19. 暗号化に関する知識 I

1. 科目の概要

OSS アプリケーションのセキュリティを確保するために必須の技術である暗号化について、公開鍵・秘密鍵暗号、認証などの各手法とその実装方法、および実用的な無線 LAN の暗号化やセキュアシェル(SSH)などの技術を解説する。

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
I-19-1. 暗号化の意義と効果、課題、注意点	OSSにおけるセキュリティの基本概念と全体像を概説する。OSSに求められるリスクとは何か、暗号化でどのような対応が可能か、暗号化処理の種類と利用時の課題、留意点などについて説明する。	1
I-19-2. 共通鍵暗号方式の仕組み	暗号化方式のひとつである「共通鍵暗号方式」の基本概念と仕組み、特徴、利点と欠点、OSSにおける利用状況について説明する。また、米国で標準化されたAES (Advanced Encryption Standard)を紹介する。	2
I-19-3. 公開鍵暗号方式の仕組みと重要性	暗号化方式のひとつである「公開鍵暗号方式」の基本概念と仕組み、特徴、利点と欠点、OSSにおける利用状況について説明する。インターネット利用時の暗号化方式として公開鍵方式がなぜ重要なのかを議論する。	3
I-19-4. ソフトウェア、ハードウェア、通信路における暗号化方法	OSやミドルウェア、アプリケーションで求められる暗号化処理とその実装を紹介する。またハードウェアレベルでの暗号化、ネットワークにおける暗号化にはどのようなものがあるか、その目的と特徴、実装方法を説明する。	4
I-19-5. 電子証明書の仕様、仕組み、役割と必要性	ネットワークにおける各ノードの正当性を証明する電子証明書について、それらの種類、その仕様、仕組み、電子証明書の役割と必要性について述べる。	5
I-19-6. OSSと暗号化、OSSにおける実装事例	様々なOSS活用シーンにおける暗号化の必要性を示し、OSSによる暗号化処理の実装例を、OS、ミドルウェア、アプリケーションのレベルで分類して紹介する。	6
I-19-7. 無線LANに求められる暗号化の仕様、必要性、課題	無線LANにおける暗号化の必要性について述べ、その仕様、特徴、利点と欠点などについて説明する。代表的な暗号化方式であるWEP (Wired Equivalent Privacy)と、さらに強化した暗号化方式のWPA (Wi-fi Protected Access)などを紹介する。	7
I-19-8. 認証の仕組みと目的、実現方法、利点	ネットワーク利用においてユーザや文書の正当性を証明する「認証」の基本的な仕組みと実現方式を解説する。また認証を実現するうえで暗号化をどう利用しているか、その具体的な方法について説明する。	8
I-19-9. Webサーバの暗号化ツール	HTTPによるWebサーバとのやりとりを暗号化する技術の中核をなすプロトコルであるSSL (Secure Socket Layer)について、その概要、仕様、特徴などを解説する。	11
I-19-10. セキュアシェル	リモートホストへのログインや遠隔実行を実現する手段として用意され、インターネットにおける代表的な暗号化通信方法となっているSSH (Secure Shell)について、その概要、仕様、特徴などを解説する。	10

【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

「19. 暗号化に関する知識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
19. 暗号化に関する知識	<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_19.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
組織の業務と関連するシステム	1	IT-IAS 情報保証と情報セキュリティ	IT-IAS1. 基礎的な問題 [19-Ⅰ-1]	IT-IAS2. 情報セキュリティの仕組み(対策) [19-Ⅰ-5,8]	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) [19-Ⅰ-8]	IT-IAS8. 情報の状態	IT-IAS9. 情報セキュリティサービス	IT-IAS10. 脅威分析モデル	IT-IAS11. 脆弱性 [19-Ⅰ-4]		
	2	IT-SP 社会的な観点とプロフェッショナルとしての課題	IT-SP1. プロフェッショナルとしてのコミュニケーション	IT-SP2. コンピュータの歴史	IT-SP3. コンピュータを取り巻く社会環境	IT-SP4. チームワーク	IT-SP5. 知的財産権	IT-SP6. コンピュータの法的問題	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 [19-Ⅰ-5,8]	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. データ割り当てと変換	IT-IPT3. 統合的コーディング	IT-IPT4. スクリプティング手法	IT-IPT5. ソフトウェアセキュリティの実現 [19-Ⅰ-2]	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 [19-Ⅰ-1, 2, 3, 4, 7, 8, 9, 10, 11]	IT-NET5. アプリケーション分野	IT-NET6. ネットワーク管理 [19-Ⅰ-7]							
	10	CE-NWK テレコミュニケーション	CE-NWK0. 歴史と概要	CE-NWK1. 通信ネットワークのアーキテクチャ	CE-NWK2. 通信ネットワークのプロトコル	CE-NWK3. LANとMAN	CE-NWK4. クライアントサーバコンピューティング	CE-NWK5. データのセキュリティと整合性 [19-Ⅰ-2, 3, 4, 8]	CE-NWK6. ワイヤレスコンピューティングとモバイルコンピューティング	CE-NWK7. データ通信	CE-NWK8. 組込み機器向けネットワーク	CE-NWK9. 通信技術とネットワーク概要	CE-NWK10. 性能評価	CE-NWK11. ネットワーク管理	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 [19-Ⅰ-4,8]	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インターフェイス	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、OSS 特有のセキュリティに関する話題や、SSH プロトコルのオープンソース実装である OpenSSH などの暗号化技術に関連した OSS の実装に関する知識がある。

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	第9回	第10回	第11回
19. 暗号化に関する知識 I	(1)オープンソースセキュリティの全体像	(1)共通鍵暗号方式の仕組み	(1)公開鍵暗号方式の仕組み	(1)ソフトウェア情報の暗号化	(1)電子証明書の種類	(1)オープンソースOS と暗号化	(1)無線LAN 暗号化プロトコル WEP の仕様	(1)認証とはされること	(1)VPN の構成	(1)SSH とは-2. OpenSSH	(1)SSL の概要
	(2)暗号化の意義と課題	(2)AES の概要	(2)インターネットでの公開鍵方式の重要性	(2)ハードウェアの暗号化	(2)電子証明書の仕様	(2)OSS における暗号化の実装	(2)WPA の仕様	(2)メッセージダイジェストによる認証／改ざん防止機能	(2)Ipsec	(2)IKE による IPSec の設定	(2)SSL の仕様
				(3)通信路の暗号化	(3)証明書発行に関わる当事者と発行までの流れ (4)CA 局による電子証明書発行、暗号化			(3)メッセージ認証で確認	(3)セキュアな MPLS による IP-VPN		(3)SSL の安全性 (4)SSL 通信の構成

（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 I	基本
習得ポイント	I-19-1. 暗号化の意義と効果、課題、注意点	
対応する コースウェア	第1回（セキュリティ機能と暗号化の位置づけ）	

I-19-1. 暗号化の意義と効果、課題、注意点

OSS におけるセキュリティの基本概念と全体像を概説する。OSS に求められるリスクとは何か、暗号化でどのような対応が可能か、暗号化処理の種類と利用時の課題、留意点などについて説明する。

【学習の要点】

＊ OSS はソースコードが公開されていることから、セキュリティの問題への対応は素早く行えるが、コミュニティにより開発されるため、セキュリティの保証主体が明確ではない。開発者だけでなく、利用者にもセキュリティの評価・検討を行うことが求められる。

＊ セキュリティに対する脅威としては、秘密が漏れる盗聴、情報が書き換えられる改竄、正しい送信者のふりをするなりすまし、後から当事者でないと宣言する否認、とが挙げられる。

＊ 脅威に対する防衛のための暗号技術として、対称暗号（共通鍵暗号）、公開鍵暗号、一方向ハッシュ関数、メッセージ認証コード、デジタル署名、議事乱数生成器が特に重要である。

