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】

Information-Technology Engineers Examination

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

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。

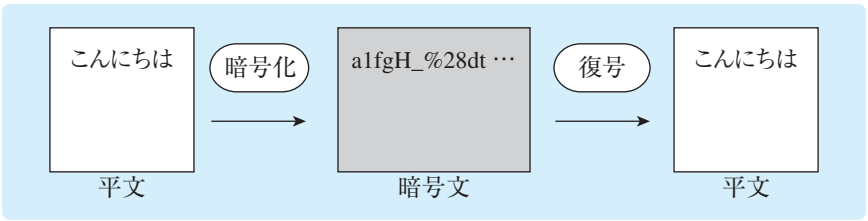

図4.1　暗号化と復号

●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。

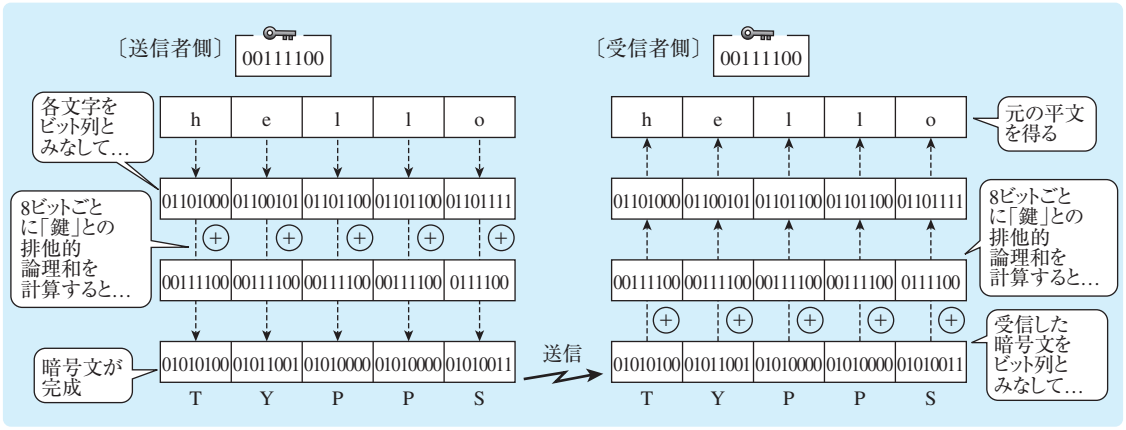

図4.2　暗号化と鍵

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。

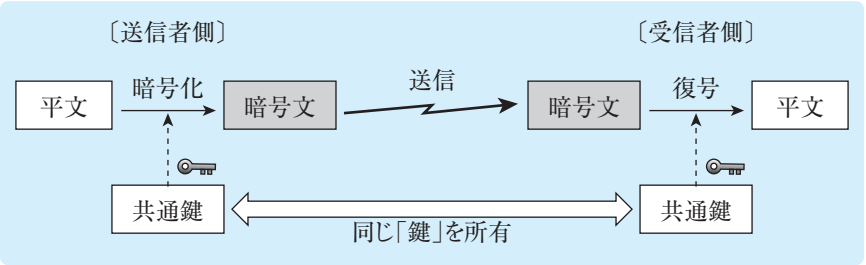

図4.3　共通鍵暗号方式の概念

●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。

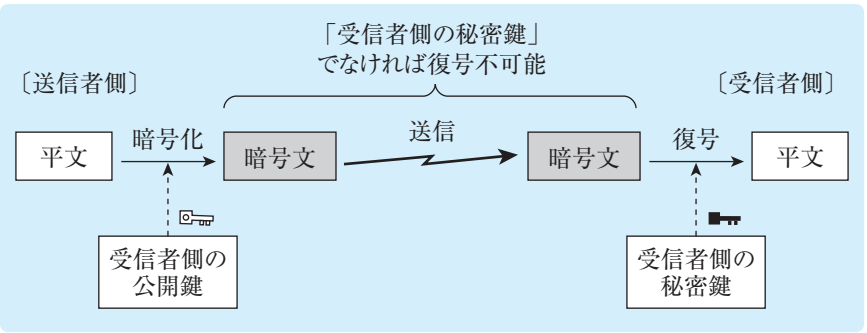

図4.4　公開鍵暗号方式の概念

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

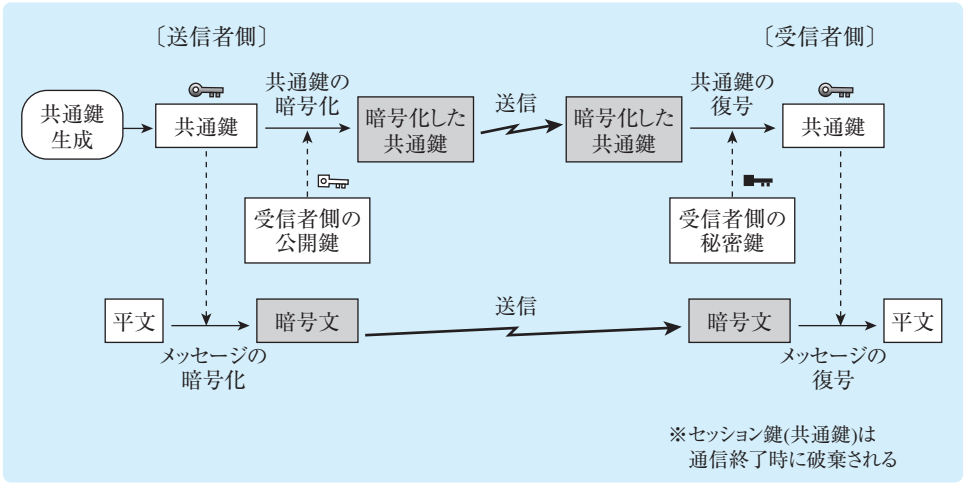

図4.5　ハイブリッド暗号方式

【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
