20. ネットワークセキュリティに関する知識 II

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それらに対する対策手法の具体的な方法として、パケットフィルタリングや侵入検知システムの利用、DeMilitarized Zone の構築といった各種の対策方法について解説する。

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
II-20-1. パケットフィルタリングによるセキュリティ確保	Netfilterやiptablesなどのソフトウェアを利用したパケットフィルタリングによりセキュリティを確保する方法について解説する。また、xinetdのフィルタリング設計や、実際のtelnetサーバでフィルタリングをどのように設定するかといった具体的な手法を説明する。	9
II-20-2. ネットワークの脆弱性調査	ネットワーク脆弱性調査の必要性、目的と意義について説明する。また、脆弱性調査に利用できるツールを紹介し、脆弱性調査の実施体制や評価結果をネットワーク設計に反映させる方法について解説する。	10
II-20-3. Webシステムの脆弱性	ネットワークサーバの中でも主流のWebシステムに関して、その脆弱性評価の方法とリスク、対処方法を説明する。ApacheやOpenSSLといった個別の実装に関する脆弱性に加え、パラメータ操作による攻撃やOSコマンド/SQLインジェクションといった攻撃に対する対策、Webアプリケーションを監査するツールについて述べる。	10
II-20-4. ネットワークセキュリティの新たな要件	ネットワークセキュリティに対する要件として、モバイルアクセスや移動端末など新たに考慮すべき要素を説明する。さらに検疫ネットワークやハニーポットといった新しいセキュリティ対策の実装について解説する。	11
II-20-5. 侵入検知システム(IDS)の仕組み	ネットワークサーバへの不正アクセスを検知する侵入検知システム、Intrusion Detection System (IDS)の原理、機能と効果、侵入検知を行う必要性について解説する。またIDSが持つ課題として検知ポリシーの問題点やIDSを意識した攻撃への対策について説明する。	12
II-20-6. IDSの導入と設定方法	代表的なIDSであるsnortやtripwireを例としてその導入や設定方法について説明する。またネットワークIDSとサーバIDSといった概念の違いを説明する。さらに検知ルールやアクションの設定と行った実際の運用方法について言及する。	13
II-20-7. IDSによるネットワーク監視の作業手順	IDSを用いたネットワーク監視の作業手順として、セキュリティリスクの検討、セキュリティポリシーの検討、ネットワーク構成への反映、IDSが受信した不正アクセスのブラックリスト化といった具体的な作業手順を説明する。	13
II-20-8. ネットワークセキュリティ要件の分析	サーバのセキュリティ要件、クライアントのセキュリティ要件、ネットワークセキュリティ要件といったそれぞれのケースに関して、実際のケースを想定し、具体的なセキュリティの問題と対応策をまとめる。	14
II-20-9. DeMilitarized Zone (DMZ)の設計方法	インターネットとLANの間にファイアウォールを設けてセキュリティを確保すると共に、外向きのサービスを集中的に配置して管理するDeMilitarized Zone (DMZ)の設計と構築する。DMZに配置したサーバを適切に運用するためのフィルタリングルールの設定について解説する。	14
II-20-10. モバイル環境のセキュリティ	モバイルコンピューティングの活用について論じ、そのリスクについて解説する。リモートアクセスのリスク、不正アクセスの問題と対処方法、認証サーバの利用やワンタイムパスワードの仕組みと利用方法などを説明する。	15

【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Ⅱ」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
19. 暗号化に関するスキル	<セキュリティ機能と暗号化の位置づけ>	<暗号化の方式・共通鍵暗号方式>	<暗号化の方式・公開鍵暗号方式>	<情報システムにおける暗号化適用の方式>	<電子証明書の仕組み>	<OSSの活用シーンと暗号化>	<無線LANの暗号化>	<認証と暗号化>	<IPsecによる暗号化通信>	<SSHによるトンネリング>	<SSLプロトコルの仕組み>	<VPN通信の構築>	<PKI(公開鍵暗号化基盤)の仕組み>	<認証基盤構築実習>	<暗号化・これからの活用シーンと課題>

[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 [20-1]	IT-IAS2. 情報セキュリティの仕組み（対策） [20-1, 7] [20-12, 13]	IT-IAS3. 運用上の問題 [20-1]	IT-IAS4. ポリシー [20-1]	IT-IAS5. 攻撃 [20-2, 3, 4, 5]	IT-IAS6. 情報セキュリティ分野 [20-1, 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 [20-1]	IT-IAS10. 脅威分析モデル	IT-IAS11. 脆弱性 [20-3, 4] [20-14]		
	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 [20-1]	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 [20-11]	IT-WS5. 脆弱性 [20-1, 5] [20-14]	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. データ割り当てと交換	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-NE14. セキュリティ [20-7, 8] [20-11, 12, 13, 14]	IT-NET5. アプリケーション分野	IT-NE16. ネットワーク管理 [20-7]							
	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WAN	CE-NWK4. クライアントサーバコンピューティング [20-10]	CE-NWK5. データのセキュリティと整合性 [20-7, 8] [20-14]	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 [20-15]	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 [20-7, 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ハードウェア	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. GPU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 [20-1]	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、ネットワーク・Web システムの脆弱性評価に関する実践的な知識がある。IDS や IPS の具体的な OSS に基づいた説明を行う。

科目名	第9回	第10回	第11回	第12回	第13回	第14回	第15回
20.ネットワークセキュリティに関する知識Ⅱ	(1)パケットフィルタリング (2)セキュリティ環境の構築	(1)ネットワーク脆弱性調査 (2)Web システムの脆弱性評価	(1)ネットワークセキュリティの新しい要件 (2)検疫ネットワーク構築 (3)ハニーポット	(1)IDS (Intrusion Detection (2)IDS の課題	(1)ネットワーク監視の要件 (2)IDSの導入と設定 (3)IDS によるインシデント監視と検知	(1)ネットワークのセキュリティ要件整理 (2)セキュリティ技術の配置 (3)ファイアウォールの導入と設定 (4)ネットワークの脆弱性評価と検証	(1)モバイルコンピューティングの活用シー (2)モバイルコンピューティングのリスク (3)リモートアクセスのリスク (4)不正アクセスの防止策 (5)認証サーバの導入 (6)ワンタイムパスワードによる認証 (7)安全なモバイルコンピューティング

（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　Ⅱ	応用
習得ポイント	Ⅱ-20-1. パケットフィルタリングによるセキュリティ確保	
対応する コースウェア	第 9 回 Linux のネットワークセキュリティ対策	

Ⅱ-20-1. パケットフィルタリングによるセキュリティ確保

Netfilter や iptables などのソフトウェアを利用したパケットフィルタリングによりセキュリティを確保する方法について解説する。また、xinetd のフィルタリング設計や、実際の telnet サーバでフィルタリングをどのように設定するかといった具体的な手法を説明する。

【学習の要点】

- Linux のネットワークシステムには netfilter と呼ばれるサブシステムが含まれ、これはパケットフィルタリングと NAT 機能を提供する。
- netfilter は、通過するパケットのヘッダを見て、そのパケットをアクセプトするかドロップするかを決定するカーネル内のフレームワークである。iptables はフィルタリングまたは NAT ルールを読みこんで、netfilter を制御するツールである。
- xinetd は、ACL (Access Control List) により自ホストへの接続を制御する。また、特定のホストからの同時接続数や接続率を制限することにより、応答機能の停止を狙った攻撃に対処することができる。

