徹底攻略

情報セキュリティマネジメント過去問題集

平成28[2016年]年度秋期

五十嵐 聡［著］

電子版無料ダウンロード！※

2大特典

スマホで学べる単語帳アプリ
「でる語句200」付き

「攻略のカギ」付き
過去問と模擬問題で
合格力UP!

「情報セキュリティマネジメント重要用語334選」付き！

過去問 1 回分＋模擬問題 3 回分

インプレス

目　次

購入者限定特典のご案内

●スマホで学べる単語帳アプリ「でる語句200」のダウンロード

巻頭記事「情報セキュリティマネジメント重要用語」から、暗記に適した用語をピックアップしてまとめた、いつでもどこでも暗記できる単語帳アプリ「でる語句200」を無料でダウンロードいただけます。手順については，258ページをご参照ください。

●電子版の無料ダウンロード

本文全文の電子版（PDFファイル。印刷不可）を無料でダウンロードいただけます。答案用紙のPDF（印刷可能）をダウンロードいただけます。

IPAが第1回試験開始前に、参考として公開したサンプル問題（午前・午後）の解答・解説PDFをダウンロードいただけます。

PDFのダウンロードについては，以下のURLをご確認ください。

ダウンロードURL：
http://book.impress.co.jp/books/1115101152

※画面の指示に従って操作してください。
※ダウンロードには，無料の読者会員サービス「CLUB Impress」への登録が必要となります。

※本特典のご利用は，書籍をご購入いただいた方に限ります。

情報セキュリティマネジメント

攻略ガイド

情報セキュリティマネジメント試験の概要

情報セキュリティマネジメント試験は，経済産業省が創設し，平成28年4月からIPA（独立行政法人情報処理推進機構）が実施している国家資格です。近年増加しているサイバー攻撃や内部不正などの脅威に対抗するために，情報セキュリティ人材の育成と確保を目的としている試験で，4月（春期）と10月（秋期）の年2回実施されます。

この試験は，一般企業において必要とされる「情報セキュリティマネジメント人材」を対象としています。

◆情報セキュリティマネジメント人材

「情報セキュリティマネジメント人材とは、部門の情報資産に対して適切な情報管理を実施し、組織の情報セキュリティポリシーやルールを部門内のメンバーに周知して順守を促すなど、部門内で情報セキュリティマネジメントを推進する人材です。具体的には、部門内で不審メールを受信した場合には注意喚起を行い、速やかにCISO・情報システム部門に報告する、またサイバー攻撃の被害やインシデントが発生した場合には、企業内のインシデント対策チームであるCSIRTと連携し、情報共有を行うことで被害を最小限に抑える役割などを担うと考えられます」（http://www.ipa.go.jp/about/press/20151016.html より引用）

情報セキュリティマネジメント試験では，情報セキュリティマネジメント人材がもつべき知識やスキルを測ることを目的としています。特に，情報セキュリティマネジメントの計画，運用，評価，改善を通して，自らが所属する組織の情報セキュリティ管理体制を確立し，安全性を向上させるために必要な知識が重要視されます。

◆午前試験の概要

	試験時間	出題数（解答数）	出題形式	基準点
午前試験	90分 （9:30～12:00）	50問 （50問）	多岐選択式 （四肢択一）	60点 （100点満点）

午前試験では四肢択一（4つの選択肢から1つを選ぶ）の問題が50問出題されます。

ポイント

・90分の試験時間中に全問解答するには，1問に約1分48秒しか費やせません。後述するテクニックを用いて，解答時間を削減する必要があります。

◆午後試験の概要

	試験時間	出題数（解答数）	出題形式	基準点
午後試験	90分 （12:30～14:00）	3問 （3問）	多岐選択式	60点 （100点満点）

午後試験では，8～10ページの長文の問題が3問出題されます。全問必須です。

ポイント

・90分の試験時間中に全問解答するには，1問に30分しか費やせません。
・全問必須なので，得意分野の問題をあらかじめ特定しておき，試験が開始したらその問題だけを解くといったことができません。情報セキュリティ全般に関する知識と応用力が要求されます。

◆主な出題範囲（IPA公表　情報セキュリティマネジメント試験要綱　重点分野のみ抜粋）

大分類	中分類	小分類	主な知識項目
技術要素（セキュリティ）	セキュリティ	情報セキュリティ	機密性・完全性・可用性，不正プログラム，暗号方式，ディジタル署名，公開鍵基盤など
		情報セキュリティ管理	情報資産とリスクの概要，リスク対応，情報セキュリティポリシなど
		セキュリティ技術評価	PCI DSS，CVSSなど
		情報セキュリティ対策	情報セキュリティ対策，不正プログラム対策，不正アクセス対策，セキュリティ製品・サービスなど
		セキュリティ実装技術	セキュアプロトコル，ネットワークセキュリティなど
企業と法務（法務）	法務	知的財産権	著作権法，不正競争防止法など
		セキュリティ関連法規	不正アクセス禁止法，個人情報保護法など
		労働関連・取引関連法規	労働基準法，守秘義務など
		その他の法律・ガイドライン・技術者倫理	コンプライアンス，情報倫理など
		標準化関連	JIS，ISO，IEEEなど

（https://www.jitec.ipa.go.jp/1_13download/youkou_ver2_0_sg_bassui.pdf を参考に作成）

◆平成28年度春期試験における出題内容（午前）

大分類	中分類	小分類	出題内容
技術要素（セキュリティ）	セキュリティ	情報セキュリティ	不正のトライアングル，2要素認証，APT，クロスサイトスクリプティング，クリックジャッキング，ハッシュ関数，認証局，ドライブバイダウンロード，パスワードリスト攻撃，バックドア，AES，ポートスキャン，公開鍵暗号方式
		情報セキュリティ管理	CSIRT，クリアデスク，情報セキュリティ監査，JIS Q 27001-リスク受容，情報セキュリティ方針，特権的アクセス権

大分類	中分類	小分類	出題内容
技術要素（セキュリティ）	セキュリティ	情報セキュリティ対策	情報漏えい対策，組織における内部不正防止ガイドライン，アクセスログの取扱い，BYOD，IDS，WAF，マルウェア対策，内部不正の防止，ディジタルフォレンジックス，磁気ディスクの廃棄，HDDパスワード
企業と法務（法務）	法務	知的財産権	不正競争防止法
		セキュリティ関連法規	個人情報保護法，電子計算機損壊等業務妨害，特定電子メール送信適正化法
		労働関連・取引関連法規	請負契約
		その他の法律・ガイドライン・技術者倫理	OECDプライバシーガイドライン
コンピュータシステム	システム構成要素	システムの評価指標	レスポンスタイム
技術要素（セキュリティ以外）	データベース	データベース応用	データウェアハウス
	ネットワーク	データ通信と制御	ルータ
		ネットワーク応用	プロキシサーバ
サービスマネジメント	サービスマネジメント	サービスマネジメント	SLA
		サービスマネジメントプロセス	RTO
	システム監査	システム監査	スプレッドシートの利用に係るコントロール，従業員の守秘義務，情報セキュリティ監査基準
システム戦略	システム戦略	ソリューションビジネス	SaaS
	システム企画	調達計画・実施	RFP
企業と法務（法務以外）	企業活動	経営・組織論	事業継続計画，コーポレートガバナンス
		OR・IE	積上げ棒グラフ

◆平成28年度春期試験における出題内容（午後）

問題	内容
問1	標的型攻撃メール，マルウェア，ウイルスメール，ソーシャルエンジニアリング
問2	業務委託，利用者ID，ロール
問3	URLフィルタリング，リモート接続，アクセスログ，最小権限の原則，チェックリスト，CSA

現時点で本試験はまだ1回しか実施されていないので，今後どの内容が多く出題されるかは不明です。しかし，情報処理試験では過去に出題された問題や用語が繰り返し出題される可能性が高いので，今回出題された内容が再度出題されることを見越しておきましょう。

試験の位置付け・時間・出題形式

◆位置付け：基本情報技術者試験と同じレベル２の試験
全問マークシート（多岐選択式）午前・午後とも全問必須

ITを利活用する者	
ITの安全な利活用を推進する者	
ITの安全な利活用を推進するための基本的知識・技能	情報セキュリティマネジメント試験（SG）
全ての社会人	
ITを利活用するための共通的基礎知識	ITパスポート試験（IP）

情報処理技術者（ベンダ側／ユーザ側）										
高度な知識・技能	ITストラテジスト試験（ST）	システムアーキテクト試験（SA）	プロジェクトマネージャ試験（PM）	ネットワークスペシャリスト試験（NW）	データベーススペシャリスト試験（DB）	エンベデッドシステムスペシャリスト試験（ES）	情報セキュリティスペシャリスト試験（SC）	ITサービスマネージャ試験（SM）	システム監査技術者試験（AU）
応用的知識・技能	応用情報技術者試験（AP）									
基本的知識・技能	基本情報技術者試験（FE）									

（https://www.jitec.ipa.go.jp/1_13download/youkou_ver2_0_sg_bassui.pdf より）

※情報セキュリティマネジメント試験の詳細はhttps://www.jitec.ipa.go.jp/1_04hanni_sukiru/_index_hanni_skill.htmlを参考にしてください

おすすめ学習法・試験のテクニック

◆過去問題の反復練習が合格のカギ

情報セキュリティマネジメント試験に限らず，情報処理技術者試験では過去問題の学習を何度も行う反復練習が効果的です。

◆午前試験では過去問題が出題される

午前試験では過去問題が高い頻度で出題されます。平成28年度春期では，基本情報技術者試験から5問（10%），応用情報技術者試験から8問（16%），情報セキュリティスペシャリスト試験などから4問（8%），計17問（約34%）が出題されています。過去の各試験のセキュリティ関連の過去問を解いておくことで，本試験で見覚えのある問題が出題される可能性が高くなります。

