

ESET Cloud Office Security
オンラインヘルプ補足資料

第 1.5 版

■改訂履歴

版数	改訂日	改訂内容
1.1	2022/3/31	プロダクト名称の変更に伴う改訂。 旧：ESET Dynamic Threat Defense (EDTD) 新：ESET LiveGuard Advanced (ELGA)
1.2	2024/5/23	目次を刷新
1.3	2024/7/31	ESET PROTECT HUB (EPH) リリースに伴う改訂
1.4	2025/2/13	・問い合わせ窓口 URL の変更 (P5) ・改訂履歴の追加
1.5	2025/3/21	・問い合わせ窓口 URL の変更 (P5)

■本書について

- 本資料は、ESET Cloud Office Security (以降、ECOS) のオンラインヘルプの内容を補完する位置づけの資料です。ECOS を使用する際には、下記オンラインヘルプも併せて参照ください。

<https://help.eset.com/ecos/ja-JP/>

- 本資料には、ライセンスの管理ポータルサイトである ESET Business Account (以降、EBA) および ESET PROTECT HUB (以降、EPH) の基本的な機能や用語に関する説明はありません。EBA/EPH の基本的な機能や用語については、EBA/EPH のマニュアルやオンラインヘルプを参照ください。
- 本資料は、本資料作成時の製品仕様の情報に基づき作成されています。ECOS のバージョンアップなどにより、記載内容と ECOS に搭載されている機能及び名称が異なっている場合があります。また本資料の内容は、改訂などにより予告なく変更することがあります。
- 本資料の著作権は、キャノンマーケティングジャパン株式会社に帰属します。本資料の一部または全部を無断で複写、複製、改変することはその形態を問わず、禁じます。
- ESET、ESET Cloud Office Security、ESET LiveGuard Advanced (旧名称: ESET Dynamic Threat Defense)、ESET Business Account、ESET MSP Administrator は、ESET, spol. s. r. o. の商標です。
- Microsoft365、Azure、Azure Active Directory、Azure Cloud Services、Microsoft Edge は、米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。
- Mozilla Firefox は、Mozilla Foundation の米国およびその他の国における登録商標です。
- Google Chrome は、Google Inc. の登録商標です。
- Opera は、Opera Software ASA の商標または登録商標です。
- Safari は、米国および他の国々で登録された Apple Inc. の商標です。

■注意事項

オンラインヘルプの注意事項を以下に記載します。
オンラインヘルプに記載されている内容と異なる場合、本資料に記載された内容を正とします。

[要件とサポート対象の Microsoft365 プラン]

- 以下の Microsoft365 プランがサポートされます。

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

- Azure Active Directory (Azure AD)への管理者アクセス
- Azure Cloud Services – Exchange / OneDrive / Teams / SharePoint のいずれかまたはすべてのサービス
- ESET Business Account または ESET PROTECT HUB のアカウント
- ECOS ポータルは以下のブラウザがサポートされます。

ブラウザ	バージョン
Mozilla Firefox	バージョン 69 以降
Microsoft Edge	バージョン 44 以降
Google Chrome	バージョン 77 以降
Opera	バージョン 63 以降
Safari	バージョン 13.x 以降

[ECOS の検出ログに記録されない/想定通りの挙動をしない場合]

- Microsoft365 セキュリティセンターの設定により Microsoft365 が検体を検出することで、ECOS で検出ログに残らない、設定した検出時の挙動を取らないといった現象が発生する場合がございます。

[ライセンス管理について]

- EBA または EPH によるライセンス管理が必要となります。

[データセンターロケーションの選択]

- ECOS を有効化する作業の中でデータセンターロケーションを選択する必要があります。日本での推奨データセンターは「EU」となります。
- データセンターは完全に分離されています。データセンターのロケーションを選択すると、変更したり、別の場所に移動したりすることはできません。データセンターロケーションを変更するには、ECOS の有効化作業を最初から行っていただく必要があります。

[お問い合わせ]

- ECOS ポータルの左部メニュー[フィードバックを送信]は日本ではご利用いただけません。弊社お問い合わせ窓口よりお問い合わせください。
- ECOS ポータル上部メニュー「ヘルプ」の[サポートフォーラム]、[フィードバックを送信]は日本ではご利用いただけません。弊社お問い合わせ窓口よりお問い合わせください。
- ECOS の誤検出については、オンラインヘルプ記載のお問い合わせ先ではなく弊社お問い合わせ窓口よりお問い合わせください。
- 弊社お問い合わせ窓口は以下となります。