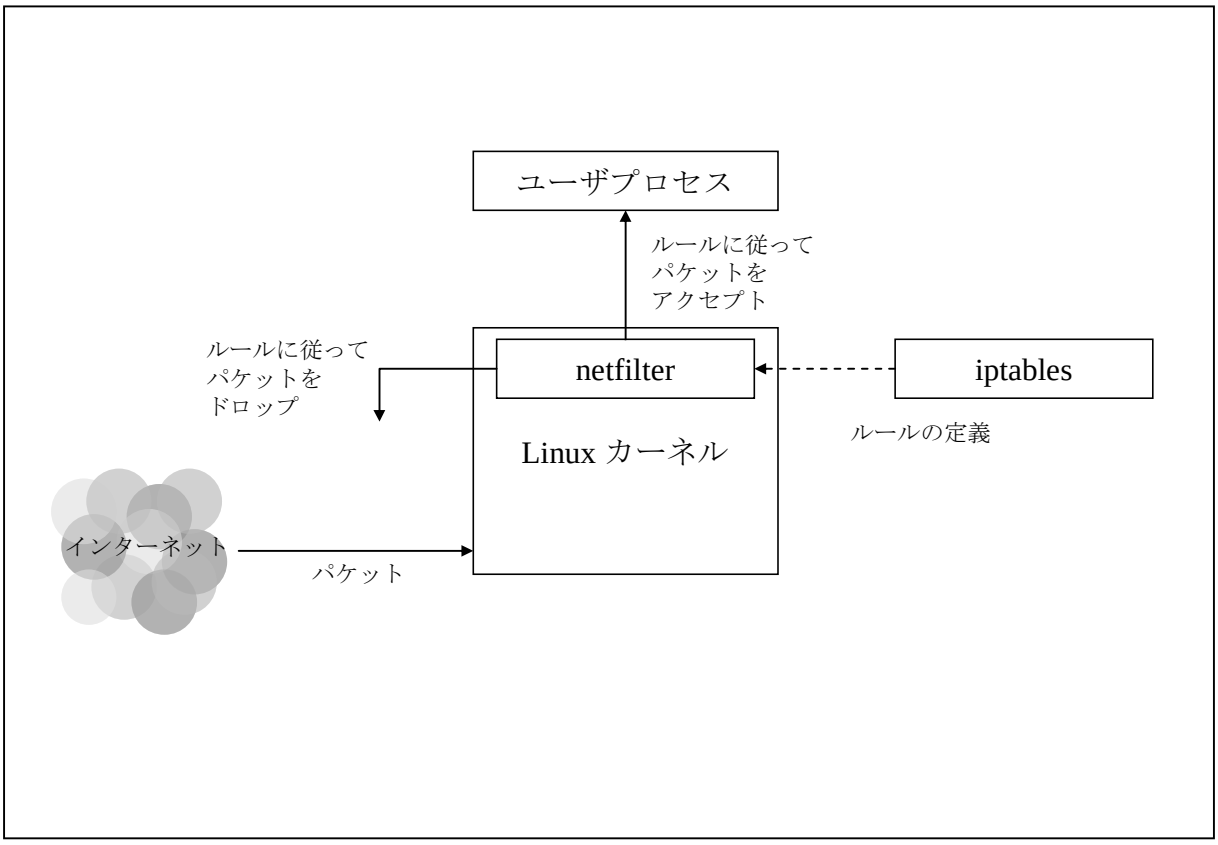

図 II-20-1.　iptables と netfilter を用いてパケットフィルタリングを行なう例

【解説】

1) netfilter とは

＊ netfilter は、Linux カーネル内のネットワークサブシステムに対して、一連のフック関数を定義するカーネル内のフレームワークである。

＊ netfilter の定義するフック関数は、Linux カーネルモジュールから利用できる。これを利用したカーネルモジュールはいくつかあるが、最も知られた実装には、パケットフィルタリングモジュールや NAT モジュールがある。

2) iptables とは

＊ iptables は、Linux カーネル内のネットワークサブシステムに対してパケットフィルタリングルールと NAT ルールを指定するためのコマンドラインツールである。

＊ iptables は、同コマンド（とそれに対応するカーネル内のサブシステム）の実現できるパケットフィルタリング機能を指して、カーネル内ファイアウォールの呼称として用いられることがある。

＊ 使用方法

- iptables コマンドで、パケットフィルタリングルールと NAT ルールを指定する。これは即座に反映されるが、OS の再起動によりリセットされる。 例えば telnet の使用するポート 23 への接続を拒否するには以下のようにする。

  ```
  iptables –A INPUT –p tcp –dport 23 –j DROP
  ```

- iptables-save コマンドで、現在カーネルに対して指定されているルールをダンプすることができる。これをファイルに出力することでルールを永続化することができる。

- iptables-save コマンドにてダンプしたルールは、iptables-restore コマンドにて再度カーネルに指定することができる。一部のディストリビューションでは、デフォルトで用意されている起動スクリプトにて iptables-restore コマンドを実行する（ルールは指定の書式でファイルとして予め記述しておく）。

3) xinetd

＊ xinetd は、各種デーモンプロセスが自身でポートをリッスンする代わりに、xinetd が代表して必要なポートをすべてリッスンすることでシステムのリソースを節約することを目的に設計されたデーモンである。前身として inetd があるが、xinetd はこれを改良したものであり、共にスーパーサーバと呼ばれることがある。

＊ 各種デーモンプロセスの代わりに xinetd がこれを代表することで、接続制御やログ機能を xinetd が一手に引き受けることができる。xinetd は、予め指定された ACL（アクセスコントロールリスト）を読み込んで、接続制御を行なう。

＊ 特定のサービスに対する接続要求が来ると、xinetd は対応するサーバを起動する。各種サーバの設定は、/etc/xinetd.conf にて行なう。一部のディストリビューションでは、/etc/xinetd.d/ディレクトリ内にサービス毎のファイルを用意し、デフォルトでこれらをすべて読み込むよう構成されているものもある。

＊ xinetd の制御は、同時接続数や接続率を基に行なうことができる。この機能によって、DoS（Denial of Services）攻撃からの被害を抑えることができる。

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 II	応用
習得ポイント	II-20-2. ネットワークの脆弱性調査	
対応する コースウェア	第 10 回 ネットワーク脆弱性調査	

II-20-2. ネットワークの脆弱性調査

ネットワーク脆弱性調査の必要性、目的と意義について説明する。また、脆弱性調査に利用できるツールを紹介し、脆弱性調査の実施体制や評価結果をネットワーク設計に反映させる方法について解説する。

【学習の要点】

＊ ネットワークへの攻撃を試みる者からすると、サービスのタイプや、そのサービスの利用するポートやバージョンを知ることは難しいことではない。通常知られても問題ない情報であっても、ソフトウェアのバグにより危険要素となることがあることを念頭に置いておく必要がある。

＊ ネットワークの脆弱性を調べるツールを利用すると、広く使用されているソフトウェアの特定のバージョンの含むバグによる危険因子などを突き止めることができる。

＊ しかし、ツールに頼りすぎることもよくない。管理しているネットワークの特徴を理解し、ツールの検出した危険因子を再度確認することを怠ってはいけない。

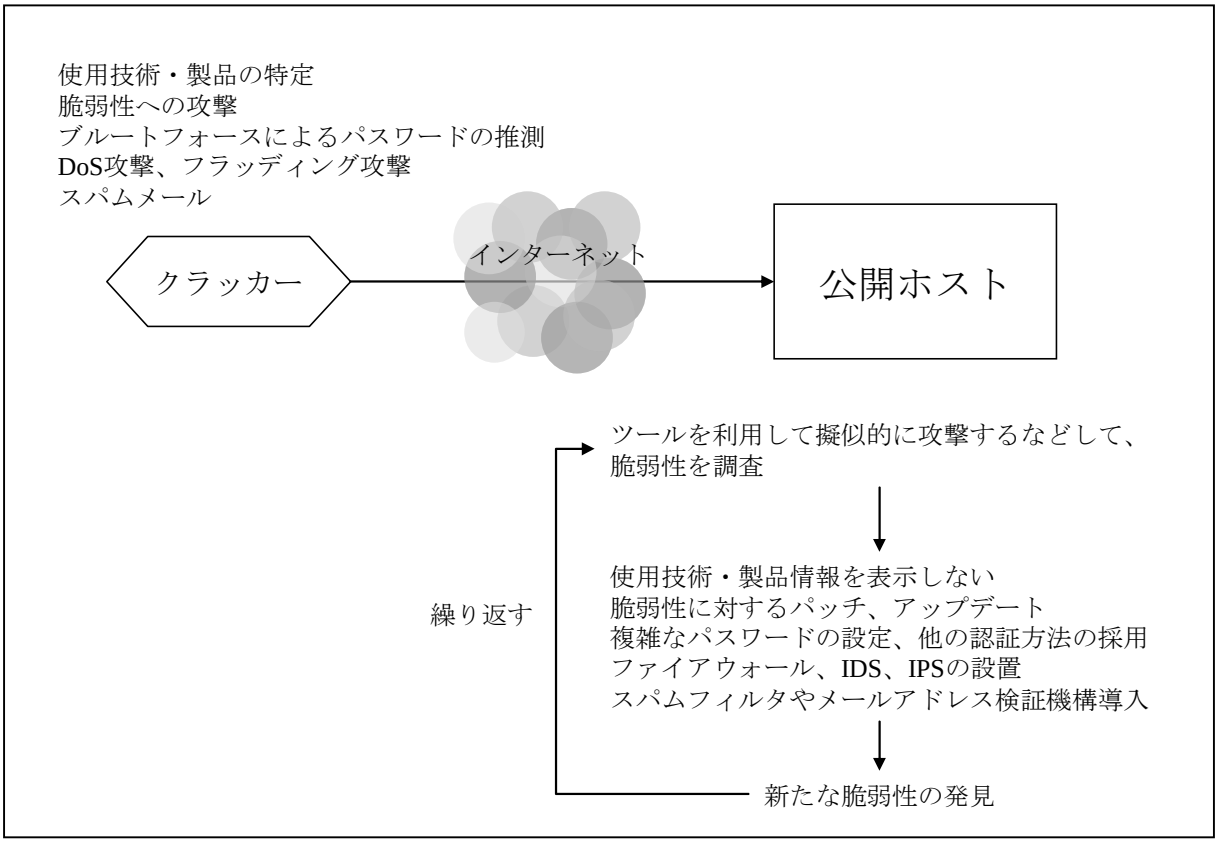

図 II-20-2.　脆弱性への対応

【解説】

1) ネットワークの脆弱性

＊ インターネットに対してサービスを公開しているサーバは常に危険と隣り合わせである。ネットワークやシステムが脆弱であれば、クラッカーの手によっていとも簡単に侵入され、root 権限を取得されてしまう。

＊ ネットワークを経路して侵入されてしまうケースで最も多いのは、公開中のサービスを実現するソフトウェアのバグ、脆弱なパスワードの漏洩、設定の誤りなどへの攻撃によるものである。

＊ Linux の多くのディストリビューションでは、利便性のため、デフォルトで多くのソフトウェアパッケージがインストールされ、起動された状態になっている。これはまったくの無防備状態であり、必要なデーモンのみを起動するようにしなければならない。

