20. ネットワークセキュリティに関する知識 I

1. 科目の概要

ネットワークにおけるセキュリティのリスクと、各種リスクに対する対策手法の概要、機能、実装などについて述べる。具体的なセキュリティ要件を説明し、サーバ運用やネットワーク設計におけるセキュリティ実装について実務的な知識を解説する。

2. 習得ポイント

本科目の学習により習得することが期待されるポイントは以下の通り。

習得ポイント	説　明	シラバスの対応コマ
I-20-1. ネットワークセキュリティの基本概念、リスクの種類	ネットワークセキュリティの基本概念とセキュリティ確保に必要な機能を解説する。ネットワークセキュリティに関するリスクの種類を説明し、様々なリスクに対するセキュリティ実装技術を紹介する。	1
I-20-2. ネットワークセキュリティに関連する法律とセキュリティポリシー	不正アクセス禁止法、刑法、電子署名法、個人情報保護法など、ネットワークセキュリティに関連する法整備について解説する。また組織におけるセキュリティポリシーの位置づけについて説明し、構成員の情報セキュリティ意識を高める工夫やセキュリティポリシーの定め方について触れる。	1
I-20-3. コンピュータウィルスの種類と特性	コンピュータウィルスについて、その特性、発生する理由、ウィルスの種類、動作原理などを解説する。またどのような経路で感染が拡大するのか、どのような被害が生じる可能性があるのかを説明する。	2
I-20-4. ウィルス対策ソフトウェアの特徴と運用方法	ウィルス対策ソフトウェアの基本的な考え方を紹介する。さらに、クライアント、サーバ、ゲートウェイといったネットワーク上におけるそれぞれのノードで動作するウィルス対策ソフトウェアの特徴と、運用方法、運用上の留意点について述べる。	2
I-20-5. ネットワークに対する攻撃	ネットワークセキュリティに関して、攻撃の種類、攻撃方法の概要を説明する。攻撃手段としては、パスワード推定、設定・プログラムのミスや脆弱性によるセキュリティホールへの攻撃、DoS、ソーシャルエンジニアリングなどについて言及する。	3
I-20-6. 各種サーバへの不正アクセス手法	TCPの仕様に基づいて攻撃する不正アクセスの種類と内容を解説する。具体的には、Telnet、FTP、SSH、SMTP、POP3、IMAPといった各種サーバへの不正アクセスについて述べ、さらにLandやPing of Deathといったセキュリティの弱点をつく攻撃についても触れる。	4
I-20-7. Webシステムへの不正アクセスと対策	Webシステムのセキュリティリスクについて解説し、バッファオーバフローやDoS攻撃などのWebサービス/Webサーバへの不正アクセスや攻撃の内容と手順、およびそれらに対する対策について説明する。	5
I-20-8. IPプロトコルに対する不正アクセスと対策	IPアドレスの偽造、経路制御の不正、IPソースルーティング、ルーズソースルーティングといったIPプロトコルを悪用した不正アクセスによるセキュリティリスクを紹介し、それぞれの内容と対策について解説する。	6
I-20-9. インターネットセキュリティとネットワークセキュリティの設計と実装方法	TCP/IPネットワークの持つセキュリティリスクと、インターネットで動作するアプリケーションに関するネットワークセキュリティの設計方法、実装方法について解説する。	7
I-20-10. ファイアウォールの仕組みとアクセス制御/フィルタリングの設定方法	ネットワークセキュリティの重要技術であるアクセス制御とフィルタリングについて説明し、その実装であるファイアウォールの機能と設定方法、運用の考え方について解説する。	8

【学習ガイダンスの使い方】

1. 「習得ポイント」により、当該科目で習得することが期待される概念・知識の全体像を把握する。
2. 「シラバス」、「IT 知識体系との対応関係」、「OSS モデルカリキュラム固有知識」をもとに、必要に応じて、従来の IT 教育プログラム等との相違を把握した上で、具体的な講義計画を考案する。
3. 習得ポイント毎の「学習の要点」と「解説」を参考にして、講義で使用する教材等を準備する。

3. IT 知識体系との対応関係

「20. ネットワークセキュリティに関する知識 I 」と IT 知識体系との対応関係は以下の通り。

科目名	基本レベル（I）								応用レベル（II）						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
20. ネットワークセキュリティに関する知識	<ネットワークセキュリティの概要>	<ウィルスの特性と対策>	<ネットワーク攻撃方法の簡易的な分類>	<TCPにおけるセキュアな技術>	<Webにおける攻撃>	<IPにおける不正アクセス技術>	<TCP/IPネットワークセキュリティの設計方法>	<アクセス制御の仕組みとファイアウォールの機能>	<Linuxのネットワークセキュリティ対策>	<ネットワーク脆弱性調査>	<セキュアなネットワークの構築>	<侵入検知システムの仕様と導入>	<IDSによる侵入検知>	<ネットワークセキュリティ構築>	<モバイルコンピューティングとリモートアクセスのセキュリティ>

[シラバス：http://www.ipa.go.jp/software/open/ossc/download/Model_Curriculum_05_20.pdf]

<IT 知識体系上の関連部分>

分野		科目名	1	2	3	4	5	6	7	8	9	10	11	12	13
組織関連事項と情報システム	1	IT-IAS. 情報保証と情報セキュリティ	IT-IAS1. 基礎的な問題 [20-I-1]	IT-IAS2. 情報セキュリティの仕組み（対策） [20-I-1, 7]	IT-IAS3. 運用上の問題 [20-I-1]	IT-IAS4. ポリシー [20-I-1]	IT-IAS5. 攻撃 [20-I-2, 3, 4, 5]	IT-IAS6. 情報セキュリティ分野 [20-I-7]	IT-IAS7. フォレンジック（情報証拠）	IT-IAS8. 情報の状態	IT-IAS9. 情報セキュリティサービス [20-I-1]	IT-IAS10. 脅威分析モデル	IT-IAS11. 脆弱性 [20-I-3, 4]		
	2	IT-SP. 社会的な観点とプロフェッショナルとしての課題	IT-SP1. プロフェッショナルとしてのコミュニケーション	IT-SP2. コンピュータの歴史	IT-SP3. コンピュータを取り巻く社会環境	IT-SP4. チームワーク	IT-SP5. 知的財産権	IT-SP6. コンピュータの法的問題 [20-I-1]	IT-SP7. 組織の中のIT	IT-SP8. プロフェッショナルとしての倫理的な問題と責任	IT-SP9. プライバシーと個人の自由				
応用技術	3	IT-IM 情報管理	IT-IM1. 情報管理の概念と基礎	IT-IM2. データベース問合わせ言語	IT-IM3. データアーキテクチャ	IT-IM4. データモデリングとデータベース設計	IT-IM5. データと情報の管理	IT-IM6. データベースの応用分野							
	4	IT-WS Webシステムとその技術	IT-WS1. Web技術	IT-WS2. 情報アーキテクチャ	IT-WS3. デジタルメディア	IT-WS4. Web開発	IT-WS5. 脆弱性 [20-I-1, 5]	IT-WS6. ソーシャルソフトウェア							
ソフトウェアの方法と技術	5	IT-PF プログラミング基礎	IT-PF1. 基本データ構造	IT-PF2. プログラミングの基本的構成要素	IT-PF3. オブジェクト指向プログラミング	IT-PF4. アルゴリズムと問題解決	IT-PF5. イベント駆動プログラミング	IT-PF6. 再帰							
	6	IT-IPT. 技術を統合するためのプログラミング	IT-IPT1. システム間通信	IT-IPT2. データ割り当てと変換	IT-IPT3. 統合的コーディング	IT-IPT4. スクリプティング手法	IT-IPT5. ソフトウェアセキュリティの実現	IT-IPT6. 種々の問題	IT-IPT7. プログラミング言語の概要						
	7	CE-SWE. ソフトウェア工学	CE-SWE0. 歴史と概要	CE-SWE1. ソフトウェアプロセス	CE-SWE2. ソフトウェアの要求と仕様	CE-SWE3. ソフトウェアの設計	CE-SWE4. ソフトウェアのテストと検証	CE-SWE5. ソフトウェアの保守	CE-SWE6. ソフトウェア開発・保守ツールと環境	CE-SWE7. ソフトウェアプロジェクト管理	CE-SWE8. 言語翻訳	CE-SWE9. ソフトウェアのフォールトトレランス	CE-SWE10. ソフトウェアの構成管理	CE-SWE11. ソフトェアの標準化	
	8	IT-SIA システムインテグレーションとアーキテクチャ	IT-SIA1. 要求仕様	IT-SIA2. 調達/手配	IT-SIA3. インテグレーション	IT-SIA4. プロジェクト管理	IT-SIA5. テストと品質保証	IT-SIA6. 組織の特性	IT-SIA7. アーキテクチャ						
システム基盤	9	IT-NET ネットワーク	IT-NET1. ネットワークの基礎	IT-NET2. ルーティングとスイッチング	IT-NET3. 物理層	IT-NET4. セキュリティ [20-I-7, 8]	IT-NET5. アプリケーション分野	IT-NET6. ネットワーク管理 [20-I-7]							
	10	CE-NWK テレコミュニケーション	CE-NWK0. 歴史と概要	CE-NWK1. 通信ネットワークのアーキテクチャ	CE-NWK2. 通信ネットワークのプロトコル	CE-NWK3. LANとMAN	CE-NWK4. クライアントサーバコンピューティング	CE-NWK5. データのセキュリティと整合性 [20-I-7, 8]	CE-NWK6. ワイヤレスコンピューティングとモバイルコンピューティング	CE-NWK7. データ通信	CE-NWK8. 組込み機器向けネットワーク	CE-NWK9. 通信技術とネットワーク概要	CE-NWK10. 性能評価	CE-NWK11. ネットワーク管理 [20-I-7, 8]	CE-NWK12. 圧縮と伸張
			CE-NWK13. クラスタシステム	CE-NWK14. インターネットアプリケーション	CE-NWK15. 次世代インターネット	CE-NWK16. 放送									
	11	IT-PT プラットフォーム技術	IT-PT1. オペレーティングシステム	IT-PT2. アーキテクチャと機構	IT-PT3. コンピュータインフラストラクチャ	IT-PT4. デプロイメントソフトウェア	IT-PT5. ファームウェア	IT-PT6. ハードウェア							
	12	CE-OPS オペレーティングシステム	CE-OPS0. 歴史と概要	CE-OPS1. 並行性	CE-OPS2. スケジューリングとディスパッチ	CE-OPS3. メモリ管理	CE-OPS4. セキュリティと保護	CE-OPS5. ファイル管理	CE-OPS6. リアルタイムOS	CE-OPS7. OSの概要	CE-OPS8. 設計の原則	CE-OPS9. デバイス管理	CE-OPS10. システム性能評価		
コンピュータアーキテクチャとアーキテクチャ	13	CE-CAO コンピュータのアーキテクチャと構成	CE-CA00. 歴史と概要	CE-CA01. コンピュータアーキテクチャの基礎	CE-CA02. メモリシステムの構成とアーキテクチャ	CE-CA03. インタフェースと通信	CE-CA04. デバイスサブシステム	CE-CA05. CPUアーキテクチャ	CE-CA06. 性能・コスト評価	CE-CA07. 分散・並列処理	CE-CA08. コンピュータによる計算	CE-CA09. 性能向上			
複数領域にまたがるもの	14	IT-ITF IT基礎	IT-ITF1. ITの一般的なテーマ [20-I-1]	IT-ITF2. 組織の問題	IT-ITF3. ITの歴史	IT-ITF4. IT分野（学科）とそれに関連のある分野（学科）	IT-ITF5. 応用領域	IT-ITF6. IT分野における数学と統計学の活用							
	15	CE-ESY 組込みシステム	CE-ESY0. 歴史と概要	CE-ESY1. 低電力コンピューティング	CE-ESY2. 高信頼性システムの設計	CE-ESY3. 組込み用アーキテクチャ	CE-ESY4. 開発環境	CE-ESY5. ライフサイクル	CE-ESY6. 要件分析	CE-ESY7. 仕様定義	CE-ESY8. 構造設計	CE-ESY9. テスト	CE-ESY10. プロジェクト管理	CE-ESY11. 並行設計（ハードウェア、ソフトウェア	CE-ESY12. 実装
			CE-ESY13. リアルタイムシステム設計	CE-ESY14. 組込みマイクロコントローラ	CE-ESY15. 組込みプログラム	CE-ESY16. 設計手法	CE-ESY17. ツールによるサポート	CE-ESY18. ネットワーク型組込みシステム	CE-ESY19. インタフェースシステムと混合信号システム	CE-ESY20. センサ技術	CE-ESY21. デバイスドライバ	CE-ESY22. メンテナンス	CE-ESY23. 専門システム	CE-ESY24. 信頼性とフォールトトレランス	

