セキュリティマネジメント
Summit 2021 Winter

壊滅的なサイバー攻撃から従業員を守る

セキュリティ革新2022の勘所

2022年1月26日

キヤノンマーケティングジャパン株式会社
峯森　惇平

Canon

- 峯森 惇平（みねもり じゅんぺい）
  - キヤノンマーケティングジャパン
  - ESET製品を中心としたマーケティング
  - 販売促進・事業推進業務に従事

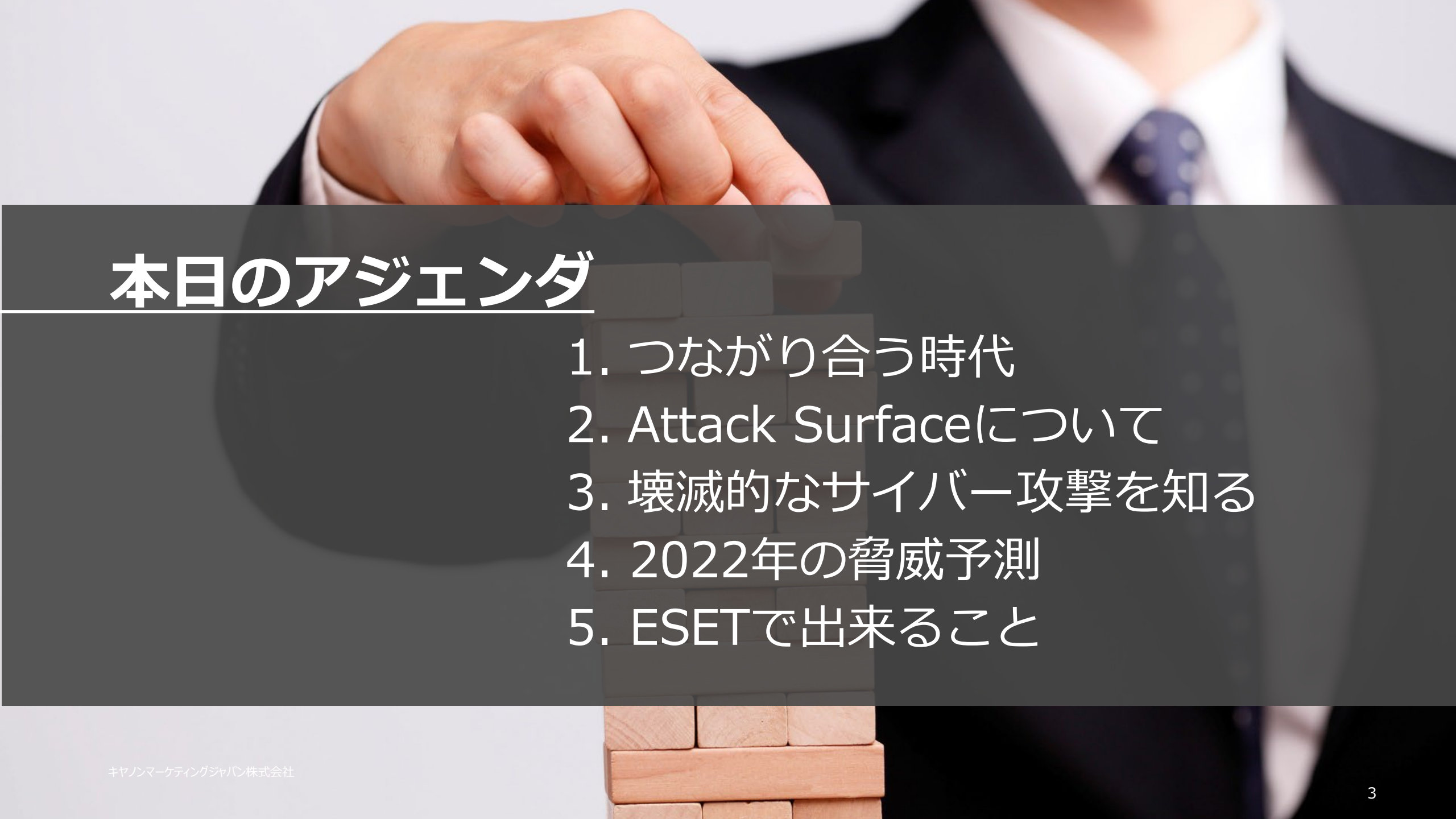
第020006号

当社Webサイト（canon.jp/it-sec）
マルウェア対策の「5つの備え」

IPA（情報処理推進機構）
情報セキュリティマネジメントの勧め

マイナビニュース
いまEDTDが求められる理由とは?