◆攻略のカギ

自分の苦手な分野などを洗い出すために，解説欄の「攻略のカギ」を利用してください。午前の「攻略のカギ」には問題に関連する用語や要点，計算に関しては必要な計算式を，午後の「攻略のカギ」には問題を解くためのヒントを掲載しています。

◆間違えた問題は必ず復習する

間違えた問題は必ず復習して，次に解答するときは正解できるようにします。本書掲載の問題にはチェックボックスが付いています。チェックボックスに×印などをつけておき，解説をよく読んで間違えた理由を理解します。

- **解答群が全て単語の午前問題や，解答群から語句を選ぶ形式の午後の設問を間違えた場合：**正解の単語を記憶する。また，他の問題で正解以外の単語が出題されることもあるので，正解以外の単語もおろそかにせず，本書解説などで調べておくこと
- **解答群が文章の午前問題を間違えた場合：**正解の選択肢で説明されている内容と，出題されたテーマの単語とを結び付けて記憶する

◆繰り返し問題を解く

時間の許す限り，何回も繰り返して問題を解き，重要な語句や内容を覚えましょう。前述したように，午前試験では過去問題が出題される頻度が高いので，過去問題を何度も読むことで，問題（図表も含む）と正解のイメージをできるだけ多く頭に入れていくことが必要です。

午後試験では，問題文を全て熟読する必要はありません。問題文を流し読みして概要をつかんだら，先に設問に目を通し，各設問に対応する問題文の一部だけを参照することで，大部分の設問の正解そのものまたはそのヒントを得ることができます。

◆時間を計る

午前試験及び午後試験の時間は限られています。本試験で時間が足りなくなり，解ける問題に解答できなかったということがないように，実際の試験を受けていると想定して，時間を正確に測って問題を解く練習をしてみましょう。

情報セキュリティマネジメント重要用語334選

情報セキュリティマネジメント分野の問題を解く上で必要な関連用語を集めました。これらの用語を押さえつつ問題を解くことで，より実力アップが図れます。

アルファベット

あ

か

さ

た

な

は

ま

ら

情報セキュリティ

情報のCIA

情報セキュリティを維持するために必要となる要素です。JIS Q 27001（ISO/IEC 27001）などの主要な情報セキュリティの規格では，次の三つの要素を情報のCIA（または情報セキュリティの３要素）としています。

要素	概要
機密性（Confidentiality）	不特定多数からデータにアクセスされないようにして，適切な権限をもつ者だけがアクセスできるようにする性質
完全性（Integrity）	データの内容が不正に削除されたり改ざんされたりしないようにして，内容を矛盾なく保つようにする性質
可用性（Availability）	適切な権限をもつ者が，必要なときにシステムやデータを利用できるようにする性質

真正性

情報セキュリティに関連する要素で，情報やその利用者が本物である（なりすましではない）という性質です。

責任追跡性

情報セキュリティに関連する要素で，事故や事件が発生したとき，情報システムに残されたログなどを参照して，その実行者を特定できる性質です。

否認防止

情報セキュリティに関連する要素で，処理を実行した人が，後からそれを否定できないようにする性質です。

信頼性

情報セキュリティに関連する要素で，情報システム及びその構成要素が意図したとおりに稼働している性質です。

脅威

情報システムに対して悪い影響を与える要因のことです。JIS Q 27001で定義されています。

物理的脅威

脅威の一種で，重要な設備が格納されている建物に不正侵入され，物理的な破壊や盗難などの被害を受けることです。

技術的脅威

脅威の一種で，マルウェアなどに感染させられたり，サーバに不正アクセスされたりすることで，機密情報の漏えいや改ざんなどの被害を受けることです。

人的脅威

脅威の一種で，自社の従業員が意図的に情報を持ち出したり，または偶発的に操作ミスをしたりすることで，機密情報を盗んだり外部に漏えいさせたりすることです。

情報漏えい

自社が管理していた機密情報や顧客の個人情報などを，外部に漏えいさせることです。

ソーシャルエンジニアリング

不正なユーザが本人になりすまして，パスワードなどのセキュリティに関する情報をセキュリティ管理者などから不正に聞き出す行為です。

マルウェア

コンピュータに悪影響を与えることを目的として作成された不正なソフトウェアです。

ウイルス

マルウェアの一種で，攻撃対象のコンピュータ内のファイルなどに感染し，特定の日時になるまで潜伏した後，発病して不正な動作をするという特徴をもちます。

マクロウイルス

マクロとは，ワープロソフトや表計算ソフトなどの機能の一つで，一連の操作を呼び出して実行できるように，簡易なプログラムのような形式でまとめたものです。マクロは，ワープロソフトのファイルなどと一緒に保存されます。
マクロウイルスは，マクロの仕組みを悪用したウイルスで，

ワープロソフトの文書ファイルや表計算ソフトのスプレッドシートなどに，通常のマクロと同様の形式で保存されます。マクロウイルスが感染した文書ファイルなどを開くと，ワープロソフトのテンプレート（文書の定型）などにマクロウイルスが感染します。その後に，別の文書ファイルを開いたり新規作成したりすると，そのファイルにもマクロウイルスが感染します。

ポリモーフィック型ウイルス

感染するごとにランダムに変化させた暗号化鍵を用いて，ウイルスのコードを暗号化することで自身の内容を常に変化させて，同一のパターンで検知されないようにするウイルスのことです。

ワーム

不正侵入や感染などの行為を単独で実行できるタイプのマルウェアです。ワームは，OSやアプリケーションソフトの脆弱性を突くなどの方法により，パソコンやサーバなどに侵入して，当該コンピュータ上で不正な行為を実行したり，同じネットワーク内の他のコンピュータに自身のコピーを送りつけて，さらに感染範囲を広げたりすることを行います。

ボット

マルウェアの一種で，攻撃対象のコンピュータに潜伏し，攻撃者が用意した外部のマルウェアから指令を受け取ると，情報を漏えいさせるなどの特定の行動をします。

スパムメール

広告宣伝などを目的として，受信者の意向に関係なく，不特定多数の利用者に無差別に送信されるメールのことです。

ファイル共有ソフト

インターネット上で，利用者間でファイルを共有するためのソフトウェアです。一部のマルウェアは，ファイル共有ソフトの脆弱性を突いて感染しようとするため，ファイル共有ソフトを不用意に使用すると，マルウェアに感染する危険性が高まります。

トロイの木馬

正当なプログラムを装ってインストールされ，秘密裏に不正行為を働くマルウェアのことです。

スパイウェア

通常の無害なソフトウェアに見せかけてコンピュータ内にインストールされるマルウェアです。インストールされたスパイウェアは，秘密裏にコンピュータ内の個人情報やパスワードなどの情報を特定の外部サーバに送付したり，Web閲覧時にユーザの意図しない広告を勝手に表示したりするなどの処理を行います。

ランサムウェア

マルウェアの一種で，コンピュータに感染した上で内部のファイルを勝手に暗号化し，利用者を脅迫して元に戻すための代金を払わせようとします。

キーロガー

コンピュータへのキー入力を記録し，その内容を外部に送信するソフトウェアです。キーロガーは，キーボードから入力された他人のパスワードを盗むために悪用されることがあります。

ルートキット

OSなどに秘密裏に組み込まれたバックドアなどの不正なプログラムを，隠蔽するための機能をまとめたツールのことです。

バックドア

攻撃者が，マルウェアに感染したPCに今後もアクセスできるようにするために，PC内に秘密裏に作られる攻撃用の侵入経路のことです。

脆弱性

情報システムや情報資産に存在する，脅威が顕在化する確率のことです。JIS Q 27001で定義されています。

バグ

プログラムやシステムに内在している誤りのことです。

セキュリティホール

コンピュータやシステムに内在している，情報セキュリティ上の弱点のことです。マルウェアは，セキュリティホールを突くことでコンピュータなどへの攻撃を実行します。

サイバー攻撃

インターネットを経由して，インフラや政府機関などのシステム及びサーバなどを攻撃し，改ざんや破壊などの被害を与えることで，社会を混乱させようとする行為です。

ハックティヴィズム

情報技術を利用し，宗教的または政治的な目標を達成するという目的をもった人，または組織のことです。

サイバーテロ

サイバー攻撃と同様に，インフラや政府機関などのシステム及びサーバなどを攻撃し，社会を混乱させようとする行為です。

ブルートフォース

考えられる全ての種類の暗号化鍵またはパスワードを総当りで作成して，それをもって暗号解読を試みたり，他人になりすましたりすることです。

辞書攻撃

辞書に掲載されている一般的な名詞などの単語(“apple”など)，及び単語の組合せなどの文字列をパスワードとして入力していき，標的ユーザのパスワードを推定しようとする攻撃方法です。

