これから“セキュリティ技術”を学ぶ方へ

◎『セキュリティ技術の教科書』の執筆コンセプト

本書は，次のような方を想定読者として執筆しました。

・これから社会人になり，IT パーソンとして活躍しようと志している学生の方
・既に IT パーソンとして実務を行いながら，セキュリティ技術全般を学習しようとする方
・情報処理安全確保支援士試験の午前Ⅱ試験におけるセキュリティ分野の専門知識を効率的，かつ，しっかりと理解したい方

セキュリティに係わる IT パーソンは，ホワイトハッカー（3.1.2 節参照）と呼ばれるようなセキュリティプロフェッショナルと，その他の様々な領域の IT プロフェッショナルに分類されます。後者の“様々”というのは，プログラマやシステムアーキテクト，ネットワークエンジニアや基盤系エンジニア，フィールドエンジニア，データベースエンジニアや組込みエンジニア，IT コンサルタントやプロジェクトマネージャ，サービスマネージャやシステム監査人などです。

セキュリティに係わる IT パーソンのうち，95％は後者だと言われています。職種が多いので当然です。重要なポイントは，セキュリティプロフェッショナルはもちろん，他のいずれの領域で活動するにしても，セキュリティ技術の知識が必要だということです。

このような多様な IT パーソンの方向けに，ITSS（IT スキル標準）レベル 3 ～ 4 のセキュリティ技術全般の基礎を整理しました。そのため，ITSS レベル 2（基本情報技術者）の IT 知識をもっている方がより知識を深めるのに最適です。

◎執筆に当たって

本書は，情報処理安全確保支援士試験（情報セキュリティスペシャリスト試験）の対策セミナー向けのレジュメをベースに制作しました。レジュメに対する典型的なご意見は，「コンパクトでよくまとまっているけど，読んだだけでは分からない部分があります」でした。今回，書籍として制作する機会を得て，「読んで分かる」を目指して再構成・加筆しました。

IT 技術全般と同様，セキュリティ技術の学習では，目に見えない概念的（論理的）な内容を理解することが必要です。そこで，本書では図解を心がけています。理解を定着させるためには，自分で図を描いてみることをお勧めします。

本書を学習して十分に理解したセキュリティ技術の基本が，現場におけるセキュリティ実践の礎として役立つことを期待しています。

2017.6　著者　長嶋　仁

◎本書の構成と使い方

(1) 本書の構成と使い方

11 章に分類したセキュリティ技術の説明と，各章の大きな節ごとの例題演習で構成しています。例題は，情報セキュリティスペシャリスト試験や応用情報技術者試験の午前問題です。インプットとアウトプットを組み合わせるのが効果的です。例題の解答解説は，全体をまとめて第 12 章に記載しています。

(2) 英字の略号のルビについて

ルビを付けているのは，アルファベット読みではないものです。読み方は唯一ではないものもあります。本書では代表的なものを掲載しています。

例 ARP（アープ） “エーアールピー”ではなく“アープ”なのでルビを付けています。
TLS “ティーエルエス”なのでルビを付けていません。

(3) 法令，規格，ガイドラインについて

法令，規格，ガイドラインなどは，出版後に改正される可能性がありますので，必要に応じて最新の情報を確認してください。

Pick up　―情報処理安全確保支援士試験とは―

前述のとおり，本書は情報処理安全確保支援士試験の学習にもご活用いただけます。そこで，簡単に試験の概要を紹介します。※以下，IPA ホームページ（https://www.jitec.ipa.go.jp/）より要約

(1)「情報処理安全確保支援士」の創設

サイバー攻撃の急激な増加により，企業などにおけるサイバーセキュリティ対策の重要性が高まる一方，サイバーセキュリティ対策を担う実践的な能力を有する人材は不足しています。そこで，サイバーセキュリティに関する実践的な知識・技能を有する専門人材の育成と確保を目指して，国家資格「情報処理安全確保支援士」制度が創設されました。

「情報処理安全確保支援士」はサイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し，サイバーセキュリティ対策の調査・分析・評価やその結果に基づく指導・助言を行います。

(2) 登録のメリット

- 国家資格「情報処理安全確保支援士」の資格名称を使用ができる。
- 情報セキュリティに関する高度な知識・技能を保有する証になる。
- 毎年の講習受講により，情報セキュリティに関する最新知識や実践的な能力の維持ができる。

