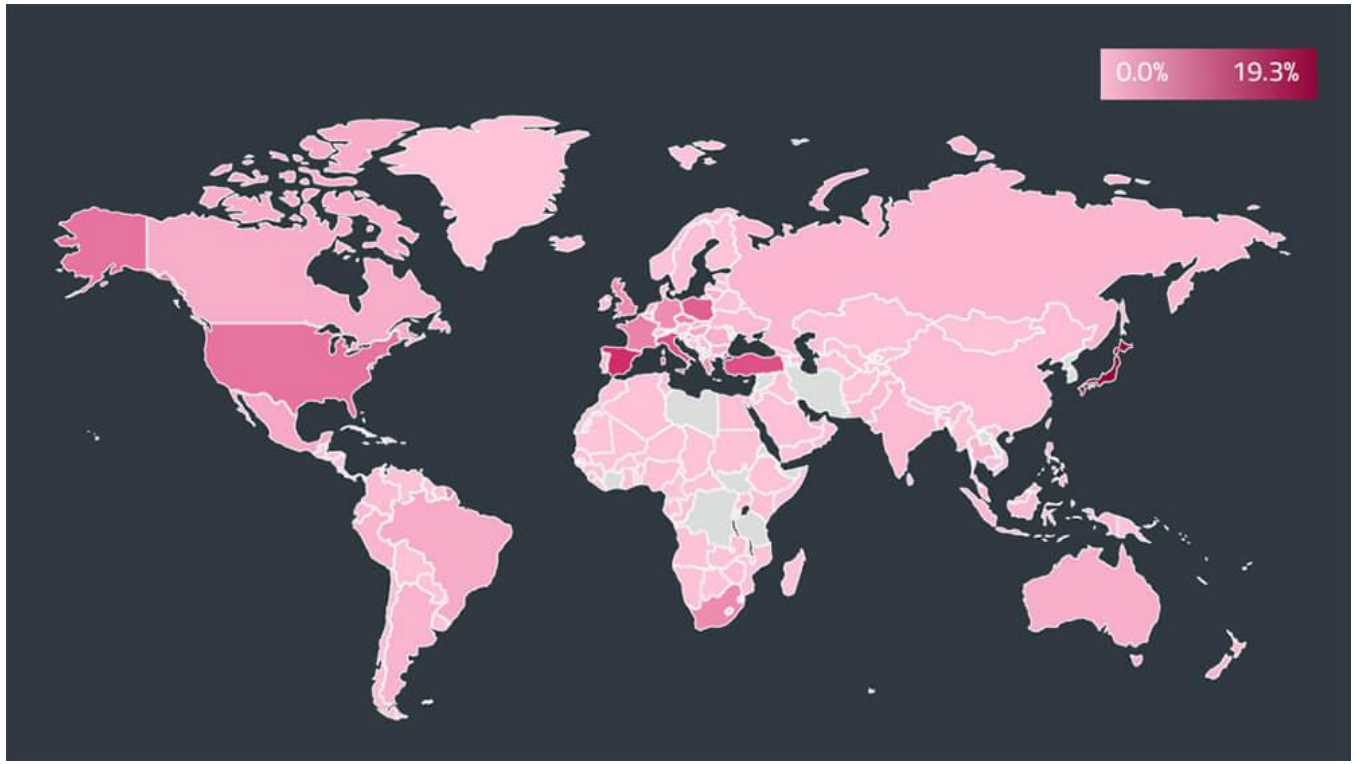
脅威動向から見る、
エンドポイントセキュリティ対策の最適解

2021年9月15日

キヤノンマーケティングジャパン株式会社
植松　智和

Canon

不正なメールの検出



不正なメールの検出分布

第1位 日本 19.3%

第2位 スペイン 7.6%

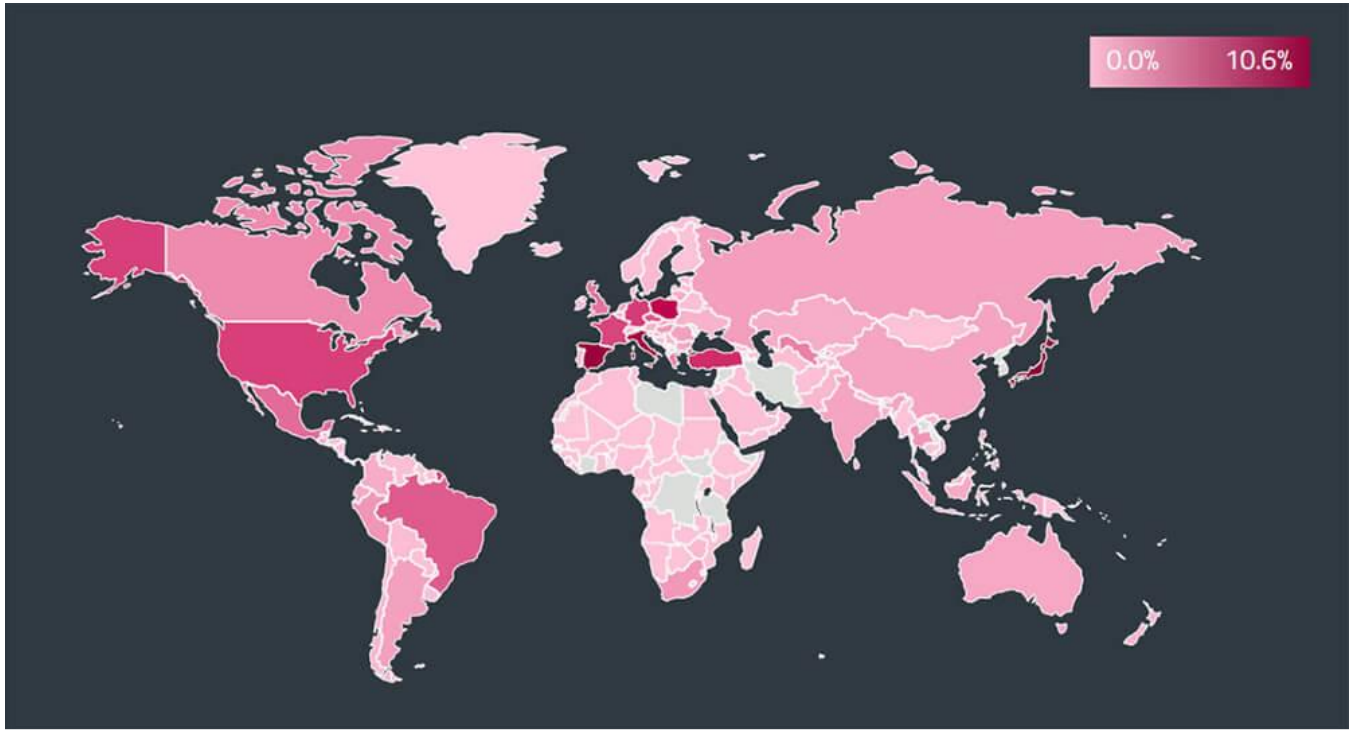
第3位 トルコ 5.8%

第4位 イタリア 5.5%

第5位 ポーランド 5.0%

出典：ESET, spol. s r.o.「ESETサイバーセキュリティ脅威レポート 2021年第1三半期版」 調査期間：2021年1月～4月
https://www.eset.com/jp/blog/threat-report/2021-t1/

ダウンローダーの検出



ダウンローダーの検出分布

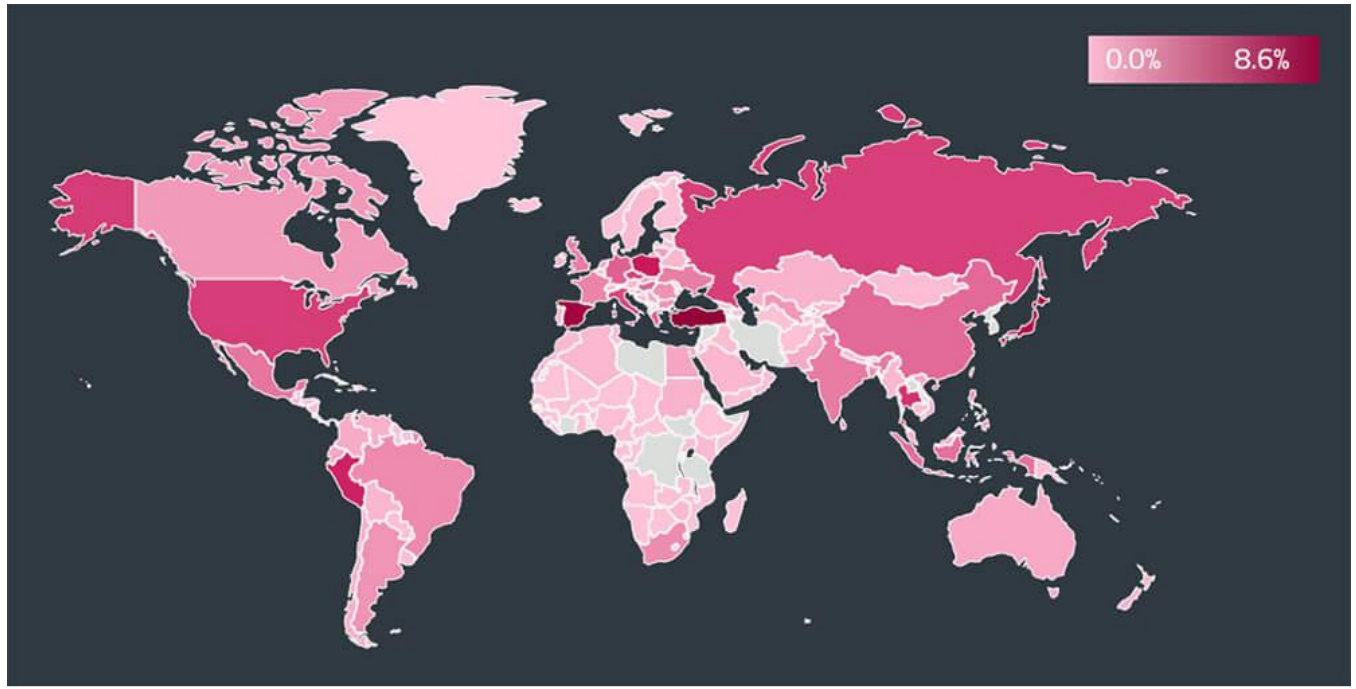
第1位 日本 10.6%

第2位 スペイン 9.7%

第3位 イタリア 8.5%

出典：ESET, spol. s r.o.「ESETサイバーセキュリティ脅威レポート 2021年第1三半期版」 調査期間：2021年1月～4月
https://www.eset.com/jp/blog/threat-report/2021-t1/

