01 情報セキュリティとは

私たちの世界は高度な情報社会へと成熟していますが、その結果として、情報セキュリティの重要性はますます高まっています。ここでは主に「情報セキュリティ」とは何かについて解説します。

情報セキュリティの定義

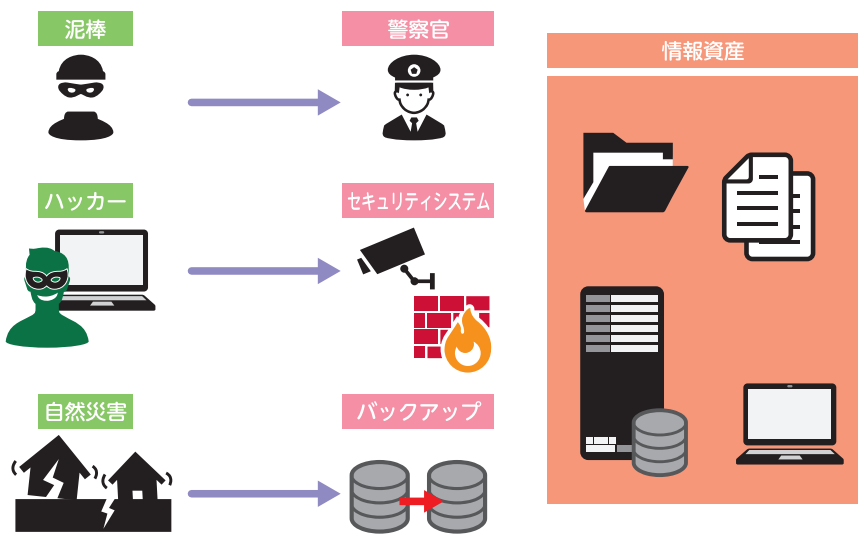
情報セキュリティの究極の意味は、「情報資産を守ること」です。それでは、「情報資産」とは何でしょうか。それは組織にとって何らかの資産価値を生むものであり、具体的な内容は組織によって異なります。ある組織では顧客情報であったり、ある組織では特許であったりとさまざまです（P.016、018参照）。

そして、これらの情報資産はさまざまなかたちで保管されています。すぐに思い浮かぶのは紙の文書ですが、そうした紙の文書も近年ではデータに置き替わっています（もちろん紙の文書がなくなったわけではありません）。データはパソコンのハードディスクやSSDに保存されるだけではなく、会社に設置されたサーバーや外部のクラウドにも保存されます。持ち歩き可能なスマートフォンやUSBメモリなどに保存されるデータも大切な情報資産といえます。

つまり多くの場合、情報資産はさまざまな場所に主にデータとして分散して保存されています。保存されていると同時に、その情報資産はメールで送信されたり、サーバーからダウンロードされたりして、移動しています。組織にとって重要な情報資産は、まずはこのように扱われていることを理解してください。

次にこうした情報資産をどのように守っていくか、ということになります。強盗などの物理的脅威から守ることも必要ですし、サイバー攻撃などの論理的脅威から守ることも欠かせません。また、事業継続のために、自然災害などの脅威も考慮する必要があります。前述したとおり、情報資産は分散して保存され、通信によって移動もしているということを考え合わせると、情報セキュリティ＝情報資産を守ることは、それほど容易なことではありません。

■情報資産を脅かす脅威はさまざまなかたちで守られる



本書の位置付け

本書は、「情報セキュリティ」を全般的に学びたい方、または、「情報セキュリティマネジメント試験」に合格したい方が、**幅広く「情報セキュリティ」を学べるように構成**しています。

具体的には、以下の方々を読者対象にしています。

- 情報セキュリティの分野で仕事をしている若手エンジニア（2〜3年以内）
- 情報セキュリティの分野で営業、広告、広報などの業務を行っている方
- 情報セキュリティの分野に就職／転職を考えている方（学生を含む）
- 普段行っている業務以外にも情報セキュリティに興味がある若手エンジニア

