ESET PROTECTソリューション
Cloud Workload Protection機能について

第1版
2026年5月

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

1 .はじめに

近年、多くの企業が Amazon Web Services、Microsoft Azure、Google Cloud Platform（以降、それぞれAWS、Azure、GCPと表記）といったパブリッククラウド上で仮想マシン（以降、VMと表記）を活用しています。
クラウド上の VM は、オンプレミス環境のサーバーと同様に OS や業務アプリケーションが稼働しており、**マルウェアやランサムウェアといった脅威の性質自体は変わりません。**そのため、ESET PROTECT とエージェントを用いることで、クラウド環境においても VM を保護することは可能でした。
一方で、クラウド環境では VM の作成や削除が動的に行われるため、**VM の増減を把握し続けることや、保護対象として漏れなく管理することが運用上の課題**となりがちです。
ESET Cloud Workload Protection（CWP）は、**クラウドテナントと ESET PROTECT を連携することでクラウド上の VM を把握**し、必要に応じて **数クリックでエージェントおよびESET セキュリティプログラムを展開できる仕組み**を提供します。
これにより、オンプレミス環境で当たり前に行ってきたエンドポイント管理を、**クラウド環境でも無理なく実現可能**です。
本資料はESET PROTECTソリューションの以下の製品を対象としております。

製品名
ESET PROTECT Advanced
ESET PROTECT Complete
ESET PROTECT Elite
ESET PROTECT MDR
ESET PROTECT Enterprise

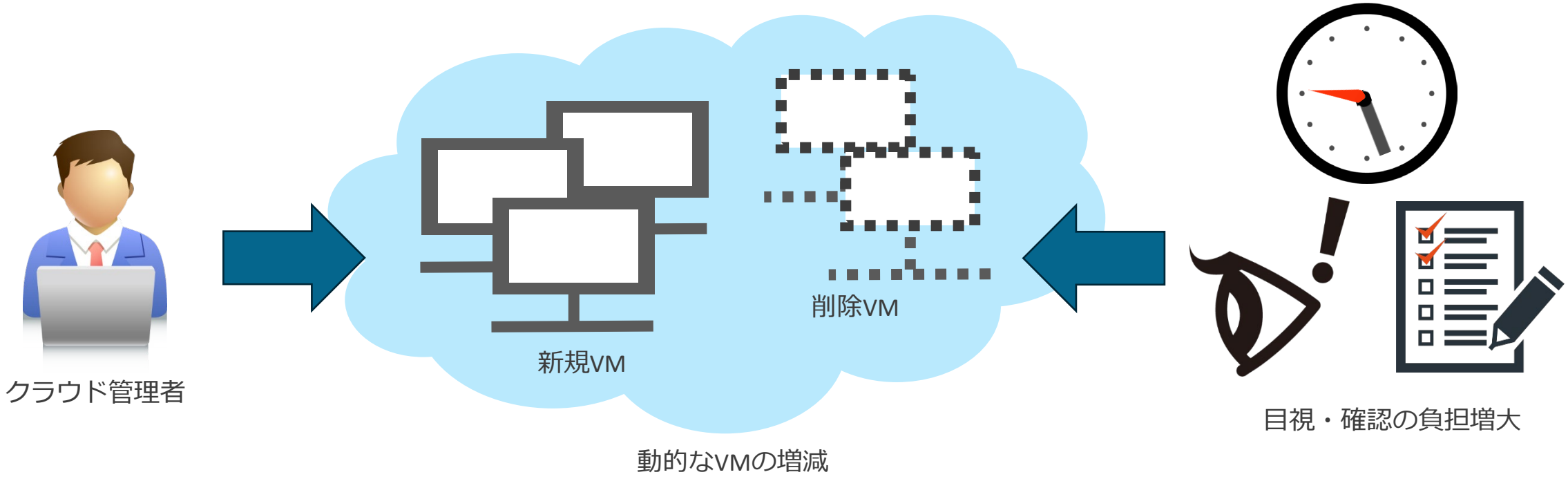
- 本資料は、本資料作成時のソフトウェア及びハードウェアの情報に基づき作成されています。
  ソフトウェアのバージョンアップなどにより、記載内容とソフトウェアに記載されている機能、名称及び画面などが異なっている場合があります。また、本資料の内容は将来予告なく変更することがあります。
- 本製品の一部またはすべてを無断で複写、複製、改変することはその形態に問わず、禁じます。
- ESET PROTECTは、ESET,spol. s r.o. の商標です。
- Microsoft Azure（Azure）は、米国Microsoft Corporationの米国、日本およびその他の国における登録商標または商標です。
- Amazon Web Services（AWS）は、Amazon.com, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。
- Google Cloud Platform（GCP）は、Google LLC の米国およびその他の国における商標または登録商標です。

