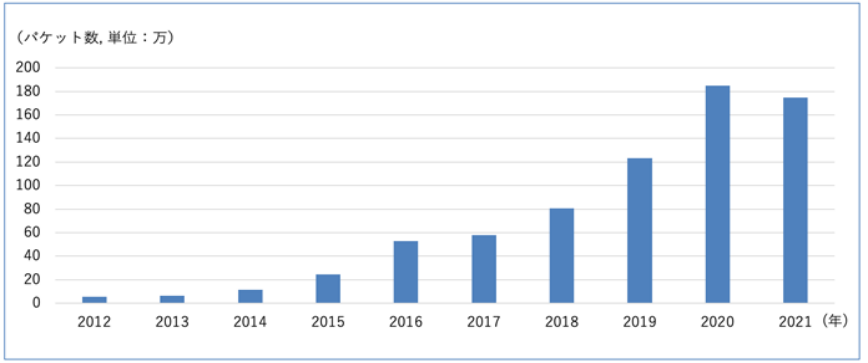
エンドポイントセキュリティ技術の定性評価

吉岡　克成

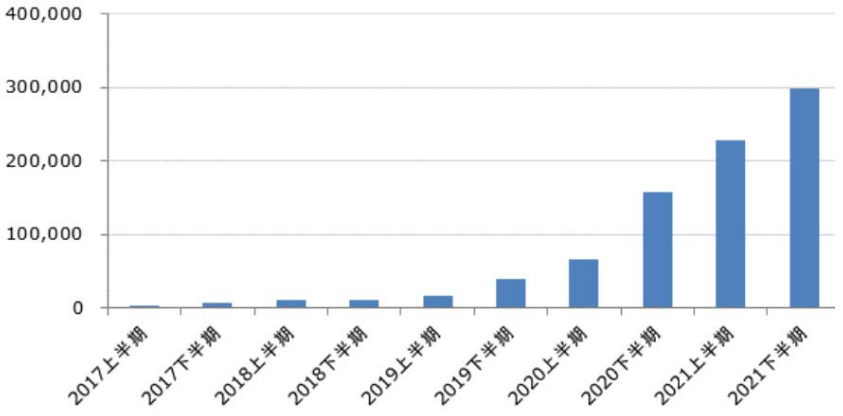
横浜国立大学
大学院環境情報研究院/先端科学高等研究院

サイバー攻撃の巧妙化・深刻化

- **頻度、規模、対象が拡大（量的な脅威の増大）**
  - なりすましメール
  - フィッシング
  - 脆弱なVPN装置、IoT機器を狙う攻撃
  - 重要インフラを狙う攻撃
  - 超大規模サービス妨害攻撃



- **高度化、組織化、ビジネス化の進展（質的な脅威の増大）**
  - ソーシャルエンジニアリング攻撃
  - サプライチェーン攻撃
  - ゼロデイ攻撃
  - 〇〇-as-a-Service
  - ランサム攻撃における多重脅迫
  - 世論操作、心理的攻撃

