ESET PROTECTソリューション
オンプレミス型セキュリティ管理ツール
ESET PROTECT V8
レポート機能紹介資料

第2版
2021年7月1日

キヤノンマーケティングジャパン株式会社

もくじ

1 .はじめに（本資料について）

本資料はセキュリティ管理ツールのレポート機能を紹介している資料です。セキュリティ管理ツールに関する機能紹介は別資料でご用意しています。本資料は、オンプレミス型セキュリティ管路ツールであるESET PROTECT（以降、EP）V8を例に、セキュリティ管理ツールのレポート機能を紹介しています。

※EP V8以上とEPCではEES/EEA V6.6以下、EFSW V6.5以下を管理することはできません。

プログラム名	略称	備考
ESET PROTECT	EP	オンプレミス型セキュリティ管理ツール ※ESET Security Management Centerの後継
ESET PROTECT Cloud	EPC	クラウド型セキュリティ管理ツール

※セキュリティ管理ツールのバージョンによって管理できるクライアント用プログラムに差異があります。
詳細は以下サポートページをご参照ください。
https://eset-support.canon-its.jp/faq/show/143?site_domain=business

1 .はじめに（本資料について）

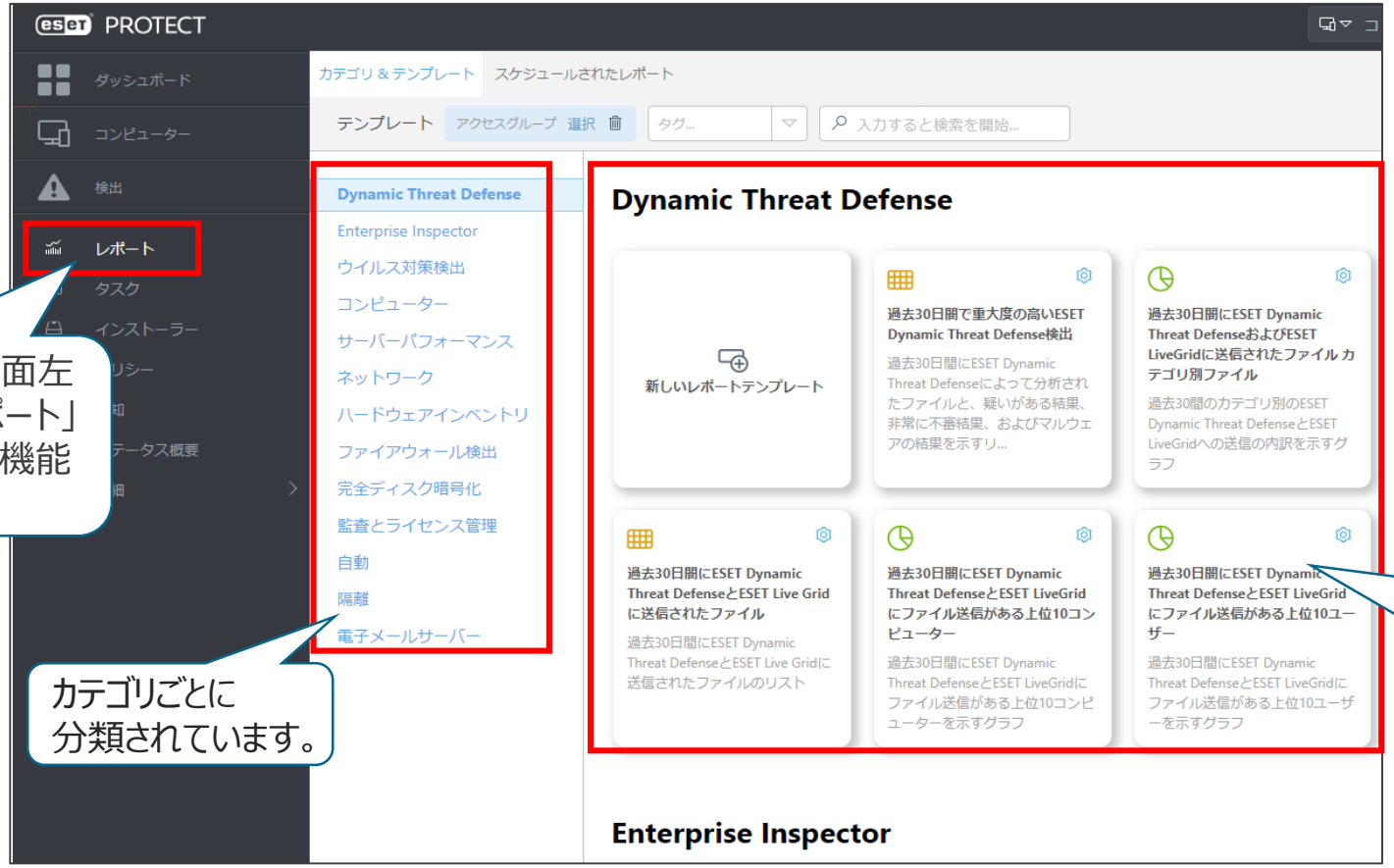
- 本資料で使用しているESET製品の画面イメージは使用するバージョンにより異なる場合があります。
  また、今後画面イメージや文言が変更される可能性がございます。
- ESET、NOD32、ThreatSense、LiveGrid、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET File Security、ESET NOD32アンチウイルス、ESET Security Management Center 、ESET PROTECT、ESET Dynamic Threat Defense、ESET Enterprise Inspector、 ESET Full Disk Encryption は、ESET,spol. s. r. o.の商標です。
- Windows、Windows Server、Microsoft Edge、Internet Explorerは、米国 Microsoft Corporation の米国、日本およびその他の国における商標登録または商標です。 macOS、OS X および iPhoneは、米国およびその他の国で登録されている Apple Inc. の商標です。

２ .レポートとは？

Canon
キヤノンマーケティングジャパン株式会社

2 .レポートとは？

クライアントから収集した情報やセキュリティ管理ツールの情報をもとにレポートを作成することができます。
既に定義されているレポートテンプレートは約120種類あり、テンプレートをもとに独自にレポートを作成することもできます。