＊ クラッカーは、ポートスキャンによってそのサーバのオープンしているポートを簡単に知ることができる。Nessus のようなツールを用いて実際に試してみることができるが、使用しているソフトウェアのバージョンや、OS を特定することはとても容易なことである。

＊ ソフトウェアのバージョンが特定されると、クラッカーはそのバージョンに存在するバグに対して攻撃することができるようになる。一見無害な情報でも、特定の条件下では脆弱性因子になることを知っておく必要がある。

2) ネットワーク脆弱性調査に使用できるツール

＊ nmap

nmap は、ホストがどのようなタイプのサービスを提供しているかをスキャンするツールである。nmap は、UDP、TCP connect、TCP SYN、ICMP など、さまざまな種類のリクエストに対応しており、その応答によりサービスの有無を調べることができる。オプションで、OS の推測を行なったり、スキャンするポートの範囲を指定したりといったことが可能である。

＊ Nessus

Nessus は、脆弱性調査のためのフリーの統合ツール（最新バージョンではソースは非公開）であり、nmap の機能も含んでいる。Nessus は、一般的な情報から、特定の OS の特定のプログラムの持つ脆弱性を知らせてくれる機能を持つ。プラグインをインストールすることで、最新のセキュリティホールに対応することができる。また、実際に侵入を試みる機能も持つ。GUI によるわかりやすいインタフェースを利用することができるという点も特徴のひとつである。

3) 脆弱性に対する考え方

＊ 公開されている脆弱性に加え、ツールでは発見できない脆弱性も実際には存在する。これらを検知するのは非常に難しいため、ツールでの調査を 100%信頼してよいわけではないことを念頭に置いておく必要がある。

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 II	応用
習得ポイント	II-20-3. Web システムの脆弱性	
対応する コースウェア	第 10 回 ネットワーク脆弱性調査	

II-20-3. Web システムの脆弱性

ネットワークサーバの中でも主流の Web システムに関して、その脆弱性評価の方法とリスク、対処方法を説明する。Apache や OpenSSL といった個別の実装に関する脆弱性に加え、パラメータ操作による攻撃や OS コマンド/SQL インジェクションといった攻撃に対する対策、Web アプリケーションを監査するツールについて述べる。

【学習の要点】

* Web システムは、ユーザの入力できる値（フォームフィールド、クエリパラメータ）から脆弱になることが多い。入力値を常に適切にサニティチェックを行う必要がある。
* 定評のある Apache，OpenSSL にも潜在的な不良が存在する可能性がある。報告されている脆弱性に対するパッチを適切なタイミングで適用する必要がある。
* Web に限らず、ソフトウェアに対してすべての脆弱性を発見できるとは限らないが、パターン化された攻撃に対しては必ず対策を講じる必要がある。Web アプリケーションの場合、SQL インジェクション、クロスサイトスクリプティング、セッションハイジャックなど、よく知られた攻撃は確実に避けられるべきである。

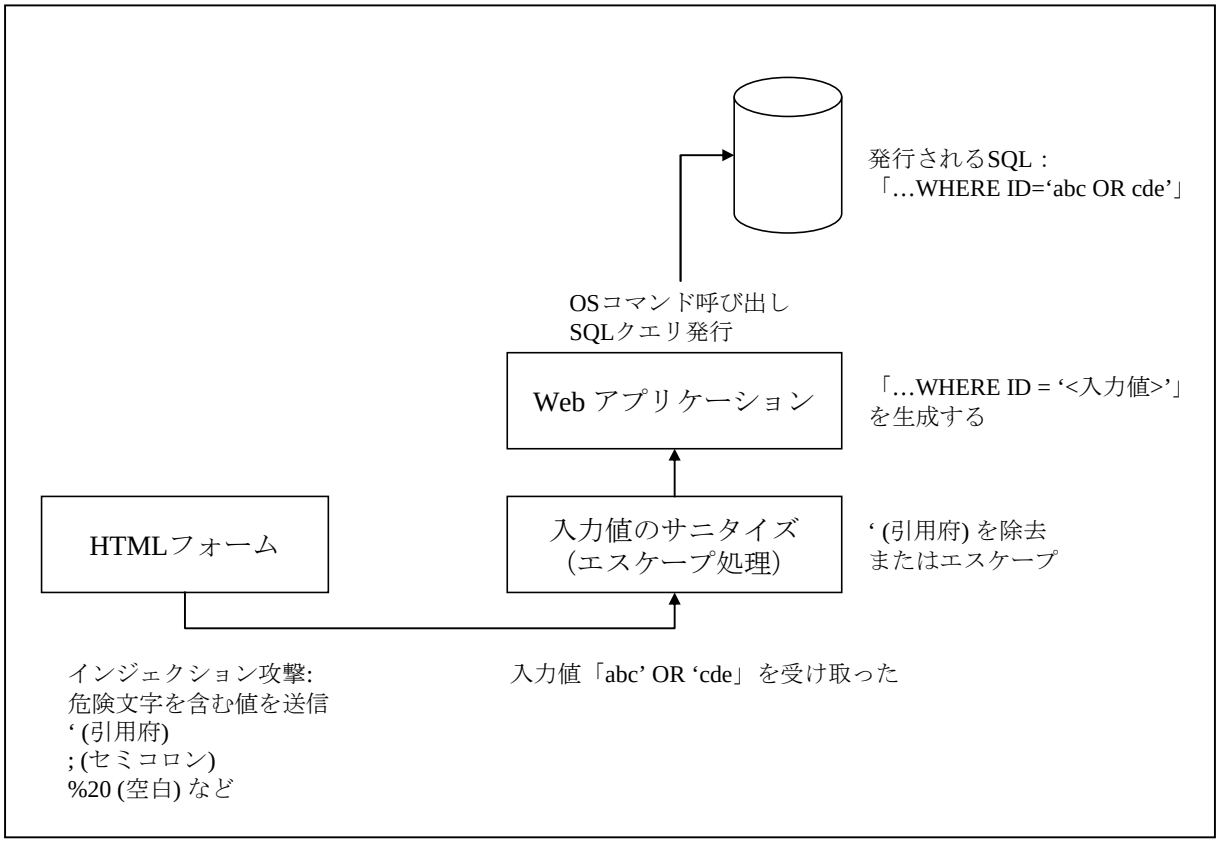

図 II-20-3.　インジェクション攻撃への対策

【解説】

1) Web システムの潜在的危険性

＊ Web システムは、CGI や SSI といった、ユーザが実行できるプログラムを含むことができる。プログラムが脆弱であったり、不適切なパーミッションであれば、悪意のある者が任意のプログラムを実行できてしまうことがある。

＊ Web システムの使用するディレクトリツリーは、適切な所有権とパーミッションを設定し、不用意に CGI や SSI の実行を許可するべきではない。

2) Web アプリケーションの脆弱性

＊ 多くの Web アプリケーションは、HTML のフォームに入力された値を GET または POST メソッドで受け取る。受け取った値について十分な検証が行なわれるべきである。

＊ Web アプリケーションの実体がシェルによる CGI であったり、Web アプリケーションから外部プログラムを起動していたり、SQL でデータベースに問い合わせを行なっているような場合、悪意のある者によって任意のプログラムが実行されたり、不適切な情報を取得されたりすることがあり得る。これらについて十分に対策を施す必要がある。

＊ Web アプリケーション内で、バッファオーバーフローを発生させるような関数を使用するべきではない。よく知られたバッファオーバーフローを発生させる関数には、gets(), strcpy(), getwd(), scanf(), sprintf()などがある。

＊ Perl や PHP を使用しているからといって、バッファオーバーフローの問題を無視してよいわけではない。これらの言語が内部的に C 言語の gets()や strcpy()を使用する拡張関数を定義する場合はとりわけ注意が必要である。

3) パターン化された Web アプリケーションへの攻撃

＊ Web アプリケーションの受け取るリクエストパラメータの値に巧みに制御文字を含ませることにより、任意の OS コマンドを実行したり、任意の SQL 文を発行することが可能である。これらは、OS コマンドインジェクション、SQL インジェクションとして知られる。

＊ インジェクション攻撃は、Web アプリケーション内で、リクエストパラメータの値に対してサニティチェックを行い、無害化することで避けることができる。具体的には制御文字を含むかどうかを検査し、含んでいる場合はエスケープ処理により無害化するか、アクセスを禁止する。

＊ リクエストパラメータの値を適切に無害化しないことによる被害は他にもある。Javascript や Java アプレット、ActiveX のコードを起動するコードの書かれた値がリクエストパラメータとして送信され、サーバ側で無害化を行なわずにブラウザにそのまま入力値を表示することにより、ユーザのブラウザ上で悪意のあるスクリプトが実行される。この手口はクロスサイトスクリプティング（XSS)として知られる。

＊ XSS による具体的な被害として、セッションハイジャック、フィッシングなどが挙げられ、被害は利用者側に及ぶ。

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 II	応用
習得ポイント	II-20-4. ネットワークセキュリティの新たな要件	
対応する コースウェア	第 11 回 セキュアなネットワークの構築	

II-20-4. ネットワークセキュリティの新たな要件

ネットワークセキュリティに対する要件として、モバイルアクセスや移動端末など新たに考慮すべき要素を説明する。さらに検疫ネットワークやハニーポットといった新しいセキュリティ対策の実装について解説する。

