目 次

はじめに iii
謝辞 v

第1章 セキュリティコンサルティングの現場から
——多くの誤解のままセキュリティ対策が検討されている実態 1

1-1 ◆情報流出が続く理由 2
1-2 ◆うっかり PC を紛失したときを想定した対策をしていますか 4
Column 情報セキュリティ対策に役立つフェイルセーフ 8
1-3 ◆セキュリティインシデントごとに命名される攻撃名称に翻弄されていませんか 9
1-4 ◆ID +パスワードによる認証の認識不足について 13
1-5 ◆パスワードは 8 文字と 128 文字のどちらが安全か？ 18
Column キーロガーに見る技術の二面性 19
1-6 ◆「暗号化していれば安全なのに」は本当か？ 21
1-7 ◆放置される情報セキュリティポリシー 23
1-8 ◆情報セキュリティの基本 26

第2章 現在の状況　攻撃側と防御側の実態 27

2-1 ◆なぜ、セキュリティが経営上の深刻な課題になってきたのか 28
2-2 ◆報道やニュースの事実だけで対策していませんか？ 30
2-3 ◆「セキュリティはサーバールームの課題から役員室の課題に」の本当のところ
～情報セキュリティはもともと経営の課題 32
2-4 ◆1,425% という数字の衝撃 34
2-5 ◆セキュリティ関連担当者の実態 35
2-6 ◆ROI 算出の仮説に見る攻撃側のプロフェッショナリズム 39
2-7 ◆防御側の弱点が共通化する理由 42
2-8 ◆情報セキュリティの現状 45
Column ちょっとうれしかったこと 46

第3章　もう一度「基礎」に立ち戻る 47

3-1 ◆情報セキュリティは科学であること 48
3-2 ◆リスクを理解するために大切な観点 51
3-3 ◆認証とセキュリティが結びつかない方へ 54
3-4 ◆効果的対策のための 3 つの重要ポイント 58
1. 根本原因を特定して対策すること 58
2. 運用の重要性 58
3. 目的志向の重要性 59
3-5 ◆情報セキュリティとサイバーセキュリティは何が違うのか 61
3-6 ◆情報セキュリティはいつ設計するのか 63
あとからセキュリティを考えるとは 63
セキュリティファーストにしていくために 65

3-7 ◆情報セキュリティの基本対策 67
Column 「脅威と脆弱性とリスク」の違いを理解していますか？ 68

第4章 復習 「認証基盤とは何か」 69

4-1 ◆なぜ情報流出防止のために認証基盤が重要なのか？ 70

4-2 ◆そもそも認証基盤とは何か 72
AAAをイメージするために 72
複数の認証基盤が混在するケースの課題 74
アカウンティングの課題とは 75
フェデレーションとは 76

4-3 ◆識別・認証・認可をきちんと説明できますか？ 79
認可とは 79
識別と認証 79

4-4 ◆3つの認証方式の特徴と注意点 82
知識による認証 82
所有による認証 83
Column スマートカード 84
生体による認証 85
Column パスワードのポリシーの変化について 86

4-5 ◆説明責任（アカウンタビリティ）を支える認証基盤 87
Column あえて共有アカウントを利用するシーンとは 88

第5章 Windows環境における認証基盤 Active Directoryの構築勘所 89

5-1 ◆認証基盤としてのActive Directoryを狙う攻撃 90

5-2 ◆認証基盤を守りぬくには 94
管理権限のある資格情報の保護 94
ドメインコントローラーの脆弱性の排除 96
ドメインコントローラーの適切な構成 97
ドメインコントローラーが守られていることの確認（監視） 97

5-3 ◆あらためて最小特権の原則を理解する——委譲と委任の違い 99
Column 権限の委任先 100

5-4 ◆構築後のActive Directoryをどのように運用するのか 103
構成が維持されているかの確認 103
稼働状態の確認 104
オブジェクトの状態の確認 105

5-5 ◆利用されないまま眠っているグループポリシーも効果抜群 106

5-6 ◆管理用アカウントは専用端末からだけログオンさせる方法 108

5-7 ◆攻撃の予兆を監視するには 111
注目すべきイベント 113
Column Advanced Threat Analytics (ATA) 115

第6章 認証基盤とクラウド 117

6-1 ◆オンプレミスからクラウドへ 118
Column クラウドの特徴 119

6-2 ◆クラウド利用時も考慮するべきセキュリティとは 120
Column パスワードリスト攻撃の温床を断つには 123

6-3 ◆より多くのクラウドサービスとの連携 125

6-4 ◆信頼できるクラウドサービスの選別 128

6-5 ◆クラウド利用により適したOSへの移行 129

認証方式の窃取・再利用防止機能……129
パスワード以外の認証方式……130
Column Microsoft Passport……131
Column TPM (Trusted Platform Module)……132

6-6 ◆新しい OS に移行するときの注意点……133

第7章　認証基盤が奪われたらゲームオーバー　135

7-1 ◆防災の考え方からセキュリティをとらえる……136
Column 巨大防潮堤のもう1つの課題……138

7-2 ◆情報流出だけがセキュリティインシデントではない……139

7-3 ◆セキュリティ対策の「部品」を「構造物（アーキテクチャ）」にするには？……141
Column ゼロデイ攻撃……142

7-4 ◆想定外は本当に想定外か？……144

7-5 ◆情報セキュリティ人材不足の本当のところ……147

7-6 ◆安全と安心の違い……151

7-7 ◆情報セキュリティの「変わること」と「変わらないこと」……153

索引……156
あとがき……163