

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 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の対策セミナー向けのレジюмеをベースに制作しました。レジюме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。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。

◎第 2 版について

第 2 版は、第 1 版のマイナーチェンジ版で全体の構成は変わりません。変更点は次のとおりです。

- ・第 1 版へのご意見や技術の動向を考慮して、文章表現や説明内容を見直しました。
- ・第 1 版の出版後に情報処理安全確保支援士試験で出題された、DMARC や FIDO といった重要技術を追加しました。
- ・例題演習の問題を 3 割入れ替えました。

2020.3 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 “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 ー情報処理安全確保支援士試験とはー

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。

試験に関心をもたれた方、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。

<https://www.ipa.go.jp/siensi/index.html>



目次

これから“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	40
2.3.8 その他のプロトコル	43
2.3.9 例題演習	47
2.4 ネットワーク機器	50
2.4.1 ネットワーク接続機器	50
2.4.2 無線アクセスポイント	51
2.4.3 例題演習	52
2.5 データベース技術	53
2.5.1 SQL文	53
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	77
3.2.5	情報機器への攻撃	82
3.2.6	例題演習	83

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	97
4.1.3	共通鍵暗号方式と公開鍵暗号方式の比較	100
4.1.4	例題演習	101
4.2	ハッシュ関数とメッセージ認証	102
4.2.1	ハッシュ関数	102
4.2.2	メッセージ認証	104
4.2.3	例題演習	107
4.3	デジタル署名と PKI	109
4.3.1	デジタル署名	109
4.3.2	PKI	112
4.3.3	秘密鍵の保護	123
4.3.4	タイムスタンプと XML 署名	125
4.3.5	ブロックチェーン	129
4.3.6	例題演習	131
4.4	認証方式	135
4.4.1	利用者認証の方式	135
4.4.2	パスワード認証	135
4.4.3	共通鍵認証と公開鍵認証	139
4.4.4	その他の認証方式	142
4.4.5	例題演習	144

第5章 通信の制御とサイバー攻撃対策技術 145

5.1	ファイアウォール	146
5.1.1	ファイアウォールの目的	146
5.1.2	ファイアウォールの機能	146
5.1.3	例題演習	151
5.2	プロキシサーバ	153
5.2.1	プロキシサーバの種類	153
5.2.2	プロキシサーバの機能	155
5.2.3	例題演習	157
5.3	IDS・IPS	158
5.3.1	IDS・IPSの種類	158

5.3.2	IDS・IPSの検知方法と動作	160
5.3.3	例題演習	162
5.4	WAF	163
5.4.1	WAFの機能と運用	163
5.4.2	例題演習	166
5.5	サイバー攻撃対策技術	167
5.5.1	マルウェア対策技術	167
5.5.2	標的型攻撃に対する内部拡大・出口対策	170
5.5.3	例題演習	174

第6章 Webシステムのセキュリティ 177

6.1	HTTP	178
6.1.1	HTTPメッセージ	178
6.1.2	Cookie	184
6.1.3	HTTP認証	185
6.1.4	例題演習	188
6.2	Webアプリケーションへの攻撃と対策	189
6.2.1	セッションハイジャック	191
6.2.2	セッションフィクセーション	194
6.2.3	SQLインジェクション	195
6.2.4	クロスサイトスクリプティング (XSS)	197
6.2.5	クロスサイトリクエストフォージェリ (CSRF)	202
6.2.6	ディレクトリトラバーサル	205
6.2.7	OSコマンドインジェクション	206
6.2.8	バッファオーバーフロー (BOF)	207
6.2.9	クリックジャッキング	210
6.2.10	HTTPヘッダインジェクション	211
6.2.11	メールヘッダインジェクション	213
6.2.12	例題演習	215

第7章 メールシステムのセキュリティ 219

7.1	メールシステムにおける脅威	220
7.1.1	攻撃メール	220
7.1.2	踏み台攻撃	223
7.1.3	メールの盗聴・改ざん、誤送信	224
7.1.4	例題演習	225
7.2	メールシステムのセキュリティ機構	226
7.2.1	SMTP, POPのセキュリティ	226
7.2.2	S/MIME, PGP	228
7.2.3	送信ドメイン認証 (SPF, DKIM, DMARC)	231

7.2.4	メールのフィルタリング	241
7.2.5	OP25B	242
7.2.6	Web メール	243
7.2.7	例題演習	244

第8章 DNS システムのセキュリティ 247

8.1	DNS システムにおける脅威と対策	248
8.1.1	DNS キャッシュポイズニング	248
8.1.2	DDoS 攻撃	253
8.1.3	その他の DNS セキュリティ	255
8.1.4	例題演習	257

第9章 セキュアプロトコル 259

9.1	トランスポート層のセキュアプロトコル	260
9.1.1	TLS	260
9.1.2	SSH	274
9.1.3	例題演習	278
9.2	ネットワーク層のセキュアプロトコル	280
9.2.1	IPsec	280
9.2.2	例題演習	288
9.3	LAN のセキュリティ規格	289
9.3.1	IEEE802.1X	289
9.3.2	無線 LAN のセキュリティ規格	292
9.3.3	例題演習	295
9.4	認証・認可プロトコル	297
9.4.1	SAML	297
9.4.2	OAuth	299
9.4.3	FIDO	300
9.4.4	例題演習	303