2.クラウド環境特有の運用上の課題

2.クラウド環境特有の運用上の課題

(1) クラウド環境におけるVM運用の特徴

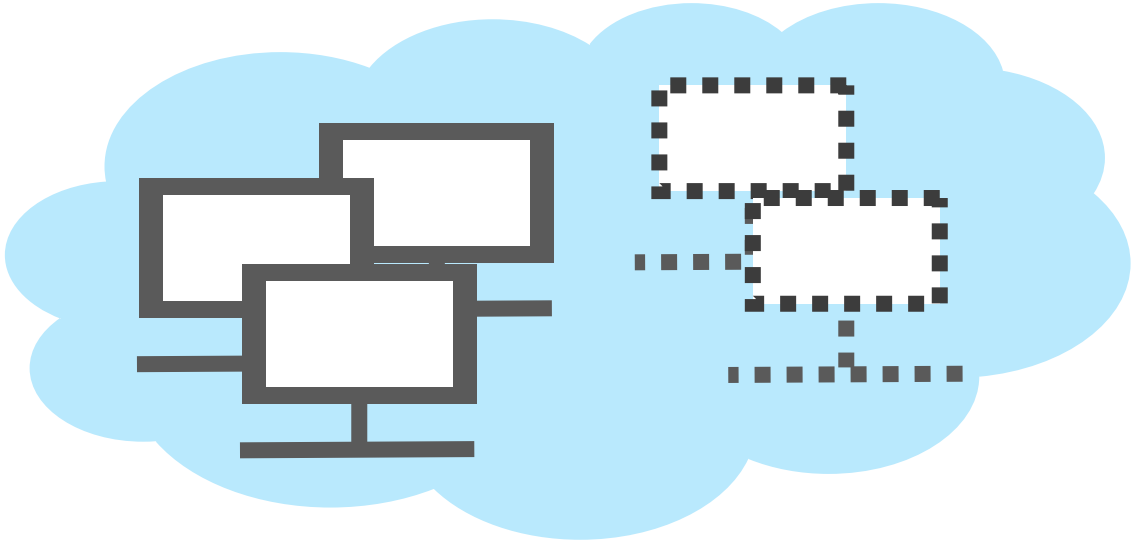
パブリッククラウド環境では、 VM はオンプレミス環境と比べて**より動的に作成・削除される**特徴があります。
オートスケールや自動化、IaC （Infrastructure as Code）の活用により、VM は人の操作を介さずに増減するケースも多く、その変化のスピードは年々高まっています。
このような環境では、一台一台の VM に対して個別に状況を確認し、セキュリティ対策を適用し続ける運用は、**管理者の手作業や気付きに依存しやすくなります。**
結果として、「守る仕組みは用意されているが、**VM の増減を把握し続けること自体が負担になる**」という状況が起こりやすくなります。
クラウド環境における課題は、新たな脅威が生まれたという点ではなく、**環境の変化に運用が追いつき続けることの難しさ**にあります。



2.クラウド環境特有の運用上の課題

(2) その変化を把握し続けられていますか？

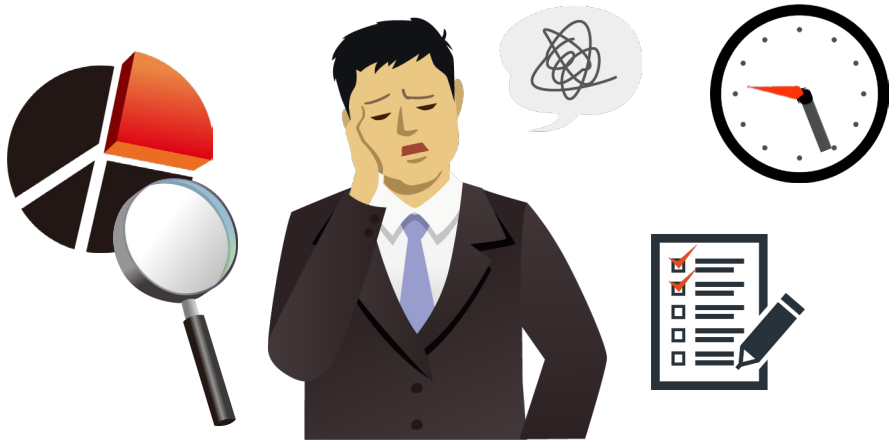
クラウド環境では、**VM が動的に増減することを前提とした運用が一般的**であり、
継続的な把握と確認が求められます。