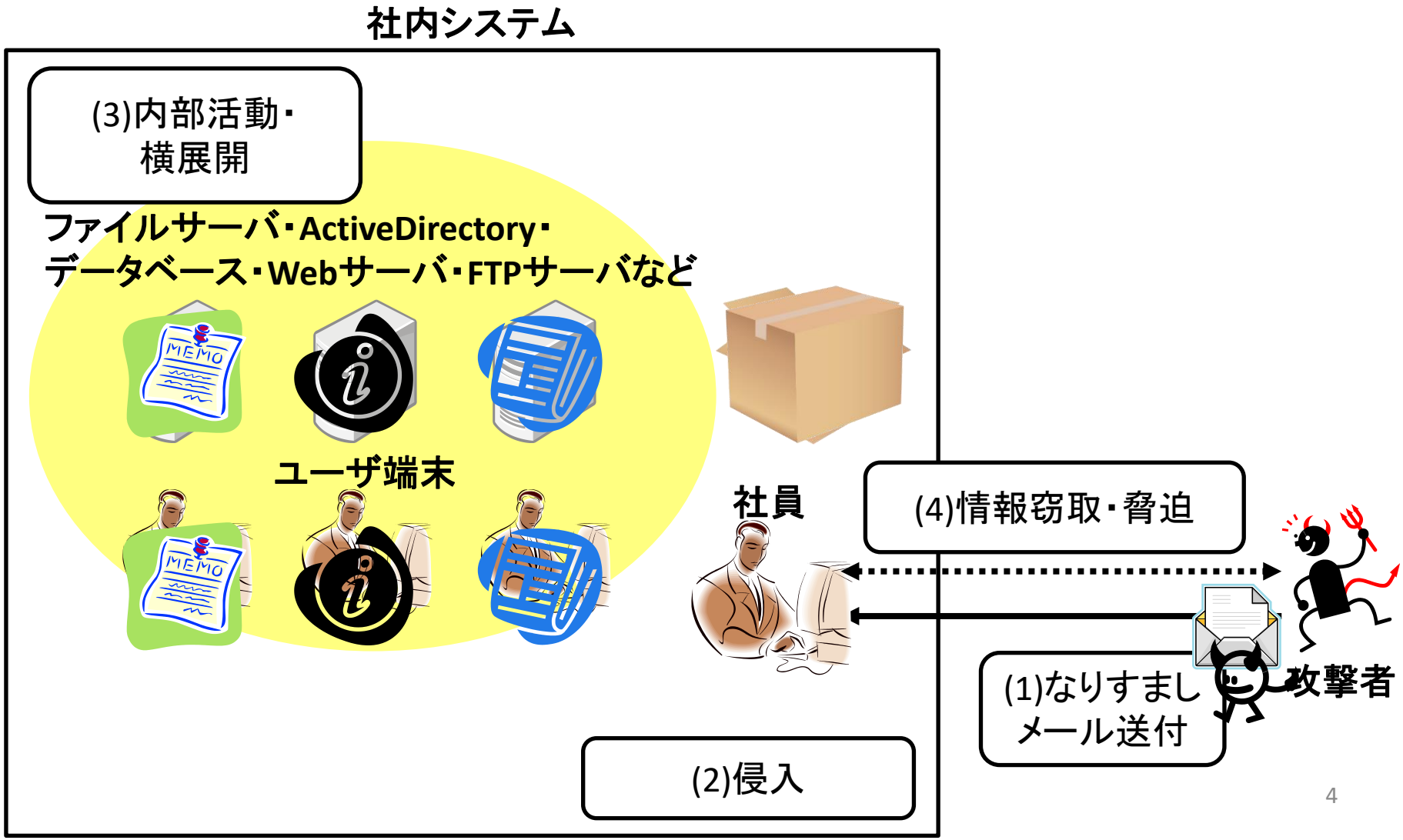


DX、働き方の多様化、社会情勢の変化（例：パンデミックやウクライナ情勢）により、広い分野でサイバー脅威が高まっている

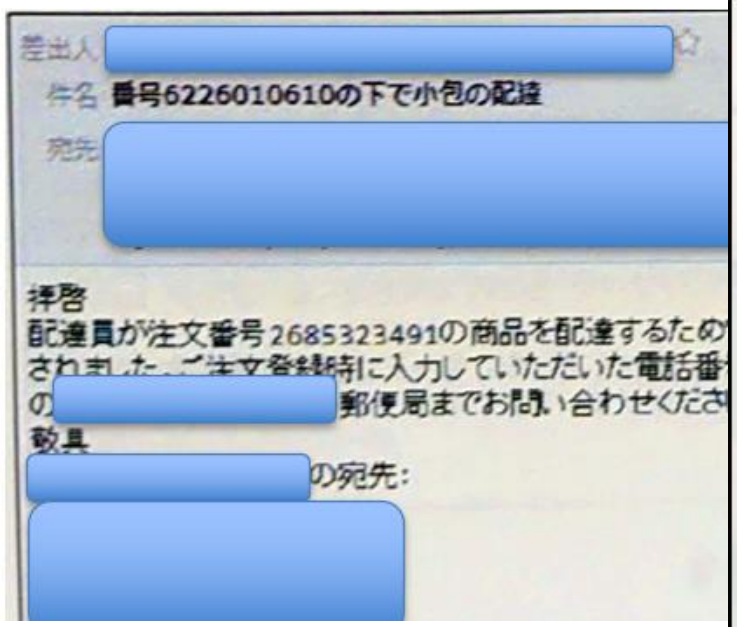
情報通信研究機構 NICTER観測レポート2021の公開, https://www.nict.go.jp/press/2022/02/10-1.html
フィッシング対策協議会　フィッシングレポート, 2022 https://www.antiphishing.jp/report/phishing_report_2022.pdf

