ESET Cloud Office Security
機能紹介資料

CLOUD OFFICE SECURITY

第12版

2024年11月

Canon

キヤノンマーケティングジャパン株式会社

はじめに

- 本資料はESET PROTECTソリューションで提供しているクラウドアプリケーションセキュリティ製品「ESET Cloud Office Security(以降、ECOS)」の機能を紹介した資料です。

- 本資料で使用している画面イメージや文言は今後変更される可能性がございます。また本資料では、Microsoft365のテナント管理をベースにご紹介しておりますが、Google Workspaceでもご利用いただけるようになりました。
- ECOSのライセンスは保護されているユーザー数(共有メールボックス含む)でカウントされます。

- ECOSをご利用いただくにはESET PROTECT HUB (以降、EPH)の作成とEPHへのライセンス登録が必要です。
  https://protecthub.eset.com
  ※既存のお客さまはESET Business Accountでのライセンス登録が必要です。

- Azure、Active Directory、Microsoft 365、Microsoft Teams、Office 365、OneDrive、Outlook、SharePoint、Teamsは、米国Microsoft Corporationの、米国、日本およびその他の国における登録商標または商標です。

- ESET PROTECTソリューションではWindows、Mac、Android OS向けのプログラムもご使用いただけます。また、Windowsサーバー、LinuxサーバーOS向けのプログラムもご使用いただけます。

©Canon Marketing Japan Inc.

もくじ

©Canon Marketing Japan Inc.

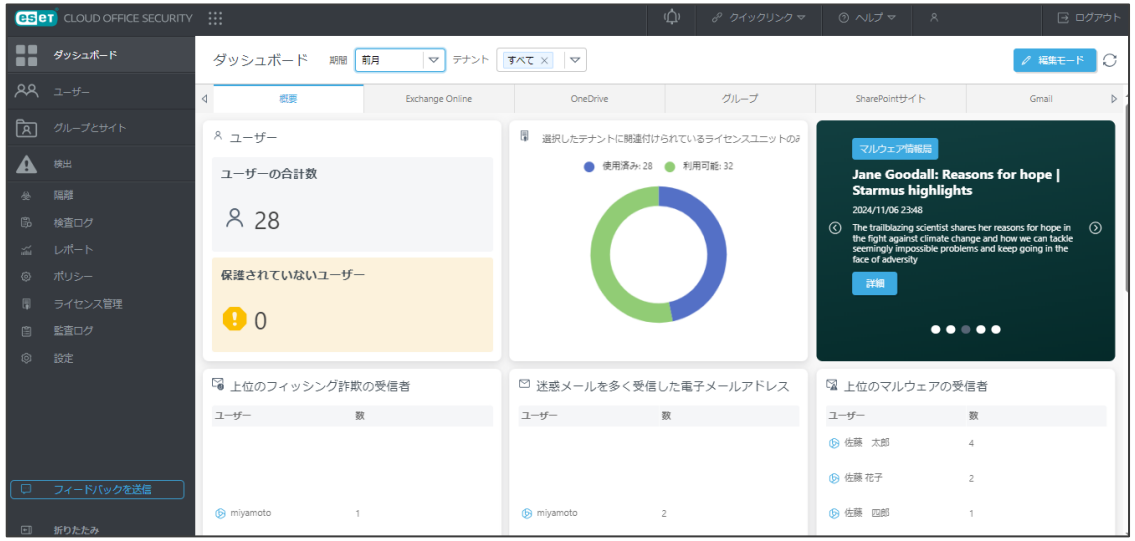
1. ESET Cloud Office Securityとは

1. ESET Cloud Office Securityとは

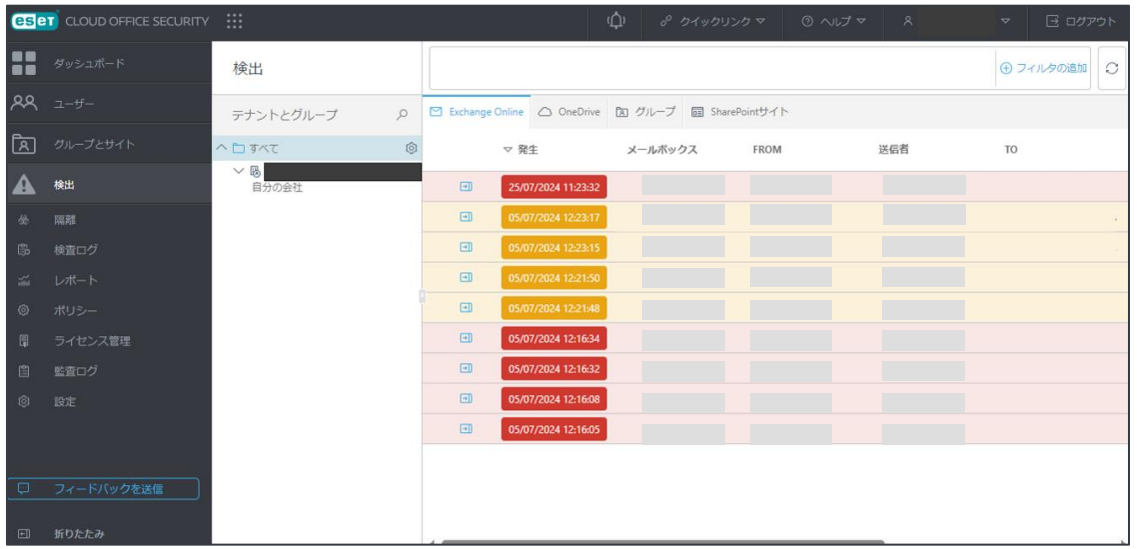
ECOSの概要

- ECOSはSaaS型のクラウドサービスとして、お客様がご利用のMicrosoft365またはGoogle Workspaceのサービスと連携させてすぐに保護を開始することができ、Webコンソールを介してどこからでも管理することができます。ECOSはマルウェア対策、スパムメール対策、フィッシング対策の組み合わせにより、企業の通信とクラウドストレージを保護します。また、ECOSは検出したメールやファイルの確認だけではなく、検出が発生するとすぐに管理者に通知することができます。

■Webコンソール画面例(ダッシュボード)



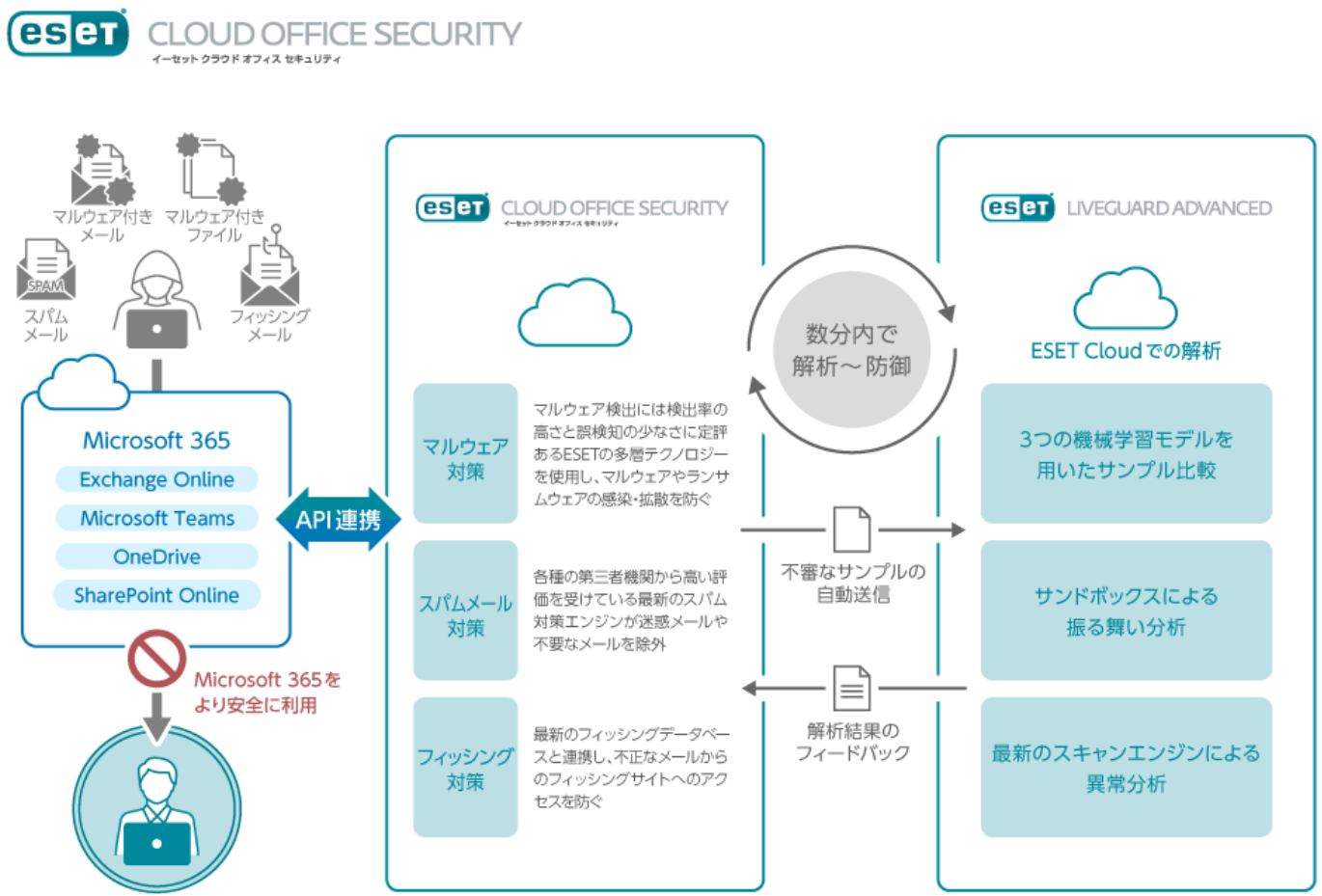
■Webコンソール画面例(検出)



©Canon Marketing Japan Inc.

1. ESET Cloud Office Securityとは

ECOSの構成



※上図ではMicrosoft365の例となっておりますがGoogle Workspaceにも対応しております。

- **導入が簡単**
  - SaaS型のクラウドサービスであるため、お客様環境でのサーバ構築が不要
  - Microsoft 365/Google WorkspaceとAPI連携を行うため、お客様のサービスに影響を与えることなく利用可能
  - API連携型のサービスであるため、お客様環境のMXレコードやDNSの書き換えが不要
  - ポリシー設定を行うだけで、 ESET LiveGuard Advanced(クラウドサンドボックス)が利用可能
- **運用が容易**
  - Microsoft 365/Google Workspaceからユーザ、グループ情報を自動で取得するため、ECOSで追加作業が不要
  - ECOSの保護を有効とする対象を絞ることができるため、テスト導入などのスモールスタートが可能
  - ESETが管理するクラウドサービスであるため、お客様によるECOSのバージョンアップが不要

©Canon Marketing Japan Inc.

1. ESET Cloud Office Securityとは

ECOSの主な機能(1)

機能	説明
Exchange Online/Gmailに対する保護機能	
- マルウェア対策	メールと添付ファイルのチェックを実施し脅威を排除
- 迷惑メール対策	最先端の迷惑メール対策エンジンを使用し、高検出率で迷惑メールおよびフィッシングの試みを防止
- フィッシング対策	電子メールメッセージの本文と件名を検索し、フィッシングWebページにつながるリンクをチェック
OneDrive/Google Driveに対する保護機能	
- マルウェア対策	OneDrive/Google Driveに作成/変更されたファイルのチェックを実施し脅威を排除
SharePointサイトに対する保護機能	
- マルウェア対策	SharePointサイトに作成/変更されたファイルのチェックを実施し脅威を排除
グループに対する保護機能	
- マルウェア対策	グループに作成/変更されたファイルのチェックを実施し脅威を排除

※ECOSのマルウェア対策ではESETのクライアント用プログラムと同等の検出技術を使用しています。

©Canon Marketing Japan Inc.

