

Chapter
1

セキュリティの基本

1-01	何をどう守るのか セキュリティの必要性	12
1-02	機密性、完全性、可用性の3つ セキュリティの三要素	14
1-03	「セキュリティの三要素」以降に追加された4つの要素 セキュリティの追加要素	16
1-04	セキュリティ上の脅威 情報漏えい、改ざん、サービス妨害	18
1-05	守るべきもののリスクを特定して対処を検討する セキュリティを確保するために必要なこと	20
1-06	セキュリティを確保する理由から守るべきものを導き出す セキュリティを確保すべきもの	22
1-07	個人を特定する情報 個人情報	24
1-08	いわゆるマイナンバーを含む個人情報 特定個人情報	26
1-09	セキュリティは難しい？	28

Chapter
2

セキュリティの確保に必要な基礎知識

2-01	セキュリティを守るための原則から手順まで セキュリティポリシー	30
2-02	検知、初動対応、復旧、事後対応 セキュリティ事故対応の4つのフェーズ	32
2-03	相手を正しく認識し、相手によって正しい権限を付与する仕組み 認証と認可	34

2-04	第三者から情報を守るための仕組みの1つ 暗号	36
2-05	データの改ざんをチェックする ハッシュ	38
2-06	基本的かつ地道な対策の積み重ねによって守りを固める ハードニング	40
2-07	古くから使われている認証方法だが、使い回しは厳禁 パスワード	42
2-08	生体を持つ特徴を認証に応用する バイOMETリック認証	44
2-09	1回だけ使用できるパスワード ワンタイムパスワード	46
2-10	素性の異なる2種類の情報を組み合わせる認証 二要素認証	48
2-11	認証1回で複数システムの利用権を設定 シングルサインオン	50
2-12	電子データが改ざんされていないことを保証する技術 電子署名とその応用の例	52
2-13	自身が正しい存在であることを示すための仕組み 証明書と認証局	54
2-14	データを他者から守る方法の1つ 暗号化ファイルシステム	56
2-15	マルウェアを識別し、駆除するための仕組み ウイルススキャン	58
2-16	昔からあるプログラム修正の考え方が、脆弱性対応の王道でもある パッチ	60
2-17	通信を制御するための基本的な仕組み パケットフィルタリングとアプリケーションゲートウェイ	62
2-18	状態を観測し、必要なアクションにつなげるための施設 セキュリティオペレーションセンター (SOC)	64

2-19	セキュリティを考慮した開発工程 SDL (Security Development Lifecycle) ……66
2-20	攻撃を受けたことを確認する手がかり 各種ログ ……68
2-21	セキュリティ事故に対応し、ダメージを最小限に抑える仕組み CSIRT ……70
2-22	多角的なアプローチ ……72

Chapter 3

攻撃を検知・解析するための仕組み

3-01	怪しいものを封じ込める「砂場」 サンドボックス ……74
3-02	攻撃者が残したものを動作させて挙動を解析する 動的解析 ……76
3-03	攻撃者が残したものを動作させず挙動を解析する 静的解析 ……78
3-04	コンピューターを徹底的に家探しする フォレンジック ……80
3-05	ネットワークのデータを取得する パケットキャプチャ ……82
3-06	各種ログ解析を実施し、攻撃の痕跡を見つけ出す仕組み SIEM ……84
3-07	攻撃を観測するための仕組み ハニーポットとハニーネット ……86
3-08	敵を知る ……88

