカテゴリごとにグループ化されたブロック済みURLの数がウィジェットに表示されます。 このウィジェットでは、ブロック済みURLの数が多い順に、7つのWebサイトカテゴリがリストアップされます。また残りのWebサイトカテゴリは、**その他**としてまとめて表示されます。 Webサイトのカテゴリの詳細については、Cyber ProtectionのURLフィルタリングのトピックを参照してください。
セキュリティインシデントのバーンダウン	このウィジェットでは、選択した会社のインシデントがクローズ状態になるまでの効率性が表示されます。この効率性は、オープン状態のインシデントの数と、一定期間内にクローズされたインシデントの数の比較により表わされます。 列をホバーすると、選択した日付におけるクローズ状態およびオープン状態のインシデントの内訳が表示されます。括弧内の%数値により、前期比での増減が表わされます。
インシデントMTTR	このウィジェットでは、セキュリティインシデントの平均解決時間を表示します。これは、インシデントの調査や解決のスピードを示しています。 列をクリックすると、重要度（**重大**、**高**、**中**）別のインシデントの内訳と、重要度レベル別の解決に要した時間が表示されます。括弧内の%数値により、前期比での増減が表わされます。

ウィジェット	説明
脅威のステータス	このウィジェットでは、企業のワークロードに存在する現在の脅威のステータス（ワークロードの数に関係なく）が表示されます。また、現時点で脅威が軽減されておらず、調査が必要なインシデントの数が強調表示されます。ウィジェットにはさらに、（手動で、またはシステムにより自動で）軽減措置が適用されたインシデントの数も表示されます。
保護技術で検知した脅威	指定した日付範囲に検出された脅威の数が、以下の保護技術ごとにグループ化されてウィジェットに表示されます。 • マルウェア対策スキャン • 振る舞い検知エンジン • クリプトマイニングからの保護 • エクスプロイト防御 • ランサムウェアアクティブプロテクション • リアルタイム保護 • URLフィルタ処理

バックアップウィジェット

次の表に、**バックアップ**セクションのウィジェットについての詳細を示します。

ウィジェット	説明
バックアップ済みのワークロード	ウィジェットには、登録されたワークロードの合計数がバックアップステータス別に表示されます。 **バックアップ済み** - レポートの日付範囲内でバックアップされた（少なくとも1回のバックアップが成功した）ワークロードの数。 **未バックアップ** - レポートの日付範囲内でバックアップされなかった（バックアップが成功しなかった）ワークロードの数。
物理デバイスごとのディスク状態のステータス	このウィジェットでは、物理デバイスのディスク状態のステータスに基づいて、集約されたヘルスステータスが表示されます。 **OK** - このディスク状態のステータスは、値 [70-100] に相当します。デバイス内のすべてのディスクでステータスが**OK**であれば、デバイスのステータスも**OK**となります。 **警告** - このディスク状態のステータスは、値 [30-70] に相当します。デバイス内の少なくとも1つのディスクのステータスが**警告**であり、さらにステータスが**エラー**のディスクが存在しない場合、デバイスのステータスは**警告**となります。 **エラー** - このディスク状態のステータスは、値 [0-30] に相当します。デバイス内の少なくとも1つのディスクのステータスが**エラー**である場合、デバイスのステータスは**エラー**となります。 **ディスクデータの計算中** - デバイスのディスクステータスがまだ計算されていない場合、デバイスのステータスは**ディスクデータの計算中**となります。

ウィジェット	説明
バックアップストレージの使用状況	ウィジェットには、指定した期間における、クラウドとローカルストレージにあるバックアップの合計数と合計サイズが表示されます。

