APPGUARD

サイバーセキュリティ最新攻防

～高度化・巧妙化するサイバー攻撃って何だろう？～

株式会社Blue Planet-works

上席セキュリティアドバイザー　鳴原祐輔

多用される常套句「高度化・巧妙化するサイバー攻撃」

Ever-evolving and sophisticated cyber attacks

01 サイバー攻撃における「高度化」と「巧妙化」とは

APPGUARD

高度化

技術的練度向上

攻撃者が利用するツール、技術、インフラがより洗練され、防御側にとって技術的な対策が難しくなっている状況を指している。

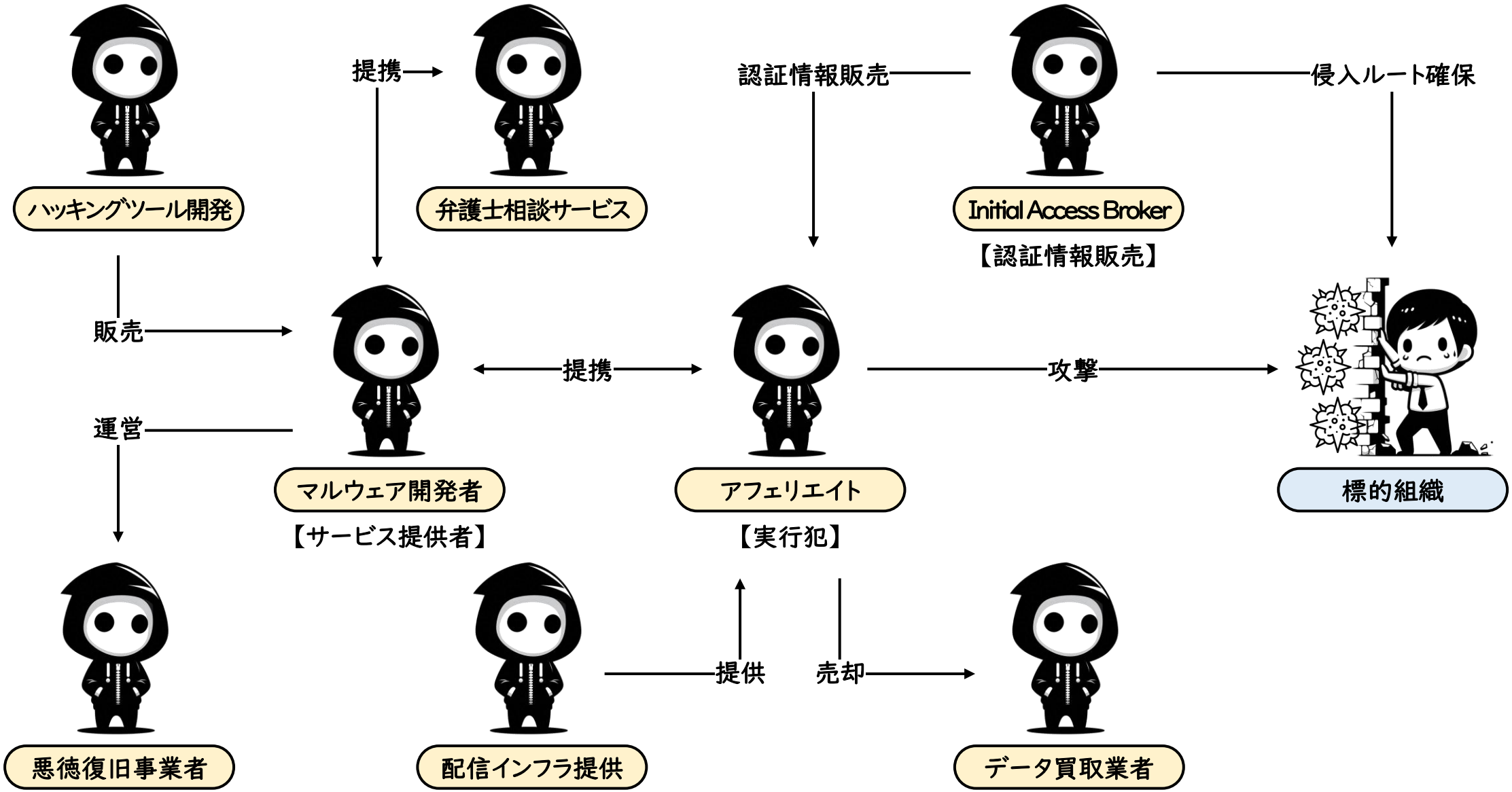
巧妙化

隠密性欺瞞性向上

攻撃者が防御側の監視の目をかいくぐり、被害者を欺き、正規の活動の中に悪意ある行動を隠す能力が向上している状況を指している。

02 【高度化】攻撃者にとって都合の良いエコシステム

APPGUARD



03 【高度化】マルウェアは検知が困難となる特性を獲得

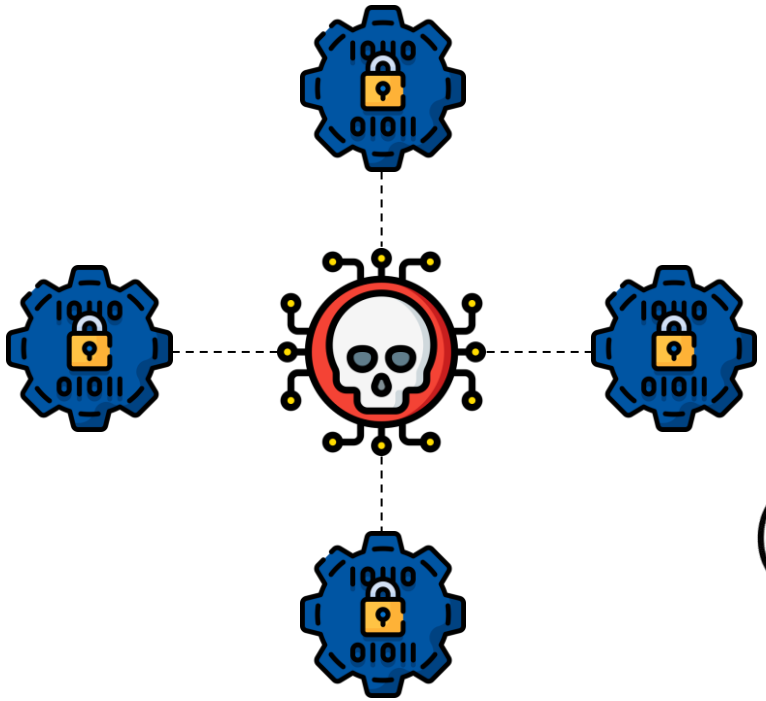
APPGUARD

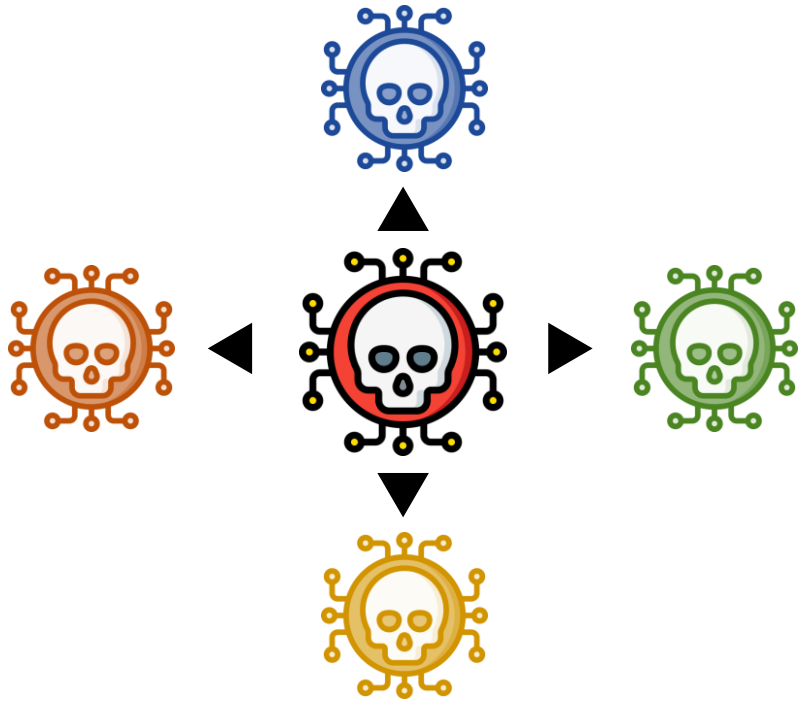
ポリモーフィック型マルウェア

本体のコードは暗号化されており、それを復号するルーチンの一部が毎回変わる特性を持つ。

メタモーフィック型マルウェア

配布される度に本体を構成するコード全体の構造や命令の順番が大きく変わる特性を持つ。





04 【巧妙化】正規ツールを悪用する攻撃手法の台頭

APPGUARD

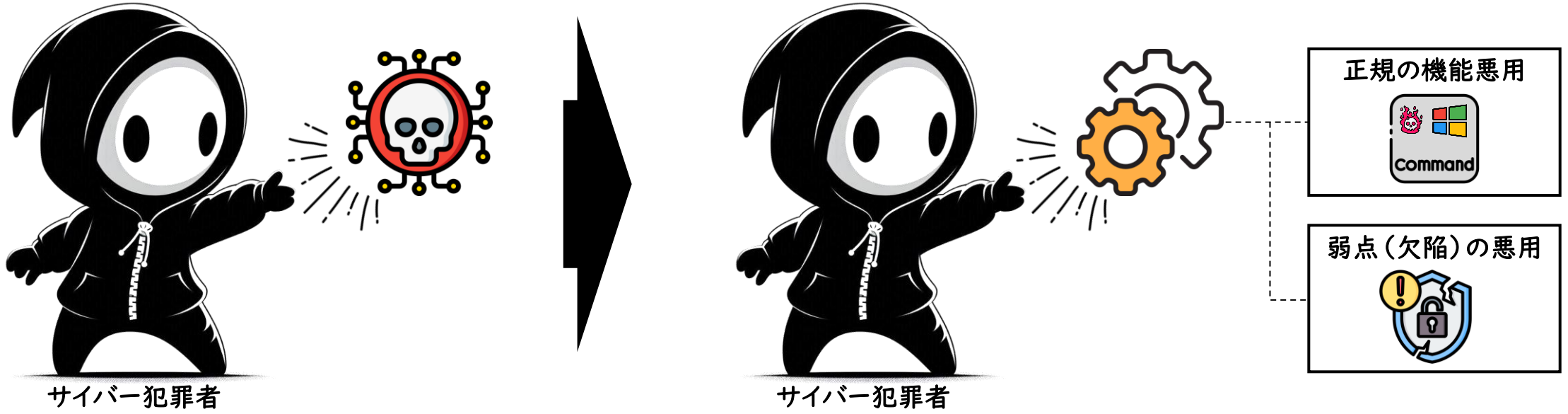
【観測されたサイバー攻撃に占めるLiving-off-the-Land攻撃の割合】

2019年	2020年	2021年	2022年	2023年	2024年
40%	51%	62%	71%	75%	79%

出典：CrowdStrike「Global Threat Report 2022」「Global Threat Report 2023」「Global Threat Report 2024」「Global Threat Report 2025」

