DIGITAL SERIES

未来へつなぐ
デジタルシリーズ

ネットワークセキュリティ

Connection to the future with Digital series

高橋　修　監修

関　良明
河辺義信
西垣正勝
岡崎直宣
岡崎美蘭
本郷節之
岡田安功　著

36

共立出版

第1章
ネットワークセキュリティ序説

□ 学習のポイント

ネットワークセキュリティの序説として，本章では社会基盤となったインターネットの発展を振り返り，そこに潜む具体的な脅威を紹介する．ここでは，技術の進化に伴って深刻化する脅威に対抗するネットワークセキュリティの必要性と重要性を学ぶ．また，本書が網羅する主な技術とトピックスを紹介し，次章以降への準備とする．

- 社会基盤となったインターネットの生い立ちを知る．
- ネットワークセキュリティの必要性と基本的な考え方を理解する．
- インターネットに潜む脅威を学び，ネットワークセキュリティの重要性を認識する．

本書では，インターネット，コンピュータシステム，情報数学などに関する基礎的な知識を修得していることを前提としている．必要に応じて文献を参照されたい．

□ キーワード

ネットワークセキュリティ，インターネット，盗聴，暗号解読，パスワードクラック，マルウェア，コンピュータウイルス，ワーム，トロイの木馬，エクスプロイト，スパイウェア，ボット，ポートスキャン， DoS 攻撃， P2P の悪用，クロスサイトスクリプティング，ドライブバイダウンロード，ファーミング，スパムメール，フィッシング，ソーシャルエンジニアリング，サイバー攻撃

1.1 インターネットの発展と潜在する脅威

インターネットは，世界中に張り巡らされた巨大なコンピュータネットワークである．World Wide Web（以後 Web と略す）や電子メールなどインターネットを使った様々なアプリケーションが開発され，情報メディアとしても多様な発展を遂げている．近年では，インターネットの向こう側にあるコンピュータ資源を仮想的に利活用するクラウドコンピューティングが，ビジネスや生活に浸透してきている．身近な情報機器としては，インターネットへ容易に接続可能なスマートフォンやタブレット端末などが世界的に急速に普及している．これらのネットワーク環境を背景として，オンラインショッピングや SNS（Social Networking Service：ソーシャルネットワーキングサービス）など社会生活を豊かにするネットワークサービスの進化が

加速されている．

一方で，企業や組織の機密情報漏えいや金銭詐欺，サービスの妨害など，コンピュータネットワークに対する脅威やコンピュータを悪用する重大事件が増加してきた．このような状況の中で，コンピュータを含むコンピュータネットワークを様々な脅威から守ることがますます重要になってきている．コンピュータネットワークを基盤とする社会では，目に見えない相手やシステムと情報のやりとりをすることが多く，日常生活における対面の人間相手のやりとりとはまったく異なり，安心・安全な環境の実現が特に重要な要件となる．

本節では，1.1.1 項でインターネットの発展を振り返り，1.1.2 項でインターネットに潜む脅威を紹介し，1.1.3 項で脅威に対するネットワークセキュリティ技術の考え方を概観する．また，1.1.4 項で本書が扱う主な技術とトピックスを紹介する．

1.1.1 インターネットの発展

19 世紀に電気通信技術が登場し，20 世紀半ばからのコンピュータサイエンスの進化が情報処理に革命をもたらした．コンピュータが高速に処理するデジタル情報を，ネットワークが高速，正確，大量に伝達し共有することを可能にした．以下にインターネットの発展の歴史を振り返る．

(1) 中央集約型から分散型ネットワークへ

インターネットの起源は，アーパネット (ARPANET) というコンピュータネットワークである．ARPANET は，米国防総省の ARPA（Advanced Research Project Agency：高等研究計画局）の支援を受けて 1969 年に構築が始まった．

