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

Ver.9.1

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

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。

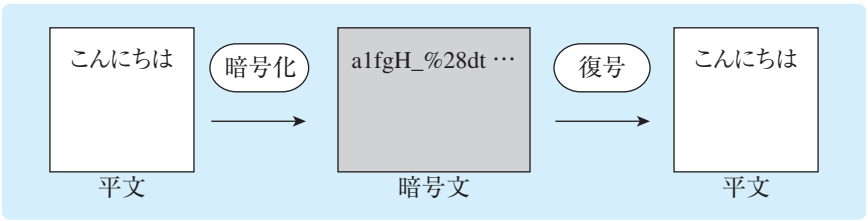


図4.1　暗号化と復号

●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。

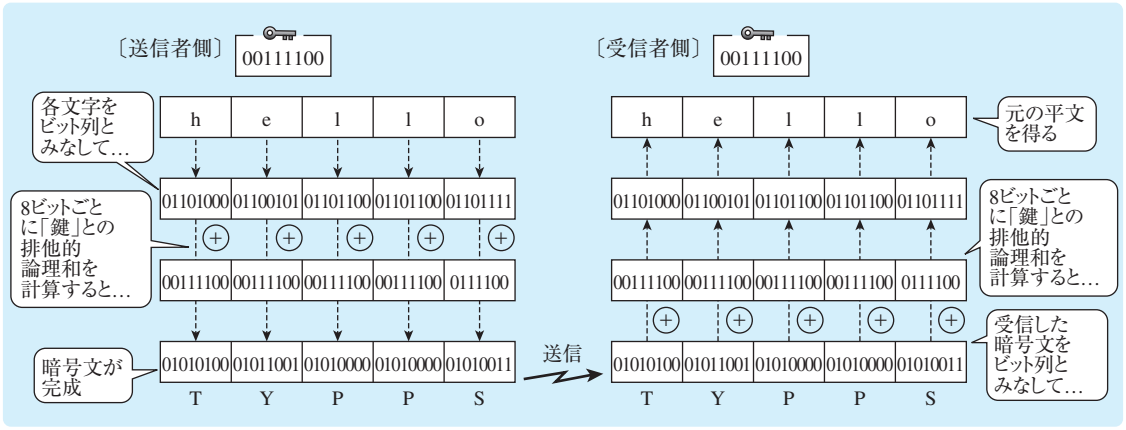


図4.2　暗号化と鍵

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。

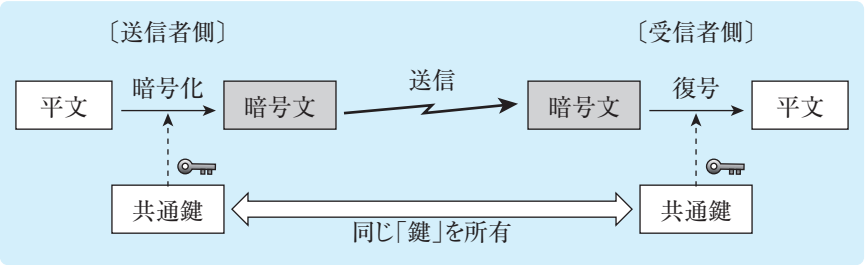


図4.3　共通鍵暗号方式の概念

●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。

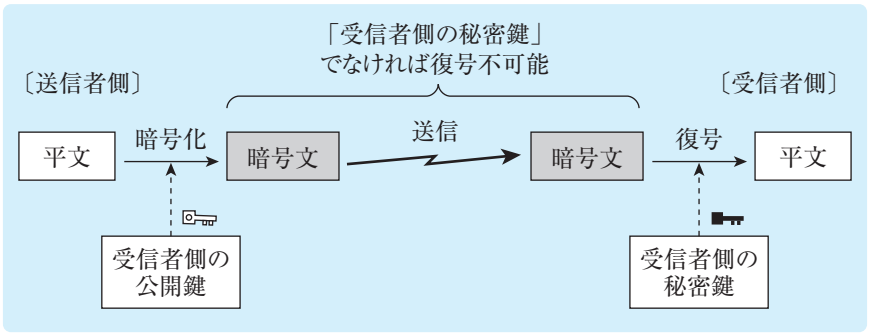


図4.4　公開鍵暗号方式の概念

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

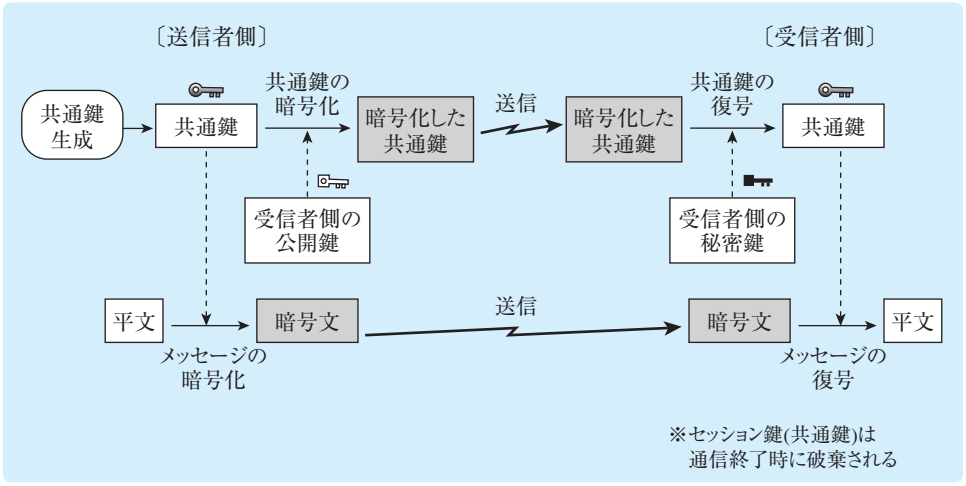


図4.5　ハイブリッド暗号方式

> **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。

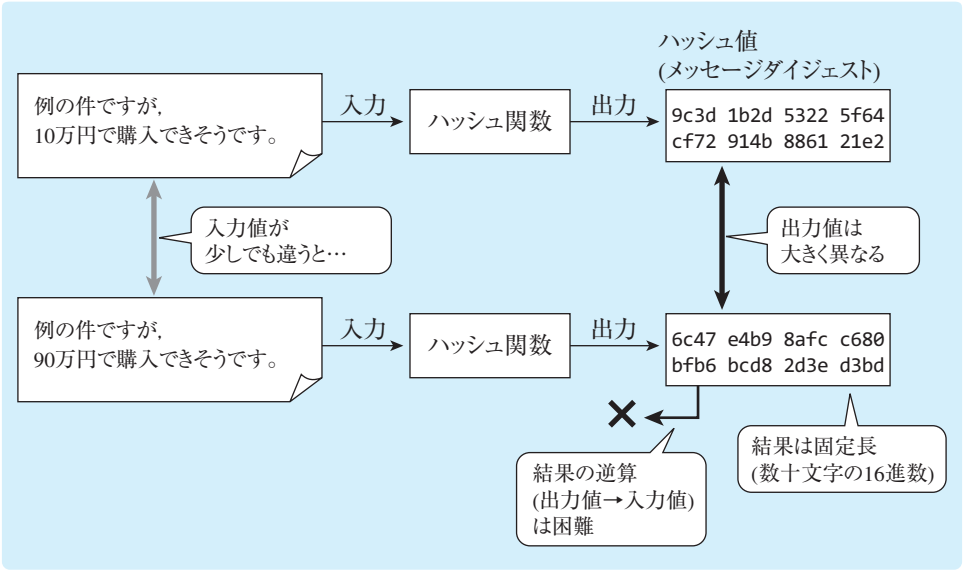


図4.6　ハッシュ関数

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。

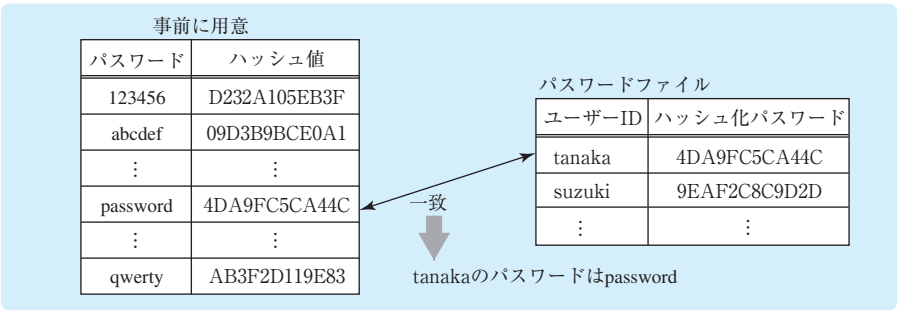


図4.7　パスワードファイルの解析

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。

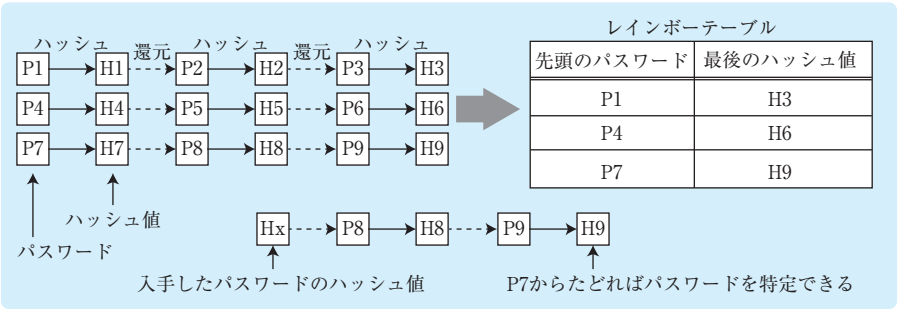


図4.8　レインボー攻撃

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。

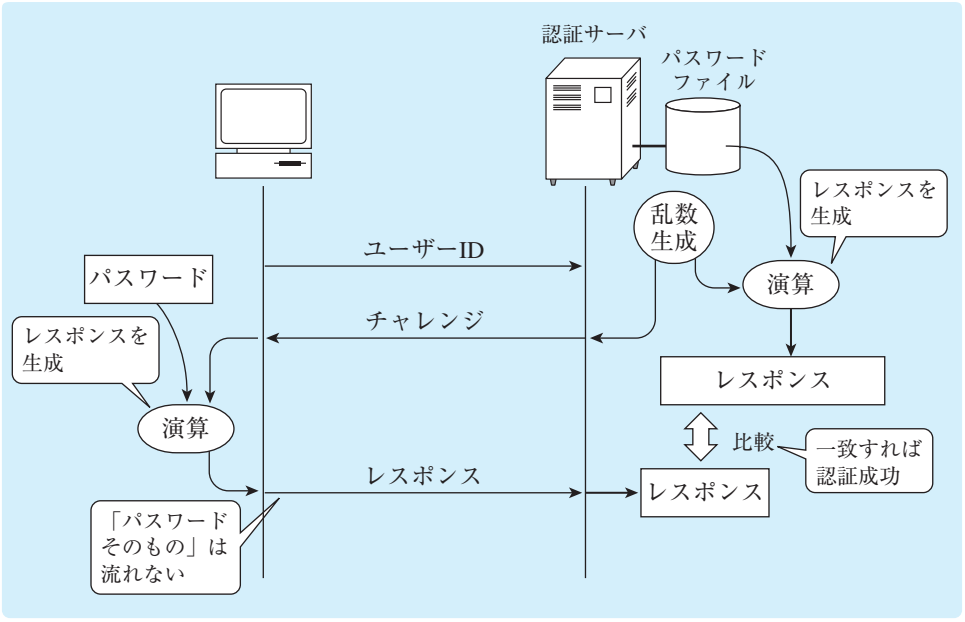


図4.9　チャレンジレスポンス方式

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。

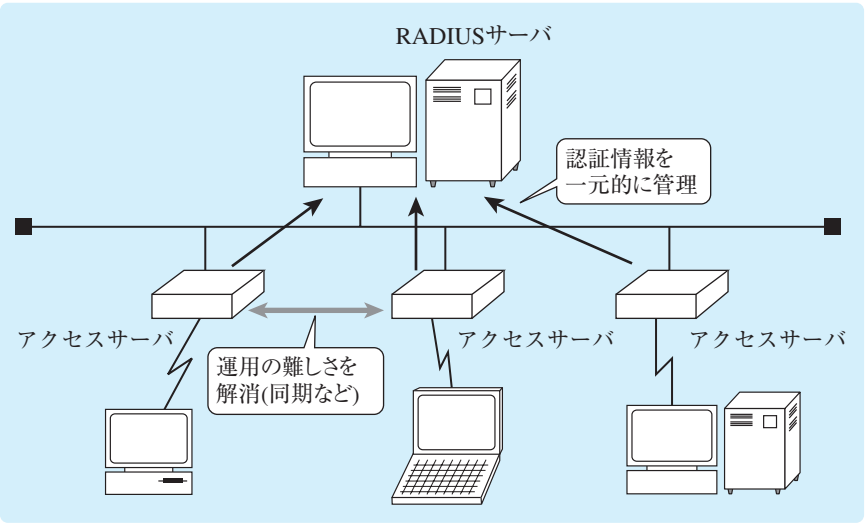


図4.10　RADIUSの概念

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。

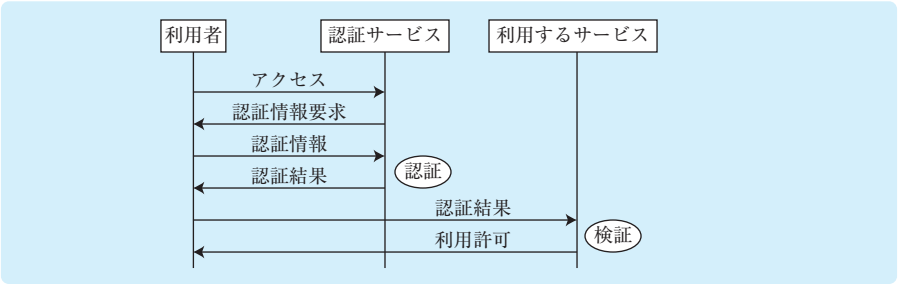


図4.11　SAML

(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。

