LANSCOPE
Endpoint Manager

LANSCOPE
Cyber Protection

# 未知の脅威に対抗する エンドポイント セキュリティ対策

## 会社概要

| | |
|---|---|
| 会社名 | エムオーテックス株式会社 |
| 代表取締役社長 | 徳毛 博幸 |
| 設立 | 1990年7月 |
| 従業員数 | 472名（2025年4月現在） |
| 株主 | 京セラコミュニケーションシステム株式会社<br>（2012年から資本参加） |
| 事業内容 | 自社製品の開発・販売、サイバーセキュリティのコンサルティング・ソリューション導入・運用監視サービス |

## 拠点

| | |
|---|---|
| 本社 | 大阪市淀川区西中島5-12-12<br>エムオーテックス新大阪ビル |
| 東京本部 | 東京都港区三田3-5-19<br>住友不動産東京三田ガーデンタワー 22階 |
| 名古屋支店 | 名古屋市中区錦1-11-11<br>名古屋インターシティ 3階 |
| 九州営業所 | 福岡市博多区博多駅前1-15-20<br>NMF博多駅前ビル 2階 |
| 長崎Innovation Lab | 長崎県長崎市出島町1-41<br>クレインハーバー長崎ビル 3階 |

# 未知・亜種のマルウェアもマシンラーニングで99%検知！次世代のアンチウイルス

## 次世代 AI アンチウイルス

Aurora Protect

AI を活用したマシンラーニングによる予測検知が可能で、未知・亜種のマルウェアも 99%※ の高検知が実現。別途オプションの Focus（EDR） で感染原因の調査も可能

- AI による高精度な予測検知
- シグネチャレスで日々のアップデート不要
- 誤検知が少なく低負荷

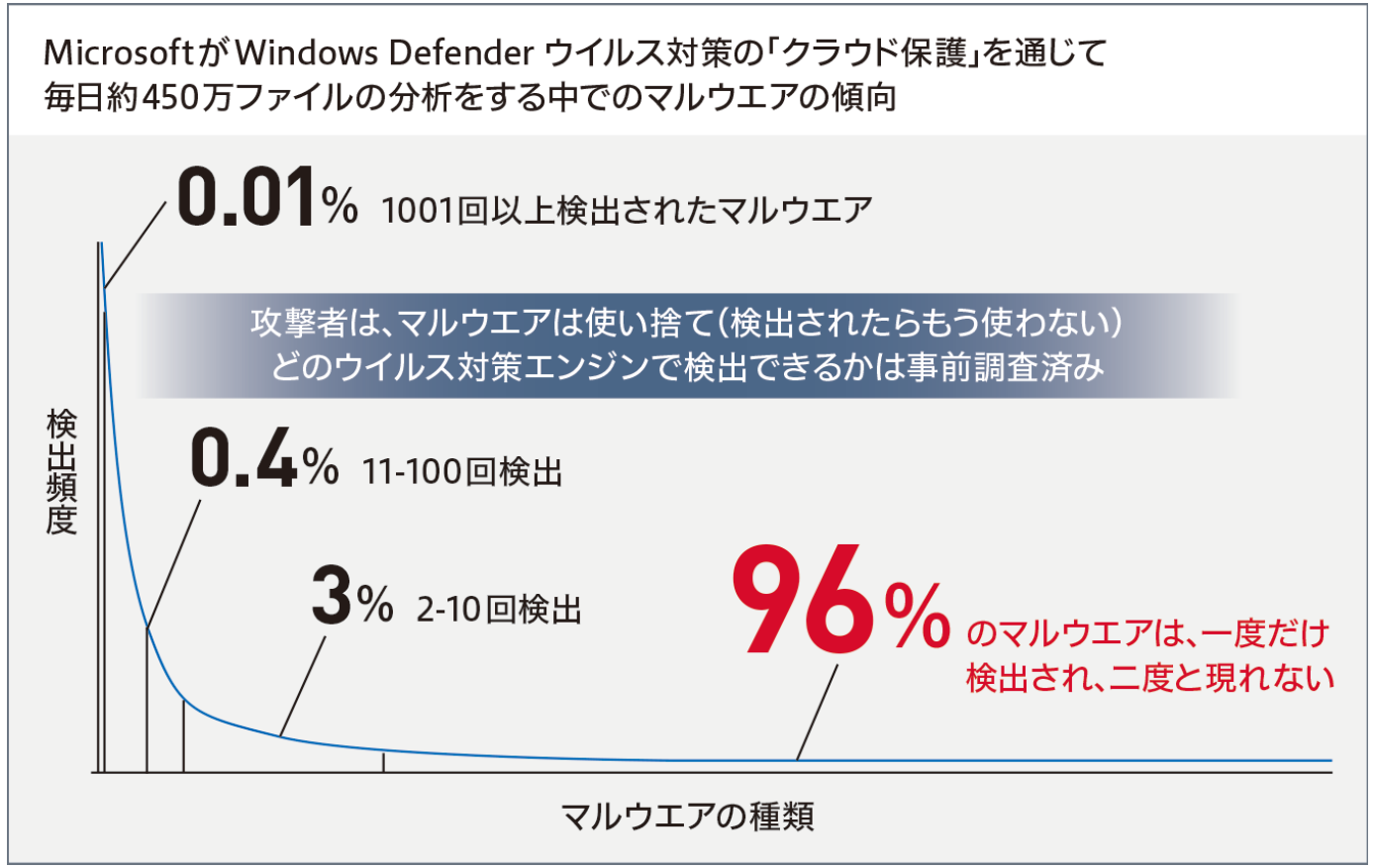
※2024年5月 Tolly 社のテスト結果より

# 最新の脅威動向

サイバー攻撃の傾向と手法・実例

# マルウェアの数が爆発的に増加し ”使い捨て” の未知のマルウェアが急増傾向が顕著に

昨今はマルウェアの量も増加、寿命が短く1企業1マルウェアが当たり前に＝未知のマルウェアが急増しています




※デジタルイノベーション2019「ビルトインセキュリティは常に変化する脅威への最適解」日本マイクロソフト株式会社

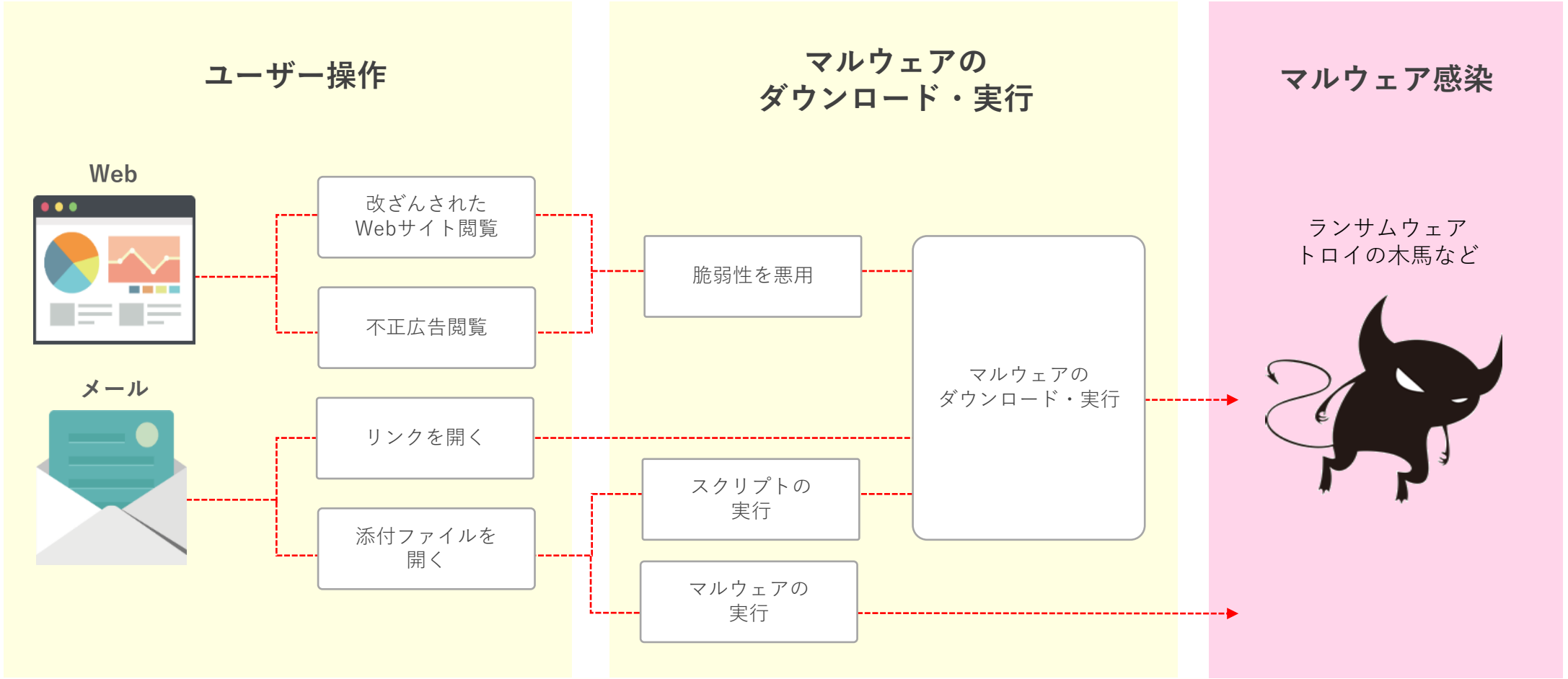
## 二度と検出されないマルウェア

# 96%

- 1001回以上検出された 0.01%
- 11～100回以上検出された 0.4%
- 2～10回以上検出された 3%

# メールやWeb経由で人の脆弱性を攻撃！ユーザー操作からマルウェア実行

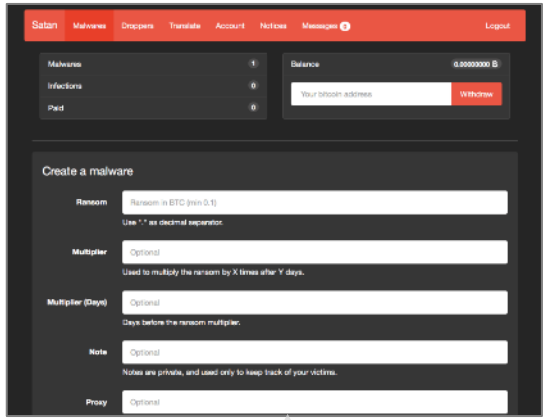
Webやメールなどの「人の操作」をトリガーとして、マルウェア・ランサムウェアは感染します



# RaaSサイトから無料で入手できる成功報酬型ビジネス化で誰でも手軽ランサムウェア攻撃

闇サイトには無料でマルウェアを提供するサイトが多数存在。成功報酬を山分けすることで稼げる手法です

## ランサムウェア作成




闇サイトのRaaSサイトを活用。必要事項を入力するだけで、簡単にランサムウェアを作成！

## 攻撃

作ったランサムウェアでPCを攻撃。データを暗号化し、身代金を請求

## 報酬を山分け

【RaaS提供者】　【攻撃者】

振り込まれた身代金をRaasサイト提供者と攻撃者で山分け

# 「ランサム攻撃による被害」が5年連続で1位に

## サイバー攻撃被害が増加傾向にあり、セキュリティ対策の強化が必須

| 順位 | 組織 | 昨年順位 |
|---|---|---|
| 1位 | ランサム攻撃による被害 | 1位 |
| 2位 | サプライチェーンや委託先を狙った攻撃 | 2位 |
| 3位 | システムの脆弱性を狙った攻撃 | 5位,7位 |
| 4位 | 内部不正による情報漏えい等 | 3位 |
| 5位 | 機密情報等を狙った標的型攻撃 | 4位 |
| 6位 | リモートワーク等の環境や仕組みを狙った攻撃 | 9位 |
| 7位 | 地政学的リスクに起因するサイバー攻撃 | NEW |
| 8位 | 分散型サービス妨害攻撃（DDoS攻撃） | NEW |
| 9位 | ビジネスメール詐欺 | 8位 |
| 10位 | 不注意による情報漏えい等 | 6位 |

※引用：IPA「情報セキュリティ10大脅威2025」

### 今期のポイント

**1位：「ランサムウェアによる被害」**

2024年もランサムウェア被害は多く確認されました。ランサムウェア感染によってシステムに障害が発生し、一時的に業務が停止した企業もありました。また、ファイルを暗号化せずに窃取だけ行い、身代金を要求するといった手口（ノーウェアランサム）も確認されています。

