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

総務省
情報流通行政局
情報流通振興課
情報セキュリティ対策室

目次

1. 本解説書の目的

日々、巧妙化・複合化し続ける標的型攻撃等の新たなサイバー攻撃に対応するためには、標的型攻撃への対応方法について深く認知し、必要な対策を機能させるための対応（又は対応指示）を行う必要がある。

本解説書では、標的型攻撃防御モデルについての検討結果を基に、標的型攻撃から情報システムを防御するための対策（標的型攻撃防御）に関する理解促進を行う。

表 1-1 近年のサイバー攻撃の事例（政府機関等）

メディア掲載日及び団体名		概要
平成 23 年 11 月 17 日	衆議院、参議院	衆議院および参議院の公務用 PC やサーバがサイバー攻撃を受けた可能性があり、15 日間メールを閲覧された形跡があった。
平成 24 年 1 月 17 日	宇宙航空研究開発機構（JAXA）	宇宙航空研究開発機構（JAXA）は 1 月 13 日、同機構の端末がウイルス感染し、当該端末内の情報と同端末を利用する職員がアクセス可能なシステムに関する情報が外部に漏えいしていた。
平成 25 年 1 月 22 日	独立行政法人日本原子力研究開発機構（原子力機構）	独立行政法人日本原子力研究開発機構（原子力機構）は 1 月 18 日、同機構の PC がウイルスに感染したことで情報が外部に漏えいした可能性があった。
平成 25 年 4 月 25 日	宇宙航空研究開発機構（JAXA）	「きぼう」関連の情報など、宇宙航空研究開発機構（JAXA）のサーバに外部から不正アクセスがあった。
平成 26 年 1 月 9 日	独立行政法人日本原子力研究開発機構（原子力機構）	独立行政法人日本原子力研究開発機構（原子力機構）の事務処理用 PC（「もんじゅ」の発電課当直員が使用する事務処理用 PC）がウイルス感染、情報漏えいの可能性があった。
平成 27 年 6 月 1 日	日本年金機構	日本年金機構で不審メールに起因する不正アクセスによって 125 万件の個人情報が外部流出した。
平成 27 年 11 月 23 日	厚生労働省	DDoS とみられる攻撃により、厚生労働省の Web サーバに閲覧障害が発生した。
平成 28 年 1 月 31 日	複数の省庁	DDoS とみられる攻撃により、複数の省庁（中央省庁 5 件以上）の Web サーバにおいて閲覧障害が発生した。

2. 用語

本解説書の用語を示す。

表 2-1 用語

【A】	
AD	Active Directory の略称。
AP	Application の略称。
APFW	Application FireWall の略称。本解説書では L7FW と同義として扱う。
API	Application Programming Interface の略称。ソフトウェアプラットフォームが開発者向けに提供している命令や関数の集合。
【C】	
C&C サーバ	Command And Control サーバの略称。感染した PC をネットワーク経由で操作し、情報の収集や攻撃の命令を出すサーバ。
C2 ホスト	C&C サーバとして動作するホストのこと。
CIA	情報セキュリティの根幹を成す重要な要素である“Confidentiality”（機密性）、“Integrity”（完全性、保全性）、“Availability”（可用性）の頭文字をつなげた標語。
CMS	Content Management System の略称。ウェブコンテンツを構成するテキストや画像などのデジタルコンテンツを統合・体系的に管理し、配信など必要な処理を行うシステムの総称。
Compromise	プライベート鍵が紛失・不正コピーなどの疑いから厳格な本人性の証明に使えなくなった状態。
CSIRT	Computer Security Incident Response Team の略称。セキュリティ上の問題を中心として、監視対象となるネットワーク環境上で何らかの問題が起きていないかどうかを監視すると共に、問題が発生した場合にその原因解析や影響範囲の調査を行う組織。
【D】	
DB	Data Base の略称。複数の主体で共有、利用したり、用途に応じて加工や再利用がしやすいように、一定の形式で作成、管理されたデータの集合のこと。
DHCP	Dynamic Host Configuration Protocol の略称。インターネットなどのネットワークに一時的に接続するコンピュータに、IP アドレスなど必要な情報を自動的に割り当てるプロトコル。
DLP	Data Loss Prevention の略称。データの機密性・重要性に基づき、ユーザによる機密データのコピー、外部送信等を監視・制御する。

DMZ	DeMilitarized Zone（非武装地帯）の略称。インターネットのような攻撃の危険を伴う外部ネットワークと、内部ネットワークの中間に置かれる領域。外部向けの Web サーバ等を配置する。
DNS	Domain Name System の略称。インターネットなどの TCP/IP ネットワーク上でドメイン名やホスト名と IP アドレスの対応関係を管理するシステム。
【E】	
EP	End Point の略称。
【F】	
FW	FireWall の略称。
【I】	
IDS	システムに対する侵入／侵害を検出・通知するシステム。システムを監視し、セキュリティポリシーを侵害するような行為を検出した場合に、その行為を可能な限り早く管理者に伝えると共に、調査分析の作業を支援するために必要な情報を保存・提供することが目的である。ネットワークベース IDS と、ホストベース IDS に分類されることがある。その分類法は、搭載場所がゲートウェイであるかホストであるかによる場合と、検査対象がネットワークパケット情報かホスト内で生成する情報かによる場合がある。
IP	Internet Protocol の略称。複数の通信ネットワークを相互に接続し、データを中継・伝送して一つの大きなネットワークにすることができる通信規約（プロトコル）の一つ。
IPS	Intrusion Prevention System の略称。サーバやネットワークへの不正侵入を阻止するツール。ネットワークの境界などに設置する専用の機器（アプライアンス）や、サーバに導入するソフトウェアなどの形で提供される。
【L】	
L7FW	Layer 7 FireWall の略称。アプリケーション毎の通信の監視や制御を行う。
LAN	Local Area Network の略称。ケーブルや無線などを使って、同じ建物の中にあるコンピュータや通信機器、プリンタなどを接続し、データをやり取りするネットワーク。
【N】	
NGFW	Next Generation FireWall の略称。本解説書では L7FW と同義として扱う。
NW	Network の略称。複数の要素が互いに接続された網状の構造体のこと。
【O】	
OS	Operating System の略称。機器の基本的な管理や制御のための機能や、多くのソフトウェアが共通して利用する基本的な機能などを実装した、システム全体を管理するソフトウェア。

【P】	
P2P（ピアツーピア）	ネットワーク上で対等な関係にある端末間を相互に直接接続し、データを送受信する通信方式及びそのような方式を用いて通信するソフトウェアやシステムの総称。
PsExec	PsExec は、PsTools という Sysinternals のコマンドラインツールキットの一部。PsTools は、ローカルシステムとリモートシステムの管理をサポートするツールキット。
PW	Pass Word の略称。
【S】	
SRC/DST	Source/Destination の略称。Source は送信元を示しており、Destination は、送信先を示している。
【U】	
URL	Uniform Resource Locator の略称。インターネット上に存在する情報資源（データやサービスなど）の位置を記述するためのデータ形式。資源の取得方法（種類）や、ネット上での当該資源の存在するコンピュータの位置、コンピュータ内部での資源の位置などで構成される。
USB	Universal Serial Bus の略称。キーボードやマウス、モデムなどの周辺機器とパソコンを結ぶデータ伝送路の規格の一つ。
【W】	
WAF	Web Application Firewall の略。ウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを保護する。
【ア】	
インシデント	情報セキュリティ分野における「セキュリティインシデント（security incident）」は、情報セキュリティリスクが発現・現実化した事象をいう。
エクスプロイト	コンピュータの脆弱性を利用して攻撃するプログラム。
エンドポイント	通信回線やネットワークの末端に接続された端末やコンピュータ、情報機器などのこと。
【カ】	
クラウド	ソフトウェアやハードウェアの利用権などをネットワーク越しにサービスとして利用者に提供する方式を「クラウドコンピューティング」（cloud computing）と呼び、データセンターや、その中で運用されているサーバ群のことをクラウドという。
【サ】	
サイト情報	IP アドレスや URL、ドメイン名、FQDN 等、Web サイト等サーバのホスト情報やコンテンツ情報を示す情報。

サンドボックス	保護された領域でプログラムを動作させることにより、プログラムの不正な動作を防ぐセキュリティモデル。
ソーシャルエンジニアリング	コンピュータやネットワークの管理者や利用者またその関係者などから、話術や盗み聞き、盗み見などの手段によって、パスワードやセキュリティ上重要な情報を不正に入手すること。
【タ】	
ドメイン	インターネット上でコンピュータやネットワークを識別する名前の体系。
ドライブバイダウンロード（Drive by Download）	不正アクセスの手法の一つ。Web サイトなどに不正なソフトウェアを隠しておき、閲覧者がアクセスすると気づかないうちに自動でダウンロード・実行する攻撃手法。
【ハ】	
バックドア	マルウェア等により攻撃を受けたサーバに設けられた、不正侵入を行うための裏口。
ハッシュ値	ハッシュ関数を用いて計算を行った値。ハッシュ関数は与えられたデータに対して代表的な値の計算を行う。計算されたハッシュ値は同じデータでなければ同じ値が計算される可能性は低く、ユニークな値として考え、データを示す特徴的な値として利用される。ハッシュ関数の種類として、MD5 は SHA1、SHA256 が存在する。
ビーコン通信	本解説書では、マルウェアが C&C サーバに情報を送る仕組みのことを示している。主に HTTP（HTTPS）通信が利用される。
フォレンジック	不正アクセスや情報漏えい等の犯罪が生じた場合に、原因究明に必要な機器やデータ等を収集・分析し、犯罪が発生した事実の法的証拠を見つけ出す技術。
プロキシ	クライアントとサーバの間に存在し、情報元のサーバに対してはクライアントの情報を受け取る、クライアントに対してはサーバの働きをするもの。
プローブ	本解説書では、C&C サーバに送るための情報を収集するための仕組みのことを示している。
【マ】	
マルウェア	コンピュータウイルス、ワーム、スパイウェアなどの「悪意のこもった」ソフトウェア。
【か】	
可用性	システムの利用者から見て、システムが利用可能である度合い。可用性は、数値としては稼働率で表される。
完全性	情報セキュリティの目標事項の一つ。データが正確で完全であること、或いは、データを格納する情報システムが正確で完全であることを確保する。
機密性	情報セキュリティの目標事項の一つ。正当な権限を持った者だけが情報に触れることができる状態。また、そのような状態を確保・維持すること。