脅威例：なりすましメール攻撃

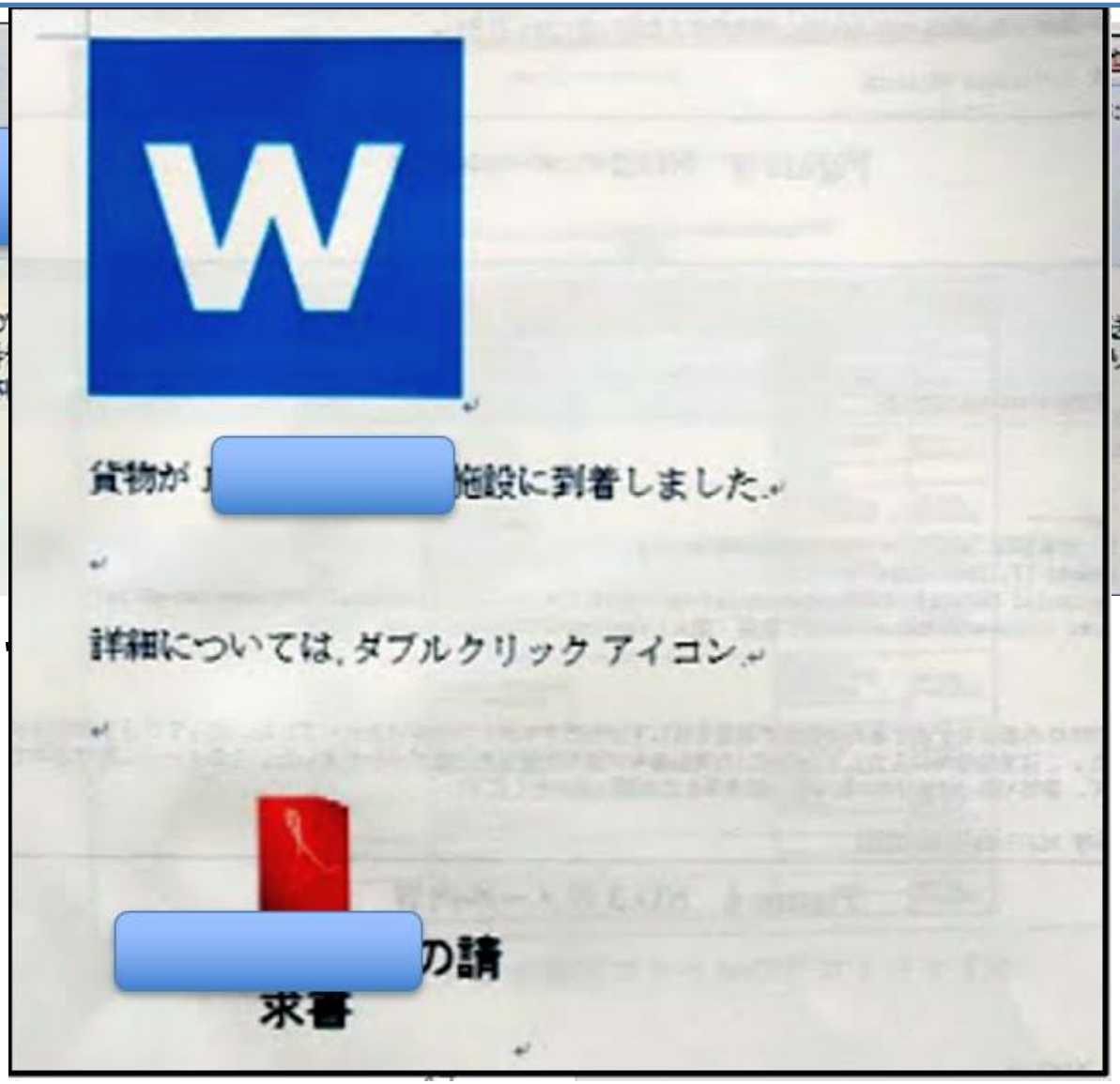
一般的な標的型メール攻撃



なりすましメール攻撃の例



「郵便物未配達のお知ら
メールが届く



例． 注文確認、 支払い通知、 領収書等

発行日 2016/8/31

お支払通知書

株式会社 御中

振込手数料 ¥756 差引後

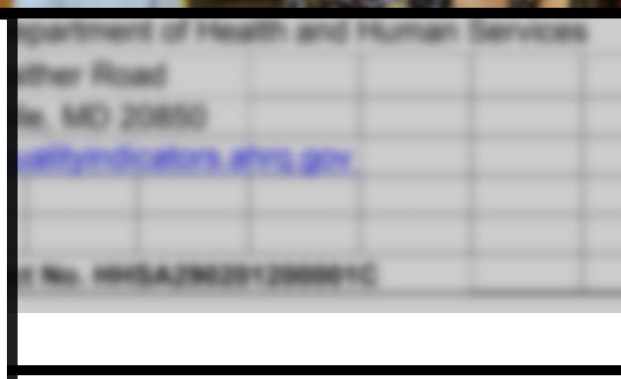
下記のとおりお振込いたします。

振込金額	¥375,700
支払日	2016/9/16
対象期間	2016/8/1 ～ 2016/8/15

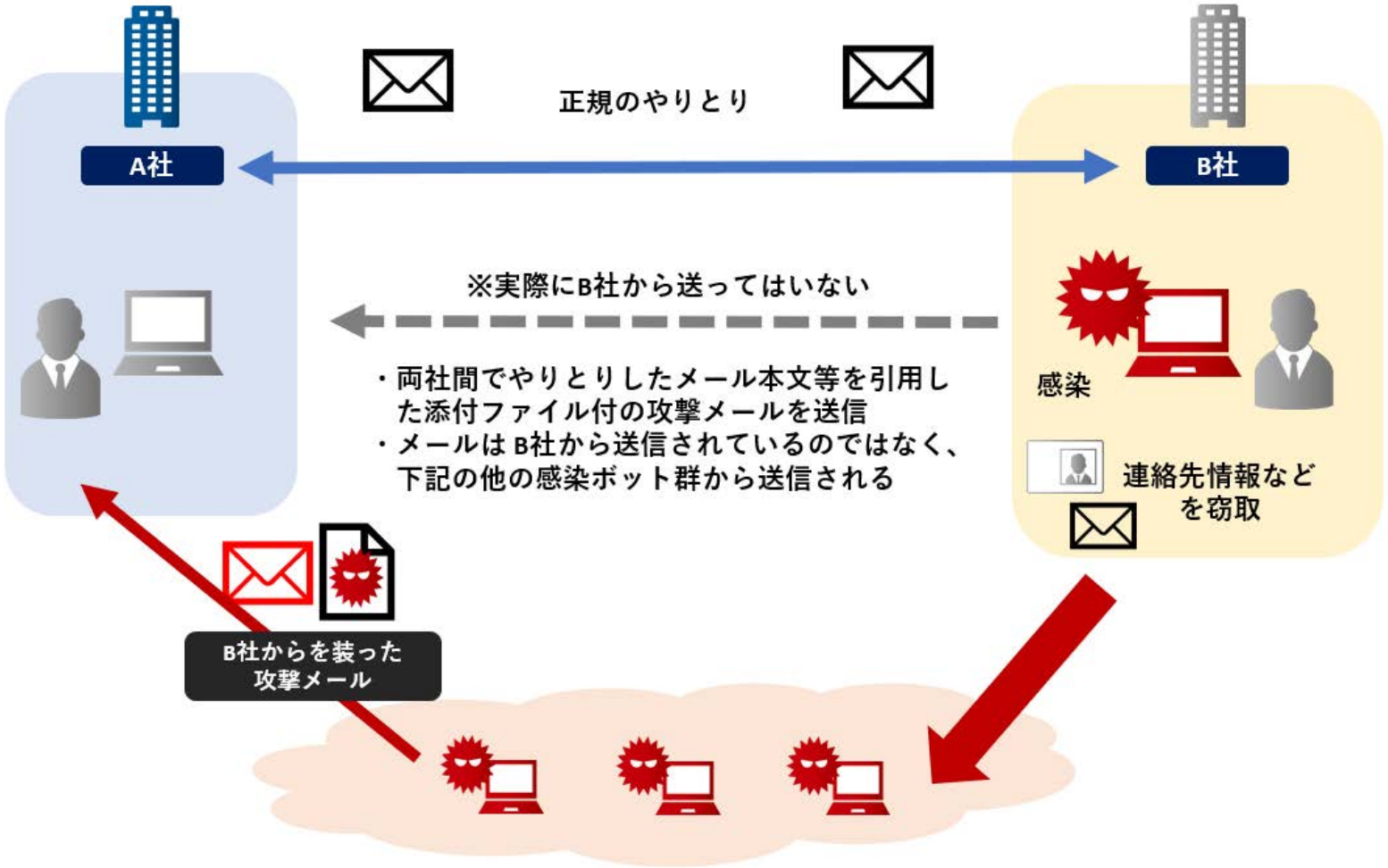
例．履歴書

例：コロナウイルス関連

新型コロナウイルスに関するQ&A（一般の方向け）

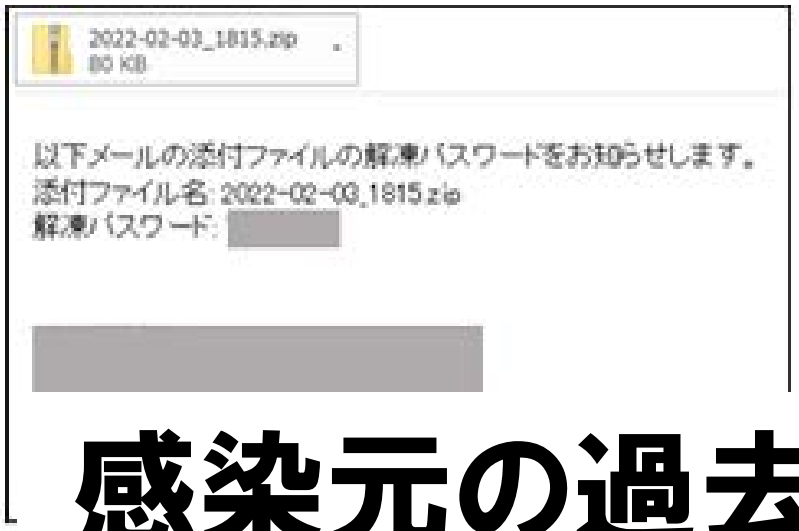


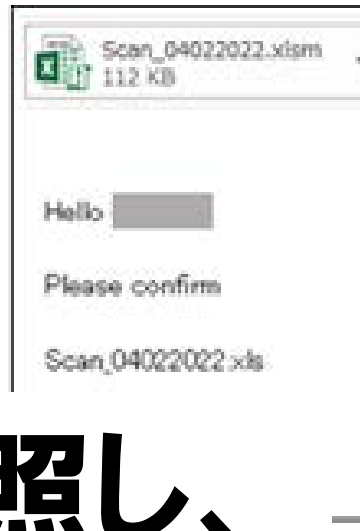
Emotet