Logmi Biz



本日のアジェンダ

1. つながり合う時代
2. Attack Surfaceについて
3. 壊滅的なサイバー攻撃を知る
4. 2022年の脅威予測
5. ESETで出来ること

1. つながり合う時代

COVID-19が
日本のビジネス環境に
与えた**インパクト**

2020

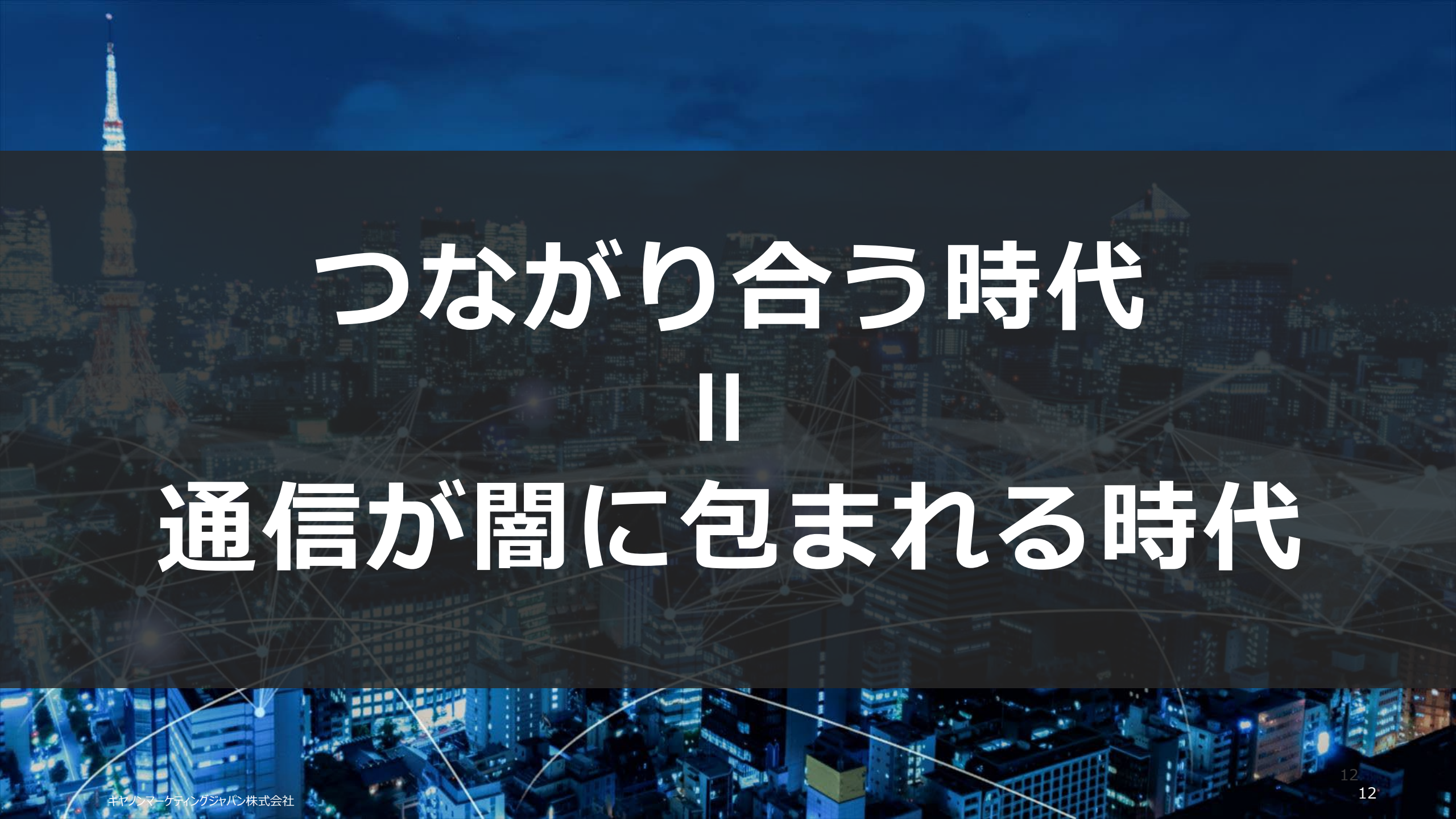
自分が考える
テレワーク中のユーザー

情シス担当者から見た
テレワーク中のユーザー

ITとは
生活を豊かにするもの

誰一人取り残さない、
人に優しいデジタル化を

出典：デジタル庁
https://www.digital.go.jp/policies


つながり合う時代
=
通信が闇に包まれる時代

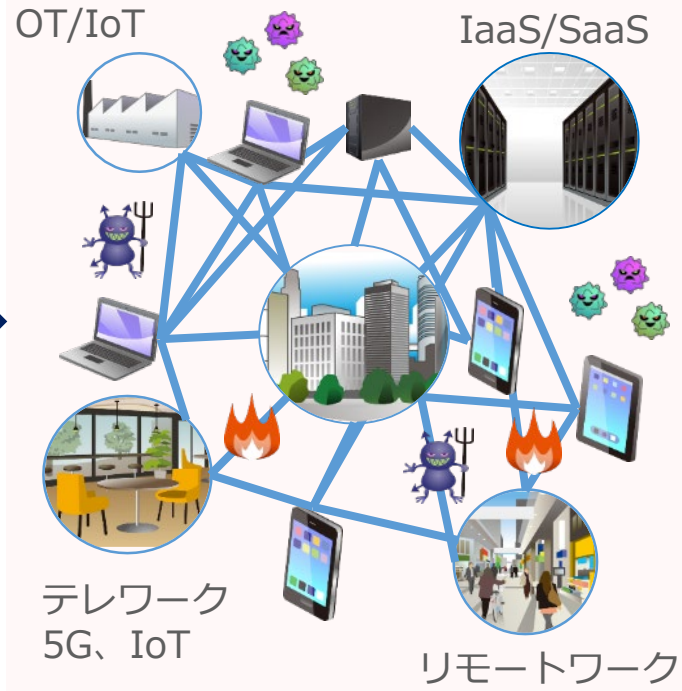
多くの通信が暗号化プロトコルを利用

境界型防御の時代

社内と社外の“境界”を
守るのが主流

保護対象は
境界内部に
留まらない

ゼロトラスト
セキュリティの時代

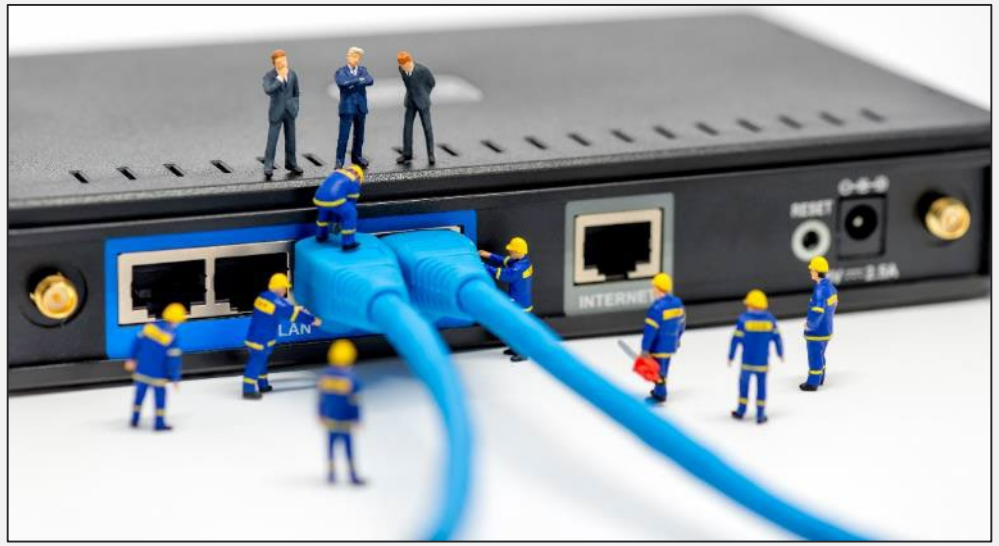


情報資産が社外にも
存在する状態

2．Attack Surfaceについて

AttackSurfaceとは「攻撃対象領域」

物理的な
Attack Surface



物理境界（FW・PROXY）

拡がる
Attack Surface

リモートワーク端末
クラウドサービス
IoTデバイス＆5G
VPN/RDP

Attack Surfaceの拡大
攻撃の高度化＋巧妙化

Attack Surfaceの拡大
攻撃の高度化＋巧妙化

複雑になるセキュリティ対策
限られたリソース

３．壊滅的なサイバー攻撃を知る

壊滅的なサイバー攻撃

壊滅的なサイバー攻撃とは

人命にかかわる

事業継続できなくなる

顧客に強烈な影響を与える

企業を事業停止に追い込んだ攻撃

攻撃者：DarkSide

- **Colonial Pipeline事例**
  - **2021年　米国／石油パイプライン企業（重要インフラ）**
    - Attack Surface：VPN認証情報の管理不備といわれている
    - ランサムウェアによる攻撃を受け、予防的措置として業務を一時停止
    - 順次事業再開まで1週間程度／5億円弱の身代金支払い
    - FBIはDarkside RaaSが利用されたと声明
    - **Win32/Filecoder.DarkSide（ESET検出名）：2020年10月から使用されている**

以下のサイトを参考に作成
ESETブログ「welivesecurity」米国パイプライン大手企業のColonial Pipeline社への攻撃： 物理的な環境へのハッキング
https://www.eset.com/jp/blog/welivesecurity/colonial-pipeline-attack-hacking-physical-world/
The White House FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks
https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/
FBI Statement on Compromise of Colonial Pipeline Networks
https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks

自社の顧客に強烈に影響を与えた攻撃

- **1．Kaseya社事例**
  - 自社ソフトウェア（VSA製品）のゼロデイ脆弱性
  - 自社ソフトウェアアップデートに合わせてマルウェアをMSP経由で配布し感染拡大
  - サプライチェーン攻撃（1,500組織へ影響／MSP約60社経由）
  - Attack Surface：リモート監視・管理サーバー