<https://canon.jp/biz/solution/security/it-sec/lineup/eset/support>

目次

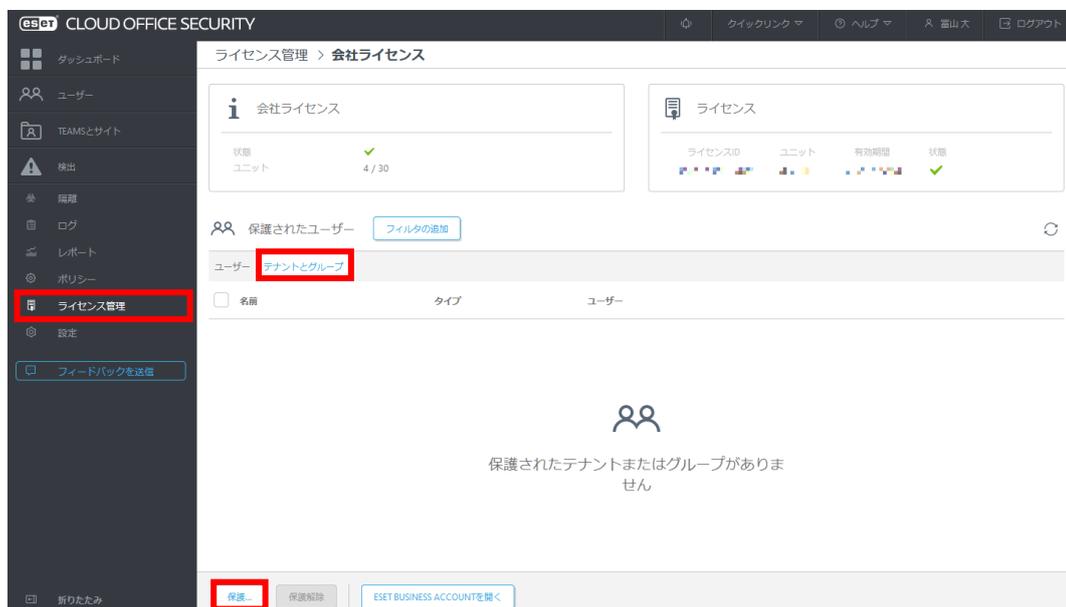
1	保護設定	7
1.1	テナントまたはグループでユーザーを保護	7
1.2	ユーザーを個別で保護する	9
1.3	ESET LiveGuard Advanced(旧名称：ESET Dynamic Threat Defense)を有効にする ..	11
2	グループとサイトの表示条件	15
2.1	グループ	15
2.2	SharePoint サイト	15
3	ECOS のタイプ設定を利用する際の注意点	16
3.1	タイプ設定の有効化	16
4	付録	19
4.1	お問い合わせ時に求められる情報	19

1 保護設定

1.1 テナントまたはグループでユーザーを保護

ECOS 導入後、Microsoft365 より新規で作成されたユーザーを自動で保護することができるためテナント全体を保護することを推奨いたします。ここではテナントまたはグループ単位でユーザーを保護する手順を記載いたします。