1. ESET Cloud Office Securityとは

ECOSの主な機能(2)

機能	説明
管理コンソール	Webコンソールでユーザーやログなどの管理が可能
マルチテナント	1つのECOSから複数のMicrosoft 365テナント、Google Workspaceテナントを保護および管理が可能
ポリシー	選択したテナント、ユーザー、グループ、またはSharePointサイトにポリシーベースの保護設定の割り当てが可能
ダッシュボードと検出統計情報	検出状況などの概要を表示
フィルタリングオプションを使用した検索	特定の検出に関する追加情報(侵入、ファイルハッシュなどの名前など)を使用して、探している情報をフィルタリングし、効果的に検索が可能
ユーザー管理	ユーザー毎に保護の実施設定や適用するポリシーの選択が可能
機械学習保護	Endpointに搭載されている高度な機械学習が、高度な保護レイヤーとして検出エンジンに追加
ESET LiveGuard Advancedによる保護	クラウドサンドボックスであるESET LiveGuard Advancedを使用した検査を行い、その検査結果は挙動分析レポートとして確認が可能
レポート	ECOSでの保護の統計データを、PDF形式またはCSV形式でレポートを生成しダウンロード、さらに指定した時刻に電子メールでレポートの受信が可能

©Canon Marketing Japan Inc.

1. ESET Cloud Office Securityとは

動作要件とサポートブラウザ

- **動作要件**
  - サポートされているMicrosoft 365サブスクリプションプラン
  - Azure Active Directory への管理者アクセス
  - Azure Cloud Service (Exchange Online / OneDrive / SharePoint / Teamsのいずれかまたはすべてのサービス)
  - EBAまたはEPHポータルアカウント(※)

※ESET社が提供するライセンス管理を行うWebシステムです。ECOSのサービス開始やログインに使用します。

- **サポートブラウザ**
  - Microsoft Edge 44以降
  - Google Chrome 77以降
  - Mozilla Firefox 69以降
  - Opera 63以降
  - Safari (13.x以降)

※Microsoft Internet Explorerはサポートされていません。

©Canon Marketing Japan Inc.

1. ESET Cloud Office Securityとは

利用可能なMicrosoft 365プラン

- 以下のMicrosoft 365サブスクリプションプランが利用可能です。

プラン名	
Microsoft 365 enterpriseプラン	•Microsoft 365 Apps for enterprise •Microsoft 365 E3 / E5 / F3 •Office 365 E1 / E3 / E5 / F3
Microsoft 365 businessプラン	•Microsoft 365 Business Basic •Microsoft 365 Business Standard •Microsoft 365 Business Premium •Microsoft 365 Apps
Microsoft 365 Educationプラン	•Microsoft 365 A3 •Microsoft 365 A5
Exchange Onlineプラン	•Exchange Online (Plan 1) (Plan 2) •Microsoft 365 Business Standard
OneDriveプラン	•OneDrive for Business (Plan 1)（Plan 2) •Microsoft 365 Business Basic •Microsoft 365 Business Standard

©Canon Marketing Japan Inc.

2. Webコンソールの紹介

2. Webコンソールの画面ご紹介

Webコンソールの画面構成：概要

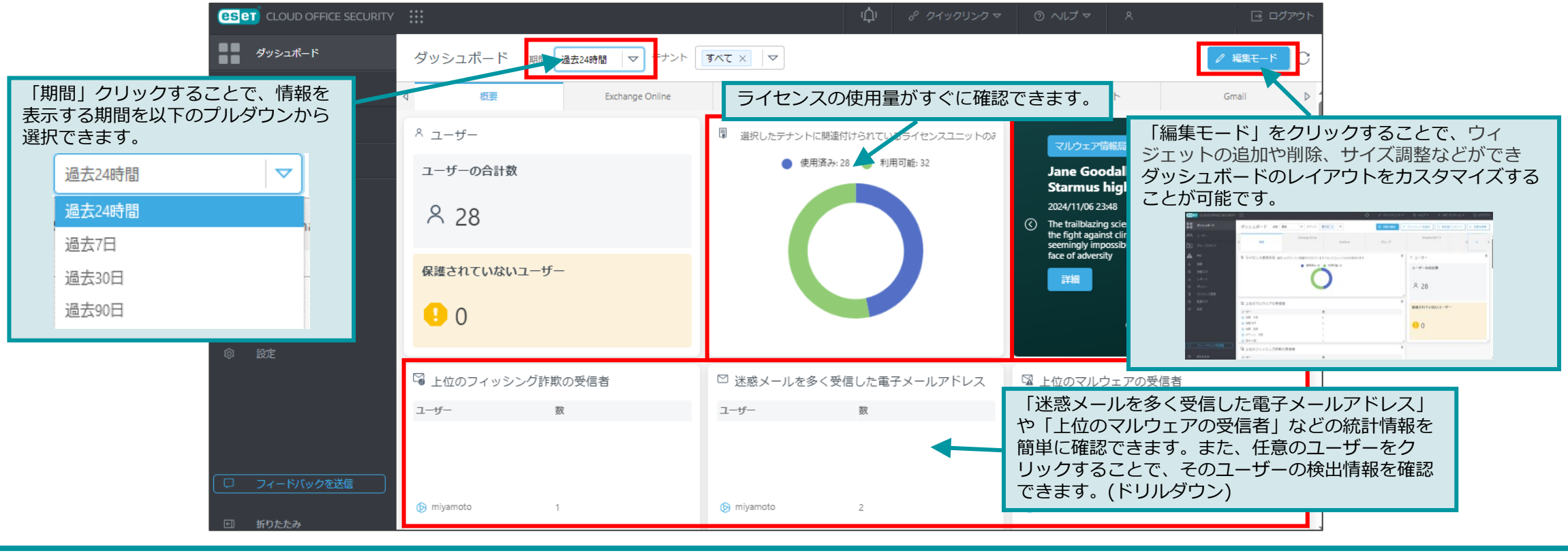
- Webコンソールにログインすると以下の画面が表示されます。画面左のメインメニューより、各種メニューを選択することで、ダッシュボードやユーザーの閲覧、各種設定、管理機能を使用することができます。

©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

ダッシュボード：(1)概要

- ダッシュボードはECOSにログインするとはじめに表示される画面です。
  「概要」では、ユーザーやテナントの合計数やライセンス使用状況、迷惑メールを多く受信した電子メールアドレスなどが確認できます。



©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

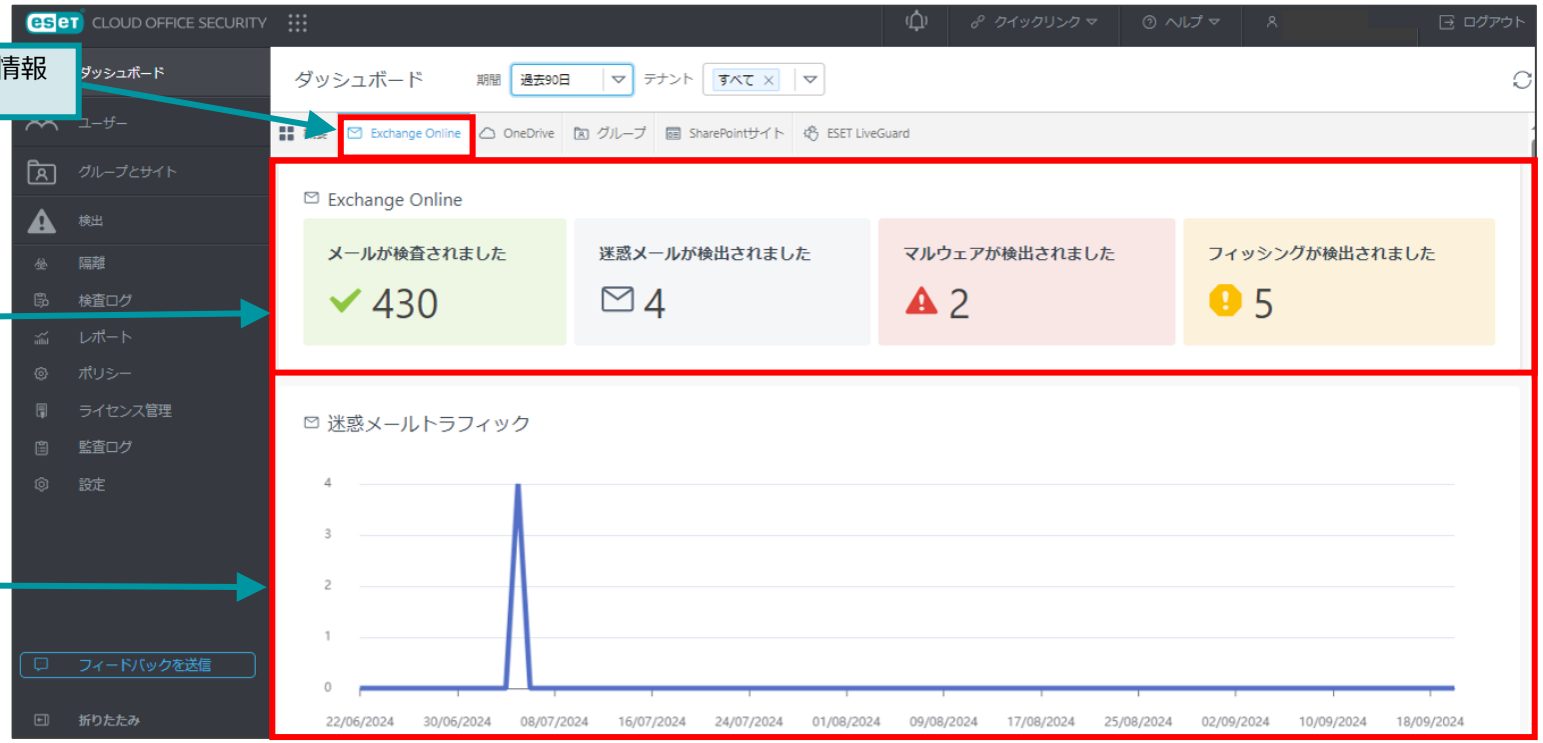
ダッシュボード：(2)Exchange Onlineタブ(例)

- 「Exchange Online」では、検出されたマルウェア数や迷惑メール数などが確認できます。上部のタブを切り替えることで「OneDrive」「グループ」「SharePointサイト」「ESET LiveGuard」での検出数も確認可能です。

上部タブを切り替えると各サービスでのステータス統計情報が確認できます。

検査済み電子メールの総数と、検出が確認されたメールの内訳を表示します。

時間ごとの検出数がグラフで表示されます。 タブを切り替えた「OneDrive」「グループ」「SharePointサイト」でも同様のグラフで表示されます。



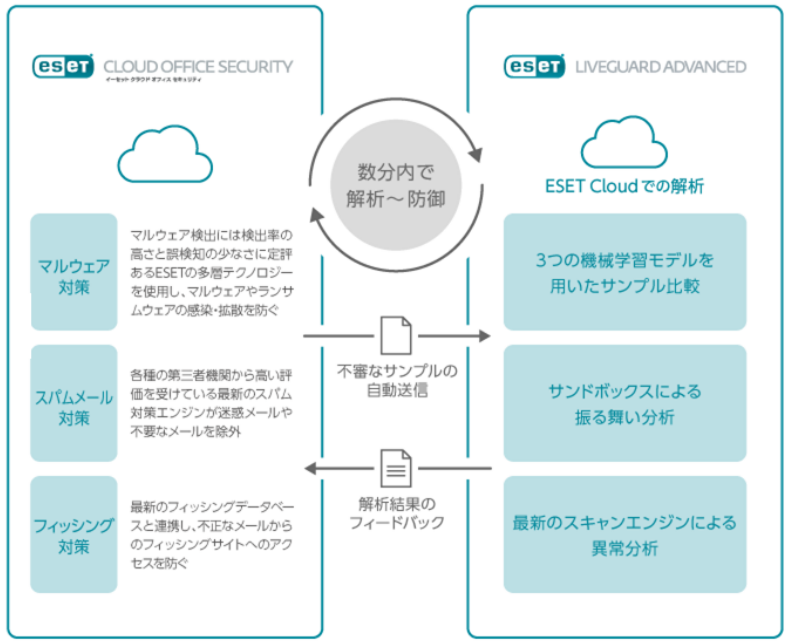
©Canon Marketing Japan Inc.

