サイバー脅威の最新トレンドと
いま注目を集めるセキュリティでのAI活用

米国 Deep Instinct
バイスプレジデント APJセールスエンジニアリング担当
乙部幸一朗

Agenda

- サイバー脅威の最新トレンド
- セキュリティでの AI 活用

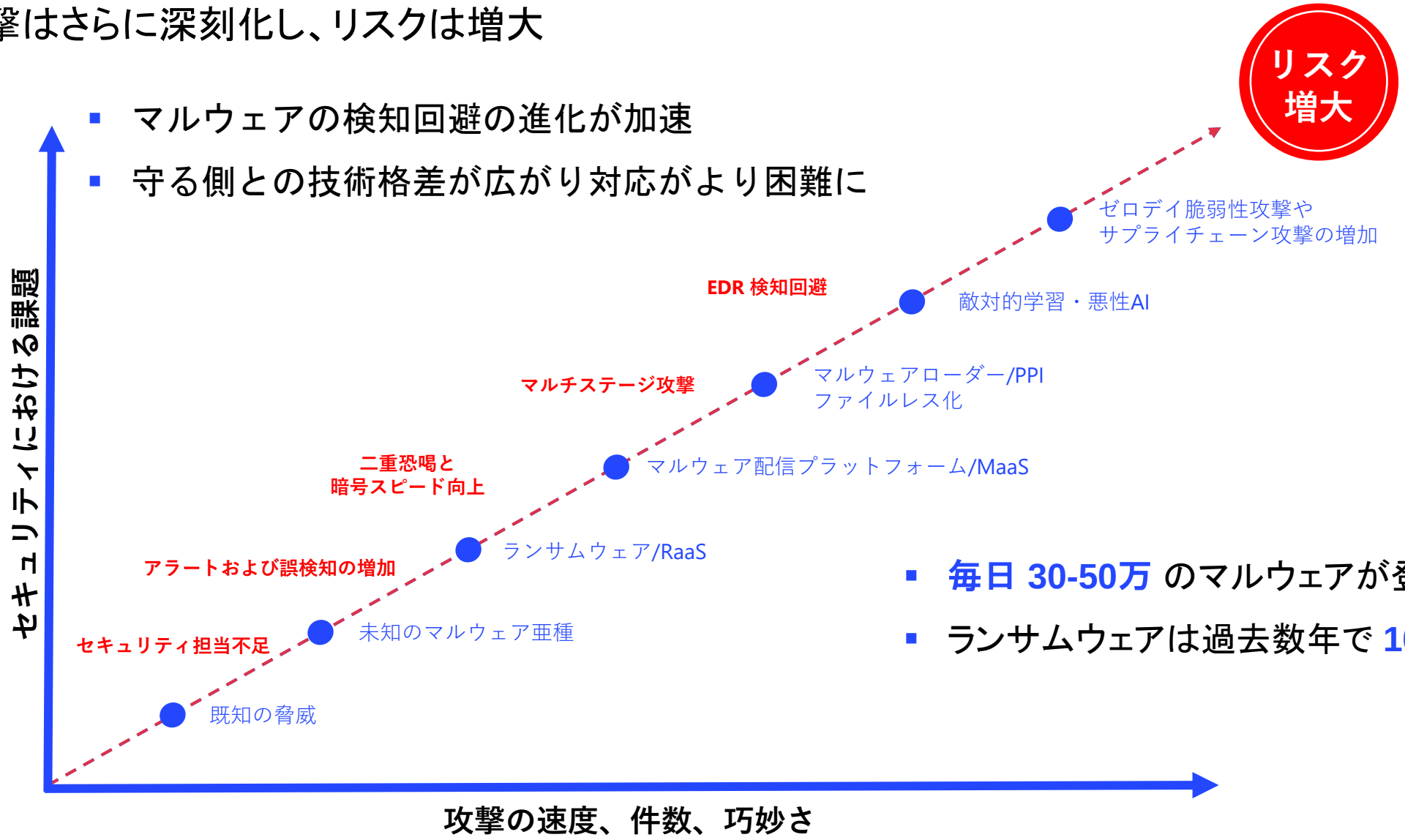
Agenda

- サイバー脅威の最新トレンド
- セキュリティでの AI 活用

高度化するサイバー脅威

攻撃はさらに深刻化し、リスクは増大

- マルウェアの検知回避の進化が加速
- 守る側との技術格差が広がり対応がより困難に