情報窃取マルウェアの検出



情報窃取マルウェアの検出分布

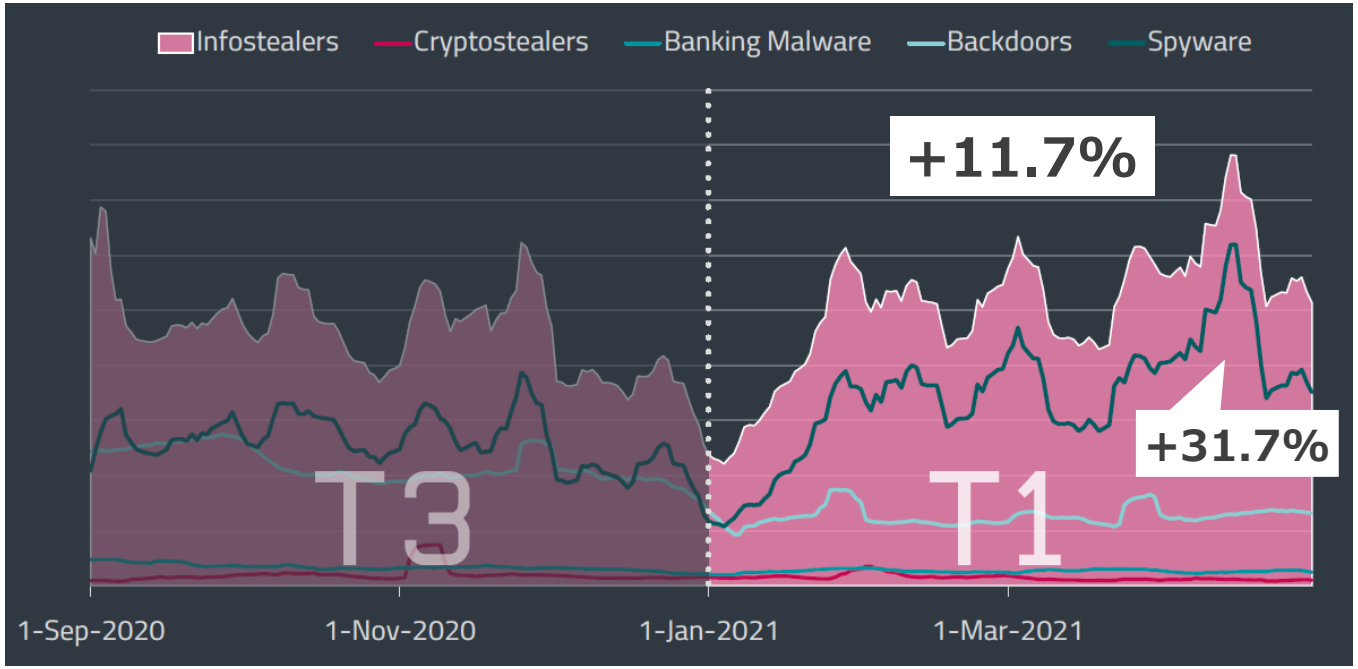
第1位 トルコ 8.6%

第2位 スペイン 7.2%

第3位 日本 5.6%

出典：ESET, spol. s r.o.「ESETサイバーセキュリティ脅威レポート 2021年第1三半期版」 調査期間：2021年1月～4月
https://www.eset.com/jp/blog/threat-report/2021-t1/

増加する情報窃取マルウェア



前期比+11.7%

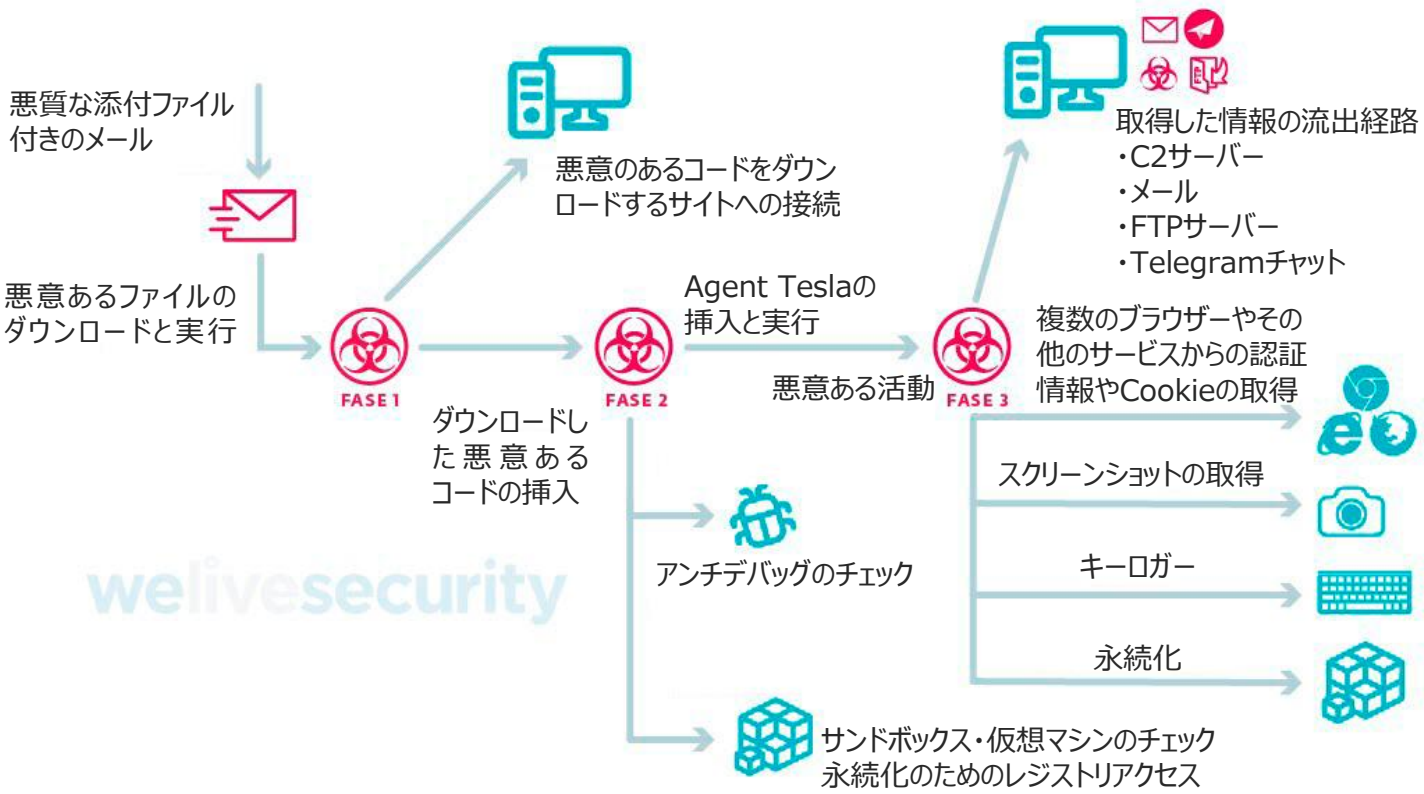
うち、スパイウェア+31.7%

その他のマルウェアは減少

¼を占めるAgentTesla

出典：ESET, spol. s r.o.「ESETサイバーセキュリティ脅威レポート 2021年第1三半期版」 調査期間：2021年1月～4月
https://www.eset.com/jp/blog/threat-report/2021-t1/