＊ 暗号化を行えば全ての脅威から守られるわけではない。暗号化はセキュリティのほんの一部にすぎないことに注意をする必要がある。

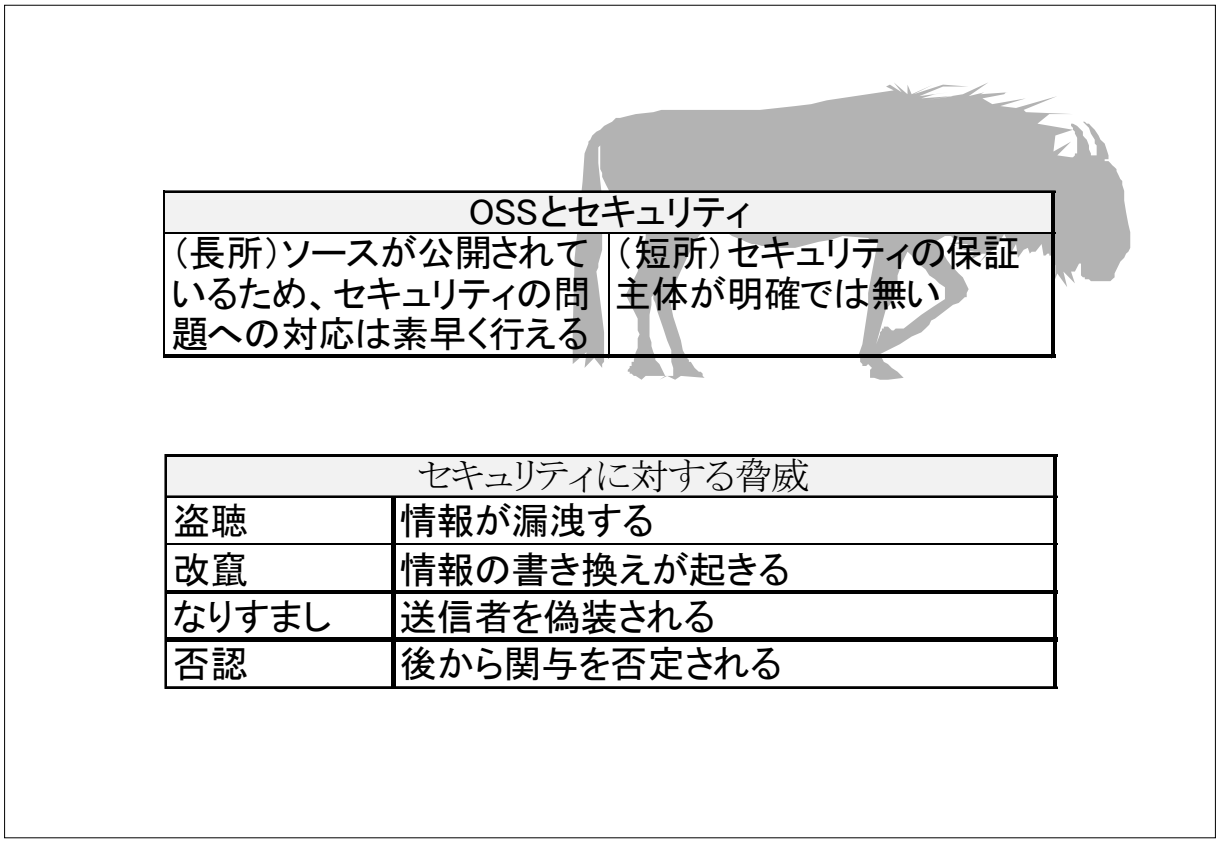

図 I-19-1.　OSS とセキュリティ

【解説】

1) オープンソースセキュリティの全体像

OSS はソースコードが公開されていることから、セキュリティの問題への対応は独自に素早く行うことも可能である。また、活発な開発がされている OSS では、こうした問題への対応も素早く行われる。しかし、OSS 独自の問題もあり、考慮が必要である。

＊ OSS のセキュリティリスク
OSS はコミュニティにより開発されるため、セキュリティの保証主体が明確ではない。また、十分なメンテナンスやサポートのない OSS にはセキュリティ脆弱性のリスクがある。

＊ OSS に求められるセキュリティ
上記セキュリティリスクに対処するため、開発者だけでなく、利用者にもセキュリティの評価・検討を行うことが求められる

2) 暗号化の意義と課題

OSS に限らず一般にセキュリティに対する脅威としては、情報の漏洩が起こる盗聴、情報が書き換えられる改竄、送信者の偽装をされるなりすまし、後から当事者でないと宣言する否認、とが挙げられる。

＊ 暗号化の機能と効果
脅威に対する防衛のための暗号技術として特に重要な役割を持つものに、対称暗号（共通鍵暗号）、公開鍵暗号、一方向ハッシュ関数、メッセージ認証コード、デジタル署名、議事乱数生成器が挙げられる。

＊ 暗号化の処理形態
暗号化する前のメッセージである平文を暗号化することで、意味のわからない暗号文になる。暗号文を復号化すると、元の平文に戻る。暗号化の手順を暗号アルゴリズムと呼び、暗号アルゴリズムには鍵（キー）が必要となる。鍵は非常に大きな数列からなる。

＊ 暗号化の注意点と課題
暗号化に関して注意すべき点は次の通り。

- 秘密のアルゴリズムを使わずに、実績のある暗号を使った方が、結果的には高い強度の暗号化につながる。
- 弱い暗号により、利用者が機密性に対して過信し、危険性の意識を下げるのであれば、暗号化の意味がない。
- 絶対に解読されない現実的な暗号は存在しない。
- 暗号化暗号はセキュリティのほんの一部にすぎず、結局利用者の意識が低ければ意味をなさない。

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	19　暗号化に関する知識 I	基本
習得ポイント	I-19-2. 共通鍵暗号方式の仕組み	
対応する コースウェア	第 2 回（暗号化の方式・共通鍵暗号方式）	

I-19-2. 共通鍵暗号方式の仕組み

暗号化方式のひとつである「共通鍵暗号方式」の基本概念と仕組み、特徴、利点と欠点、OSS における利用状況について説明する。また、米国で標準化された AES (Advanced Encryption Standard) を紹介する。

【学習の要点】

＊ 暗号化方式のひとつである共通鍵暗号では、1 つの鍵で情報を暗号化し、同じ鍵で復号化する。実際に利用する場合には、鍵の共有方法が問題となる。

＊ 米国では政府標準の共通鍵暗号が選定されている。これまで標準とされていた DES (Data Encryption Standard, 1977)に代わって、新しい標準となる AES（Advanced Encryption Standard）が 2000 年に選定された。

＊ AES では複数候補の中から Rijndael（ラインダール）という暗号アルゴリズムが採用されている。現在のところ Rijndael に対する有効な攻撃は見つかっていない。