攻撃者：REvil
（Sodinokibi）

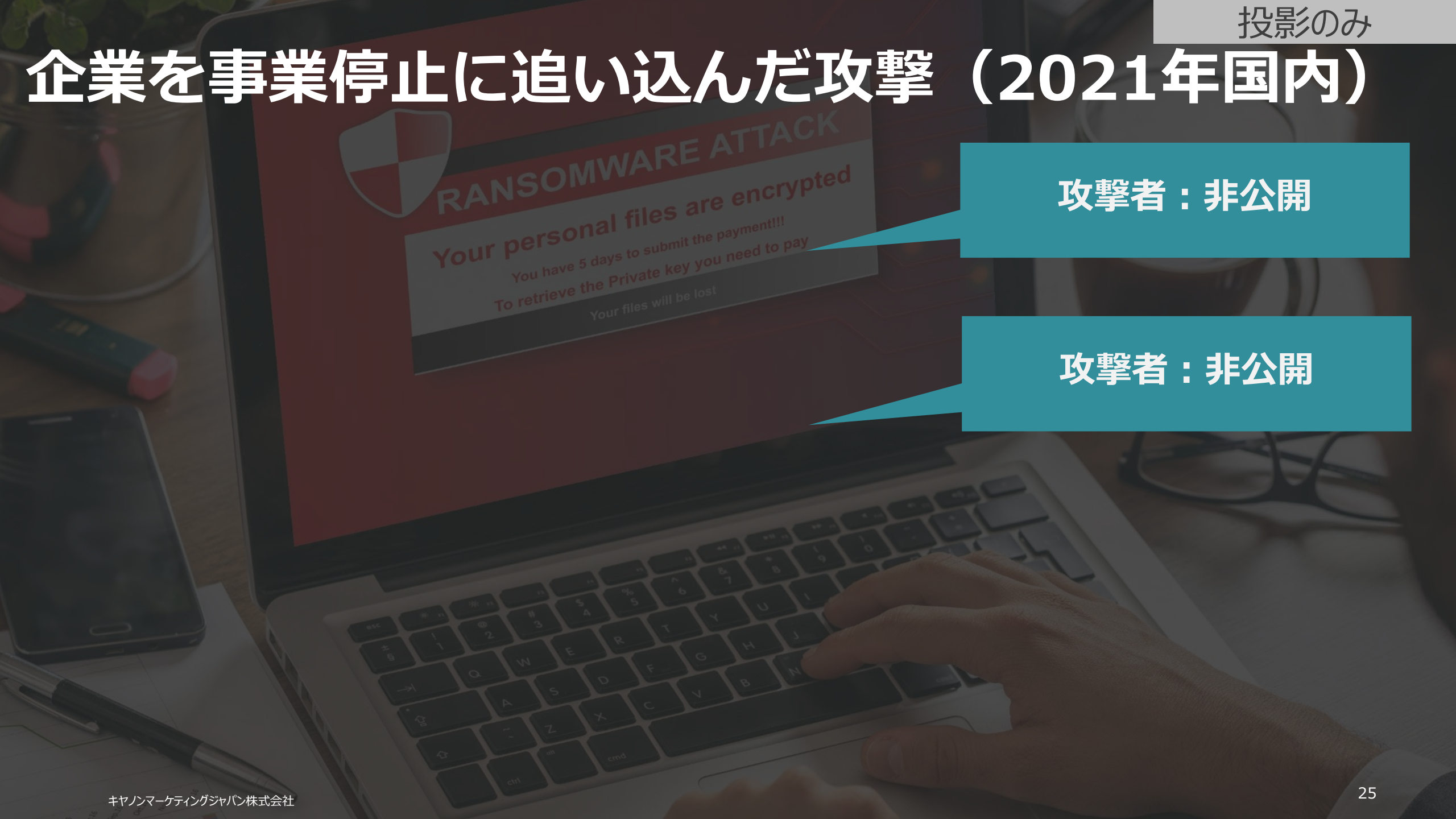
- **2．SolarWinds社事例（Orion Platform）**
  - IT管理ツールのアップデートを通じマルウェア配布・2次配布
  - サプライチェーン攻撃（18,000組織へ影響／米国政府機関含）
  - Attack Surface：従業員のメール受信
  - **ESETではMSIL/SunBurst.A.で検出**※ただしSolarWinds及びCISAからのガイダンスに従うよう警告

攻撃者：The Dukes

以下のサイトを参考に作成
キヤノンマーケティングジャパン サイバーセキュリティ情報局　MSP選定時に確認すべきポイント：Kaseyaが受けた脆弱性を狙ったゼロデイ攻撃から学ぶサードパーティによるサイバーセキュリティリスク
https://eset-info.canon-its.jp/malware_info/special/detail/210916.html
ESET社Webページ　Does ESET protect me from the SolarWinds supply-chain attack?
https://support.eset.com/en/kb7765-does-eset-protect-me-from-the-solarwinds-supply-chain-attack

対岸の火事？

企業を事業停止に追い込んだ攻撃（2021年国内）



攻撃者：非公開

攻撃者：非公開

投影のみ

企業を事業停止に追い込んだ攻撃（2021年国内）

攻撃者：非公開

攻撃者：非公開

サイバー空間に国境はない

2021年7月8月 マルウェアレポート

https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2108.html

多重脅迫型（ランサム）攻撃

LockBit 2.0	CONTI	CL0P	REvil Sodinokibi
Ransom Exx	RAGNAR _LOCKER	Prome-theus	Grief DoppelPaymer
Netfilim	DarkSide	Avaddon	STOP Djvu

・・・

多重脅迫型（ランサム）攻撃

※参考／赤字：LockBit2.0で用いられる脅迫手段

1. **ファイル・システムのロックアップによる脅迫**
2. **ドキシングによる脅迫（窃取情報を曝す）**
3. **DDoS攻撃による脅迫**
4. **身代金要求を大量に印刷**
5. **コールセンターと契約し大量にTEL**
6. **被害企業の顧客にメール通知**