パスワードリスト攻撃

Webサービスや組織などから流出した，利用者IDとパスワードの組のリストを入手して，それを用いて他のWebサービスに不正ログインしようとする攻撃方法です。

SQLインジェクション

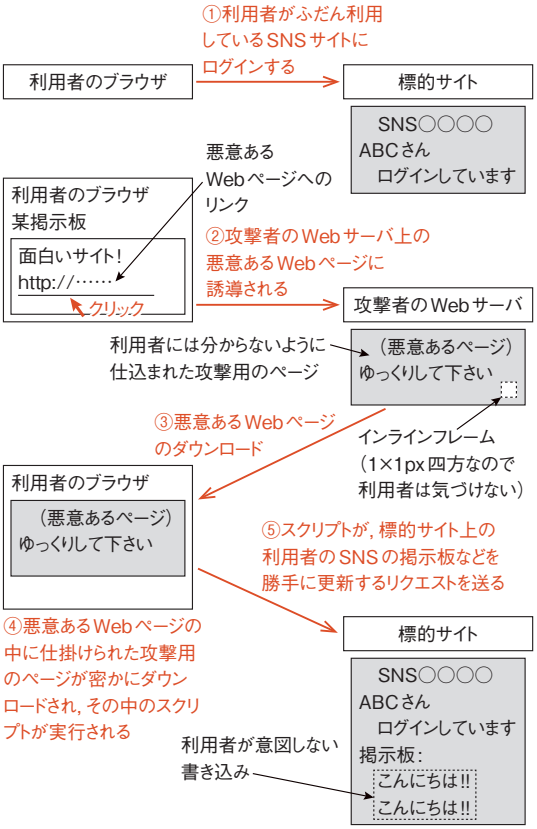
Webページ上の入力フォームに不正な文字列を入力し，入力フォームから受け取った値をもとにして生成されたSQL文を不正なものにして，Webアプリケーションを誤動作させたり，データベースの内容を削除したりする攻撃方法です。

クロスサイトスクリプティング

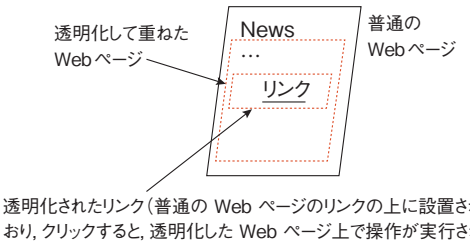
悪意を持ったスクリプト(JavaScriptなど)を利用者のブラウザに送り込み，利用者を標的サイトに誘導することで，標的サイト上で当該スクリプトを動作させ，利用者の個人情報を盗み取る攻撃方法です。

CSRF(クロスサイトリクエストフォージェリ)

悪意あるスクリプトを含んだ攻撃用のページを密かにダウンロードして，そのスクリプトを自動的に実行するWebページを閲覧させるなどの方法で，利用者がログインしている状態の標的サイトに対して別のWebサイト上のページから不正なリクエストを送り，意図しない操作を行わせる攻撃方法です。



クリックジャッキング



HTMLのiframeタグなどを用いることで，Webページの中に別のWebページを埋め込むことができます。当該レイヤを透明にすることで，一見問題がないように見えるWebページの上層に，別のWebサイトのWebページを透明化して密かに埋め込むことが可能になります。

このようなWebページ上で操作を行うと，利用者が気付かないうちに，別のWebサイトのWebページ上で不正な操作が行われます。このような攻撃をクリックジャッキングといいます。

ドライブバイダウンロード

攻撃用のWebページを閲覧した際に，利用者に気づかれることなく，秘密裏にマルウェアをダウンロードさせ，PCに感染させる攻撃のことです。

ディレクトリトラバーサル

ファイル名などをパラメタとして受け取るフォームの入力欄に，“../passwd”などといった不正なファイル名や相対パス名を入力することで，Webサーバに格納されている重要なファイルを表示させたり，削除させたりする攻撃手法のことです。

中間者攻撃

利用者Aと利用者Bがインターネット上で通信を行っているときに，攻撃者がAとB間に割り込んで，公開鍵などをすりかえるなどの方法で，やり取りされているデータを横取りしたり盗聴・改ざんしたりする攻撃手法のことです。

第三者中継

自社のメールサーバのセキュリティ対策が甘いため，外部から第三者宛てに送信するメールが転送可能な状態になっていることです。この状態では，悪意のユーザが発信したスパムメールなどの転送の肩代わりをさせられ，自社が不正行為に加担させられてしまいます。

IPスプーフィング

送信元IPアドレスを攻撃対象の組織内のIPアドレスに偽装したIPパケットを当該組織のネットワークに送付し，誤動作を起こさせたり，不正侵入を試みたりする攻撃手法です。

キャッシュポイズニング

DNSサーバなどに対して，ドメイン名などを改ざんした不正な情報を送り込み，そのサーバを参照したPCの利用者を，本来のWebサーバとは異なるWebサーバに誘導する攻撃手法のことです。

セッションハイジャック

Webサーバとブラウザの間で行われる継続的なやり取り（セッション）を維持するためのセッションIDを攻撃者が推測して，正当なブラウザになりすましてWebサーバに送り込み，ブラウザとWebサーバ間のセッションを乗っ取る攻撃方法のことです。

リプレイ攻撃

盗聴者が，正当な利用者のログインシーケンス（ログインするときに送受信されるパケットのやり取り）をそのまま記録してサーバに送信し，利用者になりすまそうとする攻撃方法のことです。

DoS攻撃

Denial of Service攻撃。DNSサーバなどを踏み台にして問合せを大量に行い，攻撃対象のサービスを妨害する攻撃手法のことです。

DDoS攻撃

Distributed Denial of Service攻撃。多数のホストにボットを感染させ，特定の日時になったときに全てのボットから攻撃対象のサーバに一斉に攻撃を仕掛けることで，攻撃対象のサービスを妨害する攻撃手法のことです。

メールボム

同じ宛先メールアドレスに大量の電子メールを送信することで，受信者の業務を妨害するなど，各種の被害を与えることです。

フィッシング

サイトの偽装や偽造電子メールの使用によって，ユーザを騙して個人情報などを不正に入手したりする行為です。具体的な方法は次のとおりです。

①標的のサイトのWebページによく似せたWebページを作成する。

②当該サイトの利用者に対して“本人確認の再確認が必要なのでこのURLにアクセスして入力してください”という主旨の，偽装した電子メールを送る。

③そのメールに騙された利用者が，URLに示されたページにアクセスしてIDやパスワードを入力すると，入力したデータが詐取される。

標的型攻撃

特定の企業または個人を対象にした攻撃手法の総称です。対象に深く関連する人や組織（上司，同僚，得意先など）を送信元に偽装して，業務に関係する表題や内容の電子メールを送り付け，添付ファイルを開くよう促すなどの方法で，マルウェアに感染させようとします。

APT

Advanced Persistent Threats。攻撃者が特定の組織を標的として，複数の手法を組み合わせて執拗に攻撃を繰り返す手法です。

水飲み場型攻撃

RSAセキュリティ社が2012年に公表した攻撃手法で，次のような手順をとります。

①攻撃者は，攻撃対象の利用者がWebを利用する様子

を観察し，頻繁にアクセスするWebサイトを特定する。
②攻撃者は，攻撃対象の利用者が頻繁にアクセスするWebサイトを改ざんして，攻撃用のコードを埋め込み，その利用者がアクセスしたときだけマルウェアをダウンロードするように設定する。
③攻撃対象の利用者が②のWebサイトにアクセスすると，攻撃が行われてマルウェアがダウンロードされる。

水飲み場型攻撃という名前は，攻撃者をライオン，攻撃対象の利用者が頻繁にアクセスするWebサイトを動物の水飲み場に例え，ライオンが水飲み場の近くで動物を待ち伏せすることから来ています。

ゼロデイ攻撃

新種のウイルスなど，対策が存在しなかったり，または公表されていなかったりするマルウェアによって行われる攻撃のことです。

RLO

文字の表示順を変えるUnicodeの制御文字を利用することで，ファイル名の拡張子を偽装することです。RLOを利用して，実行ファイル(拡張子がexe)を圧縮ファイル(拡張子がzip)などに見せかけて，マルウェアを実行させようとする手口が存在します。

例

dummydatapiz.exe ← マルウェアのファイル名

この位置に，以降の文字の表示順を「左から右」から「右から左」に変えるUnicode制御文字を入れる

dummydataexe.zip ← というファイル名で表示される（実体はマルウェア）

サイドチャネル攻撃

暗号化装置のソフトウェアやハードウェアをさまざまな方法で解析して，その消費電流などの物理量やエラーメッセージなどから暗号の解読を試みたり，機密情報を得たりする攻撃のことです。

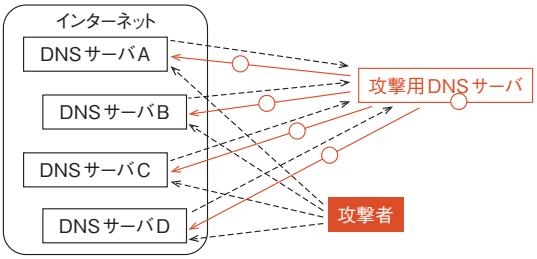
タイミング攻撃

サイドチャネル攻撃の一種で，複数の平文データを暗号化装置に与えて，それらを暗号化する処理時間の差異を観察することで，暗号化装置の演算アルゴリズムを推測しようとすることです。

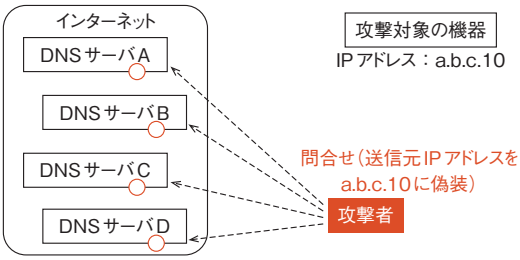
DNS amp攻撃

次のような攻撃手法のことです。

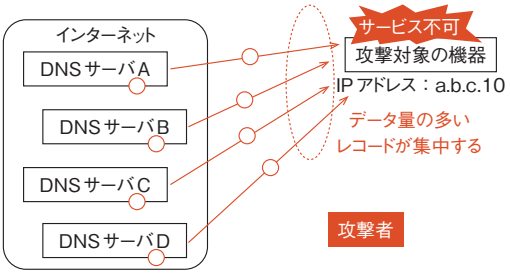
①攻撃者は，攻撃用DNSサーバにデータ量の多いレコード(以下，攻撃用レコードという)を記録しておき，インターネット上の多数のDNSサーバに，攻撃用レコードへの問合せを行う。インターネット上の各DNSサーバは，攻撃用DNSサーバに攻撃用レコードを問い合わせて，攻撃用DNSサーバから受け取った攻撃用レコードをキャッシュする。



