21. OS セキュリティに関する知識 I

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を、Linux を題材として解説する。ローカルで利用する際のセキュリティ対策を示し、さらにネットワーク経由で利用する際のセキュリティ対策のうち、とくに OS のセキュリティ管理に必要な部分に焦点を当てて説明する。

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-21-1. サーバセキュリティに関する基本概念	現在のOSに求められるセキュリティの基本的な概念と、OSをとりまくリスクの種類とその対策方法など、OSのセキュリティを確保するために必要な事項を解説する。	1
I-21-2. Linuxサーバのローカルセキュリティ対策の基本と設定方法	Linuxサーバの運用時、ネットワーク利用の有無に関わらず必要となるローカルセキュリティ管理について、その基本的な項目の内容と各種の設定方法、セキュリティが保たれているかどうかのチェック方法を説明する。	2
I-21-3. Linuxサーバのネットワークセキュリティ対策の基本と設定方法	Linuxサーバのネットワークセキュリティ管理について、その基本的な項目の内容と各種の設定方法を解説する。またネットワーク上の通信に関してプライバシを保護するための対策についても触れる。	3
I-21-4. ログを用いたセキュリティ管理の基本	Linuxサーバの運用時に得られるログを利用して、サーバセキュリティ管理を行う手法についての基本的な概念と方法を説明する。改ざんが行われたなど、サーバに対する攻撃が行われたことをログを利用してチェックする方法を解説する。	2
I-21-5. Linuxサーバを使用したファイアウォールの設計と導入	ファイアウォールとは何か、ファイアウォールとDMZ (DeMilitarized Zone)の関係、安全なネットワーク構築方法について触れ、さらにLinuxサーバを利用したファイアウォールの構築方法、設定ポリシーの考え方などを説明する。	4
I-21-6. iptablesによるセキュリティ管理方法	Linuxサーバによるファイアウォールを実現するiptablesの目的や役割について概説する。またiptablesの具体的な設定方法を紹介し、その運用手順について解説する。	4
I-21-7. セキュリティを考慮したLinuxサーバの適切な設定	サーバソフトウェアのインストール方針やサービス提供方針など、Linuxサーバにおけるセキュリティ管理の基本的な方針について説明し、さらにサーバ上で十分なセキュリティを確保するために必要な作業と留意点を示す。	5
I-21-8. セキュアシェルの利用、その基本と応用	リモートからの安全なアクセスを実現するSSH (Secure SHell)について解説する。SSHの基本的な動作とOpenSSHの導入、SSHに関する各種の設定などを説明し、さらにSSHの応用としてリモートからのコマンド実行やTCPポートフォワーディングにも言及する。	6
I-21-9. SSLによる仮想専用ネットワーク(VPN)の設定	Webの暗号化通信技術SSLを利用して仮想専用ネットワーク(VPN)を実現するSSL-VPNの仕組みについて解説する。利用できるアプリケーションが限定されるが、導入が容易であることに言及する。	7
I-21-10. DNSに関するセキュリティ対策	DNS (Domain Name System)の基本的な動作とDNSに求められるセキュリティ要件を解説する。標準的なDNSサーバの実装であるBINDを紹介し、BINDにおけるセキュリティ対策について述べる。	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

「21. OS 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
21. OSセキュリティに関する知識	<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	IT-IAS4. ポリシー	IT-IAS5. 攻撃	IT-IAS6. 情報セキュリティ分野	IT-IAS7. フォレンジック（情報証拠）[21-Ⅰ-2]	IT-IAS8. 情報の状態	IT-IAS9. 情報セキュリティサービス [21-Ⅰ-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	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-Ⅰ-8]	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-NET4. セキュリティ [21-Ⅰ-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-Ⅰ-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-Ⅰ-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-Ⅰ-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-Ⅰ-1]		
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-CAO0. 歴史と概要	CE-CAO1. コンピュータアーキテクチャの基礎	CE-CAO2. メモリシステムの構成とアーキテクチャ	CE-CAO3. インタフェースと通信	CE-CAO4. デバイスサブシステム	CE-CAO5. CPUアーキテクチャ	CE-CAO6. 性能・コスト評価	CE-CAO7. 分散・並列処理	CE-CAO8. コンピュータによる計算	CE-CAO9. 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、ネットワークセキュリティに関する OSS の利用方法がある。具体的にはファイアウォールを構築する際に用いる iptables や遠隔地からのサーバ管理に欠かせない SSH などを含む。

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
21.OS 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概要 (2)リスクの構成要素の識別と評価	(1)基本的な行動 (2)改ざんチェック	(1)ネットワークセキュリティの基本設定 (2)盗聴対策	(1)ファイアウォールとDMZ アーキテクチャの種類 (2)サーバファイアウォール設定のポリシー (3)iptables によるセキュリティ管理	(1)サーバとしての管理方針と実施方法 (2)サーバでのセキュリティ実施方法	(1)セキュアシェルの基礎知識 (2)SSH の応用	(1)トンネリングの仕組みと設定 (2)IPsec による暗号化通信の導入 (3)IPsec による暗号化通信ワークショップ	(1)DNS の基本動作 (2)DNS セキュリティの原則 (3)BIND における セキュリティ対策 (4)djbdns

（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 I	基本
習得ポイント	I-21-1. サーバセキュリティに関する基本概念とリスク対策	
対応する コースウェア	第 1 回（OS のセキュリティ機能）	

I-21-1. サーバセキュリティに関する基本概念とリスク対策

現在の OS に求められるセキュリティの基本的な概念と、OS をとりまくリスクの種類とその対策方法など、OS のセキュリティを確保するために必要な事項を解説する。

【学習の要点】

＊ サーバを管理するには、継続的なセキュリティ情報の収集と対策が不可欠である。

＊ セキュリティの確保が十分でない場合には、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。

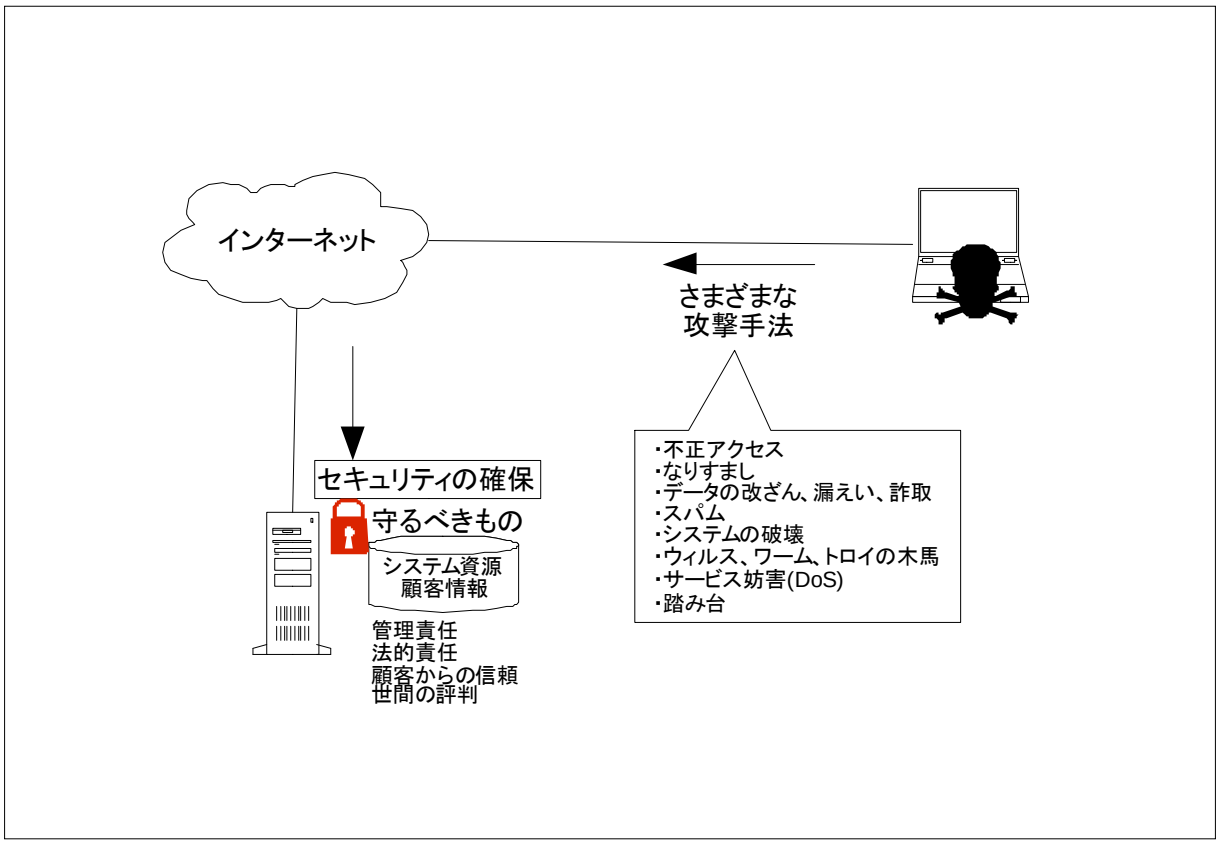

図 I-21-1.　サーバに求められるセキュリティ

【解説】

1）現在の OS に求められるセキュリティの基本的な概念

セキュリティとは、攻撃に対して防衛し、脅威から守ることである。ここで守るべきものとは、システム資源だけではなく、顧客情報の管理責任、その他法的責任、顧客からの信頼、世間の評判なども含まれる。