動的なVMの増減

把握・確認が運用上の負担に

- ? 稼働中の VM をすぐに一覧できるか？
- ? VM の増減をいつ把握しているか？
- ? そのVMは確実に保護されているか？



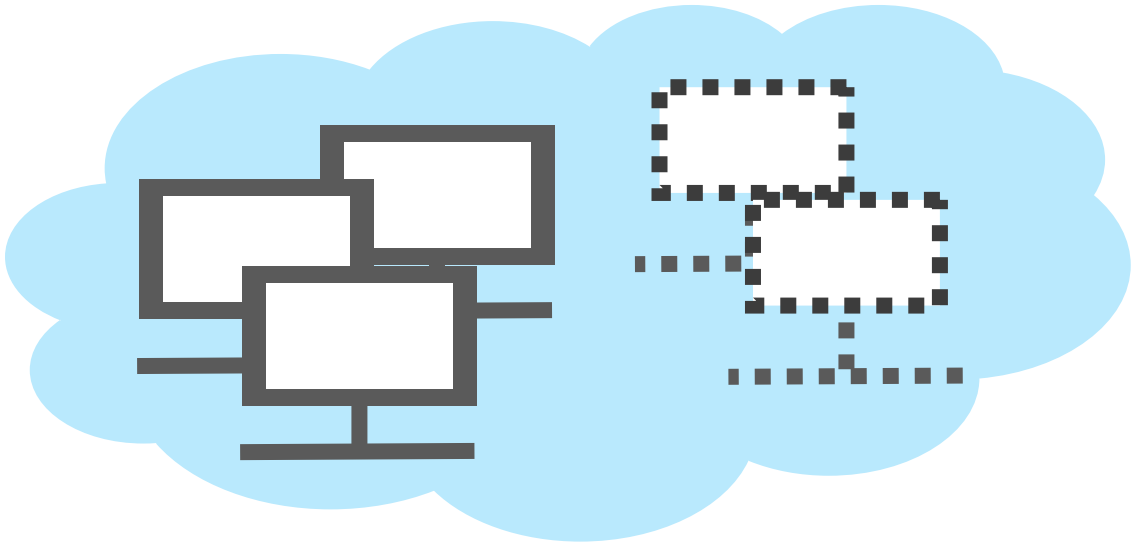
VMの増減を前提とした
新しい管理の考え方が必要です！

3. Cloud Workload Protection機能について

3.Cloud Workload Protection機能について

(1)Cloud Workload Protection機能とは

ESET Cloud Workload Protection（CWP）は、**クラウドテナントと ESET PROTECT を連携することでクラウド上の VM を把握**し、必要に応じて **数クリックでエージェントおよびESET セキュリティプログラムを展開できる仕組み**です。
これにより、オンプレミス環境で当たり前に行ってきたエンドポイント管理を、**クラウド環境でも無理なく実現可能**です。



動的なVMの増減

ESET
PROECT

EP経由で運用の負担を軽減

- ✓ 稼働中の VM を一覧可能
- ✓ VM の増減を把握可能
- ✓ VM の保護状態をチェック可能

3.Cloud Workload Protection機能について

(2)従来のEPによる端末管理について

従来のEPでは、管理したい端末に対して、初めのステップとしてESET Managementエージェント（EMエージェント）を導入する必要がありました。

ESET PROTECT（EP）

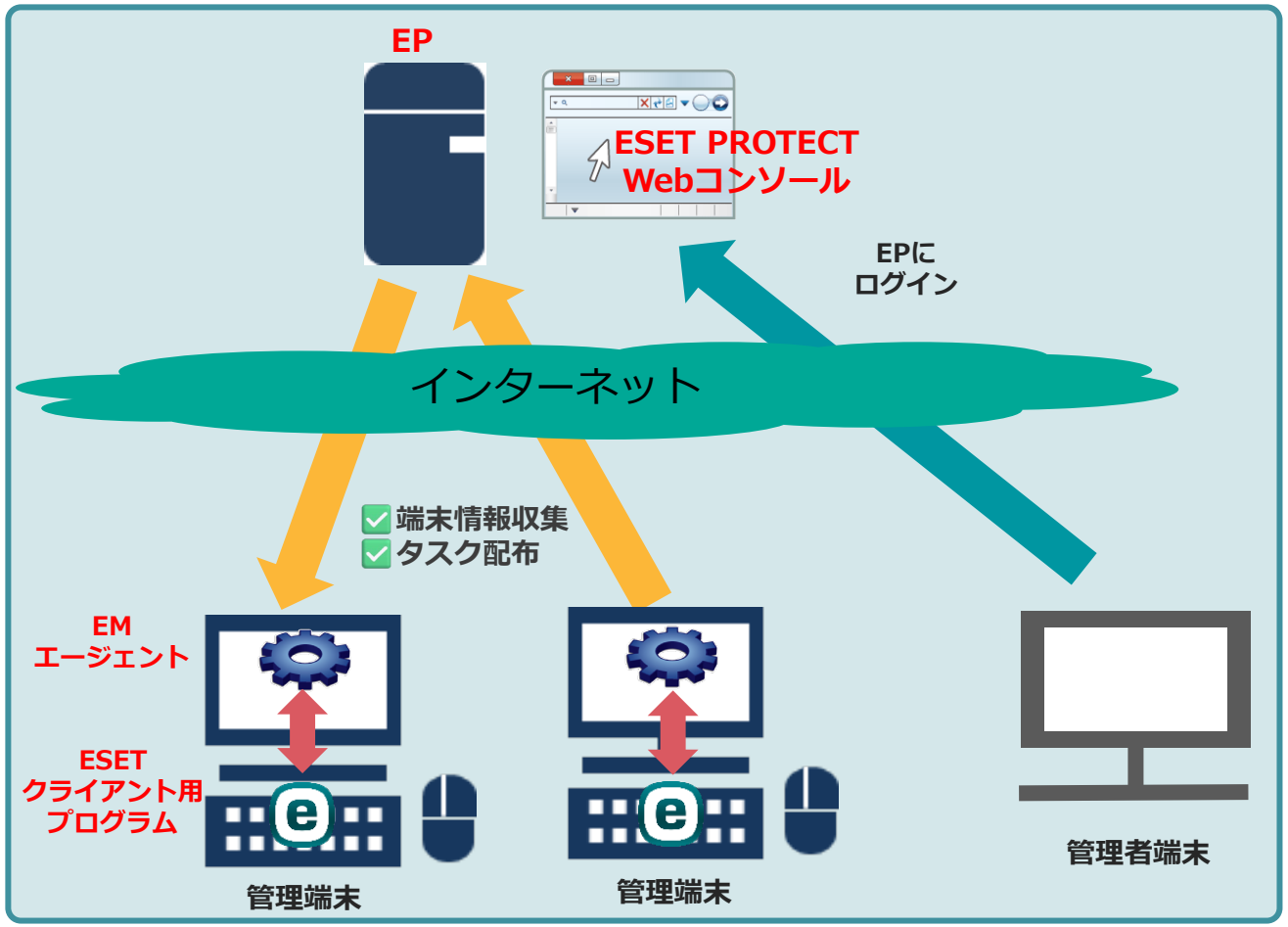
EPはクライアントプログラムの情報収集やタスク配布などを行います。クライアントとの通信はエージェント経由で行います。