②攻撃者は，①の全てのDNSサーバに対して，送信元IPアドレスを攻撃対象の機器のアドレスに偽造して，攻撃用レコードに関する問合せを行う。



③①の全てのDNSサーバは，攻撃対象の機器のIPアドレス宛てに攻撃用レコードを返答する。インターネット上の多数のDNSサーバから，攻撃対象の機器に対してデータ量の多いレコードが大量に送信されてくるので，攻撃対象の機器の負荷が増大し，サービスができなくなる。



smurf攻撃

ICMPの応答パケットを大量に発生させ，攻撃対象の通信負荷を大きくさせてサービスの停止などを狙う攻撃手法

のことです。攻撃対象のIPアドレスを送信元IPアドレスとして偽装したICMPの要求パケットを，攻撃対象の所属するネットワークの全コンピュータ宛てに，ブロードキャストで送信します。ICMP要求を受信した各コンピュータは，ICMPの応答パケットを攻撃対象に一斉に返送するので，通信負荷が大きくなってしまいます。

EDoS攻撃

Economic Denial of Service攻撃。経済的な損失を狙ったサービス妨害攻撃です。ファイル共有などの機能を提供しているクラウドサービスの中には，利用者から事業者のネットワークに対して与えられたトラフィックの量に応じて課金する，従量制の料金体系をとっているものもあります。そのようなサービスに対して，利用者のネットワークを経由して多数のアクセスを与えてリソースを大量に消費させることで，多額の料金を利用者に請求させます。

ICMP flood攻撃

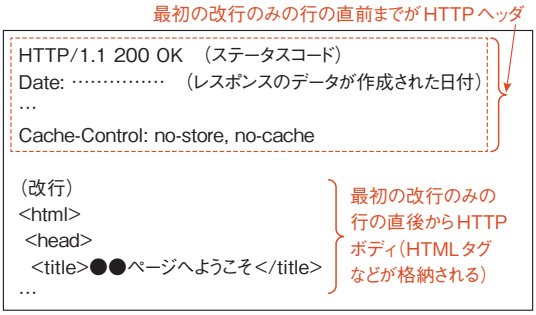
pingコマンドを用いて，攻撃対象のサーバに対して大量の要求パケットを同時に発信し，当該サーバに至るまでの回線を過負荷にしてアクセスを妨害する攻撃手法です。

テンペスト攻撃

コンピュータやディスプレイなどから発せられる電磁波中の電磁的な信号を，測定用の機器を用いて観測し収集することで，操作中の画面の内容を再現したり，暗号化鍵や暗号化アルゴリズムなどの情報を不正に入手したりする攻撃方法のことです。

HTTPヘッダインジェクション

Webサーバは，次のようなテキスト形式の応答をブラウザに返します。



HTTPヘッダインジェクションは，HTTPヘッダとHTTPボディが改行で区切られているというHTTPの仕組みを悪用して，HTTPレスポンスの中に不正なヘッダを仕込んだり，不正なHTMLタグなどを挿入したりする攻撃手法です。

OSコマンドインジェクション

Webページ上の入力欄にOSのコマンドライン（コマンドプロンプト）上で有効なコマンドを入力させ，Webサーバ上で不正な命令を実行させる攻撃方法です。例えば，UNIXやLinuxをOSとしているWebサーバで公開しているWebページの入力欄に，“……（正当なデータ）; rm …”のような文字列を入力すると，正当なデータの処理の後に，“rm …”という，Webサーバ上のファイルを削除する命令が実行されてしまいます。

バージョンロールバック攻撃

SSL／TLSを実装する一部のソフトウェアでは，ブラウザとWebサーバとの間で使用する暗号化通信方式を決定するための通信（ハンドシェイクプロトコル）を行ったときに，通信経路に介在する攻撃者がその通信内容を改ざんして，暗号化通信方式の新しいバージョン（TLS1.0）ではなく古いバージョン（SSL2.0など）を使用するように強制することができます。SSL2.0などで使用する暗号化方式には暗号化鍵が短いなどの問題があるため，攻撃者はブラウザとWebサーバとの間で送受信される暗号化通信のパケットの内容を解読することができます。このような攻撃手法を，バージョンロールバック攻撃といいます。

SEOポイズニング

SEO（Search Engine Optimization，検索エンジン最適化）とは，自社のWebページのURLが検索サイトの検索結果の上位に表示されるように，Webページのタイトルや内容を改善することです。

SEOポイズニングとは，Web検索サイトの順位付けアルゴリズムを悪用して，キーワードで検索した結果の上位に悪意のあるサイトを表示させるために，そのサイトの内容を構成する手法のことです。

ポートスキャン

サーバなどの脆弱性を検出するときに用いる手法です。対象ホストに対して，宛先ポート番号を順次増加させながらアクセスしていき，対象ホストから正常な応答が返ってきたときに，そのポート番号のサービスが稼働している（対象ポートが開いている）と判断します。

迷惑メール

次のようなメールのことです。

①広告宣伝などを目的として，受信者の意向に関係なく，不特定多数の利用者に無差別に送信されるメール（スパムメール）。

②フィッシングなどの攻撃または詐欺を目的として，不特定多数の利用者に送信されるメール。

CRYPTREC暗号リスト

CRYPTREC（Cryptography Research and Evaluation Committees）は，「電子政府推奨暗号の安全性を評価・監視し，暗号技術の適切な実装法・運用法を調査・検討するプロジェクト」のことです。CRYPTRECは，電子政府推奨暗号リストというリストを公開しています。このリストには，公的な機関によって客観的に評価され，安全性や実装性に優れると判断された暗号方式（DSA，AESなど）やハッシュ関数（SHA-1など）が掲載されています。

暗号化技術

特定のアルゴリズムに従って，データの置換・並べ替えなどの操作を行うことで，データの内容を解読不能にすることを暗号化といいます。暗号化されたデータを元の内容に戻すことを復号といいます。暗号化や復号を行うために用いられる情報を鍵といいます。鍵の作成や暗号化・復号の方法に関する技術を，暗号化技術といいます。

共通鍵暗号方式

暗号化と復号に同じ鍵（共通鍵）を用いる方式です。この方式では，ネットワークにN人の利用者がいるとき，ネットワーク全体では（N－1）＋（N－2）＋……＋2＋1＝N（N－1）／2個の共通鍵が必要になります。

DES（Data Encryption Standard）

1977年に公表された共通鍵暗号方式で，56ビットの鍵を用いて暗号化を行います。現在は，鍵長が短く暗号を復号されやすい点で問題があり，後続の暗号方式であるAESを利用することが勧められています。

AES（Advanced Encryption Standard）

2001年に公表された共通鍵暗号方式で，128ビット，192ビットまたは256ビットの鍵を用いて暗号化を行います。

公開鍵暗号方式

一人の利用者に対してペア（対）で生成される「公開鍵」と「秘密鍵」の二つの鍵を，それぞれ暗号化や復号に用いる方式です。「公開鍵」はネットワーク上に公開して誰でも利用可能とし，「秘密鍵」は鍵の所有者が専有し，厳重に保管して他人には知られないようにします。利用者Aが利用者Bにデータを送るとき，AはBの公開鍵でデータを暗号化して送信し，それを受信したBは自身の秘密鍵でデータを復号します。

この方式では，ネットワークにN人の利用者がいるとき，ネットワーク全体では2N個の鍵が必要になります。

RSA

素因数分解の計算の困難さを利用した公開鍵暗号方式。鍵長は1,024ビット，2,048ビットまたは4,096ビット。

S/MIME

電子メールの暗号化方式規格。RSA securityにより提案され，IETFにより標準化されています。

- メッセージ本文を暗号化するために，共通鍵暗号方式の共通鍵を用いる。
- 共通鍵を送信者と受信者との間で安全に受け渡すことと，電子メールの改ざんを検出することを目的として，公開鍵暗号方式によるディジタル署名の仕組みを用いている。

PGP

共通鍵暗号技術と公開鍵暗号技術を併用した電子メールの暗号化・復号技術です。

- メッセージ本文を暗号化するために，メール送信の都度ランダムに生成した共通鍵暗号方式の共通鍵を用いる。
- 共通鍵を送信者と受信者との間で安全に受け渡すことを目的として，ディジタル署名の仕組みを用いている。

ハイブリッド暗号

公開鍵暗号方式と共通鍵暗号方式とを組み合わせた暗号方式のことです。公開鍵暗号方式には暗号化・復号に必要な時間が長いという欠点があり，共通鍵暗号方式には鍵の個数が過大になるという欠点があります。データの送信の都度，共通鍵をランダムに生成し，その共通鍵を公開鍵暗号方式によって安全に相手に送信してから，データを共通鍵で暗号化して相手に送信することがハイブリッド暗号の例です。