**2位：「サプライチェーンや委託先を狙った攻撃」**

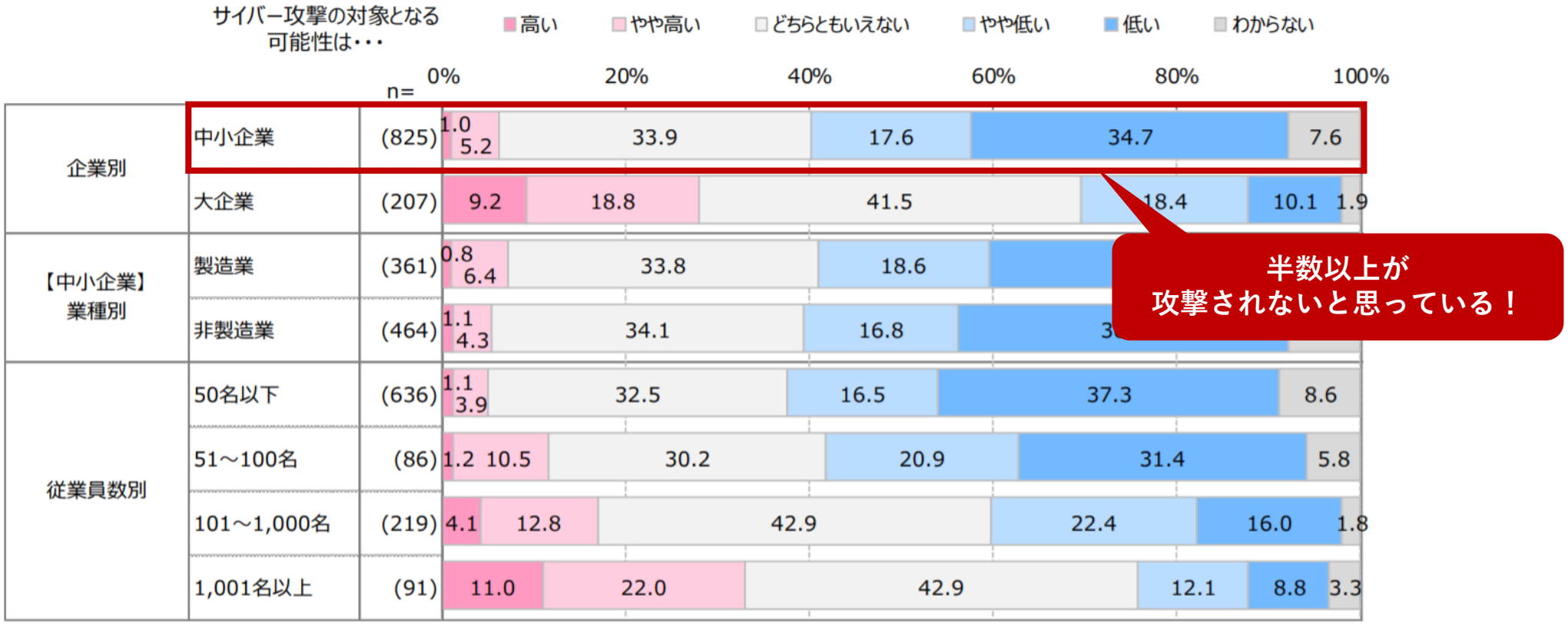
業務委託先の企業が攻撃されることで、委託元の企業に感染が広がってしまったというケースが確認されています。その結果、委託元企業の業務が一時停止するなどの被害が発生しています。

**3位：「システムの脆弱性を狙った攻撃」**

昨年5位の「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」を7位の「脆弱性対策情報の公開に伴う悪用増加」に統合したため順位が上昇。特に、VPN の脆弱性を悪用して社内環境に侵入するといった被害が多く確認されています。

# 自社が狙われる心配はないと思う中小企業経営者が未だ多く、その盲点を突き攻撃される

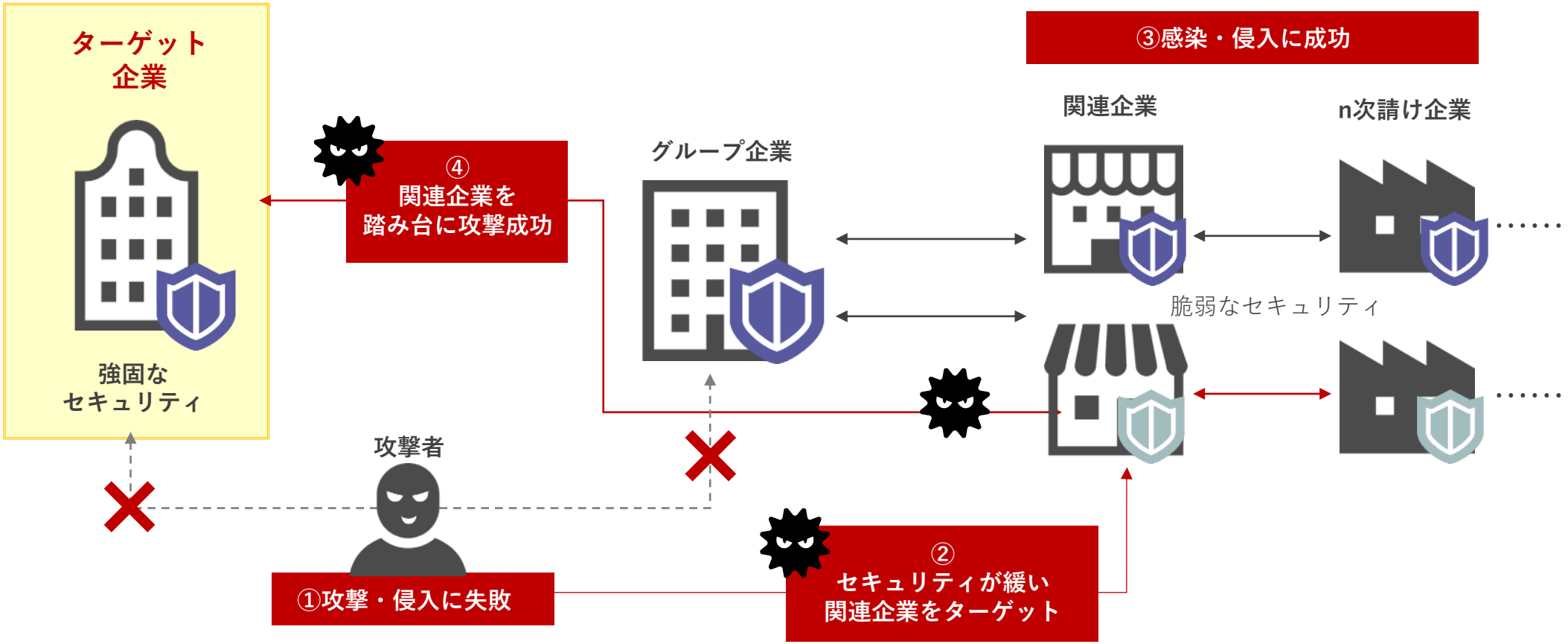
＜　**貴社がサイバー攻撃の対象となる可能性は、どの程度あると考えていますか**　＞




