産業分野を含むサイバー攻撃対策実務、特にデジタル・フォレンジックの５W１Hとは

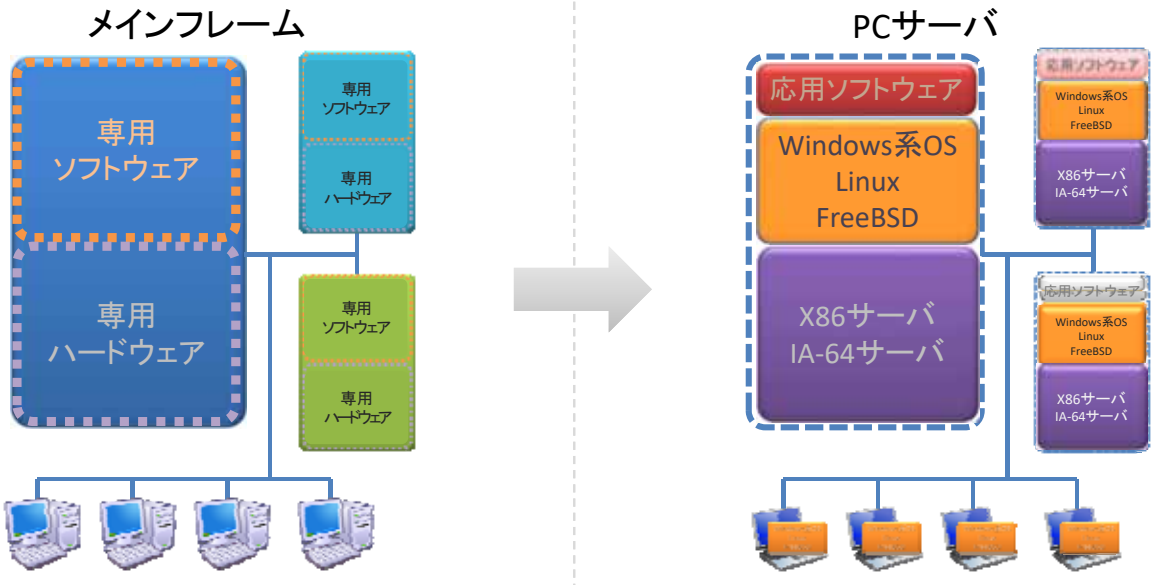
2016年12月

株式会社サイバーディフェンス研究所　専務理事／上級分析官
デジタル・フォレンジック研究会　理事
名和 利男

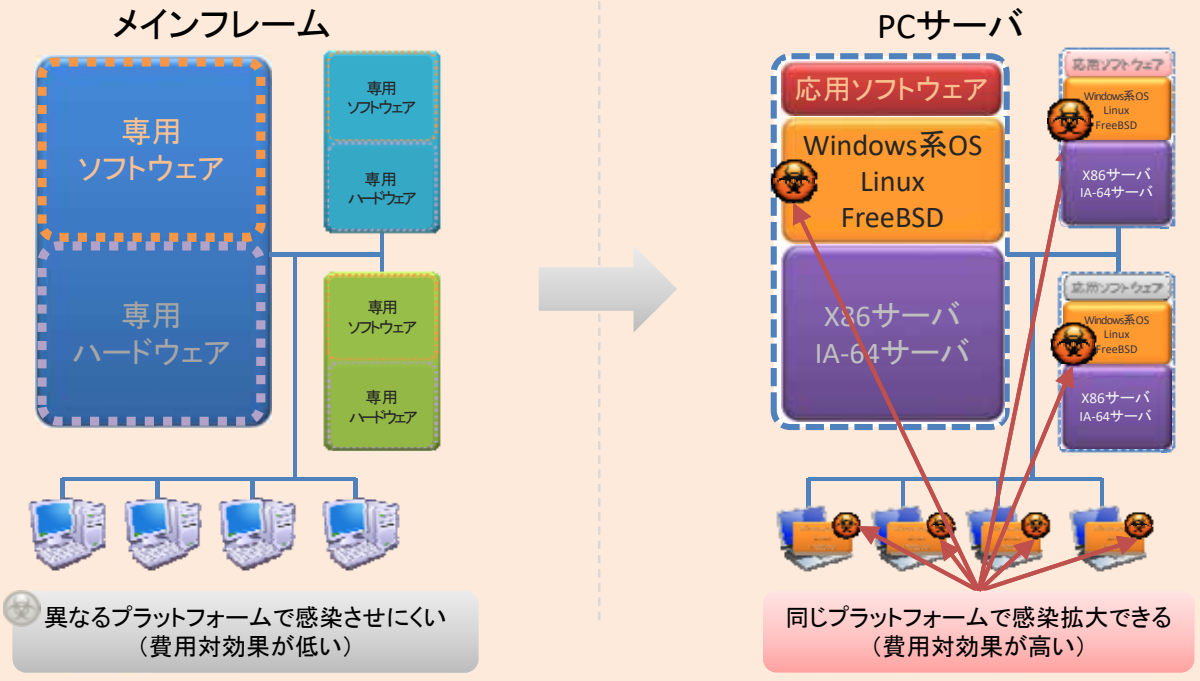
「情報通信システム」と「産業制御システム」における加速度的な変化

認識すべき現場の実態

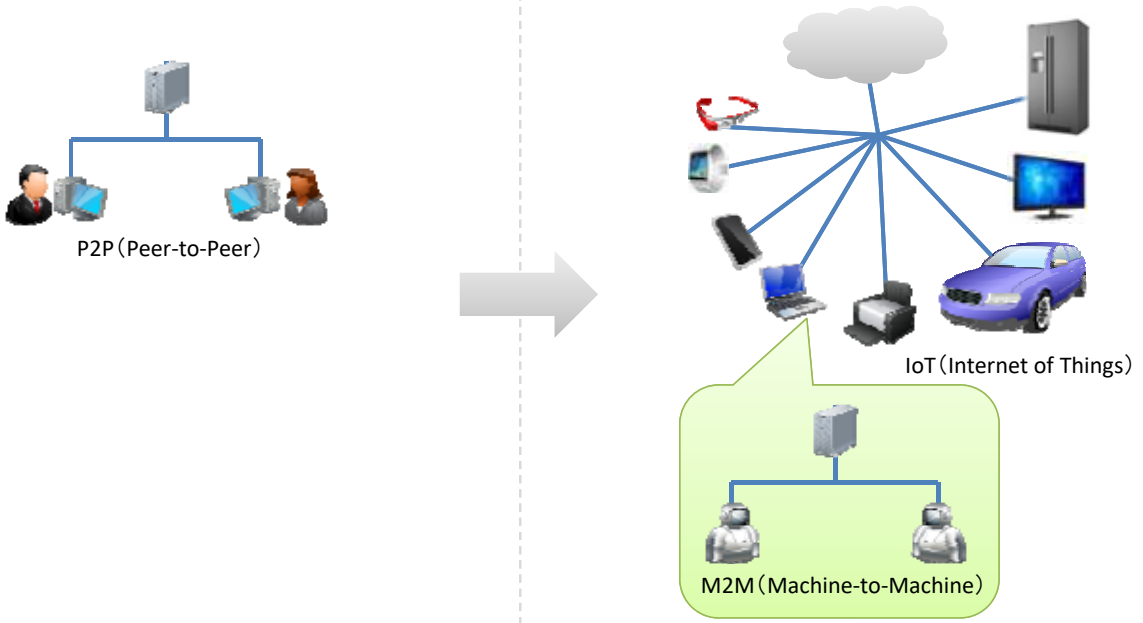
「一体型」から「分割型」へ



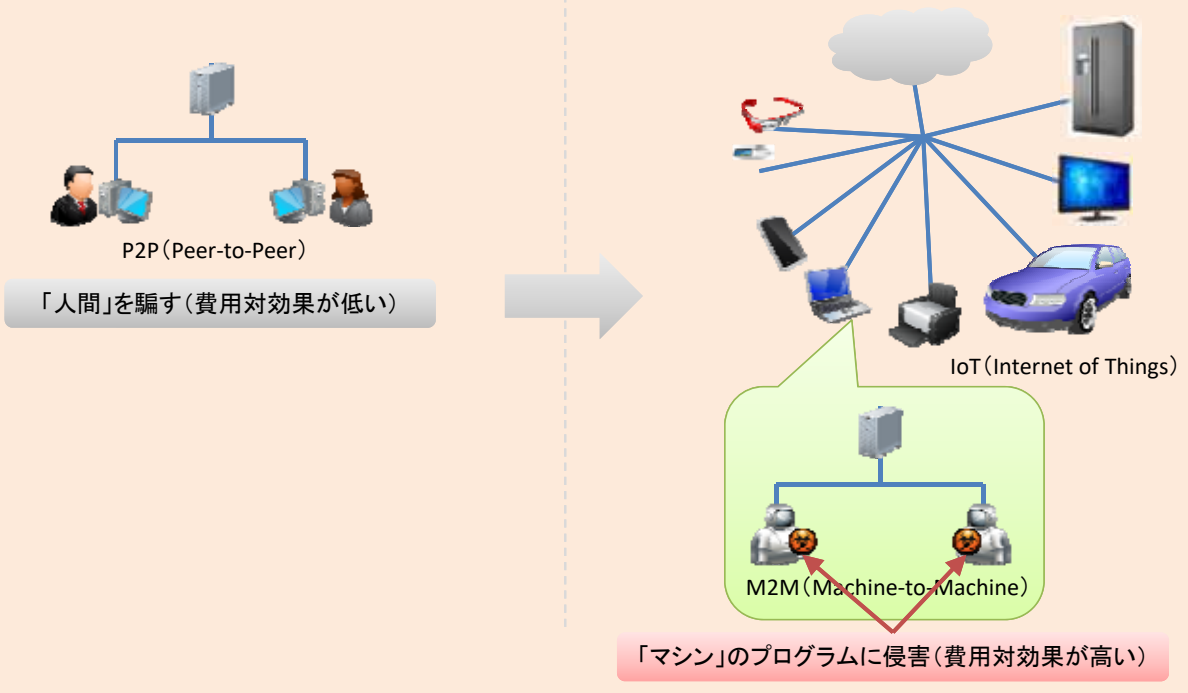
「一体型」から「分割型」へ



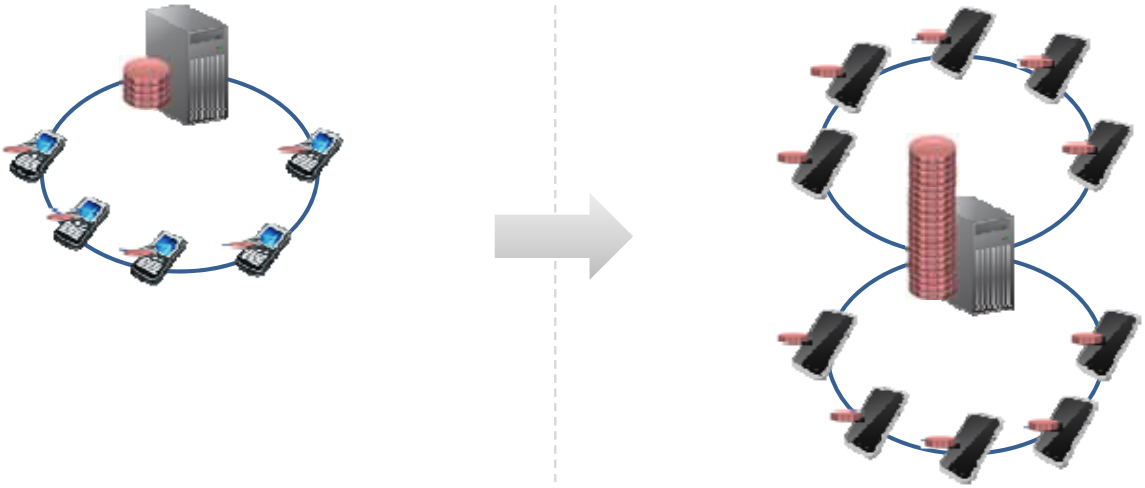
P2P（利用者間通信）からM2M（マシン間通信）へ



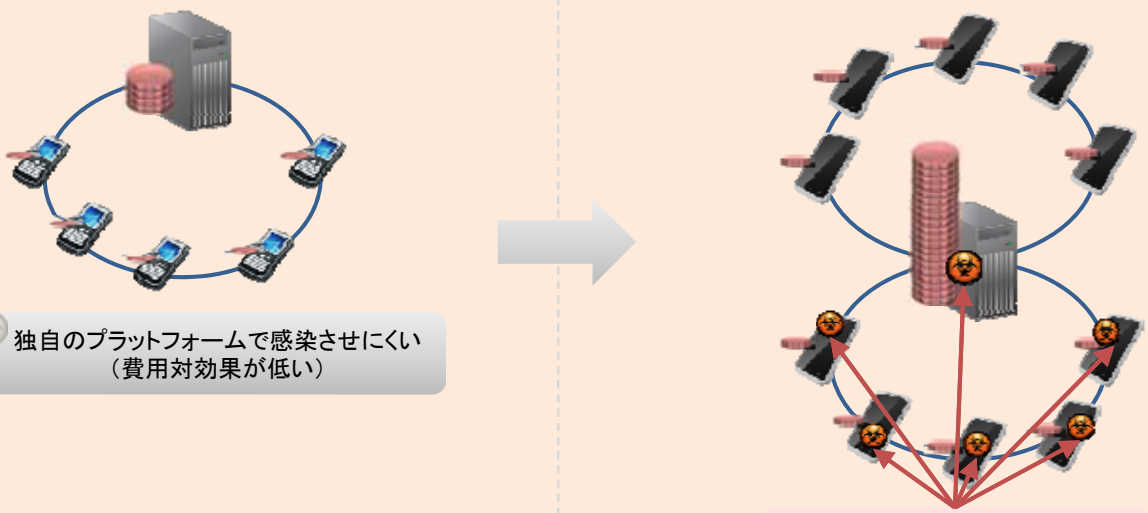
P2P（利用者間通信）からM2M（マシン間通信）へ



「急増するデータ量」



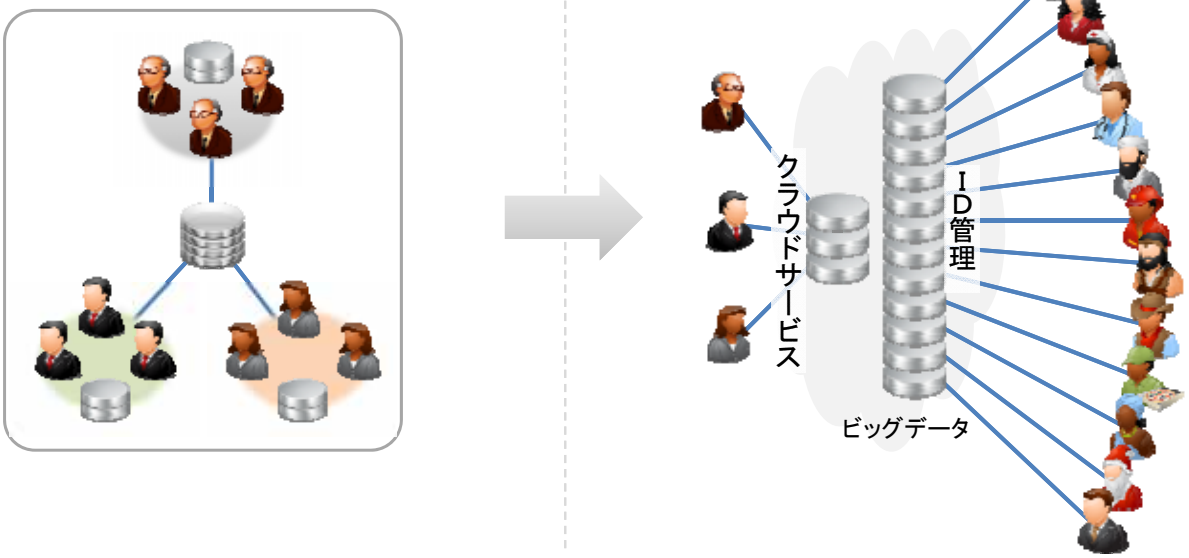
「急増するデータ量」