ハッシュ関数

任意の長さのデータを入力すると，固定長のハッシュ値（メッセージダイジェストともいう）を出力する関数です。

【特徴】

- 出力されたハッシュ値から入力データの内容を推定（復元）することは困難。
- 入力データがわずかでも異なれば，ハッシュ値は著しく異なるものになる。

● 入力データの長さが異なっていても，ハッシュ値は同じ長さになる。

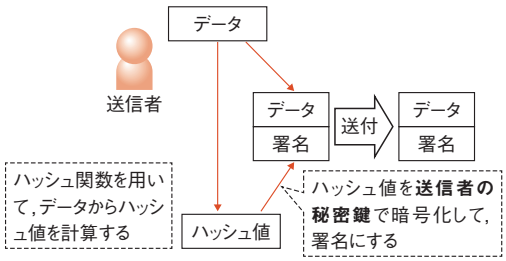
危殆化

安全でない状態になること，または安全が脅かされる状態になることです。暗号アルゴリズムの危殆化とは，パソコンなどの処理速度の向上によって暗号鍵の推定が容易にできるようになり，暗号の安全性が低下することを指します。

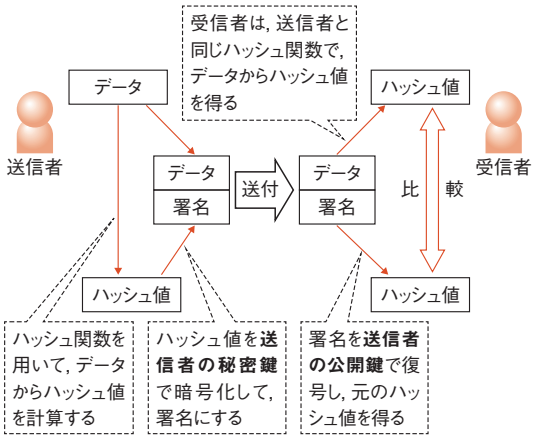
ディジタル署名

通信相手に送付するデータの正当性を送信者が証明するための技術です。ハッシュ関数と公開鍵暗号方式を利用します。

①送信者は，送付データ全体に対してハッシュ関数を用いて，ハッシュ値を求める。さらにそのハッシュ値を**送信者の秘密鍵**で暗号化して送信者の署名を作り，データと一緒に添付して受信者に送付する。



②受信者は，送信者と同じハッシュ関数を用いてデータ本体からハッシュ値を生成する。さらに，送信者の署名を**送信者の公開鍵**で復号して，元のハッシュ値を入手する。この二つのハッシュ値が一致すれば，そのデータは送信者からのものであると確認できる。送信者以外は使用できない**送信者の秘密鍵**で送信者の署名が暗号化されているので，そのデータが確かに送信者本人の管理下にあったと証明できる。



メッセージ認証

ディジタル署名と同様に，通信相手に送付するデータの正当性を送信者が証明するための技術です。共通鍵暗号方式を利用します。

送信者と受信者は同じ共通鍵を共有します。送信者はメッセージから共通鍵を用いてメッセージ認証符号(MAC：Message Authentication Code)を生成し，メッセージとともに送ります。受信者は，受け取ったメッセージからMACを生成して，送られてきたMACと一致することを確認します。

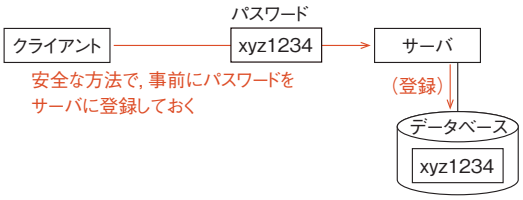
MAC

メッセージ認証において，送信者と受信者が共有する共通鍵を用いてメッセージから生成される認証用の符号です。

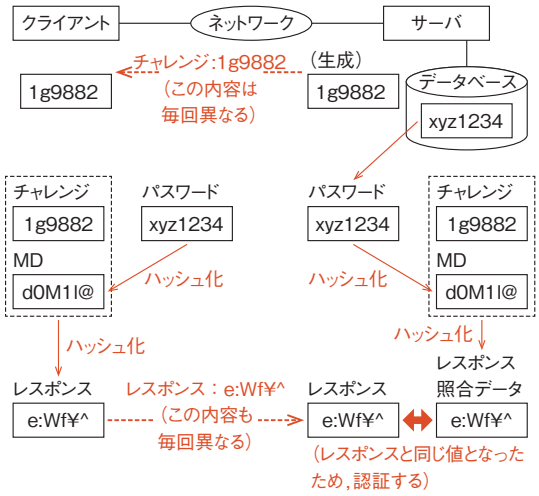
チャレンジレスポンス

次のような方法でクライアント(利用者)を認証する方式です。

①パスワードをサーバ側に事前に登録しておく



②クライアント-サーバ間で認証を行う



注記 MDはメッセージダイジェストの略である
また，利用者IDの送受は省略している

● サーバ(認証する側)は認証時に適当な長さのランダムな内容の電文(チャレンジ)を作成し，クライアント(認証される側)に送信する。

● クライアントは利用者のパスワードのメッセージダイジェストを計算し，送信されたチャレンジと合わせたものから，

さらにメッセージダイジェストを計算してレスポンスを生成する。

- クライアントは，利用者IDとともにレスポンスをサーバに返す。
- サーバは，クライアントから受け取った利用者IDで利用者情報を検索し，取り出したパスワードから計算したメッセージダイジェストとチャレンジとを合わせたものから，メッセージダイジェストを計算してレスポンス照合データを生成する。レスポンス照合データと，クライアントから受信したレスポンスが同じ値になれば，クライアントに送ったチャレンジが正しいパスワードのメッセージダイジェストと合わさって，レスポンスとして返送されてきたことが証明されるため，クライアントを認証する。

タイムスタンプ

文書の存在証明(ある時点よりも前に，文書が確かに存在していたことの証明)と原本保証性(文書が作成された時刻以降にその文書が変更・改ざんされていないこと)を証明するために，信頼できる第三者機関(タイムスタンプ機関)によって作成され，文書に添付されるデータのことです。

利用者認証

IDやパスワードなどを用いて利用者の本人性を証明し，情報システムなどの利用を可能とするための技術です。

多要素認証

複数の認証技術を併用することで，安全性を高める手法です。インターネットバンキングシステムで，パスワードだけではなく，トークンに表示されているワンタイムパスワードも一緒に入力しないと振込をできないようにすることが多要素認証の例です。他人にパスワードを知られても，トークンをもっていなければワンタイムパスワードを入力できないので，不正操作をされる危険性が減ります。

生体認証(バイオメトリクス認証)

生体認証(バイオメトリクス認証)とは，指紋，網膜，顔の形状などの，人間の身体的特徴から個人の識別を行う認証システムのことです。このシステムでは，認証を受けるユーザの指紋の形状などと，登録した本人の指紋の形状などとを比較し，両者の類似の度合いが一定以上であれば，本人と識別します。

公開鍵基盤(PKI)

公開鍵暗号方式及びディジタル署名(電子署名)の仕組みを応用した，公開鍵の正当性を証明し，公開鍵とその利用者を結び付けるための仕組みのことです。ある利用者がネットワーク上に公開している公開鍵が，本当にその利用者が作成して公開しているものか(本人性があるか)を証明するために，ディジタル証明書が用いられます。信頼できる第三者機関(認証局)が利用者の本人確認をして，ディジタル証明書を発行します。

ディジタル証明書

利用者の公開鍵の本人性を証明するためのもので，公開鍵と認証局の署名が含まれます。

- 秘密鍵と公開鍵証明書の発行を受けた利用者は，秘密鍵は公開せず厳重に保管し，公開鍵証明書はネットワーク上に公開する。
- ある利用者の公開鍵証明書を入手した者は，ディジタル署名の手続きと同様に，公開鍵証明書中の認証局の署名を認証局の公開鍵で復号する。
- 復号に成功すれば，その公開鍵証明書の署名は，認証局しか使用できない認証局の秘密鍵で暗号化されていたことが証明できる。すなわち，公開鍵証明書の利用者の本人性を認証局が確認しており，本人性が保証される。

CRL

Certificate Revocation List。有効期限内に無効になった(失効した)公開鍵証明書のシリアル番号を掲載したリストのことです。利用者が規約違反行為をするなどの理由で，ディジタル証明書が無効となることがあります。相手から受け取ったディジタル証明書を使うとき，現在もそれが有効かを判定する必要があります。ディジタル証明書とCRLとを付き合わせることで，有効かどうかを判断できます。

ワンタイムパスワード

毎回異なる認証データを送信することで，なりすましの危険性を低減する認証方式です。ワンタイムパスワードでは，ハッシュ関数の性質を利用して，毎回値が異なる使い捨てのパスワードを認証データとして用いています。

シングルサインオン

一度の利用者認証によって，複数のシステムやOSなどを利用可能とするための技術です。複数のシステムが存在し，それぞれのシステムについて異なったパスワードなどを用いて認証処理を経なければ，どのシステムも利用できないような状況では，「個々のシステムを利用する際に，その都度IDとパスワードの入力を求められる」ことになり，利用者にとって不便です。このような場合には，「一度利

用者認証に成功すれば，その後は全てのシステムやOSなどを，認証なしで利用できるようになる」という形態のシステムを導入することで，問題点を解決できます。

エージェント方式

シングルサインオンを利用する各システムに，エージェントというソフトウェアを組み込む方式です。利用者が一度入力した認証情報は，エージェントソフトによって認証情報を含んだクッキーというデータに加工され，各システム間で自動的に授受されます。その後，各システムにおいてクッキー内の情報が検証され，認証の成否が確認されます。

リバースプロキシ方式

シングルサインオンにおいて，認証用のサーバ(認証サーバ)を設置し，利用者の認証及び各システムへのアクセスを認証サーバに引き受けさせる方式です。認証の成功後は，認証サーバはプロキシ(代理)サーバとして機能し，利用者から各システムに送られた接続要求をいったん受け取ります。その後，認証サーバは利用者の代理として各システムに接続し，接続要求を送ります。そして，各システムから返却された業務処理の応答データなどを，利用者に返します。

