令和2年度「専修学校による地域産業中核的人材養成事業」

セキュアなシステム運用教材

Society5.0 に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

令和 2 年度「専修学校による地域産業中核的人材養成事業」

セキュアなシステム運用教材

Society5.0 に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

目次

第１章　セキュリティ構築

1-1　情報システムにおける脅威と脆弱性

情報システムにおいて、「脅威」とはシステム又は組織に損害を与える可能性のある因子のことをいい、人為的なものから環境によるものまで、さまざまな種類があります（表 1-1)。

表 1-1　脅威の例

区分		脅威の例
人為的	意図的	マルウェア、不正アクセス、改ざん、なりすまし、盗難など
	偶発的	人為的ミス、障害・誤作動など
環境的		災害など

特定の企業や個人、あるいは不特定多数に対し被害をもたらすサイバー攻撃は、悪意を持つ攻撃者による「人為的で意図的な脅威」とされます。

そうした脅威によって付け込まれる可能性のある設計上の欠陥やシステムの不備、物理的保護の不備を「脆弱性」と呼びます（表 1-2)。

表 1-2　脆弱性の例

区分	脆弱性の例	対応する脅威
ハードウェア	記憶媒体が管理されていない	故障、情報漏えい
	温度や湿度の変化が大きい	故障、誤作動
ソフトウェア	仕様書に不備がある	ソフトウェア障害、誤作動
	アクセス制御に不備がある	改ざん、なりすまし、情報漏えい
	ログ管理に不備がある	不正アクセス
	バックアップに不備がある	復旧不能
環境、施設	出入口の物理的保護に不備がある	盗難
	電源設備が不安定である	停電、誤作動
	災害が多い地域に所在している	災害

サイバー攻撃は、悪意ある攻撃者が意図的に脆弱性を悪用し、資産への損害を発生させます。そのため、脆弱性を正しく認識し、適切な対策を講じることが必要となります。

1-2　サイバー攻撃対策の考え方

サイバー攻撃の変遷

サイバー攻撃の代表的な手法にマルウェア（Malicious Software）と不正アクセスがあります（図 1-1）。

マルウェアにはコンピュータウイルスなどの種類があります。不正アクセスは、マルウェアなどを用い、インターネット経由で組織のネットワークに侵入・攻撃を行います。具体的には、他人の ID を利用して機密情報を閲覧したり、アクセス制御の不備に乗じて制限を超え改ざんを行うといった攻撃が知られており、入念な準備の上で組織的かつ持続的に行われる「標的型攻撃」も見られます。

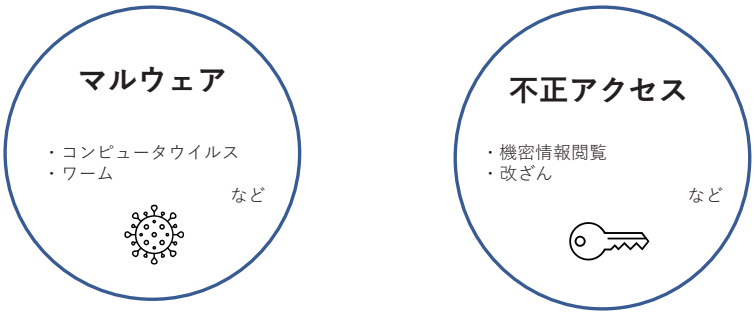


図 1-1　サイバー攻撃の代表的な手法

サイバー攻撃の歴史を振り返ると（図 1-2）、1980 年代のはじめに出現したウイルス等は愉快犯による自己顕示を目的としたものが多く被害も限定的でしたが、1980 年代半ばからはウイルス作成用キットの公開などにより、攻撃行為が徐々に増加していきました。

1990 年代になるとインターネットが普及し、攻撃対象や被害規模が拡大しました。とはいえ、性質としては Web サイトの改ざんによるいたずらやコンピュータ画面に画像を次々と表示させるといった愉快犯的なケースがいまだ主流でした。

攻撃の目的や手法が大きく変わり始めたのは、2000 年代に入ってからです。インターネットのさらなる浸透、モバイル機器の普及などもあり、個人から組織に至るあらゆるユーザーが攻撃対象となり、金銭や機密情報の入手などを目的とした組織的・計画的な攻撃が増加し

ました。その過程でウイルスやワームの高度化が進み、スパイウェアやフィッシングなどさまざまな攻撃手法が現れていきました。

2010 年代以降は一層その傾向が強まり、標的型攻撃が増加しています。また、国家間で互いの国力を弱体化させるための攻撃も大きな問題となっています。

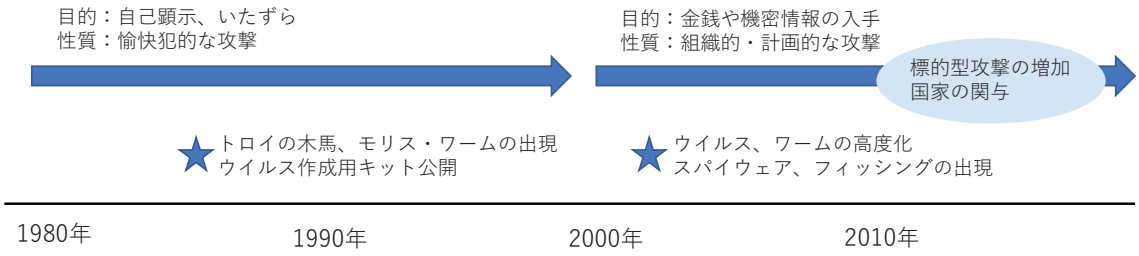


図 1-2　サイバー攻撃の変遷

サイバー攻撃対策のフレーム

増加するサイバー攻撃への対応は、国家から自治体、学校、企業などさまざまな組織の重大な課題となっています。

しかし、組織によってリスクが異なり、各々の状況に応じて技術的、法的、倫理的な対応を総合的に行う必要があるため、一律的な対策を明示することは困難です。

その中で有効な対策フレームとして考えられているのが、NIST（National Institute of Standards and Technology：アメリカ国立標準技術研究所）のサイバーセキュリティフレームワークです（表 1-3)。組織のセキュリティ対策として、リスクの特定や攻撃に対する防御の手順、危機管理体制などの標準化を図るものであり、2014 年に公開されて以降、世界標準として広がりつつあります。

フレームワークの日本語訳（重要インフラのサイバーセキュリティを改善するためのフレームワーク）は独立行政法人情報処理推進機構の Web サイトで見ることができます（https://www.ipa.go.jp/security/publications/nist/)。同サイトには NIST が発行するその他のセキュリティ関連文書も掲載されているため、参考にするとよいでしょう。

表 1-3　サイバーセキュリティフレームワークの構成

要素	詳細
フレームワーク・コア	サイバーセキュリティ対策の 5 つの機能ごとに標準的な対応等を明示。 特定：対策すべきリスクを特定 防御：適切な防御策を実施 検知：サイバー攻撃の発生を検知 対応：検知された攻撃に対応 復旧：攻撃による被害を復旧
インプリメンテーション・ティア（階層）	組織によるリスクへの取り組みの段階を整理。 ティア 1：部分的 ティア 2：リスク情報を活用 ティア 3：繰り返し適用可能 ティア 4：適応
フレームワーク・プロファイル	セキュリティ対策の優先順位設定や進捗の測定などの考え方を提示。

フレームワーク・コアに「復旧」の項目があるように、侵入の完全な予防を前提とはせず、受けた攻撃からいかに早く復旧するかという考えの下、組織の種類や規模にかかわらず共通するセキュリティ対策が示されています。

多層的な防御の必要性

サイバー攻撃対策の技術的対策は、入口対策と出口対策に分けられます（図 1-3）。

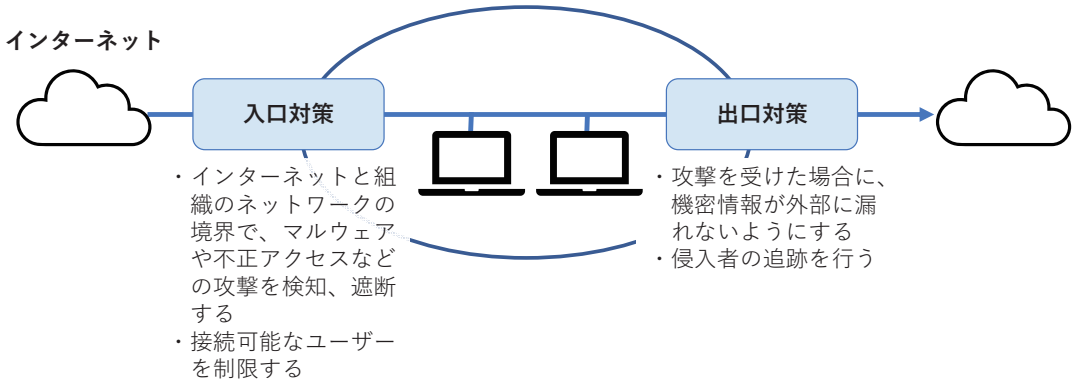


図 1-3　入口対策と出口対策

すべてのマルウェア等の攻撃を入口対策で防ぎ切るのは難しいため、入口対策をすり抜けた攻撃に対する出口対策も併せて行うこと必要です。

そうした多層的な防御を行う上で、NIST は①準備、②検知、分析、③封じ込め、根絶、復旧、④インシデント後の対応の 4 つの対策フェーズを示しています（4-2 を参照）。段階的なリスク低減を考慮することで、被害を最小限にとどめるようなセキュリティ対策を設計することが大切になります。

1-3　主なセキュリティ技術

ネットワークセキュリティの構築

サイバー攻撃対策として、組織はセキュリティ機器やシステムを利用したネットワークセキュリティを構築します。そこで用いられる代表的な防御手法には、ファイアウォールや IDS・IPS などがあります。

【ファイアウォール】

決められた基準に従って通信の可否を制御し、外部からの不正な通信を阻止します。ネットワーク上に配置して組織の構成機器を守るネットワーク型と、個々のコンピュータを守るホスト型に分けられます（図 1-4）。

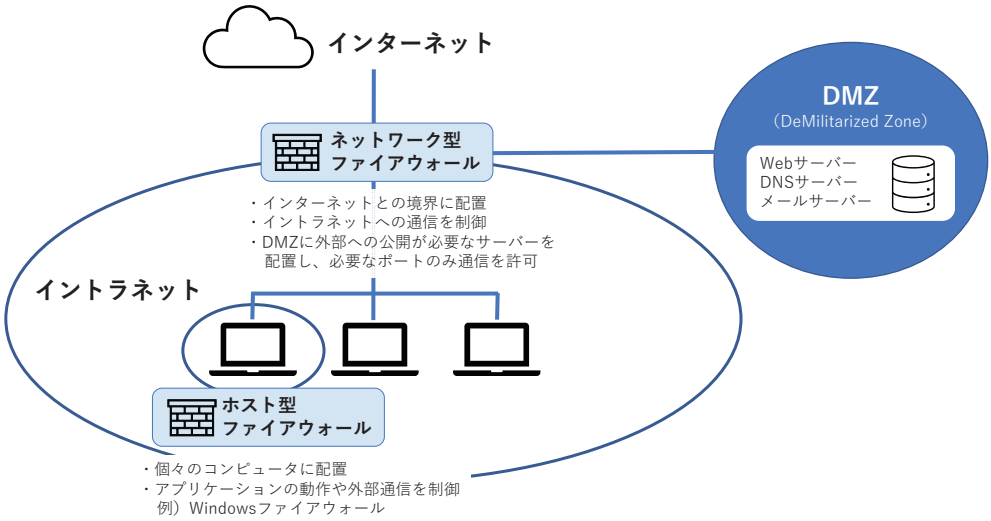


図 1-4　ファイアウォールの配置と役割

IP アドレスやポートによってアクセスを制御するパケットフィルタリング、TCP 接続又は UDP セッション単位で通信を中継しながらアクセスを制御するサーキットレベルゲートウェイ、アプリケーションのセッション単位で通信を中継しながらアクセスを制御するアプリケーションゲートウェイなどの方式があります。

なお、従来のファイアウォールは各アプリケーションがルールに沿ってネットワークを利用することが前提でしたが、Web メールやオンラインストレージ、SNS、P2P ソフトなど従来のトラフィック制御では対応できないケースが増えてきたことから、より高いレイヤーでアプリケーションを識別し、アクセス制御を行う次世代ファイアウォールが登場してきています。

【IDS・IPS】

IDS（Intrusion Detection System：不正侵入検知システム）は、外部からの不正なアクセスやその兆候が見られた場合に管理者に通知する仕組みです。

IPS（Intrusion Prevention System：不正侵入防止システム）は、外部からの不正なアクセスの検知や機密情報の漏洩などの挙動を検知した場合に、トラフィック遮断などの措置を行う仕組みです。

ファイアウォールと同様にネットワーク型とホスト型があります（図 1-5）。

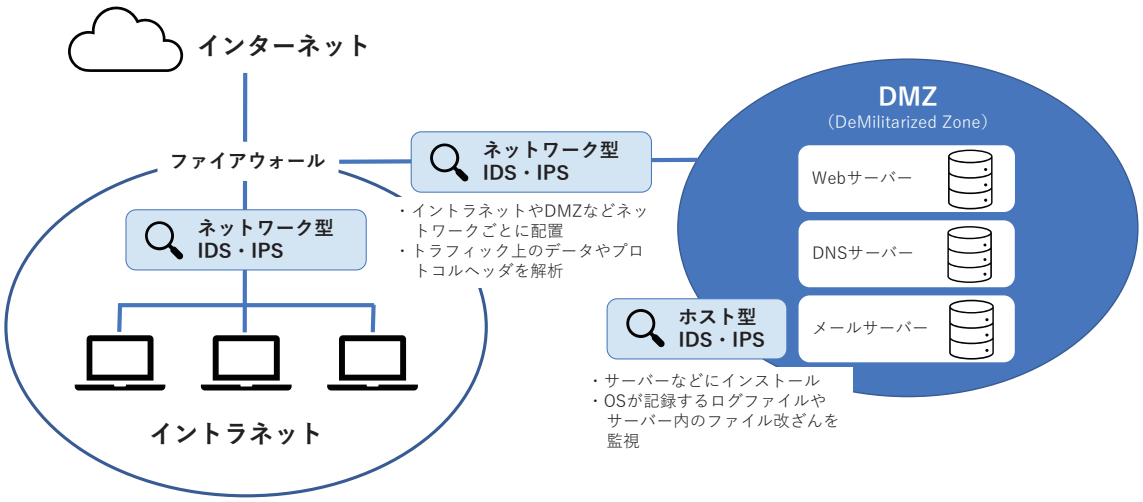


図 1-5　IDS・IPS の配置と役割

検知方法にも 2 種類あり、「シグネチャ型」は、過去に認識した攻撃パターンをデータベース化して検知します。過去のデータに基づくため、未知の攻撃には弱いという面があります。

「アノマリ型」は、通常時のネットワークトラフィック量などのしきい値を違反した場合

を検知します。未知の攻撃に対応できるケースもある一方で、しきい値の設定によっては漏れが生じる場合もあります。

【WAF（Web Application Firewall)】

WAF は、Web アプリケーションに対して送信されるリクエストを解析し、不正な文字列が含まれているかを判断したり、通信自体を監視することで、正常なリクエストのみ送信を許可する仕組みです。シグネチャによる検出のほか、Web サーバーへの HTTP リクエストの内容解析、ログによる HTTP レスポンスの確認などにより防御を行い、ファイアウォールや IDS・IPS で防げない攻撃にも対応します。

入口対策の重要な手法となっており、大きく分けてホスト型、ゲートウェイ型、クラウド型があります（図 1-6)。

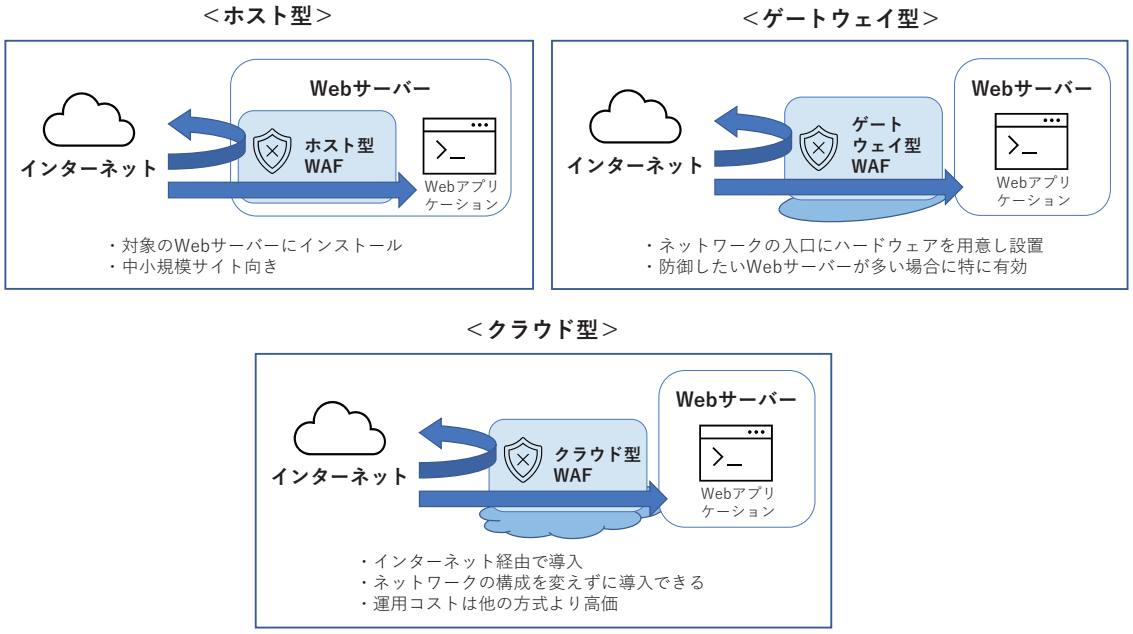


図 1-6　WAF の種類と特徴

【フィルタリング】

悪質な Web サイトへのアクセスを防ぐ仕組みをフィルタリングといいます。近年はアクセス禁止に加え、掲示板や SNS への書き込みの禁止や記録を行うことで情報漏えいを防ぐという面も比重が大きくなっています。

アクセスの制御方法はカテゴリ方式が主流で、ホワイトリスト方式やブラックリスト方式は設定や更新の作業負担が少なくありません（表 1-4)。

表 1-4　フィルタリングの方式

カテゴリ方式	制限したいカテゴリごとアクセス可否を設定
ホワイトリスト方式	アクセス可能な Web サイトを登録
ブラックリスト方式	アクセスを制限する Web サイトを登録

【エンドポイント】

パソコンやスマートフォンなどの端末をエンドポイントといい、アンチウイルスソフトなどのパッケージ化されたセキュリティ対策が用いられます。マルウェア対策や危険な URL へのアクセス制御、暗号化や認証、OS・ソフトウェアの脆弱性対策などが含まれます。

シグネチャをアップデートすることで防御範囲を広げますが、新たなマルウェア等に追いつけないケースもあります。

【DLP（Data Loss Prevention)】

DLP は、フィンガープリント（ユーザーや端末情報を識別する“指紋”の役割を持つデータ）やファイルが含む個人情報の量などから機密情報を識別し、送信やコピーを制限して外部への漏えいを防ぐ仕組みです。USB メモリの利用制限機能なども含め、複合的な対策がとられます。

【UTM・SIEM】

UTM（Unifired Threat Management：統合脅威監視）は、ファイアウォールや IDS・IPS など複数の異なる防御手法を統合するもので、防御機能の強化や一元化による精度向上、運用のしやすさといったメリットがあります。ただし、処理負担が増加するため、導入には組織の状況も鑑みる必要があります。

SIEM（Security Information and Event Management：セキュリティ情報イベント管理）は、さまざまな機器やソフトウェアのログを統合的に収集・分析してリアルタイムでのインシデント対応を可能にする仕組みです。

サイバー攻撃の種別対策

セキュリティを構築する上では、サイバー攻撃の特性を知り、攻撃の種類に応じた対策を行う必要があります。

【マルウェア】

ウイルスやワームは日々増加し、対策を回避する機能が付加されていくため、画一的な対策では不十分となります。マルウェアの種類や動作、機能への理解が不可欠です（表 1-5)。

表 1-5　マルウェアの全体像

分類	ウイルス	プログラムに寄生して、動作を妨げたり、ユーザーが意図しない動作を行う。画像を表示するだけのものから、データを削除するものまで幅広い。USB デバイス、ネットワーク共有、電子メールなどを介して拡散される。
	ワーム	ネットワークの脆弱性を悪用し、システムやネットワークの性能を劣化させたり、ファイルの削除、別のコンピュータへの侵入といった活動を行う。一度感染するとユーザーの関与を必要とせず、自らを複製し、短時間で広がる。
	トロイの木馬	ユーザーに気付かれないようにコンピュータに侵入し、ユーザー権限を利用して悪意ある操作を行う。イメージファイルや音声ファイル、ゲームなどに含まれていることが多く、実行ファイルとは別に動作する。自己増殖はしない場合が多いが、他のコンピュータに攻撃を仕掛けるなど、自由に操られる可能性がある。
	スパイウェア	破壊ではなく、侵入先のコンピュータでのアクティビティの把握やキーストロークの収集、データの取得などを行う。パスワードや権限情報を盗み取り、他のコンピュータへの侵入の足がかりとするなど、攻撃の起点として利用されることも多い。
	ボット	感染したコンピュータは外部から与えられた命令に自動的に従い、不正な行為を実行する。
感染経路	自動感染	自動的に対象内部に侵入して感染させる。
	ファイル感染	実行ファイルやデータファイルを書き換えて潜伏し、感染させる。
	実行ファイル	単独の実行ファイルとして感染させる。
	メモリ常駐	メモリに常駐して潜伏して感染させる。
	自動起動	OS 起動時やログイン時に起動して感染させる。
機能	拡散	自己の複製を潜伏している PC 以外に拡散させる。
	暗号化・改変	暗号化や改変などを行い、発見・駆除を回避する。
	DoS 攻撃	多量のパケット送信を行い過剰な負荷をかける。
	改ざん・破壊	データの改ざん、システムの破壊を行う。
	スパイ	PC 上の情報を収集・記録し、外部の攻撃者等へ送信する。
	スパム	スパムメールを中継したり、自動生成して送信する。
	アップデート	データをダウンロードして自身のバージョンアップを行う。
	命令・踏み台	リモートログインを有効化したり、攻撃命令に従って動作する。

＜対策＞

マルウェアの検出方法として一般的なのはパターンマッチングですが、未知のマルウェアへの対応が難しいため、ヒューリスティック検出など、他の検出方法と組み合わせて使用することが重要です（図 1-7）。

