

目次

はじめに	iii
謝辞	v

第 1 章 サイバー攻撃に勝つための 根本的な対策とは

1

1-1 サイバー攻撃に関する情報で 混乱していませんか？	2
コンサルタントの仕事とは何か？	2
セキュリティの理論と実践	4
1-2 サイバー攻撃のリスクが 高いままでもいいですか？	8
1-3 サイバー攻撃の歴史を振り返る	12
媒体型のウィルスの時代	12
電子メールウィルスの時代	12
ネットワークワームの時代	12
マルウェアを使ったアンダーグラウンドビジネスの確立	13
ボットネットの登場	13
ハクティビズムの台頭	14
サイバーエスピオナージとサイバーウォーフェア (サイバースパイとサイバー紛争)	14
1-4 サイバー攻撃：数字に見る現状	16
1-5 敵を知る：犯罪を起こす条件とは？	19
手段も豊富	19
機会も豊富	19
動機も豊富	20
1-6 制御を奪われるな	22
情報セキュリティのC・I・Aとは？	22
品質管理ノウハウをセキュリティに応用	25

第2章 なぜ禁止するだけの セキュリティ対策ではダメなのか？ 27

2-1	禁止されたら抜け道を考えるだけ	28
2-2	そもそも情報セキュリティの目的とは何か？	31
	なぜ情報の機密性、完全性、可用性を維持するのか	31
	セキュリティと生産性の関係を考えていますか？	31
2-3	セキュリティと security は同じ意味？	36
	アメリカと日本の違い	37
2-4	スマホ・タブレットへの期待は 現状への不満の表れ？	39
	BYOD は時代の流れ	39
	会社主導でモバイル端末を支給する場合	40
	BYOD 導入以前の不便さ	41
2-5	マイクロソフト社内事例	43
2-6	イソップ物語 「北風と太陽—どちらが目的を達成できるか？」	45
	禁止するか、許すか	45
	ブラックリスト型対策 vs ホワイトリスト型対策	47
	セキュリティで非効率になっていませんか？	49

第3章 よく言われている入口対策/ 出口対策だけでは不十分な理由 51

3-1	不十分な理由その1 「こんなネットワーク構成で安心していませんか？」	52
	インターネットに接続しモバイル環境も 充実させているパターン	52

典型的なネットワーク構成でどこまで守れるか	53
モバイル端末がセキュリティをすり抜ける現状	54
インターネットに接続しないから安心とは言えない	55
攻撃の入口の多様化	57
3-2 不十分な理由その2	
「こんな検討をしていませんか？」	59
新しい攻撃パターンの発生	59
3-3 リスクを見つけるために	
サイバー攻撃の歴史を探る	61
従来型サイバー攻撃	61
境界型セキュリティ対策	62
昨今のサイバー攻撃「標的型攻撃」	63
進化する攻撃者	64
3-4 内部犯行はないという前提の危うさ	66
3-5 入口対策／出口対策は境界型対策の言い換え!?	68
3-6 多層防御と多重防御について	69
How defense in depth goes wrong	69
品質管理をセキュリティに当てはめる	70
3-7 この章のまとめ	72

第4章 なぜウィルス対策ソフトウェア だけでは足りないのか？ 75

4-1 ウィルス対策ソフトウェアとパターンファイルの 最新化はもちろん大事だけど……	76
期待される対策機能が果たされていますか？	76
ウィルス対策ソフトウェアの仕組みと問題点	77
4-2 日々変化する攻撃者のアプローチテクニック	79
高度なサイバー攻撃とは何か？	79
4-3 ウィルス対策ソフトウェアと多層防御の関係	83

切っても切れないCIAの関係	83
4-4 リスク分析していますか？	85
セキュリティチェックリストだけでは足りない理由	85
ウィルス対策ソフトウェアの限界	86
4-5 FTAの勧め	87
FTAとは	87
日常生活でのFTA	87
FTAによるセキュリティ分析の実際	89
4-6 この章のまとめ	93

第5章

定番どおりではやられ放題。 セキュリティの定石は裏口だらけ？

95

5-1 Active Directoryは どのように守っているのか？	96
莫大なユーザー数とサーバー数を管理	96
なぜセキュリティ上の危険にさらされないのか？	97
5-2 サーバルームのよくある運用	100
機密性の基本：物理的な保護を実施する	100
完全性の基本：正しい設備・環境で運用する	101
可用性の基本：安定運用するために備える	102
5-3 ついついサーバルームに入らず 遠隔操作で済ませていませんか？	103
5-4 知っているつもり!? Active Directory	104
認証基盤の仕組みを押さえる	104
Active Directoryはどのように使うのか？	104
5-5 Active Directoryはどのように攻撃されたのか？	112
サイバー攻撃の方法	112
サイバー攻撃への対策	114
Active Directoryの認証と監査の仕組みとは	115

5-6 Administratorで 直接ログオンしたらなぜダメなのか？	117
ドミノ倒しを防ぐ方法を考えていますか？	117
管理者アカウントの絶大な威力を忘れていませんか	117
Administratorを守る6の方法	118
5-7 この章のまとめ	121

第6章

ICカード認証でセキュリティの 足下をすくわれていませんか？ 123

6-1 ICカードによるPCログオンの運用実態	124
非接触ICカード導入は正しいか？	124
非接触ICカード利用の盲点とは何か？	124
PC（端末）ではなくネットワークを守る	128
非接触ICカードの意外な盲点	130
6-2 ICカード単体のセキュリティと ネットワークの認証強度は結び付かない!?	132
HSMをご存じですか？	132
6-3 ICカードの導入前に整備すべきこと	135
IDが散在している場合の課題	135
6-4 IDのライフサイクルで重要なポイント	138
入社での課題	138
異動での課題	138
退職での課題	139
6-5 ICカードに関するライフサイクル	141
カード発行	141
カード配布	141
カード返却	141
カード紛失・盗難	142
6-6 業界標準技術を使うということ	143

6-7 Active DirectoryとICカードに格納する データの関係	147
Active Directoryのケルベロス認証	147
そもそもスマートカードログオンの優位点とは	151
6-8 マイクロソフト社のICカード運用事例	152
パスワードによる認証とICカードによる認証	152
仮想スマートカードログオン	153
6-9 まとめ	155

第7章	
実効性ある対策のための 戦略と戦術の提言	157

7-1 日本は情報セキュリティまでガラパゴスか？	158
7-2 「初期の攻撃」と「被害内容」に 焦点が当たりすぎていないか？	160
7-3 プロアクティブなセキュリティ対策を	162
プロアクティブか、リアクティブか	162
リスク分析とセキュリティ監査	163
「予防措置」をいかに実現するか	164
7-4 情報セキュリティのキャズム	167
なぜ継続的に情報セキュリティポリシーが 実践されないのか	167
スムーズな運用ができるセキュリティポリシーとは	170
7-5 3つのPとは	172
情報システム運用のための構成要素をまとめよう	172
PDCAのサイクルの回し方	173
7-6 戦略は大胆に、戦術は緻密に	176
ラグビーの戦略をビジネスに活かす	177
 索引	 181