はじめに

最近では、世界中のさまざまな場所からでもネットワークを接続することができるようになり、それを使って大量のデータベースの中から、いつでも必要なときに必要な情報を引き出せるようになりました。しかし、このように便利になった反面、情報の漏えいなどの事故も起き“セキュリティ”に関わる報道も、新聞やテレビなどでもよく見かけるようになりました。社会的な信用低下などを恐れて、今やセキュリティ対策を考えない企業や団体はほとんどなくなりました。

このように報道される“セキュリティ”の多くが「情報セキュリティ」のことを指しています。現在ではそれだけ、企業や団体、また個人でも、情報セキュリティの脅威を感じ、その対策に時間とお金をかけるようになっています。ただ、情報セキュリティの対策には「完全」というものがありません。また、そのセキュリティレベルがどの程度なのかといった指針も明確なものがなく、あいまいな知識でセキュリティ対策や管理を行うことにより、セキュリティの脅威にさらされてしまうことすらあります。

情報セキュリティに従事している（もしくは興味のある）方は、これらの知識を体系的に知っておく必要があります。しかし、そのような知識をじっくりと学ぶことも難しいのではないでしょうか。

資格試験や検定試験はそのような方の学習の機会を広げてくれる場であると考えてください。

本書は、「情報セキュリティ初級認定試験」対策用の書籍とはなっていますが、情報セキュリティの基礎を体系的に学びたい方に対して、管理と技術の両面から脅威と対策に分けて情報セキュリティに必要な内容を掲載しています。そのため、検定試験を受験する、しないに関わらず本書を利用することでセキュリティの知識が身に付くような構成となっています。

本書を利用して、みなさまの情報セキュリティ知識と意識が向上することを心から願います。

2021年4月

五十嵐　聡

Ⅲ-7 外部からの攻撃の脅威

コンピュータシステムをネットワークに接続していると、外部からさまざまな方法で攻撃を受ける可能性があります。攻撃の種類と脅威について理解しておきましょう。

KEYWORD

□辞書攻撃	□ブルートフォース攻撃	
□リバースブルートフォース攻撃	□パスワードリスト攻撃	
□DoS攻撃／DDoS攻撃	□無線LAN	□MACアドレス
□ESSID	□WPA2／WPA3	□コンピュータウイルス
□踏み台	□不正中継	□クッキー（Cookie）

ネットワークを使用した攻撃

コンピュータシステムをネットワークに接続している場合、外部からのさまざまな脅威が考えられます。代表的なものを説明します。

◎パスワードの推測

辞書攻撃は、辞書などに載っている単語を順にパスワードとして試していき、パスワードを推測する攻撃です。また、文字、数字、単語などのすべての組み合わせを順に試してパスワードを推測する**総当たり（ブルートフォース攻撃）**もあります。そのため、管理者用をはじめとする各種パスワードを推測しにくいものにすることはもちろん、定期的に変更することも必要です。また、最近ではありそうなパスワードを固定してIDを順に変えてアクセスする**逆総当たり（リバースブルートフォース）攻撃**でログインするケースもあります。

◎パスワードリスト攻撃

あるWebサイトから流出した利用者IDとパスワードのリストを用いて、他のWebサイトに対してログインを試行する攻撃のことです。

◎DoS攻撃／DDoS攻撃

DoS（Denial of Service）**攻撃**または**DDoS**（Distributed Denial of Service）**攻**

撃とは、大量のパケットをサーバに送りつけてサーバが他の処理を実行できない状態にし、正規のユーザからのアクセスを受け付けられないようにする攻撃のことです。DoS攻撃にはSYN FLOOD、LAND、TEAR DROP、Ping of Deathなどがあります。

