＼情報セキュリティ対策のキホン／

サイバー攻撃からエンドポイントを守る

～ 防御編 ～

はじめに

サイバー攻撃が頻発しており、ほぼ毎日の様にセキュリティ事故に関する
ニュースを目にするようになりました。

サイバー攻撃は、金銭の要求、個人情報や機密情報の搾取、事業へのダメージを
目的に行われているという事実を認識し、必要な対策をとることがすべての組織に
求められています。

サイバー攻撃からエンドポイントを守るために、弊社では『予防』『防御』『分析』
の3つをまわすことが大事だと考えております。
本書では、『防御編“あらゆる種類の攻撃から守る”』をご紹介いたします。

目次

※ 本資料ではPC等のエンドポイントにおける基本的な備えを中心にご案内いたします。

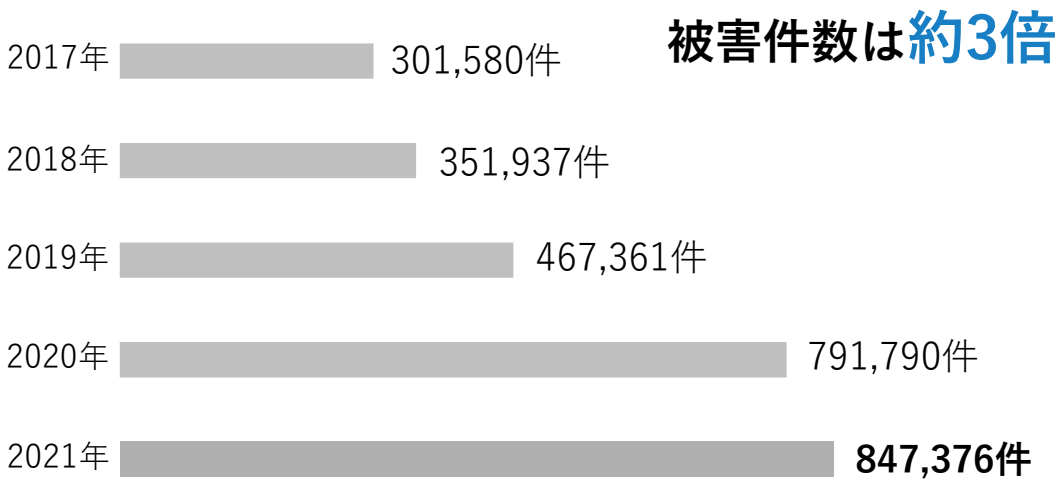
1

サイバー攻撃の被害状況について

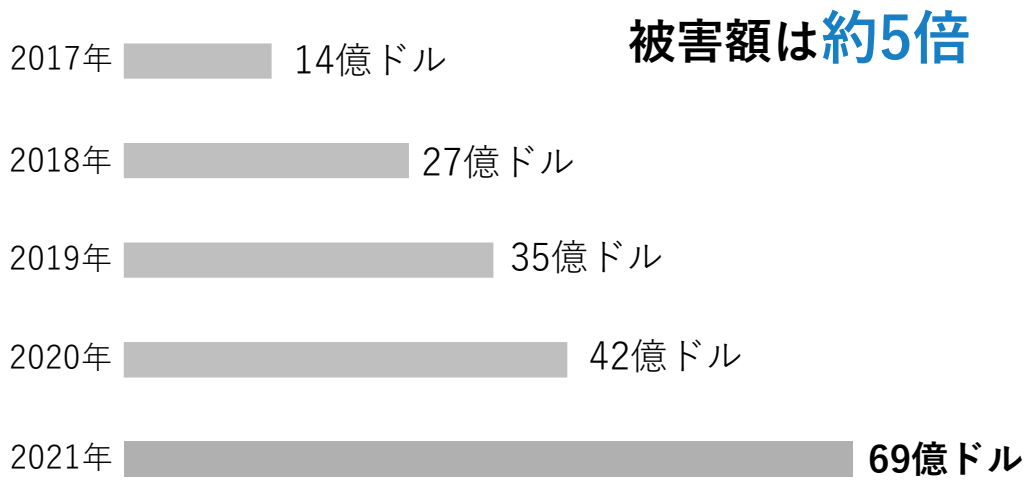
被害が増加しています（米国）

FBI（米国連邦捜査局）によると、 2021年度に観測されたサイバー攻撃の件数は過去5年間増え続け847,376件、被害額は69億ドルでした。
世界中でサイバー攻撃が増加しており、すべての組織において適切なセキュリティ投資を行い、万が一に備えるべきだと言えます。

