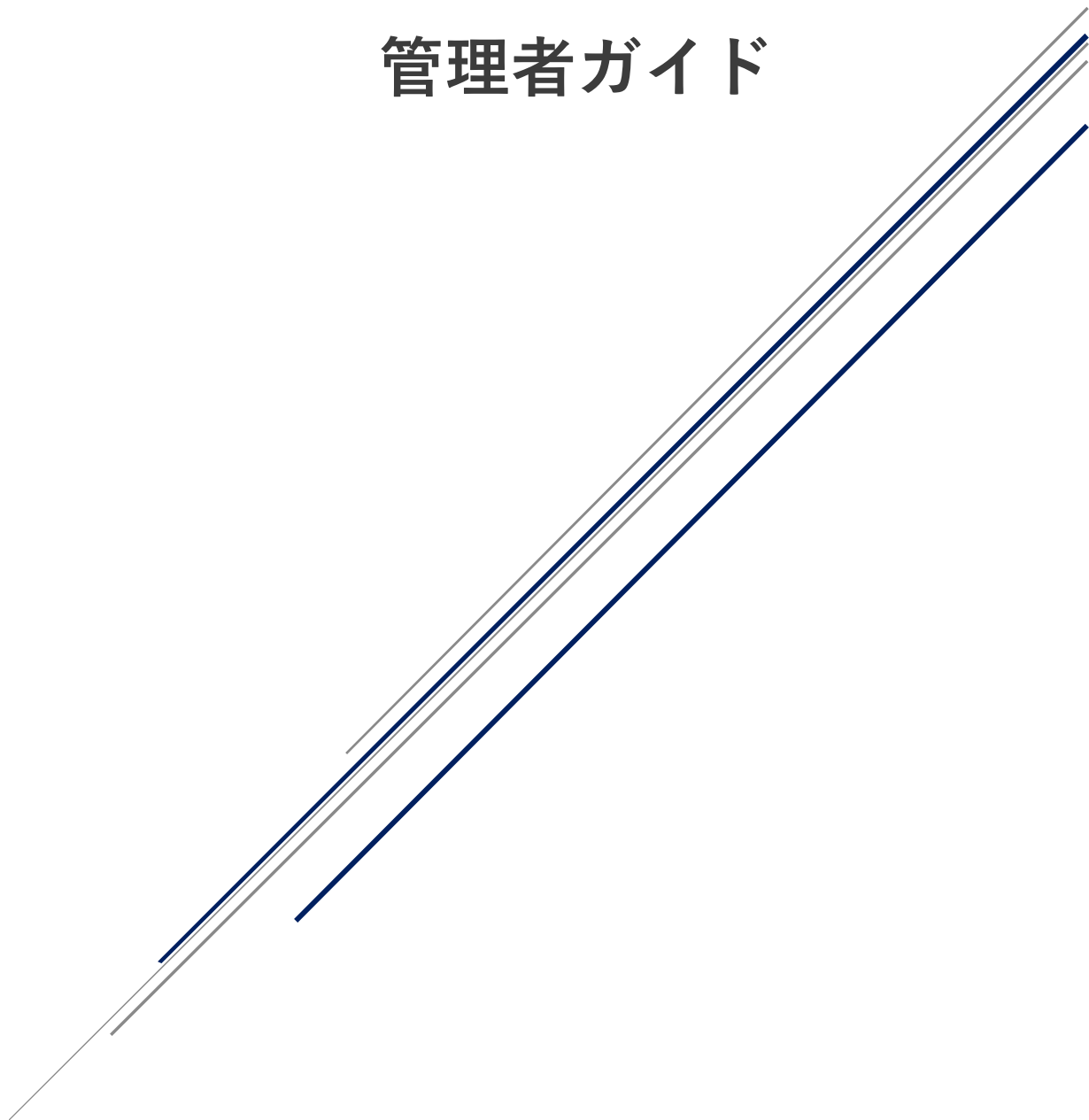


WithSecure™ Elements Security Center 管理者ガイド



W / T H®
secure

ウィズセキュア株式会社

改版履歴

履歴	リビジョン	リリース日
初版	1.0	2022/09/30
機能の追加/削除	1.1	2022/11/11
ログイン URL の変更	1.2	2022/11/20
ESC の変更に伴う全面改訂	1.3	2024/05/13

●免責事項

本書は、本書記述時点の情報を基に記述されており、特に断りのない限り、本書内の記述は、本書記載時の製品のバージョンを基にしております。例の中で使用されている会社、名前およびデータは、別途記載のない限り架空のものとなります。

ウィズセキュア株式会社（以下、弊社）は、本書の情報の正確さに万全を期していますが、本書に記載されている情報の誤り、脱落、または、本書の情報に基づいた運用の結果について、弊社は、如何なる責任も負わないものとします。本書に記載されている仕様は、予告なく変更される場合があります。

本書は 2024 年 5 月現在の情報を基に記述されております

●商標

WithSecure™及びそのロゴはウィズセキュア株式会社の登録商標です。また、弊社の製品名および記号／ロゴは、いずれも弊社の商標です。本書に記載されている全ての製品名は、該当各社の商標または登録商標です。弊社では、自社に属さない商標および商標名に関する、いかなる所有上の利益も放棄します。

●複製の禁止

本書の著作権は弊社が保有しており、弊社による許諾無く、本書の一部であっても複製することはできません。また、譲渡もできません。

●お問い合わせ

弊社は常に資料の改善に取り組んでいます。そのため、本書に関するご質問、ご意見、ご要望等ございましたら、是非 japan@withsecure.com までご連絡ください。

内容

1.	はじめに	6
2.	Elements Security Center 概要	7
2.1.	対応ブラウザ	7
2.2.	Elements EPP の構成要素	7
2.3.	Elements Security Center アカountの概念	8
2.4.	ライセンスキーの概念	9
2.5.	使用開始までの流れ	9
3.	Elements Security Center への接続とログイン	10
4.	Elements Security Center の画面	11
4.1.	Elements Security Center メニュー概要	11
5.	ホーム	12
5.1.	Elements Security Center ホーム概要	12
5.2.	新規デバイスの追加	13
6.	環境 15	15
6.1.	デバイス	15
6.1.1.	アクションメニュー	16
6.1.2.	ステータス表示のカスタマイズ	19
6.1.3.	[コンピュータ]タブ	22
6.1.4.	[モバイルデバイス]タブ	27
6.1.5.	[Connector]タブ	28
6.1.6.	[保護されていないデバイス]タブ	29
6.2.	デバイスのセキュリティ態勢	30
6.3.	パッチ管理	31
6.3.1.	適用されていないアップデート	31
6.3.2.	インストールログ	33
6.4.	ソフトウェアレピュテーション	33
7.	イベント	34
7.1.	セキュリティイベント	34
7.2.	Broad Context Detection	35
7.2.1.	Broad Context Detection	35
7.2.2.	イベント検索	37
7.3.	応答	37
8.	セキュリティ構成	38
8.1.	プロファイル	38
8.1.1.	プロファイルの作成	39
8.1.2.	プロファイル設定項目のロック	40
8.1.3.	プロファイルのエクスポート / インポート	40
8.1.4.	プロファイルの指定ルール	41
8.1.5.	プロファイルのアクションメニュー	43
8.1.6.	アウトブレイクルール	46
8.2.	自動アクション	47
9.	レポート	48
9.1.	マイレポート	48
9.2.	メールと通知	49
9.3.	Detection and Response のレポート	51
9.4.	デバイス	53

9.5.	セキュリティイベント	53
9.6.	ソフトウェアアップデート	54
10.	管理 55	
10.1.	組織の設定	55
10.1.1.	セキュリティ管理者	55
10.1.2.	Endpoint Protection のアカウント	58
10.1.3.	API クライアント	58
10.1.4.	Detection and Response の設定	58
10.2.	サブスクリプション	58
10.3.	監査ログ	59
10.4.	ダウンロード	59
11.	セキュリティサービス	60
12.	サポート	61
13.	Appendix	62

1. はじめに

本書は WithSecure™ Elements EPP for Computers（以下、「Elements EPP」）の契約ユーザー、または評価ユーザーとしてお使いくださるお客様を対象とした、WithSecure™ Elements Security Center（以下「ESC」）のガイドです。

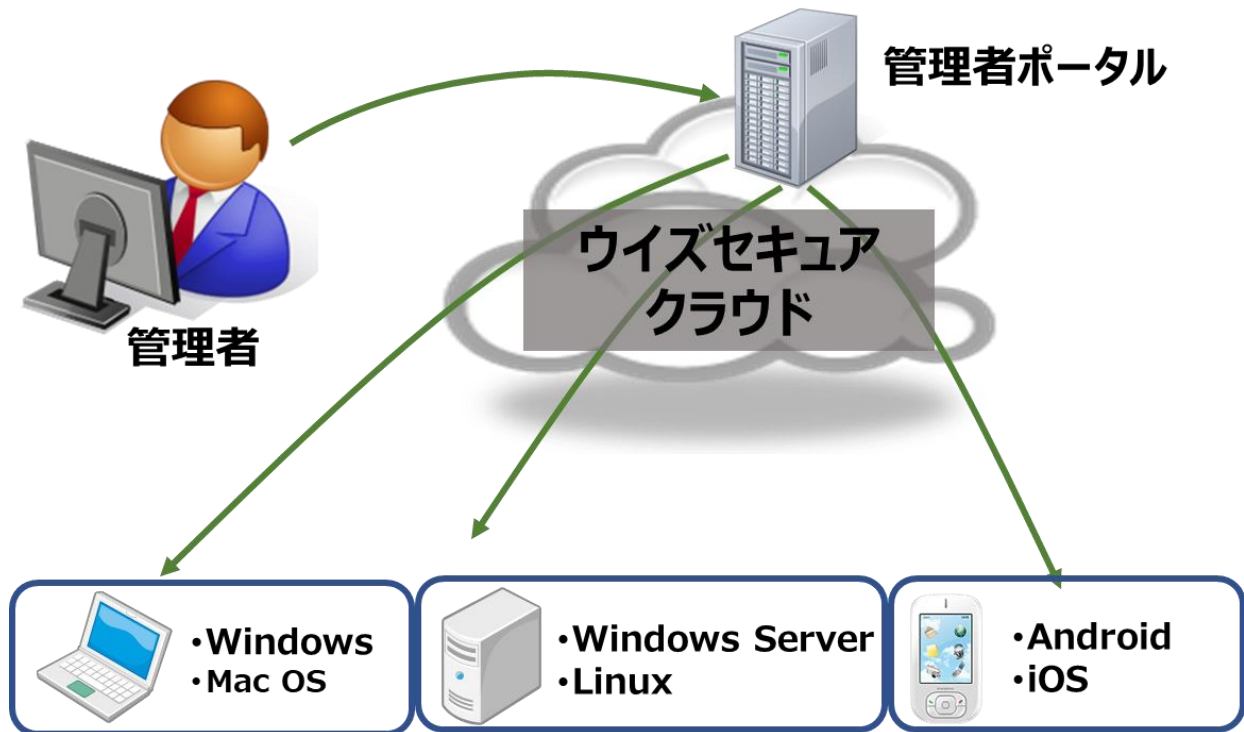
まず、「2.Elements Security Center 概要」において、ESC の概要と、独自の概念と技術について説明します。

この章の内容は、「3. Elements Security Center への接続とログイン」以降の内容をご理解いただくための準備に位置づけられています。

※本書は 2024 年 2 月現在の情報を基に記述されています。今後、予告なく内容が変更される可能性があります。

2. Elements Security Center 概要

ここでは、下図の構成概念図に従って、ESC の概要について説明します。



2.1. 対応ブラウザ

ESC は、以下のブラウザに対応しています。

- Microsoft Edge の最新のバージョン
- Google Chrome の最新のバージョン
- Mozilla Firefox の最新のバージョン
- Safari の最新のバージョン

2.2. Elements EPP の構成要素

Elements EPP は、各コンピュータにインストールされる Elements EPP クライアントと、それらを集中管理するための ESC によって構成されています。

- **Elements EPP クライアント**

Elements EPP のクライアントには3つの種類があります。

- クライアント用エージェント
クライアント OS 向けのソフトウェアです。Windows 用と Mac 用があります。
- サーバー用エージェント
サーバー OS 向けのソフトウェアです。Windows Server 用、Linux 用があります。
- モバイル用エージェント

モバイル OS 向けのソフトウェアです。Android 用と iOS 用があります。

- **Elements Security Center**

クラウド上にあるポータルサイトです。WEB ブラウザを使ってアクセスします。
ESC から Elements EPP クライアントを集中管理することができます。

※Elements EPP クライアントのインストールプログラムは、ESC からダウンロードしてください。

CD-R/DVD-R 等の媒体での提供方法はございません。

2.3. Elements Security Center アカウントの概念

ESC には以下 2 種類のアカウントがあります。

- **企業アカウント**

お客様の所属する企業(または組織)を表すアカウントです。

Elements EPP をご契約いただいたお客様は、通常 1 つの企業アカウントを保持します。

企業アカウントの中に、Elements EPP クライアントをインストールした自社のコンピュータが登録されます。

- **ユーザアカウント**

ESC へログインするためのユーザアカウントです。

企業アカウント作成時に、その企業の管理者としてユーザアカウントを作成します。

企業アカウント及び所属する Elements EPP クライアントを管理するには、ユーザアカウントを使用して ESC へログインし、各種の集中管理機能を使用します。

ユーザアカウントは、追加作成・削除が可能です。

ユーザアカウントには以下 2 つの権限があります。

- **管理者**

すべての ESC 機能を使用できます。

- **読み取り専用**

情報の読み取りだけで変更はできません。

※ユーザアカウントは、自動作成されません。お客様ご自身でユーザアカウントを作成してください。

2.4. ライセンスキーの概念

Elements EPP で扱われるライセンスキーは、英数字 20 桁からなるコードです。このライセンスキーを使用し、企業アカウントの作成、Elements EPP クライアントのインストールを行うことができます。ライセンスキーには以下の仕様と特徴があります。

- ライセンスキーは、Elements EPP クライアントのインストール時に必要です。ライセンスキーが無い場合、Elements EPP クライアントを使用することはできません。
- 1つのライセンスキーを複数の端末で利用できますが、利用可能な台数は契約により決められています。
- 企業アカウントの作成時にライセンスキーコードが必要です。
- ライセンスキーには有効期限日があります。有効期限日を過ぎるとそのライセンスキーを使用している Elements EPP クライアントは使用できなくなります。
- ライセンスキーは弊社全製品を通して一意(ユニーク)です。
- 20 桁の英数字から成り、4 桁ずつハイフンを挟んで表記されます（但し、モバイル端末用のキーは、この限りではありません）。
例：1234-ABCD-5678-EFGH-90JK

2.5. 使用開始までの流れ

Elements EPP を利用するための準備として、以下の手順が必要になります。

- ESC へアクセスする為のユーザアカウントを作成します
- ESC からインストールプログラムをダウンロードし、Elements EPP クライアントをインストールします。
- インストールが完了すると、各コンピュータが ESC へ自動登録され、集中管理ができるようになります。