無線LAN

最近では無線LANを使用するシステムが増加しており、その分セキュリティ上の脅威も大きくなっています。

◎無線LANの仕様

無線LANの主な仕様は、次のとおりです（**表Ⅲ-7-1**）。

▼**表Ⅲ-7-1　無線LANの仕様**

無線LANの規格	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n	IEEE 802.11ac
周波数	5GHz	2.4GHz	2.4GHz	2.4GHz/ 5GHz	5GHz
最大実効速度	54Mbps	11Mbps	54Mbps	600Mbps	6.9Gbps
変調方式（物理層）	OFDM	CCK、QPSKなど	OFDM、PBCC	OFDM	OFDM
MAC層	CSMA/CA				

◎無線LANへの脅威

無線LANについては、次のような脅威が存在します。

1. MACアドレスの盗聴

無線LANでは、アクセスポイントに無線端末の**MACアドレス**を送信します。このとき、MACアドレスが暗号化されていないため、MACアドレスの盗聴によりなりすましが可能となってしまいます。

2. ESSIDの脅威

ESSID（Extended Service Set Identification）は、無線端末が接続できるアクセスポイントを識別するために使用するIDです。ESSIDも暗号化されていないために、盗聴の危険があります。また、ESSIDとして「ANY」を使用するとすべてのアクセスポイントに接続できます。これは、悪意のある第三者による不正アクセ

Ⅲ-8 ネットワーク攻撃対策

ネットワークに接続しているコンピュータシステムは、外部からさまざまな方法で攻撃を受ける可能性があります。攻撃の種類と脅威に応じた対策について学習します。

KEYWORD

□プロキシ	□フォワードプロキシ	□URLフィルタリング機能
□リバースプロキシサーバ	□IEEE 802.1X	□IEEE 802.11i
□TKIP	□AES	□WPA2
□CCMP	□WPA3	□GCMP

プロキシサーバ（フォワードプロキシ）

インターネット上のサーバに組織内のコンピュータが直接アクセスすると、そのコンピュータのIPアドレスなどが外部に判明してしまい、不正アクセスなどの危険性が増加します。そこで、組織内に外部とのアクセスを中継するサーバを設置し、そのサーバが外部のサーバに代理でアクセスし、コンピュータに返す方法を取ります。このために設置するサーバを**プロキシサーバ**といいます（**図Ⅲ-8-1左**）。

この方法によって、プロキシサーバのIPアドレスだけが外部に判明するため、安全性が高まります。また、プロキシサーバには、一度アクセスしたWebコンテンツをキャッシュする機能もあるため、同じ組織内の別のコンピュータが同じページにアクセスした場合、プロキシサーバに保存されているページの内容が結果として返されます。これによって、アクセス速度の高速化を図れます。

◎URLフィルタリング機能

プロキシサーバには、URLフィルタリングやキーワードフィルタリング機能が備えられています。設定したURLやキーワードへのアクセスを禁止したり、設定したURLへのアクセスだけ許可し、他のURLへのアクセスをすべて禁止したりすることができます。

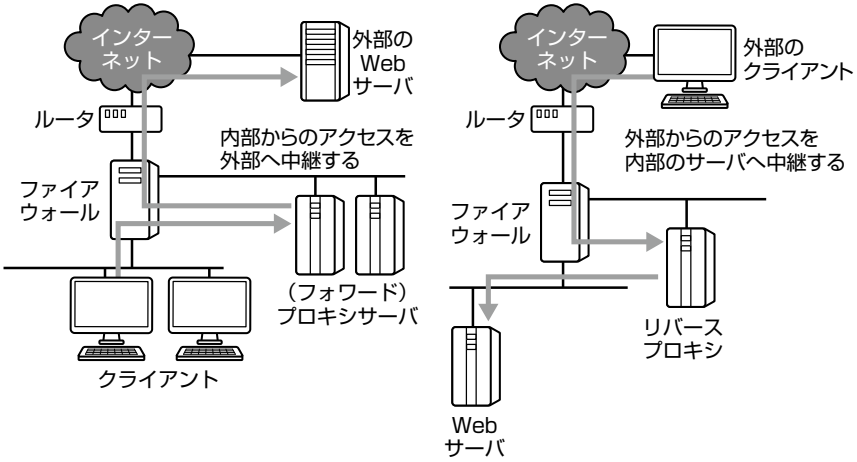
リバースプロキシサーバ

主にDMZ上に設置されるサーバで、外部から社内のWebサーバに対して到達す

るアクセスをいったん受け取り、そのアクセスをWebサーバに割り振る役割をします（**図Ⅲ-8-1右**）。利用するメリットは次のとおりです。

- Webサーバが外部からのアクセスに直接さらされなくなるので、安全性が向上する。
- 複数のWebサーバに、平均的にアクセスを分けることで負荷分散が実現できる。

