管理ポータル

24.03

企業管理者ガイド

リビジョン: 2024/04/10

目次

このドキュメントについて

この文書は、クラウド管理ポータルを使用して、ユーザーアカウント、ユニット、クォータの作成と管理、クラウド組織へのアクセスの設定と制御、クラウド組織の使用状況と運用の監視を行いたいと考えているカスタマーの管理者を対象としています。

管理ポータルについて

管理ポータルは、データ保護サービスを提供するクラウドプラットフォームへのWebインターフェースです。

各サービスにはサービスコンソールと呼ばれる独自のWebインターフェースがありますが、管理ポータルを使用することで、サービスの使用状況を管理し、ユーザーアカウントと部署を作成し、レポートを生成するなどできます。

アカウントと部署

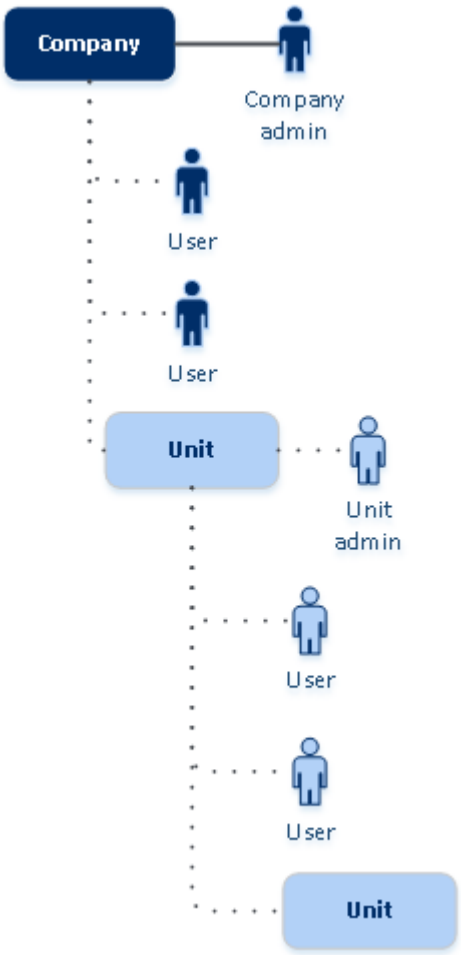
ユーザーアカウントには、管理者アカウントとユーザーアカウントの2つの種類があります。

- **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。

管理者は、組織の部署または部門に対応する部署を作成できます。各アカウントは、企業または部署レベルのいずれかに存在します。

管理者は、階層における管理者のレベルより下位の部署、管理者アカウント、ユーザーアカウントを管理できます。

次の図は、企業と2つの部署で構成される3つの階層レベルを示しています。点線で示している部署とアカウントはオプションで設定します。



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	管理者
部署の作成	いいえ	はい
アカウントの作成	いいえ	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
サービスの使用	はい	はい
使用状況レポートの作成	いいえ	はい

制限値（クォータ）管理

制限値（クォータ）はテナントのサービス利用能力を制限します。

管理ポータルで、サービスプロバイダーにより組織に割り当てられたサービスの制限値（クォータ）を表示できますが、それらを管理することはできません。

ユーザーのためのサービス制限値（クォータ）を管理できます。

組織の制限値（クォータ）を表示

管理ポータルで **[概要]** > **[使用状況]** へ進みます。組織に割り当てられた制限値（クォータ）が表示されたダッシュボードを見ることができます。各サービスの制限値（クォータ）は別のタブに表示されます。

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。

重要

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

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

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"（10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）

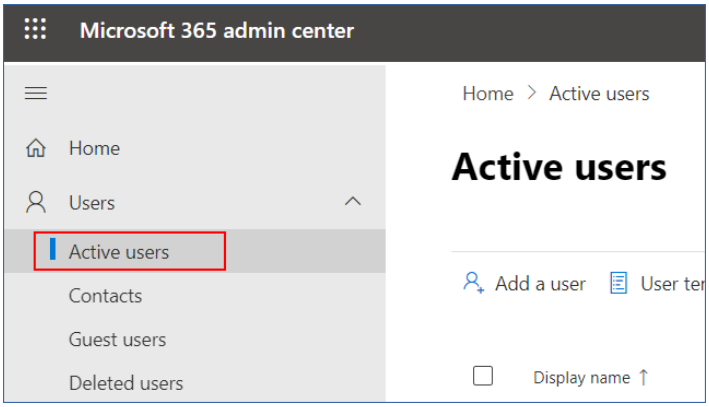
- **ローカルバックアップ**
  ローカルバックアップの制限値（クォータ）は、クラウドインフラストラクチャを使用して作成されたローカルバックアップの合計サイズを制限します。この制限値（クォータ）には追加容量を設定できません。
- **クラウドリソース**
  クラウドリソースの制限値（クォータ）は、バックアップストレージのための制限値（クォータ）とディザスタリカバリのための制限値（クォータ）を統合します。バックアップストレージの制限値（クォータ）は、クラウドストレージに保存されているバックアップの合計サイズを制限します。
  バックアップストレージの制限値（クォータ）容量を超過すると、バックアップは失敗します。

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。

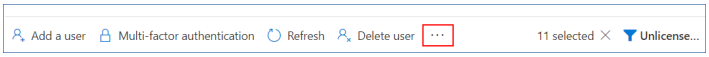
ライセンス対象外のユーザーのサインインを防止するには

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バックアップストレージのサイズを示しています。ディザスタリカバリストレージの使用量は、ディザスタリカバリサーバーで保護されているワークロードのバックアップストレージの使用量と同じになります。このストレージサイズは、サーバーが現在稼働しているかどうかにかかわらず、復元サーバーが作成された時点から計算されます。このクォータの追加容量に達した場合、プライマリサーバーと復元サーバーの作成や、既存プライマリサーバーのディスクの追加/拡張は実行できなくなります。このクォータの追加容量を超過した場合、フェールオーバーの開始、または停止したサーバーの起動が実行できなくなります。実行中のサーバーは引き続き実行されます。
- **コンピュートポイント**
  この制限値（クォータ）は、請求期間中にプライマリおよびリカバリサーバーによって消費されるCPU および RAM リソースを制限します。この制限値（クォータ）の追加容量に達した場合、すべて

のプライマリおよびリカバリサーバーがシャットダウンされます。次の請求期間の開始までこれらのサーバーを使用することはできません。デフォルトの請求期間は完全な暦月です。

制限値（クォータ）が無効に設定されている場合、請求期間に関係なくサーバーを使用することはできません。

- **パブリック IP アドレス**

  この制限値（クォータ）は、プライマリサーバーと復元サーバーに割り当てることができるパブリックIPアドレスの数を制限します。この制限値（クォータ）の追加容量に達した場合、それ以上サーバーにパブリックIPアドレスを有効にできなくなります。サーバー設定で **[パブリック IP アドレス]** チェックボックスをオフにすると、サーバーがパブリック IP アドレスを使用できないようにすることができます。その後、別のサーバーにパブリック IP アドレスを使用させることができます。パブリック IP アドレスは通常同じものではありません。

  制限値（クォータ）が無効にされている場合、すべてのサーバーがパブリックIPアドレスの使用を停止し、インターネットから到達できなくなります。

- **クラウドサーバー**

  この制限値（クォータ）はプライマリサーバーとリカバリサーバーの総数を制限します。この制限値（クォータ）の追加容量に達した場合、プライマリサーバーや復元サーバーを作成することはできません。

  制限値（クォータ）が無効になっている場合、サーバーはCyber Protectコンソールに表示されますが、利用できる操作は **[削除]** のみです。

- **インターネットアクセス**

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

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

File Sync & Share制限値（クォータ）

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。

- **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。

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。

- **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）

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。

- **Notaryのストレージ**
  公証済ファイル、署名済みファイル、および公証または署名が進行中のファイルの最大クラウドストレージスペースを定義します。
  このクォータの使用量を減らすには、既に公証済または署名済みのファイルを公証ストレージから削除します。
- **ノータリゼーション**
  公証サービスを使用して公証済にできる、最大のファイル数を定義します。
  ファイルは、公証ストレージにアップロードされるとすぐに公証済と見なされ、公証ステータスが **[実行中]** に変更されます。
  同じファイルが複数回ノータライズ（公証）されると、各ノータリゼーションは新しいノータリゼーションとしてカウントされます。
- **電子署名**
  デジタル電子署名の最大数を定義します。

ユーザーのための制限値（クォータ）定義

クォータにより、ユーザーのサービスの使用を制限できます。ユーザーのためのクォータを設定するには、**[企業管理]** 以下の **[ユーザー]** タブでユーザーを選択し、**[クォータ]** セクションで鉛筆アイコンをクリックします。

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。

制限値（クォータ）追加を指定すると、制限値（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。ユーザ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ユーザーに送られますが、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ユーザーに送られます。さらに25台に達するとCyber Protectionサービスが無効化されます。

Backup制限値（クォータ）

バックアップストレージのクォータと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。

ストレージの制限値（クォータ）

- **バックアップストレージ**

バックアップストレージのクォータにより、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が制限されます。バックアップストレージのクォータを超過すると、バックアップは失敗します。

重要
ローカルエージェントとクラウドエージェントは別個のクォータを消費します。両方のエージェントを使用して同じワークロードをバックアップした場合、二重に課金されます。例:
- ローカルエージェントを使用して120人のユーザーのメールボックスをバックアップし、クラウドエージェントを使用して同じユーザーのOneDriveファイルをバックアップする場合、Microsoft 365の240シート分が課金されます。
- ローカルエージェントを使用して120人のユーザーのメールボックスをバックアップし、クラウドエージェントを使用して同じメールボックスをバックアップする場合、Microsoft 365の240シート分が課金されます。

File Sync & Share制限値（クォータ）

ユーザーのために、以下のFile Sync & Share制限値（クォータ）を定義できます。

- **個人用ストレージ領域**
  ユーザーのファイルに割り当てられるクラウドストレージスペースを定義します。

Notary制限値（クォータ）

ユーザーのために、以下のNotary制限値（クォータ）を定義できます。

- **Notaryのストレージ**
  公証済ファイル、署名済みファイル、および公証または署名が進行中のファイルの最大クラウドストレージスペースを定義します。
  このクォータの使用量を減らすには、既に公証済または署名済みのファイルを公証ストレージから削除します。
- **ノータリゼーション**
  公証サービスを使用して公証済にできる、最大のファイル数を定義します。
  ファイルは、公証ストレージにアップロードされるとすぐに公証済と見なされ、公証ステータスが **[実行中]** に変更されます。
  同じファイルが複数回ノータライズ（公証）されると、各ノータリゼーションは新しいノータリゼーションとしてカウントされます。
- **電子署名**
  デジタル電子署名の最大数を定義します。

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。

詳細手順

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。説明します。

- 管理者アカウントの承認
- 管理ポータルとサービスへのアクセス
- 部署の作成
- ユーザーアカウントの作成

管理者アカウントの承認

サービスに登録すると、次の情報が含まれている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"（16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。

管理ポータルとサービスへのアクセス

1. サービスコンソールのログインページに移動します。
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。
4. 次のいずれかを実行します。
   - 管理ポータルにログインするには、**[管理ポータル]** をクリックします。
   - サービスにログインするには、サービスの名前をクリックします。

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。

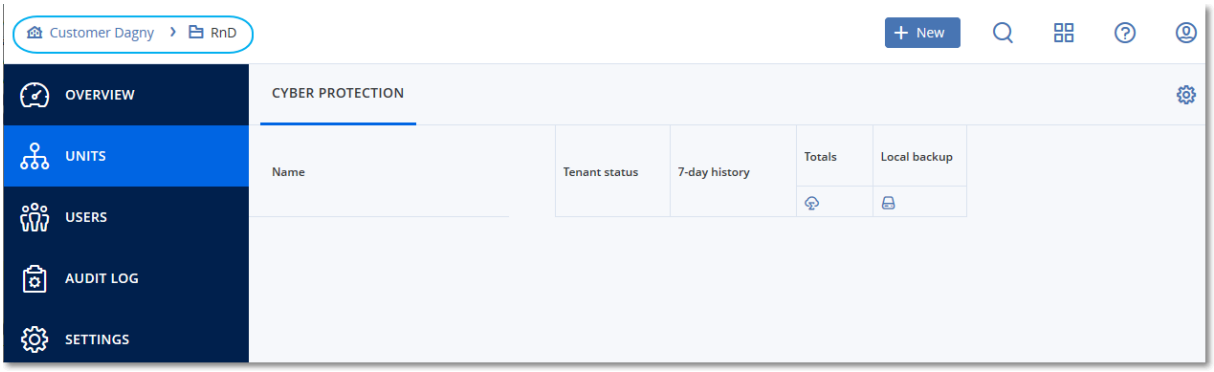
管理ポータルとサービスコンソールを切り替える

管理ポータルとサービスコンソールを切り替えるには、右上にある アイコンをクリックして、**[管理ポータル]** または移動先のサービスを選択します。

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、企業レベルまたは部署レベルで操作します。これは左上隅に示されています。

