

19. 暗号化に関する知識 II

1. 科目の概要

セキュリティ確保に必須の技術である暗号化や電子認証の仕組みについて解説する。VPN の設定方法や Public Key Infrastructure (PKI)による電子認証基盤の確立、Certification Authority (CA)の位置付けなど、セキュリティ確保のための様々な技術を解説する。

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
II-19-1. IPsecによるVPN通信	VPNとは何か、IPsecの機能や仕組みについて説明し、IPsecを利用したVPNの構築に関する手順や機能を解説する。また暗号化鍵の指定やAuthentication Header (AH)とEncapsulating Security Payload (ESP)といった二つのプロトコルの違いなど、IPsecによるVPNの実現に必要な項目について説明する。	12
II-19-2. IPsecの設定方法	動作モードの設定やSecurity Association (SA)の設定など、IPsecの具体的な設定について解説する。さらに、IPsecにより通信路が実際に暗号化されている状態を確認する方法についても説明する。	12
II-19-3. PKIの役割、仕組みと重要性	暗号化を運用するための基盤を提供するPublic Key Infrastructure (PKI)の目的や仕組み、役割、適用分野などを解説する。PKIを適用する分野や実際の運用状況、代表的なPKIの種類や特徴に関しても言及する。	13
II-19-4. CA局の仕組みとその機能	電子証明書に電子署名(Digital Signature)を行う第三者機関であるCertification Authority (CA)局の役割や目的を説明し、CA局の仕組みやCA局が提供する機能、CA局を構成するソフトウェア、CA局による暗号化の手順などについて解説する。	13
II-19-5. CA局の運用	CA局の運用環境やCA局の運用に必要な事項について解説する。また電子証明書の発行許可を与えるRegistration Authority (RA局、登録局)や、電子署名の有効性を確認するValidation Authority (VA局、検証局)、実際に電子証明書の発行を行うIssuing Authority (IA局、発行局)といった違いを説明する。	13
II-19-6. BtoC型の認証構造	BtoC型の認証構造を構築し、PKIの仕組みを検証する。CA局を構築するソフトウェアによりCA局を作成し、サーバに対するサーバ証明書とクライアントに対するクライアント証明書発行の動作や仕組みについて解説する。	14
II-19-7. BtoB型の認証構造	BtoB型の認証構造を構築し、PKIの仕組みを検証する。具体的な手順として、相互認証する相手認証局に対して相互認証証明書を相互に発行することで、サーバ間の相互認証を行う仕組みについて解説する。	14
II-19-8. 電子証明書の管理と発行 ※	電子証明書を利用する際に必要となる情報の収集方法や、発行した電子証明書の配送方法、電子証明書の活用方法など、電子証明書の発行とその管理に関する様々な項目について説明する。	14
II-19-9. ユビキタスネットワークの暗号化	オープンソースソフトウェアの新しい活用基盤である近傍無線技術やユビキタスネットワーク等の新しいネットワーク環境における暗号化の位置付けや意義、実装の仕様、課題、役割、必然性、メリットやデメリットについて説明する。	15
II-19-10. IPv6における暗号化	オープンソースソフトウェアのもうひとつの新しい活用基盤であるIPv6、その新しいネットワーク環境における暗号化の位置付けや意義、実装の仕様、課題、役割、必然性、メリットやデメリットについて説明する。	15

【学習ガイダンスの使い方】

- 「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。
- 「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。
- 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

「19. 暗号化に関する知識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>	<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による暗号化通信>	<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/oss/download/Model_Curriculum_05_19.pdf]

<IT 知識体系上の関連部分>

分野	科目名	IT 知識体系													
		1	2	3	4	5	6	7	8	9	10	11	12	13	
組織運営事項と情報システム	1	IT-1AS 情報保証と情報セキュリティ [19-1]	IT-1AS2 情報セキュリティの仕組み(可変)	IT-1AS3 運用上の問題 [19-5, 8]	IT-1AS4 ポリシー	IT-1AS5 攻撃	IT-1AS6 情報セキュリティ分野 [19-8]	IT-1AS7 フォレンジック(情報保証)	IT-1AS8 情報状況	IT-1AS9 情報セキュリティサービスマネジメント	IT-1AS10 評価モデル	IT-1AS11 脆弱性診断 [19-4]			
	2	IT-1SP 社会的な観点とプロフェッショナルとしての課題	IT-1SP2 プロフェッショナルとしてのコミュニケーション	IT-1SP3 コンピュータの歴史と社会環境	IT-1SP4 チームワーク	IT-1SP5 知的財産権	IT-1SP6 コンピュータの法的問題	IT-1SP7 組織の中のIT	IT-1SP8 プロフェッショナルとしての倫理的な問題と責任	IT-1SP9 プライバシーと個人の自由					
応用技術	3	IT-1W 情報管理	IT-1W1 情報管理の概念と基礎	IT-1W2 データベース関係性言語	IT-1W3 キーワードアーキテクチャ	IT-1W4 データモデリングとデータベース設計	IT-1W5 データと情報の管理	IT-1W6 データベースの応用分野							
	4	IT-1RS Webシステムとその技術	IT-1RS1 Web技術	IT-1RS2 情報データベース	IT-1RS3 デジタルメディア	IT-1RS4 Web開発	IT-1RS5 直感性	IT-1RS6 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-1PF プログラミング基礎	IT-1PF1 基本データ構造	IT-1PF2 プログラムの基本的構成要素	IT-1PF3 オブジェクト指向プログラミング	IT-1PF4 アルゴリズムと問題解決	IT-1PF5 イベント駆動プログラミング	IT-1PF6 高階							
	6	IT-1PT 技術を統合するためのプログラミング	IT-1PT1 システム間連携	IT-1PT2 データやり取りと交換	IT-1PT3 統合的コーディング	IT-1PT4 スクリプトプログラミング手法	IT-1PT5 ソフトウェアセキュリティの実現 [19-2]	IT-1PT6 種々の問題	IT-1PT7 プログラミング言語の概要						
システム構築	7	IT-1SE ソフトウェア工学	IT-1SE0 歴史と概要	IT-1SE1 ソフトウェアプロセス	IT-1SE2 ソフトウェアの要求と仕様	IT-1SE3 ソフトウェアの設計	IT-1SE4 ソフトウェアのテストと検証	IT-1SE5 ソフトウェアの保守と検証	IT-1SE6 ソフトウェア開発・保守ツールと環境	IT-1SE7 ソフトウェアプロジェクト管理	IT-1SE8 言語翻訳	IT-1SE9 ソフトウェアのフォールトトレランス	IT-1SE10 ソフトウェアの構成管理	IT-1SE11 ソフトウェアの標準化	
	8	IT-1SA システムインテグレーションとアーキテクチャ	IT-1SA1 要求仕様	IT-1SA2 調達/手配	IT-1SA3 インテグレーション	IT-1SA4 プロジェクト管理	IT-1SA5 システム品質保証	IT-1SA6 組織の特性	IT-1SA7 アーキテクチャ						
ネットワーク	9	IT-1NE ネットワーク	IT-1NE1 ネットワークの基礎	IT-1NE2 ルーティングとスイッチング	IT-1NE3 物理層	IT-1NE4 セキュリティ	IT-1NE5 テラリケーション分野	IT-1NE6 ネットワーク管理							
	10	IT-1NK ネットワーク	IT-1NK0 歴史と概要	IT-1NK1 通信ネットワークのアーキテクチャ	IT-1NK2 通信ネットワークのプロトコル	IT-1NK3 LANとMAN	IT-1NK4 クラウド環境	IT-1NK5 ネットワークのセキュリティと整合性	IT-1NK6 ワイヤレスネットワークのセキュリティとモビリティ	IT-1NK7 テータ連携	IT-1NK8 端末機器向けネットワーク	IT-1NK9 通信技術	IT-1NK10 性能評価	IT-1NK11 ネットワーク管理	IT-1NK12 性能と信頼
プラットフォーム	11	IT-1PI プラットフォーム技術	IT-1PI1 オペレーティングシステム	IT-1PI2 データベースと連携	IT-1PI3 コンピューティングプラットフォーム	IT-1PI4 デバイスドライバ	IT-1PI5 ファームウェア	IT-1PI6 ハードウェア							
	12	IT-1OS オペレーティングシステム	IT-1OS0 歴史と概要	IT-1OS1 並行性	IT-1OS2 スケジューリングとプロセス管理	IT-1OS3 メモリ管理	IT-1OS4 セキュリティと保護	IT-1OS5 ファイル管理	IT-1OS6 リアルタイムOS	IT-1OS7 OSの進化	IT-1OS8 設計の原則	IT-1OS9 テキスト管理	IT-1OS10 システム性能評価		
ハードウェア	13	IT-1CA コンピュータアーキテクチャ	IT-1CA0 歴史と概要	IT-1CA1 コンピュータアーキテクチャの基礎	IT-1CA2 メモリシステムの構成とアーキテクチャ	IT-1CA3 インタフェースと通信	IT-1CA4 パラメータシステム	IT-1CA5 アプリケーション	IT-1CA6 性能・コスト評価	IT-1CA7 分散処理	IT-1CA8 コンピュータによる計算	IT-1CA9 性能向上	IT-1CA10 性能向上		
	14	IT-1IF IT基礎	IT-1IF1 ITの一般的なテーマ	IT-1IF2 組織の問題	IT-1IF3 ITの歴史	IT-1IF4 IT分野(学際)と関連のある分野(学際)	IT-1IF5 応用領域	IT-1IF6 IT分野における管理・統計学の活用							
情報処理推進機構にまつものの	15	IT-1ESY 組み込みシステム	IT-1ESY0 歴史と概要	IT-1ESY1 組み込みシステムアーキテクチャ	IT-1ESY2 実用設計	IT-1ESY3 組み込みシステム設計	IT-1ESY4 組み込みシステム設計	IT-1ESY5 ライフサイクル	IT-1ESY6 要件分析	IT-1ESY7 仕様設計	IT-1ESY8 構造設計	IT-1ESY9 テスト	IT-1ESY10 プロジェクト管理	IT-1ESY11 移行設計(ハードウェア・ソフトウェア)	IT-1ESY12 実装
		IT-1ESY13 リアルタイムシステム設計	IT-1ESY14 組み込みシステムアーキテクチャ	IT-1ESY15 組み込みシステム設計	IT-1ESY16 組み込みシステム設計	IT-1ESY17 ツールによる開発	IT-1ESY18 ネットワーク組み込みシステム	IT-1ESY19 インタフェース設計	IT-1ESY20 センサシステム	IT-1ESY21 デバイスドライバ	IT-1ESY22 メンテナンス	IT-1ESY23 専門ソフトウェア	IT-1ESY24 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 固有の項目は、PKI に関するソフトウェアの OSS 関連情報が該当する。他の項目は VPN などを運用する上で必要となる知識を掘り下げている。

