平成30年度「専修学校による地域産業中核的人材養成事業」

システムセキュリティ構築

Society5.0に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

平成 30 年度「専修学校による地域産業中核的人材養成事業」

システムセキュリティ構築

Society5.0 に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

■目次

1　目次 3

第 1 章．現在・近未来 9

1　SOCIETY5.0 とは？ 10
2　情報セキュリティの必要性 12
3　セキュリティの三要素：ＣＩＡ 14
4　近未来を支える技術 16
5　演習問題 18

第 2 章．暗号化・認証 19

1　通信文の傍受・改ざん対策が必要 20
2　傍受を防ぐには暗号化が必要 21
3　暗号通信には鍵とアルゴリズムが必要 22
4　共通鍵方式と公開鍵方式 23
5　共通鍵方式は鍵の管理が煩雑 24
6　公開鍵方式では鍵を公開できる 25
7　公開鍵方式は鍵の管理が簡単 26
8　公開鍵と共通鍵を適材適所で併用する 27
9　DIFFI-HELLMAN 鍵交換方式 28
10　認証とは？ 29
11　主体認証とメッセージ認証 30
12　二者間認証と三者間認証 31
13　主体認証の実現方法 32
14　ハッシュ関数の性質 33
15　ハッシュ関数の応用 34
16　パスワード認証の脆弱性(1) 35
17　パスワード認証の脆弱性(2) 36
18　ワンタイムパスワード認証 37
19　チャレンジ・レスポンス方式 38
20　時間同期方式 39
21　メッセージ認証＝完全性検証と否認防止 40
22　暗号化だけでは改ざんは防げない 41
23　完全性検証コードを付加して改ざん防止 42
24　デジタル署名により否認防止 43
25　共通鍵・公開鍵・ハッシュを併用する 44
26　公開鍵の真正性をどう担保する？ 45

27　第三者認証により公開鍵の認証を得る 46
28　第三者認証：サーバー証明書の記載事項 47
29　TLS 通信開始時の検証ポイント 48
30　第三者認証：公開鍵基盤 49
31　第三者認証：プライベート CA 50
32　IC カードによる認証 51
33　内部認証の手順 53
34　外部認証の手順 54
35　耐タンパ性 55
36　識別・認証・認可・アカウンティング 58
37　認証のための資格情報は集中管理したい 60
38　認証手順の多様性にどう対応する？ 62
39　認証用データのカプセル化 63
40　CHAP 64
41　EAP パケット・フォーマット 65
42　EAP パケットのカプセル化 66
43　IEEE802.1X の役割 67
44　TLS 接続手順と EAP-TLS 接続手順の比較 68
45　802.1X 関連プロトコルの連携 72
46　RADIUS：認証/認可/アカウンティング 73
47　RADIUS パケット・フォーマット 74
48　演習問題 75

第 3 章．セキュリティプロトコル 77

1　2 点間暗号化通信の技術概要 78
2　カプセル化とは 79
3　通信におけるカプセル化 80
4　暗号化・メッセージ認証とカプセル化 81
5　セキュリティ・アソシエーション 82
6　暗号化区間のパターン 83
7　LAN 間接続とトンネリング 84
8　トンネリングの実装イメージ 86
9　暗号化通信プロトコルと TCP/IP スタック 87
10　IPSEC の 2 つのモード 88
11　トランスポート・モードの動作イメージ 89
12　トンネル・モードの動作イメージ 90
13　GRE/IPSEC の動作イメージ 91
14　セキュリティ・アソシエーションの生成 92
15　IKE フェーズ 1 93

16 SA の生成と破棄 94
17 メッセージ認証・暗号化・リプレイ拒否 95
18 AH および ESP のフォーマット 96
19 SSL/TLS とは 97
20 TLS を利用する上位層 98
21 提供されるセキュリティ・サービス 99
22 TLS 通信の安全性の限界 100
23 TLS 通信が規定する 4 種のプロトコル 101
24 TLS 通信パラメータの相関図 102
25 TLS 通信開始のハンドシェイク手順 104
26 演習問題 106

第 4 章. 不正アタック対策 107

1 情報セキュリティ対策の基本 108
2 ソフトウェアの更新（脆弱性対策） 110
3 パスワードの適切な管理・認証強化 111
4 設定の見直し 112
5 脅威・手口を知ることが重要 113
6 トラフィック制御メカニズム概要 114
7 ステートフルインスペクション 117
8 アプリケーションレベルゲートウェイ 118
9 プロキシサーバの動作イメージ 119
10 TLS 通信のトンネル処理 123
11 侵入検知・防御システム 124
12 シグネチャ型とアノマリ型 126
13 ウイルス対策 128
14 メールのスキャン 129
15 WEB コンテンツフィルタリング 130
16 演習問題 131

第 5 章. 可用性、物理的セキュリティ 133

1 可用性管理対象と脅威の概要 134
2 データの可用性とシステムの可用性 136
3 データの可用性 137
4 システムの可用性 139
5 冗長構成 140
6 DOS 攻撃 142
7 SYN フラッド 143
8 UDP フラッド 144

9　分散型 DoS 攻撃 145
10　物理的セキュリティで考慮すべき項目 147
11　演習問題 149

第 6 章. 情報セキュリティマネジメント 151

1　ISMS:セキュリティマネジメント 152
2　PDCA サイクル 154
3　ハザード、リスク、リスク評価 155
4　回避・低減・移転・保有（1） 157
5　回避・低減・移転・保有（2） 159
6　ISMS 構築手順 160
7　インシデント・レスポンスと CSIRT 165
8　システム監査の必要性 171
9　システム監査基準とシステム管理基準 173
10　セキュリティ監査、プライバシーマーク 174
11　演習問題 176

第 7 章. サーバーとシステム基盤 177

1　サーバー要塞化の基本 178
2　DNS の仕組み 180
3　送信元偽装に弱い UDP 182
4　DNS リフレクタ 183
5　DNS キャッシュの仕組み 184
6　DNS キャッシュポイズニングの仕組み 185
7　迷惑メール対策 187
8　演習問題 189

第 8 章. WEB システム 191

1　セキュアな情報システム構築マネジメント 192

第 9 章. VPN 197

1　VPN は仮想的な専用線 198
2　IPsec：LAN 間接続形態 200
3　IPsec：リモートアクセス形態 201
4　SSL-VPN の動作方式 202
5　リバースプロキシ方式 203
6　ポートフォワーディング 205
7　ポートフォワーディング（詳細） 206
8　L2 フォワーディング 208
9　L2 フォワーディング（詳細） 209

10　演習問題 210

第 10 章.　無線 LAN 213

1　無線 LAN の規格 214
2　無線 LAN の構成イメージ 215
3　無線 LAN 認証・暗号化技術の構成要素 217
4　無線 LAN 認証・暗号化技術の構成要素 219
5　パケット鍵の生成過程 220
6　WEP,WPA, WPA2 の比較 222
7　無線 LAN のセキュリティ対策 225
8　演習問題 227

第 11 章.　セキュアプログラミング 229

1　DB サーバーのセキュリティ 230
2　SQL インジェクションの原理 232
3　SQL 文が実行されるまでの手順 233
4　特殊文字の置換による無害化（サニタイジング） 235
5　セッション ID による利用者識別の弱点 236
6　クロスサイトスクリプティング 238
7　XSS 脆弱性（入力無害化不全） 240
8　セッション管理の脆弱性を狙う攻撃 241
9　クロスサイトリクエストフォージェリ 242
10　その他の攻撃 243
11　演習問題 244

第 12 章. 個人を対象とする攻撃 247

1　考慮すべきセグメントと脅威の種類 248
2　インターネットバンキングやクレジットカード情報等の不正利用 251
3　ランサムウェアによる被害 253
4　ネット上の誹謗・中傷 254
5　スマートフォンやスマートフォンアプリを狙った攻撃 255
6　ウェブサービスへの不正ログイン 256
7　ウェブサービスからの個人情報の窃取 257
8　偽警告によるインターネット詐欺 258
9　演習問題 259

第 13 章. 組織や不特定多数を対象とする攻撃 261

1　組織に対する攻撃 262
2　標的型攻撃 264
3　攻撃のビジネス化 265

4 IoT 機器の不適切な管理 266
5 制御システムへの攻撃 268
6 Web サイトの乗っ取りと改ざん 270
7 仮想通貨問題：法定通貨の基本 271
8 仮想通貨のセキュリティ 273
9 演習問題 277

第 14 章. セキュリティ・インシデントへの対応 279

1 社会的な取り組みで求められる観点 280
2 セキュリティ関連法案 283
3 演習問題 285

第 15 章. SOCIETY5.0 の担い手として 287

1 総まとめ 288
2 セキュリティに強い技術者を目指そう 290
3 これからのロードマップ 291
4 演習問題 293

演習問題回答 295

1 演習問題回答 296

第1章.

現在・近未来

1 Society5.0 とは？

今、社会は生活のすみずみまで IT が深く融合したものへと変わりつつあります。そのような新しい社会のあり方を、内閣府では「Society5.0」と呼んで次のように定義しています。

> **【Society5.0】**
> **サイバー空間（仮想、浄法空間）とフィジカル空間（現実空間）を**
> **高度に融合させたシステムにより**
> **経済発展と社会的課題の解決を両立する**
> **人間中心の社会（Society）**

5.0 という数字の背景には人類の進化発展を 5 段階のエポックメイキングな「変化」でとらえる視点があります。

Society1.0 はおおむね数十万年前、現生人類が地球上に誕生して、狩猟・採集により生活していた時代を指します。

約 1～2 万年前に農耕が始まって生まれたのが Society2.0 です。農耕によって人類はより安定的に食料を得る手段を獲得しました。

その後約 200 年前から産業革命により始まる「工業」の時代が Society3.0 です。石炭や石油のエネルギーを「動力」に変えて使えるようになり、大量生産・大量広域輸送が可能になったのがこの時代の特徴です。

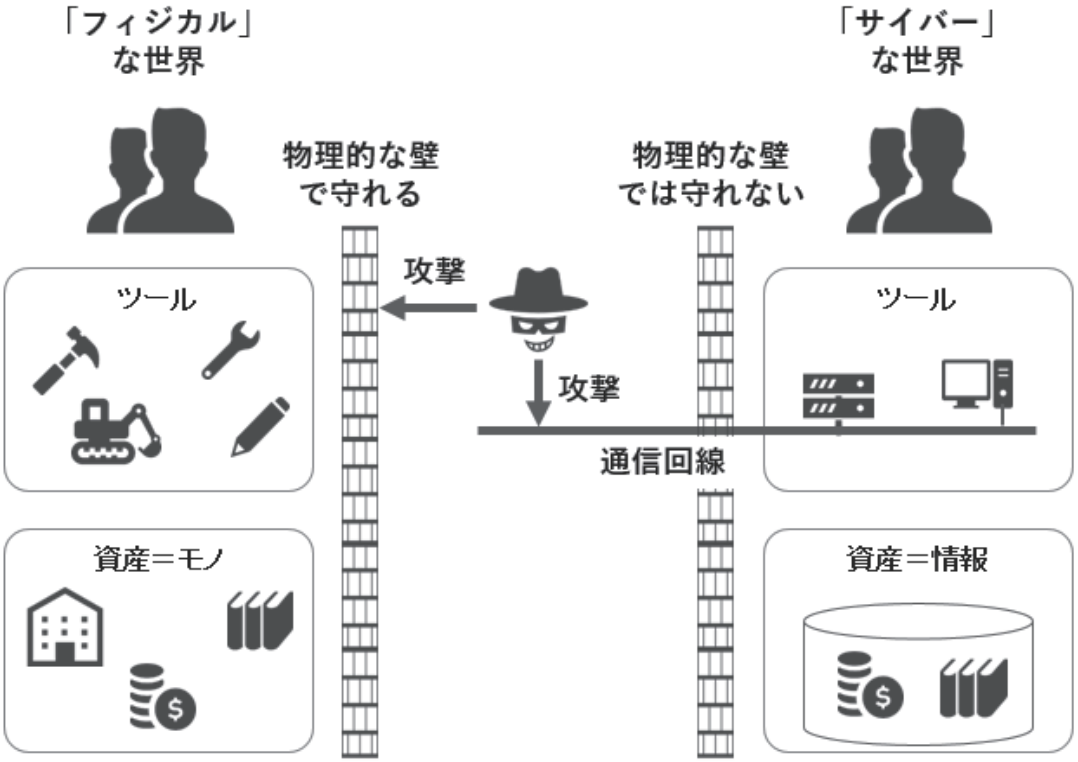
さらに約 60〜70 年前から Society4.0、「情報」の時代が始まります。その頃実用化されたコンピュータと情報通信の技術は、大量の情報処理（情報保存・伝達・計算・検索）に革命をもたらしました。

しかし、「情報」の時代にはまだサイバーとフィジカルは融合していませんでした。たとえば現代の工業技術の塊とも言える自動車の運転は今でも人間が筋肉を使って行わなければなりません。Society4.0 ではまだ、カーナビという「サイバー（情報）」の世界と、運転という「フィジカル」の世界を人間の運転手が仲立ちしています。

その融合が始まりつつあるのが現代、Society5.0 への移行期です。自動運転車の開発はそのひとつの象徴と言えます。Society5.0 の時代にはあらゆる領域でフィジカルな世界とサイバーな世界が融合し、これまでとは次元の違う形でさまざまな社会的課題の解決と経済発展が可能になると予想されています。

一方で、その時代に極めて重要性を増してくるのがセキュリティです。

2 情報セキュリティの必要性



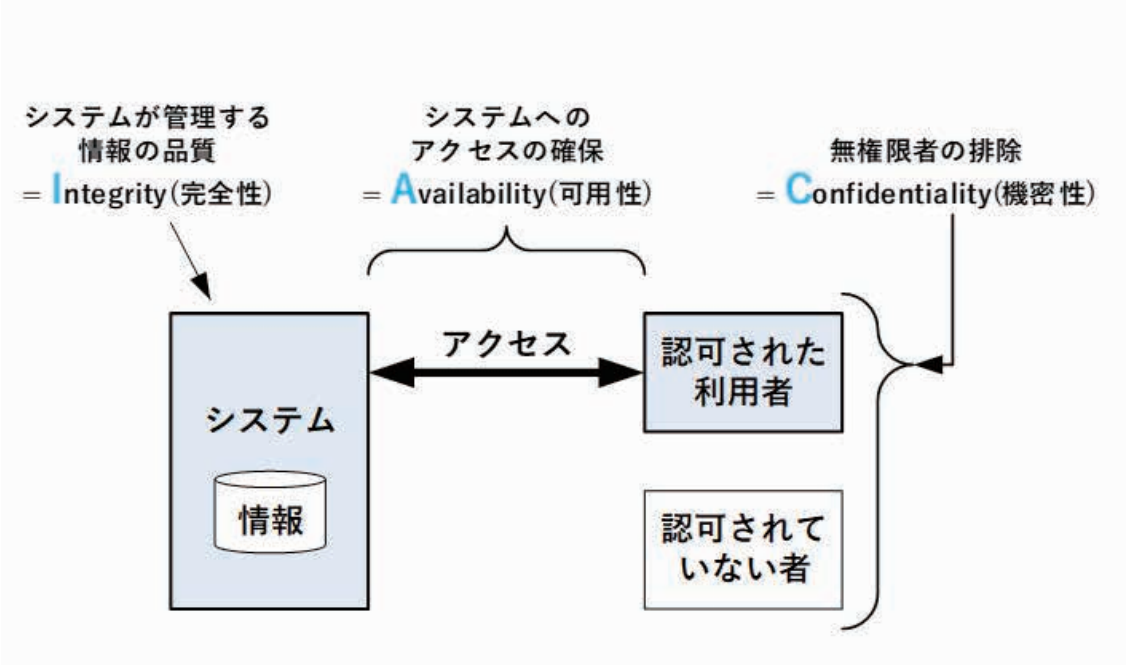
サイバー・フィジカルが融合する Society5.0 の時代に情報セキュリティが重要になるのはなぜでしょうか？

人間はもともと「フィジカル」な世界でさまざまなツールを使って「モノ」を生産・加工してきました。フィジカルな世界では、モノという資産の窃取や破壊を狙う攻撃者がいても、物理的に壁を築いて侵入を阻止すれば守ることができます。仮に窃盗犯などに侵入されたとしても、少なくともその場に不審者がいるかどうかは「目で見てわかる」ため、その後の警戒を厳重にしておけば被害は一時的なものにとどまります。フィジカルな世界ではモノを盗もうとしても大量に運搬するのは困難ですし、盗品を近隣で売買すると足がつきやすいため、盗む側のリスク、コストも大きいことがある程度の抑止力になります。

ところが、サイバーな世界ではその前提が成り立ちません。インターネットを通じて世界とつながったコンピュータには、地球の裏側からでも一瞬で侵入されます。サイバーな世界では「情報」が資産になりますが、情報はコピーができるため流出していてもすぐには気がつきませんし、ウイルス等を通じて継続的に盗聴されている場合もあります。印刷された紙であればトラックでなければ運び出せないような大量の情報も、ネットでは簡単に送信できてしまいます。

さらに「サイバー・フィジカル」の融合が進む Society5.0 においては、「情報」で実世界の「モノ」を動かすことができるため、自動車・水道・電気などの「生存を支えるインフラ」を物理的に破壊される可能性さえあります。このような背景のもとで、「情報セキュリティ」の重要さが格段に増しています。

3 セキュリティの三要素：ＣＩＡ



情報セキュリティには「CIA」と呼ばれる３つの基本要素があります。日本語では「機密性・完全性・可用性」と訳されるこの３要素は、「認可された利用者が、システムが管理する情報にアクセスする」というフレームワークのそれぞれに対応する、以下のような概念です。

C = Confidentiality（機密性）

認可されていない者を排除し、認可された利用者にのみアクセスを許可すること。

I = Integrity（完全性）

情報の喪失や改ざんを防ぐこと。

A = Availability（可用性）

必要な時に必ず情報へのアクセスが可能であること。

セキュリティが保てない事例

以上のような概念を踏まえて、C・I・A がそれぞれ侵害されるケースを例示すると以下のようになります。

ケース 1：正規に認可された利用者が ID/パスワードのメモを紛失し、それを入手した第三者が不正アクセスに成功する　→　Confidentiality 侵害

ケース 2:Web サイトに脆弱性があり、第三者が ID/パスワードを入力せずに情報入手に成功する　→　Confidentiality 侵害

ケース 3:「システム（Web サイト）」に対してインターネット上から大量のパケットが送りつけられ、正規の利用者がシステムを利用できなくなる　→　Availability 侵害

ケース 4：Web サイトが改ざんされる　→　Integrity 侵害

ケース 5：上司に叱責された職員がデータを流出させる　→　Confidentiality 侵害

ケース 6：偽の発注情報を紛れ込まされて業務処理が混乱する　→　Integrity 侵害

ケース 7：メールのご送信によりデータ流出が起きる　→　Confidentiality 侵害

ケース 8:誤操作により DB に高い負荷を与えるクエリーを発行した結果、性能が極端に悪化する　→　Availability 侵害

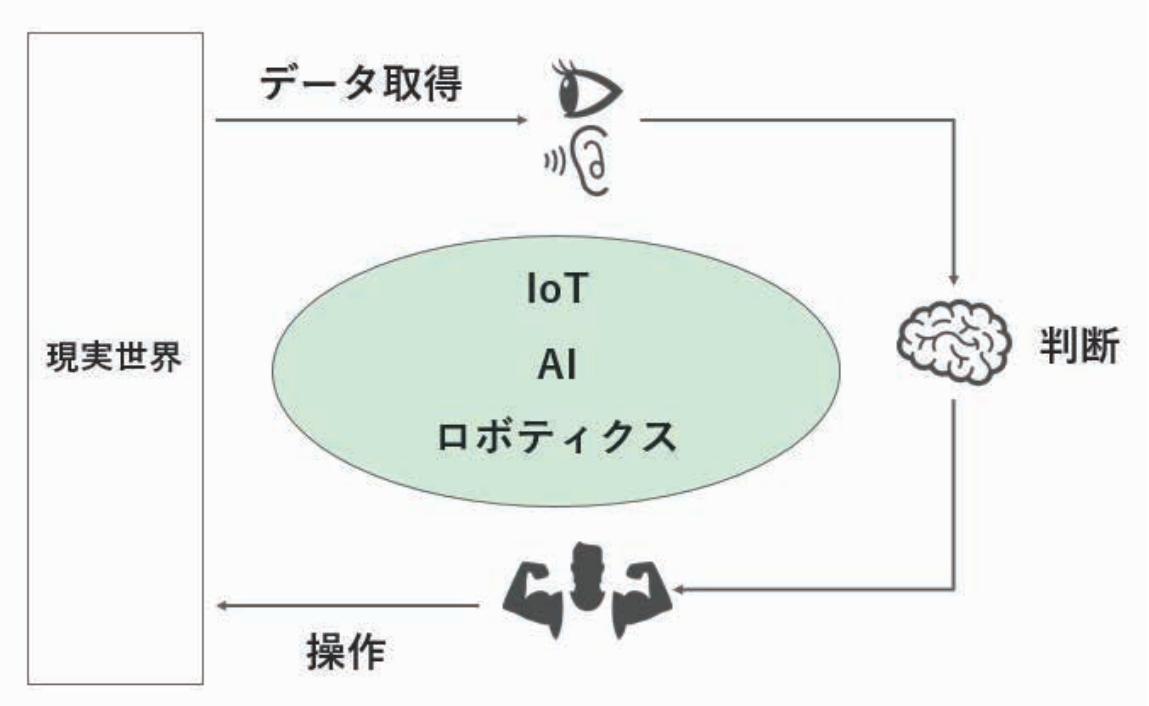
ケース 9：大地震により電力供給が途絶え、サーバーが利用できなくなる　→　Availability 侵害

ケース 10：システム更新のオペレーションにミスがあり、データが消滅する　→　Integrity 侵害

悪意ある攻撃者がいなくてもセキュリティ喪失は発生する

上記のケース 7〜10 に見られるように、「悪意ある攻撃者」が不在でもセキュリティ喪失事案は発生しますし、組織内部の人間が「悪意ある攻撃者」である場合もあります(ケース 5)。セキュリティ対策はさまざまな可能性を視野に入れて行わなければなりません。

4 近未来を支える技術



Society5.0 を支える、既に実現されていてさらに発展しつつある技術として IoT、AI、ロボティクスなどがあります。これらはいずれもこれまで人間がやってきた仕事をある程度代替するものと言えます。

人間は「現実世界」の情報を主に目や耳で感じ取り（他に嗅覚・触覚・温覚もあります)、その意味あいを「判断」して、筋肉（手足）で現実世界の対象物を操作しています。つまりこの一連の動きは「データ取得→判断→操作」のループと考えることができますが、現在さまざまな分野でこれを IT により代替する技術開発が進んでいます。

IoT = Internet of Things、モノのインターネット

IoT は主に「データ取得」のほうを中心とした概念です。コンピュータ技術が開発された初期の応用分野は給料計算や受発注管理など、文字および数値というデジタル情報を扱うものでした。しかし現在はセンサから得られるアナログ情報をデジタル化し通信に乗せてインターネットを通じてサーバーに届けるプラットホームが確立しました。「IoT」という場合は主に「センサを使って現実世界の情報を集める、さらにある程度の判断をする」機能/システムのことを呼ぶのが一般的です。もちろん、「操作」の部分まで行う IoT システムもあります。

AI = Artificial Intelligence、人工知能

AI は主に「判断」を IT で行うことを指します。そのために使われる技術に Machine Learning(機械学習)があり、さらにその一部に Deep Learning(ディープラーニング、深層学習)があります。AI 化することによって人間に比べて圧倒的に短時間で大量のデータ処理をすることが可能です。監視カメラの画像から不審人物や指名手配者を割り出す、製造業の検査工程で不良品を発見する、音声を解析して自動的に文字起こしをする、翻訳するなど、これまでは人間でなければできなかったさまざまな「判断」の代替が進んでいます。セキュリティの分野では、ウイルス検査や攻撃の兆候検出の用途で応用されつつあります。

ロボティクス ＝ Robotics、ロボット工学

「ロボット」はもともと「人間のように動く機械」を表す造語で、その研究開発・応用を行う工学分野がロボティクスです。ロボットには「データ取得、判断、操作」のすべてが必要です。特に「操作」を実現するためには「人間の筋肉や骨格の動きを代替しうるメカトロニクス技術」が必要で、「情報処理」が中心である IoT や AI とは違った難しさがあります。

情報セキュリティはどの分野においても必要

以上のように Society5.0 を支える技術には IoT、AI、ロボティクスなどがありますが、いずれの分野にしてもサイバー化が高度に進んでいる以上、情報セキュリティへの対策は欠かせません。

5 演習問題

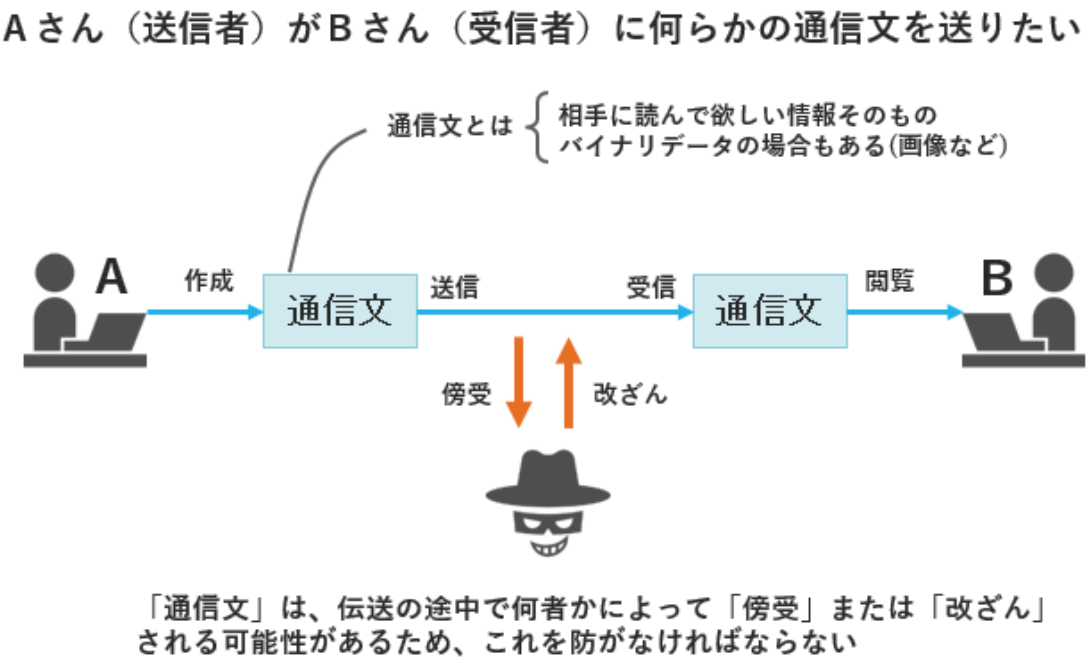
問 1

機密性侵害、完全性侵害、可用性侵害の例をそれぞれ挙げてください。

第2章.

暗号化・認証

1 通信文の傍受・改ざん対策が必要



Aさん（送信者）がBさん（受信者）に何らかの通信文を送りたいとします。

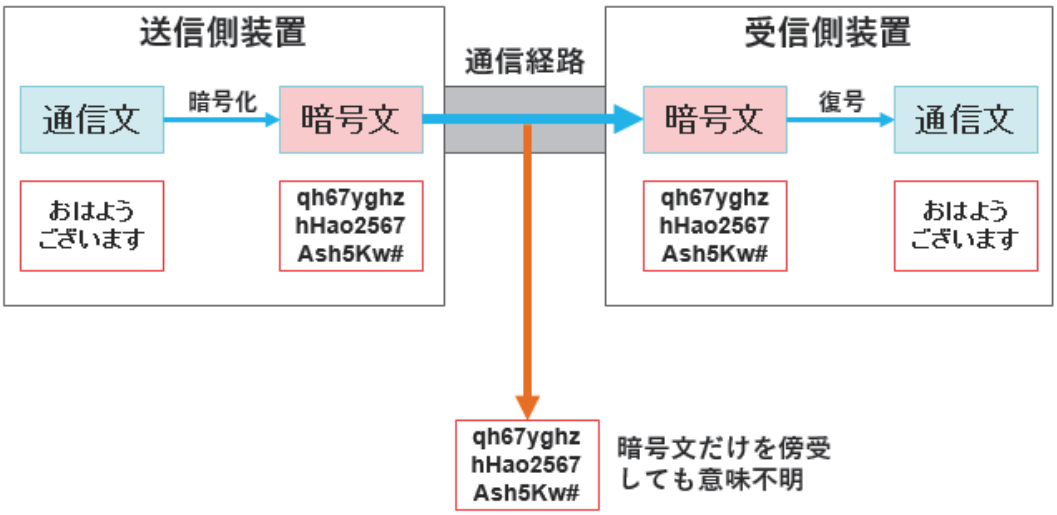
郵便に例えると、封書に入れて通信文を送る場合は他の人に読まれる心配はありませんが、葉書は途中で誰かに見られる可能性があります。さらに、不正に内容を書き換える「改ざん」の被害が起きることもあり得ます。

コンピュータ間の通信は基本的に葉書と同様、「傍受される（＝他人に見られる）」「改ざんされる」ことがありうると考えなければなりません。そこで、傍受・改ざんを防ぐ対策が必要になります。

葉書の場合、「改ざん」についてはある程度痕跡が残りますが、コンピュータ通信でやりとりされるデジタルデータでは、受け取ったデータそのものには痕跡が残らないため、改ざんの問題はより深刻になります。

2 傍受を防ぐには暗号化が必要

- 傍受そのものを防ぐことは不可能
- 傍受されても意味不明となるように暗号化する

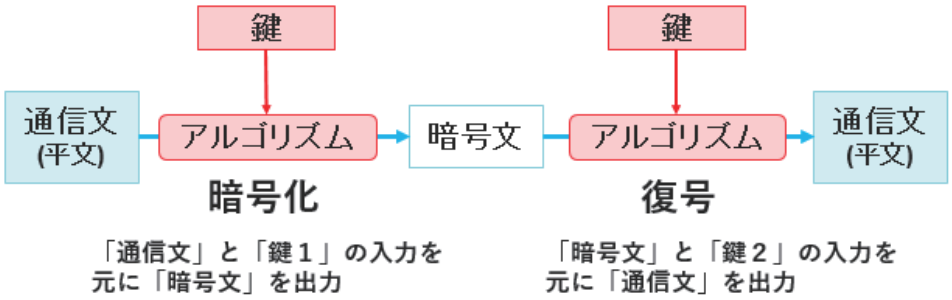


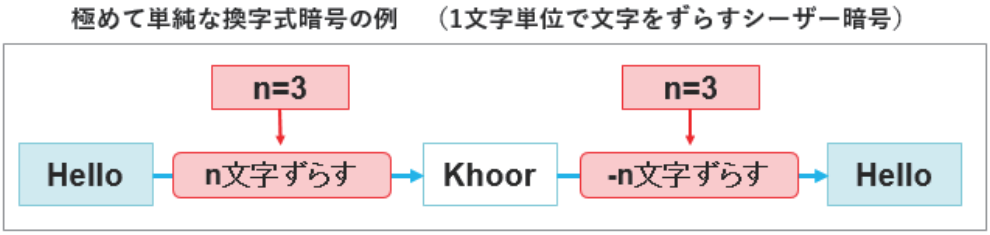
コンピュータ間の通信、特にインターネット通信では「傍受」そのものを防ぐことは不可能です。通信の秘密を守るためには、傍受されても意味不明となるように暗号化しなければなりません。

図は、「おはようございます」という通信文を「qh67～」から始まる文字列へと暗号化した例です。通信経路上に流すデータを暗号文だけにすれば、暗号文だけを傍受しても意味不明です。受信側装置で暗号を解読すれば「おはようございます」という元の通信文を復元できます。

通信文から暗号文を作る操作を「暗号化」
逆に暗号文から通信文を作る操作を「復号」と言います（「復号化」と間違えやすいので注意）。

3 暗号通信には鍵とアルゴリズムが必要





暗号通信をするためには「鍵」と「アルゴリズム」が必要です。

図の下段はシーザー暗号と呼ばれる極めて単純な換字式暗号の例で、「Hello」を 3 文字ずらして「Khoor」という暗号文を作り、復号ではそれを 3 文字戻して「Hello」を復元しています。この場合、「n 文字ずらす」という処理ロジックが「アルゴリズム」、「n=3」が「鍵」に該当します。

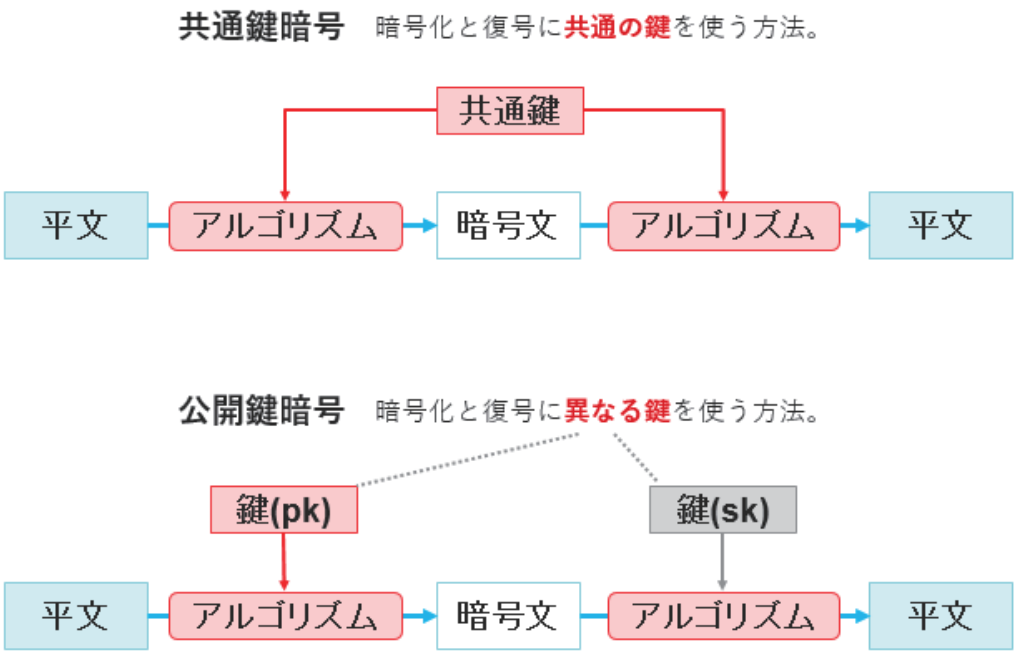
アルゴリズムが共通でも、鍵が違えば違う暗号文が生成されるため、通信相手によって違う鍵を使えばアルゴリズムは共通のものを使い回せます。

もちろん、シーザー暗号のような単純なアルゴリズムでは簡単に解読されてしまうため、現代ではより解読されにくいアルゴリズムが開発されています。

一般に、「解読」とは鍵が与えられていない状態で鍵をつきとめて通信文を復元することを言い、「解読の難しさ」のことを暗号強度と言います。暗号強度は「アルゴリズム」と「鍵の複雑さ」によって決まり、同じアルゴリズムでも鍵が複雑な方が暗号強度が高くなります。「鍵の複雑さ」は実際には「鍵の長さ」によって決まります。

なお、暗号化されていない文のことを「平文（ひらぶん）」と呼びます。「通信文」は通信経路上を流れるデータのことを呼ぶ場合もあるため、今後は暗号化されていない文の呼称は「平文」で統一します。

4 共通鍵方式と公開鍵方式



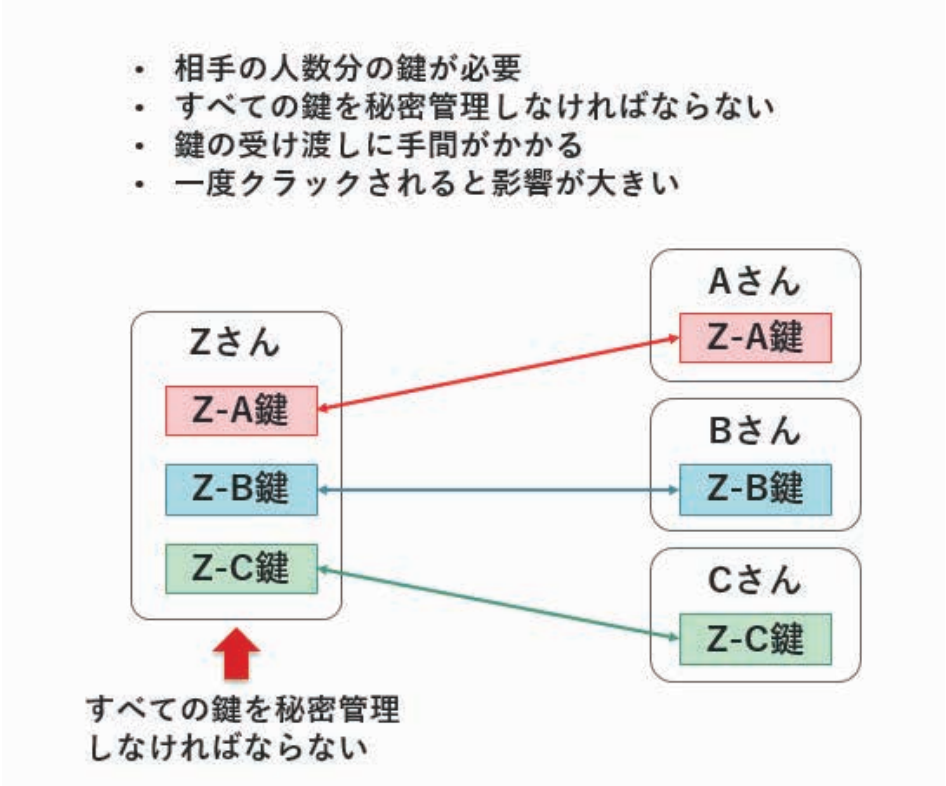
暗号アルゴリズムには大別して共通鍵暗号方式と公開鍵暗号方式があります。

共通鍵暗号は暗号化と復号に共通の鍵を使う方式、公開鍵暗号は異なる鍵を使う方式です。

公開鍵暗号では一度の通信で 2 種類の鍵を使うため、今後は pk, sk のような略称で表記します。

pk：public key　（公開鍵）
sk：secret key　（秘密鍵）

5 共通鍵方式は鍵の管理が煩雑



共通鍵方式は直感的にわかりやすい方法ですが、通信相手が増えたときに鍵の管理が煩雑になる欠点があります。

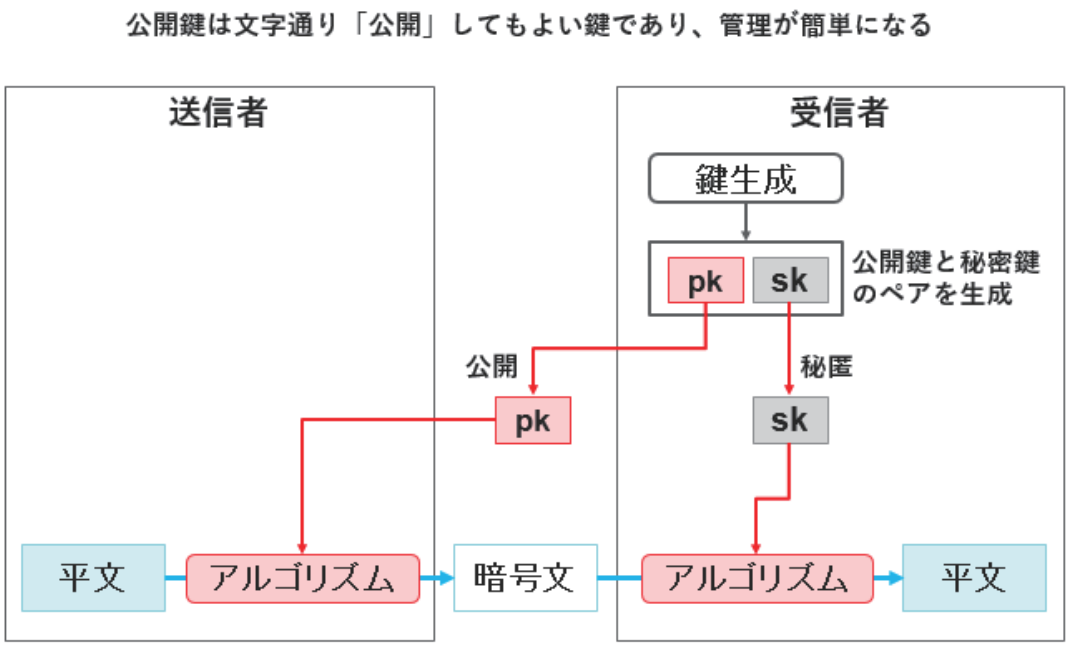
図はZさんがA～Cさんと通信をする場合のイメージですが、Zさんは Z-A, Z-B, Z-C という3つの鍵をすべて秘密に管理しなければなりません。相手の数が増えると鍵もその分増えます。

特に問題なのは「鍵の受け渡しに手間がかかる」ことです。共通鍵はどちらか一方で生成して相手に渡さなければなりませんが、鍵を渡そうとするときにはまだ暗号が使えません。鍵そのものを傍受されてしまったらいくら暗号化をしても無駄で、その後その鍵を使った暗号はすべて危険になります。インターネット上の通信路は基本的にすべて「傍受されうる」と考えなければならないため、鍵の受け渡しはインターネット以外の手段、または特殊な鍵交換プロトコルで行わなければならず、手間がかかってしまいます。

また、「多くの鍵を秘密に管理しなければならない」ということは、いったんそれを破られたときは影響が大きいということです。Zさんのマシンがクラックされて鍵が流出した場合、その鍵を使用するすべての関係者が鍵を変更しなければならなくなります。

こうした欠点を解消できるのが「公開鍵暗号」方式です。

6 公開鍵方式では鍵を公開できる



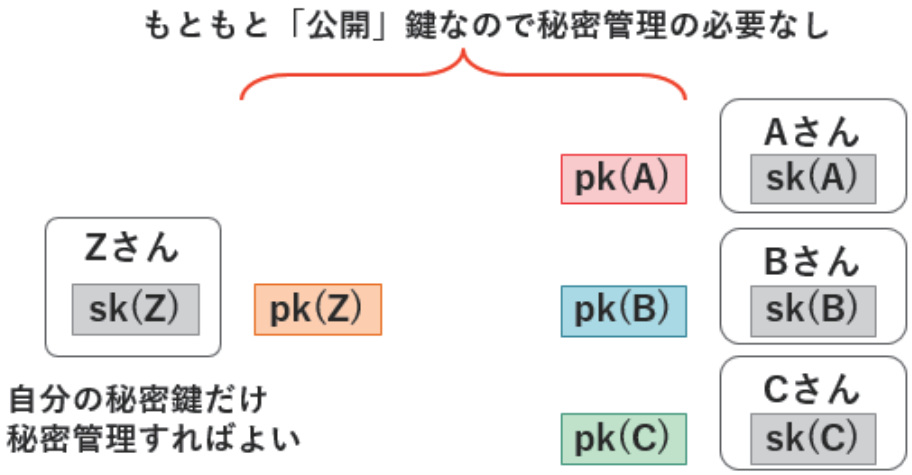
図は公開鍵暗号方式の基本的なしくみです。まず受信者が 2 つの鍵を生成し、一方(pk)を自分の公開鍵として公開します。これは誰にでも「公開」する鍵なので暗号化せずに送ることができます。
送信者はその公開鍵を使って平文を暗号化します。

ここで重要なのが、「この暗号文は公開鍵(pk)では復号できない」ということです。
公開鍵で暗号化した暗号文を復号するためには、秘密鍵(sk)が必要です。

秘密鍵(sk)は受信者が pk と同時に生成した後は自分自身で秘匿しておくもので、他人に「受け渡す」必要がないため共通鍵方式最大の弱点を回避できます。

7 公開鍵方式は鍵の管理が簡単

- 自分の秘密鍵だけ秘密管理すればよい
- 公開鍵は平文で送れる
- クラックされた場合の影響範囲が狭い



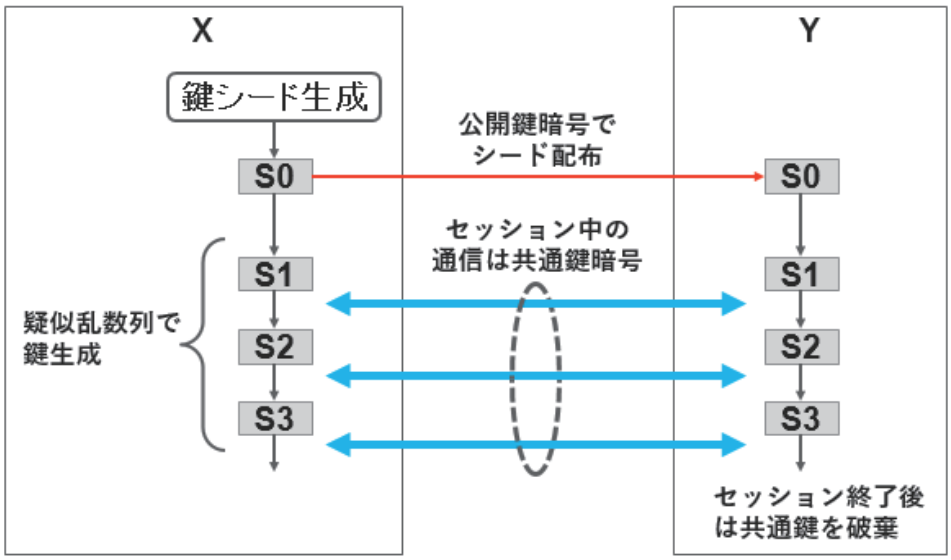
「公開鍵は公開できる、秘密鍵は受け渡す必要が無い」というこの特長によって、公開鍵暗号方式では鍵の管理が簡単になります。

共通鍵暗号方式の場合、Z さんは A〜C さん全員分の鍵を秘密管理する必要がありましたが、公開鍵暗号方式の場合は各自が自分の秘密鍵だけを秘密管理すればよく、公開鍵は平文で送ることができます。もともと他人に影響する秘密鍵を持っていないので、Z さんのマシンがクラックされたとしても影響範囲は狭くなります。

このようなメリットがあるため、公開鍵暗号方式は現在広く使われています。

8 公開鍵と共通鍵を適材適所で併用する

- 公開鍵暗号は処理速度が遅いため、大量の通信には向かない
- 適材適所で、共通鍵（速い）と公開鍵（鍵配布が簡単）を組み合わせる
- 臨時の共通鍵を生成し、公開鍵暗号はその鍵の配布に使う



公開鍵暗号は共通鍵暗号に比べて処理速度が非常に遅いため、大量の通信には向きません。実用的には、共通鍵（速いが鍵配布が困難）と公開鍵（遅いが鍵配布が簡単）の長所を組み合わせて使う方法があります。

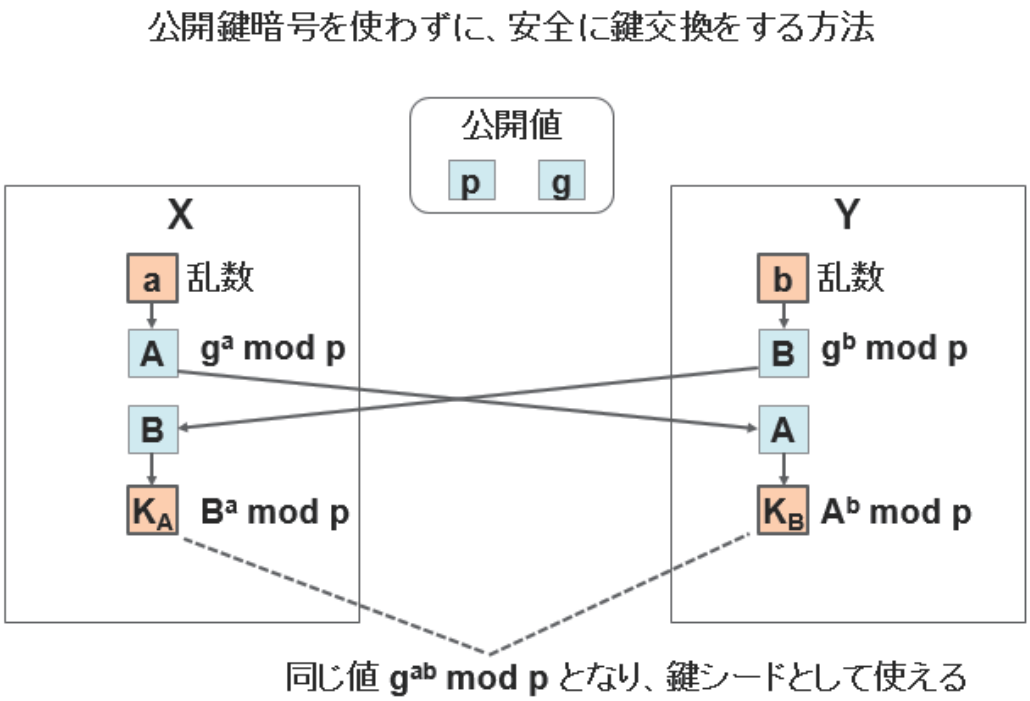
X と Y が通信をしようとするとき、まず X が「鍵シード」（または初期化ベクトル IV：Initial Vector）と呼ばれる数値を生成し、それを公開鍵暗号で Y へ配布します。ここはデータ量が少ないため、遅い公開鍵暗号でも問題ありません。これで X と Y が同じ鍵シード S0 を共有できます。

X と Y で同じ疑似乱数アルゴリズムと同じシード S0 を使えば、生成される疑似乱数列 S1、S2・・・も同じになるため、これを共通鍵として使うことができます。一連の通信セッション中の通信は共通鍵暗号で行います。

同じ鍵を長時間使うと解読される危険が高まるため、一連のセッション中でも共通鍵は短時間で変えていかなければなりません。鍵シード S0 をそのまま使わず疑似乱数列 S1、S2・・・を生成させるのはそのためです。これらの鍵はセッション終了後破棄します。S0 から始まるこのような共通鍵を、通信セッション中のみ使われる鍵という意味でセッション鍵とも呼びます。

「安全に鍵を共有することが難しい」のは共通鍵暗号方式の弱点ですが、その問題を解決する方法の 1 つがこのように公開鍵暗号を併用することです。

9 Diffi-Hellman 鍵交換方式



共通鍵暗号方式の弱点である「安全に鍵を共有することが難しい」問題を解決する方法には、公開鍵暗号併用方式の他にも、Diffi-Hellman 鍵交換方式（または DH 法）という方法もあります。

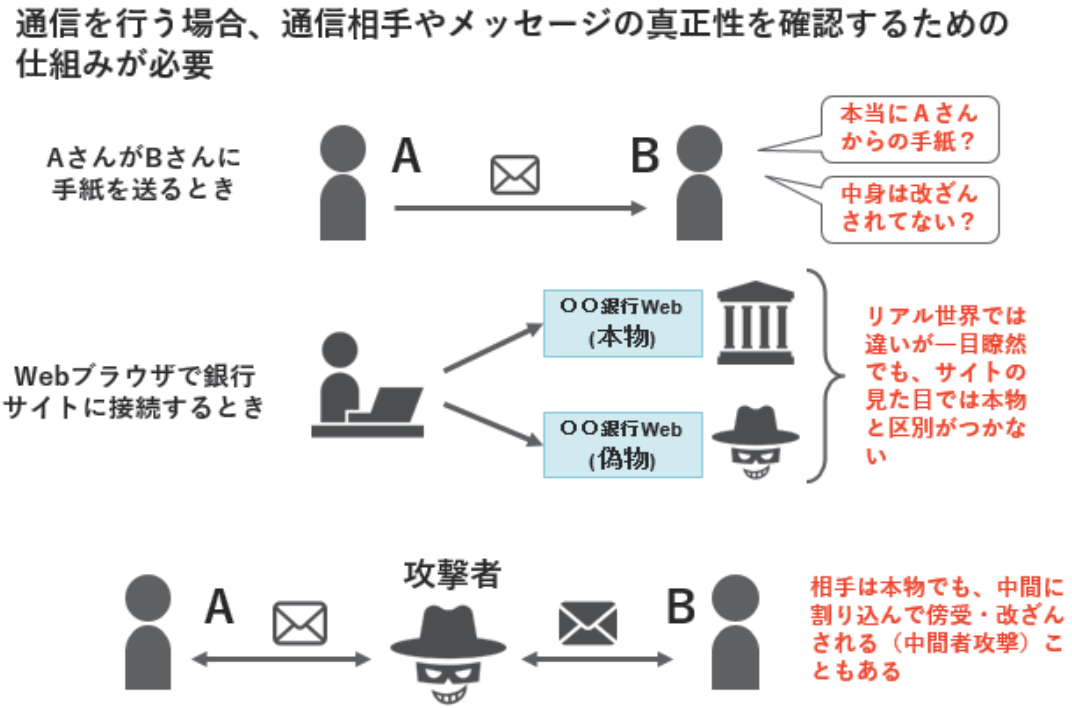
X と Y が通信をしようとする場合、DH 法では大きな素数 p と小さな数 g を事前に決めておくかセッション確立時に共有します。p と g は公開しても構いません。その後 X と Y がそれぞれ乱数 a、b を生成し、値 $A=g^a \bmod p$ と $B=g^b \bmod p$ を計算して相手に送信します。X と Y がそれぞれ受信した B, A を元に再び同じ計算をすると $K_A=K_B= g^{ab} \bmod p$ となり、この値は鍵シードとして使うことができます。

暗号化せずに通信路を流れる A、B および公開値である p, g がわかったとしても、$g^{ab} \bmod p$ を計算することは難しいのがこの方式のポイントです。X と Y も相手方の生成した乱数 a, b そのものはわかりませんが、$g^{ab} \bmod p$ は計算により共有できるため鍵シードとして使用できます。

鍵シード共有後は前ページ同様、疑似乱数列を生成して共通鍵として使用します。

DH 法は SSL/TLS や IPsec 通信で採用されています。

10 認証とは？



A さん（送信者）が B さん（受信者）に物理的な手紙/葉書を送る場合でも、開封された形跡がなかったとしてもそれが真に A さんからの手紙とは限りません。

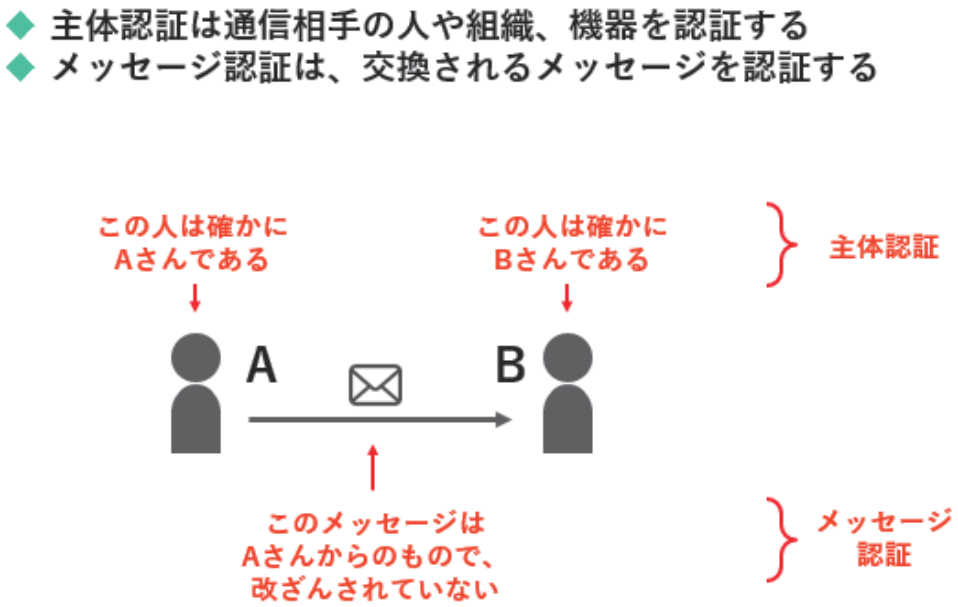
【なりすまし】　何者かが A さんになりすまして偽の手紙を送ってきた
【改ざん】　A さんの手紙を何者かが途中で開封・改ざんし封筒ごと差し替えた

といった可能性があります。物理的な手紙は途中で開封しにくく、改ざんの痕跡も残りやすいため実際にこれらの脅威は少ないですが、インターネット上のデジタル通信では痕跡が残らずこれらの攻撃を非常に簡単に行えてしまうため、対策が必要です。このために必要なのが「認証」です。

たとえば Web ブラウザで銀行サイトに接続するとき、暗号化をすれば通信路で盗聴されることはありませんが、そもそも接続先が偽物のサイトだったら暗号化をしても無意味です。リアルの世界では本物と偽物が一目瞭然でも、Web サイトの見た目では本物と区別がつかないため、何らかの手段で「真正（本物）であることの証明」＝認証を行わないと安全な通信ができません。

「接続先が偽物」という場合の他に、何者かが中間に割り込んで傍受・改ざんされるケースもあります。暗号化の節で触れた DH 鍵交換法は「中間者攻撃」に弱いため、通信相手の認証を鍵交換とは別な方法で行わなければなりません。

11　主体認証とメッセージ認証



そもそも「通信」とは、通信を行う「主体」が何らかの「メッセージ」を交換する行為です。
そこで、認証を対象者で分類すると主体認証とメッセージ認証の 2 種類があります。

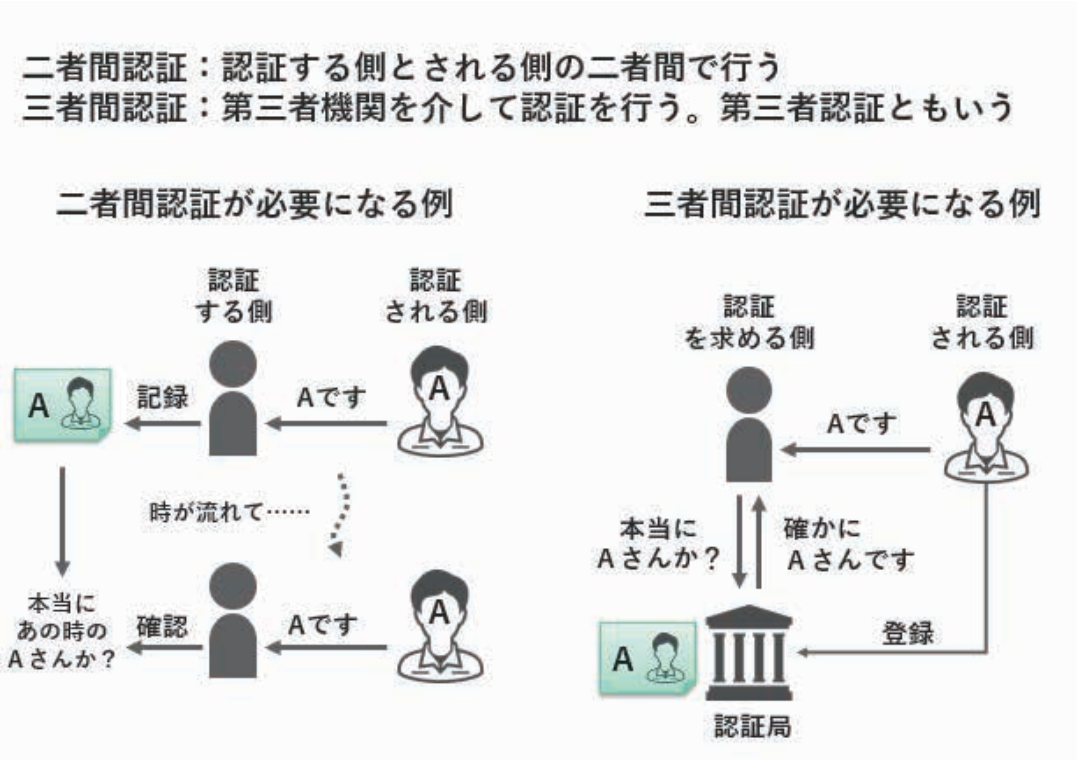
主体認証は通信相手の人や組織、機器を認証するもので、

- この人は確かに A さんである
- この Web サイトは確かに S 社の Web である
- この IC カードは確かに S 社の入館証である

などの証明を行います。

メッセージ認証は交換されるメッセージを認証するもので、「このメッセージは A さんからのもので、改ざんされていない」ことを証明します。

12 二者間認証と三者間認証

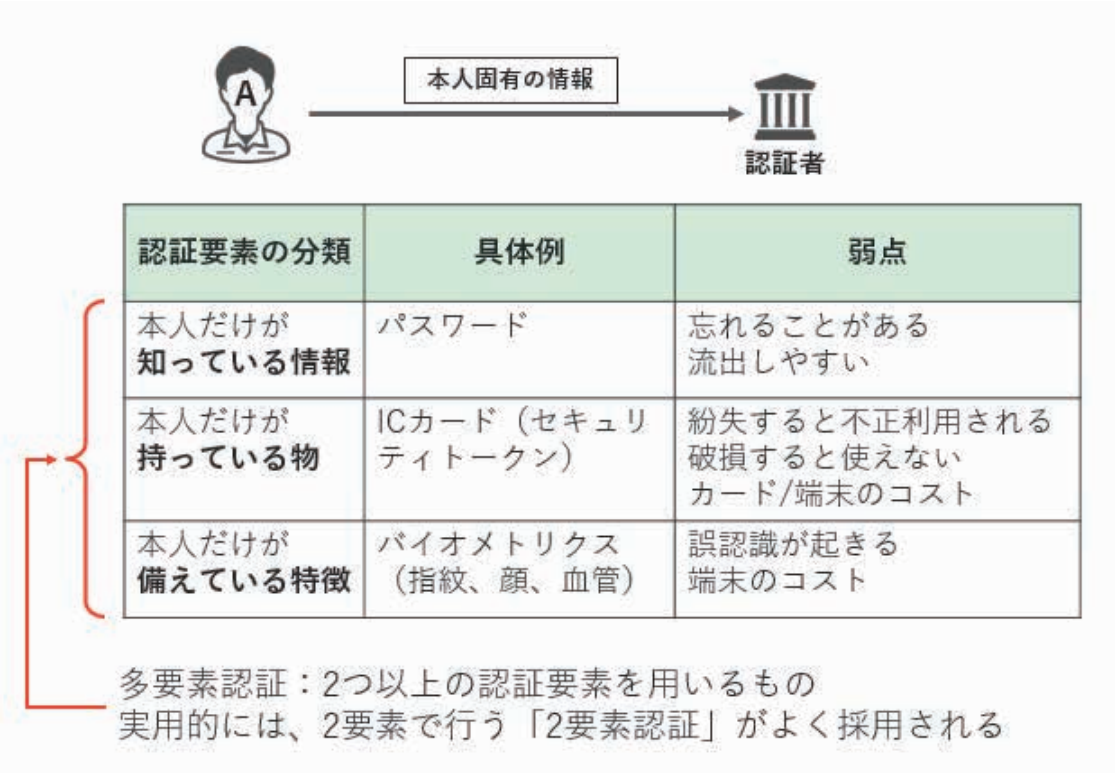


「誰が認証を行うのか？」について考えると、二者間認証と三者間認証（第三者認証）の 2 種類があります。

二者間認証は認証する側とされる側の二者間で行うもので、会員登録制の店舗などに例えることができます。認証する側が何らかの記録を持っておき、後日「A さん」が現れたときに記録と照合して「A さん」本人であることを自分自身で認証します。

三者間認証は第三者機関を介して認証を行います。認証される側は自分の情報を認証局という第三者機関に登録しておきます。認証を求める側は「A です」という申告を受けたら「本当に A さんか？」を認証局に問合せ、認証局が A さんの登録情報と照合して「確かに A さんです」と認証します。

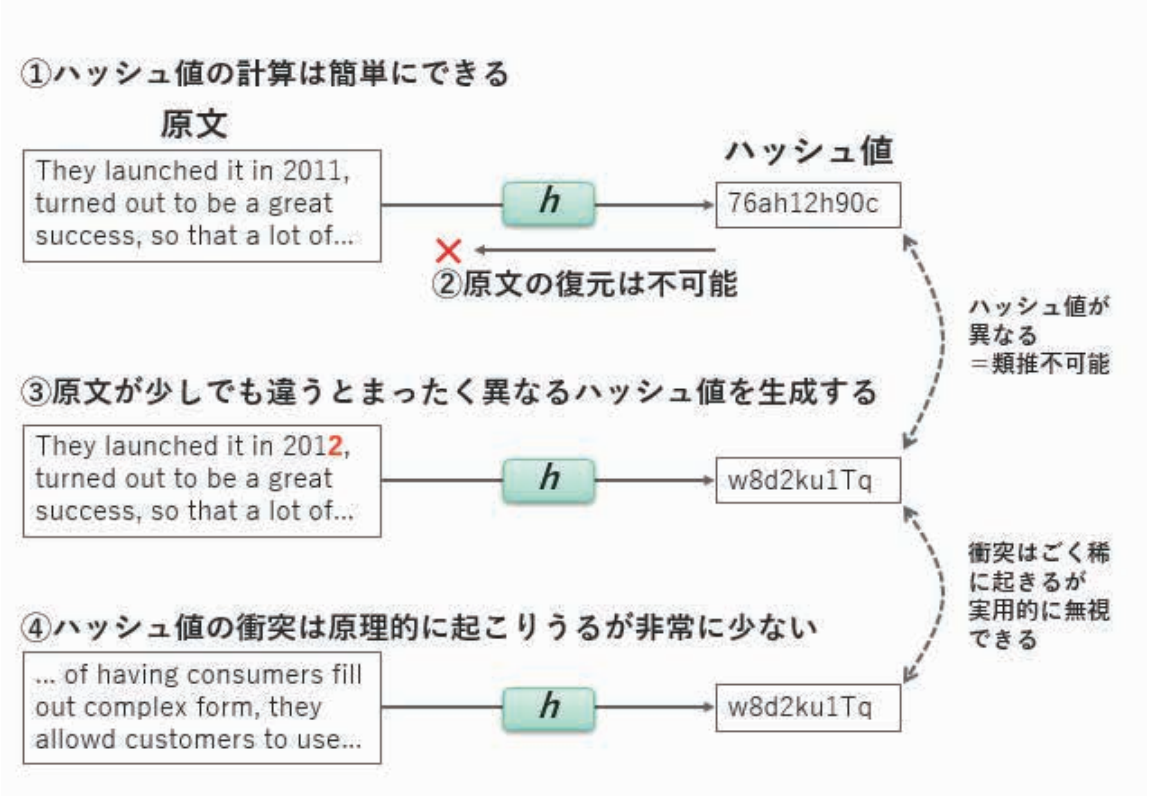
13 主体認証の実現方法



主体認証は、認証される本人固有の情報を認証者に送ることによって行います。
「本人固有の情報」の源泉を「認証要素」と言います。
「認証要素」は、本人だけが「知っている情報」「持っている物」「備えている特徴」の 3 種類におおまかに分かれます。具体例はそれぞれ上図の表のようになり、それぞれ一長一短があります。

複数の認証要素のうち 2 つ以上を用いる認証方式を多要素認証と言い、強固なセキュリティシステムを必要とする場合に用いられます。実用的には、2 要素で行う 2 要素認証がよく使われています。

14 ハッシュ関数の性質

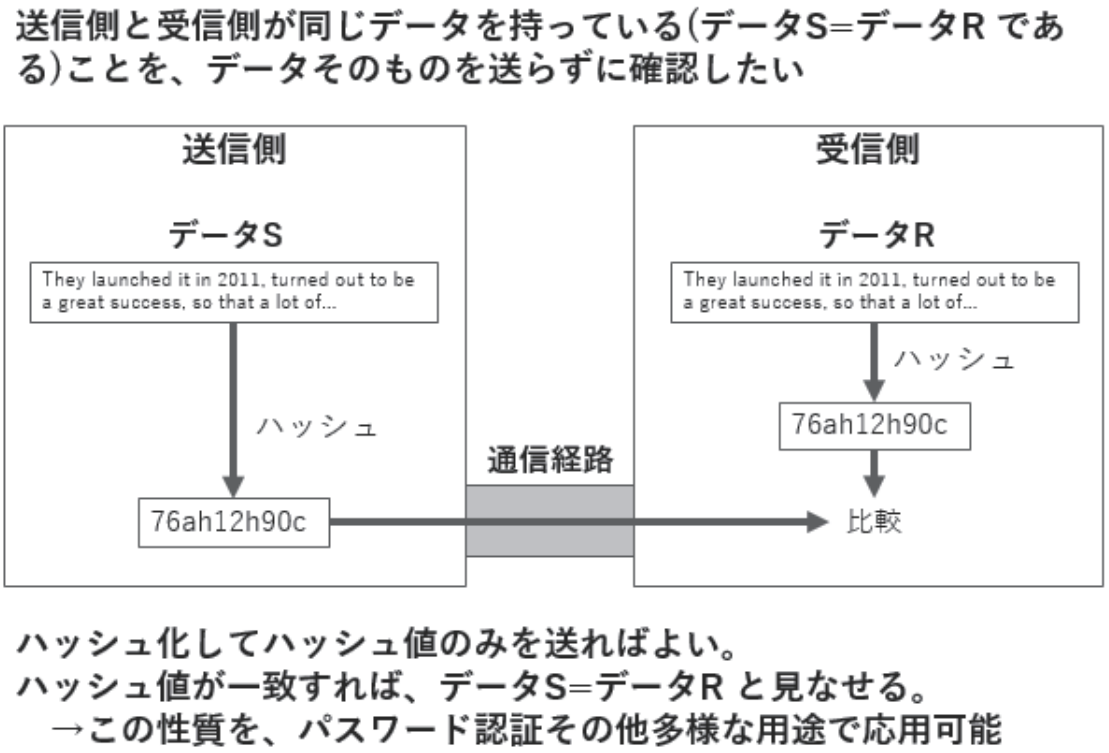


認証を行うために多用される「ハッシュ関数」の基本的な性質を知っておきましょう。

ハッシュ関数とは、図中の h の箱の部分で、任意長の「原文」を入力したときに固定長の「ハッシュ値」を出力する関数です。
ハッシュ関数のうちで、①ハッシュ値を簡単に計算することができ、②ハッシュ値から原文を復元することが不可能で、③原文が少しでも違うとまったく異なるハッシュ値を生成し、④ハッシュ値の衝突（偶然一致すること）がごく稀にしか起きないものが認証処理に使われます。

「原文が少しでも違うとまったく異なるハッシュ値を生成する」条件が満たされない場合、似たハッシュ値を持つ原文は似た文であることが類推できるため脆弱です。

15 ハッシュ関数の応用



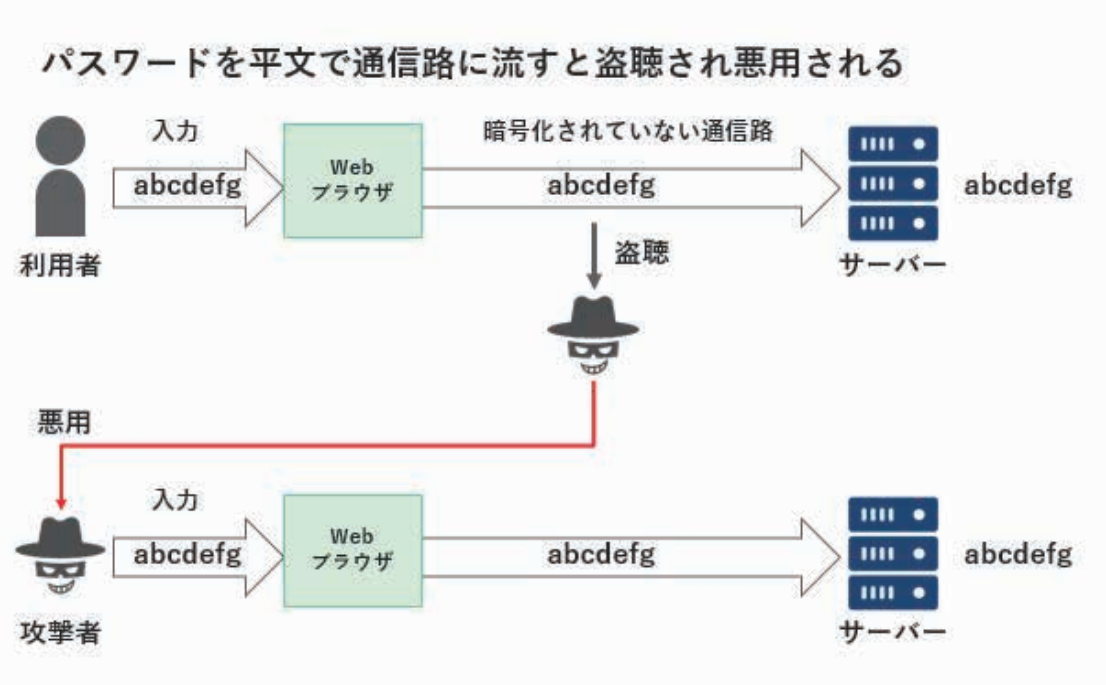
ハッシュ関数を認証に応用するもっともシンプルな例を示します。

送信側と受信側が同じデータを持っていることを、データそのものを送らずに確認したい場合があります。たとえば「パスワードを確認する」場合がその例です。

このような場合、送信側でデータ S のハッシュ値を計算してハッシュ値のみを送り、受信側でもデータ R のハッシュ値を計算して比較します。双方のハッシュ値が一致すれば S=R であろうとみなせます。

ただし、この例はもっとも単純な応用のイメージであり、実用的にはより複雑な手順が必要です。

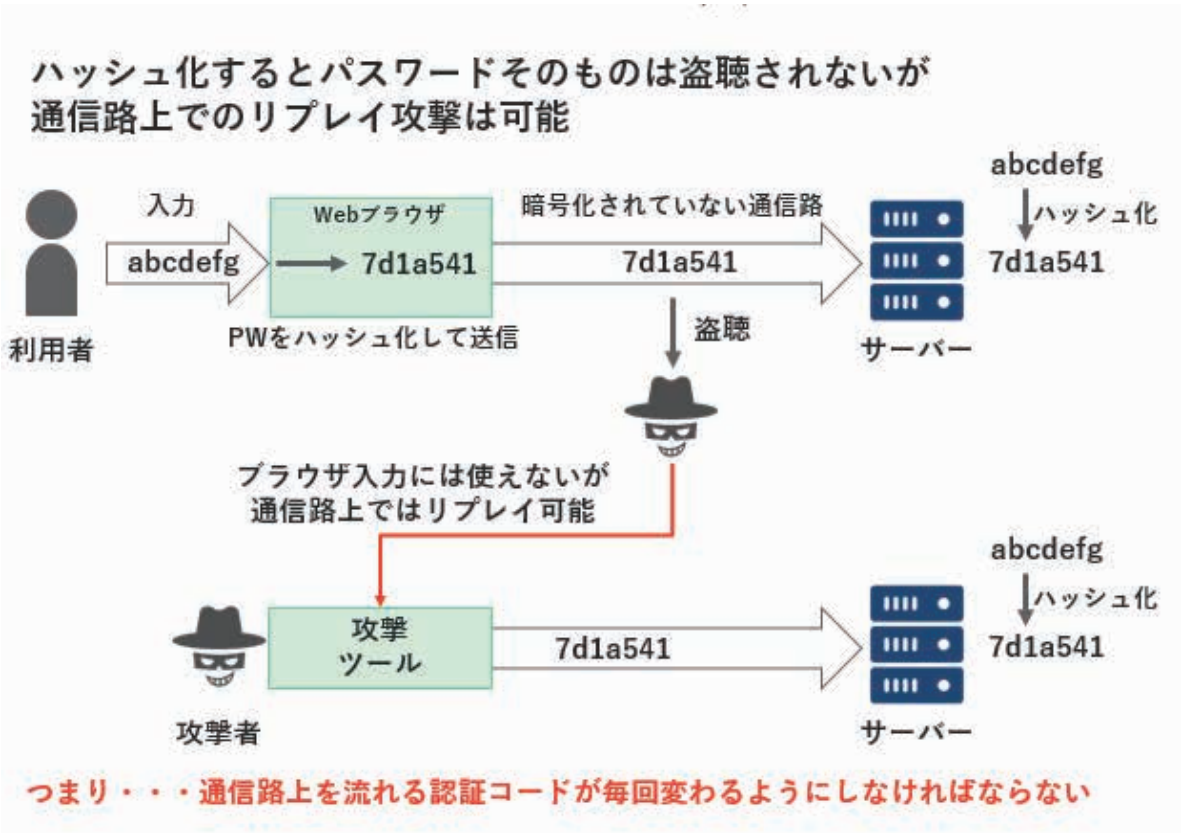
16 パスワード認証の脆弱性(1)



パスワードは主体認証のために最もよく使われる手軽な方法です。Web ブラウザでアクセスできる会員制のサイトを作る場合など、ユーザーID とパスワードによる主体認証がよく使われているため、パスワードを使う機会は多いものです。

しかし、パスワードを平文で通信路に流すと盗聴され悪用されてしまいます。攻撃者は盗聴したパスワードを正規の利用者と同じように Web ブラウザから入力すれば悪用できてしまいます。

17 パスワード認証の脆弱性(2)

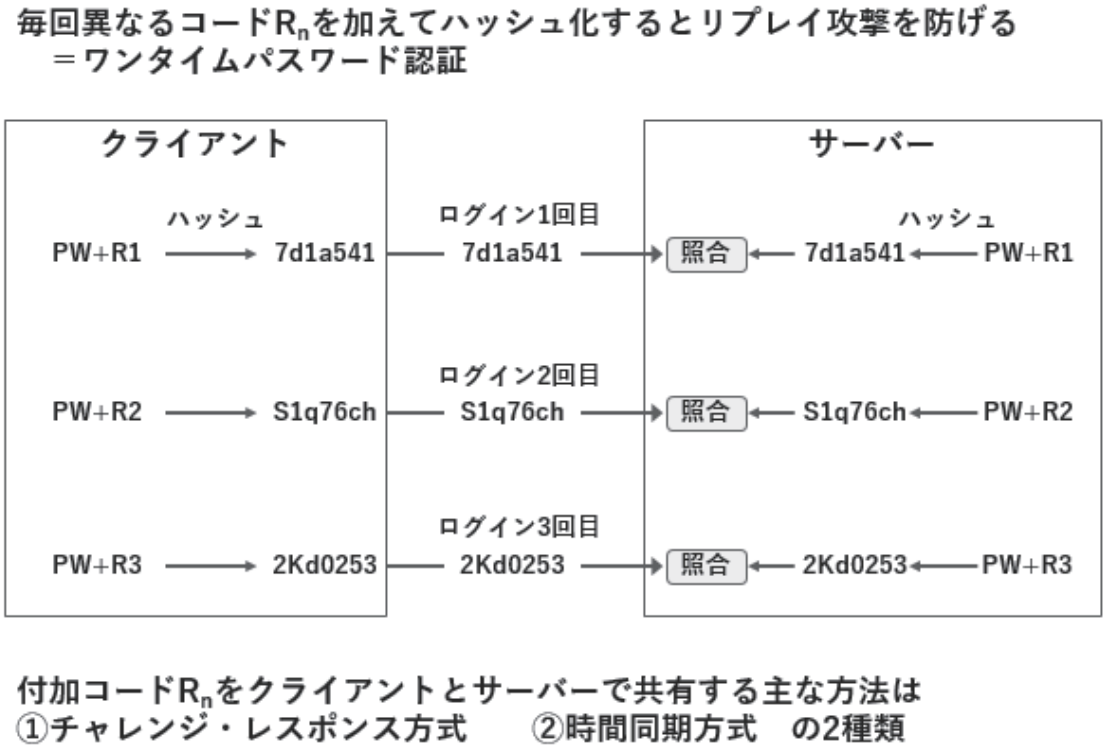


盗聴されてもパスワードがわからないように、Web ブラウザ上でパスワードをハッシュ化して送信してみましょう。サーバー側で同じようにハッシュ値を計算して照合する仕組みにすれば、通信路上をパスワードが流れることはないため、パスワードそのものは盗聴できません。ハッシュ値を盗聴してもそこから元のパスワードを復元することはできないため、利用者と同じ方法でアクセスすることはできません。

しかし、ブラウザとは別に攻撃ツールを作り、ハッシュ値そのものを流せば元のパスワードが分からなくても不正アクセスが可能です。これをリプレイ攻撃と言います。

ログイン時に通信路上を流れる認証コード（パスワードのハッシュ値）が毎回同じだとリプレイ攻撃が可能になってしまいます。したがって、通信路上を流れる認証コードはログイン試行の度に変わるようにしなければなりません。

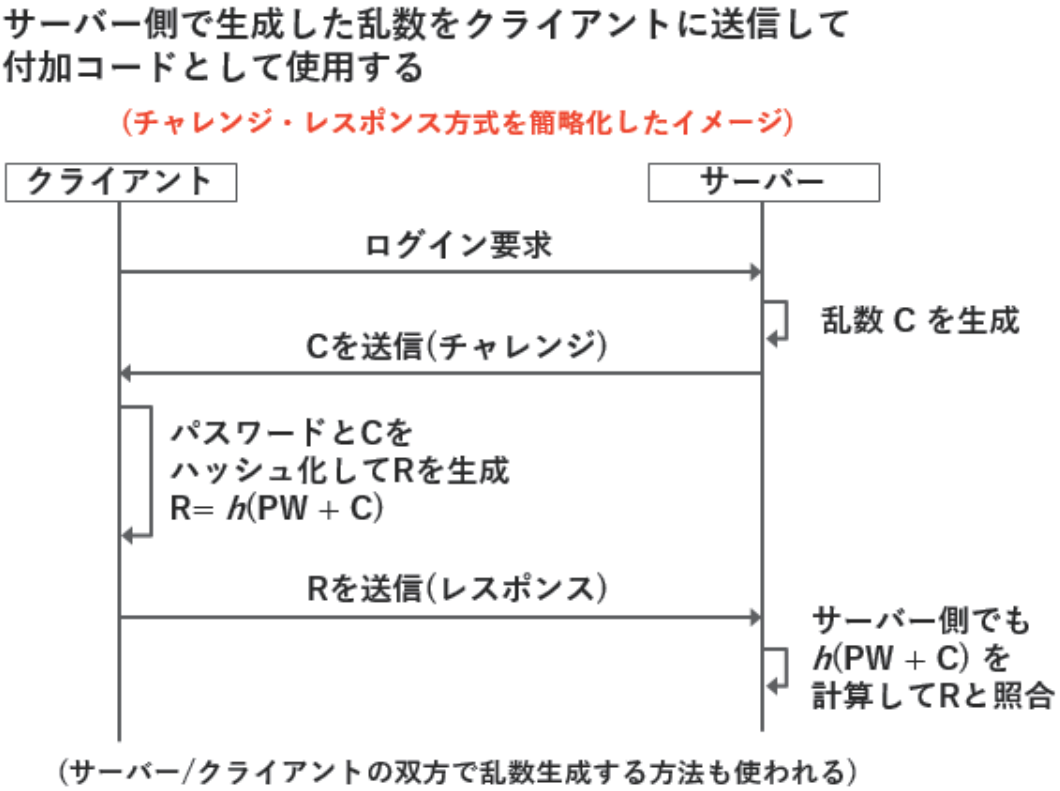
18 ワンタイムパスワード認証



ログイン試行の度に毎回異なるコード R_n を加えてハッシュ化するとリプレイ攻撃を防げます。
このように認証のために通信路上を流れるコードが毎回変わるようにする方法をワンタイムパスワード認証と言います。

そのためには付加コード R_n をクライアントとサーバーで共有しなければなりません。そのための主な方法としては　①チャレンジ・レスポンス方式　　②時間同期方式　の 2 種類があります。

19 チャレンジ・レスポンス方式



チャレンジ・レスポンス方式は、パスワードに乱数を加えてハッシュ化を行う方法です。
上図はその実際のチャレンジ・レスポンス認証を簡略化して要点だけを示したイメージです。