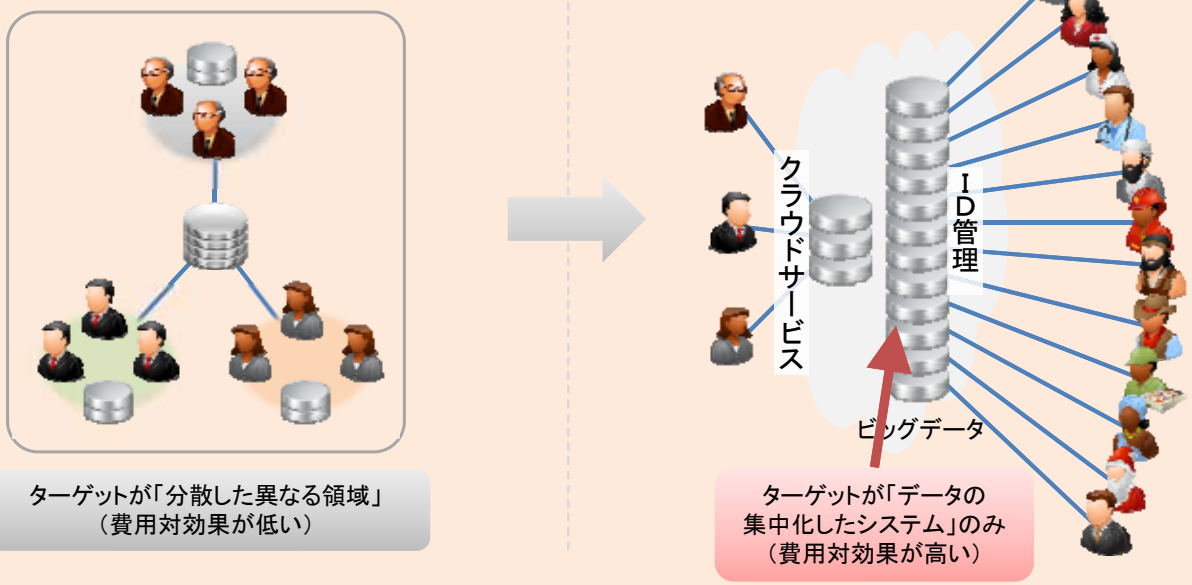
独自のプラットフォームで感染させにくい
（費用対効果が低い）

同じプラットフォームと
興味を引くアプリで感染させやすい
（費用対効果が高い）

「集中化するデータ」と「大規模なID管理」



「集中化するデータ」と「大規模なID管理」



ターゲットが「分散した異なる領域」
（費用対効果が低い）

ターゲットが「データの
集中化したシステム」のみ
（費用対効果が高い）

劇的に変化するサイバー攻撃対策

サイバー攻撃対策の実務について

サイバー攻撃対策の実務 - 全体

事前対応	事中対応	事後対応
サイバー脅威リサーチ • ゼロデイ攻撃リサーチ • サイバー攻撃(犯罪)プロファイリング • 新たなる脅威のリサーチ	**セキュリティイベント分析** • 情報インフラのログ分析 • 内部関係者による脅威の検知 • ログの相関分析と特徴抽出	**コンピュータフォレンジック** • ネットワーク及びコンピュータのポリシー違反検知 • ネットワークフォレンジックとプロトコル分析
