進化する脅威との戦い
～未来の安心をつむぐリサーチチームの活動～

2022年 12月 7日
NTT セキュリティホールディングス株式会社　与沢 和紀
NTT セキュリティ・ジャパン株式会社　羽田 大樹

NTT Security Holdings

Agenda

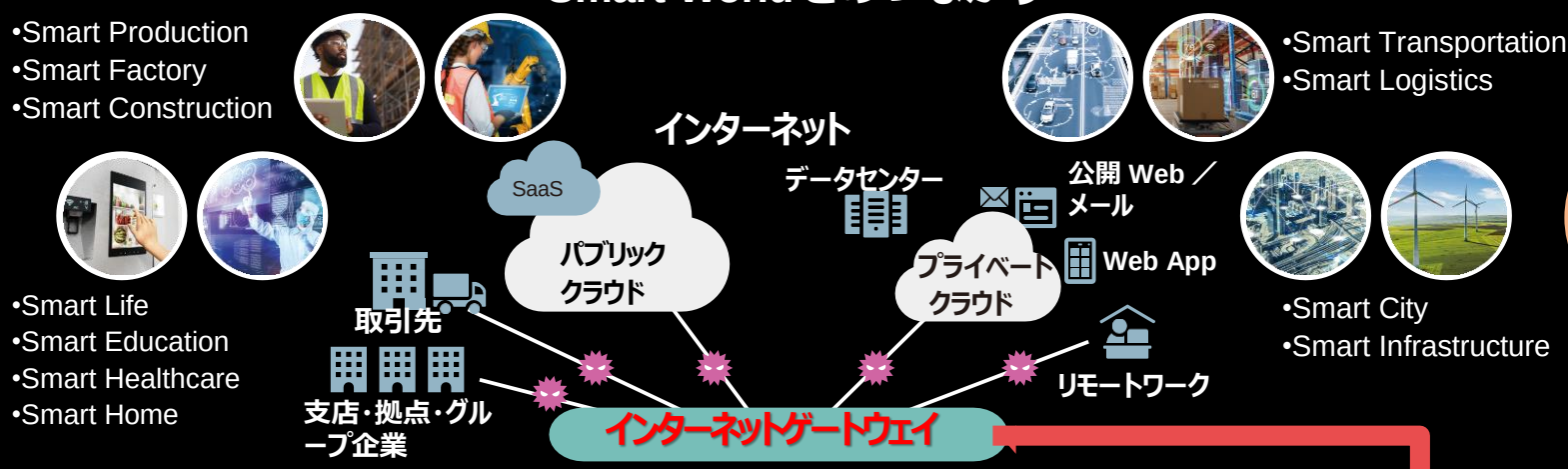
1. NTT セキュリティホールディングスの
   サイバーディフェンス全体像

2. NTT セキュリティ・ジャパンのリサーチ活動
   1. リサーチ活動の取り組み
   2. リサーチ活動の事例
   3. Red Team との連携
   4. リサーチ活動を通じて伝えたいこと

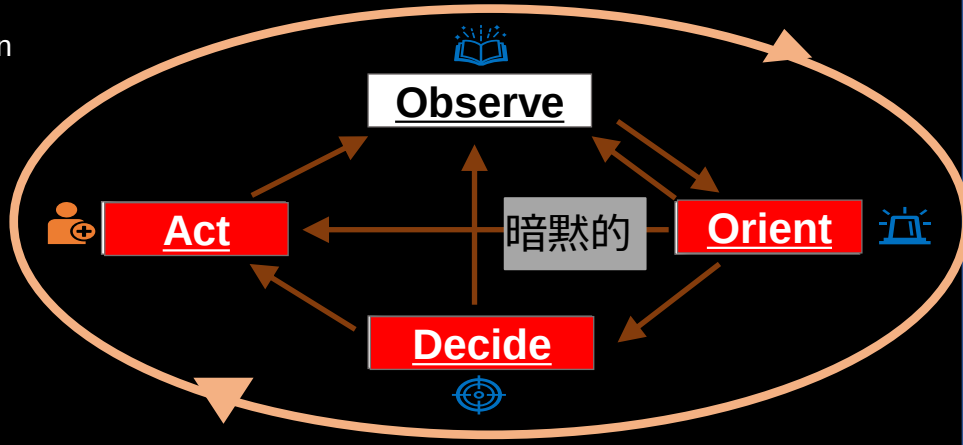
迅速な攻撃検知によりハイブリット社会を守る

NTT Security Holdings

Smart World とのつながり



OODAループ



リサーチ活動

高度攻撃解析（マルウェア解析、IoC収集・分析等）

独自脅威インテリジェンス

SOC リアルタイム分析の全体像と高度化のポイント

EDR Proxy FW UTM Sandbox IPS

大量ログの取得で
脅威発見機会 UP

843,622,263,620 logs
+pcap

Point ①
- 独自シグネチャ/IoC
- パケット詳細分析

1,119,299 alerts

Point ②
- 機械学習と独自 SIEM エンジン
- EDR-SIEM, 遡り分析, pcap 自動分析

305
reports

Point ③
- アナリストによる脅威度・進行度の判定
- EDR 追加分析

詳細な相関分析で
過通知 Down

※2022/10の1か月あたり実データ
（Global）

NTT Security Holdings Functions and Roles

NTT Security Holdings

NTT Group

docomo business | NTT Communications | NTT EAST WEST | NTT DATA Trusted Global Innovator | NTT Anode Energy | NTT FACILITIES | NTT FINANCE