【学習の要点】

* モバイル端末の小型化によって、ネットワークへのセキュリティ要件は複雑化している。モバイル端末はネットワークを渡り歩くことになるので、盗聴やウィルスの感染をはじめとする危険因子は多い。モバイル端末からの接続を許可するときは、従来とは違った検査が必要となる。
* 検疫ネットワークは、接続してきた端末を隔離、検査し可能であれば治療する。これにより、有害端末が重要なネットワークに接続されるのを防ぐ。
* ハニーポットとは、トラップとなるホスト、データ、ネットワークを用意し、重要なリソースが攻撃されるのを防ぐ技術の総称である。

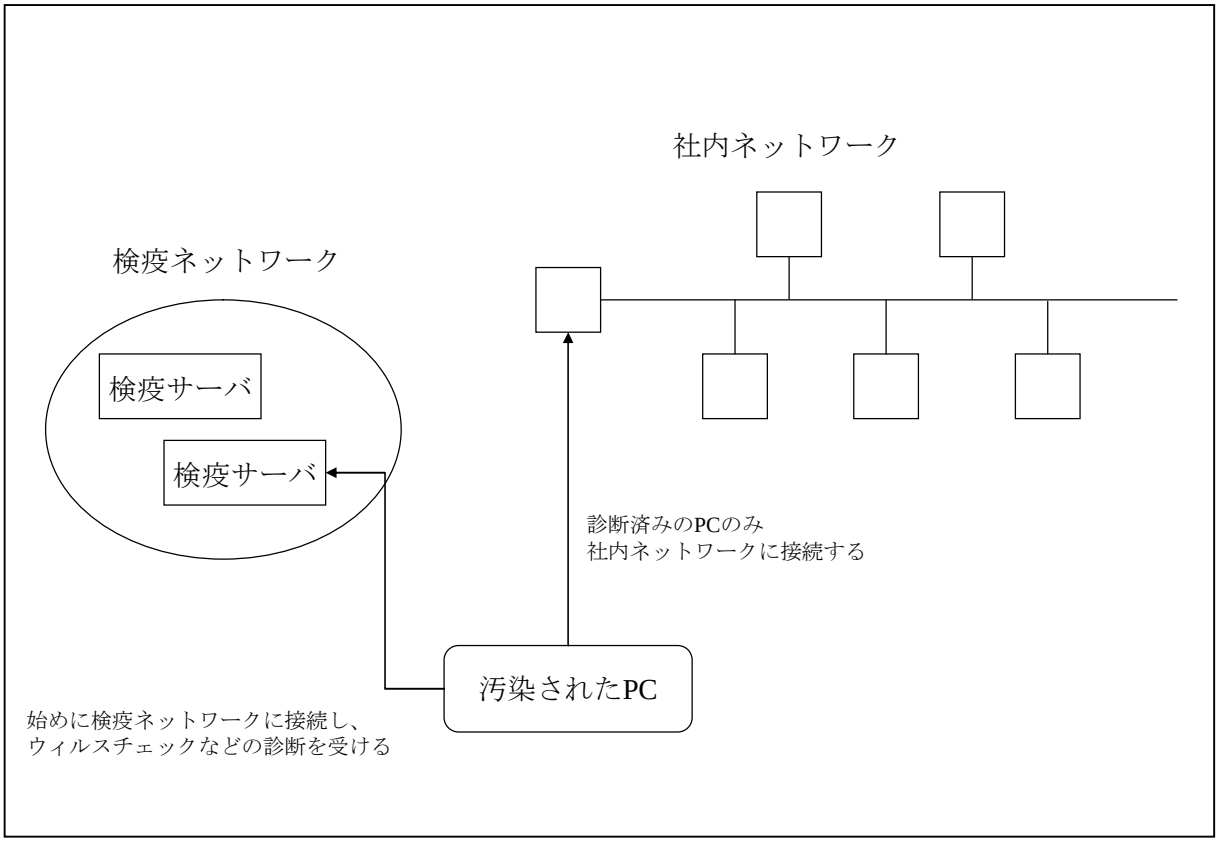

図 II-20-4. 検疫ネットワーク

【解説】

1）モバイル端末に対するセキュリティの考え方

＊ 近年の、ノート型 PC の小型化、Wi-Fi 標準装備端末の普及などにより利便性の高まる反面、モバイル環境でのセキュリティリスクが高まっている。

＊ 企業において最も身近で大きな無線ネットワークによる危険リスクは、モバイル端末を経由した社内 LAN への不正侵入、ウィルスやマルウェアの混入、また経路盗聴による情報流出であろう。

＊ 様々なネットワークへの接続を頻繁に繰り返すモバイル端末の接続を許可する場合には、従来とは違った検査が必要である。他のネットワーク経由で端末の OS やソフトウェアが汚染されている可能性があるからである。

＊ モバイルセキュリティリスクに対する技術的な対策アプローチは数多く提案されており、有効に利用するべきである。同時に利用者のセキュリティに対する意識や知識を高めさせる教育もまた不可欠であることを知っておく必要がある。

2）無線 LAN セキュリティ

＊ 現在流通しているほとんどのノート型 PC は、標準で無線 LAN へ接続することができる。企業 LAN への接続に適切に認証、暗号化が施されていても、PC の設定によっては、PC を踏み台にして LAN に侵入される恐れがある。

＊ 有線の場合と違い、建物構造による物理的なセキュリティは期待できないため、ネットワーク設計者とその利用者は、従来よりもセキュリティを意識する必要がある。

＊ 企業の無線 LAN の場合、利用者が限定されるため、MAC アドレスを予めアクセスポイントに登録し、登録済みの端末からのみ接続を許可する方法が一般的である。この場合も、アクセス制御のみでは経路の暗号化は施されないためこれには別の仕組みが必要である。

＊ Wi-Fi CERTIFIED を名乗るデバイスでは、WPA/WPA2 セキュリティプロトコル実装している。これらは認証と暗号化、メッセージ認証符号を含む。それぞれ Personal と Enterprise があり、認証方法が異なる。Personal は Pre Shared Key を用いて認証を行い、Enterprise は IEEE 802.1x 認証サーバにより認証を行なう。

＊ ネットワークレイヤ 3 より上位のデータの保護には、依然として SSL, SSH, GPG, PGP など、アプリケーションレベルの暗号化機構が有効である。

3）検疫ネットワークとハニーポット

＊ 社内のネットワークへ接続しようとする PC に対して、一旦隔離し、接続した PC の安全性を検査するネットワークのことを検疫ネットワークという。検疫ネットワークの目的は、悪意のある者の侵入を防止することや、PC 内のウィルスやワームがネットワークに侵入することを防ぐことである。

＊ ハニーポットとは、いわば囮である。悪意のある者が本当に重要な情報にアクセスするのを防ぐため、偽の情報で悪意のある者をおびき寄せる仕組みである。ハニーポットには、OS やソフトウェア、サーバをエミュレートするものなど、いくつかの種類が存在する。

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 II	応用
習得ポイント	II-20-5. 侵入検知システム(IDS)の仕組み	
対応する コースウェア	第 12 回 侵入検知システムの仕様と導入	

II-20-5. 侵入検知システム(IDS)の仕組み

ネットワークサーバへの不正アクセスを検知する侵入検知システム、Intrusion Detection System (IDS)の原理、機能と効果、侵入検知を行う必要性について解説する。また IDS が持つ課題として検知ポリシーの問題点や IDS を意識した攻撃への対策について説明する。

【学習の要点】

* 侵入検知システム(IDS)は、ファイアウォールで防ぐことのできない不正プログラムの侵入や行為を発見する仕組みである。
* ファイアウォールは、サービスを行っていない接続ポートに対してのパケット侵入を遮断するものである。サービスを行っているポートへの不正パケットを検出する IDS は、ファイアウォールとは別に必要である。
* 現在の IDS による不正パケット侵入検知のアルゴリズムには精度の問題がある。また、設計によって IDS システムに負荷が集中し、その性能がサービスへ影響することも考えられる。

