

# ESET Cloud Office Security

## 機能紹介資料



CLOUD OFFICE  
SECURITY

第12版

2024年11月

**Canon**

# 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あります。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。

# もくじ

## 1. ESET Cloud Office Securityとは

- ECOSの概要
- ECOSの構成
- ECOSの主な機能
- 動作要件とサポートブラウザ
- 利用可能なMicrosoft 365プラン

## 2. Webコンソールの紹介

- Webコンソールの画面構成
- ダッシュボード
- ユーザー
- グループとサイト
- 検出
- 隔離
- 検査ログ
- レポート
- ポリシー
- ライセンス管理
- 監査ログ
- 設定

## 3. 注意事項 / 制限事項

- 各種データの保持期間
- ファイルが検査されない条件
- ファイルの隔離に関する制限

## 4. その他操作について

- ECOSへのログインユーザーの管理
- AzureポータルからECOSを削除する方法

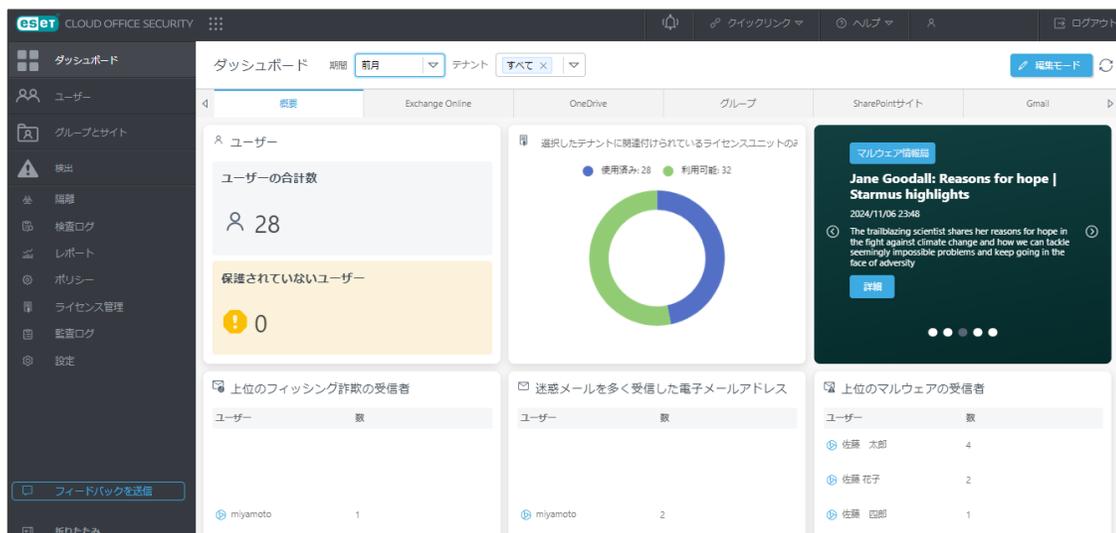
# 1. ESET Cloud Office Securityとは

# 1. ESET Cloud Office Securityとは

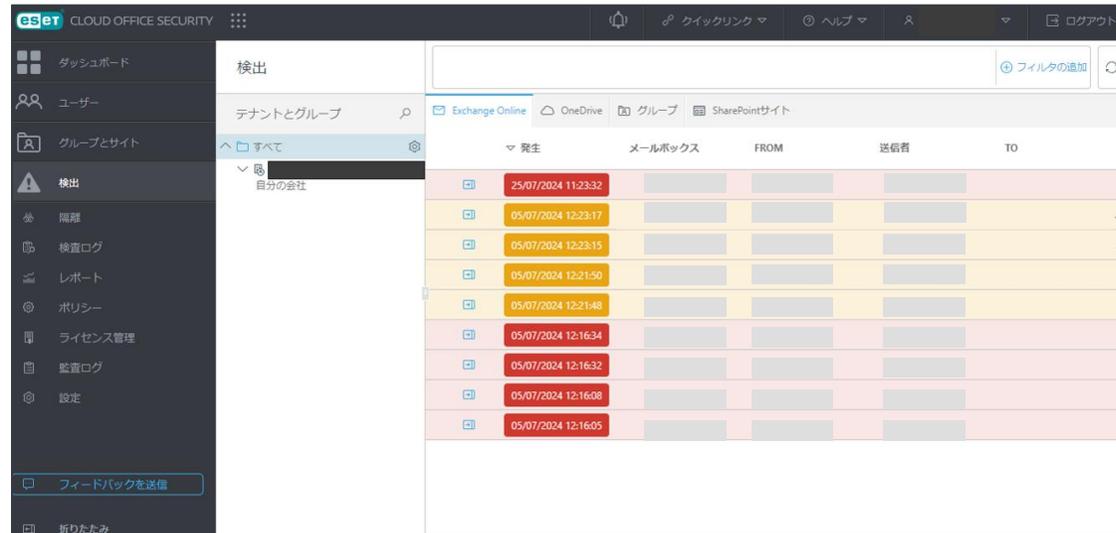
## ECOSの概要

- 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)

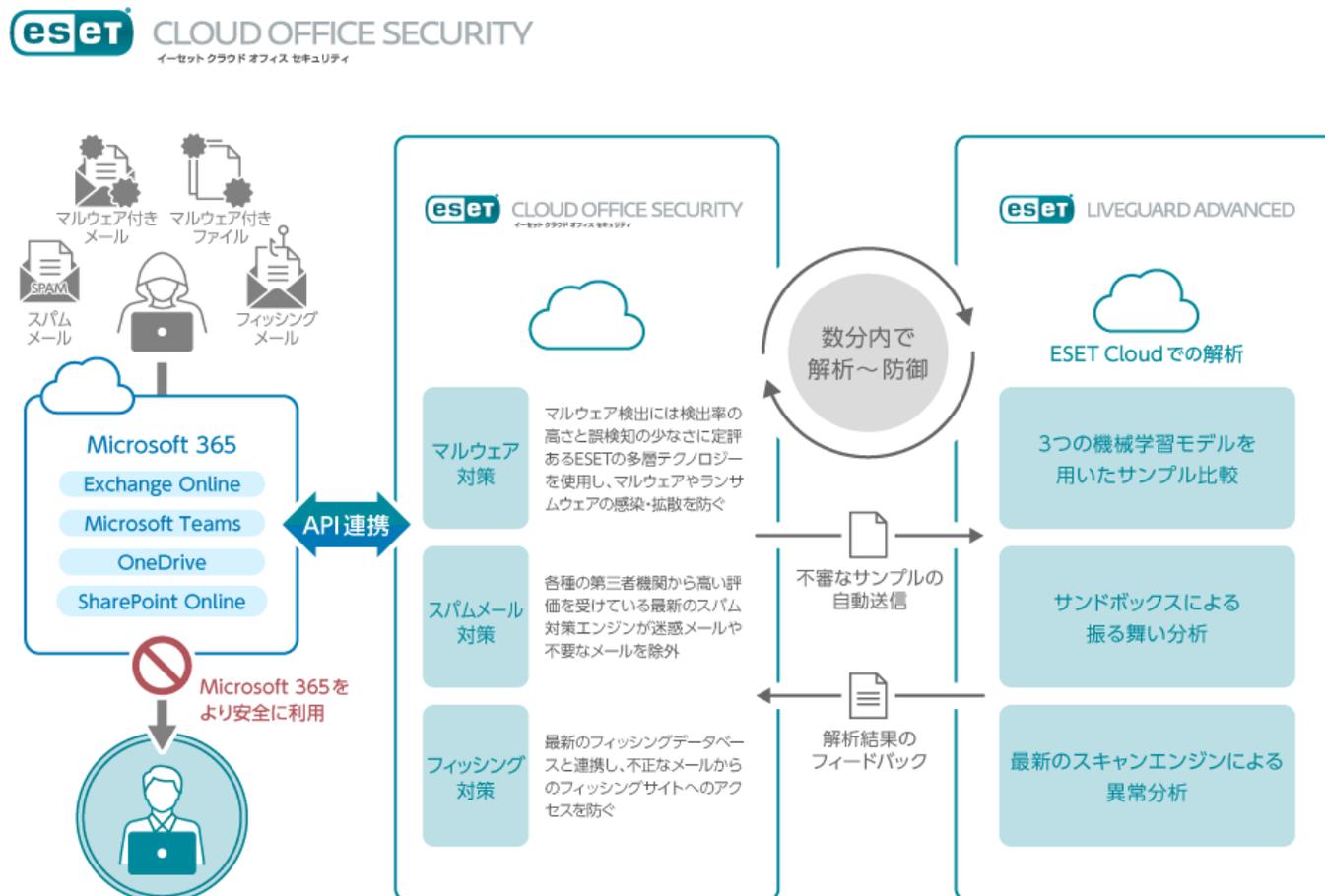


The detection screen shows a list of detected items with the following columns: 発生 (Occurrence), メールボックス (Mailbox), FROM, 送信者 (Sender), and TO.

発生	メールボックス	FROM	送信者	TO
25/07/2024 11:23:32				
05/07/2024 12:23:17				
05/07/2024 12:23:15				
05/07/2024 12:21:50				
05/07/2024 12:21:48				
05/07/2024 12:16:34				
05/07/2024 12:16:32				
05/07/2024 12:16:08				
05/07/2024 12:16:05				