攻撃者に絶大な人気を誇るAgentTesla



2014年から活動するRAT

高機能

- キーロガー、スクリーンショット
- 複数の窃取対象ソフト
- 複数の手法での外部送信

利用のしやすさ

- MaaS
- 15-69

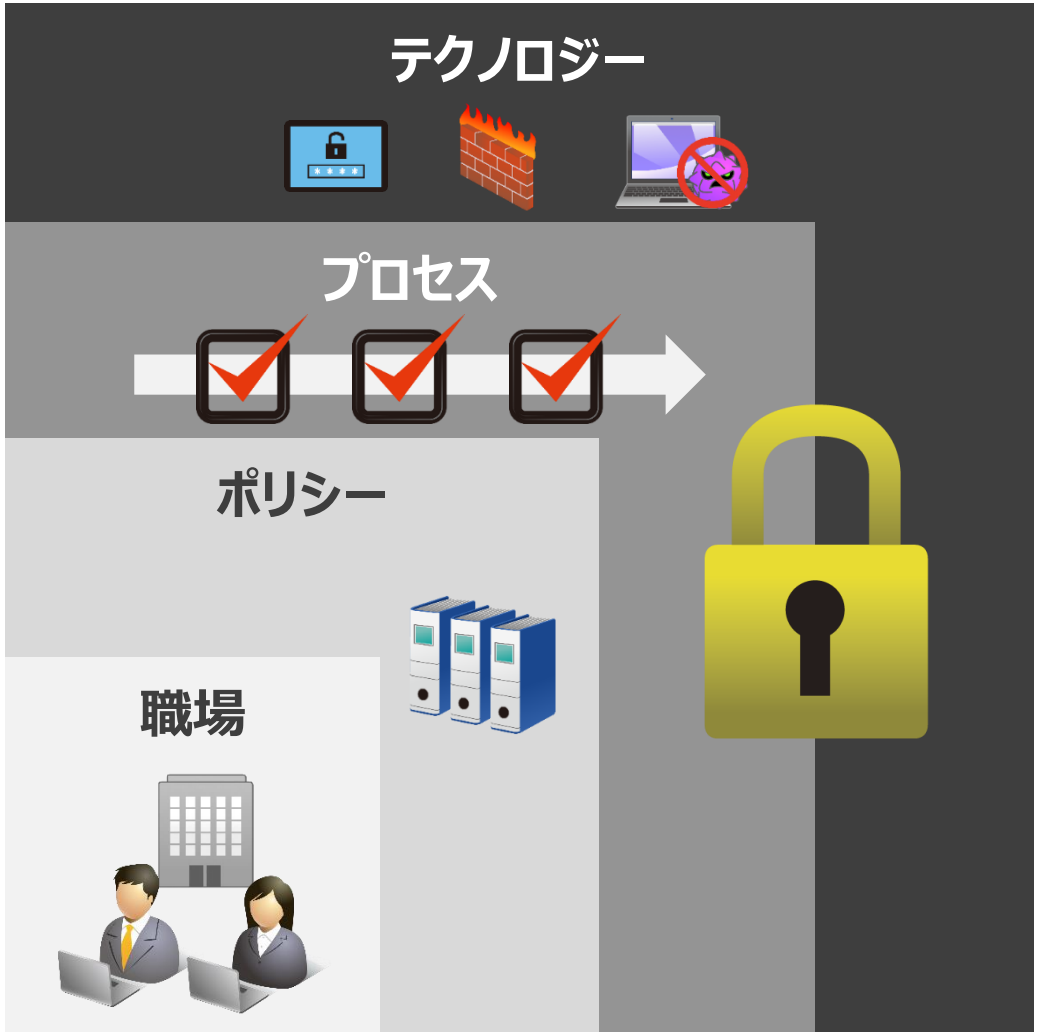
出典：ESET, spol. s r.o.「Agent Tesla: principales características de este malware」を翻訳
https://www.welivesecurity.com/la-es/2021/04/28/agent-tesla-principales-caracteristicas-este-malware/

テレワークの実施

58.9%

出典：IPA「テレワークにおける実施およびルール策定の 状況、実施に伴う業務委託に関する不安に関する調査結果」
https://www.ipa.go.jp/about/press/20201224.html

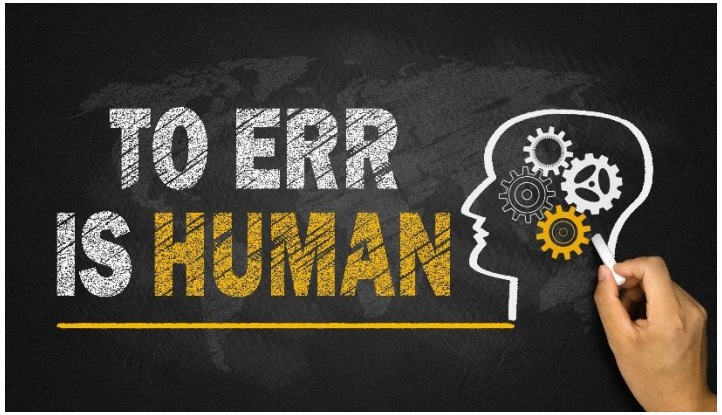
テレワークに潜むリスク



従業員そのものが死角に

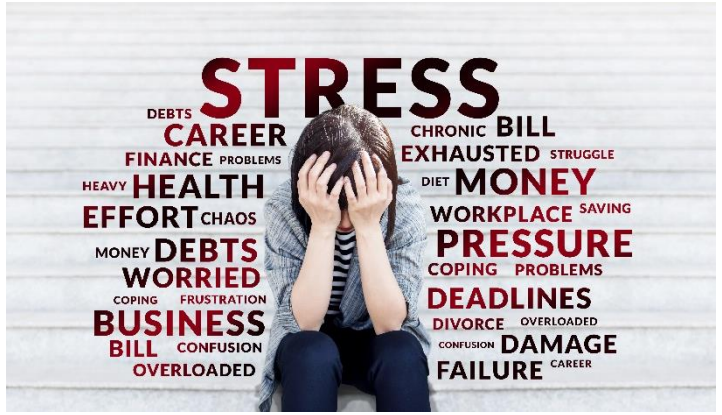
+63%

ロックダウンが始まってから起きた
サイバー犯罪



80%

人的要因によって引き起こされる
サイバーセキュリティリスクの増大



47%

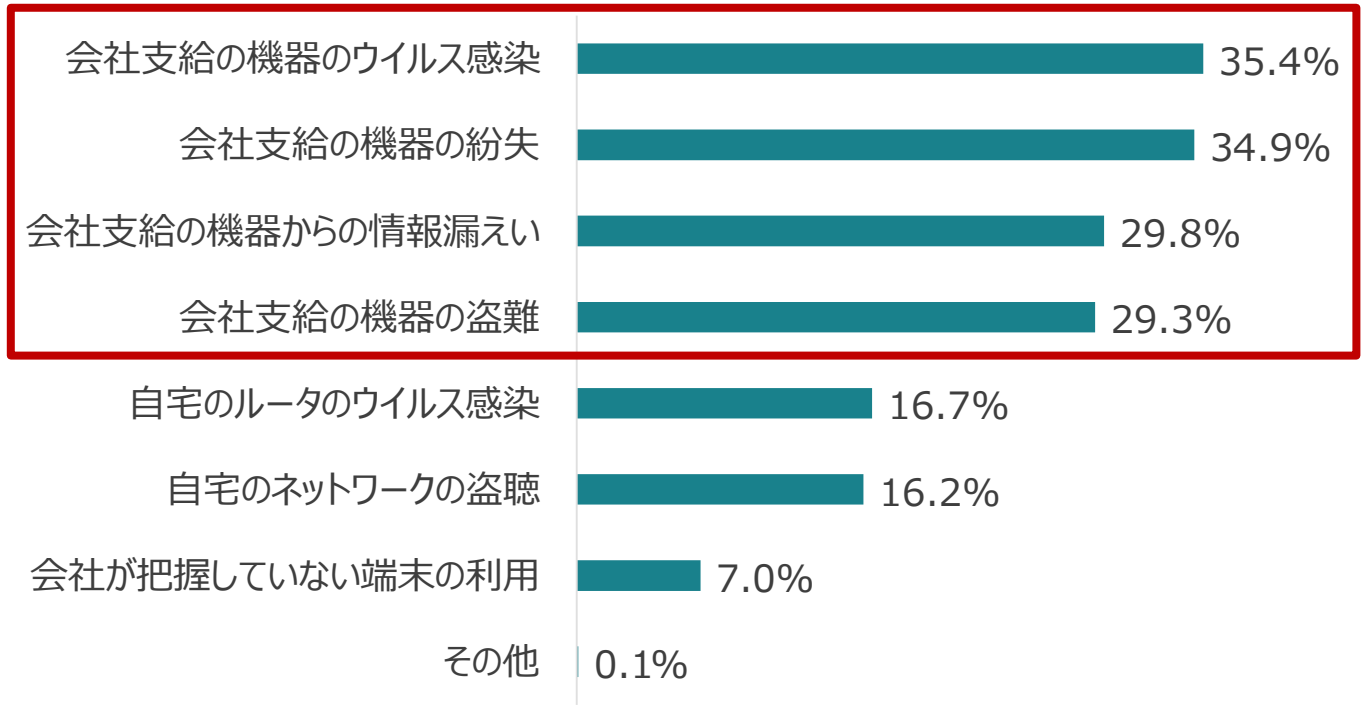
COVID-19危機時の
ストレス管理に対する不安

性格により異なるストレス耐性：パニック、注意力低下、スリルを求める、etc…
→不用意な開封・クリック、違反の未報告

出典：ESET, spol. s r.o.「Cyberchology, The Human Element of Cybersecurity」
https://www.eset.com/uk/business/cyberchology/

自分の責任に不安

自分の責任になってしまうのではないかと
不安のあるセキュリティインシデント



出典：IPA「ニューノーマルにおけるテレワークとITサプライチェーンのセキュリティ実態調査 個人編 中間報告」
https://www.ipa.go.jp/about/press/20201224.html