それまでのコンピュータネットワークは，中央の巨大なコンピュータ（ホストコンピュータ）にすべての端末を接続する中央集約型の形態をとっていた．この方式には，中央のホストコンピュータが故障するとすべての通信が途絶えてしまうという欠点があった．このため，ホストコンピュータに依存せず，コンピュータを相互に接続する分散型ネットワークが考案された．ARPANET には，この分散型ネットワークの考え方が取り入れられた．

(2) インターネットに至るまでの歴史

1983 年以降，ARPANET は米国各地に置かれたコンピュータが相互に通信できる環境を提供する研究目的のネットワークとなった．ARPANET の通信に用いるプロトコルとして，コンピュータやネットワーク機器の特性などに依存せず，高い信頼性を維持できる TCP/IP (Transmission Control Protocol / Internet Protocol) が採用された．

NSF（National Science Foundation：米国科学財団）も ARPANET のシステムを参考にして，スーパーコンピュータと各研究機関を結ぶネットワーク構想を打ち立てていた．この構想に基づき，複数の研究機関が接続され，全米各地から利用可能なコンピュータネットワークとして，1986 年，NSFNET の運用が始まった．やがて NSFNET と ARPANET は相互に接続されるようになった．

1990 年に ARPANET は運用を停止し，NSFNET が ARPANET の基幹ネットワークを引

き継ぐことになった．この時点では NSFNET は学術目的に使用を限定されていた．翌 1991 年には CIX Association（Commercial Internet eXchange Association：商用インターネット相互接続協会）が設立され，商用ネットワークの運用が開始された．これにより，インターネットは利用目的を問わない全米規模のコンピュータネットワークとなった．

(3) 日本でのインターネットの幕開け

日本では大学を中心に，1984 年に JUNET（Japan University NETwork または Japan UNIX NETwork）が発足した．これが海外との接続を実現して WIDE(Widely Integrated Distributed Environment) プロジェクトへと発展した．また，同時期に NTT（日本電信電話株式会社）の研究所が所有するコンピュータネットワークが NSFNET へ接続した．1992 年には初の商用プロバイダ IIJ(Internet Initiative Japan) が設立され，日本における現在のインターネットの基礎が築かれた．

1995 年にマイクロソフトから PC（Personal Computer：パーソナルコンピュータ）向けの OS（Operating System：オペレーティングシステム）Windows95 が発売された．Windows95 は TCP/IP を標準サポートするほか，Web ブラウザやメールクライアントを搭載しており，それまでに比べて簡単にインターネット接続できるようになった．これにより，インターネットを利用する個人ユーザが急増した．

1999 年に NTT ドコモの i モード，DDI の EZweb，J-Phone の J-スカイのサービスの提供が開始され，携帯電話からインターネットへのアクセスが可能となった．これにより，PC を持たないユーザでもインターネットが利用できるようになり，インターネットのユーザ数が大幅に増加した．

(4) インターネットの発展

商用プロバイダによってインターネットへの接続が個人に提供されて以降，PC の普及と ICT（Information and Communication Technology：情報通信技術）インフラの整備を経て，誰もがインターネットを利用できるようになった．利用形態も Web サイトの閲覧や電子メールの交換といった基本的なものから，音楽・動画配信，ネットショッピング，宿泊先やチケット予約，オンラインバンキングなど，あらゆる分野に及んでいる．使用する機器も PC，携帯電話，スマートフォン，情報家電などと多様化している．特にスマートフォンの世界的な普及により，いつでも，どこでも，誰もが簡便にインターネットを利用できる環境が整ってきている．そこでは，様々な社会的コミュニティのコミュニケーションに利便性をもたらす SNS が提供されている．

社会生活は，ICT の発展のおかげで飛躍的に便利になった．いまやインターネットに代表されるコンピュータネットワーク環境は，通信やメディアとしての役割に留まらず，産業や日々の暮らしを支える重要な社会基盤である．

以上のように，インターネットは，使用目的が限定された性善説に基づく研究用の分散型ネットワークを起源としている．商用ネットワークに移行してからも新しい技術を常に取り入れ，