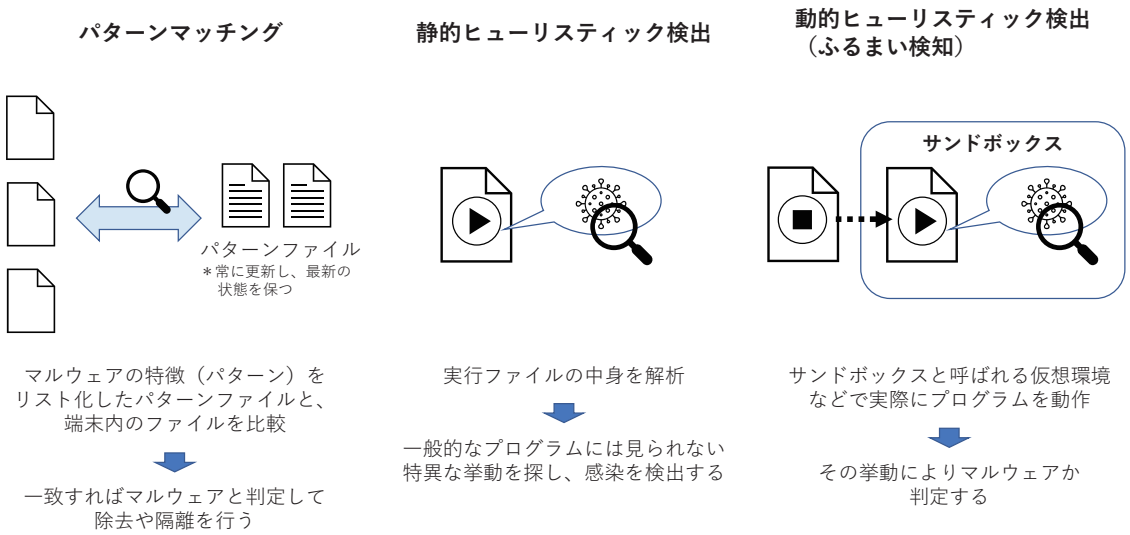


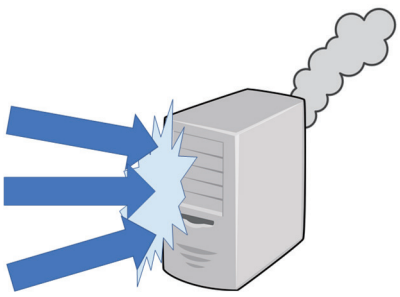
図 1-7　マルウェアの検出方法

【不正アクセス】

マルウェアや脆弱性に乗じた攻撃により、サーバーやシステムに侵入し、データの破壊や情報漏えいなどをもたらす不正アクセスには、下記のような手法が用いられます。

◎DoS/DDoS 攻撃

DoS（Denial of Service）攻撃は、Web サーバーやルーターなどのネットワーク上のデバイスやサービスに、大量のデータを送信することで、サービスを利用不能に追い込んだり、誤動作を引き起こす。複数のデバイスを一斉コントロールして攻撃する場合、DDoS（Distributed Denial of Service）攻撃という。



DoS 攻撃の 1 つである SYN flood 攻撃は、意図的にハーフオープンの TCP 接続を大量に行い、サーバーのリソースを消費させる（図 1-8）。クライアントが IP を偽装することで、②の送信を空振りさせ、③～④の状態が発生する。

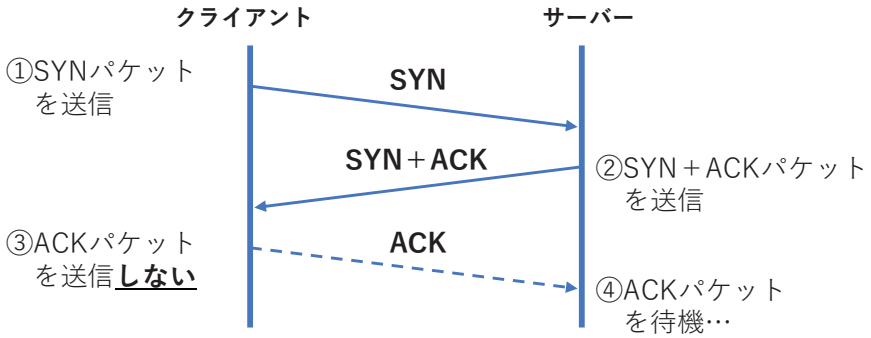


図 1-8　SYN flood 攻撃

＜対策＞

正当なホストからの接続リクエストのみに対応する SYN cookies や SYN cache といった手法が用いられます。

また、送信元を偽装した IP パケットの転送を防ぐイングレスフィルタリングの導入も進んでいます。

◎ゼロデイ攻撃

ゼロデイとは脆弱性が発見されてから修正プログラム（パッチ）が適用されるまでの期間を指し、その間に脆弱性を利用した攻撃を行う手法をゼロデイ攻撃という。Adobe Flash Player や Oracle Java といった広く使われているソフトウェアに対しても攻撃が行われている。また、機密情報の漏えいや不正送金被害など大きな被害をもたらすケースも見られる。

＜対策＞

プログラムの起動・実行を許可したもののみに制限するホワイトリスト方式の対策や、サンドボックスを活用するとともに、運用面でも常にアップデートを行い、脆弱性情報をチェックするといった注意が必要となる。

◎標的型攻撃

特定の組織などを標的にする攻撃を標的型攻撃と総称する。政府や公的機関、製造業などが多く標的となり、事前に組織内のネットワーク情報やシステム構成などを調査の上で、マルウェアを利用するなどして巧妙な攻撃を仕掛ける（表 1-6）。125 万件の年金情報が漏洩した日本年金機構の個人情報漏えい事件（2015 年）など、社会的影響の大きい事例も発生している。

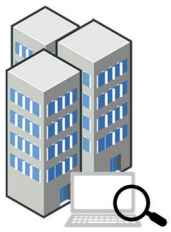


表 1-6　標的型攻撃の手順

①事前調査	標的決定、マルウェア等の準備、C&C サーバー（権限を窃取した端末に指示を出す攻撃用のサーバー）の準備などを行う
②初期侵入	組織の構成員にメールでマルウェアを送りつけ、端末を感染させる
③重要な情報の入手	より権限の高い端末に侵入し、機密情報などを入手する

＜対策＞

組織ごとに攻撃手順が用意されるため一律的な対策は難しいですが、多層防御の体制を整備し、各段階で検出・防御の網を張ることで、仮に侵入されたとしても最小限の被害に抑えることが重要な対策となります。

【Web アプリケーションへの攻撃】

インターネットショッピングやインターネットバンキングなどの Web アプリケーションでは、脆弱性を突いた攻撃が行われており、サービス停止や情報漏えいなどの被害が生じています。

◎インジェクション攻撃

Web サイトの入力フォームや URL のパラメーターなどに不正な文字列を入力して情報窃取や改ざん、破壊などを命令する（表 1-7）。

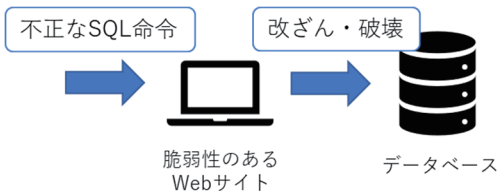


表 1-7　インジェクション攻撃の種類

SQL インジェクション	データベースに不正な SQL 命令を行う。
OS コマンドインジェクション	Windows や Linux のシェルを不正に動作させる。
LDAP インジェクション	LDAP（Lightweight Directory Access Protocol）の権限情報を不正操作して認証を行ったり、他のユーザー情報を窃取する。

＜対策＞

危険な文字が含まれる場合にエスケープ処理を行うことや、エラーメッセージを非表示にしてサーバーに関する情報を与えないようにすること、データベースの権限や格納する情報の見直しなどが対策となります。また、SQL の場合はバインド機構を利用するなど、言語に応じた対策もとられます。

◎クロスサイトスクリプティング（XSS）

スクリプトを埋め込んだ Web サイトを用意し、アクセスしたユーザーを攻撃する。攻撃には、検索結果の表示画面や会員登録、アンケートなどの入力確認画面、エラー表示などの脆弱性が利用される（表 1-8）。

表 1-8　XSS の種類

Reflected XSS	標的を特定の URL に誘導し、クリックをすると HTTP リクエスト中に含まれるスクリプトが動作する。
Stored/Persistent XSS	掲示板などの投稿中に含まれるスクリプトが動作する。
DOM Based XSS	Web ページに含まれる正規のスクリプトにより、動的に Web ページを操作した際に意図しないスクリプトが動作する。

＜対策＞

インジェクション攻撃と同様にエスケープ処理が有効です。また、Web ページに出力するリンク先の画像 URL が動的に生成される場合に、href タグに「http://」か「https://」から始まる文字列のみを出力するようにしてスクリプトが仕込まれることを防ぐ方法もとられます。加えて、動的に生成される要素の見直しや、CSS（Cascading Style Sheets）の取り込みの見直しなど、スクリプトを仕込むことができる要素を排除することも重要です。

◎バッファオーバーフロー

確保されたメモリ量を超えたデータを入力し、バッファがあふれることを利用して攻撃する。データの破壊、プログラムの停止を引き起こしたり、他のプログラムを動作させたりする。

＜対策＞

領域長とデータ長を意識してプログラミングを行うことが重要となります（図 1-9）。

バッファオーバーフローが起こり得る場合

```
1 #define MAXSIZE 256
2 int foo(char *source) {
3     char dest[MAXSIZE];
4     strcpy(dest, source);
5     ……
6 }
```

対策の例

```
1 #define MAXSIZE 256
2 int foo(char *source) {
3     char dest[MAXSIZE];
4     if (source == NULL) …不当な引数を考慮
5       return ERROR;
6     memset (dest, 0, MAXSIZE); …領域のゼロクリア
7     if (MAXSIZE – 1 < strlen(source))…領域長とデータ長の比較（あふれの検査）
8       return ERROR;
9     strncpy (dest, MAXSIZE - 1, source); …転送バイト数に上限のある関数の使用
10    ……
11 }
```

図 1-9　バッファオーバーフロー対策のプログラミング例

また、ソースコードの検査ツールによる脆弱性のチェックや領域あふれを検出するデバッグなど開発時の対策も求められます。

なお、セキュアでない関数は上限バイト数を指定できる代替関数の使用が望まれます。例えば、「get → fgets」「sprintf → snprintf」「strcat → strncat」などがあります。

◎パスワード認証への攻撃

ID やパスワード情報の悪用は、個人情報や機密情報の漏えい、インターネットバンキングや EC サイトの不正利用、SNS アカウントの乗っ取りなど、さまざまな被害をもたらす。攻撃には、パスワードを総当りで試す手法やパスワードリストを使用する手法などがある（表 1-9）。

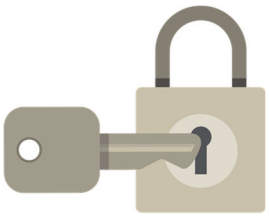


表 1-9　パスワード認証への攻撃の種類

ブルートフォース攻撃	特定の ID に対し、パスワードを総当たりで試す攻撃。コンピュータの性能が向上し、ツールも入手しやすいため、特別な知識がなくても実行できる。
パスワードリスト攻撃	何らかの手段で得た ID とパスワードの一覧（パスワードリスト）を使う攻撃。複数のサイトで同じパスワードを使い回しているユーザーが多いことを悪用する。
辞書攻撃	パスワードとして使いがちな単語をあらかじめ辞書登録しておき、試行する攻撃。サイトやサービスだけでなく、IoT 機器など初期パスワードが共通のものが一斉攻撃を受けるリスクがある。
リバースブルートフォース攻撃	1 つのパスワードに対し、複数の ID で認証を試行する攻撃。パスワード試行回数による制限などの対策が難しい面がある。

＜対策＞

まずは文字種・文字列をできるだけ複雑にすることが大切です。ただし、複雑なパスワードは利便性が悪く、また、メモ帳などに保管することでかえってリスクが上がる可能性があります。

ブルートフォース攻撃や辞書攻撃では、認証を複数回失敗したら一時的にアカウントを停止する処置が有効です。追加パスワードやパターン認識、ワンタイムパスワード、メールや SMS への一時パスワードの通知などの多要素認証も活用が進んでいます。

1-4　セキュアプロトコル

セキュアプロトコルの必要性

暗号技術は基本的には、あらかじめ決められた手順＝プロトコルに従って用いられます。暗号技術はそれ自体が安全なものであっても、正しく組み合わせないと必要な安全性が確保できない場合があります。例えば、パスワードを暗号化しても、なりすまし被害が起きる事例があります（図 1-10）。このケースの場合、暗号化自体は正しくなされているものの、利用法の面で脆弱性が生じています。

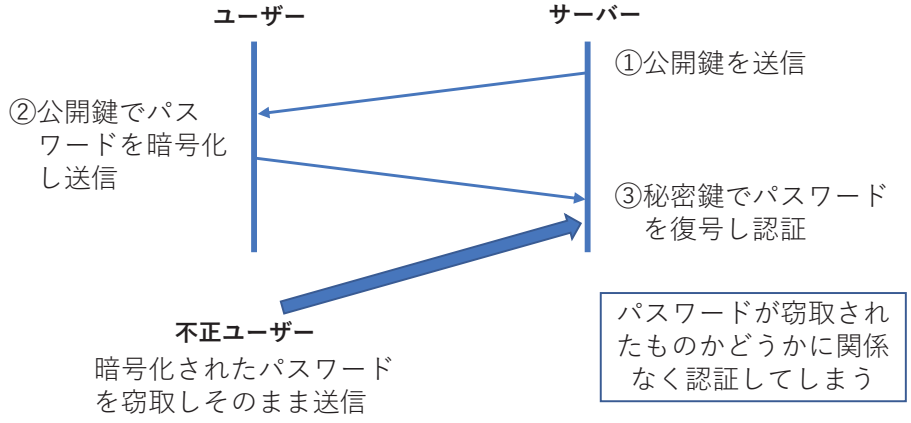


図 1-10　不十分な暗号化

セキュアプロトコル（セキュリティプロトコル）とは、さまざまな暗号関連技術を組み合わせたり、技術そのものを改良することによって、実現しようとするサービスに必要な安全性を確保するための方法・枠組みを提供するものといえます。プロトコルには多くの種類がありますが、基本的には「暗号化」「認証」「アクセス制御」「鍵管理」の機能は共通します。

図 1-10 の例を適切なセキュアプロトコルに基づいて利用すると、図 1-11 のようになります。

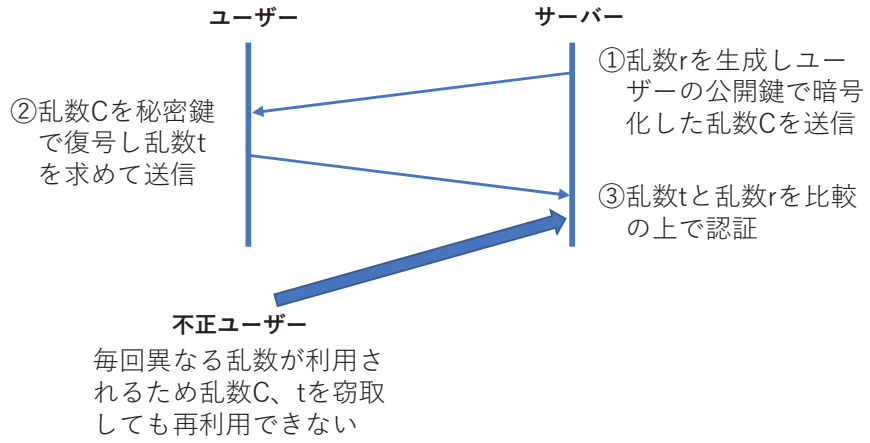


図 1-11　適切なセキリュアプロトコルによる暗号化

暗号プロトコル

1976 年に提案されたディフィー・ヘルマン鍵共有は、共通鍵暗号方式における鍵の受け渡しを安全に行うことを目的としています。傍受される可能性のある通信路を使って、暗号鍵の共有を可能にするプロトコルです。

具体的には、送受信者がそれぞれ公開データと秘密データを用意した上で公開データのみを送信し、各自が自分の秘密データと受信した公開データから共通鍵を作成します（図 1-12）。従って、公開データが盗み見られても、鍵は生成されません。

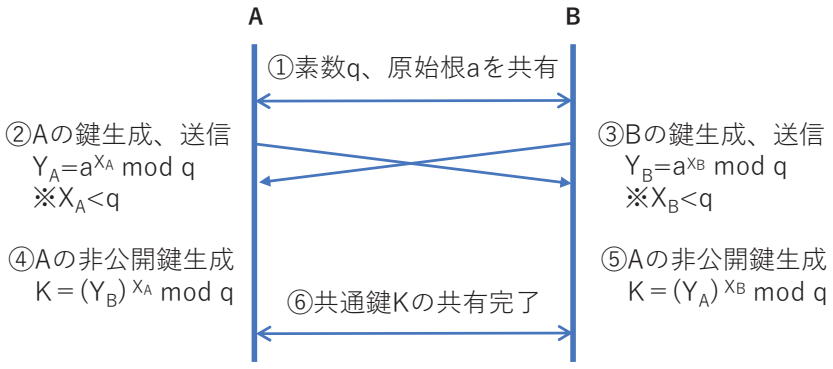


図 1-12　ディフィー・ヘルマン鍵共有

トランスポートプロトコル

SSL（Secure Sockets Layer）と TLS（Transport Layer Security）は、インターネット上で

データを暗号化して送受信し、安全な通信を行うためのプロトコルです。ハンドシェイクプロトコルで鍵を生成し、レコードプロトコルで暗号化通信を行います（図 1-13）。

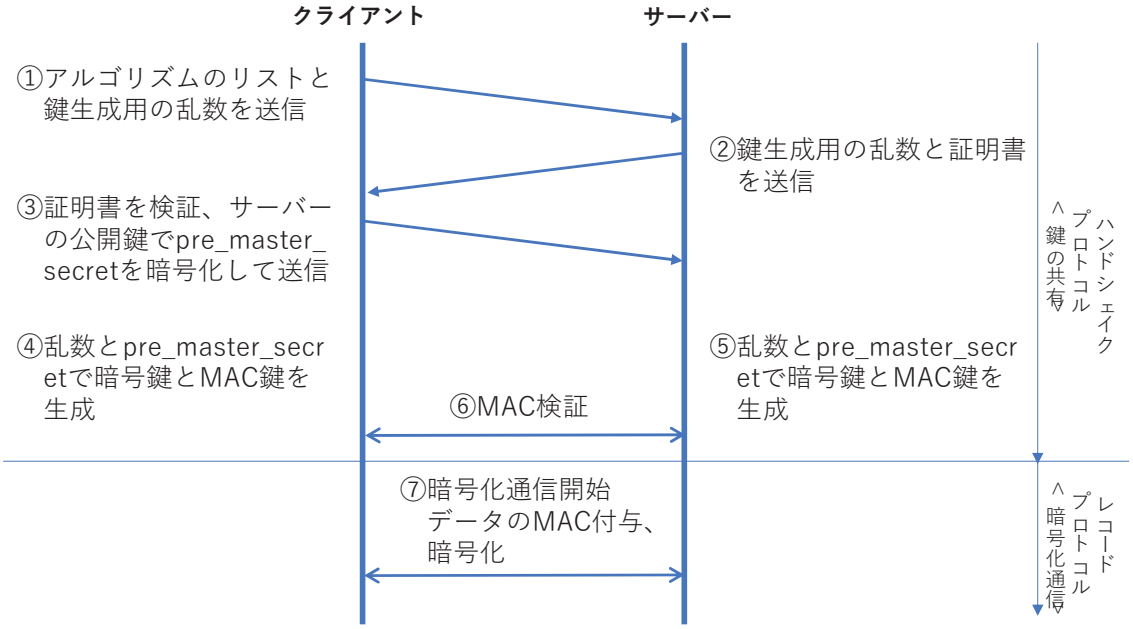


図 1-13　SSL/TLS

ネットワークプロトコル

IPsec はネットワーク層において、暗号技術と認証技術を利用し、IP パケットの安全な通信を実現するためのプロトコルです。通信送信元の認証、通信の暗号化、メッセージの認証、トンネリングによる安全な通信経路を確保し、データを保護します。

使用するプロトコル、モード、暗号化アルゴリズム、鍵などのセキュリティパラメーターを指定するため、SA（Security Association）を生成して、IPsec 通信を行います。SA の管理は手動と自動があり、自動の場合は IKE（Internet Key Exchange）により鍵を共有します。

IPsec には、AH と ESP の 2 つのプロトコルがあります（図 1-14）。

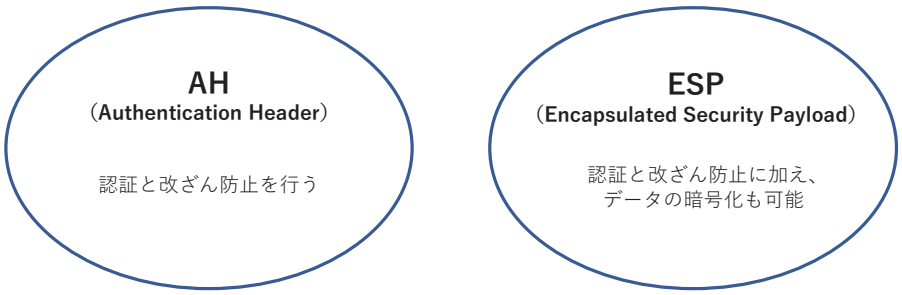


図 1-14　IPsec の 2 つのプロトコル

さらに、トランスポートモードとトンネルモードが存在します（図 1-15）。

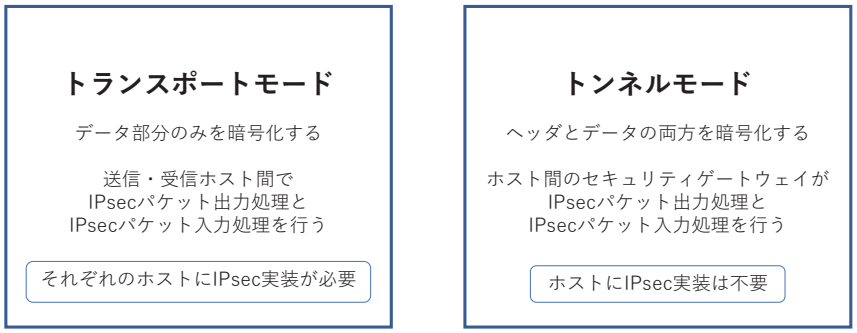


図 1-15　IPsec の 2 つのモード

AH、ESP 及びトランスポートモード、トンネルモードの組み合わせは表 1-10 のように整理できます。

表 1-10　IPsec の概要

	AH	ESP
トランスポートモード	AH ヘッダを IP パケットのヘッダとデータの間に挿入し、AH ヘッダを含む IP パケットに対する改ざん検知コードを作成。	ESP ヘッダを IP パケットのヘッダとデータの間に挿入し、ESP トレイラは後ろに付加。 ESP トレイラと元の IP パケットのデータは暗号化され、IP ヘッダを除くデータに対する改ざん検知コードを作成し、ESP トレイラの後ろに付加。
トンネルモード	IP パケット全体をデータとして、AH ヘッダと新規 IP ヘッダを付加し、AH ヘッダ、新規 IP ヘッダ、元の IP パケット全体に対する改ざん検知コードを作成。	IP パケット全体をデータとして、データの前に ESP ヘッダと新規 IP ヘッダ、後ろに ESP トレイラを付加。 元の IP パケットと ESP トレイラは暗号化され、新規 IP ヘッダを除くデータに対する改ざん検知コードを作成。

