Secure Innovation
沖縄から日本、アジア、そして世界へ

セキュリティ被害の最小化を支援する

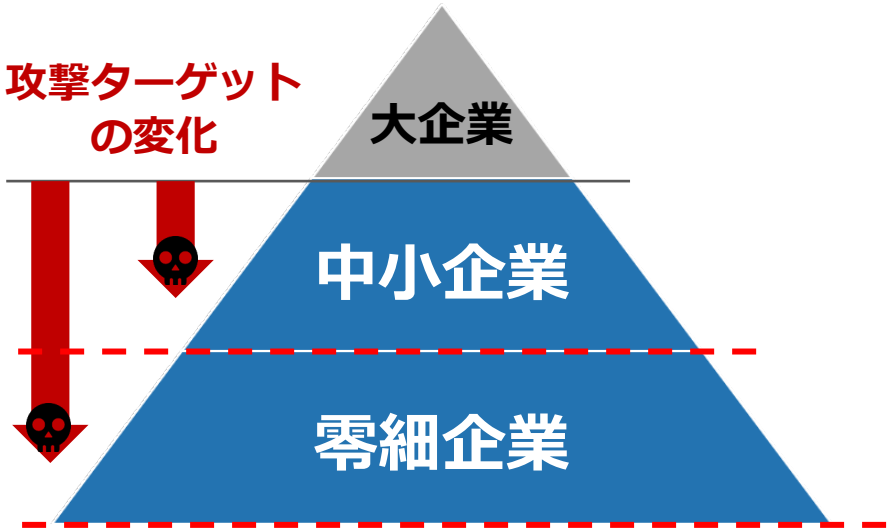
サイバー攻撃早期発見サービス

昨今のセキュリティインシデントの傾向

Secure Innovation
沖縄から日本、アジア、そして世界へ

サイバー攻撃対象の変化

サイバー攻撃の**ターゲット**が
大企業に留まらず、
中小・零細企業にまで
シフトしてきている



対象変化の理由①　大企業に比べて、対策が充分ではない

攻撃者側から見たときに、リスクや、投下リソースが少ないわりに、実入り（リターン）が大きい。

対象変化の理由②　大企業へ繋がる情報を持っている

大企業の取引情報や特許に関わる内部データ
担当者情報（標的型攻撃のネタ）
踏み台にされる（オンライン連携・サプライチェーン）

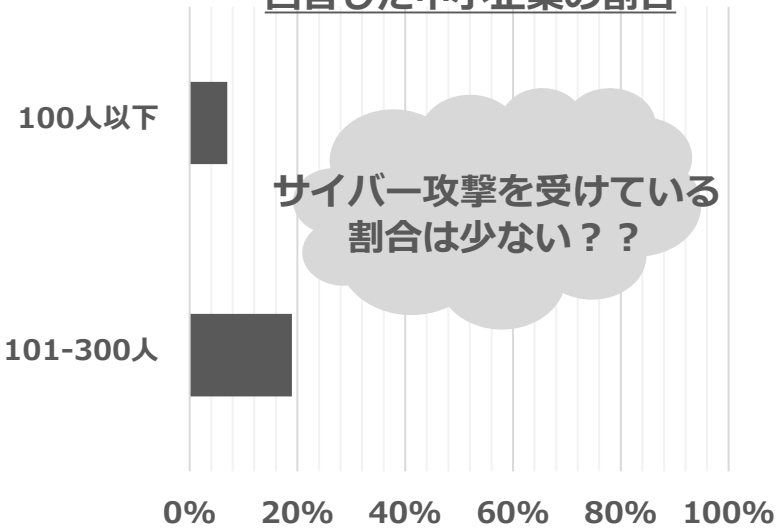
中小企業へのサイバー攻撃の実情

Secure Innovation
沖縄から日本、アジア、そして世界へ

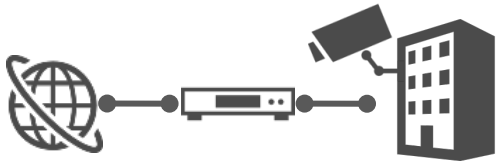
認識と実態には大きなギャップがある

攻撃されているかの自覚 ⟷ **実態として攻撃をうけているか**

実際にサイバー攻撃を受けたと回答した中小企業の割合



IDS(侵入検知システム)を設置して実態調査した結果



中小企業30社中30社(100%)で攻撃を観測

- ほぼ毎日、外部からのポートスキャンで脆弱性の探索
- 外部の不正サイトと通信
- 外部(外国)からPCをリモート操作
- 感染可能性のあるファイルを送信・受信

※尚、被害を受けた数社はマルウェア対策ソフトを、利用するパソコンに適用していた。もしくは、パソコンに適用していると信じていた会社である。

※引用：大阪商工会議所・神戸大学・東京海上日動2018年度共同研究(大阪府内の様々な業種・規模の中小企業30社で数か月間調査)