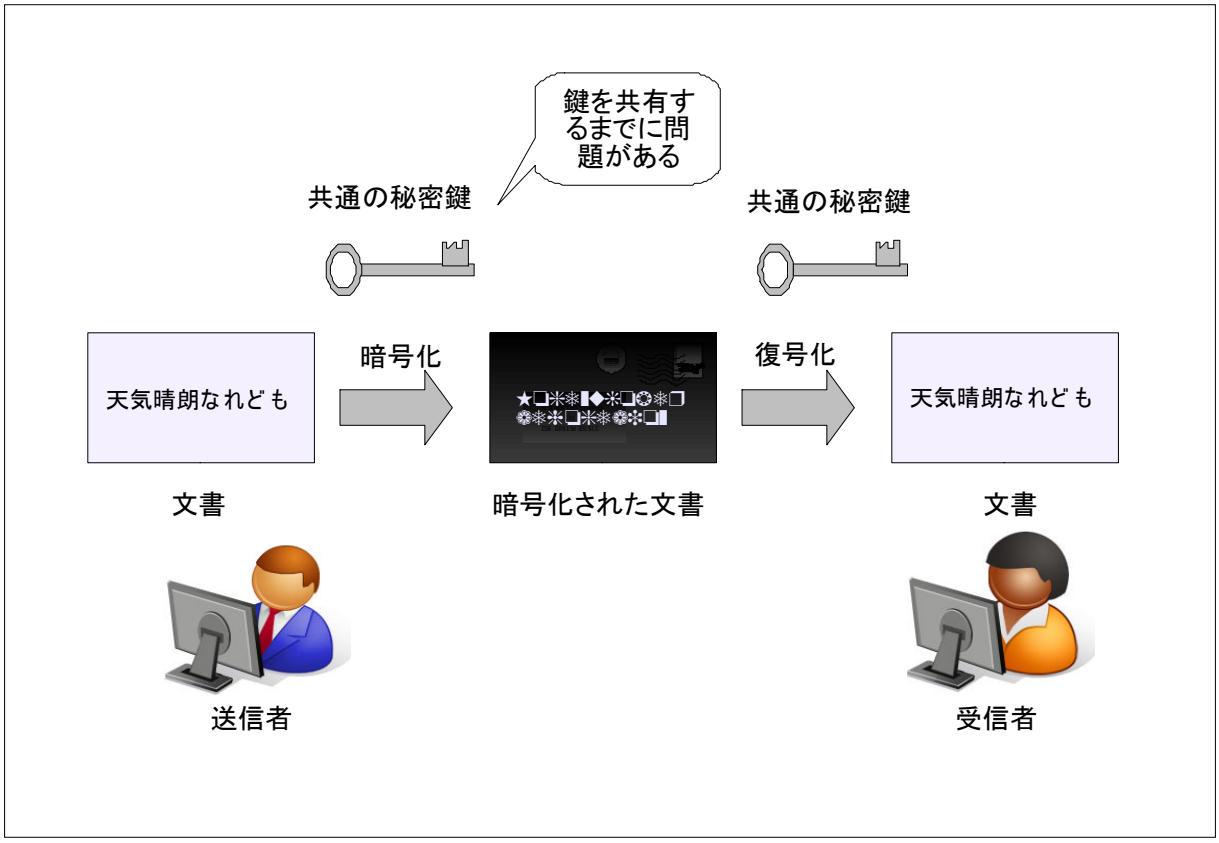

図 I-19-2.　共通鍵暗号方式の仕組み

【解説】

1) 共通鍵暗号方式

共通鍵暗号方式とは、暗号化と復号化に同じ鍵を用いる暗号方式のことを言う。秘密鍵暗号、対称鍵暗号とも呼ばれる。

＊ 共通鍵暗号方式の特徴

- 十分に大きな鍵空間を持ち、アルゴリズムの脆弱性が発見されていない共通鍵暗号を用いると、平文の機密性を維持することができる。
- 高速な暗号・復号処理ができる。
- 共通鍵暗号を利用した通信を行う場合、鍵を安全に共有する方法に問題が残る。

＊ 共通鍵暗号方式の暗号化の動作仕様

以下の手順において、ビット列の XOR 演算などを用いて暗号化を行う。

- 平文 A を、鍵 B で暗号化して、暗号文 A⊕B を得る。(⊕はここでの説明用の記号)
- 暗号文 A⊕B を、鍵 B で復号化して、平文 A を得る。

＊ OSS への実装状況

例えば、OpenPGP(RFC4880)を実装した GnuPG などがある他、様々な OSS で利用されている。

2) AES の概要

米国では政府標準の共通鍵暗号が選定されている。これまで標準とされていた DES (Data Encryption Standard, 1977)に代わって、新しい標準となる AES(Advanced Encryption Standard)が 2000 年に選定された。

＊ AES の暗号強度

- AES では複数候補の中から Rijndael(ラインダール)という暗号アルゴリズムが採用されている。
- 現在のところ Rijndael に対する有効な攻撃は見つかっていない。

＊ OSS への実装状況

- SSH プロトコルの OSS 実装である OpenSSH など、様々な OSS 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 I	I
習得ポイント	I-19-3. 公開鍵暗号方式の仕組みと重要性	
対応する コースウェア	第 3 回（暗号化の方式・公開鍵暗号方式）	

I-19-3. 公開鍵暗号方式の仕組みと重要性

暗号化方式のひとつである「公開鍵暗号方式」の基本概念と仕組み、特徴、利点と欠点、OSS における利用状況について説明する。インターネット利用時の暗号化方式として公開鍵方式がなぜ重要なのかを議論する。

【学習の要点】

＊ 暗号化方式のひとつである公開鍵暗号方式では、公開鍵で情報を暗号化し、秘密鍵で復号化する。

＊ 公開鍵暗号を使う場合、復号化のための鍵を受信者に送る必要がなくなり、共通鍵暗号を利用する際に起きた鍵共有の問題を回避できる。

＊ 公開鍵暗号の問題としては、公開鍵が本当に正しいかわからないという公開鍵の認証と、秘密鍵より数百倍遅いという処理速度とがある。

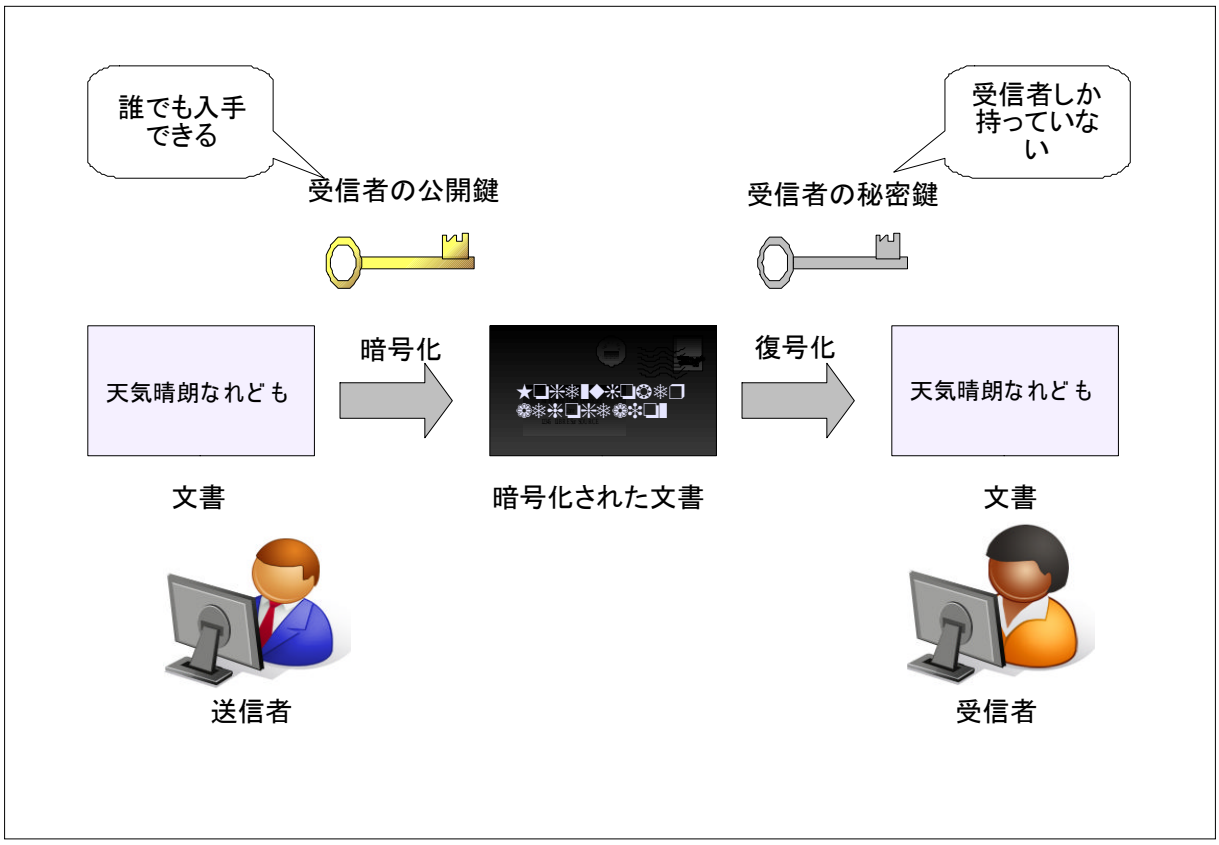

図 I-19-3.　公開鍵暗号方式の仕組み

【解説】

1) 公開鍵暗号方式の仕組み

暗号化方式のひとつである公開鍵暗号方式では、公開鍵で情報を暗号化し、秘密鍵で復号化する。

＊ 公開鍵暗号方式の特徴

- 公開鍵暗号を使う場合、復号化のための鍵を受信者に送る必要がなくなり、共通鍵暗号を利用する際に起こる鍵共有の問題を回避できる。
- 公開鍵暗号の問題としては、公開鍵が本当に正しいかわからないという認証と、秘密鍵より数百倍遅いという処理速度とがある。

