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あり，従来のソフトウェア開発技術者試験(SW)の後継に位置付けられる試験です。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情報処理技術者講座

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)　情報セキュリティの定義

●情報セキュリティとは

情報セキュリティ関連の規格であるJIS Q 27001では，情報セキュリティとは，「情報の機密性，完全性及び可用性を維持すること」と定義されている。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

機密性 (Confidentiality)	認可されていない個人，エンティティまたはプロセスに対して，情報を使用不可または非公開にする特性
完全性 (Integrity)	資産の正確さ及び完全さを保護する特性
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

すなわち，組織がもつ情報を資産(情報資産)として捉え，事業の継続や事業リスクの最小化，事業機会の最大化などを目的として，電子的あるいは物理的に保管，伝達，表示された情報資産の機密性，完全性，可用性を保つことが情報セキュリティであるといえる。

参考：AAR

JIS Q27001では，情報セキュリティは「さらに真正性，責任追跡性，否認防止及び信頼性のような特性を維持することを含めてもよい」とされており，これらは情報セキュリティ関連の規格であるJIS Q 13335-1では，次のように定義されている。

真正性 (Authenticity)	ある主体又は資源が,主張どおりであることを確実にする特性
責任追跡性 (Accountability)	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 (Non-Repudiation)	ある活動又は事象がおきたことを,後になって否認されないように証明する能力
信頼性 (Reliability)	意図した動作及び結果に一致する特性

これらの真正性，責任追跡性，信頼性の頭文字をとって，AARともいう。

●脅威と脆弱性

予期しない，または望まない情報セキュリティを脅かす可能性が高い出来事(イベント)をインシデント(あるいは情報セキュリティインシデント)という。サービスの停止や設備の故障，過負荷状態，人為的なエラーなどがインシデントに該当する。

このインシデントの潜在的な原因を脅威という。脅威は，人為的脅威と環境的脅威に分類される。人為的脅威は人間の行為によって発生し，さらに偶発的脅威と意図的脅威に分類できる。偶発的脅威は，偶然発生する脅威であり，エラーや不注意などが該当する。意図的脅威は盗難や不正利用といった，人間により故意に行われる脅威を指す。環境的脅威は，自然災害や経年劣化による故障といった環境によって自然に発生する。

一つ以上の脅威が利用する弱点のことを脆弱性という。たとえば，施錠されていないドアやスプリンクラのない建物，エラーチェック機能のないプログラム，アクセス制御機能をもたないシステムなどのほか，プログラムの実装あるいは設計上のバグといったセキュリティホール，個人に対する行動規範の不備といった人為的脆弱性などが該当する。

情報資産の脆弱性に対して脅威が発生することにより，組織に損害を与える可能性が生じる。これをリスクといい，発生確率と影響度の組合せによって評価できる。情報セキュリティにおいては，リスクを適切に評価し，管理策を講じることが重要となる。

> **参考：脅威の分類**
> 脅威は，技術的脅威，人為的脅威，物理的脅威に分類されることもある。

(2)　情報セキュリティマネジメント

●ISMSのプロセス

保護すべき情報資産のCIA(AARなども含む)をバランス良く維持し，継続的に改善する一連の管理活動を情報セキュリティマネジメントといい，この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)という。情報セキュリティマネジメントシステムの規格であるJIS Q27001ではPDCAモデルを採用しており，情報セキュリティ要求事項や期待に基づき，必要な活動やプロセスを経て情報セキュリティを達成し，維持するとともに，情報セキュリティ管理体制に継続的な改善の機会を提供する。

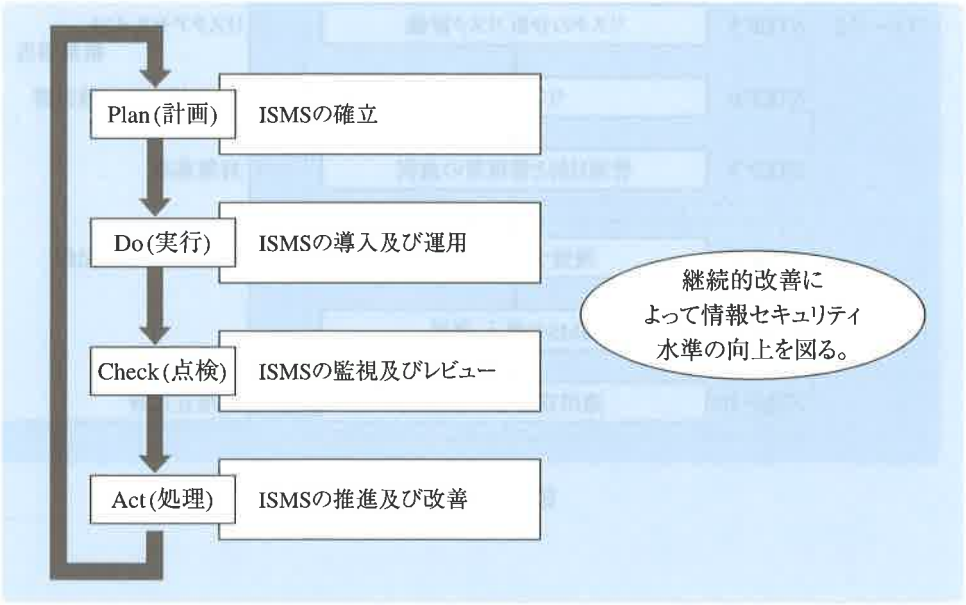


図4.1　ISMSのプロセス

これらの各プロセスにおいて，経営陣がISMSの構築・運用に関与することは企業統治(コーポレートガバナンス)の観点からも重要であり，組織として情報セキュリティの実施責任を宣言するコミットメントや経営資源の提供，各種文書の承認，実施状況の確認などを行う必要がある。

> **参考：ISMS適合性評価制度**
>
> 日本情報処理開発協会(JIPDEC)が運用しているISMS適合性評価制度では，その組織がISMSを適切に維持・運用しているか否かを第三者機関(認証機関)が客観的に評価し，認証する。組織はISMS認証を取得することにより，対外的な信頼性の確保や事業競争力の強化などが期待できる。また，この認証業務を行っている認証機関には，認証業務を遂行するにあたり，適格かつ信頼できると承認されるための認定基準がある。

●ISMSの確立

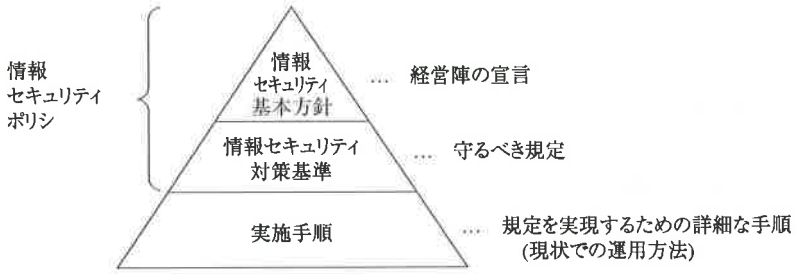
このプロセスでは，適用範囲と基本方針の定義(フェーズ1)，リスクマネジメント(フェーズ2)，リスクに対応する計画の策定(フェーズ3)といった形でISMSを確立する。ここでは，脅威や脆弱性を洗い出し，対応策を検討するリスク管理(リスクマネジメント)が重要になる。リスク管理の詳細については次節で解説する。

図4.2　ISMSの確立

ここで作成される基本方針，対策基準は情報セキュリティポリシともよばれ，ISMSのプロセスを実施する上での中核となる。

参考：情報セキュリティポリシの階層モデル

情報セキュリティポリシは，階層構造で考えることが多い。階層の構成にはいくつかのモデルがあるが，本書では次のような2階層ポリシモデルを前提とする。



参考：基本方針と対策基準の違い

基本方針には，情報セキュリティの目標及び原則を支持する経営陣の意向，リスクマネジメントを含め管理目的・管理策を設定するための枠組み，情報セキュリティマネジメントにおける責任の定義といった，組織が情報セキュリティに取り組むための基本的な方針(何をどのような脅威から，なぜ保護するのか)が盛り込まれる。

