Cyber Protect Cloud

23.02

パートナー管理者ガイド

リビジョン: 2023/02/28

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のバージョン情報

Cyber Protect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。

このサービスは、パートナーレベル、顧客企業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。

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。

管理ポータルにより、管理者は以下を行うことができます:

- 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
- テナントの管理
- ユーザーアカウントの管理
- サービスとテナントの制限値（クォータ）の設定
- ストレージの管理
- カスタマイズの管理
- サービス使用状況レポートの生成

Cyber Protectサービス

このセクションでは、2021年3月に導入された機能セットと新しい課金モデルについて説明します。 新しい課金モデルの利点について詳しくは、 Cyber Protectデータシートを確認してください。

Cyber Protect Cloudで利用できるサービスと機能セットは次のとおりです:

- **Cyber Protect**
  - **保護** - 基本製品にはセキュリティと管理機能が含まれています。また、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は従量課金制で利用可能であり、これらを活用して包括的なサイバープロテクションを実現できます。この機能は、追加料金を支払ってAdvanced保護パックを使用することで拡張できます。
    Advanced保護パックは、Advanced Backup、Advancedセキュリティなど、個別の機能分野に関するより高度なシナリオを扱う独自機能を集めたものです。Advancedパックは、標準のCyber Protectサービスで利用できる機能を拡張します。
    Advanced Protectionの詳細については、「"Advanced Protectionパック"（119ページ）」を参照してください。
  - **File Sync & Share** - 時間や場所を問わず、どのデバイス上の企業コンテンツであっても安全に共有するためのソリューション。
  - **物理データ配送** - ハードドライブで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。
  - **ノータリー** - 共有コンテンツの真正性を確保するブロックチェーンベースのソリューション。
- **Cyber Infrastructure SPLA**

管理ポータルでは、テナントが利用できるサービスと機能セットを選択できます。「テナントの作成」で説明されているように、構成はテナントのプロビジョニングまたは編集時にテナントごとに行われます。

Cyber Protectの課金モード

課金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。課金モードでは、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。課金モードは、パートナーがカスタマーレベルで設定できます。

ライセンスエンジンにより、保護計画でどの機能がリクエストされているかに応じて、自動的に提供項目が取得されます。ユーザーは、保護計画をカスタマイズすることで、保護のレベルとコストを最適化できます。

注意
各カスタマーテナントで使用できる課金モードは、1種類のみです。

保護コンポーネントの課金モード

保護には2つの課金モードがあります:

- ワークロードあたり
- ギガバイトあたり

どちらの課金モードでも機能セットは同じです。

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の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。付属機能の使用は記録されますが、課金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、"Cyber Protectサービス"（6ページ）で確認できます。

アドバンスドパックがカスタマーに対して有効になっていますが、課金が開始されるのは、カスタマーが保護計画に含まれているパックの機能を使用し始めた後になります。保護計画内にアドバンスド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ワークロードごとに割り当てられます。

アドバンスド機能の利用を停止すると、ライセンスは取り消され、課金も停止されます。ライセンスエンジンは、各機能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。

ライセンスを割り当てることができるのは、Cyber Protectサービスの標準機能のみです。高度な機能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。

注意
Advanced保護機能に対する課金は、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、カスタマーが保護計画内で高度な機能の使用を開始した後になります。機能セットが有効になると、記録され使用状況レポートに含まれますが、機能が使用されない限り課金対象とはなりません。

File Sync & Shareの課金モード

File Sync & Shareには、次の課金モードがあります:

- ユーザーあたり
- ギガバイトあたり

File Sync & Shareのレガシーエディションの課金ルールも適用できます。

注意
Advanced File Sync & Share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、カスタマーが高度な機能の使用を開始した後になります。高度な機能セットが有効になると、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。

ノータリーの課金

ノータリーの課金は、使用量に応じた支払いモデルになります。

レガシーエディションでの課金モデルの使用

現行の課金モデルに移行していない場合、レガシーエディションに代えて、いずれかの課金モードによって提供項目を使用できます。ライセンスエンジンにより、請求額が最も少なくなるように、カスタマーに割り当てられるライセンスが自動的に最適化されます。

注意
エディションと課金モードを混在させることはできません。

レガシーエディションから現行のライセンスモデルへの切り替え

プロファイルを編集し、提供項目を選択することで、テナントへの提供項目を手動で切り替えることができます。切り替えプロセスの詳細については、「"エディションと課金モード間の切り替え"（9ページ）」を参照してください。

複数のカスタマーを対象にエディションから課金モードへ切り替えるには、「複数のカスタマーを対象とした多数のエディションの切り替え（67942）」を参照してください。

エディションと課金モード間の切り替え

管理ポータルでテナントアカウントを変更し、課金モード間（ワークロードあたりからギガバイトあたり、もしくはその逆）、レガシーエディションと課金モード間で提供項目を切り替えることができます。

テナントの切り替えを一括で行う場合の詳細については、「複数のカスタマーを対象とした多数のエディションの切り替え（67942）」を参照してください。

切り替えプロセスには、以下の手順が含まれます。

1. 元の提供項目で利用できた機能に一致するように、新しい提供項目をカスタマーテナントにプロビジョニングする（提供項目を有効にしてクォータを設定する）。
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）。

次の表に、それぞれの場合のプロセスについて示します。

	切り替えの方向	
	エディション>課金モード	**課金モード>課金モード**
提供項目の切り替え	切り替え元のエディションで利用できた機能を満たす提供項目を有効にする。	提供項目と同一のセットが有効になります。
クォータの切り替え	クォータは切り替え元の提供項目から切り替え先の提供項目に複製されます。切り替え元のStandard製品→切り替え先のStandard製品。切り替え元のStandardパック→切り替え先のパック。 **注意** サブエディションがあるエディションから切り替える場合（例:「Cyber Protect（ワークロード単位）」）、クォータはまとめられます。	クォータは切り替え元の提供項目から切り替え先の提供項目に複製されます。
使用状況の切り替え	提供項目は、ワークロードに割り当てられた保護計画でリクエスト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。	

例:Cyber Protect Advanced Editionをワークロード単位の課金に切り替える

このシナリオでは、カスタマーテナントにおいて Cyber Protect Advanced Editionが8台のワークステーション上で使用されており、クォータが10のワークロードに設定されています。3台のワークステーションが保護計画でソフトウェアインベントリとパッチ管理を使用しており、2台のワークステーションが保護計画でURLフィルタリングを有効にしています。そして、1台のマシンが継続的データ保護を使用しています。次の表で、エディションから新しい提供項目への変換について示します。

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
Cyber Protect Advanced Workstation 8/10	• ワークステーション - 8/10 • Advancedセキュリティ - 2/10 • Advanced Backupワークステーション - 1/10 • Advanced管理 - 3/10

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。
2. クォータが新しい提供項目で複製されました。
3. 使用数は保護計画での実際の使用状況に応じて調整されます。具体的には、3つのワークロードでAdvanced管理パックの機能を使用し、2つのワークロードでAdvancedセキュリティパックの機能を使用し、1つのワークロードでAdvanced Backupパックの機能を使用します。

例: Cyber Protectで、ワークロード単位のエディションからワークロード単位の課金へ

この例では、カスタマーが複数のエディションをワークロードに割り当てています。各ワークロードで割り当てられるエディションと課金モードはそれぞれ1つずつのみです。

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
Cyber Protect Essentials Workstation - 6/12	• ワークステーション - 14/42 • Advanced Backupワークステーション - 2/42 • Advancedセキュリティ - 13/42 • Advanced管理 - 5/42
Cyber Protect Standard Workstation - 5/10	
Cyber Protect Advanced Workstation - 2/10	
Cyber Backup Standardワークステーション - 1/10	

切り替え時には、次の手順が実施されました:

1. すべての切り替え元のエディションで利用できた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。

パートナーテナントの課金モードを変更する

パートナーテナントの課金モードを変更するには

1. 管理ポータルで **[クライアント]** へ進みます。
2. 課金モードを変更するパートナーテナントを選択し、省略記号アイコンをクリックしてから **[設定]** をクリックします。
3. **[Cyber Protect]** タブで、課金モードを変更するサービスを選択し、**[編集]** をクリックします。

4. 任意の課金モードを選択し、必要に応じて利用可能な提供項目を有効または無効にします。
5. **[保存]** をクリックします。

カスタマーテナントの課金モードを変更する

次の方法で、カスタマーテナントの課金方式を変更できます。

- 提供項目の有効化または無効化により元の課金モードを編集する。
- 完全に新しい課金モードへの切り替え。

利用可能な提供項目の編集方法の詳細については、「提供項目の有効化または無効化」を参照してください。

カスタマーテナントの課金モードを切り替えるには

1. 管理ポータルで **[クライアント]** へ進みます。
2. エディションを変更するカスタマー テナントを選択し、省略記号アイコンをクリックしてから **[設定]** をクリックします。
3. **[構成]** タブの **[サービス]** 以下で、新しい課金モードを選択します。
   新しい課金モードへの変更を知らせるダイアログがポップアップで表示されます。
4. ユーザー名を入力して、選択内容を確認します。

注意
変更が完了まで最大10分かかります。

提供アイテムおよび制限値（クォータ）管理

このセクションでは、以下について説明します。

- サービス、提供項目とは？
- 提供アイテムはどのように有効または無効となるか？
- 課金モードとは？
- Advanced保護パックとは？
- レガシーエディション、サブエディションとは？
- ソフトおよびハード制限値（クォータ）とは？
- いつハード制限値（クォータ）を超えることができるか？
- バックアップ制限値（クォータ）変換とは？
- 提供アイテムの可用性はサービスコンソールにおけるインストーラ可用性にどのように影響するか？

サービスと提供項目

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サービス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。 Cyber Protectサービスは、保護、File Sync & Share、ノータリー、物理データ配送など、複数のコンポーネントで構成されます。これらはAdvanced保護パックを使用することで、高度な機能による拡張が行えます。 付属機能と高度な機能の詳細については、「"Cyber Protectサービス"（6ページ）」を参照してください。

提供アイテム

提供項目は、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の個別のワークロードの種類または機能ごとにグループ化されたサービス機能の組み合わせです。 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、Advanced保護パックの有効/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"（62ページ）」を参照してください。

機能の使用状況がサービスから収集され、提供項目に反映されます。これはレポートや以降の課金に使用されます。

課金モードとエディション

レガシーエディションでは、ワークロードごとに提供項目を1つ有効にできます。課金モードでは機能が分割されています。そのため、ワークロードごとに複数の提供項目（サービス機能とAdvancedパック）を有効にして、カスタマーのニーズにより適合した内容を提供できます。また、カスタマーが実際に使用している機能だけを対象とした、より正確な課金を行うことができます。

Cyber Protectの課金モードの詳細については、「"Cyber Protectの課金モード"（7ページ）」を参照してください。

課金モードまたはエディションを使用して、テナントで利用できるサービスを構成できます。カスタマーテナント1つにつき、課金モードやエディションを1つ選択できます。つまり、サービス機能ごとに異なる課金モードを適用するために、カスタマー向けに複数のテナントを作成することが必要になります。たとえば、カスタマーがMicrosoft 365メールボックスをギガバイトあたりの課金モードにし、Teamsをワークロードあたりの課金モードにしたい場合は、このカスタマー向けにカスタマーテナントを別個に2つ作成する必要があります。

提供項目でサービスの使用を制限するには、その提供項目のクォータを定義します。"ソフトおよびハード制限値（クォータ）"（13ページ）をご覧ください。

提供アイテムの有効化/無効化

「テナントの作成」で説明されているように、特定のエディションや課金モードではすべての提供項目を有効にできます。

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。

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	使用状況がゼロに等しい場合、無効にすることができます。	ローカル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。
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）のバックアップと復元はカスタマーテナント内で利用できなくなります。
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	使用状況がゼロに等しい場合、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	使用状況がゼロに等しい場合、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。

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。

ソフトおよびハード制限値（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。制限値（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。

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

クライア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. クォータを設定したいクライアントを選択します。
3. **[保護]** タブを選択して **[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**リンクをクリックすると、**[クォータを編集]** ウィンドウが表示されます。

- 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. **[クォータを編集]** ウィンドウで、**[完了]**、**[保存]** の順にクリックします。

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。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シートのライセンス体系は、Cyber Protectionで選択された課金モードによって異なります。
  ワークロード単位の課金モードでは、**Microsoft 365シート**のクォータは一意のユーザーごとにカウントされます。一意のユーザーとは、次のいずれかを少なくとも1つ所有しているユーザーです。
  - 保護対象のメールボックス
  - 保護対象のOneDrive

- 保護対象である少なくとも1件の企業レベルリソースに対するアクセス:Microsoft 365 SharePoint Onlineサイト、またはMicrosoft 365 Teams。
  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。

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"（18ページ）を参照してください。

以下のMicrosoft 365シート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

ギガバイト単位の課金モードで利用できるライセンスオプションの詳細については、Cyber Protect Cloud:Microsoft 365（GB単位のライセンス）を参照してください。
ワークロード単位の課金モードで利用できるライセンスオプションの詳細については、Cyber Protect Cloud:Microsoft 365のライセンスと価格設定の変更を参照してください。

- **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 SharePoint Online**
  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。このクォータにより、SharePoint Onlineサイトの保護機能を有効または無効にします。また、保護できるサイトのコレクションおよびグループのサイトの上限を設定します。
  企業管理者は管理ポータルでクォータを表示できます。企業管理者はまた、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。
- **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。

Microsoft 365シートは、少なくとも1つの保護計画がユーザーのメールボックスまたはOneDriveに適用されていれば、保護されているとみなされます。Google Workspaceシートは、少なくとも1つの保護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。

シート数を超過すると、企業管理者は保護計画をそれ以上のシートに適用できなくなります。

ストレージの制限値（クォータ）

- **ローカルバックアップ**

  ローカルバックアップの制限値（クォータ）は、クラウドインフラストラクチャを使用して作成されたローカル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。
- **クラウドリソース**

  クラウドリソースの制限値（クォータ）は、バックアップストレージのための制限値（クォータ）とディザスタリカバリのための制限値（クォータ）を統合します。バックアップストレージの制限値（クォータ）は、クラウドストレージに保存されてい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制限値（クォータ）容量を超過すると、バックアップは失敗します。

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。

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アイテム制限値（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、サービス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）。

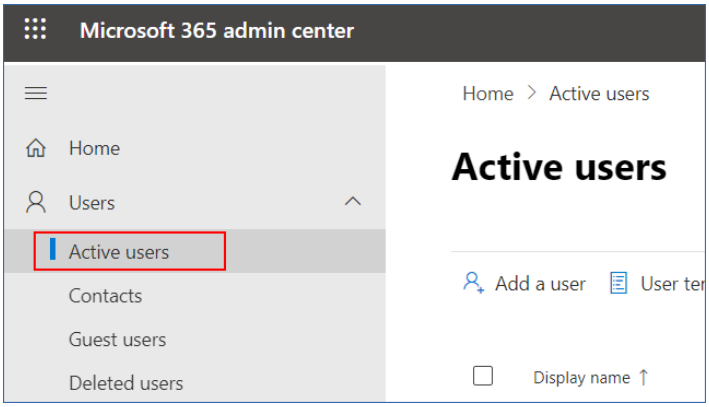
最初に、システムは割り当てられた**仮想マシン**制限値（クォータ）があるかどうかをチェックします。それが見つからない場合、システムは自動的に**ワークステーション**制限値（クォータ）の取得を試みます。それも見つからない場合、他の制限値（クォータ）は自動的に取得されません。**仮想マシン**制限値（クォータ）よりも高コストの制限値（クォータ）が十分にあり、それが仮想マシンに適用可能な場合、サービスコンソールにログインし、手動で**サーバー**制限値（クォータ）を割り当てることができます。

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。

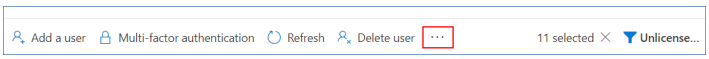
ライセンス対象外のユーザーのサインインを防止するには

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。

Disaster Recovery制限値（クォータ）

注意
ディザスタリカバリ提供項目は、Disaster Recoveryアドオン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。

- **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コールドストレージのサイズを示しています。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や、停止したサーバーの起動が行えなくなります。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、サーバーはサービス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）

テナントのために、以下のFile Sync & Share制限値（クォータ）を定義できます。

- **ユーザー**
  制限値（クォータ）は、このサービスにアクセスできるユーザー数を定義します。
  管理者アカウントは、このクォータの一部としてはカウントされません。
- **クラウドストレージ**
  これはユーザーのファイルを保存するクラウドストレージです。制限値（クォータ）は、クラウドストレージ内でテナントに割り当てられた領域を定義します。

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**
  ノータリー（公証）のストレージは、ノータライズ（公証）済みファイル、署名済みファイル、およびノータリゼーションまたは署名が進行中のファイルが保存されるクラウドストレージです。このクォータは、これらのファイルが占有できる最大の領域を定義します。
  このクォータの使用量を減らすには、既にノータライズ（公証）済みまたは署名済みのファイルをノータリー（公証）のストレージから削除します。
- **ノータリゼーション**
  このクォータは、ノータリー（公証）サービスを使用してノータライズ（公証）できる最大のファイル数を定義します。ファイルは、ノータリー（公証）のストレージにアップロードされるとすぐにノータライズ（公証）済みとみなされ、ノータリゼーションステータスが [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。
- **eSignatures**
  このクォータは、ノータリー（公証）サービスを使用して署名できる最大のファイル数を定義します。ファイルは署名のために送信されるとすぐに署名済みとみなされます。

マシンのサービスクォータの変更

マシンの保護レベルは、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、マシン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、保護計画が最初にマシンに適用されるときに、自動的に割り当てられます。

保護されているマシンの種類、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。
- デスクトップのWindows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上で動作し、プロテクションエージェントがゲストオペレーティングシステム内にインストールされているデスクトップマシン（例: Windowsエージェント）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の場合、**仮想マシン**クォータが使用できないときに、**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、同じマシンにさらに高度な保護計画を適用するには、マシン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マシン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、それを別のマシンに割り当てることもできます。

個別マシンまたはマシンのグループのサービスクォータを変更できます。

個別マシンのサービスクォータを変更するには

1. Cyber Protectionサービスコンソールで **[デバイス]** に進みます。
2. 対象のマシンを選択して、**[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. **[ライセンスの変更]** ウィンドウで、希望する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。

マシンのグループのサービスクォータを変更するには

1. Cyber Protectionサービスコンソールで **[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. **[ライセンスの変更]** ウィンドウで、希望する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。

提供アイテムにおけるエージェントインストーラ依存関係

許可された提供アイテムに応じて、対応するエージェントインストーラがサービスコンソールの**[デバイスの追加]** セクションで使用可能になります。下の表では、有効な提供アイテムに応じて、エージェントインストーラとサービスコンソールでの可用性を見ることができます。

有効な提供アイテム / エージェントインストーラ	サーバー	ワークステーション	仮想コンピュータ	Microsoft 365シート	Google Workspaceシート	モバイルデバイス	Webホスティングサーバー	Webサイト
ワークステーション - Windowsエージェント		+	+					+
ワークステーション - Mac OSエージェント		+	+					+
サーバー - Windowsエージェント	+		+				+	+
サーバー - Linuxエージェント	+		+				+	+
エージェント for Hyper-V			+					
エージェント for VMware			+					
エージェント for			+					

Virtuozzo								
エージェント for SQL	+		+					
Exchangeエージェント	+		+					
エージェント for Active Directory	+		+					
Microsoft 365 エージェント				+				
Google Workspaceエージェント					+			
Windows用のフルインストーラ	+	+	+				+	+
モバイル（iOSおよびAndroid）						+		

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 29以降
- Mozilla Firefox 23以降
- Opera 16以降
- Microsoft Edge 25以降
- macOSおよびiOSオペレーティングシステムで稼働するSafari 8以降

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。

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"（24ページ）を参照してください。

パスワード要件

ユーザーアカウントのパスワードは9文字以上にする必要がありますまた、パスワードの複雑さもチェックされ、以下のいずれかのカテゴリに分類されます。

- 弱
- 中
- 強

9文字以上であっても、脆弱性のあるパスワードを保存することはできません。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。

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

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、受信したアカウント承認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. パスワードを入力して **[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. 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、アクティブ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。

企業プロファイルウィザードで連絡先を構成する

所属会社の連絡先を設定できます。指定されたの連絡先には、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。

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。

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。

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. **会社情報**で、所属会社に関する以下の情報を提供します。
   - **正式な（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（名前）** - 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. 課金連絡先を業務連先または技術連絡先としても使用する場合は、**課金連絡先**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。「会社の連絡先の構成」で説明されているように、管理コンソールの **[会社の管理]** > **[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。

