21. OS セキュリティに関する知識 II

1. 科目の概要

OS のセキュリティを確保するために必要な機能や対策方法を、Linux サーバを題材として解説する。電子メールのセキュリティ対策として個別の MTA ソフトウェア設定を説明し、Web サーバのセキュリティ対策としてサーバ設定や CGI スクリプトでセキュリティを保つ方法を説明する。さらに FTP サーバの設定や進入検知について解説する。

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-21-1. 電子メールのセキュリティ対策	電子メールを配送するMail Transfer Agent (MTA)サーバの運用時に実施すべきセキュリティ対策について解説する。SMTPを取り扱う際のセキュリティ要件を示し、迷惑メール対策やその他のセキュリティ対策手法を紹介する。	9
II-21-2. SendmailとPostfixの設定におけるセキュリティ項目	代表的なMTAソフトウェアであるSendmailとPostfixのセキュリティ項目を解説する。Sendmailの長所短所を示し、Sendmailの入手と導入、設定の手順を示す。さらにセキュリティを確保したSendmailの運用方法を示す。同様にPostfixの導入と設定、運用方法を示す。	9
II-21-3. Webサーバのセキュリティ対策	Webサーバのセキュリティ対策について概説する。Webの抱えるセキュリティに関する問題と対策を示し、各種報告される脆弱性情報に対してどのようなタイミングで対策を講じるべきか、またWebサーバのセキュリティ対策に関する原則について解説する。	10
II-21-4. Apacheの設定におけるセキュリティ項目	代表的なWebサーバのソフトウェアであるApacheウェブサーバのセキュリティ項目を解説する。Apacheの入手と導入、Apacheが利用するファイルの構成、設定の手順を示す。さらにセキュリティを確保したApacheの運用・設定方法を示す。	10
II-21-5. CGIスクリプトにおけるセキュリティ対策	サーバにおける動的コンテンツを実現するServer-Side Includes (SSI)やCommon Gateway Interface (CGI)の仕組みを簡単に説明し、ファイルの取り扱いやデータベースへのアクセスなど、CGIスクリプトの取り扱いで留意すべきセキュリティ対策の項目について解説する。	10,11
II-21-6. Webサーバのセキュリティ機能	認証機能、アクセスコントロール、セッション管理とクッキーの利用、ファイルアップロードの設定など、Webサーバが持つ機能でセキュリティ管理に関係する機能について説明する。またSOAPやWebサービスといった新しい形態でセキュリティをどう保つか、攻撃の検知と回避をどうするかといった話題も言及する。	11
II-21-7. FTPサーバのセキュリティ対策	ファイル転送サービス(FTPサービス)の提供で設定すべきセキュリティ要件について解説する。FTPセキュリティの原則を論じ、匿名FTP利用時の留意事項や、FTP over SSL/TLS (FTPS)、Secure FTP (SFTP)やSecure Copy (SCP)などFTP以外のファイル共有方法の検討について説明する。	12
II-21-8. FTPサーバの設定におけるセキュリティ項目	パーミッションの設定方法や、FTPでファイル書き込みを防止する方法、welcome.msgの利用やアクセス制御、ftp.usersやftp.hostsといった各種の設定方法について解説し、FTPサーバをセキュアに保つ具体的な手順を説明する。	12
II-21-9. Linuxにおけるシステムログ管理の実際	システムログを管理するsyslogの仕組みや機能、導入と運営管理の方法について解説する。またloggerを使ったシステムログのテストや、swatchを用いたログ管理の自動化方法、これらツールの導入と設定方法などについて説明する。	13
II-21-10. 侵入検知の仕組みと運用方法	サーバに対する侵入検知の必要性と、侵入検知ツールの仕組みや方法を解説する。具体的にはホスト型進入検知ツールのTripwireと、ネットワーク型進入検知ツールのSnortについて、それらの導入方法と設定方法、これらのツールを使った進入検知手順などを紹介する。	14

【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

「21. OS 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
21. OSセキュリティに関するスキル	<OSのセキュリティ機能>	<Linuxサーバのローカルセキュリティ対策>	<Linuxのネットワークセキュリティ対策>	<Linuxによるファイアウォール構築>	<Linuxのサーバセキュリティ設定>	<安全なリモートアクセス>	<SSLによるサーバVPNとCA>	<ドメインネームサービスのセキュリティ対策>	<電子メールのセキュリティ対策>	<Webのセキュリティ対策(1)>	<Webのセキュリティ対策(2)>	<ファイルサービスのセキュリティ対策>	<システムログの管理>	<Linuxによる侵入検知の手法>	<サーバのセキュリティ監査と設定の自動化>

[シラバス：http://www.ipa.go.jp/software/open/ossc/download/Model_Curriculum_05_21.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	IT-IAS2. 情報セキュリティの仕組み（対策）	IT-IAS3. 運用上の問題 [21-15]	IT-IAS4. ポリシー	IT-IAS5. 攻撃	IT-IAS6. 情報セキュリティ分野 [21-10]	IT-IAS7. フォレンジック（情報証拠） [21-2]	IT-IAS8. 情報の依怙	IT-IAS9. 情報セキュリティサービス [21-2]	IT-IAS10. 脅威分析モデル	IT-IAS11. 脆弱性		
	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	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 [21-11]	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 [21-8] [21-10, 11]	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 [21-15]	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. ソフトウェアの標準化	
	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 [21-1, 3, 4]	IT-NET5. アプリケーション分野	IT-NET6. ネットワーク管理							
	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	CE-NWK5. データのセキュリティと整合性 [21-3, 4, 7]	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 [21-4]	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 [21-1]	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 [21-1]		
コンピュータアーキテクチャ	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	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、Web サーバ、メールサーバ、FTP サーバの OSS をセキュアにする方法がある。また、ログ管理や IDS の実践的な運用について習得する。

科目名	第9回	第10回	第11回	第12回	第13回	第14回	第15回
21.OS セキュリティに関する知識Ⅱ	(1)MTA と SMTP セキュリティ	(1)Web サーバのセキュリティ	(1)CGI スクリプトのセキュリティ対策	(1)FTP のセキュリティ	(1)syslog	(1)Tripwire	(1)サーバのセキュリティ監査方針
	(2)Sendmail のセキュリティ	(2)Apache のセキュリティ構築	(2)Web サーバのセキュリティ応用機能	(2)FTP サーバのセキュリティ設定内容と手	(2)swatch を用いたログ監視の自動化	(2)Snort	(2)監査ツール
	(3)Postfix						(3)ログの設定、運用、監視

（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	21　OS セキュリティに関する知識 II II	応用
習得ポイント	II-21-1. 電子メールのセキュリティ対策	
対応する コースウェア	第 9 回 電子メールのセキュリティ対策	

II-21-1. 電子メールのセキュリティ対策

電子メールを配送する Mail Transfer Agent (MTA)サーバの運用時に実施すべきセキュリティ対策について解説する。SMTP を取り扱う際のセキュリティ要件を示し、迷惑メール対策やその他のセキュリティ対策手法を紹介する。

【学習の要点】

* 電子メールシステムのセキュリティ対策においては主に、スパムメール、フィッシングメール、ウィルスメールの排除が要件となる。
* MTA の見地から電子メールのセキュリティを確保するための大前提は、不特定多数や信用できないクライアントからのリレーを拒否することである。
* フィッシングにおいては、送信者が身元を詐称できないような仕組みが望まれる。Sender ID や Domain Keys は、この仕組みを提供する技術としてよく知られている。