EP Webコンソールの画面左のメインセクションの「レポート」をクリックすると、レポート機能が表示されます。

カテゴリごとに分類されています。

レポートはCSV、PDF形式でブラウザから直接ダウンロードすることができます。

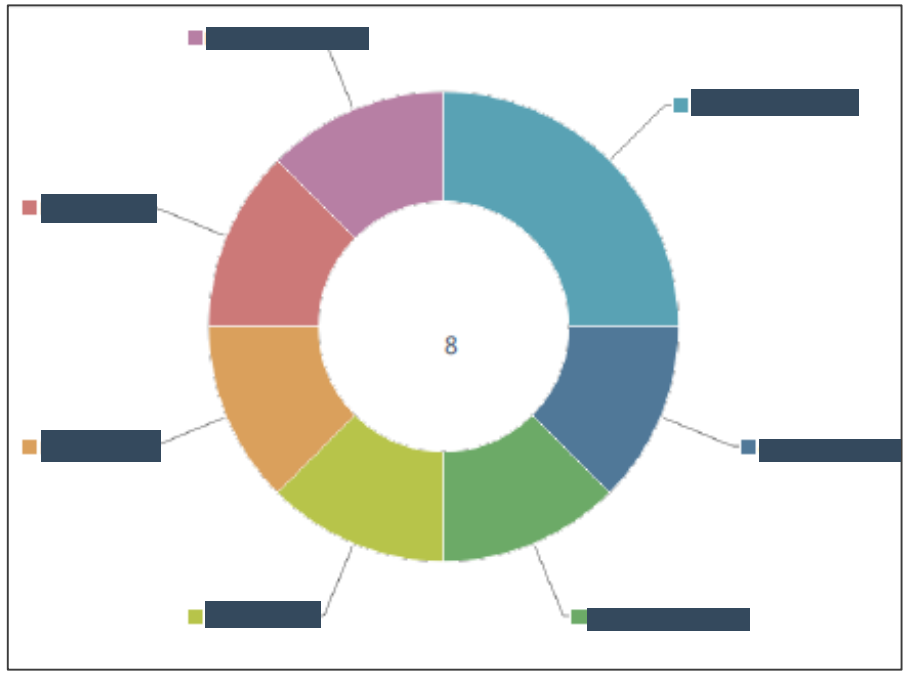
3.運用に役立つレポートテンプレートの紹介

Canon
キヤノンマーケティングジャパン株式会社

3 .過去7日間に検出イベントがあった上位のコンピューター

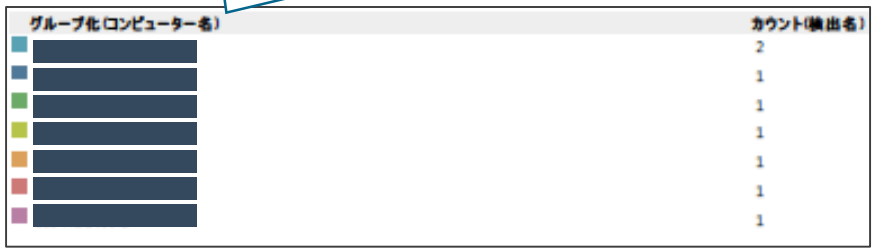
「過去7日間に検出イベントがあった上位のコンピューター」レポートはデータ※「ウイルス対策検出」の情報をもとにウイルス警告の多いコンピューターを抽出し、レポート化します。
ウイルス警告の多いクライアントを把握することで、ウイルスの感染・標的型攻撃の可能性が無いかなど、問題の早期発見に役立ちます。

※レポートで表示させるデータを指しております。データはレポート作成時に設定することができます。データの設定につきましては本資料の「P25　5. レポートテンプレートの作成手順」をご参照ください。



円グラフにてウイルス警告の多いコンピューターの割合を表示します。

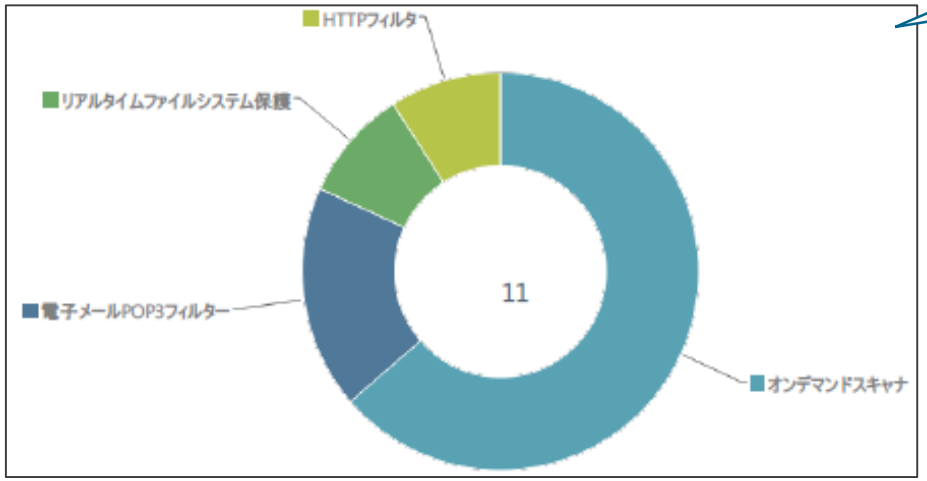
ウイルス警告の多いコンピューターを一覧表の形で表示します。



※PC名、ユーザー名などは非表示にしております。

3.スキャナー別過去30日のウイルス対策の検出

「スキャナー別過去30日のウイルス対策の検出」レポートはデータ「ウイルス対策検出」の情報をもとにウイルス検出した保護機能を抽出し、レポート化します。
保護機能ごとの比率を出すことで、ウイルスの侵入経路の割合を確認することができます。
HTTPフィルタであればインターネット経由、POP3フィルタであればメール経由、リアルタイムファイルシステム保護であれば外部ストレージ経由など、推測することが可能です。



円グラフにてスキャナー別ウイルス対策の検出の割合を表示します。

スキャナー別ウイルス対策の検出を一覧表の形で表示します。

グループ(スキャナー)	カウント(スキャナー)
オンデマンドスキャナ	7
電子メールPOP3フィルター	2
リアルタイムファイルシステム保護	1
HTTPフィルタ	1

3．過去7日間のアクティブな高重要度検出イベント

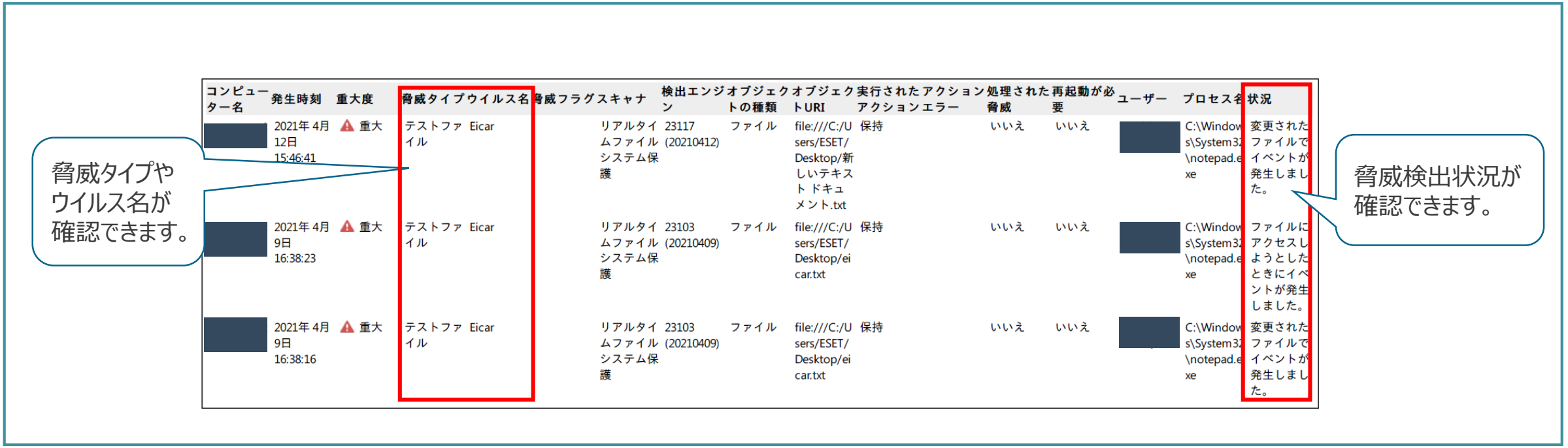
「過去7日間のアクティブな高重要度検出イベント」レポートはデータ「ウイルス対策検出」の情報をもとにウイルス検出後の処理が未解決のクライアントを抽出し、レポート化します。

抽出されたクライアントは、脅威が駆除/削除されずにクライアント内に存在している可能性があります。その場合、該当のクライアントの調査又はレスキューCDを利用した検査※の実施を検討ください。