NTT Global IP Backbone

NTT Honeypod

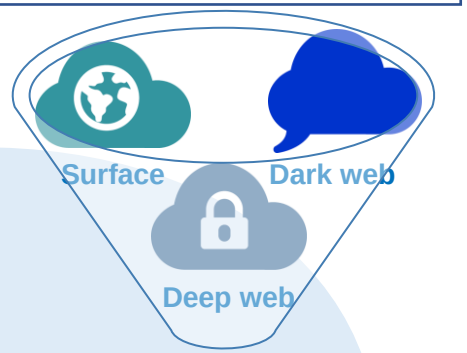
TI Alliance Partner

CYBER THREAT ALLIANCE | RED SKY ALLIANCE | Microsoft | EUROPOL EC3 European Cybercrime Centre | NCFTA

Other technical Partner

OSINT | Recorded Future | VirusTotal

Surface / Dark web / Deep web



Global Threat Intelligence Center

Global Threat Intelligence Platform

- Proprietary tools
- Commercial feeds
- Open sources

Real-time sharing among SOC & feed into TI system

- Threat Feed
- Threat Advisories
- Threat Research
- Context
- Prioritization

MSS Platform

SOC

Incident Responders

Consulting Services

NTT R&D

innovative R&D by NTT

NTT CERT

NTT Security Services

Threat Detection	Device Mgmt	Incident Response

NTT Security Holdings

NTT セキュリティ・ジャパンのリサーチ活動について

講演者情報

NTT セキュリティ・ジャパン 株式会社 NTT Security

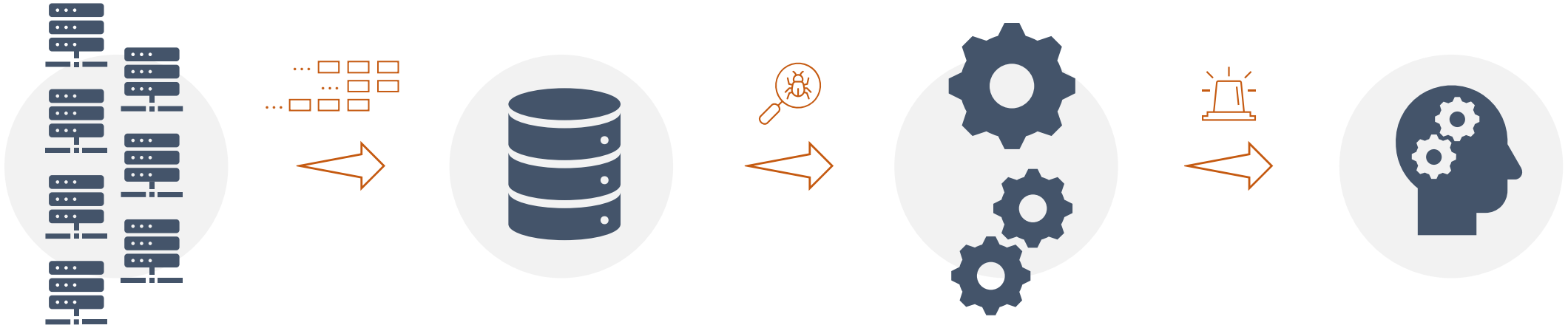
博士（情報学）

羽田 大樹

セキュリティプリンシパル

【経歴等】
- SOC アナリスト, Red Team 等
- BlackHat USA/Europe Arsenal
- 技術評論社「セキュリティのためのログ分析入門」

