

はじめに	iii	プロトコルレベルでの暗号化およびクライアント認証	86
謝辞	v	セキュリティエンジニアリングチェック表	91
監修者まえがき	vi		
第 1 章 Web アプリケーションの世界におけるセキュリティ	1	第 4 章 HyperText Markup Language	93
情報セキュリティとは	1	HTML ドキュメントを支える基本概念	94
Web が歩んできた道	11	ドキュメントのパーズモード	95
脅威の進化と変遷	19	HTML パーサーの振る舞いを理解する	98
		エンティティエンコーディング	102
第 I 部 Web の構成要素	27	HTTP/HTML を統合するセマンティクス	105
		ハイパーリンクとコンテンツのインクルード	106
第 2 章 URL から始めよう	29	セキュリティエンジニアリングチェック表	114
URL の構造	30		
予約文字とパーセントエンコーディング	39	第 5 章 Cascading Style Sheets	117
一般的な URL のスキームとその機能	46	CSS の基本構文	118
相対 URL の解決	49	パーサーの再同期に関連するリスク	121
セキュリティエンジニアリングチェック表	52	文字エンコーディング	123
		セキュリティエンジニアリングチェック表	125
第 3 章 HyperText Transfer Protocol	55		
HTTP トラフィックの基礎構文	56	第 6 章 ブラウザサイドスクリプト	127
HTTP リクエストの種類	69	JavaScript の基本的な特徴	128
サーバーレスポンスコード	72	標準オブジェクト階層	143
キープアライブセッション	76	スクリプトの文字エンコーディング	149
チャンクデータの送受信	78	コードのインクルードモードとネストの危険性	151
キャッシュの振る舞い	79	死んだはずだよ: Visual Basic	153
HTTP クッキーのセマンティクス	81	セキュリティエンジニアリングチェック表	154
HTTP 認証	84		
		第 7 章 HTML 以外のドキュメント	157
		プレーンテキストファイル	157
		ビットマップ画像	158

オーディオ/ビデオ	159
XML ベースのドキュメント	160
描画不可能なファイルタイプについて一言	166
セキュリティエンジニアリングチェック表	168
第 8 章 ブラウザプラグインを使用したコンテンツ描画	169
プラグインの起動	170
ドキュメント描画ヘルパー	173
プラグインベースのアプリケーションフレームワーク	174
Sun Java	179
ActiveX コントロール	182
その他のプラグインとの共存	183
セキュリティエンジニアリングチェック表	185
第 II 部 ブラウザのセキュリティ機能	187
第 9 章 コンテンツ分離ロジック	189
DOM の同一生成元ポリシー	190
XMLHttpRequest における同一生成元ポリシー	196
Web ストレージと同一生成元ポリシー	198
クッキーのセキュリティポリシー	200
プラグインのセキュリティ規則	207
曖昧な生成元と意図とは異なる生成元のコピー	214
その他の生成元	219
セキュリティエンジニアリングチェック表	220
第 10 章 生成元の継承	223
about:blank で生成元を継承する	224
data: URL での継承	225

javascript:URL と vbscript:URL における継承	228
制約を受ける擬似 URL について一言	230
セキュリティエンジニアリングチェック表	231
第 11 章 同一生成元規則以外のこと	233
ウィンドウとフレームのインタラクション	234
ドメインを超えたコンテンツのインクルード	243
プライバシーに関連した副チャンネル	247
その他の抜け穴とその使用法	250
セキュリティエンジニアリングチェック表	251
第 12 章 その他のセキュリティ境界	253
要注意のスキームへのナビゲーション	253
内部ネットワークへのアクセス	255
禁止ポート	257
サードパーティのクッキーを制限する	259
セキュリティエンジニアリングチェック表	263
第 13 章 コンテンツを識別する仕組み	265
ドキュメントタイプの検出ロジック	266
文字セットの処理	277
セキュリティエンジニアリングチェック表	285
第 14 章 不正なスクリプトの取り扱い	287
DoS 攻撃	288
ウィンドウの位置と外観についての問題	296
ユーザーインターフェイスへのタイミングアタック	299
セキュリティエンジニアリングチェック表	302

第 15 章 外部サイトの特権	303
権限：ブラウザ管理のサイトとプラグイン管理のサイト	304
フォームベースのパスワードマネージャー	306
Internet Explorer のゾーンモデル	308
セキュリティエンジニアリングチェック表	313
第 III 部 次にくるもの	315
第 16 章 新たなセキュリティ機能	317
セキュリティモデル拡張フレームワーク	318
セキュリティモデルを制約するフレームワーク	325
その他の発展	337
セキュリティエンジニアリングチェック表	341
第 17 章 その他のブラウザの機構について	343
URL レベル／プロトコルレベルの提案	343
コンテンツレベルの機能	346
I/O インターフェイス	348
第 18 章 広く知られている Web の脆弱性	351
Web アプリケーションに固有な脆弱性	351
Web アプリケーション設計時の注意点	353
サーバーサイドのコードに見られる一般的な問題	355
付録 A エピローグ	359
付録 B リソース	361
索引	378