CompTIA Network+

Network+

Vol.2 テキスト

N10-004対応

TAC

6-3

暗号化と認証

6-3-1 暗号化

学習ポイント

ネットワークを介した情報のやり取りには、第三者に盗み見られてしまう（盗聴）危険性が伴います。盗聴に対するセキュリティ対策として暗号化技術があります。
暗号化技術について、そのしくみと特徴を理解しましょう。

1 暗号化とは

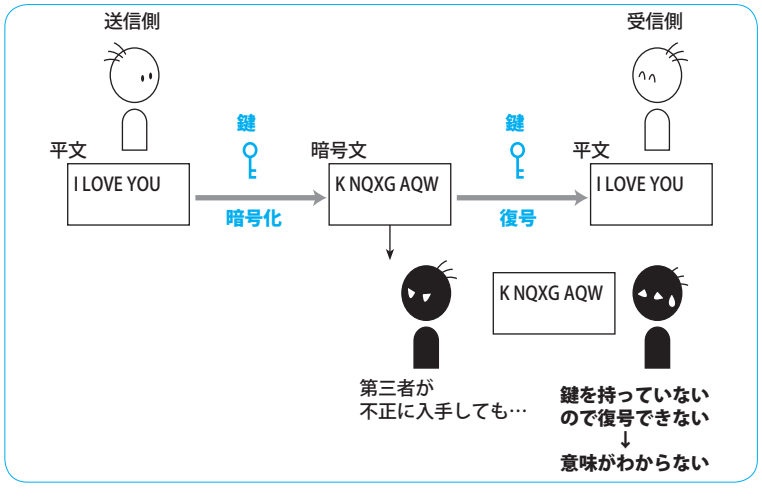
暗号化とは、データの盗聴や改ざんを避けるために、データを決まった規則に従って変換することをいいます。暗号化される前の元のデータを**平文**といい、暗号化されたデータを**暗号文**といいます。
暗号化処理は、次の２つの要素で成立しています。

- アルゴリズム … 暗号化の規則
- **鍵**…… 変換するための具体的な情報

例えば、暗号化処理として、「平文の各文字について、アルファベットを辞書順に２文字ずつずらす」という方法を用いる場合、次のようになります。

- アルゴリズム … 各文字のアルファベットをずらす
- 鍵…… ２（文字）

また、暗号文を元の形に戻すことを**復号**といいます。

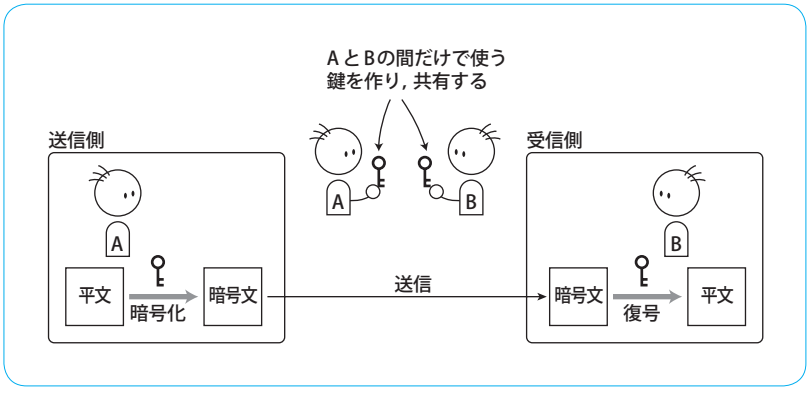


暗号化の概念

暗号化の方式は、鍵の使い方によって、**共通鍵暗号方式**と**公開鍵暗号方式**の２種類に大別できます。

2 共通鍵暗号方式

共通鍵暗号方式※は、暗号化と復号に同じ鍵（**共通鍵**）を利用します。送信側と受信側が、あらかじめ同じ鍵を共有しておき、この鍵を利用して暗号化・復号が行われます。