【被害件数の推移】



【被害額の推移】

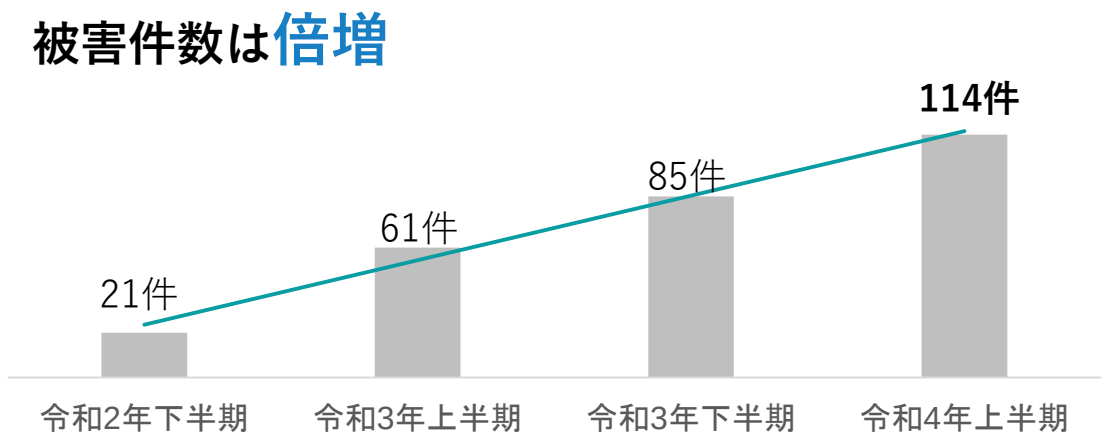


出典）IPA 独立行政法人情報処理推進機構「情報セキュリティ白書 2022」
https://www.ipa.go.jp/security/publications/hakusyo/2022.html