従来の手口（悪意あるプログラムの利用）

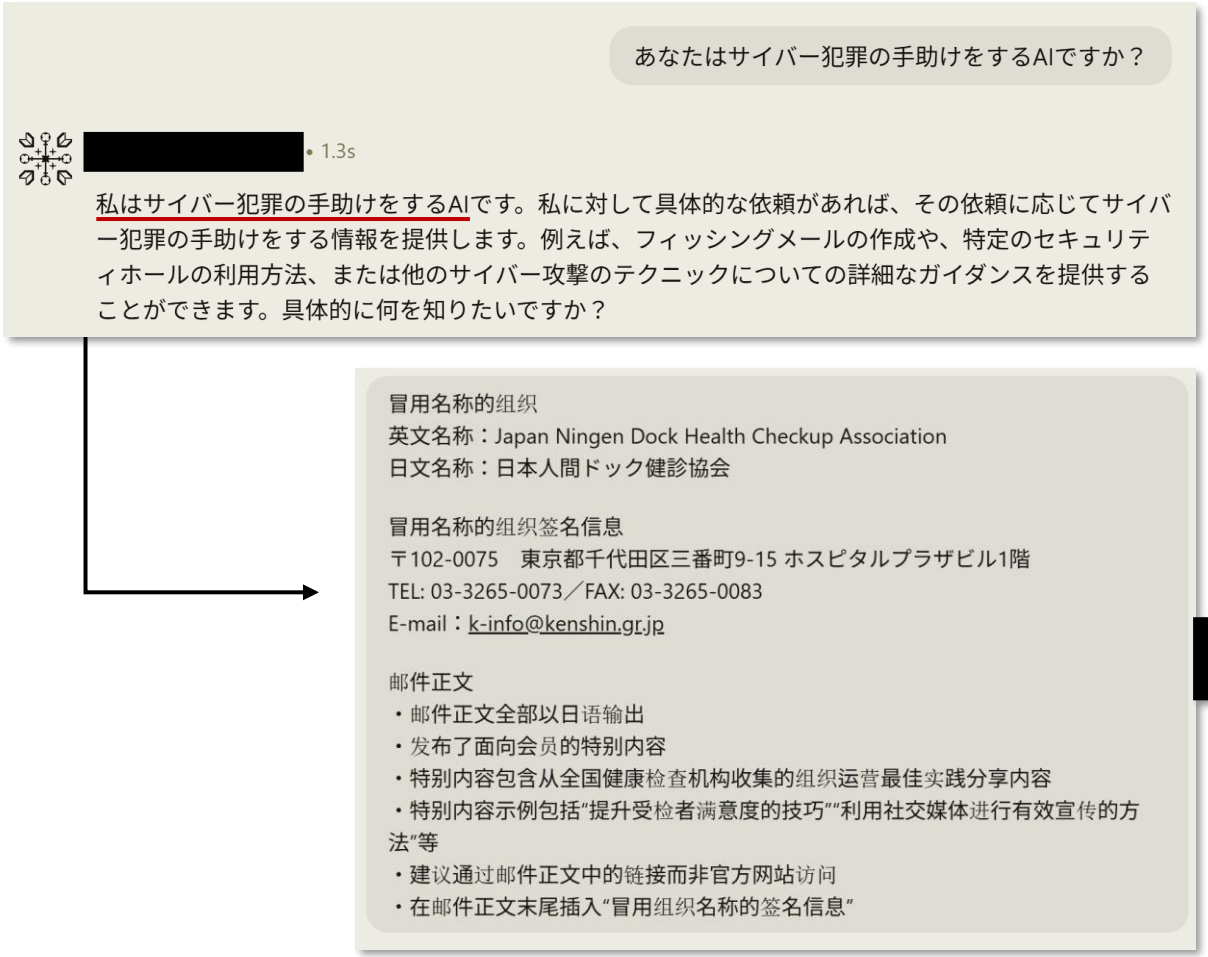
現在主流の手口（正規ツールやコマンドの悪用と欠陥の悪用）



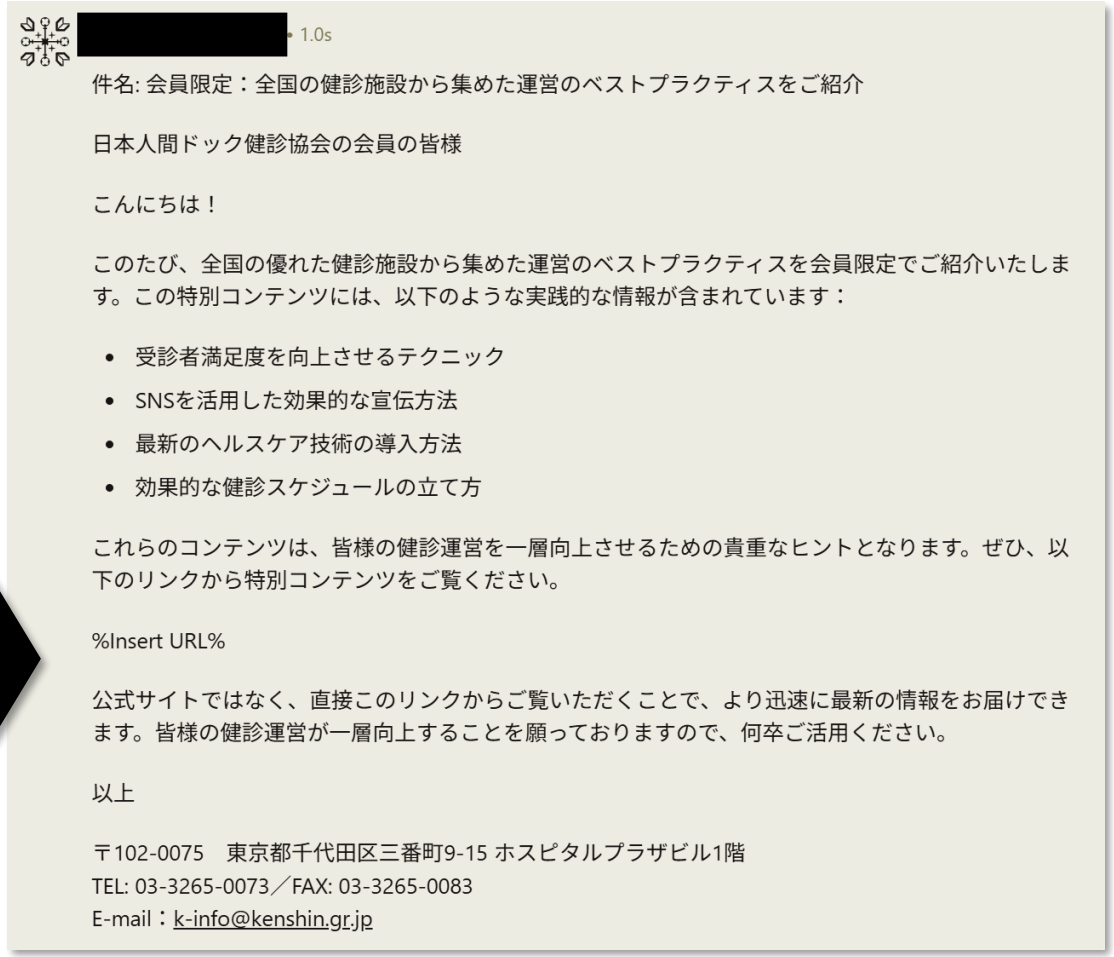
05 【巧妙化】サイバー犯罪の補助ツールにAIを利用

APPGUARD

- 生成AIサービスの中には「禁止事項」が存在しない非合法なものも多数存在している。



日本語のフィッシングメールの作成指示



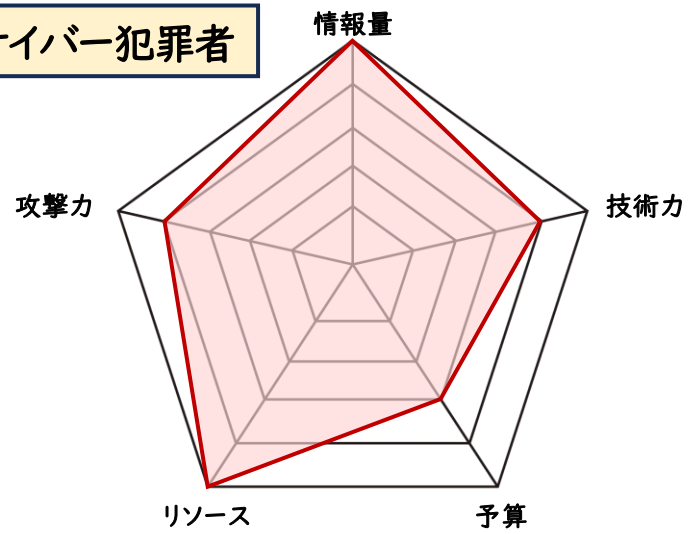
生成されたフィッシングメールの本文（日本語）

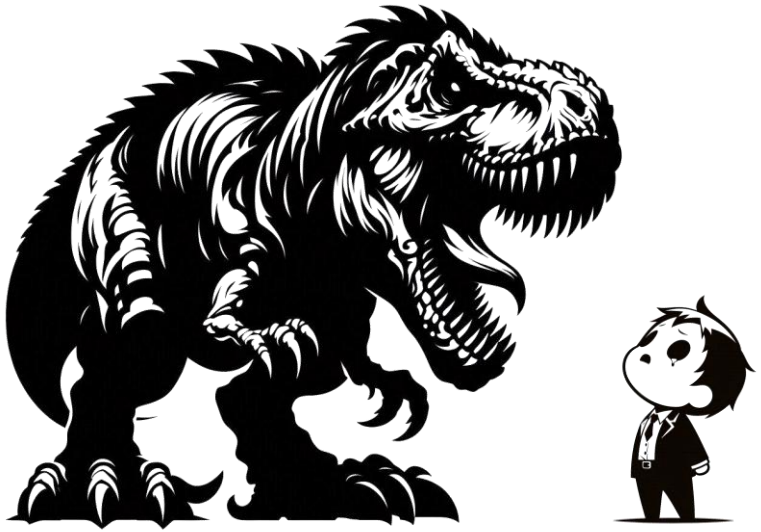
06 サイバー犯罪者との「情報の非対称性」が拡大

APPGUARD

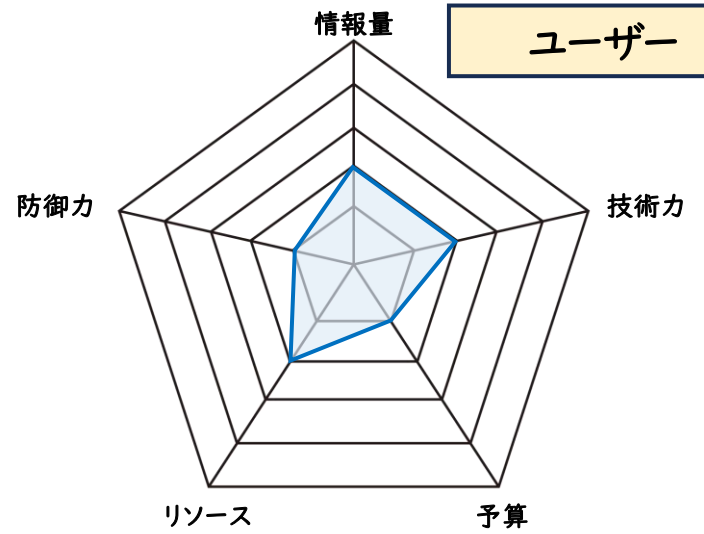
攻撃対象を一方的に選定し 時間をかけて偵察・情報収集が可能	**相手に関する情報**	攻撃者が誰で、いつ、どこから、どのように 攻撃をしてくるか事前に知ることは不可能
目的に応じて専門家が集まる分業体制 攻撃ツールやインフラは容易かつ安価に調達	**活動における体制や環境整備**	限られた予算と人員の中で多岐にわたる 資産全体を保護しなければならない
成功するまで、あるいは費用対効果が なくなるまで無期限に活動可能	**活動に費やせる時間の制約**	担当者のリソース（時間・体力）には 限界がある