管理ポータルからCyber Protection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。

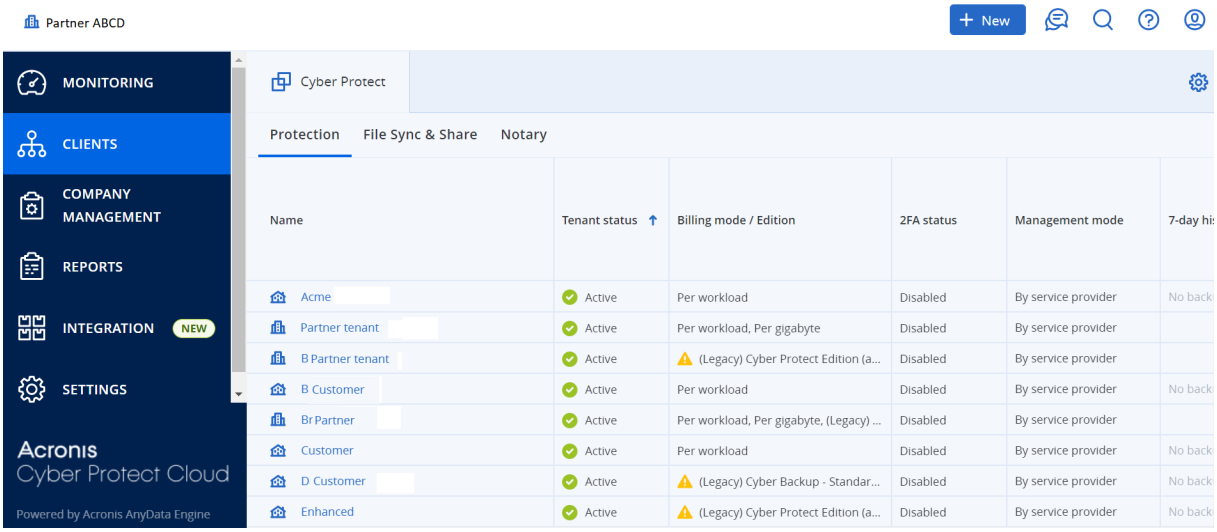
   または、**[クライアント]** の下でカスタマーを選択してから、**[サービスの管理]** をクリックします。

これにより、Cyber Protectionコンソールにリダイレクトされます。

管理ポータルにおけるテナントの指定

管理ポータルを使用する場合、対象となるテナントを指定して操作します。左上にはこのテナントの名前が表示されています。

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テナントのみが表示されます。
- **[企業管理]** 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。

Webインターフェー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。

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ている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. **[ログイン制御]** 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。

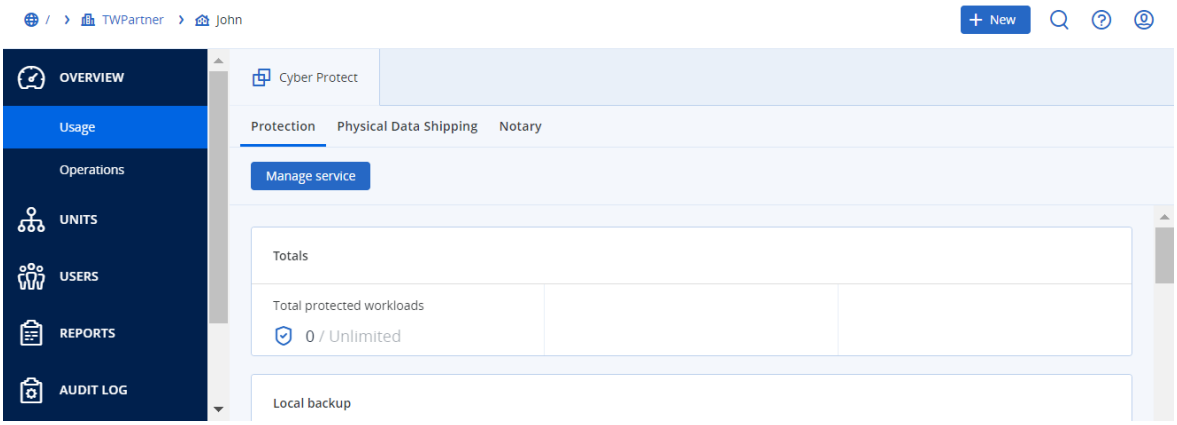
サービスへのアクセス

[概要] タブ

[概要] > **[使用状況]** セクションでは、サービスの使用状況 の概要が表示され、操作中のテナントのサービスにアクセスすることができます。

[概要] タブを使用してテナントのサービスを管理する方法

1. サービスを管理するテナントに移動し、**[概要]** > **[使用状況]** をクリックします。
   一部のサービスはパートナーテナントと顧客テナントレベルで管理できますが、他のサービスは顧客テナントレベルでのみ管理できることに注意してください。
2. 管理するサービスの名前をクリックし、**[サービスの管理]** または **[サービスの設定]** をクリックします。
   サービスの使用方法については、サービスコンソールで使用可能なユーザーガイドを参照してください。



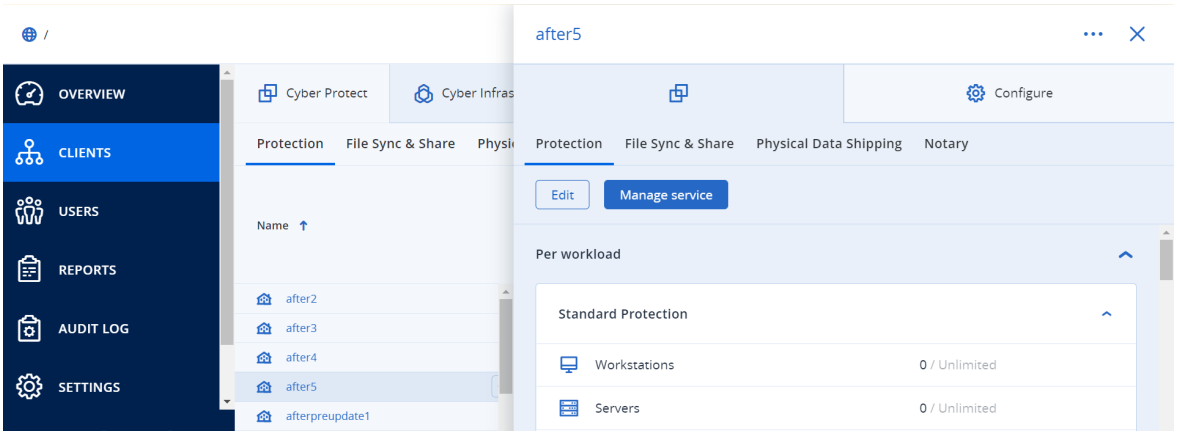
[クライアント] タブ

[クライアント] タブには操作中のテナントの子テナントが表示され、その中のサービスにアクセスすることができます。

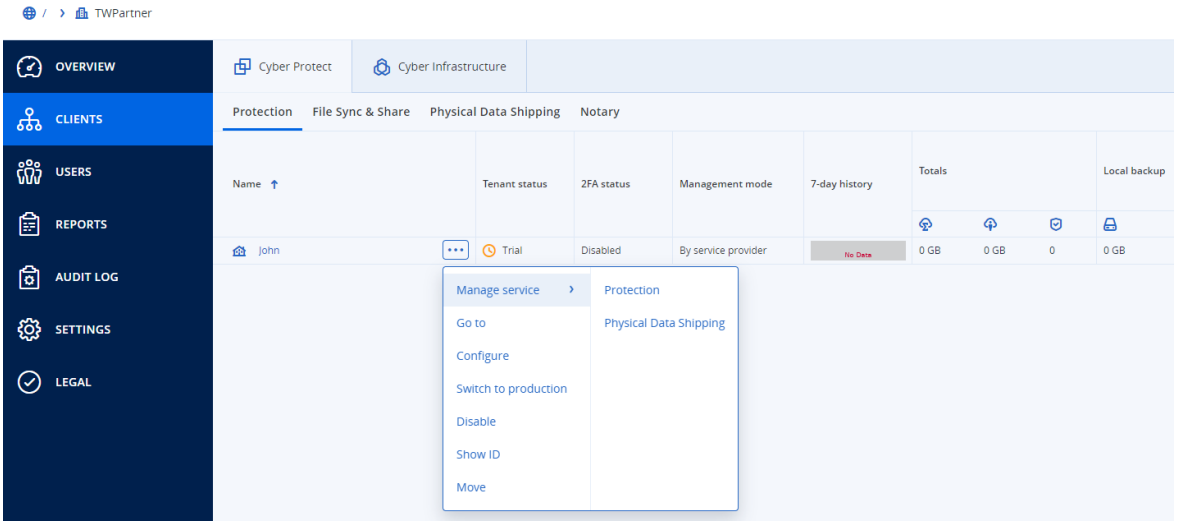
[クライアント] タブを使用してテナントのサービスを管理する方法

1. 次のいずれかを実行します。
   - **[クライアント]** をクリックして、サービスを管理するテナントを選択し、管理するサービスの名前またはアイコンをクリックしてから、**[サービスの管理]** または **[サービスの設定]** をクリックし

ます。



- **[クライアント]** をクリックして、サービスを管理するテナントを選択し、サービスを管理するテナント名の横にある省略記号アイコンをクリックしてから、**[サービスの管理]** をクリックして、管理するサービスを選択します。



一部のサービスはパートナーテナントと顧客テナントレベルで管理できますが、他のサービスは顧客テナントレベルでのみ管理できることに注意してください。

サービスの使用方法については、サービスコンソールで使用可能なユーザーガイドを参照してください。

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

色	説明
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。

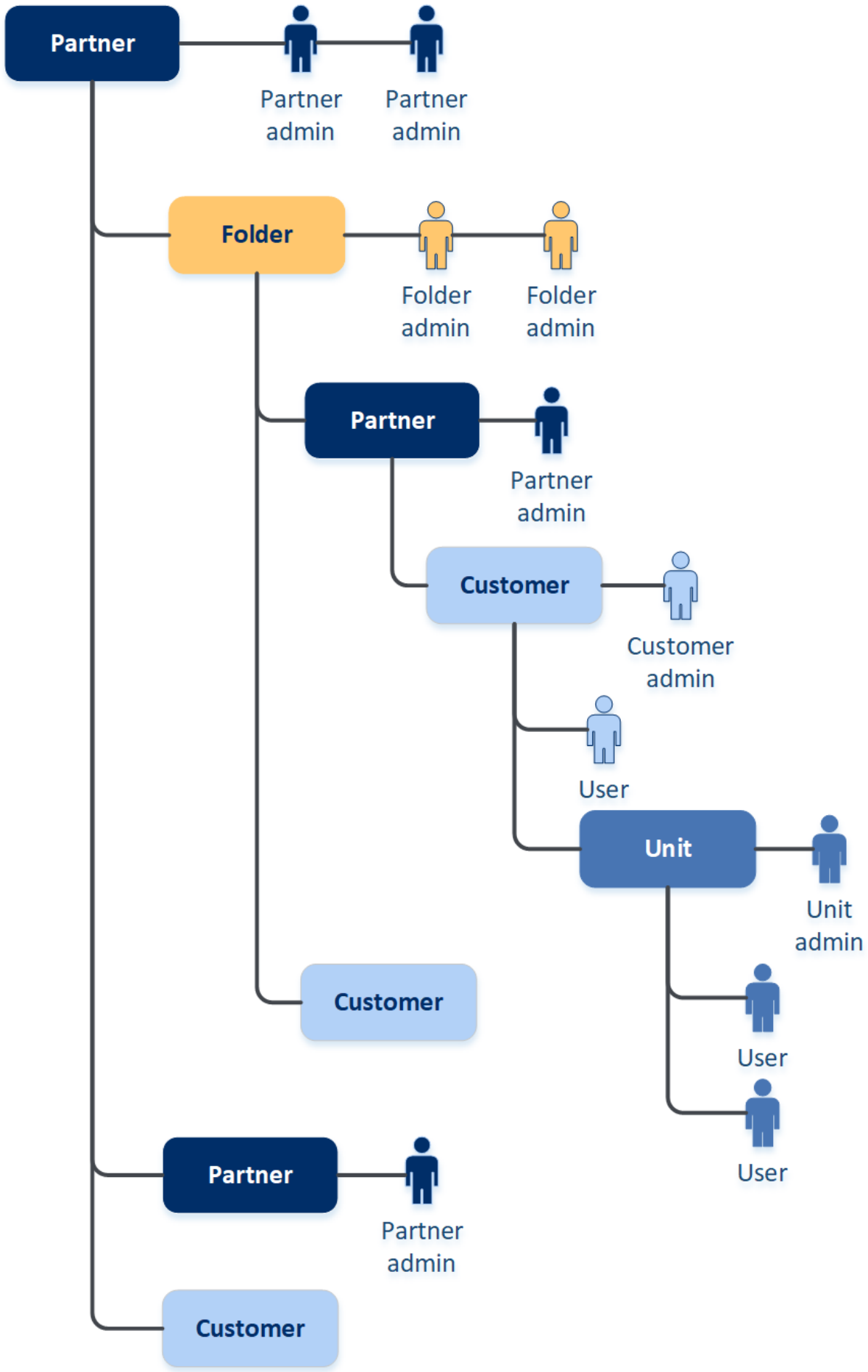
それぞれのアカウントはテナントに属しています。テナントは、パートナーや顧客専用の管理ポータルリソース（ユーザーアカウントや子テナントなど）とサービス提供（有効なサービスとその中のソリューションアイテム）の一部です。テナント階層は、サービスユーザーとプロバイダーの間のクライアント/ベンダーの関係と一致させる必要があります。

- **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**カスタマー**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	×*
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

*これらの操作を実行する必要があるパートナー管理者は、顧客管理者またはユーザーアカウントを自身で作成できます。

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、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を設定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、サービスを新しい組織単位（OU）に拡張するために、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選択します。
3. テナントの提供項目を構成します。

テナントの作成

1. 管理ポータルにログインします。
2. 新規作成する対象のテナントを指定します。
3. 右上にある **[新規]** をクリックしてから、作成するテナントの種類に応じて、次のいずれかをクリックします:
   - **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、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を設定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、サービスを新しい組織単位（OU）に拡張するために、カスタマーのテナント内に作成されます。

4. **[名前]** で、新しいテナントの名前を指定します。
5. （パートナーテナント作成時のみ）**正式な（法的な）会社名**（必須）と、**付加価値税番号/納税者ID/会社登録番号（オプション）**を入力してください。
6. [顧客テナントを作成する場合のみ] **[モード]** で、試用版モードまたは製品版モードでテナントがサービスを使用するかどうかを選択します。月次サービス使用状況レポートには、試用版モードのテナントの使用状況データは含まれません。

重要

月の途中でモードをトライアル版から製品版に切り替えた場合、その月全体のデータが月次サービス使用状況レポートに反映されます。このため、月の初めにモードを切り替えることをおすすめします。テナントが丸1ヵ月間トライアル版で利用された場合、自動的に製品版に切り替わります。

テナントのトライアルモードを自動的に製品モードに切り替えるには、次の2つのシナリオが考えられます。

- 月の途中の場合は、***次の***1か月分も使用状況レポートに反映されます。
- （推奨オプション）月の初日 - その場合、当月のみカウントされます。

---

7. **管理モード**で、テナントへのアクセスを管理するモードを以下から選択します。
   - **セルフサービス** - 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、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。
   - **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テナントへのフルアクセス（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。

   セルフサービスの場合、管理モードの変更が行えるのは作成したテナントの管理者のみです。変更するには、作成したテナントの管理者で **[設定]** > **[セキュリティ]** に移動し、**サポートアクセス**スイッチを設定します。

   [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。
8. **[セキュリティ]** では、テナントの二要素認証を有効または無効にすることができます。
   有効にすると、テナントのすべてのユーザーでアカウントの二要素認証の設定が必須になり、さらなるセキュアアクセスが実現できます。ユーザーは、2つ目の要素となるデバイスに認証アプリケーションをインストールし、コンソールへのログイン時には、従来のログインとパスワードに合わせて1回限りでその都度生成されるTOTPコードを使用する必要が生じます。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。
9. （カスタマーのテナントが強化セキュリティモードで作成された場合のみ）**[セキュリティ]** で、**[強化セキュリティモード]** 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。そうでない場合、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、"強化セキュリティモード"（34ページ）を参照してください。

重要
テナント作成後に、強化セキュリティモードを無効にすることはできません。

10. **[管理者を作成]** 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およびパートナーテナントの場合、管理者の作成が必須となります。

a. 管理者アカウントのログイン名と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。
b. 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。
c. 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。

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。

11. **[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。
12. 次のいずれかを実行します。
- テナントの作成を終了するには、**[保存して閉じる]** をクリックします。この場合、すべてのサービスはテナントに対して有効になります。保護サービスの課金モードはワークロードあたりに設定されます。
- テナントのサービスを選択するには、**[次へ]** をクリックします。"テナントのサービスの選択"（35ページ）をご覧ください。

強化セキュリティモード

強化セキュリティモードでは、厳格なセキュリティ要件を運用しているクライアントに対して特別な設定を提供します。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。

パートナー管理者は、新しいカスタマーテナントを作成するときにのみ、セキュリティ強化モードを有効にすることができます。後からこのモードを無効にすることはできません。既存のテナントでセキュリティ強化モードを有効にすることはできません。

セキュリティ強化モードでは、カスタマーテナントとそのユニットに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ビットキーで自動的に暗号化されます。ユーザーは保護されたデバイスでのみ暗号化パスワードを設定することができます。保護計画で暗号化パスワードを設定することはできません。

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、セキュリティ強化モードのテナントでは、以下の機能を利用できません。

- サービスコンソールを介した復元
- サービス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
- 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

制限事項

- 強化セキュリティモードは、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。
- 強化セキュリティモードは、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。

テナントのサービスの選択

デフォルトでは、新しいテナントを作成すると、すべてのサービスが有効になります。テナント内のユーザーとその子テナントで利用できるサービスを選択できます。

また、既存の複数のテナントに対して、1回の操作でサービスを選択し、有効化することができます。詳細については、"複数の既存テナントへのサービス提供を有効化する"（37ページ）を参照してください。

この手順は部署テナントには適用されません。

テナントのサービスを選択するには

1. 作成/編集テナントダイアログの **[サービスを選択]** セクションで、課金モードかエディションを選択します。
   - **[ワークロード単位]** か **[ギガバイト単位]** の課金モードを選択し、テナントで無効にするサービスのチェックボックスをオフにします。
     どちらの課金モードでもサービスのセットは同じです。

Advancedディザスタリカバリの場合、独自のディザスタリカバリロケーションをアカウントに登録していれば、ドロップダウンリストからディザスタリカバリ用のロケーションを選択できます。

- レガシーエディションを使用するには、**[レガシーエディション]** ラジオボタンを選択し、ドロップダウンリストからエディションを選択します。

無効なサービスは、テナントとその子テナント内のユーザーには表示されません。

2. 次のいずれかを実行します。
   - テナントの作成を終了するには、**[保存して閉じる]** をクリックします。この場合、選択されたサービスのすべての提供項目が、クォータの制限なくテナントで有効になります。
   - テナントの提供項目を構成するには、**[次へ]** へクリックします。"テナントの提供項目の構成"（36ページ）をご覧ください。

テナントの提供項目の構成

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。

この手順は部署テナントには適用されません。

テナントの提供項目を構成するには

1. 作成/編集テナントダイアログの **[構成サービス]** セクションの各サービスタブで、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。

   注意
   Advanced保護機能に関連する提供項目は無効にできますが、ユーザーが保護計画で高度な機能を有効にすると、自動的に再度有効になります。

2. 一部のサービスに対しては、新しいテナントが使用できるストレージを選択できます。ストレージはロケーション別にグループ化されます。テナントが利用できるロケーションとストレージのリストから選択できます。
   - 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。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。

   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」を参照してください。
3. アイテムの制限値（クォータ）を指定するには、提供アイテムの横にある **[無制限]** リンクをクリックします。

これらの容量は「ソフト」です。これらの値のいずれかを超過した場合、テナント管理者と親テナントの管理者にメール通知が送信されます。この場合、サービスの使用に関する制限は適用されません。パートナーテナントの場合、提供アイテムの使用量がクォータを超過することが予想されます。これは、パートナーテナントの作成時に平均値を設定できないためです。

4. [顧客テナントの作成時のみ] 追加容量を指定します。
   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。
5. **[保存して閉じる]**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、編集するセクションの鉛筆アイコンをクリックします。