4. OSS モデルカリキュラム固有の知識

OSS モデルカリキュラム固有の知識として、コンピュータウィルスに関する実践的な知識がある。ウィルスへの具体的な対処法や検出技術を扱う。また、IP プロトコルを悪用した不正などの解説も含む。

科目名	第1回	第2回	第3回	第4回	第5回	第6回	第7回	第8回
20.ネットワークセキュリティに関する知識 I	(1)インターネットセキュリティのリスク (2)セキュリティ実装技術 (3)ネットワークセキュリティに関連する法整備 (4)組織におけるセキュリティポリ	(1)コンピュータウィルスの特性 (2)コンピュータウィルスへの対処 (3)未知のコンピュータウィルスの検出技術	(1)攻撃手段による分類 (2)攻撃方法の段階	(1)サーバへの侵入準備 (2)セキュリティの弱点をつく攻撃	(1)Web のセキュリティリスク (2)攻撃の種類と特性	(1)IP アドレスのセキュリティリスク	(1)インターネットからの侵入対策 (2)ネットワークセキュリティ設計手順	(1)ファイアウォールの機能

（網掛け部分は IT 知識体系で学習できる知識を示し、それ以外は OSS モデルカリキュラム固有の知識を示している）

スキル区分	OSS モデルカリキュラムの科目	レベル
セキュリティ分野	20　ネットワークセキュリティに関する知識 I	基本
習得ポイント	I-20-1. ネットワークセキュリティの基本概念、リスクの種類	
対応する コースウェア	第 1 回（ネットワークセキュリティの概要）	

I-20-1. ネットワークセキュリティの基本概念、リスクの種類

ネットワークセキュリティの基本概念とセキュリティ確保に必要な機能を解説する。ネットワークセキュリティに関するリスクの種類を説明し、様々なリスクに対するセキュリティ実装技術を紹介する。

【学習の要点】

* インターネット社会において、ネットワークセキュリティの確保は格段に重要性を増している。
* セキュリティの確保がずさんだと、攻撃の被害者になるだけでなく、加害者になる恐れもある。
* インターネットは自律ネットワークの結合であり、自己の自律ネットワークに関してセキュリティを確保することは、インターネット参加者の義務である。

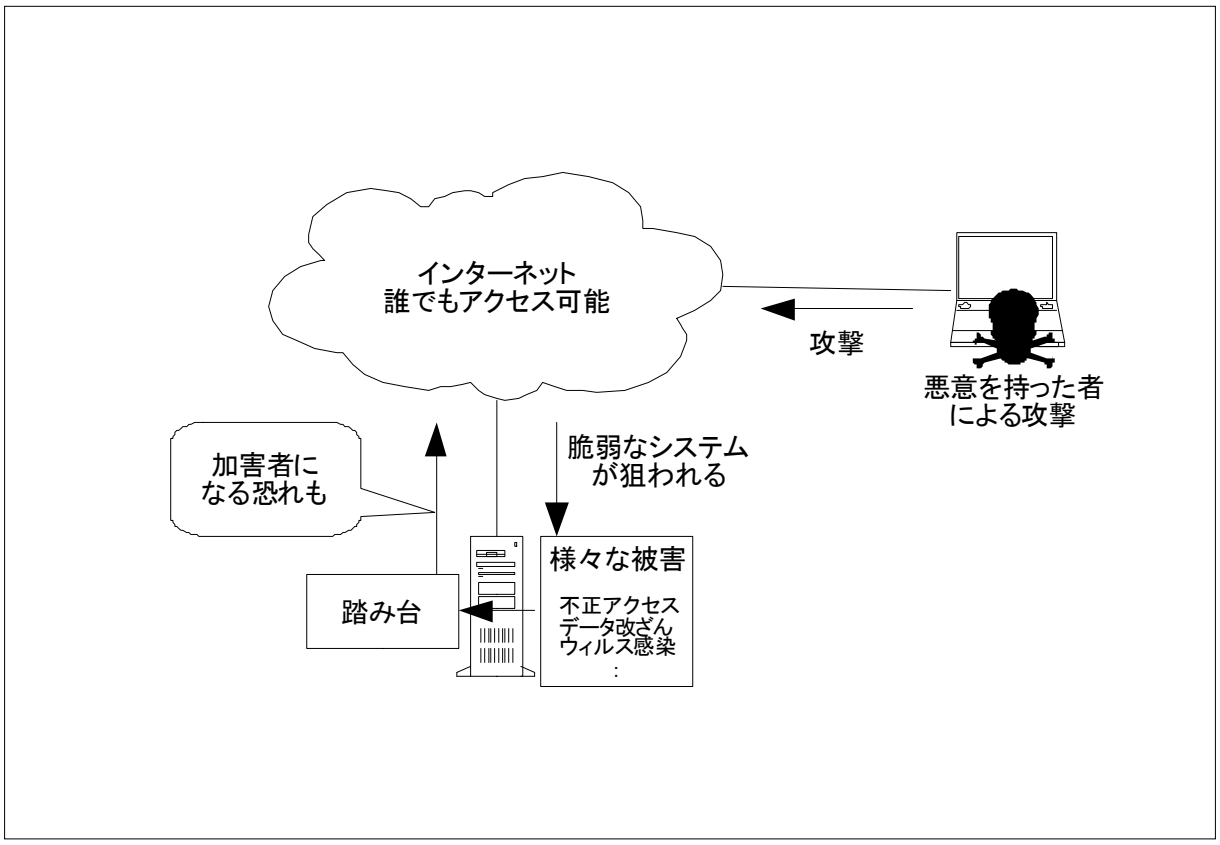

図 I-20-1.　インターネット社会の危険性

【解説】

1) ネットワークセキュリティとは

ネットワークセキュリティとは、コンピュータネットワークを利用した攻撃に対して防衛し、脅威から守ること、または、脅威に対する安全性を指す。

2) ネットワークにおいてリスクとなる脅威の種類

* 不正アクセス
  許可されていない方法でのシステムへのアクセス。
* なりすまし
  他のユーザのふりをしたサービスの利用。
* 盗聴
* データの改ざん、漏えい、詐取
* スパム
  無差別大量なメール配信。
* システムの破壊
* ウィルス、ワーム、トロイの木馬
  他のシステムに侵入、拡散する、悪意を持って作成されたプログラム。
* サービス妨害(DoS)
  不正なデータ、膨大なデータを送りつけてシステムの機能停止/低下を起こす行為。
* 踏み台
  不正アクセスやスパムの中継のために乗っ取られたシステム。

3) ネットワークセキュリティ確保のための機能や実装技術

* ウィルス対策ソフトウェア
* セキュリティパッチ
* パスワード管理ソフトウェア
* 暗号化
* バックアップ
* IRR (Internet Routing Registry)
* プロキシサーバ
* IDS (侵入検知システム)
* DMZ (非武装地帯)
* NAT (Network Address Translation)
* アクセス制御
* フィルタリング
* ファイアウォール

スキル区分	OSS モデルカリキュラムの科目	レベル
セキュリティ分野	20　ネットワークセキュリティに関する知識 I	基本
習得ポイント	I-20-2. ネットワークセキュリティに関連する法律とセキュリティポリシー	
対応する コースウェア	第 1 回（ネットワークセキュリティの概要）	

