INTRODUCTORY CYBER SECURITY

INTRODUCTORY CYBERSECURITY
2nd Edition

# サイバーセキュリティ入門［第2版］

図解×Q&A

Hamuro Eitaro
羽室英太郎

慶應義塾大学出版会

# 第2版に際して

新型コロナウイルスの影響は現在も続いています。

テレワーク、リモート授業等、“密”な環境を避けるためにネットワークの活用は急激に進みました。クラウドサービスの利用も伸長しましたし、技術開発の面でも5GやIoTの利用を前提としたサービスの展開が推進され、メタバース事業が強化されています。

一方、セキュリティ対策の方はどうでしょうか？　サイバー空間のセキュリティ確保についても、サイバー空間の利用状況に応じた対策が必要ではないでしょうか？

従来から、個人情報保護の重要性は説かれていますが、未だにSNS上等では個人の写真や情報等が公開されたり、盗み出されたりしています。ネットワーク上の「安全・安心」と口では言っていても、実際には「ゼロトラスト」、誰も信用できない物騒な空間になりつつあります。

サイバー犯罪やサイバー攻撃等も、多くの人が利用するツールやアプリ等が攻撃対象となっています。

“DX（デジタル・トランスフォーメーション）だ！”、“クラウドへ移行しよう！”と口で言っているだけで内容を理解していない人、“格好いいメタバースのアバターを作ろう！”等と見栄えだけ気にしているような人は、サイバー犯罪やサイバー攻撃のみならず、“なりすまし”等の犯罪の餌食になってしまうかもしれません。ビデオ会議等で利用するアプリやブラウザも利用者が増加すれば、不正アクセスやマルウェア感染等の攻撃対象となります。

セキュリティは固定されたものではありません。このような状況の変遷に追随して対応策を考え、迅速に実行に移すことでしか実現できないものです。利用者が身を守るすべとして初版で記載した内容も、情勢の変化にあわせて書き換えなければならない箇所が多く見受けられるようになりましたので、改訂することと致しました。

初版刊行以降時代も変わりました。私自身も在職していた警察庁を退官しました。

従来の体裁を変えない範囲で手を加えましたので、不十分な点も多いのですが、逐次見直して参りたいと思います。ご寛容の程、お願い致します。

セキュリティ情報のカタログとして使用して頂ければ幸いです。

2022年春

羽室　英太郎

# 目　次

第２版に際して　i
初版 はじめに　ii

## 第１章　サイバーセキュリティとは？

新型コロナウイルス感染症が「サイバーセキュリティ」を変えた　2
1-1　サイバーセキュリティと「情報セキュリティ」は違う？　5
1-2　「サイバーセキュリティ基本法」とは？　8
1-3　サイバー空間の脅威？　12

## 第２章　セキュリティ上の「リスク」？

1　情報の漏えいはどのようにして生じる？　16
2-1　「脅威」と「リスク」、「インシデント」はどう違う？　18
2-2　「障害対応」も情報セキュリティ？　20
2　組織やビジネスにおけるセキュリティ上の脅威はどこに？　22
2-3　ファイル作成から廃棄まで～適切な情報の管理　24
2-4　システム設計・構築時や廃棄時の脅威　26
2-5　「サイバー攻撃」ってどのようなもの？　28
2-6　サイバー攻撃手法の変遷　30
3　プライベートに潜むセキュリティリスク　32
2-7　フィッシング詐欺やスミッシングに騙されない！　34
2-8　スマートフォンの盗難・亡失が実際に発生！～どうすれば？　37
2-9　公共の場での入力～個人情報が見られていませんか？　39

## 第３章　他人事ではないサイバー攻撃

1　「サイバー攻撃」の目的と対象～何が狙われる？　42
3-1　脆弱性（弱点）を見つける方法　44
3-2　脆弱性（弱点）を放置すれば？　46
3-3　ソーシャル・エンジニアリングとは？　48

2　弱み（脆弱性）に付け入る攻撃手法　50

3-4　アカウント管理～パスワードの使い回しに注意！　52

3-5　基本ソフト（OS）やアプリケーションへの攻撃　54

3-6　サーバや開発システムへの攻撃　57

3-7　OSS（オープンソースソフトウェア）への攻撃とは？　60

3-8　ホームページを見ただけでウイルスに感染するのか？　62

3-9　家庭の様々な機器が狙われる　64

3-10　防犯カメラや業務用・制御用のシステムも狙われている　67

3-11　端末以外も！～調達時に潜む危険性～サプライチェーン管理　71

3　システム侵入後、マルウェアは何をするのか？　75

3-12　マルウェアの危険性　79

3-13　ワンクリックウェアやクリックジャッキングの仕組み？　81

3-14　バックドアやルートキットとは？　83

3-15　“ボット”の機能と高度化　85

3-16　バンキングトロイ（不正送金ウイルス）とは？　89

3-17　ランサムウェア～マルウェアによる脅迫　93

3-18　ウイルスを作成することは罪になる？　97

3-19　スクリプトウイルス？　99

3-20　マルウェアは検出を逃れようとする　103

4　脆弱性がなければ安心？　108

3-21　標的型攻撃と水飲み場型攻撃　110

3-22　なりすましにひっかからない！　114

3-23　「アクセス集中！」かと思っていたら…DoS 攻撃？　127

3-24　Web を利用したマーケティング？ クッキー？ クッキーレス？　140

3-25　DNS への攻撃・DNS の悪用　152

第４章　セキュリティを確保する！――事前の準備とその対策

1　組織のセキュリティ対策に必要なこと？　156

4-1　リスク分析とその評価　158

4-2　リスク評価の指標とは？　160

4-3　情報セキュリティマネジメントシステムとは？　162

4-4　P マークだけじゃダメ？ GDPR の施行！～個人情報保護対策　166

2　攻撃状況が「見えない」ことが難しい！　172

4-5　セキュリティ対策①　組織・人的対策　174

4-6　セキュリティ対策②　物理的対策　178

4-7 セキュリティ対策③ 運用管理（監視）～攻撃の「見える化」 184
4-8 アクセス制御と認証 195
4-9 日常業務～マルウェア対策・ソフトウェア更新 209
4-10 セキュリティ監査とペネトレーションテスト 215
4-11 バックアップと仮想化 217

3 「Web アプリケーション」のセキュリティ確保 227
4-12 SSL（TLS）や VPN の仕組み～ネットワークのセキュリティ確保 229
4-13 電子証明書や認証局の役割と仕組み 234
4-14 メール送付における「送信ドメイン認証」 240
4-15 Web アプリケーションへの攻撃 244
4-16 PPAP なぜ禁止？ 264

第 5 章 「異常」発生？――検知（検出）と対処

平素の運用状況（定常状態）を把握し、“異常”発生時に備える！ 268
5-1 エンドポイント・セキュリティと「ゼロトラスト」 270
5-2 「サンドボックス」～振る舞いの検知？ 272
5-3 検疫ネットワーク・出口対策 275
5-4 インシデント・レスポンスの留意点 278
5-5 デジタル・フォレンジックとは？ 280
5-6 ネットワーク・フォレンジックとトレース 288

第 6 章 端末機器のセキュリティ
――職場のパソコンや自分のスマホは大丈夫？

1 職場で「セキュリティ担当」に指名されたら？ 292
6-1 職場の PC や端末の管理は？ 294
6-2 ルータ、ハブ、NAS、Wi-Fi 機器にも注意！ 301
6-3 オフィスの複合機（MFP）に注意？ 303
6-4 コンプライアンスや内部統制、監査との関係？ 305
6-5 「ウイルスが検出されました！」と表示されたら？ 307
6-6 「リベンジポルノ」と「ネットストーカー」 309

2 スマートフォンの危険性？ 312
6-7 スマートフォンへの攻撃 314
6-8 「ワンクリック詐欺」に引っかからない！ 319
6-9 スマートフォンを業務で利用する？ 322

6-10 スマートフォンにおけるフィルタリング設定 325
6-11 ネット選挙と SNS の利用 329
6-12 スマートフォンでも P2P には要注意 331
6-13 スマートフォンの迷惑メール？ 338
6-14 スマートフォンがおサイフ？ 344
6-15 スマートフォンで仮想通貨の取引…大丈夫？ 354
6-16 ネット詐欺に騙されないためには？ 367

## 第７章　IT サービスの高度化とセキュリティ確保

暗号・匿名・分散技術の進展とセキュリティ対策 374
7-1 匿名性を確保するためのサービス？ 377
7-2 個人情報の匿名性を確保するには？ 381
7-3 ビッグデータ、IoT 機器のセキュリティ 385
7-4 制御システムのセキュリティ 390