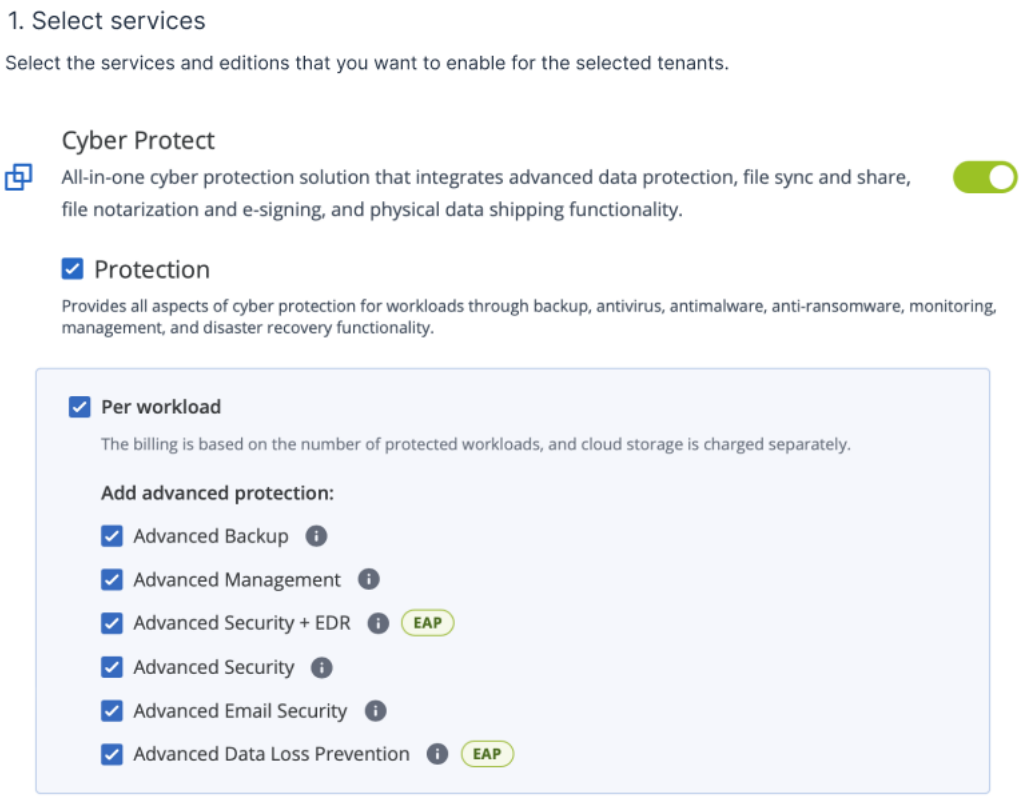
複数の既存テナントへのサービス提供を有効化する

複数のテナントに対して、サービス、エディション、パック、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、サブルート、パートナー、フォルダ、およびカスタマーの各テナントに適用されます。これらの異なるタイプのテナントを同時に選択できます。

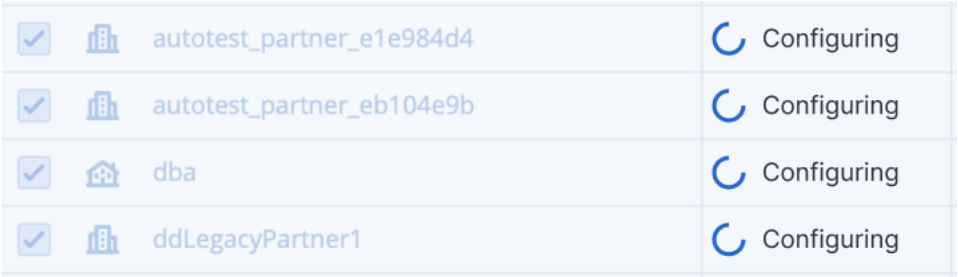
複数テナントのサービスを有効化するには

1. 管理ポータルで **[クライアント]** へ進みます。
2. 右上にある **[サービスを構成]** をクリックします。
3. サービスを有効にするテナント名の横にあるチェックボックスを選択して、**[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関連サービスを選択し、**[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、エディション、および提供項目は、有効な状態が維持されます。

5. **[サービスを構成]** 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、適用されるテナントの選択したサービスや提供項目がすべて表示されます。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）。



8. 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

パートナーユーザーは、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。

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. **[企業管理]** > **[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。

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. **[構成]** 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。

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。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。

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。

社内の連絡先を構成するには

1. 管理コンソールで、**[会社の管理]** > **[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。

       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（名前）** - 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。

      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、**[構成]** 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。

         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（名前）** - 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。

      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。

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、 の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る場合、親テナント管理者はテナントのプロパティのみを変更できます。アカウントと子テナントはまったく表示されません。

上位層の管理者がテナントにアクセスできないようにするには

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。

無効にすると、親テナントの管理者によるテナントへのアクセスが制限されます。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、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。

サポートアクセススイッチが有効になると、親テナントの管理者にはテナントへのフルアクセスが付与されます。親テナントの管理者は、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が行えるようになります。

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。

重要
テナントを削除すると、元に戻すことはできません。

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。

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/ユニット管理者アカウント - カスタマー/見込み客/ユニットそれぞれへのアクセス許可が制限されている他のユーザーに、サービス管理を委任するためのアカウントです。
- 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。["管理ポータルにおけるテナントの指定"（26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、**[企業管理]** > **[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:
   - **ログインID**

     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。

   - **Eメール**

     重要
     ユーザーがFile Sync & Shareサービスに登録している場合、File Sync & Share登録に使用したEメールアドレスを指定してください。
     なお、カスタマーのユーザーアカウントには、それぞれ一意のEメールアドレスが必要です。

   - **名**
   - **姓**
   - （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]** 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。

   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権限を選択します。

   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権限がある場合と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、ユーザーは選択したサービスにおける選択したロールを持ちます。
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、**[企業管理]** 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 **[企業管理]** > **[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（例えば、 Cyber Infrastructureの登録）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。

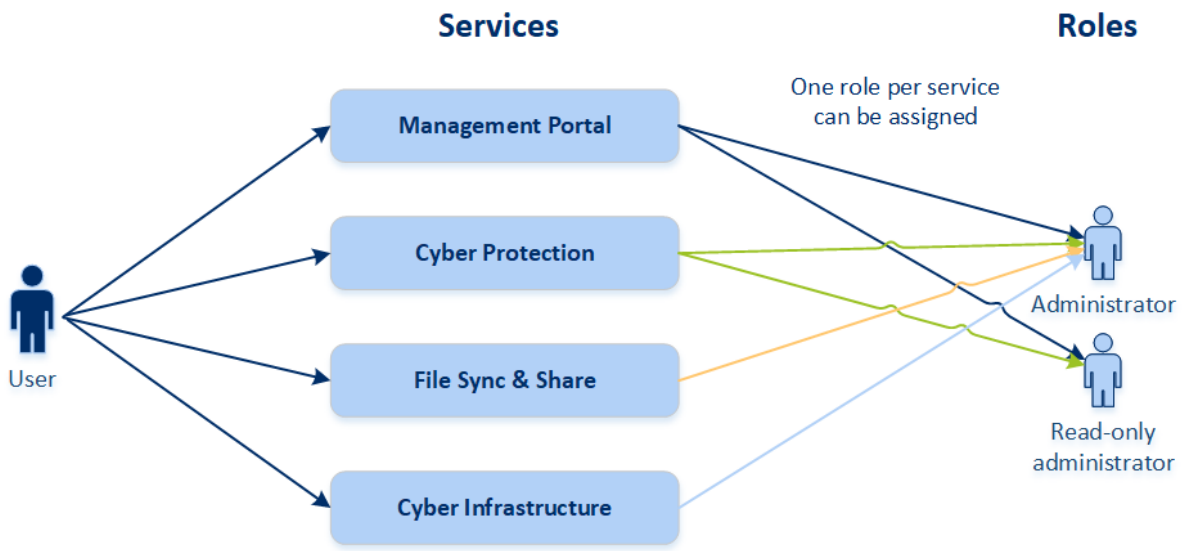
ユーザーアカウントをサービスアカウントタイプに変換するには

1. 管理ポータルで **[企業管理]** > **[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

ユーザーには複数のロールを設定できますが、1つのサービスに指定できるロールは1つだけです。



各サービスでは、ユーザーにどのロールを割り当てるか定義できます。

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。 このロールにより、企業の許可リストへのアクセスを許可します。企業向けのCyber ProtectionサービスのDisaster Recoveryアドオンが有効になっている場合、このロールによりディザスタリカバリ機能へのアクセスを許可します。
管理ポータル	管理者	このロールにより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。

	読み取り専用管理者 パートナーレベル	このロールでは、パートナーの管理ポータルにあるすべてのオブジェクトと、このパートナーの全カスタマーの管理ポータルに対する読み取り専用アクセスが提供されます。このロールを割り当てられたユーザーは、組織に属する他のユーザーのデータに読み取り専用モードでアクセスできます。
	読み取り専用管理者 カスタマーレベル	このロールでは、企業全体の管理ポータル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。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読み取り専用モードでアクセスできます。
	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。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読み取り専用モードでアクセスできます。
Cyber Protection	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、Cyber Protection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、Advanced Managementパックを有効にしたテナントでのみ利用可能です。
	管理者	このロールにより、カスタマーのCyber Protectionの設定と管理が可能になります。 このロールは、ディザスタリカバリ機能と企業の許可リストを構成および管理するために必要です。
	読み取り専用管理者	このロールでは、Cyber Protectionサービスの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。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読み取り専用モードでアクセスできます。 読み取り専用の管理者が、ディザスタリカバリ機能または企業の許可リストを構成および管理することはできません。
	演算子を復元	このロールは、Microsoft 365およびGoogle Workspace組織のバックアップへのアクセスを提供します。これにより、機密コンテンツへのアクセスを制限しながら、必要な復元操作を実行できるようになります。
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。

読み取り専用管理者ロール

このロールを付与されたアカウントは、Cyber ProtectionWebコンソールに読み取り専用でアクセスできます。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。

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。
- 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できません。

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。

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

復元オペレータロール

このロールは、Cyber Protection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うことができます。

- 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参照し、リフレッシュする。
- 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。復元オペレータは、バックアップされたファイルの名前、Eメールの件名、および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。
- カスタムロケーションにバックアップをリカバリする際に、フォルダの作成、削除、名前の変更を行う。
- 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。

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、自分のテナントとその子テナント内のオブジェクトを管理できます。上位の管理者レベルのオブジェクトがある場合、そのオブジェクトを閲覧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。

- 企業管理者

  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。

<table>
<tr><th rowspan="2">ロール</th><th rowspan="2">目的</th><th colspan="3">スクリプトのステータス</th></tr>
<tr><th>下書き</th><th>テスト中</th><th>承認済み</th></tr>
<tr><td rowspan="2">サイバー管理者
企業管理者</td><td>スクリプト計画</td><td>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</td><td>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</td><td>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</td></tr>
<tr><td>スクリプト</td><td>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</td><td>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</td><td>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</td></tr>
<tr><td>管理者
ユーザー（それぞれが所有するワークロード）</td><td>スクリプト計画</td><td>表示
取り消し
無効にする
停止</td><td>表示
実行をキャンセル</td><td>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</td></tr>
</table>

	スクリプト	作成 編集 クローンを作成 削除 実行をキャンセル	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
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

ユーザー向け通知設定の変更

ユーザーの通知設定を変更するには、**[企業管理]** > **[ユーザー]** に移動します。通知を設定するユーザーを選択し、**[設定]** セクションの鉛筆アイコンをクリックします。以下の通知設定は、ユーザーを作成したテナントでCyber Protectionサービスが有効になっている場合に利用できます。

- **クォータの超過に関する通知**（デフォルトで有効）
  クォータの超過に関する通知。
- **スケジュール済み使用状況レポート**（デフォルトでは有効）
  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**（デフォルトでは無効）
  Cyber Protectクラウドサービスのカスタム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。
- **失敗に関する通知**、**警告通知**、および**成功の通知**（デフォルトで無効）
  保護計画の実行結果および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です。
- **アクティブアラートに関する日次概要**（デフォルトで有効）
  日時概要は、サービス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、概要の生成と同じタイミングで生成されます。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、アクティブ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クリアした場合や、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**（デフォルトでは無効）
  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。
- **復元通知**（デフォルトでは無効）
  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**（デフォルトでは無効）
  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。
- **セキュリティインシデント通知**（デフォルトでは無効）
  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。
  2種類のオプションが利用可能です:**[軽減済み]** と **[軽減されていない]** です。これらのオプションは、エンドポイント検知と応答（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）に関連しています。
  EDRアラートが作成されると、該当するユーザーに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た場合、新しいEメールが送信されます。このEメールには、ユーザーがインシデントの詳細を確認したり（インシデントが軽減された場合）、インシデントを調査して修復したり（インシデントが軽減されなかった場合）できるようにするための操作ボタンが含まれています。
- **インフラ通知**（デフォルトでは無効）
  ディザスタリカバリインフラの問題に関する通知: ディザスタリカバリ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。

通知はすべてユーザーの電子メールアドレスに送信されます。

ユーザーロールごとの受信通知

Cyber Protectionが送信する通知は、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	ユーザー	カスタマー管理者
自身のデバイスに関する通知	はい	はい
組織内のすべてのデバイスに関する通知	使用不可	はい（**セキュリティインシデントの通知**以外）
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

通知タイプ¥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。

無効にしたユーザーアカウントを有効にするには、ユーザーリストでそのアカウントを選択し、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。

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。

重要
ユーザーアカウントを削除すると、元に戻すことはできません。

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。

- そのユーザーアカウントが削除されます。
- 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。

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。

二要素認証を設定

二要素認証（2FA）は複数の要素による認証の一種で、2つの異なる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。

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。

仕組み

1. 組織レベルで二要素認証を有効にします。
2. すべての組織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。推奨オーセンティケータ:
   - 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TOTPシークレットを使用し、認証アプリケーションへ手動で追加できます。

   重要
   保存することを強くお勧めします（QRコードの印刷、TOTPシークレットの記録、クラウドへのコードのバックアップをサポートするアプリケーションの使用）。第2要素デバイスを紛失した場合、二要素認証をリセットするためにTOTPシークレットが必要になります。

6. ワンタイム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。
7. ユーザーは、パスワードの入力後に「二要素認証を設定」スクリーン上でTOTPコードを入力する必要があります。
8. 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。

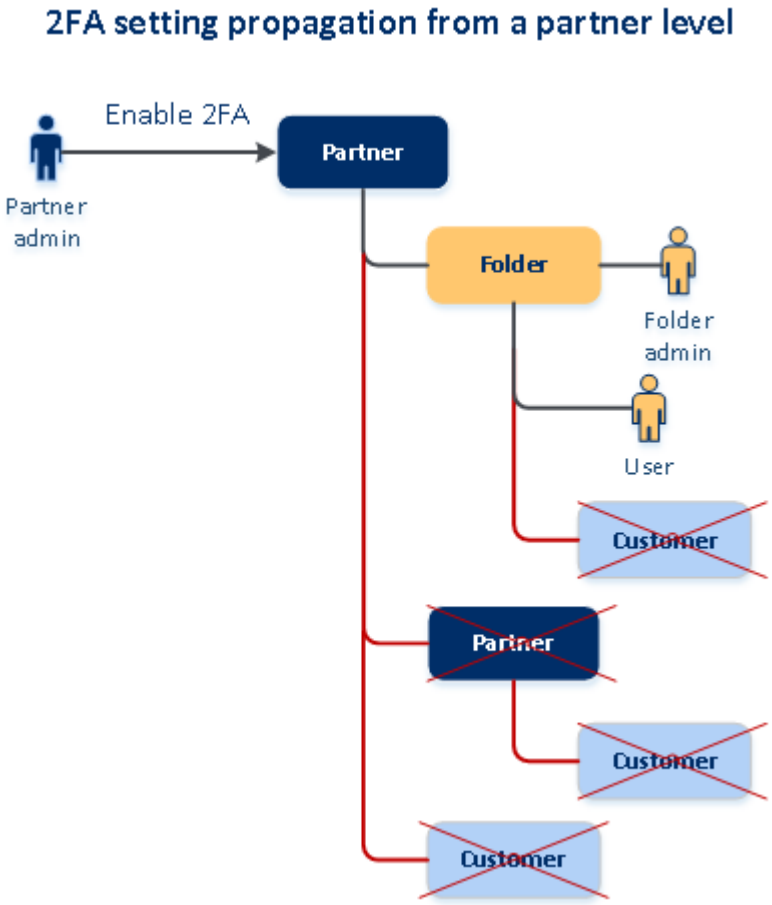
二要素設定のテナントレベル内での伝達

二要素認証は**組織**レベルで設定されます。二要素認証を有効または無効にすることができます。

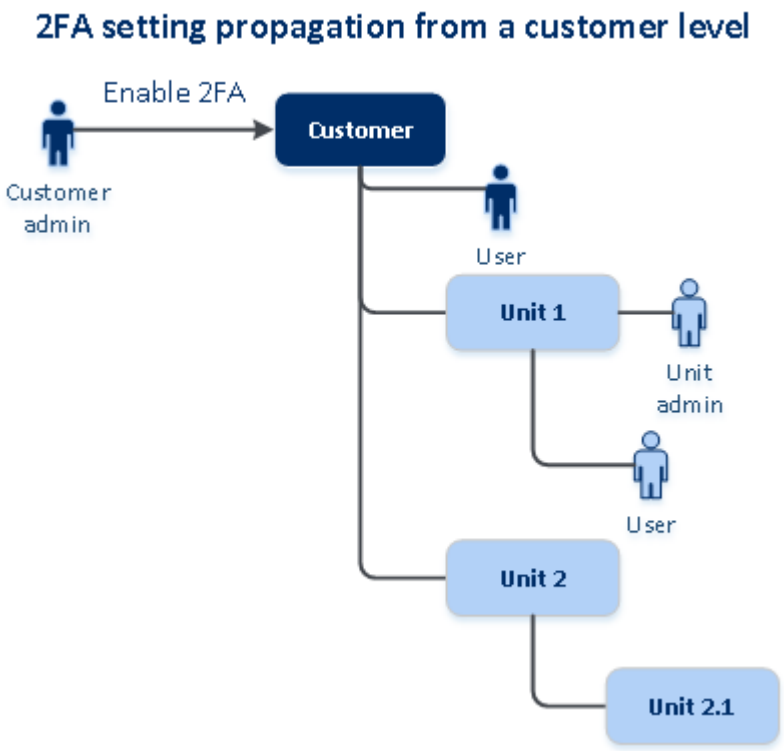
- 自分の組織について。
- 子テナントについて（**サポートアクセス**オプションがその子テナント内で有効になっている場合のみ）。

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を設定

管理者は、組織で二要素認証を有効にすることができます。

テナントの二要素認証を有効にするには

1. 管理ポータルで **[設定]** > **[セキュリティ]** へ進みます。
2. **[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、**[企業管理]** > **[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]** となります。

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。

テナントの二要素認証を無効にするには

1. 管理ポータルで **[設定]** > **[セキュリティ]** へ進みます。
2. 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。
3. （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。

結果として、組織用の二要素認証が無効になり、すべての秘密情報が削除され、信頼済みブラウザーはすべて無効になります。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。**[企業管理]** > **[ユーザー]** タブの **[2FAステータス]** 列は非表示となります。

ユーザーの二要素認証を管理する

管理ポータルの **[企業管理]** > **[ユーザー]** タブから、すべてのユーザーに関する二要素認証設定の監視と設定のリセットを実行できます。

監視

管理ポータルの **[企業管理]** > **[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 **[企業管理]** > **[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。

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 **[企業管理]** > **[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。

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 **[企業管理]** > **[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。

ユーザーの二要素認証を有効にするには

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 **[企業管理]** > **[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。

Cyber Protectionにはいくつかのレガシーエディションがあり、それぞれ機能や価格が異なっています。基本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備えたより上位のエディションをおすす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化または無効化できます。デフォルトでは、アップセルオプションは無効化されています。カスタマー向けのアップセルを有効にすると、カスタマーには追加の機能が表示されるようになります。ただしこれらの機能は、カスタマーが販促対象のエディションを購入するまで利用できません。この追加の機能は、販促対象のエディションの名前またはアイコンを示すラベルでマークが付けられます。名前やアイコンはすべてオレンジ色で強調表示されます。これらのアップセル要素をカスタマー側に表示することで、より上位のエディションを購入するモチベーションを高めることができます。これらのアップセル要素をクリックすると、カスタマー側により上位のエディ

ションの購入を促すダイアログが表示されます。該当のエディションを購入すると希望の機能が有効になります。

アクション項目は、カスタマーユーザーのタイプによって異なります。ユーザーのタイプ（購入者または非購入者）は、プラットフォームAPIで設定できます。詳細については、APIのマニュアルを参照してください。カスタマー側に表示されるアクション項目の詳細については、次の表を参照してください。

カスタマーテナントでのユーザーのタイプ	アクション項目
管理者、購入者	ユーザーインターフェースに、**[今すぐ購入]** ボタンが表示されます。*
管理者、非購入者	ユーザーインターフェースに、「エディションをアップグレードする場合は、パートナーにご連絡ください」というメッセージが表示されます。
ユーザー、購入者	ユーザーインターフェースに、「エディションをアップグレードする場合は、パートナーにご連絡ください」というメッセージが表示されます。
ユーザー、非購入者	ユーザーインターフェースに、「エディションをアップグレードする場合は、パートナーにご連絡ください」というメッセージが表示されます。

* **[今すぐ購入]** ボタンのリンクにより、カスタマーはより上位のエディションを購入するWebサイトにリダイレクトされます。これは、**[設定]** > **[カスタマイズ]** で設定できます。**[アップセル]** セクションで、**[購入URL]** を指定できます。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/フォルダとカスタマーにカスタマイズ設定が適用されます。