リサーチ結果を活用する独自アーキテクチャー



デバイス性能最大化

- カスタムシグネチャ
- マスターポリシー
- パケット収集

ストレージ集約

- さかのぼり検知 (1年)
- ブラックリスト抽出
- ナレッジ共有

分析エンジン

- SIEM 分析（AI/ルール）
- ブラックリスト検知
- パケット自動分析

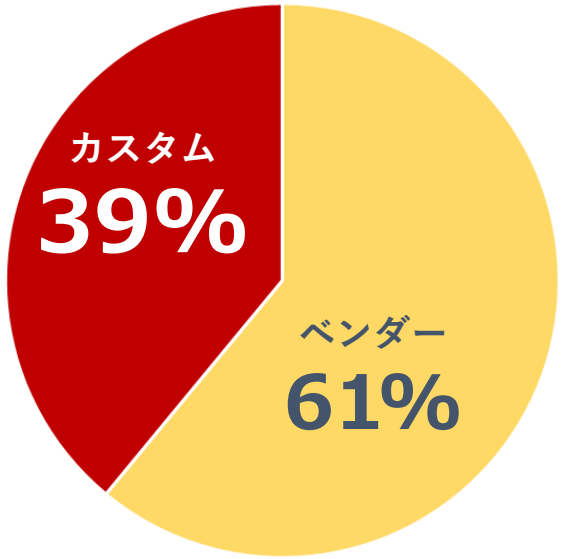
アナリスト分析

- アナリスト分析
- レポーティング自動化
- **インテリジェンス収集**

リサーチ成果の例：カスタムシグネチャ/IoC の検知率

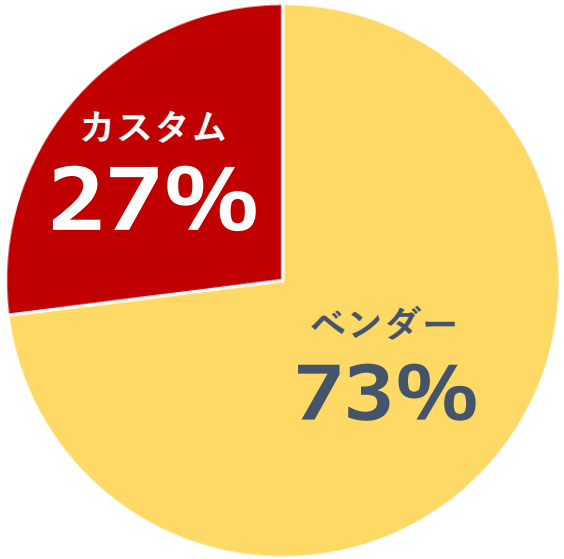
- リサーチの成果をカスタムシグネチャ/IoC として実装
- デフォルトで IPS 39%, EDR 27% (赤色部分) の事象は検知できなかった

