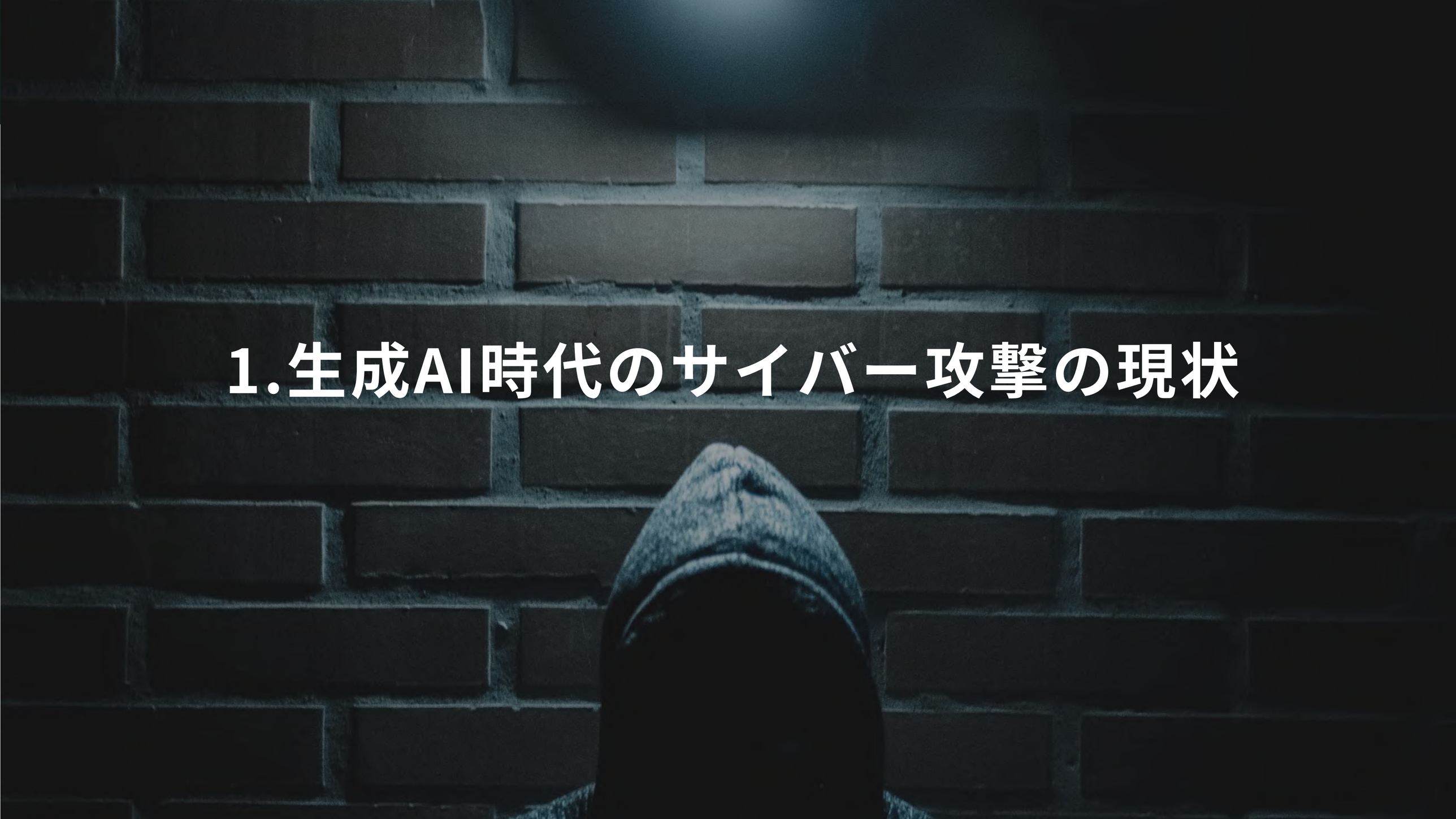
生成AI時代の
サイバー攻撃対策ハンドブック

株式会社ヤグラ

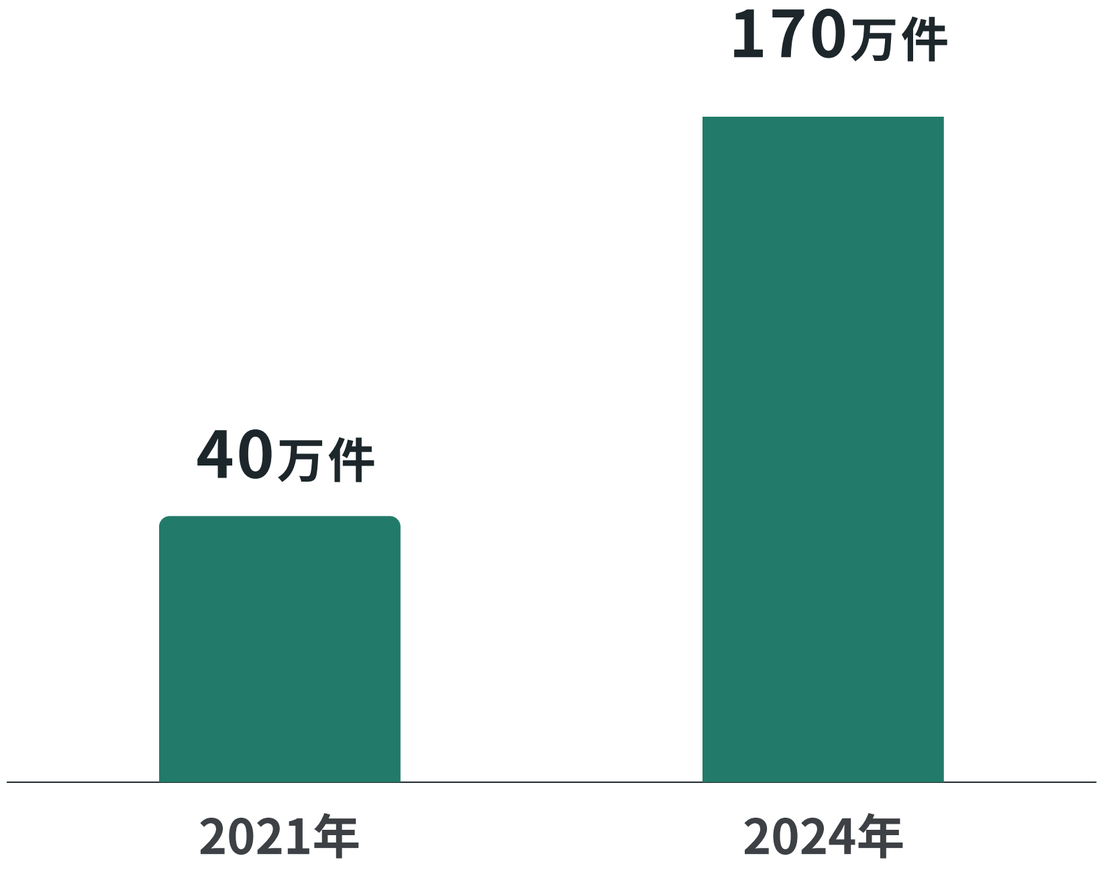
Yagura



1.生成AI時代のサイバー攻撃の現状

現状

生成AIがサイバー攻撃を量産する時代へ



※警察庁が公表した令和６年版統計

生成AI登場後の
フィッシング攻撃数

約4倍

現状

過去にない新しいサイバー攻撃の手口が増加