カスタマーごとにアップセル機能を有効化または無効化する

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て右側ペインに進み、**[設定]** タブをクリックします。
3. **[アップセル]** セクションで以下の手順を実行します。
   - **[追加的なAdvanced Editionの宣伝]** を有効にし、カスタマー向けのアップセル施策を有効化します。
   - **[追加的なAdvanced Editionの宣伝]** を無効にし、カスタマー向けのアップセル施策を無効化します。

アップセル要素がカスタマーに表示されます

脆弱性一覧

サービスコンソールの **[ソフトウェア管理]** > **[脆弱性]** で脆弱性の一覧を確認できます。ユーザーがスティッチのアイコンをクリックすると、より上位のエディションを購入するようにユーザーを促す、エディション販促用のダイアログが開きます。

保護計画の作成または編集

サービスコンソールの **[計画]** > **[保護]** で実行できます。**[計画の作成]** をクリックします。Cyber Backup Editionでは、**[バックアップ]** および **[脆弱性]** モジュールのみが有効になります。他のモジュー

ルについては、Cyber Protect Editionでのみ利用可能です。カスタマーがCyber Protect Editionのいずれかを購入すると、すべてのモジュールが有効になります。

自動検出ウィザード

このウィザードは、サービスコンソールの **[デバイス]** > **[すべてのデバイス]** から実行できます。カスタマーが **[追加]** をクリックすると自動検出ウィザードが立ち上がります。その後 **[複数のデバイス]** セクションに移動し、**[Windowsのみ]** をクリックします。自動マシン検出メソッドは、Advanced Editionでのみ利用可能です。

デバイス一覧のアクション

この一覧は、サービスコンソールの **[デバイス]** > **[すべてのデバイス]** から表示できます。カスタマーがマシンを選択すると、左側のペインに2つの追加オプションが表示されます。

- **[HTML5クライアント経由で接続]**
- **[パッチ]**

カスタマーが現在利用中のエディションより上位のエディションを購入すると、これらのオプションが利用可能になります。

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。

ストレージの操作の詳細については、「ストレージの管理」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。

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する必要があります。

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。

不変ストレージの構成

パートナーレベルおよびカスタマーレベルで、不変ストレージを構成できます。

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。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。

カスタマーテナントの場合、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**
  管理者はこのモードで、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。
- **コンプライアンスモード**
  このモードを選択すると、不変ストレージを無効化することはできなくなり、そのモードや保持期間を変更することもできなくなります。

子テナントにカスタム設定が適用されていない場合、子テナントは親テナントの設定を継承します。

管理者アカウントが属するテナントで二要素認証が有効な場合のみ、不変ストレージの構成を実行できます。

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。

注意
21.12リリースから新規パートナーのテナントでは、不変ストレージ（14日間の保持期間）がデフォルトで有効になっています。既存のテナントの場合、不変ストレージを手動で有効にする必要があります。

パートナーテナントの不変のストレージを有効化するには

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]** へ進みます。
2. **[不変ストレージ]** スイッチを有効にします。
3. 14～999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。

パートナーテナントの不変のストレージを無効化するには

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]** へ進みます。
2. **[不変ストレージ]** スイッチを無効にします。

   警告
   この変更は、不変ストレージのカスタム設定を使用していないすべての子テナントにより継承されます。すべての削除済みバックアップが完全に消去されます。新しいバックアップも恒久的に削除されます。

3. **[無効化]** をクリックしてこの選択内容を確認します。

カスタマーテナントの不変のストレージを有効化するには

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]** へ進みます。
2. カスタマーテナントの設定を編集するには、その名前をクリックします。
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]** スイッチを有効にします。
5. 14～999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ます。

   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なくなり、そのモードや保持期間を変更することもできなくなります。

7. **[保存]** をクリックします。

カスタマーテナントの不変のストレージを無効化するには

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]** へ進みます。
2. カスタマーテナントの設定を編集するには、その名前をクリックします。
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]** スイッチを無効にします。

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。

警告
不変ストレージを無効にすると、すべての削除済みバックアップが完全に消去されます。新しいバックアップも恒久的に削除されます。

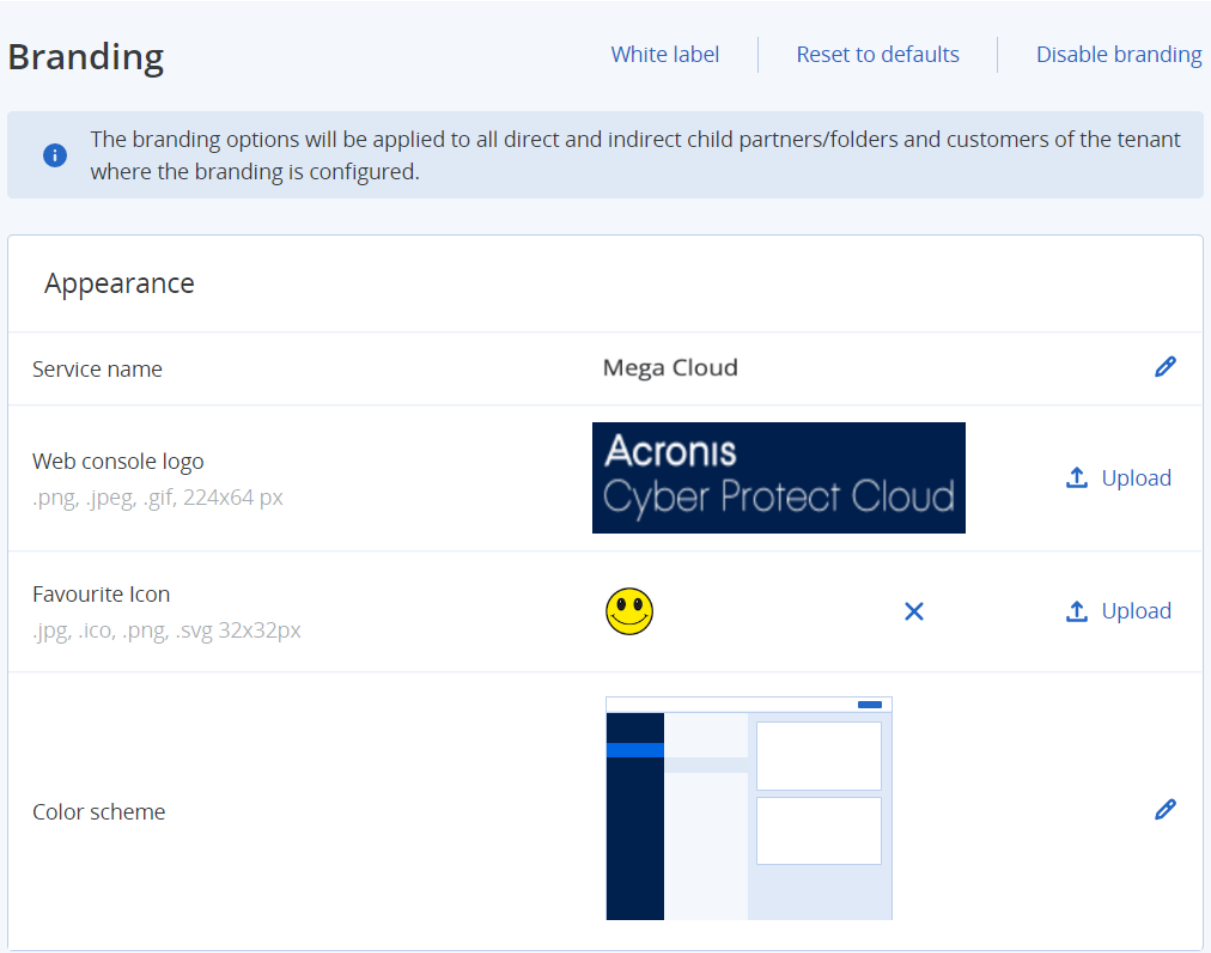
5. **[無効化]** をクリックしてこの選択内容を確認します。

制限事項

- 不変ストレージは、Acronis Cyber Infrastructureバージョン4.7.1以降を利用する、Acronisホステッドストレージまたはパートナーホステッドストレージで使用できます。
  不変ストレージでは、Acronis Cyber Infrastructureのバックアップゲートウェイサービスに対応するため、TCPポート40440を開放しておく必要があります。バージョン4.7.1以降の場合、TCPポート40440が、**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。

カスタマイズとホワイトラベルの構成

[設定] > **[カスタマイズ]** セクションでは、パートナー管理者が管理ポータルと**Cyber Protection** サービスのユーザーインターフェー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。



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 **[構成]** 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）の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。

- **[送信元]**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エージェントと（Windows、macOS、およびLinuxの）Cyber Protectionモニタ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、エージェントと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モニタ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。

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 [**構成**] 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レコードの構成を要求するには、「ブランディングWebコンソールURL（58275）」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」の条件の詳細については、https://letsencrypt.org/repository/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。
6. [**送信**] をクリックして変更を適用します。

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。

エージェントの自動アップデート

Cyber Protectには、保護されているマシンにインストール可能な、3種類のエージェントがあります。つまり、Windowsエージェント、Linuxエージェント、Macエージェントです。

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、すべてのマシンの全エージェントに対して、自動の無人アップデートを構成（または無効化）することができます。

重要
現在、保護を有効化しているパートナーおよびカスタマーのみ、エージェントアップデートの管理機能を利用できます。

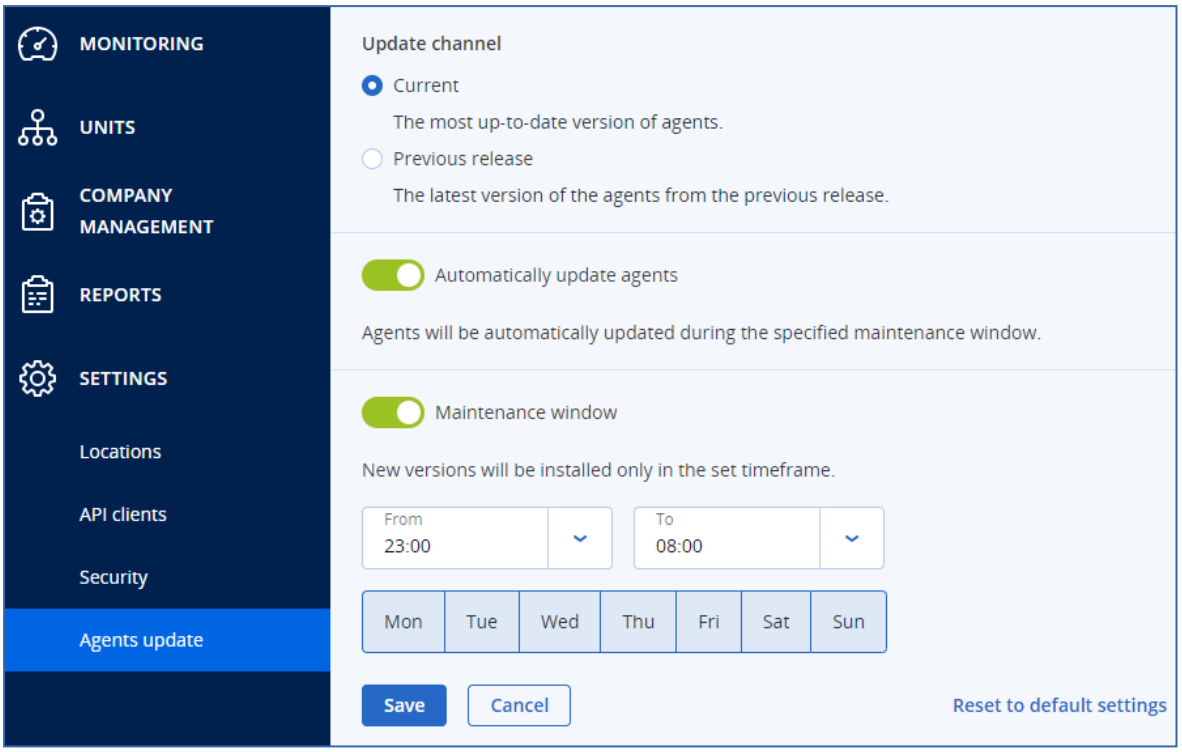
注意
個別マシン上のエージェントを管理し、自動アップデートの設定をカスタマイズする場合、『Cyber Protectユーザーガイド』の「エージェントの更新」セクションを参照してください。

エージェントを自動アップデートするには

注意
File Sync & Shareエージェントの自動アップデートに関する設定は、プロテクションが有効化されていないパートナーおよびカスタマーに継承されます。

管理ポータルのトップページからエージェントの自動アップデートを設定するには

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. 自動アップデートで検出するバージョンを**現在**または**以前のリリース**から選択します。
   （デフォルトは**現在**です）。
3. **[エージェントを自動的にアップデートする]** をオンに切り替えます
   （デフォルトは**オン**です）。
4. メンテナンスの時間帯を設定します。
   （デフォルトは23:00～08:00です）。

   注意
   エージェントのアップデートプロセス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. （オプション） 自動アップデートが実行される日付を指定します。
6. **[保存]** を選択します。

注意
自動アップデートは、以下のバージョンでのみ利用可能です:

- Cyber Protectエージェント、バージョン15.0.26986（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。

エージェントのアップデートを監視するには

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場合、『Cyber Protectユーザーガイド』の「アラート」と「アクティビティ」の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。

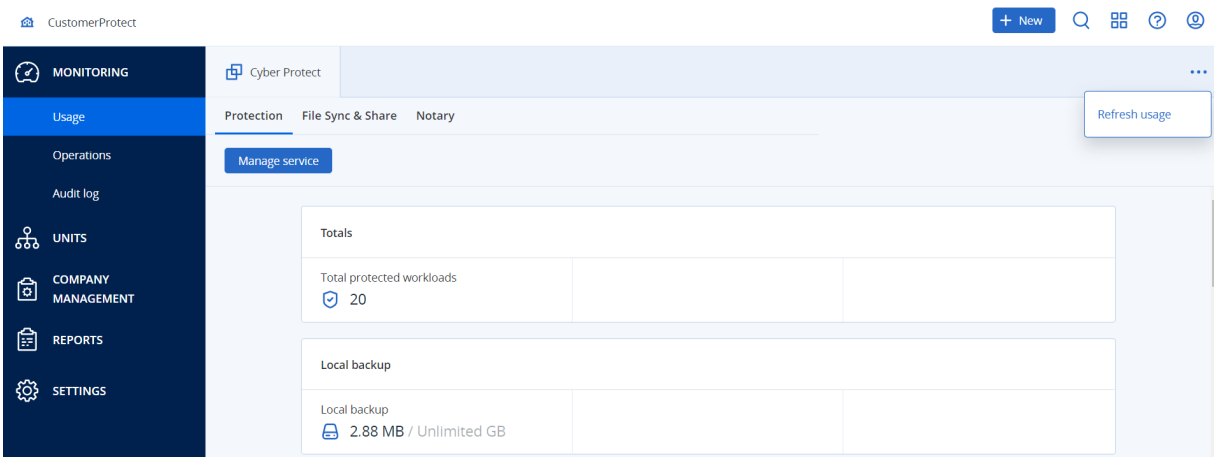
使用状況

[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。

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。



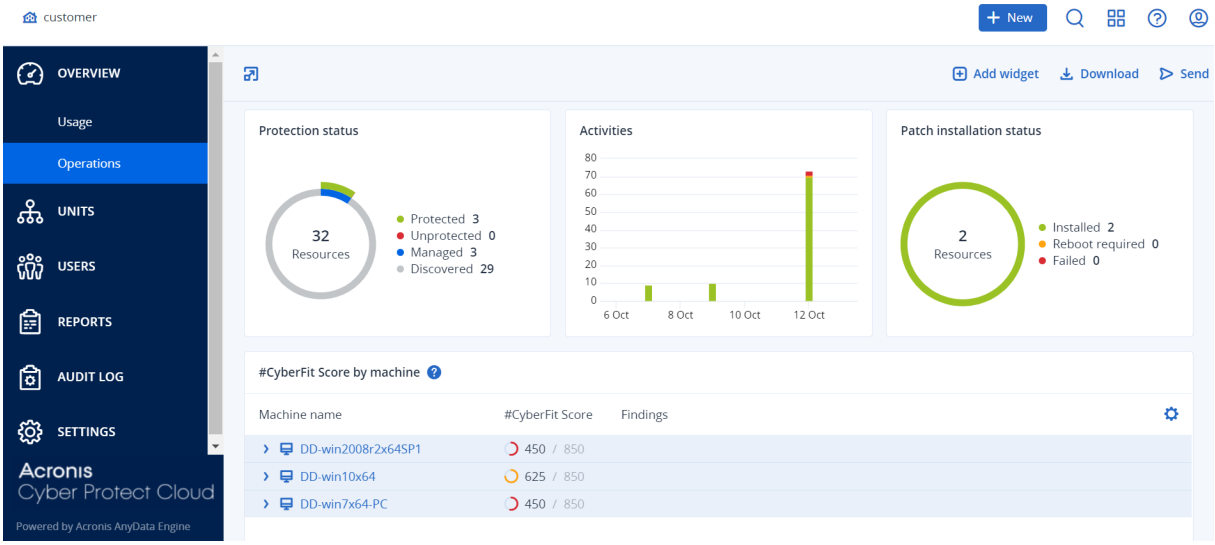
処理

[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

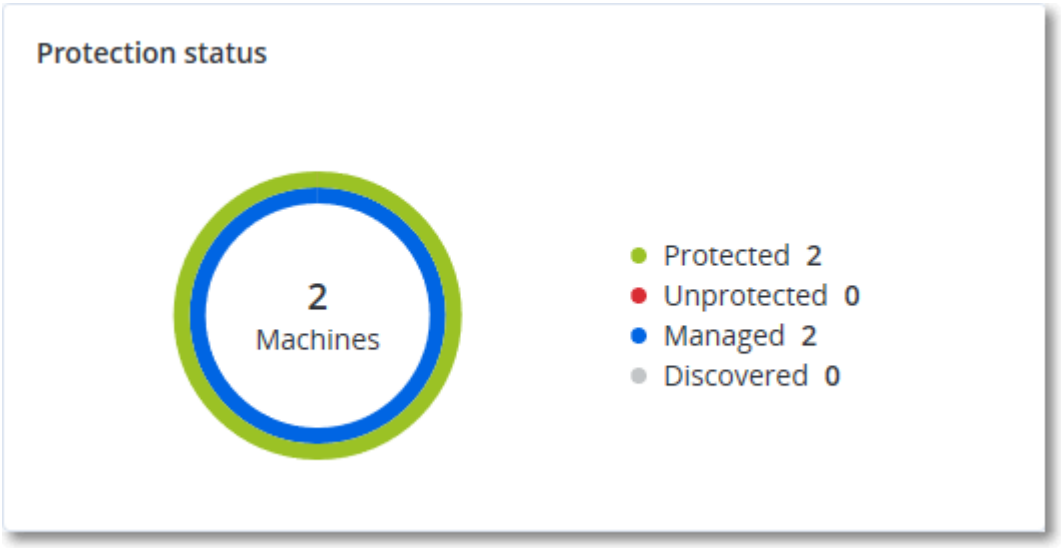
保護ステータス

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。

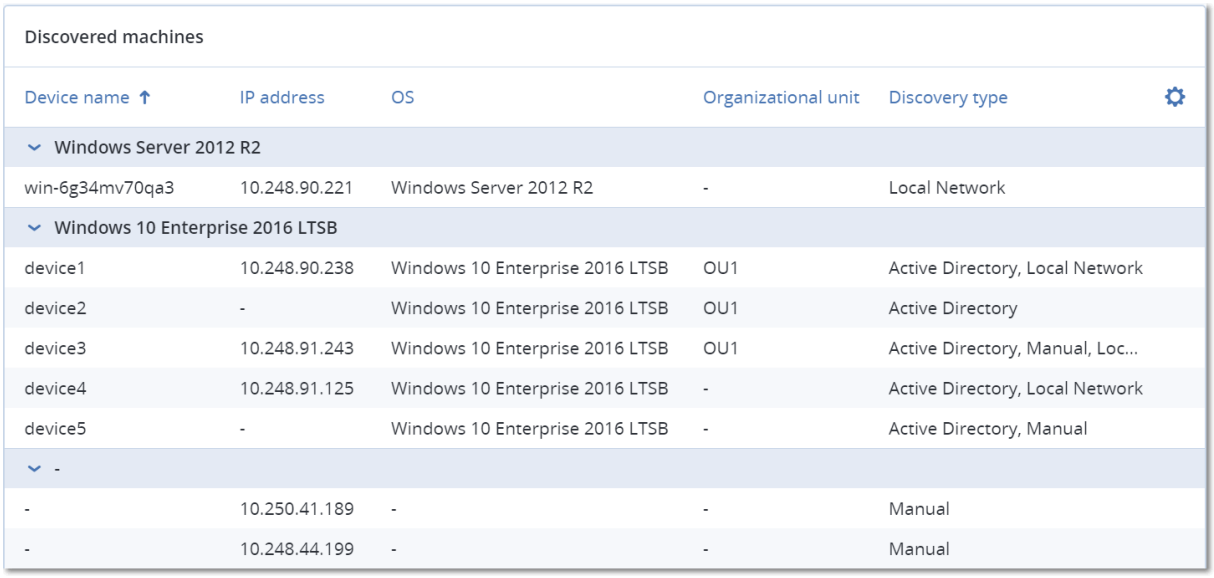
- **保護対象** - 保護計画が適用されているマシン。
- **保護対象外** - 保護計画が適用されていないマシン。これらには、保護計画が適用されていない検出済みマシンと管理対象のマシンの両方が含まれます。
- **管理対象** - プロテクションエージェントをインストール済みのマシン。
- **検出済み** - プロテクションエージェントを未インストールのマシン。