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。部署名をクリックすると階層の詳細を確認できます。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、現在操作している企業または部署のみが表示され、設定の範囲になります。。例:

- **[新規]** ボタンを使用すると、この企業または部署でのみ部署またはユーザーアカウントを作成できます。
- **[部署]** タブには、この企業または部署の直下の部署のみが表示されます。
- **[ユーザー]** タブには、この企業または部署に存在するユーザーアカウントのみが表示されます。

部署の作成

部署にアカウントを作成しない場合は、この手順をスキップします。

後で部署を作成する場合、既存のアカウントを部署間または企業と部署の間で移動できませんのでご注意ください。まず、部署を作成して、そこにアカウントを作成する必要があります。

部署を作成するには

1. 管理ポータルにログインします。
2. 新しい部署を作成する部署を指定します。
3. 右上にある **[新規]** > **[ユニット]** をクリックします。

4. **[名前]** で、新しい部署の名前を指定します。
5. [オプション] **[言語]** で、この部署で使用される通知、レポート、およびソフトウェアのデフォルト言語を変更します。
6. 次のいずれかを実行します。
   - 部署管理者を作成するには、**[次へ]** をクリックしてから、手順4から開始して『ユーザーアカウントの作成』に記載されている手順に従います。
   - 管理者なしで部署を作成するには、**[保存して閉じる]** をクリックします。後で部署に管理者とユーザーを追加することができます。

新しく作成された部署が **[部署]** タブに表示されます。

部署設定を編集する、または連絡先情報を指定する場合は、**[部署]** タブで部署を選択して、編集するセクションの鉛筆アイコンをクリックします。

ユーザーアカウントの作成

追加のユーザーアカウントを作成しない場合は、この手順をスキップします。

次の場合は、追加のアカウントを作成することができます:

- 企業管理者アカウント - 管理業務を他の人と共有する場合
- 部署管理者アカウント - 部署に限定したサービス管理を委任する場合
- ユーザーアカウント - 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

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. 新しいユーザーアカウントを作成する部署を指定します。
3. 右上にある **[新規]** > **[ユーザー]** をクリックします。
4. アカウントの次の情報を指定します:
   - **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。

   - （オプション）**名**
   - （オプション）**姓**
   - **[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. 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。
   - **[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。
   - **[部署管理者]** チェックボックスをオンにすると、ユーザーは管理ポータルにアクセスできますが、サービスに応じてサービス管理者ロールを持つ場合と持たない場合があります。
   - チェックボックスをオンにしない場合、ユーザーは選択したサービスにおける選択したロールを持ちます。
6. **[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、**[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。企業向けの保護サービスのディザスタリカバリ機能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。 例えばこのロールでは、エンドポイント検知と応答画面に対する完全な許可（ウィジェットを含む）が付与されます。
	読み取り専用管理者 パートナーレベル	このロールを割り当てられたユーザーには、パートナーの管理ポータルの全オブジェクトに対する読み取り専用アクセスと、このパートナーと関連するすべてのカスタマーの管理ポータル内にある全オブジェクトに対する読み取り専用アクセスが付与されます。また、このロールのユーザーは、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。これらのユーザーは保護計画を編集できますが、スクリプト計画、監視計画、またはエージェント計画に対する変更を保存することはできません。
	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。
保護	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、カスタマーの保護の設定と管理が可能になります。 このロールは、例えば、ディザスタリカバリ機能やエンドポイント検知と応答機能、または企業の許可リストを構成および管理するために必要となります。
	読み取り専用管理者	このロールでは、保護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やエンドポイント検知と応答機能、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。
	ユーザー	このロールにより、管理者権限がなくても保護サービスが使用できるようになります。このロールを割り当てられたユーザーは、エンドポイント検知と応答などの機能にアクセスできますが、組織内の他のユーザーのデータにアクセスすることはできません。
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。このロールを持つアカウントでは、機能へのアクセスが提供されないため、**ユーザー**クォータの一部としてカウントされることはありません。
	ユーザー	このロールにより、File Sync & Shareサービスが使用できるようになります。ユーザーは、自分自身のデータと共有されているデータにのみアクセスできます。
	ゲスト	このロールを持つアカウントは、File Sync & Shareユーザーが、File Sync & Shareサービスを使用することができないCyber Protect Cloudユーザー、または非Cyber Protect Cloudユーザーとコンテンツを共有するときに作成されます。 Guestロールには同期フォルダが付帯しません。またクラウドストレージが消費されず、機能へのアクセスが提供されないため、**ユーザー**クォータの一部としてカウントされることはありません。ゲストは、ユーザーまたは管理者ロールに「昇格」することができます。
Notary	管理者	このロールにより、ユーザーのNotaryの設定と管理が可能になります。
	ユーザー	このロールにより、管理者権限がなくともNotaryサービスが使用できるようになります。このロールを割り当てられたユーザーは、組織の他のユーザーのデータにはアクセスできません。

読み取り専用管理者ロール

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

- システムレポートなどの診断用データの収集。
- バックアップの復元ポイントを確認できますが、バックアップコンテンツにドリルダウンしたり、ファイル、フォルダ、またはEメールを表示したりすることはできません。

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、Cyber Protectコンソールに表示されるアクティブアラートのリストに基づいて、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

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。

ユーザーアカウントを削除するには

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

作成が完了すると以下のようになります。

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

ユーザーアカウントの所有権の移転

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32桁のコードを使用し、認証アプリケーションへ手動で追加できます。

重要
コードを保存しておくことを強くお勧めします（QRコードの印刷、一時ワンタイムパスワード（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一時ワンタイムパスワード（TOTP）シークレットが必要になります。

6. 一時ワンタイムパスワード（TOTP）コードは認証アプリケーション内に生成されます。30秒間隔で自動的に再生成されます。
7. ユーザーは、パスワードの入力後に**二要素認証を設定**画面上でTOTPコードを入力する必要があります。
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。

新しいデバイスで二要素認証を復元するには

以前設定したモバイル認証アプリにアクセスできる場合:

1. 新しいデバイスに認証アプリをインストールします。
2. デバイスで二要素認証を設定した際に保存したPDFファイルを使用します。このファイルには、認証アプリをアクロニスアカウントに再度リンクする際に認証アプリに入力する必要がある、32桁のコードが含まれています。

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

3. セットアップ中にPDFファイルを保存していなかった場合:

   a. *[二要素認証をリセット]をクリックして、事前にセットアップしたモバイル認証アプリに表示されているワンタイムパスワードを入力します。*

   b. 画面の指示に従います。

   以前セットアップしたモバイル認証アプリにアクセスできない場合:

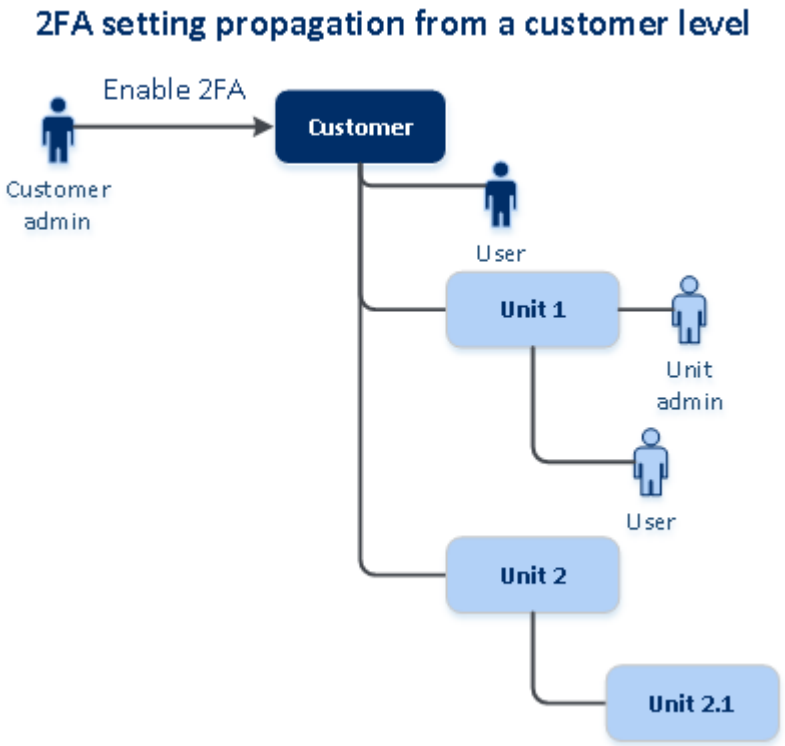
   1. 新しいモバイルデバイスを用意します。
   2. 保存されたPDFファイルを使用して、新しいデバイスをリンクします（デフォルトのファイル名は `cyberprotect-2fa-backupcode.pdf`）。
   3. バックアップからアカウントへのアクセス権を復元します。バックアップがモバイルアプリでサポートされていることを確認してください。
   4. アプリでサポートされている場合は、別のモバイルデバイスから同じアカウントでアプリを開きます。

二要素設定のテナントレベル内での伝達

二要素認証は**組織**レベルで設定されます。二要素認証を自分の組織限定で設定できます。

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。

- 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. 部署レベルの二要素認証を設定することはできません。
2. 子組織（部署）のユーザーのための二要素認証設定を管理できます。

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。

エージェントの自動アップデート

重要
現在、保護を有効にしている場合のみ、エージェントのアップデート管理機能にアクセスできます。

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。

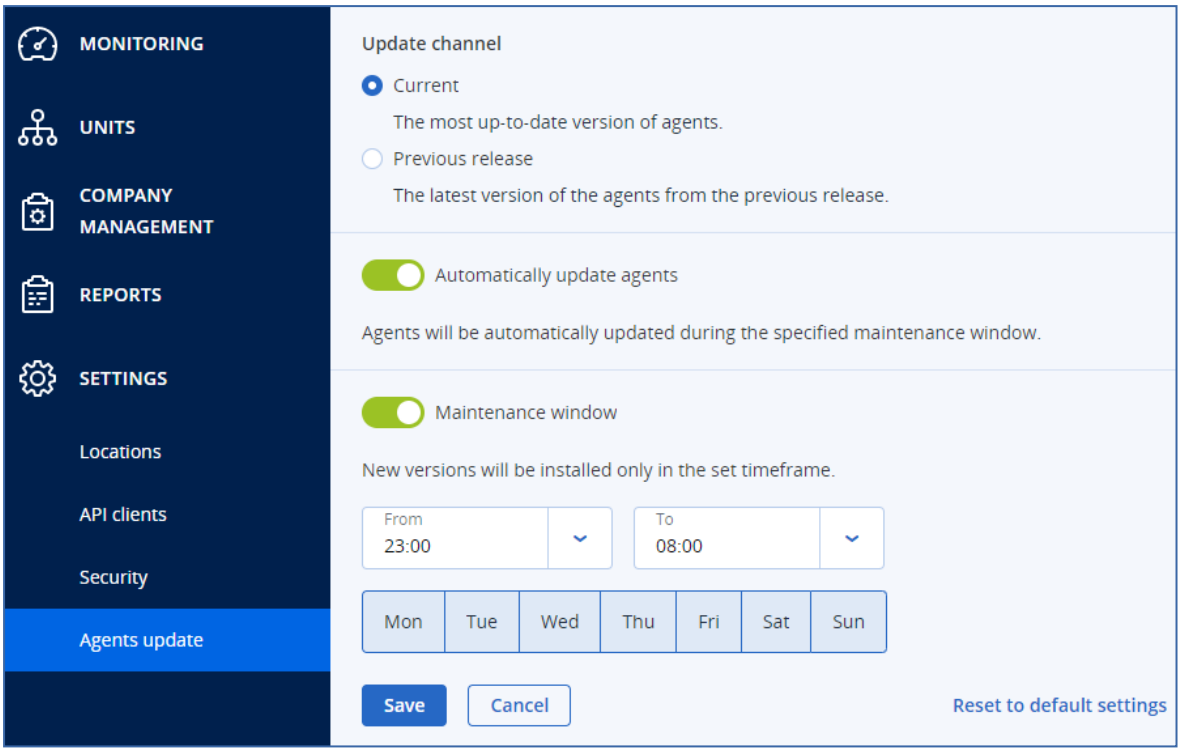
注意
個別マシン上のエージェントを管理し、自動アップデートの設定をカスタマイズする場合、『Cyber Protectユーザーガイド』の「エージェントの更新」セクションを参照してください。