香港では、ディープフェイクCFOがZoom会議に現れ送金指示をすることで約40億円を詐取

香港 ディープフェイク送金事件
被害額

約40億円

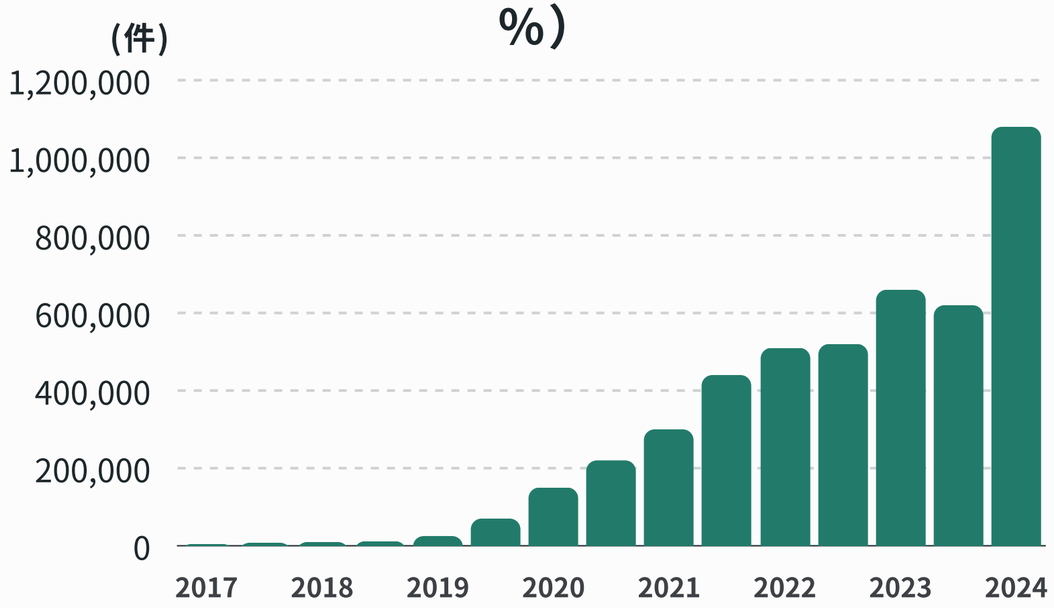
Yagura

現状

数値で見るサイバー攻撃の実態

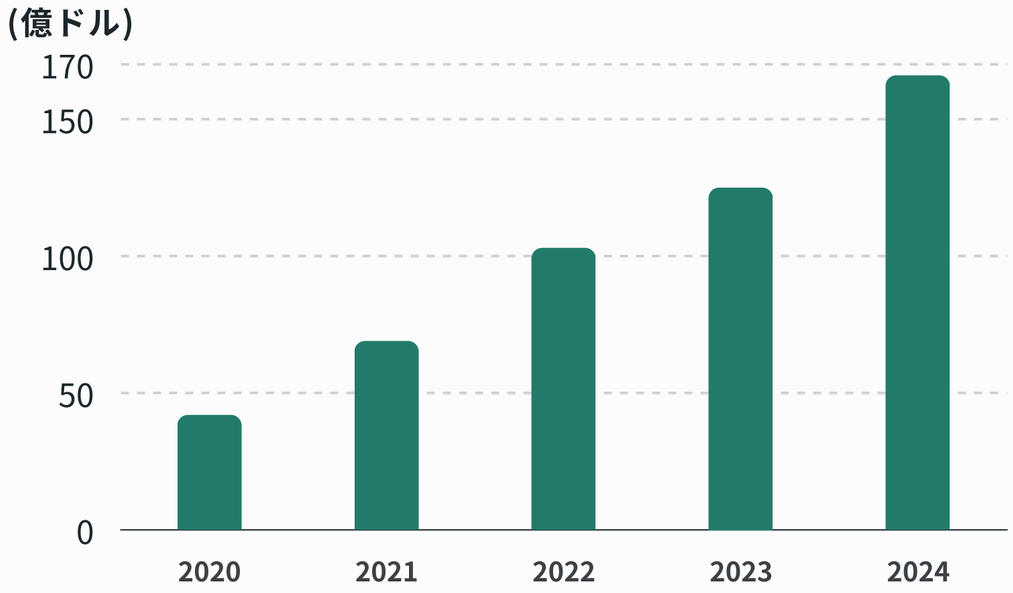
攻撃者が生成AIを活用する時代となり、サイバー攻撃数が飛躍的に増えている。

フィッシング攻撃は前年比 52 万件増（＋44％）