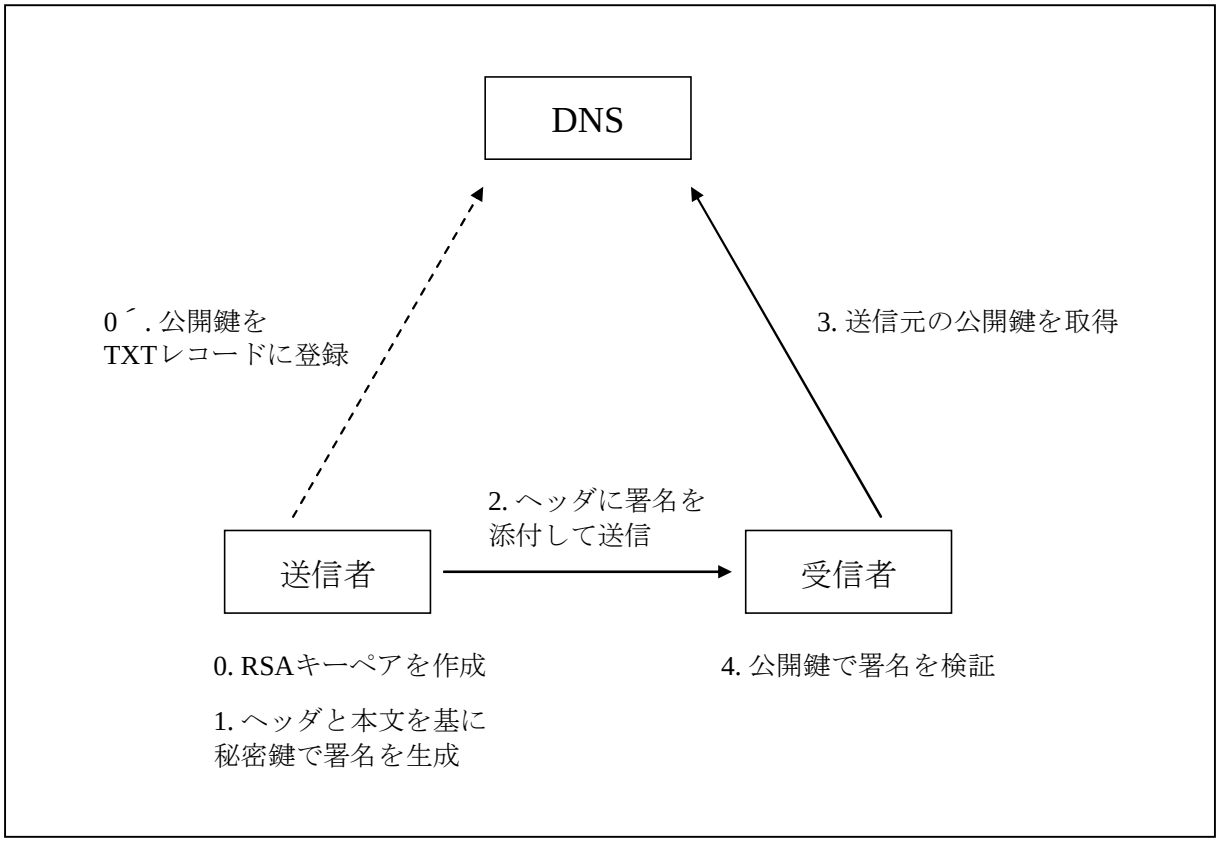

図 II-21-1.　DomainKeys の仕組み

【解説】

1) 電子メールのセキュリティ

＊ 電子メールサービスを提供するにあたって留意するセキュリティ要件は主に、以下のような迷惑行為に対する防止である。

- MTA の不正利用
- 送信元アドレスを偽装したメール（フィッシングメール）
- 迷惑メール（スパムメール）
- ウィルスを含むメール

＊ メールサーバは通常インターネットからアクセスできる必要があるため、DMZ に配置される。

2) 不特定多数のリレーの防止

＊ 企業のドメイン内でメールサービスを運用する場合、関係のない部外者がメールサービスを使用することを禁止する必要がある。

＊ MTA は、設定によっては不特定多数のメールをリレーすることを許可することができる。通常こういった設定は不適当であるため、以下のような制限を設ける。

- ドメイン内からのリレー要求のみを許可
- ドメイン内の送信元メールアドレスを持つメールのみリレーを許可
- 明示的に指定した信頼できる IP からのリレー要求のみ許可

＊ ノート PC やモバイル端末を使用して、インターネットを経由して企業のメールサーバへのリレー要求を必要とする場合、POP before SMTP や SMTP-AUTH といった認証メカニズムが使用されることが多い。

3) フィッシング／スパムメールの防止

＊ 近年、送信元メールアドレスを偽装したメールによるフィッシングやスパムメールの被害が拡大している。

＊ メールアドレスの偽装を防ぐために考案された技術して、Sender ID や DomainKeys がある。Sender ID はマイクロソフト社の運用する Hotmail で採用されている。また DomainKeys はヤフー社の提供する Yahoo! Mail にて採用されている。

＊ Sender ID は、メールの送信元 IP アドレスと、DNS 上に設けられた TXT (SPF) レコードから返される IP アドレスを比較し、照合することで送信元を検証する。

＊ DomainKeys は、送信時に RSA 秘密鍵を用いてヘッダと本文を基に署名を生成し、メールのヘッダに署名をする。公開鍵は予め DNS に登録しておく。受信時に DNS から取得した公開鍵で署名を検証する。

4) スパムメール、ウィルスメールの防止

＊ スパムメールやウィルスメールを検査する仕組みは、サーバ側、クライアント側で動作する多くの実装が存在する。Google 社の Gmail を始めとする Web ベースのメールサービスではスパムフィルタを利用者全員で共有できる仕組みを提供する。

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	21　OS セキュリティに関する知識 II II	応用
習得ポイント	II-21-2. Sendmail と Postfix の設定におけるセキュリティ項目	
対応する コースウェア	第 9 回 電子メールのセキュリティ対策	

II-21-2. Sendmail と Postfix の設定におけるセキュリティ項目

代表的な MTA ソフトウェアである Sendmail と Postfix のセキュリティ項目を解説する。Sendmail の長所短所を示し、Sendmail の入手と導入、設定の手順を示す。さらにセキュリティを確保した Sendmail の運用方法を示す。同様に Postfix の導入と設定、運用方法を示す。

【学習の要点】

* Red Hat 系の Linux OS（例えば CentOS）では、OS をインストールすると同時に Sendmail もインストールされる。
* Sendmail はデフォルトでは、自ドメイン内からしかメールが送信できないよう、リレーに制限がかかっている。
* Sendmail では、メールリレーのポリシーを選択することができる。スパムメールを防ぐという意味でも、適切なリレーポリシーの決定とアクセス許可リストの設定、メールアドレスによるフィルタリングの設定等を行った上で運用することが望まれる。
* Sendmail 以外にも代替となる MTA が存在し、要件にあわせて選定する。

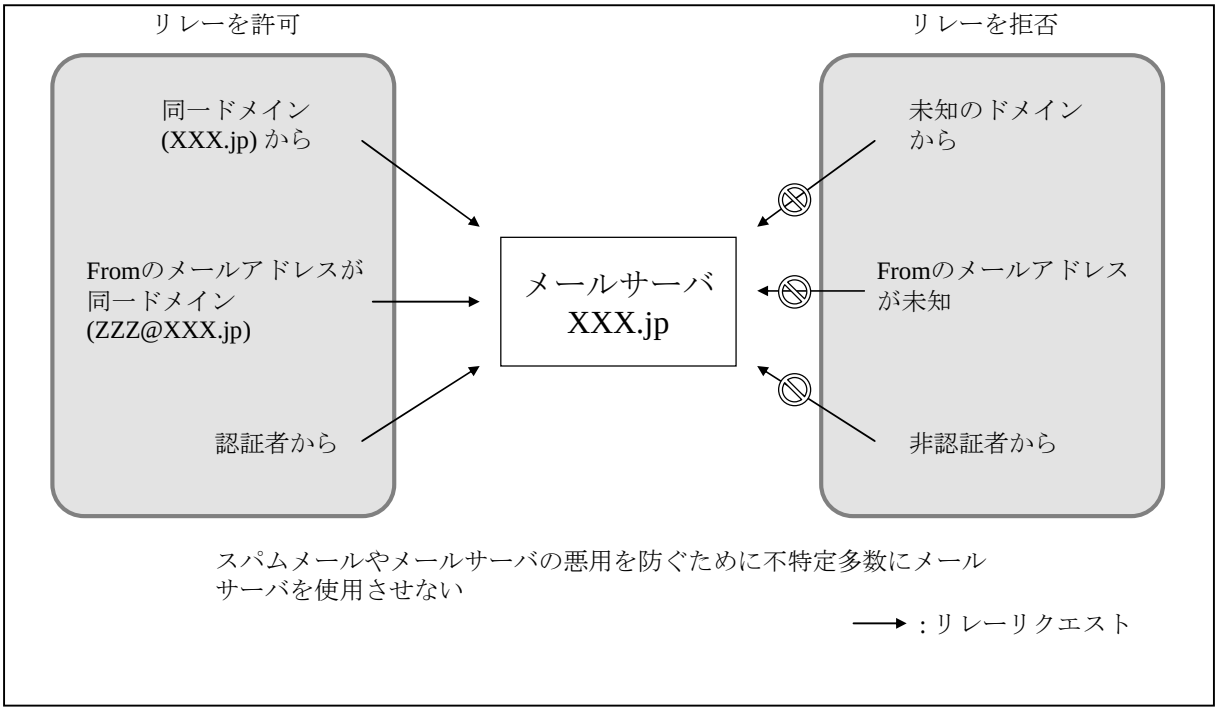

図 II-21-2.　代表的な MTA の比較

【解説】

1) Sendmail

* Sendmail は、歴史のある MTA であり、多くのプロトコルに対応しており、柔軟な設定項目を持つ。
* Sendmailの設定ファイルは、現実的には設定を手作業で設定することは難しい。管理者はm4と呼ばれるマクロ言語などを使って設定ファイルを編集することになる。
* 設定ファイルが難解であることで、動作の見通しを悪くするという意見がある。Sendmail に限らず、設定ミスによるセキュリティホールは少なくない。

2) Sendmail の代替 MTA の存在

* Postfix を始めとする Sendmail の後継を唱う MTA は、Sendmail の設定の難解さを解消しようとしている。これによって動作の見通しをよくし、設定ミスによるセキュリティホールを最小化する効果がある。
* 設定の容易さや方法、ポリシーなど、それぞれの MTA によって特徴がある。管理者のスキルや経験に合わせて適切なソフトウェアを選択することが望まれる。