一方，対策基準は基本方針をどのように実現すればよいのか，といった観点から遵守すべき行為や判断の基準などを規定したものであり，次のような内容が盛り込まれる。

- 組織・体制
- 情報の分類と管理
- 物理的セキュリティ
  - 入退室管理
  - 施錠管理
- 人的セキュリティ
  - 教育・訓練
  - 事故や欠陥に対する報告
  - パスワードの管理
- 技術的セキュリティ
  - システムの管理
  - アクセス制御
  - システムの開発・導入・保守等
  - コンピュータウイルス対策
- 運用
  - 情報システムの監視及びポリシーの遵守状況の確認
  - 侵害時の対応策
- 法令遵守
- 情報セキュリティに関する違反に対する対応

参考：事業継続管理

組織が情報システムの重大な障害や大規模災害といった危機に直面した場合，事業活動や業務プロセスの中断など，事業の存続が危うくなる。このような危機に備え，要求された時間内に情報処理施設あるいは情報資産の損失を受容可能なレベルまで回復し事業を継続することが求められる。ISMSにおいても，事業継続計画(BCP：Business Continuity Plan)の策定・導入・運用・検証といった事業計画管理(BCM：Business Continuity Management)の概念が取り入れられている。

なお，事業継続計画と似た概念に，緊急時対応計画(コンティンジェンシープラン)がある。どちらも緊急事態の発生に備えて対応計画を策定する点は同じであるが，緊急時対応計画が緊急事態が発生した直後の行動を想定した計画であるのに対し，BCPは業務プロセスのインパクト(影響度)分析を行った結果に基づく総合的な計画である点が異なる。

●ISMSの導入及び運用

このプロセスでは，リスク対応計画の策定・実施，教育・訓練の実施，ISMS運用の管理，インシデントへの対応などが行われる。

・リスク対応計画の策定・実施

基本方針や対策基準に基づき，選択した管理目的及び管理策について，スケジュールや優先順位，詳細な作業計画，責任者などを計画し，資源，責任などを割り当てて実施する。このとき，管理策の運用の手順やインシデント対応手順などを文書化し，周知する。

・教育・訓練の実施

ISMSは，人の手によって確立・導入・運用・維持される。したがって，経営陣は要求される業務を実施できるような対策を行う責任がある。このためには，ISMSと関連する要員に必要な力量を決め，その力量がもてるような訓練・教育などの処置を実施する。また，処置の有効性を評価し，要員が保有する技能，経験，資格，実施した教育・訓練に関する記録を維持する。

・ISMS運用の管理

管理策を適切に実施するための手順や監視方法を策定し，手順書として文書化する。これに含まれる監視方法に基づいた監視が行われ，内部監査などでも用いられる。

・インシデント対応

インシデントに対応するための手順，責任者，報告体制などを策定し，手順書として文書化する。報告時に用いる報告書には，インシデントが検出された場合のインシデントの記録，管理策の問題点，処置内容，追加すべき管理策などが必要であり，これらの情報が後のマネジメントレビューのインプットとなる。

●ISMSの監視及びレビュー

このプロセスでは，内部監査の結果やインシデント報告，利害関係者からのフィードバックといったマネジメントレビューに必要な情報を収集し，経営陣がマネジメントレビューを行ってISMSの有効性や経営資源の割当て，セキュリティ計画の見直しなどを行う。

●ISMSの推進及び改善

このプロセスでは，是正処置や予防措置といった改善策を実施するとともに，講じた処置をすべての利害関係者に伝達した上で，合意を得る。

(3)　情報セキュリティマネジメントに関連する国際規格

●JIS Q 27001，JIS Q 27002

JIS Q 27001，JIS Q 27002は情報セキュリティマネジメントに関する規格であり，

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：情報セキュリティマネジメントの実践のための規範

が規定されている。これらは，BS7799という英国の標準規格がISOによって国際標準化され，日本工業規格によって国内規格化されている。これらは同一の規格と考えてよい。

BS7799-2　→　ISO/IEC 27001　→　JIS Q 27001

BS7799-1　→　ISO/IEC 17799　→　ISO/IEC 27002　→　JIS Q 27002

なお，ISO/IEC 17799はJIS X 5080として国内規格化されていたが，JIS Q 27002に代わられている。

●ISO/IEC 15408

ISO/IEC 15408は，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。CC(Common Criteria)を国際標準化しており，IT製品の調達において，要件として指定されることもある。

ISO/IEC 15408では，ハードウェア，ソフトウェア，システム全体などが評価対象(TOE：Target Of Evaluation)となり，評価対象ごとに各製品のセキュリティ機能が満足すべきセキュリティ要件などを記述したST(Security Target)として作成する。このとき，必要に応じて，ある分野の製品が備えるべき実装に依存しないセキュリティ要件などを記述した要求仕様(PP：Protection Profile)を参照する。

TOEを評価した結果はEAL(evaluation assurance level；評価保証レベル)で表される。EALは，EAL1～EAL7の7段階で表され，上位のレベル(数字が大きい)ほど厳格に評価されたことを意味する(セキュリティ強度が高いという意味ではない)。

> **参考：CEM**
>
> 日本では，製品のセキュリティ機能をISO/IEC15408に基づいて評価機関が評価した結果を認証機関が認証する制度がある。この制度の認証を受けた製品は，同様の制度を運営し，協定に参加する他国においても認証を受けた製品とみなされる。
>
> ISO/IEC15408では，評価する評価機関や制度が異なっても評価結果が異ならないよう，評価対象や判断基準などを明確化した共通の評価方法(CEM：Common Evaluation Methodology)が用いられ，CEMもISO/IEC 18045として標準化されている。

●JIS Q 13335-1

ISOによって規定された技術報告書(Technical Report：TR)のうち，ISO/IEC TR 13335として規定されたITセキュリティマネジメントのためのガイドラインをGMITS(Guidelines for the Management of IT Security)という。GMITSは，情報技術を用いたセキュリティ管理を対象とし，紙媒体なども含むISMSと比べると対象範囲こそ狭いものの，リスク管理の手法やセキュリティの実装などについても言及している。GMITSは次の5部構成で規定されている。

第1部：ITセキュリティの概念及びモデル
第2部：ITセキュリティのマネジメントと計画
第3部：ITセキュリティのマネジメント手法
第4部：セーフガードの選択
第5部：ネットワークセキュリティにおけるマネジメントの手引き

このうち，第1部と第2部を統合した国際標準規格がISO/IEC 13335-1である。これを国内対応させた規格がJIS Q 13335-1(情報通信セキュリティマネジメント 第1部「情報通信セキュリティマネジメントの概念及びモデル」)であり，情報通信技術(ICT：Information and Communications Technology)セキュリティのマネジメントについての手引きが規定されている。

●OECD「情報システムのセキュリティに関するガイドライン」

OECD(経済協力開発機構)では，セキュリティ文化の発展や促進を目的に，「OECD 情報システム及びネットワークのセキュリティに関するガイドライン」を制定している。本ガイドラインは，強制力はないが加盟国が尊重すべき指針を示しており，その九つの原則は情報セキュリティマネジメントの概念を導入している。

表4.2　OECD 情報システム及びネットワークのセキュリティに関するガイドラインの原則

認識 (Awareness)	参加者は，情報システム及びネットワークのセキュリティの必要性並びにセキュリティを強化するために自分達にできることについて認識すべきである。
責任 (Responsibility)	すべての参加者は，情報システム及びネットワークのセキュリティに責任を負う。
対応 (Response)	参加者は，セキュリティの事件に対する予防、検出及び対応のために，時宜を得たかつ協力的な方法で行動すべきである。
倫理 (Ethics)	参加者は，他者の正当な利益を尊重するべきである。
民主主義 (Democracy)	情報システム及びネットワークのセキュリティは，民主主義社会の本質的な価値に適合すべきである。
リスクアセスメント (Risk assessment)	参加者は，リスクアセスメントを行うべきである。
セキュリティの設計及び実装 (Security design and implementation)	参加者は，情報システム及びネットワークの本質的な要素としてセキュリティを組み込むべきである。
セキュリティマネジメント (Security management)	参加者は，セキュリティマネジメントへの包括的アプローチを採用するべきである。
再評価 (Reassessment)	参加者は，情報システム及びネットワークのセキュリティのレビュー及び再評価を行い，セキュリティの方針，実践，手段及び手続に適切な修正をすべきである。

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からなる。

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
リスク分析	リスク因子の特定とリスク算定
リスク因子の特定	リスク因子(脅威と脆弱性の組合せ)を特定
リスク算定	リスク因子が発生する可能性と影響度を検討
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

