実務に役立つ情報セキュリティの基礎

CompTIA Security+™

S+ Security テキスト

現場でも役立つ知識が身に付く

合格に必要な全知識をわかりやすく解説

SY0-301対応

TAC

2-1 暗号化

2-1-1 暗号化とは
2-1-2 対称暗号方式と非対称暗号方式
2-1-3 ハイブリッド方式とその他の暗号方式
2-1-4 暗号アルゴリズム
2-1-5 ハッシュ化
2-1-6 暗号の利用

2-1-1 暗号化とは

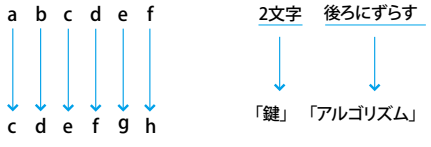
学習ポイント

暗号とは、送信者と受信者以外の他人には見られたくない情報を安全にやりとりするための方法です。ここでは暗号とはどういうものなのか学習します。鍵とアルゴリズムという用語をキーワードに暗号の仕組みを理解しましょう。

1 暗号技術

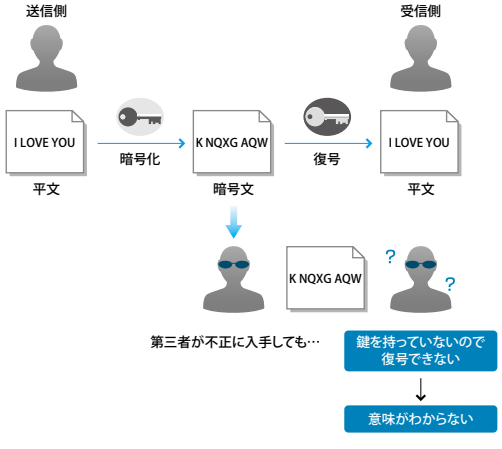
機密性と完全性を維持するための情報セキュリティの基盤技術のひとつが、暗号技術です。プログラムやデータなどを、一定の規則で変換し、意味が通らない情報とすることで、一定の規則を知るもののために機密性と完全性を担保します。変換する前の情報を「**平文**（ひらぶん）」、変換後の情報を「**暗号文**」と呼び、平文を暗号文に変換することを「**暗号化**」といいます。

例えば「abc」という文字列の場合、それぞれの文字をアルファベットの並びで2文字後ろにずらすと「cde」という文字列になります。これを暗号化といいます。このとき、「後ろにずらす」という変換方法を「**アルゴリズム**」と呼び、何文字なのかといった部分（手順を制御する規則となるデータ、因数）が暗号化の「**鍵**」になります。例にあげたこの方法は「**シーザー暗号**」と呼ばれています。



シーザー暗号の仕組み

暗号文は、適切なアルゴリズムと鍵を用いることで平文へ戻すことができます。これを**復号**といいます。暗号技術はこの考え方を発展させ、特徴の異なる多くの技術が開発されています。暗号技術を目的にあわせて選択ができるようにしましょう。



暗号化の概念

2-1-2 対称暗号方式と非対称暗号方式

学習ポイント

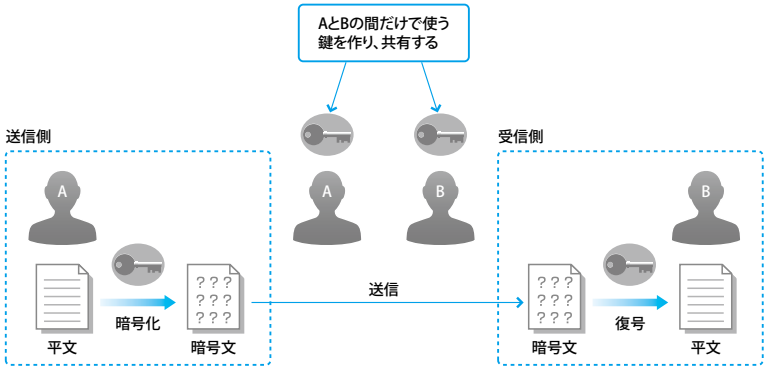
暗号化の方式は、大きく2種類に分けられ、それぞれ、暗号化のための鍵をどのように利用するかによって分類されます。ひとつは対称暗号（共通鍵暗号）方式で、もうひとつは非対称暗号（公開鍵暗号）方式と呼ばれる方法です。

1 対称暗号方式

対称暗号（**共通鍵暗号**）方式は暗号化処理と復号処理に同じ鍵を利用します。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。これは、共通の鍵を持っていれば玄関のドアを開けられるのと同じ使い方です。

対称暗号方式は、暗号化を行う処理と復号するための処理を高速に行うことが可能です。しかし、暗号化/復号を行うためには、情報を伝えたい相手にあらかじめ共通に利用する鍵を渡しておかなければなりません。また、複数の相手とやりとりを行う場合は、相手別に個別の鍵を用意する必要があるため鍵の数が多くなります。