2）OS をとりまくリスクの種類とその対策方法

＊ 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
他のユーザーのふりをしたサービスの利用。

＊ 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）OS のセキュリティを確保するために必要な事項

＊ 脆弱性の排除
セキュリティパッチの適用や、セキュリティ対策を施したシステム構築など。入力データのサイズをチェックする処理をプログラムに組み込んでおくことにより、バッファオーバーフロー攻撃に関する脆弱性を取り除くことができるほか、脆弱性を判定するシステムを利用することも検討する。

＊ 攻撃のブロック
ファイアウォールの設置により、攻撃自体をブロックする。また、外部からのアクセスのログを定期的に参照し、不審なアクセスがないかどうかを確認する。

＊ データの暗号化と分散
重要なデータの暗号化や分散化により、攻撃者にとって、仮にデータを入手してもそれだけでは価値がないような形態にしておくことが必要である。また、デジタル署名がされていれば、攻撃者は内容を改ざんできない。

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 I	基本
習得ポイント	I-21-2. Linux サーバのローカルセキュリティ対策の基本と設定方法	
対応する コースウェア	第 2 回（Linux サーバのローカルセキュリティ対策）	

I-21-2. Linux サーバのローカルセキュリティ対策の基本と設定方法

Linux サーバの運用時、ネットワーク利用の有無に関わらず必要となるローカルセキュリティ管理について、その基本的な項目の内容と各種の設定方法、セキュリティが保たれているかどうかのチェック方法を説明する。

【学習の要点】

＊ 多くの Linux ディストリビューションでは、インストール直後は脆弱な状態になっている場合が多く、セキュリティの確保のために設定変更が必要である。

＊ 必要最小限の権限を与えるようにするのが、セキュリティ対策の基本である。

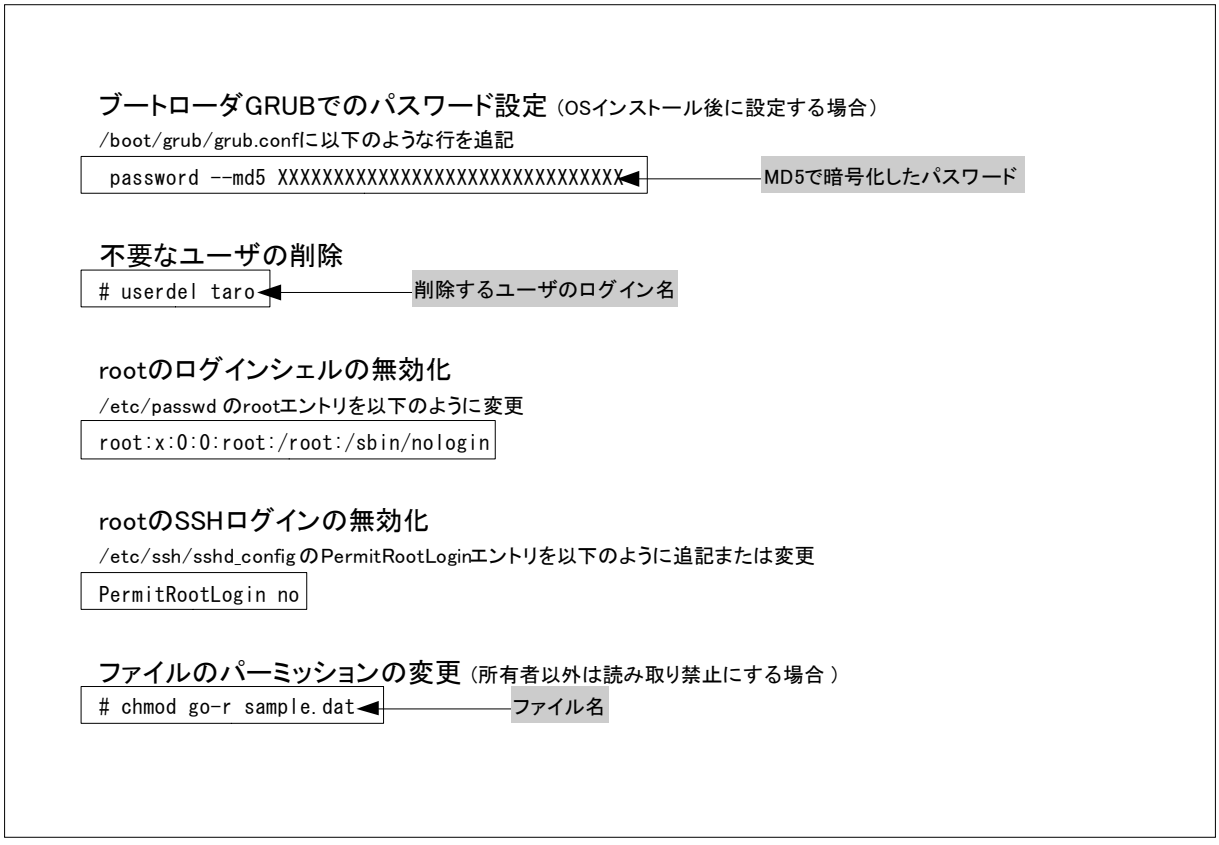

図 I-21-2.　ローカルセキュリティのためのコマンドや設定ファイルの例

【解説】

1) 起動

ブートローダはコンピュータの起動時に OS をメモリにロードするプログラムである。ブートローダには GRUB(GRand Unified Bootloader)や LILO(LInux LOadrer)があるが、これらにパスワードを設定することで、許可のないユーザーが、リムーバブルメディアやシングルユーザーモードで起動するのを防ぐことができる。また、BIOS(Basic Input/Output System)には、起動時パスワードが設定できるものがあり、BIOS がブートローダを起動する前にパスワード入力を求めるようにできる。BIOS 管理パスワードが設定できる BIOS では、起動ドライブ等の BIOS 設定を変更する際にパスワード入力を求めるようにできる。マシンを起動/再起動した際は、いつ行ったかを記録し、不正な起動があった場合に発見できるようにすべきである。

2) ユーザアカウントとパスワード

必要最小限のアカウントを作成するよう注意する。身元の不明な人物にアカウントを提供しない。使われていないアカウントは削除する。ログイン日時/場所を記録するようにする。複数人でユーザ ID を共有するのは(操作を行った人物の特定が困難なため)避けなければならない。パスワードは安易で見破られやすいものが使われないように留意する。

3) root アカウント

root はマシン全体に対する権限を持つアカウントである。操作ミスなどの影響が大きい root でのアクセスは極力減らすべきである。ユーザ切り替えコマンドの su や、管理者権限でコマンドを実行できる sudo からのみ管理者権限を利用できるようにし、ログを採取するのが望ましい。root でのアクセス拒否の設定としては、/etc/passwd ファイルを編集して root のシェルを無効にする、root ログインを禁止する、SSH デーモンの設定ファイルを編集して SSH での root ログインを禁止する、PAM（Pluggable Authentication Module）の設定ファイルを編集して root を禁止する、といった方法がある。一方、sudo で実行できるコマンドやユーザの設定は visudo で行う。