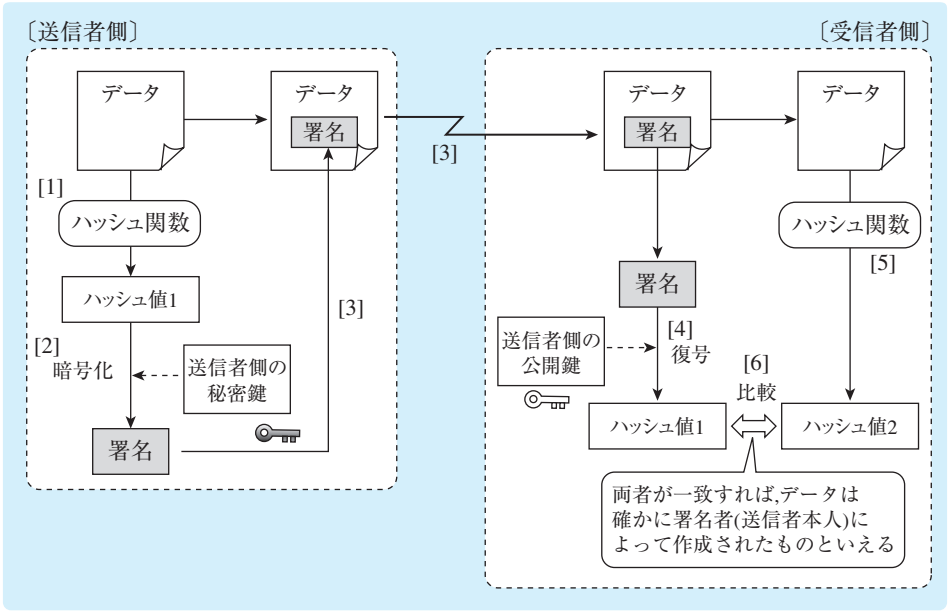


図4.12　デジタル署名

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。

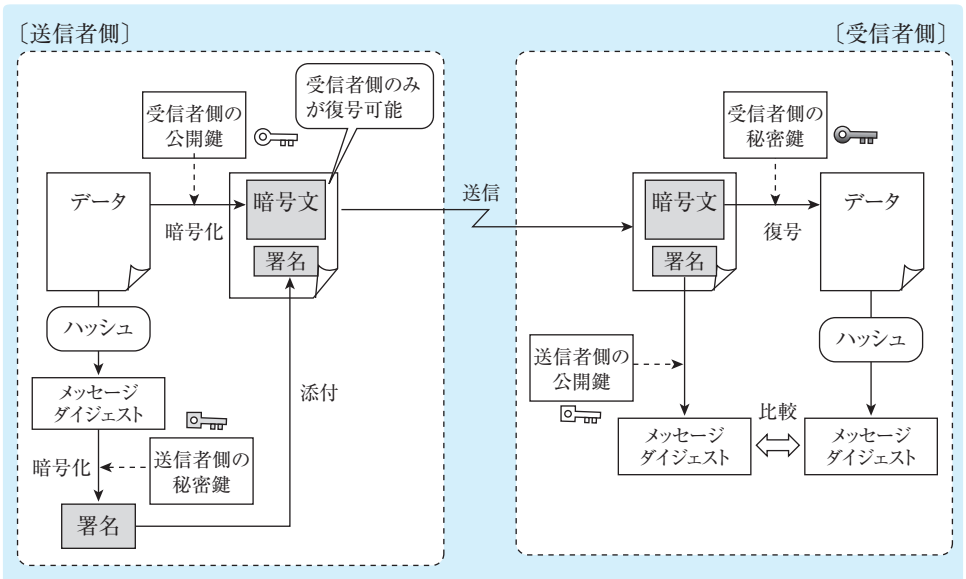


図4.13　デジタル署名と暗号化の組合せ

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。

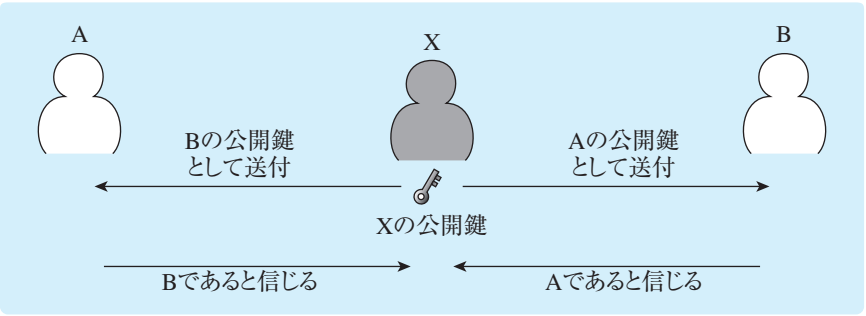


図4.14　中間者攻撃

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。

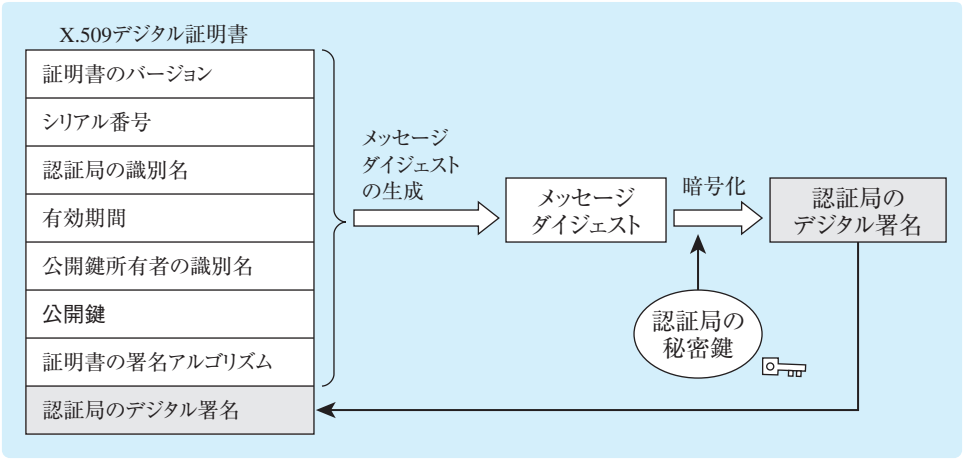


図4.15　デジタル証明書の構成

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。

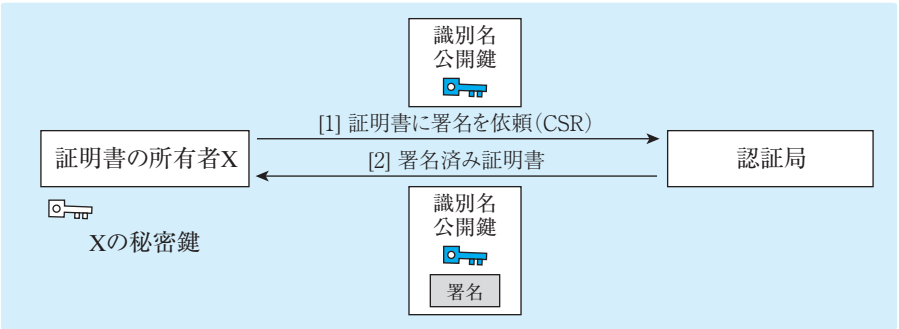


図4.16　証明書の発行

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。

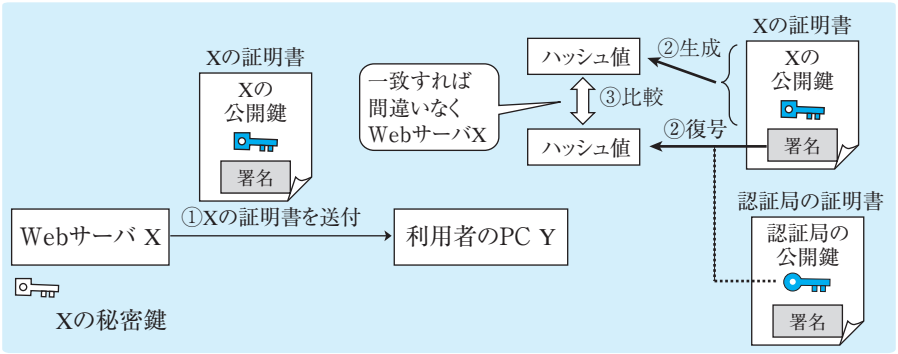


図4.17　証明書の利用

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。

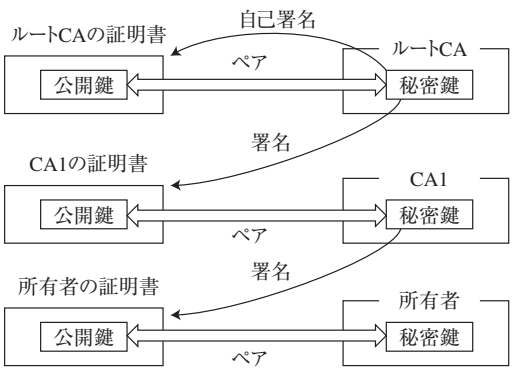
表4.9　証明書の失効状態の確認手段

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　4－9

マルウェア対策

マルウェアは，悪意をもって作成された不正なプログラムを指す。以前はコンピュータウイルスともよばれていた。マルウェアの種類には，次のようなものがある。

表4.17　マルウェアの種類と特徴

種類	特徴
マクロウイルス	ワープロや表計算といったアプリケーションのマクロ機能を利用し，データファイルに感染する不正プログラム
ワーム	単体での動作が可能であり，システム上で自身を複製して自己増殖する機能を持つ不正プログラム
トロイの木馬	単体での動作が可能であり，有用なプログラム(ユーティリティやゲームなど)を装って実行されるのを待つ不正プログラム
スパイウェア	ユーザーの行動履歴や個人情報を収集するプログラム。有用なプログラムの一機能として含まれる場合もある。
ボット	感染したコンピュータを乗っ取り，C&Cサーバ(攻撃指示用のコンピュータ)の指示に従って遠隔操作する不正プログラム。主にスパムメールの送信やDDoS攻撃の踏み台として利用される。ボットに感染したコンピュータで構成したネットワークをボットネットという。
ランサムウェア	システムのハードディスクドライブを暗号化するなど，システムの使用を不可能あるいは制限し，利用者に身代金を支払うよう促すメッセージを表示する不正プログラム
ダウンローダ	別の不正プログラムなどをダウンロードすることによって自身の変化や機能拡張などを行う不正プログラム