第10章 システムセキュリティ 305

10.1	OS 関連のセキュリティ	306
10.1.1	アクセス管理	306
10.1.2	システムのセキュリティ管理	311
10.1.3	スマートフォンのセキュリティ	313
10.1.4	例題演習	314
10.2	データベースセキュリティ	315
10.2.1	データベースのセキュアな運用	315
10.2.2	例題演習	317
10.3	情報ハイディング技術	318

10.3.1	ステガノグラフィ, 電子透かし	318
10.3.2	例題演習	319
第 11 章 情報セキュリティマネジメント		321
11.1	ISMS の構築と運用	322
11.1.1	ISMS (情報セキュリティマネジメントシステム)	322
11.1.2	リスクマネジメント	323
11.1.3	セキュリティの検査・監視とシステム管理	324
11.1.4	脆弱性管理	326
11.1.5	インシデント対応	330
11.1.6	内部不正対策	333
11.1.7	情報セキュリティの点検	334
11.1.8	例題演習	336
11.2	情報セキュリティ関連規格, ガイドライン, 制度	341
11.2.1	CRYPTREC	341
11.2.2	ISO/IEC 27000 シリーズ	342
11.2.3	その他の関連規格・基準	343
11.2.4	情報セキュリティ関連ガイドライン	345
11.2.5	情報セキュリティ関連制度	346
11.2.6	例題演習	348
11.3	情報セキュリティ関連法規	350
11.3.1	サイバーセキュリティ基本法	350
11.3.2	刑法	350
11.3.3	不正アクセス禁止法	351
11.3.4	知的財産権関連法規	352
11.3.5	個人情報保護法	354
11.3.6	その他の情報セキュリティ関連法規	355
11.3.7	例題演習	358
第 12 章 例題演習の解答・解説		359
用語 INDEX		422
参考文献 / URL		429

商標表示

各社の登録商標及び商標、製品名に対しては、特に注記のない場合でも、これを十分に尊重いたします。

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、最近では、「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

▶情報セキュリティ：
information security

(1) 情報セキュリティの定義と特性

JIS Q27000:2019 “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図表 1-1 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、情報に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、ハッシュ値の比較やメッセージ認証、デ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があります。

〔セキュリティ対策〕…攻撃を遮断する侵入防止システム（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、攻撃者や攻撃者の制御する機器が、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動作することです。また、電子データに関しては、デジタル証明書（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、デジタル署名など様々な方法があります。電子データの真正性を確認する方法には、デジタル署名やメッセージ認証があります。

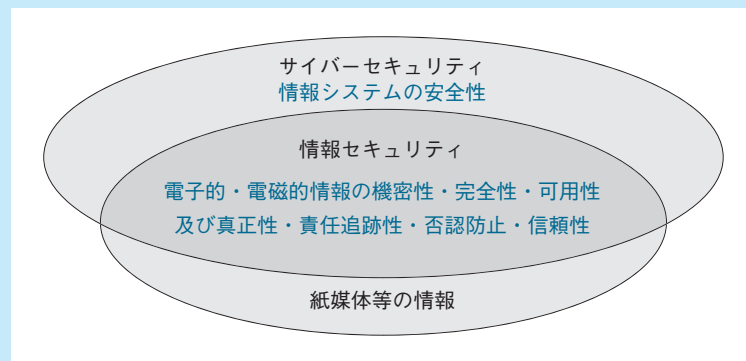
FAQ

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の関係

情報システムの企画・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。

問 1-3

■ H29 秋 -SG 問 9

情報セキュリティマネジメントにおける、脅威と脆弱性に関する記述のうち、最も適切なものはどれか。

- ア 管理策の欠如によって脅威が高まり、脆弱性の深刻度が低くなる。
- イ 脅威が存在しないと判断できる場合、脆弱性に対処する必要性は低い。
- ウ 脅威のうち、脆弱性によってリスクが顕在化するのは環境的脅威である。
- エ 脆弱性の有無に関わらず、事故の発生確率は脅威の大きさで決まる。

3.1 脅威と攻撃者

3.1.1 脅威の分類

脅威の分類の例を図表 3-1 に示します。大きくは、情報や情報システムに対する人間の直接的な操作に関する脅威と、情報システムを取り巻く自然災害などの環境的な要因に関する脅威に分かれています。さらに、人間に関する脅威を、悪意をもってセキュリティを侵害する意図的な脅威と、悪意はないものの過失や手落ちなどのヒューマンエラーに起因する偶発的な脅威に分類しています。最近見られる、アルバイトで知り得た秘密の情報を SNS 上で公開してしまうといった軽率な行動は、意図的と偶発的の中間的な脅威といえます。

第3章では、主に人間に関する意図的な脅威を説明します。以降の説明では、悪意のある人間のことを攻撃者といいます。

人間		環境
意図的	偶発的	
盗聴 情報の改ざん システムのハッキング 悪意のあるコード 盗難	誤り及び手ぬかり ファイルの削除 不正な経路 物理的事故	地震 台風 落雷 洪水 火災