※出典：「中小企業の経営者のサイバーリスク意識調査2019」一般社団法人 日本損害保険協会　https://www.sonpo.or.jp/

# 急増するサプライチェーン攻撃！自社の対策だけでは絶対に防げないのが急増する要因

セキュリティ強度が弱い取引先（サプライチェーン）を次々と踏み台にし、最終的なターゲット企業を攻撃する手法です



# 【参考情報】流行したマルウェアEmotet（bot・ランサムウェア）

Emotetの特徴と対策方法

**＜2014年頃の初期Emotet＞**

オンラインバンク狙いのトロイの木馬

オンラインバンキングの情報を窃取する

## ＜最新Emotetの基本機能＞

### ①電子メールメッセージを大量に収集

実際のメールへの返信を装ったばらまきメールで

巧妙にEmotet本体のダウンロードを誘導

### ②自己増殖能力を持つ

ネットワーク内の他のデバイスへ自ら感染を拡大し、

大規模な組織の内部での大きな被害を引き起こす

### ③他のマルウェアに感染させる機能がメイン

ランサムウェアなどのさらに強力なマルウェアを

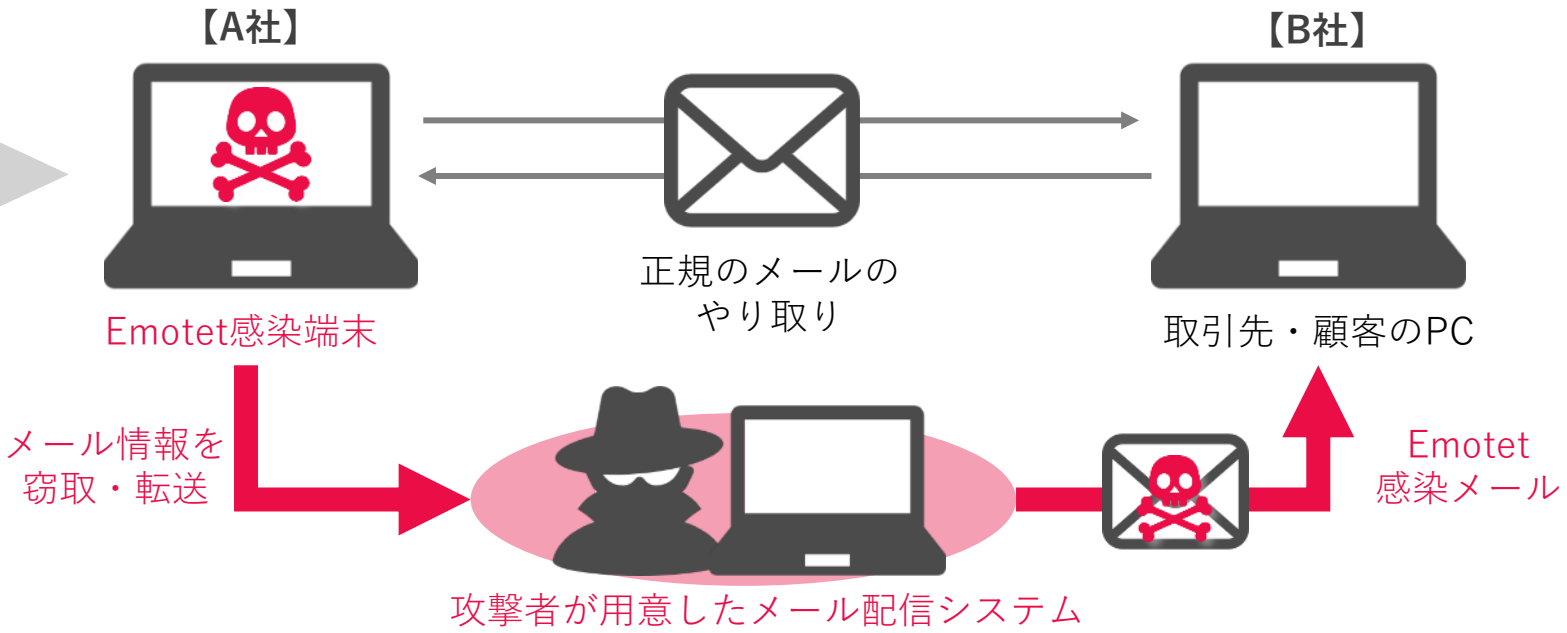
呼び寄せるプラットフォームとして動作し、被害を拡大

最終的にはランサムウェアなどを用いて自らの活動の

痕跡を消し去る

# 窃取したメール情報を悪用し、取引先や顧客に対してEmotetのばらまきメールを送信

【窃取される恐れのある情報】
- 端末やブラウザに保存されたパスワード等の認証情報
- メールアカウントとパスワード
- メール本文とアドレス帳の情報



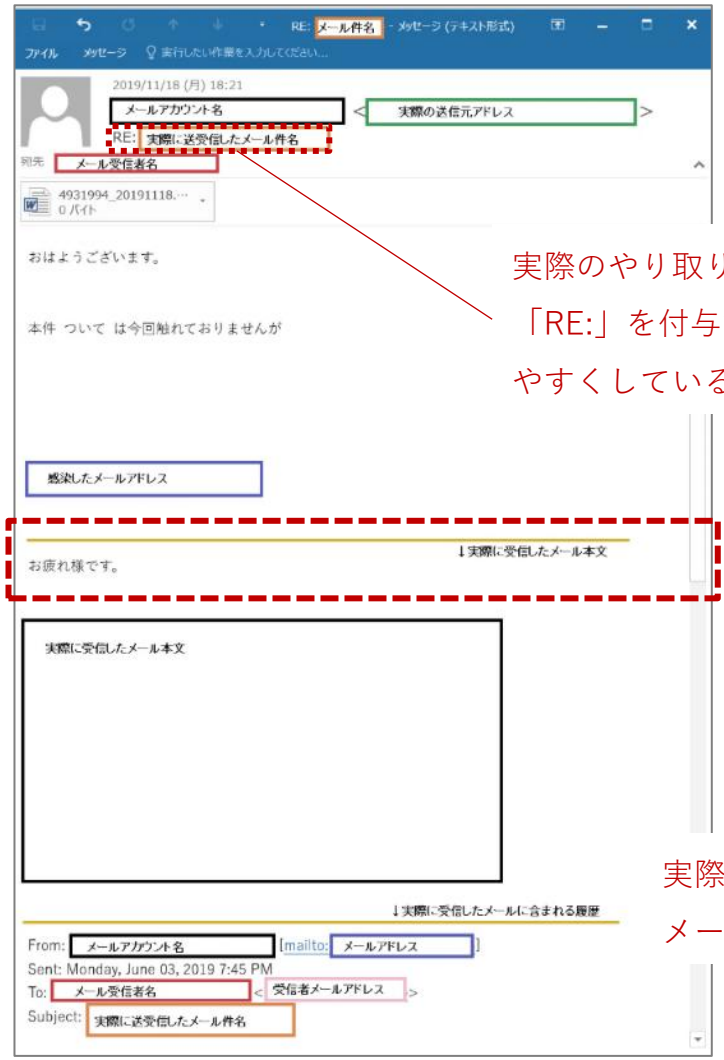

**Emotetの被害が拡大**

**ブランドイメージの低下**

**損害賠償・取引停止**

# Emotet感染メールと添付ファイルの例

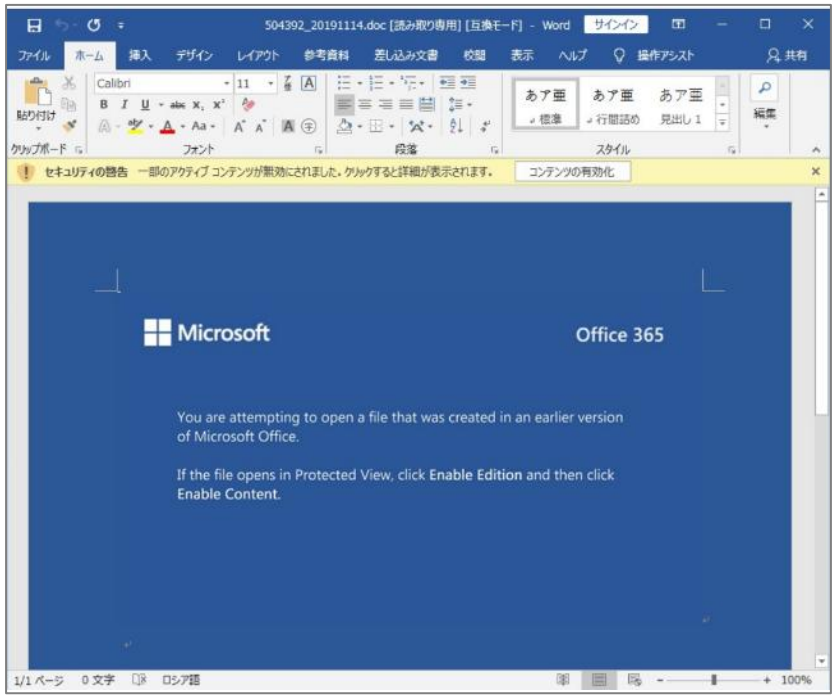
▼ Emotetの感染メールのイメージ




実際のやり取りのメール件名に「RE:」を付与することでメールを開きやすくしている

実際のやり取りのメール本文を引用

▼ Emotetの感染メールに添付されるファイルのイメージ



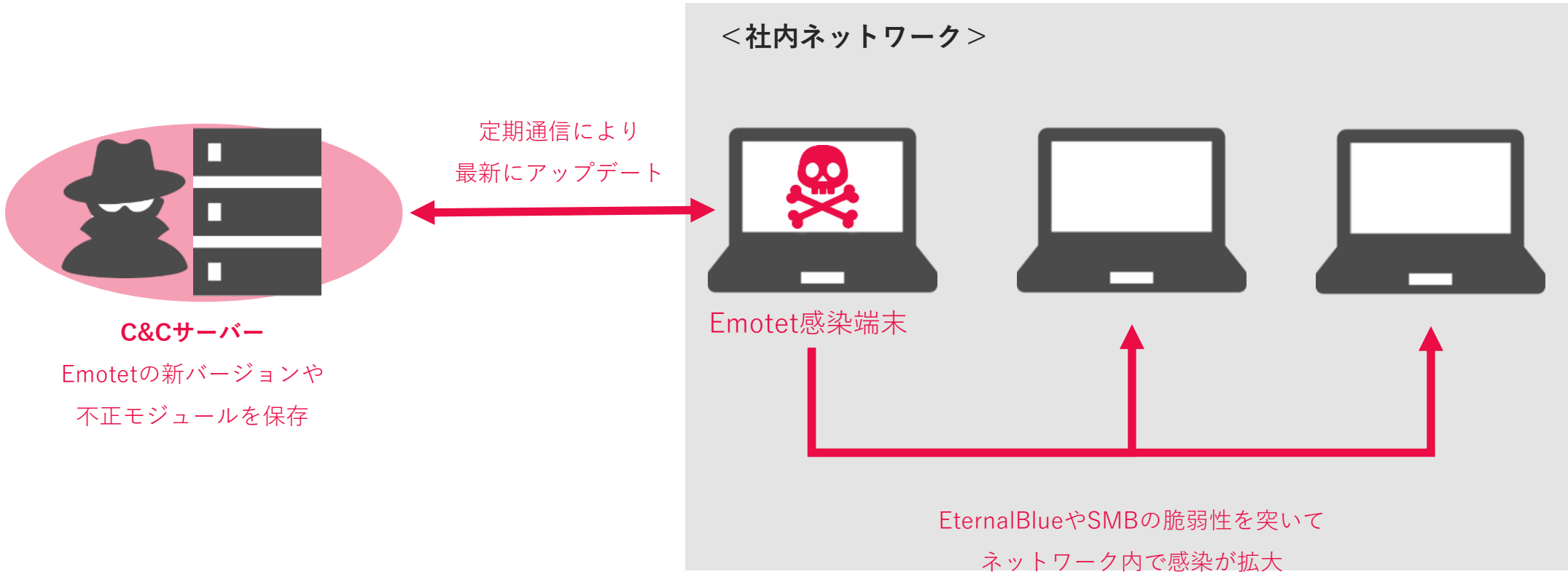

Emotetのファイル自体が添付されるのではなく、マクロ付きのMicrosoft Wordドキュメントが送られてきます。

添付ファイルのマクロが実行されると、複数の PowerShell やコマンドが実行され、Emotet本体がダウンロードされます。

出典：JPCERT/CC

# 自己増殖能力を持ち、潜伏しながら頻繁にアップデートし続ける増殖型マルウェア

新たな脆弱性の発見が感染拡大の引き金となるかのように、どんどんと脆弱性をついて拡散していきます



# 情報窃取が完了したらランサムウェアを呼び寄せ、自身の活動の痕跡を隠して調査不能に

情報を搾取した痕跡をフォレンジックされないよう消した上で暗号化するという厄介な攻撃手法

**Emotetに感染**

ばらまきメールに添付したMicrosoft Wordドキュメントのマクロが実行され、EmotetがPCに侵入、感染する。

**情報窃取などの不正行為**

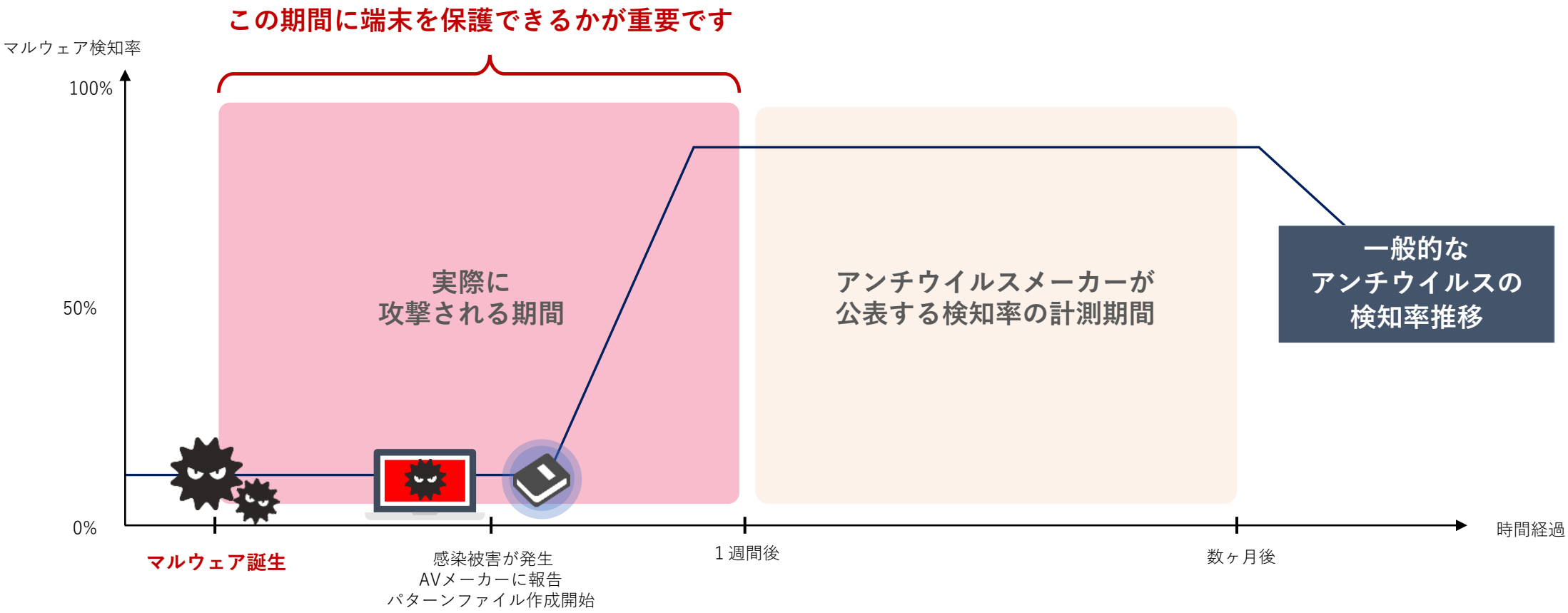
PCに潜伏したEmotetが様々な不正モジュールをダウンロードし、認証情報の窃取や他のPCへの侵入を試みる。