まとめ

- **情報資産とは資産価値を生むものであり、組織によって異なる**
- **情報セキュリティとは、あらゆる脅威から情報資産を守ること**

02 情報セキュリティを構成する７つの要素

ここではまず、情報セキュリティの3大要素である「機密性」「完全性」「可用性」について解説します。また、この3つの要素に付け加えて理解すべき「真正性」「責任追跡性」「否認防止」「信頼性」の4つの要素についても確認しましょう。

機密性

機密性（Confidentiality）とは、許可されたユーザーだけが情報資産にアクセスできるようにすることです。許可されていないユーザーは、端末やデータにアクセスすることができないようにしたり、データを読むことだけを許可して変更はできないようにしたりすることを指します。そのため、情報漏洩防止、アクセス権の設定、暗号の利用などの対策が必要になります。

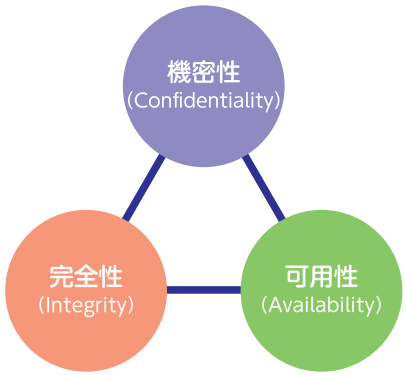
完全性

完全性（Integrity）とは、情報が正確であり、完全である状態を保持し、保護することです。つまり、情報が改ざんされたり、破損されたりしてしないことを指します。同時に、その情報が古いものであった場合も完全性が損なわれていることになるので、最新の情報である必要があります。そのため、改ざん防止、検出などの対策が必要になります。

可用性

可用性（Availability）とは、許可されたユーザーが必要なときにいつでも情報資産にアクセスできるようにすることです。サーバーが停止したり、パソコンが壊れたりした場合、この可用性が損なわれることになります。そのため、電源対策、システムの二重化、バックアップ、災害復旧計画などの対策が必要になります。

■情報セキュリティを成立させる３大要素



付加的要素である、「真正性」「責任追跡性」「否認防止」「信頼性」についても理解しておきましょう。以下はそのポイントになります。

■３大要素に加えて重要な４つの要素

要素名	定義	対策
真正性 (Authenticity)	ユーザーや情報そのものが本物であることを明確にすること	デジタル署名、多要素認証、生体認証などを導入する
責任追跡性 (Accountability)	ある行為が誰によって行われたかを明確にすること	アクセスログ、操作ログなどのログを取得する
否認防止 (Non-Repudiation)	情報の作成者が作成した事実をあとから否認できないようにすること	取得したアクセスログ、操作ログなどが改ざんされないようにする
信頼性 (Reliability)	情報システムの処理が、欠陥や不具合なく確実に行われること	システム不具合などが発生しないよう、余裕ある設計と検証を実施する

まとめ

- **情報セキュリティ対策とは、3大要素である「機密性」「完全性」「可用性」に加え、4要素（「真正性」「責任追跡性」「否認防止」「信頼性」）に準拠すること**

09 サイバー攻撃の攻撃者

サイバー攻撃やサイバーセキュリティ上の不正を行う攻撃者は、どのような人たちなのでしょうか。ここでは攻撃者について分類し、その特徴を解説します。攻撃を防御するためにも、攻撃者と攻撃内容について知っておくことは重要です。

スクリプト・キディ

スクリプト・キディとは、インターネット上に公開されている、他人の作ったサイバー攻撃用の「スクリプト」を使う「お子様（キディ）」という意味です。サイバーセキュリティやサイバー攻撃に興味を持ち、ツールを使えば比較的容易に実現できる攻撃を行う初心者を指します。

彼らの行う攻撃に対しては、すでに対策されているものがほとんどで、適切なセキュリティパッチを適用するなどすれば、防ぐことができます。ただし、DDoS攻撃（P.110参照）やエクスプロイト攻撃（P.116参照）など対策が難しく、初学者でも比較的容易に実現できる攻撃も存在します。

■ スクリプト・キディの特徴

・興味本位で行動
・セキュリティ・システムの初学者
・攻撃に詳しくない
・攻撃の痕跡を残すことが多い

愉快犯

かつてのサイバー攻撃者のほとんどは**愉快犯**とされていました。スキルを誇示したい、ハッカーとして有名になりたいといった自己顕示欲や他者を攻撃し反応を見て楽しむといった動機で攻撃を行う、いわゆる「困った人」たちです。

