サイバー攻撃（標的型攻撃）対策
防御モデルの解説

平成29年７月

Agenda

1. 標的型攻撃の防御について

1.1.防御モデルの前提

1.2.防御モデルの概要

2. 人・組織対策

2.1.インシデントレスポンスプランニング

2.2.インシデントハンドリング

3. 技術的対策

3.1.事前対策

3.2.検知

3.3.事後対策

1.標的型攻撃の防御について

1.1. 防御モデルの前提

1. 標的型（諜報）攻撃

金銭や知的財産等の重要情報の窃取を目的として特定の標的に対して行われるサイバー攻撃

「具体的な標的に対して行われること」「密かに行われること」

「標的への攻撃指向性が強いこと」

「それらゆえにカスタマイズされた手段で行われること」

2. 攻撃経路

- 標的型メール攻撃
- Drive-by-Download
- 不正コード混入ソフトウェア
- USBメモリ
- 保守業者持込み機器
- クラウドサービス

1.1. 防御モデルの前提

3. 攻撃フェーズ

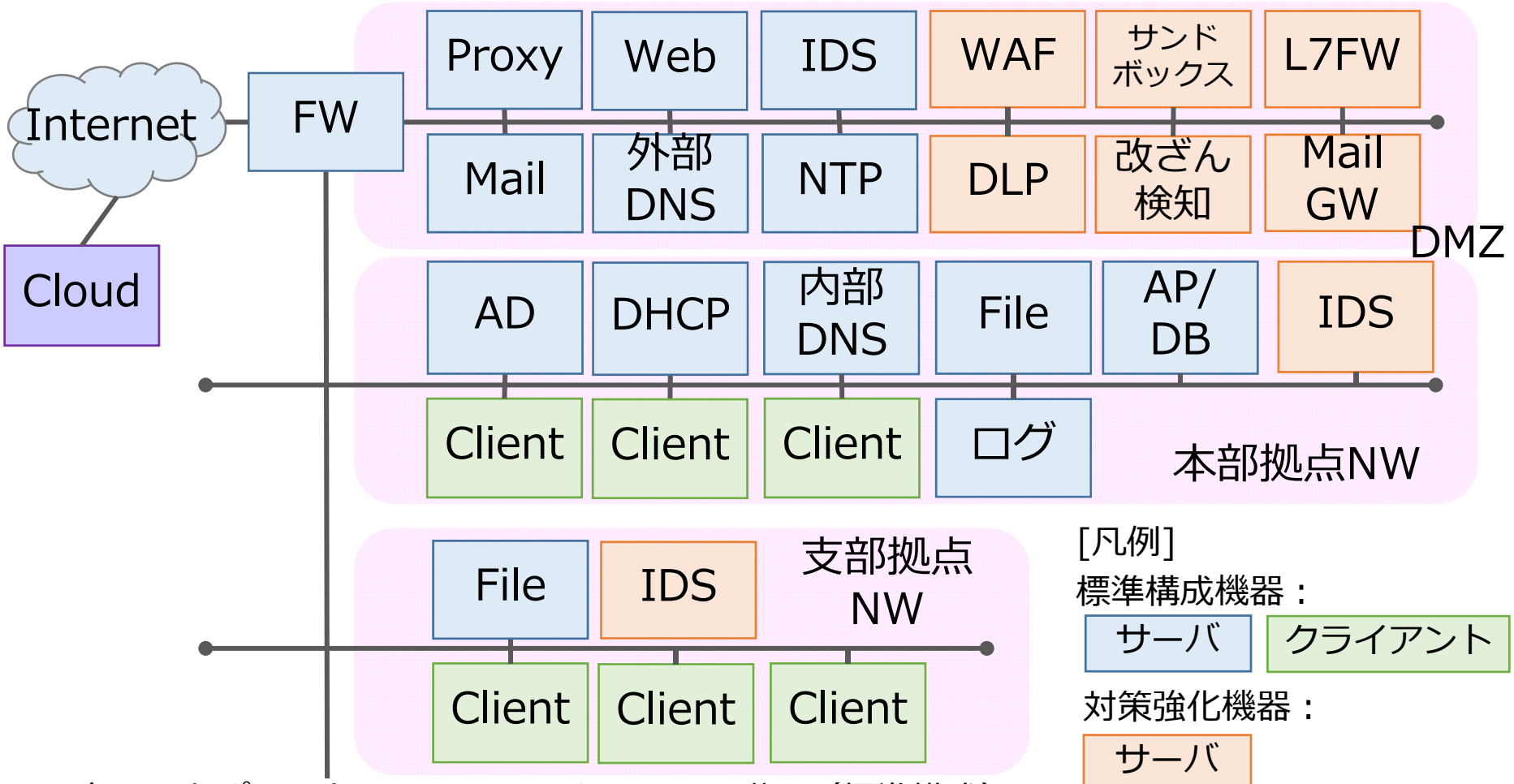
攻撃段階	① ターゲットの情報収集	② ターゲットに対するマルウェアの入込み	③ ターゲット内における足場固め	④ ターゲット内での感染拡大	⑤ C2ホストとの積極的な通信	⑥ 本格的な攻撃実行
攻撃例	●ソーシャルエンジニアリング ●公開ホストに対するペネトレーションテスト	●標的型メール（悪性ファイル添付、悪性サイトリンク） ●Drive-by-Download（サイト改ざんによる悪性サイト誘導やマルウェアダウンロード）	●ドロッパー生成、別マルウェアのダウンロード（マルウェア機能UP） ●ソフトウェア設定変更（再起動時の実行設定による常駐化等）	●バックドア通信経路の確保 ●脆弱性を利用した権限昇格 ●認証情報窃取（ブルートフォース攻撃、パスワードリスト攻撃等）	●検知回避を施したC2通信確立とビーコン通信 ●内部のコンピュータシステムの挙動監視 ●ホスト名取得やプローブによる内部調査	●他のコンピュータシステムへの展開活動 ●取得情報のパッケージ化と暗号化 ●検知回避を施した機密情報の外部送信