【さ】	
脆弱性	情報セキュリティ分野において、通常、脆弱性とは、システム、ネットワーク、アプリケーション、又は関連するプロトコルのセキュリティを損なうような、予定外の望まないイベントにつながる可能性がある弱点の存在、設計若しくは実装のエラーのことをいう。
【な】	
認証	認証、若しくは本人認証は、ユーザが本人であることを証明する過程をいう。認証のプロセスは、典型的には、本人であることの証拠として、ユーザの知識として自らの名前とパスワードやパスフレーズの入力を要求する。近年、ユーザの持ち物（例：スマートカード）や、ユーザの身体的特徴（バイオメトリクス）に基づく認証機構も普及しつつある。
【は】	
標的型攻撃	特定の個人や組織、情報を狙ったサイバー攻撃のこと。企業や国家の機密情報の詐取を目的に行われることが多い。

用語に関する出典元

- IPA（http://www.ipa.go.jp/security/pki/111.html）
- NICT（https://www.nict.go.jp/）
- MITRE 社（https://maec.mitre.org/）
- IEEE（http://standards.ieee.org/develop/indconn/icsg/mmdef.html）
- e-words（http://e-words.jp/）
- MicroSoft（https://technet.microsoft.com/ja-jp/sysinternals/psexec.aspx）
- wikipedia（https://ja.wikipedia.org/wiki）

3. 本解説書の想定読者と構成

3 章では、3.1 に本解説書の想定読者を 3.2 に本解説書の構成を説明する。

3.1. 本解説書の想定読者

本解説書は、情報システム等の安全性を確保する立場から、標的型攻撃に対応する担当者及び関係者を想定読者とする。以下に概要図を示す。

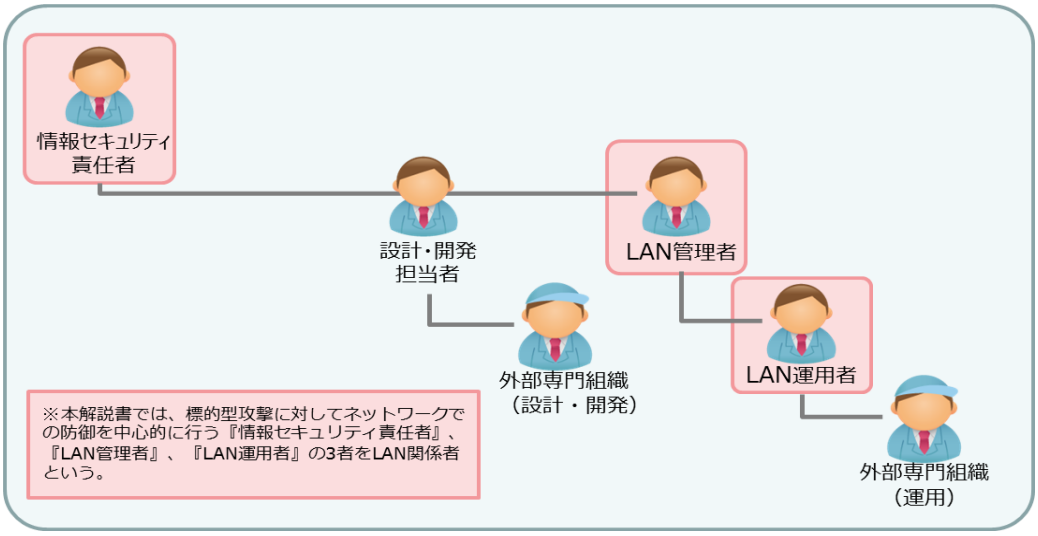

図 3.1-1 想定読者の概要図

本解説書の想定読者は、自組織内の 4 者及び外部専門組織の 2 者である。以下に詳細を示す。

表 3.1-1 想定読者の説明

想定読者		説明
自組織	情報セキュリティ責任者	自組織の情報セキュリティ責任者（CISO 等も含む）
	設計・開発担当者	自組織の情報システムに関する設計・開発の担当者
	LAN 管理者	自組織の LAN 管理者
	LAN 運用者	自組織の LAN 運用者
外部専門組織	設計・開発者	自組織の設計・開発者からの依頼に基づき一部の設計・開発を行う外部専門組織の設計・開発者
	運用者	自組織の LAN 管理者又は LAN 運用者からの依頼に基づき LAN の運用を行う外部専門組織の運用者

なお、本解説書では、情報セキュリティ責任者、LAN 管理者、LAN 運用者の 3 者をまとめて LAN 関係者という。

3.2. 本解説書の構成

本解説書は、「1.解説書の目的」「2.用語」「3.解説書の想定読者」「4.標的型攻撃の防御について」「5.人・組織対策」「6.技術的対策」「7.まとめ」で構成されている。

表 3.2-1 本解説書の構成と想定読者

<table>
<tr><td colspan="2" rowspan="3">解説書の構成</td><td colspan="5">想定読者</td></tr>
<tr><td colspan="3">自組織</td><td colspan="2">外部専門組織</td></tr>
<tr><td>情報セキュリティ責任者</td><td>LAN 管理者・運用者</td><td>設計・開発
担当者</td><td>運用者</td><td>設計・開発者</td></tr>
<tr><td colspan="2">1.解説書の目的</td><td rowspan="4">○</td><td rowspan="4">○</td><td rowspan="4">○</td><td rowspan="4">○</td><td rowspan="4">○</td></tr>
<tr><td colspan="2">2.用語</td></tr>
<tr><td colspan="2">3.解説書の想定読者</td></tr>
<tr><td colspan="2">4.標的型攻撃の防御について</td></tr>
<tr><td colspan="2">5.人・組織対策</td><td>○</td><td>○</td><td>—</td><td>○</td><td>—</td></tr>
<tr><td colspan="2">6.技術的対策</td><td>—</td><td rowspan="7">○</td><td rowspan="7">○</td><td rowspan="7">○</td><td rowspan="7">○</td></tr>
<tr><td rowspan="2">6.1.事前対策</td><td>目的、概要、ポイント</td><td>○</td></tr>
<tr><td>対策の詳細、対策ツール</td><td>—</td></tr>
<tr><td rowspan="2">6.2.検知</td><td>目的、概要、ポイント</td><td>○</td></tr>
<tr><td>対策の詳細、対策ツール</td><td>—</td></tr>
<tr><td rowspan="2">6.3.事後対策</td><td>目的、概要、ポイント</td><td>○</td></tr>
<tr><td>対策の詳細、対策ツール</td><td>—</td></tr>
<tr><td colspan="2">7.まとめ</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td></tr>
<tr><td colspan="2">付録１：インシデントハンドリングフェーズの定義</td><td rowspan="4">—</td><td rowspan="4">○</td><td rowspan="4">○</td><td rowspan="4">○</td><td rowspan="4">○</td></tr>
<tr><td colspan="2">付録２：システムログ一覧（IOC）</td></tr>
<tr><td colspan="2">付録３：暫定対処策一覧</td></tr>
<tr><td colspan="2">付録４：システムログ一覧（証拠保全）</td></tr>
</table>

「1.解説書の目的」から「4.標的型攻撃の防御」は、本解説書の位置づけ及び利用方法を示すもので、すべての読者に読んでいただく内容となっている。「5.人・組織対策」は、インシデントレスポンスに関係する人・組織対策を解説した内容であり、自組織の情報セキュリティ責任者、LAN 管理者、LAN 運用者、外部専門組織（運用者）を想定読者とする。

「6.技術的対策」の各節の「目的」、「概要」、「ポイント」は、技術的対策を行うために機器の構成や設計及び情報システムの開発も関係するため自組織の情報セキュリティ責任者、LAN 管理者、LAN 運用者、設計・開発担当者及び、外部専門組織（運用者と設計・開発者）を想定読者とする。また、「6.技術的対策」の各節の「対策の詳細」及び「対策ツール」は、具体的な対策内容を検討するための解説内容であり、自組織の LAN 管理者、LAN 運用者、設計・開発担当者及び、外部専門組織（運用者と設計・開発者）を想定読者とする。「7.まとめ」は本解説すべてのまとめであるため情報セキュリティ責任者、自組織の LAN 管理者、LAN 運用者、設計・開発担当者及び、外部専門組織（運用者と設計・開発者）を想定読者とする。

また、以下に各組織の検討内容に合わせた本解説書と付録の利用方法を示す。

表 3.2-2　各組織の検討内容に合わせた本解説書と付録の利用方法

各組織の検討内容	本解説書と付録の該当箇所
標的型攻撃とは何か？標的型攻撃対策として必要なことは何か（概要レベル）確認したい	本解説書の 4 が該当
CSIRT 体制化にあたり必要となるプロセス（実施すべき作業）とその流れを確認したい	本解説書の 5.1 が該当
インシデントハンドリングにおいて誰が具体的に何を実施すべきか、実施にあたり必要となる能力スキルは何か確認したい	本解説書の 5.2 と付録 1 が該当
標的型攻撃対策（事前対策）の目的と具体的対策内容を確認したい	本解説書の 6.1 が該当
標的型攻撃対策（検知）の目的と具体的対策内容を確認したい	本解説書の 6.2 と付録 2 が該当
標的型攻撃対策（事後対策（暫定対処））の目的と具体的対策内容を確認したい	本解説書の 6.3.1、6.3.2、6.3.3、6.3.4[1]、6.3.5[1][2]と付録 3、4 が該当
標的型攻撃対策（事後対策（本格対処））の目的と具体的対策内容を確認したい	本解説書の 6.3.1、6.3.2、6.3.3、6.3.4[2]が該当

4. 標的型攻撃の防御について

4 章では、標的型攻撃の防御モデルを理解するために、4.1 に防御モデルの前提を 4.2 に防御モデルの概要を説明する。

4.1. 防御モデルの前提

4.1.1 に標的型攻撃の概要、4.1.2 に具体的な標的型攻撃の経路、4.1.3 に標的型攻撃のフェーズ、4.1.4 に機器構成を示す。

4.1.1. 標的型攻撃とは

最近、特定の企業や組織を狙った標的型攻撃により、重要な情報が盗まれる事件が頻発している。標的型攻撃は、対象となる組織の担当者や特定の業務を標的として巧妙に作り込まれたマルウェアを侵入・感染させる。近年では、府省庁や大企業だけではなく地方公共団体や中小企業もターゲットとなり、情報システムの脆弱性に限らず、ソーシャルエンジニアリングを利用するなど、様々な経路が攻撃に利用されている。標的型攻撃を防御するために理解すべき具体的な標的型攻撃の経路を 4.1.2 に、標的型攻撃のフェーズを 4.1.3 に示す。