Webサイトに対してセキュリティ上の脆弱性を発見し、親切心で忠告しているつもりで攻撃しているつもりはなかった、など自分本位な理由で正当化しやすいのも特徴です。10〜20代の若い人に多く、サイバー攻撃自体が犯罪であるという意識はあるものの、軽率な行動であることが多いようです。

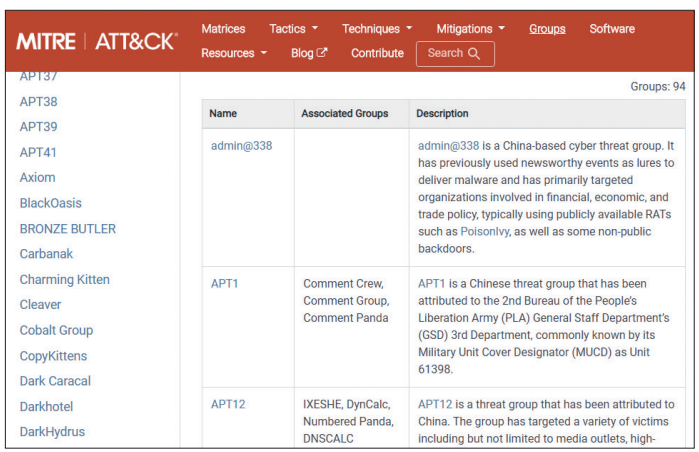
■ 愉快犯の特徴

・自己顕示欲、他者優位性が強い
・セキュリティ知識が高い
・システム上のモラルはあるが欲求が勝る

故意犯

内部犯、詐欺犯、海外ではサイバーテロリストや、国家単位で行うサイバー攻撃者（国家公務員という立場になるのでしょうか）などが**故意犯**に該当します。米国マイター社が運営するMITRE ATT&CK（マイター・アタック）には、実在するサイバーセキュリティ集団に関するレポートが多数公開されています。集団の特徴・バックグラウンドや、実際に行った攻撃の手口に関する詳細が閲覧できます。

■ セキュリティ脅威となる集団のページ
（マイター・アタック：https://attack.mitre.org/groups/）



故意犯に対して、過失や注意義務を怠った結果、攻撃者に加担してしまう場合は過失犯となります。

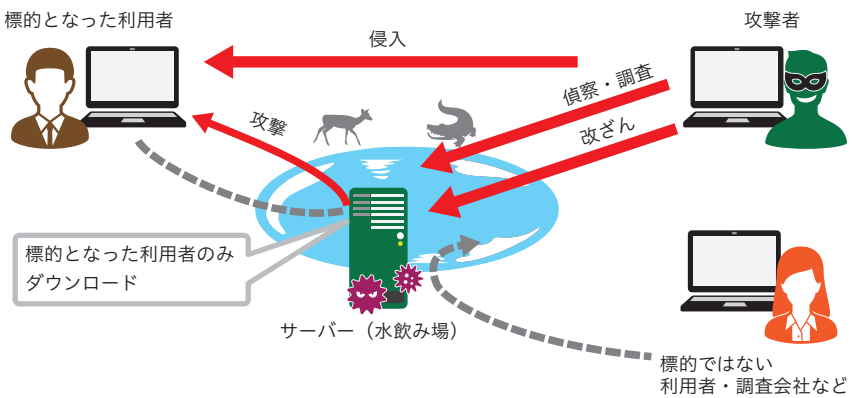
14 標的型攻撃

セキュリティエンジニアと、攻撃者であるハッカーやクラッカーとの闘いは「標的型攻撃」が代表的なもので、攻撃者の手口は年々巧妙化・多様化しています。ここでは代表的な標的型攻撃について解説します。

水飲み場攻撃

水飲み場攻撃（watering hole attack）は、標的とする特定の人や組織に属する人が頻繁に閲覧するWebサイトやSNSサイトを改ざんして、不正プログラムなどをダウンロードさせる攻撃です。改ざんされたWebサイトをサバンナの水飲み場になぞらえて、攻撃者が水飲み場にやって来た獲物（標的となった人）を待ち伏せしている様子から名付けられました。

