＼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

～ 予防編 ～

はじめに

サイバー攻撃の手口はますます巧妙化し、被害は日々増え続けています。
大規模から中堅中小といった組織規模や、セキュリティ専門家がいない、人手が
足りないといった課題を抱える組織も少なくないと思いますが、セキュリティ対策が
手薄になっている組織から被害に遭遇する可能性が高くなると言えます。

万が一、サイバー攻撃による情報漏えい事故などが起きてしまえば、営業停止や
ブランドイメージの低下を招く可能性もあるため、サイバー攻撃への予防措置が
必要不可欠です。

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、『予防編』として“すべてのエンドポイントの脆弱性をつぶす”
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。

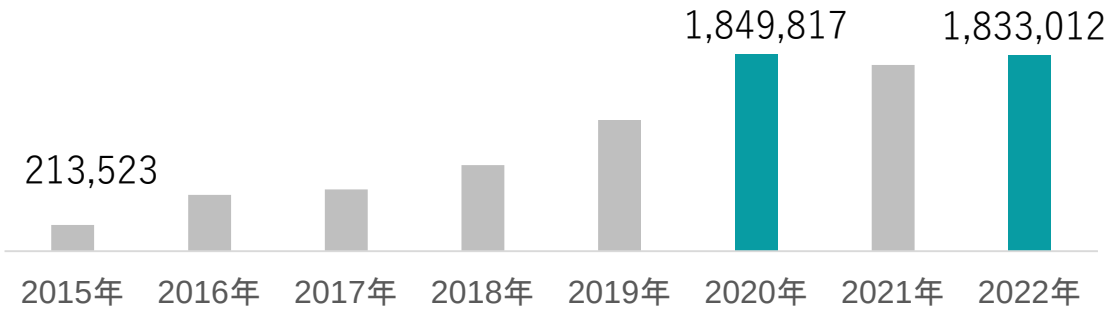
1

サイバー攻撃の
動向と手口について

サイバー攻撃の動向

2015年から2020年にかけてサイバー攻撃の件数は約8.5倍に増加しています。
このような状況下で被害を受けないためにも、社員一人一人の意識を高めないといけませんが、日々の業務に追われ、細心の注意を払えない時もあるかと思います。
とある組織で標的型攻撃の訓練サービスを実施したところ、6割もの社員が怪しいURLを開いてしまったという結果も出ています。手口が巧妙化し、人の意識だけで防ぐことが難しくなっているため、セキュリティホールを放置しないことに加え、システムを利用した対策が必要となっていると言えます。

５年間で約8.5倍以上増加



出典）国立研究開発法人情報通信研究機構「NICTER観測レポート 2022」
https://csl.nict.go.jp/report/NICTER_report_2022.pdf

10人に6人がURLに接続

サイバー攻撃の代表的な手口

ランサムウェア

【目的】

お金の要求

**ソフトウェアを
ダウンロードして感染**

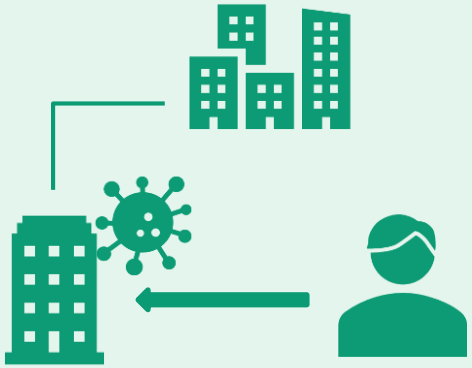
標的型攻撃

【目的】

情報窃取

上司を装ったメールで感染

サプライチェーンリスク



［目的】

ダメージ

海外のサプライヤーや
取引先企業を攻撃される

2

すべてのエンドポイントの脆弱性をつぶす３つの対策

3つの対策でサイバー攻撃を“予防”する

サイバー攻撃に対抗するには、攻撃する隙を作らずセキュアな状態を維持する「内部対策」、Webサイトなどインターネットを経由したウイルスの侵入を防ぐ「入口対策」、万が一ウイルスが侵入した場合に、感染したPCを踏み台に機密データを格納したサーバへの感染拡大を防ぐ「出口対策」を複合的に行い、多層防御することが有効です。
ここからは、ISM CloudOneを中心としたエンドポイントセキュリティ対策をご紹介します。