4.1.2. 標的型攻撃の経路

近年、発生している標的型攻撃の代表的な経路は以下の 6 つに分類できる。

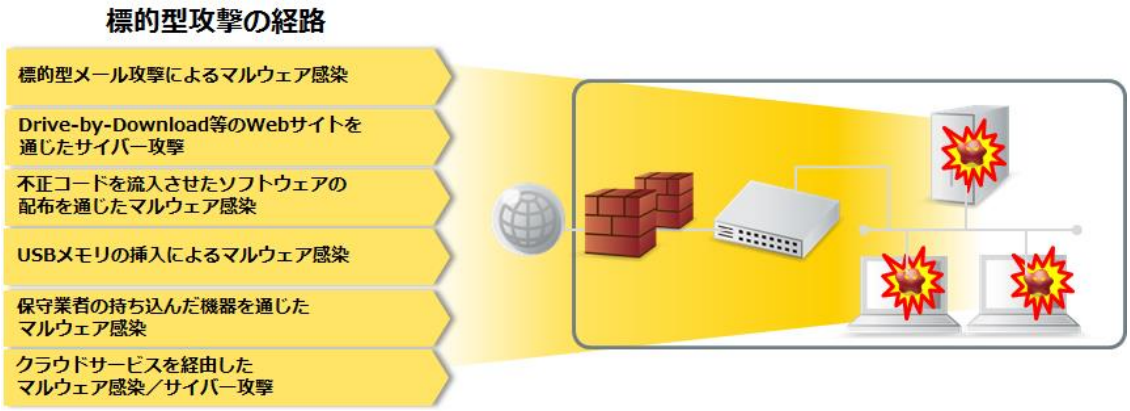

図 4.1-1 標的型攻撃の経路

表 4.1-1 標的型攻撃の経路の概要

標的型攻撃の経路	概要
標的型メール攻撃によるマルウェア感染	ここ数年、大きな問題になっている標的型メール攻撃は、「明確な意思と目的を持った攻撃者が、特定のターゲットに対して特定の目的のために行うサイバー攻撃の一種」である。特に、業務上よく利用する電子メールを利用して攻撃を仕掛けてくる特徴がある。
Drive-by-Download 等の	標的型メール攻撃に次いで、よく見られる Web サイトを通じたサイバ

Web サイトを通じたサイバー攻撃	一攻撃には、様々な攻撃手段が存在する。 ウェブブラウザや OS（オペレーティングシステム）の脆弱性を利用して、Web サイトを閲覧するユーザに気づかれないようにブラウザを介してウイルスをダウンロードさせ、感染させる「Drive-By-Download」、人間の心理的な隙や行動のミスにつけ込んで悪性サイトに誘導する「フィッシング詐欺攻撃」などマルウェアをダウンロードさせるような不正 Web サイトに誘導するサイバー攻撃である。
不正コードを流入させたソフトウェアの配布を通じたマルウェア感染	インターネットや高機能デバイスの進展と普及に伴い、利便性の高いソフトウェア（アプリを含む）が非常に入手しやすい状況となり、これに乗じた、マルウェア感染事例も多発している。
USB メモリの挿入によるマルウェア感染	重要情報の取扱いや生産・供給に関する運用をするネットワークは、セキュリティの観点からインターネット等の外部ネットワークとは隔離された状態にある。しかし、業務に必要な情報資料等を内部へ持込み、また外部へ持ち出すため、USB メモリ等の外部記憶媒体を利用することがある。特に最近は、ウイルス対策ソフトでは検知することが難しいマルウェアが急増しているため、このような外部記憶媒体を通じたマルウェア感染が増加傾向にある。
保守業者の持ち込んだ機器を通じたマルウェア感染	ユーザが、自らの努力によるセキュリティ対策を行っても、サイバー攻撃を受ける状況が発生している。その多くが、所有しているシステムの保守を担当させている委託業者を通じた不正コードの混入によるサイバー攻撃である。
クラウドサービスを経由したマルウェア感染／サイバー攻撃	クラウドサービスの発展に伴い Web アプリが急増している。また、知的財産の概念やその重要性が浸透していない地域ではファイルストレージや P2P による海賊版ソフトウェア等の問題が深刻化している。

4.1.3. 標的型攻撃のフェーズ

標的型攻撃はマルウェアの侵入から攻撃に至るまで攻撃のフェーズによって挙動や振る舞いが異なる。昨今の標的型攻撃のすべてを未然に防ぐことは、困難なため、本格的な攻撃実行の前に如何に検知できるかによって被害の最小化や拡大防止が可能になる。

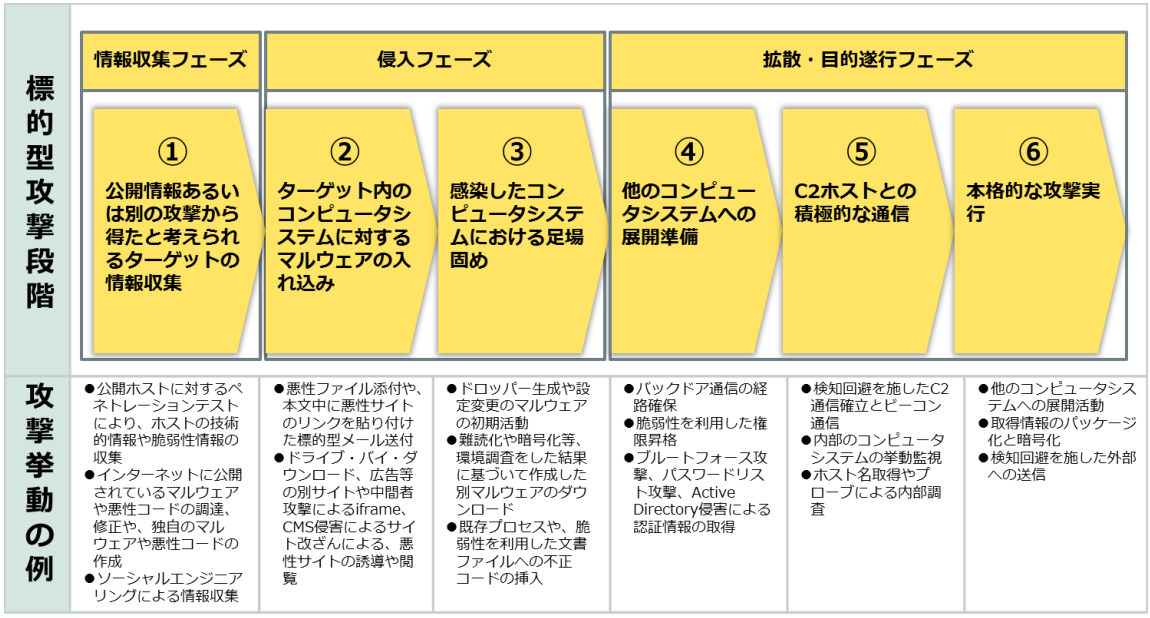

図 4.1-2 標的型攻撃のフェーズ

上記で示したとおり、「①公開情報或いは別の攻撃から得たと考えられるターゲットの情報収集」は、情報収集フェーズであり、「②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み」、「③感染したコンピュータシステムにおける足場固め」は、侵入フェーズ、「④他のコンピュータシステムへの展開準備」、「⑤C2 ホストとの積極的な通信」、「⑥本格的な攻撃実行」は拡散・目的遂行フェーズに分類できる。

4.1.4. 機器構成

防御モデルの機器の構成を以下に示す。防御モデルのネットワーク構成は、DMZ 及び本部拠点ネットワーク、支部拠点ネットワークから構成する。

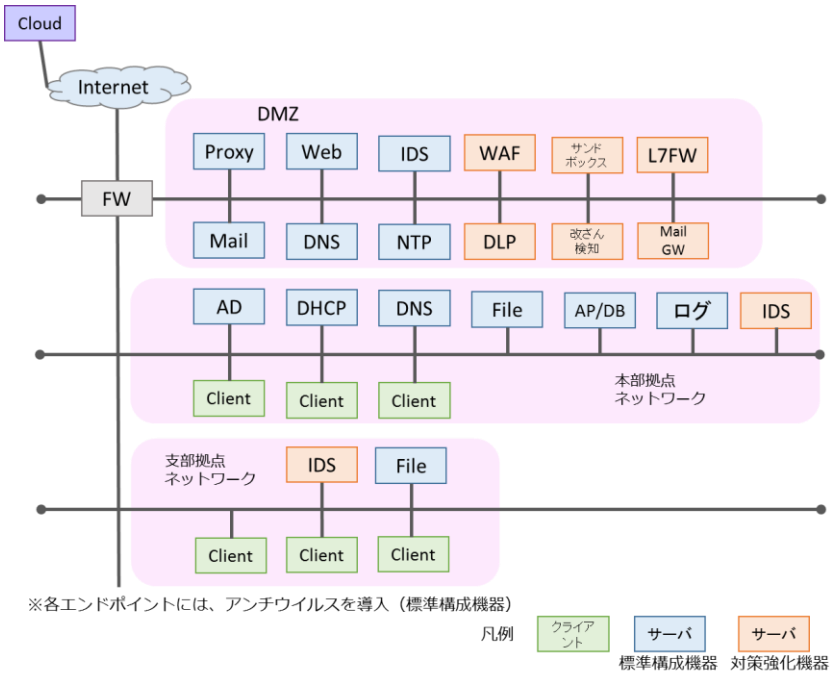

図 4.1-3 機器構成図

また、機器構成は、導入・運用コストを考慮し、標準構成機器と対策強化機器（表 4.1-2 機器構成表）に分類する。標準構成機器は、企業が一般的に設置することが想定される機器であり、対策強化機器は、標準的な機器構成を基に、さらに標的型攻撃への対策を強化したい場合は、導入検討する機器である。

表 4.1-2 機器構成表

区分	機器設置場所	機器
標準構成機器	DMZ	ファイアウォール（FW）
		ネットワーク型 IDS
		Web サーバ
		AP サーバ
		DB サーバ
		プロキシサーバ
		DNS サーバ
		メールサーバ
	内部セグメント	スイッチ／ルータ
		ドメインコントローラ
		DHCP サーバ