RAT(Remote Access Trojan)	攻撃者からの指示に従って感染したコンピュータを不正に操作するプログラム。RATは主に標的型攻撃に用いられ，より高度な情報の窃取などを行う点がボットと異なる

マルウェアは，攻撃者が金銭を得るために利用されることも多い。MITB攻撃（Man In The Browser攻撃）は，マルウェアを用いた中間者攻撃の一つであり，金融機関との通信を検出するとWebブラウザの通信を乗っ取ってデータの盗聴や改ざんを行う。MITB攻撃に対しては，利用者がWebブラウザで入力した情報とサーバが受信した情報に差がないことを検証するトランザクション署名などが有効になる。また，感染したコンピュータの計算資源（CPUなど）を不正に使用して暗号資産を得るための計算（マイニング）を行う手法を，クリプトジャッキングという。マルウェアへの感染だけでなく，不正なJavaScriptを組み込んだWebサイトを訪問することでクリプトジャッキングが行われることもある。

●マルウェア対策の基礎

マルウェアは，有用なプログラムや安全なデータを装う，OSやアプリケーションの脆弱性を利用してWebサイトの閲覧や電子メールのプレビューによって自動実行する，LANやUSBメモリを経由して自己増殖(感染)するといった手段で感染する。このため，怪しいWebサイトを閲覧しない，電子メールに添付されたファイルなどの出所が不明なファイルを不用意に開かない，安易にプログラムをダウンロードしないといった基本的な行動に加え，

・OSやアプリケーションの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)を適用してOSやアプリケーションを最新の状態に保つ

・マルウェア対策ソフト(ウイルス対策ソフト)を利用する

といった対策が重要になる。ソフトウェアを入手する際は，プログラムコードに開発元のデジタル署名を付与するコードサイニングによって，開発元が作成し，改ざんされていないことを確認するという方法もある。

●マルウェア対策ソフト(ウイルス対策ソフト)

マルウェア対策ソフトは，次のような検出手法でマルウェアを検出する。

表4.18　マルウェアの検出手法

コンペア法	安全に保管されている原本と検査対象を比較する。
チェックサム法	情報に符号(チェックサム)を用いる。
パターンマッチング法	特徴的なマルウェアのコードが登録された定義ファイルを用いて検出する。
ビヘイビア法	マルウェアによって引き起こされる動作パターンを監視して検出する。

代表的な検出手法であるパターンマッチング法では，マルウェアの特徴的な部分を定義したパターンファイル(シグネチャファイル，ウイルス定義ファイル)と検査対象のファイルを比較する。パターンファイルに登録されていないマルウェアは検出できないので，パターンファイルを常に最新に保つことが重要になる。ビヘイビア法のように動的な解析を伴う場合は，実環境とは隔離された仮想的な領域上で動作させ，悪影響の拡散を防ぐ。このような領域をサンドボックスという。いずれの方法であっても，正常なファイルをマルウェアと判断する偽陽性(フォールスポジティブ)や，マルウェアを正常なファイルと判断する偽陰性(フォールスネガティブ)といった誤検知が発生し得る。また，ウイルス(マルウェア)側も，対策ソフトによる検知をすり抜けるように工夫してくる場合もある。以下に例を示す。