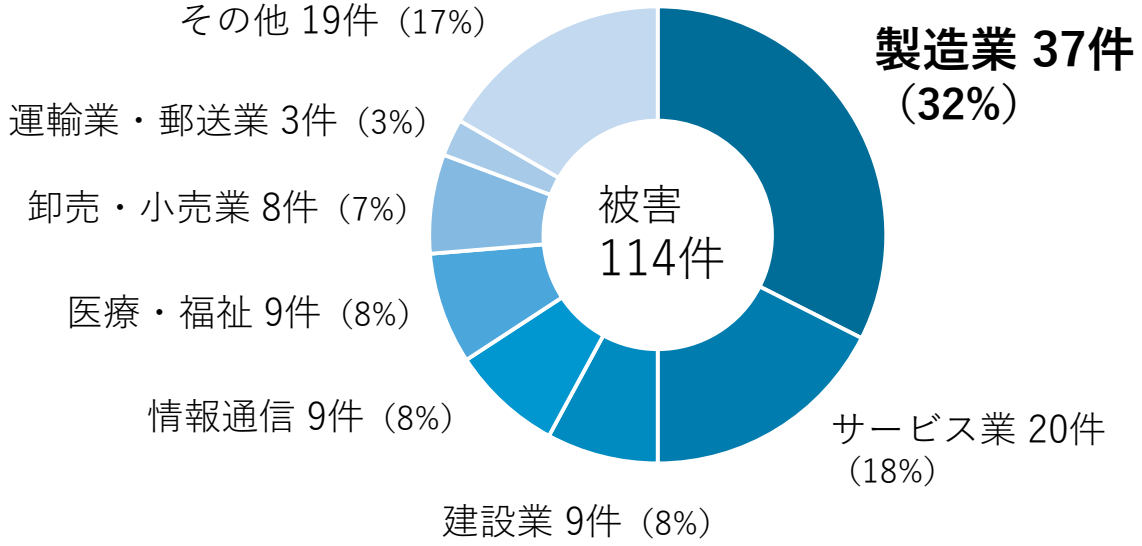
被害が増加しています（日本）

サイバー攻撃の代表的な手口の一つであるランサムウェアの情勢をご紹介します。
警察庁が発表したデータによりますと、ランサムウェアの被害は令和2年下半期から令和4年上半期にかけて右肩上がりで増加しています。
このうち、製造業が全体の32%を占めていますが、**業種を問わず被害に遭っている**ことが確認できます。さらに警察への報告を行わなかったり、被害に気付いていないケースを含めると、被害件数は相当な数と思われます。

【被害件数の推移】



【被害の業種別報告件数】

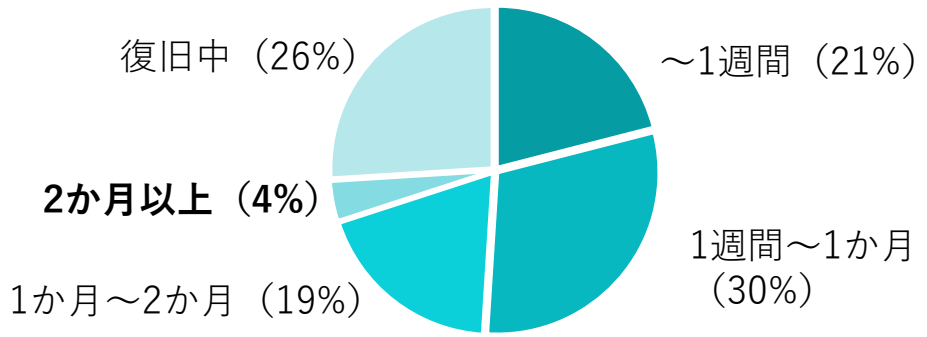


出典）警察庁 「令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

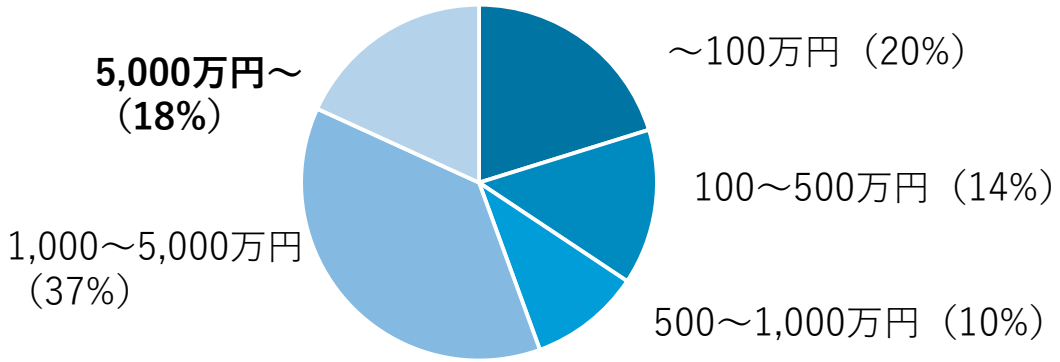
復旧や調査費用の実態（日本）

サイバー攻撃の被害に遭った場合、感染したシステム等の**復旧までに2か月以上**要した事例や、**調査・復旧に5,000万円以上**のコストを費やしたという事例が確認されています。

【復旧に要した期間】



【調査・復旧費用の総額】



出典）警察庁「令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

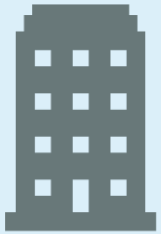
また、被害内容の確認やPC内部に残された証拠解析による影響・被害範囲を特定するフォレンジック調査を実施する場合、PCとサーバー数台でも数百万円、被害状況によっては数千万円のコストが必要になるというレポートも公開されています。