アプリケーションプロトコル

さまざまなアプリケーションに応じたプロトコルが開発されています。研究が進んでいるものとして、電子投票があります。

2002 年より法的に可能となった電子投票のプロトコルには、いくつかの手法があります。その 1 つとして、署名者に文書の中身を知らせずに電子署名してもらう技術であるブラインド署名が挙げられます。これは、いわば封筒の上から中の紙に署名するという技術です。

図 1-16 に示すように、選挙管理人は有権者情報のみを確認し、開票管理者は投票内容のみを確認します（乱数から有権者は特定不可）。これにより匿名性を確保しつつ、正しい有権者情報に基づいた投票を実現するという仕組みです。

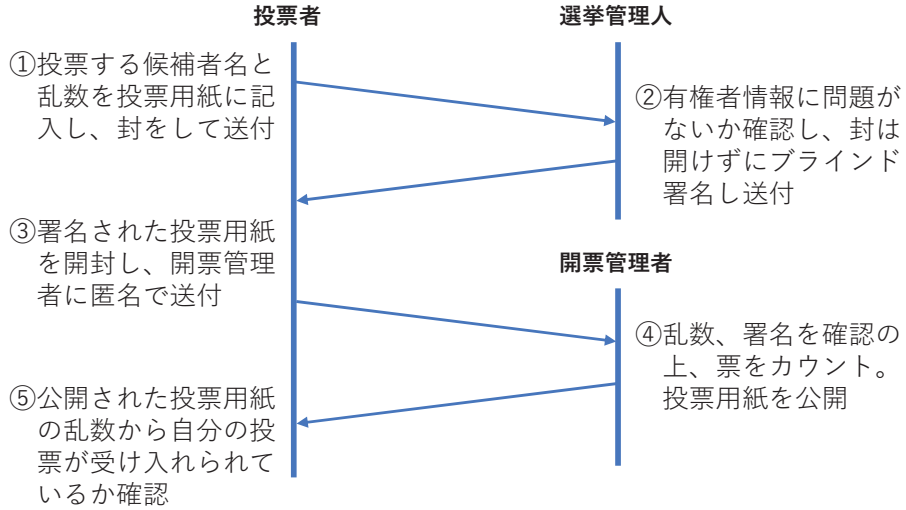


図 1-16　電子投票へのブラインド署名の活用

1-5　ハードウェアへの実装

耐タンパー性

「タンパー」とは「許可なく改ざんする」こと、すなわち暗号に対する攻撃を意味し、その攻撃に耐えられる強さを「耐タンパー性」といいます。耐タンパー性は、機器や装置などを物理的に暗号解析困難な構造にする、暗号解析を検知したら暗号機能を停止する、漏洩しそうな情報を消去するといった仕組みにより実現されます（図 1-17）。

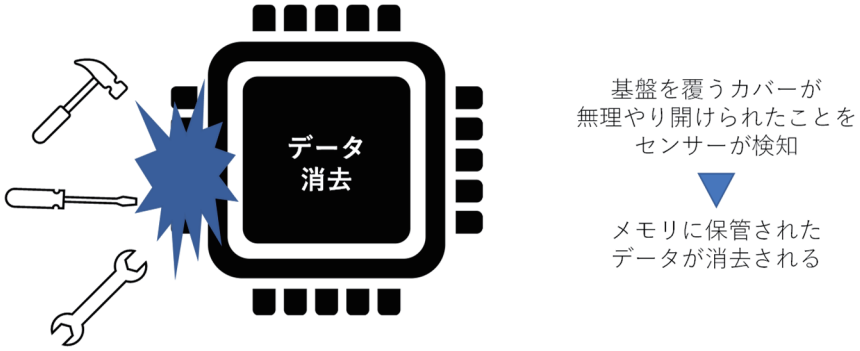


図 1-17　耐タンパー性の実現例

基本的に半導体はそれ自体として耐タンパー性は高いとされていますが、SEM（Scanning Electron Microscope：走査型電子顕微鏡）や FIB（Focused Ion Beam：集束イオンビーム）などの機器により半導体内部を解析することは可能です。ただし、装置は数千万円～数億円と利用者が限られていることから、守るデータの価値などを鑑みた上で対策を行うことが大切になります。

サイドチャネル攻撃への対応

暗号解読手法の 1 つであるサイドチャネル攻撃は、暗号装置の電磁波や熱、電力量や処理時間の違いなど、物理的な条件から暗号解読を試みるというものです（図 1-18）。

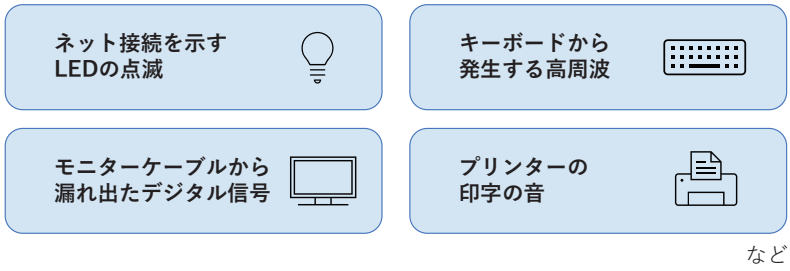


図 1-18　サイドチャネル攻撃の手がかり

ログの残らないさまざまな副次的情報が解読の手がかりに利用されるため、攻撃の痕跡を追うことが難しく、また、前述した高価な機器も不要なため低コストで実現可能という特徴があります。

耐タンパー性を考える上では、こうした攻撃も想定する必要があり、「処理時間が一定になるようにする」「消費電力に特徴のあるものは常に動作させる」といった対策がとられています。

暗号の処理速度向上

共通鍵暗号やハッシュ関数は、ソフトウェアで CPU を用いて実装するより、ハードウェアの専用回路で実装したほうが、処理速度を上げることができます。ハードウェアは共通鍵暗号におけるビット単位のデータの並び替えがソフトウェアより容易に行うことができ、また、処理の並列度を上げて多重化できるためです。

例えば、暗号アルゴリズムのうち新しいもの（AES など）は、32bitCPU で効率的に動作するように標準的な命令だけで実装できるようになっています。しかし、古いもの（DES など。現在は非推奨）では、ビットの並べ替えをソフトウェアで効率的に実装することは難しく、ハードウェアであれば配線を変えるだけで実現することができます。

ユーザーインターフェイス

ハードウェア実装では、セキュリティを保った状態で機能の追加・変更が難しいため、ユーザーインターフェイスが重要となります。例えば、携帯電話は通話が目的であり、ユーザーは通話中の暗号化処理に関与するわけではありません。暗号化処理は、ユーザーが関知しない LSI などで実施されています。つまり、ユーザーにとって大事なのは、「暗号処理を行うこと」なのではなく、「データを秘匿して通信すること」であり、ハードウェアで暗号処理を行うことでユーザーが負荷なく使えることを念頭に置く必要があります。

実装レベルでの脆弱性

暗号はアルゴリズムだけでなく、実装レベルの評価も大切です。実装レベルで脆弱性がある場合、暗号機能を実装したソフトウェアやハードウェアに対する攻撃で鍵が露呈し、被害を受ける可能性があります。

暗号の実装に関する規格として、暗号モジュールに対するセキュリティ要求事項を規定した ISO/IEC 19790 を参照することができます（表 1-11）。

セキュリティレベル 1 は、セキュリティが最も低いレベルで、市販品に求められる基本のセキュリティ要求事項が規定されています。

セキュリティレベル 2 は、レベル 1 の物理的セキュリティを強化したものです。物理的アクセスがあった場合に破壊されるコーティング又はシールなどタンパー証跡に関する要求事項が追加されています。また、管理者やユーザーといった役割ベースの認証機能が必須とされます。

セキュリティレベル 3 は、侵入者の暗号モジュール内の CSP に対するアクセス防止を図るもので、暗号モジュールの開封を検出してデータ消去などの応答をする、タンパー検出・応答に関する要求事項が規定されています。ID ベースの認証機能が必須とされ、また、重

要情報の入出力に関する要求事項が追加されています。

セキュリティレベル 4 は、いかなる物理的な攻撃に対してもタンパー検出・応答をするための、暗号モジュール部分を完全に被覆保護する物理的メカニズムを加えたレベルです。さらに、正常な電圧・温度の範囲を超えた環境条件・変動に関する要求事項も追加されています。

表 1-11　暗号モジュールのセキュリティ要求事項（要約）

<table>
<tr><th></th><th>セキュリティレベル 1</th><th>セキュリティレベル 2</th><th>セキュリティレベル 3</th><th>セキュリティレベル 4</th></tr>
<tr><td>暗号モジュールの仕様</td><td colspan="4">暗号モジュール、暗号境界、承認されたセキュリティ機能、通常動作モード、縮退動作モードの仕様。すべてのハードウェア、ソフトウェア及びファームウェアの構成要素を含む暗号モジュールの記述。すべてのサービスは、承認された暗号アルゴリズム、セキュリティ機能又はプロセスを承認された方法で使用していることを表す状態を表示</td></tr>
<tr><td>暗号モジュールインターフェイス</td><td colspan="2">必須及び追加のインターフェイス。すべてのインターフェイス、すべての入出力データパスの仕様</td><td>高信頼チャネル</td><td>–</td></tr>
<tr><td>役割、サービス・認証</td><td>必須及び追加の役割並びにサービスの論理的な分離</td><td>役割ベース又は ID ベースのオペレータ認証</td><td>ID ベースのオペレータ認証</td><td>多要素認証</td></tr>
<tr><td>ソフトウェア/ファームウェアセキュリティ</td><td>承認された完全性技術、定義された SFMI、HFMI 及び HSMI</td><td>承認されたデジタル署名又はメッセージ認証子に基づく完全性テスト</td><td colspan="2">承認されたデジタル署名に基づく完全性テスト</td></tr>
<tr><td>動作環境</td><td>変更不可、限定又は変更可能な動作環境。SSP の制御</td><td>変更可能な動作環境</td><td colspan="2">–</td></tr>
<tr><td>物理セキュリティ</td><td>製品グレードの構成要素</td><td>タンパー証跡
不透明なカバー又は囲い</td><td>カバー及びドアに対するタンパー検出・応答。強固な囲い又はコーティング。EFP 又は EFT</td><td>タンパー検出・応答が可能な包被。EFP。故障誘導対策</td></tr>
</table>

<table>
<tr><td colspan="2">非侵襲セキュリティ</td><td colspan="3">付属書 F に規定された非侵襲攻撃に対処するよう設計</td></tr>
<tr><td colspan="2"></td><td colspan="2">付属書 F に規定された対処技術の有効性の文書化</td><td>対処技術テスト</td></tr>
<tr><td colspan="2" rowspan="3">Sensitive Security Parameter 管理</td><td colspan="3">乱数ビット生成器、SSP の生成、確立、入出力、格納及びゼロ化</td></tr>
<tr><td colspan="3">自動化された SSP の転送方法又は承認された方法を用いた SSP の確立</td></tr>
<tr><td colspan="2">手動で確立される SSP は、平文で入出力されてもよい</td><td>手動で確立される SSP は、暗号化された形式又は知識分散法を使って入出力</td></tr>
<tr><td colspan="2" rowspan="2">自己テスト</td><td colspan="3">動作前自己テスト：ソフトウェア/ファームウェア完全性テスト、バイパステスト、重要機能テスト</td></tr>
<tr><td colspan="3">条件自己テスト：暗号アルゴリズムテスト、鍵ペア整合性テスト、ソフトウェア/ファームウェアのロードテスト、手動鍵入力テスト、条件バイパステスト及び重要機能テスト</td></tr>
<tr><td rowspan="4">ライフサイクル保証</td><td>構成管理</td><td colspan="2">暗号モジュール、構成要素及び文書に対する構成管理システム。ライフサイクルを通じて各々の構成要素が一意に識別・追跡可能</td><td>自動化された構成管理システム</td></tr>
<tr><td>設計</td><td colspan="3">すべてのセキュリティ関連サービスのテストを可能にするような設計</td></tr>
<tr><td>FSM</td><td colspan="3">有限状態モデル</td></tr>
<tr><td>開発</td><td>注釈付きソースコード、回路図又は HDL</td><td>高級言語の使用</td><td>事前条件、事後条件の文書化</td></tr>
<tr><td colspan="2">ベンダ試験</td><td colspan="2">機能試験</td><td>詳細試験</td></tr>
<tr><td colspan="2">配付及び運用</td><td>初期化手順</td><td>配付手順</td><td>ベンダ提供認証情報に基づくオペレータ認証</td></tr>
<tr><td colspan="2">ガイダンス</td><td colspan="3">管理者及び非管理者ガイダンス</td></tr>
<tr><td colspan="2">その他の攻撃への対処</td><td colspan="2">試験要件が整備されていない攻撃への対処技術の仕様</td><td>試験要件と攻撃への対処の仕様</td></tr>
</table>

第 2 章　セキュアなシステム設計

2-1　セキュリティアーキテクチャ

セキュリティアーキテクチャとは

セキュリティアーキテクチャは、IT 製品において、脅威に対するセキュリティ機能を実装するための設計方針・プログラムの構造・仕組みのことを指します。

セキュリティ機能とは、ユーザーの重要なデータを不正アクセス等から守るための機能や組織のセキュリティ方針を実現するための機能であり、第 1 章で紹介したさまざまなセキュリティ技術などが用いられます。

セキュリティアーキテクチャという概念が重要であるのは、そうしたセキュリティ機能をかいくぐる攻撃が存在するためであり、認証やアクセス制御といった個々のセキュリティ機能だけでなく、それらを統括し、セキュリティ機能自体を攻撃から守る視点が必要だからです。

具体的に想定すべき攻撃として、「バイパス（回避）」と「改ざん」があります。

■バイパス（回避）

セキュリティ機能が適用されないように回避して不正アクセスを行う攻撃のことをいいます（図 2-1）。

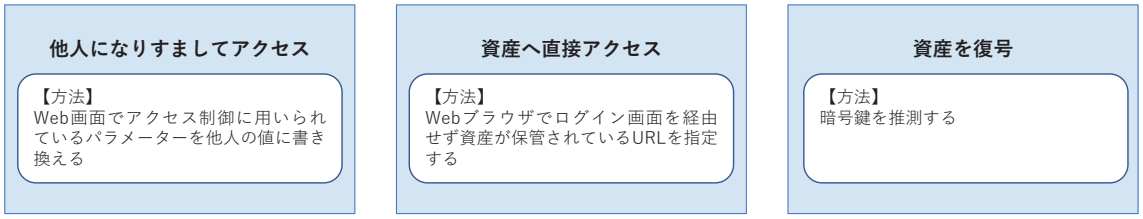


図 2-1　バイパスの攻撃例

■改ざん

セキュリティ機能を改変したり破壊したりする攻撃のことをいいます（図 2-2）。

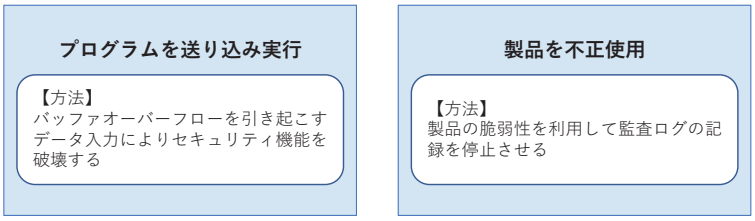


図 2-2　改ざんの攻撃例

こうした攻撃に対し、セキュリティアーキテクチャが実現すべきものとして、セキュリティドメイン、自己保護、非バイパス性、セキュアな初期化という 4 項目があります。

セキュリティドメイン

セキュリティドメインは、情報資産やセキュリティ機能に悪影響を及ぼす可能性のあるプログラムの動作を、ある限られた範囲内に封じ込めるという概念です。

外部からダウンロードして製品内部に取り込まれたプログラムや、ユーザーが新規に作成したプログラム、あるいは製品に組み込まれておりユーザーの操作で動作するプログラムは、正当なプログラムであっても悪影響を及ぼす可能性があります。プログラムの実装ミスや攻撃者の不正操作、ユーザーの操作ミス、コンピュータウイルスなどの不正なプログラムによる攻撃への悪用などがありうるためです。

そのような情報資産やセキュリティ機能に対してアクセス可能なプログラムの動作を囲い、封じ込めた範囲をセキュリティドメインといい、セキュリティドメインの範囲を制限し外部にアクセスできないようにすることをドメイン分離といいます（図 2-3）。

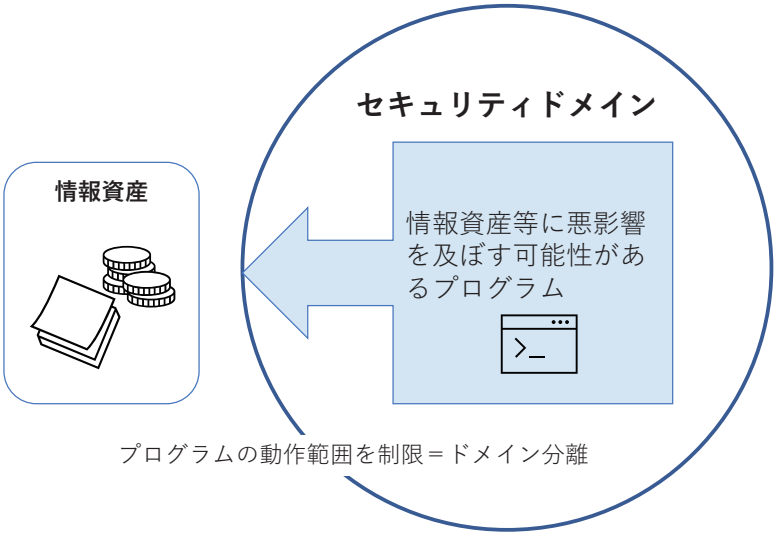


図 2-3　セキュリティドメインとドメイン分離

ドメイン分離の実現方法としては、例えばユーザーが使用するアドレス空間とシステムが使用するアドレス空間を明確に分離するハードウェア機構やアドレス管理方式などがあります。また、製品が、ハードウェアやオペレーティングシステムを含まないアプリケーションプログラムである場合には、製品の範囲に含まれていないオペレーティングシステムの提供する仕組みを利用して、ドメイン分離を実現している場合もあります。

ドメイン分離の仕組みが実装されていれば、プログラムによる攻撃の経路が正当なインターフェイスに限定されるため、そのインターフェイスにおいてセキュリティ機能のバイパス・改ざんを防止する対策を実施すれば、攻撃に一括対処することができます。

自己保護

自己保護とは、セキュリティ機能以外のプログラムや製品のユーザーによってセキュリティ機能が改ざんされないよう、製品のセキュリティ機能が自分自身を保護する仕組みです（図 2-4）。

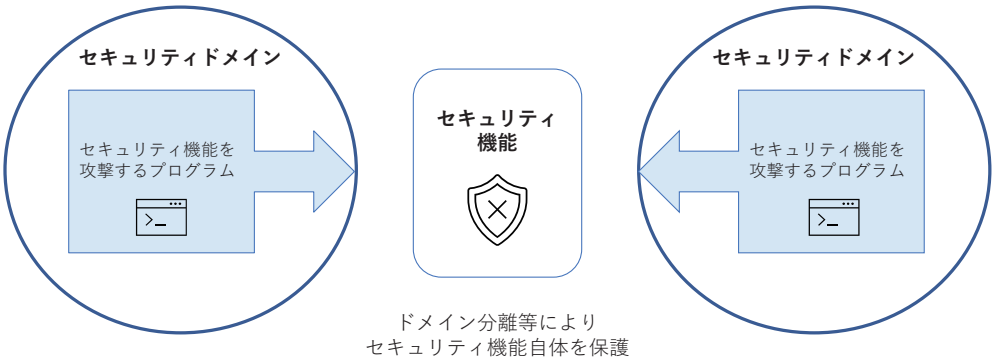


図 2-4　セキュリティ機能の自己保護

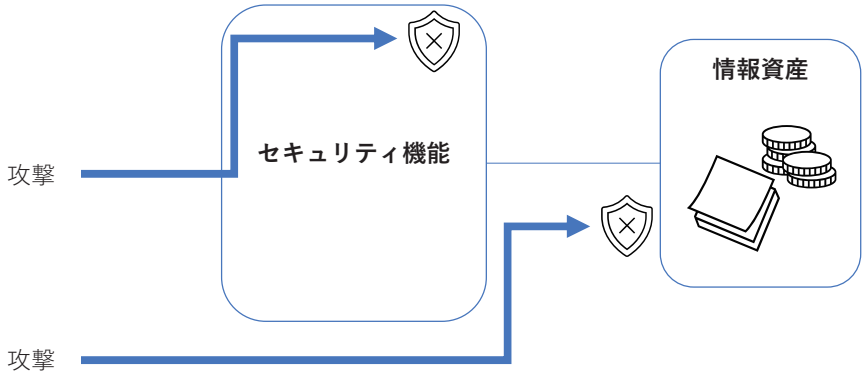
自己保護は、ドメイン分離及びドメイン分離では対処できないインターフェイス等の保護対策で実現されます。インターフェイスの保護対策とは、バッファオーバーフローや SQL インジェクションなどのインターフェイスに不正な入力を行う攻撃に対する対策が該当します。

開発者は、セキュリティ機能への攻撃の可能性があるすべての経路と改ざん方法を認識し、ドメイン分離その他の仕組みを利用して、改ざんを防止する対策を漏れなく設計・実装する必要があります。