ポリモーフィック型：自身の複製時に異なる鍵で暗号化を行い，内容を変化させる

メタモーフィック型：自身の複製時に「同機能を実現する別のコード」に変化する

ファイルレスマルウェア：実行ファイルが補助記憶装置に保存されず，主記憶装置上で攻撃を行う

●企業におけるマルウェア対策

企業内では，マルウェアの感染に加えて組織内部での感染拡大を防ぐことも重要になる。このため，不用意に見知らぬファイルを開かない，USBメモリはマルウェアチェックされた承認されたものだけを使用する，といった基本的な対策を周知・徹底する人的な対策も重要となる。

また，OSやアプリケーションのセキュリティパッチを定期的に適用して最新の状態を保つ，PCなどの機器にマルウェア対策ソフトを導入するといった基本的な対策も重要である。ネットワークの境界付近やメールサーバなどでマルウェアチェックを行うことも効果的であるが，感染経路はネットワーク経由のみとは限らないので，PCなどの末端の機器にマルウェア対策ソフトを導入することは必須といえる。

万が一，コンピュータがマルウェアに感染した場合の対応手順は，すべての要員が理解し，遵守する必要がある。近年はネットワーク経由で感染を拡大するマルウェアも多いので，不審な挙動を発見したら初動としてLANケーブルを抜くなどしてコンピュータをネットワークから切断し，感染拡大を防いだ上でシステム管理者に連絡して指示を仰ぐ。

システム管理者は，影響範囲を局所化した上で，被害状況の分析やマルウェアの除去，システムの回復などを行う。この際，主記憶装置上にある情報(実行しているマルウェアやデータなど)は電源を切ってしまうと失われてしまうので，安易に電源を切るべきではない場面もある。

マルウェアに感染した場合，マルウェアを駆除したとしても破壊されたデータは復旧しない。このため，データを定期的にバックアップしておくことが重要になる。ランサムウェアなどは，アクセス可能な範囲のファイルを暗号化してしまうので，バックアップしたデータが被害を受けないような対策も重要である。具体的には，バックアップしたデータを保管するサーバや機器はネットワーク経由でアクセス可能な状態としないことに加え，バックアップしたデータはWORM(Write Once Read Many)のような書き換えが不可能な記録媒体に記録する，3-2-1ルールに従うなどの方法がある。3-2-1ルールとは，

・データは「オリジナル」「コピー1」「コピー2」の3つ用意する
・2つのコピーはそれぞれ異なる媒体に保存する
・コピーのうちいずれか1つを遠隔地に保存する

とルールに基づいてバックアップ運用を行うものであり，バックアップの理想とされる。

●マルウェアを利用した攻撃手法

(a) ガンブラー(Gumblar)

ガンブラーとは，Webサイトの改ざんとマルウェアを組み合わせ，Webサイトを閲覧した不特定多数のコンピュータをマルウェアに感染させる手法の総称である。ガンブラーでは正規のWebサイトを改ざんして攻撃用サイトに誘導し，OSやアプリケーションソフトの脆弱性を突いて攻撃するようなマルウェア(攻撃コード)をダウンロードさせる。閲覧者のコンピュータに脆弱性が存在すれば，そのコンピュータはマルウェアの侵入を許してしまい，マルウェアに感染する。このようなWebサイトを閲覧しただけでマルウェアに感染するような手法をドライブバイダウンロードという。