IPS シグネチャ



	カスタム	ベンダー
Critical	38%	62%
Serious	17%	83%
Medium	39%	61%
Info	28%	72%

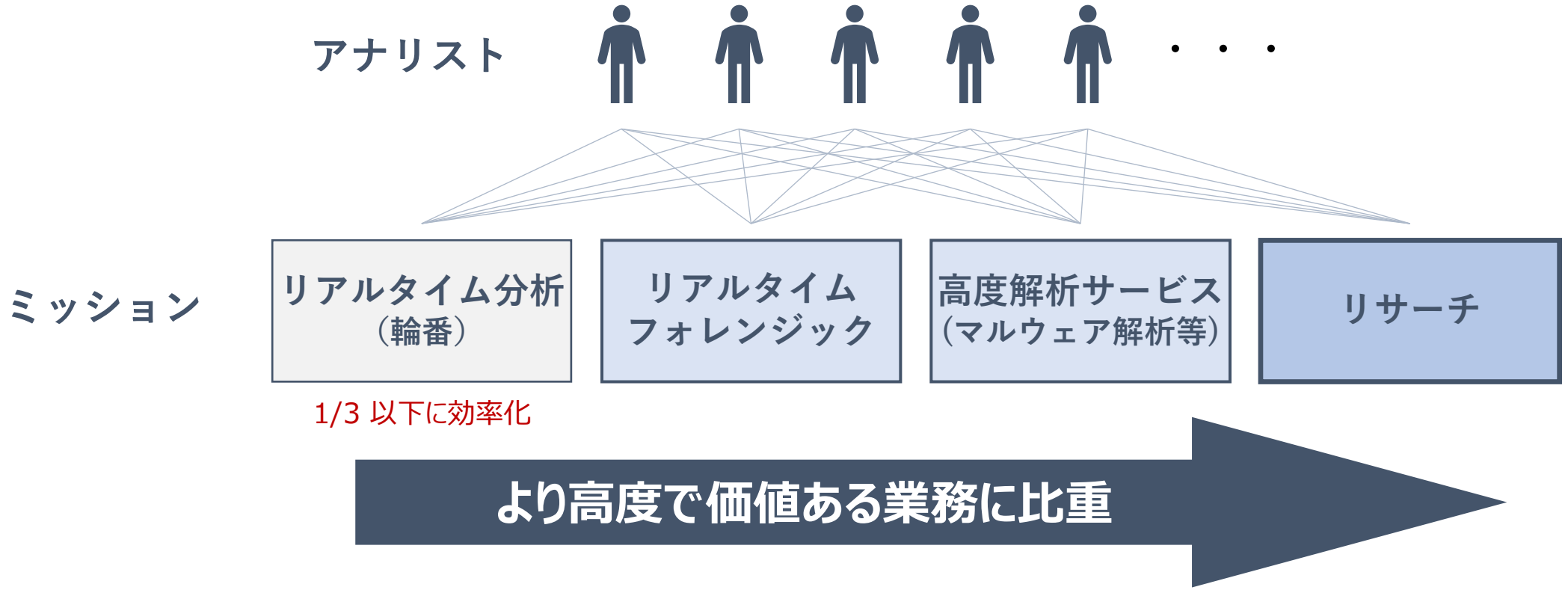
EDR IoC



	カスタム	ベンダー
Critical	15%	85%
Serious	48%	52%
Medium	5%	95%
Info	33%	67%

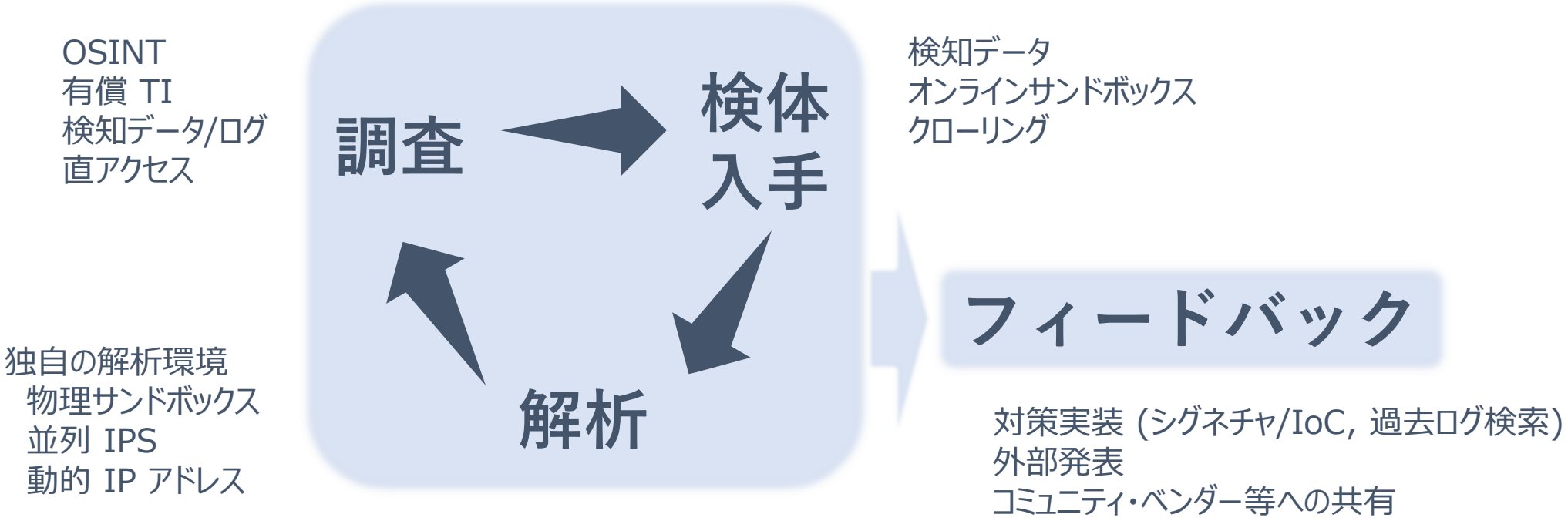
アナリストとリサーチの関係

- 従来のリアルタイム分析は 5年間で 1/3 以下に効率化し, 高度業務にシフト
- アナリスト全員がリサーチ活動に貢献

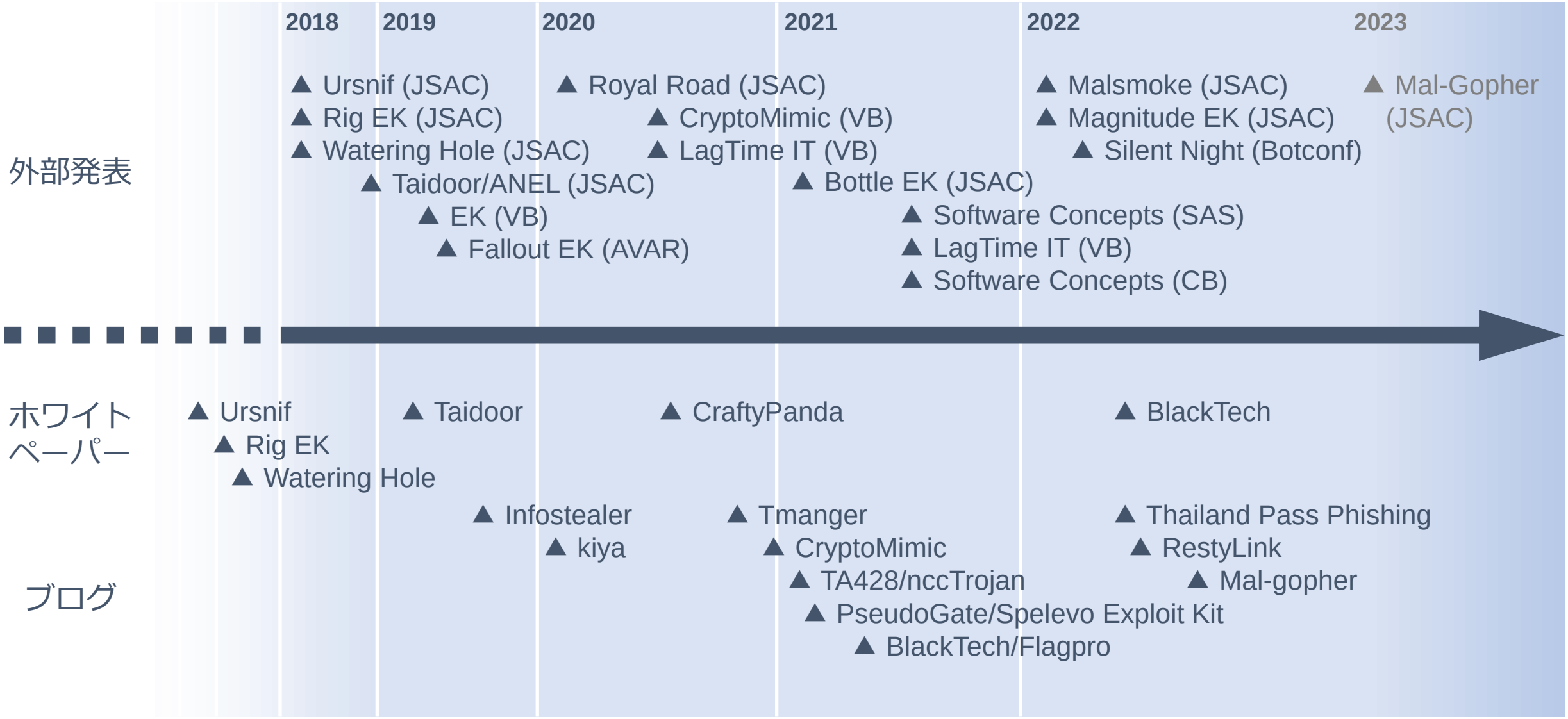


リサーチとは

- 未知の攻撃に対する検知・分析精度の向上のためのナレッジ蓄積
- IP アドレス, ドメイン, ハッシュ, 通信, プロセス, パス, 永続化手法, 等の特徴