▼**図Ⅲ-8-1　フォワードプロキシとリバースプロキシの例**



無線LANの対策

無線LANでは、脅威への対策としてMACアドレスのフィルタリングやESSIDを使用した認証などが考えられます。また、以前は暗号化にWEPが使われていましたが、WEPには暗号化のかぎ長が短いなどの問題があるため、現在では主に次の技術が利用されています。

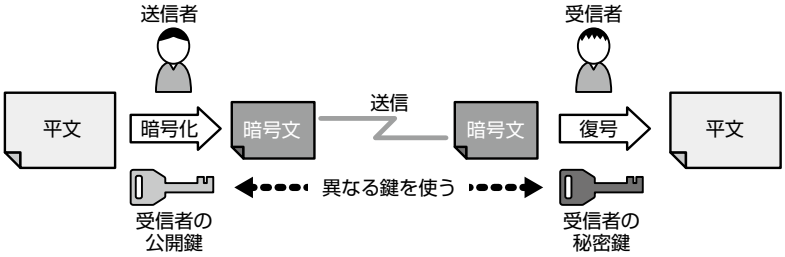
◎IEEE 802.1X

IEEE 802.1Xは、認証サーバ(RADIUSなど)を用いてEAP(Extensible Authentication Protocol）をベースに認証を行うための規格です。

◎IEEE 802.11i

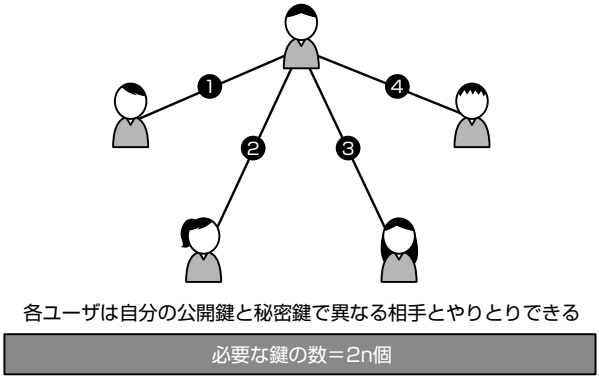
IEEE 802.11iは認証にIEEE 802.1Xを、暗号に**TKIP**（Temporal Key Integrity Protocol）および**AES**（Advanced Encryption Standard）を使用するセキュリティ

▼図Ⅲ-9-3　公開鍵暗号方式の特徴



公開鍵暗号方式では、暗号化する鍵（**公開鍵**）と復号する鍵（**秘密鍵**）が異なるため、複数の送信相手に対して同じ鍵で暗号化を行い、データを送信することができます（**図Ⅲ-9-4**）。

▼図Ⅲ-9-4　公開鍵暗号方式で利用する鍵の数



公開鍵暗号方式の場合、n人の間で使用するネットワークでは2n個の鍵が必要になります。このとき、各ユーザが管理する鍵の数は2個です。

公開鍵暗号方式の種類

公開鍵暗号方式には、いくつかの種類があります。

1. RSA

RSA（Rivest Shamir Adleman）では、暗号を解読するのに非常に大きな数の素因数分解を行う必要があります。そのため、効率的な解読方法は発見されていませ