Emotet に感染した端末で構成されるメール送信用のボットネット
感染先から窃取した連絡帳やメール認証情報を使って攻撃メールの配信を行う。

https://www.jpcert.or.jp/newsflash/2019112701.html





感染元の過去メール等を参照し、簡易ななりすましを行う（返信を装う等）

→自動化が容易なため、攻撃が急増

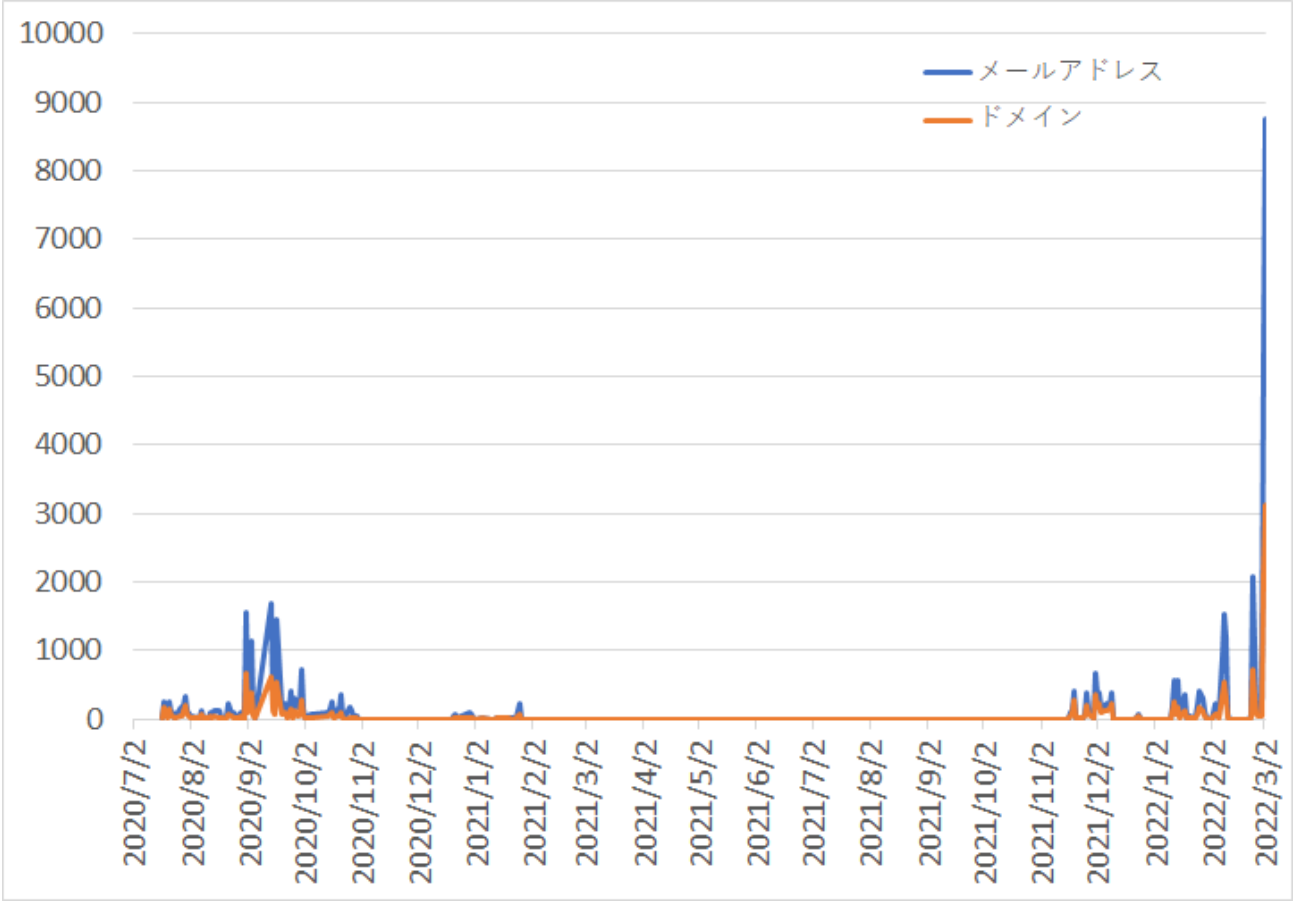
本文が英語で書かれ、パスワード付き
ZIPファイルが添付された攻撃メール

不正なURLリンクを含む攻撃メール

IPA,「Emotet(エモテット)」と呼ばれるウイルスへの感染を狙うメールについて
https://www.ipa.go.jp/security/announce/20191202.html#L19

Emotet感染再拡大

Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数の新規観測の推移 (外部からの提供観測情報)（2022年3月3日更新）