※レスキューCDを利用した検査につきましては以下をご参照ください。

▽レスキューメディア（レスキューCD）にてコンピューターの検査を実施する手順

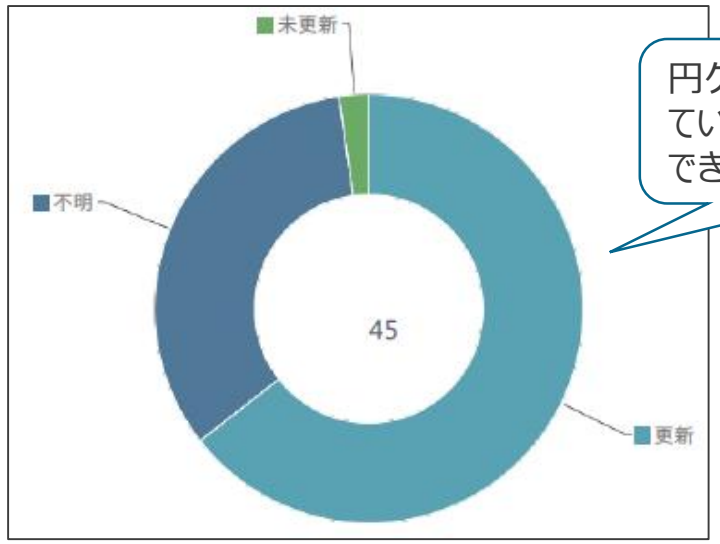
https://eset-support.canon-its.jp/faq/show/3639?site_domain=business



コンピューター名	発生時刻	重大度	脅威タイプウイルス名	脅威フラグ	スキャナ	検出エンジン	オブジェクトの種類	オブジェクトURI	実行されたアクション	アクションエラー	処理された脅威	再起動が必要	ユーザー	プロセス名	状況
[redacted]	2021年 4月 12日 15:46:41	重大	テストファイル Eicar		リアルタイムファイルシステム保護	23117 (20210412)	ファイル	file:///C:/Users/ESET/Desktop/新しいテキスト ドキュメント.txt	保持		いいえ	いいえ	[redacted]	C:\Windows\System32\notepad.exe	変更されたファイルでイベントが発生しました。
[redacted]	2021年 4月 9日 16:38:23	重大	テストファイル Eicar		リアルタイムファイルシステム保護	23103 (20210409)	ファイル	file:///C:/Users/ESET/Desktop/eicar.txt	保持		いいえ	いいえ	[redacted]	C:\Windows\System32\notepad.exe	ファイルにアクセスしようとしたときにイベントが発生しました。
[redacted]	2021年 4月 9日 16:38:16	重大	テストファイル Eicar		リアルタイムファイルシステム保護	23103 (20210409)	ファイル	file:///C:/Users/ESET/Desktop/eicar.txt	保持		いいえ	いいえ	[redacted]	C:\Windows\System32\notepad.exe	変更されたファイルでイベントが発生しました。

3．検出エンジンの更新ステータスの割合

「検出エンジン更新状況の割合」レポートはデータ「検出エンジン」の情報をもとに、アップデート状況を抽出し、レポート化します。
セキュリティレベルを高めるためには、検出エンジンが最新である必要があります。
アップデートがされていないクライアントが存在する場合は、検出エンジンのアップデートタスクを配信することを検討します。
※検出エンジンのアップデートタスクを配信する手順につきましては以下をご参照ください。
▽クライアント管理用プログラムから、クライアント用プログラムの検出エンジン（ウイルス定義データベース）をアップデートするには？
https://eset-support.canon-its.jp/faq/show/13247?site_domain=business



円グラフにて、更新されていない端末数を確認できます。

不明にはモバイルデバイスなどが含まれます。
モバイルデバイスの検出エンジン更新状況は別のレポートテンプレート(モバイルデバイス検出エンジン更新ステータスの割合)にて確認ください。

グループ化(ス	カウント(ステータス)
更新	29
不明	15
未更新	1

3. OS

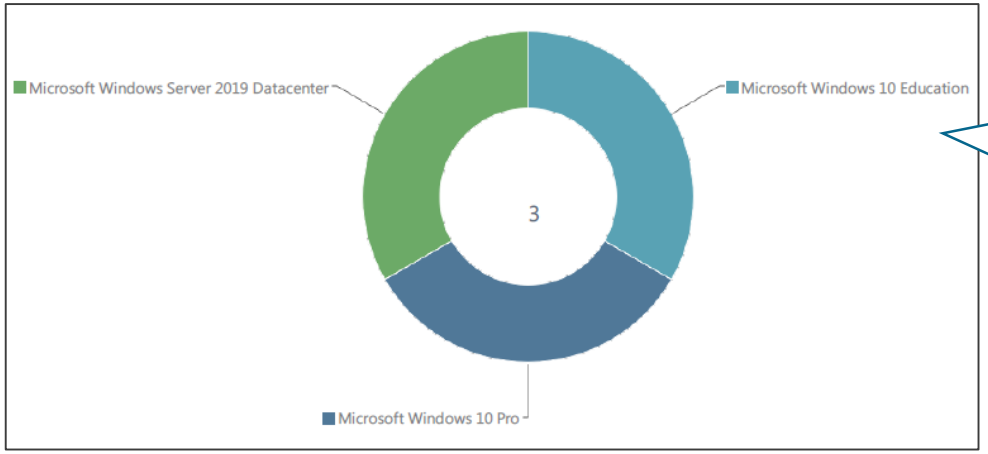
「OS」レポートはデータ「OSエディション」の情報をもとに、クライアントのOS情報を抽出し、レポート化します。

クライアントのOSを把握することで、レガシーOSの有無を確認することができます。レガシーOSは脆弱性を悪用した攻撃の対象になりやすいため、把握しておくことが重要です。また、クライアントで使われているOSを確認することで、クライアント用プログラムのバージョンアップ計画の参考にすることができます。

※レガシーOSの注意点につきましては以下をご参照ください。

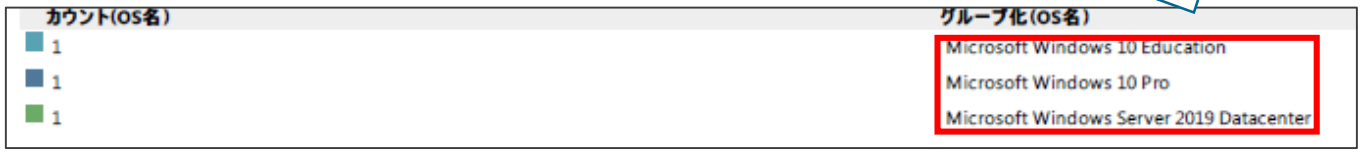
▽マイクロソフト社のサポートが終了したOSの利用を継続する場合の注意事項

https://eset-support.canon-its.jp/faq/show/303?site_domain=business



円グラフにて、OSの数量を確認できます。

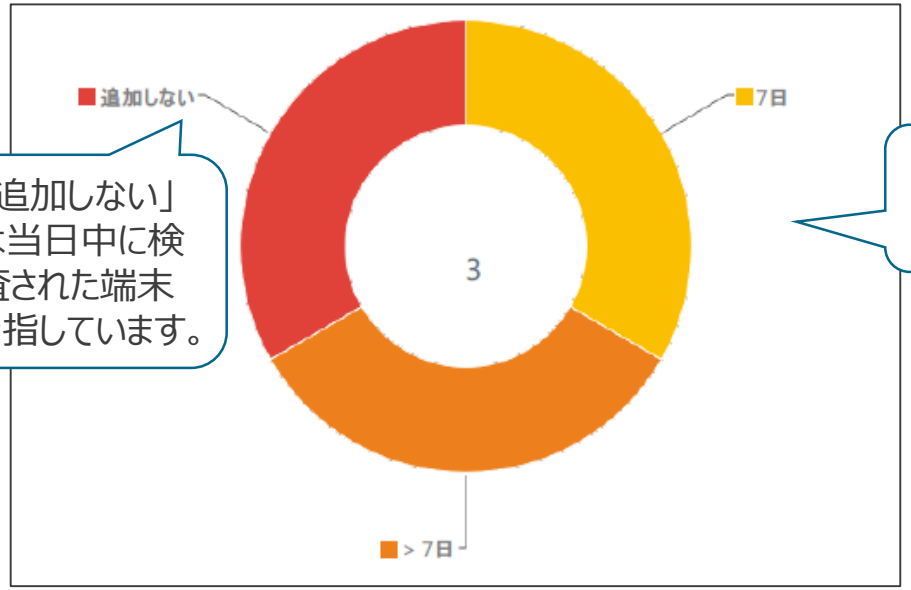
OS毎に数量が確認できます。OSのエディション毎にカテゴライズされて表示されます。