I-20-2. ネットワークセキュリティに関連する法律とセキュリティポリシー

不正アクセス禁止法、刑法、電子署名法、個人情報保護法など、ネットワークセキュリティに関連する法整備について解説する。また組織におけるセキュリティポリシーの位置づけについて説明し、構成員の情報セキュリティ意識を高める工夫やセキュリティポリシーの定め方について触れる。

【学習の要点】

* コンピュータやインターネットの普及に伴って増大している「ハイテク犯罪」に対し、法整備がされてきている。
* セキュリティ関連の法案を把握しておくことで、トラブルを未然に防ぐことができる。
* 個人情報の取り扱い方針やセキュリティポリシーは、多くの組織が公開するようになってきている。

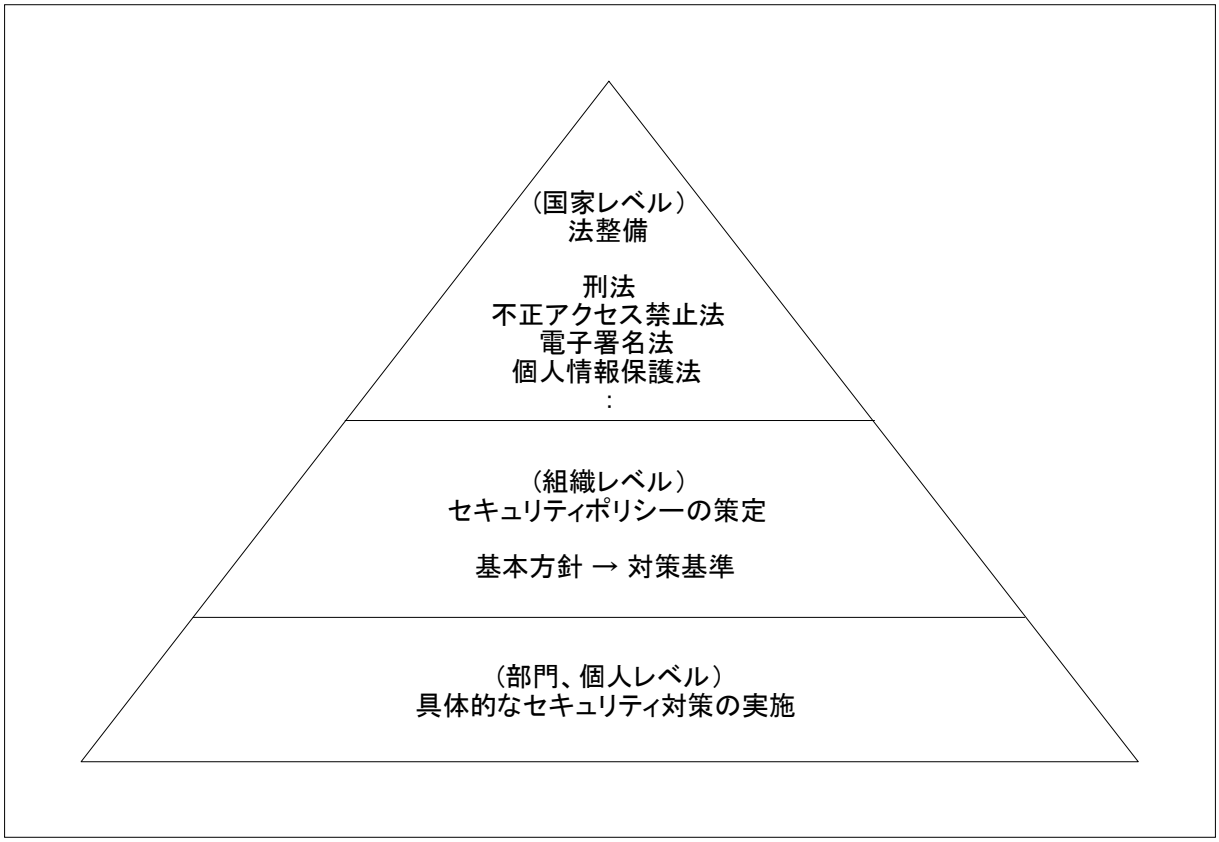

図 I-20-2.　セキュリティに関する法律とセキュリティポリシーの位置づけ

【解説】

1) ネットワークセキュリティに関連する日本での法整備

＊ 刑法

従来、日本では刑法の対象は物理的な財物に対するものとなっていたが、1987 年に、プログラムや情報といった無体物に対しても適用するよう法改正され、俗に「コンピュータ犯罪防止法」と呼ばれる条文が整備された。修正された条文では「電磁的記録」について定義され、文書偽造の罪として「電磁的記録不正作出及び供用」、信用及び業務に対する罪として「電子計算機損壊等業務妨害」、詐欺及び恐喝の罪として「電子計算機使用詐欺」に関する条文が盛り込まれている。

＊ 不正アクセス行為の禁止等に関する法律

2000 年に施行され、俗に「不正アクセス禁止法」と呼ばれる。「アクセス制御機能」について定義され、アクセス制御をかいくぐるような行為を「不正アクセス行為」と位置づけている。不正アクセス行為を禁止するだけでなく、不正アクセス行為を助長する行為の禁止、アクセス管理者による防御措置、都道府県公安委員会による援助等についても盛り込まれている。

＊ 電子署名及び認証業務に関する法律

2001 年に施行され、俗に「電子署名法」と呼ばれる。「電子署名」「認証業務」「特定認証業務」について定義され、特定認証業務の認定について定められている。

＊ 個人情報の保護に関する法律

2005 年に施行され、俗に「個人情報保護法」と呼ばれる。「個人情報」「個人データ」「保有個人データ」について定義され、個人情報データベース等を事業用に供している者は「個人情報取扱事業者」とされ、個人情報取扱事業者の義務などについて盛り込まれている。

2) セキュリティポリシー

組織で取り扱う情報のセキュリティを確保するための、組織として取り組むべき方針や基準のことを、セキュリティポリシーという。組織の情報資産のセキュリティ対策の頂点に位置するものであり、セキュリティポリシーに則って、具体的なセキュリティ対策実施手順が決定される。

＊ 組織構成員のセキュリティ意識の向上

組織構成員にとって、セキュリティと利便性はトレードオフになる場合もあり、歓迎されない場合が多い。セキュリティ確保の重要性について十分に教育し、構成員の行動をセキュリティ面から評価することにより、自発的な行動を促すことが必要であり、セキュリティポリシーにも重要性や評価基準を盛り込むよう工夫する。

＊ セキュリティポリシーの定め方

まず基本方針を定め、それに基づいて、対策基準を定める。

- 基本方針

  セキュリティポリシーの目的、対象範囲、管理体制、義務、罰則などを記述。

- 対策基準

  セキュリティ確保のための遵守事項や判断のための基準を「パスワード管理」「Web サイトの閲覧」「電子メール」などのテーマ毎に記述。

参考として「情報セキュリティポリシーに関するガイドライン」が挙げられる。

http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html

スキル区分	OSS モデルカリキュラムの科目	レベル
セキュリティ分野	20　ネットワークセキュリティに関する知識 I	基本
習得ポイント	I-20-3. コンピュータウィルスの種類と特性	
対応する コースウェア	第 2 回（ウィルスの特性と対策）	

I-20-3. コンピュータウィルスの種類と特性

コンピュータウィルスについて、その特性、発生する理由、ウィルスの種類、動作原理などを解説する。またどのような経路で感染が拡大するのか、どのような被害が生じる可能性があるのかを説明する。