ESET PROTECT Webコンソール

WebコンソールはWebベースのインターフェースであり、ブラウザーを使用してEPへアクセスします。ブラウザー経由でクライアント情報の閲覧やタスクの実行などを行うことができます。

ESET Managementエージェント（EM エージェント）

エージェントは、クライアントから情報を収集し10分間隔でEPへデータを送信します。また、EPからのタスク配布などはエージェントへ送信されたのち、エージェントがクライアントへ送信します。

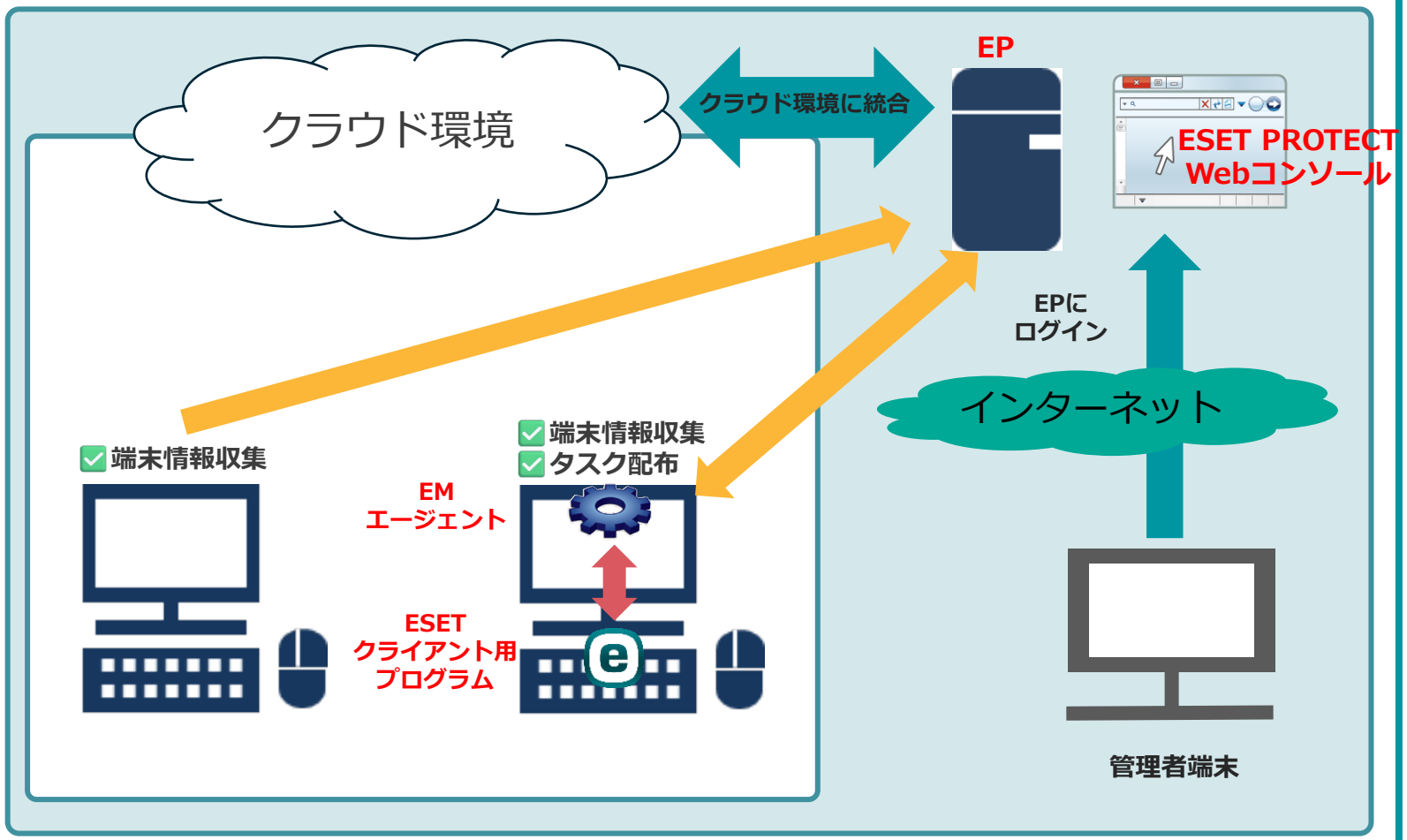


3.Cloud Workload Protection機能について

(3)CWPによる端末管理について

CWP機能を利用してEPとクラウド環境（Azure、AWS、GCP）を統合することによって、クラウド環境で管理されている端末が**EMエージェントなしでもEPで管理可能になりました**（※ただし、EMエージェントで管理されている端末に対して、一部の端末情報収集のみ可能です）。