科目名	第12回	第13回	第14回	第15回
19. 暗号化に関する知識Ⅱ	(1)IPsec の設定	(1)PKI の仕組みと特徴	(1)B to C 形態での認証構造の構築	(1)暗号化の新しい活用シーン
	(2)暗号化の状態確認	(2)CA 局の仕組みとその機能 (3)CA 局の運用	(2)B to B 形態での認証構造の構築	

(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	19. 暗号化に関する知識	応用
習得ポイント	II-19-1. IPsec による VPN 通信	
対応する コースウェア	第 12 回 (VPN 通信の構築)	

II-19-1. IPsec による VPN 通信

VPN とは何か、IPsec の機能や仕組みについて説明し、IPsec を利用した VPN の構築に関する手順や機能を解説する。また暗号化鍵の指定や Authentication Header (AH) と Encapsulating Security Payload (ESP) といった二つのプロトコルの違いなど、IPsec による VPN の実現に必要な項目について説明する。

【学習の要点】

- * VPN とは公衆網であるコンピュータネットワークを利用して、ポイント間を認証化や暗号化手法で結ぶ仮想専用ネットワークである。
- * VPN を実現する手段として主に IPsec を用いた IPsec-VPN と SSL を用いた SSL-VPN がある。
- * IPsec では IP ヘッダの後ろにアタッチする拡張ヘッダを利用して暗号化機能と認証機能を実装する。
- * 暗号化データ + 暗号化ヘッダ + IP ヘッダを ESP (Encapsulated Security Payload) という。
- * IPsec を用いた VPN には、アウトサイドトンネル/インサイドトンネルという二つのタイプがある。

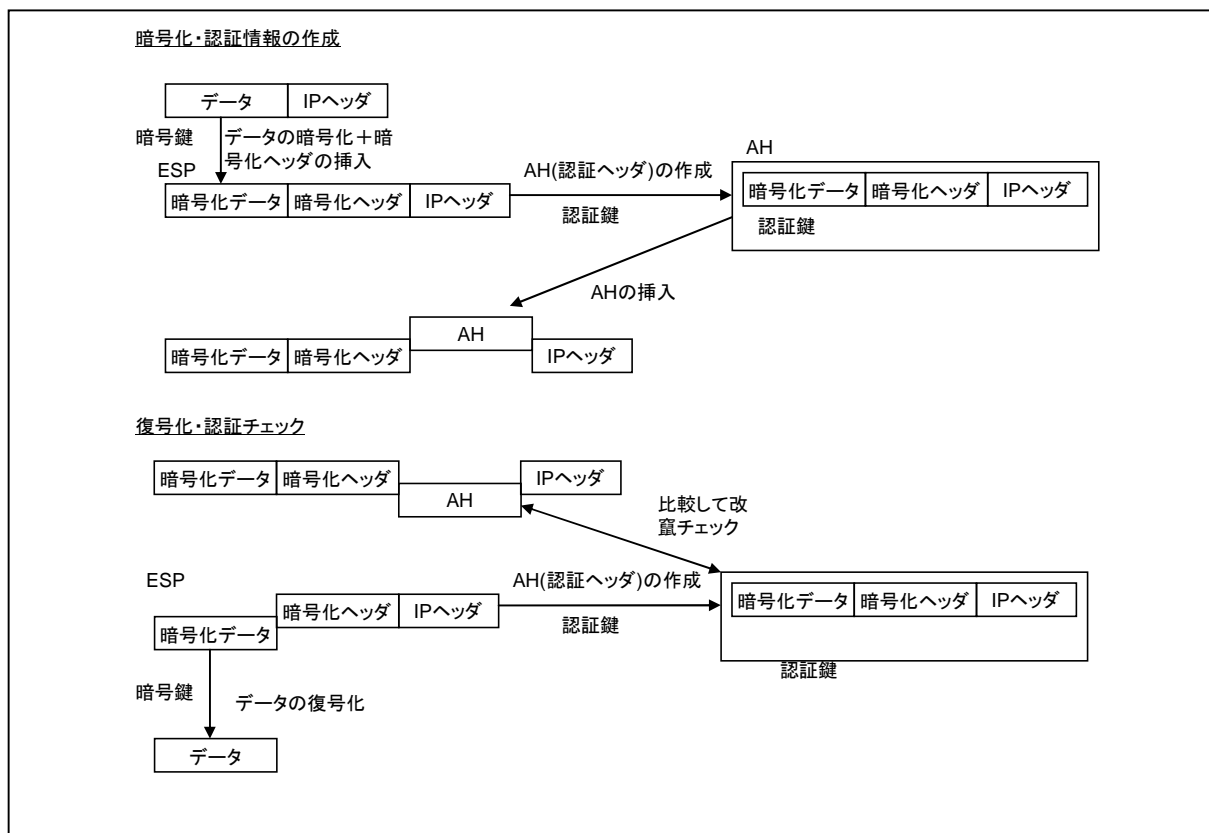


図 II-19-1. IPsec による VPN 通信

【解説】

1) VPNとは

- * VPNとは公衆網であるコンピュータネットワークを利用して、ポイント間を認証化や暗号化手法で結ぶ仮想専用ネットワークである。VPNを用いてポイント間を接続すれば、同じLAN環境を共有することができる。
- * VPNを実現する手段として主にIPsecを用いたIPsec-VPNとSSLを用いたSSL-VPNがある。

2) IPsecの仕組み

- * IPSecではIPヘッダの後ろにアタッチする拡張ヘッダを利用して暗号化機能と認証機能を実装する。つまり拡張ヘッダにより暗号情報、認証情報をやりとりする。
- * 暗号化/認証化には暗号鍵、認証鍵が必要であるが、これはホスト間で予め設定されている必要がある。
- * 暗号化・認証情報の作成手順は次の通り
 - まずデータ+IPヘッダがあるとする。
 - データを暗号鍵で暗号化する。これをデータ部に戻した後に、暗号化されたことを明示する暗号化ヘッダを、データ部とIPヘッダの間に挿入する。この暗号化データ+暗号化ヘッダ+IPヘッダをESP(Encapsulated Security Payload)という。
 - ESPに対して認証鍵をもちいて認証ヘッダを作成する。これをAH(Authentication Header)という。
 - 上記のAHを、暗号化ヘッダとIPヘッダの間に挿入する。この暗号化データ+暗号化ヘッダ+AH+IPヘッダの一体となったパケットを通信するホストに送信する。
- * 復号化・認証情報のチェックの仕組みは次の通り
 - 送信元から受け取ったパケットからAHを除いた暗号化データ+暗号化ヘッダ+IPヘッダについて、認証鍵をもちいて新たに認証ヘッダを作成する。この新たに作成した認証ヘッダとAHを比較し、改竄の有無をチェックする。
 - ESPからIPヘッダと暗号化ヘッダを取り除き、暗号化ヘッダの情報に基づき、暗号鍵を用いて復号化する。

3) IPsecを用いたVPNの実現

- * IPsecを用いてVPNを通信する場合、VPNトンネルをファイアウォールの外に確立するか、それともファイアウォールの中から確立するかで、アウトサイドトンネル/インサイドトンネルという二つのタイプがある。
- * インサイドトンネルの場合、あたかも同じLAN環境になったかのように振る舞うことができ、LANで利用できるアプリケーションはすべて利用できる。通常同じ会社の異なる拠点間を接続する場合に用いる。
- * アウトサイドトンネルの場合、トンネルを通じた通信がファイアウォールに阻まれるために、ファイアウォールが許可するアプリケーションの通信だけが利用できる。取引先企業との接続を行う場合はこの接続形態になる。

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	19. 暗号化に関する知識	応用
習得ポイント	II-19-2. IPsec の設定方法	
対応する コースウェア	第 12 回 (VPN 通信の構築)	

II-19-2. IPsec の設定方法

動作モードの設定や Security Association (SA)の設定など、IPsec の具体的な設定について解説する。さらに、IPsec により通信路が実際に暗号化されている状態を確認する方法についても説明する。

【学習の要点】

- * IPsec には二つのモードがあり、ひとつは Transport モード、もう一つは Tunnel モードである。Transport モードはデータ部だけを暗号化する。Tunnel モードは IP ヘッダも含めて暗号化する。
- * SA(Security Association)とはホスト同士が共有するアルゴリズムと鍵の情報である。
- * 鍵管理プロトコルとして IKE がある。