第3章で説明する脅威

図表 3-1 脅威の分類の例

3.1.2 攻撃者の種類と動機

▶ スクリプトキディ：
script kiddie スクリプトは一定の手順、キディは子どもの意味

(1) スクリプトキディ

スクリプトキディは、自身で攻撃コードを作成するほどの高度な技術はもたず、インターネット上に公開されているツールや方法に従って不正アクセスやマルウェアを送りつける攻撃者です。スクリプトキディの攻撃の動機としては、主に興味本位や愉快犯、自己顕示などが考えられます。

(2) 内部関係者

内部関係者としては、組織に所属する社員やアルバイトなどの従業者、情報

3.2 様々な脅威

3.2.1 マルウェア

▶ マルウェア：malware

(1) マルウェア

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。

▶ コンピュータウイルス：
computer virus

(2) ウイルス (コンピュータウイルス)

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、次の機能の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

もあります。

(3) ファイル感染型ウイルス、マクロ感染型ウイルス、システム感染型ウイルス

ウイルスを感染形態に着目して分類したものです。

- ・ファイル感染型…exe, com, sysなどの拡張子をもつ実行型のファイルに感染する。
- ・マクロ感染型…OAソフトウェアで使用するマクロに感染する。実行ファイルではなく、データファイルに感染する点の特徴である。単に**マクロウイルス**ともいう。古くから観測されているが、最近でも猛威をふるっている。
- ・システム感染型…ハードディスクのブートセクタなどのシステム領域に感染する。ブートセクタのコードは、コンピュータの起動時（ブート時）に実行されるので、コンピュータ全体の制御に影響が及ぶという特徴がある。

(4) ステルス技術をもつウイルス

ステルス技術は、ウイルスの存在を検知されにくくする機能で、ポリモーフィック型ウイルスとメタモーフィック型ウイルスに分類されます。

ポリモーフィック型ウイルスは、異なる暗号鍵を用いて自身を暗号化することによって、自身のコードを多様化させます。

メタモーフィック型ウイルスは、コードの順序や命令を変更して自身のコードを変化させます。

(5) ワーム

ワームは、ウイルスのように他のプログラムに寄生せずに自立して存在し、ネットワークを経由して自身を複製しながら自己拡散するマルウェアです。増殖して感染を拡げる点は、ウイルスと共通する特徴です。

(6) トロイの木馬

トロイの木馬は、独立した不正なプログラムで、増殖をしないマルウェアです。利用者からは、ゲームソフトや便利なツールソフトのように見え、実際に正しい機能を提供しながら攻撃活動を行うものがあり、感染に気付かずに長く使い続けてしまうことがあります。

(7) バックドア, RAT, ボット

バックドアは、侵入したシステム内のコンピュータと攻撃者が通信を行うためのマルウェアです。トロイの木馬の一種で独立したプログラムとして存在します。以前は、外部からの接続を待ち受ける機能が特徴でした。最近では、外部から内部ネットワークへの接続がファイアウォールで禁止されていることから、感染した内部のコンピュータから、攻撃者の制御する外部のコンピュータ

▶ポリモーフィック型ウイルス: polymorphic virus (多様型のウイルス)

▶メタモーフィック型ウイルス: metamorphic virus (変異型のウイルス)

▶ワーム: worm (虫)

▶トロイの木馬: Trojan horse (ギリシャ神話のトロイの木馬に由来)

▶バックドア: back door (裏口)

▶ ^{ラット}RAT :
Remote Administration
Tool (遠隔操作ツール)

▶ ボット : bot

▶ クローラ : crawler (イ
ンターネットを検索し
て、検索データベー
スを自動的に作成す
るプログラム)

▶ スパイウェア :
spyware

▶ キーロガー :
key logger

▶ スクリーンロガー :
screen logger

▶ ルートキット : rootkit

へ接続して、指令を受ける機能をもつことが特徴です。

RAT は、バックドアと同様のマルウェアで、攻撃者が標的のコンピュータを遠隔操作する機能に着目した命名です。

ボット は、攻撃者からの指令を受けて、さらに他のコンピュータやネットワークに対して攻撃をすることが特徴のマルウェアです。ボットに感染したPCはボットPCと呼ばれます。ボットPCの集合体をボットネットワークといい、数万台以上のボットネットワークから、一斉に攻撃を仕掛けるDDoS攻撃が発生しています。ボットという名称はロボット (robot) に由来します。

なお、ボットには、マルウェアに分類されるものの他に、検索エンジンのクローラや、企業のWebサイト上で顧客の質問に自動で応答するチャットボットのように、正しい機能を提供するソフトウェアもあります。

(8) ダウンローダ

ダウンローダ は、感染したPCに、さらに他のマルウェアをダウンロードする機能をもつマルウェアです。ダウンローダは、組織内から、攻撃者が制御するインターネット上のコンピュータへアクセスします。

