信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

サイバー攻撃の最新動向と今必要なエンドポイントセキュリティ

セコムトラストシステムズ株式会社
ソリューションデザイン部
田中　則通
情報処理安全確保支援士（登録番号008070）

［セミナー資料］　2018/09/11

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

アジェンダ

■会社紹介

■サイバー攻撃の最新動向と
今必要な対策
（NGAV、EDR）

■セコムのサイバー攻撃対策
ソリューション

✓セキュアエンドポイント

田中 則通
セコムグループの情報セキュリティ対策を2003年から担当。
これまでの経験を活かし、お客様の情報セキュリティ対策を
支援しています。
情報処理安全確保支援士（登録番号008070）

セコムトラストシステムズ株式会社

セコムグループの情報・ネットワークシステムの構築・運用を担うと共に、ここで培った技術力・運用力・ノウハウで、
お客様の
『事業継続（BCP）』支援
を行なうために、情報セキュリティ事業と大規模災害対策事業を主力に、それぞれが緊密に連携し高品質なサービスを提供しています。

セコムグループ全体の
サイバーセキュリティを支えています。

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

STS の 事業領域

セキュアデータセンター

・24万㎡、国内最大クラス
・最高水準の物理＆情報セキュリティ

電子認証局

・国内唯一の国産電子認証局
・国の認定認証局

あんしん情報センター、SOC

・24時間365日対応
・BCPノウハウも有する
セキュアオペレーション

ヒト・モノ・システムを駆使し、
セコムならではのサービスを構築

セコムクラウド

・「安全・安心」を機能レンタル
・数多くの個人情報を厳格管理

物理セキュリティ

・情報資産の盗難・破壊・漏洩対策
・証拠・証跡（フォレンジック）の確保

サイバー消防団

情報漏洩緊急相談窓口
サンキューオーセコム
0120-39-0756

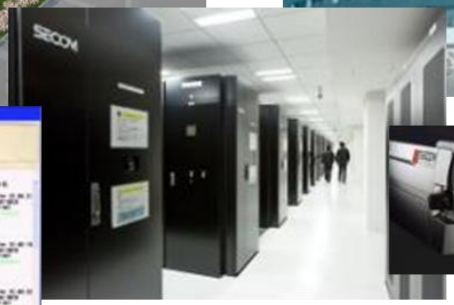
サイバー消防団

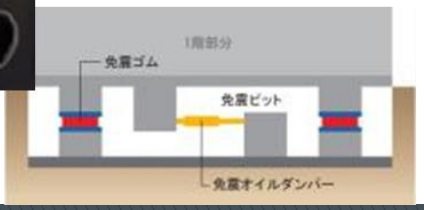
・70名超のセキュリティ専門家集団
・現地に駆けつけ緊急対処

★情報システムを「預かる」

セコムは国内最大クラスのデータセンター事業者

- 国内11ヶ所、総延床面積約24万㎡
- 官公庁、金融機関などの重要システムをお預かり
- セコムグループのサービスの中枢拠点としても機能





★サイバー事故を「対処する」

●サイバー“消防団” ～有事の際の緊急初動対応部隊～

- ウイルス感染、不正アクセス、情報漏洩などに関する緊急要請に対し、お客様先に駆けつけ、初動対応を迅速にサポート
- ご契約の無いお客様からの相談にも対応
- 団員数70名以上

情報漏洩緊急相談窓口
サンキューオーセコム
0120-39-0756
※情報漏洩やウイルスでお困りの場合はこちら

●サイバー“道場”
～サイバー攻撃に対する社会的な対処力向上への取組み～

- サイバー攻撃に対処する技術者養成を目的とした研修
- 本物のサイバー攻撃やウイルス感染が体験できる環境を使った演習
- 技術者不足という社会的課題に向き合う取組み