**ランサムウェアで痕跡抹消**

PCのデータが暗号化され、使用不可に。データを復元できないため、Emotetが原因なのか、どんな情報が窃取されたのか、調べることすらできない。

# 未知のマルウェアは既存アンチウイルスの検知方式では攻撃を受けてしまう期間が発生

現在主流となっているやシグネチャ型は、攻撃を受けてからパッチを作成します。その間は攻撃を防ぐ手出てはありません

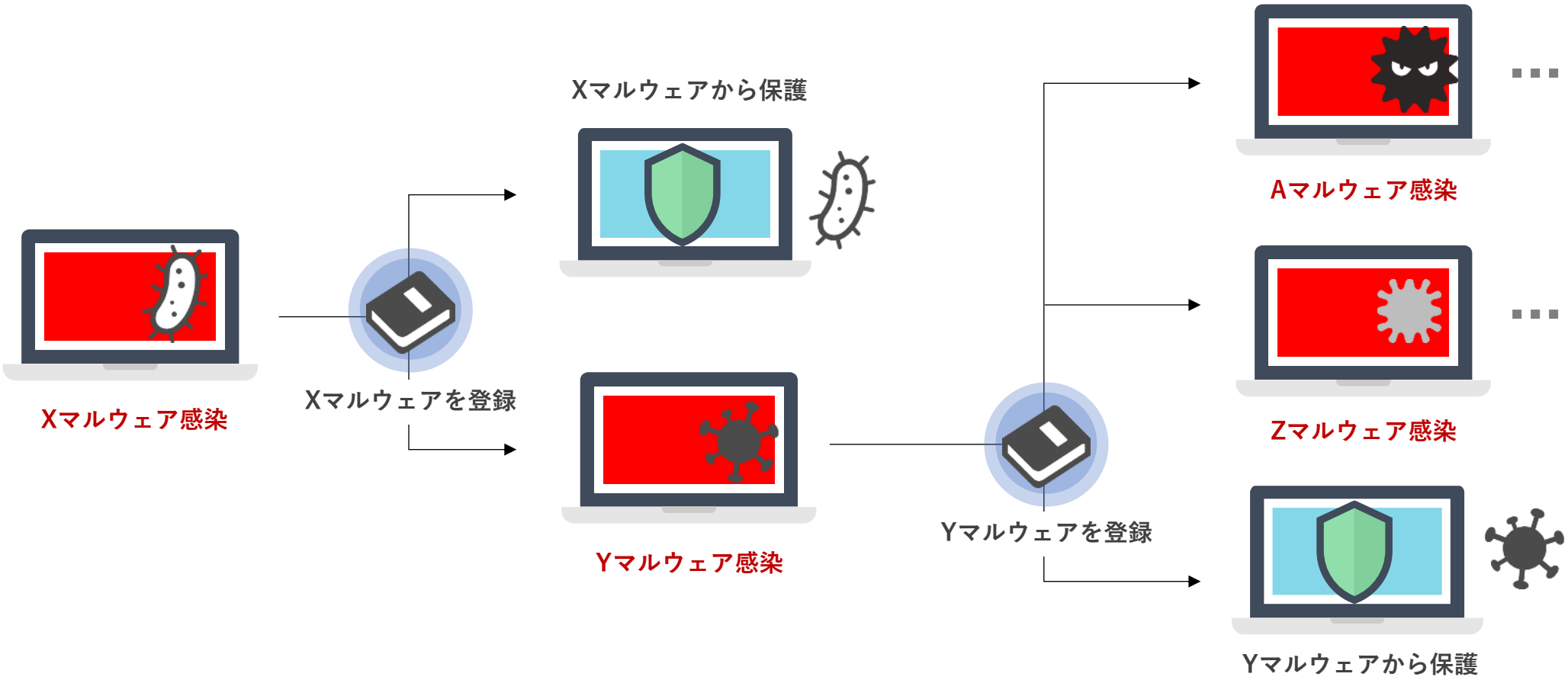


# セキュリティ対策の現状と課題

既存対策の課題

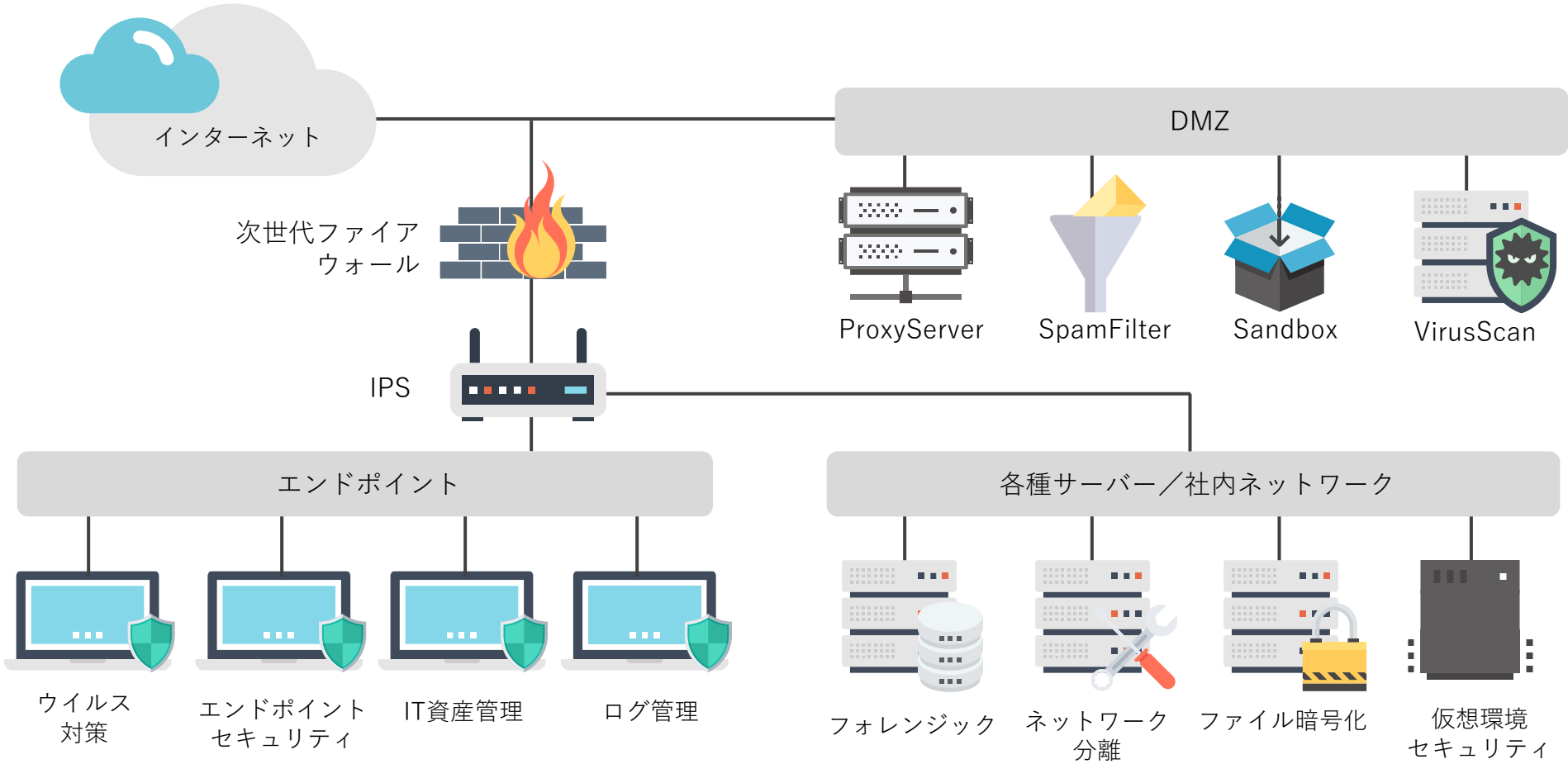
# 攻撃は使い捨て未知のマルウェアばかり…シグネチャベースのパターンマッチングでは限界