＊ 公開鍵暗号方式の暗号化の動作仕様

以下の手順でメッセージが送信される。暗号の説明の際によく使われる Alice と Bob を送信者、受信者の呼び名として使う。

- (Bob)鍵ペア(公開鍵とプライベート鍵)の作成
- (Bob)公開鍵を暗号化に利用してもらうために Alice に送付
- (Alice)Bob の公開鍵を使って、メッセージを暗号化
- (Alice)暗号文を Bob に送付
- (Bob)プライベート鍵で暗号文を復号化

＊ デジタル署名とは

- デジタル署名は、印鑑の捺印に相当する手法であり、改竄やなりすましの検出ができる。

＊ デジタル署名の仕組み

- デジタル署名は公開鍵暗号を逆に使うことで実現される。
- メッセージをプライベート鍵で暗号化することが署名に相当し、公開鍵で復号することが、署名の検証に相当する。

＊ OSS への実装状況

SSH の OSS 実装である OpenSSH など、様々な OSS で利用されている。

2) インターネットでの公開鍵方式の重要性

- インターネットにおいては、盗聴やなりすましなどが問題となる。特に、共通鍵暗号方式の際には鍵を事前に共有する際に盗聴のリスクが非常に大きかった。
- 公開鍵を用いることで、そのリスクを回避できる利点がある。
- 現在では、公開鍵で鍵共有の問題を解決し、共通鍵の高速な暗号通信を用いるハイブリッド方式が利用される。

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 I	I
習得ポイント	I-19-4. ソフトウェア、ハードウェア、通信路における暗号化方法	
対応する コースウェア	第 4 回（情報システムにおける暗号化適用の方式）	

I-19-4. ソフトウェア、ハードウェア、通信路における暗号化方法

OS やミドルウェア、アプリケーションで求められる暗号化処理とその実装を紹介する。またハードウェアレベルでの暗号化、ネットワークにおける暗号化にはどのようなものがあるか、その目的と特徴、実装方法を説明する。

【学習の要点】

＊ 業務で使われるソフトウェアは機密情報やプライバシーにかかわる情報を扱うことが多い。情報漏洩を防ぎ、信頼性を維持するために OS、データベース、アプリケーションレベルでの暗号化が行われる。

＊ 主記憶、ハードディスク、外部記憶媒体といったハードウェアレベルでの暗号化も、情報漏洩の危機管理などの観点から行われる。

＊ ネットワークレベルの暗号化も通信の安全性・機密性を高めるために行われる。ネットワークレベルの暗号化には IPsec、 SSL/TLS などの選択肢がある。

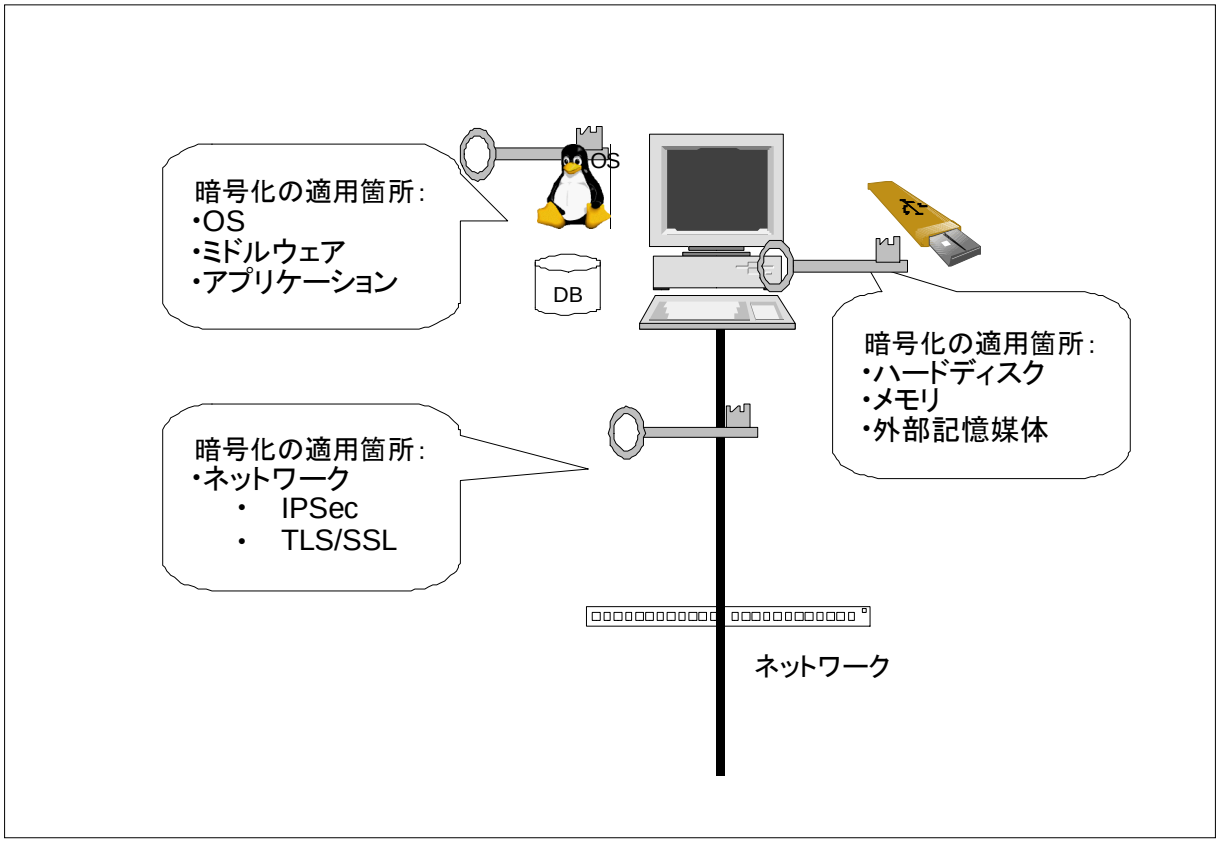

図 I-19-4.　ソフトウェア、ハードウェア、ネットワークに対する暗号化の適用

【解説】

1) ソフトウェア情報の暗号化

＊ 業務で使われるソフトウェアは機密情報やプライバシーにかかわる情報を扱うことが多い。

＊ 情報漏洩を防ぎ、信頼性を維持するためにソフトウェア情報の暗号化は重要である。

＊ OS、データベース、および機密データを扱うアプリケーションのそれぞれにデータを暗号化して処理する枠組みが用意されている。

2) ハードウェアの暗号化

ソフトウェアのみで情報が改竄されないことを担保するのは、原理的にも実際的にも困難なため、主記憶、ハードディスク、外部記憶媒体といったハードウェアにおける暗号化も行われる。

＊ ハードディスク、外部記憶媒体の暗号化

ハードディスクや外部記憶媒体に送られてきたデータをすべて暗号化して書き込む技術も、商品化されている。暗号化処理は、ハードウェア回路を使って実行している。

＊ ハードウェア暗号化の利点／欠点

ハードウェア回路を使った暗号の場合、暗号化処理は高速、高信頼に実行できる。その反面、暗号化回路が必要となり比較的高価になる。

3) 通信路の暗号化

ネットワークレベルの暗号化も通信の安全性・機密性を高めるために行われる。ネットワークレベルの暗号化には IPsec、SSL/TLS などの選択肢がある。

＊ ネットワーク暗号化の利点／欠点

通信路の機密性は保たれる。しかし、処理コストがかかるため、ネットワーク性能のボトルネックになることもある。

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 I	I
習得ポイント	I-19-5. 電子証明書の仕様、仕組み、役割と必要性	
対応する コースウェア	第 5 回（電子証明書の仕組み）	