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

サイバー攻撃の最新動向と今必要な対策

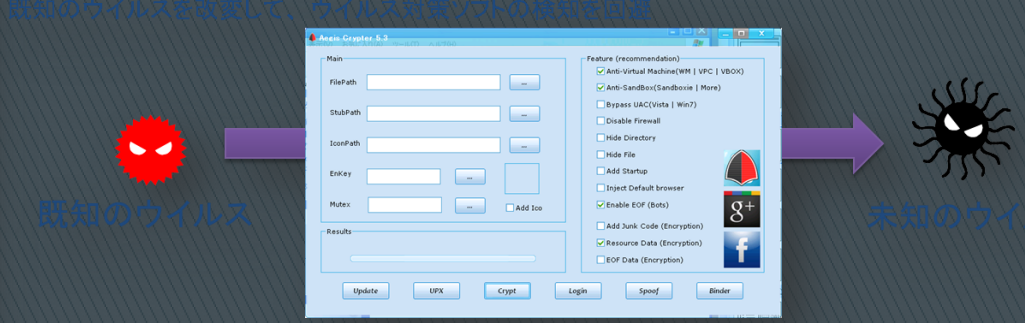
- 『サイバー消防団』での対処実例を元に。

脅威トレンド（未知のウイルス）

- 送付されるウイルスの約2割はウイルス対策ソフトで検知できない
- 新たなウイルスに対してウイルスパターンの作成が追い付かない
- 検出不可能なウイルスを容易に作成可能
- メール添付ファイルによる侵入経路の増大