共通鍵暗号方式

● 共通鍵暗号方式の特徴

共通鍵暗号方式は、一般に次のような特徴があります。

● 鍵の種類が多くなる

複数の相手と暗号化によるデータのやり取りを行う場合は、AとB専用の共通鍵、AとC専用の共通鍵といったようにそれぞれすべて個別の鍵を用意する必要があります。

● 安全な鍵管理が困難

あらかじめ共通鍵を電子メールや郵便などで渡さなければならないため、相手に渡す過程において、第三者に鍵を盗み見られてしまう危険があります。

● 処理速度が速い

公開鍵暗号方式よりしくみが単純なため、暗号化・復号の処理速度は、公開鍵暗号方式に比べ速くなります。

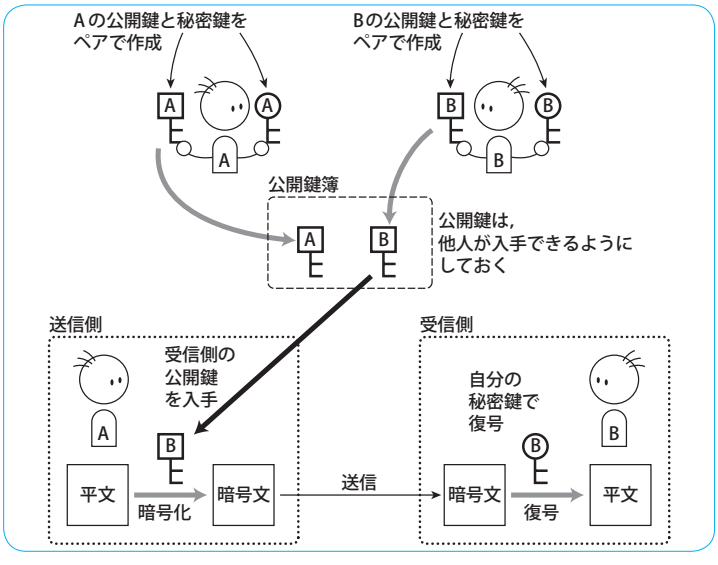
共通鍵暗号方式
対称鍵暗号方式、慣用鍵暗号方式、機密鍵暗号方式と呼ぶこともある。

3 公開鍵暗号方式

公開鍵暗号方式は、暗号化と復号に、それぞれ異なる鍵を用います。ユーザーは**公開鍵**と**秘密鍵**のペアを作成し、**公開鍵だけを公表します**。

メッセージを暗号化して送信するときは、送信者は**受信者の公開鍵で暗号化**した後に送信し、受信者は受け取った暗号文を、**受信者の秘密鍵で復号**します。

受信者の秘密鍵は受信者本人しか知らないので、この暗号文を第三者が入手しても、内容を知ることはできません。



公開鍵暗号方式

● 公開鍵暗号方式の特徴

公開鍵暗号方式は、一般に次のような特徴があります。

● 鍵の数が少なくて済む

各ユーザーがそれぞれ「自分の公開鍵」と「自分の秘密鍵」を作っておけば、暗号化通信が行えます。

● 鍵の管理が容易

公開鍵は、「公表してもよい鍵」なので、秘匿する必要がなく、秘密鍵は、「自分だけが知っていればよい」ので、他者に電子メールや郵送などで送る必要はありません。

● 処理速度が遅い

共通鍵暗号方式より仕組みが複雑なため、暗号化・復号の処理速度は、共通鍵暗号方式に比べ遅くなります。

4 ハイブリッド方式

ハイブリッド方式は、共通鍵暗号方式と公開鍵暗号方式の長所をうまく組み合わせ、効果的な暗号通信を行うための方式です。

ハイブリッド方式の手順

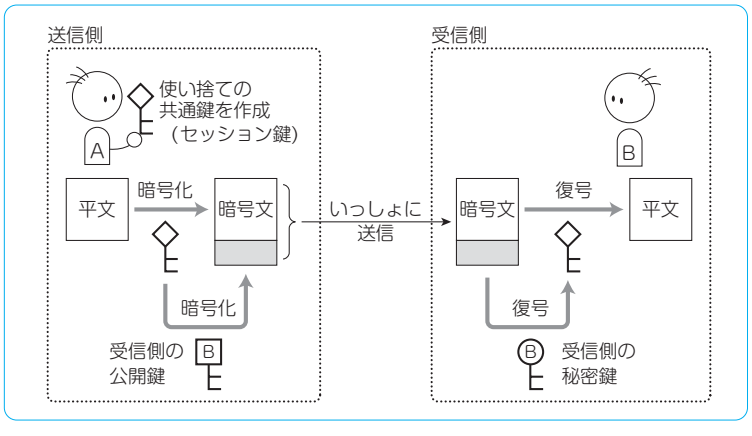
ハイブリッド方式の手順は次のようになります。

■送信側

① 今回の通信だけに用いる**使い捨ての共通鍵**（**セッション鍵**）を生成する。
② ①の共通鍵で、メッセージを暗号化する。
③ ①の共通鍵を、受信側の公開鍵で暗号化する。
④ ②で暗号化したメッセージと③で暗号化した共通鍵をセットにして、受信側へ送信する。