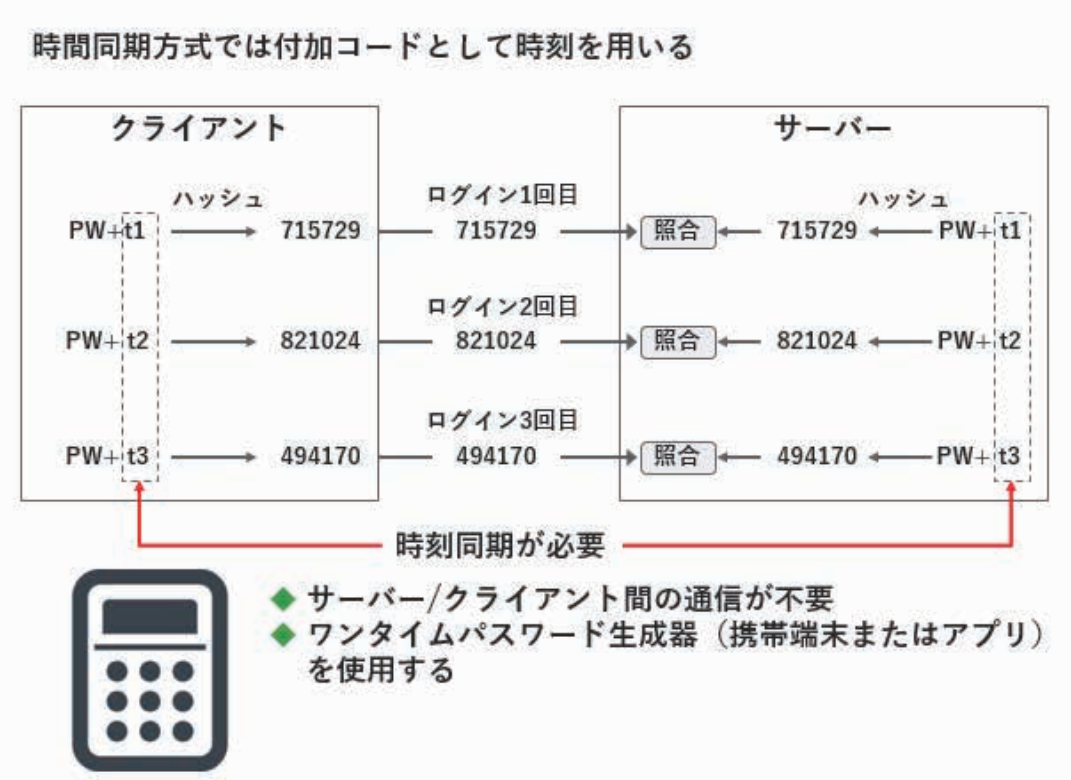
クライアントがサーバーにログイン要求を出すと、サーバーは乱数 C を生成して返信します。これをチャレンジと言います。

クライアントはパスワードと C を結合したものをハッシュ化して R を生成して送信します。$h()$ はハッシュ関数です。サーバー側でも保存してある PW と C を結合してハッシュ値を計算し、R と照合します。

この手順でパスワード認証を行うと、通信路上を流れるハッシュ値は毎回変わるためリプレイ攻撃に対しても強靭になります。

この方式はサーバー/クライアント間でリアルタイムに通信を行える場合に採用できます。

20 時間同期方式



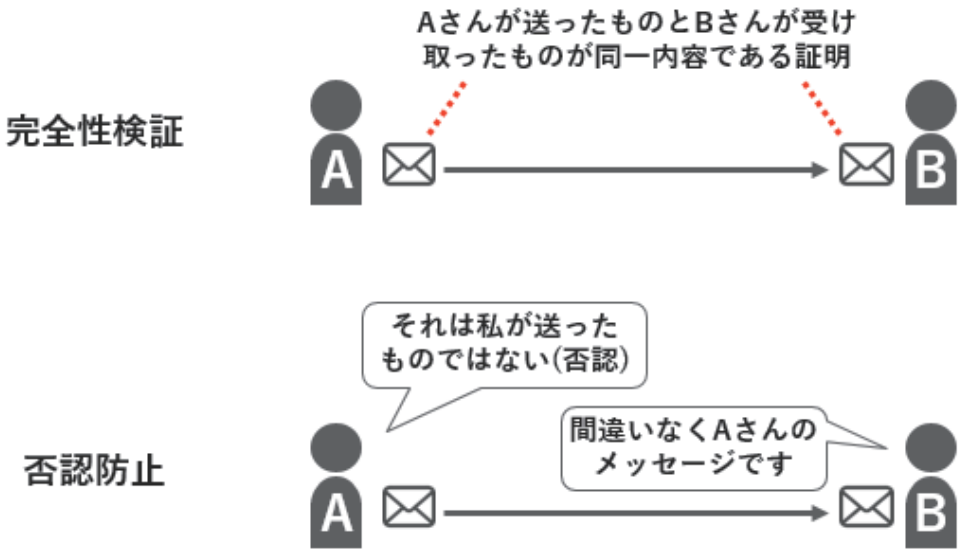
時間同期方式は、付加コードとして時刻を用いる方法です。ワンタイムパスワード生成器やセキュリティトークンと呼ばれる小さな機器のボタンを押すと、その時の時刻を加えてハッシュ化した数値が表示されます。その数値を入力すると認証されます。

この方式ではサーバー/クライアント間の通信が不要ですが、携帯端末またはアプリのワンタイムパスワード生成器が必要です。ハッシュ化された認証コードは人間が読んで入力するため、入力しやすいように通常は数桁の数字のみが使用されます。

携帯端末とサーバーの時刻はズレていくため、何らかの方法で時刻ズレを同期する仕組みが必要です。

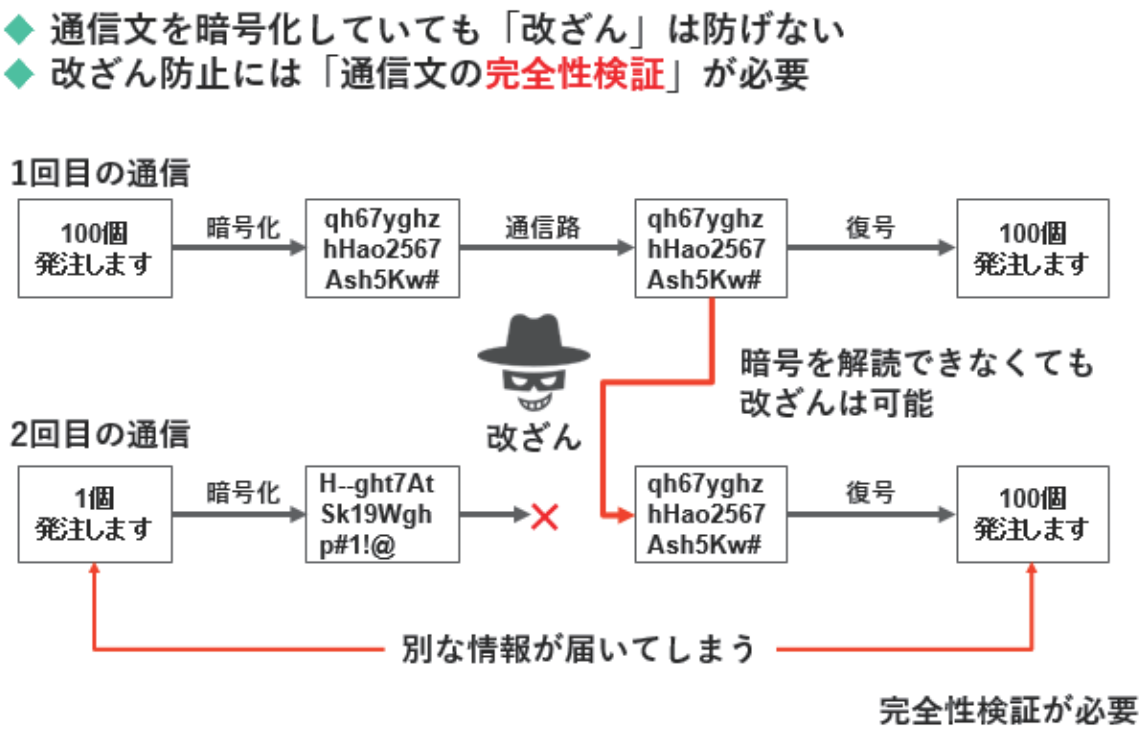
21　メッセージ認証＝完全性検証と否認防止

◆ 通信路での改ざんを検出できなければならない（完全性検証）
◆ 送信者の否認を防止できなければならない（否認防止）



メッセージ認証は通信内容（メッセージ）を認証するもので、通信路上での改ざんを検出する「完全性検証」と、送信者が否認することを防ぐ「否認防止」機能が求められます。

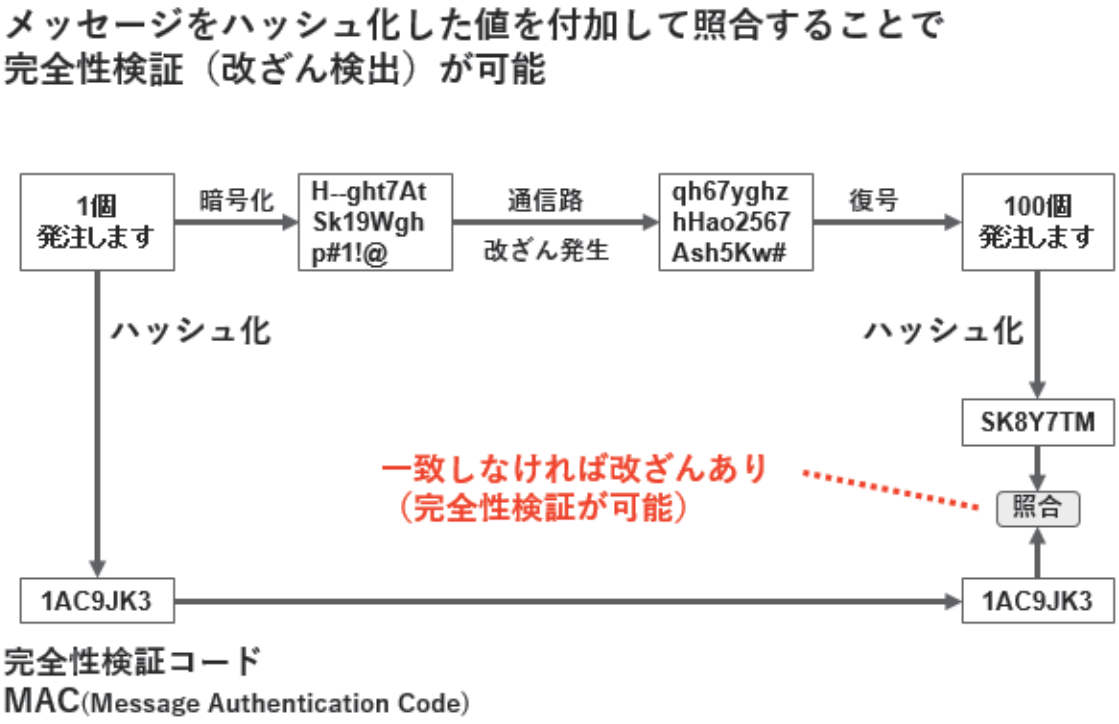
22 暗号化だけでは改ざんは防げない



通信文を暗号化すると解読は防げますが、暗号を解読できなくても改ざんはできる場合があります。

図は 1 回目の通信で使われた暗号文を攻撃者が 2 回目の通信のときに差し替えてしまったケースで、別な情報が届いてしまいます。このような攻撃を防ぐために完全性検証が必要です。

23 完全性検証コードを付加して改ざん防止



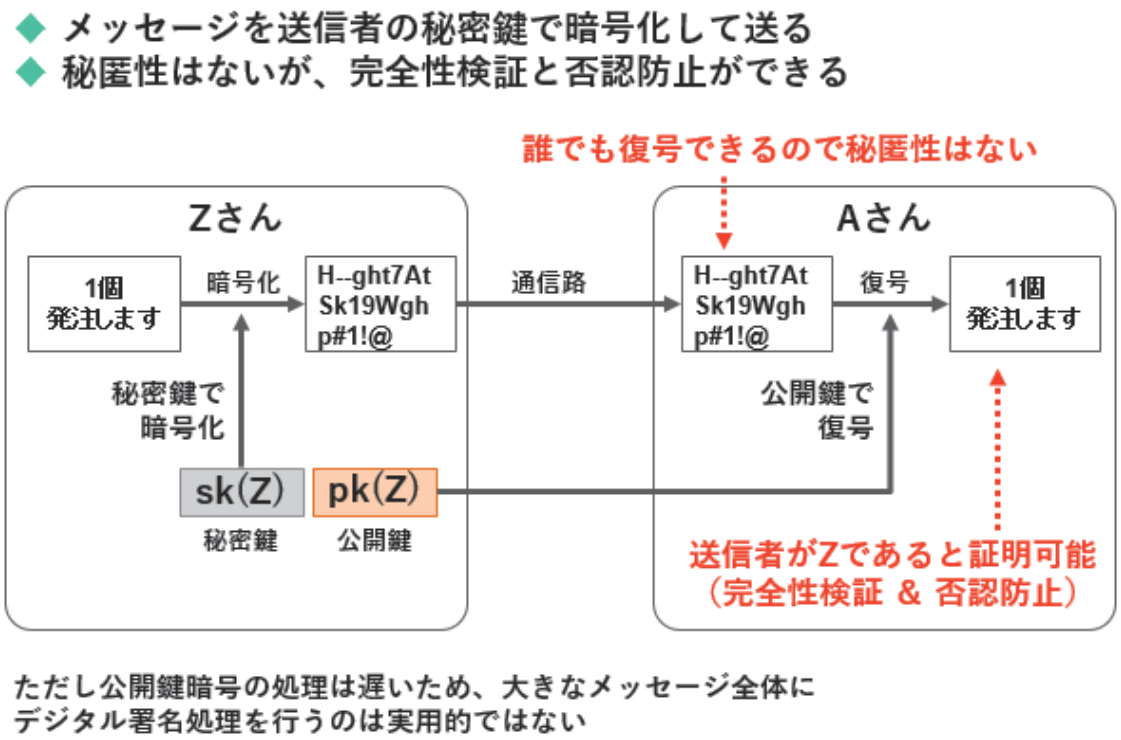
ハッシュ化=ダイジェスト化、ダイジェスト処理ともいう

完全性の検証にもハッシュ関数を利用します。メッセージをハッシュ化した値を付加して照合することで、完全性検証（改ざん検出）が可能です。

この目的で使われるハッシュ値をメッセージの完全性検証コード、Message Authentication Code（略称：MAC）と呼びます。

このようなメッセージのハッシュ化のことをダイジェスト化やダイジェスト処理とも呼びます。

24 デジタル署名により否認防止



否認防止のために使われる技術をデジタル署名と言い、公開鍵暗号を応用します。

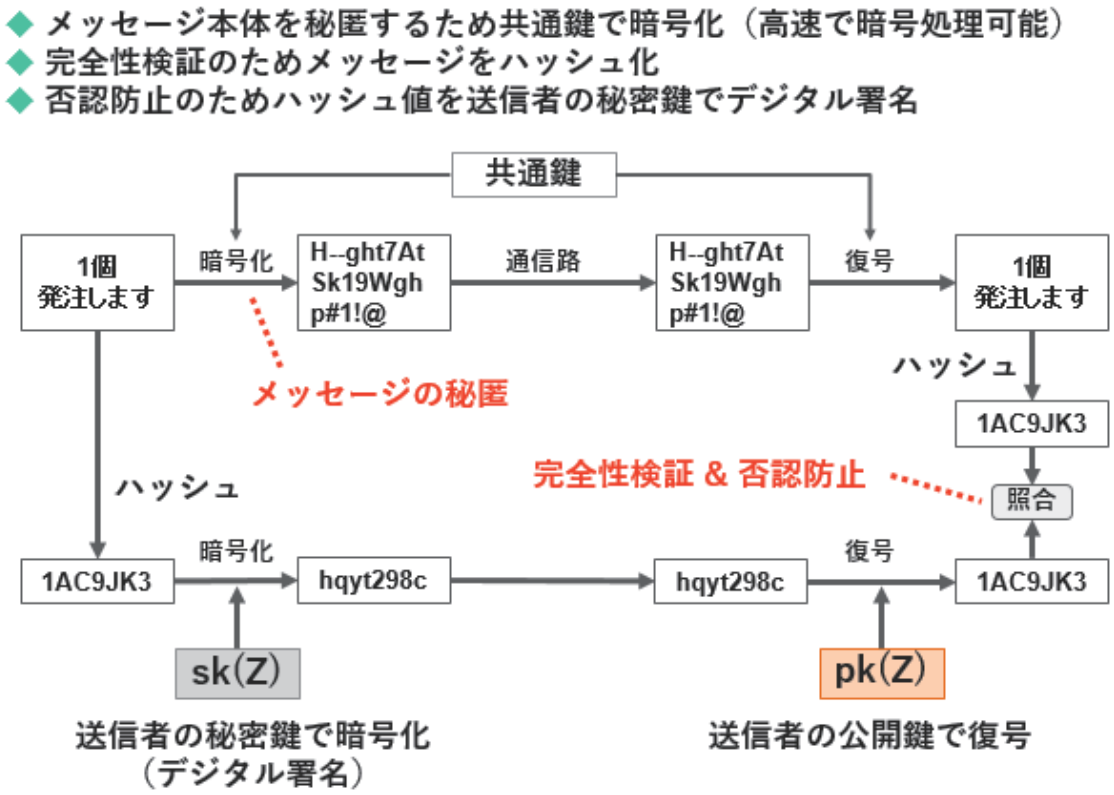
メッセージを秘匿するために公開鍵暗号を使う場合は「受信者の公開鍵で暗号化」しますが、デジタル署名では逆に「送信者の秘密鍵で暗号化」を行います。

具体的には、送信者 Z が自分の「秘密鍵」でメッセージを暗号化して受信者 A に送信します。この暗号文は送信者 Z の公開鍵で誰でも復号できるため、秘匿性はありません。しかし次のようなロジックで送信者が Z であることが証明されます。

1. 暗号文を Z の公開鍵で復号できた
2. つまりその暗号文は Z の秘密鍵で暗号化されたものである
3. それが可能なのは秘密鍵を持つ Z だけである
4. したがってこの暗号文は Z が作成したものである

これがデジタル署名で、この方法により完全性検証と否認防止が可能です。
ただし公開鍵暗号の処理は遅いため、大きなメッセージ全体にデジタル署名処理を行うのは実用的ではありません。

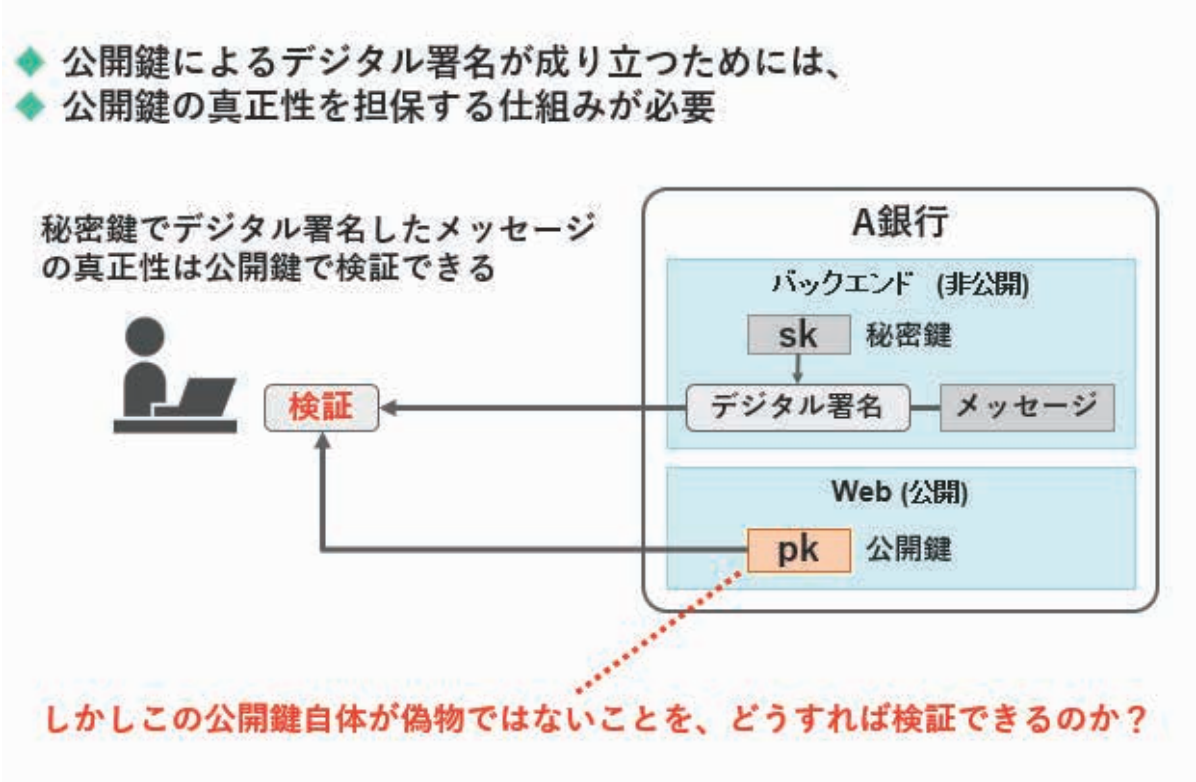
25 共通鍵・公開鍵・ハッシュを併用する



大きなメッセージの全体を秘匿しつつデジタル署名を行うためには、共通鍵暗号・公開鍵暗号・ハッシュを併用します。

具体的にはメッセージ本文は共通鍵で暗号化し、ハッシュ値にデジタル署名を行って送信します。これによってメッセージの秘匿・完全性検証・否認防止が同時に可能です。

26 公開鍵の真正性をどう担保する？

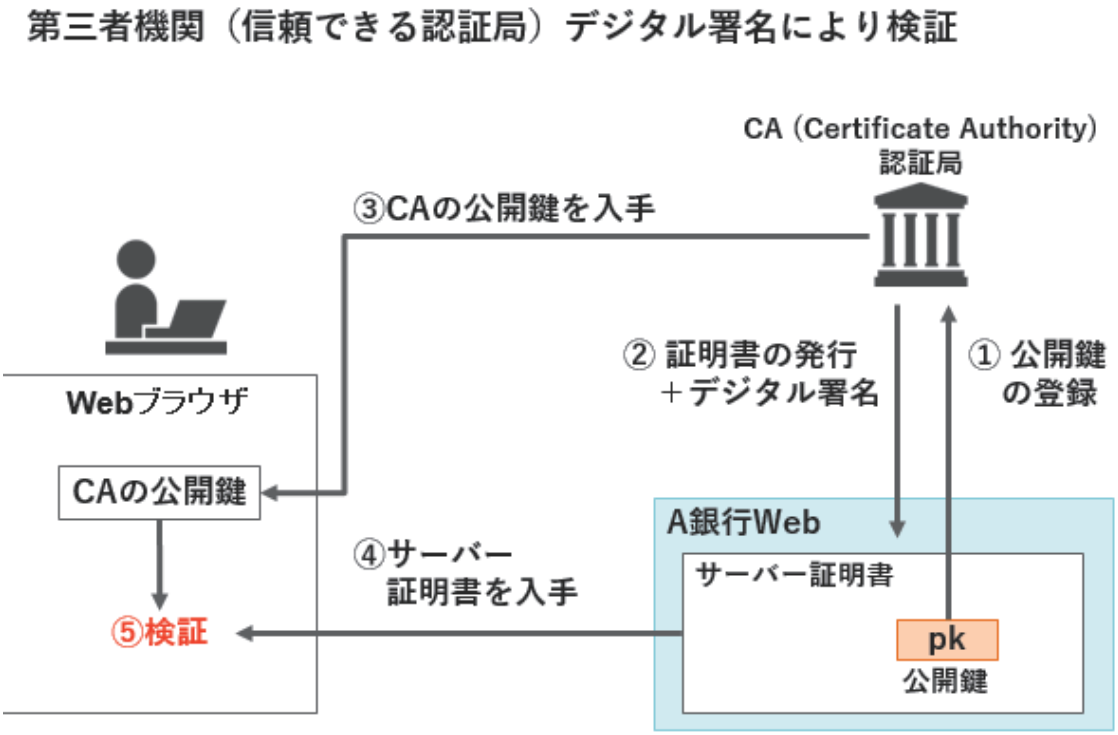


公開鍵暗号はデジタル署名にも応用できる便利な仕組みですが、これが成り立つためには公開鍵自体の真正性が保証されていなければなりません。

たとえばオンラインバンキング等で銀行の Web サイトにアクセスするような場合、正しい公開鍵がわかっていれば、銀行から送られてくるメッセージのデジタル署名を検証できます。しかし、その Web サイト自体が偽物であったら、公開鍵も偽物を用意しておくことでしょう。

銀行のリアルな店舗に出向けば間違いなく本物の公開鍵を入手できますが、それでは手間がかかりすぎて現実的ではありません。インターネット上で完結できる方法で公開鍵の真正性を担保する仕組みが必要です。

27 第三者認証により公開鍵の認証を得る



ここで役立つのが第三者認証です。図中の A 銀行は Web を開設するにあたり、Web サーバーの公開鍵を用意して「認証局(Certificate Authority, CA)」という機関に登録します。認証局はサーバー証明書にデジタル署名をして発行し、A 銀行はそのサーバー証明書を Web サーバーに設置します。

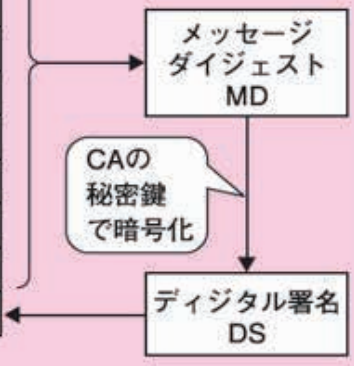
銀行の利用者が A 銀行 Web にアクセスするとき、Web ブラウザは A 銀行 Web のサーバー証明書をダウンロードして認証局の公開鍵によりそのデジタル署名を検証して「確かに認証局が発行した証明書に間違いない」ことを確認し、証明書の記載内容に照らして Web サーバーが本物であることを確認します。

このとき重要なのが「認証局の公開鍵」ですが、「信頼できる認証局」の公開鍵は一般の Web ブラウザにはあらかじめインストールされており（図中③）、ブラウザのメーカーの手によりその真正性が担保されています。

28 第三者認証：サーバー証明書の記載事項

サーバ証明書の記載事項

No	項　目	必須／任意
①	フォーマットのバージョン情報	必須
②	シリアル番号	必須
③	CAが⑪の署名に利用したアルゴリズム	必須
④	CAの名称	必須
⑤	証明書の有効期間	必須
⑥	主体者	必須
⑦	証明する公開鍵, 利用するアルゴリズム	必須
⑧	CAに付与されるID	任意
⑨	証明対象に付与されるID	任意
⑩	拡張領域	任意
⑪	CAのディジタル署名	必須

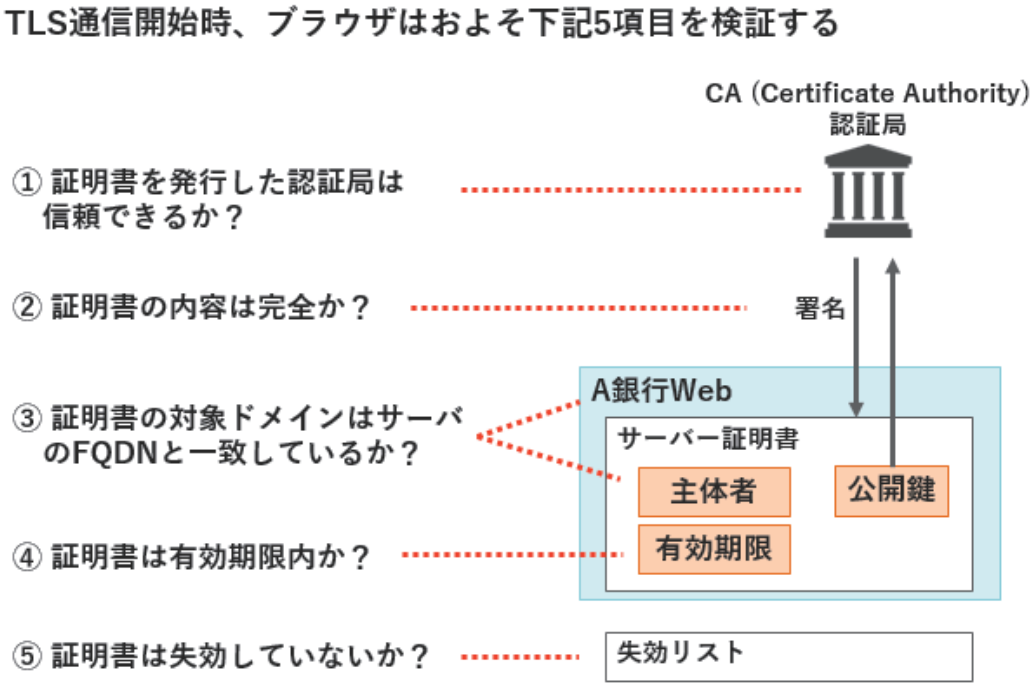


図：電子証明書の記載事項

サーバー証明書には、図中の①～⑪の情報が記載されています。①～⑩の範囲が証明される内容で、これをハッシュ化したもの（メッセージダイジェスト、MD）を CA の秘密鍵で暗号化したデジタル署名を⑪に記載します。

ブラウザはあらためて①～⑩からメッセージダイジェストを生成した上で、あらかじめ入手してある CA の公開鍵で⑪を復号して比較します。一致すれば証明書の記載内容が正しいことを確認できます。

29 TLS 通信開始時の検証ポイント



Web を閲覧する際の通信の通信暗号化方式を SSL と呼びますが、実際には現在は SSL を発展させた TLS という方式が使われています。SSL 通信または SSL/TLS 通信と表記されている場合も実際には TLS 通信のことを表しています。

TLS 通信を開始するとき、ブラウザは検証大まかに下記 5 項目を検証します。

①証明書を発行した認証局は信頼できるか？　→　あらかじめブラウザにインストールされている「信頼できる認証局の名前と公開鍵」を使って証明書内の CA の名前とデジタル署名を検証します。

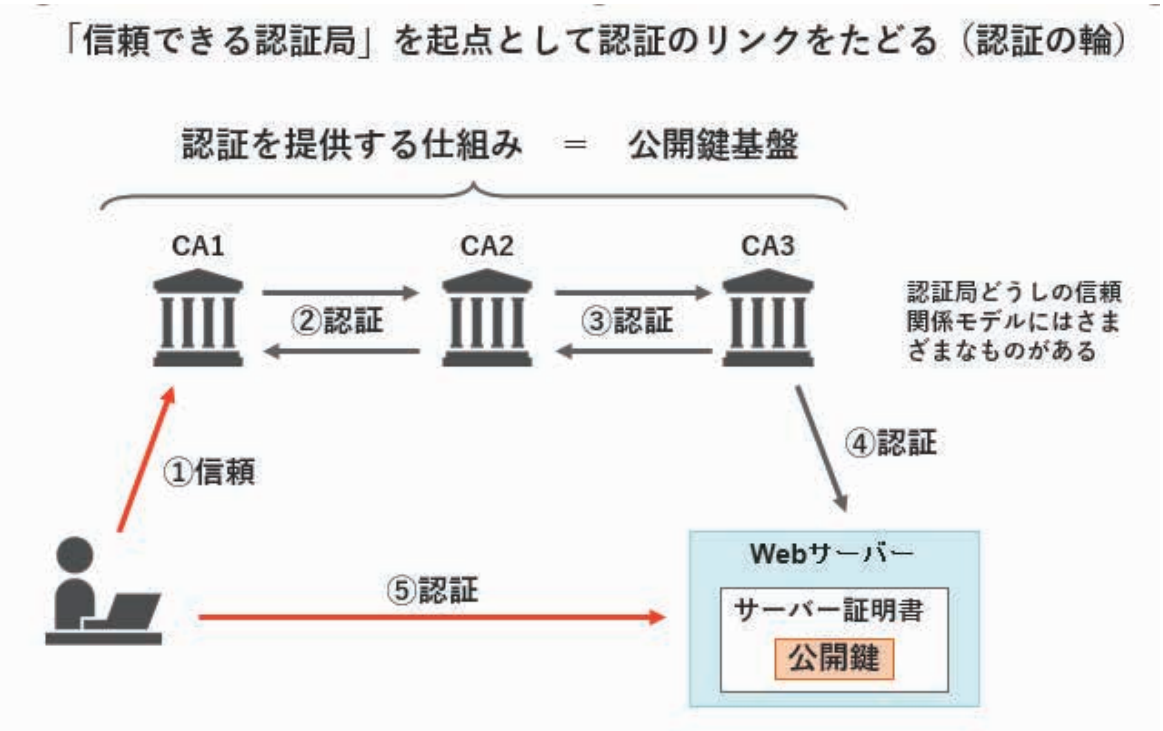
②証明書の内容は完全か？　→　証明書の内容とデジタル署名が一致していることを検証します。

③証明書の対象ドメインはサーバーの FQDN と一致しているか？　→　証明書の対象ドメインは証明書内の項目 6 番、「主体者」に書かれています。これとサーバーの FQDN（URL ホスト名）が一致することを検証します。

④証明書は有効期限内か？　→　証明書内の項目 5 番、「有効期限」内であることを検証します。

⑤証明書は失効していないか？　→　期限内であっても何らかの理由で証明書が失効とされる場合があるため、別途 CA から入手する失効リストに含まれていないことを検証します。

30 第三者認証：公開鍵基盤



公開鍵の認証を提供する「認証局」は多くの種類があります。

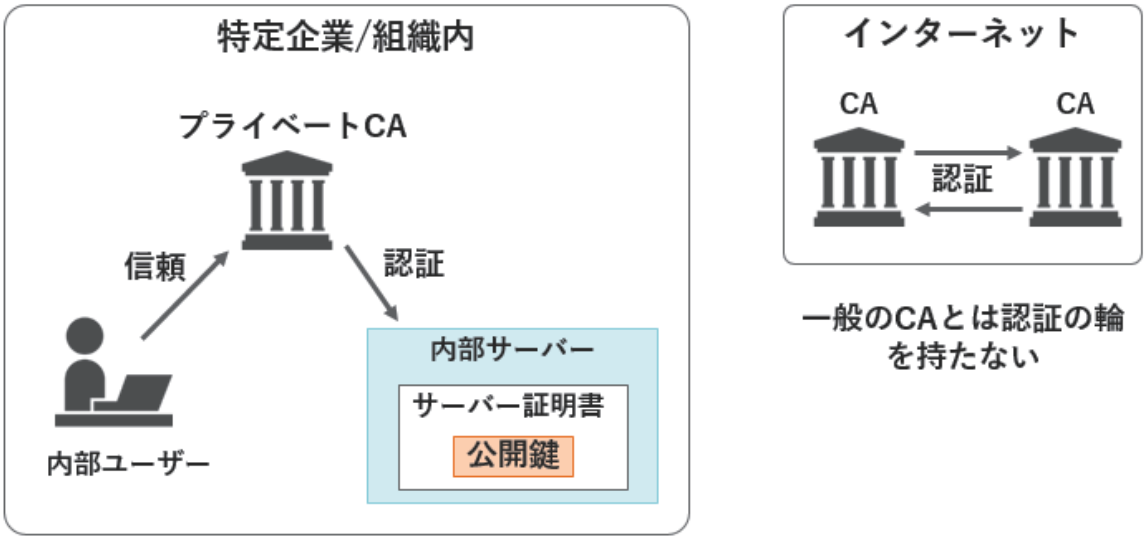
利用者が「信頼できる認証局」が CA1 なのに対して、アクセス先の Web サーバーを認証している（証明書の発行元である）認証局が CA3 だったとします。この場合でも認証局 CA1 と CA2 の間、CA2 と CA3 の間で相互認証が行われていれば、最終的に利用者はアクセス先の Web サーバーの認証を得ることができます。

このように、「信頼できる認証局」を起点としてリンクをたどることで複数の機関による認証を提供する仕組みを公開鍵基盤と言います。「認証局」どうしの相互認証のことを「認証の輪」とも言います。

認証局同士の信頼関係モデルには単独モデル、階層型モデル、Web モデルなどさまざまなものがあります。

31 第三者認証：プライベート CA

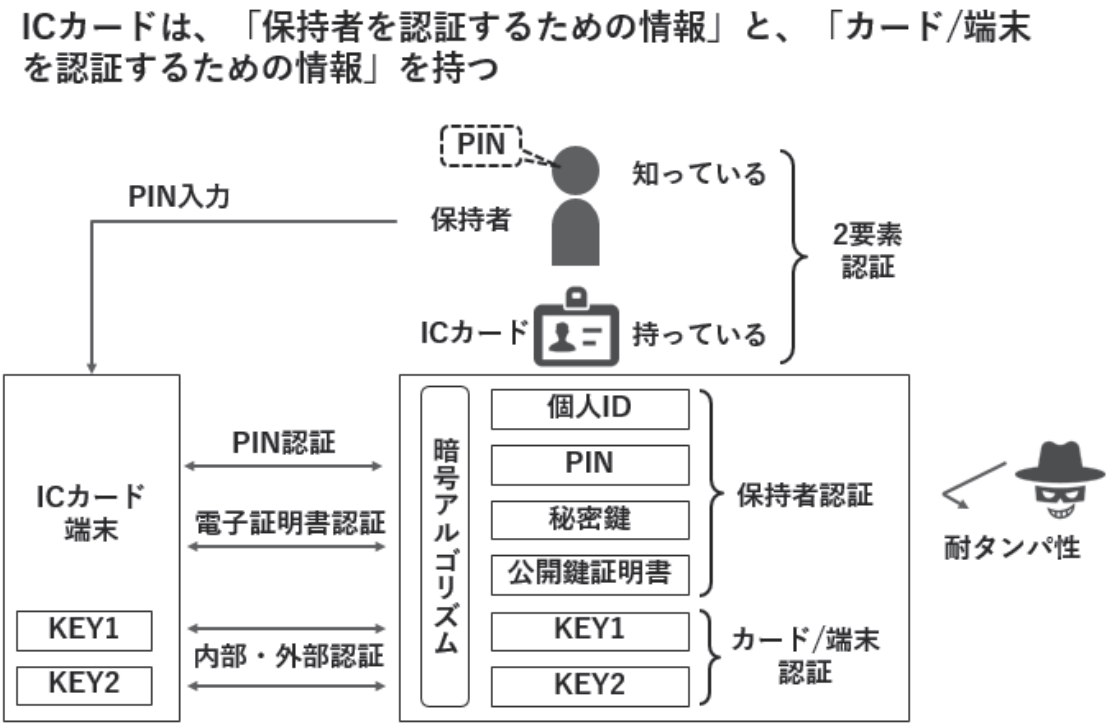
- 特定の企業/組織内でのみ運用するCAをプライベートCAと呼ぶ
- 証明書発行コストを抑えることができる



一般の認証局への登録には費用がかかるため、たとえば企業が社内でのみ使用するサーバーや PC の証明書発行に利用するのは現実的ではありません。このような場合、特定企業/組織内でのみ運用するプライベート CA を立てることで証明書発行コストを抑えることができます。

プライベート CA はインターネット上の一般の CA とは認証の輪を持ちません。

32 IC カードによる認証



個人の主体認証のためによく使われる仕組みの一つに IC カードがあり、企業の入館証、クレジットカードやキャッシュカードなどで応用されています。

IC カードは「保持者を認証するための情報」と「カードおよび端末を認証するための情報」を持っています。

IC カードやカード端末は偽造されることがあるため、カードを使用する場合、カードと端末が相互にお互いが「偽造されたものではない」ことを認証しなければなりません。端末が IC カードの正当性を認証することを内部認証と言い、IC カードが端末の正当性を認証する手順を外部認証と言います。このために IC カードと端末の双方に KEY1、KEY2 という 2 種類の同じ暗号鍵が記録されています。内部・外部認証は PIN の入力に先立って行われます。

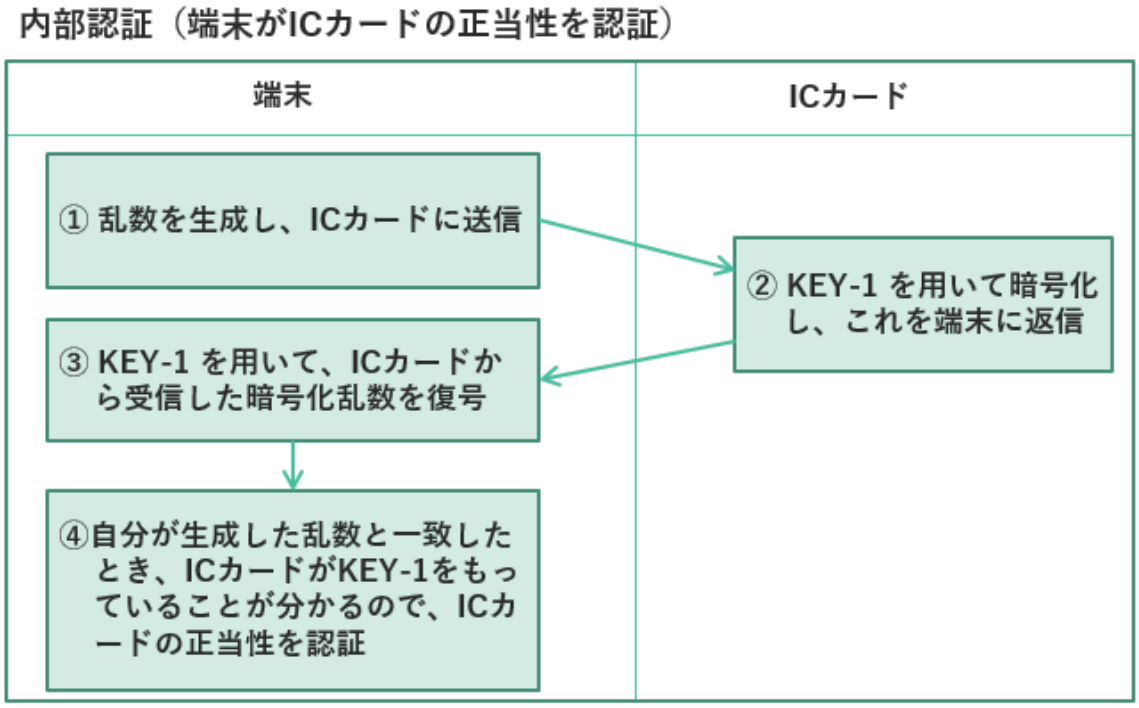
IC カードを主体認証のために利用する場合、PIN コードを併用することが多く、保持者がカードを端末に接続すると PIN コードの入力を求められ、端末に PIN を入力するとカードに記録されている PIN との照合を行って保持者を個人 ID にひもづけられた本人として認証します。この場合、IC カードを「持っていること」と PIN コードを「知っていること」の 2 つの情報を用いた 2 要素認証になります。

ＩＣカードの中には利用者の秘密鍵と公開鍵証明書を保存して、電子証明書を用いた利用者認証を行えるものもあります。

耐タンパ性とは、内部の情報を読み取られたり、改ざんされたりしないようにする仕組みです。

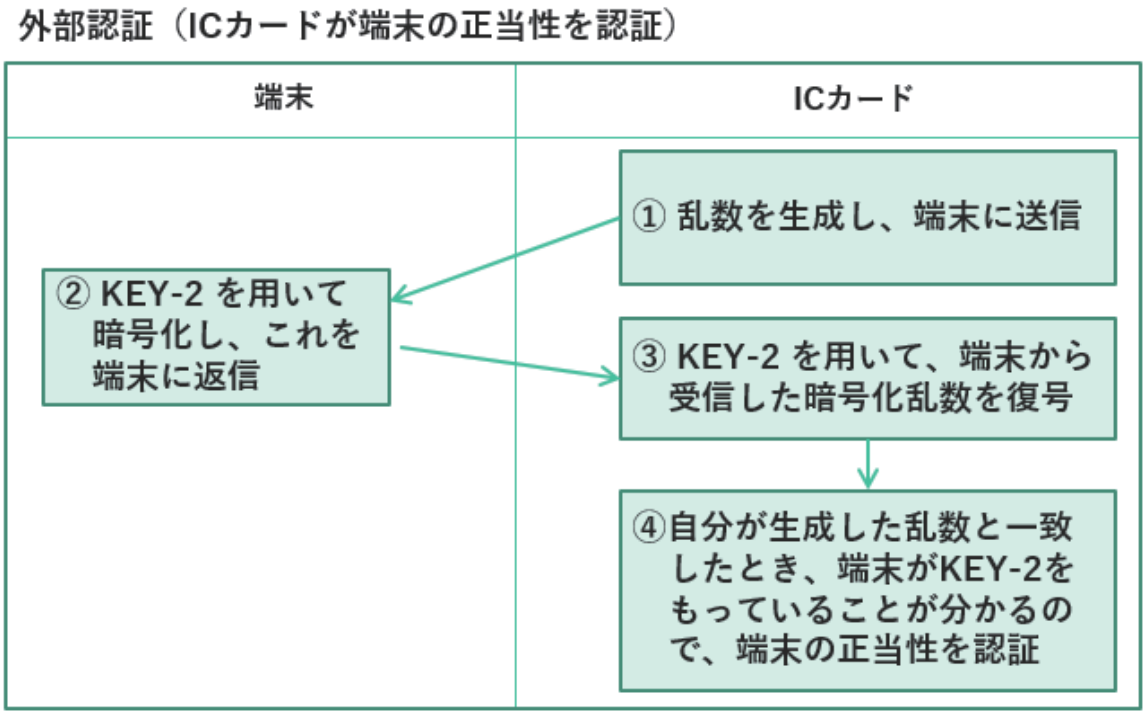
今日、利用者認証に用いられる IC カードの多くは、端末（カードリーダ）と接触せずに使用することができます。このような IC カードを非接触型といい、端末が発する電磁波を利用して発電した電力により内部の IC を動作させています。

33 内部認証の手順



内部認証では端末が乱数を生成して IC カードに送信し、カードは KEY1 を用いてその乱数を暗号化して端末に返信します。端末は KEY1 を用いて IC カードから受信した暗号化乱数を復号します。その結果自分が生成した乱数と一致したとき、IC カードが KEY-1 をもっていることが分かるので IC カードの正当性を認証できます。

34 外部認証の手順



外部認証では逆に IC カードが乱数を生成して端末に送信し、端末は KEY2 を用いてその乱数を暗号化してカードに返信します。カードは KEY2 を用いて端末から受信した暗号化乱数を復号します。その結果自分が生成した乱数と一致したとき、端末が KEY2 をもっていることが分かるので端末の正当性を認証できます。

35 耐タンパ性

- 内部の情報を読み取られたり、改ざんされたりしない仕組み
- 論理的耐タンパ性
  - データの暗号化による難読化
- 物理的耐タンパ性
  - ICカードをこじ開けようとすると物理的に回路を破壊する
  - 光に当たるとメモリの内容を消去する

耐タンパ性には、論理的な耐タンパ性、物理的な耐タンパ性の 2 種類があります。

論理的な耐タンパ性は、データの暗号化による難読化です。

物理的な耐タンパ性には、例えば IC カードをこじ開けようとすると物理的に回路を破壊するものや、光に当たるとメモリの内容を消去するものがあります。

本章では認証・認可・アカウンティング（＝AAA）に関わるセキュリティプロトコルを扱いますが、細部の話に入る前に、それらがおおまかにどのような用途に使われるものなのかの概要をつかんでおきましょう。

例として、社内 LAN を従業員が利用する場面を考えてください。図の「ネットワーク」は社内 LAN、「サービス１，２，３」はそのネットワーク上で提供されているサービスです。ファイルサーバーや社内ポータル、メールサーバーなどが代表的です。「User A、B」は従業員で、それぞれ端末 A、B で「AP」を通してネットワークに接続します。AP は無線 LAN アクセスポイントのイメージですが、実際には有線のハブやスイッチ、ルータの場合もあります。

以上の構図の中で「User によるネットワーク利用」をコントロールするためには、①識別、②認証、③認可、④アカウンティングという 4 つの機能が必要になります。

①識別とは、User や端末の個体を特定する機能です。通常、個人識別のためにはなんらかの ID を使用します。端末の識別には MAC アドレスが使われます。
②認証とは、識別した個体の真正性（本物であること）を確認する機能です。個人の認証にはパスワードや指紋、ID カード等が使われることが多く、端末の認証にはクライアント証明書や MAC アドレスが使われます。ただし MAC アドレスは容易に偽装できるため、厳密な意味の識別・認証には使用できません。
③認可とは、認証した相手（User や端末）に対して特定のサービスの利用を許可することを言います。User の権限に応じて、アクセス可能な情報の範囲を変えるために必要な機能です。
④アカウンティングとは、利用状況を記録する機能です。ネットワークへの接続開始時刻・切断時刻、サービス毎の利用開始時刻・終了時刻、データ量など、サービスに応じてさまざまなデータを記録します。設備計画の立案や勤務状況の把握、異常な利用状況の検出と対応、情報漏洩インシデントの調査などに必要です。

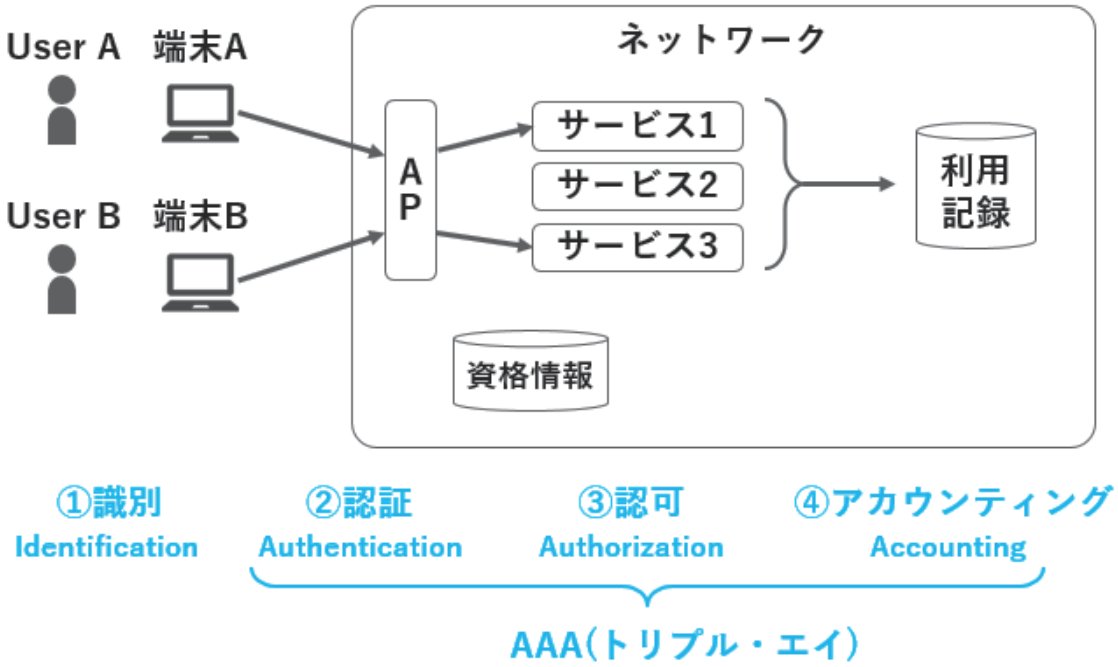
これら 4 つの機能のうち、②認証(Authentication)、③認可(Authorization)、④アカウンティング(Accounting)の 3 つがいずれも A で始まることから、総称して AAA（トリプル・エイ）機能とも呼ばれます。

認証・認可・アカウンティング　＝　AAA（トリプル・エイ）

AAA 機能に必要なユーザーID、パスワード、権限種別などの情報を総称して「資格情報」と言います。資格情報はサービスごとに個別管理される場合もありますが、企業単位で一元化することが望ましいものです。

これらの機能はいくつかのセキュリティプロトコルの連携によって成り立ちます。詳細は後述しますので、本節では全体のイメージをつかんでおいてください。

36 識別・認証・認可・アカウンティング



本章では認証・認可・アカウンティング（＝AAA）に関わるセキュリティプロトコルを扱いますが、細部の話に入る前に、それらがおおまかにどのような用途に使われるものなのかの概要をつかんでおきましょう。

例として、社内 LAN を従業員が利用する場面を考えてください。図の「ネットワーク」は社内 LAN、「サービス１，２，３」はそのネットワーク上で提供されているサービスです。ファイルサーバーや社内ポータル、メールサーバーなどが代表的です。「User A、B」は従業員で、それぞれ端末 A、B で「AP」を通してネットワークに接続します。AP は無線 LAN アクセスポイントのイメージですが、実際には有線のハブやスイッチ、ルータの場合もあります。

以上の構図の中で「User によるネットワーク利用」をコントロールするためには、①識別、②認証、③認可、④アカウンティングという 4 つの機能が必要になります。

①識別とは、User や端末の個体を特定する機能です。通常、個人識別のためにはなんらかの ID を使用します。端末の識別には MAC アドレスが使われます。
②認証とは、識別した個体の真正性（本物であること）を確認する機能です。個人の認証にはパスワードや指紋、ID カード等が使われることが多く、端末の認証にはクライアント証明書や MAC アドレスが使われます。ただし MAC アドレスは容易に偽装できるため、厳密な意味の識別・認証には使用できません。

③認可とは、認証した相手（User や端末）に対して特定のサービスの利用を許可することを言います。User の権限に応じて、アクセス可能な情報の範囲を変えるために必要な機能です。
④アカウンティングとは、利用状況を記録する機能です。ネットワークへの接続開始時刻・切断時刻、サービス毎の利用開始時刻・終了時刻、データ量など、サービスに応じてさまざまなデータを記録します。設備計画の立案や勤務状況の把握、異常な利用状況の検出と対応、情報漏洩インシデントの調査などに必要です。

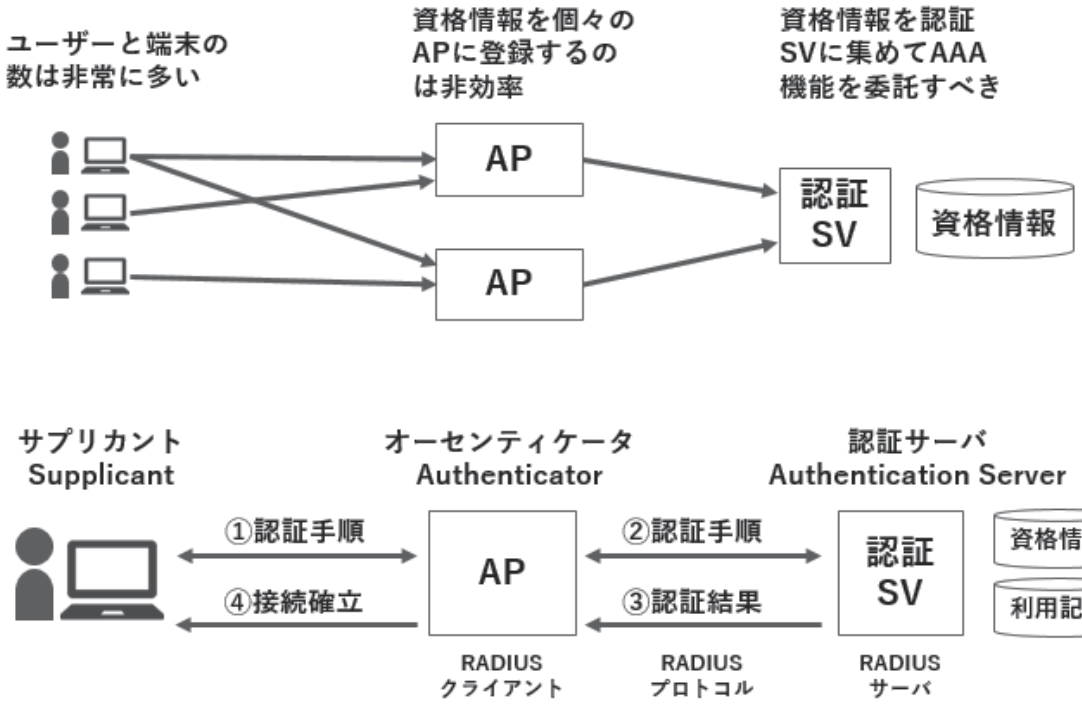
これら 4 つの機能のうち、②認証(Authentication)、③認可(Authorization)、④アカウンティング(Accounting)の 3 つがいずれも A で始まることから、総称して AAA（トリプル・エイ）機能とも呼ばれます。

認証・認可・アカウンティング　＝　AAA（トリプル・エイ）

AAA 機能に必要なユーザーID、パスワード、権限種別などの情報を総称して「資格情報」と言います。資格情報はサービスごとに個別管理される場合もありますが、企業単位で一元化することが望ましいものです。

これらの機能はいくつかのセキュリティプロトコルの連携によって成り立ちます。詳細は後述しますので、本節では全体のイメージをつかんでおいてください。

37 認証のための資格情報は集中管理したい



認証プロトコルについて考える時にまず知っておかなければならないのは、「認証のための資格情報は集中管理すべきである」ということです。

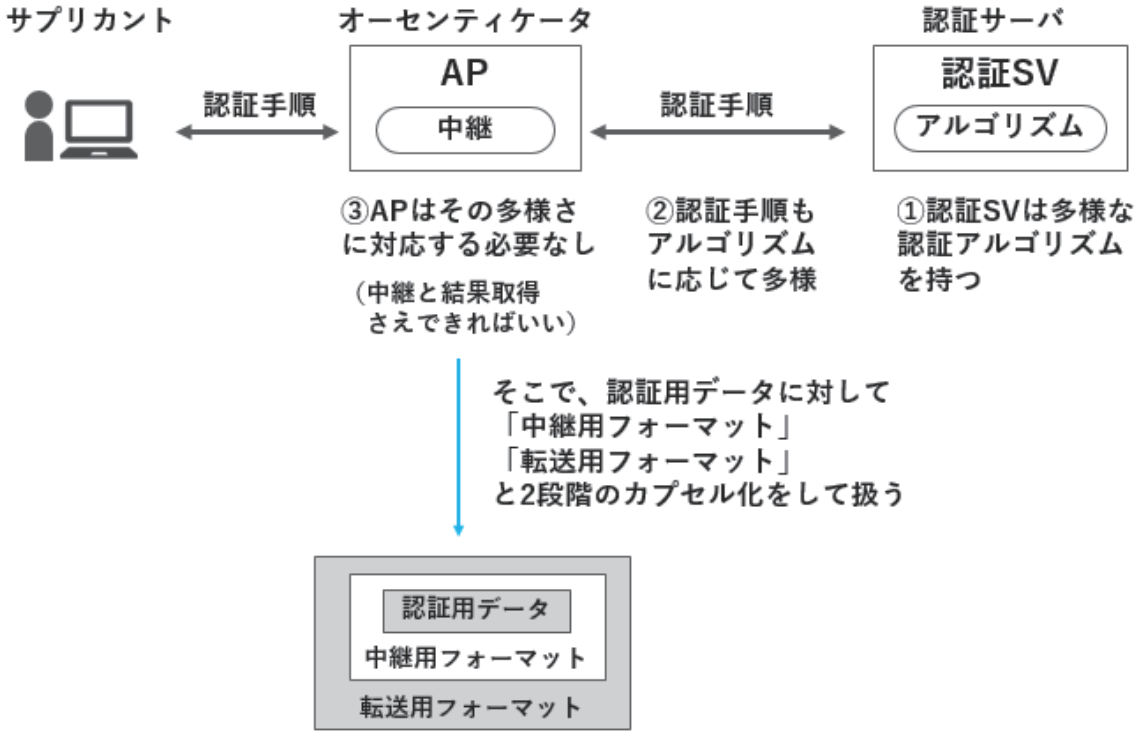
無線 LAN による社内 LAN への接続をコントロールするためにユーザーと端末を認証する場面を例に取ります。一般に、ユーザーと端末の数は非常に多く（数百〜数千クラスは普通、大企業では数十万人に達することもある)、端末が接続する AP（アクセスポイント）も多ければ数万基のオーダーで存在します。ユーザーは移動するため、同じユーザーでも場合によって違う AP に接続を試みます。仮に個々の AP にユーザーと端末の資格情報(ID、パスワード等)を登録していると、1 人でも情報に変更がある度にすべての AP にその変更を反映させなければなりません。これは極めて非効率ですので、資格情報は 1 箇所に集めて「認証 SV(認証サーバー)」として認証機能を持たせ、個々の AP から認証 SV に対して認証機能を委託するのが合理的です。

このように「資格情報を 1 箇所に集めて認証を行う」という仕組みを「サプリカント／オーセンティケータ／認証サーバー」モデルと言います。サプリカントはユーザーや端末のことを指し、オーセンティケータはサプリカントからの認証要求を直接受け付ける装置で、AP や一般のサーバーに該当します。
大まかな処理の流れとしては①サプリカントがオーセンティケータに認証要求を出して認証手順を開始する。②オーセンティケータはサプリカントと認証 SV の間で認証手順を中継する。③認証 SV

がオーセンティケータとサプリカントに認証結果を通知する。④認証成功の場合はオーセンティケータがサプリカントとの接続を確立する、という流れです。

ここでいう認証 SV 機能を担うのが RADIUS サーバーで、RADIUS サーバーに対応するオーセンティケータ機能を持つ装置を RADIUS クライアントと言います。RADIUS サーバーとクライアントの間で使われるプロトコルが RADIUS プロトコルです。RADIUS は認証・認可・アカウンティングの AAA 機能の標準となっています。

38 認証手順の多様性にどう対応する？



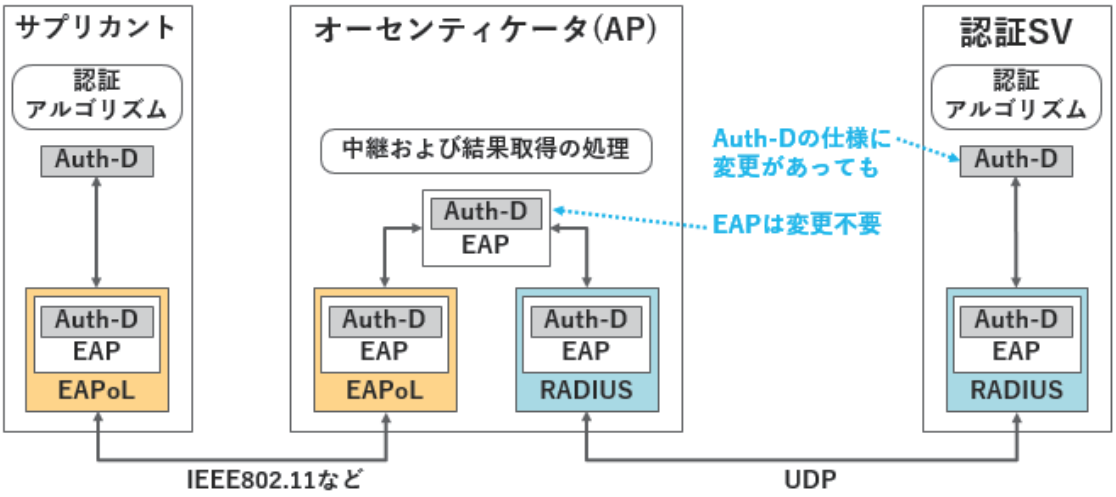
企業や自治体のような組織には、誰にでも見せられる情報から極めて機密性の高い情報まで、多様なセキュリティレベルの情報やサービスが混在します。そこで、①認証 SV は多様な認証アルゴリズムを持っており、これに応じて②認証手順も多様なものになります。

しかし、③オーセンティケータはその多様さに対応する必要がありません。これは、認証を受けるのはサプリカントであってオーセンティケータ自身ではないからです。オーセンティケータは認証手順の中継と結果取得さえできればよく、自身が複雑な認証手順を解釈する必要はありません。

そこで、認証用データ（認証するためにサプリカントと認証サーバーの間でやりとりされる資格情報）を通信する際は「中継用フォーマット」をかぶせてさらに「転送用フォーマット」をかぶせるという 2 段階のカプセル化をします。

39 認証用データのカプセル化

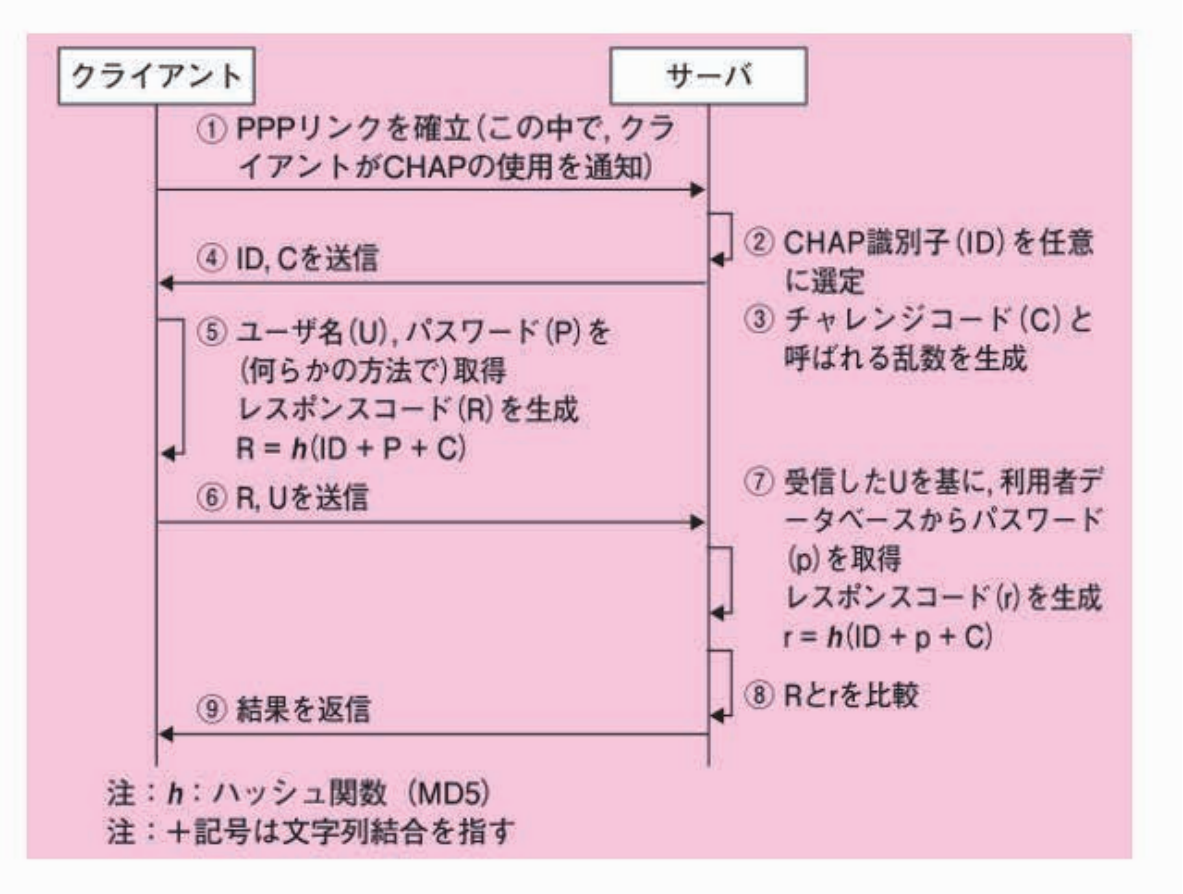
Auth-D ：認証用データ（認証アルゴリズムに応じて異なる）
EAP　　：中継用フォーマット。オーセンティケータが処理する
RADIUS：EAPを認証SV～AP間で転送する際に使うフォーマット
EAPoL ：EAPをサプリカント～AP間で転送する際に使うフォーマット



図中の Auth-D は認証用データ（資格情報を含んでいる）を表します。Auth-D はサプリカントと認証 SV の間で交換されるもので、オーセンティケータは Auth-D を解釈しません。
Auth-D は EAP の中にカプセル化して運ばれます。オーセンティケータは EAP を読んで処理を行います。Auth-D の仕様が変わっても EAP は変更不要のため、オーセンティケータの処理がシンプルになります。

EAP を機器間で転送する場合は、サプリカント~オーセンティケータ間は EAPoL フォーマットで、オーセンティケータ~認証 SV 間は RADIUS フォーマットでカプセル化して転送します。これはそれぞれの下層で使えるプロトコルが違うためです。無線 LAN-AP への接続認証のケースでいうと、サプリカント（PC 端末）がオーセンティケータ(AP)に接続を求めてきた段階では、端末～AP 間はまだ IP 接続が確立していません。そこで、この段階でも使える IEEE802.11 上に EAP を載せるための EAPoL フォーマットを使います。一方、AP～認証 SV 間は UDP/IP が使えるため、その上で動く RADIUS フォーマットの中に EAP を載せて転送します。

40 CHAP

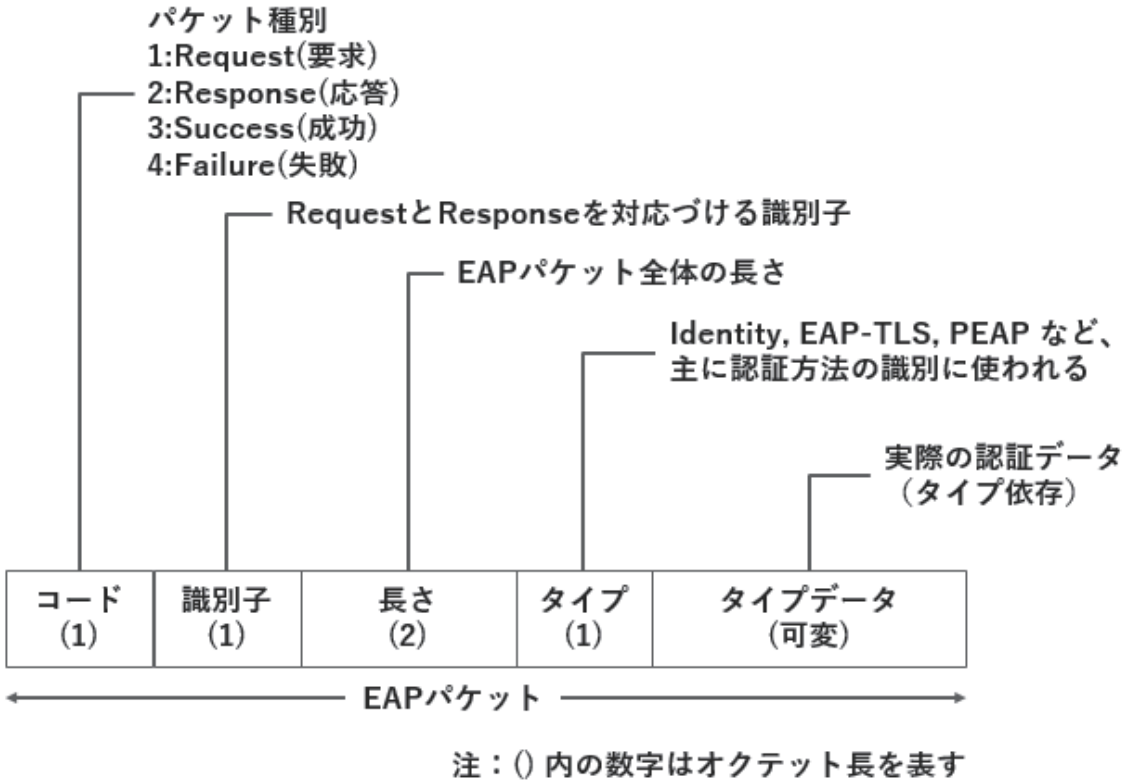


CHAP(Challenge Handshake Authentication Protocol)はワンタイムパスワード方式で認証を行うプロトコルで、PPP などにおけるユーザー認証方式として使われています。

CHAP では，PPP のリンク確立後に，一定の周期でチャレンジメッセージを送り，それに対して相手がハッシュ関数による計算で得た値を返信します。このようなユーザー認証方式をチャレンジ／レスポンス方式と呼びます。

クライアントが管理しているパスワード「P」と，サーバーが管理しているパスワード「p」が同じものであれば，ハッシュ関数「h」の演算結果「R」と「r」は一致します。チャレンジコード「C」は乱数なので，レスポンスコード「R」は毎回異なります。回線を伝達する情報が毎回異なっているので，ワンタイムパスワードを実現できます。また，「R」はハッシュ値なので，仮に盗聴されても「P」
を推定することはほぼ不可能です。

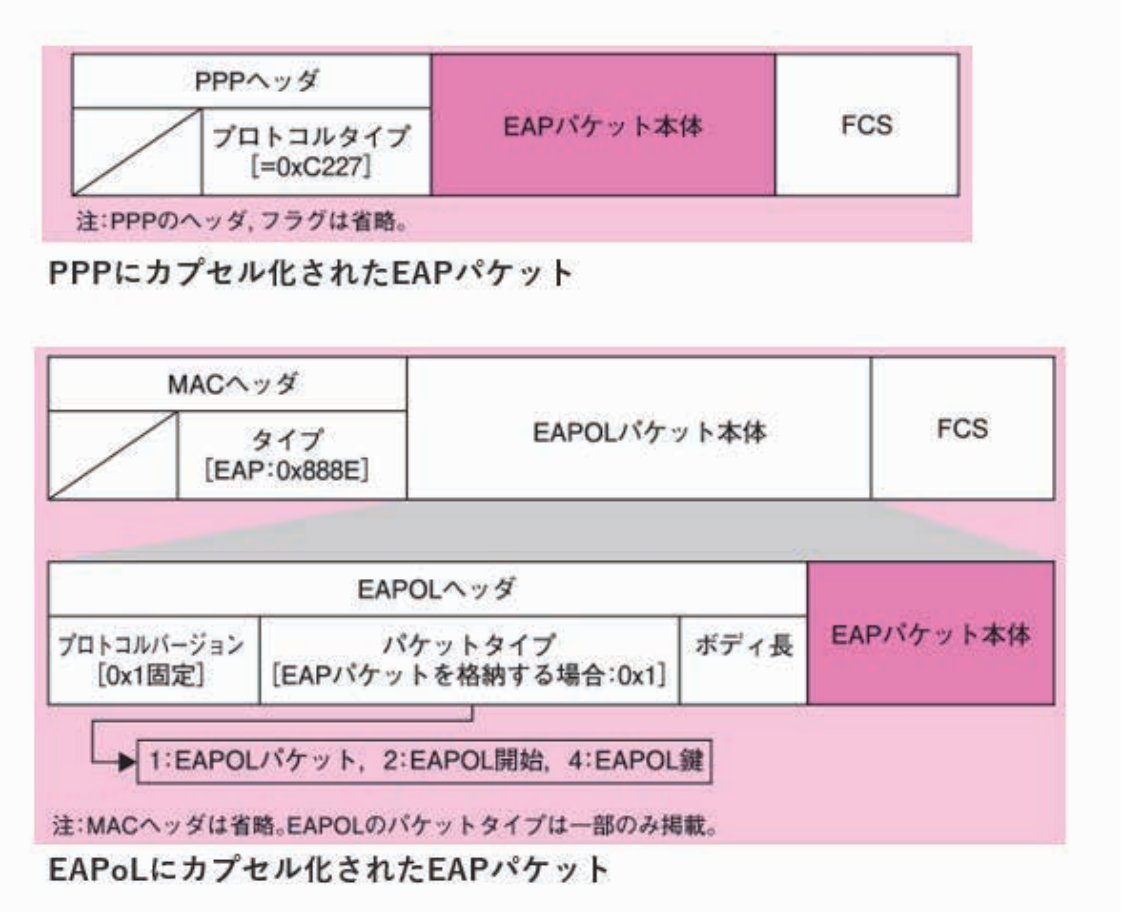
41 EAP パケット・フォーマット



EAP（Extensible Authentication Protocol）は，様々な認証方式をカプセル化する仕組みをもち，PPP，IEEE802.1X（EAPover LAN）など，様々なプロトコルで使用することができます。
サポートされている認証方式には，TLS（Transport Layer Security），PEAP などがあります。EAP でやり取りするパケットの種別は，要求（Request），応答（Response），認証成功，認証失敗の 4 種類です。このうち，Request，Response には，認証方式などを指定する「タイプ」領域と，指定された認証方式のデータを格納する「タイプデータ」領域があります。

認証に先立ち，サーバーはクライアントに対し，ユーザー ID の送信を要求します。クライアントがこれに応答する際にも EAP パケットが用いられます。それぞれアイデンティティ要求／アイデンティティ応答と呼び，「タイプ」領域には「アイデンティティ」が指定され，「タイプデータ」領域にユーザー ID が格納されます。

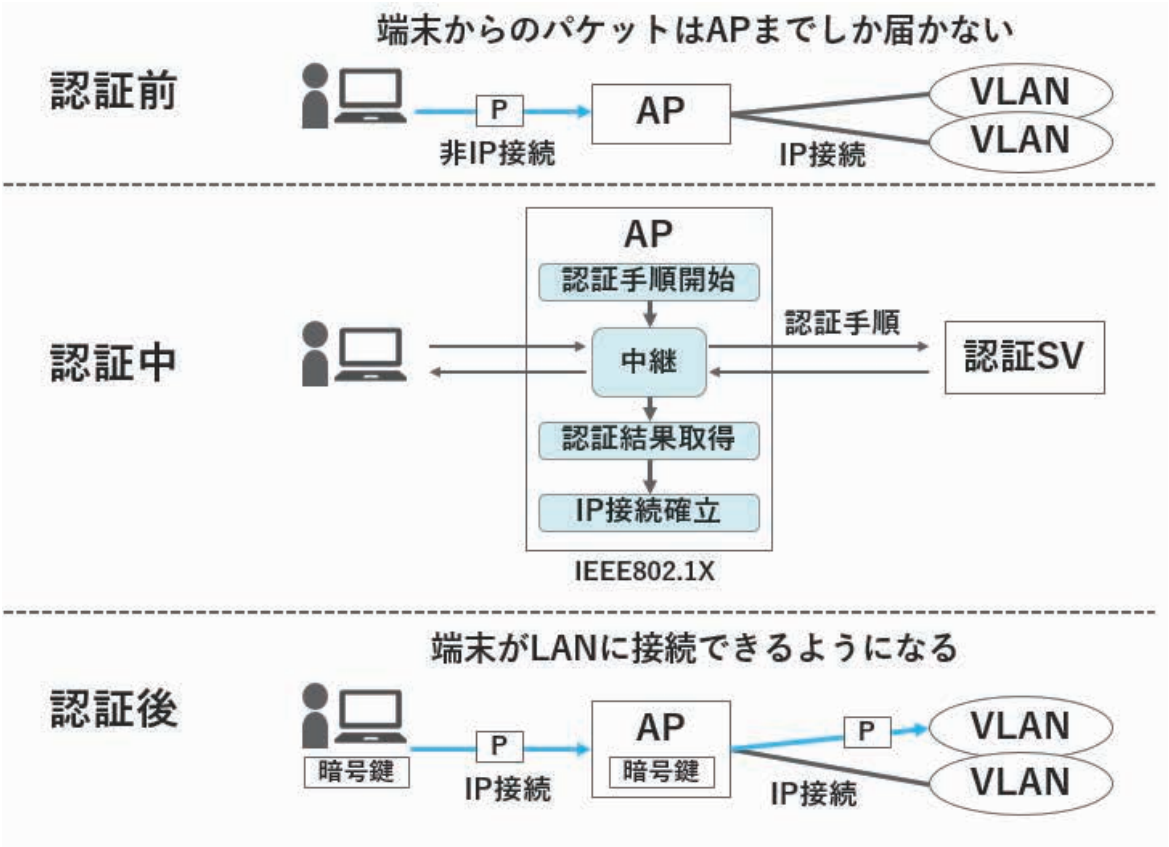
42 EAP パケットのカプセル化



PPP にカプセル化する場合は，プロトコルタイプ領域で EAP（0xC227）を指定し，PPP データに EAP パケット本体を格納します。

IEEE802.1X では，EAP over LAN（以下,「EAPOL」と称する）というフレームフォーマットに EAP フレームをカプセル化します。MAC フレームのタイプ領域で EAP を指定し，MAC フレームのデータ部分に EAPOL フレームを格納します。さらに，EAPOL フレームのデータ部分に EAP フレームを格納します。

43 IEEE802.1X の役割



IEEE802.1X は、認証に成功した端末だけが VLAN や無線 LAN に接続できるようにする技術です。

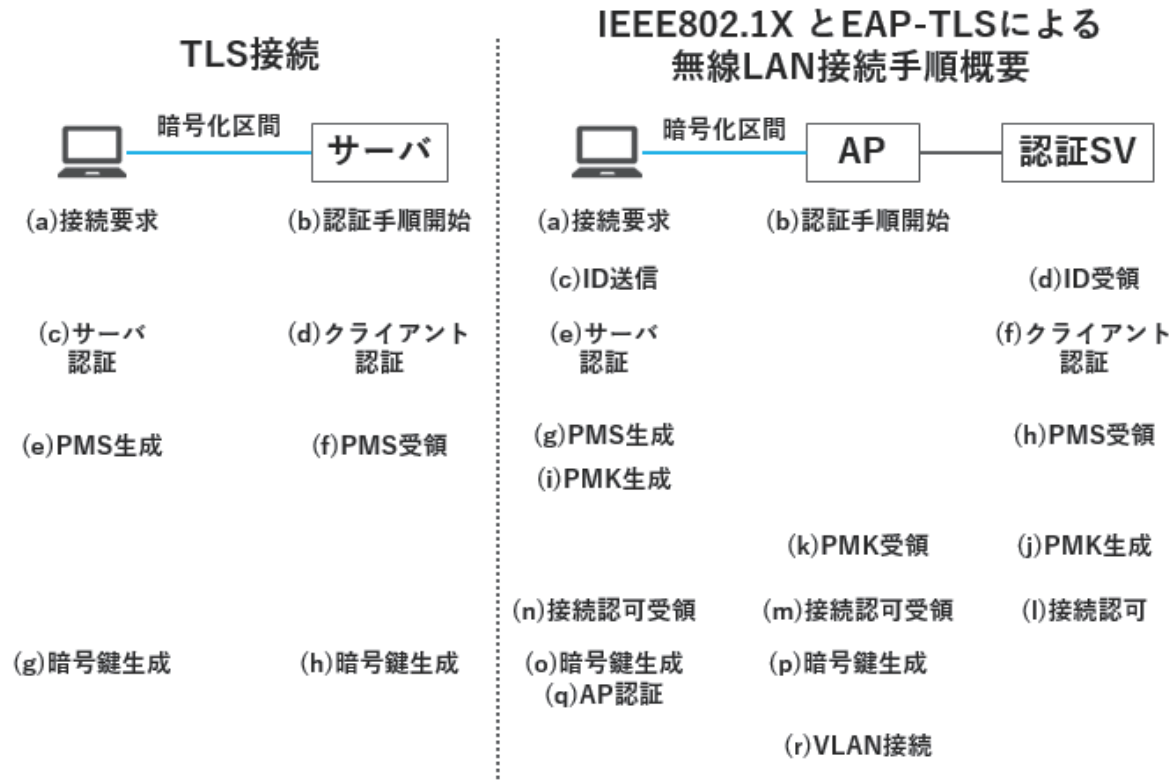
大まかな動作イメージは上図のようになります。「AP」は無線 LAN アクセスポイントまたは VLAN のスイッチです。認証前の端末からのパケットは AP までしか届かず、背後の LAN には接続できません。

認証後は端末～AP 間で IP 接続が確立し、その端末に割り当てられた VLAN に接続できるようになります。無線 LAN の場合は AP と端末に共通の暗号鍵が配布されて無線区間は暗号化されます。

認証自体は認証 SV が行い、AP は「認証手順開始」「中継」「認証結果取得」「IP 接続確立」という処理を行います。

IEEE802.1X はこれらの枠組みを定めています。

44 TLS 接続手順と EAP-TLS 接続手順の比較



IEEE802.1X で認証を行う方法のうち、高いセキュリティが求められる場合に使われるのが EAP-TLS 認証で、これは暗号化通信の TLS 接続の手順を IEEE802.1X に応用したものです。TLS 接続と EAP-TLS を比較して共通点と相違点を理解しましょう。

図の左側は TLS 接続で、これは端末～サーバーの 2 者間に暗号通信を確立するための手順です。右側は EAP-TLS で、端末～AP～認証 SV という 3 者間で認証と暗号通信を確立する手順です。いずれも、プロトコルの詳細ではなくポイントになる部分のみ記載しています。

TLS 接続は 2 者間ですので話が単純で、「お互いを相互に認証し、暗号鍵の元を作って送る」だけの手順です。一方、EAP-TLS は 3 者間で役割を分担するため複雑になります。以下、1 つずつ確認します。なお、図中(a)～(r)の記号は必ずしも時間軸を反映したものではありません。

(a)接続要求に対して(b)認証手順を開始するのは AP の役割ですが、それに応じて端末が(c)ID 送信をすると、その(d)ID を受領するのは認証 SV です。
次の(e)サーバー認証、(f)クライアント認証、(g)PMS 生成、(h)PMS 受領、と続きます。PMS(プリマスタシークレット、Pre Master Secret)は暗号鍵生成に使われるタネとなる乱数です。ここまでは TLS 接続の手順とほぼ同じですが、その後が異なります。

暗号化区間の違いに注意

PMS は通信の暗号鍵を生成するための基になる乱数です。TLS では(f)で PMS を端末とサーバーの両者が共有します。暗号化区間もその両者に一致するため、そのまま両者で(g)(h)暗号鍵生成をすれば暗号通信が可能です。

一方、EAP-TLS では(h)で PMS を受領した認証 SV ではなく、AP が暗号化区間の端になるため、このままでは暗号化ができません。そこで、認証 SV で(j)PMK を生成してそれを AP に送信します。PMK とは Pre Master Key の略で、これも最終的に暗号鍵を作るための途中段階のひとつです。
端末側でも同じ(i)PMK を生成しているため、AP が認証 SV から(k)PMK を受領したとき、この両者は一致します。