（出典）フィッシング対策協議会、フィッシング報告状況（月次報告書）より

サイバー犯罪の被害額は166億ドルに到達



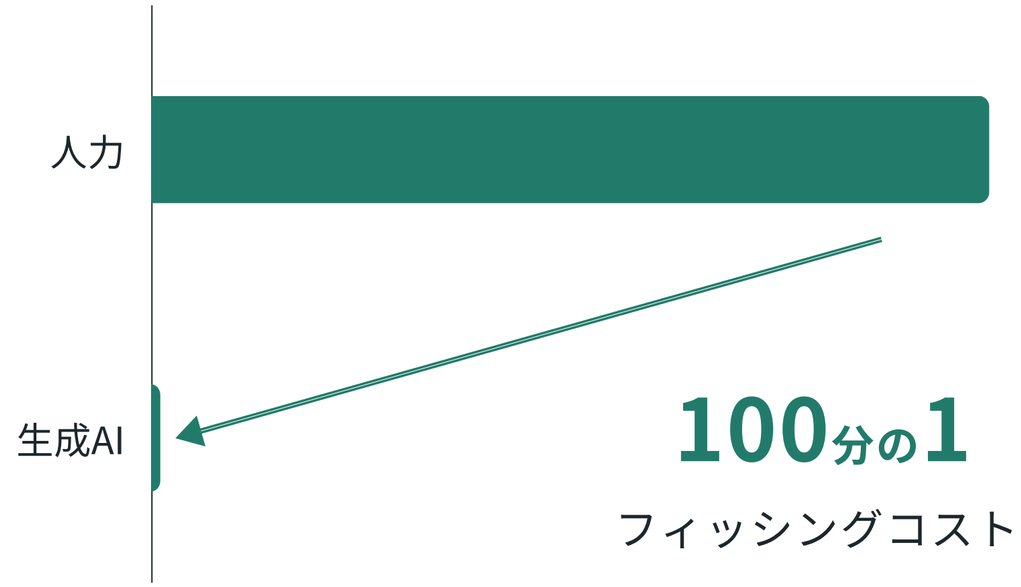
（出典）FBI「Internet Crime Report 2024」を基に IPA が作成

サイバー攻撃における最新の動向

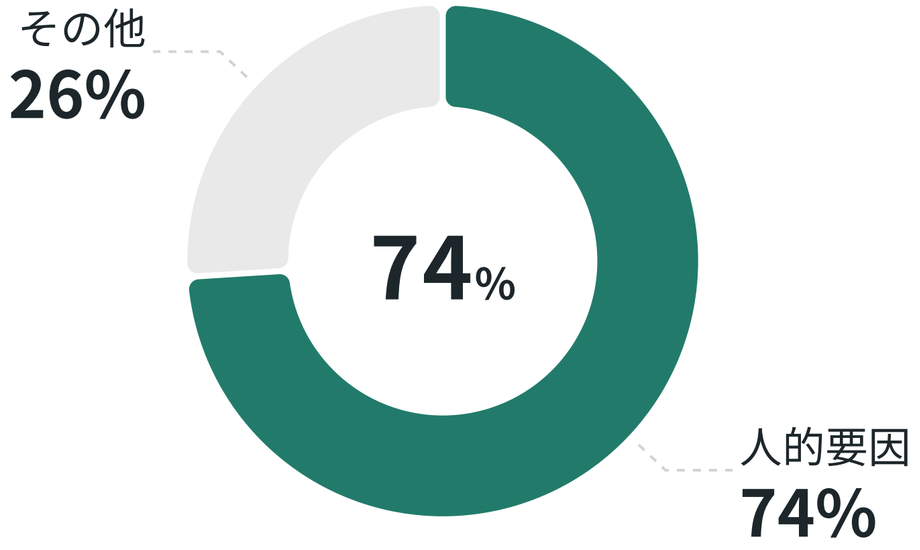
技術防御は必要条件――突破点は“人”

最新のエンドポイントセキュリティがあるからこそ、攻撃者は標的を「人」へと変更し大量の攻撃を展開。

生成AIによるフィッシングコストは100分の1に



サイバー事故は人的要因が過半数を占める



（出典） Verizon DBIR 2024

サイバー攻撃における最新の動向

生成AI時代における攻撃手法の劇的な変化

これまでの攻撃

- □ 一斉送信・低頻度（手作業中心）
- □ **メール中心**の単一チャネル
- □ 文面の粗さ・不自然さが目立つ
- □ なりすましは**テキスト**主体（画像/音声なし）

