IOWN INTEGRAL
NTT R&D FORUM 2024

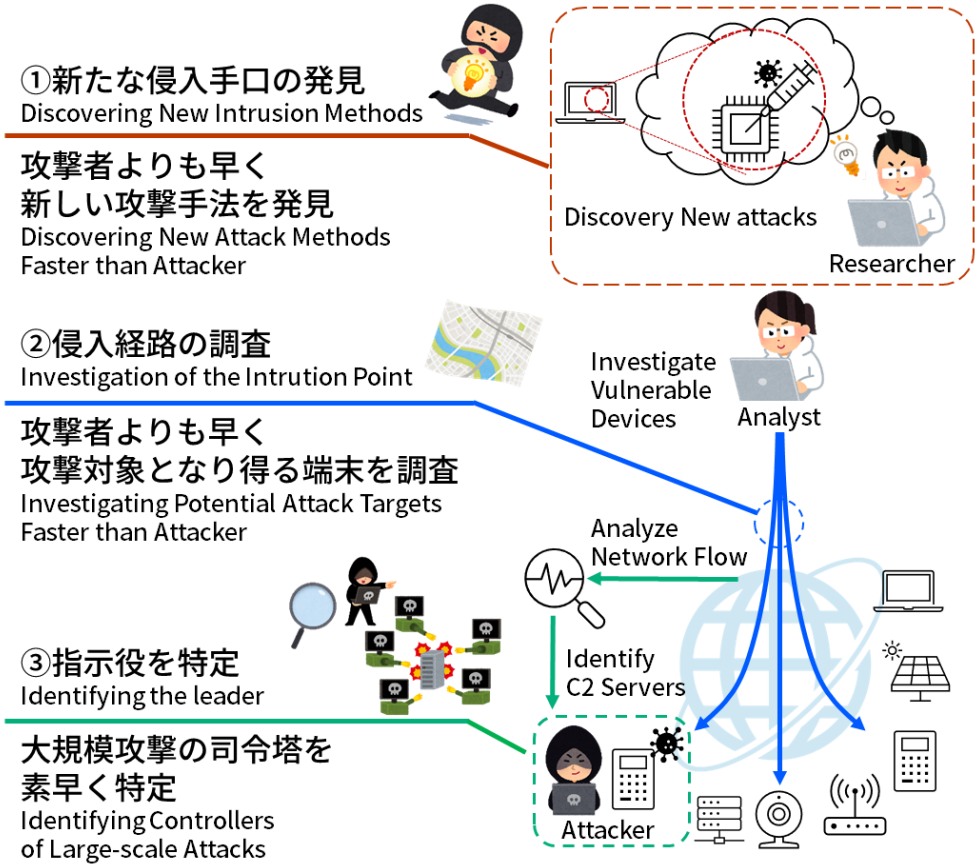
RESEARCH
γ 04-04

攻撃者に先回りしたサイバー攻撃対策

大規模化・巧妙化するサイバー攻撃に
先回りして対策を取り、被害極小化へ

#レジリエンス

サイバー攻撃の被害極小化に向けて
Minimizing the damage caused by cyberattack



///技術課題

サイバー攻撃の被害を極小化するため、従来の対策では難しかった攻撃前の対応を可能にする新しい技術を確立する必要があります。

///研究目標

脆弱性や攻撃元を発見する技術を確立し、迅速な対策を行うことで、サイバー攻撃の被害を極小化します。

---要素技術

①プログラム実行過程で悪性コードを良性プロセスに隠蔽して実行する新たな技術
②ホストのポート利用傾向の共起性を基に効率的なスキャンを実現する独自のスキャン先選定技術
③ネットワークフロー情報から攻撃の司令塔を特定する独自のAI／グラフマイニング技術

---市中技術差異点

①87.5%のセキュリティ製品による検知回避を確認
②既存技術によるスキャン方法と比べて約3倍のIPアドレス・ポート発見率を達成
③判定結果の30%以上は市中インテリジェンスより早期(最大1か月)に検知。

---適用ビジネス

サイバーセキュリティ分野において、
①自社防衛のためのレッドチームでの活用に適用（技術確立：2025年度1Q頃）
②IPv6空間のホストに対する脆弱性調査に適用（技術確立：2024年度3Q頃）
③自社防衛や脅威情報配信サービスに適用（NTTセキュリティから商用サービス提供中。技術改良：2025年度1Q頃）

出展社＝日本電信電話株式会社／NTTセキュリティホールディングス株式会社　関連リンク＝YouTube

問い合わせ先URL