情報漏洩の現状①

Secure Innovation
沖縄から日本、アジア、そして世界へ

情報漏洩が発覚するまでの期間【2022～2023 サイバーセキュリティクラウドレポート】

攻撃発生

攻撃発覚

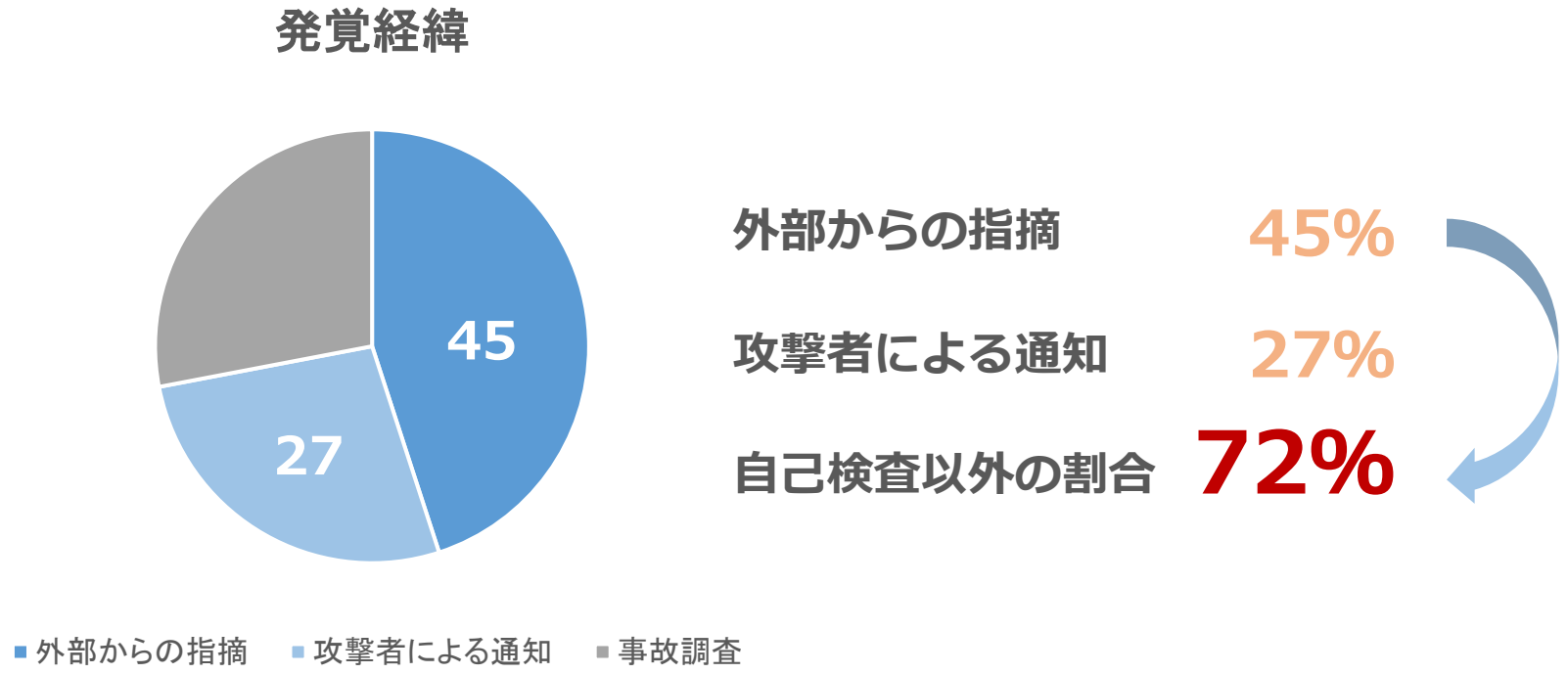
情報漏洩が発覚するまでの期間

2021～2022調査時	349日
2022～2023調査時	397日

情報漏洩の現状②

Secure Innovation
沖縄から日本、アジア、そして世界へ

情報漏洩が発覚した原因が自己検査以外による割合【2023　トレンドマイクロレポート】



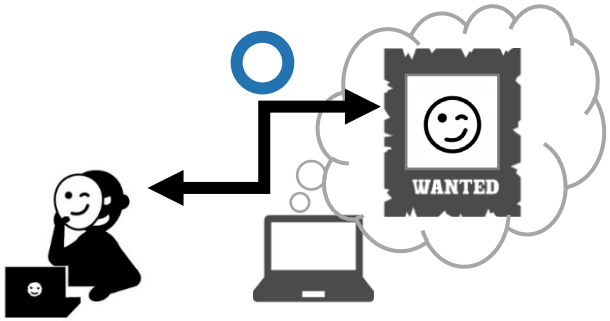
自社では情報漏洩の被害に気付くことさえ出来ず、放置されている状態

ウィルス対策ソフトの現状

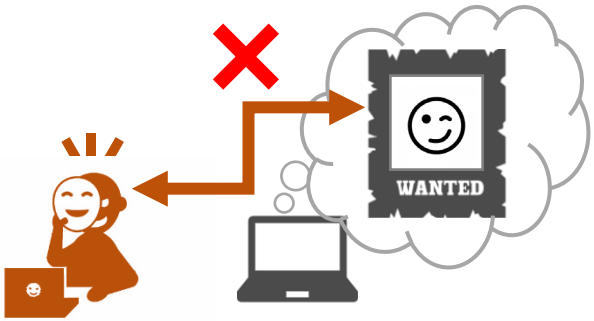
Secure Innovation
沖縄から日本、アジア、そして世界へ

同じ性質でありながら、それぞれが**顔を変えて攻撃を仕掛ける**こともあり、指名手配書（パターンファイル）で判別するウイルス対策ソフトでは見分けるのが難しい状況。