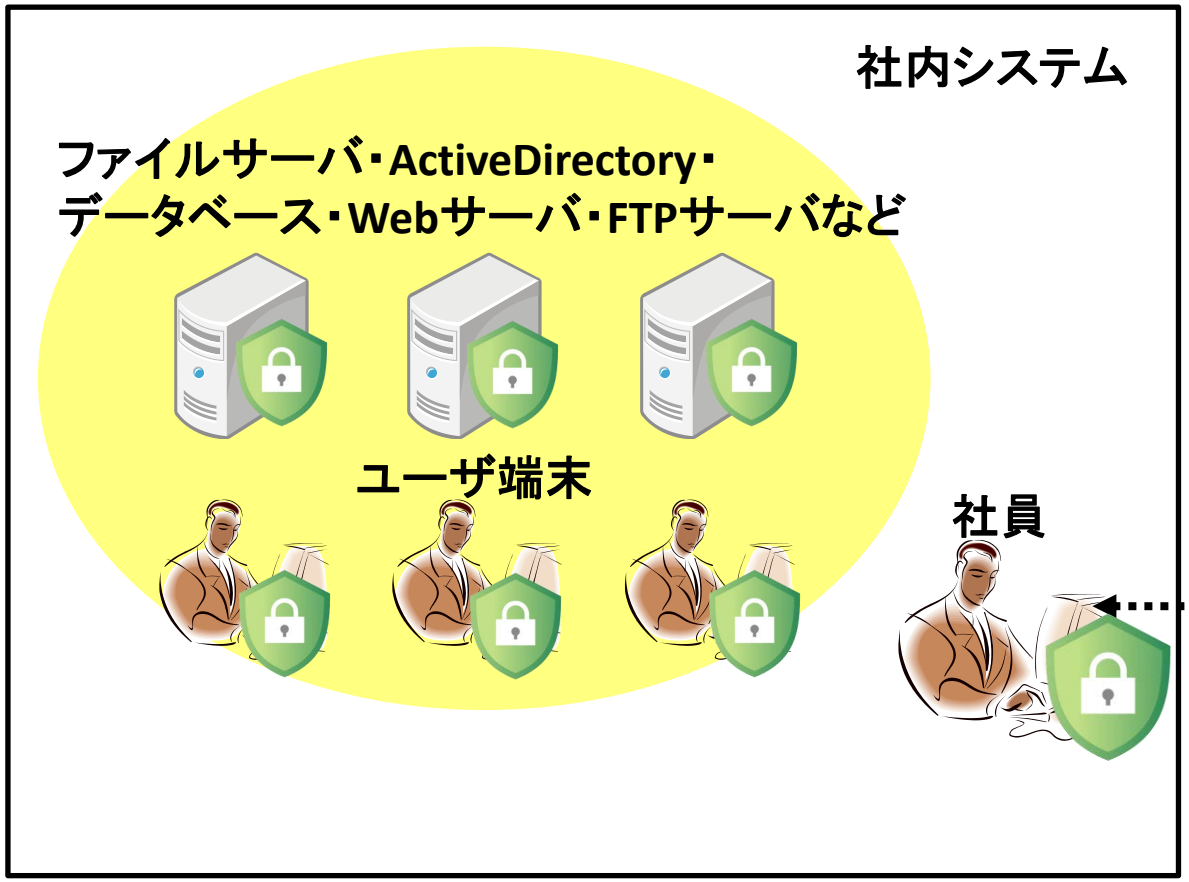


JPCET/CC, マルウェアEmotetの感染再拡大に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220006.html

脅威に対抗する
エンドポイントセキュリティ技術

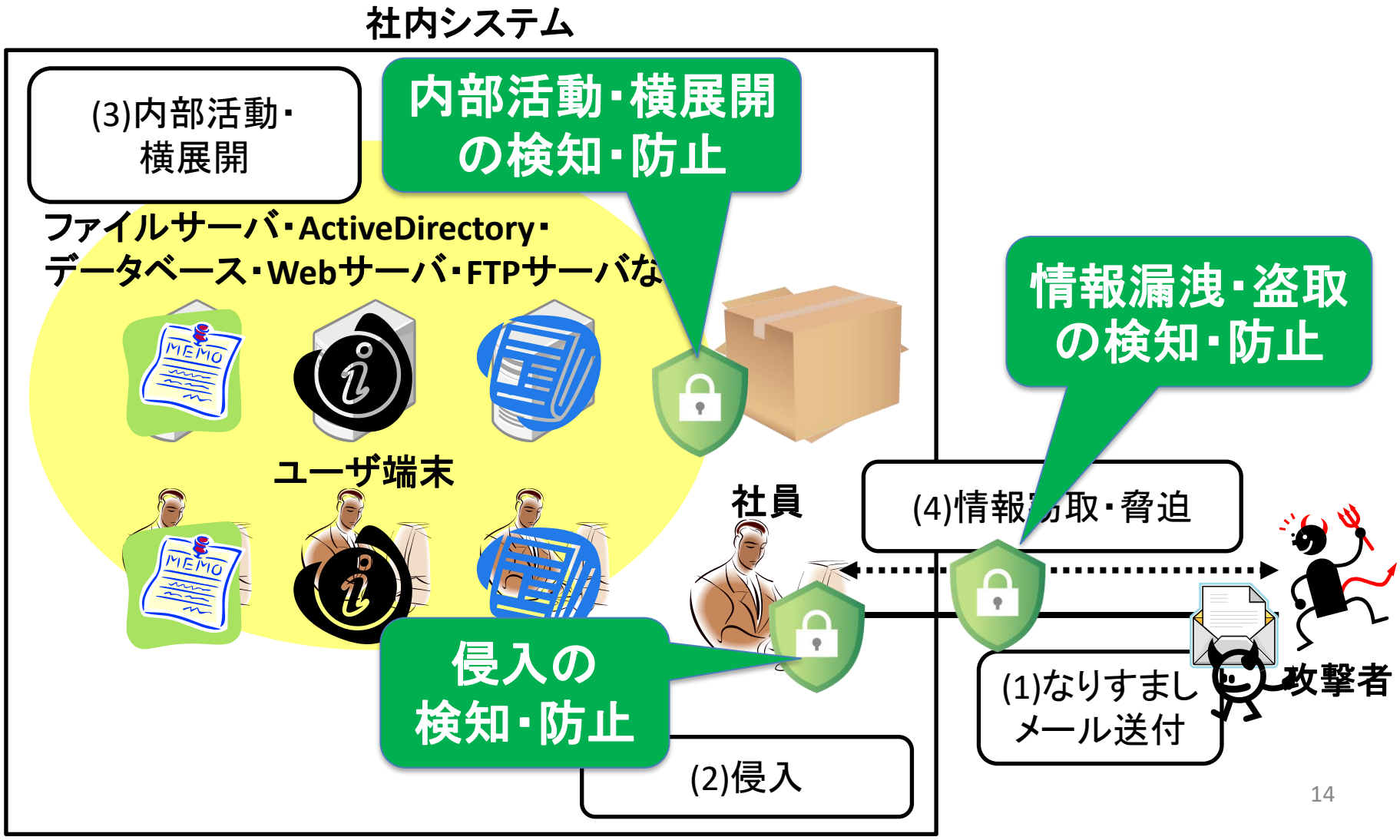
エンドポイントセキュリティ技術

パソコンやサーバなどのエンドポイントに対して導入するセキュリティ技術．DXや多様な働き方の実現により境界防御が難しくなる現在、組織のセキュリティの最後の砦ともいえる。