ペネトレーションテスト • ネットワークペネトレーションテスト • ソーシャルエンジニアリングテスト • アプリケーションテスト	**インシデントハンドリング** • インシデントハンドリングプロセス(検知 → トリアージ → 対処) • 専任チームによる運用 • 事前訓練(模擬演習)	**他者とのコミュニケーション** • 上位レイアに対するレポート • 他領域の理解と連携 • 国際連携(複数言語を使用)
脆弱性マネジメント • 脆弱性のスキャニング • 脆弱性の評価 • 脆弱性の改善	**マルウェア解析** • マルウェアの収集 • マルウェアの解析(呼び出しAPI、レジストリ変更、プロセス等の調査等) • 特定マルウェア(Web感染型、ファイル感染型)の解析	**ソリューションエンジニアリング** • セキュアネットワークデザイン • 情報セキュリティコントロールデザイン • カスタムオートメーション開発

サイバー攻撃対策実務 - 事前対応

- **「サイバー脅威リサーチ」**
  - WHAT
    - さまざまな情報（Open Source Information）の収集、整理統合、分析、評価とレポーティング。主に、攻撃メカニズムの解明と影響度評価
    - 攻撃者コミュニティへの入り込み、その活動観察、動向評価及び報告
    - 人的ネットワークの徹底的な構築
  - WHO
    - 高い倫理観と強い目的意識 ⇐ 役職とプロジェクト責任の付与