このような攻撃に対しては，ウイルス対策ソフトを導入してパターンファイルを最新の状態に保つ，OSやアプリケーションソフトのセキュリティパッチを適用して脆弱性を解消する，といった基本的な対策が重要になる。

(b) 標的型攻撃

機密情報の窃取などを目的として特定の組織（企業や官公庁）を狙った攻撃を標的型攻撃という。標的型攻撃の手法はさまざまであるが，主にソーシャルエンジニアリングの手法を用いた偽装メールとマルウェアを組み合わせた標的型攻撃メールを用いたものが多い。

標的型攻撃メールは，攻撃者は事前に標的となる組織や取引先などの関連組織などに関する情報を調査して作成される偽装メールであり，一般的には次のような特徴が挙げられる。

・実際の組織名や個人名などを送信者名として詐称する。
・件名，本文，添付ファイル名を工夫し，業務連絡などを装う。
・PDFファイルや文書ファイルなどに偽装したマルウェアを開くよう，あるいはマルウェアをダウンロードさせる不正サイトに接続するよう誘導する。

添付されたマルウェアは，不特定多数の利用者に無差別に送付されるものではなく，その組織への攻撃に最適化されているため，ウイルス対策ソフトでのパターンマッチングによる検出が難しい。さらに，バックグラウンドで次のような活動を行う。ファイルの破壊や改ざんといった目立った活動を行わない場合，感染に気づくことも難しくなる。

・バックドアの作成
・外部のC&C(Command & Control)サーバに対するコネクトバック通信
・システムに関する情報（システム構成など）の取得
・取得した情報の外部への送信
・新たなマルウェアのダウンロードや機能拡張
・ネットワーク経由の感染・拡散
・USBメモリ経由での隔離されたクローズ系システムへの侵入

コネクトバック通信とは，感染した端末がC&Cサーバにアクセスし，攻撃者がそれに応答する形で端末に接続するバックドア通信のことである。この通信にはHTTPやHTTPSが用いられることが多く，一見すると通常のWebアクセスと見分けるのが難しいため，ファイアウォールを通過しやすくなる。

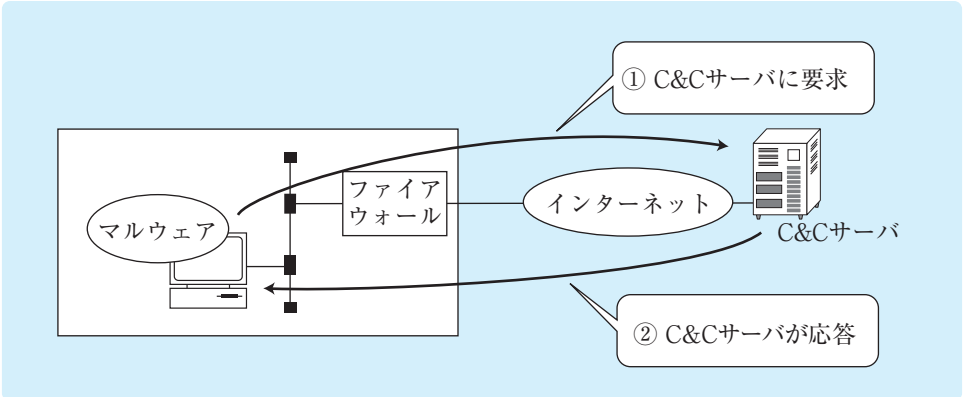


図4.26　コネクトバック通信

標的型攻撃で用いられる手法は特別に新しいものではなく，ソーシャルエンジニアリングやダウンローダ，ドライブバイダウンロード，バックドア，マルウェア，USBワーム，ゼロデイ攻撃など，既存の技術を組み合わせたものである。ただし，標的となる組織に対して長期的に調査や攻撃を行い，攻撃手法を最適化していく点が従来のものとは異なる。このような標的に特化した手段で長期的に行う攻撃をAPT(Advanced Persistent Threat)ともいう。

このほかにも，標的となる組織の従業員が頻繁に閲覧するサイトを改ざんして攻撃コードを埋め込み，アクセス時にマルウェアをダウンロードさせるような手法も用いられる。これを水飲み場型攻撃という。

標的型攻撃を防ぐためには，不審な添付ファイルを開かない，URLを安易にクリックしない，OSやアプリケーションソフトのセキュリティパッチを適用して最新に保つ，重要情報はネットワークから隔離するといった従来どおりの技術的対策や利用者教育などが重要となる。これらを確実に実施したとしてもシステムへの侵入を確実に防止できるとは限らないので，重要情報が組織外部(インターネット)に出て行くことを防止する出口対策も重要となる。

出口対策の一つに，プロキシサーバで認証を行う認証プロキシを利用するというものがある。この際，マルウェアが認証情報を窃取しないよう，PCには認証情報を保存しないといった対策も考慮する。

学習テーマ　4－10

インターネットセキュリティ

(1)　HTTP における認証

●HTTP 基本認証

HTTP はそれ自体が基本認証 (basic 認証) とよばれる認証機能をもつため，Web サイトや特定のディレクトリなどに対して，ユーザー ID とパスワードによるアクセス制限を設定できる。

ただし，この基本認証では，ユーザー ID とパスワードは平文で送信される。このため，盗聴される可能性もあり，アクセス制御が重要なシステムでは SSL/TLS によって通信内容を暗号化することが望ましい。また，多くのブラウザは，基本認証によって入力されたユーザー ID やパスワードを記憶する機能をもつ。このため，複数人で 1 台のパソコンを共有するような場合は，パスワードを記憶させないように設定しておく必要がある。

(2)　SSL/TLS

●SSL/TLS の機能

SSL(Secure Sockets Layer) やその後継規格である TLS(Transport Layer Security) は，TCP/IP モデルにおけるアプリケーション層とトランスポート層の間に位置し，アプリケーションプロトコルに対して次のような機能を提供するセキュリティプロトコルである。

表 4.19　SSL/TLS の機能

サーバ認証， クライアント認証	サーバ (またはクライアント) が提示する証明書を検証し，通信相手を認証する。どちらか一方の認証 (あるいは両方とも認証しない) も可能であり，WWW においては，サーバ認証が行われることが多い
暗号化	アプリケーションプロトコルのデータを暗号化する
メッセージ認証	メッセージ認証符号を用いて，改ざんを検出する

SSL/TLS はトランスポート層に TCP を用いるさまざまなアプリケーションプロトコルの下位層として利用することができる。Web においては，上位層に HTTP を利用する HTTPS(HTTP over TLS) が主に用いられ，ウェルノウンポート番号として 443 が用いられる。