国際的にオープンな運営方針は継承されている．また，多種多様な管理運営主体によるアクセス網が相互に接続する巨大なネットワークの集合体でもある．このインターネットには，個人の PC やスマートフォンだけでなく，政府機関や重要インフラのネットワーク，センサネットワーク，モノをつなぐ IoT(Internet of Things) も接続されている．

1.1.2 インターネットに潜在する脅威

インターネットの起源は，悪意を持ったユーザの存在を想定しない，性善説に基づくものであった．そのため，善意のユーザにとっては便利な環境でも，悪意を持ってコンピュータネットワークの機能やサービスを利用すれば，盗聴，なりすまし，改ざん（図 1.1），および不正アクセス（図 1.2）などの不正行為を容易に行える環境を提供している．

インターネットの用途拡大と，利便性向上と引き換えに，インターネットに潜在する脅威に社会が直面するリスクも確実に拡大し，複雑化してきている．

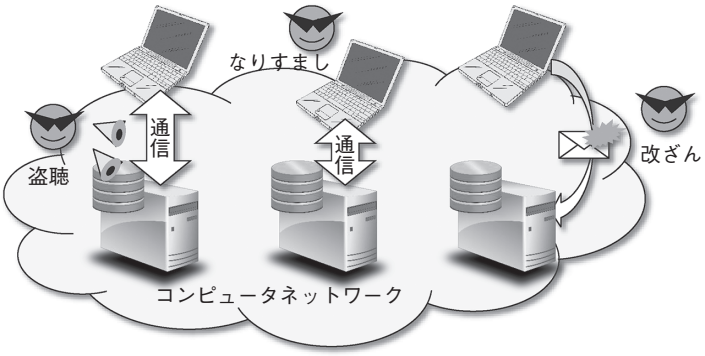

図 1.1 盗聴・なりすまし・改ざん．

(1) 盗聴

コンピュータネットワークを流れるデータを傍受したり，コンピュータ内部のデータを不正に収集したりして，情報を盗み取ることである．ユーザ名やパスワード，企業の機密情報などがターゲットとなりえる．

(2) なりすまし

他人のメールアドレス，パスワード，クレジット番号などを不正に使用し，当事者になりすましてコンピュータやネットワークサービスにログインしたり，メール送信やオンラインショッピングなどを行ったりすることである．

(3) 改ざん

コンピュータネットワークを流れるデータやコンピュータ内部のデータを不正に書き換えることである．たとえば，Web サイトの改ざん，不正侵入の痕跡を消すための改ざん，メール内

容の改ざんなどが挙げられる.

(4) 不正アクセス

近年，標的とするコンピュータやコンピュータネットワークに侵入してデータの盗取やシステムの機能不全を引き起こすサイバー攻撃が社会問題となっている．サイバー攻撃は，正当な権利を持たない第三者による不正アクセスである．不正アクセスには，不正な手段を用いてコンピュータやコンピュータネットワークの内部へ侵入する直接的攻撃と，コンピュータウイルスなどのマルウェアを使ってコンピュータを遠隔操作する間接的攻撃，インターネットを悪用してサービスを妨害する DoS(Denial of Service) 攻撃などが挙げられる（図 1.2）．DoS 攻撃については，1.2.4 項 (2) で説明する.

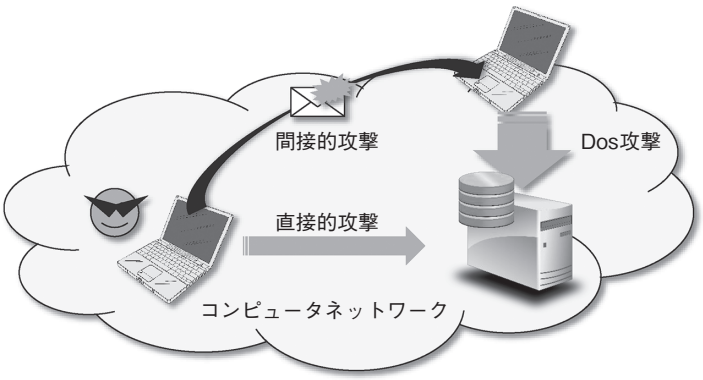

図 1.2 不正アクセス.

