

FUJITSU 人材育成・研修サービス
情報セキュリティ対策実践シリーズ
基礎から学ぶセキュア環境構築・運用入門編



テキスト

USA04L1N-04

目次

第1章 情報セキュリティの考え方

1.1 情報セキュリティの現状と必要性	15
1.1.1 情報セキュリティインシデントの状況	15
<アイスブレイク 1> 情報セキュリティインシデントを思い返そう	16
1.1.2 情報セキュリティインシデントの影響	17
1.1.3 企業・組織における情報セキュリティの位置付け	18
<参考> 国内における情報セキュリティに関する法制度	19
1.1.4 情報セキュリティガバナンスの概要	20
1.1.5 ISMS の活動	21
<参考> 情報セキュリティポリシーの文書体系と策定プロセス	22
1.1.6 ISMS 認証制度	23
<参考> 国際規格の状況	24
1.1.7 安心安全な情報社会	25
1.2 情報セキュリティの基本概念	26
1.2.1 情報セキュリティの定義	26
1.2.2 情報セキュリティ対策の取り組み	27
1.2.3 組織的な情報セキュリティ対策の運用	28
1.2.4 リスクの定義	29
<参考> リスクマネジメントの概念	30
1.2.5 リスク対応による機能	31
1.2.6 リスク対応の考え方	32
<参考> 情報セキュリティ対策の検討例	33
1.2.7 情報ライフサイクルを取り巻く環境	34
<参考> 情報セキュリティの主な脅威とその対策(概観図)	35
<アイスブレイク 2> 情報資産に関わる脅威を考えてみよう	36
1.2.8 情報ライフサイクルとリスク対応の関係	37
1.2.9 業務活動への影響	38
1.2.10 情報セキュリティの維持	39

第2章 ICTシステムにおける情報セキュリティ対策技術

2.1 ICTシステムにおける技術的対策	43
2.1.1 ICTシステムにおける脅威と要素ごとの対策	43
<参考> ICTシステムに対する主な攻撃手法	44
2.1.2 情報セキュリティを確保する主な技術的対策	45
2.1.3 サイバー攻撃への対応	46
2.1.4 ICTシステムのセキュア環境	47

2.2 ネットワークにおけるセキュリティ対策.....	48
2.2.1 ネットワークの脅威とその影響.....	48
<参考> ネットワークにおける脅威の捉え方.....	49
2.2.2 ファイアーウォールにおけるネットワークの境界防御.....	50
2.2.3 ネットワークにおけるアクセス制御の種類と侵入防御.....	51
2.2.4 パケットフィルタリングによるアクセス制御.....	52
2.2.5 ステートフルパケットインスペクションによるアクセス制御.....	53
2.2.6 IDS/IPS による不正侵入防御.....	54
2.2.7 UTM によるネットワーク制御.....	55
2.2.8 ネットワーク構成における多層的な防御.....	56
2.2.9 アクセスルートの制御による防御.....	57
<参考> インターネットへの代理アクセス(Proxy).....	58
2.3 コンピュータウイルスへの対策.....	59
2.3.1 ウイルスにおける脅威とその影響.....	59
<参考> サイバー攻撃やサイバー犯罪の活動傾向.....	60
2.3.2 ウイルスの主な種類.....	61
<参考> ウイルスの主な特徴.....	62
2.3.3 標的型攻撃の概要.....	63
2.3.4 標的型攻撃の特徴.....	64
<アイスブレイク 3> 標的型攻撃メールにおける対策の検討.....	65
2.3.5 ウイルスに対する基本的な対策.....	66
2.3.6 ウイルス対策ソフトの検知方法.....	67
2.3.7 サンドボックスによる未知のウイルス対策.....	68
2.3.8 日常業務におけるウイルス感染予防と情報漏えい対策.....	69
2.4 暗号技術の利用.....	70
2.4.1 暗号技術の必要性.....	70
2.4.2 暗号方式と特徴.....	71
2.4.3 公開鍵暗号方式によるデジタル封書の仕組み.....	72
2.4.4 公開鍵暗号方式によるデジタル署名の仕組み.....	73
<参考> ハッシュ関数の特徴.....	74
2.4.5 認証局と証明書の役割.....	75
<参考> 証明書の流れと内容.....	76
2.4.6 証明書の種類とフォーマット.....	77
<参考> 認証局の階層型モデル.....	78
2.4.7 PKI 環境の必要性と基本構成.....	79
<参考> PKI の適用例～電子申請、電子入札～.....	80
2.4.8 SSL/TLS による Web サーバとクライアント間の暗号通信.....	81
2.4.9 インターネット VPN による暗号通信.....	82
<参考> 無線 LAN における暗号通信.....	83
2.5 認証技術の適用.....	84
2.5.1 認証技術の必要性.....	84