(9) スパイウェア

スパイウェア は、感染したコンピュータを含む情報システムの情報を窃取することを目的としたマルウェアです。コンピュータやネットワークの構成情報や設定情報、保存されたデータファイル、ネットワークを流れる通信の情報など、様々な情報を攻撃者の制御するコンピュータへ送信します。

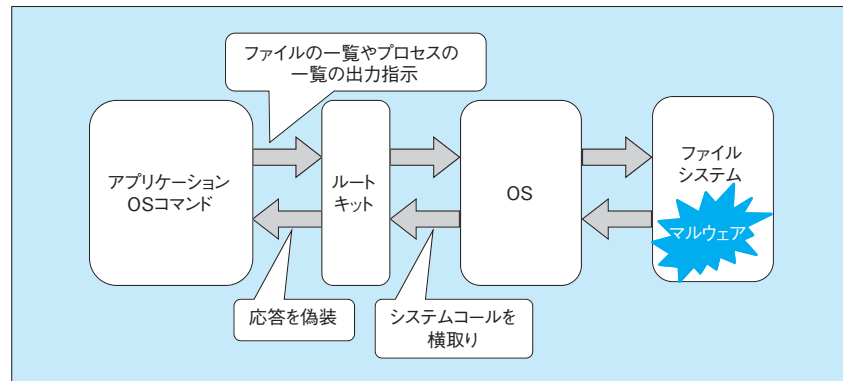
(10) キーロガー、スクリーンロガー

キーロガー は、キーボードの操作履歴を記録して、利用者IDとパスワードなどを窃取するマルウェアです。**スクリーンロガー** は、ディスプレイに表示された情報をまるごとスクリーンショットによって窃取するマルウェアです。キーロガーとスクリーンロガーは、スパイウェアの一種といえます。

(11) ルートキット

ルートキット (rootkit) は、侵入したコンピュータ上において、攻撃活動を行うための不正なプログラムやツールをパッケージ化したものです。そして、それらの不正なプログラムを検知されにくくするために、ファイルやプロセス、ディレクトリ、その他のシステムオブジェクトを隠ぺいする機能をもっていることがルートキットの特徴です。

ルートキットの例を図表3-2に示します。利用者がファイル管理ソフトやOSコマンドを使って、ファイルの一覧やプロセスの一覧を出力させようとした際に、ルートキットがシステムコールを横取りして応答を偽装します。そのため、マルウェアのファイルや、マルウェアが動作している不正なプロセスが隠ぺいされます。



図表 3-2 ルートキットの例

- ▶ ランサムウェア：
ransom were ランサムは身代金の意味
- ▶ TOR：The Onion Router

(12) ランサムウェア

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（暗号資産）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。

- ▶ マイニングマルウェア：
mining malware
マイニングは採掘の意味で、ブロックチェーンの取引台帳への追記作業を行う。

(13) マイニングマルウェア

マイニングマルウェアは、感染した機器のCPUなどのリソースを使用して仮想通貨（暗号資産）のマイニングを行うマルウェアです。マイニングマルウェアを用いて報酬として仮想通貨（暗号資産）を得る攻撃を**クリプトジャッキング**と呼びます。

- ▶ ファイルレスマルウェア：
fileless malware

(14) ファイルレスマルウェア

ファイルレスマルウェアは、メモリ上で動作し、ファイルとして保存されないマルウェアです。そのため、ファイルを対象とするマルウェアスキャンでは検出できません。WindowsのPowerShellのスクリプトを改ざんし、攻撃コードをメモリにダウンロードしながら活動するマルウェアなどが報告されています。

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
	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
	バッファオーバーフロー	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
	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。

7.1 ■ メールシステムにおける脅威

メールシステムのセキュリティに関しては、2.3.6節「メールサービスとSMTP、POP3、IMAP4」において、メールサービスの概要、SMTPと電子メールの転送、メールアドレスの構造を説明しています。本章の説明は、2.3.6節の続きの内容になります。

7.1.1 攻撃メール

(1) 様々な攻撃メール

攻撃メールの目的は、標的の端末をマルウェアに感染させることや、罠サイトへ誘導して秘密情報を窃取することなどです。攻撃メールの例を図表7-1に示します。標的型攻撃メールからやり取り型メールの四つは、3.2.2節のサイバー攻撃でも説明しています。

図表 7-1 攻撃メールの例

メソッド	説明
標的型攻撃メール	特定の組織のメンバや個人に対して、関係者を装った内容のメールを送信する。添付ファイルや本文中のURLをクリックさせて、マルウェアに感染させる。
フィッシングメール	メールに記載したURLをクリックさせて、偽りサイトへ誘導する。金融機関や関係企業になりすます手口も見られる。
ばらまき型メール	不特定多数の受信者に対して、マルウェアを添付した、あるいは罠サイトへ誘導させるメールを送信する。
やり取り型メール	顧客対応窓口などを標的として、何回かのメールのやり取りを経て、最終的に添付ファイルをクリックさせる。
スパムメール	迷惑メールの意味で、受信者の許可を得ずに一方的に宣伝メールなどを送りつける。広義では、マルウェア感染を目的とした攻撃メールを含めて、スパムメールという。