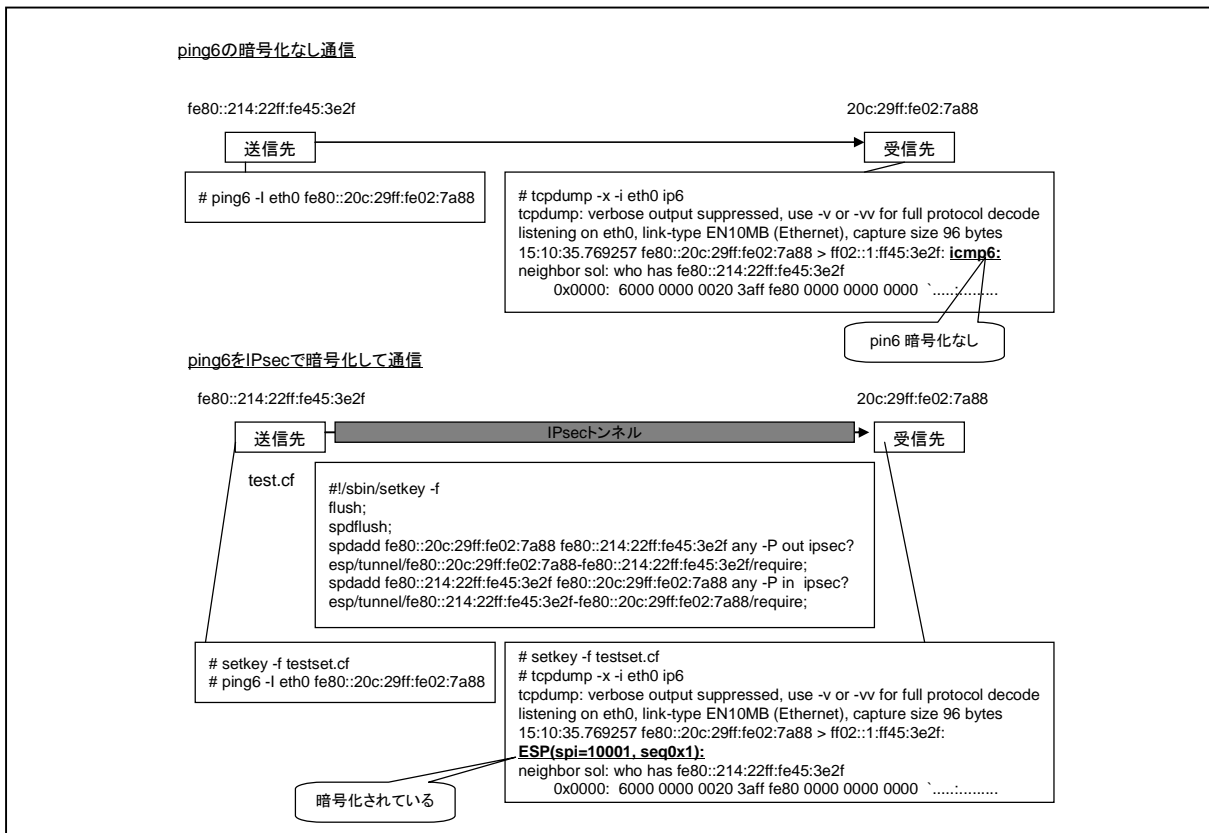


図 II-19-2. IPsec による暗号化の確認方法

【解説】

1) IPsec のモード

- * IPsec には二つのモードがあり、ひとつは Transport モード、もう一つは Tunnel モードである。
- * Transport モードはデータ部だけを暗号化し、IP ヘッダは暗号化されない。つまり通信内容だけを保護するモードが Transport モードである。
- * Tunnel モードは IP ヘッダも含めて暗号化する。このモードが VPN の基盤となっている。通常の VPN の場合、IPsec 機能を持ったルーターを設置して VPN を構築する 경우가多く、その場合 Tunnel モードの間はルーター間の暗号化処理、復号化処理によりパケット全体が保護されることになる。

2) SA とは

- * SA(Security Association)とは通信するピア間で合意されたアルゴリズムと鍵の情報である。
- * SA の要素は、鍵、暗号化、認証手段、そしてアルゴリズムで利用される追加パラメータである。
- * SA は単方向性であるために、セキュリティサービスごとに異なる SA が必要になる。例えば暗号化と認証という二つのサービスを利用する場合、暗号で一つの SA、復号で一つの SA という具合に一つのサービスで二つの SA を利用するため、二つのサービスを運用する場合は 4 つの SA が必要になる。

3) 鍵管理について

- * IPsec は暗号鍵の仕様を前提としているために、鍵管理の仕組みが別途必要になる。この鍵管理プロトコルとして IKE(Internet Key Exchange)がある。
- * IKE はネットワーク上で鍵を安全かつ自動的に交換するプロトコルである。
 - IKE は UDP ポート番号 500 上で通信され、いくつかのフェーズに分けて認証と暗号化を行い、鍵を安全に交換する。
 - IKE には v1 と v2 があり、IKEv1 は RFC2490 で規定されており、IKEv2 は RFC4306 で規定されている。
- * IKE による認証にはホスト間で SA を確立し、相互認証をおこなわなければならない。相互認証には二つフェーズがある。
 - フェーズ 1 は IKE で使用する SA の確立である。
 - フェーズ 2 は IPsec で使用する SA の確立である。

4) IPsec による通信の確認方法

- * ping6 コマンドを利用して IPsec による通信の暗号化を実際に体験するには次の手順を行う。
 - 暗号鍵、認証鍵や暗号化アルゴリズムの方法を記述した security policy (SP)を記述し、送信側受信側で、setkey コマンドでその SP を設定する。
 - 受信側で tcpdump で監視
 - 送信側で ping6 コマンドを発行
 - もしも IPsec が動作していれば、ダンプされるパケットには icmp ヘッダがなく、単に ESP という暗号化ヘッダの文言だけが表示される。

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	19. 暗号化に関する知識	応用
習得ポイント	II-19-3. PKI の役割、仕組みと重要性	
対応する コースウェア	第 13 回 (PKI(公開鍵暗号化基盤)の仕組み)	

II-19-3. PKI の役割、仕組みと重要性

暗号化を運用するための基盤を提供する Public Key Infrastructure (PKI)の目的や仕組み、役割、適用分野などを解説する。PKI を適用する分野や実際の運用状況、代表的な PKI の種類や特徴に関しても言及する。

【学習の要点】

- * PKI はユーザ同士の本人認証を、事前の直接的なコンタクトなしに、実現するコンピュータシステム基盤である。
- * PKIは公開鍵暗号方式を用いて、本人認証を行う仕組みであり、PKIの要素は証明書・認証局・リポジトリである。
- * PKI の適用分野は e-commerce、ドキュメントのリーガルドキュメント化、原本証明、公的機関への入札等の本人証明が必要なすべての分野に渡る。
- * PKI の運用状況は、Web においては SSL、メールの暗号化・署名に S/MIME、PDF などの電子文書の署名、スマートカードの本人認証、電子マネーの本人認証、無線 LAN の認証等がある。
- * 代表的な PKI の種類について、もっとも数が多いものは Windows Server に組み込まれた PKI であり、OSS では OpenCA、EJBCA、商用では Entrust 社、RSA Security 社など多数存在する。