■受信側

⑤ 受信したデータから③の部分を取り出し、公開鍵で暗号化された共通鍵を自分の秘密鍵で復号し、共通鍵を得る。
⑥ ⑤で得た共通鍵で②の共通鍵で暗号化されたメッセージを復号する。



ハイブリッド方式

この時用いられる使い捨ての共通鍵は、通信が終わったら破棄されます。その通信（セッション）の間だけ有効な鍵なので、**セッション鍵**とも呼ばれています。

ハイブリッド式のメリット

ハイブリッド方式を用いると、次のようなメリットが得られます。

- メッセージの暗号化や復号は共通鍵暗号方式で行うので、高速になる。
- 共通鍵を公開鍵暗号方式で暗号化して送信するので、安全である。

6-3-2 デジタル署名

学習ポイント

ここでは、ハッシュ関数、デジタル署名、PKIについて学習します。これらは、データ通信における信頼性と安全性を確保し、なりすましや改ざんにおけるリスク対策として利用されています。そのしくみや特徴を理解しましょう。

1 ハッシュ関数

ハッシュ関数とは、任意の長さの情報から一定の長さの情報を作成する関数のことで、メッセージダイジェスト関数とも呼ばれています。

ハッシュ関数で作成された情報は、**ハッシュ値**と呼ばれ、ハッシュ値から元の情報へ戻すことはできません。また、異なった情報から同じハッシュ値を作成することは極めて困難です。この特性を利用して暗号化の補助やデジタル署名で、情報が改ざんされていないこと（完全性）の確認に応用されています。

2 デジタル署名

デジタル署名とは、メッセージ、ファイル、画像や映像など電子データについて、作成者が「本人のものであるかどうか」を証明するための技術です。デジタル署名が付いていれば、そのデータは、作成者本人のものであることが証明されます。一般にデジタル署名では、公開鍵暗号方式とハッシュ関数を利用しています。

メッセージにデジタル署名を添付する基本的な手順を次に説明します。

■送信側

① ハッシュ関数を使って、メッセージからハッシュ値を作成します。

② ①のハッシュ値を送信者が持つ秘密鍵で暗号化し、デジタル署名を作成します。

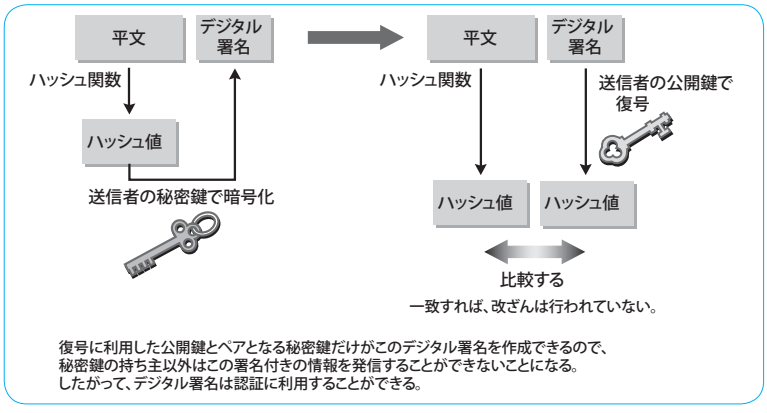
③ ②のデジタル署名をメッセージに添付して送信します。

■受信者側

④ 受信したデータからメッセージを取り出しハッシュ値を作成します。

⑤ 受信したデジタル署名を取り出し、送信者の公開鍵で復号します。

⑥ ④で作成したハッシュ値と⑤で復号したハッシュ値を比較し一致すれば、受け取ったメッセージは改ざんされていないことが証明されます。また、公開鍵で復号したデジタル署名は、ペアとなる秘密鍵だけが作成できるので、持ち主以外は、この署名付きの情報を発信できないことになり、作成者が本人であることを証明できます。



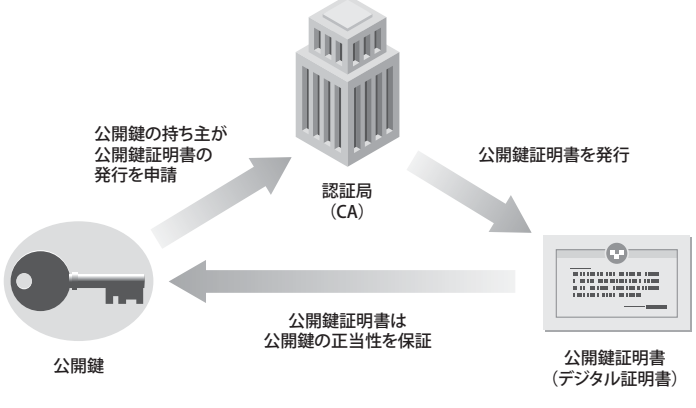
デジタル署名のしくみ

3 PKI

悪意の第三者が送信者になりすまし、「私は○○です。これが私の公開鍵です」と言って偽の公開鍵を送ってきた場合、デジタル署名を検証しても意味がないことになります。このような「**なりすまし**」を排除するために、公開鍵の正当性を証明する第三者機関が存在します。この第三者機関を**認証局**（**CA**：シーエー：Certificate Authority）といいます。