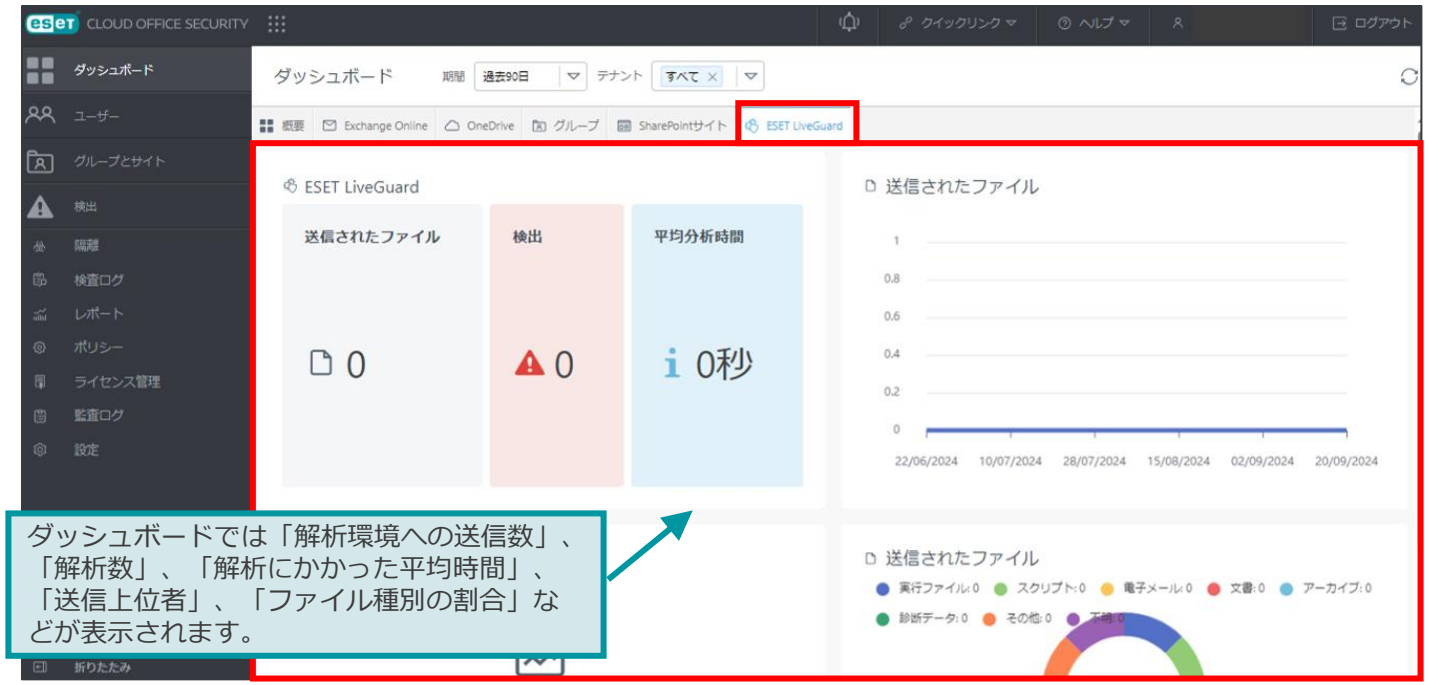
2. Webコンソールの画面ご紹介

ダッシュボード：(3) ESET LiveGuard Advancedタブ(例)

- ECOSでは、クラウドサンドボックスであるESET LiveGuard Advancedと連携し詳細な検査が可能です。これにより、ECOSで発見された不審なサンプルは自動でESETのクラウドサンドボックスへ送信されて分析されます。また、本機能による検査結果はレポートにて確認が可能です。

■ECOSとELGAの連携イメージ





2. Webコンソールの画面ご紹介

ユーザー：(1)一覧画面

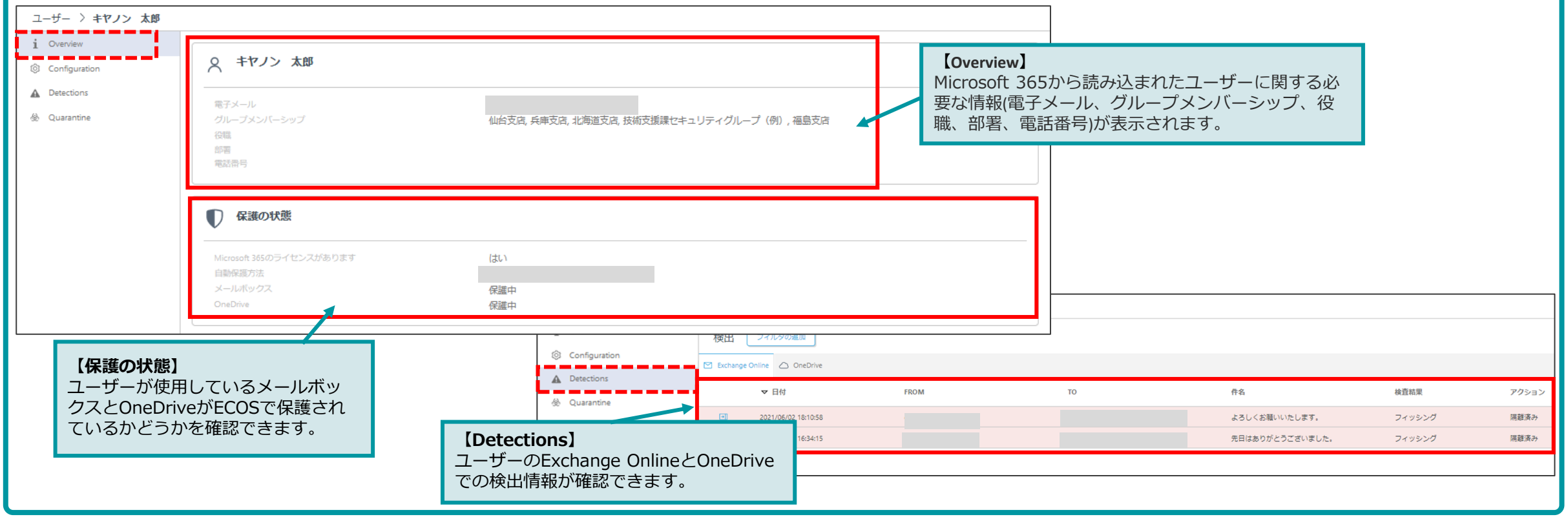
- ECOSが保護する中心的なエンティティはユーザーアカウントです。ユーザーの詳細情報の確認だけではなく、どのユーザーを保護するか、または保護解除するかも選択できます。

©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

ユーザー：(2)詳細画面

- 任意のユーザーを選択することで、概要、ポリシーによって定義された設定、ユーザーに割り当てられたポリシーのリスト、Exchange Online/Gmail、OneDrive/Google Driveでの検出などの情報を確認することができます。

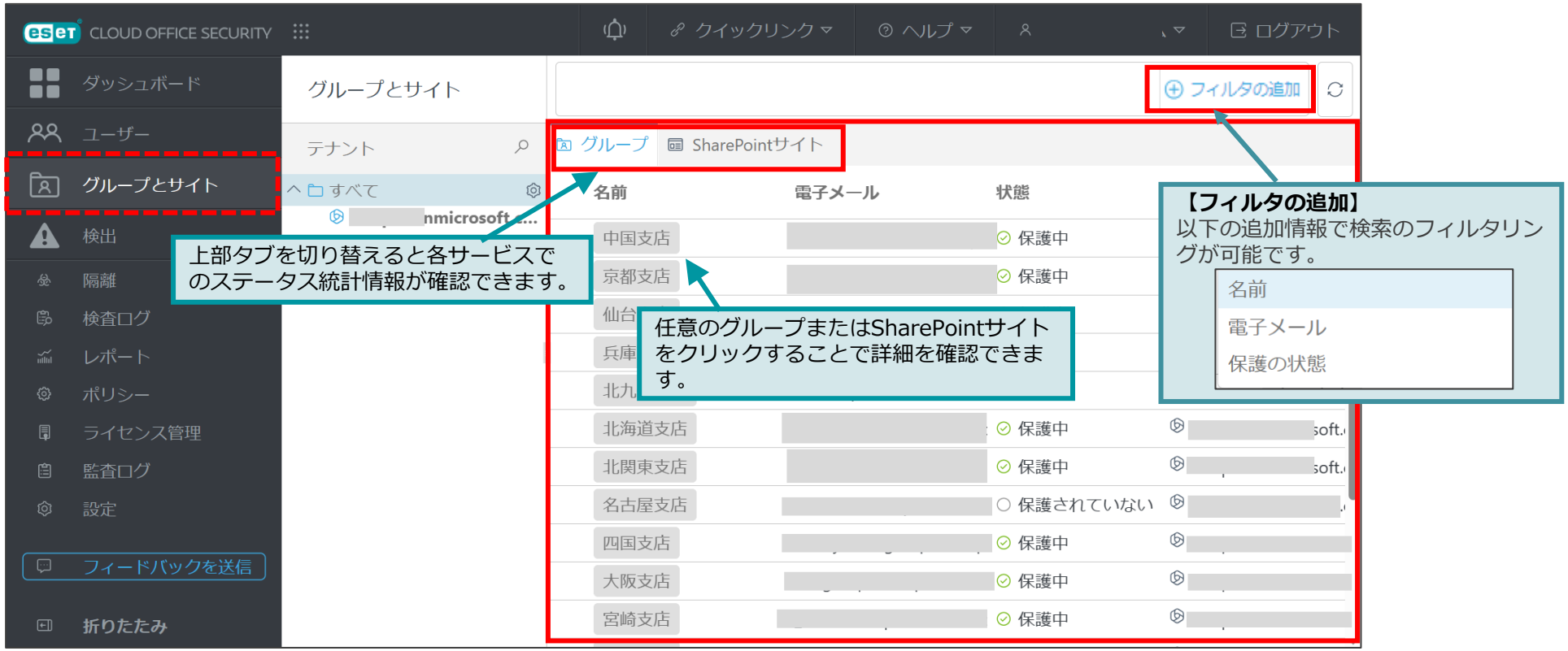


©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

グループとサイト：(1)一覧画面

- 各テナントのグループまたはSharePointサイトの一覧が表示されます。グループを保護するには、1つ以上のメンバーがECOSで保護されたユーザーであることを確認してください。SharePointサイトは、サブサイトを含め自動的に保護されます。



©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

グループとサイト：(2)詳細画面

- 詳細画面では、TeamsグループまたはSharePointサイトの概要、割り当てられたポリシーやその内容の確認、検出や隔離情報をそれぞれ確認することができます。

■Teamsグループの概要

【Overview】
Microsoft 365から読み込まれたTeamsグループまたはSharePointサイトに関する必要な情報(電子メール、所有者、メンバー、作成者、URLなど)が表示されます。

■SharePointサイトの概要(一部抜粋)

