応用情報技術者

試験対策テキストⅡ【システムの利用と開発編】

無料体験入学者用

TAC

はじめに

応用情報技術者試験(AP)は2009年春期より実施された試験区分です。対象者像は,

「高度IT人材となるために必要な応用的知識・技能をもち,
高度IT人材としての方向性を確立した者」

とされています。基本情報技術者試験(FE)で求められる基本的な知識に加え,さらに専門的・詳細な内容を含めた応用的知識が問われることになります。

本書は応用情報技術者試験の出題範囲であるテクノロジ系,ストラテジ系,マネジメント系のうち,テクノロジ系の周辺技術要素であるヒューマンインタフェース,マルチメディア,データベース,ネットワーク,情報セキュリティ,そしてシステム開発に関する分野の知識を網羅しています。その上で,読者の皆さんが効率よく学習が行えるよう,基礎的な用語や考え方を分かりやすく解説するように心がけました。

本書により,読者のみなさんが応用情報技術者試験に合格されることを願ってやみません。

TAC情報処理講座

目　次

第４章

情報セキュリティ

学習テーマ　4－1

情報セキュリティマネジメント

(1)　情報セキュリティマネジメント

●情報セキュリティの定義

情報セキュリティマネジメントシステムの用語を定めた規格であるJIS Q 27000では，情報セキュリティを「情報の機密性，完全性及び可用性を維持すること」と定義している。これらの特性は，頭文字をとって情報セキュリティのC.I.Aともいう。

表4.1　情報セキュリティのC.I.A

特性	意味
機密性（confidentiality）	認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しない特性。
完全性（integrity）	正確さ及び完全さの特性。
可用性（availability）	認可されたエンティティが要求したときに，アクセス及び使用が可能である特性。

JIS Q 27000では情報セキュリティについて，「さらに，真正性，責任追跡性，否認防止，信頼性などの特性を維持することを含めることもある」と規定されている。これらの用語は，次のような意味をもつ。なお，ここでのエンティティ(実体)とは，情報を扱う組織，人，設備，ソフトウェアなどが該当する。

表4.2　各用語の意味

特性	意味
真正性	エンティティは，それが主張するとおりのものであるという特性
責任追跡性	あるエンティティの動作が，その動作から動作主のエンティティまで一意に追跡できることを確実にする特性
否認防止	主張された事象又は処置の発生，及びそれを引き起こしたエンティティ（利用者など）を証明する能力
信頼性	意図する行動と結果とが一貫しているという特性。

●JIS Q 27000シリーズ

情報セキュリティのC.I.Aを維持するとともに継続的に改善する仕組みを，情報セキュリティマネジメントシステム(ISMS：Information Security Management System)という。JIS Q 27000シリーズはISO/IEC27000シリーズを基に策定された情報セキュリティマネジメントに関する規格群であり，次のような規格が制定されている。

JIS Q 27000：情報セキュリティマネジメントシステム－用語
JIS Q 27001：情報セキュリティマネジメントシステム－要求事項
JIS Q 27002：情報セキュリティ管理策の実践のための規範

JIS Q 27001に基づき，組織が構築した情報セキュリティマネジメントシステムの適合性を評価する制度を，ISMS適合評価制度という。

●情報セキュリティポリシー

情報セキュリティマネジメントシステムの構築においては，組織が情報セキュリティに取り組む際の方針を定める必要がある。これを情報セキュリティポリシーまたは情報セキュリティ方針という。情報セキュリティポリシーには多様な解釈があり，複数の文書で構成されることも多いが，情報セキュリティに関する企業の考え方や取組みを明文化したものを，情報セキュリティ基本方針という。情報セキュリティ基本方針は，企業の経営層が承認・宣言したものであり，社内外に広く公開すべきである。また，時勢や環境の変化に伴い，柔軟に変更していくことが望ましい。

●情報セキュリティインシデント

JIS Q 27000では，「情報セキュリティ方針への違反若しくは管理策の不具合の可能性，又はセキュリティに関係し得る未知の状況を示す，システム，サービス若しくはネットワークの状態に関連する事象」を情報セキュリティ事象と定義しており，「望まない単独若しくは一連の情報セキュリティ事象，又は予期しない単独若しくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの」を情報セキュリティインシデントと定義している。すなわち，情報セキュリティインシデントとは，サービスの停止や情報の漏えいなど，情報セキュリティを脅かす可能性が高い（または実際に脅かされた）出来事であり，単にインシデントともいう。

このインシデントの潜在的な原因を脅威といい，一つ以上の脅威によって付け込まれる可能性のある，資産又は管理策の弱点を脆弱性という。脅威には盗聴やシステムのクラッキング，誤り，地震などが該当する。脆弱性には，プログラムのセキュリティ上のバグ(セキュリティホール)，暗号化されていないデータ，施錠されていない入口などが該当する。

情報資産の脆弱性に対して脅威がつけ込むと，損害が発生する可能性が生じる。これをリスク又は情報セキュリティリスクという。情報セキュリティにおいてはリスクを適切に評価し，管理策を講じるリスクマネジメントが重要となる。

(2)　その他のセキュリティ規格・ガイドライン・関連組織

●ISO/IEC 15408

ISO/IEC 15408は，システム及び製品に関する情報技術セキュリティ評価基準を定めた国際標準であり，情報技術を利用した製品やシステムのセキュリティ機能が，評価基準に適合するかを評価するための規格である。日本ではJIS X 5070として標準化されており，コモンクライテリア(CC：Common Criteria)ともいう。この規格を評価基準とした制度にITセキュリティ評価及び認証制度がある。これは，情報技術に関連した製品のセキュリティ機能の適切性，確実性を第三者機関が評価し，その結果を公的に認証する。

●クラウドサービス利用のための情報セキュリティマネジメントガイドライン

JIS Q 27002では，第三者が提供するサービスの利用に関する管理策も定められているが，ITを所有せずにクラウドコンピューティングを全面的に利用するような組織に対しては十分といえない。そこで，クラウドサービスの利用者が情報セキュリティ対策を円滑に行えるように，JIS Q 27002の管理策を補完するために経済産業省によって作成された指針がクラウドサービス利用のための情報セキュリティマネジメントガイドラインである。

●JIS Q 27017

JIS Q 27017は，JIS Q 27002の内容に基づいてクラウドサービスのための情報セキュリティ管理策を実践する際の規範集である。適用対象はクラウドサービスプロバイダ(クラウドサービスを他者に提供する事業者)及びクラウドサービスカスタマ(そのサービスの利用者)であり，それぞれの立場ごとに内容が記されている。

●JIS Q 27014

JIS Q 27014は，情報セキュリティガバナンスに関する規格である。情報セキュリティガバナンスを“組織の情報セキュリティ活動を指導し，管理するシステム”と定義し，その実現のための指針を記述している。組織が実施すべきプロセスとしては，以下のようなものがある。

- 経営陣は統治のために“評価”，“指示”，“モニタ”及び“コミュニケーション”の各プロセスを実行する。
- さらに“保証”プロセスによって，ガバナンス及び達成レベルについての独立した客観的な意見が得られる

●リスクマネジメントに関する規格

リスクマネジメントに関する規格には，JIS Q 31000やJIS Q 0073がある。JIS Q 31000では，リスクマネジメントの原則及び指針を，JIS Q 0073ではリスクマネジメントの用語を定めており，JIS Q 27000シリーズはこれらの規格と整合するようになっている。

●サイバーセキュリティ経営ガイドライン

経済産業省とIPAが策定したサイバーセキュリティ経営ガイドラインは，企業の経営者を対象とした，サイバー攻撃から身を守る観点で認識すべき3つの原則や，情報セキュリティ対策を実施する上で責任者に指示すべき重要項目などを取りまとめたものである。

3つの原則には，サイバーセキュリティリスクを認識してリーダーシップによって対策を進めること，ビジネスパートナー及び委託先を含めたセキュリティ対策が必要なこと，関係者との適切なコミュニケーションが必要なことがある。

●中小企業の情報セキュリティ対策ガイドライン

中小企業では，情報セキュリティの重要性を理解していないことや，取り組む経済的余裕がないことも珍しくない。IPAが公表した中小企業の情報セキュリティ対策ガイドラインは，中小企業や小規模事業者を対象として，経営者が認識し実施すべき指針や，社内において対策を実践する際の手順や手法をまとめた文書である。当ガイドラインは，できるところから始め，ステップアップしていくことを目的としており，当ガイドラインに沿って中小企業などが情報セキュ

リティに取り組むことを自己宣言する制度を，SECURITY ACTIONという。

●CSIRT

CSIRT(Computer Security Incident Response Team)は，コンピュータセキュリティインシデントに対応するための組織である。企業などの組織内に設置される組織内CSIRTや，CSIRTをサービスとして提供する企業などがある。

●JPCERTコーディネーションセンター

JPCERTコーディネーションセンターは，日本国内におけるインシデントの受付･対応の支援･発生状況の把握・手口の分析・再発防止のための対策の検討や助言などを技術的な立場から行う政府機関や企業から独立した組織である。インシデント対応においてCSIRT間の情報連携や調整などを行うコーディネーションセンターの機能をもち，CSIRTの構築や運用を支援するためのCSIRTマテリアルや，インシデント発生時にCSIRTが行うべき解決までの一連の処理手順を表したインシデントハンドリングマニュアルなどの文書も公表している。インシデントハンドリングマニュアルでは，次のような基本的な流れを提示している。

・検知／連絡受付　…　自組織での検知や外部からの連絡によるインシデント発生の認識
・トリアージ　…　インシデントの事実確認と対応の優先順位付け
・インシデントレスポンス　…　インシデントの分析や実際の対処
・報告／情報公開　…　プレスリリースや官公庁への報告など

●JVN

JPCERTコーディネーションセンターは，IPAと共同でJVN(Japan Vulnerability Notes)を運営している。JVNは，日本で使用されているソフトウェアなどの脆弱性に関連する情報や対策方法を提供するポータルサイトである。JVNでは以下のような仕組みを採用し，情報公開している。

・CVSS(Common Vulnerability Scoring System：共通脆弱性評価システム)
　情報システムに存在する脆弱性を評価するための基準であり，基本評価基準，現状評価基準，環境評価基準の三つの基準で構成されている。この基準を採用することによって，情報システムのセキュリティ脆弱性の深刻度をベンダ，セキュリティ専門家，管理者，ユーザなどの間の共通の言葉として比較評価できるようになる。
・CVE(Common Vulnerabilities and Exposures)識別子
　共通脆弱性識別子とも呼ばれる。個別の製品に含まれる脆弱性を識別する情報。さまざまな組織が発表するそれぞれの脆弱性対策情報を，製品の脆弱性ごとにCVE識別子によって関連づけることが可能となる。
・CWE(Common Weakness Enumeration)
　共通脆弱性タイプ一覧。SQLインジェクション，クロスサイトスクリプティング，バッファオーバフローなど，ソフトウェアの脆弱性の種類を識別するために利用される。