通常のアンチウィルスソフトの場合



指名手配書（パターンファイル）と
一緒だと見つけられる



指名手配書（パターンファイル）と
違うと気づきにくい

指名手配書ではなく、泥棒の触った特徴的な痕跡を見つけ、
顔が変わっていても、潜入されていることに気づく仕組みが必要

サイバーセキュリティへの考え方の変化①

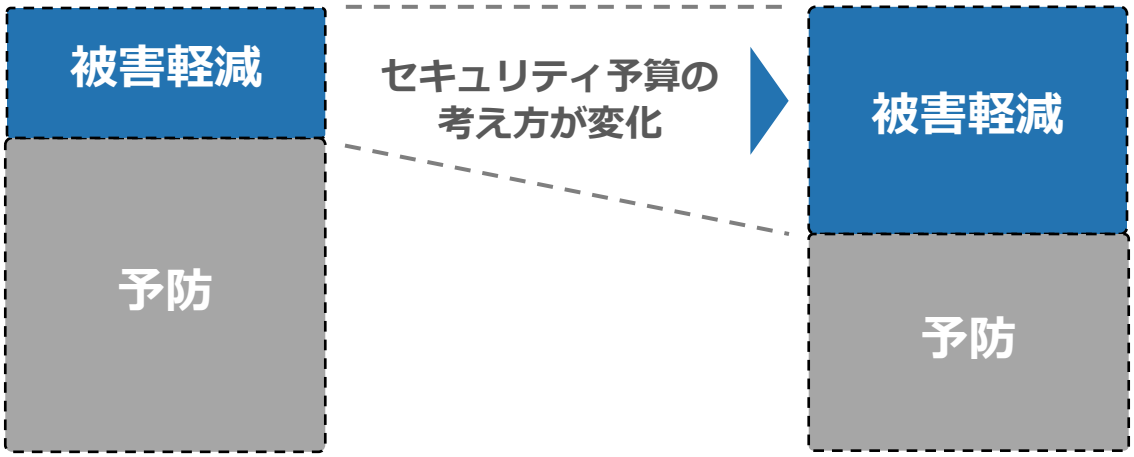
Secure Innovation
沖縄から日本、アジア、そして世界へ

経産省「サイバーセキュリティ経営ガイドラインver.2.0」

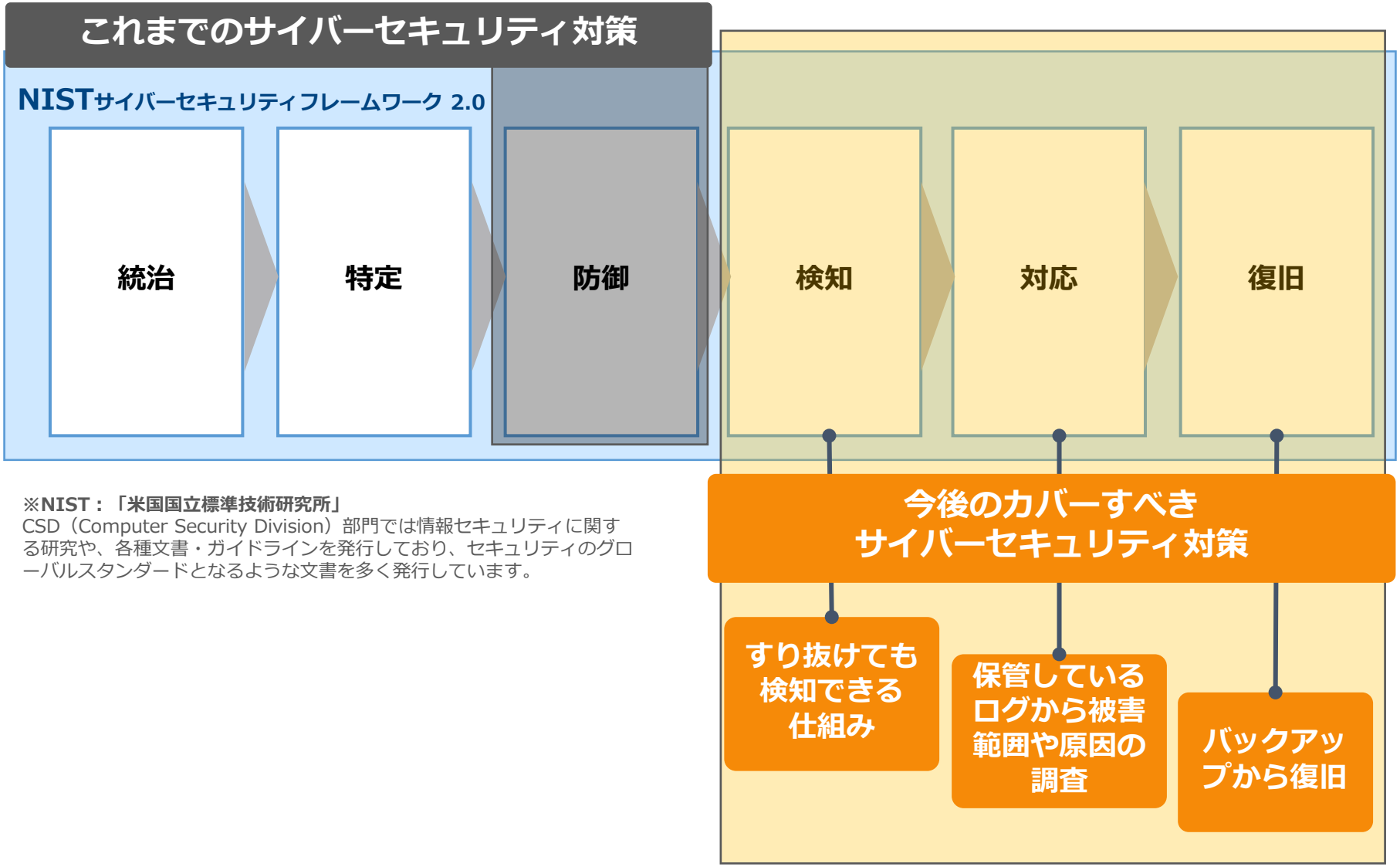
改訂のポイント

- **「攻撃の検知」**を含めたリスク対応体制の構築
- サイバー攻撃を受けた場合の**「復旧への備え」**

「防ぐ」から → **被害に遭う前提で**



サイバーセキュリティへの考え方の変化②



※NIST：「米国国立標準技術研究所」
CSD（Computer Security Division）部門では情報セキュリティに関する研究や、各種文書・ガイドラインを発行しており、セキュリティのグローバルスタンダードとなるような文書を多く発行しています。

（参考）ログ・証跡管理の必要性

Secure Innovation
沖縄から日本、アジア、そして世界へ

経済産業省

情報セキュリティ管理基準（平成28年版）

12.4.1	利用者の活動、例外処理、過失及び情報セキュリティ事象を記録した イベントログを取得し、保持し、定期的にレビューする。
12.4.2	ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護する。
12.4.3	システムの実務管理者及び運用担当者の作業は、 記録し、そのログを保護し、定期的にレビューする。

厚生労働省

医療情報システムの安全管理に関するガイドライン（平成２９年５月版）

6.5-B(3)	個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、 定期的にその内容をチェックして不正利用がないことを確認しなければならない。

公益財団法人 金融情報システムセンター

金融機関におけるコンピュータシステムの安全管理基準（令和２年3 月版）

実10	アクセス履歴を管理すること
実38	オペレーションの記録、確認を行うこと。
実63	取引の端末機操作の内容を記録・検証すること。

実際に、**被害が発生**した際に**証拠となる情報を確保**しておく必要があり、
近年、様々なガイドラインで、ログ・証跡管理の必要性が示されている。

しかし、それを解決するには・・・

Secure Innovation
沖縄から日本、アジア、そして世界へ

主に検討される製品

EDR（Endpoint Detection and Response）

ログ管理製品

３K（高い）が導入ハードル

高度な専門性

高額な料金

高負荷な運用

EISS（アイズ）の製品コンセプト

Secure Innovation
沖縄から日本、アジア、そして世界へ

セキュアイノベーションのEISSなら
低コストで自ら早期発見が可能に

少ない投資でセキュリティ被害を極小化

EISS（Endpoint Incident Scanning Service）

エンドポイントにおける様々なログや揮発性データを定期的に記録、分析することにより情報漏洩等の被害の可能性に気付かせ、早期の事後対処アクションにつなげる。

予防		被害軽減・事後対処
ウィルス対策ソフト	×	EISS アイズ

EISSの特長

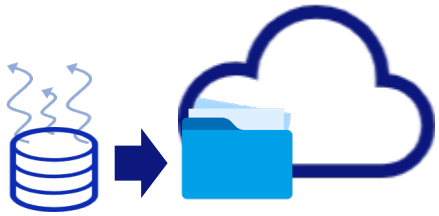
Secure Innovation
沖縄から日本、アジア、そして世界へ

デジタルフォレンジックの観点による検知

EPPが行うようなマルウェア自体の検知ではなく、
マルウェア感染後に発生する痕跡を元に危険性を検知します。
検知後の調査やバックアップからの切り戻し等、
お客様による早期対応に寄与します。

重要なログデータ保管（揮発性データの保管）

インシデント発生後の追跡調査にはマルウェアの痕跡を示す
ログ等のデータが必要になるため、それを保管しておくことが重要です。
但し、それらのデータの多くは揮発性(=電源を切ると削除される）があり、
利用者がよほど意識しない限りはその保管は難しいと言えます。
EISSはそれらの重要なログデータを毎日収集しており、
お客様に代わりクラウド上に保管しているため、
ファストフォレンジックが必要なケース等、
いざという際のデータ活用が可能です。



EISSの効果①

Secure Innovation
沖縄から日本、アジア、そして世界へ

従来型のアンチウイルスソフト

すり抜けた攻撃に気付かないことが多い

情報漏洩が発覚するまでの期間
【2022～2023 サイバーセキュリティクラウドレポート】

397日

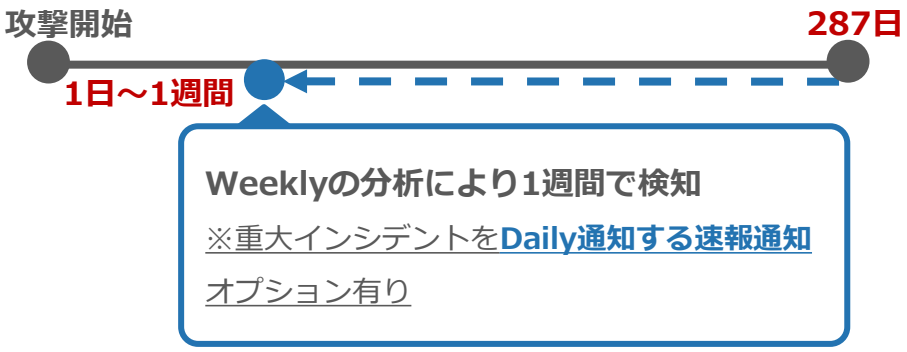
情報漏洩が発覚した原因が
自己検査以外による割合
【 2023 トレンドマイクロレポート 】

72%

アンチウイルスソフトをすり抜ける

EISS アイズ

EISSなら、攻撃検知への遅れを劇的に短縮



ログから攻撃の痕跡を発見

- プロセスリスト
- レジストリ情報
- 権限付与情報
- USB接続情報
- Wi-Fi 情報
- ネットワーク接続リスト
- イベントログ情報
- Windowsセキュリティ情報