ウイルス感染
紛失・盗難
情報漏洩

不安・ストレスは
国内でも同様

攻撃者にも起きている”ジョブ型”の波

リモートアクセス・ブローカー

システム・サーバーへの認証情報を販売
情報窃取マルウェア、フィッシング、スパム

初期アクセス・ブローカー

高レベルのアクセス権を販売
初期アクセス、偵察、特権昇格、ツール導入

ランサムウェア・アフィリエイト

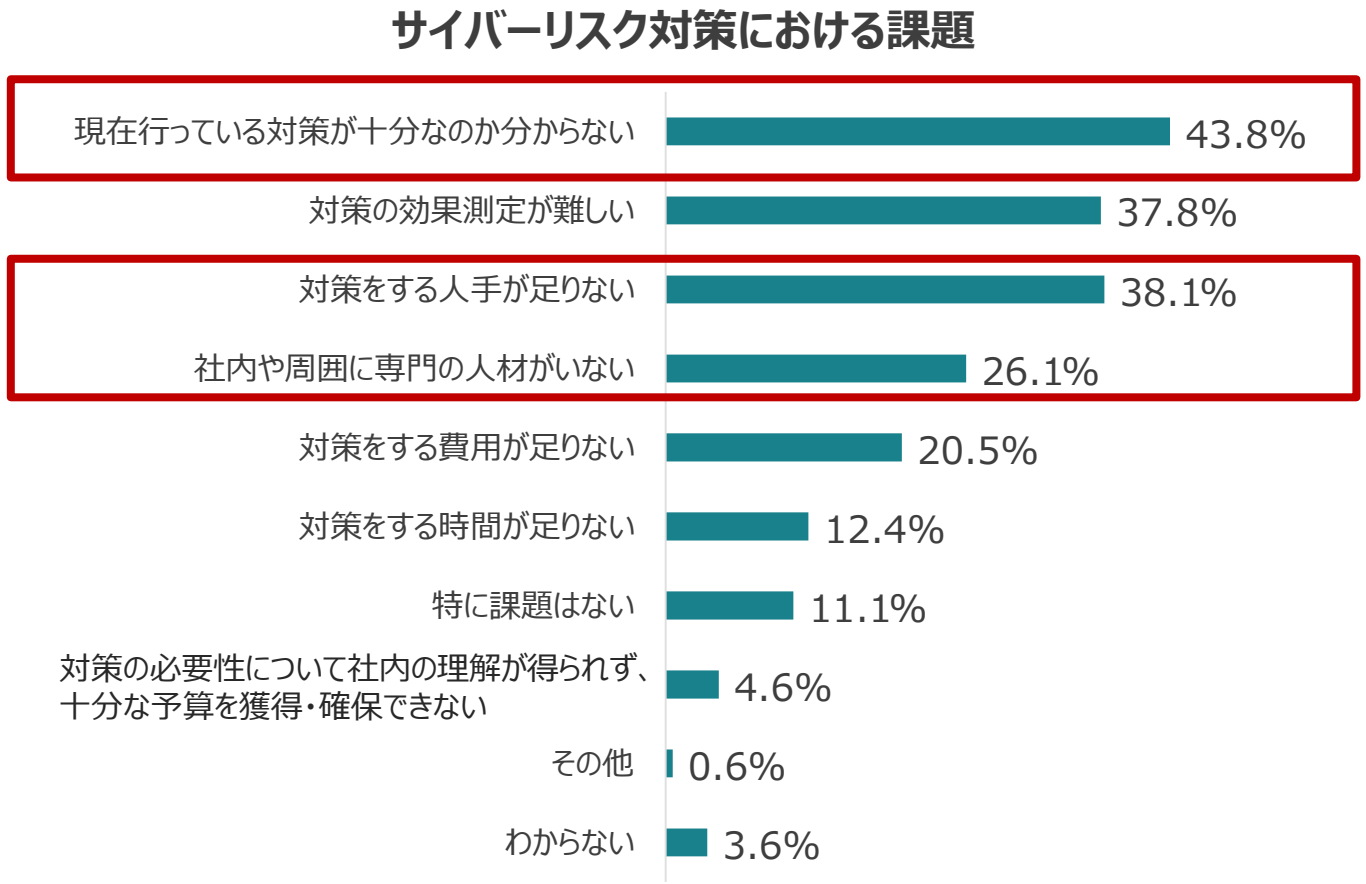
ランサムウェア攻撃の実行役
横展開、情報窃取、暗号化、脅迫

ランサムウェア・オペレーター、開発者

ランサムウェアインフラ、ソフトウェアの開発、提供
被害者との交渉

分業、専門性
攻撃のサプライチェーン化

対策に悩む経営者、管理者



判断はより難しくなった

人手・人材不足に懸念

出典：一般社団法人 日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査2020」
https://www.sonpo.or.jp/cyber-hoken/data/2020-01/

