用語集

AES（エー・イー・エス）
暗号化方式の一要素。利用する無線LANの暗号化方式にAESという文字が入っている、WPA-PSK(AES)やWPA2-PSK(AES)という方式は、「暗号キー」を共有しない範囲では安全とされる。また無線LANに限らずファイルやディスクの暗号化方式としても用いられ、数字＋bitで記述される「鍵長」の数字が大きいほど、不正な解読が困難とされる

BIOSパスワード（バイオス・パスワード）
Windowsマシンなどで電源投入時に、OSが立ち上がる前に求められるパスワード

DDoS攻撃（ディードスこうげき）
Distributed Denial of Service Attack。攻撃者などがゾンビ化した多量のパソコンなどから攻撃目標に一斉に多量の問合せなどを行い、攻撃対象の反応が追いつかず利用できない状況にする攻撃。何種類かの類型がある

ECサイト（イーシー・サイト）
Electronic Commerceサイト。インターネット上にある商品販売店舗

EV-SSL証明書
（イーブイ・エスエスエルしょうめいしょ）
Extended Validation証明書。従来のSSL証明書に対して、審査を厳格に行った証明書。証明書を取得した会社名が表示されるため、詐欺サイトではないか、簡単に確認することができる

GPS（ジー・ピー・エス）
Global Positioning System。多数の人工衛星で構成される衛星測位システム。この衛星からの電波を使い計算を行うことで、現在地を測定することができる。主として米国が運用しているが、2018年春より日本版GPS「みちびき」が運用予定

ID（アイ・デイー）
機器やウェブサービスなどを利用する時に、利用者を識別する名称。「ログインパスワード」とセットで、正統な利用者であることを証明する

IMAP（アイマップ）
Internet Message Access Protocol。メールサーバからメールを受信するための通信上のお約束（方法）。POPと異なるのは、メールがサーバ上にメールを残した状態で管理できるので、ウェブブラウザがあればどこからでもアクセス出来るウェブメールなどで使われることが多い。メールソフトでも利用可能。通常はVer.4のIMAP4が使われる

IoT（アイ・オー・ティー）
Internet of Things.。「物のインターネット」とも言われるが、何でもかんでもネットにつなげてしまおうというイメージの考え方。しかし、製造する業者が全てネットワークセキュリティに詳しいとは限らず、攻撃者から見て踏み台にしやすい機器を増やす原因ともなっている

JailBreak（ジェイルブレイク）
AppleのiPhone、iPadなどで規約に反した改造を行い、公式ストアでは認められていないアプリなどをインストールする行為。製造メーカーが設計したセキュリティ思想から逸脱するため、マルウェアへの感染や乗っ取りなどの攻撃に遭う確率が高くなるため、大変危険な行為。やっちゃだめ、絶対

Linux（リナックス）
Windows、macOSとも別の、基本的には「みんなで作る無料のOS」。一般の人も利用可能だが、サーバや工業機器やIoTなど、あまりコンピュータであることを意識しない電子機器でよく使われている。様々な種類のLinuxが存在する他、私たちが普段使っている著名なOSの元になっている場合もある

LTE（エル・ティー・イー）
Long Term Evolution。携帯電話の最近の通信規格。携帯電話回線を提供する会社が個別に名称をつけている場合もあるが、主に４Ｇと呼ばれるタイプのものの総称。高速な無線通信回線ネットワークとしてWANと呼ばれることもある

microSD（マイクロエスディー）
パソコンやスマホなどで使われる、小型のメモリカード。SDカードの超小型版

NISC（ニスク）
National center of Incident readiness and Strategy for Cybersecurity。内閣官房内閣サイバーセキュリティセンターの略称　→内閣サイバーセキュリティセンター。内閣府ではない。

Office製品（オフィスせいひん）
Microsoft Officeなどに代表される、ワープロ、表計算、プレゼン用ソフトなどの総称。

OpenID（オープン・アイ・ディー）
→ソーシャルログイン

OS（オー・エス）
Operating System。
→オペレーティングシステム

「PINコード」（ピンコード）
狭い意味ではスマホなどを利用する時に打ち込む、暗証番号のようなもの。複数回入力を間違うと明示的な入力遅延や入力画面がロックされるなどの規制がかかるものを指す。間違えすぎると強制的にデータを消去する「ワイプ」機能があるものも。本書では機器やサービス利用時に、4〜6桁程度の数字で打ち込むものとして定義

POP（ポップ）
Post Office Protocol。メールサーバからメールを受信するための通信上の規約。IMAPと異なり、基本的にはメールをメールサーバからダウンロードして管理する。ただし、メールソフトの側で「メールサーバ」に残すという設定をした場合は、複数のメールソフトからダウンロードすることも可能。通常はVer.3のPOP3が使われる

POSレジ（ポスレジ）
Point of Salesレジ。販売した段階でその情報が送信され、集中管理されるシステム。内部にはコンピュータが入っており、ネットに接続されているのでマルウェアに感染する事例もある。IoT機器