【学習の要点】

＊ インターネットの普及に伴い、メールや Web サイトの閲覧によるウィルス感染が増えている。

＊ 感染経路を理解し、コンピュータ操作の際に注意することで、ウィルス感染の多くを防ぐことができる。

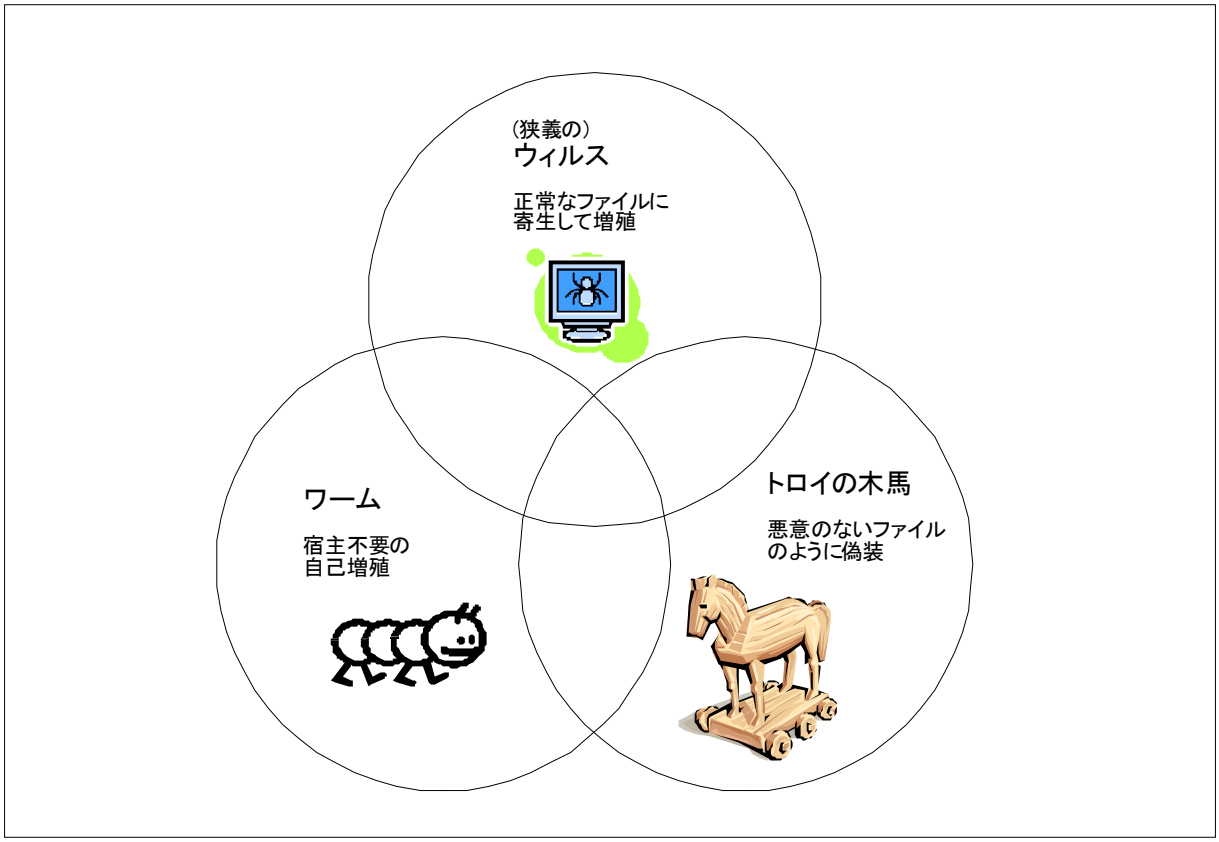

図 I-20-3.　ウィルスの種類と特性

【解説】

1) ウィルスの種類と特性

ウィルスには主に以下のような種類があるが、現在の多くのウィルスはこれらの組み合わせとなる「ハイブリッド型」である。

＊ ウィルス（狭義のウィルス）
正常なファイル(実行型ファイル、マクロ付きファイルなど)や記憶装置のブートセクタなどの「宿主」に寄生し、増殖する不正プログラム。

＊ ワーム
「宿主」を必要としない、自己増殖(自己複製)する不正プログラム。

＊ トロイの木馬
増殖(複製)活動を行わない不正プログラム。悪意のないファイルやプログラムのように偽装し、別の不正な活動を行う。

2) 発生の理由

ウィルスの作者が特定されるケースは少ない。技術力の誇示や愉快犯が多いと思われるが、政治的事由、経済的またはビジネス的事由によるものも少なくない。

3) おもな感染経路

＊ メールの添付ファイルとして届く。
＊ システムのセキュリティホールから侵入する。
＊ ワームに感染したコンピュータから感染する。
＊ セキュリティ的に脆弱なサーバに仕掛けられ、訪問者に感染する。
＊ ファイル共有ネットワークにより感染を拡げる。

4) 動作原理

＊ 感染　　感染経路を通じて感染する。
＊ 潜伏　　目立った症状を出さずに、増殖や拡散を行う。
＊ 発症　　被害を与えるような症状を起こす。

5) おもな被害

＊ ソフトウェアが予期せぬ動作をしたり、使用できなくなったりする。
＊ エラーが発生する。
＊ 処理速度が低下する
＊ ファイルの内容やサイズが書き換えられる。
＊ ディスクの空き容量が次第に減少する。
＊ 外部への送信が増える（勝手にインターネットへ接続しようとする）。
＊ 不明なファイルが作成される。
＊ メールが勝手に送信される。
＊ 情報が漏えいされる。

スキル区分	OSS モデルカリキュラムの科目	レベル
セキュリティ分野	20　ネットワークセキュリティに関する知識 I	基本
習得ポイント	I-20-4. ウィルス対策ソフトウェアの特徴と運用方法	
対応する コースウェア	第 2 回（ウィルスの特性と対策）	

I-20-4. ウィルス対策ソフトウェアの特徴と運用方法

ウィルス対策ソフトウェアの基本的な考え方を紹介する。さらに、クライアント、サーバ、ゲートウェイといったネットワーク上におけるそれぞれのノードで動作するウィルス対策ソフトウェアの特徴と、運用方法、運用上の留意点について述べる。

【学習の要点】

＊ ウィルス対策ソフトウェアの導入は、セキュリティ対策における最も基本的な事項であり、インターネット利用者の責務である。

＊ インターネットとの接点にウィルス対策ソフトウェアを導入するのが効果的であるが、外部記憶装置などからの侵入を防ぐため、各クライアントでの導入も必要である。

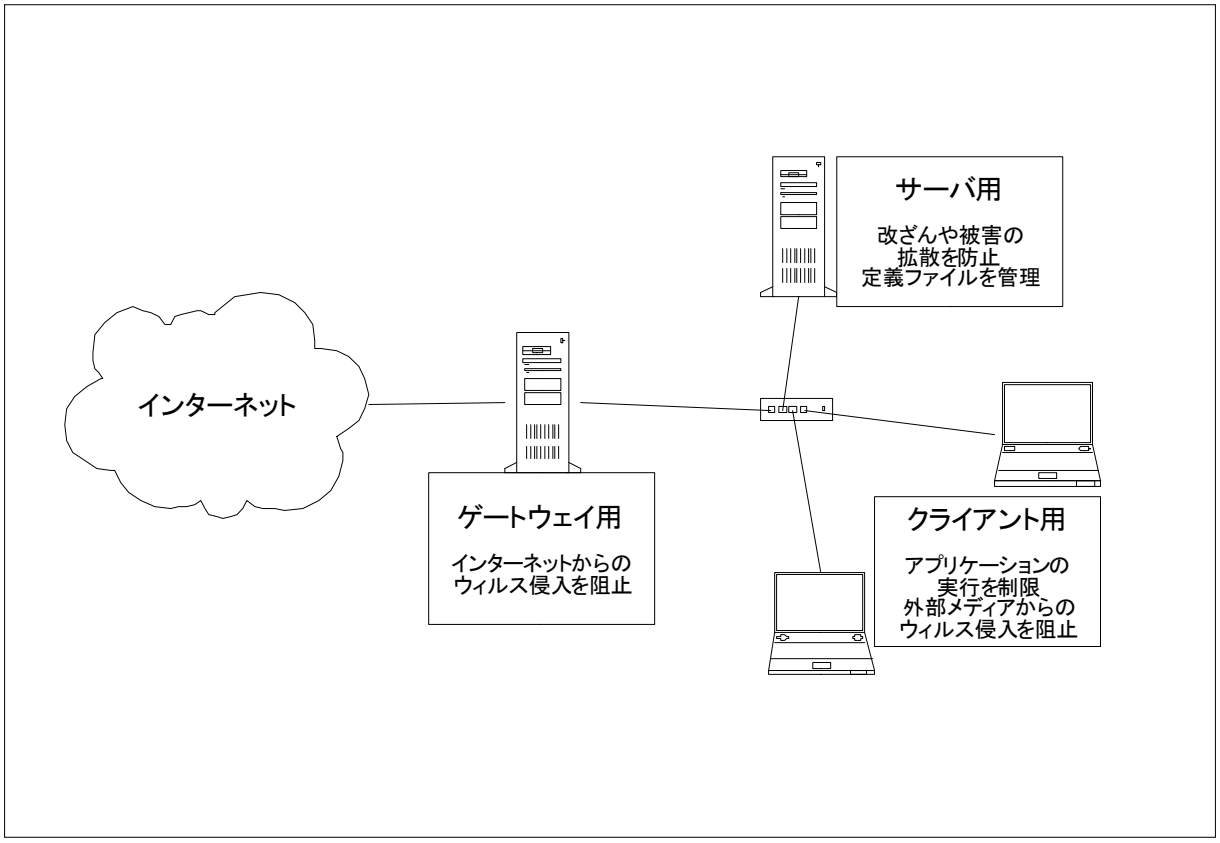

図 I-20-4.　ウィルス対策ソフトウェアの主な用途

【解説】

1) ウィルス対策ソフトウェアの基本

＊ 過去に発見されたウィルスの情報や、ウィルスの可能性が高いと考えられる特徴を記録した定義ファイルを保持する。ウィルスの探索の際は、定義ファイルとの照合によりウィルス検出を行う。

＊ コンピュータ内のファイル、ブートセクタから、侵入済みのウィルスを探索し、検出された場合は、警告、ウィルス駆除、宿主のファイルを削除や隔離といった処理を行う。

＊ システムに常駐し、ファイルの読み書き、メールの送受信、Web サイトへのアクセスといったイベントを監視し、ウィルスを探索する。また、感染の恐れのある操作に対して警告を発する。

＊ 最近では、ファイアウォールの機能を持つものも増えている。

2) ウィルス対策ソフトウェアのノード別の特徴

＊ クライアント用

セキュリティ上の警告を画面表示や音声で通知する機能を持つものが一般的である。また、実行されるアプリケーションは多岐にわたるため、インターネットへ接続するアプリケーションの実行可否をネットワークで一元制御できる機能があり、管理者によって許可されていないアプリケーションを実行できないようにすることができる。

＊ サーバ用

ファイルサーバなどの組織内サーバでは、共有されるファイルが多く含まれるため、ウィルスの拡散を防ぐための侵入検知/防止が特に重要となる。さらに Web サーバなど公開サーバにおいては、改ざん防止が重要である。また、ウィルス対策ソフトウェア自体のサーバとしての機能もあり、定義ファイルやプログラムの一括更新などが可能である。警告は、クライアント用とは異なり、ログ記録や管理者宛のメール通知となる。

＊ ゲートウェイ用

組織内 LAN とインターネットとの接点に導入される。専用のハードウェアとして提供される場合もある。SMTP、POP、FTP、HTTP といった特定のアプリケーションプロトコルで、ゲートウェイまたはプロキシサーバとして振る舞い、パケットの監視や転送を行う。インターネットとの接点で一括で処理するため、効果的だが処理負荷がかかる。ウィルス対策以外に、スパムメール検査なども効果的である。プロキシサーバとして稼動させる場合は、アプリケーションにて適切な設定を行なう必要がある。

