■3 群（コンピュータネットワーク）

7 編 コンピュータネットワークセキュリティ

Security of Computer Network

（執筆者：吉浦　裕）［2009 年 8 月 受領］

■概要■

コンピュータネットワークは水道や電気のような社会の重要インフラになっている．インターネットを中心に，イントラネット，モバイルネット，センサーネット，携帯電話網が重層的に結合し，社会の隅々まで行き届いている．そして，これらのネットワーク上で，行政や金融，流通からコミュニケーション，エンターテインメントに至る多様なサービスが稼働し，人々の生活を支えている．ネットワークがなくては一日も生活できないと言っても過言ではない．コンピュータネットワークセキュリティは，これらのネットワークやサービスを保護し，利用者に安心をもたらす必要不可欠な技術である．

ネットワークの利用形態が多様化し，社会との接点が広がるにつれて，セキュリティ上の問題も多様化・複雑化している．例えば，攻撃の対象は，従来のサーバシステムに加えて，クライアントシステムに広がっている．また，ネットワーク層，トランスポート層から，アプリケーション層更にはコンテンツ層，人間層へと広がっている．このような問題の多様化に従って，それに対処するセキュリティ技術も多様化・複雑化が進んでいる．

しかし，ネットワークへの攻撃は，(1) 不正者による直接的な攻撃（不正侵入）と (2) マルウェアの植付けによる間接的な攻撃の組合せであるという基本的な構造は変わっていない．また，攻撃への対処は，(a) セキュリティプロトコルを用いて，ネットワーク自体を攻撃されにくい構造にする，(b) アクセス制御によって侵入を水際で防止する，(c) 侵入検知によって侵入されたことを早期に把握し回復を図る，の 3 点が基本である．

【本編の構成】

本編では，上記の基本的な分類に沿って，攻撃及び対策技術の基礎と最新動向について述べることにする．すなわち，7 編 1 章（7-1 章）では．コンピュータネットワークセキュリティの動向を説明する．ここでは，システムの安定的稼働（ディペンダビリティ）という上位の目的に沿ってセキュリティの位置づけを示し，人間系を含めた総合的な対策の重要性を述べている．7-2 章は，基本的技術であるアクセス制御を取り上げ，その手法と標準について述べる．7-3 章は，不正侵入手法を説明する．スタックオーバーフロー，SQL インジェクションなどの代表的な侵入手法とその最新動向について述べている．7-4 章は，マルウェアについて取り上げ，古典的なウィルスから DDOS ツール，スパム中継ウィルスなど様々な手法を概観した後，近年大きな問題となっているボットネットについて詳細な分析を示している．7-5 章では，侵入検知システムを説明する．ホスト型，ネットワーク型の基本的な技術を説明した後，通信切断などの対処機能を含む IDPS，より上位層を監視する PIDS，APIDS などの最新動向を説明する．7-6 章はセキュリティプロトコルについて述べる．ネットワークのレイヤに沿って代表的な標準技術（IPSEC，SSL/TLS，S/MIME，XML 署名・暗号）を説明する．7-7 章は，セキュリティ対策をサービスシステムの中に組み込むための実装と運用について述べる．インシデントの未然防止と再発防止の基本技術を述べた後，可用性の維持など実用面の技法，及び不正を告発するためのフォレンジック技術を説明する．セキュリティ

技術を実際に利用するときには，限られたコストで，できるだけ重要なリスク及び多くのリスクに対処する必要がある．最後の 7-7 章では，そのようなリスクの洗い出しと最適な対策選定を目的とするセキュリティマネジメントについて説明する．

【7 編 知識ベース委員会】

編主任：　佐々木良一（東京電機大学）

編幹事：　安田なお（日本ネットワークセキュリティ協会／サイバー大学）
　　吉浦　裕（電気通信大学）
　　寺田真敏（株式会社 日立製作所）

執筆委員：工藤道治（日本アイ・ビー・エム株式会社）
　　小倉秀敏（日本アイ・ビー・エム株式会社）
　　高橋正和（マイクロソフト株式会社）
　　渡辺勝弘（独立行政法人　理化学研究所）
　　鶴岡信彦（独立行政法人　理化学研究所）
　　菊池浩明（東海大学）
　　羽田知史（日本アイ・ビー・エム株式会社）
　　西本逸郎（株式会社 ラック）
　　黒田征太郎（株式会社 ラック）
　　関　宏介（株式会社 ラック）
　　長谷川長一（株式会社 ラック）