# 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

# 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。

# 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

# 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。

# 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。

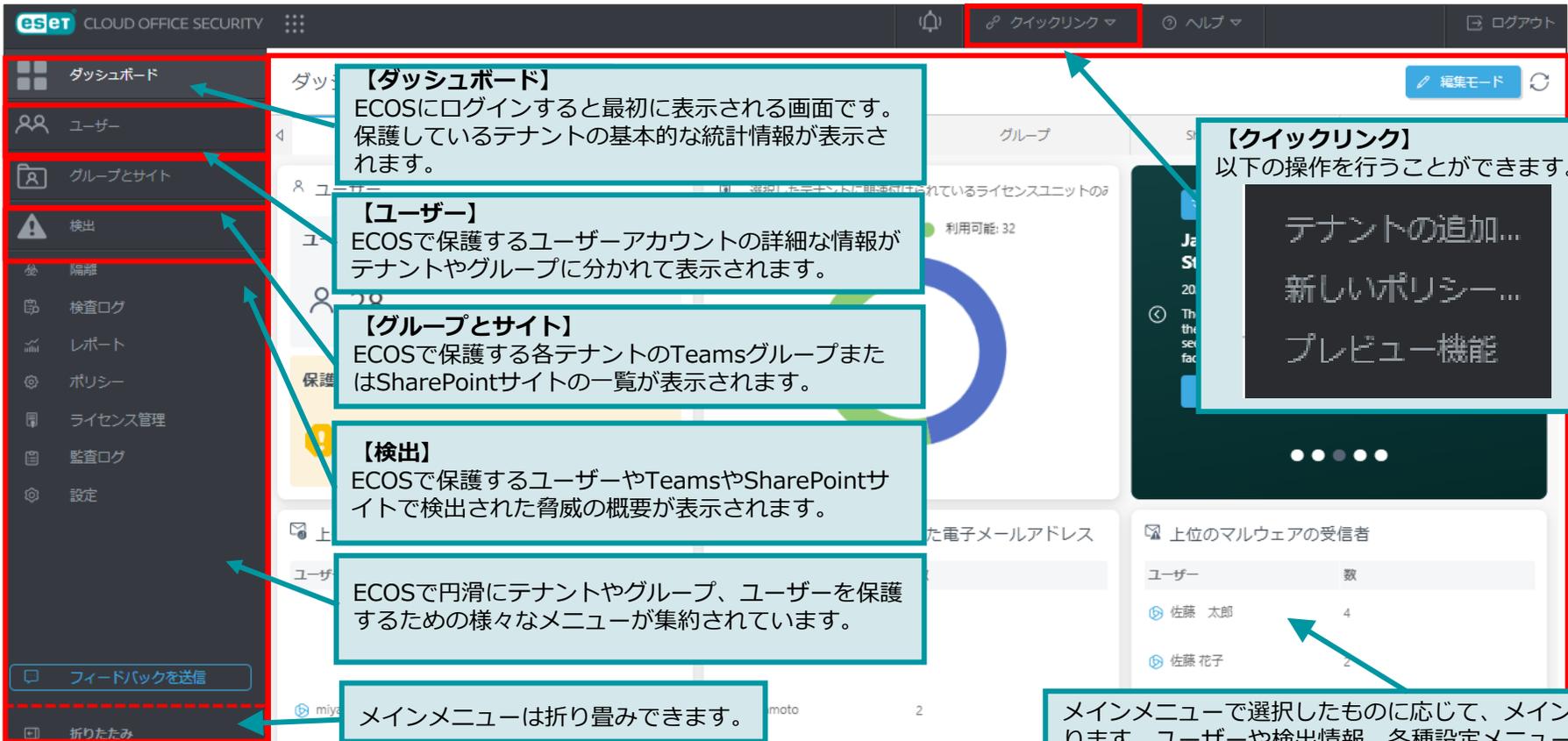
プラン名	
Microsoft 365 enterpriseプラン	<ul style="list-style-type: none"> <li>●Microsoft 365 Apps for enterprise</li> <li>●Microsoft 365 E3 / E5 / F3</li> <li>●Office 365 E1 / E3 / E5 / F3</li> </ul>
Microsoft 365 businessプラン	<ul style="list-style-type: none"> <li>●Microsoft 365 Business Basic</li> <li>●Microsoft 365 Business Standard</li> <li>●Microsoft 365 Business Premium</li> <li>●Microsoft 365 Apps</li> </ul>
Microsoft 365 Educationプラン	<ul style="list-style-type: none"> <li>●Microsoft 365 A3</li> <li>●Microsoft 365 A5</li> </ul>
Exchange Onlineプラン	<ul style="list-style-type: none"> <li>●Exchange Online (Plan 1) (Plan 2)</li> <li>●Microsoft 365 Business Standard</li> </ul>
OneDriveプラン	<ul style="list-style-type: none"> <li>●OneDrive for Business (Plan 1) (Plan 2)</li> <li>●Microsoft 365 Business Basic</li> <li>●Microsoft 365 Business Standard</li> </ul>

## 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。



The screenshot shows the ESET Cloud Office Security web console interface. The main menu on the left is highlighted with a red box. Callouts provide details for each menu item:

- 【ダッシュボード】**  
ECOSにログインすると最初に表示される画面です。保護しているテナントの基本的な統計情報が表示されます。
- 【ユーザー】**  
ECOSで保護するユーザーアカウントの詳細な情報がテナントやグループに分かれて表示されます。
- 【グループとサイト】**  
ECOSで保護する各テナントのTeamsグループまたはSharePointサイトの一覧が表示されます。
- 【検出】**  
ECOSで保護するユーザーやTeamsやSharePointサイトで検出された脅威の概要が表示されます。
- 【設定】**  
ECOSで円滑にテナントやグループ、ユーザーを保護するための様々なメニューが集約されています。

Additional callouts include:

- 【クイックリンク】**  
以下の操作を行うことができます。  
テナントの追加...  
新しいポリシー...  
プレビュー機能
- メインメニューは折り畳みできます。
- メインメニューで選択したものに依って、メイン画面が切り替わります。ユーザーや検出情報、各種設定メニューが表示されます。

## 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。



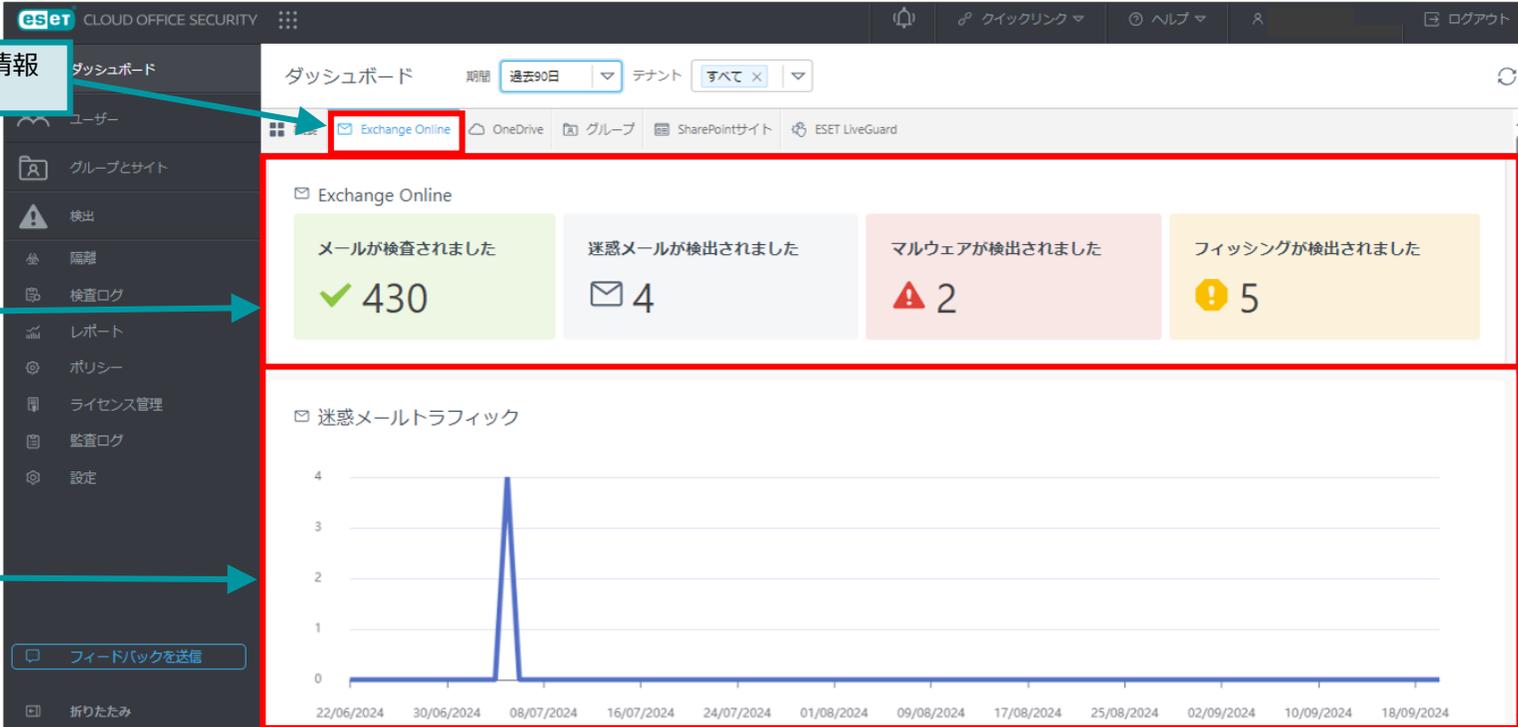
The screenshot shows the ESET Cloud Office Security dashboard. Key elements include:

- Header:** ESET logo, "CLOUD OFFICE SECURITY", navigation icons, and user profile.
- Navigation:** "ダッシュボード" (Dashboard) menu, "期間" (Period) dropdown set to "過去24時間" (Last 24 hours), and "編集モード" (Edit Mode) button.
- Summary Cards:**
  - ユーザー (Users):** Shows a total of 28 users and 0 users not protected.
  - ライセンス (Licenses):** A donut chart showing 28 used and 32 available licenses.
  - 迷惑メール (Spam):** A table listing users who received many spam emails, with "miyamoto" having 2.
  - マルウェア (Malware):** A table listing top malware recipients, with "Jane Goodal Starmus high" as the top recipient.
- Callouts:**
  - Callout 1:** Explains that the "期間" dropdown allows selecting the time period for data (options: 過去24時間, 過去7日, 過去30日, 過去90日).
  - Callout 2:** Points to the license usage chart, stating that usage is confirmed immediately.
  - Callout 3:** Explains that "編集モード" allows customizing the dashboard layout.
  - Callout 4:** Explains that clicking on users in the spam or malware tables provides detailed detection information for that user.