■水飲み場攻撃のしくみ



ポータルサイトや大手SNSサイトではない中規模サイト、改ざんやセキュリティ対策が充分でないサイト、標的がよく利用するサイトなどを改ざんし、標的となる利用者のみに攻撃が成立するよう細工される特徴を持つため、発覚までに時間がかかります。攻撃対象を絞って特定の人や組織をターゲットにし、特定の条件でしか攻撃が発生しないことで、セキュリティ対策企業の調査や攻撃の発覚を遅らせる効果があります。攻撃には未知のマルウェアや発見されていない脆弱性を利用する場合もあります。

水飲み場攻撃は主に3つの段階から構成され、サイバー・キルチェーンやマイター・アタックに当てはめてモデル化することが出来ます。

■水飲み場攻撃の3つの段階

段階	概要
偵察・調査	標的となる人や組織の取引先、情報収集のために訪問するサイトやSNSなどを調べ、脆弱性を調べて「水飲み場」となるサイトを絞り込む。標的の組織が利用するサーバー（資産管理サーバーやドキュメントサーバー）が直接狙われることもある
改ざん	脆弱性を利用して絞り込んだサイトを「水飲み場」へ変える。標的となる組織・人に対して直接マルウェアを送り込むリンクを書き込んだり、特定のIPアドレス範囲からのアクセスのみマルウェアをダウンロード可能にさせたりする
攻撃・侵入	改ざんした「水飲み場」サイトで標的となる利用者を待ち受け、マルウェアに感染させたり、Webブラウザへの攻撃で個人情報を抜き取り、遠隔操作やデータの盗聴などを行い、機密情報の摂取や諜報活動を行う

標的となった利用者向けの対策

最低限の対策としては、OSやアプリケーションのセキュリティ・パッチ、アンチウイルスソフトの定義を常に最新に保つことが必要になります。加えて、侵入後の被害拡大を防ぐ取り組みも欠かせません。パソコンには機密情報を保管せずWebブラウザにもパスワードを保管しないなどの対策を行います。また、定期的にネットワーク機器のログからアクセス先の確認などを行い、業務で必要のないサイトや普段とは異なるURL、アクセス先IPアドレスなどを遮断するなどの対策も有効です。

「水飲み場」サイトにならないための対策

攻撃者は対策されていない脆弱性やセキュリティ・ホールを放置しているサイトやサーバーを探して攻撃を行います。そのため、対策としては最新のセキュリティパッチを適用するほか、不要なサービスの停止、管理者権限を利用した

21 暗号化技術の基礎

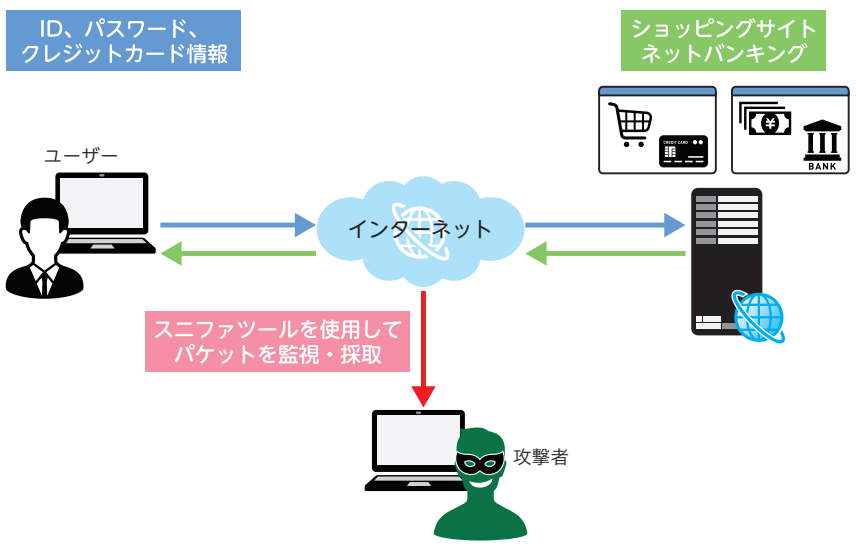
ネットワーク上を流れる情報は常に狙われています。攻撃者は、盗聴、またはスニッフィングと呼ばれる行為により、データを採取・解析して情報を盗み取ります。そのため、大切なデータの機密性や完全性を保つために暗号化技術が使われます。

