

## 目次

2 情報セキュリティにおける脅威.....	4
2.1 脅威の分類と概要.....	4
2.1.1 脅威の分類.....	4
2.1.2 災害の脅威.....	4
2.1.3 障害の脅威.....	5
2.1.4 人の脅威.....	6
2.1.5 サイバーセキュリティ情報を共有する取り組み.....	9
2.2 ポートスキャン.....	10
2.2.1 ポートスキャンの目的と実行方法.....	10
2.2.2 ポートスキャンの種類と仕組み.....	10
2.2.3 ポートスキャンへの対策.....	12
2.3 バッファオーバーフロー攻撃.....	13
2.3.1 BOF 攻撃の仕組み.....	13
2.3.2 バッファオーバーフロー攻撃の影響.....	14
2.3.3 攻撃されないための対策.....	15
2.3.4 DoS 攻撃との違い.....	16
2.4 パスワードクラック.....	17
2.4.1 パスワードクラックの種類と実行方法.....	17
2.4.2 パスワードクラックへの対策.....	20
2.5 セッションハイジャック.....	23
2.5.1 セッションハイジャックとは.....	23
2.5.2 セッションハイジャックの原因とは.....	24
2.5.3 セッションハイジャック攻撃による影響.....	24
2.5.4 セッションハイジャックされないための対策.....	25
2.6 DNS サーバに対する攻撃.....	26
2.6.1 DNS サーバの種類.....	26
2.6.2 攻撃の種類.....	26
2.6.3 ゾーン転送とは.....	26
2.6.4 DNS キャッシュポイズニング攻撃.....	27
2.6.5 カミンスキー攻撃.....	28
2.6.6 DNS リフレクション攻撃とは.....	29

2.6.7 DNS 水責め攻撃（ランダムサブドメイン攻撃） .....	32
2.6.8 攻撃の分類.....	34
2.6.9 DDoS 攻撃全般.....	36
2.6.10 DNS サーバの影響？ .....	36
2.6.11 対策.....	37
2.7 DoS 攻撃.....	41
2.7.1 DoS 攻撃とは.....	41
2.7.2 特殊な DoS 攻撃、F5 アタックとは.....	41
2.7.3 DDoS 攻撃の種類 1.....	42
2.7.4 DDoS 攻撃の種類 2.....	43
2.8 Web アプリケーションに不正なスクリプトや命令を実行させる攻撃.....	47
2.8.1 種類.....	47
2.8.2 クロスサイトスクリプティング.....	47
2.8.3 SQL インジェクション.....	48
2.8.4 OS コマンドインジェクション.....	48
2.8.5 HTTP ヘッダインジェクション.....	48
2.8.6 メールヘッダインジェクション.....	49
2.8.7 ディレクトリトラバーサル攻撃.....	49
2.8.8 Web アプリケーションにみられる脆弱性.....	50
2.8.9 Web アプリケーションの脆弱性が生まれる原因.....	50
2.8.10 現在知られている Web アプリケーションの主要な脆弱性.....	51
2.9 マルウェアによる攻撃.....	53
2.9.1 種類.....	53
2.9.2 コンピュータウイルス、ワーム.....	53
2.9.3 トロイの木馬.....	54
2.9.4 悪意あるモバイルコード.....	54
2.9.5 スパイウェア.....	54
2.9.6 ボット.....	54
2.9.7 ランサムウェア.....	59
2.9.8 ドロップ.....	61
2.9.9 Gumbler.....	61
2.9.10 標的型攻撃.....	63
2.9.11 マルウェアを検出する手法.....	68