1.1.3 脅威に対抗する技術

不正行為から善意のユーザやサービス提供者，ネットワーク接続機器などを安全に守るためにネットワークセキュリティが必要となる.

(1) ネットワークセキュリティ

ネットワークセキュリティは，不正なユーザによるアクセスからコンピュータネットワークそのもの，およびコンピュータネットワークからアクセスできる資産を守るために，情報セキュリティとコンピュータネットワーク技術を融合した技術と捉えることができる．情報セキュリティとは，「正当な権利を持つ個人や組織が，情報や情報システムを意図通りに制御できること」である．ISMS（Information Security Management System：情報セキュリティマネジメントシステム）の国際標準 ISO/IEC27002 では，「情報の機密性 (Confidentiality)，完全性 (Integrity) および可用性 (Availability) を維持すること」と定義している．また，情報セキュリティでは，脅威から守るべき資産を情報資産と呼び，それらは，ハードウェア，ソフトウェア，ネットワーク，データ，ノウハウなど様々な形態をとる．情報セキュリティマネジメント

については，第 9 章で詳細に解説する．

ネットワークセキュリティは，情報セキュリティの技術的な側面に注目するものであり，コンピュータセキュリティやクラウドセキュリティも含む概念と言える（図 1.3）．コンピュータセキュリティは，コンピュータの脆弱性 (Vulnerability) を解消し，第三者による不正利用を阻止し，コンピュータの安全性を保持することである．ネットワークセキュリティで扱うコンピュータには，サーバや PC だけでなく，スマートフォンやタブレット端末，携帯電話なども含まれる．クラウドセキュリティでは，ハードウェアやネットワーク (Infrastructure)，OS などのプラットフォーム (Platform)，アプリケーションソフトウェア (Software) がサービス (XaaS: X as a Service) として提供されるため，IaaS，PaaS，SaaS などサービス提供者の事業継続性や，セキュリティ対策への依存が新たな課題となっている．

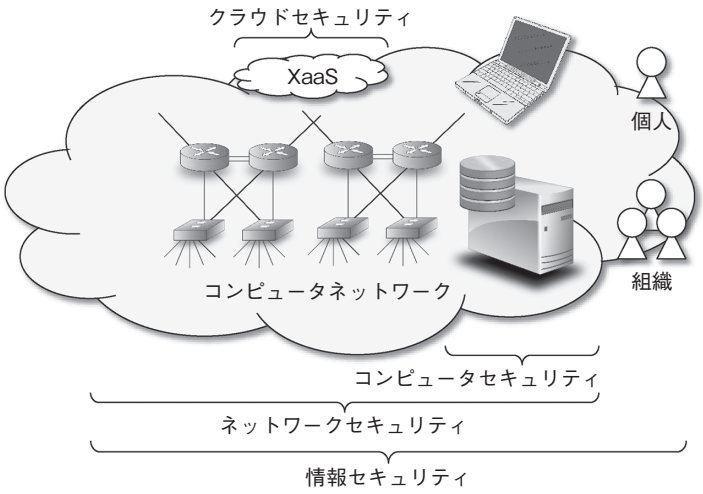

図 1.3 ネットワークセキュリティの位置付け．

(2) 脅威への対策

一般にセキュリティ対策の基本的な考え方は，脆弱性の解消，多層防御，最小権限である．

脆弱性は，コンピュータやコンピュータネットワークが抱える保安上の弱点である．コンピュータもコンピュータネットワークも新しい技術を常に取り入れ進化し続けている．そこには，当初想定していなかった攻撃に対する弱点が組み込まれてしまう可能性も高い．攻撃が予想された時点で，脆弱性を解消するためのアップデートを実施することが対策の基本である．