CAPTCHA

ゆがんだ文字など，人間なら認識できるがプログラムでは正常に認識できない画像データをサーバから送って，利用者にそれを読み取らせて入力させることによって，アカウントの作成や認証をする方式です。

パスワードリマインダ

利用者がパスワードを忘れた場合に，本人があらかじめ設定していた秘密の質問に答えることで，メールで送付するなどの方法で利用者にパスワードを教えることです。

本人拒否率

生体認証において，正規の利用者本人を他人と誤認識して拒否してしまう確率です。判定しきい値を厳しくするほど上昇します。

他人受入率

生体認証において，他人を正規の利用者と誤認識して受け入れてしまう確率です。判定しきい値を厳しくするほど低下します。

IEEE 802.1X

無線LANの端末を認証するためのプロトコルです。アクセスポイントなどの機器(認証装置またはオーセンティケータ)を経由して，無線LANの端末(クライアント)にインストールされたクライアントプログラム(サプリカント)と認証サーバとの間で認証情報がやり取りされます。認証を行うための利用者情報などは，認証サーバが管理します。

OCSP

Online Certificate Status Protocol。利用者が受け取ったディジタル証明書の失効状態を確認するためのプロトコルです。

ディジタル証明書を受け取った利用者は，それを発行したCA(認証局)にOCSPメッセージを送信し，失効状態の問合せを行います。OCSPメッセージを受信したCAは，ディジタル証明書の失効状態を確認して，利用者に返答します。

FIPS 140-2

Federal Information Processing Standardization 140-2。暗号モジュール(暗号化を行うソフトウェアやハードウェア)に関するセキュリティ要件の仕様を定めている規格のことです。暗号モジュールのセキュリティレベルを，レベル1からレベル4までの4段階のレベルで規定しています。

XMLディジタル署名

XMLディジタル署名は，XML文書の全体または一部の要素に対して付加できるディジタル署名の記述方法や署名アルゴリズムなどを定めたものです。署名を行うXML文書中に署名用の要素(<signature>)を埋め込んだり，署名対象のXML文書と別のファイルに署名用要素を用意したりすることが可能です。

XMLディジタル署名では，従来のディジタル署名方法と比較して，文書(データ)の一部のエレメント(要素)にだけ署名すること

情報セキュリティ管理

情報資産

企業の業務に関連する顧客情報，財務情報，個人情報，製品情報などのデータと，それを保管・管理するためのシステム及び装置などのことです。

JIS Q 31000

リスクマネジメントの原則や組織のリスクマネジメントの取組みを継続的に改善することについて規定している規格です。

残留リスク

JIS Q 31000で定義されている「リスク対応後に残るリスク」のことです。リスク対応においては，発生確率や被害額が大きいリスクに対しては適切な対策を施しますが，発生確率や被害額が非常に小さいリスクは，その被害額よりも対策費用の方が大きくなることがあるので，あえて対策をとらず許容することがあります。このようにして残したリスクが残留リスクです。

リスク

脅威が情報資産の脆弱性につけこみ，情報資産に損失などを与える可能性のことで，JIS Q 27001で定義されています。

リスクマネジメント：リスクの防止，リスク発生時に被害を最小限にするための施策の制定，及びリスク発生により生じる費用に対する積み立てなどの措置を実施するなどの手法によってリスクを管理すること。

リスクアセスメント（リスク評価）：自社の事業に関する固有のリスクの発見と調査を行い，リスクの被害額や発生確率を評価することで，各リスクに適切に対処しようとすること。

リスクマネジメントに関する用語

用語	概要
リスク分析	リスクの発生頻度や被害額などを判定し，重要なリスクと重要でないリスクとを区別し，各リスクについての対処方法などを決定すること。
リスク対策	リスクを防止するための各種手法。 ● **リスクコントロール** リスクが現実のものにならないようにするための，または現実化したリスクによってもたらされる被害を最小限にするための対策。 **リスク回避：**事業から撤退するなどの方法で，リスクそのものを発生させなくすること **リスク低減（軽減）：**リスクの発生確率や損失額を減らすこと ● **リスクファイナンス** リスクが発生することは不可避であると仮定し，リスクによる損失に備えて保険に加入したりすることで，リスクが現実化したときに生じる損失金額を少なくするための対策。 **リスク移転（転嫁）：**保険に加入したり，事業を外部に委託したりすることで，リスク発生時の影響，損失，責任の一部または全部を他者に肩代わりさせること **リスク保有（受容）：**軽微なリスクに対してはあえて対策を行わず，リスクが発生した場合の損失は自社で負担すること

モラルハザード

従業員の倫理観が著しく欠如した状態となり，社内の情報を意図的に漏えいさせるなどの脅威を発生させたり，情報セキュリティに関する業務を怠ったりすることです。

コンティンジェンシープラン

「緊急時対応計画」または「不測事態対応計画」のことで，障害や事故などの事態が発生することを想定し，その対策を事前に定めた計画案のことです。

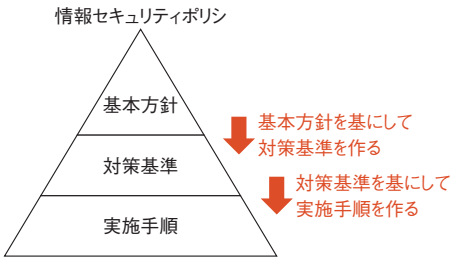
情報セキュリティポリシ

ISMS（情報セキュリティマネジメントシステム）を運用する際に必要となる，組織の情報セキュリティ維持体制を規定し，内外に公表するための文書です。

基本方針：情報セキュリティポリシの構成要素の最上位にある文書で，自社の情報セキュリティに対する基本的な考え方や姿勢を示す。

対策基準：情報セキュリティ対策のために必要な組織の規則と，その適用範囲を示す。

実施手順：対策基準で示した規則を遵守するために必要となる，具体的な業務手順を示す。



プライバシポリシ

企業が個人情報を管理する際に必要となる，個人情報管理体制を規定し，内外に公表するための文書です。

ISMS

Information Security Management System，情報セキュリティマネジメントシステム。情報システム上に存在する情報資産のセキュリティ管理体制のことです。ISMSを確立するとき，情報セキュリティポリシを作成して遵守することが重要となります。

CSIRT

Computer Security Incident Response Team。インターネット上で各種の問題（特に，セキュリティに関する問題＝セキュリティインシデント）が発生していないかを監視し，発生した問題の報告を受け取ってその原因を調査したり，対策を想定したりする組織です。

SOC

Security Operation Center。CSIRTの一部として配置される組織で，ファイアウォールやIDSなどの装置を常時監視し，セキュリティインシデントの発生を検知した場合はCSIRTに報告して対処を依頼します。

ホワイトハッカー

情報セキュリティやコンピュータネットワークに関する高度な知識をもち，それを生かすことで，情報セキュリティの構築や攻撃からの防御など善良な活動をする人のことです。

JVN

Japan Vulnerability Notes。JPCERT/CCとIPAが共同で管理している，脆弱性情報データベースです。

脆弱性情報データベース

ソフトウェアなどに存在する脆弱性の一覧を集約し，公開しているデータベース。

JIS Q 27001

ISMS（情報セキュリティ管理システム）の国際標準規格であるISO/IEC 27001をJIS規格化したものです。情報の機密性，完全性，可用性の維持を管理するシステムが正常に機能しているかを監査対象としています。

JIS Q 27002

組織における情報セキュリティマネジメントの導入，実施，維持及び改善のための指針及び一般的原則を規定しているJIS規格です。

JIS Q 27014

情報セキュリティガバナンスについての概念及び原則に基づくガイダンスを提示しているJIS規格です。国際規格ISO/IEC 27014に対応しています。

セキュリティ技術評価

PCI DSS

Payment Card Industry Data Security Standard。クレジットカード情報などを保護することを目的として，VISAなどのクレジット会社が共同で策定した基準です。

CVSS

Common Vulnerability Scoring System，共通脆弱性評価システム。米国のインフラストラクチャ諮問委員会（NIAC，National Infrastructure Advisory Council）が2004年に原案を作成したシステムで，情報システムの脆弱性を汎用的な基準に基づいて評価するためのものです。

ペネトレーションテスト

対象の情報システムに対して実際に攻撃を行い，侵入を試みることによって，ファイアウォールや公開サーバなどに存在するセキュリティホールや脆弱性，及び設定ミスなどを発見するテスト手法のことです。このテストは，セキュリティのコンサルティングを行っている企業や専門家などに依頼した上で，外部から実施されます。

情報セキュリティ対策

need-to-know

情報セキュリティの維持に関する原則の一つで，情報を知ったり使用したりする必要がある人にだけアクセス権限を与え，そうでない人には与えないようにすることで，情報の漏えいなどを防止することです。

ログ管理

サーバやネットワーク機器などが取得するログ（アクセスしてきた利用者のIDや送信元IPアドレスなどを記録したデータ）を収集・分析して，不正アクセスなどの攻撃の検知に役立てることです。

アクセス制御

システムやデータにアクセスするための権限を利用者に設定し，適切なアクセス権限をもつ者だけアクセスを可能にし，そうでない者はアクセスできないように管理することです。

クラッキング

インターネットなどのネットワークを通じてサーバなどに不正に侵入し，データの改ざんや破壊を行うことです。

侵入検知システム（IDS）

Intrusion Detection System。内部ネットワークに対する外部（インターネットなど）からの攻撃を検知するためのシステムのことです。

NIDS（ネットワーク型IDS）

ネットワーク中のファイアウォールなどの重要な機器内に設定され，ネットワーク上を流れているパケットの内容を解析し，攻撃に使用されるタイプのパケットや，挙動の疑わ

しいパケットを判別し警告を発するタイプのIDSです。

HIDS（ホスト型IDS）

ネットワーク上の個々のコンピュータやサーバに設定され，自機器に到達したパケットの内容を解析し，攻撃に使用されるタイプのパケットを解析し警告するタイプのIDSです。