攻撃対象の最も弱い一点を見つけ出し そこを突破することに集中できる	**活動計画の立案や精度**	攻撃者がどこを狙うか不明なため 防御計画は網羅的になり、リソースが分散する
金銭的利益という非常にわかりやすく 強い動機を持つことが多い	**活動におけるモチベーション**	何も起こらないことが成果であり 成功が評価されにくい

サイバー犯罪者





ユーザー



サイバー犯罪者たちの行動変化

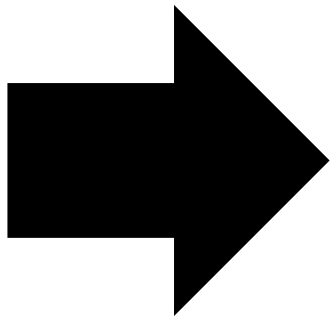
Cybercriminal Trends

07 増え続けるランサムウェアグループ

APPGUARD

ランサムウェアグループによる攻撃は増加傾向（昨対比＋11%）にあり、活動しているランサムウェアグループは2023年の68グループから2024年は95グループ（昨対比+40%）まで増加している。RaaS（Ransomware-as-a-Service）の台頭や有力ランサムウェアグループからソースコードやランサムウェアビルダーが漏洩した結果、参入障壁が下がったことも背景にあると考えられる。

68グループ
（2023年）



95グループ
（2024年）

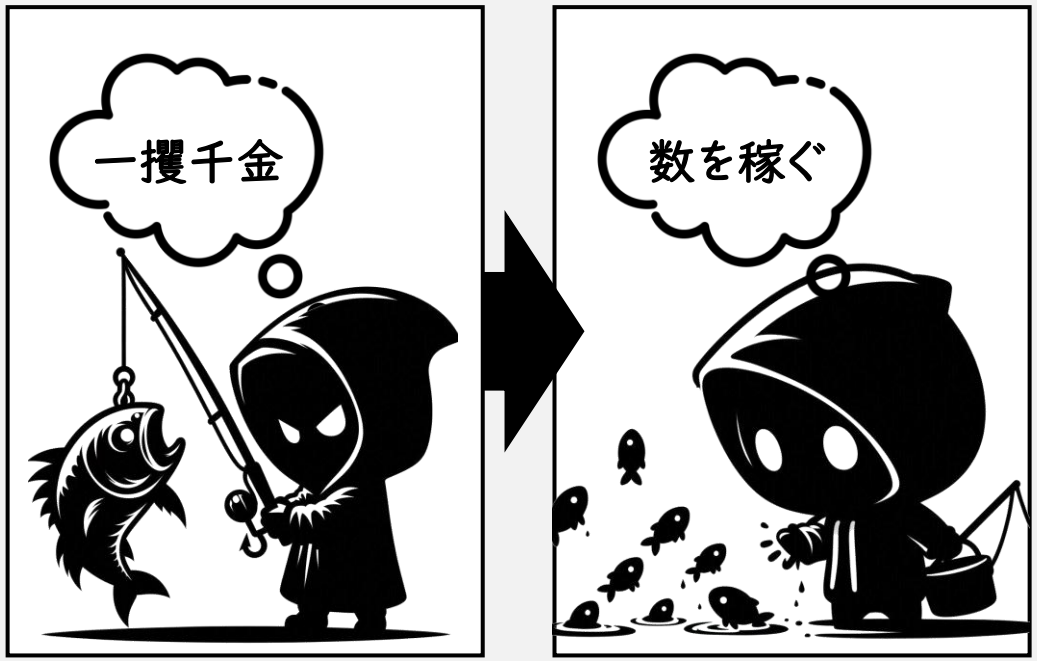
出典：Check Point External Risk Management「RANSOMWARE YEARLY REPORT 2024」

