サイバー攻撃（標的型攻撃）対策
防御モデルの解説

付録 1　インシデントハンドリングフェーズの定義

目 次

1. インシデントハンドリングフェーズの定義の概要

実態調査に基づくインシデントハンドリングフェーズは、その主体が取り扱う「情報」の遷移、及び「アクション」の機能や性質の違いに着目して分類すると、次の図のような概要となる。

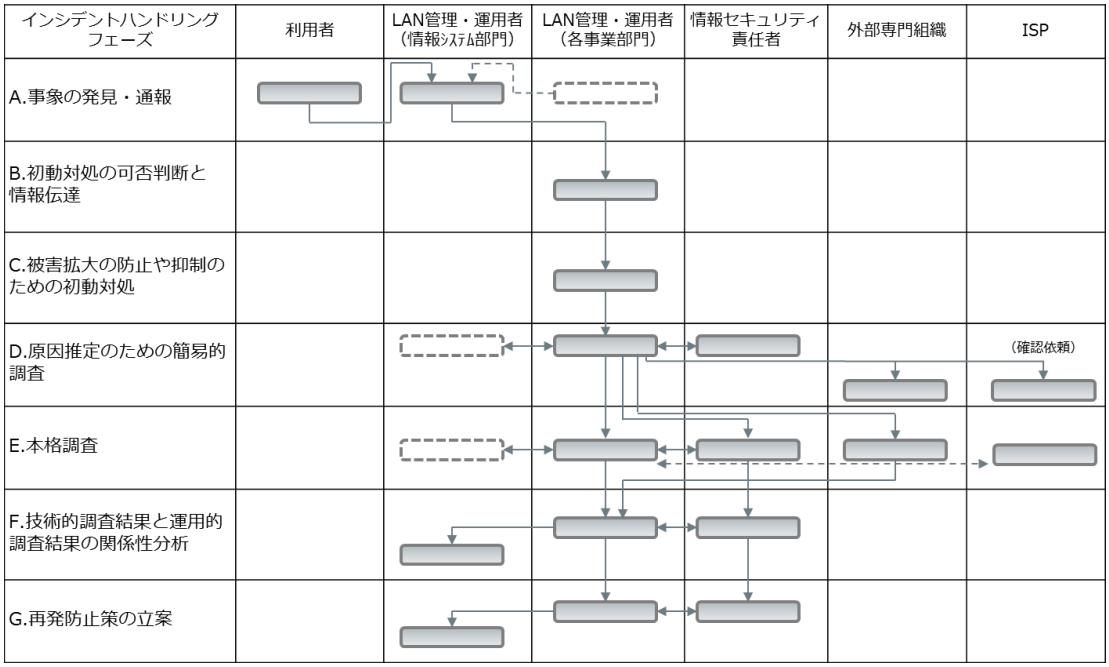

図 1 インシデントハンドリングフェーズの概要

1-1. インシデントハンドリングの主体

それぞれの主体の役割を、「利用者、LAN 管理者、LAN 運用者、情報セキュリティ責任者、外部専門組織」の 5 つに分類することとした。ただし、LAN 管理者、LAN 運用者、情報セキュリティ責任者を総称して LAN 関係者と呼称する。

- 利用者： LAN 環境及び LAN 環境内システムで提供されるサービス利用者
- LAN 管理・運用者（情報システム部門）： LAN 環境及び LAN 環境内システム運用者及び管理者（利用者との接点部門）
- LAN 管理者・運用者（各事業部門）： LAN 環境及び LAN 環境内システム運用者及び管理者（外部専門組織との接点部門）
- 情報セキュリティ責任者： 官公庁・大企業の情報セキュリティ対策の運用に係る総責任者
- 外部専門組織： LAN 環境及び LAN 環境内システム運用者（事業部門）の技術支援組織
- ISP： LAN 関係者の所属組織が契約しているインターネットサービス・プロバイダ

1-2. インシデントハンドリングフェーズ分類基準

インシデントハンドリングフェーズを上記の A～G に分類するにあたっての基準は、次のとおりである。

- 主体の役割と能力（特に対応限界）
- インシデントハンドリングに関与する部門の増減
- 状況（攻撃及び被害）認識の範囲拡大のタイミング
- 意思決定のタイミング