多層防御は，あらかじめ被害に遭うことを想定して，複数の対策を多層で行うことである．情報資産に対する攻撃は日々高度化しており，1 つの対策が破られただけで，コンピュータネットワークとしての安全性，特に可用性が保てなくなる事態は避けなければならない．したがって，対策を施す上では，複数の対策をもって，必要とするセキュリティを確保しようとする多層防御の考え方が望ましい．たとえば，ファイアウォールとユーザ認証を組み合わせてアクセ

ス制御を強化する，不正アクセスが成功してもデータを暗号化しておくことでデータ漏えいによる実質的な被害をなくすなど，複数の対策手段を組み合わせて，対策の相乗効果を上げることが肝要である．

最小権限は，許可されたユーザであることを認証するとともに，アクセスが許されるファイルやアプリケーション，コマンドを限定し，ユーザごとに必要最小限の権限を付与することである．これによって，被害の範囲を小さくすることができる．

1.1.4 本書で扱う主な技術とトピックス

ネットワークセキュリティは，コンピュータが接続されたネットワークの可用性を維持することを基本として，ネットワークで通信され，コンピュータで処理される情報の機密性，完全性，可用性（いわゆる，情報の CIA）を維持することが重要と考えられる（図 1.4）．

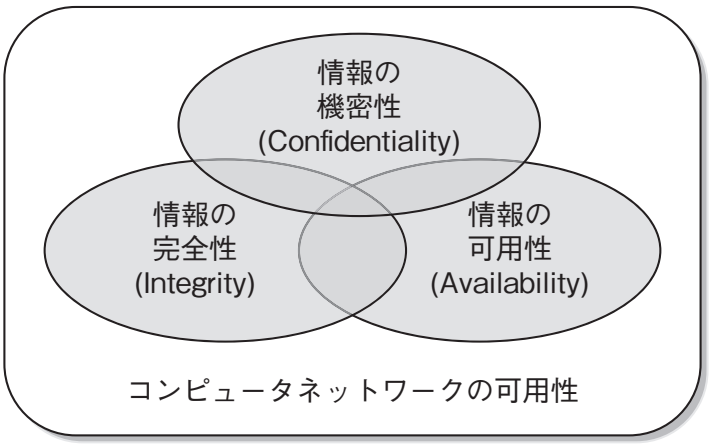

図 1.4 ネットワークセキュリティの CIA.

本書では，ネットワークセキュリティの社会的な重要性の高まりを考慮して，技術的な側面だけでなく，情報セキュリティの領域である組織と法制度にも深く言及している．構成としては，セキュリティ要素技術（第 2〜6 章）と応用セキュリティ（第 7〜11 章）に分けて，ネットワークセキュリティに関する技術とトピックスを網羅している．

(1) セキュリティ要素技術

第 2〜5 章は，情報の漏えいを防ぐ機密性と，情報の改ざんを防ぐ完全性を担う暗号技術を詳細に解説している．ここで暗号は，ある一定の法則（Algorithm：アルゴリズム）に基づいてデータを変換し，元のデータ（Plaintext：平文）を第三者に知られないようにする技術である．**第 2 章 古典的な暗号** では，暗号アルゴリズムと鍵，転置暗号，換字暗号を紹介し，基本的な考え方を解説する．**第 3 章 共通鍵暗号** では，その代表例として，DES および DES に対する解読法，トリプル DES，AES を解説する．また，暗号アルゴリズムの適用事例としてブロッ

ク暗号とストリーム暗号を説明する．**第 4 章 公開鍵暗号（1）-基本的な考え方** では，共通鍵の問題を解決するために発明された公開鍵暗号の代表例として RSA を解説する．また，その応用としてハイブリッド暗号を説明する．**第 5 章 公開鍵暗号（2）-デジタル署名と公開鍵の配送** では，公開鍵暗号における本人の秘密鍵を使用して，メッセージやファイルに付加する電子的なデータであるデジタル署名を解説する．デジタル署名は，確かに本人が承諾したことを認めるための署名・捺印を電子化したものである．また，公開鍵の配送における中間者攻撃と PKI（Public Key Infrastructure：公開鍵基盤）の仕組みを説明する．