ISMSの計画(Plan)プロセスでは，

・リスクアセスメントの取組み方法の定義
・リスクの特定
・リスクの分析・リスク評価
・リスク対応，管理目的と管理策の選択

といった各ステップがリスクマネジメントに該当する。以下では，ISMSの計画プロセスに基づき，リスクマネジメントについて解説する。

参考：リスクの種類

リスクには，金融商品のように利益と損失をもたらす可能性がある投機的リスクと，損失のみをもたらす純粋リスクがある。情報セキュリティにおいては，純粋リスクが管理対象となる。

●リスクアセスメントの取組み方法の定義

ここでは，リスクアセスメントの分析手法を選択し，アセスメントの手順や目的，リスク対応の目標や方針，受容可能なリスク水準といった，リスクマネジメントの基準を設定する。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。

●リスクの特定

・資産の識別

ここでは，最初にISMSの対象範囲となっている資産を洗い出し，資産目録を作成する。資産目録には，資産の形態や保管場所，保管期間などに加え，その特性(求められる機密性，完全性，可用性など)や価値も明確にしておくことが望ましい。

参考：リスクの種類

ISMSが対象とする資産には，次のようなものがある。

情報資産	データベース，ファイル，契約書，運用手順，事業継続計画など
ソフトウェア資産	業務用ソフトウェア，開発ツール，システムソフトウェアなど
物理的資産	ハードウェア，記憶媒体など
サービス	計算処理サービス，通信サービスなど
人的資産	人材，保有する資格，技能，経験など
無形資産	会社の評判，イメージ，営業権など

・リスク因子の明確化

続いて，リスク因子を明確化するために，脅威と脆弱性を識別する。脅威は，環境により発生するものと人為的に発生するものがあり，人為的なものは，意図的(故意)によるもの，偶発的なものに分類できる。

表4.5　脅威の例

人間		環境
意図的	偶発的	
盗聴	誤り及び手ぬかり	地震
情報の改ざん	ファイルの削除	落雷
システムのハッキング	不正な経路	洪水
悪意のあるコード	物理的事故	火災
盗難		

JIS Q 13335-1より引用

脆弱性は，それ単体では組織や情報システムに損害を与えることはないが，脅威が加わることによって損害や障害に発展する可能性がある。このため，ここでは，脅威が存在する脆弱性を中心に洗い出す。

表4.6　脆弱性の例

脅威	脆弱性
盗聴	暗号化処理の欠如
誤り及び手ぬかり	エラーチェックの欠如
地震	耐震装置のない建物
ファイルの削除	バックアップの欠如

●リスクの分析・リスク評価

作成した資産目録に基づき，事業上の損害，脅威と脆弱性を評価する。リスク分析の手法には，定性的リスク分析手法と定量的リスク分析手法がある。

・定量的リスク分析手法

定量的リスク分析手法では，識別された資産価値，脅威，脆弱性を評価したうえで，金額などの絶対的な指標を用いてリスク値を評価する。たとえば，次のような年間予想損失額でリスクを評価する方法がある。

年間予想損失額 ＝ 予想損失額 × 発生確率(回数／年)

参考：ALE法

定量的リスク分析手法の一つに，米国商務省標準のALE法がある。ALE法では，年間予想損失額(ALE)を，損失が発生する頻度(f)と一回当たりの損失予想額(i)を用いて，

$$ALE = 10^{(f+i-3)\div 3}$$

として求める。

・定性的リスク分析手法

定性的リスク分析手法は，過去のデータが十分にそろっていないなど，絶対的な評価が難しい場合に有効である。資産，脅威，脆弱性を価値や発生確率，管理策の実施度合いなどに基づいて，点数あるいは「高」,「中」,「低」など，数段階の相対的な指標で評価する。そして，これらの指標を用いて，たとえば，

リスク値 = 資産価値 × 脅威 × 脆弱性

のようにリスク値を算出する。この場合，仮に資産価値が1 ～ 5，脅威が1 ～ 3，脆弱性が1 ～ 3の点数で評価されるのであれば，リスク値は1 ～ 45で評価されることになる。算定されたリスクは，経営陣によって承認されたリスク評価基準(受容可能なリスクの水準)と比較し，受容できる範囲内ではないリスクについて対応を検討する。

なお，事業上の損害は，資産の種類によっても，特性(機密性，完全性，可用性)からも損害を被った時の影響度が異なる。このため，事業上の損害は資産ごと特性ごとに評価することが望ましい。たとえば，企業紹介のホームページであれば機密性が損なわれても影響は小さいが，完全性が損なわれた場合の影響は大きい。

参考：定性的リスク分析の手法

定性的リスク分析手法において，リスクを評価するために用いられる手法には，次のようなものがある。

質問書法	リスクに関する質問を行い，その回答に応じてリスクを評価する。
得点法	質問書法と同様に質問を行い，回答ごとに割り当てられた点数を集計してリスクを評価する。
スレッドシナリオ法	分析チームがブレーンストーミング方式でリスクを洗い出し，評価する。
JRAM(JRMS)	日本情報処理開発協会(JIPDEC)が考案した手法。JRAM質問表と分析シートによってリスクを評価する。
CRAMM	英国大蔵省，英国規格協会(BSI)が考案した手法。質問表を用いて5段階で評価する。

●リスク対応

JIS Q 27001では，リスク対応とは「リスクを変更させるための方策を選択及び実施するプロセス」と定義されている。リスクを変更させるための方策は，リスクが現実化する確率や現実化したときの損害を最小限に抑えるリスクコントロールと，リスクが現実化した場合の資金的な対策を行うリスクファイナンスに大別される。具体的には，次のようなものがある。

表4.7　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，最も多く用いられるのがリスク低減である。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する。したがって，管理策適用後のリスク値は適用前よりも小さくなる。リスク低減においては，受容できる範囲内であることが前提となる。これは，残留リスクとして受容される。

参考：その他のリスク対応

リスク低減は，リスク最適化という名称が用いられる場合もあり，損失予防，損失軽減，リスク分離，リスク集中と，さらに細かく分類されることもある。また，認知されていないリスクも含めて損失額を受容するリスク対応をリスク保有とする考え方もある。

●管理目的と管理策の選択

リスク対応において方策を選択した各リスクに対して，管理目的を明確化する。管理目的は，基本方針に沿ったものでなければならない。また，明確化された管理目的に基づき，どのような管理策を選択するかを検討する。

参考：残留リスクの承認

リスクは，いかなる手段を用いてもリスク値が0になるわけではない。受容リスク水準以下のリスクや，管理策の適用により受容リスク水準以下になるものについては，経営陣が確認し，適切と判断した場合は残留リスクとして承認する。

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。

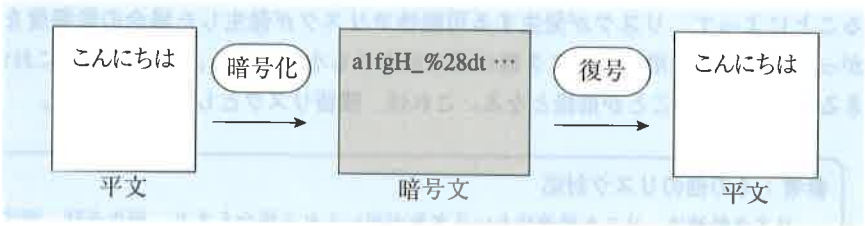


図4.3　暗号化と復号

●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。

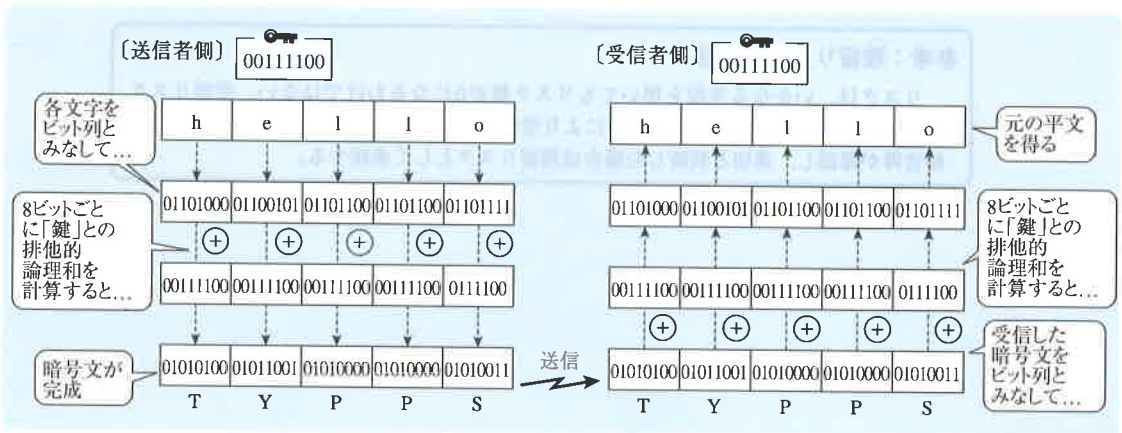


図4.4　暗号化と鍵

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。共通鍵暗号方式は，秘密鍵暗号方式や慣用暗号方式，対称鍵暗号方式などともよばれる。