RMT（リアル・マネー・トレード）
Real Money Trade。ゲームなどで出現したレアな装備を、現実世界の通貨で売買すること。ゲームの規約違反となっていることもある。また販売に関して詐欺や様々なトラブルの発生もしている。レア武器は自力で出しましょう

root化（ルートか）
Androidスマホなどで本来提供されていない、機器の管理者権限を奪取する改造。通常インストール出来ないアプリなどがイントール可能となる。これを行う事はメーカー本来のセキュリティ設計思想を逸脱しサイバー攻撃に弱くなるため、行ってはいけない

SIM（シム）
スマホなどで携帯電話回線を利用するために挿入する小型のカード。電子的なeSIMもある。

SIM認証（シムにんしょう）
公衆無線LANなどで、「暗号キー」を他人と共用しないように、それぞれの利用者によって異なるSIMの情報を使って認証を行う方式

SIMフリー（シムフリー）
スマホなどの端末が、特定の携帯電話会社のSIMだけでなく、どの会社のSIMでも利用できるようになっている状態。使えないように制限されている状態はSIMロックと言う。ただし、SIMフリー端末であっても、どの会社の回線でも利用可能とは限らない。携帯電話会社が提供している周波数とスマホが使える周波数が合っている必要がある。

SMS（ショートメッセージ）
スマホなどで電話番号宛てで送受信できるメッセージ。携帯電話回線契約があればデータ通信契約が無い状態でも送受信出来る。一方、電話番号が無い場合や、データ通信専用SIMでSMSが提供されていない契約では送受信出来ない。SMSがオプションとして提供されている場合もある

SNS（エス・エヌ・エス）
Social Networking Service。会員制のサービスで、メッセージのやりとりやブログ風の発信などを行う。アカウントを作らないと閲覧できないものと、アカウントがなくてもウェブブラウザから閲覧できるものなど、様々な形態がある

SSD（エスエスディー）
Solid State Drive。従来パソコンなどで用いられてきた大容量ディスクであるハードディスク(HDD)に代わり、回転や可動部分がなく、電子的なメモリだけでこれを代替する機器。HDDより小容量で比較的高価だが高速

SSL（エス・エス・エル）
→SSL/TLS

SSL/TLS
（エス・エス・エル／ティー・エル・エス）
Secure Socket Layer / Transport Layer Security。データを暗号化して送受信する方法で、SSLのほうが古く、これを改訂して進化させたものがTLS。SSLがTLSの元になったこともあり、未だにSSLと呼ばれたり、SSL/TLSと書かれたりするが、古い資料やバージョンを明記しているものを除けば同義の意味と考えて良い

SSL証明書
（エス・エス・エルしょうめいしょ）
SSLで通信を行うサーバの身分証明書のようなもの

Stuxnet（スタックスネット）
イランの核燃料施設を攻撃するために用いられたマルウェア。USBメモリを経由しエアギャップを越えて感染するように設計されている。攻撃するだけであれば、人の手を使いエアギャップを越えることは可能であることを示した例

TKIP（ティーキップ）
Temporal Key Integrity Protocol。暗号化方式の一つだが難しく考えないで、無線LANアクセスポイントの暗号化方式にこの文字が入っていたら、危険と考え利用を避ける

TLS（ティ・エル・エス）
→SSL/TLS

TPM（ティー・ピー・エム）
Trusted Platform Module。パソコンなどの内蔵ディスクの暗号化を加速するチップ。「暗号キー」を秘匿し、本体が盗難された場合でも解読を困難にする。内蔵ディスクだけが盗まれた場合は、TPMは本体に残るので「暗号キー」は秘匿され、当然解読が困難になる

UPnP
（ユニバーサル・プラグ・アンド・プレイ）
Universal Plug and Play。ルータに内蔵されている機能で、家や会社のLAN側にある機器を、難しい設定抜きでインターネット側からアクセス可能にする。LAN内の機器がインターネット側からアクセスされ、「踏み台」にされる事もあるので、利用しない方が安全

URL（ユー・アール・エル）
インターネットのウェブサイトの住所を示す文字列

USB（ユー・エス・ビー）
Universal Serial Bus。パソコンなどに周辺機器を簡単に接続する為の規格

USBキー（ユー・エス・ビー・キー）
USB端子に接続して、機器やサービスの正統な利用者である事を証明する物理的な鍵の役割を果たすもの

USBチャージャー（ユー・エス・ビー・チャージャー）
USB経由で機器を充電出来るようにするためのもの。AC電源、乾電池や充電池、車の電源ソケットを利用して充電できるものがある

VPN（ブイ・ピー・エヌ）
Virtual Private Network。仮想プライベートネットワーク。業務用としてはインターネットを利用しながらセキュリティを守りつつ、独立したネットワーク間をLANのように接続する。一般の利用者用には、自分の機器からインターネット上の安全とされる出口サーバまでの区間の通信をすべてまるっと暗号化する