●J-CRATとJ-CSIP

サイバーレスキュー隊(J-CRAT：Cyber Rescue and Advice Team against targeted attack of Japan)は，IPAが発足させた，標的型サイバー攻撃の被害拡大防止のための支援体制である。標的型サイバー攻撃を受けた組織や個人から提供された情報を分析し，社会や産業に重大な被害を及ぼしかね

ない標的型サイバー攻撃の把握，被害の分析，対策の早期着手の支援を行う。

サイバー情報共有イニシアティブ(J-CSIP：initiative for Cyber Security Information sharing Partnership of Japan)は，IPAにサイバー攻撃などの情報を集約し，参加組織間で情報共有を行って高度なサイバー攻撃への対策につなげていく取組みである。

●CRYPTREC

CRYPTREC(CRYPTography Research and Evaluation Committees)とは，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・検討する組織である。電子政府における調達のために推奨すべき暗号リスト(CRYPTREC暗号リスト)を策定し，電子政府推奨暗号リスト，推奨候補暗号リスト，運用監視暗号リストを公開している。

●サイバーセキュリティ戦略本部とNISC

サイバーセキュリティ基本法は，サイバーセキュリティに関する基本理念や国及び地方公共団体の責務などを定めた法律である。電磁的方式によって記録・発信・伝送・受信される情報を対象としており，サイバーセキュリティに関する施策を総合的かつ効果的に推進するために，内閣にサイバーセキュリティ戦略本部を置くことを定めている。サイバーセキュリティ戦略本部は内閣官房長官を本部長とし，サイバーセキュリティ戦略の案の作成や，サイバーセキュリティ対策の基準の作成などを行う。また，内閣官房にはNISC（National center of Incident readiness and Strategy for Cybersecurity；内閣サイバーセキュリティセンター）が設置されている。NISCはサイバーセキュリティ政策に関する総合調整を行いつつ，我が国をサイバー攻撃から防衛するための司令塔機能を担う。

●情報セキュリティサービスの評価

経済産業省では，“情報セキュリティサービス審査登録制度”を設けている。これは，情報セキュリティサービス事業者が提供するサービスについて一定の品質の維持向上が図られていることを第三者機関が客観的に審査(判断)し，登録する制度である。

審査基準としては，“情報セキュリティサービス基準”が用いられる。基準に適合して登録対象となったサービスは，IPAが“情報セキュリティサービス基準適合サービスリスト”としてとりまとめ，インターネット上で公開する。

また，政府情報システムのためのクラウドサービスを評価・登録する制度として，ISMAP(Information system Security Management and Assessment Program)がある。クラウドサービス事業者は情報セキュリティ対策の実施状況について監査を受け，妥当と判断されたクラウドサービスがISMAPクラウドサービスリストに登録される。

ISMAPの管理基準は，ガバナンス基準，マネジメント基準，管理策基準の三つで構成されている。ガバナンス基準は経営陣が実施すべき事項，マネジメント基準は管理者が実施すべき事項，管理策基準は業務の実施者が実施すべき事項を定めている。

学習テーマ　4－2

リスク管理

●リスクマネジメント

組織におけるリスクを特定し，リスクの除去や最小化といった管理を行う一連の活動をリスクマネジメントという。リスクマネジメントは，次のようなプロセスで構成される。

表4.3　リスクマネジメント

リスクマネジメント			リスクを管理する一連の活動
	リスクアセスメント		リスク分析からリスク評価にいたるプロセス
		リスク特定	リスク因子(脅威と脆弱性の組合せ)を特定
		リスク分析	リスク発生する可能性と影響度を分析
		リスク評価	リスクの重大さをリスク評価基準と比較する
	リスク対応		リスクに対する対策を選択･実施する
	リスク受容		リスク対応後の残留リスクを受容
	リスクコミュニケーション		リスクに関する情報の共有

●リスクアセスメント

JIS Q 27001では，ISMSの適用範囲内における情報の機密性，完全性及び可用性の喪失に伴うリスクを特定するために，情報セキュリティリスクアセスメントのプロセスを適用することが求められている。リスクアセスメントとは，リスク特定，リスク分析，リスク評価から構成されるプロセス全体のことである。

リスクアセスメントを実施するにあたり，リスク基準などを設定する必要がある。リスク基準とは，リスクの重大性を評価するための目安とする条件であり，組織の目的，外部状況及び内部状況に基づいて決定する。リスクアセスメントの分析手法には，次のようなものがある。

表4.4　リスクアセスメントの分析手法

ベースラインアプローチ	確保すべき一定のセキュリティ水準(ベースライン)をあらかじめ決めておき，対象となるシステムに一律に適用する手法。省力化が期待できるが，セキュリティ対応策が不十分または過剰になるおそれがある。
詳細リスク分析	資産ごとにリスク識別を実施する手法。脅威や脆弱性からリスクを評価し，対応策を選択する。適切な対応策が期待できるが，労力は大きくなる。
組合せアプローチ	ベースラインアプローチと詳細リスク分析を組み合わせ，双方の弱点を相互に補完する手法。
非形式的アプローチ	現場担当者がもつ知識や経験，判断に基づく手法。省力化が期待でき，適切な対応策が期待できるが，客観性に欠ける場合がある。

・リスク特定

リスク特定は，リスクを発見・認識及び記述するプロセスであり，リスクの原因となる脅威や脆弱性，起こり得る結果等を特定する。このために，過去のデータや専門家の意見，ステークホルダ(利害関係者)のニーズなどを含むことがある。

・リスク分析

リスク分析は，リスクの特質を理解し，リスクレベルを決定するプロセスである。リスクレベルは，JIS Q 27000において「結果とその起こりやすさの組合せとして表現される，リスクの大きさ」と定義されており，次のように考えることもできる。

リスクレベル ＝ 資産価値 × 脅威 × 脆弱性

・リスク評価

リスク評価は，リスクレベルが受容可能かを決定するために，リスク分析の結果をリスク基準と比較するプロセスであり，この結果を受けてリスクの優先順位付けを行う。

●リスク対応

リスク対応はリスクを修正するプロセスである。このための手法には，次のようなものがある。

表4.5　リスクを変更するための方策

方策	内容	例
リスク低減	適切な管理策(コントロール)を採用することにより，リスクが発生する可能性やリスクが発生した場合の影響度を低減する。	セキュリティ技術の導入， 入口の施錠， スプリンクラの設置　など
リスク回避	リスクと資産価値を比較した結果，コストに見合う利益が得られない場合など，資産ごと回避する。	業務の廃止， 資産の廃棄　など
リスク移転	資産の運用やセキュリティ対策の委託，情報化保険など，リスクを他者に移転する。	ハウジングサービスの利用， 情報化保険の加入　など
リスク受容	識別されており，受容可能なリスクを意識的，客観的に受容する。リスクが顕在化したときは，その損害を受け入れる。	会社が損失額を負担する など

このうち，リスク低減では，適切な管理策を適用することによって，リスクが発生する可能性やリスクが発生した場合の影響度を低減させる。したがって，管理策適用後のリスクレベルは，管理策の適用前よりも小さくなる。これが受容できるリスク基準の範囲内であれば，残留リスクとして受容することになる。残留リスクとは，リスク対応後に残ったリスクのことであり，特定されていないリスクが含まれている場合もある。リスクの対応計画や残留しているリスクの受容については，リスク所有者(リスクの運用管理についてアカウンタビリティ及び権限をもつ者)の承認を得る。

学習テーマ　4－3
暗号技術

暗号技術は，情報を不正に取得する盗聴などの脅威から保護するための基盤技術であり，当初は機密性を実現するために用いられてきたが，現在では，後述の認証技術にも用いられている。

(1)　暗号化の概念

●暗号化と復号

暗号技術において，元の(暗号化されていない)データを平文(ひらぶん)といい，暗号化されたデータを暗号文という。また，平文を暗号文に変換することを暗号化，(正規の手順で)暗号文を平文に変換することを復号という。なお，本来なら復号できないはずの利用者が，暗号文から平文を得ることを解読という。

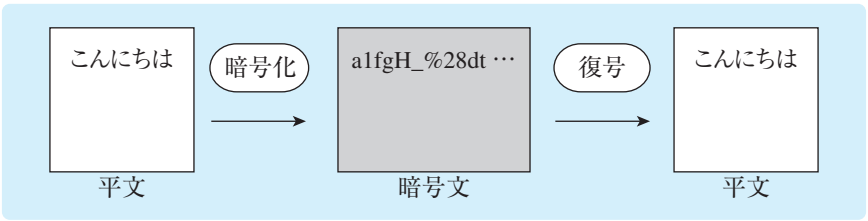


図4.1　暗号化と復号

●暗号化アルゴリズムと暗号化鍵

暗号技術は，暗号化を行う手順である暗号化アルゴリズムと，暗号化に必要なパラメタ(ビット列)である鍵から構成される。たとえば，「鍵との排他的論理和を求めた結果を暗号文とする」というような暗号化アルゴリズムによって作成された暗号文は，暗号化アルゴリズムを知っていても鍵となるビット列を知らなければ復号できない。

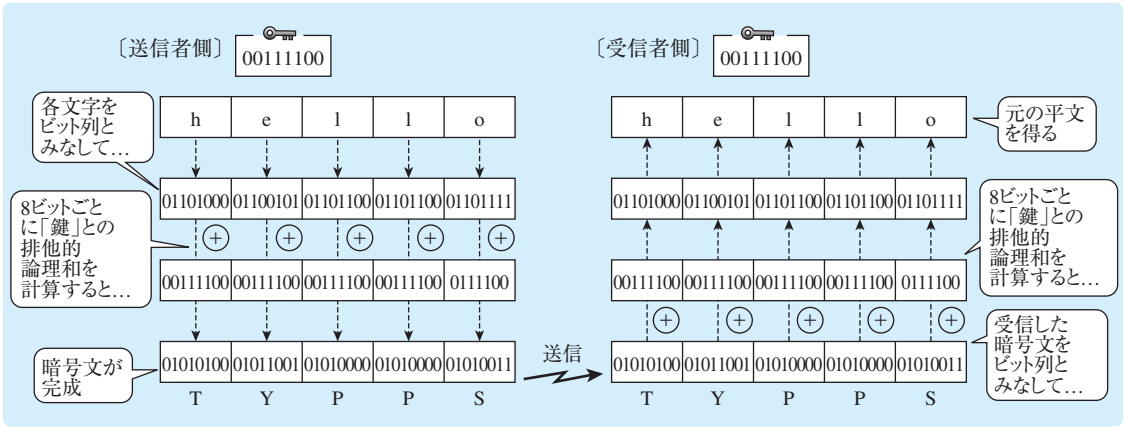


図4.2　暗号化と鍵

このように，暗号化技術は暗号化アルゴリズムが公開されていても，鍵さえ知られなければ解読されない(解読に膨大な時間を要する)という理論に基づくため，鍵の管理が重要になる。