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として，56ビットの共通鍵を用いるブロック暗号のDES (Data Encryption Standard)，DESの後継規格であるAES(Advanced Encryption Standard)，ストリーム暗号のRC(RC4, RC5, RC6など)などがある。なお，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方式をブロック暗号という。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。

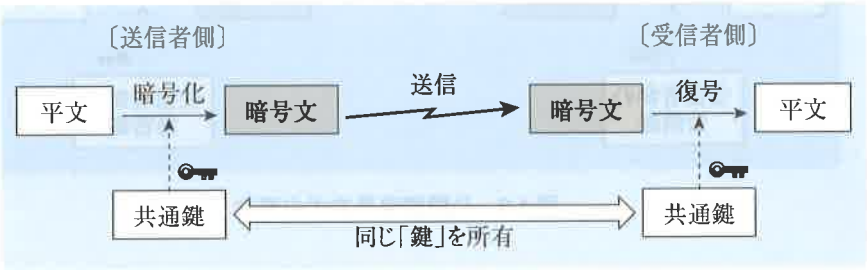


図4.5　共通鍵暗号方式の概念

●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】

共通鍵暗号方式

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。

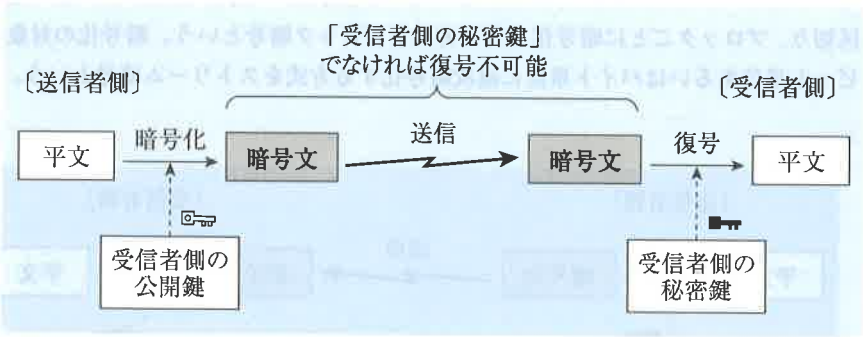


図4.6　公開鍵暗号方式の概念

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】

公開鍵暗号方式の

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し，誰に知られても構わない公開鍵のみを配送する。これにより，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。また，自身の公開鍵を複数の相手が使っても問題がない。したがって，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)を管理すればよく，システム中に存在する鍵の種類は，

$2n$

となるので，鍵の管理が容易となる。このような特徴から，公開鍵暗号方式は，不特定多数と

の通信に適しているといえる。

ただし，公開鍵暗号方式は暗号化や復号の処理時間が長いという特徴をもつため，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】

公開鍵暗号方式

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。

安全な鍵の配送が可能。

(4) セッション鍵暗号方式(ハイブリッド方式)

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4.8 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セッション鍵暗号方式(ハイブリッド方式)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，セッション鍵暗号方式は，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であり，次のような流れで処理を行う。

[1] まず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

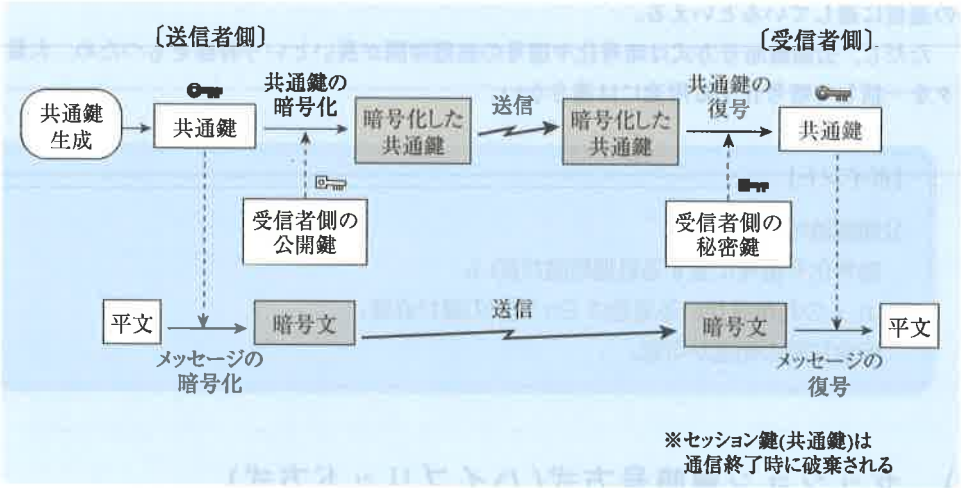


図4.7　セッション鍵暗号方式

【ポイント】

共通鍵を公開鍵暗号方式で暗号化することにより高速かつ安全な暗号化通信を実現
→セッション鍵暗号方式が主流

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ための技術を利用者確認(ユーザ認証)といい，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。

・パスワードを人に教えない。
・パスワードを紙に記録して保管しない。
・極端に短いパスワードは使用しない。
・「良質」なパスワードを使用する(後述)。
・パスワードは定期的に変更し，古いパスワードを再使用しない。
・パスワードの変更や発行時は，仮のパスワードを発行し，初回アクセス時に変更する。
・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。
・アルファベットの大文字・小文字，数字などを混在させる。
・同一文字の繰返しを避ける。
・辞書に記載されるような単語を避ける。

参考：パスワードの解析手法

パスワードを解析するための手法には，辞書に載っている単語をパスワードとして試行する辞書攻撃，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。このため，辞書に載っている単語や短いパスワードは極めて危険といえる。このような解析手法に対しては，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，その利用者ID(アカウント)をロックし，一定期間使用できなくなる機能が有効である。

●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(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(他人受入率)が高くなる。このため，必要に応じてパスワードや持ち物などを組み合わせて利用することが多い。

●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，磁気カードやIC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り，建物への入退室管理やシステムの利用などに多く利用されている。この場合は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。

> **参考：多要素認証**
>
> 複数の異なる認証方式を組み合わせて認証を行うことを多要素認証といい，二つの認証方式を組み合わせたものを二要素認証ともいう。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。

(2)　リモートアクセス環境におけるユーザ認証

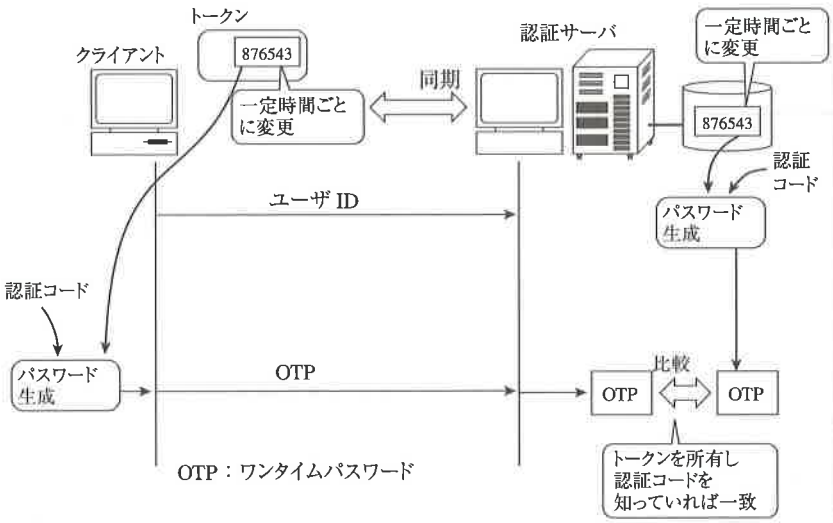
●ワンタイムパスワード

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すると，認証サーバはそれを検証してアクセスの可否を返す。