非バイパス性

非バイパス性とは、製品を利用する際に適切なタイミングで必ずセキュリティ機能が適

用され、そのセキュリティ機能がバイパスされないという、セキュリティ機能が備えるべき特性のことです（図 2-5）。



バイパス経路が生じないように設計

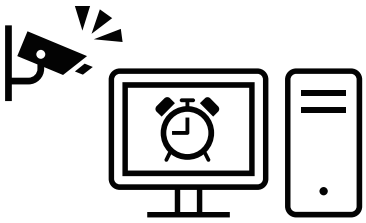
図 2-5　非バイパス性

非バイパス性は、開発者がセキュリティ機能を設計・実装する際に、バイパス経路が生じないように設計・実装することで実現されます。具体的には、セキュリティ機能の保護すべき資産にアクセス可能なすべての経路についてセキュリティ機能の適用漏れがないように設計・実装することが必要で、アクセス経路が多い場合はドメイン分離で経路を限定することが有効です。

また、セキュリティ機能が適用されるインターフェイスにおいて、想定外の利用順序の変更や想定外のパラメーター入力などによりセキュリティ機能が適用されなくなることがないよう、セキュリティ機能内部にも注意が必要です。例えば Web アプリケーションでは、正当な画面遷移とは異なる画面にアクセスされたり、セッション管理に使用されるパラメーターを他人の値に変更された場合でも、識別認証やアクセス制御などのセキュリティ機能が間違いなく適用されるようにしなければなりません。

セキュアな初期化

セキュアな初期化とは、起動途中の製品のセキュリティを確保する仕組みのことです。すなわち、製品が起動途中のときはセキュリティ機能が正常に動作しておらず、攻撃に対抗できない場合があるため、製品を起動してから運用状態に至るまでの間であっても、製品が攻撃に対抗し、セキュリティ機能の初期化処理が正しく行われる仕組みを設計・実装しなければなりません。



起動途中のセキュリティを確保

セキュアな初期化は、セキュリティ機能が有効になる前に情報資産にアクセス可能な経路や機能が存在しないように設計・実装することで実現されます。

2-2　CC の概要と構成

CC とは

セキュリティ機能の設計・実装を評価する標準として、CC（Common Criteria）があります。これは欧米諸国で各国が独自に策定していた基準を統合したもので、「セキュリティ対策の十分性」と「セキュリティ対策の正確性」を評価しています（図 2-6）。

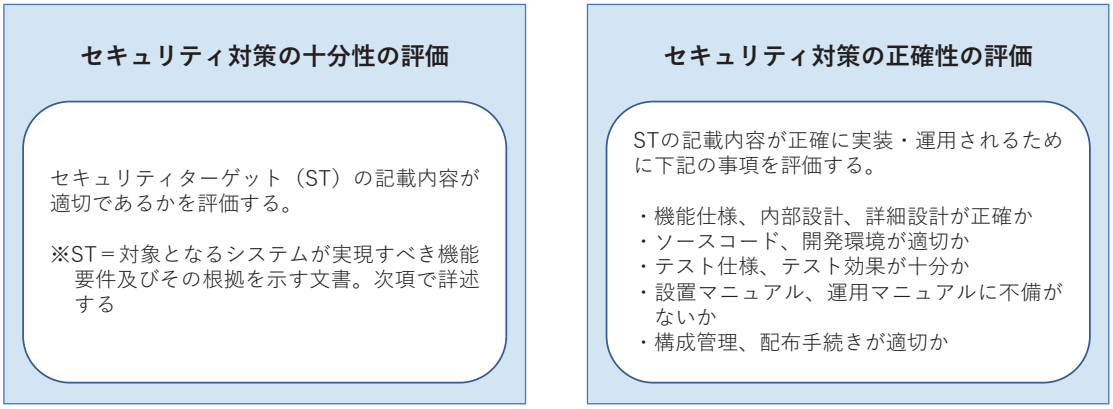


図 2-6　CC による評価の概要

CC が対象とするのは、情報技術を用いた製品やシステムのセキュリティ機能です。ソフトウェアだけでなく、ハードウェア、ファームウェア、あるいはシステム全体が評価対象になります。また、製品形態としては、ファイアウォールなど直接セキュリティに関係する製品だけでなく、オペレーティングシステムやデータベース、あるいはグループウェアなど、保護すべき資源を保有する製品はすべて評価対象となります。

なお、CC は ISO 標準としては ISO/IEC 15408 として定められており、内容は同じですが規格としての発行のタイミングとバージョンは異なっています。

CC の日本語訳は、独立行政法人情報処理推進機構の Web サイトで見ることができます（https://www.ipa.go.jp/security/jisec/cc/index.html）。

CC の構成

CC は 3 つのパートで構成されています（図 2-7）。

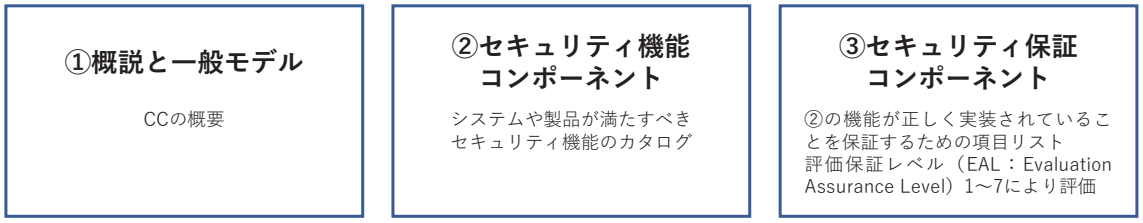


図 2-7　CC の構成

セキュリティターゲットの作成プロセス

セキュリティ対策の十分性を確保するには、開発プロセスにおける要求分析の段階でセキュリティ対策を正確に設計することが大切です。

セキュリティターゲット（ST）はこのときに作成する文書で、下記①〜④により、通常は製品の開発者が作成します。

①ST 概説

セキュリティ対策の評価対象（TOE：Target of Evaluation）を明確に規定します。TOE 概要と TOE 記述からなります（表 2-1）。

表 2-1　ST 概説の内容

TOE 概要の記述項目	・TOE がどのように用いられ、どのようなセキュリティ機能を提供するか ・TOE がどのような種別（ファイアウォール、データベース等）に属すか ・TOE が動作するために TOE 以外のハードウェア、ソフトウェア、ファームウェアで何が必要か
TOE 記述の記述項目	・TOE を構成するすべてのハードウェア、ソフトウェア、ファームウェアの詳細 ・TOE が提供する論理的なセキュリティ機能の詳細

②適合主張

CC 等への適合の主張とその根拠を記述します。

③セキュリティ課題定義

TOE において対策すべきセキュリティ課題を定義します。課題は脅威、組織のセキュリティ方針、前提条件からなります（表 2-2）。

表 2-2　セキュリティ課題定義の内容

脅威	・資産、脅威エージェント、脅威エージェントの有害なアクションの観点から、どのような脅威が想定されるか分析する ・資産とは、コンピュータが保持する情報の機密性など、TOE が保護しなければならないエンティティを指す ・脅威エージェントとは、ハッカーやユーザーなど資産に有害な影響を与える可能性のあるエンティティを指す ・脅威エージェントの有害なアクションとは、不正アクセスやなりすましなど脅威エージェントが資産に対して行うアクションを指す
組織のセキュリティ方針	・行おうとしているセキュリティ対策が、TOE の運用管理を行う組織におけるセキュリティ方針（規則やガイドライン）に適合していることを確認する
前提条件	・TOE がセキュリティ対策を運用する上で前提となる環境条件を明確にする ・物理的な前提条件としては、TOE が入退室を管理するサーバー室に設置されているといったことがある ・人的な前提条件としては、TOE 運用者が十分な訓練を受けているといったことがある ・接続に関する前提条件としては、TOE が信頼できるネットワークに接続されているといったことがある

③セキュリティ対策方針

②で定義したセキュリティ課題へのセキュリティ対策の方針を策定します。TOE 自体で実現する方針と、TOE の運用環境で実現する方針の 2 面から策定します（表 2-3）。

この 2 面の対策がセキュリティ課題をすべて解決することも検証し、セキュリティ対策方針根拠として明示することも求められます。

表 2-3　セキュリティ対策方針の内容

TOE 自体のセキュリティ対策方針	・セキュリティ課題定義で示された「脅威」に対するための機能、「組織のセキュリティ方針」に沿った機能を記述する
TOE の運用環境で実現するセキュリティ対策方針	・セキュリティ課題定義の「脅威」や「組織のセキュリティ方針」に対し運用環境面で実現する必要がある項目や、「前提条件」を適切に達成するために必要な項目を記述する

④セキュリティ要件

CC に示される「セキュリティ機能コンポーネント」(表 2-4)、「セキュリティ保証コンポーネント」(表 2-5) に基づき、③で定めた方針を再定義します。これには、セキュリティ対策方針の記述レベルの標準化を図るという目的があります。

表 2-4　セキュリティ機能コンポーネントの概要

クラス	略号	概要
セキュリティ監査	FAU	セキュリティ関連のアクティビティに関する情報の認識、記録、格納、分析に関するもの。監査結果記録は、どのようなセキュリティ関連のアクティビティが実施されているか、及び誰がそのアクティビティに責任があるかを限定するために検査され得るものである。
通信	FCO	データ交換に携わるパーティの識別情報の保証に関係する、送信情報の発信者の識別情報の保証（発信の証明）及び、送信情報の受信者の識別情報の保証（受信の証明)。これらのファミリは、発信者がメッセージを送ったことを否定できないこと、また受信者がメッセージを受け取ったことを否定できないことを保証する。
暗号サポート	FCS	TOE が暗号機能を実装する場合に使用されるもの。その実装はハードウェア、ファームウェア及び／またはソフトウェアにおいて行われ、暗号鍵管理と暗号操作の 2 個のファミリから構成される。
利用者データ保護	FDP	利用者データの保護に関連するもの。利用者データ保護におけるセキュリティ機能方針、利用者データ保護の形態、オフライン格納・インポート及びエクスポート、TOE セキュリティ機能間通信の 4 つのファミリのグループに分割される。
識別と認証	FIA	請求された利用者の識別情報を確立し検証するための機能に関するもの。適切なセキュリティ属性（例：識別情報、グループ、役割、セキュリティあるいは完全性レベル）に利用者が関連付けられていることを保証するために要求される。利用者の識別情報の判定と検証、TOE とやり取りするための利用者の権限の判定、及び各々の許可利用者に対するセキュリティ属性の正しい関連付けを取り扱う。
セキュリティ管理	FMT	TOE セキュリティ機能のいくつかの側面（セキュリティ属性、TOE セキュリティ機能データと機能）の管理を特定す

		ることを意図したもの。実施権限の分離のような、異なる管理の役割とこれらの相互の影響を特定することができる。
プライバシー	FPR	プライバシーに関するもの。他の利用者による識別情報の露見と悪用から利用者を保護する。
TOE セキュリティ機能の保護	FPT	TOE セキュリティ機能を構成するメカニズムの完全性及び管理、TOE セキュリティ機能データの完全性に関係するもの。TOE におけるセキュリティ機能方針が改ざんやバイパスされ得ないという要件の提供が必要とされる。
資源利用	FRU	処理能力及び／または格納容量など、必要な資源の可用性のサポートに関するもの。耐障害性ファミリ、サービス優先度ファミリ、資源割当てファミリの 3 つのファミリからなる。
TOE アクセス	FTA	利用者セッションの確立を制御する機能に関するもの。
高信頼パス/チャネル	FTP	利用者と TOE セキュリティ機能間の高信頼通信パス、及び TOE セキュリティ機能と他の高信頼 IT 製品間の高信頼通信チャネルに関するもの。高信頼パスを介した利用者応答は、信頼できないアプリケーションによる改変やそれへの暴露から保護されていることが保証される。

表 2-5　セキュリティ保証コンポーネントの概要

クラス	略号	概要
プロテクションプロファイル評価	APE	プロテクションプロファイル（PP）※が信頼でき内部的に一貫していること、及び PP が 1 つまたは複数の PP またはパッケージに基づいている場合に、それらの PP やパッケージを PP が正しく具体化していることを実証するための要件。 ※再利用可能なセキュリティ要件のセット、要求仕様のフレームで、ST のテンプレートといえるもの
プロテクションプロファイル構成評価	ACE	PP 構成が信頼でき一貫していることを実証するための要件。
セキュリティターゲット評価	ASE	ST が信頼でき内部的に一貫していること、及び ST が 1 つまたは複数の PP またはパッケージに基づいている場合に、それらの PP やパッケージを ST が正しく具体化していることを実証するための要件。
開発	ADV	TOE に関する情報を提供する要件。6 つのファミリからなり、AVA クラス及び ATE クラスで記述されている TOE に対する脆弱性分析とテストを実施するための基礎として使用される。
ガイダンス文書	AGD	すべての利用者の役割に対するガイダンス証拠資料に関する要件。TOE の意図しない間違った構成や、取り扱いについての可能性についても扱う。
ライフサイクルサポート	ALC	TOE の開発及び保守中に、TOE を改良するプロセスに統制と管理を確立するための要件。
テスト	ATE	TOE セキュリティ機能が記述（機能仕様、TOE 設計、及び実装表現）に従ってふるまうことの保証を提供する要件。カバレージ、深さ、独立テスト、及び機能テストの 4 つのファミリからなる。
脆弱性評定	AVA	TOE の開発または運用で生じる悪用可能な脆弱性の可能性を扱うための要件。
統合	ACO	統合 TOE が、すでに評価されたソフトウェア、ファームウェア、またはハードウェアコンポーネントが提供するセキュリティ機能性に依存する場合にセキュアに動作するという信頼を提供するための要件。5 つのファミリを含む。

2-3　テレワークに必須なゼロトラストセキュリティ

ゼロトラストセキュリティの経緯

現在、セキュリティモデルの主流は、ファイアウォールや IPS/IDS など組織の内部と外部の境目で外部からの攻撃を検知・防御する「境界型セキュリティ」です。この考え方の根底には、「組織内の端末は安全であり、脅威は外部から侵入してくる」という発想があります。しかし、境界型には一度内部に侵入されたら無力であるといった弱点が指摘されており、考え方の転換が求められるようになった中で浮上したのが「ゼロトラストセキュリティ」というモデルです（図 2-8）。

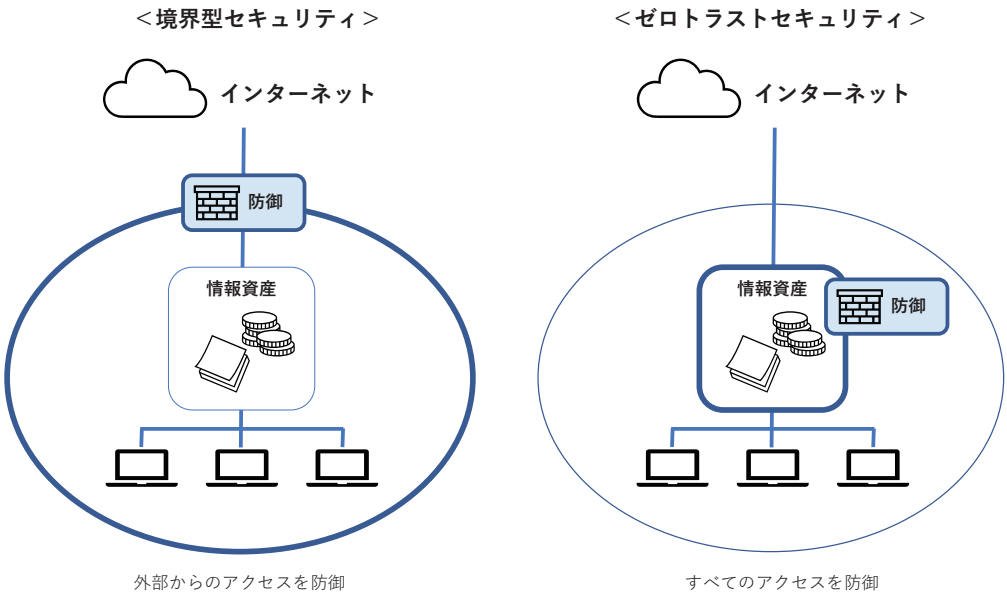


図 2-8　境界型セキュリティとゼロトラストセキュリティ

ゼロトラスト、すなわち「完全に信頼できるものは 1 つもない」という考え方は、2010 年に米国の調査会社フォレスター・リサーチのジョン・キンダーバーグにより提唱されました。ゼロトラストはホスト自体に防御力を確保するのではなく、「信頼できない限り一切の活動を許可しない」という原則に基づきます。

ゼロトラストに関する明確な概念は定まっていませんが、標準化を目指す指針として、下記に挙げた教義などを含む、NIST による「SP 800-207：Zero Trust Architecture （ZTA）」（https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf）を参

考にすることができます。

＜ゼロトラストの教義＞

1.すべてのデータソース、コンピューティングサービスはリソースと見なされる

2.ネットワークの場所に関係なく、すべての通信が保護される

3.個々の組織リソースへのアクセスは、セッションごとに許可される

4.リソースへのアクセスは、動的なポリシー（クライアントID、アプリケーション及び要求元の資産の監視可能な状態を含む）によって決定され、その他の動作属性を含めることができる

5.企業は所有し関連するすべてのデバイスが可能な限り最も安全な状態であることを保証し、それらが可能な限り最も安全な状態を継続していることを監視する

6.すべてのリソースの認証と許可は動的であり、アクセスが許可される前に厳密に実施される

7.企業はネットワークインフラと通信の現状に関する情報を可能な限り収集し、それによりセキュリティ体制を改善する

ゼロトラストセキュリティ導入の必要性を訴える声は近年、日増しに高まっています。その背景には、クラウドサービスの普及によりネットワークの外部と内部の境界があいまいになってきたことや、内部不正への対応の必要性、さらには働き方改革及び 2020 年の新型コロナウイルス感染症の流行に伴うテレワークの増加があり、いずれも従来の境界型セキュリティでは十分な対応ができないことが指摘されています。

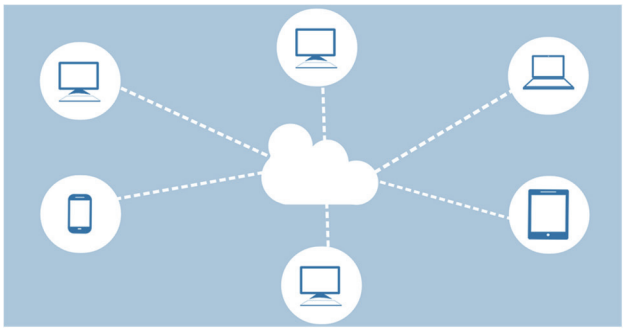
境界型セキュリティの弱点

境界型セキュリティでは、全体を壁で覆うという考え方の下、「内部に攻撃者を侵入させないこと」や「壁を強固にすること」を重視します。

「内部に攻撃者を侵入させない」ためには外部と内部を遮断する必要がありますが、情報の厳密な遮断は利便性の観点から難しく、また、過度な制限は個人所有の情報端末を無断で使用する「シャドーIT」を招きかねません。

加えて、サイバー攻撃技術の進化もあり、「壁を強固にすること」には限界があります。

仮にネットワーク上で内部と外部を 100%遮断できたとしても、USB メモリ等の媒体経由でのマルウェア感染、標的型攻撃による詐欺的な手法、内部犯行のリスク等も存在します。



システム利用が組織内に閉じていた時代には境界型セキュリティは有効でしたが、外部との連携やクラウドの利用の増大に伴い、その限界が顕在化してきました。

現在、リモートアクセスのセキュリティ技術は VPN が主流です。しかし、ユーザーの増加等により通信速度が遅くなること、クラウドサービスとの相性が悪いこと、そして VPN に接続さえできればリソースへのアクセスができてしまうという境界型セキュリティの問題を抱えていることなどから、増大するテレワークに対応するセキュリティとしては不十分と考えられています。

ゼロトラストセキュリティの構築

ゼロトラストセキュリティでは、「信頼できる者にのみ実行許可を与える」という考え方から、図 2-9 のような多要素認証をクリアした場合に初めてアクセス権限が与えられるのが基本となります。

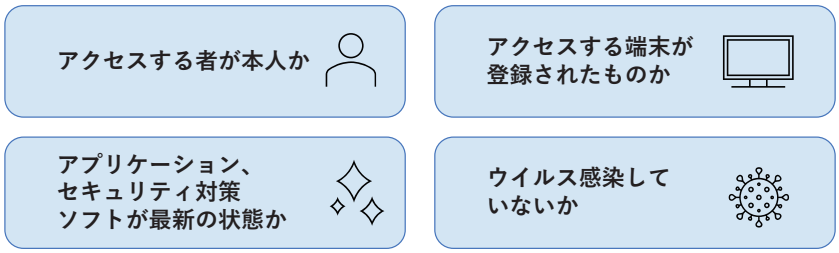


図 2-9　多要素認証

こうした認証はアクセスのたびに行われるなど、アクセス権限は常に最小限にされます。また、インシデント発生時の被害を抑えるため、ネットワーク、ユーザー、端末、アプリケーションをマクロセグメント化し、ログの記録や脅威の検知・対応を行います。

ゼロトラストを実現するためのコンポーネントは、ID を中心に整理されます（表 2-6）。

表 2-6　ゼロトラストのコンポーネント群

ID	ユーザー（ID）がゼロトラストの中心であり、ID をリアルタイムで多要素認証し、最小限のアクセス権限が許可される。
端末	ID がリソースへのアクセスを許可されると、IoT デバイスからスマートフォン、BYOD（Bring Your Own Device：私物端末の業務利用）端末、オンプレミスからクラウドサーバーに至るまで、さまざまな場所にデータが流れる可能性がある。こうした多様なデバイスを念頭に置き、その健全性の監視・強化が必要とされる。
ネットワーク	すべてのデータは最終的にネットワークを介してアクセスされるため、ネットワークを可視化し、適切なアクセス制御を行うことで、境界型セキュリティのリスクである「不正アクセス後の横断的な悪影響」を防ぐ。また、通信は暗号化し、監視・分析を行えるようにする。
データ	ゼロトラストセキュリティでは、データ保護に重点が置かれる。データは正しく分類、暗号化し、制限する。また、企業が管理するデバイス、アプリケーションなどはオフラインでも安全に管理する必要がある。
アプリケーション	オンプレミス、PaaS、SaaS 等のアプリケーションは、リアルタイムで異常な動作を監視し、ユーザーのアクションを制御する。また、シャドーIT を把握し、減らすことも必要。