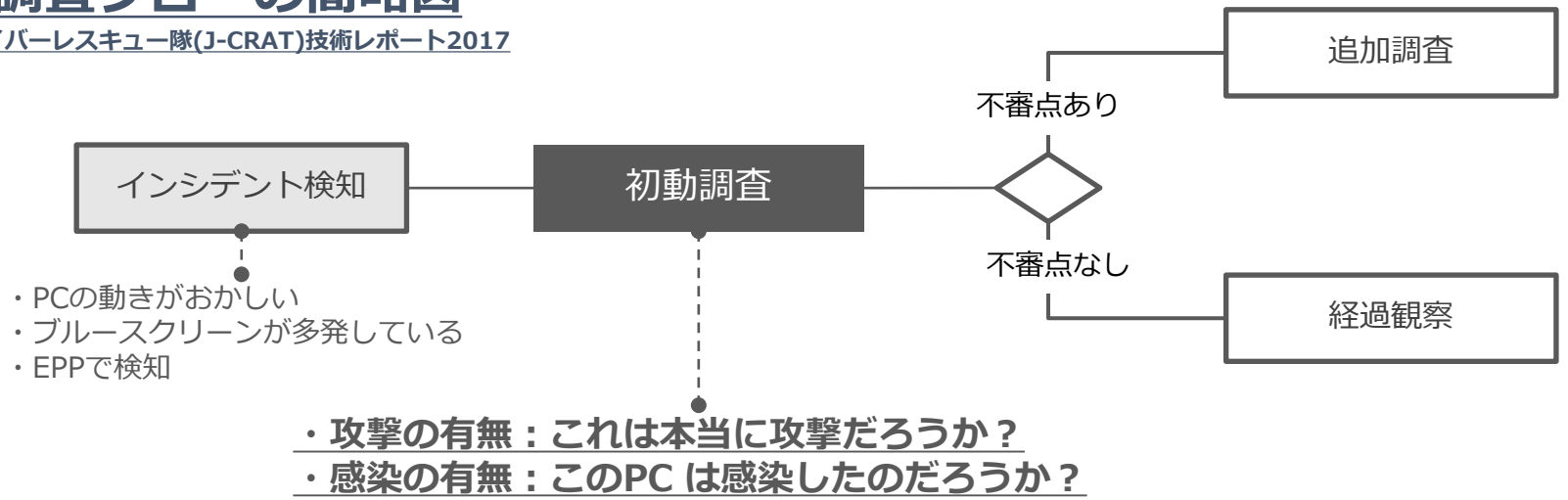
…etc

EISSの効果②

Secure Innovation
沖縄から日本、アジア、そして世界へ

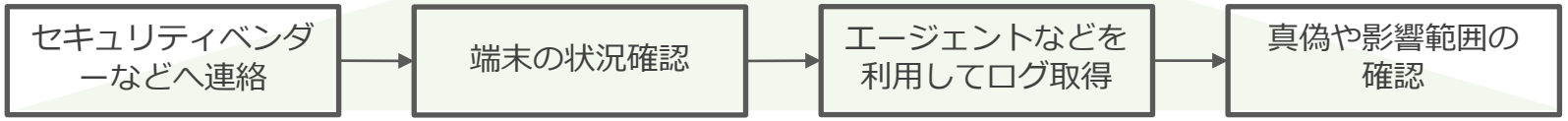
初動調査フローの簡略図

引用：サイバーレスキュー隊(J-CRAT)技術レポート2017



・攻撃の有無：これは本当に攻撃だろうか？
・感染の有無：このPC は感染したのだろうか？

初動調査には、時間も費用がかかり、その間に被害や費用が拡大します



EISSでは、インシデント発生時に有効なログデータを保管することで、
迅速な原因究明と対応を支援します。

EISSの効果③（その他機能）

Secure Innovation
沖縄から日本、アジア、そして世界へ

セキュリティ推奨構成のチェック

Microsoftが公開している「セキュリティ構成フレームワークの概要（通称SecCon）」について
【レベル１ エンタープライズ基本セキュリティ】情報の収集も行っています。
ご要望に応じて、ログの提供も可能となっております。

Office製品のセキュリティ設定チェック

EISSでは、Office製品における、マクロの有効化などのセキュリティ設定について、マクロが
無条件に有効になってセキュリティ性を低下させていないかなどをチェックすることが可能です。

Microsoft Defenderの一括管理

EISS管理画面から、Microsoft Defenderの各端末の詳細状況を一括で確認可能です。

- 稼働状況
- 動作監視・ファイルスキャン等の有効性
- Microsoft Defenderのエンジンやシグネチャのバージョン情報　等

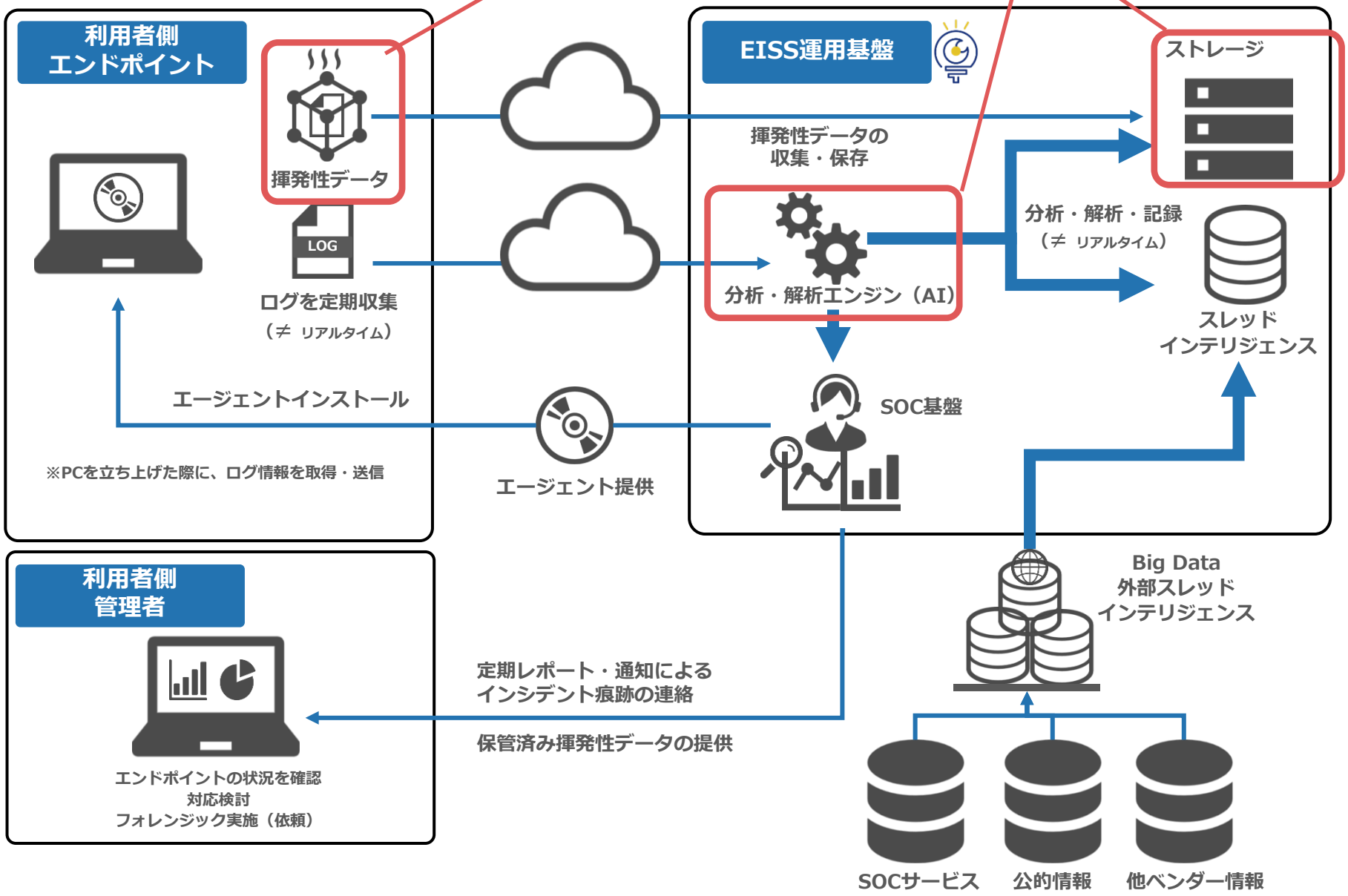
各端末におけるMicrosoft Defenderの稼働状況を個別で確認する手間が省け、テレワークによる在宅ワーク・支店利用等の各拠点で利用している状況においても一括でご確認いただけます。