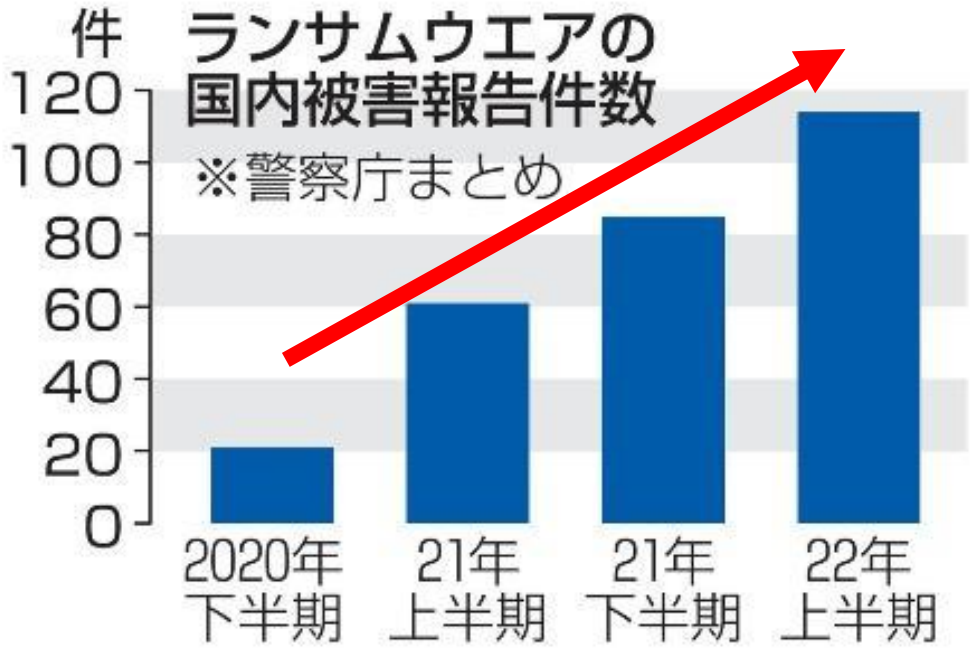


- **毎日 30-50万** のマルウェアが登場
- ランサムウェアは過去数年で **10倍** 以上に*

* Deep Instinct調べ: Threat Research 2021 Mid-Year Report * Deep Instinct調べ

日本企業のランサムウェアの被害状況

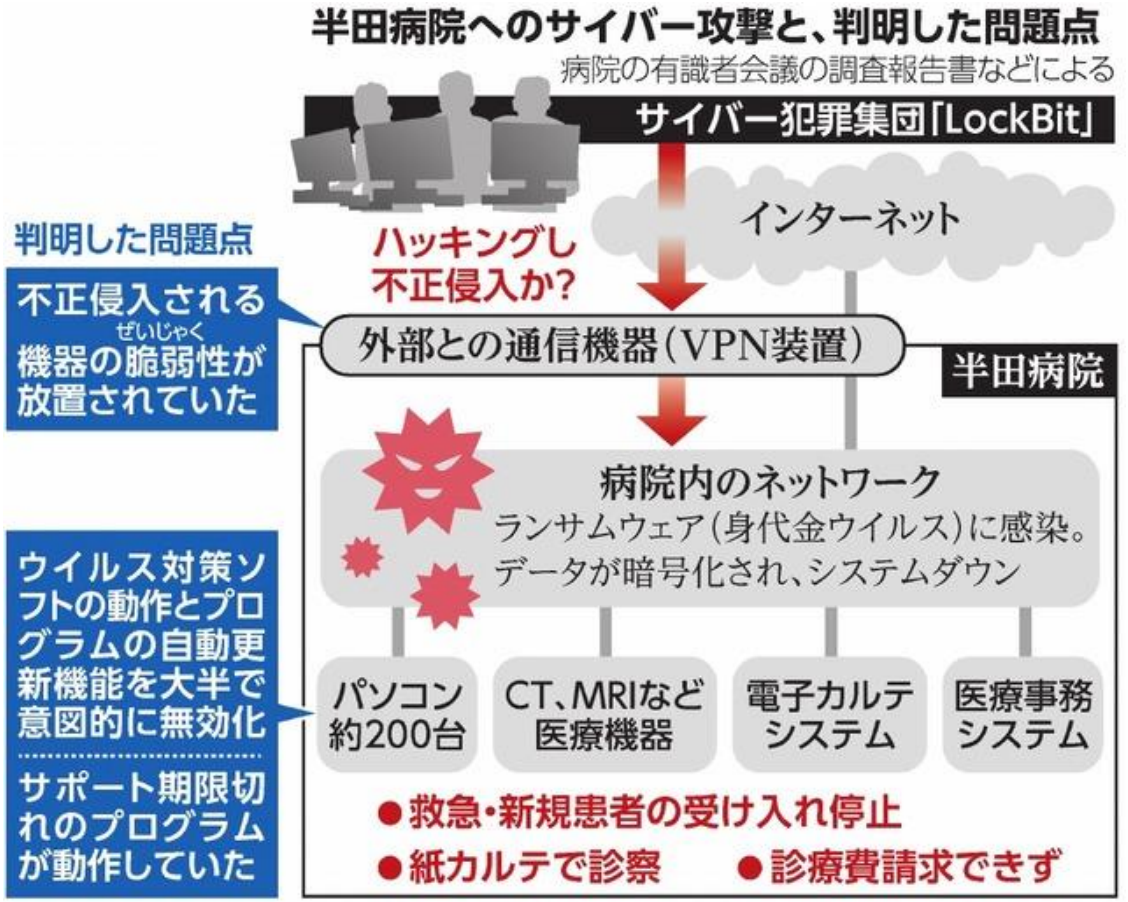
2022年も被害件数は増加傾向
被害報告のうち**二重恐喝**の手口が6割
VPN機器からの侵入、リモートデスクトップからの侵入がほとんど