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。



検出されたマシン

このウィジェットには指定された時間内に検出されたマシンのリストが表示されます。



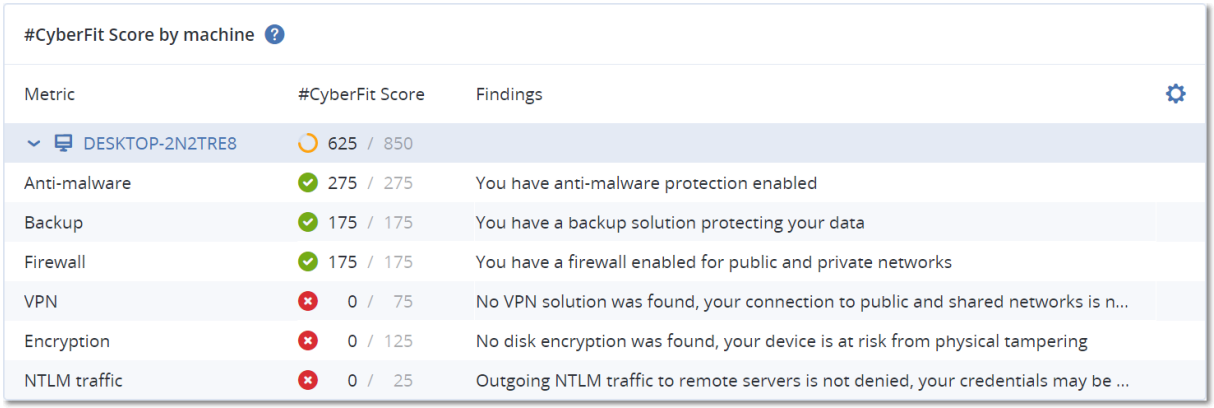
マシンごとの #CyberFit スコア

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。



エンドポイント検知と応答（EDR）ウィジェット

重要
本書は、EDR文書の早期提供版です。機能や説明の一部が不完全な場合があります。

エンドポイント検知と応答（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

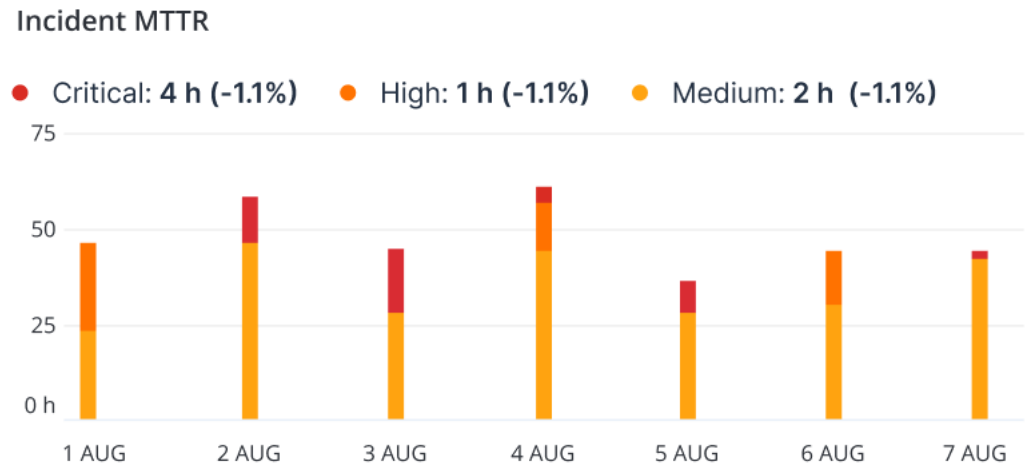
このウィジェットには、インシデントの数が多い、上位5つのワークロードが表示されます（[**すべて表示**] をクリックすると、ウィジェットの設定に応じてフィルタリングされたインシデントのリストにリダイレクトされます）。

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**、**完了**、**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。

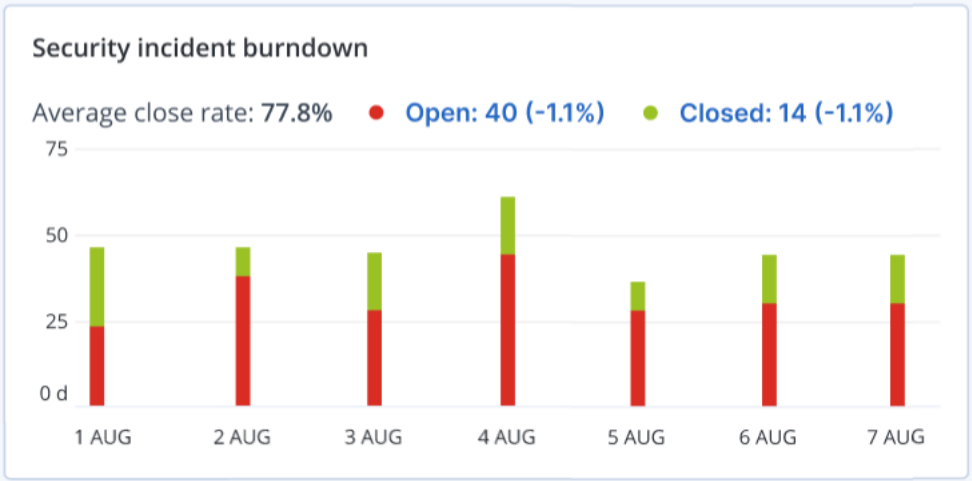


セキュリティインシデントのバーンダウン

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（**クローズ**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。

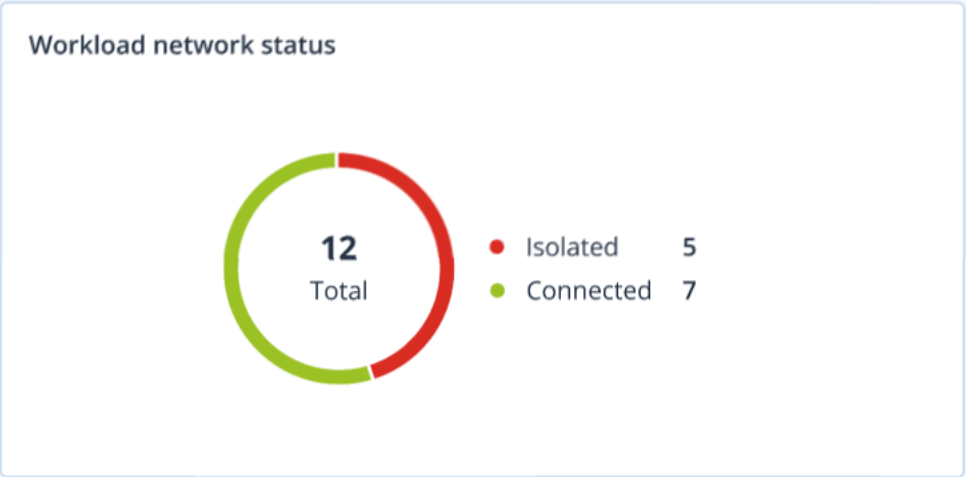
括弧内の%数値により、前期比での増減が表わされます。



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。
- NVMeドライブの場合、ディスク状態の監視は、Windows APIを介してSMARTデータを送受信するドライブでのみサポートされています。ドライブから直接SMARTデータを読み取る必要があるNVMeドライブでは、ディスク状態の監視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。

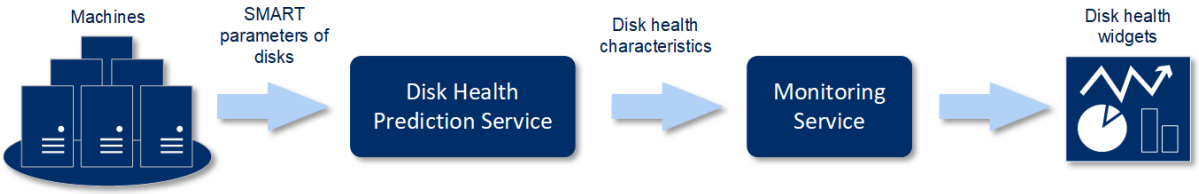
- **OK**
  ディスク状態が70～100%です。
- **警告**
  ディスク状態が30～70%です。
- **重大**
  ディスク状態が0～30%です。
- **ディスクデータの計算中**
  現在のディスク状態と予測を計算中です。

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、サービス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、サービス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。

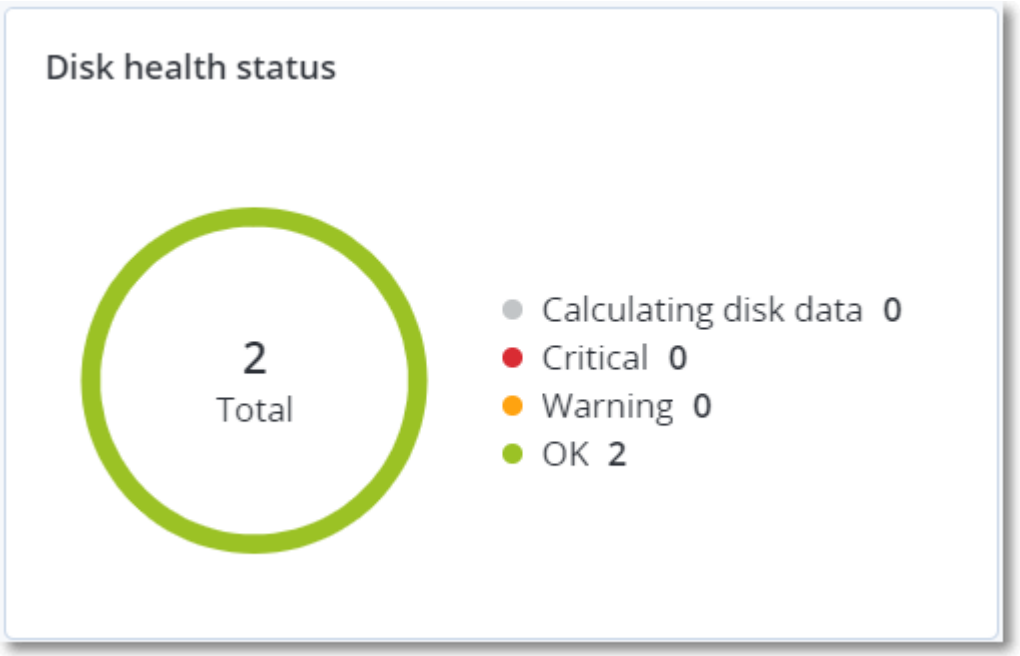
- **ディスク状態の概要**は、階層の詳細情報を含むツリー図ウィジェットです。階層は、ツリーをたどるようにして切り替えることができます。
  - マシンレベル

    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<ディスク名>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<ディスク名>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。

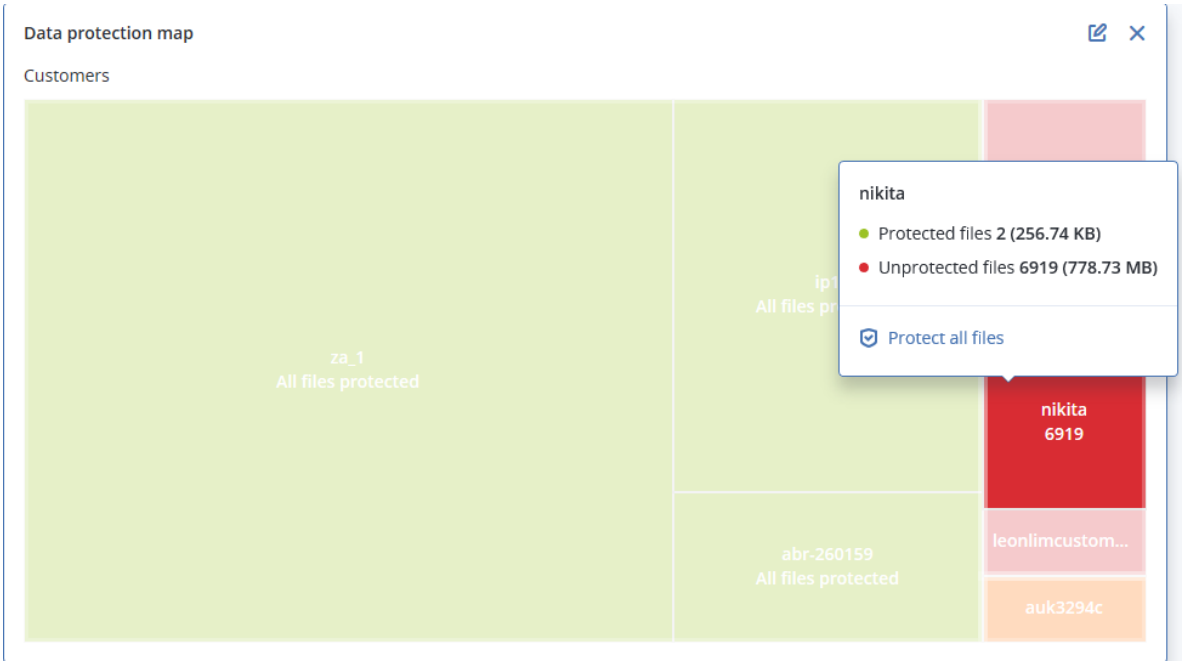
各ブロックのサイズは、カスタマー/マシンに属する重要なすべてのファイルの合計数/サイズによって異なります。

ファイルは次のいずれかの保護ステータスになります。

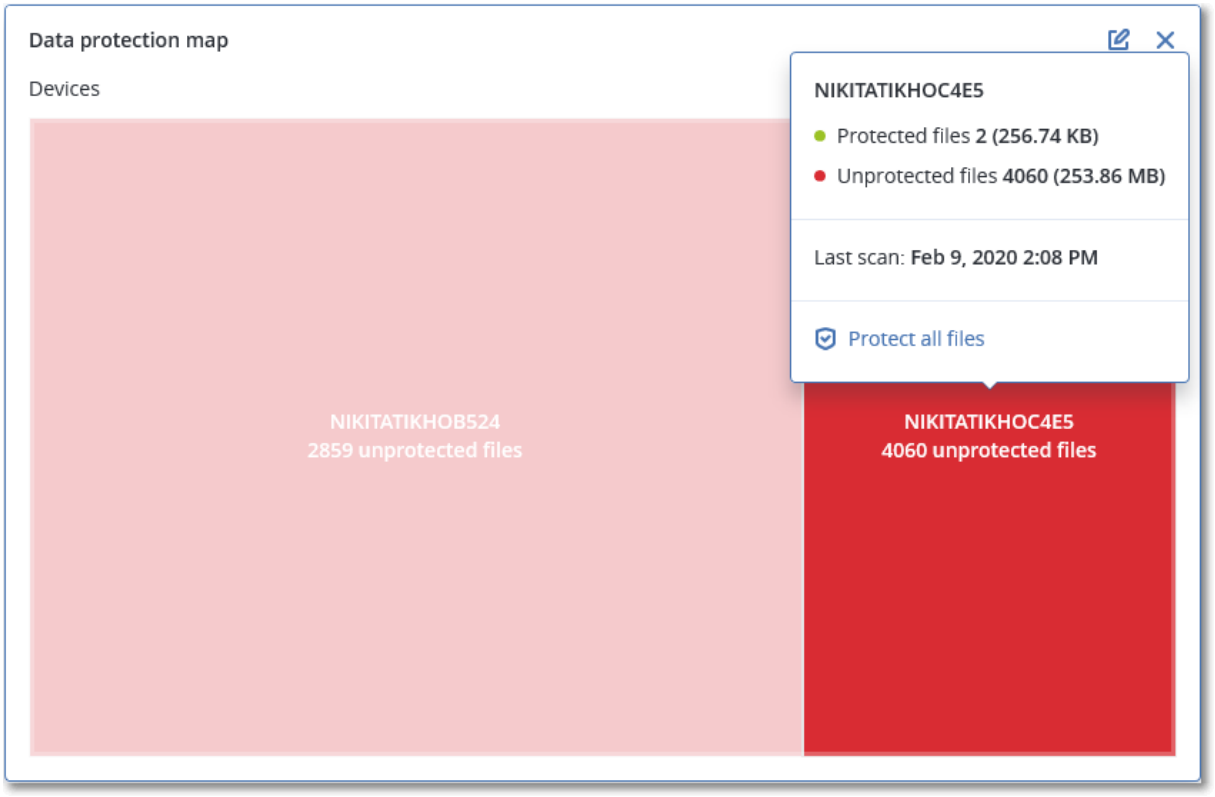
- **重大** - 選択済みカスタマーのテナント/マシン/ロケーションで、バックアップ対象に指定されていない拡張子を持つ保護非対象のファイルが、51～100%存在します。
- **低** - 選択済みカスタマーのテナント/マシン/ロケーションで、バックアップ対象に指定されていない拡張子を持つ保護非対象のファイルが、21～50%存在します。
- **中** - 選択済みカスタマーのテナント/マシン/ロケーションで、バックアップ対象に指定されていない拡張子を持つ保護非対象のファイルが、1～20%存在します。
- **高** - 選択済みカスタマーのテナント/マシン/ロケーションで、すべてのファイルが保護（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。

