調査５ モデルカリキュラムの提言 コースウェア

１９．暗号化に関するスキル

Ⅰ．概要	OSS アプリケーションのセキュリティ保持に必須の暗号化技術について、実際の開発・運用の際に必要な管理知識・手法の種類と特徴、内容を理解する。暗号化基盤として、実際にインターネット上で暗号化を担当する暗号化基盤の仕組みを理解する。
Ⅱ．対象専門分野	職種共通
Ⅲ．受講対象者、受講前提	基礎的なコンピュータ科学、セキュリティ工学基礎（ITSS レベル１程度）を習得、経験を持つレベルの知識を有すること。
Ⅳ．学習目標	・ 暗号化の基本技術を理解する。 ・ 暗号化の必要シーンと必要条件を理解する。 ・ オープンソースシステムを運用する際に必要となる暗号化セキュリティの知識を、マシン実習を含めて習得し、安全な暗号化の仕組みを導入できる。 ・ 公開鍵認証方式を用いた暗号化通信、及び VPN の設定ができる。
Ⅴ．使用教科書、教材等	【レベル 1】 未経験レベルの技術系学生から ITSS 職種の若手社員の利用を想定 『暗号化技術入門』 結城浩著、ソフトバンククリエイティブ刊 【レベル 2】 オリジナル教材を作成する。もしくはワークショップ主体のため 教科書、教材等は使用しない。
Ⅵ．習得スキルの評価方法	講義終了後の受講レポート、定量アンケート、知識確認ミニテスト、 演習問題の取り組み状況を総合的に判断して評価を行う。
Ⅶ．カリキュラムの構成	レベル 1　第 1 回～第 11 回 レベル 2　第 12 回～第 15 回

講座内容

第 1 回　セキュリティ機能と暗号化の位置づけ（講義　90 分）

OSS におけるセキュリティの基本概念とそこでの暗号化の役割、必然性、利点などを理解する。

⑴オープンソースセキュリティの全体像

1. OSS のセキュリティリスク
2. OSS に求められるセキュリティ
3. 暗号化の機能

⑵暗号化の意義と課題

1. 暗号化の効果
2. 暗号化の処理形態
3. 暗号化の注意点と課題

第 2 回　暗号化の方式・共通鍵暗号方式（講義　90 分）

暗号化の方式である「共通鍵暗号方式」の基本概念と仕組み、利点／欠点、動向を理解する。

⑴共通鍵暗号方式の仕組み

1. 共通鍵暗号方式とは
2. 共通鍵暗号方式の特徴
3. 共通鍵暗号方式の利点／欠点
4. 共通鍵暗号方式の暗号化の動作仕様
5. OSS への実装状況

⑵AES の概要

1. AES の位置づけと目的
2. AES の暗号強度
3. OSS への実装状況

第 3 回　暗号化の方式・公開鍵暗号方式（講義　90 分）

暗号化の方式である「公開鍵暗号方式」の基本概念と仕組み、利点／欠点、動向を理解する。

なぜ公開鍵方式がインターネット利用において重要なのかを理解する。

(1)公開鍵暗号方式の仕組み

1. 公開鍵暗号方式とは
2. 公開鍵暗号方式の特徴
3. デジタル署名とは
4. デジタル署名の仕組み
5. 公開鍵暗号方式の利点／欠点
6. 公開鍵暗号方式の暗号化の動作仕様
7. OSS への実装状況

(2)インターネットでの公開鍵方式の重要性

1. インターネットでの暗号化の条件
2. 公開鍵の利点
3. 暗号化の状況

第 4 回　情報システムにおける暗号化適用の方式（講義　90 分）

実際の情報システムにおいて、暗号化がどのようなところで活用されているか、ソフトウェア、ハードウェア、ネットワークそれぞれについて、実装方法、目的、機能について理解する。

(1)ソフトウェア情報の暗号化

1. アプリケーション暗号化の必要性
   - アプリケーションデータの暗号化
   - アプリケーションソフトウェアの暗号化
   - アプリケーション暗号化の利点／欠点
2. OS、ミドルウェアの暗号化
   - OS データの暗号化
   - データベースの暗号化

(2)ハードウェアの暗号化

1. 主記憶の暗号化
2. ハードディスクの暗号化
3. 外部記憶媒体の暗号化
4. ハードウェア暗号化の利点／欠点

(3)通信路の暗号化

1. ネットワークの暗号化
2. VPN
3. インタフェースの暗号化
4. ネットワーク暗号化の利点／欠点

第 5 回　電子証明書の仕組み（講義＋ワークショップ　90 分）

インターネットビジネスに必須のセキュリティ機能である電子証明書の仕様、仕組み、役割、必然性、利点などを理解する。

(1)電子証明書の種類

1. VPN 証明書
2. Web 証明書
3. クライアント証明書

(2)電子証明書の仕様

1. 電子証明書に必要な情報
2. X.509 の仕様

(3)証明書発行に関わる当事者と発行までの流れ

1. 証明書発行に関わる当事者
   - 運営者
   - 契約者
   - 利用者
   - 信頼者
2. 発行までの手順
   - RA 局、CA 局による証明書発行の手順
   - CPS：認証局運用規定
   - CP：証明書ポリシー

