

日本のサイバーセキュリティを「連携」「学び」「創造」

SEA/J 基礎編テキスト改訂 講師育成プロジェクト

JNSA 教育部会 教育実証 WG

基礎編テキスト改訂について

基礎編テキスト 改定背景

- **技術の進化:** クラウド技術やID管理など、近年の技術進化に対応した内容が含まれていない。
- **最新情報の必要性:** 現在の技術トレンドや業界標準に合わせた最新情報を提供する必要がある。
- **市販の書籍との近似性が乏しい:** 現在よく利用されている書籍や教育目的動画等と章立てが剥離している部分があり、受講生の理解向上や補助教材の導入が難しい部分がある。

テキスト全体にわたる大幅な改定をすることで、より効率のよい講義・学習定着が期待できる

- 今後は年次で内容のマイナーアップデートを実施予定

スケジュール

2024 年 7 月：リニューアル版の章立て・概要完成

｜リニューアル版作成・作成部内部レビュー

｜

2024 年 12 月末：リニューアル版 ドラフト完成

｜最終レビュー

｜フィードバックを基にした修正

2024 年 2 月末：完成

改定後の章立て

改定後内容	改訂前内容
1章 情報セキュリティマネジメント	1章 情報セキュリティマネジメント
	1.1 情報セキュリティの構成要素
	1.1.1 情報資産
	1.1.2 情報セキュリティの6つの要素
	1.1.3 脅威と脆弱性
	1.1.4 リスク
	1.2 情報セキュリティマネジメントシステム
	1.2.1 PDCAサイクル
	1.2.2 情報セキュリティマネジメントの標準規格
	1.3 情報セキュリティポリシー
	1.3.1 情報セキュリティポリシー
	1.3.2 情報セキュリティポリシーの構成
	1.3.3 情報セキュリティ対策基準の標準規格
	1.4 教育・訓練
	1.4.1 教育訓練計画
	1.4.2 実施と効果測定
	1.5 情報セキュリティ監査
	1.5.1 情報セキュリティ監査
2章 物理的セキュリティ	2章 セキュリティ運用
	2.1 物理的セキュリティ
	2.1.1 入退出管理
	2.1.2 クリアデスク・クリアスクリーン
	2.1.3 情報資産の持ち出し
	2.1.4 情報資産の破棄

改定後の章立て

改定後内容	改訂前内容
3章 人的セキュリティ脅威と対策	2.2 人的セキュリティ
	2.2.1 人員管理
	2.2.2 ソーシャルエンジニアリング

改定後の章立て

改定後内容	改訂前内容
4章 ネットワークセキュリティ脅威と対策	4.2 情報収集
	4.2.1 公開情報からの情報収集
5章 無線のセキュリティ	4.2.2 偵察行為
	4.3.3 サービス停止
	4.3.4 盗聴
	15.2.3 SSH (Secure Shell)
	15.2.4 TLS (Transport Layer Security) / SSL (Secure Socket Layer)
	15.2.5 Isec
	4.3.5 改ざん

改訂前内容
5.1 ファイアウォールの概念
5.1.1 ファイアウォール
5.2 ネットワークアクセスコントロール
5.2.1 ネットワークアクセスコントロール
5.2.2 パケットフィルタリング
5.2.3 ステートフルインスペクション
5.2.4 サーキットレベルゲートウェイ
5.2.5 アプリケーションゲートウェイ
5.3 NAT
5.3.1 NAT(アドレス変換技術)
5.3.2 静的NAT
5.3.3 動的NAT

改訂前内容
5.4 ファイアウォールの導入・運用
5.4.1 フィルタリングルール設計
5.4.2 DMZ設計
5.4.3 ログ解析
6章 侵入検知
6.1 IDS概要
6.1.1 ファイアウォールとIDS
6.2 IDSの構成
6.2.1 ネットワーク型IDS
6.2.2 ホスト型IDS
6.2.3 IDSの構成
6.4.1 IPS (Intrusion Prevention System)
6.4.2 ハニーポット