さらに、指定した端末やグループに対して、**数クリックでEMエージェントとESETクライアント用プログラムを展開することが可能**です。

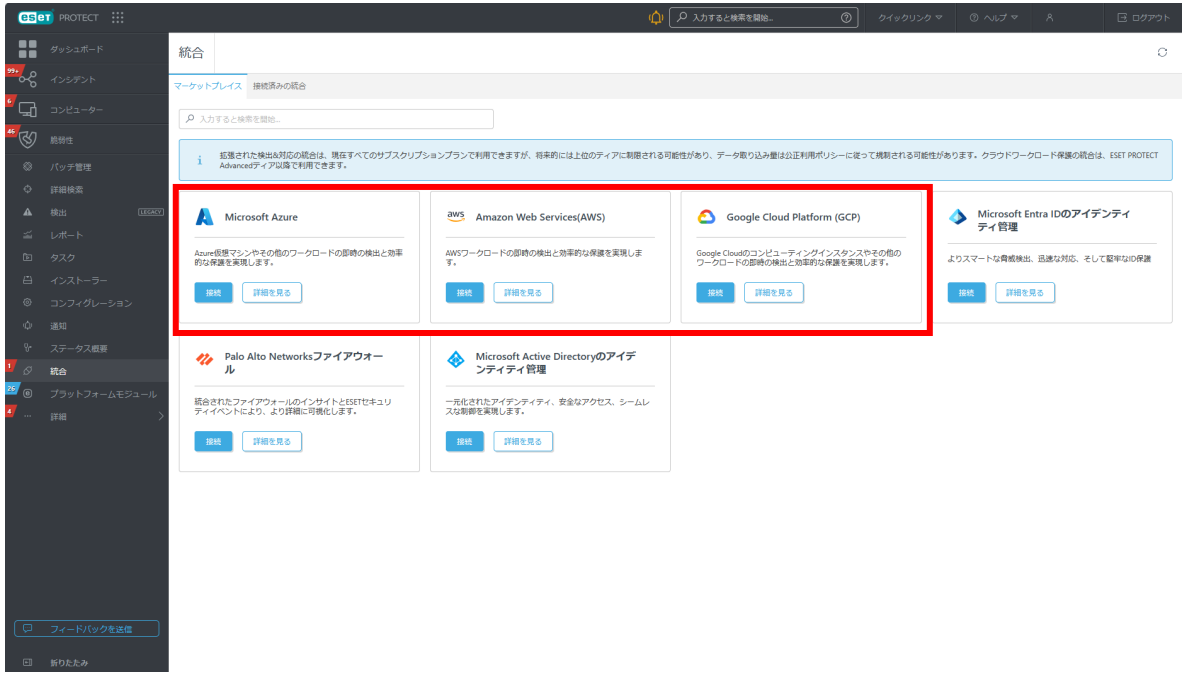


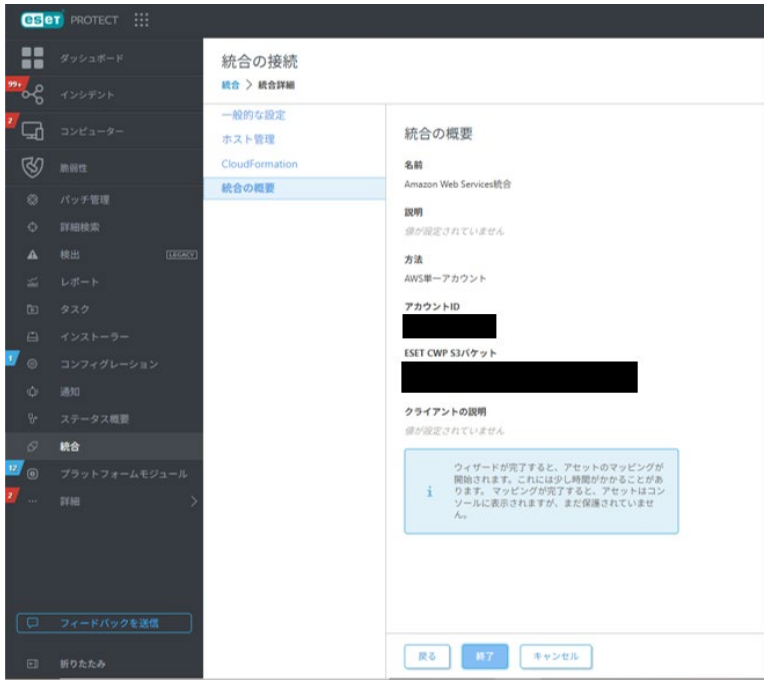
4. Cloud Workload Protectionの有効化手順

4. Cloud Workload Protectionの有効化手順

(1)EPとクラウド環境の統合

CWP機能をご利用いただくには、ESET PROTECTとクラウド環境（Azure、AWS、GCP）の統合が必要です。
ESET PROTECT Webコンソールのマーケットプレイスから、EPに統合したいクラウド環境を設定します。
□手順：
「統合」メニューより、クラウド環境（AWS / Azure / GCP）の「接続」を選択してクラウド環境の情報を入力