(2)　共通鍵暗号方式

●共通鍵暗号方式の概念

暗号化と復号に同じ鍵を用いる暗号方式のことを，共通鍵暗号方式という。共通鍵暗号方式においては，任意のビット列を共通鍵とし，通信を行う二者で共有する。この共通鍵を用いてビットの入れ替えや排他的論理和の演算などを繰り返し，暗号化と復号を行う。代表的な共通鍵暗号方式には，AES(Advanced Encryption Standard)がある。AESは，暗号化の対象となるデータを一定長のブロックに区切り，ブロックごとに暗号化を行うブロック暗号方式を採用しており，鍵長は128ビット，192ビット，256ビットのいずれかを選択できる。なお，暗号化の対象となるデータをビット単位あるいはバイト単位に逐次暗号化する方式を，ストリーム暗号という。

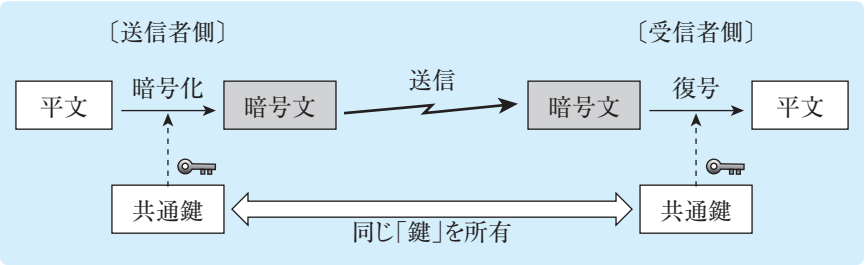


図4.3　共通鍵暗号方式の概念

●共通鍵暗号方式の特徴

共通鍵暗号方式は，暗号化や復号に要する処理時間が短い。このため，大量のデータを一括して暗号化する用途に適している。しかし，鍵を通信相手と共有するときに鍵が盗聴されるリスクがあるため，ネットワークを用いた鍵の配送には適さない。

また，データを第三者から秘匿するためには，同じ鍵を異なる相手に使うことはできない。このため，システム中でn人の利用者が相互に通信を行う場合，各利用者はn－1個の鍵を管理し，システム中に存在する鍵の種類は，

$$n(n-1)\ /\ 2$$

となる。すなわち，利用者が多くなるほど鍵の種類が増え，鍵の管理が煩雑になる。

【ポイント】

暗号化と復号に同一の鍵を用いる。
公開鍵暗号方式に比べ，暗号化や復号に要する処理時間が短い。
n 人の利用者がいる場合は合計n (n － 1) ／ 2種類の鍵が必要。

(3)　公開鍵暗号方式

●盗聴防止の仕組み

公開鍵暗号方式は，対となる二つの鍵(鍵ペア)を利用する方式である。鍵ペアには，

・一方の鍵で暗号化したデータは，対となる鍵でなければ復号できない

・一方の鍵から，もう一方の鍵を推測できない

という特徴がある。このため，一方の鍵を秘密鍵(Private Key)として他者に知られないよう厳重に管理すれば，もう一方の鍵は公開鍵(Public Key)として公開しても問題がない。

公開鍵暗号方式を用いた暗号化では，受信者本人のみが復号できる暗号文を生成する。したがって，暗号文は受信者の秘密鍵でのみ復号できればよい。このために，暗号化は対となる受信者の公開鍵で行う。

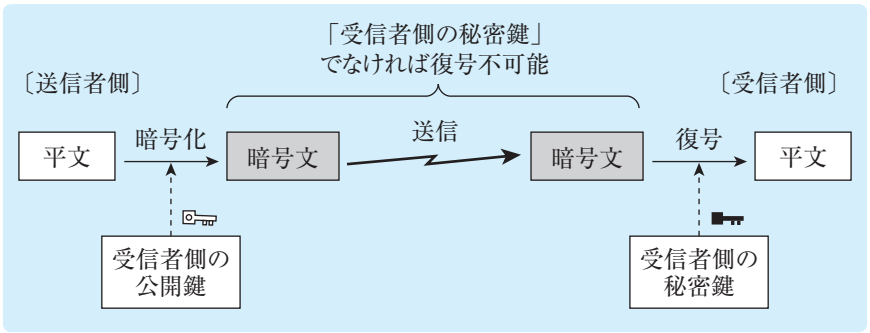


図4.4　公開鍵暗号方式の概念

公開鍵暗号方式の代表的なものには，素因数分解の複雑さを利用したRSA，離散対数暗号，楕円曲線暗号などがある。

【ポイント】

暗号化 →「受信者側」の「公開鍵」を利用
復号　 →「受信者側」の「秘密鍵」を利用

●公開鍵暗号方式の特徴

公開鍵暗号方式では，秘密鍵を本人のみが所有して秘匿するため，共通鍵暗号方式の課題であった安全な鍵の配送が実現できる。システム中でn人の利用者が相互に通信を行う場合，各利用者は二つの鍵(秘密鍵と公開鍵)を管理するので，システム中に存在する鍵の種類は2nとなり，共通鍵暗号方式に比べて鍵の管理が容易となるが，暗号化や復号の処理時間が長いため，大量のデータを一括して暗号化する用途には適さない。

【ポイント】

安全な鍵の配送が可能だが，暗号化や復号に要する処理時間が長い。
n 人の利用者がいる場合は 2n 種類の鍵が必要。

(4)　ハイブリッド暗号方式

共通鍵暗号方式と公開鍵暗号方式は，次のような相反する特徴をもつ。

表4.6　公開鍵暗号方式と共通鍵暗号方式の特徴

	処理時間	鍵の安全な配送
公開鍵暗号方式	長い	容易
共通鍵暗号方式	短い	困難

これらの長所を用いて，もう一方の短所を補完するように組み合わせた方式を**ハイブリッド暗号方式**という。具体的には，

> データの暗号化：共通鍵暗号方式(処理時間が短い)
> 共通鍵の暗号化：公開鍵暗号方式(鍵の配送が安全)

という用途に各暗号方式を用いる。なお，共通鍵をその通信(セッション)限りの使い捨てとする方式をセッション鍵暗号方式ともいい，次のような流れで処理を行う。

[1]　送信者側が通信に先立ち，「使い捨て」の共通鍵を生成する
[2]　送信者は，共通鍵を「受信者側の公開鍵」を用いて暗号化し，受信者側に送信する
[3]　受信者側が暗号化された共通鍵を受け取り，自身の秘密鍵で復号して共通鍵を得る
[4]　以降，その共通鍵を用いてメッセージをやりとりする
[5]　通信が終了したら，双方で共通鍵を破棄する

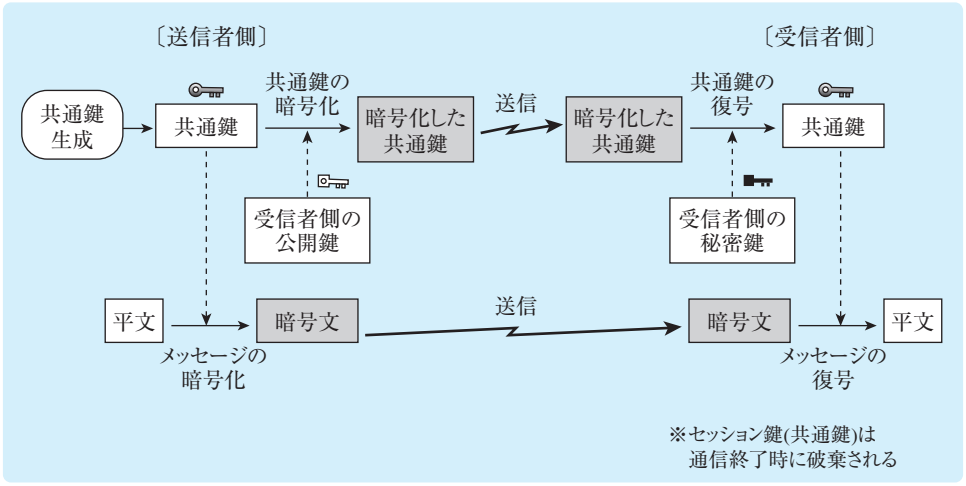


図4.5　ハイブリッド暗号方式

> **参考：暗号アルゴリズムの危殆化**
> 暗号アルゴリズムは，コンピュータの計算能力向上などにより，十分な安全性が得られなくなることがある。そのような事態を危殆化(きたいか)と呼ぶ。

(5)　ハッシュ関数

ハッシュ関数は，可変長のデータから固定長のビット列であるハッシュ値（メッセージダイジェスト）を生成する関数である。出力値から入力値を求めることが困難(原像計算困難性あるいは一方向性)という特徴や，異なる入力値から同じ出力値が得られる“衝突”が発生しにくい(衝突困難性)という特徴をもつことから，同じハッシュ値となるデータを偽造することが難しい。このため，データが同一であるか，変更・改ざんされていないかなどを確認する目的に用いられる。

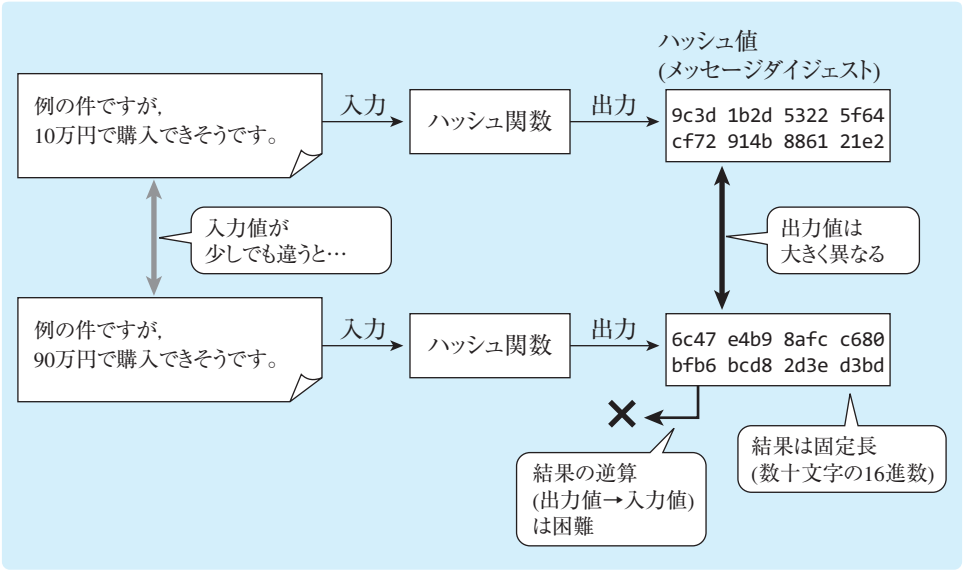


図4.6　ハッシュ関数

代表的なハッシュ関数には，256ビットのハッシュ値を生成するSHA-256がある。SHA-256は，SHA-1の後継規格群であるSHA-2の一部であり，これ以外にもSHA-384やSHA-512がある。さらにSHA-2の後継であるSHA-3も策定されている。