1.1. 防御モデルの前提

4. ネットワーク構成・構成機器

■標準構成機器：前提とするLAN構成機器及び導入を推奨する対策機器

■対策強化機器：標的型攻撃対策をさらに強化する構成機器



※ 各エンドポイントには、アンチウイルスを導入（標準構成）

1.2. 防御モデルの概要

■防御モデル：『**人・組織対策**』と『**技術的対策**』で構成

[人・組織対策]

- **■インシデントレスポンスプランニング　⇒　まずは計画**
- **■インシデントハンドリング　⇒　計画実行**

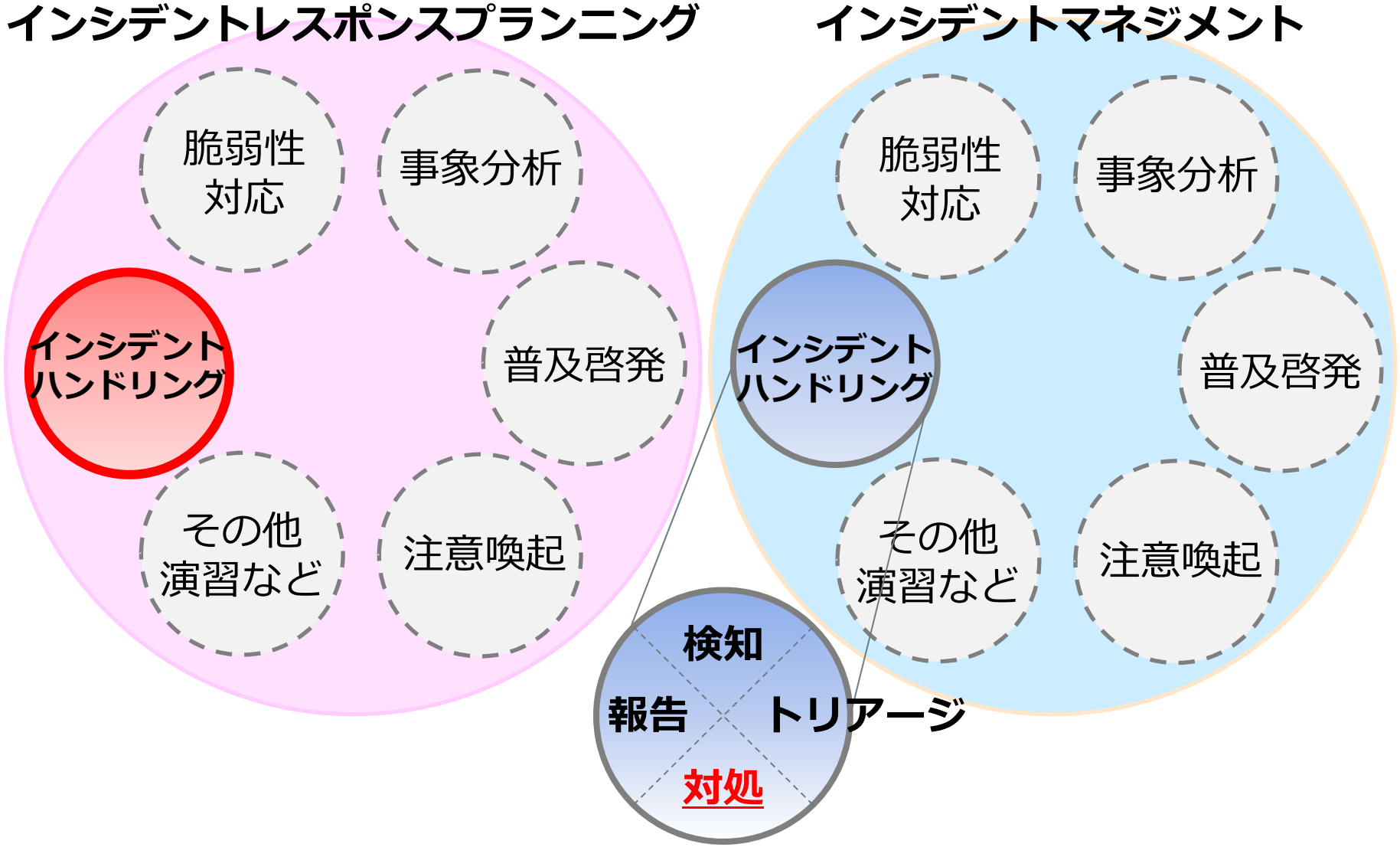
[技術的対策]