エージェントを自動アップデートするには

注意
プロテクションが有効化されていない場合、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サービスプロバイダーから継承されます。

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
プロテクションモジュールを有効化している場合、エージェントアップデートの監視のみ実行可能です。

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。

不変ストレージの構成

不変ストレージを使用すると、指定した保持期間中に削除されたバックアップにアクセスできます。これらのバックアップからコンテンツをリカバリすることはできますが、それらを変更、移動、または削除することはできません。保持期間が終了すると、削除済みバックアップは恒久的に削除されます。

不変ストレージには以下のバックアップが含まれています。

- 手動で削除されたバックアップ。
- 保護計画の **[保持する期間]** セクションまたはクリーンアップ計画の **[保持ルール]** セクションの設定に従って自動的に削除されるバックアップ。

削除されたバックアップは不変ストレージに保存され、ストレージスペースを消費します。また消費量に応じて課金が発生します。

削除されたテナントは、不変ストレージを含め、ストレージの利用料はかかりません。

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**
  不変ストレージを無効にしたり、再度有効にしたりできます。保持期間の変更や、コンプライアンスモードへの切り替えもできます。
- **コンプライアンスモード**

  警告
  一度コンプライアンスモードを選択すると、元に戻せなくなります。

  不変ストレージを無効にすることはできません。保持期間を変更したり、ガバナンスモードに戻したりすることはできません。

不変ストレージを構成すると、管理者アカウントが属するテナントで二要素認証が必須となります。

注意
削除されたバックアップへのアクセスを許可するには、受信接続用にバックアップストレージのポート40440を開く必要があります。

不変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. 14～3650日の範囲で保持期間を指定します。
   デフォルトの保持期間は14日間です。保持期間が長くなると、ストレージの使用量が増える可能性があります。
4. 不変ストレージモードを選択し、プロンプトが表示されたら選択を確定します。
5. **[保存]** をクリックします。

   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。このモードを選択した後は、不変ストレージを無効にしたり、モードや保持期間を変更したりすることはできません。

6. 既存のアーカイブで不変ストレージをサポートするには、該当のアーカイブに新しいバックアップを作成します。
   新しいバックアップを作成するには、手動またはスケジュールで保護計画を実行します。

   警告
   アーカイブで不変ストレージがサポートされていない状態でバックアップを削除すると、バックアップは永久に削除されます。

不変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。

   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しても、すぐに変更が適用されるわけではありません。14日間の猶予期間中、不変ストレージは引き続き有効であり、元の保持期間に従って削除済みバックアップにアクセスできます。猶予期間が終了すると、不変ストレージ内のすべてのバックアップは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。

サポートされるストレージとエージェント

- 不変ストレージはクラウドストレージのみでサポートされます。
  不変ストレージは、 Cyber Infrastructureバージョン4.7.1以降を利用する、Acronisまたはパートナーがホストするクラウドストレージストレージで使用できます。
  Cyber Infrastructure ストレージ、Amazon S3 および EC2 ストレージ、Microsoft Azure ストレージなど、 Cyber Infrastructure Backup Gatewayで使用できるすべてのストレージがサポートされています。

不変ストレージでは、 Cyber Infrastructure のバックアップゲートウェイサービス用にTCPポート40440が開放されている必要があります。バージョン4.7.1以降では、TCPポート40440は、**[バックアップ（ABGW）パブリック]** トラフィックタイプで自動的に開放されます。トラフィックタイプの詳細については、Acronis Cyber Infrastructureの文書を参照してください。

- 不変ストレージには、プロテクションエージェントバージョン21.12（ビルド15.0.28532）以降が必要です。
- TIBX（バージョン12）バックアップのみがサポートされています。

監視

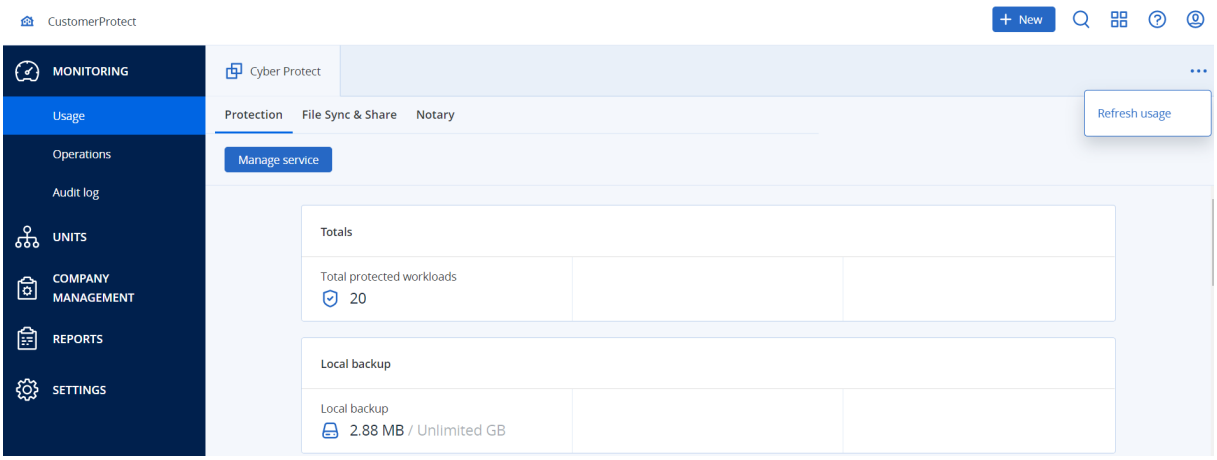
サービスの使用状況や操作に関する情報にアクセスするには、**[監視]** をクリックします。

使用状況

[使用状況] タブには、サービスの使用状況（制限値（クォータ）があればそれを含む）の概要が表示され、サービスコンソールにアクセスできます。

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。



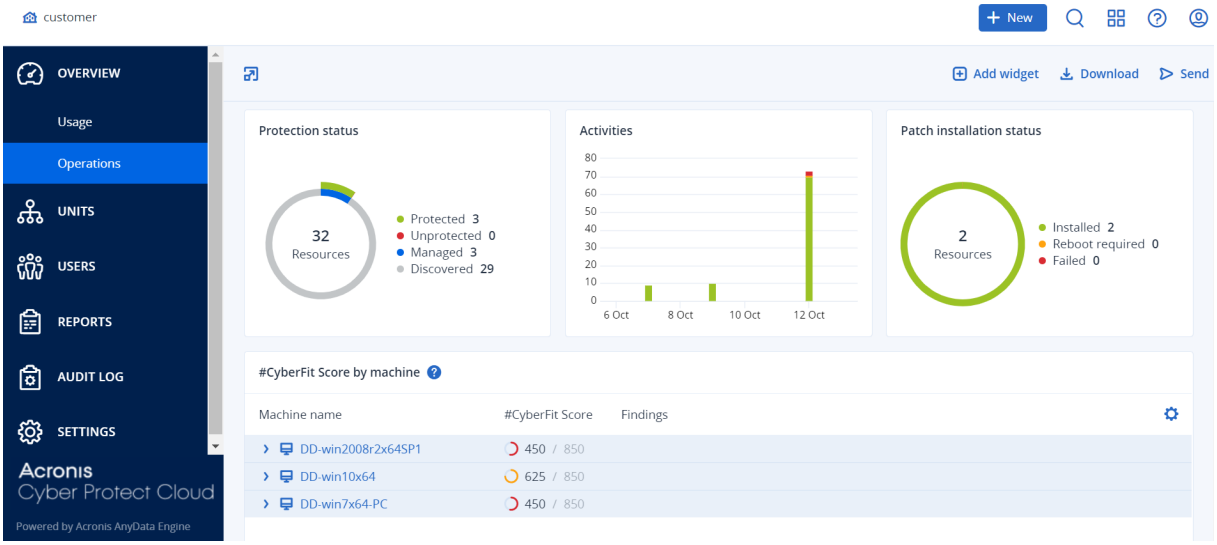
操作ダッシュボード

[操作] ダッシュボードは、企業レベルでの運用時には企業管理者のみが使用できます。

[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。

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、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。同じ種類の複数のウィジェットを異なるフィルタで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、フィルタを設定したり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鉛筆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

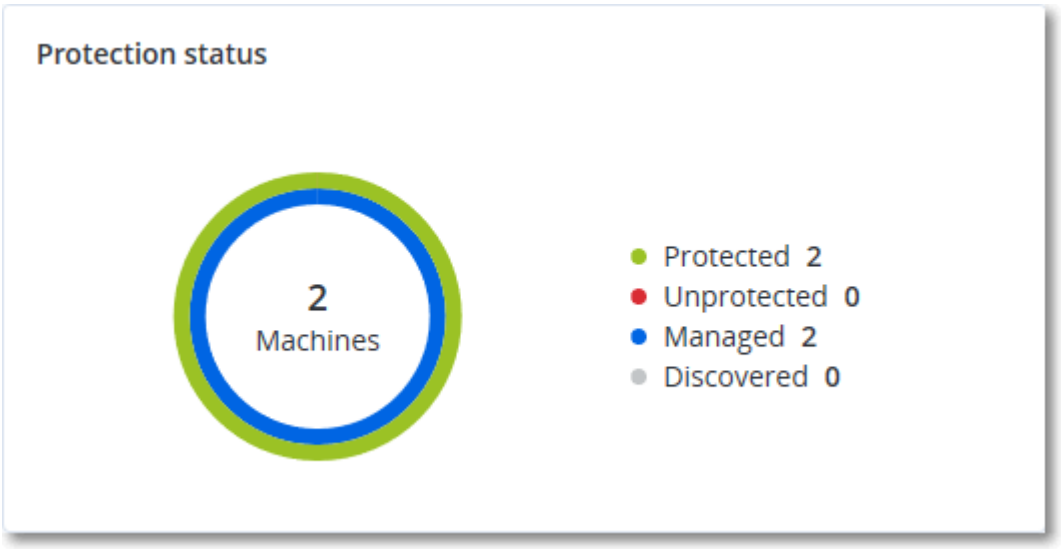
保護ステータス

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。

Discovered machines

Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

マシンごとの #CyberFit スコア

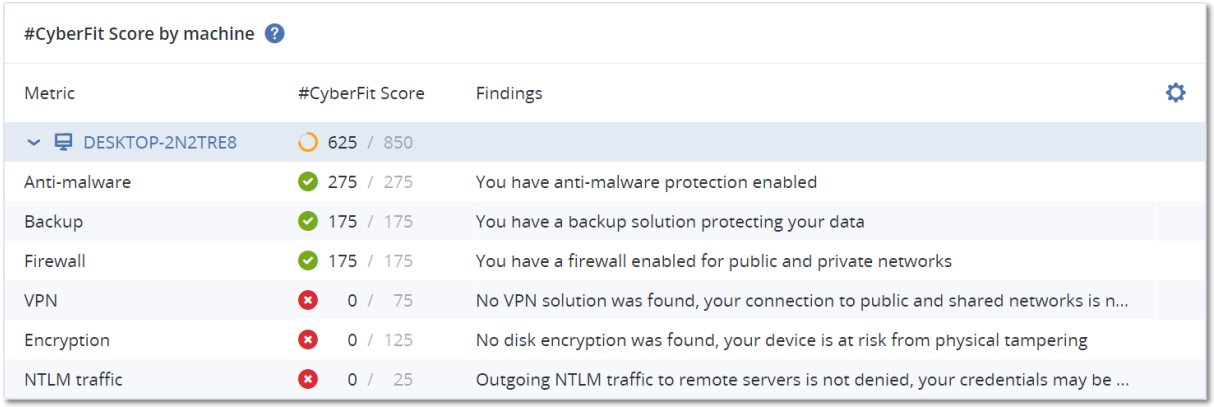
このウィジェットは、各マシンの合計#CyberFitスコア、その複合スコア、および次の各メトリクスに関する評価結果を示します。