    - 多分野の文化、常識、価値観の理解 ⇐ 他分野コミュニティの参加や国際カンファレンスへの積極的な参加
- **「ペネトレーションテスト」**
  - WHAT
    - 攻撃技術の深い理解と実施可能
    - システム及びネットワークの構築及び運用に関する経験と深い知識
    - 人間行動に関する特性理解と客観的な観察
  - WHO
    - 攻撃技術の理解と実行可能 ⇐ 興味ある技術領域に関する作業割り当て 等
    - システム及びネットワークの構築及び運用に関する業務経験 ⇐ 出向、転職（中途採用）等
- **「脆弱性マネジメント」**
  - WHAT
    - ソフトウェアに関する構造の理解
    - ソフトウェアの運用特性の理解、及び業務（運用）への影響度評価
  - WHO
    - ソフトウェア開発の業務経験 ⇐ 出向、転職（中途採用）等

サイバー攻撃対策実務 - 事中対応

- **「セキュリティイベント分析」**
  - WHAT
    - ネットワーク及びシステムの監視業務の経験と深い知見・ノウハウ
    - 監視装置等の出力データの収集、分析、評価及び報告
  - WHO
    - 攻撃技術の理解と実行可能 ⇐ 興味ある技術領域に関する作業割り当て 等
    - ネットワーク及びシステムの監視の業務経験 ⇐ 出向、転職（中途採用）等
    - 最低限必要なツールの自己開発 ⇐ プログラム開発の教育機会の提供
- **「インシデントハンドリング」**
  - WHAT
    - インシデントハンドリングの基本的プロセスの理解
    - レスポンダーズマインド（Responder's mind）の醸成
    - 管轄領域の業務に関するプロセス及び環境の理解と一定レベルの影響力の保有
  - WHO
    - CSIRT と知見・ノウハウの習得 ⇐ CSIRT 構築 及び CSIRT コミュニティへの参加
    - インシデント対応の経験 ⇐ サイバー演習の実施或いは積極的な参加
- **「マルウェア解析」**
  - WHAT
    - ハードウェア及び基本ソフトの徹底的な構造理解
    - プログラム開発及びネットワーク構築に関する深い知見とノウハウ
    - 解析技術及びツールの理解と活用
  - WHO
    - プログラム開発及びネットワーク構築に関する経験 ⇐ 自前サーバの構築及び運用 等
    - 解析作業に対する強い興味 ⇐ 興味を持つ作業の割り当て
    - 最新技術と動向の情報収集 ⇐ 国際カンファレンスへの積極的な参加