- ① ECOS ポータルより[ライセンス管理] – [テナントとグループ]タブをクリックし、画面下部の「保護」ボタンをクリックします。



- ② [保護するユーザーを選択する]画面で保護するテナント、またはグループにチェックを入れ「保護」ボタンをクリックします。

保護するユーザーを選択する

保護されたすべてのユーザーに既定のポリシーが割り当てられます。[ポリシー]でカスタムポリシーを作成してください



- ③ ユーザー画面で選択したテナント内のユーザー、またはグループ内のユーザーが保護されていることを確認します。



ワンポイント

テナント全体を保護した場合、個別でユーザーの保護を解除することはできません。

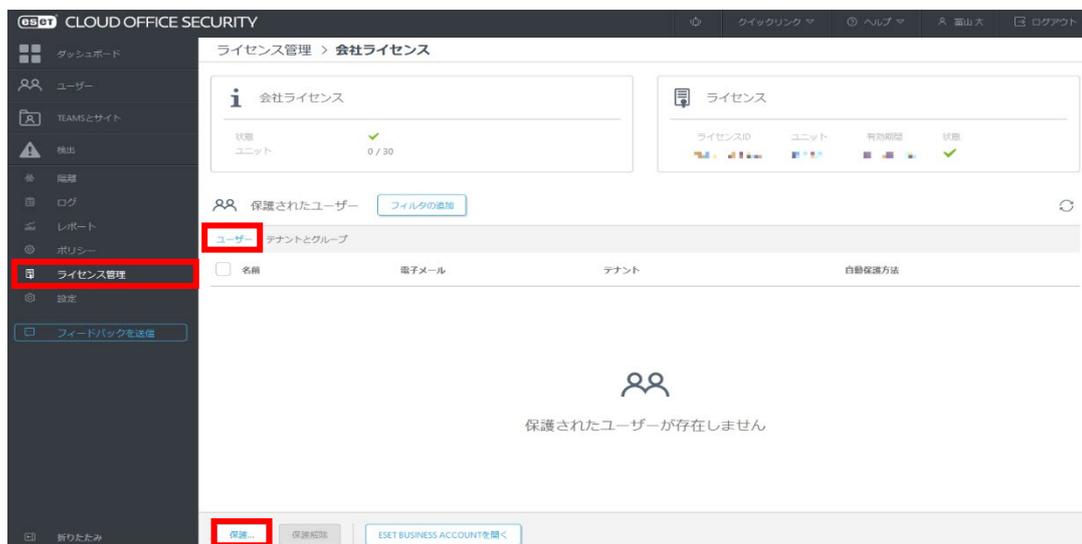
1.2 ユーザーを個別で保護する

本設定は ECOS を保護ユーザー個別で指定したい場合やスモールスタートしたい場合に利用します。ここではユーザーを選択して保護する手順を記載いたします。

! 重要

Microsoft365 より新規で作成されたユーザーを ECOS は自動で保護しません。ご注意ください。

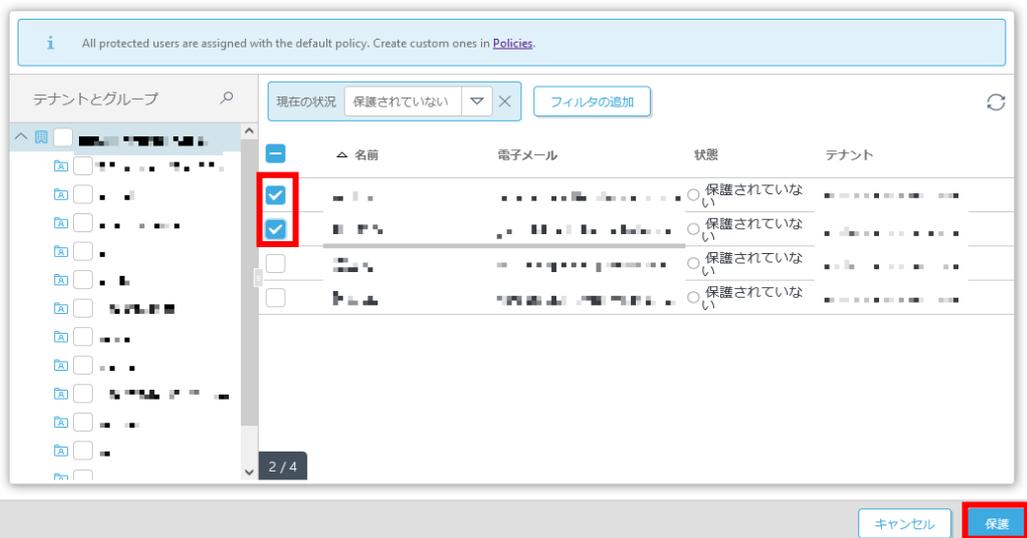
- ① ECOS ポータルより[ライセンス管理] - [ユーザー]タブをクリックし、画面下部の「保護」ボタンをクリックします。



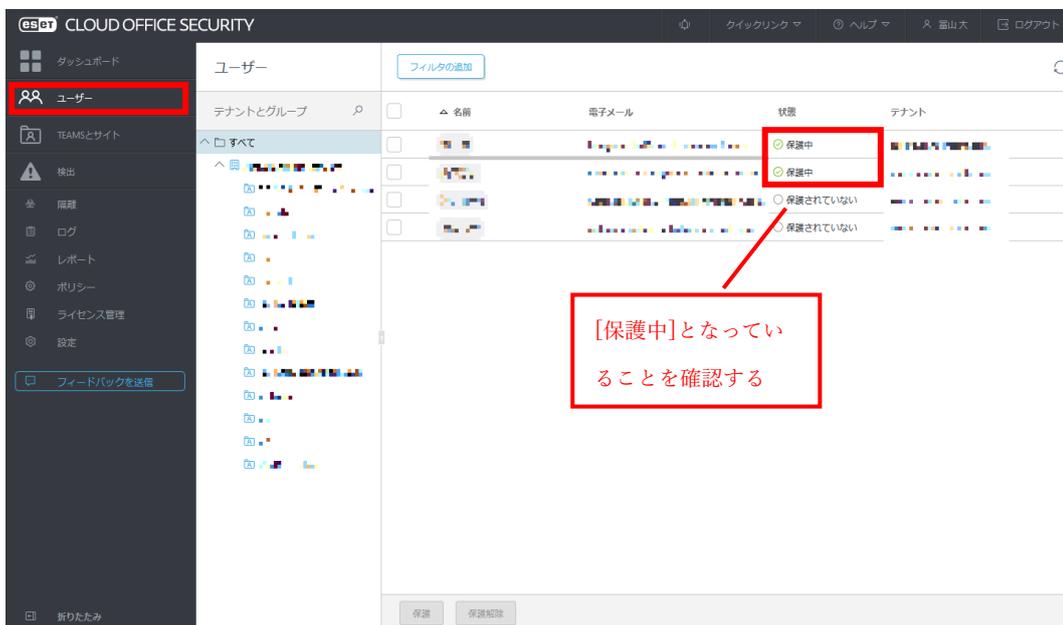
- ② [保護するユーザーを選択する]画面で保護するユーザーにチェックを入れ「保護」をクリックします。