2. インシデントハンドリングフェーズ毎のアクションの定義

A. 事象発見・通報

アクション

- 発生した異常な事象を発見・認識し、適切な担当者に通報すること
  - 事象情報の受領と認識、事象の発見・記録保持
  - 事象（情報）に基づいた、組織への関係性、重要レベル及び優先レベルの推量・判断
  - 通報先の特定
  - （事業部門と事前相談をした上で）適切な手段による通報
  - 迅速な関連情報の集約

インプット

- 利用者
  - 利用しているコンピュータシステムからのアラート情報（基本 OS やセキュリティ対策アプリケーションが出力するアラート情報等）
  - 利用しているコンピュータシステムの不正挙動の認識
- LAN 管理・運用者（情報システム部門）
  - 外部組織から通知される情報（セキュリティ脅威情報、インターネットを通じて提供しているサービスの利用阻害等）
  - 組織内の偶発的事象から顕在化したサイバー攻撃を示唆する情報（会計監査対応時の電子媒体の情報資産レビュー、他のセキュリティ事象への対応活動 等）
  - IDS／IPS、Firewall 等からのエラー情報及びアラート情報
  - コンピュータシステム及びネットワークシステムの監視活動から得られる不自然な挙動情報

アウトプット

- 利用者
  - 不正挙動或いはその恐れがあると認識された事象情報
  - 適切な部門等（情報システム部門）に通報すべきと判断された事象情報
- LAN 管理・運用者（情報システム部門）
  - 不正挙動或いはその恐れがあると認識された事象情報
  - 適切な部門等（LAN 管理者）に通報すべきと判断された事象情報
  - 明らかに組織に対して関係ない、或いは影響ないと判断された事象情報

要求事項（能力スキル）

- 利用者
  - 利用しているコンピュータシステムの基本 OS の設定やセキュリティ対策アプリケーションからアラートを出力する設定ができること
  - 認識したアラート情報や不正挙動の意味を理解し、それらの重要レベルと優先レベルを推量或いは判断できること
  - どの部門や管理者に通報すべきかを把握していること
  - 通報手段を知っており、利用することができること
- LAN 管理・運用者（情報システム部門）
  - 受領及び認識した情報の内容を理解できること
  - 受領及び認識した情報について、組織への関係性の判断ができること
  - 受領及び認識した情報の重要レベルや優先レベルを推量或いは判断できること
  - 受領情報の変更管理ができること
  - どの部門の管理者に通報すべきかを把握していること
  - 通報手段を知っており、利用することができること
  - コンピュータシステム及びネットワークシステムに実装されているセキュリティ対策アプリケーション等がエラー情報やアラート情報を出力可能な状態にしていること
  - 認識した情報の重要レベルや優先レベルを推量及び判断できること
  - 認識した情報の原因推定や、コンピュータシステム及びネットワークシステムに対する影響評価を行うことができる担当者を特定し、通報することができること
  - 適切な通報手段を知っており、利用することができること

B. 初動対処の可否判断と情報伝達

アクション

- 受領した事象情報に基づく初動対処の可否判断と、適切な部門・組織に対して、情報を流通すること
  - 受領した事象情報の分類や位置付けの判断
  - 受領した事象情報と他の対応中のインシデントとの関連性の確認
  - 受領した事象情報の初動評価（重要度及び優先度の判断）
  - 受領した事象情報の識別性を与える属性情報の付与
  - 対処すべき担当者への作業割り当て
  - 報告および周知

インプット

- LAN 管理・運用（各事業部門）
  - エラー情報（基本 OS や搭載されているアプリケーションが出力するエラー情報）
  - アラート情報（基本 OS やセキュリティ対策アプリケーションが出力するアラート情報等）
  - IDS／IPS、Firewall 等からのエラー情報及びアラート情報
  - コンピュータシステムやネットワークシステムにおける不正挙動に関する情報
  - 組織に関係する情報
  - 外部から受領した情報（セキュリティ脅威情報、インターネットを通じて提供しているサービスの利用阻害等）
  - 受領或いは認識した情報が組織に明らかに関係しない場合、破棄して対応を終了する
  - 組織内の偶発的事象から顕在化したサイバー攻撃を示唆する情報（会計監査対応時の電子媒体の情報資産レビュー、他のセキュリティ事象への対応活動 等）