【ポイント】

入力データが異なればハッシュ値は異なる

- ハッシュ値が同じであれば元のデータは同一
- ハッシュ値が異なっていれば元のデータは異なる（改ざんされている）

参考：ブロックチェーン

ネットワーク内で発生する取引履歴などのデータをブロックとよばれる領域に格納し，ブロックとハッシュ値の組を繋げて管理する分散型の台帳をブロックチェーンという。この台帳は，ネットワーク上の多数のコンピュータが同期しながら管理する。仮に，あるブロックに含まれるデータを改ざんしたとしても，後続のブロックのハッシュ値を全て算出しなおさなくては整合性を保てないことから，改ざんを防止できる。すなわち，ブロックチェーンは完全性と可用性を確保することができる。

学習テーマ　4－4
認証技術

認証技術は，通信相手や情報の内容の正当性を検証するための技術であり，エンティティ(利用者，コンピュータ，アプリケーションなど)を認証するエンティティ認証と情報を認証するメッセージ認証に大別できる。

(1)　利用者確認

情報システムを利用する利用者が確かに本人であることを検証する技術を利用者確認(ユーザー認証)という。このために，本人の知識(記憶)，身体的特徴，所有物などの特徴を用いる。

●パスワード認証

パスワード認証は，利用者IDなどの識別符号と本人しか知りえない情報(文字列)であるパスワードをシステムに登録し，利用者が入力したパスワードと登録されたパスワードを比較して本人認証を行う。適用が容易な反面，パスワードが一致すれば本人と認識されてしまう。このため，パスワードを他人に知られないように管理するとともに，推測または解析されないようなパスワードを用いる必要がある。具体的には，次のような対策が有効である。

・パスワードは厳重に管理し，組織内外の関係者であっても漏えいしないようにする。
・パスワードを紙，ソフトウェアのファイル，携帯用の機器に記録して保管しない。ただし，パスワード保管システムなどのように，承認され，セキュリティを確保して保管されている場合を除く。
・パスワードに対する危険の兆候が見られる場合はパスワードを変更する。
・十分な最短文字数をもつ「良質なパスワード」を使用する。
・個人用のパスワードを共有しない。

「良質なパスワード」が満たす特徴としては，以下のようなものが挙げられる。

・覚えやすい。
・容易に推測可能な利用者の関連情報(氏名，電話番号，誕生日など)に基づかない。
・辞書に含まれる語から成り立っていない。
・仮パスワードは，最初のログオン時点で変更する。

参考：管理者アカウントの共有

管理者アカウントは，必ずしも共有してはならないというわけではない。ただし，共有する場合は，パスワードの機密性を確実に維持する必要がある。JIS Q 27002では，「例えば，頻繁にパスワードを変更する，特権を与えられた利用者が離職する又は職務を変更する場合はできるだけ早くパスワードを変更する，特権を与えられた利用者の間で適切な方法でパスワードを伝達する」などの方法が定められている。

●バイオメトリクス認証

バイオメトリクス認証(生体認証)は，指紋，静脈パターン，虹彩(アイリス)，声紋，顔(顔面)，網膜といった身体的特徴により本人確認を行う技術である。これらは，忘却や紛失によって認証できなくなることがない反面，経年変化や外的要因(外傷，健康状態など)によって変化する可能性がある。そこで，利用者本人であるにも関わらず拒否される確率(FRR：False Rejection Rate；本人拒否率)を低くするように基準を緩くすると，利用者本人ではない者(他人)が利用者本人と誤認識される確率(FAR：False Acceptance Rate：他人受入率)が高くなる。このため，適切な基準に設定することが重要であり，必要に応じて他の認証方式を組み合わせることもある。

●所有物を用いた認証

利用者の所有物を用いた認証方式には，スマートカード，USBトークン(認証を補助する装置)などを用いた方式がある。所有物の盗難などによって不正にアクセスされる恐れがあるので，紛失や盗難には十分に留意する必要がある。

●二要素認証

知識，身体的特徴，所有物の異なる認証方式のうち，二つを組み合わせて認証を行うことを二要素認証という。具体的には，セキュリティトークンとパスワードを組み合わせる，ICカードと暗証番号(PIN：Personal identification number)を組み合わせる，などが二要素認証に該当する。

また，認証のプロセスを二段階で行うことによってセキュリティを強化する手法は，二段階認証ともいう。たとえば，最初にユーザーIDとパスワードによる認証を行い，認証に成功した場合は事前に設定した“秘密の質問”の答えを入力させる方式などは，二段階認証に該当する。

●その他の認証方式

利用者が普段から利用するIPアドレスなどの情報を収集し，普段と異なる環境からのアクセスがあった場合に追加の本人認証を行うことによって安全性を高める方式を，リスクベース認証という。また，パスワードに依存しない利用者認証方法を総称してパスワードレス認証という。代表的なものに，生体認証をベースとしたFIDO(Fast IDentity Online)認証がある。FIDO認証では，利用者端末に内蔵または外付けされた認証器で指紋認証，顔認証などによる本人確認を行い，その結果にデジタル署名を付与してサーバに送信する。

●パスワードに対する攻撃手法

本人の誕生日や名前といった属性やパスワードに用いられやすい文字列など，パスワードを推測して試行する攻撃を類推攻撃という。このほかにも，パスワード解析用辞書を用いて試行する辞書攻撃，特定のアカウントに対してすべての文字を組み合わせて試行する総当たり攻撃(ブルートフォース攻撃)などがある。これらの手法に対しては，良質なパスワードを用いるとともに，一定回数認証に失敗したら当該のアカウントを一定期間使用できなくするアカウントロック（アカウントのロックアウト）が有効である。

よく使われるパスワードに対してアカウントを総当たりで試行するリバースブルートフォース攻撃については，同一のアカウントで連続して認証に失敗することがないので，アカウントロックが機能しにくい。このため，良質なパスワードを用いることが重要であり，同一のIPアドレスからの認証が連続して失敗した場合に攻撃とみなすなどの工夫も必要になる。

この他にも，別のサービスやシステムから流出した認証情報を用いて，認証情報を使い回しているアカウントを攻撃するパスワードリスト攻撃などがある。被害の拡大を防ぐためには，複数のサービスで同じユーザー ID とパスワードを設定しないことが重要になる。

●パスワードのハッシュ化

不正アクセスなどによってサーバに保管しているパスワードファイルが窃取された場合，パスワードを平文で保存していると全てのパスワードが漏えいしてしまう。この対策として，パスワードファイルにパスワードそのものではなく，パスワードのハッシュ値を保存する方法がある。ハッシュ値から元のパスワードを復元(逆算)することは困難なので，パスワードファイルが窃取されてもパスワードの漏洩を防ぐことができる。サーバが認証を行う際は，

・利用者が入力したパスワードを，サーバ側でハッシュ値に変換する
・サーバに保存された利用者のハッシュ値と照合する

という手順で正しいパスワードが入力されたかを確認する。

ただし，パスワードをハッシュ化して保存しても，大量の「想定されるパスワードとハッシュ値の組」を事前に用意しておき，パスワードファイル中のハッシュ値と照合すれば，元のパスワードを特定できてしまう。

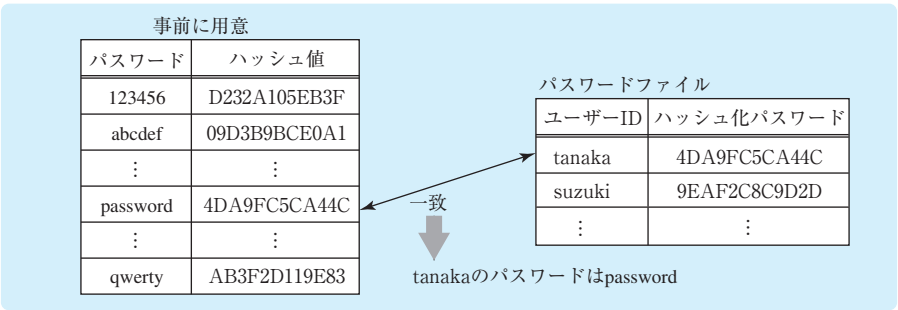


図4.7　パスワードファイルの解析

この方法でパスワードを解析する場合，事前に用意するパスワードとハッシュ値の組が膨大な量になってしまう。そこで，ハッシュ値から別のパスワードの候補を生成（還元という）し，そのハッシュ値を求める操作を繰り返すチェーンとよばれる仕組みでパスワードとハッシュ値の組を効率よく管理し，ハッシュ値から元のパスワードを解析する攻撃手法もある。これをレインボー攻撃という。

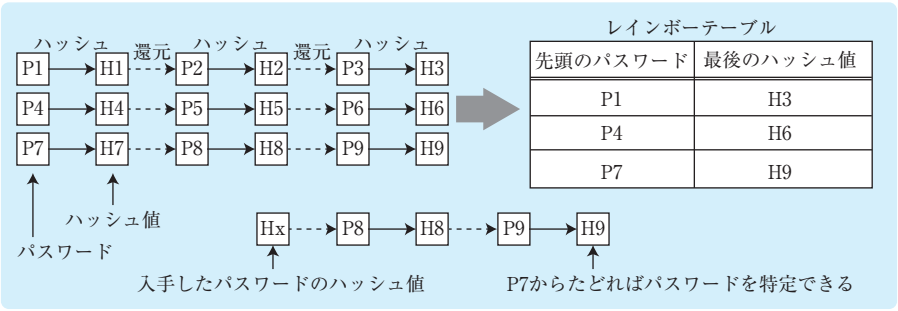


図4.8　レインボー攻撃

このような攻撃への対策として，登録したパスワードにソルトとよばれる文字列を連結し，そこから得たハッシュ値を保存する方法がある。ソルトを用いるとハッシュ値は全く異なる値になるので，攻撃者は事前にレインボーテーブルを用意するにあたり，一つのパスワードに対して膨大な数のハッシュ値を求めなければならなくなる。また，ハッシュ値の生成を複数回繰り返すストレッチングとよばれる方法も，攻撃や準備に要する時間を長くすることにより，実質的に攻撃を防ぐ効果が期待できる。

●ワンタイムパスワード

ネットワークを介してシステムに接続するリモートアクセス環境では，利用者が認証情報をもつサーバ(認証サーバ)に対して認証情報を送信し，認証サーバがそれを検証した結果を返す。

この場合，認証情報がネットワーク中を流れることになるため，パスワードには暗号化するなどの対策が求められる。しかし，単純にパスワードを暗号化しただけでは，暗号化されたパスワードをそのまま再利用するリプレイ攻撃のおそれがある。そこで，毎回異なるパスワードを生成するワンタイムパスワード(OTP：One Time Password)の利用が有効となる。