WAN（ワン）
Wide Area Network。LANに対になる言葉で、広域な無線通信回線ネットワークを指す。LTE（4G）やWiMAXがこれに含まれる

WEP（ウェップ）
Wired Equivalent Privacy。暗号化方式の一つだが、容易に解読可能で安全ではない。無線LANアクセスポイントの暗号化方式にこの文字が入っていたら危険と考え利用を絶対に避ける

Wi-Fi（ワイ・ファイ）
→無線LAN

Wi-Fiルータ（ワイ・ファイ・ルータ）
→ルータ

WiMAX（ワイマックス）
高速な無線通信回線ネットワークの一つ。WANと呼ばれることも

WPA（ダブリュー・ピー・エー）
Wi-Fi Protected Access。無線LANの暗号化方式の一つで、WPA-PSK(AES)と書かれたもので、「暗号キー」を他人と共有しない限り安全。TKIPと入っていれば利用を避ける。公衆無線LANでこの方式を採用している場合は、「暗号キー」を他人と共有する場合もあるので注意

WPA2（ダブリュー・ピー・エー・ツー）
Wi-Fi Protected Access 2。WPAをより強力にしたもので、AESが標準となった。「暗号キー」を他人と共有しない範囲では安全とされている。もしTKIPと入っているものがあれば利用は避ける。公衆無線LANでこの方式を採用している場合、「暗号キー」を他人と共有する場合は危険

WPA3（ダブリュー・ピー・エー・スリー）
Wi-Fi Protected Access 3。WPA2で近年発見された特殊な脆弱性や、その他無線LANにまつわる問題点の多くを解消する暗号化方式。

アオリ行為
SNSやブログなどを使って、他人の発言を取り上げ、批判的なコメントをして「炎上」状態にしようとすること

アクセスポイント
無線LANで通信するために、使用している機器を接続する先、およびその機器

アクティベーションコード
ソフトウェアをインストールしたり、コンビニなどで売っている、音楽サービスやゲームなどへのチャージカードを、利用可能にするために用いる。認証処理をするために入力時にネットに接続されている必要がある場合もある。

アタッカー
→攻撃者

アップデート
セキュリティ改善要素が含まれているかどうかは関係なく、ソフトウェアやアプリの更新

アップデートファイル
アップデートを行うためのインストールファイル

アバター
ゲームやSNSなどで自分の代わりの役割を担うキャラクター。あるいは現実世界で代理をになうロボット

アプリ
パソコンやスマホなどで、何らかの機能を実現するプログラム。主にスマホで使われ、一部パソコンでも使われている名称

アプリ連携
複数のアプリ間で機能を連携する事。カメラアプリにSNSアプリの投稿機能を連携し、カメラアプリから直接写真付き投稿を行えるようにするなど。権限を渡すことになるので、攻撃者のサイバー攻撃の手口になるので利用非推奨

アンインストール
インストールしてあるプログラムやアプリを機器から削除すること

暗号化
文章などを正統な利用者以外が読めないように加工すること

暗号化キー
暗号化と復号のために利用する鍵となる文字列。短く複雑でない暗号化キーは総当たりによって探り当てられやすい。また何らかの理由で流出したり、意図せず共有すると、キーを入手したものによって暗号化した内容が復号される。本書では「暗号キー」という

暗号化チップ
暗号化をより高速に行う為の、専用のチップ。≒TPM

暗号化方式
暗号化の方式。一部の古い方式では「暗号キー」がなくても解読出来るものもある。暗号化するときには利用する暗号化方式の安全性に注意が必要

暗号化メディア
暗号化されたメディア。SSDやHDD、USBメモリなどのメディアを暗号化する

「暗号キー」
本書では暗号化と復号に使う鍵の名称として定義

アンダーカバー
潜入調査

インストール
プログラムやアプリを、スマホやパソコンに導入し、使える状態にすること

インターネットバンキング
インターネットを使って銀行の取引を行うサービス

インターフェース
パソコンやスマホを利用する為の操作画面や操作方法

ウイルス定義ファイル
セキュリティソフトがマルウェアを検出するためのファイル。実世界で言えば顔写真付きの手配書のようなもの

ウェブサーバ
ネット上でホームページを表示するためのサーバ

ウェブブラウザ
ネット上で公開されているウェブサーバを閲覧するためのソフトウェアやアプリ

オフラインアタック
攻撃者が暗号化されたデータなどを入手し、制限がない環境で解読攻撃を行うもの。主にネットに接続しないで出来る攻撃なので、オフラインという。＝オフライン攻撃

オペレーティングシステム
パソコンやスマホの機器の上で動作し、利用者に操作用のインターフェースを提供するソフトウェア。Windowsパソコンの Windows。Apple社パソコンの mac OS、Androidスマホの Android OS、iPhone/iPadの iOSなど

オレオレ証明書
本来認証局に申請して発行してもらう証明書を、勝手に発行し暗号化通信を行うために利用するもの。この証明書を利用しているウェブサイトにウェブブラウザでアクセスすると、警告が表示される。接続してはいけない