脆弱性診断とパッチ管理ウィジェット

次の表に、**脆弱性診断とパッチ管理**セクションのウィジェットについての詳細を示します。

ウィジェット	説明
パッチ適用済みの脆弱性	ウィジェットには、指定された日付範囲における脆弱性診断のパフォーマンスの結果が表示されます。 **合計** - パッチ適用済みの脆弱性の合計数です。 **Microsoftソフトウェアの脆弱性** - すべてのWindowsデバイス上で修正されたMicrosoftの脆弱性の合計数です。 **Windowsサードパーティ製のソフトウェアの脆弱性** - すべてのWindowsデバイス上で修正されたWindowsサードパーティの脆弱性の合計数です。 **スキャン済みのワークロード** - 指定された日付範囲に、少なくとも1回脆弱性スキャンが正常に実行されたデバイスの合計数です。
インストール済みパッチ	ウィジェットには、指定された日付範囲におけるパッチ管理のパフォーマンスの結果が表示されます。 **インストール済み** - すべてのデバイスで正常にインストールされたパッチの合計数です。 **Microsoftソフトウェアパッチ** - すべてのWindowsデバイスでインストールされたMicrosoftソフトウェアパッチの合計数です。 **Windowsサードパーティ製のソフトウェアパッチ** - すべてのWindowsデバイスでインストールされたWindowsサードパーティ製のソフトウェアパッチの合計数です。 **パッチ適用済みのワークロード** - パッチが適用されたデバイスの合計数（指定された日付範囲に、少なくとも1つのパッチが正常にインストール済み）。

ソフトウェアウィジェット

次の表に、[**ソフトウェア**] セクションのウィジェットについての詳細を示します。

ウィジェット	説明
インストールステータス	このウィジェットには、カスタマーの管理対象デバイスにおけるステータス別にグループ化されたインストールアクティビティの合計数が表示されます。ドーナツグラフのセグメントをクリックすると、[**アクティビティ**] ページにリダイレクトされ、対応するステータスのアクティビティのみが日付順に表示されます。

ウィジェット	説明
削除ステータス	ウィジェットには、カスタマーの管理対象デバイスにおけるステータス別にグループ化された削除アクティビティの合計数が表示されます。ドーナツグラフのセグメントをクリックすると、[**アクティビティ**] ページにリダイレクトされ、対応するステータスのアクティビティのみが日付順に表示されます。
ソフトウェアインストール履歴	このウィジェットでは、カスタマーの管理対象のデバイスにおけるソフトウェアのリモートインストールに関する詳細なステータス情報が表示されます。[**インストールステータス**] 列のステータスをクリックすると、[**アクティビティ**] ページにリダイレクトされ、アクティビティと対応するステータスが時系列順に表示されます。
ソフトウェア削除履歴	ウィジェットでは、カスタマーの管理対象のデバイスからのソフトウェアのリモート削除に関する詳細なステータス情報が表示されます。[**削除ステータス**] 列のステータスをクリックすると、[**アクティビティ**] ページにリダイレクトされ、アクティビティと対応するステータスが時系列順に表示されます。

Disaster Recoveryウィジェット

次の表に、**ディザスタリカバリ**セクションのウィジェットについての詳細を示します。

ウィジェット	説明
Disaster Recoveryの統計情報	ウィジェットには、指定した日付範囲のDisaster Recoveryの主要なパフォーマンスメトリクスが表示されます。 **本番フェールオーバー** - 指定した期間での本番フェールオーバー処理の回数です。 **テストフェールオーバー** - 指定した期間に実行されたテストフェールオーバー処理の回数です。 **プライマリサーバー** - レポート作成時点でのプライマリサーバーの合計数です。 **復元サーバー** - レポート作成時点での復元サーバーの合計数です。 **パブリックIP** - レポート作成時点でのパブリックIPアドレスの合計数です。 **消費済み合計計算ポイント** - 指定した期間に消費された計算ポイントの合計数です。
テスト済みのDisaster Recoveryサーバー	ウィジェットには、Disaster Recoveryで保護され、テストフェールオーバーでテストされたサーバーに関する情報が表示されます。 ウィジェットには以下のメトリクスが表示されます。 **保護されたサーバー** - レポート作成時点での、Disaster Recoveryによって保護されているサーバー（復元サーバーが1台または複数あるサーバー）の数です。 **テスト済み** - Disaster Recoveryによって保護されているすべてのサーバーのうち、指定した期間にテストフェールオーバーを使用してテストされたサーバーの数です。