- 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

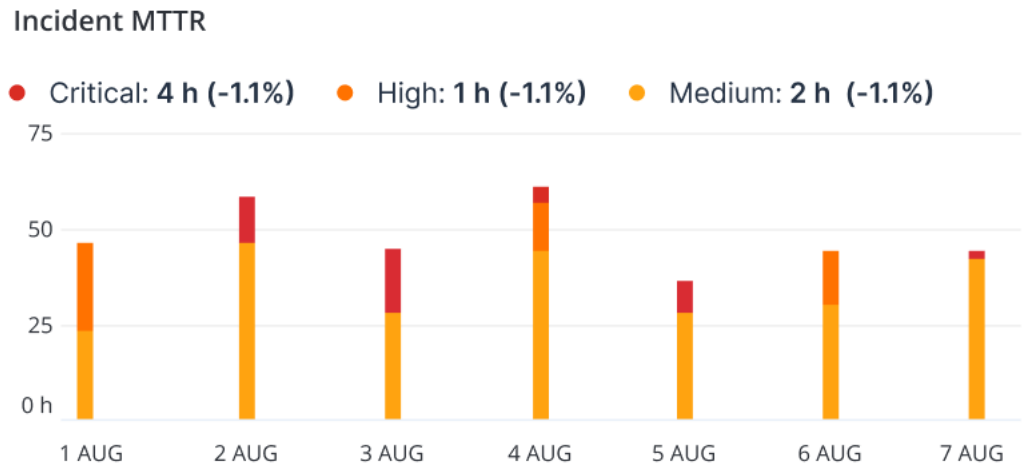
このウィジェットには、インシデントの数が多い、上位5つのワークロードが表示されます（[**すべて表示**] をクリックすると、ウィジェットの設定に応じてフィルタリングされたインシデントのリストにリダイレクトされます）。

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**、**閉鎖済み**、**偽陽性**の順に表示されます。続いて、詳細に分析したいワークロードをクリックし、表示されたポップアップで関連するカスタマーを選択すると、ウィジェットの設定に応じてインシデントのリストがリフレッシュされます。

インシデントMTTR

このウィジェットでは、セキュリティインシデントの平均解決時間を表示します。これは、インシデントの調査や解決のスピードを示しています。

列をクリックすると、重要度（**重大**、**高**、**中**）別のインシデントの内訳と、重要度レベル別の解決に要した時間が表示されます。括弧内の%数値により、前期比での増減が表わされます。

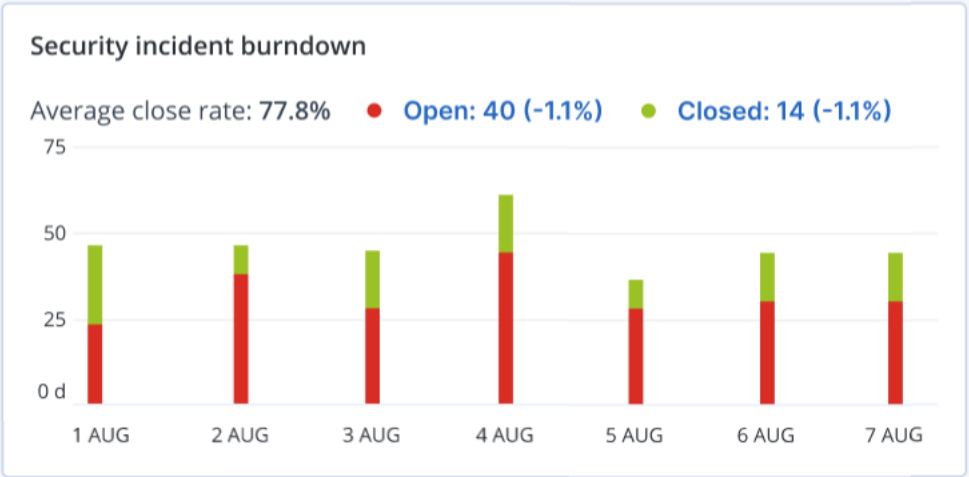


セキュリティインシデントのバーンダウン

このウィジェットでは、インシデントがクローズ状態になるまでの効率性が表示されます。この効率性は、オープン状態のインシデントの数と、一定期間内にクローズされたインシデントの数の比較により表わされます。

列をホバーすると、選択した日付におけるクローズ状態およびオープン状態のインシデントの内訳が表示されます。[オープン] の値をクリックするとポップアップが表示され、関連するテナントを選択できます。選択したテナントについて、現在オープンな状態のインシデント（**調査中**または**開始前**のステータス）を表示するフィルターが適用されたインシデントリストが表示されます。[クローズ] の値をクリックすると選択したテナントについて、現在オープンな状態ではないインシデント（**閉鎖済み**または**偽陽性**のステータス）を表示するフィルターが適用されたインシデントリストが表示されます。

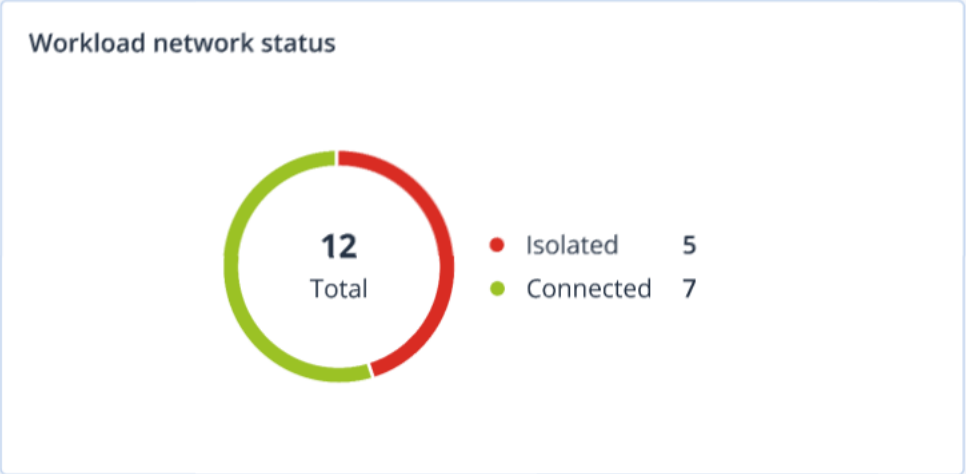
括弧内の%数値により、前期比での増減が表わされます。



ワークロードのネットワークステータス

このウィジェットでは、ワークロードの現在のネットワーク状態が表示され、分離されているワークロードの数と接続済みのワークロードの数が示されます。

[分離] の値をクリックすると、ポップアップが表示されるので、関連するテナントを選択します。表示されるワークロードビューではフィルターが適用され、分離されたワークロードが表示されます。[接続済み] の値をクリックすると、接続済みのワークロード（選択したテナントの）を表示するフィルターが適用されたエージェントリストとワークロードが表示されます。



ディスク状態監視

ディスク状態の監視は、現在のディスク状態のステータスに関する情報と予測情報を提供し、ディスク障害に関連して発生する可能性のあるデータ損失を防ぐことができます。HDDおよびSSDディスクがサポートされています。

制限事項

- ディスク状態の予測はWindowsを実行するマシンのみをサポートします。
- 物理マシンのディスクのみを監視します。仮想マシンのディスクは監視対象ではなく、ディスク状態ウィジェットに表示されません。
- RAID構成はサポートされていません。ディスク状態ウィジェットには、RAIDが実装されたマシンに関する情報は含まれていません。
- NVMe SSDはサポートされていません。

ディスク状態は、次のいずれかのステータスで示されます。

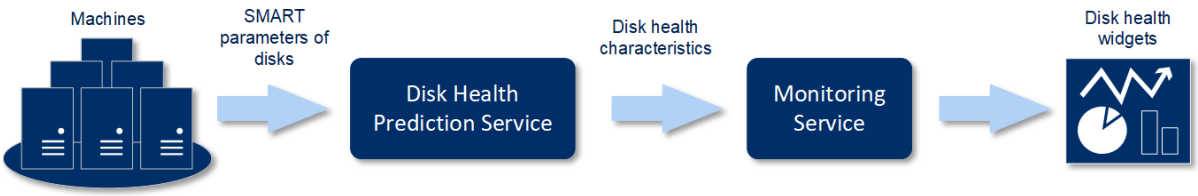
- **OK**
  ディスク状態が70～100%です。
- **警告**
  ディスク状態が30～70%です。
- **重大**
  ディスク状態が0～30%です。
- **ディスクデータの計算中**
  現在のディスク状態と予測を計算中です。

仕組み

ディスク状態予測サービスは、AI ベースの予測モデルです。

1. プロテクションエージェントがディスクのSMARTパラメータを収集して、このデータをディスク状態予測サービスに渡します。
   - SMART 5 - リアロケートされたセクタの数です。
   - SMART 9 - 通電時間です。
   - SMART 187 - 報告された未修正エラーです。
   - SMART 188 - コマンドタイムアウトです。
   - SMART 197 - 現在保留されているセクタの数です。
   - SMART 198 - オフラインの未修正セクタの数です。
   - SMART 200 - 書き込みエラー発生率です。
2. ディスク状態予測サービスは、受信したSMARTパラメータを処理して予測を実行し、次のようにディスク状態の特性を提供します:
   - ディスク状態の現在のステータス:OK、警告、重大。
   - ディスク状態の予測: 陰性、安定、陽性。
   - ディスク状態の予測は百分率で示されます。

   予測期間は1か月間です。
3. 監視サービスはこれらの特性情報を受信し、Cyber Protectコンソールのディスク状態ウィジェットに関連情報を表示します。



ディスク状態ウィジェット

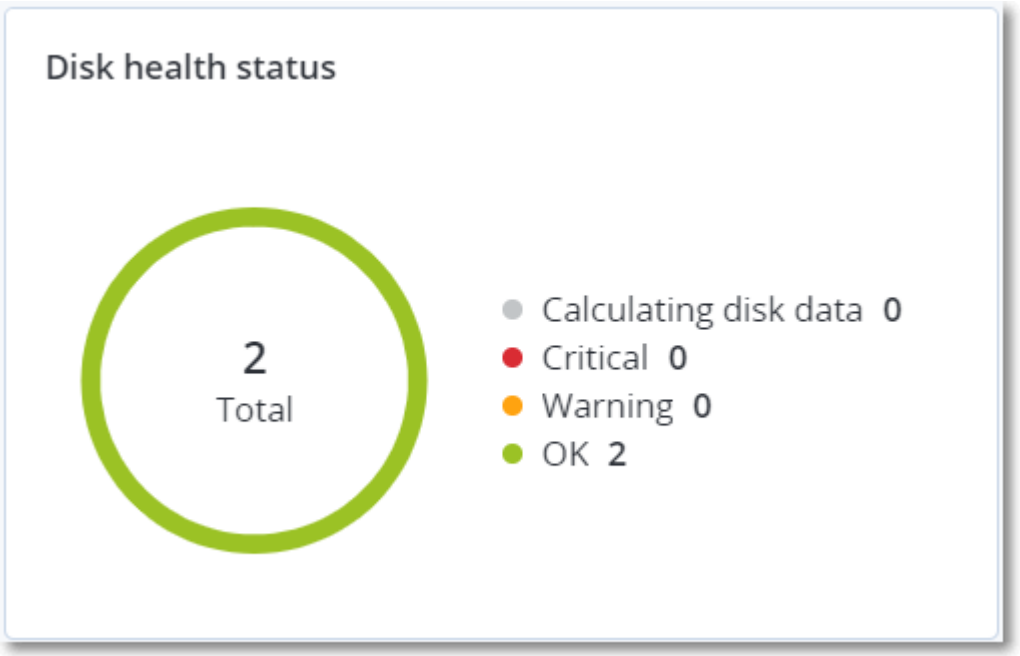
ディスク状態の監視結果は、Cyber Protectコンソールで利用できる以下のウィジェットに表示されます。

- **ディスク状態の概要**は、階層の詳細情報を含むツリー図ウィジェットです。階層は、ツリーをたどるようにして切り替えることができます。
  - マシンレベル
    選択したカスタマーのマシンに関する、ディスク状態ステータスの要約情報を表示します。最も重大なディスクステータスのみが表示されます。他のステータスは、該当するブロックにマウスを移動（ホバー）することでツールの先端に表示されます。マシンのブロックサイズは、該当するマシンの全ディスクの合計サイズによって異なります。マシンのブロックの色は、見つかったもっとも重大なディスクステータスによって異なります。

- ディスクレベル
  選択済みのマシンに現在搭載されている全ディスクのディスク状態ステータスを表示します。各ディスクブロックには、以下のいずれかのディスク状態予測とその確率がパーセンテージで表示されます。
  - 低下傾向
  - 安定傾向

- 改善傾向

- **ディスク状態ステータス**は、円グラフウィジェットで各ステータス別にディスクの数を示します。



ディスク状態アラート

30分間隔でディスク状態のチェックが実行されるとともに、対応するアラートが1日に1回生成されます。ディスク状態が**警告**から**重大**に変化する場合、必ずアラートが生成されます。