企業名	報道されている被害内容
鹿島	海外子会社で約130万件のデータが流出
HOYA	米国子会社の情報が漏洩、一部公開される
富士フィルム	システム遮断などの影響もあり、業務に影響
ニップン	基幹システムが停止し、四半期報告が遅延
オリエンタル コンサルタンツ	公共事業などの情報の流出？ 7億5000万円の特別損失を計上
JVCケンウッド	欧州拠点で個人情報流出
半田病院	約2ヶ月間全面診療停止に、2億円の復旧費用
小島プレス	部品供給の問題でトヨタの工場が一時稼働停止
ブリジストン	米国工場が一時稼働停止
デンソー	図面データなど15万件以上の情報が流出
森永製菓	164万人以上の個人情報流出？
日本アンテナ	社内パソコンが使用できない状態に

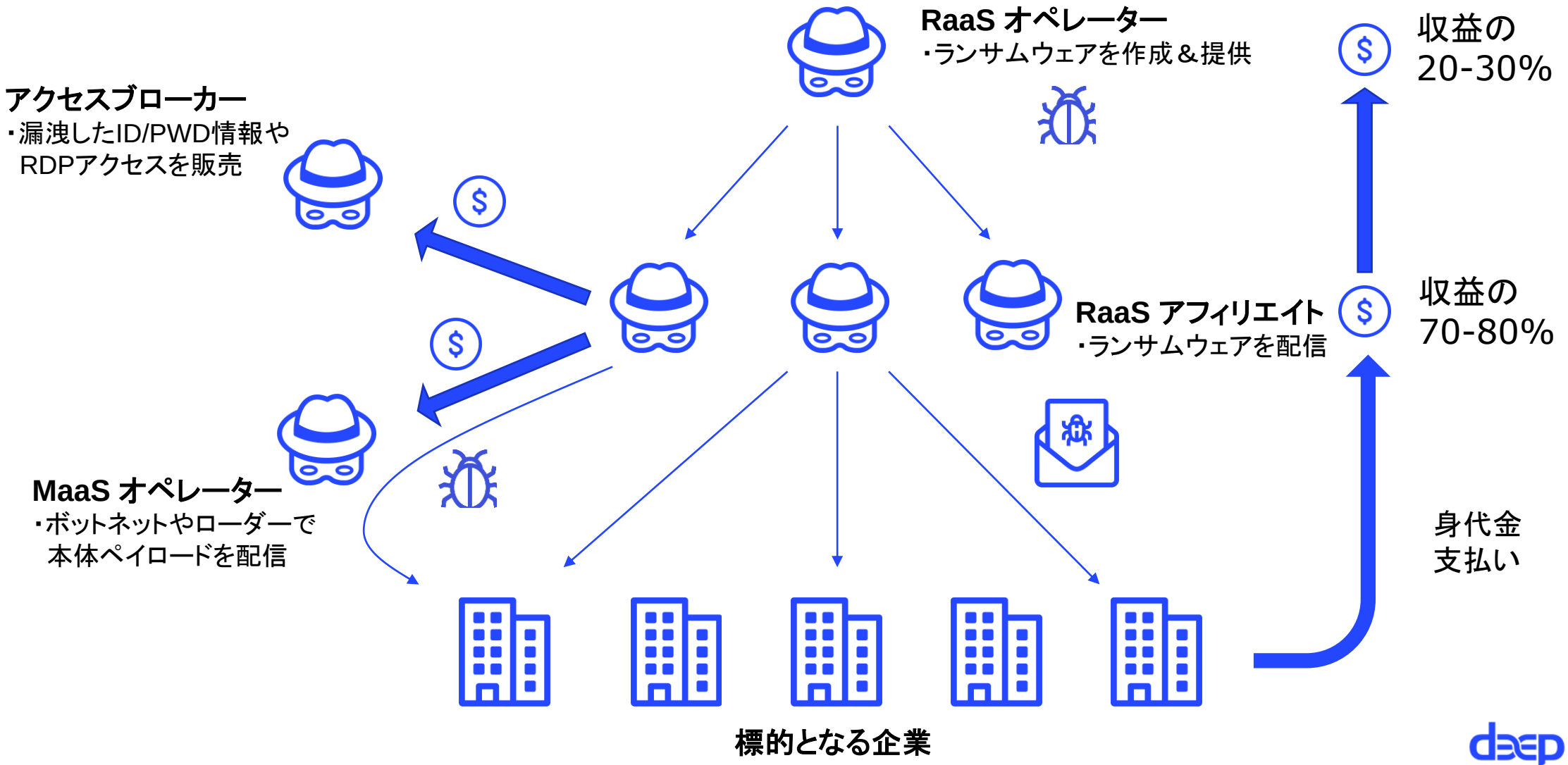
ランサムウェア攻撃の実例：徳島県半田病院

- ランサムウェア感染により2ヶ月間の診療停止に
  - VPN装置（Fortigate)の脆弱性から侵入、更にそこからMimikatzやpsexecなどを使ってパスワード奪取や水平展開をされたと見られる
  - 侵入から3時間半で40台のサーバとバックアップサーバがすべて暗号化されて、電子カルテデータも閲覧できなくなり、すべてのシステムが利用不可能になり、診療ができなくなった
  - 攻撃に使われたランサムウェアは高速暗号化で有名な RaaS の1つ「Lockbit2.0」とみられる
  - 身代金は支払わず、結果的に復旧までに直接的な費用として2億円と2ヶ月の期間がかかった