- 特に, 日本企業を狙った APT を重点的にリサーチ



リサーチ結果の外部発表（抜粋）



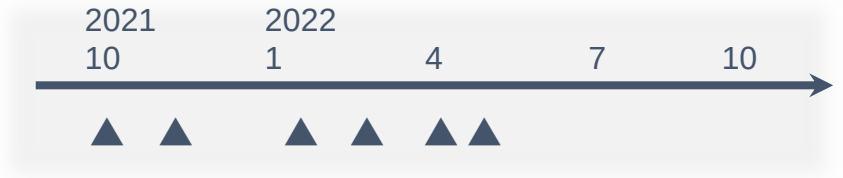
日本を狙う APT グループ (1) BlackTech

- 日本の組織を狙う APT グループ
  - 標的組織を入念かつ継続的に調査
  - 取引先からの標的型メールや海外拠点からの侵害
  - 公開系サーバーへの攻撃, Linux マルウェア, など多様な手法
- 活発なマルウェア開発
  - Flagpro, HeavyROT Loader, SelfMake Loader, IamDown, 等
  - 通信プロトコル, フォーマット, 挙動など仕様は異なるが, 開発者の癖は随所に見られる
- 通信やエンドポイントの特徴を捉える（例: Flagpro）
  - C2 通信: `index.htmld?flag=[Base64]`, `index.htmld?flagpro=[Base64]`
  - エンドポイント: `%TEMP%¥~MY[0-9A-F].tmp`, 等