01 内部対策

- セキュリティレベルを確認
- 脆弱性の発見から是正措置までをスムーズに

02 入口対策

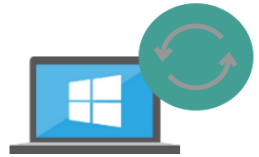
- 豊富なURLデータベース
- カテゴリごとにアクセス制御

03 出口対策

- 外部の不審なサーバとの通信を制御
- インターネット経由の情報漏えいを防止

内部対策 ～セキュアな状態を維持する～

自動脆弱性診断



ウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）を最新の状態にしておくことで、パターンにマッチングするウイルスの感染を防ぐことができます。また、OSやAdobe等のソフトウェアを最新の状態で使用することで、ゼロデイ攻撃のリスクも低減できます。

●セキュリティレベルを確認

ISM CloudOneをインストールしているPCのセキュリティ状態を総合的に診断

●脆弱性の発見から是正措置までをスムーズに

インストールされているソフトウェアのバージョンやパッチの適応状況を収集し、あるべき理想の姿と突合することで、是正措置が必要な端末をあぶり出す

入口対策 ～ウイルスの侵入経路を減らす～

URLフィルタリング

ウイルスの感染経路である有害なWebサイトや、外部の不審なサーバとの通信をブロックすることで、インターネットを経由したウイルスの侵入と感染を防ぐことができます。

●豊富なURLデータベース

国内シェアNo.1を誇る148種 67億16825万コンテンツ（2023年4月10日現在）を基に、柔軟なフィルタリングとセキュアなインターネット環境を実現

時世に即したカテゴリ区分

児童ポルノ	ライブ動画
マルウェア	ストレージサービス
DBD攻撃	Webメール
著作権や商標権の侵害行為	URL転送変換サービス

出典）アルプスシステムインテグレーション株式会社 「マルチデバイス対応Webフィルタリング InterSafe Csts データベース」
https://www.alsi.co.jp/security/iscats/database/

●カテゴリごとにアクセス制御

アクセスレベルを5段階から選ぶことができるため、組織の運用に併せたアクセス制御が可能

閲覧許可	サイトの閲覧, 書き込み共に可能
規制	規制画面を表示（閲覧不可）
書き込み規制	サイトの閲覧を許可し、 書き込みのみ規制
一時解除 （パスワード入力）	パスワードで例外的に 規制を解除
一時解除 （警告表示）	警告画面を表示 （ボタンクリックで閲覧続行）

出口対策 ～感染拡大による二次被害リスクを最小化～

URLフィルタリング

万が一、PCがマルウェアに感染した場合でも、C&Cサーバとの通信を
遮断することで、攻撃者による悪意ある情報窃取を防ぐことができます。

●外部の不審なサーバとの通信を制御

攻撃者が遠隔操作しているC&Cサーバへのアクセスを遮断し
機密情報を持ち出させない

クラッキング	ウイルスの製造方法やネットワーク、コンピュータ、モバイル端末への不正侵入や不正使用に関連する情報
マルウェア	ウイルスやスパイウェア感染の恐れがあるサイト。 C&C（コマンド＆コントロール）サーバーなどの不正攻撃サイト。※3
DBD攻撃	閲覧することにより、自動的にマルウェア（不正なプログラム）などをダウンロードさせられる恐れがあるサイト
フィッシング詐欺・ワンクリック詐欺	フィッシングサイトやクリックしただけで料金を請求される詐欺サイト※4
公開プロキシ	フィルタリング機能を回避する公開プロキシ
フィルタリング回避	フィルタリング機能を回避する目的ではないが、結果的にフィルタリング機能を回避してしまうサービス

●インターネット経由の情報漏えいを防止

ストレージサービスを利用した情報の持ち出しや、SNSサイトへの
不正書き込みによる情報漏えいを防ぐ

ストレージサービス	インターネット上のディスクスペース提供など、各種ストレージサービス
SNS・ミニブログ	SNS(会員向けコミュニティサイト)およびミニブログサービス※5
掲示板・チャット	ウェブ上の掲示板およびチャットサービス※5
質問サイト	質問者に回答するコミュニティーサービス
ブログ	ブログサービス※5
ウェブメール	ウェブ上でのメールの送受信サービスおよびグリーティングサービスの提供
メーリングリスト	メーリングリストサービス

出典）アルプスシステムインテグレーション株式会社 「マルチデバイス対応Webフィルタリング InterSafe Csts データベース」
https://www.alsi.co.jp/security/iscats/database/