対称暗号方式では、あらかじめ鍵を渡さなければならないため、相手に渡す過程で鍵が盗まれないようにしなくてはなりません。また、その鍵を双方で安全に管理する環境も必要です。



対称暗号方式

● 対称暗号方式の鍵の管理

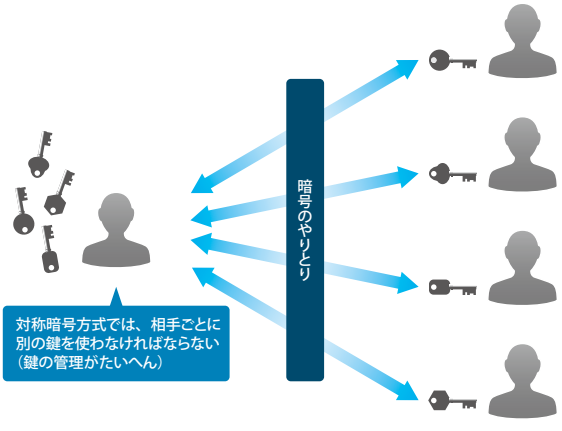
AさんとBさんが互いに暗号化通信を行う場合を考えてみましょう。

まず対称暗号方式を利用する場合では、互いが暗号化と復号のための処理に利用する共通の鍵を持つ必要があります。この共通鍵は他のだれにも知られないようにしておかなければなりません。鍵そのものが他人にもれてしまうと、暗号化した内容が覗き見られてしまうだけでなく、AさんやBさんになりすまして、偽の情報を送ることも可能になります。

つまり、AさんがBさん以外の人とさらに暗号化通信を行うような場合には、さらに「別の」共通鍵が必要になります。

もし、Aさんが、数十人程度の相手と暗号化通信を行うだけであれば、多少の苦労はしますが、鍵を管理することは可能です。

しかし、それ以上の何千、何万の人とそれぞれに暗号化通信を必要とする場合には、おそらく鍵の管理に多大な負荷がかかるでしょう。



鍵の管理（対称暗号方式の場合）

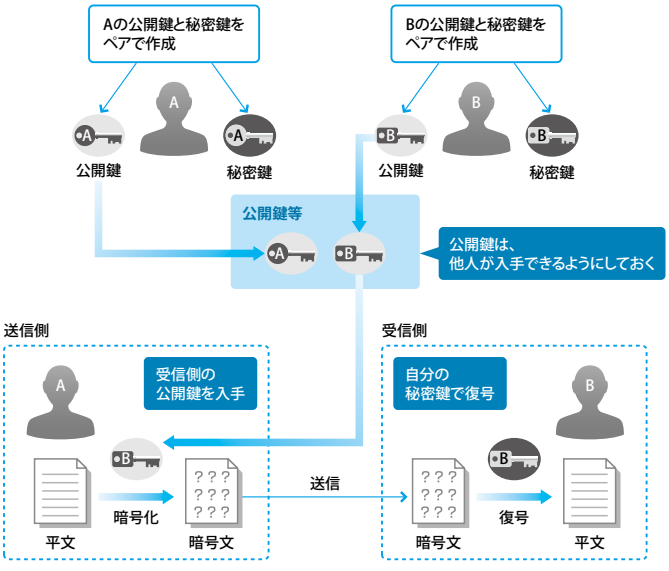
2 非対称暗号方式

非対称暗号（**公開鍵暗号**）方式は、暗号化処理と復号処理に別々の鍵を利用する方法です。

ユーザーは**公開鍵**と**秘密鍵**のペアを作成し、公開鍵だけを公開します。送信者は受信者の公開鍵で暗号化して送信し、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。

非対称暗号方式では、暗号化のための鍵はだれもが利用できるように公開しておくことができます。そのため、自分宛に暗号化した情報を送ってもらうときに、だれもが同じ公開鍵を利用して暗号化処理ができるので、復号のための鍵は1つで済むことになり、鍵の管理が簡単になります。

ただし、非対称暗号の暗号化/復号にかかる時間は、対称暗号方式にくらべると仕組みが複雑なため非常に長い時間がかかります。そのため、リアルタイム性が必要とされるような情報のやりとりには向いていません。