ゼロトラストセキュリティのアーキテクチャを概念的に示すと、図 2-10 のようになります。

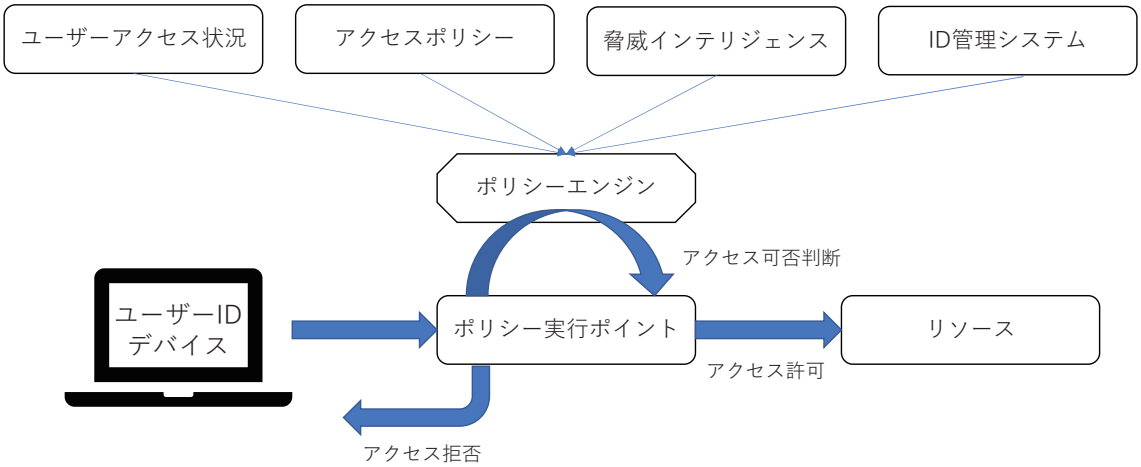


図 2-10　ゼロトラストセキュリティのアーキテクチャ

・ユーザーアクセス状況
ユーザーのアクセス状況に関するログやネットワークトラフィック状況、リソースの状態監視情報などを含む動的な情報。

・アクセスポリシー
ポリシーエンジンに解釈されるユーザー属性情報、OS やパッチバージョンなどのデバイス属性情報、それらを考慮してリソースに対するアクセス条件を定義した静的な情報。

・脅威インテリジェンス
マルウェア情報、攻撃情報、脆弱性情報、IP アドレスや DNS のブラックリスト情報など外部から得られる動的な情報。また、該当組織の SIEM 等による内部で得られる動的な情報。

・ID 管理システム
名前、メールアドレス、証明書、所属組織、職種、アクセス権限と関連システムなどのユーザー属性情報を作成、保存、管理するシステム。

・ポリシーエンジン
静的に定義されたポリシーや、脅威インテリジェンスなどの動的な各種情報を解釈し、リソースに対する対象のクライアントのアクセス可否を決定。

・ユーザーID/デバイス
ID 管理システムに登録されたユーザーID を提示する仕組みと実装されたデバイスを含むエンドポイント。

・ポリシー実行ポイント
対象クライアントとリソースの間のコネクションを監視し、ポリシーエンジンの決定にしたがってコネクションの確立や切断を一元的に実行。

・リソース
サーバー、クラウドサービス、API など該当組織が業務のために必要とする IT 関連リソース。

ゼロトラストの実装プロセス

ゼロトラストはセキュリティに対する考え方であり、これをすれば達成できるというものではありません。既に稼働しているシステムを一律に入れ替えるにもリスクが生じるため、組織ごとに環境やコスト等に応じ、前述したコンポーネント群に沿って段階的に進めるのが現実的です。

まずは、指紋認証やワンタイムパスワードなどを用いたIDの多要素認証の導入が有効です。また、業務システムを信頼できるクラウドサービス（IaaS/PaaS/SaaS）に移行することも優先的な取り組み事項に挙げられます。メールやファイルサーバー等のコミュニケーションシステムも含めてクラウド化を進め、境界型セキュリティの防御範囲を縮小していきます。

端末等のエンドポイントセキュリティの強化も重要となります。EDR（Endpoint Detection and Response）やMDM（Mobile Device Management）により、デバイス単体での自立的なセキュリティ構築を図ります。

さらに、セキュリティ対策のクラウド化も必須になりつつある考え方で、CASB（Cloud Access Security Broker）が該当します（図2-11）。これは、ユーザーと複数のクラウドプロバイダーの間に単一のコントロールポイントを置くことで、セキュリティ体制の一貫性を担保する仕組みであり、シャドーITも防ぐことができます。

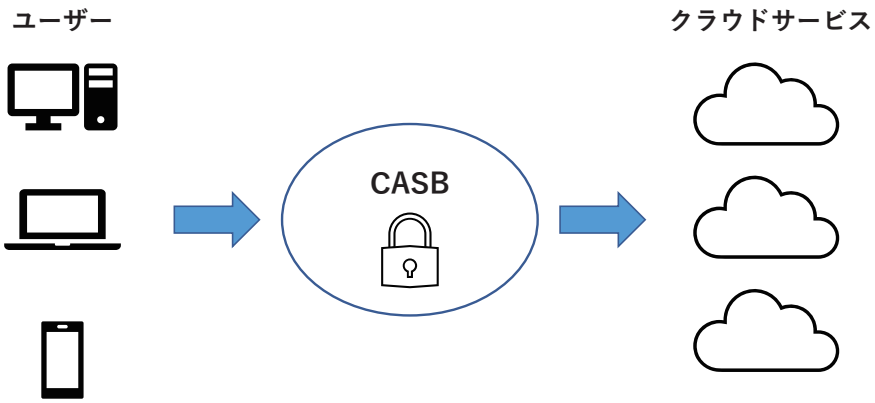


図2-11　CASBの概念

事例：BeyondCorp（Google）

BeyondCorpは、Googleが2010年頃から検討・実装を開始したゼロトラストセキュリティのモデルです。アクセス制御地点をネットワークの境界から個々のユーザーやデバイスに移すことで、VPNを使うことなく、ユーザーがどこからでも、より安全にインターネットを利用できるようにすることを目的としています。ユーザーベース、デバイスベースで認

証・アクセス制御を行う仕組みで、現在、ほとんどの Google 社員が日常的に使用しています。

アクセス制御方法としては、ロールベースアクセス制御などが用いられています（表 2-7）。

表 2-7　BeyondCorp のアクセス制御方法

ID・パスワード認証	入力された ID やパスワードが正しい場合に、ユーザーを信頼する。ID・パスワードの流失リスク等があり、これだけでは不十分。
ロールベースアクセス制御　（RBAC）	ユーザーと権限を直接紐付けず、ロール（仕事上の機能）を通して権限管理をシンプルかつ柔軟に行う。管理権限、閲覧権限、編集権限、支払い権限などをユーザーごとに正しく制御できる。
ルールベース認証	条件を事前に列挙する形式であり、「誰は」「何に」「いつ」「どの端末から」「どのアプリに」「アクセス化／不可」などのルールに沿って制御できる。
リスクベース認証	アクセスのたび、リアルタイムで「ユーザー」「端末」「ネットワーク」「場所」「時間」などに基づき、過去のアクセス状況と環境を比較してアクセスを制御する。厳密な定義が難しいルールベース認証よりも、手間なくセキュアに認証できる。

第 3 章　セキュリティマネジメント

3-1　リスクマネジメント

リスクマネジメントの基本

セキュリティを運用する上では、リスクマネジメントの視点も重要です。セキュリティ対策を行うには、組織におけるセキュリティ上のリスクを特定して分析・評価（リスクアセスメント）し、評価したリスクをどのように管理するかを決定・実施するプロセスが欠かせないためです。

セキュリティに限らず一般的なリスク全般に対するリスクマネジメントの原則・指針を定める規格として、国際規格の ISO 31000 及びその国内規格として JIS Q 31000 があります。

JIS Q 31000 では図 3-1 のリスクマネジメントプロセスが示されており、後述する情報セキュリティマネジメントシステム（ISMS）においても本プロセスの実施が求められるなど、情報セキュリティの基盤とされています。

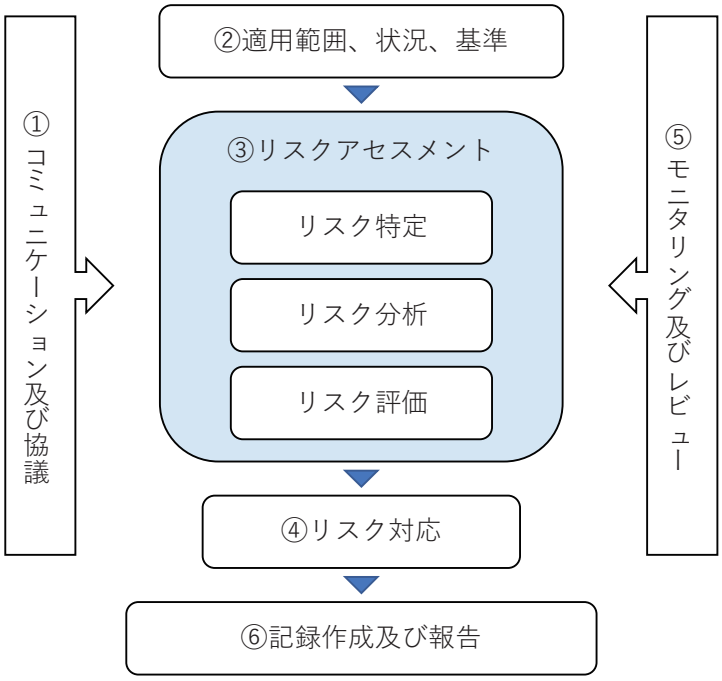


図 3-1　リスクマネジメントプロセス

①コミュニケーション及び協議

関連するステークホルダーが、リスク、意思決定の根拠及び特定の活動が必要な理由が理解できるように支援します。コミュニケーションはリスクに対する意識・理解の促進を目指すもので、協議は意思決定を裏付けるためのフィードバックと情報の入手を含みます。

このプロセスは、リスクマネジメントプロセスの各段階及び全体を通して実施することが望まれます。

②適用範囲、状況、基準

適用範囲、状況及び基準を確定することで、リスクマネジメントプロセスを組織に合わせ、効果的なリスクアセスメント及び適切なリスク対応を可能にします。

③リスクアセスメント

リスクを特定し、特定したリスクを分析及び評価するプロセスで、 ステークホルダーの知識及び見解を生かし、体系的、反復的、協力的に行われることが望まれます。

④リスク対応

リスクに対処するための選択肢を選定し、実施します。 具体的には、リスク対応の選択肢を選定してリスク対応を計画、実施します。そして、その対応の有効性を評価し、残留リスク※が許容可能かどうかを判断した上で、許容できない場合はさらなる対応を実施します。

※残留リスクとは リスクを完全に除去することは不可能であり、対策をした後でも残るリスクを残留リスクと呼びます。残留リスクに対し、さらなる対策を検討するか、あるいは許容するかについては、対策にかけるコストとリスク発生による損害の程度を比較して対策の合理性・妥当性を検討する必要があり、経営的な判断が求められます。

⑤モニタリング及びレビュー

プロセスの設計、実施及び結末の質及び効果を保証し、改善します。継続的なモニタリングと定期的なレビューを計画に位置付け、プロセスのすべての段階で行うことが望まれます。

⑥記録作成及び報告

リスクマネジメントプロセス及びその結末を文書化し、報告します。

情報セキュリティリスクマネジメント

前項で述べたリスクマネジメントプロセスの中心となる③リスクアセスメント、④リスク対応は、情報セキュリティの場合、下記のように具体化することができます。

①情報セキュリティリスクの特定

組織において守るべき情報資産が何かを整理し、望ましくない影響を与えうるリスクを特定します（図 3-2）。

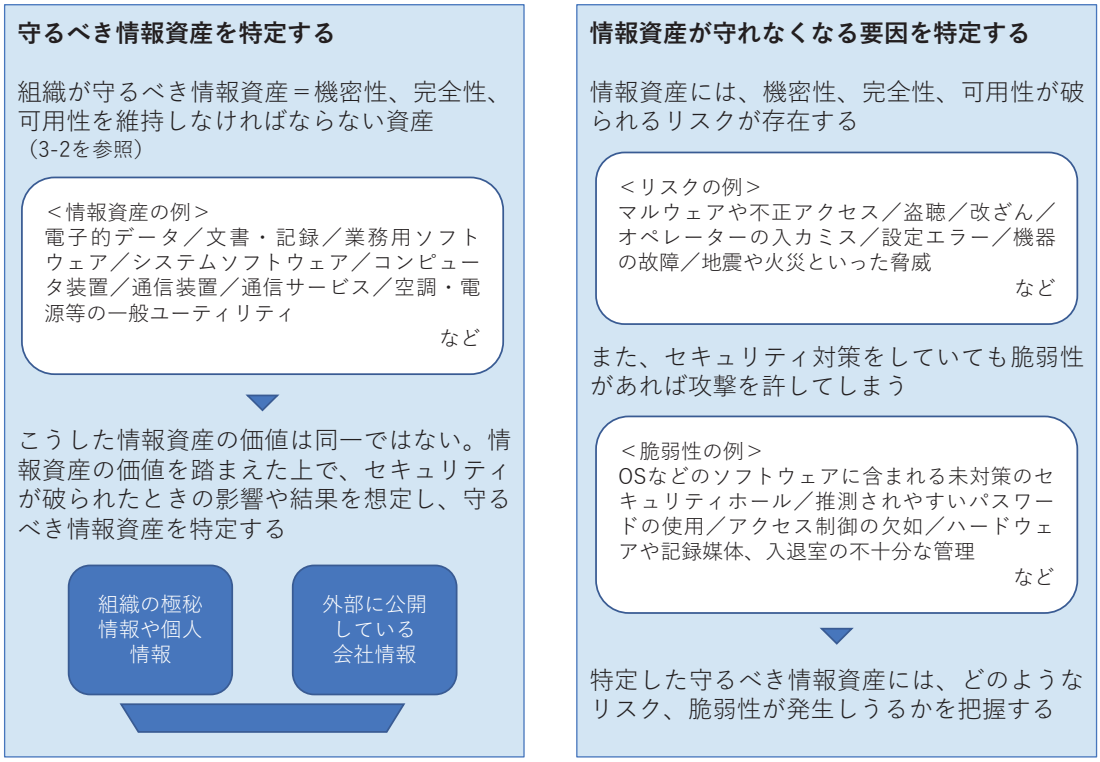


図 3-2　情報セキュリティリスクの特定方法

②情報セキュリティリスクの分析

①で特定した情報セキュリティリスクが実際に発生する可能性と、発生した場合に生じる影響の大きさ（結果）を評価し、リスクの大きさ（リスクレベル）を分析します。

リスクレベルの分析は、情報資産の価値や脅威の発生可能性、セキュリティ対策に存在する脆弱性の程度により評価を行います（図 3-3）。

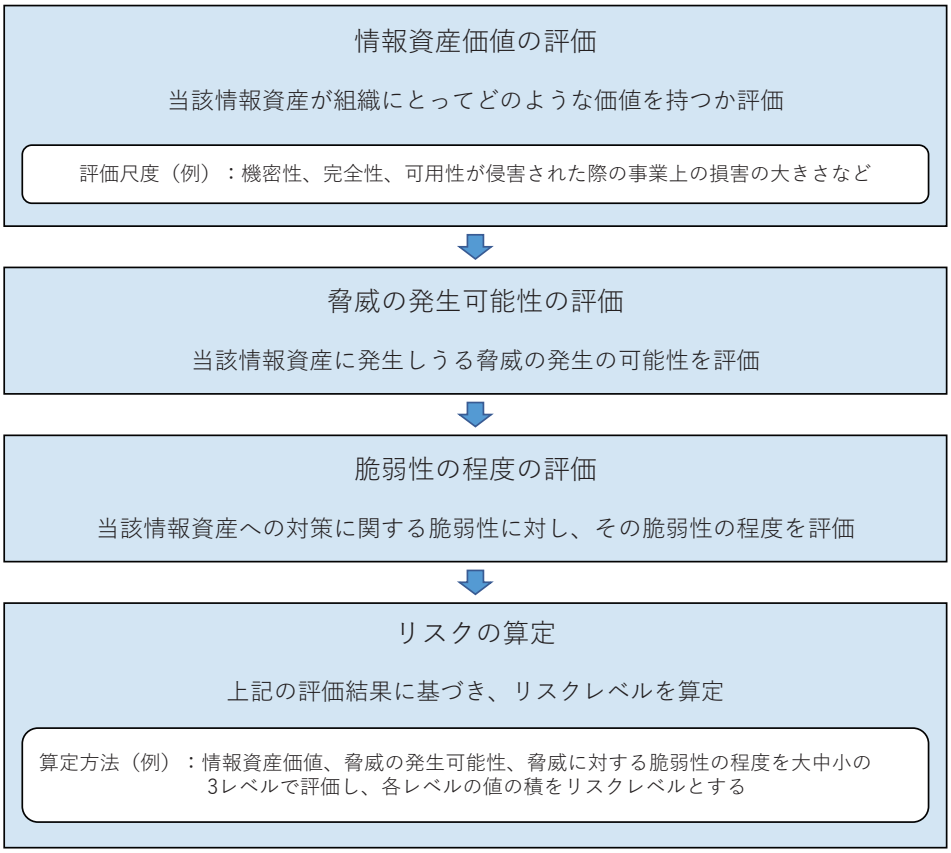


図 3-3　リスクレベルの分析プロセス

③情報セキュリティリスクの評価

②で算出したリスクレベルを、P43 の「②適用範囲、状況、基準」で設定するリスク基準（リスクの重大性を評価するための目安とする条件）と比較します。

リスク基準より高いレベルのリスクに対しては、リスク対応を行い、リスク基準以下のレベルに低減することが必要となります。一方、リスク基準より低いレベルのリスクは、組織にとって受容可能なリスクであると判断されます。

④情報セキュリティリスクへの対応

③でリスク対応を行う必要があると判断されたリスクに対し、対策として考えられる選択肢を選び、実施します。

具体的に選択肢としては、「リスク低減」「リスク受容」「リスク回避」「リスク共有」といった対応が考えられます（図 3-4）。

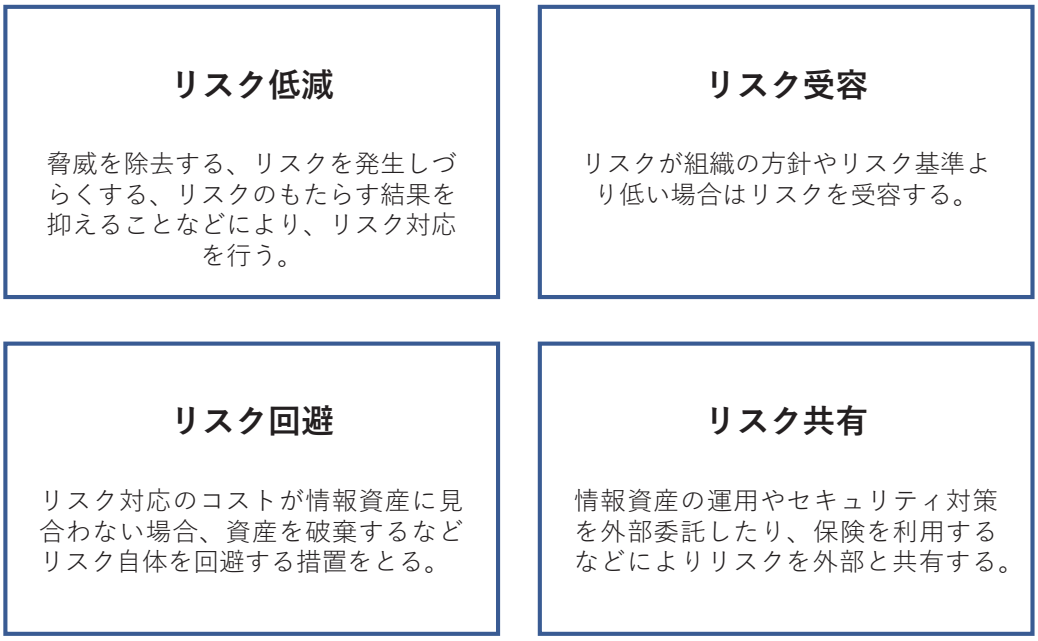


図 3-4　セキュリティリスク対応の選択肢

⑤対応策の評価

リスク低減やリスク共有の対応をとる場合、それによりリスクレベルがどの程度低減されるか評価する必要があります。評価は、②のリスク分析を、対応策を行った場合の効果を考慮して再度行うことにより算出されます。

再算出したリスクレベルが、リスク基準より下回っていれば対応策が有効であり、リスク基準より大きいままであれば、対応策の再検討が必要になります。

リスクアセスメントへの 4 種類のアプローチ

リスクアセスメントには決まった手法があるわけではなく、それぞれの組織に応じて行われることが重要です。アプローチ方法としては、一般財団法人日本情報経済社会推進協会（JIPDEC）が発行している『ISMS ユーザーズガイド－リスクマネジメント編－』による 4 種類のアプローチを参考にすることができます（表 3-1）。

表 3-1　リスクアセスメントへのアプローチ方法

詳細リスク分析	前項のようにリスクアセスメントを詳細に行うアプローチ。 対象となる組織に応じたセキュリティ対策を選択することが可能だが、リスクアセスメントの対象が大規模な場合、対象すべてに適用するのは、非常に作業量が多くなり、経営資源の制約や効率性の観点から現実的ではない場合があり得る。

ベースライン アプローチ	あらかじめ一定の確保すべきセキュリティレベルと、そのセキュリティレベルで実施すべき対策のセットを準備しておき、対象となる組織に一律に対策のセットを適用するアプローチ。 リスクアセスメントにかかる作業量は少なくて済むが、一律的な対策となるため、リスクに対し不十分あるいは過剰な対策がとられる可能性がある。
非形式的 アプローチ	分析対象に精通した専門家が、自分の知識や経験に基づく考察によりリスクを判定するアプローチ。 専門家個人の経験やノウハウに基づく効率的な分析が可能である一方、リスクの見落としや偏った対策がとられる可能性があり、また、分析結果の根拠の正当化が困難という懸念もある。
組み合わせ アプローチ	複数のアプローチを併用し、それぞれのアプローチの長所短所を相互に補完し、作業の効率化や分析精度の向上を図るアプローチ。 例えば、重要な情報資産に対しては「詳細リスク分析」を行い、それ以外は「ベースラインアプローチ」を適用するといった方法がある。

3-2　情報セキュリティマネジメントシステム（ISMS）

情報セキュリティマネジメントシステム（ISMS）とは

情報セキュリティリスクマネジメントを適切に実行するためには、新しい脅威や脆弱性に柔軟に対応する仕組みや従業員の内部不正による情報漏えいの防止策、シャドーIT などの人的管理を適切化するルール、環境の変化に合わせた基準等の見直しプロセスの確立など、多様な観点を踏まえる必要があります。

そのため、情報セキュリティ技術の管理・運用だけでなく、紙の書類まで含めた情報管理や設備管理、人的管理など、組織全体での実行体制が求められます。

こうした総合的な情報セキュリティ対策を実現し、維持・改善してゆくための仕組みを、情報セキュリティマネジメントシステム（ISMS：Information Security Management System）といいます。