3. Elements Security Center への接続とログイン

ESC サイトへの接続は、WEB ブラウザにて以下の URL を入力します。

<https://elements.withsecure.com/>

以下の画面が開きますので、ここから「ユーザー名」と「パスワード」を入力し、ログインボタンをクリックします。



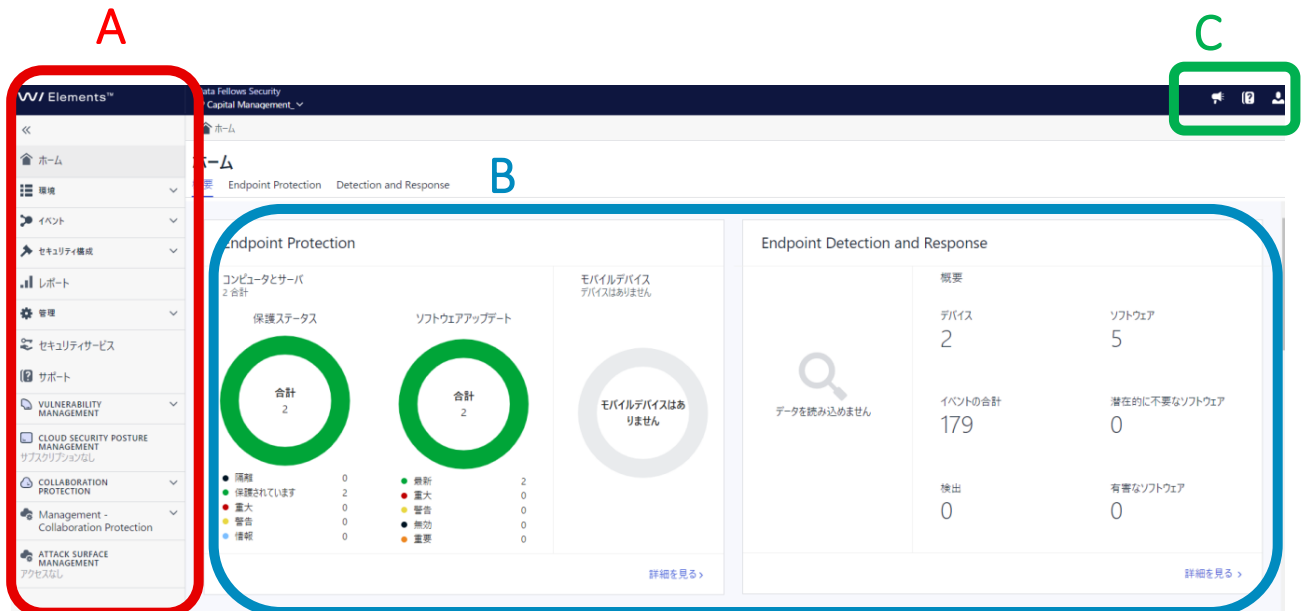
※2024年6月30日以降ユーザー名が廃止となります為、メールアドレスをご利用ください。

4. Elements Security Center の画面

ここでは、ESC にある操作用のメニューについて説明します。

4.1. Elements Security Center メニュー概要

ESC へログインをすると、以下の画面が表示されます。



A. サイドメニュー

機能ごとにメニューがまとめられています。所持している製品によりアクセスできるメニューに制限があります。

B. 表示画面

選択したサイドメニューの情報を表示します。

C. その他メニュー

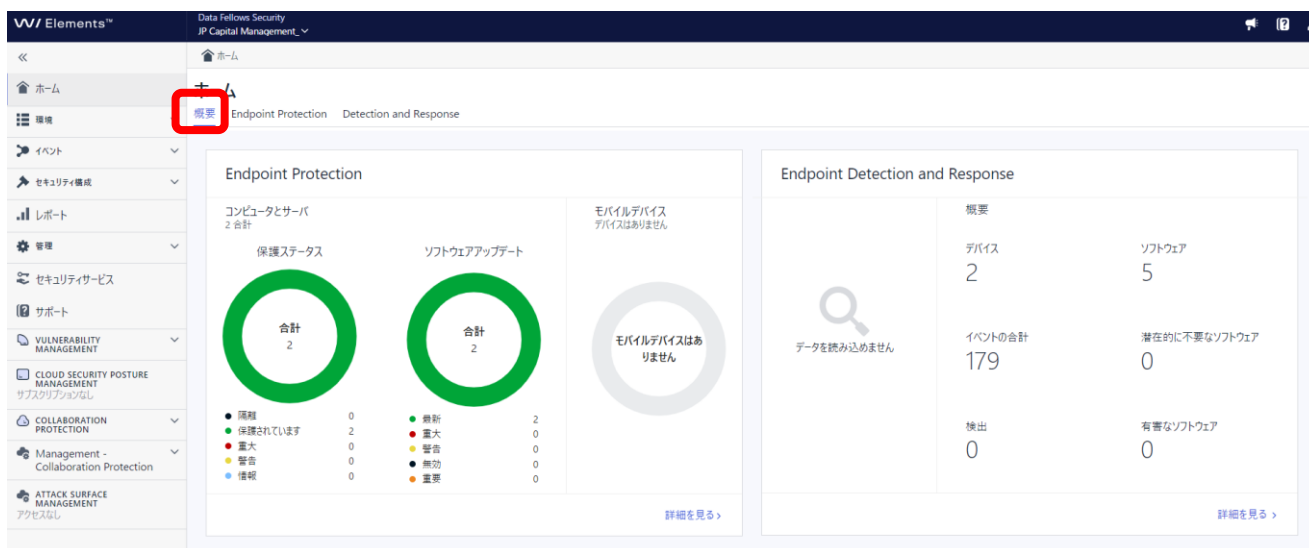
その他のメニューボタンです。

5. ホーム

ここでは、ESC のホームについて説明します。

5.1. Elements Security Center ホーム概要

ESC のホームを選択すると、以下の画面が表示されます。



- 概要
Elements 製品の全体的な状況を把握できます。

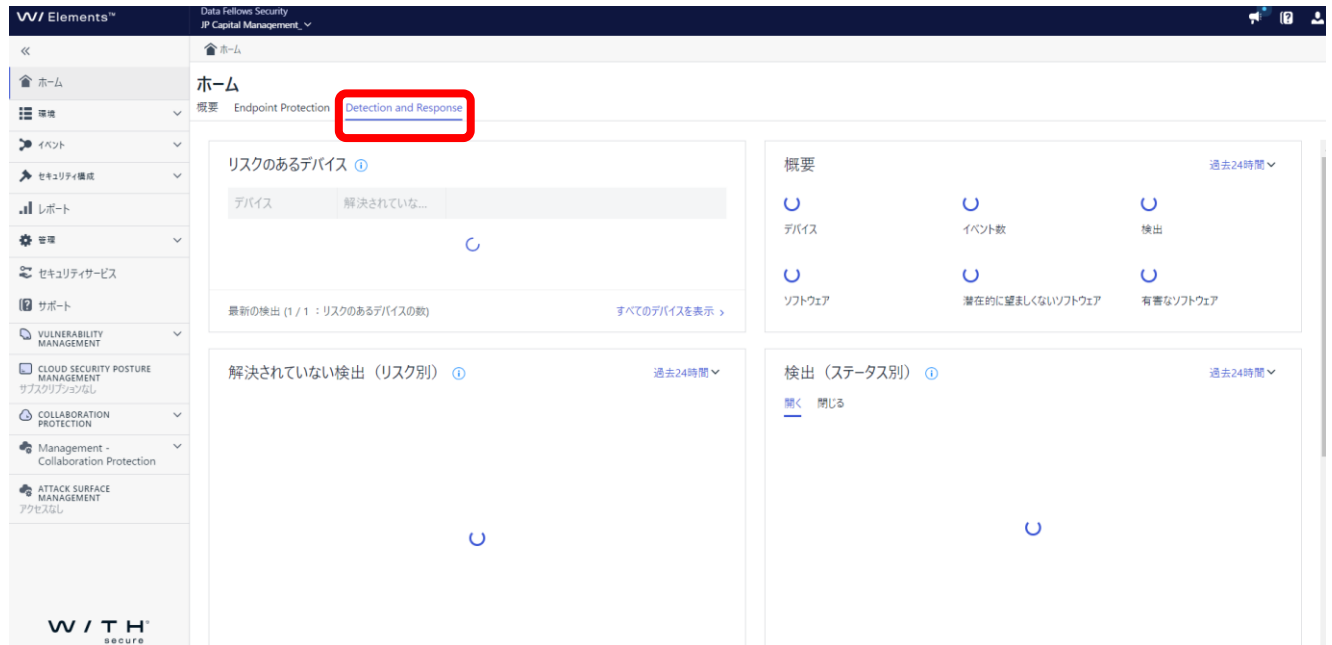


➤ Endpoint Protection

Elements Endpoint Protection に関するダッシュボードです。

端末やサーバーの状況をグラフィカルに把握することができます。

また、下部にある問題の項目では、対処が必要な可能性のある事象が記載されています。



➤ Detection and Response

Elements Endpoint Detection and Response に関するダッシュボードです。

インシデントの発生や対応の状況を概観することができます。

5.2. 新規デバイスの追加

Endpoint Protection の画面では管理するデバイスを新規に追加することができます。

この項目では、対象のデバイスを使用しているユーザーにライセンスキーとインストールモジュールをダウンロードできる URL を送信することができます。

ユーザーは受信したメールに記載されている URL から、自分自身でエージェントをインストールする必要があります。



① 追加する製品を選択します。

製品の選択

WithSecure Elements Vulnerability Management <input type="radio"/> [Redacted] 有効期限: 2024/5/18	Windows用のオンデバイス脆弱性スキャン。このサブスクリプションは、Elements EPPまたはEDRがインストールされていないデバイスにのみ使用してください。
WithSecure Elements EDR and EPP for Computers Premium <input type="radio"/> 49個のライセンスが残っています [Redacted]、継続ライセンス)	WindowsとMacコンピュータのセキュリティ保護。 WindowsとMacのヘルプセンターで対応OSが記載されています。
WithSecure Elements EDR and EPP for Servers Premium <input type="radio"/> 49個のライセンスが残っています [Redacted] 継続ライセンス)	Windowsサーバーのセキュリティ保護。 ヘルプセンターで対応OSが記載されています。
WithSecure Elements EPP for Mobiles <input type="radio"/> 50個のライセンスが残っています [Redacted] 継続ライセンス)	AndroidとiOSスマートデバイスのセキュリティ保護、管理、VPN。

[キャンセル](#) [次へ](#)

② インストールリンクを送信するメールアドレスを入力し、送信ボタンをクリックします。

新規デバイスを追加
JP Capital Management

このページから、インストールリンクを記載した招待メールを送信できます。下記の内容を入力して招待状を1つ送信するか、CSVファイルからデータを取り込んで複数の招待状を送信することができます。

言語
招待状の言語を選択してください。
日本語

デバイスの詳細を追加する
メールアドレス (必須)
[Redacted]
姓
[Redacted]
エイリアス
[Redacted]

CSVファイルからインポート
予想されるCSVファイル形式: <所有者のメールアドレス><所有者の姓><所有者の姓><エイリアス>
<owner_email>のみが必須で、その他のフィールドはオプションです。オプションのフィールドが省略された場合は、セパレータを維持する必要があります。

ファイルを選択 [Redacted]
[Redacted]

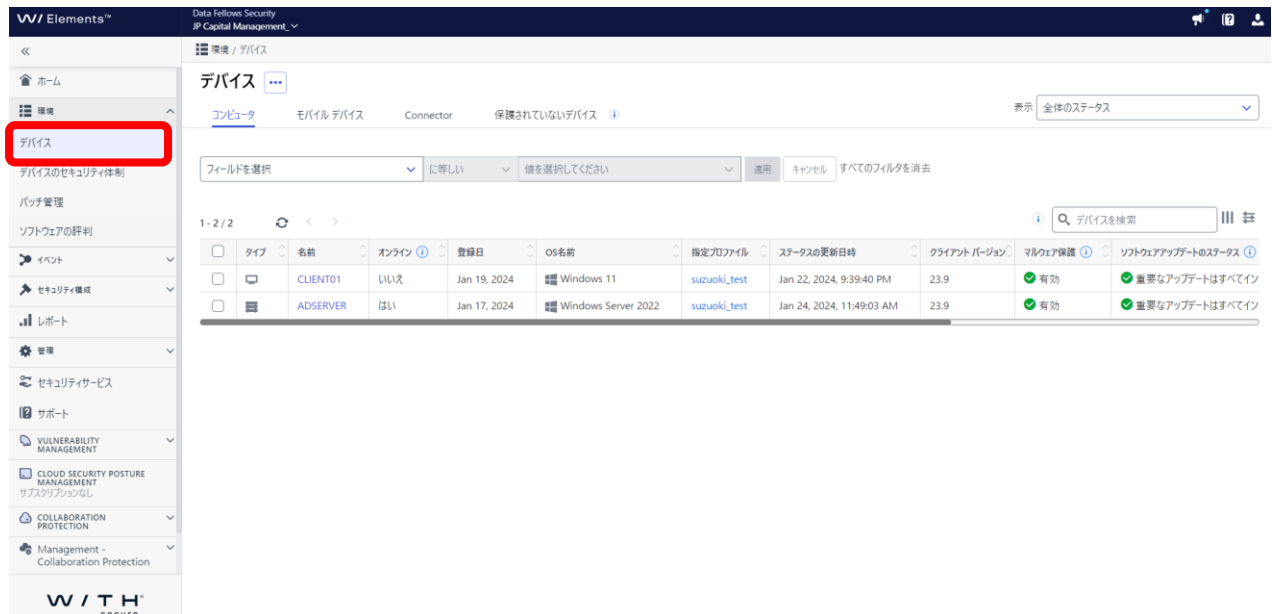
[戻る](#) [送信](#)

- 複数のメールアドレスに送る際は複数のメールアドレスをカンマ、セミコロン、新しい行で区切りことができます。これにより複数のメールアドレスへ一度に送信できます。
- 送信先を CSV ファイルからインポートすることも可能です。
- [送信]ボタンを押すことで対象のメールアドレスにメールが送信されます。

6. 環境

6.1. デバイス

[デバイス] では、登録されているデバイスのステータス情報を確認することができます。



デバイス

コンピュータ モバイルデバイス Connector 保護されていないデバイス

コンピュータ/モバイルデバイス/レガシーモバイルデバイス/Connector/保護されていないデバイスのタブを選択して、各デバイスの情報を表示します。
タブメニューではそのアカウント内の全てのコンピュータとモバイル等一覧で表示されます。

項目名	内容
コンピュータ	企業アカウント内の全てのコンピュータが一覧で表示
モバイルデバイス	企業アカウント内の全てのモバイルが一覧で表示
Connector	企業アカウント内の全ての Connector が一覧で表示
保護されていないデバイス	Active Directory を使用した際に EPP がインストールされていない端末を一覧で表示

