CTC Engineer's Insight #4

CTCが挑んだ、現場で効く金融ITセキュリティ

― 運用・検証・生成AI活用から攻撃トレンド対処まで

# エンドポイントセキュリティ実検証からみる再検証の必要性

伊藤忠テクノソリューションズ株式会社
金融セキュリティ技術部
伊藤　早紀

MS&ADシステムズ株式会社
サイバーセキュリティ推進部
西城　秀行

# 登壇者のご紹介（CTC）

## 講演者名

伊藤　早紀（いとう　さき）

## 部署

伊藤忠テクノソリューションズ株式会社
金融事業グループ　金融システム技術本部　金融セキュリティ技術部

## 経歴

- 証券会社向けのインフラ構築案件・保守運用を担当
- 金融業界向けのセキュリティソリューションの企画、プリセールス、技術支援などの幅広い業務に従事

# 登壇者のご紹介（MS&ADシステムズ）

## 講演者名

西城　秀行（さいじょう　ひでゆき）

## 部署

MS&ADシステムズ株式会社
基盤運用本部　サイバーセキュリティ推進部　セキュリティコンサルティンググループ
兼 三井住友海上火災保険株式会社 データマネジメント部 企画チーム
兼 MS&ADホールディングス データマネジメント部 サイバーチーム

## 経歴

- 主にグループのサイバーセキュリティ施策(アタックサーフェスマネジメント、脅威ベースのペネトレーションテスト)の運用等を担当。
  役職は主任セキュリティスペシャリスト。
- CRTO、HTB CPTS、HTB CBBH、CISSP、CEH、AWS SCSを保持

# MS&ADシステムズとは


**ＭＳ＆ＡＤインシュアランスグループ**

**ASEAN損保シェア**

総収入保険料 **1位**

**国内保険シェア**

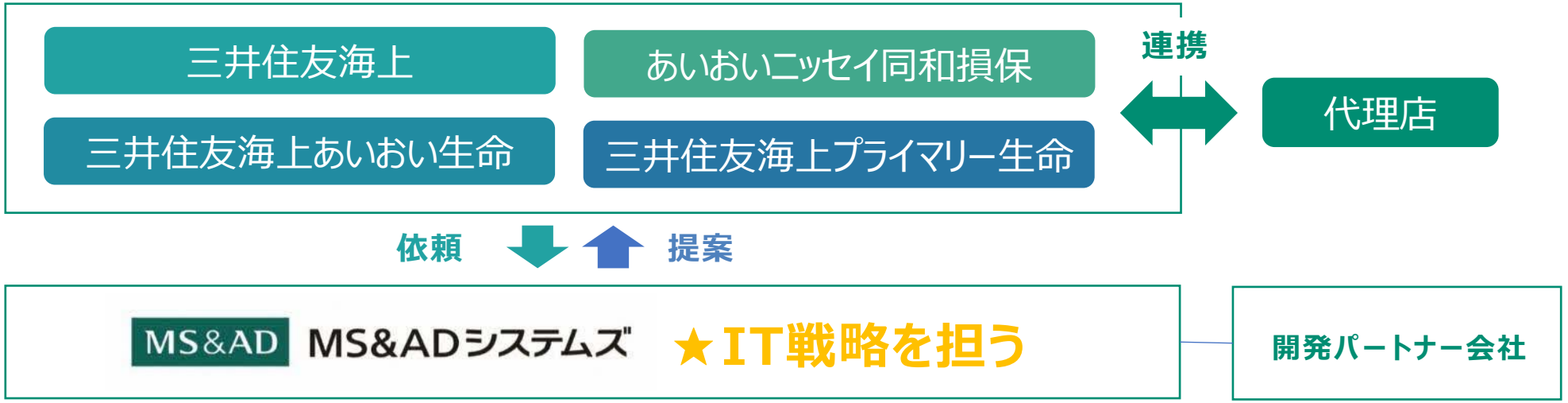
正味収入保険料 **1位**

# 事業内容

● MS&ADインシュアランスグループ各社の **保険システム全般にわたる企画から運用・保守までの業務** を一気通貫で担っています

企画 → 要件定義 → 設計 → 開発・テスト → 運用

● **保険会社や代理店のIT戦略** を支えており、商品開発から販売、事故受付や保険金のお支払いまで、すべてに関わるシステムを構築しています




● サイバーセキュリティ推進部ではサイバーセキュリティの動向をタイムリーに捕捉し、必要な対策を行ない、**MS&ADグループのサイバーセキュリティ態勢を強化**しています