4.前回の検査

「前回の検査」レポートはデータ「前回の検査」の情報をもとに、クライアントが前回の検査のタイミングをレポート化します。長期間検査を実施していないクライアントを確認することができます。定期的に検査を行うことでセキュリティを保つことができます。長期的に検査を実施していないクライアントがある場合は該当のクライアントに対して検査を実施するなど検討してください。

※クライアントに対して検査をさせる設定手順につきましては以下をご参照ください。
▽クライアントに対して定期的にファイルの検査をさせるには？
https://eset-support.canon-its.jp/faq/show/100?site_domain=business



「追加しない」は当日中に検査された端末を指しています。

円グラフにて一定の検査日数毎で表示されます。

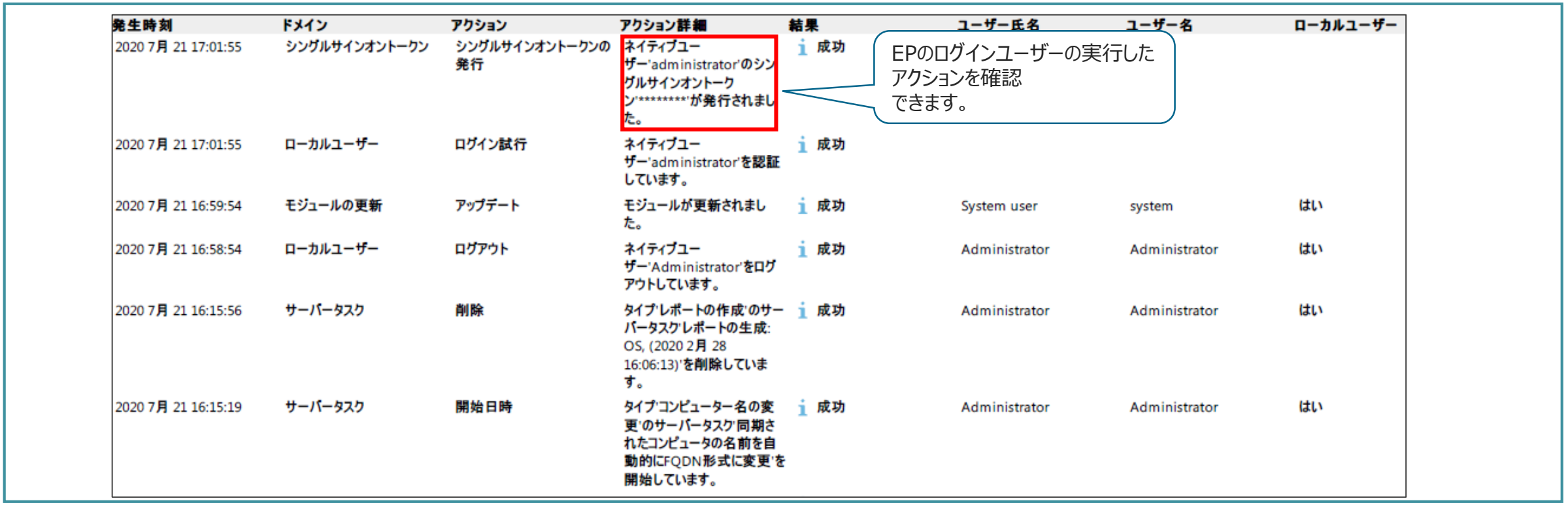
日数毎にカテゴライズされて表示されます。

カウントロンピューター)	可変間隔リスト(発生時間)
1	7日
1	> 7日
1	追加しない

4.監査ログ

「監査ログ」レポートはデータ「監査ログ」の情報をもとに、 EPのログインユーザーの動作を抽出し、レポート化します。各ログインユーザーがEP Webコンソール上で行った操作（ログイン情報、ポリシーの作成や変更、タスクの実行など）を確認することができます。管理者は、拠点ごとに複数のログインユーザーいる場合などはEP Webコンソールで実行されたアクティビティを検査することで、各ログインアカウントに対するユーザーの権限設定の見直しに役立てることが可能です。

※監査ログは「監査ログ」機能でも確認することができます。(監査ログのデータを出力することはできません。)監査ログのデータを出力する場合はレポート機能をご利用ください。



発生時刻	ドメイン	アクション	アクション詳細	結果	ユーザー氏名	ユーザー名	ローカルユーザー
2020 7月 21 17:01:55	シングルサインオントークン	シングルサインオントークンの発行	ネイティブユーザー'administrator'のシングルサインオントークン'*********'が発行されました。	成功			
2020 7月 21 17:01:55	ローカルユーザー	ログイン試行	ネイティブユーザー'administrator'を認証しています。	成功			
2020 7月 21 16:59:54	モジュールの更新	アップデート	モジュールが更新されました。	成功	System user	system	はい
2020 7月 21 16:58:54	ローカルユーザー	ログアウト	ネイティブユーザー'Administrator'をログアウトしています。	成功	Administrator	Administrator	はい
2020 7月 21 16:15:56	サーバータスク	削除	タイプ'レポートの作成'のサーバータスク'レポートの生成: OS, (2020 2月 28 16:06:13)'を削除しています。	成功	Administrator	Administrator	はい
2020 7月 21 16:15:19	サーバータスク	開始日時	タイプ'コンピューター名の変更'のサーバータスク'同期されたコンピュータの名前を自動的にFQDN形式に変更'を開始しています。	成功	Administrator	Administrator	はい