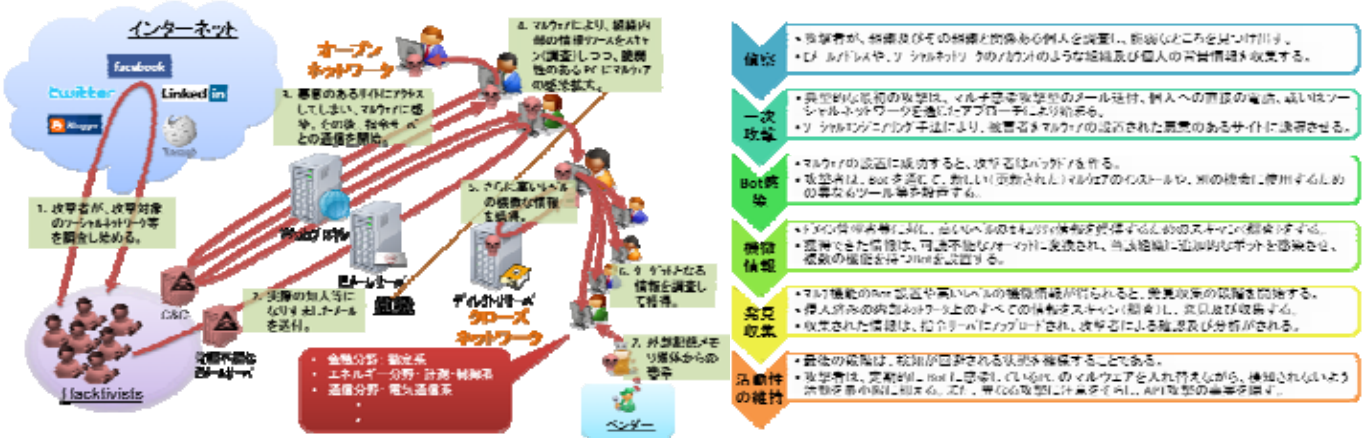
サイバー攻撃対策実務 - 事後対応

- **「コンピュータフォレンジック」**
  - WHAT
    - ハードウェア及び基本ソフトの徹底的な構造理解
    - フォレンジック技術とツールの理解と活用
  - WHO
    - 解析作業に対する強い興味 ⇐ 興味を持つ作業の割り当て
    - コンピュータフォレンジックの現場経験 ⇐ フォレンジック経験者の活動への同行と支援
    - 最新技術と動向の習得 ⇐ 国際カンファレンスへの積極的な参加
- **「他者とのコミュニケーション」**
  - WHAT
    - 他のレイア層（マネジメント、他の事業分野、安全保障、政府関連 等）の内情理解
    - 複数の言語能力（英語、中国語、ロシア語、スペイン語、韓国語 等）
    - 他国のエキスパートとのコミュニケーション維持
  - WHO
    - 国際コミュニケーション能力向上 ⇐ 国際的なコミュニティ及びカンファレンスへの積極的な参加
    - 言語能力教育 ⇐ 多国語スクールへの入学
- **「ソリューションエンジニアリング」**
  - WHAT
    - 最新のソリューションプロダクト及びサービスの深い知識と実装に関する知見
    - セキュリティを意識した開発手法の知見と実装経験
  - WHO
    - 製品及びサービスに関する知識習得 ⇐ さまざまなカンファレンスやセミナーへの積極的な参加
    - 改善提案の立案と実施支援の経験 ⇐ ソリューションエンジニアリング経験者の活動への同行と支援

例：「サイバー攻撃リサーチ」の活動（例）

- 恒常的なリサーチ業務
  - 確認するサイバー脅威に関する記事：200以上／1日
  - 作成するサイバー脅威インテリジェンスレポート：　3つ以上／1ヶ月
  - 国際的なエキスパートとやり取り：4通以上／1日、5コール以上／1週間
  - 国際的なコミュニティ活動時間：5時間以上／1週間
  - 国際カンファレンスへの参加回数：4回以上／1年