パターンマッチング方式は、感染報告後シグネチャに登録されれば、検知・保護が可能だが初見では検知が難しい仕組みです



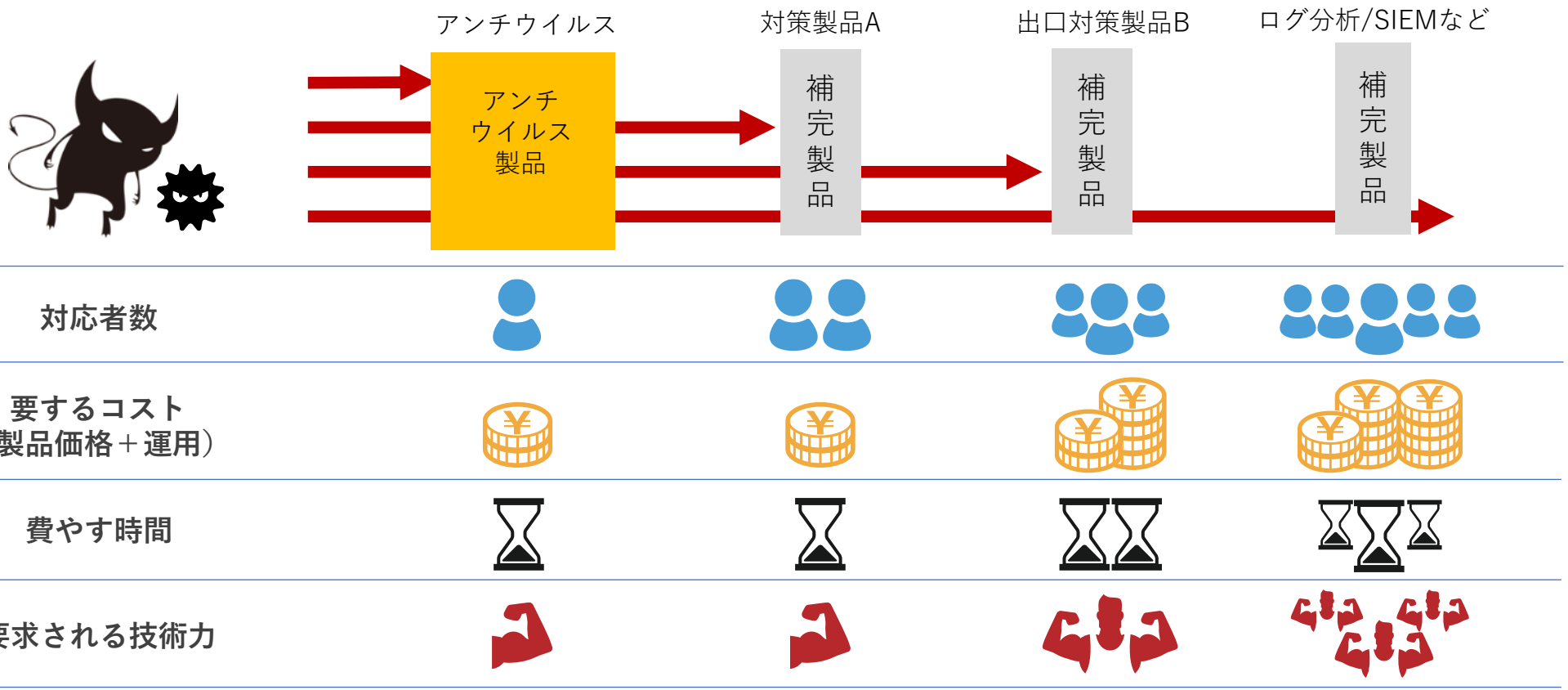
# 多様化する脅威に対抗する多層防御！増大するコスト、求められる専門スキル

すり抜けを少しでも防ぐために強固なセキュリティが求められており、多層的に対策する=多層防御が効果的です

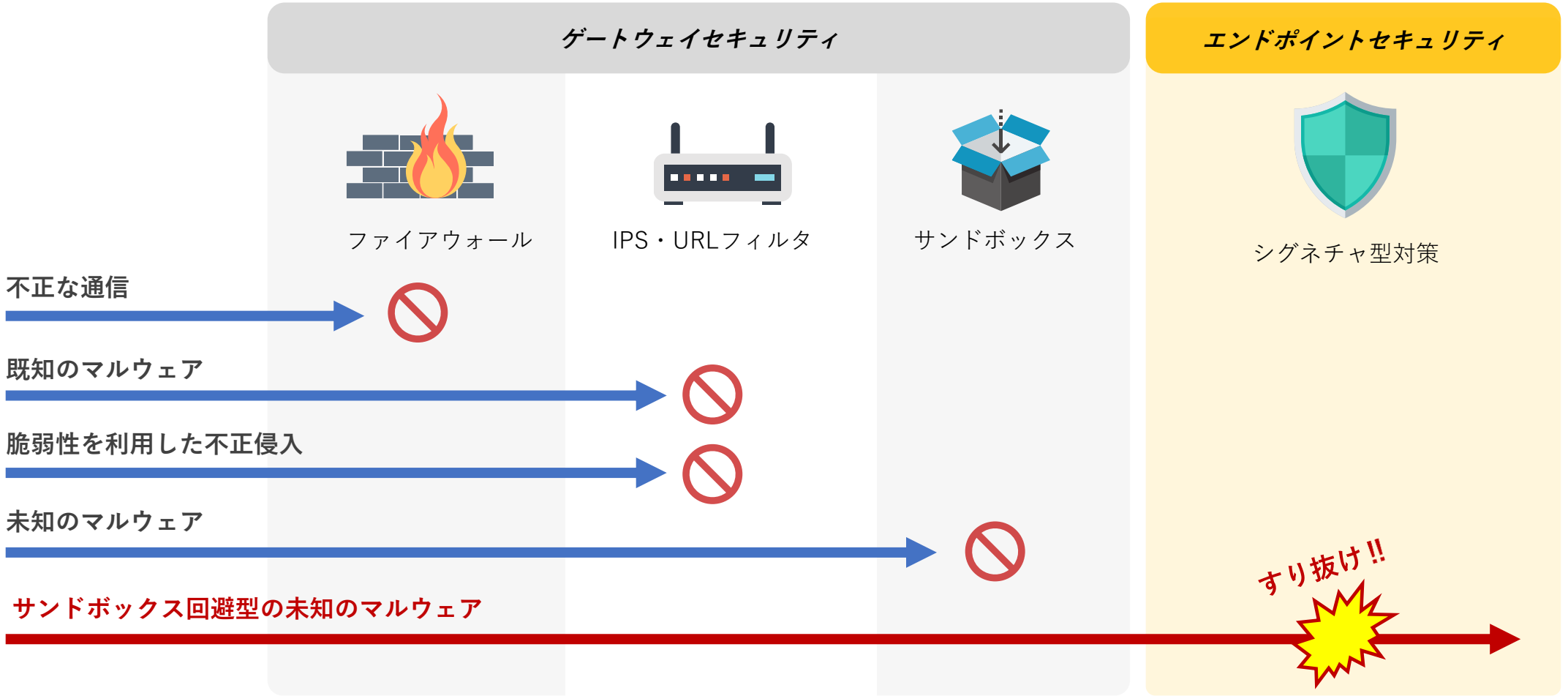


# 対策製品を多数導入するという事は、専門技術や管理工数・運用コスト・対策コストが必要

多層防御の強みは様々なツールで防御することが可能ですが、その分の様々なリソースをかく確保する必要があります



# 多層防御を以てしても巧妙化する未知のマルウェアを止めることが困難な時代が到来



# 多層防御のパフォーマンスを発揮させるには

# 「お金」と「人」と「スキル」が伴う

# AIアンチウイルス「Aurora Protect」

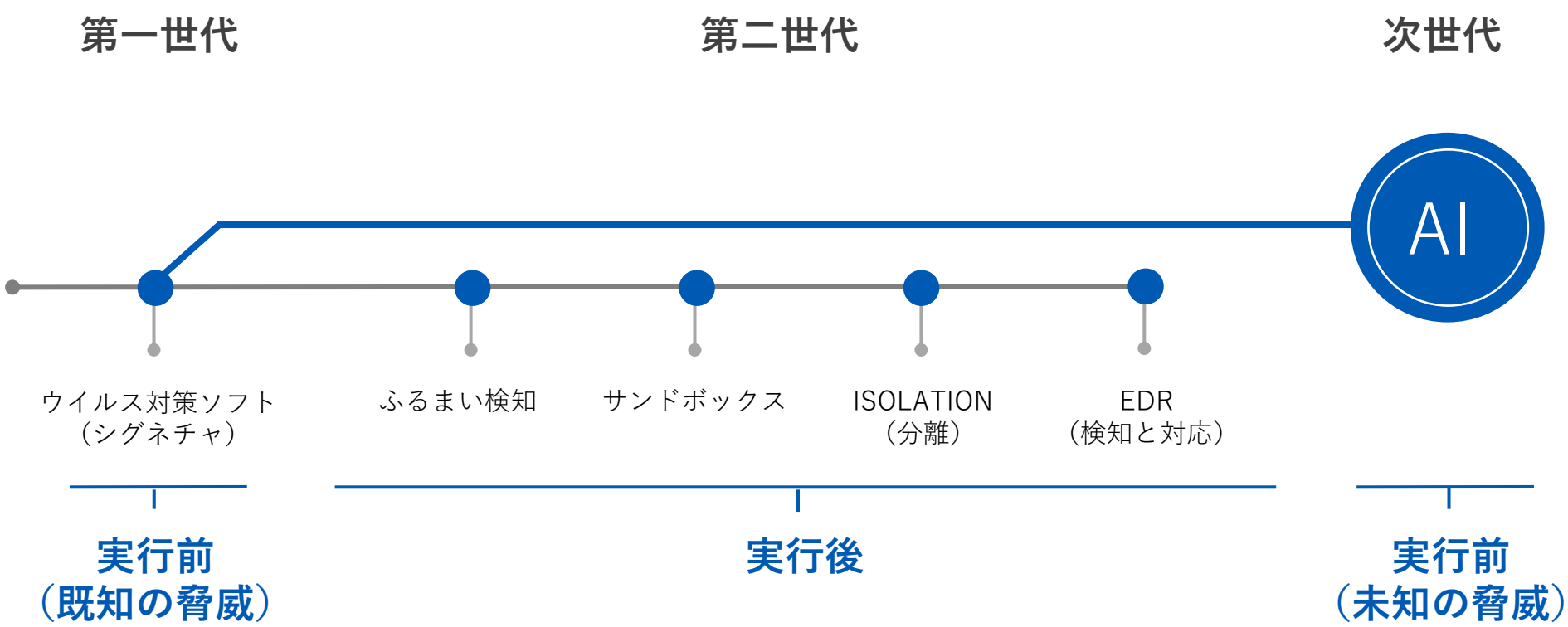
会社概要／導入実績と受賞履歴／検知率比較テスト結果／AI活用方法と差別化ポイント

# フォーチュン500企業、政府機関が採用！世界中のエンドポイントに導入

世界的有名企業や政府が採用する高性能なアンチウイルス製品として成長

# 「止められない」が前提の実行後対策ではなく、実行前に止める次世代型AIエンジン

アンチウイルスの変遷は時と共に変化しており、Aurora Protectを始めとしたAIによる検知は次世代型と言われています



# 未来に発生するマルウェアを予測して検知！あらゆる未知・亜種のマルウェアから保護

Aurora Protectの検知方式は、2年以上前の過去の検知エンジンでも、未知のマルウェアを予測検知しています

**MyWebSearch**
26か月前に予測

**Emotet**
27か月前に予測

**PolyRansom**
28か月前に予測

**GandCrab**
26か月前に予測

**installCore**
27か月前に予測

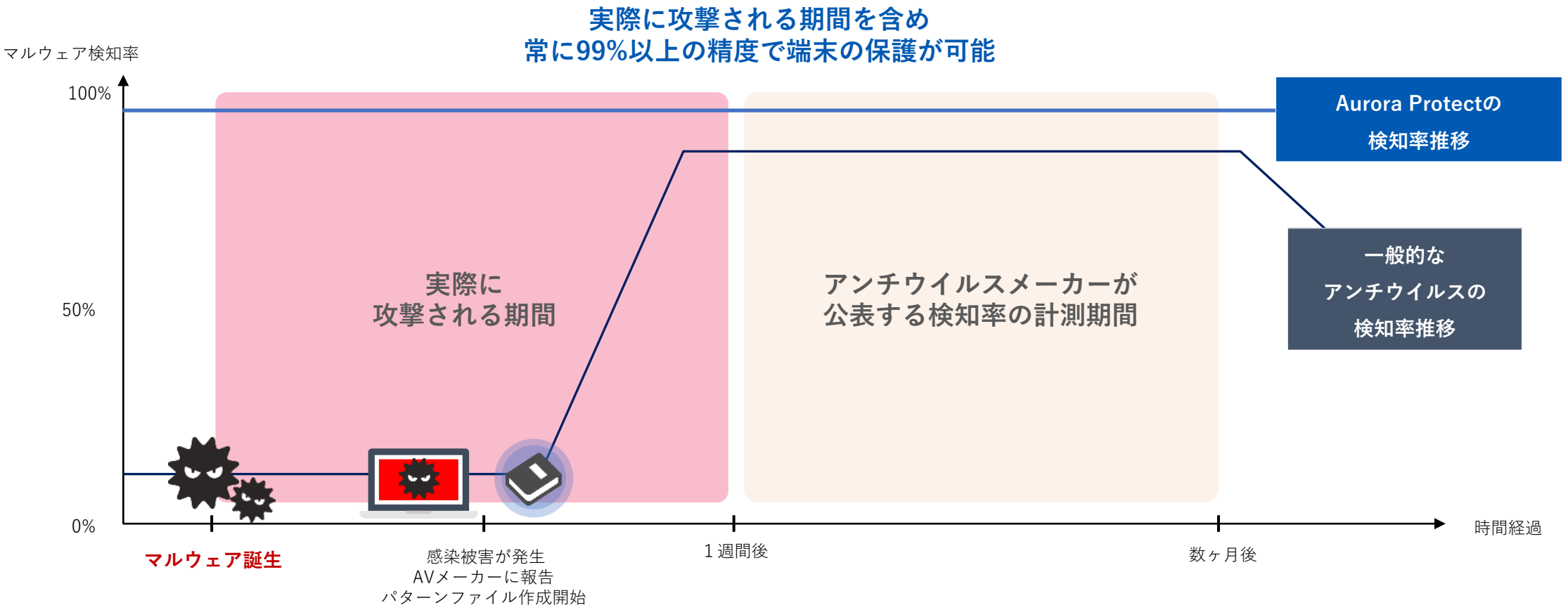
**GoldenEye**
13か月前に予測

**Petya-Like**
20か月前に予測

**WannaCry**
19か月前に予測

# シグネチャレスのためパッチの有無に左右されないため、未知のマルウェアにも即対応が可能

AIによるこれまでにない検知方式を採用することで、マルウェアの種類・時期に関係なく安定した検知率を保てています



# AIによる機械学習の特許技術を活用した「予測防御」という検知方式

マルウェアはもちろん、正しいとされる通常のファイルも機械学習するため、より高精度に判別することが可能です


## 収集と学習

正常なファイルとマルウェアを10億以上収集し、クラウド上のAIに教師データとして学習させる

## 特徴抽出・数値化

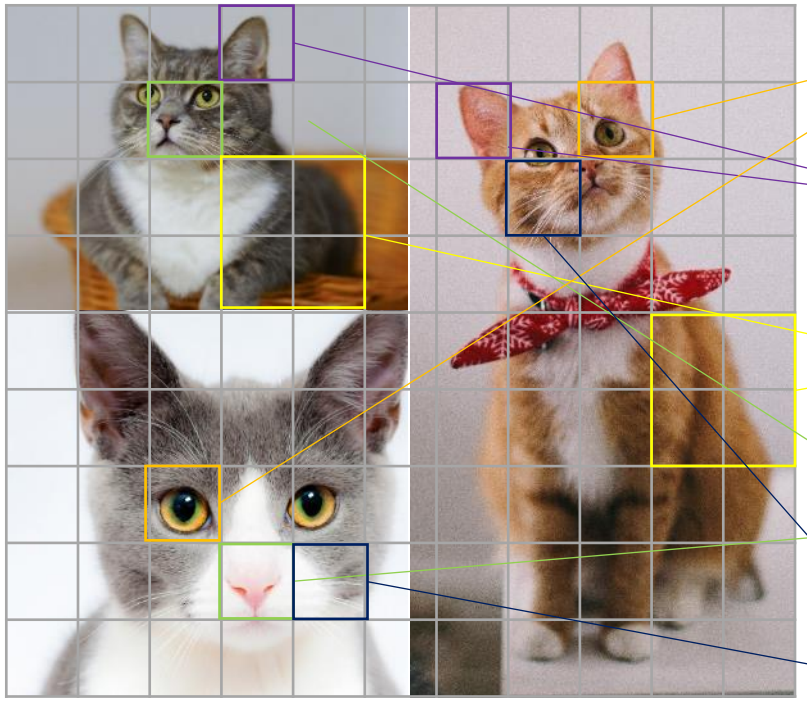
教師データの特徴点を抽出（1ファイルあたり最大700万の特徴点）、各ファイルのマルウェアらしさを数値化