## 第８章　クラウドの活用とセキュリティ対策

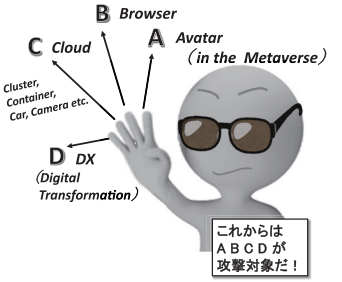
クラウドの活用とセキュリティの確保 398
8-1 クラウドとは？どのような種類があるのか？テレワークでも利用？ 400
8-2 仮想化技術とクラウド、コンテナ？ 404
8-3 サーバレス？マイクロサービス？何のこと？ 409
8-4 クラウドへの攻撃 411
8-5 クラウドネイティブ、ゼロトラスト 415
8-6 クラウド防護の手法 418
8-7 クラウド環境におけるフォレンジック 425
8-8 クラウド・セキュリティに関する標準・ガイドライン 430
8-9 「ゼロトラスト」関連の規定等 436

## 第９章　組織の情報セキュリティ管理のために

国際標準や規格等 440
9-1 ISO/IEC 27000 シリーズ（情報セキュリティマネジメント）の規定 442
9-2 ISMS と ITSMS、BCMS、DR 444
9-3 個人情報・プライバシー保護 448
9-4 IT ガバナンスと IT 統制 450

9-5　プロジェクトマネジメントとリスクやセキュリティの管理　454
9-6　ITSEC（IT 製品のセキュリティ）　456
9-7　暗号・認証技術の規格　460
9-8　ソフトウェア開発とセキュリティの確保　463
9-9　自動車のソフトウェア開発と CSMS　468
9-10　会計システムのセキュリティ　471
9-11　セキュリティ関連の資格・団体　475

あとがき　479
INDEX　480




本書の電子版はイラストがカラーになっています。
右の QR コードから見本をご覧いただけます。

# 新型コロナウイルス感染症が「サイバーセキュリティ」を変えた

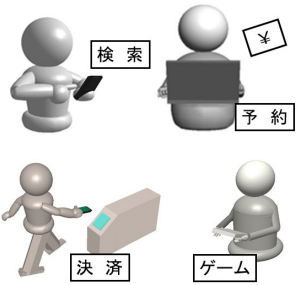
## ◆DX と「サイバーセキュリティ」

**「風が吹けば桶屋が儲かる」**と言うのに似た**「新型コロナが DX（デジタルトランスフォーメーション）を加速した」**という表現ですが、新型コロナ禍は、単に IT（ICT）化の推進や浸透を促進し、生活を一変しただけでなく、セキュリティ対策の仕組みや考え方も大きく変えてしまいました。

**ロボット**や**IoT**（Internet of Things）、**AI**（Artificial Intelligence）、**AR/ VR**（Augmented Reality/ Virtual Reality）等の技術、さらにはこれらの技術を活用して、仮想空間の中に現実空間のような世界を構築する**デジタルツイン**（デジタル複製）等、DX には様々な要素技術が含まれます。

テレワークや Web 会議等、リモート環境における業務の継続と推進を図らざるを得ない状況下、DX 技術でも何でもよいから、一刻も早く仕事ができる環境を構築するため、「クラウド」の活用も急速に伸びました。

## ◆「サイバーセキュリティ」の必要性




パソコンやスマホは、各種サービスの利用やその予約、物品等の売買・決済ツールとして、あるいはゲームや音楽・映像を楽しむ道具として欠かせないものとなっています。

十数年前には**「パソコンも携帯も不要！」**と言って済ませることができました。

しかし、今やスマホやパソコンが使えなければ、社会生活自体が非常に不便な状況にもなってきています。

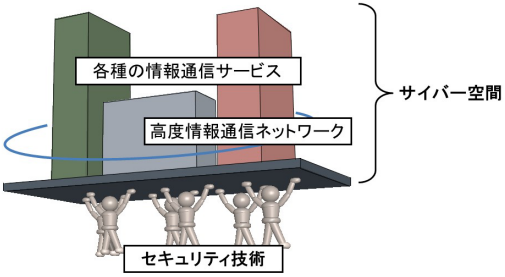
高齢の方で高機能なスマートフォンを駆使している人も多数おられますが、まだまだ拒否反応を示す人も多いのではないでしょうか。


それでも、ガラケー自体の生産・販売が行われなくなると、不得意でも使用しなければ生活に困ります。

従来、**「情報セキュリティ」**は、会社や行政の業務で利用するコンピュータ端末やパーソナルコンピュータのセキュリティを確保することに重点が置かれてきました。

個人が使用する携帯電話やスマートフォンについては、その安全な使用方法や「詐欺」等に騙されないための啓発活動は推進されてはきましたが、「端末」の操作手法やパスワード管理等、いわゆる「エンドポイント」に限定したセキュリティ対策が中心で、ネットワークやシステム等、全体像が見えない、と感じる人も少なくないのではないでしょうか？

## ◆「クラウドサービス」とセキュリティ




各種サービスの基盤や高度情報通信ネットワークが「サイバー空間」で、その信頼性や安全を確保するために必要な技術が「セキュリティ」である、という説明を行ってきましたが、これも、大きく変わってき

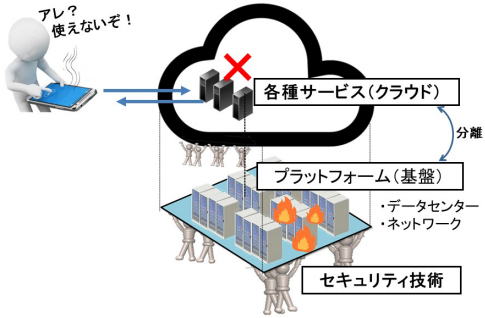
ました。

もともと、個人情報やネットワークを保護するためには、暗号技術や認証技術等、様々な、かつ高度なセキュリティ技術が用いられていて、これらの技術を理解し、適切な利用を行うことが、IT サービスの安全性の確保につながっていたのですが、スマートシティ（スーパーシティ）の物流や防災等のサービスを提供するための基盤として各種データを集約・連携し活用するための**「都市 OS」**という概念も打ち出されるようになってきました。

また**「バーチャル」**と呼ばれるような、多様な「仮想化」技術により、サービス自身の多様性も増大して**「メタバース」**とも呼ばれるようになりました。その様々なサービスの多くも**「クラウド」**を基盤とし、複雑化も進展しています。


企業や行政組織までも、情報システムを構築する際には、その基盤として、自前のシステムを構築（オンプレミス）するのではなく、事業者の提供するクラウドサービスを利用することを優先的に考慮するという**「クラウド・ファースト」**の考え方を導入するようになってきました。

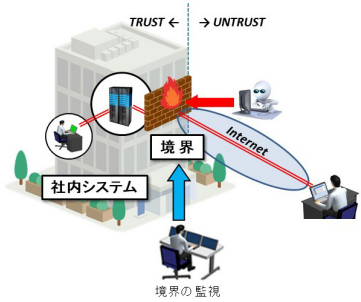
特に政府情報システムの構築・整備に際しては、クラウドサービスの利用を第一義的に検討する**「クラウド・バイ・デフォルト原則」**も打ち出されていますが、一方で、2021年の**「サイバーセキュリティ戦略」**や**「サイバーセキュリティ 2021」**では、**「Cybersecurity for All」**や**「DX with Cybersecurity」**等、全ての面でセキュリティの確保が重要であることを強調しています。




クラウド利用により、自営システムの構築や保守が不要になれば、クラウドサービス事業者だけがセキュリティを考慮すればよいのでしょうか？　他の利用者はセキュリティを考慮しなくてもよいのでしょうか？

いえいえ、クラウドサービス自体も事業者のプラットフォームに依存していますので、これらを含めトータルなセキュリティ確保を行うことが重要となります。

オンラインの決済サービスが急に使えなくなった。どのような障害が発生しているのか！とサービス主体に問い合わせても、情報通信基盤側のシステム障害等の場合には、サービス主体側では原因究明や障害部位の特定等を迅速に行い復旧する作業が行えず、**「早く直せ！」**と督促することしかできなくなる事態に陥る、という障害事例も実際に発生していますので、サービス主体側もプラットフォーム側も、どちらもセキュリティ対策が重要となります。




### ◆「ゼロトラスト」の時代へ

テレワークや自宅からの Web 会議が普通の状況となれば、従来のように勤め先のシステム利用環境のみを防護する、という考え方では情報セキュリティの確保は難しくなります。

この従来型の情報セキュリティ対策では、インターネット等の回線を経由して外部から到達するコンピュータ・ウイルス等のマルウェアが内部の安全なネットワークに侵入することを阻止する**「境界防御」**が中心で、このためにファイアウォール等、外部との接点での監視を強化することにより、内部の安全を確保する、という考え方が中心となっていました。