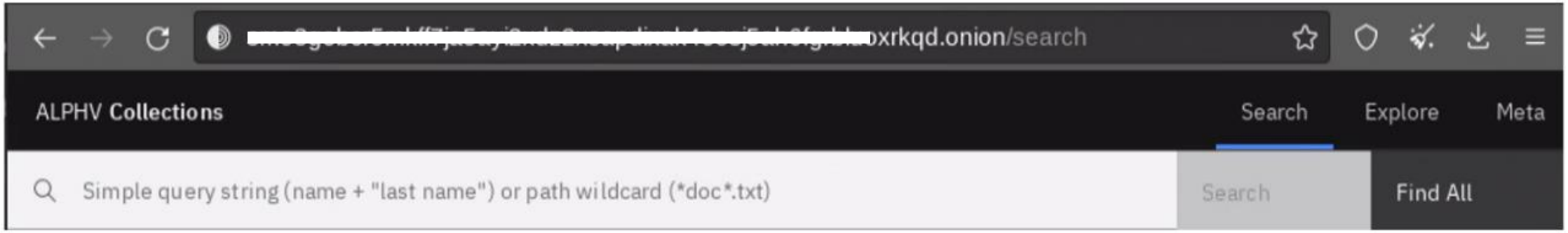
参照：朝日新聞「閉じられたネット」病院を取り巻く安全神話　身代金ウイルス被害

ランサムウェアを中心としたビジネスモデル：RaaS & MaaS & アクセスブローカー



ランサムウェアの新しいトレンド:
RaaS の主流は暗号化からデータ持ち出しへ

2022年7月ランサムウェア運用者である BlackCat / ALPHV が新たな漏洩サイトを発表
同様の漏洩サイト/データベースが少なくとも 17 以上存在

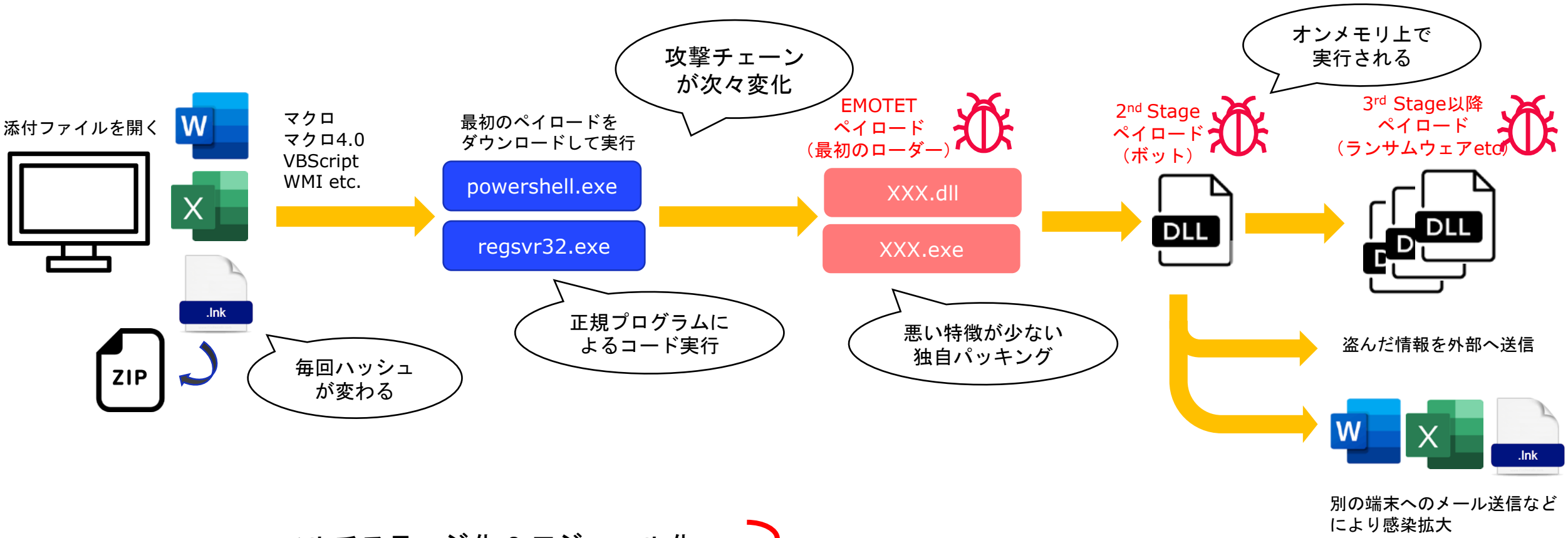


漏洩・公開されているデータの例

企業の従業員情報、決算情報、人事/給与情報、管理者情報、事業計画、取引情報 etc.