3) ウィルス対策ソフトウェアの運用

＊ 管理体制

ネットワーク管理者を設置し、ネットワーク上のウィルス対策の一元管理を行う。

＊ 設定

ウィルス対策ソフトウェアの全機能を有効にすると、警告通知が頻発したり、処理負荷がかかりすぎて実用に耐えない場合もあるので、必須設定や推奨設定を調査検討する。

＊ 定義ファイルの更新

定義ファイルを常に最新のものとなるように保つ。

スキル区分	OSS モデルカリキュラムの科目	レベル
セキュリティ分野	20　ネットワークセキュリティに関する知識 I	基本
習得ポイント	I-20-5. ネットワークに対する攻撃	
対応する コースウェア	第 3 回（ネットワーク攻撃方法の簡易的な分類）	

I-20-5. ネットワークに対する攻撃

ネットワークセキュリティに関して、攻撃の種類、攻撃方法の概要を説明する。攻撃手段としては、パスワード推定、設定・プログラムのミスや脆弱性によるセキュリティホールへの攻撃、DoS、ソーシャルエンジニアリングなどについて言及する。

【学習の要点】

＊ 攻撃の種類を把握することで、セキュリティ確保のための具体的な策を講じることができる。

＊ 攻撃方法は日々進化しているので、既知の攻撃への対処で安心することなく、新手についての情報収集を行い、常に監視の目を光らせることが重要である。

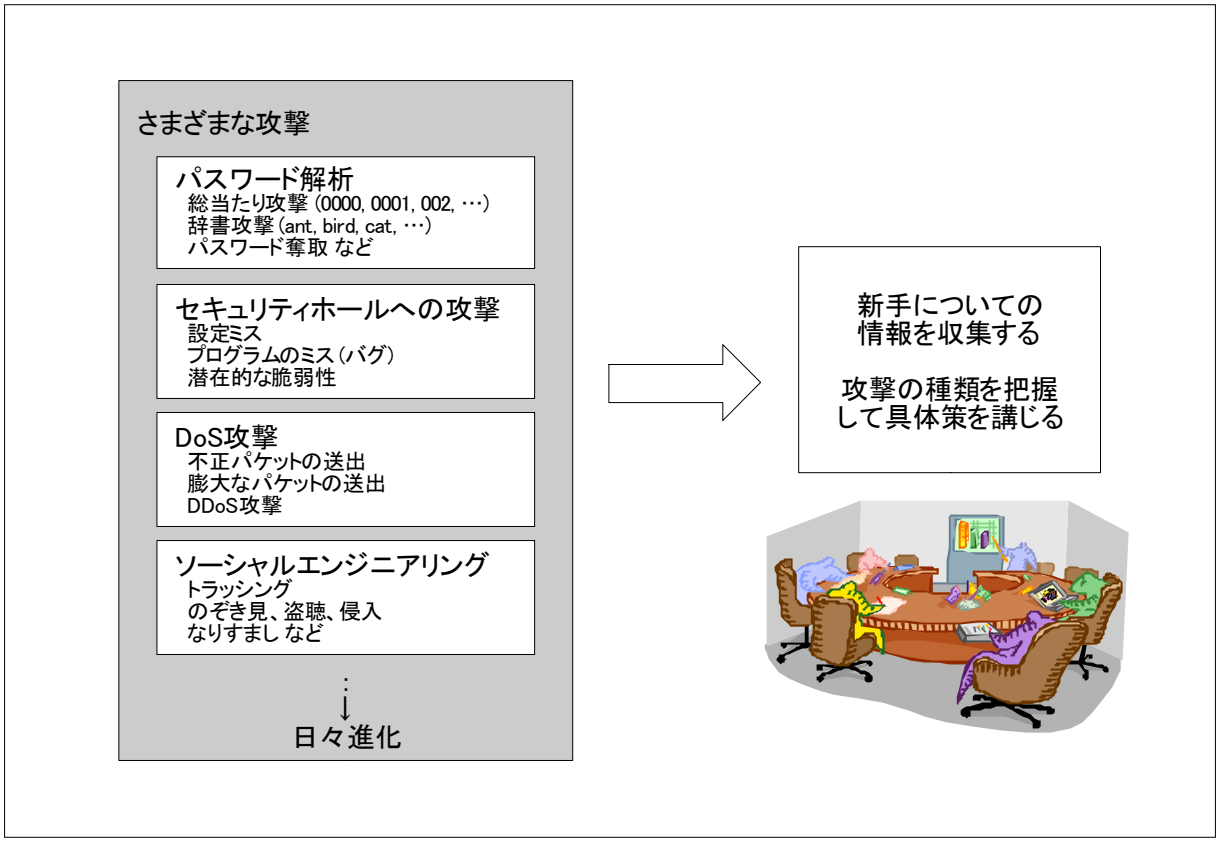

図 I-20-5.　ネットワークにおけるさまざまな攻撃

【解説】

1) パスワード解析

パスワード解析とは、類推などによって不明なパスワードを特定しようとする行為である。特定されたパスワードでなりすまし等の攻撃を行う。パスワード解析には以下のような手法がある。

＊ 総当たり攻撃
ブルートフォース攻撃ともいう。パスワードに使用するすべての文字の順列を総当たりで試みる。解析の時間がかかる方法だが、短いものであれば、時間さえかければ確実にパスワードを奪取することができる。

＊ 辞書攻撃
一般的な単語、固有名詞、誕生日など、パスワードに用いられると想定した文字列の辞書を用意し、その辞書の文字列を試みる。

＊ その他
トロイの木馬(偽装したログイン画面などでパスワードを入力させる)、ソーシャルエンジニアリング(電話などで管理者を装ってパスワードを尋ねたり、キー操作やメモを盗み見たりする)、キーロガー(キーボードからの入力を記録するツールを埋め込む)、経路盗聴といった行為によってパスワード奪取が行われる。

2) セキュリティホールへの攻撃

ネットワークやプログラムの設定ミス、プログラムのミス(バグ)や、潜在的な脆弱性によるセキュリティホールを突いてくる攻撃。バッファオーバーフロー(バッファオーバーラン)はその一例で、C 言語などメモリアクセスの自由度が高い言語で適切なメモリ管理がなされていない場合、想定外のメモリ領域を使用され、任意のプログラムを実行されたりする。

3) DoS 攻撃

DoS(Denial of Service)攻撃とは、ターゲットのシステムに対して意図的に不正なパケットや膨大なパケットを送りつけることで、そのシステムの機能が正常に動作できない状態に陥れる行為である。DoS 攻撃には以下のような手法がある。

＊ CPU、メモリ、ディスク等のリソースを過負荷状態やオーバーフロー状態にする。

＊ 大量パケットを送りつけ、ネットワーク帯域を使い切る。

＊ セキュリティホールへの攻撃により、プログラムを終了させたり、異常な状態にさせる。

また、乗っ取ったホストを踏み台にして、複数のホストから一斉にDoS 攻撃をしかけてくる行為もあり、DDoS(Distributed DoS)攻撃と呼ばれる。

4) ソーシャルエンジニアリング

ソーシャルエンジニアリングという語は、不正アクセスのためにオフラインで行われる情報収集活動を指すことがある。主な手法は以下の通りである。

＊ トラッシング（ゴミとして廃棄されたものから情報を取得する）

＊ のぞき見、盗聴、建物や室内への侵入

＊ なりすまし（管理者を装った電話など）

＊ その他（不正アクセスのために構成員となったり関係者と仲良くなるなど）

スキル区分	OSS モデルカリキュラムの科目	レベル
セキュリティ分野	20　ネットワークセキュリティに関する知識 I	基本
習得ポイント	I-20-6. 各種サーバへの不正アクセス手法	
対応する コースウェア	第 4 回（TCP における不正アクセス技術）	

I-20-6. 各種サーバへの不正アクセス手法

TCP の仕様に基づいて攻撃する不正アクセスの種類と内容を解説する。具体的には、Telnet、FTP、SSH、SMTP、POP3、IMAP といった各種サーバへの不正アクセスについて述べ、さらに Land や Ping of Death といったセキュリティの弱点をつく攻撃についても触れる。