(3) 情報処理安全確保支援士試験

「情報処理安全確保支援士」制度の創設に伴い，従来の情報セキュリティスペシャリスト試験は廃止され，平成 29 年 4 月から新たに情報処理安全確保支援士試験が実施されています。情報処理安全確保支援士試験の合格者は，登録をすることによって，独占的に「情報処理安全確保支援士」の資格名称を使用することができます。

試験に関心を持たれた方，受験を考えている方は，IPA の WEB サイトで詳細情報をご確認ください。支援士資格の登録，講習の受講などに関する FAQ も掲載されていますので，こまめに確認しておきましょう。

http://www.ipa.go.jp/siensi/index.html

目次

これから“情報セキュリティ技術”を学ぶ方へ …… 2

第１章　情報セキュリティとサイバーセキュリティ …… 9
1.1　情報セキュリティからサイバーセキュリティへ …… 10
1.1.1　情報セキュリティとは何か …… 10
1.1.2　サイバーセキュリティとは何か …… 13
1.1.3　例題演習 …… 16

第２章　インターネット技術の基礎 …… 17
2.1　インターネット技術の概要 …… 18
2.1.1　インターネット技術の重要な要素 …… 18
2.2　IP アドレス，ポート番号，MAC アドレス …… 20
2.2.1　IP アドレスと NAT …… 20
2.2.2　ポート番号と NAPT …… 23
2.2.3　MAC アドレス …… 24
2.2.4　例題演習 …… 25
2.3　プロトコルとサービス …… 26
2.3.1　TCP/IP プロトコル群 …… 26
2.3.2　IP …… 27
2.3.3　TCP と UDP …… 28
2.3.4　LAN の通信と ARP …… 30
2.3.5　Web サービスと HTTP …… 34
2.3.6　メールサービスと SMTP，POP3，IMAP4 …… 37
2.3.7　DNS サービスと DNS …… 39
2.3.8　その他のプロトコル …… 42
2.3.9　例題演習 …… 46
2.4　ネットワーク機器 …… 49
2.4.1　ネットワーク接続機器 …… 49
2.4.2　無線アクセスポイント …… 50
2.4.3　例題演習 …… 51
2.5　データベース技術 …… 52
2.5.1　SQL 文 …… 52

第３章　セキュリティに対する脅威 …… 55
3.1　脅威と攻撃者 …… 56
3.1.1　脅威の分類 …… 56
3.1.2　攻撃者の種類と動機 …… 56
3.2　様々な脅威 …… 58
3.2.1　マルウェア …… 58
3.2.2　サイバー攻撃 …… 61

3.2.3　なりすましと不正アクセス …… 71
3.2.4　通信の盗聴や改ざん …… 76
3.2.5　情報機器への攻撃 …… 81
3.2.6　例題演習 …… 82

第４章　暗号技術・認証技術，PKI …… 89
4.1　共通鍵暗号方式と公開鍵暗号方式 …… 90
4.1.1　共通鍵暗号方式 …… 90
4.1.2　公開鍵暗号方式 …… 95
4.1.3　共通鍵暗号方式と公開鍵暗号方式の比較 …… 98
4.1.4　例題演習 …… 99
4.2　ハッシュ関数とメッセージ認証 …… 100
4.2.1　ハッシュ関数 …… 100
4.2.2　メッセージ認証 …… 102
4.2.3　例題演習 …… 105
4.3　ディジタル署名と PKI …… 107
4.3.1　ディジタル署名 …… 107
4.3.2　PKI …… 109
4.3.3　秘密鍵の保護 …… 120
4.3.4　タイムスタンプと XML 署名 …… 122
4.3.5　例題演習 …… 126
4.4　認証方式 …… 130
4.4.1　利用者認証の方式 …… 130
4.4.2　パスワード認証 …… 130
4.4.3　共通鍵認証と公開鍵認証 …… 133
4.4.4　その他の認証方式 …… 137
4.4.5　例題演習 …… 139

第５章　通信の制御とサイバー攻撃対策技術 …… 141
5.1　ファイアウォール …… 142
5.1.1　ファイアウォールの目的 …… 142
5.1.2　ファイアウォールの機能 …… 142
5.1.3　例題演習 …… 147
5.2　プロキシサーバ …… 149
5.2.1　プロキシサーバの種類 …… 149
5.2.2　プロキシサーバの機能 …… 151
5.2.3　例題演習 …… 153
5.3　IDS・IPS …… 154
5.3.1　IDS・IPS の種類 …… 154
5.3.2　IDS・IPS の検知方法と動作 …… 156