検出不可能なウイルスの作成イメージ

改変ソフト（パッカー）は誰でも入手可能



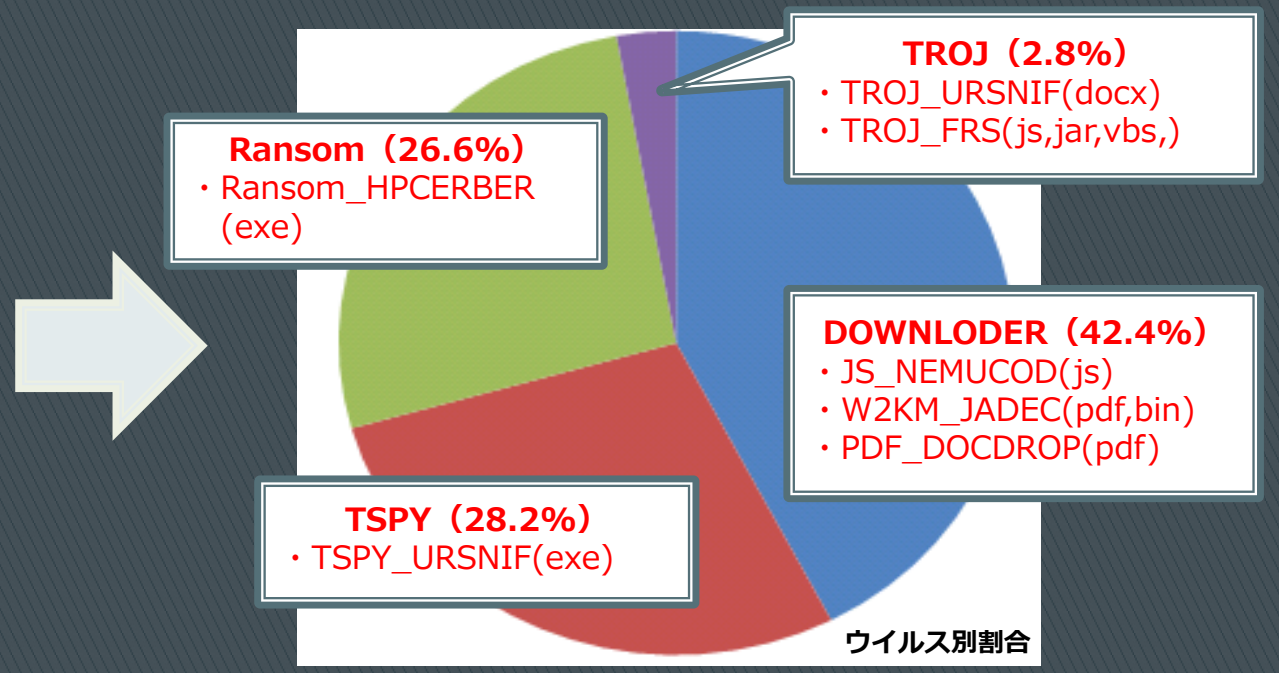
パッカーによるウイルス改変

攻撃事例）

メールに添付されたウイルス

	ウイルス件数
4月	3,270件
5月	814件
6月	1,170件
合計	5,254件

集計期間： 2017年04月～2017年06月



侵入時は **未知のウイルス**

64件

- 全てがランサムウェア,オンライン銀行詐欺ツールに関連するウイルス