【学習の要点】

＊ TCP の仕様に基づく攻撃は、インターネット上で絶えず行われている。

＊ 暗号化されていないサービスとの通信は、データだけでなくパスワードも盗聴される恐れがある。

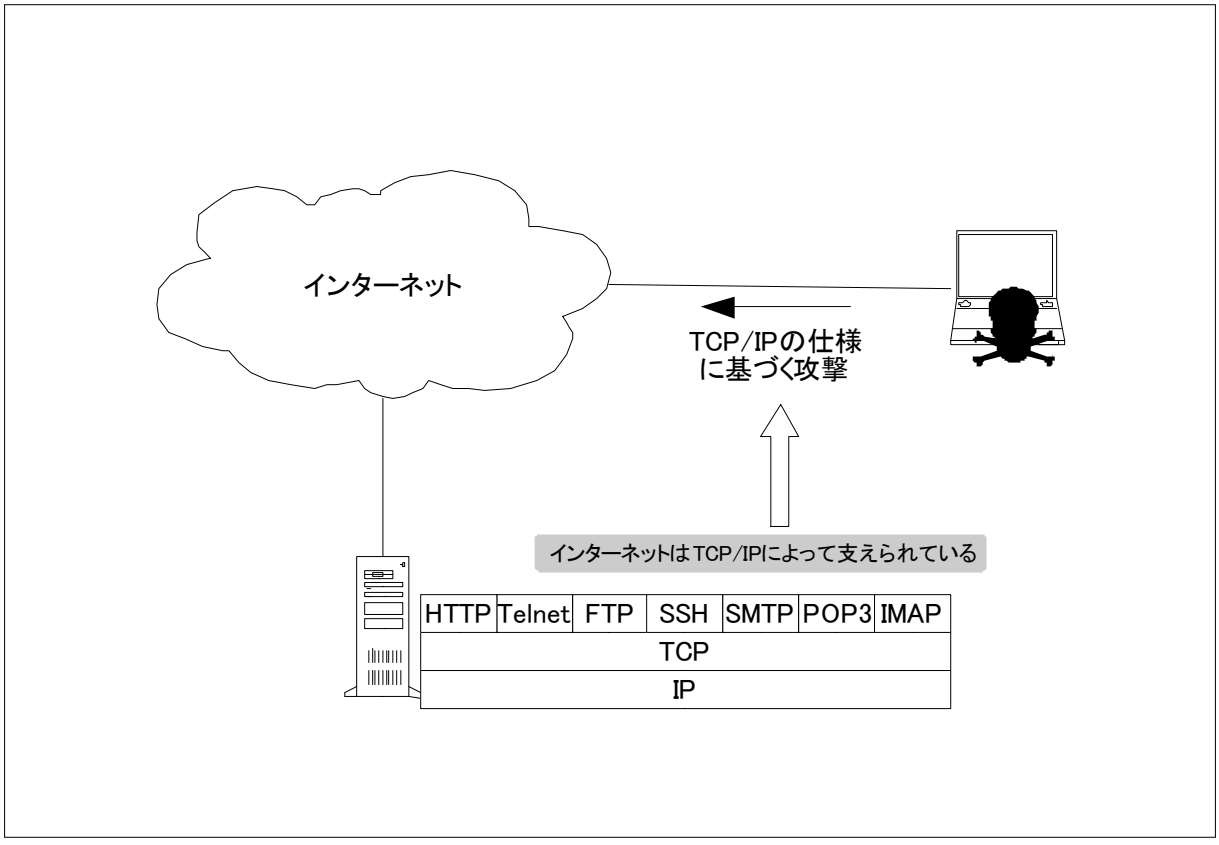

図 I-20-6.　TCP/IP の仕様に基づくサーバへの攻撃

【解説】

1) ポートスキャン

TCP(および UDP)では、各サービスにポート番号が割り当てられている。ターゲットホストのポートがアクティブかどうかの調査を、ツールなどにより自動実行することを、ポートスキャンという。ポートスキャンでは、各ポートのバナー情報(提供しているアプリケーションの種類やバージョン番号)を取得することも可能である。telnet コマンドによりポートスキャンを行うことができる。

2) 各種サーバへのおもな不正アクセス

* Telnet
  ID/パスワードによる認証において、辞書攻撃が行われる。暗号化されないクリアテキスト(平文)で通信されるため、盗聴されやすい。
* FTP
  ID/パスワードによる認証において、辞書攻撃が行われる。暗号化されないクリアテキスト(平文)で通信されるため、盗聴されやすい。
* SSH
  ID/パスワードによる認証において、辞書攻撃が行われる。
* SMTP
  SMTP を単独で認証機能無しで設置されているケースが多く、そのような場合はスパムの踏み台にされやすい。SMTP over SSL/TLS 等で暗号化されない場合、盗聴されやすい。
* POP3
  ID/パスワードによる認証において、辞書攻撃が行われる。POP3 over SSL/TLS 等で暗号化されない場合、盗聴されやすい。
* IMAP
  ID/パスワードによる認証において、辞書攻撃が行われる。IMAP over SSL/TLS 等で暗号化されない場合、盗聴されやすい。

3) TCP、ICMP におけるその他の攻撃

* Land 攻撃
  DoS 攻撃の一手法で、宛先 IP アドレス/TCP ポート番号と、送信元 IP アドレス/TCP ポート番号とを同一にした TCP 接続要求を大量に送り込み、サービスを停止させる手法の攻撃。
* Ping of Death
  相手ホストの応答の有無を調べるツール ping を使って、相手ホストの許容量を超えるデータを送り付ける手法の攻撃。古い OS には Ping of Death についてのセキュリティホールを有するものがある。
* Smurf 攻撃
  上記同様に、ping を悪用し、送信元 IP アドレスを偽装して相手のネットワークに送信し、応答パケットを相手のホストに集中させる手法の攻撃。

スキル区分	OSS モデルカリキュラムの科目	レベル
セキュリティ分野	20　ネットワークセキュリティに関する知識 I	基本
習得ポイント	I-20-7. Web システムへの不正アクセスと対策	
対応する コースウェア	第 5 回（Web における攻撃）	

I-20-7. Web システムへの不正アクセスと対策

Web システムのセキュリティリスクについて解説し、バッファオーバフローや DoS 攻撃などの Web サービス/Web サーバへの不正アクセスや攻撃の内容と手順、およびそれらに対する対策について説明する。

【学習の要点】

＊ Web アプリケーションに多くのセキュリティホールを抱えた Web サイトが非常に多く公開されており、不正アクセスの格好のターゲットとなっている。

＊ Web アプリケーションのセキュリティホールは、ファイアウォール、IDS、ウィルス対策では役立たないことが多く、アプリケーション側で対策をしなければならない。

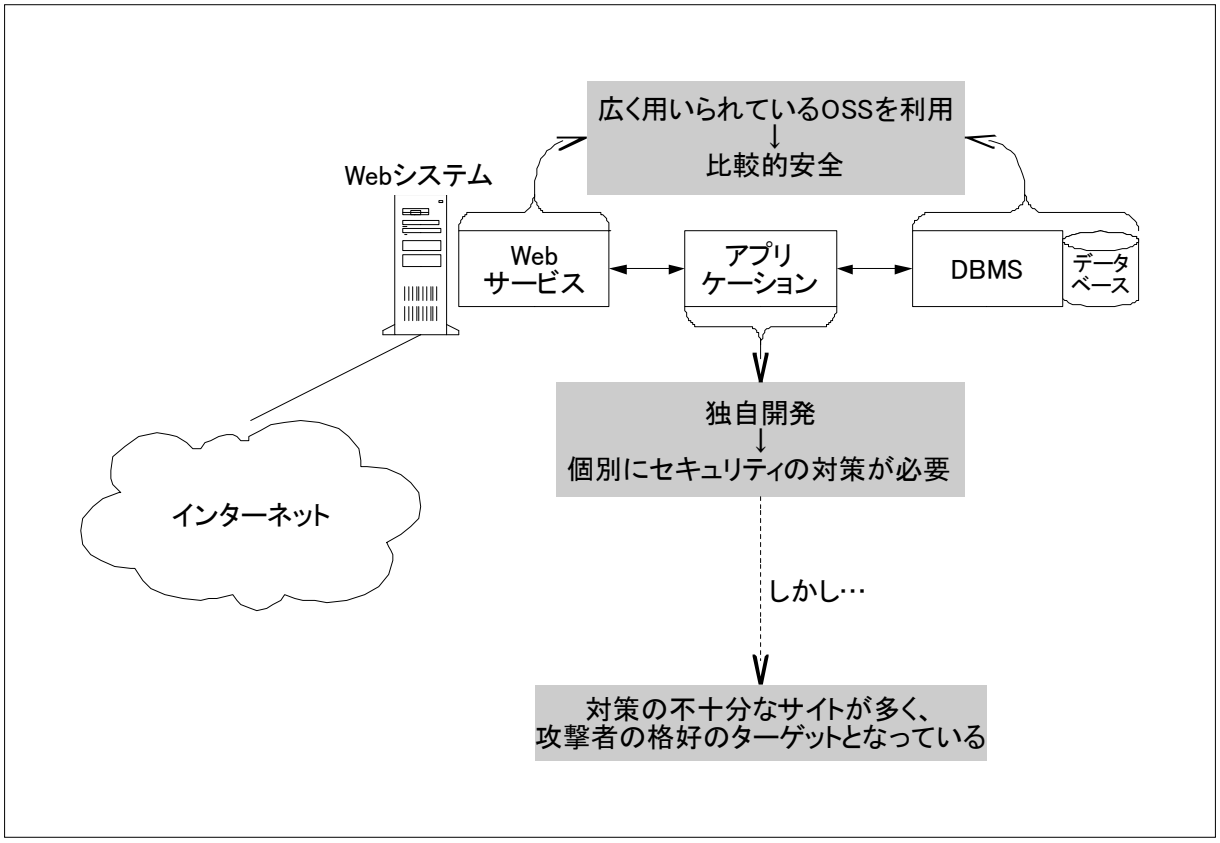

図 I-20-7.　一般的な Web サイトのセキュリティリスク

【解説】

1) Web システムのセキュリティリスク

例えば DoS 攻撃の場合、IDS（不正侵入検知システム）の導入が効果的な場合もあるが、Web システムへの攻撃の多くは、Web アプリケーションのセキュリティホールを狙ったもので、ファイアウォール、IDS、ウィルス対策では役立たない。Web アプリケーションのセキュリティホールを狙った攻撃には、Web アプリケーション側で、攻撃を防ぐような設計、実装をしなければならない。

2) Web アプリケーションのセキュリティホールを狙った攻撃

* アプリケーション・バッファオーバーフロー
  入力フォーム等に異常に長い文字列を入力し、誤動作させる。
* クロスサイトスクリプティング
  ユーザのブラウザ上で不正なスクリプトを実行。
* パラメータ改ざん
  アプリケーションが想定しない値を送信し、誤動作をさせる。
* バックドア、デバッグオプション
  開発/管理用の入り口を探し出す。
* セッションハイジャック
  セッションの盗用を行う。
* SQL インジェクション
  不正入力により任意の SQL 文を実行させる。
* OS コマンドインジェクション
  不正入力により任意の OS コマンドを実行させる。
* エラーコード
  出力されたエラーメッセージからシステムの情報を取得し、攻撃に利用する。
* 強制的ブラウズ
  リンクの張られていない URL に直接アクセスする。
* 盗聴
  HTTPS を利用していない重要な情報のやり取りを盗聴する。
* フィルタのバイパス
  エンコードした文字列を用いてフィルタを回避する。
* クロスサイトリクエストフォージェリ
  正規のユーザの権限を利用し、不正なページに誘導する。
* パストラバーサル
  想定しないパスのファイルにアクセスする・

スキル区分	OSS モデルカリキュラムの科目	レベル
セキュリティ分野	20　ネットワークセキュリティに関する知識 I	基本
習得ポイント	I-20-8. IP プロトコルに対する不正アクセスと対策	
対応する コースウェア	第 6 回（IP における不正アクセス技術）	

I-20-8. IP プロトコルに対する不正アクセスと対策

IP アドレスの偽造、経路制御の不正、IP ソースルーティング、ルーズソースルーティングといった IP プロトコルを悪用した不正アクセスによるセキュリティリスクを紹介し、それぞれの内容と対策について解説する。