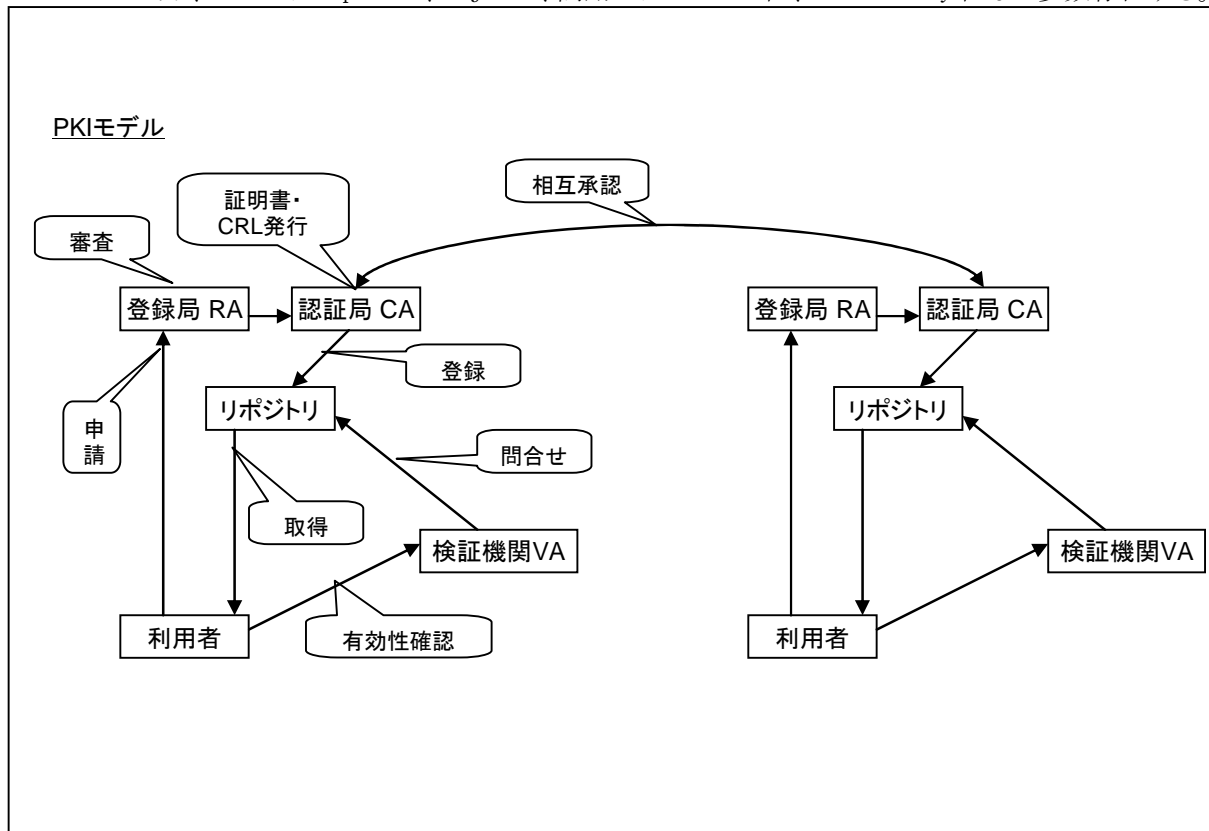


図 II-19-3. PKI の仕組みと流れ

【解説】

1) PKI とは

- * PKI はユーザ同士の本人認証を、事前の直接的なコンタクトなしに、実現するコンピュータシステム基盤である。コンタクトなしに認証を実現するためには、信頼できる第三者機関(TTP: Trusted Third Party)が信頼関係を確立するための重要な責をもっている。
- * PKI は公開鍵暗号方式を用いて、本人認証を行う仕組みであり、PKI モデルの要素は次の通りである。
 - 認証局(CA: Certification Authority)
秘密鍵と公開鍵の鍵ペアの所持者に対して公開鍵証明書を発行する機関である。CA が証明書を発行するさいにはRAの審査が終了していることが必要である。CAは証明書を発行するさいに、自分自身の鍵をもちいて、所持者の証明書に署名をして、リポジトリに登録する。これをもってCAが所持者に信頼を与えたとする。
 - 登録局(RA: Registration Authority)
公開鍵証明書を発行するために資格審査を行う要素である。
 - リポジトリ
公開鍵証明書を保管、開示するための手段である。
 - 公開鍵証明書
公開鍵ペアの所持者であることを証明した情報である。CAにより署名がされている。
 - 失効リスト(CRL: Certificate Revocation List)
有効期限切れや資格喪失等により証明できない証明書一覧を記述したリストである。CRLはCAにより署名される。
 - 証明書有効性検証機関(VA: Validation Authority)
公開鍵証明書が有効であるかどうかを検証する要素である。信頼されたCAにより署名が行われていること、CRLに載っていないこと、そして有効期限内であることの検証が行われる。
 - 証明書利用者
秘密鍵の所有者で、公開鍵証明書を利用する人やプログラムである。

2) PKI の適用

- * PKI の適用分野は e-commerce、ドキュメントのリーガルドキュメント化、原本証明、公的機関への入札等の本人証明が必要なすべての分野に渡る。
- * PKI の運用状況は、Web においては SSL、メールの暗号化・署名に S/MIME、PDF などの電子文書の署名、スマートカードの本人認証、電子マネーの本人認証、無線 LAN の認証等がある。
- * 代表的な PKI の種類について、もっとも数が多いものは Windows Server に組み込まれた PKI であり、OSSではOpenCA、EJBCA、商用ではEntrust社、RSA Security社など多数存在する。

3) PKI の規格

- * ITU-T X.509
- * IETF PKIX
- * PKCS 標準

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	19. 暗号化に関する知識	応用
習得ポイント	II-19-4. CA 局の仕組みとその機能	
対応する コースウェア	第 13 回 (PKI(公開鍵暗号化基盤)の仕組み)	

II-19-4. CA 局の仕組みとその機能

電子証明書に電子署名(Digital Signature)を行う第三者機関である Certification Authority (CA)局の役割や目的を説明し、CA 局の仕組みや CA 局が提供する機能、CA 局を構成するソフトウェア、CA 局による暗号化の手順などについて解説する。

【学習の要点】

- * CA 局は公開鍵証明書および失効リストを発行し、他の CA 局の信頼性を担保する役割を担っている。
- * CA 局の種類は、Public CA と Private CA の二種類がある。
- * CA 局の機能は、証明書の作成、証明書の登録・管理、CRL の発行、信頼モデルに基づいた信頼の構築である。
- * CA 局を構成するソフトウェアは、PKI を構築するために利用するソフトウェアである。例えば OpenSSL や Windows Server の CA 機能が利用される。
- * CA 局における暗号化手法は、公開鍵暗号化標準(PKCS)沿った暗号化が用いられる。

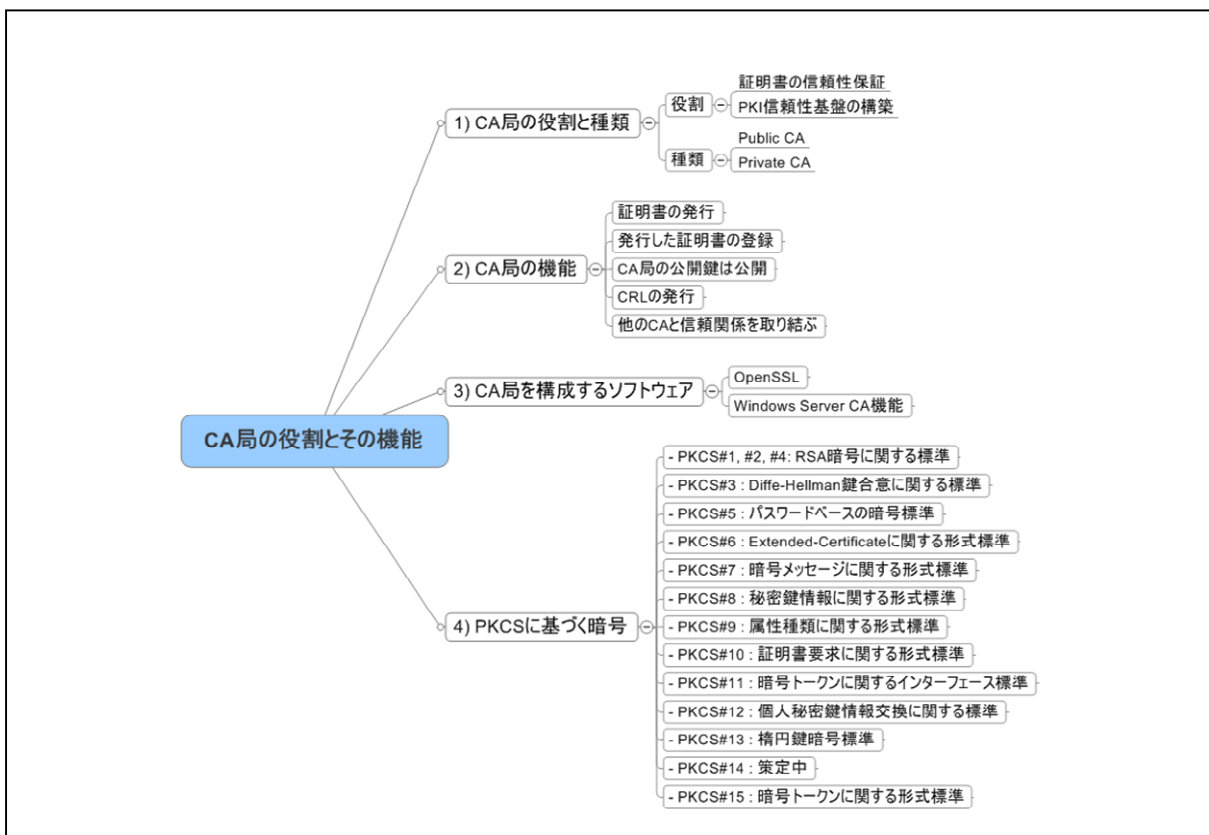


図 II-19-4. CA 局の役割とその機能

【解説】

1) CA 局の役割と種類

- * CA 局は PKI で利用される公開鍵証明書の信頼性を保証する役割を担っている。また、他の CA 局と相互認証を行うことにより、PKI の信頼性基盤を構築する礎となる。
- * CA 局の種類は次の二つである
 - Public CA: 第三者により発行される証明書で本人性を証明する。一般に広く利用される。
 - Private CA: 組織内や限られた範囲で利用される。

2) CA 局の機能と暗号化の手順

- * CA 局は、PKI の基盤に則り公開鍵証明書を発行し、第三者として本人性を保証する仕組みを提供する。
- * CA 局の暗号化手順は下記のとおりである。
 - 利用者の公開鍵に対して、CA 局の秘密鍵を用いて電子署名を行い、これを公開鍵証明書として発行する。
 - 発行した公開鍵証明書はリポジトリに登録され、利用者が証明書を受け取ることができるようにする。
- * CA 局の公開鍵は、公開鍵証明書の検証のために公開される。
- * 公開鍵証明書の失効したリスト(CRL)を発行する。
- * 信頼モデルに基づいて他の CA と信頼関係を取り結ぶ。
- * CA 局の秘密鍵は、PKI の信頼性基盤を形づくる上で最重要の要素であるために、厳重に保管されなければならない。

3) CA 局を構成するソフトウェア

広く利用されている CA 局を構成するソフトウェアは、オープンソースソフトウェアでは OpenSSL、企業のイントラネットでは Windows Server の CA 機能である。これ以外にも商用のソフトウェアが各ベンダから発売されている。

4) CA 局における暗号化手法

- * CA 局では暗号化手法として、米国 RSA 社の提唱する PKI を実現するための技術仕様のグループである PKCS (Public Key Cryptography Standards) に実質的に準拠しているといえる。
- * 現在、PKCS #1 から PKCS#15 までが策定されている。
- * PKCS#1 など、IETF (Internet Engineering Taskforce) の RFC といった標準技術団体に採用されているものもある。

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	19. 暗号化に関する知識	応用
習得ポイント	II-19-5. CA 局の運用	
対応する コースウェア	第 13 回 (PKI(公開鍵暗号化基盤)の仕組み)	

II-19-5. CA 局の運用

CA 局の運用環境や CA 局の運用に必要な事項について解説する。また電子証明書の発行許可を与える Registration Authority (RA 局、登録局)や、電子署名の有効性を確認する Validation Authority (VA 局、検証局)、実際に電子証明書の発行を行う Issuing Authority (IA 局、発行局)といった違いを説明する。