ん。公開鍵暗号方式では、最も代表的な暗号方式として知られています。鍵に使用できるビット長には、512ビット、1,024ビット、2,048ビットなどがあります。

2. 楕円曲線暗号方式

楕円曲線暗号方式は、楕円曲線という特殊な計算を行って暗号化する方式です。この方式では、RSAより短い長さの鍵で暗号化を行うことができます。そのため、ICカードなどのハードウェアで使用されることがあります。

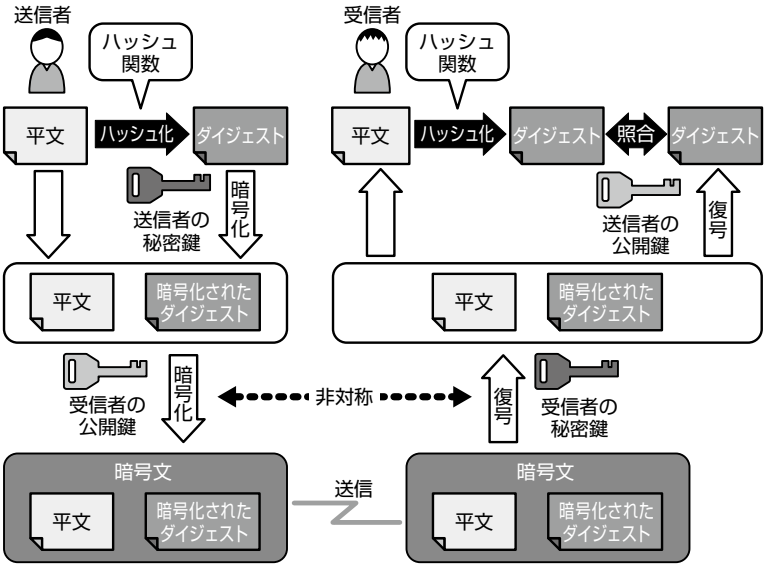
3. DSA

DSA（Digital Signature Algorithm）は、エルガマル署名を改良して作られた暗号方式です。鍵長が1,024ビット以下で、署名鍵の生成などを特定の方法で運用するデジタル署名に利用されます。

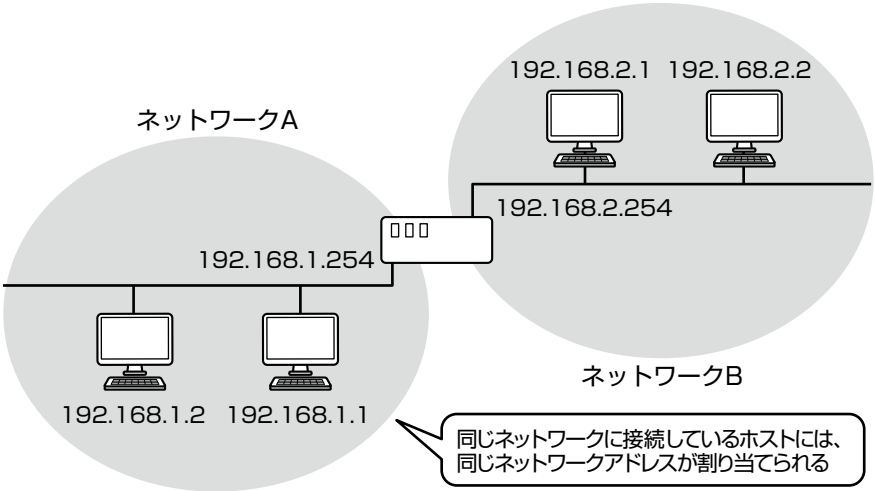
デジタル署名

公開鍵暗号方式を使用しても暗号化を行った人物が本人である保証はありません。そこで、なりすましや改ざんが行われていないかどうかを検知する方法として**デジタル署名**（**図Ⅲ-9-5**）や**MAC**（メッセージ認証コード）などを利用することができます。