4) ファイルアクセス

ファイルのパーミッションは、所有ユーザと所有グループを設定でき、所有ユーザ/所有グループ/その他のグループそれぞれについて、読取権/書込権/実行権が設定できるようになっている。不必要な権限は極力与えないようにすべきである。ただしシステムファイルのパーミッションは安易に変更しないよう注意が必要である。パーミッションは chown、chgrp、chmod といったコマンドで設定可能である。また、umask コマンドで新規作成時のデフォルトパーミッションを極力弱いものにするのが望ましい。ファイル改ざんの監視としては、md5sum コマンドでチェックサム値を保存/確認することができる。

5) ログ

通常、/var/log/ディレクトリ配下のファイルにログが出力される。必要な情報を出力し、不要な情報を抑制するように設定すべきである。一般ユーザで実行しない処理のログは、一般ユーザが書き換えできないようにパーミッションを設定する。

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 I	基本
習得ポイント	I-21-3. Linux サーバのネットワークセキュリティ対策の基本と設定方法	
対応する コースウェア	第 3 回（Linux のネットワークセキュリティ対策）	

I-21-3. Linux サーバのネットワークセキュリティ対策の基本と設定方法

Linux サーバのネットワークセキュリティ管理について、その基本的な項目の内容と各種の設定方法を解説する。またネットワーク上の通信に関してプライバシを保護するための対策についても触れる。

【学習の要点】

＊ Linux には、ネットワークセキュリティを確保するための様々な技術が搭載されている。

＊ セキュリティに関する設定項目を理解することで、堅牢なサーバを構築することができる。

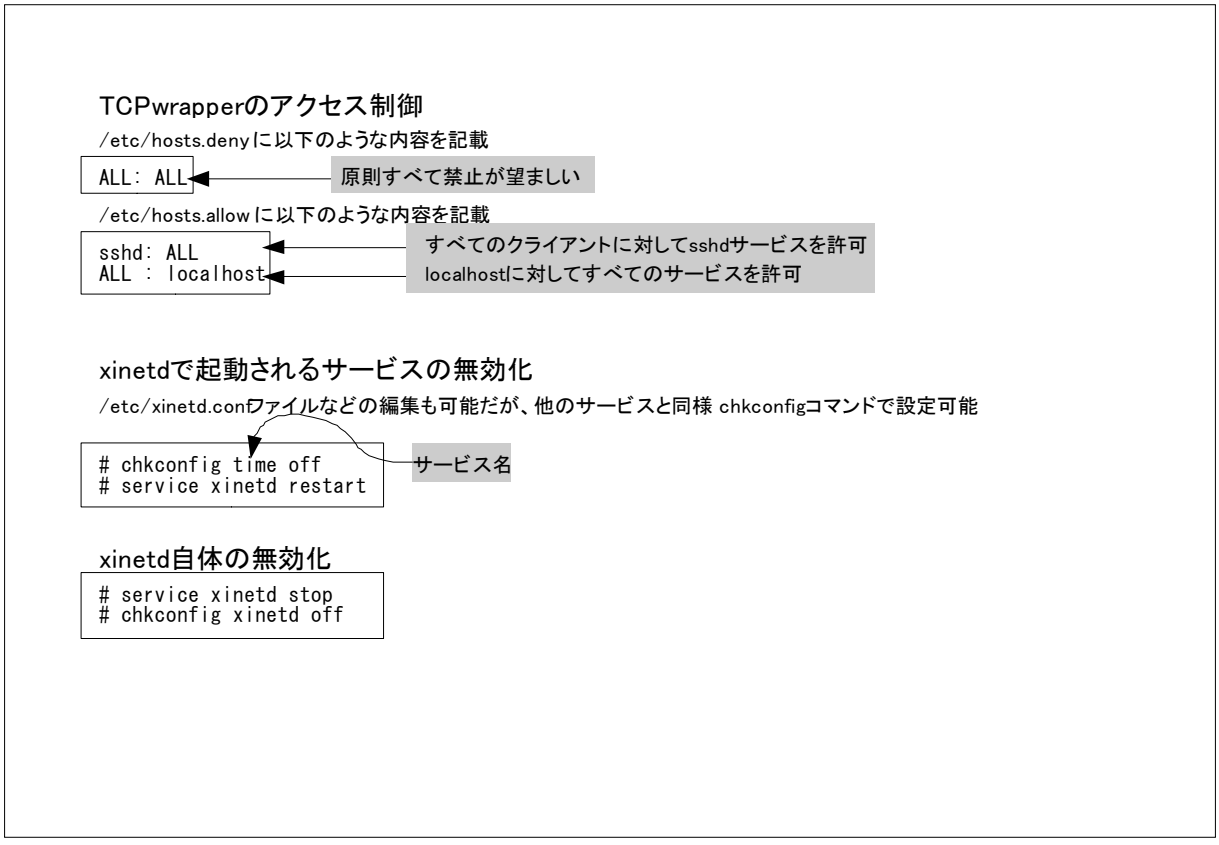

図 I-21-3.　ネットワークセキュリティのためのコマンドや設定ファイルの例

【解説】

1) パケットフィルタリング

Linux では iptables コマンドによりパケットフィルタリングの設定が可能である。ネットワーク層での制御となるので、ネットワークインタフェースごとの制御が可能である。

2) TCPwrapper

TCPwrapper はサービスやポートに対してアクセス制御や監視を行うためのプログラムであり、外部からの接続を送信元(ホスト名または IP アドレス)の情報をもとに制限する機能を有する。具体的には、以下の手順を踏む。

* /etc/hosts.allow に記述されたパターンに合致する場合は接続許可
* hosts.allow に合致せず、/etc/hosts.deny に記述されたパターンに合致すれば接続拒否
* いずれにも合致しなければ接続許可

パケットフィルタリングとは異なり、TCPwrapper はアプリケーション層での制御となる。ネットワークインタフェース毎の制御はできないが、ドメインの部分一致などによるアクセス制御が可能である。

3) xinetd

xinetd は、設定されたあるサービスへの要求があった場合に、そのデーモンを起動する役割を担い、スーパーサーバと呼ばれる。スーパーサーバでは、応答速度が遅くなる反面、常駐しない分メモリを節約できるので、利用頻度の低いサービスが登録される。TCPwrapper によるアクセス制御が可能である。

* xinetd の設定
  xinetd の設定は/etc/xinetd.confファイル(またはこのファイルから呼び出すファイル)に記述する。必要のないサービスは設定を無効化すべきである。xinetd に登録すべきサービスが何もない場合は、xinetd 自体を起動しないようにすべきである。
* inetd と xinetd
  xinetd は、以前に使われていた inetd を、セキュリティを含めて機能強化したものである。inetd は使わずに xinetd を使用することが望ましい。また、xinetd はそれ自身にアクセス制御の仕組みを備えたため、TCPwrapper の併用は減少しているが、併用することにより二重のアクセス制御ができ、セキュリティが強化される。

4) Telnet

Telnet の代わりに、通信経路を暗号化した SSH を使用するのが望ましい。Telnet が必要な場合は以下の対策を行うべきである。

* ログインメッセージの抑止（/etc/issue.net ファイルの編集）
* ポート番号を既定値(23)以外に変更（/etc/services ファイルの編集）
* root ログインの拒否（/etc/securetty ファイルの編集）

多くの Linux ディストリビューションでは、xinetd 経由で Telnet を起動するようになっている。

5) 通信の暗号化

多くの Linux ディストリビューションには OpenSSL が標準で導入され、SSL に対応したアプリケーションで暗号化通信が実現でき、プライバシ等を保護することができる。SSH もその一つである。

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 I	基本
習得ポイント	I-21-4. ログを用いたセキュリティ管理の基本	
対応する コースウェア	第 2 回（Linux サーバのローカルセキュリティ対策）	

I-21-4. ログを用いたセキュリティ管理の基本

Linux サーバの運用時に得られるログを利用して、サーバセキュリティ管理を行う手法についての基本的な概念と方法を説明する。改ざんが行われたなど、サーバに対する攻撃が行われたことをログを利用してチェックする方法を解説する。

【学習の要点】

＊ ログ管理がなくてはセキュリティは片手落ちである。

＊ 必要なログの採取と不要なログ出力の抑制を行うことで、効率的なログ管理ができ、セキュリティ向上につながる。

/var/log/messages の例

```
Nov 15 01:26:28 sv syslogd 1.4.1: restart.
Nov 15 01:26:28 sv kernel: klogd 1.4.1, log source = /proc/kmsg started.
Nov 15 01:26:28 sv kernel: Linux version 2.6.18-8.el5 (mockbuild@builder4.centos.org) (gcc ver
sion 4.1.1 20070105 (Red Hat 4.1.1-52)) #1 SMP Thu Mar 15 19:57:35 EDT 2007
```