→ ハイブリッド暗号方式

(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)，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)という特徴をもつことから，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。

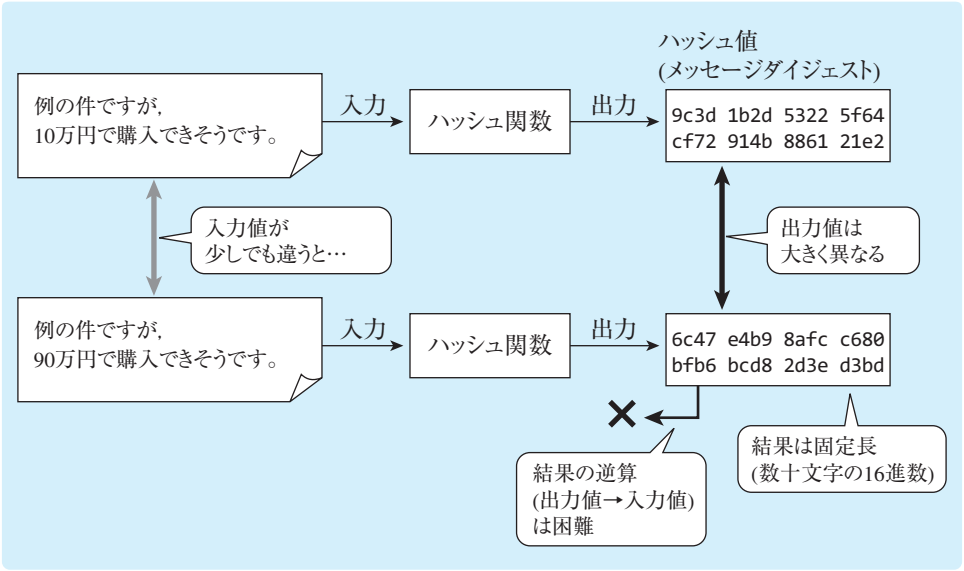

図4.6　ハッシュ関数

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。

【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

→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。

●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本人しか知りえない“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。

●リスクベース認証

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。

●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は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，パスワードの漏洩を防ぐことができる。認証の際は，

