

情報セキュリティ入門

目次

第1章 情報セキュリティの概要	
1.1 情報セキュリティの概要	3
1.1.1 情報セキュリティの目的	3
1.1.2 情報セキュリティの定義	4
1.1.3 情報セキュリティの機能	5
1.1.4 情報セキュリティの重要性	6
1.2 不正アクセスの現状	7
1.2.1 情報システムに対する脅威	7
1.2.2 不正アクセスの報告件数	8
<参考>情報セキュリティ 10 大脅威 2020	9
1.3 情報セキュリティ対策の概要	10
1.3.1 情報セキュリティ対策とは	10
1.3.2 三つの情報セキュリティ対策	11
1.3.3 セキュリティポリシー	12
1.3.4 情報セキュリティマネジメントシステム	13
<参考>高度標的型攻撃	14
<参考>2019 年のインシデント事例	15
第2章 人的・管理的セキュリティ対策	
2.1 人的・管理的セキュリティの概要	19
2.2 役割と責務	20
2.2.1 役割と責務の明確化	20
2.2.2 罰則と免責	22
2.2.3 報告の義務と連絡経路	23
2.3 利用者への徹底	24
2.3.1 教育	24
2.3.2 利用手順・運用手順	25
2.3.3 情報セキュリティ規程	26
第3章 物理的・環境的セキュリティ対策	
3.1 物理的・環境的セキュリティ対策の概要	29
3.2 設備	30
3.2.1 敷地、建物、フロア環境	30
3.2.2 サーバルーム	31
<参考> データセンタの利用	32
3.2.3 建屋/電源/空調設備	33
3.3 情報機器	34
3.3.1 サーバ本体	34
3.3.2 ネットワークケーブル	35
<参考> 無線 LAN	36
3.3.3 記録媒体	38
<参考> 敷地外における利用	39
第4章 技術的セキュリティ対策	
4.1 技術的セキュリティ対策の概要	43
4.2 ネットワークセキュリティ	44
4.2.1 ルータにおけるパケットフィルタリング	44
<参考> ステートフルインスペクション	46
4.2.2 Proxy サーバ（アプリケーションゲートウェイ）	47
4.2.3 アドレス変換	48
(1) NAT	48

(2) NAPT	50
4.2.4 ファイアウォール	51
4.2.5 ファイアウォールの構成	53
4.2.6 ネットワーク型 IDS	54
4.3 ホストセキュリティ(サーバセキュリティ)	55
4.3.1 セキュリティパッチの適用	55
4.3.2 アカウント管理	56
4.3.3 サービス管理	57
4.3.4 ファイルシステムのアクセス権	58
4.3.5 ログ管理	59
4.3.6 ホスト型ファイアウォール	60
4.3.7 ホスト型 IDS	61
4.3.8 脆弱性監査	62
4.3.9 Web サーバセキュリティ	63
4.3.10 Mail サーバセキュリティ	64
4.3.11 DNS サーバセキュリティ	65
4.4 ホストセキュリティ(クライアントセキュリティ)	66
4.4.1 利用上の制限事項	66
4.4.2 セキュリティパッチの適用	67
4.4.3 電子メールのセキュリティ	68
4.4.4 Web ブラウザのセキュリティ	69
4.4.5 パケットフィルタリング	70
4.5 ウィルス対策	71
4.5.1 ワクチンソフトの適用箇所	71
4.5.2 ウィルス対策の基本	72
4.6 暗号化	73
4.6.1 暗号アルゴリズム	74
(1) 共通鍵暗号方式	74
(2) 公開鍵暗号方式	75
(3) ハイブリッド方式	76
4.6.2 デジタル署名	77
4.6.3 代表的な暗号化機能	78
(1) SSL	78
(2) S/MIME、PGP/MIME	79
<参考> S/MIMEとPGP/MIMEの違い	80
(3) SSH	81
(4) VPN	82
4.7 認証システム	83
4.7.1 認証方式	84
4.7.2 メール送信	85
4.7.3 代表的な認証システム	86
(1)スマートカード	86
(2)バイオメトリクス認証	87
(3)第三者認証	88
(4) PKI	89
(5) PAP/CHAP	90
(6)ワンタイムパスワード	91
<参考> 高度標的型攻撃に対する対策	92
(1)入口対策	93
(2)内部対策	94
(3)出口対策	95
第5章 情報セキュリティの運用管理	99
5.1 ISMSのプロセスサイクル	99

5.2 情報セキュリティの管理	100
5.2.1 リスク分析、評価	100
5.2.2 セキュリティポリシー	101
5.2.3 セキュリティポリシーの策定	102
5.2.4 情報セキュリティ対策の適用	103
5.2.5 情報システムの管理	104
5.3 インシデント発生時の対処	105
5.4 セキュリティ基準への準拠	106