非対称暗号方式

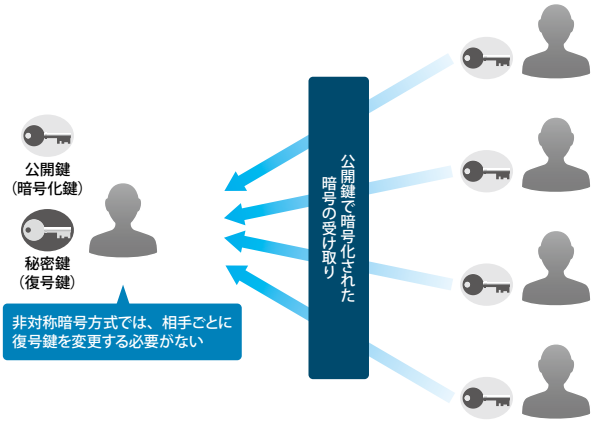
● 非対称暗号方式の鍵の管理

次に非対称暗号方式を利用する場合を考えてみます。

Aさん宛に送られる情報を暗号化するために公開鍵を利用すると、Aさんはその暗号文を復号するためには、その公開鍵に対応する秘密鍵を利用します。

この場合では、Aさん宛に暗号化した情報を送りたいと希望する人は、だれもがAさんの持つ秘密鍵とペアとなる公開鍵を利用すればよいことになります。

つまり、暗号化通信を不特定多数の人と行う場合でも、人数分の鍵を用意する必要はないのです。



鍵の管理（非対称暗号方式の場合）

確認問題　2-1 暗号化

次の［　　］に当てはまる語句を答えてください。

□ 1. シーザー暗号では、意味が通る文字列をそれぞれの文字をアルファベットの並びで数文字ずつ後ろにずらし、暗号化します。このときの「後ろにずらす」ことを［①］と呼び、「何文字ずらす」ということを［②］といいます。

□ 2. 暗号化の方式は、暗号化と復号に同じ鍵を使う［③］暗号（対称暗号）と暗号化と復号に異なる鍵を使う［④］暗号（非対称暗号）があります。また、［③］と［④］を組み合わせた暗号方法を［⑤］方式といいます。

□ 3. ［⑥］関数は、不特定な長さのデータから固定長のデータを生成する関数です。生成されたデータを［⑥］値（または［⑦］ダイジェスト）と呼びます。

□ 4. 暗号アルゴリズムには、暗号化の対象となる情報をある大きさに区切って暗号処理を行う［⑧］暗号と、情報の単位ごとに暗号処理を行う［⑨］暗号があります。

□ 5. ［⑩］署名は、情報の完全性を保証するため、送信する平文（情報）のメッセージダイジェストを送信者側の秘密鍵で暗号化し、平文に付加して送信します。受信側は受信した平文からメッセージダイジェストを生成します。さらに、受信したデジタル署名を送信者側の［⑪］鍵で復号し、平文から生成したメッセージダイジェストとデジタル署名を復号したメッセージダイジェストが一致することを確認します。

□ 6. 画像データなどに他のデータを埋め込むことを［⑫］といいます。［⑫］を応用すると、著作権保護のための情報を画像などに含ませることができるため、［⑬］の技術として利用できます。

□ 7. ［⑭］は、乱数によって生成された1回限り有効な鍵のことです。［⑭］によってデータの暗号化と復号を行いますが、一度使った鍵は再利用せず破棄されます。

答え

①アルゴリズム　②鍵　③共通鍵　④公開鍵　⑤ハイブリッド　⑥ハッシュ　⑦メッセージ
⑧ブロック　⑨ストリーム　⑩デジタル　⑪公開　⑫ステガノグラフィー　⑬電子透かし
⑭ワンタイムパッド

章末問題

Q1

自宅の無線LANではAESによる暗号を利用しています。これは次のどの暗号方式ですか。

- **a.** 対称暗号
- **b.** 非対称暗号
- **c.** 公開鍵暗号
- **d.** 量子暗号

A a

無線LANでデータの暗号化に使用されるAESは高速な処理が可能な対称暗号方式です。対称暗号方式は送受信に同じ鍵を使用する簡単な仕組みのため、非対称暗号方式よりも処理が高速であるという特徴があります。そのため、リアルタイム通信では対称暗号方式がよく使用されています。

共通鍵はその受け渡しに注意しないと、セキュリティレベルを保つことが難しくなります。そこで、暗号化処理は対称暗号で行い、その共通鍵の受け渡しに非対称暗号を利用する、といったハイブリッド方式を使う場合が多くなっています。

Q2

ハッシュを使用する目的はどれですか。

- **a.** データの暗号
- **b.** ユーザー認証
- **c.** 盗聴防止
- **d.** 改ざん検出

A d

ハッシュ関数は、作成された情報から元となる情報を導き出すことはできません。作成される情報（メッセージダイジェスト）は、原則的に元の情報が異なるものであれば、同じものにはなりません。このため、インターネット上でのやりとりなどで、情報の改ざん検出に利用されています。

送受信されるデータを通信途中で盗聴されないために、インターネット上では、VPN技術などに内蔵される暗号化が使用されています。VPNでは、暗号とともに認証を行うことで、適切な相手とだけ通信を行うことができます。