ウィジェット	説明
	未テスト - Disaster Recoveryによって保護されているすべてのサーバーのうち、指定した期間にテストフェールオーバーを使用してテストされていないサーバーの数です。 また、このウィジェットには、レポート作成時のDisaster Recoveryストレージのサイズ（GB）が表示されます。これは、クラウドサーバーのバックアップサイズの合計です。
Disaster Recoveryで保護済みのサーバー	ウィジェットには、Disaster Recoveryで保護されているサーバーと、保護されていないサーバーの情報が表示されます。 ウィジェットには以下のメトリクスが表示されます。 レポート作成時点の、カスタマーのテナントに登録されているサーバーの合計数です。 **保護済み** - 登録されているすべてのサーバーのうち、レポート作成時点で、Disaster Recoveryによって保護されているサーバー（1台または複数の復元サーバーとサーバー全体のバックアップがある）の数です。 **未保護** - レポート作成時点で登録されているすべてのサーバーのうち、保護されていないサーバーの合計数です。

データ漏洩防止ウィジェット

次のトピックでは、**データ漏洩防止**セクションのブロック済み周辺デバイスに関する詳細な情報を示します。

ウィジェットでは、指定した日付範囲のブロック済みデバイスの合計数（デバイスタイプ別の合計数も付記）が表示されます。

- リムーバブルストレージ
- 暗号化リムーバブル
- プリンター
- クリップボード - クリップボードとスクリーンショットキャプチャーのデバイスタイプを含みます。
- モバイル デバイス
- Bluetooth
- 光学ドライブ
- フロッピードライブ
- USB - USBポートとリダイレクトされたUSBポートのデバイスタイプを含みます。
- FireWire
- マッピングされたドライブ
- リダイレクトされたクリップボード- リダイレクトされたクリップボード受信とリダイレクトされたクリップボード送信のデバイスタイプを含みます。

このウィジェットでは、ブロック済みデバイスの数が多い順に7つのデバイスタイプが表示されます。また残りのデバイスタイプは**その他**デバイスタイプとしてまとめて表示されます。

File Sync & Shareウィジェット

次の表に、**File Sync & Share**セクションのウィジェットについての詳細を示します。

ウィジェット	説明
File Sync & Share統計情報	ウィジェットには以下のメトリクスが表示されます。 **使用済みクラウドストレージの合計** - 全ユーザーの使用済みクラウドストレージの合計です。 **エンドユーザー** - エンドユーザーの総数です。 **エンドユーザーあたりの平均ストレージ使用量** - エンドユーザーあたりの平均ストレージ使用量です。 **ゲストユーザー** - ゲストユーザーの総数です。
エンドユーザーごとのFile Sync & Shareストレージ使用状況	このウィジェットでは、ストレージ使用量が以下の範囲に相当する、File Sync & Shareのエンドユーザーの総数が表示されます。 • 0〜1GB • 1〜5GB • 5〜10GB • 10〜50GB • 50〜100GB • 100〜500GB • 500GB〜1TB • 1TB以上

Notaryウィジェット

次の表に、**Notary**セクションのウィジェットについての詳細を示します。

ウィジェット	説明
サイバーNotary統計情報	ウィジェットには以下のNotaryメトリクスが表示されます。 **使用済みNotaryクラウドストレージ** - Notaryサービスで使用済みのストレージの合計サイズです。 **公証済ファイル** - 公証済ファイルの合計数です。 **電子署名済み文書** - 電子署名済み文書と電子署名済みファイルの合計数です。
エンドユーザー全体で公証済のファイル	全エンドユーザーの公証済ファイルの合計数を表示します。ユーザーは、保有する公証済ファイルの数に応じてグループ化されます。 • 最大10件のファイル • 11〜100ファイル • 101〜500ファイル • 501〜1000ファイル

ウィジェット	説明
	• 1000件以上のファイル
エンドユーザー全体で電子署名された文書	ウィジェットには、すべてのエンドユーザーの電子署名された文書と電子署名されたファイルの合計数が表示されます。ユーザーは、保有する電子署名済みの文書とファイルの数に応じてグループ化されます。 • 最大10件のファイル • 11～100ファイル • 101～500ファイル • 501～1000ファイル • 1000件以上のファイル