アウトプット

- LAN 管理・運用（各事業部門）
  - 被害拡大が進行していると判断された事象情報
  - 分類、位置付け、初動評価（重要度、優先度の判断）された事象情報
  - 他の対応中のインシデントに関連付けられた事象情報
  - 初動対処すべき担当者に割り当てられた事象情報
  - 明らかに組織の関係ない、或いは影響のないと判断された事象情報

要求事項（能力スキル）

- LAN 管理・運用（各事業部門）
  - 受領する事象情報の内容を理解し、コンピュータシステムやネットワークシステムに技術的及び運用的な影響を与える箇所を特定することができること
  - 事象が発生したコンピュータシステムやネットワークシステム周辺の業務の内容や流れを把握及び理解し、その業務の管理者や責任者と連絡調整ができること
  - 受領する事象情報が、自組織のコンピュータシステムやネットワークシステムに与える影響（重要度）と対処する序列（優先度）を見積ることができること
  - 受領する事象情報が、他に対応している対応中のインシデントの存在を把握しており、かつ、それとの関係性の有無を判断できることができること
  - 受領する事象情報の優先度及び重要度に基づいて、作業を割り当てる担当者を特定できること
  - 作業を割り当てた担当者に対して迅速かつ適切な連絡や依頼をすることができること

C. 被害拡大の防止や抑制のための初動対処

アクション

- 被害拡大が進行していると判断された事象情報の場合、技術的及び運用的の両面で、被害拡大の防止や抑制に必要な措置を特定し、迅速に実行すること
  - 被害拡大の防止や抑制のための技術的手段や運用的指示の適否・可否判断及び決定
  - 決定された手段や指示の実行
  - 実行結果の状態の確認と影響評価による見直し
  - 被害拡大の防止や抑制の完了判断と関係箇所への報告・通知
  - （甚大な被害が明確な場合に限った）システムの一部運用の停止

インプット

- LAN 管理・運用（各事業部門）
  - 被害拡大が進行していると判断された事象情報
  - 初動対処すべき担当者に割り当てられた事象情報

アウトプット

- LAN 管理・運用（各事業部門）
  - 被害拡大の防止や抑制のための技術的手段や運用的指示の情報
  - 被害拡大の防止や抑制のための意思決定と実行結果
  - 被害拡大の防止や抑制の完了通知

要求事項（能力スキル）

- LAN 管理・運用（各事業部門）
  - 事象が発生したコンピュータシステムやネットワークシステムに対する、被害拡大の防止や抑制のための技術的手段や管理的指示の手段を立案することができること
  - 立案した技術的手段や管理的指示が、コンピュータシステムやネットワークシステム周辺業務の内容や流れに与える影響を特定し、それを評価することができること
  - 評価された技術的手段や管理的指示の実行のための意思決定ができること
  - 決定した技術的手段や管理的指示を実行するための技術的能力や管理的権限を有していること
  - 実行した技術的手段や管理的指示の結果を把握し、その影響評価をすることができること

- 影響評価された技術的手段や管理的指示の結果に基づいて、完了したことを意思決定できること
- 完了した結果を関係箇所に報告、通知することができること

D. 原因推定のための簡易的調査

アクション

- 被害進行がされておらず、かつ事象が直接的及び間接的に確認できている（顕在化している）場合、本格的調査を行う前の段階として、事象が発生した周辺の LAN 関係者により簡易的な確認作業を行うこと
  - 顕在化している事象を詳細かつ多角的に観察及び調査
  - 顕在化している事象の発生原因及び発生経路を推定
  - 本格的調査に影響を与えない範囲の、技術的及び運用的な簡易的調査
  - システム及び業務の流れで関係性のある部署に対する、顕在化している事象の有無の確認
  - 発生事象をインシデントとして認定
  - 関連情報の積極的な収集及び確認
  - 本格的調査の範囲及び対象の見積もり
  - 外部専門組織の選定と、依頼内容の立案と確定
  - ISP に対する連絡（問い合わせ）や相談、及び契約約款に基づく依頼事項の立案と確定

インプット

- LAN 管理・運用（各事業部門）
  - 分類、位置付け、重要度、優先度が明確化（判断）された事象情報
  - 他の対応中のインシデントに関連付けられた事象情報
  - 初動対処すべき担当者に割り当てられた事象情報
  - 被害拡大の防止や抑制のための技術的手段や運用的指示の情報
  - 被害拡大の防止や抑制のための意思決定と実行結果