製品の全体像

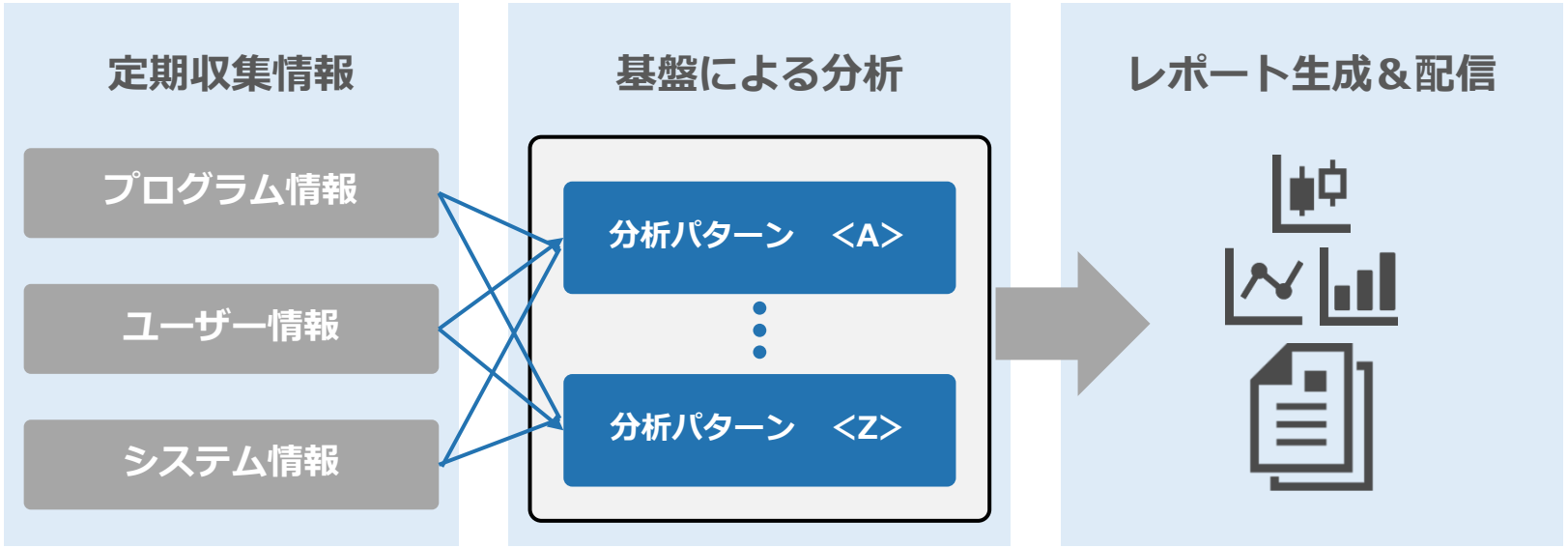
キャッシュデータやプロセス情報等の重要な情報源となるが**揮発性のあるデータ**

マルウェア自身ではなく、マルウェアによる挙動自体をデジタル**フォレンジックの観点**で分析

お客様に代わり、デジタルフォレンジックにも活用可能な**重要データを保存**。



処理内容



公的セキュリティ研究機関が危険な兆候だと示すものや、
MITRE ATT＆CKの一部の検知条件等を検知

※MITRE ATT＆CKとは？
MITRE（マイター）社が開発している攻撃者の攻撃手法、戦術を分析して作成されたセキュリティのフレームワーク・ナレッジベース

検知内容（一部）

- 不正なログイン、許可されていないネットワーク接続履歴などを検知
- 標的型攻撃で利用されるようなツールの利用履歴を検知
- 攻撃に利用されることがあるレジストリの変更を検知
- 管理画面から指定した不正ファイルを検知

収集ログ（一部）

- プロセスリスト
- ネットワーク接続リスト
- イベントログ情報
- レジストリ情報
- USB接続情報
- Wi－Fi情報
- 権限付与情報
- Windowsセキュリティ情報

運用管理の全体像(管理者)

Secure Innovation
沖縄から日本、アジア、そして世界へ

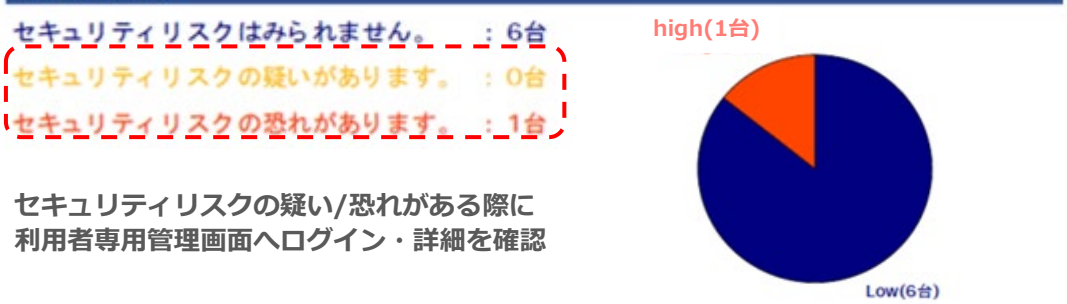
EISS アイズ

利用者側
管理者

①週次レポート送信

②レポート受信

＊メール添付レポート(一部)



セキュリティリスクの疑い/恐れがある際に
利用者専用管理画面へログイン・詳細を確認

③管理画面ログイン

＊アラート該当端末の対処方法確認
（サンプル）

アラート端末・内容を
確認し管理者にて対応
実施

④ヘルプデスク
(メール平日10-17時)

・検知内容等に不明点がある場合
→メール問い合わせ

（オプション）
・ヘルプデスク(TEL)
・不正アクセス原因分析
・フォレンジック対応依頼
→フォレンジック用
・ヒアリングシートの記載・提出

ご利用料金

Secure Innovation
沖縄から日本、アジア、そして世界へ

EISS アイズ

お客様 ご提供価格	年間　1,800円/端末 （税込 1,980円）［月あたり150円程度］
ログ保管期間	90日
ヘルプデスク内容	メール対応(平日10-17時)

※対応OS：Windows 8.1/ Windows 10/ Windows 11 64bit版が対象です。

【ご提案】
グループ企業や多店舗のPCセキュリティ管理
インシデント対応ツール「EISS(アイズ)」

グループ企業や複数店舗等のパソコンのセキュリティ管理や、
インシデント発生の備えにお困りではありませんか？
月額150円で万が一のインシデント発生時に有効なログデータを保管することで、
迅速な原因究明と対応を支援します。

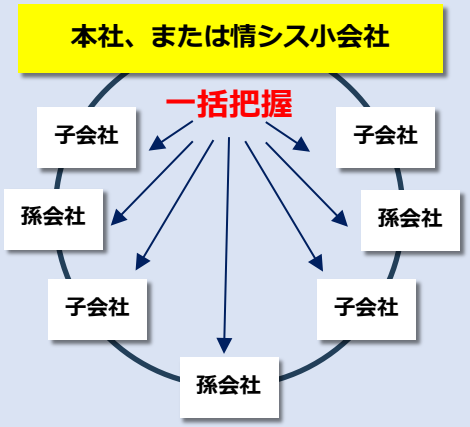
多くのグループ企業を抱える企業や、多店舗展開している企業の情報セキュリティ担当者向け
PCセキュリティ管理、及び重要なログデータの保管ツールとしてEISSを活用いただけます。

特徴：複数拠点のPCセキュリティを遠隔で一括把握することが可能で、親会社の情シス担当やCSIRT等が、遠隔管理、または重要なログデータの保管によりインシデント発生時の調査を支援することが可能です。

展開例：

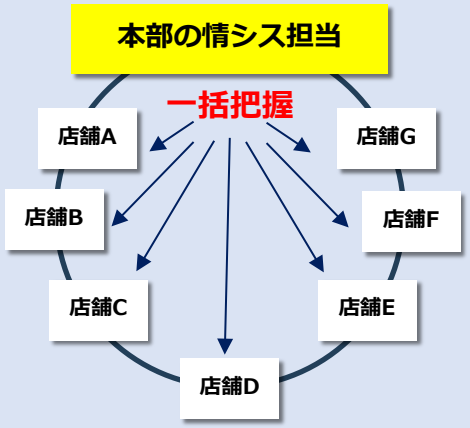
グループ企業向け展開

子会社や孫会社等を有するグループ企業様で、本社で管理、または情シス子会社に管理を委託している大手企業様向けに展開。



多店舗向け展開

複数店舗を運営している企業の情シス担当、CSIRT等におけるセキュリティ管理をサポート。



【ご提案】
中堅・中小企業の
セキュリティ対策のベストプラクティス

①導入済み製品

Microsoft Defender

Windows10搭載以降、**AV-Comparatives**での高い評価や、**AV-TEST.org**の評価結果でも性能の高い**「TOP PRODUCT」**の認定を受け、無償でも十分活用できる性能です。