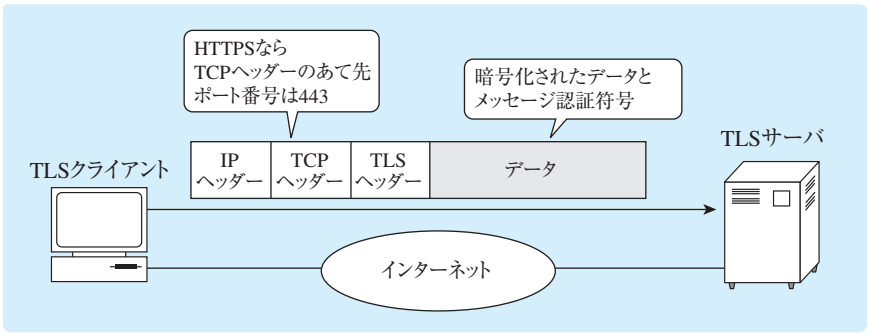


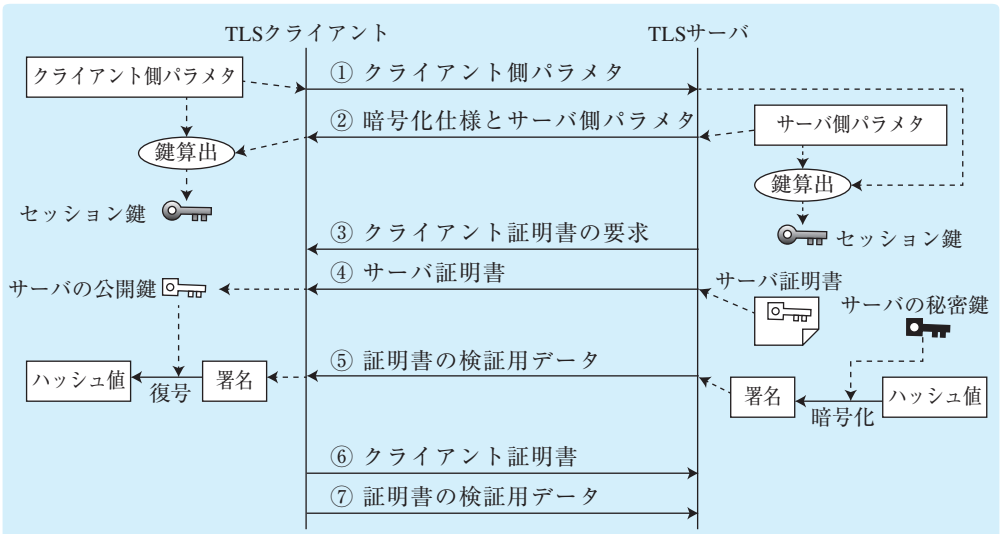
図4.27　TLSを利用した通信

●TLSの通信手順

TLSでは，通信に先立って

・利用するTLSのバージョンや暗号化アルゴリズムなどについての合意
・鍵交換（使用するセッション鍵の合意と生成）
・通信相手の認証（サーバ認証，クライアント認証）

などが行われる。これをハンドシェイクという。ハンドシェイクの詳細な手順は，SSLを含むTLSのバージョンや認証の有無などによって異なる。また，通信内容の暗号化に用いられるセッション鍵は，DH（Diffie–Hellman）鍵交換を応用して生成される。DH鍵交換とは，クライアントとサーバでパラメタとなる乱数を交換し，公開鍵暗号の理論によって第三者に推測不可能な共通鍵を生成する方法である。



注記1：③，⑥，⑦はクライアント認証を行う場合に，サーバ認証と同様の手順で行われる。
注記2：検証用データの基となるハッシュ値は，それまでに送受信されたメッセージから生成される。

図4.28　TLSの通信シーケンス

●SSL/TLSを利用する場合の留意点

SSL/TLSは現状では十分なセキュリティを確保することができるため，通信内容の保護に関しては大きな問題はない。ただし，SSL/TLSを利用する場合は以下の点に注意する必要がある。

・SSL/TLSの利用による処理性能の低下

SSL/TLSを利用すると，証明書の交換やセッション鍵の生成などの処理が発生する。処理件数によってはサーバには大きな負荷がかかるため，SSL/TLSを利用するサーバには高い処理能力が要求される。このため，必要に応じてSSLアクセラレータ(TLSアクセラレータ)とよばれる「SSL/TLSの処理を行う専用装置」を用いて負荷を分散する。

・通信内容に基づく制御

SSL/TLSに限らず，通信を暗号化した場合は通信内容が第三者に傍受される可能性を低減できる反面，その内容を解析することも困難になる。このため，ウイルスを検出するためのウイルスチェックや不正な通信内容を遮断するコンテンツフィルタなどは，正常に機能しなくなる。また，HTTPのメッセージボディやcookieなどにセッションIDなどを格納してセッション維持を行うようなケースでも，暗号化を解除しないと制御ができなくなってしまう。

(3)　電子メールの暗号化と署名

送信元からあて先まで電子メールの内容を暗号化する場合，「電子メールを送信する前にメッセージを暗号化する」ことが基本となる。このために，S/MIMEやPGPなどが用いられる。

S/MIME(Secure MIME)は，PKIとMIMEの仕組みを利用して電子メールに暗号化とデジタル署名の機能を提供するプロトコルであり，ハイブリッド暗号方式でメールメッセージの暗号化を行う。暗号化されたメールメッセージや署名，暗号化された公開鍵などは，MIMEの機能を用いて添付ファイルの形で送受信される。このため，S/MIMEに対応していないメールソフトでは，署名のみを行ったメールであればメッセージを読むことは可能だが，署名を検証することはできない。

なお，S/MIMEで暗号化を行う場合，送信者の公開鍵で暗号化された共通鍵と，受信者の公開鍵で暗号化された共通鍵の両方が格納される。これは送信者と受信者の双方がメールを復号できるようにするためである。

> 参考：PGP
>
> PGP（Pretty Good Privacy）は，S/MIMEと同様にハイブリッド暗号方式を用いてメールメッセージの暗号化やデジタル署名などを実現する仕組みである。PGPは，認証局のような公開鍵の所有者を保証する仕組みをもたない。公開鍵に対して所有者を保証するための署名を，各ユーザーが相互に付加することによって公開鍵を信頼する。このような仕組みを，信頼の輪という。

(4)　メールサーバにおけるセキュリティ

●電子メールの不正中継対策

メールの送信に用いられるSMTPは，元々は認証機能をもっていなかった。このため，詐欺や広告の送信などを目的に不特定多数の宛先に無差別にメールを送信するスパムメール(迷惑

メール)が問題となっている。スパムメールの送信には，他者が所有するメールサーバを踏み台に用いることが多い。仮に自社のメールサーバが踏み台に利用されると，メールサーバのリソースが不正に利用されるだけでなく，スパムメールの送信元と見なされて社会的信用を失う恐れもある。スパムメールの踏み台として利用されないための対策として，リレー制限やSMTP-AUTHの利用などが挙げられる。

(a)　リレー制限

自社のメールサーバが「外部(社外)からのメールをさらに外部へ中継する」ことを許可した状態(オープンリレーと呼ばれる)になっていると，スパムメールを送信する踏み台として自社のメールサーバが利用されるリスクが高まる。このような電子メールの不正中継(第三者中継ともいう)を防ぐためには，メールサーバに電子メールの中継を制限するリレー制限を設定する方法が効果的である。具体的には，内部(社内LANなど)から発信された電子メールは外部(社外など)へ転送するが，外部から発信された電子メールは外部に転送しないように設定を行うことにより，電子メールの不正中継を防ぐことが可能となる。

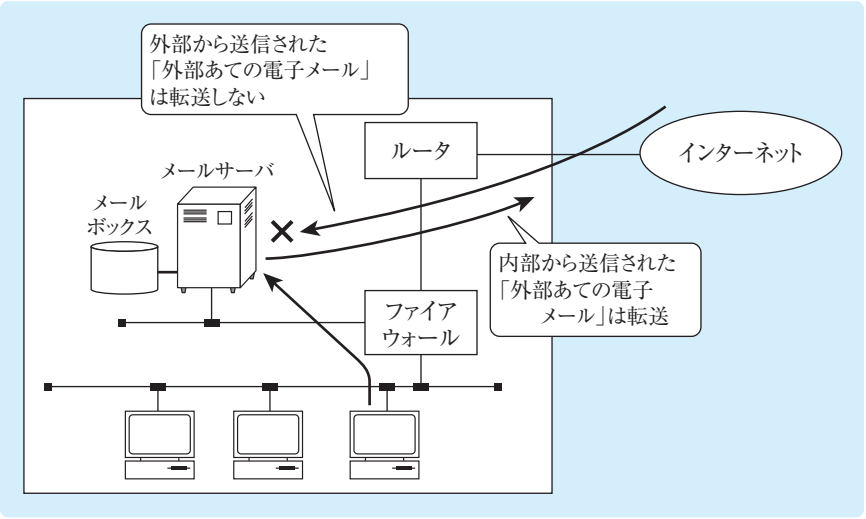


図4.29　電子メールのリレー制限

また，メールサーバを分離することによって不正中継対策のルールを単純化し，メールボックスへの攻撃を防ぐ効果が期待できる。たとえば，外部用メールサーバと内部用メールサーバを用意して，次のように設定することが考えられる。