3) Sendmail の導入

* Sendmail は Red Hat 系の Linux ではデフォルトでインストールされる。既に起動さえしている場合があるので ps コマンドなどで確認してみるとよい。
* インストールされていない場合は、rpm コマンドなどを使用して簡単にインストールすることができる。
* Sendmail の動作は、設定ファイル sendmail.cf によって制御する。sendmail.cf が複雑であることが Sendmail が難しいと言われる所以である。通常は、Sendmail に付属する cf ツールを使用して sendmail.cf を作成することになる。
  - まず、m4 マクロを使用して mc ファイルを作成し、これを m4 コマンドで展開することで sendmail.cf を生成する。
  - 管理者は mc ファイルと関連するいくつかの設定ファイルを編集することで、MTA デーモンの設定やリレー許可の設定、アクセス制限などを行うことになる。
  - mc ファイルから sendmail.cf を生成するには、以下のコマンドを実行する。

    m4 cf.m4 sendmail.mc > sendmail.cf

4) Sendmail の主なリレー設定項目

* FEATURE(`promiscuous_relay')…すべてのリレーを許可
* FEATURE(`relay_entire_domain')…送信先や送信元をドメイン内のリレーに限定
* FEATURE(`relay_hosts_only')…設定ファイルで許可したホストはリレーを許可
* FEATURE(`relay_based_on_MX')…送信先のドメインパートの MX レコードにホスト自身が含まれていれば許可
* FEATURE(`relay_local_from')…送信先アドレスがホストと同じ場合許可

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	21　OS セキュリティに関する知識 II II	応用
習得ポイント	II-21-3. Web サーバのセキュリティ対策	
対応する コースウェア	第 10 回 Web のセキュリティ対策①	

II-21-3. Web サーバのセキュリティ対策

Web サーバのセキュリティ対策について概説する。Web の抱えるセキュリティに関する問題と対策を示し、各種報告される脆弱性情報に対してどのようなタイミングで対策を講じるべきか、また Web サーバのセキュリティ対策に関する原則について解説する。

【学習の要点】

* Web サーバに関連する脆弱性は、Web サーバ自体に起因するものと、その上で動くアプリケーションに起因するものに分けられる。今日では、アプリケーションの脆弱性は、Web サーバ自体に起因するそれよりも深刻であることが多い。
* Web サーバ自体に潜む脆弱性を回避するには、Web サーバ自体にパッチを当てる必要があるので、有事にはサービスに支障を来すことがある。このようなことから、Web サーバはセキュリティの観点から十分実績のあるものを選ぶ必要がある。
* Web サイトが危険にさらされるケースとして、ユーザが入力できる部分に起因する場合が多い。Web アプリケーションからローカルファイルシステムにアクセスする場合など、Web サーバの実行ユーザとファイルを所有するユーザを分けるなどの対策は定石である。

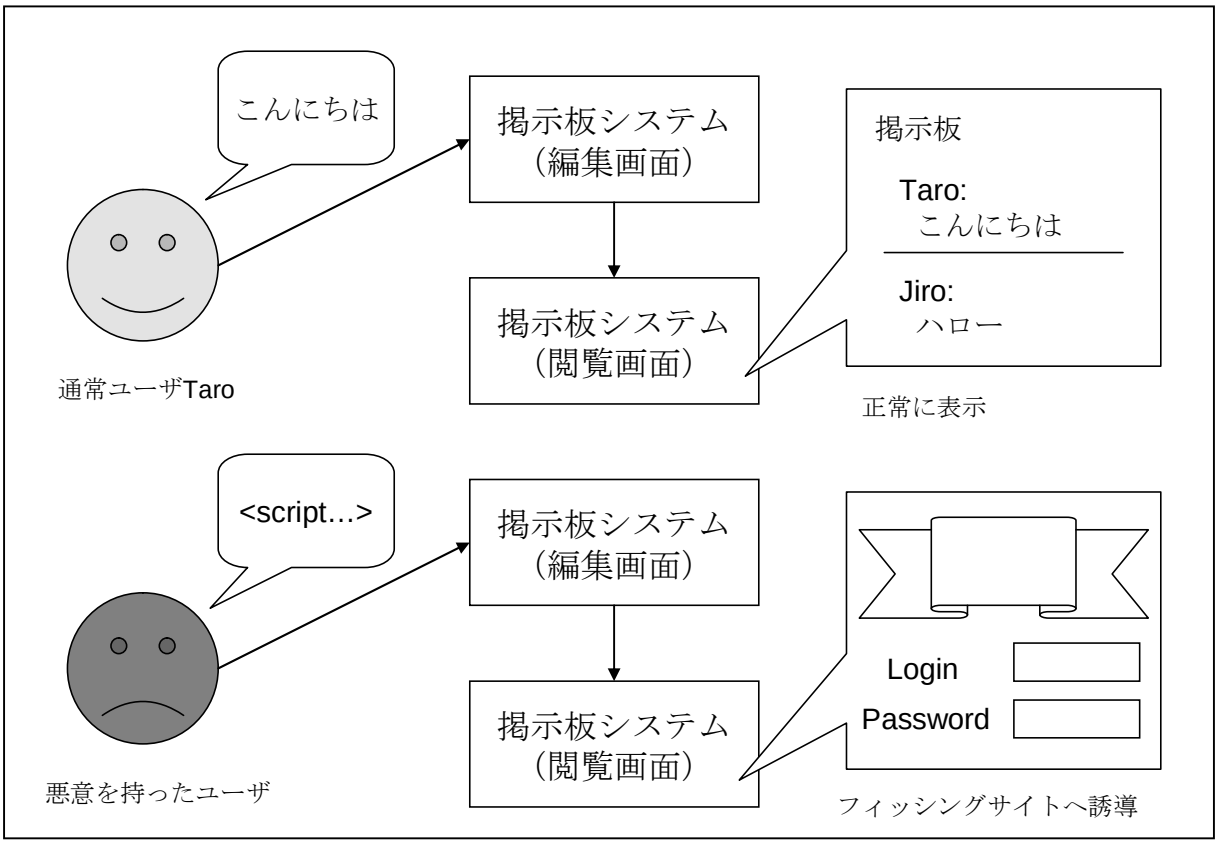

図 II-21-3.　XSS を用いたフィッシングの例

【解説】

1) Web のセキュリティ

＊ Web システムを運用する上で留意すべきセキュリティ要件はいくつかの側面から考えることができる。

- Web サーバは、それ自身がバグを含んでいる場合、セキュリティホールとなる可能性がある。この問題への対応は、できるだけバグの少ない（と思われる）枯れた Web サーバを使用することと、定期的に報告されたセキュリティホールを引き起こすバグに対するパッチを当てることである。
- Web サーバは、任意の CGI スクリプトや SSI スクリプトを実行することができる。これらのスクリプトがセキュアでない場合は、セキュリティホールとなることがある。これらのスクリプトを実行する必要がないのであれば、これらの機能を無効にしておくべきである。
- Web サイトは、インターネットに公開されるため、ネットワーク的なセキュリティも考慮する必要がある。通常 Web サイトをホストするサーバは DMZ におかれ、社内ネットワークへの侵入を禁止する。
- Web サイトの性格上、ユーザ情報を入力する必要がある場合、SSL によって通信経路を暗号化する方法が取られる。同様に認証が必要なサイトでは、プレーンなパスワードがネットワーク経路を流れないような対策を取る。
- Web サイト上で動作するアクティブスクリプト（ActiveX や Java アプレットなど）を悪用したクラッキングが横行している。クライアント PC にウィルスやワームが侵入したり、XSS（Cross Site Scripting）などの被害をもたらす。必要に応じてこれらのスクリプトの実行を禁止することも考える必要がある。

2) Web サーバのセキュリティリスク

＊ Web サーバにバグが潜んでいたり、間違った設定をそのままにして置くことで、以下のような攻撃を受ける可能性が考えられる。

- 機密情報が漏洩する
- ホストに侵入され、システムを改竄または破壊される
- DoS 攻撃を仕掛けられ、システムを使用不可にされる

＊ Web サーバは、複雑で多くの機能を有している。利便性のためこれらの機能は提供されているが、有効にする機能が多ければ多い程セキュリティホールとなりうる箇所は増える。

＊ デバッグのために有効にしている機能をそのままにしてしまうことは避けるべきである。基本的な項目として以下の点を確認すべきである。

- サーバルート以下のディレクトリツリーは適切な所有者とパーミッションが設定されているか。
- サービスに不要な機能を有効にしていないか。ディレクトリリスティングや SSI など。
- サーバを root で起動していないか。

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	21　OS セキュリティに関する知識 II II	応用
習得ポイント	II-21-4. Apache の設定におけるセキュリティ項目	
対応する コースウェア	第 10 回 Web のセキュリティ対策①	

II-21-4. Apache の設定におけるセキュリティ項目

代表的な Web サーバのソフトウェアである Apache ウェブサーバのセキュリティ項目を解説する。Apache の入手と導入、Apache が利用するファイルの構成、設定の手順を示す。さらにセキュリティを確保した Apache の運用・設定方法を示す。