アウトプット

- LAN 管理・運用（各事業部門）
  - 推定された顕在化している事象の発生経路及び発生原因
  - 他の事象との関係性
  - 技術的及び運用的な簡易的調査の結果
  - 見積もられた本格的調査の範囲及び対象
  - 外部専門組織の選定結果
  - ISP に対する連絡（問い合わせ）や相談、及び依頼事項に対する結果

要求事項（能力スキル）

- LAN 管理・運用（各事業部門）
  - 顕在化している事象が発生する一般的原因やメカニズムに関する知見を有していること
  - 事象が発生しているシステムに対して、顕在化している事象の一般的原因やメカニズムの適合性を評価できること
  - 本格的調査の内容を把握及び理解し、システム上の残存している痕跡に影響を与えない範囲で、技術的及び運用的な調査手段の知見を有し、かつ、それを実施することができること
  - 推定された発生原因及び発生経路をもとに、システム及び業務の流れに関係性のある部署を特定できる知見や経験を有していること
  - 推定された発生原因と発生経路と他の顕在化している事象等の情報等から、事前の取り決めにしたがって「インシデント」として認定することができること
  - 本格的調査により期待できる結果を見積ることができること
  - 外部専門組織の能力や経験を把握していること
  - 外部専門組織が実施可能な依頼内容を作成できること
  - ISP との契約約款を把握し、依頼内容を作成できること

E. 本格的調査

アクション

- LAN 関係者が、外部専門組織に依頼した内容以外の技術的調査、及び組織業務やシステム運用の観点に基づく管理的調査を行うこと
  また、調査結果に基づき影響範囲の特定を行い、本格的対処実施後、被害事象の継続発生有無の確認を行うこと
  - インシデントによる影響範囲（関係部署）を特定
  - 影響範囲に対する技術的及び管理的調査の実施
  - 調査結果の取りまとめ、報告書作成及び報告・説明の実施
  - 調査結果に基づき影響範囲の特定を行い、本格的対処実施後、被害事象が継続発生していないことを確認
- 外部専門組織が、LAN 関係者によって推定された発生原因や発生経路を、さらに追求及び確定する目的で、LAN 関係者の経験や知見の限界を超える範囲において技術的調査を行うこと
  - 依頼内容の理解と調査計画の立案
  - 調査活動及び被害組織との連携
  - 調査結果の取りまとめと報告書作成
  - LAN 関係者に報告
- ISP が、契約約款に基づいて、LAN 関係者の依頼事項への対応及び連携活動を行うこと
  - 依頼内容の対応可否及び対応方針
  - 対応活動（技術的或いは運用的対応）及び LAN 関係者とのやり取り
  - 対応結果の取りまとめと回答書作成

インプット

- LAN 管理・運用（各事業部門）、情報セキュリティ責任者、外部専門業者
  - 推定された顕在化している事象の発生経路及び発生原因
  - 技術的及び運用的な簡易的調査の結果
  - 見積もられた本格的調査の範囲及び対象
- ISP
  - 契約約款に基づく依頼内容

アウトプット

- LAN 管理・運用（各事業部門）
  - （本格的調査を伴わない）技術的調査の結果
  - 組織業務やシステム運用の観点で行った管理的調査の結果

- 影響範囲の特定及び本格的対処実施後、被害事象の継続発生有無の確認結果

- 情報セキュリティ責任者
  - 情報資産の被害範囲及び程度の調査結果
- 外部専門業者
  - フォレンジック調査やマルウェア解析等による技術的調査の報告
- ISP
  - 契約約款に基づいて対応した結果の回答

要求事項（能力スキル）

- LAN 管理・運用（各事業部門）
  - インシデントの影響範囲（関係部署）の業務の内容や流れを把握していること
  - インシデントの影響範囲（関係部署）に対して、技術的及び管理的調査を行うことができる権限を有している、或いは承諾を得る受けることができること
  - 技術的及び管理的調査を行う手段と、それを実施することができる知見と能力を有していること
  - 外部専門組織から高いレベルの技術的な報告内容を理解することができること
- 情報セキュリティ責任者
  - 情報資産の所在及び運用状況を把握していること
  - 情報セキュリティに関する規程類上の判断事項を熟知していること
- 外部専門業者
  - 電磁的証拠（ログや痕跡等）の収集、取得、保全が適切にできること
  - 攻撃痕跡を見出す解析作業（マルウェアによる攻撃痕跡の特定）が出来ること
  - メモリダンプ解析や特定できた痕跡等から、タイムライン分析ができること
  - LAN 関係者に理解可能な報告書の作成及び報告・説明ができること
- ISP
  - 契約約款に基づいた対応ができること