アラート名	重大度	ディスク状態ステータス	説明
ディスク障害が生じる可能性があります	警告	(30 – 70)	このマシン上の<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。

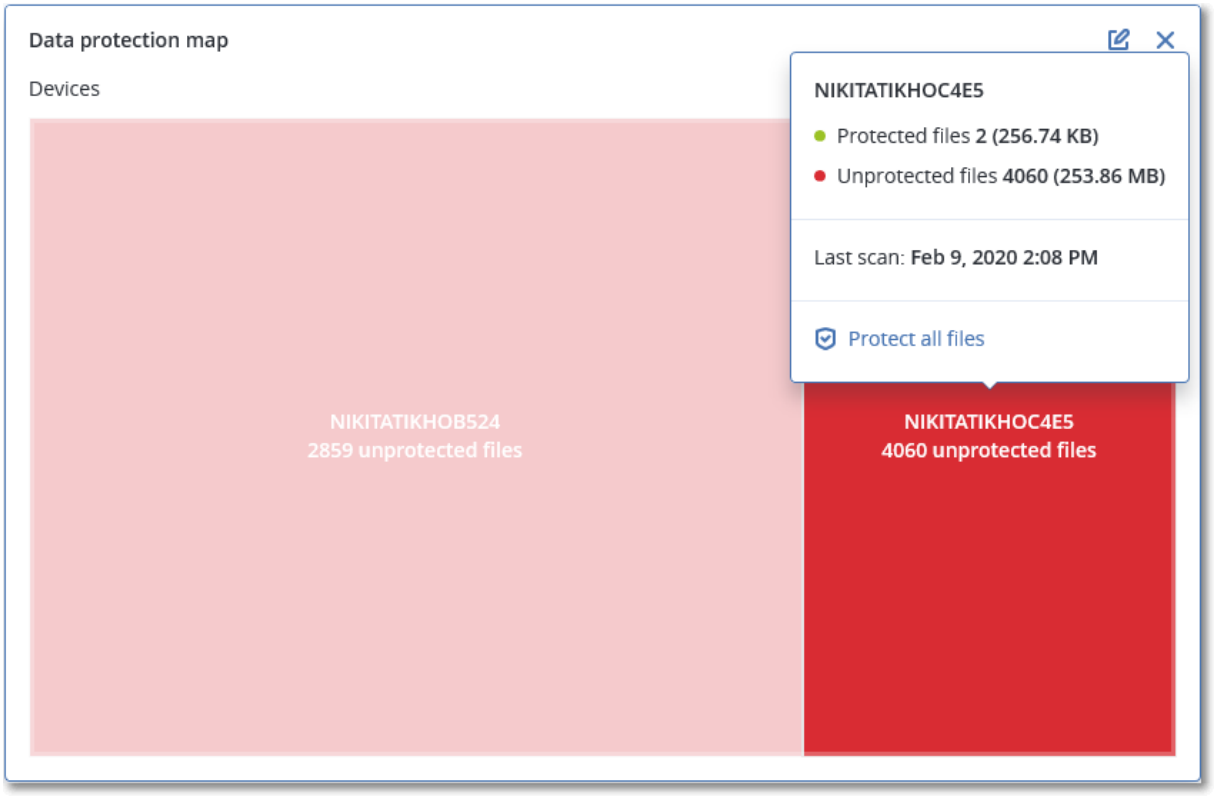
各ブロックのサイズは、カスタマー/マシンに属する重要なすべてのファイルの合計数/サイズによって異なります。

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** - 選択済みのマシン/ロケーションにおける既存のバックアップの設定で、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** - 選択済みのマシン/ロケーションにおける既存のバックアップの設定で、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** - 選択済みのマシン/ロケーションにおける既存のバックアップの設定で、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** - 選択済みのマシン/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。ツリーマップウィジェットにはマシンレベルの詳細が表示されます。

- 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。

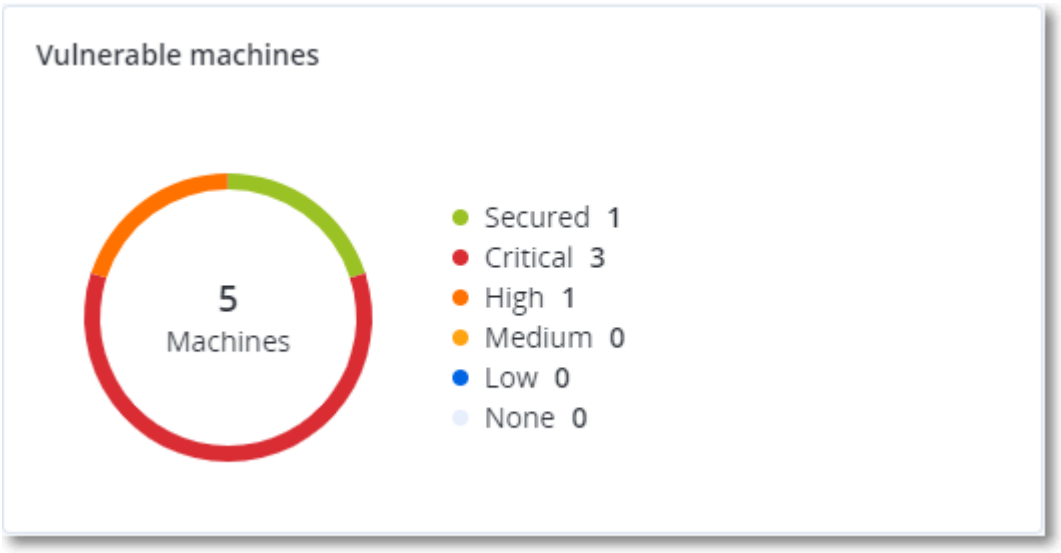
脆弱性診断ウィジェット

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。

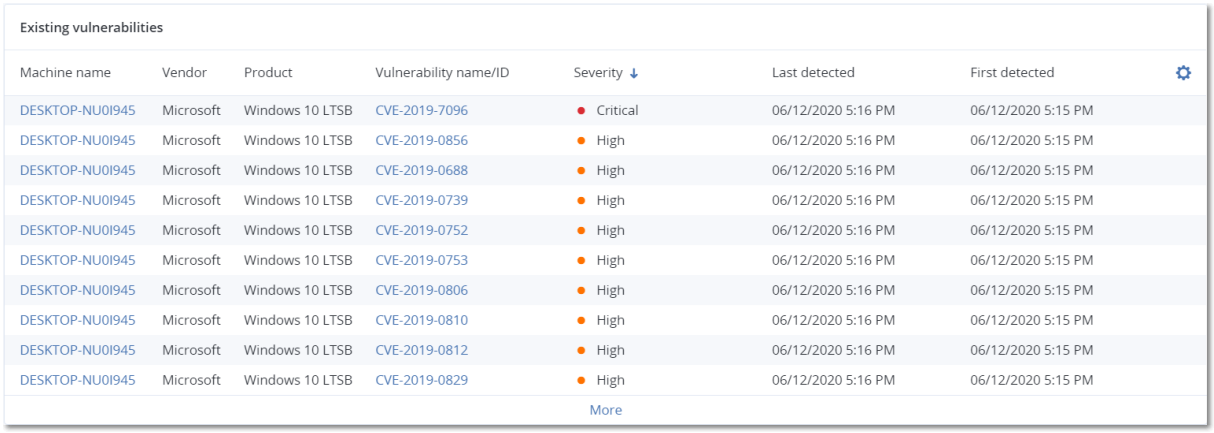
- セキュア: 脆弱性が見つからない
- 重大:9.0 - 10.0 CVSS
- 高:7.0 - 8.9 CVSS
- 中:4.0 - 6.9 CVSS
- 低:0.1 - 3.9 CVSS
- なし:0.0 CVSS



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

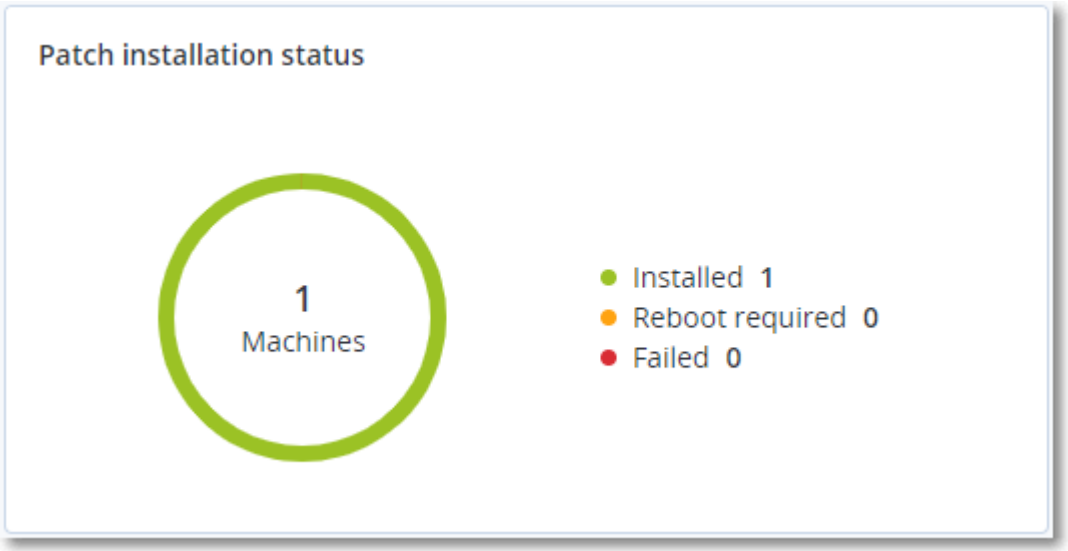
パッチインストールウィジェット

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

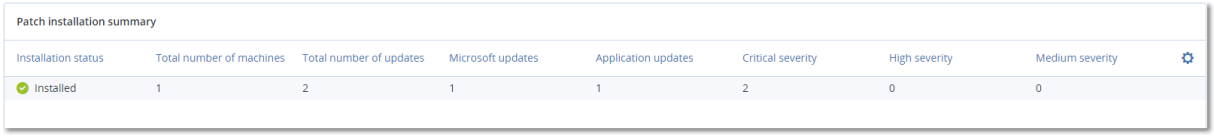
このウィジェットは、パッチインストールステータスでグループ化したマシンの数を表示します。

- **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。



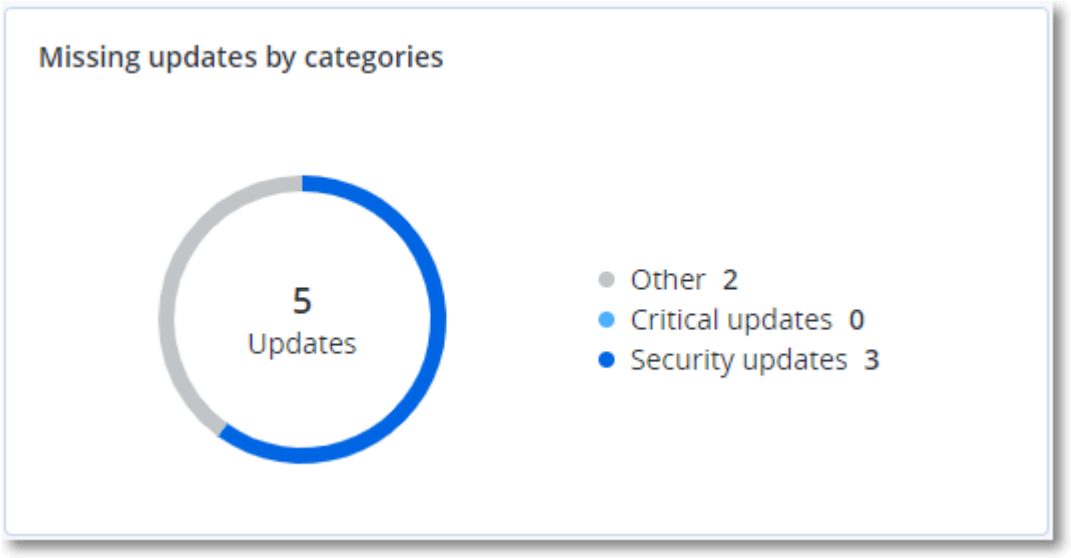
パッチインストール履歴

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

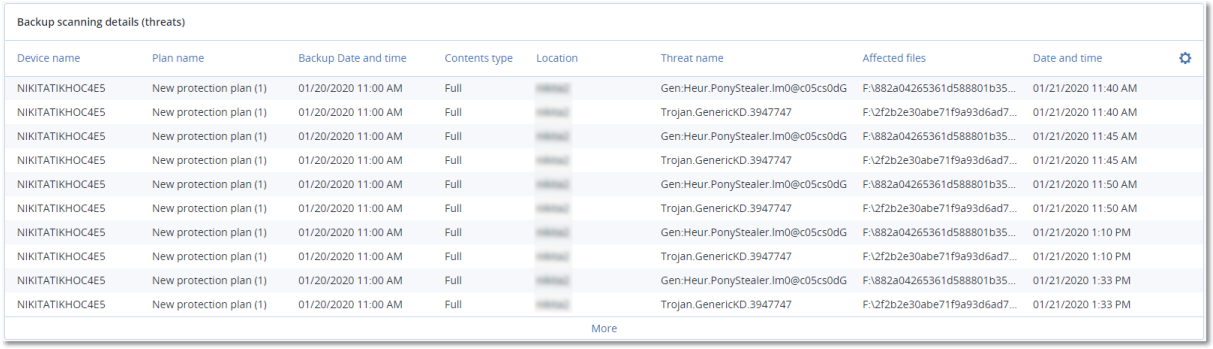
このウィジェットは、見つからないアップデートの数をカテゴリ別に表示します。次のカテゴリで表示されます。