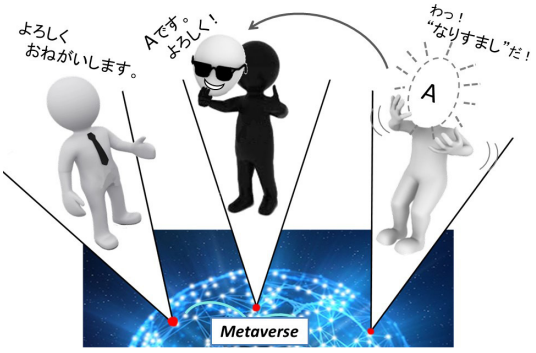
しかしながら、外出先や家庭からも業務に関係する情報データにアクセスする等の利用方法が主となれば、通信相手を信用することも簡単にはできなくなります。盗聴やなりすまし等の脅威から常時防護することが重要となります。

防護を行うにも、家庭の通信環境やクラウドサービス等、関係する全てのシステムやサービスの安全性を常に確保する必要がありますが、これらのネットワークやデータベース、サーバ等も、従来の物理的なものから仮想化されたもの、即ちソフトウェアによって構築されたものへと変化していて、**SDP（Software Defined Perimeter）**と呼ばれる新たな境界モデルへと変わってきています（§8-2参照）。

このように、ネットワークや端末、サーバのみならず、情報資産そのものへのアクセスの正当性を常にチェックする等、ユーザや端末（デバイス）の認証を的確に行うことにより多様な脅威から防護する考え方は**「ゼロトラスト」**と呼ばれ、近年の多様化が進んだネットワークにおける情報セキュリティ確保を行う際の主流となってきています。

各種 IT サービスの利用者の立場とすれば、全てのサービス提供者がセキュリティ対策も含めて安全なシステムを構築し、安全・安心なネットワーク利用が簡単に行えることが理想ですが、現実は様々な脅威に晒されている状況にあります。

現実世界が仮想空間内に**「デジタルツイン」**として再現され、自身の分身ともいえるアバターが**「メタバース」**上で活動する時代ですが、これらのデータが偽者である可能性は否定できません。




ICT 社会における情報セキュリティ確保のためには、その対象となる情報やシステムの全体像を捉えることが必要である、との考えでこの本の執筆をはじめましたが、ほんの一部分にしか迫れていません。各種の脅威やセキュリティを確保するための機器や用語、被害の予防方策、実際に被害に遭った場合の対処等、ネットワーク上での“護身術”の基礎的な部分について理解できるよう、難解な技術的な説明は避け、直感的に理解して頂けるように図を多く入れたつもりですが、いかんせん、横文字の用語がそのまま使われることの多いセキュリティ技術ですので、なかなか詳細な説明まで行うことはできませんでした。

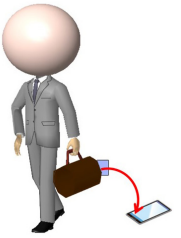
解りにくい用語、従来と意味合いが異なる用語も増えています。たとえば従来「レジストリ」といえばパソコン等設定情報等を記録したものを指すことが多かったのですが、「クラウド」が主流となった現在では、リポジトリ、アーカイブ等と同様の用い方となり、私のような老人は困惑を覚えることも多くあります。これらの多様な用語の詳細説明を網羅することはできませんでしたが、ご容赦下さい。

# 3　プライベートに潜むセキュリティリスク


「テレワーク」での業務推進の際に気になるのは、自宅等のセキュリティ環境ではないでしょうか。多くの人は、パソコンにウイルス対策ソフトを導入する等、適切な防護対策を取っていると思います。でも、パソコンのウイルス対策だけでは、セキュリティ対策が万全とは言えません。企業秘密の情報をプリントアウトしたりゴミ箱に捨てたりはしていませんか？

現在は、エンドポイントにおける確実な「多層防御」が求められる時代となってきています。

## ◆IT ツールの多様化



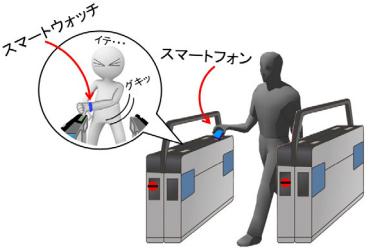
個人のスマートフォンやタブレット等にも、仕事関係者の氏名と連絡先が入っていることは多いでしょう。


このようなモバイルツールは、持ち運びの際に本体を落としてケースの破損だけでなく中のデータが消滅してしまったり、**「ながらスマホ（歩きスマホ／スマホゾンビ）」**で自転車や歩行者にぶつかる等のトラブルを招いたりする状況も多く発生しています。

ソフトウェア（OS やウイルス対策ソフト）の更新等を怠っていると、ウイルス感染によるデータの流出事故等が発生することも懸念されます。


## ◆多機能化

また、スマートフォン自体の多機能化も進展しています。既に定期券や財布代わりとして、実際に実生活の多くの場面で活用している人も多いのではないでしょうか。

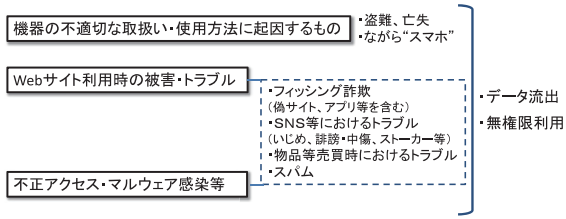




これらはスマートフォンやスマートウォッチ内の NFC や Felica チップ（IC）内に残額データ等が記録され、これを読み取ったり、チャージの際には増加させた値を書き込むもので、その方式は国際標準で規定されています。このため、その方式を熟知している者による「電子スリ」のような行為も出現しています。

## ◆機器は「小型」でも被害は大きい

個人情報や財産価値を有するデータが詰まったスマートフォンやパソコンは、そのデータ自体が狙われるだけではありません。




もし端末等を落としたりした場合には、その端末やアカウントを利用して、特定のサイトにログインすることも可能となります。

SNS 等へ勝手に変な書き込みをされて「炎上」を招いたり、家族の個人情報や写真が流出する危険性もあります。

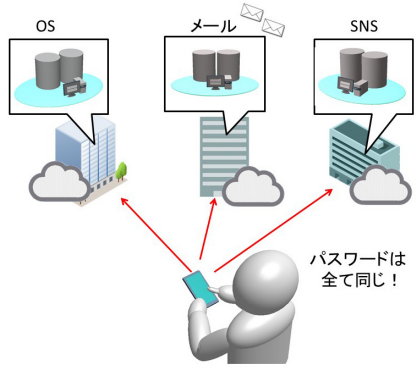

## ◆まずは端末の適正管理

端末機器はうっかり忘失・落とさないようにすることが肝心ですが、もし落とした場合でも、他人に中のデータ等が覗き見られることがないよう重要なデータは基本的には保存しない、もし保存する場合は暗号化する、指紋や最近では**顔認証（FaceID）**等の生体認証でガードする等の対策が重要です。

また、端末を操作する際には、覗き見防止のプライバシーシール（フィルム）を活用したりすることも重要です。

実際に、窓の外からパソコンに入力したパスワードを見られる、隣席の人がスマホを覗き込んで、個人情報を盗み見られる等の被害も発生しています。

パスワードの管理も重要です。クラウド上でメールや様々なアプリを利用することも多くなってきましたが、結構多くの人が複数のサイトを利用する場合に同一パスワードを利用していますので、もし、１つのサイトでパスワード等の流出事故等があれば、他サイトのデータも危険に晒されることになります。

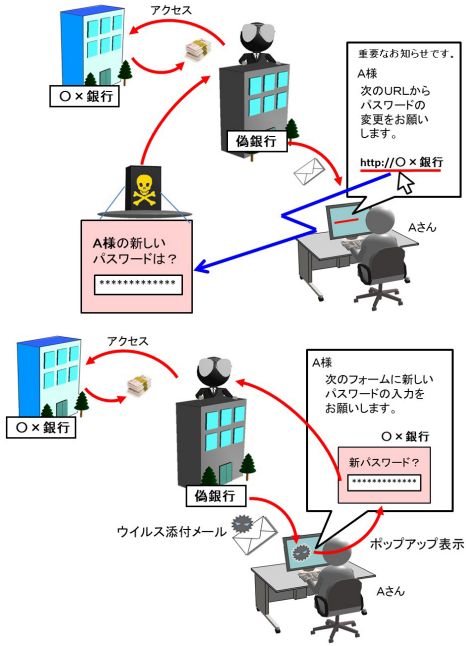



パスワードの使い分けをきちんと行う、そもそも信頼できるサイト、アクセスポイントやアプリを利用するように心がける、アプリも含め常に最新の状態となるよう、日課としてアップデートを行うよう心掛ける等、何事にも地道な努力が必要でしょう。

## §2-7　フィッシング詐欺やスミッシングに騙されない！

「不審なサイトにアクセスしたり安易にクリックやダブル・クリックしたりするのはやめましょう」と言われるが、それでフィッシング詐欺やスミッシング被害を防止することはできるのだろうか？