区分	機器設置場所	機器
		DNS サーバ（内部 DNS）
		ファイルサーバ
		エンドポイント（Windows、Linux、ブラウザ、AntiVirus）
対策強化機器	DMZ	L7FW（NGFW、APFW）
		DLP
		Mail ゲートウェイ
		WAF
		サンドボックス
		改ざん検知
	内部セグメント	ホスト型 IDS

なお、ホスト型 IDS は、DMZ 及び内部セグメントに設置する場合があるため、上記の表では、DMZ 及び内部セグメントの双方に記載。

4.2. 防御モデルの概要

防御モデルは、『人・組織対策』と『技術的対策』で構成する。人・組織対策は、インシデントレスポンスに関するプランニングとインシデントハンドリングで構成する。また、技術的対策は、事前対策と検知、事後対策から構成する。

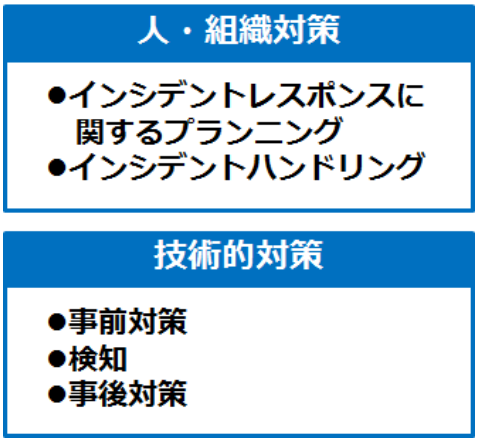

図 4.2-1 防御モデル（人・組織対策と技術的対策）

- インシデントレスポンスに関するプランニングは、標的型攻撃などを受けた場合を想定し、インシデントハンドリングをどのように行うかについての計画（プランニング）をする。

- インシデントハンドリングは、標的型攻撃を受けるなど、インシデント（又はおそれ）が発生した時に行う活動のうち、特にインシデント（又はおそれ）の発生から解決までの一連の処理を実施する。
- 事前対策は、被害を未然に防ぐ、又は攻撃者の攻撃コストを高め被害に遭いにくくするための技術的な対策を実施する。
- 検知は、システムログ等の分析により事前対策をすり抜けた攻撃を認知するための技術的な対策を実施する。
- 事後対策は、標的型攻撃を受けた後の被害拡大の防止・抑制のための対処及び標的型攻撃による被害の全貌の分析と把握を実施する。

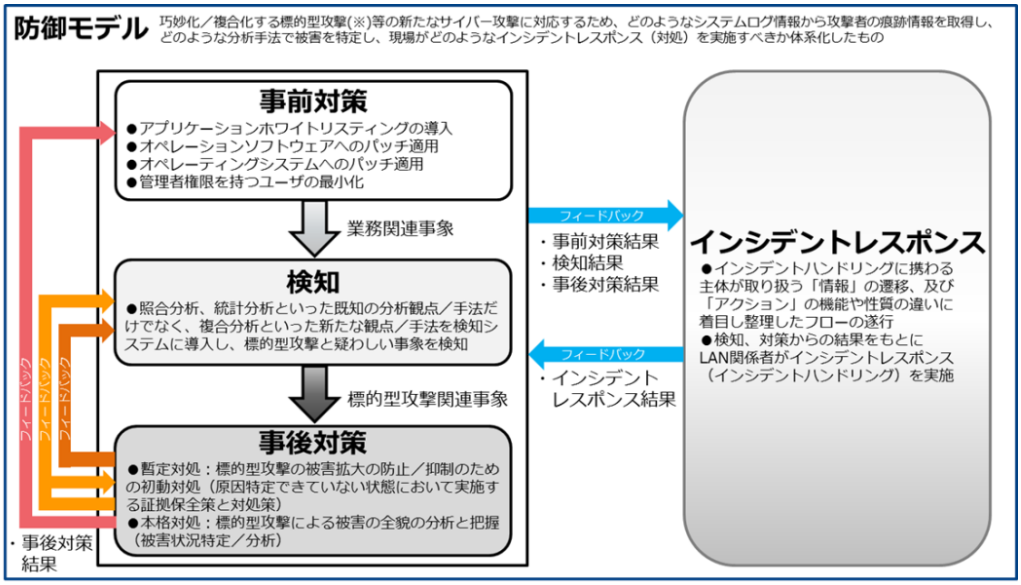

図 4.2-2 防御モデルの概要図

5. 人・組織対策

5 章では、標的型攻撃などを受けた場合を想定し、インシデントレスポンスについて説明する。インシデントレスポンスは、インシデントマネジメント、インシデントハンドリング及びプランニングを包含するため、以下のように再定義した。人・組織対策では、このなかで特に重要となる対策として 5.1 にインシデントレスポンスに関するプランニングを、5.2 にインシデントマネジメントのインシデントハンドリングを示す。

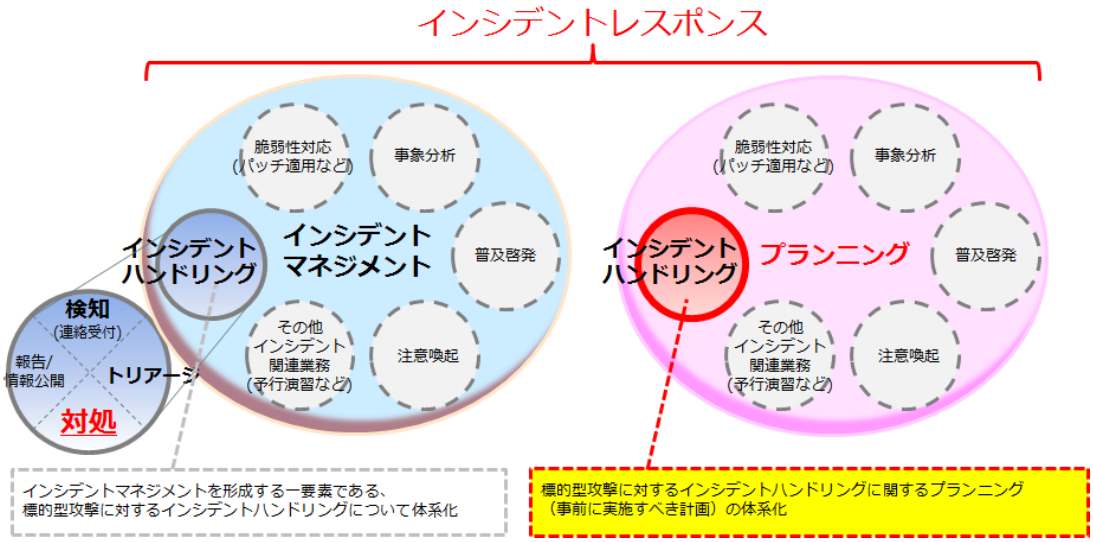

図 5-1 インシデントレスポンスの定義

なお、JPCERT/CC「CSIRT ガイド」より引用し加筆修正（記載変更箇所は下線付き赤字で記載）

5.1. インシデントレスポンスに関するプランニング

5.1.1. 目的

標的型攻撃などを受けた場合を想定し、実際にインシデントハンドリングを行うために必要となる体制や規定等を整備するとともに、組織としての対応計画を策定する。

5.1.2. 概要

インシデントレスポンスに関するプランニングは、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 つのプロセスで構成される。①～③は、CSIRT 体制設置を目的としたプロセスを示している。

表 5.1-1 プランニングの 5 つのプロセス

プロセス	目的	活動
①参考文献調査及び情報収集	体制作りのための資料の獲得	JPCERT/CC 公的文書やネットメディア特集記事を収集
②経営層からの体制構築の承認獲得	経営層からの CSIRT 体制構築の承認獲得	CSIRT の必要性の説明
③組織内の現状把握及び関係部門との調整	CSIRT 体制のリソース確保と役割設定	関連する部門との協議
④CSIRT 体制の設置及び簡易的な演習	CSIRT 活動開始の宣言	経営層に報告及び社内報で全社員に通知
⑤活動に係る文書作成と定期レビュー	活動内容の説明	インシデント対処の流れの作成

5.1.3. ポイント

プランニングの各プロセスにおける検討のポイントを以下に示す。

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）

実行性を確保した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を、詳細な情報の収集や経験者へのインタビュー等をもとに行う。

② 経営層からの体制構築の承認獲得（体制構築及び準備活動等の獲得）

CSIRT の必要性の説明だけではなく、現状の対応体制／能力の課題（不足等）やその課題を踏まえた計画の提示を行う。

③ 組織内の現状把握及び関係部門との調整

関連する部門におけるインシデントに対する認識と対応活動の状況について把握し、協議により連携のための取決めを行うことで協力姿勢を醸成させる。

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等（セミナー、ワークショップ、机上演習）により、関連部門が取るべき行動の実効性を確保する。

⑤ CSIRT 活動に係る文書作成と定期レビュー

現状の変化に基づく定期レビューの実施を規定に盛込み、組織内へ周知徹底する。

5.1.4. 詳細

インシデントレスポンスに関するプランニングの詳細を以下に示す。

表 5.1-2 インシデントレスポンスに関するプランニング（詳細）

プロセス	NO	項目	詳細
① 参考となる文献調査	1	利害関係者及び内部関係者の見出し	CSIRT 体制の計画段階で関与すべき関係者、レスポンス支援する担当者、組織内外との情報共有する担当者などの役割を規定化
	2	情報収集	外部にある関連情報の収集、組織内状況や過去の組織等の把握
② 経営層からの体制構築の承認獲得	3	管理者層の支援を獲得	支持をいただく役員を見つける／ビジネスにもたらすメリット作成／リサーチや情報収集のリソースを獲得
	4	CSIRT プロジェクト計画を作成	プロジェクトリーダーを指定／管理者層のコンセプトをタスクに反映させる
	5	サービス対象の見出し	最初のサービス対象を決定／提供サービスの特定／戦略的パートナーの特定／サービス対象とのやり取り方法
	6	CSIRT 運用のための財源獲得	スタッフの教育訓練、使用機器、レスポンス情報の保護のための施設のための財源を獲得
	7	スタッフ、設備、インフラのリソースの要求事項を特定	インフラのセキュリティ確保／情報処理プロセスの明確化／スタッフの訓練計画
	8	役割、責任、権限の明確化	全ての CSIRT機能を発揮させるため／権限を行使する領域の曖昧或いは重複する領域を見出し
③ 組織内の現状把握及び関係部門との調整	9	情報収集	組織内状況理解のために様々な利害関係者と意見交換の場を持つ／関係組織との取決めを策定
④ CSIRT 体制の設置及び簡易的な演習	10	CSIRT ミッションの明文化	本質的かつ長期的なもの／最優先の達成すべき水準を決定／利害関係者と合意形成
	11	提供サービスの範囲とレベルを決定	既存の専門知識やリソースで実現可能なものから開始／提供サービスの可能時間や方法の決定
	12	CSIRT 報告機構、権限、組織モデル	組織の状況に見合った体制を設定し、継続的に更新／スタッフの教育準備
	13	やり取り及び連絡窓口の明確化	組織内部門及び外部組織との連携の確立／CSIRT スタッフ間の内部コミュニケーション方法の確立