●チャレンジレスポンス方式

ソフトウェアによってワンタイムパスワードを実現する方式の一つに，チャレンジレスポンス方式がある。チャレンジレスポンス方式では，次のように認証を行う。

① 認証サーバがランダムなチャレンジ(要求文字列)を生成してクライアントに送る。

② クライアントはハッシュ関数などを用いた演算を行い，チャレンジとパスワードからレスポンス(応答文字列)を生成してサーバに送る。

③ サーバは自身でも同じ演算を行ってレスポンスを生成し，クライアントから送られたレスポンスと比較し，両者が一致すれば認証に成功する。

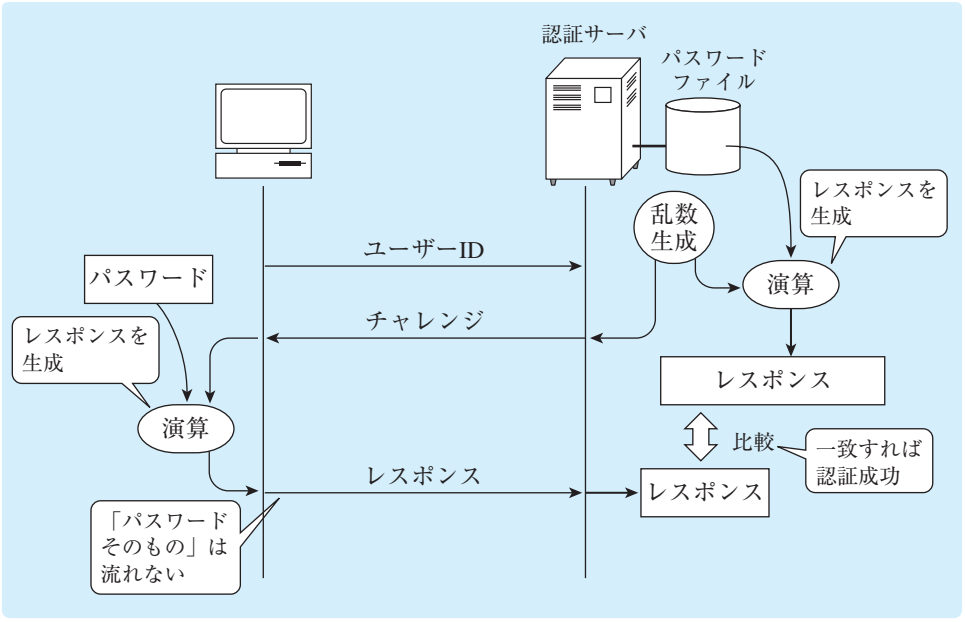


図4.9　チャレンジレスポンス方式

チャレンジレスポンス方式では，毎回異なるレスポンスが返され，パスワードそのものはネットワークに流れない。このため，推測困難なチャレンジを生成することで，パスワードの漏えいを防ぎ，リプレイ攻撃を防止することができる。なお，ポイントツーポイント接続を行うプロトコルのPPPでは，チャレンジレスポンス方式による認証プロトコルとして，CHAP (Challenge Handshake Authentication Protocol) を利用できる。

チャレンジレスポンス認証を用いることで，秘密情報であるパスワードを直接相手に提供することなく，安全に「秘密情報を知っているという事実」を証明できる。このような仕組みのことをゼロ知識証明と呼ぶ。

●RADIUS

RADIUS（Remote Authentication Dial In User Service）は，リモートアクセス環境において，認証情報やアカウンティング情報（接続の事実など）をやり取りするプロトコルである。従来はダイアルアップ接続における認証で用いられていたが，現在は無線LANにおける認証など，認証サーバで認証情報を一元管理する場面で広く利用されている。

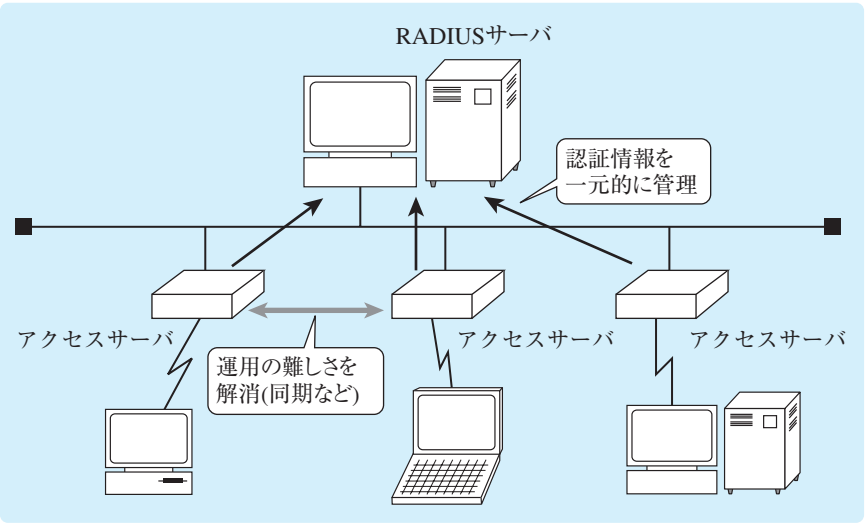


図4.10　RADIUSの概念

RADIUSでは，RADIUSサーバ（認証サーバ）が認証情報を一元管理しており，アクセスサーバや無線LANのアクセスポイントなどの接続要求を受ける機器がRADIUSクライアントとなる。RADIUSクライアントは，接続する端末から受信した認証情報をRADIUSサーバに送ると，RADIUSサーバが認証を行い，認証結果を返す。なお，RADISはAAAを実現できる。AAAとは，次の3要素の総称である。

表4.7　AAA

Authentication(認証)	アクセスを要求する者が，主張した利用者本人かを確認する
Authorization(認可)	認証された利用者が，要求した資源を利用できるか確認する
Accounting(報告)	接続した事実を記録する

●シングルサインオン

シングルサインオン(SSO：Single Sign On)は，一度の認証に成功すると，複数のサーバやサービスを利用できる技術である。サーバごとに認証を行う必要がないため，認証情報を一元管理できる。また，複数のパスワードなどを管理する必要がないので，利用者の負担も軽減できる。

シングルサインオンを実現する技術の一つであるSAML（Security Assertion Markup Language）は，XMLをベースに異なるインターネットドメイン間で利用者情報や認可情報を共有・交換する規格である。利用者が利用するサービスとユーザー認証を行うサービスでIDを連携しておき，利用者が認証サービスで認証を受けると，認証結果が発行される。利用者は，利用するサービスに対して認証結果を提示すると，認証を行うことなくサービスを利用できる。

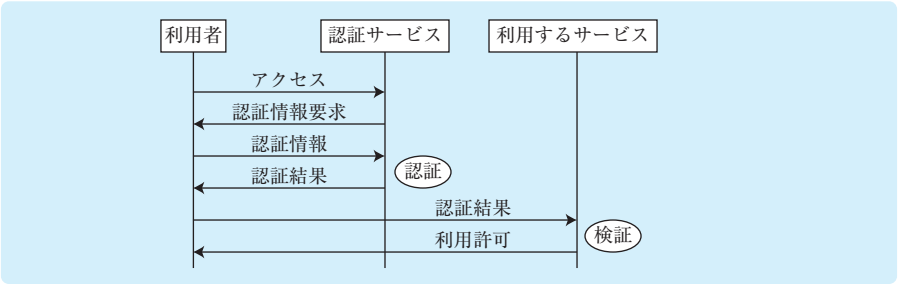


図4.11　SAML

(2)　メッセージ認証

メッセージ認証とは，改ざんの有無を確認し，メッセージ(データ)の完全性を保証する技術である。その一つであるメッセージ認証符号(MAC：Message Authentication Code)では，送信者が共通鍵と元のメッセージからメッセージ認証符号を生成し，受信者に送付する。受信者は，共通鍵を用いて同じ手順でメッセージからメッセージ認証符号を生成し，受信したメッセージ認証符号と比較する。両者が一致すれば，当事者間で「メッセージは改ざんされていない」ことを確認できるが，否認防止性はもたない。メッセージ認証符号の生成方法はさまざまであるが，共通鍵とハッシュ関数を用いる方法(HMAC)や，ブロック暗号(共通鍵暗号方式)を用いる方法(CMAC)がある。

(3)　デジタル署名

デジタル署名は，データの正当性を保証するための情報(データ)であり，データの作成者を証明し，かつデータが改ざんされていないことを保証する。デジタル署名は，公開鍵暗号方式を用いて次のような手順で生成する。

[1]　送信者側は，送信するデータのハッシュ値(ハッシュ値1とする)を生成する。
[2]　送信者側は，送信者側の秘密鍵でハッシュ値1を暗号化してデジタル署名を生成する。
[3]　デジタル署名（以下，署名という）をデータに付加して受信者側に送信する。
[4]　受信者側は，付加された署名を送信者側の公開鍵で復号し，元のハッシュ値1を得る。
[5]　受信者側は，受信したデータからハッシュ値(ハッシュ値2とする)を生成する。
[6]　受信者側は，ハッシュ値1とハッシュ値2を比較する。両者が一致していれば，データは送信者本人が送信し，かつ，改ざんされていないことが証明できる。

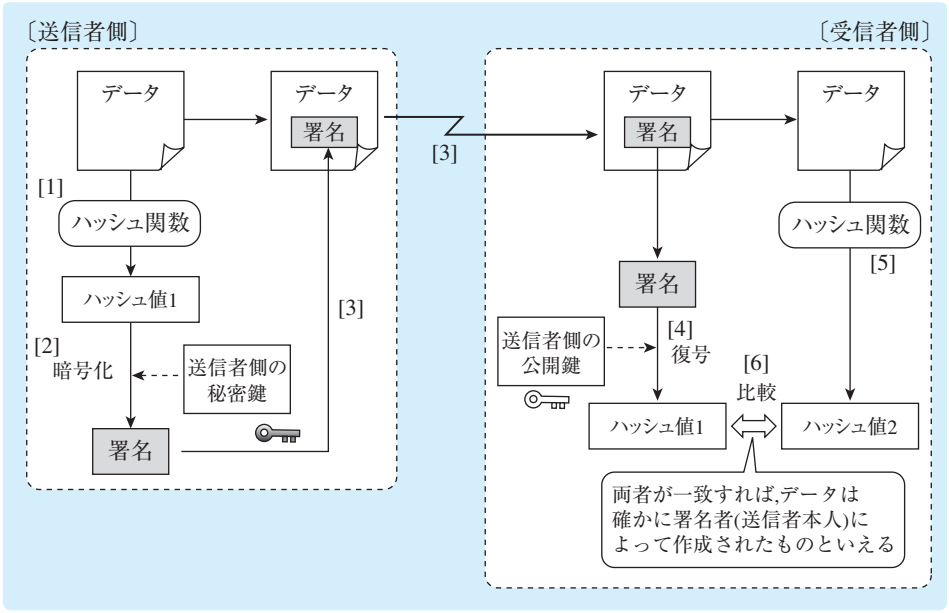


図4.12　デジタル署名

送信者の公開鍵で復号できたということは，送信者の秘密鍵で暗号化された事実を裏付ける。すなわち，デジタル署名はメッセージ認証（データが改ざんされていない）だけでなく，エンティティ認証（誰がそのデータを作成したか）の側面ももつため，否認防止性を実現できる。