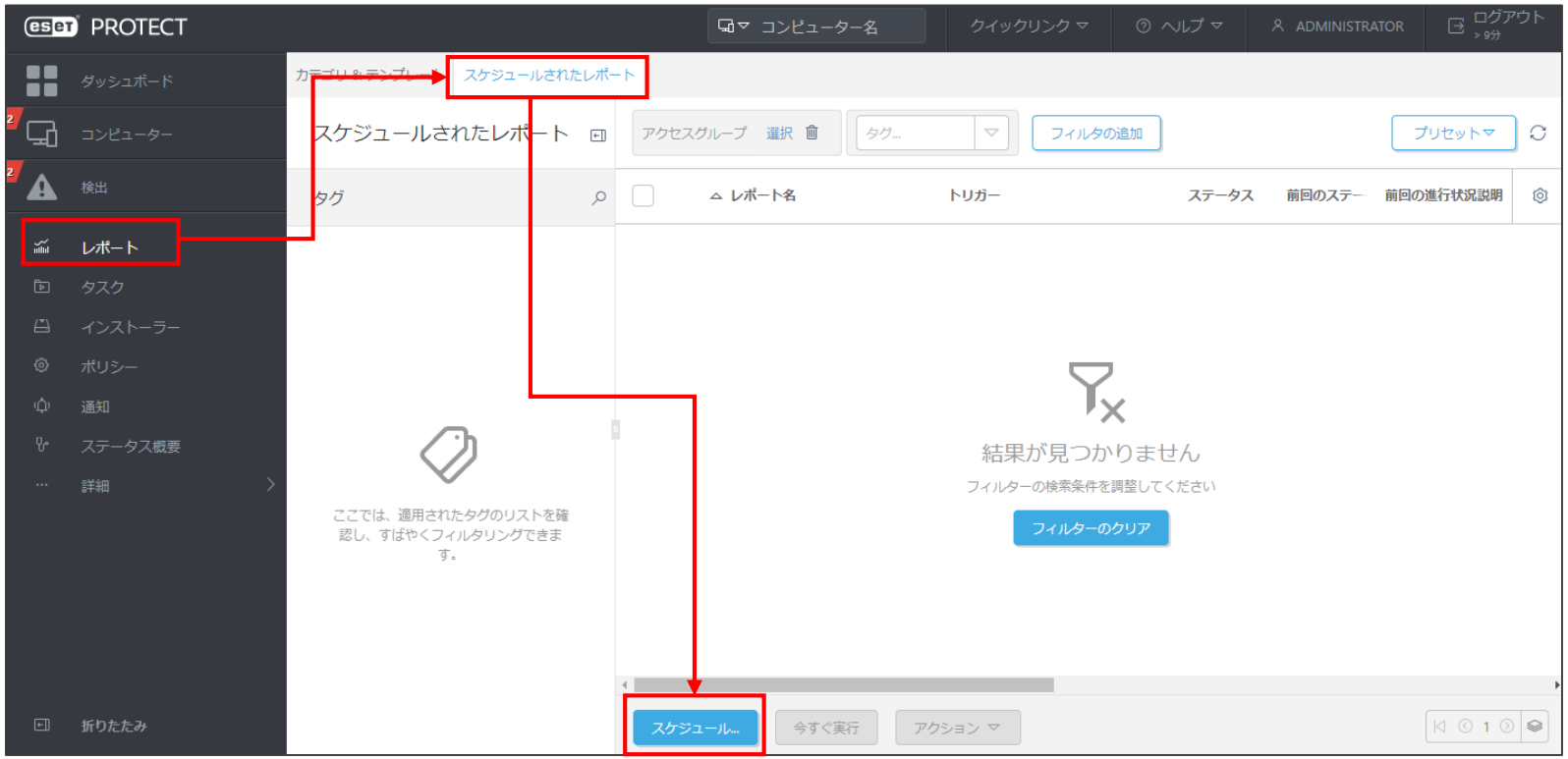
EPのログインユーザーの実行したアクションを確認できます。

４.レポートのスケジュール機能

Canon
キヤノンマーケティングジャパン株式会社

4 .レポートのスケジュール機能

「レポートのスケジュール」では指定したレポートテンプレートを定期的に作成することができます。
定期的に作成するタイミングは時間やイベント(動的グループのクライアントが変更されたタイミングなど)で設定することができます。
また、作成したレポートは「電子メールで送信」「フォルダに保存」ができます。



※「ESETクライアント管理 クラウド対応オプション」および「ESETクライアント管理 クラウド対応オプション Lite」では、レポートの自動作成および電子メールでの送信はできませんが、ブラウザよりダウンロードが可能です。

４.レポートのスケジュール機能設定手順

「1日1回レポートをメールで送信する」場合を例に、レポートのスケジュール設定手順を紹介します。

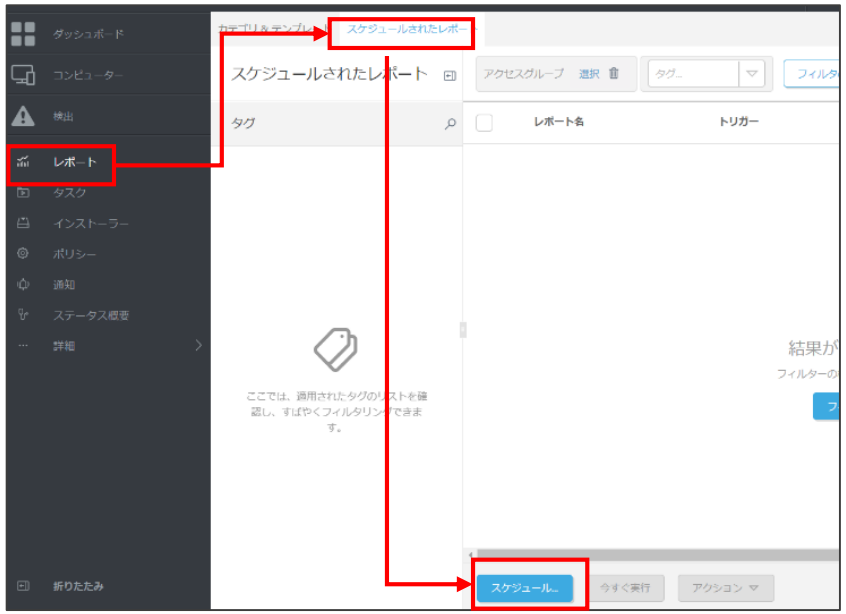
①EP Webコンソール を起動して、ESET PROTECT に接続します。ユーザー名とパスワードを入力し、「ログイン」をクリックします。

※ EP Webコンソールには以下のURLよりアクセスできます。
https://＜セキュリティ管理ツールのサーバー名、または、IPアドレス＞/era/

②EP Webコンソールの画面左のメインセクションの［レポート］より、［スケジュールされたレポート］、[スケジュール…]の順にクリックします。

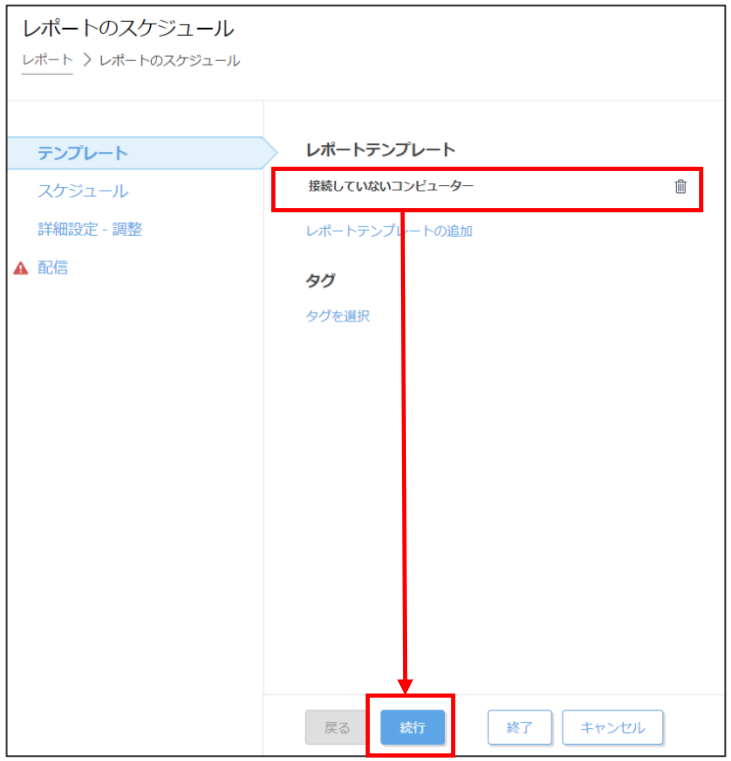
①の画面

②の画面



4 .レポートのスケジュール機能設定手順

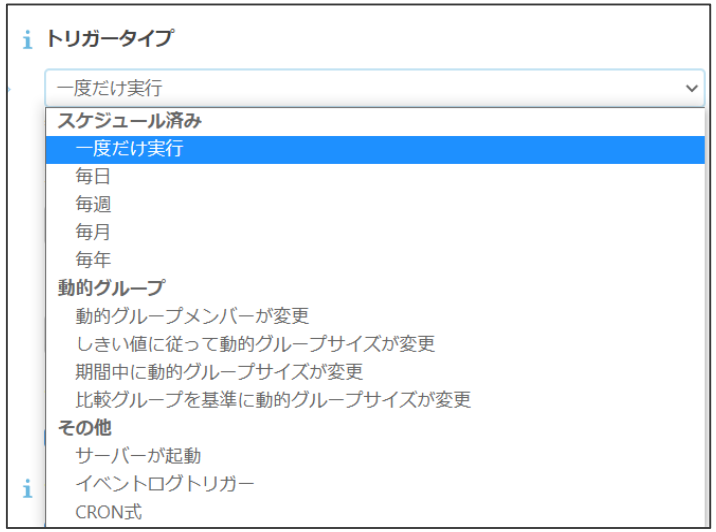
③「テンプレート」ではレポートテンプレートを設定します。
設定したいレポートテンプレートを［レポートテンプレートの追加］で選択します。必要に応じて［タグ］を選択してください。
テンプレートの設定が終わりましたら、［続行］をクリックします。
例）名前　：　接続していないコンピューター