I-19-5. 電子証明書の仕様、仕組み、役割と必要性

ネットワークにおける各ノードの正当性を証明する電子証明書について、それらの種類、その仕様、仕組み、電子証明書の役割と必要性について述べる。

【学習の要点】

* 電子証明書は暗号通信の際に使われる公開鍵が正しいものであることを証明するものである。
* 証明書の標準規格としては X.509 が存在しており、多くのアプリケーションでサポートされている。
* 証明書発行の際には認証局を利用することになる。この証明書発行までの一連の流れを理解する。

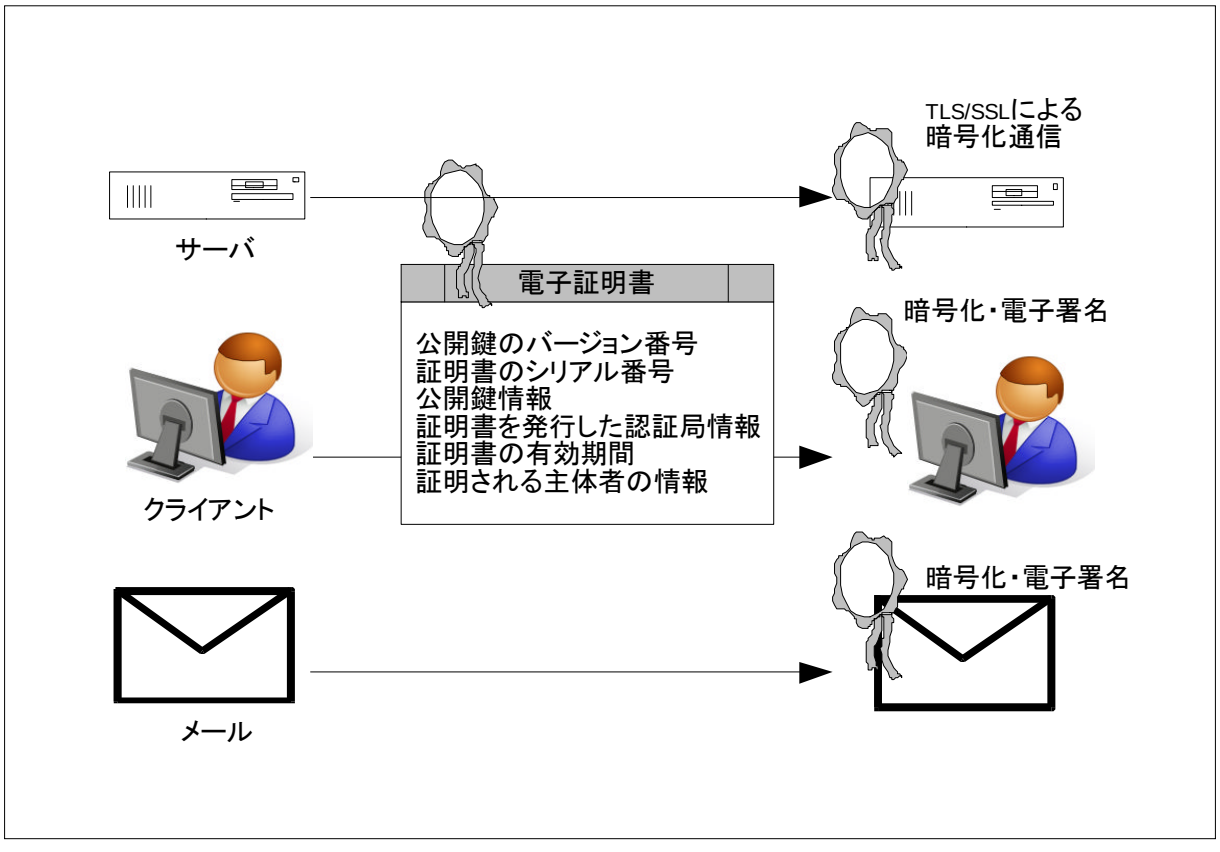

図 I-19-5.　電子証明書

【解説】

1) 電子証明書の仕組み

電子証明書は暗号通信の際に使われる公開鍵が正しいものであることを証明するものである。

＊ 電子証明書の種類
電子証明書の種類には、サーバ証明(VPN, Web)、クライアント証明、メール証明、ソフトウェア証明などがある。

＊ 電子証明書の仕様

- 証明書の標準規格としては X.509 が存在しており、多くのアプリケーションでサポートされている。
- X.509 は公開鍵のバージョン番号、証明書のシリアル番号、公開鍵情報、証明書を発行した認証局情報、証明書の有効期間、証明される主体者の情報、拡張領域といった項目で構成される。

2) 証明書発行に関わる当事者と発行までの流れ

証明書発行の際には認証局を利用することになる。公開鍵基盤(PKI: Public-Key Infrastructure)は公開鍵を運用するために定められた企画や仕様の総称である。PKI における証明書発行までの一連の流れは以下の通り。

＊ 証明書発行に関わる当事者

- 認証局
  証明書を発行する人
- 利用者
  PKI を利用する人
- リポジトリ
  証明書を保管しているデータベース

＊ 発行までの手順

- 利用者が公開鍵を認証局に登録し、認証局は利用者の公開鍵に認証局のデジタル署名を付けたものを証明書としてリポジトリに保存する。
- 公開鍵を利用する利用者はリポジトリから証明書をダウンロードする。

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 I	I
習得ポイント	I-19-6. OSS と暗号化、OSS における実装事例	
対応する コースウェア	第 6 回（OSS の活用シーンと暗号化）	

I-19-6. OSS と暗号化、OSS における実装事例

様々な OSS 活用シーンにおける暗号化の必要性を示し、OSS による暗号化処理の実装例を、OS、ミドルウェア、アプリケーションのレベルで分類して紹介する。

【学習の要点】

＊ OSS の活用されている多くのサーバソフトウェアにおいて暗号化処理が実装されている。

＊ OSS の OS、ミドルウェア、アプリケーションにおける暗号化処理の実際をデータベースソフトウェア、ネットワークアプリケーションなどを通して理解する。

図 I-19-6.　OSS の暗号化モジュール、ツール

【解説】

1) オープンソース OS と暗号化

オープンソース OS の活用されているサーバおよびクライアントにおいても暗号化機能は様々なシーンで活用される。例えば Linux ではカーネルにも暗号化モジュールが組み込まれている。暗号化ファイルシステムといった機能も提供される。

＊ OS の活用シーンと暗号化

- サーバとして
  イントラネットサーバ・インターネットサーバとして稼働する際に、SSL/TLS は標準的に利用されている。また、SSH によるアクセスを受け付ける際にも用いられる。
- クライアントとして
  SSL/TLS、SSH でサーバにアクセスする際、およびディスクデータの暗号化などが行われる。

＊ 暗号化の有効性評価

有効性評価には、いくつかの確認すべき項目がある。

- 暗号技術評価プロジェクト CRYPTREC（Cryptography Research and Evaluation Committees）などの機関で推奨する暗号を利用しているかどうか。
- TLS などの暗号化モジュールはセキュリティホールに対してパッチが当てられた最新版を利用しているかどうか。
- 鍵の管理など、セキュリティポリシーが制定・遵守されているかどうか。

2) OSS における暗号化の実装

OS のほか、ミドルウェア、アプリケーションなどでも暗号化の実装を活用する場面がある。

＊ ミドルウェア

データベースソフトウェア、運用管理ソフトウェア、信頼性・性能向上ツール、

＊ アプリケーション

ネットワークアプリケーション、汎用業務アプリケーション

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 I	I
習得ポイント	I-19-7. 無線 LAN に求められる暗号化の仕様、必要性、課題	
対応する コースウェア	第 7 回（無線 LAN の暗号化）	