ISMS については、国際標準規格として ISO/IEC 27000 が策定されています。日本規格では JIS Q 27000 が定められ、対象とする情報セキュリティについて「情報の機密性、完全性及び可用性を維持すること」と定義しています（図 3-5）。

ISMS は、組織が保護すべき情報資産における機密性、完全性、可用性の維持・改善を基盤に構築・運用します。

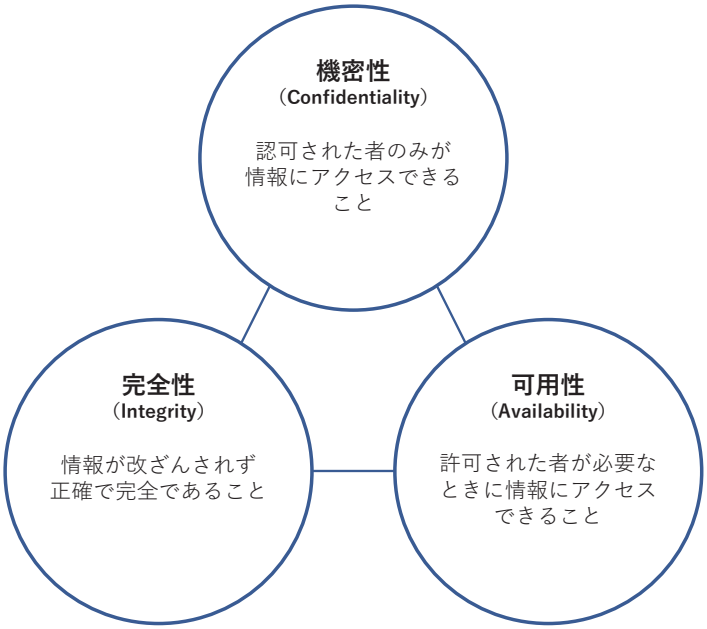


図 3-5　機密性、完全性、可用性

ISMS の適用範囲

ISMS は、組織が推進する事業や組織の状況に応じて構築されるものです。そのため、まず ISMS の適用範囲の検討が必要となります。具体的には、組織全体に対して ISMS を構築するのか、特に必要な部署に対して構築するのかについて、下記の観点から判断します。

＜事業＞

・組織が行っている事業の特徴から ISMS が必要か

＜組織＞

・ISMS の対象に社内及び社外（業務委託先や顧客など）の組織をどこまで含むか
・ISMS に関連する利害関係者の要求事項に何があるか
・他の組織の活動との間の役割分担や責任分界点をどう設定するか

＜場所＞

・ISMS の対象に建物や土地などをどこまで含むか

＜技術＞

・ISMS の対象にネットワークやシステム及びそれらのインターフェイスをどこまで含むか

＜資産＞

・ISMS の対象に情報資産をどこまで含み、情報資産に対する責任をどこまで含むか

ISMS 構築・運用の PDCA サイクル

ISMS は、①計画（Plan）、②実施（Do）、③点検（Check）、④処置（Act）の PDCA サイクルによる継続的な運用・管理が前提とされています（図 3-6）。

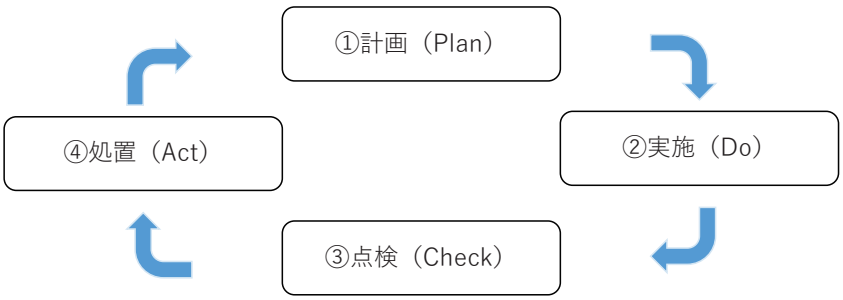


図 3-6　PDCA サイクル

①計画（P）…セキュリティポリシーの策定

組織における情報セキュリティの基本方針（セキュリティポリシー）を策定します（3-3 を参照）。セキュリティポリシーは、組織として事業を継続する上でどのようなセキュリティを達成する必要があるかを示す「情報セキュリティ基本方針」、その基本方針の下でどのようなセキュリティ対策を行うかの方針を定める「情報セキュリティ対策基準」から構成されるのが一般的です。

情報セキュリティ対策基準の策定は、3-1 で述べた情報セキュリティリスクマネジメントのプロセスが相当し、組織にとってどのようなセキュリティ上のリスクがあるかを分析・評価し、その結果に基づきリスクをどのように管理してセキュリティを守るかを決定します。

②実施（D）…ISMS の導入・運用

対策基準で示された施策を、各部署で具体的な対策に展開・実装し、運用していきます（表 3-2）。

表 3-2　ISMS の運用事項

対策の適用	①で策定した技術的対策については、その対策システムを設計、構築し、対象の情報システムに組み込む。 また、物理的対策についても、入退室管理設備を備えたセキュリティ区域の整備などの対策を行う。
対策実施手順の整備	運用・操作手順書、利用者ガイダンス等の書類を整備し、各管理担当者、利用者に周知する。
運用体制の整備	セキュリティ管理を行う担当者の責任、権限、義務を明確化するとともに、組織内におけるセキュリティ管理・運用に関する教育・訓練等を定期的に行う。
対策の運用	実際にセキュリティ対策を運用・記録する。

ISMS の運用体制としては、セキュリティ管理責任者を中心に、必要に応じて委員会等を設置して対応します（図 3-7）。

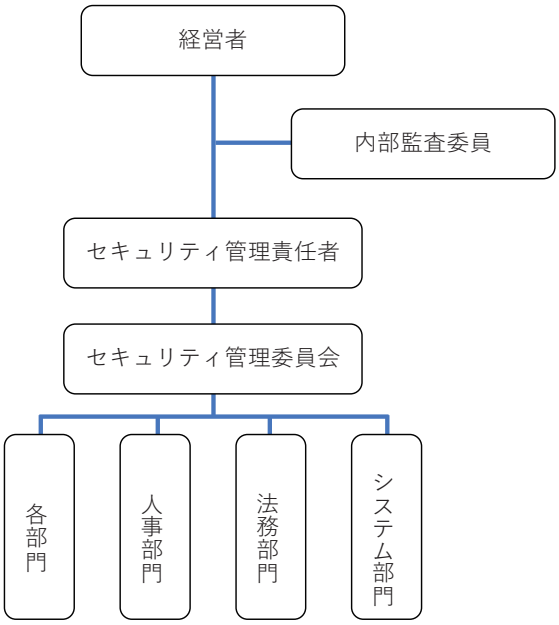


図 3-7　ISMS の運用体制

③点検（C）…ISMS の監視・評価

情報セキュリティ対策基準で規定された対策が手順書通りに運用され有効に機能しているか、また、その手順に改善点がないかなどを、運用記録や従業員へのヒアリング等を通じてチェックします。

このフェーズで重要なのが情報セキュリティ監査です。情報セキュリティ監査には、組織

内部の監査部門等が行う内部監査と、外部の監査会社等が行う外部監査とがあり、通常、ISMS の点検フェーズでは内部監査が実施されます。

④処置（A）…ISMS 有効性の維持・改善

③の結果に基づき、セキュリティポリシーの見直しも含めて改善計画を作成・実行します。このフェーズでは、組織の経営層を含めてレビュー（マネジメントレビュー）を行うことが重要となります。

3-3　セキュリティポリシーの策定

セキュリティポリシーとは

セキュリティポリシーは、組織がどのように情報セキュリティに対処するかについての基本となる方針を示す文書です。

セキュリティポリシーは、組織の全構成員に対し公開され、各人が内容を理解することで、組織員のセキュリティ意識、組織内モラルの向上が見込まれます。セキュリティ対策においては人員管理に関する項目も含むことから、組織員の十分な理解が不可欠となります。

セキュリティポリシーは、その実行性を高めるため、基本的に経営層からトップダウンで示されるべきであり、組織のセキュリティに対する方針が示されるため組織外には非公開とするのが一般的です。

セキュリティポリシー

・組織全体のルール
・どのような情報資産を、どのような脅威から、どのように守るのか
・情報セキュリティを確保するための体制

など

セキュリティポリシーの構成

前述したようにセキュリティポリシーは「情報セキュリティ基本方針」と「情報セキュリティ対策基準」からなり、これに規則・細則や手順書、ガイドライン等のマニュアル類から構成されるのが一般的です（図 3-8）。

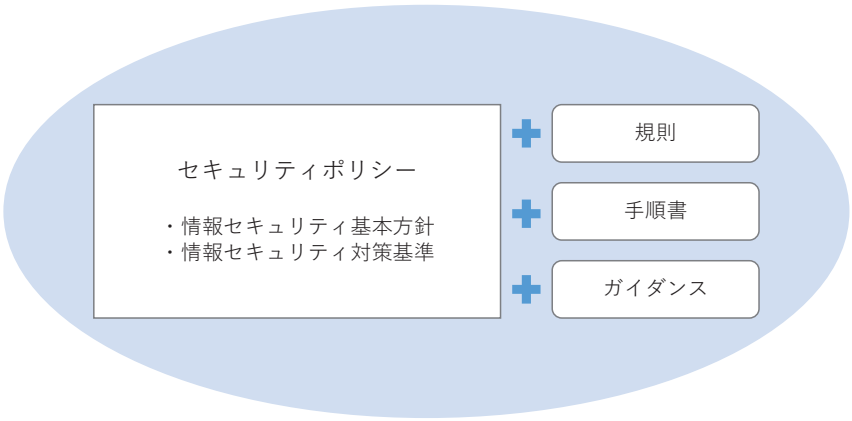


図 3-8　セキュリティポリシーの構成

情報セキュリティ対策基準

情報セキュリティ対策基準は、情報セキュリティ基本方針を実現するために取るべき施策の基準を示す文書です（図 3-9）。

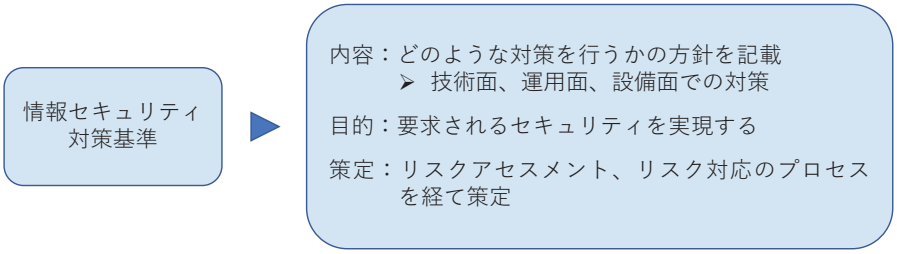


図 3-9　情報セキュリティ対策基準の概要

リスクを分析・評価し、評価したリスクを許容できるレベルまで低減するために、どのような対策を取るべきかを検討・評価した結果が、情報セキュリティ対策基準となります。

情報セキュリティ対策基準には、表 3-3 のような項目が記載されます（JIS Q 27001 附属書 A より）。

表 3-3　情報セキュリティ対策基準の項目

情報セキュリティのための方針群	・情報セキュリティのための経営陣の方向性
情報セキュリティのための組織	・内部組織 ・モバイル機器及びテレワーキング
人的資源のセキュリティ	・雇用前 ・雇用期間中 ・雇用の終了及び変更

資産の管理	・資産に対する責任 ・情報分類 ・媒体の取扱い
アクセス制御	・アクセス制御に対する業務上の要求事項 ・利用者アクセスの管理 ・利用者の責任 ・システム及びアプリケーションのアクセス制御
暗号	・暗号による管理策
物理的及び環境的 セキュリティ	・セキュリティを保つべき領域 ・装置
運用のセキュリティ	・運用の手順及び責任 ・マルウェアからの保護 ・バックアップ ・ログ取得及び監視 ・運用ソフトウェアの管理 ・技術的ぜい弱性管理 ・情報システムの監査に対する考慮事項
通信のセキュリティ	・ネットワークセキュリティ管理 ・情報の転送
システムの取得、開発及び 保守	・情報システムのセキュリティ要求事項 ・開発及びサポートプロセスにおけるセキュリティ ・試験データ
供給者関係	・供給者関係における情報セキュリティ ・供給者のサービス提供の管理
情報セキュリティ インシデント管理	・情報セキュリティインシデントの管理及びその改善
事業継続マネジメントにおける情報セキュリティの側面	・情報セキュリティ継続 ・冗長性
順守	・法的及び契約上の要求事項の順守 ・情報セキュリティのレビュー

規則、手順書、ガイドライン

規則・細則や手順書、ガイドライン等のマニュアル類は、情報セキュリティ対策基準で示される対策を具体化し、システム実装後に運用を行うための手順を具体的に記述するものです。情報セキュリティ対策基準に則り、それぞれの部署の状況に応じて作成されるもので、管理者やユーザーはこれらの手順書・マニュアルに従って実際の操作、運用、記録、報告等を行います。

3-4　ISMS の規格

ISMS に関する標準規格

ISMS に関する主要な規格として、国際標準規格の ISO/IEC 27001（日本規格は JIS Q 27001）と ISO/IEC 27002（日本規格は JIS Q 27002）があります。国際規格と日本規格の実質的な内容は同一です。

また、ISO/IEC27000 及び JIS Q 27000 は、 ISMS に関する用語及び定義を規定する規格となっており、27001、27002 を参照する際には、この規格も必要に応じて参照します。

JIS Q 27001：ISMS の要求事項

JIS Q 27001 は、組織が ISMS を構築する際の要求事項を示しており（表 3-4）、PDCA サイクルにおいては、4〜6 が「計画（P）」、7〜8 が「実施（D）」、9 が「点検（C）」、10 が「処置（A）」に相当します。

なお、附属書 A には表 3-3 に示した情報セキュリティ対策基準に相当する内容が盛り込まれており、リスク低減のための対策を附属書 A の 114 項目から選択するというように用います。

表 3-4　JIS Q 27001 の目次

0 序文	0.1 概要 0.2 他のマネジメントシステム規格との両立性
1 適用範囲	
2 引用規格	
3 用語及び定義	
4 組織の状況	4.1 組織及びその状況の理解 4.2 利害関係者のニーズ及び期待の理解 4.3 情報セキュリティマネジメントシステムの適用範囲の決定 4.4 情報セキュリティマネジメントシステム
5 リーダーシップ	5.1 リーダーシップ及びコミットメント 5.2 方針 5.3 組織の役割，責任及び権限
6 計画	6.1 リスク及び機会に対処する活動 6.2 情報セキュリティ目的及びそれを達成するための計画策定
7 支援	7.1 資源 7.2 力量 7.3 認識 7.4 コミュニケーション 7.5 文書化した情報
8 運用	8.1 運用の計画及び管理 8.2 情報セキュリティリスクアセスメント 8.3 情報セキュリティリスク対応
9 パフォーマンス評価	9.1 監視、測定、分析及び評価 9.2 内部監査 9.3 マネジメントレビュー
10 改善	10.1 不適合及び是正処置 10.2 継続的改善
附属書 A（規定）管理目的及び管理策 参考文献	

JIS Q 27002：情報セキュリティマネジメント実践のガイドライン

JIS Q 27002 は、情報セキュリティマネジメントの実践のためのガイドラインを示すものであり（表 3-5）、JIS Q 27001 の附属書 A の解説書という位置付けです。そのため、JIS Q 27001 の附属書 A から選択した対策を実装する場合のガイドラインとして、JIS Q 27002 の内容を参照するという使い方をします。

表 3-5　JIS Q 27002 の目次

0 序文	0.1 背景及び状況 0.2 情報セキュリティ要求事項 0.3 管理策の選定 0.4 組織固有の指針の策定 0.5 ライフサイクルに関する考慮事項 0.6 関連規格
1 適用範囲	
2 引用規格	
3 用語及び定義	
4 規格の構成	4.1 箇条の構成 4.2 管理策のカテゴリ
5 情報セキュリティのための方針群	5.1 情報セキュリティのための経営陣の方向性
6 情報セキュリティのための組織	6.1 内部組織 6.2 モバイル機器及びテレワーキング
7 人的資源のセキュリティ	7.1 雇用前 7.2 雇用期間中 7.3 雇用の終了及び変更
8 資産の管理	8.1 資産に対する責任 8.2 情報分類 8.3 媒体の取扱い
9 アクセス制御	9.1 アクセス制御に対する業務上の要求事項 9.2 利用者アクセスの管理 9.3 利用者の責任 9.4 システム及びアプリケーションのアクセス制御
10 暗号	10.1 暗号による管理策
11 物理的及び環境的セキュリティ	11.1 セキュリティを保つべき領域 11.2 装置

12 運用のセキュリティ	12.1 運用の手順及び責任 12.2 マルウェアからの保護 12.3 バックアップ 12.4 ログ取得及び監視 12.5 運用ソフトウェアの管理 12.6 技術的ぜい弱性管理 12.7 情報システムの監査に対する考慮事項
13 通信のセキュリティ	13.1 ネットワークセキュリティ管理 13.2 情報の転送
14 システムの取得、開発及び保守	14.1 情報システムのセキュリティ要求事項 14.2 開発及びサポートプロセスにおけるセキュリティ 14.3 試験データ
15 供給者関係	15.1 供給者関係における情報セキュリティ 15.2 供給者のサービス提供の管理
16 情報セキュリティインシデント管理	16.1 情報セキュリティインシデントの管理及びその改善
17 事業継続マネジメントにおける情報セキュリティの側面	17.1 情報セキュリティ継続 17.2 冗長性
18 順守	18.1 法的及び契約上の要求事項の順守 18.2 情報セキュリティのレビュー
参考文献	

第 4 章　セキュアなシステム運用

4-1　情報セキュリティ監査

情報セキュリティ監査

前章で述べたとおり、セキュリティシステムを適切に運用するためには、日々変化する脅威や組織を取り巻く環境に応じてリスクアセスメントを行い、情報セキュリティ対策を策定・見直すサイクルを回していく情報セキュリティマネジメントシステム（ISMS）を確立させることが必要となります。

ISMS における PDCA サイクルで、「点検（C）」に該当するのが、情報セキュリティ監査です。「計画（P）」で策定した情報セキュリティ基本方針、情報セキュリティ対策基準に従い、「実行（D）」で対策が有効に実施されているかについて、評価を行うというものです。この監査結果に基づき、次の「処置（A）」で ISMS の改善を図ることになります（図 4-1）。

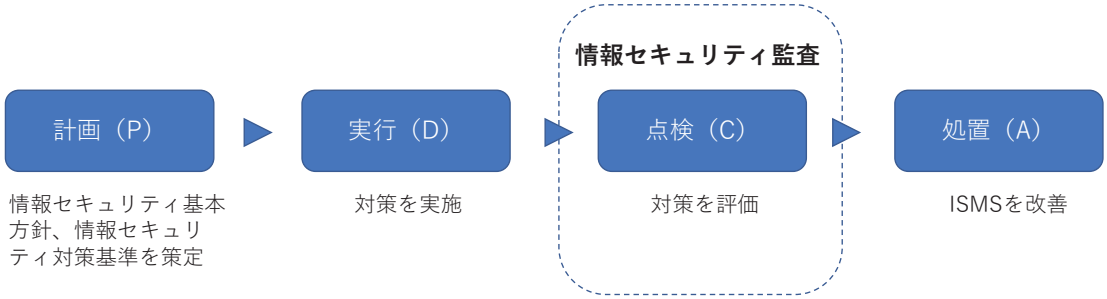


図 4-1　PDCA サイクルにおける情報セキュリティ監査

監査方式の種類

情報セキュリティ監査には、助言型監査と保証型監査という 2 つの監査方式が存在します（図 4-2）。ISMS における点検（C）のフェーズでは、助言型監査が主流となっています。

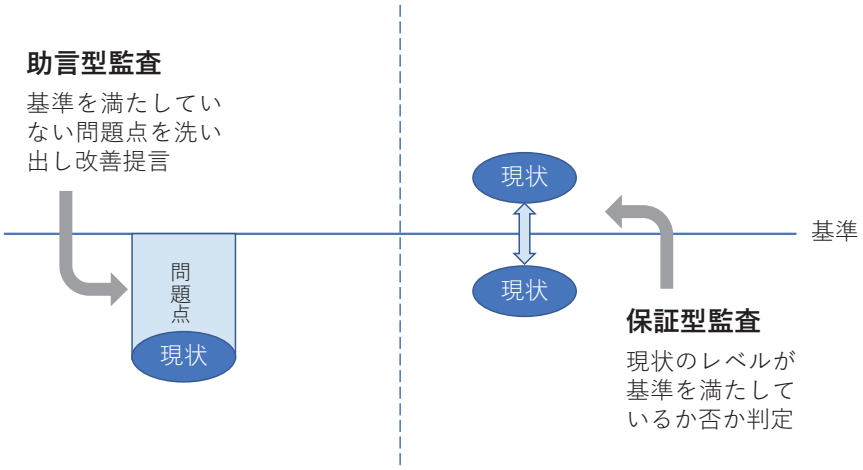


図 4-2　助言型監査と保証型監査

■助言型監査

情報セキュリティに関するマネジメントの改善を目的として、監査対象の情報セキュリティ対策上の問題点を洗い出し、問題点に対する改善提言を行う監査方式です。改善提言は情報セキュリティ対策に対して一定の保証を付与するものではなく、情報セキュリティ監査人の意見として扱われます。

組織内部の対策向上のために行われるもので、監査人の所属は内部・外部を問いませんが、通常は内部監査人が実施することが一般的です。

■保証型監査

監査対象の情報セキュリティに関するマネジメントが、監査手続きを実施した限りにおいて、適切か不適切かを伝達する監査方式です。

主に外部の利害関係者に対して利用され、外部の第三者である監査人が行うのが基本です。

なお、インシデントが発生しないという絶対的な保証ではなく、情報セキュリティ監査人が監査基準に従い、監査手続きを行った範囲における合理的な保証という位置付けになります。

監査に関する制度

ISMS の監査に関する制度として、「ISMS 適合性評価制度」と「情報セキュリティ監査制度」があります。

■ISMS 適合性評価制度

ISMS 適合性評価制度は、組織の情報セキュリティのための仕組みが国際規格に適合して

いることを証明する制度です。セキュリティ管理に対する第三者適合性評価制度として、2002 年より一般財団法人日本情報経済社会推進協会 （JIPDEC）が本運用を行い、2018 年からは同協会から独立した一般社団法人情報マネジメントシステム認定センター（ISMS-AC）が認定業務を行っています（図 4-3）。審査は、組織が構築した ISMS が JIS Q 27001（ISO/IEC 27001）に適合しているかを確認することによってなされます。