第 6 章 ユーザ認証 は，スマートフォン，PC，Web サイトへのログインの際に実施する最も身近なセキュリティコントロールであるユーザ認証の仕組みを解説する．また，ユーザが悪意のある自動プログラムではなく，人間であることを認証する CAPTCHA 技術を説明する．

(2) 応用セキュリティ

第 7 章と第 8 章は，これまで学んできた暗号や認証などのセキュリティ要素技術を応用し，様々な脅威からネットワークを守るための仕組みについて解説している．**第 7 章 組織内ネットワークのセキュリティ** では，様々なネットワーク機器を用いて実現できるセキュリティ対策を説明する．また，外部の攻撃から組織内のネットワークを守るためのファイアウォールと，不正侵入を検知し防御する IDS/IPS の仕組みについて解説する．**第 8 章 インターネットのセキュリティ** では，Web や電子メール，リモートアクセス，プライベートネットワークなど，インターネットを安全に利用するための仕組みを解説する．また，安全性の高い通信プロトコルとして，SSL，S/MIME，SSH，VPN，IP-SEC の仕組みを説明する．

第 9 章 情報セキュリティマネジメント は，情報の CIA を担う ISMS の考え方を，基本方針，対策基準，実施手順，ガイドラインからなる情報セキュリティポリシーの策定などによって説明する．また，体制の構築から始まる一連の取り組みの概要を解説する．

第 10 章と第 11 章は，社会的な仕組みとして，プライバシーを保護し情報セキュリティを保護する制度のトピックスを解説している．**第 10 章 プライバシーの保護と情報セキュリティの確保** では，日本の情報セキュリティ政策に大きな影響を与えている OECD（Organisation for Economic Co-operation and Development：経済協力開発機構）の情報セキュリティに関するガイドラインを中心に解説する．情報セキュリティという概念は，情報技術の進歩に伴って変化するべきものである．そこで，ガイドラインの時系列に沿って，プライバシー権の説明，プライバシーの保護と個人情報の保護の関係，これらと情報セキュリティの保護の関係を説明する．**第 11 章 日本の情報セキュリティ法** では，行政法，刑事法，民事法の観点から情報セキュリティが侵害された場合の対応を解説する．

次節では，これらの技術とトピックスが重要であることの理解を助けるために，具体的な脅威を紹介する．

1.2 具体的な脅威

コンピュータネットワークを基盤とする社会においては，コンピュータネットワークが抱えているリスクをユーザやシステム管理者が正しく理解し，脅威を常に意識して行動することが求められる．ここでは，1.2.1 項でインターネットに悪意を持って外部から侵入する不正アクセスの特徴を概観する．1.2.2 項以降では，そこで行われる不正行為をデータ，コンピュータ，コンピュータネットワーク，利用者にそれぞれ着目した具体的な事例を紹介する．さらに，1.2.6 項でネットワークセキュリティの社会的な背景を概観する．

1.2.1 脅威の特徴

インターネットに悪意を持って外部から侵入する不正アクセスによって生じる脅威は，脅威を受ける対象によって以下のように分類できる（図 1.5）．

- データに対する脅威： 盗聴，暗号解読，パスワードクラック
- コンピュータに対する脅威： マルウェア，コンピュータウイルス，ワーム，トロイの木馬，エクスプロイト，スパイウェア，ボット
- コンピュータネットワークに対する脅威： ポートスキャン，DoS 攻撃，P2P の悪用，クロスサイトスクリプティング，ドライブバイダウンロード，ファーミング
- 利用者に対する脅威： スパムメール，フィッシング，ソーシャルエンジニアリング