## 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」でも同様のグラフが表示されます。

検出項目	検出数
メールが検査されました	430
迷惑メールが検出されました	4
マルウェアが検出されました	2
フィッシングが検出されました	5

迷惑メールトラフィック

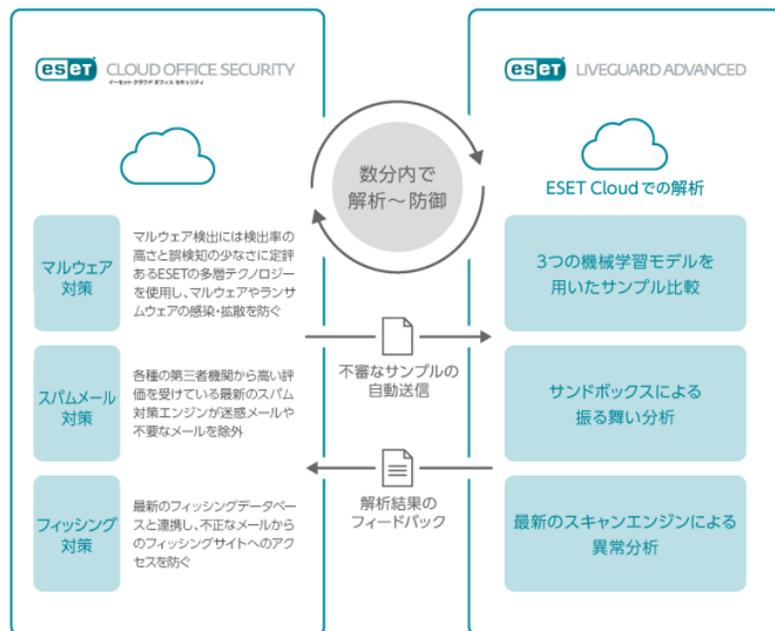
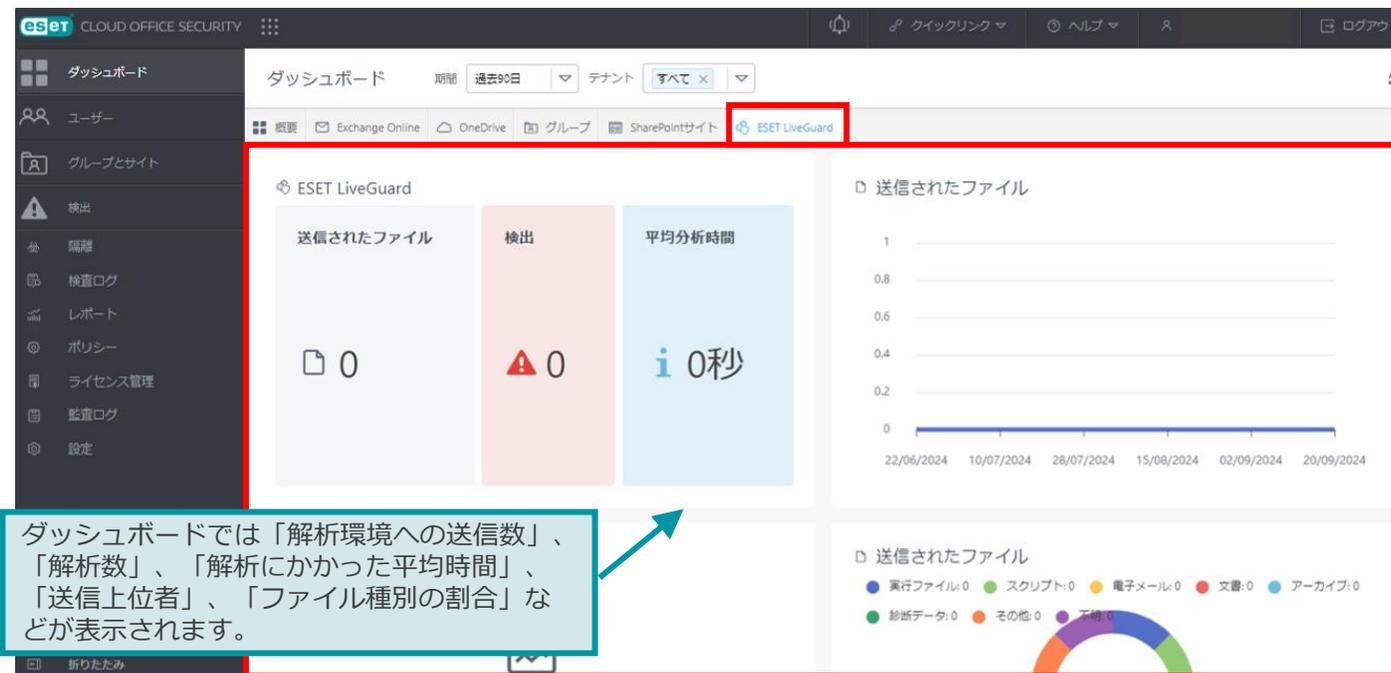
日付	検出数
22/06/2024	0
30/06/2024	0
08/07/2024	4
16/07/2024	0
24/07/2024	0
01/08/2024	0
09/08/2024	0
17/08/2024	0
25/08/2024	0
02/09/2024	0
10/09/2024	0
18/09/2024	0

## 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

The screenshot shows the ESET LiveGuard Advanced dashboard. The main section displays the following metrics:

- 送信されたファイル: 0
- 検出: 0
- 平均分析時間: 0秒

Below these metrics is a line chart showing the number of sent files over time, with data points for 22/06/2024, 10/07/2024, 28/07/2024, 15/08/2024, 02/09/2024, and 20/09/2024. At the bottom, there is a donut chart for '送信されたファイル' with a legend:

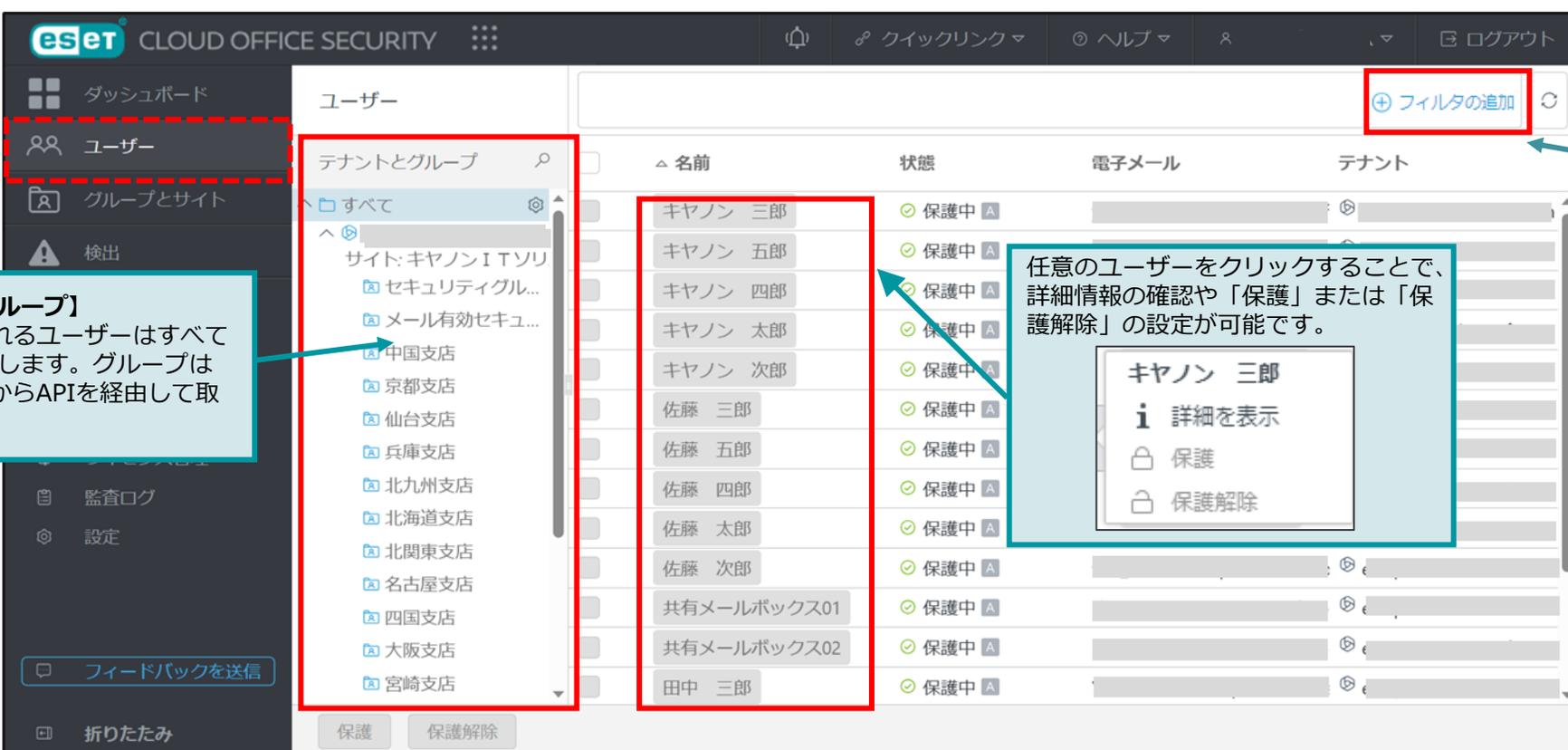
- 実行ファイル: 0
- スクリプト: 0
- 電子メール: 0
- 文書: 0
- アーカイブ: 0
- 診断データ: 0
- その他: 0
- 不明: 0

A callout box points to the dashboard content, stating: 「ダッシュボードでは「解析環境への送信数」、「解析数」、「解析にかかった平均時間」、「送信上位者」、「ファイル種別の割合」などが表示されます。」

## 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なく、どのユーザーを保護するか、または保護解除することも選択できます。



The screenshot shows the ESET Cloud Office Security user management interface. The main table lists users with columns for Name, Status, Email, and Tenant. A sidebar on the left shows navigation options like 'ダッシュボード', 'ユーザー', 'グループとサイト', and '検出'. A top navigation bar includes 'クイックリンク', 'ヘルプ', and 'ログアウト'. A search bar and a '+ フィルタの追加' button are at the top right.

**【テナントとグループ】**  
ECOSで管理されるユーザーはすべてグループに所属します。グループはMicrosoft 365からAPIを経由して取得されます。

**【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。  
保護の状態  
自動保護  
名前  
電子メール  
タイプ

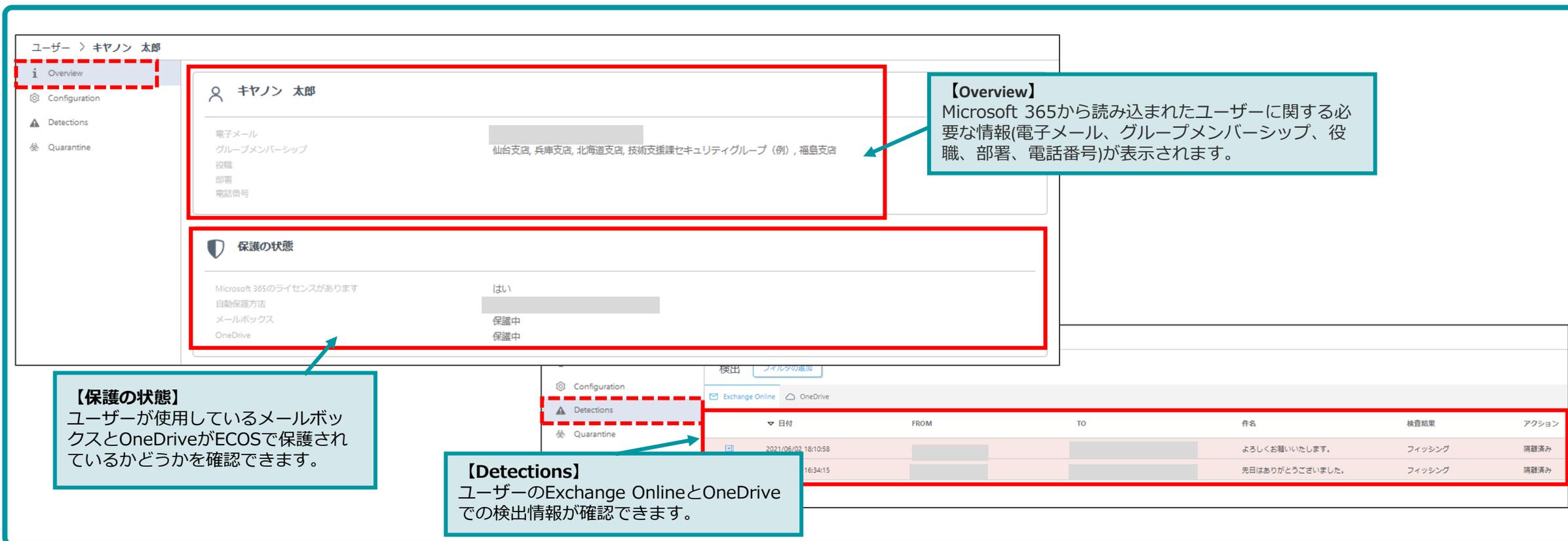
任意のユーザーをクリックすることで、詳細情報の確認や「保護」または「保護解除」の設定が可能です。

名前	状態	電子メール	テナント
キヤノン 三郎	保護中		
キヤノン 五郎	保護中		
キヤノン 四郎	保護中		
キヤノン 太郎	保護中		
キヤノン 次郎	保護中		
佐藤 三郎	保護中		
佐藤 五郎	保護中		
佐藤 四郎	保護中		
佐藤 太郎	保護中		
佐藤 次郎	保護中		
共有メールボックス01	保護中		
共有メールボックス02	保護中		
田中 三郎	保護中		