I-19-7. 無線 LAN に求められる暗号化の仕様、必要性、課題

無線 LAN における暗号化の必要性について述べ、その仕様、特徴、利点と欠点などについて説明する。代表的な暗号化方式である WEP (Wired Equivalent Privacy)と、さらに強化した暗号化方式の WPA (Wi-fi Protected Access)などを紹介する。

【学習の要点】

＊ 無線 LAN はオフィスや家庭などでその利便性から広範に利用されるが、安易な設定ではデータ盗聴のリスクがある。

＊ 代表的な暗号化プロトコルである WEP では、RC4 という共通鍵暗号方式を用いている。しかし、WEP のプロトコル自体には数多くの脆弱性が指摘されている。

＊ WEP の問題点を補うために構築された WPA では、TKIP（Temporal Key Integrity Protocol）という暗号化方式を用いる。TKIP により鍵長の拡張のほか、一定時間ごとに暗号鍵を更新することで、暗号の強度を高めている。

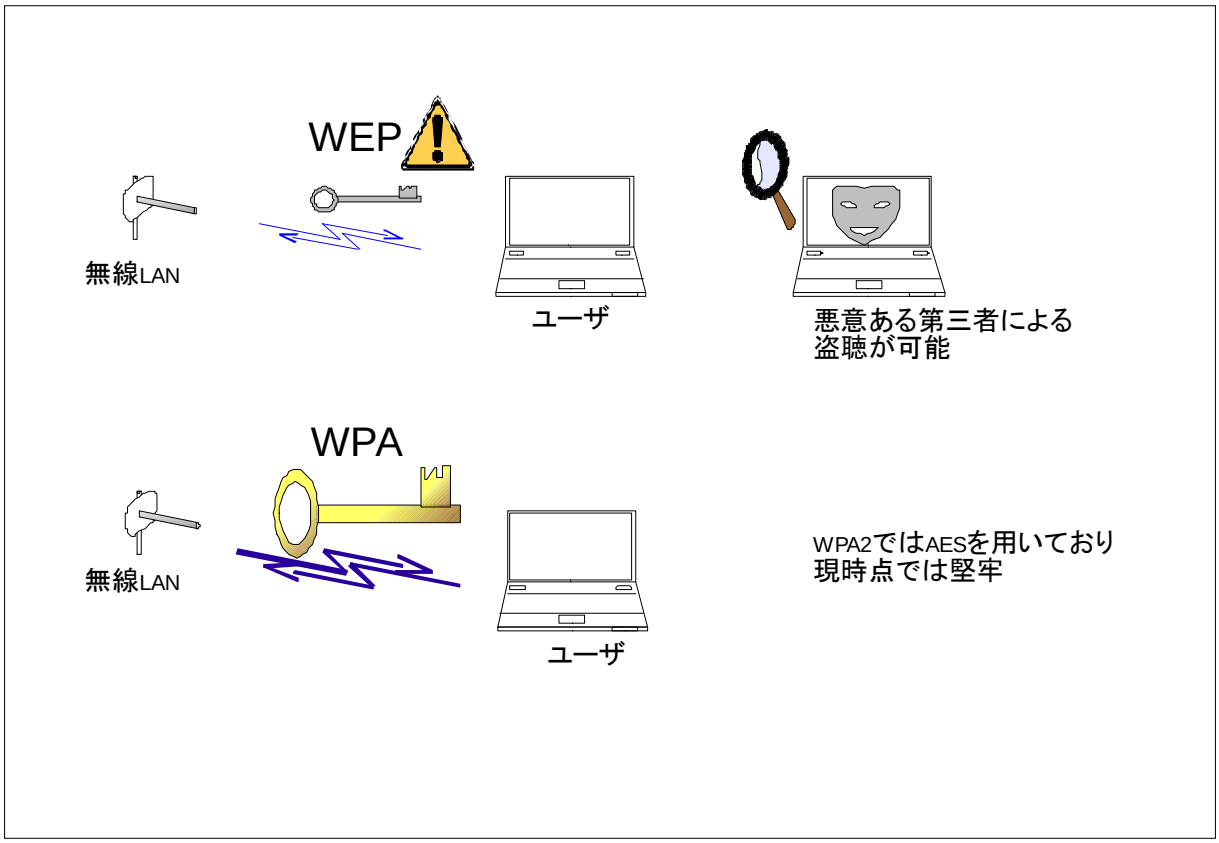

図 I-19-7.　無線 LAN の暗号化

【解説】

1) 無線 LAN 暗号化プロトコル WEP の仕様

＊ 無線 LAN 暗号化のリスク

- WEP は無線 LAN のセキュリティを確保するために標準的に用いられている暗号化プロトコルである。
- WEP には以前から脆弱性が指摘されており、データの盗聴や不正利用といったリスクがある。

＊ WEP プロトコルの暗号化手順

- WEP では、データ・パケットを共通鍵で暗号化する際に RC4 ストリーム暗号を使う。
- RC4 では、疑似乱数列と平文との XOR が暗号文となる。

＊ WEP のリスクとその対応

- RC4 暗号が既に解読されていることと、WEP の動作手順自体にも脆弱性が認められている。
- WPA や WPA2 などより高度なセキュリティ・プロトコルを使い，定期的にパスワードを変えることが望ましい。

2) WPA の仕様

＊ WEP の問題点を補うために構築された WPA では、TKIP（Temporal Key Integrity Protocol）という暗号化方式を用いる。

＊ TKIP により鍵長の拡張のほか、一定時間ごとに暗号鍵を更新することで、暗号の強度を高めている。

＊ WPA では、鍵管理の方法を工夫することでセキュリティの強化を行っている。

- しかし、内部で用いている暗号方式が RC4 であることから、時間をかければ解読が可能である。
- そのため、WPA2 では、AES（Advanced Encryption Standard）を採用している。

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 I	I
習得ポイント	I-19-8. 認証の仕組みと目的、実現方法、利点	
対応する コースウェア	第 8 回（認証と暗号化）	

I-19-8. 認証の仕組みと目的、実現方法、利点

ネットワーク利用においてユーザや文書の正当性を証明する「認証」の基本的な仕組みと実現方式を解説する。また認証を実現するうえで暗号化をどう利用しているか、その具体的な方法について説明する。

【学習の要点】

* 認証により、なりすまし（送信者を偽装する）による信用被害などを防ぐ。
* エンティティ（送信者など）の認証には、デジタル署名などによる本人確認が行われる。
* メッセージの認証には、一方向ハッシュ関数である MD5, SHA などが利用される。一方向ハッシュ関数はメッセージ固有のハッシュ値であるメッセージダイジェストを計算することができる。 メッセージダイジェストによりメッセージが同じかどうかを調べることができる。