- 最近のサイバー攻撃（米国：APT、日本：標的型攻撃）の挙動メカニズムに関するリサーチ（一般化したもの：一部）



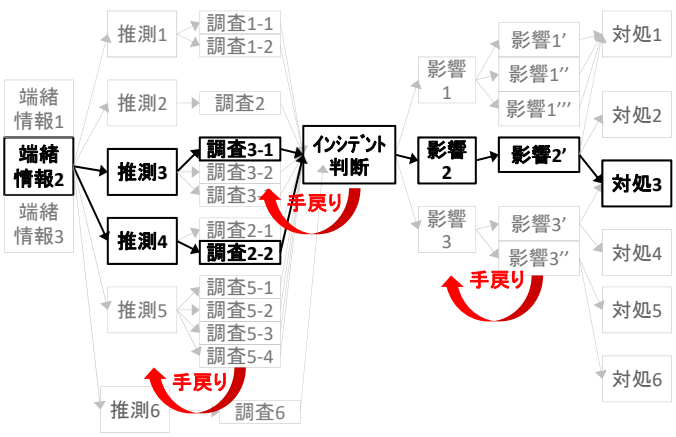
例:「(現場の)インシデントハンドリング」の活動

- 「インシデントの検知(Detect)」に関するプロセス設計

サブプロセス	サブプロセス 要求事項	記述すべき手続き	キーパーソン	利用技術
D1:イベントの認識(事後対処)	• 指定された職員が、異常活動或いはその恐れを認識し、CSIRTに報告する • 信頼する外部組織がCSIRTに注意喚起や警報を送付する インプット: • 一般的な指標 / アウトプット: • イベント報告	• 指定された職員は、CSIRTに対して情報を報告するための「インシデント報告ガイドライン」に従うこと • 信頼する外部組織は、CSIRTに対して情報を報告するための「運用手続き」と「監視手続き」に従うこと	• イベントを認識し、報告をするために指定された職員 - CSIRT及び支援対象 - 被害或いは影響のあるサイト - 一般的な外部組織 - 信頼ある外部組織 - ITスタッフ - コーディネーションセンター	• イベントを認識し報告するときに利用する技術 - セキュリティツール(IDS等) - デスクトップワークステーション - コミュニケーションチャネル、必要の都度暗号化(Email, ビデオ会議グループウェア)
D2:情報の受領	• 指定された職員が、報告をレビュー及び事実確認し、何をするかを決定する • 自動化ツールが、報告を受領し「T:イベントのトリアージ」に転送する インプット: • 「D1:イベントの認識」からのイベント報告 • イベント報告 • 一般的な対処要請/報告 / アウトプット: • イベント情報 • 再割当てされたイベント • 終了したイベント	• 指定された職員は、報告をレビュー及び事実確認し、何を行なうかを決定するための「報告収集手続き」に従うこと • 指定された職員は、イベントを再割当て及び終了するための「適切な手続き」に従うこと • 自動化ツールは、報告を受領し転送するための「報告収集手続き」に従うよう設計されていること	• 報告された情報を受け取るために指定された職員 - ヘルプデスクスタッフ - CSIRTのトリアージスタッフ/ホットラインスタッフ/マネージャ/インシデントハンドラー - 情報セキュリティ管理者 - システム/ネットワーク管理者 - 第三者の伝言サービス - コーディネーションセンター	• 報告された情報を受領、レビュー及び何をすべきかを決定するために利用される技術 - セキュリティツール(Whois、ポート番号リスト、暗号) - コミュニケーションチャネル、必要の都度暗号化 - データベース - 意思決定支援ツール
D3:指標の監視(事前対処)	• 指定された職員が、事前対処として、発生し得るイベントの指標に関する様々な情報源を監視する • 自動化ツールが、一般的な指標のためにシステム及びネットワークを監視する インプット: • 一般的な指標 / アウトプット: • イベント指標	• 指定された職員は、一般的な指標を監視及びレビューするための「運用手続き」に従うこと • 自動化ツールは、一般的な指標のためにシステム及びネットワークを監視するための「運用手続き」に従うこと	• 事前対処として、監視するために指定された職員 - ITスタッフ - 選抜されたCSIRTスタッフ - 第三者 - コーディネーションセンター	• 一般的指標を監視するときに利用する技術 - セキュリティツール(IDS等) - データ操作ツール - インターネット検索エンジン - コミュニケーションチャネル、必要の都度暗号化 - データベース/アーカイブ - 自動化ツール
D4:指標の分析	• 指定された職員が、イベント指標をレビュー及び分析し、情報をどうするかについて決定する • 自動化ツールが、イベント指標を分析し、「T:イベントのトリアージ」に転送する時期を決定する インプット: • イベント指標 / アウトプット: • イベント情報 • 再割当てされたイベント • 終了したイベント	• 指定された職員は、イベント指標をレビュー及び分析し、何を行なうかを決定するための「運用手続き」に従うこと • 指定された職員は、イベントを再割当て及び終了するための「適切な手続き」に従うこと • 自動化ツールは、イベント指標を分析し、「T:イベントのトリアージ」に転送する時期を決定するための「運用手続き」に従うこと	• 指標を分析するために指定された職員 - ITスタッフ - 選抜されたCSIRTスタッフ - 第三者 - コーディネーションセンター	• イベント指標をレビュー、分析し、何をすべきか決定するために利用される技術 - コミュニケーションチャネル、必要の都度暗号化 - データベース - 意思欠低支援ツール • 自動化検知ツール

例:「(組織全体の)インシデントマネジメント」の活動

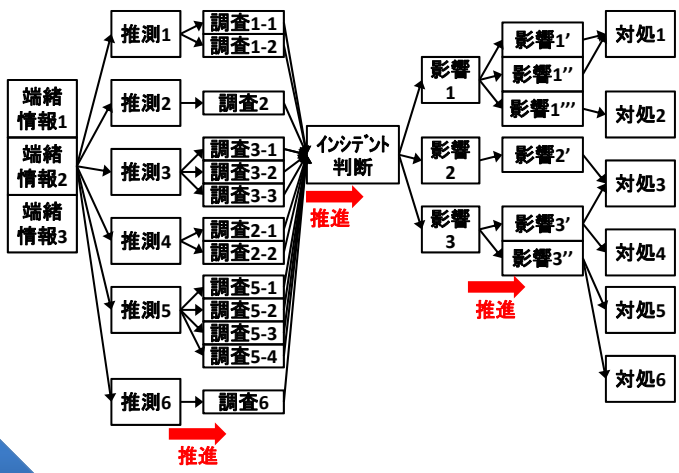
CSIRT体制に実務能力なし



*認識が可能な領域(太文字)が少なく、認識が不能/困難な領域が多い(薄文字) → 手戻りが多い

- 端緒情報、推測、調査、影響評価のすべてにおいて、発生可能性のあるサイバー攻撃に対する対処が限定的或いは的外れとなる。
- そのため、サイバー攻撃が発生した場合、潜在化及び残存する攻撃挙動への対応が事実上できないため、被害が甚大化する。