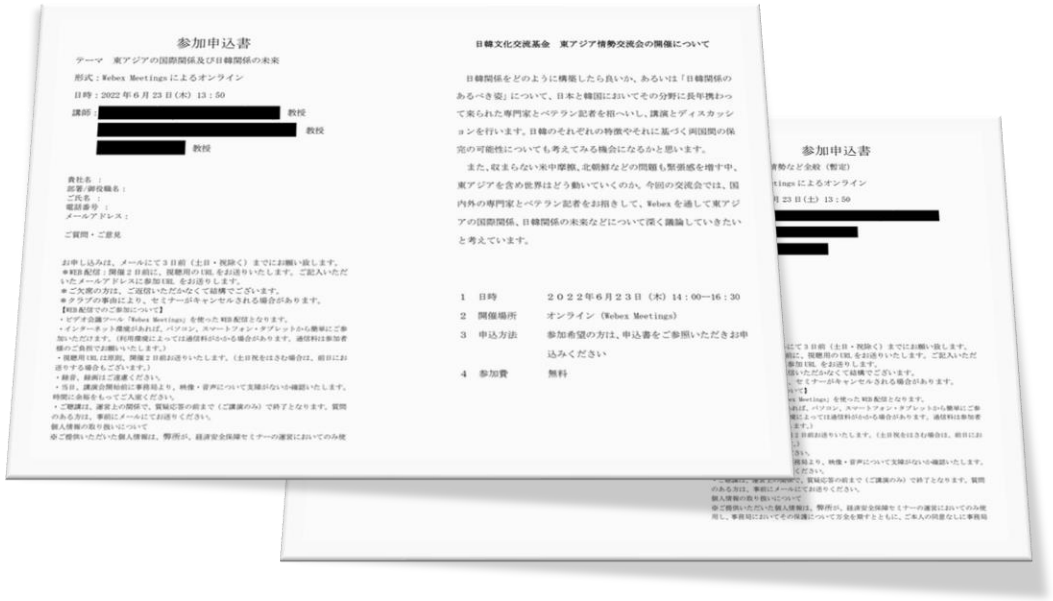
SOC で観測・通知した事例

日本を狙う APT グループ (2) RestyLink

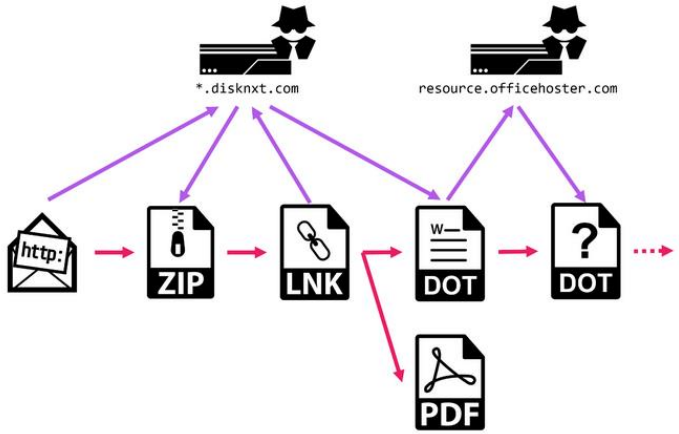
- 日本の組織を狙う APT グループ
  - 2021年10月より継続して関連する攻撃を観測
  - デコイファイルは東アジアの外交に関するセミナー案内
  - 地理的情報を用いたアクセス制御など



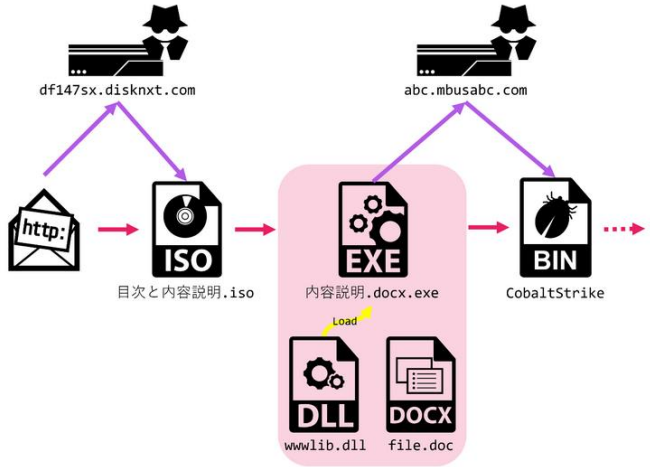
SOC で観測・通知した事例



2022年4月中旬

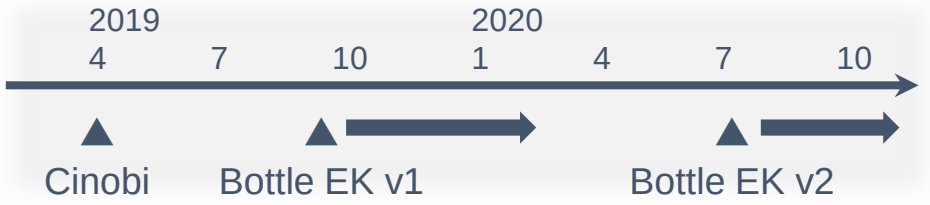


2022年4月下旬

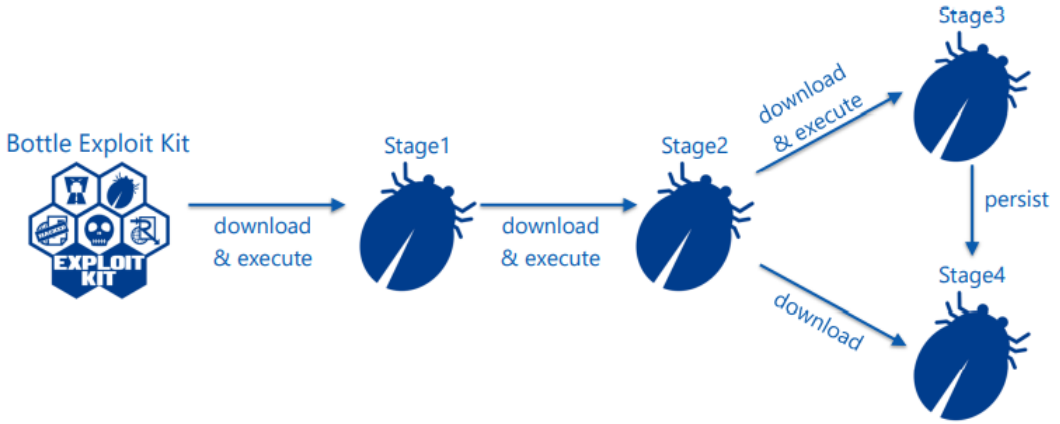


日本を狙う Exploit Kit: Bottle EK

- 日本の組織を狙う攻撃ツール
  - NTT セキュリティ・ジャパンのリサーチャーが世界で初めて発見・報告
- 海外セキュリティ製品の検知が困難
  - 日本語環境チェック, タイムゾーンによる絞り込みが実装
  - SIEM で検知
- その他の検知回避技術
  - HTTPS 通信
  - Shellcode とマルウェアの暗号化
  - Control Flow Flattening