- 2重拡張子（.doc.exeや.pdf.exe）で偽装
- マクロウイルスを含んだOfficeファイルが添付

［提案資料］

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

動画

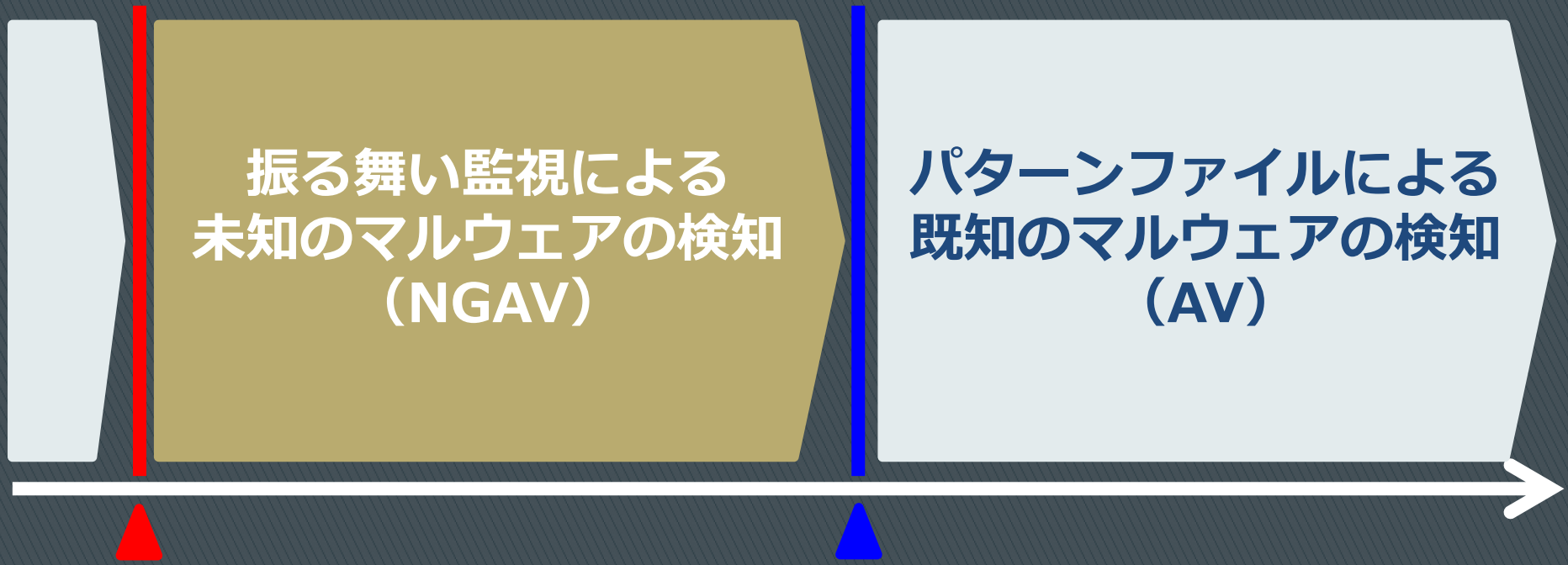
信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