【学習の要点】

* 一般的に Apache HTTP Server のインスタンスは、ドキュメントルートディレクトリ、サーバインスタンス設定ファイル、ログファイル、プロセス ID ファイルで構成される。これらのファイルの置き場所、所有者やパーミッションを適切に設定しておくのはセキュリティの基本である。
* Apache のワーカープロセスは root ユーザにするべきではない。これは、サーバが乗っ取られた際に、システムに対する攻撃を最小限に抑えるためである。
* ディレクトリアクセス制御（Allow, Deny）を常に正しく設定するべきである。また CGI や SSI が不要な場合は、これらの機能を組み込まないか、実行不可に設定しておくべきである。

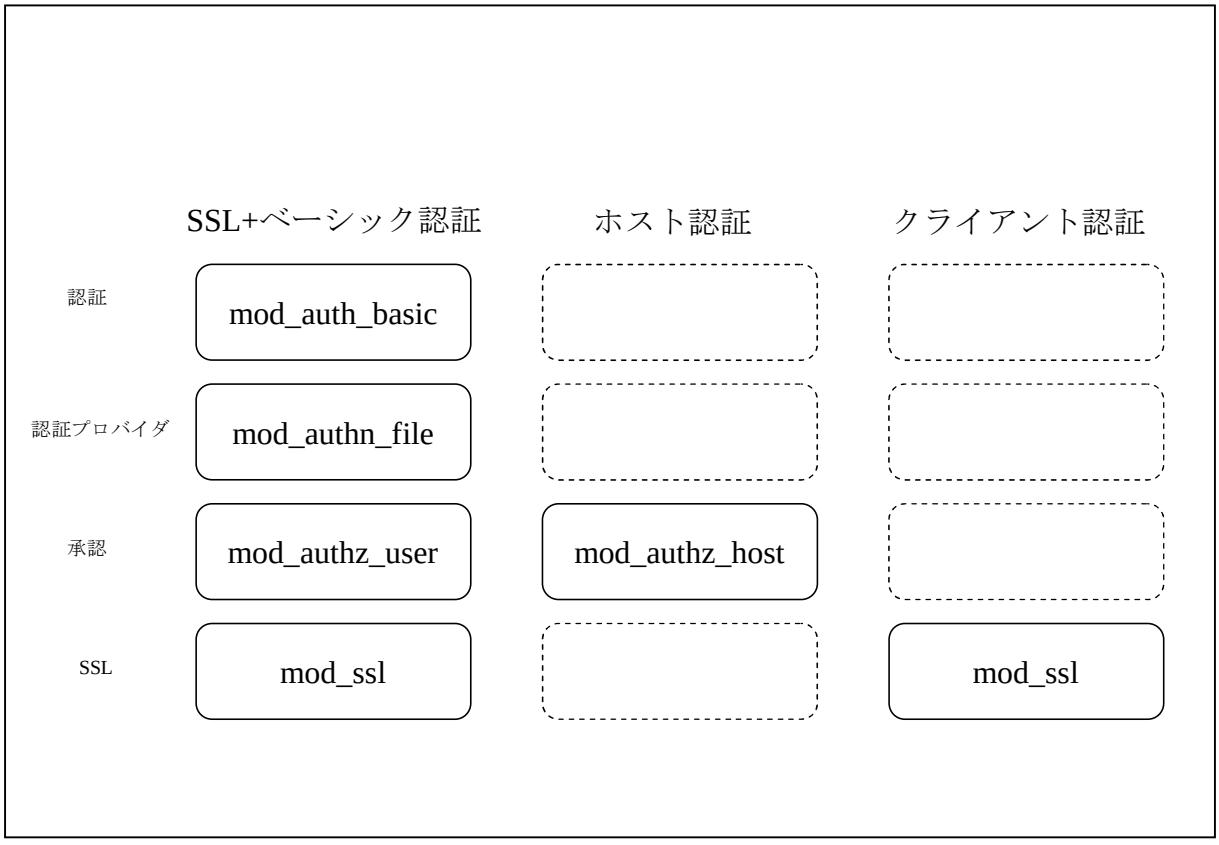

図 II-21-4.　よく使われる認証形式と関連するモジュール

【解説】

1) セキュリティ保護関連の Apache モジュール

＊ Apache のコア以外の機能はモジュールとして提供されるが、HTTP のベーシック認証やダイジェスト認証用のモジュールは、Apache のディストリビューションと一緒に配付され、最初から利用可能な場合が多い。

- mod_auth_basic
  ベーシック認証を行なうモジュール。照合対象のデータベースは別途モジュールとして提供される。例えば mod_authn_dbm は、DBM 形式のファイルに格納されるプリンシパルに対して認証を行なう。
- mod_auth_digest
  ダイジェスト認証を行なうモジュール。mod_auth_basic と同様、照合対象のデータベースは別途モジュールとして提供される。

＊ SSL (Secure Socke Layer) は、https での通信を実現する。Apache では、mod_ssl を導入することができる。mod_ssl は OpenSSL ライブラリを利用する。

＊ SSL を導入することで、サーバ認証、クライアント認証、通信経路の暗号化を実現することができる。SSL とベーシック認証を組み合わせることで、安全な暗号経路を用いた認証機構を比較的簡単に実現することができる。

＊ クライアント認証は、公開鍵認証を実現する。ベーシック認証やダイジェスト認証でのパスワードを用いた認証と比べてよりセキュアであると考えられる。

2) セキュリティ保護関連の Apache ディレクティブ

＊ Apache のモジュールは、機能を設定ファイル上で有効にするための追加的なディレクティブを定義する。

- AuthType
  認証のタイプを指定する。mod_auth_basic や mod_auth_digest を組み込むことでそれぞれ、basic, digest が指定可能となる。
- AuthName
  認証ドメイン(レルム)の名前を指定する。
- Require
  認証済みユーザに対して承認メカニズムを定義する。通常はユーザやグループを指定する。追加的な承認モジュールを追加することで指定項目は拡張することができる。
- AuthBasicProvider
  ベーシック認証の照合対象のデータベースを指定する。mod_authn_ldap や mod_authn_dbd はそれぞれ、LDAP、リレーショナルデータベースに対して認証を行なうことを可能にする。
- Allow, Deny
  ホストベースのアクセス制御を行なう。特定のホスト名や IP アドレスからのアクセスを許可したり禁止したりする。

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	21　OS セキュリティに関する知識 II II	応用
習得ポイント	II-21-5. CGI スクリプトにおけるセキュリティ対策	
対応する コースウェア	第 10 回 Web のセキュリティ対策① 第 11 回 Web のセキュリティ対策②	

II-21-5. CGI スクリプトにおけるセキュリティ対策

サーバにおける動的コンテンツを実現する Server Side Includes (SSI)や Common Gateway Interface (CGI)の仕組みを簡単に説明し、ファイルの取り扱いやデータベースへのアクセスなど、CGI スクリプトの取り扱いで留意すべきセキュリティ対策の項目について解説する。

【学習の要点】

＊ CGI スクリプトはホストで動作する任意のプログラムである。適切なセキュリティ制限の設けられていないシステム上では、CGI スクリプトの作者に悪意があれば、システムを破壊することもできることを念頭において導入する必要がある。

＊ SSI もまた CGI と同様、システムに対して影響を与えかねない強い権限を持つプログラムである。SSI を必要としないシステムではこれをオフにしておくことが賢明である。

＊ CGI スクリプトの受け取る入力値は常にサニティチェックが行われるべきである。特にユーザの入力値をもとに、リレーショナルデータベースに SQL を使ってアクセスするような CGI スクリプトは、確実に入力値をサニタイズすることが要求される。