・・・

「悪意のある第三者」の分業

マルウェア
ディストリビューター

RaaS
（Ransom as a Service）

イニシャルアクセス
ブローカー

攻撃用マルウェアの開発
攻撃インフラ提供

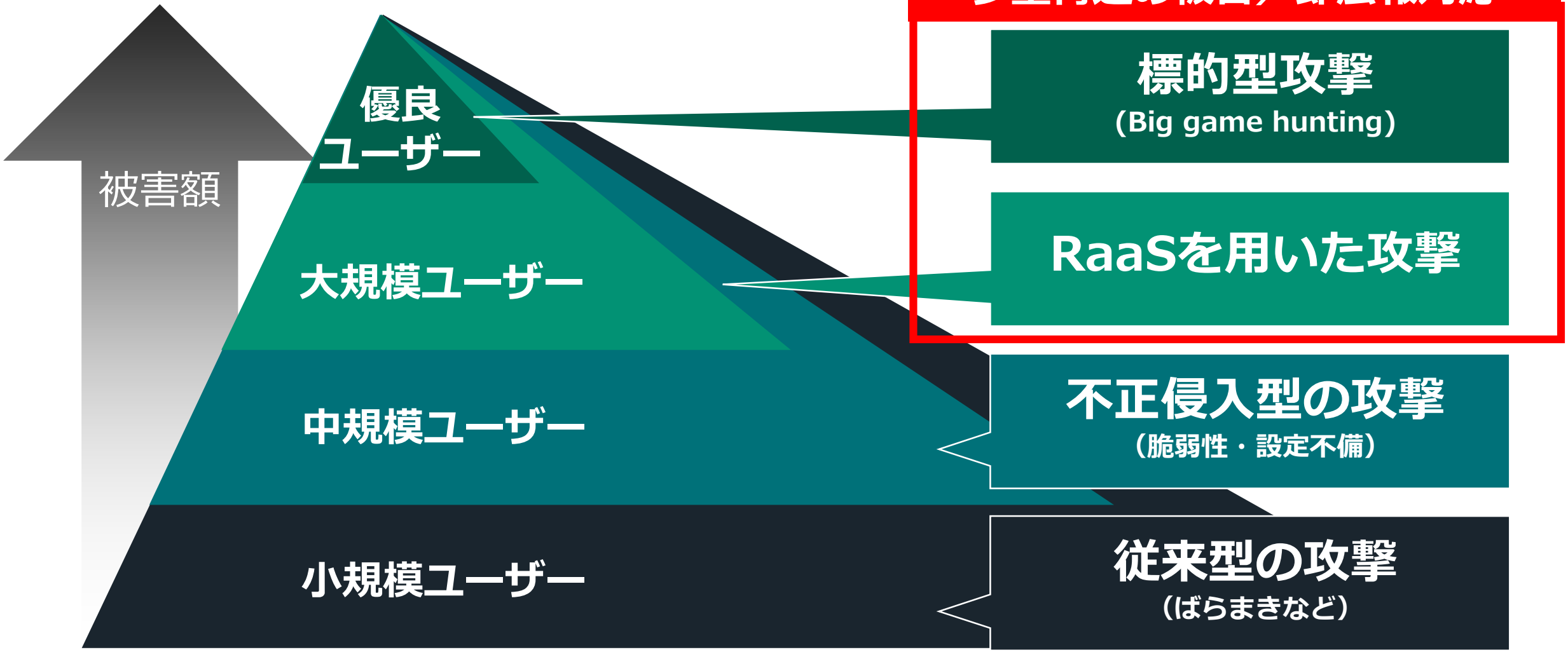
オペレーター
アタッカー

過去情報が流出した
認証情報（AD）など
情報搾取型マルウェア
（Infostealer）

人的資源の市場も存在

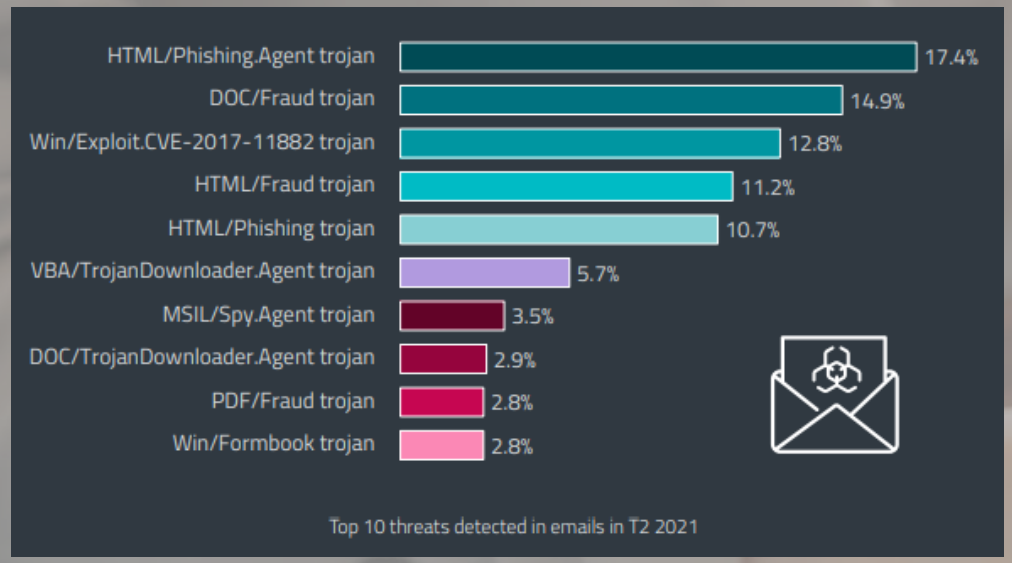
被害ユーザーの
Attack Surface

狙われる層

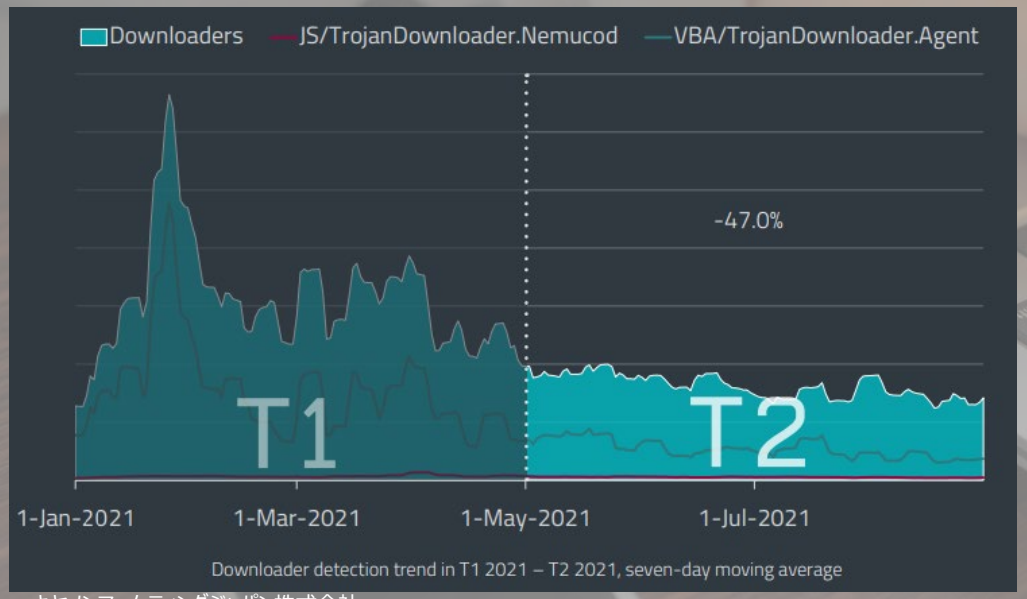

被害額
優良ユーザー
大規模ユーザー
中規模ユーザー
小規模ユーザー
多重脅迫の被害／即広報対応
標的型攻撃
(Big game hunting)
RaaSを用いた攻撃
不正侵入型の攻撃
（脆弱性・設定不備）
従来型の攻撃
（ばらまきなど）