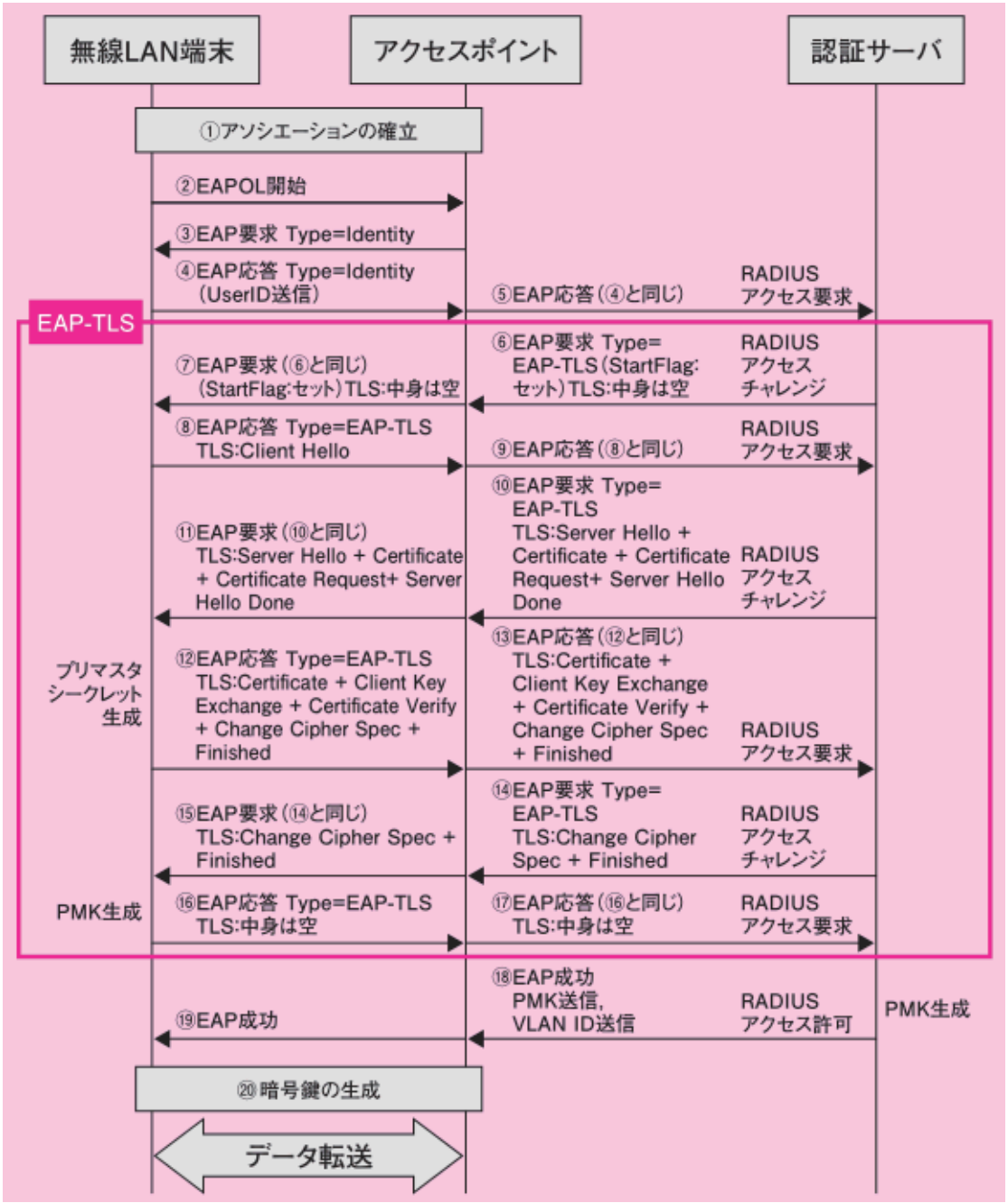
接続認可情報の伝達

(f)認証を終えると認証 SV は(l)端末の接続を認可します。この情報は(m)(n)AP と端末の両者が受領します。その後 AP は PMK を元に(p)暗号鍵を生成します。端末でも同様に PMK を元に(o)暗号鍵を生成し、さらに(q)AP を認証して通信を開始します。一方、AP は接続認可情報に含まれる VLAN 割当指示に従って、(r)端末を所定の VLAN に接続します。

AP 認証の必要性と方法

(e)と(f)で端末と認証 SV は相互に認証を行っていますが、端末にとって AP は認証されていません。無線 LAN の場合、有線 LAN と違って偽の AP に接続してしまう可能性があるため、端末側から AP を認証する必要があります。そこで、AP を認証するために PMK を使います。PMK はもともと、端末から認証 SV に送った PMS を元に認証 SV が生成して AP に送ったものです。ということは、端末と AP が同じ PMK を持っていれば、その AP は認証 SV から正しく PMK を受領した正規の AP であることが確認できます。このような方法で (q)AP 認証を行います。

では実際のプロトコル上でどのようなシーケンスで認証が行われているかを確かめましょう。



無線 LAN での IEEE802.1X を使った認証シーケンスは上図の①～⑳の流れで行われます。１回のパケットに複数の情報を載せて送ります。図中の太枠で囲んだ部分が TLS 手順をもとにした EAP-TLS と呼ばれる仕組みです。

最初に、①無線 LAN 端末と AP（アクセスポイント）間でアソシエーションが確立されて通信が可能になります。しかしこの段階では認証が行われていないため、無線 LAN 端末は AP を超えてデータを転送することはできません。

次に端末が②EAPoL 開始パケットを送ります。これが(a)接続要求に該当し、次の③EAP 要求が(b)認証手順開始に該当します。③EAP 要求パケットは AP から送られますが、以後の EAP パケットは基本的に端末〜認証 SV 間で交換されます。

③は Type=Identity で ID を要求するので、端末はその応答で④UserID を送信します。これを AP は⑤RADIUS アクセス要求として認証 SV に中継します。以後、AP〜認証 SV 間の通信は基本的に EAP パケットを RADIUS パケットの中にカプセル化して行われます。
⑥で認証 SV が EAP-TLS による認証シーケンスを開始し、AP がそれを⑦端末に中継します。

⑧⑨で端末から認証 SV へ送られる Client Hello と、⑩⑪で認証 SV から端末に送られる Server Hello + Certificate + Certificate Request + Server Hello Done は 2 点間で TLS 接続を開始する手順と同じです。これに対する応答⑫⑬も TLS 接続手順と同じで Certificate + Client Key Exchange + Certificate Verify + Change Cipher Spec + Finished を含んでいます。この応答で(e)サーバー認証と(f)クライアント認証が行われます。

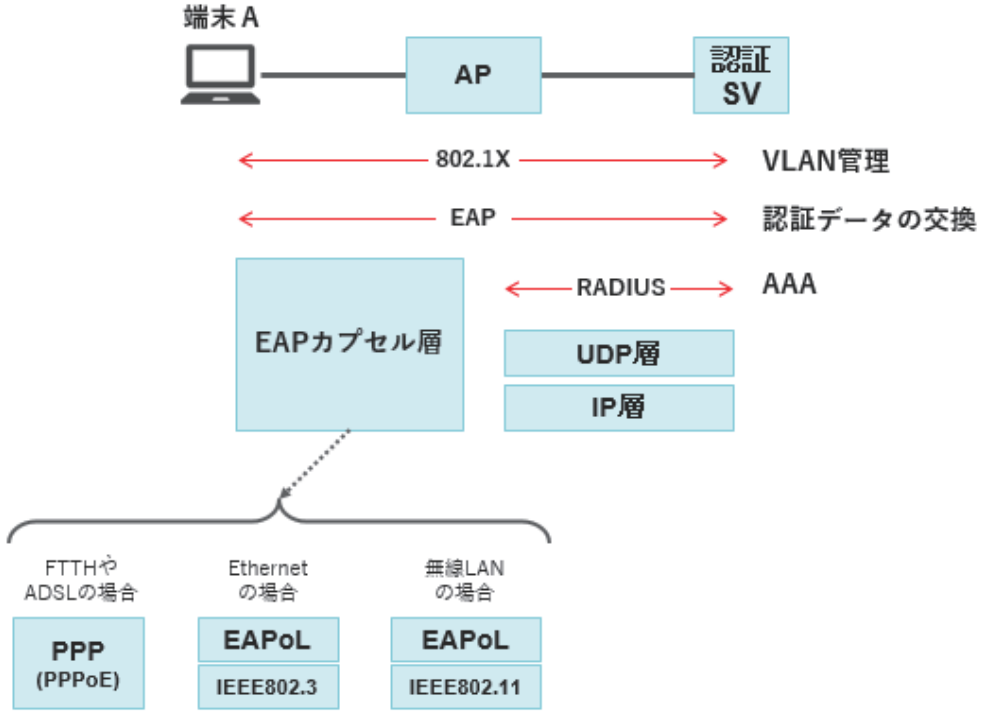
⑫⑬の応答前に端末はプリマスタシークレット(PMS)を生成しており、それを⑫の Client Key Exchange に含めて認証 SV に送信するため、(g)PMS 生成と(h)PMS 受領も同時に行われます。これに対して⑭⑮で認証 SV から端末に Change Cipher Spec+Finished を返します。このパケットは EAP 要求として送られますが、EAP は要求~応答を一対で行うため、⑯⑰で端末から認証 SV に EAP 応答パケットを返します。これで EAP-TLS 手順は完了します。

⑯の前に端末側で(i)PMK を生成しますがこれは認証 SV には送信されません。認証 SV 側では⑫⑬の手順で受信した PMS を使って同じように(j)PMK を生成して⑱EAP 成功パケットに収めて(k)AP に送信します。⑱には(l)VLAN ID も含まれており、AP は(m)その指示に従って(r)端末を VLAN に接続します。

AP はさらに⑲EAP 成功のパケットを端末に送信します。ここでは(n)EAP 成功を伝えるだけで、PMK や VLAN ID は含まれません。

この時点で端末は EAP-TLS の認証が無事終了したことを確認できますが、端末にとって AP は認証されていません。そこで、⑳で双方でそれぞれ(o)(p)暗号鍵を生成して通信を行うことにより、(q)AP 認証を行います。

45 802.1X 関連プロトコルの連携



前項「TLS 接続手順と IEEE802.1X 手順の比較」で記したさまざまな機能はいくつかのセキュリティプロトコルの連携によって実現します。その役割分担のイメージが上図です。

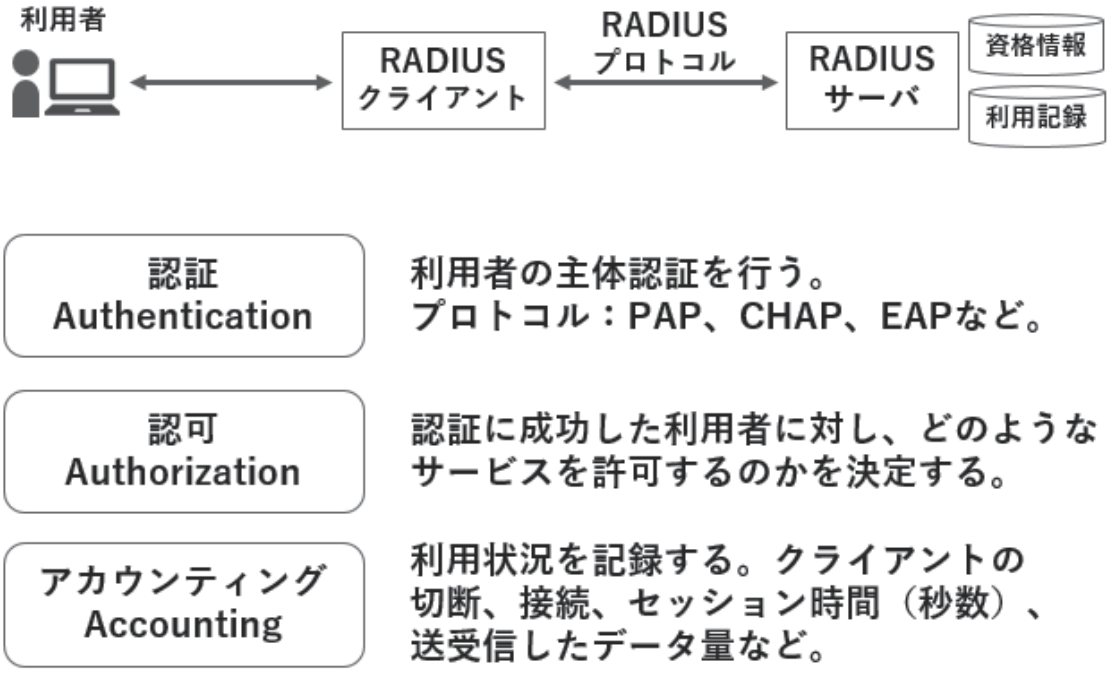
IEEE802.1X は VLAN の管理をするプロトコルで、手順全体の枠組みを作ります。
IEEE802.1X の枠組みの中で端末～AP～認証 SV 間で認証データを交換するために使われるのが EAP です。

EAP のパケットは、AP～認証 SV 間では RADIUS プロトコルにカプセル化して運ばれます。
RADIUS は本来は AAA つまり認証、認可、アカウンティングを行うためのプロトコルで、RADIUS の下は UDP、IP 層です。AP～認証 SV 間は既に IP 通信が確立しているため、UDP/IP を前提とする RADIUS の中に EAP をカプセル化できます。

一方、端末～認証 SV 間で認証を行う段階では端末～AP 間は IP 接続が確立していません。そこで IP に依存しないプロトコルで EAP をカプセル化します。図中の「EAP カプセル層」は具体的には PPP または EAPoL になります。端末～認証 SV 間の EAP パケットは、AP が RADIUS と EAP カプセル層の載せ替えを行って中継します。

これらのプロトコルの詳細については本章の中で後述します。

46 RADIUS：認証/認可/アカウンティング



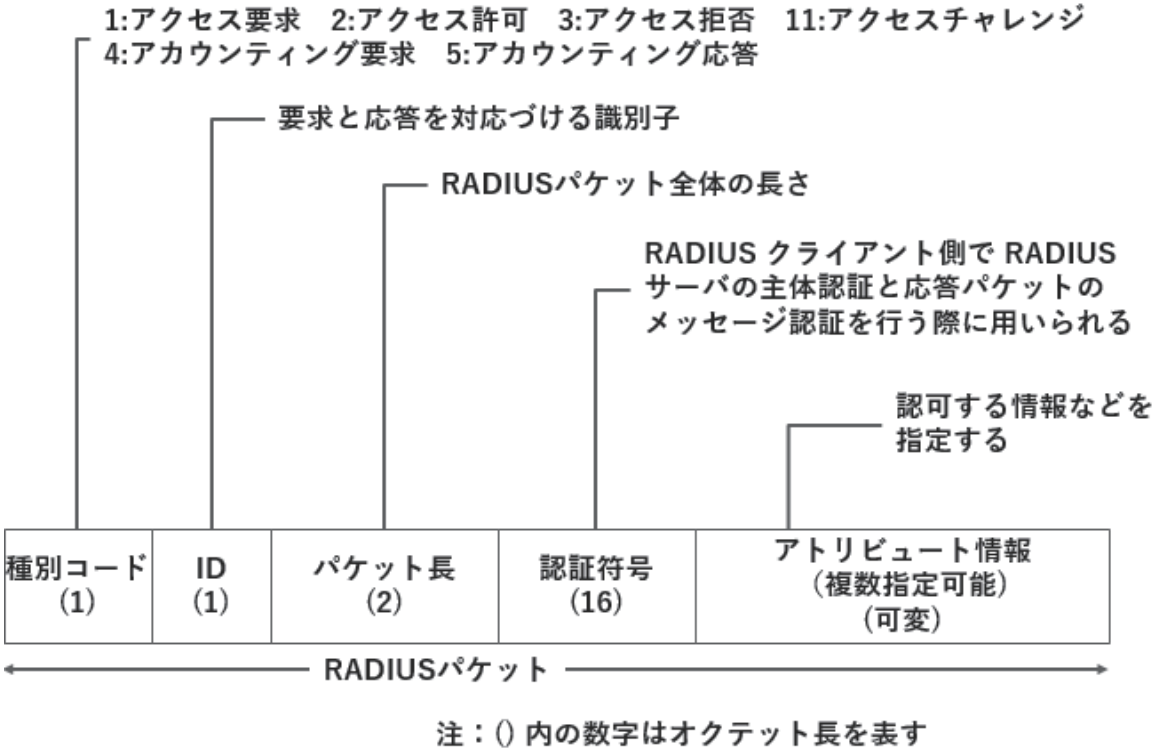
RADIUS（Remote Access Dial In User Service）は，認証（Authentication），認可（Authorization），アカウンティング（Accounting）の三つの機能を提供するプロトコルです。この 3 機能を，それぞれの頭文字を取って AAA モデルと呼びます（「トリプル・エイ」と読む）。

認証機能は，利用者の主体認証を行います。RADIUS プロトコルは RADIUS サーバーと RADIUS クライアント間のプロトコルですが、RADIUS クライアントは，実際の利用形態ではアクセスサーバですので、認証対象の「利用者」とはアクセスサーバから見たクライアント（リモートアクセスしたユーザ）のことです。認証には，PAP、CHAP、EAP など種々のプロトコルを使用することができます。

認可機能（アクセス制御機能）は，認証に成功した利用者に対し，どのようなサービスを許可するのかを決定します。たとえば無線 LAN や VLAN スイッチへの接続許可がその例です。許可する情報はパケットの中のアトリビュートを用いて指定します。RFC 標準のもの以外に、ベンダ拡張のアトリビュートも数多く規定されています

アカウンティング機能は，接続、切断、データ量などの利用状況を記録します。

47 RADIUS パケット・フォーマット



種別コードは，アクセス要求、アクセスチャレンジなどの RADIUS パケットの種別を示します。

ID は、要求と応答の対応付けに用いられる識別子で、要求ごとに生成されます。

パケット長は、図に示した RADIUS パケットの全体の長さです。

認証符号は、RADIUS クライアント側で RADIUS サーバーの主体認証と応答パケットのメッセージ認証を行う際に用いられます。

アトリビュート情報は、規定のフォーマット（本書では省略）に従って、複数のアトリビュートを指定することが可能です。

アクセス要求、アクセス許可、アクセス拒否、アクセスチャレンジには 1812 ／ UDP を、アカウンティング要求、アカウンティング応答には 1813 ／ UDP を使用します。

48 演習問題

問 1

次に示す観点に基づいて、共通鍵方式と公開鍵方式を比較し、どちらの方式が優れているかを述べてください。

観点	共通鍵方式	公開鍵方式	優劣
暗号化と復号の速度			
導入容易性			
管理の容易性			
共有や配布の容易性			

問 2

RADIUS がもつ認証（Authentication），認可（Authorization），アカウンティング（Accounting）の三つの機能の説明として、最も適切な組合せはどれでしょうか？次の選択肢ア～エの中から一つを選んでください。

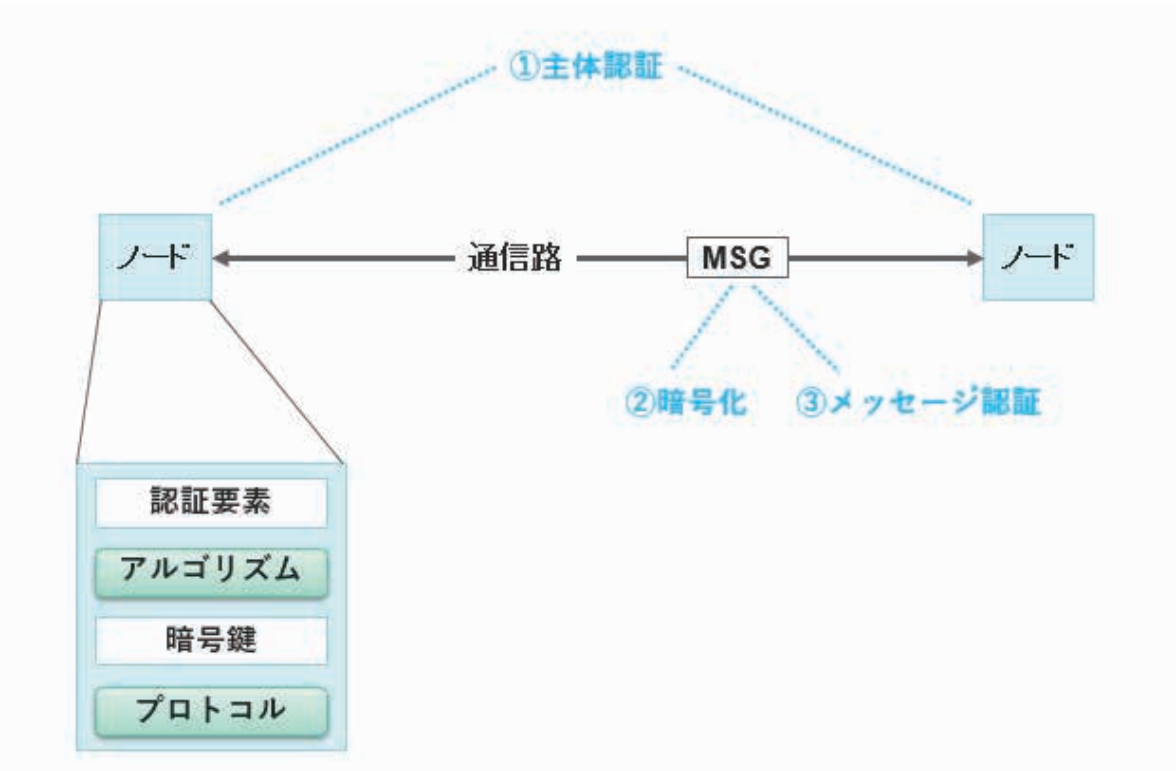
項番	機能の説明
a	クライアントの主体認証を行います。
b	サーバーの主体認証を行います。
c	接続、切断、データ量などの利用状況を記録します。
d	認証に成功した利用者に対し，どのようなサービスを許可するのかを決定します。

	認証	認可	アカウンティング
ア	a、b	c	d
イ	a、b	d	c
ウ	a	c	d
エ	a	d	c

第3章.

セキュリティプロトコル

1 2点間暗号化通信の技術概要



本章ではIP通信の暗号化に使われるプロトコルについて学びますが、本節では細部の話に入る前に知っておきたい大まかなポイントを説明します。

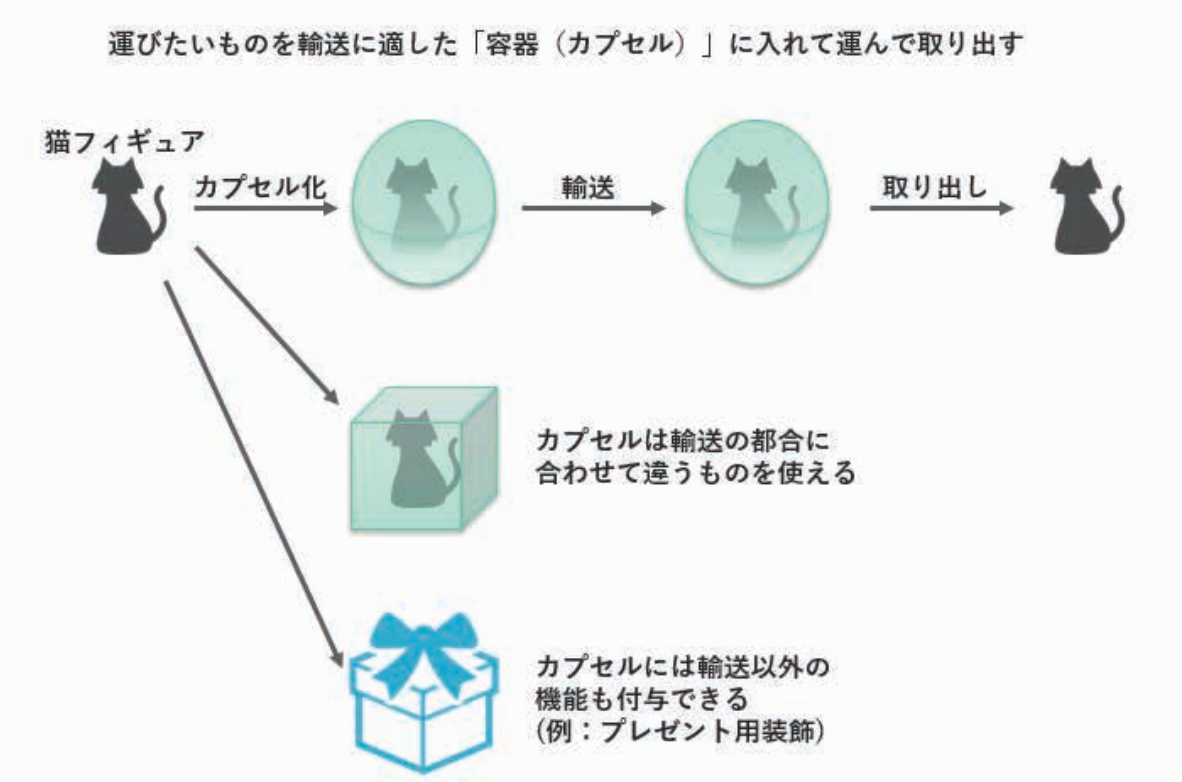
２つの「ノード」間の通信を暗号化するには大まかに①主体認証、②暗号化、③メッセージ認証をしなければなりません。

①主体認証　：　ノードが真正なものである（なりすまされてない）ことを確認する
②暗号化　：　メッセージが傍受されても読めないように暗号化する
③メッセージ認証　：　メッセージが改ざんされていないことを検証する

これらを行うためには、双方のノードに「認証要素」、「アルゴリズム」、「暗号鍵」、「プロトコル」が必要です。

「プロトコル」には大まかにIPsecとSSL/TLSの2種類があります。

2 カプセル化とは



暗号化技術について触れる前に、通信技術一般に関わりの深い「カプセル化」という概念を確認しておきます。

カプセル化とは、運びたいものを輸送に適した「容器（カプセル）」に入れて運ぶ操作を言います。

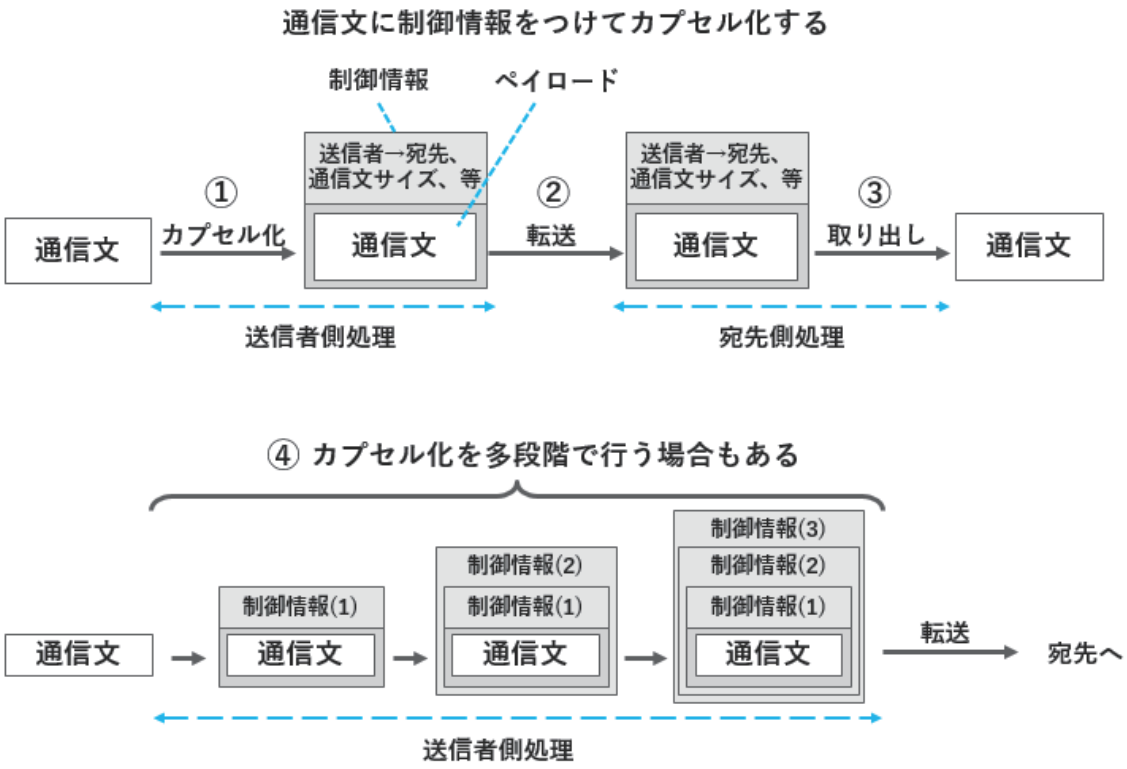
図は、猫フィギュアをカプセル化して輸送し、受け取ったら取り出すイメージを表しています。カプセルから取り出した中身（猫フィギュア）はカプセル化する前と同じものです。

カプセルは輸送の都合に合わせて違うものを使うことができます。通信の場合は物理的な回線がEthernet でも無線や光ファイバーでも同じデータを送れるようにするために、下層の通信フォーマットに合わせて上層のデータを埋め込む操作がカプセル化に該当します。

カプセルには輸送以外の機能を持たせる場合もあります。図中の例はカプセルにプレゼント用の装飾を加えています。あるいは郵便で使う「封筒」というカプセルは、内部の文書を読まれないようにする「秘匿」の機能を持っています。

通信を暗号化する場合は、カプセル化に際して暗号処理を行います。

3 通信におけるカプセル化

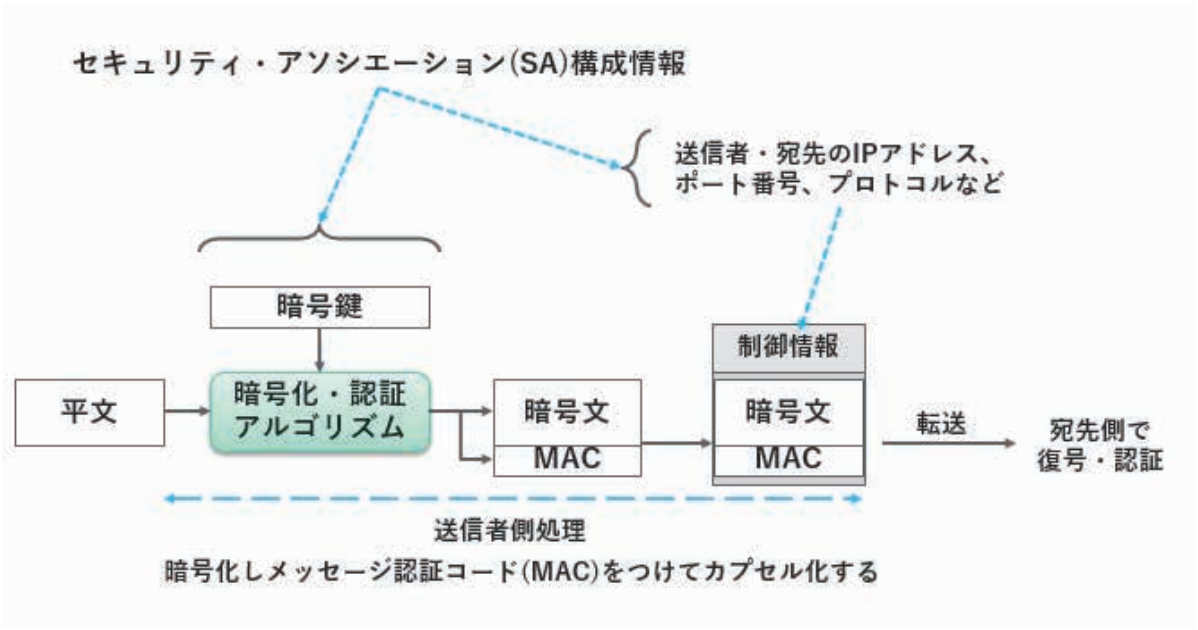


デジタル通信では、通信文に「制御情報」をつけることを「カプセル化」と言います。カプセル化したものを転送して受信（宛先）側で中身を取り出すことで通信文を復元できます。

「制御情報」には送信者と宛先の情報や通信文のサイズなどがあります。カプセル化して運ばれる通信文そのもののことを一般にペイロードと言います。「パケット」は制御情報とペイロードをまとめた全体のことを言います。

カプセル化を多段階で行う場合もあります。図中の下段は通信文を 3 段階でカプセル化して送る例です。一般に通信プロトコルは階層構造になっていて、上層から下層へ進むごとにカプセル化を行います。

4 暗号化・メッセージ認証とカプセル化



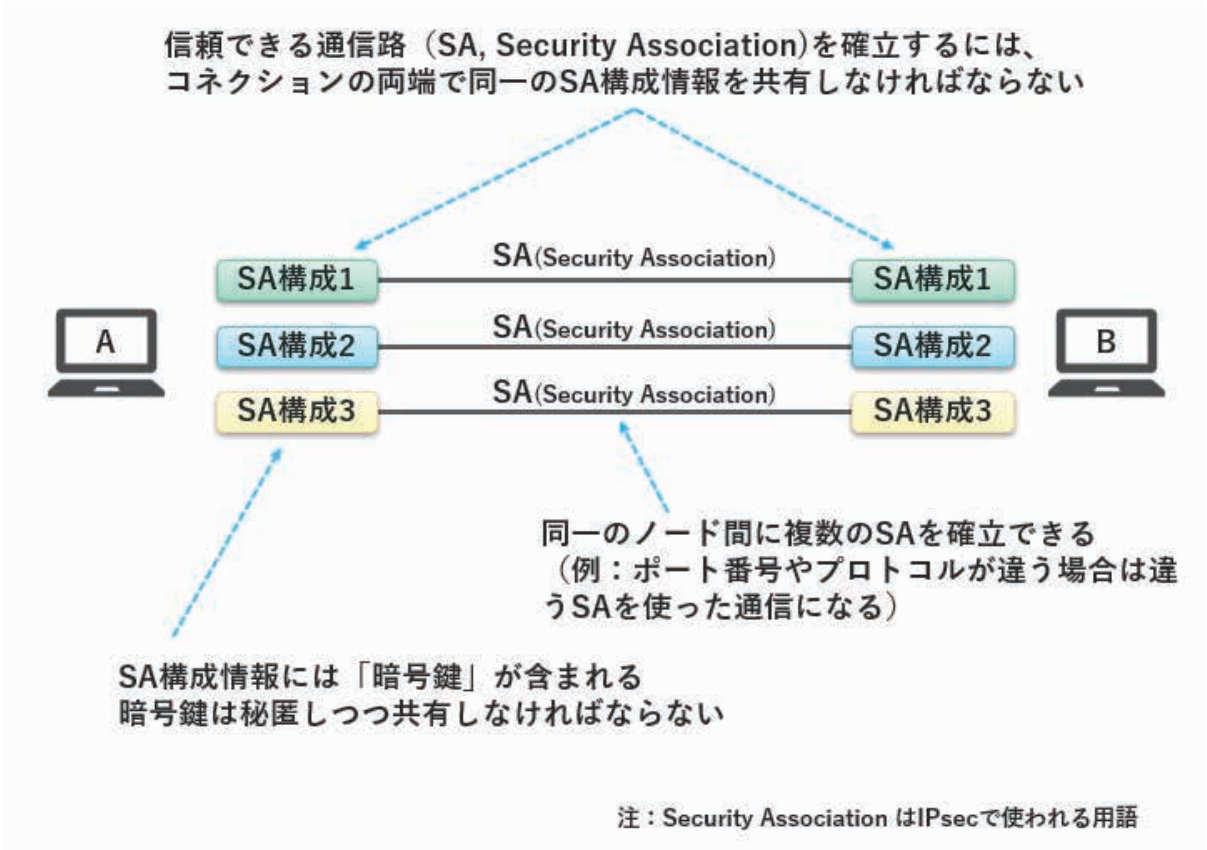
暗号化とメッセージ認証を行う場合は、平文を暗号化・認証アルゴリズムにかけて暗号文と MAC（Message Authentication Code、メッセージ認証コード。改ざん検出に使われる）を生成し、そこに制御情報をつけてカプセル化し転送します。

図中の「制御情報」と「暗号鍵」「暗号化・認証アルゴリズム」を合わせて本書ではセキュリティ・アソシエーション（SA）構成情報と呼びます。

（注：セキュリティ・アソシエーションは IPsec の用語）

暗号化通信を行う場合、ひとかたまりの平文データを分割して暗号化するため、一連のセッションの中で多数の暗号化パケット交換が発生します。この間、「パケット」の内容は常に変わりますが、SA 構成情報は基本的に変化しません。

5 セキュリティ・アソシエーション

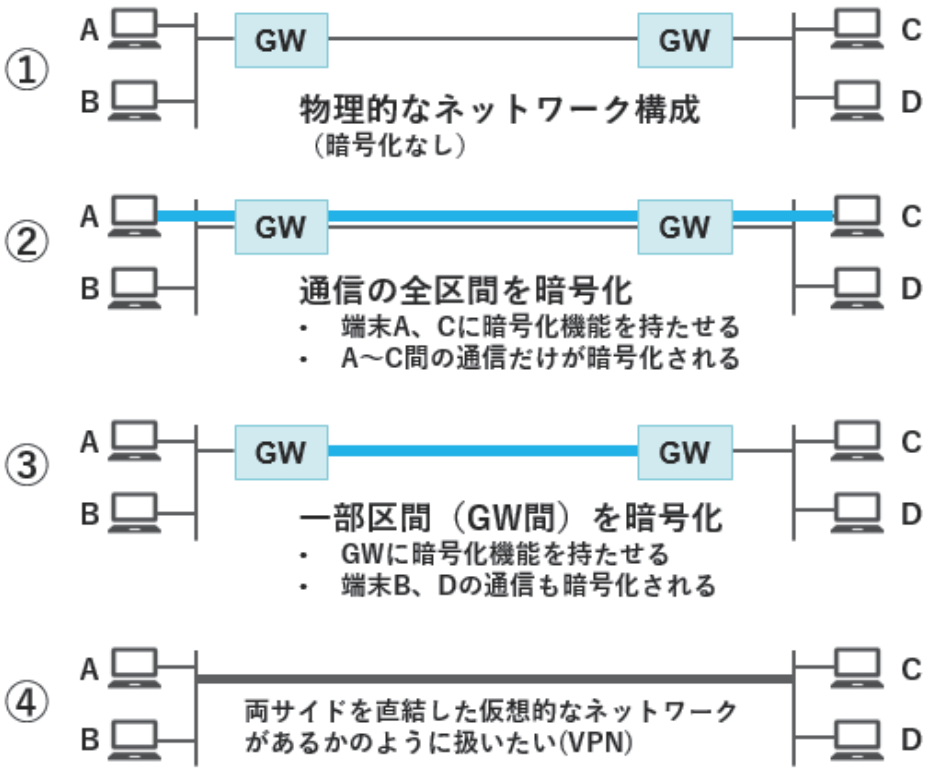


セキュリティ・アソシエーション(SA, Security Association)とは IPsec の用語で、信頼できる通信路という意味です。SA を確立するためにはコネクションの両側で同一の SA 構成情報を共有しなければなりません。

SA 構成情報には「暗号鍵」が含まれます。暗号鍵は秘匿しつつ共有しなければなりません。SA 確立前の「信頼できる通信路」が存在しない状態で暗号鍵を共有するために、適切な手順で鍵交換を行う必要があります。

IPsec では同一のノード間に複数の SA を確立することができます。詳しくは IPsec の節で解説します。

6 暗号化区間のパターン



通信区間全体のどの範囲を暗号化するかについて、パターンが大まかに 2 つあります。

①のような構成のネットワークを想定して考えます。GW(ゲートウェイ)の間はインターネットで、途中で傍受／改ざんされる恐れのある「信頼できないネットワーク」だとします。

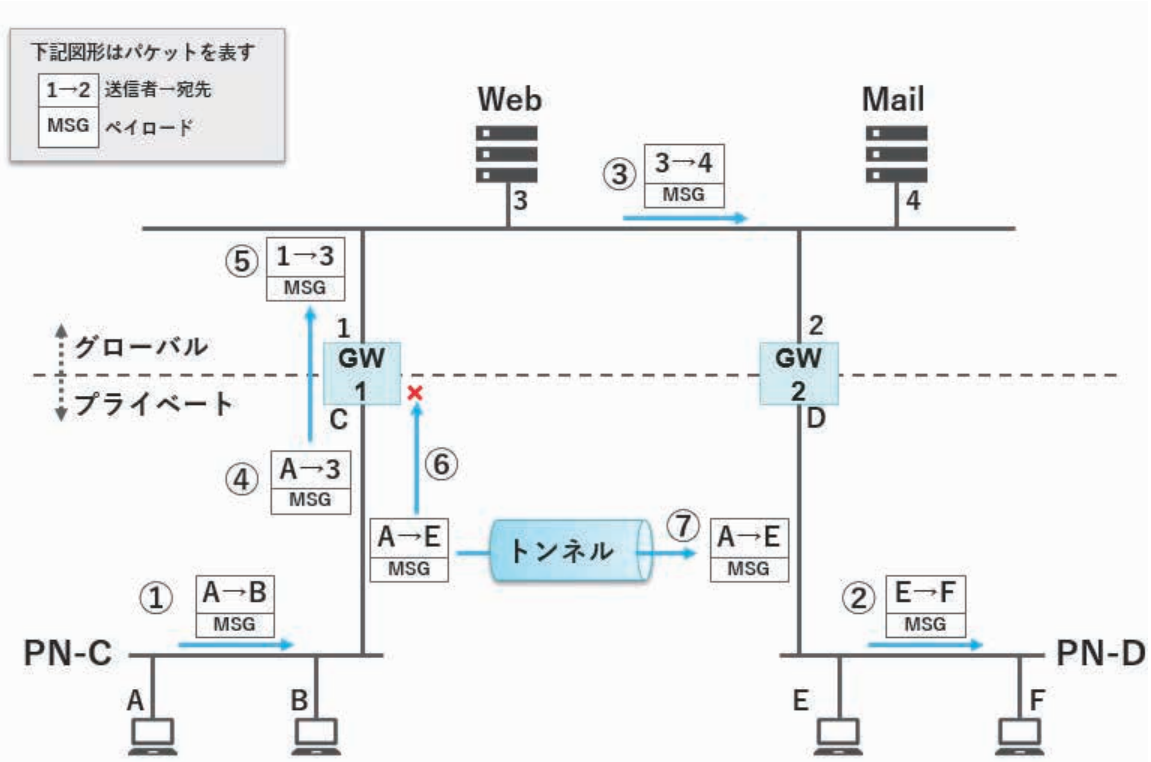
②は①の環境下で通信の全区間を暗号化するパターンです。この場合、A、C のような端末に暗号化機能を持たせる必要があります。たとえば端末 B や D は暗号化機能を持たないとすると、A～C 間だけは暗号化されますが、それ以外の組み合わせでは暗号化されません。

③は GW 間のみを暗号化するパターンです。この場合は GW に暗号化機能を持たせれば端末には必要ありません。この方法だと A～B 間、C～D 間のような LAN 区間では暗号化されませんが、「信頼できないネットワーク」の区間はすべて暗号化されます。多数の端末に個別に暗号化機能を設定しなくてもすべての端末が安全に通信できるため、手間がかかりません。

④　③の方法は、実質的には 2 つの GW の両側を直結した仮想的なネットワークがあるかのように扱うことができます。これが VPN と言われる概念で、さまざまな実現方法があります。

なお、実際には②と③の中間（端末～GW 間で暗号化を行う）のパターンもあります。

7 LAN 間接続とトンネリング



VPN(Virtual Private Network)は、LAN と LAN を WAN 経由で接続する、「LAN 間接続」と呼ばれる仕組みのひとつです。この図では、WAN（たとえばインターネット）経由で LAN 間接続を行う場合に必要になる「トンネリング」という機能のイメージをつかんでください。

上図は 2 つのプライベートネットワーク、PN-C と PN-D がそれぞれ GW 1 と GW2 を通してインターネットにつながっているイメージです。①～⑦までの数字の横にある箱は IP パケットを表しています。アドレス表記は数字または英字 1 文字に簡略化してあります。

2 つの GW はインターネット側ではそれぞれ 1，2 というグローバル IP アドレスを持ち、プライベートネットワーク側ではそれぞれ C､D というプライベート IP アドレスを持っています。

この構造の中で①は端末 A から B へ送られるパケットを表します。A、B はいずれも PN-C 内部の端末ですので問題なく通信可能です。同様に②のパケットも PN-D 内部ですので通信可能、③はインターネット側でこれも通信可能です。

④は PN-C からインターネット側への通信ですが、これは GW1 が中継し IP アドレスを「1→3」に書き換えてパケット⑤としてグローバル IP「 3 」を持つノード（Web サーバ）に送り出されるため

通信可能です。「３」からの返信はやはり GW1 で端末 A 宛にアドレスを書き換えて PN-C 側に中継されます（これは図に記載なし）。

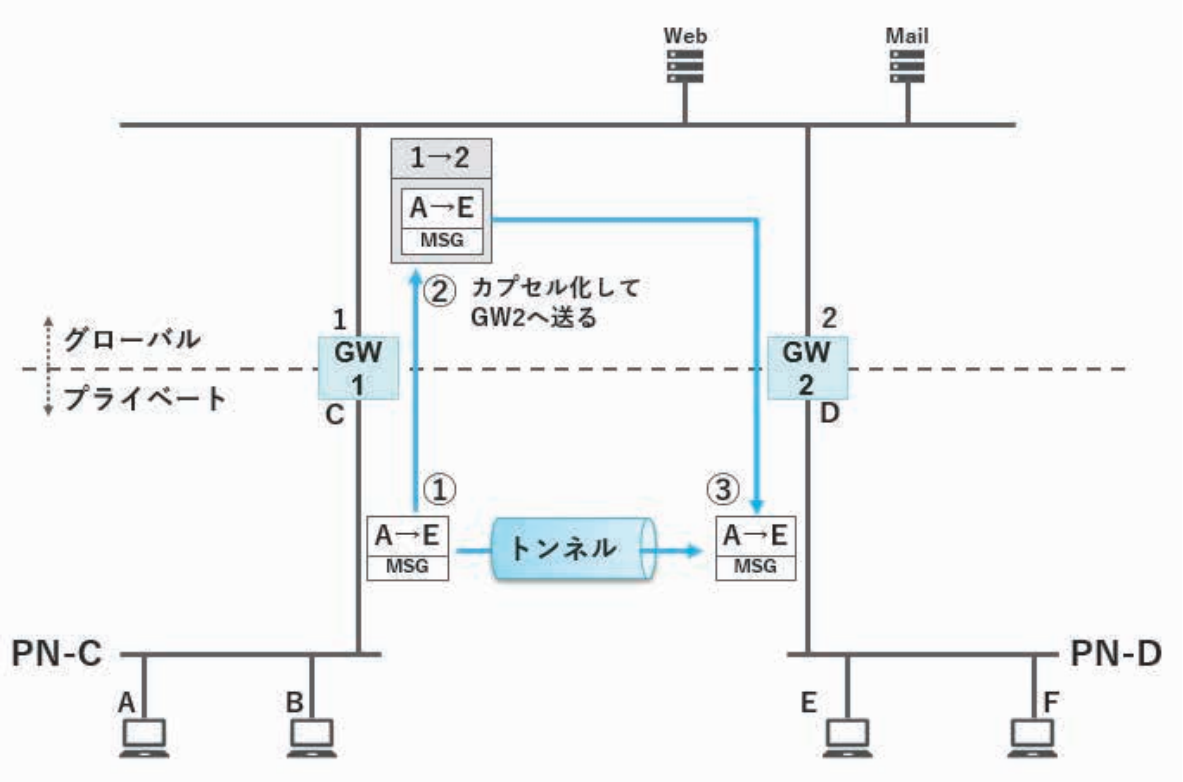
問題はこの先のパケット⑥です。PN-C 内の端末 A から PN-D 内の端末 E 宛のパケットが GW1 に届いても、GW1 は E がどこにあるか知らないため中継できません。⑥のパケットはアドレスがいずれもプライベートネットワークであることに注意してください。図の GW は「インターネットとプライベートネットワークの中継」をするのが役割であり、アドレスが両方ともプライベートアドレスの場合は中継できないのです。

そこで、パケット⑥をインターネットへ流さず PN-D に送り込んで（⑦）しまう、「トンネル」のようなものが欲しくなります。図中の「トンネル」は、インターネットから隔離された空間を通って PN-C と PN-D を結ぶものと考えてください。ちょうど現実世界のトンネルが山をぶちぬいて山登りせずに反対側の平地に出られるように、通信の世界の「トンネル」は「インターネット」という山をぶち抜いてプライベートネットワークどうしを直結するものと見なせます。

これができれば、PN-C と PN-D が実質的に直結しているかのように扱えます。それが VPN です。

しかし実際には PN-C と PN-D を直結する回線はありませんので、このような「トンネル」を実現するためには、なんとかしてインターネットを通してパケット⑥を PN-D に送り込まなければ(⑦)なりません。それはどうすれば可能になるでしょうか？

8 トンネリングの実装イメージ

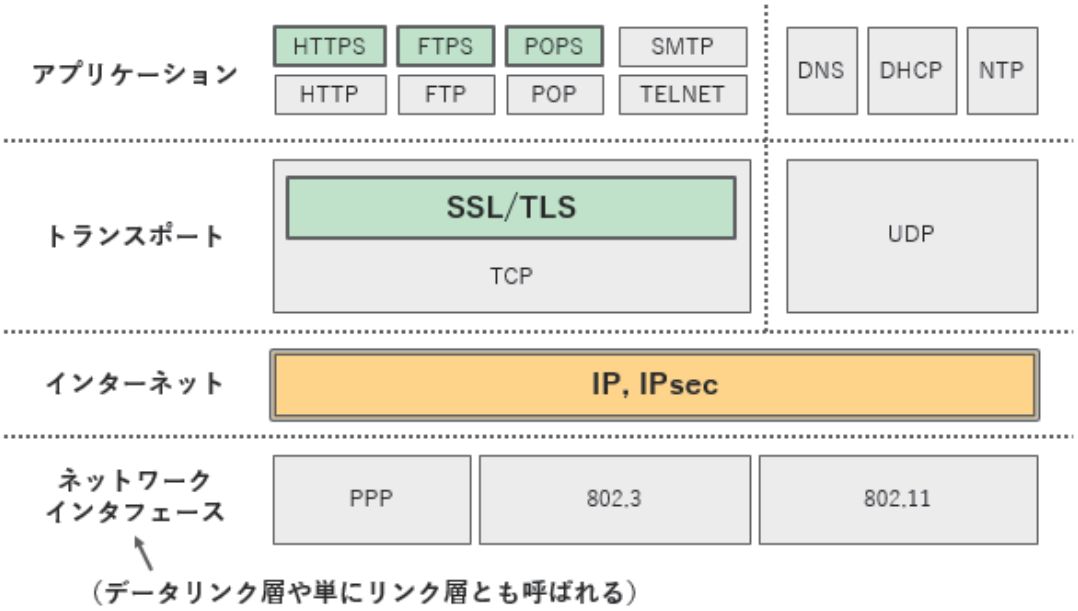


そこで GW にトンネリングの機能を持たせます。図中の①が PN-C から PN-D へ送りたいパケットです。GW1 がこれを受信したらそれをカプセル化し、②新しいアドレス「1→2」をつけて GW2 へ送ります。GW2 はそれを受け取ったら③カプセル化された元のパケットを取り出して PN-D へ送り出します。この方法であたかも①～③を直結するトンネルがあるかのような通信を実現できます。

これが「トンネリング」のイメージで、元のパケットを保ったまま新しいアドレスをつけて別なネットワーク上を転送し、転送先で元のパケットを復元する機能を一般に「トンネリング」と言います。

ただし「トンネリング」そのものには「暗号化・改ざん防止」は含みません。したがって、VPN を構築する場合は、トンネリングに加えてパケットの暗号化とメッセージ認証を合わせて行う必要があります。

9 暗号化通信プロトコルと TCP/IP スタック



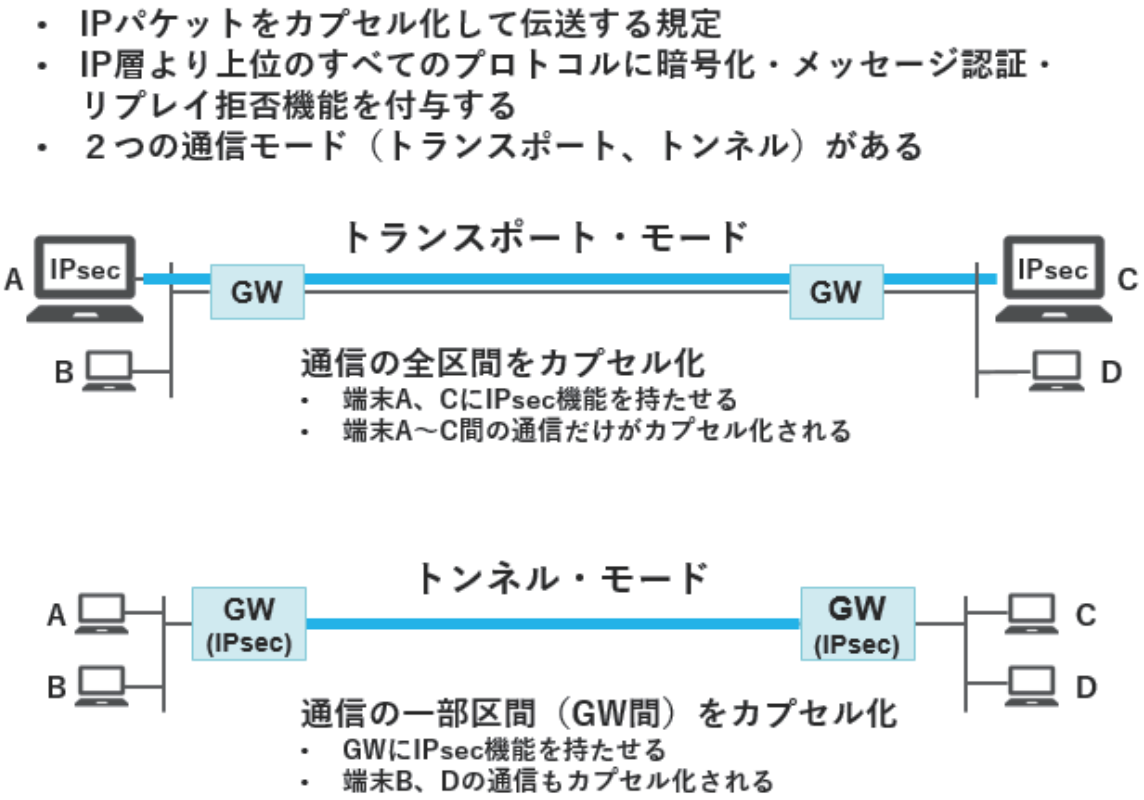
本章で扱う暗号化通信プロトコルは IPsec と SSL/TLS の 2 種類です。この両者は TCP/IP プロトコルスタック上の違う階層で動作することに注意が必要です。

図中に示したように、IPsec プロトコルはインターネット層で IP の代替のように動作します。一方、SSL/TLS はトランスポート層で TCP の上位階層のように動作します。

この違いによって以下のような差が生まれます。

	IPsec	SSL/TLS
階層	IP の代替のように動作し、すべての IP パケットの暗号化を行う	TCP の上位で動作する
暗号化が有効になるプロトコルの範囲	TCP、UDP を問わずすべての上位プロトコルの通信で暗号化が有効になる	UDP 系プロトコルはすべて対象外。TCP を使うアプリケーションは暗号化できる。ただしアプリケーション層で TLS セッション開始のハンドシェイクを行うため、それに対応したアプリケーションを使う必要がある。
設定の難しさ	ルータの NAT 機能や FW の設定と不整合を起こしやすく、運用が難しい	シンプルな設定で動作し、ルータの NAT 機能や FW に影響されにくい

10 IPsec の 2 つのモード



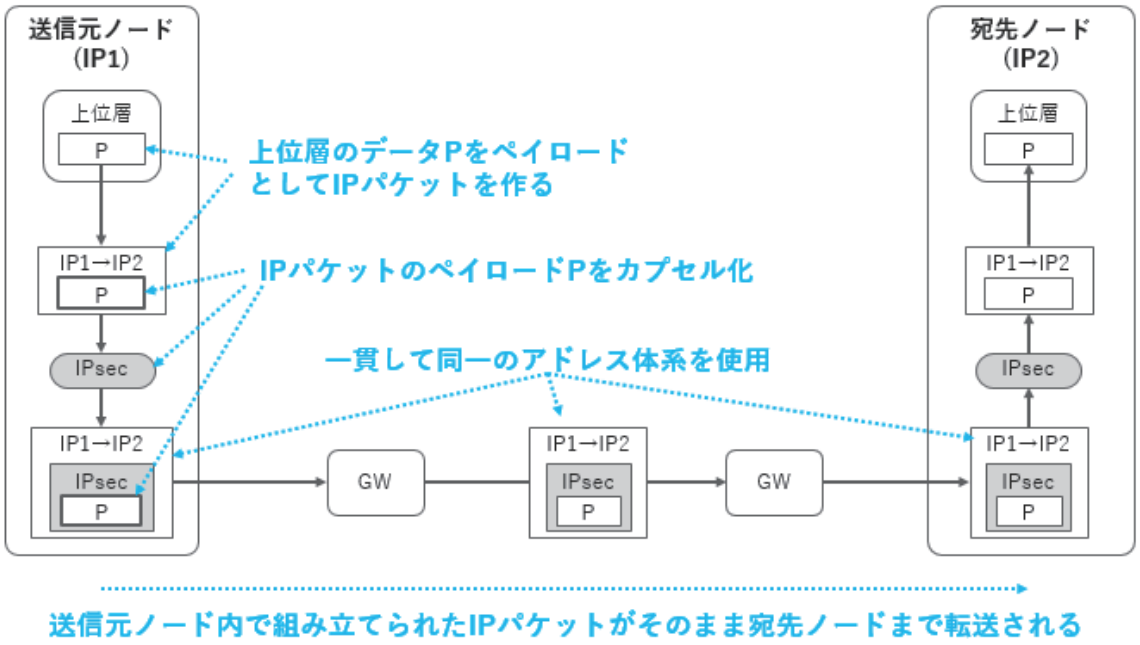
IPsec(IP security) は IP パケットそのものをカプセル化して伝送する規定で、IP 層より上位のすべてのプロトコルによる通信に、暗号化・メッセージ認証・リプレイ拒否機能を付加できます。IPv4、IPv6 の双方で使用できます。

IPsec には通信路の全区間をカプセル化するトランスポート・モードと，一部の区間だけをカプセル化するトンネル・モードの 2 種類の通信モードがあります。

上図では太線部分がカプセル化の範囲です。トランスポート・モードでは端末間、トンネル・モードでは GW 間がカプセル化されるイメージですが、実際には端末をトンネル・モードで動かすことも可能です。

IPsec モジュールは、受信または転送するパケットの種類を調べてその種類に応じて PROTECT(IPsec の処理を行う)、BYPASS(IPsec の処理を行わず、通常の IP パケットとして通過させる)、DISCARD(パケットを破棄する)のいずれかの動作をします。パケットの種類に応じた動作設定の情報をセキュリティポリシーと言います。

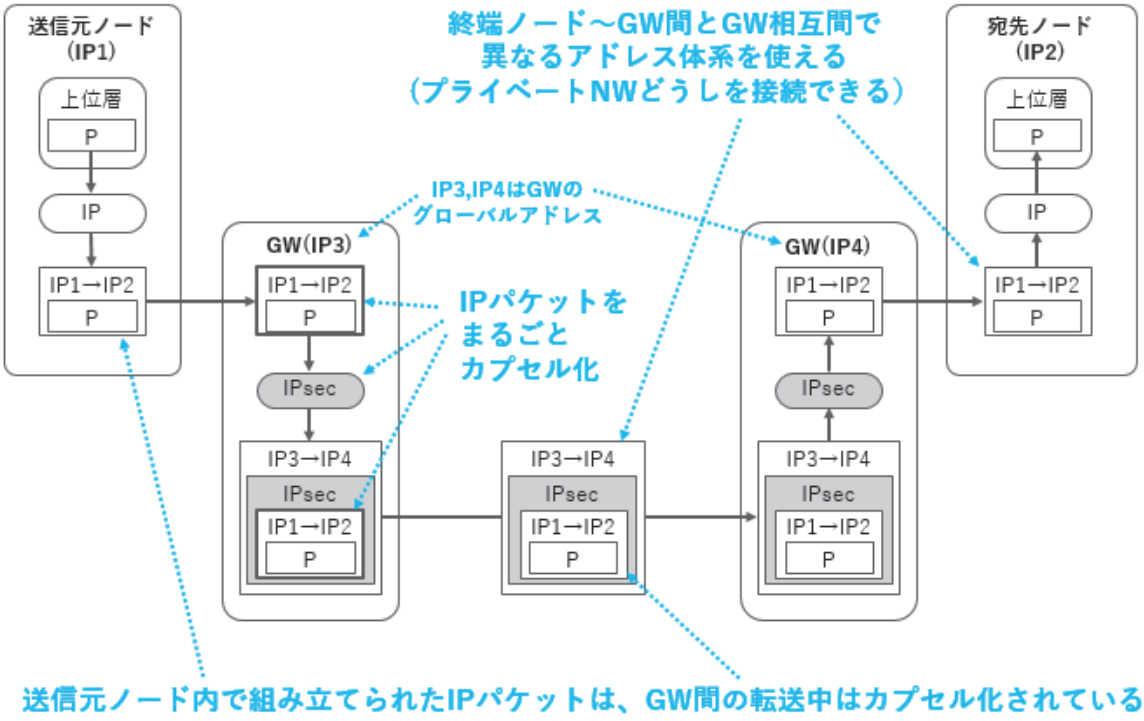
11　トランスポート・モードの動作イメージ



トランスポート・モードの動作イメージです。
「送信元ノード」と「宛先ノード」の IP アドレスがそれぞれ IP1、IP2 であるとします。送信元ノードの上位層のデータ P を宛先ノードに送信する場合、P をペイロードとして IP パケットを作ります。「IP1→IP2」は送信元→宛先ノードのアドレスですが、ここは IP ヘッダ全体を表していると考えてください。ここまでは通常の IP の処理です。

IPsec のトランスポート・モードではこの IP パケットのペイロード部分を送信元ノード内でカプセル化して宛先ノードまで転送します。送信元ノード内で組み立てられた IP パケットがそのまま宛先ノードまで転送されること、そのため送信元ノードから宛先ノードまで一貫して同一のアドレス体系「IP1→IP2」が使用されていることに注意してください。

12　トンネル・モードの動作イメージ

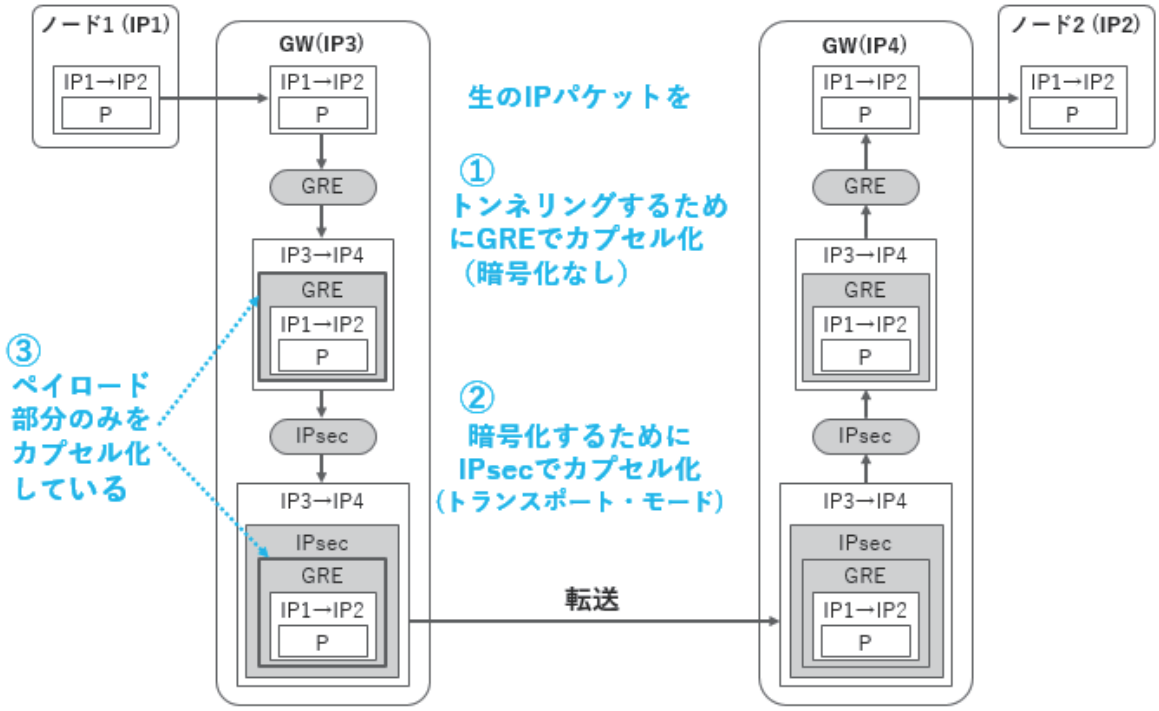


トンネル・モードの動作イメージです。GW のプライベートネットワーク側アドレスは省略し、グローバルアドレス IP3,IP4 のみを記載しています。

終端ノード内では IPsec の処理を行なわず、GW 内で IP パケットをまるごとカプセル化します。トランスポード・モードではペイロード部分のみを対象としていたのに対して、ここでは「IP1→IP2」の部分まで含めてカプセル化し、新しく「IP3→IP4」の送信元／宛先アドレスを設定した IP ヘッダをつけます。

つまり、送信元ノード内で組み立てられた IP パケットは GW 間の転送中はカプセル化されているため、終端ノード～GW 間と GW 相互間で異なるアドレス体系を使えます。これはインターネットを通してプライベート NW どうしを接続できることを意味します。

13 GRE/IPsec の動作イメージ

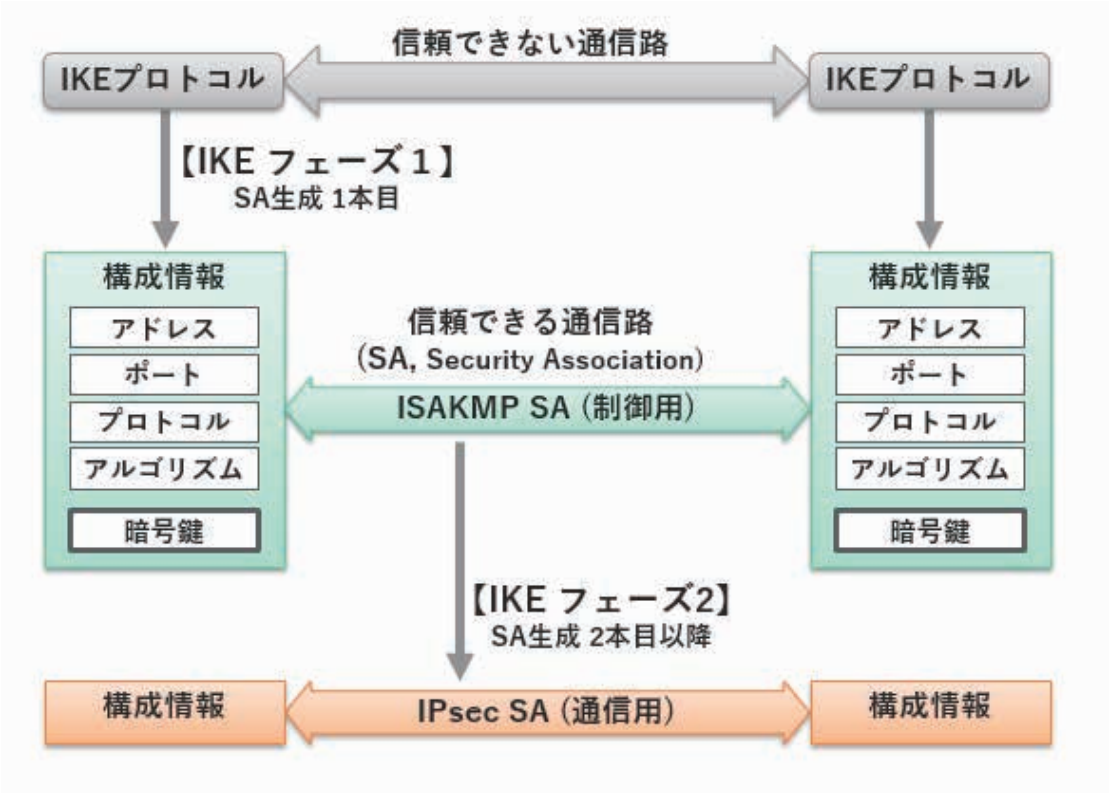


VPN(Virtual Private Network)の実装によく使われる GRE/IPsec は、トンネリング・プロトコル GRE を IPsec で暗号化して VPN を実現する方法です。

この場合、生の IP パケットをまず①GRE でまるごとカプセル化します。これでトンネリングが可能になりますが、GRE には暗号化機能はないため、暗号化はされていません。

そのうえで②暗号化するために IPsec を使用します。ここではペイロード部分のみをカプセル化するため、トランスポート・モードを使用します。

14 セキュリティ・アソシエーションの生成

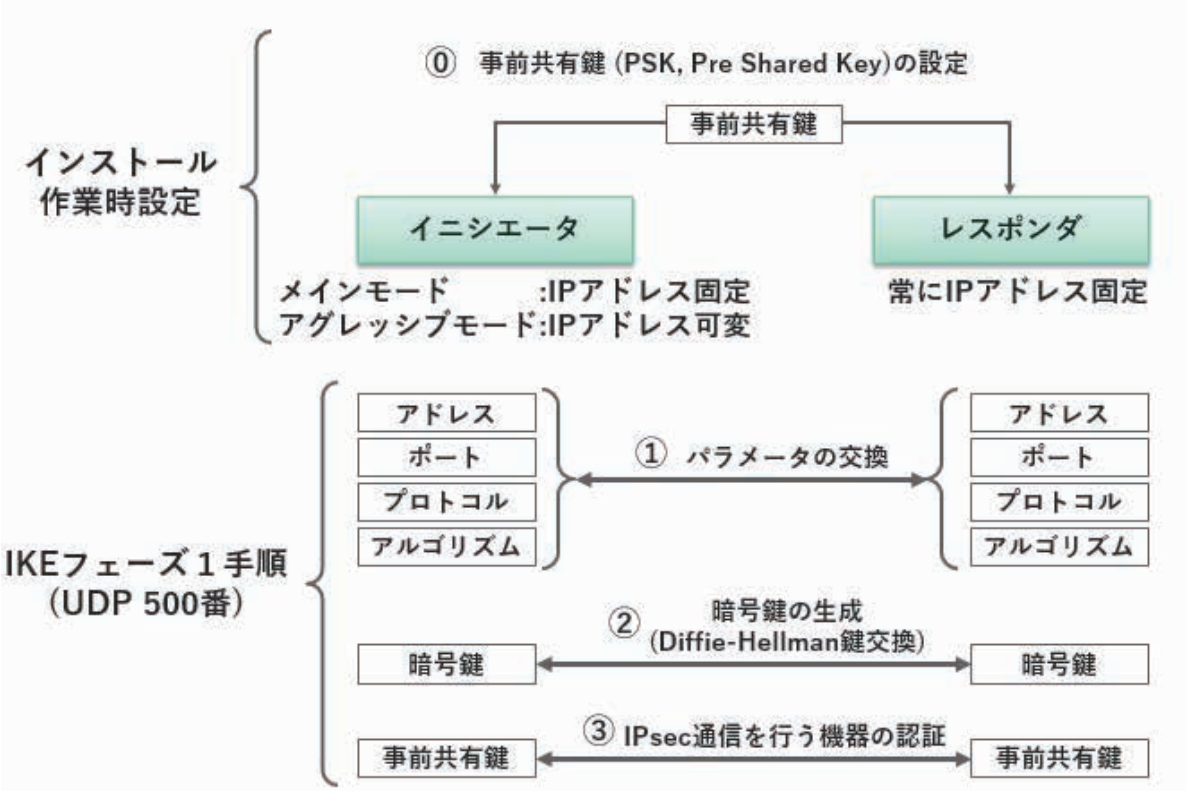


IPsec がノード間に開設する「信頼できる通信路」のことを SA(Security Association)と言います。SA には制御用の ISAKMP SA（アイサカンプ SA）と通信用の IPsec SA の 2 種類があります。

SA を開設するためには、両端のノードどうしで SA の構成情報を交換しなければなりません。構成情報には、両者のアドレス、ポート番号、TCP/UDP などのプロトコル、認証や暗号化に用いるアルゴリズム、暗号鍵などがあります。
暗号化アルゴリズムは共通鍵暗号方式を用いるため、暗号鍵は秘匿しなければなりません。しかし、1 本目の SA を開設する前の段階では「信頼できない通信路」しか存在しないため、暗号鍵を直接送信できません。そこで、信頼できない通信路で暗号鍵を含む構成情報を安全に交換するために IKE(Internet Key Exchange)というプロトコルを使います。IKE はフェーズ 1 とフェーズ 2 に分かれていて、1 本目の SA 生成にはフェーズ 1 を使い、2 本目以降の SA 生成にはフェーズ 2 を使います。

1 本目の SA 生成で作るのが ISAKMP SA です。2 本目以降の SA(IPsec SA)はこの ISAKMP SA を通して構成情報を交換して作ります。

15 IKE フェーズ1



IKE(Internet Key Exchange)は IPsec 鍵交換のためのプロトコルで、起動側をイニシエータ、応答側をレスポンダと言います。メインとアグレッシブの 2 種類のモードがあり、メインモードでは双方とも IP アドレス固定、アグレッシブモードではレスポンダ側のみアドレス固定となります。イニシエータ、レスポンダには事前に共有鍵(PSK, Pre Shared Key)を設定しておかなければなりません。

IKE フェーズ 1 の手順は、①パラメータの交換、②暗号鍵の生成、③機器認証、の 3 段階です。

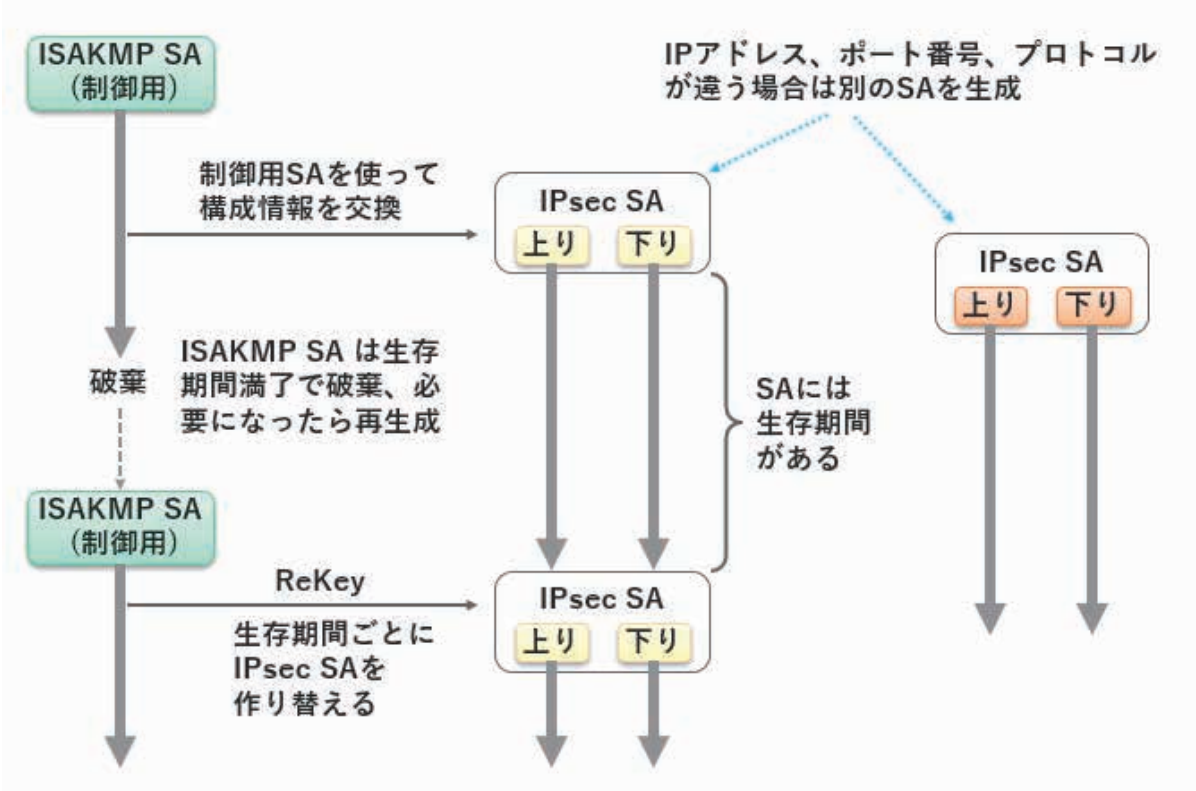
①では②,③に必要な暗号化アルゴリズムや認証アルゴリズムなどを交換します。

②では Diffie-Hellman 鍵交換方式によって、暗号化に使う鍵を生成します。

③では通信相手の真正性を認証します。通常、事前共有鍵方式を使用します。

IKE フェーズ 1 では UDP500 番ポートを通してこれらの手順を実行します。⓪「事前共有鍵(PSK)」はそれ以前に設定しておかなければなりません。

16 SA の生成と破棄



SA の生成と破棄の動きのイメージです。

最初に ISAKMP SA を生成し、それを使って構成情報を交換することで 2 本目以降の SA（IPsec SA）を生成します。IPsec SA は上り用と下り用の 2 本を同時に生成します。宛先や送信元の IP アドレス，ポート番号，TCP や UDP といった通信プロトコルが異なると別々の IPsec SA を生成するため、同じノード間に複数の IPsec SA が開設されます。

暗号化には共通鍵暗号方式を用い、SA が生成される度に異なる暗号鍵を生成して使用します。
一般的に、同じ鍵を長期間使用すると解読されるリスクが高まるため、SA には生存期間を定めてあり、生存期間ごとに新しい暗号鍵を生成して SA を作り替えます。この操作をリキー(ReKey)と呼びます。

IPsec SA については生存期間が満了する前に後継の IPsec SA が作成され、通信が遮断されないように SA の移行が行われます。ISAKMP SA については、生存期間が満ちて SA が破棄されても、ISAKMP SA を必要とする通信が起こるまでは新しい SA は作成されません。

17 メッセージ認証・暗号化・リプレイ拒否

AH ： Authentication Header
ESP： Encapsulating Security Payload

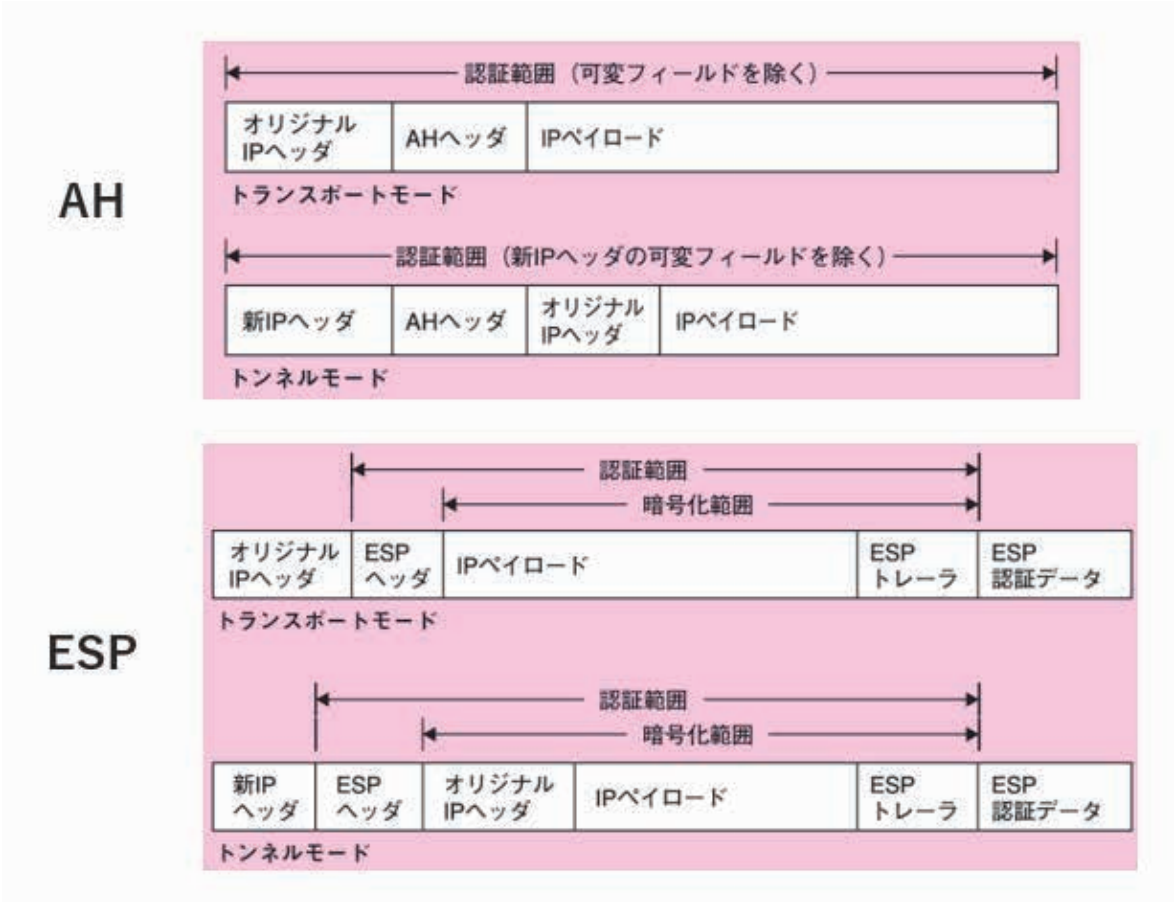
サービス	内　容	AH	ESP
メッセージ認証	データの改ざんチェック。AH と ESP では認証の範囲が異なる	○	○
暗号化	ESP のみ対応している	×	○
リプレイ攻撃の拒否	AH ヘッダ，ESP ヘッダにはシーケンス番号が格納されており，送信側はパケットを送信するたびに，これをカウントアップする。受信側はこの番号の順序を確認することで，リプレイ攻撃に対処できる	○	○

IPsec が上位層のプロトコルに提供するセキュリティ・サービスはメッセージ認証、暗号化、リプレイ攻撃拒否の 3 種類です。これらの実装プロトコルには AH と ESP の 2 種類があります。

AH(Authentication Header)はメッセージ認証とリプレイ拒否を行い、暗号化は行いません。
ESP(Encapsulating Security Payload)はメッセージ認証、暗号化、リプレイ拒否のすべてを行います。

実用的には、暗号化を行う ESP を使用するのが主流です。

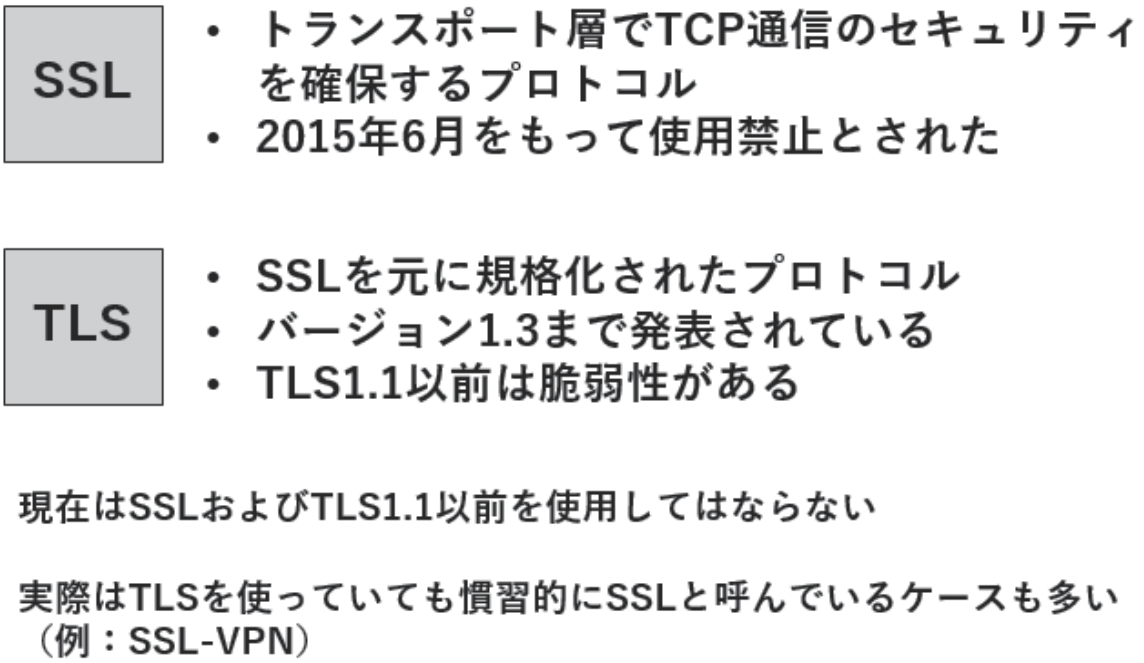
18 AH および ESP のフォーマット



AH では IP ヘッダを含む IP パケット全体を認証します。ただし IP パケットの伝送中に値が変化する可能性がある可変フィールドは除きます。

ESP では IP ヘッダを除くペイロード部分を暗号化・認証します。

19 SSL/TLS とは



SSL はトランスポート層で TCP 通信のセキュリティを確保するプロトコルで、それを発展させて規格化されたものが TLS です。SSL は脆弱性が発見されたために 2015 年 6 月をもって使用禁止とされています。