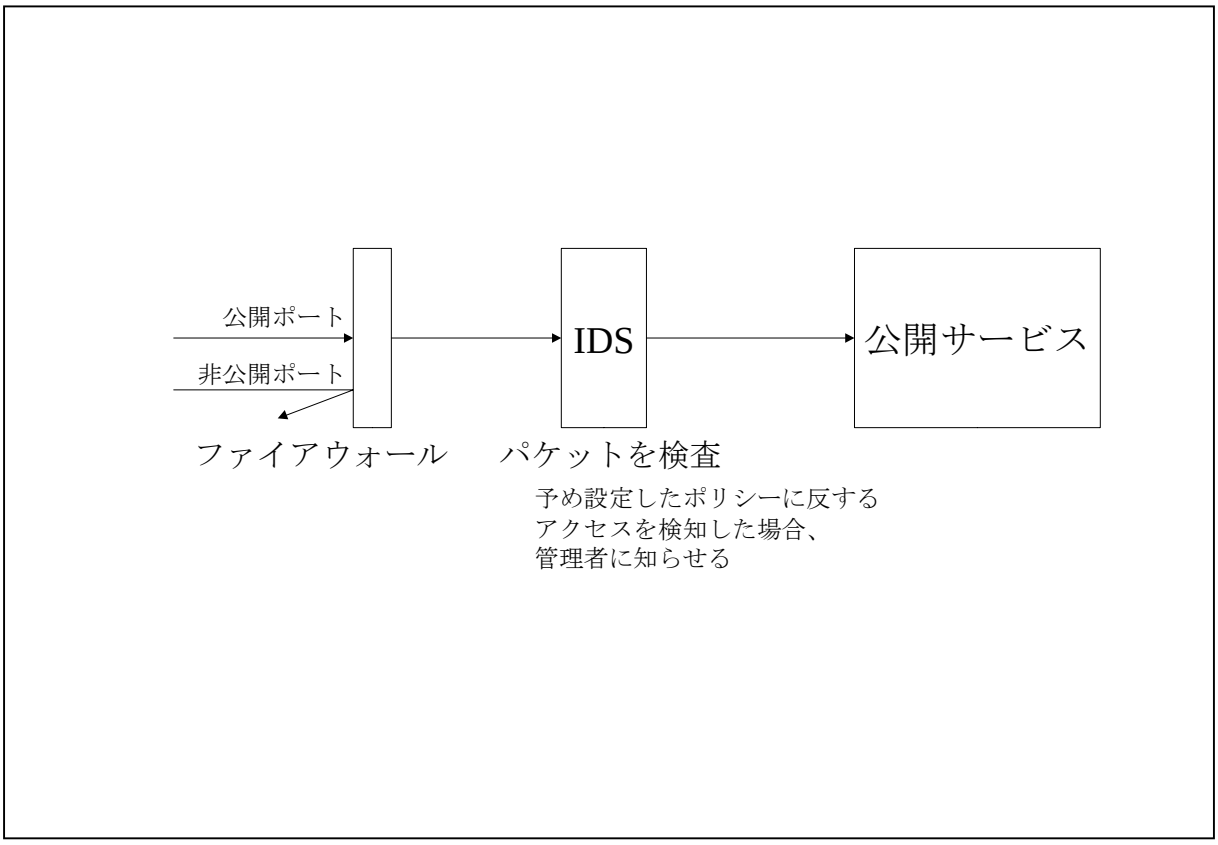

図 II-20-5. ネットワーク型 IDS の例

【解説】

1) 侵入検知システムの原理

＊ 侵入検知システム(IDS)は、インターネットなどを経由して不正にネットワークに侵入しようとする行為を検知するような機構である。

＊ ファイアウォールによる保護とは違い、公開サービスのために解放しているポートを使って不正に侵入されたことを検知することが IDS の目的である。

＊ 侵入検知システムは、侵入行為をブロックすることはしない。侵入行為が検知されると、管理者にメールなどで知らせる。管理者はこれを受けて手動で対応することになる。

＊ ホストへの侵入検知に対する対策の歴史は長い。例えば、定期的に syslog を監視し、内容をメールやその他の方法で外部に保管し、ログをその場でトランケートするといった方法は、単純であるが非常に有効な手段であり、侵入検知に対する考え方として重要である。

2) 侵入検知システムの種類

＊ 侵入を検知するアルゴリズムの観点から、通常作業との比較により異常を検出するもの(anomaly 型)と、予め用意した不正行為パターンへのマッチングを行うもの(signature 型)の 2 種類にわけられる。

＊ ネットワーク型 IDS、ホスト型 IDS という分類を行なうこともある。ネットワーク型はネットワークの境界に設置され、ウィルスの侵入や DoS 攻撃を検知する。ホスト型は、サーバにインストールされるソフトウェアエージェントであり、OS 上での不正な行為を検知する。ファイルの改竄を検知するものもある。

3) 侵入検知システムの性能・精度

＊ IDS の検知は、100%信用できるとは限らない。signature 型でパターンをすべて網羅することは現実的に不可能であるからである。つまり、未知の攻撃には対応できない。また、多くのパターンへのマッチングには多くの計算リソースを消費する。検知アルゴリズムの精度向上や、性能の問題は今後の課題である。

＊ anomaly 型 IDS の誤った検知は、False Positive と False Negative として知られる。前者は問題のないイベントを異常として誤って検知することで、後者は問題のあるイベントを見過ごしてしまうことである。

＊ サーバ運用を行なっていると、悪意のある者からのポートスキャンや、不正ログインの試みは日常茶飯事である。こういったパターン化した攻撃に対しては侵入検知システムは非常に有効である。

＊ 構成方法としては、ファイアウォールと組み合わせるのが一般的である。ファイアウォールによって不正なポートへのパケットを遮断し、ファイアウォールを通過したパケットの中身を IDS によって検査する。

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 II	応用
習得ポイント	II-20-6. IDS の導入と設定方法	
対応する コースウェア	第 13 回 IDS による侵入検知	

II-20-6. IDS の導入と設定方法

代表的な IDS である Snort や Tripwire を例としてその導入や設定方法について説明する。またネットワーク IDS とサーバ IDS といった概念の違いを説明する。さらに検知ルールやアクションの設定と行った実際の運用方法について言及する。

【学習の要点】

* ネットワークベースの IDS は、監視対象ネットワークの境界や DMZ など、すべてのパケットが通過するネットワークの入口に置かれる。
* ホストベースの IDS は、あるホストにインストールされるソフトウェアであることが多い。ホスト内で行われる行為が IDS によって監視されることになる。
* Snort はネットワーク型 IDS、Tripwire はホスト型 IDS として有名である。

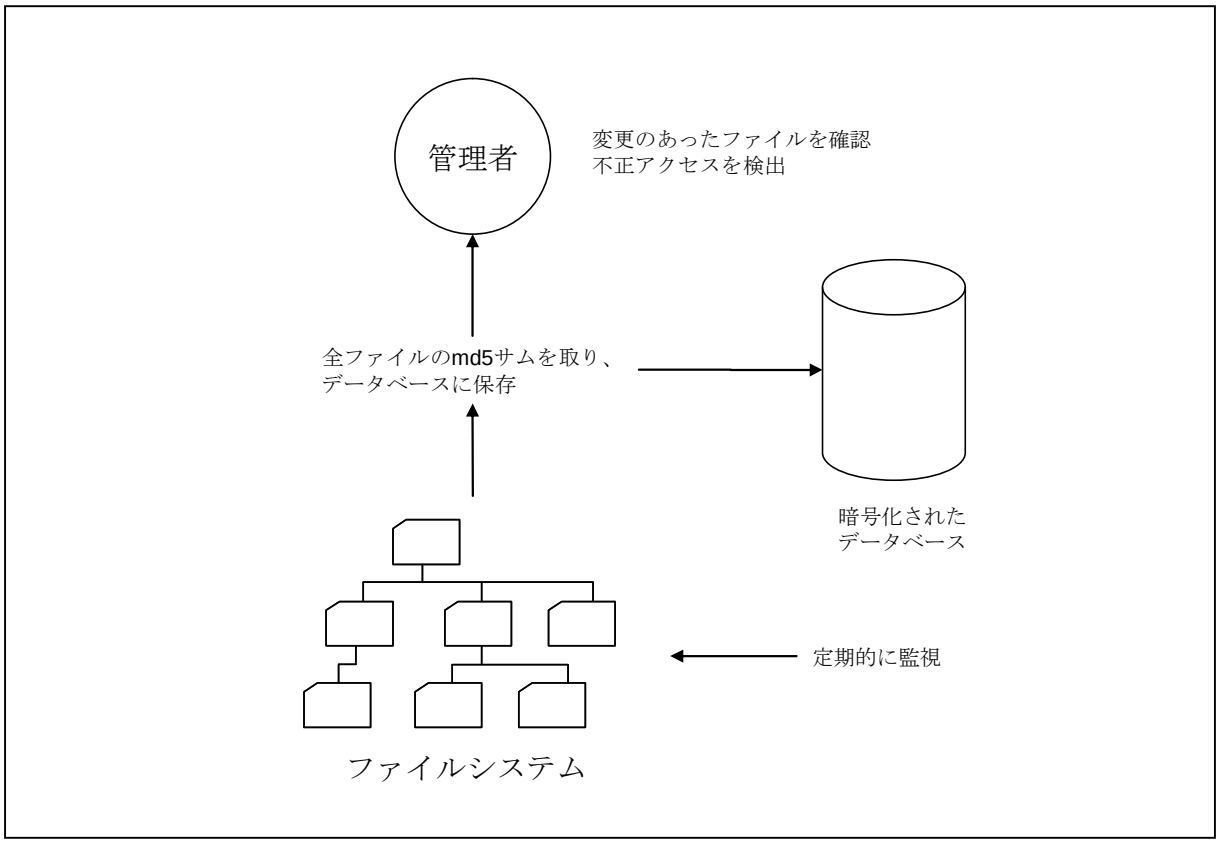

図 II-20-6. Tripwire

【解説】

1) Tripwire

* Tripwire は、ホストにインストールするホスト型 IDS である。Tripwire は商用バージョンもあるが、オープンソースバージョンは特に Open Source Tripwire と呼ばれている。
* Tripwire を用いれば、ホストにあるファイルの改竄を監視することができる。ファイルの MD5 チェックサムを計算し、前回分と比較することによりこれを行なう。
* Tripwire 使用の大まかな流れは以下の通りである。
  - インストール
  - ポリシーファイルの設定(twpol.txt の編集)
  - ポリシーファイルの暗号化
  - データベースの初期化
  - 整合性チェック
  - レポートの作成
* Tripwire に類似したソフトウェアには、AIDE (http://www.cs.tut.fi/~rammer/aide.html) や AFICK (http://afick.sourceforge.net) などがある。