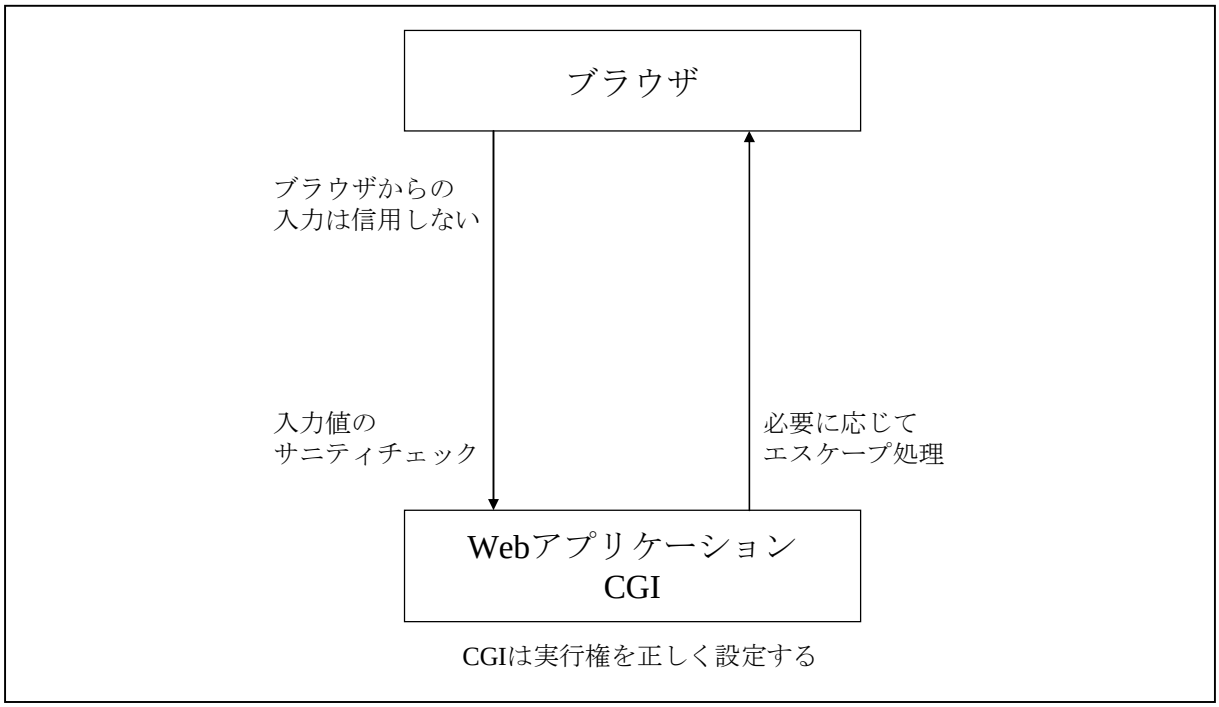

図 II-21-5.　CGI の動作原理

【解説】

1) CGI スクリプトと SSI

* CGI（Common Gateway Interface）は、Web サイトからプログラムを呼び出す標準的なインタフェースである。呼び出されるプログラムは、OS のシェルで実行できる任意のコマンドであればよい。CGI を呼び出す Web サーバは、環境変数とプログラム引数をセットして該当プログラムを呼び出す。
* SSI（Server Side Include）は、HTMLドキュメントに挿入されたSSIコマンドを実行する仕組みである。SSIエンジンの解釈するコマンドはいくつかあり、ファイルの最終更新日時を出力したりOSの任意のコマンドを実行したりすることができる。

2) CGI スクリプトの危険性

* 仮に Web サーバ自身にセキュリティホールが存在していなくても、CGI スクリプトが追加的にセキュリティホールを生成することがある。
* CGI スクリプトのセキュリティの確保には、経験と専門的な知識が必要とされるが、CGI スクリプトの作者がこれを満たしていることは多くない。
* CGI スクリプトが取得するリクエストパラメータの値は慎重に検査されるべきである。これを怠ると、OSコマンドインジェクション、SQL インジェクション、XSS などの攻撃に対して非常に脆弱になる。

3) CGI スクリプトの取り扱い

* CGI スクリプトは、サーバのドキュメントルートではなく、cgi-bin ディレクトリを作り、そこに入れることが推奨されている。例えば、サーバ上にある CGI ファイルを直接エディタで編集しようとするとき、エディタがスワップファイルを作ることがあるが、このようなファイルが予期せずドキュメントルートに公開されないようにするためである。
* シェルコマンドを呼び出す場合は、その必要性を十分に検討するべきである。C 言語を使用している場合は、コマンドを呼び出すよりも、ライブラリの API を呼び出すべきである。その方が効率が良い場合が多い。Perl や PHP を使用している場合は、十分に入力文字列の検査をしてからコマンドを組み立てるよう留意する。可能であれば言語の外部拡張機能を利用して API 化することも検討する。
* とりわけ C 言語を用いて CGI スクリプトを作成する場合、バッファオーバーフローに十分に注意する必要がある。ユーザの入力する文字列を十分な検査なしに不用意に固定長のバッファに割り当てることは避けられるべきである。
* CGI スクリプトは、デフォルトの状態では Web サーバのユーザで実行される。Apache の suEXEC は、CGI スクリプトの実行ユーザを他のユーザ（と適切なパーミッション）に切り替えることを可能にする。

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	21　OS セキュリティに関する知識 II II	応用
習得ポイント	II-21-6. Web サーバのセキュリティ機能	
対応する コースウェア	第 11 回 Web のセキュリティ対策②	

II-21-6. Web サーバのセキュリティ機能

認証機能、アクセスコントロール、セッション管理とクッキーの利用、ファイルアップロードの設定など、Web サーバが持つ機能でセキュリティ管理に関係する機能について説明する。また SOAP や Web サービスといった新しい形態でセキュリティをどう保つか、攻撃の検知と回避をどうするかといった話題も言及する。

【学習の要点】

* 一般に Web サーバは、様々なレベルでコンテンツを保護するためにセキュリティ機構を備えている。認証・承認は、Web サーバに必要とされるよく知られたセキュリティの基本項目である。
* 接続ユーザや接続元 IP によってアクセスを制御（アクセスコントロールリストを作成）することもしばしばである。
* SSL は、通信経路の暗号化、サーバ認証、クライアント認証の機能を提供する。これは、今日の Web サーバの運用では必要不可欠な機構である。

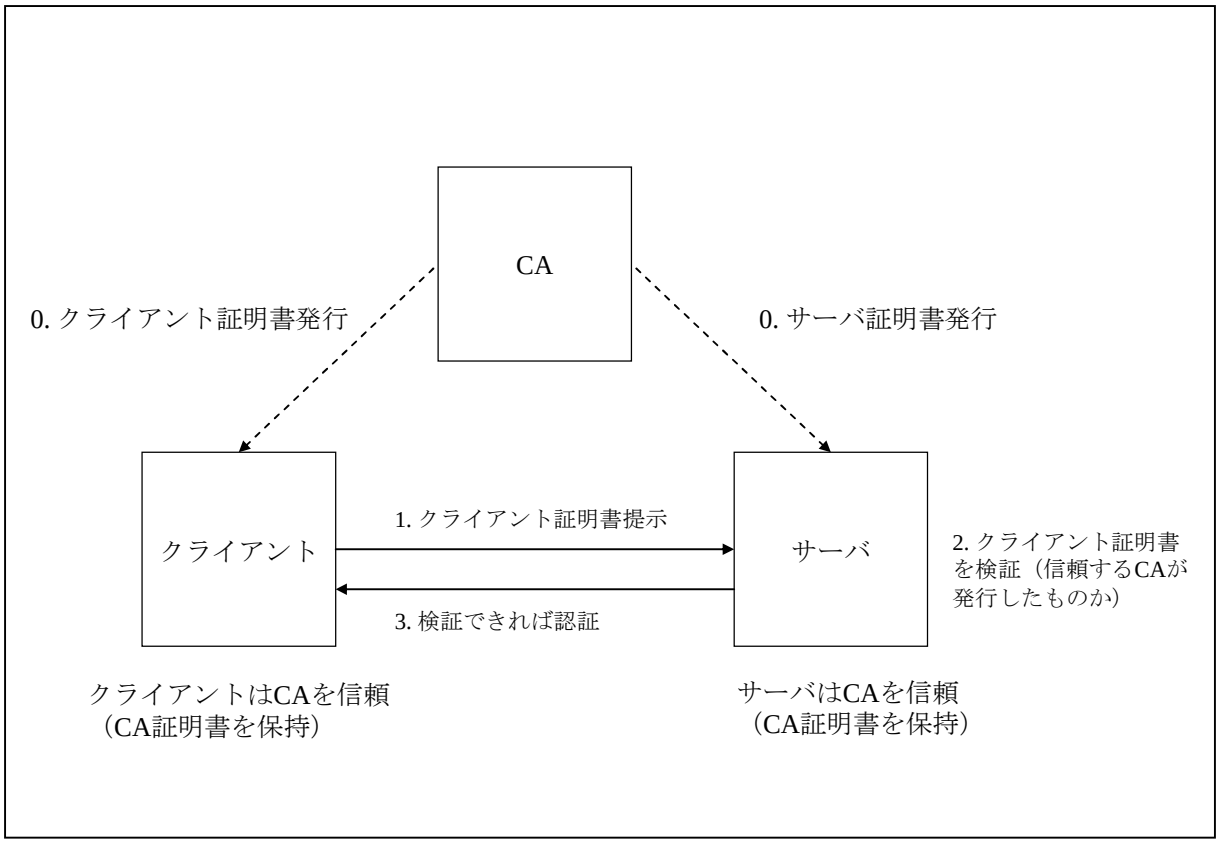

図 II-21-6.　クライアント認証の仕組み

【解説】

1) 認証

＊ Web サイトにあるコンテンツを保護するための最も一般的な方法はユーザ認証である。ユーザ認証は、訪れたユーザがそのコンテンツにアクセスする権限をもっているかどうかを検証する仕組みである。

＊ ユーザ名（ログイン ID）とパスワードの組み合わせが、予めサーバに登録されたものと等しいかどうかで検証を行なう方法が最も一般的である。よりセキュアな方法として、公開鍵認証を行なう場合もある。

＊ ベーシック認証とダイジェスト認証は、HTTP/1.1 の仕様にて定義されており、多くの Web サーバは、Web アプリケーションにこういった認証機構を簡単に紐付けることができる。社内システムや簡易認証として用いられることが多い。

＊ 独自の HTML フォームとクッキーを使用して、認証を行なう方法は最も一般的なインターネットサイトで使用されている認証方法である。パスワードが通信経路で盗聴されないように、SSL を組み合わせて使用する。

＊ SSL クライアント認証は、X.509 証明書（秘密鍵）を保持するクライアントからのみアクセスを許可するような公開鍵認証方式である。同時に通信経路暗号化も行われる。

2) アクセスコントロール

＊ 特定の IP から接続を遮断したりする機能は、ファイアウォールや OS レベルで行なうことができるが、Web サーバ自体も、IP によるアクセス制御を行なうことができる。

