

サイバー攻撃におけるインシデント対応 ～疑似環境を用いた解析～

目次

第1章 サイバー攻撃の現状を理解する	
1.1 サイバー攻撃の実態	2
1.1.1 サイバー空間(領域)の問題	2
1.1.2 サイバー攻撃とは	3
1.1.3 サイバー攻撃の現状	4
1.2 サイバー攻撃の傾向	6
1.2.1 サイバー攻撃と対策の変遷	6
1.2.2 高度標的型攻撃	7
1.3 サイバー攻撃の実例	8
1.3.1 国内のサイバー攻撃事案	8
1.3.2 サイバー攻撃の事例(1)	9
1.3.3 サイバー攻撃の事例(2)	10
第2章 サイバー攻撃の手口を理解する	
2.1 高度標的型攻撃の手口	12
2.1.1 高度標的型攻撃の流れ	12
2.2 準備段階	13
2.2.1 事前調査	13
2.2.2 使用デバイスの調査	14
2.3 攻撃準備段階	15
2.3.1 侵入のシナリオ	15
2.3.2 標的型メール攻撃の動向	16
2.3.3 標的型メール攻撃	17
2.3.4 水飲み場攻撃	18
2.4 初期侵入段階	19
2.4.1 コネクトバック	19
2.4.2 C&C サーバによる遠隔操作	20
2.5 内部侵入拡大・情報探索段階	21
2.5.1 ネットワーク情報・ユーザー情報の調査	21
2.5.2 運用管理ツールによる内部侵入拡大	22
2.6 目的遂行段階	23
2.6.1 収集した機密情報の外部への持ち出し	23
第3章 インシデント対応を理解する	
3.1 インシデント対応とは何か	26
3.1.1 インシデント対応とは	26
3.1.2 CSIRT(コンピュータセキュリティインシデントレスポンスチーム)とは	27
3.2 インシデント対応の手順を理解する	28
3.2.1 インシデント対応のプロセス	28
3.2.2 CSIRT によるインシデント対応の流れ	29
3.2.3 事前準備	30
3.2.4 インシデント発生時の初動対応	35
3.2.5 データ保全	40
3.2.6 調査・解析	45
3.2.7 報告と情報開示	49
3.2.8 復旧および対処	53
3.3 インシデント対応における留意事項を理解する	57
第4章 インシデント対応を疑似体験する	
4.1 インシデント対応の疑似体験実習	60

第5章 サイバー攻撃に備える

5.1 3つの対策	62
5.1.1 入口対策	64
5.1.2 内部対策	71
5.1.3 出口対策	77
参考1 メモリ保全	83
参考2 HDD 保全	93
参考3 メモリ解析	107
参考4 復元	123
参考5 タイムライン解析	129
参考6 ファイル解析	157
参考7 アプリケーション履歴	183
参考8 レジストリ解析	193
参考9 OSForensics	247