TLS1.1 はバージョン 1.3 まで発表されていますが、1.1 以前には脆弱性が発見されているため、新しいシステムに TLS を実装する場合は 1.1 以前は使用すべきではありません。

ただし、実際には TLS を使っていても、「SSL-VPN」のように SSL を含む名前が技術用語として定着している場合はその名前が使われていることがあります。あるいは単に慣習的に SSL と呼んでいるケースもよくあります。

20 TLS を利用する上位層

アプリケーション	TLS使用有無	プロトコル名	ポート番号
WWW	使用しない	http	80
	使用する	https	443
Telnet	使用しない	telnet	23
	使用する	telnets	992
メール送信	使用しない	smtp	25 (*)
	使用する	smtps	465
メール受信	使用しない	pop3	110 (*)
	使用する	pops	995

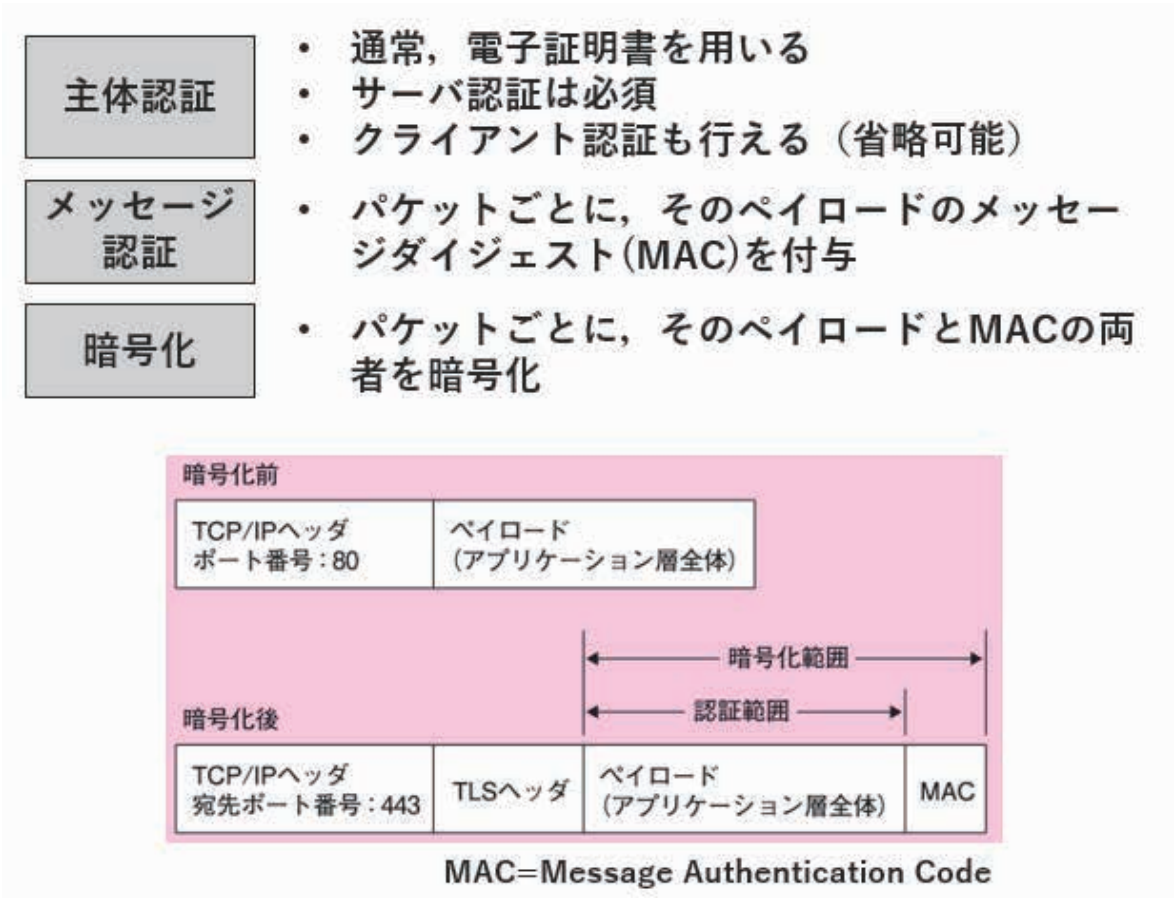
(*) smtp、pop3ではポート番号25, 110 のままで通信の
途中からTLSを用いた暗号化通信に切り替えることも可能

TLS は HTTP、FTP、SMTP、POP3 などさまざまな上位層プロトコルで使われますが、よく使われているのは HTTP です。通常、TLS を使用する場合はポート番号とプロトコル名が変わります。たとえば HTTP（ポート 80）は、TLS を使用するときは HTTPS(ポート 443)になります。

ただし SMTP､POP3 では通信の途中から TLS を用いた暗号化通信に切り替えることも可能であり、その場合はポート番号はそれぞれ 25, 110 のままで変わりません。

TLS で暗号化されるのはトランスポート層のペイロード部分、つまりアプリケーション層全体です。

21 提供されるセキュリティ・サービス



TLS が提供するセキュリティ・サービスには主体認証、メッセージ認証、暗号化の 3 つがあります。

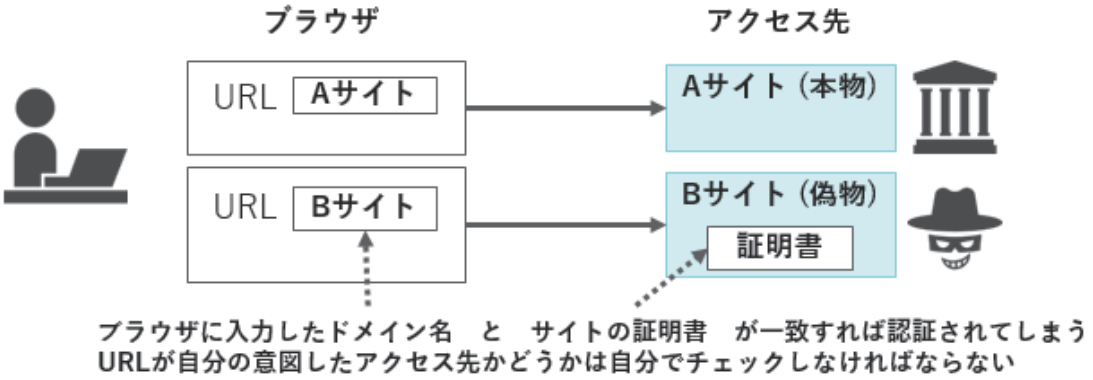
主体認証には通常、電子証明書を用います。サーバー認証に加えてクライアント認証も行えます。

パケットごとにペイロードのメッセージダイジェストを付与してメッセージ認証を行います。このメッセージダイジェストを MAC(Message Authentication Code，メッセージ認証コード)と呼びます。

パケットごとにペイロードと MAC の両者を暗号化します。

22 TLS 通信の安全性の限界

- サーバの電子証明書が認証するのは，あくまで通信相手の公開鍵の正当性
- 利用者は，自分の意図している通信相手が電子証明書に記載されている公開鍵の所有者と一致しているかを確認する必要がある



- ブラウザは，有効期限，失効の有無（失効リストを確認する機能を有効にした場合）などを確認して，電子証明書の有効性が疑われる場合に警告メッセージを出す。利用者はそれを無視してはならない

TLS 通信のセッションが確立したとしても、それが安全性を完全に保証するものではないことには注意が必要です。

サーバーの電子証明書が認証するのは，あくまで通信相手の公開鍵の正当性であり、サイト運営者が悪意のない者かどうかまでは保証しません。たとえば B サイトが A という正規サイトの偽物で利用者が意図せず B サイトにアクセスしていたとしても、ブラウザの URL 欄のドメイン名とアクセス先サイトの証明書記載のドメイン名が一致していれば警告は出ません。利用者は，自分の意図したアクセス秋「A」がブラウザの URL 欄に正しく入力されているかを自分で確認する必要があります。

ブラウザは，有効期限，失効の有無（失効リストを確認する機能を有効にした場合）などを確認して，電子証明書の有効性が疑われる場合に警告メッセージを出さなければならず、利用者はそれを無視してはなりません。

23 TLS 通信が規定する 4 種のプロトコル

- 1. アプリケーションデータプロトコル
  - アプリケーション通信を暗号化した通信
- 2. ハンドシェークプロトコル
  - TLSセッション確立するための通信
  - アプリケーションデータプロトコルの通信に先立って実施され,
  - 通信相手の主体認証と共通鍵の交換を行う
- 3. change cipher spec プロトコル
  - TLSセッション確立の最終段階でやり取りされる通信
  - セッション確立手順の一部であり、ハンドシェークプロトコルの途中で行われる
  - 便宜上、ハンドシェークの一部として説明する
- 4. アラートプロトコル
  - 警告やエラーを相手に伝えるための通信

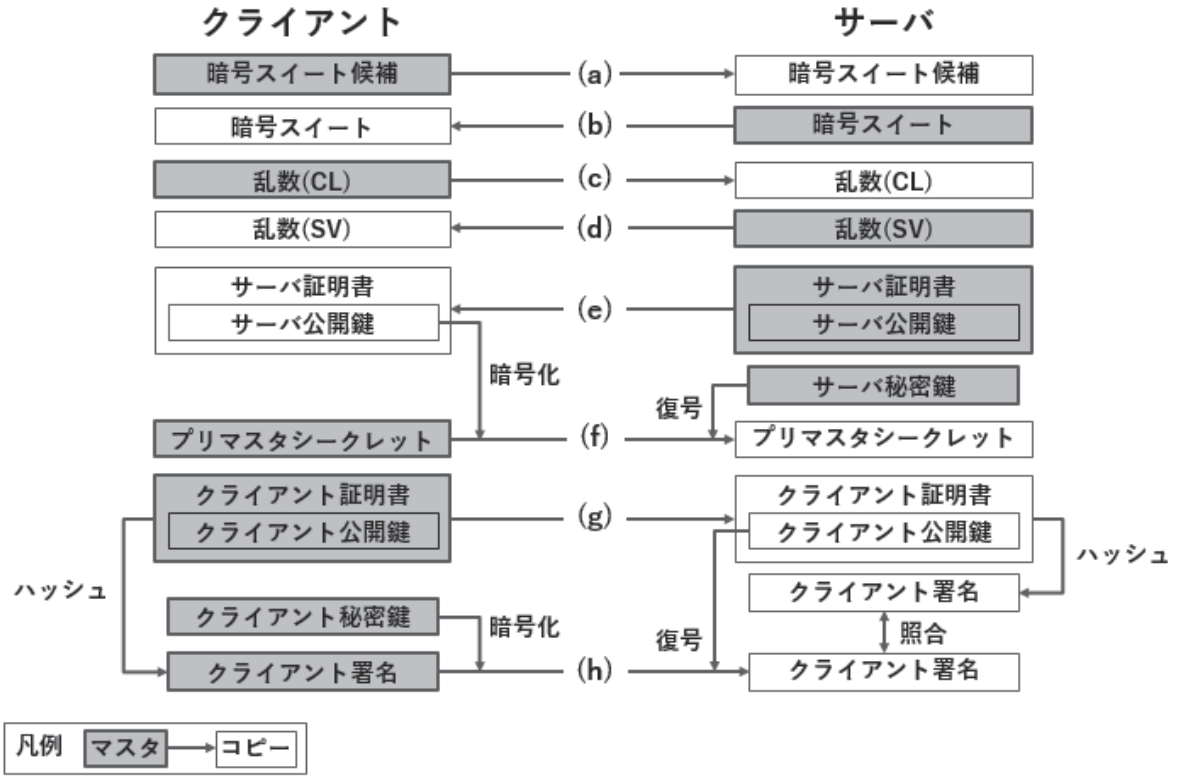
TLS の仕様は 4 種類の通信を規定しており、それぞれアプリケーションデータプロトコル、ハンドシェークプロトコル、change cipher spec プロトコル、アラートプロトコルと呼ばれています。

TLS の通信は、大まかに

- セッションの確立（ハンドシェークプロトコルおよび change cipher spec プロトコル）
- アプリケーション層の暗号化通信（アプリケーションデータプロトコル）

という順序で行われます。

24 TLS 通信パラメータの相関図



TLS 通信セッションを確立するために必要なパラメータの相関図を示します。
この図は左下の凡例のように、網掛けの箱がマスタ、白地の箱がコピーを表しています。マスタを持っている側がそれを送信すると反対側がそのコピーを得られます。たとえば(a)はクライアントが暗号スイート候補を送信してサーバーがそれを受信することを意味します。
実際のハンドシェイクのシーケンスとは異なりますが、通信セッションを確立する上での意味はこの図を先に見たほうがわかりやすいので、以下順次説明します。なお、図中の(a)～(h)は実際のプロトコル上で処理される順番とは一致しません。

(a)ではクライアントが対応可能な暗号スイートの候補をサーバーに伝えます。「暗号スイート」とは、暗号化とハッシュに用いるアルゴリズムの組み合わせのことです。TLS では RSA, DSA, AES, RC4, SHA-1, SHA-2, Diffie-Hellman などのアルゴリズムが規定されており、そのうちどれを優先して使用するか、禁止するかはクライアントとサーバーの双方で設定することができます。

サーバーは暗号スイート候補の提示を受けて実際に使用するスイートを決定して(b)でクライアントに送信します。

乱数(CL)はクライアントが生成する乱数、乱数(SV)はサーバーが生成する乱数です。これらの乱数は(c)、(d)で交換した後でプリマスタシークレットとともに暗号鍵を生成するために使われます。

(e)でサーバーがサーバー証明書をクライアントに送信すると、クライアントはアクセス先のドメイン名とサーバー証明書に記載されたドメイン名が一致しているかを確かめることによって、その証明書を認証します。

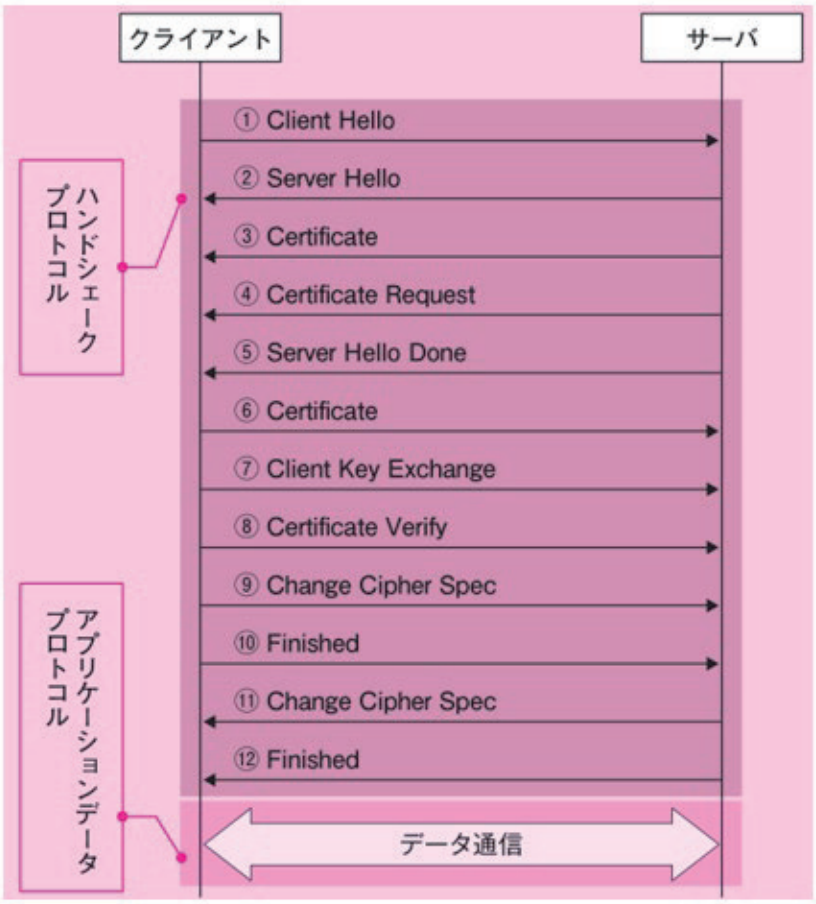
認証を終えたら(f)クライアントはプリマスタシークレットを生成しサーバー公開鍵で暗号化してサーバーに送信します。サーバーは自分の秘密鍵でそれを復号します。(f)の送信時は暗号化されているため、プリマスタシークレットを第三者に傍受されることはありません。プリマスタシークレットは乱数(CL)、乱数(SV)と合わせて暗号鍵生成に使われるタネとなる情報です。

クライアント認証が求められている場合、クライアントは(g)でクライアント証明書をサーバーに送信し、サーバーはその証明書を認証します。

(h)はクライアント認証の手順です。クライアント証明書は公開されているため誰もが入手できますし、サーバー証明書のようにドメイン名で相手を確認できないため、サーバーと同じ方法では認証できません。そこで、クライアント証明書を送る際は、証明書のハッシュ値を計算した上で、正規のクライアントしか持っていない秘密鍵で暗号化しクライアント署名として送信します。サーバー側でクライアント証明書の公開鍵で復号したうえで、受信したクライアント証明書のハッシュ値を独自に計算して照合することにより、通信相手がクライアント証明書に適合する秘密鍵を持つ正規のクライアントであることを認証できます。

TLS 通信では、このような方法によってセキュリティの保たれた通信路を開設します。

25 TLS 通信開始のハンドシェイク手順



それでは具体的なハンドシェークプロトコルを見ていきましょう。

①Client Hello では、暗号スイートの候補とクライアント側の乱数を送信します（前ページ(a)と(c)に該当）。
②Server Hello では、決定した暗号スイートとサーバー側の乱数を送信します（前ページ(b)と(d)）。
③Server Certificate でサーバー証明書を送信し（前ページ(e)）、④Certificate Request でクライアント証明書を要求します。ただし④は省略されることがあります。
⑤Server Hello Done はサーバー側からすべてのハンドシェークメッセージを送信したことを通知しています。
⑥は④への応答でクライアント証明書を送信します（前ページ(g)）。④が省略された場合は⑥も省略されます。
⑦はプリマスタシークレットの交換です。クライアント側でプリマスタシークレットを計算し、サーバーの公開鍵で暗号化してサーバーに送信します（前ページ(f)）。
⑧はクライアント署名の送信です（前ページ(h)）。

ここまでの手順で TLS 通信に必要なパラメータの交換は完了するため、これ以後暗号化通信モードに切り替える処理を行います。

⑨は②で選定された暗号化スイートの使用を開始することを通知し、以後クライアント側から送信するメッセージはすべて暗号化されたものとなります。
⑩は暗号通信開始後最初に送るメッセージで、これまで交換したメッセージやパラメータを組み合わせたものをハッシュ化したものを送信します。

⑪、⑫は、⑨、⑩と同じ処理をサーバー側でも行ったものです。

⑩と⑫の Finished メッセージを相互に検証すると、クライアントとサーバーの双方で TLS 通信のパラメータを正しく共有できていることを確認出来るため、これ以後はアプリケーションデータの通信を開始できます。

TLS の仕様上，複数のハンドシェークプロトコルのメッセージを 1 個のパケットに格納して送信することができます。例えば，このシーケンスについては，①，②〜⑤，⑥〜⑩，⑪〜⑫という 4 個のパケットのやり取りで実行できます。

26 演習問題

問 1

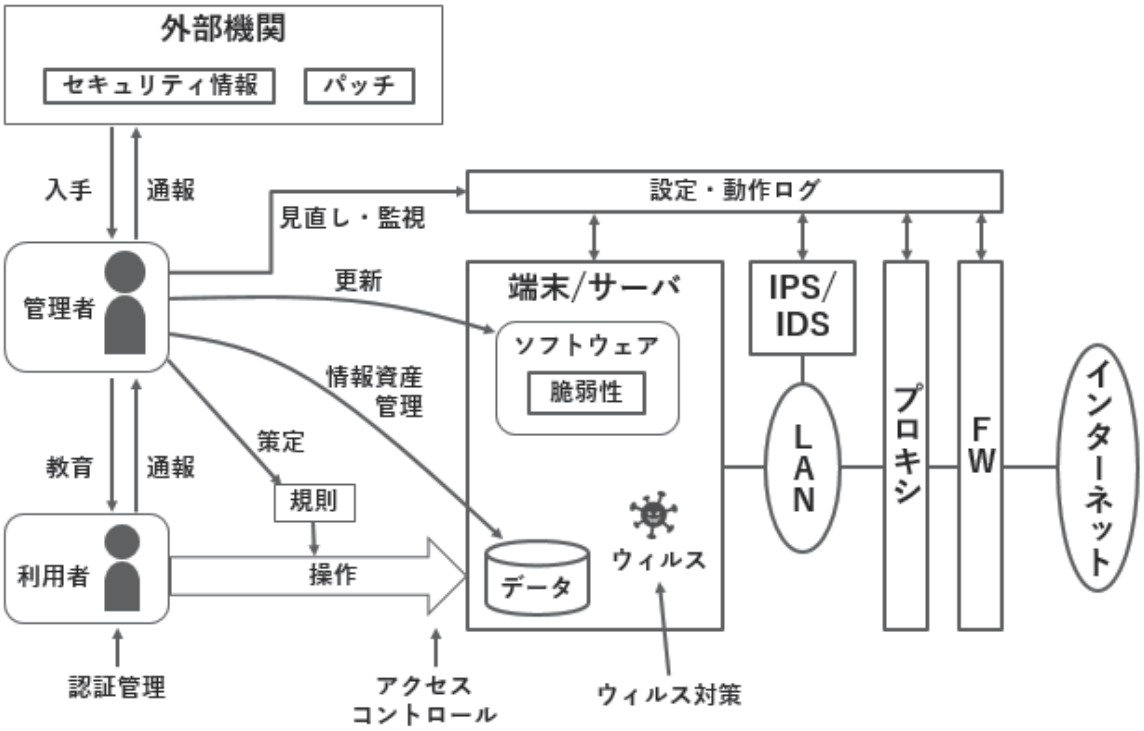
次に示す観点に基づいて、IPsec と TLS を比較してください。

観点	IPsec	TLS
暗号化できるプロトコルの種類は何か		
主体認証の機能があるか		
メッセージ認証の機能があるか		
リプレイ攻撃を拒否する機能があるか		
クライアント端末に専用ソフトウェアをインストールする必要があるか		

第4章.

不正アタック対策

1 情報セキュリティ対策の基本



上図は情報セキュリティ対策の基本的な事項をまとめたものです。
会社の執務環境には多くの端末やサーバーがあり、そこにはデータがありソフトウェアが稼働していて、それを利用者が操作します。端末/サーバーは LAN で接続されてプロキシやファイアウォール（FW）を通してインターネットに接続されています。

この環境下で安全に業務を続けるためにはさまざまなセキュリティ対策を施さなければなりません。大きな項目としては、FW については「5.2 節　ファイアウォール」で、プロキシについては「5.3 節　プロキシサーバ」で、IPS/IDS（侵入検知・防御システム）については「5.4 節　侵入検知・防御システム」で、ウイルス対策については「5.5 節　ウイルス対策」で扱います。

さらにその他にも様々な対策が必要ですので下記にまとめます。

脆弱性対策・ソフトウェア更新

ソフトウェアにはさまざまな「脆弱性」があります。通常は脆弱性が発見され次第ソフトウェアベンダーから修正プログラム（パッチとも呼ばれる）が提供されるので、パッチを入手してソフトウェアの更新をしなければなりません。

セキュリティ情報入手

脆弱性等に関する最新のセキュリティ情報を入手し対策を講じる必要があります。

情報資産管理

どこにどんなデータがあるかを把握し、不要なものを削除し、必要なものには適切なアクセス権限の設定や保全措置を取ることを言います。個人の端末に無秩序に保存されている個人情報等を隅から隅まで洗い出すことが重要です。

認証管理

利用者を正しく認証するために必要な措置を言います。ID の使い回しや不適切なパスワード使用の防止、失効 ID の削除等が該当します。

アクセスコントロール

認証された利用者による、端末/サーバー（あるいはそこで稼働するサービスや保存されているデータ）へのアクセスを管理することです。利用者に適切な権限を付与し、アクセス制限が正しく働くように設定するなどの管理を行います。

規則の策定・教育

セキュリティ上知っておくべき知識や運用のルールをまとめて「規則」として策定し、それを利用者に教育します。「規則」から「操作」への矢印は、利用者が規則に従って操作を行うことを意味します。セキュリティポリシーを規定し就業規則や秘密保持契約等にも明示しておくことは内部不正に対する「心のブレーキ」としても重要です。

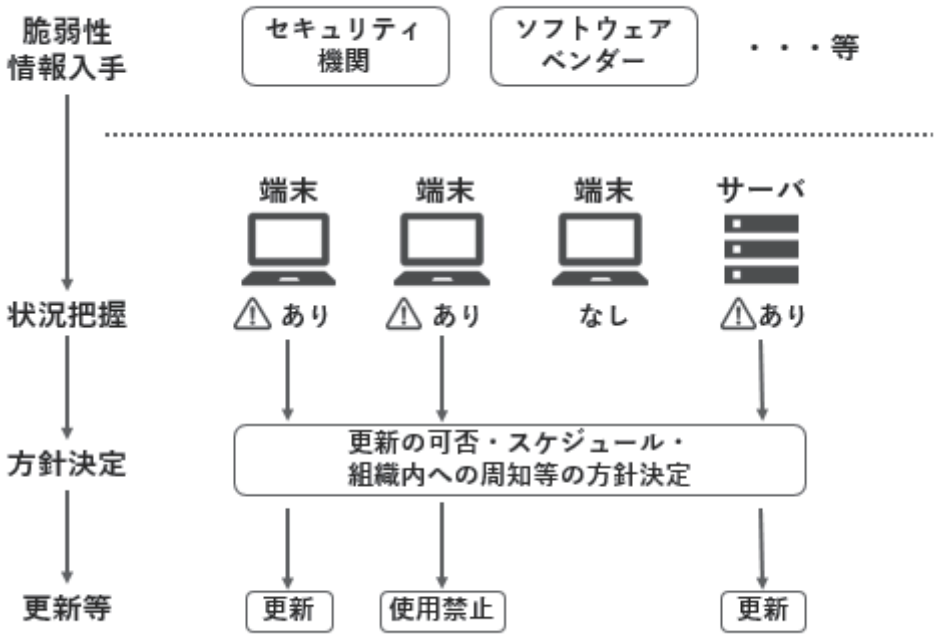
設定・動作ログの見直し・監視

端末/サーバー、IPS/IDS、プロキシ、FW 等はいずれも何らかの設定に従って稼働し、動作ログを残します。ソフトウェアのインストール直後等の初期状態ではセキュリティの弱い設定になっていることが多いため、設定の見直しおよび動作ログを監視して異常な兆候をつかむなどの方法をとります。

通報

セキュリティ事案に気づいた場合にはためらわずに管理者や関係機関に通報し相談できるような組織体制・組織文化を醸成しなければなりません。

2 ソフトウェアの更新（脆弱性対策）



ソフトウェアの脆弱性については､該当するソフトウェアベンダーやセキュリティ機関から脆弱性情報を入手し、社内で使用している端末/サーバー等に必要な対処を行います。

状況把握

多くの場合、脆弱性は特定のソフトウェアや OS に存在します。そこで組織内のどの端末/サーバーに脆弱性があるのか、その状況を把握します。

方針決定

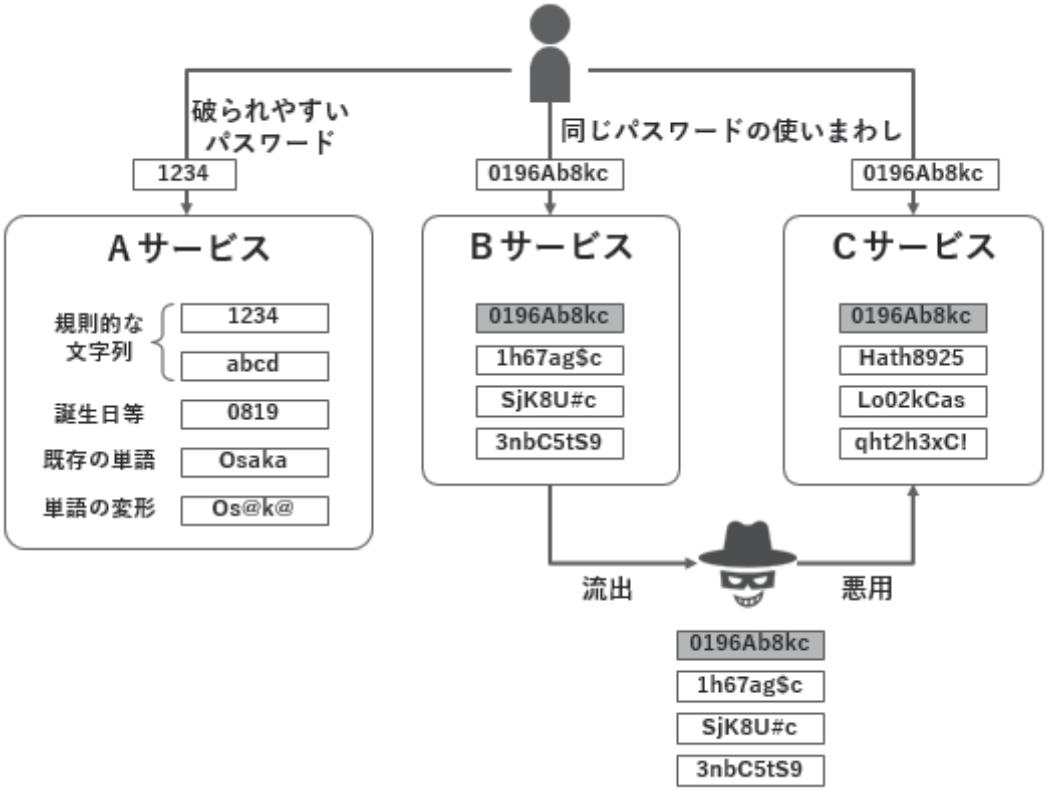
ソフトウェアの更新が可能か否か、またそのスケジュール等の方針を決定し組織内に周知します。

更新等

対象の端末/サーバーのソフトウェア更新を行います。更新ができない場合は使用禁止にする、隔離環境でのみの使用を許可するなどの処置をとります。

状況把握や更新等の処置を組織内の多数の端末/サーバーについていちいち手作業で行うのは現実的ではないため、端末は自動更新されるように設定しておくのが基本です。また、管理台数の多い組織では IT 資産管理ツールを使用するのが一般的です。

3 パスワードの適切な管理・認証強化



破られやすいパスワードを避ける

規則的な文字列、誕生日等、単語として辞書に存在する言葉、それらの単純な変形などを行ったパスワードは脆弱つまり破られやすいため避けなければなりません。破られにくいパスワードを作るには、8 文字以上の文字列でアルファベットの小文字や大文字、数字や記号を組み合せます。社内で運用するサービスについては、脆弱なパスワードを使用できないような仕組みを作り、強靭なパスワードを強制することが望まれます。

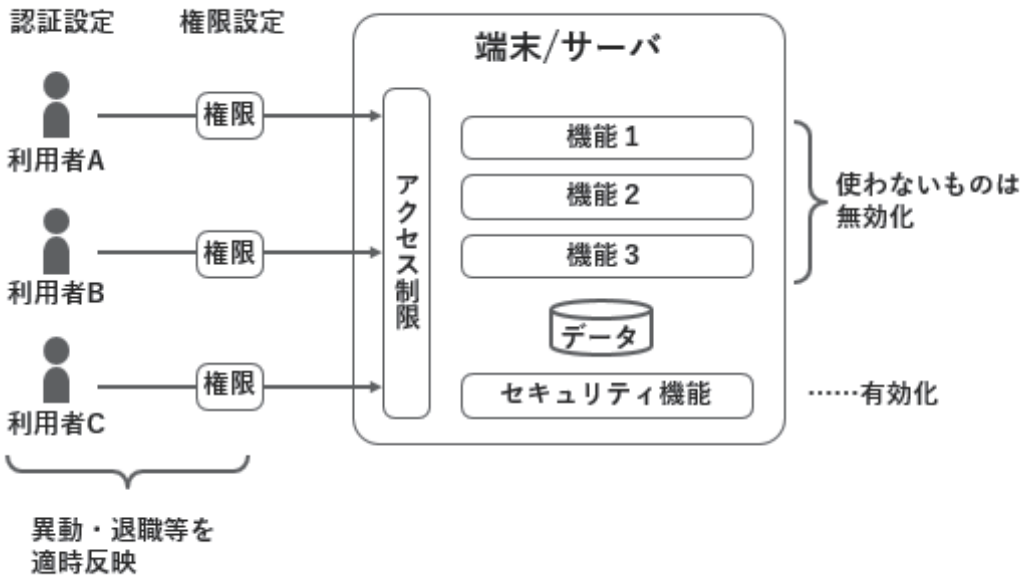
パスワードの管理方法

強靭なパスワードは一般に記憶しづらいためなんらかの形で記録（メモ）する必要がありますが、今度はその記録が流出するケースがあるため、パスワードを適切な方法で管理することも重要です。

パスワードの使い回しを避ける

強靭なパスワードを設定していたとしても、同じ ID とパスワードを複数のウェブサービスで使い回していると、どこか一つのサービスから ID とパスワードが流出した場合にはそれを悪用した「パスワードリスト攻撃」に晒されます。図では B と C で同じ「0196Ab8kc」というパスワードを使用しているため危険です。サービス毎に異なるパスワードを設定しておく必要があります。

4 設定の見直し



機能の有効化・無効化

端末/サーバーには複数の機能（サービス）がありますが、初期設定で稼働している機能が実際には必要ない場合も少なくありません。稼働している機能が多いほどセキュリティホールも増えるため、使わないものは無効化しておきます。逆に、セキュリティ機能についてはできるだけ有効化しておきます。

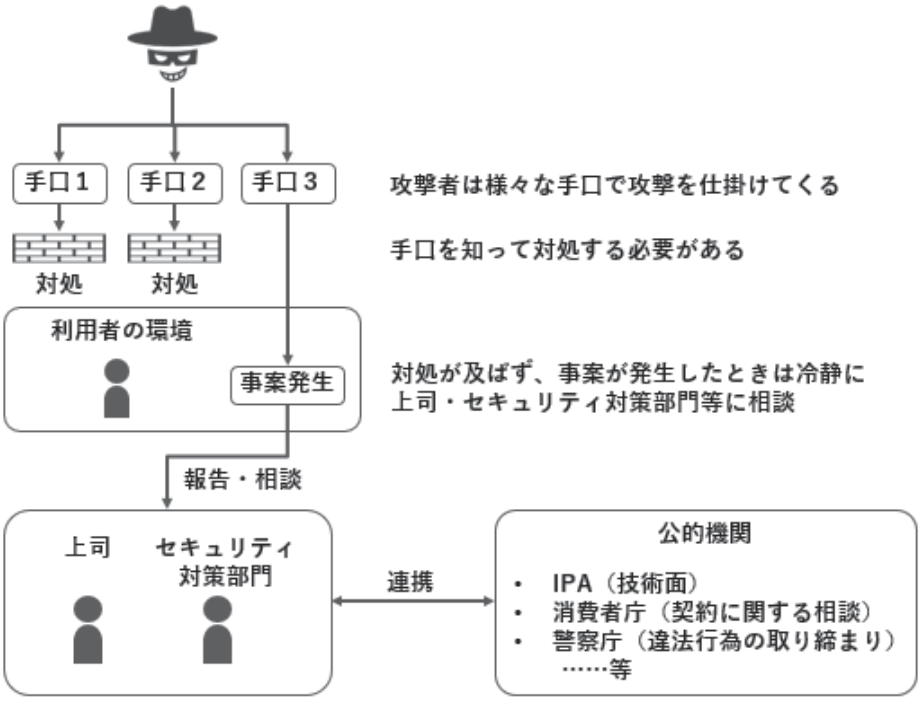
認証設定・権限設定

サービスを利用するためのアカウントは基本的に利用者毎に別のアカウントを発行します。不正ログインを防ぐには、パスワードや ID カード等を適切に管理する必要があります。また、利用者に付与する権限は個人ごとに明確に決定し、それをアカウントにひもづけてシステム的にアクセス制限を行う仕組みを導入します。

アカウントの見直し

異動・退職等が発生した時はそれに応じて速やかにアカウントの抹消や権限変更の処置をとります。

5 脅威・手口を知ることが重要



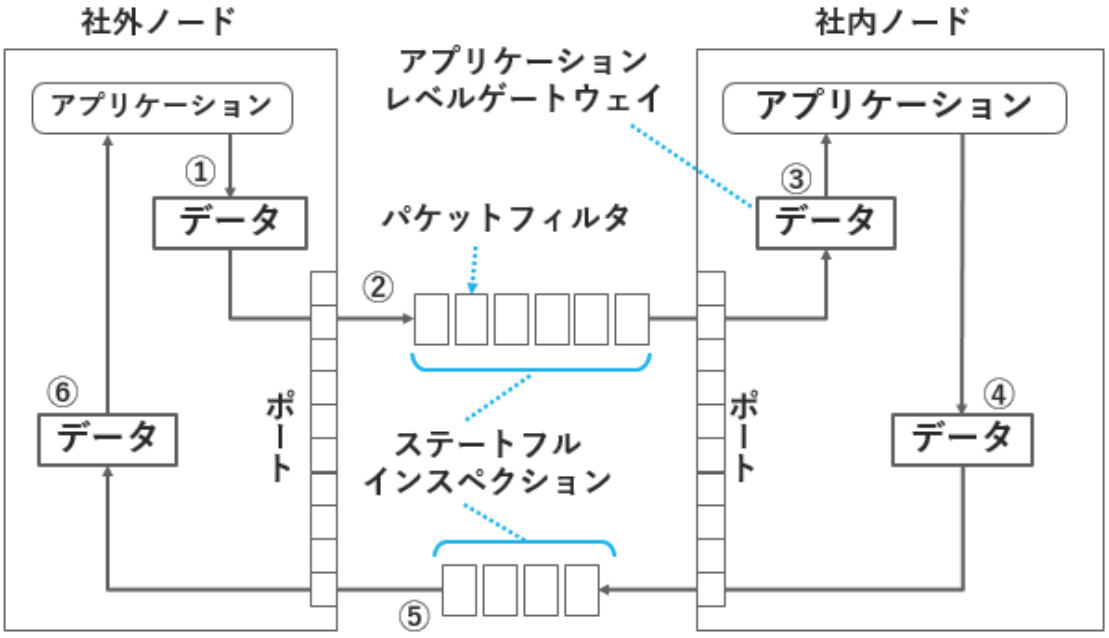
攻撃者はさまざまな手口で攻撃を仕掛けてきます。その手口の中にはメールや Web サイトで利用者を言葉巧みに騙して危険な行動を取らせるものもあります。

- 取引先や組織内の関係者を語ってメールの添付ファイルを開けさせる手口
- 会費無料と謳っておきながら突然高額な請求画面を表示するワンクリック請求と呼ばれる手口
- 有用なソフトと偽ってウイルス等をインストールさせる手口

これらの手口の中にはシステムで防ぐのが困難なものもあるため、利用者自身も知識を持って対処していかなければなりません。（例：添付ファイルや外部リンクのあるメールに注意する、Web サイトが偽物でないかどうか確認する、など）

また、対処が及ばずセキュリティ事案が発生した場合は、慌てると不適切な行動により二次三次の被害を広げてしまいます。万一の時は速やかに上司やセキュリティ対策部門に報告します。セキュリティ対策部門を中心に組織として公的機関と連携して事後対応を進める必要があります。セキュリティ管理者は一般の利用者がそのような行動を取れるように、必要な教育および組織体制・組織文化の整備を行なわなければなりません。ミスをした個人の責任追及に躍起になるような組織では、こうした事案が発生しても隠蔽されやすく、報告が遅くなり被害を広げがちです。セキュリティ対策の実効性には組織文化も大きく影響します。

6 トラフィック制御メカニズム概要

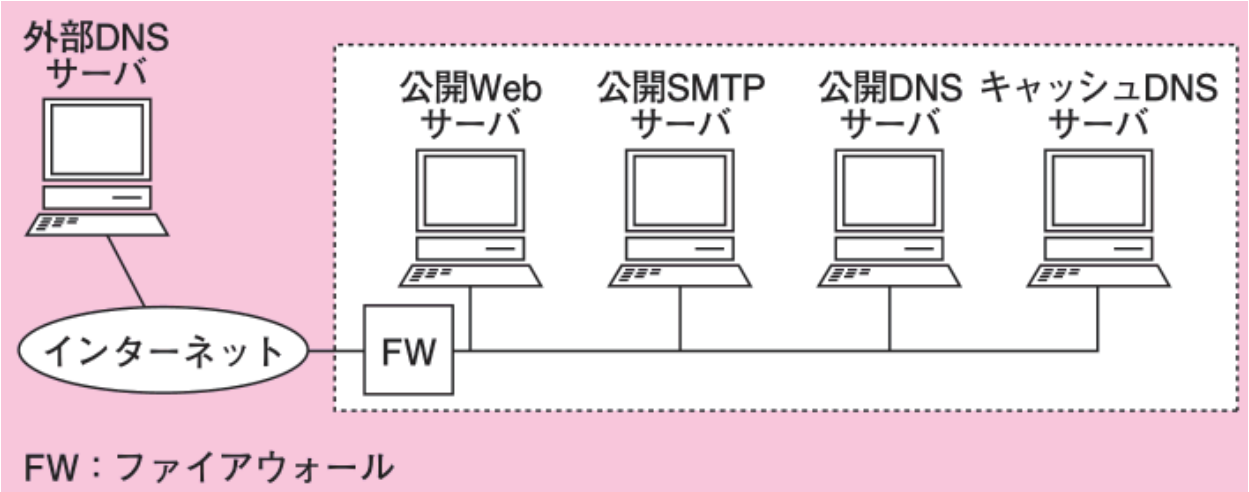


ファイアウォール（firewall）は，外部ネットワークと内部ネットワークの間に置いて通過するトラフィックを制御することによりセキュリティを確保する仕組みです。ファイアウォールのトラフィック制御方式はパケットフィルタリング，ステートフルインスペクション，アプリケーションレベルゲートウェイの 3 種類に大別することができます。

上図は社外ノードと社内ノードの間で通信を行う場面の模式図です。社外ノードのアプリケーションから出力された①データは、②パケットに分割されて通信回線上を流れ、宛先の社内ノードのポートから入って再び③データとして組み立てられてアプリケーションに渡ります。返信のデータは同様に④⑤⑥と逆のルートをたどって行きます。

ファイアウォールで最も基本となるパケットフィルタは、パケット単体を検査して通過を許可/拒否する機能です。パケットの送信者・受信者アドレス、ポート番号、プロトコル、向きなどを基準にルールを設定してフィルタリングを行います。それに対して、ステートフルインスペクションは送信/受信の流れも含めたパケットのシーケンスを検査し、アプリケーションレベルゲートウェイはアプリケーションに渡るデータを検査します。

以下、パケットフィルタリングの設定を行う例を示します。下記のような構成のネットワークを例に取ります。



このネットワークでパケットフィルタリングの設定をした例が下記になります。

表：パケットフィルタリングの設定例

	方向	送信元IPアドレス	宛先IPアドレス	プロトコル	SYNビット	ACKビット	送信元ポート番号	宛先ポート番号	通信動作
①	内向き	外部	内部	TCP	任意	オン	任意	任意	接続
②	外向き	内部	外部	TCP	任意	オン	任意	任意	接続
③	外向き	内部	外部	TCP	オン	オフ	任意	任意	接続
④	内向き	外部	公開Web	TCP	オン	オフ	任意	80	接続
⑤	内向き	外部	公開SMTP	TCP	オン	オフ	任意	25	接続
⑥	外向き	キャッシュDNS	外部	UDP			任意	53	接続
⑦	内向き	外部	キャッシュDNS	UDP			53	任意	接続
⑧	内向き	外部	公開DNS	UDP			任意	53	接続
⑨	外向き	公開DNS	外部	UDP			53	任意	接続
⑩	内向き	外部	内部	任意	任意	任意	任意	任意	切断
⑪	外向き	内部	外部	任意	任意	任意	任意	任意	切断

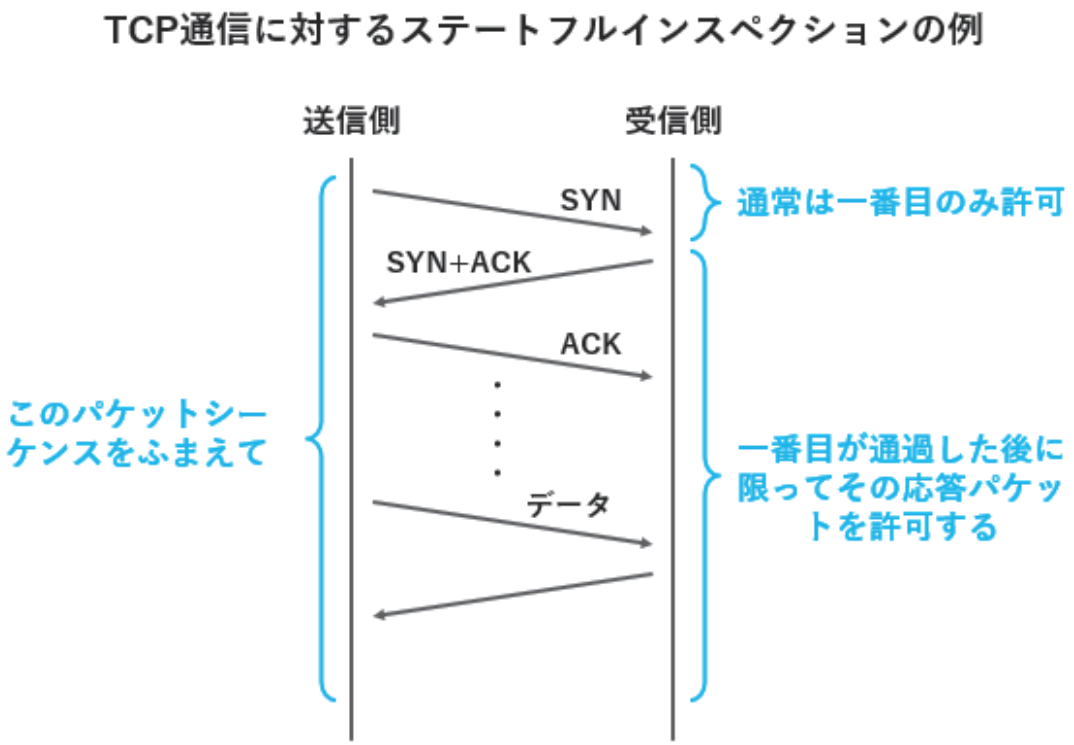
注：「プロトコル」はIPヘッダのプロトコル番号に対応した項目で，TCP，UDP，ICMPが該当する。

このような設定により、下記 A〜F の通信のみを許可し、それ以外の通信はすべて切断することができます。

通信	クライアント	サーバ	通信プロトコル	適用される行
A	内部	外部	任意の TCP 通信	①, ②, ③
B	外部	公開 Web サーバ	HTTP	①, ②, ④
C	外部	公開 SMTP サーバ	SMTP	①, ②, ⑤
D	公開 SMTP サーバ	外部	SMTP	①, ②, ③
E	キャッシュ DNS サーバ	外部	DNS	⑥, ⑦
F	外部	公開 DNS サーバ	DNS	⑧, ⑨

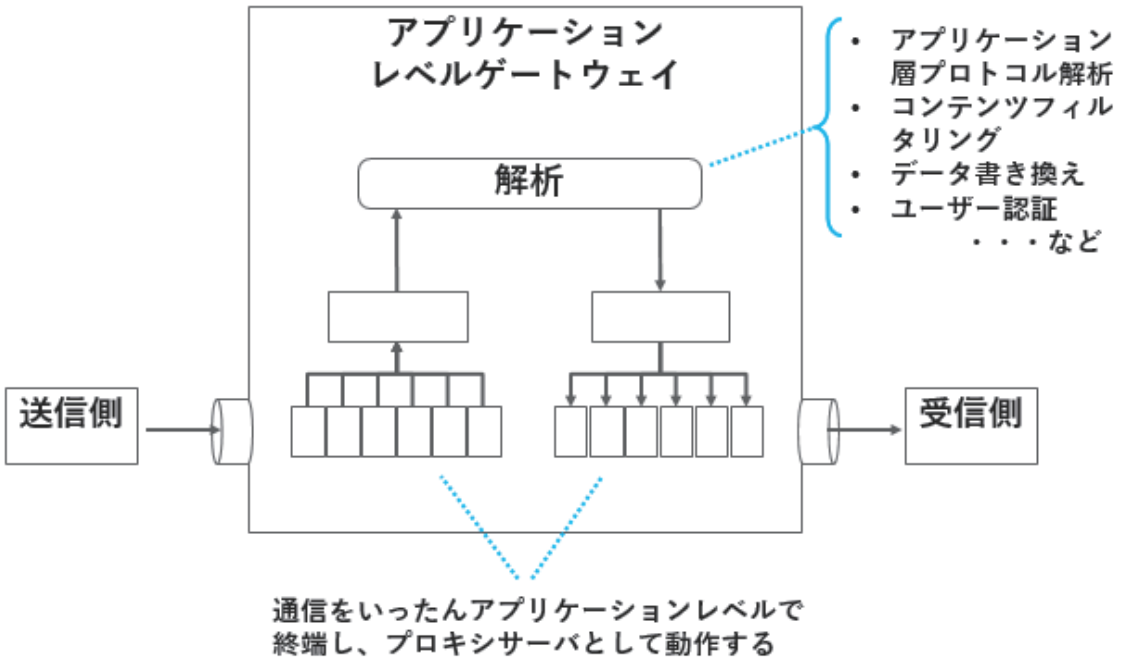
このように「原則としてすべてのポートを塞ぎ、必要な通信プロトコルとポートのみを開けておく」のがパケットフィルタリングの基本です。

7 ステートフルインスペクション



ステートフルインスペクションはパケット単体ではなく、送信・受信にともなう一連のパケットの流れを検査します。一般に、一続きのデータを送る際は最初のパケットの性質によって後続のパケットの性質が返信分も含めてある程度定まるため、「A タイプのパケットが通過した後に限って B タイプのパケット通過を許可する」のようなルールを設定すると、パケット単体のみを検査するパケットフィルタリングよりも厳格なセキュリティを実現できます。このように「A タイプパケットが通過する前か、後か」のような「状態（ステート）」の違いによってルールを変えるのがステートフルインスペクションです。

8 アプリケーションレベルゲートウェイ

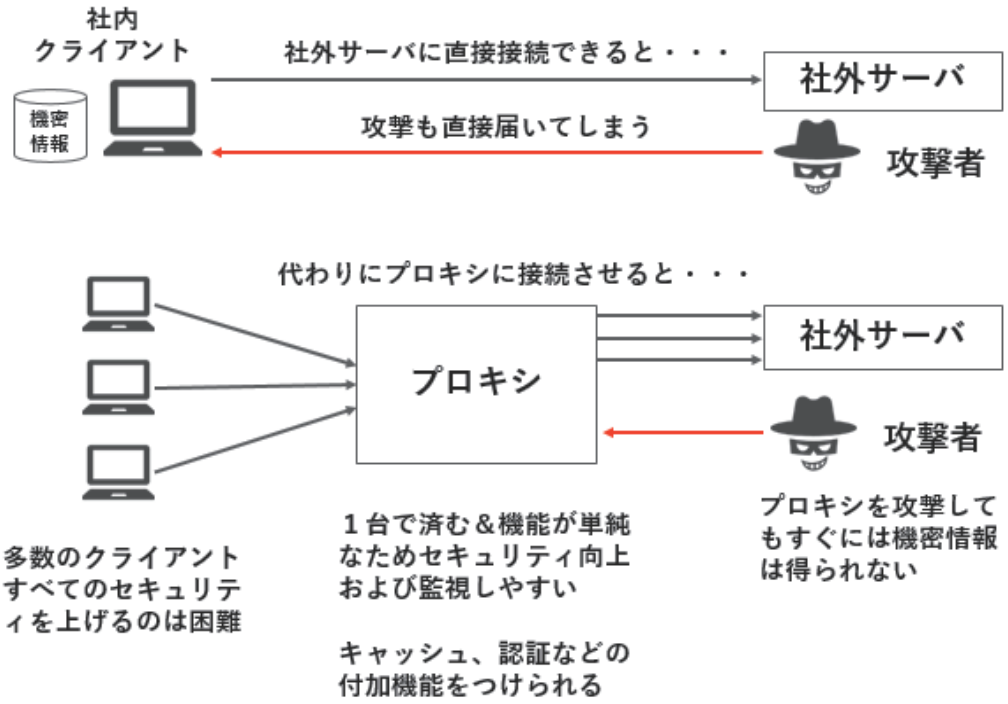


アプリケーションレベルゲートウェイはパケットではなくアプリケーションに渡るデータを検査します。アプリケーションレベルで動作するため、通信をいったん終端してプロキシサーバとして動作する仕組みになります。

アプリケーション層のプロトコルを解析するため、単にパケットの通過/拒否にとどまらず、ユーザー認証、コンテンツフィルタリング、データ書き換えなどさまざまな機能を付与することができます。

近年では，1 台の機器の中に，ファイアウォール機能，IPS 機能，アンチウイルス機能，コンテンツフィルタリング機能，VPN 機能などの様々なセキュリティ機能を搭載したものが市場に出まわっています。このような機器を UTM（Unified Threat Management）といいます。

9 プロキシサーバの動作イメージ



プロキシは「代理」という意味を持ちます。プロキシサーバは，クライアントに代わってインターネット上の目的のコンテンツ（Web ページなど）を取得する役割を担います。

プロキシなしで社内クライアントから社外サーバーに直接接続できると、攻撃者からの攻撃も直接クライアントに届いてしまいます。この場合、クライアント端末のセキュリティレベルを上げなければなりませんが、多数存在する端末すべてのセキュリティを上げるのは困難です。

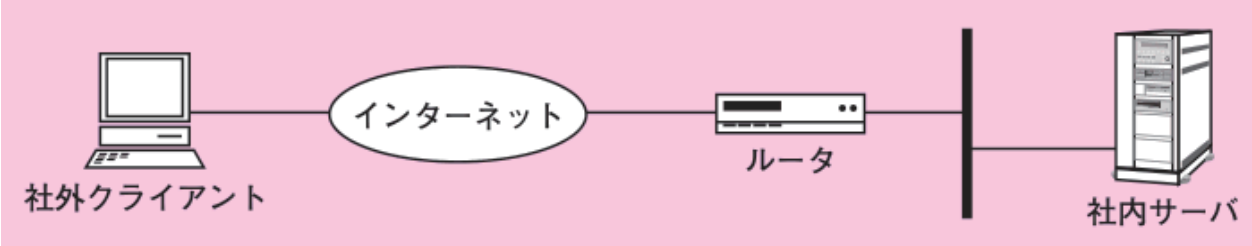
そこで、社内クライアントから直接インターネットに出ることを禁止して必ずプロキシを通すようにすると、攻撃者からの攻撃もいったんプロキシが受けることになりますが、攻撃者にとってはプロキシを攻撃してもすぐには機密情報は得られません。さらに、プロキシは 1 台で済むうえに機能が単純なためセキュリティの向上・監視がしやすくなります。プロキシにはキャッシュや認証などの付加機能を搭載することも可能です。

【付加機能の例】

キャッシュ機能	クライアントからリクエストを受けたとき，対象となるコンテンツがプロキシサーバにキャッシュされていれば，それを送り返す。同じコンテンツを再取得する必要がなく，レスポンスタイムが短縮される
先読み機能	参照中の Web ページに含まれるリンク情報を用いて，利用者が次に読み込む可能性のある情報を先読みし，キャッシュに蓄積しておく

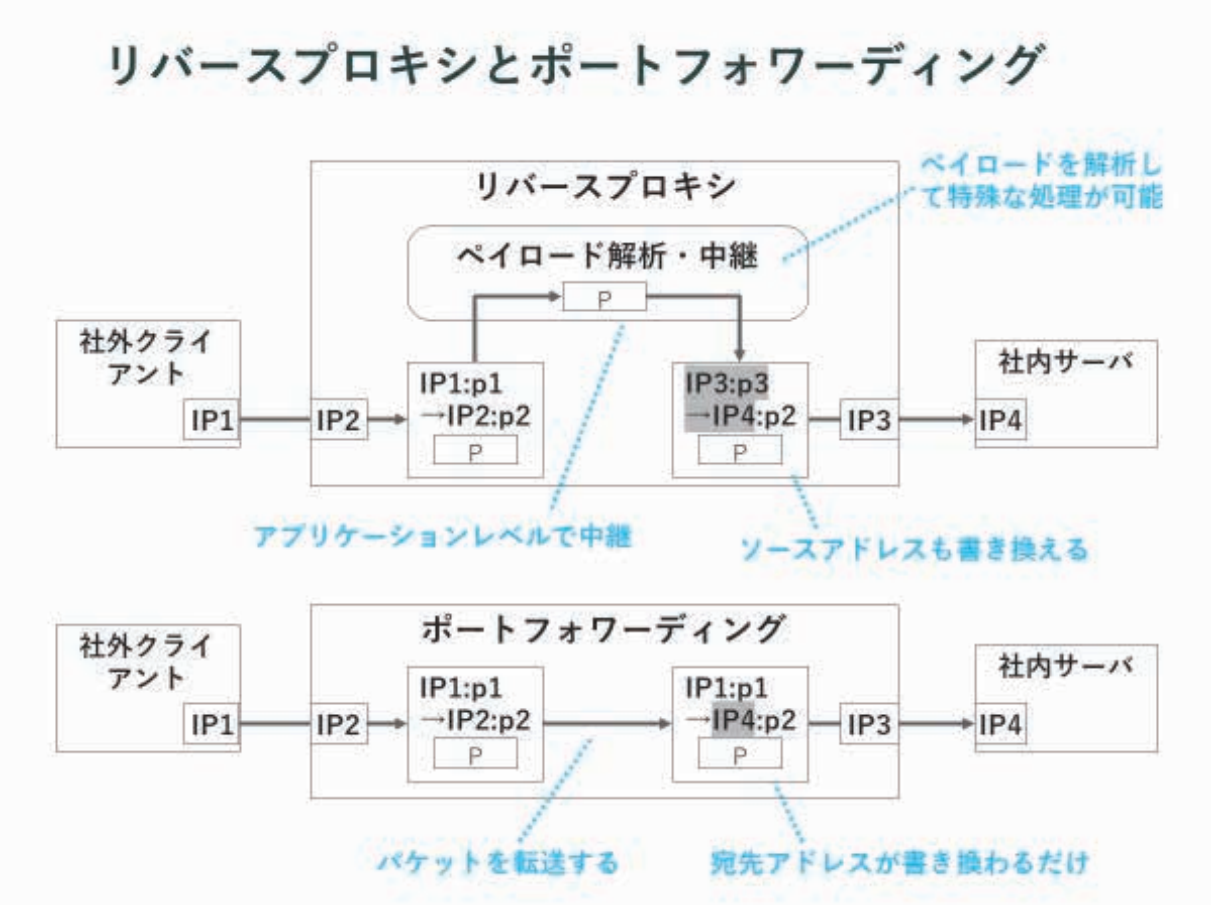
認証機能	ブラウザがプロキシサーバを経由してインターネットにアクセスする際，その通信に先立ち，強制的に利用者認証を行わせる
ログ機能	アクセス先 URL、（認証機能をもつ場合は）認証の成否を記録します。ウイルスが外部と通信するときは認証に失敗するので、ログを分析することでウイルスの発見につながります

次に示すネットワーク構成で、ルータの内側にある社内 Web サーバ（プライベートアドレスで運用）を公開して社外クライアントからのアクセスを受け付ける場合、主に静的 NAT、リバースプロキシ、ポートフォワーディングの 3 種類の方法があります。いずれもルータがその役割を果たします。



静的 NAT は、ルータの公開アドレスとは別に社内 Web サーバー用の公開アドレスをルータの外部インタフェースに割り当てておき、そのアドレスへのアクセスが来たら社内 Web サーバーのプライベートアドレスに変換してパケットを転送する方法です。

リバースプロキシとポートフォワーディングの動作モデルが下記のようになります。



IP1 は社外クライアントのアドレス、IP2 はルータの外部アドレス、IP3 はルータの内部アドレス、IP4 は社内サーバーの内部アドレスとします。p2 は社内 Web サーバー用のポートで、ルータは p2

ポート宛のアクセスがあった時はそれを社内 Web サーバーに転送するものとします。この場合の転送メカニズムにはリバースプロキシとポートフォワーディングの 2 種類があります。

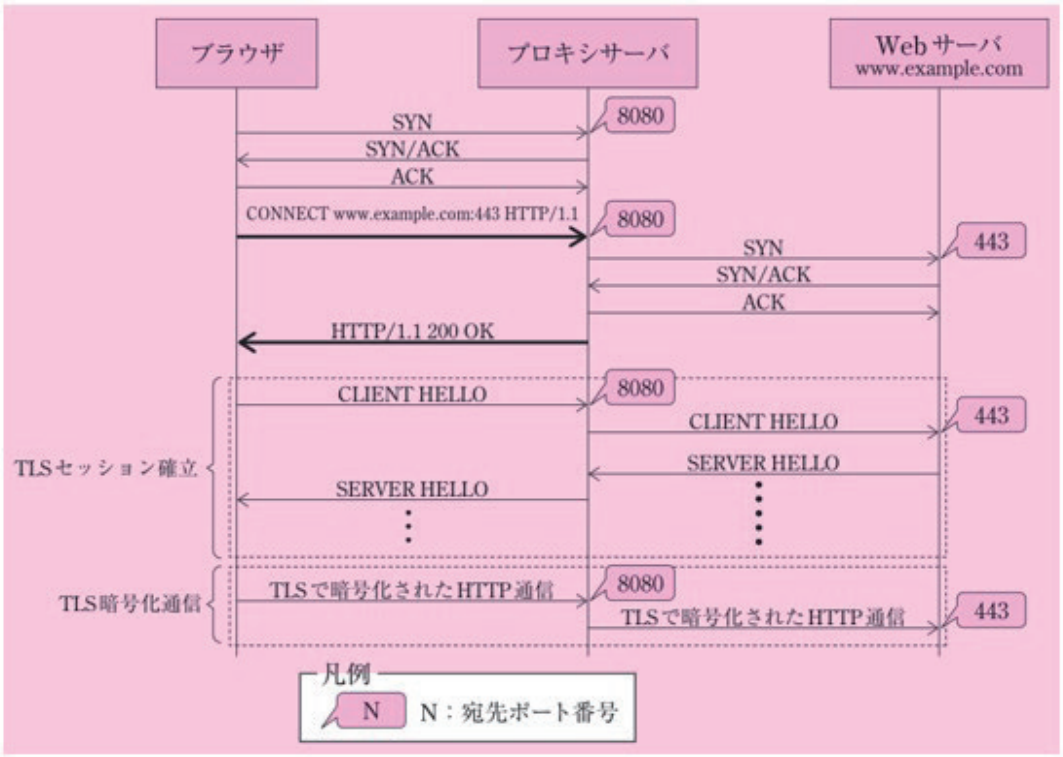
リバースプロキシは通信をいったん終端し、アプリケーションレベルでパケットのペイロードを解析し新たなパケットを作って中継する方法です。新たなパケットは送信元アドレスと宛先アドレスの双方が書き換わります。この方式ではペイロードを解析するため、特殊な処理が可能になります。

通常のプロキシは内部から外部へのアクセスに用いるものでしたが、リバースプロキシは「リバース（逆）の名前の通り外部から内部への逆方向で用いるプロキシです。外部から公開サーバーのオリジナルコンテンツに直接アクセスさせないことによる改ざん防止、キャッシュによる応答速度の向上、及び複数のサーバーでの負荷分散を行う目的で用いられます。

ポートフォワーディングは通信を終端せずにパケットのあて先アドレスだけを書き換えて転送します。これは静的 IP マスカレードとも呼ばれる方法です。

リバースプロキシ、ポートフォワーディングのいずれにしても、外部に対してはあたかもルータが公開 Web サーバーであるかのように見せかけることができます。

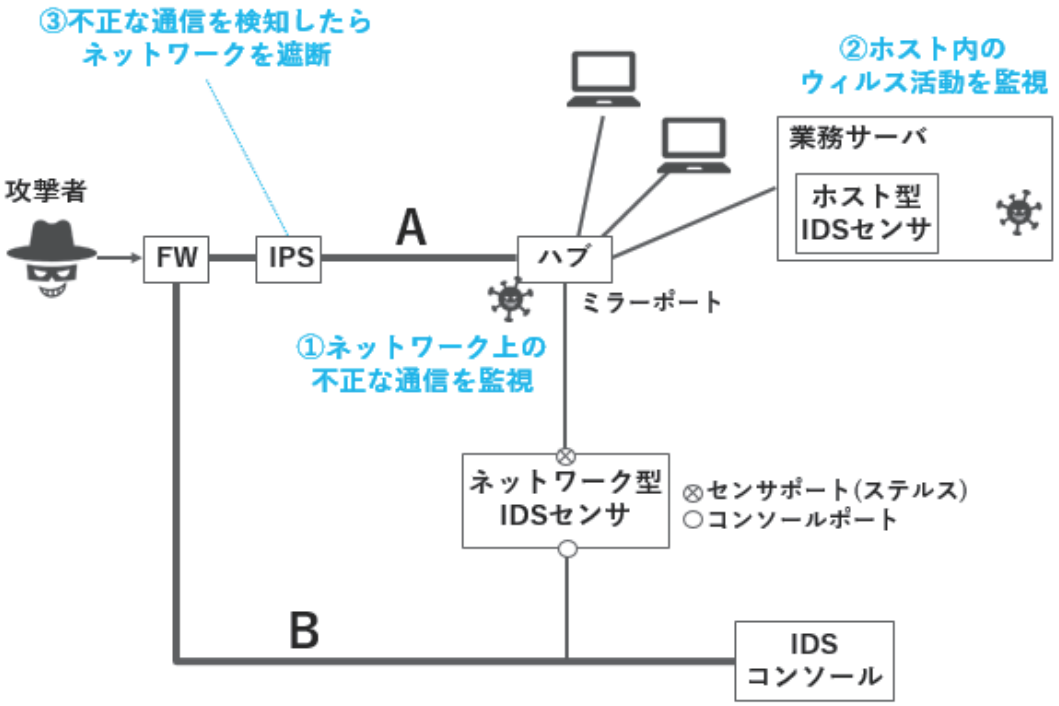
10 TLS 通信のトンネル処理



プロキシサーバを経由して PC と Web サーバー間で TLS 通信を行うことができます。このとき，PC のブラウザはプロキシサーバに CONNECT メソッドを発行します。メソッドの中に，TLS 通信の接続先となる Web サーバーが指定されています。CONNECT メソッドを受信したプロキシサーバは，PC と Web サーバー間の TLS 通信を中継します。このとき，TCP コネクションは，ブラウザとプロキシサーバ間，及び，プロキシサーバと Web サーバー間の二つがあります。プロキシサーバは両者の間の TCP データをそのまま転送しているだけで，TLS セッションは PC と Web サーバー間で確立されています。

TLS セッションの確立後はブラウザ～Web サーバー間の通信は暗号化されるためプロキシサーバは内容を解読できません。したがって、キャッシュ、先読みなどのアプリケーションレベルの付加機能は無効になります。

11 侵入検知・防御システム



侵入検知システム（IDS：Intrusion Detection System）は不正アタックを検知して管理者に通知し、侵入防御システム(IPS：Intrusion Prevention System)は検知に加えて防御（不正アタックの遮断）を行うシステムです。FW では遮断できない不正アタックが発生した場合や、内部ネットワークにコンピュータウイルス等の不正なプログラム（以下、ウィルスと総称）が活動している場合に役立ちます。

IDS

IDS は監視対象によってホスト型とネットワーク型に分かれます。
上図は FW 内部に業務サーバーや端末が稼働する A セグメントとネットワーク管理用の B セグメントという 2 つの LAN が引かれている構成を想定した模式図です。

ネットワーク型 IDS センサは A セグメントを監視します。A セグメントを使うノードすべてを監視対象にできますが、①ネットワーク上の不正な通信のみを監視するため、ホスト内のウイルス活動を直接検出することはできません。
ホスト型 IDS センサはサーバーや端末等のホスト上で稼働するソフトウェアで、②ホスト内のウイルス活動を監視できますが、インストールしたホスト以外の監視はできません。

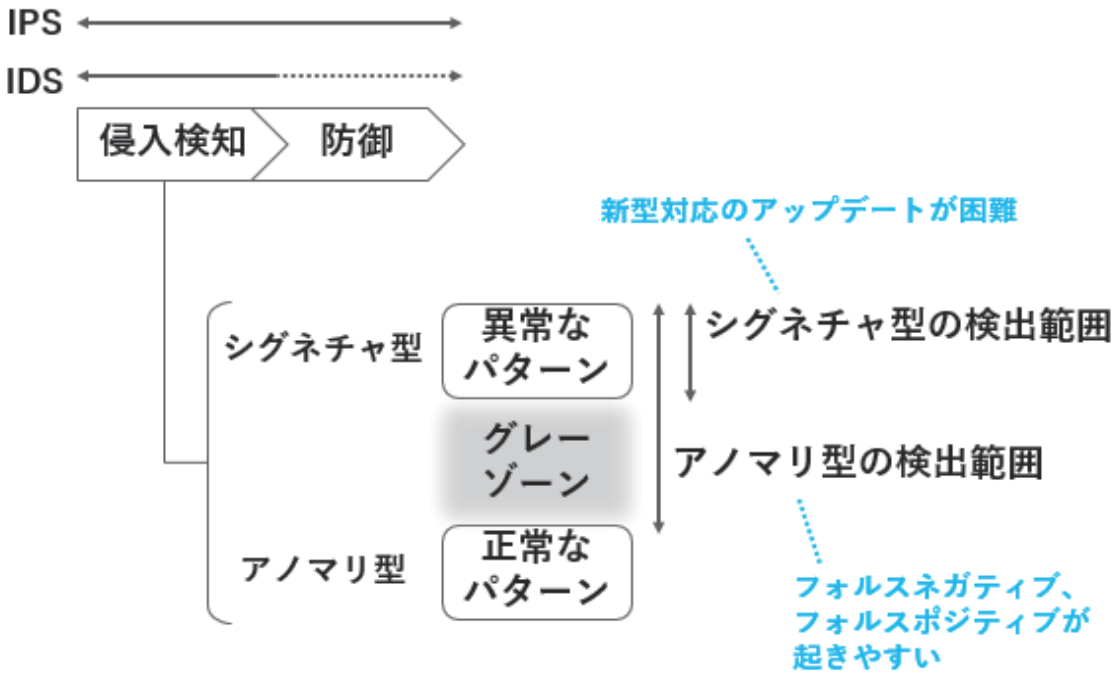
ホスト型にしてもネットワーク型にしても、IDS は通常「IDS センサ」と「IDS コンソール」という 2 つのモジュールに分かれた構成になります。IDS センサは不正アタックの検知部であり、検知した情報は IDS コンソールに送られてアラーム処理が行われます。製品によっては、さらに FW やホストに特殊なコマンドやパケットを送って通信を遮断し不正アタックの被害を軽減する機能をもつものもあります。

ネットワーク型 IDS センサは通常、センサポートとコンソールポートを持ち、コンソールポートを B セグメントに接続して IDS コンソールと通信可能にします。センサポートは監視対象セグメントのハブに接続します。しかし現代の LAN にはスイッチングハブが使われるため、通常は自ホスト宛でない通信を読み取ることはできません。そこで A セグメントのハブのうちセンサポートに接続する側のポートはミラーポート（すべてのパケットをミラーリングして流す）に設定し、センサポートはプロミスキャスモード（すべてのパケットを読み取る）に設定します。通常、センサポートは外部からの攻撃を避けるため、IP アドレスを設定しない「ステルス」モードで運用します。

IPS

侵入防御システム（IPS：Intrusion Prevention System）は，通信の経路上（インライン）に設置することで，③不正アタックを検知するだけでなく，検知した際にこれを遮断する機能をもつネットワーク機器です。上図は IDS と IPS の双方を描いていますが、この両者は機能的に類似しているもののそれぞれ独立した機器であり、併用も可能ですが基本的にはそれぞれ単独で機能します。IPS は通信の経路上に設置されるため、不正通信を検知したら自身でそれを遮断する機能を持っていますが、IDS にはそれがありません。ただし IDS でも FW との連携や RST パケットの送出などにより防御措置を講じる機能を持つものがあります。

12 シグネチャ型とアノマリ型



IDS、IPS のどちらにしても、運用としては侵入を検知した場合は防御措置を行うのが基本です。ただし IDS が行うのは侵入検知までで防御は人的オペレーションを要するのに対して、IPS は防御まで自動で行うのが基本です。ただし実際には IDS でも防御まで自動対応可能な場合があります。

一方、侵入を検知する方法にはシグネチャ型とアノマリ型の 2 種類があり、簡単に言うと「攻撃と分かっているものを見つけるのがシグネチャ型、正常と確信できないものを見つけるのがアノマリ型」です。犯罪捜査に例えるならば、顔写真や指紋を元に指名手配犯を発見するのがシグネチャ型、挙動不審な人間を発見するのがアノマリ型と言えます。

シグネチャ型

既知の侵入手口のパターンと照合することにより検出します。

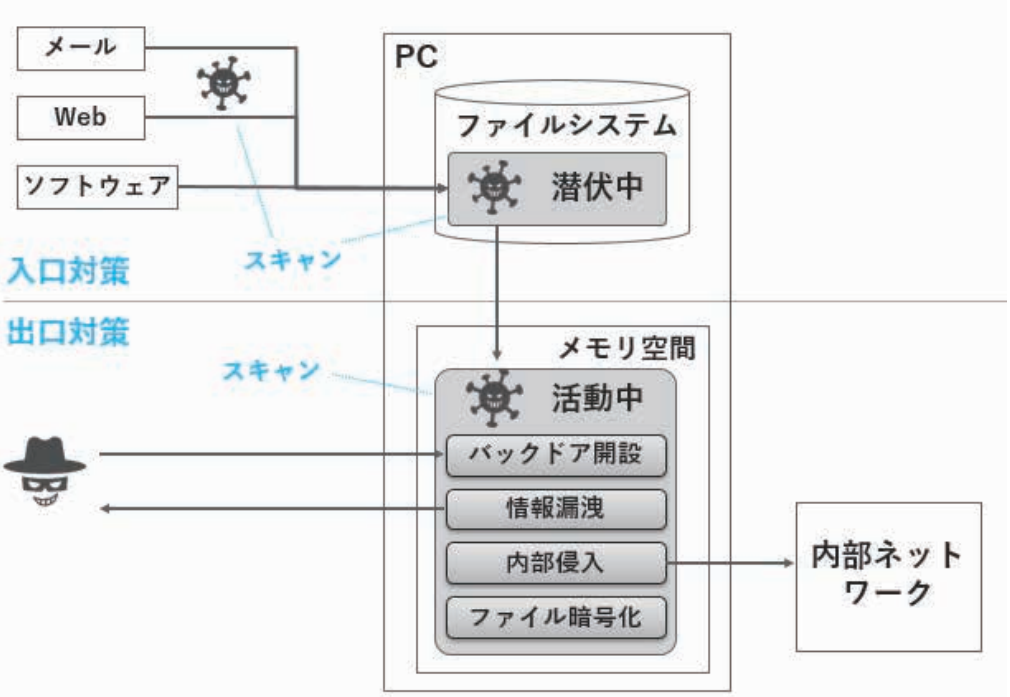
アノマリ型

定義された正規の通信の仕様とは異なる振る舞いを検出することによって侵入を推測します。例えばプロトコル異常検出の場合、RFC に違反するような異常なビット列を含むヘッダフィールド，異常に長い文字列や無効な文字を使用したペイロード等をチェックします。

フォルスポジティブ、フォルスネガティブ

シグネチャ型は「既知の攻撃」に対しては高精度に検出可能ですが、逆に言えば「未知の攻撃」に対しては無力であり、日々生み出されている新しい攻撃パターンは検出できません。
アノマリ型は未知の攻撃へもある程度対応可能ですが、正常な通信を誤って不正なものと検知してしまう「フォルスポジティブ」が起きやすくなります。それを防ぐために検出ルールを緩くすると逆に不正な通信を見逃してしまう「フォルスネガティブ」が起きやすくなります。防御を自動的に行うIPS ではこの両者のバランスが運用上大きな問題になりやすい傾向があります。

13 ウイルス対策



コンピュータウイルスは一般にメールや Web など（他に USB メモリなども）を通じて端末に侵入し、ファイルシステム上で潜伏します（ただし現在ではファイルを作らないウイルスもあります)。その後、起動されて活動を始めるとバックドアを開設して攻撃者が用意した C&C(Command & Control)サーバーと通信を始め、情報漏洩、内部侵入、ファイルの暗号化（ランサムウェア）などの活動を行います。

このうち、侵入～潜伏までの段階への対応を入口対策と言い、活動を始めた段階への対応を出口対策と言います。入口で完全に防ぐことは不可能と言ってよいため、侵入されることを前提に出口対策も講じて被害を最小化することが求められます。

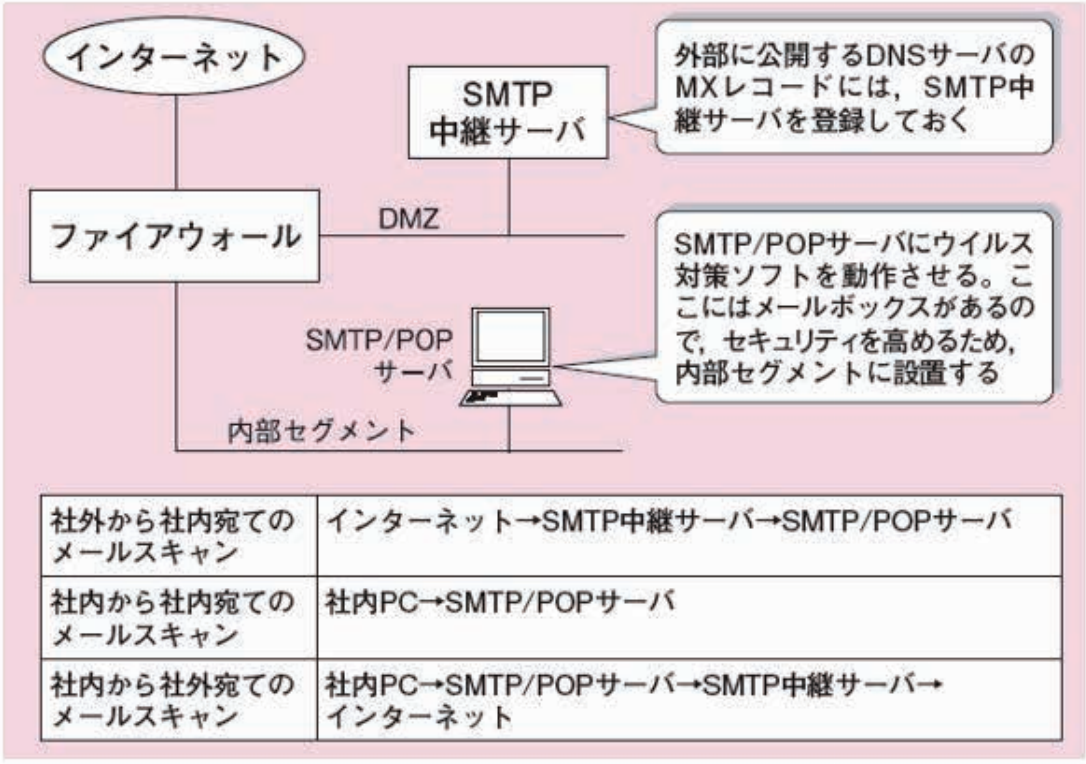
出口対策 1：ファイアウォール

ウイルスと C&C サーバーの通信を防ぐため、自サイトから外部に出ていく通信も最小限のものに限定するよう、ファイアウォールを設定します。

出口対策 2：プロキシ

インターネットアクセスはプロキシを経由するようにして、認証機能・ログ機能をもたせます。
ウイルスは認証に失敗するので、C&C サーバーと通信できなくなります。さらに、失敗の記録がログに残るのでバックドア通信が分かります

14 メールのスキャン



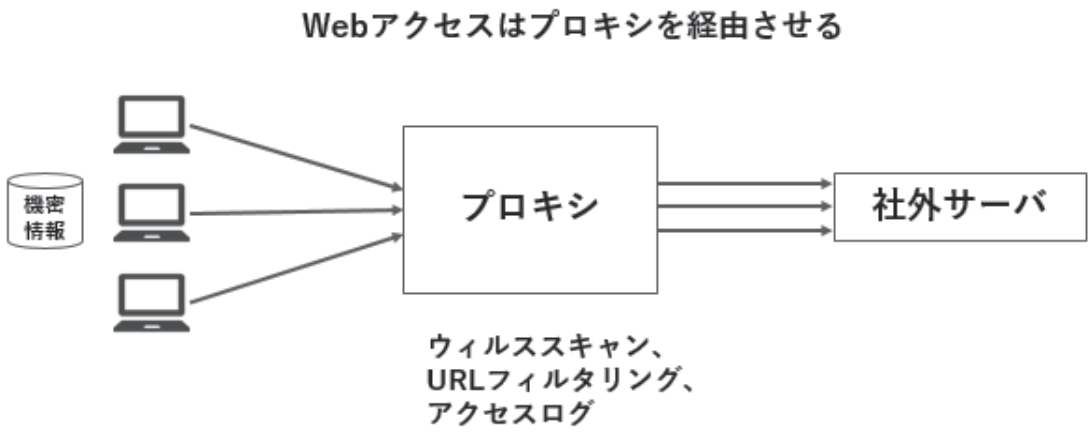
社外から社内宛てのメールスキャン	インターネット→SMTP中継サーバ→SMTP/POPサーバ
社内から社内宛てのメールスキャン	社内PC→SMTP/POPサーバ
社内から社外宛てのメールスキャン	社内PC→SMTP/POPサーバ→SMTP中継サーバ→インターネット

上図はウイルス対策のためにメールスキャンを行うサーバーを設置する例です。ウイルス感染の多くはメール経由によるものであり、一般的に，メールを通してマルウェアに感染する径路は大きく二つあります。

- マルウェアが埋め込まれた添付ファイルを不用意に開くことによる感染
- マルウェアが仕込まれた Web サイトへのリンク先を示す URL に不要にアクセスすることによる感染

そこで，メールサーバーでメールを中継する際，メールスキャンを実施するのが一般的です。これをメールフィルタリングなどと呼びます。スキャニングの対象となるのは，メール本文と添付ファイルですが、メールサーバー上では暗号化されたメールのスキャンはできないため、クライアントでのスキャンも不可欠です。

15 Web コンテンツフィルタリング



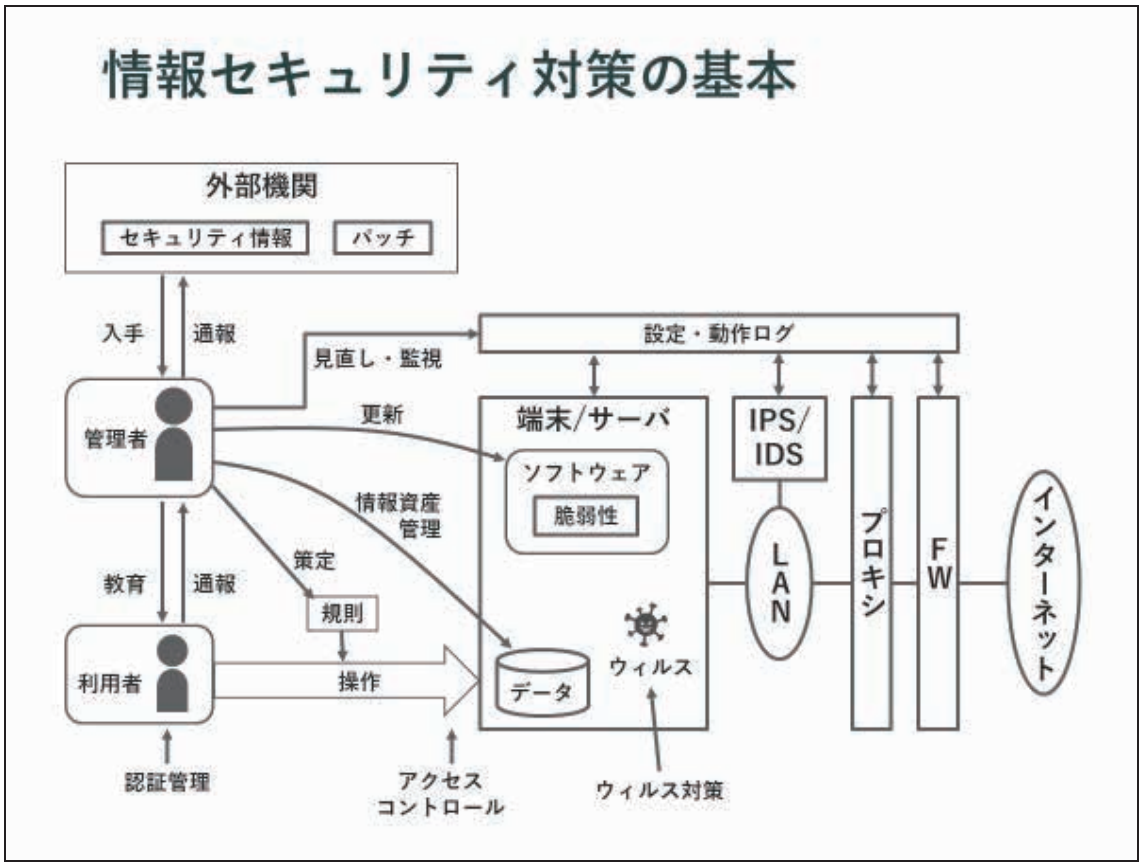
メールそのものにウイルスが含まれている場合はメールスキャンが有効ですが、メールに記載されたリンク先へのアクセスでウイルスをダウンロードさせられる場合はメールスキャンでは防げません。

そこで、Web にアクセスするときに必ずプロキシサーバを経由するようにし，プロキシサーバ上で Web トラフィックに対してウイルススキャンを実施する方法があり、コンテンツフィルタリングなどとも呼ばれています。なお，プロキシサーバ上でのスキャンは TLS などの暗号化通信には無力ですので，クライアントでのスキャンも不可欠です。

16 演習問題

問 1

5.1 節に登場する下記の図について、次の設問(1)〜(4)に答えてください。



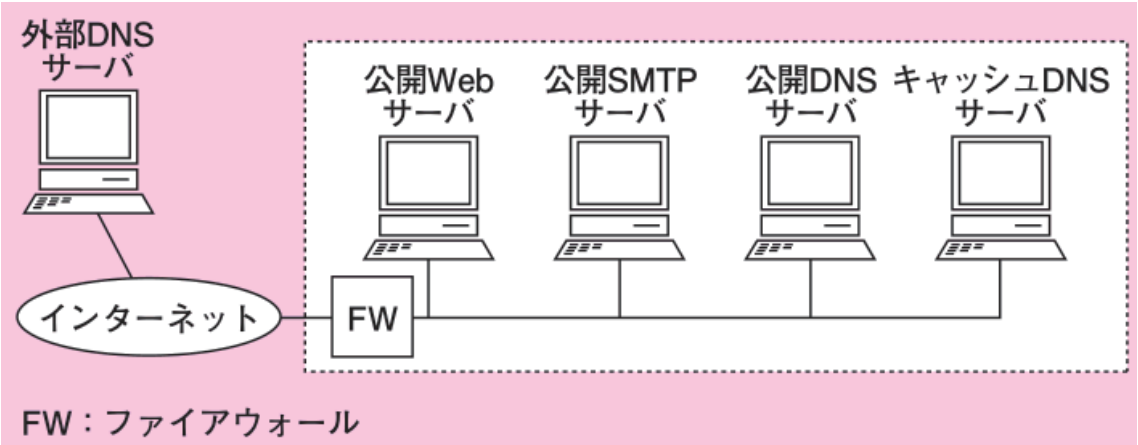
設問(1) 管理者が外部機関から入手する「セキュリティ情報」の具体例を挙げてください。

設問(2) 利用者が端末／サーバーに操作するのを制御する「アクセスコントロール」の具体例を挙げてください。

設問(3) IPS／IDS のログを定期的に監視する必要がある理由を挙げてください。

問 2

5.2 節に登場する下記のネットワークにおいて、公開 Web サーバーが外部からの TLS アクセスを受け付けるように変更します。

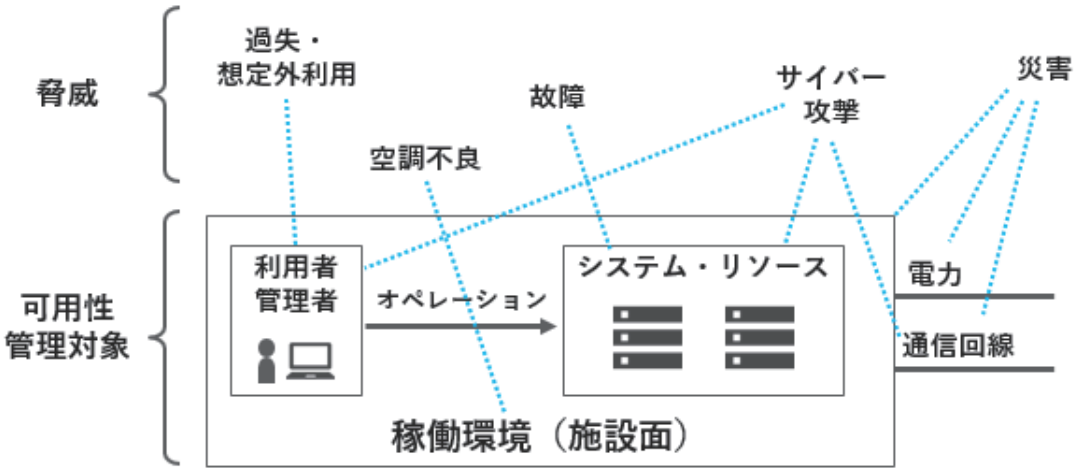


この結果、5.2 節で解説した「表：パケットフィルタリングの設定例」に新たなルールを追加する必要が生じました。どのようなルールを追加するか、そのルールを追加する位置はどこが適切であるかを答えてください。

第5章.