# MS&ADグループ／システムズが目指すもの

MS&ADグループは
リスクソリューションのプラットフォーマー として
社会課題の解決に貢献し、社会と共に成長していきます

MS&AD

MS&ADシステムズ

デジタルやデータの力で
**保険商品やサービスの高度化**
を実現する役割を担う

# 1．検証の背景

# エンドポイントセキュリティ検証の背景

## ①背景

- 担当のエンドポイント保護製品は導入から一定期間を経ており、再評価を実施したいニーズが存在
  導入当初評価が高い製品でも、年月の経過で状況が変わる恐れあり。

## ②課題

- 机上評価のみでは、限界
  ⇒費用対”効果”を検討するにも、起点となる脅威検知”効果”は不透明で説明困難
  (“定性的な”検出は可能な製品が多いがその**精度や網羅性は不明**)
- 実機評価には、複雑な環境構築や危険度の高い検体、シップディップコンピューター等の環境が必要

## ③対応策

- 机上のみでなく、社外のパートナーの協力を得て、実機でもエンドポイントセキュリティの比較評価を実施
- 結果としてエンドポイント保護製品の脅威検知**効果を正しく把握**

# ２．検証方法と注意事項

# 検証内容

エンドポイントセキュリティ製品の脅威検知効果を評価するため、
合計**7製品**の検知率を測定し、検知率比較を行う

## ①マルウェア検知率検証

マルウェア検体を用いて検知試験をオフライン環境で実施
- 既知マルウェア
- 未知マルウェア

※社外への不正アクセスを防ぐため**オフライン**で実施

新種や亜種のマルウェアが増加しているため、
**未知のマルウェア**含めて検証を実施

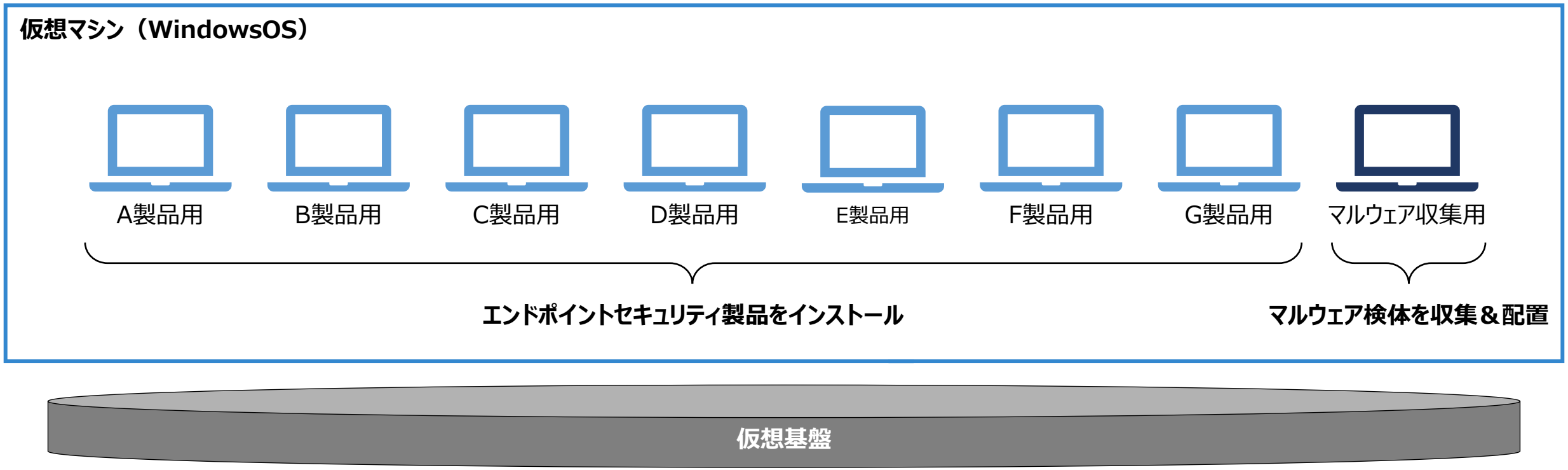
## ②振る舞い検知率検証

テストスクリプト及びツールを用いてオンライン環境で実施
- ファイルレス攻撃
- コマンド&コントロール
- EDR無効化

ファイルレスマルウェアを活用した攻撃が増加しているため、
**振る舞い検知能力**についても検証を実施

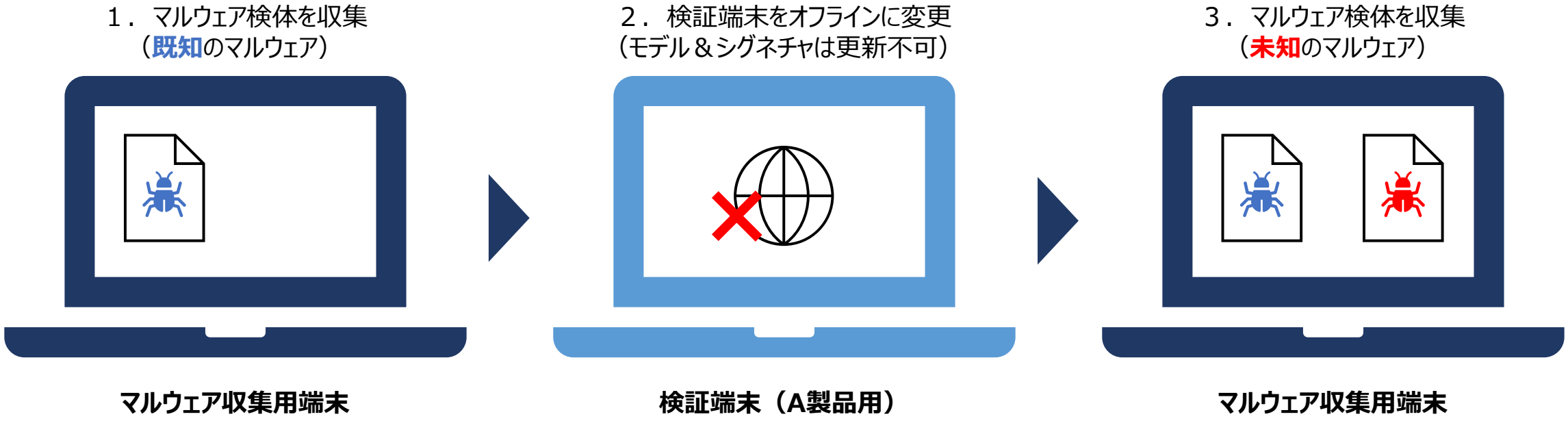
# 試験構成

- CTC検証用の仮想基盤上に仮想マシンを8台構築
- 7台の仮想マシンにエンドポイントセキュリティ製品をインストールして、検証端末として使用
- 1台の仮想マシンはマルウェア収集用端末として使用