SOC の観測状況



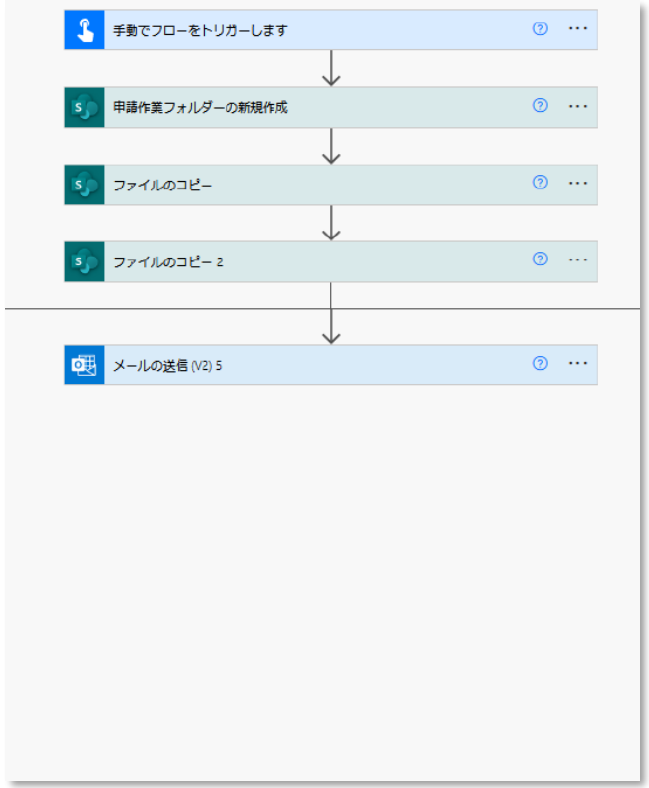
レッドチームとの連携・議論

NTT Security Holdings

- NTT グループに対して内部侵入を調査・検証するチーム（TeamV）
  - 最高レベルの攻撃手法, 検知回避手法に対する防御側の限界と改善策を議論
  - 個々の技術論において全ての検知・対策技術は回避可能だが, 一連の行動の中でミスや手間取り逸脱した行為が発生し得る
- Lateral Movement の脅威
  - 通信の暗号化, EDR の停止, など痕跡の隠ぺいを徹底
  - 独自プログラムの実装不備による権限昇格（規模や歴史のある組織ほど容易）
  - Mimikatz に代表される典型的な攻撃ツールは本当に発見できるか？
- 対策の不備
  - コンプライアンス機能に対する過大な期待
- UEBA 等の仕組みとリサーチでのインテリジェンスによる対策が有効

Power Automate の脅威

- 攻撃者に Power Automate が悪用される事例
- 豊富な機能, クラウドで完結, 被害者が気づきにくい, ログが残りにくい
- C2 サーバーとの通信も可




AVTokyo 2022 で「Power Automate C2」を発表しました

11月18日, 2022

Hiroki Hada

こんにちは、羽田です。11月3日の AVTokyo 2022 Day2 にて、Power Automate C2 というタイトルで発表しました。Power Automate は Microsoft 365 上で多様なサービスと連携して反復的なタスクを自動化するための強力なプラットフォームで、日常業務を簡略化するための様々なコネクタが用意されており、ノーコードでフローを作成できることから多くの利用者がいます。一方で、VECTRA 社のレポート のように、攻撃者に悪用されるケースも報告されています。この Power Automate のコネクタを眺めていて攻撃者に悪用されそうなシナリオを考えたので、今回の発表ではそのコンセプトと簡単なデモを紹介しました。

ちなみに、当日は現地参加が叶わなかったため動画での発表となってしまいました。現地の雰囲気を楽しむことができず残念でしたが、来年こそはオンサイトで発表できるように新たなネタを探したいと思います。

Power Automate の制約

攻撃者がある被害者ユーザーのアカウントで Power Automate にログインできる状況を想定します。この時、攻撃者は Power Automate で新着メールや共有ファイルなどを外部に送信するフローを作成することができます。このフローの実行ログは 28日間残りますが、フロー自体を削除するとログも即座に削除されます。例えば、攻撃者が外部に送信した情報の詳細を知られ

NTT セキュリティ・ジャパン ブログ
https://insight-jp.nttsecurity.com/post/102i1ak/avtokyo-2022-power-automate-c2