・利用者が入力したパスワードをハッシュ値に変換する
・保存されたハッシュ値と照合する

という手順で正しいパスワードかを確認する。

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。

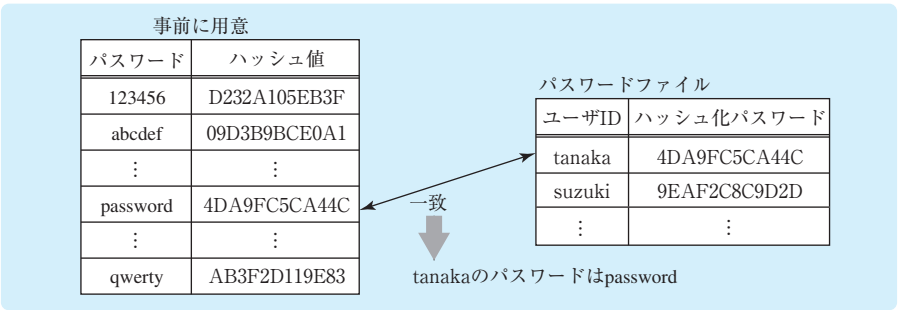

図4.7　パスワードファイルの解析

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。

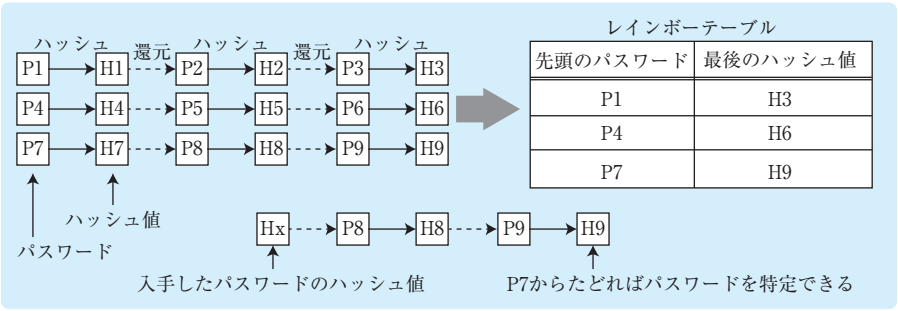

図4.8　レインボー攻撃

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。

(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。

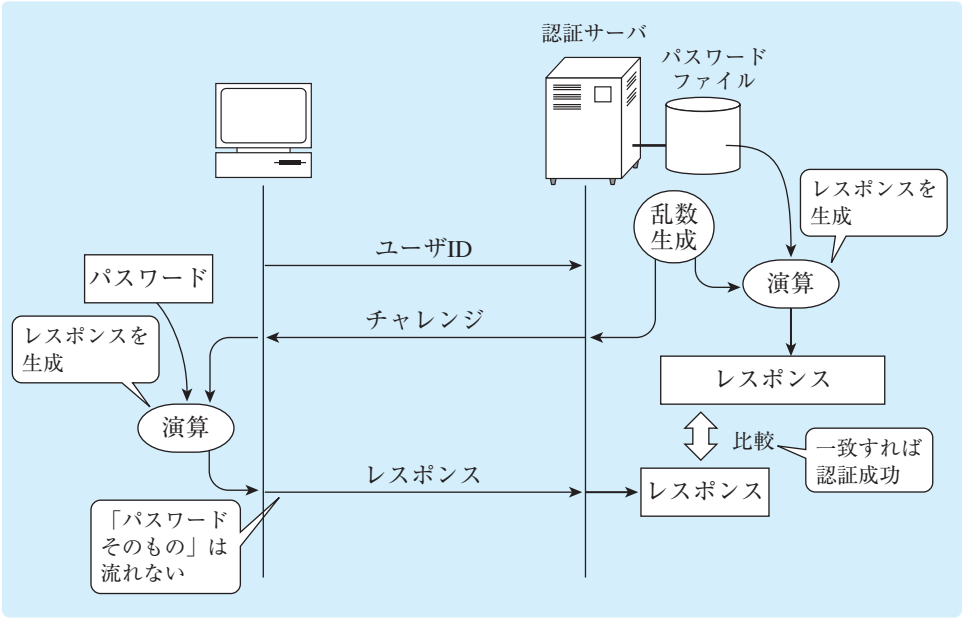

図4.9　チャレンジレスポンス方式

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。

●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，広く利用されている。

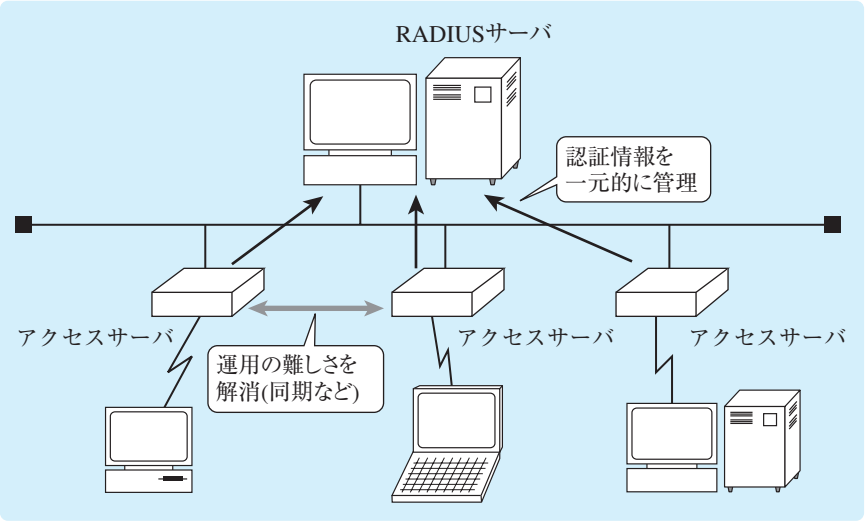

図4.10　RADIUSの概念

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。

参考：AAA

AAAとは，Authentication(認証)，Authorization(認可)，Accounting(アカウンティング)の総称である。RADIUSはAAAを実現できるため，広く用いられている。

表4.7　AAA

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
アカウンティング	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。