公開鍵の作成者は正当性を保証してもらうために、あらかじめ認証局へ申請を行い、認証局は、作成者の情報と公開鍵を含んだデジタル証明書を発行します。公開鍵を使ってデジタル認証の確認を行うユーザーは、デジタル証明書により本物の公開鍵であることが確認できます。

このように、認証局を利用して公開鍵の正当性を確認しながら、公開鍵暗号を安全に利用できるようにするしくみを**公開鍵基盤**（**PKI**：ピーケーアイ：Public Key Infrastructure）といいます。



PKIの構成要素

6-3-3 ユーザー認証

学習ポイント

不正アクセスを防止するための技術としてユーザー認証があります。ここでは、ユーザー認証の種類について、その特徴を理解しましょう。

1 ユーザー認証とは

ユーザー認証とは、ある資源を利用するユーザーが、**正当なユーザーかどうかを検証する**ことをいいます。例えば、コンピュータを使用する際やあるWebサービスを利用する際、社内のネットワークに接続する際、銀行のATMを利用する際、特定の部屋へ入室する際など、さまざまな場面で不正なアクセスから守るため、ユーザー認証が用いられています。
ユーザー認証の方式には次のようなものがあります。

● パスワード認証

パスワード認証は、ユーザーに対して割り当てられた識別番号であるユーザー名とパスワードをセットで用います。入力されたユーザー名とパスワードは、クリアテキスト（平文）として送信されます。ただし、これでは危険なため、パスワードを暗号化して送信するよう設定されているのが一般的です。

パスワード認証の例

● ワンタイムパスワード

ワンタイムパスワードは、同じパスワードを何回も使うのではなく、ログインのたびに使い捨てのパスワードを生成・利用する方式です。仮にその時に使ったパスワードが漏洩しても、次のログイン時には使えなくなっているので、強固なセキュリティが実現できます。

ICカード認証

ICカード認証は、半導体集積回路（ICチップ）を埋め込んだ**ICカード**を利用して、本人の正当性を認証する認証方式です。ICチップに持ち主の情報を保存し、ログイン時にそれを読み取って照合することで、認証を行います。ICカードは、**スマートカード**とも呼ばれ、キャッシュカードやクレジットカード、電子マネー用カード、身分証IDカード、交通機関の乗車券、オフィスの入退出管理など幅広く活用されています。

また、ICチップにある情報は、暗号化が可能なため、偽造は難しいとされています。

バイオメトリクス認証

バイオメトリクス認証は、ユーザー認証のひとつで、ユーザーを識別するために指紋や虹彩、声紋、手のひらの静脈パターンといった、人間の身体的な特徴を利用する認証方式です。「生体認証」と訳されるもので、すでに銀行のATMでも利用され始めています。

また、バイオメトリクス認証は、ユーザー本人の生体特徴を認証に使用するため、偽造されにくく、盗難されないというメリットがあります。

指紋を利用したバイオメトリクス認証のUSBフラッシュメモリ

ゼロ知識証明

ゼロ知識証明（Zero Knowledge Proof）とは、パスワードなど、本人だけが知っている秘密情報を使った認証において、秘密情報自体を証明者と検証者の間で送受信することなく証明する認証方式です。**ゼロ知識対話証明**とも呼ばれています。

具体的には、検証者が持っている情報と乱数から演算した結果を問いにして、証明者が答えるというやり取りを複数回行うことで、証明者の正当性が証明されます。証明者は、秘密情報を送ることなく正当性を証明できるので、盗聴によるなりすましを防止できます。

二要素認証

二要素認証とは、ユーザーに固有な二つの要素を組み合わせて確実に認証する方式です。

例えば、銀行のATMを利用するときなどでは、ユーザー所有のキャッシュカードとユーザーだけが知っている暗証番号という2つの要素を組み合わせて、認証を行います。

6-3-4 認証プロトコル①

学習ポイント

ここでは、認証、認可、アカウンティングの3つの制御を持ったシステムや機能、枠組みを指すAAAと認証プロトコルのRADIUS、TACACS+について学習します。
AAA、RADIUS、TACACS+それぞれの特徴やしくみについて理解しましょう。