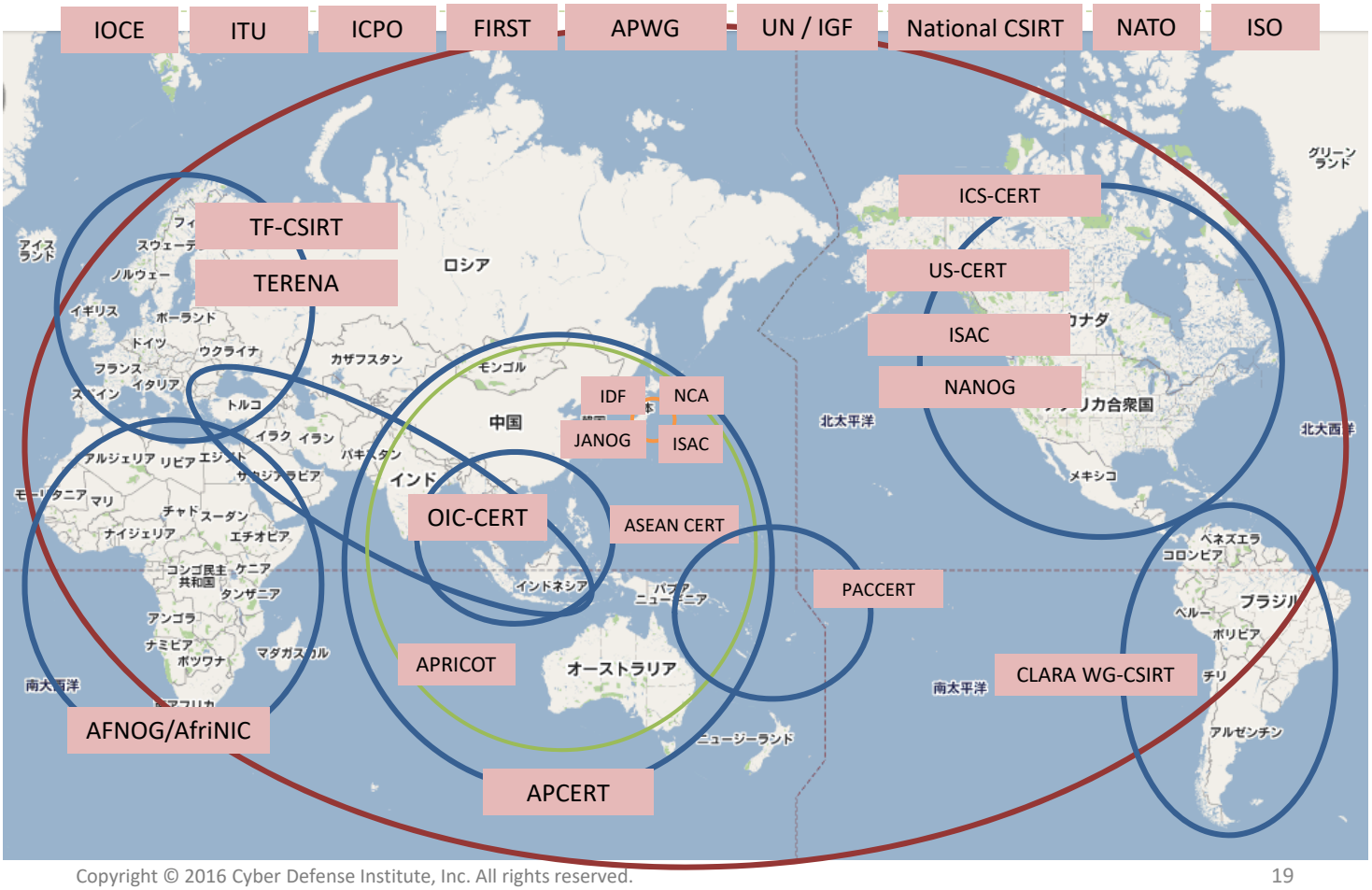
CSIRT体制に実務能力あり



*網羅性の高い認識が可能 → 手戻りが少ない

- 端緒情報、推測、調査、影響評価の充足度が向上し、発生可能性のあるサイバー攻撃に対する対処の網羅性及び適切性が高まる。
- サイバー攻撃が発生した場合、潜在化及び残存する攻撃挙動が局限化でき、被害が限定的になる。

例：「他者とのやり取り」（民間ベースの国際的・国内連携）



研究会1の議論

「産業分野を含むサイバー攻撃対策実務、特にデジタル・フォレンジックの5W1Hとは」

産業分野を含むサイバー攻撃対策実務、特にデジタル・フォレンジックの5W1Hとは

- **いつ（When）**
- **どこで（Where）**
- **だれが（Who）**
- **なにを（What）**
- **なぜ（Why）**
- **どのように（How）**

有識者によるミニ講演及び
パネルディスカッションを通じて、
重要事項を考察します。

本資料に関する連絡先

名和 利男（Toshio NAWA）

情報分析部 部長／上級分析官
サイバーディフェンス研究所

e. nawa@cyberdefense.jp
t. 03-3242-8700
w. www.cyberdefense.jp (office)
www.cirt.jp (response team)