中小企業が少ない負担で行えるベストなセキュリティ対策

＋

② EISS アイズ

月額150円/PC1台で、攻撃の痕跡を週1チェックして早期発見！

・マルウェアそのものではなく、マルウェアが悪意的に行う**アクションや挙動を検知**。

・実際にセキュリティ被害を受けてしまった際の対処（フォレンジック）に必要となるデータのスナップショットをお客様に代わり保存し、**感染後の対応を支援**。

・**ウィルス対策ソフトと併用**利用することで、**セキュリティ強度が高く**なります。

③ EASY クラウドバックアップ

格安で利用でき、自動で差分バックアップ負担もかからず利用可能！

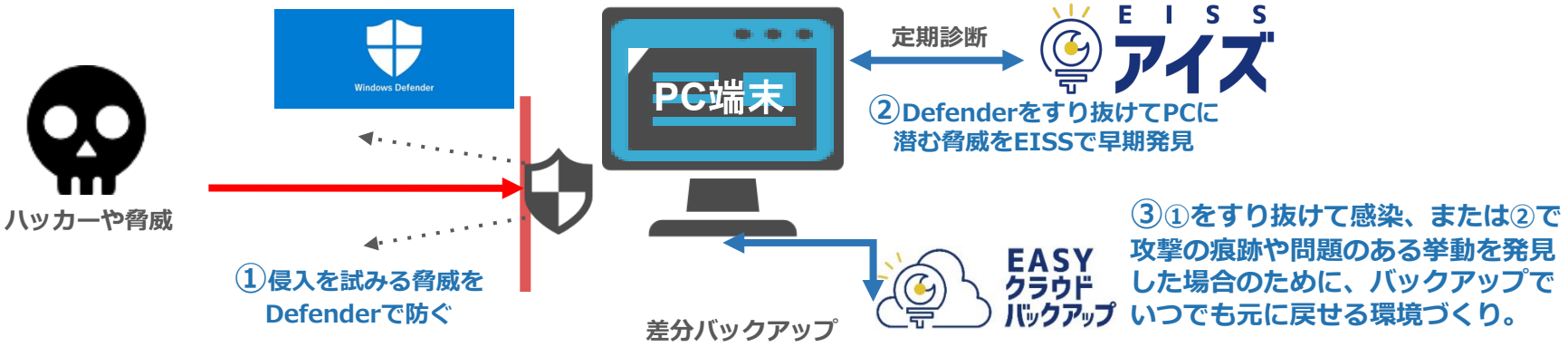
・クラウドに直接バックアップ保存し、**操作も感覚的**に操作しながら管理ができます。

・初回のフルバックアップ後は変更分のみをバックアップして帯域や容量を節約。

・**ランサムウェアによる攻撃も検知、遮断**し暗号化されてしまった部分も**バックアップから復旧**。

・コストも**初期費用無し**で、上限超過時の費用も含め、お手軽にご利用いただけます。

導入負担の少ない製品の組み合わせで、多層防御を実現して強度UP！



【参考】ASPIC アワード受賞 / 特許取得

Secure Innovation
沖縄から日本、アジア、そして世界へ

ASPIC IoT・AI・クラウドアワード受賞

当社のEISS（アイズ）が『第15回　ASPIC IoT・AI・クラウドアワード2021』において、支援業務系ASP・SaaS部門　「先進技術賞」を受賞いたしました。（受賞日：2021年11月17日）

ASPIC IoT・AI・クラウドアワードについて

本アワードは一般社団法人ASP・SaaS・AI・IoTクラウド産業協会（東京都品川区西五反田 会長：河合輝欣、以下ASPIC）が主催しており、IoT・ AI ・クラウドサービスが社会の情報基盤としてさらに発展・確立することを支援するために、ASPICが総務省などの後援により、日本国内で優秀かつ有益な IoT・AI ・クラウドサービスを審査・表彰し、サービス提供事業者、並びにユーザー企業の事業拡大を支援する目的のもと行われている取り組みです。

特 許 取 得

2023年8月8日、日本特許庁にて「EISS（アイズ）」の特許が正式に登録ました。

【特許概要】

特許番号	第7328635号
発明の名称	セキュリティインシデント検知装置、セキュリティインシデント検知システム及びセキュリティインシデント検知方法
登録日	令和5年8月8日
特許権者	株式会社セキュアイノベーション

導入までの流れ

Secure Innovation
沖縄から日本、アジア、そして世界へ

①お申込み

利用申込書をお送り致します。必要事項を記載のうえ、お申込みください。

②インストール＆管理コンソールログイン

弊社でお申込み内容を確認し、エージェントインストール情報と管理コンソール画面のログイン情報についてのダウンロードサイトをご案内します。
エージェントのインストール、管理コンソールへのログインをご確認ください。

③サービス提供開始

インストール＆管理コンソールログインからサービス提供開始となりますので、
管理コンソールの各種メニュー情報をご確認ください。

④週次分析レポート

翌指定曜日から週次レポートのメール送信を開始します。
分析結果の詳細は、管理画面へログインして確認いただけます。

導入事業者 事例

Secure Innovation
沖縄から日本、アジア、そして世界へ

EISS導入事業者　事例		
大手医療法人グループ	地方商工会・商工会議所	広告代理店
大手観光ホテルグループ	経営コンサル・市場調査サービス	人材派遣会社
信用組合(金融)	建築・工業関連会社	法律事務所
食品関連会社	研究開発会社 (バイオ・医療・環境)	保険代理店
農業生産法人団体	情報通信研究開発事業社	システム開発会社
学習教室	印刷会社	イベント制作会社
飲食店	不動産・賃貸サービス会社	その他多数実績あり

【参考】EISS利用に際しての留意点

Secure Innovation
沖縄から日本、アジア、そして世界へ

1. 対象端末
EISSサービスがご利用いただけるのはWindows OS（バージョン8.1および10）となります。
なお、Mac OSは提供対象外となります。

2. 契約単位
EISSサービスは端末数での契約となり、5端末～ご契約いただけます。（ 1台1,800円/年税抜き）
1端末を複数ユーザーで利用している場合も端末数は1となります。
※管理画面上はユーザー単位での分析結果の出力になります。

3. 契約期間
EISSサービスはお申込書・注文書を受領した月から年単位での契約となります。（自動更新）

4. 追加契約
本サービスは年間契約でご利用いただくサービスとなりますので、端末を追加される場合は、初期契約に対し残りの月数で利用期間を区切って追加契約とし、翌年、契約更新時に合わせて1年間の契約とさせていただきます。（自動更新）

5. ログ送信
EISSは端末起動時にログ収集し、定期的(1日1回）にサーバーへ送信します。

6. ログ分析
週次レポートにおいて契約（導入）端末数とログ収集台数が異なる場合は、管理画面より端末の最新ログ送信日を確認ください。以下の理由が考えられます。
①PC起動をしていない、②ネットに繋がっていない、③サービス不具合
ログ送信が行われない端末は当該週の分析をスキップします。

【参考】分析レポート通知メール(週次)

Secure Innovation
沖縄から日本、アジア、そして世界へ

Subject:[様]分析レポート(yyyy/mm/dd)
From:no-reply@secure-iv.com
Date:yyyy/mm/dd hh:mm
To:レポート送信先メールアドレス