## 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。



ユーザー > キヤノン 太郎

**Overview**

キヤノン 太郎

電子メール  
グループメンバーシップ  
役割  
部署  
電話番号

仙台支店, 兵庫支店, 北海道支店, 技術支援課セキュリティグループ (例), 福島支店

**保護の状態**

Microsoft 365のライセンスがあります  
自動保護方法  
メールボックス  
OneDrive

はい  
保護中  
保護中

**【Overview】**  
Microsoft 365から読み込まれたユーザーに関する必要な情報(電子メール、グループメンバーシップ、役職、部署、電話番号)が表示されます。

**【保護の状態】**  
ユーザーが使用しているメールボックスとOneDriveがECOSで保護されているかどうかを確認できます。

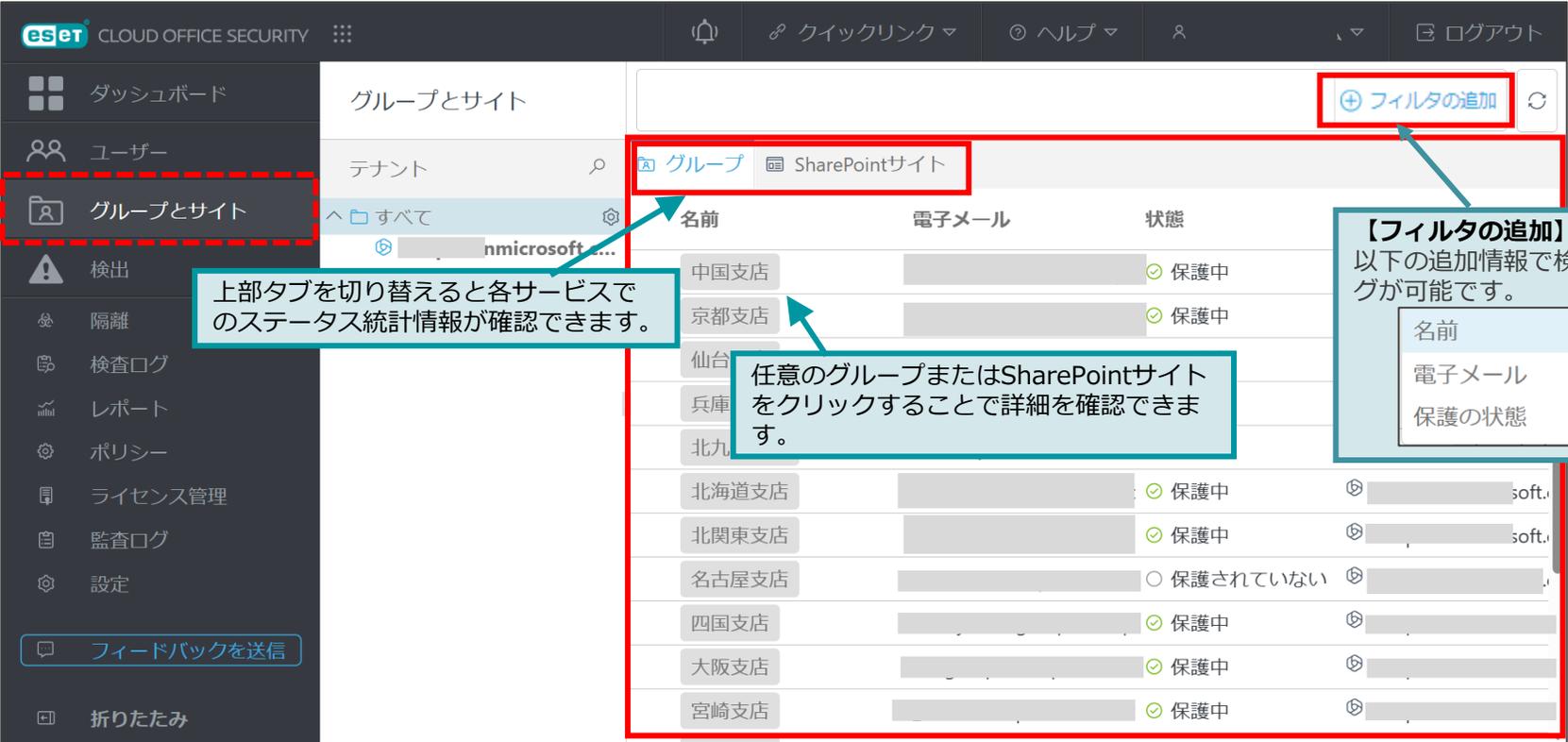
**【Detections】**  
ユーザーのExchange OnlineとOneDriveでの検出情報が確認できます。

日付	FROM	TO	件名	検査結果	アクション
2021/06/02 18:10:58			よろしくお疲れいたします。	フィッシング	隔離済み
16:34:15			先日はありがとうございました。	フィッシング	隔離済み

## 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。



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。

任意のグループまたはSharePointサイトをクリックすることで詳細を確認できます。

**【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。

- 名前
- 電子メール
- 保護の状態

名前	電子メール	状態
中国支店		保護中
京都支店		保護中
仙台		
兵庫		
北九		
北海道支店		保護中
北関東支店		保護中
名古屋支店		保護されていない
四国支店		保護中
大阪支店		保護中
宮崎支店		保護中

## 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**

グループ > 東京本社

Overview

Configuration

Detections

Quarantine

**【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。

東京本社

電子メール  
所有者: キヤノン 太郎  
メンバー: キヤノン 四郎, キヤノン 次郎, 佐藤 五郎, 佐藤 次郎

**■ SharePointサイトの概要(一部抜粋)**

Team Site

URL: https://[redacted]

作成者: [redacted]

テンプレート: [redacted]

サブサイト: 0

記憶域の使用量: 1.71 MB

メンバー: [redacted]

**【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。

保護の状態

グループ: 保護中

**【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。

グループ > 東京本社

Overview

Configuration

Detections

Quarantine

検出: フィルタの適用

日時	オブジェクト	位置	検出	検出結果	アクション
18/01/2022 11:33:32	資料.zip	/General	Eicar test file	マルウェア	テストで削除
17/01/2022 17:00:17	資料.zip	/案件	Eicar test file	マルウェア	テストで削除