▼**図Ⅲ-9-5　デジタル署名**



▼図Ⅳ-5-3　ネットワーク部とホスト部の概念



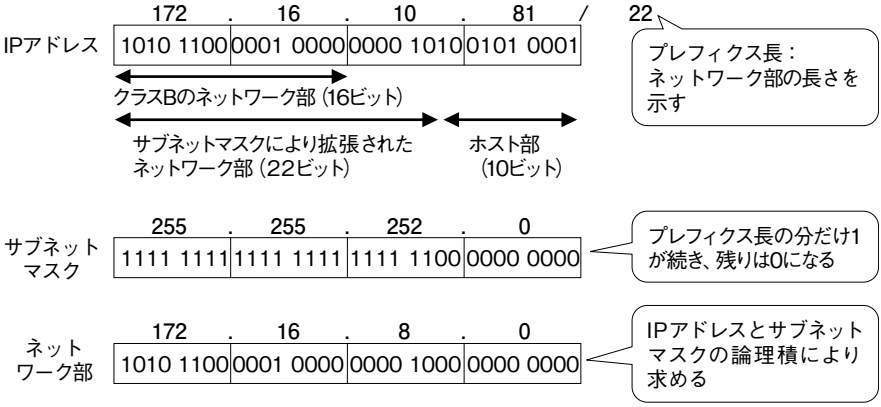
◎サブネットワーク

IPアドレスでは、どこまでがネットワーク部で、どこからがホスト部なのかを**クラス**（P.174）という概念によって決めています。**サブネットワーク**は、従来クラスによって定められているネットワーク部の長さを、ホスト部の範囲まで拡張するしくみです。サブネットワークを利用することにより、ネットワーク部とホスト部の範囲を細かく指定し、IPアドレスを無駄なく利用することができるようになります。

IPアドレスにサブネットワークの概念を適用するには、**サブネットマスク**を使ってネットワーク部の長さを調整します。サブネットマスクとは、ネットワーク部がすべて1、ホスト部がすべて0である数値で、IPアドレスと同様に255.255.255.0のように表記します。サブネットマスクのネットワーク部の長さは、IPアドレスに**プレフィクス長**を併記することにより示します。

たとえば、ネットワーク部とホスト部がそれぞれ16ビットであると決められているクラスBのIPアドレスがあるとしましょう。このIPアドレスのネットワーク部を22ビットにしたい場合には、プレフィクス長を22ビットとして255.255.252.0というサブネットマスクを利用します。クラスBのネットワーク部は16ビットであることから、これにより6ビット拡張したことになります（**図Ⅳ-5-4**）。

▼図Ⅳ-5-4　サブネットマスクとプレフィクス長の概念



この例の場合、IPアドレスのうち22ビットはネットワーク部になるため、ホスト部として利用できるのは10ビットです。したがって、IPアドレスを割り当てられるホストの数は2^{10} = 1,024となります。しかし、ホスト部がすべて0のアドレスとすべて1のアドレスは特定の用途に使われるため、割り当て可能なアドレスは1,024 − 2 = 1,022個になります。

NOTE

ホスト部がすべて0のアドレスは、ネットワークそのもののアドレスを示すネットワークアドレスとして利用されます。一方、すべて1のアドレスはブロードキャストアドレスです。ブロードキャストアドレスは、同一ネットワーク内のすべての端末にデータを送信するときに利用されます。

TCP/IPで使われる代表的なプロトコル

TCP/IPネットワークでは、メールの送信やファイルの転送といったサービスは、アプリケーション層のプロトコルとして定義されています。ここでは、代表的なプロトコルについて説明します。