	14	運用開始時における CSIRT 周知	管理者層から正式な告知をしてもらう／CSIRT サービスに関する情報の入手方法を確立
⑤ CSIRT 活動に係る文書作成と定期レビュー	15	ワークフローの文書化	CSIRT のプロセス及びやり取りの文書化／品質を確保するための方法及びコンポーネントの構築
	16	ポリシー及び対応プロシージャの構築	用語解説／インシデント種別、優先度、対応割り当ての決定／報告及び公開方法
	17	実装計画とフィードバック報告の作成	利害関係者とサービス対象から実装計画に関するインプットを得る／フィードバックを基にした計画更新
	18	CSIRT のパフォーマンス評価方法を作成	インシデント報告及びハンドリングに関するベースラインを作成／サービス対象へのフィードバック
	19	CSIRT の全構成要素のバックアップ計画	CSIRT の重要な機能、サービス、施設を特定／リカバリープランの設計／緊急時の対応訓練
	20	臨機応変（≒変更管理）	状況変化に応じたサービス変更、新しいスキルセットの習得、連携すべきパートナー探しの実施及びそれに伴う変更管理

5.2. インシデントハンドリング

5.2.1. 目的

標的型攻撃を受けるなど、インシデントが発生したときに行う活動のうち、特にインシデントの発生から解決までの一連の処理を行う。

5.2.2. 概要

インシデントハンドリングを行うための状況把握や意思決定は、事象の発見から調査・対処及び再発防止策までが必要となり、インシデントハンドリングにおいて状況把握・意思決定に必要な以下の 7 つの活動で構成される。

表 5.2-1 7 つの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

5.2.3. ポイント

インシデントハンドリングにおいて状況把握・意思決定に必要となる検討のポイントを以下に示す。

表 5.2-2 状況把握・意思決定に必要となる検討のポイント

インシデント ハンドリングフェーズ	検討のポイント
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する。
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を行うとともに、適切な部門・組織に対して必要な情報を伝達する。
C. 被害拡大の防止や抑制のための初動対処	被害拡大が進行していると判断された事象の場合、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。
D. 原因推定のための簡易的調査	被害が拡大しておらず、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。
E. 本格調査	技術的調査を外部専門組織に依頼するとともに、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的な観点に基づく管理的調査を LAN 関係者が行う。
F. 技術的調査結果と運用的調査結果の関係性分析	外部専門組織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管理的調査の結果について関係性を分析し、インシデントの実態を判定する。
G. 再発防止策の立案	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する技術的及び管理的な対策立案を行う。

5.2.4. 詳細

インシデントハンドリングは、6 つの主体（役割）が、7 つのフェーズで求められる「アクション」、アクションを行うために必要となる「インプット」、アクション後の「アウトプット」及び「要求事項（能力スキル）」等が必要となる。6 つの主体（役割）を以下に示す。

表 5.2-3 インシデントハンドリングの 6 つの主体（役割）

主体（役割）	概要
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	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

（情報システム部門）	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	組織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

各フェーズにおけるアクション及びインプットとアウトプットの概要を以下に示す。なお、詳細は本解説書の付録 1 のインシデントハンドリングフェーズの定義を参照。

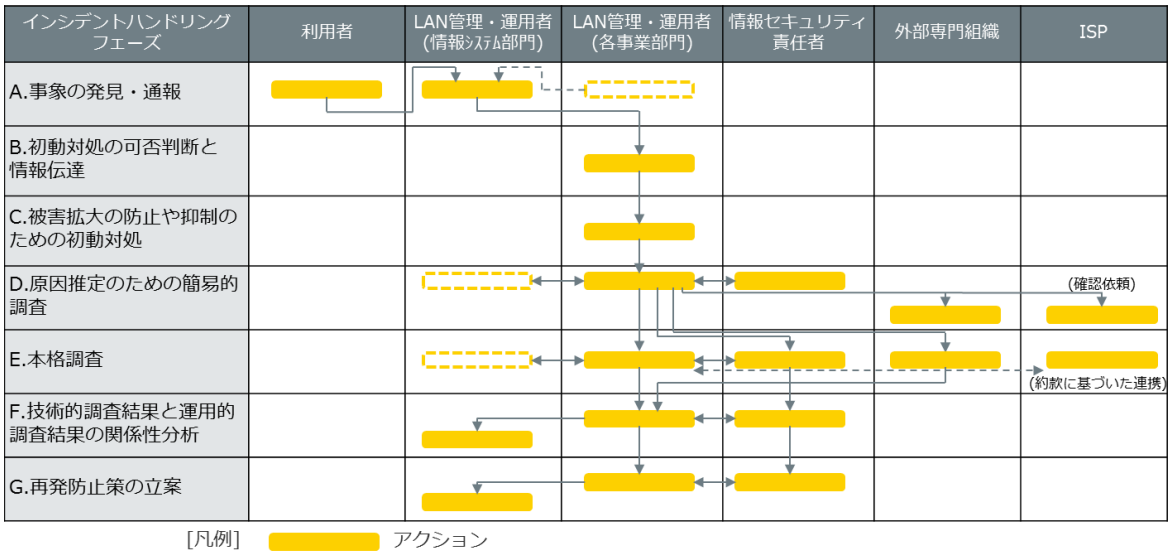

図 5.2-1 インシデントハンドリングにおけるアクション概要

5.2.5. 対策ツールの利用方法

[1] 付録 1 ：インシデントハンドリングフェーズの定義

付録 1 のインシデントハンドリングフェーズの定義は、6 つの主体（役割）が、7 つのインシデントハンドリングフェーズで求められる「アクション」、及びアクションを行うために必要となる「インプット」やアクション後の「アウトプット」及び「要求事項（能力スキル）」を示している。この付録 1 を参考に各主体がインシデントハンドリングフェーズにおいて具体的なアクション等を想定したインシデントハンドリングに関する計画を検討できる。以下に LAN 管理・運用者（各事業部門）の C.被害拡大の防止や抑制のための初動対策に関する「アクション」、「インプット」、「アウトプット」の具体例を示す。

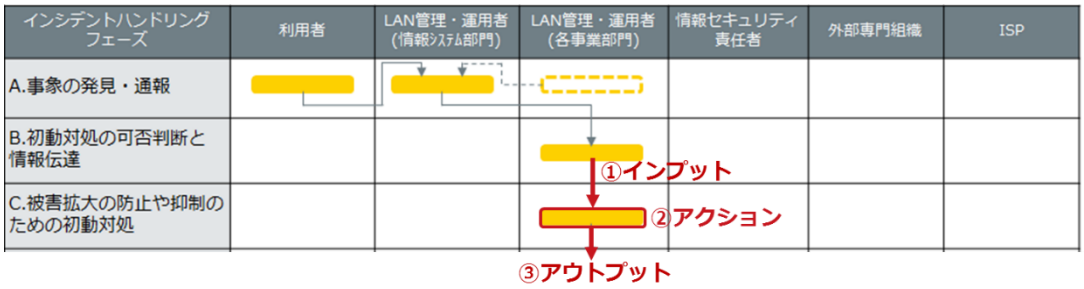

図 5.2-2 LAN 管理・運用者（各事業部門）のインシデントハンドリングフェーズ C
（付録 1 の抜粋）

表 5.2-4 LAN 管理・運用者（各事業部門）のアクション等の具体例
（付録 1 の抜粋）

インプット	・ 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
アクション	・ 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
アウトプット	・ 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

以下に具体例として、「A.事象の発見・通報」から「G.再発防止策の立案」の各フェーズにおける LAN 管理・運用者（各事業部門）のアクションを示す。

なお、6 つの主体（役割）が各フェーズで求められる「アクション」や「要求事項（能力スキル）」については、付録 1 を参照。

表 5.2-5 具体的なインシデントハンドリングのアクション
（LAN 管理・運用者（各事業部門））

活動項目	LAN 管理・運用者（各事業部門）のアクション
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
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
C.被害拡大の防止や抑制のための初動対処	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
D.原因推定のための簡易的調査	被害進行がされていなく、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
E.本格調査	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
F.技術的調査結果と運用的調査結果の関係性分析	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
G.再発防止策の立案	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

6. 技術的対策

6 章の技術的対策は、6.1 節に事前対策を 6.2 節に検知を 6.3 節に事後対策を示す。

6.1. 事前対策

6.1.1. 目的

被害を未然に防ぐ、又は攻撃者の攻撃コストを高め被害に遭いにくくするための技術的な対策を実施する。

6.1.2. 概要

事前対策は、以下の 3 つの対策で構成する。

表 6.1-1 3 つの事前対策

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管理権限の最小化

6.1.3. ポイント

[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することにより、未承認のアプリケーションの実行を防止する。

[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）

アプリケーション及びオペレーティングシステムのセキュリティパッチ適用に際しては、特にリスクの高い脆弱性について、セキュリティパッチの公開後迅速に適用する。

[3] 管理権限の最小化

OS やアプリケーションに対する管理者権限（特権）を持つユーザ数を最小化するだけでなく、特権を持たない一般利用者権限アカウントで定常運用を行う。また、特権の最小化を維持するために発行済アカウントの棚卸を定期的に行う。

なお、前述の標準構成機器による一般的な対策が行われていることを前提としている。

表 6.1-2 標準構成機器による一般的な対策

対策	実現内容
ファイアウォール	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

6.1.4. 詳細

[1] アプリケーションの利用制限

正規アプリケーション（標的型攻撃と関連性が認められない、業務目的のアプリケーション）の挙動のみを許可する。

正規アプリケーションの特徴情報をホワイトリスト化し、正規アプリケーションのみ起動を許可することで、エンドポイントの事前対策（予防対策）を実施する。

[2] アプリケーション／オペレーティングシステムを最新の状態に保持

IT システムで利用される OS、又はアプリケーションでは、セキュリティ上の欠陥である脆弱性が定期的に発見され、対処するためのセキュリティパッチが公開されていることから、組織のネットワークに接続する機器の OS やソフトウェアの一覧表を保持し、脆弱性情報の収集やパッチ適用を実施する。