6.1.1. アクションメニュー

デバイス数の右側にあるアクションメニューをクリックすると、デバイスの追加やエクスポートに関するメニューが表示されます。



- アクションメニュー

項目名	内容
新規デバイスを追加	[新規デバイスを追加]画面に移動します。 「5.2 新規デバイスの追加」を参照
デバイスの招待状を管理する	[デバイスの招待を管理する]画面に移動します
自動削除を管理する	[自動削除を管理する]画面に移動します。
運用の管理	[運用の管理]画面に移動します。
削除されたデバイスの管理	[削除されたデバイスの管理]画面に移動します。
デバイスをエクスポート（CSV）	コンピュータのレポートが CSV 形式でダウンロードされます。

- デバイスの招待状を管理する

新規デバイスを追加した際の招待メールのステータスを管理します。

デバイスの招待状を管理する

JP Capital Management

保留中 期限切れ

これらのデバイスには、保護アプリケーションがまだインストールされていません。インストールリンクがまだ有効である間、30日以内にリマインダーを送信できます。その後、招待状は期限切れの招待状に移動され、[新しいデバイスの追加] から再度招待する必要があります

<input type="checkbox"/>	メール アドレス	サブスクリプション名	名	姓	エイリアス	メールを送信しました	有効期限
招待状が見つかりません。							

閉じる

保留事項を削除する

リマインダーを送信

➤ 送信したメールの無効化、再送を実施することができます。

● 自動削除を管理する

オフラインのデバイスを自動的にポータルから削除する機能です。デバイスが削除されるまでのオフラインの期間を定義することができます。

自動削除を管理する

設定した日数（最低7日間）オフラインになったデバイス（携帯電話、コネクタを除く）を自動的に削除する ⓘ

☐ 選択した期間でオフラインになったデバイスを自動的に削除する

7 日

- 設定可能な期間は7日から365日です。
- 削除されたデバイスがオンラインになった場合、ライセンス数に空きがあれば、再びポータルに登録されます。空きが無い場合は、ライセンスは無効のままとなり、端末は保護されません。

● 運用の管理

端末への操作の履歴を確認できます。

運用の管理

JP Capital Management_

9回の操作 🔁

🔍 操作検索

コンピュータ	操作	開始	ステータス	ステータスの更新日時	詳細	処理
CLIENT01	脆弱性スキャン	5日前 2024/01/19, 15:49:21	成功。操作が実行されました	5日前 2024/01/19, 15:49:34	OK	
CLIENT01	プロファイルを指定する	5日前 2024/01/19, 15:43:35	成功。操作が実行されました	5日前 2024/01/19, 15:43:35	理由: インストーラにパラメータとして渡されるプロファイルID プロファイル: suzuoki_test	
ADSERVER	ネットワークの隔離から解放する	5日前 2024/01/19, 15:07:22	成功。操作が実行されました	5日前 2024/01/19, 15:08:16	OK	
ADSERVER	ネットワークから隔離する	5日前 2024/01/19, 15:06:05	成功。操作が実行されました	5日前 2024/01/19, 15:06:10	OK	
ADSERVER	プロファイルを指定する	5日前 2024/01/19, 14:41:35	成功。操作が実行されました	5日前 2024/01/19, 14:41:35	理由: ポータルで手動で割り当てられたプロファイル プロファイル: suzuoki_test	
ADSERVER	プロファイルを指定する	5日前 2024/01/19, 14:40:44	成功。操作が実行されました	5日前 2024/01/19, 14:40:44	理由: ポータルで手動で割り当てられたプロファイル プロファイル: suzuoki_test	
4960b9c3-3c82-4812-b4bb-864c83f20345	プロファイルを指定する	5日前 2024/01/19, 14:37:18	成功。操作が実行されました	5日前 2024/01/19, 14:37:18	理由: 新しくインストールされたデバイスに割り当てられたプロファイル プロファイル: Capital_Connector_Test	

● 削除されたデバイスの管理

削除されたデバイスを再度有効にすることができます。

削除されたデバイスの管理									処理
名前	デバイスの状態	削除日	ライセンス キーコード	OS 名前	IP アドレス	DNS アドレス	シリアル番号	UPN	
AD-SERVER	削除済み	9日前 2024/01/17, 15:39:37	[REDACTED]	Windows Server 2022	172.25.241.131/20	AD-Server.Elements-AD.test	[REDACTED]	デバイス有効にする	...
WINCLIENT002	削除済み	9日前 2024/01/17, 15:39:35		Windows 10	192.168.56.105/24 10.0.3.15/24 192.168.56.1/24	WinClient002			...
ELEMENTSWINCLIE	削除済み	2年前 2022/01/18, 16:28:08		Windows 10	192.168.56.102/24 10.0.3.15/24 fe80::515b:5469:4504:27a6/64 fe80::29d9:217c:fab5:2d56/64	ElementsWinClients			...
CP001	削除済み	2年前 2021/08/02, 17:49:25			10.0.2.6/24	CP001			...
CP001	削除済み	2年前 2021/08/02, 17:49:25			10.0.2.6/24	CP001			...

● デバイスをエクスポート (CSV)

登録されているデバイス一覧を CSV でエクスポートすることができます。

6.1.2. ステータス表示のカスタマイズ

デバイスのステータス表示をカスタマイズすることができます。

● ビルトインのステータスセット

ビルトインのステータスセットを変更することで、表示するステータスを変更することができます。コンピュータ・モバイルデバイス・Connector の各タブで表示される内容は異なります。

デバイス

コンピュータ

モバイル デバイス

Connector

保護されていないデバイス

フィールドを選択

に等しい

値を選択してください

適用

キャンセル

すべてのフィルタを消す

1 - 2 / 2

リフレッシュ

前

次

<input type="checkbox"/>	タイプ	名前	オンライン	登録日	OS 名前	指定プロファイル	ステータスの更新日時	クラス
<input type="checkbox"/>	クライアント	CLIENT01	いいえ	Jan 19, 2024	Windows 11	suzuki_test	Jan 22, 2024, 9:39:40 PM	23.9
<input type="checkbox"/>	サーバー	ADSERVER	はい	Jan 17, 2024	Windows Server 2022	suzuki_test	Jan 26, 2024, 4:00:41 PM	23.9

表示

全体のステータス

マイビュー

ビューを保存してここで表示

システムビュー

☒ 全体のステータス デフォルト
 ☐ 構成の詳細
 ☐ コンプライアンス
 ☐ ハードウェア情報
 ☐ 再起動が必要
 ☐ スペース不足
 ☐ すべてのフィールド
 ☐ EDRステータス

デフォルトとして設定する

名前を付けて保存...

• カスタマイズビューの設定

ビューをカスタマイズして保存することができます。

① 列の選択のボタンをクリックします。

デバイス ...

コンピュータ モバイル デバイス Connector 保護されていないデバイス ⓘ										
表示 test view										
フィールドを選択 に等しい 値を選択してください 適用 キャンセル すべてのフィルタを消去										
1 - 2 / 2 🔍 デバイスを検索 ☰										
<input type="checkbox"/>	タイプ	名前	オンライン ⓘ	登録日	OS名前	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護 ⓘ	ソフ
<input type="checkbox"/>	🖥️	CLIENT01	いいえ	Jan 19, 2024	Windows 11	suzuoki_test	Jan 22, 2024, 9:39:40 PM	23.9	有効	✓
<input type="checkbox"/>	🖥️	ADSERVER	はい	Jan 17, 2024	Windows Server 2022	suzuoki_test	Jan 26, 2024, 4:00:41 PM	23.9	有効	✓

② 表示したい列を選択します。

デバイス ...

コンピュータ モバイル デバイス Connector 保護されていないデバイス ⓘ										
フィールドを選択 に等しい 値を選択してください 適用 キャンセル すべてのフィルタを消去										
1 - 2 / 2 🔍 デバイスを検索 ☰										
<input type="checkbox"/>	タイプ	名前	オンライン ⓘ	登録日	OS名前	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護 ⓘ	ソフ
<input type="checkbox"/>	🖥️	CLIENT01	いいえ	Jan 19, 2024	Windows 11	suzuoki_test	Jan 22, 2024, 9:39:40 PM	23.9	有効	✓
<input type="checkbox"/>	🖥️	ADSERVER	はい	Jan 17, 2024	Windows Server 2022	suzuoki_test	Jan 26, 2024, 4:00:41 PM	23.9	有効	✓

列の選択

- ☒ 指定プロファイル
- ☒ ステータスの更新日時
- ☒ クライアントバージョン
- ☒ マルウェア保護
- ☒ ソフトウェアアップデートのステータス
- ☒ ラベル
- ☒ IP アドレス
- ☒ コメント
- ☐ デバイスの重要度
- ☐ 保護ステータスの概要
- ☐ 全体保護
- ☐ プロファイルの指定ステータス
- ☐ OSバージョン
- ☐ ファイアウォール
- ☐ デバイス制御
- ☐ アプリケーション制御 (Premium)
- ☐ データガード (Premium)
- ☐ ネットワークの隔離

- [列の選択]でドラッグアンドドロップすることでステータstableでの表示位置を変更することができます。

③ [名前を付けて保存]をクリックします。



④ ビュー名を入力し[保存]をクリックします。



⑤ [マイビュー]に作成したビューが保存されます。



6.1.3. [コンピュータ]タブ

Windows、Mac、Linux に関する情報を一覧で見ることができます。また、デバイスを選択することで対象端末へのアクションを実施することができます。

デバイス ...

コンピュータ モバイル デバイス Connector 保護されていないデバイス ⓘ

表示 全体のステータス

フィールドを選択 値を選択してください 適用 キャンセル すべてのフィルタを消去

1 - 2 / 2

	タイプ	名前	オンライン ⓘ	登録日	OS名前	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護 ⓘ	ソフトウェアアップデイト
<input type="checkbox"/>	サーバー	ADSERVER	はい	Jan 17, 2024	Windows Server 2022	suzuoki_test	Feb 14, 2024, 9:12:55 AM	24.1	有効	重要なアップデイト
<input checked="" type="checkbox"/>	クライアント	CLIENT01	はい	Jan 29, 2024	Windows 11	suzuoki_test	Feb 14, 2024, 3:07:08 PM	24.1	有効	重要なアップデイト

アクション

1台のデバイスを選択しました

ステータス アップデートを送る 延期された操作をキャンセルする ソフトウェア アップデートをインストール スキャン プロファイルを指定する ラベルを管理する ライセンスを変更する

デバイスを削除する ネットワークの隔離 再起動 診断操作 デバイスにメッセージを送信する セキュリティ機能をオフにする

セキュリティ機能を復元する アンインストール

- アクション

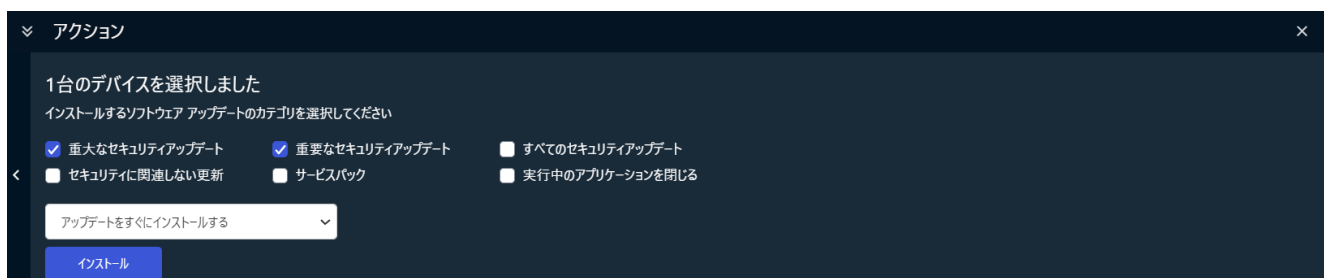
項目名	内容
ステータスアップデートを送る	ESC に登録されているデバイス情報を最新の状態にアップデートします。
延期された操作をキャンセルする	[アクション]で指定した操作をキャンセルします。
ソフトウェアアップデートをインストール	[パッチ管理]に表示されているパッチをインストールします。
スキャン	ウイルススキャンやパッチ管理対象のソフトウェアのスキャンをします。
プロファイルを指定する	適用するプロファイルの変更をします。
ラベルを管理する	ラベルの追加、交換、削除をします。
ライセンスを変更する	デバイスに適用するライセンスキーコードを変更します。
デバイスを削除する	ESC から登録されているデバイスを削除します。
ネットワークの隔離	ネットワークからデバイスの隔離、解放をします。
再起動	デバイスの再起動、もしくは WithSecure Agent の再起動をします。
診断操作	診断ファイルのリモート取得、もしくは、デバッグログの有効化をします。
デバイスにメッセージを送信する	デバイスにメッセージを送信し、ポップアップ表示させます。
セキュリティ機能をオフにする	Elements EPP の各機能を無効化にします。
セキュリティ機能を復元する	無効化した Elements EPP の各機能を有効化します。

アンインストール	デバイスにインストールした Elements Agent をアンインストールします。
----------	--

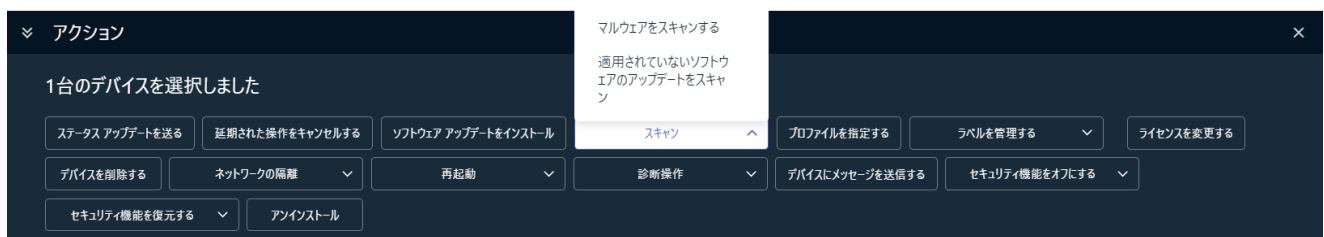
- ステータスアップデートを送る
デバイスの情報を ESC に送信し、ステータスを最新にします。

- 延期された操作をキャンセルする
[デバイスにメッセージを送信する]、[ソフトウェア アップデートをインストール]のアクションをキャンセルすることができます。

- ソフトウェアアップデートをインストール
ソフトウェアアップデートのインストールを指示することができます。このパッチを指定するのではなく、重大度などのカテゴリを指定します。また、インストールのスケジュールを指定することもできます。



