ESET PROTECT MDR Lite

エンドポイント見守りサービス × クラウド型統合ID管理（IDaaS）

端末監視 × クラウドサービスの不正アクセスを防ぎます

Cybersecurity
Progress. Protected.

狙われるエンドポイントとID

近年、エンドポイントから流出した認証情報（IDやパスワード）などを悪用し、Microsoft 365などのクラウドサービスに不正アクセスするサイバー攻撃が増加しています。

エンドポイントのマルウェア感染 ▶ 認証情報の窃取 ▶ クラウドサービスへの不正アクセス ▶ クラウドサービスからの情報漏えい

エンドポイントを守る「ESET PROTECT MDR Lite」

侵入後の対策（XDR）だけでなく、エンドポイント保護も対象とした包括的な監視体制を構築。運用はESET／キヤノンMJグループのエンジニアが代行し、組織のセキュリティ強化を支援します。

予防・検知・対応をする **セキュリティツール** ＋ セキュリティエンジニアによる **監視・運用サービス**

監視体制
24時間・365日お客様環境を監視・分析

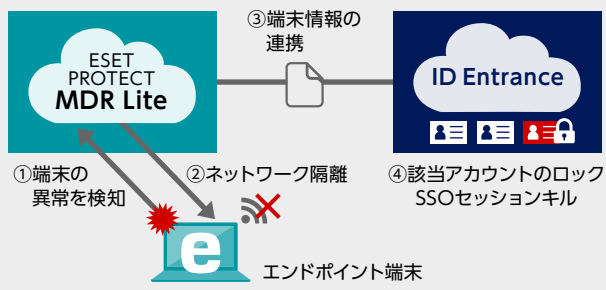
インシデント対応
平均6分で初動対応を実施

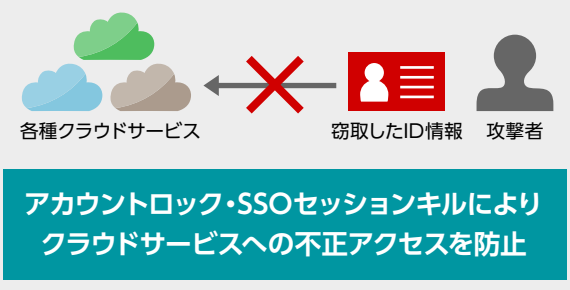
レポート提供
モニタリング結果の
集計レポートを利用可能（週次／月次）

日本語でのサポート
WEBシステムより
24時間・365日お問い合わせ可能

IDaaSとの連携ソリューション

- ESETで端末の異常を検知し脅威であると判断すると、端末をネットワークから隔離します。
- ネットワーク隔離をトリガーに、IDaaS（※）で自動的に該当アカウントをロック・シングルサインオン（SSO）セッションを切断。クラウドサービスへの不正アクセスを防止します。





アカウントロック・SSOセッションキルにより クラウドサービスへの不正アクセスを防止

※IDaaS ― ID・パスワードを管理するクラウドサービス
※IDaaS連携対象製品は「ID Entrance」です。

IDaaSの機能について、詳しくは裏面へ

ID Entrance

クラウド型統合ID管理（IDaaS）によるセキュリティ強化

アカウントの一元管理やアクセス権の制御を実現します

IDを守る「ID Entrance」

クラウドサービス（SaaS）の利用が拡大する中、アカウントやアクセス権の管理は煩雑化しており、クラウド上の機密情報を適切に管理することが重要です。ID Entranceは、クラウドサービスのアカウントを一元管理し、アクセス権を制御することで、ユーザーの利便性向上に加え、管理負荷の軽減とセキュリティ対策の強化を実現します。また、ESETと連携することで、万が一インシデントが発生した場合でも、迅速なアカウント対処が可能となり、クラウド侵害や情報漏えいを防ぎます。

シングルサインオン

一度のログインで複数のサービスにアクセスでき、
利便性の向上に繋がります。
クラウドサービスや社内システム等に対応しています。

アクセス制御

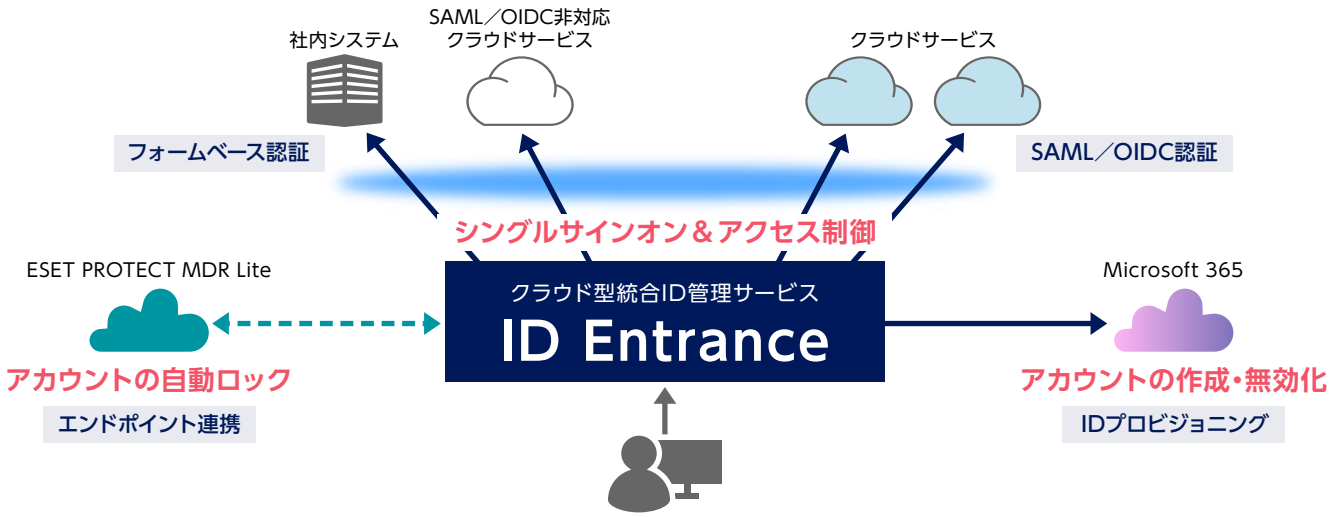
ログイン条件を柔軟に設定することで適切なユーザーの
アクセスを制限できます。クライアント証明書やワンタイムパスワード、
IPアドレス制限など、多様な認証機能を提供します。

アカウントの自動ロック

ESET PROTECT MDR Liteと連携し、自動でアカウントロック・
シングルサインオンのセッションの切断を実施し、
クラウドサービスからの情報漏えいや、不正アクセスを防ぎます。

アカウントの作成・無効化

ID Entranceに登録されているアカウント情報をもとに、
連携したクラウドサービス（Microsoft365）に対して
アカウントの作成・無効化が可能です。



年額 1,800円～（1ユーザーあたり） ※月額換算150円～利用可能！

製品に関する情報はこちらでご確認いただけます。

セキュリティソリューション ホームページ
canon.jp/it-sec

●お求めは信用のある当社で

Canon キヤノンマーケティングジャパン株式会社
〒108-8011 東京都港区港南2-16-6 CANON S TOWER

2026年3月現在
EID2603CMJS-PDF