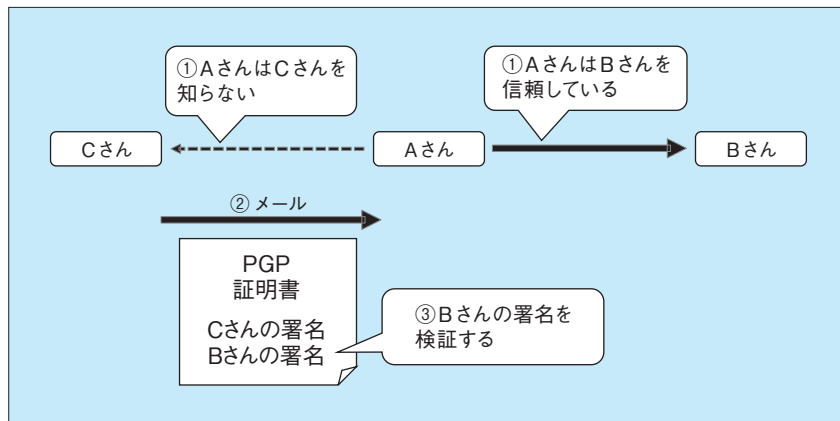
▶ スпамメール：
spam mail

(2) メールヘッダと送信元情報の詐称

メールヘッダには、送信者や転送経路の情報が格納されます。メールヘッダの一部を図表7-2に示します。

って、信頼の範囲を広げていきます。この考え方を、**信頼の輪 (web of trust)** といいます。信頼の輪の考え方を図表 7-13 に示します。

- ① Aさんは、信頼しているBさんの公開鍵を所有している。
- ② Aさんが知らないCさんからPGPメールを受信する。
- ③ CさんのPGP証明書には、Bさんが署名を付与しているので、Bさんの公開鍵でBさんの署名を検証する。検証に成功した場合、Aさんは、自分が信頼するBさんが信頼するCさんを信頼できると判断する。



図表 7-13 信頼の輪の考え方

7.2.3 送信ドメイン認証 (SPF, DKIM, DMARC)

送信ドメイン認証は、攻撃メールやスパムメール対策のために、送信側のドメインに基づいて、メールを受信したメールサーバが送信側のメールサーバの正当性を検証する仕組みです。本節では、送信ドメイン認証の実装技術のうち、SPFとDKIM、及びこれらを補完・強化するDMARCを説明します。

(1) SPF

▶ SPF : Sender Policy Framework

SPFは、ドメイン情報と送信元のIPアドレスの組合せの妥当性を検証する、送信ドメイン認証メカニズムです。

SPF検証を行うためには、事前に送信側ドメインの権威DNSサーバにSPFレコードを登録します。SPFレコードには、ドメイン名、認証する送信元のIPアドレス、認証しない送信元のIPアドレスなどを設定します。次にSPFレコードの例を示します。

・ SPFレコードの例
example.co.jp. IN TXT "v=spf1 +ip4:x.y.z.10 +ip4:x.y.z.20 -all"

9.4 ■ 認証・認可プロトコル

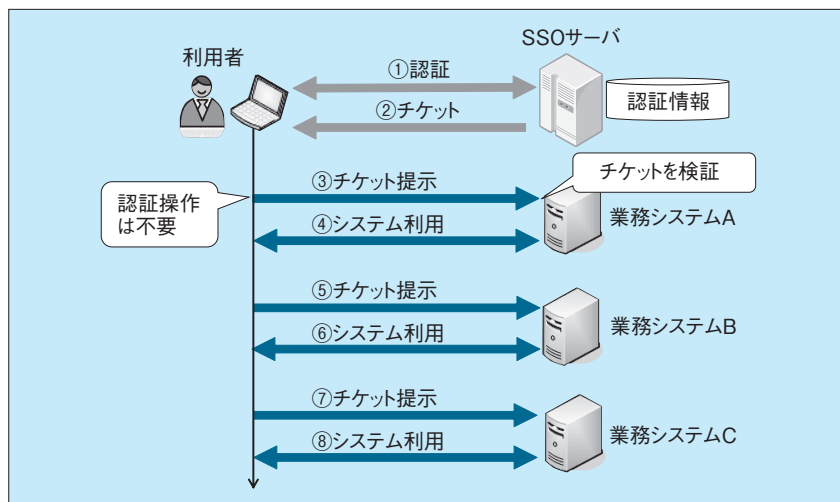
9.4.1 SAML

▶ シングルサインオン： SSO (Single Sign On)

(1) シングルサインオン (SSO)

シングルサインオンは、利用者が1回の認証操作に成功すると、設定された時間内は、アクセス権限のある複数のシステムを認証動作なしに利用できるような認証の仕組みです。シングルサインオンの概念を図表 9-38 に示します。社内の複数システムに対するシングルサインオンの例です。SSO サーバと各業務システムのサーバには、事前共有鍵を設定するなどして、あらかじめ信頼関係を構築しておきます。