生成AI時代の攻撃

- □ **1対1で最適化**（役職/業務/公開情報ベース）
- □ マルチチャネル（メール / **SMS / 電話 / チャット / SNS**）
- □ 大量・高速・自動（AI Agentで24時間）
- □ **音声・画像・動画のディープフェイク**

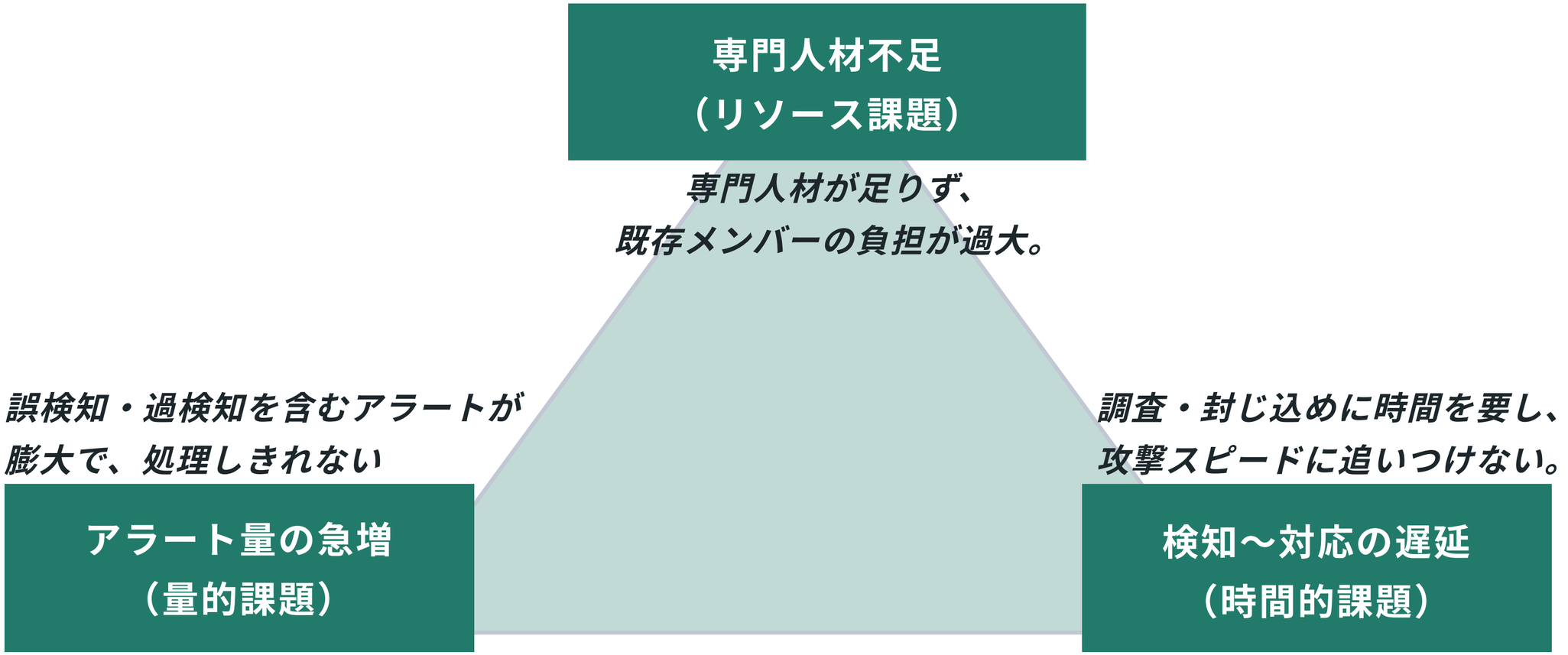
従来の年1回eラーニング＋メール模擬訓練ではギャップを埋められず
ヒューマンファイアウォールが決壊