- スキャン
マルウェアのスキャンもしくは未適用のソフトウェアアップデートのスキャンを指示することができます。



- プロファイルを指定する
プロファイルを変更することができます。



- ラベルを管理する
ラベルの追加、交換、削除をできます。



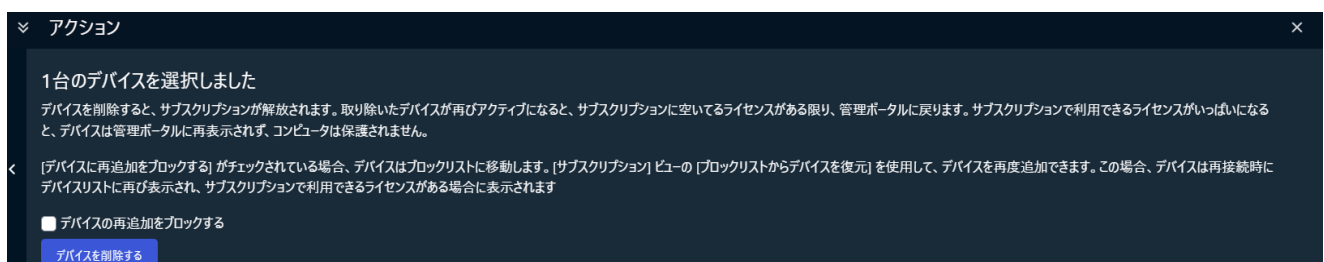
- ライセンスを変更する

Windows、Mac デバイスで使用するライセンスを変更することができます。



- デバイスを削除する

ESC から登録されているデバイスを削除します。通常は、デバイスが再度 ESC に接続された場合、そのデバイスは再登録されます。[デバイスの再追加をブロックする]オプションを指定すると、デバイスは再登録されません。



- ネットワークの隔離

デバイスをネットワークから隔離と、隔離されたデバイスの開放をすることができます。



- 再起動

OS の再起動、もしくは Elements Agent のみの再起動をすることができます。



- 診断操作

不具合解析に必要な診断情報を取得することができます。取得した診断情報は、ESC へ自動的にアップロードされます。また、デバッグログを有効にすることで、通常の診断情報以上の情報を得ることができます。



- デバイスにメッセージを送信する

デバイスにメッセージを送信できます。メッセージの送信は、即時とスケジュールのどちらも可能です。



➤ 送信されたメッセージは、下図のようにポップアップ表示されます。



- セキュリティ機能をオフにする

Elements EPP で提供しているセキュリティ機能をオフにすることができます。



- セキュリティ機能を復元する

オフにしたセキュリティ機能を再度有効化することができます。



- アンインストール

デバイスから Elements EPP をアンインストールし、ESC からデバイスを削除します。対象デバイスに関する ESC 上のデータも全て削除されます。

6.1.4. [モバイルデバイス]タブ

モバイルデバイスに関する情報を一覧で見ることができます。また、デバイスを選択することで対象端末へのアクションを実施することができます。



- アクション

項目名	内容
ステータスアップデートを送る	ESC に登録されているデバイス情報を最新の状態にアップデートします。
スキャン	ウイルススキャンやパッチ管理対象のソフトウェアのスキャンをします。
ラベルを管理する	ラベルの追加、交換、削除をします。
デバイスを削除する	ESC から登録されているデバイスを削除します。
診断操作	診断ファイルのリモート取得、もしくは、デバッグログの有効化をします。
デバイスにメッセージを送信する	デバイスにメッセージを送信し、ポップアップ表示させます。

6.1.5. [Connector]タブ

Elements Connector に関する情報を一覧で見ることができます。また、デバイスを選択することで対象端末へのアクションを実施することができます。

デバイス

コンピュータ

モバイル デバイス

Connector

保護されていないデバイス

表示

すべてのコネクター

フィールドを選択

に等しい

値を選択してください

適用

キャンセル

すべてのフィルタを消去

1 - 1 / 1

🔍 デバイスを検索

≡

🗑

<input type="checkbox"/>	タイプ	名前	企業名	登録日	ステータスの更新日時	ラベル	コメント	OS名前	OSバージョン	指定プロファイル	プロファ
<input checked="" type="checkbox"/>	🖨	ADSERVER	JP Capital Management_	Jan 19, 2024	Mar 6, 2024, 1:30:00 PM			Windows Server 2022	21H2	suzuoki_test	最新

✖ アクション

✕

1台のデバイスを選択しました

プロファイルを指定する

ラベルを管理する

デバイスを削除する

- アクション

項目名	内容
プロファイルを指定する	適用するプロファイルの変更をします。
ラベルを管理する	ラベルの追加、交換、削除をします。
デバイスを削除する	ESC から登録されているデバイスを削除します。

6.1.6. [保護されていないデバイス]タブ

Active Directory 内の保護されていないデバイスを検索します。この機能を利用するためにはドメインコントローラが ESC に登録されている必要があります。

デバイス

コンピュータ モバイル デバイス Connector **保護されていないデバイス** ⓘ

前回のスキャン: 2024/01/26, 16:54:08

Active Directory組織単位のステータス (1ノード) **スキャンを開始** ☐ Scan daily

ノード	ステータス	スキャン操作に使用されるデバイス ⓘ
com.example.TestAD	✓ スキャン完了	ADSERVER

フィールドを選択 に等しい 値を選択してください 適用 キャンセル すべてのフィルタを消去

DNS名	作成済み	前回のログイン	Active Directory のコ	OS	Active Directory組織単位	AD GUID	コメント	ステータス
Client01.TestAD.example.com	Jan 17, 2024, 2:39:48 PM	Jan 17, 2024, 2:39:48 PM		Windows 11 Pro v. 10.0 (22H2)	com/example/TestAD/Computers/CLIENT01	725cd73a-014b-48a0-b4f0-e4bde1cfd216		信頼されていない

- [スキャン開始]をクリックすると、AD の端末情報と ESC の端末情報を比較し、登録されていない端末を表示します。

6.2. デバイスのセキュリティ態勢

セキュリティ態勢（Security Posture）は、利用しているデバイスとプロファイル进行分析し、デバイスの侵害や機密データの漏えいにつながる問題を表示します。

ホーム

環境

デバイス

デバイスのセキュリティ体制

パッチ管理

ソフトウェアの評判

イベント

セキュリティ構成

レポート

管理

セキュリティサービス

サポート

VULNERABILITY MANAGEMENT

CLOUD SECURITY POSTURE MANAGEMENT
サブスクリプションなし

COLLABORATION PROTECTION

Management

セキュリティ態勢は、限られた数の評価のみをサポートする機能です。ぜひ、ご意見をお聞かせください。

デバイスのセキュリティ態勢（パイロット）

セキュリティに関する推奨事項
● 準拠：8 ● 非準拠：5

フィールドを選択 に等しい 値を選択してください 適用 キャンセル すべてのフィルタを消去

セキュリティに関する推奨事項	ステータス	デバイス	プロファイル	対応
ユーザーは、プロファイルでパスワードなしでクライアントをアンインストールできます	●	1	5	Windows Apple Linux
システムドライブの暗号化が無効になっています	●	1	0	Windows Apple Linux
RDPが有効で、アカウントロックアウトの閾値が設定されていません	●	1	0	Windows Apple Linux
ワークステーションの10%以上で、最終ログインしたユーザーは管理者です。	●	1	0	Windows Apple Linux
RDPが有効で、アカウントロックアウトの閾値が設定されていません	●	1	0	Windows Apple Linux
ローカルドライブはネットワークに共有されています	●	0	0	Windows Apple Linux
共有フォルダの匿名列挙は有効です	●	0	0	Windows Apple Linux
プロファイルでディープガードが有効になっていません	●	0	0	Windows Apple Linux
プロファイルで改ざん防止機能が有効になっていません	●	0	0	Windows Apple Linux

- 各項目をクリックすると、詳しい説明や手順が表示されます。
- 表示される項目は随時変更されます。

セキュリティ態勢は、限られた数の評価のみをサポートする機能です。ぜひ、ご意見をお聞かせください。

デバイスのセキュリティ態勢（パイロット）

セキュリティに関する推奨事項
● 準拠：8 ● 非準拠：5

フィールドを選択 に等しい 値を選択してください

セキュリティに関する推奨事項

ユーザーは、プロファイルでパスワードなしでクライアントをアンインストールできます

システムドライブの暗号化が無効になっています

RDPが有効で、アカウントロックアウトの閾値が設定されていません

ワークステーションの10%以上で、最終ログインしたユーザーは管理者です。

RDPが有効で、アカウントロックアウトの閾値が設定されていません

ローカルドライブはネットワークに共有されています

共有フォルダの匿名列挙は有効です

プロファイルでディープガードが有効になっていません

プロファイルで改ざん防止機能が有効になっていません

RDPが有効で、アカウントロックアウトの閾値が設定されていません

説明

RDPが有効で、アカウントロックアウトのしきい値が設定されていないデバイスがある場合、攻撃者はRDP接続を介してパスワードをブルートフォース攻撃で入力することができるようになります。
これらのデバイスでRDPを有効にする必要があるかどうかを検討してください。
詳細については、次の説明を参照してください。

RDPが有効で、アカウントロックアウトの閾値が設定されていません

潜在的リスク

RDPが有効で、アカウント閾値のポリシーが設定されていないデバイスは、リモート接続デスクトップ経由でブルートフォース攻撃を受ける可能性があります。

閉じる

6.3. パッチ管理

適用されていない OS やアプリケーションのパッチを管理することができます。

6.3.1. 適用されていないアップデート

適用されていないパッチの一覧です。

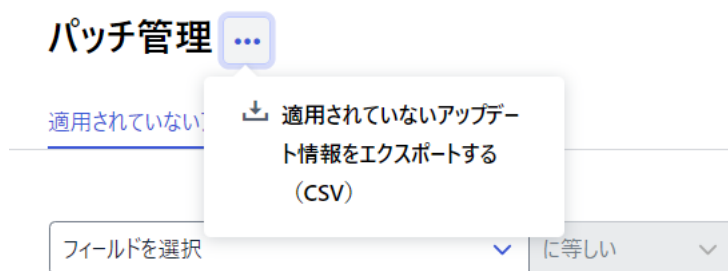


The screenshot shows the 'Patch Management' (パッチ管理) page. The left sidebar contains navigation links: ホーム, 環境, デバイス, デバイスのセキュリティ体制, パッチ管理 (selected), ソフトウェアの評判, イベント, セキュリティ構成, レポート, 管理, セキュリティサービス, サポート, VULNERABILITY MANAGEMENT, and CLOUD SECURITY POSTURE MANAGEMENT. The main area is titled 'パッチ管理' with a sub-header '適用されていないアップデート' (Updates not applied). Below this is a filter bar with a dropdown for 'フィールドを選択' (Select field), a dropdown for 'に等しい' (Equal to), and a text input for '値を選択してください' (Please select a value). There are buttons for '適用' (Apply) and 'キャンセル' (Cancel), and a link to 'すべてのフィルタを消去' (Clear all filters). The table below shows a list of updates. The first row is for Google Inc. Google Chrome, with current version 120.0.6099.225 and target version 121.0.6167.86. It is categorized as '重要なセキュリティ' (Important security) with a CVE ID of CVE-2024-0807. The table has columns for 'ベンダー' (Vendor), 'ソフトウェア' (Software), '現在のバージョン' (Current version), 'ターゲットバージョン' (Target version), 'カテゴリ' (Category), 'CVE ID', 'セキュリティ情報番号' (Security information number), 'ワークステーション' (Workstation), and 'サーバ' (Server).

ベンダー	ソフトウェア	現在のバージョン	ターゲットバージョン	カテゴリ	CVE ID	セキュリティ情報番号	ワークステーション	サーバ
Google Inc.	Google Chrome	120.0.6099.225	121.0.6167.86	重要なセキュリティ	CVE-2024-0807	FSPM-41-39233-4/x64	0	1

- アクションメニュー

未適用パッチ一覧を CSV で出力できます。



● アップデートのインストール

この画面からアップデートをインストールすることができます。

The screenshot shows the 'Patch Management' (パッチ管理) interface. On the left is a sidebar with navigation options like 'ホーム', '環境', 'デバイス', and 'パッチ管理'. The main area displays a table of updates. One update from 'Google Inc.' for 'Google Chrome' is selected, indicated by a red circle and the number ③. Below the table, a modal titled '1件のアップデートを選択しました' (1 update selected) is open. It allows selecting the installation timing (e.g., 'アップデートをインストールする時間を指定してください (Windowsのみ)') and the target devices (e.g., 'ワークステーション' or 'サーバ'). Red circles and numbers ①, ②, and ③ highlight these selection areas.

ベンダー	ソフトウェア	実行バージョン	ターゲットバージョン	カテゴリ	CVE ID	セキュリティ情報番号	ワークステーション	サーバ	
<input checked="" type="checkbox"/>	Google Inc.	Google Chrome	120.0.6099.225	121.0.6167.86	重要なセキュリティ	8.1 CVE-2024-0807	FSPM-41-39233-4/x64	0	1

- ① 適用したいアップデートにチェックを入れます。
- ② インストールするタイミングを選択します。
 - Windows の場合のみ日時を選択してインストール可能です。
- ③ インストールする端末を選択します。
 - ワークステーション、サーバーごとの一括インストールが可能です。
 - インストールする端末を個別に選択することも可能です。その場合、[アップデートするデバイスの選択]をクリック後、下の画面から対象デバイスを選択します。

This screenshot shows the 'Device Selection' (デバイスの選択) modal. It contains a table of devices. The first device, 'ADSERVER', is highlighted with a red circle. The modal also includes buttons for 'キャンセル' (Cancel) and '更新' (Update).

コンピュータ名	デバイスタイプ	企業	OS	プロファイル	ラベル
<input checked="" type="checkbox"/> ADSERVER	server	JP Capital Management	Windows Server 2022 21H2	suzuoki_test	

6.3.2. インストールログ

インストール操作やその進行状況を確認することができます。

パッチ管理 ...

適用されていないアップデート [インストールログ](#)

フィールドを選択

に等しい

値を選択してください

適用

キャンセル

すべてのフィルタを消去

1 - 2 / 2

🔍

インストールログを...

インストール時間	コンピュータ名	インストールのステータス	インストールコード	ベンダー	ソフトウェア	インストールされたバージョン	以前にインストールされたバージョン	カテゴリ
Jan 30, 2024 11:11:41 AM	CLIENT01	✔ インストールが完了しました	OK (0)	Google Inc.	Google Chrome	121.0.6167.86	121.0.6167.85	🔵 セ
Jan 29, 2024 10:46:19 AM	ADSERVER	🔄 クライアントへの配信待ち		Google Inc.	Google Chrome	121.0.6167.86	120.0.6099.225	🟠 重

● アクションメニュー

インストールログの一覧を CSV で出力できます。

パッチ管理 ...