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されるリプレイ攻撃のおそれがある。そこで，アクセスするごとに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)を利用することが望ましい。

参考：タイムシンクロナス方式

タイムシンクロナス方式(時刻同期方式)は，「トークン」とよばれるハードウェア(あるいはソフトウェア)を用いてワンタイムパスワードを生成する。認証サーバとトークン間では時刻を同期しており，一定時間ごとにトークンに表示されるコードが変更される。利用者はトークンに表示されたコードと，PINコード(暗証番号)などの認証コードから，ワンタイムパスワードを生成し，認証サーバ側でも同様の手順でワンタイムパスワードを生成し，両者を比較する。



●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がある。チャレンジレスポンスでは，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て，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。

チャレンジレスポンス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(ゼロ知識証明という)ため，安全性に優れる。

なお，ポイントツーポイント接続を行うPPPでは，パスワードを平文で送る認証プロトコルであるPAP (Password Authentication Protocol)に加え，チャレンジレスポンスによる認証プロトコルであるCHAP (Challenge Handshake Authentication Protocol) を利用できる。

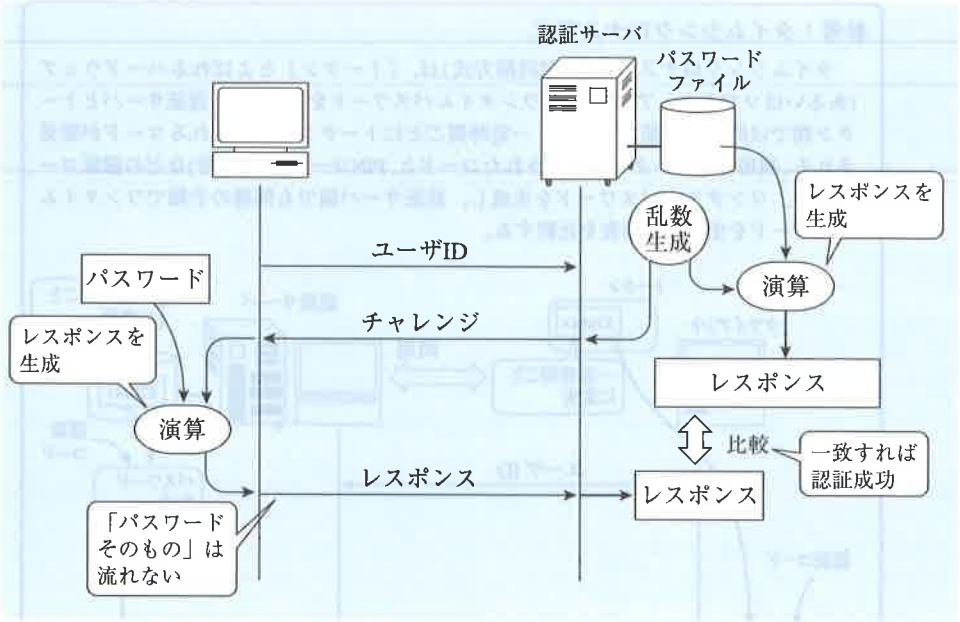


図4.8　チャレンジレスポンス

●RADIUS

負荷の分散などを目的に複数の認証サーバを利用する場合，各認証サーバに同じ認証情報を登録する必要がある。このとき，認証情報を一元管理するサーバを用意すれば運用負荷を軽減できる。このような仕組みにRADIUS（Remote Authentication Dial In User Service）がある。

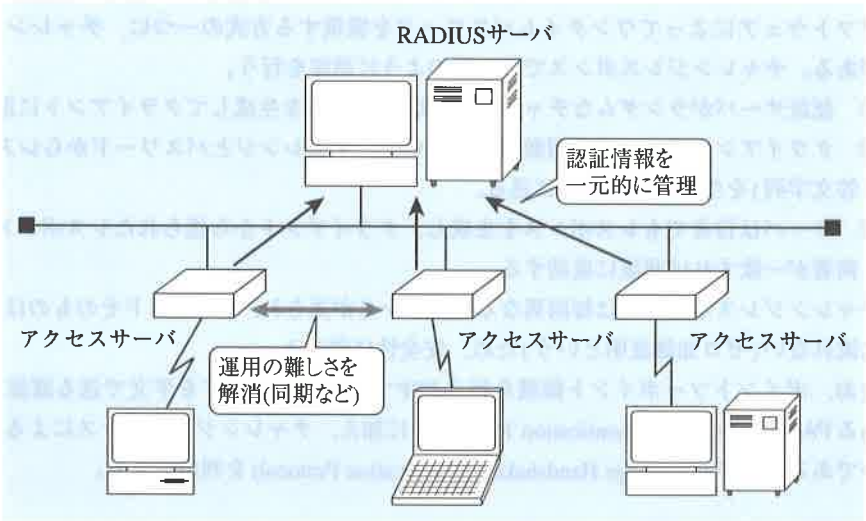


図4.9　RADIUSの概念

RADIUSでは，RADIUSサーバが認証情報を一元管理する。各認証サーバはクライアントから送られてきた認証情報をRADIUSサーバに送り，認証結果を得る。RADIUSを用いた認証の例を次に示す。

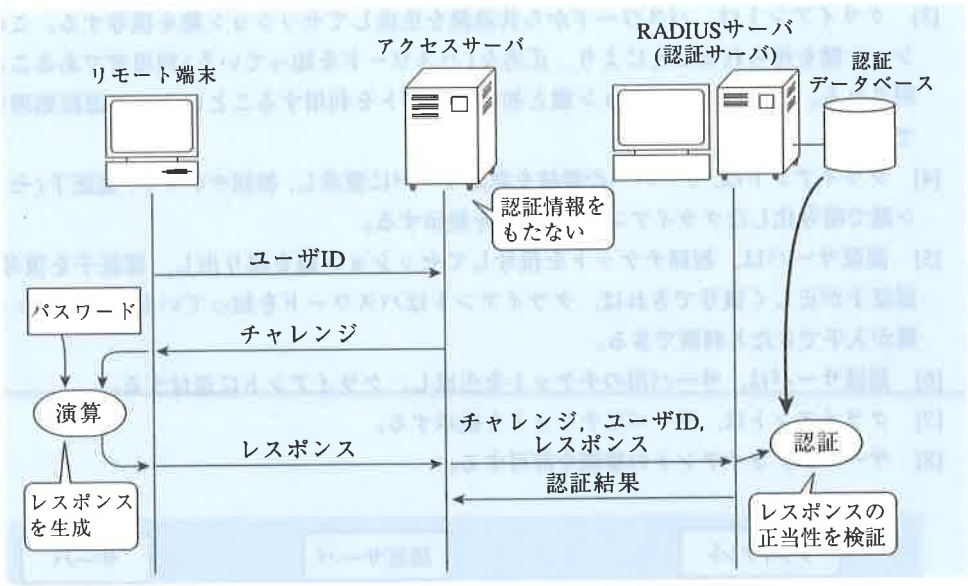


図4.10　RADIUSを用いた認証

参考：AAA

AAAとは，Authentication(認証)，Authorization(認可)，Accounting(監査・課金)の頭文字であり，認証技術において重要な概念となっている。RADIUSはAAAを実現することができるため，さまざまな用途で用いられる。

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
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
監査･課金	接続した内容の記録や課金管理

●Kerberos認証

複数のサーバが存在する環境では，各サーバが認証情報をもち，サーバごとに認証を行うことも多い。しかし，認証情報の一元管理や利用者の負荷軽減の観点からは，認証サーバから一回認証を受けると，その後は各サーバの認証が不要となるシングルサインオン(SSO：Single Sign On)の仕組みが望ましい。シングルサインオンを実現する技術の一つにKerberos認証(ケルベロス認証)がある。