保護するユーザーを選択する

保護されたすべてのユーザーに既定のポリシーが割り当てられます。[ポリシー]でカスタムポリシーを作成してください



- ③ ユーザー画面で選択したユーザーが保護されていることを確認します。



1.3 ESET LiveGuard Advanced(旧名称：ESET Dynamic Threat Defense)を有効にする

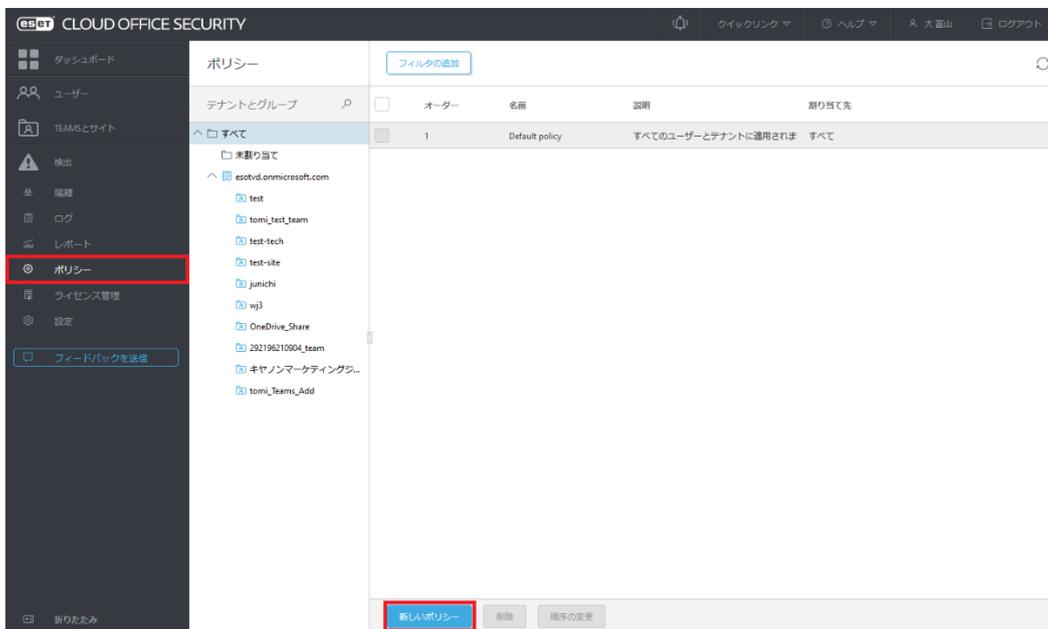
本設定はECOSでESET LiveGuard Advanced(旧名称:ESET Dynamic Threat Defense)(以降、ELGA(旧名称:EDTD))を有効にしたい場合に利用します。ここではテナント全体で保護する手順を記載いたします。