### ◆フィッシング詐欺の手口




フィッシング（Phishing）詐欺の多くは、口座番号やアカウント、カード番号等を含む個人情報を詐取することを目的に、金融機関等を装って電子メールを送りつけ、その中のリンクをクリックさせて別の偽サイトに誘導し、個人情報を入力させる手口が一般的でした。

その後、今から10年程前になると、**不正送金ウイルス**が登場しました。ウイルスを添付したメールを送りつけ、別サイトへクリックさせて誘導しなくても、マルウェアが動作してポップアップ画面を表示し個人情報の入力を促す、というものです。本人は正規の金融機関サイトにアクセスしていると思っていても、実際にはその情報は偽サイト等に送付される、という手口です。

正規のサイトの入力フォームに悪意のあるスクリプト等を埋め込み、入力内容を悪意のある第三者に送信させる攻撃は「フォームジャッキング攻撃」等とも呼ばれています。

### ◆スミッシング

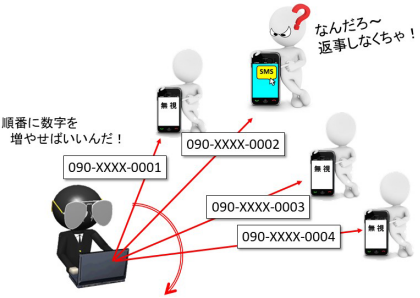

SMS（ショートメッセージ）を用いたフィッシング詐欺、という意味ですが、スマートフォンの普及に伴い増加しています。

金融機関だけでなく、運送（宅配便）業者の不在通知を装って、記載されたリンク先にアクセスさせたり、電話連絡を取らせるようなメールを送付します。携帯電話事業者等に扮して「**重要なお知らせ**」と称するメールを送付したりします。

SMS は、メールアドレスを知らなくても電話番号だけでテキストメッセージを送付することができますので、電

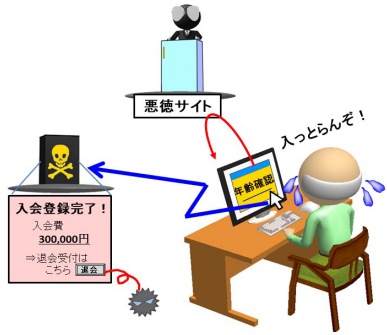
話番号を順次増やしたりランダムにセットして送り付けることが簡単にできます。

送付されたSMSの中のリンク先のURLは、短縮形等にして本来のドメイン名等が判別しにくくなっていることも多いので、見知らぬ相手から送付されたURLのリンク先にはアクセスしないことが重要です。OSやアプリを最新に保つ、そもそも怪しいアプリはインストールしない等の対策が必要です。



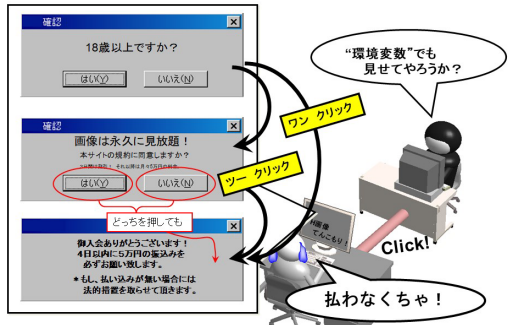

## ◆「ワンクリック詐欺」も「ツークリック詐欺」も同じ！

ちょっとエッチな動画（アダルト）サイトを見ようとして、「年齢確認」等のボタンをクリックした途端に、「入会登録完了！」等のメッセージが表示され、高額の入会金が請求される、そこで慌てて退会しようとボタンを押したりメールを送付したりすると、その場合も高額な利用料や解約手続に要する高額費用が請求されるというものがワンクリック詐欺です。




ボタンやリンクをクリックした際にマルウェアをダウンロードさせ、メールアドレス等の個人情報を盗み出したり、延々と支払い督促画面を表示させるような動作を行わせるのがワンクリックウェア（ワンクリウェア：§3-13参照）と呼ばれるものです。このワンクリウェアには実行形式のプログラム（exe）やVBScript（VBS）、ブラウザで自動実行可能なHTML Applications（HTA）ファイルが多く用いられています。


場合によっては、法等を遵守して手続を行っているかのように錯覚させたり、あえて分かりにくくするために「ツークリック」させる手口も取られています。




IPアドレス等を表示させ「入会者」が特定されているかのように思わせた

## §3-8　ホームページを見ただけでウイルスに感染するのか？

「ホームページを見ただけでウイルスに感染する」というのは本当だろうか？
また「ウイルス感染」と表示されたら、どうすればよいのだろうか？

### ◆本当に感染しているのか？


インターネットを利用していて、ブラウザ上に「ウイルスに感染」とか「ファイルが破損しています」等と表示されたら、ほとんどの人が驚くのではないでしょうか？

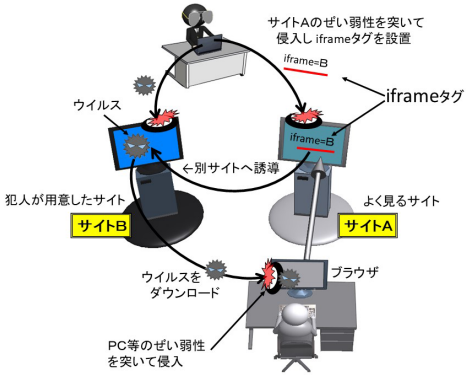
実際には感染していないのに、あたかもウイルスに感染しているかのような表示を行うスケアウェア（Scareware：恐怖心を煽るソフト）とかフェイクアラートと呼ばれるものがスマートフォンでも増加しています。まず落ち着いて、本当にウイルスに感染しているのかどうかを確認しなければなりません。


画面に「○○（電話 XXX）に連絡（電話）してください」等と表示されていても、システムの修復やウイルス対策ソフトの提供を名目に架空請求を行う詐欺かもしれませんので、電話してはいけません。

また、ウイルス対策ソフト自体が表示させる警告と同じような画面で「ボタンを押せ！」等の表示を行っている場合、ボタンを押してしまうと、マルウェア等をダウンロードしたりインストールさせるトリガーとなって、結果的にウイルスに感染してしまいますので、ボタンを押さないことが重要です。

また、ポップアップ警告画面等は「閉じる」を押しても応答しないように設定されていることも多いので、ブラウザを終了させてから、ウイルス対策ソフト（アプリ）によりコンピュータやスマホ内をスキャンしウイルスの有無をチェックしましょう。

このような偽セキュリティソフトは、Fake AV とか詐欺的セキュリティソフト、ボーガスウェア（bogus（偽物）の software）、ローグウェア（Rogueware：偽装ソフト）等とも呼ばれます。



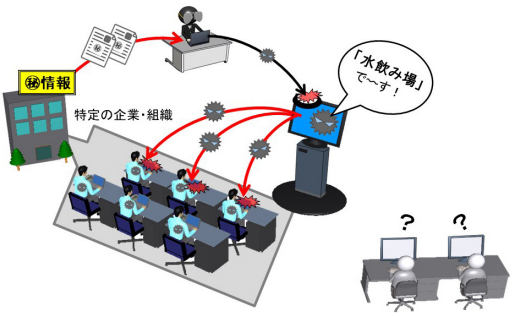

### ◆実際にウイルスに感染していた！（ドライブ・バイ・ダウンロード攻撃）

実際に、ホームページを見ただけでウ

イルスに感染することはあり得ます。このような攻撃手法は「ドライブ・バイ・ダウンロード（Drive-By Download）」と呼ばれています。

2001年のNimda（ニムダ）や2003年のRedlof（レッドロフ）等、感染したWebページを閲覧させることによりウイルスに感染させる手法は過去にもありました。

2009年以降、企業や組織等のWebページが改ざんを受け、そのホームページを見ただけでウイルス（Gumblar：ガンブラー）に感染する被害が発生したのは、悪意のあるJavaScriptやVB Script等のコードを埋め込んだりiframeタグ（§3-13参照）等で別のサイトに誘導し、マルウェアをダウンロードさせるという手法によるものです。




いつもチェックしているサイトでも、一見気付かれないような形でウイルスや不正タグを挿入されていたため、閲覧の際に被害に遭った、ということも多かったようです。

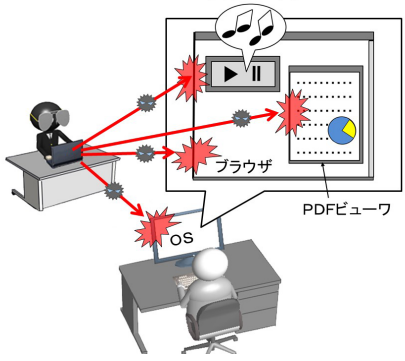
もっと限定的な閲覧者に対してウイルス等を感染させたい場合には、このようなサイトも限定して仕掛けを施すことになり、「水飲み場型攻撃（Watering Hole Attack）」と呼ばれています（§3-21参照）。