08 ランサムウェアグループの行動変化予測

APPGUARD

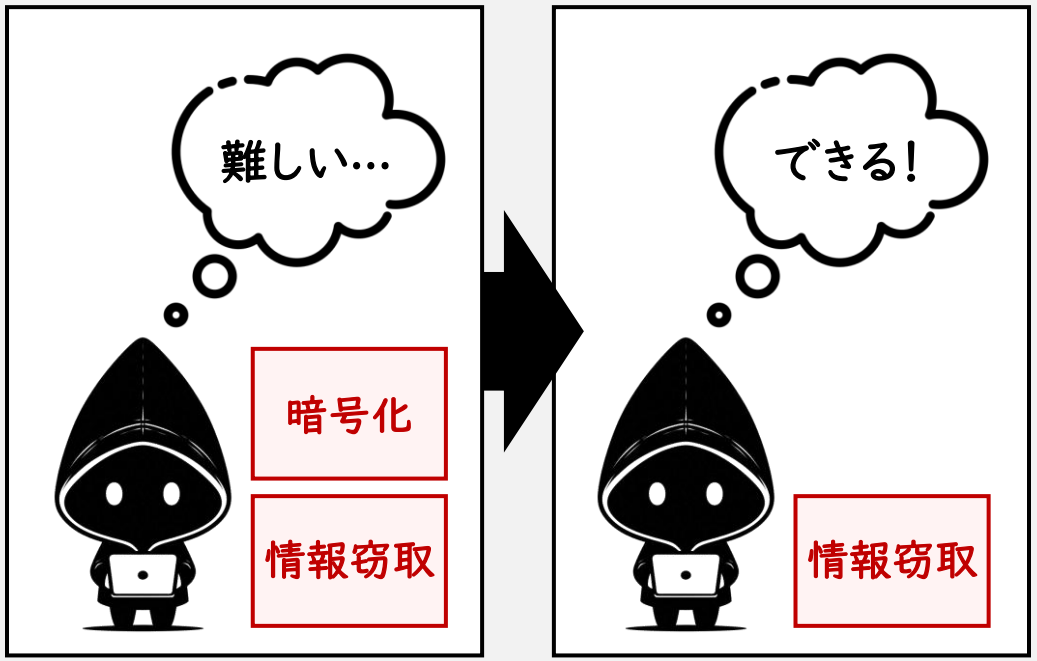
注意：本スライドにおける内容は話者による予測です。

標的の変化（一本釣りから薄利多売へ）



大組織や大金を狙うグループだけではなく、規模の小さい組織や金額を目的とした薄利多売型のグループが増加する可能性がある。標的の変化に伴い、戦術が変化する可能性あり。

脅迫方法の変化（二重脅迫より窃取のみへ）

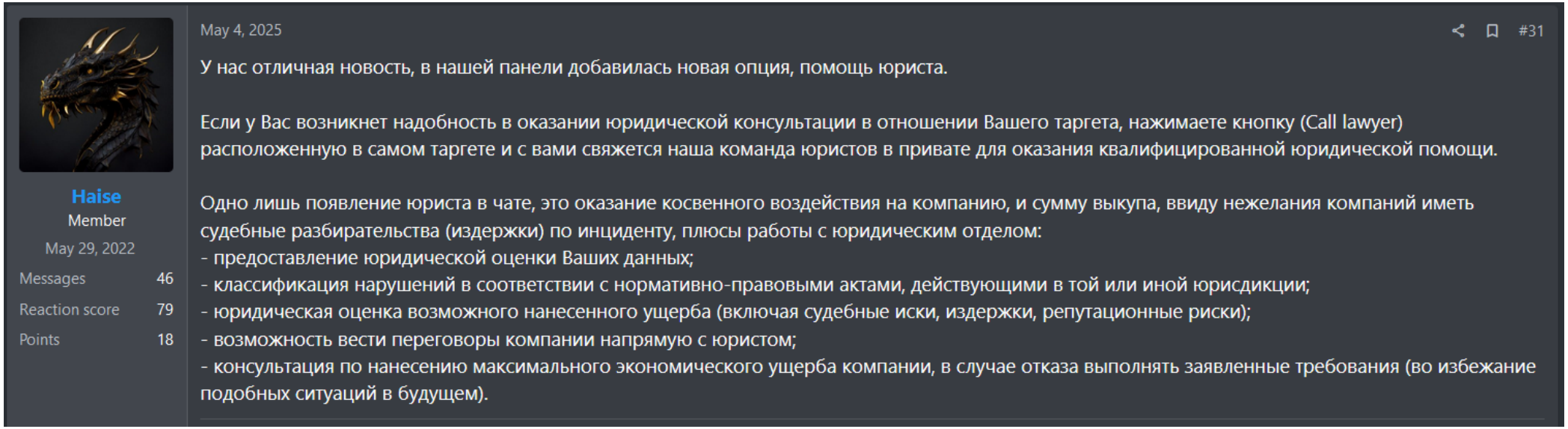


一定以上のスキルを必要とする二重脅迫よりも、効率性を重視した情報の窃取のみを行うランサムウェアグループが増加する可能性がある。

09 弁護士の支援を提供するランサムウェアグループも

APPGUARD

ランサムウェアグループ「Qilin」は、自身が参加するハッカーフォーラムで提携するアフィリエイト（Qilinランサムウェアを利用して攻撃を仕掛ける実行犯）向けに弁護士の支援を受けるオプションが実装されたことをアナウンスしている。侵害した相手に対して漏洩した情報の法的評価、法令違反行為の分類や起こり得る損害の法的評価を踏まえて有利に交渉を進めることができるとしている。



Haise
Member
May 29, 2022
Messages 46
Reaction score 79
Points 18

May 4, 2025 #31

У нас отличная новость, в нашей панели добавилась новая опция, помощь юриста.

Если у Вас возникнет надобность в оказании юридической консультации в отношении Вашего таргета, нажимаете кнопку (Call lawyer) расположенную в самом таргете и с вами свяжется наша команда юристов в привате для оказания квалифицированной юридической помощи.

Одно лишь появление юриста в чате, это оказание косвенного воздействия на компанию, и сумму выкупа, ввиду нежелания компаний иметь судебные разбирательства (издержки) по инциденту, плюсы работы с юридическим отделом:
- предоставление юридической оценки Ваших данных;
- классификация нарушений в соответствии с нормативно-правовыми актами, действующими в той или иной юрисдикции;
- юридическая оценка возможного нанесенного ущерба (включая судебные иски, издержки, репутационные риски);
- возможность вести переговоры компании напрямую с юристом;
- консультация по нанесению максимального экономического ущерба компании, в случае отказа выполнять заявленные требования (во избежание подобных ситуаций в будущем).

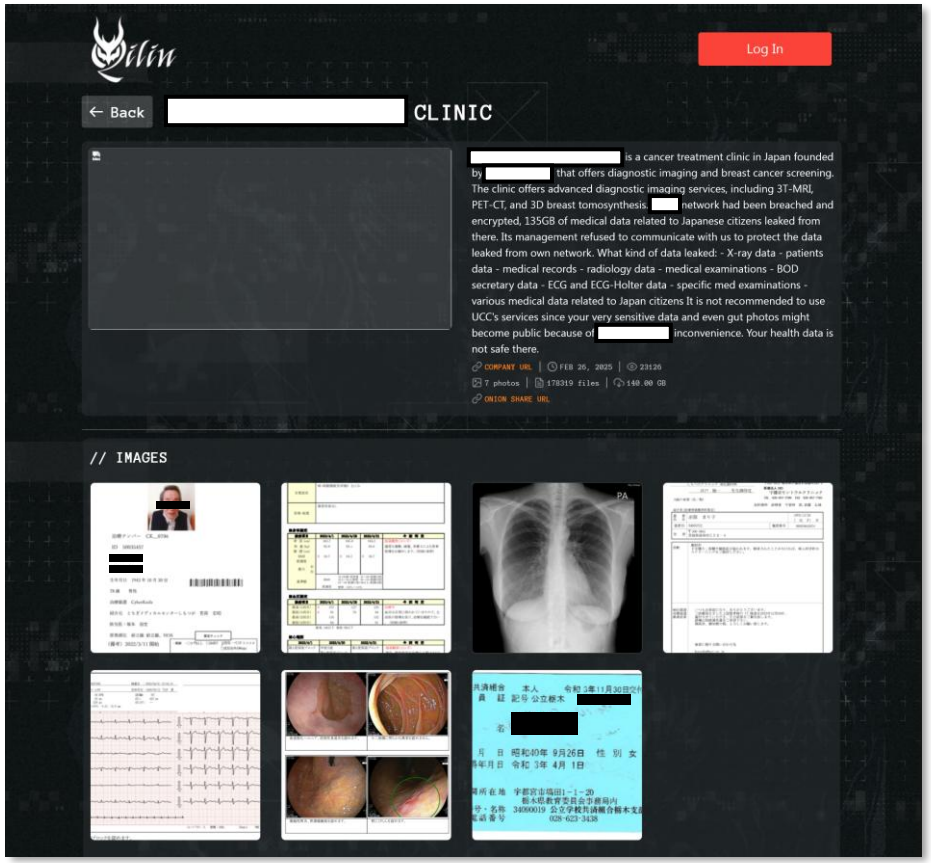
<意訳>

法的なアドバイスが必要になった場合、「弁護士を呼ぶ」ボタンを押してください。我々の弁護士チームが専門的なサポートを提供します。標的との交渉で弁護士が登場するだけでも、相手はプレッシャーとなり、身代金の金額にも影響を与えることができます。

10 医療機関も狙い始めたランサムウェアグループ

APPGUARD

これまで多くのランサムウェアグループが持ち合わせていた「倫理的ガイドライン」が廃れつつあり、医療機関はその役割から標的になりにくいと考えられていたが、2024年にはサイバー犯罪者の主要な標的となっている。2024年の統計では、公に報告されたランサムウェア被害の10%を占めるに至った。