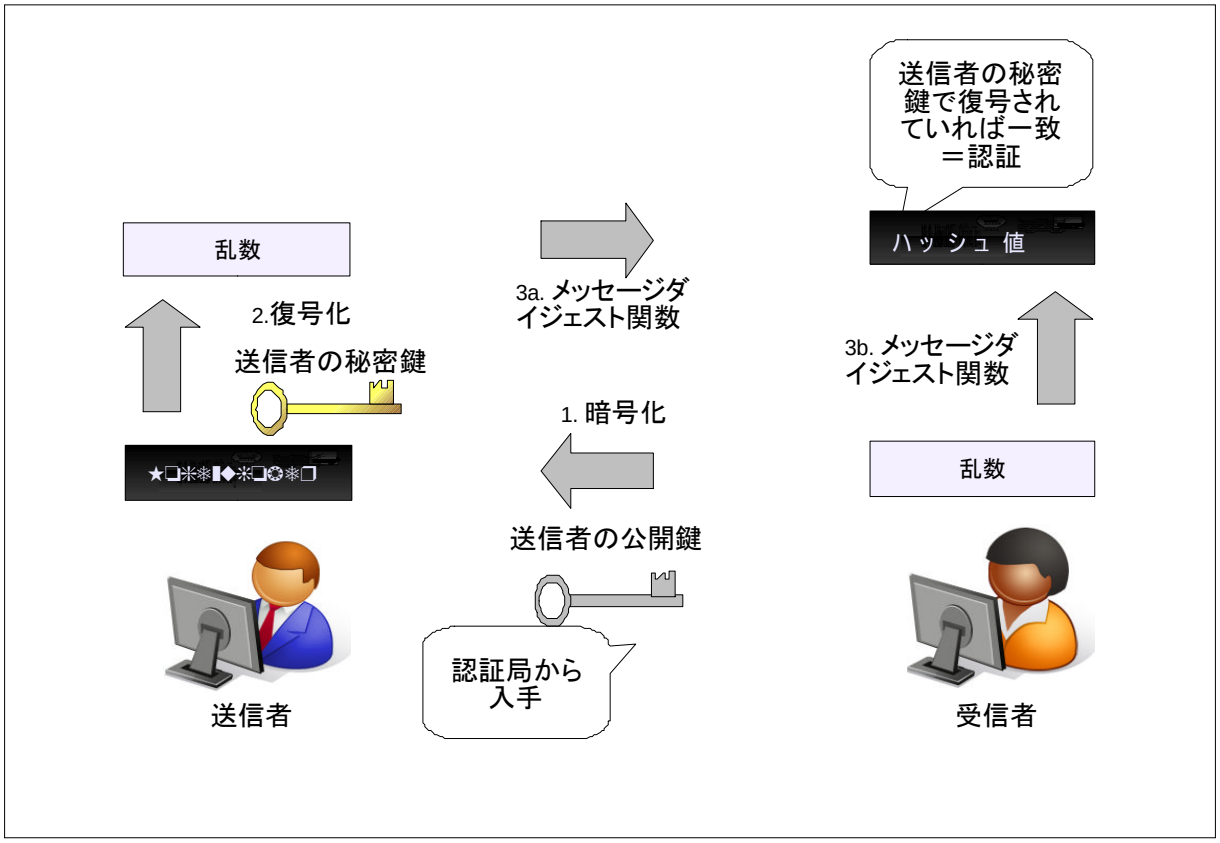

図 I-19-8.　認証の仕組み

【解説】

1) 認証とは

認証は、なりすまし(正しい送信者のふりをする)を防ぐために重要な仕組みである。

＊ なりすましのリスク

なりすましは、他人のユーザ ID などを盗用してネットワーク上で活動することを指す。これにより、機密情報の流出や、濡れ衣を着せられるなどのリスクがある。

＊ 認証の仕組み

送り主が本当にその人かを確認するエンティティ認証と、メッセージが送信時のまま届いたかを確認するメッセージ認証とがある。

- エンティティ認証

  デジタル署名を用いた場合、本人しか知りえない鍵を持っているという事実から本人と認証する。

- メッセージ認証

  一方向メッセージダイジェスト(ハッシュ)関数である MD5、SHA などを用いて、メッセージ送受信の前後のメッセージダイジェスト(ハッシュ値)を比較する。メッセージダイジェストの変化の有無によりメッセージ改竄の有無を判定する。

2) メッセージダイジェストによる認証／改ざん防止機能

＊ メッセージダイジェスト

- メッセージから一方向メッセージダイジェスト関数を用いて一意に求まる値をメッセージダイジェストと呼ぶ。
- メッセージダイジェストはメッセージの同一性の確認に利用できる。
- また、メッセージダイジェストの値は常に固定サイズである。

＊ メッセージダイジェストプロトコル

- MD5

  MD5 はメッセージダイジェスト関数の一つで、128 ビットのメッセージダイジェストを持つ。MD は Message Digest の略である。

- SHA

  SHA-1 は NIST(National Institute of Standards and Technology)で作られたメッセージダイジェスト関数の一つ。SHA-1 は 160 ビットのメッセージダイジェストを持つ。SHA-256、SHA-384、SHA-512 も存在する。

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	19　暗号化に関する知識 I	I
習得ポイント	I-19-9. Web サーバの暗号化ツール	
対応する コースウェア	第 11 回（SSL プロトコルの仕組み）	

I-19-9. Web サーバの暗号化ツール

HTTP による Web サーバとのやりとりを暗号化する技術の中核をなすプロトコルである SSL（Secure Socket Layer)について、その概要、仕様、特徴、実行の手順などを解説する。

【学習の要点】

＊ SSL/TLS((Secure Socket Layer/Transport Layer Security)は世界で最も利用されている暗号通信の方法である。HTTP による Web サーバの通信を暗号化する際に利用されている。

＊ SSL/TLS により、クライアントの送信する機密情報の盗聴を防と改竄を防ぐ。また、送信先の Web サーバが本物の送信相手である確認をすることもできる。

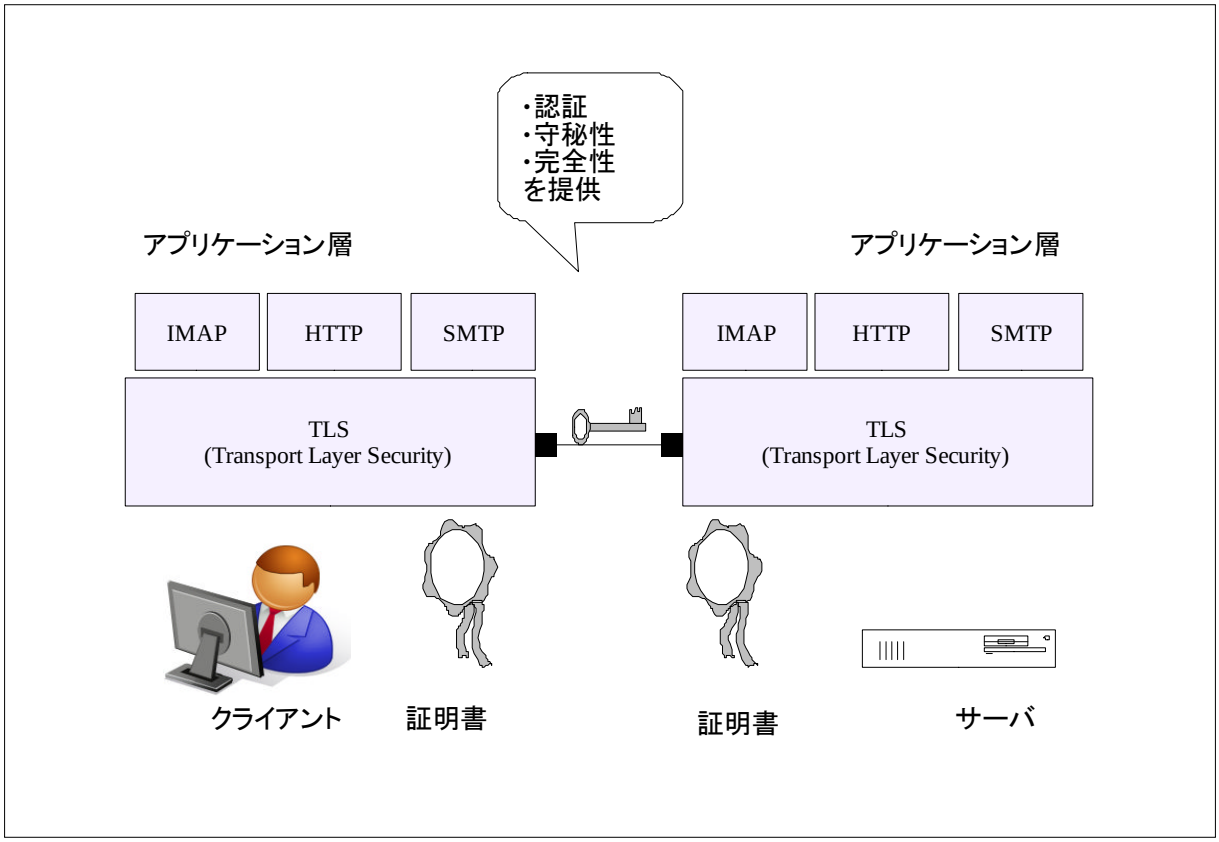

図 I-19-9.　サーバの暗号化(TLS)