4.　2022年の脅威予測

ESET製品で検出したメールへの攻撃



Top 10 threats detected in emails in T2 2021



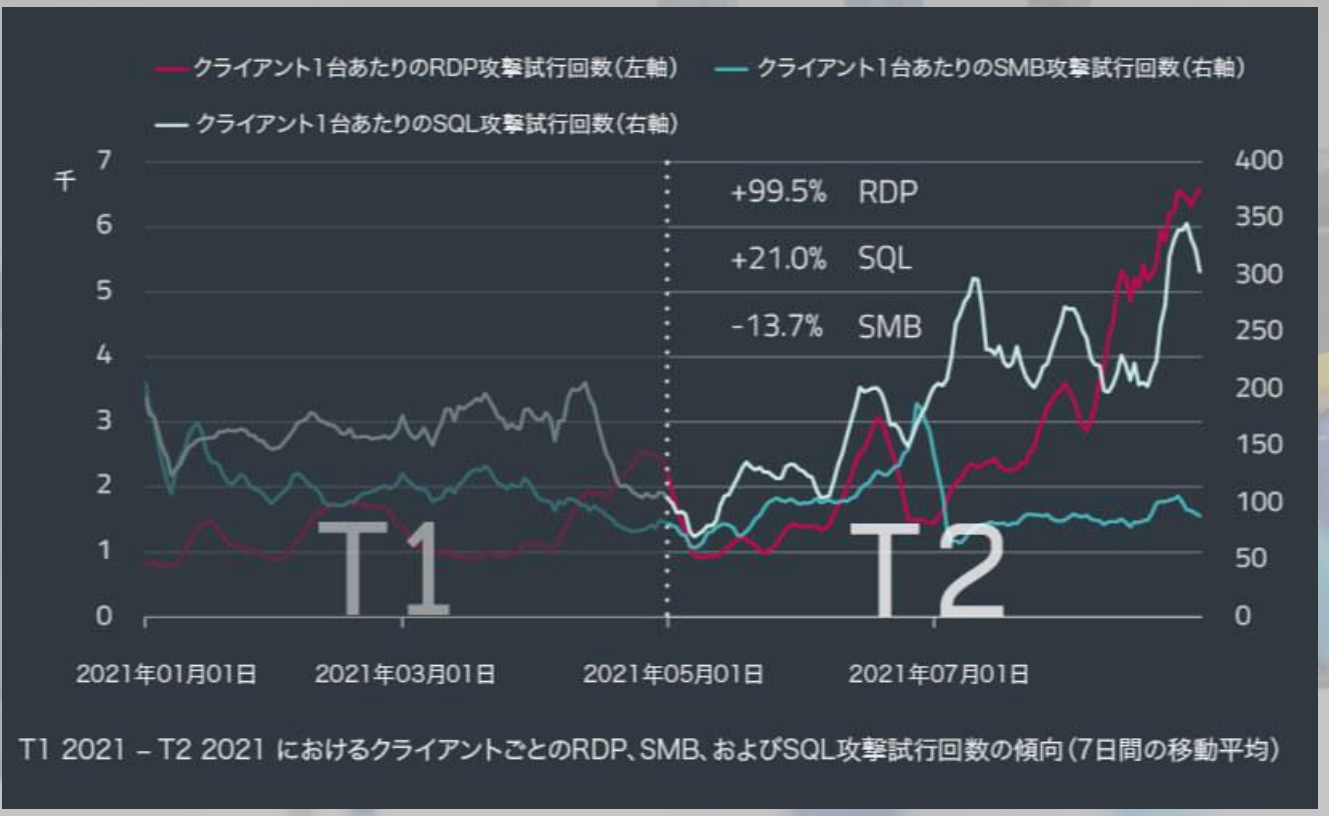
Downloader detection trend in T1 2021 – T2 2021, seven-day moving average

フィッシング

今後Emotetの動静に注意

ダウンローダ

ESET製品で検出したAttack Surface（台当り）



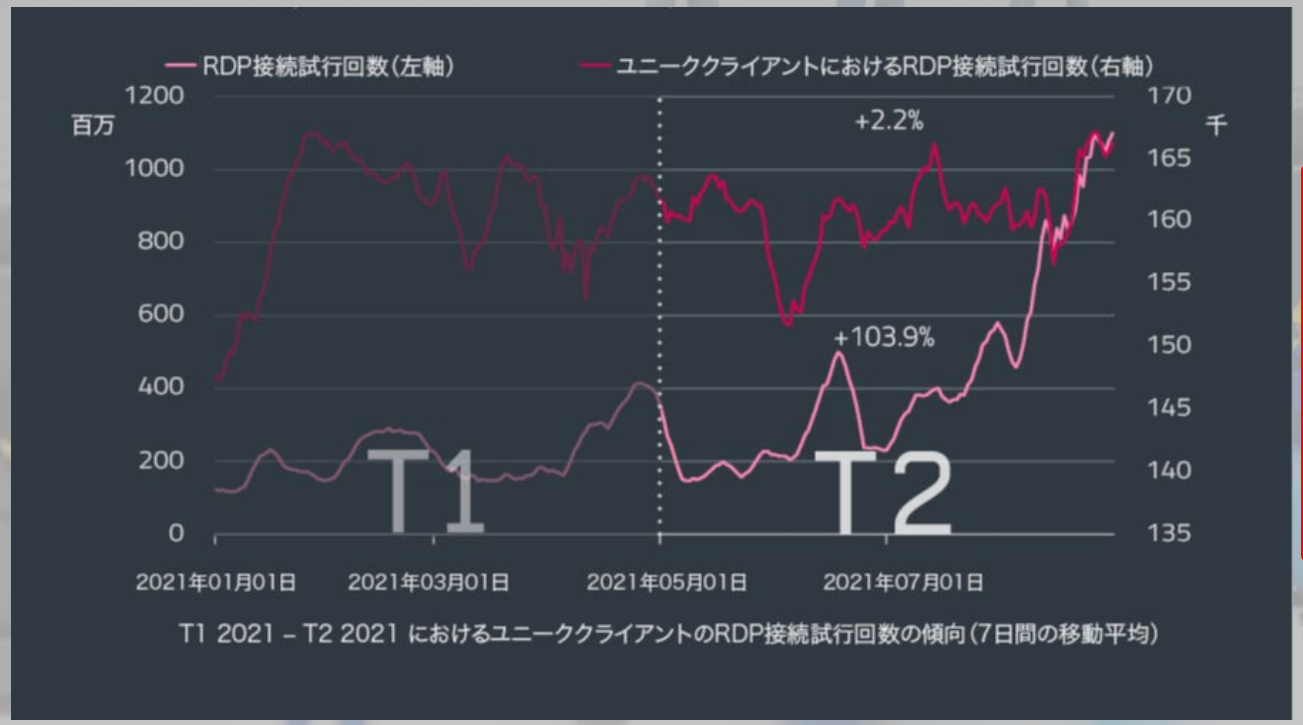
T1 2021 – T2 2021 におけるクライアントごとのRDP、SMB、およびSQL攻撃試行回数の傾向（7日間の移動平均）

RDP狙い
+99.5%

SQL狙い
+21.0%

SMB狙い
-13.7%

狙いすましたRDPへの攻撃



T1 2021 – T2 2021 におけるユニーククライアントのRDP接続試行回数の傾向(7日間の移動平均)

RDP攻撃試行数

+103.9%

特定対象へのRDP攻撃試行

約**16**万台前後で**推移**

RDPを狙った総当たり

550億回

2021年5月＝10月までの6か月間

今後日本を取り巻く脅威予測

- 2021年の特筆すべきこと
  - ITインフラセキュリティのスパゲティ化
  - ランサムウェア攻撃の高度化・巧妙化（LockBit2.0など）
  - 高度なマルウェア感染手法を用いたサプライチェーン攻撃
- 2022年に向けて考えること
  - Attack Surfaceを減らすための投資
  - 壊滅的被害をもたらすマルウェアへの防御
  - 少ない人的リソース前提のインフラ検討