盗聴

攻撃者は、**スニファツール**（盗聴ツール）を使用して特定のネットワークを通過するすべての**データパケットを監視し、採取**します。このときにデータが暗号化されておらず、平文でネットワーク上を流れている場合、パスワードやアカウント情報を含むあらゆる情報を攻撃者に盗み取られてしまいます。

なお、スニファとは匂いを嗅ぐ英語の「sniff」から来ており、ネットワークを流れるトラフィックを嗅ぎ取るという意味合いを持っています。このように説明するとスニファが悪者のようなイメージを抱いてしまいますが、スニファはLANアナライザの別名として呼ばれることもあり、それ自体が悪意を持つというものではありません。

■盗聴のしくみ



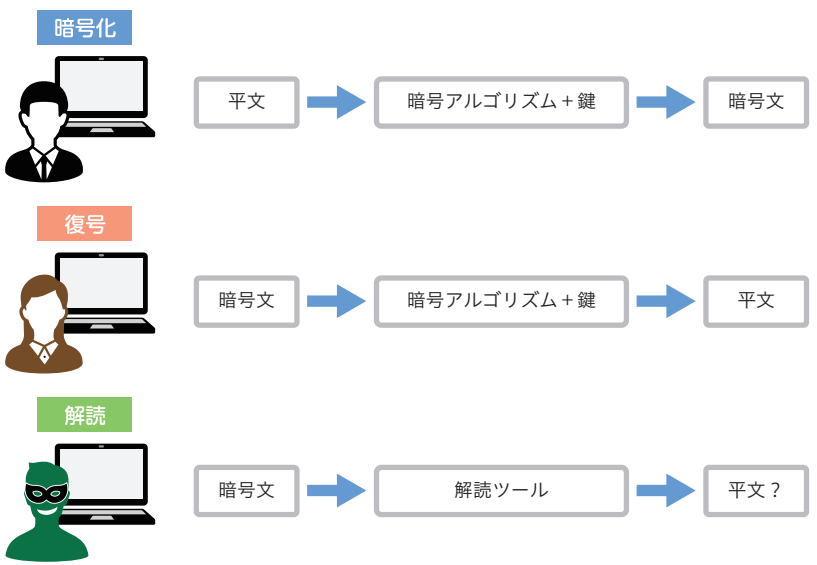
暗号化と複合、解読

暗号化技術は、ネットワークを流れる情報、Eメールメッセージ、チャットセッション、Webトランザクション、個人のデータ、企業のデータ、電子商取引アプリケーションなどの機密データの保護のために用いられます。

暗号化とは、暗号化アルゴリズム（暗号化の手法）と暗号化鍵を使用して、平文を読めない状態にデータ変換することをいいます。**復号**とは、暗号化して読めない状態にしたデータを、暗号化する際に使用した暗号アルゴリズムと復号鍵を使って平文へ戻すことをいいます。**解読**は暗号化の際の情報や復号鍵がない状態で、暗号化されたデータを平文へ戻すことをいいます。

暗号化技術については、現代のITは暗号化技術が支えているといっても過言ではないほど、切っても切れない関係で成り立っています。注目キーワードでいえば、たとえばブロックチェーンなども暗号化技術抜きには語れません。

■暗号化・復号・解読のしくみ



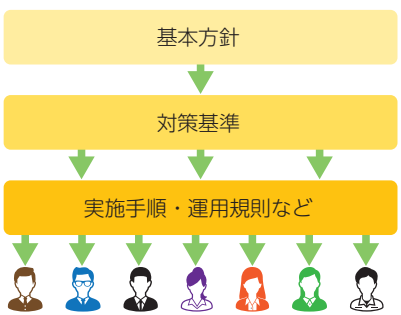
30 情報資産と無形資産

ここでは情報資産と無形資産に関連する用語について解説します。情報資産は読んで字のごとく情報やデータを指し、無形資産は目には見えない特許やブランドなどを指します。

情報セキュリティポリシー

情報資産／無形資産を考察するうえで欠くことのできない用語が**情報セキュリティポリシー**です。この言葉は、企業や組織において実施する情報セキュリティ対策の方針や行動指針を意味します。内容は企業の規模によって異なりますが、情報セキュリティポリシーがなければ資産を守る具体的なセキュリティ対策も立てられないため、企業にとって重要な概念となります。 情報セキュリティポリシーは、以下の図のように「**基本方針**」「**対策基準**」「**実施手順**」の3つの階層で構成されることが一般的です。