適用されていない

↓ インストールログをエクスポートする (CSV)

6.4. ソフトウェアレピュテーション

デバイスにインストールされているソフトウェアの評価を表示します。評価は弊社クラウド上の DB を参照します。

ソフトウェアレピュテーション (23)									
1 - 20 of 23									
ソフトウェア名	内部名	説明	ベンダー	デバイス	会社名	評価			
F-Secure Ultralight	obusclient2	F-Secure OBUS Client	F-Secure Corporation	3	JP Capital Management_	安全			
Windows Installer - Unic...	msi_messages	Windows® Installer Inte...	Microsoft Corporation	3	JP Capital Management_	安全			
F-Secure ORSP Client	orspplug	F-Secure ORSP Client DL...	F-Secure Corporation	3	JP Capital Management_	安全			
Windows Drive Optimizer	Defrag.EXE	Disk Defragmenter Mod...	Microsoft Corp.	3	JP Capital Management_	安全			
WithSecure Ultralight	pisces	WithSecure File Manage...	WithSecure Corporation	3	JP Capital Management_	安全			
WithSecure™ OneClient	WithSecure.Tools.dll	WithSecure.Tools	WithSecure Corporation	3	JP Capital Management_	安全			
Microsoft OneDrive	OneDriveStandaloneUpd...	Standalone Updater	Microsoft Corporation	2	JP Capital Management_	安全			
Microsoft Edge Installer	setup_exe	Microsoft Edge Installer	Microsoft Corporation	2	JP Capital Management_	安全			
Google Chrome Installer	mini_installer	Google Chrome Installer	Google LLC	2	JP Capital Management_	安全			
Google Chrome	optimization_guide_inter...	Google Chrome	Google LLC	2	JP Capital Management_	安全			

7. イベント

7.1. セキュリティイベント

各デバイスで発生したセキュリティのイベント一覧を確認できます。セキュリティイベントには EPP の様々な機能による検知、EDR のインシデント概要が表示されます。表示させる情報を制限したい場合は、フィルタ機能を利用してください。

日付	深刻度	ソース	対象	説明	確認済み	メニュー
1時間前 2024/01/31 15:19:11	注意	ブラウザ保護	CLIENT01	ドメイン名がブロックされているため、Webページがブロックされました。	なし	...
3時間前 2024/01/31 14:59:18	注意	ブラウザ保護	CLIENT01	ドメイン名がブロックされているため、Webページがブロックされました。	なし	...
2時間前 2024/01/31 14:19:23	注意	ブラウザ保護	CLIENT01	ドメイン名がブロックされているため、Webページがブロックされました。	なし	...
3時間前 2024/01/31 14:13:35	注意	EDR	CLIENT01	ID(2569324-262)のセキュリティCDインシデントが検出されました。	なし	...
3時間前 2024/01/31 14:12:19	注意	ファイル スキャン ファイル/フォルダ (1,394件)	CLIENT01	製品が「断続 予兆」ドキュメント (1)で「EICAR_Test_File」を検出し、ファイルを開閉しました。	なし	...
9日前 2024/01/22 17:28:38	対応が必要です	EDR	AD-SERVER	ID(2569324-187)のセキュリティCDインシデントが検出されました。	なし	...
9日前 2024/01/22 17:28:48	注意	デフォルト ファイル/フォルダ (1,394件)	AD-SERVER	悪意のあるアプリケーション「Droptool」が検出されました。	なし	...
14日前 2024/01/17 17:40:27	注意	EDR	AD-SERVER	ID(2569324-121)のセキュリティCDインシデントが検出されました。	なし	...
7日前 2023/06/26 10:55:58	対応が必要です	EDR	AD-SERVER	ID(2569324-55)のセキュリティCDインシデントが検出されました。	なし	...
8日前 2023/06/26 10:57:15	対応が必要です	EDR	AD-SERVER	ID(2569324-23)のセキュリティCDインシデントが検出されました。	なし	...

- セキュリティイベントの保存期間は深刻度に依存します。
 - ・ 情報：7 日間
 - ・ 注意：6 か月
 - ・ 対応が必要：13 か月

● アクションメニュー

項目名	内容
セキュリティイベントのエクスポート (JSON)	セキュリティイベントを JSON 形式でエクスポートします。
感染警告の構成	ウイルススキャンやパッチ管理対象のソフトウェアのスキャンをします。

■ セキュリティイベントのエクスポート (JSON)

セキュリティイベントを JSON 形式でエクスポートします。エクスポートした JSON ファイルをエクセルにインポートする場合には、以下のコミュニティ記事を参照してください。

[security events JSON ファイルを Microsoft Excel にインポートする](#)

■ 感染の警告

Elements EPP でマルウェアなどを検知した際に、登録したメールアドレスへ通知をする設定です。

感染警告の構成

Data Fellows Security

🔔

アラートは、感染型イベントがトリガーとなります。詳細を表示

🔴

メール通知を送る

言語*

日本語

メールアドレス*

test@test.com

受信者を追加

メール通知

この機能を使用すると、次のようなイベントが発生したときに、メール通知が送信されます。

- AMSI
- ディープガード
- ファイル スキャン
- スケジュールされたスキャンまたはローカル/リモートでトリガーされたスキャン
- Webスキャン

セキュリティイベントで感染を表示

7.2. Broad Context Detection

Elements EDR にて検知したインシデントを表示します。

7.2.1. Broad Context Detection

検知したインシデント（Broad Context Detection : BCD)の一覧です。表示させる情報を制限したい場合は、フィルタ機能を利用してください。

Broad Context Detection

Broad Context Detection イベント検索

合計: 42

表示: システムのデフォルト

フィルタ: 選択してください。 選択してください。 フィルター値を入力して... 追加

すべてのフィルターを解除

会社名 に等しい すべて


タイプ に等しい エンドポイント, クラウド

リスク に等しい 深刻, 高, 中

ステータス に等しい 新規, 確認済み, 進行中, 監視

アーカイブ済み に等しい 不正

ID	タイプ	リスク	カテゴリ	会社名	デバイス名	検出済み	変更済み
<input type="checkbox"/> 781619-113	エンドポイント	深刻	Recon 活動	FI NextGen Marketing	Win10RDB	4年前 11.12.2019 16:59:06 UTC+09:00	2ヶ月前 19.01.2024 19:12
<input type="checkbox"/> 781619-141	エンドポイント	深刻	Recon 活動	FI NextGen Marketing	Win10RDB	4年前 29.01.2020 17:45:31 UTC+09:00	20時間前 06.03.2024 16:03
<input type="checkbox"/> 2532078-9495	エンドポイント	中	異常なプロセス実行	FR IT-Sec	MacBook-Pro-de-GKPROD.local	1日前 06.03.2024 08:21:17 UTC+09:00	1日前 06.03.2024 08:22
<input type="checkbox"/> 2505387-1229	エンドポイント	中	異常なライブラリまたはモジュール	DE Stark Industries_	SLI-LH	2日前 05.03.2024 18:27:21 UTC+09:00	2日前 05.03.2024 19:25
<input type="checkbox"/> 2532078-9469	エンドポイント	中	異常なライブラリまたはモジュール	FR IT-Sec	DESKTOP-S8CKCOD	5日前 02.03.2024 23:54:46 UTC+09:00	5日前 02.03.2024 23:55
<input type="checkbox"/> 2484972-1541	エンドポイント	中	異常なネットワーク接続	IT International Sales	DESKTOP-SIQ6NN2	5日前 02.03.2024 18:18:00 UTC+09:00	5日前 02.03.2024 18:18
<input type="checkbox"/> 2532078-9459	エンドポイント	中	異常なネットワーク接続	FR IT-Sec	DESKTOP-TLFMF7L	6日前 01.03.2024 17:00:22 UTC+09:00	6日前 01.03.2024 17:07
<input type="checkbox"/> 2532078-9224	エンドポイント	高	権限のエスカレーション	FR IT-Sec	DESKTOP-TLFMF7L	18日前 18.03.2024 01:47:00 UTC+09:00	7日前 28.03.2024 03:54

- BCD の ID をクリックすることで、その BCD の詳細を確認することができます。BCD の確認の仕方などは、弊社トレーニング資料などを参照ください。
- 右上にある  メニューにて表示する項目を変更することができます。

Broad Context Detection

Broad Context Detection イベント検索



合計: 42

フィルタ: 選択してください。 選択してください。 フィルター値を入力して... 追加

すべてのフィルターを解除

会社名 に等しい すべて タイプ に等しい エンドポイント, クラウド リスク に等しい 深刻, 高, 中 × ステータス に等しい 新規, 確認済み, 進行中, 監視

ID	タイプ	リスク	カテゴリ	会社名	デバイス名
781619-113	エンドポイント	深刻	Recon 活動	FI NextGen Marketing	Win10RDR
781619-141	エンドポイント	深刻	Recon 活動	FI NextGen Marketing	Win10RDR
2532078-9495	エンドポイント	中	異常なプロセス実行	FR IT-Sec	MacBook-Pro-de-GKPR
2505387-1229	エンドポイント	中	異常なライブラリまたはモジュール	DE Stark Industries_	SLI-LH
2532078-9469	エンドポイント	中	異常なライブラリまたはモジュール	FR IT-Sec	DESKTOP-S8CKCOD
2484972-1541	エンドポイント	中	異常なネットワーク接続	IT International Sales	DESKTOP-SIQ6NN2
2532078-9459	エンドポイント	中	異常なネットワーク接続	FR IT-Sec	DESKTOP-TLFMF7L
2532078-9224	エンドポイント	高	権限のエスカレーション	FR IT-Sec	DESKTOP-TLFMF7L

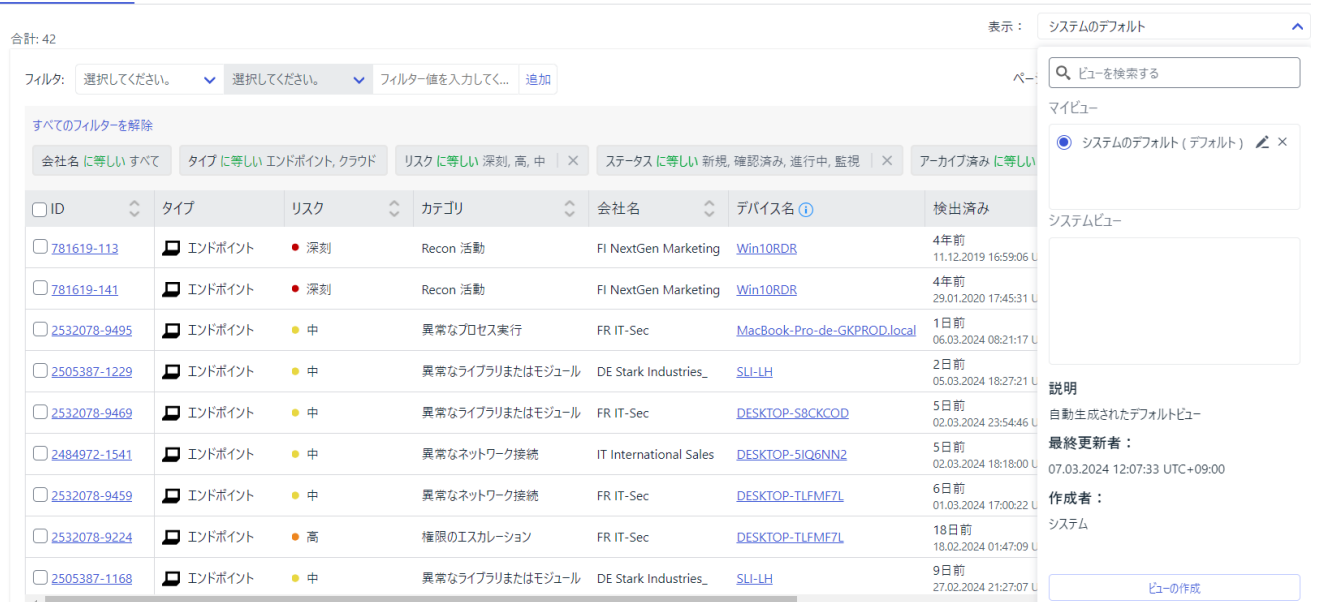
表示される列: ID, タイプ, リスク, カテゴリ, 会社名, デバイス名, 検出済み, 変更済み, ステータス, 解決, 昇格タイプ, プロパティ, コメント, 分析

非表示の列: エスカレーション ステータス, 位置ID

- 現在表示されている画面構成を保存し、次回から同じ内容を表示させることができます。

Broad Context Detection

Broad Context Detection イベント検索



合計: 42

フィルタ: 選択してください。 選択してください。 フィルター値を入力して... 追加

すべてのフィルターを解除

会社名 に等しい すべて タイプ に等しい エンドポイント, クラウド リスク に等しい 深刻, 高, 中 × ステータス に等しい 新規, 確認済み, 進行中, 監視 × アーカイブ済み に等しい

ID	タイプ	リスク	カテゴリ	会社名	デバイス名	検出済み
781619-113	エンドポイント	深刻	Recon 活動	FI NextGen Marketing	Win10RDR	4年前 11.12.2019 16:59:06 U
781619-141	エンドポイント	深刻	Recon 活動	FI NextGen Marketing	Win10RDR	4年前 29.01.2020 17:45:31 U
2532078-9495	エンドポイント	中	異常なプロセス実行	FR IT-Sec	MacBook-Pro-de-GKPROD.local	1日前 06.03.2024 08:21:17 U
2505387-1229	エンドポイント	中	異常なライブラリまたはモジュール	DE Stark Industries_	SLI-LH	2日前 05.03.2024 18:27:21 U
2532078-9469	エンドポイント	中	異常なライブラリまたはモジュール	FR IT-Sec	DESKTOP-S8CKCOD	5日前 02.03.2024 23:54:46 U
2484972-1541	エンドポイント	中	異常なネットワーク接続	IT International Sales	DESKTOP-SIQ6NN2	5日前 02.03.2024 18:18:00 U
2532078-9459	エンドポイント	中	異常なネットワーク接続	FR IT-Sec	DESKTOP-TLFMF7L	6日前 01.03.2024 17:00:22 U
2532078-9224	エンドポイント	高	権限のエスカレーション	FR IT-Sec	DESKTOP-TLFMF7L	18日前 18.02.2024 01:47:09 U
2505387-1168	エンドポイント	中	異常なライブラリまたはモジュール	DE Stark Industries_	SLI-LH	9日前 27.02.2024 21:27:07 U