## 数理モデル作成

数学者やアナリストのチューニング後、膨大なノウハウを反映した数理モデルを作成。端末上は数理モデルのみ稼動

# AIが画像を詳細に分析し特長を機械学習！一致要素をDNAレベルで総合的に判断

一部の要素が一致しなくても総合的に猫の可能性が高いと判定できる技術を、マルウェアに応用しています



大きな目が2つ

三角の耳

ふわふわの体毛

ピンク色の鼻

長いひげ

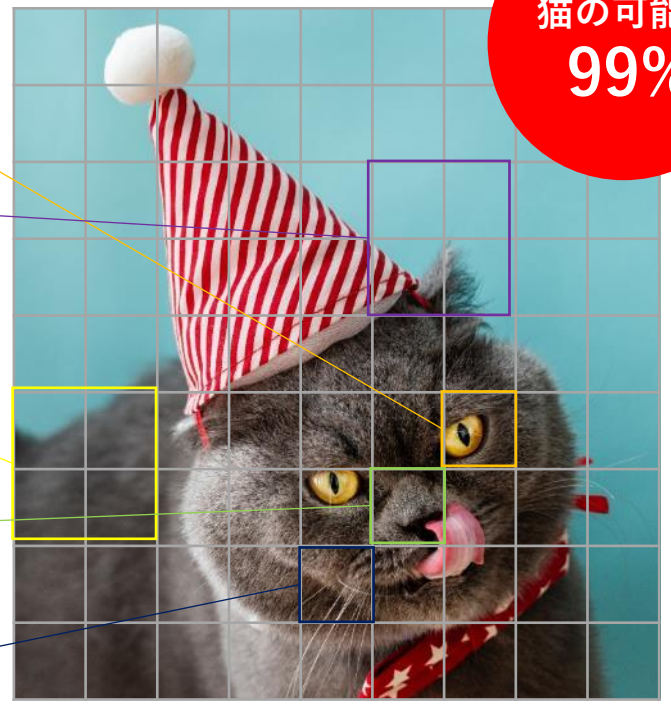
○

×

○

×

○




猫のサンプル写真を細かに分析し
猫の特長を学習

対象の写真を細かに分析し
猫の特長と一致するかで猫かどうかを判定

# 10億以上のファイルをAIが機械学習・分析した膨大なデータベースを活用し判定！

**マルウェアのモデル**

過去に発見されたマルウェアなど
ありとあらゆる危険なファイルの
特長を分析・数理モデル化

**【700万の特徴点】**

ファイルサイズ

アイコン

**比較**

セクションヘッダ

セクションデータ

文字列

etc…


**検査対象のファイル**

マルウェアのモデルと比較することで
過去に発見されたマルウェアと全く同じでなくとも
その特徴からマルウェアであると特定できる

# シグネチャでの既知の脅威検知や、マルウェアの動作後のふるまい検知は行わない

Aurora ProtectはAIの機械学習による新しい検知方式をなので、マルウェアを動かさずして予測検知が可能です

**シグネチャ**

**ふるまい検知**

**サンドボックス**

# 数理モデルに基づくアプローチ！人工知能が未知のマルウェアを動作前に防御

検知の高さはもちろん、シグネチャレスなのでアップデートの手間・クライアント負荷がありません

**DNAレベルの**
**マルウェア解析**

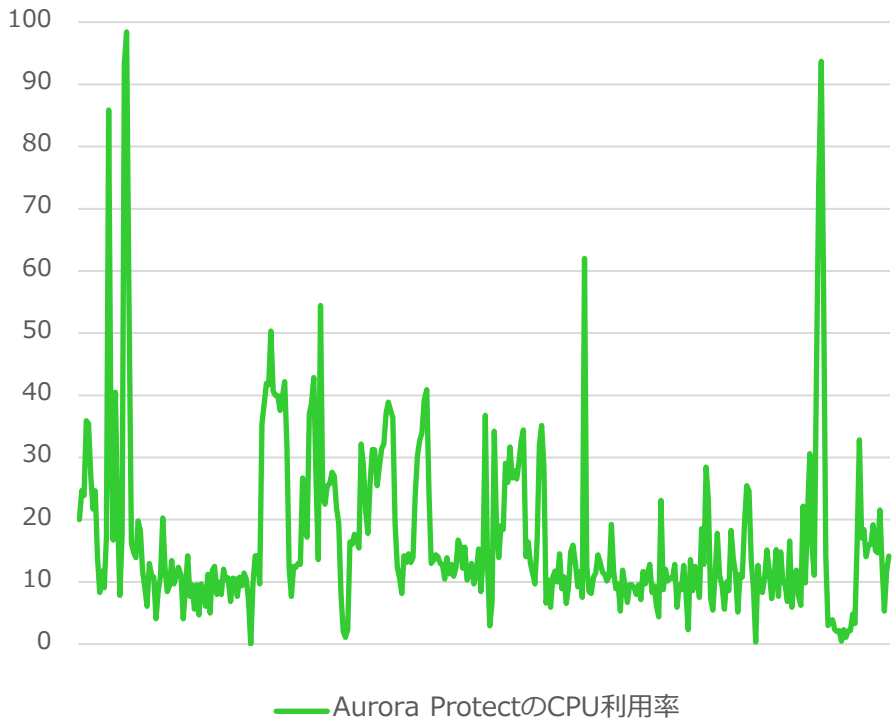
**AI（人工知能）**
**による自動判断**

**毎日のアップデートや**
**インターネット接続不要**

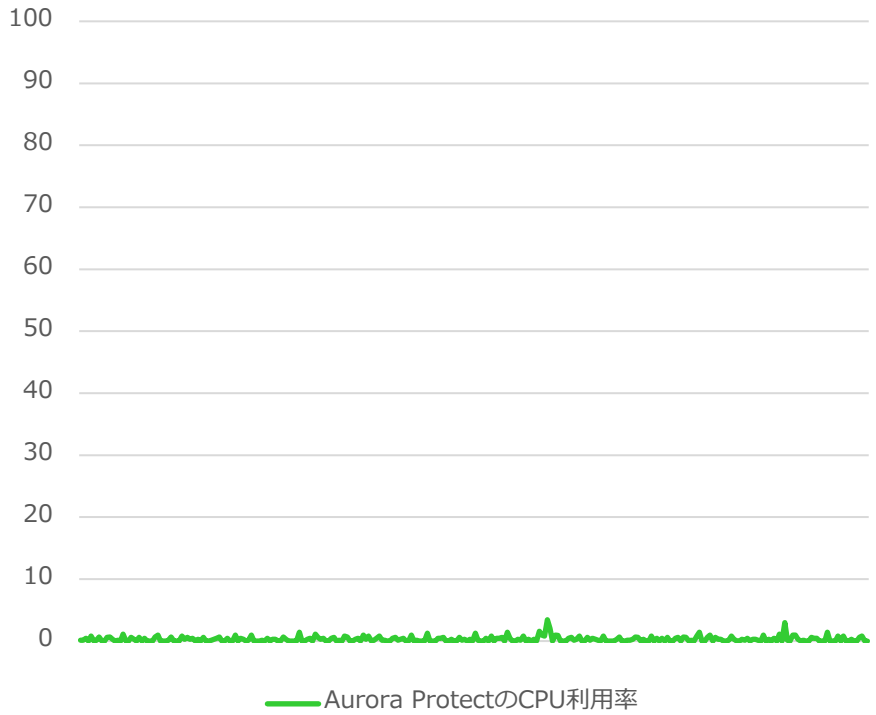
# 新規インストール時のみフルスキャン！以降は低負荷でCPU負荷平均0.3%

フルスキャンは初回インストール時のみ！その後は新しいデータが入ってきたタイミングで検知・隔離を行います

**フルスキャン時（平均17%）**

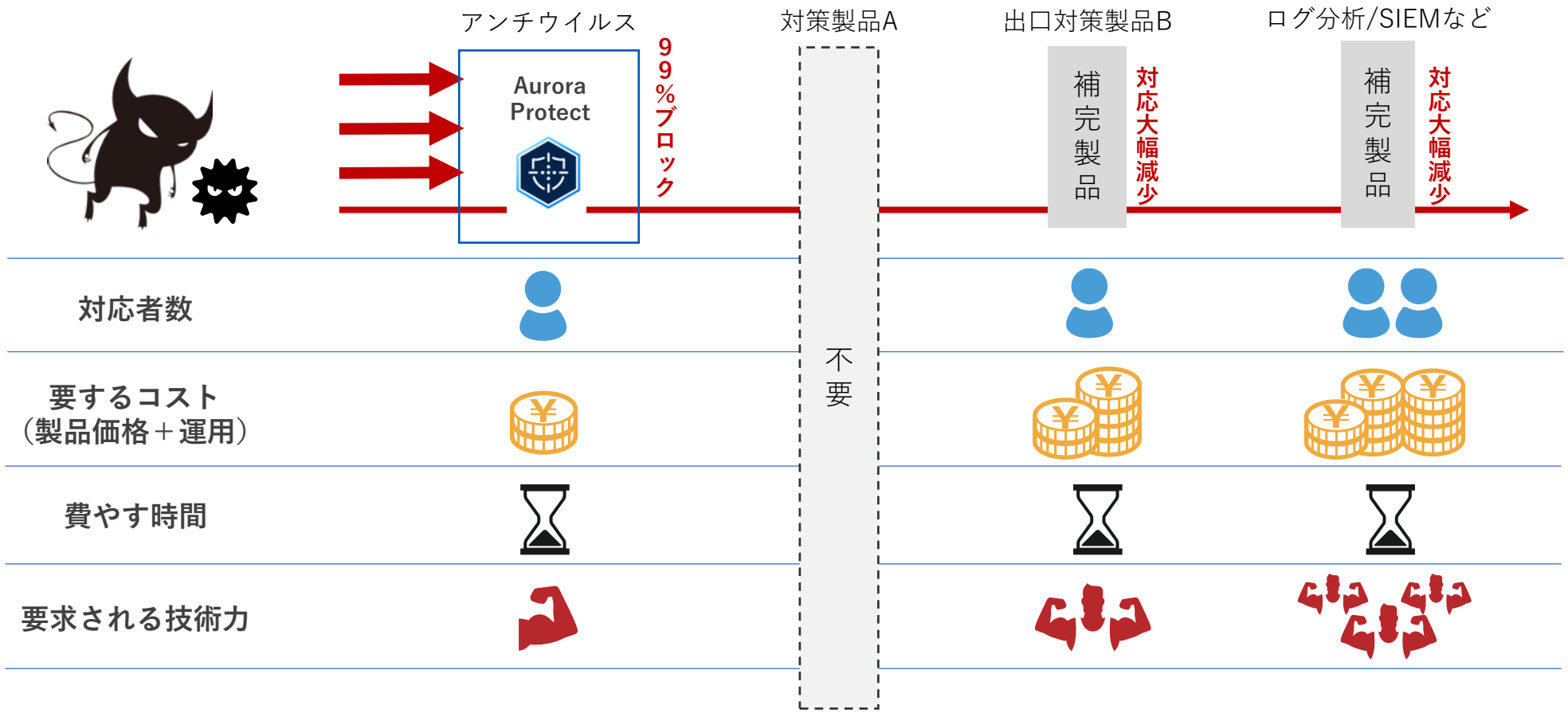



**フルスキャン後（平均0.3%）**



# エンドポイントを最大限保護する事で、すり抜けが減りインシデント対応工数を大幅削減

Aurora Protectで99%マルウェアを止めるので、たとえば対策ツールの見直しや、その先の対策工数を大幅に削減できます

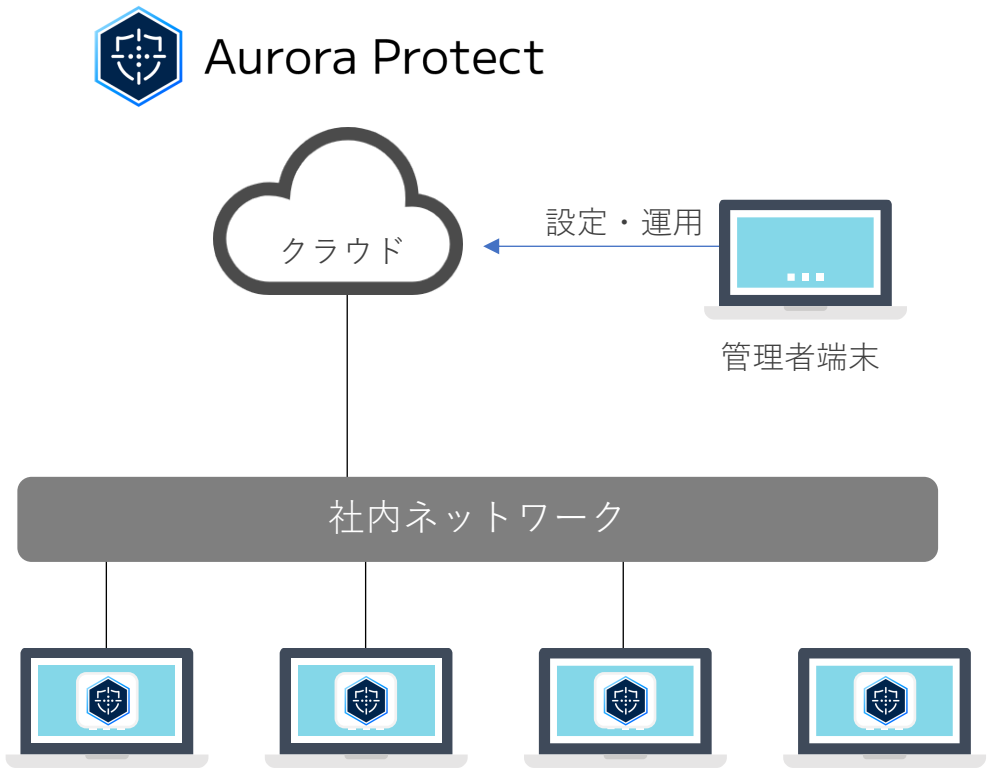


# システム構成と導入・運用

システム構成／導入期とランニング期／導入期の検知運用／ランニング期の自動隔離運用

# Aurora Protectはサーバー構築不要！エンドポイントセキュリティをクラウドで管理

Aurora Protectモジュールをクライアント PCにインストールすることで、エンドポイントでマルウェア検知・隔離が実現します




エンドポイント端末上で検知（非ネット接続環境下でも検知）

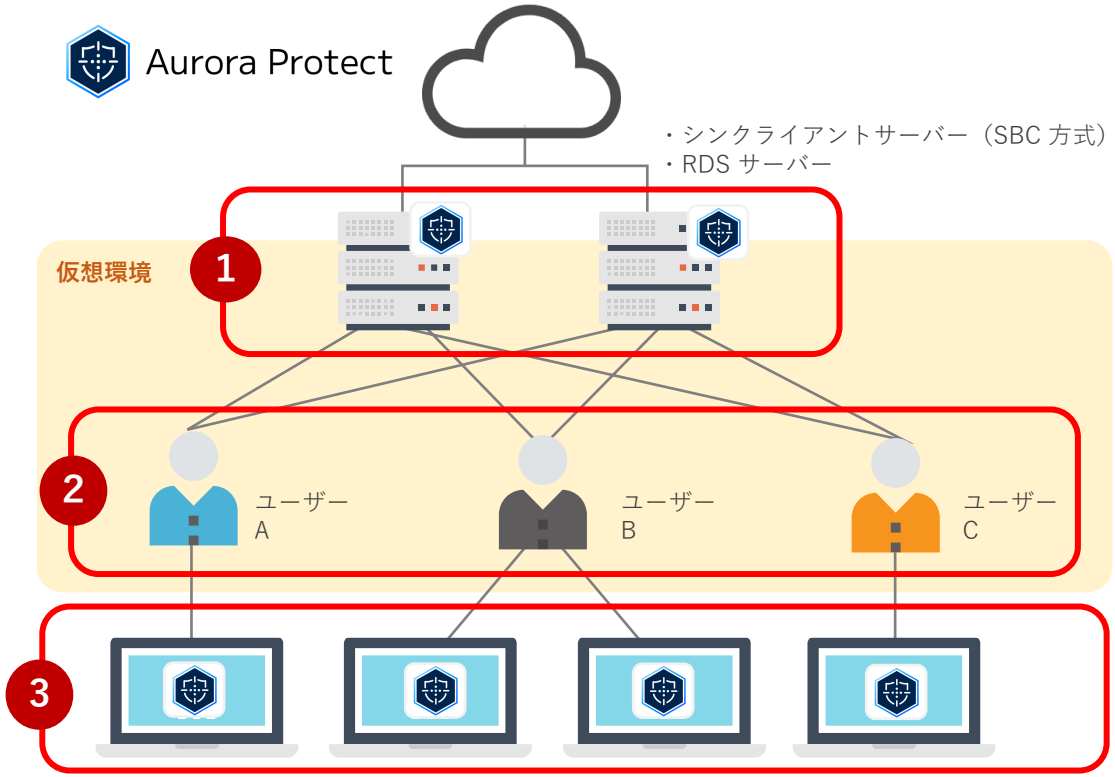
| | Windows | macOS | Linux |
|---|---|---|---|
| OS | ・Windows XP SP3 ※<br>・Windows Vista ※<br>・Windows 7 ※<br>・Windows 8 ※、8.1<br>・Windows 10<br>・Windows 11<br>・Windows Server 2012 、2012 R2<br>・Windows Server 2016、2019、2022 | ・macOS Catalina ※<br>・macOS Big Sur<br>・macOS Monterey<br>・macOS Ventura<br>・macOS Sonoma | ・Ubuntu LTS<br>・SUSE Linux Enterprise Server<br>・CentOS<br>・Red Hat Enterprise Linux など ※ |
| メモリ | 2 GB | | |
| HDD 空き | 600MB | | |
| その他 | ・.NET Framework 3.5 (SP1) 以上<br>・インターネットブラウザ<br>・インターネット経由でログイン、インストーラーにアクセスし製品登録が行える環境<br>・インストールを行うための管理者権限 | | |