なお，送信者の秘密鍵での暗号化は，データの秘匿を目的としていないため，データを秘匿する場合はデータ自体を暗号化する処理が必要となる。たとえば，公開鍵暗号方式でデータの暗号化とデジタル署名を行うのであれば，次のように暗号化を行う。

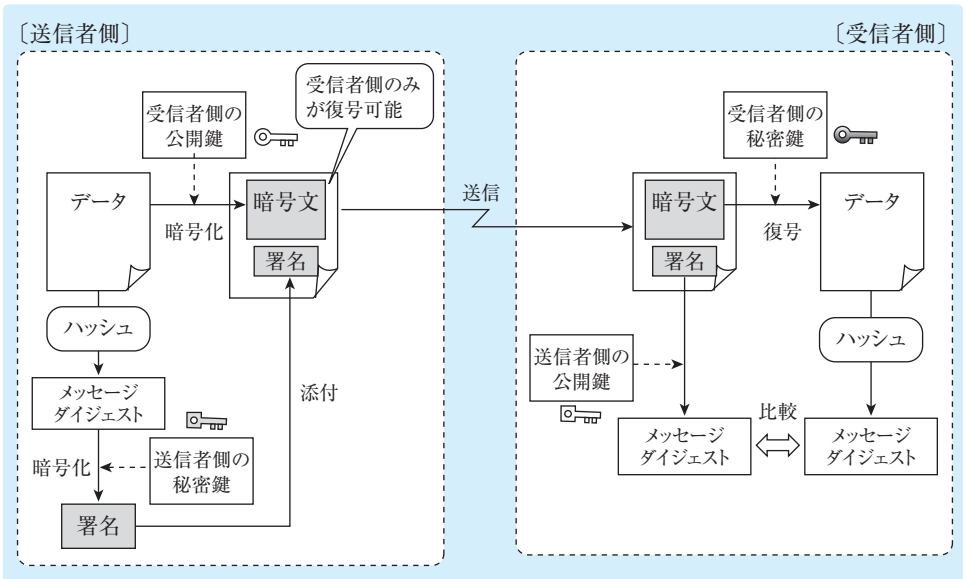


図4.13　デジタル署名と暗号化の組合せ

学習テーマ　4－5
PKI(公開鍵基盤)

●公開鍵暗号方式における問題

公開鍵暗号方式によるデジタル署名では，改ざんの検出や送信者の証明が可能となるが，これは「公開鍵が確かに通信相手のもの」であることが前提となる。仮に，公開鍵そのものを偽造された場合は，公開鍵暗号方式の安全性が覆されることになる。

たとえば，利用者Aと利用者Bの間に，第三者Xが仲介し，AとBの両方にXの鍵を相手の鍵として偽る中間者攻撃(man-in-the-middle Attack)では，XがAあるいはBとして振る舞うことができるため，公開鍵暗号方式自体が無意味となる。

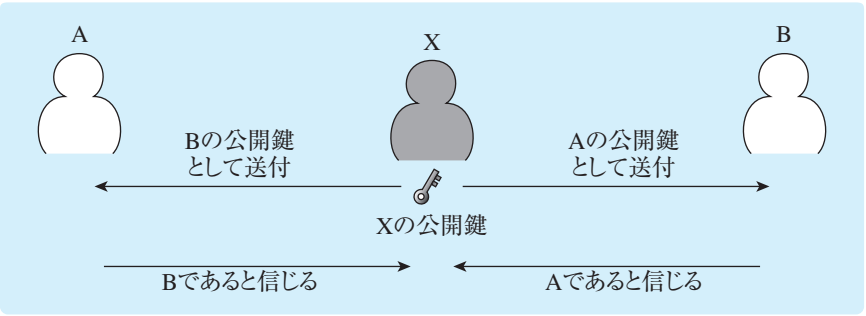


図4.14　中間者攻撃

このため，公開鍵暗号方式では，「公開鍵の正当性」を証明する仕組みが必要になる。

●PKIの概念

PKI(Public Key Infrastructure；公開鍵基盤)は，認証局(CA：Certificate Authority)とよばれる第三者機関がデジタル証明書とよばれる証明書を発行することにより，「この鍵は確かにAさんの公開鍵である」という公開鍵の正当性を証明する技術である。

PKIは公開鍵の正当性を保証するための基盤(インフラ)に過ぎない。PKIを用いたアプリケーションプロトコルには，SSL/TLS(Secure Socket Layer/Transport Layer Security)やS/MIME(Secure MIME)などがあり，SSL/TLSにおいてはWebサーバの証明書(サーバ証明書)やクライアントの証明書(クライアント証明書)などが用いられる。

> **参考：タイムスタンプサービス**
>
> 信頼できる第三者機関がタイムスタンプ(時刻印)を発行することにより，ある時刻にその文書が存在し，改ざんされていないことを証明するサービスをタイムスタンプサービスという。タイムスタンプサービスにおける第三者機関をTSA(Time-Stamping Authority：タイムスタンプ局)という。

●証明書の形式

PKIにおける証明書は，ITU-Tによって制定されたX.509の規格に沿ったものが多く利用されている。X.509における証明書のフォーマットは次のとおりである。

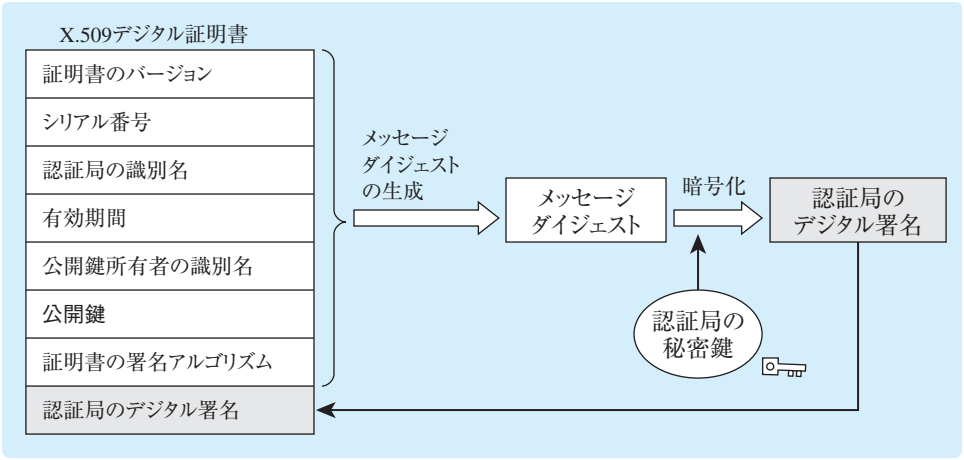


図4.15　デジタル証明書の構成

ここで，証明書のフィールドには，公開鍵や認証局のデジタル署名が含まれている(正確には，公開鍵の部分には使用アルゴリズムなどの情報も付加されている)。すなわち，認証局が署名した(正当性が証明されている)証明書を受け取ることにより，その中に含まれている公開鍵は，間違いなく「証明書に記録されている所有者(ユーザーやサーバなど)の公開鍵」となる。

また，証明書には有効期間（開始時刻と終了時刻から構成される）が設定されており，この範囲内にない証明書は有効とは認められない。

●証明書の発行

サーバに設定する証明書（サーバ証明書）を用意する場合，証明書の所有者は自身のサーバなどで公開鍵と秘密鍵の鍵ペアを生成してからCSR（Certificate Signing Request；証明書署名要求）を生成し，認証局に提出する。CSRには，公開鍵や証明書の所有者を表す情報である識別名(DN：Distinguished Name)が含まれる。認証局はCSRを確認し，正しければCSRに署名し，証明書として返す。

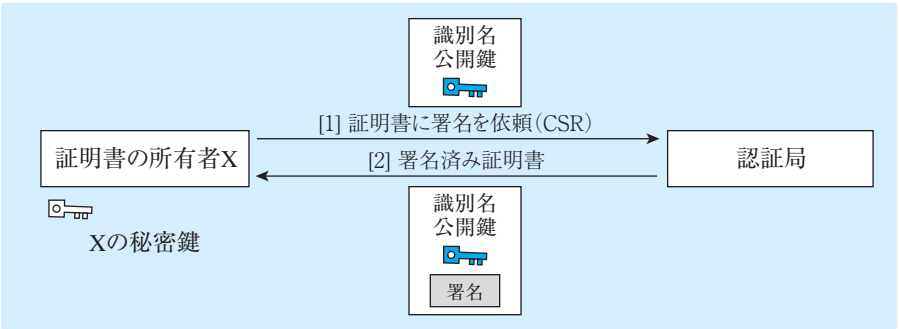


図4.16　証明書の発行

識別名は，次のような項目から構成される。一般名（Common Name）には，サーバのFQDN，IPアドレス，ワイルドカードなどを指定できる。認証局によっては，IPアドレスは指定できないこともある。また，ワイルドカードは同一ドメイン内の複数のサーバに適用可能である。

表4.8　識別名(DN)に含まれる項目

項目	説明	例
Common Name	・FQDN(完全なドメイン名) ・IPアドレス ・ドメイン名のワイルドカード	www.tac-school.co.jp 52.193.x.112 *.tac-school.co.jp
Organization	組織名	TAC Co.,Ltd.
Organization Unit	組織の部署名	Information System
City of Locality	組織の市区町村	Chiyoda-ku
State of Province	組織の都道府県	Tokyo
Country	国	JP

●証明書の検証

WebサーバとPCがSSL/TLSを用いた通信を行う場合など，証明書の利用者（Webブラウザなど）は証明書の所有者(Webサーバなど)から受け取った証明書が信頼できる認証局によって発行されたものかを確認するために，認証局の証明書に含まれる認証局の公開鍵で署名を復号するとともに，証明書のハッシュ値を生成して両者を比較する。一致すれば証明書は有効と判断でき，認証局によって正当性が保証された正しい公開鍵を入手できる。