【学習の要点】

* IP プロトコルでは、通信相手の特定を IP アドレスに頼っているが、その通信相手が偽装されているかどうかの確認が困難であり、セキュリティリスクを抱えている。
* IP プロトコルはセキュリティリスクより利用するメリットが大きく、様々なリスク軽減措置を整えながら利用されている。

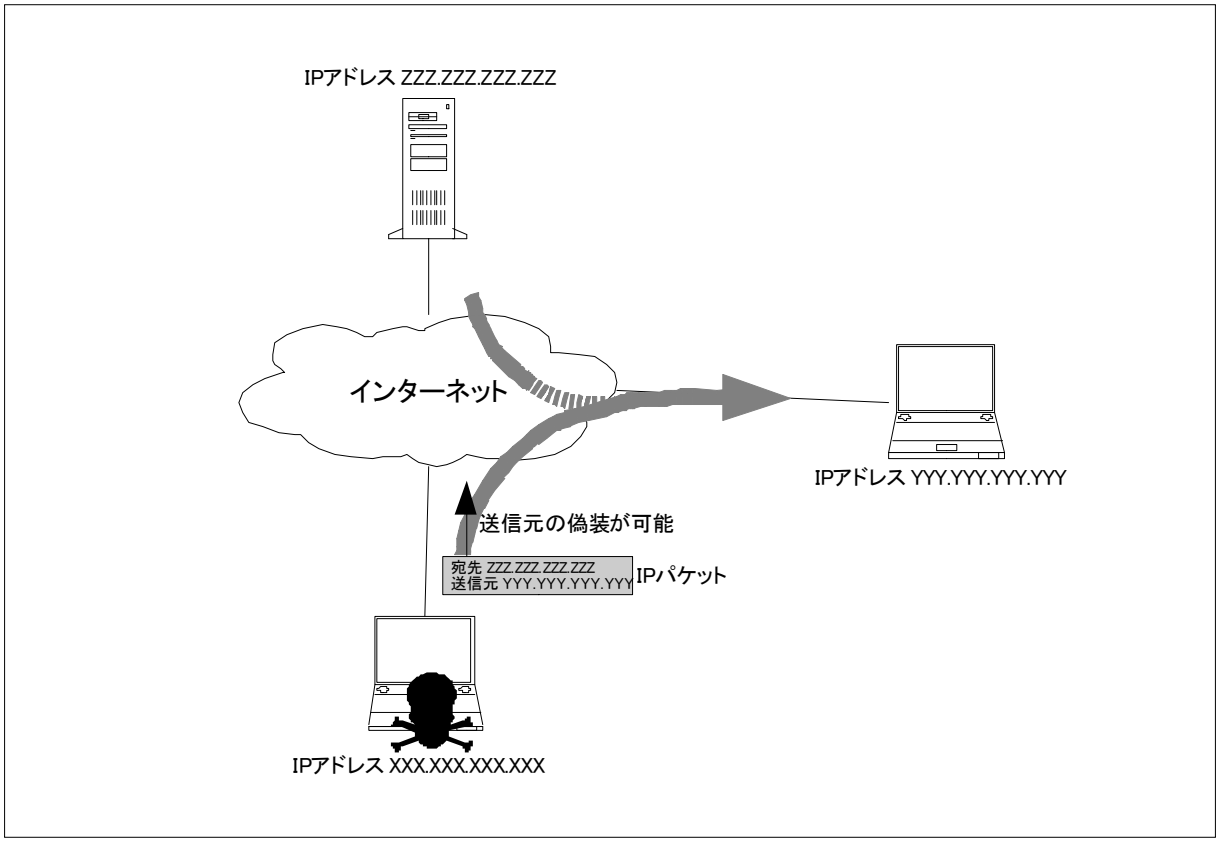

図 I-20-8.　IP アドレスの偽装

【解説】

1) IP アドレスの偽造

送信元 IP アドレスを偽装したパケットを送出する攻撃手法。IP スプーフィングともいわれる。IP プロトコルでは IP アドレスを元に経路制御を行うが、送信元 IP アドレスは偽造が可能であるため、DoS 攻撃パケットの大半は IP アドレスが偽造されている。現状根本的な対策はなく、IP よりも上位層のプロトコルにおいて、接続先の認証やファイアウォールを併用するのが望ましい。

2) IP ソースルーティング

送信元が IP パケットの経路を指定する機能。通常は管理やテストのために用いられる機能だが、これを悪用した攻撃をソースルーティング攻撃といい、以下のようなものがある。

* プライベートアドレスホストへの侵入
  プライベート IP アドレスを使用しているホストに対し、本来外部からはアクセスできないが、プライベート IP アドレスにアクセスできるルータをソースルーティングとして指定することにより、外部からのアクセスが可能となる場合がある。対策としては、IP ソースルーティングが指定されている IP パケットをルータで破棄する方法がある。なお、このように経路の一部を指定するソースルーティングを、ルーズソースルーティングと呼ぶ。
* IP アドレス偽造との併用
  送信元 IP を偽造しても経路を指定しなければ本来の IP アドレスを持つホストに応答が返るが、IP ソースルーティングが利用されている場合、応答パケットも偽造した悪意ある者に返され、IP アドレス認証等を無視した相互通信が可能になる。この理由により、多くの組織では、他ネットワークとの境界にあるルータで、IP ソースルーティングを無効化している。

3) 経路制御の不正

IP ルーティングはルータ同士が経路情報を交換することで成り立っている。ISP(インターネット接続業者)同士の経路情報の交換には、一般に BGP というプロトコルが利用されているが、その経路情報には正しさを証明する裏付けがなく、悪意を持った者が不正な経路情報を送り込むことが可能となっている。このような経路制御上のセキュリティリスクに対しては、以下のような対策、検討がなされている。

* IRR (Internet Routing Registry)
  インターネットの経路情報やその優先性に関する情報を蓄積するデータベース。IRR では経路情報に加えその経路が誰に管理されているかという管理情報も持つ。優先性に関する情報は、ある ISP(インターネット接続業者)が複数ネットワークと接続している際にどの接続からどのようなデータをどのように優先的に流すかという情報である。IRR は経路情報の信憑性を確認するのに有効である。
* soBGP、S-BGP
  soBGP、S-BGP はともに、BGP を拡張した規格で、電子署名技術を利用し、経路情報の正当性を検証できる枠組を構築したものである。両者は電子署名の方式が異なっているが、いずれも既存の BGP からの段階的な移行が可能となっており、普及が検討されている。

スキル区分	OSS モデルカリキュラムの科目	レベル
セキュリティ分野	20　ネットワークセキュリティに関する知識 I	基本
習得ポイント	I-20-9. インターネットセキュリティとネットワークセキュリティの設計と実装方法	
対応する コースウェア	第 7 回（TCP/IP ネットワークセキュリティの設計方法）	

I-20-9. インターネットセキュリティとネットワークセキュリティの設計と実装方法

TCP/IP ネットワークの持つセキュリティリスクと、インターネットで動作するアプリケーションに関するネットワークセキュリティの設計方法、実装方法について解説する。

【学習の要点】

* インターネットとの接続点では、インターネットからの不正アクセスをブロックするような設計が必要である。
* インターネットに公開するサーバは、万一乗っ取られても被害が最小限となるような設計が必要である。
* 内部ネットワークからの攻撃にも対策が必要である。

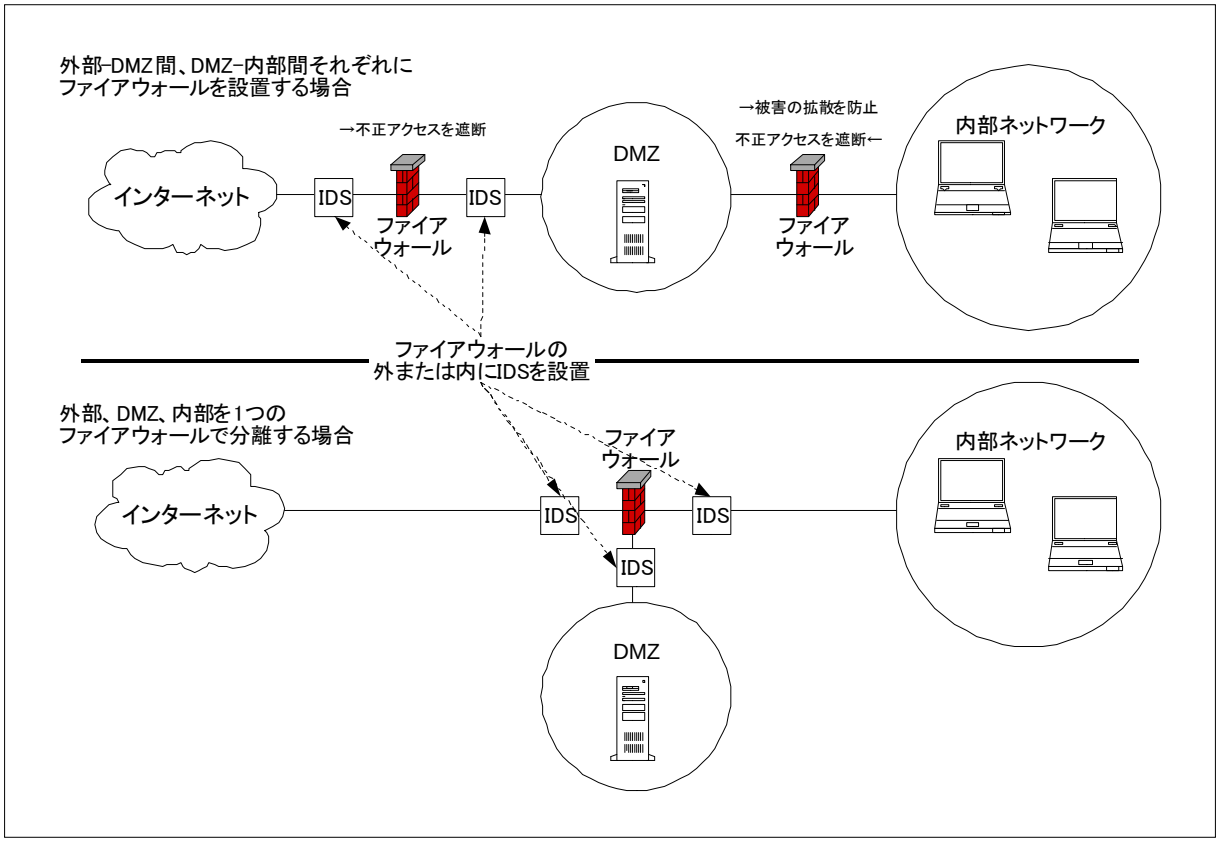

図 I-20-9.　セキュリティを考慮したネットワーク設計の例

【解説】

1) セキュリティの考え方

TCP/IP ネットワークのレベルでセキュリティリスクを捉えると、情報収集や攻撃のための不正アクセスと、攻撃による被害の拡散とが考えられる。そこで、セキュリティ確保には以下のような対策が考えられる。