Kerberos認証では，「チケット」とよばれる特殊なデータを用いて次のように認証を行う。

[1]　クライアントが認証サーバに認証を要求する。

[2]　認証サーバは初回チケットとセッション鍵を発行し，クライアントに送付する。セッション鍵は「パスワードから生成できる共通鍵」で暗号化されている。また，初回チケットはセッション鍵やクライアントの情報(名前やアドレス)を暗号化したもので，認証サーバのみが復号できる。

[3]　クライアントは，パスワードから共通鍵を生成してセッション鍵を復号する。このセッション鍵を得られることにより，正当な(パスワードを知っている)利用者であることが証明される。以降は，セッション鍵と初回チケットを利用することにより，認証処理を省略できる。

[4]　クライアントは，サーバへの接続を認証サーバに要求し，初回チケット，認証子(セッション鍵で暗号化したクライアントの情報)を提示する。

[5]　認証サーバは，初回チケットを復号してセッション鍵を取り出し，認証子を復号する。認証子が正しく復号できれば，クライアントはパスワードを知っているためにセッション鍵が入手できたと判断できる。

[6]　認証サーバは，サーバ用のチケットを生成し，クライアントに送付する。

[7]　クライアントは，サーバにチケットを提示する。

[8]　サーバがクライアントの接続を許可する。

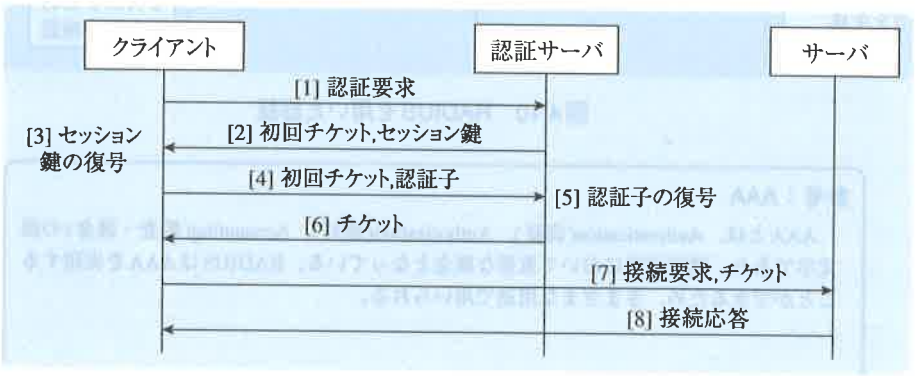


図4.11　Kerberos認証

チケットには有効期限が設定されており，有効期限内であればクライアントは認証サーバに初回チケットを送付するだけで認証処理を行う必要がない。この結果，シングルサインオンを実現できる。なお，実際には，サーバに提示するチケットも「クライアントとサーバ間で共有するセッション鍵」で暗号化されており，Kerberos認証にはクライアントとサーバ間でセッション鍵を共有する仕組みが備わっている。

(3)　メッセージ認証

●メッセージ認証とは

メッセージ認証とは，メッセージ(データ)の完全性を保証するための技術である。メッセージを認証するためには，元のメッセージに認証用の短いデータを付加する。これをメッセージ認証符号(MAC：Message Authentication Code)という。メッセージ認証符号には，共通鍵暗号方式を用いたものとハッシュ関数を用いたものがある。

ハッシュ関数(セキュアハッシュ関数，メッセージダイジェスト関数ともいう)は，次のような特徴をもつ関数である。

・どのような入力値でも出力値のサイズは同一
・出力値から入力値を求めることが困難(一方向性)
・入力値が少しでも変われば，出力値は大きく変わる
・異なる入力値から，同じ出力値を求めることが困難(衝突が発生しにくい)

ハッシュ関数の出力値となるハッシュ値(ビット列)をメッセージダイジェストあるいは単にダイジェストという。ハッシュ関数には，MD-5，SHA-1，SHA-2などがあり，現在ではSHA-2などの利用が推奨されている。

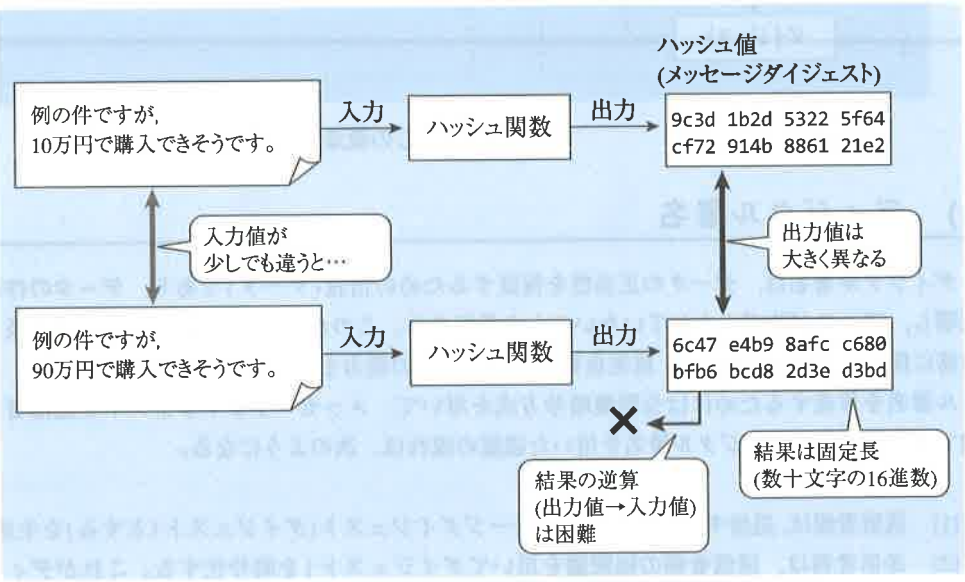


図4.12　ハッシュ関数

【ポイント】

ハッシュ関数の特徴
→出力値から入力値を求めることが困難
→同じハッシュ値をもつ異なるデータを生成することが困難

ハッシュ関数は誰でも生成できるため，単体では改ざんやなりすましを防止できない。そこで，送信者と受信者の双方で共通鍵(MAC鍵ともいう)を共有し，元のメッセージに共通鍵を連結した結果のダイジェストを得る。これをメッセージ認証符号として用いると，共通鍵を知らない第三者は同一のダイジェストを得ることができないため，改ざんやなりすましを検出できる。これをHMAC(Keyed-Hashing for Message Authentication Code)という。

受信側が生成したダイジェストが送信側で生成したものと一致すれば，メッセージは改ざんされておらず，第三者によってなりすまされていないと判断できる。

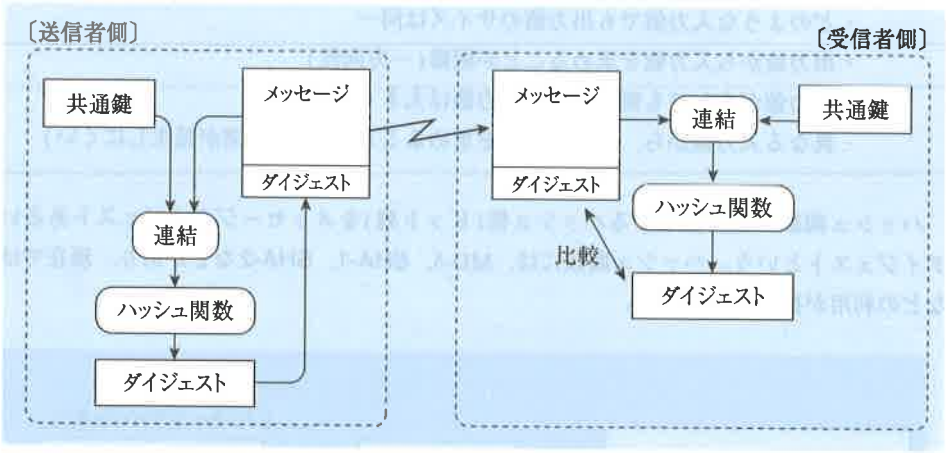


図4.13　HMACの概念

(4)　ディジタル署名

ディジタル署名は，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，データが改ざんされていないことを保証する。このため，電子署名法(電子署名及び認証業務に関する法律)において，現実世界の署名と同様の効力をもつことが定められている。ディジタル署名を作成するためには公開鍵暗号方式を用いて，メッセージダイジェストを送信者の秘密鍵で暗号化する。ディジタル署名を用いた認証の流れは，次のようになる。