5.3.3 例題演習 …… 158
5.4 WAF …… 159
5.4.1 WAF の機能と運用 …… 159
5.4.2 例題演習 …… 162
5.5 サイバー攻撃対策技術 …… 163
5.5.1 マルウェア対策技術 …… 163
5.5.2 標的型攻撃に対する内部拡大・出口対策 …… 166
5.5.3 例題演習 …… 170

第6章 Web システムのセキュリティ …… 173
6.1 HTTP …… 174
6.1.1 HTTP メッセージ …… 174
6.1.2 Cookie …… 180
6.1.3 HTTP 認証 …… 181
6.1.4 例題演習 …… 183
6.2 Web アプリケーションへの攻撃と対策 …… 184
6.2.1 セッションハイジャック …… 186
6.2.2 セッションフィクセーション …… 188
6.2.3 SQL インジェクション …… 190
6.2.4 クロスサイトスクリプティング（XSS） …… 192
6.2.5 クロスサイトリクエストフォージェリ（CSRF） …… 196
6.2.6 ディレクトリトラバーサル …… 199
6.2.7 OS コマンドインジェクション …… 200
6.2.8 バッファオーバフロー（BOF） …… 202
6.2.9 クリックジャッキング …… 204
6.2.10 HTTP ヘッダインジェクション …… 206
6.2.11 メールヘッダインジェクション …… 207
6.2.12 例題演習 …… 210

第7章 メールシステムのセキュリティ …… 213
7.1 メールシステムにおける脅威 …… 214
7.1.1 攻撃メール …… 214
7.1.2 踏み台攻撃 …… 217
7.1.3 メールの盗聴・改ざん，誤送信 …… 218
7.1.4 例題演習 …… 219
7.2 メールシステムのセキュリティ機構 …… 220
7.2.1 POP before SMTP，SMTP-AUTH，APOP …… 220
7.2.2 S/MIME，PGP …… 222
7.2.3 送信ドメイン認証（SPF，DKIM） …… 225
7.2.4 メールのフィルタリング …… 232

7.2.5 OP25B …… 233
7.2.6 Web メール …… 234
7.2.7 例題演習 …… 235

第8章 DNS システムのセキュリティ …… 239
8.1 DNS システムにおける脅威と対策 …… 240
8.1.1 DNS キャッシュポイズニング …… 240
8.1.2 DNS リフレクション …… 245
8.1.3 その他の DNS セキュリティ …… 247
8.1.4 例題演習 …… 249

第9章 セキュアプロトコル …… 251
9.1 トランスポート層のセキュアプロトコル …… 252
9.1.1 TLS …… 252
9.1.2 SSH …… 263
9.1.3 例題演習 …… 268
9.2 ネットワーク層のセキュアプロトコル …… 270
9.2.1 IPsec …… 270
9.2.2 例題演習 …… 278
9.3 LAN のセキュリティ規格 …… 279
9.3.1 IEEE802.1X …… 279
9.3.2 無線 LAN のセキュリティ規格 …… 282
9.3.3 例題演習 …… 285
9.4 認証・認可プロトコル …… 287
9.4.1 SAML …… 287
9.4.2 OAuth …… 289
9.4.3 例題演習 …… 291

第 10 章 システムセキュリティ …… 293
10.1 OS 関連のセキュリティ …… 294
10.1.1 アクセス管理 …… 294
10.1.2 システムのセキュリティ管理 …… 299
10.1.3 スマートフォンのセキュリティ …… 301
10.1.4 例題演習 …… 302
10.2 データベースセキュリティ …… 303
10.2.1 データベースのセキュアな運用 …… 303
10.2.2 例題演習 …… 305
10.3 情報ハイディング技術 …… 306
10.3.1 ステガノグラフィ，電子透かし …… 306
10.3.2 例題演習 …… 307