【保護の状態】
TeamsグループとSharePointサイトがECOSで保護されているかどうかを確認できます。

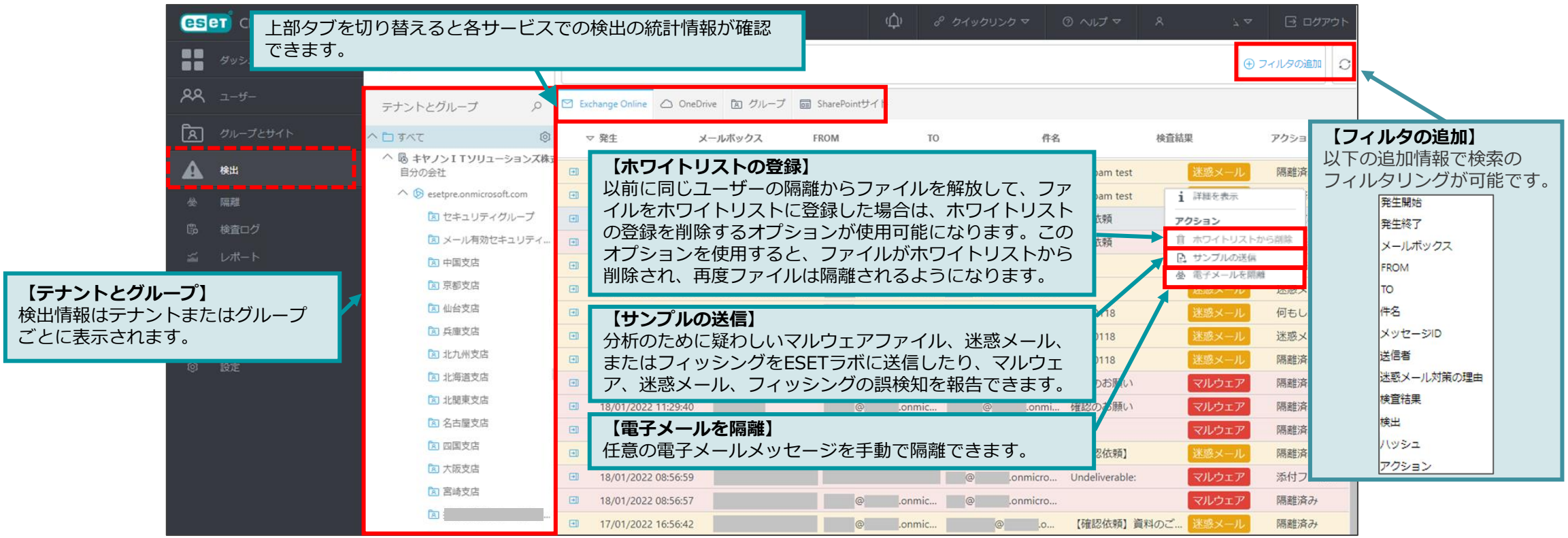
【Detections】
TeamsグループまたはSharePointサイトでの検出情報が確認できます。

©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

検出：(1)一覧画面

- ECOSによるすべての検出の一覧が表示されます。
  タブを使用して、Exchange Online/Gmail、OneDrive/Google Drive、グループ、およびSharePointサイトを切り替えます。各検出に関する重要な情報が表示されます。



©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

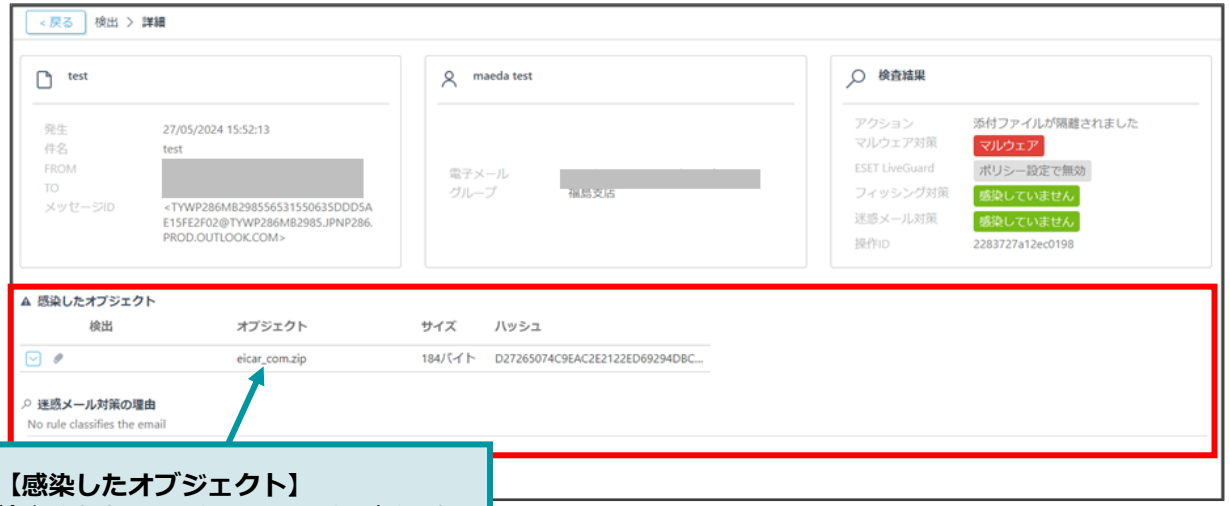
検出：(2)詳細画面

- 検出の詳細画面では、検出された電子メールやファイルの概要、検出されたサイトやグループ情報、検査結果が表示されます。

■検出(迷惑メールが検出された場合)の詳細画面

【迷惑メール対策の理由】
検出された迷惑メールの理由が表示されます。
※本資料ではGTUBE(迷惑メールのテスト用ストリング)が検出されています。

■検出(マルウェアが検出された場合)の詳細画面



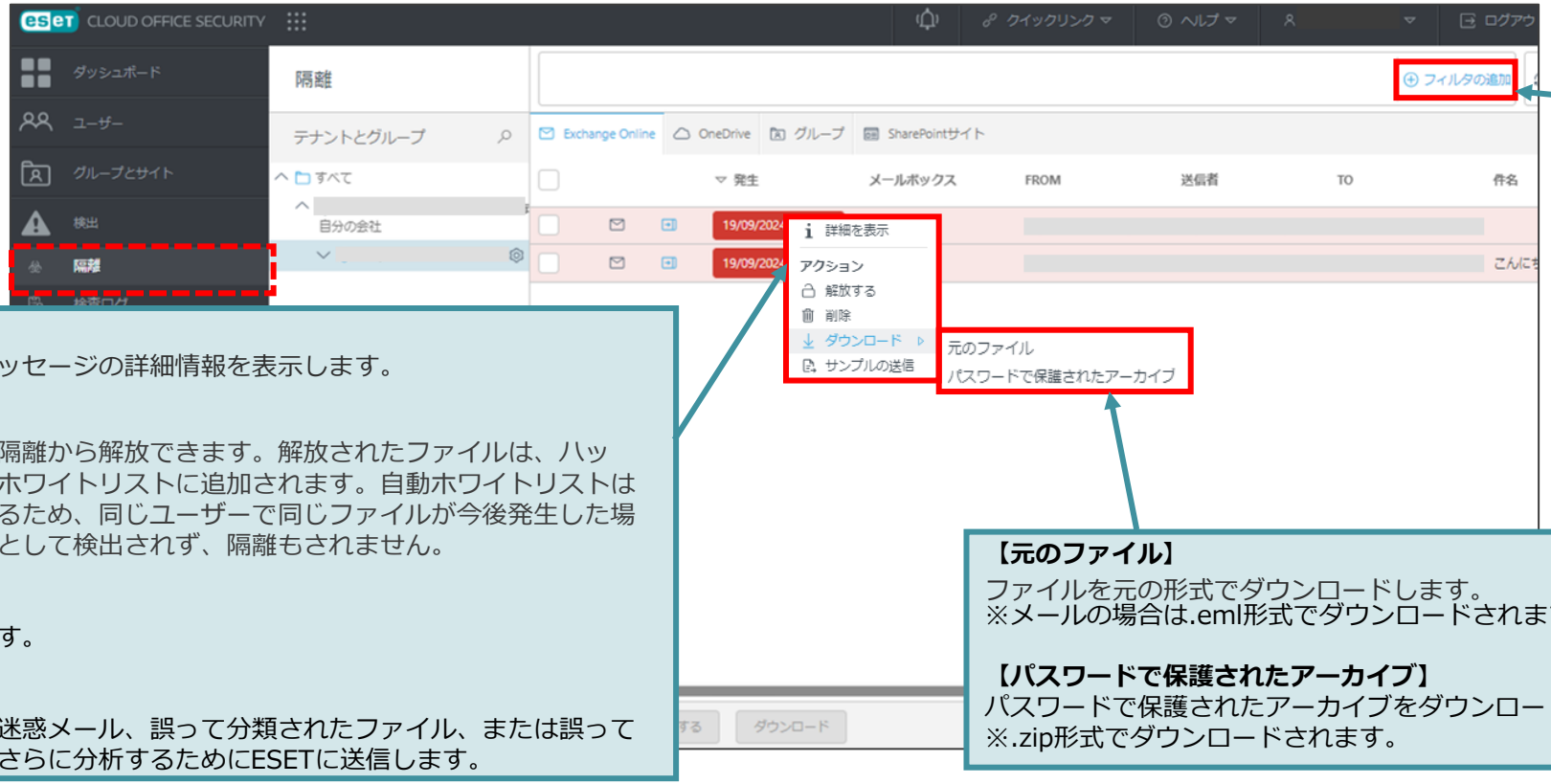
【感染したオブジェクト】
検出されたファイルのファイル名やサイズ、ハッシュの情報が確認できます。

©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

隔離：(1)一覧画面

- ECOSによって隔離された電子メールとファイルを管理できます。
  タブを使用して、Exchange Online/Gmail、OneDrive/Google Drive、グループ、およびSharePoint サイトを切り替えて表示します。



【詳細を表示】
隔離された電子メールメッセージの詳細情報を表示します。

【解放する】
誤検出されたファイルを隔離から解放できます。解放されたファイルは、ハッシュに基づいて自動的にホワイトリストに追加されます。自動ホワイトリストはユーザーごとに実行されるため、同じユーザーで同じファイルが今後発生した場合、一切不審なファイルとして検出されず、隔離もされません。

【削除】
項目を隔離から削除します。

【サンプルの送信】
不審なファイル、不審な迷惑メール、誤って分類されたファイル、または誤って分類された迷惑メールをさらに分析するためにESETに送信します。

【フィルタの追加】
以下の追加情報で検索のフィルタリングが可能です。

- 発生開始
- 発生終了
- メールボックス
- FROM
- TO
- 件名
- メッセージID
- 送信者
- 迷惑メール対策の理由
- 検査結果

【元のファイル】
ファイルを元の形式でダウンロードします。
※メールの場合は.eml形式でダウンロードされます。

【パスワードで保護されたアーカイブ】
パスワードで保護されたアーカイブをダウンロードします。
※.zip形式でダウンロードされます。

©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

隔離：(2)詳細画面

- 隔離の詳細画面では、隔離された電子メールやファイルの概要、検出されたサイトやグループ情報、検査結果が表示されます。また、隔離された電子メールのヘッダーが確認可能です。

■隔離(マルウェアが隔離された場合)の詳細画面

■隔離(フィッシングメールが隔離された場合)の詳細画面

【ヘッダー】
隔離されたメールのヘッダー情報が確認できます。

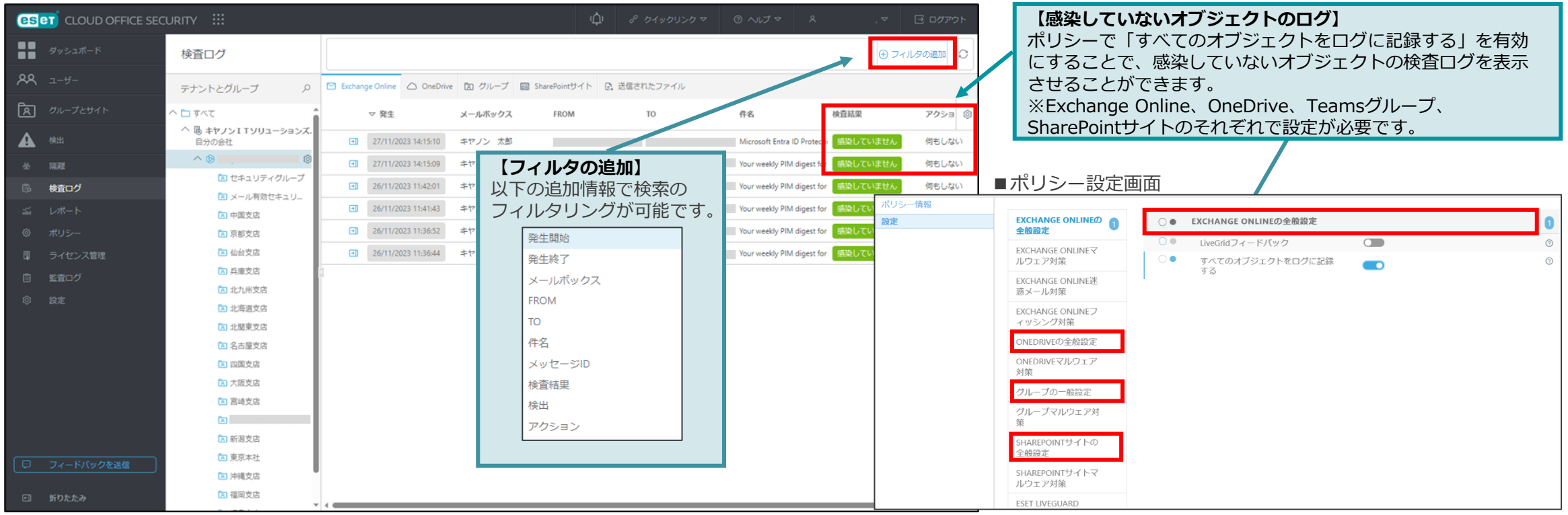
【フィッシングリンク】
フィッシングメール内で確認されたフィッシングのリンク情報が確認できます。