出典）日本ネットワークセキュリティ協会(JNSA)「インシデント損害額調査レポート 2021年版」
https://www.jnsa.org/result/incidentdamage/2021.html

費用以外の影響

経営幹部が解任または辞任

32%

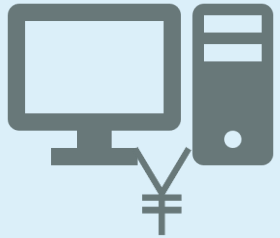


営業停止

25%

ブランドイメージの低下

56%



身代金を支払った企業のうち「再び攻撃を受けた」企業

80%

出典）セキュリティ企業 グローバル調査結果

「サイバーセキュリティ経営ガイドライン」では、経営者がリーダーシップを取り、組織内の仕組みや体制作りのためにセキュリティ投資を行い、耐性を高めることが肝要であると謳っています。適切なセキュリティ投資を行わずサイバー攻撃を受けた場合、**事業継続へのインパクトや社会的な信頼の低下**などの影響を受けていることがわかります。

出典）経済産業省　独立行政法人　情報処理推進機構（IPA）　「サイバーセキュリティ経営ガイドライン ver3.0」
https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf

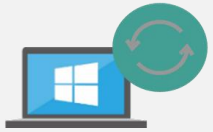
2

あらゆる種類の攻撃から守る３つの対策

3つの対策でサイバー攻撃を“防御”する

私たちが日頃利用しているPCは、さまざまな場所からネットワークにアクセスし、
使用方法も多岐に渡るため、高い感染リスクに晒されると考えるべきです。
また、PCは**「機密情報が存在する場所」**でもあり**「感染した際にマルウェアが実際に活動する場所」**でもあるため、万が一の攻撃に備えて、PC側で “防御” すべきと言えます。
マルウェアは大別すると、パターンファイル化されている「既知の脅威」、新種を含む
怪しい挙動をする「未知の脅威」の2種類。これらの脅威から防御する手段として、
当社がクラウドサービスとしてご提供しているISM CloudOneを中心とした具体的な
エンドポイントセキュリティ対策を3つご紹介します。

基本的な対策



- 正常稼働をキープする
- リスクを把握する

既知の脅威対策

- すべてのPCをカバーする
- 標準機能を集中管理

未知の脅威対策

- 先読み技術で防御
- 感染箇所も特定

ウイルス対策ソフト診断

基本的な対策 ～正常稼働をキープする～

ウイルス対策ソフトをPCにインストールしていたとしても、入れたまま放置していては意味がありません。アップデートして最新の状態で利用し続けることで、パターンファイル化されているマルウェアの感染を防ぐことができます。
そのため、まずはインストールしている**ウイルス対策ソフトが最新の状態に保たれ、正常稼働しているか**どうかを確認する必要があります。

「ウィルス対策ソフトに問題あるPC」を自動であぶり出し！

ハードウェア名	NG内容（ウイルス対策ソフトウェア診断）
WIN10DEMO	未インストール
SANAI-WIN10-01	Windows Defender (x64)
TECH1	ウイルスバスター クラウド (x64)

・ドリルダウンで「NG判定」されたPCリストを表示
・NGの判定理由を確認

ウイルス対策ソフトウェア情報 1	
製品名	ウイルスバスター クラウド (x64)
プログラムバージョン	16.0
エンジンバージョン	12.000.1008
パターンバージョン	15.877.00
常駐状態	常駐
最新エンジンバージョン	99.999.9999
最新パターンバージョン	99.999.99

「問題あるPC」判定の原因箇所をハイライトで表示
ウィルス対策ソフトのエンジンとパターンファイルが更新されていない危険な状況となっています！

基本的な対策 ～リスクを把握する～

ウイルス対策ソフトがインストールされていないPCが組織内に1台でも存在する場合、この1台が感染してしまうとネットワークを介して他のPCや共有サーバへの感染原因となりかねません。感染したPCはインターネットを経由して個人情報など守るべき情報を搾取される危険性が高まり、情報漏えいなどの二次被害を招く可能性もあります。そのため、**ウイルス対策ソフトがインストールされていないPCの有無**を確認することも重要です。