【学習の要点】

- * CA 局の運用は、認証局運用規定(CPS: Certificate Practice Statements)として策定される。CPS には、CA 局の運用に関わる情報や証明書のライフサイクル等の規定が必要である。
- * RA 局が発行許可を与えた電子証明書の発行は IA 局が行う。VA 局はその有効性を保証する。
- * 信頼性の担保という観点から、CA によって発行された公開鍵証明書にはライフサイクルという考え方をすることが重要である。ライフサイクルには証明書の発行からはじまり、失効、そして再発行に至るまでの証明書の各状態と CA 局の関わりが決められなければならない。

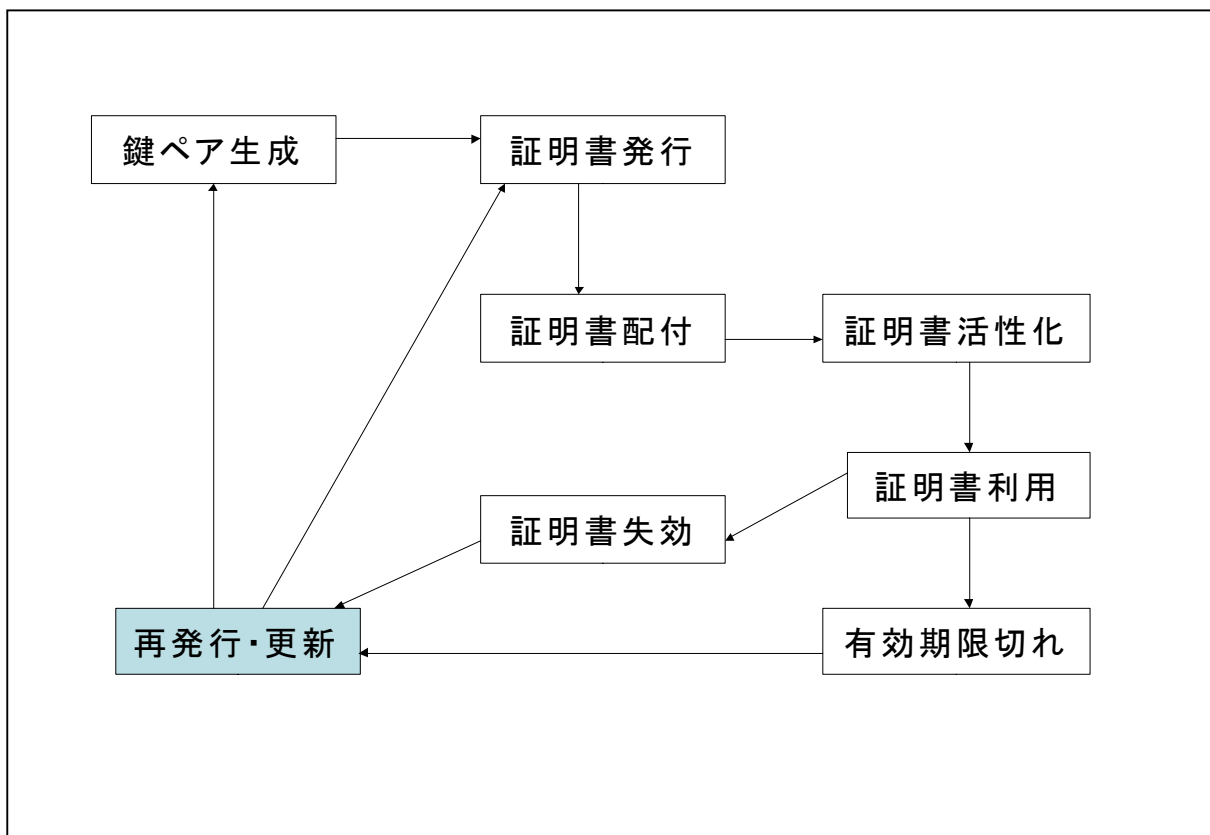


図 II-19-5. 公開鍵のライフサイクル

【解説】

1) CA 局の運用

CA 局の運用は、認証局運用規定(CPS: Certificate Practice Statements)として策定され、CA 運用の信頼性を高めるために利用される。CPS には以下の項目が必要である。

- * CA 局の義務と責務、資産の責任、解釈と実行、料金、公開とリポジトリ、準拠するべき監査、機密に関するポリシー、知的財産権に関する情報。
- * CA や RA に関して適用される認証手順要件。
- * CA, CA 証明書、RA、利用者に関する運用要件。
- * 物理的な手続き、スタッフのセキュリティに関するの制御要件。
- * CA 局の暗号鍵、リポジトリに関する保護要件。
- * 証明書と CRL のフォーマット要件。
- * CPS 自体の仕様書の管理要件。

2) RA 局、VA 局、IA 局

- * RA 局は、申請に基づき電子証明書の発行許可を与える。
- * VA 局は、CA 局とは別に電子証明書の有効性を保証する役割を担う。
- * IA 局は、RA 局の許可に基づき電子証明書を発行する。
- * 独自の基準で電子証明書を発行したい組織向けに各局の運営を支援するサービスが多くのベンダから提供されている。

3) 公開鍵証明書のライフサイクル

信頼性の担保という観点から、CA 局によって発行された証明書にはライフサイクルという考え方をすることが重要である。

- * 鍵ペア生成: 公開鍵と秘密鍵のペアの生成。利用者であるエンドエンティティで行う場合もある。
- * 証明書発行: RA 局の審査後に行う。有効期限を含める。
- * 証明書配付: 安全な手段で証明書を配布する。
- * 証明書開示: リポジトリへ利用者の証明書を開示する。
- * 証明書活性化: 利用者により証明書を活性化する。配布時点で活性化する運用もある。
- * 証明書利用
- * 証明書失効: 秘密鍵の信頼性の喪失、CA 秘密鍵の信頼性の喪失等により、有効期限前に証明書を失効させること。
- * 有効期限切れ: 証明書に記述された有効期限を超過すると証明書は失効する。
- * 再発行・更新: 失効した証明書を新たに発行すること。有効期限切れの場合は鍵はそのまま、期限だけを書き換えて更新する場合もある。

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	19. 暗号化に関する知識	応用
習得ポイント	II-19-6. BtoC 型の認証構造	
対応する コースウェア	第 14 回 (認証基盤構築実習)	

II-19-6. BtoC 型の認証構造

BtoC 型の認証構造を構築し、PKI の仕組みを検証する。CA 局を構築するソフトウェアにより CA 局を作成し、サーバに対するサーバ証明書とクライアントに対するクライアント証明書発行の動作や仕組みについて解説する。

【学習の要点】

- * BtoC 型の認証構造は、ルート証明書をクライアント側にインポートすることを期待できないモデルであり、クライアントソフトウェアにプリインストールされたルート証明書を利用する。
- * BtoC 型の認証構造の信頼モデルの根拠は、PKI を利用するアプリケーションのメーカーが選定する商用ルート CA の基準にある。
- * BtoC 型の認証構造の典型的な例は、WWW で頻繁に利用される SSL 通信である。

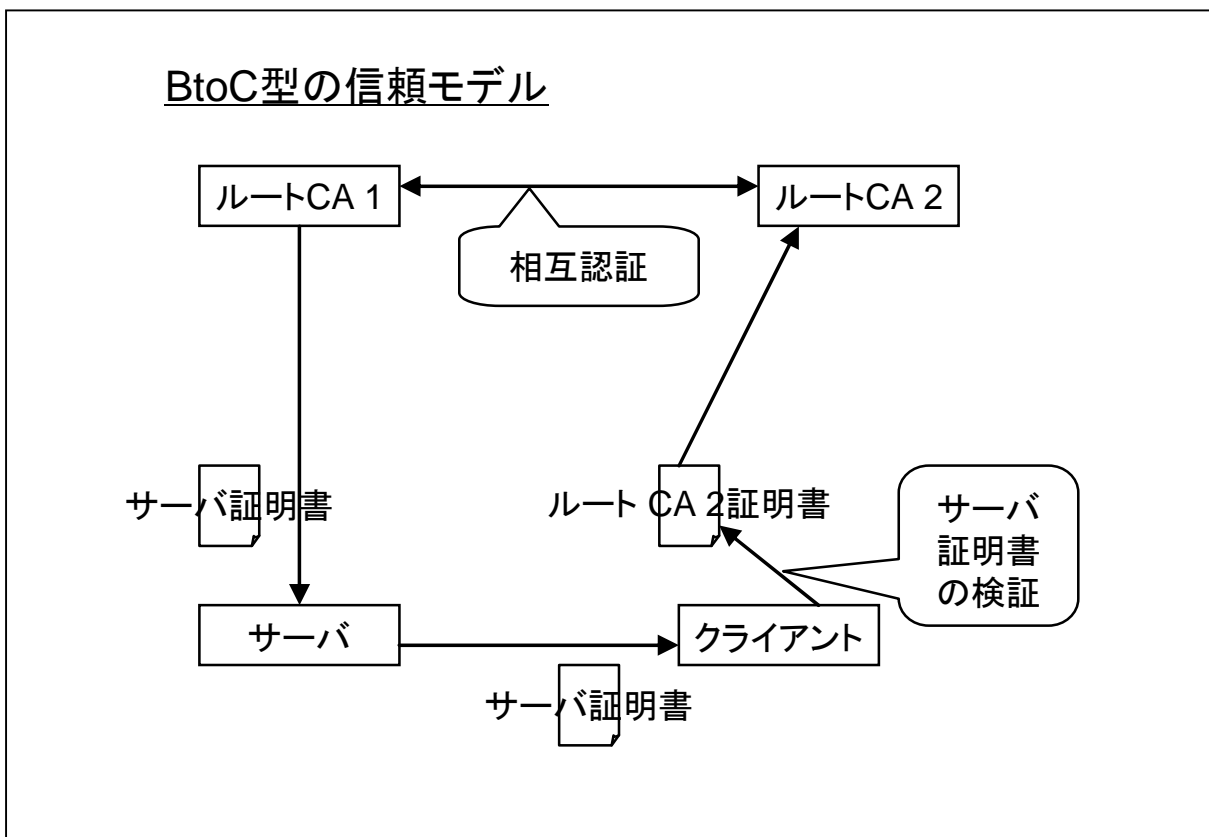


図 II-19-6. BtoC 型の認証構造

【解説】

1) BtoC 型認証構造

- * BtoC 型の認証構造は、ルート証明書をクライアント側にインポートすることを期待できないモデルであり、クライアントソフトウェアにプリインストールされたルート証明書を利用する。
- * サーバ側は一般的には商用のルート証明サービスを利用し、サーバ証明書を商用の証明書サービスに発行依頼をするか、自局の CA 局を商用のトラステッドツリーに組み込むサービスを利用するか、いずれかの手段をとる。
- * クライアント側は商用のルート証明書をプリインストールされている。その商用ルート CA の信頼性モデルに基づいてサーバのサーバ証明書の認証検証を行う。
- * 商用のルート CA としてベリサイン、グローバルトラスト、クロストラスト等会社があり、それぞれの会社が信頼できる第三者機関として、サーバの運営者を審査し、サーバ証明書を発行する。