(4)CA 局による電子証明書発行、暗号化通信（ワークショップ）

第 6 回　OSS の活用シーンと暗号化（講義　90 分）

OSS におけるセキュリティの基本概念とそこでの暗号化の役割、必然性、利点などを理解する。

(1)オープンソース OS と暗号化

1. OS の活用シーンと暗号化
   - インターネットサーバとして
   - イントラネットのサーバとして
   - クライアントとして
2. 暗号化の有効性評価

(2)OSS における暗号化の実装

1. OS
2. 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
3. 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

第 7 回　無線 LAN の暗号化（講義　90 分）

無線 LAN における暗号化の仕様、必然性、利点／欠点、運用仕様などを理解する。

(1)無線 LAN 暗号化プロトコル WEP の仕様

1. 無線 LAN 暗号化のリスク
2. WEP プロトコルの仕様
3. WEP による暗号化の手順
4. WEP のリスクとその対応
5. TKIP の仕様

(2)WPA の仕様

1. WPA の仕様
2. WEP との違い
3. 実装方法と課題

第 8 回　認証と暗号化（講義　90 分）

ネットワークにおける認証の実現方式と暗号化の役割、必然性、利点などを理解する。

(1)認証とは

1. なりすましのリスク
2. 認証の仕組み
   - エンティティ認証
   - メッセージ認証
3. 暗号化による認証の仕様
4. ダイジェストとは

(2)メッセージダイジェストによる認証／改ざん防止機能

1. メッセージダイジェストの機能と効果
2. メッセージダイジェストプロトコル
   - MD5
   - SHA

(3)メッセージ認証で確認されること

第 9 回 IPsec による暗号化通信 （講義 90 分）

新しいオープンソースネットワーク基盤における VPN のもととなる IPsec プロトコルについて、仕様、課題、役割、必然性、利点などを理解する。

(1)VPN の構成

1. VPN（Virtual Private Network）とは
2. VPN の構成
   - LAN 間接続による VPN
   - リモートアクセスによる VPN
   - IP-VPN
3. トンネリングとは
4. VPN の仕様

(2)IPsec

1. IPsec の仕組み
2. VPN 構築への利用
3. IPsec の利点／欠点
4. IPsec を使えるシステム
5. IKE の機能

(3)セキュアな MPLS による IP-VPN

1. IP-VPN のセキュリティ
2. MPLS によるトンネル

第 10 回 SSH によるトンネリング （講義 90 分）

SSH を用いたクライアント／サーバ間の暗号化通信の仕組み、特徴、実装手順について理解する。

(1)SSH とは

1. SSH の機能と特徴
2. OpenSSH
3. SSH クライアントコマンド
4. 公開鍵認証

(2)IKE による IPSec の設定

1. IKE による IPSec の設定方法
2. トランスポートモードの設定
3. トンネルモードの設定

第 11 回 SSL プロトコルの仕組み(講義 90 分)

インターネット暗号化の仕組みの中核をなすプロトコルである SSL について、その仕様、課題、役割、必然性、利点などを理解する。

(1)SSL の概要

1. SSL の機能
2. SSL のネットワークでの役割と利点

(2)SSL の仕様

1. SSL の仕様
2. SSL の種類と特徴
   - TLS（Transport Layer Security）
   - OpenSSL

(3)SSL の安全性

1. サポートする暗号化アルゴリズム
2. セキュリティ強度

(4)SSL 通信の構成

1. SSL の処理シーケンス
2. 設定内容

第 12 回　VPN 通信の構築(講義＋ワークショップ　90 分)

IPsec を用いた VPN を設定構築し、その手順、機能効果、暗号化の状況などを理解する。

(1)IPsec の設定

1. 暗号化鍵の指定
2. ヘッダの種類と特徴
   - AH
   - ESP
3. 動作モードの設定
4. SA の設定
5. 動作モード
6. 鍵管理プロトコルの動作

(2)暗号化の状態確認

第 13 回　PKI(公開鍵暗号化基盤)の仕組み(講義　90 分)

暗号化を運用する重要な基盤である PKI について、仕様、課題、役割、必然性、利点などを理解する。また、実際の運用仕様、代表的な PKI についても理解する。

(1)PKI の仕組みと特徴

1. 公開鍵暗号を利用した電子認証のメカニズム
2. PKI の必要条件
3. PKI 適用分野
4. 代表的な PKI の種類と特徴
5. オープンソースとの関わり

(2)CA 局の仕組みとその機能

1. CA 局とは
2. CA 局のソフトウェア構成
3. CA 局の運用環境
4. CA 局による暗号化の手順

(3)CA 局の運用

1. RA 局の仕組み
2. VA の仕組み

第 14 回　認証基盤構築実習 （講義＋ワークショップ　90 分）

PKI の仕組みを SSL によって実際に構築し、その動作仕様や暗号化の様子を検証する。

(1)B to C 形態での認証構造の構築

1. CA 局ソフトウェア（Opera など）を用いた CA 局の構築
2. サーバへのサーバ証明書の発行
3. クライアントからの証明書発行

(2)B to B 形態での認証構造の構築

1. サーバ間での相互認証の構築

第 15 回　暗号化・これからの活用シーンと課題（講義　90 分）

新しいオープンソースネットワーク基盤における暗号化のニーズとその仕様、課題、役割、必然性、利点などを概説する。

(1)暗号化の新しい活用シーン

1. ユビキタスネットワークでの暗号化
   - 近傍無線技術での活用
   - 活用シーンとセキュリティリスク
   - 暗号化の仕様
   - 暗号化の課題
   - 携帯通信の暗号化仕様
2. IPv6 での暗号化仕様
   - 活用シーンとセキュリティリスク
   - 暗号化の局面
   - 暗号化の仕様

以上