＊ Apache では、Allow, Deny, Limit ディレクティブを使用してアクセス制御を行なうことができる。Satisfy ディレクティブを用いることで、ホストベースのアクセス制御と、ユーザ認証を組み合わせて使用することができる。

3) WS-Security

＊ WS-Security は、SOAP メッセージを拡張し、エンドツーエンドのセキュリティを保証する機構である。SOAP Web サービスで使用することができる。

＊ WS-Security は、認証（Security Token）、メッセージ完全性（Message Integrity）、メッセージ暗号化（Message Confidentiality）を SOAP メッセージ交換において実現する方法を定義する。

＊ WS-Security の Security Token は、具体的な認証方式を定義しない。ひとつ以上の任意の認証技術を使用することができる（例えば、Kerberos 認証、X.509 認証など）。これらの認証で使用するバイナリトークンのエンコード方式は、WS-Security によって規定されている。

＊ 完全性や暗号化を実現する技術は、それぞれ XML Signature、XML Encryption を SOAP メッセージに統合したものである。

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	21　OS セキュリティに関する知識 II II	応用
習得ポイント	II-21-7. FTP サーバのセキュリティ対策	
対応する コースウェア	第 12 回 ファイルサービスのセキュリティ対策	

II-21-7. FTP サーバのセキュリティ対策

ファイル転送サービス(FTP サービス)の提供で設定すべきセキュリティ要件について解説する。FTP セキュリティの原則を論じ、匿名 FTP 利用時の留意事項や、FTP over SSL/TLS (FTPS)、Secure FTP (SFTP)や Secure Copy (SCP)など FTP 以外のファイル共有方法の検討について説明する。

【学習の要点】

＊ FTP を多数のユーザにサービスする場合には、運用方針によって許可しない限り、互いのユーザのコンテンツが不用意に見えてはいけない。柔軟性の裏には、常に適切な設定を施す必要があることは忘れてはならない。

＊ FTP 仕様にはユーザ認証が含まれているが、ネットワーク上を流れるパスワードは暗号化されない。通信経路を暗号化するためには、クライアント側もそれに対応しなければならない。

＊ 今日の FTP クライアントの中には、FTPS, SFTP, SCP に対応しているものがある。これらのプロトコルは通信経路を暗号化する仕様が含まれているため、可能であれば FTP に代わってこれらのプロトコルを使用することが望まれる。

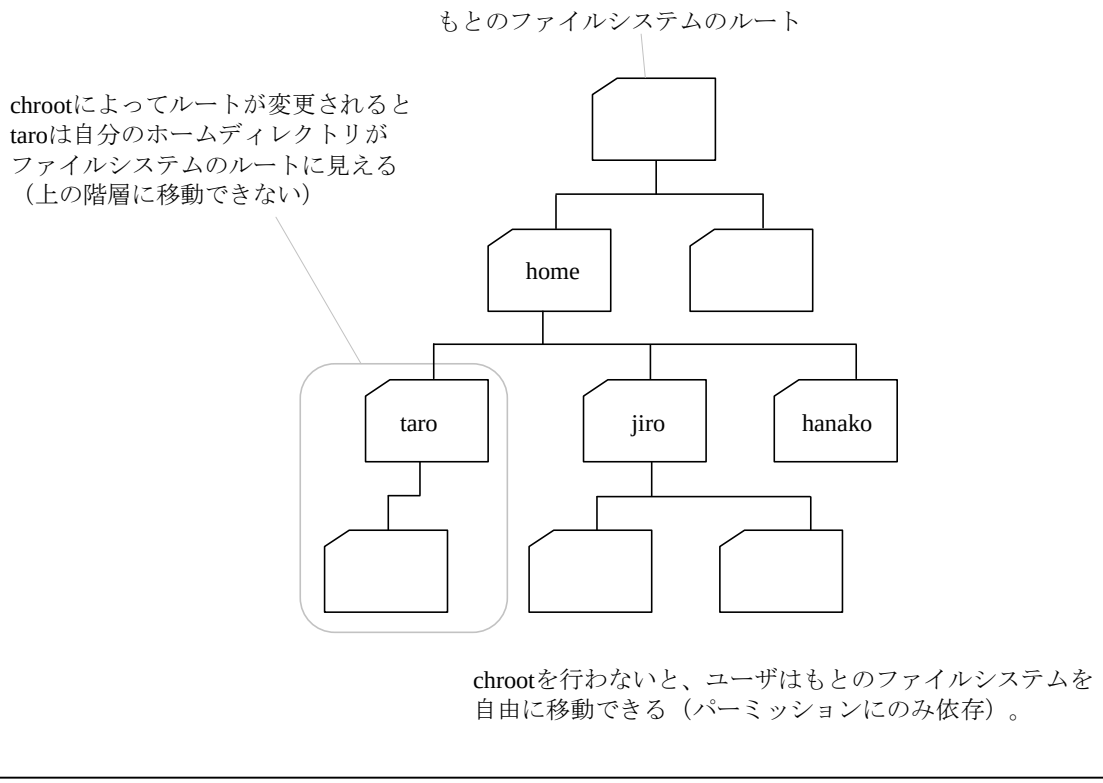

図 II-21-7.　chroot の効果

【解説】

1) FTP の潜在的なセキュリティリスク

＊ FTP プロトコルには、通信経路を暗号化する方法がない。このため、経路を流れるパケットを容易に盗聴することができる。転送されいているファイルの内容や、認証の際のユーザ名、パスワードもこれに含まれる。

＊ SCP（Secure Copy）、SFTP（SSH File Transfer Protocol、または Seucure File Transfer Protocol）や、FTPS（FTP over SSL）は、通信経路を暗号化するために仕様が含まれる。FTP の持つ潜在的なセキュリティリスクを回避するために、これらのプロトコルを代替として使用することが望まれる。

2) FTP サーバの設定上の留意事項

＊ FTP プロトコルは、その性格上、常にファイルシステムの公開に対するリスクが存在する。適切なセキュリティが施されている場合は問題とならないが、そうでない場合には、システムの重要なファイルにアクセスされる恐れがある。

＊ 匿名ユーザとは、パスワードなしでログインできるユーザである。パブリックな FTP サイトでは使用されることがあるが、必要でない場合は匿名ユーザを有効にするべきではない。FTP サーバの実装の中には、デフォルトで匿名ユーザが有効になっているものがあるので留意する必要がある。

＊ FTP サーバでは、ログインしたユーザが自分のホームディレクトリより上位のディレクトリにアクセスできないよう、chroot を使用する。chroot は、設定によっては無効にすることができるため、実運用を考えている FTP サーバでは必ずこの項目を確認することが必要である。

＊ 多くの FTP サーバの実装では、OS のユーザをそのまま FTP のユーザとして使用する。この場合は、ログインを許可するユーザとしないユーザを設定できるので、実運用前に確認するべきでる。もし root ユーザやシステム上権限の強いユーザが許可ユーザリストに含まれている場合はその必要性を再検討する。

3) SFTP

＊ SFTP は、OpenSSH に含まれており、多くの Linux ディストリビューションでは利用できる状態になっている。OpenSSH の SFTP 実装は、SSH により通信経路を暗号化する。

＊ OpenSSH の SFTP 実装は、認証に SSH を利用するので、SSH 公開鍵認証をそのまま使用することができる。

＊ SFTP は、FTP における経路の暗号化問題を解決するが、それ以外のすべての問題を解決するわけではない。例えば、OpenSSH の SFTP 実装では、FTP のように簡単に chroot を利用できない。

＊ FTP に比べてクライアントが普及してないことも導入上の問題である。FTP は多くの OS でデフォルトで備えている機能であるが、SFTP の場合は専用のクライアントソフトウェアが必要となる。

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	21　OS セキュリティに関する知識 II II	応用
習得ポイント	II-21-8. FTP サーバの設定におけるセキュリティ項目	
対応する コースウェア	第 12 回 ファイルサービスのセキュリティ対策	

II-21-8. FTP サーバの設定におけるセキュリティ項目

パーミッションの設定方法や、FTP でファイル書き込みを防止する方法、welcome.msg の利用やアクセス制御、ftp.users や ftp.hosts といった各種の設定方法について解説し、FTP サーバをセキュアに保つ具体的な手順を説明する。

【学習の要点】

* vsftpd は、セキュリティを重視した FTP サーバデーモンであり、いくつかの Linux ではデフォルトの FTP デーモンとなっている。
* vsftpd は、chroot、IPv6、SSL/TLS をサポートする。また、inetd や xinetd の下で動かすことも、単独で動かすこともできる。
* 匿名ユーザの設定、chroot の設定、ACL の設定は、FTP サーバを使用する場合、特に気をつける必要のある設定項目である。