狙われる日本企業

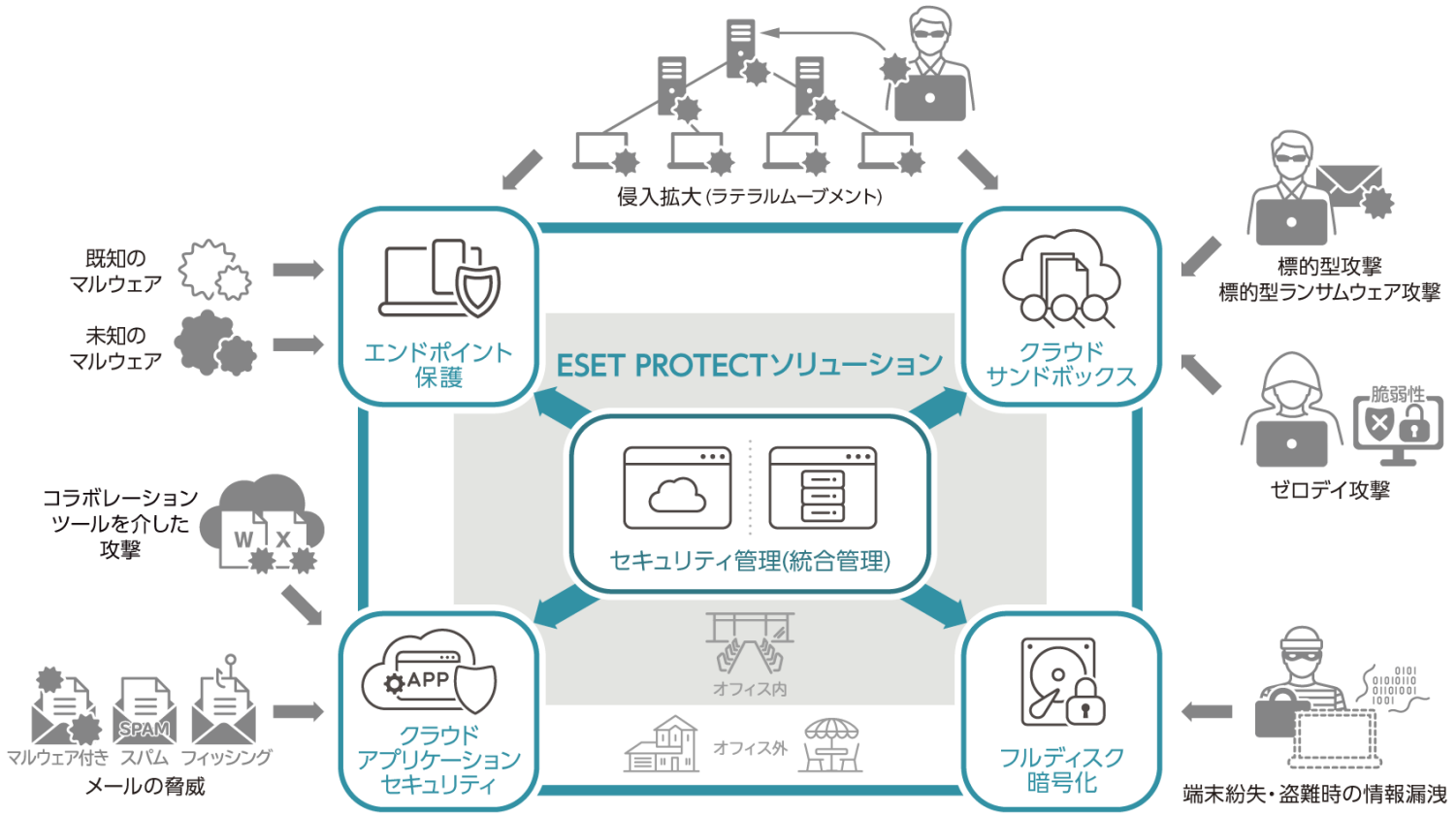
テレワークの脆弱性、人の脆弱

対策には自信も人材も足りない


Solution
Problem

ESET PROTECTソリューション

各種対策をパッケージ化した包括的なセキュリティ対策



ESET PROTECTソリューションラインアップ

標的型攻撃や情報漏洩などへの包括的な対策、リモートワークを含む社内外の端末管理など、ニーズにあわせて8種のソリューションをラインアップ

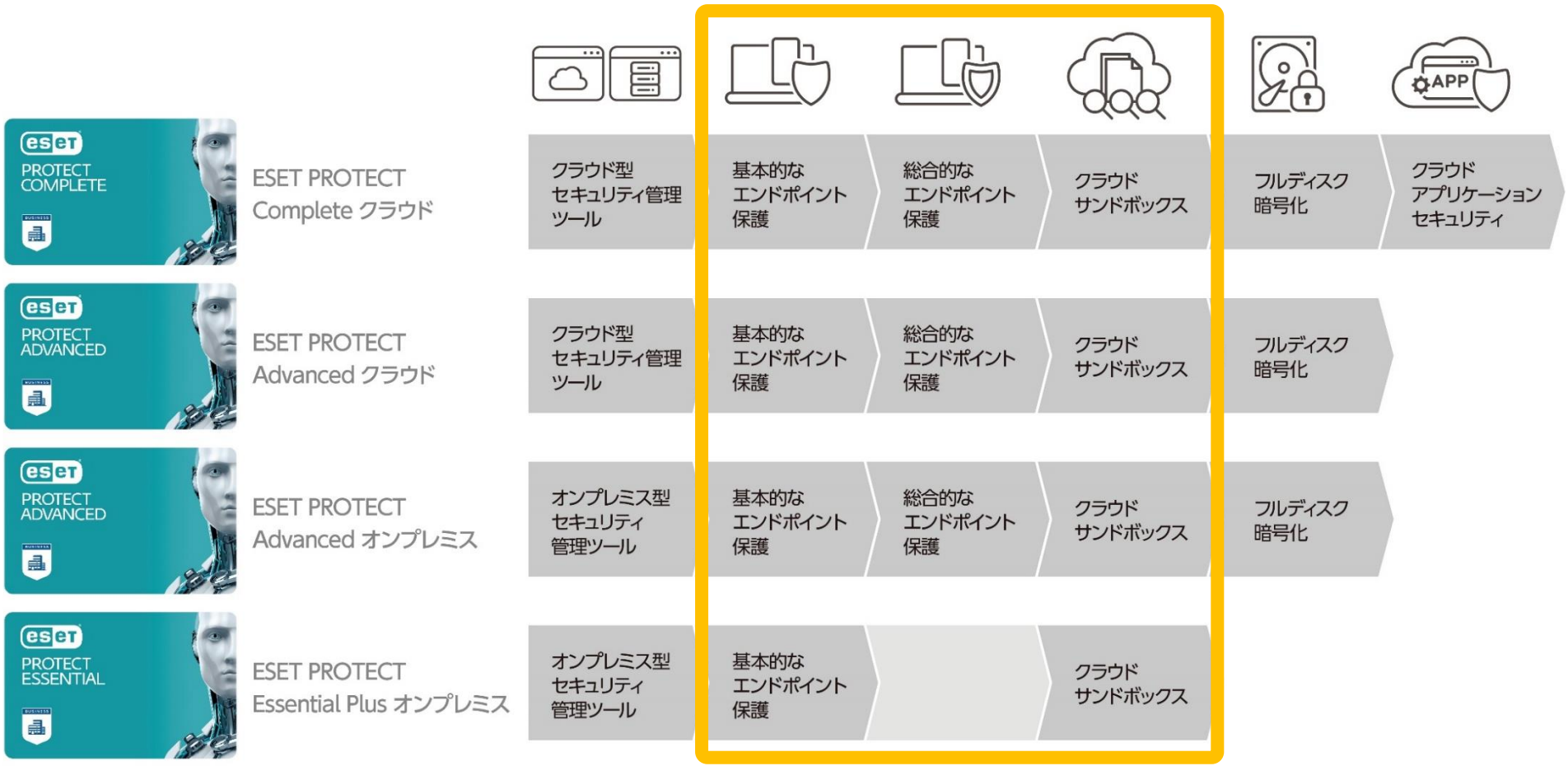
	クラウドでのセキュリティ管理	オンプレミスでのセキュリティ管理
中堅・大企業向け (100名以上)	 **ESET PROTECT Complete** クラウド	 **ESET PROTECT Advanced** オンプレミス
	 **ESET PROTECT Advanced** クラウド	 **ESET PROTECT Essential Plus** オンプレミス
中小企業向け (99名以下)	 **ESET PROTECT Entry** クラウド	 **ESET PROTECT Entry** オンプレミス (旧名称：ESET Endpoint Protection Advanced)
	 **ESET PROTECT Essential** クラウド	 **ESET PROTECT Essential** オンプレミス (旧名称：ESET Endpoint Protection Standard)

中堅・大企業向けラインアップ

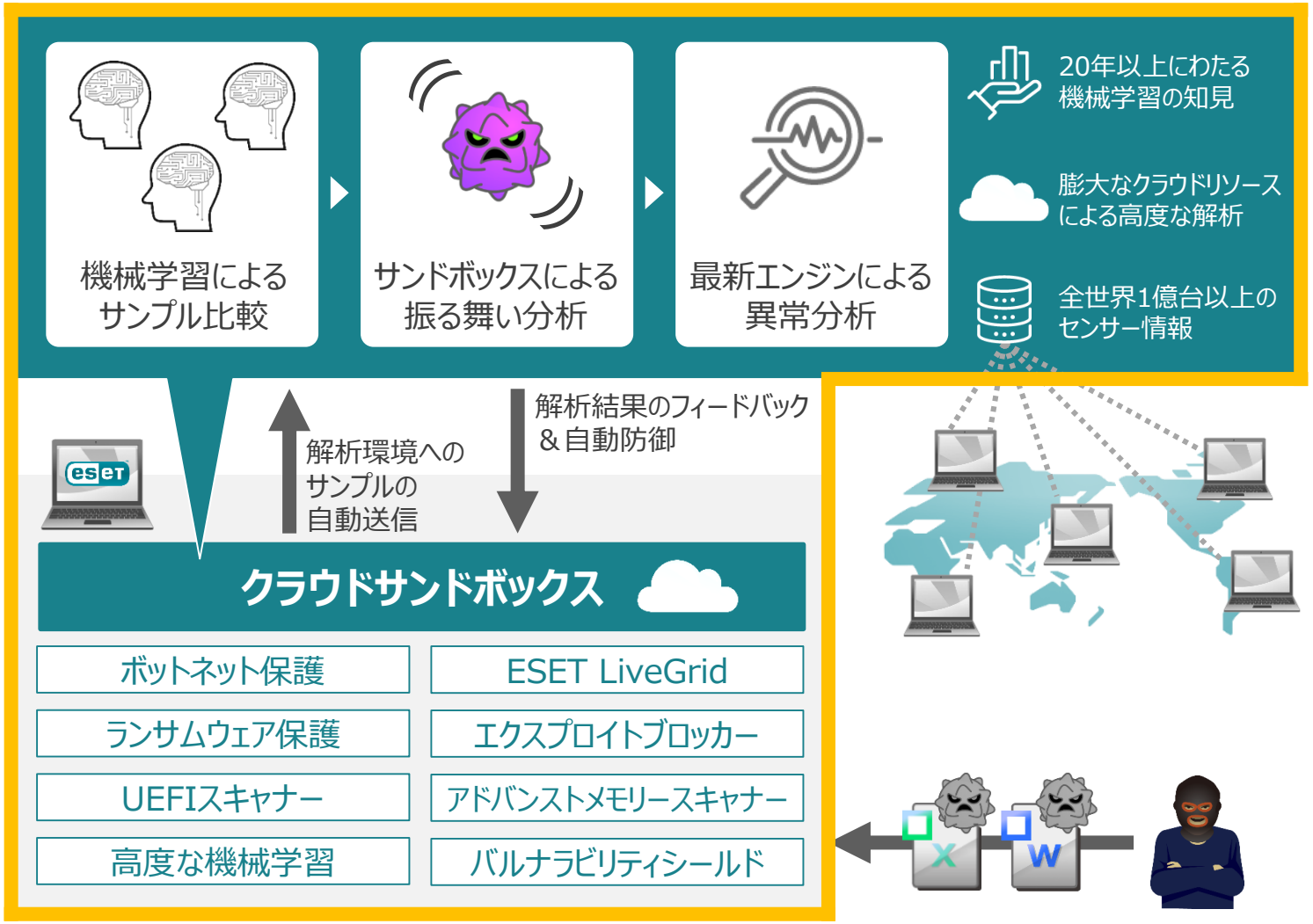
セキュリティ管理のニーズ	セキュリティ保護のニーズ	ソリューション
クラウド管理 ● 管理ツールをクラウド(SaaS)で運用したい ● 管理ツールのサーバー構築やメンテナンス負荷を軽減したい	● テレワーク時にエンドポイント保護を総合的に強化したい ● 標的型メール、ビジネスメール詐欺などのメールの脅威に対抗したい ● Microsoft 365を安全に利用したい ● ランサムウェアやゼロデイ攻撃などの脅威に対抗したい	 **ESET PROTECT Complete クラウド**
	● テレワーク時にエンドポイント保護を総合的に強化したい ● ランサムウェアやゼロデイ攻撃などの脅威に対抗したい	 **ESET PROTECT Advanced クラウド** 推奨
オンプレミス管理 ● オンプレミスサーバーや自社で契約するIaaSで運用したい ● 管理ツールのバージョンアップは自社でコントロールしたい	● テレワーク時にエンドポイント保護を総合的に強化したい ● ランサムウェアやゼロデイ攻撃などの脅威に対抗したい	 **ESET PROTECT Advanced オンプレミス**
	● ランサムウェアやゼロデイ攻撃などの脅威に対抗したい	 **ESET PROTECT Essential Plus オンプレミス**

ESET PROTECTソリューションの構成要素

コア・テクノロジー：エンドポイント保護＋クラウドサンドボックス



コア・テクノロジー (エンドポイント保護＋クラウドサンドボックス)