・外部用メールサーバは外部から送られた内部向けの電子メールを内部用メールサーバに転送し，内部用メールサーバから転送された電子メールのみを外部に転送する
・内部用メールサーバは，(クライアントマシンの)各メールソフトから送られてきた外部向け電子メールのみを外部用メールサーバに転送し，外部用メールサーバから転送された電子メールと内部でやりとりされる電子メールをメールボックスに蓄積する

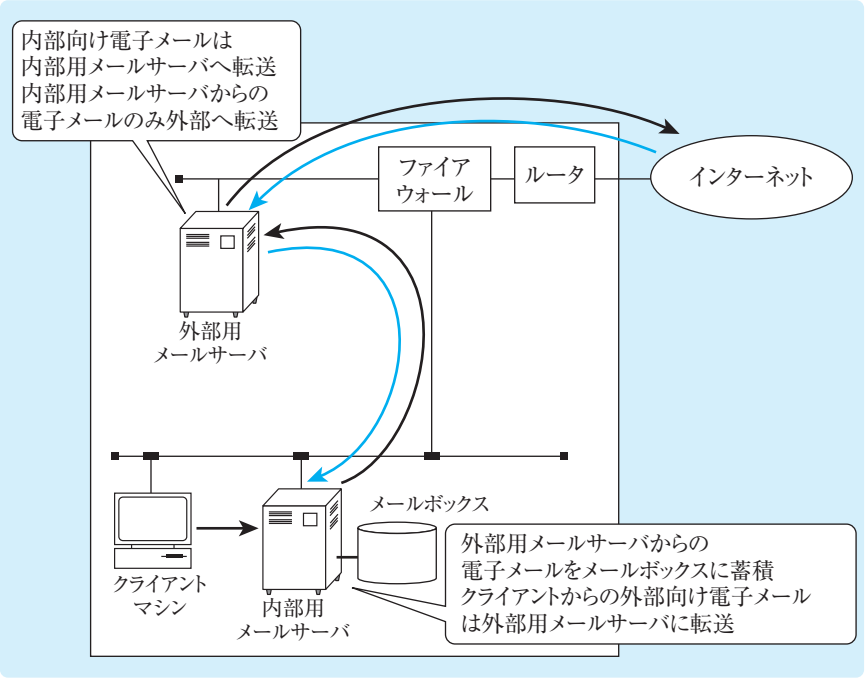


図4.30　メールサーバの分割

このほかにも，「送信用のメールサーバと受信用のメールサーバを別にする」，「メールマガジン配送用など，大きな負荷がかかるメールサーバは別に用意する」など，メールサーバの負荷分散やセキュリティリスクの分散などを目的に，メールサーバの分割を行うこともある。

(b)　SMTP-AUTH

SMTP-AUTH(SMTP AUTHentication)は，SMTPそのものに認証機能を追加したSMTPの拡張仕様である。ユーザーは認証に成功した場合のみ，電子メールを送信できる。SMTP-AUTHでは，25番(SMTP)ではなく，サブミッションポートとよばれる587番のポート番号を用いる。

現在では，悪意ある顧客やボットに感染したPCなどが自社のドメインからスパムメールを送信するのを防ぐため，自社のメールサーバを経由せずにインターネットに出ていくSMTP通信(ポート番号は25)を遮断するISPが多い。これをOP25B(Outbound Port25 Blocking)という。OP25Bではサブミッションポートによるメール送信はブロックしないので，正当なメールアカウントをもつ利用者は問題なく他のISPのメールサーバを利用することができる。

(c)　送信ドメイン認証

電子メール送信者のアドレスがなりすまされておらず，信頼できるネットワーク領域(ドメイン)から送信されていることを証明することを，送信ドメイン認証という。送信ドメイン認証を実現する技術には，送信元ドメインのDNSサーバにメールサーバのIPアドレスを登録・公開しておき，受信側がそれを参照・確認するSPF(Sender Policy Framework)や，メールサーバがメールに署名するDKIM(DomainKeys Identified Mail)などがある。

SPFでは，メールの送信元となる組織が，自ドメインからメールを送信するサーバのIPアドレスをDNSサーバのTXTレコードに登録しておく。このレコードをSPFレコードという。

受信側のメールサーバは，メールを受信すると送信元ドメインのDNSサーバにSPFレコードを問い合わせ，メールの送信元となるIPアドレスがSPFレコードに含まれているかを確認する。SPFレコードに含まれている場合は，メールは正規のメールサーバから送信されたと判断する。含まれていない場合は，メールサーバがなりすまされていると判断する。

DKIM(DomainKeys Identified Mail)では，送信元の組織がDNSサーバに公開鍵を登録しておき，送信側メールサーバが電子メールのヘッダーにデジタル署名を付加する。受信側メールサーバは，デジタル署名を公開鍵で検証し，メールサーバがなりすましでないかを確認する。

(5)　Webサイトのセキュリティ対策

●Webサイト改ざん対策

Webサイトの運営においては，Webページの改ざんというリスクがつきまとう。Webサイトを改ざんするための手法は様々であるが，ここではサーバに保存されたWebページを改ざんする手法について解説する。

Webページを改ざんするためには，Webサーバに侵入して管理者権限などのWebページを書き換える権限を得る。このための代表的な手法として，次の二つが挙げられる。

・パスワードクラックや推測，盗聴などによってWebサーバに直接侵入する

・OSやWebサーバソフトの脆弱性を攻撃し，管理者権限を奪取する

このため，強固なパスワードを設定して定期的に変更する，ベンダーから公表される脆弱性情報を収集してセキュリティパッチを適用する，あるいは推奨された対応策を適用するなどの対策が必要になる。

●フィッシング対策

電子メールなどを用い，正規のWebサイトを装った偽のWebサイト（フィッシングサイト）に誘導してクレジットカード番号を窃取するといった詐欺行為をフィッシングという。フィッシングサイトは，巧妙に正規のWebサイトを装っているが，ドメイン名が異なっていたり，ドメイン名ではなくIPアドレスを用いていたりする。このため，URLに注意すれば被害にあうことは少なく，利用者側の対策が重要となる。

また，正規のドメイン名を用いて偽のWebサイトに誘導する手口もある。これをファーミングという場合もあり，実現する手法には次のようなものが挙げられる。

(a)　hostsファイルの書き換え

hostsファイルとは，ホスト名(ドメイン名)とIPアドレスの対応を記述したテキスト形式のファイルであり，DNSと同様にドメイン名に対応するIPアドレスを得るために用いられる。マルウェアの中には，正規のドメイン名へのアクセスを不正なサーバに誘導するために，hostsファイルを書き換えるものもある。また，特定のドメイン名への接続を防止するためにhostsファイルを悪用する場合もある。たとえば，ウイルス定義ファイルの提供元となるFQDNを，PC自身を表すIPアドレス（ループバックアドレス）である127.0.0.1に対応付けると，その機器は提供元のサイトにアクセスすることができず，ウイルス定義ファイルをダウンロードできなくなる。

(b)　DNSサーバへの不正侵入

DNSサーバに不正侵入されてゾーン情報のAレコードが書き換えられた場合も，正規のドメイン名へのアクセスが不正なサーバに誘導されてしまう。このような不正侵入を防ぐためには，Webサーバと同様にDNSサーバのセキュリティを確保するために適切なパスワード管理や脆弱性の解消などが重要となる。