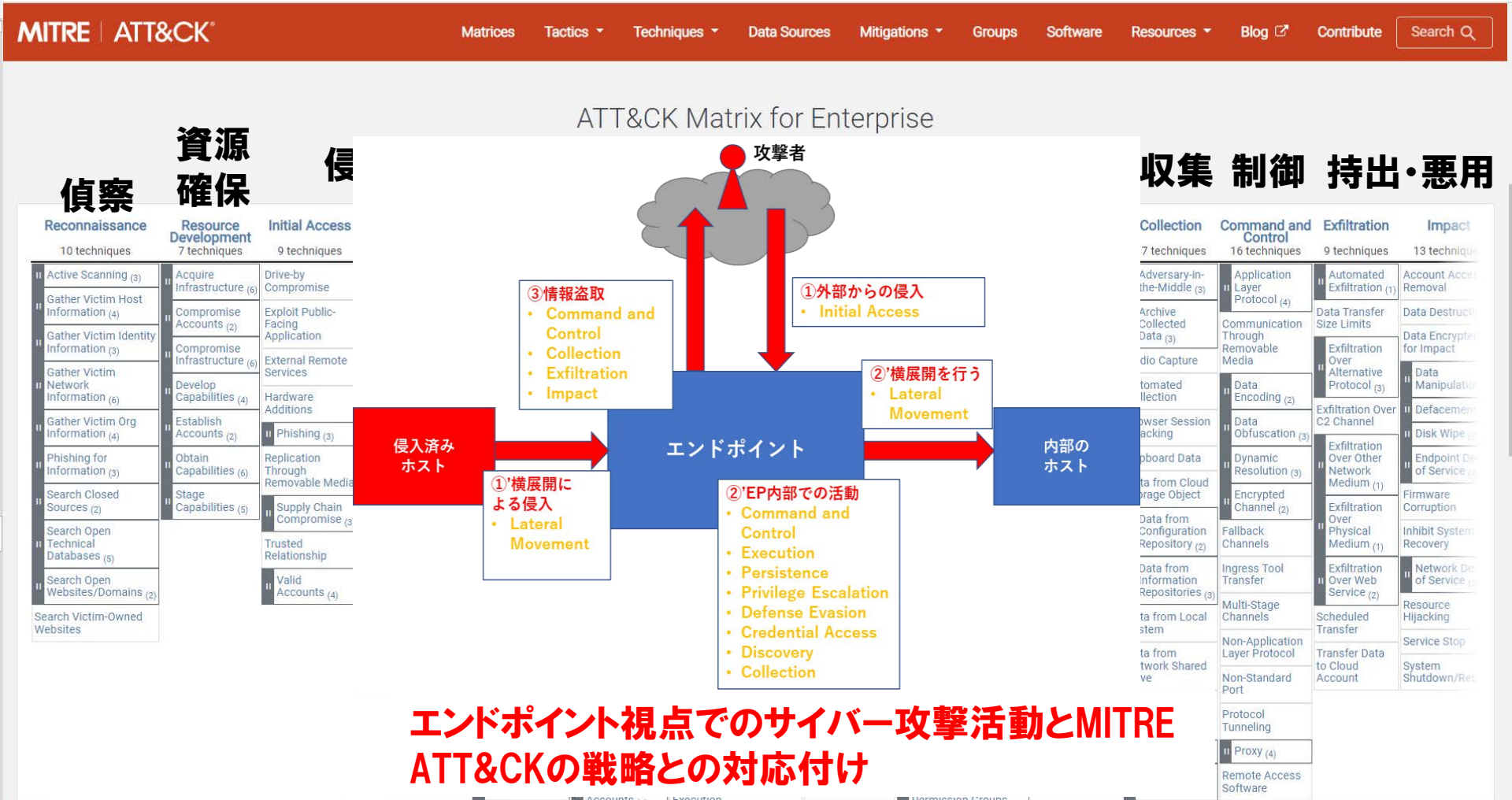
- NGAV（Next Generation AV）
- アプリケーション隔離
- EDR（Endpoint Detection & Response）