/var/log/secure の例

```
Nov 15 01:57:36 sv sshd[1807]: Failed password for root from 192.168.0.1 port 32781 ssh2
Nov 15 01:57:40 sv sshd[1807]: Accepted password for root from 192.168.0.1 port 32781 ssh2
Nov 15 01:57:40 sv sshd[1807]: pam_unix(sshd:session): session opened for user root by (uid=0)
```

図 I-21-4.　ログの出力例

【解説】

1）ログ管理の重要性

ログ管理は実行を怠ってしまいがちであるが、事後的なチェック・確認のために、ログデータの管理は必須である。

＊ 障害の発生要因を解明し、障害復旧やその他の問題解決の糸口となる

＊ 不正アクセスなどの攻撃情報が得られる

2) セキュリティのためのログ確認と設定

通常、/var/log/ディレクトリ配下のファイルにログが出力される。syslog などのログツールでは、あらかじめログの設定がされているが、初期設定をそのままカスタマイズせずに使っていては、不要なログ情報があふれ必要なログ情報の抽出が困難になり、必要な情報がログとして出力されない場合があるので注意が必要である。必要なログを採取し、不要なログは抑制する必要がある。また、ログを参照する場合には、システムが置かれている状況によって異なる判断が必要であることに注意しなければならない。

＊ 正常な状態と異常な状態
正常な状態でのログの件数や内容を確認しておくことで、正常な状態と異常な状態とを見分けられる。

＊ 大量のログ情報からの効率的な異常の発見
例えば SSH 認証において、失敗の記録が多い場合には辞書攻撃などによる不正アクセスで認証が失敗しているケースが考えられる。ログ監視ツールにて、SSH 認証失敗を抽出するようにしたり、あるいは SSH 認証成功のログ出力を抑制したりすることで、効率的なログ管理が可能となる。

3) syslog

syslog は最も広く利用されているログツールであり、/etc/syslog.confファイルにより、以下のようなログ出力の設定が可能である。

＊ ファシリティ（ログの分類）

＊ 優先度（デバッグ、情報、警告などのレベル）

＊ 動作（通常ファイルや画面などのデバイスファイルの名前）

4) Syslog-ng (syslog new generation)

Syslog-ng は syslog の次世代版として開発され、セキュリティ面で以下のような利点がある。

＊ ログ監査の自動化

＊ ログ受信時のアクセス制御

＊ root 以外のユーザー権限で動作可能

＊ TCP ポートによるログ転送

5) swatch

swatch はログ監視ツールであり、ログが書き込まれるときに、指定したパターンが見つかった場合に、指定したコマンドを実行することができる。

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	21　OS セキュリティに関する知識 I	基本
習得ポイント	I-21-5. Linux サーバを使用したファイアウォールの設計と導入	
対応する コースウェア	第 4 回（Linux によるファイアウォール構築）	

I-21-5. Linux サーバを使用したファイアウォールの設計と導入

ファイアウォールとは何か、ファイアウォールと DMZ（DeMilitarized Zone)の関係、安全なネットワーク構築方法について触れ、さらに Linux サーバを利用したファイアウォールの構築方法、設定ポリシーの考え方などを説明する。

【学習の要点】

* Linux では iptables というツールが用意されており、ファイアウォールの構築を簡単に行うことができる。
* Linux が持つ他のセキュリティ技術と組み合わせることで、堅牢なシステムを構築できる。

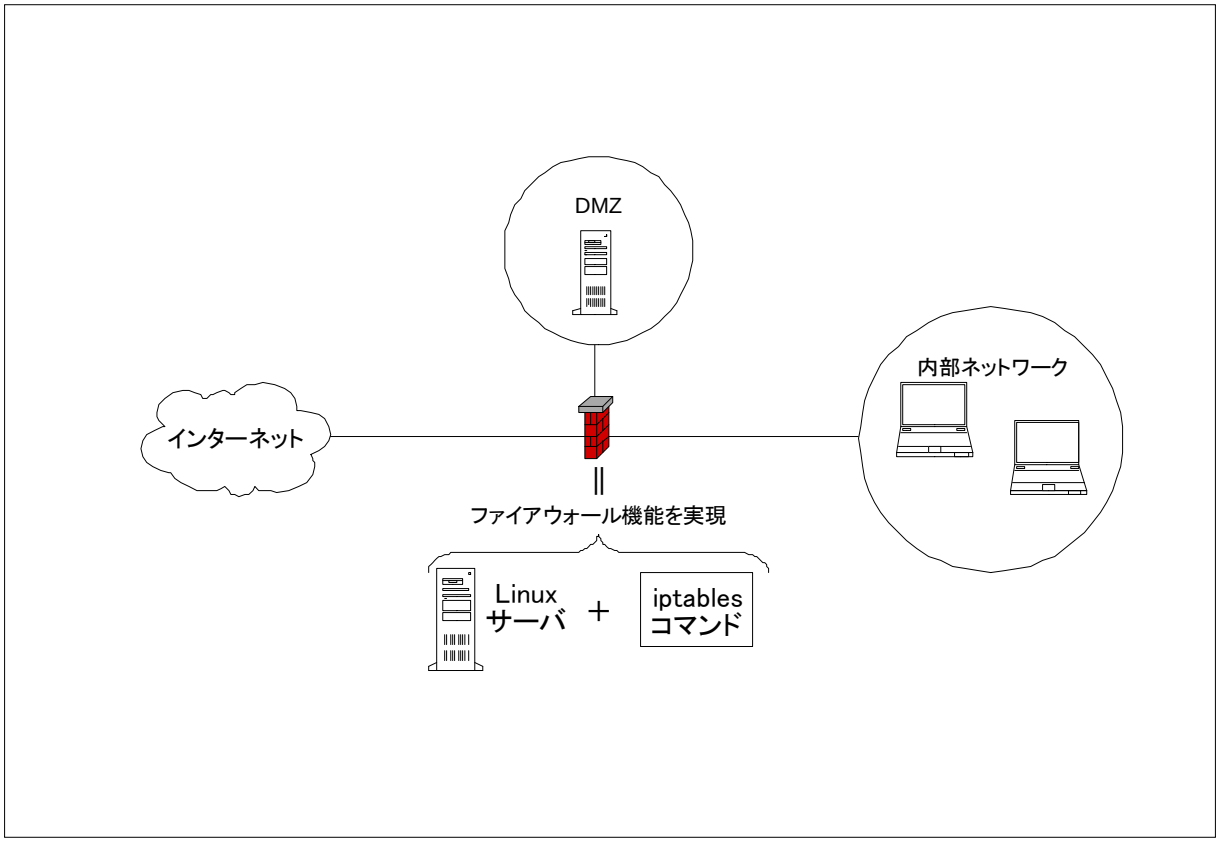

図 I-21-5.　Linux サーバで構築できるファイアウォール

【解説】

1) ファイアウォールとは

ファイアウォールとは、アクセス制御に基づいて接続許可/接続拒否(パケット破棄)を行う機能である。狭義では、この機能により、ネットワークとネットワークとを分離するシステムをファイアウォールという。

2) ファイアウォールと DMZ の関係

DMZ(非武装地帯)は、外部ネットワーク(インターネット)と内部ネットワークとの間に位置し、それぞれのネットワークとファイアウォールで区切られているネットワークを指す。DMZ には外部公開するサーバを設置する。

3) 安全なネットワークの構築

セキュリティのためには、外部とDMZ、DMZと内部、外部と内部のそれぞれ双方向で、必要最小限のパケットを通過させるように、ファイアウォールを設定する必要がある。また、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は防ぐことが出来ず、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することが重要である。

4) Linux サーバを利用したファイアウォールの構築

Linux には iptables というツールが用意されており、これによって、Linux サーバをファイアウォールにすることが可能となる。

* NAT(Network Address Translator)の例
  外部ネットワークと公開サーバのあるネットワークとの境界にファイアウォールを設置する場合を考える。ファイアウォールとなる Linux サーバには、外部側と公開サーバ側それぞれにネットワークインタフェースを用意し、外部側には、各公開サーバ毎に割り当てる仮想 IP アドレスを設定する。iptables で NAT の設定を行えば、NAT が構築できる。
* パケットフィルタ型ファイアウォールの構築
  上記 NAT において、iptables でフィルタリングの設定を行うことで、ファイアウォールが構築できる。