第 11 章　情報セキュリティマネジメント …… 309
11.1　ISMS の構築と運用 …… 310
11.1.1　ISMS（情報セキュリティマネジメントシステム）… 310
11.1.2　リスクマネジメント …… 311
11.1.3　セキュリティの検査・監視とシステム管理 …… 312
11.1.4　脆弱性管理 …… 314
11.1.5　インシデント対応 …… 317
11.1.6　内部不正対策 …… 320
11.1.7　情報セキュリティの点検 …… 320
11.1.8　例題演習 …… 322
11.2　情報セキュリティ関連規格，ガイドライン，制度 …… 327
11.2.1　CRYPTREC …… 327
11.2.2　ISO/IEC 27000 シリーズ …… 328
11.2.3　その他の関連規格・基準 …… 329
11.2.4　情報セキュリティ関連ガイドライン …… 331
11.2.5　情報セキュリティ関連制度 …… 332
11.2.6　例題演習 …… 334
11.3　情報セキュリティ関連法規 …… 336
11.3.1　サイバーセキュリティ基本法 …… 336
11.3.2　刑法 …… 336
11.3.3　不正アクセス禁止法 …… 337
11.3.4　知的財産権関連法規 …… 338
11.3.5　個人情報保護法 …… 340
11.3.6　その他の情報セキュリティ関連法規 …… 341
11.3.7　例題演習 …… 344

第 12 章　例題演習の解答・解説 …… 345

用語 INDEX …… 406
参考文献 …… 414

1.1 情報セキュリティからサイバーセキュリティへ

これまでは，「情報セキュリティの確保が課題である」といわれてきましたが，最近は，「サイバーセキュリティの確保が課題である」といわれます。その理由は，IoT システムの拡大を背景として，情報セキュリティの確保に加えて，情報システムの安全性の確保も求められているからです。

1.1 節では，セキュリティ技術を活用する目的となる，情報セキュリティとは何か，そして，サイバーセキュリティとは何かを説明します。

1.1.1 情報セキュリティとは何か

(1) 情報セキュリティの定義と特性

▶情報セキュリティ：information security

JIS Q27000:2014“情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語”では，**情報セキュリティ**は次のように定義されています。

> **情報セキュリティ**
> 情報の機密性，完全性，及び可用性を維持すること。さらに，真正性，責任追跡性，否認防止，信頼性などの特性を維持することを含めることもある。

すなわち，情報の機密性，完全性，可用性のいずれかが損なわれると，セキュリティが侵害されたことになります。情報セキュリティの特性のうち，はじめの三つの特性の機密性，完全性，可用性は，**情報セキュリティの 3 要素**と呼ばれ，その頭文字を並べて**情報セキュリティの CIA** ともいいます。

七つの情報セキュリティの特性の意味を次に示します。

図表 1-1　情報セキュリティの特性

番号	特性	説明
①	機密性	権限をもつ人だけが情報にアクセスできる特性
②	完全性	情報が改ざんされることなく正確な状態を保つ特性
③	可用性	情報が使用可能である特性
④	真正性	通信相手や情報が本物で確かである特性
⑤	責任追跡性	動作や事象を追跡できる特性
⑥	否認防止	活動や事象を後から否定させない特性
⑦	信頼性	操作や処理の意図と実行結果が一貫している特性

▶機密性：confidentiality
▶完全性：integrity
▶可用性：availability
▶真正性：authenticity
▶責任追跡性：accountability
▶否認防止：non-repudiation
▶信頼性：reliability

七つの特性について，どのような事象が発生すると情報セキュリティが損なわれるかと，典型的な情報セキュリティ対策の例を次に示します。セキュリティ侵害の要因となる攻撃は第3章，情報セキュリティ対策は第4章以降で具体的に説明します。

①機密性

〔セキュリティ侵害の例〕‥個人情報や社外秘の技術情報のような秘密情報の漏えい，電子メールやWebアクセスにおける通信の盗聴などが挙げられます。

〔セキュリティ対策〕‥機密性対策といえば，情報の暗号化が基本です。他に，情報に対するアクセス制御や不要な情報の確実な消去などがあります。

②完全性（インテグリティ）

〔セキュリティ侵害の例〕‥Webサイトのコンテンツや文書データ，通信でやり取りするメッセージの改ざんが代表例です。**改ざん**とは，情報を不正に変更することです。

〔セキュリティ対策〕‥完全性の対策は，改ざんを防止する対策と改ざんを検知する対策に分かれます。防止対策として，情報に対するアクセス制御，コンピュータやネットワークの物理的な保護，検知対策として，メッセージ認証やディジタル署名があります。