オンラインアタック
攻撃者がウェブサービスなどに、不正にログインを試みる攻撃など。ネットを経由した攻撃が主なのでオンラインという。＝オンライン攻撃

オンラインストレージ
ネット上に存在するデータ保管用のサーバ

ギブアンドテイク
ソーシャルエンジニアリングの手法で、相手に何かのメリットを与える事で、自分の目的の情報を引き出す手法

クラウドサーバ
インターネット上に存在する、データやアプリなどを保存しておくサーバ。主に「機器のディスクと同等に利用できる」「利用している意識はないが使っている」状態のものを指す。これに対して転送を意識して使用するものは「オンラインストレージ」と呼ばれやすい。スマホなどでは設定をよく確認しないと、知らないうちに、写真などのバックアップに使ってしまっていることもあるので注意

クラッキング
攻撃者が他者のアカウントや機器、サーバなどに不正に侵入すること。セキュリティを割って入るの「割る」の Crack から来ており、クラッキングを行う攻撃者をクラッカーとも呼ぶ

検体
セキュリティ会社などがセキュリティソフトでマルウェアを排除できるように、そのマルウェアを解析するための実物のサンプル

攻撃者
悪意を持ってサイバー攻撃やそれに付随する攻撃を行うもの。悪意のハッカー。ブラックハットハッカー。本書では「ハッカー」の語源が悪意があるかどうかとは関係が無いので、攻撃を行うものとして「攻撃者」とする。＝アタッカー。≒クラッカー

虹彩
目の中にある円盤状の膜で、人によって違っており、生体認証の要素として使われる

公衆無線 LAN
街中や店舗などで、不特定多数に対して インターネット接続環境を提供する無線 LAN のこと

サービス連携
パソコンなどを使って複数のウェブサービスの間で連携をすることをサービス連携と呼ぶ。その中で特にスマホ上でアプリによって連携をすることをアプリ連携と呼ぶ場合があるが、内容は同じ

辞書攻撃
「ログインパスワード」などによく使われる文字列を集めて辞書化したものを使い、不正に他人のアカウントにログイン出来ないかを試みる攻撃

侵入テスト
会社や組織のネットワークに、外部から不正侵入することが出来ないか行うテスト。ペネトレーションテストともいう

スタンドアロン
ネットワーク（繋がっていること）と対になって使われる言葉で、ネットワークに繋がっておらず単独で存在すること。ただし、ネットに繋がっていて、かつ他の機能や機器と連携しないで動作する場合もスタンドアロンと表現する

ステルス状態
パソコンなどが起動していないように見えて、実際は動作している状態

スパムメール
元々はインターネットの初期、不特定多数に対して多量に送られてきた広告メールなどの迷惑メールを指す。攻撃者がこの方法を用いてマルウェア感染などを狙う攻撃をしたり、詐欺サイトに誘導するフィッシングメールなどに利用することもある。この場合はスパムメールでありフィッシングメールでもあることになる。サイバー攻撃に用いられる場合は、特定の誰かを狙った「標的型攻撃（標的型メール）」に対して不特定多数を狙うため「ばらまき型攻撃」と呼ばれることもある

スマートウォッチ
スマホと連動したり、単独でネットに接続して何らかの情報をやり取り出来る腕時計型の機器

スマート家電
単独でネットに接続して、何らかの情報をやり取りしたり、動作の指示を受け付けられる家電機器

セキュリティアプリ
スマホなどのセキュリティを確保することに貢献するアプリ

セキュリティホール
パソコンやスマホのシステム上、攻撃者が不正な侵入などを行える状態になっている「穴」のこと

セキュリティキー
→「暗号キー」

セキュリティソフト
パソコンなどのセキュリティを確保することに貢献するソフトウェア

セキュリティパック
パソコンやスマホなどのセキュリティを向上するために、複数の機能がパッケージになって提供されているもの

セキュリティパッチ
パソコンやスマホのシステム上に開いた、セキュリティの「穴」を塞ぐために、メーカーなどから提供される修正プログラム。パッチワークのパッチから来ている

ゼロデイ攻撃
セキュリティホールが公になってから、メーカーなどがその穴を塞ぐための修正プログラムを提供するまでの期間に行われる攻撃。この期間に攻撃を受けると、防ぐ手段はないため、利用者自身が「避ける手段」を講じる必要がある

総当たり攻撃
攻撃者が「ログインパスワード」や「暗号キー」を破るために、全ての文字などの組み合わせを試す攻撃

ソーシャルログイン
特定のSNSやウェブサービスのIDを使って、他のSNSやウェブサービスを利用可能にする規格。特定の身分証明書で、他のサービスを利用できるイメージ。新しいサービスを利用するためにいちからアカウントを作る手間を省く事ができる。OpenIDとほぼ同義だが、他にもソーシャルログインに見える機能は存在する。本書では非推奨