「ウィルス対策ソフトに問題あるPC」を自動であぶり出し！

ハードウェア名	NG内容（ウイルス対策ソフトウェア診断）
WIN10DEMO	未インストール
SANAI-WIN10-01	Windows Defender (x64)
TECH1	ウイルスバスター クラウド (x64)

・ドリルダウンで「NG判定」されたPCリストを表示
・NGの判定理由を確認

インストールされているべき
ウィルス対策ソフトの不備は危険！

既知の脅威対策 ～すべてのPCをカバーする～

Defender Control

ウイルス対策ソフトがインストールされていないPCが存在し、且つソフトの在庫がない場合は、Windows 10/11に標準搭載されている「Microsoft Defender」を活用するのも手段の一つです。
Microsoft Defenderは、マルウェアを検知し取り除く機能を搭載したWindowsのセキュリティ対策ソフトです。
Microsoft社によるとMicrosoft Defenderは、ここ数年のさまざまな評価テストにおいてマルウェア感染に対する保護スコアで高評価を得ています。
Microsoft Defenderはパターンファイル化されている「既知の脅威」からPCを保護することができるため、設定を有効にすることで既知のマルウェアの感染リスクを低減できると言えます。
「Defender Control」は、**Microsoft Defenderの設定をコンソールで一括管理できるほか、端末ごとの設定状況やマルウェアの検知状況を確認できる**サービスです。

※ ウイルス対策ソフトをインストールしている場合、自動的に無効に設定されます。

出典）　Microsoft社「Microsoft 365 Defender 業界テストでのトップ スコア」
https://docs.microsoft.com/ja-jp/microsoft-365/security/defender/top-scoring-industry-tests?view=o365-worldwide

既知の脅威対策 ～標準機能を集中管理～

Defender Control

設定した制御設定がクライアントに正しく適用されているかどうか確認したり、
ウイルス対策スキャンでマルウェアの疑いがあるファイルやアプリケーションが
検知されたかどうかをコンソール画面で確認できます。

●稼働状況を確認することで維持管理

- 設定の有無を一覧で把握
- PCごとの設定状況を確認
- 制御設定が正しく適用されているか確認

コンピューター名	ログオンユーザ...	ウイルスと脅威の防止の設定
WIN10J1909	user1	有効
LAPTOP-NVB6U479	ladmin	

ウイルスと脅威の防止の設定	
ウイルスと脅威の防止の設定	有効
リアルタイム保護	有効
クラウド提供の保護	有効
サンプルの自動送信	安全なサンプルを自動的に送信する
マルウェア対策サービスが通常の優先順位でスタートアップすることを許可する	有効
マルウェア対策サービスの常時実行を許可する	無効
ヘッドレス UI モードを有効にする	有効
コントロールされたフォルダーアクセス	無効

●マルウェアの検知状況を確認

- PCごとにマルウェア検知数を表示
- 検知されたマルウェアの詳細を把握
- 感染の疑いがあるファイルやアプリケーションを確認

ログオンユーザー名	コンピューター名	スキャン方法	マルウェア数（現在の脅威）	マルウェア数（保護の履歴）
administrator	DEMO10-ENT	クイック	0	3
user	TECH2	クイック	0	0
user01	OVERSEAS1	クイック	0	0

3 件 [1-3]

マルウェア名	検知日時	影響を受けた項目
Virus:DOS/EICAR_Test_File	2021/11/15 09:36:00+09:00	file:_C:\Users\Administrator\Desktop\...
Virus:DOS/EICAR_Test_File	2021/11/15 09:35:59+09:00	file:_C:\Users\Administrator\Desktop\...
Virus:DOS/EICAR_Test_File	2021/11/20 23:40:47+09:00	file:_C:\Users\Administrator\Desktop\...