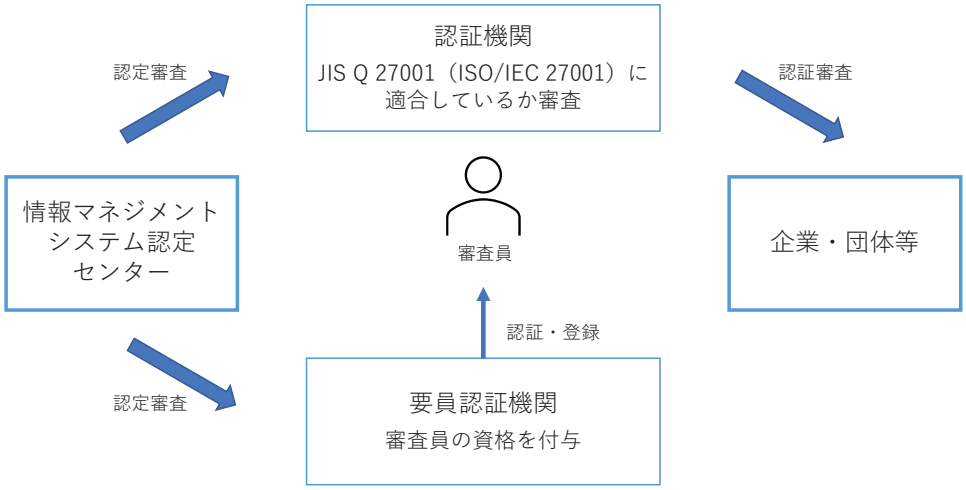


図 4-3　ISMS 適合性評価制度の運用

制度の背景には、電子商取引の安全性・信頼性を確保するため、国際水準の情報セキュリティ対策が求められていることがあります。国内のみならず国際的にも信頼を得られる情報セキュリティ管理を評価・認証し、日本における情報セキュリティレベル全体の向上を図っています。

■情報セキュリティ監査制度

情報セキュリティ監査制度は、情報セキュリティ監査業務の品質を確保し、有効・効率的に監査を行うことを目的とした制度です。信頼できる外部の独立した専門組織に情報セキュリティ対策の監査を依頼できる体制を整備するため、2003 年から経済産業省により運用が開始され、特定非営利活動法人日本セキュリティ監査協会（JASA）が制度の普及促進を行っています。

本制度と ISMS 適合性評価制度の評価基準は基本的に同じですが、本制度は監査内容について基本的に被監査主体の選択の自由度が高く、一部を重点評価することも可能です。そのため、本制度で部分的な監査を積み重ね、一定の段階で ISMS 適合性評価制度の認証を取得するといったプロセスも想定されています。

情報セキュリティ監査制度における監査基準

情報セキュリティ監査制度では、「情報セキュリティ管理基準」と「情報セキュリティ監査基準」の 2 つの基準から情報セキュリティ監査が行われています。

■情報セキュリティ管理基準

情報セキュリティ監査に当たっての判断の尺度となる基準で、ISO/IEC 17799（国内規格は JIS X 5080）をベースに策定されています。「マネジメント基準」と「管理策基準」から構成され（図 4-4）、ISMS の国際標準規格である ISO/IEC 27001（国内規格は JIS Q 27001）、ISO/IEC 27002（国内規格は JIS Q 27002）との整合性がとられています。

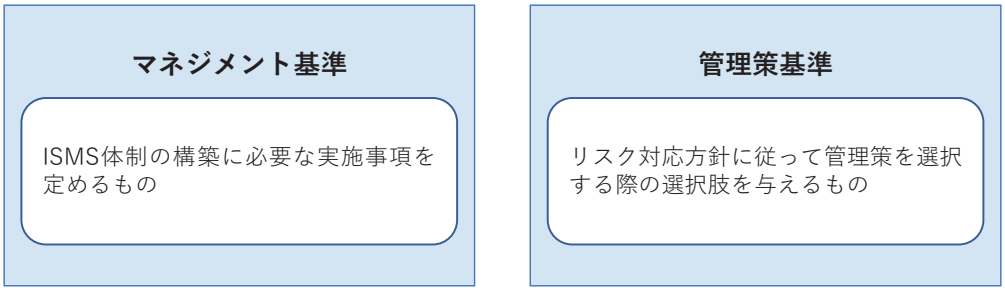


図 4-4　情報セキュリティ管理基準の内訳

情報セキュリティ監査を行う際は、この管理基準を参照して、監査対象組織に対し確認すべき項目を策定します。マネジメント基準は原則としてすべて実施すべき事項ですが、管理策基準は監査対象となる組織の状況に応じて取捨選択し、または修正・追加などを行います。

■情報セキュリティ監査基準

情報セキュリティ監査を行う主体の行為規範を定めるもので、監査人の要件や監査の各プロセスで実施すべき事項、監査報告が示されています。

監査人としての適格性及び監査業務上の遵守事項を規定する「一般基準」と、監査計画の立案及び監査手続の適用方法を中心に監査実施上の枠組みを規定する「実施基準」、監査報告に係る留意事項と監査報告書の記載方式を規定する「報告基準」により構成されています（表 4-1）。

表 4-1　情報セキュリティ監査基準（概要）

一般基準	外観上の独立性	監査人は、監査を客観的に実施するために、監査対象から独立していなければならない。
	精神上の独立性	監査人は、監査に当たり、偏向を排し、常に公正かつ客観的に監査判断を行わなければならない。
	職業倫理と誠実性	監査人は、職業倫理に従い、誠実に業務を実施しなければならない。
	専門能力	監査人は、適切な教育と実務経験を通じて、専門職としての知識及び技能を保持しなければならない。
	注意義務	監査人は、専門職としての相当な注意をもって業務を実施しなければならない。
	守秘義務	監査人は、監査の業務上知りえた秘密を正当な理由なく他に開示し、自らの利益のために利用してはならない。
	品質管理	監査人は、監査結果の適正性を確保するために、適切な品質管理を行わなければならない。
実施基準	監査計画の立案	監査人は、実施する監査の目的を有効かつ効率的に達成するために、監査手続の内容、時期及び範囲等について適切な監査計画を立案しなければならない。監査計画は、事情に応じて適時に修正できるように弾力的に運用しなければならない。
	監査証拠の入手と評価	監査人は、監査計画に基づいて、適切かつ慎重に監査手続を実施し、保証又は助言についての監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければならない。
	監査調書の作成と保存	監査人は、実施した監査手続の結果とその関連資料を、監査調書として作成しなければならない。監査調書は、監査結果の裏付けとなるため、監査の結論に至った過程がわかるように秩序整然と記録し、適切な方法によって保存しなければならない。
	監査業務の体制	監査人は、監査の目的が有効かつ効率的に達成されるように、適切な監査体制を整え、監査計画の立案から監査報告書の提出及び改善指導までの監査業務の全体を管理しなければならない。
	他の専門職の利用	監査人は、監査の目的達成上、必要かつ適切と判断される場合には、他の専門職による支援を考慮しなければならない。他の専門職による支援を仰ぐ場合であっても、利用の範囲、方法、及び結果の判断等は、監査人の責任において行われなければならない。

報告基準	監査報告書の提出と開示	監査人は、実施した監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならない。監査報告書の外部への開示が必要とされる場合には、監査人は、監査の依頼者と慎重に協議の上で開示方法等を考慮しなければならない。
	監査報告の根拠	監査人が作成した監査報告書は、監査証拠に裏付けられた合理的な根拠に基づくものでなければならない。
	監査報告書の記載事項	監査報告書には、実施した監査の対象、実施した監査の概要、保証意見又は助言意見、制約又は除外事項、その他特記すべき事項について、監査人が監査の目的に応じて必要と判断した事項を明瞭に記載しなければならない。
	監査報告についての責任	監査報告書の記載事項については、監査人がその責任を負わなければならない。
	監査報告に基づく改善指導	監査人は、監査の結果に基づいて所要の措置が講じられるよう、適切な指導性を発揮しなければならない。

4-2　インシデント対応の基本

インシデント対応プロセス

どんなにセキュリティ対策を強固に行っても、インシデントの発生を完全に防ぐことはできません。大切なのは、インシデントが発生した際に、いかに被害を極小化できるかです。

インシデント対応のプロセスは、①準備、②検知、分析、③封じ込め、根絶、復旧、④インシデント後の対応というフェーズにより構成されます（図 4-5。NIST「SP 800-61 Rev.2：コンピュータセキュリティインシデント対応ガイド」より）。

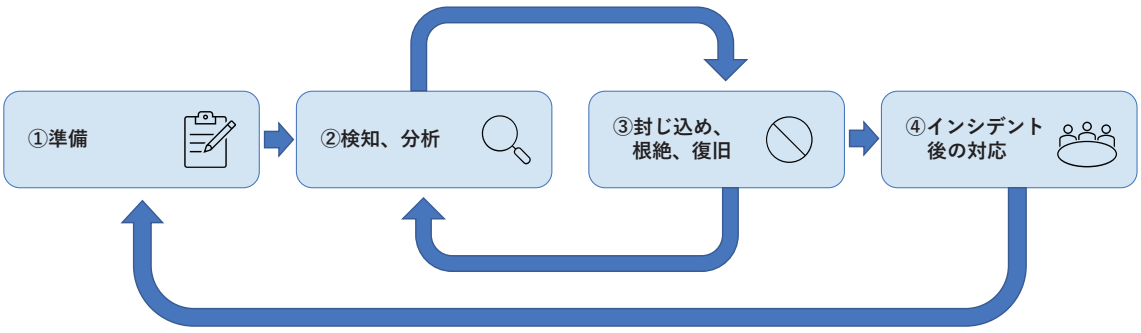


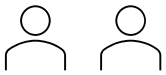
図 4-5　インシデント対応のサイクル

①準備

組織がインシデントに適切に対応するためには、事前の準備が必要です。準備には、CSIRT（Computer Security Incident Response Team、シーサート）と呼ばれる専門チームの構築（図 4-6）、インシデント対応方針・計画の作成、手順の作成や、必要な技能の一覧化、対応要員の技能育成や訓練などがあります。専門家を組織内部で確保するのが難しい場合は、事前に外部委託先を洗い出し、何を委託するか整理しておく必要があります。

そして、インシデント発生時に証拠収集ができるように、ログ検索基盤の設置などを行うのもこの段階です。ネットワーク機器のパケットやコンピュータのログは、インシデントが発生する前に設定しておかなければ取得できません。

情報共有

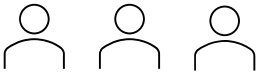


担当者	役割
社外PoC	自組織外連絡
社内PoC	自組織内連絡、IT部門調整
リーガルアドバイザー	法的アドバイス
ノーティフィケーション担当	自組織内調整、情報発信

自組織内教育

担当者	役割
教育担当	教育・啓発

情報収集・分析



担当者	役割
リサーチャー	情報収集
キュレーター	情報分析
脆弱性診断士	脆弱性の診断・評価
セルフアセスメント担当	自組織の現状分析
ソリューションアナリスト	セキュリティ戦略
リサーチャー	情報収集

インシデント対応

担当者	役割
コマンダー	CSIRT全体統括
インシデントマネージャー	インシデント管理
インシデントハンドラー	インシデント処理
インベスティゲーター	調査・捜査
トリアージ担当	優先順位選定
フォレンジック担当	鑑識

図 4-6　CSIRT のメンバーとその役割

②検知、分析

インシデントの発生は、侵入検知システム（IDS）やファイアウォールによるアラート、ユーザーや組織外部からの通報などにより知ることになります。CSIRT 要員は、そうした情報の事実確認を行い、影響範囲を特定して対応の優先順位を決定します。

③封じ込め、根絶、復旧

インシデントに対する措置の第一歩は、被害が広がらないよう、封じ込めを行うことです。コンピュータをネットワークから隔離したり、悪性な IP アドレスとの通信をファイア

ウォールで遮断するなど、インシデントの種類に応じて封じ込め策を講じます。

続いて、インシデントの原因を突き止め、問題を除去するとともに、システムやネットワークに必要な追加対策を行い、問題の根絶を図ります。

そして、状況を監視しつつ、システムや業務を通常状態へと復旧します。

④インシデント後の対応

①～③の対応が一段落した後に大切なのは、インシデントで得た教訓を次の機会に生かすことです。一般的にはインシデント報告書の作成や、反省会などが行われます。

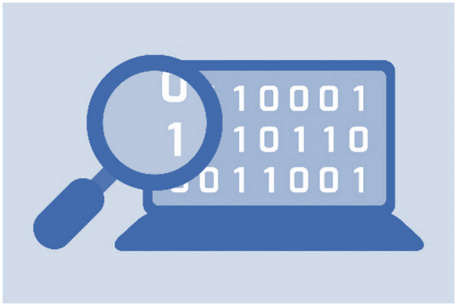
また、収集した証拠の保管にも注意します。外部からの要請がある場合を除いて、証拠保管期間を定め、期限が過ぎたら確実に廃棄することが求められます。

4-3　デジタルフォレンジックのプロセス

デジタルフォレンジックとは

フォレンジックは直訳では「法廷の」「法医学の」といった意味であり、事実を確定するための法的証拠の適正な取り扱いに関する科学的手法・手順を指します。

デジタルフォレンジックとは、主にサイバー犯罪に関する証拠の収集・調査などを行う分野です。事件が発生した場合、鑑識課が衣服の繊維や指紋など現場に残る証拠を保全・採取し、専門的な分析を行いますが、デジタルフォレンジックは、その対象が電磁的記録になります。



電磁的記録：電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるもの（刑法 7 条の 2）

電磁的記録は 0 と 1 で表現されるため、人間が内容を理解できるよう変換する必要があり、デジタルフォレンジックでは証拠を分析する技術が求められます。また、電磁的記録は複製や消去、改変が容易であることから、証拠を保全する手順や復元する技術も重要とされます。

デジタルフォレンジックの経緯

1980 年代以降、コンピュータの普及に伴い、法執行機関はサイバー犯罪への対応が求められるようになり、例えば FBI（米国連邦捜査局）は 1984 年にサイバー犯罪に関する部門を設置しています（図 4-7）。日本では、1996 年に電磁的記録解析が警察庁情報管理課の管掌とされ、 2000 年には警察庁情報通信局に技術対策課が発足され、デジタルフォレンジックの技術が広く用いられるようになりました。

サイバー犯罪は国境を越えて行われる性質を持つことから、国際協力体制を構築するべく、2004 年にはサイバー犯罪条約が発効されました。この条約は、サイバー犯罪を禁じる立法措置を締約国に義務付け、フォレンジックに関連する証拠収集などの捜査手続きや国際協力を規定するものです。日本は 2011 年に刑法改正により法整備上の条件が整えられ、2012 年に批准しています。

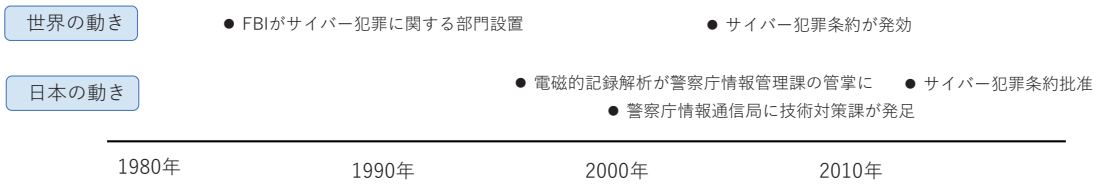


図 4-7　デジタルフォレンジックの経緯

デジタル化の進展により、刑事事件だけでなく民事事件においてもデジタルフォレンジックの重要性は高まっています。知的財産を巡る訴訟や労働紛争、取引紛争などの民事訴訟など、民事裁判では文書の成立が真正であることを証明しなければなりませんが、改変の容易な電磁的記録が裁判において証拠として採用されるためには、デジタルフォレンジックの技術に基づく適切な対応が必要となります。

また、企業などの組織が従業員の不正行為（横領やハラスメント等）の疑いを調査する必要があるとき、真偽を確かめたり、証拠を見つけるためにもデジタルフォレンジックの技術が使用されるようになっています。従業員が使用している PC の HD や SSD を複製して分析したり、アプリケーションサーバーやメールサーバー、ファイルサーバーなどのログを調査したりします。

フォレンジックプロセス

デジタルフォレンジックは、訴訟手続きや内部懲戒処分のための証拠収集、マルウェアインシデントや運用上の特別な問題への対応など、さまざまな状況で必要とされる可能性があります。しかし、いずれにしても基本的なプロセスは①収集、②検査、③分析、④報告の 4 フェーズが共通しています（NIST「SP 800-86：インシデント対応へのフォレンジック技

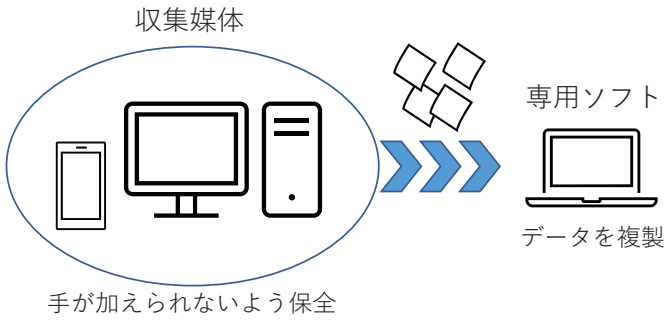
法の統合に関するガイド」より)。

①収集

データの完全性を保護する手続きに従いながら、関連するデータを識別し、ラベル付けし、記録し、ソースの候補から取得します。

まずは、インシデントの種類に応じて、データ収集対象の媒体を特定します。例えば、マルウェアによる攻撃を受けた場合はメモリ情報、内部犯行者によるデータの持ち出しの場合は PC のストレージや USB デバイスなどがソースとなります。

データ収集対象となる媒体は、変更が加えられないように保全し、データの取得を図ります。例えばハードディスクが対象の場合、専用ソフトで原本となるハードディスクの内容全体を複製し、イメージファイルとして保存しておきます。複製物を作成するのは、②検査や③分析の過程で証拠が破壊されるためです。複製元と複製先のイメージファイルのハッシュ値を比較し、一致することを確認して、複製が正確であることを確認します。



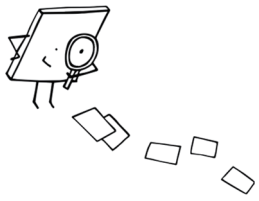
ただし、ストレージの大容量化に伴い、ディスク全体を複製するには時間がかかりすぎ、迅速なインシデント対応が困難なケースも生じています。こうした場合には、一部のデータだけを取得して分析を進めるファストフォレンジックの手法が有効です。

また、インシデント対応における封じ込めのフェーズでは、稼働中のシステムに変更が加わるため、デジタルフォレンジックのプロセスが阻害される可能性があります。コンピュータがワームに感染した場合、メモリ情報を取得してから LAN ケーブルを抜線することがフォレンジック上は望ましいですが、インシデント対応の原則としては直ちに抜線する必要があります。

②検査

データの完全性を保護しながら、収集したデータを自動的手法及び手動的手法を組み合わせてフォレンジック的に処理することにより、特に注目に値するデータを見定めて抽出します。

収集したデータはすべてが証拠としての重要性を持つわけではありません。また、データが暗号化されていたり、削除されていたりする場合には、復元する必要があります。データの種類に応じてツールや技法を用いて抽出した、分析に有用な情報をアーティファクトといいます。



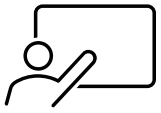
アーティファクト
・不正プログラム等のさまざまな処理により必然的にディスクやメモリ上に残る痕跡
・科学的手法により抽出し、分析に用いる

③分析

法的に正当と認められる手法及び技法を使って検査結果を分析することにより、収集と検査を行う原因となった疑問を解決するのに役立つ情報を導き出します。

フォレンジック担当は、「②検査」で得たアーティファクトを時系列に並べ、インシデントを解明するべく仮説検証や事実検証を行います。検証作業により、インシデントの全体像など、明らかにしたい事柄に対して妥当な事実を推論したり、得られたアーティファクトでは想定が裏付けられないことを確かめます。

④報告



分析結果を報告します。ここには、使用された措置の記述、ツールや手続きの選択方法の説明、実行する必要があるそのほかの措置の特定、フォレンジックプロセスのポリシー、手続き、ツールなどの改善事項の提示といった内容も含まれます。

報告書を作成するに当たっては、受領者のニーズを理解し、それに合った内容にする必要があります。受領者が経営陣であれば、技術的事項は簡潔にとどめ、事業への影響を中心に報告します。一方、IT 部門やセキュリティ部門の場合は、今後の再発防止策や追加的な監視項目が検討できるようにします。

インシデントが進行している間は時間もなく報告が省略されがちになりますが、作業記録を欠かさないようにし、以降のセキュリティ体制改善に資するようにします。

なお、各フェーズにおいては、一連の手順が適正であり証拠の連続性が担保されていることを示すために、媒体情報を記録しておくことも大切です。これは保管の連続性（CoC：Chain of Custody）といわれるもので、例えばハードディスクであれば、製造業者や型番、シリアルナンバーなどを記録し、また、受け渡し履歴を追跡できるように、作業日時、作業場所、作業従事者を記録します。これにより証拠が変更や改ざんなどされていないことを保証し、裁判における証拠としての信頼性確保を図ります。

CSIRT によるインシデント対応

不正アクセスやマルウェアなどのサイバー攻撃によるインシデントに対し、デジタルフォレンジックの観点から対応するための体制として増加しているのが、4-2 でも紹介した CSIRT の設置です。