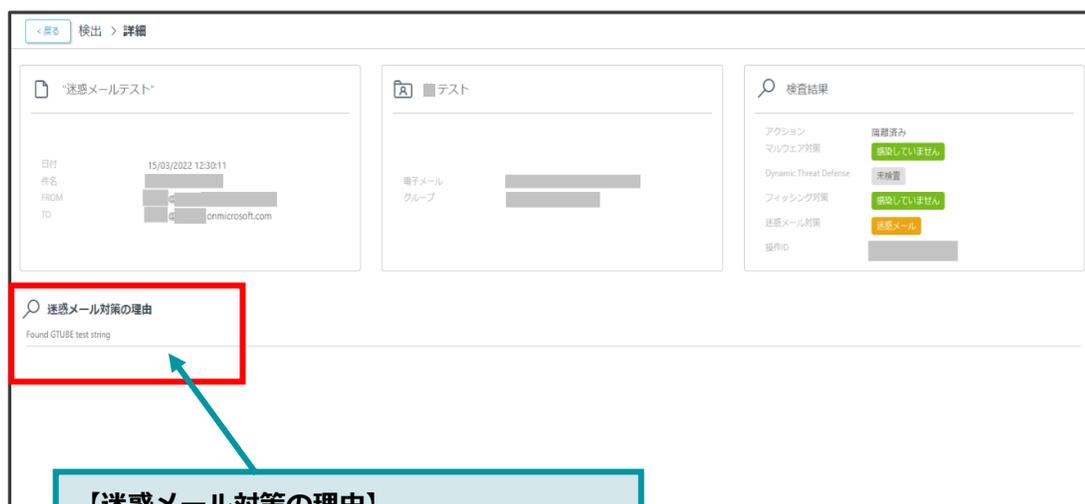


## 2. Webコンソールの画面ご紹介

### 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。

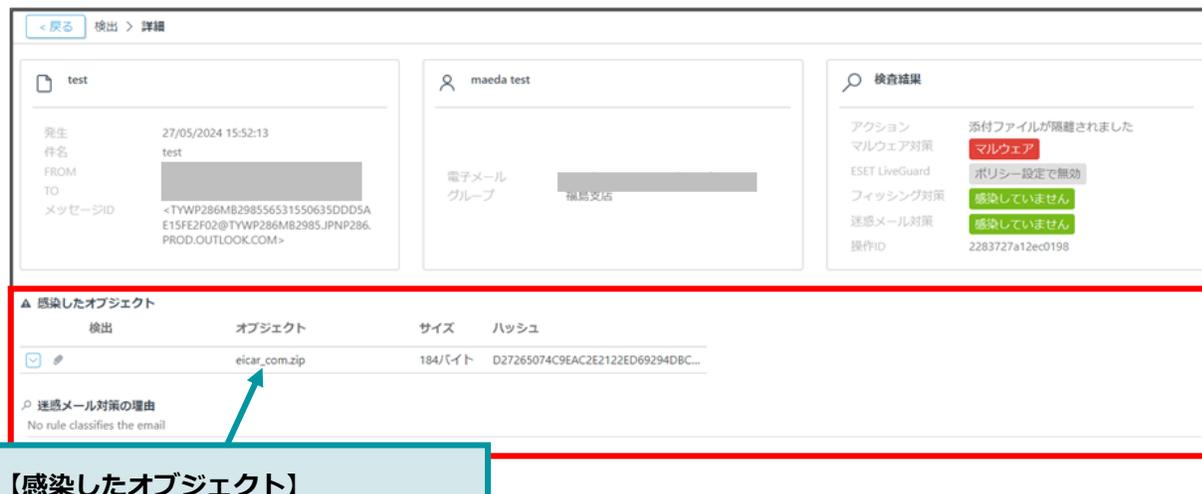
■ 検出(迷惑メールが検出された場合)の詳細画面



迷惑メール対策の理由  
Found GTUBE test string

**【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



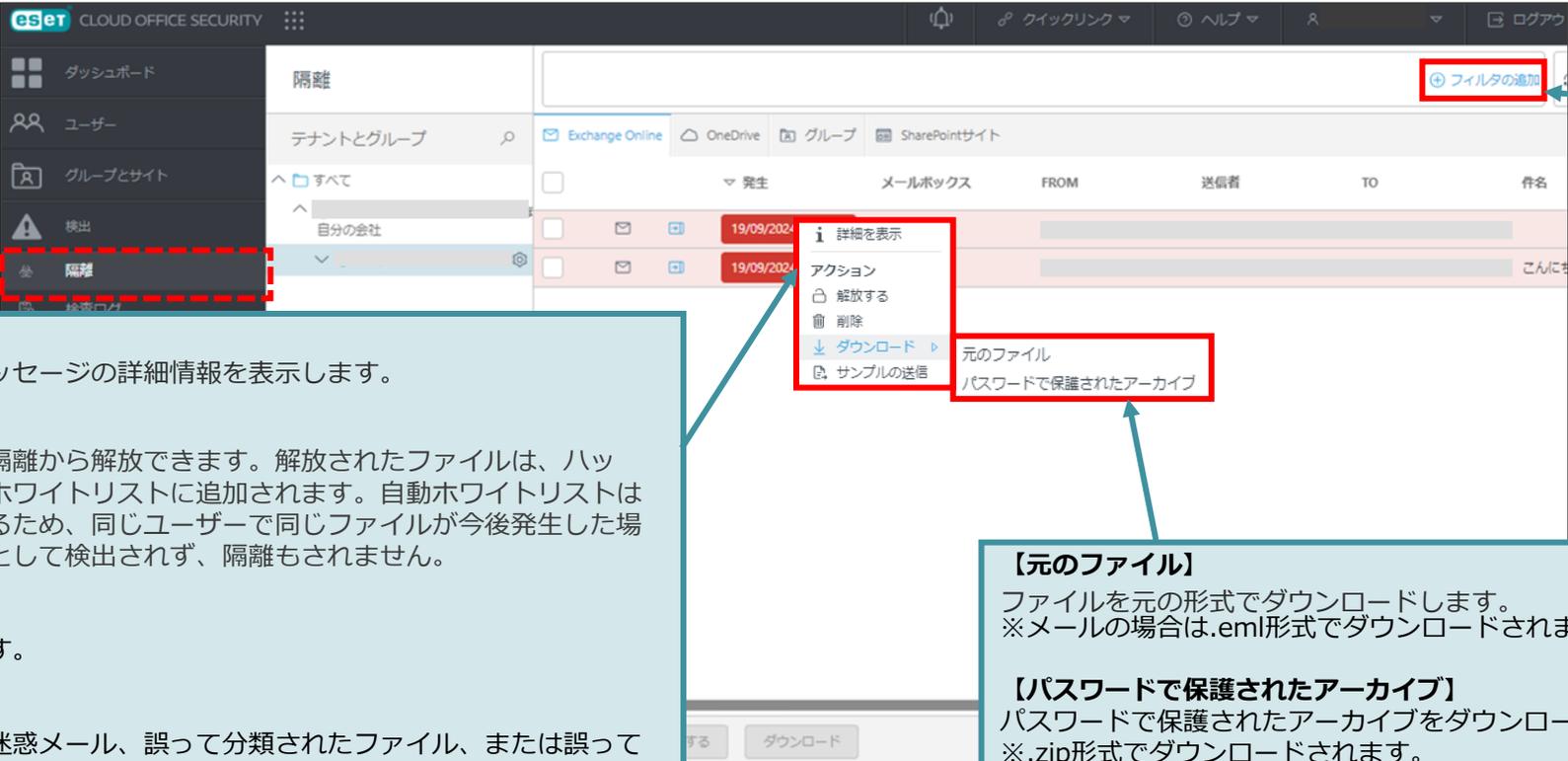
感染したオブジェクト	検出	オブジェクト	サイズ	ハッシュ
		eicar_com.zip	184バイト	D27265074C9EAC2E2122ED69294DBC...

**【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。

## 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。

**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。

**【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。

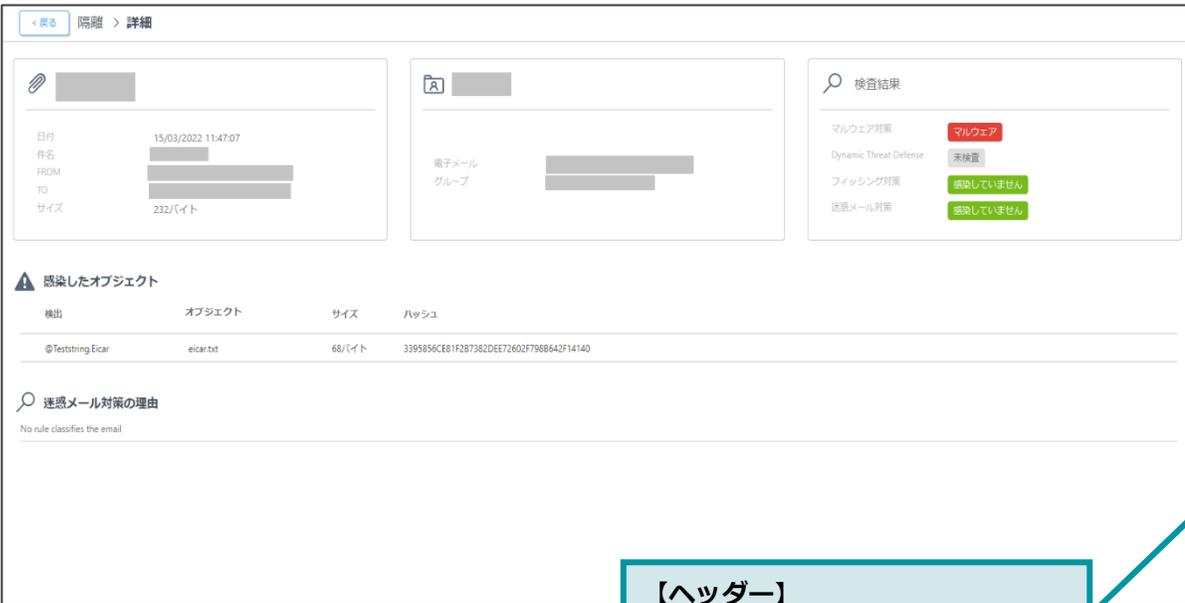
- 発生開始
- 発生終了
- メールボックス
- FROM
- TO
- 件名
- メッセージID
- 送信者
- 迷惑メール対策の理由
- 検査結果

## 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



**感染したオブジェクト**

検出	オブジェクト	サイズ	ハッシュ
©Teststring Eicar	eicar.txt	68/バイト	339585CE81F2B7382DEE72602F788642F14140

**迷惑メール対策の理由**  
No rule classifies the email

#### ■ 隔離(フィッシングメールが隔離された場合)の詳細画面



**迷惑メール対策の理由**  
No rule classifies the email

**フィッシングリンク**  
https://[redacted]  
https://[redacted]

**ヘッダーの表示**

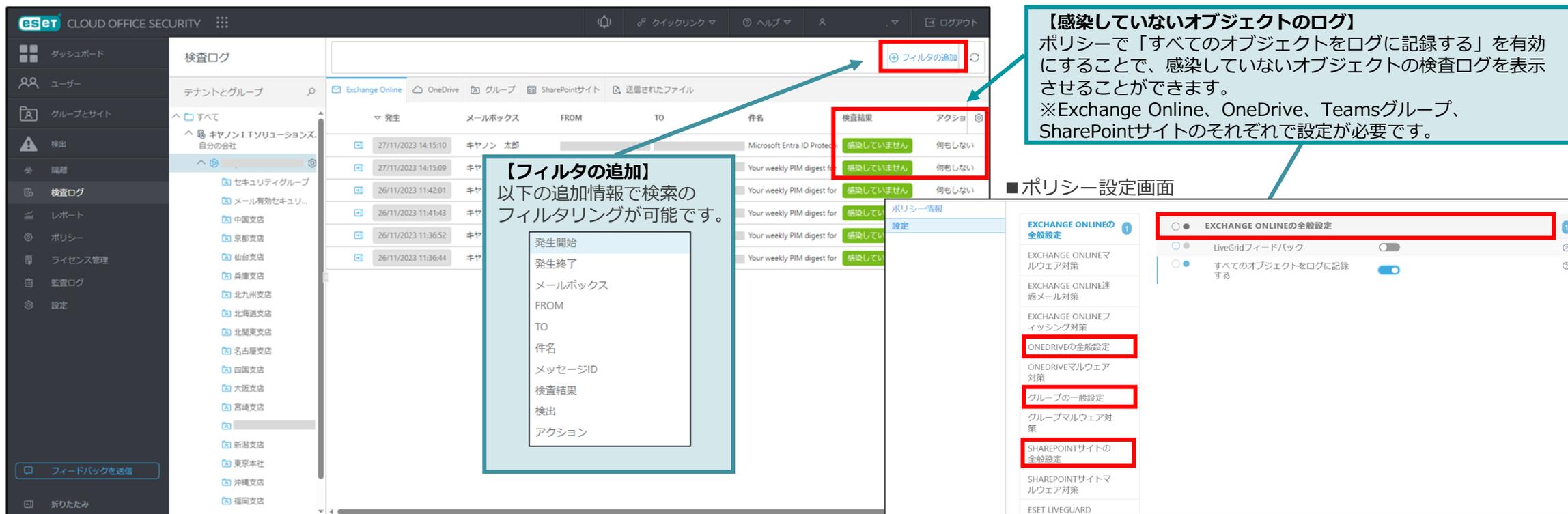
**【フィッシングリンク】**  
フィッシングメール内で確認されたフィッシングのリンク情報が確認できます。

**【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。

## 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。



**【感染していないオブジェクトのログ】**  
 ポリシーで「すべてのオブジェクトをログに記録する」を有効にすることで、感染していないオブジェクトの検査ログを表示させることができます。  
 ※Exchange Online、OneDrive、Teamsグループ、SharePointサイトのそれぞれで設定が必要です。