# ①マルウェア検知率検証（マルウェア収集）

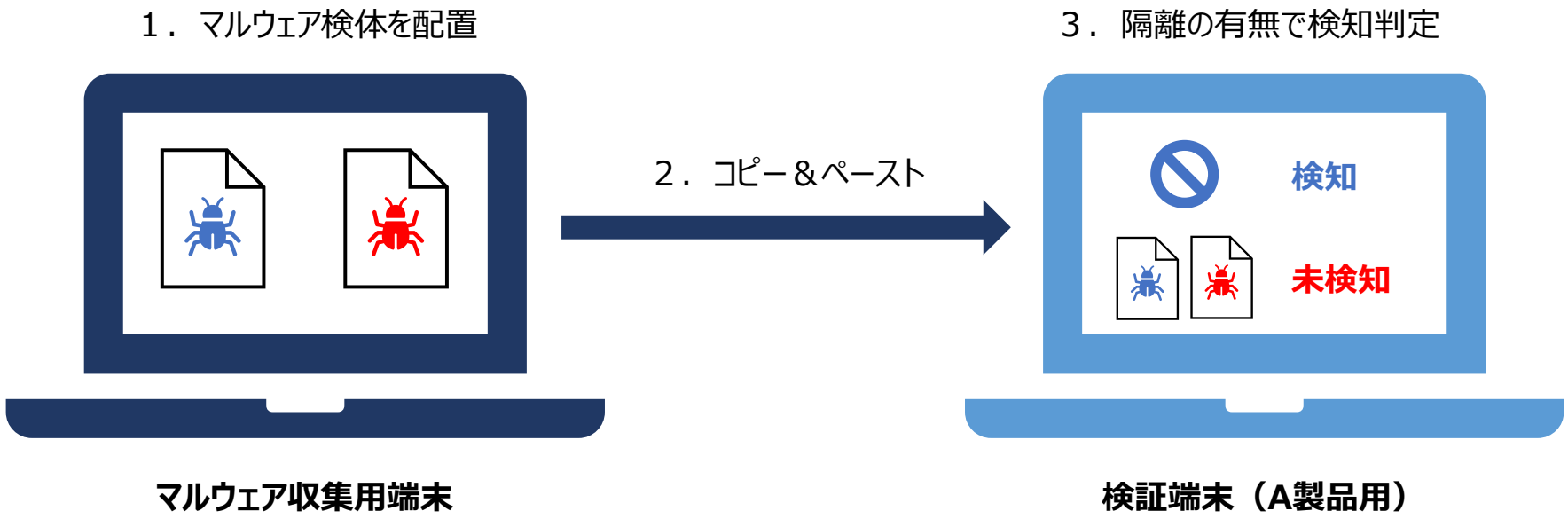
1. マルウェア収集サイトでマルウェア検体300件を収集　→**既知**のマルウェア
2. 検証端末をオフラインに変更（この時点でエンドポイントセキュリティ製品のモデル＆シグネチャは更新不可）
3. マルウェア収集サイトで、オフライン後に登場したマルウェア検体300件を収集　→**未知**のマルウェア



# ①マルウェア検知率検証（試験方法）

1．マルウェア収集用端末にマルウェア検体を配置
2．マルウェア検体をコピーして各製品用の検証端末内のフォルダにペーストする
3．マルウェア検体が隔離された場合は**「検知」**、隔離されずフォルダ内に残った場合は**「未検知」**と判定

※社外への不正アクセスを防ぐため、**オフライン環境**で実施



# ②振る舞い検知率検証（試験方法）

1. 各製品用の検証端末でテストスクリプトやツールを実行
2. 各製品の管理コンソールからファイルレス攻撃などの検知有無を確認
3. 検知イベントを確認できた場合は**「検知」**、確認できなかった場合は**「未検知」**と判定

| カテゴリ | 試験項目（例） |
|---|---|
| ファイルレス攻撃 | Windows標準ツールを利用した悪意あるコマンド実行時の検知可否（WMI・certutil等） |
| | プロセスインジェクション実行時の検知可否 |
| コマンド&コントロール | 遠隔操作ツール起動時の検知可否 |
| | 遠隔操作ツールから悪意あるコマンド実行時の検知可否 |
| EDR無効化 | EDR無効化ツールを実行時の検知可否 |

# 検証する上での注意点や苦労した点

## 検知ポリシー設定について

- 製品によって、検知ポリシーの考え方や設定項目が大きく異なるため、条件を揃えることが難しい

検知ポリシーの設定方針を
事前に**関係者と合意**しておくことが重要

## 許可リスト登録について

- 振る舞い検知率検証はテストツールを許可リストへ適切に登録しないと、ツールが実行防止されることで後続の試験ができなかったり、過剰に検知を止めてしまうケースがある