可用性、物理的セキュリティ

1 可用性管理対象と脅威の概要



可用性とは、情報システムの利用を許可された者が、必要な時にいつでも情報システムを利用できることを言います。可用性は、機密性、完全性と並んで情報セキュリティの３要素をなしています。

上図は可用性を実現するために管理しなければならない対象と、それらへの脅威の概要です。

一般に情報システムは何らかの「稼働環境」の中に「システム・リソース」を組み合わせて作られており、「利用者・管理者」がその操作（オペレーション）を行います。

「システム・リソース」とはサーバーやネットワーク機器のことで、「稼働環境」とはそれらを収納する建屋やラックのことを言います。極端な例で言えばサーバーを普通の事務所の簡易なラックに置いておくのは、温度湿度管理もできませんし、地震発生時に転落して故障したり、停電によって停止したりするケースも考えられるため、可用性という観点ではマイナスです。

以下、可用性に対する脅威の例を列挙します。

災害

大規模な地震、火災、水害等が発生すると、停電、通信断、建屋自体の崩壊が起きる可能性があります。データセンターは一般にこれらの事象にも被害を受けにくい特徴を備えていますが、広域災害では電力や通信の復旧に時間がかかることがあるため、遠隔地に予備系を用意しておくことが望まれます。

サイバー攻撃

サイバー攻撃はさまざまなポイントで発生します。サーバー自体に侵入されたり、管理者の端末に侵入されたりするとリモート操作でシステムを破壊あるいは停止させられる場合があります。通信回線に膨大なトラフィックを送り込まれて事実上使用不能になるケースもあります。

故障

システム機器はいつか必ず故障します。故障してもデータを失わない、稼働を止めずに済む、短時間で復旧できる、などの目標を達成できるような対策が必要です。

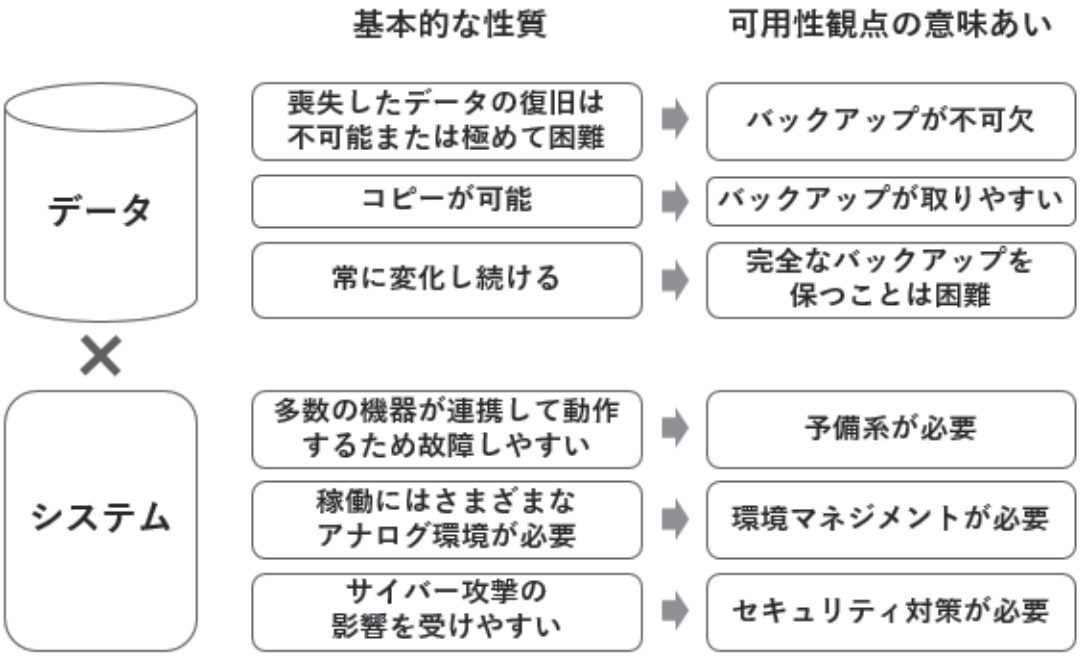
過失・想定外利用

利用者・管理者ともに思わぬ過失を起こすものです。例えばシステムメンテナンス中に管理者が誤ってデータを全削除してしまったケースもあります。想定外の利用としては、利用者が特定の画面を頻繁にリロードしたために高負荷が発生するケースがあります。会社に恨みを持つオペレータなど、悪意のある利用者・管理者がシステム破壊を試みるケースも考えられます。

空調不良

システム機器を極端な高温・低温環境で使用すると寿命が縮みやすく、また一時的な熱暴走を起こす場合もあります。一般的には、システム機器が発生する熱を逃がすための冷却を考えた空調設計が欠かせません。また、高湿度環境では結露が起きやすく、乾燥していると静電気が起きやすいため湿度にも気を配る必要があります。

2 データの可用性とシステムの可用性



可用性には大まかにデータの可用性とシステムの可用性の 2 つの面があり、それぞれ基本的な性質の違いにより可用性観点で注意すべき意味あいも違ってきます。

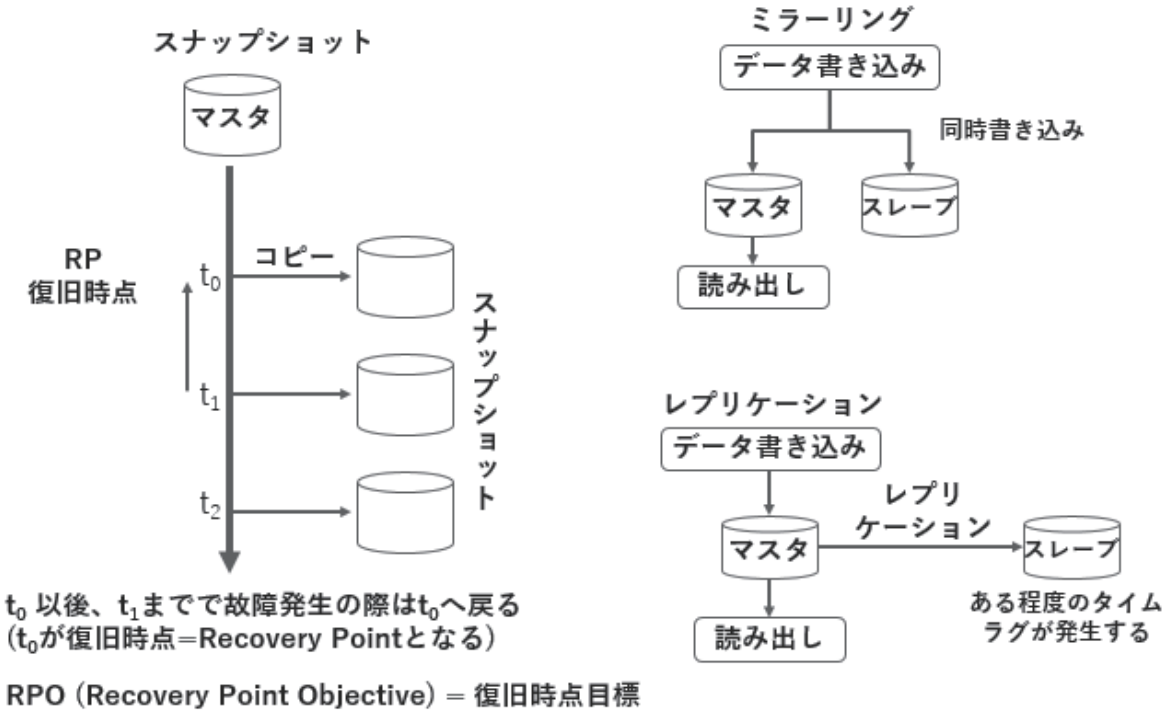
データ

完全に喪失したデータの復旧は不可能または極めて困難なため、バックアップが不可欠です。
一方、システムはコピーできませんがデータはコピーが可能なためバックアップが取りやすい特徴があります。
しかしながらデータは常に変化し続けるため、完全なバックアップを保つことは困難であるという特徴もあります。

システム

システムは多数の機器が連携して動作するため故障が発生しやすく、予備系の備えが欠かせません。
稼働に必要なアナログ環境とは、空調・電力・耐震性などのことで、これらの環境マネジメントが必要になります。
データのバックアップはサイバー攻撃を受けない場所に保管できますが、システムへのサイバー攻撃リスクを完全に除去することは不可能であり、セキュリティ対策が必要になります。

3 データの可用性



注：ミラーリング、レプリケーションはスナップショットの代替にはならない

データの可用性について重要な観点をまとめておきます。

図中左側は「マスタ」データの運用中、随時「スナップショット」というコピーを取ることでデータのバックアップを行う想定です。
RPO（Recovery Point Objective；復旧時点目標）は、データを損失した場合にどの時点のデータまで復旧できるようにするかを示す指標です。スナップショットを取っていれば、マスタが破壊された場合は一世代前のスナップショットに戻ることができます。たとえば t_0 以後 t_1 までの間に故障が発生したときは t_0 まで戻ることができます。つまりこの間の Recovery Point(復旧時点)は t0 です。当然、復旧時点は故障時点に近い（新しい）ほど良いのですが、最悪の場合でもここまでで済む、という目標値を RPO(Recovery Point Objective)=復旧時点目標と言います。スナップショットを取る間隔は RPO よりも短くなければなりません。

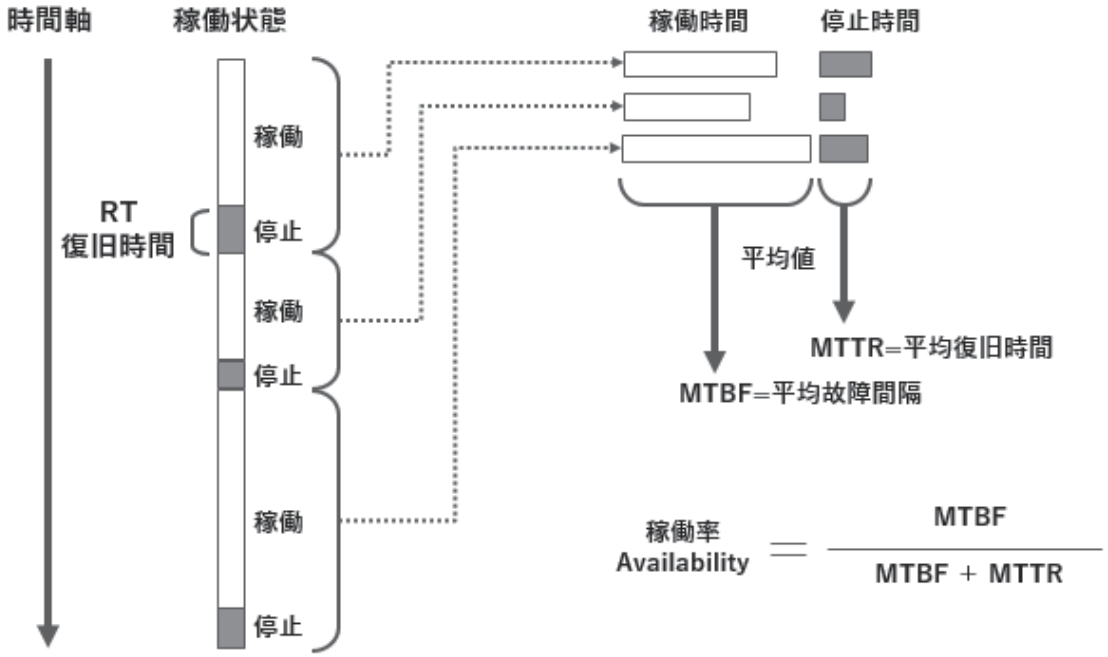
これに対してミラーリングはマスタとスレーブという 2 つ以上のデータに同時に書き込む運用方法を言います。書き込みは同時に行いますが読み出しはマスタからとなり、マスタが故障した場合はスレーブへ切り替える形です。一般に RAID1（レイド 1）と言われる仕組みがこれに該当します。同時に書き込みを行うため、RPO は基本的にゼロとなります。

レプリケーションはマスタのデータをネットワーク越しにスレーブへリアルタイムにコピーする方法です。マスタとスレーブが基本的に同期しているという点ではミラーリングに似ていてRPOはゼロですが、ネットワーク越しにコピーが行われるためある程度のタイムラグが発生します。マスタデータ更新後、コピーを完了する前にマスタ故障が発生した場合はデータ喪失が起こります。しかし、ミラーリングは基本的に同一筐体内のディスク間で行うため火災等で同時に失われるリスクがあるのに対して、レプリケーションは遠隔拠点間で行えるためそのリスクがありません。

なお、ミラーリングとレプリケーションはディスクの物理故障への対策としてのみ有効で、スナップショットの代替にはならないことには注意が必要です。たとえばオペレータの誤操作やプログラムのバグ、サイバー攻撃などにより全データ消去の操作をしてしまった場合、マスタとスレーブが同時に消去されるためバックアップとして機能しません。その場合でもスナップショットであれば一世代前に戻ることが可能です。

したがって基本的にスナップショットによるバックアップは必須であり、その上で物理故障時の復旧時間を縮めるためにミラーリングやレプリケーションを併用するのが一般的です。

4 システムの可用性



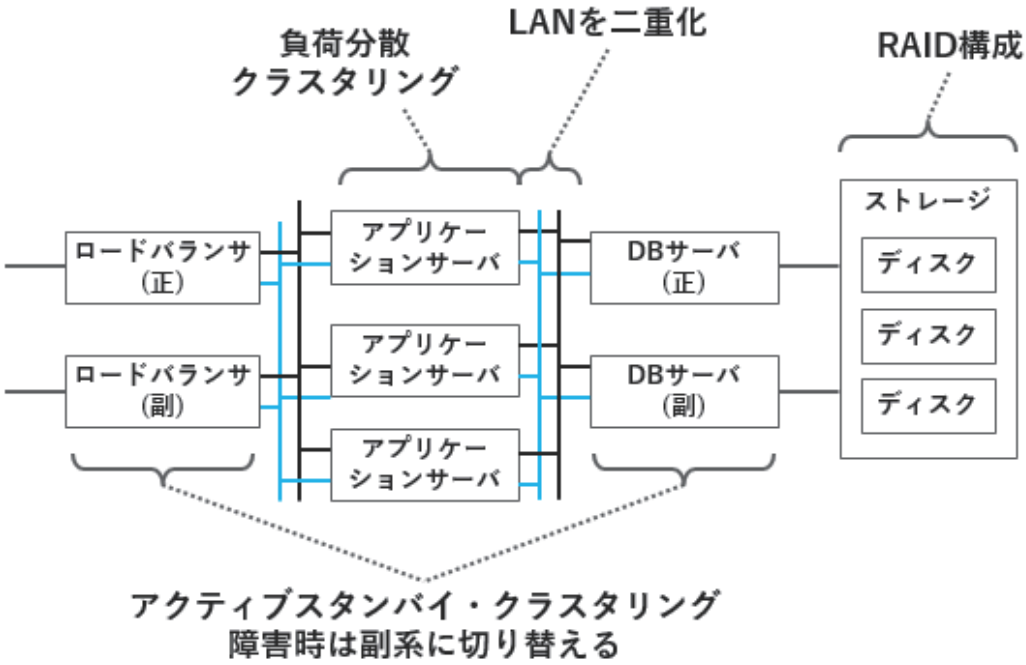
RTO (Recovery Time Objective) = 復旧時間目標

システムの可用性について重要な観点をまとめておきます。

一般に、システムは稼働状態と停止状態を交互に繰り返します。停止後、復旧するまでにかかる時間RT(Recovery Time)はできるだけ短い方が良く、この目標値を RTO(Recovery Time Objective)と言います。稼働時間の平均値を MTBF(Mean Time Between Failure)=平均故障間隔、停止時間の平均値を MTTR(Mean Time To Repair)=平均復旧時間と言います。稼働と故障、停止と復旧の用語が錯綜して紛らわしいので勘違いしないように注意してください。

MTBF と MTTR から Availability=稼働率を計算できます。可用性を検討する時にこれらの数字がよく使われます。

5 冗長構成



データについてはバックアップを取ることが不可欠だったように、システムの可用性を高めるためには同じ役割を持つ機材を二重化しておく「冗長構成」をとることが不可欠です。図は Web システムを冗長構成で構成する例です。

同じ役割を持つ機材を複数同時に一体的に使用することを一般にクラスタリングと言います。クラスタリングの目的は

- 冗長構成によって可用性を高めること
- 並列処理によって性能を高めること

の 2 種類があります。アクティブスタンバイ・クラスタリングは冗長構成の一種で、正系と副系を用意していずれも起動しておき、通常は正系のみ使用しつつ、正系に障害が発生したときは即座に副系に切り替える方法を言います。これに対して、通常は副系を起動せず、障害が起きてから起動する方法をコールドスタンバイと言います。

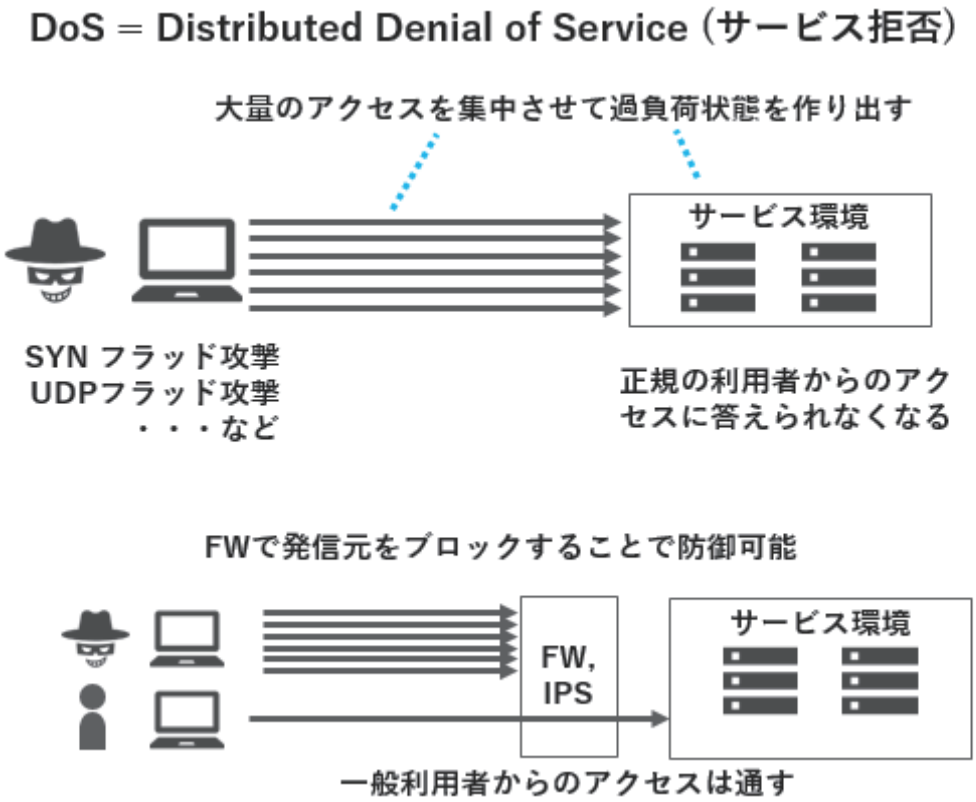
負荷分散クラスタリングは並列処理の一種で、複数の機材を同時に使用します。単独で使用する場合よりも全体として性能が上がるとともに、一部が故障しても性能は落ちるものの完全に止まることなく稼働し続けられるメリットがあります。負荷分散クラスタリングは並列処理が可能なパートにのみ使用できます。

高可用性システムを構築する場合は、1 箇所で障害が発生したらすべてが止まる

SPOF(Single Point Of Failure)＝単一障害点

を極力作らないように設計します。たとえばすべての通信が集中するハブやスイッチは、稼働率が高くても障害が発生した場合はそこに接続しているすべての機器が機能を停止するため SPOF になりやすいポイントです。そこで高可用性システムでは LAN も二重化を行います。

6 DoS 攻撃

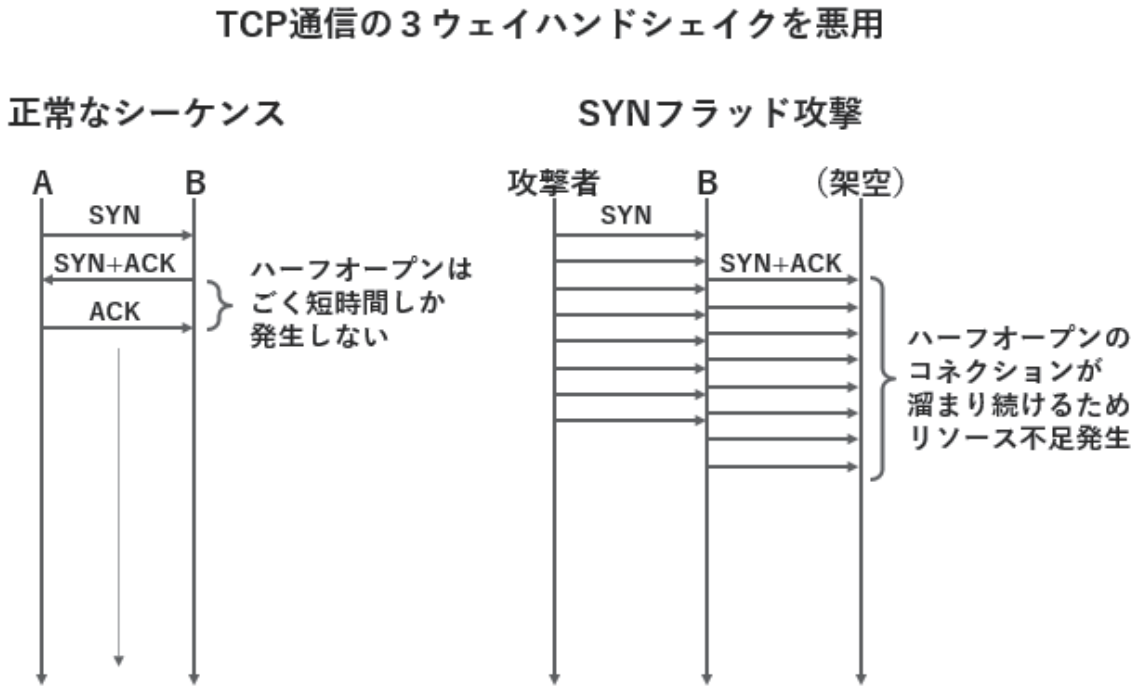


DoS（Denial of Service、サービス拒否）攻撃とは，標的サーバーの通信量を増大させ，ネットワークやサーバーのリソースを無駄に消費させて正常なサービスを妨害する攻撃です。過負荷状態に陥ったサーバーに正規の利用者がアクセスしようとしても、まったく反応がないか極端に遅くなり事実上使えなくなるため、「可用性が損なわれる」事態を招きます。

DoS 攻撃に使われる手法として SYN フラッド攻撃や UDP フラッド攻撃などが知られています。フラッド(flood)とは洪水を表す英語で、TCP/IP 通信プロトコルの隙を突いて大量のアクセスを送り込んでくることからこう呼ばれています。

DoS 攻撃一般の防御方法として、発信元アドレスが限られている場合は攻撃が始まったら FW や IPS でそのアドレスをブロックすることである程度防御可能です。

7 SYN フラッド

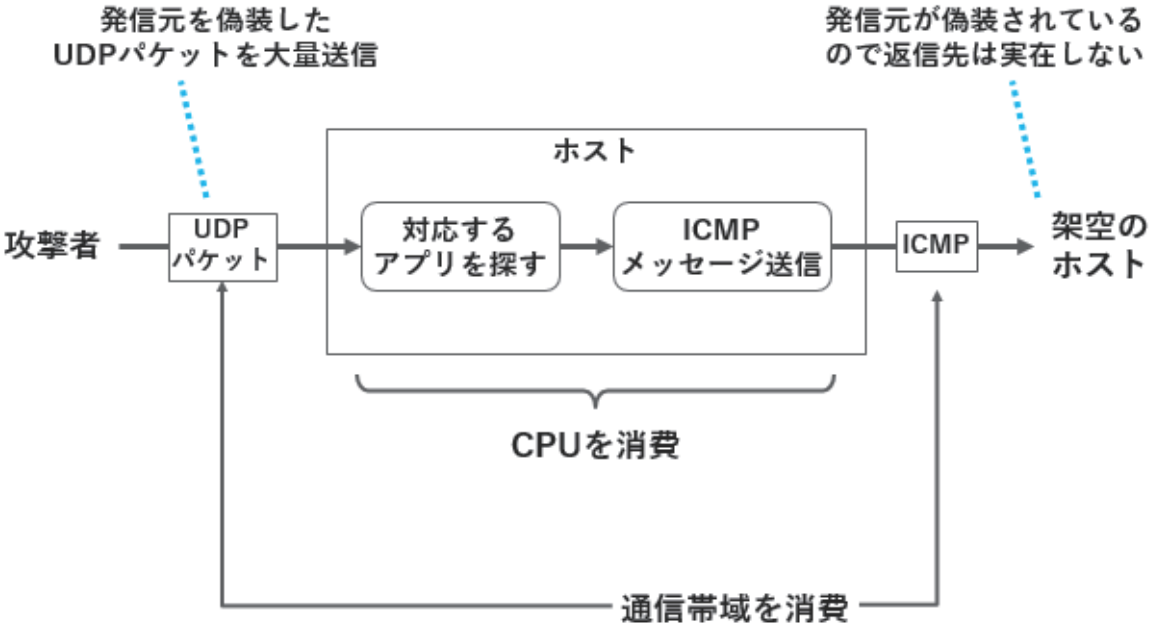


SYN フラッド攻撃は TCP 通信の 3 ウェイハンドシェイクという手続きを悪用する方法です。

TCP 通信を開始する際は 2 つのホスト間で SYN, SYN+ACK, ACK という 3 つのパケットを送りあってコネクションを開設します。これを 3 ウェイハンドシェイクと言います。ホスト B が SYN+ACK を返送した後でホスト A から ACK が返ってくるまでの間、ホスト B はコネクションが半分開いた状態という意味で「ハーフオープン」という状態になります。正規の通信であればすぐに ACK が返ってくるためハーフオープンの状態はごく短時間で終了し、そのために保持していたメモリも解放できます。

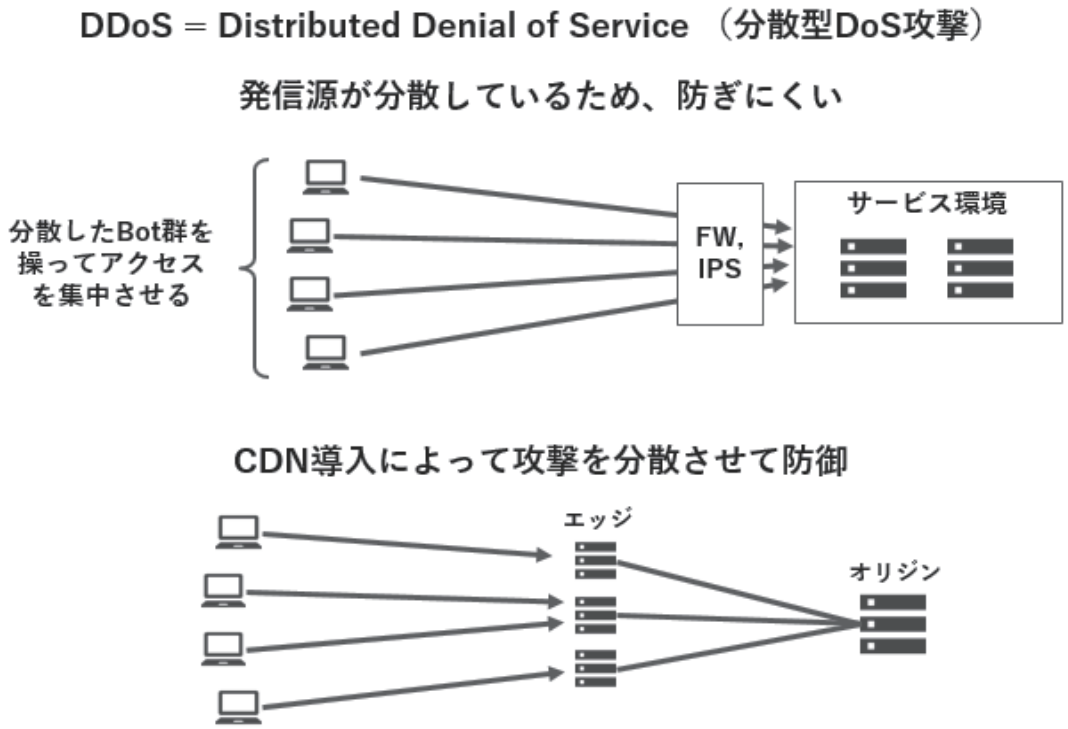
SYN フラッド攻撃では攻撃者は発信元を架空のアドレスに偽装した SYN パケットだけを短時間に大量に送り付けます。発信元を偽装しているため、ホスト B がそのアドレスに SYN+ACK を送っても ACK は返って来ませんので、ホスト B には本来短時間で解消されるはずのハーフオープンのコネクションが溜まり続けます。その結果リソース不足が発生して、それ以上の通信を受け付けられなくなります。

8 UDP フラッド



UDP フラッドでも SYN フラッド同様、攻撃者は発信元を偽装した UDP パケットを大量送信します。その際の UDP パケットはそれを処理するアプリケーションが存在しないポートを指定したものが使われます。そのパケットを受信したホストは、対応するアプリを探すもののそれが存在しないため、その結果を通知する ICMP メッセージを発信元ホスト（アドレス偽装されているため架空のもの）に向けて送ります。この過程でホストは CPU と通信帯域を消費するため、過負荷に陥り正常な通信が受け付けられなくなります。

9 分散型 DoS 攻撃



近年深刻化しているのが分散型 DoS (Distributed DoS, DDoS)と呼ばれる攻撃で、分散した Bot 群を操ってアクセスを集中させる方法です。Bot というのはマルウェアに侵入されて攻撃者によるリモートコントロール可能な状態になったホストのことで、攻撃者が Bot 群を操り一気に莫大なアクセスを集中して通信回線やサーバーを過負荷にさせ、正常なサービスの継続を不可能にさせてしまいます。

発信元が限られている単純な DoS 攻撃と違って、この方法では個々の Bot からの通信量は多くないため正常なアクセスと区別しにくく、FW や IPS では防ぎにくい特徴があります。

防御方法としては、(1)CDN の導入、(2)海外からのアクセス遮断、などがあります。

CND とは、自社サーバーが提供するコンテンツをインターネット上の複数のサーバーにコピーして設置することによって、アクセス分散と応答の高速化を実現するネットワークです。自社サーバーをオリジンサーバ、コピーして配置したサーバーをエッジサーバといいます。
CDN を利用すると、あるクライアント端末が自社サービスにアクセスする際、そのクライアントから見て最寄りのエッジサーバが選択されます。DDoS 攻撃により世界中から大量のアクセスが押し寄せたとしても、それらは世界各地のエッジサーバに分散します。その結果、個々のエッジサーバが受ける負荷は少なくなりダウンしにくくなるため、可用性が損なわれることがなくなります。
CDN は、akamai 社をはじめとする CDN 事業者や、主要なクラウド事業者が提供しています。

「海外からのアクセス遮断」とは、国内向けの利用者しか想定していないサービスの場合に可能な方法です。Bot の大半を占める海外からのアクセスを遮断することで DDoS 攻撃をある程度回避できます。

10 物理的セキュリティで考慮すべき項目

項目	目的	具体例
区画定義	適切な機密レベルを設定する	区画内にある情報を精査しその機密性に応じてセキュリティレベルを設定する
区画分離	セキュリティ区画の範囲を明示する	施錠、門番の配置などにより物理的に入室を制限するとともに、セキュリティ区画を示すプレートを掲示する
認証	入室しようとする者の身分を明らかにする	外部者には身分証明書の提示や内部者による保証を求める。内部者にはICカード等を発行する例が多い
認可	入室目的を明らかにして入室の許可を得る	申請書またはそれに準じる手段により入室申請を行う。認可にともなって名札等を交付する例が多い
記録	認証・認可および入退室の事実を記録する	ICカードによる入退室管理システムでは通常、自動的に入退室の時刻が記録される
標識	入室者の身分を明示する標識を義務付ける	内部者には身分証を兼ねるICカード、外部者には名札の着用を義務づける例が多い

物理的セキュリティとは、データやシステムへのアクセスを許可された者だけが物理的にアクセスできるようにすることを言い、その代表的なものに入退室管理があります。

以下、物理的セキュリティで考慮すべき項目の主要なものを列挙します。

区画定義

必要以上に高すぎるセキュリティは現場での運用破りが起きやすく、かえってセキュリティを下げる原因になりがちです。場所に応じた適切なセキュリティレベルを設定するためには、その場所で管理する情報を精査して区画を定義しなければなりません。

区画分離

定義した区画は誰からもわかりやすいように明示され、かつ、簡単に入れないように分離されていなければなりません。

認証

セキュリティ区画に入ろうとする者に対して身分を明らかにすることを求めるのが「認証」です。外部者には身分証明書の提示や内部者による保証を求め、内部者にはICカード等を発行する例が多くあります。

認可

入室目的を明らかにして入室の許可を得るのが「認可」です。申請書またはそれに準じる手段により入室申請を行って、権限を持つ者の認可を求めます。認可にともなって名札等を交付する例が多くあります。

記録

認証・認可および入退室の事実を記録します。セキュリティ・インシデント発生時に原因究明や影響調査を行うために重要です。ICカードによる入退室管理システムでは通常、自動的に入退室の時刻が記録されます。システムが導入されていない場合は紙の入室申請書にまとめて記入する例も多くあります。

記録

セキュリティ区画に入る者が、正当な手続きの上で入っていることを誰にでもわかりやすく明示するのが「標識」の役割です。通常、内部者には身分証を兼ねるICカードを、外部者には名札やビジターカードの着用を義務づける例が多くあります。

11 演習問題

問 1

可用性を損なう要因を、人為的なもの、非人為的なものに分けてみました。
それぞれについて可能性を損なう事象を具体的にいくつか挙げてください。

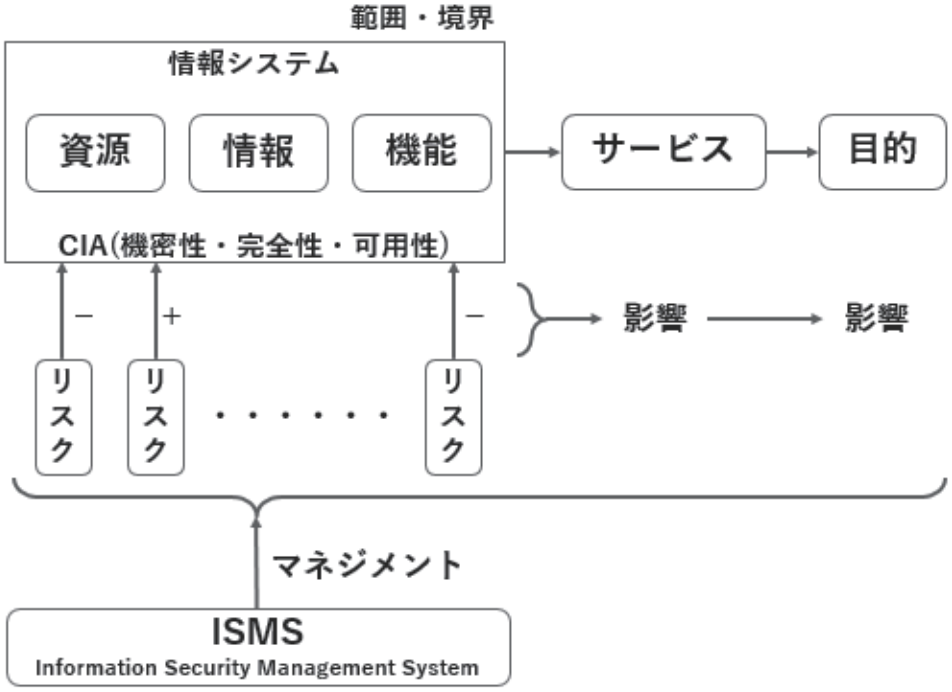
要因	分類	具体例
人為的	サイバー攻撃	
	過失・想定外利用	
	故障、空調不良(*)	
非人為的	災害	

(*) 不適切な製造・運用が一因となっている側面があるため、人為的に分類しています。

第6章.

情報セキュリティマネジメント

1 ISMS:セキュリティマネジメント



情報システムは、何らかの目的に向けたサービスを提供しています。例えば電子メールシステムは電子メールという「サービス」を提供していますが、その目的は「コミュニケーション」といえます。一般に情報システムは

情報：個人情報、受注情報など、いわゆる「データ」
機能：発注、製造、配送、返品など、「○○処理」と呼ばれるもの
資源：人員、電力、資金、機材など

といった要素で構成されており、これらはセキュリティの CIA（機密性・完全性・可用性）を満たしていなければなりません。

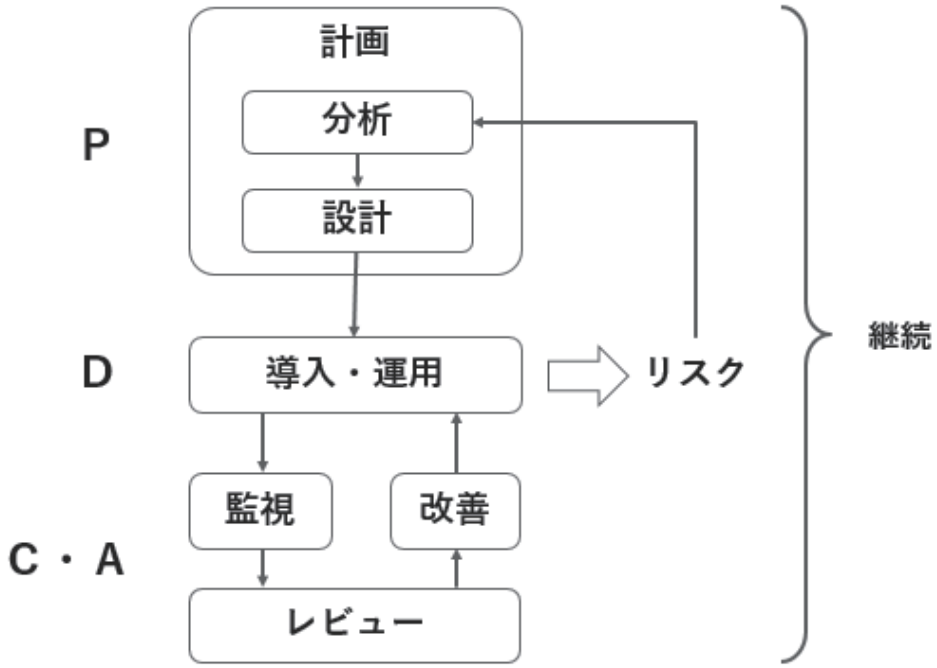
「リスク」とは情報システムに対して何らかのネガティブ（−）またはポジティブ（+）な影響を与える可能性があるもの、ただしあくまでも可能性であって現実化するかどうかは不確かなものを言います。ネガティブな影響があるものだけをリスクと考えがちですが、「不確かなもの」であればポジティブなものもリスクと考える必要があります。というのはたとえば「商品が爆発的に売れる」というようなポジティブな事象も「品切れになり機会損失が発生する」「多忙のために接客がおろそかになり顧客を不快にさせる」といったネガティブ事象を引き起こすことがあるため、「不確かさ」自体をすべて考慮しておく必要があるためです。

情報システムに関する多種多様なリスクのマネジメントは、情報システムを所有・運用する組織全体で総合的に行わなければなりません。そのためのしくみを Information Security Management System、ISMS と言います。

リスクが現実化して情報システムに影響を与えると、それはシステムが提供している「サービス」とそれが意図していた「目的」にも影響を与えます。そこで、ISMS は目的まで考慮に入れて行わなければなりません。たとえば、電子メールシステムが停止したとしても、それが目的としている「コミュニケーション」を行う代替手段が他にあれば、メールシステム停止の影響は限定的になります。代替手段は「目的」を元に考える必要があるため、ISMS はシステムだけでなく目的まで考慮して行います。

現在は API を通じて他社のサービスを組み合わせてシステムを構成したり、逆に他社サービスの一部となる API を提供している場合も多く、情報システムの「範囲・境界」は直観的な理解とは一致しない場合があります。ISMS がマネジメントの対象とするのはどの範囲で、その境界をどう定めるかは注意深く定義する必要があります。

2 PDCA サイクル

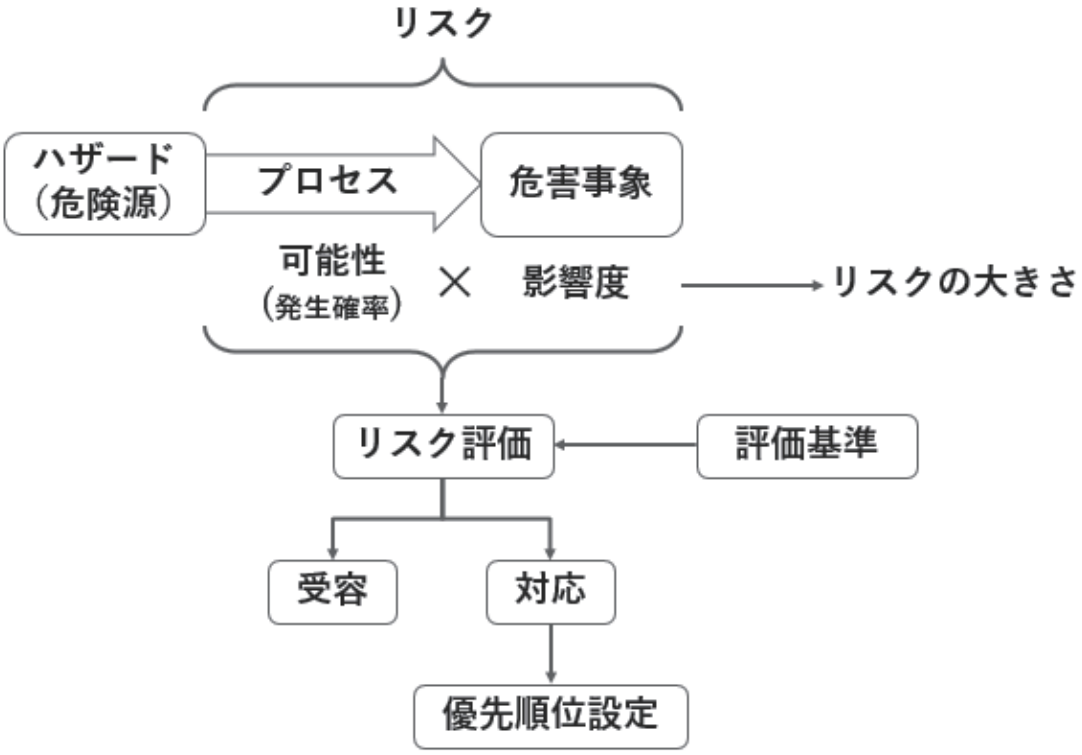


リスクが存在する場合、分析し対応策を設計して導入・運用します。さらにその運用状況を監視・レビューして改善します。PDCA サイクルの考え方で言えば分析と設計が PLAN、導入・運用が DO、監視・レビュー・改善が CHECK と ACT に該当します。

「改善」が設計変更を伴う場合には分析も含めてやり直す場合もあり、これらの活動は随時繰り返して継続的に行うべきものです。

（注：PDCA の A を ACT の代わりに ADJUST と考える見方もありますが、この議論においてはどちらでもかまいません）

3 ハザード、リスク、リスク評価



リスクは「危険」と呼ばれることもありますが、危険という単語は意味が広すぎるためあいまいになりがちです。最低限、リスクとハザードは区別しておきましょう。

たとえば火があったとするとそれは火傷や火事の原因になることがありますが、この場合「火」はハザードで、「火傷や火事」は危害事象（危害が発生した状態）です。ハザードそのものは問題ではなく、それがなんらかのプロセスによって危害事象を引き起こすことが問題であり、それを総称してリスクと言います。

プロセスについてはそれが実際に起きる「可能性（発生確率）」を、危害事象についてはそれが起きた場合の「影響度」を考えます。リスクの大きさは発生確率と影響度の掛け算で考えます。人間の直観的な判断は発生確率と影響度の実情を踏まえていない場合が多く、リスクを評価する際はこれらを分解して考えなければなりません。

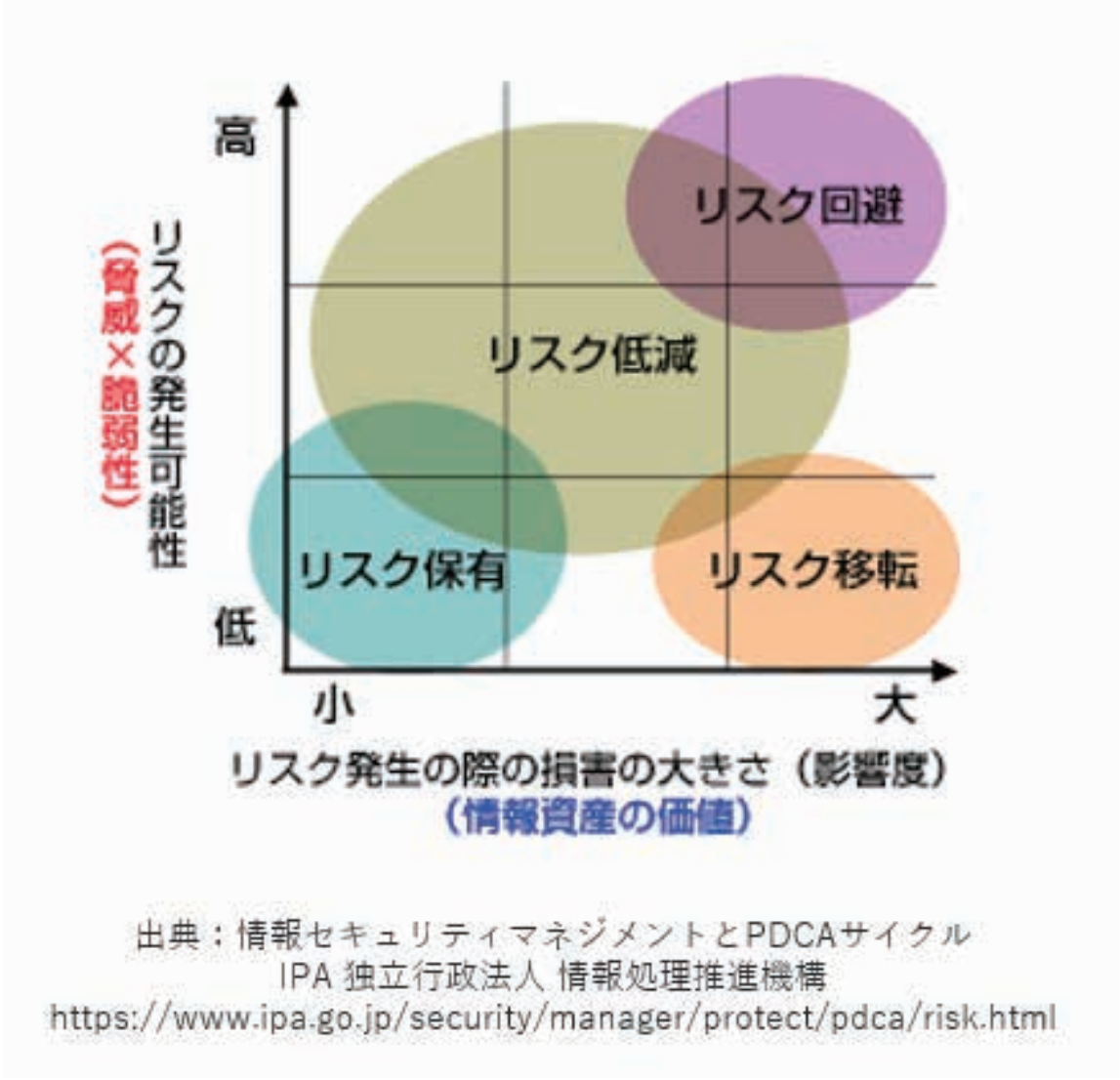
リスク評価には「評価基準」が必要です。評価基準を明確に言語化しておかないと人によってまちまちな判断をしがちです。

リスクを評価した後はそれを「受容」するか「対応」するかに分かれます。たとえば道路に出れば交通事故に遭うリスクがありますが、だからといって外に出ないという選択は普通行いません。これはリスクを「受容」することです。しかし、事故による出費のリスクに備えて保険をかけることはします。これは「対応」に当たります。

情報システムにかかわるリスクは多種多様なものがあり、そのすべてに即座に対応することはできません。そこで、対応するものについては優先順位を設定する必要があります。

ハザードは「危険源」と訳されることもあります。単なる「危険」という用語はハザードと危害事象のどちらの意味にも使われるためあいまいになりがちです。「危険」という用語を使う場合、リスクを厳密に定義するためにはそれがハザードなのか危害事象なのかを区別するように習慣づけましょう。

4 回避・低減・移転・保有（1）



出典：情報セキュリティマネジメントとPDCAサイクル
IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/manager/protect/pdca/risk.html

リスクへの対応を大まかに回避・低減・移転・保有の 4 種類に分ける考え方があります。

回避

リスクが発生する行動そのものを避けることです。「睡眠不足なので車の運転を止める」のはリスク回避の例です。影響度と発生可能性がともに大きなリスクについては一般に「回避」が推奨されます。

低減

影響度または発生可能性を減らすことです。自動車でシートベルトを締めたり、エアバッグを装備するのは「影響度の低減」に該当し、衝突被害軽減ブレーキ（自動ブレーキ）を装備するのは衝突その

ものを減らすという点では「発生可能性の低減」に、衝突が起きてしまった時でもその衝撃を緩和できるという点では「影響度の低減」に該当します。

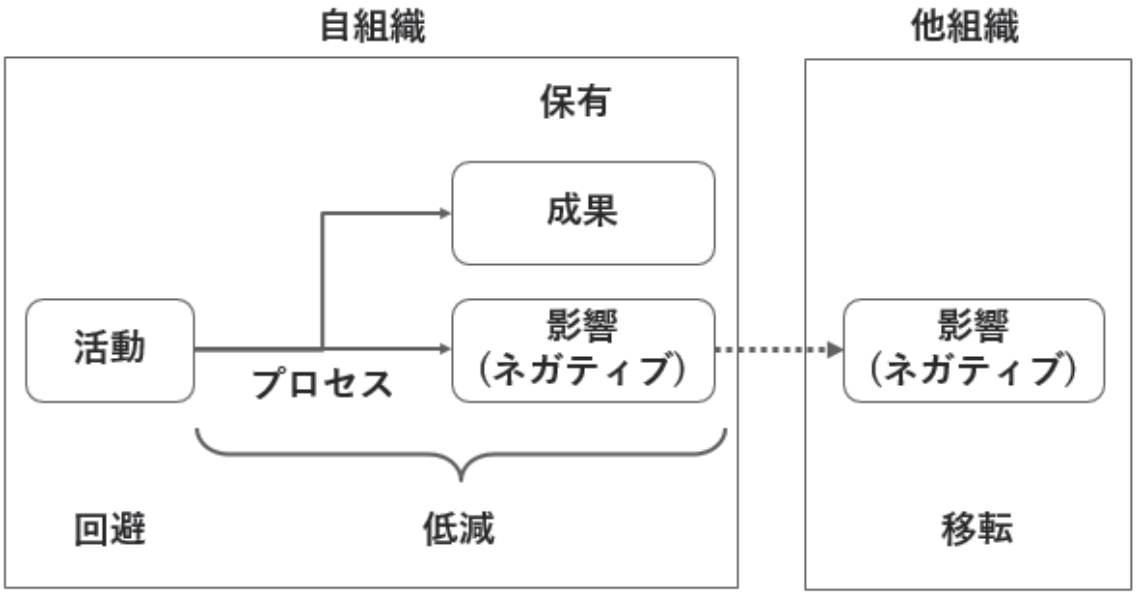
移転

回避や低減が不可能なリスクについては「移転」の対応を取ります。たとえば事故の発生そのものを完全にゼロにするのは一般に不可能ですが、発生時の出費については保険をかけることができます。これはリスクを誰かに分担してもらう「移転」に該当します。

保有

影響度・発生可能性がともに十分小さなリスクについては一般に「保有」で対応します。たとえば料理のために刃物を使うことには指を切るといったリスクがともないますが、影響度・発生可能性とも大きくないため特別な対応は行ないません。

5 回避・低減・移転・保有（2）



回避・低減・移転・保有を別な観点から整理します。

何らかの「活動」が、あるプロセスを経てネガティブな「影響」をもたらすとします。たとえば「火を使う」ことによって「火事が起きる」ケースを考えましょう。

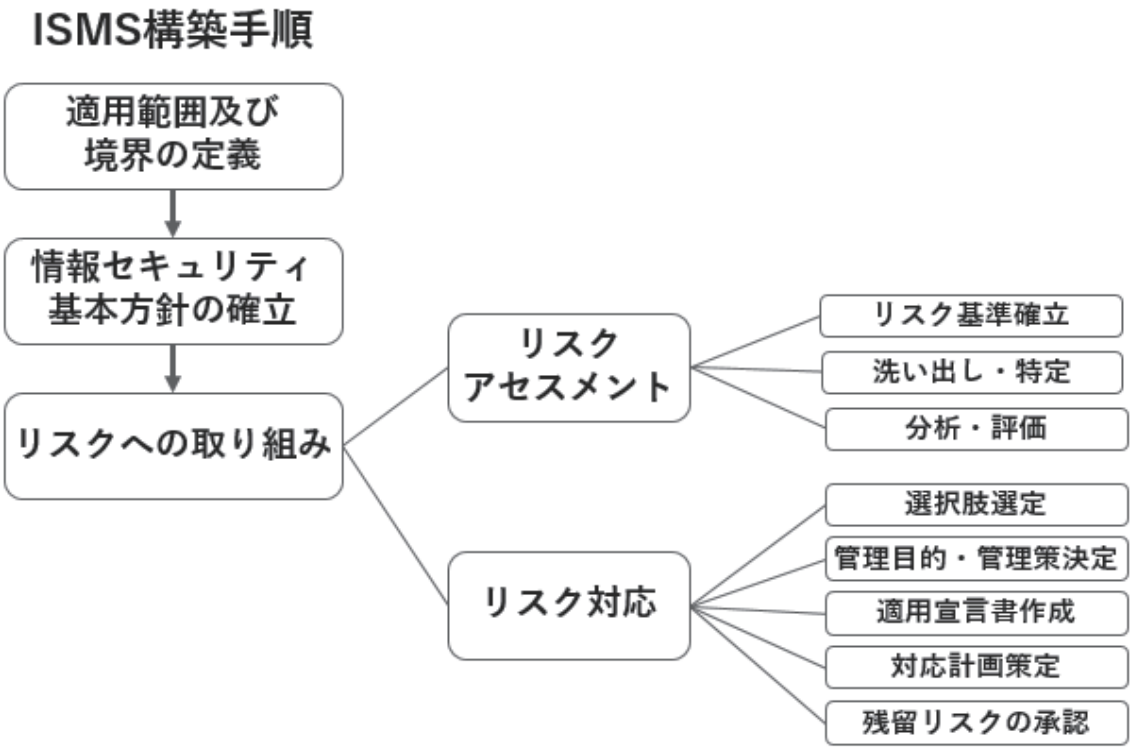
「火を使うこと自体をやめる」のが「回避」にあたり、「火の回りに可燃物を置かない、消火器を用意する」などの措置を講じるのが「低減」にあたります。

「移転」はそのネガティブな影響を他の組織に転嫁する行為で、最も良くあるのは「保険」です。

活動は一般に何らかの「成果」を得るために行うものであり、活動を止める（リスクを回避する）とネガティブな影響を避けられる一方で、「成果を失う」という別な影響が起きます。たとえば料理屋が「火を使う」ことを避けていたらそもそも営業ができません。

そこで、成果とリスクを比べた時に成果のほうが十分大きい場合は通常、リスクを「保有」（受容）します。

6 ISMS 構築手順



ISMS は国際標準 ISO27001 で定義されており、その構築手順は主に 10 ステップあります。

1. ISMS の適用範囲および境界の定義
   事業・組織・所在地・資産・技術の特徴の見地から、ISMS の適用範囲及び境界を定義します。境界を明確にするというのは、適用範囲の周囲に存在するであろう「適用除外」を明確にすることと解釈できます。たとえば、自社だけを考えるとしたら取引先・委託先を適用除外とした理由、自社内のある部門だけを適用範囲としているならば、別の部門を適用除外にした理由、などを考える必要があります。
   適用範囲の境界線が明確で合理的に説明可能であること、適用除外とした理由とその妥当性を説明可能であることが求められます

2. 情報セキュリティの基本方針の確立

   トップマネジメントは次の事項を満たす情報セキュリティ方針を確立し、文書化します。
   ・組織の目的
   ・ISMS を確立する目的
   ・情報セキュリティに関する要求事項
   ・ISMS の継続的改善

3. リスクへの取り組み

(1) 情報セキュリティリスクアセスメント

リスクとは、「目的に対する不確かさの影響」（ISO31000）であり、好ましくない影響のみならず、好ましい影響もリスクとなります。
リスクアセスメントとは、リスクの分析から評価に至るまでの一連のプロセスです。
ステップ３（１）で実施することは、情報セキュリティリスクアセスメントのプロセスを定め、それを実際に適用することです。

① リスク基準を確立する

あらゆるリスクには対処できないので、リスクを受容する場合の基準（リスク受容基準）を決定します。
情報セキュリティリスクアセスメントを実施するための基準や手順を決定します。その手順を実際に繰り返し適用したときに、一貫性及び妥当性が確保されるかどうか、比較可能な結果が得られるかどうかを見定めます。

② リスクを特定する

リスクを特定する方法は、概ね次の手順を踏みます。

1．ISMS の適用範囲内における情報資産を洗い差し、資産目録にまとめる。
　情報資産の例
　　情報、ソフトウェア資産、ハードウェア資産、サービス、人（技能・経験、等）、無形資産（組織の評判）
2．情報資産に対する脅威・脆弱性を洗い出す。
3．機密性・完全性・可用性の喪失に伴うリスクを特定する。
4．リスクを特定したら、そのリスクの所有者（リスクが顕在化したときに責任を持つ人）も特定しておく。

③ リスクを分析・評価する

ステップ３（１）②で特定されたリスクに関し、実際に生じた場合に起こり得る結果について、現実的な起こりやすさについて、分析・評価を行います。
ステップ３で決定した受容基準を比較し、リスクを受容するか、あるいは、何らかの対応が必要であるかを決定します。
リスク対応のために、分析したリスクの優先順位付けを行います。

(2) 情報セキュリティリスク対応

ステップ３（２）で実施することは、情報セキュリティリスク対応のプロセスを定め、適用することです。

① リスク対応の選択肢を選定する

リスクアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定します。
リスク対応の選択肢には、例えば、次の事項を含むことがあります（ISO31000）。

- リスクを生じさせる活動を開始又は継続しないと決定することによって、リスクを回避する。
- リスク源を除去する。
- 起こりやすさを変える。
- 結果を変える。
- 一つ以上の他者とそのリスクを共有する（契約及びリスクファイナンシングを含む。
- 情報に基づいた意思決定によって、そのリスクを保有する。
- ある機会を追求するために、そのリスクを取る又は増加させる。

「結果を変える」はわかりにくいですが、たとえば災害に見舞われやすい場所からは貴重な物品を撤去する、といった行動が該当します。災害そのものは避けがたくとも、それがもたらす結果は変えることができます。

② リスク対応のための管理目的及び管理策を決定する

選定した情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定します。
決定した管理策を、ISO27001 附属書 A に示された管理策と比較し，必要な管理策が見落とされていないことを検証します。

- 附属書 A は、分類、管理目的、管理策の 3 つの階層からなる。
- 分類は全部で 14 個ある。
- 分類の下に管理目的が定義されており、合計で 35 項目ある。
- 管理目的に沿って管理策が定義されており、合計で 114 項目ある。

なお、附属書 A に規定した管理策は全てを網羅してはいないため、追加の管理目的及び管理策が必要となる場合があります。

付属書 A の分類

A.5　情報セキュリティのための方針群
A.6　情報セキュリティのための組織
A.7　人的資源のセキュリティ
A.8　資産の管理
A.9　アクセス制御
A.10　暗号
A.11　物理的及び環境的セキュリティ
A.12　運用のセキュリティ
A.13　通信のセキュリティ
A.14　システムの取得、開発及び保守
A.15　供給者管理
A.16　情報セキュリティ・インシデント管理
A.17　事業継続マネジメントにおける情報セキュリティの側面
A.18　順守

③　適用宣言書を作成する

次の内容を含む適用宣言書を作成します。

- 選択した管理目的及び管理策、それを選択した理由
- 実施済みの管理目的及び管理策
- 適用除外とした管理目的及び管理策、それを除外した理由

④　リスク対応計画を策定する

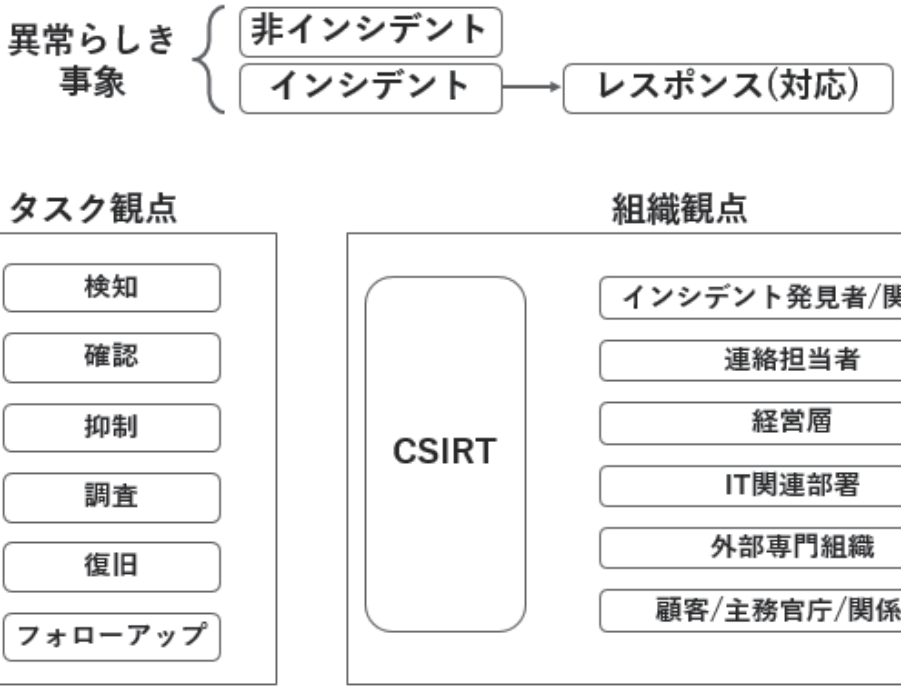
対応するリスクごとに、具体的な計画を策定します。
一般的に言って、次の内容を含んでいます。

- スケジュール
- 責任者・実施者
- 優先順位
- 具体的な対応手順
- 教育・訓練
- 管理策の有効性を測定する方法と測定結果の評価方法

⑤　残留リスクについて承認を得る

残留リスクとは、リスク対応を行った後にまだ残っているリスクのことです。
残留リスクが受容基準を満たしているかどうかを検証・ 確認します。
残留リスクについて、リスク所有者からの承認を得ます。

7 インシデント・レスポンスと CSIRT



「インシデント」という単語は、安全管理用語としての本来の意味は「事件・事故につながる恐れがある事象」であって、事件・事故そのものは含みません。しかし情報セキュリティ分野では慣用的に事件・事故そのものを含む意味でインシデントと呼んでいます。たとえば Web サイトで本来パスワードを設定すべきページでその設定が漏れていた場合、それによって情報漏れが発生していてもいなくてもインシデントとなります。

情報システムにおいて何らかの「異常らしき事象」が発生した場合は、インシデントとそれ以外（非インシデント）に分けて、インシデントについては何らかの対応をしなければなりません。この対応のことをレスポンスと言い、異常の発見からレスポンスまでの一連の流れをインシデント・レスポンスと総称します。

インシデント・レスポンスを「何を行うべきか」というタスクの観点で見ると上図左下のように「検知、確認、抑制、調査、復旧、フォローアップ」に分けることができ、大まかにこの流れで進めます。「検知」は異常らしき事象を発見すること、「確認」はそれがインシデントであるか（対応が必要であるか）どうかを確認することです。「異常らしき事象」は勘違い等で報告される場合も多く、その場合は対応不要となります。

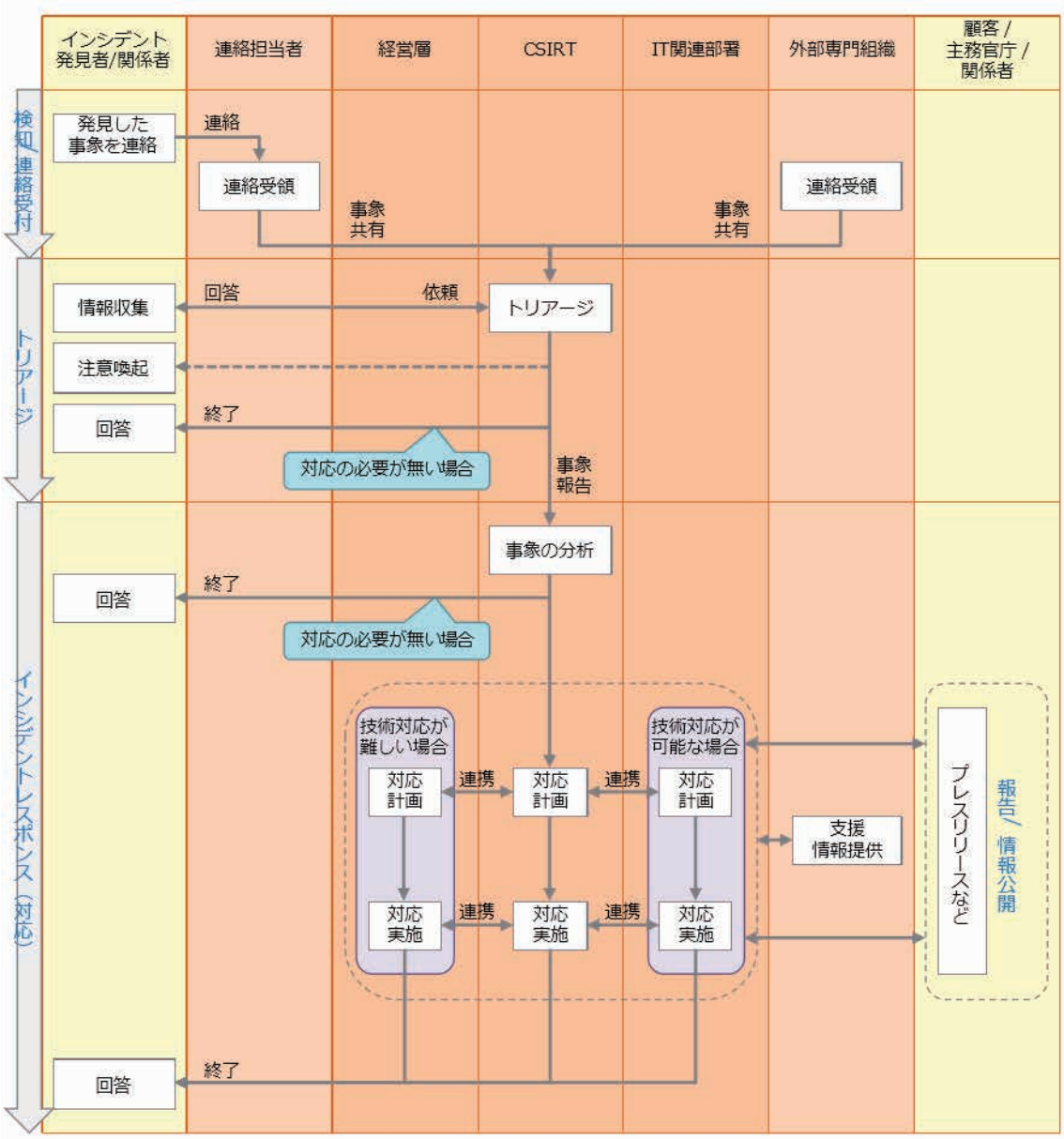
「抑制」は被害の拡大を防ぐ緊急措置のことを言います。たとえば不正プログラムによる情報流出が起きている場合には、いったん外部へのネットワーク接続を遮断してそれ以上の流出を防ぐことが

「抑制」にあたります。通常、原因究明や復旧手順の検討には時間がかかるため、その間の被害拡大を防ぐ抑制措置が必要な場合があります。

「調査」では原因を究明して復旧手順を検討します。「復旧」は止まった業務を再開するために必要な対処を行って元のレベルで再開することを指し、「フォローアップ」では再発防止や事後広報等を行います。

一方、これらの対応にはさまざまな組織が関わります。インシデント・レスポンスを「誰が当事者であるか」という組織の観点で見ると上図右下のようにCSIRT(Computer Security Incident Response Team)の他に大きく6つに分類される組織や関係者があります。インシデント・レスポンスを成功させるためには、これらの関係者の行動を適切に統制していかなければなりません。情報セキュリティ・インシデントが発生した状況においては、関係者との十分なコミュニケーションを取りながら短時間のうちにさまざまな大きな意思決定を行っていく必要があります。その役割を担うのがCSIRTです。これは個人の力でできることではないため、事前に十分な想定・計画・訓練を行ったチームを編成しておく必要があります。

一般社団法人 JPCERT コーディネーションセンターが定めたインシデントハンドリングマニュアルでは、インシデント・レスポンス対応の流れがより細かく整理されています。



出典：インシデントハンドリングマニュアル、一般社団法人 JPCERT コーディネーションセンター、https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf

インシデントが発生してから解決するまでの対応は、次に示す 4 つのフェーズからなります。

1. 検知と連絡受付　（タスク観点の「検知」に該当）
2. トリアージ　（タスク観点の「確認」に該当）
3. インシデント・レスポンス　（タスク観点の「抑制」「調査」「復旧」「フォローアップ」に該当）
4. 事後の報告と情報公開　（タスク観点の「フォローアップ」に該当）

1. 検知と連絡受付

インシデントの検知は、自分の組織内で検知する場合、外部からの通報により検知する場合があるため、いずれの場合にも対応できるようにしておきます。

自分の組織内で検知する場合は、インシデントのチェック項目を定め、「異常」事態であるか否かの判定基準を決めておきます。

外部からの通報により検知する場合は、問い合わせ窓口を作り、外部に公開しておきます。

いずれの場合であっても、検知したインシデントは関係者の間で共有しておくことが大切です。

対応要否の判断はインシデントレスポンスチームに任せます。

2. トリアージ

トリアージとは、インシデントの重症度を判定し、作業対象と作業項目の優先順位を決定する作業です。

重症度の例：

レベル	内容
3	異常が発生し、本格的な対応が必要である
2	異常は発生したが迅速に駆除できたため、業務への影響はほとんど発生していない
1	インシデントを排除する設計が有効に機能したため、異常が発生していない

インシデントレスポンスチームは、得られた情報に基づいて事実関係を確認し、インシデントであるか否かを判断します。

次に示す理由により、インシデントではないと判断される場合、その判断の根拠を報告者に回答したり、関係者に報告したりします。

・誤って検知された
・「異常」の判定基準が不適切であった
・通報者の勘違いであった

インシデントレスポンスチームが対応すべきと判断した場合には、インシデントをレスポンス（対応）の対象とします。

インシデントレスポンスチームが対応するか否かに関わりなく、情報提供すべきと判断した場合には、注意喚起などの情報発信を行います。

3. インシデント・レスポンス

インシデント・レスポンスは、次の手順を踏みます。

① トリアージの結果、対応すべきと判断したインシデントに対して、事象の分析を行います。対応すべき事象か否かを再度検討し、さらに、自組織での技術的な対応が可能か否かを判断します。

② この時点で対応すべきではないと判断されたならば、自組織の情報セキュリティポリシーが許容している範囲で、通報者に回答します。

③ 自組織での技術的な対応が可能ではない場合、経営層と連携し、対応計画を策定して実施します。たとえば、外注先でなければ対応できない場合は、経営層を通じてその旨を外注先に伝え、対応してもらいます。

④ 自組織での技術的な対応が可能である場合、主に IT 関連部署と連携し、対応計画を策定し、実施します。その際、経営層との情報共有を行います。

⑤ 技術的対応の可否によらず、対応計画の策定や実施に当たっては、外部の専門機関に対応の支援を依頼したり、必要な情報を提供してもらったりします。

インシデント	外部の専門機関
マルウェア感染	IPA
ソフトウェアの脆弱性を突いた不正アクセス	IPA
フィッシング偽サイト	警察（フィッシング 110 番） フィッシング対策協議会

フィッシング 110 番
http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

フィッシング対策協議会
http://www.antiphishing.jp/

⑥ 対応計画を実施し終わったら、問題が解決しているか否かを確認します。問題が解決していない場合、再度事象を分析し、対応計画を策定・実施します

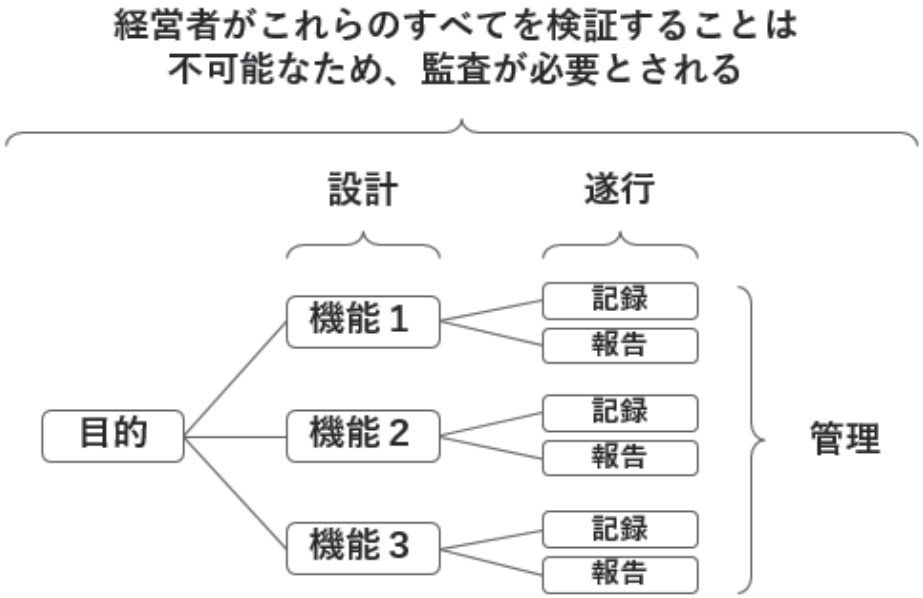
⑦ 最終的に問題が解決した段階で、自組織の情報セキュリティポリシーが許容している範囲で、事の顛末を通報者に詳細に回答します。

4. 事後の報告と情報公開

事後の報告を、必要に応じて、適切な相手に行います。
たとえば、メディアや一般向けのプレスリリース、Web サイトでの一般向けの報告、監督官庁への報告などが考えられます。

インシデントの内容や対応方法について、自組織内部で情報を共有すると共に、可能な範囲で情報を外部に公開します。情報を公開することで、他の組織に対して注意を喚起でき、他の組織から支援を得られる可能性があります。

8 システム監査の必要性



一般に、システムはいくつかの機能を組み合わせて何らかの目的を達するように設計します。現場の担当者がその機能を用いて業務を遂行すると、記録や報告が残ります（自動的に作成されるものもあれば、人手で作成されるものもあります)。これらの記録・報告を見て遂行状況を確認するのは管理者・管理部門の役割です。しかし、単に記録・報告が正しく行われているだけではシステムが経営上の目的に適合していることの検証はできません。

目的に対してシステムが適合していることを検証するための視点には大まかに下記の 4 種類があります。

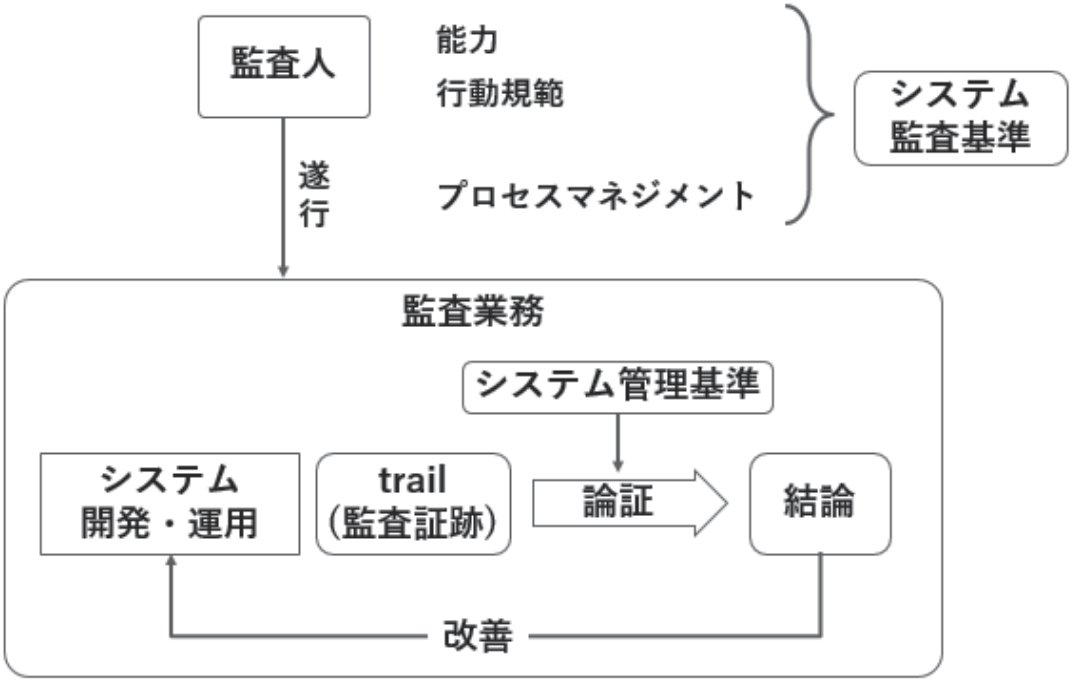
① 目的実現のフレームワーク＝「この目的を達成するためにはこれこれの機能があれば必要十分です」
② 機能検証のフレームワーク＝「これこれの機能が遂行できていることを検証するにはこれこれの記録があれば必要十分です」
③ オペレーション＝「この通り、業務を適切に遂行しています。記録はこれです。」
④ 遂行状況の確認＝「記録を確認した結果問題ありません」

①は経営戦略やビジネスモデル企画の視点、②はシステム設計の視点、③は業務担当者の視点、④は管理部門の視点です。③のレベルで正しく業務が行われて④でそれを確認できたとしても、そもそも①や②に問題がある場合にはそれを③の記録から発見することはできません。

①や②の部分は経営層とシステム部門が担うべき役割ですが、一般に経営層はITに関する深い知見を持たない場合が多く、システム設計の役割はSI会社等に外注される場合が多いため、第三者視点で保証を与えることはできません。

「システム監査」とは、このような構造のもとで専門知識を持った第三者の視点で①〜④までの全体を検証し、経営者や社外を含む利害関係者に対して「システムが経営上の目的に適合して設計されていて、正しく運用されており、継続的な改善活動も行われている」ことを保証する活動です。

9 システム監査基準とシステム管理基準



システム監査には、「システム監査基準」と「システム管理基準」の 2 種類の基準が関わります。監査業務とは、システムの開発・運用にともなって生じるさまざまな trail（監査証跡、判断の根拠・証拠となる情報のこと）を元に「システム管理基準」を踏まえて合理的な論証を経て「結論（問題なし、または問題点と改善方針の指摘）」を出す活動です。「結論」はシステム開発・運用の改善に役立つものであることが求められます。

一方、監査業務は監査人が遂行します。監査人はそれにふさわしい能力と行動規範を備えていなければならず、監査業務の遂行に当たってそのプロセスを適切にマネジメントしなければなりません。これらの能力、行動規範、プロセスマネジメントなどについての基準を規定しているのがシステム監査基準です。一方、システム管理基準はシステムそのものの合理性を判断する上での基準です。

【システム監査基準】
一般基準（5 項目）：監査人の適格性、監査業務上の遵守事項など
実施基準（6 項目）：監査計画の立案、監査手続きの適用方法など、監査実施上の基本的な枠組み
報告基準（5 項目）：監査報告に関わる留意事項、監査報告書の記載方法

【システム管理基準】
情報戦略の立案・企画・開発・運用・保守というライフサイクルに沿って、情報システムを効果的かつ安全に運用するための規範が定められている。287 項目の実施基準からなる。

10 セキュリティ監査、プライバシーマーク

■ 情報セキュリティ監査

- ❑ 情報セキュリティに関して、システム監査同様、専門性と客観性を有する監査人が実施する
- ❑ 保証型と助言型がある
- ❑ 特定分野を選択して実施できる

■ プライバシーマーク制度

- ❑ 個人情報の取り扱いについて適切な保護措置を講ずる体制を整備していることを示すマーク
- ❑ 取引先や消費者に、個人情報の取り扱いに関し安心感を与えられる

情報セキュリティ監査制度は、情報セキュリティの管理や対策が適切に実施されているかどうかについて、システム監査制度と同様、専門性と客観性を有する監査人が実施する活動です。

保証型と助言型の二つの形態が定められています。

- 保証型

  情報セキュリティのマネジメントが適切であるか（または不適切であるか）を伝達する監査です

- 助言型

  情報セキュリティの問題点を洗い出し、改善のための助言を行う監査です

ISMS では包括的な取り組みが求められるため、ISMS の認証を得るハードルは高いものがあります。

一方、情報セキュリティ監査は特定の分野を選択して監査を受けることができるため、ISMS より実施しやすい制度です。情報セキュリティ監査制度を適宜実施することで、組織体の情報セキュリティのマネジメントが徐々にレベルアップし、いずれは ISMS の基準に到達することを期待できます。

プライバシーマーク制度とは、「日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム－要求事項」に適合して、個人情報の取り扱いについて適切な保護措置を講ずる体制を整備している

事業者等に対し、その旨を示すマークとしてプライバシーマークを付与し、事業活動に関してプライバシーマークの仕様を許容する制度」です。

https://privacymark.jp/system/about/outline_and_purpose.html

プライバシーマークを認定された企業は、取引先や消費者に対して、個人情報の取り扱いに関し安心感を与えることができます。したがって、顧客情報を扱う企業にとって、プライバシーマークの認定を取得することにメリットがあります。

11 演習問題

問 1

ISMS を構築するための手順として、最も適切な順序はどれでしょうか？次の選択肢ア～エの中から一つを選んでください。

項番	手順
a	適用範囲及び境界の定義
b	リスク基準の確立、リスクの洗い出しと特定、リスクの分析と評価
c	リスク対応策の選定、リスク対応計画の策定
d	情報セキュリティ基本方針の確立
e	経営者等、リスクが顕在化したときに責任を持つ人の承認

ア	a → b → c → d → e
イ	a → d → b → c → e
ウ	a → b → c → e → d
エ	a → e → b → c → d

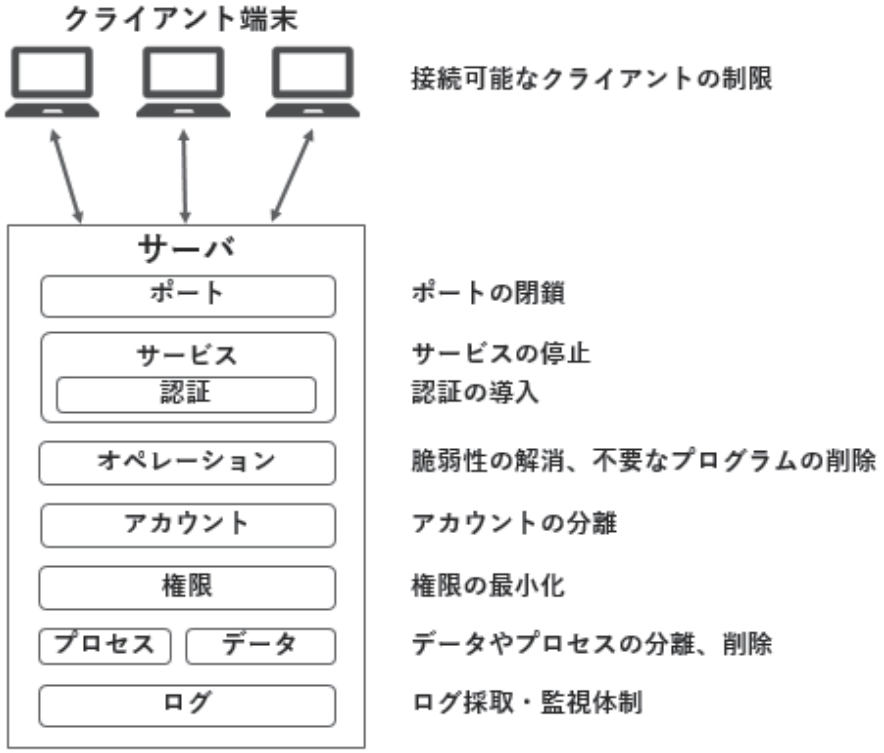
問 2

会社のパソコンで業務をしている最中、あるサイトにアクセスしたら、「あなたのパソコンはウイルスに感染しています。すぐにウイルス対策ソフトをダウンロードしてください」というメッセージが書かれていました。同じページには「ダウンロード」ボタンがありました。
この従業員が会社のセキュリティ管理者ではないとします。
この従業員がとるべき行動、セキュリティ管理者が取るべき行動について答えてください。

第7章.