4 .レポートのスケジュール機能設定手順

④「スケジュール」ではレポートの作成タイミングを設定します。
［トリガータイプ］を選択して、レポートが作成されるタイミングを設定ください。
トリガー毎に設定項目がことなります。任意の設定を行います。
テンプレートの設定が終わりましたら、［続行］をクリックします。
例）トリガータイプ　：　毎日

●トリガータイプ※

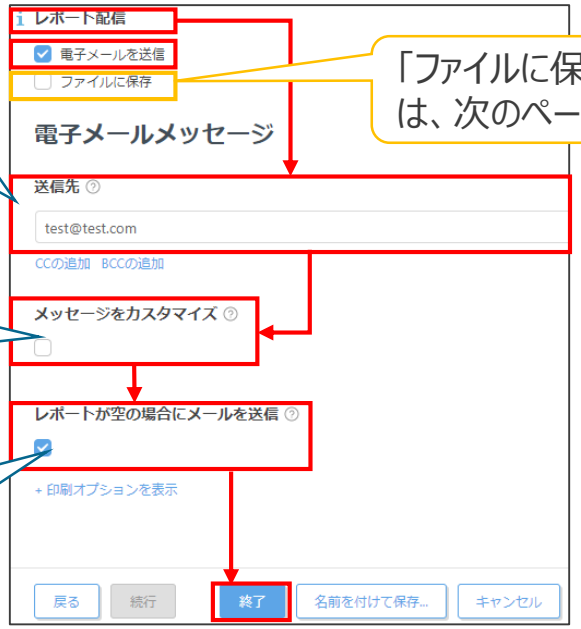


※トリガータイプつきましては以下をご参照ください。
▽タスクトリガータイプ　ESET PROTECT オンラインヘルプ
https://help.eset.com/protect_admin/80/ja-JP/?admin_st_triggers.html

4 .レポートのスケジュール機能設定手順

⑤「配信」ではレポート配信の設定をします。
［電子メール］［ファイルに保存］を選択して、レポートの出力方法を設定ください。
レポートの出力設定が終わりましたら、［終了］をクリックします。
以上で設定手順は終了です。

例）レポート配信　：電子メールに送信
送信先　：test@test.com
メッセージをカスタマイズ　：チェックなし
レポートが空の場合にメールを送信　：チェックあり



SMTPサーバー※の設定を事前に行う必要がございます。

「ファイルに保存」の詳細につきましては、次のページでご案内します。

メールの件名や本文をカスタマイズできます。

[PDF]、[CSV(表データのみ)]からレポート保存形式を設定できます。

※SMTPサーバーの詳細につきましては以下をご参照ください。
▽SMTPサーバー　ESET PROTECT オンラインヘルプ
https://help.eset.com/protect_admin/80/ja-JP/smtp_server.html

4 .(補足)レポートのスケジュール機能設定手順

フォルダにレポートを保存する際に設定する[ファイルに保存]について案内します。

- [相対ファイルパス] ではレポート保存時のフォルダの設定をします。(必ず相対パスでしてください)
  以下の形で設定をします。
  [保存先フォルダ※1] ￥ [保存時のフォルダ名※2]
  例)./TEST/%DATE%
- [レポートが空の場合にファイルを保存]ではレポートが作成できない場合の動作を指定します。

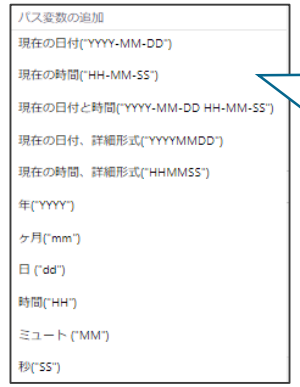
※1 既定フォルダ配下であれば任意の場所に設定できます。
既定のフォルダは以下となります。
Windowsの場合C:/ProgramData/ESET/RemoteAdministrator/Server/EraServerApplicationData/Data/GeneratedReports
Linuxの場合　/var/opt/eset/RemoteAdministrator/Server/GeneratedReports/

※2 保存時のフォルダのフォルダ名は「任意の文字列」+「パス変数」で設定できます。

設定例) ./TEST/%DATE%
上記の設定では既定のフォルダ配下の「フォルダ名：TEST」へ保存し、レポート保存時に作成されるフォルダ名は「現在の日時」となります。(レポート自体はレポート保存時に作成されるフォルダに保存されます。)

●ファイルオプション

●パス変数



パス変数は左記より指定できます。

5.レポートテンプレートの作成手順

Canon
キヤノンマーケティングジャパン株式会社

5. レポートテンプレートの作成手順

「検出エンジンのバージョンの一覧表を出力する」場合を例に、レポートテンプレートの作成手順を紹介します。

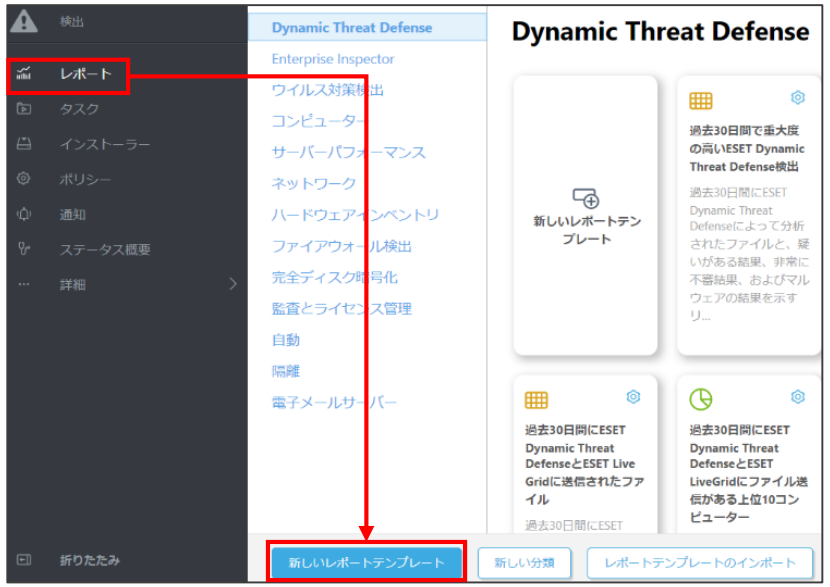
①EP Webコンソール を起動して、ESET PROTECT に接続します。ユーザー名とパスワードを入力し、「ログイン」をクリックします。