1 AAA

AAA（トリプルエー：Authentication Authorization Accounting）は、**認証**（Authentication）、**認可**（Authorization）、**アカウンティング**（Accounting）の頭文字をとったもので、認証、認可、アカウンティングの3つの制御を持ったシステムや機能、枠組みをいいます。

認証とは、正当なユーザーかどうか本人確認を行うことで、例えば、ユーザーアカウントとパスワードなどで、そのユーザーがサービスに接続する正当性があるかを確認します。

認可とは、認証済みのユーザーに対して提供できるサービス、提供できないサービスを判断することで、権限に応じて個々のユーザーが利用できるサービスを制限します。

アカウンティングは、課金とも訳されることがありますが、サービス利用の事実を記録することで、ユーザーが入力した情報や接続時間、システムイベントなどをログとして記録することをいいます。

AAAをサポートしたネットワーク機器では、アクセスしてきたユーザーに対して、認証を行い、権限に応じたアクセスを許可し、ログを取ることができ、また、認証、認可、アカウンティングを行うために、RADIUS、TACACS+、Kerberosなどの認証プロトコルを使用してサーバーと通信させるように設定するのが一般的です。

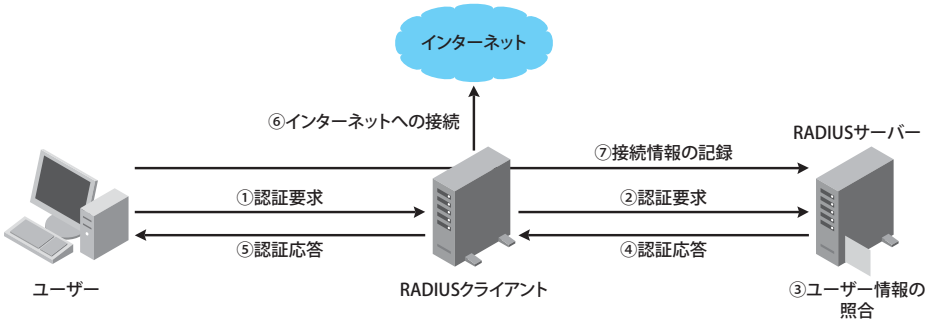
2 RADIUS

RADIUS（ラディウス：Remote Authentication Dial-In User Service）は、Livingston Enterprise社が開発した認証プロトコルです。名称にDial-Inとあるように、**ダイヤルアップ**によるインターネット接続サービスのために開発されました。現在では、ADSLや光ファイバーなどの常時接続サービスや、無線LAN、VLAN、コンテンツ提供サービスなど、さまざまなサービスで幅広く利用されています。

RADIUSでは、認証機能と接続機能を切り離し、ユーザー情報を一元管理し認証などを行う**RADIUSサーバー**と、直接ユーザーやRADIUSサーバーと通信する**RADIUSクライアント**で構成されています。

RADIUSのしくみ

ユーザーは、RADIUSクライアントに接続し認証要求を行います。RADIUSクライアントは、RADIUSサーバーにユーザーからの認証要求を送信し、認証情報を確認します。RADIUSサーバーは、管理しているユーザー情報と認証要求を照合しサービス利用の可否をRADIUSクライアントに返信します。RADIUSクライアントからユーザーに認証要求の結果が返信されます。これによりRADIUSサーバーによってサービス利用の許可を得たユーザーは、サービスを利用することができます。このとき、サービスの利用情報などは、RADIUSサーバーに記録されます。



RADIUSのしくみ

RADIUSでは、認証情報として、もともとユーザーIDと固定のパスワードが利用されていましたが、現在では、ワンタイムパスワードやバイオメトリクスなども利用できるように拡張されています。

3 TACACS+

TACACS+（タカクスプラス：Terminal Access Controller Access Control System Plus）は、BBN社が開発したTACACSをベースに、Cisco Systems社が独自に拡張した認証プロトコルです。TACACS+もRADIUSと同じように、ユーザーの認証情報を管理する認証サーバーと、ユーザーや認証サーバーと通信を行うアクセスサーバーによって、認証、認可、アカウンティングを行うことができます。RADIUSでは、クライアントとサーバーの通信において、**UDP**を使用しているのに対し、TACACS+では、**TCP**を使用し信頼性を高めています。