エグゼクティブサマリレポートを構成する

エグゼクティブサマリレポートの作成時に構成されたレポートの設定をアップデートすることができます。

エグゼクティブサマリレポートの設定をアップデートするには

1. 管理コンソールで **[レポート]** > **[エグゼクティブサマリ]** へ進みます。
2. アップデートしたいエグゼクティブサマリレポートの名前をクリックします。
3. **[設定]** をクリックします。
4. 必要に応じてフィールドの値を変更します。
5. **[保存]** をクリックします。

エグゼクティブサマリレポートを作成する

エグゼクティブサマリレポートを作成し、その内容をプレビューして、レポートの受信者を設定できます。さらに自動的に送信するタイミングをスケジュールすることができます。

エグゼクティブサマリレポートを作成するには

1. 管理コンソールで **[レポート]** > **[エグゼクティブサマリ]** へ進みます。
2. **[エグゼクティブサマリレポートを作成]** をクリックします。
3. **[レポート名]** に、レポートの名前を入力します。
4. レポートの受信者を選択します。
   - すべての直接のカスタマーにレポートを送信する場合は、**[すべての直接のカスタマーに送信]** を選択します。
   - 特定のカスタマーにレポートを送信したい場合
     a. **[すべてのダイレクトカスタマーに送信]** のチェックを外します。
     b. **[連絡先の選択]** をクリックします。
     c. 特定のカスタマーを選択します。検索を使用して、特定の連絡先を簡単に見つけることができ

ます。

d. **[選択]** をクリックします。

5. 範囲を選択:**[30日]** または **[今月]**
6. ファイル形式を選択:**[PDF]**、**[Excel]**、または **[ExcelおよびPDF]**。
7. スケジューリングの設定を構成します。
   - 受信者に対して特定の日時にレポートを送信したい場合:
     a. **[スケジュール済み]** オプションを有効にします。
     b. **[日付（今月）]** フィールドをクリックし、[最終日] フィールドをクリアして、設定したい日付をクリックします。
     c. **[時間]** フィールドに、設定したい時間を入力します。
     d. **[適用]** をクリックします。
   - 受信者に送信せずにレポートを作成したい場合は、 **[スケジュール]** オプションを無効にしてください。
8. **[保存]** をクリックします。

エグゼクティブサマリレポートのカスタマイズ

エグゼクティブサマリレポートに含める情報を決定できます。セクションの追加と削除、ウィジェットの追加と削除、セクション名の変更、ウィジェットのカスタマイズができます。また、ウィジェットやセクションをドラッグアンドドロップすることで、レポートに表示される情報の順番を変更できます。

セクションを追加するには

1. **[項目の追加]** > **[セクションの追加]** をクリックします。
2. **[セクションの追加]** ウィンドウで、セクション名を入力するか、デフォルトのセクション名を使用します。
3. **[レポートに追加]** をクリックします。

セクションの名前を変更するには

1. 名前を変更したいセクションで、**[編集]** をクリックします。
2. **[セクションの編集]** ウィンドウで、新しい名前を入力します。
3. **[保存]** をクリックします。

セクションを削除するには

1. 削除したいセクションで、**[セクションの削除]** をクリックします。
2. **[セクションを削除]** 確認ウィンドウで **[削除]** をクリックします。

デフォルト設定のウィジェットをセクションに追加するには

1. ウィジェットを追加したいセクションで、**[ウィジェットの追加]** をクリックします。
2. **[ウィジェットの追加]** ウィンドウで、追加したいウィジェットをクリックします。

カスタマイズされたウィジェットをセクションに追加するには

1. ウィジェットを追加したいセクションで、**[ウィジェットの追加]** をクリックします。
2. **[ウィジェットの追加]** ウィンドウで、追加したいウィジェットを探してから、**[カスタマイズ]** をクリックします。
3. 必要に応じてフィールドを設定してください。
4. **[ウィジェットの追加]** をクリックします。

デフォルト設定のウィジェットをレポートに追加するには

1. **[項目の追加]** > **[ウィジェットの追加]** をクリックします。
2. **[ウィジェットの追加]** ウィンドウで、追加したいウィジェットをクリックします。