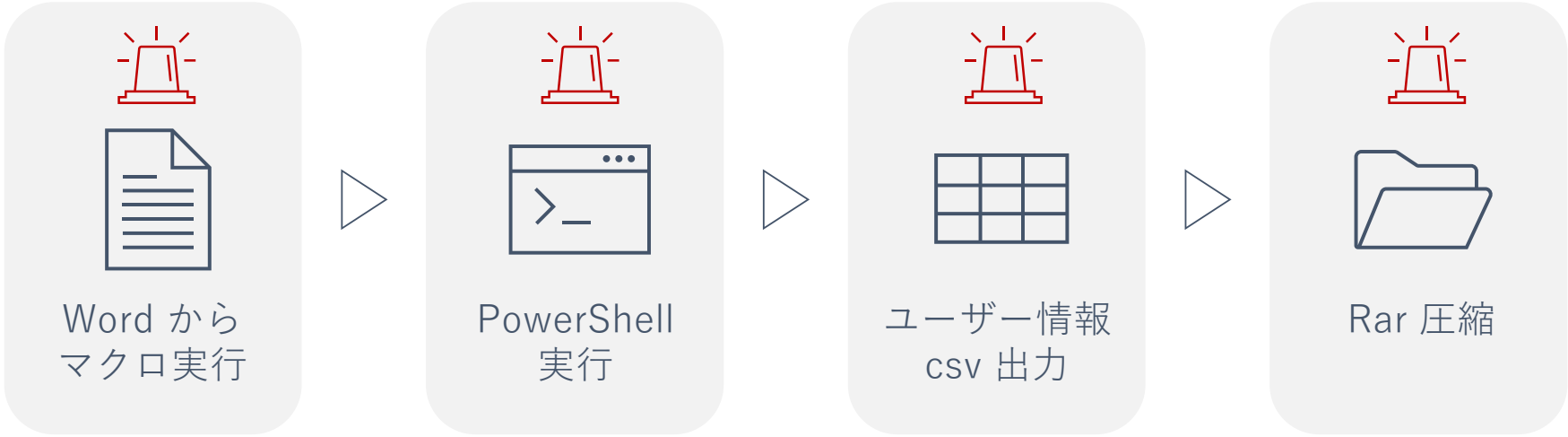
機器や製品の対策には回避手法が存在する

- ネットワーク検知の回避
  - 通信の暗号化（TLS 1.3, Encrypted SNI, DoH/DoT/DoQ）
  - パスワード圧縮
  - 独自プロトコル, 独自暗号化方式
  - ステガノグラフィー
- エンドポイント検知の回避
  - EDR の停止
  - ファイルレスマルウェア
  - サイドローディング
  - 正規の証明書で署名されたマルウェア
  - 特徴を隠すためのダミーコードの挿入

カスタム IoC による標的型攻撃の報告事例

NTT Security Holdings

- 4 個のカスタム IoC が反応



- 標的型メールと不審な実行ファイルをリアルタイム解析し，攻撃と断定して報告

C:¥Users¥...(略)...¥Content.Outlook¥...(略)...¥会議の案内.doc ⇒ 標的型メールを発見
C:¥ProgramData¥Y1U8NZ¥3BP45I.exe ⇒ マルウェアと断定

カスタムシグネチャによる標的型攻撃の報告事例

NTT Security Holdings

- 標的型マルウェアの感染後動作を検知させるカスタムシグネチャを作成
  - 文字列自体には特徴なし
  - ブラウザ依存の通信の特徴の差異を検知（不自然な HTTP ヘッダーの順番）
  - フィールドデータで評価して誤検知の可能性を排除（CDN や WAF 環境を除外）
- たびたび APT を発見

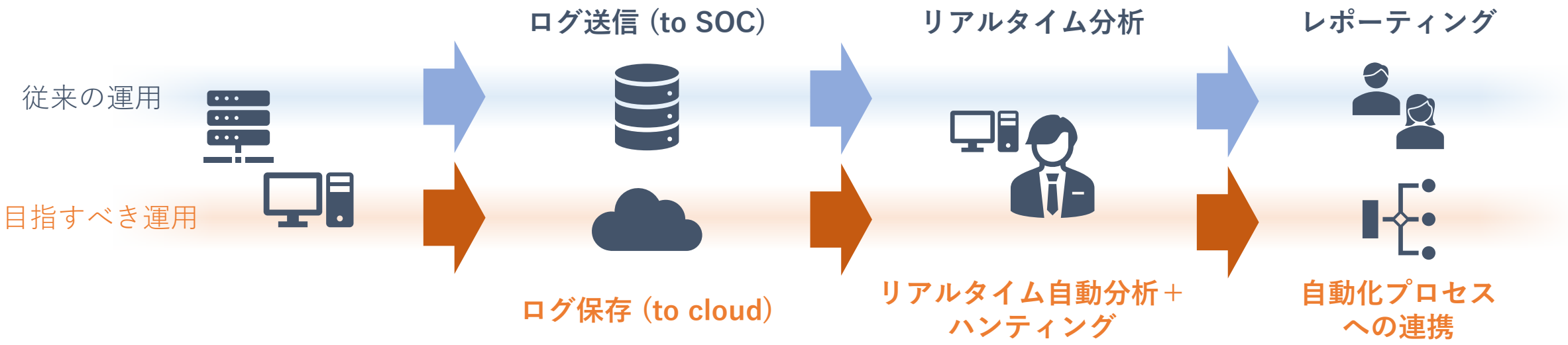
マルウェアの通信例

```
GET /xTqc/gfc.htm HTTP/1.1
Cookie: QbXn=LGZAUY1cWRAf%2BLImuhBhoTeQpOmSuhzhjevInbz2gy6JhsKBs2P%2BaoTI
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Triden
t/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Me
dia Center PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E)
Host: host.example.com
Connection: Keep-Alive
Cache-Control: no-cache
```

→ GET 行の直後に Cookie 行

SOCとエンタープライズ CSIRT が目指すべき連携

- 誤検知を前提とした間接的なログから悪性行為を発見
  - 大量の監査ログ, UEBA, AD/Azure AD からの脅威発見がますます重要に
  - 万能な AI は存在しない ⇒ インテリジェンスを活用したハンティングが最後の砦
- SOC の脅威発見と CSIRT 運用プロセスとの連携
  - 従来のリアルタイム分析 ⇒ 自動化+ハンティングへ
  - CSIRT のインシデント対応プロセス（ヒアリング, 端末交換, その他の独自運用）への接続



ご清聴ありがとうございました