ソース
「情報ソース」の意味で、発信された情報の発信元。発生した事象そのものを明確に見たり聞いたり体験した上で発信しているものを一次ソースと言う。伝聞などで発信しているものを二次ソース、三次ソースと呼び、次第に信憑性が低くなったり、本来の意味とは別の意味で使われている可能性が高くなる

ソフト
ソフトウェア(≒プログラム)の略。対になる言葉は機器を意味するハード(ハードウェア)

ソフトウェアトークン
二段階認証などで使われる使い捨てパスワード(ワンタイムパスワード)を出力するトークンを、ソフトウェアで実現しているもの。例えばソフトウェアトークンを出力するスマホ用アプリ

多要素認証
サービス利用時に行う利用者認証を、3つの要素(①知っているもの②持っているもの③本人自身に関するもの)のうち、2つ以上の要素を用いて行うもの。3つの要素すべてを使う場合などもあり得る

チート行為
ゲームなどで本来認められた方法ではなく不正な方法によるプレイ。またはそれによって利益を得る行為

通知ウインドウ
パソコンなどで、何らかの通知を出す表示の事

通知機能
エラー発生、メール受信、その他のアラートなどを利用者に通知する機能

使い捨てパスワード
二段階認証などで用いられる、利用するたびに更新されるパスワード。ワンタイムパスワード

ディクショナリアタック
→辞書攻撃

データローミング
ローミングに関して、データ通信のローミングを行う事

テザリング
パソコンなどで、スマホなどを経由してインターネット接続をする方法。スマホをルータとして利用するなど

デジタルイミグラント
現実世界からデジタル世界に、移民のようにその生活の一部を移し、これを使いこなす世代。主にパソコンが普及していない時代に生まれた人が多い

デジタルネイティブ
生まれた時代に既に十分にネットが普及しており、現実世界とデジタル世界を垣根無く一体に使いこなす世代

ドライブバイダウンロード攻撃
いずれかのウェブサイトを訪れただけで、何らかのプログラム(この場合はマルウェア)のインストールが発生する攻撃

トラッシング
ゴミ箱に捨てられた紙などから重要な情報を探し出すソーシャルエンジニアリングのテクニック

内閣サイバーセキュリティセンター
正式名称は「内閣官房内閣サイバーセキュリティセンター」。日本政府のサイバー政策の策定や政府機関へのサイバー攻撃の検知と調査を行っている機関。国民への情報セキュリティ意識の啓発も行う。通称NISC。なお内閣府ではない

二段階認証
利用者認証を2回に分けて行うもの。多要素認証と異なり、同じ認証の要素で2つの段階に分けてもそう呼ぶことがある

認証局
申請に基づきSSL証明書の発行を審査する機関

ネームドロップ
業務上の上司や立場が上の人間を装って要求を実行させるソーシャルエンジニアリングの手法

ネチズン
ネットをよく利用する人物を指す、国内ではやや古い呼称。ネットワーク市民（Network Citizen）の略

ネットワーク暗証番号
通信事業者のサービスを利用する際に、利用者が本人であることを認証するための暗証番号

ネットワークカメラ
主にネットワーク上に設置された監視カメラ。セキュリティ上は主にインターネット上から直接存在が見えるものを指し、サイバー攻撃の対象となりやすい。IPカメラとも呼ばれる。IoT機器

ネットワークキー
無線LANでアクセスポイントへの接続や通信の暗号化に使われる鍵。本書では「暗号キー」に分類している

ネットワークルータ
家庭内や会社内のLANをインターネットに接続するための窓口的役割を担う機器。無線LAN機能を内蔵している場合は「無線LANネットワークルータ」「無線LANアクセスルータ」と呼ばれる

野良Wi-Fi
野良猫のように誰が設置したか分からない無線LANアクセスポイント。主に暗号化されておらず誰でも利用できる状態になっているもの。暗号化されていない時代に設置されてそのままのものもあるが、攻撃者が情報を詐取するために設置しているものもある。災害時や観光目的に、運営主体がはっきりして設置される暗号化無しの無線LANアクセスポイントは別

バージョンアップ
アップデートファイルなどを適用して、ソフトウェアやアプリのバージョンが向上すること。セキュリティ関係の更新が含まれることもあり、積極的に適用するべきもの

バーチャル空間
仮想空間とも呼び、主に3Dなどで利用可能なネット上の世界。ゲームなどが現在の主流。VRメガネなどを利用するもののほか、通常のモニターで見るものを指す場合もある

バーチャルリアリティ
仮想空間をあたかも現実世界のように感じさせる技術

ハードウェアトークン
二段階認証などで用いられる使い捨てパスワードを、専用の物理機器として提供するもの

パスコード
一部のアプリなどでPINコードと同じ役割をするものを指す言葉

パスワード
利用しようとしている人が、その機器やサービスの正規の利用者である事を証明する、合い言葉のようなもの

パスワードリスト攻撃
→リスト型攻撃

パターンロック
スマホをロック解除するときに、画面上に表示される複数の点を、あらかじめ登録したパターンでなぞり、ロックを解除する機能

バックアップディスク
パソコンやスマホの情報を別途保存しておき、機器が故障したり紛失や盗難したりした場合に、復元するためのもの。機器の情報の一括バックアップと、目的のデータ毎のバックアップがある