改定後の章立て

改定後内容	改定前内容
6章認証	
アクセス制御、認証認可	9.7 アクセス制御手法
	9.7.1 アクセス制御手法
OSのアクセス制御	

改定後内容	改定前内容
6章アクセス制御	9.1 ID管理と認証
	9.1.1 認証の種類
	9.2 パスワード認証
	9.2.1 パスワード認証
	4.3 不正侵入
	4.3.1 不正アクセス手法
	4.3.2 パスワードクラック
	9.2.2 ワンタイムパスワード
	9.3 バイオメトリクス認証
	9.3.1 バイオメトリクス認証（生体認証）
	9.4 デバイス認証
	9.4.1 デバイス認証
	9.5 認証プロトコル
	9.5.1 認証プロトコル
	9.6 シングルサインオン
	9.6.1 シングルサインオン

改定後の章立て

改定後内容	改定前内容
7章 ソフトウェアの脆弱性	
	10.1.2 バッファオーバーフロー
	7.3.4 Webサーバに対する脅威
8章 マルウェア	
	11.1 不正プログラムの種類
	11.1.1 不正プログラムの構造による分類
	11.1.2 不正プログラムの動作による分類
	11.1.3 亜種
	11.2 不正プログラムの感染経路
	11.2.1 メールによる感染
	11.2.2 Webからの感染
	11.2.3 メディアからの感染
	11.2.4 ソフトウェアのインストールによる感染
	11.2.5 ネットワークでの感染
	11.3 不正プログラムの活動

改定後内容	改定前内容
特権昇格、情報漏洩	
	11.3.1 バックドアの作成
	11.3.2 情報発信
	11.3.3 改ざん
	11.3.4 外部への攻撃
	11.4 検出方法
	11.4.1 検出方法の種類
	11.4.2 ウイルスの処理方法

改定後の章立て

改定後内容	改定前内容
9章 暗号	12章 暗号
	12.1 暗号の基礎知識
	12.1.1 基本用語
	12.1.2 鍵交換
	12.2 共通鍵暗号
	12.2.1 共通鍵暗号の暗号化・復号
	12.2.2 共通鍵暗号の代表的なアルゴリズム
	12.3 公開鍵暗号
	12.3.1 公開鍵暗号の暗号化・復号
	12.3.2 代表的なアルゴリズム
	12.3.3 ハイブリッド方式
	12.4 その他の暗号
	12.4.1 その他

改定後内容	改定前内容
10章 電子署名	13章 電子署名
	13.1 電子署名の必要性
	13.1.1 電子署名の必要性
	13.2 改ざん検知
	13.2.1 ハッシュ
	13.2.2 代表的なハッシュアルゴリズム
	13.3 電子署名の仕組み
	13.3.1 公開鍵暗号方式を用いた署名の仕組み
	15.2.1 PGP (Pretty Good Privacy)
	15.2.2 S/MIME (Secure Multipurpose Internet Mail Extensions)
11章 PKI	14章 PKI
	14.1 電子証明書
	14.1.1 電子証明書
	14.1.2 電子証明書の検証
	14.2 認証局
	14.2.1 認証局の役割
	14.2.2 認証局が管理する情報
	14.3 PKI
	14.3.1 PKI

改定後の章立て

改定後内容	改定前内容
12章 法令・規格	16章 法令・規格
	16.1 標準規格
	16.1.1 OECD セキュリティ関連ガイドライン
	16.1.2 ISO/IECセキュリティ関連規格
	16.1.3 JIS関連規格
	16.1.4 IETFセキュリティ関連規格
	16.1.5 ITUセキュリティ関連規格
	16.2 法令
	16.2.1 刑法
	16.2.2 不正アクセス禁止法
	16.2.3 迷惑メール関連法
	16.2.4 個人情報保護法
	16.2.5 著作権法
	16.2.6 電子署名法
	16.2.7 プロバイダー責任制限法
	16.2.8 IT基本法