- セキュリティアップデート
- 重要なアップデート
- その他



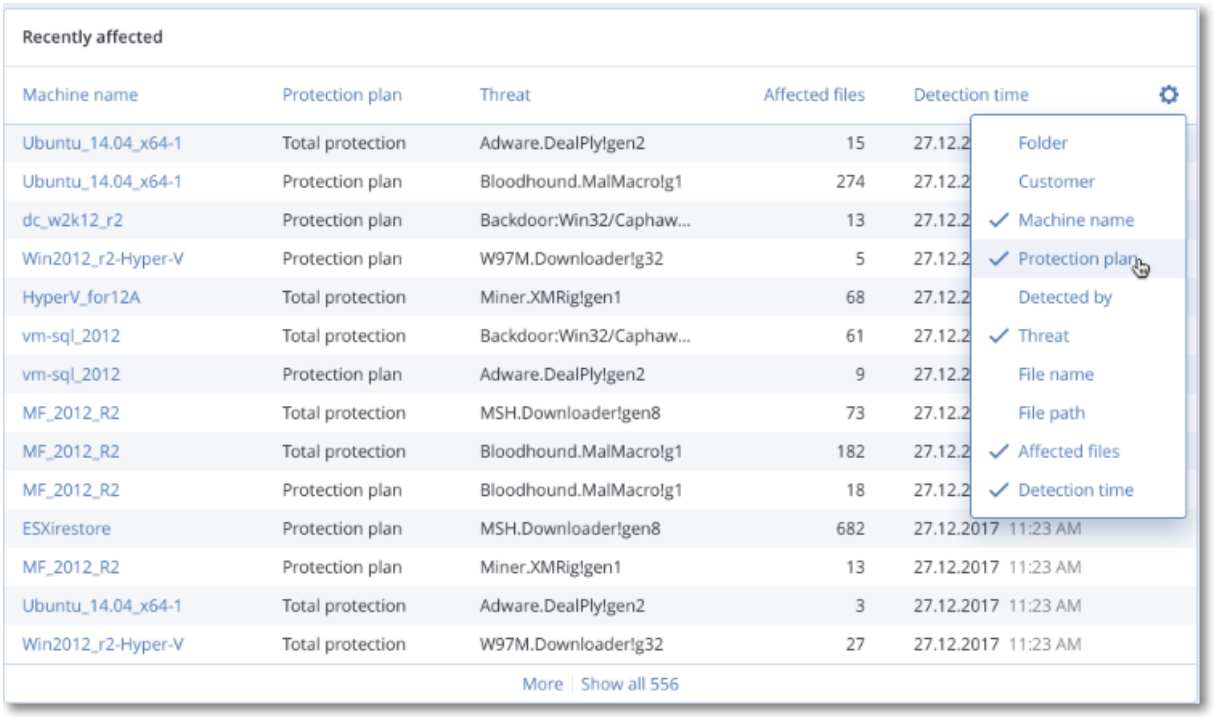
バックアップスキャンの詳細

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。

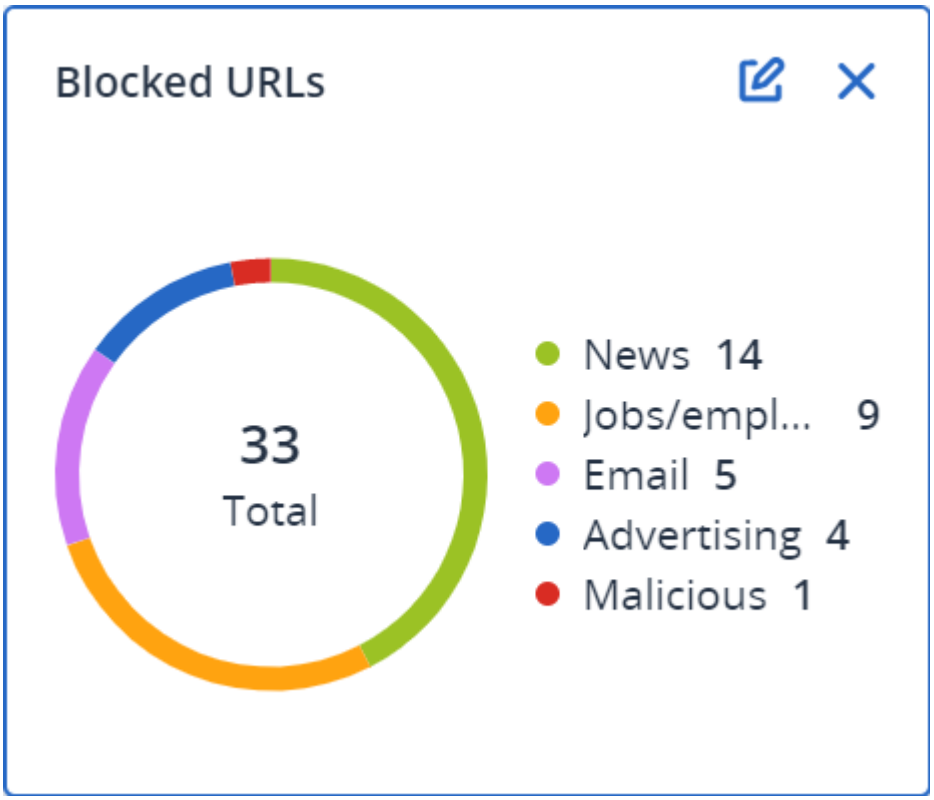
最近影響を受けたワークロードのデータをダウンロードするには

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。

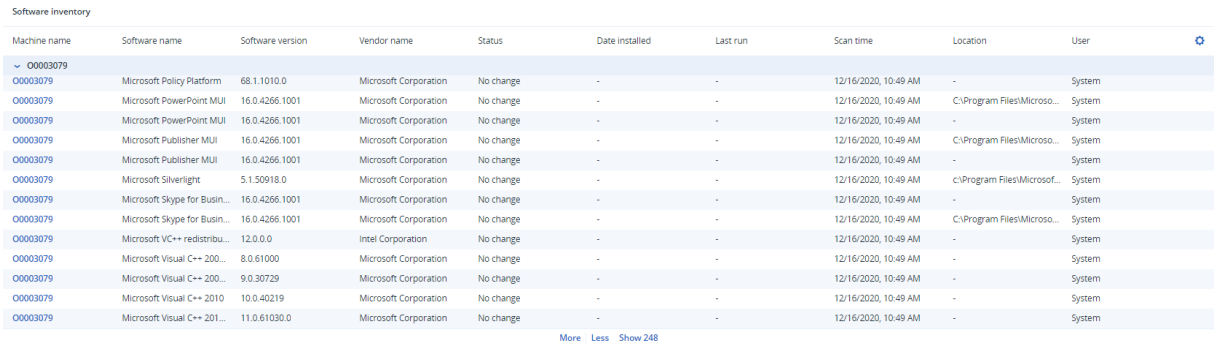
ブロックされたURL

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、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。

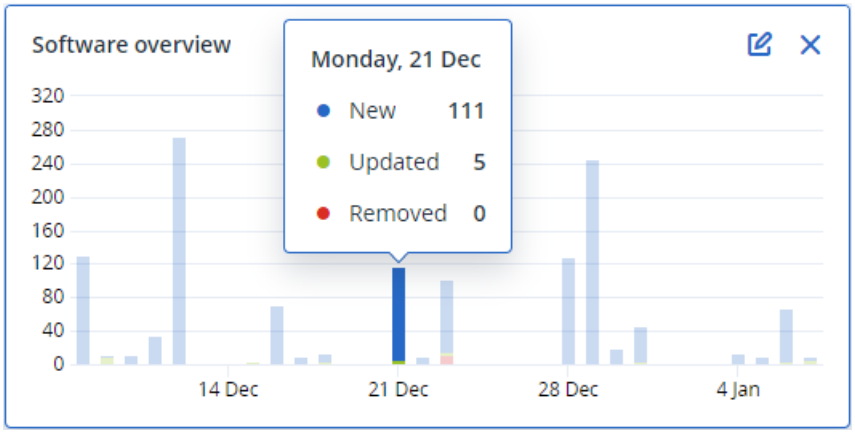


Software inventory

Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User
O0003079									
O0003079	Microsoft Policy Platform	68.1.1010.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Silverlight	5.1.50918.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	c:\Program Files\Microsof...	System
O0003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft VC++ redistribu...	12.0.0.0	Intel Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 200...	8.0.61000	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 200...	9.0.30729	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 2010	10.0.40219	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 201...	11.0.61030.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System

More Less Show 248

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。

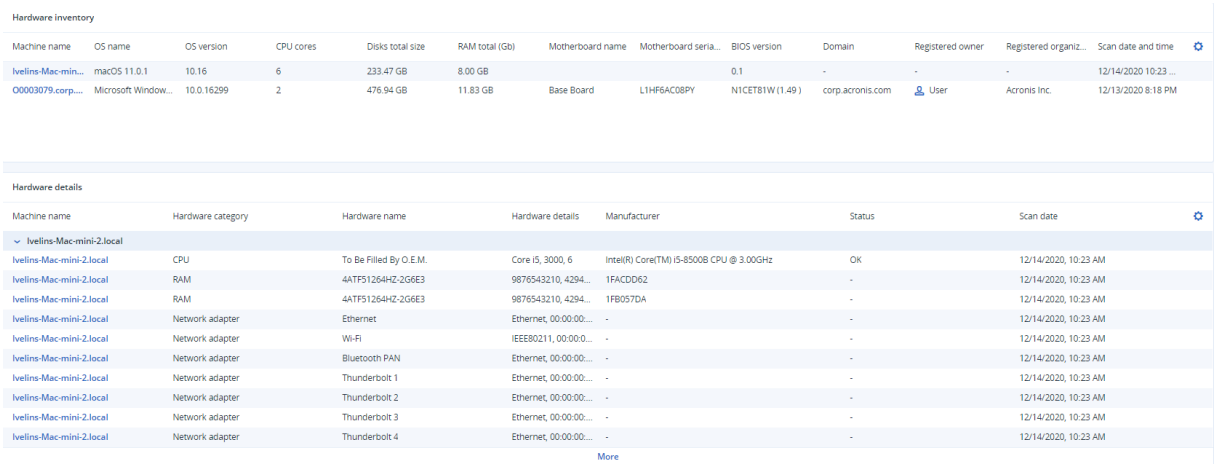
アップデート済み - アップデートされたアプリケーションの数です。

削除済み -削除されたアプリケーションの数です。

特定のステータスを示すバーの一部をクリックすると、**[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