F. 技術的調査と運用的調査の関係性分析

アクション

- 外部専門業者による本格的な技術的調査の結果と、LAN 関係者による技術的及び運用的調査の結果を関係性分析し、インシデントの実態解明の努力とその判定を行うこと
  - それぞれの調査結果の構成要素同士の相関性及び因果性の見出し
  - 相関性及び因果性の評価と確定
  - 攻撃挙動の時系列化と、システム上の攻撃経路の判定
  - 判定された攻撃実態に基づく、システムの改善箇所の特定
  - 判定された攻撃実態に関する報告書作成と報告・説明の実施

インプット

- LAN 管理・運用（各事業部門）
  - 外部専門組織から受領した、フォレンジック調査やマルウェア解析等による技術的調査の報告
  - LAN 関係者による、（本格的調査を伴わない）技術的調査の結果
  - LAN 関係者による、組織業務やシステム運用の観点で行った運用的調査の結果
- 情報セキュリティ責任者
  - 外部専門組織から受領した、フォレンジック調査やマルウェア解析等による技術的調査の報告
  - 情報セキュリティ責任者による、情報資産の被害範囲及び程度の調査結果

アウトプット

- LAN 管理・運用（各事業部門）
  - （技術的事項を軸とした）技術的調査と運用的調査の関係性分析の結果
  - 判定された攻撃実態の内容
  - システムの改善箇所の内容
- 情報セキュリティ責任者
  - （管理的事項を軸とした）技術的調査と運用的調査の関係性分析の結果
  - 明らかな被害を受けた情報資産の内容

要求事項（能力スキル）

- LAN 管理・運用（各事業部門）
  - 一つの調査結果から、他の調査結果と相関性及び因果性のある可能性のある構成要素を特定することができること
  - よく発生する攻撃の挙動や経路を把握していること

- 把握した攻撃の挙動や経路と、よく発生するものとの比較評価をすることができること
- 判定された攻撃実態について、報告先に理解可能な報告書の作成及び報告・説明ができること
- システム改善箇所に関する報告書の作成及びその報告・説明ができること

• 情報セキュリティ責任者
  - 一つの調査結果から、他の調査結果と相関性及び因果性のある可能性のある構成要素を特定することができること
  - 把握した攻撃の挙動や経路と、情報セキュリティに関する規程類上の判断事項を比較評価することができること
  - 情報セキュリティに関する規程類に基づく報告書の作成及び報告・説明ができること
  - 情報資産の管理及び運用の改善に関する報告書の作成及びその報告・説明ができること

G. 再発防止策の立案

アクション

- LAN 関係者が、判定された攻撃実態及びシステム改善箇所に基づいて、再発防止を主な目的として、技術的及び管理的な対策立案を行うこと

インプット

- LAN 管理・運用（各事業部門）
  - 技術的調査と管理的調査の関係性分析の結果
  - 判定された攻撃実態の内容
  - システムの改善箇所の内容
- 情報セキュリティ責任者
  - （管理的事項を軸とした）技術的調査と管理的調査の関係性分析の結果
  - 明らかな被害を受けた情報資産の内容

アウトプット

- LAN 管理・運用（各事業部門）
  - （技術的事項を軸とした）再発防止のための対策立案の内容
- 情報セキュリティ責任者
  - （管理的事項を軸とした）再発防止のための対策立案の内容

要求事項（能力スキル）

- LAN 管理・運用（各事業部門）
  - 判定された攻撃実態を発生させない技術的及び管理的対策と、システム改善箇所に対する技術的対策を見出すことができること
  - 立案した対策の実現性及び有効性を評価できること
  - 関係部署と合意形成をとることができること
  - 報告先に理解可能な報告書の作成及び報告・説明ができること
- 情報セキュリティ責任者
  - 情報資産に被害を発生させない再発防止のための管理的対策を見出すことができること
  - 立案した対策の実現性及び有効性を評価できること
  - 関係部署と合意形成をとることができること
  - 報告先に理解可能な報告書の作成及び報告・説明ができること