バックドア
機器やシステムに設けられた、正規のログイン方法ではないアクセス方法。攻撃者がシステムに侵入して、再度侵入するために不正に設置する場合や、システム開発者や管理者が管理の手間を省くために設置し、正規のリリース後をそれをわざと残したり忘れてしまっている場合も

パッチ
≒セキュリティパッチ

パラメータ
機器やソフトウェアの設定上の要素

ハリーアップ
ソーシャルエンジニアリングの手法で、相手を急かすことで正常な判断を出来なくなるようにして、目的の要求を通すこと

秘密の質問
ウェブサービスなどでパスワードを忘れてしまい、再度パスワードを設定し直すときなどに本人である確認をするため、あらかじめ設定しておく質問。ただし質問はサービス側が用意したものが殆どで個人情報にまつわるものが多いため、正直に答えているとSNSなどで探し当てられることも

ヒューミント
スパイの諜報活動で、ターゲットの交友関係を調査すること

ヒューリスティック分析
手配書方式のマルウェア検知方法を避ける攻撃が普及してきたため、マルウェアのプログラム上の特徴ではなく、マルウェアの挙動によって判断する方法。別称「ふるまい検知」

標的型メール
攻撃者がターゲットを定めて、マルウェアなどに感染させるために、個人宛のメールを送り付けてくる攻撃。ターゲットの名前だけで無く、業務上のメールと見分けがつかない内容や、場合によっては業務上のつきあいがある人間の名前、あるいはその人間のメールソフトを乗っ取って送られてくることもある

ファームウェア
利用する機器のソフトウェアやアプリではなく、機器自身を動かすプログラム。ソフトウェアやアプリだけでなく、更新されたら必ずアップデートしなければならないもの

ファームウェアパスワード
パソコンの電源投入時に入力を求められるパスワードの名称の一つ。これを入力しないと、そもそも起動することが出来ない。「起動パスワード」

ファイアウォール
パソコンなどのネット接続部に存在するプログラムで、内部から外部へのアクセスは通し、外部からの不正なアクセスを防ぐ壁の役割をする。また企業などでは専用の機器として存在する

フィッシングメール
攻撃者がターゲットから、お金につながる情報や個人情報を盗み取るための詐欺メール。フィッシング(phishing)は洗練された(sophisticated)＋釣る(fishing)から来ている。嘘の情報を餌にして釣り上げるというイメージ

フィルタリングサービス
青少年がネットにアクセスするに当たって、不適切なサイトを閲覧しないようにするサービス

復号
暗号化されたデータを、暗号キーを使って元に戻すこと

不正アクセス通知
利用しているウェブサービスなどに、不正なアクセスが試みられると、スマホなどに通知が送信されてくるサービス

踏み台
攻撃者がサイバー攻撃を行う際、正体を隠すためにコントロール下においたパソコンなどを一旦経由すること。≒ゾンビ化

フライトモード
スマホなどを飛行機で移動中に使えるように、外部に電波を発しない状態にするモード。それに伴い電池の消費が少なくなるので、災害時の省電力モードとしても利用できる

ブラウザ
→ウェブブラウザ

ブラウザ版
SNSなどで、アプリではなくウェブブラウザを使ってアクセスするために提供されているもの

フリーメール
無料で提供されるメールサービス。広告などが表示されるか、利用者の利用情報を提供する代わりに無料で利用できる

フレンドシップ
ソーシャルエンジニアリングのテクニック。友情を持って接する事で要求を断りにくくする

プロダクトキー
OSなどをインストールするときに、正統な利用者である事を証明するための文字列。パソコンにインストールされた状態で販売されるものは本体にシールで貼ってあり、店頭などで単体で販売される場合はパッケージ内部に封入されている。紛失すると再インストールすることが出来なくなる

プロバイダ
インターネットの接続環境を提供する企業。インターネット回線と提供する企業が同一の場合と、別々の場合がある

ベンダー企業
ソフトウェアやハードウェアなどの製品を販売する企業

ポート
パソコンやスマホがネットを通じて相手とデータを送受信するための窓口。それぞれに数字が振られ、これを「ポート番号」という。また送信するものを「送信ポート」、受信するものを「受信ポート」と呼ぶ

ボット
ロボット(robot)の短縮形。様々な作業を自動化したプログラムのことでTwitterで自動的に呟くものが有名。「悪意のボット」となると、パソコンやIoT機器などを乗っ取ってゾンビ化するためのプログラムを指す

ボットネット
悪意のボットにコントロールされた機器で構成される集合体。パソコンやIoT機器などの機器が、コントロール用のサーバによって管理され、DDoS攻撃などに利用される