©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

検査ログ：一覧画面と詳細画面

- ECOSによるすべての検査結果を一覧表示します。ログは検出と似ていますが、感染していないオブジェクトのログも含まれます。感染していないオブジェクトのログを表示させるには、ポリシーで「すべてのオブジェクトをログに記録する」を有効にする必要があります。

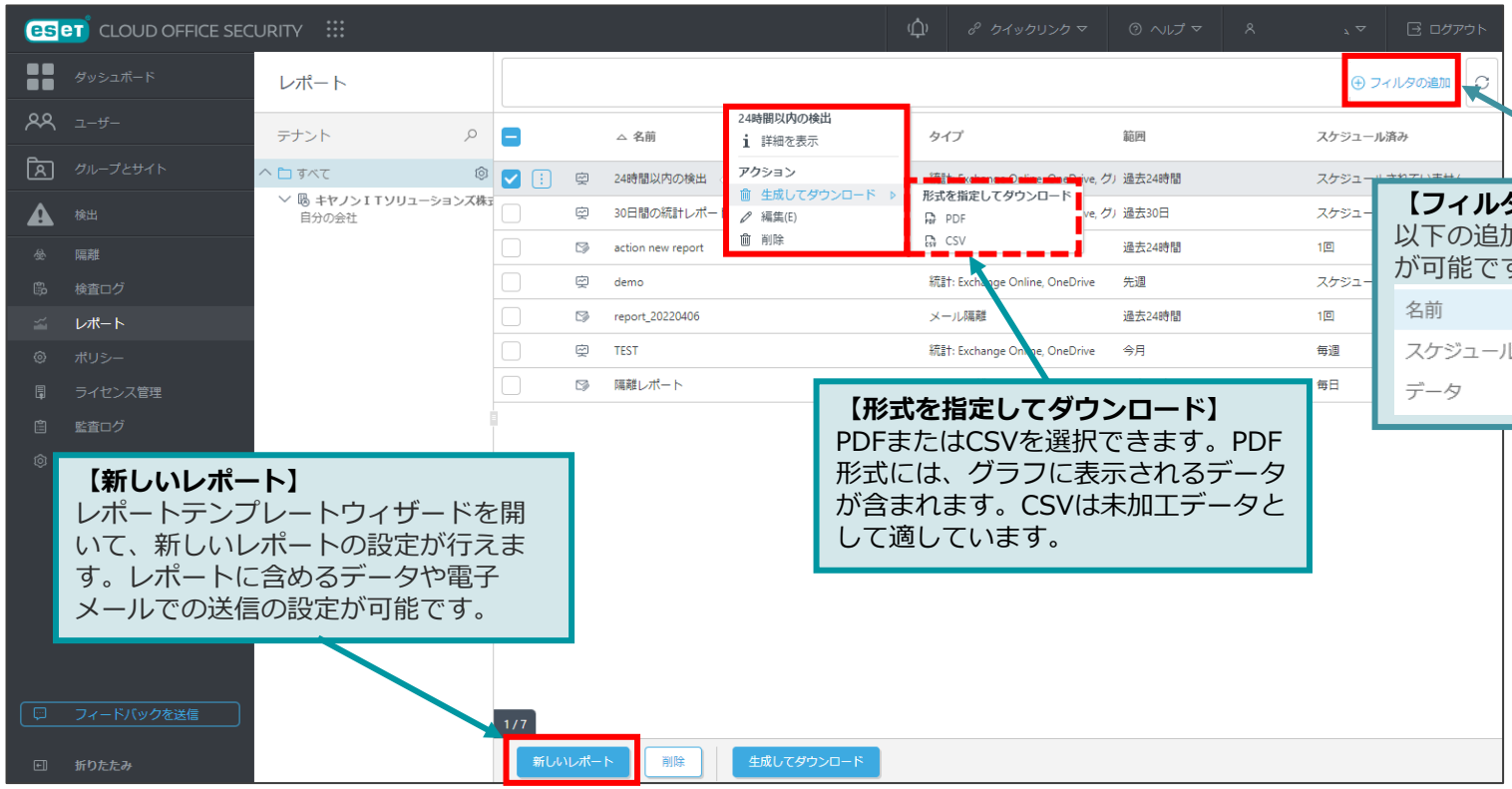


©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

レポート：(1)一覧画面

- レポートでは、ECOSの保護統計の情報が表示されます。
  Exchange Online/GmailおよびOneDrive/Google Drive保護の統計情報には、指定した期間の検査された電子メール、ファイル、検出されたマルウェア、フィッシング、および迷惑メールの数が表示されます。

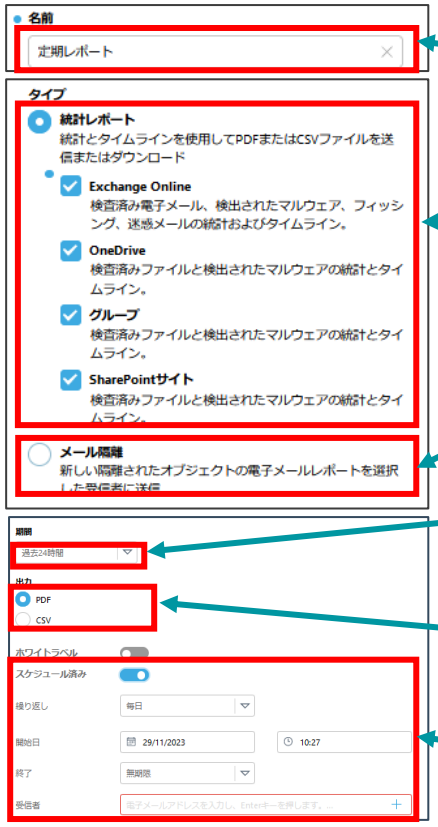


©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

レポート：(2)編集画面とレポート例)

- ECOSでは電子メールでレポートを送信することが可能なため、毎回Webコンソールにログインする必要はありません。レポートを繰り返し電子メールで送信するようにスケジュールし、電子メール受信者の指定を行います。



【名前】
任意のレポート名を設定します。「説明」の入力は任意です。

【タイプ】
ECOSで保護されているサービスを選択して、検査された電子メール、ファイル、検出されたマルウェア、フィッシング、および迷惑メールの統計とタイムラインを生成します。

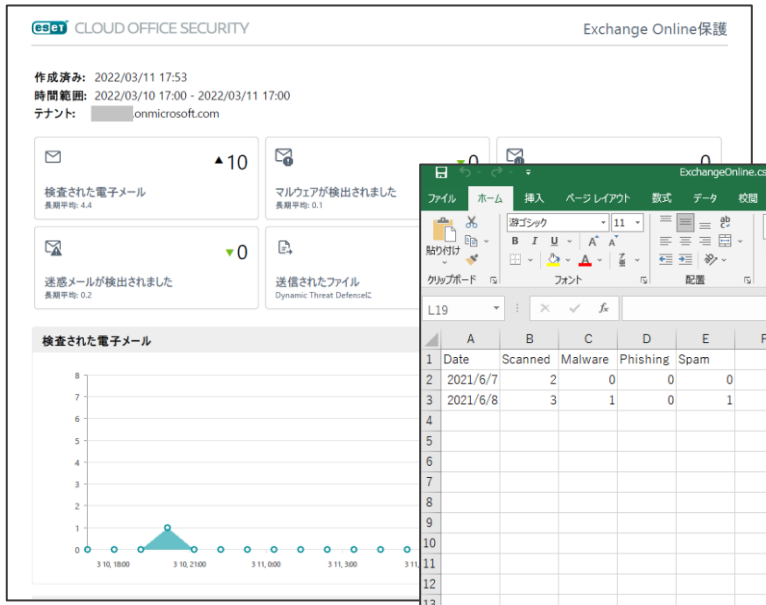
【メール隔離レポート】
新しく隔離されたオブジェクトの電子メールレポートを選択した受信者に送信する。

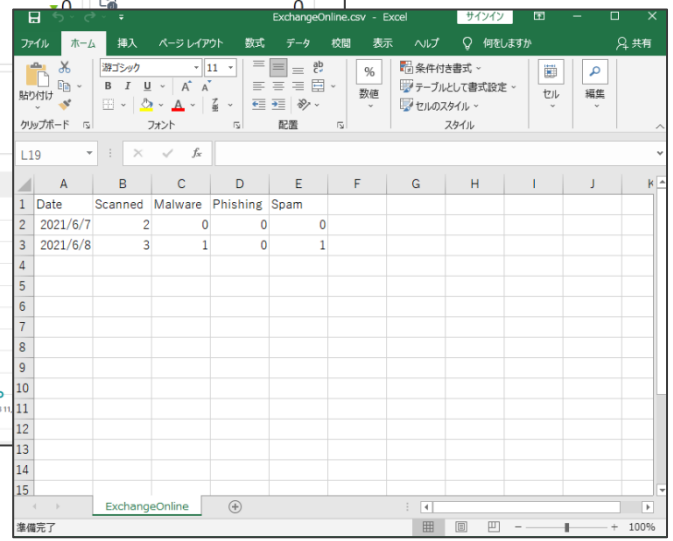
【期間】
結果を表示する期間を定義します(過去24時間、週、月)。カスタムを選択する場合、範囲(開始日と終了日)を指定できます。

【出力】
適切なファイル形式を選択し、PDFまたはCSVを選択できます。

【スケジュール済み】
指定された日時にレポートを生成し、指定した受信者に定期的に配信されます。

■PDF出力した場合のレポート例





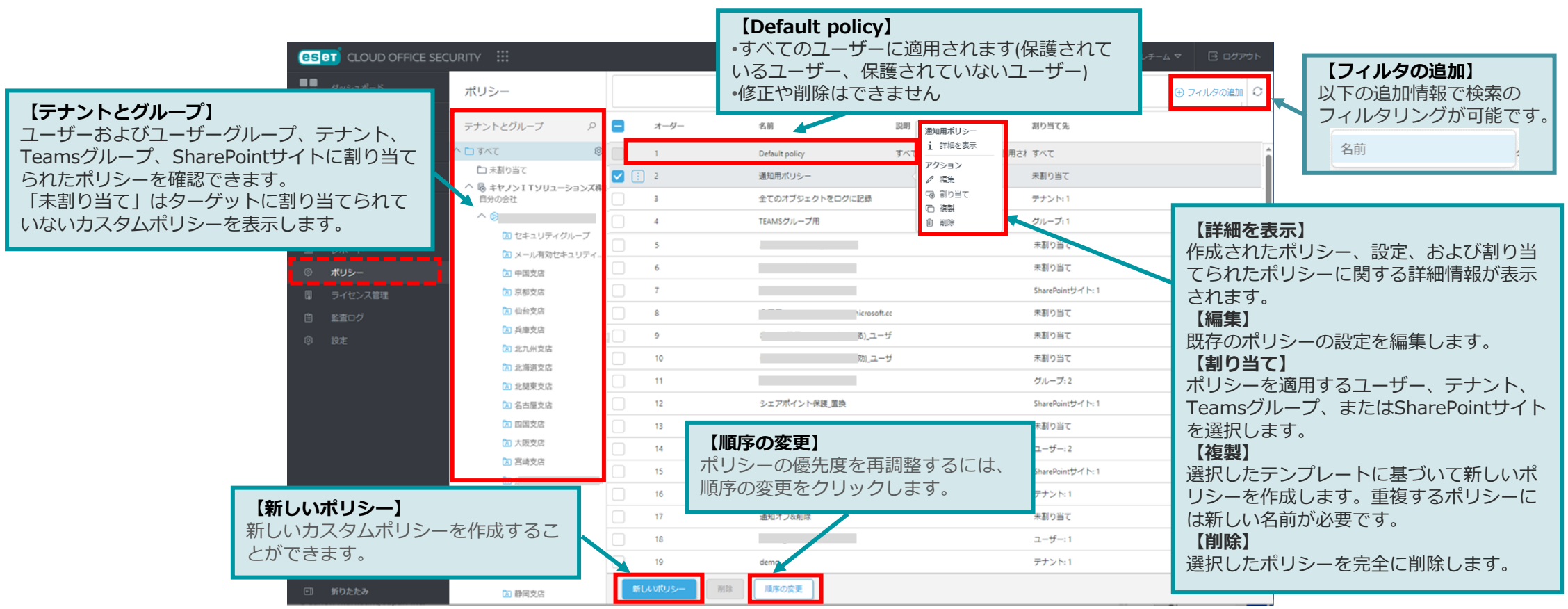
■CSV出力した場合のレポート例

©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

ポリシー：(1)一覧画面

- ECOSはポリシーを使用して保護を行います。必要に応じて保護設定をカスタマイズし、選択したユーザーおよびグループ、テナント、グループ、SharePointサイトに割り当てることができます。