関連企業が取引先が多い企業から機密情報が漏洩した場合、ID やパスワード情報
その他の情報が悪用され、ソーシャルエンジニアリング攻撃によって被害拡大も

高度化するマルウェアの代表例: EMOTET

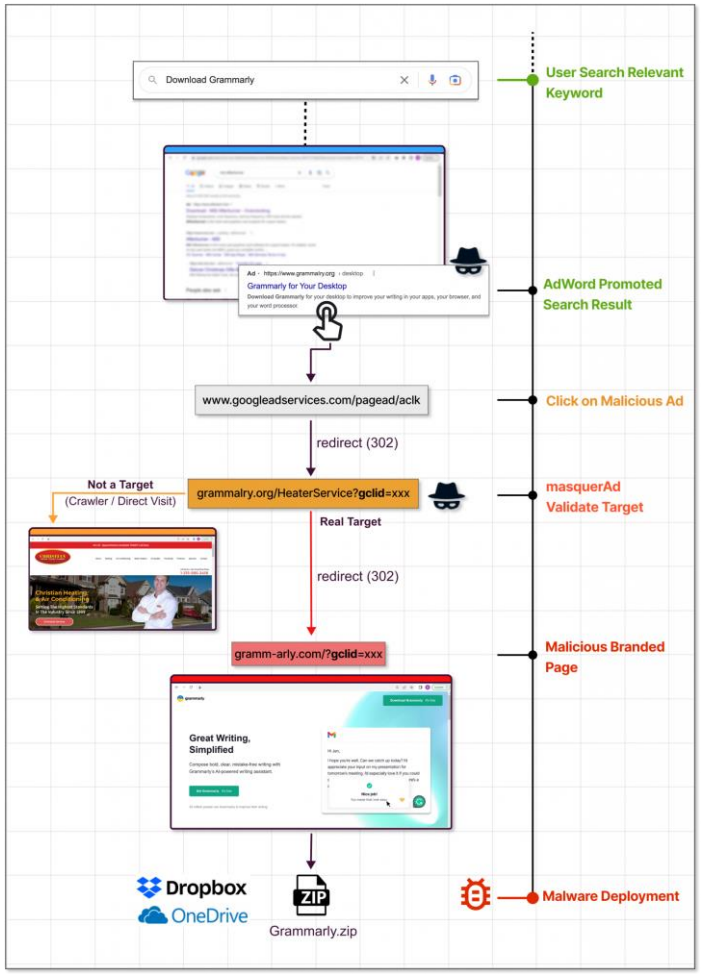


- マルチステージ化＆モジュール化
- 高度な難読化＆アンチデバッグ
- オンメモリでの実行（ファイルレス動作）
- 攻撃チェーンを次々と変化

シグネチャでは検知が難しい上に
機械学習モデルでも検知できない
イベントルールでも検知が難しい

高度化するマルウェア攻撃の例：Google 広告の悪用

- Google 広告によって不正コードを含む偽アプリに誘導
  - Google広告で有名なアプリ名などで検索した場合に
    あたかもそのアプリのサイドのような広告ページを表示
  - クリックすると偽サイトに飛ばされて、正規アプリに
    見せかけた悪性コードを含むアプリがダウンロードされる
  - Googleのチェックをすり抜けるために、広告の最初の
    リダイレクト先には正規アプリへの誘導サイトも置いておき
    ターゲットとなる端末以外はそちらにリダイレクトされる
  - フィッシング対象のアプリとして Slack, Grammarly,
    Teamviewerなど使われてることが確認



https://www.bleepingcomputer.com/news/security/hackers-abuse-google-ads-to-spread-malware-in-legit-software/

高度化するマルウェア攻撃の例：モバイルマルウェアも増加傾向

モバイルマルウェアはほとんどがアンドロイドを標的としている
情報搾取活動を行うものが主流

	ターゲットOS	アプリのなりすまし	金銭的なりすまし	マルチモーダル（ソーシャルメディア）	認証情報の窃取	マイクとカメラ	SMSによる感染	権限昇格	主な標的地域
FluBot		✓	✓	✗	✓	✗	✓	✓	アジア、イギリス、欧州
TeaBot		✓	✓	✓	✓	✗	✓	✓	イギリス、欧州
TangleBot		✗	✓	✓	✓	✓	✗	✓	北米
MoqHao		✓	✓	✓	✓	✗	✓	✗	アジア、日本