- **■事前対策　⇒　被害に遭いにくく（それでも被害は発生する）**
- **■検知　⇒　被害に気付く仕組み（被害の放置・拡大を防ぐ）**
- **■事後対策　⇒　被害に遭っても、被害を最小化・再発防止**

2.人・組織対策

2.インシデントレスポンスの全体像について

■インシデントレスポンス概念の全体像



出典：JPCERTコーディネーションセンター「CSIRTガイド」（一部記載変更（下線付き赤字））

2.1. インシデントレスポンスプランニング

■目的

標的型攻撃被害などのインシデント又はインシデント発生時の、確実かつ迅速なるインシデントハンドリングの実現

■概要

インシデントレスポンスプランニングは、「情報収集」から「活動に係る文書作成と定期レビュー」に至る、以下の５プロセスで構成

※ ①~③はCSIRT体制設置を目的としたプロセス

～ インシデントレスポンスプランニングのプロセス～

①情報収集
②活動への承認獲得
③組織内の現状把握及び関係部門との調整
④CSIRT体制の設置及び簡易的な演習
⑤活動に係る文書作成と定期レビュー

2.1. インシデントレスポンスプランニング

■ポイント：計画は大事。ただし、一気にやろうとしない。

① 参考文献調査及び情報収集（資料調査、経験者への聞き取り等）
詳細な情報収集、経験者へのインタビュー
インシデントレスポンス体制の構築に関する実務能力の見積り

② 経営層からの体制構築承認獲得（体制構築及び準備活動等の獲得）
現状の対応体制／能力の課題（不足等）提示
課題を踏まえた計画提示

③ 組織内の現状把握及び関係部門との調整
関連部門のインシデントに対する認識と対応活動状況把握
関連部門の協力姿勢の醸成（連携のための取決め）

④ CSIRT体制の設置及び簡易的な演習
簡易的なサイバー演習（セミナー、ワークショップ、机上演習）
関連部門が取るべき行動の実効性を確保

⑤CSIRT活動に係る文書作成と定期レビュー
定期レビュー実施の規定化
組織内への周知徹底

2.1. インシデントレスポンスプランニング

プロセス	項目
① 参考となる文献調査	利害関係者及び内部関係者の見出し
	情報収集
② 経営層からの体制構築の承認獲得	管理者層の支援を獲得
	CSIRTプロジェクト計画を作成
	サービス対象の見出し