カスタマイズしたウィジェットをレポートに追加するには

1. **[ウィジェットの追加]** をクリックします。
2. **[ウィジェットの追加]** ウィンドウで、追加したいウィジェットを探してから、**[カスタマイズ]** をクリックします。
3. 必要に応じてフィールドを設定してください。
4. **[ウィジェットの追加]** をクリックします。

ウィジェットのデフォルト設定をリセットするには

1. カスタマイズしたいウィジェットで、**[編集]** をクリックします。
2. **[デフォルトにリセット]** をクリックします。
3. **[完了]** をクリックします。

ウィジェットをカスタマイズするには

1. カスタマイズしたいウィジェットで、**[編集]** をクリックします。
2. 必要に応じてフィールドを編集します。
3. **[完了]** をクリックします。

エグゼクティブサマリレポートを送信する

オンデマンドで、エグゼクティブサマリレポートを送信できます。この場合、**[スケジュール済み]** の設定は無視され、レポートは直ちに送信されます。レポートの送信時には、**[設定]** で構成した受信者、範囲、ファイル形式の値が使用されます。これらの設定は、レポートを送信する前に手動で変更することができます。詳細については、"エグゼクティブサマリレポートを構成する"（231ページ）を参照してください。

エグゼクティブサマリレポートを送信するには

1. 管理ポータルで **[レポート]** > **[エグゼクティブサマリ]** へ進みます。
2. 送信したいエグゼクティブサマリレポートの名前をクリックします。
3. **[今すぐ送信]** をクリックします。
   システムにより、選択された受信者にエグゼクティブサマリレポートが送信されます。

レポートのタイムゾーン

レポートで使用されるタイムゾーンは、レポートのタイプによって異なります。参照用の情報を以下の表にまとめます。

レポートのロケーションとタイプ	レポートで使用されるタイムゾーン
管理ポータル > 監視 > 操作 （ウィジェット）	レポート生成時刻は、ブラウザを実行しているマシンのタイムゾーンで表示されます。
管理ポータル > 監視 > 操作 （PDFまたはxslxへのエクスポート）	• エクスポートしたレポートのタイムスタンプは、レポートをエクスポートしたときに使用したマシンのタイムゾーンになります。 • レポートに表示されるアクティビティのタイムゾーンはUTCです。
管理ポータル > レポート > 使用状況 > 定期レポート	• このレポートは各月の最初の日の23:59:59（UTC）に生成されます。 • このレポートは各月の2日に送信されます。
管理ポータル > レポート > 使用状況 > カスタムレポート	レポートのタイムゾーンと日付はUTCです。
管理ポータル > レポート > 操作 （ウィジェット）	• レポート生成時刻は、ブラウザを実行しているマシンのタイムゾーンで表示されます。 • レポートに表示されるアクティビティのタイムゾーンはUTCです。
管理ポータル > レポート > 操作 （PDFまたはxslxへのエクスポート）	• エクスポートしたレポートのタイムスタンプは、レポートをエクスポートしたときに使用したマシンのタイムゾーンになります。 • レポートに表示されるアクティビティのタイムゾーンはUTCです。
管理ポータル > レポート > 操作 （スケジュール配信）	• レポート配信のタイムゾーンはUTCです。 • レポートに表示されるアクティビティのタイムゾーンはUTCです。
管理ポータル > ユーザー > アクティブアラートに関する日次概要	• このレポートは1日1回、10:00から23:59（UTC）の間に送信されます。レポートが送信される時刻は、データセンターのワークロードによって異なります。 • レポートに表示されるアクティビティのタイムゾーンはUTCです。
管理ポータル > ユーザー > サイバープロテクションステータス通知	• このレポートはアクティビティの完了時に送信されます。 **注意** データセンターのワークロードによっては、レポートの送信が遅れることもあります。 • レポートに表示されるアクティビティのタイムゾーンはUTCです。

ウィジェットの種類に応じたレポートのデータ

ダッシュボードのウィジェットは、表示するデータの範囲に応じて2つの種類があります。

- 参照時やレポート作成時に、実際のデータを表示するウィジェット。
- 履歴データを表示するウィジェット。

レポートの設定で特定の期間のデータをダンプするように日付範囲を構成した場合、選択された時間範囲は、履歴データを表示するウィジェットにのみ適用されます。参照した時点の実際のデータを表示するウィジェットの場合、時間範囲のパラメータは適用されません。