【解説】

1) SSL/TLS の概要

＊ SSL/TLS は世界で最も利用されている暗号通信の方法である。HTTP による Web サーバの通信を暗号化する時などに利用されている。

＊ SSL/TLS により、通信相手を認証し、通信内容の機密性を確保することができる。

＊ SSL は 1994 年に Netscape 社によって作られたプロトコルである。

＊ TLS は SSL3.0 を元に、IETF によってつくられたプロトコルである。

＊ OpenSSL は SSL/TLS の OSS デファクト実装である。

2) TLS の仕様（以下、TLS に統一する）

TLS プロトコルは、「TLS レコードプロトコル」と「TLS ハンドシェイクプロトコル」という 2 つのプロトコルからなる。

＊ TLS レコードプロトコル

- TLS レコードプロトコルは、TLS ハンドシェイクプロトコルの下にあり、共通暗号を用いて暗号化されたメッセージ通信を行う部分である。

＊ TLS ハンドシェイクプロトコル

- TLS ハンドシェイクプロトコルは、暗号方式の決定、暗号方法の変更、エラー発生通知、データ転送という機能を持つ 4 つのプロトコルからなる。

3) TLS の安全性

＊ TLS は暗号通信の枠組み（フレームワーク）を提供している。

＊ この枠組みでは、TLS で使われる共通暗号、公開鍵暗号、デジタル署名、メッセージダイジェスト関数などを部品のように切り替えることができるということを意味する。

＊ TLS 1.1 で実装が必須とされているアルゴリズム

- 暗号化 ： 3DES
- 認証 ： RSA
- メッセージダイジェスト関数 ： SHA-1

＊ セキュリティ強度

- TLS の個々の暗号アルゴリズムは解読される恐れがあるが、その際には新しいものに切り替えて対応すれば良い。
- 利用者としては、TLS が有効か、そもそも相手が信用できるか、ということに留意する必要がある。

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	19　暗号化に関する知識 I	I
習得ポイント	I-19-10. セキュアシェル	
対応する コースウェア	第 10 回（SSH によるトンネリング）	

I-19-10. セキュアシェル

リモートホストへのログインや遠隔実行を実現する手段として用意され、インターネットにおける代表的な暗号化通信方法となっている SSH (Secure SHell)について、その概要、仕様、特徴、実行の手順などを解説する。

【学習の要点】

＊ ネットワークを介してリモートホストへのログインや処理を行う場合、セキュリティの観点と使い勝手の良さから SSH が多くの場合利用されている。

＊ SSH の各種コマンドにより、ネットワーク経由のログイン、ファイルコピーなどがデータを暗号化した状態で行うことができる。

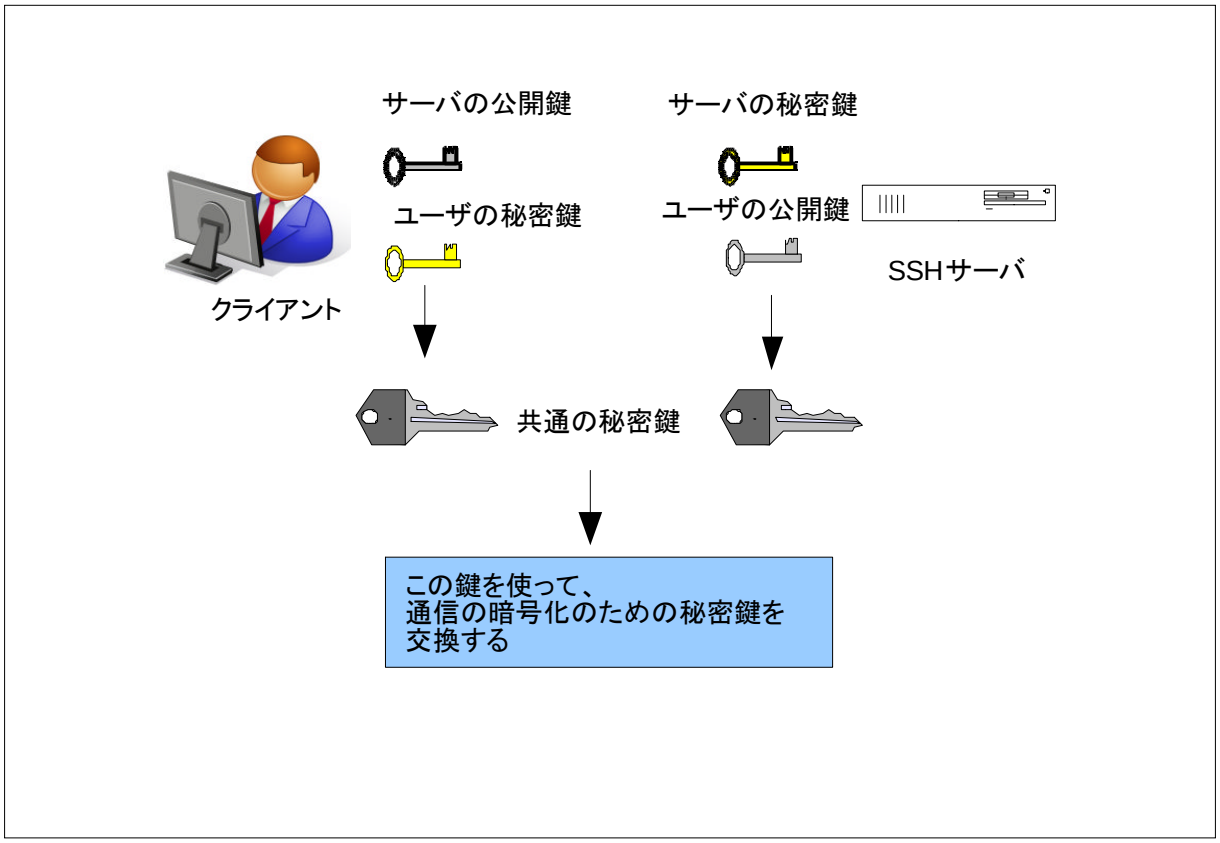

図 I-19-10.　SSH における暗号化された通信に必要な処理手順

【解説】

1) SSH とは

SSH は通信経路の暗号化や認証を強化したネットワーク越しの処理を可能とする、トランスポート層のプロトコルである。

＊ 機能と特徴

- SSH を用いることで、ネットワーク経由のログイン、ファイルコピーなどがデータを暗号化・圧縮した状態で行うことができる。
- リモートホストにログインする slogin、リモートのシェルを利用する ssh、リモートホスト間でのファイルコピーを行う scp や、FTP を代用するための sftp が用意されている。
- 従来のプロトコル通信を暗号化するポート転送機能も有している。

＊ OpenSSH

- SSH プロトコルを実装するデファクトの OSS である。
- OpenBSD プロジェクトにより開発・メンテナンスされている。
- 上述した機能を実装したクライアント側の実装と、サーバ側の実装とが配布されている。

＊ 公開鍵暗号の利用

- SSH の暗号通信は、公開鍵暗号（RSA または DSA）を用いて共通鍵暗号（3DES、Blowfish、AES、Arcfour など）の共通鍵を暗号化して鍵交換を行う。
- 通信自体は高速な共通鍵暗号を用いる。

2) SSH における通信路の暗号化

＊ 事前に作成してあるホスト公開鍵をサーバからクライアントに送る。
＊ クライアント側、サーバ側、それぞれで公開鍵・秘密鍵ペアを作成する。
＊ それぞれの公開鍵を交換する。
＊ 共通の秘密鍵を作成し Diffie-Hellman 法によりこの鍵を交換する。
＊ 公開鍵暗号化アルゴリズムを決定する。
＊ 共通鍵暗号化アルゴリズムを決定する。
＊ メッセージ認証アルゴリズムを決定する。
＊ メッセージダイジェストアルゴリズムを決定する。