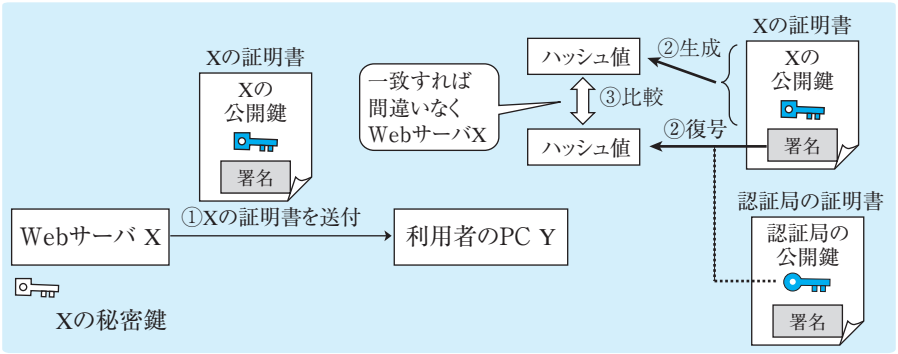


図4.17　証明書の利用

また，証明書の利用者は，証明書の有効性だけでなく次のような内容も確認する。

・信頼できる認証局によって署名されているか
・アクセス先がコモンネームと一致しているか（正しいサーバか）
・有効期間内か
・証明書が有効か（失効していないか）

一般的に信頼できるとされる商用認証局の証明書は，PCなどの機器に設定されているため，改めて入手する必要はなく，意識せずに使用することができる。一方，独自に設置したCAサーバ（プライベート認証局）によって発行された証明書は，信頼できる認証局として登録されていない。このため，プライベート認証局を利用すると警告が表示されてしまう。手順書などで証明書をインストールさせる方法もあるが，不特定多数を対象としたシステムには適さない。

●証明書の失効

証明書の有効期間内であるにも関わらず，証明書の内容を変更する必要が生じた場合，新しい内容の証明書を発行するとともに，古い証明書が使われ続けないよう無効とする必要がある。これを失効という。主な失効事由には，次のようなことが考えられる。

・記載内容（ドメイン名など）の変更
・鍵ペアの再発行（秘密鍵の紛失や漏洩・危殆化が疑われる場合）

また，入手した証明書が有効であるかを確認するための手段には，次のようなものがある。

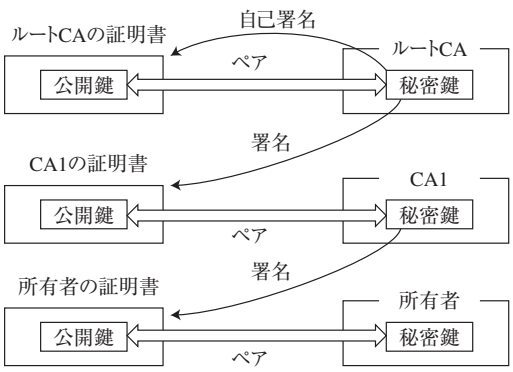
表4.9　証明書の失効状態の確認手段

項目	説明
CRL（Certificate Revocation List; 証明書失効リスト）	失効した証明書のシリアル番号の一覧を記載したリスト。認証局によって定期的に公開される
OCSP（Online Certificate Status Protocol）	オンラインで証明書の有効性をOCSPサーバ(OCSPレスポンダ)に問い合せ，確認するプロトコル

参考：CAの証明書

認証局の証明書はその認証局自身，または他の認証局が署名を行う。他の認証局が署名を行った場合，署名を行った認証局が上位，証明書の発行を受けた認証局が下位の階層構造となる。下位の認証局の証明書を検証するためには，署名を行った上位の認証局の証明書（公開鍵）が必要になる。

そのために上位の認証局をたどっていくと，最終的には最上位の認証局に到達する。この最上位の認証局をルートCA(ルート認証局)という。一般的にはルートCAの証明書は，ルートCA自身が署名を行った自己署名証明書となっている。自己署名証明書を検証する場合は，その認証局が信頼できるものか否かが重要になる。



学習テーマ　4－6

情報セキュリティ対策

情報セキュリティ対策は，人的セキュリティ対策，物理的セキュリティ対策，技術的セキュリティ対策に大別される。これらは，セキュリティ対策を行う組織によって異なり，その範囲も多岐にわたる。ここでは，その代表的なものを解説する。

(1)　人的セキュリティ対策

人間によるエラー，盗難，紛失，不正行為といったリスクを軽減するためには，各要員が必要とされる能力を備えた上で，情報セキュリティポリシーを遵守した行動をとることが求められる。このためには，次のような対策が重要であり，教育や訓練は特に重要となる。

・情報セキュリティ上の役割と責任の明確化
・情報セキュリティ遵守の合意と違反に対する懲戒手続きの明確化
・情報セキュリティ教育・訓練啓蒙などの実施
・インシデント発生時における対処マニュアルの作成と遵守

●ソーシャルエンジニアリング

技術的な技法を用いない手口で不正に情報を入手する手口の総称をソーシャルエンジニアリングという。ソーシャルエンジニアリングには，次のような手口がある。

表4.10　ソーシャルエンジニアリングの手口

スキャベンジング（トラッシング）	ごみ箱などの廃棄物の中から情報を入手する手口
ショルダーハッキング	ディスプレイに向かっている正規の利用者の肩越しに情報を盗み見する手口
なりすまし	電話やメールなどで顧客や組織の上層部，管理者などになりすまし，不正に情報を入手する手口

これらは，いずれも人間の不注意や誤認などが原因となっている。記憶媒体を廃棄する場合は回復できないよう破壊する，重要書類は施錠可能なキャビネットなどに保管し施錠する，机の上に書類などを放置せずに片付けておくクリアデスク，離席時にログアウトやスクリーンセーバによるロックなどを行うクリアスクリーンといった，情報セキュリティポリシーに基づいた適切な行動をとるよう教育し，徹底させることが重要となる。

なお，技術的な側面をもつものの，偽りのWebサイトや電子メールを用いて利用者に誤認させる詐欺の一種であるフィッシングなども利用者の心理を利用するという点では同様である。特に，企業組織を狙って電子メールを送り付け，大規模な金銭取引などの不正を引き起こす攻撃はビジネスメール詐欺(BEC：Business E-mail Compromise)と呼ばれる。

●内部不正対策

情報セキュリティは，外部からの攻撃だけでなく組織内で発生する内部不正によっても脅かされる。内部不正は，次に示す三つの要素が揃った際に生まれやすいと言われている。これは不正のトライアングルと呼ばれる。

・機会：不正行為の実行を容易に可能にする機会や環境の存在
・動機／プレッシャー：不正行為を働くことに至った事情やプレッシャー
・正当化：働いた不正行為に自らを納得させる自分勝手な理由付け

また，「軽微な不正や犯罪を放置すると，より大きな不正や犯罪を引き起こす要因となる」という，割れ窓理論と呼ばれる考え方などもある。内部不正対策はこれらの要素を考慮しながら策定する。IPAでは組織における内部不正防止ガイドラインを策定し，内部不正防止の基本原則として次の五つを挙げている。

・犯行を難しくする(やりにくくする)
・捕まるリスクを高める(やると見つかる)
・犯行の見返りを減らす(割に合わない)
・犯行の誘因を減らす(その気にさせない)
・犯罪の弁明をさせない(言い訳させない)

(2)　物理的セキュリティ対策

物理的な脅威には，地震，火災，風水害，落雷，停電，(人間の)不正侵入，妨害，盗難などがある。これらの脅威に対抗するためには，物理的セキュリティ対策が必要となる。

●入退管理

事務所やデータセンターなどの施設において，認可されていない人物からデータやシステムを保護するためには，施設のエリアごとにセキュリティレベルを設定し，レベルごとに入室できる従業員を限定するなどの対応を行うのが望ましい。この際，各エリアは鍵やICカードまたは生体認証などで制御された出入口，セキュリティゲート，有人の受付といった物理的なセキュリティ境界で分離する。

各セキュリティ境界では入退管理策を行い，入退室の事実を記録・維持すると共に，すべての利害関係者や訪問者に，目に見える形の証明書(バッジや許可証など)の着用を要求するなどの仕組みが重要となる。各エリアの中ではセキュリティレベルを考慮し，画像や音声の記録装置は認可されたものを除いて使用を許可しない，監督されていない作業を禁止する，書類などが持ち出されないよう透明なバッグを貸与してそれ以外は禁止する，といった作業に関する方針や手順を必要に応じて設計する。

また，入退室時に認証を採用している環境であっても，一人分の認証だけで複数人が一緒に入室または退室をすると，記録にない入室や退室が発生してしまう。これを共連れという。共連れでの入室は，許可されていない不審者の入室を許してしまい，機密情報の漏洩につながる。共連れを抑止・低減する仕組みの一つに，

「入室記録がない利用者については，退室を許可しない」
「退室記録がない利用者については，再入室を許可しない」

という制御を行うものがある。これをアンチパスバックという。

また，インターロックゲート(サークルロック)などと呼ばれる機構を導入することもある。これは扉を二重構造にして，確実に一人ずつしか通さないようにするものである。

> **参考：物理的なデータの不正入手**
>
> 物理的にデータを傍受するための代表的な方法には，通信機器などに不正に傍受用の機器を取り付ける方法がある。このため，通信機器はラックなどに入れて施錠することが望ましい。また，コンピュータや周辺機器から漏洩する微弱な電磁波を傍受する手口をテンペストという。テンペストの対策としては，ケーブルや筐体の電磁シールド強化，部屋そのもののシールド化などによる電磁波の遮断を行う。
>
> この他にも，暗号アルゴリズムを実装した攻撃対象の機器から処理時間や消費電力といった物理量を測定し，その装置内の秘密情報を推定する攻撃もある。このような攻撃をサイドチャネル攻撃という。サイドチャネル攻撃への対策としては，演算の必要がないタイミングでダミーの演算を行い，本来の演算時の物理量を隠ぺいするなどの方法がある。

●装置のセキュリティ対策

資産の損失，損傷，盗難，妨害活動，災害といった物理的なリスクから資産を保護するために，装置や設備(電源，空調，給排水など)に関する有効な管理策には，次のようなものがある。

表4.11　装置のセキュリティ対策

障害対策	システムの二重化やミラーリング，バックアップセンターの配置，バックアップコピーの取得など
盗難対策	盗難防止ワイヤー(セキュリティワイヤー)やのぞき見防止フィルタの取付け，補助記憶装置の暗号化など
災害対策	耐震耐火設備の導入，電力線への避雷器取付けなど
サポート設備の障害対策	電力線や通信回線の保護，電源系統や通信路の二重化，UPS や発電装置の設置，給排水設備や空調などの定期的な点検など
機器の処分対策	記憶装置に記録された情報やソフトウェアの確実な消去，記憶装置の物理的な破壊など

(3)　技術的セキュリティ対策

不正アクセス，盗聴，なりすまし，改ざんといった技術的脅威から情報やシステムを保護するための管理策(あるいは技術)は非常に多岐に渡る。ここでは，その一例を紹介し，具体的なセキュリティ実装技術については，次の学習テーマ以降で解説する。

表4.12　技術的セキュリティ対策

クラッキング対策	情報システムを不正な利用から保護するための要塞化，トラステッド OS (詳細は後述) の利用など
盗聴対策	通信回線上を流れる情報の盗聴から保護するセキュリティプロトコル (SSL/TLS，S/MIME など) の利用，記憶装置に格納された情報の不正閲覧から保護するための暗号化など
なりすまし対策	情報システムを認可されていないアクセスから保護するためのアクセス制御，正当な利用者のみとの通信を許可するセキュリティプロトコルの利用など
ネットワークセキュリティ	ネットワークを介した不正アクセスを遮断するためのファイアウォールの利用，侵入検知など
マルウェア対策	情報システムをコンピュータウイルスを代表とする不正プログラム (マルウェア) から保護するための対策，OS アップデートなど