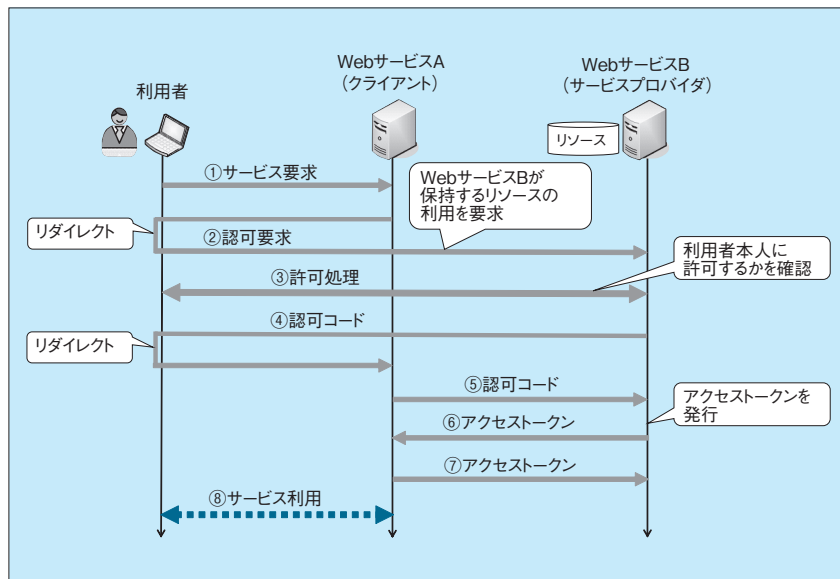
- ①②利用者は、SSO サーバに接続して認証操作を行い、認証に成功すると業務システムにアクセスするための認証チケットを受け取る。
- ③④業務システムへのアクセス時にチケットが提示され、業務システム A がチケットを検証する。業務システム A が信頼する SSO サーバが発行したチケットであることを確認すると、業務システム A は利用者のアクセスを許可する。このとき、利用者は認証操作を行う必要がなく、シングルサインオンが実現される。
- ⑤⑥⑦⑧他の業務システムについても同様に、チケットの提示でアクセスできる。



図表 9-38 シングルサインオンの概念

せる。

- ⑤ Web サービス A は、Web サービス B へ認可コードを送信して、アクセストークンを要求する。
- ⑥ Web サービス B は、リソースへの限定的なアクセスを認可するアクセストークンを発行して、Web サービス A へ応答する。
- ⑦ Web サービス A は、アクセストークンを Web サービス B に送信して、リソースへの限定的なアクセスを要求する。
- ⑧ 利用者は、リソースを利用した Web サービス A のサービスを利用開始できる。



図表 9-40 OAuth のメッセージングの例 (OAuth2.0)

9.4.3 FIDO

- ▶ ファイド FIDO : Fast Identity Online
- ▶ UAF : Universal Authentication Framework
- ▶ U2F : Universal Second Factor

(1) FIDO の機能とメッセージング

FIDO は、パスワードに依存しない、あるいはパスワードへの依存を少なくすることを目的とする認証方式の規格です。現在、FIDO には FIDO UAF, FIDO U2F, FIDO2 の三つの規格があります。三つの規格を図表 9-41 に示します。

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** [⇒P.65]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]

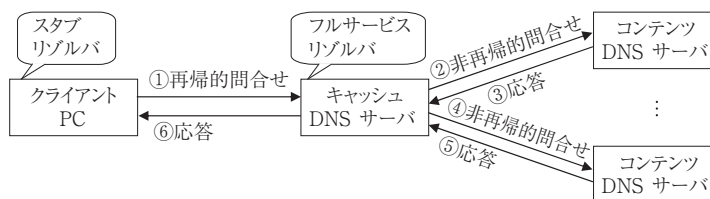
エ：**機密性 (confidentiality)** [⇒P.10]

問 2-6 ア

DNS に関する記述 ■ H28 秋 -SC 午前 II 問 18

DNS (Domain Name System) は、インターネット上でドメイン名と IP アドレスの対応付けなどを管理する分散型のデータベースシステムである。この DNS は、クライアントサーバ型で動作し、クライアントはリゾルバ (resolver)、サーバはネームサーバ (DNS サーバ) と呼ばれる。このため、DNS サーバに対して、IP アドレスに対応するドメイン名、又はドメイン名に対応する IP アドレスを問い合わせるクライアントソフトウェアがリゾルバとなる。したがって、(ア) が正しい。

なお、リゾルバと DNS サーバの関係を補足すると、次のようになる。例えば、クライアント PC がキャッシュ DNS サーバを利用する場合には、次の図に示すように、①で DNS 再帰的問合せ (DNS クエリ) を送信する。



その際、キャッシュ DNS サーバが、問合せのあった名前情報をキャッシュしていない場合には、②から権威 DNS サーバ (コンテンツ DNS サーバ) に対して順次、非再帰的問合せを繰り返していくので、キャッシュ DNS サーバもリゾルバとして動作することになる。そこで、PC のように、キャッシュ DNS サーバに対して再帰的問合せによって名前解決を依頼するリゾルバをスタブリゾルバ、キャッシュ DNS サーバのように、スタブリゾルバから要求された目的の資源レコードが得られるまで、問合せを繰り返すリゾルバをフルサービスリゾルバという。