5. ESETで出来ること

目指しているのはバランスの取れた従業員にやさしいセキュリティ

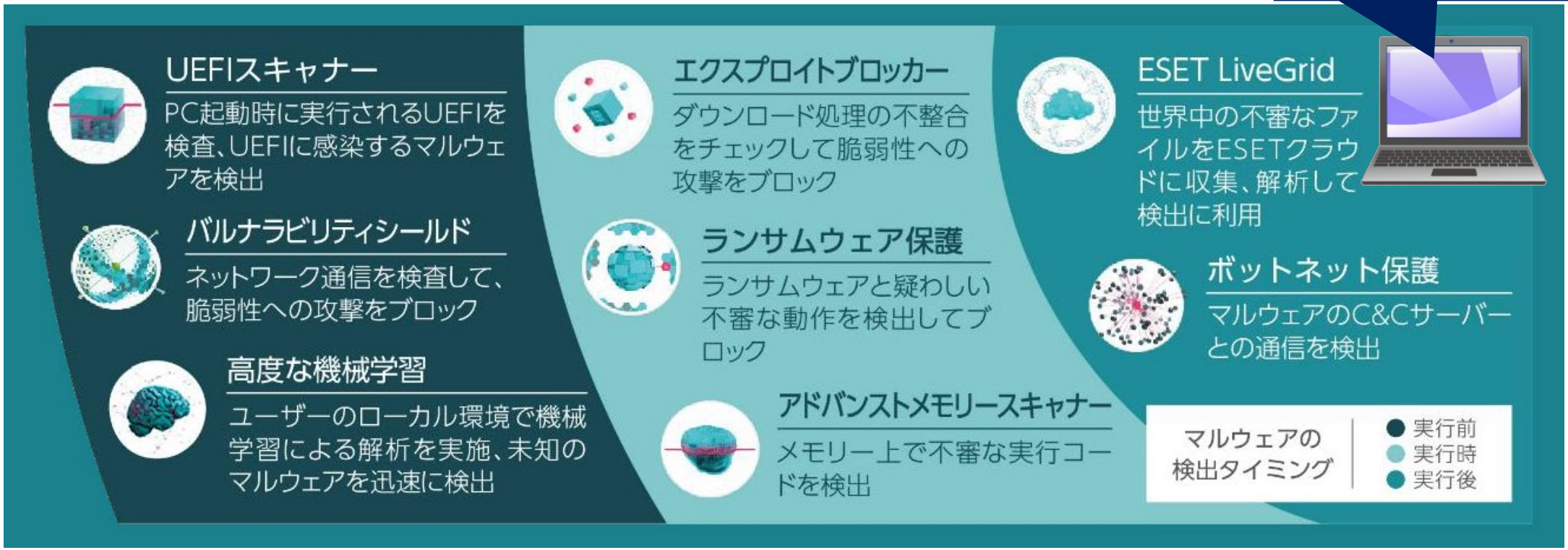
ESET PROTECTソリューションは検討に値するか

Canon

Attack Surfaceを減らすための投資	?
壊滅的被害をもたらすマルウェアへの防御	?
少ない人的リソース前提のインフラ検討	?