* 不正アクセスを抑止する
* 不正アクセスを早期に検知する
* 万一攻撃を受けた場合、被害の拡散を抑止する

2) インターネットとの接続点

インターネットとの接続点においては、インターネット側からの不正アクセスの抑止/検知が最重要ポイントとなる。不正アクセスの抑止のために、ファイアウォールを設置するのが一般的である。また、検知のために、IDS(侵入検知システム)を設置することも効果的である。インターネット側からのすべてのアクセスを検知対象としたい場合はインターネットとファイアウォールとの間に、ファイアウォールでブロックできなかったアクセスを検知対象としたい場合はファイアウォールと DMZ(非武装地帯)または内部ネットワークとの間に IDS を設置する。

3) インターネットに公開するサービス(アプリケーション)

万一公開サービスが攻撃を受けた場合、被害を最小限に止めることが重要である。Web サーバやアプリケーションサーバが攻撃を受けても、最も重要なデータベースを守るために、Web サーバやアプリケーションサーバとデータベースサーバとの間にファイアウォールを設置する方法がある。

4) 内部ネットワークとの接続点

万一公開サービスが攻撃を受けた場合、内部ネットワークへの被害拡散を防ぐには、公開サービスのホストと内部ネットワークとの間にファイアウォールを設置する方法がある。この場合、公開サービスのホストは DMZ(非武装地帯)という、インターネットからも内部ネットワークからも独立したネットワークに位置づけられる。DMZ を用いない場合でも、NAT(Network Address Translation)によってグローバル IP アドレスとプライベート IP アドレスとを変換することで、セキュリティを確保することが多い。内部ネットワークからのセキュリティリスクも考慮が必要である。DMZ と内部ネットワークとの間のファイアウォールによって不正アクセスを抑止したり、内部ネットワークに IDS を設置して、不正アクセスを監視する方法がある。また、内部ネットワークからインターネットへアクセスする際のセキュリティ確保として、プロキシサーバを設置する方法もある。NAT も一種のプロキシといえる。

スキル区分	OSS モデルカリキュラムの科目	レベル
セキュリティ分野	20　ネットワークセキュリティに関する知識 I	基本
習得ポイント	I-20-10. ファイアウォールの仕組みとアクセス制御/フィルタリングの設定方法	
対応する コースウェア	第 8 回（アクセス制御の仕組みとファイアウォールの機能）	

I-20-10. ファイアウォールの仕組みとアクセス制御/フィルタリングの設定方法

ネットワークセキュリティの重要技術であるアクセス制御とフィルタリングについて説明し、その実装であるファイアウォールの機能と設定方法、運用の考え方について解説する。

【学習の要点】

* アクセス制御とフィルタリングによって、外部からの不正アクセスをブロックすることができる。
* ファイアウォールはアクセス制御とフィルタリングを行う効果的なシステムだが、ファイアウォール以外の部分でもセキュリティを確保することが重要である。

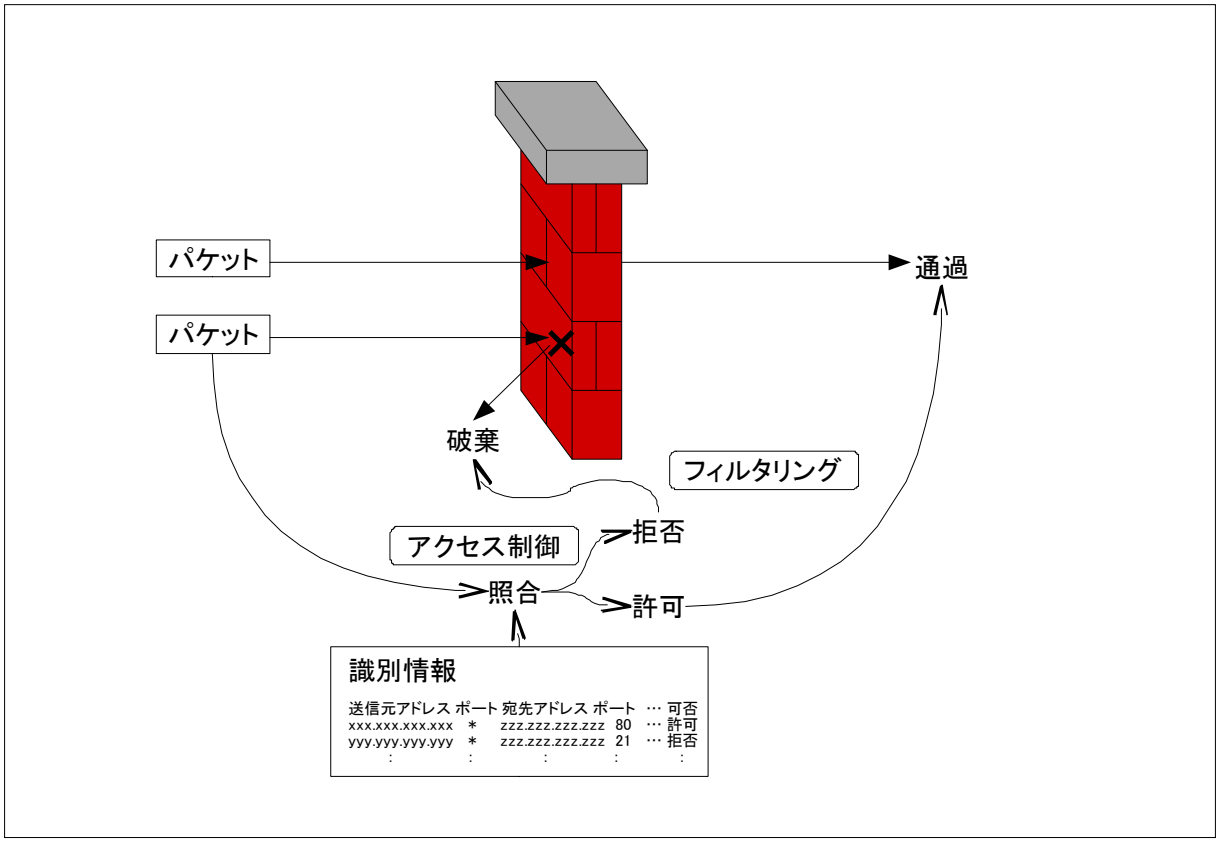

図 I-20-10.　ファイアウォールの仕組み

【解説】

1) アクセス制御とフィルタリング

アクセス制御とは、情報や機能へのアクセス要求に対し、以下のような情報をもとにアクセス可否を判断し、判断結果によってアクセスを拒否する仕組みである。

＊ アクセス要求者

＊ アクセス日時

＊ アクセス場所

＊ アクセス手段

また、フィルタリング(パケットフィルタリング)とは、送られてきたパケットを検査してふるいにかけ、通過させるか破棄するか判断する機能である。アクセス制御とフィルタリングはネットワークセキュリティの重要技術であり、アクセス制御により許可を与えられたパケットのみフィルタを通過させることで、ネットワークのセキュリティを確保するものである。

2) ファイアウォールの機能

ファイアウォールは、あらかじめ設定されたルールに従って、アクセス制御とフィルタリングを行う。

＊ パケットフィルタ型

IP ヘッダや TCP ヘッダに含まれる情報を、パケット通過/破棄の判断基準とする、基本的なフィルタリングを行うもの。判断基準とする情報には、送信元 IP アドレス/ポート番号、宛先 IP アドレス/ポート番号、プロトコル、パケット方向などがある。アプリケーション毎にアクセス制御を切り替える場合は、ポート番号を利用する。

＊ アプリケーションプロキシ型

パケットフィルタ型が主に OSI 参照モデルの第 3～4 層の情報を判断基準とするのに対し、第 7 層までのアプリケーションレベルの情報を判断基準とする。同一アプリケーション内で機能別に判断したりすることができ、細かいアクセス制御が可能だが、その分処理負荷がかかる。

＊ ステートフルインスペクション型

単純なパケットフィルタ型ではパケットを個別に判断するだけだが、過去のパケットの一部の情報も記憶して、通信状態を加味した判断基準を提供する。例えば TCP の応答パケットが正常な応答かどうかを判断することができる。アプリケーションプロキシ型とのハイブリッド型もある。

3) ファイアウォールの設定方法

パケットフィルタ型の場合、上に挙げたような情報(送信元 IP アドレス/ポート番号、宛先 IP アドレス/ポート番号、パケット方向など)の値のパターンを入力し、そのパターンに一致した場合に、パケットを通すか破棄するかを設定する。このようなパターンを複数設定することができる。

4) ファイアウォールの運用の考え方

ファイアウォールでは、ルール上許可したプロトコルを用いた攻撃を防ぐことはできない。また、ウィルスやワームなどを防ぐことにも限界がある。ファイアウォール単体でセキュリティを考えるのではなく、セキュリティポリシーに基づき、IDS やウィルス対策ソフトウェアと併用するなど、システム全体としてのセキュリティを考慮しなければならない。