NGAV と EDR
～ 未知のマルウェアへの備え ～
（検知・防御・対応）

- **NGAV**（**N**ext **G**eneration **A**nti **V**irus）
  EDR（**E**ndpoint **D**etection and **R**esponse）

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

NGAV導入の効果



※ 新しいマルウェアや脆弱性への攻撃は絶えることが無いため、
NGAVは必須の対策となっています。

事後対応の必要性

ウイルス/マルウェアの被害に遭われたお客様から以下のご要望を頂くことが多いですが、既存の対策方法ではご期待に沿えないことが多数を占めます。

■ 事態を終息させたい

- 未知のウイルスの存在確認
- ウイルスの駆除
- 再発防止
- 現状復帰

社内でウイルスが発生するたびに実施します

■ どんなことが行われたか特定したい

- 証拠の保全
- 記録の確認（ログがある場合）
- ウイルスの挙動確認（専用ソフト導入）
- 影響の分析（調査出来た場合）

専用のソフトウェアが導入されていないとそもそも特定ができません

EDR導入の効果

ユーザレベルまでのログだけでは「マルウェアに何をされていたか」を特定できません。

- ✓ お客様や株主含めたステークホルダーへの説明責任について、ログがないと、その責任を果たすことが難しくなってしまい、漏洩等の事故時にさらなる批判に晒されてしまう可能性があります。
- ✓ しかしながら一般的なウイルス対策製品ではログ取得は行っておりません。

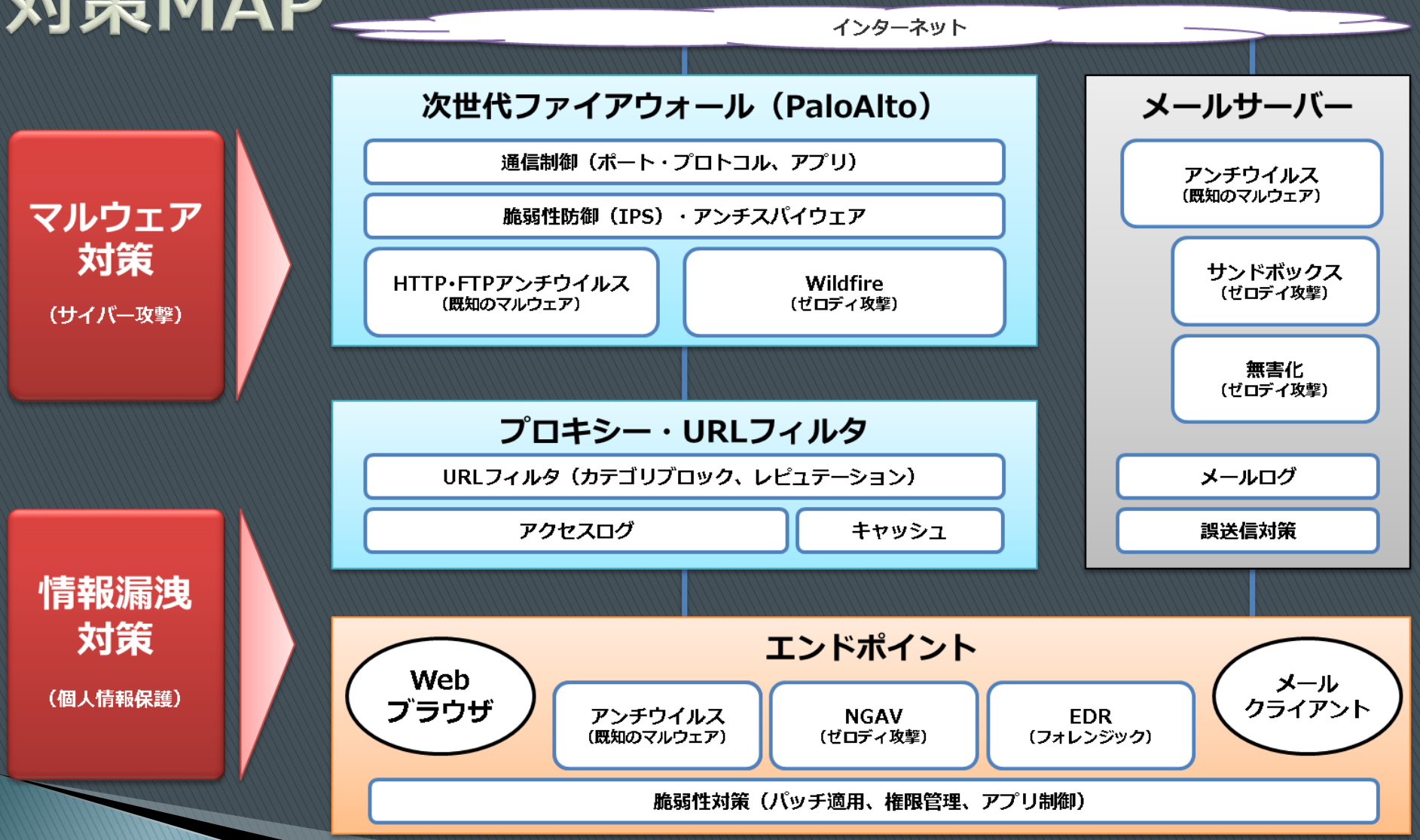
⇒ ユーザレベルのみならず、**カーネルレベルまでログを取得**。（一般的な資産管理ツールでもカーネルレベルまでは取得しません）