	CSIRT運用のための財源獲得
	スタッフ、設備、インフラのリソースの要求事項を特定
	役割、責任、権限の明確化
③ 組織内の現状把握	情報収集
④ CSIRT体制の設置	CSIRTミッションの明文化
	提供サービスの範囲とレベルを決定
	CSIRT報告機構、権限、組織モデル
	やり取り及び連絡窓口の明確化
	運用開始時におけるCSIRT周知
⑤ CSIRT活動に係る文書作成	ワークフローの文書化
	ポリシー及び対応プロシージャの構築
	実装計画とフィードバック報告の作成
	CSIRTのパフォーマンス評価方法を作成
	CSIRTの全構成要素のバックアップ計画
	臨機応変に状況変化に応じたサービス変更等及びそれに伴う変更管理

2.2. インシデントハンドリング

■目的

発生したインシデント又はインシデントの恐れの狭小化

■概要

インシデントハンドリングは、「事象の発見・通報」から「再発防止策の立案」に至る7つの活動（フェーズ）で構成

「利用者」「LAN管理・運用者（情報システム部門）」「LAN管理・運用者（各事業部門）」「情報セキュリティ責任者」「外部専門組織」「ISP事業者」の6つのロールが連携

～ インシデントハンドリングフェーズ～

A.事象の発見・通報
B.初動対処の可否判断と情報伝達
C.被害拡大の防止や抑制のための初動対処
D.原因推定のための簡易的調査
E.本格調査
F.技術的調査結果と運用的調査結果の関係性分析
G.再発防止策の立案

2.2. インシデントハンドリング

■ポイント：関係者、コミュニティ等との緊密な連携が必要

A.事象の発見・通報
発生した異常な事象を発見・認識し、適切な担当者に通報

B.初動対処の可否判断と情報伝達
受領した事象情報に基づき初動対処についての可否判断
適切な部門・組織に対して必要な情報の伝達

C.被害拡大の防止や抑制のための初動対処
技術的及び運用的両面で、被害拡大防止・抑制に必要な措置実行

D.原因推定のための簡易的調査
事象が直接的及び間接的に確認できている場合
事象が発生した周辺のLAN関係者による簡易的な事象確認

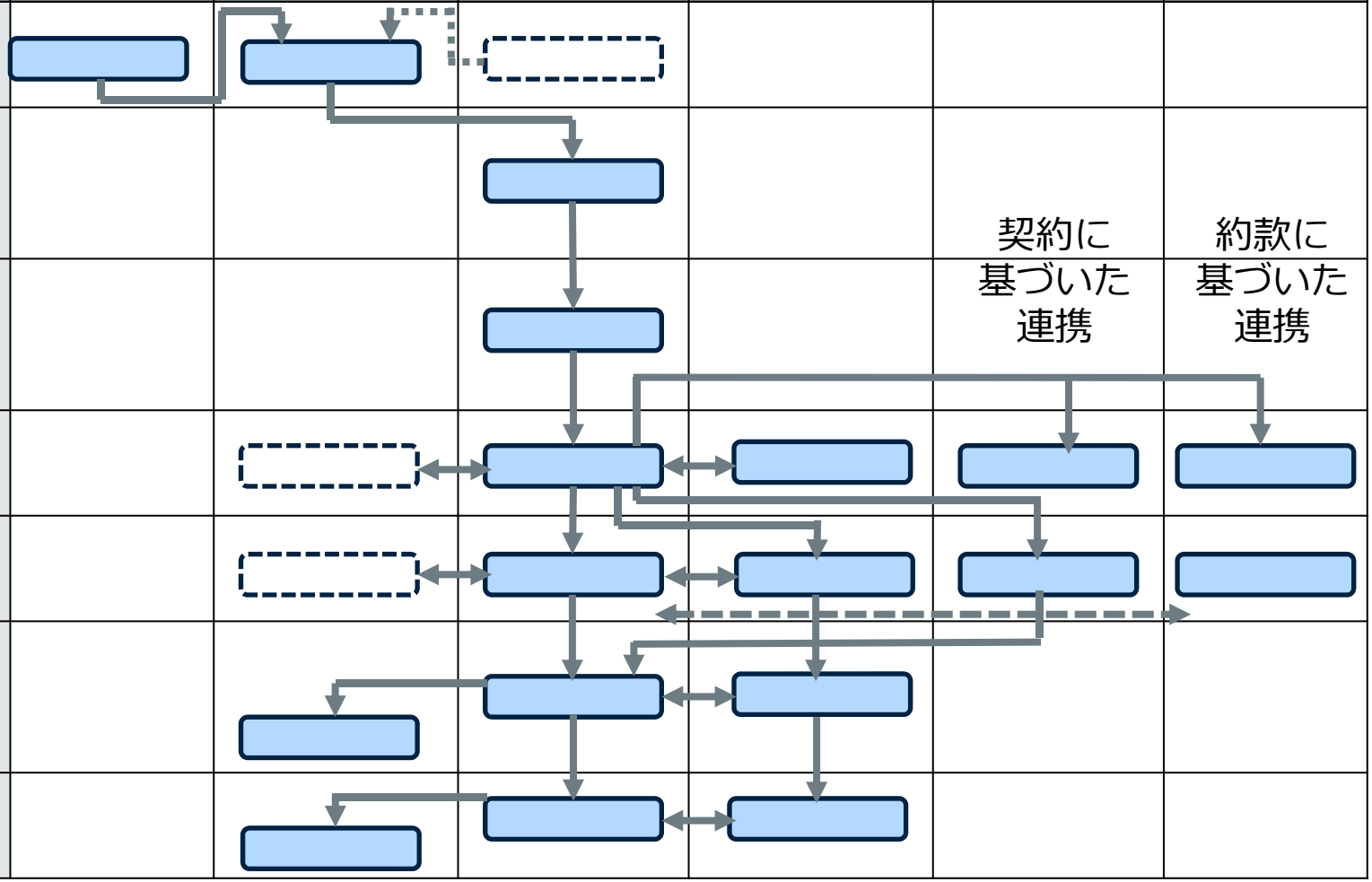
E.本格調査
技術的調査を外部専門組織に依頼
組織業務やシステム運用観点に基づく運用的調査