5) ファイアウォール設定ポリシーの考え方

iptables でファイアウォールを構築する場合、iptables で指定可能な情報(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決定する。このようなパターンを複数設定することができる。基本ポリシーとしてパケットを破棄し、必要なパケットのみ通過させるのがセキュリティ上望ましい設定ポリシーとなる。

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 I	基本
習得ポイント	I-21-6. iptables によるセキュリティ管理方法	
対応する コースウェア	第 4 回（Linux によるファイアウォール構築）	

I-21-6. iptables によるセキュリティ管理方法

Linux サーバによるファイアウォールを実現する iptables の目的や役割について概説する。また iptables の具体的な設定方法を紹介し、その運用手順について解説する。

【学習の要点】

＊ Linux には、iptables という、ネットワーク制御において非常に便利かつセキュリティ上重要なツールが用意されている。

＊ iptables の使い方を理解することで、パケットフィルタリング、NAT、IP マスカレードといったファイアウォールを Linux 上で構築できるようになる。

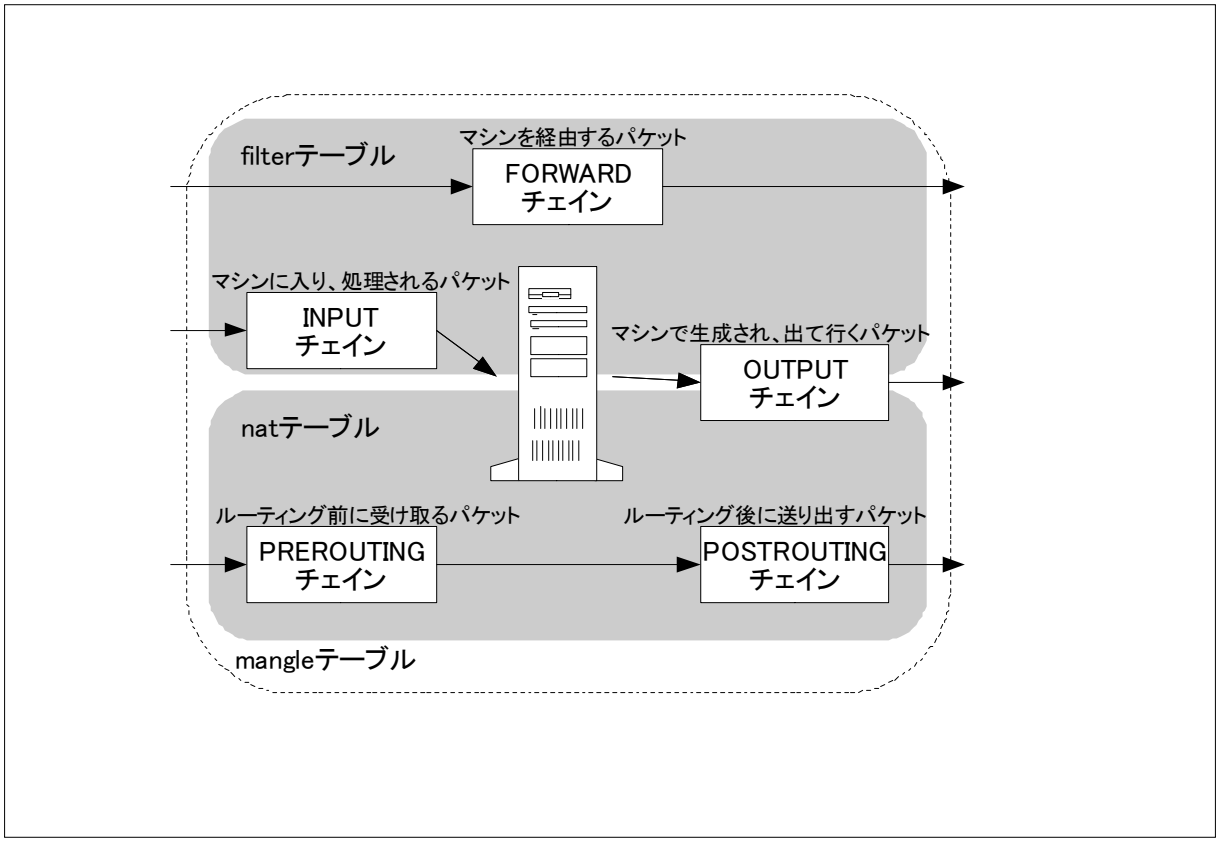

図 I-21-6.　iptables のテーブルとチェインの概念

【解説】

1) iptables の目的と役割

iptables は Linux のネットワークツールの 1 つである。様々なパケットフィルタリングルールや NAT ルールを適用することができ、Linux 上にファイアウォールを構築することができる。

2) iptables の主な設定方法

iptables の基本的な書式は、次のようになる。

iptables -t テーブル 操作の種類 チェイン ルール番号 ルール

＊ テーブル

iptables には、一連のルールを記述するテーブルという概念がある。テーブルには、filter(パケットフィルタリング用)、nat(NAT 用)、mangle(特殊な変換用)がある。「-t」に続けてテーブルを指定する。-t 省略時は filter となる。

＊ 操作の種類

操作の種類には、-P(ポリシーの設定)、-L(全ルールの表示)、-A(ルールの追加)、-I(ルールの挿入)、-R(ルールの置換)、-D(ルールの削除)、-F(全ルールの消去)などがある。-P の場合は上記書式ではなく、-P につづけてターゲットを指定する。

＊ チェイン

各テーブルでは、チェインと呼ばれるブロック毎にルールを設定する。チェインには、INPUT(入力用)、OUTPUT(出力用)、FORWARD(転送用)、PREROUTING(ルーティングの受信時用)、POSTROUTING(ルーティングの送信時用)があり、図のように、テーブルによって使用できるチェインが異なる。-L や-F ではチェインを省略し、テーブルの全チェインを対象にできる。

＊ ルール番号 (-I、-R、-D の場合)

ルールにつける番号(各チェインで一意)。-I で省略するとルール番号は 1 となる。

＊ ルール (-A、-I、-R の場合)

ルールには、条件と、条件にマッチした場合の動作を、以下のようなオプションで指定する。

-s 送信元	送信元のホスト名、ドメイン名または IP アドレスを指定
-d 宛先	宛先のホスト名、ドメイン名または IP アドレスを指定
-p プロトコル	tcp、udp、icmp、あるいは全プロトコルが対象の all を指定
--sport 番号	送信元ポート番号を指定
--dport 番号	宛先ポート番号を指定
-i インタフェース	受信ネットワークインタフェースを指定
-o インタフェース	送信ネットワークインタフェースを指定
-j 動作	ターゲットまたは次に処理するチェインを指定

＊ ターゲット

ACCEPT(通過)、DROP(破棄)、MASQUERADE(IP マスカレード) など。

3) iptables の運用手順

＊ はじめに、各チェインで「-P チェイン DROP」とし、原則破棄にするのが望ましい。

＊ その後、必要なものに限って許可のルールを加えていく。

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 I	基本
習得ポイント	I-21-7. セキュリティを考慮した Linux サーバの適切な設定	
対応する コースウェア	第 5 回（Linux のサーバセキュリティ設定）	

I-21-7. セキュリティを考慮した Linux サーバの適切な設定

サーバソフトウェアのインストール方針やサービス提供方針など、Linux サーバにおけるセキュリティ管理の基本的な方針について説明し、さらにサーバ上で十分なセキュリティを確保するために必要な作業と留意点を示す。