インシデント対応に関わる CSIRT のメンバーとその業務内容は図 4-8 のとおりです。

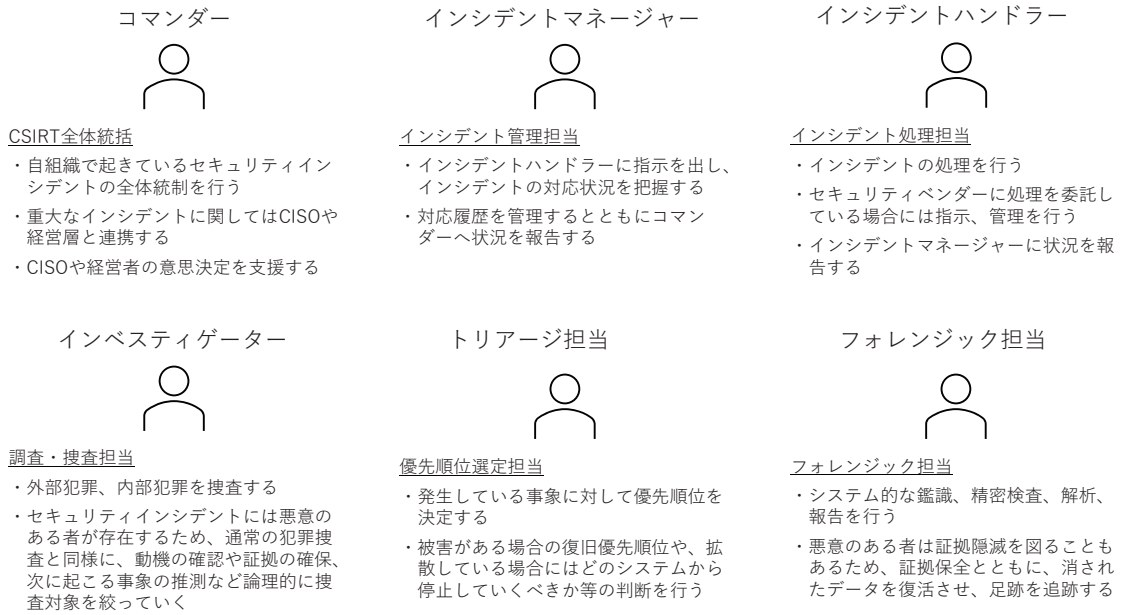


図 4-8　インシデント対応に関わる CSIRT のメンバーと業務内容

フォレンジック担当は、システム的な鑑識、精密検査、解析、報告を行います。証拠が隠滅されることもあるため、証拠保全とともに、消されたデータを復活させ、足跡を追跡することも要求されます。担当者に必要な知識として、OS やコマンド、システムファイル、プログラミング言語の構造とロジックに関する知識、脆弱性診断に関する知識が前提とされています。

インシデント対応はデジタルフォレンジックとは本来の目的が異なるため、必ずしもその両立がスムーズに行えるとは限りません。

デジタルフォレンジックをインシデント対応に統合させる上で、CSIRT 要員にはバランス感覚が必要となります。サイバー攻撃に対応する場合、攻撃者の身元や意図の特定よりも、組織への影響範囲の調査や課題是正に資するための分析を優先するといった行動原理が求められます。

なお、インシデント対応とデジタルフォレンジックを統括する概念として、DFIR（Digital

Forensics and Incident Response、ディーファー）という用語が用いられています。

4-4　デジタルフォレンジックの実践

収集の具体的手法

4-3 で述べたフォレンジックプロセス「①収集」では、ネットワークから収集する場合と、個別のコンピュータから収集する場合に大きく分けられます。

■ネットワークから収集する場合

標的型攻撃を受けた場合は複数のコンピュータが侵害されている可能性が高いため、組織におけるインシデント対応では、まずはどのコンピュータを調査するか決めるところから始める必要があります。

それにはネットワーク上のデータを分析して対象範囲を絞り込むことが有効です。そこで、ネットワークトラフィックに関するデータを収集できるように、事前にネットワーク機器やセキュリティ機器、サーバーや端末からログを取れるように設定しておきます。

その際、個々のログを都度まとめるのでは効率が悪く、また、機器が侵害を受けてログ自体が消去される可能性があることから、ログは個別に保管せず、1 か所に集約することが有効です。さらに、インデックスを付けて検索できるよう、Splunk（商用製品）や Elastic Stack（オープンソース）といったログ検索基盤を利用することも考慮すべきでしょう。

■コンピュータから収集する場合

コンピュータからデータを収集するに当たり原則となるのが、データが失われやすい証拠から優先的に取得するということです。データの失われやすさを揮発性といいますが、レジスタやキャッシュは揮発性が高く（失われやすい）、アーカイブ用メディアは揮発性が低い（失われにくい）という特徴を持ちます（図 4-9）。

メモリはディスクよりも揮発性が高いため、優先してデータを取得することが大切です。

揮発性	
高 （失われやすい）	レジスタ　キャッシュ
	ルーティングテーブル　ARPキャッシュ　プロセステーブル　カーネル統計　メモリ
	テンポラリファイルシステム
	ディスク
	当該システムと関連する遠隔ロギングと監視データ
	物理的設定　ネットワークトポロジー
低 （失われにくい）	アーカイブ用メディア

図 4-9　データの揮発性の高低

＜メモリ情報の取得＞

調査対象となるコンピュータでプログラムを実行させ、コンピュータに搭載されているメモリの全領域をダンプします。そして得られたメモリのダンプイメージに対し、専用ツールを使うなどして分析を行います。

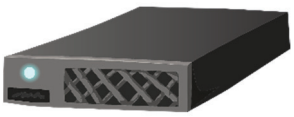
ダンプイメージの取得には、Magnet RAM Capture や FTK Imager Lite、WinPmem などのツールを利用することができます。

メモリ情報の出力は、常にスムーズにできるとも限らず、途中でシステムが不安定になり、再起動せざるを得ない場合もあります。また、ツールの相性もあるため、組織で利用している PC と相性がいいツールを事前に探しておくことも大切です。

＜ディスク情報の取得＞

ハードディスクや SSD のデータは、保全のためにシャットダウン状態にした上でディスク全体を複製することで取得します。4-3 でも述べたように、複製元と複製先とでハッシュ値を比較し、同一性を検証することが必要です。

裁判で証拠として提出する場合、複製元と同じハードディスクを用いて物理コピーを行うのが望ましく、そのための専用の複製装置が販売されています。



また、ディスク全体が暗号化されている場合は、取得したイメージが暗号化されているため分析に用いることができません。このようなケースでは、起動した PC にツールをインストールして、ディスクイメージを取得します。PC の改変を伴うため、作業者が不適切な行為を行っていないことを証明するために、ビデオカメラでの撮影などによる作業記録や作業への第三者の立ち合いが必要となります。

■ファストフォレンジック

インシデントに迅速に対応するため、ファストフォレンジックを行うケースでは、メモリダンプに加え、ストレージ格納データのうち重要と考えられるものだけを抽出して分析します。ファストフォレンジックのためのデータ取得には、CDIR Collector などのツールを使用することができます。

検査・分析の具体的手法

4-3 の「②検査」「③分析」では、大きく分けて「ファイルシステム」「オペレーティングシステム」「ネットワークトラフィック」「アプリケーション」の 4 種類のデータが利用されます。作業に必要なツールがセットになった SIFT Workstation や CAINE Linux などの Linux ベースの専用ディストリビューションが多く利用されています。

【ファイルシステムのデータ】

データファイルとは、論理的に 1 つのエンティティとしてまとめられ、ファイル名などによって参照される情報の集まりです。ファイルには、文書、画像、ビデオ、アプリケーションなど、数多くの種類があります。

こうしたファイルを格納して操作できるようにするため、OS は媒体をパーティションに区切り、各パーティションを 4KB ごとの小さな単位で区画分けして、それぞれの区画にどのようなデータが記録されているのかをメタデータとして別途管理しています。この仕組みをファイルシステムといいます（図 4-10）。コンピュータ媒体のフォレンジック処理が成功するかは、その媒体に存在するファイルを収集、検査、分析する能力にかかっています。

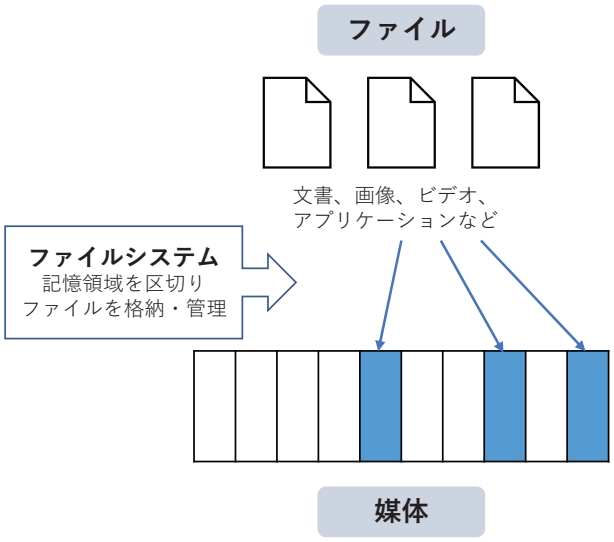


図 4-10　ファイルシステムのイメージ

攻撃者は、クラウドストレージに盗み出したデータをアップロードしてハードディスクのファイルを削除したり、分析を混乱させるため作成時刻を改ざんしたファイルを故意に残したりします。そうした攻撃者のファイル操作に的確に対応するためには、フォレンジック担当には、正確なファイルシステムの知識に基づき、得られたアーティファクトをさまざまな角度から分析し、矛盾がないかを確認することが求められます。

■データの復元

削除されたデータについては、復元する必要があります。その方法には、メタデータからの復元とカービングによる復元の 2 種類があります。

メタデータからの復元は、ファイルシステムの管理情報から復元する方法です。例えば、Windows の標準ファイルシステムである NTFS のメタデータはマスターファイルテーブル（MFT）と呼ばれ、ボリュームごとに$MFT という名前のファイルで格納されています。ファイルを削除した場合でも MFT の管理情報が変更されるだけで、実データはそのまま残されているため、MFT の管理情報を参照すれば、実データが上書きされていない限り、削除されたファイルを復元することができます。

カービングによる復元は、データが持つ特徴的な痕跡をとらえて復元する方法で、論理フォーマットなどによって MFT そのものが失われた場合に用いられます。これは、それぞれのファイルの種類に応じた特徴的なバイト列（ファイルシグネチャ）を利用するもので、例えば JPEG は「FF D8」という 16 進数(HEX)の列で始まり、「FF D9」で終わります。このファイルシグネチャにより、未使用領域に残るデータから当該ファイルを探し出します。

■タイムライン解析

タイムライン解析とはファイルシステムやログファイルなどのタイムスタンプ情報をもとに、発生した事象を時系列に並べ因果関係や原因を調査する手法のことです。ファイルシステムのタイムスタンプは MAC times と呼ばれ、タイムライン解析の根幹となります。それぞれ、更新日時、アクセス日時、メタデータ変更日時を指します（表 4-2）。NTFS の場合は MACE times といい、C は作成日時、E はエントリ更新日時＝メタデータ変更日時を指します（表 4-3）。

表 4-2　MAC times

Modified Time	Accessed Time	Changed Time
更新日時	アクセス日時	メタデータ変更日時

表 4-3 MACE times

Modified Time	**A**ccessed Time	**C**reation Time	**E**ntry Modified Time
更新日時	アクセス日時	作成日時	エントリ更新日時 （メタデータ変更日時）

ファイルに名前変更、移動、複製などの操作を加えた場合のタイムスタンプの挙動は、OS のバージョンごとに少しずつ異なります。例えば、Windows 7 以降の OS ではアクセス日時の更新がデフォルトで無効化されているため、最終アクセス日時以後にアクセスされている可能性もあります。

分析の例として、NTFS の時刻分解能は 100 ナノ秒であるため、タイムスタンプが秒以下の単位まで 0 でそろっている場合には、改ざんが疑われます。また、MFT には 2 種類（$STANDARD_INFORMATION 及び$FILENAME）のタイムスタンプ属性がありますが、改ざんツールによっては前者しか変更できないものもあり、両者の差異を比較して改ざんを発見できることがあります。

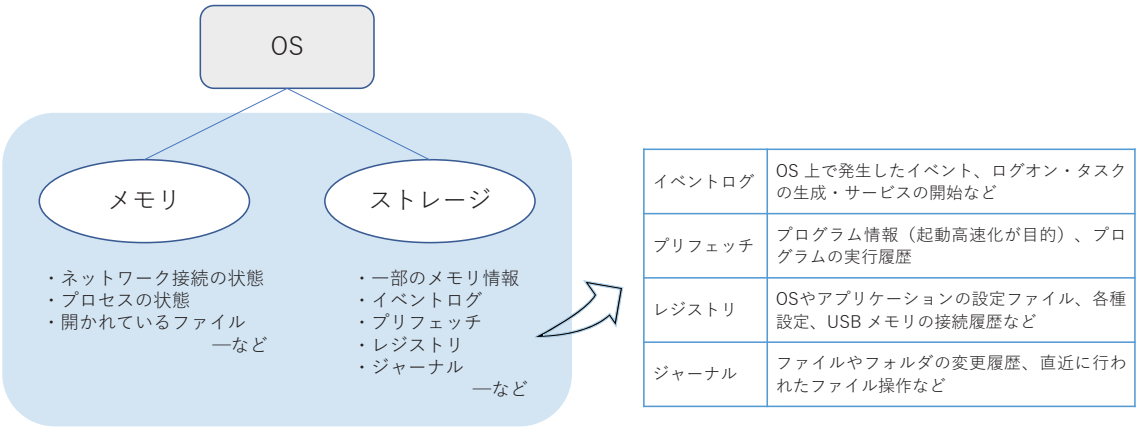
ファイルシステムの分析ツールとしては、EnCase Forensic、Forensic Toolkit（FTK）、X-Ways Forensics などの商用製品、Autopsy といったオープンソース製品を利用することができます。

【オペレーティングシステムのデータ】

オペレーティングシステム（OS）は、コンピュータ上で実行され、ほかのプログラムを実行するためのソフトウェアプラットフォームを提供するプログラムです。OS はまた、ユーザーが入力したコマンドの処理、ディスプレイへの出力の送信、データの格納や取り出しに必要な記憶装置とのやりとり、プリンターやモデムなどの周辺装置の制御を担当します。ワークステーションまたはサーバー用の一般的な OS には、Windows、Linux、UNIX、Mac OS などがあり、ネットワーク機器（ルーターなど）には Cisco の IOS など独自の OS を持つものもあります。

OS のデータは、「メモリ」と「ストレージ」の 2 種類に分けられます。メモリは揮発性データであり、ネットワーク接続の状態やプロセスの状態、開かれているファイルといった情報を得ることができます（図 4-11）。OS のあらゆる活動はメモリを通じて実行されるため、マルウェア感染に伴うインシデントの調査には、メモリの分析が欠かせません。メモリの分析には、Volatility Framework などのツールが用いられます。

また、非揮発性のストレージからは一部のメモリ情報 （仮想メモリ、ハイバネーションファイル）が得られるほか、イベントログやプリフェッチ、レジストリ、ジャーナルなどを得ることができます。



イベントログ	OS 上で発生したイベント、ログオン・タスクの生成・サービスの開始など
プリフェッチ	プログラム情報（起動高速化が目的）、プログラムの実行履歴
レジストリ	OSやアプリケーションの設定ファイル、各種設定、USB メモリの接続履歴など
ジャーナル	ファイルやフォルダの変更履歴、直近に行われたファイル操作など

図 4-11　メモリとストレージから分かること

標的型攻撃による水平展開の痕跡を発見するためには、リモートアクセスされた記録（RDP など）、リモート実行された記録（PsExec、WMI、PowerShell など）をイベントログやレジストリなどから取得し、分析につなげます。

【ネットワークトラフィックのデータ】

ネットワークトラフィックのデータを利用することで、ネットワークベースの攻撃や不適切なネットワーク使用を再構成して分析したり、さまざまな運用上の問題をトラブルシューティングしたりすることができます。ネットワークトラフィックとは、ホスト間の有線または無線ネットワークを介して伝送されるコンピュータネットワーク通信を指し、そのデータ利用のためには TCP/IP の基本知識が必須となります。

ネットワークトラフィックに関するデータには、パケット、フロー、ログがあります。

■パケット

パケットとは、ネットワークを流れるデータ（フレーム）のことで、パケットを取得することをパケットキャプチャと呼びます（図 4-12）。

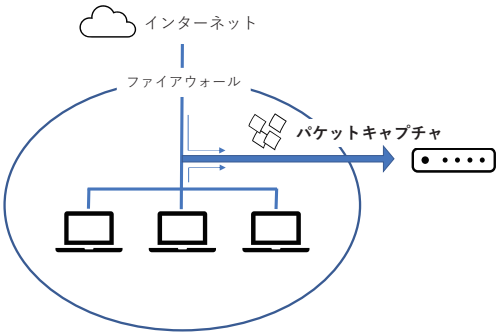


図 4-12　パケットキャプチャのイメージ

パケットキャプチャはコンピュータ上でも実施できますが、上位のネットワーク機器でポートを複製する設定を行えば、そのネットワークで流れるすべてのパケットを取得することができます。

パケットキャプチャで得られるデータには、ファイルの編集ログや外部端末との接続履歴、インターネットの閲覧履歴などがあり、さまざまな分析が可能です。SSL/TLS により暗号化された通信に対し、専用の復号装置によるパケットキャプチャを行うことも可能になっています。

分析ツールには、オープンソースの WireShark がよく用いられています。大規模な分析では、RSA Netwitness Suite や Symantec Security Analytics Platform のような商用製品のほか、オープンソース Moloch も利用することができます。

■フロー

すべてのネットワークにおいてパケットを記録しようとするのは、例えば 1Gbps の通信を 1 日間記録するのに 10TB 以上のストレージ容量が必要になるため、あまり現実的ではありません。

そこで、インターネットとの境界のみ領域を絞ってパケットキャプチャを行い、組織内部のネットワークではパケットのかわりにフロー情報を分析するといった方法がとられます。フロー情報は「送信元 IP アドレス」「宛先 IP アドレス」「送信元ポート番号」「宛先ポート番号」「プロトコル」の 5 種類のデータで構成されます。

フロー情報にはコンテンツに該当する部分が含まれませんが、通常と異なるパターンを示す通信を把握したり、標的型攻撃などのインシデント発生時に侵害範囲を特定するためには十分に有用です。

■ログ

ログは意図的に残された記録であり、分析は複数のログを組み合わせて行われます。例えばプロキシサーバーのログに不審な URL へのアクセス記録がある場合、どの PC から通信したかを知るには、MAC アドレスが必要となります。そこで、プロキシサーバーに記録された送信元 IP をキーにして、DHCP サーバーのログを確認します。また、送信元 IP をキーにして認証サーバーのログを見ることで、誰が通信したのかを知ることができます。

ログの分析では、記録された時刻を考慮することが大切です。ログを記録する機器の時刻の正確性を保つため、それぞれの機器が NTP サーバーによって時刻同期されていることを普段から確認しておきます。また、JST（日本標準時）と UTC（協定世界時）の違いにも注意が必要です。

【アプリケーションのデータ】

OS はアプリケーションを実行するために必要であり、ネットワークはアプリケーションデータをシステム間で送信するために必要であり、ファイルはアプリケーションデータ、構成設定、およびログを保存するために必要です。従って、アプリケーションに関連するデータはファイル、OS、ネットワークのそれぞれに存在します。

アプリケーションに関連するファイル分析は、サイバー攻撃の場合も内部犯行の場合でも行われます。例えば電子メールの記録を利用することで、サイバー攻撃であればマルウェアと接触した経緯を、内部犯行であれば動機の解明や共謀者の有無を確認できることが期待されます。

一般的なクライアント端末において分析対象となるアプリケーションのデータとしては、図 4-13 のデータが挙げられます。

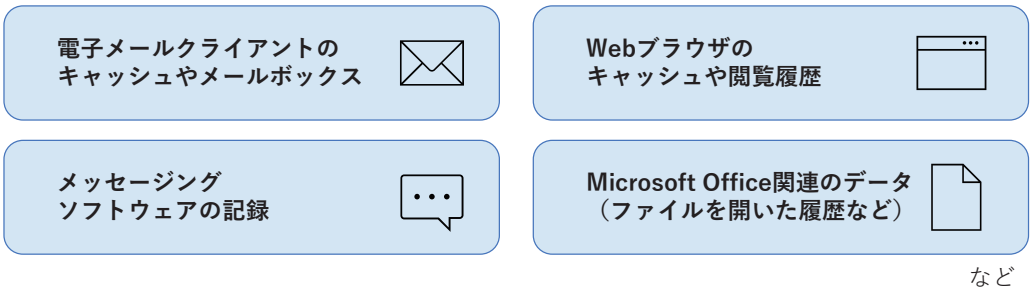
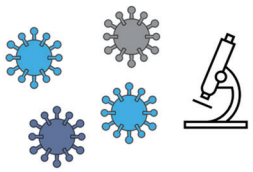


図 4-13　分析対象となるアプリケーションデータ

サーバー機器にインストールされたアプリケーションは、ログ機能を備えていることが一般的で、HTTP サーバーからアクセスログやエラーログ、アプリケーションサーバーから認証ログ、ファイルサーバーからアクセスログなどを取得・分析することができます。

マルウェアの解析

フォレンジック担当にはマルウェアを解析する役割も求められます。解析には、難易度が低い順から表層解析、動的解析、静的解析の 3 種類に分けられ、必要に応じて解析手法を組み合わせます。



■表層解析

ファイルのハッシュ値や含まれる文字列などに基づいて情報を収集し、そのファイルがマルウェアか否か、マルウェアの場合にはどのような特徴を有するのかを調査します。

■動的解析

サンドボックスでマルウェアを実行し、動作を分析します。通信やレジストリへの書き込みを分析することで、追加的な対策に必要な情報を得ることができます。

動的解析は比較的手軽に行うことができますが、サンドボックス環境では動作しないように作られているマルウェアもあります。

■静的解析

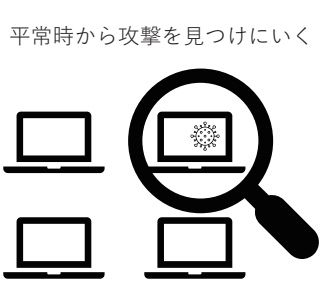
デバッガや逆アセンブラツールを利用して、実際にコードを分析します。マルウェアの詳細な機能を解明することができますが、アセンブラを理解する必要があるなど、要求される知識水準が高く、解析に時間がかかります。

脅威ハンティング

脅威ハンティングとは、従来の情報セキュリティ対策では検知が難しい脅威に対し、それらのリスクが存在することを前提としてネットワーク内部のログやプロセスを解析し、不審な振る舞い（インシデントの兆候）を検出することでサイバー攻撃を防ぐ方法です。

高度な攻撃者は、対象組織のセキュリティ体制を十分に調査した上で、セキュリティを回避して攻撃を行います。そのため、組織が侵入を受けてからインシデントを認知するまでには時間差があり、標的型攻撃を認知するのには約 100 日間かかるともいわれています。

この時間差を埋めるのが、脅威ハンティングの目的です。従来はインシデント発生時に受動的に対応していたのに対し、脅威ハンティングでは平常時（と認識されている時点）からインシデントを積極的に見つけにいきます。



脅威ハンティングを行うには、ログ検索基盤が整備されていることが必要です。また、EDR 製品などを用いて端末情報をリアルタイムで取得できるようにすることも求められます。

令和２年度「専修学校による地域産業中核的人材養成事業」
Society5.0に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

セキュアなシステム運用教材

令和３年２月

一般社団法人全国専門学校情報教育協会
〒164-0003　東京都中野区東中野1-57-8　辻沢ビル3F
電話：03-5332-5081　FAX　03-5332-5083