サーバーとシステム基盤

1 サーバー要塞化の基本



サーバーは実際の業務で役立つサービスを提供しているノードです。通常、サーバーとインターネットの間はファイアウォール(FW)、リバースプロキシ、WAF、IPS/IDS などで隔離し、インターネットからの攻撃にサーバーが直接さらされないように設計します。しかしそれらの防御も完全ではありませんし、攻撃もインターネット側からだけ来るとは限らないため、サーバー単体のセキュリティレベルも上げておくことが望まれます。これを「サーバー要塞化」と言います。

サーバーの動作モデル概念図を基にして、サーバー要塞化の基本的な考え方を理解しましょう。
サーバーが動作する時は、クライアントからの接続を「ポート」で受け取り、ポートごとに規定されている「サービス」を起動して、必要に応じてクライアントの「認証」を行い、そのサービスで規定されている「オペレーション」を行います。「サービス」プログラムは起動時に設定される「アカウント」に与えられた「権限」を持っており、その権限によって「データ」や「他のプロセス」に何らかの操作を行います。これらの一連の動きはログに記録されます。

このような動作モデルを踏まえると、「サーバー要塞化」において重要なのは「あらゆる入り口や権限を狭めておく」ことです。これはどのようなサービスにも共通する考え方であり、具体的に言うと下記の各項になります。

接続可能なクライアントの制限

クライアントが社内のみである、特定の ISP のみを使用する、日本国内からのアクセスのみ受け付けるなど、接続可能なクライアントを制限できる場合は制限します。

ポートの閉鎖

開けておく必要のないポートは閉じておきます。

サービスの停止

ポートはサービスにひも付けられていますが、単にポートを閉じるだけでなく、使わないサービスは起動せず、プログラム自体をシステム上から削除します。

認証の導入

サービス内容によりますが、ユーザー認証、クライアント認証を導入可能であれば導入します。

脆弱性の解消、不要なプログラムの削除

サービスプログラムやライブラリに脆弱性が発見されることがありますので、脆弱性は判明次第できるだけ早期に更新を当てるなどして解消します。これは「不要なプログラムを削除する」という対応も含みます。脆弱性が存在するプログラム自体を削除してしまえるなら、削除するのが最も確実な方法です。

アカウントの分離

サービスの脆弱性を通じて不正なプログラムを実行されることがあります。その際、不正プログラムはサービスを稼働させているアカウントの権限で動作するため、大きな権限を持つアカウントでサービスを稼働していると被害が拡大します。サービス毎に違うアカウントで起動し、権限も分離しておくことが望ましい方法です。

権限の最小化

サービスの設定ファイル等、デフォルトの設定では「読み取りはどのアカウントからでも可能」となっている場合が少なくありません。各アカウントが影響を及ぼせる範囲、データを読み出せる範囲等の権限を最小化しておきます。

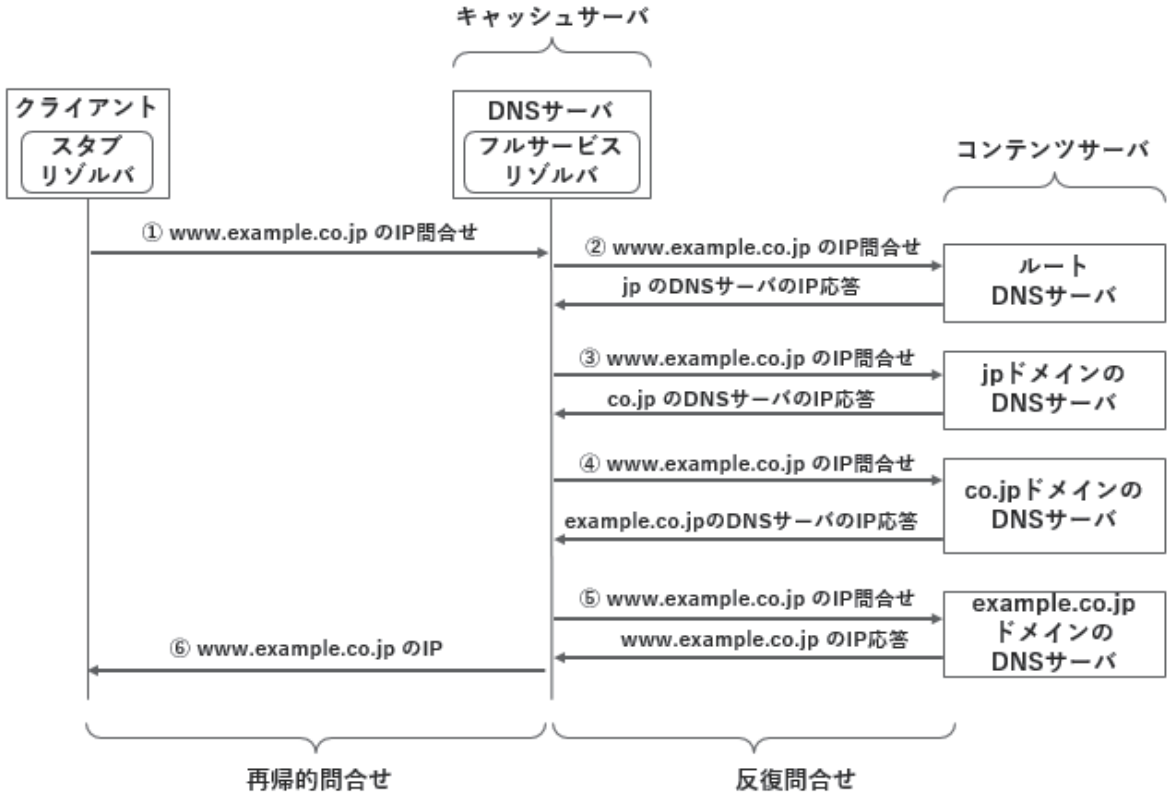
データやプロセスの分離、削除

たとえば同時に採取したデータでも、個人情報を含まない部分だけで間に合う処理に使うなら、個人情報を含む形でデータファイルを持つ必要はありません。データを要る部分と要らない部分に分離して、要らない部分は削除する等の処置を行います。

ログ採取・監視体制

ログを採取しておき、不審な兆候のリアルタイム監視、後日遡っての検証ができる体制を組みます。

2 DNS の仕組み



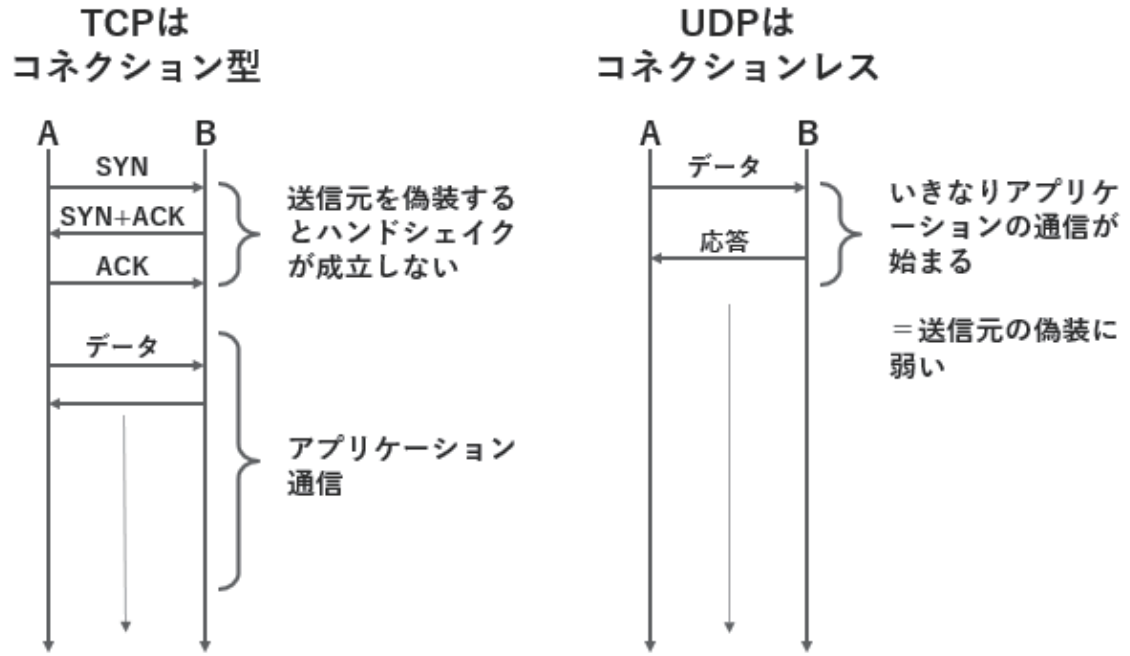
DNS の基本的な仕組みを確認しておきます。
図中の「クライアント」はたとえば一般の利用者が使う PC のことです。たとえば Web サイト http://www.example.co.jp を閲覧しようとすると、サイトの IP アドレスを知るためにクライアントは DNS サーバーに対して①www.example.co.jp の IP アドレスを問合せます。その問い合わせを受けた DNS サーバーは②、③、④、⑤と繰り返し問い合わせをして www.example.co.jp の IP アドレスを調べ、それを⑥クライアントに返信します。クライアントからの問い合わせを直接受ける DNS をキャッシュサーバ、キャッシュサーバからの問い合わせを受ける DNS をコンテンツサーバと言います。

「リゾルバ」は「解決するもの」という意味の単語で、DNS が果たす「名前から IP アドレスを調べるという課題を解決する」という役割を実際に遂行するプログラムのことをリゾルバと呼びます。クライアントで動くリゾルバをスタブリゾルバ、キャッシュサーバで動くリゾルバをフルサービスリゾルバと言います。フルサービスリゾルバが行う②〜⑤の問合せを反復問合せといい、スタブリゾルバが行う①の問合せを再帰的問合せと言います。

コンテンツサーバの「コンテンツ」とは、名前とその IP アドレスに関するオリジナルの情報、原本となる情報を保持していることを表します。キャッシュサーバの「キャッシュ」は一時的なコピーと

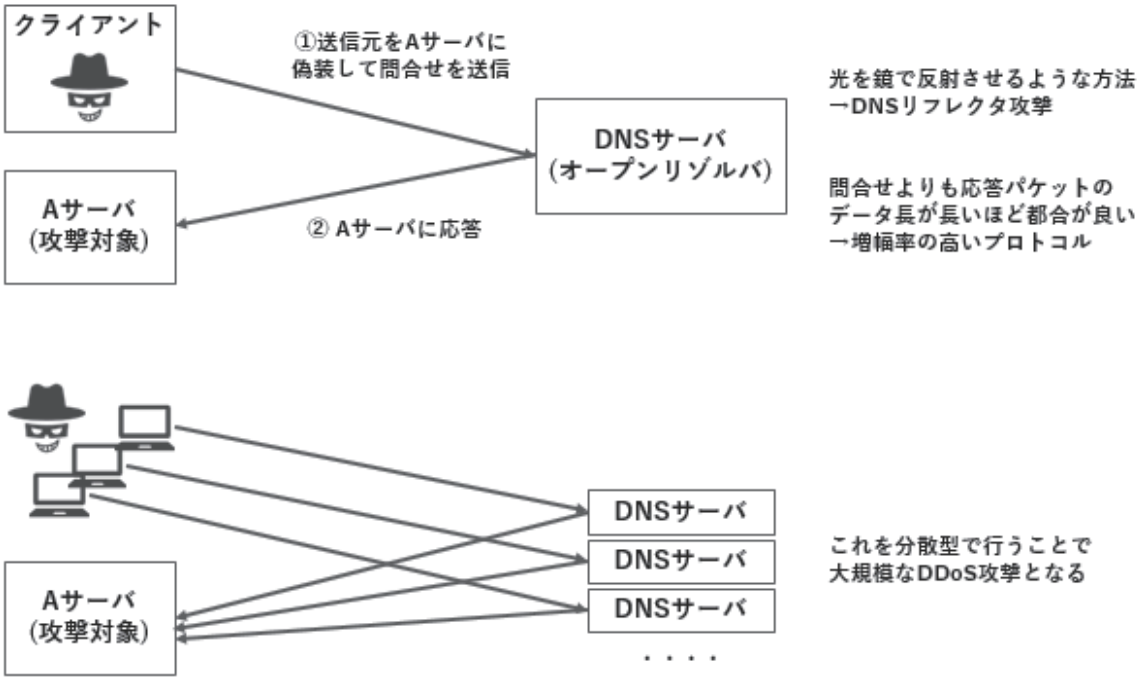
いう意味で、キャッシュサーバは必要な情報をコンテンツサーバから取得して一時的にそのコピーを保持しておく働きをします。

3 送信元偽装に弱い UDP



DNS の通信で主に使われる UDP は送信元の偽装に弱いプロトコルです。TCP の場合は実際のアプリケーション通信の前に SYN と ACK を交換する 3 ウェイハンドシェイクがあり、送信元を偽装するとハンドシェイクが成立しないため、アプリケーションレベルの通信は始まりません。しかし UDP はハンドシェイクがないため、送信元を偽装していきなりアプリケーションレベルの通信を始めることができます。この特徴を悪用する攻撃手法に、DNS リフレクタや DNS キャッシュポイズニングなどがあります。

4 DNS リフレクタ



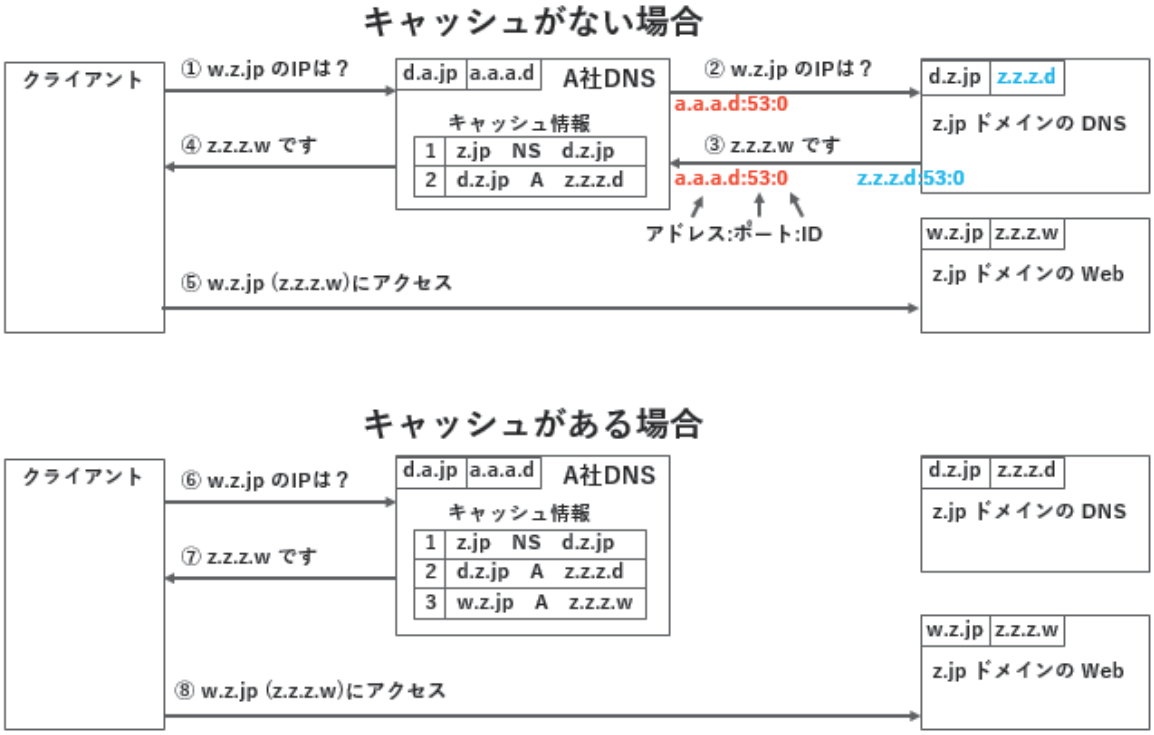
DNS リフレクタ攻撃は DoS 攻撃の一種です。A サーバーを攻撃する場合、攻撃者は①送信元を A サーバーに偽装した問合せを DNS サーバーに送信します。DNS は②A サーバーにその応答を返すため、A サーバーは送ってもいない問合せを受信するために通信回線や CPU 負荷が発生します。これを分散型で行うことで大規模な DDoS 攻撃になります。

この方法は光を鏡で反射させるような方法ということで、「反射」を意味する単語で DNS リフレクタ攻撃と呼ばれています。

オープンリゾルバとは、どのクライアントからの問合せにも答える DNS サーバーのことを言います。たとえば 1 つの社内や ISP で運用しているキャッシュサーバは、その社内や ISP 内のクライアントからの問合せにのみ応答するように設定します。それに対して、インターネット上のどこのクライアントからの問合せにも応答する DNS がオープンリゾルバです。この種の攻撃にはオープンリゾルバが悪用されます。

リフレクタ攻撃は UDP であれば原理的にどのプロトコルでも可能ですが、問い合わせよりも応答パケットのデータ長が長いほど攻撃しやすくなります。これを「増幅率が高い」と言います。DNS プロトコルはこの条件を満たすため、リフレクタ攻撃には DNS がよく使われます。

5 DNS キャッシュの仕組み



DNS キャッシュの仕組みを確認します。クライアントが w.z.jp というホスト名を持つ Web サイトを見に行く場合を考えます。これに関係するサーバーは下記の 3 つです。

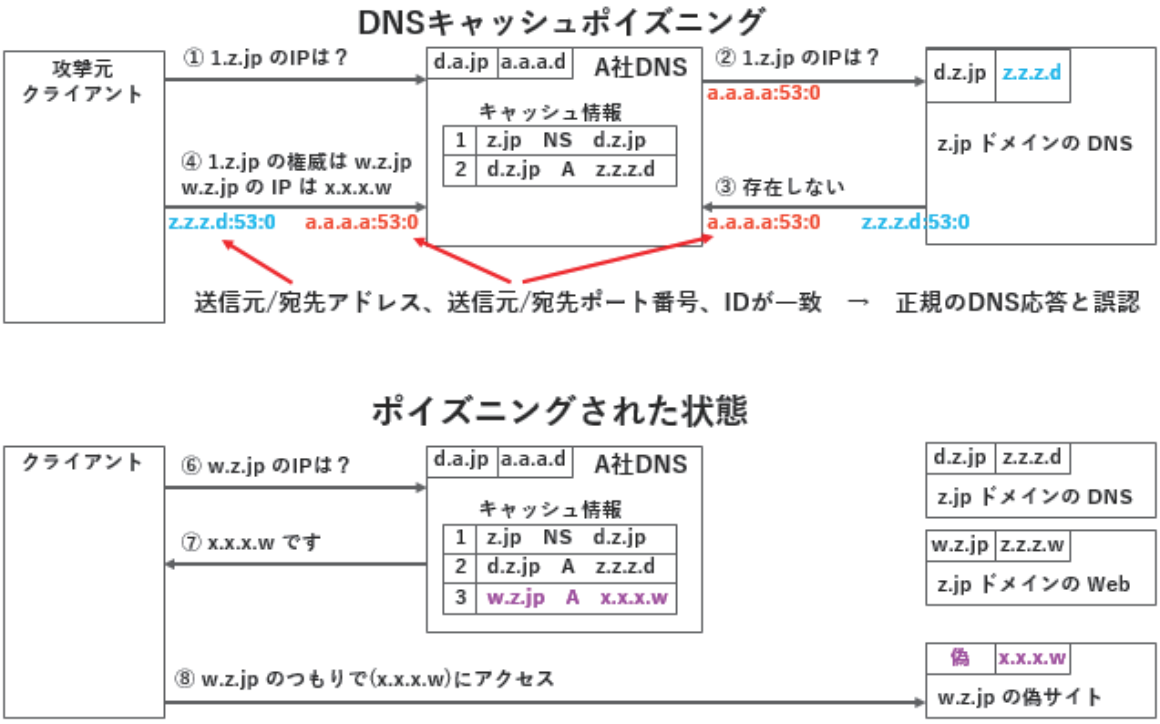
ホスト名	IP アドレス	役割
d.a.jp	a.a.a.d	クライアントからの問合せを直接受ける DNS
d.z.jp	z.z.z.d	z.jp ドメインに属すホストの情報を管理する DNS
w.z.jp	z.z.z.w	z.jp ドメインで運用されている Web サーバー

クライアントが d.a.jp に①w.z.jp の IP を問合せた段階では、d.a.jp は w.z.jp の情報を持っていません（「キャッシュ情報」の中に w.z.jp がない）。そこで②、③を経て情報を入手し④でクライアントに応答します。クライアントはそれを得て⑤で目的のサイト w.z.jp にアクセスできます。

いったんこの手順を経ると d.a.jp には w.z.jp に関する情報のキャッシュができるため、次に⑥同じ問合せを受けたときは d.z.jp への問合せを省略して⑦応答します。この「キャッシュ」の仕組みによってクライアントはすばやく答えが得られ、インターネット全体としては通信量を削減できます。

②の問合せパケットでは送信元のアドレス：ポート番号：ID が a.a.a.d：53：0 で、これは③の応答パケットの宛先と一致します。DNS は問合せと応答でこれらの数字が一致したときに正規の応答パケットであるとみなしますが、ここに脆弱性があります。

6 DNS キャッシュポイズニングの仕組み



DNS キャッシュポイズニングは、キャッシュの仕組みの脆弱性を突いてキャッシュサーバに不正なキャッシュ情報を注入する攻撃です。
攻撃元クライアントは送信元を偽装して①存在しないホスト情報についての問合せを出します。1.z.jp というホストは存在しないため d.z.jp からは③存在せずというエラー情報が帰ってきますが、このとき攻撃元クライアントからも d.z.jp からのパケットに見せかけた④偽の応答を送ります。

DNS の問合せ/応答パケットには、問い合わせ時に生成する ID という 16 ビットのランダムな値が含まれています。正規の手順であれば②の問合せに含まれる ID 値と同じ ID 値で③のパケットが送り返されてきます。DNS は送信元/宛先の IP アドレス、送信元/宛先のポート番号、ID が一致すれば正規の DNS 応答と見なします。したがって、攻撃者はそれらの情報が③と同じになるように④のパケットを組み立てて送れば正規の応答と誤認させることができます。このうち送信元/宛先の IP アドレスは公開されているため入手可能です。送信元/宛先ポート番号は多くの場合「53」という固定値が使われていました。ID はランダム値ですので本来は攻撃者が③の ID を知ることはできませんが、16 ビットしかないため多数の試行をすれば偶然一致することがありました。

そこで、1.z.jp という実在しないホスト情報についての問い合わせを、「1」の部分を変えて多数繰り返すことで ID を偶然一致させる確率を増やします。④の応答に「w.z.jp の IP アドレスは x.x.x.w である」という偽の情報を含めておくことにより、ID が一致したときにはそれがキャッシュされてポイズニングされた状態になります。

ポイズニングされた状態ではキャッシュ情報の中に w.z.jp=x.x.x.w という偽の情報があるため、次に⑥w.z.jp の問合せが来ると⑦それを返答してしまい、クライアントは w.z.jp のつもりで(x.x.x.w)にアクセスさせられてしまいます。この場合、ブラウザのアドレスバーを見ても正規のアドレスが表示されているため、偽サイトだということに気づくのは困難です。

キャッシュポイズニングを防ぐ方法としては「キャッシュサーバ隔離」と「送信元ポート番号ランダム化」があります。

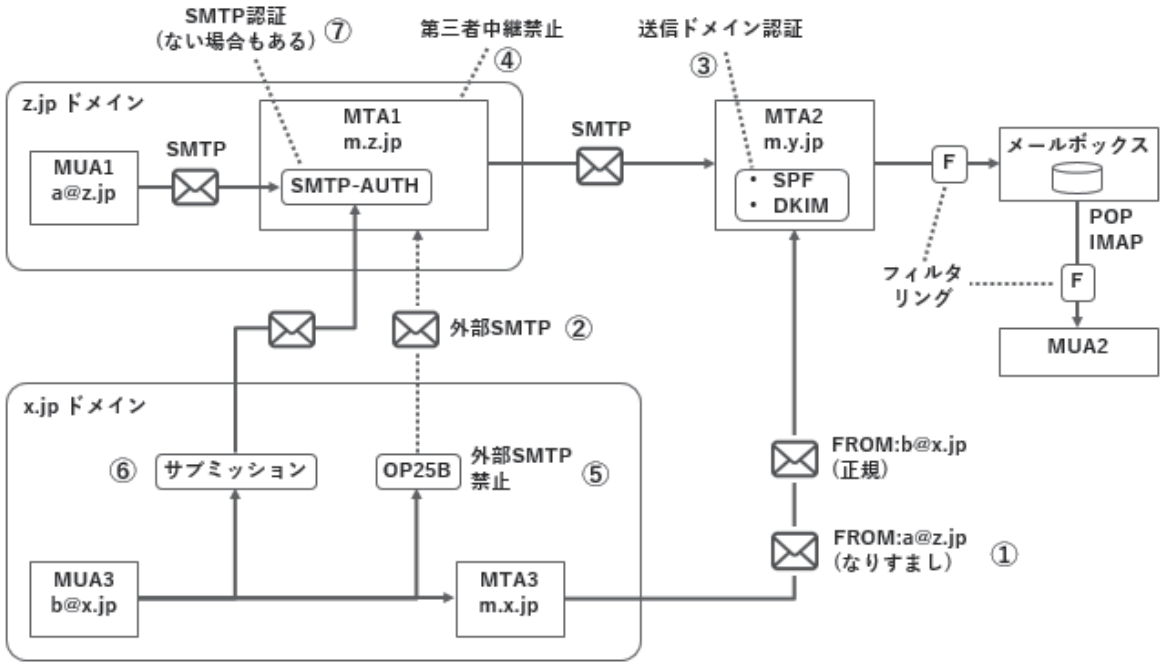
キャッシュサーバ隔離

コンテンツ DNS サーバーとキャッシュ DNS サーバーを別々に設置し、キャッシュサーバへのインターネット外部からの再帰的問合せを禁止することにより、外部からの攻撃は防げます。

送信元ポート番号ランダム化

②の問合せをする際の送信元ポート番号は本来ランダムに選べますが、古い DNS プログラムでは「53」固定となっているものがありました。ID はランダムでしたが 16 ビットしかないため総当たりで試すことが可能でした。この攻撃手法が発見された後、多くの DNS サーバーで送信元ポート番号のランダム化対応が行われています。ポート番号は 16 ビット、ID も 16 ビットで合わせて 32 ビットになるため、両方をランダム化すれば偶然一致する可能性は極めて低くなります。

7 迷惑メール対策



まず正規のメールの送受信の流れを確認します。
MUA(Mail User Agent)はメールの送受信をするために人間が操作するクライアントソフトウェアのことを言い、MTA(Mail Transfer Agent)はメールの転送をするソフトウェアのことを言います。一般に、MTA はメールサーバー上で稼働します。
z.jp ドメインに属すユーザーa@z.jp が MUA1 を使って y.jp ドメイン宛にメールを送信すると、MUA1 は z.jp ドメインのメールサーバーm.z.jp に接続して SMTP プロトコルでメールを転送します。MTA1 は宛先ドメインである y.jp のメールサーバーm.y.jp で稼働する MTA2 にメールを転送します。MTA2 はそのメールを宛先(受信者)のメールボックスに配送し、受信者は MUA2 で POP や IMAP プロトコルを使ってメールボックスを読み出します。以上が最も単純なメール送受信の流れです。

次に不正なメールのケースです。
x.jp ドメインのユーザーb@x.jp が MUA3 を使って y.jp ドメイン宛にメールを送信する際、正規の方法であれば MTA3 を介して FROM:b@x.jp というメールを送信するはずですが、①送信者を FROM:a@z.jp に偽装される場合があります。あるいは②本来利用できない z.jp ドメインの MTA1 を不正利用される場合もあります。迷惑メールやフィッシング、ウイルス等のメールは多くがこれらの不正な方法で送られているため、防がなければなりません。

①の方法による送信ドメイン偽装（なりすまし）を防ぐために使われるのが受信側の MTA で実施する③送信ドメイン認証で、大きく SPF と DKIM の 2 つの方法があります。ただしこれは送信側でも SPF、DKIM に対応していなければ機能しません。

②は本来利用資格のない b@x.jp に MTA1 を不正に利用されてしまうのが問題です。多くの迷惑メールがこの方法で送られています。これを防ぐには MTA1 の側で z.jp ドメイン外からの接続を受け付けないようにする④第三者中継禁止の設定を行い、x.jp ドメインの側では⑤外部 SMTP 禁止の設定を行います。

外部 SMTP 禁止は OP25B(Outbound Port 25 Blocking)と呼ばれる方法で、x.jp ドメインから外部への SMTP ポート(25 番)の接続を閉じるものです。x.jp ドメインを管理する ISP が行います。

この方法で多くの迷惑メールを防止できますが、しかし副作用もあります。たとえば z.jp ドメインの正規ユーザーa@z.jp が出張等の外出先で x.jp ドメインに接続した状態でメールを送信しようとしても、MTA1 には OP25B のため接続できず、MTA3 では第三者中継禁止設定により FROM を z.jp ドメインとするメールは送信出来ません。

そこで、第三者中継禁止の例外として設けられているのが⑥サブミッションポートによる接続です。サブミッションポートとしては一般に 587 番ポートが使われており、OP25B の対象ではないため x.jp ドメインからでも MTA1 に接続できます。ただし不正な第三者中継を防ぐため、送信者が正規のユーザーa@z.jp であるという認証をしなければなりません。そのために MTA1 に⑦SMTP-AUTH という SMTP 認証の仕組みを導入するのが一般的です。SMTP-AUTH は SMTP 接続を受け付ける前にユーザー名とパスワードで送信者の認証を行うものです。他のドメインからの接続を許す場合には必須ですが、自ドメイン(z.jp)内部からの接続に対しては省略する場合もあります。

8 演習問題

問 1

「サーバー要塞化」においては、「あらゆる入り口や権限を狭めておく」という【接続可能なクライアントの制限】が重要です。具体的な制限について、以下の表 A を、表 B の選択肢を使って埋めなさい。

（表 A）

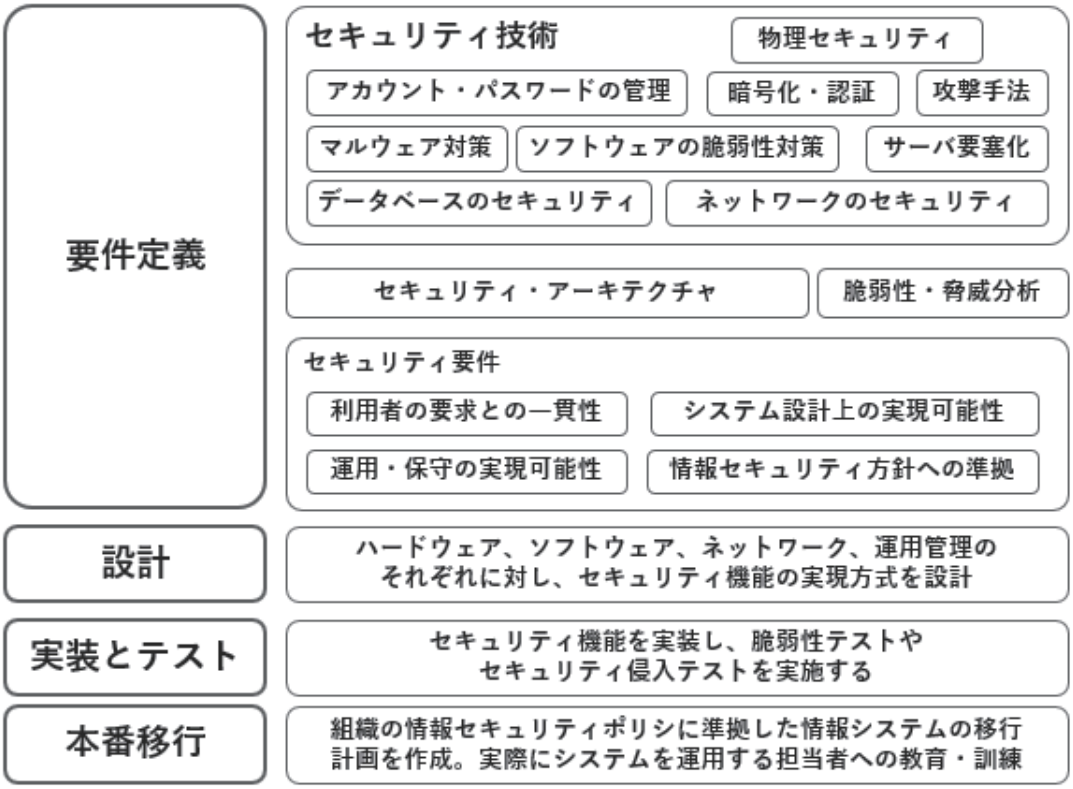
サーバー	ポートの（　　）
サービス（認証）	サービスの（　　）、認証の（　　）
オペレーション	脆弱性の（　　）、不要なプログラムの（　　）
アカウント	アカウントの（　　）
権限	権限の（　　）
プロセス、データ	データやプロセスの（　　）、（　　）
ログ	ログ（　　）・監視（　　）

（表 B）

A	解消
B	監視
C	採取
D	最小化
E	削除
F	停止
G	停止
H	導入
I	分離
J	閉鎖

第8章.
Web システム

1 セキュアな情報システム構築マネジメント



本章では、セキュアな情報システムを構築するためのマネジメントを通して、Web システムを構築する際に求められる具体的なテーマについてまとめておきます。

1．要件定義

構築する情報システムの要件定義を行う際、機能の定義だけでなく、セキュリティ要件についても明らかにします。

セキュリティ要件の定義は、システム化対象の業務が扱う情報資産について、情報セキュリティの方針に照らし、どのようなセキュリティ上の要求があるかを洗い出すことから始まります。すでに ISMS を導入している組織においては、ISMS の構築時に策定したリスク対応計画を適用します。

セキュリティ要件を具体的に定義するには、情報資産に対する脆弱性や脅威について把握しておく必要があります。そのためには、次に示すセキュリティ技術の知識が不可欠です。

- アカウント・パスワードの管理
- 暗号化・認証技術
- マルウェア対策
- サーバー要塞化

- ソフトウェアの脆弱性対策（サニタイジング等）
- データベースのセキュリティ対策
- ネットワーク（DNS、メール等の各サーバーを含む）のセキュリティ対策
- 物理セキュリティ対策
- 攻撃手法（SQL インジェクション、クロスサイトスクリプティング等）

情報資産に対する脆弱性や脅威を具体的に分析するため、セキュリティのアーキテクチャを設計します。このアーキテクチャには、関連するハードウェア、ソフトウェア、ネットワーク、運用管理が含まれます。このアーキテクチャに対し、セキュリティ・インシデントを想定したシナリオを適用し、脆弱性や脅威を分析します。

脆弱性・脅威分析により、構築する情報システムの問題点が洗い出されます。その点を踏まえ、優先度の高いリスクへの対応を中心に、セキュリティ要件を定義します。

たとえば、構築する情報システムのネットワークについては

・ファイアウォールの設置

・IPS の導入

などがセキュリティ要件となりえます。

構築する情報システムのソフトウェアについては

・利用者認証機能の導入

・権限定義に基づいたアクセス制御機能の導入

などがセキュリティ要件となりえます。

構築する情報システムの運用管理については

・サポート内容の定義

・ヘルプデスクの設置

などがセキュリティ要件となりえます。

定義したセキュリティ要件について、利用者の要求との一貫性、システム設計上の実現可能性、運用・保守の実現可能性、組織の情報セキュリティ方針への準拠性を考慮し、レビューを実施します。

レビューの結果をフィードバックし、セキュリティ要件を完成させます。

2．設計

セキュリティ要件を実現するために、セキュリティアーキテクチャを前提にして、ハードウェア、ソフトウェア、ネットワーク、運用管理のそれぞれに対し、セキュリティ機能の実現方式を設計します。

システム設計者と共同でレビューを実施した後、設計書として文書化します。

さらに、セキュリティ実装に関する作業計画、テスト仕様を作成します。

3．実装とテスト

ハードウェア、ソフトウェア、ネットワーク、運用管理のそれぞれに対してセキュリティ機能の実装を行ったうえで、脆弱性テストやセキュリティ侵入テストを実施します。

実装時にはセキュリティ機能の関するシステム文書類（設計書、利用者マニュアル、等）の更新を怠らないようにします。必要があれば、その更新した内容を組織の情報セキュリティ方針にフィードバックします。

ソフトウェア実装においては、セキュアプログラミングの手法を用います。幾つかの代表的な例を挙げます。

- 表示処理

  利用者から入力した文字列を表示するときは、文字列を無害化します。

- SQL 処理、OS コマンド処理

  利用者から入力した文字列を用いて SQL 文や OS コマンドを生成するときは、文字列を無害化します。

- ファイル指定処理

  利用者から入力した文字列を用いてファイルを指定するときは、ディレクトリトラバーサルを行わないようにします。
  ディレクトリトラバーサルとは、ファイル文字列中に他ディレクトリを指定する文字列を含ませることで、これができると、設計者が意図しないディレクトリにあるファイルを指定される事態を招きます。
  例）
  親ディレクトリの指定　　../
  サブディレクトリの指定　　./サブディレクトリ名

- 認証処理

  推測可能なパスワードの使用を禁止します。
  認証に連続して失敗したときはアカウントをロックします。

- 重要な処理の前に確認

パスワードを変更したときは、それを行おうとしている者が本人であることを確認します。そのため、本人のメールアドレスをあらかじめ登録しておき、そこにパスワード変更画面へのリンクを通知します。
ロボットではなく人間がアクセスしていることを確認するため、人間であれば解読できる画像をつかって回答を求めます。

- フォーム画面へのトークン埋め込み

重要な情報を送信するフォーム画面を偽装される攻撃に対処するため、正規のフォーム画面の Hidden フィールドにトークンを埋め込んでおきます。
トークンとはランダムな文字列であり、利用者が正規のフォーム送信用のページにアクセスするたびに、Web システムが毎回動的に生成します。
利用者がこのフォーム送信用のページから送信すると、トークンも一緒に送信されます。フォーム送信を受け取った Web システムは、自らが発行したトークンが埋め込まれているかをチェックすることにより、正規のフォーム送信用のページから送られたものであることを確認することができます。

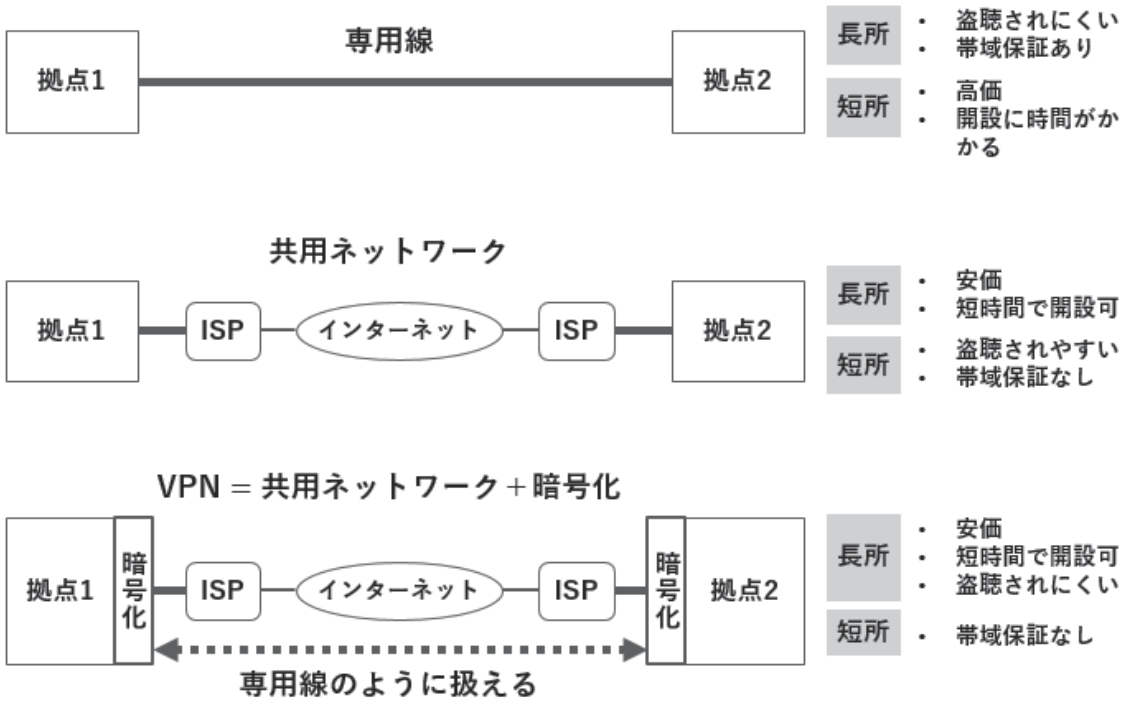
4．本番環境への移行

組織の情報セキュリティポリシーに準拠して、情報システムの移行計画を作成します。
開発されたセキュリティ機能に関して、実際にシステムを運用する担当者に教育・訓練を行います。

第9章.

VPN

1 VPN は仮想的な専用線



VPN（Virtual Private Network）とは、仮想的な専用線のことです。
専用線とは、LAN を引けない離れた拠点間を、その拠点間の通信専用に結んだ特別な回線のことを言います。第三者は専用線の通信を盗み見ることができないため、安全に通信することができます。通常、専用線には帯域保証もあります。しかし、専用線は大変高価な上に、物理的に線を引く工事が必要になるため、思い立った時にすぐに利用できないという不便さがあります。

一方、送信者と受信者がインターネットのような共用ネットワークを使用して通信する方法ならば安価かつすぐに利用できますが、共用ネットワークは盗聴されやすく、通常は帯域保証もありません。

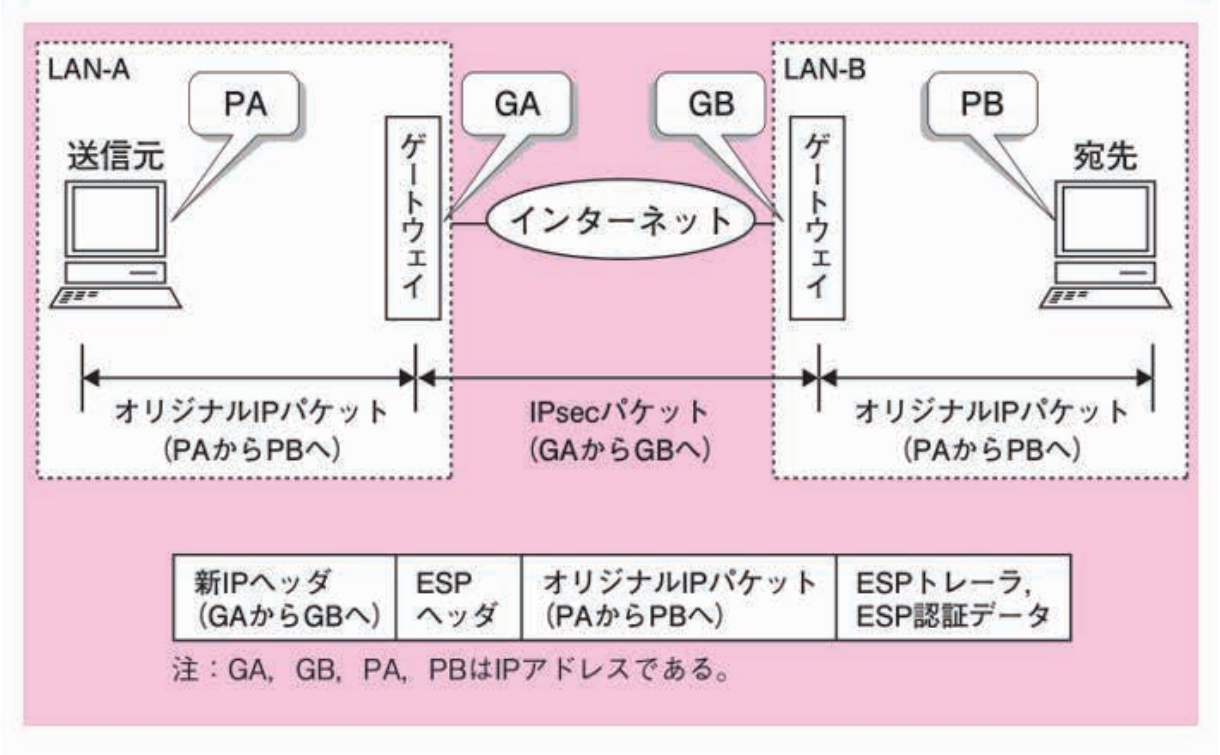
そこで、共用ネットワーク区間の通信を暗号化できれば第三者は盗聴できなくなり、送信者と受信者が専用線で結ばれているかのような状態になります。つまり VPN は暗号化技術を用いることによって、共用ネットワークで専用線と同等の安全な通信を実現する技術である。物理的な専用線に比べて構築するための経費や時間が要らないメリットがあるため、インターネットを介した通信で広く用いられています。共用ネットワークを使用するため通常は帯域保証がありませんが、通信会社が提供する VPN サービスの中にはある程度の帯域保証をするものもあります。

VPN を実現するには、共用ネットワーク区間を通過するパケットを暗号化用のプロトコルでカプセル化する必要があります。そのために使われる代表的なプロトコルは次の二つです。

1．IPsec
2．SSL

以降の節では、この二つのプロトコルを使用した VPN について解説します。

2 IPsec：LAN 間接続形態



IPsec による VPN の主な利用形態には、「LAN 間接続」と「リモートアクセス」の 2 種類があります。

LAN 間接続は 2 つの LAN の間を IPsec ゲートウェイで接続する方法で、「本社と支社の間を安全に接続したい」など、すでに双方に LAN がある場合に使われます。主な使用条件は下記のとおりです。

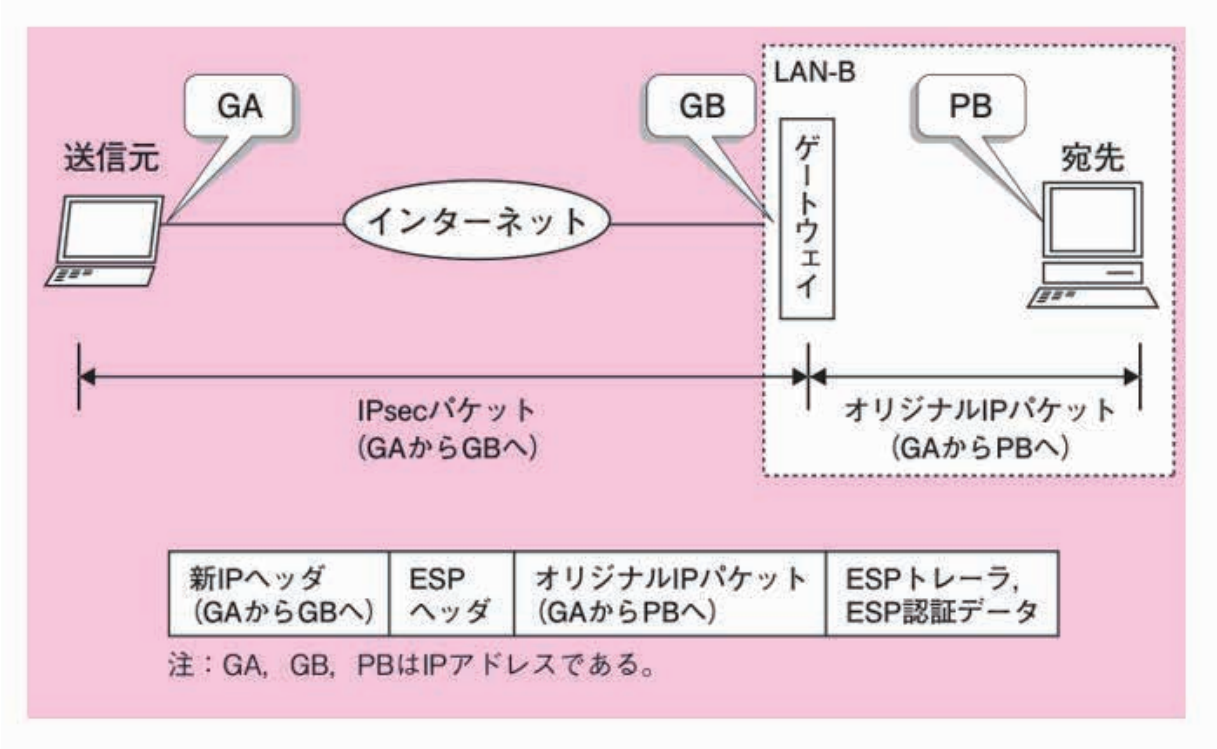
■ISAKMP SA

IPsec ゲートウェイは固定 IP アドレスを持つため、メインモードが使用されます。

■IPsec SA

実際のデータ通信は IPsec ゲートウェイ間をトンネル・モードで接続し、インターネットを介した通信では暗号化が必要なので ESP を使用して行います。

3 IPsec：リモートアクセス形態



リモートアクセスは、一台の端末をインターネットを介して拠点の LAN に接続する方法で、「外出先でモバイル回線から社内のサーバーにアクセスする」などの場面でよく使われます。主な使用条件は下記のとおりです。

■ISAKMP SA

リモートアクセス端末は固定 IP アドレスを持たないため、アグレッシブモードが使用されます。

■IPsec SA

LAN 間接続同様、実際のデータ通信はトンネル・モードで接続し、インターネットを介した通信では暗号化が必要なので ESP を使用して行います。

■IPsec クライアントソフト

リモートアクセス携帯では端末側に IPsec ゲートウェイがありません。代わりに、端末に IPsec クライアントソフトをインストールしておきます。IPsec ゲートウェイと違って、自分の端末の通信だけが VPN の対象になります。

4 SSL-VPN の動作方式

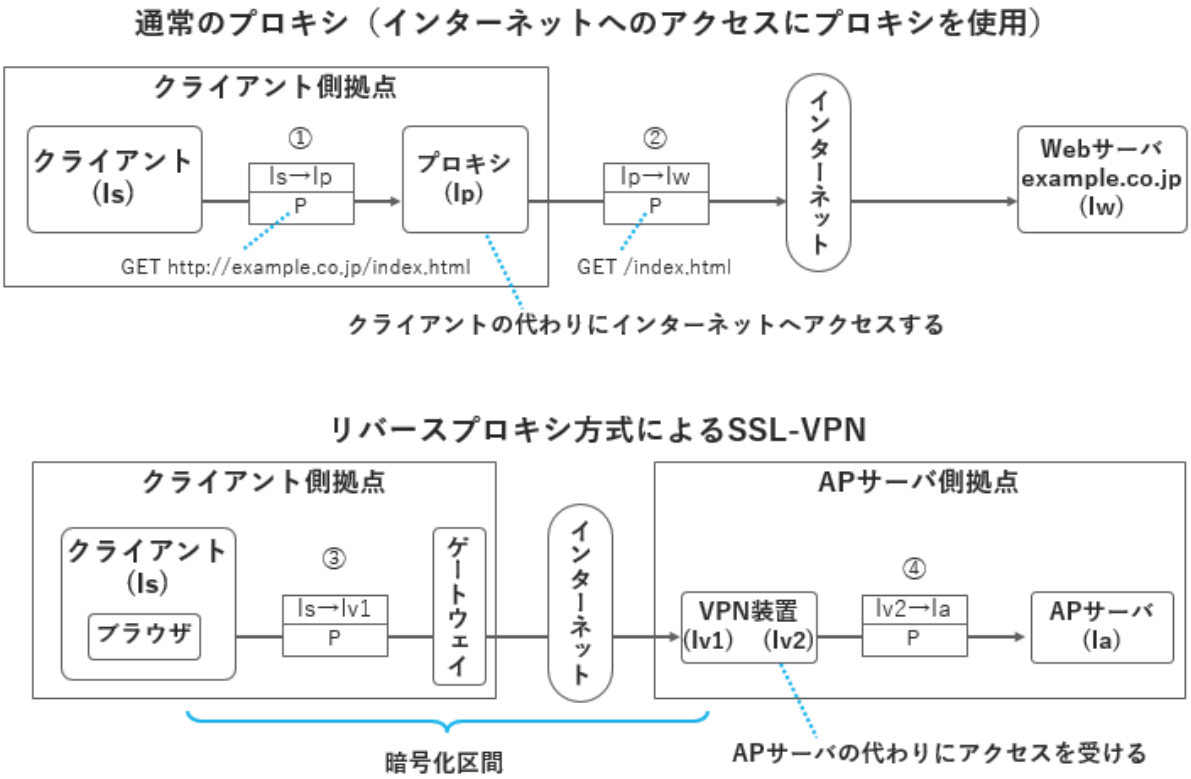
動作方式	専用モジュール	使用できるアプリケーション
リバースプロキシ方式	不要	ブラウザ上で動作できるアプリケーションに限定
ポートフォワーディング方式	必要	ポート番号が実行時に変化しないアプリケーション限定
L2 フォワーディング方式	必要	アプリケーションの制限なし

SSL-VPN は、Web の通信を高セキュリティ化するために作られた SSL を用いて VPN を実現する方法です。SSL-VPN という名前が定着しているため SSL の名前が残っていますが、実際には現在は SSL の発展形である TLS が使われています。

SSL-VPN は、拠点内のアプリケーションサーバ（AP サーバ）に PC がインターネット経由でリモートアクセスするときに利用されます。主に三つの動作方式に類別でき、それぞれ上図に示す特徴を有しています。

以下、それぞれの動作方式を解説しますが、SSL-VPN はベンダ独自の技術のため、同じ動作方式であっても、実装の詳細はベンダによって異なっています。したがって、本書で説明しているのは実装の一例と考えてください。

5 リバースプロキシ方式



リバースプロキシ方式による SSL-VPN を、通常のプロキシと比較しながら説明します。

図の上段はインターネットへのアクセスにプロキシを使用する、通常の（リバースではない）プロキシ動作です。Is, Ip, Iw はそれぞれクライアント、プロキシ、Web サーバーのアドレスとします。クライアントは①プロキシに対して Web アクセスのリクエストを出します。①の宛先アドレスが Ip（クライアント側拠点内のプロキシ）で、ペイロード P は GET http://example.co.jp/index.html のように FQDN(example.co.jp)を含んでいることに注意してください。プロキシは FQDN の名前解決を行って新しく②Web アクセスのリクエストを出します。②では送信元→宛先アドレスが Ip→Iw に変わっています。つまり、「クライアントの代わりにインターネットへアクセスする」のがこの場合のプロキシの役割です。

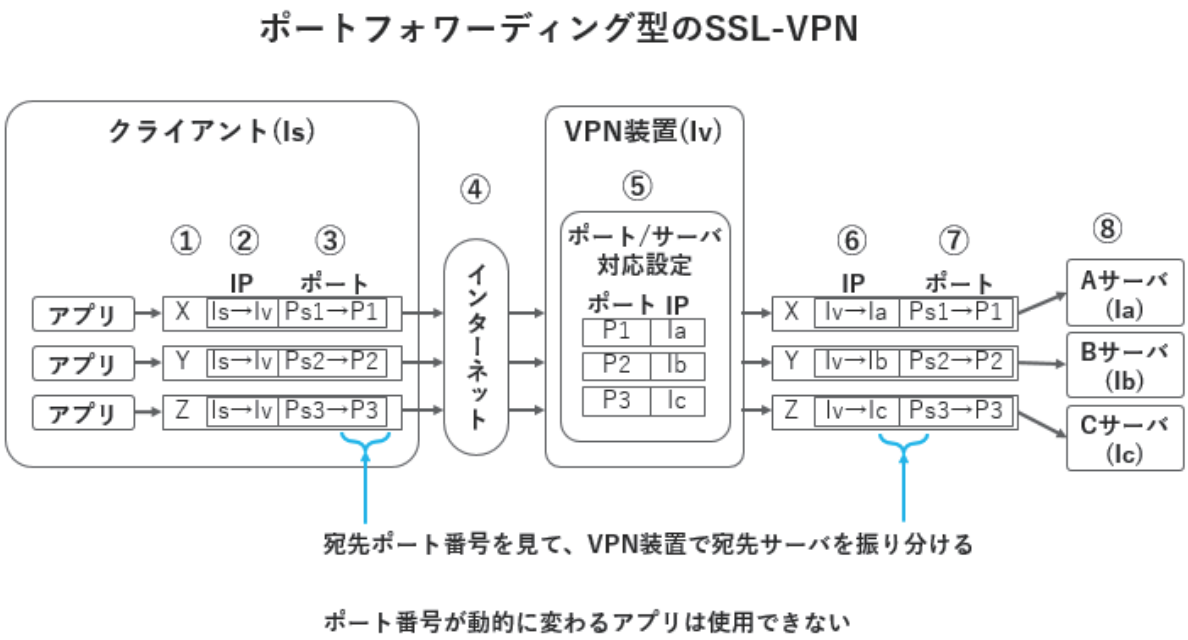
一方、下段はリバースプロキシ方式による SSL-VPN のしくみです。VPN 装置は AP サーバー側拠点内にあり、インターネット側と内部側でそれぞれ Iv1, Iv2 というアドレスを持っています。Iv1 はグローバル IP アドレス、Iv2, Is, Ia はプライベート IP アドレスです。クライアントのブラウザからの Web アクセスリクエスト③は VPN 装置(Iv1)宛です。VPN 装置はそれを受けて新しく④SP サーバーへの Web アクセスリクエストを出します。④では送信元→宛先アドレスが Iv2→Ia に変わっています。つまり、「AP サーバーの代わりにインターネットからのアクセスを受ける」のがこの場合のプロキシ(VPN 装置)の役割です。

リバースプロキシ方式での SSL-VPN の具体的な接続手順は次のようなものになります。

［1］利用者が VPN 装置宛てに TLS 通信を行う。利用者認証に成功すると、同装置が提供する Web ページの中から、AP サーバーを選択する。
［2］VPN 装置がリバースプロキシとなり、AP サーバー宛てに HTTP 通信を行う。

利用者はブラウザを用いて VPN 装置にアクセスします。PC と VPN 装置間の通信は TLS で暗号化されており、VPN 装置はこれを復号した後、AP サーバーに中継します。利用者から見ると、一連の動作はブラウザ上で行われています。したがってリバースプロキシ方式で使用できるアプリケーションは、ブラウザ上で動作できるもの（基本的に HTTP）に限定されます。

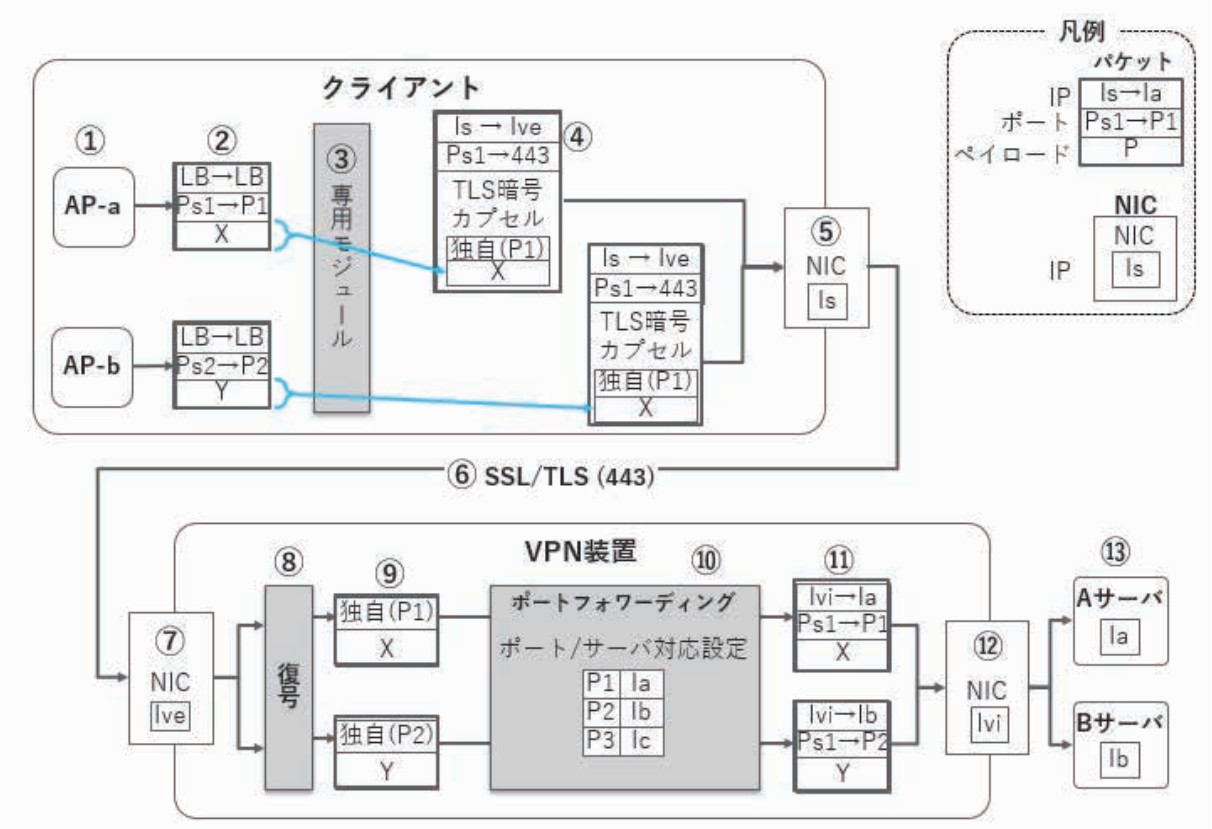
6 ポートフォワーディング



上図はポートフォワーディング方式のおおまかな動作イメージです。
Is、Iv、Ia、Ib、Ic はそれぞれクライアント PC、VPN 装置、ABC の各サーバーの IP アドレスとします。

クライアントで動作するアプリが①X、Y、Z のパケットを出し、それが最終的に⑧A、B、C の各サーバーに届くとします。①の段階では各パケットの②宛先 IP アドレスはすべて Iv(VPN 装置の IP)が指定されていて、③宛先ポートが違う状態です。このパケットをインターネットに送り出して VPN 装置に届くと、VPN 装置は⑤ポート/サーバーの対応設定を見て⑥⑦宛先 IP アドレスを設定し直して⑧サーバーへと送り出します。このように「宛先ポート番号を見て VPN 装置で宛先サーバーを振り分ける」のがポートフォワーディング方式です。したがって、ポート番号が動的に変わるアプリは使用できません。また、ポート番号ごとに宛先サーバーが一意に決まらなければならず、VPN 装置にポート/サーバーの対応関係を設定しておく必要があります。

7 ポートフォワーディング（詳細）



ポートフォワーディング方式のより詳細な動作イメージです。右上の凡例のように太枠の箱はパケットを表し、Is→Ia は送信元と宛先の IP アドレス、Ps→P1 はポート番号を表します。NIC(Network Interface Card)の箱の中の小箱の中はその NIC に設定されている IP アドレスを表します。

ポートフォワーディング方式ではクライアントに③専用モジュールをインストールしておきます。クライアント PC の中の①アプリケーションが②送り出すパケットの宛先 IP アドレスはループバックアドレス(LB)です。このパケットを③専用モジュールが受けて④ペイロードを TLS 暗号でカプセル化します。ここで IP アドレスは Is→Ive(VPN 装置の外部 IP アドレス)宛に、ポート番号は TLS 通信のポート 443 に書き換えられます。TLS 暗号カプセルにはペイロードの他に独自ヘッダ(P1)も含まれています。元のパケット②のポート番号 P1 は独自ヘッダの中に保存されています。この独自ヘッダの仕様は SSL-VPN の実装により異なります。

④のパケットは⑤NIC からインターネットへ送信され、⑥SSL/TLS ポート(443)を通って⑦VPN 装置の外部 NIC で受信されます。VPN 装置は⑧TLS 暗号カプセルを復号して⑨ペイロードを取り出し、⑩ポートとサーバーの対応設定を見て⑪新しいヘッダに IP アドレスとポートを設定して⑫内部 NIC から送信します。こうして⑬最終的な宛先サーバーに受信されます。

■ループバックアドレス

②の段階ではパケットの宛先 IP アドレスはループバックアドレスです。これを実現するためには PC の hosts ファイルを書き換えて AP サーバーのホスト名に対応する IP アドレスとしてループバックアドレスを登録する必要があります。この書き換えを専用モジュールのインストール時に行います。

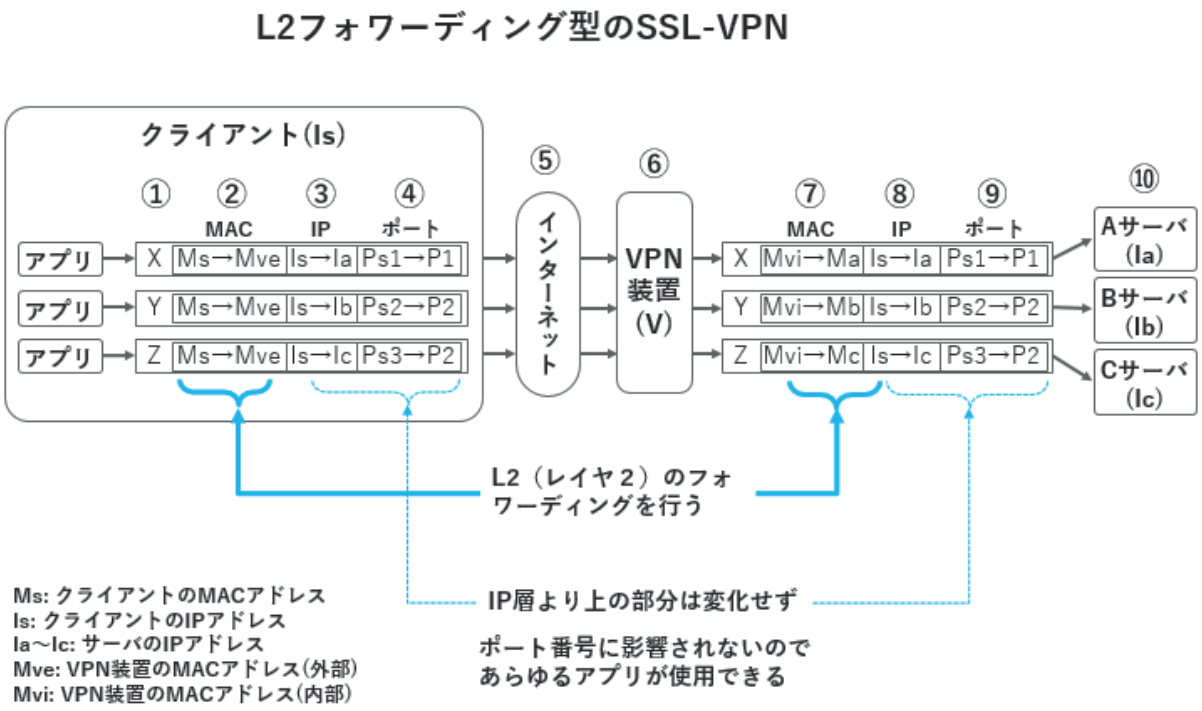
■利用者認証

前述の手順には明記していませんが、通常どこかのタイミングで利用者認証を行います。その具体的な方法は実装依存です。

■プロキシ動作

フォワーディングという名称がついていますが実際には VPN 装置はプロキシの動作をしており、TCP コネクションは VPN 装置でいったん終端します。

8 L2 フォワーディング



L2 フォワーディング方式は仮想的にみると同じ L2 ネットワーク内に VPN 装置とクライアント PC が存在する仕組みになります。このとき、VPN 装置はルータまたは L2 スイッチのどちらかの役割を担います。以降の解説では VPN 装置がルータの役割を持ち、クライアント PC のデフォルトゲートウェイと見なせる場合を例に説明します。

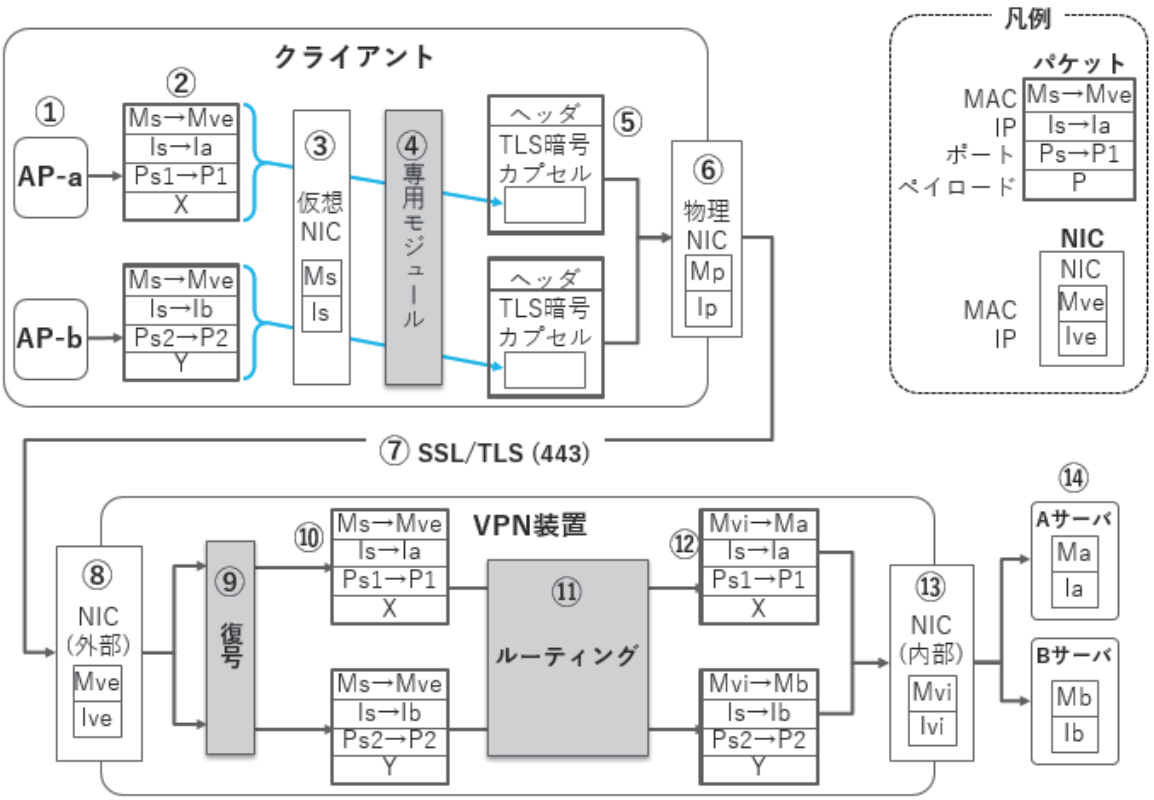
上図が L2 フォワーディング方式のおおまかな動作イメージです。
Is、Iv、Ia～Ic はそれぞれクライアント PC、VPN 装置、ABC の各サーバーの IP アドレスで、Ms、Mve、Mvi、Ma～Mc は MAC アドレスとします。

クライアントで動作するアプリが①X、Y、Z のパケットを出し、⑤インターネットに送り出され、⑥VPN 装置を経て、最終的に⑩A、B、C の各サーバーに届くとします。

①の段階で各パケットには②宛先 IP アドレスとして A～C サーバーの IP が指定されており、③④と⑧⑨を比べてみると IP とポートには変化はありません。②と⑦を比べると MAC アドレスの部分が変わることがわかります。これは VPN 装置がクライアント側 LAN と AP サーバー側 LAN の境界でルータとして機能している場合と同じ動きです。VPN 装置が L2（レイヤ 2）のフォワーディングを行うため L2 フォワーディングと呼ばれています。

IP 層より上は変化せずポート番号に影響されないため、あらゆるアプリが使用できます。

9 L2 フォワーディング（詳細）



L2 フォワーディング方式のより詳細な動作イメージです。右上の凡例のように太枠の箱はパケットを表します。ポートフォワーディング方式の時と違って MAC アドレスまで記載してあります。パケット内の MAC アドレスや IP アドレスは、NIC やサーバーの欄（③、⑥、⑧、⑬、⑭）に記載したアドレスにそれぞれ対応します。

L2 フォワーディング方式ではクライアントに④専用モジュールをインストールして③仮想 NIC を構築します。①アプリケーションが②送り出すパケットは③仮想 NIC を経て④専用モジュールで⑤TLS 暗号でカプセル化されます。ここでカプセル化されるのは②のイーサネットフレーム全体です。

⑤のカプセルには新しいヘッダをつけて⑥物理 NIC からインターネットへ送信され、⑦SSL/TLS ポート(443)を通って⑧VPN 装置の外部 NIC で受信されます。VPN 装置が⑨復号して取り出すパケット⑩は②と同じものです。その MAC アドレスを⑪⑫内部 LAN 用に書き換えて⑬内部 NIC から送信します。こうして⑭最終的な宛先サーバーに受信されます。

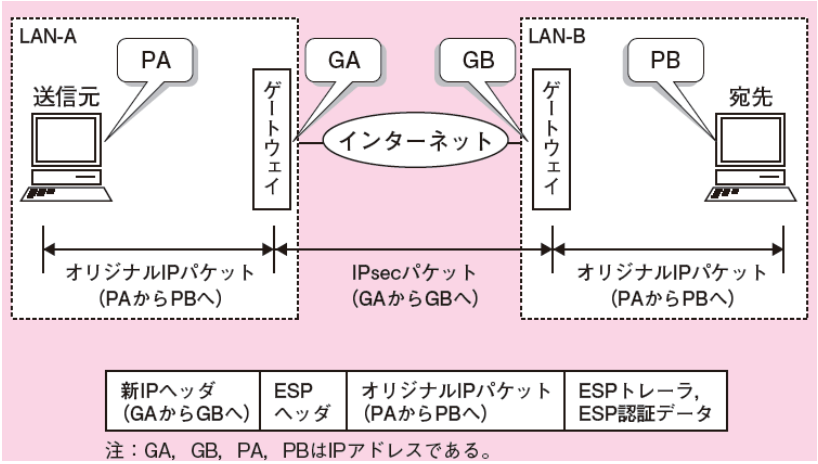
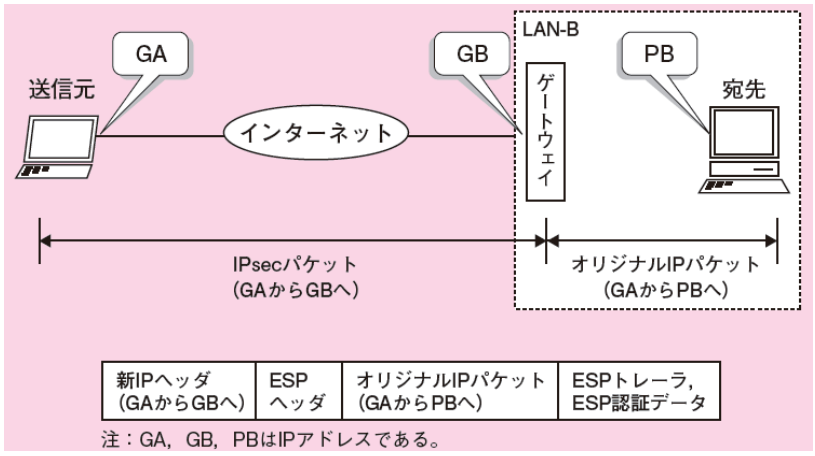
この方式では②～⑩へイーサネットフレームのトンネリングを行っているため、①アプリケーションからはクライアント PC が VPN 装置と同一の LAN 上にいるように見えます。このため IP に限らずさまざまな L3 パケットを転送できます。また、ポートフォワーディング方式では不可能な、実行中にポート番号が動的に変化する通信も転送できます。

10 演習問題

問 1

インターネット VPN を利用した LAN 間接続形態、リモートアクセス形態を比較した表を作成しました。空欄ア～カを埋めて、表を完成させてください。

主な設定		LAN 間接続形態	リモートアクセス接続形態
ISAKMP SA		ア	イ
IPsec SA	通信モード	ウ	エ
	セキュリティプロトコル	オ	カ

形態	ネットワーク構成図
LAN 間接続形態	
リモートアクセス形態	

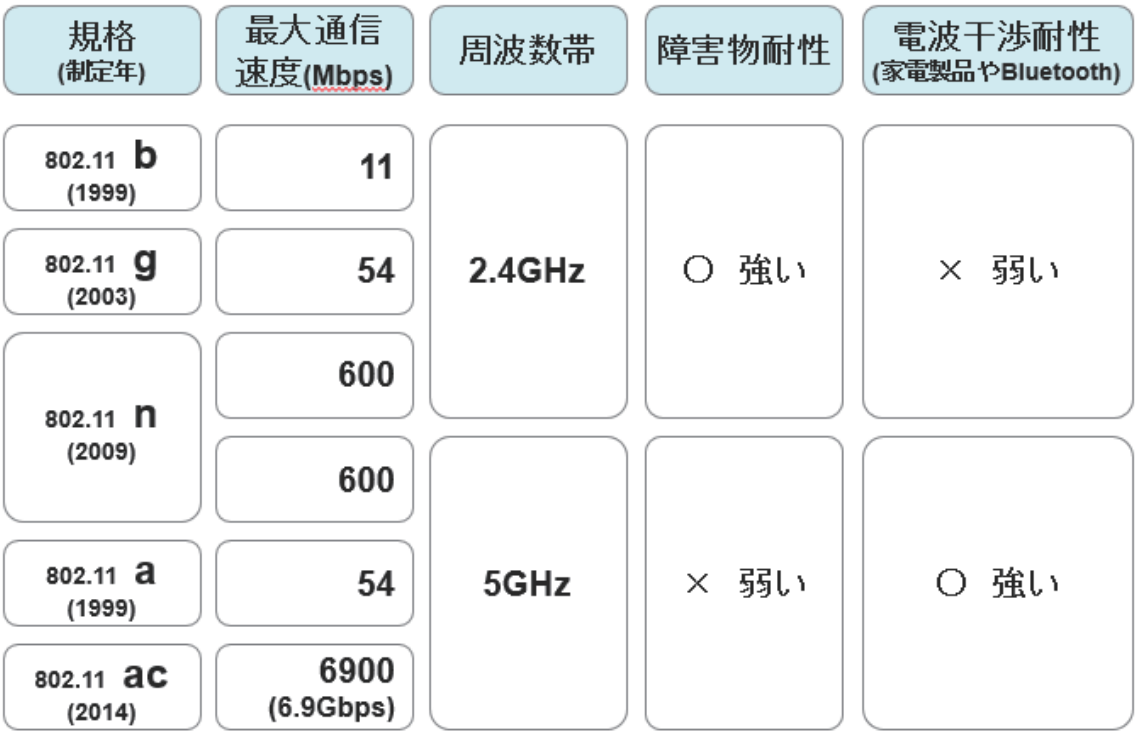
問 2

3 種類ある SSL-VPN の方式を比較した表を作成しました。空欄ア～カを埋めて、表を完成させてください。
なお、いずれの方式においても、ブラウザを搭載している端末で使用するものとします。