### ◆「動画を見ただけでウイルスに感染！」～OS以外のソフトの更新も必要

OSやブラウザ以外のプログラムも攻撃対象となります。音楽や動画等が掲示されているサイトでは、自動的にこれらのコンテンツをダウンロードさせて演奏（再生）させるようにしているかもしれません。

2020年末にAdobeのFlash Playerのサポートが終了し、最近ではFlashが稼働しないサイト・ブラウザがほとんどですが、動画・音楽再生プレイヤーやPDF（Portable Document Format）文書のリーダー等のプログラムに潜む脆弱性により、このようなWebページを閲覧した人が知らない間にマルウェアに感染してしまう可能性もあります。

ダウンロードした動画ファイルを開いて感染する場合や、Webの動画等を視聴している際に、表示されたアプリや偽広告をクリックしてマルウェアをダウンロードしたりインストールしてしまうこともあります。




動画や音楽等の再生・表示アプリもOSやブラウザと同様、常に最新の状態にアップデートしておく必要がありますが、そもそも職場のパソコン端末等の場合には、動画再生専用のアプリケーションソフトをインストールする必要が無ければインストールできないように設定する等の対策が必要となります。

# §3-12　マルウェアの危険性

ウイルスやワームを総称して「マルウェア」と呼んでいるのか？　どのような種類があるのだろうか？　その区別と危険性は？

## ◆種類

マルウェアは「悪意のあるソフトウェア（malicious software）」の意味で、有害、悪質、迷惑なプログラムを指しています。コンピュータ・ウイルスの他、ワーム、スパイウェア等も含まれます。また犯罪行為を目的とするマルウェアはクライムウェア（Crimeware）と呼ばれることもあります。

マルウェアは種々のコンピュータ言語で作成されているプログラムで、一見して「中身がわかる」訳ではありませんし、スクリプト言語で作成されたものも暗号化や難読化を行い、セキュリティ対策ソフトによる検出を逃れ、対策を無効化しようとします。マルウェアを広義の“ウイルス”と呼ぶ場合もありますが、次のように分類されることも多いようです（各種機能を兼ね備えていることも多く、ウイルス対策ベンダーによっては、同じウイルスをワームに区分することも多いし、ボット系ウイルス等と呼んだりもする）。

▶狭義のウイルス：　ファイルに感染（寄生）して、自己複製（感染拡大）を行う。

▶ワーム：　ファイルに感染（寄生）しないが自己複製（感染拡大）機能を有する、独立して実行可能なもの。

▶トロイの木馬：　自己複製（感染拡大）機能を有さず、ユーザの同意が無いままシステムに侵入するもの。一見有用なプログラムに見せかけてユーザを騙し、システムに侵入する独立プログラム。システム機能を阻害したり外部からの侵入口（バックドア）を開設する。このため、バックドアやRAT（Remote Administration Tool）とも呼ばれる（ネズミのようにコソコソ活動する、という意味を持たせている人もいる）。

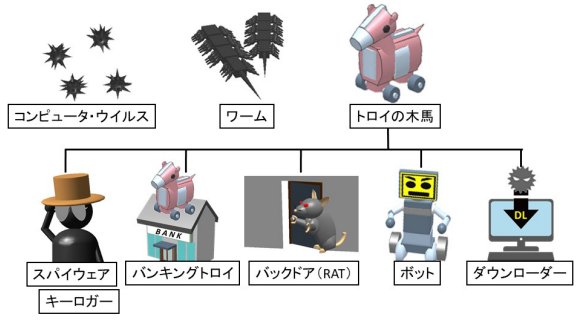
　ネットバンキングの不正送金事案に使用されるものはバンキングトロイと呼ばれる。

▶スパイウェア：　トロイの木馬の内、情報収集が目的のもの。

▶ボット：　外部から当該コンピュータを操作するために送り込まれたもので、指示に従った動作（攻撃や情報収集等）を行う。ドローンウェア等とも呼ばれる。

▶アドウェア：　好ましくない広告を勝手に表示。システムのリソースを消費する。

▶ダウンローダー（ドロッパー、トリックラー）：　利用者の了解なく他のプログラムのダウンロードやプログラムの更新を行うもの。ダウンローダーにより攻撃者が用意したサーバ等から順次取り込まれるマルウェアはシーケンシャル（多段型）マルウェアと呼ばれることもある。



▶キーロガー（スヌープウェア）：　ユーザの行動監視、個人情報やキーボード入力情報の搾取を行う。

**◆増加傾向にあるマルウェア**


また最近では、次のようなマルウェアも登場し、増加しています。

▶ランサムウェア：　画面やファイル、ハードディスク等をロック（暗号化）し、アンロックするためには仮想通貨等の支払いを行うよう警告メッセージを表示させるもの（支払ってもアンロックされない場合もある）。

▶コインマイナー：　パソコンやスマートフォンのリソースを勝手に利用して、仮想通貨の掘削（発掘）に悪用するもの。

▶ルートキット、ブートキット、ハイジャッカー：　システムの中枢や起動部（ブートセクタ）等に感染し、システムを乗っ取るもの。侵入後、遠隔操作等に必要なツール類をひとまとめにしたものをルートキットと呼ぶことも多い。

この他、コンピュータペスト、パラサイトウェア等、病原菌と同じような呼び方をされるもの、「ウイルスに感染した！」と表示し偽ウイルス対策ソフトのインストールを強要するもの（ローグウェアやスケアウェア）、レトロスピー（Retrospy）のように検出プログラムによる検知を妨害したり攻撃するものもあります。

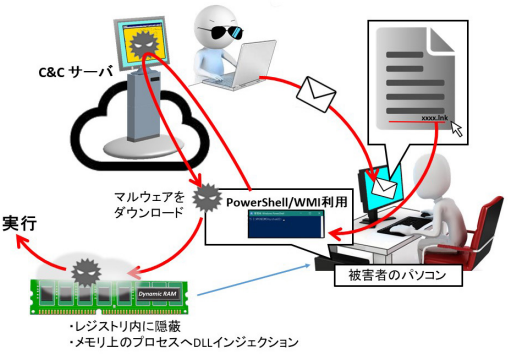
データやファイルを破壊しログを削除する破壊型のマルウェアはワイパー（Wiper）と呼ばれます。本来はコンピュータの動作や機能を向上・支援するための正規のソフトウェアである、BHO（ブラウザ・ヘルパー・オブジェクト）等の中には、そのコンピュータの情報を搾取したり改変するため、トロイの木馬（スパイウェア）として扱われるものもあります。

広告関係のアドウェア等の迷惑アプリ、スクリプトやインラインフレーム（iframe）タグ等は、PUA（Potentially Unwanted Application）と呼ばれることがあります。

**○ファイルレスマルウェア**

トロイの木馬がウイルスやワームと異なるのは増殖機能を持たない、ということですが、ウイルスやワーム、トロイ自体は「ファイル」という実体を持っています。

ところが、実行ファイルを用いることなく、メモリ上にのみ展開するマルウェアが最近増加しています。ファイルとしての実体を持たないため、セキュリティ対策ソフトでは検出できず、再起動すれば、痕跡も消えることがあるので厄介なマルウェアです。



# §4-4　P マークだけじゃダメ？ GDPR の施行！～個人情報保護対策

「P マーク」は取得してるよ！　という企業も多いかもしれないが、個人情報保護対策はそれだけでは十分とは言えない。では GDPRって何？

## ◆個人情報保護制度の動向

### ○個人情報保護関連の法制度

#### ⑴　個人情報保護法

「プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD 理事会勧告（プライバシー・ガイドライン：1980年）」を受けて、行政機関を対象とした法律（行政機関の保有する個人情報の保護に関する法律）と並び、民間事業者において個人情報を取り扱う際の保護規定として2003年に「個人情報の保護に関する法律（個人情報保護法）」として制定されたものです。

民間事業者には、この個人情報保護法だけでなく、様々なガイドラインや規格を順守することが求められています。

#### ⑵　JIS Q15001（PMS）

我が国では、諸外国に先駆け、PMS（Personal information protection Management System）として JIS 規格化（1999年）が行われています。これが JIS Q15001（個人情報保護に関するマネジメントシステム－要求事項）で、「個人情報保護管理者」の選任や事業者が備えるべき個人情報保護管理システムの整備に関して規定されています。

プライバシーマーク（P マーク）は、この JIS Q15001の要求事項を満足している事業者が認証された際に使用できる“証”です。しかしプライバシーマークを取得しているからといって、情報漏えい等が絶無である、ということを証明するものではありません。実際、大手企業を含め、P マークを取得した企業でも大量の個人情報事案が発生していることが公表されています。