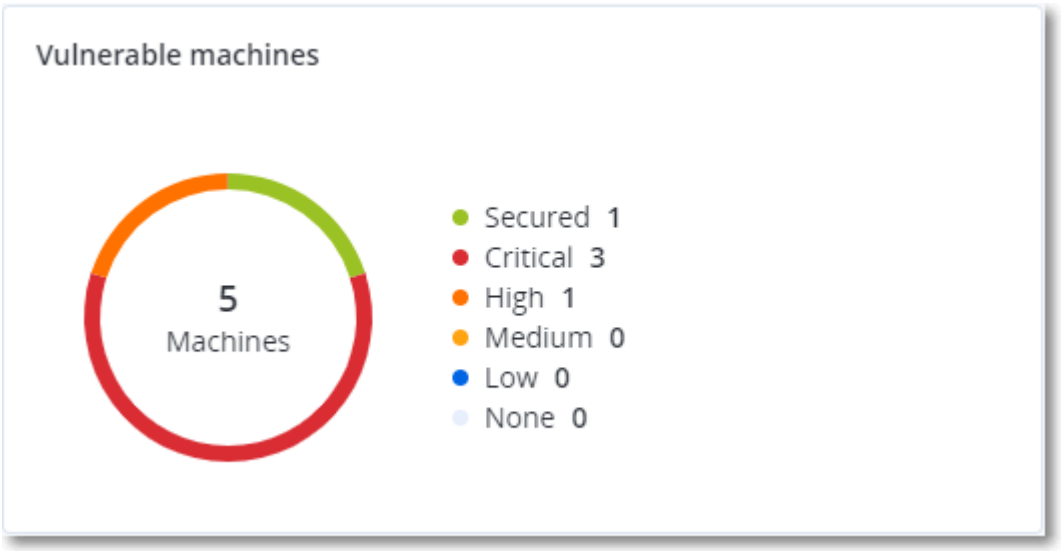
脆弱性診断ウィジェット

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

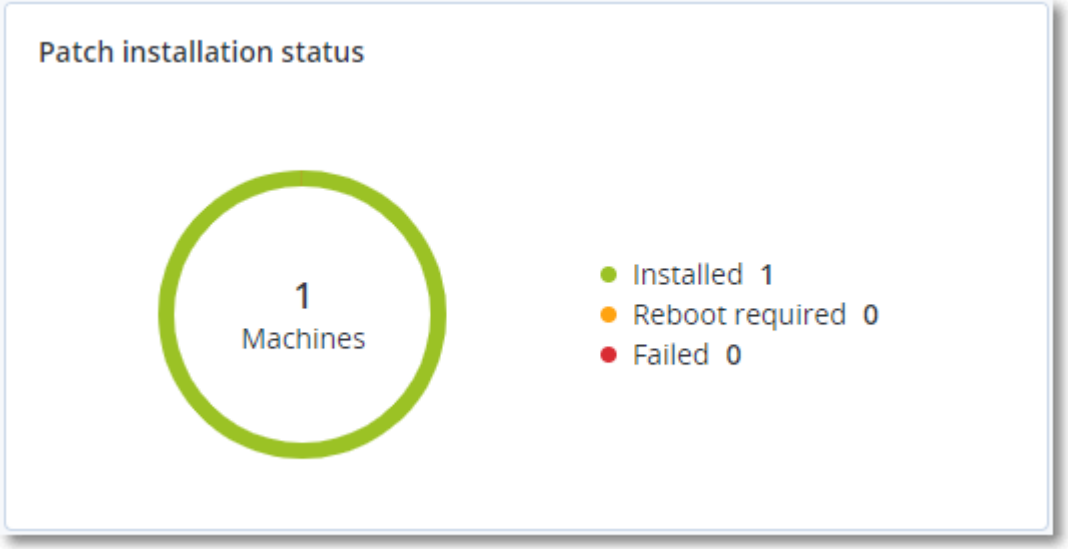
パッチインストールウィジェット

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

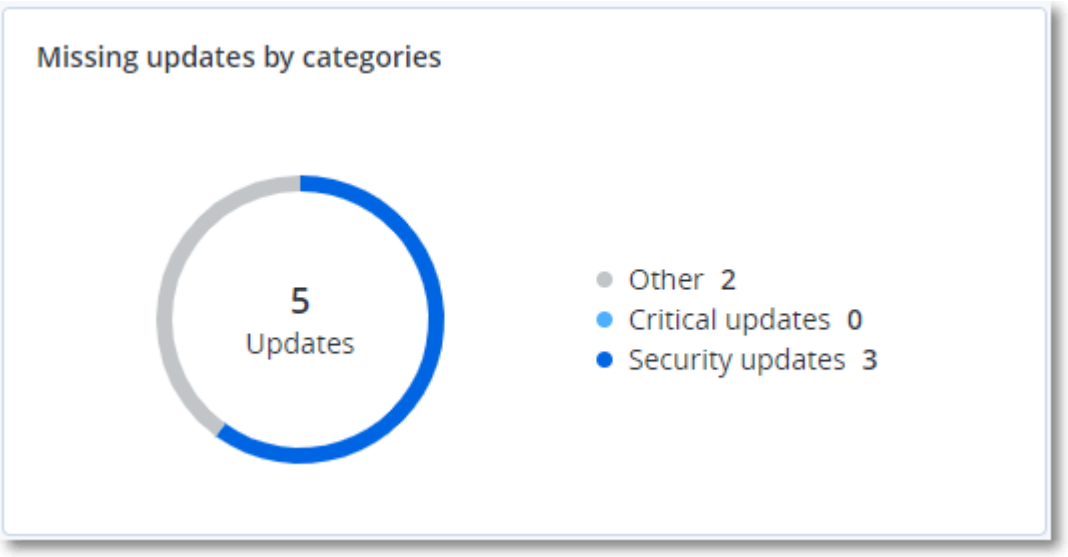
パッチインストール履歴

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

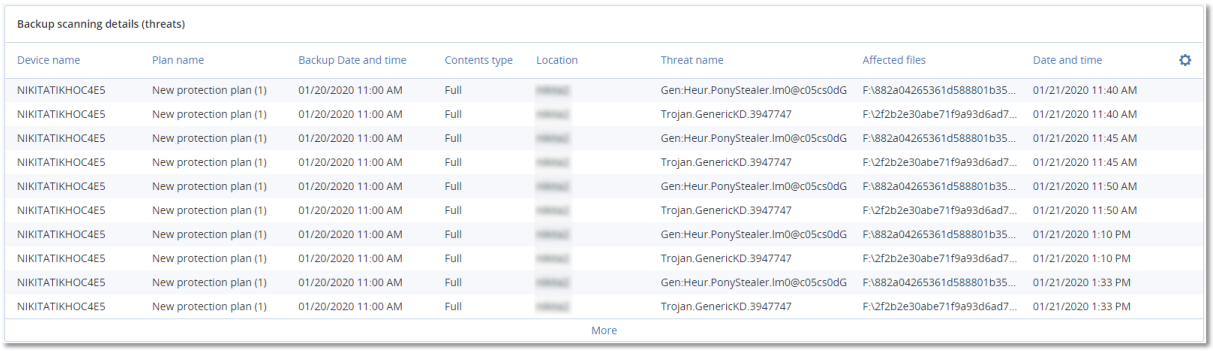
このウィジェットは、見つからないアップデートの数をカテゴリ別に表示します。次のカテゴリで表示されます。

- セキュリティアップデート
- 重要なアップデート
- その他



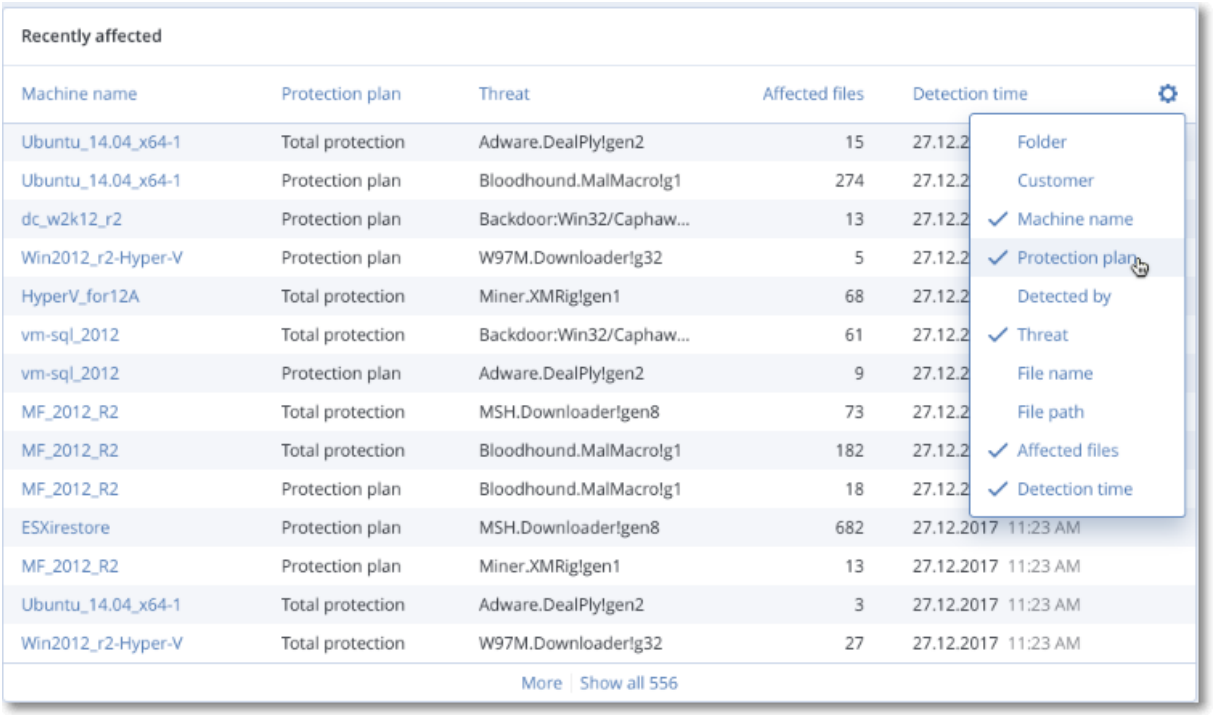
バックアップスキャンの詳細

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。

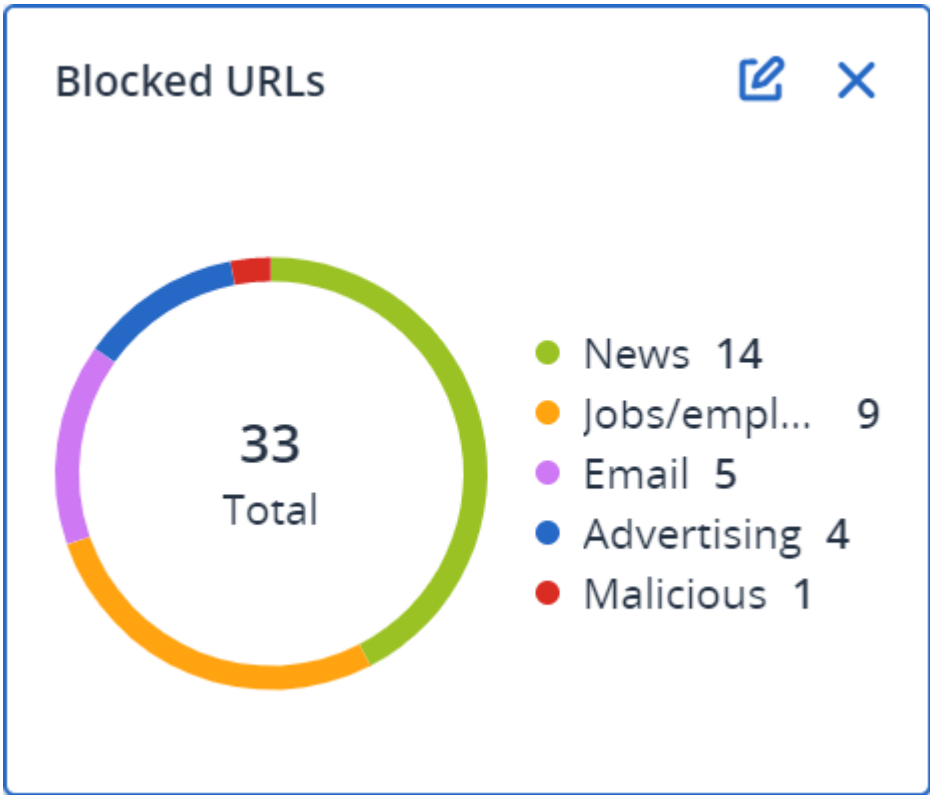
最近影響を受けたワークロードのデータをダウンロードするには

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

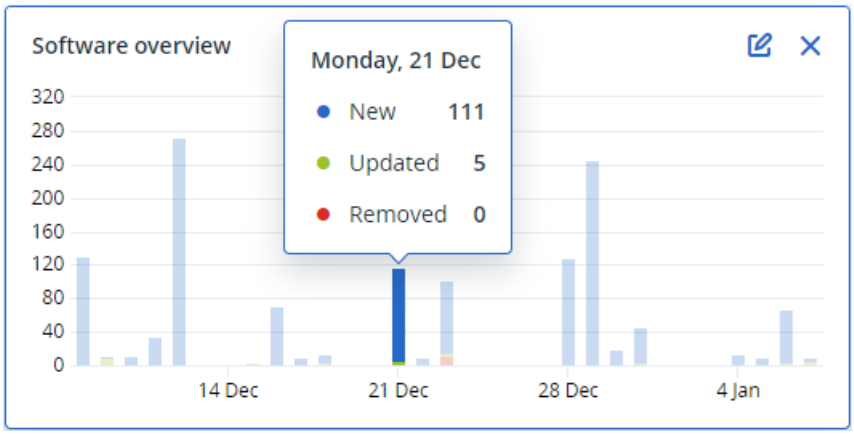
ソフトウェアインベントリテーブルウィジェットには、クライアントの組織内のWindowsおよびmacOSデバイスにインストールされている、すべてのソフトウェアに関する詳細情報が表示されます。

Software inventory

Folder name	Customer name	Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User	System type
ACP-QAZ03-A01												
ACP-QAZ03-A01												
ACP-QAZ03-A03												
folder1	rbarf4	ACP-QAZ03-A03	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	-	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\V...	System	X64
ACP-QAZ03-A04												
folder1	rbarf4	ACP-QAZ03-A04	Google Chrome	79.0.3945.130	Google LLC	New	-	-	11/28/2020, 2:49 PM	C:\Program Files (x...	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Google Update He...	1.3.36.31	Google LLC	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Notepad++	6.7.4	Notepad++ Team	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft OneDrive	20.201.1005.0009	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Update ...	2.68.0.0	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\V...	System	X64

More | Less | Show 1000+

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。

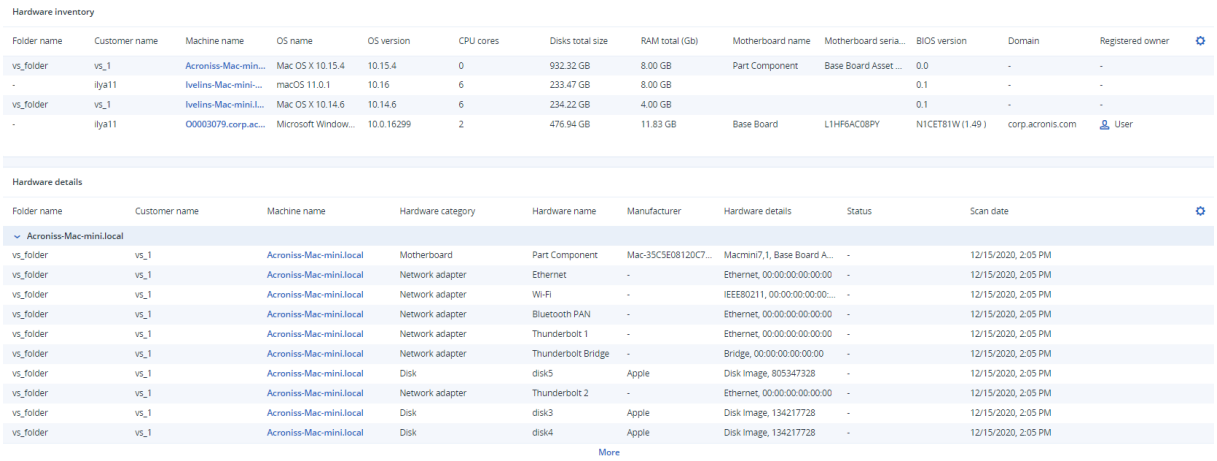
アップデート済み - アップデートされたアプリケーションの数です。

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、カスタマーのサービスコンソールの、[**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。

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。



Hardware inventory

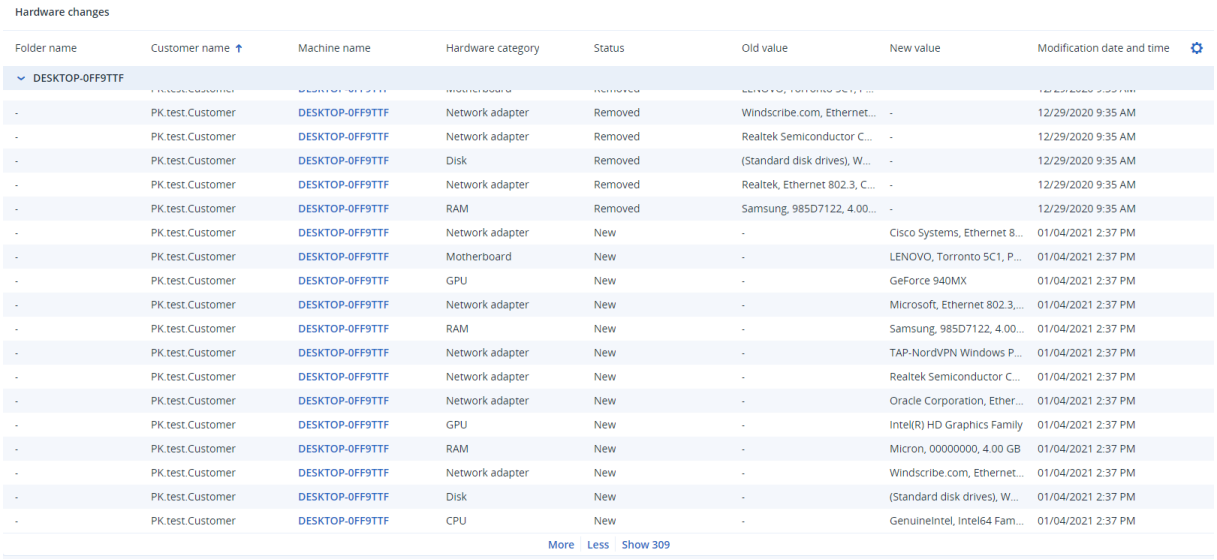
Folder name	Customer name	Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner
vs_folder	vs_1	Acroniss-Mac-min...	Mac OS X 10.15.4	10.15.4	0	932.32 GB	8.00 GB	Part Component	Base Board Asset ...	0.0	-	-
-	ilya11	Ivelins-Mac-mini-...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-
vs_folder	vs_1	Ivelins-Mac-mini.l...	Mac OS X 10.14.6	10.14.6	6	234.22 GB	4.00 GB			0.1	-	-
-	ilya11	O0003079.corp.ac...	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User

Hardware details

Folder name	Customer name	Machine name	Hardware category	Hardware name	Manufacturer	Hardware details	Status	Scan date
Acroniss-Mac-mini.local								
vs_folder	vs_1	Acroniss-Mac-mini.local	Motherboard	Part Component	Mac-35C5E08120C7...	Macmini7,1, Base Board A...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Ethernet	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Wi-Fi	-	IEEE80211, 00:00:00:00:00:...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Bluetooth PAN	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 1	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt Bridge	-	Bridge, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk5	Apple	Disk Image, 805347328	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 2	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk3	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk4	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM

More

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または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。



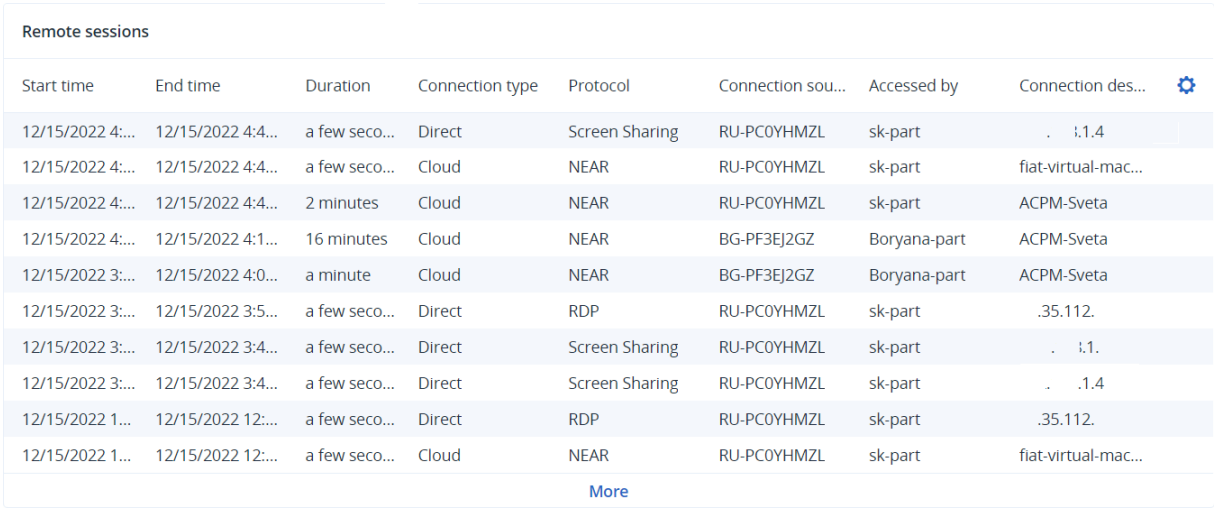
Hardware changes

Folder name	Customer name	Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF							
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Windscribe.com, Ethernet...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek Semiconductor C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	Removed	(Standard disk drives), W...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek, Ethernet 802.3, C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	Removed	Samsung, 985D7122, 4.00...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 8...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	GeForce 940MX	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Microsoft, Ethernet 802.3,...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor C...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ether...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Windscribe.com, Ethernet...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), W...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	CPU	New	-	GenuineIntel, Intel64 Fam...	01/04/2021 2:37 PM

More | Less | Show 309

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。



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

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。

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。
- **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。

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

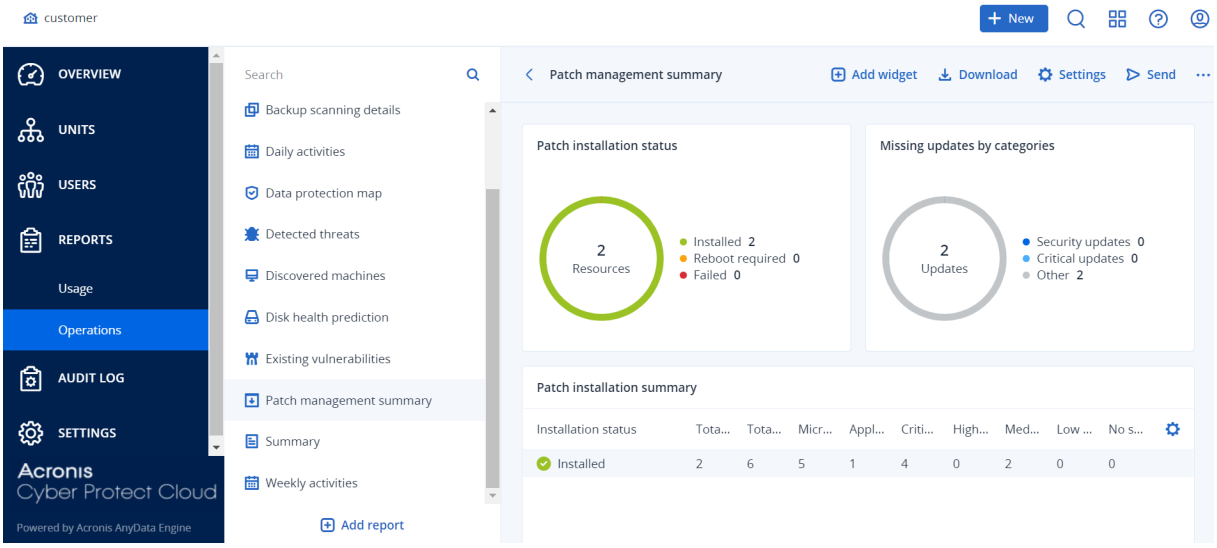
操作に関するレポートには、**[操作]** ダッシュボードウィジェットの任意のセットを含めることができます。デフォルトでは、すべてのウィジェットに操作中のテナントのサマリ情報が表示されます。ウィジェットを編集するか、レポート設定のすべてのウィジェットに対して個別に変更することができます。