(c)　DNSキャッシュポイズニング

クライアントからのDNS問い合わせを受け付けて，ゾーン情報を保持するDNSサーバ（コンテンツサーバ）に問合せを行うDNSサーバをキャッシュサーバという。DNSキャッシュポイズニングは，キャッシュサーバがもつキャッシュに偽りの情報を埋め込む攻撃である。具体的な手法としては，キャッシュサーバに問合せを依頼するとともに偽の回答を送りつけるなどがある。キャッシュサーバは，問合せを受けたドメイン名がキャッシュにあればコンテンツサーバへの問合せを行わないので，正規のドメイン名に対して不正なサーバのIPアドレスを回答してしまう。

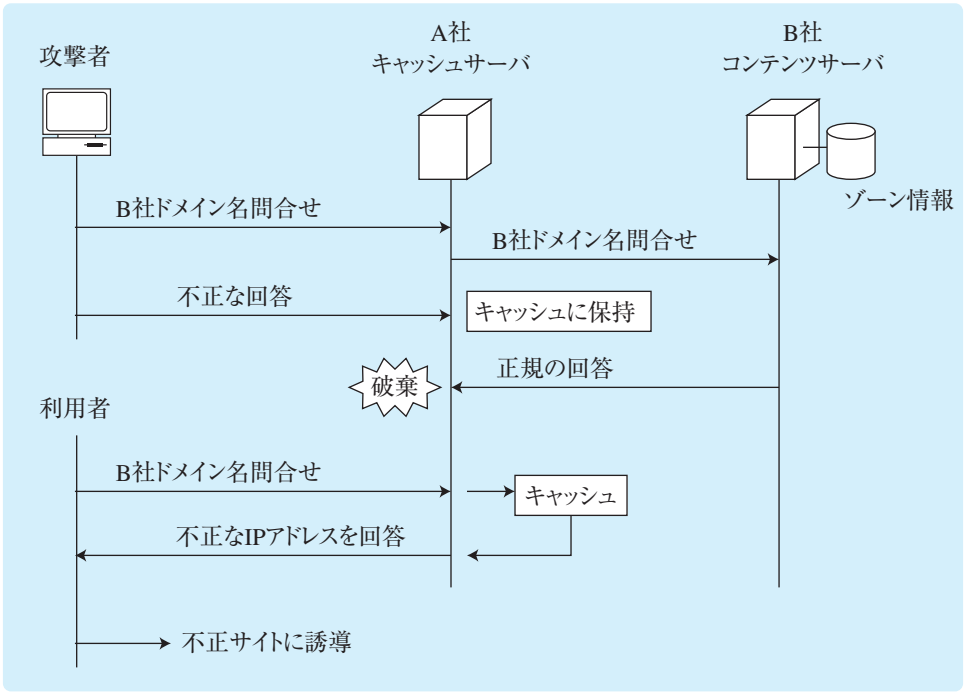


図4.31　DNSキャッシュポイズニング

外部（インターネット）からのDNS再帰問合せに応答するようなキャッシュサーバをオープンリゾルバという。オープンリゾルバは，DNSキャッシュポイズニングだけでなく，様々な攻撃にも利用されるため，自社のキャッシュサーバが外部（インターネット）からのDNS再帰問合せに応答しないよう設定する必要がある。また，キャッシュサーバが偽の回答を入手しないための技術としては，デジタル署名の仕組みを用いることによって正当なDNSサーバからの応答かをクライアント側が検証できるようにしたDNSSEC(DNS Security Extensions)などがある。

●DoS攻撃(Denial Of Service)

DoS攻撃とは，提供するサービスの妨害や停止を目的とした攻撃であり，大量のアクセスなどを発生させて過負荷をかける手法が代表的である。DoS攻撃のうち，ボットに感染したパソコンなど，多数の踏み台を利用して一斉にDoS攻撃を仕掛ける攻撃を，DDoS攻撃（Distributed DoS攻撃)ともいう。DoS攻撃及びDDoS攻撃は単なるアクセス集中と区別がつきにくく，ファイアウォールのパケットフィルタリングの設定だけで防御することは難しい。また，サーバのリソースを浪費させるDDoS攻撃とネットワーク帯域を浪費させるDDoS攻撃を組み合わせるなど，複数のDDoSを組み合わせる手法をマルチベクトル型DDoS攻撃という。DoS攻撃及びDDoS攻撃には，次のような手法がある。

表4.20　DDoS攻撃の手法

名称	内容
smurf攻撃	送信元を攻撃対象とし，宛先をブロードキャストとしたICMPエコー要求を送信する攻撃。攻撃対象には大量のICMPの応答パケットが送られる。
ICMP Flood攻撃	大量のICMPエコー要求を送信する攻撃。攻撃対象までの回線を過負荷状態にさせる。
SYN Flood攻撃	攻撃対象のサーバに対してTCPコネクションの確立を要求するSYNパケットを大量に送信する攻撃。
DNS水責め攻撃 ランダムサブドメイン攻撃	実在しない攻撃対象ドメインのサブドメイン名をランダムかつ大量に生成し，その問合せをオープンリゾルバに送信する攻撃。攻撃対象の権威サーバにはサブドメイン名に対する問合せが集中する。実在しないランダムなサブドメイン名を生成するため，DNS応答がキャッシュされない。
DNSリフレクタ攻撃 DNSリフレクション攻撃 DNS amp攻撃	送信元を攻撃対象に偽装したDNSの問合せを，大量にオープンリゾルバに送信する攻撃。攻撃対象には大量のDNS応答が集中する。DNSの応答は攻撃対象に送信されることから，オープンリゾルバが攻撃を反射しているように見える。また，DNSの応答は問合せよりもサイズが大きいので攻撃パケットのサイズを増幅させることができる。
NTPリフレクタ攻撃 NTPリフレクション攻撃	送信元を攻撃対象に偽装したNTPの問合せを，インターネット上の公開NTPサーバに送る攻撃。攻撃対象には大量のNTP応答が集中する。直前にNTP通信したホストの一覧を得るコマンド（monlistコマンド）を使用することにより，応答パケットのサイズを増幅させることができる。

DNSを用いたDDoS攻撃では，踏み台としてオープンリゾルバが利用される。自社のDNSサーバが踏み台として利用されないためにも，自社のDNSサーバはオープンリゾルバとしない設定とすべきである。この他にも，従量課金制のクラウドサービスを利用する企業に対して経済的な損失を与えるために，リソースを大量消費させるEDoS攻撃（Economic Dos攻撃）などもある。

> **参考：IPスプーフィング**
>
> 送信元のIPアドレスを偽装する手法をIPスプーフィングという。IPアドレスによる接続制限を回避する場合やDoS攻撃の攻撃元を隠蔽するなどの目的に用いられる。

(6)　その他のインターネットセキュリティ

●ダークネット

インターネット上で到達可能であるが使われていないIPアドレス空間を，ダークネットという。ダークネットはサイバー攻撃に用いられることも多く，国立研究開発法人 情報通信研究機構（NICT）では，サイバー攻撃の観測・分析システムであるNICTERによってダークネットを観測し，サイバー攻撃の動向やマルウェアの活動動向などを把握・分析している。

●ダークウェブ

インターネット上に存在するが，特定のソフトウェアや設定を使用しないとアクセスできないWebサイトやコンテンツをダークウェブといい，サイバー犯罪者の情報交換の場になっていることもある。ダークウェブを実現する仕組みの一つであるTorは，TCP/IPネットワークにおいて通信経路を匿名化する。Torブラウザなどのソフトウェアを使用することにより，Torによって構築されたネットワークにアクセスしたり，Torを経由して匿名性を保ったままインターネットにアクセスしたりすることが可能となる。