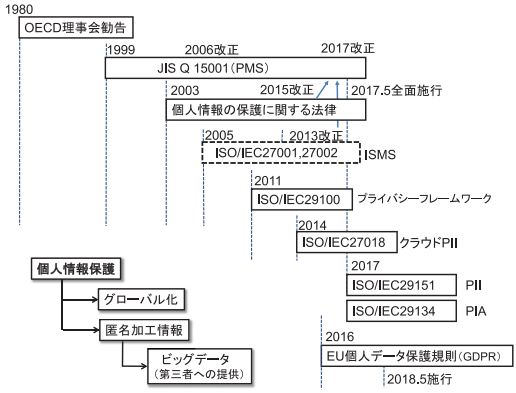
#### ⑶　個人情報保護法や JIS Q15001の改正

企業活動の海外展開にあわせて、個人情報管理のグローバル化も必要となっています。個人情報を取り扱うクラウド事業者（CSP 等）も増加し、さらにその個人情報を匿名加工化することによりビッグデータとして活用・流通するニーズも増大しています。

このため、2015年に個人情報保護法を改正し、個人情報の定義の明確化、匿名加工情報に関する加工方法や取扱い等の規定の整備を行うと共に、第三者に提供する場合の確認・記録作成義務等トレーサビリティの確保、個人情報保護委員会の新設やその権限に関する規定の整備を行っています。

たとえば「個人情報」に関しては、

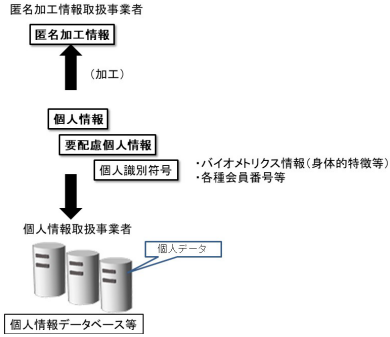
▶個人情報：　生存する個人に関する情報で、氏名、生年月日等、特定の個人を識別できるもの。



▶個人識別符号：　＊特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した、文字、番号、記号その他の符号（DNA、顔認証、指掌紋、静脈認証、虹彩（アイリス）、歩容データ等）であって特定の個人を識別できるもの。

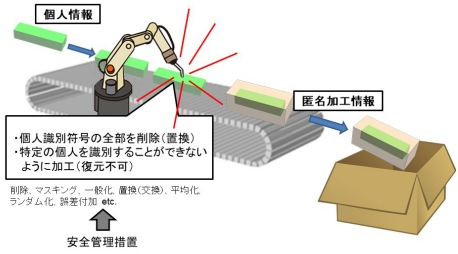
＊顧客等の個人に割り当てられる会員番号や会員カード等に記載されて利用者等を識別できるもの。

▶要配慮個人情報：　本人の人種、信条、社会的身分、病歴、犯歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述（心身の機能の障害、健康診断等の結果、刑事事件の被疑者・被告人等）が含まれる個人情報。




等の規定が行われています。

また、匿名加工情報については、個人識別符号の削除等の規定された措置を講じることにより「特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたもの」と定義されています。




この個人情報保護法の改正にあわせ、JIS Q15001も2017年に大幅に改正し、個人情報の定義等について個人情報保護法との整合性を図り、また2013年に改正されたISMS 関連の国際標準（ISO/IEC 27001、27002）の規定に準じて、リスクアセスメントにおいて残留リスクの把握・管理が必須とされています。

ただ、JIS Q15001においては、「個人情報」の定義として、個人情報保護法では生存する個人の情報が前提でしたが、JIS Q15001では「個人に関する情報で、特定の個人を識別できるもの」とあり、生死は問わない、ということに留意する必要があります。

### ⑷　仮名加工情報、個人関連情報～個人情報保護法の改正（2020年）

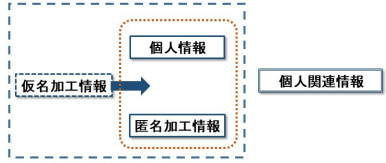
2020年に改正された個人情報保護法では、個人情報と匿名加工情報の中間に位置づけられるものとして、他の情報と照合しない場合には特定の個人を識別することができないよう加工した情報である仮名加工情報が規定されました。

また「生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないもの」として個人関連情報が位置づけされています。

いずれも、データ利活用に関する施策の一環として、デジタル流通を促進する観点から規定されたもので、2022年４月に施行されましたが、確実な個人情報保護を行うために、罰則も強化されています。

**〈2020年の改正内容〉**

2020年の改正（2022年４月施行）では、①本人の請求権の拡大（不適正な利用がなされた際に利用



# §4-16　PPAP なぜ禁止？

2020年秋に、政府機関では「PPAP 使用禁止」を発表し、追随する企業等も多い。
PPAP の問題点等は？

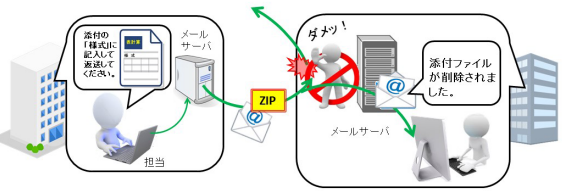
## ◆ PPAP とは？


「PPAP」は、①P：Password 付の Zip ファイルを送付、②P：Password を送付、③A：暗号化（Angou）した、④P：Protocol（プロトコル）の頭文字を続けたものですが、国内ではメール送付時に添付ドキュメントがある場合に、その添付ファイルをパスワード付 Zip ファイルとすることにより、盗聴防止等を図っていたものです。

## ◆ PPAP の廃止

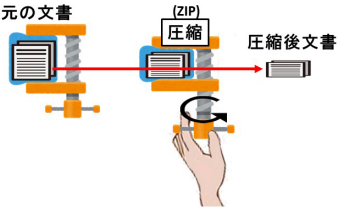
2020年11月以降、政府機関では「メールでパスワード付きファイルを送り、パスワードを別送する方法（いわゆる PPAP 方式）」については「廃止」されることになりました。

中央官庁だけでなく、プロバイダや企業の中にも、外部から受信したパスワード付きの Zip ファイルを受信時にメールサーバで自動的に削除するように変更した組織が増加しています。




メール誤送信防止のために、自動的にパスワード付き Zip ファイルにして送信する、という手法を取っていた組織では一部混乱が生じたようですが、リスク軽減のために次第に容認されるようになりました。

## ◆ PPAP の危険性



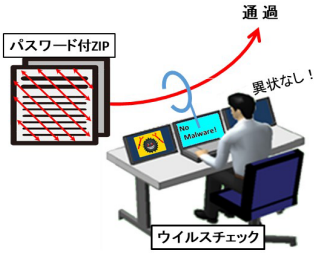

そもそも Zip は、ファイルサイズを圧縮したり、複数ファイルを単一アーカイブ（書庫）としてまとめるために使用するツールです。

圧縮ツールには Zip 以外にも多様な種類（LHA、RAR 等）がありますが、パスワードを簡単に設定できる、という点で Zip は便利です。

パスワードを設定しておくと、もしファイルを他人に誤送信した場合でも、解凍できない（パスワードが判らなければ内容が読み取れない）ため、情報保護（誤送信防止対策）の観点でも利用されてきました。

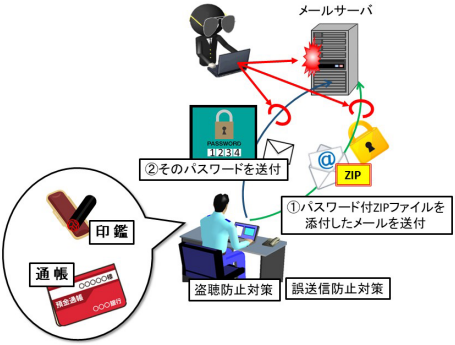
半面、簡単とはいえ、一種の暗号化を行っていますので、「パターンマッチング」

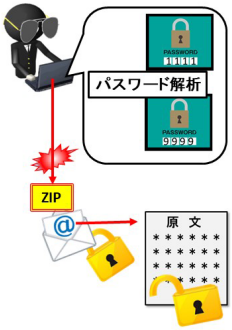
方式のマルウェア対策ソフトをすり抜けてしまう、という懸念もあります（通常は、圧縮した状態での検出が可能だったり、振る舞い検知と共に使用されるので、組み込まれたマルウェアが全て通過する訳ではありません）。




また、暗号化により盗聴防止対策にもなる、というのも利用されてきた大きな理由ですが、携帯電話等、別の通信路を用いて「パスワード」を送信するならよいのでしょうが、同一通信路で送付することは無意味です（「通帳」と「印鑑」を同一場所に保管しておくようなものだ、と喩えることもあるようです）。

「PPAP は誤送信防止に役立っている」、という人もいます。パスワードが判らなければ間違った宛先に送付してもファイルの中身を見ることはできないので安全、と思われがちです。




しかし、パスワードが判らなくても、総当たり方式や、辞書式等の攻撃手法によりパスワードを解析してしまうツールも、ネット上で出回っています。パスワード Zip 化しても、そのファイル自体が奪取された場合には、パスワードがなくても時間をかければ復号は可能なので、セキュリティの面から言えば、手間をかける割には、セキュリティ確保にはつながっていないことになります。