製品の画面上、一部旧名称(ESET Dynamic Threat Defense)表記になっている場合があります。

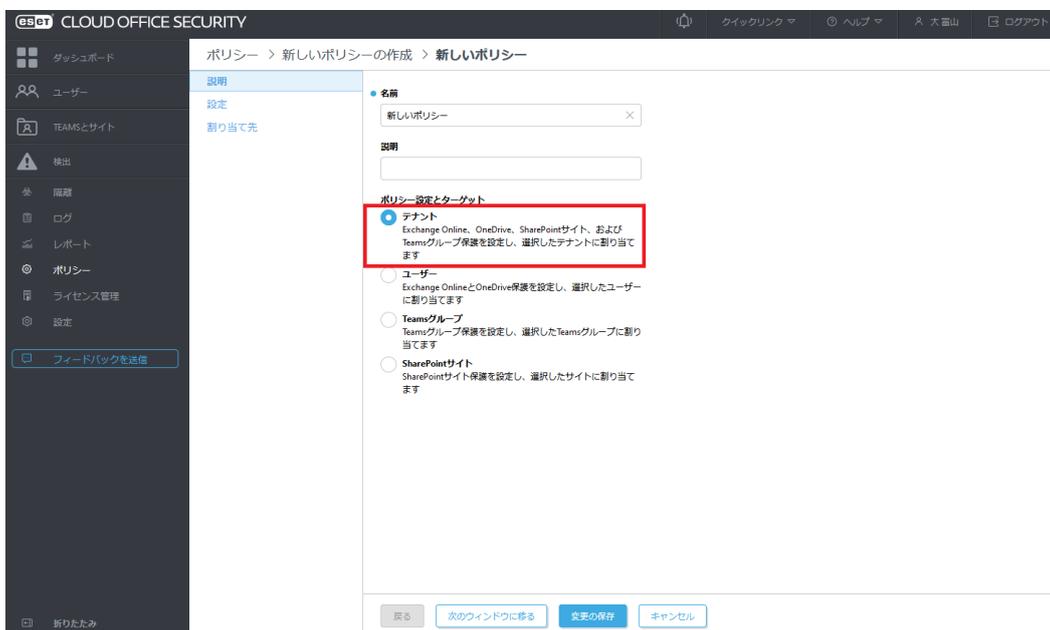
!重要

ELGA(旧名称:EDTD)を有効にする場合、LiveGrid フィードバックが有効になります。

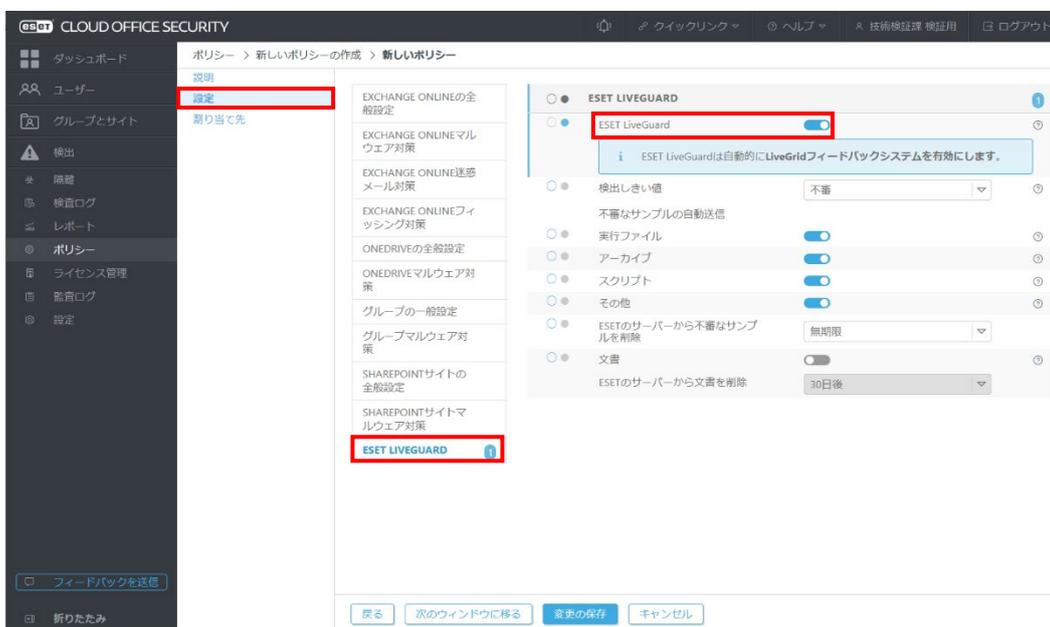
- ① ECOS ポータルより[ポリシー]をクリックし、画面下部の「新しいポリシー」ボタンをクリックします。



- ② [名前]に任意の名前を入力し、ポリシー設定とターゲットより「テナント」ボタンをクリックします。



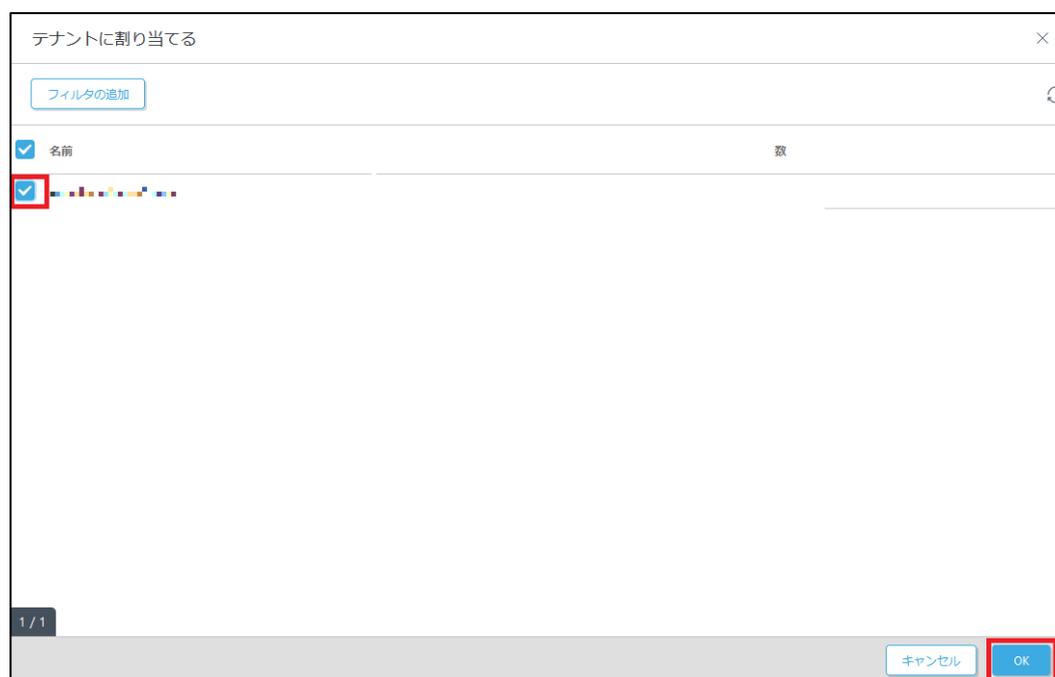
- ③ [設定]をクリックし、「ESET LIVEGUARD」を展開し[ESET LiveGuard]を有効にします。