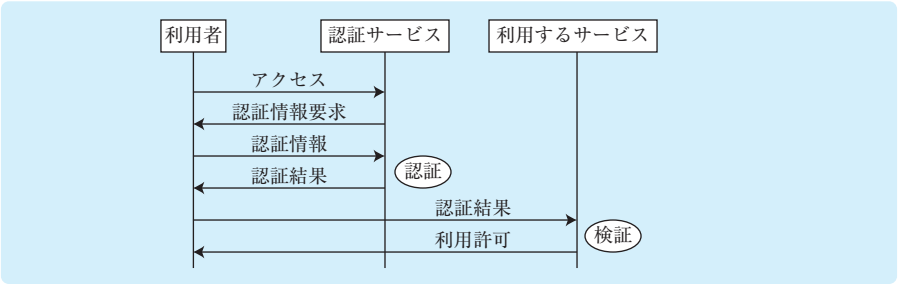

図4.11　SAML

(3)　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。

(4)　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。

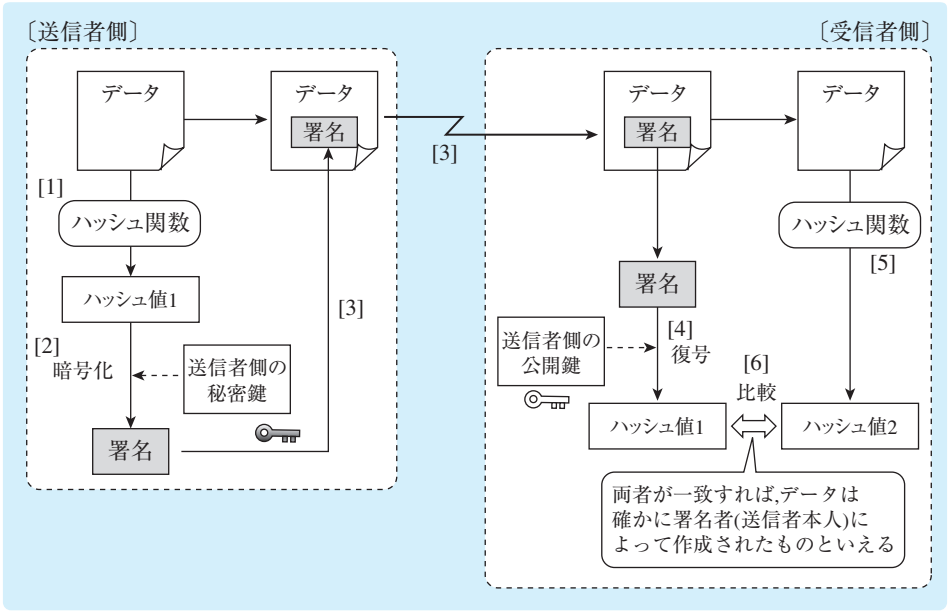

図4.12　デジタル署名

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。

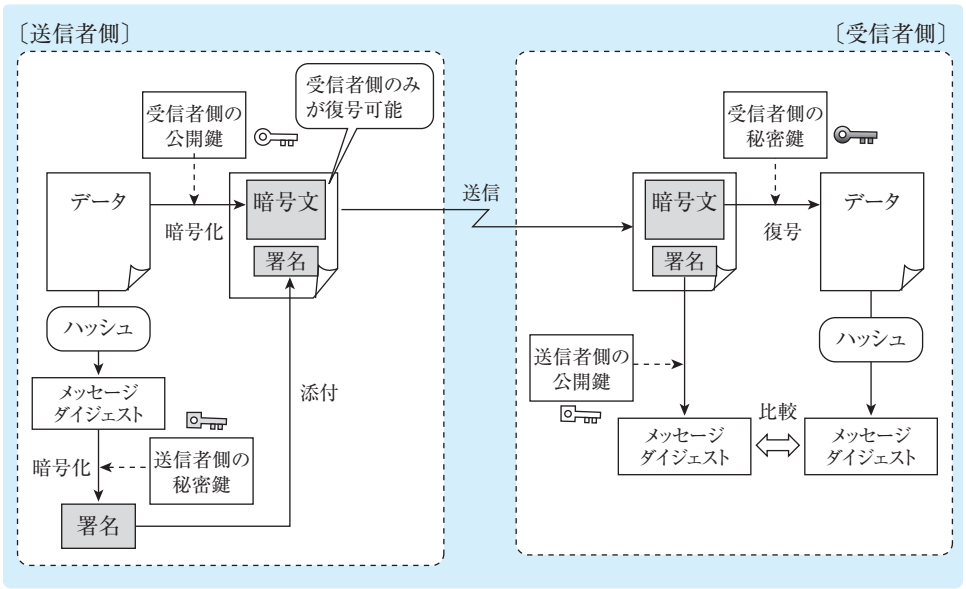

図4.13　デジタル署名と暗号化の組合せ