**【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
- 検査結果
- 検出
- アクション

■ ポリシー設定画面

EXCHANGE ONLINEの全般設定

EXCHANGE ONLINEの全般設定

EXCHANGE ONLINEマルウェア対策

EXCHANGE ONLINE迷惑メール対策

EXCHANGE ONLINEフィッシング対策

ONEDRIVEの全般設定

ONEDRIVEマルウェア対策

グループの一般設定

グループマルウェア対策

SHAREPOINTサイトの全般設定

SHAREPOINTサイトマルウェア対策

ESET LIVEGUARD

EXCHANGE ONLINEの全般設定

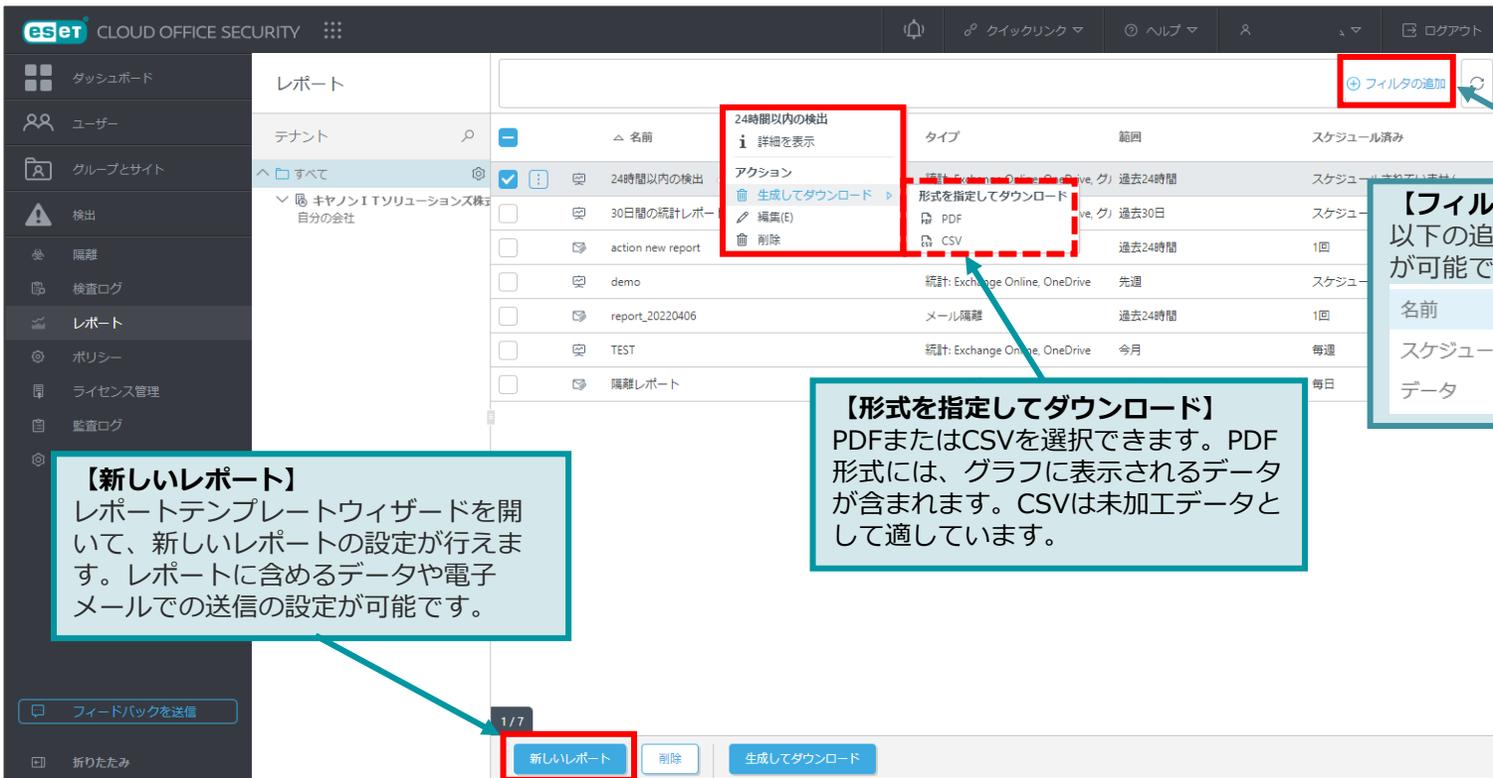
LiveGridフィードバック

すべてのオブジェクトをログに記録する

## 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。



**【新しいレポート】**  
レポートテンプレートウィザードを開いて、新しいレポートの設定が行えます。レポートに含めるデータや電子メールでの送信の設定が可能です。

**【形式を指定してダウンロード】**  
PDFまたはCSVを選択できます。PDF形式には、グラフに表示されるデータが含まれます。CSVは未加工データとして適しています。

**【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。

名前
スケジュール済み
データ

## 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

Date	Scanned	Malware	Phishing	Spam
2021/6/7	2	0	0	0
2021/6/8	3	1	0	1

## 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。

**【テナントとグループ】**  
ユーザーおよびユーザーグループ、テナント、Teamsグループ、SharePointサイトに割り当てられたポリシーを確認できます。「未割り当て」はターゲットに割り当てられていないカスタムポリシーを表示します。

**【Default policy】**  
•すべてのユーザーに適用されます(保護されているユーザー、保護されていないユーザー)  
•修正や削除はできません

**【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。  
名前

**【詳細を表示】**  
作成されたポリシー、設定、および割り当てられたポリシーに関する詳細情報が表示されます。  
**【編集】**  
既存のポリシーの設定を編集します。  
**【割り当て】**  
ポリシーを適用するユーザー、テナント、Teamsグループ、またはSharePointサイトを選択します。  
**【複製】**  
選択したテンプレートに基づいて新しいポリシーを作成します。重複するポリシーには新しい名前が必要です。  
**【削除】**  
選択したポリシーを完全に削除します。

**【順序の変更】**  
ポリシーの優先度を再調整するには、順序の変更をクリックします。

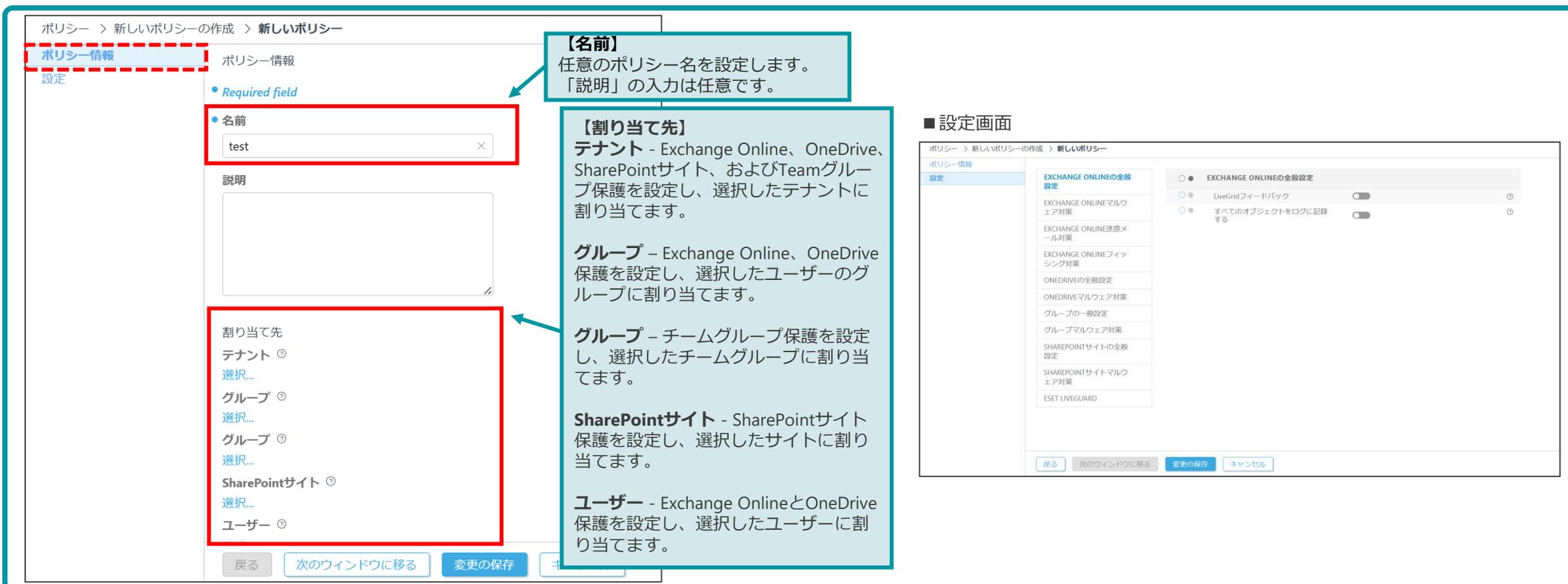
**【新しいポリシー】**  
新しいカスタムポリシーを作成することができます。

オーダー	名前	説明	割り当て先
1	Default policy	すべてのユーザーに適用されます(保護されているユーザー、保護されていないユーザー)	すべて
2	通知用ポリシー	通知用ポリシー	未割り当て
3	全てのオブジェクトをログに記録	全てのオブジェクトをログに記録	テナント:1
4	TEAMSグループ用	TEAMSグループ用	グループ:1
5			未割り当て
6			未割り当て
7			SharePointサイト:1
8		microsoftcc	未割り当て
9		る)ユーザ	未割り当て
10		知)ユーザ	未割り当て
11			グループ:2
12		シェアポイント保護_重複	SharePointサイト:1
13			未割り当て
14			ユーザー:2
15			SharePointサイト:1
16			テナント:1
17		通知オフ&削除	未割り当て
18			ユーザー:1
19		demo	テナント:1

## 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。



ポリシー > 新しいポリシーの作成 > 新しいポリシー

ポリシー情報

設定

Required field

名前

test

説明

割り当て先

テナント  選択...

グループ  選択...

グループ  選択...

SharePointサイト  選択...

ユーザー

戻る 次のウィンドウに移る 変更の保存 キャンセル

【名前】  
任意のポリシー名を設定します。「説明」の入力は任意です。

【割り当て先】  
テナント - Exchange Online、OneDrive、SharePointサイト、およびTeamグループ保護を設定し、選択したテナントに割り当てます。  
グループ - Exchange Online、OneDrive保護を設定し、選択したユーザーのグループに割り当てます。  
グループ - チームグループ保護を設定し、選択したチームグループに割り当てます。  
SharePointサイト - SharePointサイト保護を設定し、選択したサイトに割り当てます。  
ユーザー - Exchange OnlineとOneDrive保護を設定し、選択したユーザーに割り当てます。

■ 設定画面

ポリシー > 新しいポリシーの作成 > 新しいポリシー

ポリシー情報

設定

EXCHANGE ONLINEの全般設定

EXCHANGE ONLINEマルウェア対策

EXCHANGE ONLINE迷惑メール対策

EXCHANGE ONLINEフィッシング対策

ONEDRIVEの全般設定

ONEDRIVEマルウェア対策

グループの一般設定

グループマルウェア対策

SHAREPOINTサイトの全般設定

SHAREPOINTサイトマルウェア対策

ESET LIVEGUARD

EXCHANGE ONLINEの全般設定

LiveGridフィードバック

すべてのオブジェクトをログに記録する

戻る 次のウィンドウに移る 変更の保存 キャンセル

## 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。

ポリシー > 新しいポリシーの作成 > 新しいポリシー

ポリシー情報  
設定

Required field

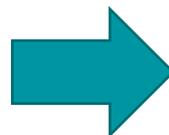
名前  
test

説明

割り当て先

- テナント ⊙  
選択...
- グループ ⊙  
選択...
- グループ ⊙  
選択...
- SharePointサイト ⊙  
選択...
- ユーザー ⊙  
選択...