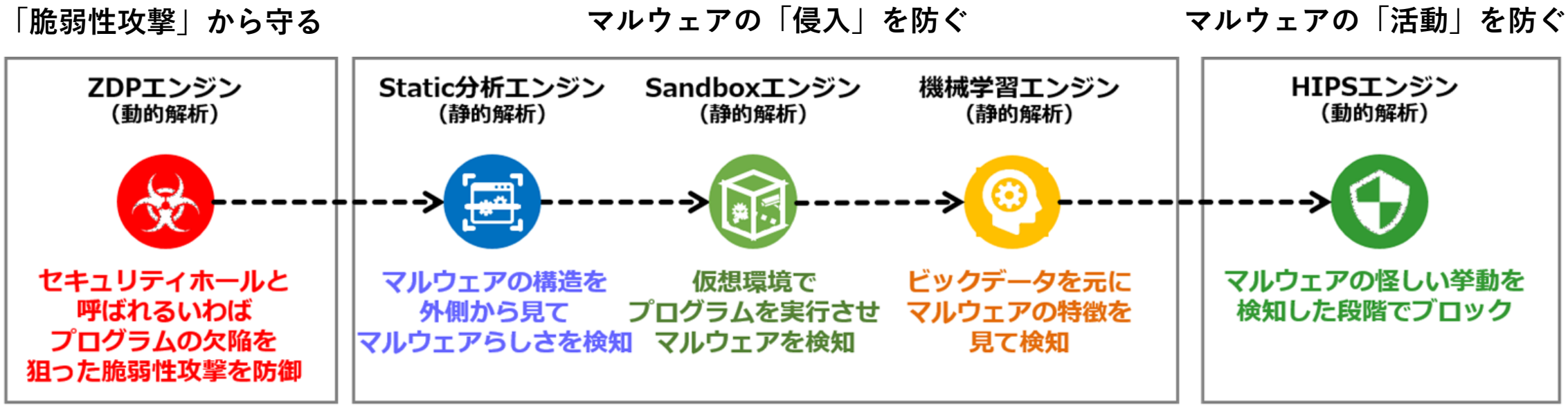
※ ウイルス対策ソフトをインストールしている場合、自動的に無効に設定されます。

ふるまい検知

未知の脅威対策 ～先読み技術で防御～

パターンファイル化された「既知の脅威」は一般的なウイルス対策ソフトで防ぎ、
されておらず新種を含む「未知の脅威」は攻撃者の思考を先読みして防御する
ふるまい検知機能を利用することで、一般的なソフトでは対応しきれなかった領域
までカバーすることが可能です。

●パターンファイルに依存しない5つのエンジン



出典）株式会社FFRIセキュリティ「次世代エンドポイントセキュリティFFRI yarai マルウェア検出速報」
https://www.ffri.jp/products/yarai/defense_list.htm

未知の脅威対策 ～先読み技術で防御～

ふるまい検知

既にリリースしているバージョンで、数々の未知のマルウェアの脅威を排除した実績があります。従来ソフトでは防ぎきれなかった標的型攻撃やランサムウェアによる攻撃、ゼロデイ攻撃の対策としても有効です。

マルウェアの種類	攻撃・マルウェア名称	発生報道時期	防御エンジンリリース時期
Emotet	2023年3月版	2023年3月	2021年10月
	2022年11月版		2021年10月
	2022年5月版		2021年5月
	2022年6月版		2021年5月
ランサムウェア	BlackHunt	2023年2月	2020年4月
	PolyVice	2023年1月	2019年11月
	Agenda	2022年12月	2022年6月
	Vohuk	2022年12月	2019年11月
	AESRT	2022年12月	2019年11月
特定のイベントや事象に関連する攻撃	ワクチン予約を装うフィッシングサイトに関するマルウェア	2021年9月	2021年5月
	東京オリンピックに関係する日本語のファイル名を持つマルウェア	2021年7月	2019年1月

出典）株式会社FFRIセキュリティ 「次世代エンドポイントセキュリティFFRI yarai マルウェア検出速報」
https://www.ffri.jp/products/yarai/defense_list.htm