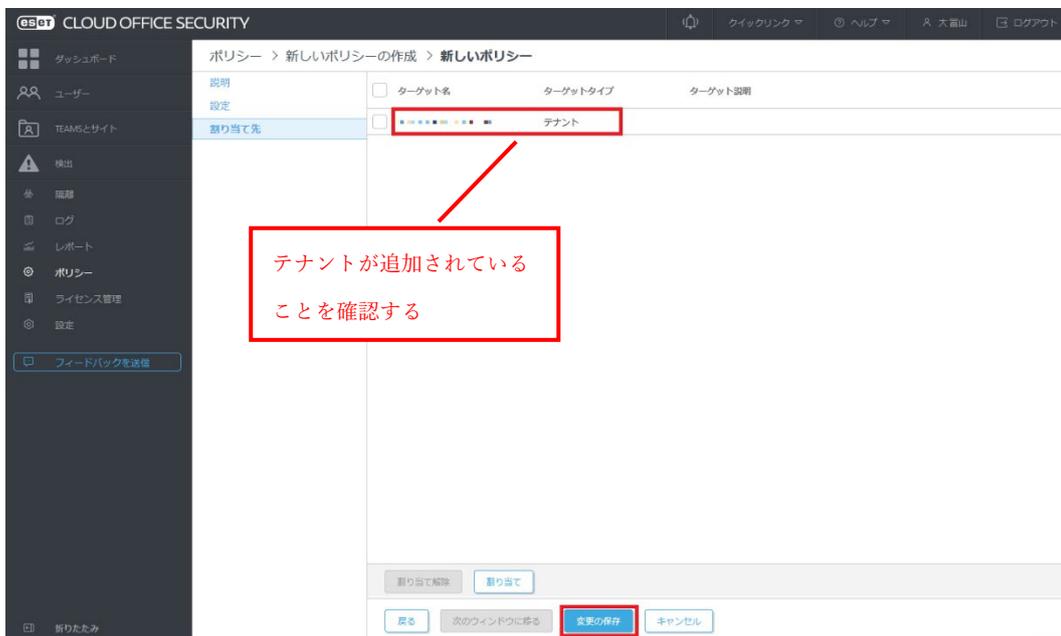
④ 「割り当て先」をクリックし、「割り当て」をクリックします。



⑤ テナントを選択し、「OK」をクリックします。



- ⑥ 割り当て先にテナントが入っていることを確認し、「変更の保存」をクリックします。



ワンポイント

LiveGuard Advanced を有効にすると自動的に LiveGrid フィードバックが有効になります。
別途 LiveGrid フィードバックを有効にする必要はありません。