戻る 次のウィンドウに移る 変更の保存 キャンセル



#### ■ 割り当て先にユーザーを選択した場合の画面

ユーザーの選択

テナントとグループ

すべて

キヤノンITソリューションズ  
自分の会社

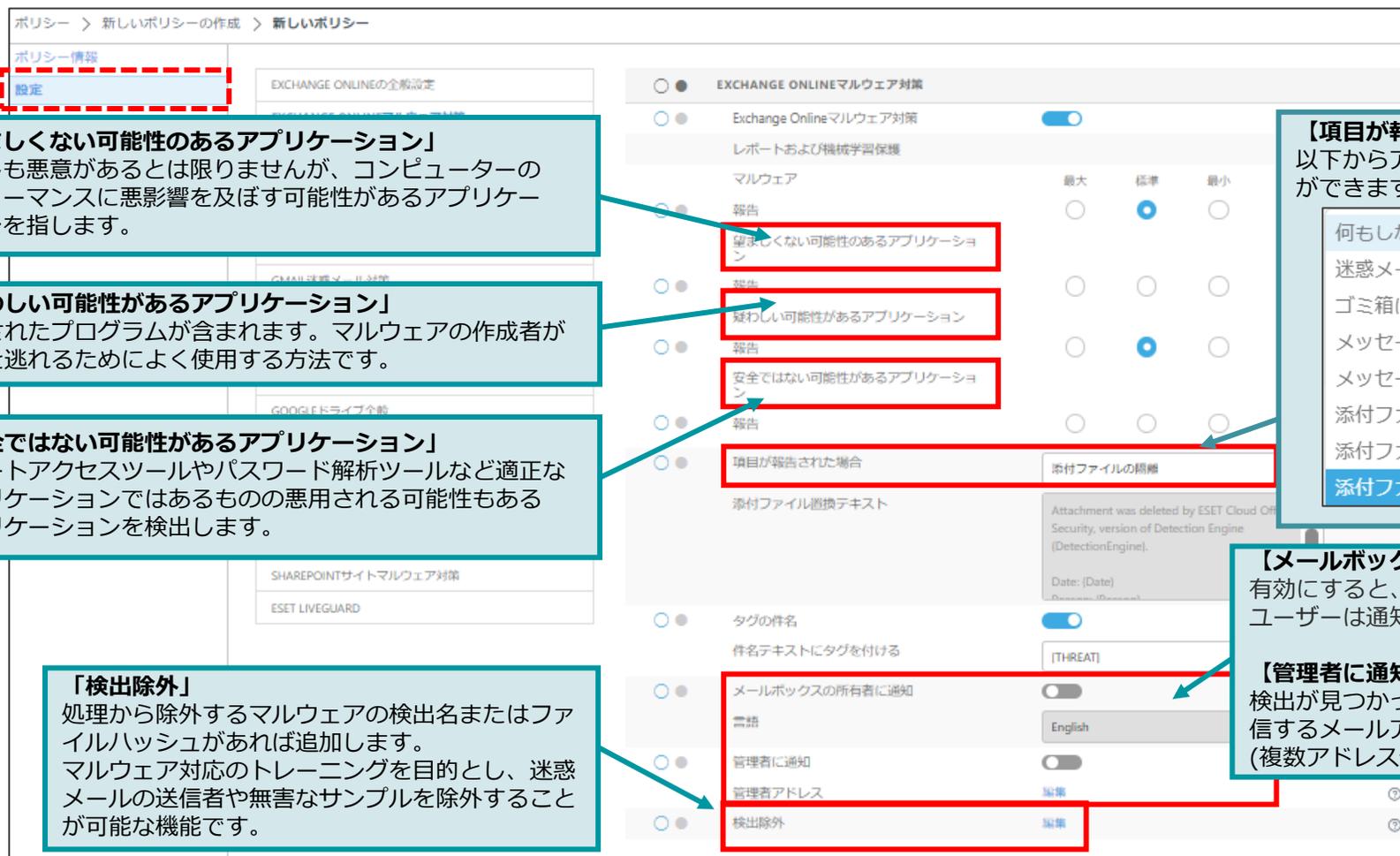
名前	状態	電子メール	テナント	タイプ
<input type="checkbox"/> 田中 次郎	保護中 A			N/A
<input type="checkbox"/> 田中 太郎	保護中 A			N/A
<input type="checkbox"/> 田中 五郎	保護中 A			N/A
<input type="checkbox"/> 共有メールボックス02	保護中 A			N/A
<input type="checkbox"/> 共有メールボックス01	保護中 A			N/A
<input type="checkbox"/> 佐藤 次郎	保護中 A			N/A
<input type="checkbox"/> 佐藤 太郎	保護中 A			N/A
<input type="checkbox"/> 佐藤 四郎	保護中 A			N/A
<input type="checkbox"/> 佐藤 五郎	保護中 A			N/A
<input type="checkbox"/> 佐藤 三郎	保護中 A			N/A
<input type="checkbox"/> キヤノン 次郎	保護中 A			N/A
<input type="checkbox"/> キヤノン 太郎	保護中 A			N/A
<input type="checkbox"/> キヤノン 四郎	保護中 A			N/A

キャンセル OK

※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。

## 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



ポリシー > 新しいポリシーの作成 > 新しいポリシー

ポリシー情報  
設定

EXCHANGE ONLINEの全般設定

EXCHANGE ONLINEマルウェア対策

Exchange Onlineマルウェア対策

レポートおよび機械学習保護

マルウェア	最大	標準	最小
報告	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
望ましくない可能性のあるアプリケーション	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
疑わしい可能性のあるアプリケーション	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
安全ではない可能性のあるアプリケーション	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
項目が報告された場合	添付ファイルの隔離		
添付ファイル置換テキスト	Attachment was deleted by ESET Cloud Office Security, version of Detection Engine (DetectionEngine). Date: (Date) Reason: (Reason)		
タグの件名	<input checked="" type="checkbox"/>		
件名テキストにタグを付ける	[THREAT]		
メールボックスの所有者に通知	<input type="checkbox"/>		
言語	English		
管理者に通知	<input type="checkbox"/>		
管理者アドレス	編集		
検出除外	編集		

「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)

## 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



**【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**

**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。

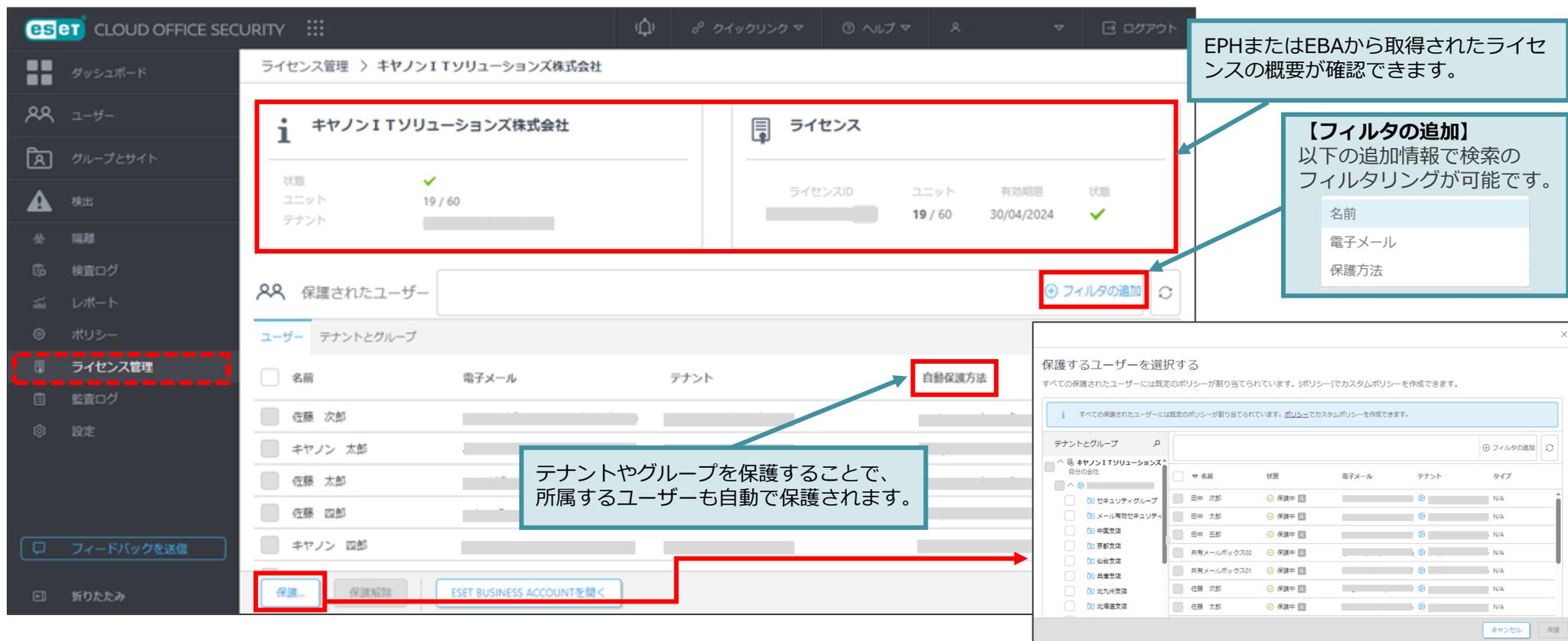
**ブロックされている送信者のリスト** - 特定の送信者またはドメインから送信された電子メールをブラックリストに追加します。

※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>

## 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。



The screenshot displays the ESET Cloud Office Security web console interface. The main content area is titled 'ライセンス管理 > キヤノンITソリューションズ株式会社'. It shows a summary of the license status, including the number of units (19/60) and the expiration date (30/04/2024). Below this, there is a table of protected users and a 'フィルタの追加' (Add Filter) button. A modal window titled '保護するユーザーを選択する' (Select users to protect) is open, showing a list of users and groups with checkboxes for selection.