2) Snort

* Snort は、ネットワーク型、signature 型の IDS である。つまり、Snort は不正アクセスのパターンデータベースと照らし合わせて、そのアクセスが不正であるかを判断する。
* Snort の処理の流れは、入ってきたパケットをプリプロセッサによりフィルタリングし、その後に検知エンジンを呼び出す。警告出力用のフィルタの種類も豊富である。
* Snort をインストールしたら、設置場所の決定と、用途に合わせた設定を行なう必要がある。ファイアウォールの外側に置くか、内側に置くかで設定も異なる。
* 設定は、signature とプリプロセッサの決定である。誤った検知を減らすためにこれらは適切に設定しておきたい。また、不要な設定は処理の負荷となるだけでなく、誤った検知を誘発することになるので注意が必要である。

3) 現状の IDS ソフトウェアの問題点

* Tripwire にしても Snort にしても、現状それ自身を保護する仕組みはない。DoS 攻撃などにより、これらのプログラムの効果を無効化されることがないわけではない。
* また、これらのソフトウェアは多くのコンピュータリソースを消費する。特に Snort をファイアウォールの外側に置いた場合、入ってくるすべてのパケットを検査する必要があるため、保護対象のホストやネットワークの提供するサービスに影響が及ぶ場合もあるだろう。

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 II	応用
習得ポイント	II-20-7. IDS によるネットワーク監視の作業手順	
対応する コースウェア	第 13 回 IDS による侵入検知	

II-20-7. IDS によるネットワーク監視の作業手順

IDS を用いたネットワーク監視の作業手順として、セキュリティリスクの検討、セキュリティポリシーの検討、ネットワーク構成への反映、IDS が受信した不正アクセスのブラックリスト化といった具体的な作業手順を説明する。

【学習の要点】

＊ IDS には未だ精度の問題があり、侵入検知が必ず正しいものとは限らない。このため、管理者は IDS からの通知を確認する必要である。また、通知が大量に発生した場合の人員確保、確認体制も整えておく必要がある。

＊ IDS を導入したら、通知ポリシーを決める必要がある。通知ポリシーは組織のセキュリティポリシーに依存する。ポリシーに従って適切にチューニングを行わないと、通知確認がボトルネックとなり、せっかくのシステムが意味を成さなくなる場合がある。

＊ IPS は、管理者に検知内容を通知するのではなく、直ちにそのアクセスを禁止する。管理者が手動で対応する必要がない点が IDS と異なる。

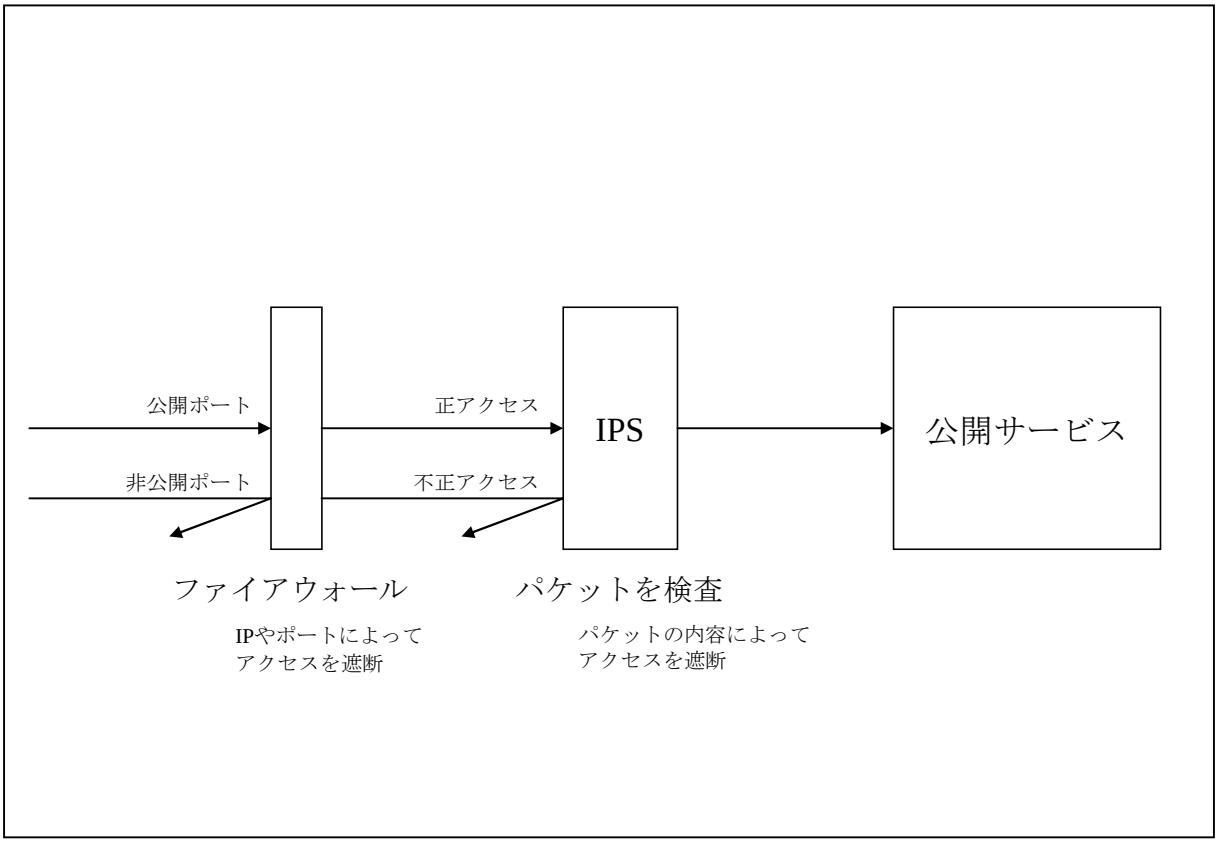

図 II-20-7. IPS 配備の例

【解説】

1) IDS を使った監視

* 侵入を検知することは、IDS を利用することだけではない。実際になぜそれが必要か、既存のものの何を補うために使用するか、セキュリティポリシーに沿っているかなどを考慮するべきであろう。
* syslog を定期的に監視することで侵入の検知ができる場合も多くある。Linux の auditd はそもそも監査目的のデーモンである。このような標準のツールの役割をよく考えた上で IDS を導入するべきであろう。
* syslog や auditd の抱える問題と同様の問題を IDS が含んでいることもある。ツールの選択の際にはその弱点もよく見極める必要がある。

2) IDS を使った監視の体制

* IDS は、侵入を検知するものでありそれを防ぐものではないことをよく知っておく必要がある。不正な侵入を検知したら、IDS は管理者に通知する。管理者はこの通知を受けて手動で対応策を施さなければならない。
* 管理者が IDS の発する通知をすべて確認し、対応するのは現実的ではない場合がある。IDS は適切にチューニングしておかないと、誤った検知により多量の警告を発する。
* 多量の警告の中から、不正アクセスを見つけ適切な対策を行なうことは困難である。意味のある検知を行なうためには適切なフィルタリングを行なわなければならない。
* 運用開始後には事前に設定したポリシーを見直したり、チューニングを適切に行っていくという作業が発生する。

3) IPS

* IPS（Intrusion Prevention System）は、IDS の考え方を発展させたもので、不正アクセスを検知したら、そのアクセスを防止するものである。
* 不正アクセスを検知した場合に、管理者に通知するだけではなく、リアルタイムにアクセスを遮断するところが IDS との違いである。このことで、IDS では管理者が手動で対応しなければならなかった作業を自動的に行なうことができるようになる。
* アクセスを遮断するという観点からは、ファイアウォールと似ているが、ファイアウォールは IP やポートに対して検査が行なわれるのに対して、IPS はパケットの内容を検査する。例えば、多くの IPS ソフトウェアは、HTTP や SMTP といった上位レイヤのプロトコルを理解する。
* IPS も IDS と同様に、主にネットワーク型とホスト型に分けられる。Snort は、IPS としての機能も実装している。
* IPS の導入によって、IDS の持つ問題がすべて解決できるわけでは決して無い。例えば誤った検知や多くのコンピュータリソースを必要とするなど、依然として問題は存在する。

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 II	応用
習得ポイント	II-20-8. ネットワークセキュリティ要件の分析	
対応する コースウェア	第 14 回 ネットワークセキュリティ構築	

II-20-8. ネットワークセキュリティ要件の分析

サーバのセキュリティ要件、クライアントのセキュリティ要件、ネットワークセキュリティ要件といったそれぞれのケースに関して、実際のケースを想定し、具体的なセキュリティの問題と対応策をまとめる。

【学習の要点】

* 重要なリソースを保護するためには、サーバ、クライアント、ネットワークそれぞれが適切なセキュリティ要件を満たしている必要がある。クライアントはセキュリティを確保するのが最も難しく、これによる被害が昨今多く報告されている。
* セキュリティと利便性は背反する二つの概念である。サーバ、クライアント間が接続する場合には、それぞれがデータ保護に対して必要十分な配慮がなされている必要がある。このことは、不要なサービスの徹底排除、適切なテクノロジーによる利便性の確保を大前提とする。