表示: システムのデフォルト

マイビュー: システムのデフォルト (デフォルト) ×

システムビュー

説明: 自動生成されたデフォルトビュー

最終更新者: 07.03.2024 12:07:33 UTC+09:00

作成者: システム

ビューの作成

7.2.2. イベント検索

Elements EDR で収集したイベントを検索することができます。表示させる情報を制限したい場合は、フィルタ機能を利用してください。

Broad Context Detection

Broad Context Detection イベント検索

合計: 6116

表示: システムのデフォルト

フィルタ: 選択してください。 選択してください。 フィルター値を入力して... 追加

作成した見直し 以内に過去7日間 組織 に等しい JP Capital Management_

	作成した見直し	受信日時	デバイス名	組織	Process Name	イベントタイプ	Process CMDL
▼	5分前 07.03.2024 15:04:59 UTC+09:00	3分前 07.03.2024 15:07:11 UTC+09:00	Client01.TestAD.example.com	JP Capital Management_	MoUsoCoreWorker.exe	new_process	"C:\Windows\us\packages\p
▼	10分前 07.03.2024 14:59:51 UTC+09:00	8分前 07.03.2024 15:02:11 UTC+09:00	Client01.TestAD.example.com	JP Capital Management_	sdbinst.exe	new_process	C:\Windows\System32\sdbins
▼	11分前 07.03.2024 14:59:10 UTC+09:00	8分前 07.03.2024 15:02:11 UTC+09:00	Client01.TestAD.example.com	JP Capital Management_	install_145810731241.exe	registry_write	install
▼	11分前 07.03.2024 14:59:10 UTC+09:00	8分前 07.03.2024 15:02:11 UTC+09:00	Client01.TestAD.example.com	JP Capital Management_	install_145810731241.exe	registry_write	install
▼	11分前 07.03.2024 14:59:10 UTC+09:00	8分前 07.03.2024 15:02:11 UTC+09:00	Client01.TestAD.example.com	JP Capital Management_	install_145810731241.exe	registry_write	install
▼	15分前 07.03.2024 14:54:59 UTC+09:00	13分前 07.03.2024 14:57:08 UTC+09:00	Client01.TestAD.example.com	JP Capital Management_	MoUsoCoreWorker.exe	new_process	"C:\Windows\us\packages\p
▼	23分前 07.03.2024 14:46:57 UTC+09:00	20分前 07.03.2024 14:49:17 UTC+09:00	ADServer.TestAD.example.com	JP Capital Management_	install_9331923441.exe	registry_write	install
▼	23分前 07.03.2024 14:46:57 UTC+09:00	20分前 07.03.2024 14:49:17 UTC+09:00	ADServer.TestAD.example.com	JP Capital Management_	install_9331923441.exe	registry_write	install
▼	23分前 07.03.2024 14:46:57 UTC+09:00	20分前 07.03.2024 14:49:17 UTC+09:00	ADServer.TestAD.example.com	JP Capital Management_	install_9331923441.exe	registry_write	install
▼	23分前 07.03.2024 14:46:57 UTC+09:00	20分前 07.03.2024 14:49:17 UTC+09:00	ADServer.TestAD.example.com	JP Capital Management_	fshoster64.exe	module_load	"C:\Program Files (x86)\F-Sec

- 検索可能期間は最大で過去 7 日間です。

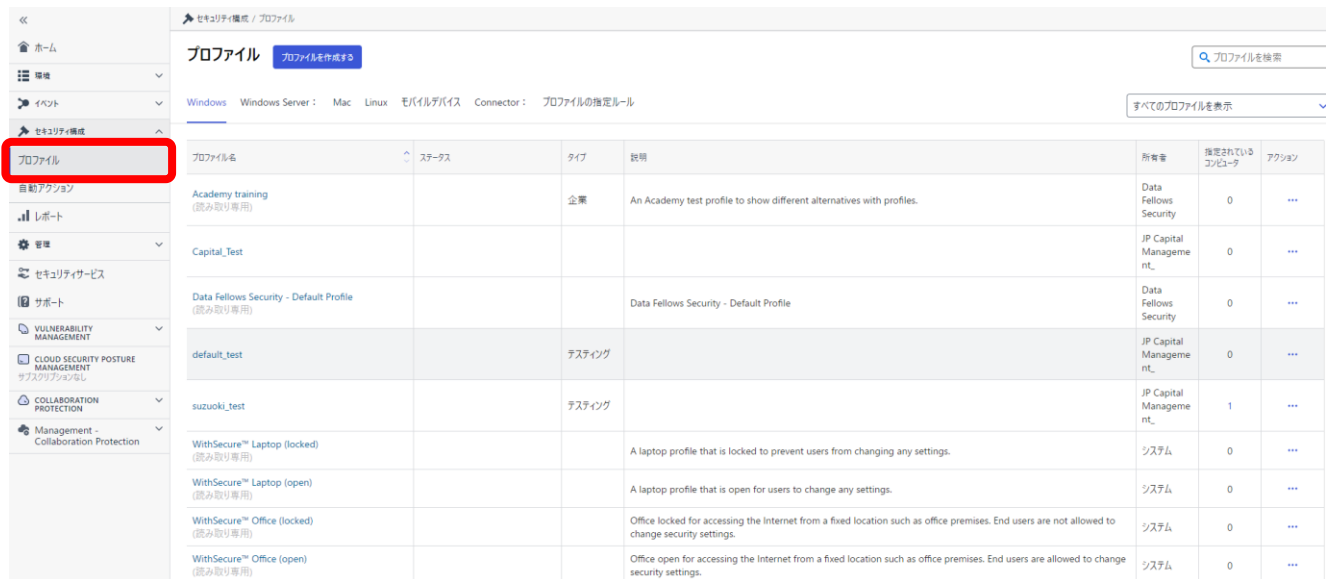
7.3. 応答

Elements EDR の[応答]機能を利用できます。[応答]機能はインシデントレスポンスのための機能で、ファイルの削除やサービス一覧の取得など、様々な機能を活用できます。[応答]機能の詳細は、弊社トレーニング資料などを参照ください。

8. セキュリティ構成

8.1. プロファイル

プロファイルとは、Elements EPP の設定のことです。各 Elements EPP クライアントや Elements Connector へプロファイルを適用することで、設定を一元管理することができます。プロファイルの設定項目の詳細な説明については、プロファイル画面にある?ボタンで確認できます。



プロファイル名	ステータス	タイプ	説明	所有者	指定されているコンピュータ	アクション
Academy training (読み取り専用)		企業	An Academy test profile to show different alternatives with profiles.	Data Fellows Security	0	---
Capital_Test				JP Capital Managemen nt.	0	---
Data Fellows Security - Default Profile (読み取り専用)			Data Fellows Security - Default Profile	Data Fellows Security	0	---
default_test		テスト		JP Capital Managemen nt.	0	---
suzuoki_test		テスト		JP Capital Managemen nt.	1	---
WithSecure™ Laptop (locked) (読み取り専用)			A laptop profile that is locked to prevent users from changing any settings.	システム	0	---
WithSecure™ Laptop (open) (読み取り専用)			A laptop profile that is open for users to change any settings.	システム	0	---
WithSecure™ Office (locked) (読み取り専用)			Office locked for accessing the Internet from a fixed location such as office premises. End users are not allowed to change security settings.	システム	0	---
WithSecure™ Office (open) (読み取り専用)			Office open for accessing the Internet from a fixed location such as office premises. End users are allowed to change security settings.	システム	0	---

プロファイル

[プロファイルを作成する](#)

[Windows](#) [Windows Server](#) : [Mac](#) [Linux](#) [モバイルデバイス](#) [Connector](#) : [プロファイルの指定ルール](#)

Elements EPP 製品ごとにプロファイルを作成できます。[プロファイルの指定ルール]では、クライアントが ESC に登録された時、もしくは、クライアントのデータに変更があった時に、自動的にプロファイルを適用することができます。

項目名	内容
Windows	Windows クライアント用のプロファイル
Windows Server	Windows サーバー用のプロファイル
Mac	Mac クライアント用のプロファイル
Linux	Linux サーバー用のプロファイル
モバイルデバイス	Elements Mobile Protection 用のプロファイル
Connector	Elements Connector 用のプロファイル
プロファイルの指定ルール	自動的にプロファイルを適用させるためのルール

8.1.1. プロファイルの作成

新規にプロファイルを作成する際に利用します。

- ① [プロファイルを作成する]をクリックします。

プロファイル

プロファイルを作成する

Windows Windows Server : Mac Linux モバイルデバイス Connector : プロファイルの指定ルール

- ② 必要な設定を入力し、[保存して発行]をクリックすると、新規プロファイルが作成されます。

Windowsのプロファイル

JP Capital Management_

...

✕

プロファイル名

test

説明

テスト用プロファイル

タイプ

テスト用

すべてのプロファイル設定

一般設定

このタブには、WithSecure™ Elements Agentのセキュリティ機能で共有される設定が含まれています。

特定の設定を検索するには、ここに入力してください...

クライアント ソフトウェアを速く利用する

この設定が有効になっている場合、このプロファイルに割り当てられているデバイスは新しい機能をリリースされる前に試すことができます。対象となるコンピュータは、他のユーザーよりも早く、数日前にソフトウェア アップデートを受け取ります。

クライアントにユーザー インターフェースを表示する

自動更新

HTTP プロキシを使用

リモート管理

手動で定義されたプロキシアドレス

10.0.0.100:80

プロキシ経由の接続を優先

プロキシの設定を隠す

保存して発行

- プロファイル名は必須項目です。
- タイプをプルダウンメニューから選択します。
- 必要に応じて説明を記載します。
- ?ボタンをクリックすると詳細な説明が表示されます。

8.1.2. プロファイル設定項目のロック

プロファイルの設定項目はユーザーが変更できないようにロックすることができます。

● プロファイルのロック

設定項目の右にある鍵マークをクリックすることで、ロック状態にできます。

Windowsのプロファイル

JP Capital Management_

指定されているコンピュータ: 0

更新日: 2022/09/07 22:00

プロファイルID: 6555126

...

一般設定	クライアント ソフトウェアを誰よりも早く利用する ?	<input type="checkbox"/>	
ウイルスのリアルタイム スキャン	クライアントにユーザー インターフェースを表示する ?	<input checked="" type="checkbox"/>	
マニュアル スキャン	▼ 自動更新 ?		
ブラウザ保護	HTTP プロキシを使用 ?	ユーザーブラウザの設定を検出 ▼	
ファイアウォール	手動で定義されたプロキシアドレス ?		

● プロファイルの一括ロック

全ての設定項目を一括でロックすることができます。

Windowsのプロファイル

JP Capital Management_

指定されているコンピュータ: 0

更新日: 2022/09/07 22:00

プロファイルID: 6555126

一般設定	クライアント ソフトウェアを誰よりも早く利用する ?	<input type="checkbox"/>	
ウイルスのリアルタイム スキャン	クライアントにユーザー インターフェースを表示する ?	<input checked="" type="checkbox"/>	
マニュアル スキャン	▼ 自動更新 ?		
ブラウザ保護	HTTP プロキシを使用 ?	ユーザーブラウザの設定を検出 ▼	
ファイアウォール	手動で定義されたプロキシアドレス ?		
ソフトウェア アップデータ	プロキシ経由の接続を優先 ?	<input type="checkbox"/>	

すべての設定をロックする
 すべての設定を解除する
 プロファイルをインポート
 プロファイルをエクスポート

8.1.3. プロファイルのエクスポート / インポート

プロファイル設定を json ファイル形式でエクスポートすることができます。エクスポートした json ファイルをインポートすることができます。

Windowsのプロファイル

JP Capital Management

指定されているコンピュータ: 0
更新日: 2022/09/07 22:00
プロファイルID: 6555126

一般設定

ウイルスのリアルタイムスキャン

クライアントソフトウェアを誰よりも早く利用する

クライアントにユーザーインターフェースを表示する

マニキュアルスキャン

自動更新

ブラウザ保護

HTTP プロキシを使用

ファイアウォール

手動で定義されたプロキシアドレス

ソフトウェアアップデート

プロキシ経由の接続を優先

すべての設定をロックする

すべての設定を解除する

プロファイルをインポート

プロファイルをエクスポート

ユーザーブラウザの設定を検出

キャンセル

複数のプロファイルに保存して発行

保存して発行

8.1.4. プロファイルの指定ルール

クライアントが登録された際に指定されるデフォルトルールや、クライアントの設定が変更された際に適用されるプロファイルを自動的に変更します。

● カスタムルール

新しいクライアントが ESC に登録された際に自動的に適用されるプロファイルを決定するルールです。ルールは上から順番に評価され、ルールが合致した際にそのプロファイルが適用されます。

プロファイルの指定ルール

☐ 変更の追跡。デバイスのルールを継続的に評価し、Active Directory組織単位、IP、リバースDNS、またはホスト名/WINS名の変更が検出されたときに、各デバイスのプロファイルとラベルの割り当てを変更します。

カスタムルールを追加する

順序	条件	クライアントタイプ	プロファイルを指定する	ラベルを追加する	説明	アクション
1	IPv4 <ul style="list-style-type: none">192.168.0.1/24	Windowsワークステーション	default_test			...
2	DNS <ul style="list-style-type: none">withsecure.com	Windowsサーバー	test_server			...

● カスタムルールの作成

[カスタムルールを追加する]をクリックし、新しいルールを作成することができます。

ルールがありません

プロファイルの指定ルール

変更の追跡。デバイスのルールを継続的に評価し、Active Directory組織単位、IP、リバースDNS、またはホスト名/WINSで変更します。

カスタムルールを追加する

順序	条件	クライアントタイプ	プロファイルを指定する	ラベルを追加
カスタムルール				
1	IPv4 • 192.168.0.1/24	Windowsワークステーション	default_test	
2	DNS • withsecure.com	Windowsサーバー	test_server	
3	ホスト名 • *-test	Linux	Test linux	
デフォルトルール				

ルールを追加

新しいプロファイルの割り当てルールは、新しいデバイスに自動的に適用されます。

条件*

オプションを選択してください。

クライアントタイプ*

オプションを選択してください。

プロファイルを指定する*

オプションを選択してください。

ラベルを追加する

キャンセル

ルールを追加

➤ ルール作成時には以下の条件を指定します。

項目名	内容
条件	<p>合致する条件を選択します。</p> <p>IPv4、DNS、ホスト名、AD OU マニュアル、AD の OU ツリー</p>
クライアントタイプ	<p>対象のクライアント OS を選択します。</p> <p>Windows ワークステーション、Windows サーバー、Linux、Mac</p>
プロファイルを指定する	適用するプロファイルを選択します。
ラベルを追加する	該当ルールを適用する際にラベルを追加します。
説明	必要に応じて説明を記載します。

● デフォルトルール

カスタムルールに合致するものがない場合、デフォルトルールで指定したプロファイルが適用されます。デフォルトルールはクライアントタイプごとに指定できます。指定は[...]メニューから実施します。

42

	デフォルト ルール ⓘ					
4	すべて	デフォルト	Windowsワークステーション	default_test		...
5	すべて	デフォルト	Windowsサーバー	WithSecure™ Server		...
6	すべて	デフォルト	Linux	WithSecure™ for Linux		...
7	すべて	デフォルト	Mac	WithSecure™ Office for Mac (open)		...
8	すべて	デフォルト	モバイル デバイス	WithSecure™ mobile (open)		...
9	すべて	デフォルト	Connector	Capital_Connector_Test		...