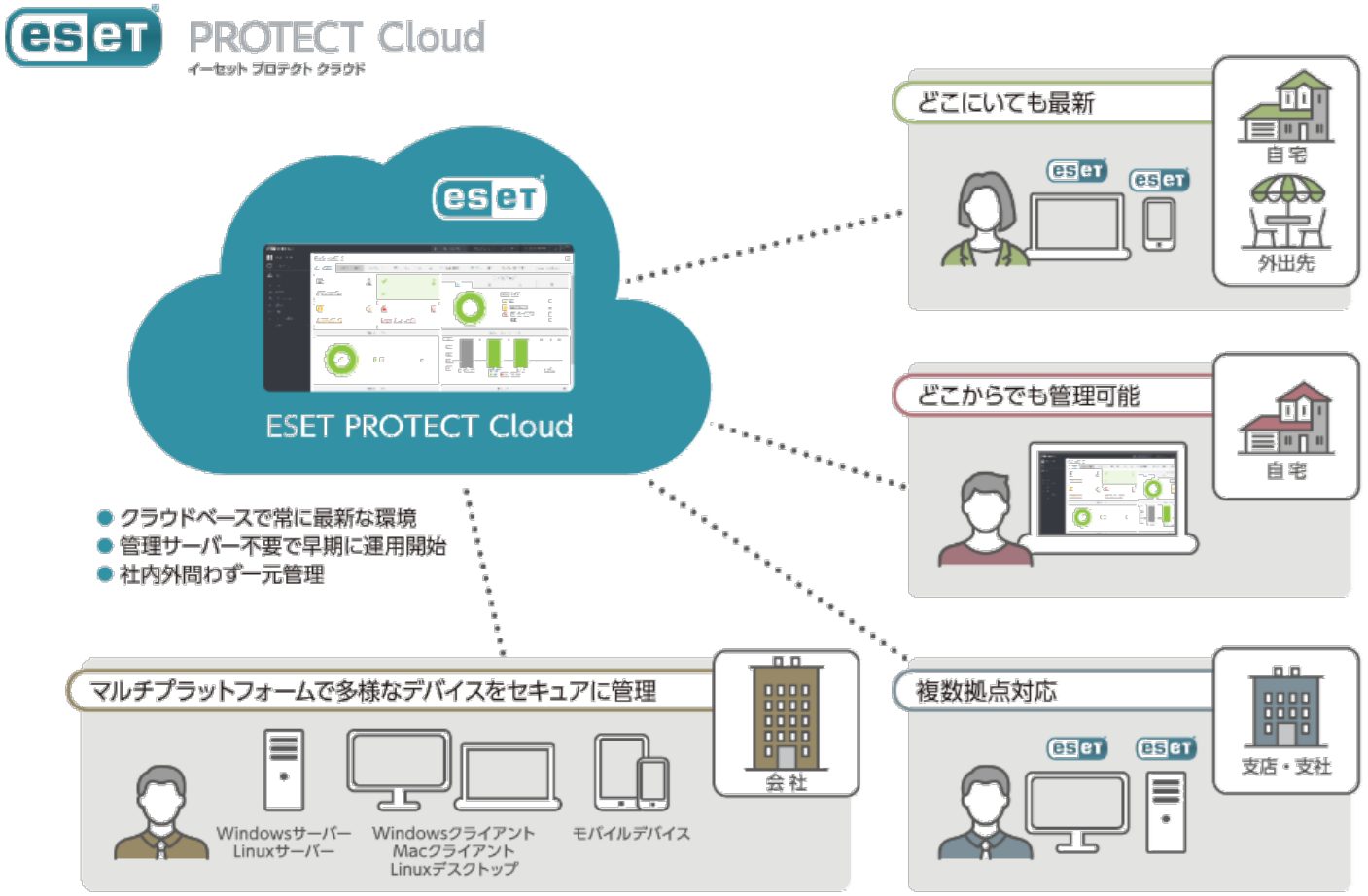
エンドポイント製品の特長

軽快な動作



8レイヤ の防御

在宅勤務対応（テレワークセキュリティ）

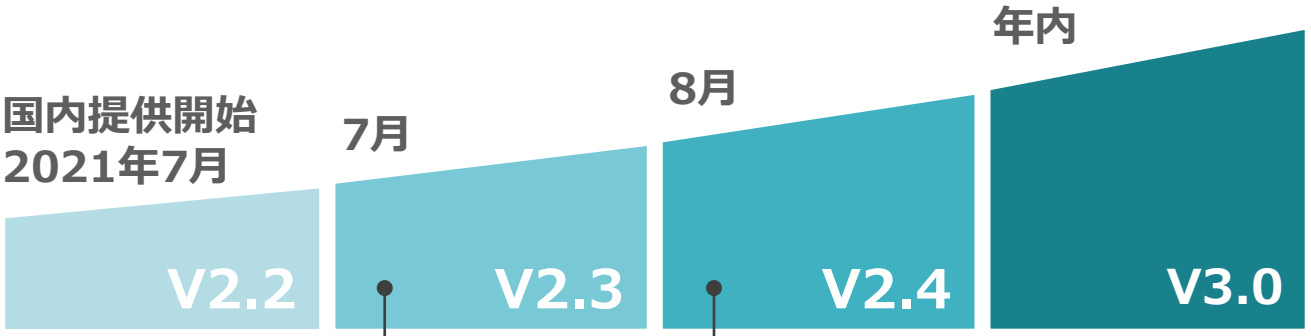


どこからでも
どこにいても
エンドポイントを
一元管理可能

※ログ管理、クライアント管理、サーバー運用管理、セキュリティ対策状況見える化、外部連携など

日々進化するニーズに対応

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

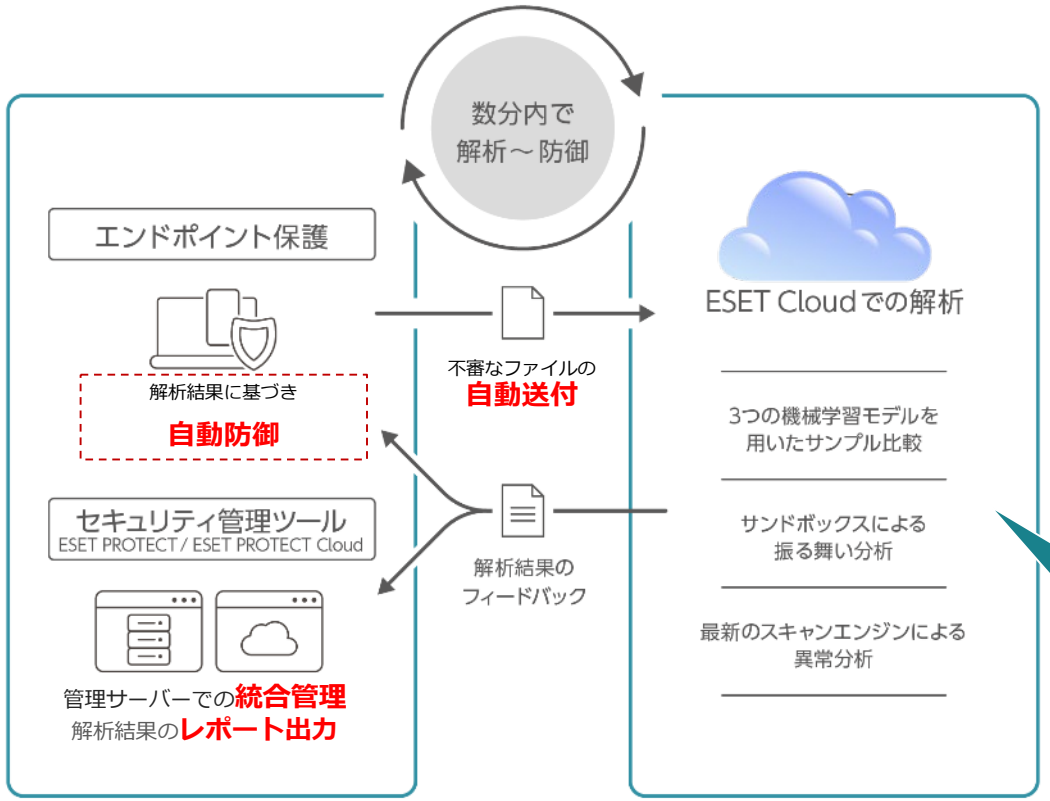
- iOS端末管理機能の追加
- フルディスク暗号化の管理機能強化

機能強化、機能改善

約9週間サイクル

クラウドサンドボックス連携

ESET DYNAMIC THREAT DEFENSE
イーセット ダイナミック スレット ディフェンス



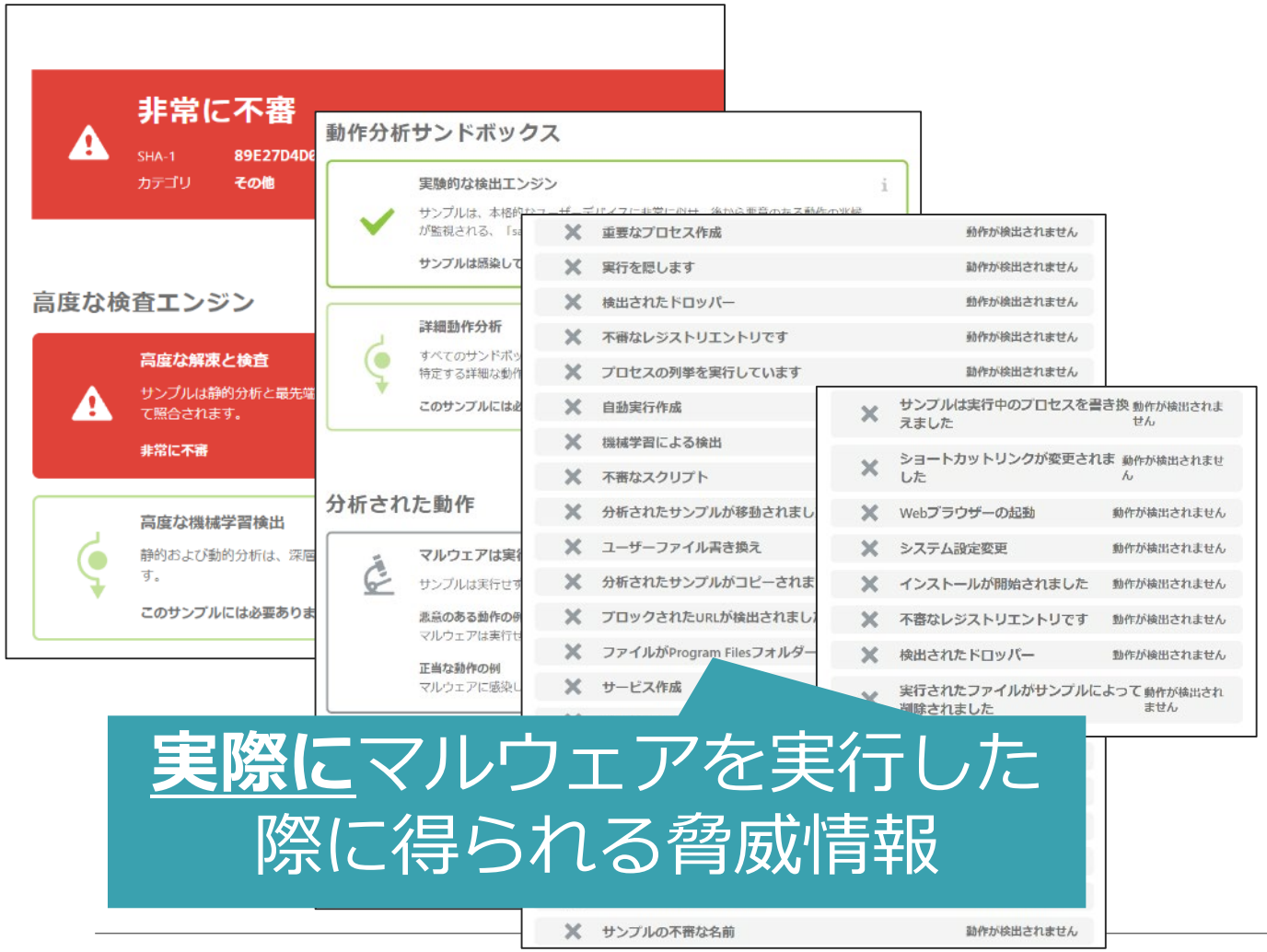
不審なファイルを
自動解析・自動防御

解析中はファイルを
不活性化
誤って実行することを防止

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

未知の脅威を発見した場合

※クラウドサンドボックス有の場合



実際にマルウェアを実行した際に得られる脅威情報

EDRがなくても
サンドボックス上の
振る舞い結果をレポート

（参考）クラウドサンドボックスのバンドル製品

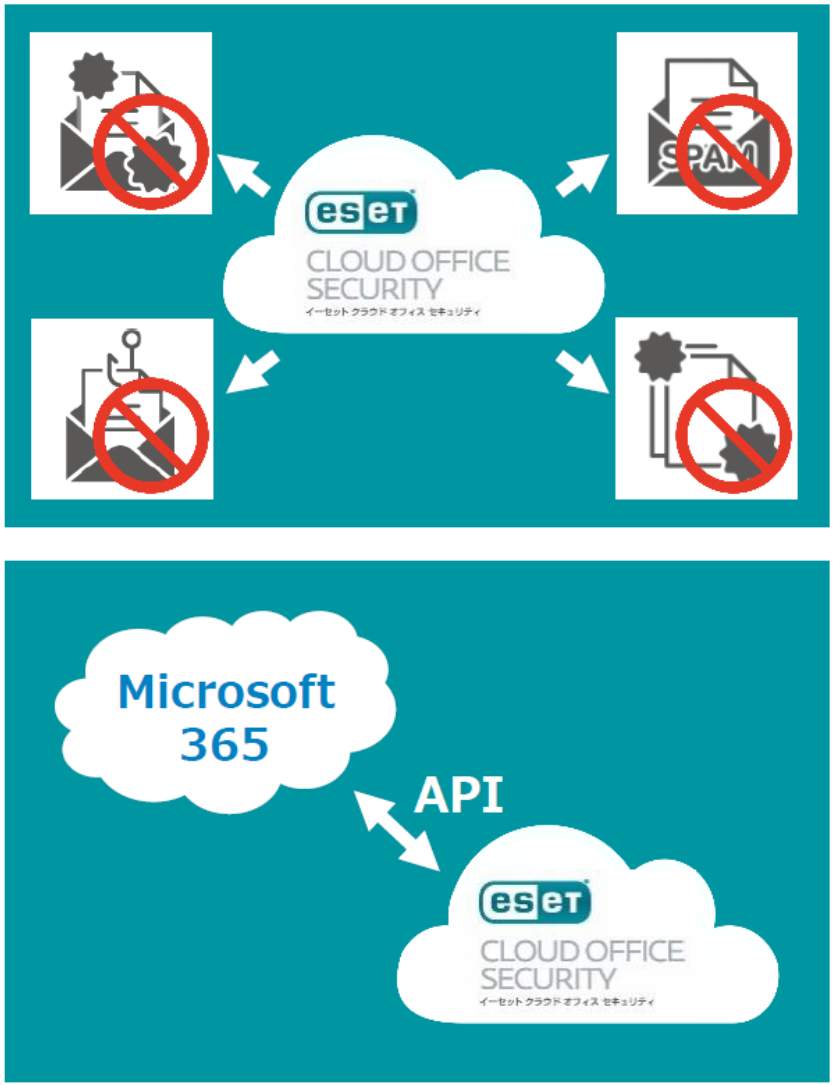
ESET PROTECT Entry クラウド

ESET PROTECT Essential クラウド

ESET PROTECT Advanced クラウド

ESET PROTECT Complete クラウド