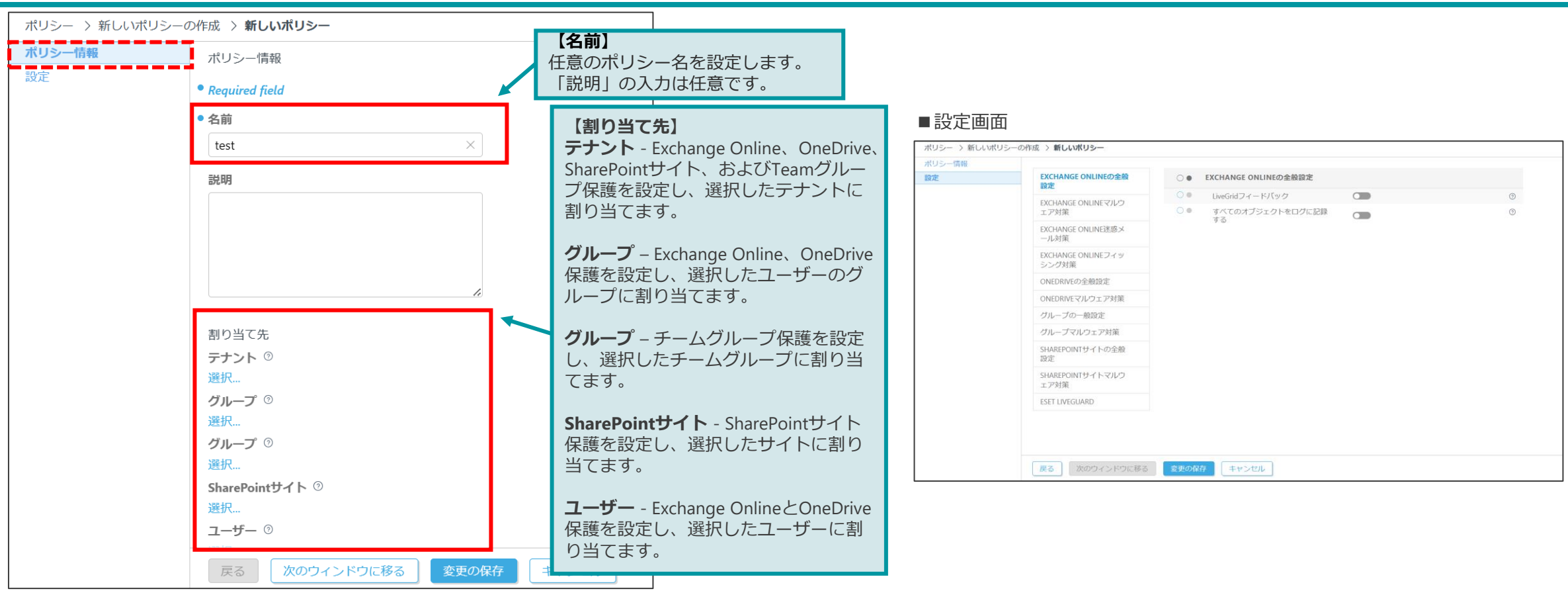


©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

ポリシー：(2)説明画面

- 説明画面では、作成するポリシーの名前やポリシー設定を行うターゲットを設定することができます。
  ターゲットの内容に合わせて設定できる項目が変わります。

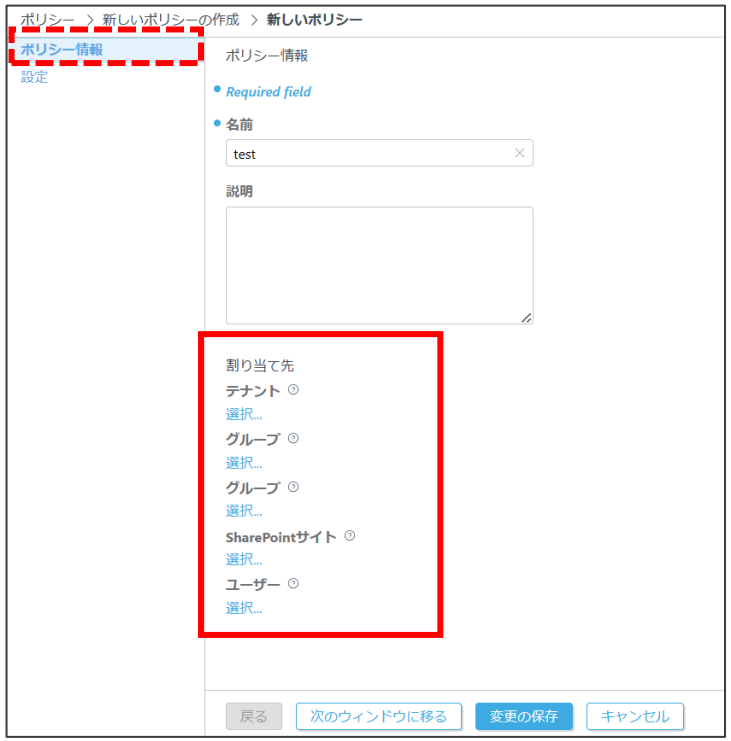


©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

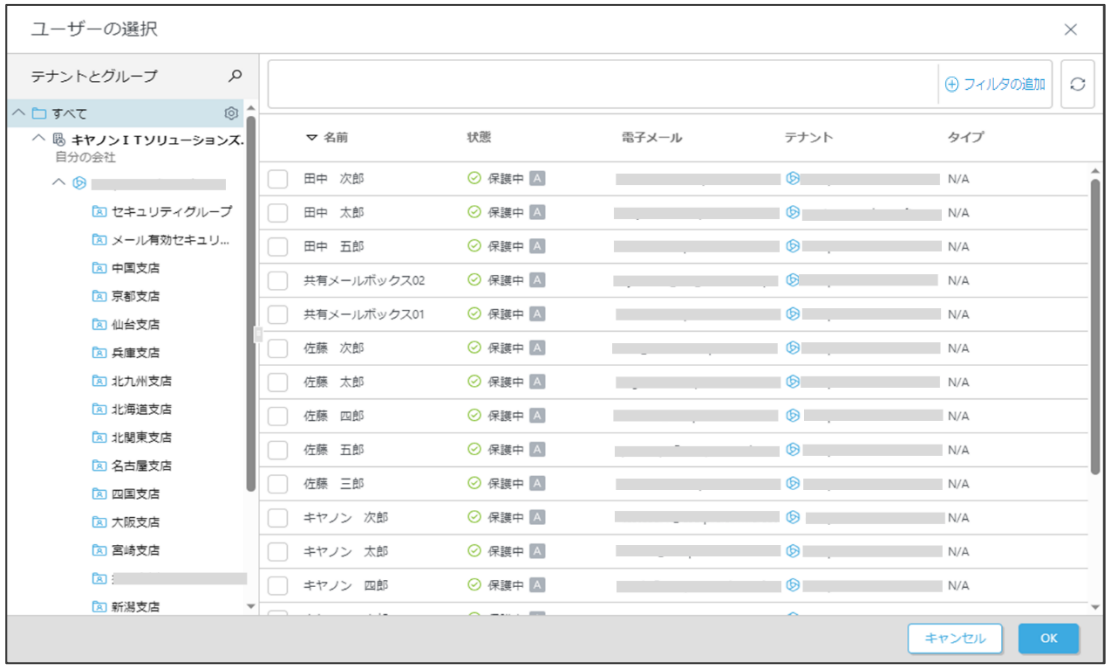
ポリシー：(3)割り当て先画面

- [割り当て先]から、ポリシーを割り当てるターゲットを選択します。[割り当て先]の設定により、ポリシーの割り当て先がユーザー、テナント、グループ、またはSharePointサイトと変わります。



※ユーザーとテナントは1つのカスタムポリシーにのみ割り当てることができます。

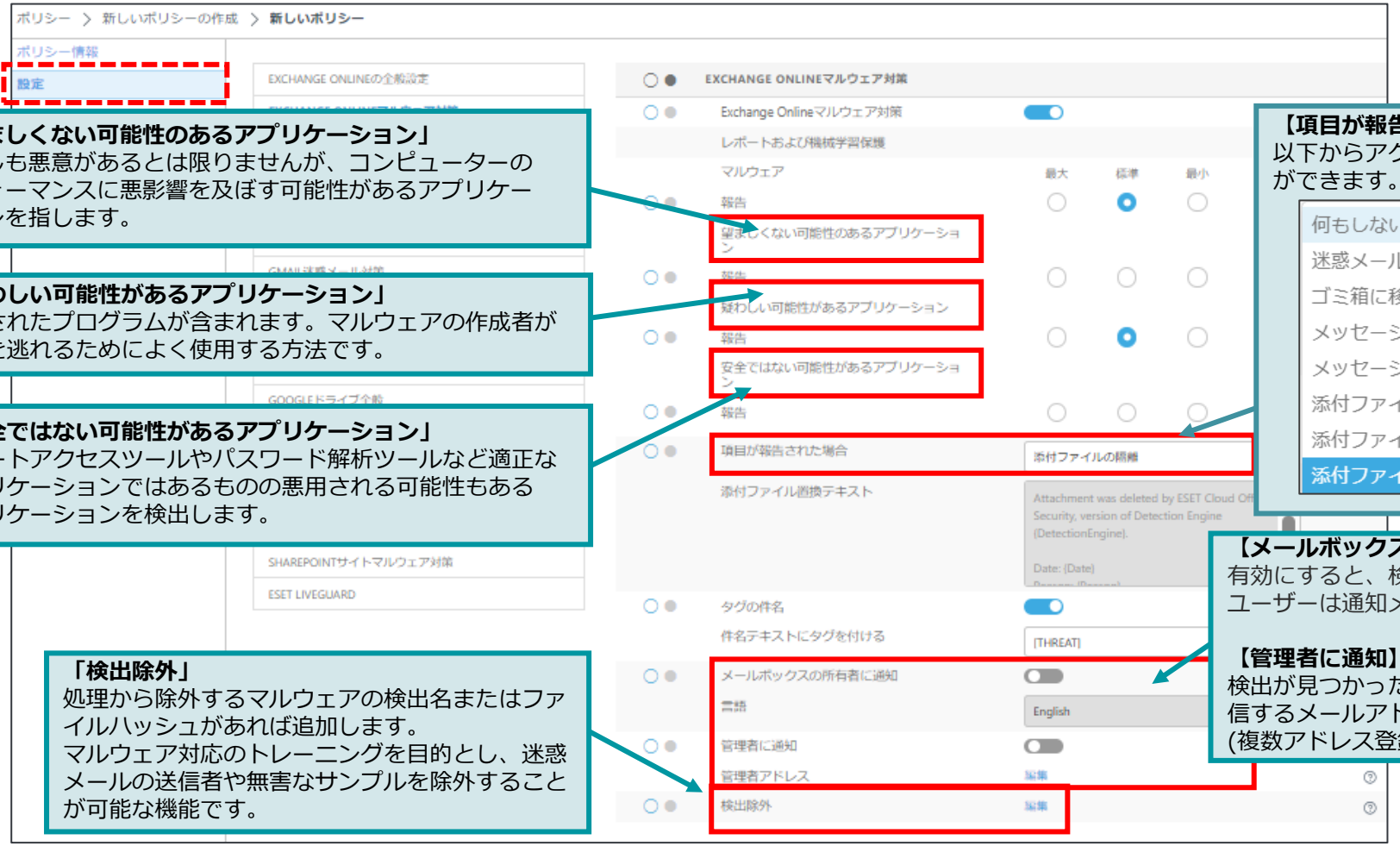
■割り当て先にユーザーを選択した場合の画面



©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

ポリシー：主な設定値の紹介①



「望ましくない可能性のあるアプリケーション」
必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーションを指します。