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"（114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。

操作に関するレポートをダウンロードしたり、Excel（XLSX）またはPDF形式によりEメールで送信したりできます。



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 Score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。
検出されたマシン	組織のネットワーク内で見つかったすべてのマシンを一覧表示します。
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。
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。
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。

レポートを表示するには、その名前をクリックします。

レポートを使用して操作にアクセスするには、レポート行の縦向きの省略記号アイコンをクリックします。同じ操作がレポート内から利用可能です。

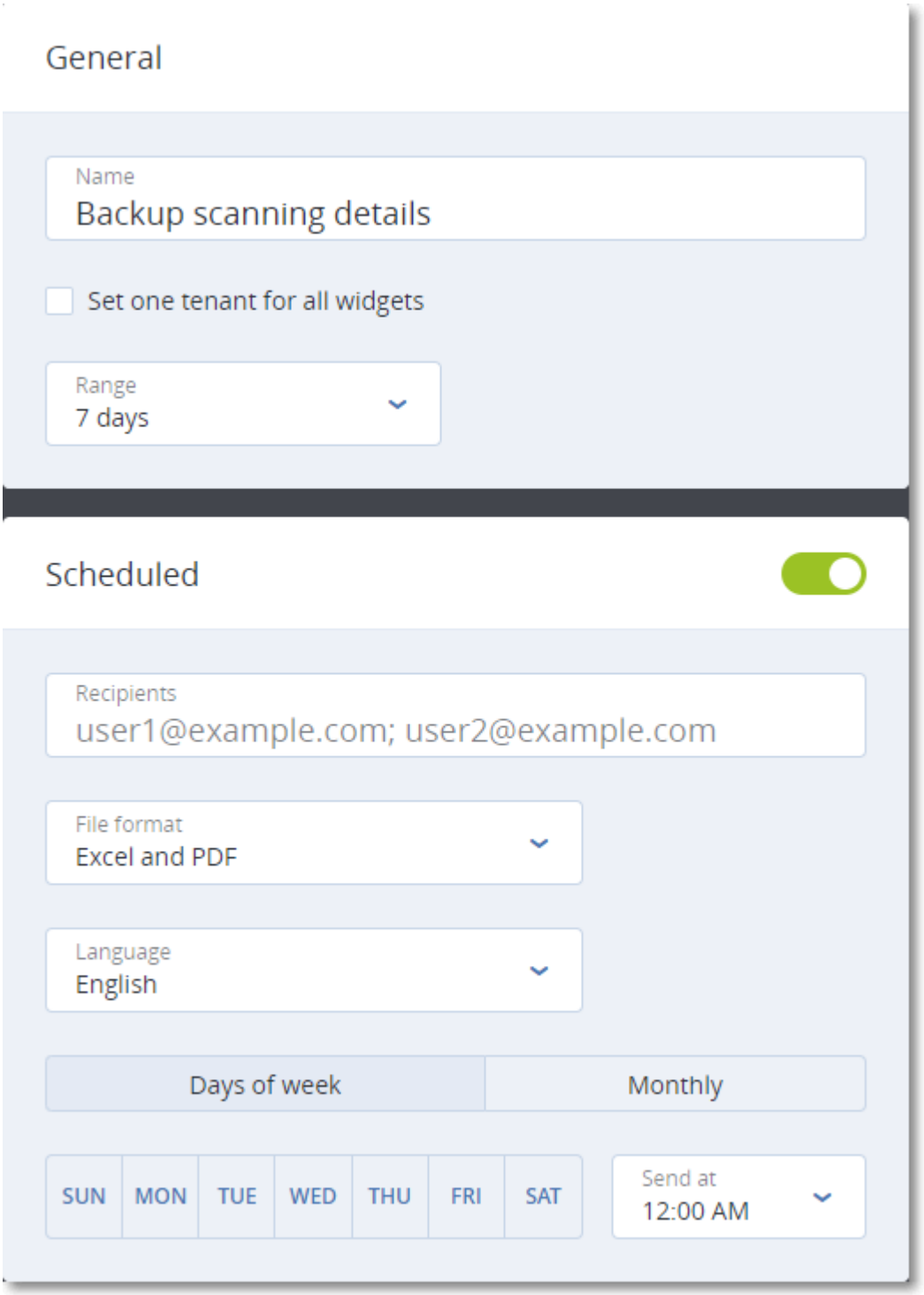
レポートの追加

1. **[レポートの追加]** をクリックします。
2. 次のいずれかを実行します。
   - 定義済みレポートを追加するには、その名前をクリックします。
   - カスタムレポートを追加するには、**[カスタム]**をクリックしレポート名（デフォルトで割り当てられた名前は **[カスタム(1)]**）のように表示された後、レポートにウィジェットを追加します。
3. （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。
4. （オプション）以下で説明するようにレポートを編集します。

レポート設定の編集

レポートを編集するには、その名前をクリックして、**[設定]** をクリックします。レポートを編集するときには、次のことができます。

- レポート名の変更
- レポートに含まれるすべてのウィジェットの表示テナントの変更
  子テナントがある場合は、**[すべてのウィジェットに1つのテナントを設定]** オプションが利用できます。このオプションを使用すると、レポートのすべてのウィジェットを対象に選択したテナントでデータをフィルタできます。このオプションが選択されていない場合、ウィジェットには現在のテナントのすべての子テナントのデータを表示されます。
- レポートに含まれるすべてのウィジェットの時間範囲の変更
- PDF/Excel形式でEメールによるレポート送信をスケジュール。



レポートのスケジュール

1. レポート名をクリックし、**[設定]** をクリックします。
2. **[スケジュール済み]** スイッチを有効にします。
3. 受信者の電子メールアドレスを指定します。
4. 以下から、レポートの形式を選択します:PDF、Excel、またはその両方。

5. レポートを送信する曜日と時刻を選択します。
6. 右上の **[保存]** をクリックします。

レポート構造のエクスポートとインポート

レポート構造（ウィジェットとレポート設定のセット）をJSONファイルにエクスポートしたり逆にインポートしたりできます。これは、あるテナントから別のテナントにレポート構造をコピーする場合に便利です。

レポート構造をエクスポートするには、レポート名をクリックし、右上にある省略記号アイコン（縦型）をクリックして、**[エクスポート]** をクリックします。

レポート構造をインポートするには、**[レポートの追加]** をクリックして、**[インポート]** をクリックします。

レポートのダウンロード

レポートがダウンロードできます。**[ダウンロード]** をクリックして、必要な形式を選択します。

- ExcelとPDF
- Excel
- PDF

レポートデータのダンプダンプ

CSVファイルのレポートデータのダンプをEメールで送信できます。ダンプには指定した時間範囲内の全レポートデータが（フィルタリングされずに）含まれます。CSVレポートに含まれているタイムスタンプはUTC形式ですが、ExcelとPDFのレポートに含まれているタイムスタンプは現在のシステムのタイムゾーンで表示されます。

ソフトウェアはデータダンプをその場で生成します。範囲が長いと、処理に時間がかかることがあります。

レポートデータをダンプするには

1. レポート名をクリックします。
2. 右上にある省略記号アイコン（縦型）をクリックし、**[データをダンプ]** をクリックします。
3. 受信者の電子メールアドレスを指定します。
4. **[時間範囲]** で、時間の範囲を指定します。
5. **[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、ディザスタリカバリ、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 • 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

ウィジェット	説明
	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** - ディザスタリカバリ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。 **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

ウィジェット	説明
	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。
クラウドワークロードの保護ステータス	**クラウドワークロードの保護ステータス** ウィジェットには、レポート生成時点での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 Drive • Google Workspace Gmail • Google Workspace Shared Drive • 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。

ウィジェット	説明
	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。

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	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

ウィジェット	説明
シデントのバーンダウン	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。
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フィルタリング

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

ウィジェット	説明
	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。
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）。

ディザスタリカバリウィジェット

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
ディザスタリカバリの統計情報	ウィジェットには、指定した日付範囲のディザスタリカバリ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。
テスト済みのディザスタリカバリサーバー	ウィジェットには、ディザスタリカバリで保護され、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、ディザスタリカバリ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** - ディザスタリカバリ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。 **未テスト** - ディザスタリカバリ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、レポート作成時のディザスタリカバリ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。
ディザスタリカバリで保護済みのサーバー	ウィジェットには、ディザスタリカバリ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、ディザスタリカバリ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。

ウィジェット	説明
	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	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

ウィジェット	説明
Sync & Shareストレージ使用状況	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 • 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"（111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 > 概要 > 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 > 概要 > 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 - 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
検出されたマシン	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
ハードウェアのインベントリ	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

監査ログ

監査ログを表示するには、**[監査ログ]** をクリックします。

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 Protectionサービス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 Protectionサービスコンソールで、ユーザーによって実行されるサイバースクリプト処理
- 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。

Advanced Protectionパック

追加料金を支払い、保護サービスに追加してパックを有効にすることが可能です。標準の機能セットや他のAdvancedパックとは重複のない独自の機能が提供されます。クライアントは、1つ、複数、またはすべてのAdvancedパックを使用してワークロードを保護できます。Advanced保護パックでは、ワークロード単位、ギガバイト単位の両方の保護サービス課金モードが利用できます。

Advanced File Sync & Share機能は、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課金モードで利用できます。

次のAdvanced保護パックを有効にできます。

- Advanced Backup
- Advanced管理
- Advancedセキュリティ
- Advanced SecurityとEDR
- Advanced Data Loss Prevention
- Advancedディザスタリカバリ
- Advanced Eメールセキュリティ
- Advanced File Sync & Share

注意
Advancedパックは、拡張する機能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、ユーザーは高度な機能を使用できません。たとえば、保護機能が無効の場合、ユーザーはAdvanced Backupパックの機能を使用できません。

Advanced保護パックが有効な場合、その機能が保護計画に表示され、Advanced機能アイコンでマークが付けられます。ユーザーがこの機能を有効にしようとすると、追加の請求が発生することが通知されます。

Advanced保護パック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、保護計画にAdvanced保護機能が表示されますが、使用の際にアクセスすることはできません。次のアイコンが機能名の横に表示されます:。管理者に連絡して必要な高度な機能セット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。

Advanced保護パックが有効ではなく、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Advanced機能が表示されません。

Cyber Protectサービスの付属機能とAdvancedパック

Cyber Protectのサービスまたは機能セットを有効にすると、付属の機能またはデフォルトで利用できる多数の機能が有効になります。さらに、Advanced保護パックを有効にすることもできます。

次のセクションでは、Cyber Protectのサービス機能とアドバンスドパックの概要について示します。提供項目の全リストについては、『Cyber Protectライセンスガイド』を参照してください。

プロテクションサービスの付属機能と高度な機能

プロテクションサービスの付属機能と高度な機能

機能グループ	付属標準機能	高度な機能
セキュリティ	• #CyberFit Score • 脆弱性診断 • ランサムウェア対策保護:Active Protection • 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。	There are two available advanced protection packs:**Advanced Security** and **Advanced Security + EDR**. Advanced Securityパックには次の内容が含まれています: • 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フィルタリング • 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 Advanced Security + EDR保護パックは、上記のすべての機能に加えて、高度な脅威や進行中の攻撃を特定するための以下のエンドポイント検知と応答（EDR）機能を備えています。 • 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します。 • セキュリティイベントを180日間保存 Advanced SecurityとEDRを有効化する方法の詳細については、"Advanced SecurityとEDRを有効にする"（124ページ）を参照してください。

機能グループ	付属標準機能	高度な機能
データ損失防止	• デバイス制御	• 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
管理	• ワークロードのグループ管理 • 保護計画の集中管理 • ハードウェアのインベントリ • 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	• パッチ管理 • ディスク状態 • ソフトウェアインベントリ • ファイルの安全なパッチ • 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、観察、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と画面共有 • 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
Eメールセキュリティ	なし	Microsoft 365やGmail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、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

機能グループ	付属標準機能	高度な機能
		• 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。
Cyber Disaster Recovery Cloud	ディザスタリカバリ標準機能を使用して、ワークロードのディザスタリカバリシナリオをテストできます。 利用可能なディザスタリカバリ標準機能と、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。	Advancedディザスタリカバリパックを有効にして、すべてのディザスタリカバリ機能を使用してワークロードを保護できます。 利用可能なディザスタリカバリの高度な機能は次のとおりです: • 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 • ランブックの操作: 作成、編集、実行。

プロテクションサービスの従量課金と高度な機能

プロテクションサービスの従量課金と高度な機能

機能グループ	従量課金制機能	高度な機能
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	• Microsoft SQLサーバーとMicrosoft Exchangeクラスター • Oracle DB • SAP HANA • データ保護マップ • 継続的データ保護

機能グループ	従量課金制機能	高度な機能
	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。	• オフホストデータ処理計画 • バックアップの公証 • Microsoft 365シート • Google Workspaceシート
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	• ノータリゼーション（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
Notary	• ファイルノータリゼーション（公証） • ファイルの電子署名 • 文書テンプレート	なし

注意
Advanced保護パックを有効にするには、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Advancedパック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Advancedパック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を使用せずにAdvanced保護パックを使用することはできません。ただし、標準保護の付属機能と合わせて特定のワークロードに関するAdvancedパックを使用することは可能です。この場合、使用するAdvancedパックに対してのみ料金が請求されます。

課金の詳細については、「"Cyber Protectの課金モード"（7ページ）」を参照してください。

Advanced Data Loss Prevention

Advanced Data Loss Prevention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。

Advanced 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Advanced 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。

Advanced Data Loss Preventionの有効化

デフォルトでは、新規テナントの設定でAdvanced Data Loss Preventionが有効になっています。テナント作成時にこの機能が無効になっていた場合、パートナー管理者は後からこの機能を有効化できます。

Advanced Data Loss Preventionを有効化するには

1. Cyber Protect Cloud管理コンソールで [**クライアント**] へ進みます。
2. 編集するテナントを選択します。
3. [**サービスを選択**] セクションで、[**保護**] までスクロールし、適用する課金モードで、[**Advanced Data Loss Prevention**] を選択します。
4. [サービスの構成] で、[**Advanced Data Loss Prevention**] までスクロールし、クォータを構成します。
   デフォルトでは、クォータは無制限に設定されています。
5. 設定を保存します。

Advanced SecurityとEDR

エンドポイント検知と応答（EDR）機能は、気づかれなかった攻撃など、ワークロード上の不審なアクティビティを検知し、インシデントを生成します。これらのインシデントは、各攻撃の概要をステップバイステップで説明しており、攻撃がどのように発生したか、またどのように再発を防止するかを理解するのに役立ちます。攻撃の各ステージに関する分かりやすい説明を提供することで、攻撃の調査に費やす時間を数分に短縮することができます。

Advanced SecurityとEDRを有効にする

パートナー管理者は、Advanced Security + EDR保護パックを有効にすることで、クライアントの保護計画にエンドポイント検知と応答（EDR）機能を提供することができます。

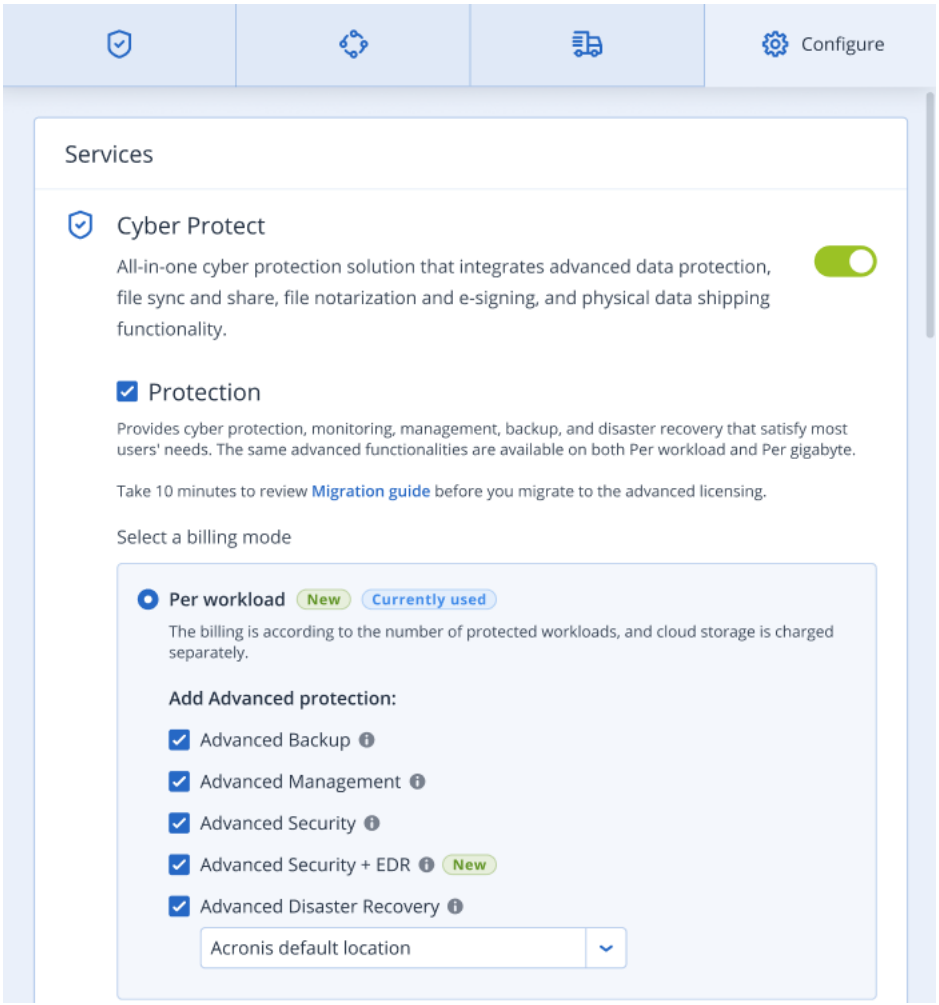
Advanced Security + EDR保護パックを有効にするには

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、Advanced Security + EDR 保護パック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. Advanced Security + EDRパックを追加する該当のクライアントをクリックします。
   [**構成**] タブで、保護セクションの下にある [**Advanced Security + EDR**] チェックボックスが選択さ

れていることを確認します。



Advancedディザスタリカバリ

Advancedディザスタリカバリパックを有効にして、すべてのディザスタリカバリ機能を使用してワークロードを保護できます。

以下の高度なディザスタリカバリ機能を利用できます。

- 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
- ランブックの操作: 作成、編集、実行。

Advanced Eメールセキュリティ

Advanced Email Securityパックは、Microsoft 365、Google Workspace、Open-Xchangeのメールボックスをリアルタイムに保護します。

- 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

Advanced 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。

構成方法については、「Advanced Email SecurityとPerception Point」を参照してください。

機能統合

サードパーティシステムとの統合

サービスプロバイダーは、 Cyber Protect Cloudとサードパーティシステムを

- そのシステムでプラットフォーム拡張機能をセットアップすることによって統合できます。
  管理ポータルの **[統合]** ページに、特に広く利用されているProfessional Services Automations（PSA）システムやRemote Monitoring and Management（RMM）システムで利用できる拡張機能のリストがあります。
  これがプラットフォーム統合に推奨される方式です。
- 該当のシステムのためにAPIクライアントを作成することによっても統合できます。そうすれば、プラットフォームのアプリケーションプログラミングインターフェース（API）やサービスにアクセスできます。APIクライアントは、プラットフォームのOAuth 2.0認証フレームワークの一部になっています。OAuth 2.0の詳細については、https://tools.ietf.org/html/rfc6749を参照してください。
  これはプラットフォームを統合する低水準の方法であり、プログラミングのスキルが必要です。システムに対応するプラットフォーム拡張機能がない場合や、利用できる拡張機能ではプラットフォームやサービスを管理できないので、システムをカスタマイズしなければならない場合などに、この方法をお勧めします。

Cyber Protect Cloudの統合を設定する

1. 管理ポータルにログインします。
2. メインナビゲーションメニューで **[統合]** に移動します。
3. 統合を有効にするサードパーティのシステムの名前をクリックします。
4. 画面の指示に従います。

サードパーティシステムとの統合に関する、ステップバイステップの文書を含む詳細な情報については、https://solutions.acronis.comを参照してください。

APIクライアントの管理

アプリケーションプログラミングインターフェース（API）を使用すれば、サードパーティシステムをCyber Protect Cloudに統合できます。このAPIにアクセスするために、APIクライアントを使用します。APIクライアントは、プラットフォームのOAuth 2.0認証フレームワークの一部になっています。