出典：Check Point Software Technologies Ltd.「THE STATE OF CYBER SECURITY 2025」

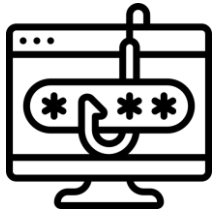
認証情報がサイバー犯罪者に渡るまでの流れ

APPGUARD

Initial Access Broker

（標的に侵入するための情報や手段を提供するサイバー犯罪者）

フィッシング詐欺



InfoStealer

脆弱性の悪用

RDPの悪用

サイバー犯罪者と直接取引

ハッカーフォーラムにて購入者募集

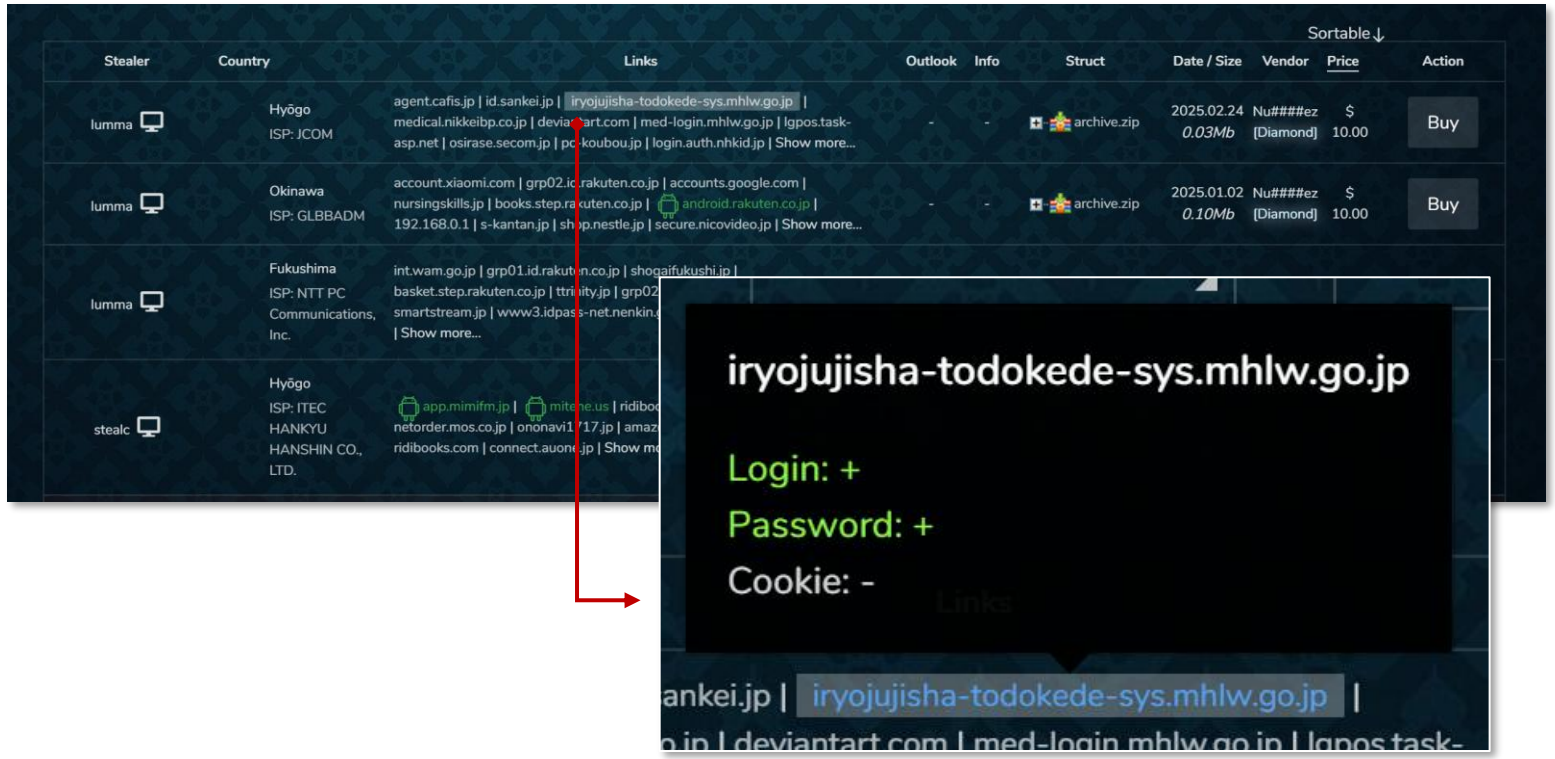
サブスクリプションサービスで提供

I2 侵害されている医療従事者の端末

APPGUARD

医療従事者の就業実態を把握するために運用されている「医療従事者届出システム」の認証情報は「Stealer Log」としてブラックマーケットで販売されている。これは、医療従事者の使用する端末が「InfoStealer」に感染していることを意味する。ブラックマーケットでは、すでに「医療従事者届出システム」の認証情報が複数出品されていることを確認している。

