
目 次

1章 情報セキュリティ	1
1.1 ネットワーク社会における危険の増大	2
1.1.1 ネットワークの時代	2
1.1.2 ネットワーク社会のリスク	3
1.2 情報セキュリティの重要性と社会的責任	5
1.2.1 情報セキュリティの重要性	5
1.2.2 情報セキュリティの社会的責任	8
1.2.3 箱のセキュリティと情報のセキュリティ	10
1.3 情報セキュリティの今後	11
1.3.1 民需領域での情報セキュリティ強化	11
1.3.2 情報セキュリティの国際的整合	15
1.4 情報セキュリティの概要	18
1.4.1 情報セキュリティおよびIT	18
1.4.2 脅威と情報セキュリティ事故	19
1.5 情報セキュリティ対策	26
1.5.1 秘密性に対する脅威への対策	26
1.5.2 完全性に対する脅威への対策	28
1.5.3 可用性に対する脅威への対策	31
1.5.4 ITの運用と管理による情報セキュリティ対策	32
1.5.5 不正アクセス対策	33
1.5.6 コンピュータウイルス対策	35
1.5.7 暗号およびデジタル署名	38
1.6 情報セキュリティ対策の構築	42
1.6.1 セキュリティポリシーの準備	42
1.6.2 セキュリティポリシーの展開	46
1.6.3 使用者の責務	50

2章 ISO15408「ITセキュリティ評価基準」とその背景	52
2.1 ITセキュリティ評価とは	53
2.1.1 情報セキュリティへの取り組み	53
2.1.2 個別セキュリティ技術への取り組み	54
2.1.3 ITセキュリティ全体への取り組み	59
2.1.4 ITセキュリティ評価基準の国際標準化ニーズ	60
2.2 ITセキュリティ評価の歴史とISO15408「CC」の背景	61
2.2.1 アメリカのTCSEC	61
2.2.2 EUのITSEC	65
2.2.3 その他の国の状況	67
2.3 CCプロジェクト	68
2.3.1 CCプロジェクトの発足	68
2.3.2 目的・効果	69
2.3.3 CCEB	70
2.3.4 CCIBとタスクグループ	71
2.3.5 CCIMB	73
2.4 ISOによる国際標準化と金融におけるセキュリティ	74
2.4.1 ISOによる国際標準化	74
2.4.2 ISO/TC68のITセキュリティに関する標準化活動	77
2.4.3 ICカードのセキュリティ	78
2.5 セキュリティ評価、認証、制度、相互承認	81
2.5.1 ITセキュリティ評価の困難さ	81
2.5.2 評価認証	83
2.5.3 セキュリティ評価・認証制度	85
2.5.4 相互承認	92
2.6 第三者評価の文化	95
2.6.1 製品評価と評価ビジネス	95
2.6.2 評価機関認定	96
2.6.3 評価機関認定の相互承認	99
2.7 ISO15408「CC」の特徴と留意点	100
2.7.1 ISO15408「CC」の特徴	100
2.7.2 ISO15408「CC」の留意点	104