「疑わしい可能性があるアプリケーション」
圧縮されたプログラムが含まれます。マルウェアの作成者が検知を逃れるためによく使用する方法です。

「安全ではない可能性があるアプリケーション」
リモートアクセスツールやパスワード解析ツールなど適正なアプリケーションではあるものの悪用される可能性もあるアプリケーションを検出します。

「検出除外」
処理から除外するマルウェアの検出名またはファイルハッシュがあれば追加します。
マルウェア対応のトレーニングを目的とし、迷惑メールの送信者や無害なサンプルを除外することが可能な機能です。

【項目が報告された場合】
以下からアクションを選択することができます。

何もしない
迷惑メールに移動
ゴミ箱に移動
メッセージを削除
メッセージの隔離
添付ファイルを削除
添付ファイルの置換
添付ファイルの隔離

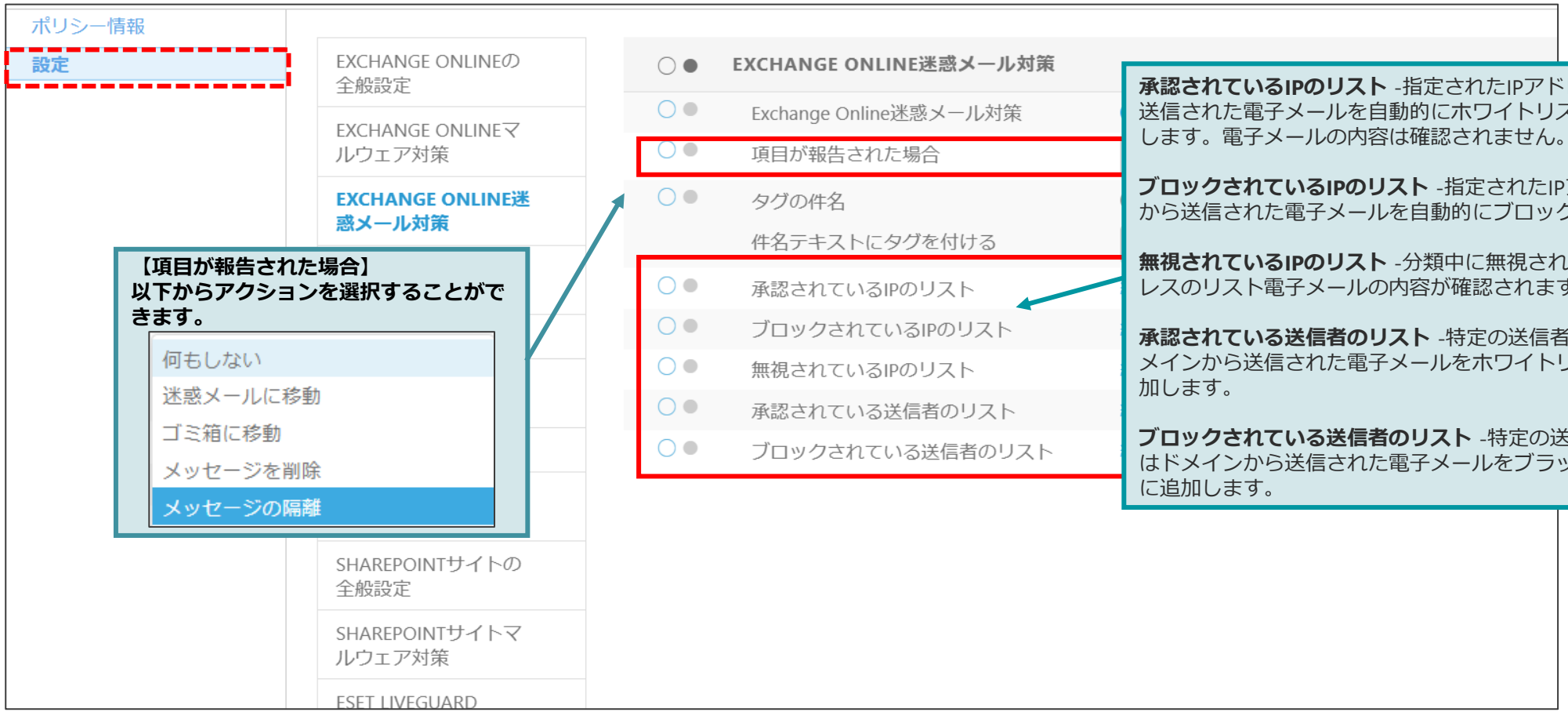
【メールボックスの所有者に通知】
有効にすると、検出が見つかったときに、ユーザーは通知メールを受信します。

【管理者に通知】
検出が見つかったときに通知メールを受信するメールアドレスを指定します。
(複数アドレス登録可能)

©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

ポリシー：主な設定値の紹介②



承認されているIPのリスト -指定されたIPアドレスから送信された電子メールを自動的にホワイトリストに追加します。電子メールの内容は確認されません。

ブロックされているIPのリスト -指定されたIPアドレスから送信された電子メールを自動的にブロックします

無視されているIPのリスト -分類中に無視されるIPアドレスのリスト電子メールの内容が確認されます。

承認されている送信者のリスト -特定の送信者またはドメインから送信された電子メールをホワイトリストに追加します。

ブロックされている送信者のリスト -特定の送信者またはドメインから送信された電子メールをブラックリストに追加します。

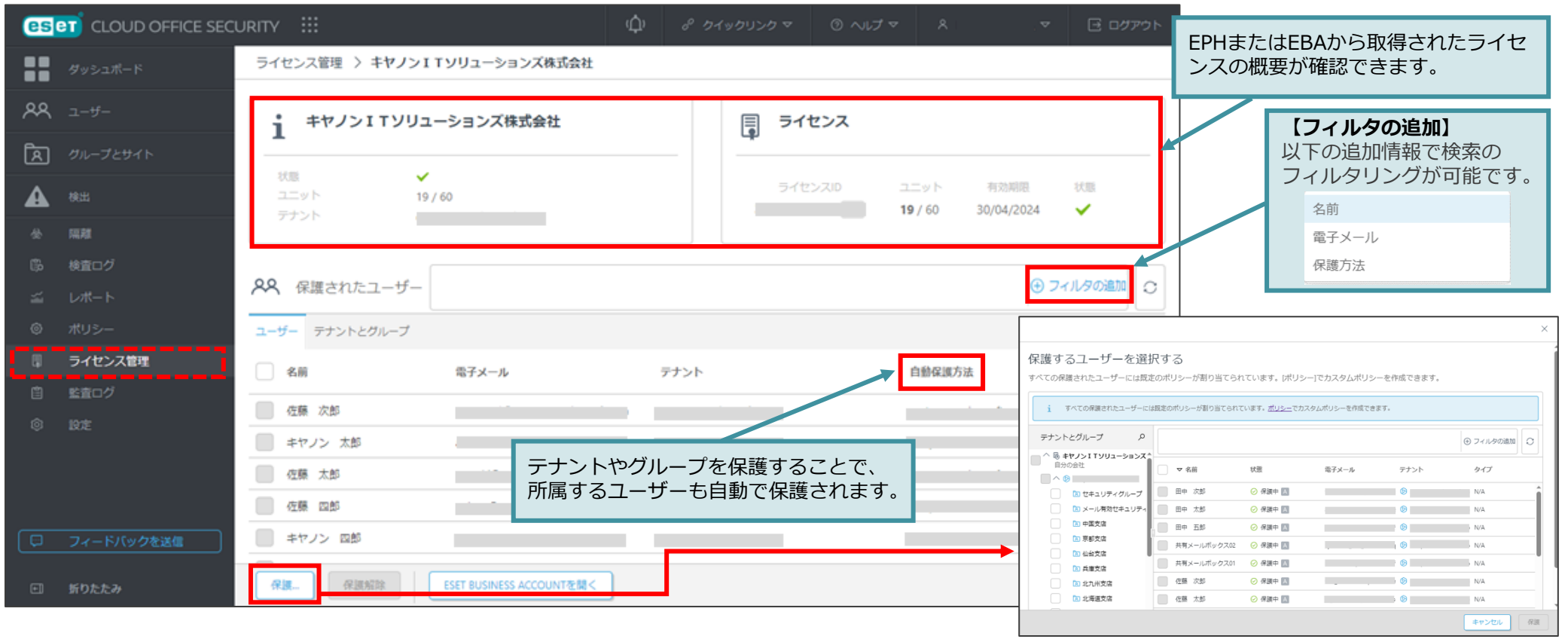
※OneDrive、Teamsグループ、SharePointサイトで設定可能なポリシーについては以下のURLをご確認ください。
https://help.eset.com/ecos/ja-JP/policies.html

©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

ライセンス管理

- ESET PROTECT HUBまたはESET Business Accountから取得されたライセンスの概要が表示されます。
  ライセンス管理では、ユーザーの保護または保護解除ができます。

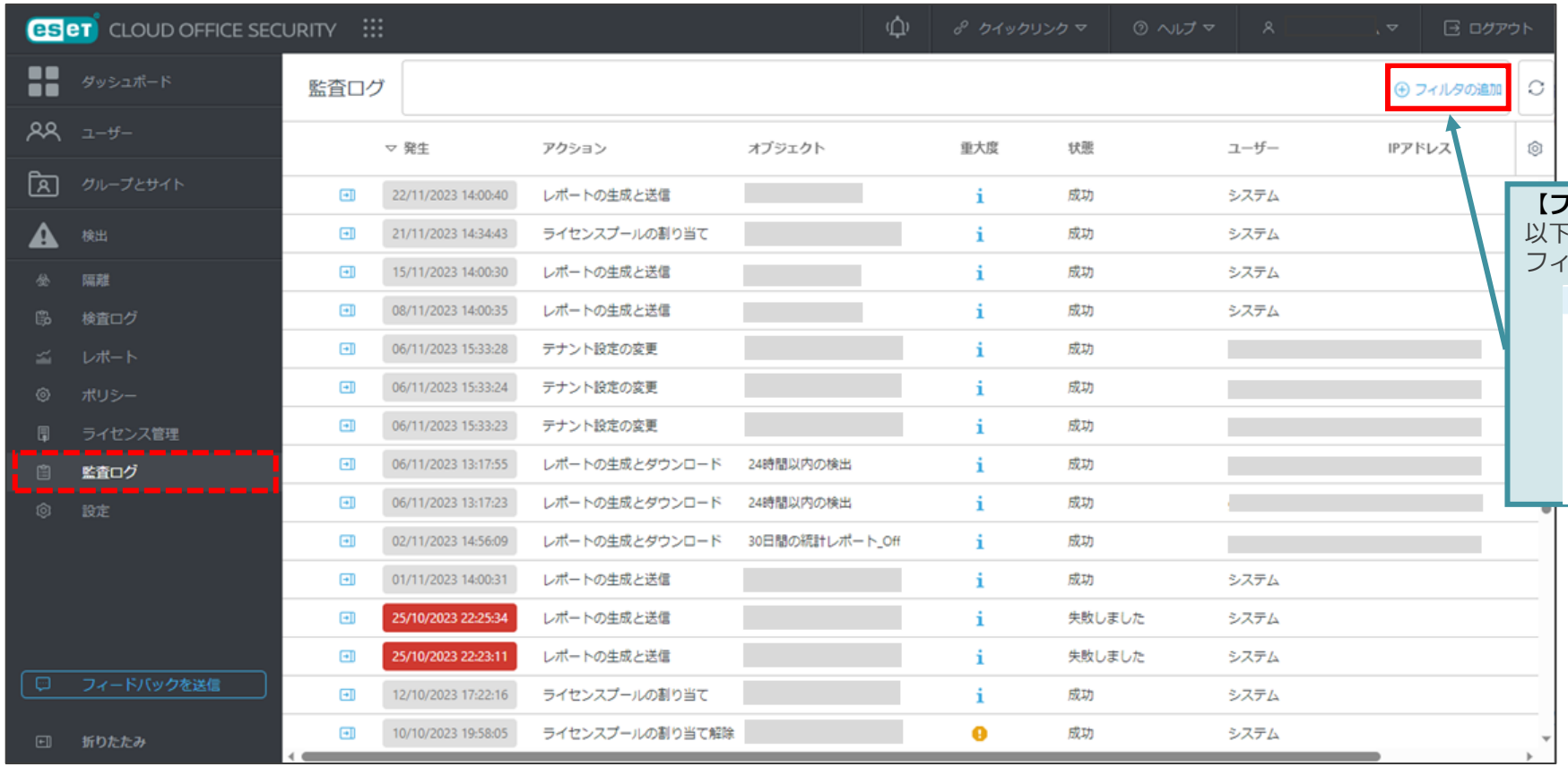


©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

監査ログ

- 監査ログでは、ログインユーザーが行った操作内容を確認することができます。また、「発生時刻」「アクション」「アクションの詳細」「重大度」「ユーザー名」などを確認することができます。



©Canon Marketing Japan Inc.