● 変更の追跡

クライアントの設定が変更された際に、条件との比較を実施し自動的に適用するプロファイルを変更するための機能です。

プロファイルの指定ルール ⓘ

☒ **変更の追跡。** デバイスのルールを継続的に評価し、Active Directory組織単位、IP、リバースDNS、またはホスト名/WINS名の変更が検出されたときに、各デバイスのプロファイルとラベルの割り当てを変更します。

8.1.5. プロファイルのアクションメニュー

プロファイルの右にある[...]メニューから各種アクションを実行できます。

プロファイル名	ステータス	タイプ	説明	所有者	指定されているコンピュータ	アクション
Academy training (読み取り専用)		企業	An Academy test profile to show different alternatives with profiles.	Data Fellows Security	0	...
Capital_Test				JP Capital Manag	0	...
Data Fellows Security - Default P... (読み取り専用)			Data Fellows Security - Default Profile			
default test		テスト				

- プロファイルをクローンする
- プロファイルを削除
- プロファイルの比較と編集
- 「Windows Server」プロファイルにコピーする
- プロファイルを別のアカウントにコピーする

- アクションメニュー

項目名	内容
プロファイルをクローンする	作成済みのプロファイルと同じ設定のプロファイルを作成します。
プロファイルを削除	不要になったプロファイルを削除することができます。
プロファイルの比較と編集	2つのプロファイルを比較し、その違いを確認することができます。また、異なるプロファイル設定を一方から他方へコピーすることができます。
「Windows Server」プロファイルにコピーする	Windows クライアントと Windows サーバー間でプロファイルをコピーすることができます。
プロファイルを別のアカウントにコピーする	SoP や SeP のユーザーアカウントでログインしている際、他の企業アカウントへプロファイルをコピーすることができます。

- プロファイルの比較と編集

① 右の[...]メニューから[プロファイルの比較と編集]を選択します。

プロファイル名	ステータス	タイプ	説明	所有者	指定されているコンピュータ	アクション
Academy training (読み取り専用)		企業	An Academy test profile to show different alternatives with profiles.	Data Fellow	0	...
Capital_Test						

プロファイルをクローンする

プロファイルの比較と編集

「Windows Server」プロファイルにコピーする

プロファイルを別のアカウントにコピーする

② 比較したいプロファイルを選択し[次へ]をクリックします。

プロファイルの比較と編集

JP Capital Management_

1

比較するプロファイルを選択

2

選択したプロファイルの比較と編集

✕

			profiles.		
<input checked="" type="checkbox"/>	Capital_Test			JP Capital Management_	0
<input type="checkbox"/>	Data Fellows Security - Default P... (読み取り専用)		Data Fellows Security - Default Profile	Data Fellows Security	0
<input checked="" type="checkbox"/>	default_test	テストイング		JP Capital Management_	0
<input type="checkbox"/>	tsuzuki_test	テストイング		JP Capital Management_	1

戻る

次へ

③ 設定が異なる項目が表示されます。

プロファイルの比較と編集

JP Capital Management_

✓

比較するプロファイルを選択

2

選択したプロファイルの比較と編集

✕

以下は、両プロファイルで異なる設定のみで、その他の設定はすべて同じです。異なる値は太字で表示されます。

プロファイル :

Capital_Test

プロファイル :

default_test

▼ 一般設定

クライアント ソフトウェアを誰よりも早く利用する

有効

↔

無効

▼ ファイアウォール

現在のファイアウォールプロファイル

Normal Workstation

↔

Normal Workstation

戻る

閉じる

➤ 矢印をクリックすると設定をコピーすることができます。

8.1.6. アウトブレイクルール

ESC に登録済みのクライアントが特定の条件に合致した場合に適用する特別なプロファイルです。

プロファイル

Windows Windows Server Mac Linux モバイルデバイス Connector : プロファイルの指定ルール

アウトブレイクルール

アウトブレイクルールを追加する

順序	条件	クライアントタイプ	プロファイルを指定する	ラベルを追加する
↑	アウトブレイクルール			

ルールがありません

プロファイルの指定ルール

変更の追跡。デバイスのルールを継続的に評価し、Active Directory組織単位、IP、リバースDNS、またはホスト名/WINS...を変更します。

ルールを追加

条件*

クライアントタイプ*

プロファイルを指定する*

ラベルを追加する

説明

キャンセル ルールを追加

項目名	内容
条件	合致する条件を選択します。 未解決の EDR インシデント、公共のインターネット上、ダイナミックリスクスコア
クライアントタイプ	対象のクライアント OS を選択します。 Windows ワークステーション、Windows サーバー、Linux、Mac
プロファイルを指定する	適用するプロファイルを選択します。
ラベルを追加する	該当ルールを適用する際にラベルを追加します。
説明	必要に応じて説明を記載します。

8.2. 自動アクション

Elements EDR にて BCD を検知した際の自動応答ルールを作成します。詳細については、弊社トレーニング資料などを参照ください。

9. レポート

各種グラフィカルレポートを確認することができます。

9.1. マイレポート

ウィジェットを追加して表示するレポートをカスタマイズすることができます。

- ① [ウィジェットを追加]をクリックします。



- ② 名前を記入し、データソースなどを選択します。



- ③ 表示したいレポートをすべて追加します。

レポート

マイレポート メール通知とレポート Detection and Responseのレポート デバイス セキュリティイベント ソフトウェアアップデート

クライアントバージョン

● クライアント バージョン 24.2: 2 デバイス

9.2. メールと通知

カスタムレポートをメールで送信することができます。

- ① [メールレポートを追加]をクリックします。

レポート

マイレポート メール通知とレポート Detection and Responseのレポート デバイス セキュリティイベント ソフトウェアアップデート

これは、カスタムメール レポートを作成できるメールレポートのセクションです。ぜひ、ご意見をお聞かせください。

このビューでは、特定のメールアドレスに配信されるアラートとスケジュールされたレポートを設定できます。

メールレポートを追加



有効	レポート名	ソース	スケジュールを	言語	受信者	アクション
メールレポートはありません						

② レポート名を入力し、データソースを選択します。

レポート

マイレポート メール通知とレポート Detection and Responseのレポート デバイス セキュリティイベント ソフトウェアアップデート

これは、カスタムメール レポートを作成できるメールレポートのセクションです。ぜひ

このビューでは、特定のメールアドレスに配信されるアラートとスケジュールされたレポートを設定できます

メールレポートを追加

有効	レポート名	ソース	スケジュールを
メールレポートはありません			

新しいメールレポートを追加

説明

レポート名 *

レポート名

データソース *

データソースを選択してください

キャンセル 保存

③ テンプレートをを選択します。テンプレートはデバイスやセキュリティイベントで保存されたビューから選択します。

レポート

マイレポート メール通知とレポート Detection and Responseのレポート デバイス セキュリティイベント ソフトウェアアップデート

これは、カスタムメール レポートを作成できるメールレポートのセクションです。ぜひ

このビューでは、特定のメールアドレスに配信されるアラートとスケジュールされたレポートを設定できます

メールレポートを追加

有効	レポート名	ソース	スケジュールを
メールレポートはありません			

新しいメールレポートを追加

テンプレート *

メールレポートのコンテンツをカスタマイズするテンプレートを選択してください

テンプレートを選択してください

Search for a template

コンピュータ

- Serveurs Windows
- TSM_Troubleshooting_View
- Test in Bulgaria
- Etat Ultra Light
- EOL devices

キャンセル 保存

④ 言語とスケジュールを設定します。

レポート

マイレポート メール通知とレポート Detection and Responseのレポート デバイス セキュリティイベント ソフトウェアアップデート

これは、カスタムメール レポートを作成できるメールレポートのセクションです。ぜひ

このビューでは、特定のメールアドレスに配信されるアラートとスケジュールされたレポートを設定できます

メールレポートを追加

有効	レポート名	ソース	スケジュールを
メールレポートはありません			

新しいメールレポートを追加

言語 *
日本語

スケジュールを

頻度 *
毎日

曜日 *
毎日

日時 *
hh:mm

タイムゾーン *

キャンセル 保存

⑤ タイムゾーンを選択し、送信先メールアドレスを入力します。

レポート

マイレポート メール通知とレポート Detection and Responseのレポート デバイス セキュリティイベント ソフトウェアアップデート

これは、カスタムメール レポートを作成できるメールレポートのセクションです。ぜひ

このビューでは、特定のメールアドレスに配信されるアラートとスケジュールされたレポートを設定できます

メールレポートを追加

有効	レポート名	ソース	スケジュールを
メールレポートはありません			

新しいメールレポートを追加

毎日

15:00

タイムゾーン *
(GMT+09:00) アジア/東京

☒ レポートにコンテンツがある場合にのみ送信する

受信者 *
Eメールアドレスをカンマ区切りで入力してください

受信者

キャンセル 保存

9.3. Detection and Response のレポート

Elements EDR に関するレポートを作成することができます。

① [スケジュールを追加]をクリックします。

レポート

マイレポート メール通知とレポート Detection and Responseのレポート デバイス セキュリティイベント ソフトウェアアップデート

スケジュールを追加

1 - 1 of 1 < 1 of 1 >

	名前	有効	レポートがあります	頻度	アクション...
^	test edr	<input checked="" type="checkbox"/>	0	Daily	...

ダウンロードできるレポート:

作成されたスケジュール: 2024-05-12

② レポート名、スケジュール、タイムゾーンを設定します。

レポート

マイレポート メール通知とレポート Detection and Responseのレポート デバイス セキュリティイベント ソフトウェアアップデート

スケジュールを追加

1 - 1 of 1 < 1 of 1 >

	名前	有効
^	test edr	<input checked="" type="checkbox"/>

ダウンロードできるレポート:

スケジュールを追加

詳細

レポート名 *

レポート名を入力してください

組織 * ⓘ

JP Capital Management_

スケジュール * ⓘ

Weekly

タイムゾーン * ⓘ

UTC

コンテンツ *

すべて解除

キャンセル

追加

③ レポートが作成されるとダウンロードリンクが作成されます。

レポート

マイレポート メール通知とレポート Detection and Responseのレポート デバイス セキュリティイベント ソフトウェアアップデート

スケジュールを追加

1 - 10 of 13 < 1 of 2 >

	名前	有効	レポートがあります	頻度	範囲	ア...
↑	andrea	<input checked="" type="checkbox"/>	14	Daily	RS GlobalCorp Inc.	...

ダウンロードできるレポート:

作成されたスケジュール: 2023-06-01

- [↓ 29 Apr 2024 \(有効期限まであと1日\)](#)
- [↓ 30 Apr 2024 \(有効期限まであと2日\)](#)
- [↓ 01 May 2024 \(有効期限まであと3日\)](#)
- [↓ 02 May 2024 \(有効期限まであと4日\)](#)
- [↓ 03 May 2024 \(有効期限まであと5日\)](#)
- [↓ 04 May 2024 \(有効期限まであと6日\)](#)
- [↓ 05 May 2024 \(有効期限まであと7日\)](#)
- [↓ 06 May 2024 \(有効期限まであと8日\)](#)
- [↓ 07 May 2024 \(有効期限まであと9日\)](#)
- [↓ 08 May 2024 \(有効期限まであと10日\)](#)
- [↓ 09 May 2024 \(有効期限まであと11日\)](#)
- [↓ 10 May 2024 \(有効期限まであと12日\)](#)
- [↓ 11 May 2024 \(有効期限まであと13日\)](#)
- [↓ 12 May 2024 \(有効期限まであと14日\)](#)

9.4. デバイス

Elements EPP に関する情報を確認することができます。期間は、直近 30 日もしくは 90 日を選択できます。表示されているレポートは画像、もしくは CSV で保存することができます。

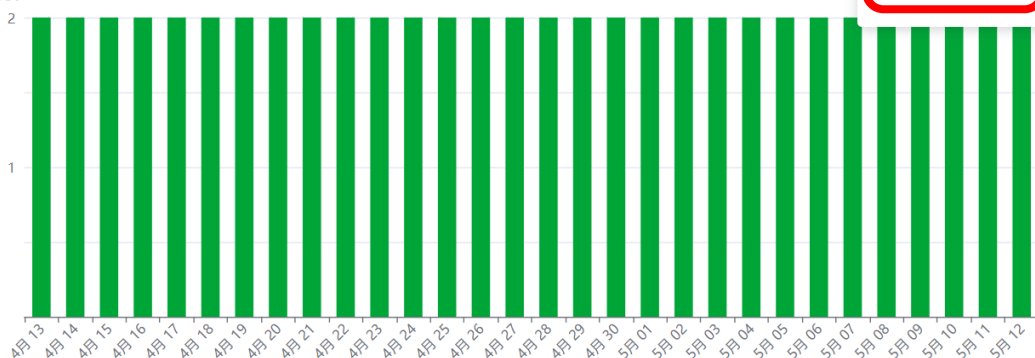
レポート

マイレポート メール通知とレポート Detection and Responseのレポート デバイス セキュリティイベント ソフトウェアアップデート

期間 最近30日

Computer Protection のステータス

2024 4月 13以降



- ☒ 最近30日
- ☐ 過去90日間



9.5. セキュリティイベント

過去 30 日間のセキュリティイベントの情報を確認することができます。表示されているレポートは画像、もしくは CSV で保存することができます。

レポート

マイレポート メール通知とレポート Detection and Responseのレポート デバイス セキュリティイベント ソフトウェアアップデート



9.6. ソフトウェアアップデート

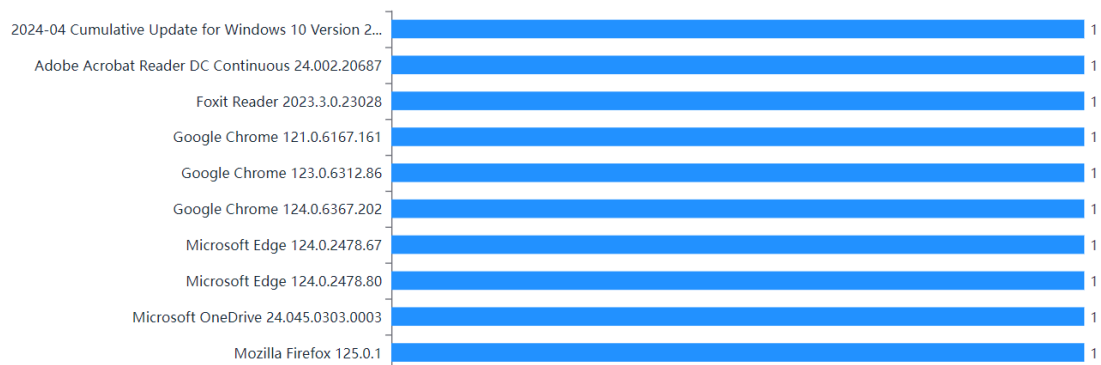
パッチ管理の情報を確認することができます。表示されているレポートは画像、もしくはCSVで保存することができます。

レポート

マイレポート メール通知とレポート Detection and Responseのレポート デバイス セキュリティイベント ソフトウェアアップデート

プラットフォームのタイプ すべてのプラットフォーム ▾ 以来: 2024/4/8

インストールされている上位のパッチ



10. 管理

10.1. 組織の設定

10.1.1. セキュリティ管理者

ESC の管理者の確認や追加を行うことができます。

- **管理者の追加**

- ① [管理者の追加]をクリックします。

組織の設定

セキュリティ管理者 Endpoint Protectionのアカウント APIクライアント Detection and Responseの設定

管理者を追加

オプションを選択

に等しい

値を追加

追加

すべてのフィルターをクリア

1 - 3 of 3

1 of 1

III

⚙

メール アドレス	ユーザ名	組織	Endpoint Pr...	Collaboration Pr...	Vulnerabilit...	Cloud Security P...	前回のログイン	MFAステー...
roman.hernandez	roman.hernand...	JP Capital Mana...		Collaboration Pr... 管理: 管理者			20.01.2021 17:05:23	無効
ringoame.frozenr	ringoame.froze...	JP Capital Mana...		Collaboration Pr... 管理: 管理者			06.11.2020 18:25:30	無効

- ② メールアドレスを入力します。

組織の設定

セキュリティ管理者 Endpoint Protectionのアカウント APIクライアント Detection and Responseの設定

管理者を追加

オプションを選択

に等しい

値を追加

追加

すべてのフィルターをクリア

1 - 3 of 3

1 of 1

III

⚙

管理者の詳細	
メールアドレス	ユーザ名
roman.hernandez	roman.hernand...
ringoame.frozenr	ringoame.froze...
julio.hirasawa+ca	julio.hirasawa+c...