2.8 ISO15408「CC」のインパクト	108
2.8.1 ITセキュリティ技術へのインパクト	108
2.8.2 IT製品ビジネスへのインパクト	110
2.8.3 ネットワークビジネスへのインパクト	112
2.8.4 評価ビジネスとの関連	113
3章 ISO15408「ITセキュリティ評価基準」の概要	114
3.1 ISO15408「CC」の構成	115
3.2 ISO15408「CC」Part1の要点と考え方	116
3.2.1 適用範囲と除外項目	116
3.2.2 利用者と利用方法	119
3.2.3 セキュリティの実現	120
3.2.4 開発プロセスと評価用提出資料	124
3.2.5 ITセキュリティ評価結果	126
3.2.6 PPおよびSTに対する留意事項	127
3.3 ISO15408「CC」Part1 付属書とCC利用法	128
3.3.1 付属書B（規定） PPの仕様	128
3.3.2 付属書C（規定） STの仕様	130
3.3.3 PP/STの内容	130
3.3.4 ISO15408「CC」と製品開発および評価の流れ	138
3.4 ISO15408「CC」Part2の要点と考え方	140
3.4.1 ISO15408「CC」Part2の構成	140
3.4.2 セキュリティ機能のモデルと用語	141
3.4.3 機能要件の構成と記述の構成	145
3.4.4 コンポーネント記述における留意事項	151
3.4.5 セキュリティ機能クラス，ファミリー一覧	154
3.5 ISO15408「CC」Part3の要点と考え方	154
3.5.1 ISO15408「CC」Part3の構成	154
3.5.2 ISO15408「CC」における保証の考え方	155
3.5.3 PPおよびSTの評価	158
3.5.4 保証要件の構成と記述の構成	159
3.5.5 セキュリティ保証クラス，ファミリー一覧	164
3.6 評価保証レベルと保証維持の考え方と要件	165
3.6.1 評価保証レベルの考え方	166

3.6.2	評価保証レベル概要	168
3.6.3	保証維持の考え方	172
3.6.4	保証要件 クラスAMA：保証維持	175

4章	情報セキュリティに貢献するISO15408「CC」	178
4.1	情報セキュリティ対策の考慮点	179
4.1.1	基本3条件	179
4.1.2	追加2条件	181
4.2	「PP/ST作成ガイド案」と情報セキュリティ	184
4.2.1	「PP/ST作成ガイド案」と情報セキュリティの関連	184
4.2.2	セキュリティニーズの決定	185
4.2.3	セキュリティ目標の決定	189
4.2.4	セキュリティ要件の決定	191
4.3	ベンダにおけるISO15408「CC」への対応と活用	193
4.3.1	ISO15408「CC」対応にむけて	194
4.3.2	ISO15408「CC」への計画的対応	196
4.3.3	セキュリティ品質の作り込み	201
4.4	ユーザにおけるISO15408「CC」の活用	202
4.4.1	PPによるセキュリティ要求仕様の提示	202
4.4.2	STを活用した製品の選択と運用	207
4.4.3	技術標準としての利用	208
4.5	ユーザにおける情報システムの運用	208
4.5.1	セキュリティ評価基準とシステムセキュリティ基準	208
4.5.2	システムセキュリティ基準	210
4.5.3	自社のシステムセキュリティ基準づくり	217
4.6	セキュリティ評価、認証の利用	217
4.6.1	ITセキュリティ評価・認証済み製品の利用	218
4.6.2	適切な評価保証レベルの選択	219
4.6.3	製品・サービスの差別化	221

付録 A	セキュリティ機能要件の概要	222
A.1	クラスFAU：セキュリティ監査	222
A.2	クラスFCO：通信／否認防止	223
A.3	クラスFCS：暗号利用	224
A.4	クラスFDP：ユーザデータ保護	225
A.5	クラスFIA：識別と確認	229
A.6	クラスFMT：セキュリティ管理	230
A.7	クラスFPR：プライバシー	232
A.8	クラスFPT：セキュリティ機能保護	233
A.9	クラスFRU：可用性とリソース管理	237
A.10	クラスFTA：アクセス制御	238
A.11	クラスFTP：高信頼性経路	239
付録 B	セキュリティ保証要件の概要	241
B.1	クラスAPE：PPの評価	241
B.2	クラスASE：STの評価	242
B.3	クラスACM：構成管理	244
B.4	クラスADO：配布と運用	245
B.5	クラスADV：開発と実装	246
B.6	クラスAGD：ガイダンス文書	250
B.7	クラスALC：ライフサイクルサポート	251
B.8	クラスATE：テスト	252
B.9	クラスAVA：脆弱性評価	252
B.10	クラスAMA：保証維持	253
参考文献・参考規格		254
参考資料		255
参考WEBページ		257
さくいん		258