[3] 管理権限の最小化

標的型攻撃においては、攻撃者が侵入後に AD サーバなどの認証サーバの管理者アカウントを窃取し、組織内の感染を拡大させる手口が用いられるため、これらを未然に防止するために必要な対策として実施する。

AD サーバなどの利用者権限の認証サーバへの管理者権限でのアクセスを最小限に限定し、アクセスログを定期的にチェックする。

なお、上記対策は、オーストラリア国防信号局（The Defence Signals Directorate：DSD）が提唱する『サイバー攻撃に対抗するプロアクティブなアプローチ[1]』の 35 の軽減戦略のうちの「アプリケーションの利用制限」、「アプリケーションを最新の状態に保持」、「オペレーティングシステムを最新の状態に保持」、「管理権限の最小化」は、上位 4 つであり、この 4 つの対策を実施することで、少なくとも 85%のサイバー攻撃が防御可能と試算している。以下に『サイバー攻撃に対抗するプロアクティブなアプローチ』に記載されている 4 つの対策の評価結果を記載する。

表 6.1-3 事前対策の評価結果

事前対策	評価軸		
	導入障壁（利用者面）	導入コスト	維持管理コスト
アプリケーションの利用制限	中	高	中
アプリケーションを最新の状態に保持	低	高	高
オペレーティングシステムを	低	中	中

[1] Strategies to Mitigate Targeted Cyber Intrusions:ASD Australian Signals Directorate http://www.asd.gov.au/infosec/top-mitigations/mitigations-2014-table.htm

最新の状態に保持			
管理権限の最小化	中	中	低

6.1.5. 対策ツール

[1] アプリケーション・ホワイトリスティングの導入

例えば、特定のアプリケーションを実行禁止や実行可能にできる AppLocker を利用する。

AppLocker は、Windows Server 2008 R2 と Windows 7 で導入されたソフトウェア制限ポリシーのアプリケーション制御機能である。AppLocker は、ファイルの固有 ID に基づいてアプリケーションの実行許可や拒否のルールを作成し、アプリケーションを実行できるユーザやグループを指定することができる。

[2] アプリケーションへのパッチ適用 ／オペレーティングシステムへのパッチ適用

例えば、更新プログラムを集中管理する Windows Server Update Services （WSUS）を利用する。

WSUS を利用して Windows オペレーティングシステムを実行しているコンピュータに対して、Microsoft 製品の最新の更新プログラムを展開できる。

6.2. 検知

6.2.1. 目的

事前対策をすり抜けた攻撃を認知するためにシステムログに残される痕跡（IOC：Indicator of Compromise）を分析し、標的型攻撃を検知する。

6.2.2. 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。

表 6.2-1 3 つの分析観点

①照合分析
②統計分析
③複合分析

6.2.3. ポイント

[1] 分析の観点

システムログによる検知では①照合分析、②統計分析だけでなく、③複合分析を行う。

[2] 照合分析及び統計分析

照合分析は、既知の標的型攻撃事象と一致するかどうか、統計分析は、既知の標的型攻撃事象との類似点があるかどうかを分析する。

[3] 複合分析

複合分析は、通常業務と不一致、又は乖離するイベントについて、同一イベントの連続性／異なるイベントの組み合わせの二観点でさらに分析する。

6.2.4. 詳細

[1] 検知の概要

標的型攻撃に利用される攻撃手法によりシステムログに残される痕跡（IOC）を検知に利用する。様々な IOC から、照合分析（＝既知の標的型攻撃事象と一致)、統計分析（＝既知の標的型攻撃事象との類似）といった既知の観点だけでなく、複合分析（＝通常業務との不一致や通常業務からの乖離といった特徴から、同一イベントの連続性／異なるイベントの組み合わせから標的型攻撃と疑わしい事象を見出す）といった新たな観点を検知システムに導入し、標的型攻撃と疑わしい事象の検知を実現する。以下に検知の概要を示す。

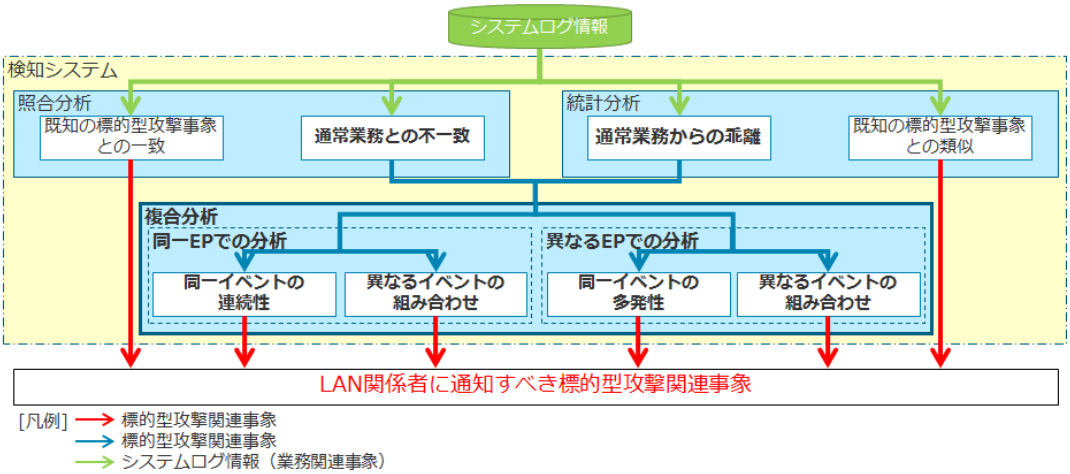

図 6.2-1 検知の概要

[2] 検知の観点

照合分析、統計分析及び、複合分析の概要と分析に利用する情報について以下に示す。

表 6.2-2 分析に利用する情報

分類	概要	分析観点	分析に利用する情報等
照合分析	単一のログレコードと「脅威の特徴情報」とを照合	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
統計分析	システムログ情報に対して、標的型攻撃の	既知の標的型攻撃関連事象との類似	・ 通信先数 ・ エラー応答数 ・ 一定間隔で発生する通信

分類	概要	分析観点		分析に利用する情報等
	量的な類似性を確認	通常業務との乖離		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
複合分析	照合･統計分析の結果、同一又は複数エンドポイントの事象を組み合わせた分析	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	同一イベントの連続性	・ 「照合分析 － 通常業務との不一致　分析観点」及び「統計分析 － 通常業務との乖離　分析観点」の組み合わせ
			異なるイベントの組み合わせ	・ 「照合分析 － 通常業務との不一致　分析観点」及び「統計分析 － 通常業務との乖離　分析観点」の組み合わせ

上記で示した分析観点及び検知した場合に想定できる事象や対処（通知）の考え方を以下に示す。

(1)　照合分析

システムログ情報における単一のログレコードを以下の分析観点で照合する。以下の 2 種類の分析観点のいずれかの条件に該当した場合、標的型攻撃関連事象として検知する。

(ア)既知の標的型攻撃関連事象との一致

過去の標的型攻撃事例において確認された、既知の標的型攻撃関連事象の脅威特徴情報を使用する。これらとシステムログ情報を照合し、いずれかの特徴情報と一致した場合、標的型攻撃関連事象として検知する。

検知した標的型攻撃関連事象は既知の標的型攻撃関連事象と特徴情報が一致することから、標的型攻撃の疑いの確度が高いと判断し、検知後、直ちに LAN 関係者に通知する。

(イ)通常業務との不一致

通常業務における業務事象での発生頻度が低い事象に見られる特徴情報を使用する。これらとシステムログ情報とを照合し、いずれかの特徴情報報と一致した場合、標的的型攻撃関連事象として検知する。

検知した標的型攻撃関連事象は、発生頻度が低い通常業務である可能性もあるため、単独では標的型攻撃の疑いの確度は低い。そのため、単独では通知せず、複合分析の対象とする。複合分析により他の標的型攻撃関連事象との関係性が見られた場合、複合分析による検知結果として LAN 関係者に通知する。

(2) 統計分析

システムログ情報における複数のログレコードを集計して得る様々な統計値の類似性を比較する。以下の 2 種類の分析観点のいずれかの条件に該当した場合、標的型攻撃関連事象として検知する。

(ア)既知の標的型攻撃関連事象との類似

過去の標的型攻撃事例において確認された、既知の標的型攻撃関連事象の統計的な特徴を使用する。これらとシステムログ情報の統計値を比較し、いずれかの特徴情報が近い値であった場合、標的型攻撃関連事象として検知する。

検知した標的型攻撃関連事象は既知の標的型攻撃関連事象と特徴情報が類似していることから、標的型攻撃の疑いの確度が高いと判断し、検知後、直ちに LAN 関係者に通知する。

(イ)通常業務との乖離

通常業務における業務事象の統計的な特徴を使用する。これらとシステムログ情報の統計値を比較し、いずれかの特徴情報から大きく乖離した値であった場合、標的型攻撃関連事象として検知する。

検知した標的型攻撃関連事象は、短時間での特定の業務の集中、発生頻度の低い大量のデータ送信業務など、一時的な統計値の変化に起因するものである可能性もあるため、単独では標的型攻撃の疑いの確度は低い。そのため、単独では通知せず、複合分析の対象とする。複合分析により他の標的型攻攻撃関連事象との関係性が見られた場合、複合分析による検知結果として LAN 関係者に通知する。

(3) 複合分析

照合分析（通常業務との不一致)、統計分析（通常業務との乖離）によって検知された単独では確度の低い標的型攻撃関連事象の組み合わせに着目した分析を行う。分析観点は以下の 4 種類に大別し、いずれかの条件に該当した場合、標的型攻撃関連事象として検知する。複合分析により検知された標的型攻撃関連事象は、全て LAN 関係者への通知対象とする。