[1]　送信者側は，送信するデータのメッセージダイジェスト(ダイジェスト1とする)を生成する。
[2]　送信者側は，送信者側の秘密鍵を用いてダイジェスト1を暗号化する。これがディジタル署名となる。
[3]　署名をデータに付加して受信者側に送信する。
[4]　受信者側は，受信したデータに付加されている署名(暗号化されたダイジェスト1)を，送信者側の公開鍵を用いて復号し，元のダイジェスト1を得る。
[5]　受信者側は，受信したデータからメッセージダイジェスト(ダイジェスト2とする)を生成する。
[6]　受信者側は，ダイジェスト1とダイジェスト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。

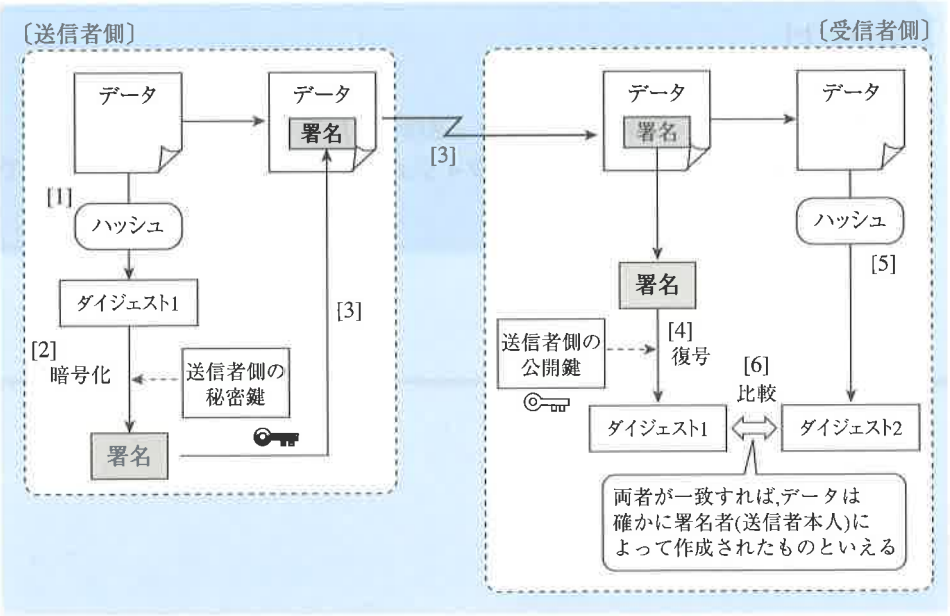


図4.14　ディジタル署名

メッセージ認証符号は第三者のなりすましを防止できるが，メッセージ認証符号を生成するための情報を共有するため，否認防止性をもたない。ディジタル署名では，公開鍵暗号方式を用いており，送信者の公開鍵で復号できたことが送信者の秘密鍵で暗号化されたことを裏付ける。これによりメッセージ認証とエンティティ認証を同時に実現し，否認防止性も実現できる。

なお，ディジタル署名で行う「送信者の鍵での暗号化」はあくまでも送信元を特定するためであり，データを秘匿する目的には使用できない。仮に公開鍵暗号方式でデータの暗号化とディジタル署名を行うのであれば，次のようになる。

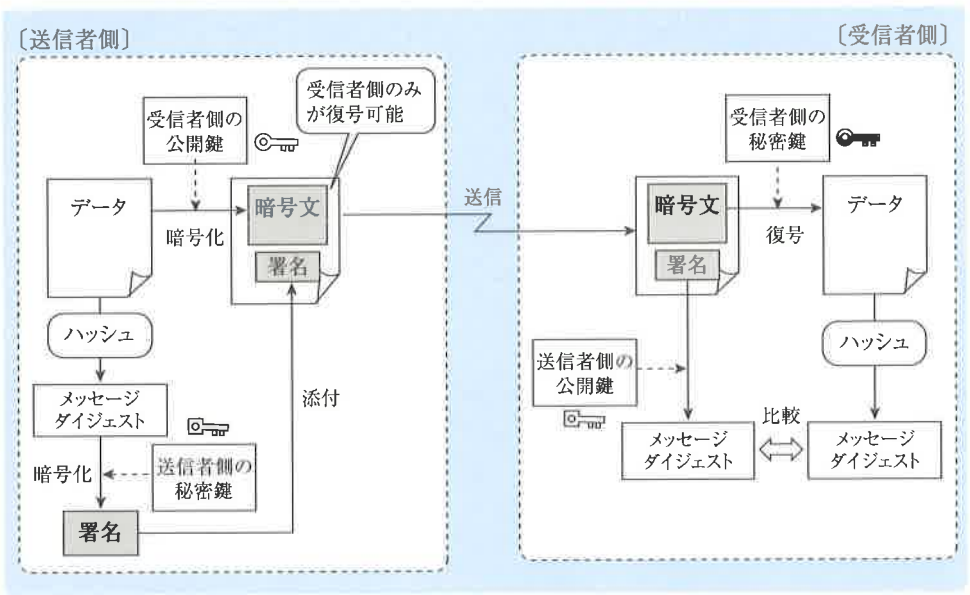


図4.15　ディジタル署名と暗号化の組合せ

【ポイント】

ディジタル署名

・送信者側はメッセージダイジェストを「送信者側」の「秘密鍵」で暗号化

・受信者側は暗号化されたメッセージダイジェストを「送信者側」の「公開鍵」で復号

参考：時刻認証

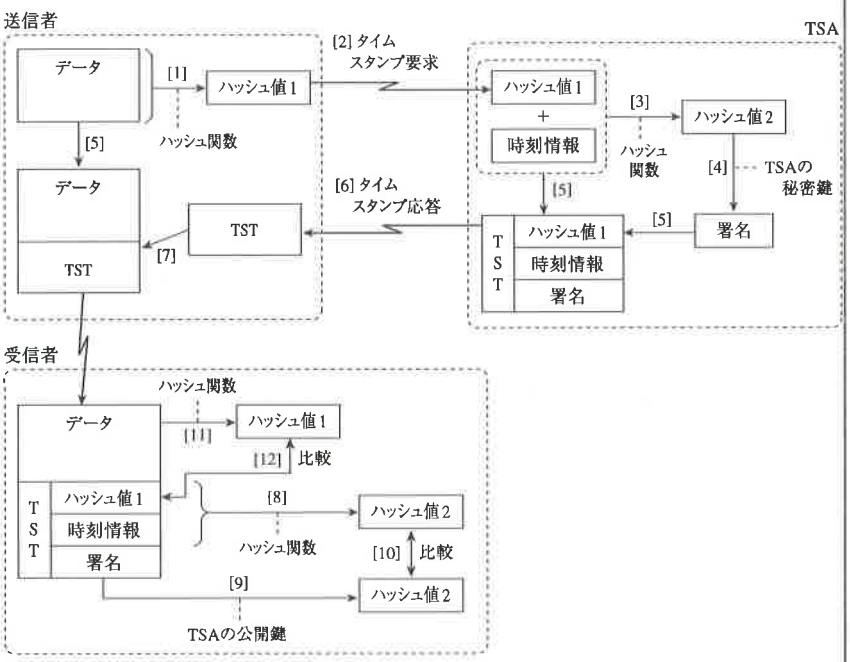
時刻認証は，信頼できる第三者機関がタイムスタンプ(時刻印)を発行することにより，ある時刻にその文書が存在し，改ざんされていないことを証明する技術である。この第三者機関をTSA(Time-Stamping Authority：タイムスタンプ局)という。時刻認証は，文書のディジタル署名と併用することが一般的であり，

タイムスタンプを発行済みの文書に署名：文書はその時刻以降に署名された

署名済みの文書にタイムスタンプを発行：文書はその時刻以前に署名されている

ことが証明できる。

ただし，時刻認証もディジタル署名の技術を応用しているため，時刻認証とディジタル署名を併用した場合は，複数の署名が存在することになる。次に示す時刻認証の手順では，混乱を避けるために文書の署名は省略してある(図中の署名は時刻を認証するためのものであり，文書の署名ではない)。