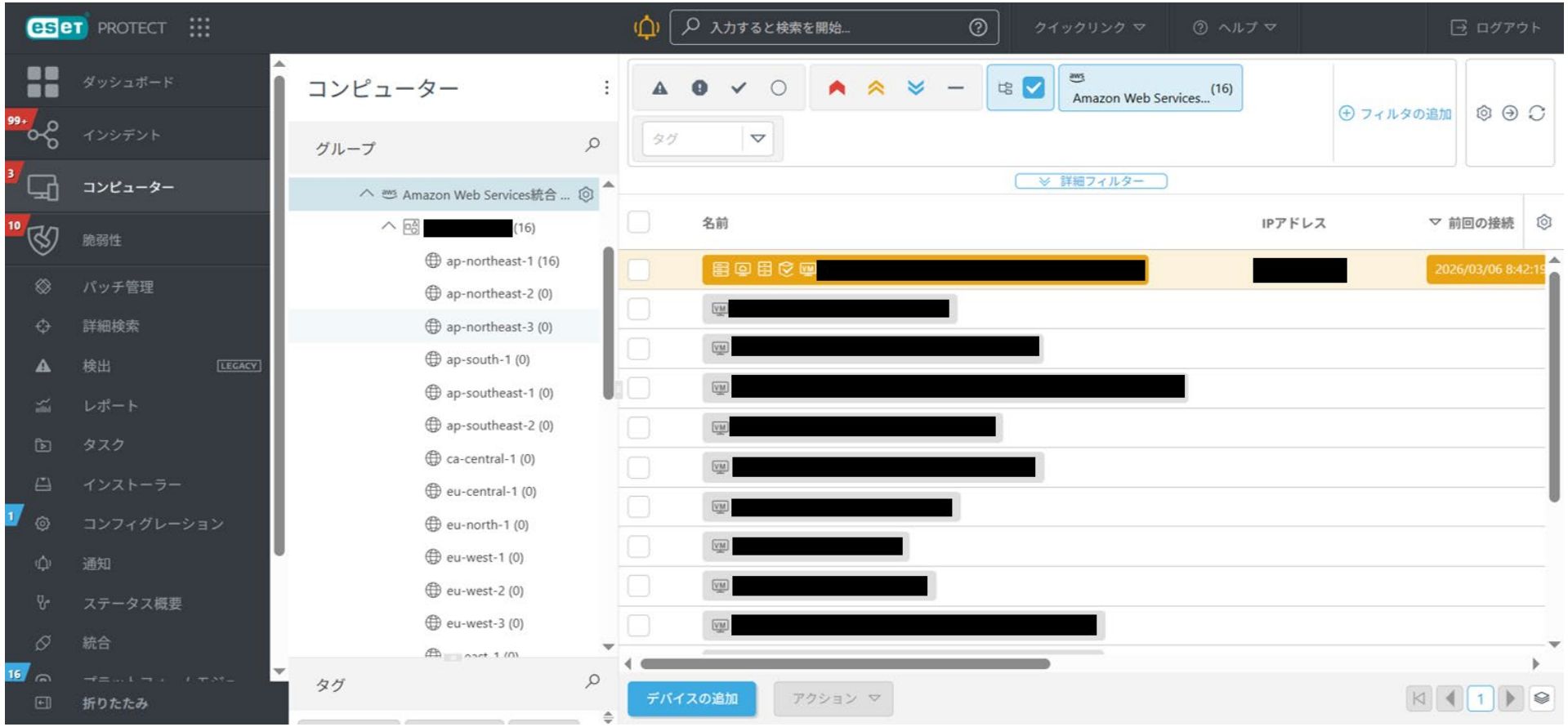


各クラウド環境で必要な設定の詳細は以下のオンラインヘルプをご参照ください。
https://help.eset.com/protect_cloud/ja-JP/?integrations.html

4. Cloud Workload Protectionの有効化手順

(2)クラウド環境のVMの一覧

統合が完了すると、コンピューター一覧にクラウド環境で管理されている端末（VM）一覧が表示されます。
さらに、クラウド環境と定期的に同期されるため、**端末の増減にも手作業なく追随可能**です。