BRATA		✓	✓	✗	✓	✗	✓	✗	イギリス、欧州、南米
TianySpy		✓	✓*	✗	✓	✗	✗	✗	日本
KeepSpy		✓	✓*	✗	✓	✗	✗	✗	日本

参照：proofpoint ブログ「欧州でモバイルマルウェアが急増中」

Agenda

- サイバー脅威の最新トレンド
- セキュリティでの AI 活用

従来のセキュリティのアプローチ は“指名手配型”

- **シグネチャ ＝ 指名手配書**
  - 確認された脅威が掲載されているブラックリスト

見たことがあるものは止めるが、、

見たことがないものは止めない（止められない）

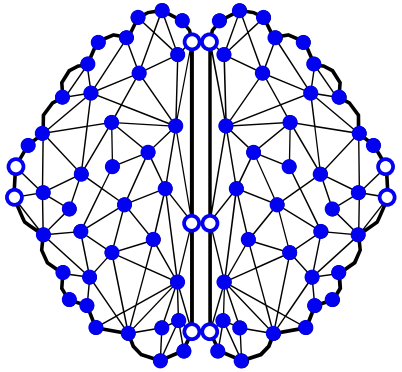
サイバーセキュリティにおける構造的な問題

攻撃が先行して
防御側が追いかける
（AVでもEDRでも同じ）

常に攻撃側優位

ディープラーニングの可能性

ディープラーニングを
サイバーセキュリティに適用



学習

収集されたデータを元に自己学習し、人間の専門家による特徴抽出を必要とすることなく、さまざまな対象に対して高精度なモデルを生成

予測

初めて見る脅威に対しても、その構造から危険性を予測し、実行される前に判定可能

予防

感染を予防することで、被害を発生させることなく安心と安全を提供

学習とモデリング

モデルを使った推論

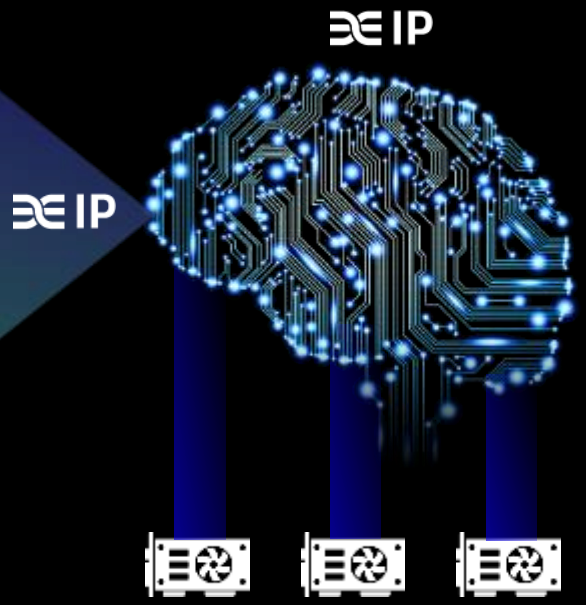
ディープラーニングを活用した学習と予測

- 第三者機関やレポジトリ
- ダークネット
- 自作マルウェア
- 亜種化

*.exe *.ppt *.xls *.pdf *.SWF *macro *.dll *.macho *.doc *.rtf *.APK

- データサンプル:
  数億を超える良性・悪性ファイル

Deep Instinct 独自
DNN フレームワーク



Nvidia GPUs

- 未知の脅威を実行前に防御
- 誤検知が少ない
- 軽量なエージェント:
  <150MB, <1% CPU
- 日々のアップデート不要
- 様々な OS 環境をサポート

deepinstinct

Phobos ランサムウェア

大阪急性期・総合医療センターを襲ったランサムウェアも2年以上前のモデルで補足

背景:

- 2022年11月、大阪急性期・総合医療センターがランサムウェアと見られる攻撃によりシステムが停止し、診療停止に追い込まれた
- 攻撃に使われたのは Phobos と呼ばれるランサムウェアで影響を受けたと見られる端末は約1300台にのぼると見られる

予防の実例:

- 2022年11月のPhobosのマルウェア検体をテストしたところ33ヶ月前の数世代前の古いD-brainのモデルでも静的なファイルスキャンで予防できていることを確認

Deep Instinct が初見で予防した他のランサムウェアファミリー

BLACK BASTA RANSOMWARE
LOCKFILE RANSOMWARE
MAZE RANSOMWARE
RAGNAR LOCKER RANSOMWARE
TESLACRYPT RANSOMWARE
REVIL RANSOMWARE
BLACKMATTER RANSOMWARE
LOCKBIT 3.0 RANSOMWARE
BITPAYMER RANSOMWARE

新種 EMOTET

VirusTotalに上がる前の新種ファイルを初見でブロック

背景:

- 2022年7月頃から活動を休止していたEmotetが11月に入り活動を再開
- 11月4日にJPCERTから新しい注意喚起が発表

予防の実例:

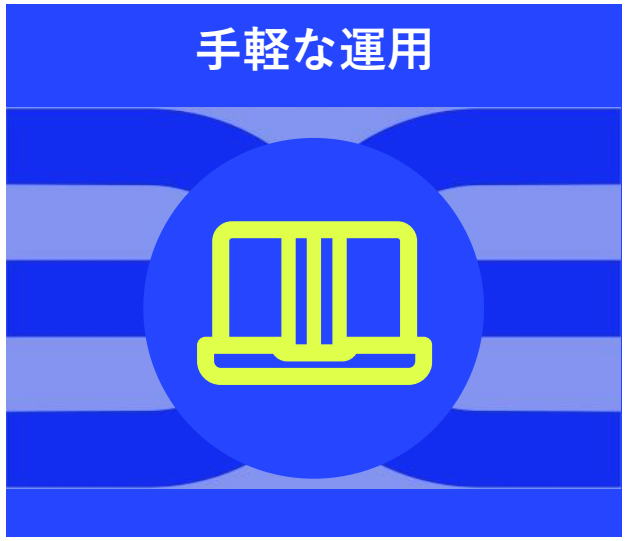
- DIを導入展開中のお客様環境において、11月3日にこの新しいEmotetの検体をメールにて受信
- メールに添付されていたExcelファイルをD-brainが静的なファイルスキャンで即時防御
- 該当のファイルがVirusTotalにアップされたのは11月7日

Deep Instinct の特徴

高度な既知/未知のマルウェアも
予測してブロック

ランサムウェアから情報搾取系
ファイルレスマルウェアまで対応

オフライン環境でも検知能力を
下げることなく自動で防御



誤検知が少ない
（従来製品比で数十～数百分の1程度）

毎日のアップデートやフルスキャンが不要
（モデルの更新は年1-2回）

CPUやメモリの消費が少なく
動作が圧倒的に軽い

Deep Instinct Prevention Platform

未知の脅威を阻止するための予防ファースト アプローチ

さまざまな環境でファイルを
スキャンし脅威を早期発見する
エージェントレス製品

ディープラーニングを活用した
業界最高レベルの防御力を誇る
エンドポイント製品

サイバーセキュリティにおけるゲームチェンジ

AI の予測により
防御側が先行できて
攻撃側が追いかける

攻撃側の先出しの優位が無くなる

顧客事例：ヤマダホールディングス

業種: 小売
規模: エンタープライズ
用途: アンチウイルス

東証プライム市場　上場

日本最大規模の家電量販店を展開　（47都道府県に1000以上の店舗）

従業員23,000人（連結）

> “セキュリティの予算、リソースには現実的な限界があります。
> その制限の中で、より良い製品を選択しなければなりません。
> ディープインスティンクトは、まさにその悩みを持つ企業の助けになるでしょう”
>
> – IT事業本部システム運用部　理事/執行役員　原田勇一 氏