(ア)同一エンドポイントにおける同一イベントの連続性

単独では確度の低い標的型攻撃関連事象が、同じエンドポイント間で連続的に発生していた場合、標的型攻撃関連事象として検知・通知する。

本分析観点では、主に、マルウェアによる C&C サーバとの定期的な通信等の継続的に発生する事象を捉えることが想定できる。

(イ)同一エンドポイントにおける異なるイベントの組合せ

単独では確度の低い標的型攻撃関連事象が、同じエンドポイント間で複数種類発生していた場合、標的型攻撃関連事象として検知・通知する。

本分析観点では、主に、特定のエンドポイントに対する攻撃段階の進行を捉えることが想定できる。

(ウ)複数エンドポイントにおける同一イベントの多発性

単独では確度の低い標的型攻撃関連事象が、異なる複数のエンンドポイント間で同時に発生していた場合、標的型攻撃関連事象として検知・通知する。

本分析観点では、主に、組織内部における攻撃の広がりを捉えることが想定できる。

(エ)複数エンドポイントにおける異なるイベントの組合せ

単独では確度の低い標的型攻撃関連事象が、異なる複数のエンドポイント間で複数種類発生しており、かつ、それらの標的型攻撃関連事象に共通的に係わるエンドポイントが確認された場合、標的型攻撃関連事象として検知・通知する。

本分析観点では、あるエンドポイントに対して攻撃が成功した後、他のエンドポイントへの攻撃対象の移行の試み（攻撃経路の繋がり）を捉えることが想定できる。

6.2.5. 対策ツールの利用方法

[1] 付録 2：システムログ一覧（IOC）

付録 2 のシステムログ一覧（IOC）は、4.1.4 で示した具体的な機器構成において、どのようなシステムログを標的型攻撃の検知に活用できるかを示している。以下に付録 2 の利用方法を示す。

ログとして扱うことができる情報				[検知]標的型攻撃関連事象の痕跡									
				②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み		③感染したコンピュータシステムにおける足場固め		④他のコンピュータシステムへの展開準備		⑤C2ホストとの積極的な通信		⑥本格的な攻撃実行	
区分	機器設置場所	機器	ログ項目	攻撃手法A	攻撃手法B	攻撃手法C	攻撃手法D	攻撃手法E	攻撃手法F	攻撃手法G	攻撃手法H	攻撃手法I	攻撃手法J
標準構成機器	DMZ	ファイアウォール(FW)	日時										
			ファイアウォールホスト名									○	
			ファイアウォールルール名及び番号			○						○	
			インバウンドインタフェース						○			○	
			アウトバウンドインタフェース						○			○	
			MACアドレス										
			パケットサイズ										
			IPパケット優先度 (TOS,PREC)										
			IPパケット生存期間 (TTL)							○			
			IPフラグメントパケット識別子 (ID)										
			IPフラグメンテーション情報 (DFビット)										
			ソースIPアドレス										
			ソースポート番号										
			宛先IPアドレス										
			宛先ポート番号										

①

②

③

図 6.2-2 付録 2 システムログ一覧（IOC）の概要図

(1) 一覧表の見方

「ログとして扱うことができる情報」は、「区分」、「機器設置場所」、「機器」、「ログ項目」によって、システムログが取得可能な機器情報と該当のシステムログが含むシステムログ項目を把握できる。

「[検知]標的型攻撃関連事象の痕跡」は、どの攻撃フェーズのどのような攻撃手法でシステムログに痕跡が残るかを通じて、検知に活用可能なシステムログ／システムログ項目を理解できる。

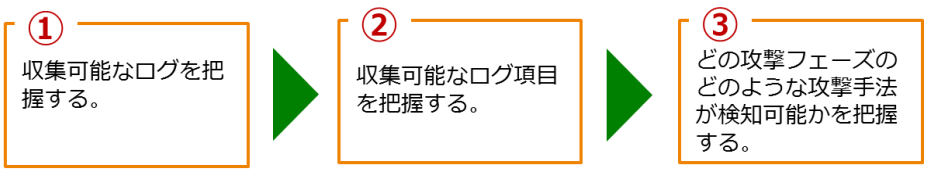

図 6.2-3 付録 2 システムログ一覧（IOC）の利用手順

(2) 利用手順

- 手順①：収集可能なログを把握する
  - 4.1.4 機器構成で示した区分（標準構成機器／対策強化機器）、機器設置場所（DMZ／内部セグメント）、機器（ファイアウォール、Web サーバ等）において収集可能なログを把握する。

- 手順②：収集可能なログ項目を把握する
  - 具体的に取得・保全すべきログ項目を把握する。

- 手順③：どの攻撃フェーズのどのような攻撃手法が検知可能かを把握する
  - 取得したシステムログが、4.1.3 標的型攻撃のフェーズで示したどの攻撃フェーズのどのような攻撃手法が検知可能であるかを把握する。
  - 付録 2 システムログ一覧（IOC）は、4.1.2 標的型攻撃の経路ごとに自組織で発生する可能性の高い経路について取得すべきシステムログを把握する。

表 6.2-3 分析に利用する情報

フェーズ分類	攻撃フェーズ（詳細）	検知の観点
攻撃侵入フェーズ	①公開情報或いは別の攻撃から得たと考えられるターゲットの情報収集	基本検知ログ
	②ターゲット内のコンピュータシステムに対するマルウェアの入れ込み	
	③感染したコンピュータシステムにおける足場固め	
拡散フェーズ	④他のコンピュータシステムへの展開準備	拡張検知ログ
	⑤C2 ホストとの積極的な通信	
目的遂行フェーズ	⑥本格的な攻撃実行	

6.3. 事後対策

6.3.1. 目的

標的型攻撃を受けた後の被害拡大の防止／抑制のための対処及び標的型攻撃による被害の全貌を分析し把握する。

6.3.2. 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」から構成される。

表 6.3-1 事後対策

①暫定対処：標的型攻撃の被害拡大の防止／抑制のための初動対処 ②本格対処：標的型攻撃による被害の全貌分析／特定

6.3.3. ポイント

[1] 暫定対処

- 原因特定できていない状態において、被害の拡大防止と被害の最小化のために実施可能な対策を実施する。
- 暫定対処策により、C（機密性）、I（完全性）、A（可用性）の喪失可能性が異なることを考慮して、実施内容を検討する。
- 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行う。

[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があり、あらかじめ組織的な対策としてインシデントレスポンスに関するプランニングも含めて検討する。

6.3.4. 詳細

暫定対処は、標的攻撃の被害拡大の防止及び抑止のための初動対処と証拠保全が必要であり、本格対処は、標的型攻撃による被害特定及び分析が必要となる。以下に暫定対処と本格対処の概要を示す。

表 6.3-2 暫定対処と本格対処の概要

区分		詳細	
暫定対処	標的型攻撃の被害拡大の防止／抑制のための初動対処	証拠保全策	本格対処を実行するために必要となるログ（証拠）の確保
		対処策	原因特定できていない状態で被害の拡大防止と被害の最小化のために実施可能な対策
本格対処	標的型攻撃による被害の全貌分析／特定	被害状況分析／特定	システムログの分析及び侵入経路情報、拡散元／拡散先情報、流出経路／流出情報、復旧必要情報の特定

[1] 暫定対処

暫定対処では、具体的な暫定対処と暫定対処を実施した場合の CIA の影響を考慮する必要がある。以下に、付録 3 暫定対処一覧に記載した具体的な暫定対処策と暫定対処を実施することで効果を及ぼす対象を示す。暫定対象の詳細な説明及び実施した場合の CIA の影響については付録 3 に示す。

表 6.3-3 具体的な暫定対処策

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、アカウント PW 変更、アカウント権限変更、アカウント無効化、アカウント削除
EP（End Point）	注意喚起、検知感度向上、マルウェア隔離 マルウェア駆除、接続先 URL 遮断 ポート番号遮断、プロトコル遮断 IP アドレス遮断、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、ドメイン・URL 遮断 DNS（ブラックホスト名）不在応答、 DNS（ブラックドメイン名）、ポート番号遮断 プロトコル遮断、IP アドレス遮断、 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

[2] 本格対処

本格対処では、標的型攻撃による被害特定及び分析を行うために、(1) 分析準備、(2) 侵入経路の調査、(3) 流出経路の調査、(4) 流出情報の調査、(5) 拡散元／拡散先の調査、(6) 復旧必要情報の調査が必要である。以下に本格対処の概要を示す。

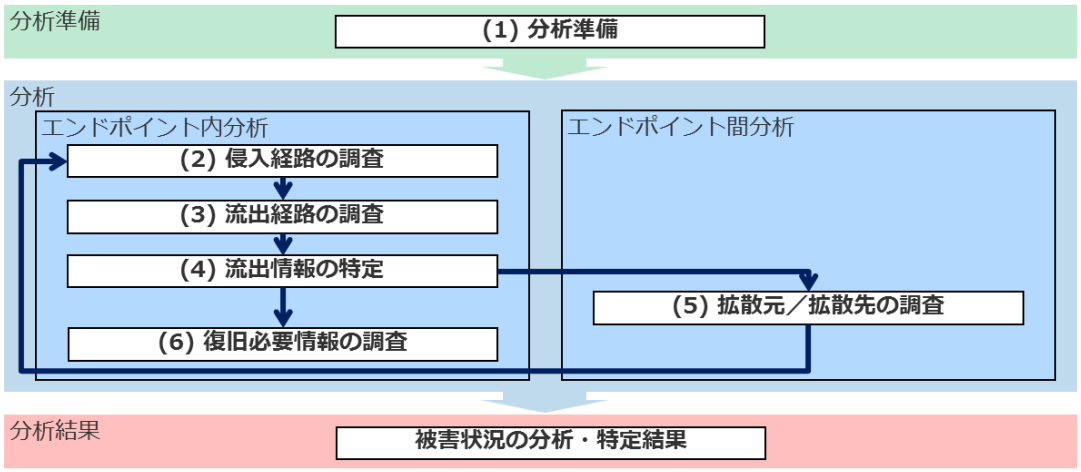

図 6.3-1 本格対処の概要

本格対処の概要で示した（2）侵入経路の調査、（3）流出経路の調査、（4）流出情報の調査、（5）拡散元／拡散先の調査、（6）復旧必要情報の調査について分析例及び分析時の確認ポイント例を以下に示す。