F.技術的調査結果と運用的調査結果の関係性分析
技術的／運用的調査結果の関係性分析、攻撃実態の把握

G.再発防止策の立案
把握した攻撃実態等から技術的／運用的再発防止策を立案

2.2. インシデントハンドリング

インシデントハンドリングフェーズ	利用者	LAN管理・運用者(情報ｼｽﾃﾑ部門)	LAN管理・運用者(各事業部門)	情報セキュリティ責任者	外部専門組織	ISP
A.事象の発見・通報						
B.初動対処の可否判断と情報伝達					契約に	約款に
C.被害拡大の防止や抑制のための初動対処					基づいた連携	基づいた連携
D.原因推定のための簡易的調査						
E.本格調査						
F.技術的調査結果と運用的調査結果の関係性分析						
G.再発防止策の立案						



[凡例] ：アクション

［参考］ 人・組織対策

■解説書付録では

人・組織対策計画（体制確立・改善）時に活用可能

[インシデントハンドリングフェーズの定義]

・インシンデントハンドリング各フェーズにおいて、6つの主体（役割）に求められる「アクション」を整理

・インシンデントハンドリング各フェーズにおいて、6つの　主体（役割）に求められる「要求事項（能力スキル）」を整理

・「アクション」実施に必要となる「インプット」及び「アクション」実施後の「アウトプット」を整理

3.技術的対策

3.1. 事前対策

■目的

攻撃者の攻撃コストを高め、被害を未然に防ぐ、又は被害に遭いにくいシステム環境の実現

■概要

代表的な事前対策は、以下3対策

①アプリケーションの利用制限（ホワイトリスト化）
②アプリケーションを最新の状態に保持
（セキュリティパッチの適用）
③管理者権限の最小化

※事前対策については、「導入障壁（利用者面）」「導入コスト」「維持管理コスト」の3軸で評価
出典：http://www.asd.gov.au/infosec/top-mitigations/mitigations-2014-table.htm

3.1. 事前対策

■ポイント：下記3対策で85%のサイバー攻撃が防御可能

① アプリケーションの利用制限（ホワイトリスト化）
業務利用のアプリケーションの実行のみを許可
未承認（業務外目的）のアプリケーションの実行を抑止

② アプリケーションを最新の状態に保持（セキュリティパッチ適用）
特に、リスクの高い脆弱性に関するセキュリティパッチは公開後、迅速に適用

③ 管理者権限の最小化
管理者権限（特権）を持つユーザ数を最小化
特権を持たない一般利用者権限アカウントでの定常運用
特権の最小化の維持（定期的に発行済アカウントの現状確認）