※ 該当の KB を適用やご利用にあたり注意点や、 Linux 対応環境の詳細はこちらをご参照ください

# 仮想化におけるクライアントライセンスの考え方

## 【SBC 方式】

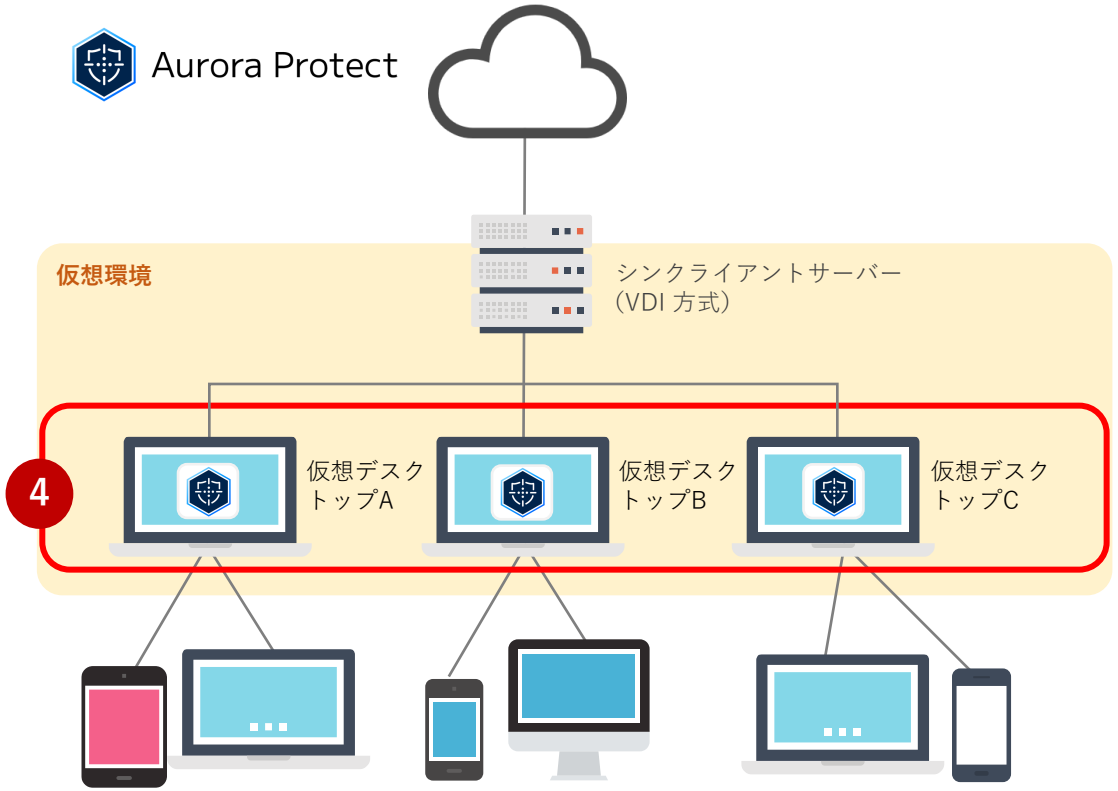
**リモートデスクトップサービス（RDSH）・XenApp など**




SBC 方式、RDS サーバーへの Aurora Protect を導入する場合は、**サーバー台数分のライセンス**（①）と、**サーバーに接続するユーザー数分のライセンス**（②）が必要です。※接続元端末にも Aurora Protect を導入する場合は、**接続元端末数のライセンス**（③）も必要です。

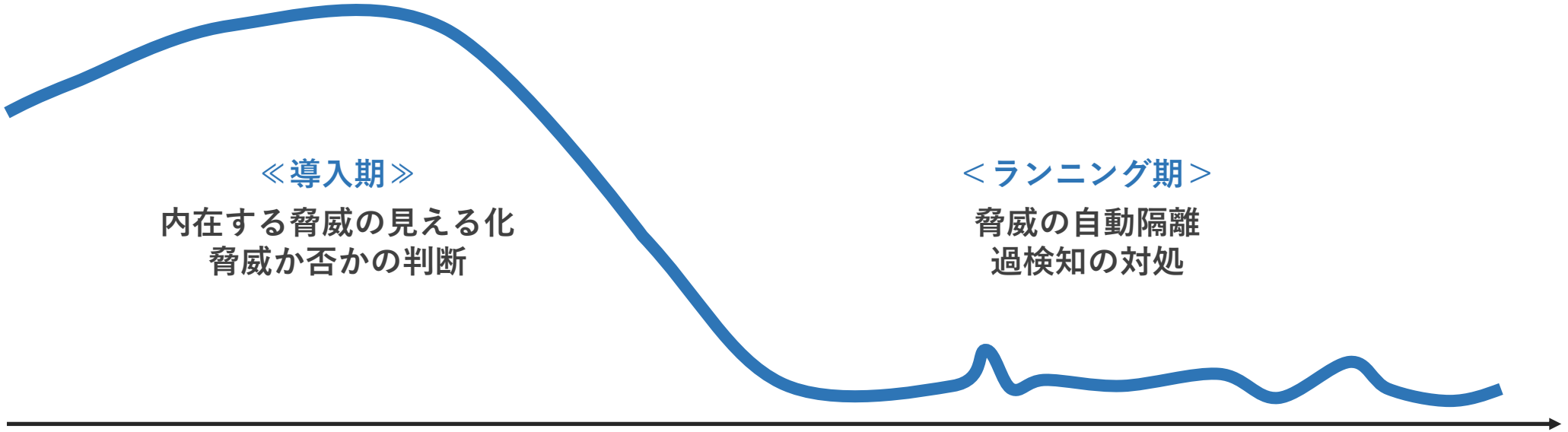
## 【VDI 方式】

**XenDesktop・Vmware View など**




VDI 方式の場合、**利用デスクトップ数分のライセンス**（④）が必要です。

# MOTEX と Aurora Protect の連携した導入支援体制で、初期導入から運用までの課題を一緒に解決




**○実施する内容（検知モード）**

- マルウェア要素をもつファイルの検知
- マルウェアを隔離
- 業務アプリをセーフリストに登録

**○実施する内容（自動隔離モード）**

- 検知したマルウェアを自動隔離
- 過検知時にセーフリストに登録
- 流入原因の調査、再発防止

# まずは検知ファイルを振り分け！実運用体制構築後に自動隔離設定へ移行が理想

Aurora Protectはバッティングしないため、既存アンチウイルスソフトとの並行運用も可能です

【振り分けのイメージ】


業務アプリケーションを隔離する可能性があるため
最初から自動隔離モードにするのは危険です。
初期設定は検知モードで運用してください。

既存アンチウイルスソフトをアンインストールする場合
運用準備が完了し自動隔離モードに変更した後、
実施されるかを検討してください

# インストール後は全ファイルスキャン！通常はダウンロード時と実行直前の検知・隔離

検知したものを解析し、企業の運用方法に合わせて、攻撃時のアクションを選択することが可能です

## 検知

### ●マルウェアダウンロード時

### ●マルウェア実行直前

## 解析

### ○マルウェア

・トロイの木馬
・ランサムウェア
・ダウンローダー
・ワーム
・フェイクAVなど

### ○PUP（有害な可能性のあるプログラム）

・ハッキングツール
・リモートアクセスツール
・ツールバーなど

## アクション

### ●検知のみ

導入期は検知のみで確認し
ホワイトリスト登録

### ●自動隔離

自動でファイル名を変更して
隔離フォルダへ移動

### ●自動アップロード

検体を提供しエンジン強化への
フィードバック

# 全ファイルをスキャンし、危険・異常を把握！許可するか隔離・駆除するかを振り分け

1000台環境では5000万ファイルをスキャン！危険度高のマルウェアを約100件検出しています

# 危険・異常で検出したファイルの詳細確認！他社の許可・隔離判断をクラウドで共有

Aurora Protectが検出した脅威のスコアや詳細を表示。ハッシュ値から第三者機関のサイトも参照することが可能です

# セーフリスト登録対象となった「特定の動きを行うアプリ」を事前に登録！

検知されるアプリは特定の動きのものがあり、先にセーフ登録することで初期運用をさらに楽にすることができます

**PC診断ツール**

**ハッキングツール**

OS・レジストリ情報の収集解析・外部へのデータ送信

**リモートコントロール**

**リモートアクセスツール**

コンピュータの遠隔アクセス・リモート操作

**特定マルウェア駆除ソフト**

**ハッキングツール**

OS・レジストリ情報の収集解析・データの削除・破壊行為

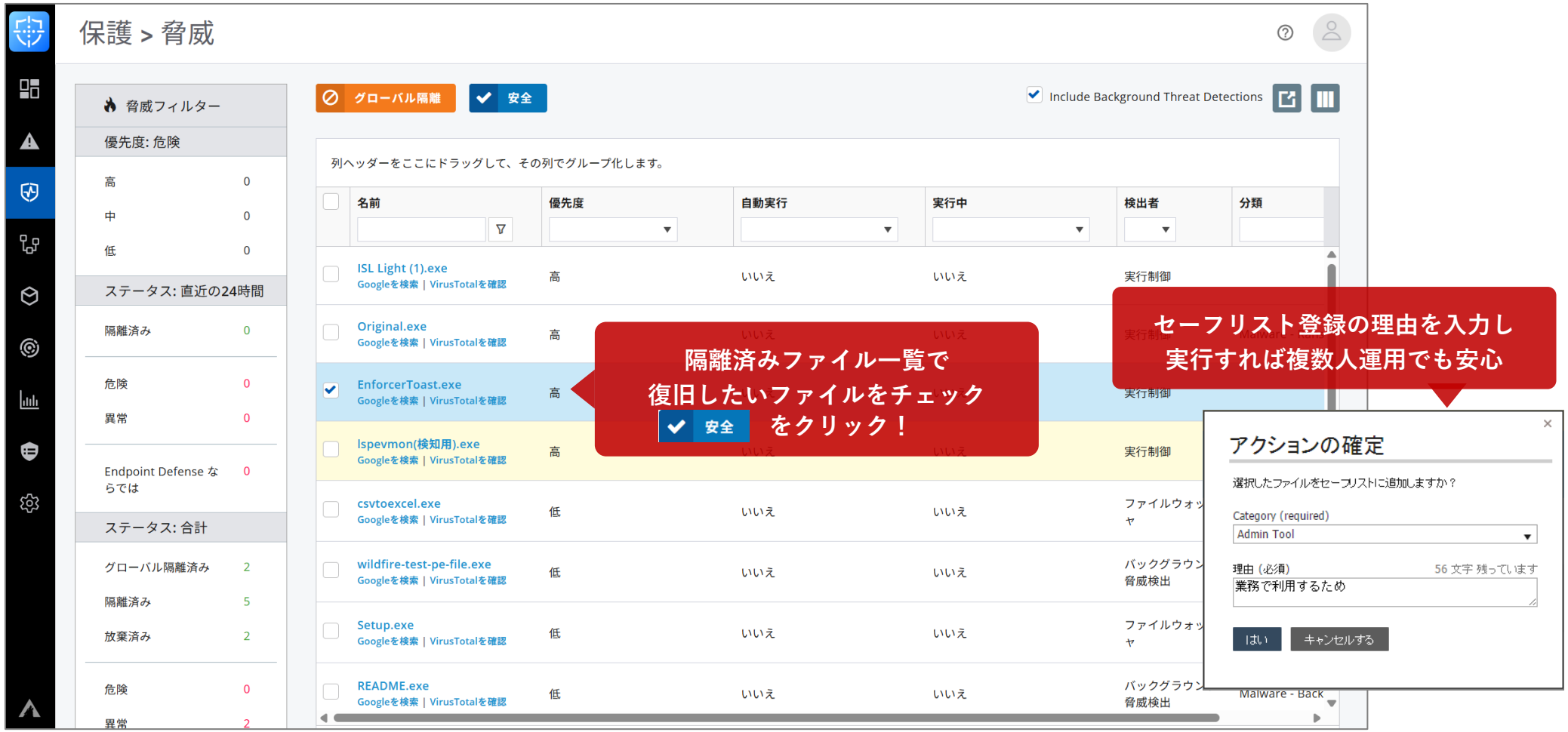
**業務アプリ**

**その他**

OS・レジストリ情報の収集解析・権限昇格、外部へのデータ送信

# 自動隔離されたファイルを簡単に復旧可能！セーフリスト登録後リアルタイムに反映

自動隔離されたファイルものワンクリックで簡単に復旧が可能。細かい設定はいらず運用工数がかかりません



# 既存アンチウイルスでスルーした脅威を検知！導入前検証での過検知率は0.002%程度

AIによる検知は精度が高く、時に過検知が心配されます。Aurora Protectは過検知が少なく、セーフリスト運用がしやすい製品です

## A病院

| | |
|---|---|
| 総ファイル | 265万件 |
| 検知総数 | 167件 |
| ・Unsafe | 105件 |
| ・Abnormal | 62件 |
| 過検知率 | 0.0029% |
| セーフリスト登録 | 76件 |