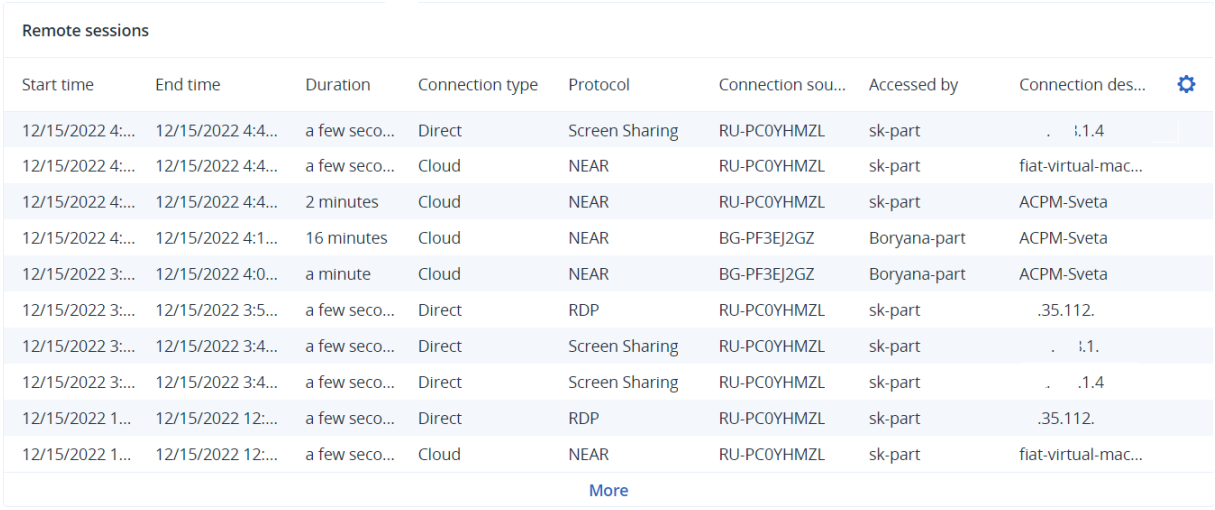
ハードウェアインベントリおよび**ハードウェアの詳細**テーブルウィジェットには、組織内の物理的および仮想的なWindows/macOSデバイスにインストールされているすべてのハードウェアに関する情報が表示されます。



ハードウェアの変更テーブルウィジェットには、指定した期間（7日、30日、または当月）に組織内の物理的および仮想的なWindows/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。

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。



監査ログ

監査ログを表示するには、**[監視]** > **[監査ログ]** に移動します。

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 Protectコンソールでユーザーが実行する、クラウドツークラウドのリソースを使った処理
- Cyber Protectコンソールで、ユーザーによって実行されるサイバースクリプト処理
- 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、現在操作している組織または部署およびその直下の部署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部署の名前です。たとえば、**ユーザーがアップデートされました**イベントのテナントは、ユーザーが配属されている部署です。**クォータに達しました**イベントのテナントは、クォータに達したユーザーです。
- **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部署の名前です。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。

レポート

サービスの使用状況や操作に関するレポートにアクセスするには、[**レポート**] をクリックします。

注意
この機能は、Cyber ProtectionサービスのStandard Editionでは利用できません。

使用状況レポート

使用状況レポートは、サービスの使用に関する履歴データを提供します。使用状況レポートは、CSV形式とHTML形式の両方で利用できます。

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。
- **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、管理している企業または部署の直下の部署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、管理している企業または部署のすべての部署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、管理している企業または部署のすべての部署、および部署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、企業または部署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. 利用可能な企業または最上位の部署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

カスタムレポートはオンデマンドで生成され、生成するタイミングを指定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部署にナビゲートします。
3. **[レポート]** > **[使用状況]**をクリックします。
4. **[カスタム]** をクリックします。
5. **[種類]** で、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、レポートのスコープを選択します。
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。

使用状況レポートのデータ

Cyber Protectionサービスの使用に関するレポートには、企業または部署に関する以下のデータも含まれます。

- 部署、ユーザー、デバイスの種類ごとのバックアップのサイズ。
- 部署、ユーザー、デバイスの種類ごとの保護されたデバイスの数。
- 部署、ユーザー、デバイスの種類ごとの価格。
- バックアップの合計サイズ
- 保護されたデバイスの合計数。
- 合計価格

注意
Cyber Protectionサービスによりデバイスの種類が検出できない場合、該当のデバイスはレポートで**未分類**として表示されます。

操作レポート

[操作] レポートは、企業レベルでの運用時には企業管理者のみが利用できます。

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。すべてのウィジェットには企業全体のサマリ情報が表示されます。
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"（75ページ）をご覧ください。

すべての履歴ウィジェットで、同じ時間範囲のデータが表示されます。この範囲はレポート設定で変更できます。

デフォルトのレポートを使用したり、カスタムレポートを作成したりできます。

レポートをダウンロードできます。またXLSX（Excel）またはPDF形式によりEメールで送信することもできます。

デフォルトのレポートの一覧は次のとおりです。

レポート名	説明
マシンごとの #CyberFit スコア	各マシンのセキュリティメトリクスと構成の評価に基づき、#CyberFit スコアと、改善するための提案が表示されます。
アラート	指定された期間に発生したアラートを表示します。
バックアップスキャンの詳細	バックアップ内に検出された脅威に関する詳細を表示します。
日次のアクティビティ	指定された期間中に実行されたアクティビティの概要を表示します。
データ保護マップ	マシン上にあるすべての重要なファイルの数、サイズ、ロケーション、保護ステータスの詳細を表示します。
検出された脅威	影響を受けたマシンの詳細情報として、ブロックされた脅威の数、および正常なマシンと脆弱なマシンの数を表示します。
検出されたマシン	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	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	組織内の物理的および仮想的なWindows/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	指定された期間に組織で実行された、リモートデスクトップとファイル転送セッションの詳細を表示します。

レポートの操作

レポートを表示するには、その名前をクリックします。

新しいレポートを追加するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. 使用可能なレポートのリスト以下で、**[レポートを追加]** をクリックします。
3. （定義済みレポートを追加するには）定義済みレポートの名前をクリックします。
4. （カスタムレポートを追加するには）**[カスタム]** をクリックしてから、レポートにウィジェットを追加します。
5. （オプション） ウィジェットをドラッグアンドドロップして並べ替えます。

レポートを編集するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストで、編集するレポートを選択します。
   以下の方法があります。
   - レポート名を変更します。
   - レポートですべてのウィジェットの時間範囲を変更します。
   - レポートの受信者と、レポートを送信するタイミングを指定します。使用可能な形式は、PDFとXLSXです。

レポートを削除するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストで、削除するレポートを選択します。
3. 省略記号アイコン（...）をクリックして、**[削除]** をクリックします。
4. **[削除]** をクリックしてこの選択内容を確認します。

レポートのスケジュールを設定するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストで、スケジュールを設定するレポートを選択してから、**[設定]** をクリックします。
3. **[スケジュール済み]** スイッチを有効にします。
   - 受信者のEメールアドレスを指定します。
   - レポートの形式を選択します。

     注意
     PDFファイルでは最大1,000件、XLSXファイルでは最大10,000件までエクスポートできます。
     PDFファイル、XLSXファイルのタイムスタンプには、ご利用のマシンのローカル時間が使用されます。

   - レポートの言語を選択します。
   - スケジュールを構成します。
4. **[保存]** をクリックします。

レポートをダウンロードするには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストでレポートを選択してから、**[ダウンロード]** をクリックします。
3. レポートの形式を選択します。

レポートを送信するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストでレポートを選択してから、**[送信する]** をクリックします。
3. 受信者のEメールアドレスを指定します。
4. レポートの形式を選択します。
5. **[送信する]** をクリックします。

レポート構造をエクスポートするには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストでレポートを選択します。
3. 省略記号アイコン（...）をクリックして、**[エクスポート]** をクリックします。

これにより、レポート構造はJSONファイルとしてマシンに保存されます。

レポートデータをダンプするには

このオプションを使用すると、カスタムされた期間のすべてのデータをフィルタリングせずにCSVファイルにエクスポートし、そのCSVファイルをEメール受信者に送信できます。

注意
CSVファイルで最大150,000項目をエクスポートできます。CSVファイルのタイムスタンプには、協定世界時（UTC）が使用されます。

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストで、データをダンプするレポートを選択します。
3. 省略記号アイコン（...）をクリックして、**[データをダンプ]** をクリックします。
4. 受信者のEメールアドレスを指定します。
5. **[時間範囲]** で、データをダンプするカスタムの期間を指定します。

   注意
   長期間を対象とするCSVファイルの準備には、時間を要する場合があります。

6. **[送信する]** をクリックします。

エクゼクティブサマリ

エグゼクティブサマリレポートでは、指定した期間における組織の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、次に示すクラウドサービスの利用状況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カスタマイズ可能な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、パッチマネジメント、ノータリー、ディザスタリカバリ、File Sync & Share。

レポートはいくつかの方法でカスタマイズできます。

- 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、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。

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 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

ウィジェット	説明
	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。

マルウェア対策保護ウィジェット

次の表に、**脅威の防御**セクションのウィジェットについての詳細を示します。

ウィジェット	説明
ファイルのマルウェア対策スキャン	ウィジェットには、指定した日付範囲にデバイスに対して実行された、オンデマンドのマルウェア対策スキャンの結果が表示されます。 **ファイル** - スキャンされたファイルの合計数 **クリーン** - クリーンなファイルの合計数 **検出済み、隔離済み** - 隔離された感染ファイルの合計数 **検出済み、未隔離** - 未隔離の感染ファイルの合計数 **保護されているデバイス** - マルウェア対策保護ポリシーが適用されているデバイスの合計数 **登録済みデバイスの合計数** - レポート生成時に登録されたデバイスの合計数
バックアップのマルウェア対策スキャン	ウィジェットには、指定した日付範囲にバックアップに対して実行された、マルウェア対策スキャンの結果が表示されます。次のメトリクスが使用されます。 • スキャンされた復元ポイントの合計数 • クリーンな復元ポイントの数 • サポートされていないパーティションにおけるクリーンな復元ポイントの数 • 感染した復元ポイントの数サポートされていないパーティションにおけるクリーンな復元ポイントの数。
ブロックされたURL	指定した日付範囲で、Webサイトのカテゴリごとにグループ化されたブロック済みURLの数がウィジェットに表示されます。 このウィジェットでは、ブロック済みURLの数が多い順に、7つのWebサイトカテゴリがリストアップされます。また残りのWebサイトカテゴリは、**その他**としてまとめて表示されます。 Webサイトのカテゴリの詳細については、Cyber ProtectionのURLフィルタリングのトピックを参照してください。
セキュリティインシデントのバーンダウン	このウィジェットでは、選択した会社のインシデントがクローズ状態になるまでの効率性が表示されます。この効率性は、オープン状態のインシデントの数と、一定期間内にクローズされたインシデントの数の比較により表わされます。 列をホバーすると、選択した日付におけるクローズ状態およびオープン状態のインシデントの内訳が表示されます。括弧内の%数値により、前期比での増減が表わされます。
インシデントMTTR	このウィジェットでは、セキュリティインシデントの平均解決時間を表示します。これは、インシデントの調査や解決のスピードを示しています。 列をクリックすると、重要度（**重大**、**高**、**中**）別のインシデントの内訳と、重要度レベル別の解決に要した時間が表示されます。括弧内の%数値により、前期比での増減が表わされます。
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

ウィジェット	説明
	ます。
保護技術で検知した脅威	指定した日付範囲に検出された脅威の数が、以下の保護技術ごとにグループ化されてウィジェットに表示されます。 • マルウェア対策スキャン • 振る舞い検知エンジン • クリプトマイニングからの保護 • エクスプロイト防御 • ランサムウェアアクティブプロテクション • リアルタイム保護 • URLフィルタ処理

バックアップウィジェット

次の表に、**バックアップ**セクションのウィジェットについての詳細を示します。

ウィジェット	説明
バックアップ済みのワークロード	ウィジェットには、登録されたワークロードの合計数がバックアップステータス別に表示されます。 **バックアップ済み** - レポートの日付範囲内でバックアップされた（少なくとも1回のバックアップが成功した）ワークロードの数。 **未バックアップ** - レポートの日付範囲内でバックアップされなかった（バックアップが成功しなかった）ワークロードの数。
物理デバイスごとのディスク状態のステータス	このウィジェットでは、物理デバイスのディスク状態のステータスに基づいて、集約されたヘルスステータスが表示されます。 **OK** - このディスク状態のステータスは、値 [70-100] に相当します。デバイス内のすべてのディスクでステータスが**OK**であれば、デバイスのステータスも**OK**となります。 **警告** - このディスク状態のステータスは、値 [30-70] に相当します。デバイス内の少なくとも1つのディスクのステータスが**警告**であり、さらにステータスが**エラー**のディスクが存在しない場合、デバイスのステータスは**警告**となります。 **エラー** - このディスク状態のステータスは、値 [0-30] に相当します。デバイス内の少なくとも1つのディスクのステータスが**エラー**である場合、デバイスのステータスは**エラー**となります。 **ディスクデータの計算中** - デバイスのディスクステータスがまだ計算されていない場合、デバイスのステータスは**ディスクデータの計算中**となります。
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。

ウィジェット	説明
	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。 **未保護** - レポート作成時点で登録されているすべてのサーバーのうち、保護されていないサーバーの合計数です。