次の表は、使用可能なウィジェットとそのデータ範囲の一覧です。

ウィジェット名	ウィジェットやレポートに表示されるデータ
マシンごとの #CyberFit スコア	実際の値
直近 5 件のアラート	実際の値
アクティブアラートの詳細	実際の値
アクティブアラート概要	実際の値
アクティビティ	履歴レポート
アクティビティ一覧	履歴レポート
アラート履歴	履歴レポート
バックアップのマルウェア対策スキャン	履歴レポート
ファイルのマルウェア対策スキャン	履歴レポート
バックアップスキャンの詳細（脅威）	履歴レポート
バックアップステータス	履歴レポート - 列内の**合計実行数**と**正常に完了した実行数** 実際の値 - その他のすべての列について
バックアップストレージの使用状況	履歴レポート
ブロック済みの周辺デバイス	履歴レポート
ブロックされたURL	実際の値
クラウドアプリケーション	実際の値
クラウドワークロードの保護ステータス	実際の値
Cyber protection	実際の値
サイバープロテクションのサマリ	履歴レポート

データ保護マップ	履歴レポート
デバイス	実際の値
テスト済みのディザスタリカバリサーバー	履歴レポート
ディザスタリカバリの統計情報	履歴レポート
検出されたデバイス	実際の値
ディスク状態の概要	実際の値
ディスク状態ステータス	実際の値
物理デバイスごとのディスク状態	実際の値
エンドユーザー全体で電子署名された文書	実際の値
既存の脆弱性	履歴レポート
File Sync & Share統計情報	実際の値
エンドユーザーごとのFile Sync & Shareストレージ使用状況	実際の値
ハードウェアの変更	履歴レポート
ハードウェアの詳細	実際の値
ハードウェアインベントリ	実際の値
アラート概要履歴	履歴レポート
ロケーションサマリー	実際の値
カテゴリ別の未適用アップデート	実際の値
未保護	実際の値
エンドユーザー全体で公証済のファイル	実際の値
Notaryの統計情報	実際の値
パッチインストール履歴	履歴レポート
パッチインストールステータス	履歴レポート
パッチインストール概要	履歴レポート
パッチ適用済みの脆弱性	履歴レポート
インストール済みパッチ	履歴レポート
保護ステータス	実際の値
最近影響を受けたもの	履歴レポート

リモートセッション	履歴レポート
セキュリティインシデントのバーンダウン	履歴レポート
セキュリティインシデントのMTTR	履歴レポート
ディザスタリカバリで保護済みのサーバー	実際の値
ソフトウェアインベントリ	実際の値
ソフトウェアの概要	履歴レポート
脅威のステータス	実際の値
保護技術で検知した脅威	履歴レポート
ワークロードごとの上位インシデントディストリビューション	実際の値
脆弱性のあるマシン	実際の値
ワークロードのネットワークステータス	実際の値
バックアップ済みのワークロード	履歴レポート
ワークロードの保護ステータス	実際の値

Cyber Protect Cloudのコストを計算ツールで推定する

Cyber Protect Cloud の試用版を使用している場合、ビルトインの計算ツールを使って費用を推定することができます。

注意
Cyber Protect Cloud計算ツールは、トライアルモードのカスタマーのみが管理ポータルからアクセスでき、トライアル以外のカスタマーやパートナーはアクセスできません。

Cyber Protect Cloud のコストを計算ツールで推定するには

1. 管理ポータルにログインします。
2. 左下にある **[月単位のコストを計算する]** をクリックします。
3. 計画しているワークロードについて、以下の詳細を指定してください。
   - ワークロードの種類別のワークロード数。例えば、仮想マシン、ワークステーション、ホスティングサーバー、Google Workplaceシート、モバイルデバイス、Microsoft 365シートの数を指定します。
   - データセンターのロケーションやストレージ容量など、データストレージの詳細。
4. （オプション）使用する計画のAdvanced Backup、セキュリティ、または管理オプションと、それぞれのワークロード数を指定します。
5. ライセンスモデルを選択: ワークロード単位またはGB単位。