【学習の要点】

＊ 多くの Linux ディストリビューションでは、導入初期の状態は、セキュリティよりも利便性を重視したものとなっている。

＊ Linux サーバを初期設定のままでなく、適切に設定を変更することで、Linux サーバのセキュリティを向上させることができる。

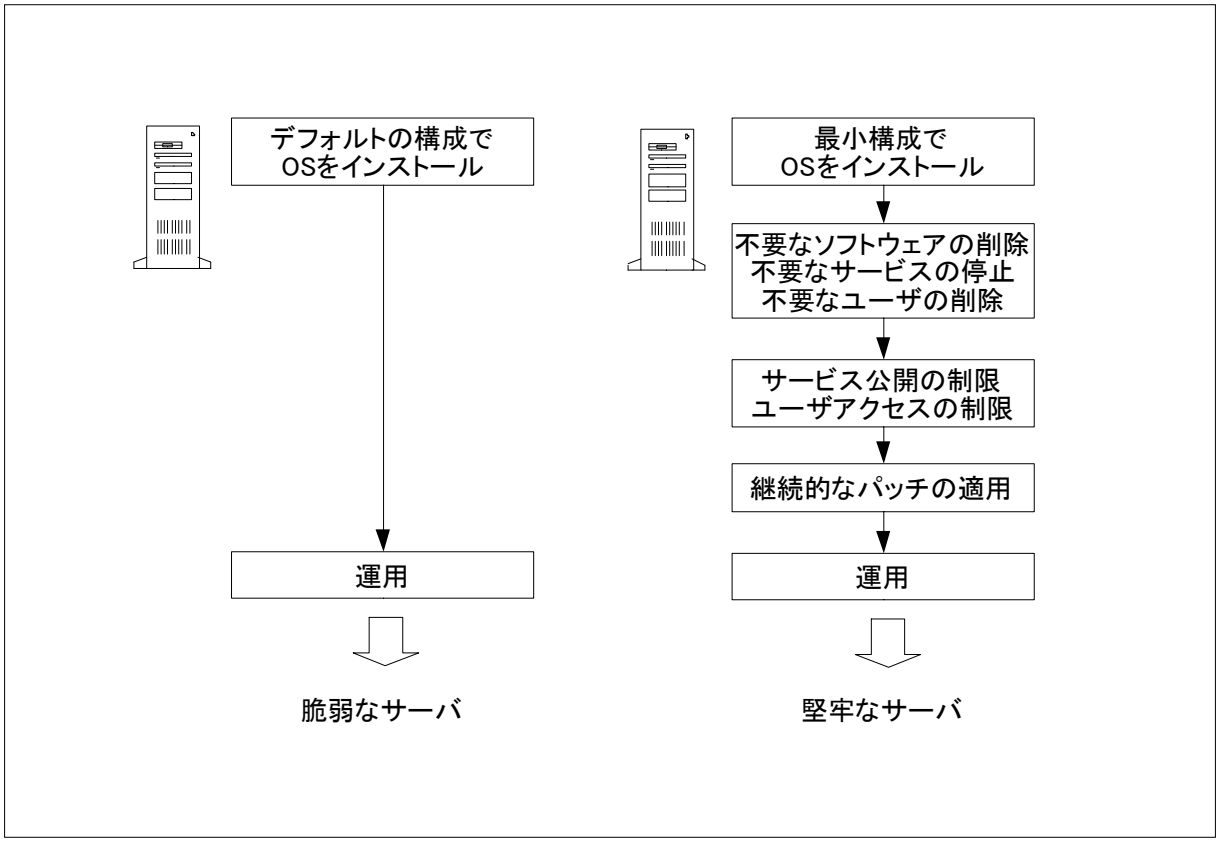

図 I-21-7.　Linux サーバの設定の必要性

【解説】

1) 不要なソフトウェアの削除または無効化

不要なソフトウェアを導入していると、それらのセキュリティホールを突かれるなど、脆弱性が増す。必要なソフトウェアのみインストールし、それ以外のものは極力削除する。不要でなくとも普段使用しないものは無効化しておく。OS インストールの段階で、最小インストールを行うのが望ましい。

2) ソフトウェアのアップデート

* 個々のパッケージのセキュリティパッチ
  リリースされ次第、直ちに適用する。
* 個々のパッケージのその他のバージョンアップ、Linux ディストリビューションのバージョンアップ
  設計上のセキュリティ強化、新たなセキュリティホールの可能性、安定性、互換性等を考慮のうえ、適用の是非を判断する。
* カーネルのバージョンアップ
  再審にしておくことが望ましいが、メジャーバージョンアップは不安定な場合が多いので、注意を要する。

3) 不要なユーザアカウントの削除または無効化

不要なユーザを用意していると、それらのユーザへのなりすましなど、脆弱性が増す。必要なユーザだけを作成し、不要なものは削除する。不要でなくとも普段使用しないユーザは無効化しておく。OS やアプリケーションのインストール時に、不要なユーザアカウントが登録される場合もあるので、不要なアプリケーション用のアカウントは削除または無効化する。

4) ユーザのシェルアクセスの制限

アプリケーション専用のユーザアカウントなどの多くはサービス用のアカウントであり、シェルを必要としない。これらのシェルアクセスを制限することで、必要のないシェルアクセスを与えないようにする。

5) 匿名アクセスの制限

FTP などのサービスへの匿名アクセス(anonymous FTP)は、必要でなければ無効化する。通常の Linux ディストリビューションでは初期設定で無効化されているケースが多い。

6) サービスの公開の制限

各サービスは原則非公開とし、公開の必要なものに限って公開のための作業を行う。

7) chroot されたシステムでのサービス実行

chroot システムコールを使用し、特定のディレクトリ配下以外のファイルにプロセスがアクセスできないよう変更する。これにより、外部からデーモンが乗っ取られた場合のファイルシステムへのアクセスを制限することができる。

8) その他

* SUID や SGID の確認
* ログ管理
* iptables によるファイアウォールの構築

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 I	基本
習得ポイント	I-21-8. セキュアシェルの利用、その基本と応用	
対応する コースウェア	第 6 回（安全なリモートアクセス）	

I-21-8. セキュアシェルの利用、その基本と応用

リモートからの安全なアクセスを実現する SSH (Secure SHell)について解説する。SSH の基本的な動作と OpenSSH の導入、SSH に関する各種の設定などを説明し、さらに SSH の応用としてリモートからのコマンド実行や TCP ポートフォワーディングにも言及する。