⇒ カーネルレベルのログでは、そのアプリケーションにどんな引数を与えて実行していたかまで特定できるため、**攻撃者の行った内容が可視化**。

※ログの例

ユーザレベル	XX時XX分XX秒	powershell.exe 起動
カーネルレベル	XX時XX分XX秒	powershell.exe cmd="-ExecutionPolicy～"

安全なインターネット利用のための対策MAP



信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

セコムの
サイバー攻撃対策ソリューション

- 未知にウイルスにも対応する
  エンドポイント・セキュリティサービス

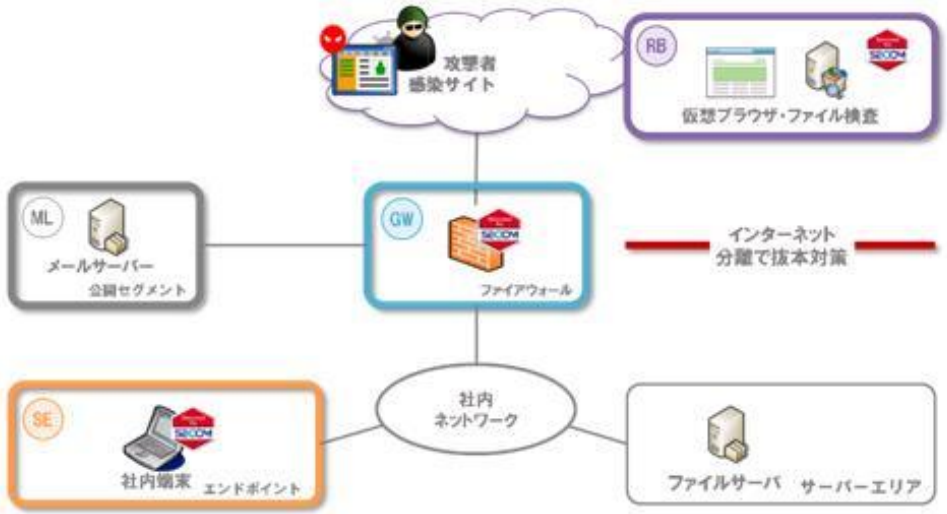
事業継続を支援するソリューション

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

巧妙化するサイバー攻撃にセコムサイバーコントロールセンター（SC3）が24時間365日の監視運用体制で対応！

セコムがおすすめする サイバー攻撃対策

巧妙化するサイバー攻撃に対して抜本対策であるインターネット分離と、
高度なセキュリティサービスで対応します。
（SC3が24時間365日監視）



▶ 事前の備えから復旧／対策まで、お客様の事業継続（BCP）をトータルに支援！

事前の備え	監視／検知	インシデント対応（EDR）	復旧／対策
RB	仮想ブラウザ、ファイル検査	インターネット分離（抜本対策）	
GW	通信制御、不審な通信の検知・遮断		
SE		マルウェア検知・隔離、論理抜線（初動対処）、ログ収集保管	再発防止策の立案・実施
ML	ウイルスフィルタ、メール無害化		
PS		駆けつけ調査・対処、ログ分析（フォレンジック）	