表 6.3-4 本格対処の分析観点

観点	分析例	分析時の確認ポイント例
侵入経路情報	どこから、どこへ、どのように侵入	・発見・検知で特定したプロセスの起動元プロセスは何か／起動元プロセスがアクセスしたファイルは何か ・そのファイルの属性は何か
拡散元／拡散先情報	どこから、どこへ、どのように拡散	・疑わしいプロセスと関連性のあるプロセスの認証試行／通信先の情報は存在するか ・疑わしいプロセスと関連性のあるプロセスが通信したエンドポイント／検索したファイルは存在するか
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	・疑わしいプロセスと関連性のあるプロセスが NW ドライブ経由で新たにファイルを生成したエンドポイントがあるか ・疑わしいプロセスと関連性のあるプロセスが USB メモリ内のファイルにアクセスしたか
復旧必要情報	発生源、パス情報、影響先	・疑わしいプロセスと関連性のあるプロセスが新たにレジストリを生成・更新したか ・プロセスが新たにファイルを生成・更新したか ・疑わしいプロセスと関連性のあるプロセスが新たにタスクを生成・更新／ハードディスクに RAW アクセスしているか

6.3.5. 対策ツールの利用方法

[1] 付録 3：暫定対処一覧

付録 3 の暫定対処一覧は、標的型攻撃などを検知した項目から CIA の影響を考慮した暫定対処の実施方法を示している。以下に付録 3 の利用方法を示す。

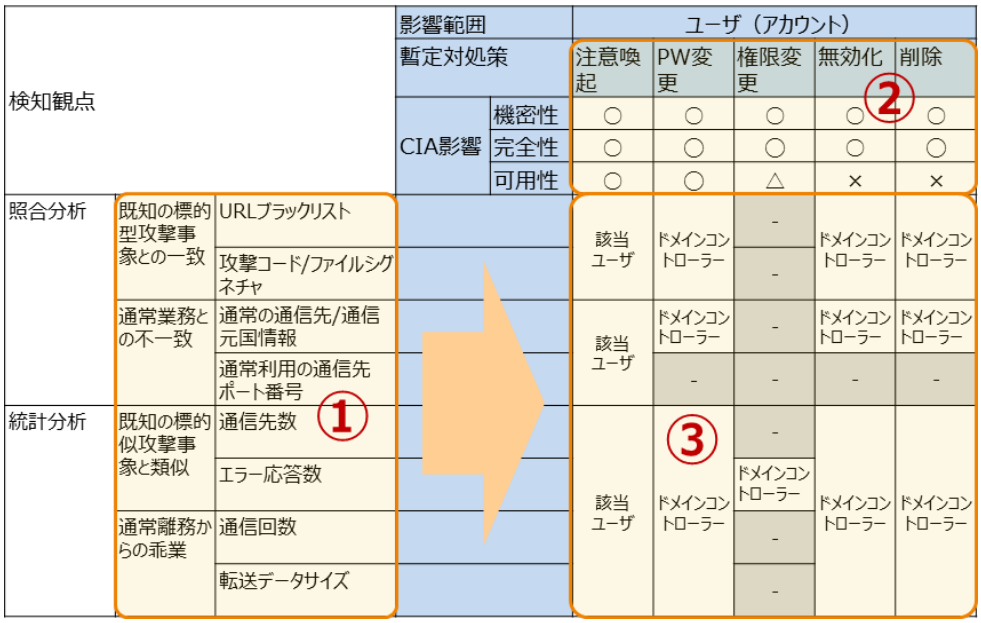

図 6.3-2 付録 3 暫定対処一覧の概要図

(1) 一覧表の見方

- 検知観点は、6.2 検知で示した検知観点（照合分析、統計分析、複合分析）に対応している。
- 影響範囲の分類は、ユーザ（アカウント）、EP（End Point）、セグメント、サービスの 4 つ（上記表はユーザ（アカウント）のみ表示）。
- 具体的な暫定対処策（上記表の暫定対処策の行）と暫定対処策を実施した場合の CIA の影響（◯ は影響無し、× は影響有り、△ は一部に影響有り）を確認できる。

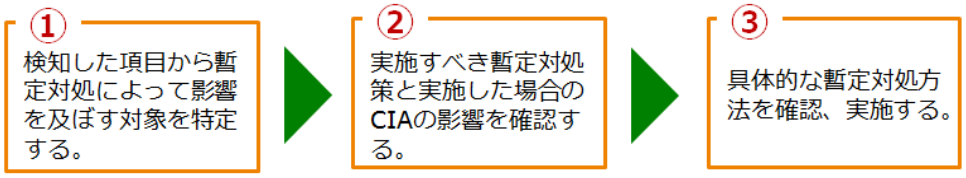

図 6.3-3 付録 3 暫定対処一覧の利用手順

(2) 利用手順

- 手順①：検知した項目から暫定対処策を特定する
  - 6.2 検知で示した検知観点（照合分析、統計分析、複合分析）から有効な暫定対処を特定する。

- 手順②：暫定対処策と CIA の影響を確認する
  - 具体的な暫定対処策と暫定対処策を実施した場合の CIA の影響を把握する。CIA 影響（機密性、完全性、可用性）は以下の通り。
    - 機密性：アクセス許可されたユーザのみが該当ユーザの情報資産にアクセスできること。
    - 完全性：ユーザの情報資産の破壊、改ざんが起きないよう保障されていること。
    - 可用性：ユーザが必要な時に該当ユーザの情報資産にアクセスできること。

- 手順③：CIA の影響を考慮した暫定対処策を確認、実施する
  - 取得したシステムログが、4.1.3 標的型攻撃のフェーズで示したどの攻撃フェーズで検知に活用できるか把握する。手順①で検知した項目と手順②で選択する暫定対処策の交点で具体的な暫定対処策を確認、実施する。

なお、手順②、③については、検知の都度暫定対処策を確認するのではなく、インシデントレスポンスのプランニングにおいて事前に計画しておくことが望ましい。

(3) 手順の例示

- 手順①：検知観点（照合分析の URL ブラックリスト）を検知。
- 手順②：ユーザに対して CIA の影響のない（機密性、完全性、可用性すべてが○）を選択。
- 手順③：該当ユーザに対して注意喚起を行う。又は、ドメインコントローラを利用しパスワードを変更する。

[2] 付録 4：システムログ一覧（証拠保全）

付録 4 のシステムログ一覧（証拠保全）は、4.1.4 で示した具体的な機器構成において、取得したシステムログを証拠保全すべきかを示している。以下に付録 4 の利用方法を示す。

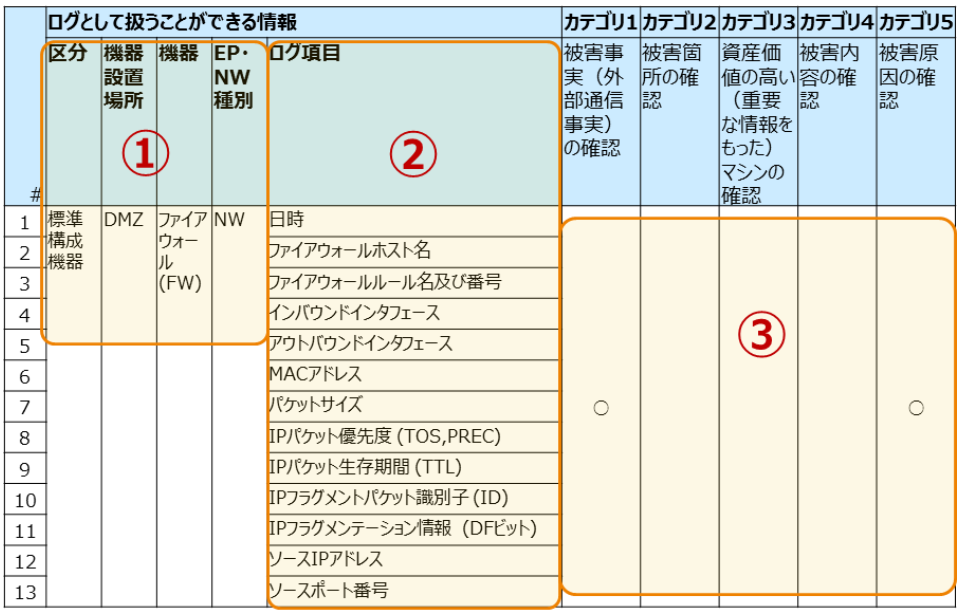

図 6.3-4 付録 4 システムログ一覧（証拠保全）の概要図

(1) 一覧表の見方

- ログとして扱うことができる情報は、4.1.4 機器構成で示した区分、機器設置場所、機器の分類に対応し、システムログを取得する具体的な機器を特定できる。
- 保全対象のログを確認すべきポイントを 5 つのカテゴリに分類し、被害内容や被害特定に応じて保全すべきログを確認できる。確認すべき 5 つのカテゴリを以下に示す。
  - カテゴリ 1：被害事実（外部通信事実）の確認
  - カテゴリ 2：被害箇所の確認
  - カテゴリ 3：資産価値の高い重要な情報をもったマシンの確認
  - カテゴリ 4：被害内容の確認
  - カテゴリ 5：被害原因の確認

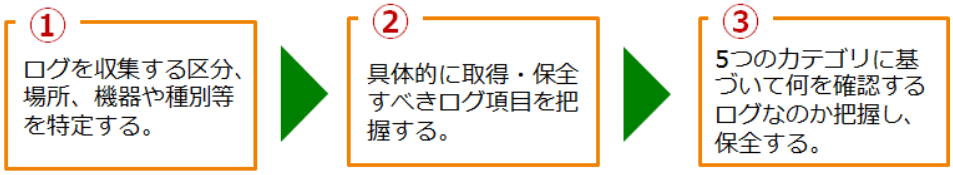

図 6.3-5 付録 4 システムログ一覧（証拠保全）の利用手順

(2) 利用手順

- 手順①：収集するシステムログの特定する
  - 4.1.4 機器構成で示した区分（標準構成機器／対策強化機器）、機器設置場所（DMZ／内部セグメント）、機器（ファイアウォール、Web サーバ等）を特定する。

- 手順②：具体的なログ項目を把握する
  - 具体的に取得・保全すべきログ項目を把握する。

- 手順③：何を確認するためのログかを確認し、証拠保全する対象を検討する
  - 確認するログの 5 つのカテゴリを証拠保全するログを検討する。

7. まとめ

標的型攻撃等サイバー攻撃に対峙するためには、人・組織側面と技術的側面の両面で対策検討が必要である。人・組織側面では、事前の計画立案だけでなく、有事の際に計画内容を実行できるよう日々の訓練も必要である。さらに、技術的側面では、最新の攻撃・対策手法、被害事例などの情報収集を継続的に実施し、常に現在の技術的対策の必要十分性の確認が必要である。