③可用性

〔セキュリティ侵害の例〕‥WebサーバやメールサーバなどへのDoS攻撃や，情報システムにおける障害発生によるサービス停止などがあります。

〔セキュリティ対策〕‥攻撃を遮断する侵入防御システム（IPS）や，情報システムの冗長化があります。**冗長化**とは，情報システムの一部の機能が停止した場合に備えて，サーバやネットワークなどの情報システムの構成要素を二重化したり，バックアップシステムを準備したりすることです。

④真正性

〔セキュリティ侵害の例〕‥なりすましや電子データの偽造・詐称です。**なりすまし**とは，攻撃者や攻撃者が制御する機器が，正当な利用者やサーバ，端末，ネットワーク機器などのふりをして行動あるいは作動することです。また，電子データに関しては，公開鍵証明書の偽造や，TCP/IP通信における送信元IPアドレスの詐称などが挙げられます。

〔セキュリティ対策〕‥真正性を確認する手段は認証です。相手を認証する方式には，パスワード認証や共通鍵認証，公開鍵認証，ディジタル署名など様々な方法があります。

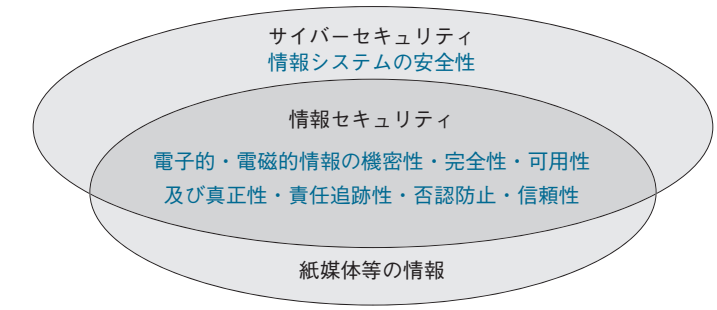
FAQ

情報セキュリティとサイバーセキュリティの違いは何ですか？

ここまでの説明のまとめとして整理します。情報セキュリティとサイバーセキュリティの関係は，図表 1-5 のようになります。

・情報セキュリティは，3 要素の機密性・完全性・可用性，及び真正性，責任追跡性，否認防止，信頼性を維持することです。
・サイバーセキュリティは，さらに安全性を維持することです。

なお，情報セキュリティでは，印刷した資料のような紙媒体の情報も保護の対象にしますが，サイバーセキュリティ基本法の定義では紙媒体の情報の保護は対象外です。



図表 1-5　情報セキュリティとサイバーセキュリティ

情報システムの設計・開発や運用において，安全性を考慮した機能を実装したり，運用手順を実施したりすることは，コストアップにつながるかもしれません。しかし，これからの IT 技術者には，コストパフォーマンスと同時に，安全性も考えていく想像力と倫理観が求められています。

1.1.3　例題演習

問 1-1　■ H24 秋 -AP 問 40

完全性を脅かす攻撃はどれか。

ア　Web ページの改ざん
イ　システム内に保管されているデータの持出しを目的とした不正コピー
ウ　システムを過負荷状態にする DoS 攻撃
エ　通信内容の盗聴。

問 1-2　■ H28 春 -AP 問 39

JIS Q 27000 で定義された情報セキュリティの特性に関する記述のうち，否認防止の特性に該当するものはどれか。

ア　ある利用者がシステムを利用したという事実を証明可能にする。
イ　意図する行動と結果が一貫性をもつ。
ウ　認可されたエンティティが要求したときにアクセスが可能である。
エ　認可された個人，エンティティ又はプロセスに対してだけ，情報を使用させる又は開示する。

3.2 様々な脅威

3.2.1 マルウェア

(1) マルウェア

▶マルウェア：malware

マルウェアは，悪意のある（malicious）ソフトウェア（software）の総称です。次項から説明する，ウイルスやワーム，トロイの木馬，ランサムウェアをはじめとして，コンピュータやスマートフォンの利用者に有害な影響を与える不正なアプリや不正なプログラムなどは，いずれもマルウェアに含まれます。

それぞれのマルウェアは，活動の特徴や攻撃の機能に着目して命名・分類されており，あるマルウェアがいずれか一つの種類に分類されるとは限りません。例えば，ある実在のマルウェアは，「トロイの木馬型のランサムウェア」のように分類されます。