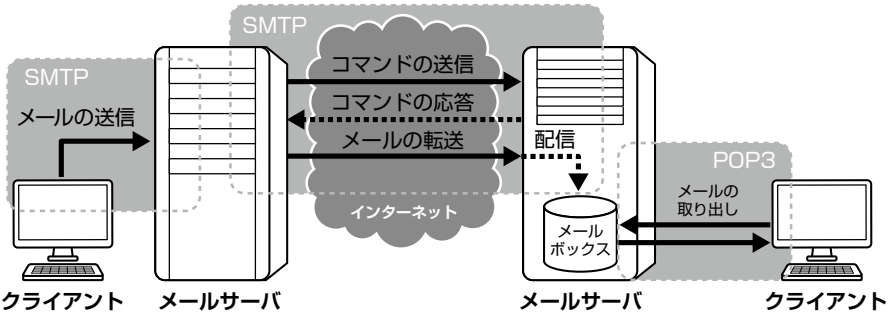
◎電子メールのプロトコル

SMTP（Simple Mail Transfer Protocol）は、電子メールシステムにおいてメールサーバ間での電子メールの送受信やクライアントからの電子メールの送信を行う

ためのプロトコルです。

一方、クライアントがメールサーバ上のメールボックスからメールを取り出して受信する際には、**POP3**（Post Office Protocol 3）や**IMAP4**（Internet Message Access Protocol 4）というプロトコルを利用します（**図Ⅳ-5-5**）。

▼**図Ⅳ-5-5　SMTPとPOP3**



電子メールではテキスト以外にも、静止画像、動画像、音声といったさまざまなデータをやりとりします。電子メールでさまざまな形式の情報を統一して扱うために、**MIME**（Multipurpose Internet Mail Extension）というプロトコルを利用します。

◎FTP

FTP（File Transfer Protocol）は、ファイルをコンピュータ間で送受信するときに使用するプロトコルです。

◎SNMP

SNMP（Simple Network Management Protocol）は、IPネットワーク上でネットワーク機器の監視と制御を行うためのプロトコルです。SNMPでは、ネットワーク機器の管理者側を**マネージャ**、被管理者側を**エージェント**といいます。マネージャは、**表Ⅳ-5-1**の5つのメッセージを使用してエージェントと情報をやりとりします。

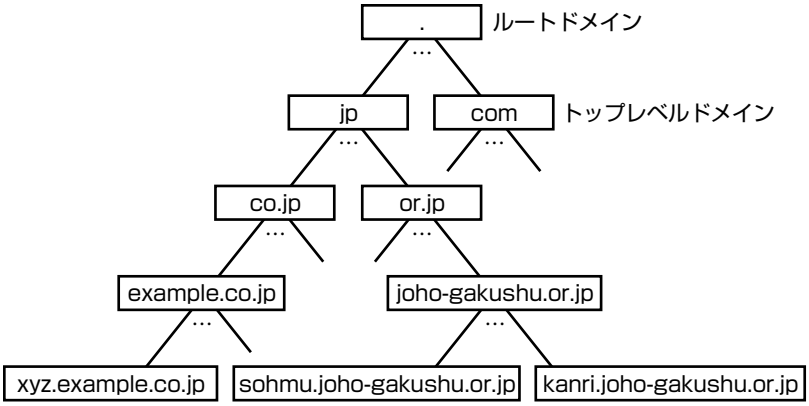
▼表Ⅳ-5-1　SNMPで使用されるメッセージ

メッセージ	送信の方向	内容
GetRequest	マネージャ　→　エージェント	情報要求
GetNextRequest	マネージャ　→　エージェント	次の情報要求
GetResponse	エージェント　→　マネージャ	GetRequestに対する応答
SetRequest	マネージャ　→　エージェント	情報の設定
Trap	エージェント　→　マネージャ	異常や緊急の信号

◎DNS

DNS（Domain Name System）とは、インターネット上にある機器のホスト名とIPアドレスを相互に対応づけるためのシステムです。ドメインは、次のようにツリー構造で表されます（**図Ⅳ-5-6**）。DNSサーバはホスト名とIPアドレスを対応づける情報を持ち、ホスト名からIPアドレスを、またはIPアドレスからホスト名を割り出します。該当する情報がなければ、他のDNSサーバに問い合わせることが可能です。

▼図Ⅳ-5-6　ホスト名の構造



◎DHCP

DHCP（Dynamic Host Configuration Protocol）は、サーバがインターネットに接続するクライアントにIPアドレスなどを動的に割り当てるためのプロトコルです。