2) BtoC 型の信頼モデル

BtoC 型の信頼モデルは一般には次のような形をとる。

- * 商用のルート CA はお互いの信頼性を相互認証している。
- * 商用ルート CA からサーバ証明書が発行される。
- * クライアントはサーバ証明書の検証を、プリインストールされた商用ルート CA の証明書を利用する。
- * プリインストールされた商用ルート証明書を利用するということは、クライアント側の信頼の根拠は、PKI を利用するアプリケーションのメーカーが選定する商用ルート CA の基準にあるということである。

3) SSL

BtoC 型の認証構造の典型的な例は、WWW で頻繁に利用される SSL 通信である。SSL 通信と特徴は次の通りである。

- * 相手認証および鍵交換には公開鍵暗号方式を利用するが、メッセージ認証にはマスターシークレットキーを利用した共通鍵暗号を利用して高速化を実現している。
- * サーバ・クライアント間のハンドシェイクプロトコルをもち、お互いの証明書を交換してメッセージ認証のマスターシークレットキーを生成する。
- * レコード層とそれ以外の二層に分割し、レコード層をハンドシェイクプロトコルから生成されたマスターシークレットキーを用いて暗号化し、メッセージ認証とする。

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	19. 暗号化に関する知識	応用
習得ポイント	II-19-7. BtoB 型の認証構造	
対応する コースウェア	第 14 回 (認証基盤構築実習)	

II-19-7. BtoB 型の認証構造

BtoB 型の認証構造を構築し、PKI の仕組みを検証する。具体的な手順として、相互認証する相手認証局に対して相互認証証明書を相互に発行することで、サーバ間の相互認証を行う仕組みについて解説する。

【学習の要点】

- * BtoB 型の認証構造は、相互認証モデルと呼ばれる認証構造をもつ。
- * 相互認証はお互いの CA 局について相互認証証明書(X-Cert)を発行して、信頼モデルを構築する。
- * 相互認証を行うときに重要なのは、利用者が安全に信頼ポイントまでの認証パスを構築することである。

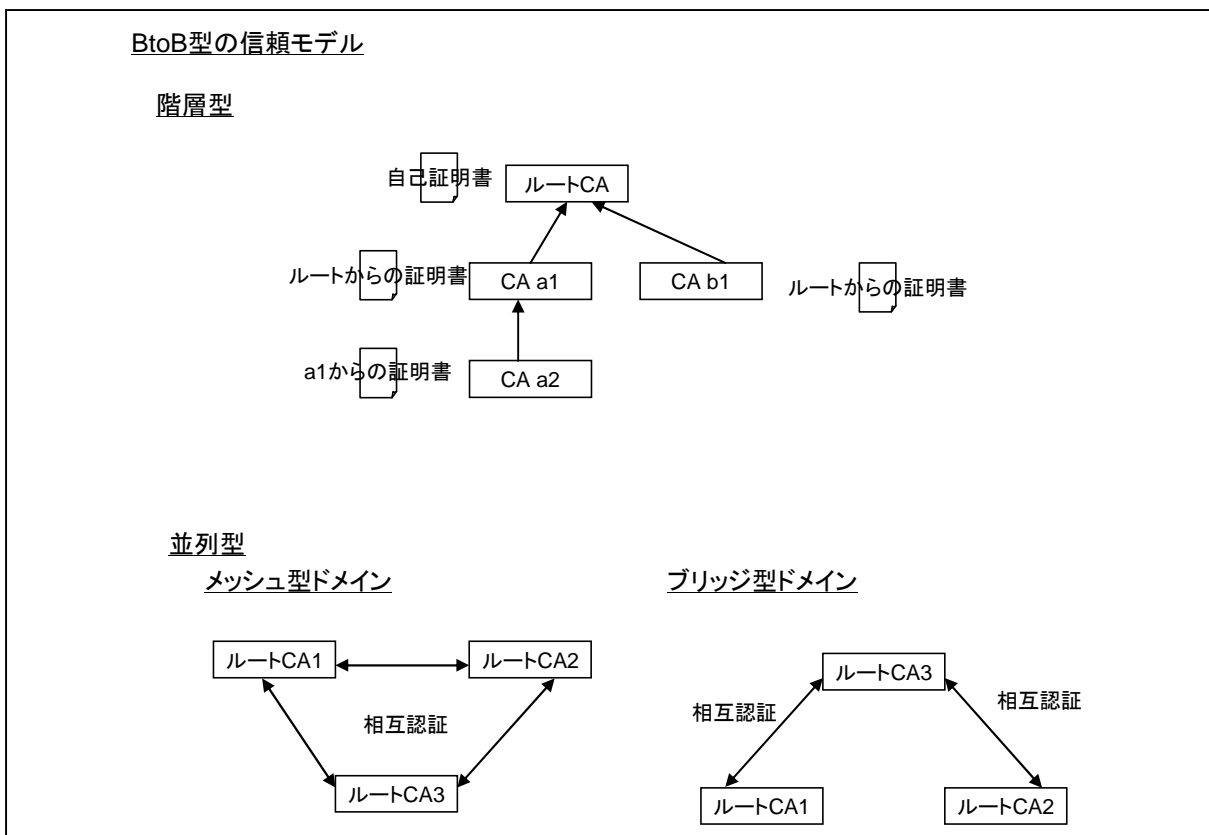


図 II-19-7. BtoB 型の認証構造

【解説】

1) BtoB 型の認証構造

BtoB 型の認証構造は相互認証モデルと呼ばれる認証構造をもつ。

- * 相互認証には大きく分けて次の二種類がある。
 - 階層型
相互証明書の発行方向は一方向である。階層型相互認証の下階層に位置する CA を中間 CA と呼ぶことがある。
 - 並列型
相互証明書の発行方向は双方向である。
- * 並列型相互認証は認証ドメインの役割に応じて更に次の二種類の構造に分けられる。
 - メッシュ型ドメイン
 - ブリッジ型ドメイン
- * 相互認証において発行される証明書を相互証明書という。
- * 相互認証を行うためには、当該の二つの CA が共通に信頼できる認証ポイントが必要であるか、証明書要求の発信元を確認するなんらかの手段である。

2) 相互証明書(X-Cert)

- * 相互証明書は同一認証ドメインであるかどうかによって次の二種類に分かれる。
 - ドメイン間相互証明書
 - ドメイン内相互証明書
- * 各 CA が持つのは相手が署名した相互証明書と自己署名証明書である。
- * 相互証明書の subject には認証された CA の名前が入り、issuer には認証した CA の名前が入る。

3) 認証パスの構築とポリシーの検証

相互認証を行うときに重要なのは、利用者が安全に信頼ポイントまでの認証パスを構築することである。

- * 認証パスを構築するには、鍵や証明書のライフサイクルが万全な CA を信頼ポイントとしなければならない。
- * CA 間の相互認証においては、各 CA ポリシー同士のマッピングが十分であることが必要である。このポリシーマッピングが各 CA 間で同等に行われるかどうかという検証が、ポリシー検証である。
- * ポリシーマッピングの状況は、CA 証明書の PolicyMapping 拡張領域に記述される。

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	19. 暗号化に関する知識	応用
習得ポイント	II-19-8. 電子証明書の管理と発行	
対応する コースウェア	第 14 回 (認証基盤構築実習)	

II-19-8. 電子証明書の管理と発行

電子証明書を利用する際に必要となる情報の収集方法や、発行した電子証明書の配送方法、電子証明書の活用方法など、電子証明書の発行とその管理に関する様々な項目について説明する。

【学習の要点】

- * 電子証明書の利用にあたっては、まずセキュリティポリシーの策定から取り組み、セキュリティ要件を定義する必要がある。
- * セキュリティポリシーは情報システムのセキュリティに関するすべての人、組織、建屋、機器、ソフトウェア、ネットワークの、セキュリティとしてあるべき姿を記述する。ただし、物理環境・組織の制約、運用及びコストの制約、そしてシステム要件のバランスをとる必要がある。
- * セキュリティ要件はセキュリティポリシーに沿って具体的なセキュリティ要件を定義するが、信頼が喪失されたときの損害のおおきさに基づいて策定されるべきである。