2 グループとサイトの表示条件

ECOS では Teams とサイト画面でテナント内に存在するグループや SharePoint サイトの保護状態を確認できます。

グループ/SharePoint サイトの表示条件について以下に記載いたします。

2.1 グループ

[グループ]タブ内に表示される条件は以下の通りです。

- ・ Teams で作成されたチーム
- ・ SharePoint チームサイト
- ・ OneDrive サイト

ワンポイント

グループは Microsoft365 グループタイプのオブジェクトを表示します。

グループを保護するには、少なくとも一人のメンバーが ECOS によって保護されたユーザーであることを確認してください。

Microsoft 365 グループには SharePoint チームサイトと OneDrive があり、これらも保護されます。

2.2 SharePoint サイト

[SharePoint サイト]タブ内に表示される条件は以下の通りです。

- ・ SharePoint コミュニケーションサイト

3 ECOS のタイプ設定を利用する際の注意点

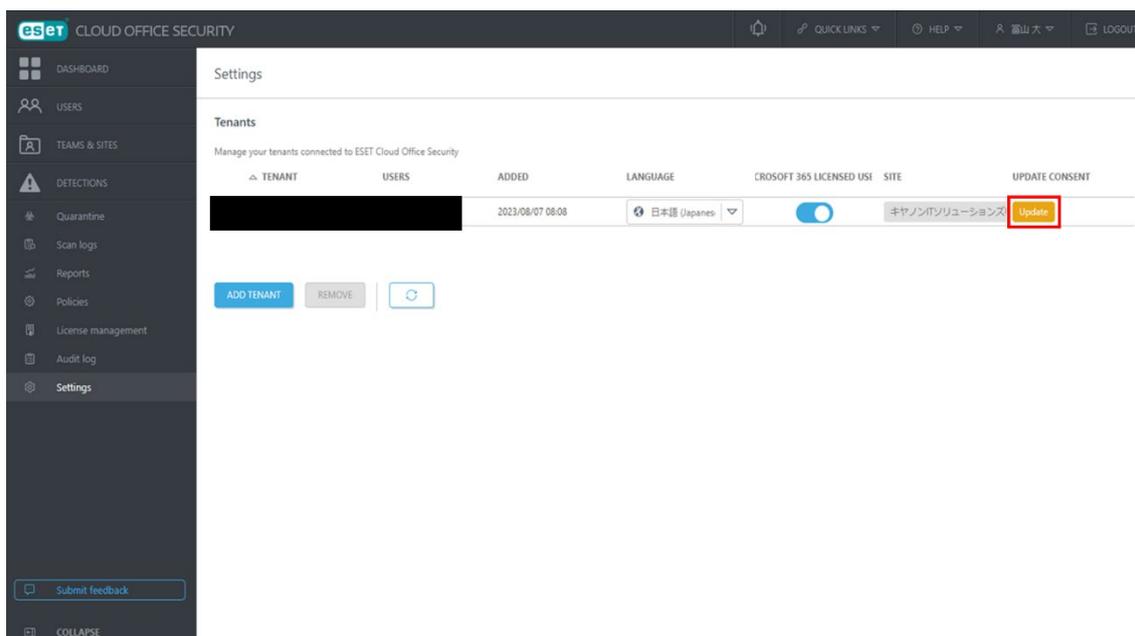
3.1 タイプ設定の有効化

ここでは、ECOS バージョン 342.5 以前より ECOS を利用している場合のタイプ設定を有効化する方法について記載いたします。

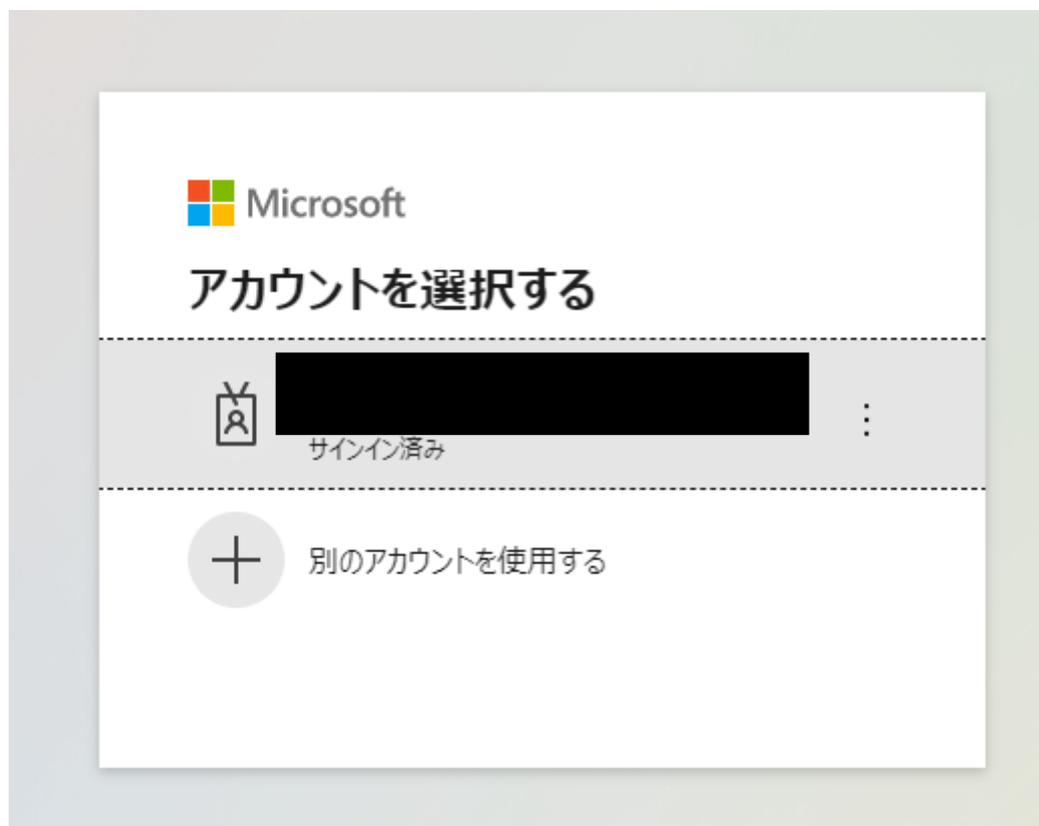
ワンポイント

ECOS バージョン 342.5 以降から ECOS をご利用されるお客様は本手順を行う必要はありません。

- ① ECOS ポータルより [Setting] をクリックし、画面上の「Update」ボタンをクリックします。



- ② 以下の画面が表示されたら、アカウントを表示します。



- ③ [承認]をクリックしてアクセス要求を承諾します。

要求されているアクセス許可 組織のレビュー

 ESET Cloud Office Security
ecos.eset.com

このアプリケーションは、Microsoft またはお客様の組織によって公開されたものではありません。

このアプリに必要なアクセス許可:

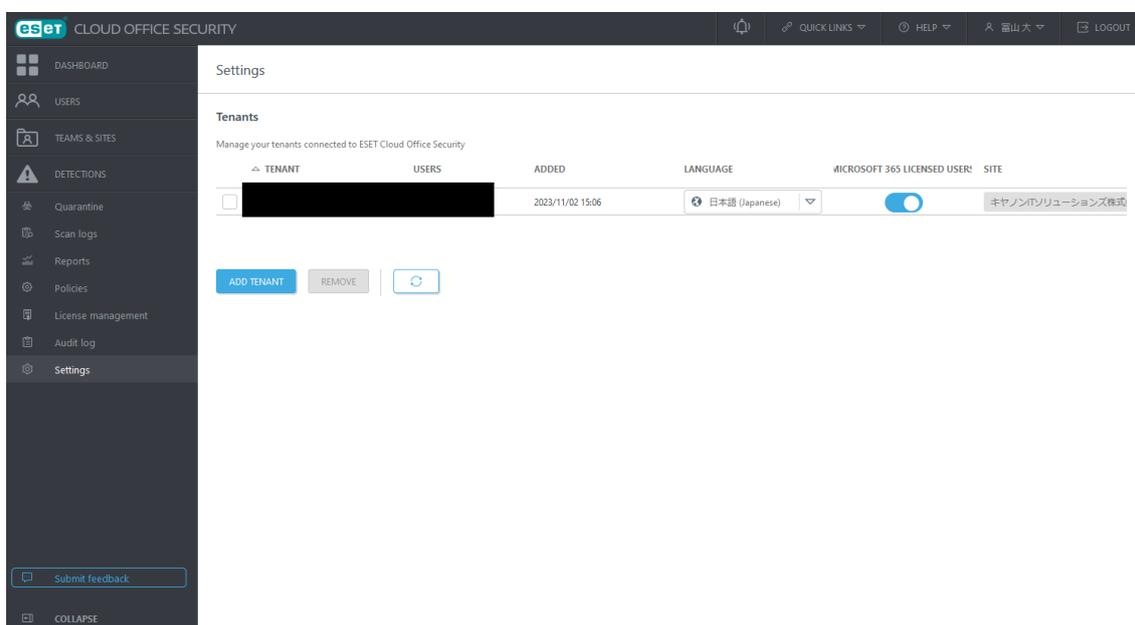
- ✓ Read and write all applications
- ✓ Read contacts in all mailboxes
- ✓ Read directory data
- ✓ Read and write directory data
- ✓ Read and write files in all site collections
- ✓ Read all groups
- ✓ Read all user mailbox settings
- ✓ Read and write mail in all mailboxes
- ✓ Read all hidden memberships
- ✓ Read all users' relevant people lists
- ✓ Create, edit, and delete items and lists in all site collections
- ✓ Read items in all site collections (preview)
- ✓ Read and write items in all site collections (preview)
- ✓ Read all users' full profiles
- ✓ サインインとユーザー プロファイルの読み取り

同意すると、このアプリは組織内のすべてのユーザーの指定のリソースにアクセスできるようになります。これらのアクセス許可の確認を求めるメッセージは、他のユーザーには表示されません。

これらのアクセス許可を受け入れることは、[サービス利用規約とプライバシーに関する声明](#)で指定されているとおりにこのアプリがデータを使用することを許可することを意味します。これらのアクセス許可は <https://myapps.microsoft.com> で変更できます。 [詳細の表示](#)

このアプリは疑わしいと思われませんか? [こちらでご報告ください](#)

④ 下記のように[Update]表記が消えたら本作業は完了です。



ワンポイント

タイプが表示されるまで最大で 24 時間かかる場合があります。

4 付録

4.1 お問い合わせ時に求められる情報

ここでは、本サービスのお問い合わせにおいて提供いただく必要のある情報について記載いたします。

お問い合わせ内容と以下記載の情報を合わせてご提示ください。

- ・利用している EBA または EPH アカウント名 (アドレス)
- ・ECOS に登録したテナント名 (ドメイン名)
- ・ECOS に登録したテナント ID

ECOS テナント ID については「[Azure Active Directory admin center](#)」より [Azure Active Directory] をクリックし表示される「テナント ID」を取得ください。