セキュリティ対策の評価項目



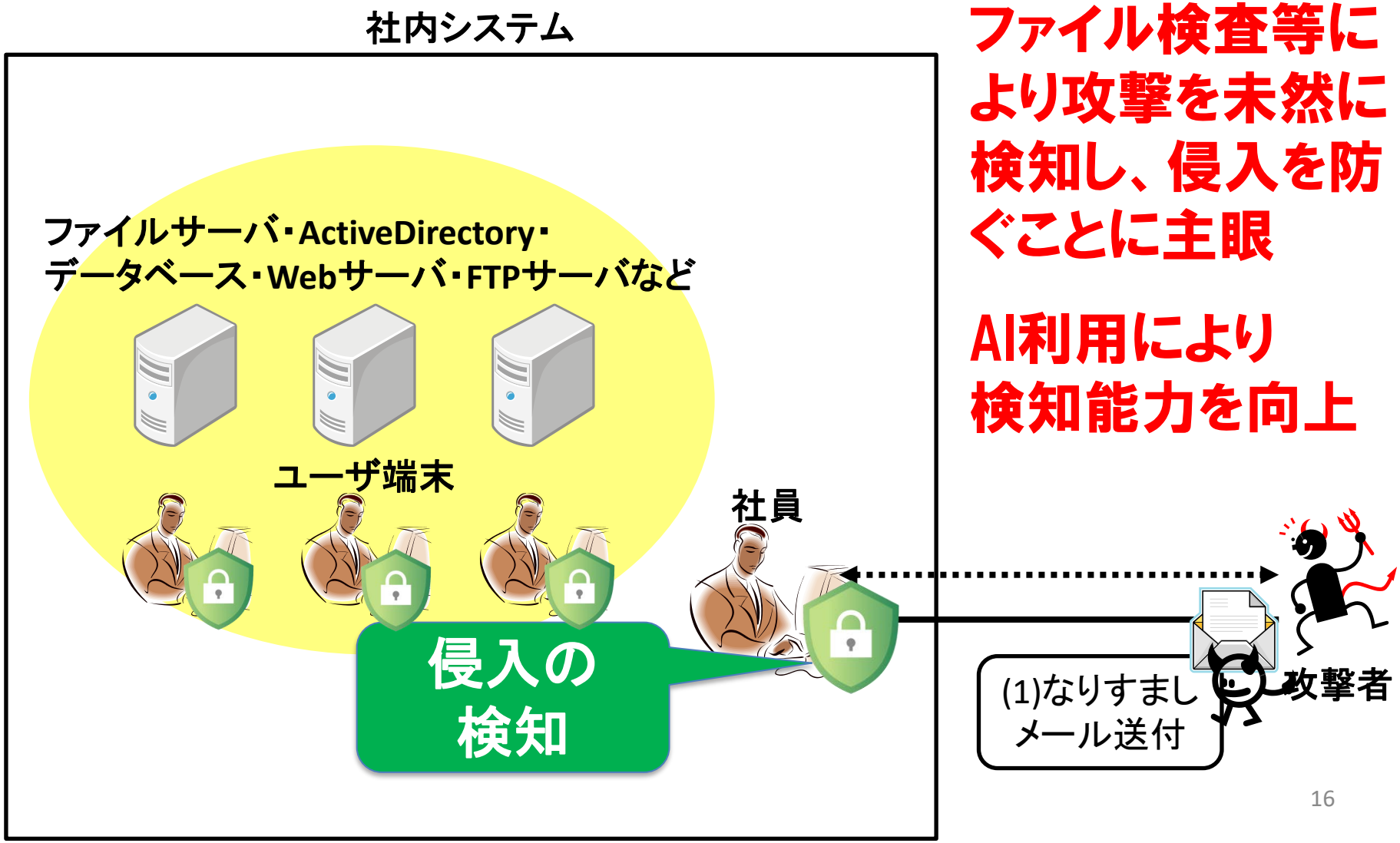
参考：詳細な攻撃のモデル化と対策技術の対応関係の分析

MITRE ATT&CK: 米国MITREによりサイバー攻撃の戦略、技術、ツール、攻撃グループなどを体系化したナレッジDB



エンドポイント視点でのサイバー攻撃活動とMITRE ATT&CKの戦略との対応付け

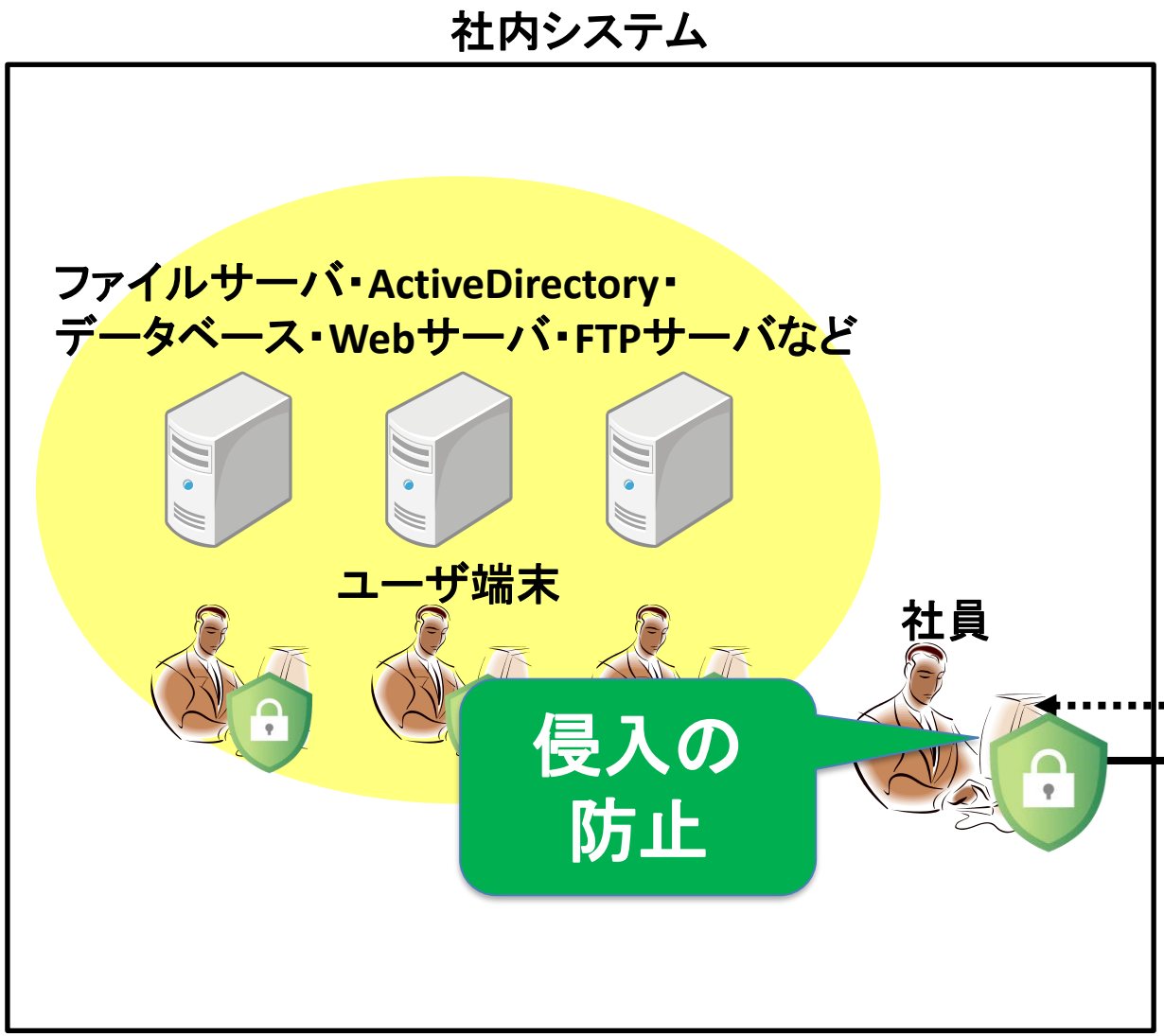
NGAV（Next Generation Anti-Virus）



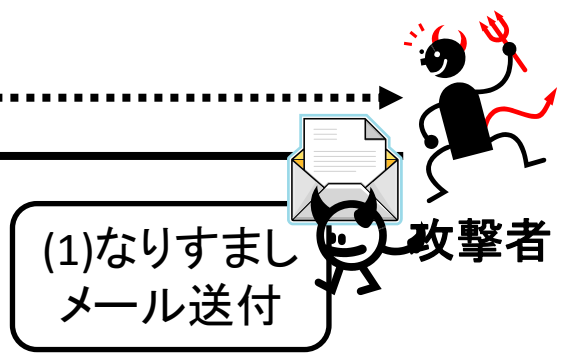
ファイル検査等により攻撃を未然に検知し、侵入を防ぐことに主眼

AI利用により検知能力を向上

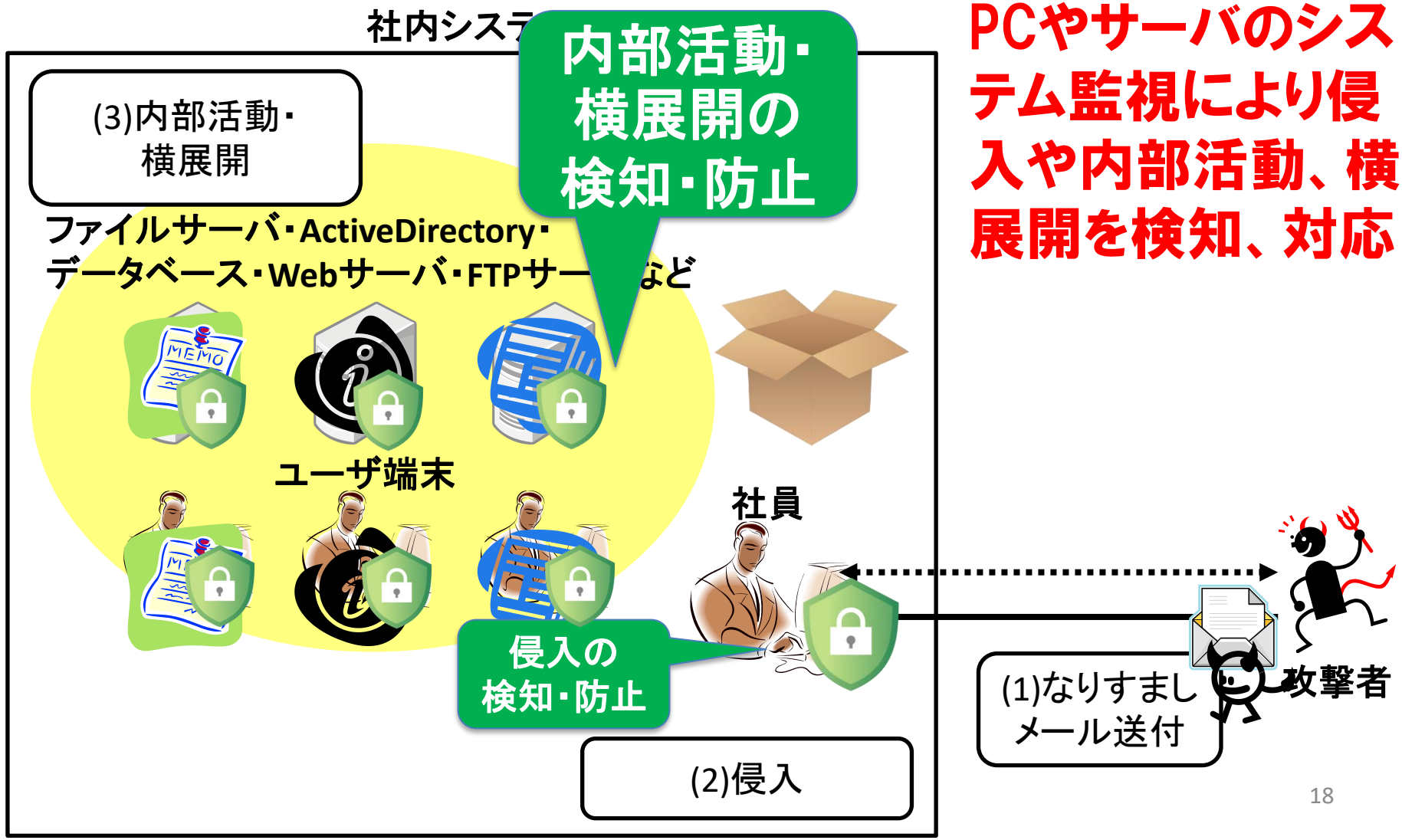
アプリケーション隔離



リスクのある業務（メール・文書閲覧、作成、Web閲覧等）を隔離された環境で実行



EDR（Endpoint Detection and Response）



PCやサーバのシステム監視により侵入や内部活動、横展開を検知、対応

各対策技術の特徴

- **NGAV:** AI等を利用した様々な検知技術を有するが、主眼は**侵入の（未然）検知**。一方、検知をすり抜ける**高度な攻撃の存在**に注意が必要。
- **アプリケーション隔離：**リスクのある作業をそもそも隔離された環境で実施することで**侵入防止**に高い効果が期待される。一方、**攻撃検知能力**については要評価。