マネタイズ
何らかの手段で得たモノや情報、システムをお金に換えること

マルウェア
攻撃者が目的とする機器を攻撃するために利用する不正なプログラム

マルバタイジング
マルウェアを含んだ広告を用いるサイバー攻撃。攻撃者がウェブサイトを閲覧したものを感染させるために広告ネットワークにお金を払って出稿する

水飲み場攻撃
攻撃者が目的とする相手(個人もしくは企業の構成員など)を、マルウェアに感染させるために、あらかじめ訪問しそうなサイトにマルウェアを仕込んで待つこと。砂漠などで動物が水があるところによってくる様子からつけられている

無線LAN
ネットで用いられる通信に、無線の信号を用いるもの。LANはLocal Area Networkの略で、通常は会社や家など小さい単位で用いる。インターネットとはルータを境にネットワーク的には分離されている(データの行き来は可能)。これに対して広範囲を対象とするネットワークはWAN(Wide Area Network)と呼ぶ

無線LANアクセスポイント
無線LANを利用するために、無線LANアクセスルータによって提供される接続環境、もしくはその機器。本書では環境を指している

無線LANアクセスルータ
無線LANアクセスポイントを提供する機器

無線WAN通信機能
WANとはLANのLocal Area NetworkにするWide Area Networkの意味。通信電波の供給範囲が広いものを指し、主に携帯電話のLTEなどによる通信ネットワークなどを指す

ランサムウェア
パソコンやスマホなどのファイルを暗号化したりロックしたりして使えなくし、「解除してほしかったら身代金(ransom)を払え」と要求してくるマルウェア

リカバリメディア
あらかじめOSがインストールされたパソコンで、不具合が起きたときのOS再インストールのため、購入後作成するべきインストール用のメディア

リスト型攻撃
ウェブサービスなどから流出したパスワードのリストなどを使って、他のサービスでログインを試みる攻撃

リモートワイプ
遠隔操作でスマホやパソコンの中身を消去すること

ルータ
インターネットなどを利用するために利用者が接続・経由する機器。会社や家庭で利用する無線LANアクセスルータの他、高速なWANの回線を利用して、主に屋外などでノートパソコンなどを接続して利用するモバイルルータがある。また有線だけで利用する有線ルータもある

ローミング
携帯電話などで、回線提供会社と個別の契約を結ばないで、他の会社の契約をもって音声通話を利用すること

ログ
その機器で行われた活動を記録したデータ。通信に関するものは「通信ログ」という

ログアウト
機器やサービスの利用している状態を終了すること。ウェブサービスの場合、利用していたウェブブラウザを終了してもログイン状態は継続される場合があるので、明示的にログアウトの操作をする必要がある

ログイン
機器やサービスに接続し、パスワードなどを入れる事で利用できる状態にすること

「ログインパスワード」
本書では機器やサービスを利用状態にするために入力するパスワードとして定義

ロック
攻撃者による不正なログインなどが試みられ、機器やウェブサービスへログインできない状態。自分の意志でその状態にすることもある

ロック画面
スマホを他者が勝手に操作できないような状態にした画面

情報セキュリティ関連サイト一覧

情報セキュリティ関連のサイト

● みんなでしっかりサイバーセキュリティ

内閣サイバーセキュリティセンター（NISC）
https://www.nisc.go.jp/security-site/
NISCが運営する、サイバーセキュリティ関連の情報を発信する普及啓発用サイト。本ハンドブックの配布も行っている。

● 国民のための情報セキュリティサイト

総務省
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
総務省が運営する、情報セキュリティに関する基礎的なことを学べるサイト。企業向けの対策についても触れられている。

● ここからセキュリティ！

独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/kokokara/
IPAが運営する情報セキュリティを学べるサイト。様々なサイトのコンテンツを集約して分類されている。ポータルサイト的存在。

● 情報セキュリティ 安心相談窓口

独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/anshin/index.html
IPAが国民に向けて開設している、一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する窓口。

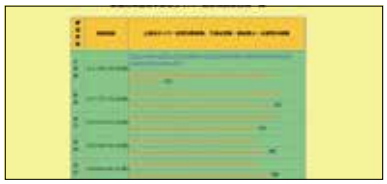
● 情報セキュリティ

独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/
IPAが解説するサイトで最新のセキュリティ情報や、情報セキュリティ啓発コンテンツなどを提供している。

● まんが「サイバーセキュリティのひみつ」

独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/keihatsu/security-himitsu/
IPAが制作協力をし、学研のマンガひみつ文庫で提供されている。子どもから大人まで楽しめる内容。

● 都道府県警察サイバー犯罪相談窓口



警察庁
https://www.npa.go.jp/cyber/soudan.htm
各都道府県の警察本部のサイバー犯罪の相談窓口と情報発信サイト。

● 消費者ホットライン

消費者庁
http://www.caa.go.jp/policies/policy/local_cooperation/local_consumer_administration/hotline/
消費生活全般の全国共通ダイヤル「１８８（いやや！）」で最寄りの消費生活相談窓口につながります。