### ◆マルウェア（Emotet）の感染拡大

2020年秋頃に登場した情報窃取に用いられるマルウェアの Emotet（エモテット）は、メールに添付されて感染が拡大するものです。

「新型コロナウイルス」をタイトルに付したり、メール返信を装って「RE：」を付して業務に関連した題材を入れて返信する形を取っているものが多いようです。

Zip 化することによりマルウェア検知を逃れる、ということも PPAP 廃止の判断につながっているようです。

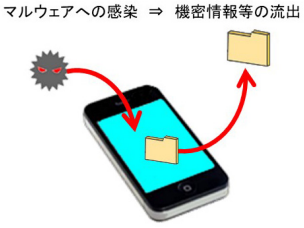
### ◆ PPAP の代替手法

文書のセキュリティ確保（暗号を破られない）と誤送信防止（別の相手に送付しない）の観点から、Zip 以外の高度な暗号により文書を暗号化して、ファイル交換サービスやオンライン・ストレージを使用する等、多様な手法やサービスが提供されていますので、適切な利用を行うことが望まれます。

# §6-1　職場の PC や端末の管理は？

端末等はウイルス対策をしっかりやっていればよいのではなかろうか？

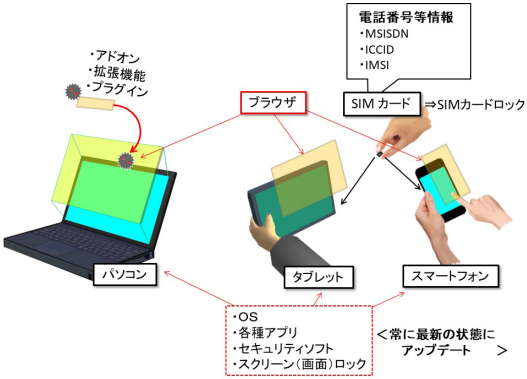
## ◆マルウェア対策




パソコンやスマートフォンのセキュリティ対策といえばウイルス対策？　と思う人が多いのではないでしょうか。確かにマルウェア感染が原因となる個人情報や機密情報の流出事件が後を絶たない、ということから、マルウェア対策をしっかりやれば情報等が流出することはない、と思われるかもしれません。

しかし特定の組織や人を狙って様々な手法により侵入を試みる標的型攻撃等も増加していて、マルウェアの侵入を未然に阻止することは非常に難しい上に、マルウェア以外の手段でも情報流出は発生しています。

### ○更新（アップデート）




パソコンのみならずタブレットやスマートフォンにも共通する対策としては、マルウェア対策ソフト等の定義ファイル（パターンファイル）を更新するだけでなく、Windows や Android、iOS 等のオペレーティングシステム、各種アプリを常に最新の状態に更新する必要があるということです。

利用者が勝手に職場の端末 PC に好きなソフト（アプリケーション）をインストールする、ということを防止するためには、平素の情報セキュリティ教養や指導が重要なのですが、物理的にも、このようなことができないよう、グループポリシーによる制限（ソフトウェア制限ポリシー：SRP（Software Restriction Policies））等を行い、WSUS サーバ（§4-9参照）を利用してソフトウェアのアップデートを的確に行っている組織も多いかもしれません。

たとえば、インターネットに接続された端末において、特定のブラウザしか利用できないようにしている組織も多いかもしれません。しかし、ブラウザに追加的に組み込んで使用するアドオン、拡張機能、プラグイン等と呼ばれていて、利用者の趣味嗜好等に応じて動画の視聴やダウンロード等が便利にできるようになる様々なソフトウェアについても、管理者側でクラス ID（CLSID）等によりグループポリシーを設定しておかなければ、勝手にインストールされてしまうかもしれません。このようなアドオン等の中には、古く更新されないまま放置されているものも多く、その中にマルウェアに汚染されたり、脆弱性を有していたり、セキュリティ・ホールが新たに見つ

かったようなものがあれば、マルウェア等に感染する危険性があります。

また、マルウェア対策ソフトやOS等のアップデートを行った場合、再起動しなければ更新が反映されないこともありますので、職場の端末等は、終業時、帰宅する前にきちんとパソコンのシャットダウンを行うよう、職員・社員に周知する必要があります。


面倒だから、とディスプレイをバタンと閉じて、スリープ（サスペンド）状態としただけで帰宅する職員等がいないか、情報セキュリティ担当者は注意しましょう。

特に、一旦蓋を閉じた端末のディスプレイを再び開けた際に、再ログインしなくても蓋を閉じる前の状態に復帰し、業務を再開できるような設定だったりすると、職員等が帰宅した後、勝手にデータやパスワード等が盗み出されてしまうかもしれません。


### ○アプリ導入時の留意点

個人所有機器を業務でも利用するBYOD（§6-9）を認めている場合には、その機器自体の安全性を確保する必要があります。


Google Play や App Store のような正規（公式）マーケット（ストア）以外のサイト等で配布されるアプリ（野良アプリ）の安全性は保証されたものではありませんし、正規ストアに登録されているアプリの中にも、トロイの木馬等のマルウェアやアドウェアが混入している可能性がありますので、信頼できるアプリかどうか、評価等を参照しつつ、必要最小限のアプリをインストールする必要があります。

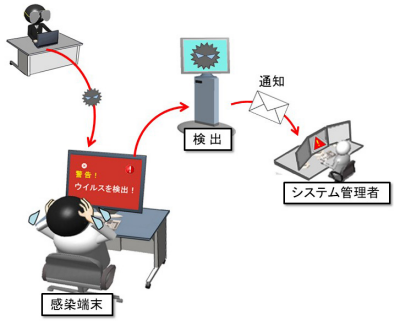
また、説明書きが外国語でのみ記載されているアプリでは、どの程度、スマートフォンの各種データにアクセスするのかが分かりにくいかもしれませんが、十分「アクセス許可」の範囲については確認する必要があります。たとえば最寄りの飲食店等を探し出すためのアプリであれば、位置情報へのアクセスは当然必要ではありますが、それ以外の個人情報等へのアクセスは果たして必要なのだろうか？　等、よく吟味した上で導入を図ることが重要です。特に**管理者権限**をこれらのアプリに与えてしまえば、利用者であってもアプリの削除が行えなくなったり、端末自体が乗っ取られてしまう恐れがあり危険です。

パソコンでも、たとえばWindows 10であれば、「設定」⇒「プライバシー」から位置情報やアカウント情報等にアクセス可能なアプリの設定を行うことができます（Windows 11の場合は「設定」⇒「プライバシーとセキュリティ」⇒「アプリのアクセス許可」から位置情報等へのアクセス可否の設定が可能です）。

## §6-5 「ウイルスが検出されました！」と表示されたら？

**「ウイルスを検出！」**という表示を見れば、パニック状態に陥ることにならないか？
冷静に対処するには、どのような点に留意すればよいのだろうか？

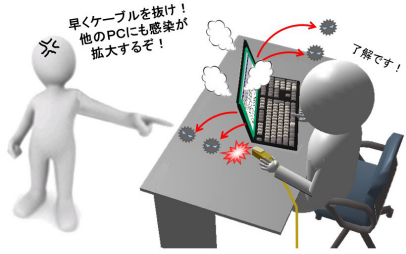
### ◆偽セキュリティソフト




§3-8で説明しましたが「直ちに削除（修復）！」等と表示されてボタンを押させようとしたり、「○○まで電話を！」と表示されるような場合に迂闊にクリックしたり電話をすることは避けなければなりません。もしクリックしてしまうと、マルウェア等のダウンロードやインストール、あるいは悪質なサイトのURLへ誘導され効果なソフトウェアの購入を勧められる危険性があります。

職場の端末であれば、直ちに部内のシステム管理者に連絡し、その指示に従うこと（セキュリティソフトにもよりますが、マルウェアに感染した場合には、そのソフトによる警告と同時にシステム管理者に通報され、システム管理者から連絡が行われることもあります）。

### ○ケーブルは抜く？

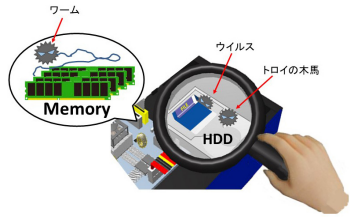



以前は、ワーム等に感染したことが判明したならば、職場中の端末にネットワーク経由で感染が拡大することを阻止するために、「直ちにLANケーブルを抜く！」ことが必要、と言われていたこともありました。

これも、組織のセキュリティ対策システムにより違いがありますが、マルウェア感染を検知した場合には、即座に自動遮断を行う機能を有しているものも多いし、Wi-Fi接続で利用している際には、LANケーブルの抜き差しを行うことに意味はありません。第一、気がついた時にケーブルを手で抜いても、その時は既に他の端末にも感染してますよね。