方式	専用 モジュール	アプリケーション
ア	必要	制限なし
イ	必要	制限あり（ポート番号が ウ しないもの）
エ	オ	制限あり（ブラウザ上で動作できるもの）

第10章.
無線 LAN

1 無線 LAN の規格



規格 (制定年)	最大通信速度(Mbps)	周波数帯	障害物耐性	電波干渉耐性 (家電製品やBluetooth)
802.11 b (1999)	11	2.4GHz	○ 強い	× 弱い
802.11 g (2003)	54			
802.11 n (2009)	600			
	600	5GHz	× 弱い	○ 強い
802.11 a (1999)	54			
802.11 ac (2014)	6900 (6.9Gbps)			

無線 LAN の主な規格は上表のようになります。無線 LAN の規格は IEEE802.11 の後ろのアルファベットで区別されるため、「規格」欄ではアルファベット部分を大きく表示してあります。上表は使用する周波数帯で大別してあり、制定年順には並んでいないことに注意してください。

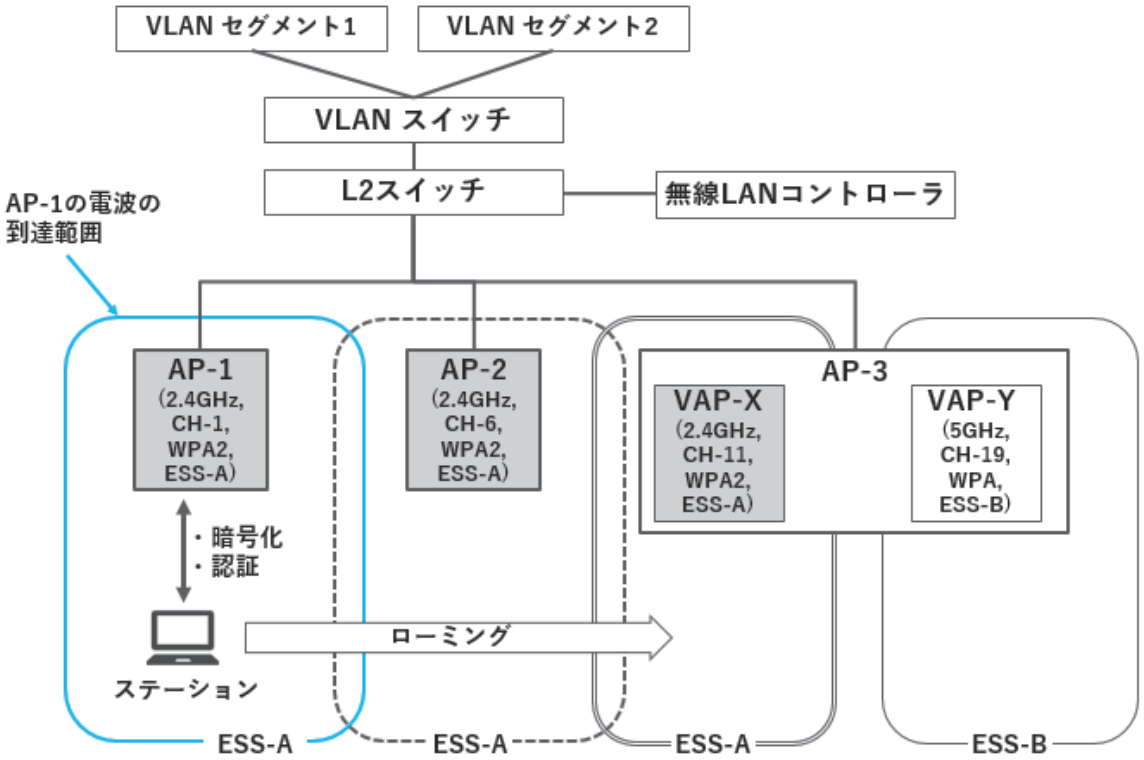
無線 LAN は 2.4GHz 帯または 5GHz 帯のいずれかの周波数帯を使用します。電波は周波数が高いほど直進性が強くなるため障害物の陰に回り込みにくくなります。そのため 2.4GHz 帯は障害物に強く、5GHz 帯は弱くなります。一方、2.4GHz 帯は

- 家電製品（電子レンジ）、医療機器（CT スキャン）や Bluetooth などの用途にも使われる
- 無線 LAN 用チャネルが 13 に分かれているが、実際に同時使用できるのは 3〜4 チャネルしかない

という理由で電波干渉に弱いのに対して、5GHz 帯は屋内では無線 LAN 以外では使用されておらず、19 チャネルを同時使用できるため干渉が起こりにくい性質があります。なお 2.4GHz 帯は屋内・屋外とも使用できますが 5GHz 帯を無線 LAN 用途に使用できるのは屋内のみです。

制定年が新しい 802.11n や 802.11ac では最大通信速度がそれぞれ 600Mbps、6.9Gbps と高速化していますが、これはデータ複数を複数のストリームに分割し、複数のアンテナを用いて同時に送受信する MIMO(Multiple Input Multiple Output)や、隣り合うチャネルを束ねて使うチャネルボンディングを使用した場合の理論値であり、受信側でもそれに対応している必要があります。

2 無線 LAN の構成イメージ



ビジネスユースの無線 LAN 環境では、複数の AP(アクセスポイント)を設置し、それらを無線 LAN コントローラで制御して VLAN につなぐ構成が一般的です。

ESS、ESS ID、SSID

端末(ステーション)が無線 LAN に接続しようとするときは、「ESS」と呼ばれる無線 LAN セグメントを選んで接続します。上図は ESS-A と ESS-B という 2 つの ESS を構成している例です。ESS-A は AP-1、AP-2、VAP-X という 3 つの AP によって提供されています。ESS の”SS”は Serivice Set を略したもので、使用する周波数帯、暗号化・認証方式、接続する VLAN セグメントなどの基本的な接続条件の定義を表しています。ESS が同じであれば同じ条件で接続できます。ESS を識別する名前を ESS ID と言い、最大 32 文字までの英数字で設定します。ESS ID は実際には多くの場合 SSID と呼ばれます。

バーチャル AP

図中の AP-3 は物理的には一台の AP ですが、その中に仮想的に 2 つの AP(VAP-X、VAP-Y)を設定しており、これをバーチャル AP 機能といいます。許可する接続条件が利用者によって異なる場合、バーチャル AP ごとに別な ESS を定義して別な接続条件を設定します。なお、図では VAP-X と VAP-Y

の電波到達範囲（ESS-A と ESS-B）が重ならないように描かれていますが、これは図を煩雑にしないための便宜上の表現であり、実際には AP-3 という物理的に一台の AP ですので両者は重なっています。

ローミング

無線 LAN を利用するステーションには、ノート PC やスマートフォン、タブレットのように頻繁に移動するものがあります。1 つの AP からの電波が届く範囲を越えて移動する場合、その前後で最寄りの AP に自動的に接続する機能をローミングと言います。ローミングをするためには対象となるすべての AP とステーションが同一の ESS に属している必要があります。また、AP がカバーする範囲（電波が到達する範囲）は重なっていなければなりませんが、電波干渉を避けるため、隣接する AP は異なるチャネルを用いる必要があります（図中、AP-1, AP-2,VAP-X のチャネル参照）。

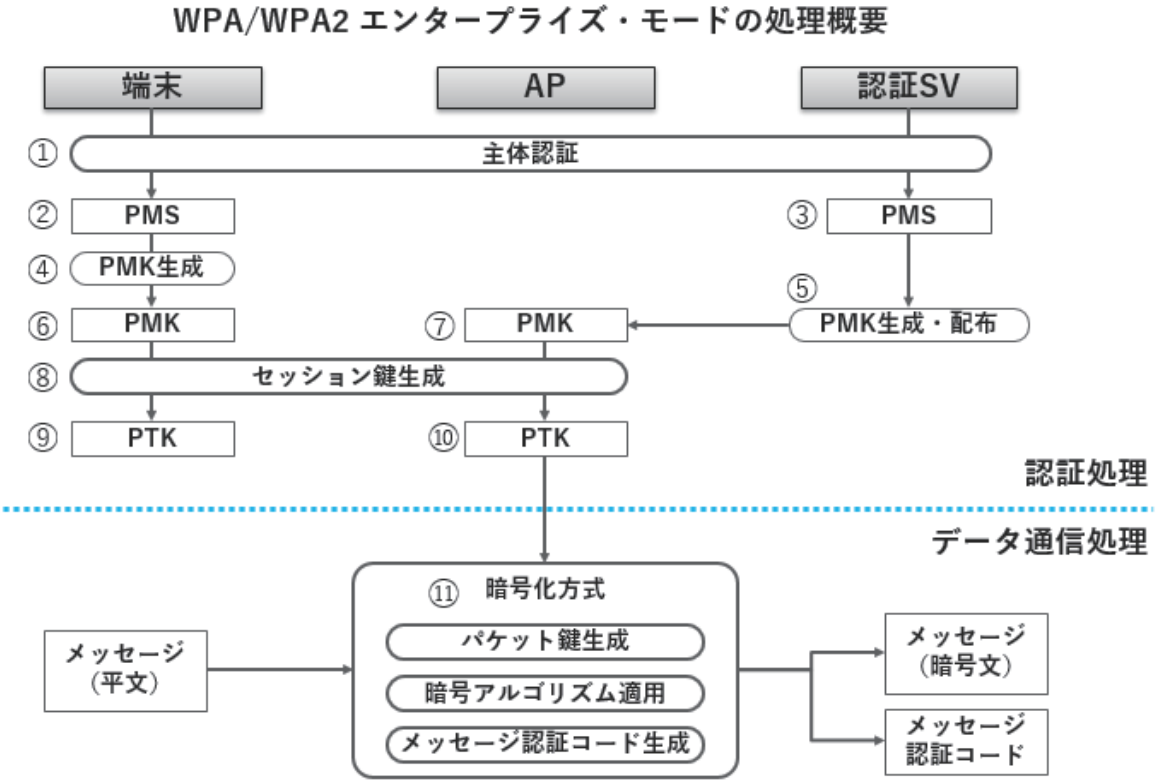
無線 LAN コントローラ

複数の AP が統合的に動作するように管理します。

認証、暗号化

電波は誰でも傍受できるため、無線 LAN での通信には認証と暗号化が不可欠です。

3 無線 LAN 認証・暗号化技術の構成要素



上図は無線 LAN の WPA/WPA2 エンタープライズ・モードでの認証・暗号化技術の構成要素の関係を示したものです。⑩PTK の下に引かれた点線より上の部分は認証処理の手順、下の部分はデータ通信処理の手順を示しています。なお、この図は「安全性を左右する要素」のイメージをつかむために細部を単純化してあり、一般的には使われていない用語も使用しています。

主体認証

端末と認証 SV は①何らかの方法(具体的には IEEE802.1X)で主体認証を行い、その結果として②③PMS(Premaster Secret)を共有します。端末と認証 SV の双方が④⑤PMS を元に PMK(Pairwise Master Key)を生成し、認証 SV から AP へ PMK を配布することにより⑥⑦端末と AP が PMK を共有します。PMK の「Master Key」という名前は、この鍵をもとにしてこの後の鍵生成を行うことを示しています。この段階では端末～AP 間の主体認証は完了していません。

セッション鍵生成

PMK を元に端末～AP 間で⑧セッション鍵生成の手順（具体的には 4way ハンドシェイク）を経て、端末～AP が相互に主体認証を行うとともに、双方で⑨⑩PTK(Pairwise Transient Key)を生成しま

す。PTK は通信セッションの間のみ使われる一時的な鍵であるため、Transient Key という名前がついています。通信のパケット数が所定の数を超えた場合、または通信セッションの途中で不正アクセスと思われるパケットを検知した場合は、PMK をもとにして PTK を作り直します。

（注：「セッション鍵」という名前は説明を分かりやすくするために本書でのみ使用する名前であり、一般的なものではありません）

暗号化方式

PTK を使って実際の通信を暗号化するプロセスには大まかにパケット鍵生成、暗号アルゴリズム適用、メッセージ認証コード生成の 3 つの要素があり、これらをまとめた暗号化処理全体の仕組みを⑪「暗号化方式」と呼び、具体的には TKIP や CCMP という方式があります。

パケット鍵生成

PTK は一つの通信セッションの間有効な鍵ですが、同一の鍵で何度も暗号化をすると解読されやすくなるため、実際に暗号化に使うカギはパケットごとに変更します。このため、PTK を基にしてパケット鍵を生成する手順が規定されています。

（注：「パケット鍵」という名前は説明を分かりやすくするために本書でのみ使用する名前であり、一般的なものではありません）

暗号アルゴリズム適用

メッセージ(平文)にパケット鍵を用いて暗号アルゴリズム（具体的には RC4 または AES）を適用し、メッセージ(暗号文)を生成します。

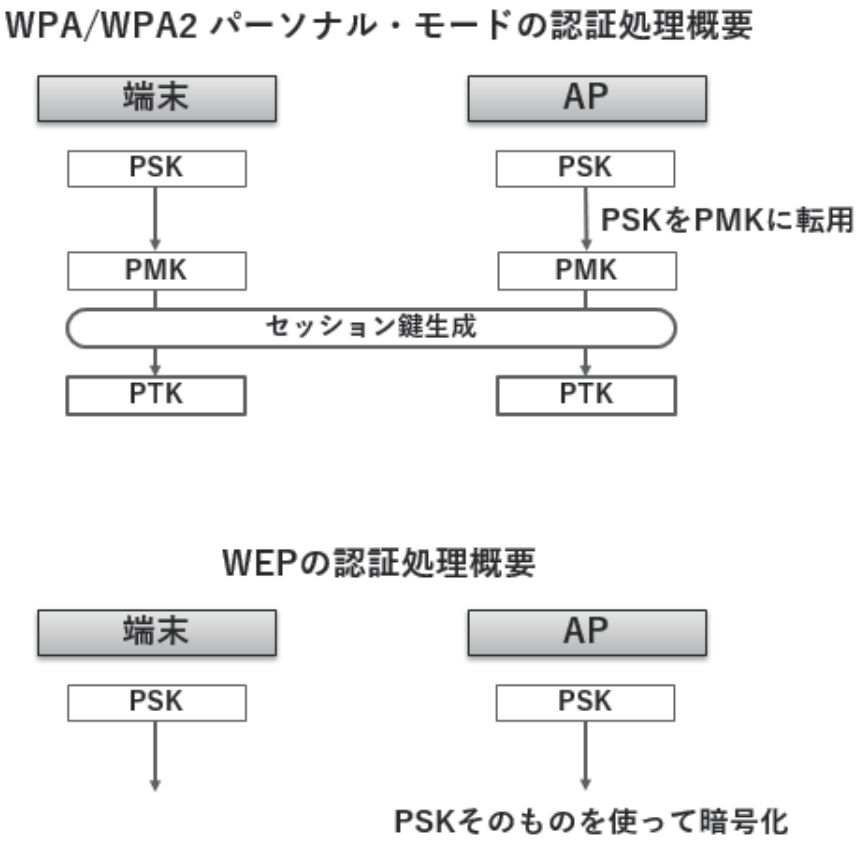
メッセージ認証コード生成

メッセージ(平文)と関連するヘッダ情報等にメッセージ認証アルゴリズム（具体的には CRC32, Michael, CBC-MAC 等）を適用してメッセージ認証コードを生成します。

通信の安全性に影響する要素

以上の各要素のうち、通信の安全性に大きく影響するのは図中の太枠で示した「主体認証方式」「セッション鍵生成方式」「暗号化方式」「パケット鍵の仕様」「暗号アルゴリズム」「メッセージ認証コード生成方式」の各要素です。WEP、WPA、WPA2 の各規格でこれらがどのように異なるかを後述します。

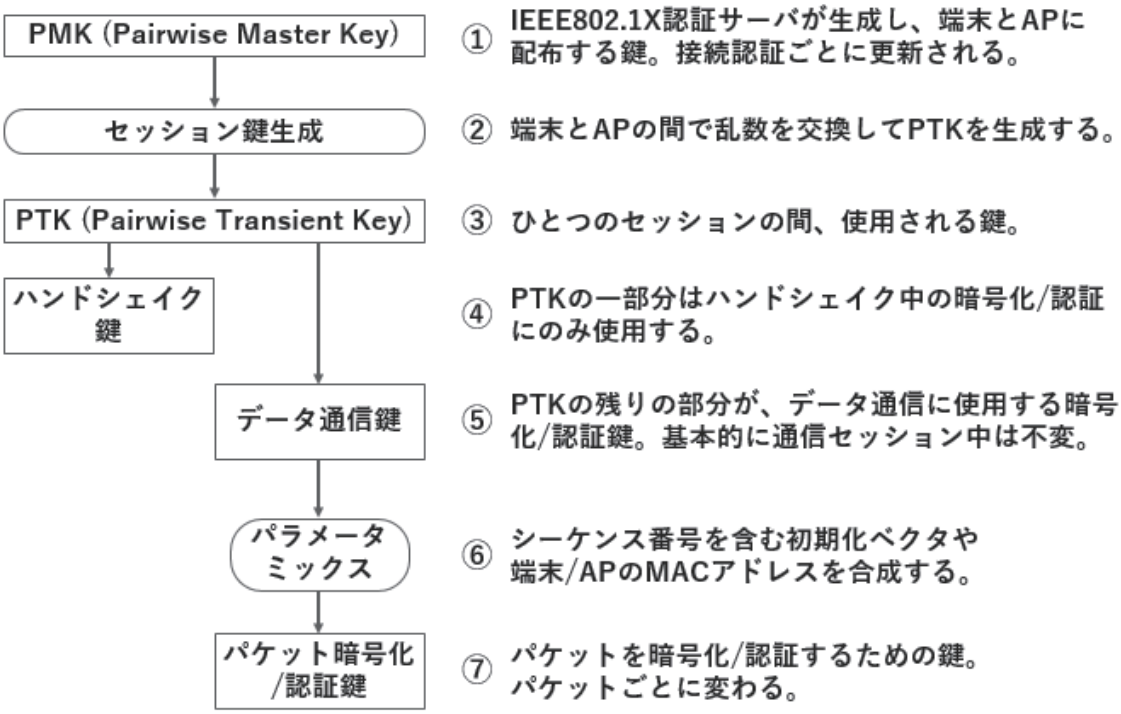
4 無線 LAN 認証・暗号化技術の構成要素



WPA/WPA2 パーソナル・モードでは認証 SV がないため、認証処理の手順が大きく異なります。パーソナル･モードでは端末と AP が PSK(Pre Shared Key, 事前共有鍵)をあらかじめ共有しており、この PSK を PMK として転用します。以後の処理はエンタープライズ・モードと同じです。長期間変更されない PSK の流出には弱い方法ですが、セッション鍵生成以後の安全性はエンタープライズ・モードと変わりません。

WEP ではセッション鍵生成の手順もなく、PSK そのものを使って暗号化します。セッション毎に変わる PTK ではなく、長期間変更されない PSK を使って暗号処理を行うため、非常に脆弱な仕組みと言えます。

5 パケット鍵の生成過程



PTK には実際には数種類の鍵が含まれていて、それぞれ別な用途に使われます。WPA/WPA2 で PTK からパケット鍵（パケットごとに変わる暗号化/認証鍵）を生成する過程は大まかに上図のようになります。

① IEEE802.1X 方式で主体認証を行うエンタープライズ・モードでは、IEEE802.1X 認証サーバーが PMK(Pairwise Master Key)を生成して、端末と AP に配布します。以後のプロセスは端末/AP の両者が同じ PMK を持っていることを前提に進行します。PSK 方式で主体認証を行うパーソナル・モードでは PSK そのものを PMK とします。

これ以後はエンタープライズ、パーソナルの両モードともに共通です。

② 端末と AP の間で乱数を交換して PTK を生成します。

③ PTK は 1 つのセッションの間、使用される鍵です。

④ PTK の一部は実際のデータ通信を始める前のハンドシェイクでの暗号化と認証にのみ使われます。PTK の長さは TKIP（後述）では 512 ビット、CCMP（後述）では 384 ビットです。

⑤ PTK のうち、ハンドシェイク鍵以外の部分を実際のデータ通信での暗号化/認証に使用します。TKIP では暗号化と認証に別な鍵を使用しますが、CCMP では同じ鍵を使用します。

⑥ データ通信用の鍵に、パケットのシーケンス番号を含む初期化ベクタ(IV, Initialization Vector)や端末と AP の MAC アドレスなどのパラメータを合成します。

⑦ ⑥の結果を実際の通信パケットの暗号化/認証に使用します。⑥で IV を合成しているためパケット暗号化/認証鍵はパケット毎に異なります。同一の鍵を二度と使用しないため解読されにくくなります。IV にはシーケンス番号を含むため、リプレイ攻撃から防御できます。

6 WEP,WPA, WPA2 の比較

	WEP	WPA	WPA2
主体認証方式	PSK	エンタープライズモード(IEEE802.1X) パーソナルモード(PSK)	
セッション鍵生成方式	なし	4wayハンドシェイク	
パケット鍵強度	PSK(104ビット) IV(24ビット)	PTK(128ビット) MACアドレス IV(48ビット)	PTK(128ビット) MACアドレス IV(48ビット)
暗号アルゴリズム	RC4	RC4	AES
暗号化方式		TKIP (Transient Key Integrity Protocol)	CCMP (Counter mode with CBC-MAC)
メッセージ認証コード生成方式	CRC32	Michael	CBC-MAC

無線 LAN の認証・暗号化規格である WEP、WPA、WPA2 を比較するとこのようになります。

WEP

WEP の主体認証は PSK 方式で行いますが、PSK は全端末共通かつ手作業で入力するため変更しづらく、通常は長期間変更されないため漏洩しやすく非常に脆弱です。個々の端末や個人を識別することもできません。WEP はセッション鍵を生成せず、PSK と IV（初期化ベクタ）を連結したものをパケット鍵として使います。以下の各項の理由により WEP の暗号化方式は非常に脆弱です。

- PSK は長期間変更されない
- IV は 24 ビットしかないため重複しやすい（通信データを長時間収集すると、同一の IV つまり同一の鍵を使用したパケットを複数収集できるため、解読しやすい）
- PSK と IV を単純連結しているため解読しやすい
- 暗号アルゴリズム RC4 も AES に比べると強度が落ちる
- CRC32 はエラーチェック程度の機能しか持たず、改ざん検知用のメッセージ認証コードとしては実質的に機能しない
- IV がランダムでシーケンスナンバーを持たないためリプレイ攻撃を防げない

WPA

WPA は WEP の脆弱性への応急処置として開発された規格であり、暗号アルゴリズム以外の部分は WEP よりも改良されています。暗号アルゴリズムが RC4 のままなのは、WEP を実装していたハードウェアでもソフトウェア更新のみで WPA に対応できるようにするためです。4way ハンドシェイクによる鍵交換を行って PTK(Pairwise Transient Key)と呼ばれる共通鍵のタネを動的に生成し、これに機器固有の MAC アドレスと 48 ビットの IV を加えて共通鍵を生成する TKIP という暗号化方式により、RC4 のままで安全性を高めています。WPA の PTK は実際には 512 ビットですが、データの暗号化にはそのうちの 128 ビットを使用します。メッセージ認証方式は CRC32 よりも強力な Michael を使用して改ざん検知を可能とし、IV がシーケンスナンバーの機能を持つためリプレイ攻撃も防ぐことができます。ただし、主体認証手順として PSK（パーソナルモード）を選んだ場合、主体認証については実質的に WEP と同等になってしまうため、企業ユースでは基本的にパーソナル・モードではなくエンタープライズ・モードを使用するべきです。

WPA2

WPA が WEP の脆弱性を緊急に置き換えるために登場した応急処置的な規格だったため暗号アルゴリズムは RC4 のままだったのに対して、WPA2 は本格的な高セキュリティ化を目指した規格です。WPA2 では暗号アルゴリズムをより強度の高い AES に変更し、それに合わせて暗号化方式と認証コード生成手順も CCMP へと変更しています。WPA が標準とする RC4-TKIP よりも AES-CCMP のほうが強力なため、可能な限り WPA2 を AES-CCMP で使用することが推奨されます。WPA2 の PTK は実際には 384 ビットですが、データの暗号化にはそのうちの 128 ビットを使用します。
WPA 同様、主体認証手順として PSK（パーソナルモード）を選んだ場合、主体認証については実質的に WEP と同等になってしまうため、企業ユースでは基本的にパーソナル・モードではなくエンタープライズ・モードを使用するべきです。

名称の混乱について

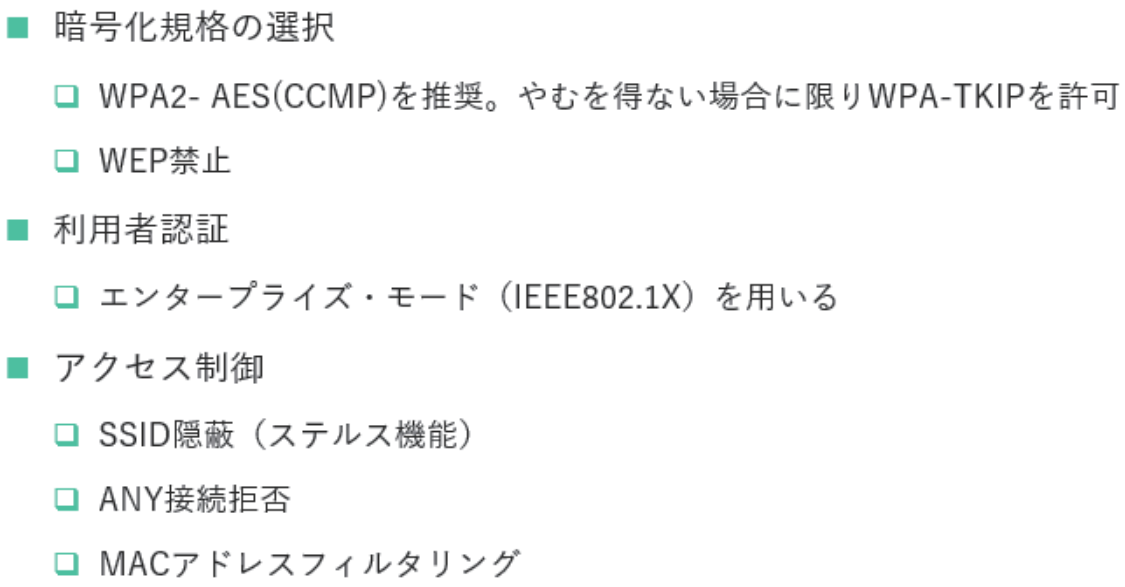
WPA、WPA2 と TKIP、CCMP、AES の名前が不統一に使われて一部に混乱を招く例がありますが、正しくは以下のような関係があります。

WPA、WPA2：主体認証から暗号化方式、メッセージ認証方式までを包括的に定めた規格
WPA：RC4-TKIP が必須、AES-CCMP は任意。
WPA2：RC4-TKIP は任意、AES-CCMP が必須。
TKIP：暗号アルゴリズム RC4 を用いる暗号化方式
CCMP：暗号アルゴリズム AES を用いる暗号化方式

このため、WPA2 規格の製品でも TKIP-RC4 を選択できる場合があり、WPA 規格の製品でも CCMP-AES を選択できる場合があります。ただし一般には次のような表記がよく使われています。

WPA-TKIP　→　WPA-RC4-TKIP、エンタープライズ・モードを意味する
WPA2-AES　→　WPA2-AES-CCMP、エンタープライズ・モードを意味する
WPA2-PSK(AES)　→　WPA2-AES-CCMP、パーソナル・モードを意味する

7 無線 LAN のセキュリティ対策



無線 LAN のセキュリティ対策の要点をまとめます。

暗号化規格の選択

極力 WPA2-CCMP(AES)を採用し、やむを得ない場合に限り WPA-TKIP を許可します。WEP は基本的に禁止します。

利用者認証

WPA/WPA2 規格でもパーソナル・モード(PSK)は事前共有鍵である PSK の漏洩リスクが非常に高いためビジネスユースには不向きです。エンタープライズ・モード(IEEE802.1X)を用います。

アクセス制御/SSID 隠蔽

通常、AP は自分の SSID を周囲に定期的に発信しています。SSID 隠蔽は、この定期的な通知を止める機能です。これにより、SSID を予め知っている正当な利用者だけに無線 LAN 通信を行わせることができます。

アクセス制御/ANY 接続拒否

無線 LAN 端末が AP に接続する際、SSID を指定せずに通信状態が最も良い AP と接続する ANY 接続という方法があります。特殊なケースを除いて、一般企業の無線 LAN 環境でこの方法を許可する理由はありません。SSID を予め知っている正当な利用者だけに無線 LAN 通信を行わせるため、AP に ANY 接続拒否の設定を行います。

アクセス制御/MAC アドレスフィルタリング

AP に接続させる無線 LAN 端末を限定するため、無線 LAN 端末の MAC アドレスを予め AP に登録することができます。MAC アドレスは無線 LAN デバイスに物理的に設定されていて偽装しにくいため、偶然パスワードを入手した人物等による、登録外の端末を使ったカジュアルな不正アクセスは防ぐことができます。しかし、MAC アドレスの偽装は不可能ではないため、明確な意図をもって不正アクセスを試みる者による攻撃をこの方法で防ぐことはできません。

8 演習問題

問 1

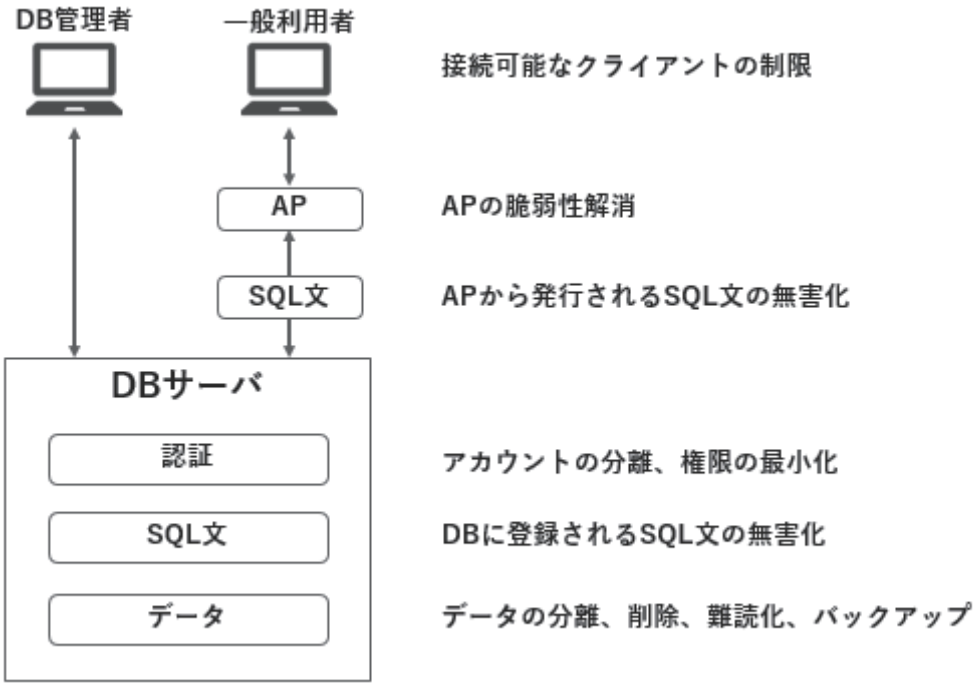
認証プロトコルに関する記述として適切なものはどれでしょうか。次の選択肢ア〜エの中から一つを選んでください。

ア	CHAP は、様々な認証方式をカプセル化する仕組みをもつ
イ	EAP は、ワンタイムパスワード方式で認証を行うプロトコルで、PPP などにおけるユーザー認証方式として使われている
ウ	IEEE802.1X は、認証に成功した端末だけが VLAN や無線 LAN に接続できるようにする
エ	RADIUS は，サプリカントとオーセンティケータ間、及び、オーセンティケータと認証サーバー間で通信を行う

第11章.

セキュアプログラミング

1 DB サーバーのセキュリティ



DB サーバーは機密情報を含む大量のデータを管理するサーバーであり、アプリケーション(AP)が動くためにも必須の場合が多いため、不正アクセスの被害を受けるとデータ流出や業務停止等の大きな被害を招く恐れがあります。

一般に、DB サーバーにアクセスするユーザーは一般利用者と DB 管理者に分けられます。一般利用者は業務アプリケーション(AP)を通じて AP の設計に沿った限定的な利用をするのに対して、DB 管理者は DB に直接接続して自由に操作できるユーザーです。どちらのユーザーについても、可能であれば接続可能なクライアントの制限をかけます。

一般利用者は本来、AP の設計に沿った限定的な利用をするものですが、AP に脆弱性があるとその限定が機能しませんので脆弱性を解消しなければなりません。

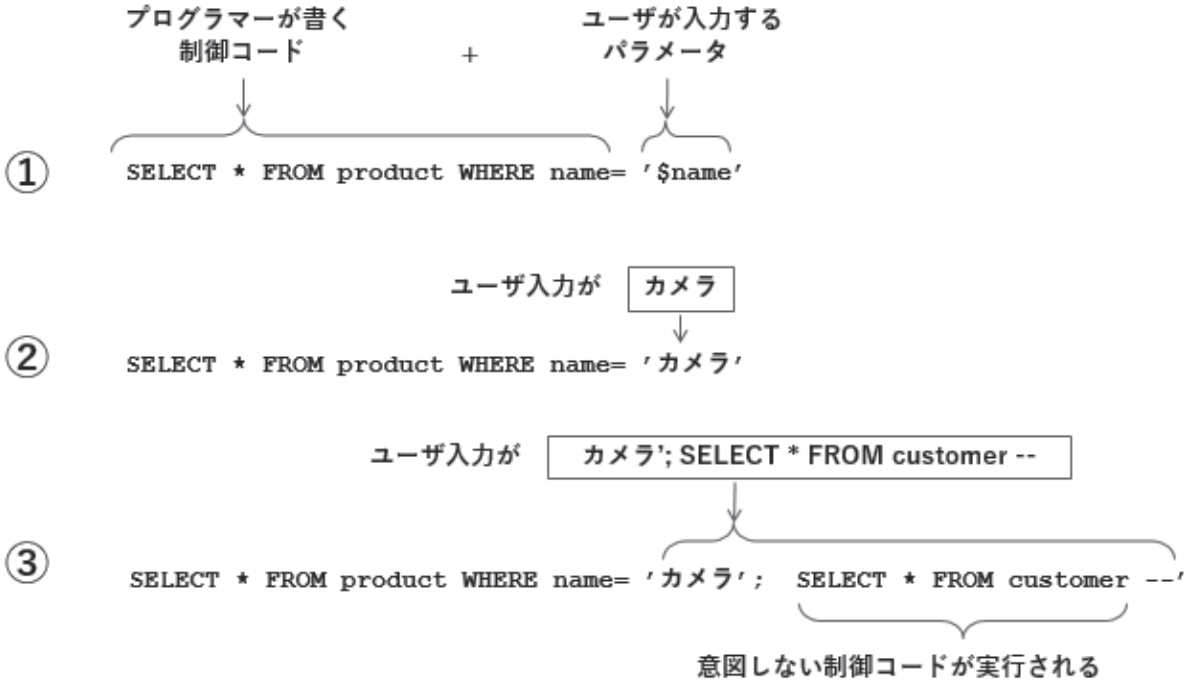
AP から RDB へのアクセスには SQL を使います。AP から発行される SQL 文には「無害化（サニタイジング)」という処理を施す必要があります。この無害化処理の不完全さが原因で DB からの情報漏洩が起きるケースは非常に多いため、十分に対策をしておくことが重要です。

DB サーバーに接続する際は DB 用のアカウントで認証を行います。このアカウントは OS が管理するアカウントではなく DB 独自のアカウントです。OS のアカウントと同じく、用途毎にアカウントを分離して権限を最小化しておきます。

「SQL 文」は AP 側で実行中に組み立てて DB に対して発行されるものの他に、DB にあらかじめ登録しておき必要に応じて呼び出して使うものもあります。ここでも SQL 文を無害化する必要があります。

「データ」については機密性の高いデータとそれ以外を分離する、必要の無いデータは削除する、流出しても解読・悪用できないように難読化（暗号化やハッシュ化）する、破壊されても復旧できるようにバックアップを取る、などの対応が必要です。

2 SQL インジェクションの原理

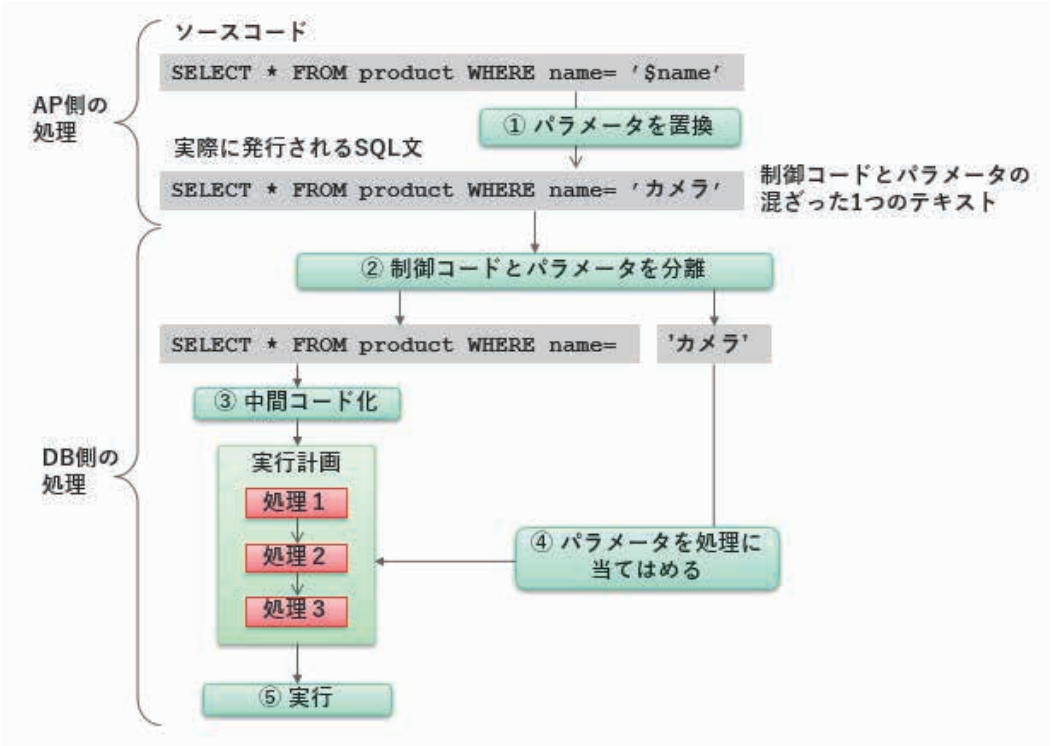


DB の中で最も広く使われている RDB（リレーショナル DB、関係 DB）ではデータを操作するために SQL という問い合わせ言語を使用します。RDB からの情報流出の原因のうち非常に大きな割合を占める SQL インジェクションという攻撃手法は、ユーザー入力に不正な SQL 文を混ぜることによって、本来想定されていない SQL 文を実行させる手法です。

SQL インジェクションの原理を確認しておきましょう。
アプリケーションが発行する SQL 文は一般に、①のように「プログラマーが書く制御コード」部分と「ユーザーが入力するパラメータ」部分に分かれます。①は特定の名前を持つ商品を検索するだけの簡単な SQL 文です。「制御コード」という用語は特殊な文字コードの意味で使われる場合もありますが、ここではパラメータ以外のプログラム・ロジックのことをそう呼んでいます。

①の SQL 文は本来、②ユーザー入力が「カメラ」のようなものであることを想定していますが、そこにたとえば③「カメラ'; SELECT * FROM customer --」という入力をすると「カメラ';」の部分でいったん SQL 文が 1 つ完結し、文法エラーもないためその後の部分は別な SQL 文として実行されます。こうして実行される「別な SQL 文」は攻撃者が自由に書けるため、意図しない制御コードが実行されてしまいます。これが SQL インジェクションの基本的な原理で、RDB を操作するプログラムでは必ずこの脆弱性を解消しておかなければなりません。このような脆弱性を解消することを「無害化（サニタイジング）」と言います。

3 SQL 文が実行されるまでの手順



SQL インジェクションへの対策をするために、RDB が SQL 文を実行する際の処理手順を確認しましょう。図中の手順は上から下に沿って①は AP 側で、②～⑤は DB 側で処理されます。

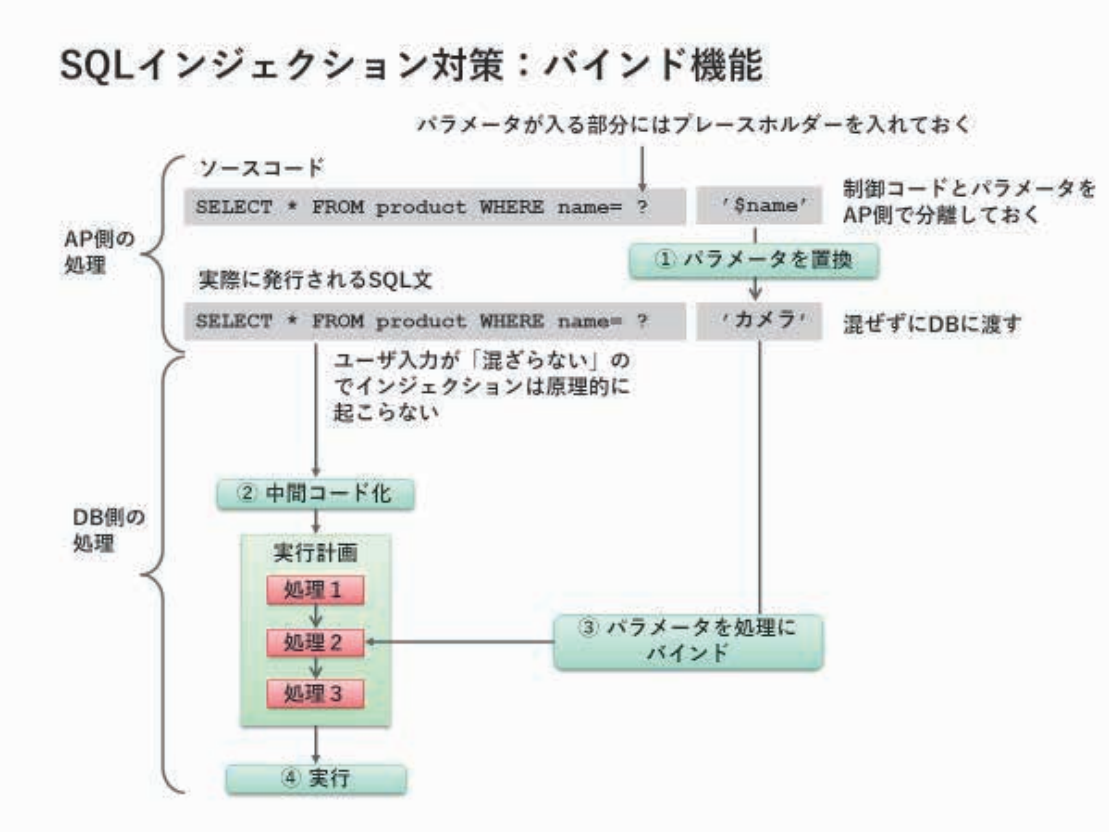
①は AP 側のソースコードのうちパラメータ部分をユーザー入力で置換する手順です。パラメータ部分はソースコード上では$name のような変数として表現されており、それを置換することで

SELECT * FROM product WHERE name = 'カメラ'

のように制御コードとパラメータの混ざった 1 つのテキストが生まれます。
AP がそれを DB に対して発行すると、DB 側では②制御コードとパラメータを分離し、③制御コード部分を中間コード化した上で、④パラメータをその一部に当てはめて⑤実行します。

問題は②の「制御コードとパラメータを分離」する部分です。SQL インジェクションは本来制御コードが入らないパラメータ部分に任意の制御コードを「混ぜ込み」、それを DB に対して制御コードと誤認させる手法です。これが発生する根本原因は、DB が「制御コードとパラメータの混ざった 1 つのテキスト」を SQL 文として受け取っていることです。

④で行う「パラメータを処理に当てはめる」操作を一般にバインド機能と言いますが、これを AP 側で積極的に利用することで SQL インジェクション対策ができます。



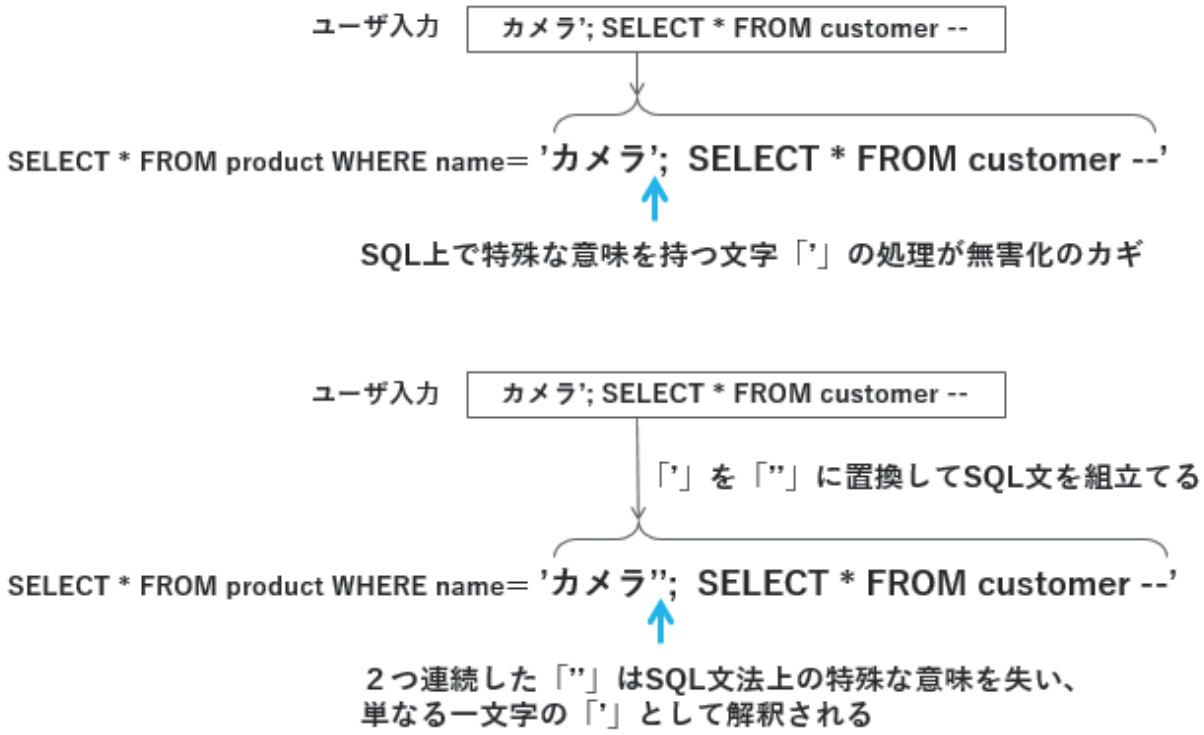
SQL インジェクション対策に効果が大きいのがバインド機能の活用です。バインドとはつまり「分かれているものを結合（バインド）する」機能です。AP 側でこれを積極的に利用したプログラミングをします。

具体的には上図のように①制御コードとパラメータを AP 側で分けたまま、混ぜずに DB に渡す方法です。制御コードの中で最終的にパラメータに置換される部分に置いておく「?」のような特殊文字をプレースホルダーと呼びます。

こうして制御コードとパラメータを分離して DB 側に渡せば、②中間コード化の対象になるのはプログラマーが書いたコードだけで、ユーザー入力が混ざらないのでインジェクションは原理的に起こりません。その後、③パラメータを処理にバインドして④実行するという流れは同じです。制御コードの基本的なロジックを変えずに、SQL インジェクションが原理的に発生しないように回収できるため、インジェクション対策は基本的にこの方法で行うことが推奨されています。

現在の主流であるアプリケーションフレームワークを使った開発をすると、DB への問合せは自動的にこの方法で行われます。しかしフレームワークを使わずに生の SQL 文を書く場合はこのような無害化処理が必要です。

4 特殊文字の置換による無害化（サニタイジング）



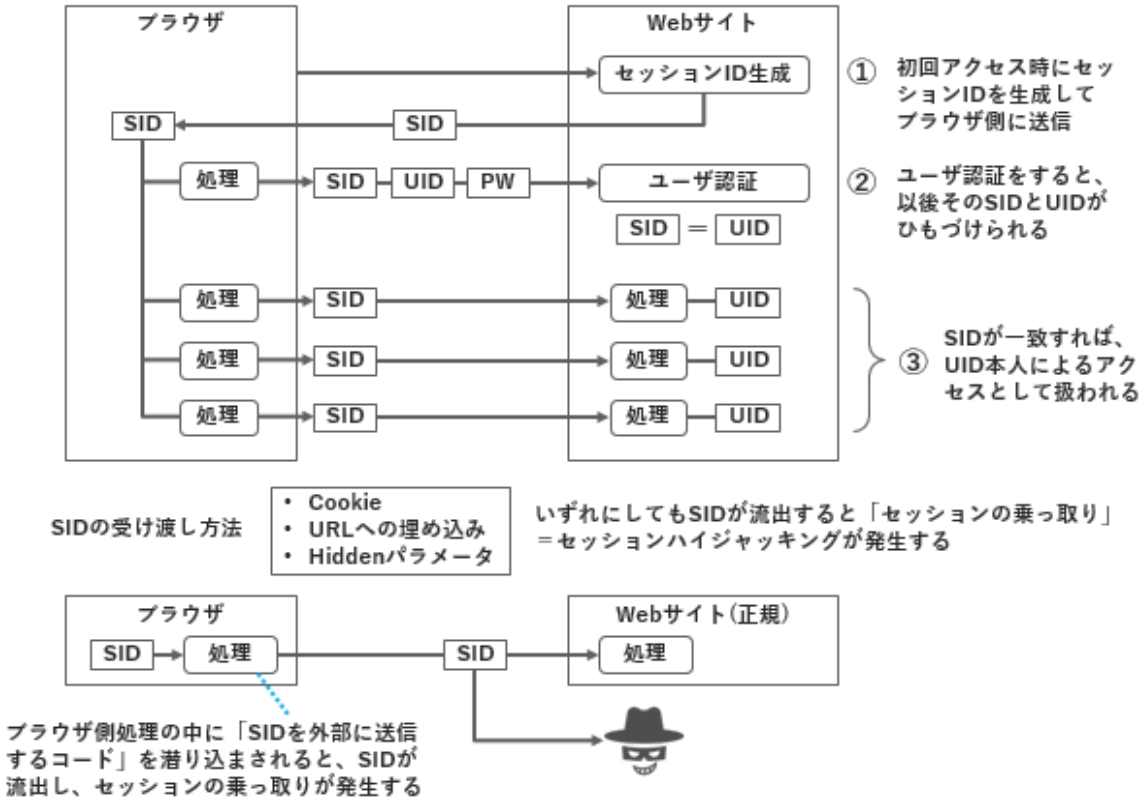
SQL 文の無害化には特殊文字を置換する方法もあります。

文字「'」（シングルコーテーション）は SQL の文法上で「文字列の開始と終了をマークする」という特殊な意味を持っています。SQL インジェクションではこれを悪用して本来単なるパラメータの文字列である部分を制御コードとして解釈させます。

これを防ぐにはユーザー入力のデータ中のシングルコーテーション「'」をすべて 2 つ連続したシングルコーテーション「''」に置換して SQL 文を組み立てます。「''」は SQL 文法上の特殊な意味を失い、単なる一文字の「'」として解釈されるため、インジェクションを防ぐことができます。

置換を必要とする特殊文字は DB 製品により差があり、シングルコーテーションだけとは限らないため注意が必要です。

5 セッション ID による利用者識別の弱点



Web システムの脆弱性・攻撃手法にもさまざまなものが存在しますが、本節では Web システムでよく使われる利用者識別方法の弱点とそれを悪用したクロスサイトスクリプティングという手法について取り上げます。

サービスを利用するためにログインが必要な会員制のサイトでは、利用者の主体認証のために ID とパスワードがよく使われます。流れとしては、①初回アクセス時に Web サイト側でセッション ID(SID)と呼ばれる乱数を生成してブラウザ側に送信します。以後ブラウザ側からサイトにアクセスする際は必ずその SID を送信することで、Web サイト側は「同じ SID を持つユーザーは同一人物であろう」と利用者識別に利用できます。

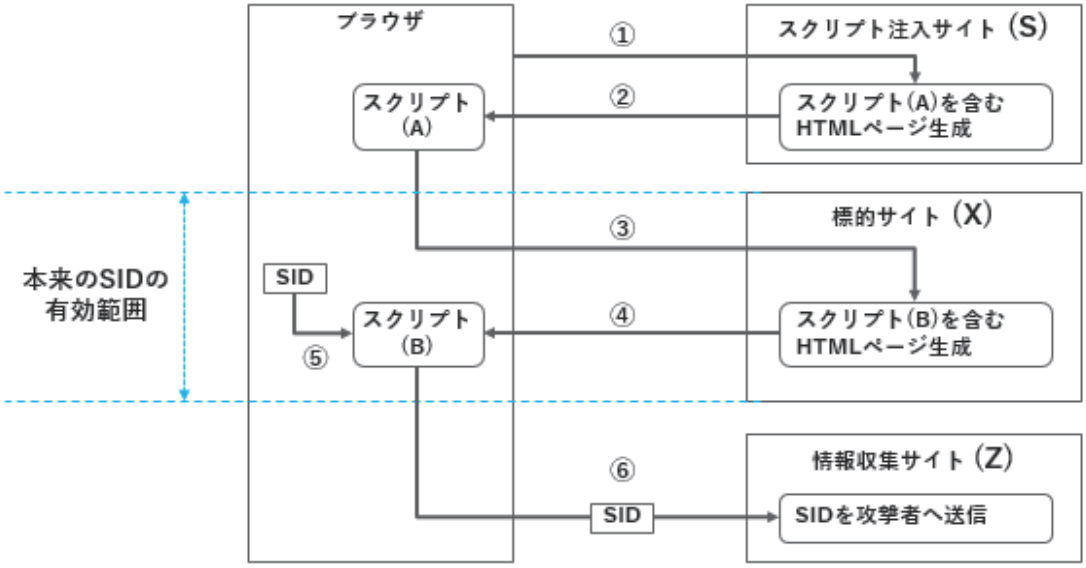
途中で②ユーザーID(UID)とパスワード(PW)によるユーザー認証をすると、Web サイト側は以後その SID と UID をひもづけて、③同じ SID によるアクセスは同じ UID を持つ本人によるアクセスとして扱います。これが多くの Web サイトで使われている利用者識別方法です。

SID を受け渡す方法には、Cookie、URL への埋め込み、FORM の Hidden パラメータへの埋め込みなどがありますが、いずれにしても SID が流出すると「セッションの乗っ取り」＝セッションハイジャッキングに悪用されます。

現在の Web システムではブラウザ側でもスクリプト言語によるプログラム処理が可能です。その処理の中に「SID を外部に送信するコード」が潜り込まされると、SID が流出します。また、そのような不正なコードがあると、SID に限らずブラウザ上で読みこめる情報をすべて流出させられてしまいます。

このような性質を悪用し、複数の Web サイトを介してブラウザ側に不正なコードを仕込む攻撃手法をクロスサイトスクリプティングと呼びます。

6 クロスサイトスクリプティング



クロスサイトスクリプティングの流れを確認します。上図は 3 つのサイト S,X,Z を介して SID 情報を摂取する例です。

サイト S は掲示板サービスのように攻撃者が任意の文を投稿して来訪者に表示させることができるサイトが使われます。
サイト X は実際の攻撃対象となるサイトで、ここから SID や個人情報を盗み出すのが攻撃の目標です。
サイト Z は盗み出した情報を収集するために使われます。

クロスサイトスクリプティングによる流れとしては、まず攻撃対象のサイト X を利用している一般の利用者がブラウザで①サイト S にアクセスしたとき、S が②スクリプト(A)を含む HTML ページを生成して表示します。このスクリプト(A)はブラウザで動きますが、この段階ではサイト X で使われる SID をスクリプト(A)が入手することはできないため被害は発生しません。

次に、③スクリプト(A)はブラウザを攻撃対象サイト(X)に遷移させ、X 上で別なスクリプト(B)を含む HTML ページを生成させて④ブラウザに表示させます。サイト X の SID は本来、サイト X を閲覧しているときにだけ有効なものです。一方、スクリプト(B)はサイト X ではなく攻撃者が作成したものですので、スクリプト(B)を他のサイト（例：サイト S など）に掲載して利用者に表示させるだけではサイト X の SID は入手できません。しかし、③によってスクリプト(B)をサイト X の一部に

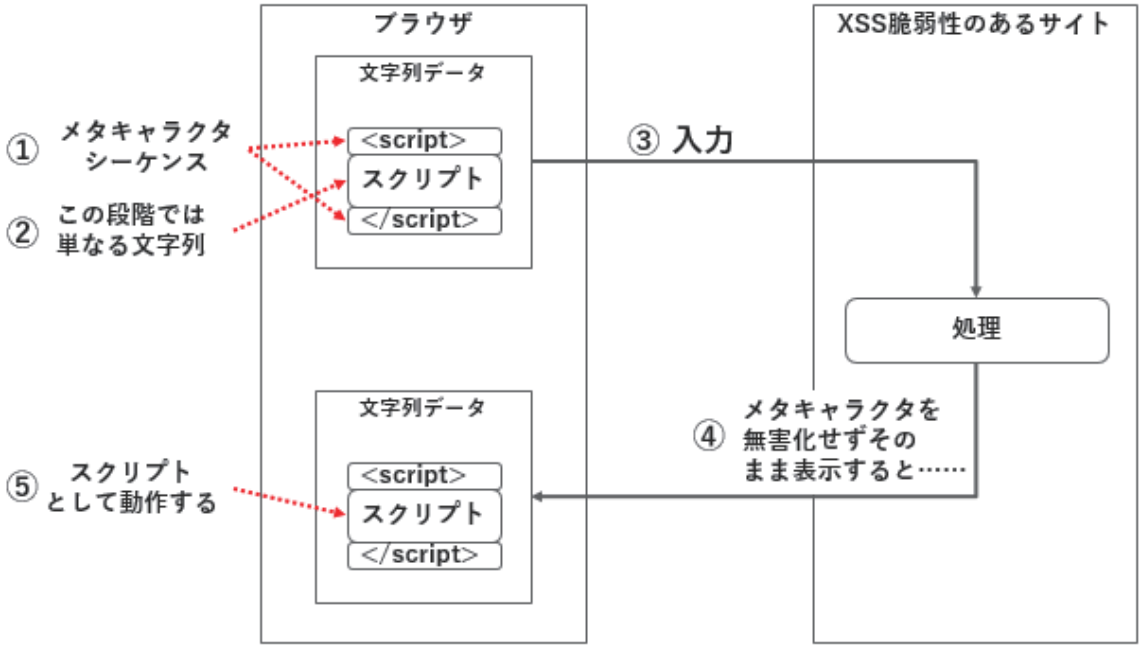
注入しているため、④の段階ではブラウザにとってスクリプト(B)はサイト X の一部となり、⑤サイト X でのみ有効な SID を入手できてしまいます。

次にスクリプト(B)はブラウザを⑥サイト Z に遷移させて SID その他の機密情報を攻撃者に送信します。

このような手順で「複数のサイトを横断的に異動してスクリプトを動かす」攻撃手法であることから、「横断」を意味する cross をとって Cross Site Scripting と呼ばれます。ただし CSS と略すと Cascading Style Sheet と紛らわしいため、略称としては XSS が使われます。

XSS 攻撃のポイントになるのは、サイト S とサイト X に潜む XSS 脆弱性です。

7 XSS 脆弱性（入力無害化不全）



XSS 脆弱性は、ユーザー入力を受け付けるサイトで入力を無害化する処理が不完全な場合に起きます。これはユーザーの入力した情報をほぼそのまま表示するような処理のあるサイトで起こりがちで、掲示板サービスがこれに該当するため、よく悪用されます。

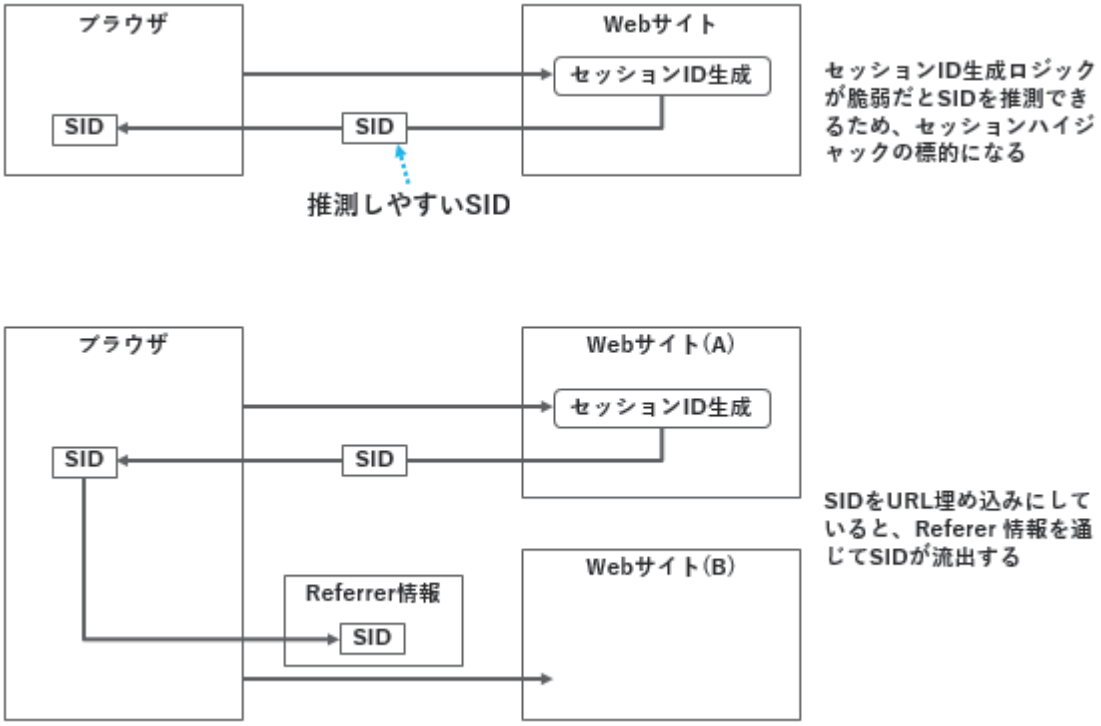
たとえば掲示板サービスの場合、そこに投稿する内容は基本的に文字列データです。ブラウザに表示された投稿フォーム上に、①メタキャラクタシーケンスで挟んだスクリプトを打ち込んだとしましょう。②この段階ではメタキャラクタもスクリプトも単なる文字列であり、スクリプトとしては動作しません。それを③サイトに入力したときに、サイト側が④メタキャラクタを無害化せずそのまま表示すると、⑤ブラウザに表示された文字列データの<script></script>に挟まれた部分はスクリプトとして動作してしまいます。これが XSS 脆弱性であり、XSS 攻撃を防ぐためには④の処理でメタキャラクタを無害化しなければなりません。

メタキャラクタとは HTML の文法上特別な意味を持つ文字であり、これらを単なる文字として表示させるようにするには、ブラウザへ応答するときに下記のようにメタキャラクタを置換します。

メタキャラクタ	置換
<	<
>	>
&	&

メタキャラクタ	置換
″	"
'	'

8 セッション管理の脆弱性を狙う攻撃

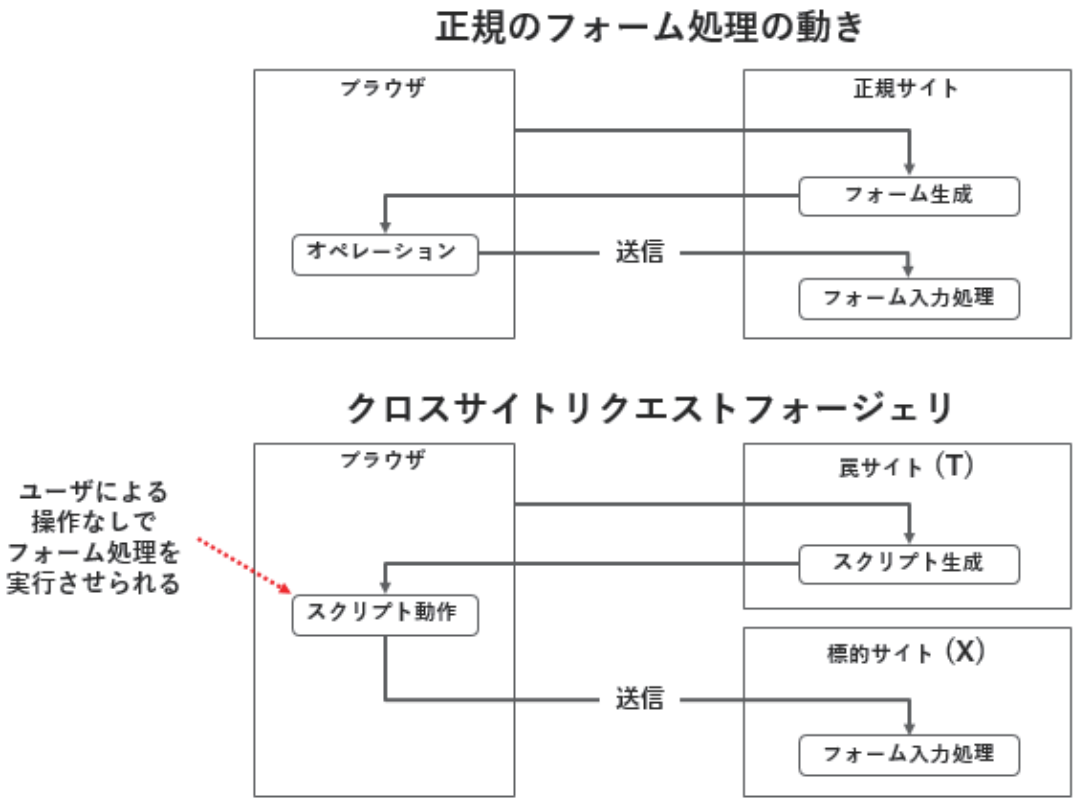


クロスサイトスクリプティングの他にもセッション管理の脆弱性を狙う攻撃があります。

セッション管理の仕組みを自作しているようなケースで、セッション ID を利用者 ID と時刻から生成するなど、ID 生成ロジックが脆弱で SID を推測できるケースがあり、セッションハイジャックの標的になります。セッション ID の発行は通常、PHP や Java 等の開発環境が提供する標準ライブラリを使用します。それらのライブラリが発行するセッション ID は十分な長さをもつランダムな文字列のため、この脆弱性はありません。

一方、Cookie を使わずに SID を URL 埋め込みにする方式でセッション管理をしていると、外部サイトへのリンクをクリックしたときに URL が Referrer として外部サイトに渡ることから SID が漏れるケースがあります。対策としては、SID を URL に埋め込む方法を使わず、Cookie で SID を受けた渡す方法を取ることが基本です。

9 クロスサイトリクエストフォージェリ



クロスサイトリクエストフォージェリ（CSRF：Cross Site Request Forgery）は、攻撃者の偽造したページを閲覧させることによって，利用者に意図せず不正なフォーム送信を行わせる攻撃です。

正規のフォーム処理であれば、サイトを閲覧したときにフォーム生成のロジックが実行されてブラウザにフォームが表示され、利用者がそのフォームへのデータ入力・ボタン押下などの「オペレーション」を行い意識的に「送信」をして初めてフォーム入力が処理されます。

一方、クロスサイトリクエストフォージェリは、利用者が罠サイトを閲覧したときにスクリプトを生成してブラウザに返送し、ブラウザ上でのスクリプトの動作によって標的サイトのフォームへの送信処理を自動的に行わせてしまいます。

この攻撃では正規サイトでの「フォーム生成」の処理を飛ばしていきなりフォーム入力が行われるため、対策としては、「フォーム生成」を経ていないフォーム入力を無視するようなプログラミングをします。具体的には、利用者が正規のフォーム送信用のページにアクセスするたびに、フォーム生成処理「トークン」と呼ばれる乱数を発生させ、それを Hidden フィールドに埋め込んだフォームを生成させます。フォーム入力処理でそのトークンを照合し、正しいトークンを持たない入力は不正な送信とみなして無視するようにします。

10 その他の攻撃

- HTTPヘッダインジェクション
  - HTTPパケットを偽造して不正なヘッダフィールドをHTTP ヘッダに埋め込み，これを受信したホストに不正な動作を行わせる
  - HTTPヘッダフィールドからパラメータを読み取るとき必ず無害化することで対応可能

- フィッシングサイト攻撃
  - 本物そっくりに偽装したサイトを用意して個人情報などをフォーム送信させ、盗み出す

HTTP ヘッダインジェクションは、HTTP パケットを偽造して不正なヘッダフィールドを HTTP ヘッダに埋め込み，これを受信したホストに不正な動作を行わせる攻撃です。サーバーからクライアントに Cookie を渡すときに使用する Set-Cookie フィールドを偽造すれば，不正な Cookie をクライアントに渡してこれをセッションハイジャック攻撃への足掛かりにすることができます。この攻撃への有効な対策は、HTTP ヘッダフィールドからパラメータを読み取る際、必ず無害化することです。開発環境が提供する標準ライブラリを利用すれば、無害化された文字列を読み取ることができます。

フィッシングサイトとは、本物そっくりに偽装したサイトのことです。攻撃者は標的をこのサイトに巧みに誘導し、個人情報などをフォーム送信させて、それを盗み出します。

11 演習問題

問 1

今、あなたは Web アプリケーションのプログラムを開発しています。
クロスサイトスクリプティング対策のため、利用者から受け取った文字列を表示する際、無害化を行うことにしました。
無害化処理の内容は、次の表「無害化対象のメタキャラクタ」に基づき、メタキャラクタを特定の文字列を置換するものとします。この処理の結果、メタキャラクタはそのままの文字として表示されることになります。

表：無害化対象のメタキャラクタ

項番	メタキャラクタ	置換後の文字
①	<	<
②	>	>
③	&	&
④	″	"
⑤	’	'

設問(1) 表「無害化対象のメタキャラクタ」に列挙されたメタキャラクタを置換する際、最初に置換する必要があるメタキャラクタはどれでしょうか？項番①～⑤の中から答えてください。

設問(2) 利用者が入力した文字を次に示します。無害化処理を行うと、この文字列はどのように変化しますか？ なお、無害化処理を行う際、設問(1)で考慮したとおり、適切なメタキャラクタを最初に置換するものとします。

利用者が入力した文字列

```
<script>alert('Hello World!')</script>
```

問2

SQL インジェクション攻撃について説明した以下の文章を読み、空欄ア、イに入れる適切な字句を答えてください。

ログイン認証を行うプログラムがある。

これは、利用者からユーザーIDとパスワードを受け取り、SQL文を発行する。

ここでは、プログラムが受け取ったユーザーIDの文字列を「X」、パスワードの文字列を「Y」とし、受け取った文字列を格納した部分を枠で囲んで目立たせている。

```
SELECT ＊ FROM 会員テーブル
WHERE ユーザーID = 'X' AND パスワード = 'Y';
```

会員Xのパスワードが Y であるとき、この SQL 文はレコードを返す。この結果、プログラムは、会員Xのログイン認証に成功したと判断する。

このプログラムは SQL インジェクション対策を行っていないため、ユーザーから受け取ったユーザーIDとパスワードをそのまま格納する仕組みになっている。

この仕組みを悪用し、攻撃者が下記のユーザーIDとパスワード入力したとしよう。

ユーザーID	ア
パスワード	イ

SQL 文中に「--」があるとき、「--」以降の文字列はコメントとして解釈されるため、実行時には無視される。それゆえ、攻撃者から受け取った文字列を格納した SQL 文は、次のものと等価である。

```
SELECT ＊ FROM 会員テーブル
WHERE ユーザーID = 'X' AND パスワード = '' OR 1 = 1;
```

この結果、プログラムは会員［ア］のログイン認証に成功したと判断する。

第12章.

個人を対象とする攻撃

1 考慮すべきセグメントと脅威の種類

多様なサイバー攻撃の脅威への対策を考えるためには、攻撃者が何を「手がかり」や「目的」とするかを知っておく必要があります。上図はそれを「人」から「社会活動・資産」までの 6 つのセグメントに分けて整理したものです。

人は何らかの行動をするためにデバイスを使います。デバイスにはそれぞれ固有の機能があり、その機能を通じてサービスを利用し、社会的な活動をしたり資産を管理したりします。

たとえば商品を購入するために PC を使うという場合、「行動」は購買、「デバイス」は PC、「機能」は通信、「サービス」は EC とクレジット、「社会活動・資産」はクレジット会社を通じて管理している財産となります。攻撃者が「財産」の不正取得を狙う場合

- 「購買」行動で錯誤を起こさせる（詐欺サイト等）
- 「PC」にマルウェアを感染させて不正操作する
- 「通信」を傍受してアカウント情報を窃取する
- 「サービス」をクラックしてアカウント情報を窃取する

など、いくつかの異なる攻撃ポイントがあり、防御する方法もそれぞれ異なります。図の下部には代表的な「脅威」をそれぞれ主に関連するセグメントの下に記載してありますが、実際には 1 つの脅

威への対策も複数のセグメントにまたがって考えなければなりません。以下、各セグメントについて考慮すべき特徴をまとめます。

人

人にはたとえば高齢者/成年/未成年/主婦/学生などさまざまな属性があり、その属性によって違う知識・動機で行動します。たとえばPCを使い慣れたビジネスマンと初めて使う高齢者ではITリテラシーに大差があります。攻撃者は対象者が持つ知識・動機・行動を想定して罠を仕掛けます。セキュリティ対策を設計するには、想定する対象者の属性を踏まえておかなければなりません。

行動

人は何らかの目的に沿った「行動」を取ります。気になっていた商品がお得に買えるキャンペーン、面白そうな動画、イベントへのお誘い、便利そうな学習アプリなど、こうしたちょっとした「行動」の中に攻撃者は罠を仕込みます。利用者への教育はセキュリティ対策の中でも重要な部分ですが、適切な教育を行うためには人がどのような「行動」をとるかを想定する必要があります。

デバイス

個人が使用するデバイスでサイバー攻撃の対象になるものが近年多様化しています。PCには以前からウイルス等の脅威が存在しましたが、PCと同等の機能・性能を持ったスマートフォンが普及するにつれてそれらへの攻撃も増加しています。USBメモリを通じてマルウェアの感染が広まるケースだけでなく、メモリに限らずUSB接続で使用する機器自体にクラッキングのハードウェアが組み込まれている場合もあります。近年増加しているIoT機器にはインターネットを通じての利用を前提とした「外出先からペットを見守るカメラ」のようなものがあり、セキュリティ機能や設定の不備を突かれて盗撮・盗聴デバイスとして悪用されているケースもあります。

機能

「デバイス」が持つ機能は大まかに「記録」「通信」「制御」等があり、これらがどのように悪用可能かという視点を持たなければなりません。たとえばUSBメモリは「通信」や「制御」の機能は持ちませんが「記録」は可能なため、情報漏洩の媒体として使われることがあります。

サービス

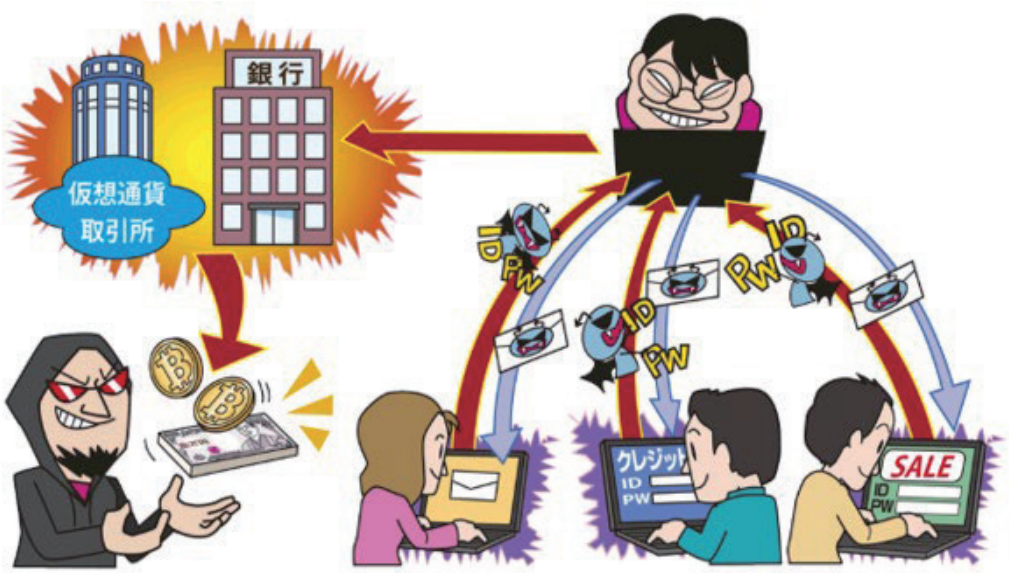
インターネットを通して提供される「サービス」もサイバー攻撃の対象になります。現在は一人で何十ものサービスに登録していることも多く、登録の都度何らかの個人情報をサービス運営者に提供す

ることになります。Web サービスの中にはそれ自体が個人情報収集を目的とするものもありますし、正規のサービスからも登録情報が流出して不正利用されるケースもあります。

社会活動・資産

人は「サービス」を通して何らかの社会的な活動をしています。たとえばメールや SNS では「コミュニケーション」をしていますし、オンラインバンキングで「財産」を管理するのも社会的活動と言えます。「オンラインバンキグの不正利用」や「SNS を通じて個人を中傷する情報を流布する」などのサイバー攻撃はこれらの社会的活動や資産を標的としたものと言えます。

2 インターネットバンキングやクレジットカード情報等の不正利用



出典：情報セキュリティ10大脅威 2018：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/10threats2018.html

現代のサイバー攻撃の多くは金銭的利益を目的としたものであり、直接的に金銭を扱うインターネットバンキング、クレジットカード情報等は格好の標的といえます。これらのサービスの ID、パスワード等を含む個人情報、口座番号、クレジットカード番号等の情報が攻撃者に流出すると、その情報だけで不正送金や不正購入の被害を受けてしまいます。

■手口 1：PC やスマートフォンのウイルス

PC やスマートフォンにウイルスを感染させてこれらの情報を窃取する手口があります。ウイルス感染した PC やスマートフォンでインターネットバンキングやオンライン購入を行うと被害が発生します。

■手口 2：フィッシングサイト

攻撃者は実在するインターネットバンキングのウェブサイトを模した偽のウェブサイト（フィッシングサイト）を作成します。その後、フィッシングサイトのリンクが記載されたメールを送信してフィッシングサイトにアクセスさせ、フィッシングサイト上で被害者が入力したログイン情報等を窃取します。

その他、正規の Web サービスサイト自体のクラッキングによる情報漏洩やパスワードの類推などが使われる場合もあります。これらの手口により不正送金・不正利用される被害が多数報告されており、IPA(独立行政法人　情報処理推進機構)がまとめた「情報セキュリティ 10 大脅威　2018 年度版」では個人に対する脅威ランク 1 位に位置づけられています。

利用される手口	個人側で可能な対策
PC やスマートフォンのウイルス	ウイルス対策ソフト／機能の有効化 身元不明なアプリのインストールを避ける OS のセキュリティ更新を確実に行う ワンタイムパスワードを使用する
フィッシングサイト	サイトの正当性を十分に確認する ワンタイムパスワードを使用する
サービスのクラッキング等による情報漏洩	パスワードの使い回しを避ける 二段階認証を利用する ワンタイムパスワードを使用する
パスワードの類推	脆弱なパスワードの使用を避ける 二段階認証を利用する ワンタイムパスワードを使用する

他に手口への対策ではなく被害の軽減策として、インターネットバンキング口座の残高や送金限度額、クレジットカード限度額を下げる、サービスへのログインや送金・引出・カード使用がメール等で通知されるように設定して不正使用を検知する、などの方法があります。

3 ランサムウェアによる被害

出典：情報セキュリティ10大脅威 2018：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/10threats2018.html

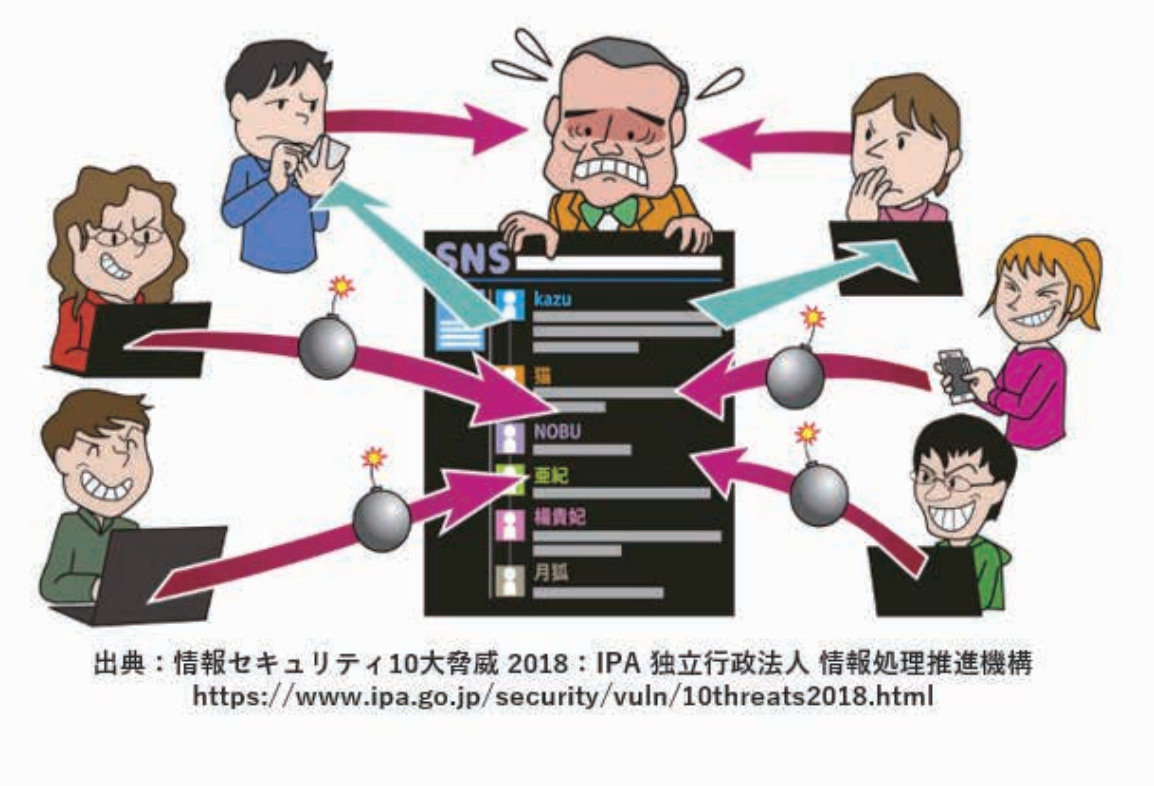
ランサムウェアとは、PC やスマートフォンにあるファイルの暗号化や画面ロック等を行ってファイルや PC そのものを使用不能にし、金銭を支払えば復旧させると脅迫するウイルスです。「情報セキュリティ 10 大脅威　2018 年度版」では個人に対する脅威ランク 2 位と評価されています。

ランサムウェアに感染した端末だけではなく、その端末からアクセスできる共有サーバーや外付け HDD に保存されているファイルも暗号化されるおそれがあります。2017 年には、OS の脆弱性を悪用し、ネットワークを介して感染台数を増やすランサムウェアも登場しました。

利用される手口	個人側で可能な対策
PC やスマートフォンのウイルス	ウイルス対策ソフト／機能の有効化 身元不明なアプリのインストールを避ける OS のセキュリティ更新を確実に行う

脅迫の材料としては、PC を使用不能にして人質に取る方法のほかに、「被害者が行っている不正行為の証拠を持っている。捜査機関に通報されたくなければ金銭を払え」などというメッセージを示す例もあります。いずれにしても指示に従って支払をしても「復旧」はされない場合が多く、支払を行うべきではありません。

4 ネット上の誹謗・中傷



出典：情報セキュリティ10大脅威 2018：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/10threats2018.html

コミュニティサイト（ブログ、SNS、掲示板等）上で、個人や組織に対して誹謗・中傷や犯罪予告をする書き込みが行われることがあります。匿名性があり、高度な技術力も必要ない手軽さから安易に投稿されてしまう傾向がありますが、これもサイバー犯罪の一種と言えます。SNS を使った犯罪は社会的な問題となっており、2017 年には殺人事件にまで発展した事例もあります。「情報セキュリティ 10 大脅威　2018 年度版」では個人に対する脅威ランク 3 位と評価されています。

サイバー犯罪という意識も持たない一般の人が軽い気持ちで「殺人予告」等を書き込んで逮捕される例もあり、子どもも含めて IT リテラシーの乏しい人々への啓蒙が重要な分野です。

他に、CSRF(クロスサイトリクエストフォージャリー)という手法により、意図せずこの種の攻撃に加担させられているケースもあります。これについてはサーバーのセキュリティ対策が必要です。

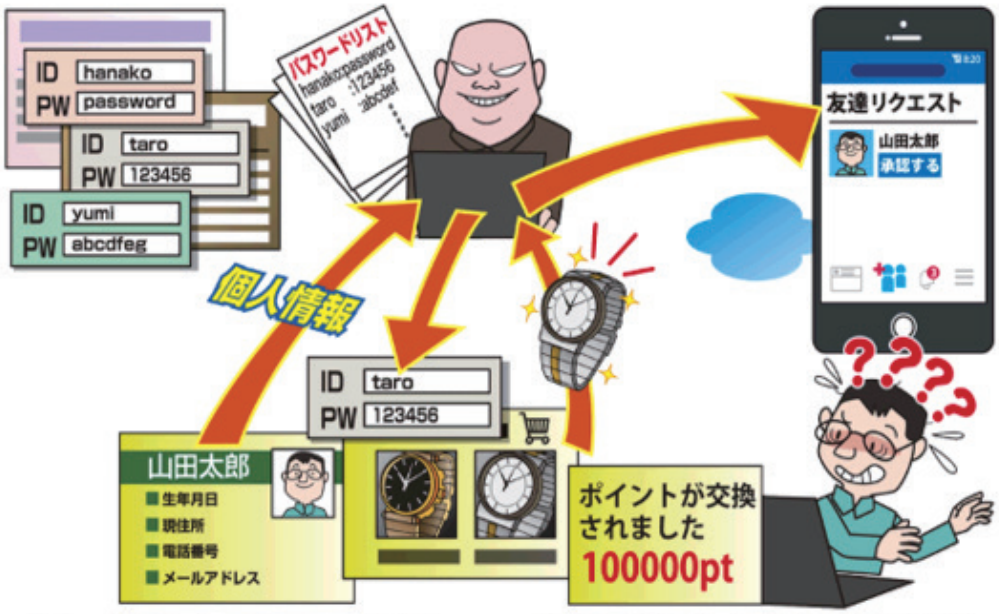
5　スマートフォンやスマートフォンアプリを狙った攻撃

出典：情報セキュリティ10大脅威 2018：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/10threats2018.html

スマートフォン利用者が不正アプリをインストールしてしまい、スマートフォン内の重要な情報を窃取されたり、不正に操作されたりする脅威です。PC の場合と同様、データの暗号化や個人情報を公開するといった脅迫を行うランサムウェアも確認されています。「情報セキュリティ 10 大脅威 2018 年度版」では個人に対する脅威ランク 4 位と評価されています。

スマートフォンは PC に比べてユーザーのすそ野が広く、IT リテラシーの低いユーザーに広がっていること、マルウェア対策の歴史が浅いこと、PC に比べて多様なアプリが必要とされること、公式サイトにも不正なアプリがはびこっているため見分けづらいこと、などの事情でこれが大きな問題となっています。

6 ウェブサービスへの不正ログイン



出典：情報セキュリティ10大脅威 2018：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/10threats2018.html

ウェブサービスに不正ログインされ、金銭的な被害や個人情報を窃取される等の被害が確認されています。インターネットには多数のウェブサービスが存在しており、1人で数十～数百ものウェブサービスに登録している例があります。利用者がそれら多数のサイトへ登録する際、推測されやすいパスワードの使用やパスワードの使いまわしをしていると、1箇所からID/パスワード情報が漏れたときにそれを悪用して他のサイトに不正ログインする「パスワードリスト攻撃」の被害を受けます。2017年に確認されたウェブサービスへの不正ログインの多くがこのようなパスワードリスト攻撃によって行われており、「情報セキュリティ 10 大脅威　2018 年度版」では個人に対する脅威ランク 5 位と評価されています。

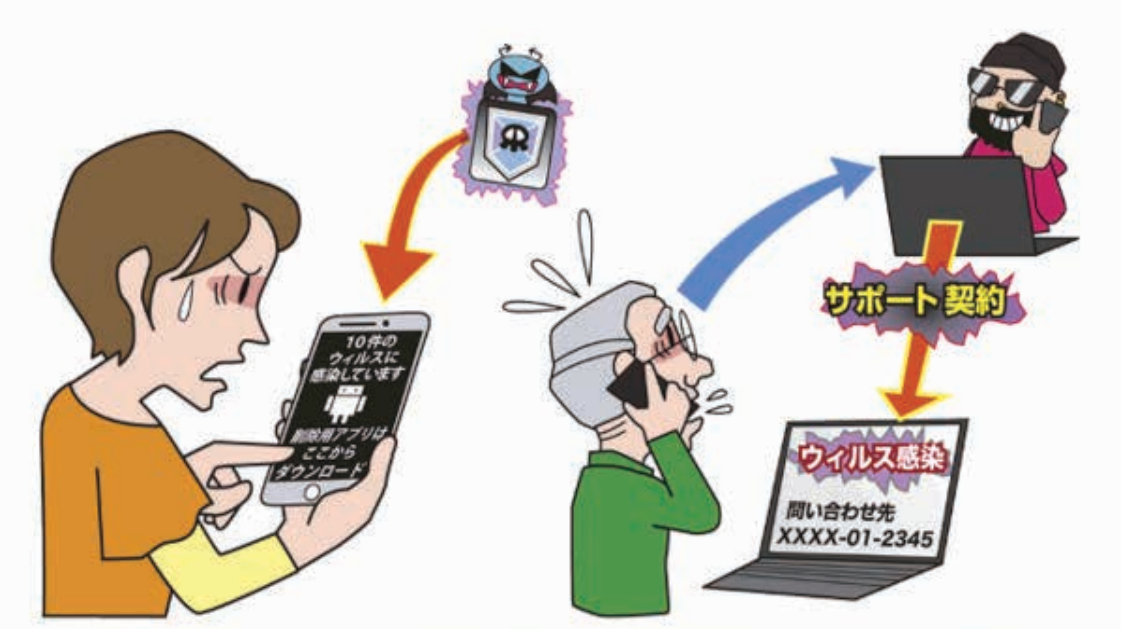
利用される手口	個人側で可能な対策
サービスのクラッキング等による情報漏洩	パスワードの使い回しを避ける 二段階認証を利用する
パスワードの類推	脆弱なパスワードの使用を避ける 二段階認証を利用する

7 ウェブサービスからの個人情報の窃取

出典：情報セキュリティ10大脅威 2018：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/10threats2018.html

ウェブサービスに登録した個人情報やクレジットカード情報を窃取される事件が多発しています。窃取した情報を悪用して不審メールを送信されたり、クレジットカード情報を不正利用されたりするおそれがあります。これはウェブサービスの SQL インジェクションなどの脆弱性を悪用されて起きる場合が多く、利用者側で防ぐことはできません。この方法で窃取した ID/パスワードがパスワードリスト攻撃に使われて「ウェブサービスへの不正ログイン」につながる例があります。「情報セキュリティ 10 大脅威　2018 年度版」では個人に対する脅威ランク 6 位と評価されています。

8 偽警告によるインターネット詐欺



出典：情報セキュリティ10大脅威 2018：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/10threats2018.html

PC やスマートフォンでウェブサイトを閲覧中に、突然「ウイルスに感染している」等の偽警告を表示して利用者の不安を煽り、偽警告に記載された操作を行わせて金銭的な被害や個人情報等を窃取される被害が発生しています。このような「警告」で表示される画面自体はマルウェアではないためアンチウイルス等のセキュリティソフトでは検出できず、本物の警告と誤認されるように巧妙な細工が施されているために、セキュリティ知識のない被害者は信じて指示に従ってしまいます。「情報セキュリティ 10 大脅威　2018 年度版」では個人に対する脅威ランク 10 位と評価されています。

これは知識の無い「人」を狙って、「行動」に錯誤を起こさせる攻撃ですので、このような偽警告をシステム的に検知・排除できるように Web コンテンツフィルタリング・システムの強化・導入を進めるとともに、「人」へのセキュリティ教育を行うことが重要です。

9 演習問題

問 1

ウイルスに感染した PC でインターネットバンキングにログインされると、どのような危険がありますか？

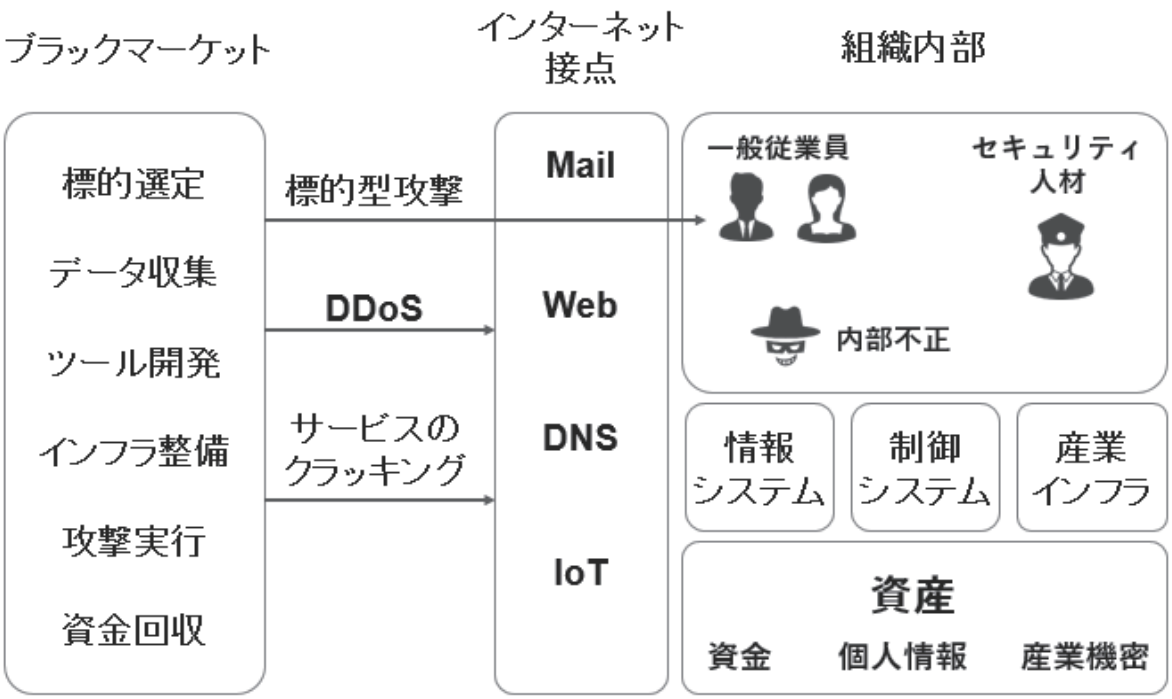
問 2

パスワードを使いまわしていると、どのような危険がありますか？

第13章.