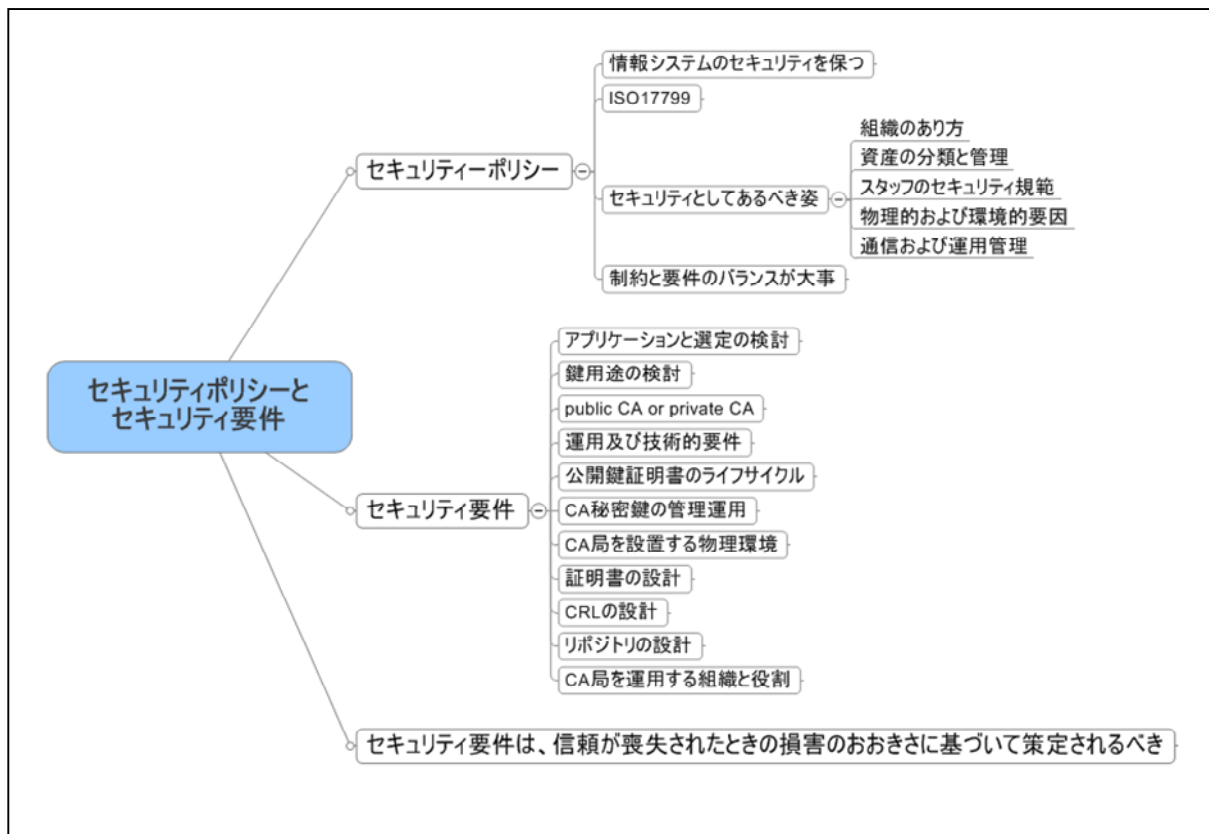


図 II-19-8. セキュリティポリシーとセキュリティ要件

【解説】

1) セキュリティポリシーとは

- * 情報システムのセキュリティを保つために必要な文書化された基本方針である。
- * 具体的な行動やシステムの個別設定を直接記述するものでない場合が多い。
- * 情報システムのセキュリティに関するすべての人、組織、建屋、機器、ソフトウェア、ネットワークの、セキュリティとしてあるべき姿を記述する。
- * ISO17799 の国際標準に沿うことが多い。
 - セキュリティとしての組織のあり方
 - 資産の分類と管理
 - スタッフのセキュリティ規範
 - 物理的および環境的要因のセキュリティ基準
 - 通信および運用管理に関する方針
- * 実際にセキュリティポリシーを作成するときは、物理環境・組織の制約、運用及びコストの制約、そしてシステム要件のバランスをとりながら、個別のシステムに合致させる必要がある。

2) セキュリティ要件

セキュリティ要件はセキュリティポリシーに沿って具体的な要件を定義するものであり、以下の項目を含む。

- * アプリケーションと選定の検討
- * 鍵用途の検討
- * public CA を利用するか、private CA を利用するか。
 - 運用及び技術的要件の定義
 - 公開鍵証明書のライフサイクルの明示と安全な鍵の配送方法
 - CA 秘密鍵の管理運用
 - CA 局を設置する物理環境の設計
 - 証明書の設計
 - CRL の設計
 - リポジトリの設計
- * CA 局を運用する組織と役割の検討
- * セキュリティ要件には、日本電子商取引組合(ECOM)がガイドラインとして提示している、次の三つのレベルがある。
 - 低レベル:暗号電子メールなどをイントラネット内で構築するレベル
 - 中レベル:比較的少額の取引が行われる環境に該当するレベル
 - 高レベル:組織間取引において高額な取引が行われる環境に該当するレベル
- * セキュリティ要件は、信頼が喪失されたときの損害の大きさに基づいて策定されるべきである。

3) 電子証明書の活用方法

- * BtoC では、e-commerce などでのフォーム入力内容の暗号化がある。
- * BtoB では、原本証明、公的機関への入札等の本人証明が必要な分野で利用されている。

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	19. 暗号化に関する知識	応用
習得ポイント	II-19-9. ユビキタスネットワークの暗号化	
対応する コースウェア	第 15 回 (暗号化・これからの活用シーンと課題)	

II-19-9. ユビキタスネットワークの暗号化

オープンソースソフトウェアの新しい活用基盤である近傍無線技術やユビキタスネットワーク等の新しいネットワーク環境における暗号化の位置付けや意義、実装の仕様、課題、役割、必然性、メリットやデメリットについて説明する。

【学習の要点】

- * 近傍無線技術の実用例としては、無線 LAN や Bluetooth、ユビキタスネットワークの例としては非接触スマートカードや RFID などがあり、オープンソースソフトウェアでも利用されている。
- * 共通の特徴として無線であることから、利用者の利便性が高いといえるが、意図しない他社の傍受の危険性も高く、常にセキュリティの強化が求められている。
- * 特定のベンダによる技術に依存している場合や電波を利用することによる法制面での規制も配慮する必要がある。

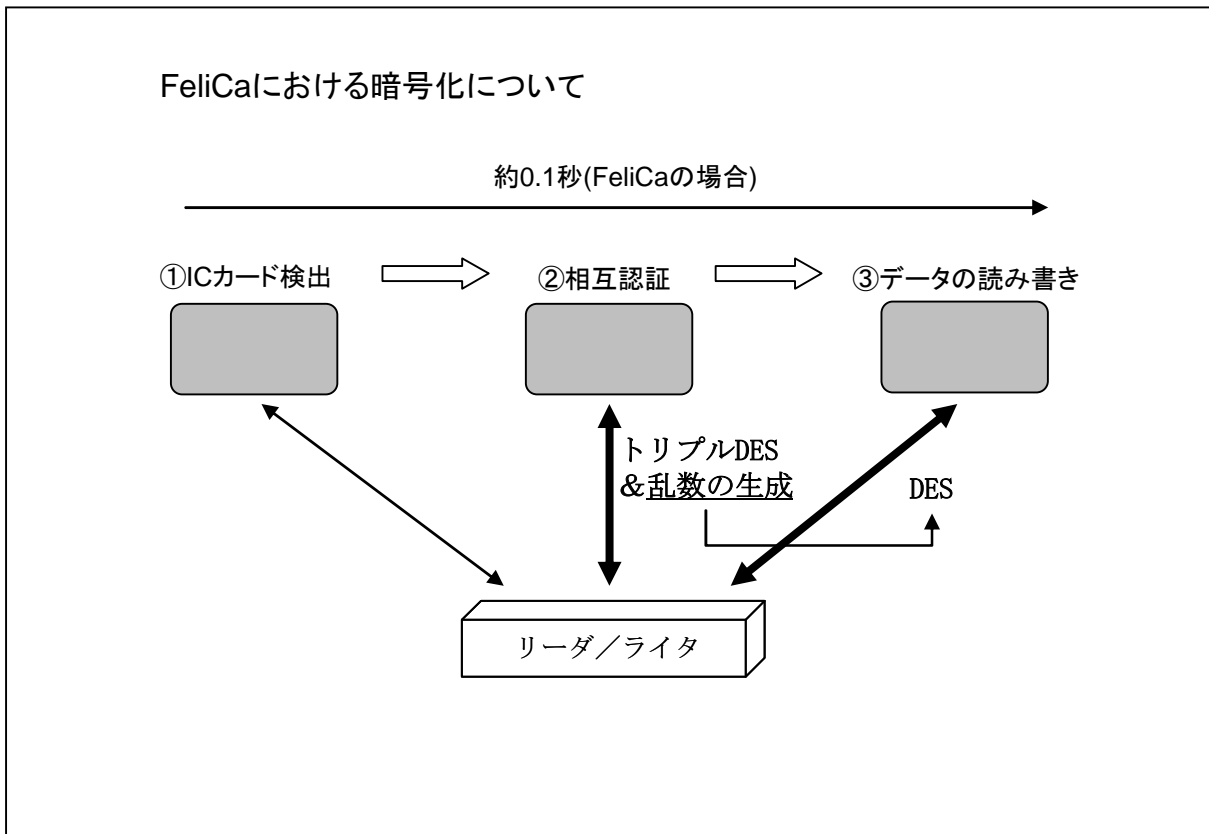


図 II-19-9. ユビキタスネットワークにおける暗号化の例

【解説】

1) 近傍無線技術・ユビキタスネットワークの暗号化の例と課題

* 近傍無線技術:無線 LAN

- 無線 LAN 技術においてセキュリティ上の問題点は3つある。アクセスポイントが発見されやすい、通信データが傍受されやすい、関係ないユーザに使われやすい、という点である。特に二点目のデータの漏洩に対して、暗号化技術が適用される。
- 無線 LAN における暗号化規格として、業界団体である Wi-Fi Alliance が 2004 年 9 月に発表した WPA2 がある。
- 2002 年 10 月に発表された WPA に比べ、改良版の WPA2 では強力な暗号化方式である AES をベースにした、CCMP と呼ばれるプロトコルを使用している。なお、WPA は IEEE 802.11i が策定される以前に Wi-Fi Alliance によって作成されたので準拠していなかったが、WPA2 は IEEE 802.11i を準拠している。
- 2006 年 3 月より、WPA2 をサポートすることが Wi-Fi 認定ロゴを製品に添付する条件になった。