セキュリティSI
セキュリティ対策としてアクセス権限管理、端末のOSやアプリケーションの脆弱性管理が必要です。
・AD、WSUS環境構築
・利用アプリケーション資産の管理

ご安心ください！

SECOM Cyber Control Center（SC3）

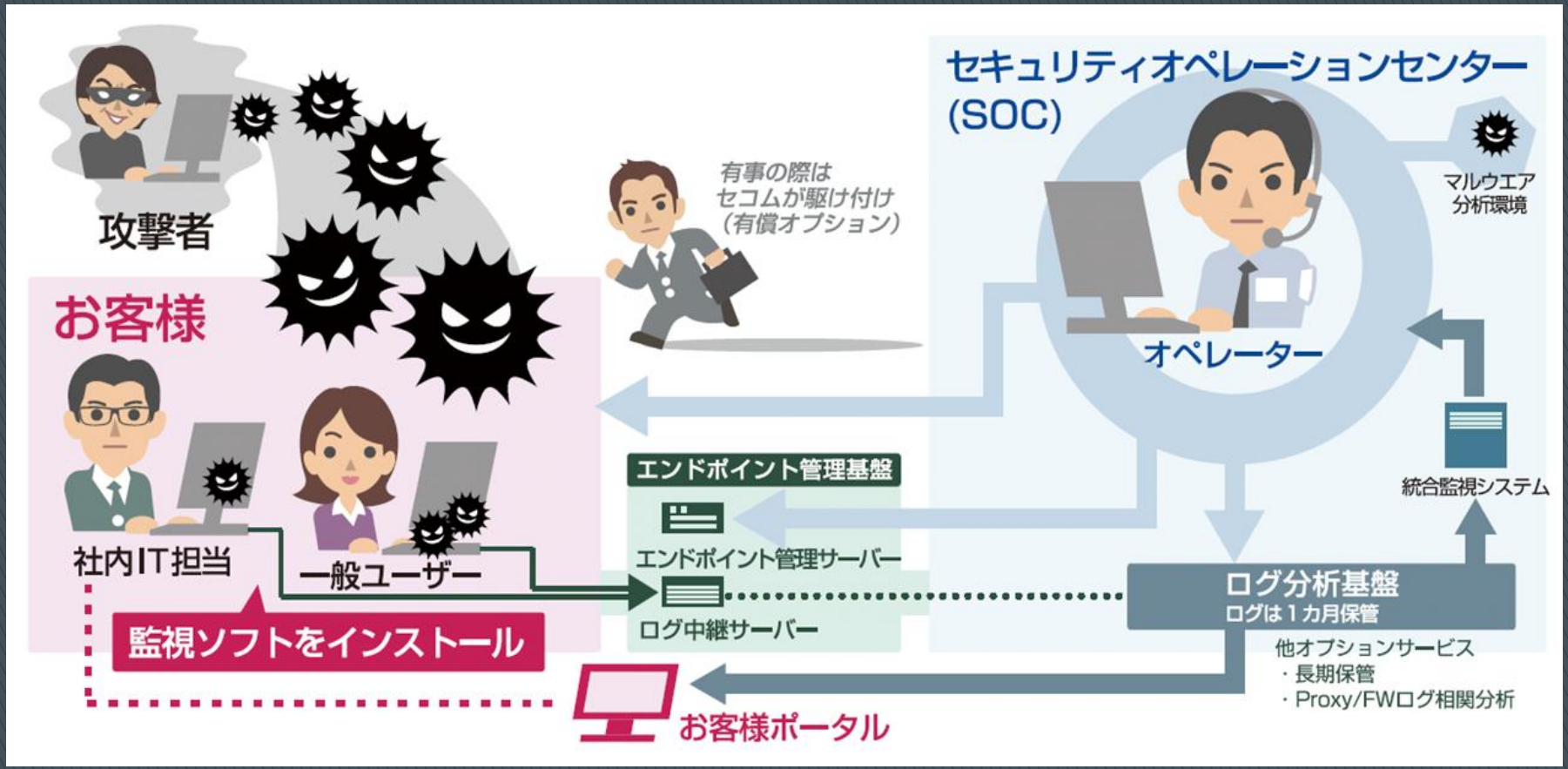
24時間365日の監視体制
有事の際の初動対応

SDC
DDoS攻撃対策などのインターネットのセキュリティサービスと安心のセコムクラウドサービスを提供する、安全・安心のサービス拠点！
セキュアデータセンター（東京／大阪）

ゲートウェイセキュリティ	インターネット分離	メールセキュリティ	エンドポイントセキュリティ	プロフェッショナルサポート
GW 次世代ファイアウォールとセコムの監視運用を組み合わせた安心のゲートウェイ対策。	RB セコムの仮想ブラウザで安全にインターネット閲覧。持込ファイルは事前検査するので安心です。	ML ウイルスチェックとスパムチェック、メールの無害化も可能なセコムのメールセキュリティ対策	SE ウイルスパターンでは検知されないマルウェアも検知・遮断。24時間365日の監視と対処を実施。	PS ウイルス感染や不正アクセスなどの緊急事態にITセキュリティのプロが駆けつけ対処します。

サイバー攻撃対策SE セキュアエンドポイント

SE サービスイメージ



サイバー攻撃対策SE セキュアエンドポイント

SE サービス導入の効果

Point 1 検知／防御

標的型攻撃・未知の脅威から防御

- ☑ パターンマッチング型の対策ソフトでは防御できない、未知のマルウェアを振る舞い防御エンジンで検知・ブロックします。
- ☑ マルウェア感染を検知した端末はセコムがリモートでネットワークから抜線、お客様の社内環境の安全を確保します。

Point 2 検体の調査

不審なファイルをセコムが調査

- ☑ リスクの高い挙動をしたファイルをセコムが調査。マルウェア情報や独自のサンドボックス解析を踏まえた調査結果をご連絡します。
- ☑ 安全と確認されたファイルを検知しないようにする除外設定はセコムが実施、お客様の運用負荷を軽減します。

Point 3 動作ログ保管

マルウェア動作ログをDCに保管

- ☑ マルウェアが、「いつから」「どの端末から」「何をきっかけに」侵入したか調査可能なログを取得、セコムのセンターに保管します。
- ☑ お客様のインシデント発生時にはセコムの「プロフェッショナルサポート（別途費用）」と合わせて、迅速・的確な対応が可能です。