[前提]前述のネットワーク標準構成機器による対策実施が一般的

- FW：業務外通信の遮断
- Proxy：業務外サイトアクセスの遮断
- IDS/IPS：不正通信の検知・遮断
- アンチウイルス：マルウェアを検知・駆除

3.2. 検知

■**目的**

システムログに残される痕跡（IOC）分析による事前対策をすり抜けた攻撃の認知　IOC：Indicator of Compromise

■**概要**

標的型攻撃の検知は、以下の3つの分析観点で実施する。

①照合分析
②統計分析
③複合分析

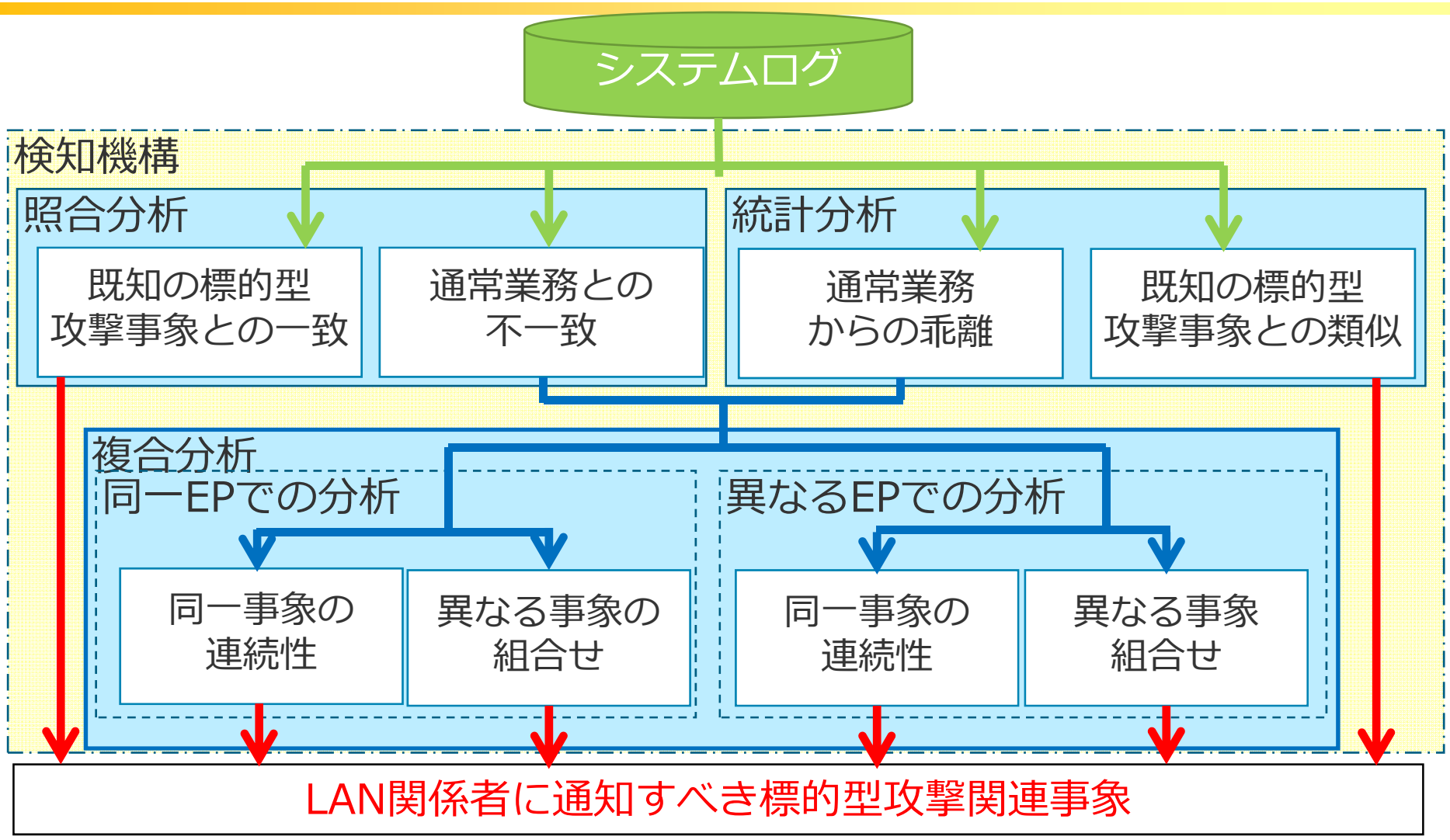
■**ポイント：通常業務との差異による検知が重要に**

① 照合分析
既知の標的型攻撃事象と一致するかどうか分析

② 統計分析
既知の標的型攻撃事象との類似点があるかどうか分析

③ 複合分析
通常業務と不一致、又は乖離する事象について、
同一事象の連続性／異なる事象の組合せの2観点でさらに分析

3.2. 検知


システムログ
検知機構
照合分析
既知の標的型
攻撃事象との一致
通常業務との
不一致
統計分析
通常業務
からの乖離
既知の標的型
攻撃事象との類似
複合分析
同一EPでの分析
異なるEPでの分析
同一事象の
連続性
異なる事象の
組合せ
同一事象の
連続性
異なる事象
組合せ
LAN関係者に通知すべき標的型攻撃関連事象
[凡例]
標的型攻撃関連事象
標的型攻撃関連事象
システムログ情報（業務関連事象）

3.2. 検知

	分析観点	分析に利用する情報等
照合分析	既知の標的型攻撃関連事象との一致	●URLブラックリスト ●攻撃コード／ファイルシグネチャ ●LAN内でのPsExec利用 ●既知の脆弱性
	通常業務との不一致	●通常の通信先／通信元国情報 ●通常の内部サーバ／アプリケーション情報 ●通常利用のアプリケーション情報 ●通常利用のサイトカテゴリ情報 ●通常利用の通信先ポート番号 ●通常実行ファイルを取得するサイト情報 ●通常送信するファイル形式 ●IP直接指定のHTTPアクセス ●通常アクセスするURLのクエリストリング情報 ●CONNECT先ポート情報 ●LAN経由のExeダウンロード実行