組織や不特定多数を対象とする攻撃

1 組織に対する攻撃



企業・官庁等の「組織」に対する攻撃では、個人とは違う観点がいくつか現れてきます。

インターネット接点

組織はメール、Web、DNS 等のサーバーや IoT デバイスを業務利用するため、個人よりもインターネットへの接点が多くなります。

内部人員による不正

組織内では社員・アルバイト・取引先等、複数の人員が業務に関わっており、内部不正が起こるケースがあります。

情報システム/制御システム/産業インフラ

組織は制御システムを持ち、産業インフラを担っている場合があります。制御システムとはたとえば工場の生産設備等をコントロールするシステムのことで、破壊されると莫大な損害をもたらします。産業インフラとは他社の事業存続の前提となっている、代替の効かない機能のことで、たとえば電力会社のシステムが破壊されて停電が起きると多くの会社の事業が停止し、他社にも莫大な損害が発生します。「情報システム」は受発注・請求支払等の「情報」を管理するシステムのことで、現在はイ

ンターネットとの接続やクラウド化が進みつつあります。通常、制御システムはインターネットから切り離されていますが、近年は制御システムに対するサイバー攻撃も発生しています。

資産

組織は個人よりも多額の資金を運用しており、顧客名簿等の個人情報、設計書類等の産業機密がある場合も多く、攻撃者にとっては「手間をかけてでも狙う価値のあるターゲット」と言えます。

ブラックマーケット

一方で、攻撃者側はサイバー攻撃に必要なさまざまな機能をそれぞれの専門家が分担する「ブラックマーケット」が発達していて、「組織セキュリティシステムやセキュリティ教育が充実した企業」をも狙う高度な攻撃事例が相次いでいます。

2 標的型攻撃

出典：情報セキュリティ10大脅威 2018：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/10threats2018.html

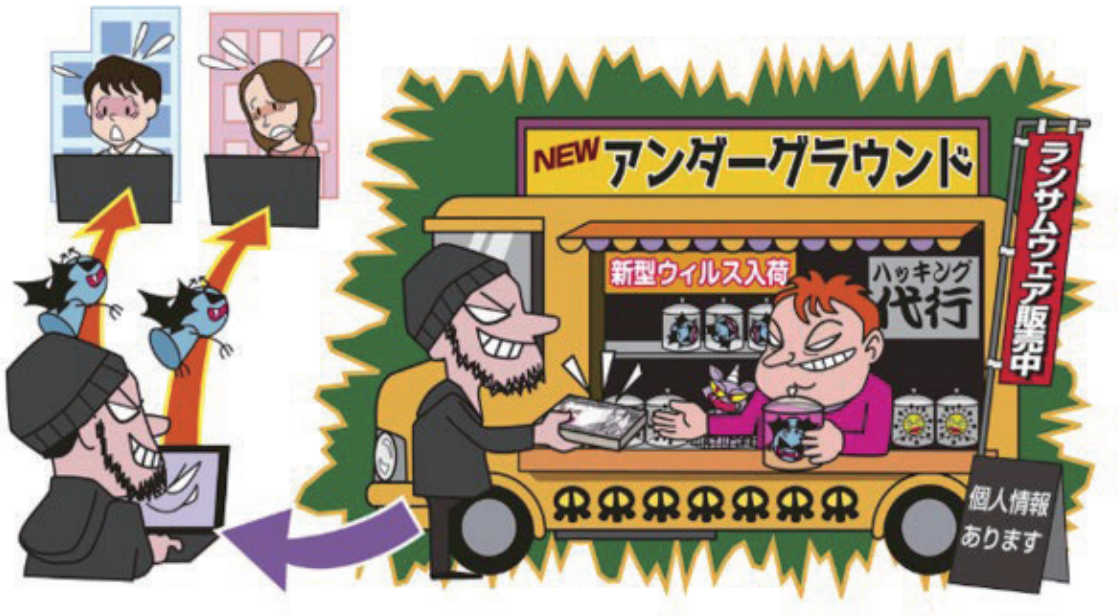
かつてのコンピュータウイルスは不特定多数にばらまかれるものでしたが、現在は企業や民間団体や官公庁等、特定の組織を狙って行われる「標的型攻撃」が大きな問題となっています。典型的な標的型攻撃で使われる手口は、実在の取引先や内部人員を装ってメールを送り、添付したウイルスを開かせるというものです。この方法は

- 標的企業専用に開発した新種のウイルスを使うためセキュリティソフトで検知しにくい
- 実在の関係者を装うため警戒感が働かない

という理由で完全に防御することが難しいものです。

ここで使われるウイルスは攻撃者側の攻撃用サーバー（コマンド＆コントロール・サーバと呼ばれます）からの指令を受け取るバックドアとして働き、攻撃者側はバックドアを通じてさまざまな攻撃用ツールを送り込んで内部ネットワークへの侵入・情報窃取を試みます。窃取した情報は小分けして外部に転送し、何らかの手段で換金します。この活動は被害企業側が探知するまで継続するため、数ヶ月から１年以上にも及ぶ場合があります。

3 攻撃のビジネス化

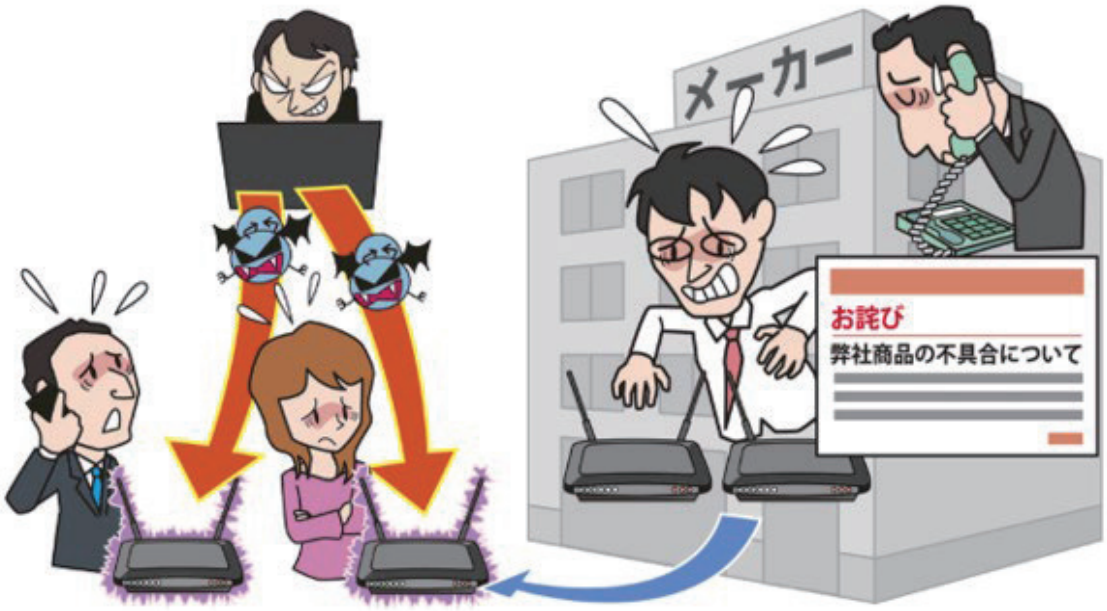


出典：情報セキュリティ10大脅威 2018：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/10threats2018.html

20 世紀のコンピュータウイルスは「個人の手による愉快犯的なもの」という印象がありましたが、近年のサイバー攻撃は組織的に行われるビジネスとなっています。たとえば標的型攻撃を遂行するには、対象となる企業の選定・標的に関する情報収集・侵入用ツール開発・コマンド＆コントロール・サーバ整備・攻撃の実行・窃取した情報の換金など、何段階もの異質な工程が必要なことから、それぞれの専門家が作業を分担し連携して行なわれています。

このような「ビジネス化」の結果、サイバー攻撃はより高度なツールや洗練された手口で行われるように進化しており、防御側にもより系統だった備えが求められつつあります。

4 IoT 機器の不適切な管理



出典：情報セキュリティ10大脅威 2018：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/10threats2018.html

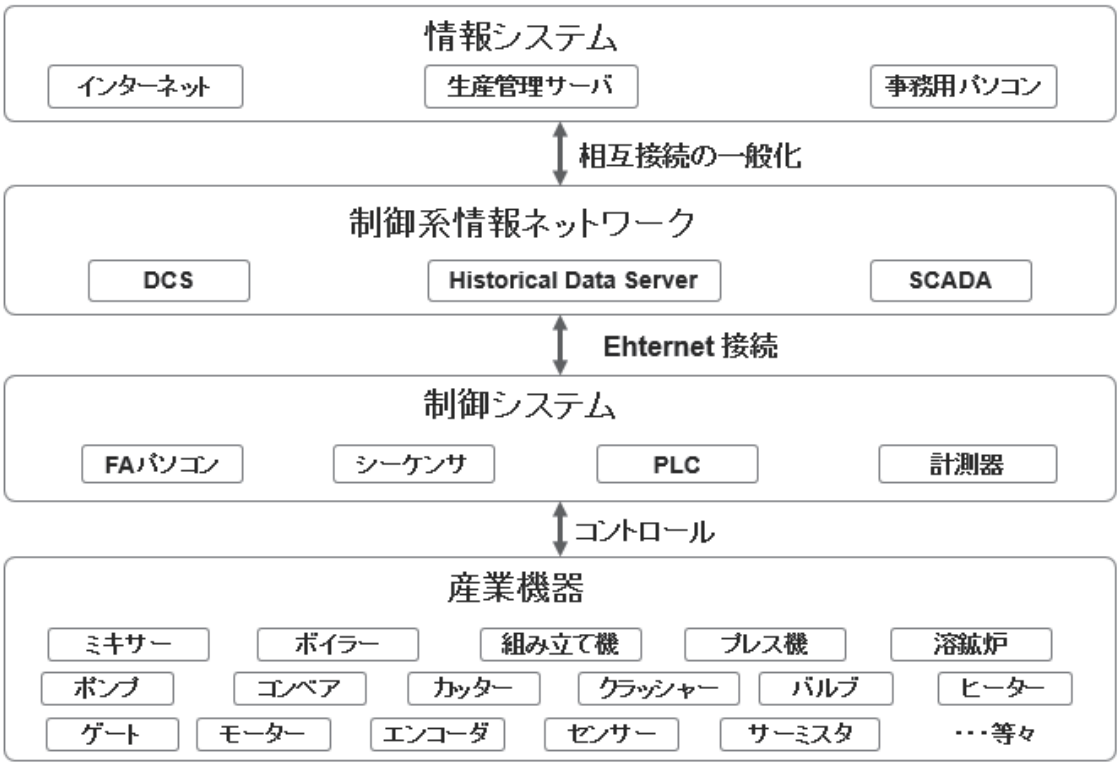
IoT(Internet of Things)の発展とともに、IoT 機器がサイバー攻撃の対象となる事例も増えています。セキュリティに関する IoT 機器特有の問題として以下のような事項があります。

- IoT デバイスは、無防備な状態でインターネットに接続されているケースが少なくない（企業内 LAN ではファイアウォール、IDS／IPS、マルウェア対策などさまざまなレイヤでセキュリティ対策が講じられている）
- メモリ、CPU、通信容量等のリソースが乏しい場合が多く、PC やサーバーと同等のセキュリティ機能を搭載するのが難しい
- 独自改修を施した OS 等でセキュリティ更新が提供されないケースがある
- PC/サーバー等に比べてライフサイクルが極めて長いものがある
- PC/サーバー等に比べてセキュリティ意識が甘くなりがちで、脆弱なパスワードのまま設置するなど、基本的な管理がなされていないケースがある

IoT 機器は今後も増え続けることが予想されており、「情報セキュリティ 10 大脅威　2018 年度版」では組織に対する脅威ランク 7 位と評価されています。具体的な攻撃事例としては次のようなものがあります。

- 不適切なパスワード設定やセキュリティ脆弱性のあるIPカメラが不正アクセスにより乗っ取られ、外部から不正な操作をされたり、映像情報がインターネット上で公開された事例
- プリンタ/コピー等の機能を持つ複合機が、遠隔管理を可能とするためのWebサーバー機能を通じて乗っ取られ、機器内に保存されている機密情報を読み取られた事例
- 適切なパスワード設定などのセキュリティ対策がなされていないIPカメラ等がボットウィルスに感染させられ、特定サイトに対するDDoS攻撃の踏み台にされた事例

5 制御システムへの攻撃



制御システムとはたとえば工場の生産設備や発電所、物流センターなどにある産業機器をコントロールするシステムのことを言います。（なお、上図は制御システムに関係のある要素を例示していますが、これらのキーワードを覚える必要はありません）

「産業機器」にも、大きなものではボイラーやプレス機、溶鉱炉など 100 トン単位のものから小さいものでは指先に乗るセンサ程度のものまで多種多様なものがあります。これらの産業機器は、情報化される以前は人間がコントロールしていましたが、やがて PLC やシーケンサという制御システムが使われるようになり、さらに 1980 年代には FA パソコンと言われる産業用パソコンの使用も一般化します。

その後コンピュータ・ネットワーク技術の進展とともにそれらを Ethernet で相互に接続して集中的に管理する「制御系情報ネットワーク」と呼ばれるシステムが発展します。

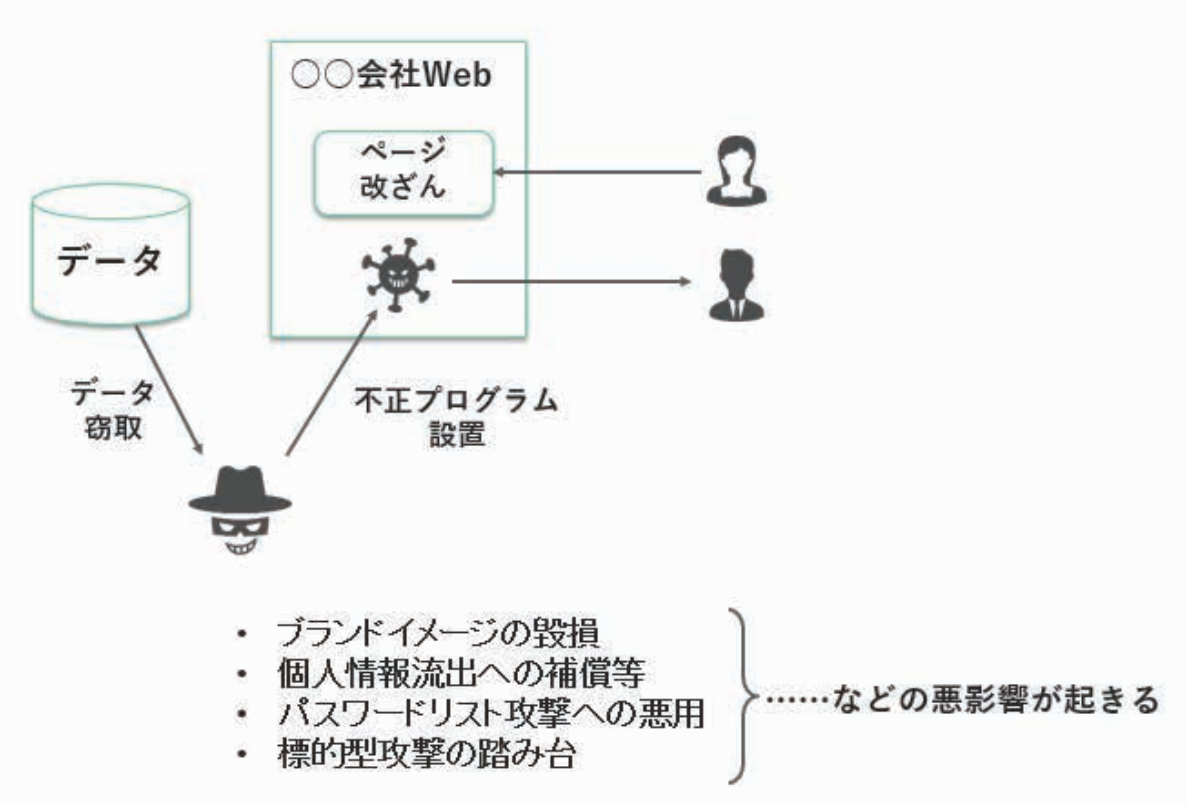
同時期にオフィスでは事務用パソコンと業務サーバーを中心とする「情報システム」が発展しており、これらを相互に連携するために、情報システムに生産管理サーバーを置いて制御系情報ネットワークと連携するようになり、情報システムと制御情報ネットワークの相互接続も一般化しました。

従来は情報系のシステムとは分離されていた制御系ネットワーク、制御システムにも Windows OS や Ethernet などのオープン技術が導入されて相互接続が進んだ結果、情報システムで蔓延したコンピュータウイルス等が制御システムにも影響を与える事態が起こり始めています。現在進展しつつある産業用 IoT やインダストリー4.0 といったイノベーションを通じて、制御システムとインターネットの接続は更に進むと考えられるため、制御システムへのセキュリティ対策はますます重要になります。これまでに発生した制御システムへの具体的な攻撃事例としては次のようなものがあります。

- 2001 年、オーストラリアの下水処理施設を解雇された元従業員が外部からリモートアクセス経由で制御システムに不正アクセスし、制御システムを操作して下水を海洋流出させる事件が発生した
- 2008 年、トルコの石油パイプラインに設置されていた監視カメラの通信ソフトの脆弱性を利用して内部ネットワークに侵入した攻撃者が動作制御系にアクセスし、管内の圧力を異常に高めて爆発を引き起こした
- 2010 年、Windows OS 上のワーム Stuxnet を用いてイランの核濃縮施設を狙った攻撃が行われ、遠心分離器に多大な被害をもたらした。当該施設の制御システムはインターネットから隔離されていたが、Stuxnet は USB を経由して感染するように設計されていた
- 2015 年、2016 年、KillDisk, BlackEnergy と呼ばれるマルウェアによりウクライナの電力システムが攻撃され、大規模な停電が発生した。

情報システムへのサイバー攻撃では直接的に死傷者が出ることは考えにくいですが、制御システムへのサイバー攻撃は停電や爆発等の物理的な破壊をともなうため、死傷者が出る可能性があります。また、情報システムはデータさえ保全されていれば機器そのものは汎用品が多く調達しやすいため比較的短期間で復旧できるのに対して、産業機器は製造に長期間要する特注品が使われていることも多く、物理破壊された機器の復旧に長い期間を要する場合があります。

6 Web サイトの乗っ取りと改ざん

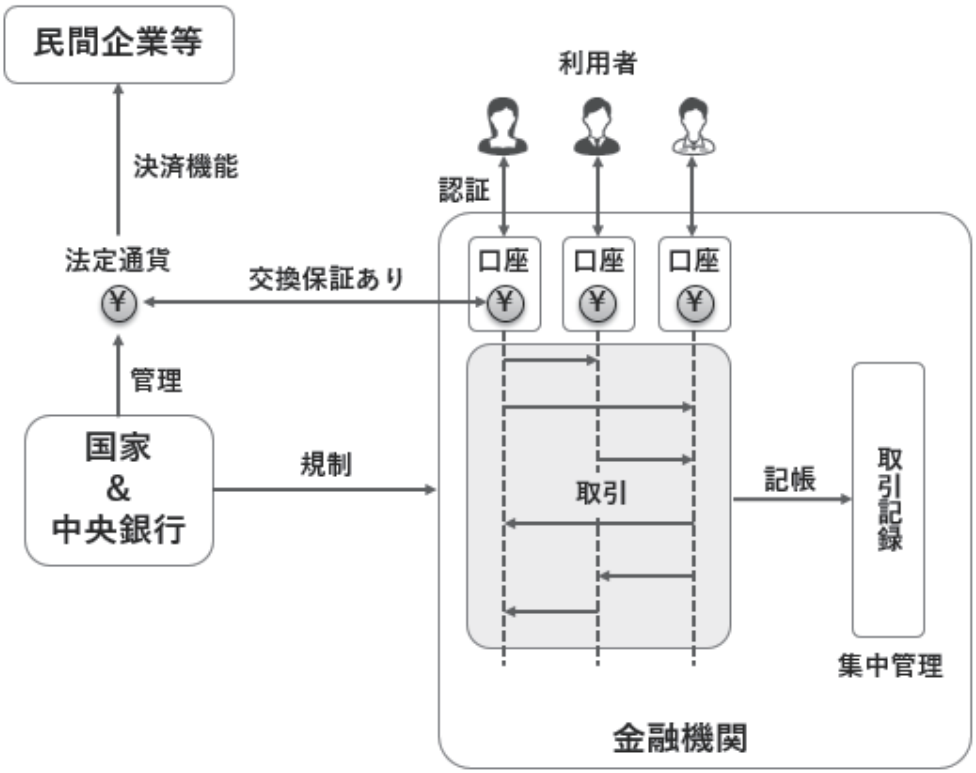


現在は極めて多くの企業が Web サイトを開設して広報やサービス提供に活用しています。Web サイトはその性質上インターネットから遮断できないためサイバー攻撃の標的になりやすく、乗っ取りや改ざんの被害が多数発生しています。これまでに発生した Web サイト改ざん事例としては次のようなものがあります。

- 2000 年、科学技術庁（当時）、総務庁（当時）、運輸省（当時）など多数の官公庁および関連団体のサイトが改ざんされる事件が発生した。
- 2015 年、成田空港および空港企業のウェブサイトが、アクセスしたユーザーにマルウェア感染を行う悪意のあるページを読み込ませるように改ざんされた。
- 2013 年、自動車会社ニュースページの一部が、閲覧したユーザーに不正プログラムをインストールさせる悪意のあるサイトに誘導するように改ざんされた。
- 2017 年、有名 CMS「WordPress」の脆弱性を突いた攻撃により、多数の Web サイトで連続買い残が発生した。

Web サイトの乗っ取り/改ざんが起きるとブランドイメージの毀損、個人情報流出への補償等、自社に損害が発生するだけでなく、流出した個人情報をパスワードリスト攻撃に悪用される、標的型攻撃のための踏み台に悪用されるなど、外部にも被害を広げてしまいます。

7 仮想通貨問題：法定通貨の基本



「仮想通貨」の代表格として知られるビットコインは 2009 年に運用が開始され、2013 年ごろから一般社会にも知られるようになり、2017～18 年にかけて歴史的な急騰を見せました。これにともない、他の仮想通貨も多数誕生しましたが、同時に仮想通貨特有のセキュリティ問題も起きています。

（注：一般的には「仮想通貨」という名称が知られており、本書でもこの用語を使用します。しかし国際機関では「暗号資産」と呼ばれていること、実質的にも「通貨」の要件は満たしていないことなどの理由で日本でも金融庁が 2018 年末に「暗号資産」へと名称を変更する方針を発表しています）

仮想通貨のセキュリティを理解するためには、前提として法定通貨の仕組みを知っておかなければなりません。法定通貨とはつまり通常のお金のことですが、通常のお金には紙幣や硬貨といういわゆる「現金」と、金融機関の口座に「情報として記録されているお金」の 2 種類があります。一方、仮想通貨には現金は存在しません。

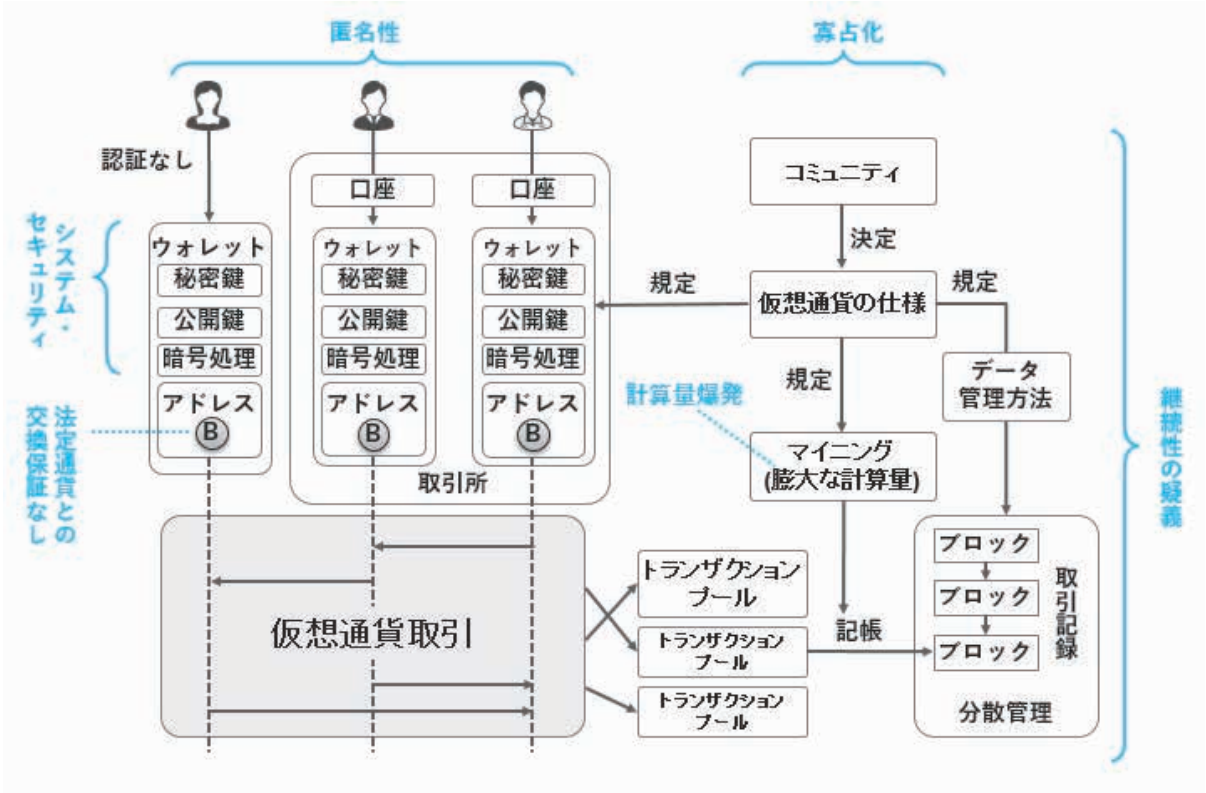
上図は金融機関の口座を通じた法定通貨の取引の仕組みを図示したものです。利用者は金融機関に口座を持ち、口座上で送金の取引を行い、その情報が取引記録に記帳されます。これらを金融機関が集中管理しており、入出金に伴い手数料を徴収されます。口座開設時に利用者の認証（本人確認）手続きが厳格に行われており、匿名で取引をすることはできません。かつ、国家による規制があり、犯罪

捜査や債権回収等の一定の事由が認められる場合は所定の手続きの上で口座凍結や強制徴収等の処置が行われることもあります。

一方で、口座に記録されているお金は法定通貨との交換保証があります。というよりも法定通貨そのものですのでいつでも現金として引き出せます。「法定通貨」は国家や中央銀行が管理し信用を与えているため通常は急激に価値が失われることはなく、「決済機能」が法的に保証されているため、確実に民間企業等への支払に使うことができます。

法定通貨は以上のような特徴を持っていますが、仮想通貨についてはこれらが当てはまりません。

8 仮想通貨のセキュリティ



2018 年末時点で既に 600 以上の仮想通貨が存在し、それぞれ仕様が異なりますが、典型的な仮想通貨の仕組みは上図のようなものです。最大の特徴は「取引を集中管理する金融機関が存在しない」ことにあります。

仮想通貨取引には認証が必要ない

法定通貨の「口座」は金融機関の情報システムの中に開設されますが、仮想通貨で「口座」にあたる「ウォレット」は利用者が管理する PC の中に存在します。ウォレットは秘密鍵/公開鍵を管理し暗号処理の機能を持つソフトウェアのことで、「アドレス」は口座番号にあたります（実際には 1 つのウォレットの中に無限に数多くの秘密鍵/公開鍵/アドレスを持つことができますが、図では単純化のため 1 つだけ記載しています)。「ウォレット」はインターネットにつながる PC やスマートフォンが 1 つあれば誰でも開設でき、認証つまり本人確認の手続きを必要としないため匿名での取引が可能です。

「取引所」では本人確認が必要

仮想通貨のウォレット自体は誰でも匿名で開設できますが、実際に個人でウォレットを管理運用するのは手間がかかるため、ウォレットの管理運用を代行する「取引所」サービスが存在します。その場合、利用者は取引所と契約を結んで取引所の口座を開設し、口座に法定通貨を入金して仮想通貨を購

入し、以後仮想通貨で取引を行う形になります。日本国内の取引所の場合、口座開設には本人確認が必要なため、この時点で匿名性は失われます。海外の取引所では本人確認不要のものがあります。

取引記録は分散管理される

仮想通貨の取引は、「アドレス」を指定して入金/出金を行います。1つの取引毎に取引当事者の公開鍵と秘密鍵でハッシュ化やデジタル署名を行い、改ざんを防止します。すべての取引はいったん「トランザクションプール」という領域に集められ、それを一定の単位毎に「ブロック」として切り出し、二重送金等の不正がないことを検証した上で、過去の取引記録ブロックにチェーンのようにつなげて「記帳」します。この「記帳」の際に力任せに暗号を解くような膨大な計算量が必要になります。過去のすべての取引記録が数多くのノードに複製されて分散管理されているため、一部のノードが停止しても失われることはありません。

匿名のコミュニティによる意思決定

ウォレットでの暗号処理やマイニング、ブロックチェーンのデータ管理方法などを規定する「仮想通貨の仕様」はコミュニティによって決定されます。コミュニティへの投票権を持つ主体は匿名であり世界中に分散しているため、国家機関による管理・規制を受けません。

仮想通貨のセキュリティ問題とは？

仮想通貨の仕組みはおおむね以上のようなものですが、このような仕組みに伴って発生するさまざまなセキュリティ上の問題が指摘されています。

法定通貨との交換保証がない

仮想通貨は法的な意味での通貨ではありませんので、法定通貨との交換はできません。法定通貨に交換したい場合は、法定通貨で仮想通貨を買いたい取引相手を見つけて販売する必要があります。その場合、購入時より高い値段で売れるとは限らず、損失を被る場合もあります。しかし、流行だからという理由で仮想通貨取引に手を出す参加者は、そのリスクを正しく認識していないことがあります。

匿名性が犯罪取引に利用される

「匿名での取引ができる」という特徴が犯罪取引に都合が良いため、ランサムウェアの身代金支払手段として指定される、マネーロンダリングに使われる、などの事例があります。

計算量爆発のエスカレーション

記帳のための「マイニング」という処理には膨大な計算量が必要ですが、仮想通貨の相場が過熱するにつれてマイニング専用設備への大規模な投資が行われるようになり、マイナー（マイニングを行う事業者）の寡占化が進んでいます。

不正防止の前提が破綻する可能性

仮想通貨システムには、法定通貨での金融機関のように「取引記録の完全性に責任を持つ、集中管理する組織」が存在しません。その代わり、「不正を行うマイナーは少数であり、大多数のマイナーは正しく処理をする」ことを前提に、一種の多数決的なアルゴリズムで「正しいブロック」を決定しています。仮想通貨の草創期には小規模なマイナーが多数存在したため、この仕組みが有効に機能しましたが、寡占化が進むとその前提が崩れる可能性が指摘されています。

コミュニティの意思決定の不透明性

仮想通貨の仕様はコミュニティによって決定されますが、コミュニティでの投票権（発言権）はマイナーが持っています。マイナーが寡占化すると一部のマイナー・グループの意向により恣意的な仕様変更が行われる恐れがあります。

システム・セキュリティ

ウォレットを運用している PC やサーバーをクラックされた場合、あるいは取引所の運用で内部不正が発生した場合は不正送金等の被害が発生します。2013 年および 2018 年に国内の取引所でそのような事例が発生しています。

継続性の疑義

2018 年までに 600 以上の仮想通貨が誕生していますが、そのすべてで継続的な取引が成り立つ保証はありません。初の仮想通貨であったビットコインを初期に取得していたユーザーがその後の値上がりで莫大な差益を手にしたことから、「新規仮想通貨公開（ICO, Initial Coin Offering)を入手すれば儲かる」というイメージが生まれました。そのイメージを利用して乱発された ICO 案件の多くに詐欺の疑いがあります。

水飲み場攻撃や不正メールへの悪用

ICO に限らず、急激に話題になった投機的な商品/証券には詐欺的な勧誘がつきものです。こうした「人の欲望」を誘う話題は SPAM メール等で不正なリンクをクリックさせるために、あるいは Web サイトにアクセスした人に不正プログラムをダウンロードさせる「水飲み場攻撃」にもよく使われるため、コンテンツフィルタリングやユーザー教育へ反映させる等の防御策を講じる必要があります。

仮想通貨のセキュリティはデジタル化社会の一つの象徴

もともと硬貨や紙幣のように物理的なものだった「通貨」は、金融の発達とともに「情報」としてのみ処理されるようになりましたが、それでも基本的には物理的な「現金」との交換性が保証され、通貨供給量や取引主体に関しては国家機関によって管理・規制されるのが前提でした。しかし現代のデジタル技術を駆使して作られた仮想通貨にはそのような前提がなく、社会基盤の根底の 1 つを揺るがしうる技術と言えます。これは社会のあらゆる面がデータ化されることにともない発生した新しい

問題の一つの象徴であり、社会が Society5.0 に向かう中で今後も同様の新しい問題が発生することでしょう。その解決には技術と社会の両面から取り組まなければなりません。

9 演習問題

問 1

A 社は、標的型攻撃への対策として、不審なメールを受け取ったときに従業員が採るべき行動を定めることにしました。どのような規程を設けたらよいかを答えてください。

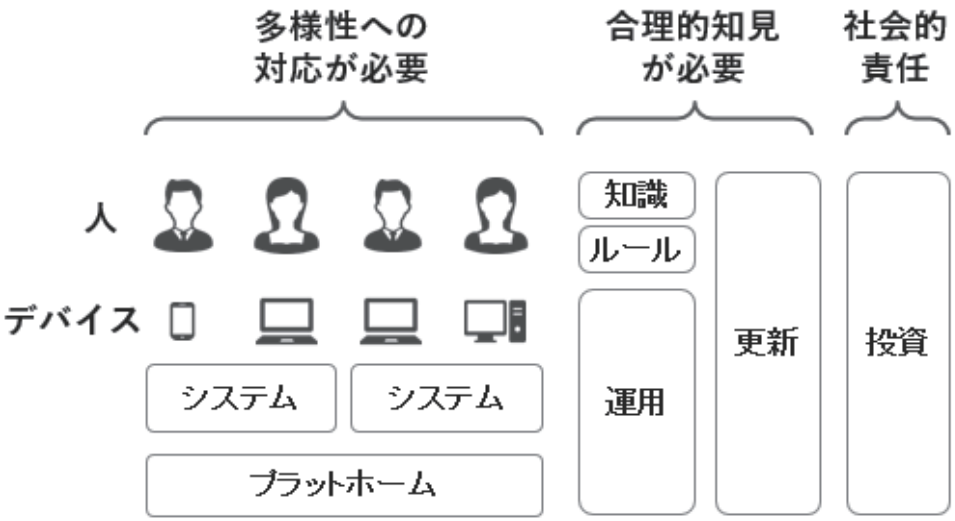
問 2

IoT 機器を利用している組織のセキュリティ対策について、次に示す観点からいくつか具体例を挙げてください。

1．被害予防の処置
2．被害を受けたときの処置
　　‹器廃棄時の処置

第14章.
セキュリティ・インシデントへの対応

1 社会的な取り組みで求められる観点



セキュリティは個人や一企業で行えばよいものではなく、社会全体で取り組んでいかなければならない課題です。社会的な取り組みにおいて求められる観点を整理します。

多様性への対応

「人」が PC やスマートフォンなどの「デバイス」を用いて企業内 LAN やインターネットを通じて「システム」を利用します。そのシステムは何らかの「プラットホーム」の上に構築されています。これらのどの段階でも固有の「多様性」の存在に注意を払わなければなりません。たとえば「人」には会社員の他に幼児・小中高生・学生・主婦・高齢者などさまざまな能力・属性があります。会社員・公務員等、何らかの組織に属する人へのセキュリティ教育はある程度組織を通じて行うことが可能ですが、組織に属さない人々にはそれが不可能ですので、社会的に何らかの対策をとる必要があります。

合理的知見の必要性

デバイス、システム、プラットホームはいずれも人が「運用」するものですが、運用するためには「ルール」が必要であり、ルールを決めるためにも守るためにも「知識」が必要です。そしてこれらを常に最新・最善のものへと「更新」していかなければなりません。ルールには業務マニュアルや就業規則のように明文化されているものと、慣習や文化のように明文規定が存在しないものがあり、双方を合理的な知見を踏まえて見直す必要があります。

特に慣習や文化については変えることへの反発・抵抗が起きるケースも少なくありません。情報セキュリティ問題に限らず、「事故」というのは日常的に起きる事態ではないため、その想定を真剣に考

えたことがない人々の理解を得るのは至難の業です。物理セキュリティに関しては以下のような例があります。

- 川へ水遊びに出かけるのに、子どもにライフジャケットを着せようとすると周囲の親に「過保護」と笑われるので着せていない
- オフィスの大掃除で高いところを掃除するのに、キャスターつき椅子の上に乗って作業する
- 自動車に乗るときにシートベルトを締めない

いずれも「安全」を合理的に考えれば決してやってはいけないことですが、世の中にはこういった合理的な思考を「面倒くさいから嫌だ」「かっこ悪い」「臆病者」のように考える人々も非常に多く、それは情報セキュリティについても例外ではありません。このような人々の行動を変えるためには、価値観や文化のレベルからの対応が必要です。場合によってはここに宗教規範も影響してくるため、さらに対応が難しくなります。たとえば近年ヨーロッパではテロ対策のために顔認証を利用した警備システムが広く導入されていますが、顔認証システムは顔が見えなければ当然機能しません。そこでいくつかの国では公共の場で顔を隠す服装をすることを禁ずる法律が施行されましたが、これは一部の宗教の服装規範に抵触するため宗教的反発が起きています。「面倒くさい」程度の話であれば根気強い話し合いや厳しい指導で対応できても、宗教規範と不整合が起きるルールについてはより難しい対応を迫られます。

社会全体で情報セキュリティの対応をしていくためには、このような多様性がある中でも「合理的な知見」を少しでも適用できるように努力していかなければなりません。

継続的更新の必要性

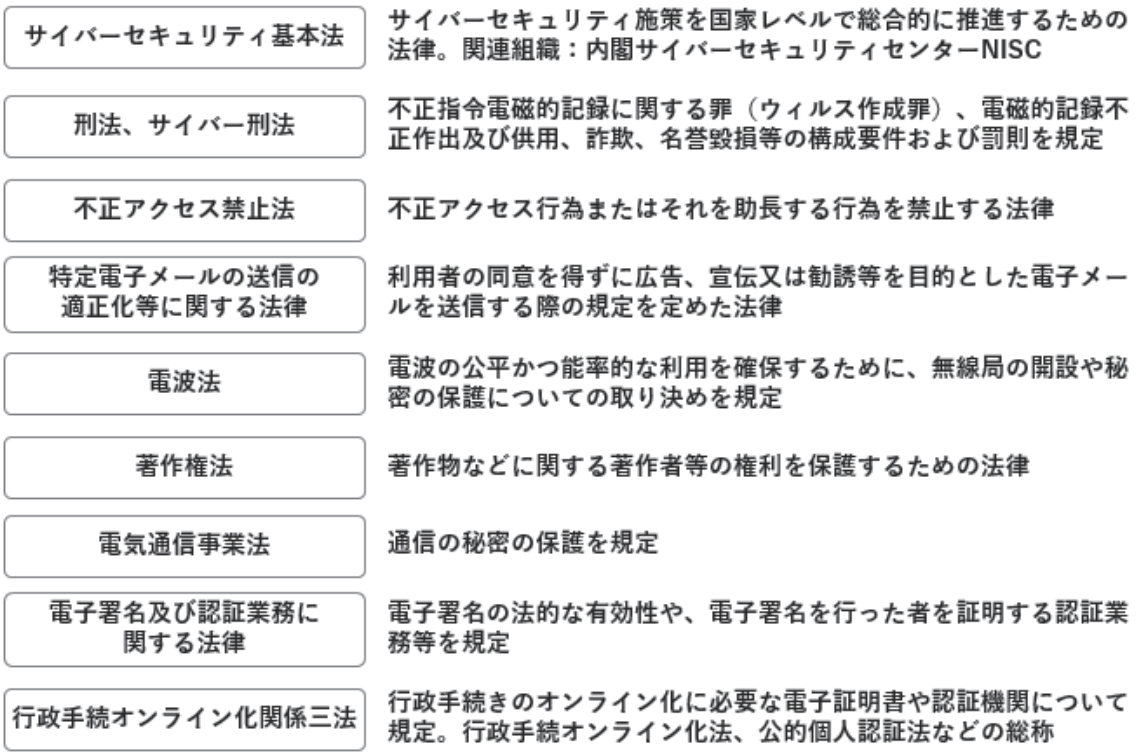
知識やルールは継続的に更新していくことが求められます。たとえばパスワードの管理について、以前は「パスワードは定期的に変更することを利用者に求めるシステム設計」が推奨されていましたが、米国立標準技術研究所(NIST)のガイドラインでは 2017 年から、日本の総務省ガイドラインでも翌 2018 年から、「パスワードの定期変更を求めるのはかえって危険性を増すため、行うべきでない」という方針へと 180 度転換しています。技術もその運用実態も時々刻々変化していくため、それに合わせてアップデートを行っていかなければなりません。

明文化されている業務マニュアル等でも、「昔からこのやり方でやっている」だけで確たる理由もなく決まっている項目があるケースは少なくないものです。長年運用しているルールであっても絶対視せずに見直していく必要があります。

社会的責任

デバイスやシステムおよびその運用、そのための人の知識やルールを更新していくために、必ず必要になるのが「投資」です。古いデバイスの入れ替え、セキュリティ教育、運用手順の改訂等、どんな対応を行うにしても必ずその費用がかかります。その費用が出せないという理由でセキュリティ対応が止まっている場合がありますが、セキュリティに関する投資を行うのは社会的責任であり、現代においてはもはや放置することは許されません。投資に関する決定権を持つのは経営者であって現場スタッフではないため、この責任を負うのは経営者です。現場で働くエンジニアの立場では、経営者に対してこのことをアピールし続けて理解を促す努力をする必要があります。

2 セキュリティ関連法案



社会全体の情報セキュリティ確保への取り組みにはさまざまな法律が関係しています。

サイバーセキュリティ基本法

省庁ごとに縦割りで進められていたサイバーセキュリティ施策を国家レベルで総合的かつ効率的に推進するための法律です。この法律をもとに内閣サイバーセキュリティセンターNISC が設置されています。

刑法、サイバー刑法

刑法は、詐欺、名誉毀損、電磁的記録不正作出及び供用等の刑法犯罪の構成要件および罰則を規定しています。サイバー犯罪の実行者を刑法犯として訴追するための根拠法の一つです。サイバー刑法はサイバー犯罪に対応するための刑法の改正を規定するもので、不正指令電磁的記録に関する罪（通称：ウィルス作成罪）等を規定しています。

不正アクセス禁止法

不正アクセス行為や、不正アクセス行為につながる識別符号の不正取得・保管行為、不正アクセス行為を助長する行為等を禁止する法律です。識別符号とは ID やパスワードのことで、他人の ID・パスワードの不正取得・保管・他者への提供、フィッシングサイトの作成、サイトの脆弱性を突いてアクセス制御の回避を試みる行為等を禁止しています。

特定電子メールの送信の適正化等に関する法律

利用者の同意を得ずに広告、宣伝又は勧誘等を目的とした電子メールを送信する際の規定を定めています。

電波法

電波の公平かつ能率的な利用を確保するために、無線局の開設や秘密の保護についての取り決めを規定しています。

著作権法

著作物などに関する著作者等の権利を保護するための法律です。

電気通信事業法

通信の秘密の保護を規定しています。

電子署名及び認証業務に関する法律

電子署名の法的な有効性や、電子署名を行った者を証明する認証業務等を規定しています。

行政手続オンライン化関係三法

行政手続きのオンライン化に必要な電子証明書や認証機関について規定しています。行政手続オンライン化法、公的個人認証法などの総称です。

3 演習問題

問 1

法律について下記のサイトを調べてみましょう。
「情報セキュリティ関連の法律・ガイドライン」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/index.html

このサイトを参考にして、次に示す行為がどの法律に違反になる可能性があるかを答えてください。

1. 海賊版のソフトウェアを入手し、それを知人に転売した
2. 不正に入手した他人の ID とパスワードを使って、オンラインショッピングのサイトにログインした
3. Web サーバーの脆弱性を利用してサーバーに侵入し、Web サーバーに保管されていたホームページの内容を消去したり書き換えたりした

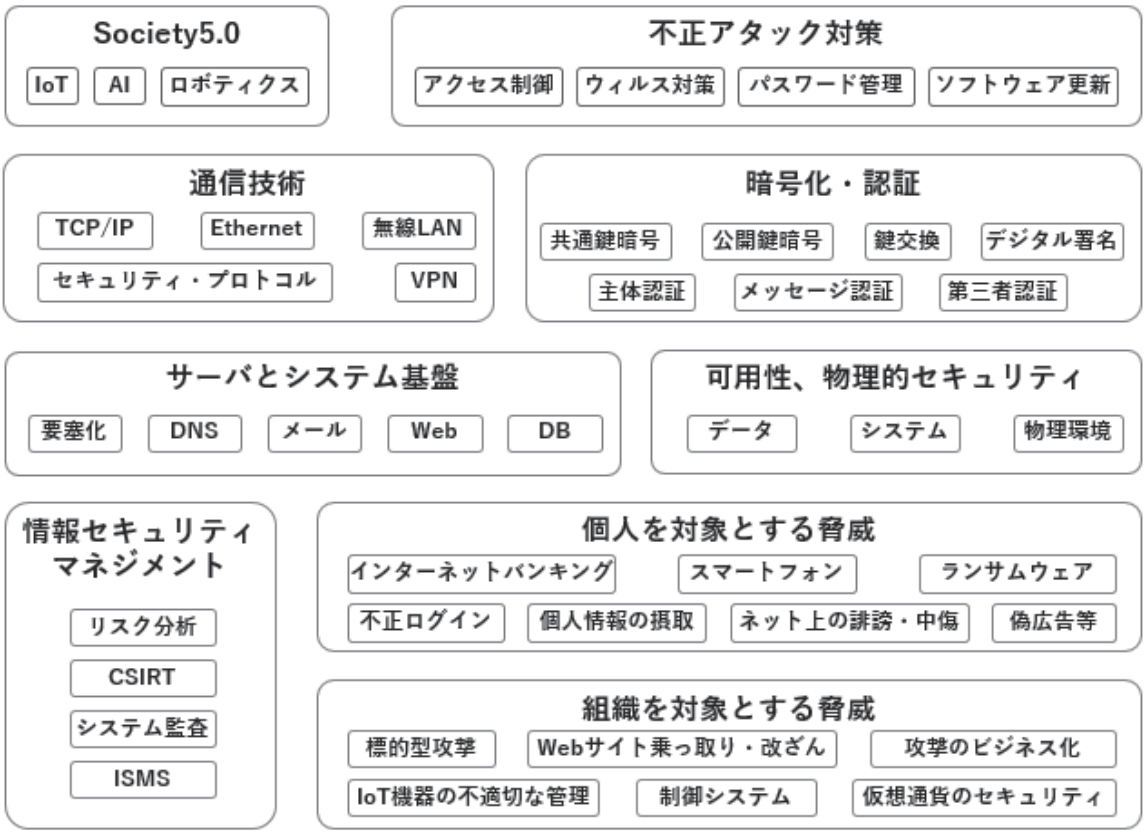
問 2

IoT 機器を利用している組織のセキュリティ対策について、次に示す観点からいくつか具体例を挙げてください。
４．被害予防の処置
５．被害を受けたときの処置
６．IoT 機器廃棄時の処置

第15章.

Society5.0 の担い手として

1 総まとめ



本書のまとめとして、これまでの内容を振り返りましょう。

それぞれの技術的な詳細については既に本書の各部で記載してありますのでここでは繰り返さず、「振り返り」をする効果的な方法をご紹介します。

「振り返り」は何のためにするのでしょうか？　人間は一度説明を読んだだけで理解できることはありません。おそらく上図のキーワードにも、理解できたものもあればピンと来なかったものもあり、覚えてさえいなかったものもあることでしょう。まずはそれぞれのキーワードについて自分の理解がどのレベルかを自己チェックしてください。キーワードのそばに理解レベルを 3 段階で記入していくと良いでしょう。

1. よくわからない(キーワード自体覚えていない、という場合も含む)
2. なんとなくわかった気はするが自信はない
3. 理解できている

「よくわからない」の項目はもう一度読み直したり、別な資料を探して学ぶなどしましょう。

「なんとなくわかった気はする」の場合、分かった範囲の内容を「自分の言葉で短く書いてみる」のが効果的です。そうすると何が分からないのかを自覚できるので、それからもう一度テキストを読み直したり、分かっている人に質問すると効率良く学ぶことができます。
「理解できている」と感じた場合は、積極的に「分かっていない人」の質問に答えましょう。人に教えるのは、自分の理解をより確実にするためのもっとも良い方法です。

自分一人で勉強していて「教える相手」がいないときは、ここでも「自分の言葉で短く書いてみる」方法がお勧めです。さらにその際、「観点」を別に列挙しておきましょう。たとえば

> 質問：共通鍵暗号と公開鍵暗号の違いは？
> 答え：暗号化には暗号鍵が必要。共通鍵暗号は、暗号化と復号に共通の鍵を使う方法。共通の鍵を送信側と受信側で秘密に管理しなければならないので手間がかかる。公開鍵暗号は、暗号化と復号で別の鍵を使う方法。片方は誰にでも公開して良い「公開鍵」であることからこの名前がある。公開鍵は秘密にする必要が無いため手間がかからない。一般に、公開鍵暗号のほうが暗号処理の負荷が重い
> 観点：鍵の数、管理の手間、暗号処理の負荷

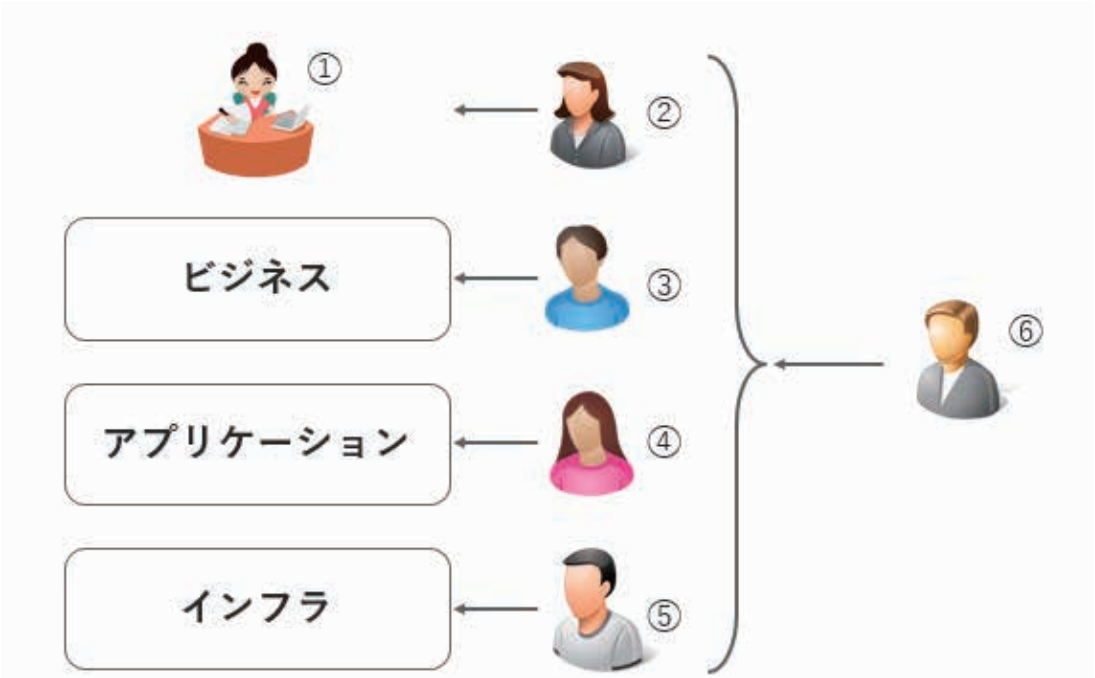
のような形で、「質問」を立てて「答え」を書いた上で、その答えに含まれる「観点」を列挙します。「観点」に漏れがあるようでは十分に理解したとは言えません。このように観点を別建てにしておくと、たとえばそれをベテランの技術者に見せたとき、「○○の観点が抜けているよ」とすぐに教えてもらえます。

よく理解できている場合は、「質問」を多数思いつくものです。たとえば暗号技術について例を挙げると、

- 共通鍵暗号と公開鍵暗号を組み合わせて使うのはなんのためか？
- 共通鍵暗号と公開鍵暗号のアルゴリズムを 2 つずつ挙げよ
- ハッシュ関数とはどのような関数か？

などが「質問」です。このような質問を自力で思いつけない場合は十分に理解できているとは言えないので、あらためて今度は「質問」を考えながら本書各章の説明を読み直してみてください。

2 セキュリティに強い技術者を目指そう

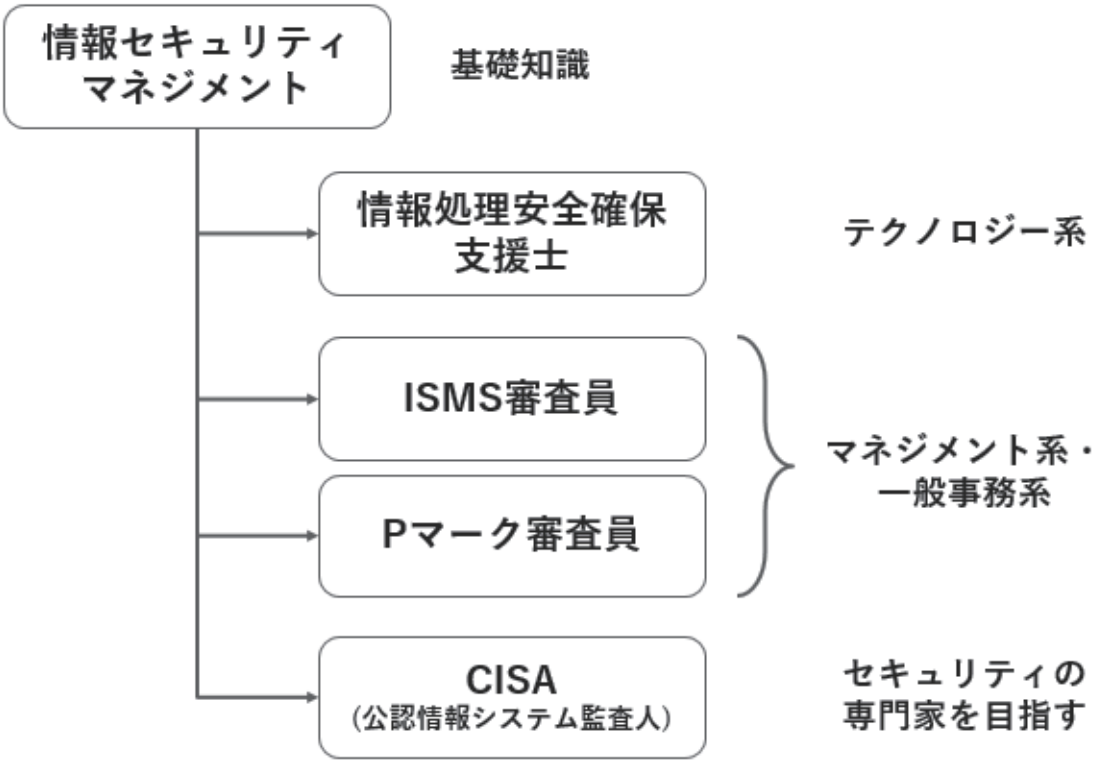


第 1 章でも触れたとおり、IT が生活のすべてに関わるようになる Society5.0 の時代に情報セキュリティは極めて重要であり、セキュリティの専門家だけが知っていれば済むものではありません。あらゆる立場の人々に、その役割に応じてある程度のセキュリティの素養が必要になります。

IT システムはおおまかにビジネス、アプリケーション、インフラの三層で出来ています。①ユーザーが実現したい「ビジネス」を設計し、それを「アプリケーション」として実装し、それを「インフラ」に載せることでシステムが稼働します。IT エンジニアにも②ユーザーのサポート、③ビジネスの設計、④アプリケーションの開発や運用、⑤インフラの構築や運用などさまざまな種類があります。⑥はセキュリティのスペシャリストとして②〜⑤のすべてを支援する役割です。

①〜⑤までの立場はセキュリティの専門家ではありませんが、その場合でもそれぞれの役割に応じてセキュリティの知識は不可欠です。IT エンジニアとしての価値を高めるためにも、セキュリティを学んでいきましょう。

3 これからのロードマップ



セキュリティを学んでいくためのロードマップとして、いくつかの公的資格を紹介します。

「情報セキュリティマネジメント試験」は情報処理技術者試験の一区分で、情報セキュリティの脅威から継続的に組織を守るための基本的な知識、スキルを認定するものです。IT 技術者に限らず、IT を利用するすべての人を対象とする試験であり、セキュリティの入門的な位置づけと言えます。

「情報処理安全確保支援士」は、情報セキュリティスペシャリスト試験の後継として 2016 年に創設されたもので、セキュアプログラミングやネットワークといった要素技術も問われます。テクノロジー系のキャリアパスを目指す人向きの、専門性の高い難関資格です。

マネジメント系・一般事務系のキャリアパスには、ISMS 審査員や P マーク審査員が適合します。

CISA(公認情報システム監査人)は、情報システムの監査および、セキュリティ、コントロールに関する高度な知識、技能および経験を有するプロフェッショナルとて ISACA（The Information Systems Audit and Control Association, Inc. 情報システムコントロール協会）が認定する国際資格です。セキュリティの専門家を目指す方に向いています。

とはいえ、どの資格であっても、資格そのものは「スタートライン」でしかありません。実際にセキュリティを守るための情報収集は資格取得後も欠かさず続けることを忘れずにいてください。

4 演習問題

問 1

あなたが考える「Society5.0 時代のエンジニアに求められるスキルや知識、また姿勢」について自由に述べなさい

演習問題回答

1 演習問題回答

1章　現在・近未来

問1　解答例

機密性侵害

- 正規に認可された利用者がID/パスワードのメモを紛失し、それを入手した第三者が不正アクセスに成功する
- 上司に叱責された職員がデータを流出させる
- メールのご送信によりデータ流出が起きる

完全性侵害

- Webサイトに脆弱性があり、第三者がID/パスワードを入力せずに情報入手に成功する
- Webサイトが改ざんされる
- 偽の発注情報を紛れ込まされて業務処理が混乱する
- システム更新のオペレーションにミスがあり、データが消滅する

可用性侵害

- Webサイトに大量のパケットが送りつけられ、正規の利用者がシステムを利用できなくなる
- 誤操作によりDBに高い負荷を与えるクエリーを発行した結果、性能が極端に悪化する
- 大地震により電力供給が途絶え、サーバーが利用できなくなる

2章　暗号化・認証

問1　解答例

観点	共通鍵方式	公開鍵方式	優劣
暗号化と復号の速度	速い	遅い	共通鍵方式
導入容易性	導入しやすい	第三者認証局に公開鍵証明書を発行してもらうのは有償となるため、導入しづらい	共通鍵方式
管理の容易性	通信相手（ペア）ごとに	自分が管理する鍵は公開鍵	公開鍵方式

	鍵を秘密裏に管理する必要があり、管理が煩雑である	と秘密鍵の 2 種類だけであり、このうち秘密裏に管理するのは秘密鍵だけとなるため、管理が容易である	
共有や配布の容易性	生成した共通鍵を通信相手と共有するため、何らかの安全な方法を用意する必要がある	公開鍵は公開してよいものなので、通信相手に配布するのが容易である	公開鍵方式

問 2　解答と解説

正解は選択肢**エ**です。
RADIUS の認証機能は、クライアントの主体認証を行います。サーバーの主体認証は行いません。
RADIUS の認可機能は、認証に成功した利用者に対し，どのようなサービスを許可するのかを決定します。
RADIUS のアカウンティング機能は、接続、切断、データ量などの利用状況を記録します。

3 章　セキュリティプロトコル

問 1　解答例

観点	IPsec	TLS
暗号化できるプロトコルの種類は何か	IP に限定	TCP を使って通信するアプリケーション層プロトコルに限定
主体認証の機能があるか	事前共有鍵（PSK）を用いた認証機能がある。 厳密に言うと、IPsec 通信を行うゲートウェイが相互に認証している	公開鍵証明書を用いた、サーバー認証とクライアント認証の機能がある
メッセージ認証の機能があるか	ある	ある
リプレイ攻撃を拒否する機能があるか	ある	ない
クライアント端末に専用ソフトウェアをインストールする必要があるか	必要	不要 (*)

(*)　ブラウザが必要であるが、PC やスマートフォンの出荷時にブラウザはインストールされているため、正解は「不要」となる

4章　不正アタック対策

問1　解答と解説

設問(1)

ソフトウェアの脆弱性、脅威となっているウイルスをはじめ、セキュリティに関する情報を入手します。
その種の情報提供を行っている外部機関として、次のものがあります。

JPCERT/CC
https://www.jpcert.or.jp/

セキュリティ対策について解説したサイトを設けている外部機関があります。
最新の情報が記載されていますので、そうした啓蒙情報も入手すべきです。
その種の情報提供を行っている外部機関として、次のものがあります。

IPA セキュリティセンター
https://www.ipa.go.jp/security/index.html

設問(2)

認証と認可を実施します。
認証は、利用者本人だけが「知っている情報」、「持っている物」、及び「備えている特徴」のうち、1つ以上の認証要素を用います。
例えば、パスワードという「知っている情報」を用いて認証を行うことができます。
認可は、認証に成功した利用者にしかるべきアクセス権限を付与することを意味します。利用者に必要以上の権限を与えすぎないように制限を設けることも、アクセスコントロールでは重要です。

設問(3)

- IDS や IPS は攻撃を防御していますから、ログを確認することで、攻撃を受けている事実を把握することができます。
  攻撃の程度や頻度に応じ、セキュリティ強化策を講ずることができます。
- IDS や IPS の初期設定は必ずしも設置環境に最適なものになっているとは限りません。また、月日が経つにつれて設定内容が現実の脅威に十分対応できなくなっているかもしれません。
  具体的に言うと、厳しすぎる設定をしておくと、正常な通信を誤って不正なものと検知してしまう「フォルスポジティブ」が生じてしまいます。
  その逆に、検出ルールを緩くすると不正な通信を見逃してしまう「フォルスネガティブ」が生じてしまいます。
  したがって、ログを監視し、フォルスポジティブ、フォルスネガティブのどちらも生じないよう、適宜チューニングする必要があります。

問2　解答と解説

追加するルール

方向	送信元 IP アドレス	宛先 IP アドレス	プロトコル	SYN ビット	ACK ビット	送信元ポート番号	宛先ポート番号	通信動作
外向き	外部	公開 Web	TCP	オン	オフ	任意	443	接続

追加する位置

- ⑩より上

5章　可用性、物理的セキュリティ

問1　解答と解説

要因	分類	具体例
人為的	サイバー攻撃	不正アクセスによるシステム停止 DoS 攻撃によるサービス妨害・性能劣化 ウイルスによる攻撃
	過失・想定外利用	不注意によるデータの削除 誤操作によるシステムの停止 アクセス急増による高負荷の発生
	故障、空調不良	ハードウェアの経年劣化や過負荷による機能停止 ソフトウェアのバグによる機能停止 空調不良による熱暴走・結露
非人為的	災害	大規模な地震、火災、水害

6章　情報セキュリティマネジメント

問1　解答例

正解は**イ**です。適切な手順は次のとおりとなります。

適用範囲及び境界の定義
情報セキュリティ基本方針の確立
リスク基準の確立、リスクの洗い出しと特定、リスクの分析と評価

リスク対応策の選定、リスク対応計画の策定
経営者等、リスクが顕在化したときに責任を持つ人の承認

まず、適用範囲及び境界を定義し（a)、セキュリティ基本方針を確立します（d)。
その後、リスクアセスメント（b)、リスク対応（c）を行います。
なお、リスク対応にはコストがかかるため、コストとの兼ね合いで対応できないリスクが残存することがあります。そうした残存リスクについて、リスクが顕在化したときに責任を持つ人（経営者や部門責任者など）の承認を得る必要があります（e)。

問2　解答例

従業員

- ダウンロードのメッセージに惑わされることなく、そのページを離れる。
- 怪しいサイトにアクセスしたので、念の為、セキュリティ管理者に通報する。

セキュリティ管理者

- 連絡を受けたら、ウイルス感染の調査を開始する。
- 重症度を判定し、作業対象と作業項目の優先順位を決定する（トリアージ)。
- ウイルスに感染している可能性がある場合､他のパソコンへの蔓延を防ぐための応急措置として、当該従業員のパソコンをネットワークから切り離す。
- ここまでの対応について、当該従業員およびその所属長等に回答する。
- 必要に応じ、他の部署にも連絡し、注意喚起を行う。
- トリアージ以降の対応については、7.3 節の「インシデント・レスポンス（対応)」を参照

7章　サーバーとシステム基盤

問1　解答

サーバー	ポートの（　J　）
サービス（認証）	サービスの（　G　）、認証の（　H　）
オペレーション	脆弱性の（　A　）、不要なプログラムの（　E　）
アカウント	アカウントの（　I　）
権限	権限の（　D　）
プロセス、データ	データやプロセスの（　I　）、（　E　）
ログ	ログ（　C　）・（　B　）体制

9章　VPN

問1　解答と解説

空欄ア、イ

LAN間接続形態は、接続拠点がそれぞれ固定IPをもっているため、空欄アの正解は「**メインモード**」です。
リモートアクセス形態はクライアントが固定IPをもたないため、空欄アの正解は「**アグレッシブモード**」です。

空欄ウ、エ

どちらの形態においても、IPsecトンネル区間は、クライアントとサーバー間の一部分です。したがって、通信モードはトンネル・モードを選択しなければなりません。
よって、空欄ウ、エの正解は「**トンネル・モード**」です。

空欄オ、カ

どちらの形態もIPsecトンネル区間はインターネット区間となっているため、インターネット上で第三者に通信を傍受される危険性があります。したがって、この区間を暗号化する必要があるため、セキュリティプロトコルは「ESP」を選択しなければなりません。
よって、空欄オ、カの正解は「ESP」です。

問2　解答と解説

空欄ア

専用モジュールが必要であり、アプリケーションに制限がないことから、空欄アの正解は「**レイヤ2フォワーディング方式**」です。

空欄イ、ウ

専用モジュールが必要であり、空欄ア以外の方式であることから、空欄イの正解は「**ポートフォワーディング方式**」です。
ポートフォワーディング方式は、ポート番号が変化しないアプリケーションしか使用できません。
よって、空欄ウの正解は「**変化**」です。

空欄エ、オ

空欄ア、イ以外の方式であり、ブラウザ上で動作できるアプリケーションしか使用できないことから、空欄ウの正解は「**リバースプロキシ方式**」です。

リバースプロキシ方式は、ブラウザさえあれば動作できるため、専用モジュールは不要となります。よって、空欄オの正解は「**不要**」です。

10章　無線LAN

問1　解答と解説

正解は選択肢**ウ**です。
選択肢**ア**は、CHAPではなく、EAPに関する記述です。
選択肢**イ**は、EAPではなく、CHAPに関する記述です。
選択肢**エ**は、RADIUSではなく、IEEE802.1Xに関する記述です。

11章　セキュアプログラミング

問1　解答と解説

設問(1)

正解は、項番**③**です。
項番③以外のメタキャラクタ、たとえば項番①「<」を最初に置換したとしましょう。
置換後の文字列は「<」となります。その後に項番③のメタキャラクタを置換するなら、「<」が「<」に変化してしまいます。
この結果、ブラウザに表示される文字は「<」ではなく「<」となります。

設問(2)

正解は次のとおりです。項番①、②及び⑤に基づき、メタキャラクタが置換されています。

```
&lt;script&gt;alert(&#39;Hello World!&#39;)&lt;/script&gt;
```

問2　解答と解説

空欄ア

正解は「**X**」です。
攻撃者が入力した文字列を格納したSQL文は、ユーザーIDの部分が「**ユーザーID = 'X'**」となっています。したがって、ユーザーIDとして「X」が入力されたことが分かります。

空欄イ

正解は「**' OR 1 = 1;--**」です。

攻撃者が入力した文字列を格納したSQL文は、パスワードの部分が次のようになっています。

```
パスワード = '' OR 1 = 1;
```

「＝」の右辺は、2個連続したシングルクォーテーションから始まっています。

1番目のシングルクォーテーションは、プログラムが用意しているSQL文に元から記述されていたものです。その後に続く文字列が、プログラムが受け取ったものを格納した部分となります。したがって、2番目のシングルクォーテーションは攻撃者が入力したものです。

それでは、攻撃者が入力した文字列は「' OR 1 = 1」なのでしょうか？

いいえ、そうではありません。プログラムが用意しているSQL文は、元々、利用者が受け取った文字列をシングルクォーテーションで囲んでいました。したがって、もしもこれが入力されたのであれば、次に示すとおり、パスワードの部分にシングルクォーテーションが 3 個存在していなければなりません。

```
パスワード = '' OR 1 = 1';
```

しかし、説明文に示されたSQL文はそうなっていないので、3番目のシングルクォーテーション以降は、攻撃者がコメント「--」を入力したことにより無効化されたに違いありません。つまり、次に示す文字列が格納されたことが分かります。格納部分を枠で囲みます。

```
パスワード = '' OR 1 = 1;--';
```

「--」以降の文字列はコメントとして解釈されるため、次のものと等価になります。

```
パスワード = '' OR 1 = 1;
```

これは、説明文に示されたSQL文のパスワード部分と一致しています。

よって、正解は上述のとおりとなります。

12章　個人を対象とする攻撃

問1　解答と解説

ウイルスは通信を監視しているかもしれない。インターネットバンキングのログイン時に送信したIDとパスワードを窃取され、それがハッカーに通知されることにより、不正ログインが行われる危険がある。

問2　解答と解説

1箇所のサイトからID/パスワード情報が漏れたとき、それを悪用して他のサイトに不正ログインされる危険がある。

13 章　組織や不特定多数を対象とする攻撃

問 1　解答と解説

次のような規程が考えられます。

- メールに添付されたファイルを開かない
- メール本文に記載されたリンク先にアクセスしない
- メールが正しい送信者から本当に送られていることを電話等で確認する
- 不審なメールの内容を、セキュリティ担当者に報告する

問 2　解答と解説

1.　被害予防の処置

- 初期パスワードから長く複雑なものへ変更する
- 使用前に説明書を確認する（下記の機能の有無を確認するため）
- 外部からの不要なアクセスを制限する機能を活用する
- IoT 機器にアクセスする端末を制限できる機能を活用する
- 自動更新機能を活用し、パッチが公開されたら迅速に更新する

2.　被害を受けたときの処置

- IoT 機器の電源を切る
- IoT 機器の初期化後、「被害予防の処置」を実施する
- 社内のセキュリティチーム（CSIRT）に報告し、対応してもらう
- （CSIRT がいない場合)、ウイルス感染により初期化できない場合は、メーカーのサポート窓口に相談する

3.　IoT 機器廃棄時の処置

- IoT 機器には重要な情報が含まれる場合があるため廃棄時は初期化する
- 廃棄業者等に出す時はデータ消去や秘密保持に関する契約をする。

14章　セキュリティ・インシデントへの対応

問1　解答と解説

1. 海賊版のソフトウェアを入手し、それを知人に転売した
   ↓
   著作権法の違反になる可能性があります。

2. 不正に入手した他人の ID とパスワードを使って、オンラインショッピングのサイトにログインした
   ↓
   不正アクセス行為の禁止等に関する法律の違反になる可能性があります。

3. Web サーバーの脆弱性を利用してサーバーに侵入し、Web サーバーに保管されていたホームページの内容を消去したり書き換えたりした
   ↓
   サーバーへの侵入は、不正アクセス行為の禁止等に関する法律の違反になる可能性があります。さらに、サーバーに保管されていたデータの消去や書き換えは、刑法に違反する可能性があります。

問2　解答と解説

1. 被害予防の処置

- 初期パスワードから長く複雑なものへ変更する
- 使用前に説明書を確認する（下記の機能の有無を確認するため）
- 外部からの不要なアクセスを制限する機能を活用する
- IoT 機器にアクセスする端末を制限できる機能を活用する
- 自動更新機能を活用し、パッチが公開されたら迅速に更新する

2. 被害を受けたときの処置

- IoT 機器の電源を切る
- IoT 機器の初期化後、「被害予防の処置」を実施する
- 社内のセキュリティチーム（CSIRT）に報告し、対応してもらう
- （CSIRT がいない場合)、ウイルス感染により初期化できない場合は、メーカーのサポート窓口に相談する

3. IoT 機器廃棄時の処置

- IoT 機器には重要な情報が含まれる場合があるため廃棄時は初期化する
- 廃棄業者等に出す時はデータ消去や秘密保持に関する契約をする。

参考サイト
「法律違反の事例」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/01.html

15 章　Society5.0 の担い手として

問 1　解答（例）

※先生方へ
この章末問題は、「今までの学習を通じて受講生がどのような意識を持つようになったか」を自由に記述させることが目的となります。
記述内容において、「エンジニアとしてどうあるべきか」のみならず、「IT システムの利用者にとって、どのような配慮や姿勢が必要か」まで言及できるかどうかをチェックください。

平成 30 年度「専修学校による地域産業中核的人材養成事業」
Society5.0 に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

システムセキュリティ構築

平成 31 年 3 月

一般社団法人全国専門学校情報教育協会
〒164-0003　東京都中野区東中野 1-57-8　辻沢ビル 3F
電話：03-5332-5081　FAX　03-5332-5083