■情報セキュリティポリシーの基本方針（総務省指針）



組織を構成する要素

組織を構成する要素とは、端的にいえば、「**人**」「**物**」「**金**」そして「**情報**」です。「人」だけでは何もできないし、「人」と「物」が揃っても「金」がないと、人件費や固定費を払えません。そして、この情報化社会の中では、「情報」は必須です。この「組織を構成する要素」で資産を守っていくことになります。

■組織を構成する要素

知的財産

知的財産とは、特許やブランド、ノウハウなどの「**価値のある情報**」のことを指します。この知的財産は知的財産基本法において定義され、知的財産を有する者は一定期間保護されることが定められています。

■知的財産の種類

まとめ

- **知的財産には、「著作物」「発明」「営業秘密」なども含まれる**

40 内部不正防止ガイドライン

人間は必ずミスを犯したり、意図せぬ過ちを犯したりするものです。ITセキュリティ上に起こりうる内部不正を防止するには、社内教育はもとより、管理のしくみをガイドラインや法令、ツールなどで作っておくことが重要です。

情報セキュリティ啓発

情報セキュリティへの意識には個人差があります。そのため、情報セキュリティ向上の啓発を行うことで意識が高まり、今まで気付いていなかったセキュリティの弱点に自然と意識するようになります。また、**社内教育を実施**して、情報の無断持ち出しが不正行為であること、ルール違反すると社内規定で罰せられることを認識させることも必要です。

パスワード管理

現在、多くのシステムの認証機能には、パスワード認証が利用されています。しかし、パスワードは完全なセキュリティ対策ではありません。推測されやすいパスワード使用していると、パスワード総当たり攻撃によってパスワード認証を突破されたりします。また、**パスワードの使い回し**をしていると、別のシステムで漏洩したパスワードを悪用されて、システムに侵入されたりします。パソコンを共有している場合は、パスワードを付箋紙などに記載し、ディスプレイなどに貼っているケースも見受けられます。

そこでパスワードの管理には、**パスワード マネージメントソフトウェア**の利用をお勧めします。ただし、ソフトウェアなので、定期的な更新が必要です。ちなみに近年では、クラウドが浸透することで環境基盤も複雑化する傾向もあり、こうしたパスワードのマネジメントには一元管理できるものが求められているようです。

利用者アクセスの管理

利用者アカウント作成のプロセス、とくに必要最小限の権限を付与しているかに留意する必要があります。また、退職などによる利用者アカウントの削除、または無効化も徹底する必要があります。

見落としがちになるのが「共有アカウント」と「開発用アカウント」です。共有アカウントの場合は、不特定の人がパスワードを知っており、パスワード変更も行われない場合が多いです。開発用アカウントはシステム開発や導入のため、一時的に作成して役割を終えれば削除するはずなのですが、今後起こるかもしれないトラブルのために、開発用アカウントを削除せずにそのまま残している場合があります。加えて、「共有アカウント」や「開発用アカウント」は不特定多数の人が利用するため、覚えやすく推測しやすいパスワードが使われる傾向にあります。

そこで利用者アクセスの管理には、定期的なアカウントの**棚卸し**が必要になります。なお、一般にいわれるところの棚卸しには、IT資産管理（ITAM：IT Asset Management）のソフトウェア、システムが利用されます。アカウントの管理だけでなく、ライセンスや使用マシンの管理など、その機能は多岐にわたります。誰がどのような条件でどのようなマシンを使っているかなど、セキュリティ管理と直結する部分もあるので、組織にとって棚卸しの実行は大切なミッションとなっています。