Chapter 4

セキュリティを脅かす存在と攻撃の手口

4-01	さまざまな意図を持って対象を攻撃する者たち 攻撃者 ……90
4-02	誤った仕様や誤った実装 脆弱性 ……92
4-03	悪意をもって開発されたソフトウェアの総称 マルウェア ……94
4-04	ソフトウェアの拡張に便利だが、悪い人が使うことも プラグイン ……96
4-05	力技だが侮れない総当たり攻撃 ブルートフォース攻撃 ……98
4-06	ターゲットに集中アクセス攻撃を仕掛ける DoS/DDoS ……100
4-07	アドレスを教えたとはずのない相手からのメール 迷惑メール ……102
4-08	水を飲みにやってくる動物を待ち構えるライオン 水飲み場型攻撃 ……104
4-09	特定の組織や企業を標的にする 標的型攻撃 ……106
4-10	気づかぬうちにマルウェアに感染してしまう ドライブバイダウンロード ……108
4-11	通信の途中で攻撃者が通信を盗聴する 中間者攻撃 ……110
4-12	バッファ領域をあふれさせて悪用する バッファオーバーフロー ……112
4-13	データベースに不正アクセスする SQL インジェクション ……114
4-14	OS を不正に操作する攻撃 OS コマンドインジェクション ……116

4-15	Web サイトを横断して攻撃を行う クロスサイトスクリプティング (XSS).....	118
4-16	他人になりすまして攻撃を行う クロスサイトリクエストフォージェリ (CSRF).....	120
4-17	データを人質にして身代金を要求するマルウェア ランサムウェア.....	122
	脅威と防御.....	124

Chapter
5

セキュリティを確保する技術

5-01	セキュリティが強化された OS セキュア OS.....	126
5-02	セキュア OS の実装例 SELinux、TOMOYO Linux.....	128
5-03	端末に情報を残さない仕組み シンクライアント.....	130
5-04	空き巣は侵入口を探している ポートスキャン.....	132
5-05	既知の攻撃手段で侵入を試みる ペネトレーションテスト.....	134
5-06	暗号化と復号に同じ鍵を使う 共通鍵暗号方式.....	136
5-07	暗号化と復号に別の鍵を使う 公開鍵暗号方式.....	138
5-08	現在、幅広く使われている共通鍵暗号方式 AES.....	140
5-09	インターネットで通信を行う際の暗号化の仕組み TLS.....	142

5-10	プログラムコードにサイン (署名) する コード署名.....	144
COLUMN	ハッキングは罪? 攻撃と防御は表裏一体.....	146

Chapter
6

ネットワークセキュリティ

6-01	攻撃から資産を守る防護壁 ファイアウォール.....	148
6-02	Web アプリケーションに特化したファイアウォール Web アプリケーションファイアウォール.....	150
6-03	本来はネットワークを有効利用する仕組みだが、セキュリティとも相性がよい プロキシサーバー.....	152
6-04	攻撃を検知し、防御につなげる仕組み IDS/IPS/UTM.....	154
6-05	安全にネットワークを利用するための仕組み VPN.....	156
6-06	VPN を実現するためのプロトコル IPsec.....	158
6-07	端末をインターネット越しに安全に内部ネットワークに参加させる仕組み PPTP と SSTP.....	160
6-08	目的や用途に応じて最適な実装方法を選択する その他の VPN 実装技術.....	162
6-09	安全なリモートログイン SSH.....	164
6-10	SSH 以前の安全でないリモートログインの手段 Telnet.....	166
COLUMN	ネットワークセキュリティの肝.....	168

セキュリティ関連の法律・規約・取り組み

7-01	セキュリティを確保するための法律 セキュリティに関する 3 つの法律	170
7-02	似て非なる 2 つの情報 個人情報とマイナンバー	172
7-03	今ある法律でセキュリティ上の脅威と闘う 従来の法律を用いた対応策	174
7-04	安全にネット社会を生きるために 法令遵守を徹底する	176
7-05	情報資産のセキュリティを管理する 情報セキュリティマネジメントシステムと 個人情報保護マネジメントシステム	178
7-06	脆弱性の届出受付機関と調整機関 IPA と JPCERT/CC	180
7-07	必要な脆弱性情報を必要なところに送り届ける仕組み 情報セキュリティ早期警戒パートナーシップ	182
7-08	情報処理安全確保支援士、CISSP セキュリティ関連の資格	184
7-09	日本政府が設置するセキュリティ機関 内閣サイバーセキュリティセンター	186
7-10	CSIRT 連携のための枠組み 日本シーサート協議会と FIRST	188