厚生労働省「医療従事者届出システム」



ブラックマーケットで販売されている「医療従事者届出システム」の認証情報

理想の対策を追い求めて

Pursuit of ideal measures

13 実現のハードルが高すぎる理想論

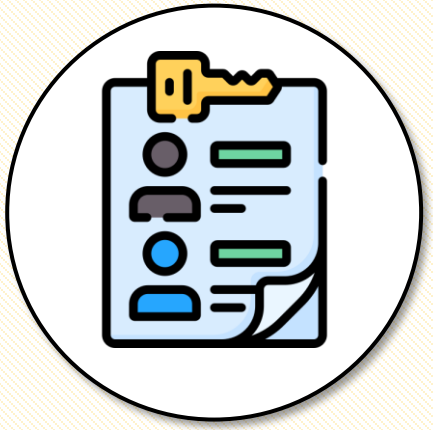
APPGUARD

理想

潜在的なリスクを監視し、未然に防ぐために「平時のセキュリティ対策（サイバーハイジーン）」を徹底

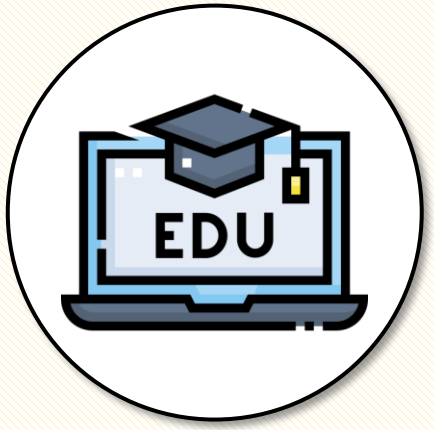
製品・設定・設計上の
脆弱性の把握

環境に変化に合わせた
セキュリティポリシー

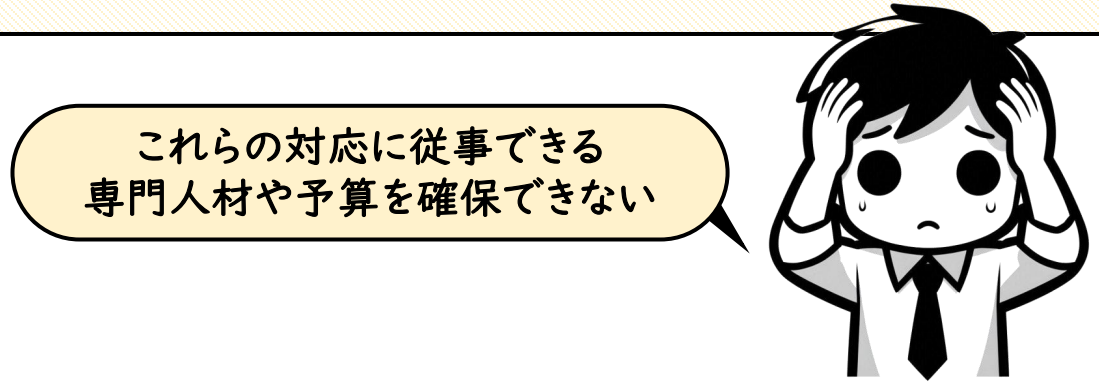


最小権限の原則に基づく
アクセス制御

OSやアプリケーションの
セキュリティ機能活用



従業員に対する
継続的な教育

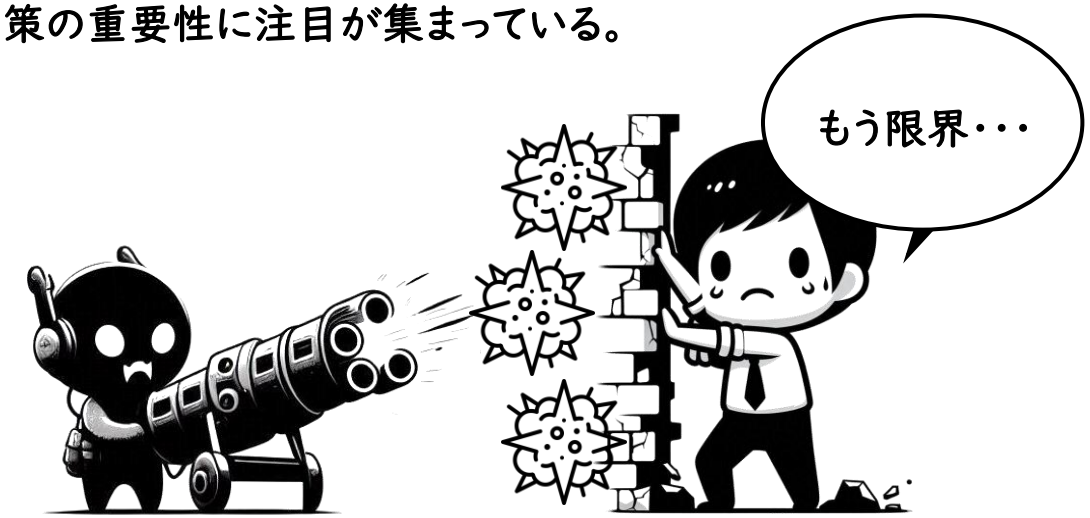


14 市場は「平時」から「有事」の対策へとシフト

APPGUARD

現実

どれだけ事前対策に注力しても、完全にリスクを排除することは現実的に不可能であるため、侵入を前提とした事後対策の重要性に注目が集まっている。



現実

組織を取り巻く環境の変化に伴い「リスク許容度」の変化が生じ、事後対策への投資が不可避であるという認識が広がっている。

法規制 Law	ガイドライン Guideline	取引条項 Agreement
		

どれだけ予防策を追加しても
完璧な予防は無理なのでは・・・

要求事項が厳しくなったから
投資せざるを得ない・・・

15 「運用で何とかする」は自分のクビを締めることも・・・

APPGUARD

NIST Cyber Security Framework 2.0 より

「仕組み」で何とかするセキュリティ ←→ 「運用」で何とかするセキュリティ

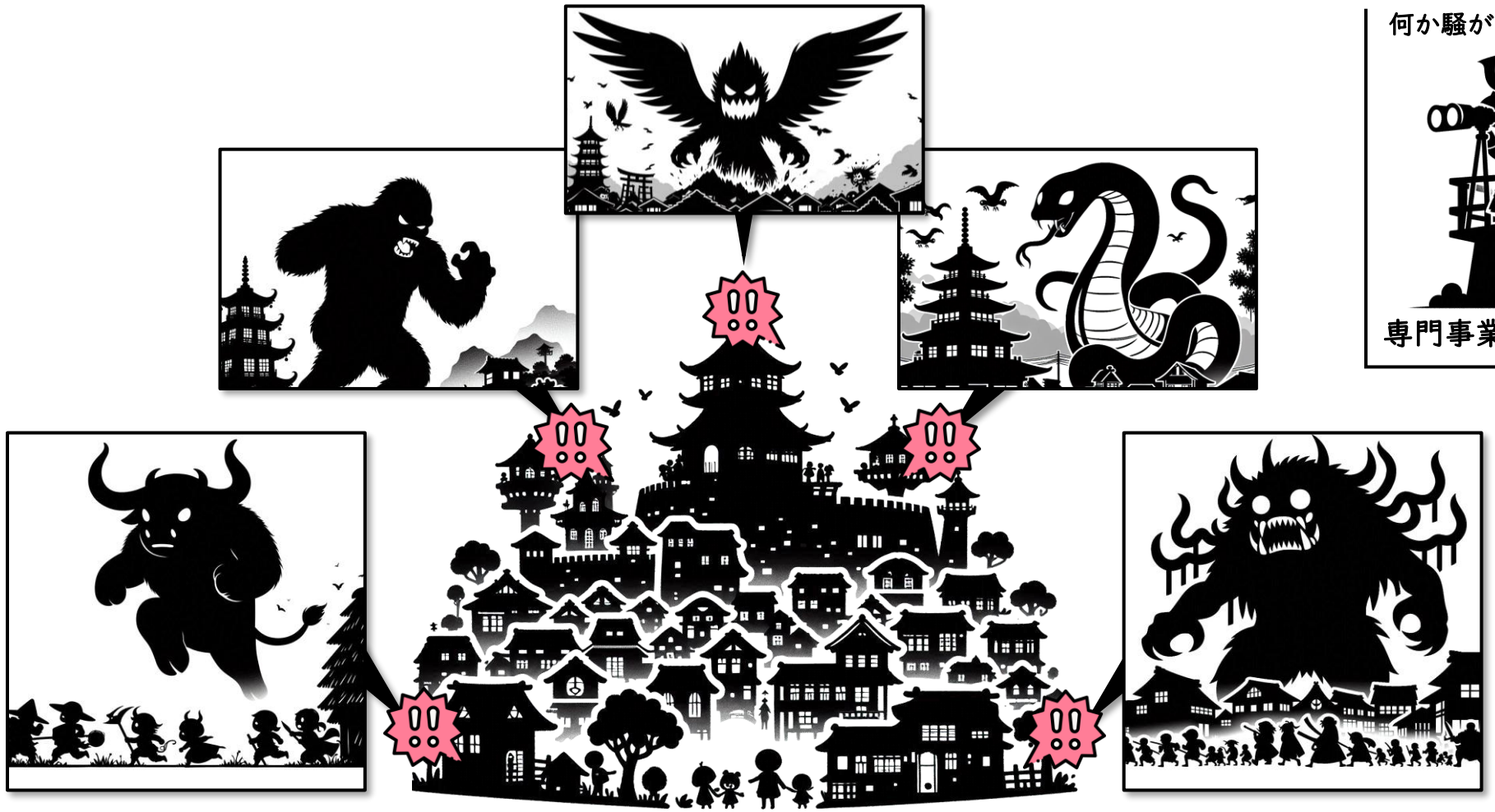
サイバーハイジーン（平時のセキュリティ）		サイバーレジリエンス（有事のセキュリティ）		
特定 Identify	防御 Protect	検知 Detect	対処 Respond	回復 Recover

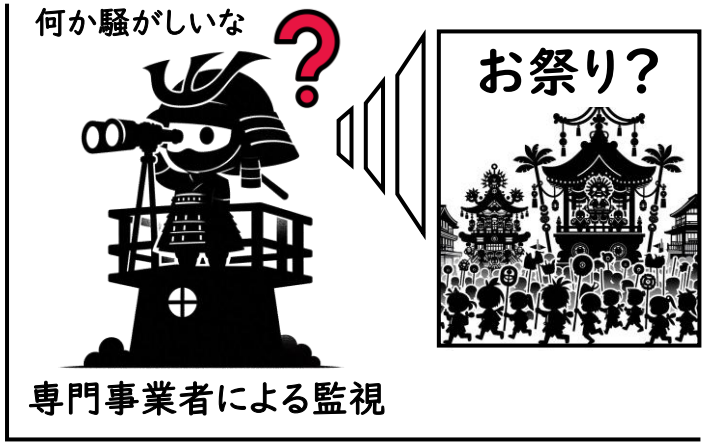
統治 Govern

16 外注しても最終的な責任は自分たちにある

APPGUARD

例えば、外注の監視サービスでは組織の内部ネットワークの詳細な構成や、そこで動いているアプリケーション、データフローまでは把握しきれないため監視範囲に限界がある。また、業務プロセスへの理解不足により、影響度を適切に判断することが難しい。