お世話になっております。
株式会社セキュアイノベーションです。
EISSより分析レポートを送付いたします。
対象期間において、分析結果は下記の通りです。

--- 分析結果概要 ----------
セキュリティリスクはみられません。：6ユーザー
セキュリティリスクの疑いがあります。：0ユーザー
セキュリティリスクの恐れがあります。：1ユーザー

添付ファイル名
analysis_report_CIxxxx-0000xx_ yyyymmdd.pdf

詳細は、管理画面サイトをご参照ください。
https://www.eiss.jp/login

※このメールには返信できません。本件についてお問い合わせがある場合は、下記メールアドレスにご連絡ください。

お問い合わせ：
株式会社セキュアイノベーション
平日（祝祭日除く）10:00~17:00
eiss-support@secure-iv.com


レポート NO : CI -000050

分析対象期間

yyyy/mm/dd~ yyyy/mm/dd

契約内容

定期実行期間 ：週次
利用端末数 ：xx台
サービス開始終了期間 ：yyyy/mm/dd~ yyyy/mm/dd

分析端末情報

送信端末数 ：7台
分析端末数 ：7台

分析結果概要

セキュリティリスクはみられません。 ：6台
セキュリティリスクの疑いがあります。 ：0台
セキュリティリスクの恐れがあります。 ：1台

分析結果詳細

端末名	ユーザー名	端末分析NO	検知内容
		CI -000050-000001	セキュリティリスクはみられません。
		CI -000050-000002	セキュリティリスクはみられません。
		CI -000050-000003	セキュリティリスクの恐れがあります。
		CI -000050-000004	セキュリティリスクはみられません。
		CI -000050-000005	セキュリティリスクはみられません。
		CI -000050-000006	セキュリティリスクはみられません。
		CI -000050-000007	セキュリティリスクはみられません。

PDF

週次レポートをメールにて通知
アラート検知の際に管理画面サイトへログイン
※レポートは管理画面上でも出力可能

【参考】ユーザー管理画面1

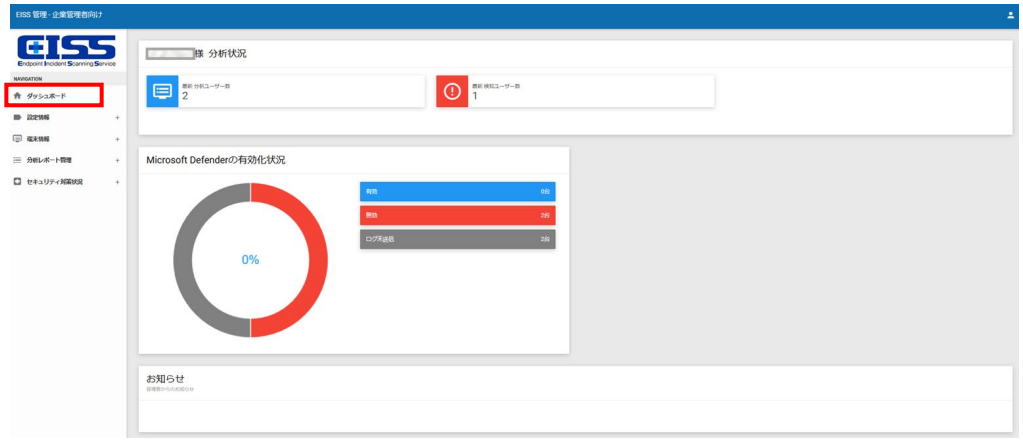
Secure Innovation
沖縄から日本、アジア、そして世界へ

ログインページ

運用開始時、EISS管理者向けにID/PWを発行

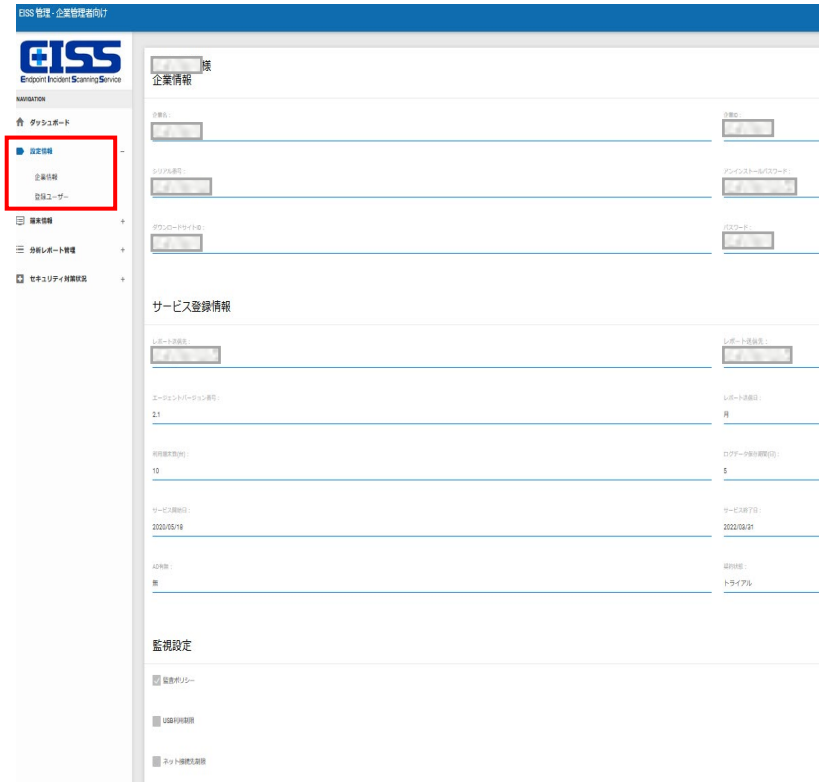
週次レポートメールでアラート検知が報告された場合は管理コンソールにて詳細を確認する

ダッシュボード



左カラムのメニュー一覧から詳細を確認可
最新分析対象PCの検知状況/Microsoft Defenderの有効化状況が確認できる

設定情報



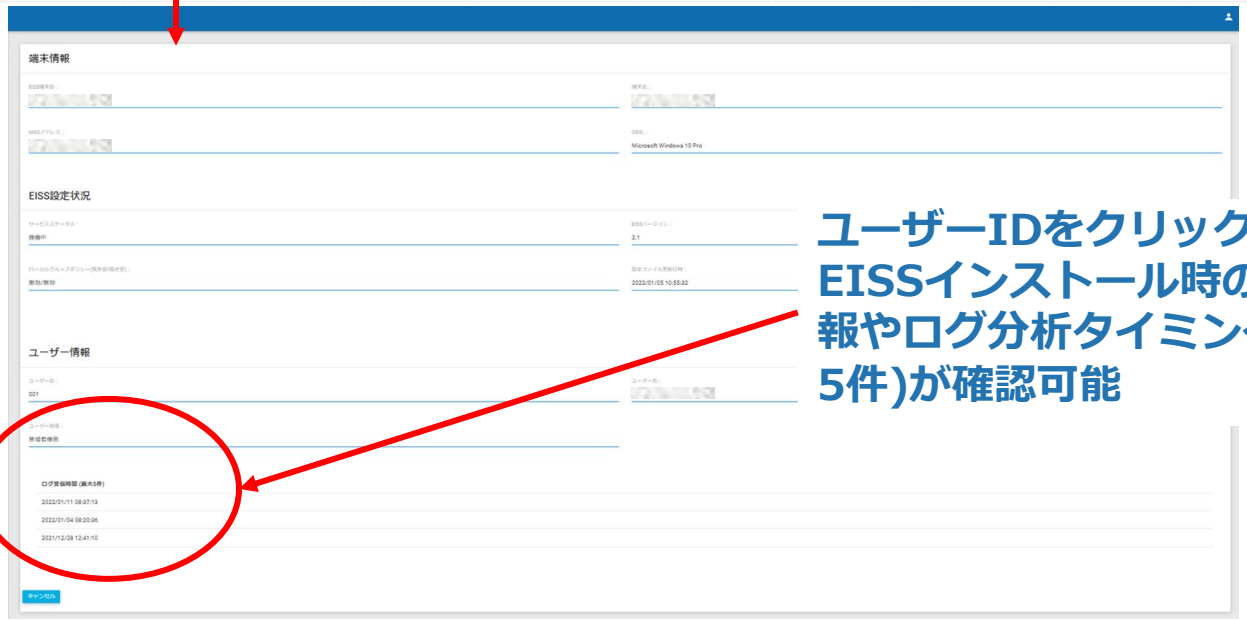
企業情報やサービス登録情報・監視設定の確認が可能
登録ユーザー一覧も閲覧できるので、アカウント追加希望があればEISSヘルプデスクへメール依頼ください