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

シェア No.1

※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

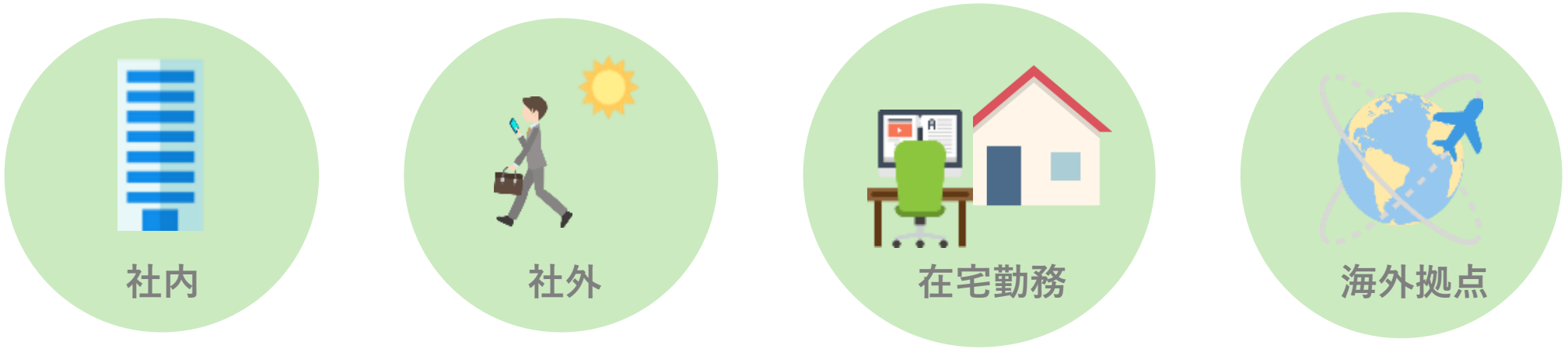
55ヵ国以上

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。

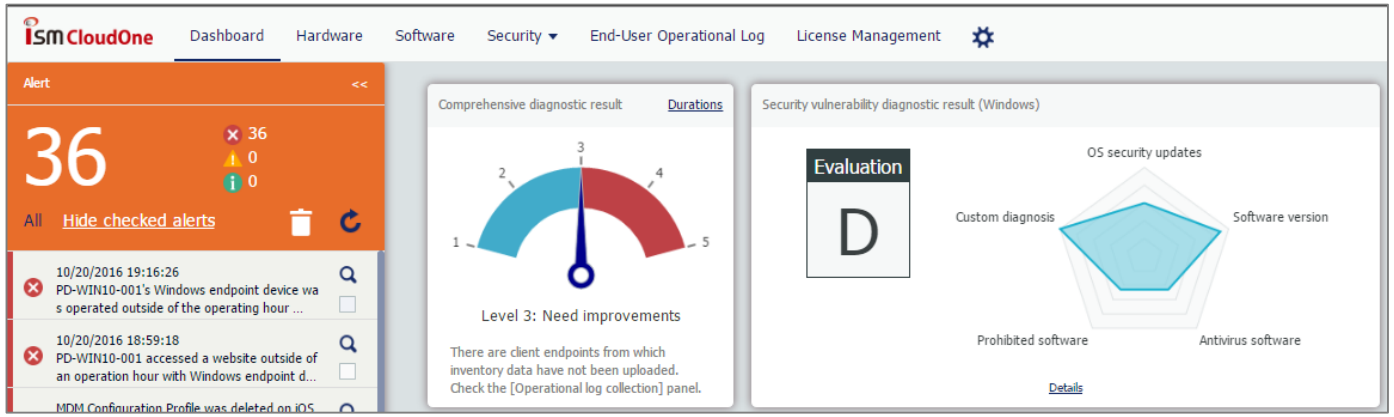


多言語対応

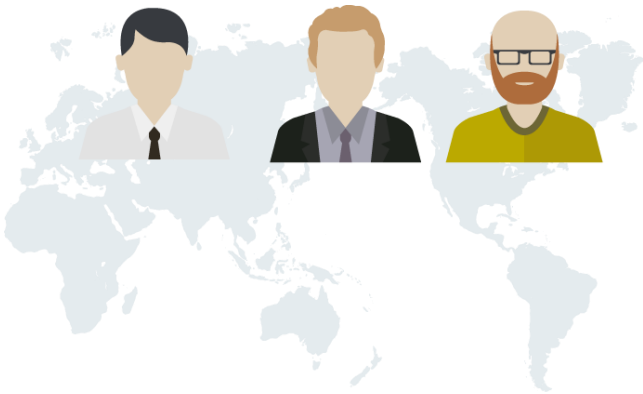
管理コンソールは日中英3か国語に対応しています。
海外現地法人に管理者がいる場合にその国だけを任せる運用も可能です。
国内のみならず海外拠点の端末管理が可能です。

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

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/