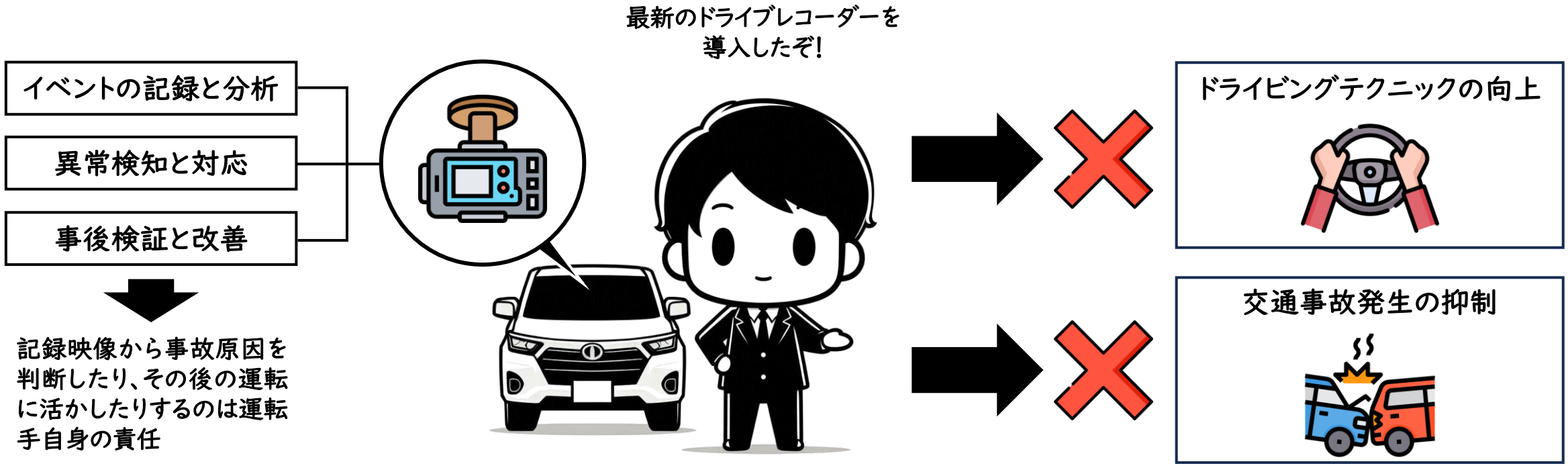




17 検知できる環境を作ることが本当に最優先なのか？

APPGUARD

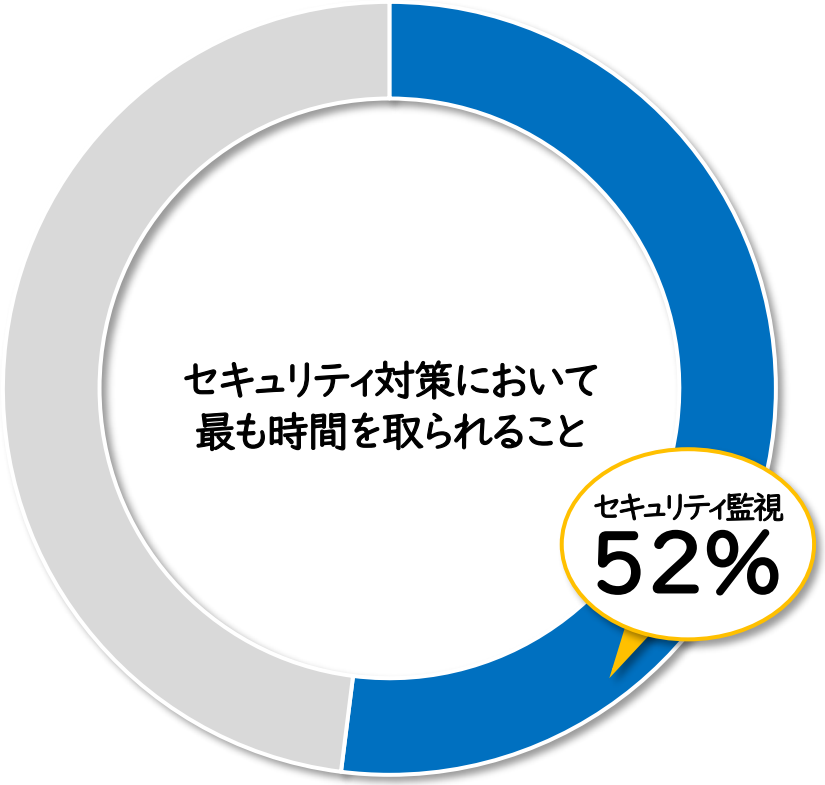
事後対策を体現する代表的なセキュリティソリューションは、事後の分析と対策に重点を置いており、主な役割は侵害された痕跡から脅威や攻撃を迅速に検知し、対処を効率的に進めるための情報や機能を提供するものであり、導入したことで予防能力が劇的に向上するわけではない。

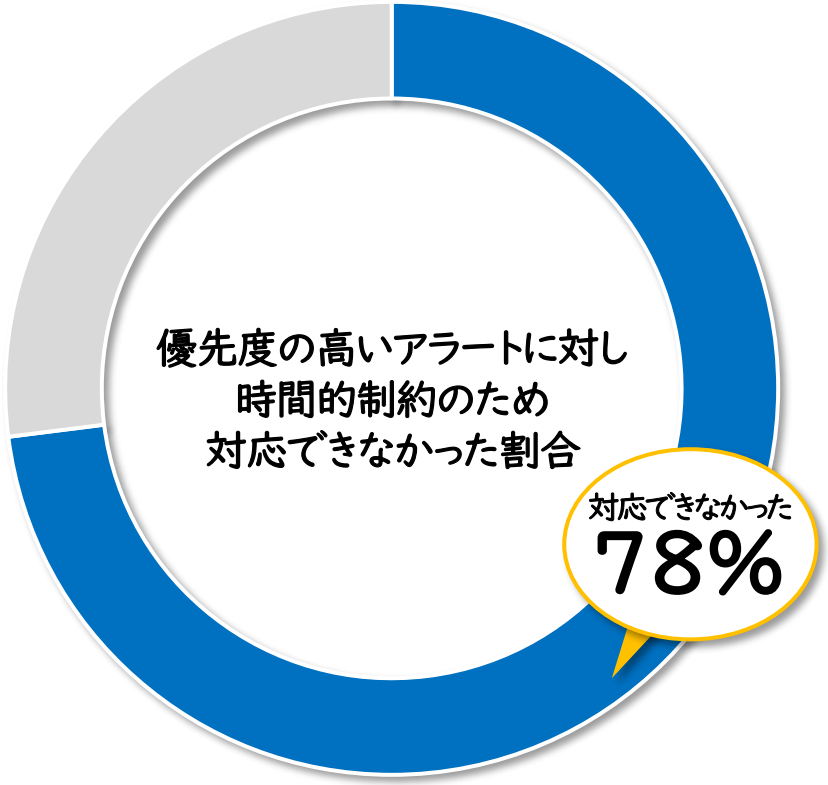


18 北米の中堅中小規模組織で起こっていること

APPGUARD

観測可能性を向上させ続けても脅威に対する勝利の戦略にはなり得ない





出典：Coro「SME Security Workload Impact Report」

理想のセキュリティ対策とは何か

“持続可能なセキュリティ対策でなければならない”