管理者の詳細

メールアドレス

test@withsecure.com

新しいユーザー。

言語

日本語

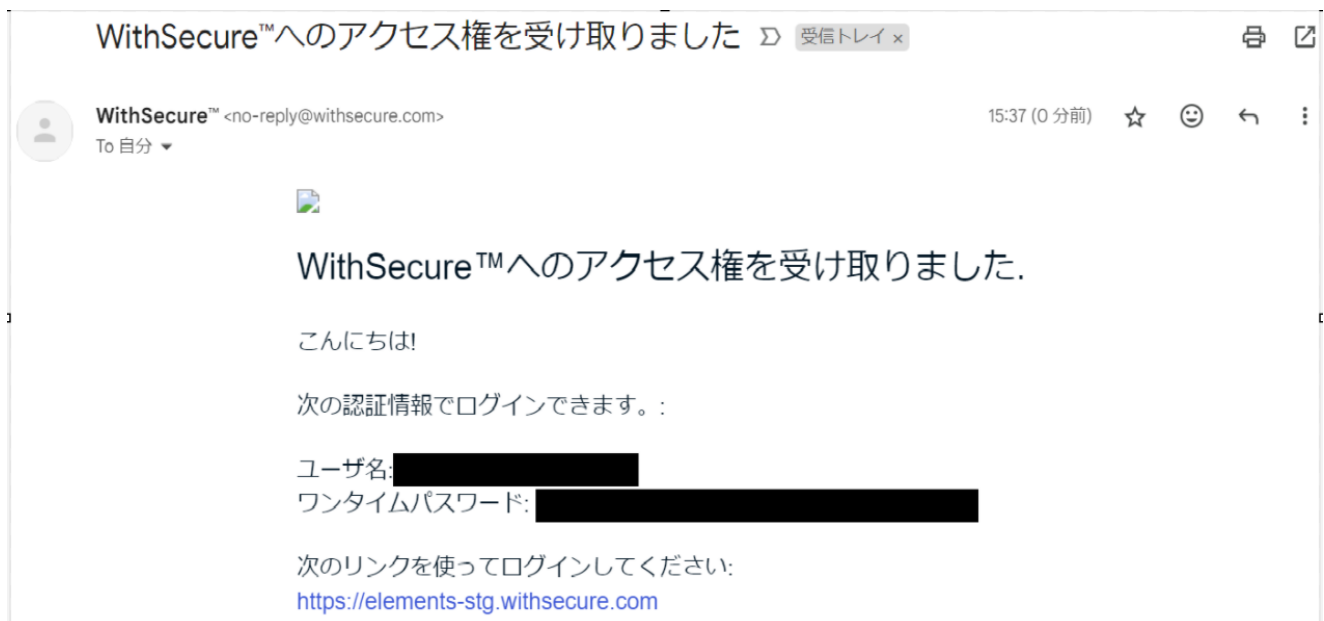
キャンセル

次へ

- ③ 各製品の権限を設定します。ライセンスを保有していない製品には権限の設定はできません。



- ④ 登録したメールアドレスへ以下のメールが送信されます。ワンタイムパスワードでログインしてください。



● 管理者の削除

- ① 削除したい管理者をクリックします。

組織の設定

セキュリティ管理者 Endpoint Protectionのアカウント APIクライアント Detection and Responseの設定

管理者を追加

オプションを選択 に等しい 値を追加 追加 すべてのフィルターをクリア

1 - 4 of 4 1 of 1

メール アドレス	ユーザ名	組織	Endpoint Pr...	Collaboration Pr...	Vulnerabilit...	Cloud Security P...	前回のログイン	MFAステー...
test@withsecure.c	test@withsecur...	JP Capital Mana...	コンピュータとモバイ... サーバ: フル編集	Collaboration Pr... 管理: 管理者	管理者	フル編集		無効
roman.hernandez-	roman.hernand...	JP Capital Mana...		Collaboration Pr... 管理: 管理者			20.01.2021 17:05:23	無効
ringoame.frozenr	ringoame.froze...	JP Capital Mana...		Collaboration Pr... 管理: 管理者			06.11.2020 18:25:30	無効

- ② 削除をクリックします。

組織の設定

セキュリティ管理者 Endpoint Protectionのアカウント APIクライアント Detection and Responseの設定

管理者を追加

オプションを選択 に等しい 値を追加

メール アドレス	ユーザ名	組織	Endpoint Pr...	Colla
roman.hernandez-	roman.hernand...	JP Capital Mana...		Colla 管理
ringoame.frozenr	ringoame.froze...	JP Capital Mana...		Colla 管理
julio.hirasawa+cap	julio.hirasawa+c...	JP Capital Mana...	コンピュータとモバイ... サーバ: フル編集	

roman.hernandez+test-company-jp2@f-secure.com

概要

メールアドレス: roman.hernandez+test-company-jp2@f-secure.com
組織: JP Capital Management_
MFAステータス: 無効

ロール

Cloud Security Posture Management

- ☐ フル編集
☒ アクセスなし

Collaboration Protection

管理

- ☒ 管理者
☐ アクセスなし

Collaboration Protection

閉じる

削除

保存

- [削除] グレーアウトしている場合は、すべて[アクセスなし]を選択し、一度保存してください。

- ③ [削除] をクリックします。

管理者を削除しますか？

test@withsecure.comを削除してもよろしいですか？この操作を元に戻すことはできません。

閉じる

削除

10.1.2. Endpoint Protection のアカウント

Elements EPP の管理者を作成できます。ただし、現在は[10.1.1 セキュリティ管理者]で実行可能なため、こちらの項目は利用する必要はありません。

10.1.3. API クライアント

Elements API を利用するための API クライアントを発行することができます。Elements API の詳細については、以下の URL を参照してください。

<https://connect.withsecure.com/>

10.1.4. Detection and Response の設定

Elements EDR の警告メールを送信するメールアドレスを設定できます。

組織の設定

セキュリティ管理者 Endpoint Protectionのアカウント APIクライアント Detection and Responseの設定

メール警告

警告メールの宛先を入力してください

複数のメールアドレスをカンマとスペースで区切って指定することができます。

10.2. サブスクリプション

契約しているライセンスの情報を確認できます。
サブスクリプションの情報は、csv と json 形式でダウンロードできます。

サブスクリプション

サブスクリプション Endpoint Protectionサブスクリプション

新しい [サブスクリプション] ページは読み取り専用モードです [詳細を表示](#)

オプションを選択 次 to 等しい オプションを選択 追加 すべてのフィルターをクリア

有効期限 次 to 等しい 有効

1 - 8 of 8 1 of 1

製品	ライセンス キーコード	組織	タイプ	使用済み	最大	有効期限
WithSecure Elements Vulne		JP Capital Management_	商業	スキャンされたターゲット数: 0	スキャンターゲットの制限: 50	有効期限 2024/05/17
WithSecure Elements Vulne		JP Capital Management_	商業	Endpoints count: 0	エンドポイントの制限: 10	有効期限 2024/05/17
WithSecure Elements EDR a		JP Capital Management_	商業	Endpoints count: 1	エンドポイントの制限: 50	継続的
WithSecure Elements EDR a		JP Capital Management_	商業	Endpoints count: 1	エンドポイントの制限: 50	継続的
WithSecure Elements EPP fc		JP Capital Management_	商業	Endpoints count: 1	エンドポイントの制限: 50	継続的
WithSecure Elements Conne		JP Capital Management_	商業	Endpoints count: 1	エンドポイントの制限: 10	継続的
WithSecure Elements EPP fc		JP Capital Management_	商業	Endpoints count: 0	エンドポイントの制限: 1	継続的

10.3. 監査ログ

ESC への管理者ログインやプロファイルの変更など、ESC に関する監査ログを確認することができます。

監査ログ

フィールドを選択

に等しい

値を選択してください

適用

キャンセル

すべてのフィルタを消去

タイムスタンプ 以内 最近14日

10件のエントリ

タイムスタンプ	説明	対象	トランザクションID
2時間前 2024/05/12, 14:46:06	管理者「junya.suzuoki+globaldemo@withsecure.com」がメールレポートスケジュール「test」を作成しました	test	0000-knyy0i0vf4m4hx29
2時間前 2024/05/12, 13:50:51	管理者「junya.suzuoki+globaldemo@withsecure.com」がメールレポートスケジュール「test」を削除しました	test	0000-o67i1b0jivjslu2
2時間前 2024/05/12, 13:48:49	管理者「junya.suzuoki+globaldemo@withsecure.com」がメールレポートスケジュール「test」を作成しました	test	0000-uljzu3vfmt2v478r
3時間前 2024/05/12, 12:59:52	管理者「junya.suzuoki+globaldemo@withsecure.com」がWindowsコンピュータのプロファイル「Capital_Test」を更新しました	Capital_Test	0000-vrmd7gyibvdsxnw
3時間前 2024/05/12, 12:58:10	管理者「junya.suzuoki+globaldemo@withsecure.com」がWindowsコンピュータのプロファイル「Capital_Test」を更新しました	Capital_Test	0000-afwrm5n0pfqrpatj
4時間前 2024/05/12, 12:28:22	管理者「junya.suzuoki+globaldemo@withsecure.com」がアカウント「JP Capital Management_」に対して変更追跡を有効にしました	JP Capital Management_	0000-xotnvtvua1mu16c
4時間前 2024/05/12, 12:20:52	管理者「junya.suzuoki+globaldemo@withsecure.com」がアカウント「JP Capital Management_」のプロファイル割り当てルールを保存しました	JP Capital Management_	0000-t1lw3oc6vnyhrqju
4時間前 2024/05/12, 12:10:26	管理者「junya.suzuoki+globaldemo@withsecure.com」がアカウント「JP Capital Management_」のプロファイル割り当てルールを保存しました	JP Capital Management_	0000-vnene69fj6vphnnt
4時間前 2024/05/12, 12:08:56	管理者「junya.suzuoki+globaldemo@withsecure.com」がアカウント「JP Capital Management_」のプロファイル割り当てルールを保存しました	JP Capital Management_	0000-ubufiz6h6hfkyywxw
4時間前	管理者「junya.suzuoki+globaldemo@withsecure.com」がアカウント「JP		

10.4. ダウンロード

Elements 製品のインストーラをダウンロードすることができます。表示される製品は、契約のあるもののみです。

ダウンロード

パブリックダウンロードページ

WithSecure™ Elements Agent for Computers

こちらからインストーラをダウンロードして、対象デバイスに転送することで、WithSecure™ Elements Agentをインストールできます。

詳細なインストール手順

Windows変更ログ

Mac変更ログ

以下のいずれかのサブスクリプションを使用できます

WithSecure Elements EPP for Computers

WithSecure Elements EDR and EPP for Computers

WithSecure Elements EDR for Computers

WithSecure Elements EPP for Computers Premium (Windowsのみ)

WithSecure Elements EDR and EPP for Computers Premium (Windowsのみ)

WithSecure Elements Vulnerability Management (Windowsのみ)

Windows

Mac

ダウンロード .exe

ダウンロード .msi

ダウンロード .mpkg

59

11. セキュリティサービス

WithSecure が提供しているサービスについての一覧を記載しています。契約がある場合、以下のように表示されます。

セキュリティサービス

My WithSecureサービス



エスカレーション

Elevate を使用すると、選択した検出を WithSecure にエスカレーションして、検出および対応チームに調査して修復ガイダンスを提供させることができます。エスカレーションはトークンを使用して行われ、様々な事前定義された組み合わせで提供されます。これらのトークンパッケージは、セールス代表を通じて一度限りの購入が可能です。

検証トークン：10

● 使用済み: 0 ● 利用可能: 10

調査トークン：10

● 使用済み: 0 ● 利用可能: 10

未使用のトークンは、EDRサブスクリプションとともに期限切れになります。



共同モニタリング

共同モニタリングサービスが正しく機能するためには、このサブスクリプションの適切な緊急連絡先詳細が記入されていることを確認してください。Out-of-officeバージョンを購入した場合は、タイムゾーンも調整してください。[自動化アクション] ビューで共同モニタリングを有効にできます。共同モニタリングではAuto-Elevate（自動昇格）が制限なく使用でき、さらに手動で検知の昇格を行うための検証トークンが3つ、調査トークンが1つ、月に提供されます。

検証トークン：10

● 使用済み: 0 ● 利用可能: 10

調査トークン：11

● 使用済み: 1 ● 利用可能: 10

これらのトークンは毎月期限切れになります。

利用可能なWithSecureサービス

共同セキュリティ

12. サポート

パートナーポータルやサポートリクエストページのリンクなどをまとめています。また、障害情報を表示するシステムステータスへのリンクも記載しています。

サポート

お問い合わせ

お問い合わせ

WithSecure PremiumまたはAdvancedサポートを利用している場合は、パートナーポータルでWithSecureサポートチームにチケットを作成したり、連絡を取ることができます。また、まだアクセス権がない場合は、このページでアクセスをリクエストすることもできます。

[パートナーポータルに移動する](#)

パートナーポータルへのアクセス権がない場合、サポートページでチケットを作成できます。

[Webサイトに移動する](#)

さらに、Webサイトからお電話いただけます。

[電話でのお問い合わせ](#)

ファイルサンプルを送信する

誤って検出または評価されたと疑われるファイルやURLのサンプルをWithSecureに送信して、さらなる分析を依頼できます。

[ファイルサンプルを送信する](#)

ホワイトリストへの登録リクエスト

誤検知を許可リストに追加して、システムは今後の同一の検出を自動的に閉じます。

[ホワイトリストへの登録リクエスト](#)

アクセス数が最も多いトラブルシューティング記事

「注目の記事」セクションで、WithSecureのトラブルシューティングに関して最もアクセスが多い記事を確認してください。

[記事を表示する](#)

システムステータス

運用状況、進行中および過去のインシデント、予定されているメンテナンスを確認してください。

[ステータスを確認する](#)

WithSecureサポートレベル

[詳細](#)

STANDARD

- すべてのWithSecureライセンス製品に含まれる内容
- サポート ケースは、パートナー ポータル、電話、または非優先キューのメールを通じて処理されます
- ベストエフォート型サービス（SLAなし）

ADVANCED

- 現地の営業時間内に利用可能
- WithSecureテクニカルサポートへの優先アクセス
- 発券とフォローアップのためのE-Serviceオンラインツール
- 定義された応答目標（応答SLA）

13. Appendix

Elements 製品が利用する URL

インターネット接続を制限している環境において Elements 製品を使用するためには、弊社 URL への接続を許可する必要があります。以下のコミュニティ記事を参照し、必要な URL への接続を許可してください。

参考 URL：

withsecure-elements-のネットワークアドレス-クラウド管理製品

<http://community.withsecure.com/ja/kb/articles/31217-withsecure-elements-のネットワークアドレス-クラウド管理製品>