Microsoft 365の対策でEDTDを動作させる



クラウド側の Attack Surface

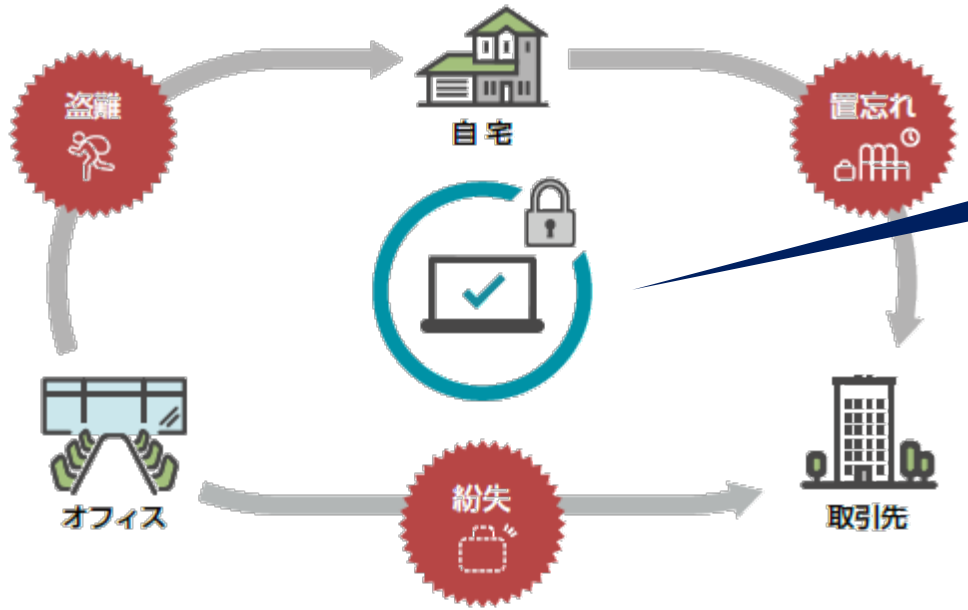
SharePoint、OneDrive ExchangeOnline、Teams で共有されてしまう 脅威に対応

クラウドサンドボックス機能（EDTD）連携を実装

（参考）クラウド対応のフルディスク暗号化

ESET FULL DISK ENCRYPTION
イーセット フルディスク エンクリプション

- クライアントPCディスク全体の暗号化



プリブート認証の導入によりPCの紛失・盗難に起因する、
内部の重要データや個人情報などの漏えいを防ぎます。

モバイルPCの AttackSurface対策

クラウド管理コンソール で**一元管理**

※1 ESET PROTECTソリューションを導入している必要があります。
※2 導入端末がクライアント管理用プログラム（ESET PROTECT）で管理されている必要があります。
※3 Windows環境のみの対応です。

ESET PROTECTソリューション シリーズは検討に値するか

Canon

Attack Surfaceを減らすための投資

壊滅的被害をもたらすマルウェア防御 (BCP)

少ない人的リソース前提のインフラ検討

8レイヤのAttack Surface対策
（＋MS365向けの対策・短スパンでの機能向上）

クラウドサンドボックス連携のスピード
（＋MS365のAttack Surfaceもカバー）

クラウドでの統合管理

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

https://eset-info.canon-its.jp/malware_info/

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**