コア・テクノロジーによる新たな多層防御

多層防御の強化

自動解析、自動防御

1億台の力を借りる

自動解析、自動防御のプロセス

①エンドポイント保護による分析

②100%白黒判断がつかなかったサンプルをクラウドの解析環境へ自動送信

④既知マルウェアとの類似性確認

ESET Cloud

⑤仮想環境でのファイル実行

機械学習による
サンプル比較

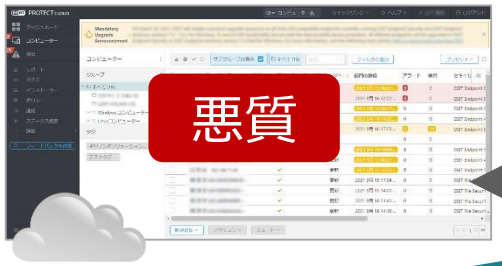
サンドボックスによる
振る舞い分析

最新エンジンによる
異常分析

③解析完了まで実行をブロック(プロアクティブ保護)

⑦解析結果に基づき自動防御

セキュリティ管理ツール



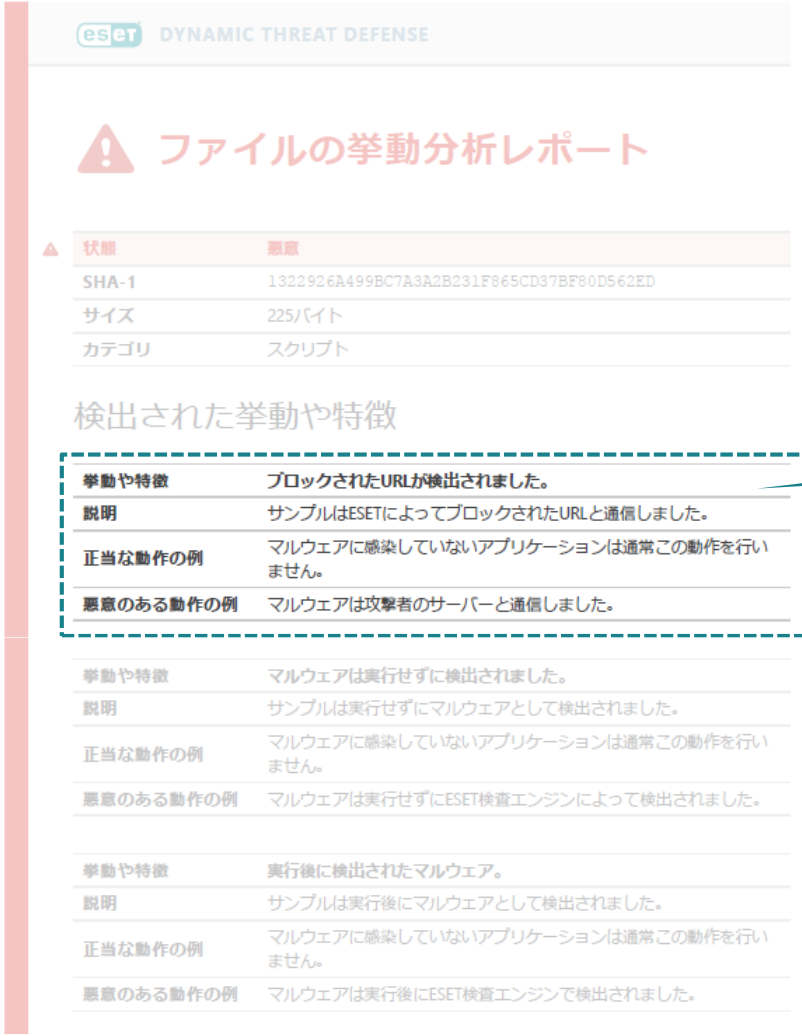
⑥巧妙化したマルウェアの検出

⑧解析結果のフィードバック(レポートによる可視化)

ここまでわずか数分

(大半は2～5分以内、解析済みファイルは即座にフィードバック)

挙動分析レポート



挙動や特徴	**ブロックされたURLが検出されました。**
説明	サンプルはESETによってブロックされたURLと通信しました。
正当な動作の例	マルウェアに感染していないアプリケーションは通常この動作を行いません。
悪意のある動作の例	マルウェアは攻撃者のサーバーと通信しました。

複数の根拠をもって判断
正当性を可視化

挙動分析レポート

挙動や特徴	サンプルは実行中のプロセスを書き換えました。
説明	サンプルは合法的なアプリケーションの実行中のプロセスにコードを挿入しました。
正当な動作の例	これはセキュリティまたはユーザー監視ツールの標準動作です。
悪意のある動作の例	マルウェアは存在を隠そうと試みました。

挙動や特徴	ブートレコードの書き換え。
説明	サンプルは、通常はアクセスできないブートレコードのデータを書き換えました。
正当な動作の例	これは一部のシステムツールの標準動作です。
悪意のある動作の例	マルウェアはシステム再起動後に実行しようとしています。

挙動や特徴	**入力デバイスの傍受。**
説明	サンプルはマウスまたはキーボード入力を傍受しました。
正当な動作の例	これはマクロを記録するアプリケーションの標準動作です。
悪意のある動作の例	サンプルにはキーロガーまたはCryptoLocker (ランサムウェア)が含まれており、復号コードを入力するためのアクセスを要求しています。

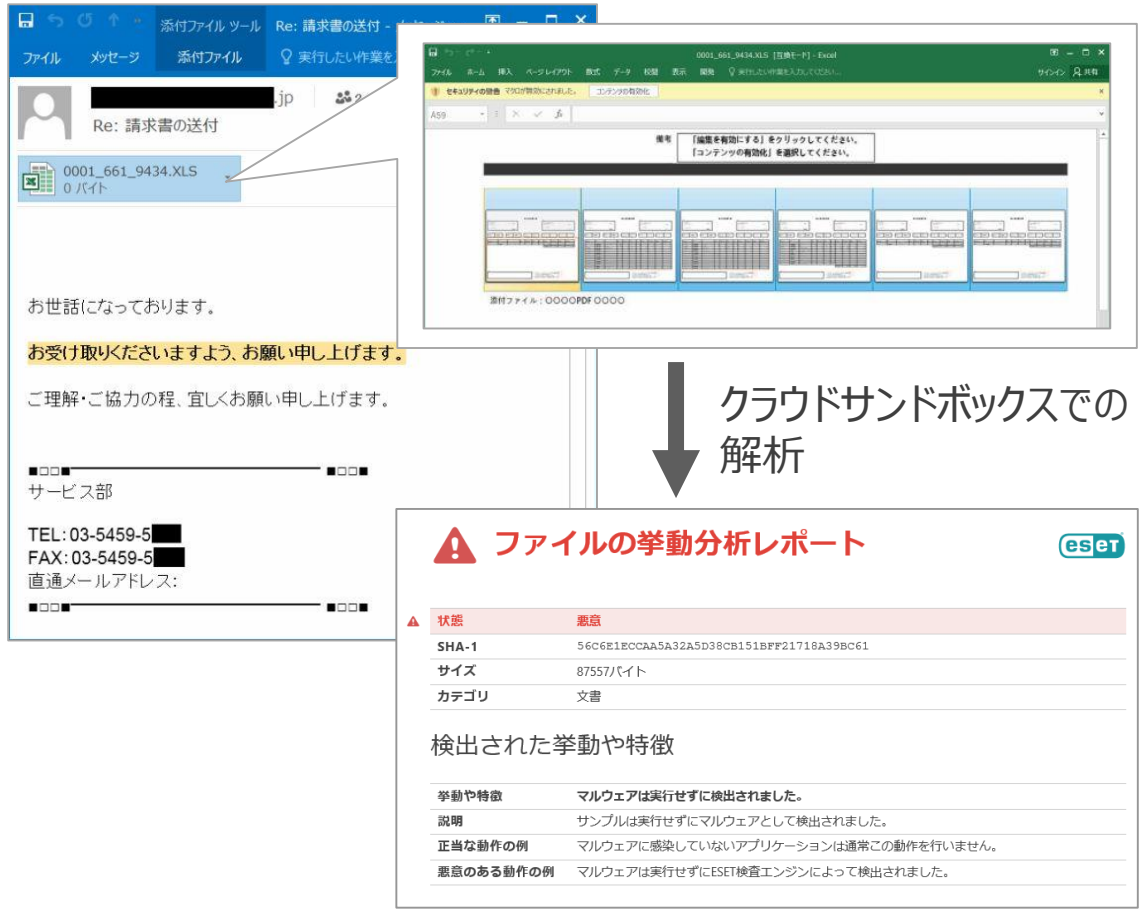
挙動や特徴	オペレーティングシステムがシャットダウンしました。
説明	サンプルはオペレーティングシステムのシャットダウンを開始しました。
正当な動作の例	これは一部のインストーラーまたはアンインストーラーの標準動作です。
悪意のある動作の例	マルウェアは存在を隠そうとしたか、強制的に再起動を試みました。

挙動や特徴	**入力デバイスの傍受。**
説明	サンプルはマウスまたはキーボード入力を傍受しました。
正当な動作の例	これはマクロを記録するアプリケーションの標準動作です。
悪意のある動作の例	サンプルにはキーロガーまたはCryptoLocker (ランサムウェア)が含まれており、復号コードを入力するためのアクセスを要求しています。