【参考】ユーザー管理画面2

Secure Innovation
沖縄から日本、アジア、そして世界へ

端末情報

EISSがインストールされている端末がユーザーごとに表示
項目ごとに並べ替え閲覧が可能

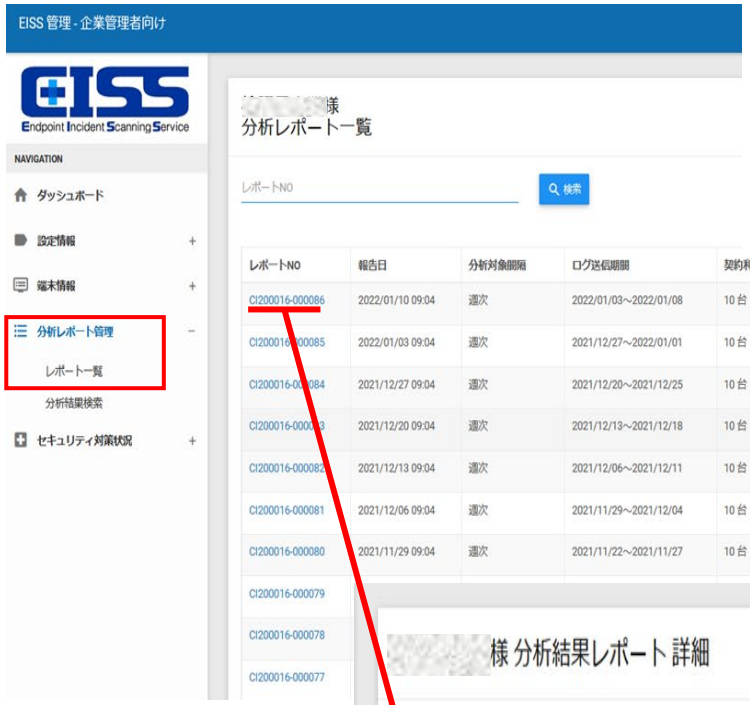


ユーザーIDをクリックすると
EISSインストール時の設定情報やログ分析タイミング(最大5件)が確認可能

【参考】ユーザー管理画面3

Secure Innovation
沖縄から日本、アジア、そして世界へ

分析レポート一覧



最新の分析レポートから降順に表示
「分析レポート」
分析レポートメールのPDFが出力
「レポートNO」
「分析結果レポート詳細ページ」が表示され、分析対象ユーザーごとの検知結果を確認

分析レポート詳細

分析ユーザー一覧=レポートメール3P以降端末一覧
検知されたユーザーは、最右項目「対処方法」よりアラートの対処方法をクリックし、詳細を確認する

【参考】ユーザー管理画面4

アラート対処方法表示

検知詳細は管理コンソールのみ確認可能
→検知内容/検知詳細等がアラートごとに表示されるので、検知結果に沿って管理者にて対処を進める

分析結果検索

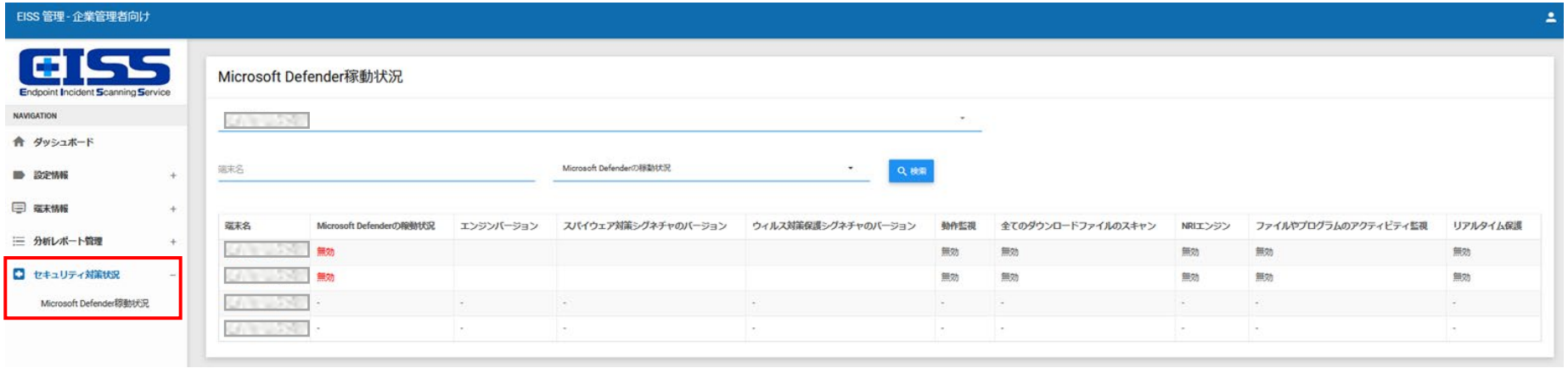
目的に応じた検索をすることが可能

- **レポートNO**
- **端末分析NO**
- **端末名**
- **報告日**

【参考】ユーザー管理画面5

Secure Innovation
沖縄から日本、アジア、そして世界へ

セキュリティ対策状況



EISSをインストールしている端末ごとにMicrosoft Defenderの詳細状況を一括で確認可能。

- 稼働状況
- 動作監視・ファイルスキャン等の有効性
- Microsoft Defenderのエンジンやシグネチャのバージョン情報　等

お問い合わせ

Secure Innovation
沖縄から日本、アジア、そして世界へ

資料請求やお見積依頼など、お気軽にお問い合わせください。
担当からすぐにご連絡いたします。

お問い合わせフォーム

https://www.secure-iv.co.jp/contact

pr@secure-iv.com

098-943-2718

受付時間 9:00～18:00（土日祝祭日を除く）

会社概要

Secure Innovation
沖縄から日本、アジア、そして世界へ

会社名	株式会社セキュアイノベーション
所在地	本社　　：沖縄県那覇市上之屋1丁目18番36号　沖縄映像センタービル3F 東京オフィス　：東京都渋谷区広尾1-7-20　TH広尾ビル 4F-N 名古屋オフィス：愛知県名古屋市中川区尾頭橋4丁目13番7号　503号室 大阪オフィス　：大阪府大阪市中央区南本町2-1-1　本町サザンビルThe DECK2F 221号室 福岡オフィス　：福岡県福岡市中央区渡辺通二丁目4番8号　福岡小学館ビル5F サービスオフィス福岡薬院18号室
設立	2015年10月21日
代表取締役社長	栗田 智明
事業内容	セキュリティ機器・ソフトウェアの運用監視 セキュリティコンサルティング、セキュリティ診断 セキュリティ人材の派遣 システム・サイトの構築および開発 地域活性化プロジェクトの企画実施
許可・認定等	JIS Q 27001:2014(ISO/IEC 27001:2013) ISMS認定取得(登録番号 IS127)［本社・東京オフィス取得］ JASA情報セキュリティサービス基準審査登録（セキュリティ脆弱性診断サービス) 労働派遣事業（許可番号：派47-300169） 脆弱性診断サービス（登録番号：019-0022-20） セキュリティ監視運用サービス（登録番号：019-0022-40）
会社ホームページ	https://www.secure-iv.co.jp/