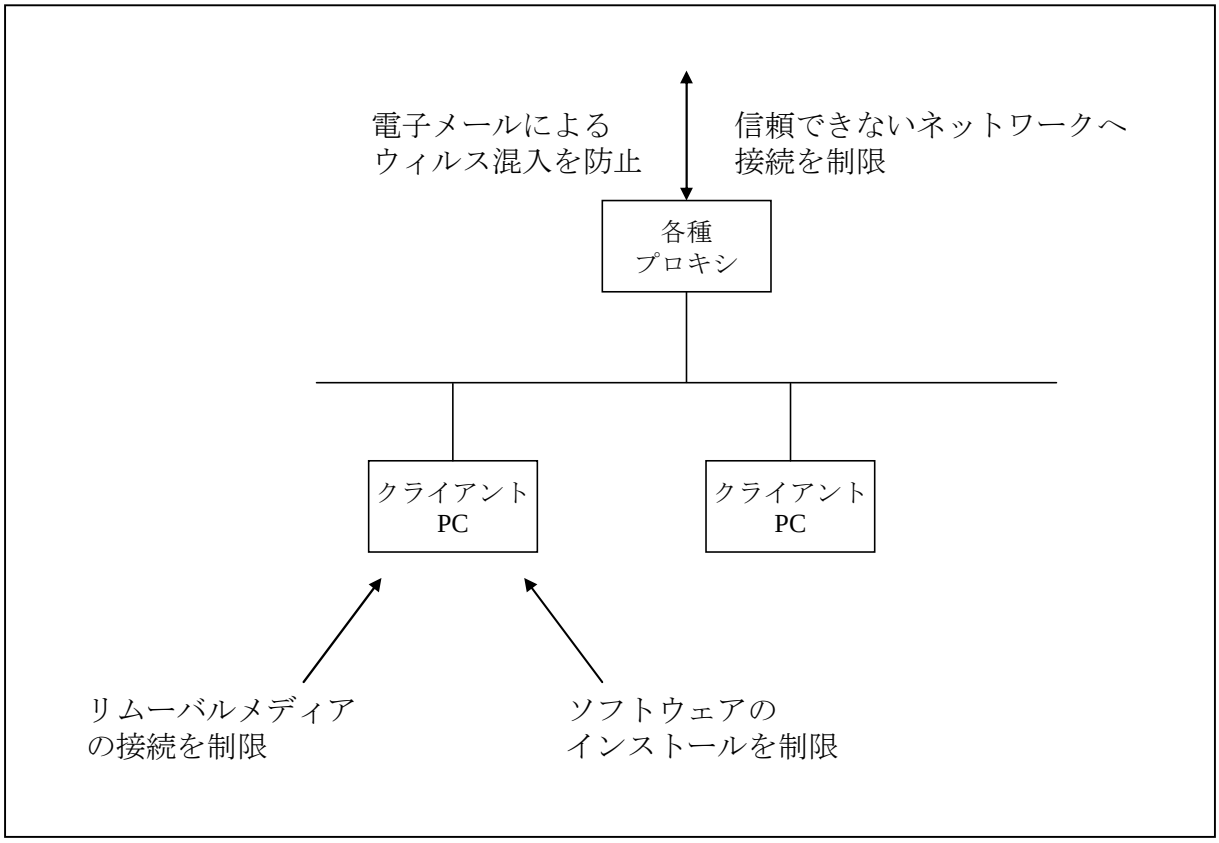

図 II-20-8. クライアントのセキュリティ

【解説】

1) サーバ、ネットワーク、クライアントのセキュリティ

＊ サーバやネットワークのセキュリティについては、II-20-1～7 にて述べた。システム全体のセキュリティは、サーバやネットワークのセキュリティ確保だけでは不十分である。サーバへ接続するクライアントもセキュリティを正しく確保する必要がある。

＊ Web システムにおいては、サーバプログラムの不備によりクライアントが被害を受ける場合が多い（XSS など）。このような場合も、クライアント側で適切なセキュリティ対策をしていれば防ぐことできる。

2) クライアントのセキュリティ対策

＊ サーバの場合と同様に、クライアントの場合も不要なサービスやアプリケーションの存在によって、セキュリティホールを生むことが多い。最近では、企業のクライアント端末に、社員が追加でソフトウェアをインストールできないような対策が施されていることが多くなってきている。

＊ クライアント端末からインターネットへの接続を、ファイアウォールによって遮断するようなセキュリティポリシーが定義されることがある。

＊ ノート PC を社外に持ちだすワークフローを持つ企業では、社員へのセキュリティ対策を徹底する必要がある。自宅のインターネット接続環境からウィルスを無意識に持ち込んでしまうことも多い。

＊ 企業の PC に接続されるリムーバルメディアの取り扱いにも注意する必要がある。ウィルスに感染した実行形式ファイルが混入する恐れは十分にあるからである。USB フラッシュメモリの接続を禁止している企業も多いだろう。

＊ 持ち込んだノート PC を企業のネットワークに接続する前に、検疫ネットワークに一度接続するのも良いアイデアである。

＊ クライアント PC は多くの場合 Windows OS がインストールされている。利用者の多い OS ではウィルスに感染する恐れが多い反面、パターン化されているウィルスなどを検出するには検疫ネットワークやアンチウィルスソフトを利用する効果は高い。

3) セキュリティと利便性

＊ セキュリティと利便性は背反する概念だと考えられることがある。セキュリティを厳しくすればするほど、利用者の利便性は損なわれてしまう。逆に利便性を追求するあまり、セキュリティ意識を低下させることも大きな問題である。

＊ セキュリティと利便性、業務の効率性を十分に考慮したセキュリティポリシーの定義が必要である。

＊ 社員に対するセキュリティ教育、採用する技術とその意義の理解促進は企業のセキュリティを守る上で非常に重要である。

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 II	応用
習得ポイント	II-20-9. DeMilitarized Zone (DMZ)の設計方法	
対応する コースウェア	第 14 回 ネットワークセキュリティ構築	

II-20-9. DeMilitarized Zone (DMZ)の設計方法

インターネットと LAN の間にファイアウォールを設けてセキュリティを確保すると共に、外向きのサービスを集中的に配置して管理する DeMilitarized Zone (DMZ)の設計と構築する。DMZ に配置したサーバを適切に運用するためのフィルタリングルールの設定について解説する。

【学習の要点】

* DeMilitarized Zone (DMZ)は、サービスをインターネットのような組織外のネットワークに対して公開するために設置されたサブネットワークである。
* DMZ は、社内ネットワークの全面に配備されるため、これを守る意味もある。たとえ、DMZ が攻撃されても、社内ネットワークはダメージを受けないように設計される必要がある。
* Web サーバ、メールサーバ、DNS サーバなどは、DMZ に配備される主たるサービスである。

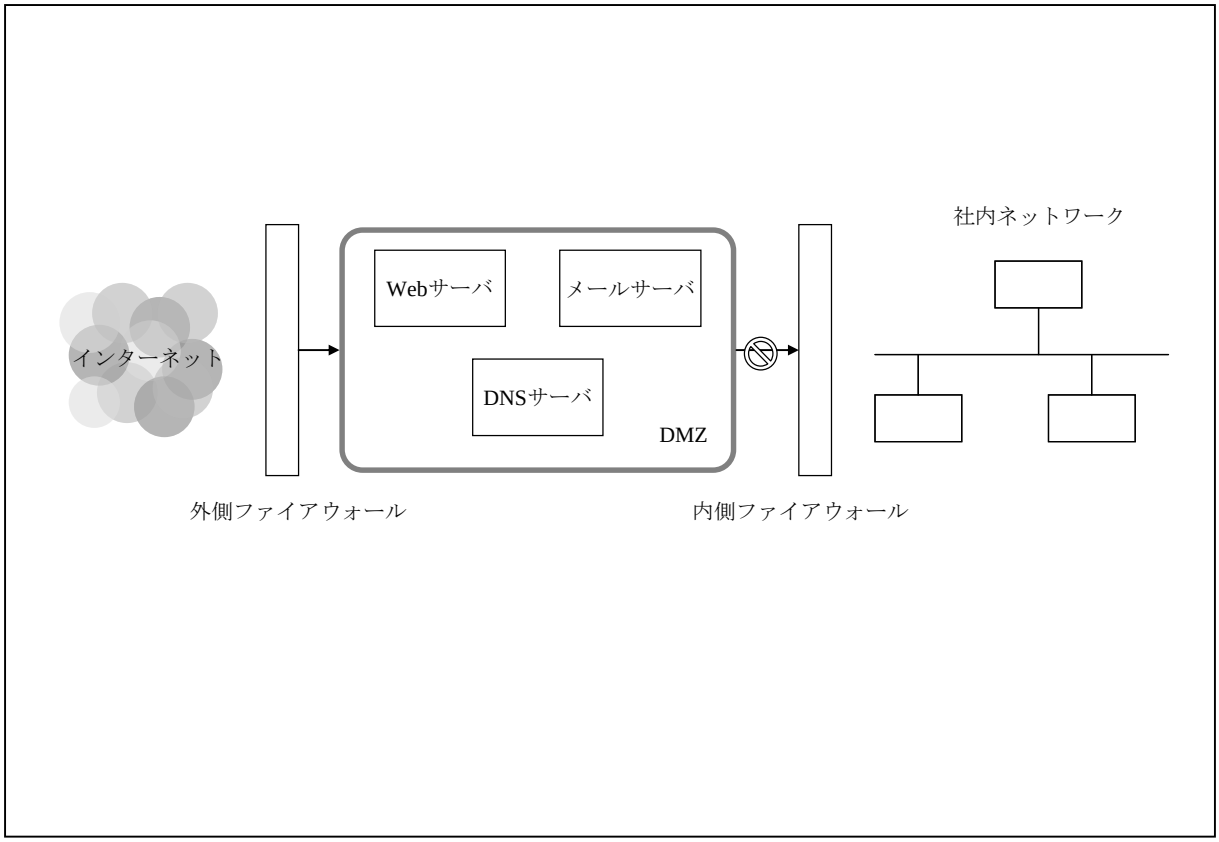

図 II-20-9. DMZ

【解説】

1) ネットワーク境界の保護

＊ LAN と WAN を接続するネットワークの境界では、不正な侵入を防ぐために強固なセキュリティによって保護する必要がある。一般的に次の仕組みが使用される。

- ファイアウォール
- DMZ (DeMilitarized Zone) の設置
- IPS (Intrusion Prevention System)