導入背景

- Symantec/Broadcom（SEP）の契約更新のタイミングで**大幅な値上げ**が発生
- SEP自身の**配布、バージョンアップの難しさ、アップデート後に発生するブルースクリーン**（BSOD）、**サポート体制などに不満**があった
- ラサムウエアなど**の未知の脅威への対策**が急務
- **導入コスト、運用コスト**を考慮しつつ、**自社で運用が可能**な製品を前提に、複数のNGAV/EDRを検討していた
- 既存のSEPはアンインストール前提。ただし、アンインストールできなかった場合の動作の共存も考慮

結果

- **15,000もの端末を未知の脅威から保護**
- **予防ファーストのアプローチ**, 実行前に防御してオフラインでも動作
- 既存 AV 製品であった Symantec/Broadcom の **EP は置き換え、追加ライセンスコストを抑制**
  ※推奨はされていないが、SEPと共存も可能
- **運用負荷を以前 の半分以下に抑え**セキュリティレベル強化を実現

採用のポイント

- **自社評価**:自社開発環境下でのフルスキャンを行い、**静的解析に関してはほぼ誤・過検知無し**
  比較した他社よりも優秀な結果を示す
  ※振る舞い分析、メモリ内の保護は若干有り
- **シンプルな管理インターフェース、グループ管理、テナント管理が可能で、自社運用が可能**と判断
  ※弊社は店舗、本部、グループ会社等が存在する為、グループ機能は必須
- ディープラーニングで作成されたモデルによる、**一定期間オフライン状態になったとしても安心できる高い検知力**
- インストーラーのファイルサイズが約27MB、圧縮後で約8MBとなり**配布が容易**
- **端末への低い負荷**。CPU使用率、メモリ使用量が低い
  ※大量のファイルアクセス等が発生した場合はそれに準じます

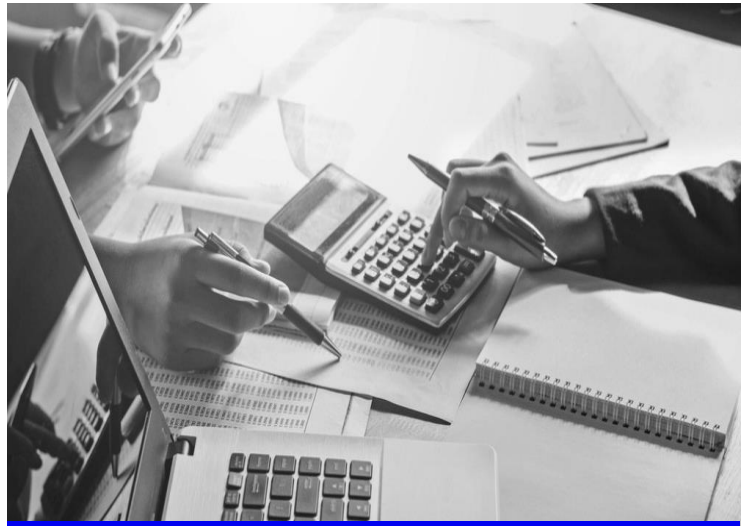
サイバーセキュリティ+ AI によって提供できる価値

誰でも使える

管理者を楽にし
従業員をハッピーに

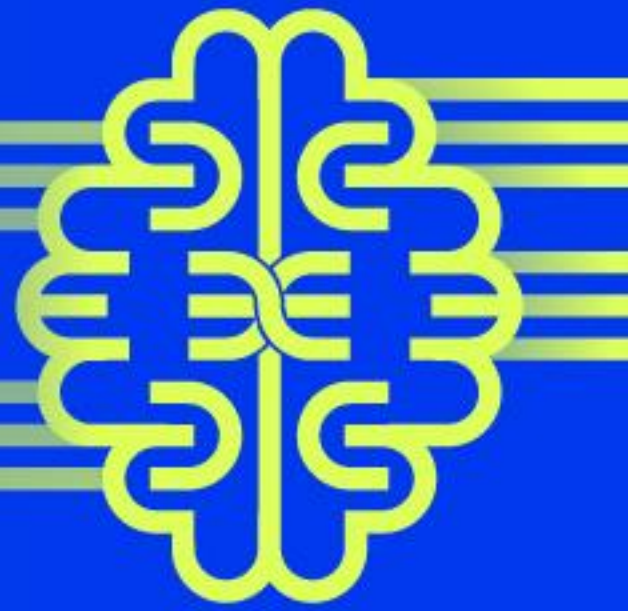
感染と被害を**予防**

ビジネスの継続性を約束



TCOを削減

Thank You



deep instinct™