DMZ

外部に公開するWebサーバやメールサーバなどを組織内のLANに配置すると，外部からのIPパケットが社内LANに入り込むことになり，不正なIPパケットをクライアントPCや非公開のサーバなどに送りつけられるといった問題が起こります。そこで，外部に公開するサーバは，ファイアウォールにて内部LANや外部と分離した特別な領域に配置し，外部から一定の条件でアクセス可能とします。このようにして，公開サーバと非公開サーバ及びクライアントとを分離して配置することによって，セキュリティが向上します。この領域のことを，DMZ（DeMilitarized Zone＝非武装地帯）といいます。

侵入防止システム（IPS）

Intrusion Protection System。IDSの機能をもつとともに，攻撃を検知するとファイアウォールに指示を送信して攻撃元からのアクセスを遮断したり，サーバを停止させたりすることで，攻撃の被害を出さないように防御するシステムのことです。

検疫ネットワーク

マルウェアが社内ネットワークに蔓延することを防ぐために設置されるシステムです。PCが社内ネットワークに接続されたとき，最初は隔離用のLANに接続させてウイルス感染の有無を検査したり，セキュリティパッチが導入されているかを確認したりして，不備がある場合は必要な措置を行い，安全な状態にしてから社内ネットワークに接続させるようにします。

電子透かし

画像データなどに，利用者には分からない形式で著作者（権利者）情報などを埋め込む技術のことです。例えば，画像データの画素の色情報のビットの値を少しずつ正規の値からずらし，差分の値を順番に組み合わせていくと，何らかの情報を表したビット列になっているようにします。

- ステガノグラフィ

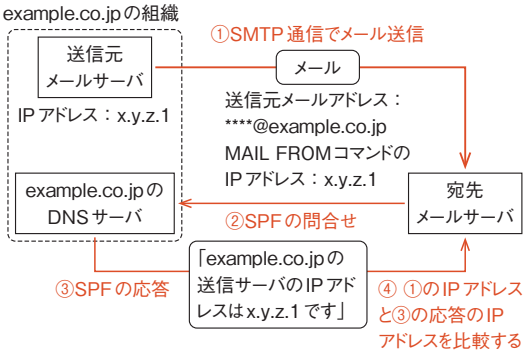
  電子透かし技術を応用し，権利情報の代わりにメッセージを極秘に埋め込む技術のことです。

SPF

Sender Policy Framework。送信ドメイン認証の方法の一つです。送信ドメイン認証とは，メールの送信者の本人性を確認することです。

この方法では，メールサーバの組織が管理しているDNSサーバに，「自組織のメールサーバに対応するIPアドレスはこの値です」という主旨の情報を追記することで，自組織のメールサーバの正しいIPアドレスを他の組織のメールサーバから確認できるようにしています。

例えば，“****@example.co.jp”という送信元メールアドレスのメールを受信した(①)宛先メールサーバは，「example.co.jp」というドメインの組織のDNSサーバに問合せを行って(②)，当該ドメインの送信サーバの情報を入手します(③)。その情報の中に記載された送信サーバのIPアドレスと，SMTP通信中にやり取りされるMAIL FROMコマンド(送信元のメールアドレスやIPアドレスを宛先に伝えるコマンド)で与えられたIPアドレスとを比較して(④)，両者が一致していれば正しいメールサーバからのメールとして受信します。一致していなければ，他のIPアドレスのメールサーバから送信されてきたメールであるため，拒否します。



DNSSEC

DNS Security Extensions。DNSサーバから送信されてきたリソースレコードに公開鍵暗号方式のディジタル署名を付加することで，ドメイン名などの情報が改ざんされた場合に，それを検知できるようにするためのプロトコルです。DNSSECを用いることで，リソースレコードの送信者の正当性やデータの完全性を検証できます。

DKIM

DomainKeys Identified Mail。公開鍵暗号方式を応用して，電子メールの送信者認証及び改ざんの検出を可能とする技術です。送信側メールサーバは電子メールの内容のハッシュ値を求め，それを自ドメインの秘密鍵で暗号化してディジタル署名を作成します。送信側メールサーバは，

作成したディジタル署名を電子メールのヘッダに付与して，受信側メールサーバに送ります。
受信側メールサーバはDNSを検索して，送信側メールサーバが所属するドメインの公開鍵を入手し，それを用いてディジタル署名を復号することで，正当なメールサーバから電子メールが送信されてきたかどうかを検証できます。

OP25B

Outbound Port 25 Blocking。内部ネットワークのコンピュータから，外部のメールサーバのTCPポート番号25番への直接の通信を遮断することで，スパムメールの送信を防ぐことです。メール送信の際の宛先ポート番号が25番（SMTP）となることから，この行為では宛先ポート番号が25番のIPパケットを遮断（ブロック）します。

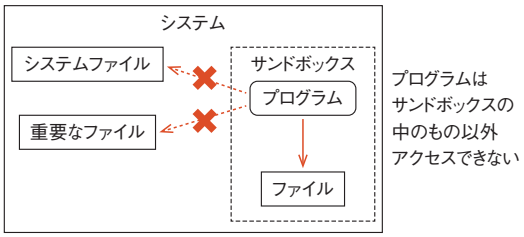
URLフィルタリング

組織内のPCからインターネット上のWebページを閲覧する際に，マルウェアに感染しているなど，不審な内容のWebページのURLをフィルタリング用の装置に登録しておき，当該Webページの閲覧を禁止することです。

コンテンツフィルタ

PCとインターネットとの間でやり取りされるWebページやメールなどの情報（コンテンツ）の内容を監視し，個人情報の流出が疑われるなど，問題がある場合は通信を遮断することです。

サンドボックス



情報セキュリティ対策技術の一つで，プログラムが実行できる機能やアクセスできるリソース（ファイルやハードウェアなど）を制限して，プログラムを動作させることです。プログラムのバグや不正な命令を組み込んだプログラムの実行などによって，システムファイルが破壊されるなどの被害を防ぐために有効です。

SSID

Service Set Identifier。ESS-IDともいいます。無線LANのアクセスポイントを識別するために，各クライアントに設定される文字列のことです。各クライアントは，同じ値のESS-IDをもつアクセスポイントのみに接続することができます。

無線LAN

通信経路として無線電波を用いるLANのことです。PCなどの端末と，アクセスポイントから成ります。アクセスポイントは従来の有線LANのスイッチングハブやルータに該当します。

WEP（Wired Equivalent Privacy）

IEEE 802.11bなどの規格において用いられている無線LANの暗号化技術で，40ビットまたは104ビットの暗号化用の情報と，通信の都度ランダムに生成した24ビットの情報（IV, Initialization Vector）とを組み合わせ，暗号化鍵を生成する方法をとっています。この機能を有効にすることで，無線LANの通信データを暗号化することが可能となります。ただし，この暗号化技術は鍵の長さが短いなどの脆弱性があることが指摘されています。

MACアドレス制限

MACアドレス制限とは，無線LANのセキュリティ機能の一つであり，指定したMACアドレスをもつ機器のみ，無線LANのアクセスポイントに接続することを可能とする機能です。

WPA2

Wi-Fi Protected Access2。鍵のビット数が少ないなどのWEPの脆弱性を改良するために作成された，無線LANの暗号規格やプロトコルなどの総称です。WPA2では，TKIP（Temporal Key Integrity Protocol）という鍵交換プロトコルや，IEEE 802.1Xという認証のためのプロトコルを利用しています。IEEE 802.1Xでは，複数のアクセスポイントが，1台のRADIUSサーバに対してユーザの情報を参照することで，ユーザ認証を行うことのできる仕組みを実装しています。WPA2では，通信中において動的に暗号鍵を更新することで，安全性を向上させています。

ファイアウォール

インターネットと社内LANとの間など，主要なネットワーク間に位置するネットワーク間接続装置で，ネットワーク間で送受信されるパケットの送信元，宛先，通信プロトコルまたは内容などを検査し，ルールに該当しない不審なパケットを破棄する役割をもちます。

WAF

Web Application Firewall。Webサーバとブラウザの間でやり取りされるデータの内容を監視し，Webアプリケーションプログラムの脆弱性を突く，XSS（クロスサイトスクリプティング）やSQLインジェクションなどの攻撃を防御するために用いられる，特別なファイアウォールのことです。

ウイルス対策ソフト

PCやサーバなどにインストールされ，ウイルス感染を防止するためのソフトウェアです。PCなどのファイルの内容を検査してウイルス感染の有無を検証し，感染していたファイルの削除や復元を行います。

DLP

Data Loss Prevention。情報システムから機密情報などが外部に流出することを防止すること，及びそのために導入・構築する装置やシステムのことです。

SIEM

Security Information and Event Management。ファイアウォールやサーバなどの各種機器から収集したログを分析して，セキュリティインシデントの発生を監視し，発生時は管理者に通知して迅速に対応するための仕組みのことです。

ディジタルフォレンジックス

コンピュータ犯罪に対する科学的調査のことで，不正アクセスなどの犯罪に対する証拠（記録・ログなど）を立証するために必要なデータを保全して収集・分析すること，及びその後の訴訟などに備えることです。