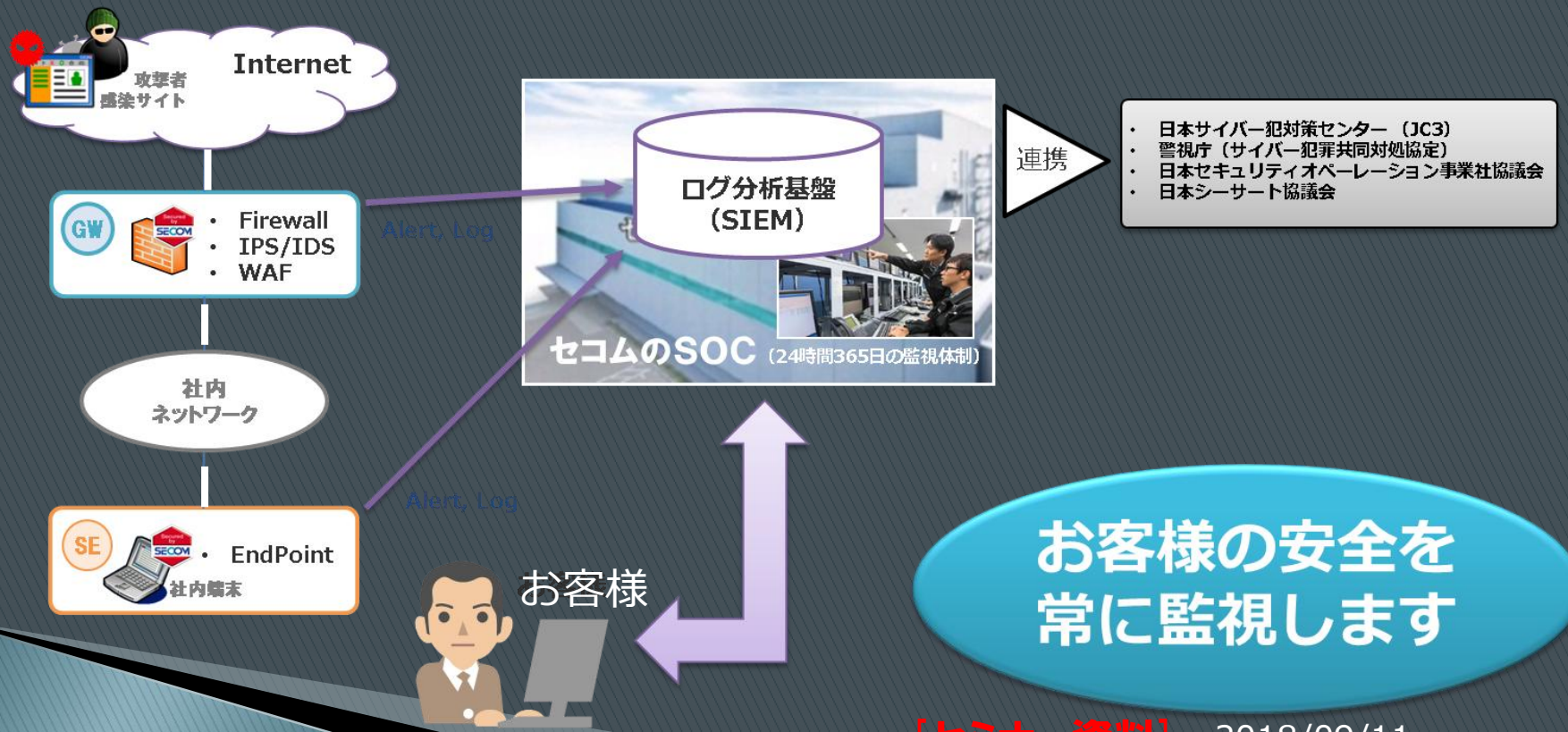
もちろん!

24時間365日の監視・運用はセコムにお任せ！

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

サイバー攻撃対策SE セキュアエンドポイント

SE 24時間365日の監視体制・初動



サイバー攻撃対策SE セキュアエンドポイント

SE サービス導入までの流れ

お申込 → **インストール** → **監視開始**

① お客様設定情報シートの記入
② センター側の設定作業

③ エージェントソフトのインストール
④ ノンブロックモードでの検知ログ収集
⑤ 検知ログの分類（除外リストの作成）
⑥ 除外設定

導入時の
チューニング
も支援します

⑦ ブロックモード
⑧ 監視開始

クラウドサービスなので簡単導入

※ 比較ポイント

セコムのセキュアエンドポイントサービス

製品マネージドサービス

マルウェア対策製品

》NGAV
- マルウェア対策（ランサム、標的型）

》EDR
- フォレンジックログ
- 検知時の操作

製品マネジメント（導入支援）

設定代行

24時間365日監視

インシデント対応（セコムのSOC）

プロフェッショナルサポート
※別途有償

サービスとして、お客様の事業継続をトータルに支援

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

ご清聴ありがとうございました。