**EPHまたはEBAから取得されたライセンスの概要が確認できます。**

**【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。  
名前  
電子メール  
保護方法

**自動保護方法**

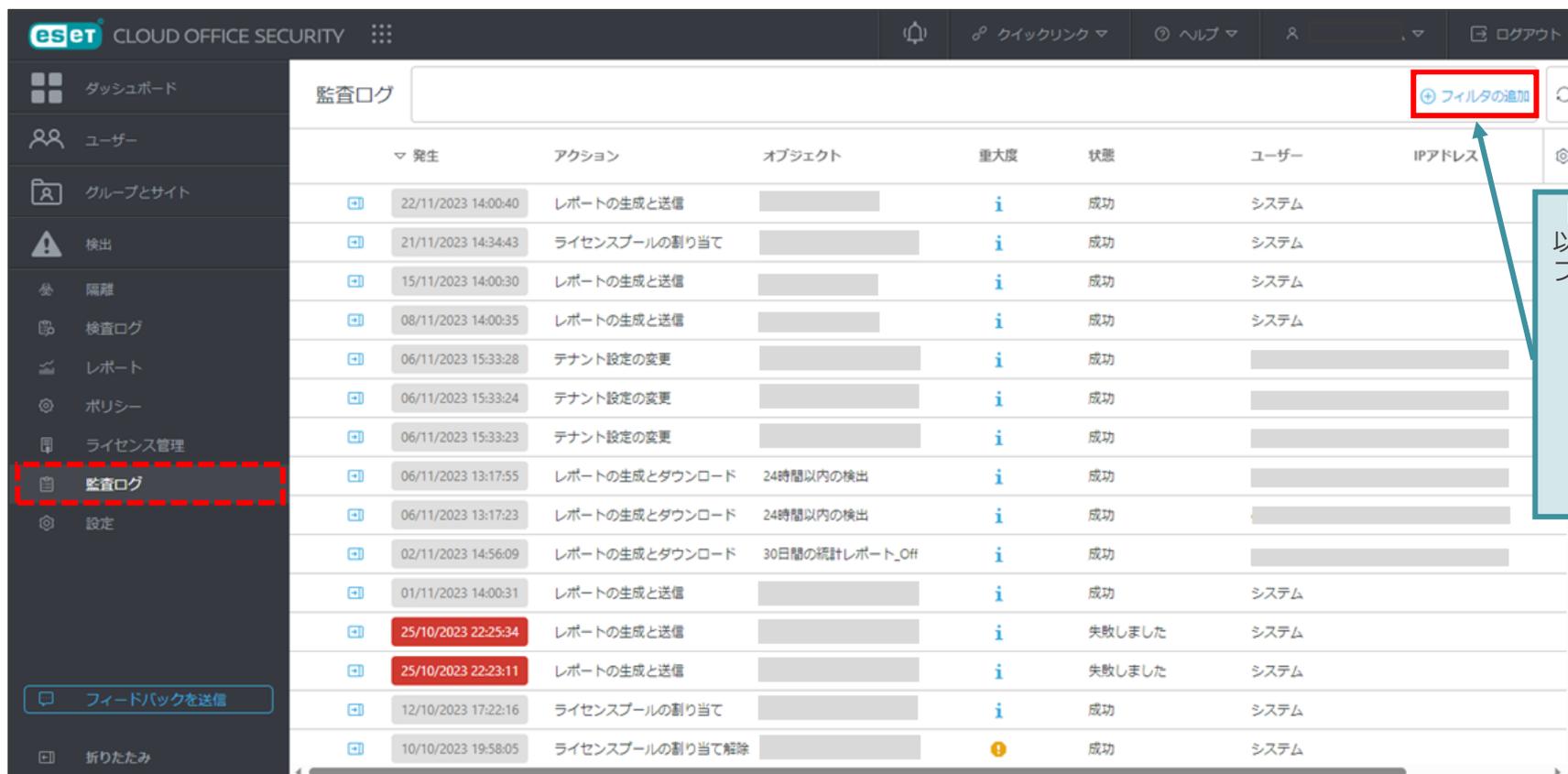
テナントやグループを保護することで、所属するユーザーも自動で保護されます。

保護... 保護解除 ESET BUSINESS ACCOUNTを開く

## 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。



発生	アクション	オブジェクト	重大度	状態	ユーザー	IPアドレス
22/11/2023 14:00:40	レポートの生成と送信		i	成功	システム	
21/11/2023 14:34:43	ライセンスプールの割り当て		i	成功	システム	
15/11/2023 14:00:30	レポートの生成と送信		i	成功	システム	
08/11/2023 14:00:35	レポートの生成と送信		i	成功	システム	
06/11/2023 15:33:28	テナント設定の変更		i	成功		
06/11/2023 15:33:24	テナント設定の変更		i	成功		
06/11/2023 15:33:23	テナント設定の変更		i	成功		
06/11/2023 13:17:55	レポートの生成とダウンロード	24時間以内の検出	i	成功		
06/11/2023 13:17:23	レポートの生成とダウンロード	24時間以内の検出	i	成功		
02/11/2023 14:56:09	レポートの生成とダウンロード	30日間の統計レポート_Off	i	成功		
01/11/2023 14:00:31	レポートの生成と送信		i	成功	システム	
25/10/2023 22:25:34	レポートの生成と送信		i	失敗しました	システム	
25/10/2023 22:23:11	レポートの生成と送信		i	失敗しました	システム	
12/10/2023 17:22:16	ライセンスプールの割り当て		i	成功	システム	
10/10/2023 19:58:05	ライセンスプールの割り当て解除		i	成功	システム	

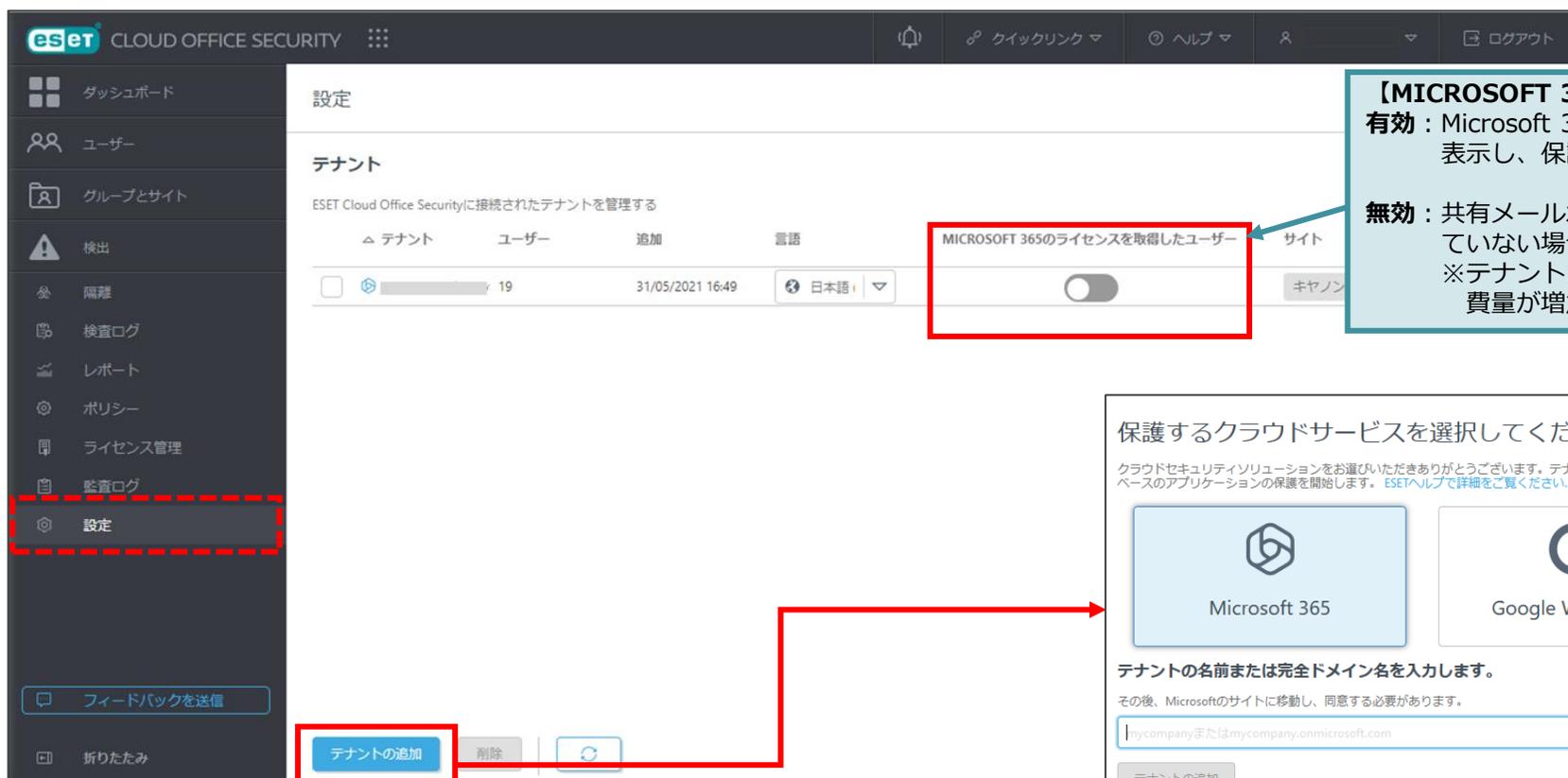
**【フィルタの追加】**  
以下の追加情報で検索のフィルタリングが可能です。

- 発生開始
- 発生終了
- アクション
- オブジェクト
- 重大度
- 状態
- ユーザー
- システムが開始されました

## 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。



The screenshot shows the ESET Cloud Office Security web console. The left sidebar contains navigation options: ダッシュボード, ユーザー, グループとサイト, 検出, 隔離, 検査ログ, レポート, ポリシー, ライセンス管理, 監査ログ, 設定 (highlighted with a red dashed box), フィードバックを送信, and 折りたたみ. The main content area is titled '設定' (Settings) and 'テナント' (Tenants). It displays a table of tenants with columns for 'テナント' (Tenant), 'ユーザー' (User), '追加' (Add), and '言語' (Language). A red box highlights a toggle switch labeled 'MICROSOFT 365のライセンスを取得したユーザー' (Users who have obtained Microsoft 365 licenses). Below the table, there are buttons for 'テナントの追加' (Add Tenant), '削除' (Delete), and a refresh icon. A red arrow points from the 'テナントの追加' button to a modal dialog box.

**【MICROSOFT 365のライセンスを取得したユーザー】**  
**有効：**Microsoft 365のライセンスを使用しているユーザーのみを一覧表示し、保護できます。  
**無効：**共有メールボックスなどのMicrosoft 365のライセンスを所有していない場合でも、すべてのユーザーを表示し保護できます。  
 ※テナントまたはグループの自動保護によって、ライセンスの消費量が増加する可能性があります。

保護するクラウドサービスを選択してください

クラウドセキュリティソリューションをお選びいただきありがとうございます。テナントを追加して、クラウドベースのアプリケーションの保護を開始します。ESETヘルプで詳細をご覧ください...



Microsoft 365



Google Workspace

テナントの名前または完全ドメイン名を入力します。

その後、Microsoftのサイトに移動し、同意する必要があります。

テナントの追加

### **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。

## 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を超えている場合
  - 添付ファイルを含む電子メッセージ全体で150MBを超えている場合

※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。

## 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。



**【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。

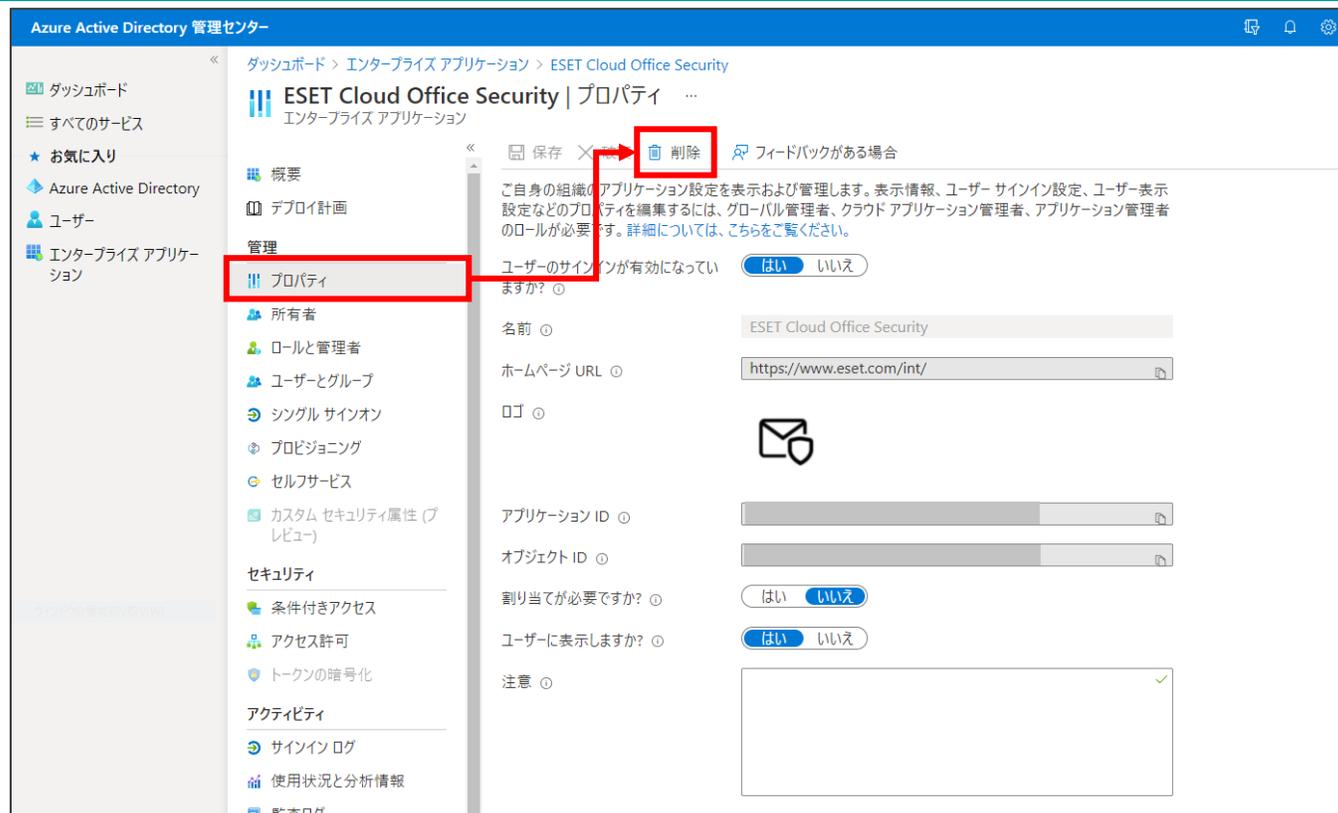
**アクセスなし**：EPHまたはEBAにECOSへのシングルサインオンのメニューが表示されず、ECOSへのログインができません。

※上記画像はEBAの画面です。

## 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。