4. Cloud Workload Protectionの有効化手順

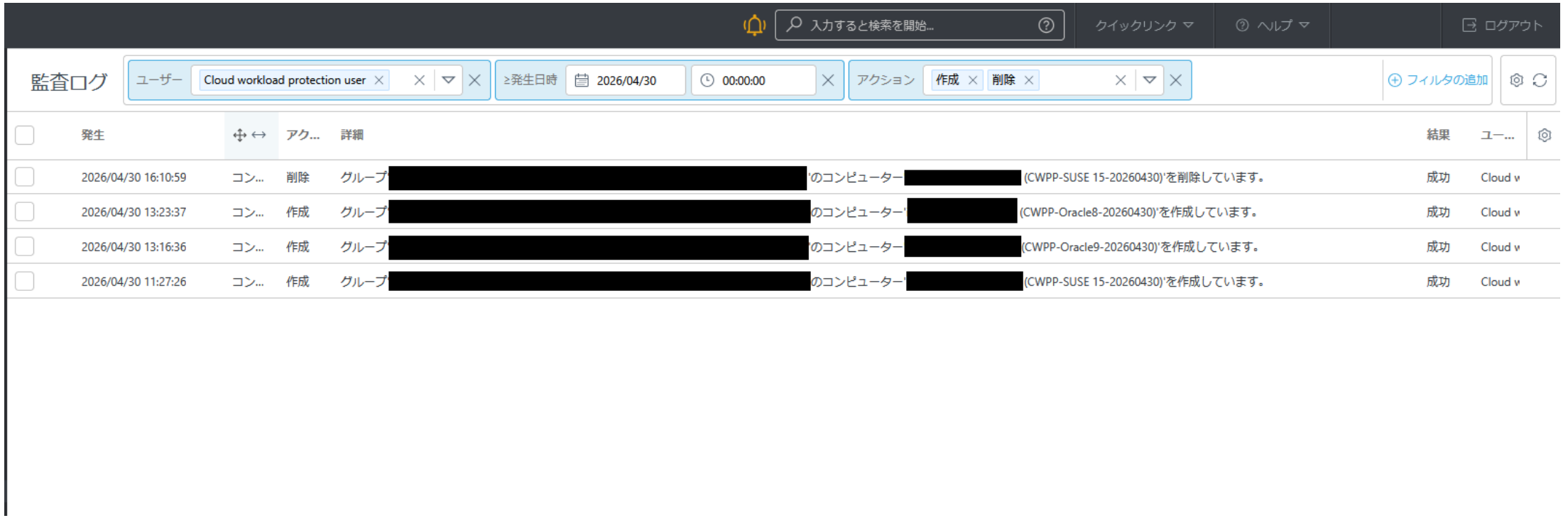
(3)VMの情報把握

EMエージェントを導入していないVMでも、一部の端末情報を閲覧することが可能です。

4. Cloud Workload Protectionの有効化手順

(4)VM増減の追跡

クラウド環境のVMの増減については、監査ログをフィルタリングすることで追跡が可能です。
例：・ユーザーを「Cloud workload protection user」に限定
　　・アクションを「作成」「削除」に限定



4. Cloud Workload Protectionの有効化手順

(5)クラウドワークロードの展開　- グループ単位で実行する場合 -

「クラウドワークロードの展開」は、指定したVMやグループに対して、数クリックでEMエージェントとESETクライアント用プログラムを展開可能な機能です。
・グループ単位で実行する場合（本手順）
・VM単位で実行する場合（P17）
・指定グループに自動で展開する場合（P18）

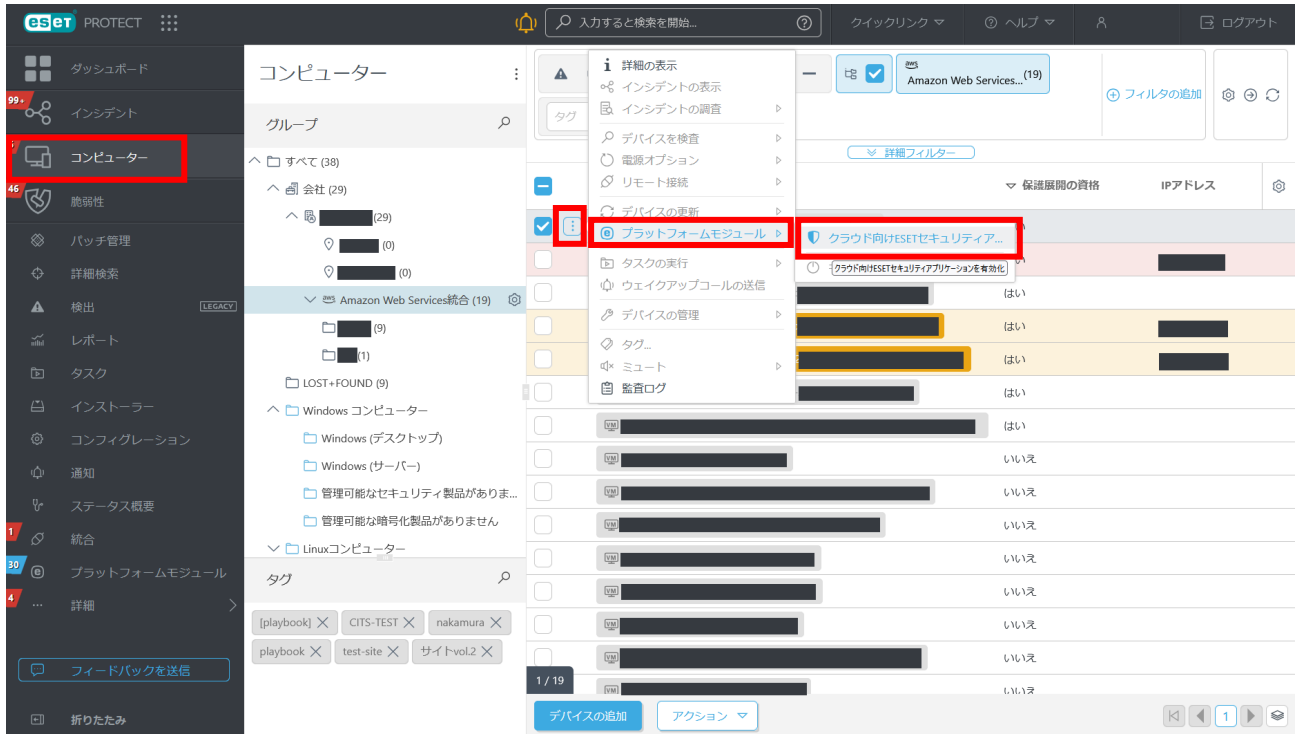
①ESET PROTECTメインメニューの[プラットフォームモジュール]を選択し、クラウドワークロードの展開の[有効]をクリックします。