* ユビキタスネットワーク:FeliCa

- FeliCa とは SONY が開発した非接触 IC カード技術で、現在日本では最も普及している。
- リーダ/ライターによる処理は、IC カードの検出、相互認証、データの読み書きという順序で行われ、FeliCa では、相互認証にはトリプル DES を使用し、通信データの暗号化には DES を使用している。
- 特に通信データの暗号化鍵は、相互認証時に乱数を生成させ、それを利用することで、動的に鍵は生成し、「なりすまし」を避けている。
- 共通鍵暗号化方式を使用する理由としては、ラッシュ時における Suica の利用に見られるように、高速処理が求められるという点が挙げられるが、より安全性が高い暗号化方式として公開鍵方式が挙げられるが、一般的に処理に時間がかかってしまうという欠点がある。

2) メリットとデメリット

- * メリットとして、無線であることから利便性が高いことが上げられる。
- * デメリットとしては、メリットの裏返しとなるが無線であるが故に意図しない他者による傍受の危険性にさらされている点があげられる。このため常に通信の暗号化の強化が求められている。

3) オープンソースソフトウェアの活用と制約

- * 近傍無線技術では、クライアント用に無線 LAN や Bluetooth の Linux スタックである BlueZ などが提供され利用されている。
- * ユビキタスネットワークにおいては、OS やミドルウェアなどの基盤としてオープンソースソフトウェアが利用されている。
- * 暗号化の実現にあたって、特定のハードウェアやソフトウェアに依存する仕様の場合には、利用したいオープンソースソフトウェアに対応したドライバや SDK の存在が必須なため制約となる場合がある。

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	19. 暗号化に関する知識	応用
習得ポイント	II-19-10. IPv6 における暗号化	
対応する コースウェア	第 15 回 (暗号化・これからの活用シーンと課題)	

II-19-10. IPv6 における暗号化

オープンソースソフトウェアのもうひとつの新しい活用基盤である IPv6、その新しいネットワーク環境における暗号化の位置付けや意義、実装の仕様、課題、役割、必然性、メリットやデメリットについて説明する。

【学習の要点】

- * IPv6 では標準的なプロトコル仕様として、暗号化を含むセキュリティ機能を IPsec として組み込んでいる。
- * エンドツーエンドのセキュリティを確保できる点が、IPv6 のもっともメリットがある点である。
- * IPsec を利用する場合、通信経路でアドレスを変更する NAT により、無効化されるので注意する必要がある。

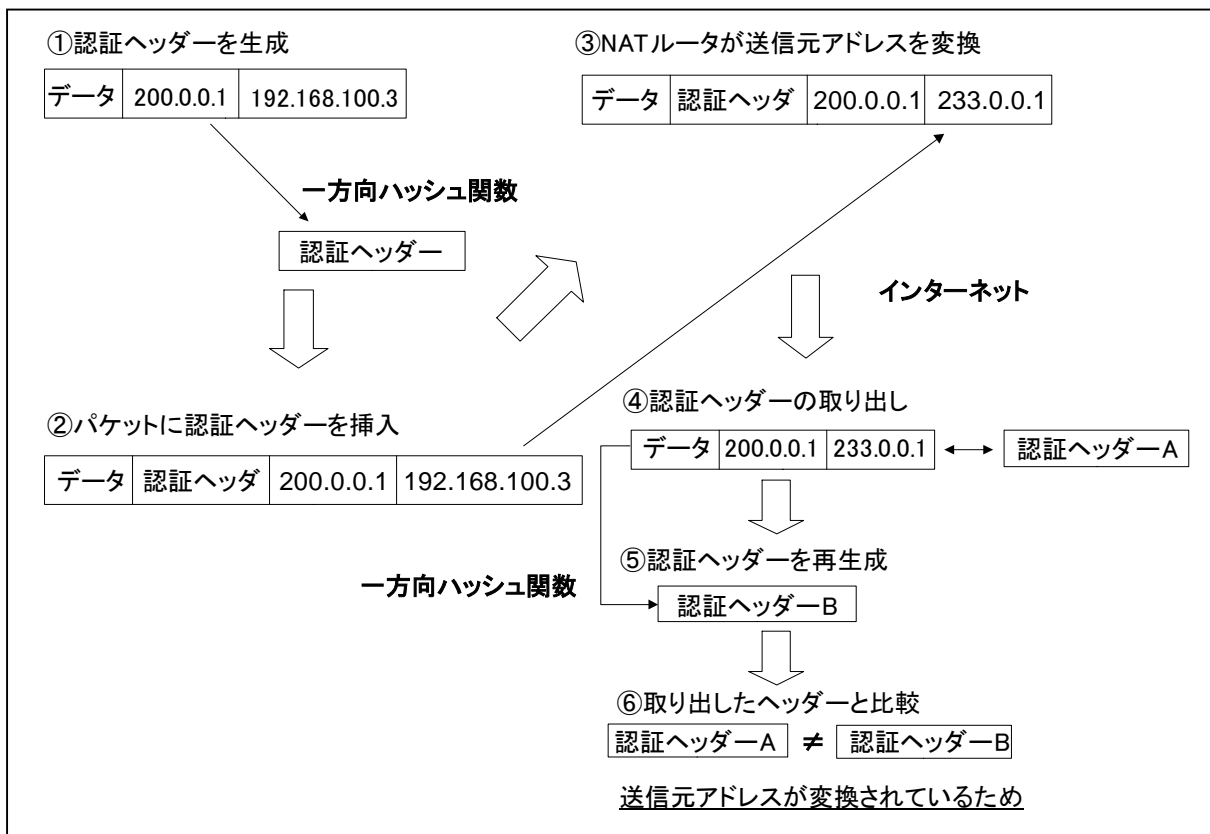


図 II-19-10. NAT による IPsec の無効化

【解説】

- 1) IPv6 における IPsec とは IP パケットの安全性と信頼性を高めるプロトコルである。
 - * IPv6 において IPsec は標準で実装される。それに対して、IPv4 においては標準ではない。
 - IPv4 においては IP アドレスが不足しているため、一般には NAT ルーターにおいてプライベートアドレスとグローバルアドレスの変換が行われている。しかし、このように通信経路でアドレス変換が行われてしまうと、認証ヘッダが食い違い IPsec を使用できない。
 - * IPsec では安全性を確保するために暗号化機能を持つ。また信頼性を確保するために、データが改竄されていないかを調べる認証機能を持つ。これらの機能はそれぞれ暗号化ヘッダと認証ヘッダ (AH) と呼ばれる個別の拡張ヘッダを使用する。
 - 暗号化ヘッダのアルゴリズムとして、対称型暗号に基づいた鍵付きメッセージ認証コードである DES やトリプル DES が使用される。
 - 認証ヘッダのアルゴリズムとして、一方向ハッシュ関数である SHA-1 や MD5 が使用される。
- 2) IPv6 におけるセキュリティ上の問題について
 - * IPv6 における IPsec は暗号化に使われる鍵の交換方法は規定されていない。そのため、鍵配送には手作業かあるいは自動になる。最近では、IPv6 用の集中証明書サーバとして、IKEv2 プロトコルをサポートするサーバによって簡略化された。
 - * エンドツーエンドの IPsec は IPv6 の大きな利点である。しかし、そのためにエンドポイント間に置かれた機器が、暗号化されたパケットを復元して検査することが不可能になってしまう。もし、すべての暗号鍵を検査のために集中管理させてしまうと、今度はそこにクラッカーが侵入されるとすべての暗号鍵が盗まれてしまうという脆弱点が出てしまう。これに対しては、中央のサーバに侵入検知パターンなどのデータベースを持たせ、クライアントは常時それを参考にしてパケットをチェックするという手段が提案されている。
 - * すべてのベンダによる IPsec における ESP の実装が守秘性機能をサポートしているとは限らない。IPv6 の実装は歴史が浅いため、IPv6 ネットワークのセキュリティ監査ツールがまだなく、実装の中には、まだ十分なテストを経っていないコードも含まれている。
 - * 従来の IPv4 ネットワークにおいては、境界にファイアウォールを設置し、NAT が使用されるセキュリティモデルが使用されてきた。しかし、IPv6 ネットワークではエンドツーエンドの透過性を確保しつつネットワーク全体のセキュリティを高める必要がある。ネットワーク規模に応じた二つの分散型セキュリティモデルが、この目的に対し挙げられる。
 - ファイアウォールをエンドポイントに分散したモデルでは、セキュリティ管理サーバがネットワーク上のエンドポイントを認証し、それらにファイアウォールポリシーを配布する。このポリシーの中には IPsec の鍵なども含まれる。つまり、エンドポイント自身が自分のセキュリティを確保する。
 - ハイブリッド型の分散ファイアウォールモデルでは、同様に管理サーバがエンドポイントを認証し、ポリシーを配布する。しかし、サーバはエンドポイントそれぞれにセキュリティレベルを決定し、それに基づいてポリシーを決定する。この場合、簡単なアクセス制御以上の複雑な制御は各エンドポイントで行われる。