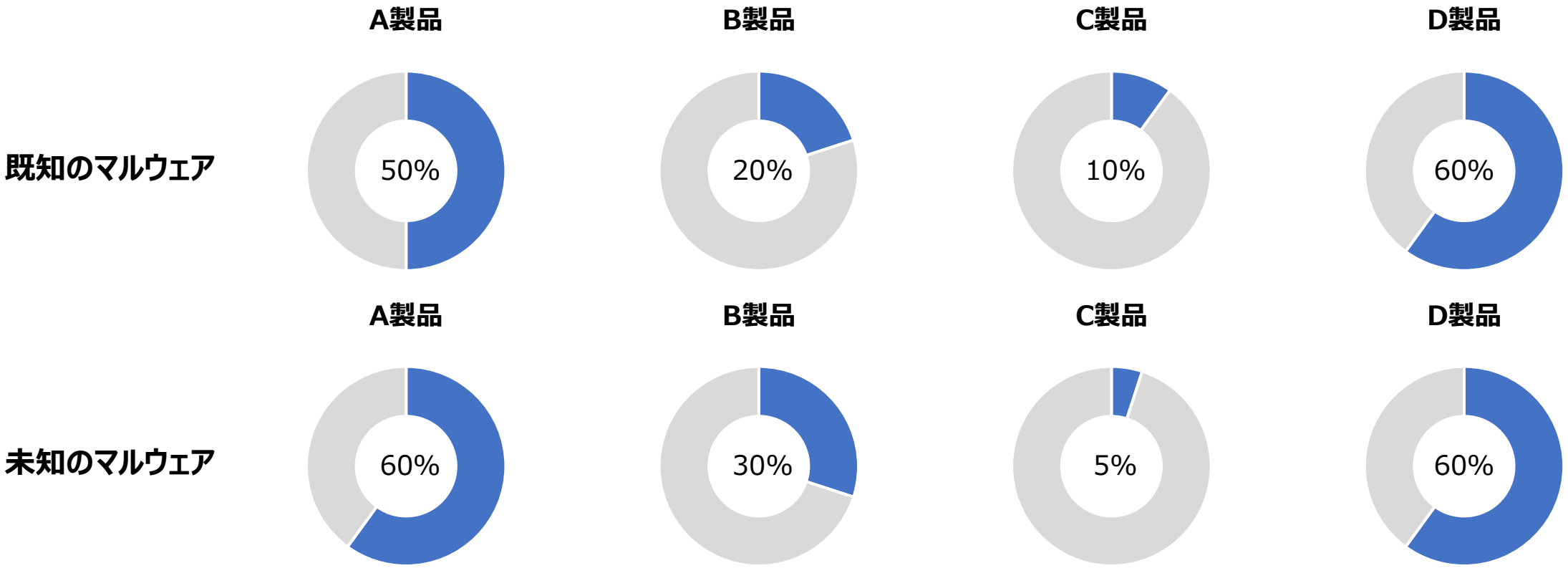
事前に各製品の
許可リスト**登録方法や影響を把握**することが重要

# ３．検証結果を踏まえて意識すべきポイント

# ①マルウェア検知率検証結果サマリ

- 製品によって検知率に大きく差がある
- 最も検知率が高い製品においても、4割程度が検知できていない

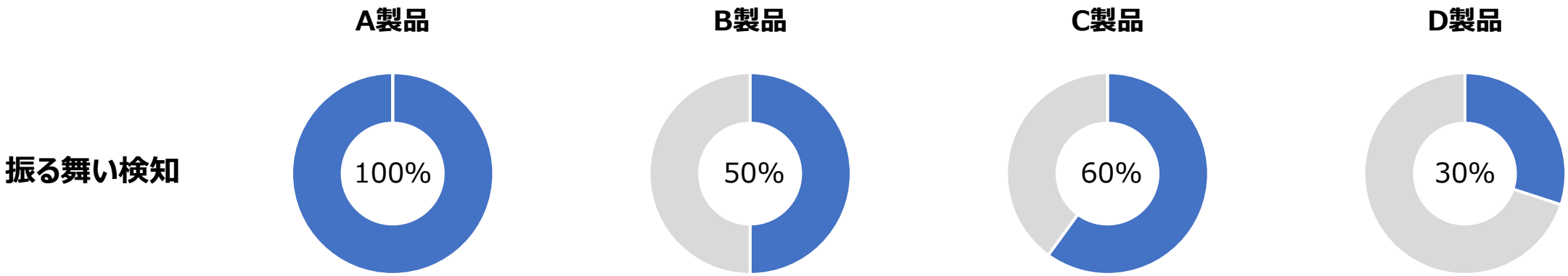
※検知率はおおよその数値となります。
※結果は検証方法や環境によって変動する可能性がございます。



# ②振る舞い検知率検証結果サマリ

- 製品によって検知率に大きく差がある
- 全て検知できた製品がある一方、他の製品においては4割～7割程度が検知できていない

※検知率はおおよその数値となります。
※結果は検証方法や環境によって変動する可能性がございます。



# 検証結果を踏まえて意識すべきポイント

## 検証結果から分かったこと

- マルウェア・振る舞い検知率検証どちらも製品ごとの検知率に大きく差があった
- 製品によっては、どのテストケースにおいても検知率が限定的だった

## セキュリティ担当者が意識すべきポイント

システム更改や契約更新のタイミングで自社環境に合わせた
エンドポイントセキュリティ製品の**再検証を行うことで対策の見直し**をすることが望ましい

# ４．MS&ADシステムズ社のコメント

# 実機検証をおえて

**業務効率化と説明責任を果たす観点での実検証**

## 1 サイバー攻撃は増加・進化中、高度なセキュリティ人財は継続して不足中

- 公開レポートやホワイトペーパーから明確な傾向　≒　対応の難易度は上がる一方
- サイバーセキュリティの人財確保は難しい　≒　運用効率の重要度は上がる一方

⇒検知精度が高い製品で防御する事で、セキュリティインシデントを防止できる確度は上昇