〔タイムスタンプの取得〕

[1]　送信者は，データからハッシュ値1を生成する。

[2]　送信者は，TSAにタイムスタンプを要求し，ハッシュ値1を送る。

[3]　TSAは，ハッシュ値1に時刻情報を結合した結果から，ハッシュ値2を生成する。

[4]　TSAは，ハッシュ値2をTSAの秘密鍵で暗号化し，署名を作成する。

[5]　TSAは，ハッシュ値1，時刻情報，署名を連結する。これをタイムスタンプトークン(TST)という。

[6]　TSAは，送信者にタイムスタンプ応答として，TSTを返す。

[7]　送信者は，受信したTSTを元のデータに付加する。

〔タイムスタンプの検証〕

[8]　TSTに含まれるハッシュ値1と時刻情報から，ハッシュ値2を生成する。

[9]　TSTに含まれる署名をTSAの公開鍵で復号し，ハッシュ値2を得る。

[10]　[8]で得たハッシュ値2と[9]で得たハッシュ値2を比較する。両者が一致すれば，TSTの時刻にデータが存在し，TSTは改ざんされていない。

[11]　受信したデータからハッシュ値1を生成する。

[12]　TSTに含まれるハッシュ値1と，[11]で生成したハッシュ値1を比較する。両者が一致すれば，TSTの時刻からデータは改ざんされていない。

学習テーマ　4－5
PKI(公開鍵基盤)

●公開鍵暗号方式における欠点

公開鍵暗号方式によるディジタル署名では，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。

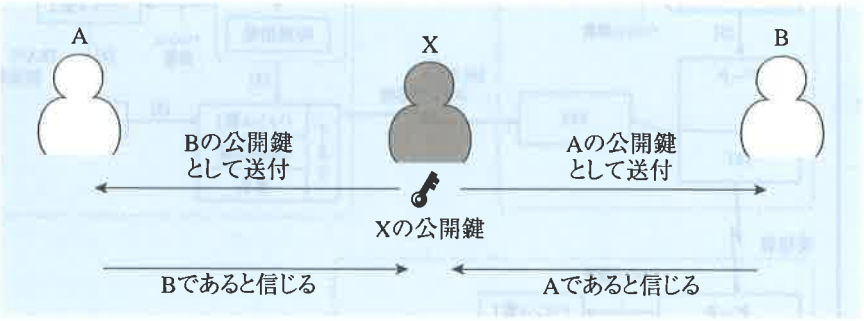


図4.16　中間攻撃

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「ディジタル証明書」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。すなわち，PKIにおいては，「認証局」と「ディジタル証明書」が重要になる。

なお，PKIは公開鍵の正当性を保証するための基盤(インフラ)を提供する手段に過ぎないため，各利用者はPKIを用いたシステム(アプリケーション)を利用することになる。このPKIを用いたアプリケーションプロトコルには，SSL(Secure Socket Layer)やS/MIME(Secure MIME)，インターネット経由でクレジットカード決済を行う仕組みのSET(Secure Electronic Transaction)などがある。

●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。

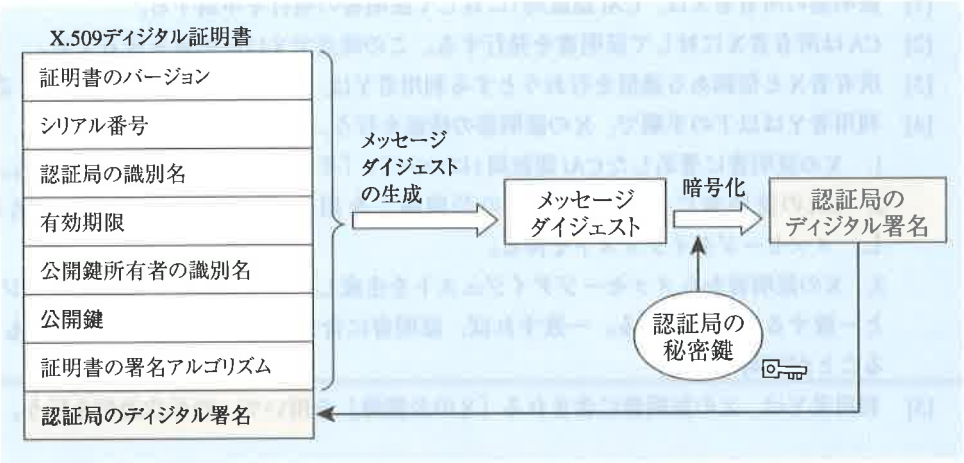


図4.17　ディジタル証明書の構成

ここで,証明書のフィールドには,「公開鍵」と「認証局のディジタル署名」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の公開鍵」となる。

●PKIにおける認証

PKIでは，受け取った証明書を検証し，それが確かにCAによって発行されたものであれば，証明書に含まれる公開鍵を正当なものとして認める。証明書の発行から証明書の検証までの流れを次に示す。

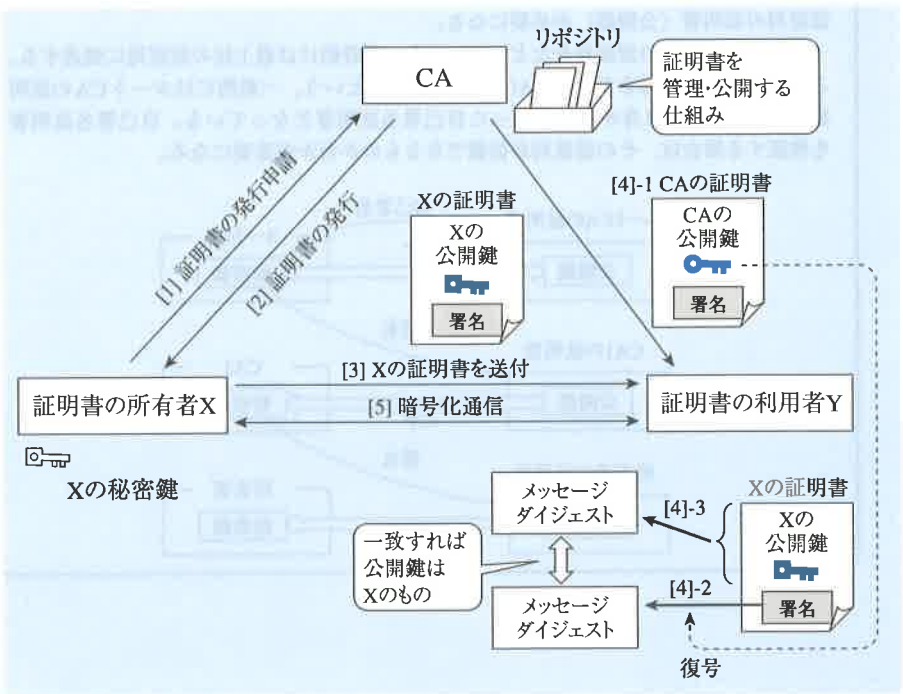


図4.18　PKIの仕組み

[1]　証明書の所有者Xは，CA(認証局)に対して証明書の発行を申請する。
[2]　CAは所有者Xに対して証明書を発行する。この時点でXは証明書を所有する。
[3]　所有者Xと信頼ある通信を行おうとする利用者Yは，所有者Xの証明書を入手する。
[4]　利用者Yは以下の手順で，Xの証明書の検証を行う。
　1.　Xの証明書に署名したCA(認証局)について，「そのCAの証明書」を入手する。
　2.　CAの証明書に含まれる「CAの公開鍵」を用いて，Xの証明書中の署名を復号し，メッセージダイジェストを得る。
　3.　Xの証明書からメッセージダイジェストを生成し，上で得たメッセージダイジェストと一致するかを検証する。一致すれば，証明書に含まれる公開鍵が所有者Xのものであることが証明できる。
[5]　利用者Yは，Xの証明書に含まれる「Xの公開鍵」を用いて，暗号化通信を行う。

なお，[3]における「証明書の入手」では，主に以下のような方法がある。
・事前にフロッピーディスクや電子メールなどで入手する。
・通信に先立ち，通信に用いるプロトコル(後述のSSLやS/MIMEなど)を用いて入手する。
・リポジトリを検索して入手する。

リポジトリとは，証明書やCRLを集中的に管理し，公開する仕組みであり，ディレクトリサーバ(LDAPやX.500のサーバ)が利用されることが多い。なお，CRL(Certificate Revocation List：証明書失効リスト)とは，証明書の誤発行や秘密鍵の漏洩といった事由により，その効果を失った(信頼すべきでない)証明書のリストであり，CRLに記載された証明書は無効となる。

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。