UTM

Unified Threat Management，統合脅威管理。ファイアウォール，IDS／IPS，ウイルス対策ソフト，及び各種フィルタリング機能といった情報セキュリティに関する各種製品の機能をまとめて保持している，統合的な管理用の機器を導入することで，情報セキュリティ対策コストの削減や情報の一元管理などを実現することです。

SSLアクセラレータ

SSL／TLSにおける暗号化・復号処理を，Webサーバの代わりに高速で実行する装置です。Webサーバの処理負荷を軽減することを目的として導入されます。

RASIS

コンピュータシステムの，５つの信頼性評価指標の総称です。

R＝信頼性（Reliability）：システムが故障せずに稼働し続ける度合いを示す指標。MTBF（平均故障間隔）で表される。

A＝可用性（Availability）：システムをいつでも通常どおりに利用できる度合いを示す指標。稼働率（MTBF／（MTBF＋MTTR））で表される。

S＝保守性（Serviceability）：システムが，故障から可能な限り短い時間で復旧できる度合いを示す指標。MTTR（平均修理時間）で表される。

I＝保全性（Integrity）：障害が発生しても，データが破壊されず整合性を保った状態である度合いを示す指標。

S＝機密性または安全性（Security）：データが，外部からの不正アクセスなどによって盗まれたり，改ざんされたりすることがないように，データを保護する度合いを示す指標。

UPS

Uninterruptible Power Supply，無停電電源装置。商用電源の一時的な停電や瞬断によって電流の供給が絶たれた場合に，コンピュータなどに一定時間安全に電流を供給するための装置です。UPSの内部にはバッテリーなどが存在し，コンセントから供給される電流が途絶えた場合にはバッテリーの電気を利用して即座に電流を供給することで，コンピュータの継続稼働を可能にしています。

瞬断

落雷などによって発電所などの施設が一時的に使用不可になると，電力会社は電源の供給ルートを切り替えるなどの措置によって電力の供給を継続させます。その際に，供給ルートを切り替えるために要したわずかな時間（数秒～数分）のみ，コンセントからの電力の供給が途切れることがあります。このような現象のことです。

MDM

Mobile Device Management。スマートフォンなどの携帯端末の情報セキュリティを管理するための機能及び管理体制のことです。管理者の許可なく携帯端末にソフトウェアをインストールすることを禁止したり，ウイルス対策ソフトのインストールやアップデートを強制したりすることです。

ミラーリング

同じデータを複数のディスクに冗長保存して安全性を高めるときに，メインのディスク装置と冗長ディスク装置の2

つを，常に同一の内容に保つことです。

遠隔バックアップ

遠隔地に用意したバックアップ用のサーバに，ネットワーク経由でバックアップデータを送信して保存させることで，バックアップを円滑に実行することです。

クリアデスク

JIS Q 27002で規定されている方針の一つで，離席時や帰宅時に，机の上の書類などを全て収納することで，機密情報が他人に知られないようにすることです。

クリアスクリーン

JIS Q 27002で規定されている方針の一つで，離席時にPCをログオフするか，スクリーンセーバなどで画面の内容を隠すことで，機密情報が他人に知られないようにすることです。

USBキー

USBにログイン用の情報を記録し，本人だけがPCを起動できるようにするための装置です。USBキーを装着していないとPCを起動できないので，USBキーをもっていない他人は勝手にPCを使用できなくなります。

セキュリティ実装技術

IPsec

インターネットなどの開かれたネットワーク上において，専用線と同様にセキュリティの確保された通信を行うための暗号化・認証プロトコルです。

トンネルモード

IPsecのうち，IPヘッダも含めたIPパケット全体を暗号化し，新たなIPヘッダを付加して受信側に送付する方法です。元の送信元・宛先IPアドレス自体を隠蔽できるため，安全性が高くなっています。しかし，もともとの送信元や宛先のIPアドレスは，暗号化によって経路上のルータなどからは読み取れなくなるため，発信ホストと受信ホストの間で暗号化したIPパケットを直接送受信することはできません。

トランスポートモード

IPsecのうち，IPパケットのデータ部のみを暗号化して送信する方法です。このモードでは，IPパケットのヘッダ部は暗号化されないため，もともとの発信側システムや受信側システムのIPアドレスをそのまま利用して通信を実行できます。そのため，発信ホストと受信ホストの間の全経路でデータが暗号化されます。

SSL/TLS

Secure Socket Layer/Transport Layer Security。Web上で安全なデータ送受信を行うためのプロトコルであり，共通鍵暗号方式と公開鍵暗号方式を組み合わせて使用することで，通信相手との安全な鍵交換と暗号化を実現します。

クライアントとWebサーバ間での，SSL／TLSの暗号化・データ送付の一般的な手順の概要を示すと，以下のとおりとなります。

①データの暗号化・復号に使用するための共通鍵を生成し，クライアントはその共通鍵を，Webサーバの公開鍵で暗号化してからWebサーバに送付する。

②Webサーバは，暗号化されて送信されてきた共通鍵を，Webサーバの秘密鍵で復号し，共通鍵を安全に入手する。

③以後，クライアントとWebサーバの間で共有できた共通鍵を用いて，データを暗号化して送受信する。なお，共通鍵を用いてデータの暗号化を行うのは，共通鍵の方が公開鍵よりも暗号化や復号に要する時間が短く，処理を高速に実行できるためである。

SSH

Secure Shell。リモートログイン（遠隔にあるコンピュータの操作）やリモートファイルコピーなどを，通信経路上のデータを暗号化した上で行えるツール及びプロトコルのことです。SSHには利用者認証機能も存在します。

Cookie

Nameの値がtaroであるという情報を，ブラウザに保存できる

Webサーバとブラウザとの間のセッション（データ送受信の順序及びその状態）の管理や，Webサーバに対するアクセスがどのPCからのものであるかを識別するために用いられるものです。CookieはWebサーバからブラウザに渡され，利用者のコンピュータのハードディスクに記録されます。そして，ブラウザからWebサーバへのアクセス時に必要に応じてWebサーバに送信され，利用されます。

パケットフィルタリング

ファイアウォールなどが行うパケット検証動作で，送信元IPアドレスなどの値を参照し，パケット送受信に関するルール（フィルタリングルール）に違反しているパケットを遮断することで，不正侵入などを防ぐことです。

ベイジアンフィルタリング

フィルタリングを行うソフトウェアが迷惑メールに含まれる特徴的な語句などを収集・解析して自己学習を行い，迷惑メールかどうかを統計的に解析して判定する，迷惑メール検知手法のことです。

ダイナミックパケットフィルタリング

次の方法で行うパケットフィルタリングのことです。

①社内のPCを送信元，インターネット上のサーバを宛先とし，送信元ポート番号を任意の値，宛先ポート番号を特定のサービスのポート番号とする，サーバ上のサービスの利用を依頼するリクエストパケットだけをフィルタリングテーブルに掲載し，通過を許可する。

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
社内のPC	WebサーバA	任意	80

（WebサーバAはHTTP（ポート番号80）サービスを提供している）

②次のようなフィルタリングテーブルを用意して，①のリクエストパケットに対応するレスポンスパケットの通過を常に許可していると，外部からの不正なパケットを侵入させてしまう可能性がある。

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
社内のPC	WebサーバA	任意	80
WebサーバA	社内のPC	80	任意

2行目のパケットを常に許可すると，社内のPCを宛先とし，送信元IPアドレスをWebサーバAのIPアドレスに偽装している，送信元ポート番号を80，宛先ポート番号を任意とした攻撃用のパケットの通過が許可されてしまう。

③したがって，レスポンスパケットをフィルタリングテーブルに掲載しないようにしておき，リクエストパケットがファイアウォールを通過したとき，それに対応する適切なポート番号をもつレスポンスパケットだけ，一時的に通過を許可する。

例えば，社内のPCからWebサーバAに対して，送信元ポート番号を2000，宛先ポート番号を80とするリクエストパケットが送信されてファイアウォールで通過を許可したとき，次のような行を一定時間だけフィルタリングテーブルに掲載し，WebサーバAから返ってくる正当なレスポンスパケットだけ通過を許可する。

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
社内のPC	WebサーバA	任意	80
WebサーバA	社内のPC	80	2000

（網掛け部分＝一定時間だけフィルタリングテーブルに掲載する行）

MACアドレスフィルタリング

ネットワーク上を流れるフレームの送信元MACアドレスを検査し，許可された送信元MACアドレスのフレームだけを通過させることで，不正な接続元からのアクセスを拒否することです。

ブラックリスト

WAFにおいて，攻撃用のスクリプトコードなどの問題のある通信データパターンを定義したものです。送信されてきたIPパケットがブラックリストに該当する場合，WAFはそのIPパケットを遮断するか，無害化します。

ホワイトリスト

WAFにおいて，問題のない正常な通信データパターンを定義したものです。

VLAN

PCやネットワーク機器が物理的に接続されている状況において，論理的にネットワークを分割できる機能のことです。

VLAN機能をもつスイッチは，自らがもつ各ポートを，それぞれ異なるネットワークに所属するように分割できます。スイッチによって分割されたポートに到達したフレームは，自分の所属するネットワーク以外のネットワークのポートには送付されなくなります。

リバースプロキシ

内部ネットワークやDMZ上に設置されるサーバで，外部（インターネット）から社内のWebサーバなどに向けて到達する要求をいったん受け取ったうえで，各要求を適切なサーバに割り振る機能をもっているサーバのことです。

リバースプロキシには，Webサーバなどの静的コンテンツをキャッシュし，同一Webサーバ上の同じページへのアクセスが外部から何度も到達する場合，キャッシュしたデータを返すことによってWebサーバの負荷を低減させることで，アクセス性能を改善させる効果があります。また，リバースプロキシ上で強固なセキュリティ対策を実現する