- **EDR:** 情報システムの状態を統合的に監視することで異常を検知する。初期侵入後の**内部活動・横展開の検知**に特に効果が期待。一方、攻撃を**未然に防ぐ効果は限定的**。

注意事項

- 実際の製品群は、単一のエンドポイントセキュリティ対策技術だけでなく、複数の対策技術要素の組み合わせ
  →各製品の機能群を正確に把握した上で有用性を判断

- セキュリティ対策機能自体も攻撃の対象となるため、これらの機能自体の正常性を担保する仕組みが必要。
  対策例：ハードウェアベースの検証により正常性を担保

- これらのセキュリティ対策技術のユーザビリティの確保も重要。組織の生産性を低下させず、セキュリティ向上を実現する必要があるが、この観点での評価は今後の課題とする。

まとめ

- 本報告では、エンドポイントセキュリティ対策技術を対象に、攻撃の各フェーズにおける対策の効果を定性的に評価した。
- その結果、NGAVはエンドポイントへの攻撃の存在を迅速に認識するための「検知」に優れており、アプリケーション隔離は、検知に依存せずに侵入を「防止」する性質を有し、EDRは侵入を受けた後に行われる内部活動を検知し、「対処」する機能に優れると判断された。
- 攻撃の増大、多様化、高度化が進む現在、攻撃のすべてを「検知」することは現実的ではないため、確実に防御が可能な「防止」の重要性はさらに高まると思われる。
- 万が一、侵入を受けた際にこれを検知、「対処」する仕組みが必要。
- これらの対策技術を併用することで攻撃活動の各フェーズに対応した、さらに強固なセキュリティ対策が実現できる。