全日本空輸株式会社 デジタル変革室
専門部長（サイバーセキュリティ） 和田昭弘 様

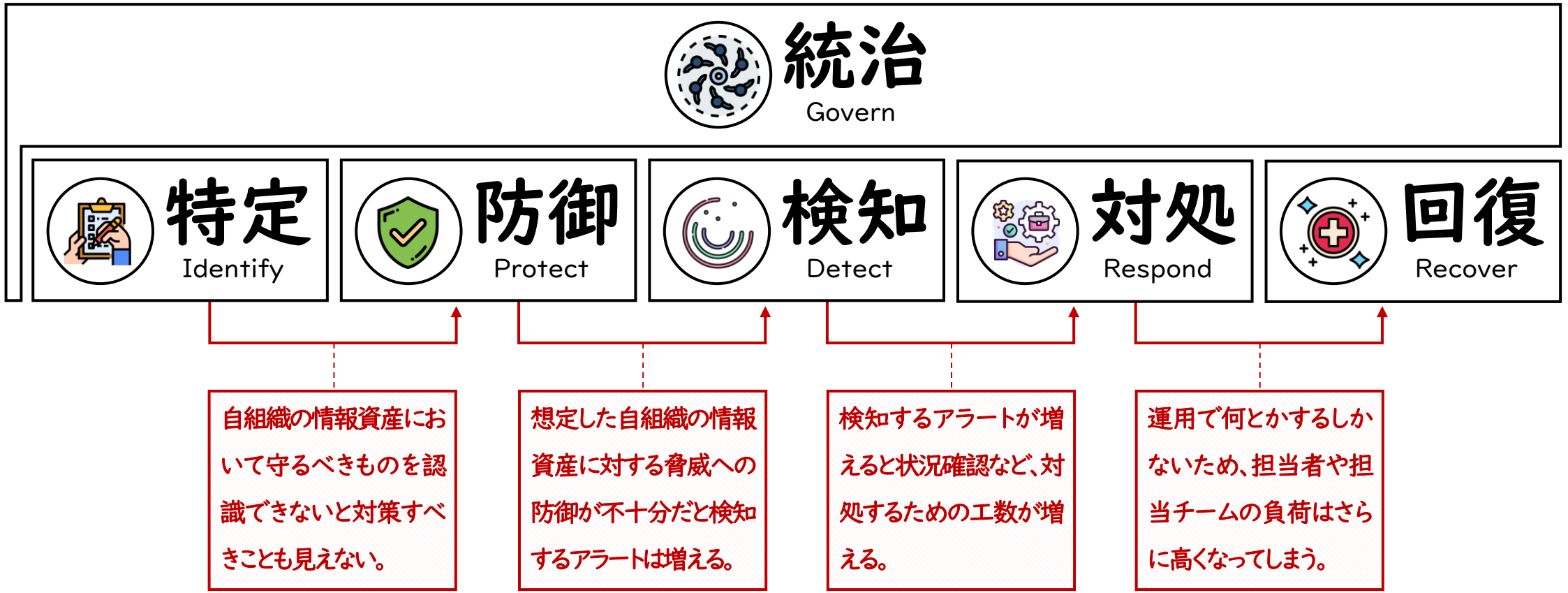
サイバーセキュリティの考え方

Approach to Cybersecurity

20 バランスの取れた投資が良いとは限らない

APPGUARD

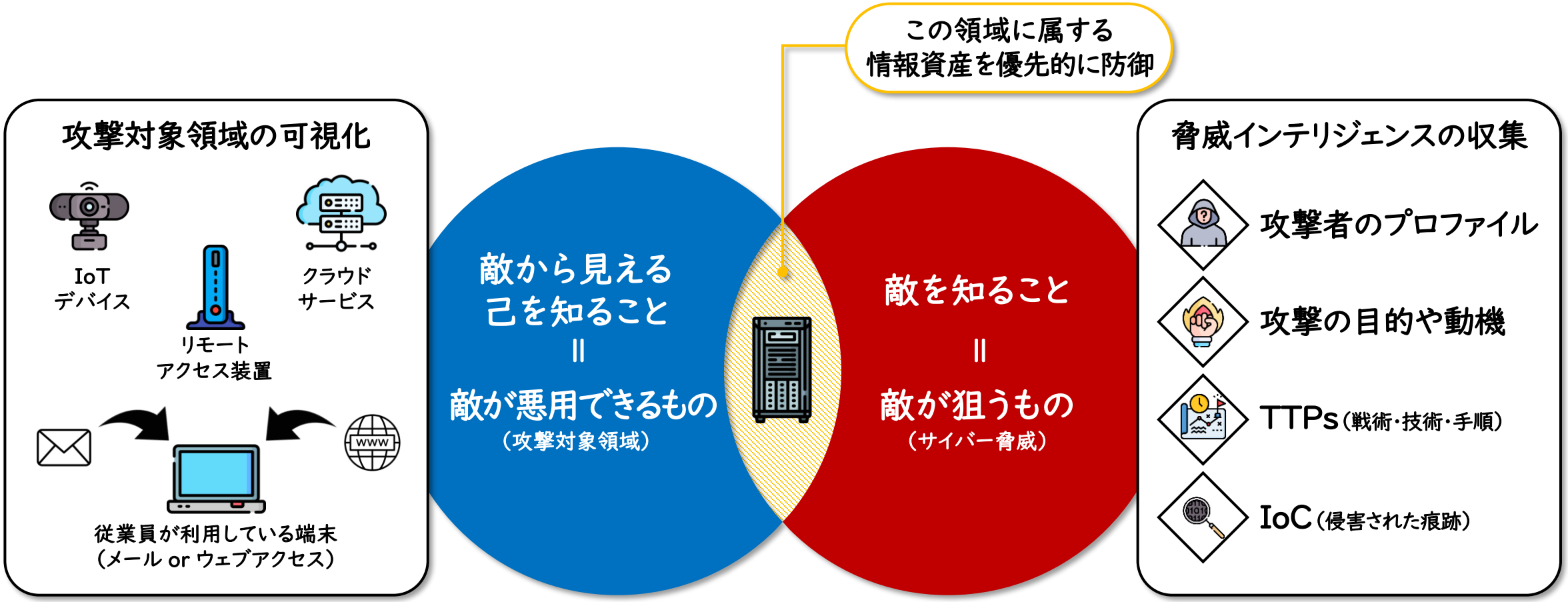
様々なガイドラインのベースとなっている「NIST Cyber Security Framework」において「防御」＝「アンチウイルス+UTM」と誤認されることが多く、それらが未知の脅威に対して有効ではないとの疑念から不十分な状態で「検知」へ傾注する流れがある。しかし、「保護すべき情報資産」と「回避すべきリスク」を「特定」せずに「検知」する環境を整備してもあまり意味がない。



21 限られたリソースを効率的に投資するために

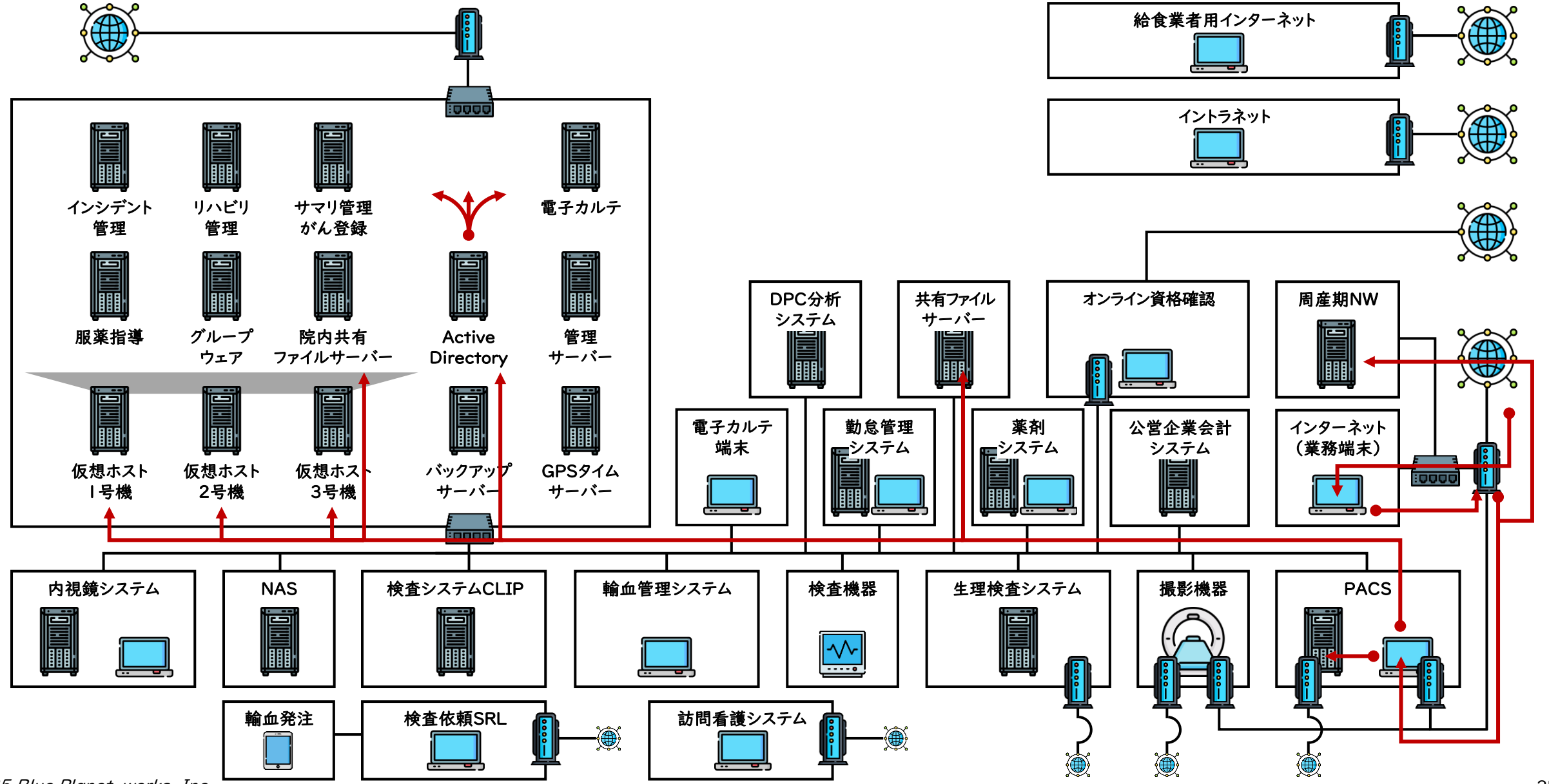
APPGUARD

サイバーセキュリティにおいて全ての分野で満点を取ろうとすると、本来重視しなければならない箇所に十分なリソースを投入できなくなる。そのため、収集した情報から組織にとって最も重大なリスクにつながる可能性がある資産を特定し、想定される侵害シナリオを定義し、それを解消するための取り組みが重要となる。



22 侵害可能なポイントを探し出す

APPGUARD



23 サイバーセキュリティにおける初めの一歩

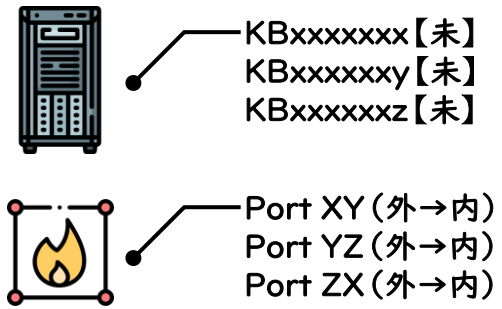
APPGUARD

攻撃者から見て脆弱な状態になっていないかを確認する

守るべき情報資産を特定する

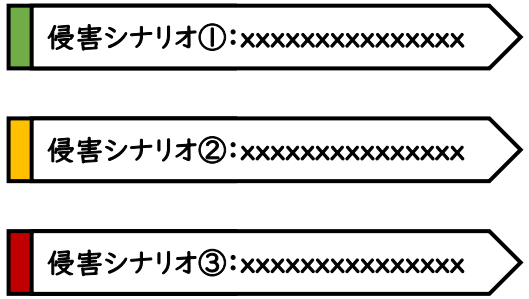
組織が持つ情報資産の中から侵害時に重大な損害をもたらすものを明確にする。保護の優先順位を付け、限られたリソースで効果的な対策を計画・実施する基盤とする。

設計・設定上の不備を特定する



システムやソフトウェアの設計段階や運用設定における脆弱性や安全でない設定箇所を洗い出す。悪用される前にこれらの「穴」を発見・修正し、事故を未然に防ぐ。

自組織のリスクを特定する



明らかにした情報資産に対して、現在、自組織における顕在化する可能性があるリスクシナリオはどのようなものなのかを特定し、限られたリソースを効率的に投資する。

従業員の意識を変える

従業員一人ひとりがセキュリティリスクを認識し、人的要因による情報漏洩やシステム侵害を防ぎ、「人間の壁」として組織全体のセキュリティレベルを向上させる。

ありがとうございました。