複数の根拠をもって判断
正当性を可視化

日本を固有に狙った攻撃の防御例

99%が国内で検出されたダウンローダー「DOC/Agent.DZ」



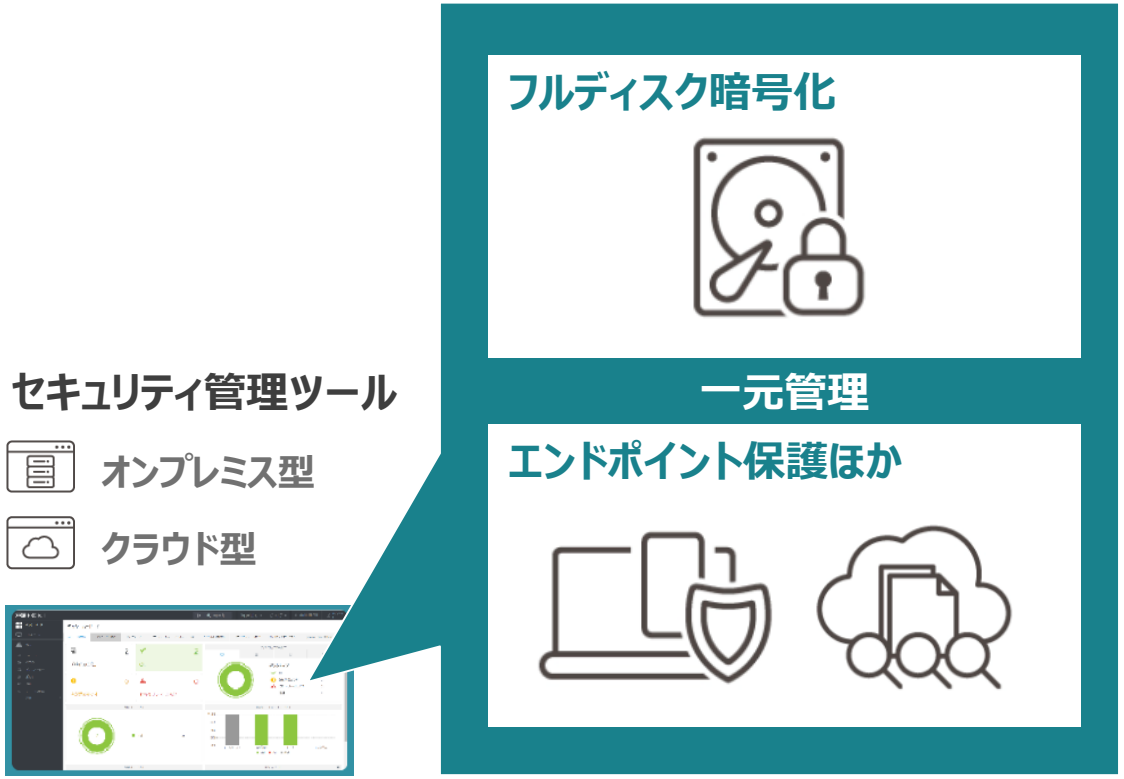
検知を妨害・回避する高度な処理

- VBAコードにロック
- 日本語環境でない場合処理を終了
- PowerShellコマンドを多重に難読化
- PowerShell v3.0以降がインストールされている環境でのみ稼働、それ以外は処理を終了
- 攻撃用データを画像ファイルに隠蔽(ステガノグラフィー)

クラウドへ送信後8秒で悪質と判定
即座に全端末でブロック

フルディスク暗号化

PC紛失・盗難時の情報漏洩リスクを低減

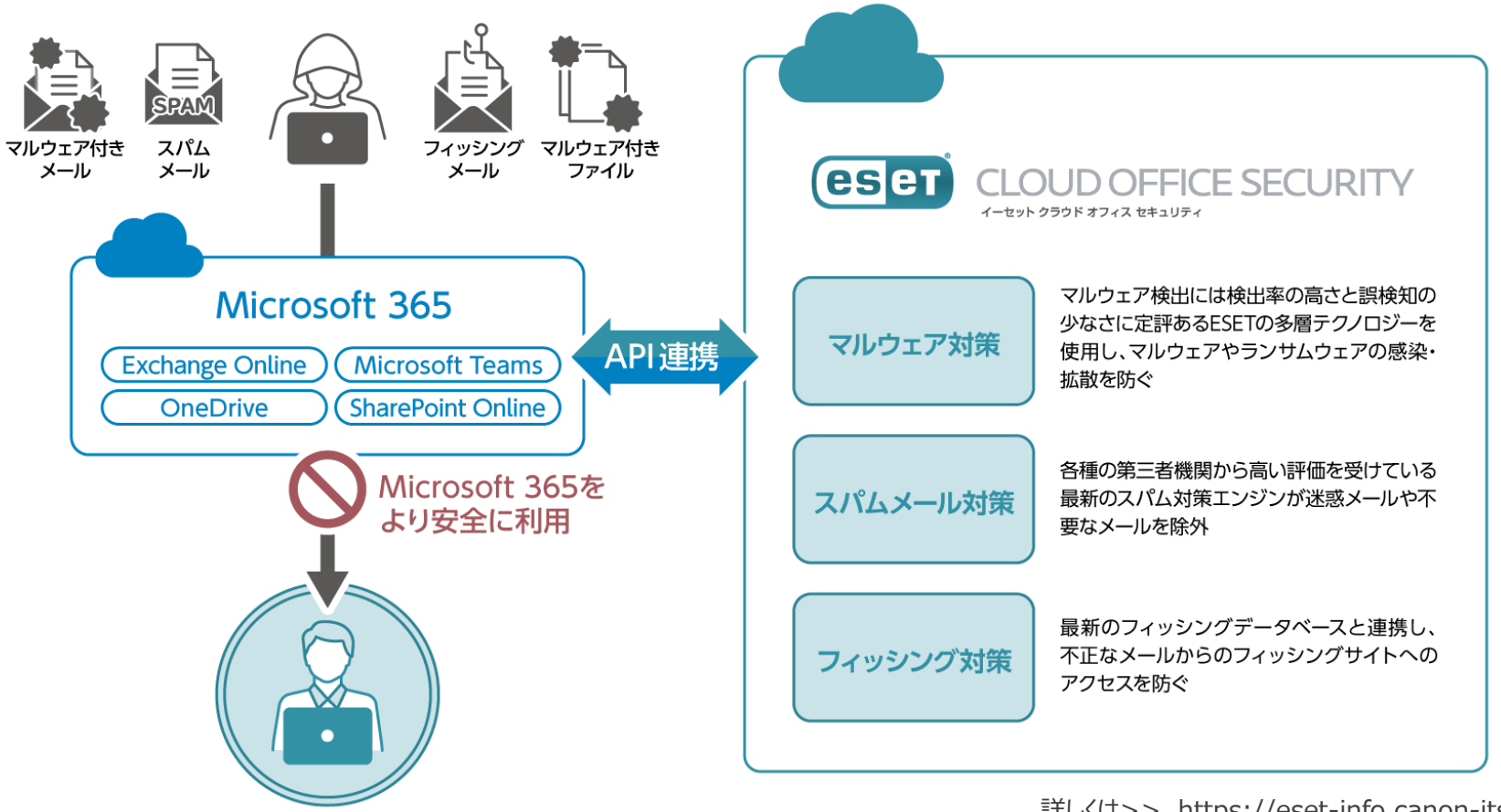


- 端末のディスク全体を暗号化
- プリブート認証により紛失・盗難時の情報漏洩を防ぐ
- セキュリティ管理ツール(クラウド型、オンプレミス型)配下でその他のセキュリティ対策とともに一元管理