## 建設会社B

| | |
|---|---|
| 総ファイル | 44万件 |
| 検知総数 | 62件 |
| ・Unsafe | 41件 |
| ・Abnormal | 21件 |
| 過検知率 | 0.0011% |
| セーフリスト登録 | 5件 |

## 製造業C

| | |
|---|---|
| 総ファイル | 32万件 |
| 検知総数 | 189件 |
| ・Unsafe | 171件 |
| ・Abnormal | 18件 |
| 過検知率 | 0.0037% |
| セーフリスト登録 | 12件 |

・過検知率は、「セーフリスト登録件数 ÷ 総ファイル数」で算出しています。

# LANSCOPE サイバープロテクション powered by Aurora Protect

運用代行や定期レポートサービスをご用意

# 未知・亜種のマルウェアもマシンラーニングで99%検知！次世代のアンチウイルス

## 次世代 AI アンチウイルス

Aurora Protect

AI を活用したマシンラーニングによる予測検知が可能で、未知・亜種のマルウェアも 99%※ の高検知が実現。別途オプションの Focus（EDR） で感染原因の調査も可能

- AI による高精度な予測検知
- シグネチャレスで日々のアップデート不要
- 誤検知が少なく低負荷

※2024年5月 Tolly 社のテスト結果より

# 企業のニーズに併せて必要なプランを選択可能

## 基本ライセンス　年額 6,000 円 or 月額 500 円※

**●Aurora Protect**

AI を活用した高精度のマルウェア検知・隔離機能をご提供

**●初期運用サポート**

Aurora Protect の製品概要や導入手順などを説明
（画面共有で約1時間）

**●保守サービス**

製品に対する保守サービス対応
受付時間：月～金 9:30 ～ 12:00 ／ 13:00 ～ 17:30
（土日祝日年末年始および当社規定の休日を除く）

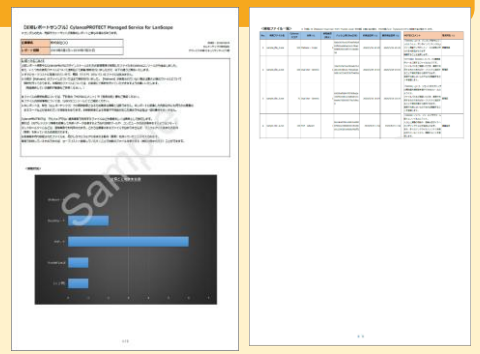
・専用 Web サイトのご利用　　・最新バージョンアップ
・専用ヘルプデスクサービス　・その他サポート

※最小購入ライセンスは5ライセンス～になります。

※2024年11月より上記価格に改定

## 定期レポート（オプション）　年額 960 円 or 月額 80 円

年に4回（利用期間開始（更新）後、3・6・9・12カ月目）、マルウェア検知結果のサマリーレポートを提供




## 運用代行（オプション）　年額 2,040 円 or 月額 170 円

お客様に代わって、エムオーテックスの技術者が Aurora Protect の運用作業を代行します。

# LANSCOPE エンドポイントマネージャー× Aurora Protect

運用イメージ__検知・隔離・流入原因の追跡

# LANSCOPE エンドポイントマネージャー にAurora ProtectをOEM連携

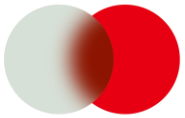
未知のマルウェアを99%検知・隔離に加え、クリックするだけでカンタン追跡・再発防止までをワンストップ

**次世代 AI アンチウイルス**

Aurora Protect

- AI による高精度な予測検知
- シグニチャレスで日々のアップデート不要
- 過検知が少なく低負荷

**統合型エンドポイントマネジメント**



LANSCOPE
Endpoint Manager

- IT 資産管理・内部不正対策・外部脅威対策がワンストップ
- 国内のみならず海外端末も一元管理、VPN 外でも管理が可能
- 必要な機能だけを選択して導入可能

**未知のマルウェアを 99% 検知・隔離・攻撃原因の追跡・再発防止策を実施**

**AI による予測検知** | **流入原因を追跡** | **再発防止対策**

# “人のPC操作”を記録することでマルウェア流入原因やルール違反を見える化

ウイルス感染のトリガーとなる「人の操作」を記録することで、抑止効果やルール作りにつながります

メール送受信
件名・添付ファイル名

Web閲覧
アップロード
ダウンロード

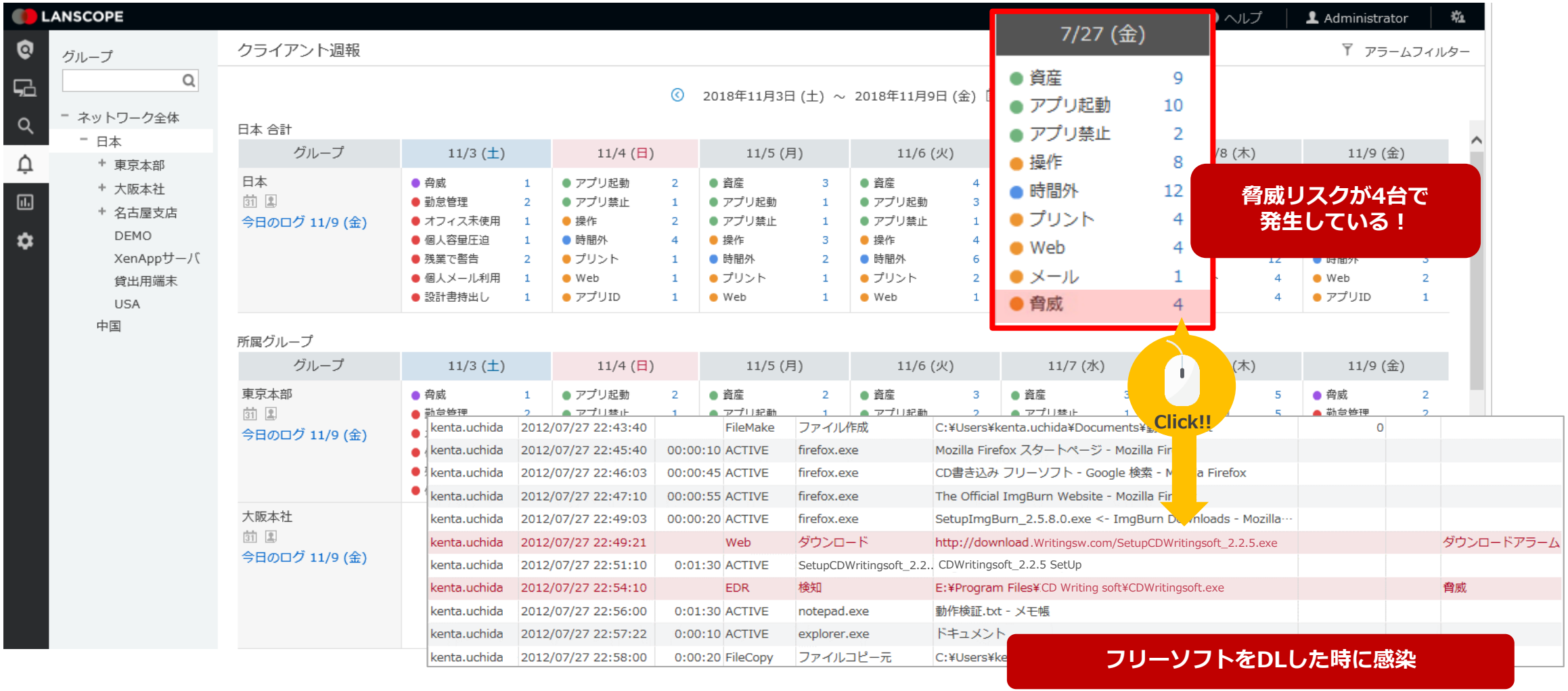
ファイル操作
作成・コピー・削除
移動・名前変更

USBメモリなど
記憶媒体利用

印刷

# マルウェア検知前後の “人の操作” を把握！侵入経路を操作ログで確認し、再発防止へ

クリックするだけで、誰がいつどんな行動をとったことが原因でマルウェア攻撃を受けたのかを追跡できます



# マルウェア流入原因の“人の脆弱性”に対してLANSCOPE エンドポイントマネージャーでポリシー強化

攻撃を受けた原因が分かれば、該当の操作を搭載されている機能（導入時に選択）で禁止・制御することが可能。再発防止策に繋がります

**●流入原因となりえるユーザー操作・感染防御への対策●**

Ｗｅｂサイト
アクセス制御

デバイス
持込み制御

不正
アクセス制御

メッセージ
による啓蒙

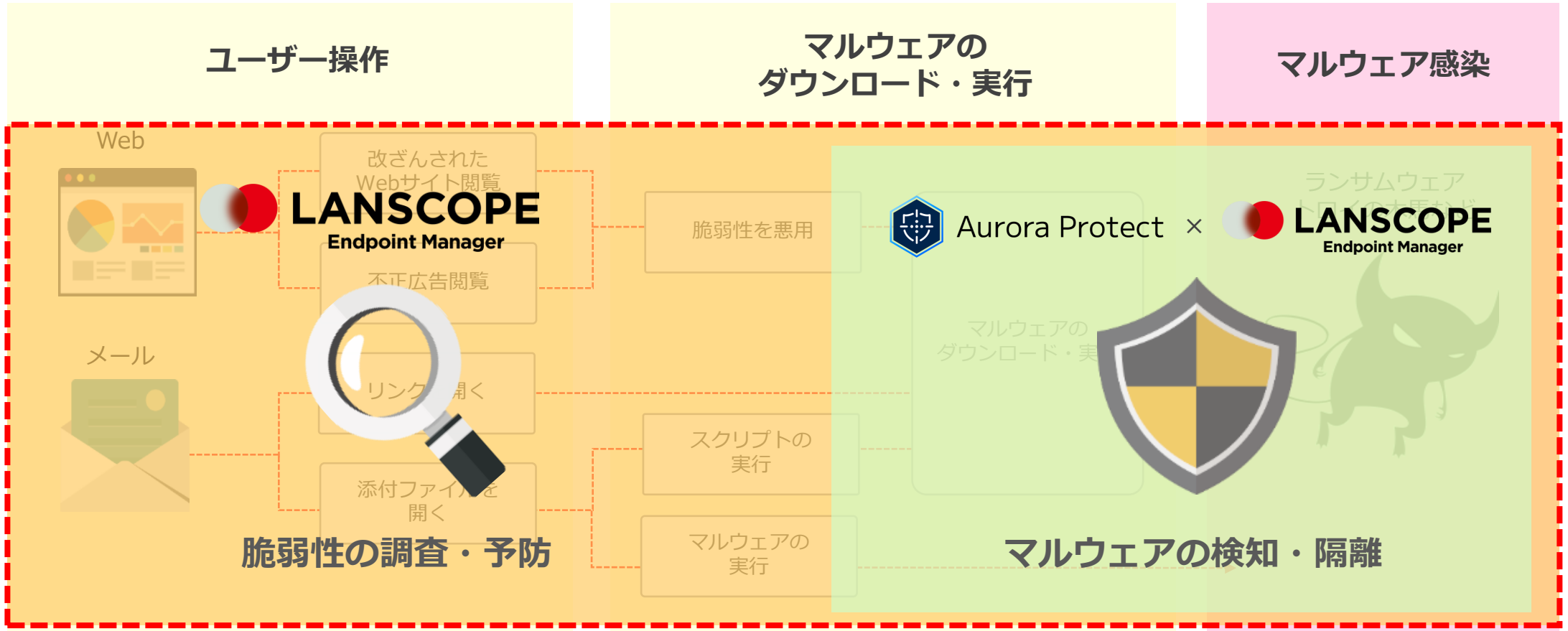
USBメモリ
制御

サーバー
監視・制御


無線
Wi-Fi制御

# マルウェア感染に伴う対策・再発防止策まで１製品でワンストップで対策が可能

感染源の特定には専門知識も高価なツールも不要！ CylancePROTECT × CylancePROTECTがあれば、検知・隔離・原因追跡・再発防止策が可能です



台数無制限　　レポート解説付

# AI アンチウイルス 1カ月無料体験版

## ～端末に潜む マルウェア を見つけ出せ！～

Aurora Protect を 1カ月無料で何台でもインストールでき、

**自社ネットワーク内に危険なマルウェアが潜んでいないかを無料で調査でき**

**EDR オプションも体験可能。**

体験後、ご希望の方にはマルウェア検知結果のサマリーレポートをプレゼントします！

**【お申し込みはこちら】**

https://go.motex.co.jp/l/320351/2019-06-27/2fv6jr

（EDR オプションの体験を希望の場合には、お申込みフォームの備考欄にご記載ください。）


**製品に関するお問い合わせ**

■ 営業本部

大阪本社　06-6308-8980
東京本部　03-3455-1811
名古屋支店　052-253-7346
九州営業所　092-419-2390
E-mail　sales@motex.co.jp

**ご導入後の製品利用に関するお問い合わせ**

サポートセンター　0120-968995 （携帯・PHSからは06-6308-8981）
お電話受付時間　9:30～12:00/13:00～17:30（平日、祝祭日除く）
Email お問い合わせ　support@motex.co.jp