Yagura

2.生成AI時代に求められる防御体制

課題：攻撃が効率化する一方で、防御側のリソース不足が顕著

攻撃側に対して、防御側における生成AIの活用が遅れる中で、セキュリティ部署にて3大課題が発生



生成AI時代のサイバー攻撃に対抗するために

株式会社ヤグラは生成AI時代のサイバーディフェンスには、以下3つが重要と考えております

- 時代の変化に伴って変化する新しい攻撃を、模擬訓練/スコアリング/教育に取り入れる
- 最新の攻撃にも対応した訓練を、少ない人手で効率的に運用する
- 人的防御だけでなく、フィッシングサイトの撲滅やシステム上の脆弱性も排除する

生成AI時代に求められる防御体制

AIエージェントの活用が必須の時代に

AIエージェントを前提としたセキュリティ体制を構築することによって、コスト削減とセキュリティ強化を同時に実現可能。もはや防御側も生成AIなしでは攻撃を防ぎきれない時代が到来。

- 人手中心の開発・監視・対応
- 高コストなシステム / 委託料
- システム運用者への属人化

セキュリティ
AIエージェント
前提の体制へ

- **AIによる開発・監視・対応**
- **運用コストを大幅削減**
- **属人化しない仕組みづくり**

Yagura

3.セキュリティAIエージェントカンパニー
株式会社ヤグラについて

ヤグラについて

セキュリティAIエージェントカンパニー 株式会社ヤグラ

東大出身のエンジニアメンバーを中心に
セキュリティAIエージェントの研究開発と運用支援を行っています。

セキュリティAIエージェントの研究開発

セキュリティエンジニア集団が
AIエージェントを研究開発
（通年実施）

セキュリティAIエージェント運用における協業を実施

実運用に向けて、
顧客先で弊社エンジニアが高速検証
（3ヶ月〜半年）

コスト削減効果測定し実ソリューション化

コスト削減効果を測定し、
実運用可能な水準に
ソリューション化（半年〜）

事例：山陰合同銀行様 ごうぎん

標的型訓練エージェントの研究開発結果をもとに、リスクある個人に対して被害可能性の高いシミュレーションを自動で運用し、パーソナライズされたガイドを配信することで、効率化を実現

Yagura

ヤグラについて

生成AI時代の防御側に必要なあらゆる対応をAIエージェントで推進します

コスト削減したい内容	AIエージェントでできること
脆弱性診断	脆弱性診断ペネトレーションテストをエージェントで補完し、他社よりも安価に提供
セキュリティリテラシー	標的型訓練を自動配信化し、リスクの高い個人を特定したら、個別指導を自動化
SOC	アラートの分類などをカスタムし、SOC担当者のアラート疲弊を軽減
インシデントレスポンス	攻撃検知後の初動対応フローを自動化し、被害拡大を防止
コンプライアンス監査	内部統制や法令遵守の自動チェックや書類の自動生成を実現
ブランド保護	フィッシングサイトや偽アカウントの検出から削除までを自動化

Yagura

標的型訓練エージェント：ヤグラAIトレーナー

ヤグラ AIトレーナーはマルチチャネルの攻撃をシミュレーションし従業員のセキュリティリスクを大幅に減らします。まずは従業員の教育から防御の第一歩を踏み出しましょう。

生成AI攻撃の
シミュレーション

→

スコアリングによる
従業員リスクの可視化

→

教育コンテンツを
AI生成・配信

ヤグラについて

ご相談お待ちしております

スピード感のあるチームで、貴社のAI時代のサイバーセキュリティ体制構築をお手伝いします。お気軽にお問い合わせください。

まずは会社詳細資料をもらう

代表取締役 CEO　迎健太

東京大学経済学部卒。在学中に株式会社VideoStep（旧LAMILA）を設立し、製造業向け育成DX事業を立ち上げ、株式会社トランスコスモスグループへのM&Aを経験、2年間グループ会社代表を務める。

執行役員CTO　今給黎成彬

東京大学工学系研究科技術経営戦略学卒。機械学習によるディープフェイク技術の研究後、ソフトバンク株式会社にてAI開発に従事。ITスタートアップを医療DX企業メドレーに売却し、技術主任を3年間担当。

プロジェクトマネージャー　田中靖祥

早稲田大学政治経済学部を卒業。卒業後、株式会社ラクスにインフラエンジニアとして入社。SaaSスタートアップに取締役として参画し、5億円以上の資金調達を実現。

Yagura


Yagura