データ漏洩防止ウィジェット

次のトピックでは、**データ漏洩防止**セクションのブロック済み周辺デバイスに関する詳細な情報を示します。

ウィジェットでは、指定した日付範囲のブロック済みデバイスの合計数（デバイスタイプ別の合計数も付記）が表示されます。

- リムーバブルストレージ
- 暗号化リムーバブル
- プリンター

- クリップボード - クリップボードとスクリーンショットキャプチャーのデバイスタイプを含みます。
- モバイル デバイス
- Bluetooth
- 光学ドライブ
- フロッピードライブ
- USB - USBポートとリダイレクトされたUSBポートのデバイスタイプを含みます。
- FireWire
- マッピングされたドライブ
- リダイレクトされたクリップボード- リダイレクトされたクリップボード受信とリダイレクトされたクリップボード送信のデバイスタイプを含みます。

このウィジェットでは、ブロック済みデバイスの数が多い順に7つのデバイスタイプが表示されます。また残りのデバイスタイプは**その他**デバイスタイプとしてまとめて表示されます。

File Sync & Shareウィジェット

次の表に、**File Sync & Share**セクションのウィジェットについての詳細を示します。

ウィジェット	説明
File Sync & Share統計情報	ウィジェットには以下のメトリクスが表示されます。 **使用済みクラウドストレージの合計** - 全ユーザーの使用済みクラウドストレージの合計です。 **エンドユーザー** - エンドユーザーの総数です。 **エンドユーザーあたりの平均ストレージ使用量** - エンドユーザーあたりの平均ストレージ使用量です。 **ゲストユーザー** - ゲストユーザーの総数です。
エンドユーザーごとのFile Sync & Shareストレージ使用状況	このウィジェットでは、ストレージ使用量が以下の範囲に相当する、File Sync & Shareのエンドユーザーの総数が表示されます。 • 0〜1GB • 1〜5GB • 5〜10GB • 10〜50GB • 50〜100GB • 100〜500GB • 500GB〜1TB • 1TB以上

Notaryウィジェット

次の表に、**Notary**セクションのウィジェットについての詳細を示します。

ウィジェット	説明
サイバーNotary統計情報	ウィジェットには以下のNotaryメトリクスが表示されます。 **使用済みNotaryクラウドストレージ** - Notaryサービスで使用済みのストレージの合計サイズです。 **公証済ファイル** - 公証済ファイルの合計数です。 **電子署名済み文書** - 電子署名済み文書と電子署名済みファイルの合計数です。
エンドユーザー全体で公証済のファイル	全エンドユーザーの公証済ファイルの合計数を表示します。ユーザーは、保有する公証済ファイルの数に応じてグループ化されます。 • 最大10件のファイル • 11～100ファイル • 101～500ファイル • 501～1000ファイル • 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。
   - すべての連絡先やユーザーにレポートを送信したい場合は、**[すべての連絡先とユーザーに送信]** を選択します。
   - 特定の連絡先とユーザーにレポートを送信したい場合
     a. **[すべての連絡先とユーザーに送信]** をクリアします。
     b. **[連絡先の選択]** をクリックします。
     c. 特定の連絡先やユーザーを選択します。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"（71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	• レポート配信のタイムゾーンはUTCです。

作 （スケジュール配信）	• レポートに表示されるアクティビティのタイムゾーンはUTCです。
管理ポータル > ユーザー > アクティブアラートに関する日次概要	• このレポートは1日1回、10:00から23:59（UTC）の間に送信されます。レポートが送信される時刻は、データセンターのワークロードによって異なります。 • レポートに表示されるアクティビティのタイムゾーンはUTCです。
管理ポータル > ユーザー > サイバープロテクションステータス通知	• このレポートはアクティビティの完了時に送信されます。 **注意** データセンターのワークロードによっては、レポートの送信が遅れることもあります。 • レポートに表示されるアクティビティのタイムゾーンはUTCです。

ウィジェットの種類に応じたレポートのデータ

ダッシュボードのウィジェットは、表示するデータの範囲に応じて2つの種類があります。

- 参照時やレポート作成時に、実際のデータを表示するウィジェット。
- 履歴データを表示するウィジェット。

レポートの設定で特定の期間のデータをダンプするように日付範囲を構成した場合、選択された時間範囲は、履歴データを表示するウィジェットにのみ適用されます。参照した時点の実際のデータを表示するウィジェットの場合、時間範囲のパラメータは適用されません。

次の表は、使用可能なウィジェットとそのデータ範囲の一覧です。

ウィジェット名	ウィジェットやレポートに表示されるデータ
マシンごとの #CyberFit スコア	実際の値
直近 5 件のアラート	実際の値
アクティブアラートの詳細	実際の値
アクティブアラート概要	実際の値
アクティビティ	履歴レポート
アクティビティ一覧	履歴レポート
アラート履歴	履歴レポート
バックアップのマルウェア対策スキャン	履歴レポート
ファイルのマルウェア対策スキャン	履歴レポート
バックアップスキャンの詳細（脅威）	履歴レポート
バックアップステータス	履歴レポート - 列内の**合計実行数**と**正常に完了した**

	実行数 実際の値 - その他のすべての列について
バックアップストレージの使用状況	履歴レポート
ブロック済みの周辺デバイス	履歴レポート
ブロックされたURL	実際の値
クラウドアプリケーション	実際の値
クラウドワークロードの保護ステータス	実際の値
Cyber protection	実際の値
サイバープロテクションのサマリ	履歴レポート
データ保護マップ	履歴レポート
デバイス	実際の値
テスト済みのディザスタリカバリサーバー	履歴レポート
ディザスタリカバリの統計情報	履歴レポート
検出されたマシン	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

機能統合

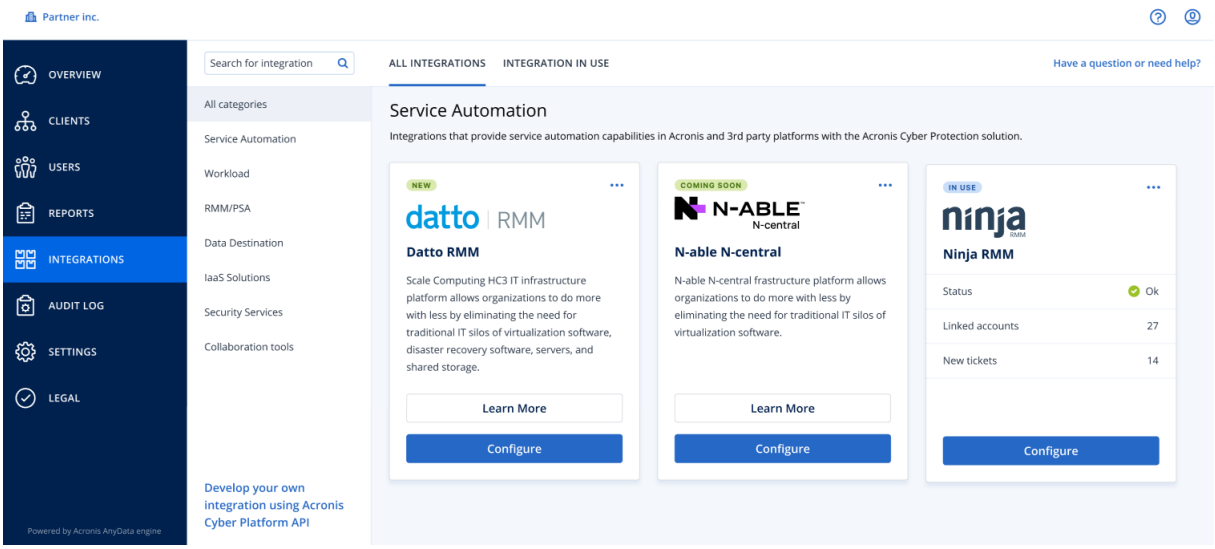
統合カタログ

このページは、すべての統合アプリケーションを登録およびアップデートするためのグローバルな機能を提供します。
ここから新しい機能統合を追加したり、既存の機能統合を変更したりできます。

注意
会社の管理者ロールを付与されたユーザーのみが統合の設定を変更できます。

すべての統合

[すべての統合] タブには、現在利用可能なすべての機能統合のリストが、タイル配列の形式で表示されます。



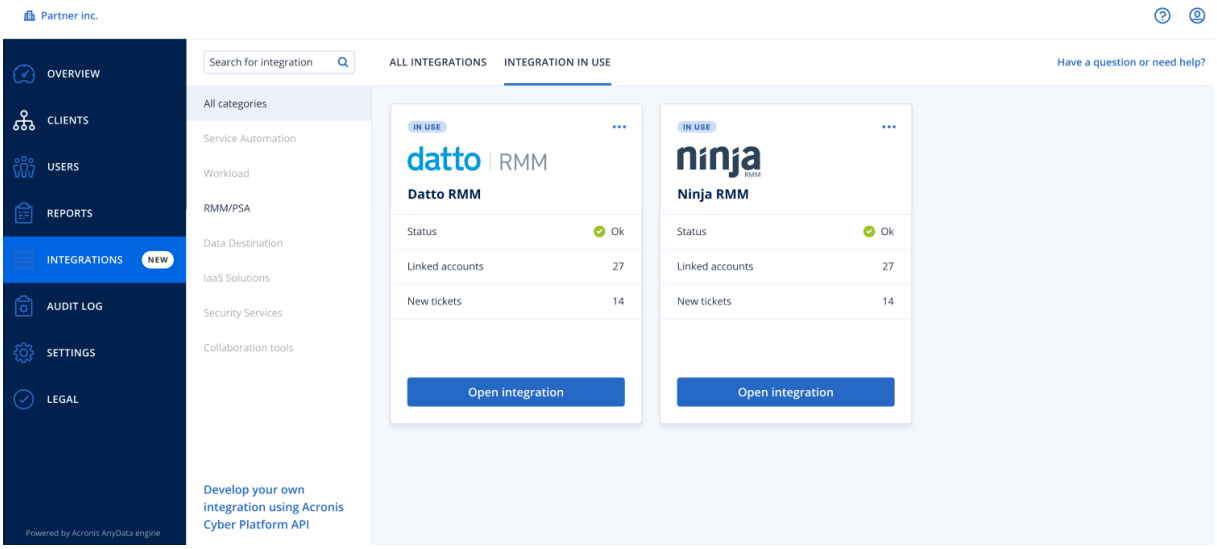
各タイルには、製品に関する短い説明と2つの追加オプションが表示されます。

- **[詳細]** - このボタンをクリックすると、特定の機能統合に関する詳細が表示されます。
  - **統合機能**
  - **文書リンク**
  - **サポート連絡先**
- **[構成]** - このオプションを使用して統合設定の一部を編集します。

非アクティブな機能統合を表すタイルはグレーアウト表示（無効）になり、「**近日リリース**」のラベルが付されることもあります。

使用中の統合

[使用中の統合] タブには、現在アクティブに使用されているすべての機能統合のリストが表示されます。また各機能統合に関する一般的な情報も示されます。



[統合を開く] をクリックすると、対応するアプリケーションに直接アクセスできます。

左側には統合カテゴリのリストがあり、すべての既存アプリケーションがサービスの自動化、ワークロード、RMM/PSAなどの特定のグループに分類されています。個別のカテゴリをクリックすると、該当のグループに属する機能統合が表示されます。現在表示しているカテゴリがハイライト表示されます。

[検索] オプションを使用してクエリーを作成し、任意の機能統合を検索します。

統合のリストは、カテゴリとラベルでフィルタリングできます。ラベルはアルファベット順に並べられます。検索結果が表示されない場合は、検索対象のカテゴリを拡大することができます。

アプリケーションを無効にするには、タイル右上の省略記号（...）アイコンをクリックし、**[非アクティブ化]** を選択します。

独自の機能統合を作成したい場合、Acronis API文書へのリンクも利用できます。

Webインターフェイスへのアクセス制限

ユーザ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って、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。部署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. アクセスを制限する部署を指定します。
3. **[設定]** > **[セキュリティ]** の順にクリックします。
4. **[ログオンコントロールを有効にする]**チェック ボックスを選択します。
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。

企業へのアクセスを制限

企業管理者は、上位層の管理者からのアクセスを制限できます。

アクセスが制限されている場合、上位層の管理者は企業のプロパティのみを変更できます。ユーザーアカウントと部署はまったく表示されません。

企業へのアクセスを制限するには

1. 管理ポータルにログインします。
2. **[設定]** > **[セキュリティ]** の順にクリックします。
3. **[サポートアクセス]** オプションを無効にします。
4. **[保存]** をクリックします。

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。

索引

わ

漢字