3.2. 検知

<table>
<tr><th></th><th colspan="2">分析観点</th><th>分析に利用する情報等</th></tr>
<tr><td>統計分析</td><td colspan="2">既知の標的型攻撃関連事象との類似</td><td>●通信先数
●エラー応答数
●一定間隔で発生する通信</td></tr>
<tr><td></td><td colspan="2">通常業務との乖離</td><td>上記と更に下記の情報を分析に利用
●通信回数
●転送データサイズ</td></tr>
<tr><td rowspan="2">複合分析</td><td rowspan="2">同一エンドポイントでの分析

又は

異なるエンドポイントでの分析</td><td>同一イベントの連続性</td><td>●「照合分析 – 通常業務との不一致」及び「統計分析 – 通常業務との乖離」の組合せ</td></tr>
<tr><td>異なるイベントの組合せ</td><td>●「照合分析 – 通常業務との不一致」及び「統計分析 – 通常業務との乖離」の組合せ</td></tr>
</table>

3.3. 事後対策

■目的

標的型攻撃による被害拡大の防止・抑制、証拠保全、被害全貌の把握

■概要

事後対策は、標的型攻撃の被害拡大の防止／抑制のための「暫定対処」と標的型攻撃による被害の全貌分析／特定を行う「本格対処」から構成

①暫定対処
②本格対処

■ポイント：本格対処結果の共有は将来的には自身のためにも

① 暫定対処
原因特定できていない状態において、実施可能な対策を実施
C（機密性）、I（完全性）、A（可用性）の喪失可能性の影響を考慮
本格対処において状況の特定、分析を行うために証拠保全を実施