その他の記述には、次のような誤りがある。

- イ：問合せを受けた DNS サーバが要求されたデータをもっていない場合に、他の DNS サーバを参照先として回答することを、委任 (referral) という。ゾーン転送は、セカンダリ DNS サーバが、プライマリ DNS サーバと同期をとるために、プライマリからセカンダリにゾーン情報を転送することである。
- ウ：ドメイン名に対応する IP アドレスを求めることは、正引きという。逆引きは、IP アドレスに対応するドメイン名を求めることである。
- エ：ドメイン名を管理する DNS サーバを指定する資源レコードは、NS (Name Server) レコード [⇒P.42] である。CNAME (Canonical NAME) レコード [⇒P.42] は、ホスト名に対する別名を定義するための資源レコードである。

問 2-7 ウ

DNS の資源レコード ■ H27 秋 -NW 午前 II 問 1

DNS サーバに登録する資源レコードには、A レコード、CNAME レコード、MX レコード、NS レコード、PTR レコード [⇒P.42] など、幾つかの種類がある。これらのうち、そのゾーン自身や下位ドメインに関する DNS サーバのホスト名を指定するためには、NS (Name Server) レコードが使用される。したがって、(ウ) が正しい。

その他の記述には、次のような誤りがある。

- ア：他の DNS サーバのキャッシュ領域に情報を残す許可時間や、ゾーン情報の更新をチェックする間隔

レンジレスポンス方式を利用するかなど)を折衝して決めるようにしている。

その他の記述が示すものは、次のとおりである。

ア：OP25B (Outbound Port 25 Blocking) [⇒ P.242] の説明である。

イ：SPF (Sender Policy Framework) [⇒ P.231] や DKIM (DomainKeys Identified Mail) [⇒ P.234] などによる送信ドメイン認証の説明である。

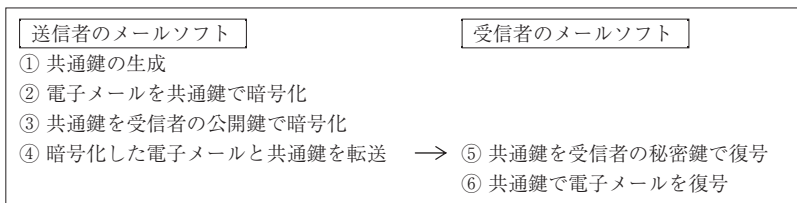
エ：送信元の認証を POP (Post Office Protocol) の認証機能を用いて行う、POP before SMTP [⇒ P.226] の説明である。

問 7-4 ア

電子メール暗号化プロトコルの組合せ ■ H28 春-SC 午前Ⅱ問 17

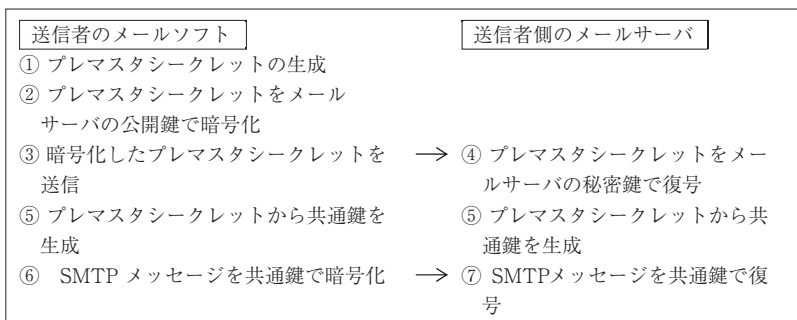
PGP (Pretty Good Privacy) [⇒ P.230], S/MIME (Secure / Multipurpose Internet Mail Extensions) [⇒ P.228], SMTP over TLS [⇒ P.228] とも、電子メールの暗号化に共通鍵(セッション鍵)を用いるが、その共通鍵を受信者あるいはメールサーバと共有するために、通信相手の公開鍵ペアを使用する。

まず、PGP と S/MIME における暗号化の処理は、次の図のように行われる。ただし、送信者の認証と電子メールの改ざんを検出するためのデジタル署名の処理は除いている。



このため、PGP と S/MIME で電子メールを暗号化するには、受信者側のメールソフトが直接対応するので、メールアドレスごとに公開鍵ペアを用意する必要がある。

次に、SMTP over TLS における暗号化の処理は、次の図のように行われる。ここでは、送信者から送信者側にあるメールサーバにメールを送信する場合を例として、暗号化に関する処理だけを示す。



このため、SMTP over TLS では、いったんメールサーバがメールを受け取るので、メールサーバ単位で公開鍵ペアを用意する必要がある。また、送信者側メールサーバから受信者側メールサーバへの通信も同様で、メールサーバ単位で公開鍵ペアを用意する必要がある。