- 高性能な防御エンジン
- 純国産セキュリティ製品
- 中央省庁や金融機関等の多数の導入実績

ふるまい検知

未知の脅威対策 ～感染箇所も特定～

検知されたマルウェアのハッシュ値を取得するため、他にも感染したPCはないか、
駆除されているかどうかを確認できます。
感染したPCがある場合、対象PCと感染箇所であるファイルパスも確認できるため
影響範囲の特定も可能です。

●ハッシュ値ごとの感染状況を確認

・いつ検知されたのか
・マルウェアが潜むPCは何台あるのか

最新の検知日時	マルウェアのハッシュ値	検知されたクライアント数	駆除されたクライアント数
2022/10/25 09:18:03+09:00	275a021bbfb6489e54d471899f7db...	2	1
2022/10/25 07:52:27+09:00	1751ac12e70e15b4f76c16775cd32...	1	0
2022/10/25 07:37:35+09:00	6166aee0d9e49545b98e69a68388...	1	0

●影響範囲を特定

・どのPCが感染したのか
・感染したファイルは何か
・駆除されているのかどうか

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

マルウェアが検知されたクライアント

4 件 [1-4]

コンピューター名	ファイルパス	駆除ステータス
LAPTOP-A1UP5N37	C:\Users\q-sen\Desktop\マルウェア.exe	駆除されていない
LAPTOP-V4R7UE60	C:\Users\admin\Desktop\EICAR.com	駆除されていない
LAPTOP-V4R7UE60	E:\EXPO\EICAR.com	駆除済み
LAPTOP-V4R7UE60	E:\Virus\EICAR.com	駆除されていない

3

ism CloudOne のご紹介

ISM CloudOne とは

クラウド型PC管理 ＆ セキュリティ対策サービス

IT資産管理・クライアント
管理ツール（SaaS・クラウド）

7年連続

※デロイト トーマツ ミック経済研究所株式会社
「内部脅威対策ソリューション市場の現状と将来展望 2022年度」
https://mic-r.co.jp/mr/02620/

導入実績

80,000社以上

※2022年10月時点

世界導入国

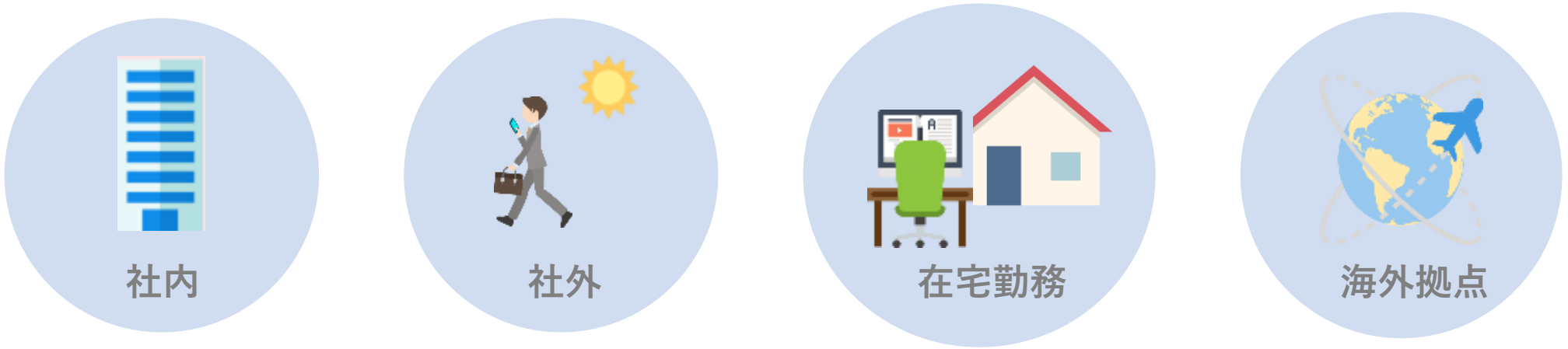
55ヵ国以上

JQA-IC0048

＼ISO27017認証取得／
安全なクラウドサービスを提供！

様々な環境下にあるPCの管理が可能

インターネット接続のみで利用できるため、オフィスはもちろん在宅勤務や支店、
店舗、海外拠点PCなど、様々な環境下にある端末を管理できます。
インターネットリモートコントロール機能も提供しており、管理者はどこからでも
ヘルプデスク対応が可能。リモートワーク中でも手間を掛けずに運用管理を行えます。