ログ管理

ハッキングされたとか、マルウェアに感染したとかなどのインシデントが発生した場合、調査にログが必要です。基本的にログは古いレコードから上書きされてしまう傾向にあります。そのため、**定期的にログを保存（エクスポートなど）**する必要があります。しかもログは法令やガイドラインにより、保存期間が異なります。ログを集中管理したい場合は、専用のSyslog（System Logging Protocol）サーバーや、SIEM（Security Information and Event Management：セキュリティ情報イベント管理）ツールなどの導入をお勧めします。

56 セキュア・プロトコル

通信を行ううえでセキュアであることは、不正アクセスやデータの盗聴を防ぎ通信の内容を保護する、必要不可欠な要件です。ここではネットワーク通信で利用する代表的なセキュア・プロトコルについて解説します。

OSI基本参照モデル

コンピューター間の通信は、通信の約束事（プロトコル）を決め、その仕様に沿った機器を有線・無線で繋いで設定することで異なるメーカー同士の機器間でも問題なく通信が行えます。ネットワークを構成しているさまざまな通信プロトコルを役割別に7階層に分類し、わかりやすく整理したモデルのことを**OSI基本参照モデル**といいます。

通信プロトコルはOSI基本参照モデルで分類された7階層に当てはめて考えることができるため、エンジニア同士でネットワーク通信の話をする場合やネットワーク・プロトコルの機能や役割を理解するのに役立ちます。

■OSI基本参照モデルの概要

階層名（階層）	代表的なハードウェア	代表的なプロトコル
アプリケーション層（レイヤ7）	プロキシサーバー、WAF、IDS	HTTP、SMTP、SMB、Telnet
プレゼンテーション層（レイヤ6）	—	FTP
セッション層（レイヤ5）	—	TLS
トランスポート層（レイヤ4）	ファイアーウォール	TCP、UDP
ネットワーク層（レイヤ3）	L3スイッチルーター	IP、ARP、ICMP
データリンク層（レイヤ2）	L2スイッチ、スイッチングHUB	PPP、Ethernet、トークンリング
物理層（レイヤ1）	リピータHUB	LANケーブル（電気信号）、光ファイバー（光信号）

- **レイヤ1：物理層**
  ハードウェアに依存した物理的な特性で分類されます。ケーブルの接続部分やケーブルを流れる電流・電圧、光信号などが該当します。
- **レイヤ2：データリンク層**
  イーサネットやトークンリングなど、隣同士で接続されたノード間のデータ送受信や送信単位であるフレームパケットに関する仕様が該当します。
- **レイヤ3：ネットワーク層**
  隣接したノードを超えて、ネットワーク同士のデータ送受信や通信先や通信元のアドレスを設定し、通信経路の決定などの役割が該当します。
- **レイヤ4：トランスポート層**
  パケット通信のエラー制御、再送処理機能で通信データの品質を確保し、信頼性のあるデータ転送を可能にする役割に分類されます。
- **レイヤ5：セッション層**
  通信経路の決定、コネクションの管理や切断などの役割が該当します。Webサーバーを例とすると、テキストとは別に画像1つ1つに対してセッションを確立し画像を表示させる機能などが該当します。
- **レイヤ6：プレゼンテーション層**
  データの表現形式（文字コードや圧縮方式、利用する暗号化方式など）が該当します。Webサーバーを例とすると、異なる文字コードであっても文字化けすることなく正しく表示させることができます。
- **レイヤ7：アプリケーション層**
  クライアント・サーバーで利用するアプリケーションの独自データのやり取りを提供します。FTPの場合、FTPサーバーとクライアント上のファイル転送プログラムの通信が該当します。

OSI基本参照モデルではさまざまなプロトコルが7層に分かれて登場しますが、ネットワーク学習はトランスポート層＆ネットワーク層のプロトコルであるTCP／IPに重点を置き、1〜4層のトランスポート層以下を重点的に学習することが重要となります。

5〜7層はレイヤ別に特化したプログラムがあることはまれで、通信機能を持つアプリケーション・プログラムが5〜7層に分類できる特徴を持つと考え

索引　Index

た行

な行

は行

ま～や行

ら行

わ行