【学習の要点】

＊ 現在、Linux の遠隔操作は、SSH を通じて行うことがほとんどである。

＊ SSH は暗号化されているからと安堵することなく、適切に設定、運用することがセキュリティ上重要となる。

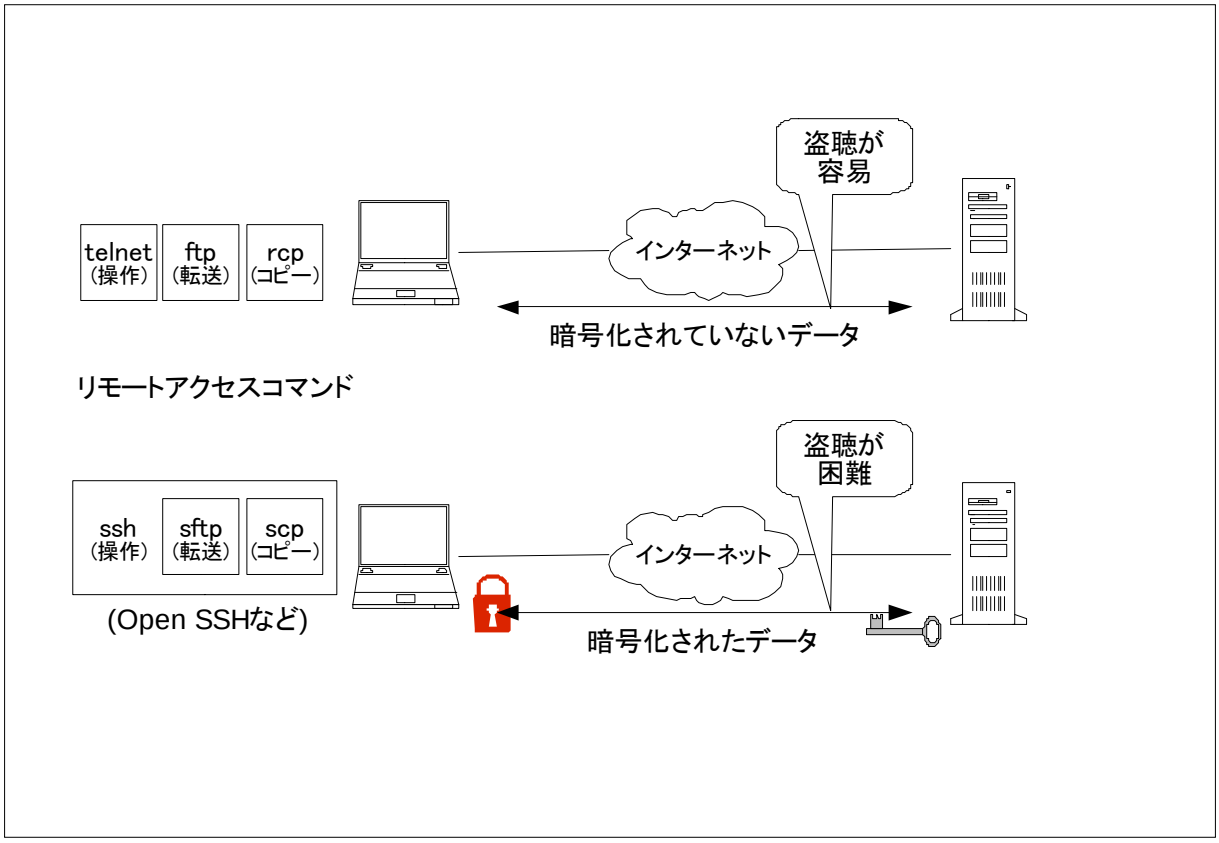

図 I-21-8.　安全なリモートアクセスを提供する SSH

【解説】

1) SSH とは

SSH は、暗号化通信を使ってリモートホストにログインし、各種処理を行うためのツールである。

2) SSH の動作

SSL を使った Web トランザクションと同様、公開鍵と秘密鍵によって生成される共通鍵で通信を暗号化する。クライアントの認証は、秘密鍵とそのパスフレーズ、または、ユーザ名とそのパスワードによって行う。SSH は、サーバデーモンの sshd、基本的なクライアントである ssh、ファイル転送用途の scp および sftp、認証のための ssh-keygen, ssh-agent, ssh-add, ssh-askpass といったツール群で構成される。

3) OpenSSH の導入

OpenSSH は SSH の OSS 実装であり、暗号機能は OpenSSL で提供される。多くの Linux ディストリビューションでは、ディストリビューションをインストールした時点で OpenSSL、OpenSSH ともインストール済みであり、導入のための作業は不要である。

4) SSH の設定

SSH では、サーバ用の sshd_config、クライアント用の ssh_config ファイルにより各種設定を行う。

* sshd_config の主なパラメータ
  - Port　　sshd の TCP ポート。
  - PermitRootLogin　　root ログインの可否。セキュリティを考え「No」にする。
  - PasswordAuthentication　　ユーザ名/パスワードによる認証の可否。
* ssh_config の主なパラメータ
  - CheckHostIP　　known_hosts に無い IP アドレスの警告の有無。
  - Cipher　　ssh バージョン 1 で使う暗号の指定。
  - Ciphers　　shh バージョン 2 で使う暗号の指定。
  - PasswordAuthentication　　ユーザ名/パスワードによる認証の可否。

5) SSH の応用

* リモートからのコマンド実行

  ssh は一般に「ssh ユーザ名@ホスト」と入力してリモートシェルセッションのために使用するが、「ssh ユーザ名@ホスト」に続けてコマンドを入力することで、リモートからコマンドを直接実行することができる。ただし、対話的入力を必要とするコマンドは使用を避けたほうがよい。

* TCP ポートフォワーディングの例

```
ssh -2 -f mbauer@zippy -L 7777:zippy:110 sleep 600
```

[Linux サーバセキュリティ (オライリー・ジャパン 2003 年発行)より引用、抜粋]

この例では、SSH バージョン 2 で、zippy ホストに mbauer ユーザで接続し、「sleep 600」を開始後、ssh をバックグランドにフォークさせている。また、ローカルのポート 7777 を zippy ホストのポート 110 に転送している。この状態で、ローカルで TCP ポート 7777 を使うアプリケーションを実行すると、zippy ホストのポート 110 に転送される。ssh プロセスは 600 秒後に終了を試みるが、フォワードされた接続が閉じるまで終了を待つ。

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 I	基本
習得ポイント	I-21-9. SSL による仮想専用ネットワーク(VPN)の設定	
対応する コースウェア	第 7 回（SSL によるサーバ VPN と CA）	

I-21-9. SSL による仮想専用ネットワーク(VPN)の設定

Web の暗号化通信技術 SSL を利用して仮想専用ネットワーク(VPN)を実現する SSL-VPN の仕組みについて解説する。利用できるアプリケーションが限定されるが、導入が容易であることに言及する。

【学習の要点】

＊ Linux では、特別な機器を用意することなく、SSL-VPN サーバを構築することができる。

＊ SSL-VPN はクライアント側での導入が非常に容易である。

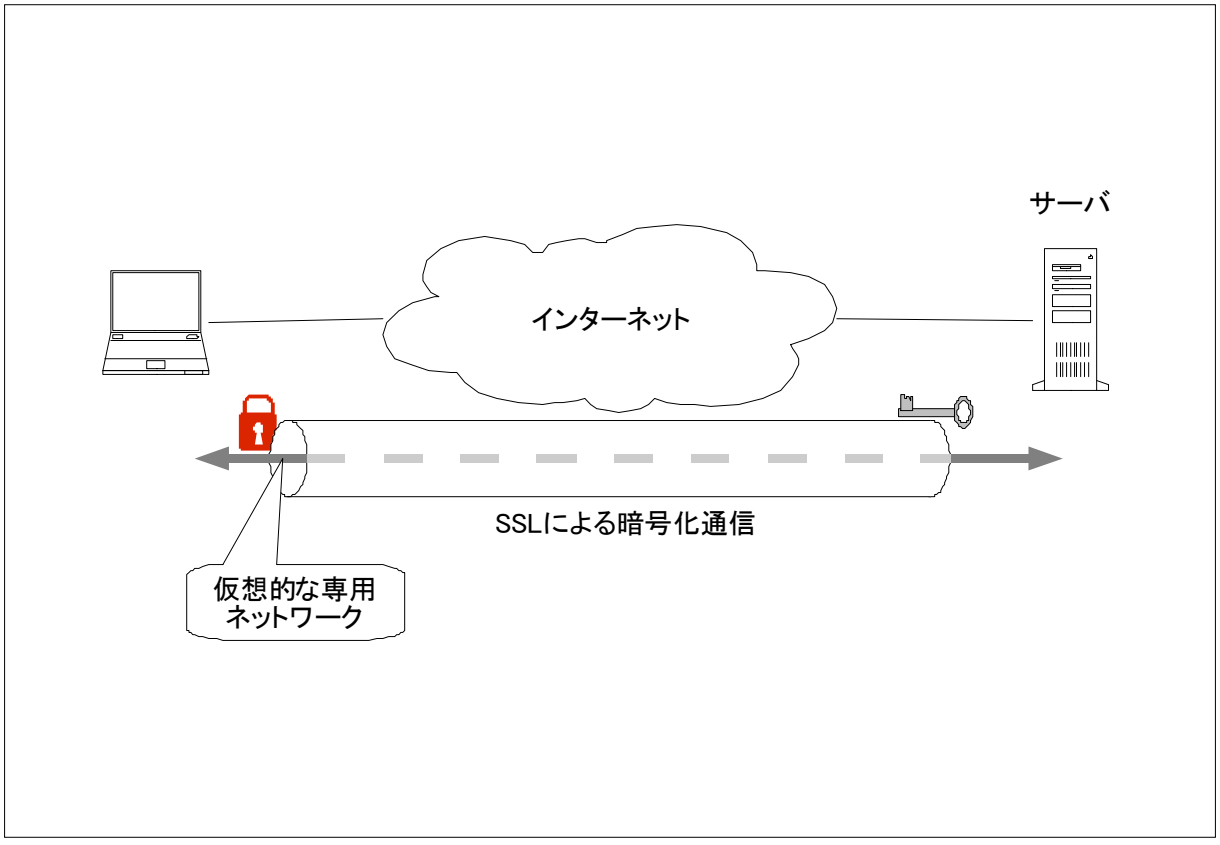

図 I-21-9.　SSL-VPN の概念

【解説】

1) SSL-VPN の仕組み

SSL-VPN は、暗号化通信のプロトコル SSL（Secure Socket Layer）を利用して実現する VPN(仮想専用ネットワーク)の技術全般を指す。SSL-VPN の動作には、Web ブラウザからのアクセスを通じてプロキシとしてアプリケーションを動作させるもの、SSL からのポートフォワーディングによってアプリケーションを動作させるものなどがある。