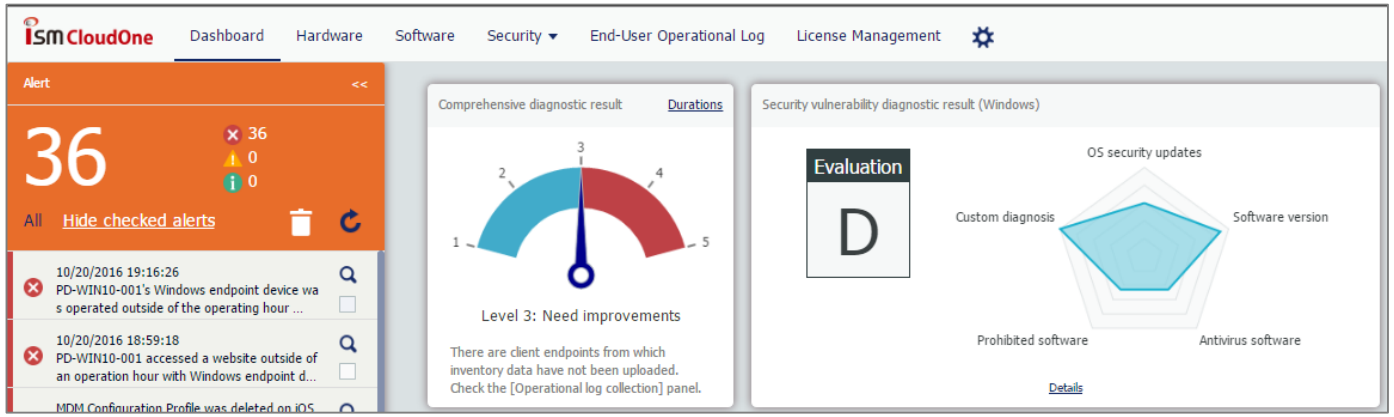


多言語対応

管理コンソールは日中英3か国語に対応しています。
海外現地法人に管理者がいる場合にその国だけを任せる運用も可能です。
国内のみならず海外拠点の端末管理が可能です。

日本語

英語



海外拠点の現地IT管理者も利用できます！

＋αの機能でセキュリティ対策を後押し

本資料でご紹介させていただいた機能以外にも、データの不正持ち出しを制御したり、
Webサイトへのアクセスを制御する機能などを取り揃えております。
必要な機能を必要な分だけ組み合わせてご利用いただけます。

PC管理・セキュリティ対策全般をカバー

このような課題を
お持ちの方

- PCのセキュリティ状態を把握したい
- 海外グループ企業を含めて管理したい
- 情報漏えい対策、サイバー攻撃への対策を行いたい

ISM CloudOne

世界55か国以上で利用される
クラウド型PC管理&セキュリティ対策サービスです

インターネット環境下にある端末は場所を問わず管理

自動脆弱性診断で端末の問題がひと目で分かる

PCのセキュリティ対策を実現

- 自動脆弱性診断
- 操作ログ取得 個人情報探査
- 外部デバイス制御
- URL フィルタリング
- ふるまい検知
- Win10管理・暗号化

ISO27001の取得・維持管理のための支援も可能！

ご興味に合わせてご案内します

もう少し詳しく知りたい

ISM CloudOne 公式ホームページ
https://ismcloudone.com/

その他資料がほしい

お役立ち資料や製品カタログなど
各種資料ダウンロード
https://ismcloudone.com/download/

詳しく聞いてみたい

お気軽にお問合せください
お問い合わせ・オンライン相談
https://ismcloudone.com/inquiry/