**高度な人財は、その人財でしかできない業務にフォーカス**できる!

## 2 システム(エンドポイント保護製品)の機能自体の補助は、運用(人、プロセス)では難しい

- エンドポイント保護製品の機能を運用で補助する事は難しい
  YARA、SIGMAルールの開発　≒　自社開発は悩みが生じやすい(情報源の有無、開発可能な人財有無など)

⇒質・量の観点で**優れた製品を選ぶ事は効果(検知と防御)に繋がりやすい**

## 3 定性的な説明だけでは不安が残る(例:EDRが動いているので大丈夫(なハズ))

- 攻撃が流行った際に子細な個別ケースを防御できるか説明する事は難しい
  ⇒評価の中に実機検証を含める事で、種別に応じた検証結果を根拠として説明に活用できる。
  **データからの説明**がお客さま・社内での**信頼向上・安心に繋がる**!

# CTCさまへのコメント

実機での製品”検知”性能の検証に対応可能なパートナーは少数と認識。

例の少ない対応にも関わらず、大規模なテストケースに短期間で対応いただけた。
(総テストケースは約1800以上)

複数種類の製品を実機で扱い、設定まで行う。難しい対応ではあったが、柔軟かつ迅速に不足部分も検証いただけた。

# ５．まとめ

# 本パートのまとめ

**POINT 01**

エンドポイントセキュリティ製品を比較検証した結果、製品によって検知率が限定的かつ差が大きい

**POINT 02**

セキュリティ担当者は再検証を行い、定期的にセキュリティ対策の見直しを行うことが望ましい

**POINT 03**

セキュリティに関するご相談はぜひCTCへ！

無限の未来と、
幾千のテクノロジーをつなぐ。

# CTC Financial Services Group

CTC
Challenging Tomorrow's Changes