以上のことから、(ア)が正しい。

解答

用語 INDEX

<番号>

3 ウェイハンドシェイク …… 29

<欧字>

< A >

AAAA レコード …… 42

AAA フレームワーク …… 292

Administrator 権限 …… 310

AES …… 91

AH …… 286

APOP …… 228

APT …… 63

ARP …… 31

ARP キャッシュ …… 33

ARP スプーフィング攻撃 …… 79

ARP テーブル …… 33

A レコード …… 42

< B >

BEC …… 71

< C >

CA …… 113

Cache-Control ヘッダ …… 183

Camellia …… 91

CAPTCHA …… 308

CBC モード …… 93

CC …… 343

CCE …… 328

CCM …… 95

CCMP …… 294

C & C サーバ …… 63

CHILD_SA …… 284

CMAC …… 104

CNAME レコード …… 42

CONNECT メソッド …… 178

Cookie …… 184

Cookie ヘッダ …… 180

CPE …… 328

CRL …… 121

CRL 配布ポイント …… 122

CRYPTREC …… 341

CRYPTREC 暗号リスト …… 341

CSIRT …… 330

CSMS 適合性評価制度 …… 347

CSR …… 119

CSRF …… 202

CTR モード …… 94

CVE …… 327

CVSS …… 328

CWE …… 329

< D >

DAC …… 309

DDoS 攻撃 …… 65

DHCP …… 43

DH アルゴリズム …… 98

DIAMETER …… 292

DKIM …… 234

DLP …… 170

DMARC …… 237

DNSBL …… 241

DNSSEC …… 251

DNS アンプ攻撃 …… 253

DNS キャッシュポイズニング

…… 248

DNS 水責め攻撃 …… 254

DNS リフレクション攻撃 …… 253

DOM …… 200

Domain 属性 …… 185

DOM ベース XSS …… 200

DoS 攻撃 …… 65

< E >

EAP …… 290

EAP-MD5 …… 290

EAP-TLS …… 290

EAP-TTLS …… 291

ECB モード …… 93

ECDHE アルゴリズム …… 264

EDoS 攻撃 …… 68

EDSA 認証 …… 347

EHLO コマンド …… 38

ESP …… 286

EV 証明書 …… 120

Expires 属性 …… 184

Exploit コード …… 70

< F >

FIDO …… 300

FIPS PUB 140-2 …… 344

FQDN …… 36

FTP …… 36, 45

< G >

GCM …… 95

GDPR …… 345

GET メソッド …… 178

< H >

Heartbleed 脆弱性 …… 328

HELO コマンド …… 38

hidden フィールド …… 193

HMAC …… 105

hosts ファイル …… 255

Host ヘッダ …… 180

HSTS プリロード …… 183

HSTS ヘッダ …… 183

HTML …… 34

- root 権限 310
 RSA 暗号 98
 RST パケット 158
- < S >
- SA 282
 Same Origin Policy 211
 SAML 298
 SCAP 327
 Secure 属性 185
 SEO ポイズニング 71
 Set-Cookie ヘッダ 182
 SHA-2 102
 SIEM 171
 SMTP 37
 SMTP-AUTH 227
 SMTPS 228
 Smurf 攻撃 66
 SOA レコード 42
 SOC 325
 SPF 231
 SQL 53
 SQL インジェクション 195
 SSH 274
 SSH ポートフォワーディング
 277
 SSID 51
 SSL 260
 SSL / TLS バージョンロール
 バック攻撃 71
 SSL サーバ証明書 119
 STARTTLS 228
 SURBL 241
 SYN Flood 攻撃 65
 syslog 312
- < T >
- TCP 28
 TCP SYN スキャン 69
 TCP コネクション 29
- TELNET 46
 TKIP 294
 TLS 36, 260
 TLS サーバ証明書 119
 TPM 124
 TSA 126
 TXT レコード 42
- < U >
- UDP 29
 UDP Flood 攻撃 66
 UDP スキャン 69
 URL 35
 URL フィルタリング 155, 169
 URL リライティング 178
 User-Agent ヘッダ 180
 UTM 168
- < V >
- VLAN 169, 172
 VPN 139
- < W >
- WAF 163
 web of trust 231
 Web フィルタリング 169
 Web メール 243
 WEP 293
 WHOIS データベース 68
 WPA 293
 WPA2 293
 WPA2-エンタープライズ 294
 WPA2-パーソナル 294
 WPA3 293
 WPA3-エンタープライズ 294
 WPA3-パーソナル 294
- < X >
- X.509 113
 XCCDF 328
- X-Forwarded-For ヘッダ 180
 X-Frame-Options ヘッダ 182
 XML 署名 127
 XOR 92
 XSS 197
 XSS フィルタ 201
- < かな >
- < あ >
- アーカイブタイムスタンプ 127
 アイデンティティ 298
 アイデンティティ連携 298
 アカウントロック 72, 312
 アグレッシブモード 282
 アドレス解決 31
 アノマリ検知 160
 アプリケーションゲートウェイ
 方式 150
 アプリケーション制御 149
 暗号化 90
 暗号モジュール試験及び認証制度
 346
 暗号利用モード 93
 安全性 14
- < い >
- 意匠法 352
 一方向性 103
 一般ユーザ権限 311
 インテグリティ 11
 インライン型 158
- < う >
- ウイルス 58
 ウイルス作成罪 351
- < え >
- 営業秘密 353
 エクスプロイトコード 70
 エスケープ 201