組織としての情報セキュリティ対策に関連する言葉としては，次のようなものもある。

BYOD(Bring Your Own Device)：従業員個人が所有しているスマートフォンやタブレット端末などの情報機器を業務に活用すること。リスクを考慮して慎重に導入する必要がある

シャドー IT：従業員個人や部署などが，情報システム部門などの許可を得ずに導入・利用している機器やサービス

DLP(Data Loss Prevention)：ミスや不正による情報の紛失・漏えいを防止する仕組み及びソフトウェアの総称。コンピュータシステムに記録された情報の機密度や重要度を識別し，規則に違反する行為があった場合には警報を発し，操作を中断するなどの措置を行う

MDM(Mobile Device Management)：スマートフォンやタブレット端末などのモバイル機器を業務で利用する際に，一元的に管理する仕組み

デジタルフォレンジックス：インターネットやコンピュータに関する犯罪や訴訟があったときに，法的な証拠となり得るサーバの履歴や通信内容などのデータを保全，収集して分析すること，及びそのための技術

SIEM(Security Information and Event Management)：さまざまな機器で個別に取得されたログを一元的に収集・管理して分析する仕組み

EDR(Endpoint Detection and Response)：PC などの組織ネットワークの末端にある機器上で動作や状態をリアルタイムで監視し，異常な動作や既知の脅威を検出すると記録や警告を行う仕組み

学習テーマ　4－7
不正アクセス対策

情報の不正な閲覧や改ざん，システムの破壊，資源の不正な利用などを行うために，情報システムへ不正に侵入する手口には次のようなものがある。これらの中で行われる攻撃対象となるPCやサーバ，ネットワークなどの情報を得ることをフットプリンティングという。

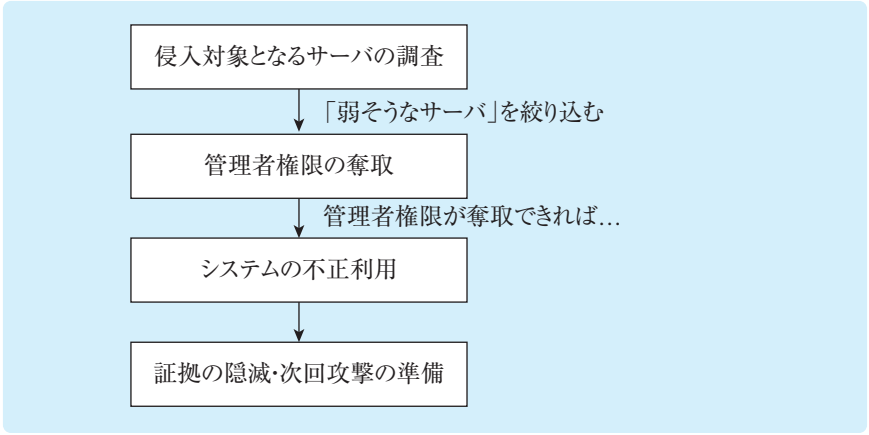


図4.18　不正アクセスの手口

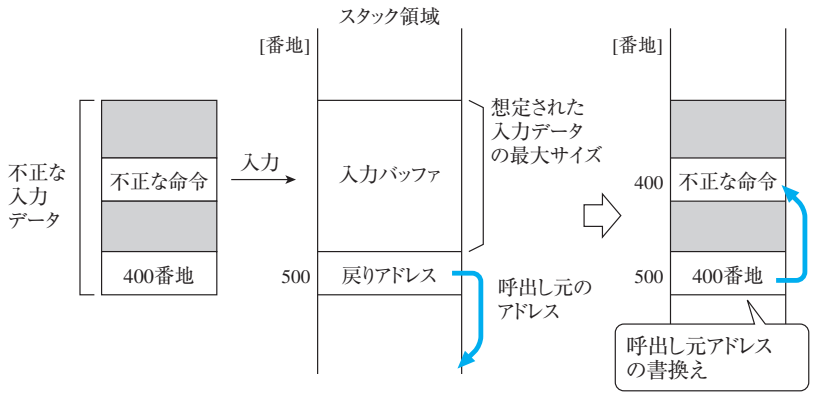
表4.13　不正アクセスの手口

侵入対象となるサーバの調査
侵入者は，最初に侵入対象となるサーバのIPアドレスやポート番号(提供しているサービス)を調査する。この行為をポートスキャンという。この結果，攻撃対象のサービスがあれば，そのサービスを提供するプログラムの種類やバージョンを調査し，既知の脆弱性を探す。
管理者権限の取得
サーバの調査が終了すると，管理者(rootなど)の権限を奪取するための攻撃を行う。この際，エクスプロイトキットとよばれる，OSやサーバプログラムの脆弱性を悪用した攻撃ツールなどが用いられる。なお，ソフトウェアなどの脆弱性を利用するために作成されたプログラムをエクスプロイトコードという。ソフトウェアの脆弱性を悪用して攻撃するために用いられるが，使い方によっては脆弱性を検査・検証するために用いられることもある。
システムの不正利用
管理者権限が奪取されると攻撃者はシステムを操作し，情報の不正な閲覧・改ざん・破壊，ソフトウェアの改変，システムの破壊，踏み台（資源やシステムの不正な利用）といった不正行為を行う。
証拠の隠滅
攻撃者は，ログの消去，改ざんといった証拠の隠滅を行う。このため，侵入後のアクセスログは信用できないものとなる。また，次回以降の侵入に備えた準備を行う。正規のアクセス手段を用いずにシステムに侵入するためのプログラムや設定などをバックドアといい，バックドアの作成や侵入した痕跡の隠蔽といった機能がパッケージ化された不正なプログラムを，ルートキット（rootkit）という。

参考：バッファオーバーフロー

管理者権限を奪取するための手法の一つに，バッファオーバーフローがある。バッファオーバーフローとは，用意された入力バッファのサイズを越える長大なデータを入力し，入力バッファをあふれさせて任意の処理を実行させる攻撃である。

たとえば，プログラムの局所変数はスタック領域に確保され，スタック領域にはそのプログラム(関数)が終了したときに制御を戻す「戻りアドレス」も記録されている。このような状態で入力バッファのサイズを超えるデータを入力すると，入力データは入力バッファを越えて戻りアドレスも書き換えてしまう。この際，戻りアドレスに不正な処理を記述すれば，その処理を実行できてしまう。



このように，入力処理におけるデータサイズのチェックに不備があるとバッファオーバーフローの脆弱性が発生するため，入力データのサイズをチェックすることが重要になる。また，バッファオーバーフローに限らず，OSやサーバプログラムなどの脆弱性が発表されたときは，速やかにセキュリティパッチを適用して最新の状態に保つ必要がある。

ロッキード・マーティン社は，サイバー攻撃が実行される流れを以下のような7段階にモデル化し，サイバーキルチェーンと名付けている。個々の攻撃手口を各段階に位置づけて考察することで，攻撃者の意図を把握しやすくなり，全体的な見通しがよくなることを目的としている。

1　偵察　…攻撃対象となる企業組織の事情を調査する
2　武器化　…　マルウェアなどの準備を行う
3　配送　…　メール配信やWebサイトの改ざんなどを行う
4　エクスプロイト　…　メール開封やWebアクセスによってマルウェアに感染させる
5　インストール　…　管理者PCなどにバックドアを設定する
6　遠隔操作　…　C&Cサーバなどによる操作，ファイルへの不正アクセスなどを行う
7　目的の実行　…　顧客情報などの盗み出しを行う

●ゼロデイ攻撃

脆弱性が発見されてからセキュリティパッチが提供されるまでの間に攻撃する手法や，ベンダーも知らない未知の脆弱性を発見して攻撃する手法をゼロデイ攻撃という。ゼロデイ攻撃は防御すること自体が困難であるため，ベンダーが一時的な回避策を提示していれば，回避策の導入を検討する必要がある。

●サーバの要塞化

不正アクセスの手口を考慮すると，ネットワークを介した攻撃に対しては，不要なサービスは停止して攻撃の機会を増やさないことや，脆弱性を解消するための修正プログラム(セキュリティパッチ)の公開情報を定期的に収集し，適用しておくことが重要になる。これらのサーバ単体でのセキュリティを強化することを，サーバの要塞化という。

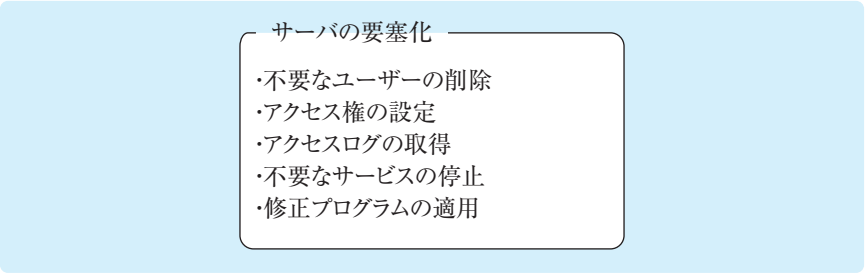


図4.19　サーバの要塞化

特に，アクセスログは，侵入の兆候の発見や侵入された場合の侵入経路の確認，影響範囲の特定などを行うために重要となる。攻撃者によってログが消去されないよう制御するとともに，複数の機器のログを取得する際には，NTP(Network Time Protocol)によって各機器の時刻を合わせておく必要がある。記録されたログの時刻がずれていた場合，事象の前後関係を把握することが困難になってしまう。

●トラステッドOS

セキュリティを強化したOSのことをセキュアOSといい，中でもTCSEC(CCのベースとなった規格の一つ)で定められた一定の基準を満たすOSをトラステッドOSという。トラステッドOSに求められる代表的な機能を次に示す。

表4.14　トラステッドOSの機能

強制アクセス制御	ファイルやデータの所有者であっても，システムのセキュリティポリシーに従ったアクセス権しか与えず，アクセス権限の変更も許可しない機能。MAC(Mandatory Access Control)ともいう
機密ラベル	プロセスやファイルなどに機密度を割り当て，機密度の大小関係でアクセス可否を判断する機能。強制アクセス制御に用いられる
最小特権	従来は管理者(rootなど)に集中していた権限を，プロセスなどの単位で細分化する概念。攻撃者が管理者権限を奪取しても，必要以上の操作が行えない
監査機能	利用者の認証失敗やアクセス権限違反といったイベントをログとして記録し，利用者の操作やアクセスの履歴を追跡可能にする機能

参考：TPM

TPM (Trusted Platform Module）は，データの暗号化や鍵の生成，ハッシュ演算といった機能をもつセキュリティチップであり，PCなどの機器に搭載される。TPMを利用することによって，端末の識別や内蔵ストレージの暗号化などを安全に実現できる。