APIクライアントとは何か

APIクライアントは、プラットフォームのAPIやサービスのデータにアクセスするために認証が必要なサードパーティシステムの代わりに使用する特殊なプラットフォームアカウントです。

このクライアントのアクセスは1つのテナントに限られていて、そのテナントで管理者がクライアントやサブテナントを作成します。

クライアントの作成時に、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ます。そのロールを後から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。

クライアントの資格情報は固有の識別子（ID）とシークレット値です。この資格情報には期限がありませんが、この資格情報を使用して管理ポータルやサービスコンソールにログインすることはできません。シークレット値はリセットが可能です。

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。

標準的な統合手順

1. サードパーティシステムが管理するテナントで管理者がAPIクライアントを作成します。
2. サードパーティシステムで管理者がOAuth 2.0クライアント資格情報フローを有効にします。
   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を使用して作成された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。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。その後システムは、そのトークンをすべてのAPI要求に追加しなければならなくなります。
   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。セキュリティ強化のために、そのトークンは2時間で有効期限が切れます。トークンの有効期限が切れると、そのトークンが追加されているAPI要求はすべて失敗し、システムがプラットフォームに新しいトークンを要求する必要が生じます。

認証APIとプラットフォームAPIを使用するための詳しい情報については、https://developer.acronis.com/doc/account-management/v2/guide/indexにある開発者ガイドを参照してください。

APIクライアントの作成

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. 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。その値が分からなくなったら、確認する方法がないので、リセットするしかありません。

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

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]** をクリックしてその操作を確定させます。
   新しいシークレット値が生成されます。クライアントのIDとデータセンターのURLは変わりません。
   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要求はすべて失敗します。
6. クライアントの新しいシークレット値をコピーして保存します。

   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。その値が分からなくなったら、確認する方法がないので、リセットするしかありません。

7. **[完了]** をクリックします。

APIクライアントの無効化

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。
   クライアントのステータスが **[無効]** に変わります。
   そのクライアントに割り当てられていたセキュリティトークンが含まれている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。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。
   クライアントを再び有効にする操作はいつでも可能です。

無効にしたAPIクライアントの有効化

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。
   クライアントのステータスが **[アクティブ]** に変わります。

そのクライアントに割り当てられていたセキュリティトークンの有効期限が切れていない限り、そのトークンが含まれているAPI要求は正常に実行されます。

APIクライアントの削除

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。
   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要求はすべて失敗します。

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。

統合リファレンス

次の表には、実装されているサードパーティとの機能統合の一覧と、各ドキュメントへのリンクが記載されています。

機能統合の名称	オンラインで表示	PDFを開く
Autotask PSA	https://www.acronis.com/support/documentation/AutotaskPSA/	https://dl.acronis.com/u/pdf/AutotaskPSA_Integration_quickstartguide_en-US.pdf
CloudBlue Commerce	https://www.acronis.com/support/documentation/CloudBlueCommerce/	https://dl.acronis.com/u/pdf/CloudBlue_Commerce_Integration_Guide_en-US.pdf
CloudBlue PSA	https://www.acronis.com/support/documentation/CloudBluePSA/	https://dl.acronis.com/u/pdf/CloudBluePSAIntegration_quickstartguide_en-US.pdf
ConnectWise Automate	https://www.acronis.com/support/documentation/ConnectWiseAutomate/	https://dl.acronis.com/u/pdf/AcronisConnectWiseAutomatePlugin_userguide_en-US.pdf
ConnectWise Command	https://www.acronis.com/support/documentation/ConnectWiseCommand/	https://dl.acronis.com/u/pdf/ConnectWiseCommandIntegration_quickstartguide_en-US.pdf
ConnectWise	https://www.acronis.com/support/documentation/ConnectWiseControl/	https://dl.acronis.com/u/pdf/ConnectWiseControl_integration_en-US.pdf

機能統合の名称	オンラインで表示	PDFを開く
Control		
ConnectWise Manage	https://www.acronis.com/support/documentation/ConnectWiseManage/	https://dl.acronis.com/u/pdf/ConnectWiseManageIntegration_quickstartguide_en-US.pdf
Datto RMM	https://www.acronis.com/support/documentation/DattoRMM/	https://dl.acronis.com/u/pdf/DattoRMMIntegration_quickstartguide_en-US.pdf
Jamf Pro	https://www.acronis.com/support/documentation/JamfPro/	https://dl.acronis.com/u/pdf/JamfProIntegration_quickstartguide_en-US.pdf
Kaseya BMS	https://www.acronis.com/support/documentation/KaseyaBMS/	https://dl.acronis.com/u/pdf/AcronisKaseyaBMSPlugin_userguide_en-US.pdf
Kaseya VSA	https://www.acronis.com/support/documentation/KaseyaVSA/	https://download.acronis.com/pdf/AcronisKaseyaVSAPlugin_userguide_en-US.pdf
Matrix 42	https://www.acronis.com/support/documentation/Matrix42/	https://dl.acronis.com/u/pdf/Matrix42Integration_quickstartguide_en-US.pdf
Microsoft Intune	https://www.acronis.com/support/documentation/MicrosoftIntune/	https://dl.acronis.com/u/pdf/MicrosoftIntuneIntegration_quickstartguide_en-US.pdf
N-able N-central	https://www.acronis.com/support/documentation/NableNcentral/	https://dl.acronis.com/u/pdf/N-able_N-central_Integration_Guide_en-US.pdf
N-able N-sight RMM	https://www.acronis.com/en-us/support/documentation/NableNsightRMM/	https://dl.acronis.com/u/pdf/N-ableN-sightRMMIntegration_quickstartguide_en-US.pdf
Ninja One	https://www.acronis.com/support/documentation/NinjaOne/	https://dl.acronis.com/u/pdf/NinjaOneIntegration_quickstartguide_en-US.pdf
Omnivoice	https://www.acronis.com/support/documentation/Omnivoice/	https://dl.acronis.com/u/pdf/OmnivoiceIntegration_quickstartguide_en-US.pdf
Plesk	https://www.acronis.com/support/documentation/Plesk/	https://dl.acronis.com/u/pdf/Acronis_Backup_extension_for_Plesk_en-US.pdf
PRTG	https://www.acronis.com/support/documentation/PRTG/	https://dl.acronis.com/u/pdf/AcronisPRTGPlugin_userguide_en-US.pdf
ServiceNow	https://www.acronis.com/support/documentation/ServiceNow/	https://dl.acronis.com/u/pdf/ServiceNow_Integration_quickstartguide_en-US.pdf
Splashtop	https://www.acronis.com/support/documentation/Splashtop/	https://dl.acronis.com/u/pdf/Splashtop_Integration_quickstartguide_en-US.pdf

機能統合の名称	オンラインで表示	PDFを開く
Tigerpaw One	https://www.acronis.com/en-us/support/documentation/TigerpawOne/	https://dl.acronis.com/u/pdf/TigerpawOneIntegration_quickstartguide_en-US.pdf
WHM & cPanel	https://www.acronis.com/en-us/support/documentation/WHMCPanel/	https://www.acronis.com/en-us/support/documentation/WHMCPanel/
WHMCS	https://www.acronis.com/en-us/support/documentation/WHMCS/	https://dl.acronis.com/u/pdf/WHMCS_Integration_Manual_en-US.pdf

VMware Cloud Directorとの統合

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では、VMware Cloud Director環境の変更を Cyber Protect Cloudに同期させることができます。
2. VMware Cloud Directorのプラグインのインストール。
   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ースに追加します。
3. 管理エージェントを配置する。
   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、それぞれ自動的にマッピングします。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。

4. 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"（32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。
- VMware Cloud Directorとの統合が構成されているパートナーテナントでは、二要素認証を無効にする必要があります。
- 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 Protectionウェブ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 10.0, 10.1, 10.2, 10.3, 10.4, 10.4.1

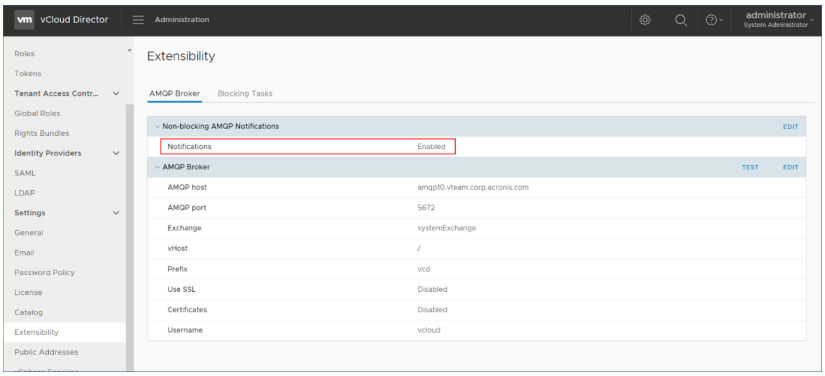
推奨 Web ブラウザ

- Google Chrome 29以降
- Mozilla Firefox 23以降
- Opera 16以降
- Microsoft Edge 25以降
- macOSおよびiOSオペレーティングシステムで稼働するSafari 8以降

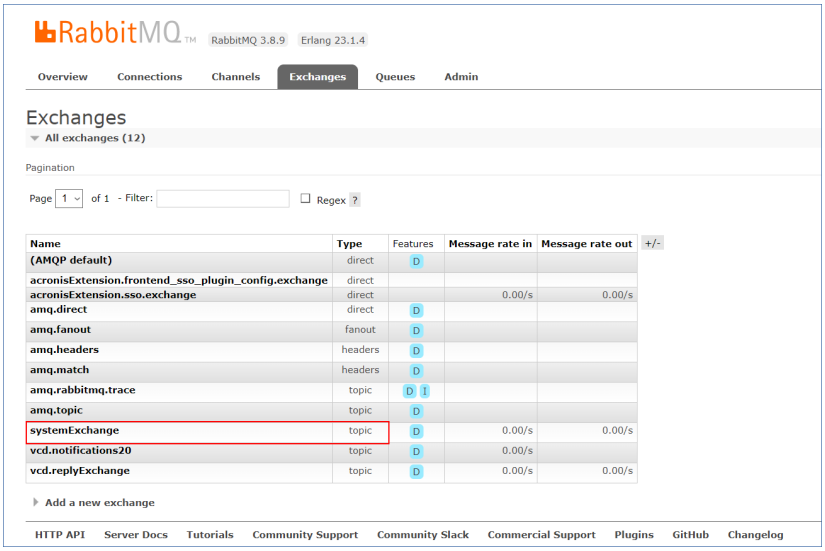
他のWebブラウザ（他のオペレーティングシステムで稼働するSafariブラウザなど）では、ユーザーインターフェースが正しく表示されないか、一部の機能が使用できない場合があります。

RabbitMQメッセージブローカーの構成

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

1. リンク先（https://dl.managed-protection.com/u/vCD/vCDPlugin.zip）から、**vCDPlugin.zip**ファイルをダウンロードしてください。
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. 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。
4. **[プラグインを管理]** タブで **[アップロード]** をクリックします。
   [プラグインをアップロード] ウィザードが開きます。
5. **[プラグインファイルを選択]** をクリックして、**vCDPlugin.zip**ファイルを選択します。
6. **[次へ]** をクリックします。
7. スコープの構成と公開:
   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。

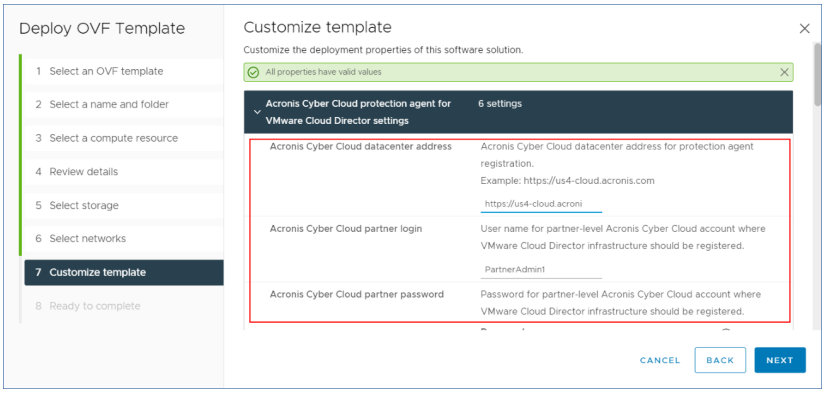
8. **[次へ]** をクリックします。
9. 設定内容を確認して、**[完了]** をクリックします。

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. **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。
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、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。

6. 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。
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"（64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. RabbitMQのパラメータ: サーバーアドレス、ポート、仮想ホスト名、管理者のログイン情報、パスワード。

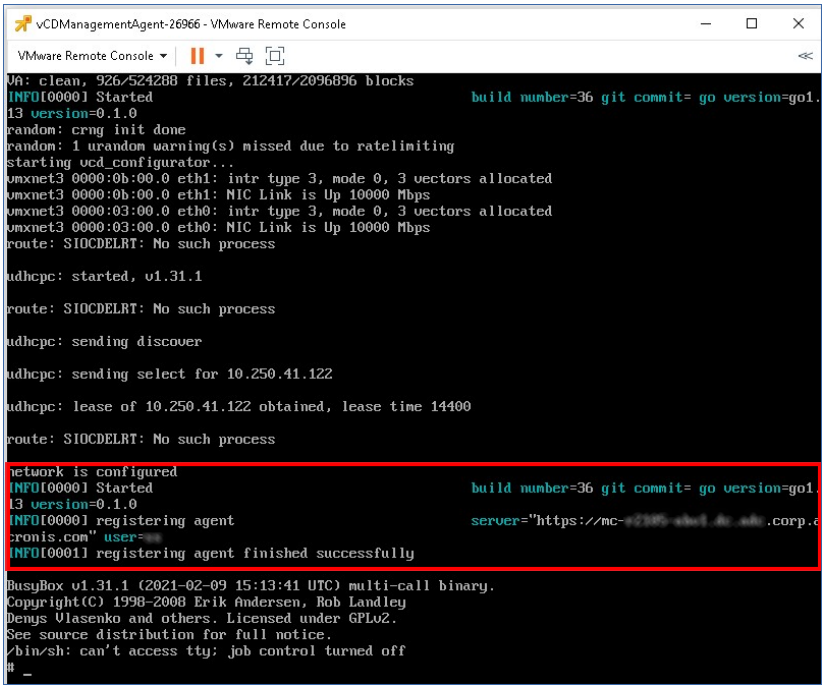
g. ネットワークパラメータ:IPアドレス、サブネットマスク、デフォルトゲートウェイ、DNS、DNSサフィックス。

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、**[構成]** > **[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。

7. （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。

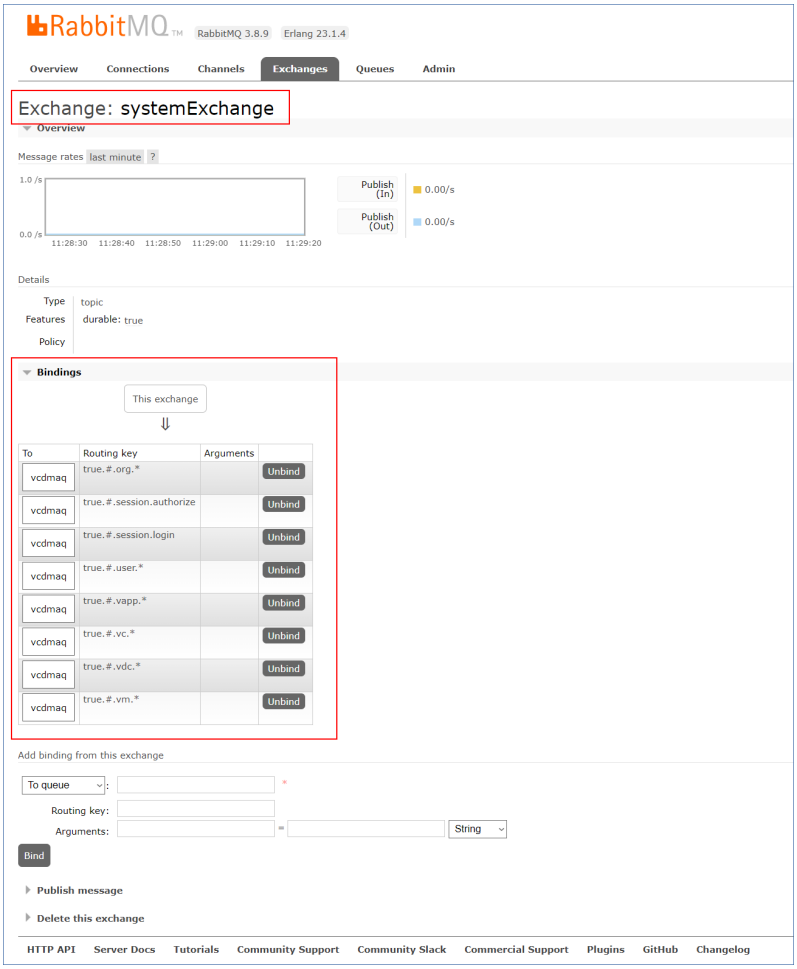


8. RabbitMQの接続を確認します。

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。



バックアップエージェントをインストールする

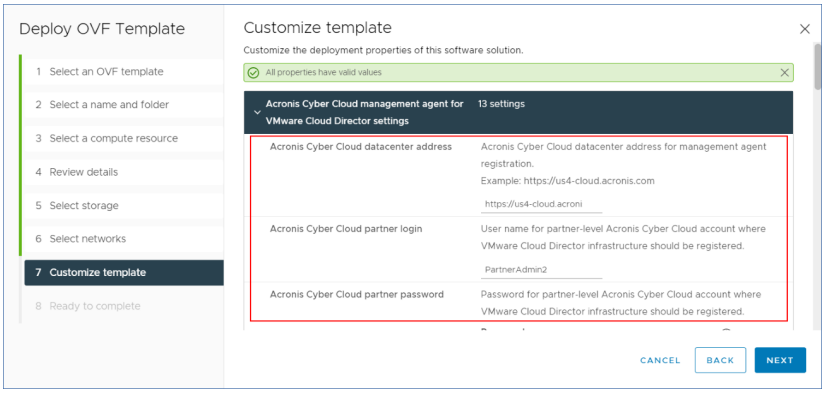
1. パートナー管理者として管理ポータルにログインします。
2. **[設定]** > **[ロケーション]** に移動し、**[VMware Cloud Directorを追加]** をクリックします。
3. **バックアップエージェント**のリンクをクリックして、ZIPファイルをダウンロードします。
4. バックアップエージェントテンプレートファイル（vCDCyberProtectAgent.ovf）と、仮想ハードディスクファイル（vCDCyberProtectAgent-disk1.vmdk）を展開します。
5. vSphereクライアントで、バックアップエージェントテンプレートを任意のESXi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10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。

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。

6. 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。
   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. 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、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。
   e. 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。
   f. 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、**[構成]** > **[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。
7. 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。

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. （オプション） 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。

Cyber Protectionウェブ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"（140ページ）」を参照してください。

管理者は、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、 Cyber Protectionカスタムウェブ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 Protectionウェブコンソールで、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 Protectionウェブ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。

制限事項

制限事項のリストは Cyber Protect Cloudの今後のリリースで変更される可能性があります。

バックアップ

- マシン全体のバックアップのみサポートしています。ファイルフィルタやディスクボリュームは利用できません。
- バックアップロケーションとしてサポートされているのは、クラウドストレージのみです。ストレージは管理エージェントの設定で構成されており、ユーザーが保護計画から変更することはできません。
- ダイナミックグループはサポート対象外です。
- 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、週単位で完全、日単位で増分**。
- 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。

復元

- 元の仮想マシンへの復元のみサポートされています。元の仮想マシンは、VMware Cloud Director環境になければなりません。
- ファイルレベルの復元はサポートされていません。

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]** の権限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"（134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

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。

プライバシー設定

プライバシー設定は、個人情報の収集、使用、開示についての意思を示すのに役立ちます。

ユーザーがCyber Protectを使用している国やサービスを提供している Cyber Protect Cloudデータセンターによっては、Cyber Protectの初回起動時に、Cyber ProtectでGoogle Analyticsを使用することに同意するかどうかを確認するよう求められる場合があります。

Google Analyticsは、匿名化されたデータを収集することで、ユーザーの行動に対する理解を深め、Cyber Protectでのユーザーエクスペリエンスを向上させるサポートを提供します。

Cyber Protectインターフェースに、Google Analyticsへの同意を求めるメッセージとメニュー項目が表示されない場合、お住まいの国ではGoogle Analyticsが使用されていないことを意味します。

Cyber Protectの初回起動時に、Google Analyticsを有効化または拒否した場合、後からいつでもその設定を変更できます。

Google Analyticsを有効または無効にするには

1. Cyber Protectコンソールで、右上にあるアカウントアイコンをクリックします。
2. **[現在のプライバシー設定]** を選択します。
3. **[Google Analyticsデータ収集]** セクションで、次のボタンのいずれかをクリックします。
   - **[オン]**: Google Analyticsを有効化
   - **[オフ]**: Google Analyticsを無効化

索引

わ

漢字