(2) ウイルス（コンピュータウイルス）

▶コンピュータウイルス：computer virus

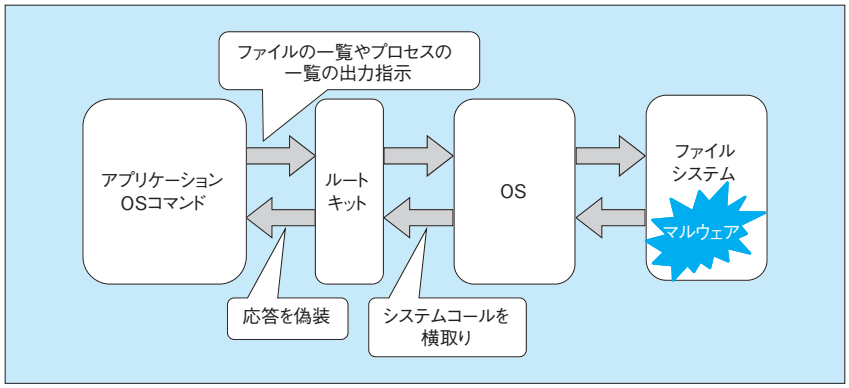
ウイルスは，自らを複製して，他のプログラムやデータファイルのコードに侵入して感染する，寄生型の不正プログラムです。プログラムやデータファイルが実行されると，ウイルスも動作します。

ウイルスの定義は一意ではありませんが，経済産業省の“**コンピュータウイルス対策基準**”では，コンピュータウイルスを次のように定義しています。

> 第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり，次の機能を一つ以上有するもの。
> (1) 自己伝染機能
> 自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより，他のシステムに伝染する機能
> (2) 潜伏機能
> 発病するための特定時刻，一定時間，処理回数等の条件を記憶させて，発病するまで症状を出さない機能
> (3) 発病機能
> プログラム，データ等のファイルの破壊を行ったり，設計者の意図しない動作をする等の機能

なお，コンピュータウイルスという用語は，長年使われて一般に普及しているため，マルウェアと同様に不正プログラムの総称として広義に使われること

隠ぺいされます。



図表 3-2　ルートキットの例

(12) ランサムウェア

▶ランサムウェア：ransom were　ランサムは身代金の意味

▶TOR（トーア）：The Onion Router

ランサムウェアは，感染したコンピュータ内やネットワーク上の記憶装置内のファイルを暗号化して，ファイルの復号と引換えに金銭を要求することが特徴のマルウェアです。匿名性を保持できるネットワークの TOR を利用して，ビットコインのような仮想通貨による支払いを要求するなど，追跡を逃れる手口が使われます。

3.2.2　サイバー攻撃

(1) インターネットサービスへの攻撃

第 2 章で説明した，Web サービス，メールサービス，DNS サービスを標的とする攻撃の例の概要を図表 3-3 に示します。これらの脅威は，セキュリティ対策とセットで学習するほうが整理しやすいため，具体的な攻撃の内容と対策を合わせて，それぞれ第 6 章，第 7 章，第 8 章で説明します。

図表 3-3　インターネットサービスへの攻撃の例

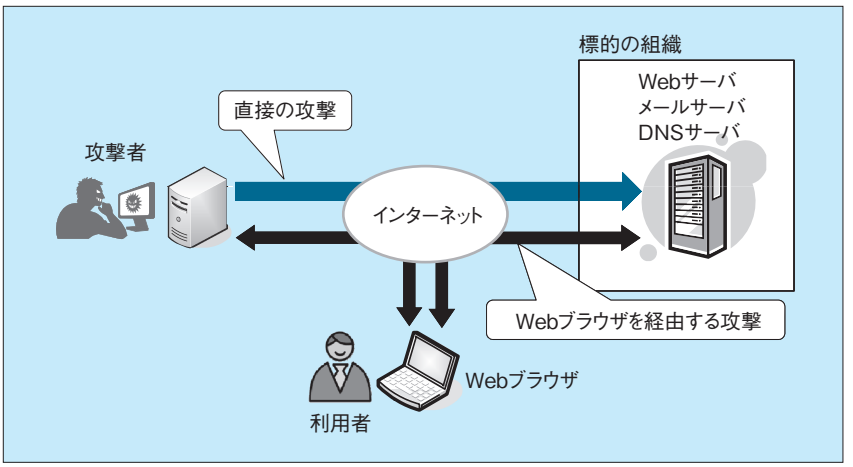
分野	攻撃の名称	概要
Web サービス（6 章）	セッションハイジャック セッションフィクセーション	他人の Web サービスのやり取りを乗っ取る
	SQL インジェクション	データベースを不正に操作する
	クロスサイト スクリプティング	Web ブラウザ上で不正な処理を実行させる
	クロスサイトリクエスト フォージェリ	端末から Web サーバへ，偽装した HTTP リクエストを送信させる