NISCのＳＮＳによる情報発信

● Twiter

内閣サイバー（注意・警戒情報）

NISC 内閣サイバーセキュリティセンター 注意警戒情報

@nisc_forecast
フィッシング詐欺・マルウェアなどの注意喚起情報やソフトウェアの更新情報を発信している。

● Twiter

内閣サイバーセキュリティセンター（NISC） 公式アカウント

NISC 内閣サイバーセキュリティセンター

@cas_nisc
NISCの取組やサイバーセキュリティに関連する情報を発信している。

● FaceBook

内閣サイバーセキュリティセンター NISC

NISC 内閣サイバーセキュリティセンター

https://www.facebook.com/nisc.jp/
NISCの活動の紹介や、サイバーセキュリティに関するお役立ち情報を原則1日1回、コラムの形で発信している。

● LINE

内閣サイバーセキュリティセンター（NISC） セキュリティ関連情報

NISC 内閣サイバーセキュリティセンター セキュリティ関連情報

LINEID: @nisc-forecast
原則1日1回、サイバーセキュリティに関するお役立ち情報をコラム形式で発信している。

災害時関連のサイト

● 防災情報のページ

内閣府
http://www.bousai.go.jp/
災害時などに政府発表の情報が逐次公開される。また防災関連会議の情報や、大規模地震対策の計画なども公開されている。

● 防災情報提供センター

国土交通省
http://www.mlit.go.jp/saigai/bosaijoho/
リアルタイムの雨量情報他、ハザードマップ、傘下の気象庁発信の情報や、知識を学べる情報なども提供されている。

● 災害用伝言板（web171）

NTT東日本、NTT西日本
https://www.web171.jp/
災害発生時に設置される「災害用伝言ダイヤル」を、ウェブ経由から利用できるようにしたのがweb171。ウェブ経由でも共有できる。

● 災害・防災情報

国土交通省
http://www.mlit.go.jp/saigai/
災害時の状況や復旧状況を、国土や交通インフラの面から提供。情報は逐次更新され、地震、火山、風水害、雪害時などの状況が発信される。

● 気象庁 ホームページ

気象庁
https://www.jma.go.jp/jma/index.html
天気予報や気象全般に係わる情報、警報注意報、地震・津波・火山などの緊急時の情報、そしてさくらの開花状況まで提供される。

● 安否情報まとめて検索

J-anpi
https://anpi.jp/top
災害時に様々な形で提供される安否確認情報を、横断検索して確認をしやすくするためのシステム。NTTとNHKが提供。

● 公衆電話 設置場所検索

NTT東日本
https://service.geospace.jp/ptd-ntteast/PublicTelSite/TopPage/

● 公衆電話 設置場所検索

NTT西日本
https://www.ntt-west.co.jp/ptd/map/

● 公衆電話インフォメーション：公衆電話の種類と利用方法について

NTT西日本
https://www.ntt-west.co.jp/ptd/mag_public_kind.html

いじめ対策関連

● 子供（こども）のSOSの相談窓口（そうだんまどぐち）

文部科学省
http://www.mext.go.jp/a_menu/shotou/seitoshidou/06112210.htm
子供が自分自身で抱える不安や悩みを相談できる相談窓口を集約してあるサイト。

● インターネット人権相談窓口へようこそ！

法務省
http://www.moj.go.jp/JINKEN/jinken113.html
差別、いじめ、嫌がらせ等人権に関する問題で困っている方が気軽に相談できる窓口を掲載。英語や中国語にも対応。

● ここにもあります！相談できる窓口が。「いじめ」しない させない 見逃さない

政府広報オンライン
https://www.gov-online.go.jp/useful/article/201505/2.html
様々な「いじめ」がある最近の現状と、大人と子どもができる「いじめ」へのかかわり方について解説された記事を掲載。

Twitterアカウント

- 首相官邸（災害・危機管理情報）@Kantei_Saigai
- 内閣府防災　@CAO_BOUSAI
- 総務省消防庁　@FDMA_JAPAN
- 気象庁　@JMA_kishou
- IPA(ICATalerts)　@ICATalerts
- JPCERTコーディネーションセンター @jpcert
- フィッシング対策協議会 @antiphishing_jp
- Twitterライフライン @TwitterLifelin

索引

た行

な行

は行

ま行

ら行

内閣サイバーセキュリティセンター (NISC)ホームページ：https://www.nisc.go.jp/
NISC「みんなでしっかりサイバーセキュリティ」：https://www.nisc.go.jp/security-site/index.html
内閣サイバーセキュリティセンター 公式Twitter: @cas_nisc
内閣サイバー（注意・警戒情報）Twitter:@nisc_forecast
内閣サイバーセキュリティセンター NISC LINE公式アカウント：@nisc-forecast
NISC facebookページ: https://www.facebook.com/nisc.jp

インターネットの安全(あんぜん)・安心(あんしん)ハンドブック

2019年1月18日　Ver 4.00発行

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

制作・著作　内閣(ないかく)サイバーセキュリティセンター
イラスト　ＫＯＴＡ