なお，利用者に対する脅威として，一般ユーザに対する直接的被害の他に，サービス提供者が攻撃を受けて，一般ユーザが二次的被害を受ける事件も多発している．

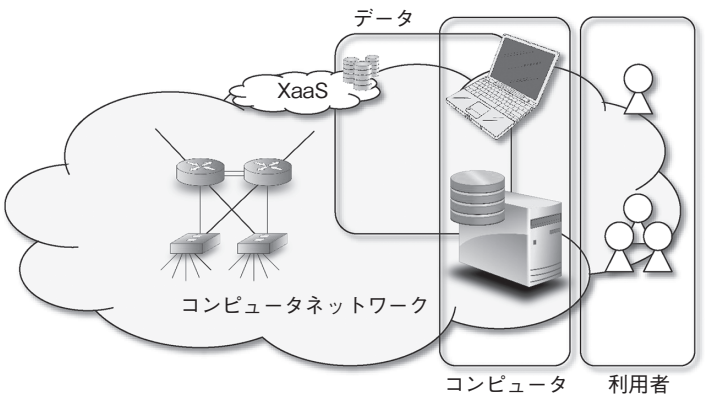

図 1.5 脅威を受ける対象による分類．

不正アクセスは，事前調査，権限取得，不正実行，後処理の 4 つの段階を経て行われる（図 1.6）．コンピュータやネットワークサービスの情報を入手するための事前調査や，操作や処理

を実行するための権限を不正に取得するための権限取得には，攻撃用ツールが使われる．攻撃用ツールとしては，コンピュータネットワークを盗聴するスニファツール，通信に使用するためのポートの状態を調べるポートスキャンツール，パスワードを破るためのパスワードクラッキングツールなどがある．権利取得の後に行われる不正実行は多岐にわたるが，特に，機密情報などを盗み取る盗聴，他人の権限を悪用してオンライン送金を行うなりすまし，Web サイトや取引情報などのデータを書き換える改ざんは，基本的な不正行為と言われている．以下では，脅威が生じる対象ごとに具体的な攻撃例や対策を挙げながら説明する．

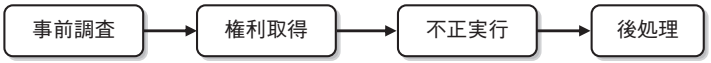

図 1.6 不正アクセスの 4 つの段階．

1.2.2 データに対する脅威

(1) 盗聴

盗聴は，コンピュータネットワークを流れるデータを傍受したり，コンピュータ内部のデータを不正に参照したりして，情報を盗み取ることである．

盗聴を防ぐ技術として，暗号技術がインターネットの普及とともに様々な場面で広く用いられるようになった．暗号は，ある一定の法則（アルゴリズム）に基づいてデータを変換し，元のデータ（平文）を第三者に知られないようにする技術である．たとえば，コンピュータネットワークにおける暗号通信は，送信者が送信したい平文を暗号化し，暗号文としてネットワークに送信する．受信者は受信した暗号文を平文に戻す正規の鍵を用いて復号し，平文を得る．暗号方式は，暗号化や復号に用いる鍵の扱いの違いに応じて，共通鍵暗号方式と公開鍵暗号方式の 2 種類に大別される．暗号技術については，第 2〜5 章で詳細に解説する．

(2) 暗号解読

暗号解読は，正規の鍵を使用せずに別の方法で暗号を解くこと，すなわち暗号文を不正に平文に戻すことである．この際に，正規の鍵を推定することも暗号解読である．なお，復号は正規の鍵を用いて暗号文を平文に戻すことであり，暗号解読と復号は区別して用いられる．

暗号解読を防ぐために暗号の強度を試す研究が行われている．研究としての暗号解読には，暗号の解読だけではなく，デジタル署名の偽造，ハッシュ関数の値が衝突する（同じ値となること）コリジョン探索，あるいは暗号を使った通信プロトコルであるセキュリティプロトコルの解読なども含まれる．

(3) パスワードクラック

パスワードクラック (Password Crack) は，コンピュータやネットワークサービスにアクセスする際のパスワードを不正に入手することである．不正アクセスの事前調査として，標的と