2. Webコンソールの画面ご紹介

設定：テナントの追加や削除

- 設定ではECOSに接続されたテナントを管理します。テナントの追加や削除を行うことができます。

©Canon Marketing Japan Inc.

3. 注意事項 / 制限事項

3. 注意事項 / 制限事項

各種データの保持期間

条件	データの保持期間
隔離されたオブジェクトの保有期間	30日間
[検出]に表示される情報レコードの保持期間	90日間
[ログ]に表示されるログレコードの保存期間	90日間 ※「すべてのオブジェクトをログに記録」ポリシーを使用している場合、検査結果の「感染していません」のログレコード保存期間は3日間となります。
テナントをECOSのWebコンソールから削除した場合	30日間 ※30日以内に再度テナントを追加する場合は、データ(ログ/ルール/検出)が復元されます。
EPHまたはEBAからECOSを削除した場合	30日間 ※この処理ではECOSがディアクティベーションされます。もう一度ECOSをアクティベーションする場合は、同じテナントを追加してすべてのデータを取得する必要があります。
ECOSライセンスが期限切れになった場合	保護は14日間継続されますが、それ以降は保護がオフになり、ECOSにログインできなくなります。また、30日以内にライセンスを更新しない場合、ECOSアカウントのすべてのデータが削除されます。

©Canon Marketing Japan Inc.

3. 注意事項 / 制限事項

ファイルが検査されない条件

- **以下の場合には、ファイルが検査されず「未検査」としてログに表示されます。**
  - ファイルサイズが200MBを超えている場合
  - 検査が2分以上かかりタイムアウトする場合
  - アーカイブファイルが10以上のネストレベル(階層)である場合
  - ファイルがパスワードで保護されている場合
  - ファイルが破損している場合

ファイルの隔離に関する制限

- **以下の場合には、隔離からファイルの解放(※)が行えません。**
  - １つの電子メール添付ファイルにつき15MB超えている場合
  - 添付ファイルを含む電子メッセージ全体で150MB超えている場合

※隔離から元のメッセージを添付ファイルとして、通知メールの形式で電子メールで元の受信者にリリースします。OneDriveアイテムの場合、ファイルはユーザーのOneDriveの元の場所にアップロードされます。TeamsグループまたはSharePointサイトからファイルをリリースするときは、ファイルは元の場所に戻って表示されます。リリースされたファイルは、ハッシュに基づいて自動的にホワイトリストに追加されます。これにより、ファイルは再度隔離されることはありません。

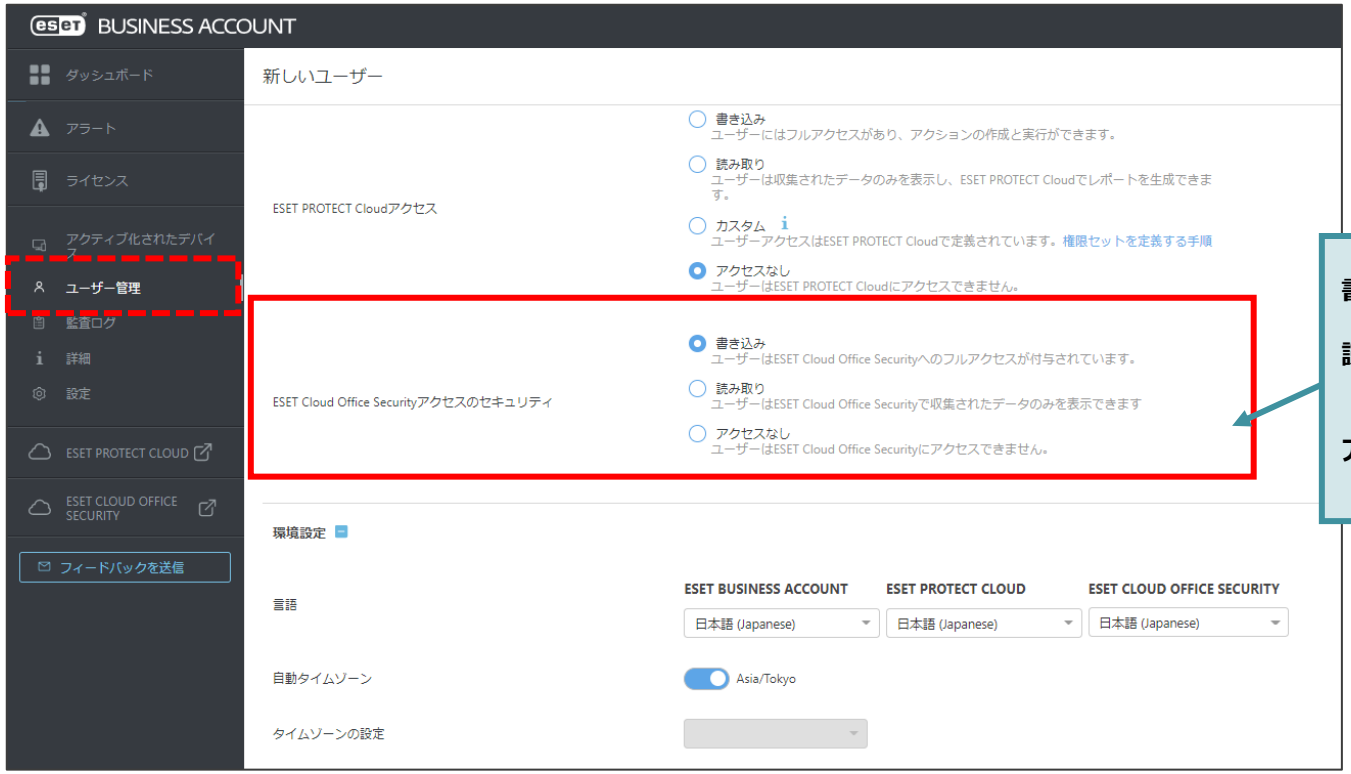
©Canon Marketing Japan Inc.

4. その他操作について

4. その他操作について

ECOSへのログインユーザーの管理

- EPHの「ユーザー」またはEBAの「ユーザー管理」からECOSにログインするユーザーを複数作成可能です。アクセス権の設定により、既定で全ての機能が実行できる「書き込み」に加えて、データの表示のみが行える「読み取り」などがあります。



※上記画像はEBAの画面です。

【ESET Cloud Office Securityアクセスのセキュリティ】
書き込み：ECOSにログインして情報の閲覧やすべての設定が行えます。

読み取り：ECOSにログインはできますが、情報の閲覧のみ可能で保護の設定やポリシー設定などを行うことはできません。

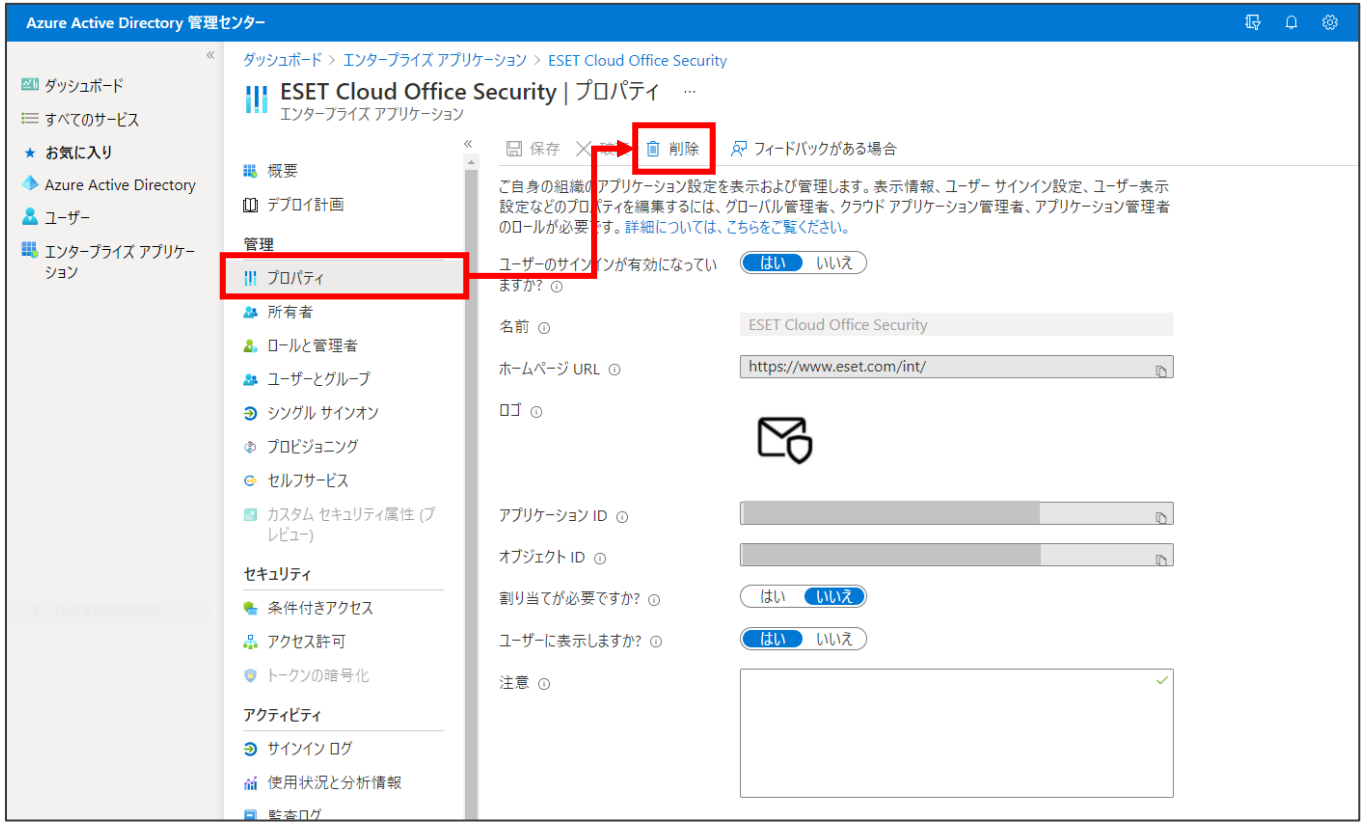
アクセスなし：EPHまたはEBAにECOSへのシングルサインオンのメニューが表示されず、ECOSへのログインができません。

©Canon Marketing Japan Inc.

4. その他操作について

AzureポータルからECOSを削除する方法

- AzureポータルからECOSを削除する場合は、Azure Active Directoryサービスからエンタープライズアプリケーション内のECOSを選択し、「プロパティ」より削除を行ってください。



※上記画像はAzure Active Directory管理センターの画面です。

©Canon Marketing Japan Inc.