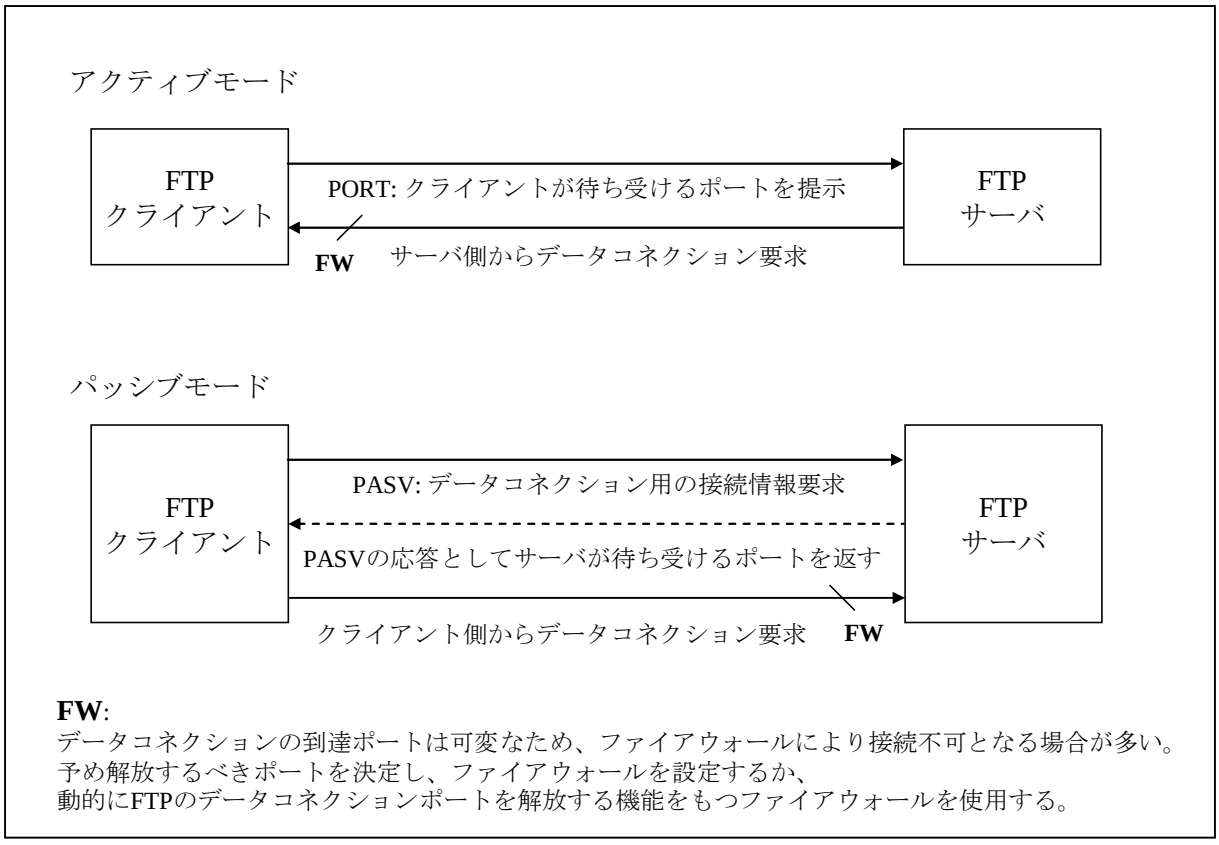

図 II-21-8.　FTP の接続形態（アクティブモードとパッシブモード）

【解説】

1) vsftpd の基本設定

* vsftpd をインストールすると、デフォルトでは匿名ユーザがファイルをダウンロードできる設定になっている。
* デフォルトで anonymous_enable は YES となっている。匿名ユーザのログインを許可しない場合は、これを NO に設定する。
* 匿名ユーザに書き込みを許す場合は、anon_upload_enable を YES に設定する。同様にディレクトリの作成を許すには anon_mkdir_write_enable を YES に設定する。共にデフォルトでは NO となっている。

2) ACL と chroot の設定

* vsftpd は、Linux の PAM（Pluggable Authentication Module）を使用する。pam_service_name によって使用する pam 設定ファイルを指定する。誤って指定すると正しく認証できないので注意する。
* システムのローカルユーザに FTP でのログインを許可するには、local_enable を YES に設定する。さらに書き込みを許すには、write_enable を YES に設定する。
* userlist_enable を YES に設定し、かつ userlist_deny を YES に設定（デフォルト）すると、userlist_file に指定されたファイルに記述されたユーザのログインを禁止する。userlist_deny を NO に設定すると、userlist_file に指定されたファイルに記述されたユーザのログインのみ許可する。
* chroot_list_enable を YES に設定し、かつ chroot_local_user を NO に設定（デフォルト）すると、chroot_list_file に指定されたファイルに記述されたユーザに chroot を実行する。chroot_local_user を YES に設定すると、chroot_list_file に指定されたファイルに記述されたユーザ以外のユーザに chroot を実行する。

3) パッシブモードとアクティブモード

* 最近の FTP クライアントでは、パッシブモードを使用することが多い。デフォルトでは YES となっており、多くの場合これを変更する必要はない。無効にしたい場合は pasv_enable を NO に設定する。
* パッシブモードで使用するポートの範囲は、 pasv_min_port と pasv_max_port で指定する。ファイアウォールでは、これらのポートでの接続を許可しておく必要がある（明示的にこれを許可する必要はなく、FTP セッションを解釈して自動的にポートを開放する設定を行うことができるデバイスも存在する）。
* PORT によるアクティブモードのサポートもデフォルトで YES となっている。無効にしたい場合は、port_enable を NO に設定する。

4) ログの設定

* log_ftp_protocol を YES にすることで、すべての FTP コマンドのログを記録することができる。運用初期段階や、トラブル時などには非常に役立つ。

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	21　OS セキュリティに関する知識 II II	応用
習得ポイント	II-21-9. Linux におけるシステムログ管理の実際	
対応する コースウェア	第 13 回 システムログの管理	

II-21-9. Linux におけるシステムログ管理の実際

システムログを管理する syslog の仕組みや機能、導入と運営管理の方法について解説する。また logger を使ったシステムログのテストや、swatch を用いたログ管理の自動化方法、これらツールの導入と設定方法などについて説明する。

【学習の要点】

* syslogd(8)は、UNIX ドメインソケットまたは INET ドメインソケットを通して任意のアプリケーションからのログを読み込み、記録する。
* syslogd は、OS の起動時に起動される。任意のアプリケーションは、直接 syslogd(8)とソケット通信をする代わりに、ライブラリ関数 syslog(3)を使うことができる。
* logger(1)は、syslogd(8)にログを送信するシェルコマンドである。

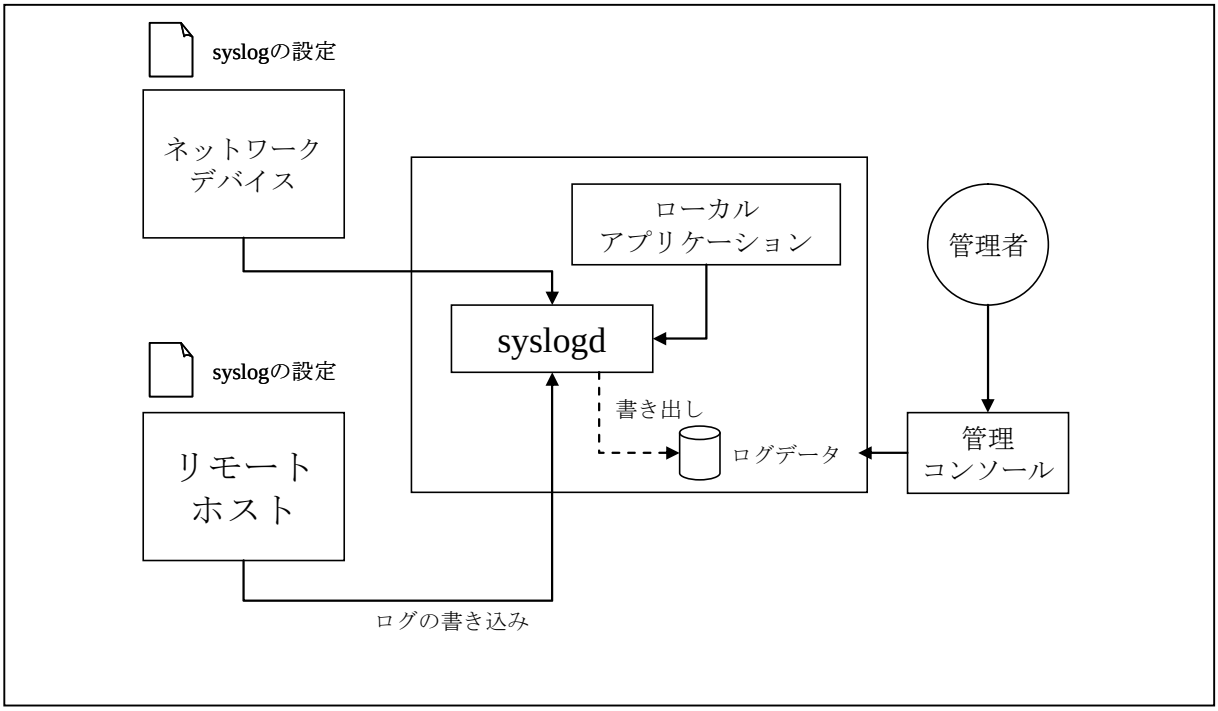

図 II-21-9.　syslog を用いたログの一元管理

【解説】

1) syslog

* syslog は、Linux など UNIX 系の OS に限らず、Windows など他の OS でも使用できるロギングの仕組みである。
* syslogd とアプリケーションは、UNIX ドメインソケットまたは INET ドメインソケットで通信する。このため、syslogd はリモートのアプリケーションからも INET ドメインソケットを通してログを受け付けることができる。
* 送信側アプリケーションは、直接ソケットを操作する代わりに、syslog(3)ライブラリ関数を用いて容易にログを送信することができる。また、シェルコマンド logger も用意されており、コマンドラインからも簡単にログを送信することができる。
* ルータやスイッチなどのネットワークデバイスは、syslog に対応しているものが多い。通常これらのデバイスは、ログを保存する十分な領域を持たないため、リモートの syslogd に対してログを送信する。
* syslogd のリモートログ機能を有効に活用すると、ネットワーク上のホスト、デバイスのログを一元的に管理することができる。