※ EP Webコンソールには以下のURLよりアクセスできます。
https://＜セキュリティ管理ツールのサーバー名、または、IPアドレス＞/era/

②EP Webコンソールの画面左のメインセクションの［レポート］より、［新しいレポートテンプレート］をクリックします。

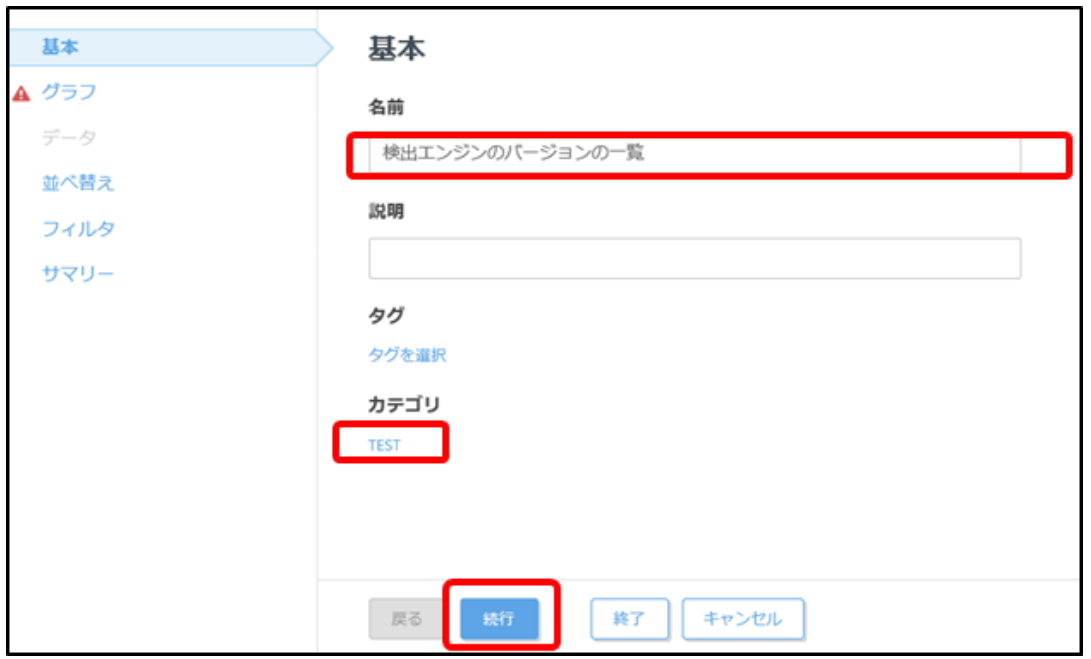
①の画面

②の画面



5. レポートテンプレートの作成手順

③「基本」ではレポートの基本情報を設定します。
作成するレポートテンプレートの［名前］を入力し、［カテゴリ］を選択します。
必要に応じて［説明］を入力し、［タグ］を選択してください。基本の設定が終わりましたら、［続行］をクリックします。
例）名前　：検出エンジンのバージョンの一覧
　　カテゴリ：TEST
※名前に「：」「＊」「＜」「＞」「／」「¥」「？」を含めないようにしてください。含めると正常にレポートが保存できないケースがありますのでご注意ください。

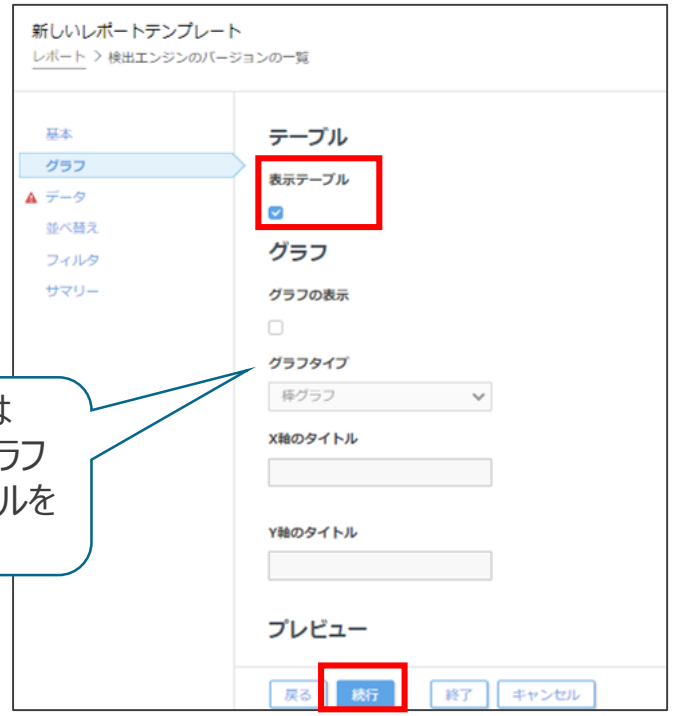


●カテゴリ一覧

既定のカテゴリも用意されていますが、任意のカテゴリも追加できます。
独自のカテゴリを追加することで既定のテンプレートと分けることができます。

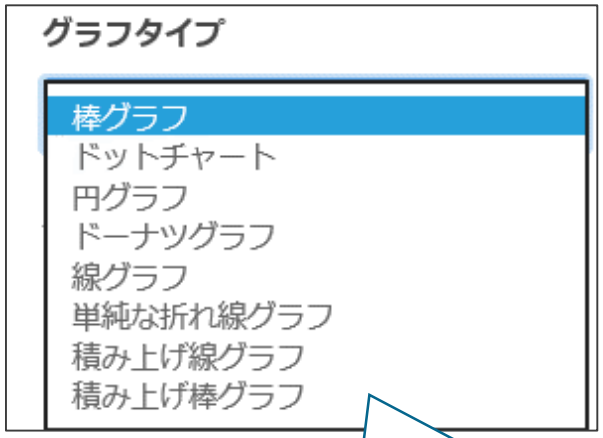
5. レポートテンプレートの作成手順

④「グラフ」では表示させるデータを設定します。
テーブルを表示させる場合は［表示テーブル］にチェックをいれます。
グラフの設定が終わりましたら、［続行］をクリックします。
例)　表示テーブル　　：チェックあり
　　グラフの表示　　：チェックなし



グラフを表示させたい場合には［グラフタイプ］を選択し、グラフで使用するX軸とY軸のタイトルを入力します。

●グラフタイプ一覧



グラフタイプは以下より選択できます。

5. レポートテンプレートの作成手順

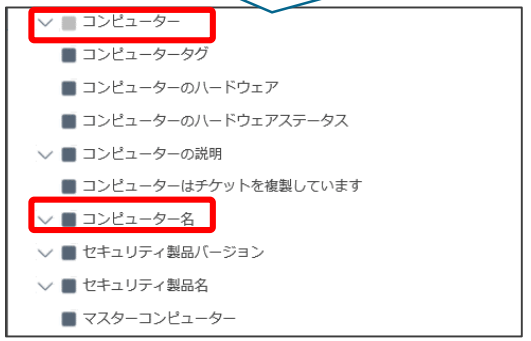
⑤「データ」では表示するデータを設定します。

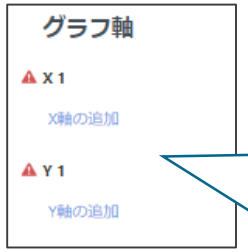
［列の追加］より、表示させるテーブル列のデータを設定します。データの設定が終わりましたら、［続行］をクリックします。

例)　テーブル列：コンピューター,コンピューター名,コンピューター名
検出エンジン,データベースのバージョン
検出エンジン,データベース日付

［印刷プレビュー］をクリックすると、作成中のテンプレートのプレビューを表示できます。

テーブルに表示させたいデータを一覧より選択します。





③にて［グラフの表示］のチェックボックスをクリックするときは、［X軸の追加］または［Y軸の追加］にて表示させたいグラフの設定をしてください。

5. レポートテンプレートの作成手順

⑥「並び替え」では表示させるデータの順番を設定できます。

［並び替えの追加］をクリックして、データの並び替えを行います。データの並び替えが終わりましたら、［続行］をクリックします。

例)　並び替え：コンピューター,コンピューター名,昇順

5. レポートテンプレートの作成手順

⑦「フィルタ」ではレポートに表示させる情報にフィルタをかけることができます。フィルタによりレポートで抽出するデータの範囲指定することができます。
［フィルタの追加］よりフィルタの設定を行います。フィルタの設定が終わりましたら、［続行］をクリックします。
例)　フィルタ条件：静的グループ,静的グループ,=(等しい),TEST
※上記の例は静的グループ「TEST」よりデータを抽出するフィルタの設定です。