右側に月単位の料金の目安が表示されます。

パートナーになるには、対応するボタンをクリックします。また、スペシャリストにチャットで依頼したり、クラウドアドバイザーに直接リクエストしたりすることもできます。これらはすべて計算ツールのページから実行できます。

また、管理ポータルの左下にある **[営業へのお問い合わせ]** をクリックすることで、営業部門との連絡を開始することができます。

Copilot

Copilotは、製品内のAIチャットアシスタントです。Copilotは、公式の Cyber Protect Cloud文書とライセンスガイドをソースとして使用し、以下のタスクで補助し、サポートする回答を生成します。

- 製品の動作を理解する。
- ライセンスに関するトピックを理解する。
- テナントの構成方法について理解する。
- サービスの構成方法について理解する。
- 最小限の労力で製品の使用を開始する。
- 機能の使用方法に関する質問に対する迅速な回答を得る。

Copilotが質問に答えられない場合、チャットの内容がライブスペシャリストに転送されます。そのタイミングでスペシャリストが対応できない場合は、チケットが送信されます。

英語だけでなく、母語でもライブスペシャリストとチャットできます。Copilotは、英語以外のすべてのチャットを自動的に翻訳するため、どんな言語でもスペシャリストとコミュニケーションを取ることができます。

チャットウィンドウのピン設定解除を行い、アプリケーションウィンドウ内の任意の場所に移動させることができます。これにより、チャットのロケーションを調整して、自分にとって最も便利な場所に配置することができます

Copilotを使った作業

Copilotは、製品に関する情報とライセンスモデルを提供し、一般的な構成タスクを支援します。より専門的な支援が必要な場合、Copilotからライブスペシャリストに接続することができます。その時点でライブスペシャリストが利用できない場合、Copilotによりチケットが作成されます。スペシャリストは、このチケットを処理するために、可能な限り早いタイミングでユーザーに連絡します。

Copilotとのチャットを評価し、フィードバックを残すことができます。

チャットの開始

Copilotとのチャットを開始するには

1. **[Copilot]** をクリックします。
2. [チャット] ウィンドウが開くので、以下のいずれかの操作を実行します。
   - 定義済みの一般的なトピックまたは質問のいずれかに関する情報を取得するには、該当する箇所をクリックします。

- 他のトピックの情報や他の質問に対する回答を取得するには、メッセージフィールドに入力してから、Enterキーを押すか、矢印アイコンをクリックします。

3. 必要な情報が得られるまで、ステップ2を繰り返します。
4. （オプション） Copilot の返信をコピーするには、返信の下にあるコピー アイコンをクリックします。

   テキストがマシンのクリップボードにコピーされます。

ライブスペシャリストとのチャット

ライブスペシャリストとのチャットを開始するには

1. **[Copilot]** をクリックします。
2. 新しいチャットまたは既存のチャットを開きます。
3. Copilotにライブスペシャリストへの接続を依頼します。

   Copilotは、提供された情報に基づいてチケットの概要を生成し、質問の種類を事前に選択します：非技術的な質問または技術的な質問。
4. Copilotによって生成された情報を確認し、必要に応じて質問の種類を変更し、概要を修正してください。
5. **[送信]** をクリックします。
6. スペシャリストとチャットします。

> **注意**
> スペシャリストがチャットを終了すると、チャットウィンドウにフィードバックフォームが表示されます。

応答の評価

チャットでCopilotの応答を評価できます。

応答を評価するには

1. **[Copilot]** をクリックします。
2. [チャット] ウィンドウが開くので、以下のいずれかの操作を実行します。
   - 定義済みの一般的なトピックまたは質問のいずれかに関する情報を取得するには、該当する箇所をクリックします。
   - 他のトピックの情報や他の質問に対する回答を取得するには、メッセージフィールドに入力してから、Enterキーを押すか、矢印アイコンをクリックします。
3. Copilot の応答を評価するには、次のいずれかを実行します。
   - 役に立った場合は、下の[いいね]アイコンをクリックしてください。
   - 役に立たない場合は、下の[あまり役立たなかった]アイコンをクリックしてください。