2.5.2 本人認証の種別.....	85
2.5.3 固定パスワードの適用.....	86
<参考> 固定パスワードの適用.....	87
2.5.4 物理認証.....	88
2.5.5 バイオメトリクスの適用.....	89
<参考> 手のひら静脈認証.....	90
2.5.6 認証サーバによる認証の一元管理.....	91
<参考> シングルサインオンの種類と特徴.....	92
2.6 サーバにおける情報セキュリティ対策.....	93
2.6.1 サーバの脅威とその影響.....	93
<参考> クラウドコンピューティングの定義と利用形態.....	94
2.6.2 サーバの要塞化を実現する要素技術.....	95
<参考> 仮想化とマルチテナント.....	96
2.6.3 サーバのソフトウェアにおける主な対策.....	97
<参考> ユーザー権利とファイルへのアクセス制限.....	98
<アイスブレイク 4> 特権 ID の管理方法を検討してみよう.....	99
2.6.4 サーバの主な可用性対策.....	100
2.6.5 サーバマシンにおけるセキュリティ環境の実現.....	101
2.7 エンドポイントにおける情報セキュリティ対策.....	102
2.7.1 エンドポイントの脅威とセキュリティ要素技術.....	102
2.7.2 エンドポイントの情報漏えい対策.....	103
2.8 運用を支える要素技術.....	104
2.8.1 IT 資産管理とログ管理における要素技術.....	104
<参考> クラウド型のセキュリティサービス.....	105
2.8.2 セキュアな ICT システムにおける効果の検証技術.....	106
2.9 情報セキュリティの有効性を確保する要素技術の全体像.....	107
<参考> 情報セキュリティ対策における強度の考え方.....	108

第3章 セキュア環境の構築・運用方法

3.1 セキュア環境の構築と運用における取り組み.....	111
3.1.1 企業・組織における情報セキュリティ環境.....	111
3.1.2 ICT システムの情報セキュリティ構築工程と手法.....	112
3.2 リスク対応方針の検討と対策の決定.....	113
3.2.1 リスクアセスメントの流れ.....	113
<参考> 情報セキュリティリスク一覧表とリスクマップの例.....	114
3.2.2 リスク対応および情報セキュリティ対策の決定.....	115
<参考> リスク対応計画表の例.....	116
3.3 情報セキュリティ環境における運用作業.....	117
3.3.1 ICT システムの平常時における運用方法.....	117
3.3.2 ICT システムの緊急時における運用方法.....	118
3.4 情報セキュリティの実現に向けた取り組み.....	119

演習問題

1. 演習目的と演習形態.....	123
2. グループ演習の進め方.....	124
3. 演習の構成.....	125
演習 1 ICT システムにおける脅威の洗い出し.....	126
演習 2 ファイアーウォールのルールを作成してみよう.....	127
<ワークシート 1> ネットワーク構成図.....	128
<ワークシート 2> アクセス制御リスト.....	129
<参考> アクセスルールの設定と通信の確認.....	130
演習 3 暗号の流れを見てみよう.....	131
演習 4 暗号利用技術をみてみよう.....	132
(1) 証明書の流れを解説してみよう.....	132
(2) SSL の鍵の流れを解説してみよう(オプション).....	133
演習 5 リスクアセスメントと対策の検討.....	134
(1) リスクマップへの配置.....	134
<ワークシート 3> リスク分析シート.....	135
(2) 対策の検討.....	136

想定企業

1. 会社概要と業務概要.....	139
2. 生産・販売・在庫業務の内容.....	140
3. 情報システムの現状.....	141
<参考> 評価ランクの例.....	142