⑧「サマリー」レポートテンプレートの設定内容を確認できます。内容を確認し、［終了］をクリックします。
以上で設定手順は終了です。

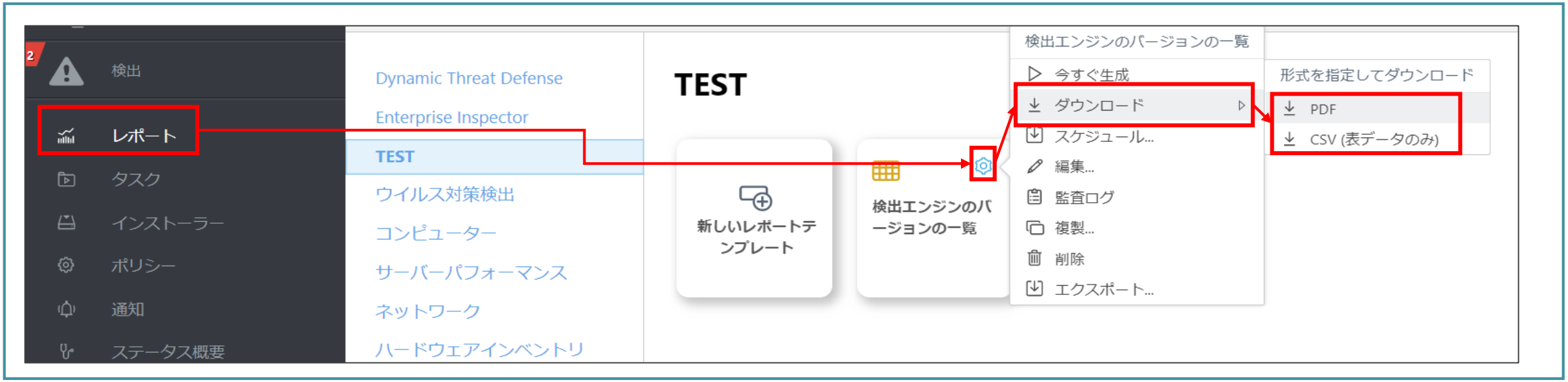
5. (補足)レポートテンプレートの作成手順

レポートテンプレートより、レポートをダウンロードする方法について案内します。

①EP Webコンソール を起動して、ESET PROTECT に接続します。ユーザー名とパスワードを入力し、「ログイン」をクリックします。
※ EP Webコンソールには以下のURLよりアクセスできます。
https:// <セキュリティ管理ツールのサーバー名、または、IPアドレス> /era/

②EP Webコンソールの画面左のメインセクションの［レポート］より、ダウンロードしたレポートのテンプレートを選択し、[歯車マーク] をクリックします。

③[ダウンロード]を選択し、ダウンロードしたいレポート形式([PDF]または[CSV(表データのみ)])をクリックします。その後、指定した形式でレポートがダウンロードされます。



6.参考情報

Canon
キヤノンマーケティングジャパン株式会社

6. 参考情報

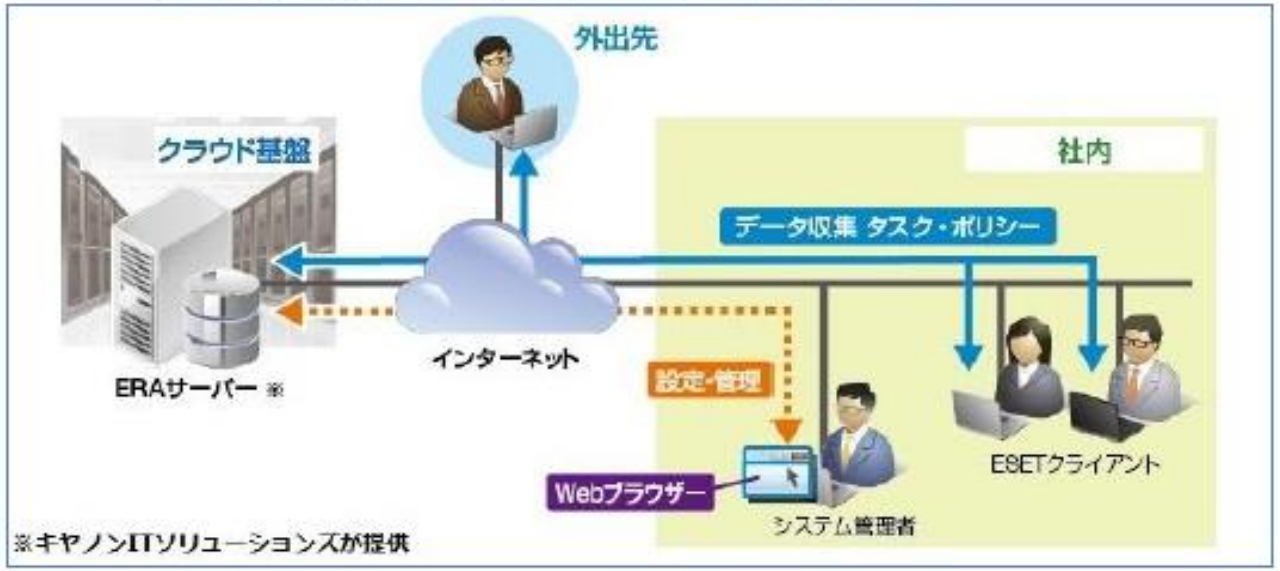
セキュリティ管理ツール(※)をクラウド上で提供するオプション製品を以下の２つのラインナップで提供しております。

・「ESETクライアント管理 クラウド対応オプション」

・「ESETクライアント管理 クラウド対応オプション Lite」

クラウド対応オプション製品では、クラウド上のセキュリティ管理ツールを使用するので、社内にサーバーを設置することなくクライアント管理を行うことができます。

<ESET クライアント管理 クラウド対応オプション利用イメージ>



※クライアント管理用プログラムは、ESET Security Management Center V7.2でご提供しています。（2021年5月現在）

6. 参考情報

レポートテンプレートカテゴリの「ESET Dynamic Threat Defense※ 1 」「ESET Enterprise Inspector※ 2 」「完全ディスク暗号化(ESET Full Disk Encryption)※ 3 」は ESET Endpoint Protection シリーズと別製品に関するものです。このレポートテンプレートを利用するには、ESET Endpoint Protection シリーズのライセンスとは別に該当の製品のライセンスを購入する必要があります。

※ 1 ESET Dynamic Threat Defense
未知のマルウェアに対する検出・防御の即時性を高め、ESET PROTECTソリューションの検出力・防御力を高めるクラウドサービスです。
製品の特長・動作環境・価格については以下のWebページをご参照ください。
https://eset-info.canon-its.jp/business/edtd/

※ 2 ESET Enterprise Inspector
組織内の端末から収集したさまざまなアクティビティをもとに、端末上の疑わしい動きを検出・分析・調査し、組織内に潜む脅威をいち早く割り出し、封じ込めることができるEDR製品です。
製品の特長・動作環境・価格については以下のWebページをご参照ください。
https://eset-info.canon-its.jp/business/eei/

※ 3 完全ディスク暗号化(ESET Full Disk Encryption)
リモートワークや社内で利用するクライアントPCのディスクを暗号化し、PC紛失・盗難時の情報漏えいから、お客さまの機密情報を守る暗号化製品です。
製品の特長・動作環境・価格については以下のWebページをご参照ください。
https://eset-info.canon-its.jp/business/efde/