②ターゲットグループを選択し、法的文書に同意（チェック）の上、[有効]をクリックします。

4. Cloud Workload Protectionの有効化手順

(6)クラウドワークロードの展開　- VM単位で実行する場合 -

①ESET PROTECTメインメニューの[コンピューター]-[VMの：メニュー]-[プラットフォームモジュール]-[クラウド向けESETセキュリティアプリケーションを有効化]をクリックします。

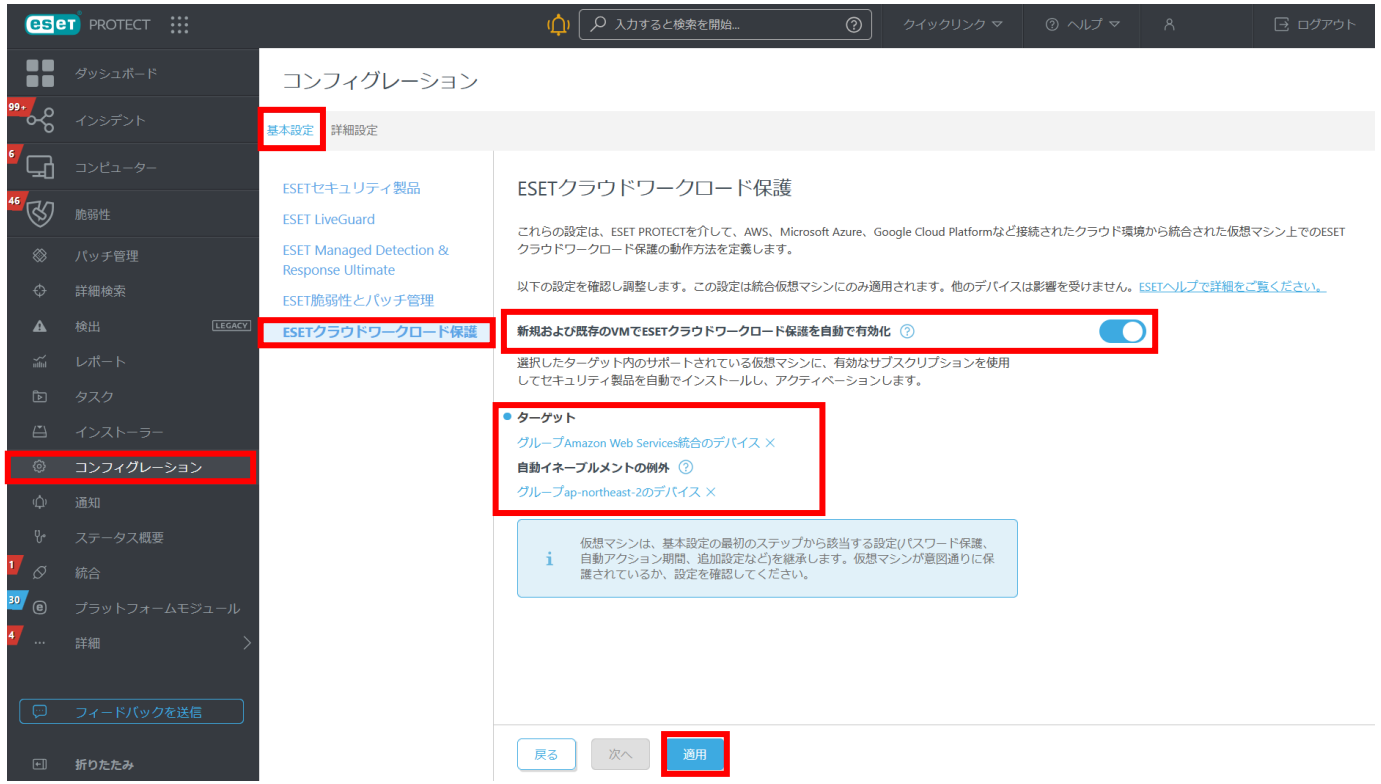


②ターゲットグループを確認し、法的文書に同意（チェック）の上、[有効]をクリックします。

4. Cloud Workload Protectionの有効化手順

(7)クラウドワークロードの展開　– 指定グループに自動で展開する場合 -

①ESET PROTECTメインメニューの[コンフィグレーション]-[基本設定]-[ESETクラウドワークロード保護]を選択します。
②「新規および既存のVMでESETクラウドワークロード保護を自動で有効化」のトグルをONにします。
③ターゲットグループ、また、必要に応じて「自動イネーブルメントの例外」のグループ（ターゲットグループ配下のサブグループ）を選択し、[適用]をクリックします。



5. 参考情報

5. 参考情報

参考情報

○ Cloud Workload Protection の有効化に必要な設定の詳細については、以下のオンラインヘルプをご参照ください。
https://help.eset.com/protect_cloud/ja-JP/?integrations.html

○「クラウドワークロードの展開」が可能なVMの要件については、以下のFAQを参照ください。
https://eset-support.canon-its.jp/faq/show/34272?site_domain=business