あらかじめ、職場におけるマルウェア感染時に、職員やセキュリティ管理担当者が、どのような対処を行う必要があるのか、規定をよく理解しておく必要があります。

### ◆マルウェア対策ソフトの動き



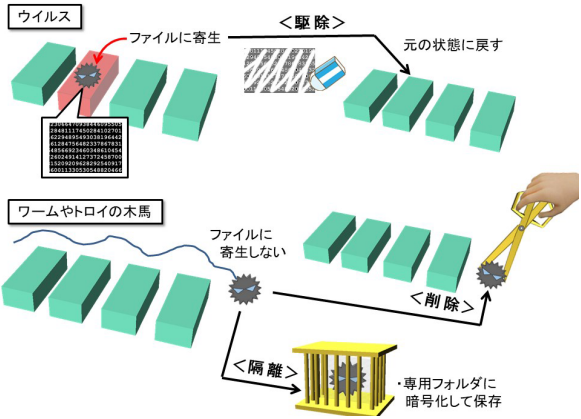

ウイルスはファイルに感染しますが、ワームやトロイの木馬は独立して動作します。ワームの動作はメモリ上で行われ、拡散活動を展開してゆきます。

マルウェアの中には、レジストリを変更したりOSの正規プログラムを乗っ取るものもあります。

これに対するマルウェア対策ソフトの「駆除」や「削除」、「隔離」等の機能は、似ているようでベンダ

ーによって違いもありますので注意が必要です。

基本的には、「駆除」はファイルに感染したウイルス部分を取り除いて、ファイルを元の正常な状態に戻すこと、「削除」はハードディスク上から文字通り削除すること、「隔離」は専用フォルダの中に、暗号化して無害化することにより、動作・実行されることがないようにすることを指すことが多く、隔離されたマルウェアは削除することが可能となりますが、削除しないと別のセキュリティソフトに入れ替えた場合には検出されてしまうことがあります。




個人でも、コンピュータ・ウイルスを溜め込んでいると、「不正指令電磁的記録保管」等に問われる可能性がありますので注意しましょう（私も随分昔（このような法の規定ができる前）に、そのままマルウェア検体を送付しようとして、受信側のセキュリティ対策ソフトで削除されてしまって焦った経験があります。マルウェアを徒に取り扱うことは危険ですね）。

### ◆修復

マルウェア感染によりコンピュータの、SSD／HDD が破壊される、OS が起動しない、そもそも BIOS が起動しない等、様々な被害が発生する場合もあれば、明確な症状が出ない場合もあります。

システムが起動しない、等の症状が出れば、システム管理者に連絡し修復・修理を行うことが可能ですが、症状が出なくとも、情報の流出が発生したりバックドアが設置され他システムへの踏み台に悪用されることもあります。

このため、一定の時刻にスケジュール・スキャンが行われるよう設定されていることも多いのですが、その時刻に電源がオン状態でなければスキャンは行われません。

このため端末の電源が投入された直後等にスキャンを行うよう設定されていることも多いのですが、このような場合には若干端末 PC 等の起動直後の動作が緩慢に思えることもありますが、セキュリティ確保のためイライラせず我慢することも重要でしょう。

マルウェア対策ソフトにリアルタイム保護機能がある場合には、「ウイルス検出」等が表示されても、その時には侵入は阻止（削除、隔離）できていることから安心してよいのですが、念のため定義パターンを最新のものにしてディスク全体のスキャンを行い、感染状態を確認することが適当でしょう。

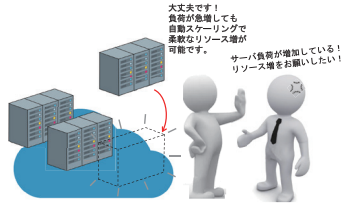
# §8-5　クラウドネイティブ、ゼロトラスト

クラウド利用の進展により「クラウドネイティブ」という言葉もよく聞かれるようになった。また「ゼロトラスト」の考え方も一般的になりつつあるようだが、これらの関係は？

## ◆クラウドネイティブ


私なぞは英語が得意ではないためか「ネイティブ」といえば、ネイティブスピーカーのことを想像してしまいがちですが、クラウドネイティブというと、クラウド、特にパブリッククラウドが持つ固有の機能を指します。

固有の機能は様々ですが、特に業務継続を確保するための機能が充実しています。障害が発生した際には自動修復、あるいは負荷が急増した際には柔軟にサーバ機能を増強し、ネットワークやストレージ容量を増大する等、クラウドの能力を十二分に引き出すことにより達成することができます。




これを実現するために、コンテナやサービスメッシュ、マイクロサービス、イミュータブルインフラストラクチャ等が利用されるようになっていますが、これらの機能がクラウドネイティブと呼ばれています。

また前項でゼロトラストへの移行について説明しましたが、ゼロトラストを実現するためのシステムを開発・整備するには、クラウドの利点を最大限に活用できるよう、システム構築に関する考え方も変化してきていて、その手法はZTA（Zero Trust Architecture）と呼ばれています。

## ◆オブザーバビリティ（可観測性）

### ○ DevOps、DevSecOps から AIOps へ

クラウドの性能を遺憾なく発揮させるためには、コンテナ等のクラウドネイティブの機能・ソフトウェアを開発する段階から、運用時のことを想定して運用担当者と連携してスピーディーにシステムを開発するDevOps、さらにはセキュリティ確保も加味したDevSecOps（§3-6参照）を備えておく必要があります。

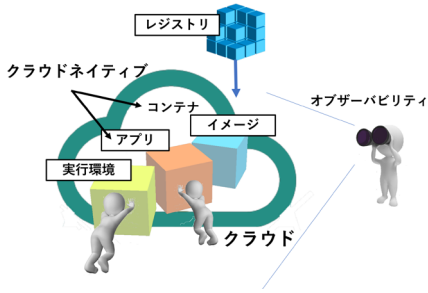
その際に重要となるのが、複雑なシステムで問題が発生した場合に、如何に迅速に検出して対処できるのか、ということが鍵となります。このため、DevOpsと同様、AIOps（Artificial Intelligence for IT Operations）と呼ばれる、ITシステムの運用管理にAI技術を適用して業務の効率化・自動化、効率化を図る手法も発展しています。

### ○状態監視・モニタリングの重要性

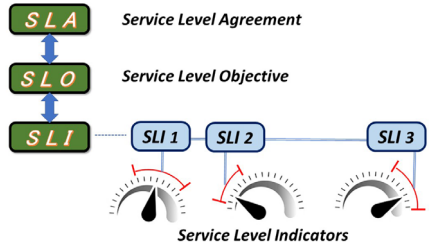
迅速な対処を行うには、障害やイベント等を的確に検出する必要がありますが、そ

のためには、常にシステムの状態を監視・モニタリングすることが求められます。

クラウドシステムの開発では、レジストリのイメージをローカル環境にダウンロード（プル）して、アプリの実行環境を整備し、クラウド上に展開（デプロイ）する過程や、そのコンテナ等の運用状況も定常的にモニタリングすることが求められます。

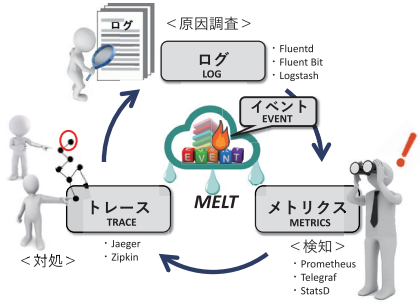



これを「オブザーバビリティ（可観測性）」と呼んでいて、APM（Application Performance Monitoring）や EUM（End User Monitoring）等のモニタリング用ツールが利用されています。またシステム全体の信頼性や効率性を向上させるための SRE（Site Reliability Engineering：サイト信頼性エンジニアリング）チームを置く組織も増加しています。SRE チームでは、サービスレベル契約（SLA）を基本に、サービスレベル目標（SLO）や、その具体的な指標となるシステムの許容された遅延時間や可用性等の信頼性に関する指標、サービスレベルインジケータ（SLO）を監視して運用管理を行います。




SRE の実践に際しては、Toil（労苦～反復して行う手作業）を抽出し、自動化等を行うことにより除去することが求められます。


また監視・観測に関しては、「オブザーバビリティ（Observability）」を実現する基本的な要素として MELT（Metrics、Event、Log、Trace の頭文字をつなげたもの）を取り上げることもあり、課題や問題点を迅速に抽出し解決するツールとして期待されています。




### ○イミュータブル～変えない

迅速に設計変更を反映したシステムをクラウド上に実装（デプロイ）したり、セキュリティ対応等で修正パッチを当てる等の作業を稼働中のシステムに対して実施することは、障害発生、サービス停止のリスクを伴います。

このため、稼働中のサーバ等に修正作業等を行わず、新しく構築したサーバに入れ替える、という、いわば IT インフラの使い捨て（Immutable Infrastructure）の考え方が、Docker コンテナの利用が進むにつれ一般的になってきました。