＊ セキュリティポリシーによって、上記の仕組みはしばしば組み合わされたり省略される場合がある。

2) ファイアウォールと DMZ

＊ ファイアウォールは、IP アドレスやポートによってパケットのフィルタリングを行なう技術である。

＊ DMZ とは、LAN と WAN の間に置かれるサブネットワークのことで、メールサーバやウェブサーバなど、外部にサービスを行なう公開サーバが設置されることが多い。

＊ DMZ に置かれるサービスには、外部ネットワークから接続することができる。多くの場合、DMZ の前面にはファイアウォールが設置され、不要なパケットはファイアウォールにより破棄される。また、ファイアウォールから DMZ への接続には、NAT (PAT) が掛けられることが多い。

＊ 内部ネットワークからも DMZ にアクセスすることが可能である。これは内部ネットワークに接続している管理者の端末から、DMZ 上のホストをメンテナンスするのに便利である。

＊ しかしながら、DMZ からは内部ネットワークへの接続は禁止する。このことにより、万が一ファイアウォールを突破して DMZ に不正に侵入された場合でも、被害が内部ネットワークに及ぶことを阻止する。

＊ DMZ を前後二つのファイアウォールによって保護するアーキテクチャもある。異なるベンダのファイアウォールを採用することで、不正な侵入をより困難にすることができる。

3) 具体的な構成方法

＊ ファイアウォールや DMZ(あるいは IPS)を構成するには、それぞれの機能をもった別々のデバイスを用意するか、またはそれほど大きくないネットワークである場合は、中規模用ルータを用意すればこれらの機能をすべて 1 台でまかなうことが可能である。

＊ 限定的であるが、一部パケットの内部を理解し、動的にアクセス制御を行なうことのできるルータ製品もある。

＊ Linux を用いてソフトウェアでこれらを実装することも可能である。このような場合は複数の NIC を用意し、カーネルの netfilter や Snort を用いて実現することができる。

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 II	応用
習得ポイント	II-20-10. モバイル環境のセキュリティ	
対応する コースウェア	第 15 回 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	

II-20-10. モバイル環境のセキュリティ

モバイルコンピューティングの活用について論じ、そのリスクについて解説する。リモートアクセスのリスク、不正アクセスの問題と対処方法、認証サーバの利用やワンタイムパスワードの仕組みと利用方法などを説明する。

【学習の要点】

* モバイル端末の普及により、外部ネットワークから組織内ネットワークへの接続できる必要性が出てきた。リモートから組織ネットワークへの接続時にセキュリティを担保する技術として、各種 VPN が広く利用されている。
* モバイル端末が、公衆無線 LAN などを使用して重要なデータのやり取りを行う際には、通信経路やデータの暗号化が徹底されている必要がある。VPN，SSL，SSH による暗号化を利用して、利便性との釣り合いを考慮する。
* パスワードの漏洩による不正アクセスを防ぐにあたって、ワンタイムパスワードを利用することが多い。

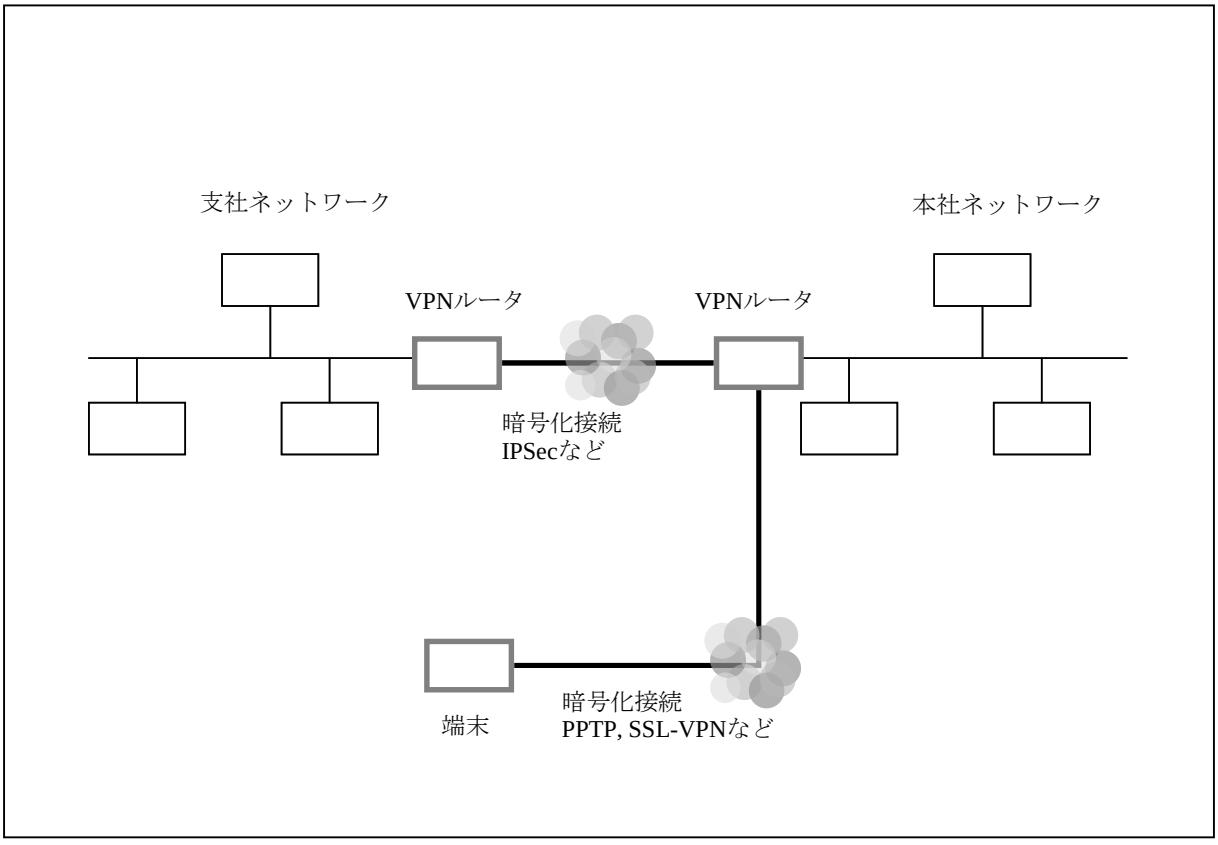

図 II-20-10. 典型的なインターネット VPN 接続の例

【解説】

1) モバイルアクセスのリスク

＊ ノート PC を利用する局面が増えてくると、それに伴ってセキュリティリスクが高まってくる。もっとも危険な要因は、利用者のセキュリティ意識の低さと知識不足である。

＊ モバイルアクセスが多用されるようになってくると、このような危険因子は従来以上にクリティカルである。他のネットワークの接続形態を知らないまま接続し、その後社内のネットワークへ接続することが、この上なく危険な行為であることを知らない利用者は多い。

＊ 技術的な問題で解決できない部分は、利用者に喚起するしかないことを知っておく必要がある。

2) モバイルアクセスのリスクを軽減させる技術

＊ 外部から社内のネットワークへ接続する場合は、VPN が用いられることが多い。よく利用される VPN 技術は、ネットワークレイヤ 3 を暗号化する。

- PPTP は、リモートアクセス VPN を実現する技術であるが、Windows や Mac OS X といったクライアント OS で始めから利用することができる。
- IPSec は、拠点間を接続するためによく利用される VPN 技術である。Cisco や Yamaha のルータ間で、互いに暗号経路を構築することができる。

＊ より高レイヤの VPN 技術には、例えば SSH や SSL を利用したものがある。

- SSH は Linux などの OS ではほぼ標準でインストールされており、アプリケーションレイヤで動作する。各種 TCP/UDP パケットを容易にトンネリングさせることができる。
- SSL-VPN は、SSL を利用して汎用 VPN を構築する技術である。ほとんどのブラウザやメールクライアントは SSL に対応しているため、これらのソフトウェアの暗号接続を通して任意のパケットをトンネリングすることにより暗号経路を確立する。

＊ ワンタイムパスワード

- 上記 VPN 接続と組み合わせて、ワンタイムパスワードが用いられることがある。ワンタイムパスワードは、認証に必要なパスワードを固定的なものではなく、時間とともに変化するものを使用する。利用者は配付されるトークンに表示されるワンタイムパスワードと暗証番号を入力して認証を受ける。
- VPN の暗号経路確立時の認証に、ワンタイムパスワードを利用することがある。ワンタイムパスワードは、時間とともに変化するため、万が一パスワードが破られた場合でも、次のパスワード変化の時刻が来ると同時に無効となるため、被害の拡大を抑えることができる。