チャットの評価

Copilot の応答が含まれるチャットを終了するときに、評価できます。

チャットの評価

1. 有効なチャットウィンドウで、**X** アイコンをクリックします。
   フィードバック フォームが開きます。
2. チャットの体験を評価してください（1-悪い～5-素晴らしい）。
3. テキストフィールドにフィードバックを入力します。

> **注意**
> この手順はスコア1～4では必須ですが、スコア5ではスキップできます。

4. **[フィードバックを送信]** をクリックします。
   チャットウィンドウが閉じます。

チャットを終了します

Copilotとのチャットを終了すると、チャット履歴は削除されません。体験の評価を求められます。

チャットを終了するには

1. 有効なチャットウィンドウで、**X** アイコンをクリックします。
   フィードバックウィンドウが開きます。フィードバックを送信するか、スキップできます。
2. （オプション） フィードバックを送信しない場合は、**スキップ**をクリックします。
   チャットウィンドウが閉じます。チャットを削除するまで、チャットリストからアクセスできます。
   フィードバックを送信していない場合は、チャットを閉じるたびにフォームが表示されます。

チャットの管理

Copilotとのチャットセッションの一覧を表示し、不要なセッションを削除できます。

チャットの一覧を表示してチャットを削除するには

1. **[Copilot]** をクリックします。
2. ハンバーガーアイコンをクリックして、チャットの一覧を表示します。
3. 削除するチャットにホバーして、ゴミ箱アイコンをクリックします。

パートナーポータルの使用

パートナーポータルは、CyberFitパートナープログラムに参加するサービスプロバイダー、ディストリビューター、リセラー向けに設計されています。

パートナーポータルでは、 コンテンツ、ツール、トレーニングにアクセスできます。

パートナーポータルの使用を開始する

1. 次のいずれかの方法でパートナーポータルにアクセスできます。
   - 管理ポータルの左下にある **[パートナーになる]** をクリックする。
   - パートナーポータルのWebサイトにアクセスする。
2. 自社をパートナープログラムに登録します。
3. アクセスの詳細が記載されたEメールが届きます。

パートナーポータルのロール

パートナーポータルでは、必要に応じてユーザーに割り当てることができるいくつかのロールを利用できます。

以下の表では、利用可能な各ロールと、パートナーポータル内で各ロールに割り当てられた権限を説明しています。

ロール	説明
ベーシック	すべてのユーザーに適用されるデフォルトのロールです。 このロールには、パートナーポータルの基本的な機能へのアクセス権が付与されます。これには、ダッシュボード、パートナープログラム、コンテンツハブ、トレーニングが含まれます。
トレーニング	このロールを付与されたユーザーはトレーニング資料にアクセスできます。ただし、パートナーポータルの他の機能は利用できません。
マーケティング	このロールでは、マーケティング担当者に必要なパートナーポータルの機能へのアクセスが許可されます。アクセスできる機能には、ダッシュボード、パートナープログラム、マーケティング、コンテンツハブ、トレーニング、データセンターのステータス、およびデータベース管理が含まれます。
営業	このロールを付与されたユーザーは、ダッシュボード、パートナープログラム、セールス、コンテンツハブ、トレーニング、データセンターのステータス、データベース管理など、営業担当者に必要なパートナーポータルの機能にアクセスできます。
営業およびマーケティング	このロールでは、営業およびマーケティングを兼任する担当者に必要とされるパートナーポータル機能へのアクセスが許可されます。アクセスできる機能には、ダッシュボード、パートナープログラム、セールス、マーケティング、コンテンツハブ、トレーニング、データセンターのステータス、およびデータベース管理が含まれます。
管理者	管理者は、ダッシュボード、パートナープログラム、セールス、マーケティング、コンテンツハブ、トレーニング、データセンターステータス、データベース管理など、パートナーポータルのすべての機能にアクセスできます。さらに、管理者はパートナーユーザーの許可を管理し、会社情報を変更す

ロール	説明
	ることができます。

索引