2) swatch

* swatch は、syslog が出力するログファイルを監視して、ログがあるパターン（正規表現）にマッチすると、メールで管理者に知らせたり、他のプログラムを呼び出したりする機能を持つ。
* swatch を導入することで、予め怪しいとわかっているログを他のログファイルに切り分けることができる。

3) sudo の例

* 通常、syslog に対応したアプリケーションのマニュアル（例えば man ページ）には、そのアプリケーションが出力する syslog のファシリティが記述してある。これは設定ファイルなどで変更できることが多い。これらのファシリティに対応するログをどこに出力するかは、syslog 側の設定として、/etc/syslog.conf にて行なわれる。
* 例えば sudo コマンドは、デフォルトでは authpriv ファシリティで syslog に出力する。Cent OS では、デフォルトで authpriv ファシリティへのログは/var/log/secure に出力されるよう、/etc/syslog.conf の設定がなされている。
* この仕組みによって、su コマンドで root ユーザとなってシェルコマンドを実行する代わりに、sudo コマンドを使用することで、root 権限で実行したすべてのコマンドのログを syslog 経由で出力することができるようになっている。

4) logrotate

logrotate は、溜まったログを定期的にローテート（古いログを削除したり圧縮したりすること）することを目的としたプログラムである。ローテートのタイミングで、ログの内容をメールで送信するなどすることで、不正にログが消去されることに対して対策を講じることができる。

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	21　OS セキュリティに関する知識 II II	応用
習得ポイント	II-21-10. 侵入検知の仕組みと運用方法	
対応する コースウェア	第 14 回 Linux による侵入検知の手法	

II-21-10. 侵入検知の仕組みと運用方法

サーバに対する侵入検知の必要性と、侵入検知ツールの仕組みや方法を解説する。具体的にはホスト型進入検知ツールの Tripwire と、ネットワーク型進入検知ツールの Snort について、それらの導入方法と設定方法、これらのツールを使った進入検知手順などを紹介する。

【学習の要点】

* 侵入検知システムは、インターネットなどを通して不正に内部ネットワークまたはホスト内に侵入し、データの改竄やシステムの破壊を試みる行為を事前に検知し、管理者に知らせるものである。
* 侵入検知システムは、センサによって悪意のある行為を検知し、ルールエンジンやパターンエンジンによってフィルタリングし、コンソールで管理者と対話する構成が一般的である。
* 侵入検知システムは、センサのカバーする範囲や動作によって分類することができる。ネットワーク型はネットワーク内を監視するセンサを有し、ホスト型はあるホストのシステムを監視するセンサを有する。

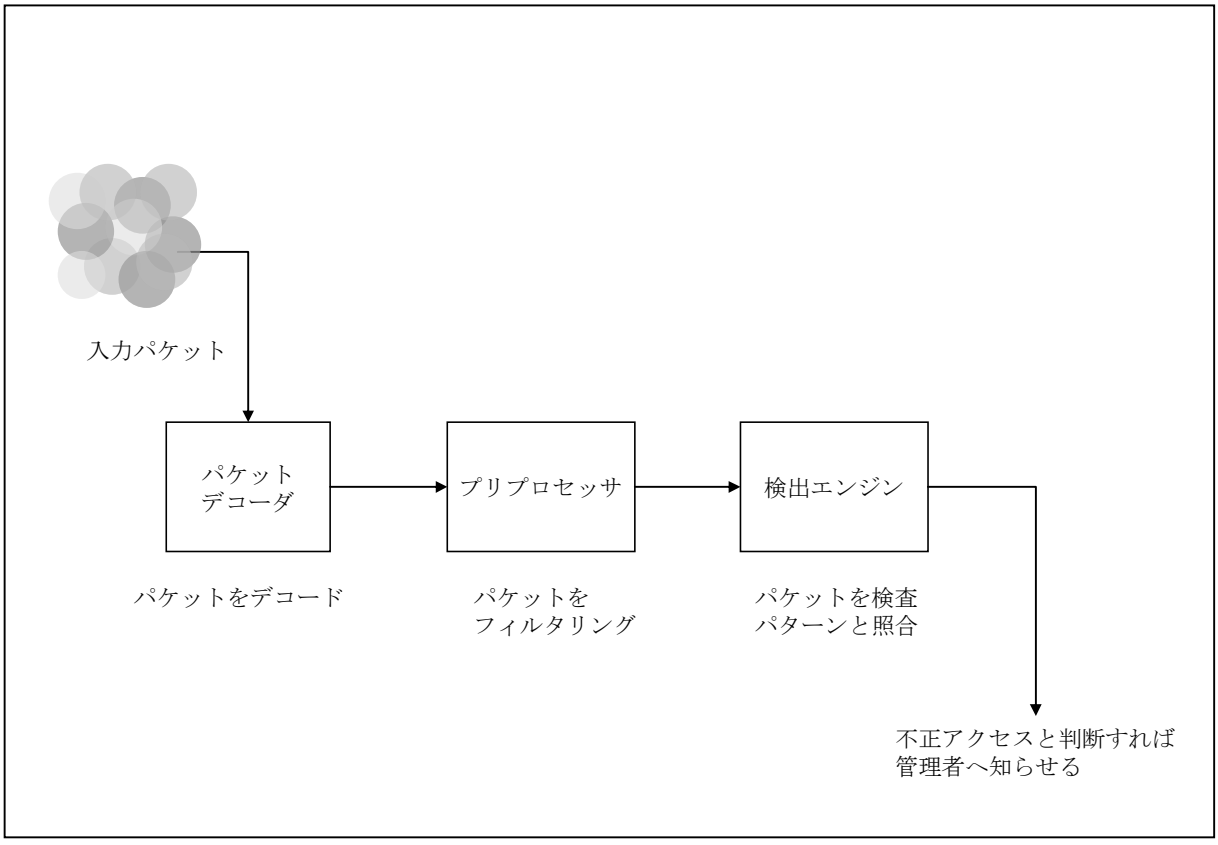

図 II-21-10.　Snort による侵入検知処理の一例

【解説】

1) 侵入検知システムの必要性

＊ 侵入検知システム(IDS)は、保護されるべき領域に不正に侵入されたことを検知し、管理者にそれを知らせるためのシステムである。

＊ 不正な侵入そのものを防ぐことはしないが、公開ポートを経由して侵入されたことに対してこれを検知することができるため、ファイアウォールで防ぎきれないリスクをヘッジすることができる。

＊ 侵入検知システムを発展させたものとして、侵入防止システム(IPS)がある。IDS や IPS は、ファイアウォールと組み合わせて使用されることが多い。

2) 侵入検知システムの分類

＊ 侵入検知システムは、大分類として、ホスト型とネットワーク型に分けることができる。ホスト型は、OS のソフトウェアとして実装され、ホストで実行される不正な行為を検出する。ネットワーク型は、ファイアウォールの前後に置かれ、ネットワークへの不正な侵入や攻撃を検出する。

＊ ネットワーク型の侵入検知システムは、専用のハードウェアが存在する。侵入検知システムの処理には多くの計算機リソースを消費するため、ハードウェアの方が効率が良いからである。

＊ 不正侵入だと判断する根拠は主に二通りあり、一つは通常作業との比較により以上を検出する方法と、もう一つは予め用意した不正行為パターンへのマッチングを行なうものである。

3) 侵入検知システムのソフトウェア実装

＊ ホスト型の侵入検知システムの実装としては、Tripwire が有名である。ネットワーク型の場合は、Snort が有名である。

＊ Tripwire は、ホストのファイルが不正に改竄されていないかを検出するのに最適なソフトウェアである。Tripwire は、最初にファイルシステムに存在するすべてのファイルの MD5 チェックサムを保存しておき、定期的にそれらの整合性をチェックする。

＊ Snort は、ネットワークへのアクセスを監視し、不正アクセスのパターンと照合する。もし予め登録された不正アクセスパターンにマッチすると、管理者に知らせる。

＊ ネットワーク型の侵入検知システムである Snort は、そこを通過するパケットをすべて検査していたのでは、到底処理が追いつかない。通常、プリプロセッサを設定して、検査するべきパケットを選択する。また、ファイアウォールの内側に設置することで、ファイアウォールを通過したパケットのみ検査と対象とすることで、検査対象パケットを大幅に減らすことができる。