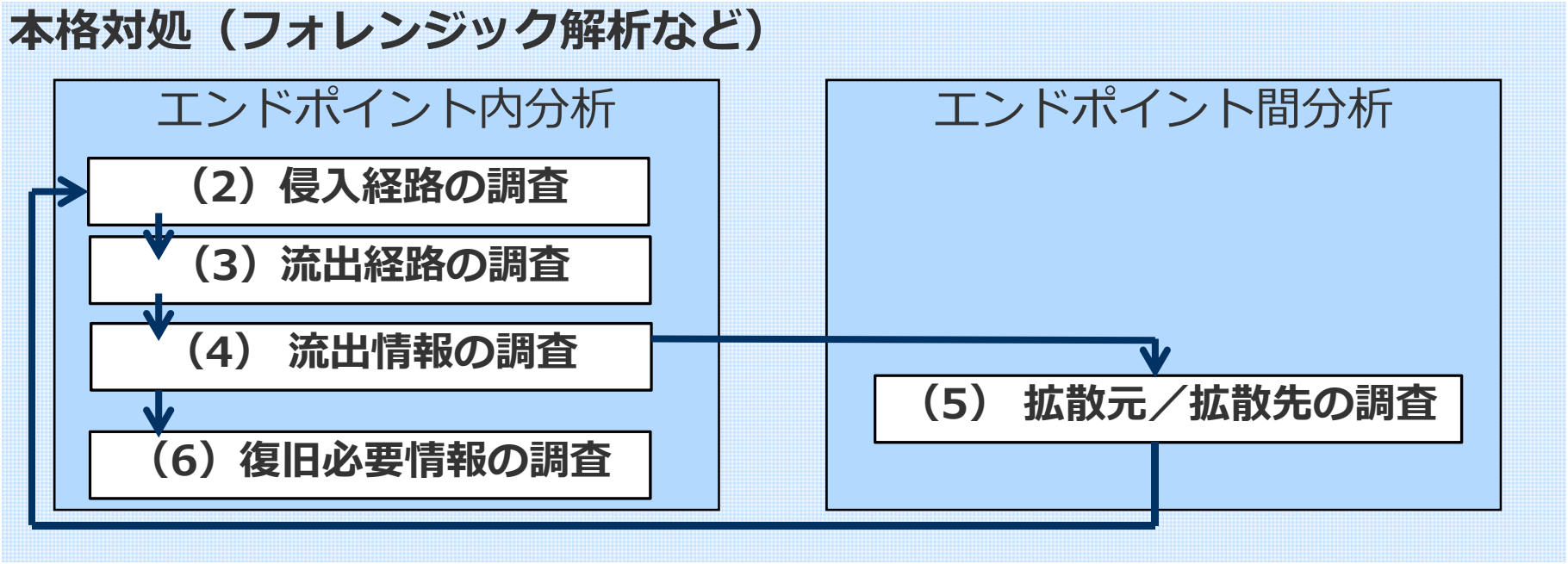
② 本格対処
フォレンジック解析などの専門事業者と連携して実施する必要あり
「侵入経路情報」「拡散元／拡散先情報」「流出経路／流出情報」
「復旧必要情報」を調査

3.3. 事後対策

効果を及ぼす対象	暫定対処策
ユーザ(アカウント)	注意喚起
	PWや権限の変更
	無効化
	削除
EP	注意喚起
	検知感度向上
	マルウェア隔離、駆除
	接続先URL、ポート番号、プロトコル、IPアドレスを遮断
	所属NWの変更
	EPをIP遮断
	抜線
	電源断
セグメント	注意喚起
	検知感度向上
	DNS（ブラックホスト名）不在応答
	DNS（ブラックドメイン名）
	ドメイン・URL、ポート番号、プロトコル、IPアドレスを遮断
	SRC／DSTセグメント間通信遮断
	接続NWの変更
	NWごと抜線
サービス	サービス一部停止
	サービス全停止

3.3. 事後対策

本格対処（フォレンジック解析など）



調査情報	内容
侵入経路情報	どこから、どこへ、どのように侵入
拡散元／拡散先情報	どこから、どこへ、どのように拡散
流出経路／流出情報	どこから、どこへ、どのように、 どんなものが流出
復旧必要情報	発生源、パス情報、影響先

[参考] 技術的対策

■解説書付録では

人・組織対策計画（体制確立・改善）時、技術的対策計画（システム運用）時、双方に活用可能

[システムログ一覧（IOC）／システムログ一覧（証拠保全）]

・システムの構成要素ごとに、どのような攻撃手法／攻撃フェーズでどのシステムログ項目に痕跡が残るかを整理

・インシデント発生時にインシデントハンドリング目的ごとに、証拠保全すべきシステムログを整理

[暫定対処策一覧]

・インシデント発生時に選択可能な暫定対処策と暫定対処策実行の際の影響を整理