詳しくは>> https://eset-info.canon-its.jp/business/efde/

クラウドアプリケーションセキュリティ

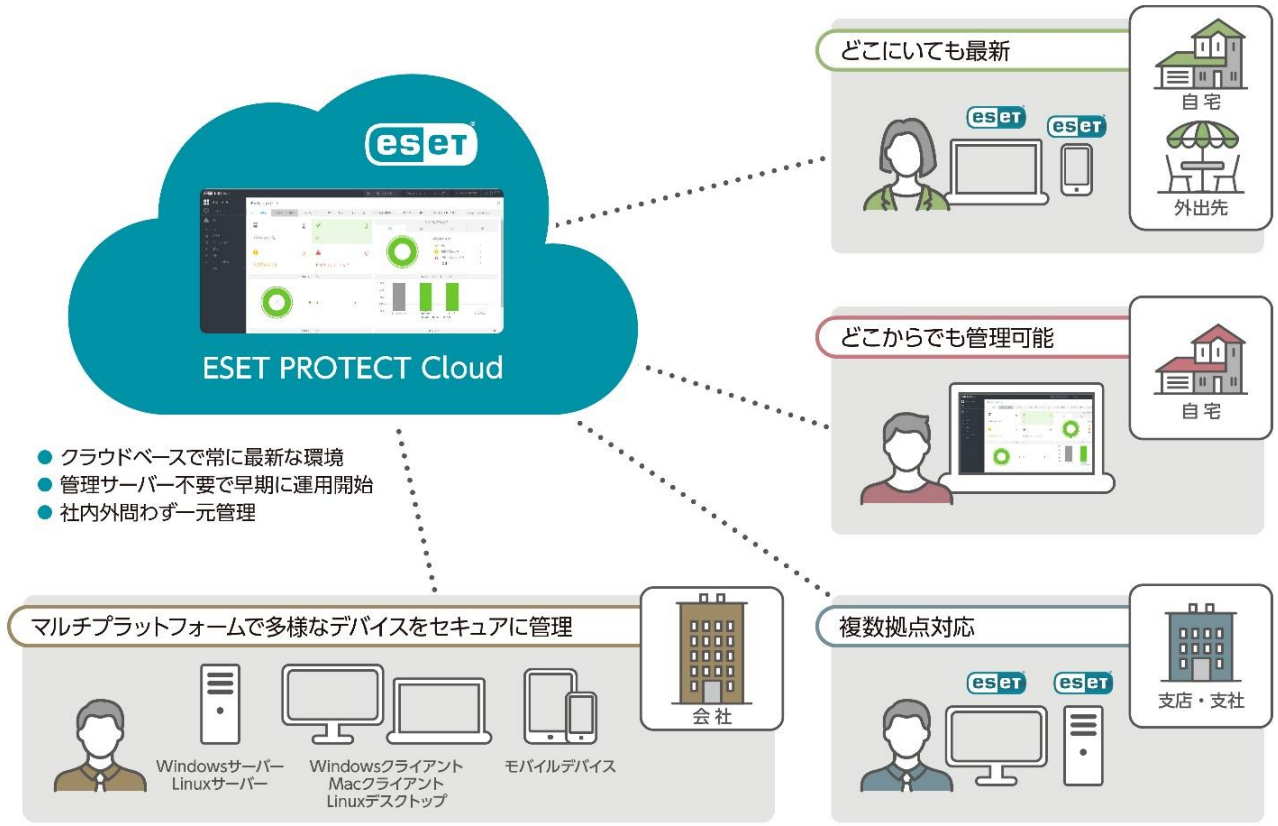
メールを含むMicrosoft 365環境をさらにセキュアに



詳しくは>> https://eset-info.canon-its.jp/business/ecos/

クラウド型セキュリティ管理ツール

どこからでも、どこにいても、エンドポイントを一元管理



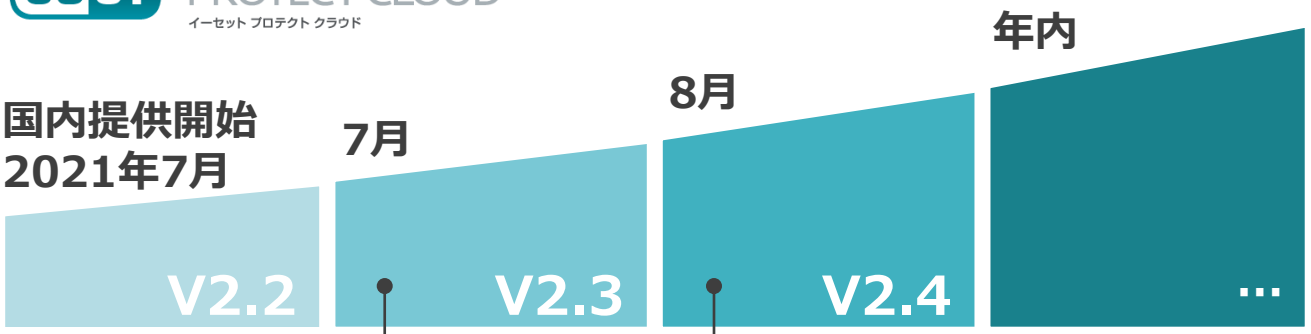
- 社内外を問わずエンドポイントをセキュアに管理
- サーバー構築・保守不要で早期の導入、運用開始と運用コスト低減を実現
- 多様なデバイスにまたがる多重の対策を1コンソールで管理
- 自動バージョンアップで常に最新の環境を利用可能

詳しくは>> https://eset-info.canon-its.jp/business/ep-cloud/

セキュリティ管理も進化する

クラウド型セキュリティ管理ツール

ESET PROTECT CLOUD
イーセット プロテクト クラウド

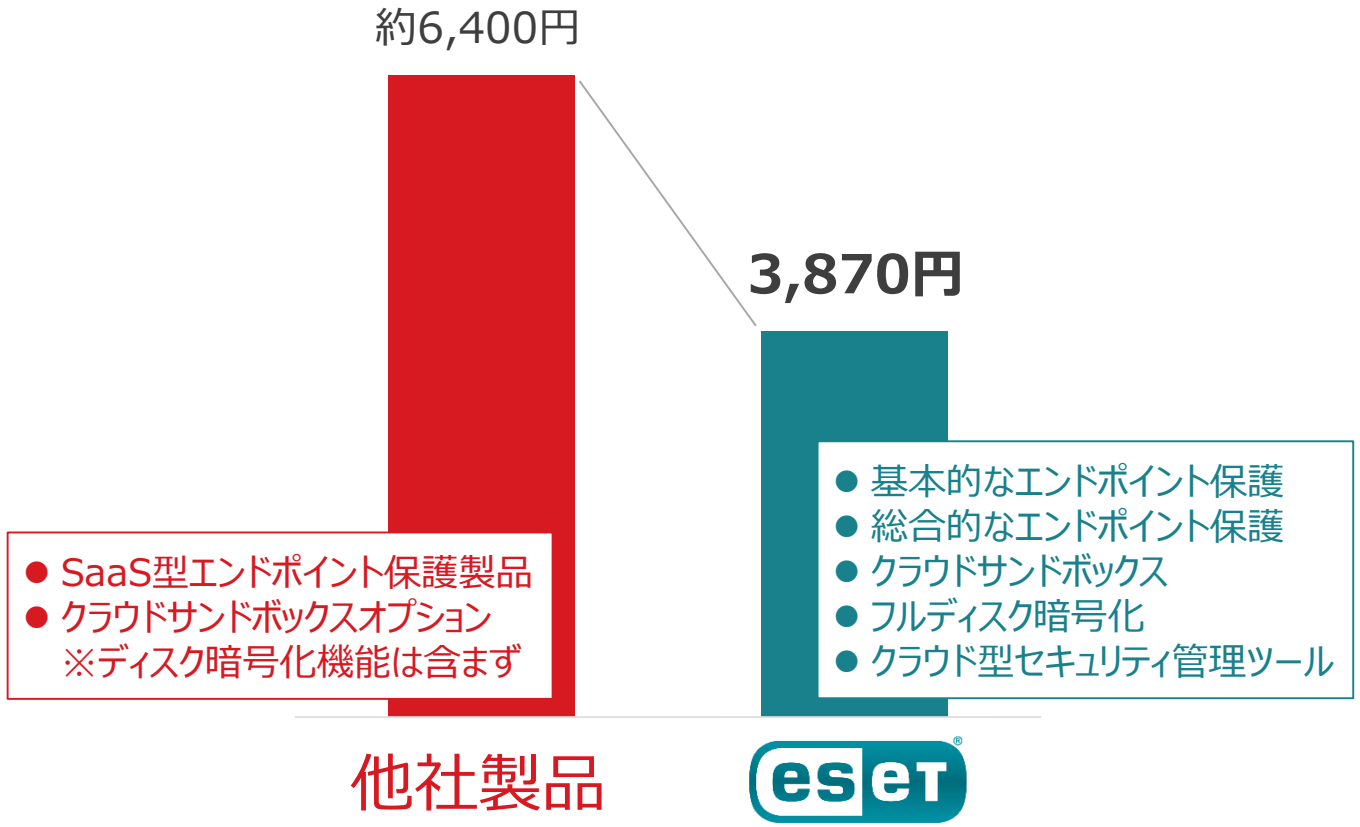


- 管理対象台数を2.5万台に拡張
- クラウドサンドボックスの全世界での検出状況表示

- iOS端末管理機能の追加
- フルディスク暗号化の管理機能強化

約9週間サイクルで
機能強化、機能改善

圧倒的なコストメリット



他社の6割に抑えられる
高いコストパフォーマンス

＊合計ライセンス数250ライセンスにおける1ライセンスあたりの税別価格。ESET製品はESET PROTECT Advanced クラウドの標準価格。他社製品の価格は2021年9月1日時点でのカタログ、ウェブ等に記載されている標準価格をもとにしたイメージです。

ESET PROTECTソリューションによる解決

エンドポイントを取り巻くさまざまなリスクに対応

狙われる日本企業	日本を固有に狙う攻撃も対応
テレワークの脆弱性 人の脆弱性	テレワークを狙う攻撃や ヒューマンエラーによるサイバーリスクを低減
対策には自信も 人材も足りない	ESET社が考えるベストプラクティスなソリューション

デジタルセキュリティで
お客さまのビジネス変革を支える

canon.jp/it-sec

参考情報

ESET PROTECTソリューション関連サイト

- ESETセキュリティソリューションシリーズ
  https://eset-info.canon-its.jp/business/
- ESET PROTECT Advanced クラウド
  https://eset-info.canon-its.jp/business/ep-advanced-c/
- エンドポイント保護
  https://eset-info.canon-its.jp/business/endpoint-protection-comp/
- クラウドサンドボックス
  https://eset-info.canon-its.jp/business/edtd/
- フルディスク暗号化
  https://eset-info.canon-its.jp/business/efde/
- クラウドアプリケーションセキュリティ
  https://eset-info.canon-its.jp/business/ecos/
- クラウド型セキュリティ管理ツール
  https://eset-info.canon-its.jp/business/ep-cloud/

高度サイバー攻撃対策に関する情報サイト

進化するサイバー攻撃に立ち向かうためのお役立ち情報が満載
EDRまるわかりガイドや、piyokango氏、辻伸弘氏と弊社セキュリティエンジニアの対談記事なども掲載

詳しくはこちら＞＞　https://eset-info.canon-its.jp/business/threat-solution/

サイバーセキュリティ情報局

国内外のトレンド
国内の脅威動向など、
最新情報を発信

サイバーセキュリティ情報局