2) SSL-VPN の特徴

SSL が使える普通の Web ブラウザで対応することが可能で、別途クライアントソフトウェアをインストールする必要がなく、導入が容易であるといった利点がある。Java アプレットなどを使えば、ブラウザ以外のユーザインタフェースも利用できる。また、POP over SSL に対応したメールクライアントなど、SSL 対応のアプリケーションであればブラウザなしで利用できる。

3) Stunnel による SSL-VPN 構築

SSL-VPN を構築するためのソフトウェアはいくつかあるが、ここでは Stunnel を使ったポートフォワーディングのケースについて説明する。

＊ Stunnel とは
Stunnel は、さまざまなアプリケーションの通信データを SSL プロトコルで包むことができるツールである。Stunnel の暗号機能は OpenSSL で実現されている。また、TCPwrapper を利用したアクセス制御が可能である。

＊ Stunnel による SSL-VPN 実装手順の例(サーバ)

- サーバ証明書を作成し、設置する。
- アプリケーション用のポートを/etc/services に追加する。
- /etc/hosts.allow で接続を許可する。
- 次のコマンドを実行する。ここで、(1)は services に追加したサービス名、(2)は転送させるローカルポート名、(3)は hosts.allow で許可したサービス名、(4)は証明書ファイルのパスが入る。

  stunnel -d (1) -r localhost:(2) -p (4) -N (3)

＊ Stunnel による SSL-VPN 実装手順の例(クライアント)

- /etc/services にサーバに追加したものと同じポートを追加する。
- /etc/hosts.allow でサーバと同じ接続を許可する。
- 次のコマンドを実行する。ここで、(1)～(3)はサーバと同じ値、(5)サーバのホスト名が入る。

  stunnel -c -d (2) -r (5):(1) -N (3)

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 I	基本
習得ポイント	I-21-10. DNS に関するセキュリティ対策	
対応する コースウェア	第 8 回 (ドメインネームサービスのセキュリティ対策)	

I-21-10. DNS に関するセキュリティ対策

DNS (Domain Name System)の基本的な動作とDNS に求められるセキュリティ要件を解説する。標準的な DNS サーバの実装である BIND を紹介し、BIND におけるセキュリティ対策について述べる。

【学習の要点】

* BIND は最も普及している DNS 実装であり、バージョン 9 でセキュリティも大幅に強化されたが、古いバージョンからの移行が遅れている。
* BIND のセキュリティ強化のポイントは、named からの操作の制限と、named.conf の設定である。

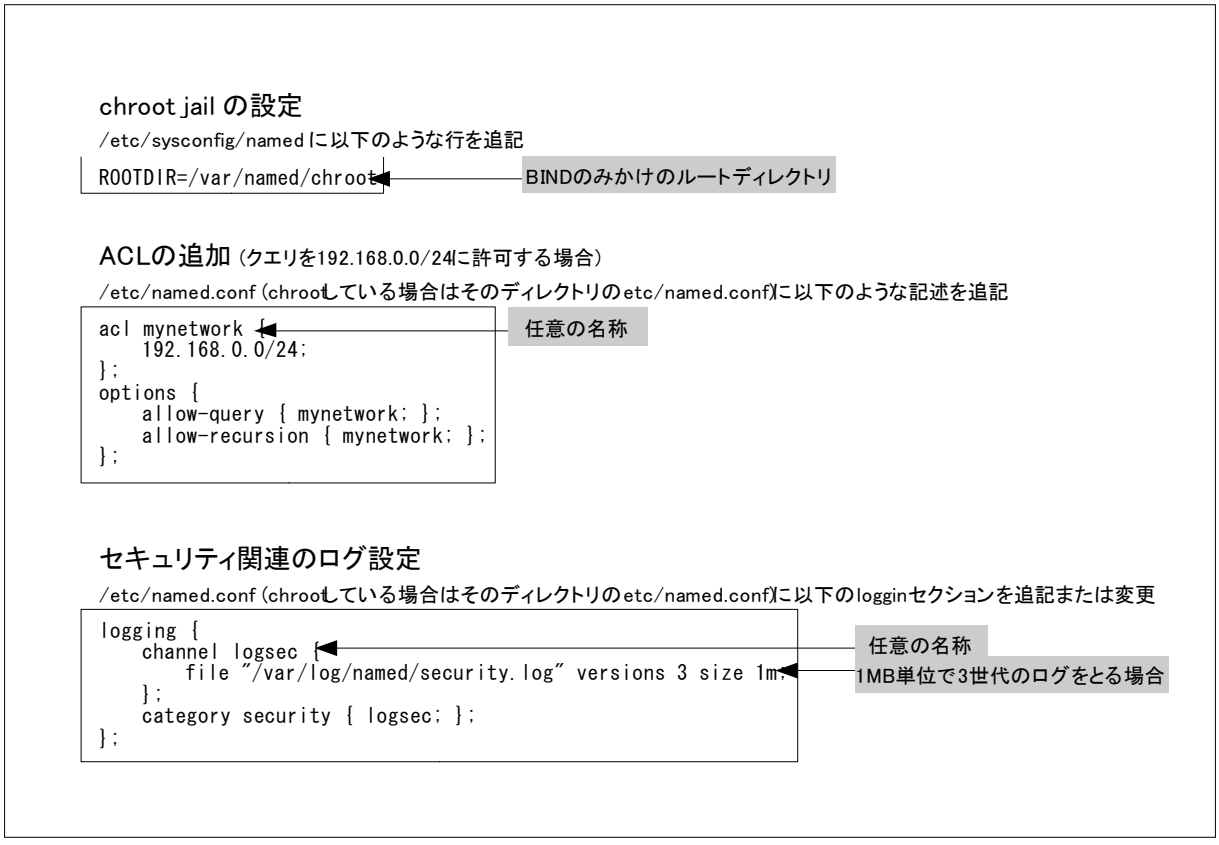

図 I-21-10.　BIND のセキュリティ対策のためのファイル設定例

【解説】

1) DNS(Domain Name System)の基本動作

DNS による通常の名前参照は以下のように行われる。

＊ クライアントは、ネームサーバ(A)に、問い合わせたいホスト名/ドメイン名を提示する。

＊ ネームサーバは、当該ドメイン情報を保持していない場合は、ルートネームサーバに問い合わせる。(再帰的問い合わせ)

＊ ルートネームサーバは、ネームサーバ A に、当該ドメイン情報を保持するネームサーバ(B)の情報を返す。

＊ ネームサーバ A は、ネームサーバ B に、問い合わせたいホスト名を提示する。

＊ ネームサーバ B は、ネームサーバ A に、ホストの IP アドレスを返す。

2) DNS に求められるセキュリティ要件

＊ DNS ソフトウェアを最新バージョンに保つ
使用している DNS にセキュリティホールが発見されたまま放置されると、そのセキュリティホールを狙った攻撃の影響を受けてしまう。

＊ 不必要な情報やサービスを提供しない
悪意のあるものに余計に情報やサービスを提供すると、それを利用して DNS を操作されるリスクが増大する。ネームサーバの IP アドレスを不必要に知らせない、DNS のレコードに不必要な情報を登録しない、再帰的な問い合わせを制限または無効化する、DNS サービスを公開部分と非公開部分とに分割する、などにより、余計な情報やサービスを提供しないようにする。

3) BIND のセキュリティ対策

BIND は、歴史があり、もっとも広く利用されている DNS ソフトウェアである。UNIX 系 OS の場合の具体的な対策は以下の通りである。

＊ バージョン 9 以降の最新バージョンを利用する。
バージョン 8 以前では脆弱性を抱えた設計となっている。バージョン 9 で大幅に設計しなおされ、セキュリティも強化された。

＊ named の実行を root 以外の制限ユーザ/グループで行う。
named は常駐する DNS サービスの名称である。named の実行を特権のないユーザ/グループで行うことで、万一 named がハイジャックされた場合でも、システムに対する操作が限定される。

＊ BIND がみなすルートディレクトリを「/」以外の安全な場所に変更する。
BIND には chroot jail という、named のルートディレクトリを設定できる。chroot jail をシステムのルート「/」以外にすることで、万一 named がハイジャックされた場合でも、操作可能なファイルが限定される。

＊ named.conf に ACL(アクセス制御リスト)を追加する。
named.conf は BIND の設定ファイルである。named.conf には ACL を記述でき、ホストアドレスやネットワークアドレスにより、実行可能な操作を制限できる。

＊ named.conf にログ設定を追加する。
named.conf に対し、セキュリティ関係のイベントをログに記録するように設定する。