（次頁に続く）

図表 3-3　インターネットサービスへの攻撃の例（続き）

分野	攻撃の名称	概要
Web サービス（6 章）	ディレクトリトラバーサル	Web サービス側が意図しないファイルやディレクトリにアクセスする
	OS コマンドインジェクション	Web サーバ上で OS コマンドを実行させる
	バッファオーバフロー	Web サーバに送り込んだ不正なコードを実行させたり，データを書き換えたりする
	クリックジャッキング	Web サービスに対して意図しないマウス操作を実行させる （次頁に続く）
	HTTP ヘッダインジェクション	HTTP ヘッダを改ざんして，不正な HTTP レスポンスを送信させる
	メールヘッダインジェクション	メールヘッダを改ざんして，不正なメールを送信させる
メールサービス（7 章）	メールの踏み台攻撃	メールサーバから攻撃メールを送信させる
	スパムメール送信	攻撃メールや迷惑メールを送信する
DNS サービス（8 章）	DNS キャッシュポイズニング	DNS サーバに不正なリソースレコードをキャッシュさせる
	DNS リフレクション	DNS サーバを踏み台として，攻撃パケットを送信させる

インターネットサービスへのこれらの攻撃は，図表 3-4 のように，インターネットサーバを直接，あるいは，利用者の Web ブラウザを経由して実行されます。



図表 3-4　インターネットサービスへの攻撃

(2) 標的型サイバー攻撃，APT

標的型サイバー攻撃は，特定の企業や団体，特定企業のサプライチェーン，

第12章 例題演習の解答・解説

1.1.3 例題演習

問 1-1　ア　　完全性を脅かす攻撃　■ H24 秋 -AP 問 40

情報セキュリティの概念には，**完全性（インテグリティ）**［⇒ P.10］，**機密性**［⇒ P.10］，**可用性**［⇒ P.10］の三つがあり，これらを維持することがセキュリティを維持することになる。完全性とは，情報資産の正確さや完全さを保護する特性のことで，データが改ざんされたり削除されたりするリスクのある攻撃は，完全性を脅かす攻撃である。したがって，（ア）が正しい。

イ：機密性を脅かす攻撃である。機密性は，認可されていない利用者などに対して，情報を使用不可あるいは非公開にする特性のことで，権限外のアクセスや不正コピー，情報漏えいや盗聴などの攻撃は機密性にかかわる。

ウ：可用性を脅かす攻撃である。可用性は，認可された利用者などが，要求時にアクセス及び使用できる特性のことで，DoS 攻撃でシステムが正常に使えなくなるのは，可用性にかかわる。ちなみに，DoS（Denial of Service）攻撃とは，サーバなどに大量のデータを送りつけることで，そのサーバが提供するサービスを妨害する攻撃のことである。

エ：機密性を脅かす攻撃である。

問 1-2　ア　　否認防止の特性に該当するもの　■ H28 春 -AP 問 39

JIS Q27000“情報技術－セキュリティ技術－情報セキュリティ－マネジメントシステム－用語”には，**否認防止（non-repudiation）**［⇒ P.10］について「主張された事象又は処置の発生，及びそれを引き起こしたエンティティを証明する能力」と定義されている。ある利用者がシステムを利用したという事実を証明可能にすることは，この否認防止に該当するので，（ア）が正解である。否認防止の実現手段としては，ディジタル署名が代表的である。システム利用時に当該利用者のディジタル署名を含む記録を残しておくことによって，システムを利用した事実を証明可能にすることができる。

解答群のその他の記述は，次の特性に該当する。

イ：**信頼性（reliability）**［⇒ P.10］

ウ：**可用性（availability）**［⇒ P.10］

エ：**機密性（confidentiality）**［⇒ P.10］