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記憶装置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。WPA3はこれ以上の安全性をもつ

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が立ち上がる前に入力を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、攻撃対象のサーバなどを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。オンラインショッピングサイト

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」が運用開始

ID（アイ・デイー）
機器やウェブサービスなどを利用するときに、利用者を識別する文字列。「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規格。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でき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.。「モノのインターネット」ともいわれる。コンピュータの入った電子機器をなん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、IoT機器製造業者がすべてネットワークセキュリティに詳しいとは限らず、攻撃者から見て乗っ取っ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機器など、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が存在するほか、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、おもに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。さらに高速な5Gが登場しつつある

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。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。

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ときに打ち込む、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から6桁以上の数字で打ち込むもので入力ミスでペナルティがあるものとして定義

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。通常インストールできないアプリなどがイントール可能となる。これを行うこと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。逆に使えないように制限されている状態はSIMロックという。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などが合っている必要がある。

SMS（ショートメッセージ）
Short Message Service。スマホなどで電話番号宛てで送受信できるテキストメッセージ。携帯電話回線契約があればデータ通信契約が無い状

態でも送受信できる。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、送受信できない。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補助記憶装置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、半導体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。→補助記憶装置

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いい

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。認証局が審査を行って発行する。最近は審査がいい加減だったり、無料で発行する認証局の登場により、安全であることの目安とはならない状況になりつつある。より審査の厳しいEV-SSL証明書も存在する

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記憶装置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。内蔵記憶装置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、当然解読がより困難になる

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」にされることもあるので、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ための規格

USBセキュリティキー（ユー・エス・ビー・せきゅりてぃ・キー）
USB端子に接続して、機器やウェブサービスの正統な利用者であることを証明する物理的な鍵

の役割を果たすもの。NFC、Bluetoothに対応しているものもある

USBチャージャー（ユー・エス・ビー・チャージャー）
USB経由で機器を充電でき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サービス

WAN（ワン）
Wide Area Network。LANと対になる言葉で、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

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。一方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、そのほか無線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機器が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仮想のキャラクター。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、なんらかの機能を実現するプログラム。おもにスマホで使われ、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こと。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ため利用は非推奨

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通常の手段では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、なん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ための、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」がなくても解読できるものもある。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

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ため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定義情報が入ったファイル。実世界でいえば顔写真付きの手配書のようなもの

ウェブサーバ
ネット上でウェブサイト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、入力制限がない環境で解読攻撃を行うもの。おもにネットに接続しないでできる攻撃なので、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の iOSなど

オレオレ証明書
通信の暗号化に際し本来認証局に申請して発行してもらう証明書を、勝手に発行して暗号化通信に利用するもの。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

記憶装置
コンピュータ内部や、外部バスに接続され、データを保存する装置。ハードディスクやSSD

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、相手になにかのメリットを与えることで、その代償として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、データなどを保存しておくサーバ。おもに「機器の記憶装置と同等に利用できる」「特別なサービスを利用している意識はないが使えている」「でもどこにあるかわからない」雲のような存在感からCloudと呼ばれる。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」そのものは悪意があるかどうかとは関係がないので、特に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でき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できないか行うテスト。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（つながっていること）と対になって使われる言葉で、ネットワークにつながっておらず単独で存在すること。ただし、ネットにつながっていて、かつほか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こともある

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した。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少量の「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なんらかの情報をやり取りできる腕時計型の機器

スマート家電
単独でネットに接続して、なん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。IoT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プログラム上の「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携帯電話キャリアなどから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、すべての文字などの組み合わせを試す攻撃

ソーシャルエンジニアリング
対人（アナログ）、サイバーを問わず、人間の心の隙を突き、相手に自らの望むような行動をさせるテクニック。対人の代表的な例が「オレオレ詐欺」などの特殊詐欺、サイバーの代表的な例が「標的型メール」やBECなど

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、ほかのSNSやウェブサービスにログインし利用可能にする規格。特定の身分証明書で、ほか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ことができる。OpenIDとほぼ同義だが、ほかにもソーシャルログインに見える機能は存在する。鍵となるアカウント情報が流出すると連鎖的に乗っ取られるため、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いう。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、なんらかの通知を出す表示のこと

通知機能
エラー発生、メール受信、そのほか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こと

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方法など

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。おも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な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、なんらかのプログラム(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、内閣府と内閣官房は違う組織ですってば。おーぼーえーてー！

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つの段階に分けて認証する場合もそう呼ぶ。一方、異なる要素を組み合わせて2回認証を行う場合は二要素認証とも呼ぶ。同じ要素2回よりは異なる要素2回の方がセキュリティレベルは高くなる

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
おもに、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、おも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飼い主か分からない無線LANアクセスポイント。おもに、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、おもに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ことを証明する、合い言葉のような文字列

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
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たりしている場合も

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でき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ほとんどで内容も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、個人宛のフィッシングメールを送り付けてくる攻撃。ターゲットの名前だけでなく、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できない。「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、不適切なウェブ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こと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こと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できなくなる

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
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

ホームページ
→ウェブサイト

補助記憶装置
→記憶装置

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、スマホ、IoT機器などが、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
なんらかの手段で得たモノや情報、システムをお金に換えたり、それを用いて稼いだりすること

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ウェブ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、おもに携帯電話の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、ほか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アクセスルータのほか、高速なWANの回線を利用して、おも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、ほか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こと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くなった状態。自分の意志でその状態にすることもある。ロックをした画面をロック画面という

索引

アルファベット

AES ・・・・・・・・・・ 72,74,75,90,154
BIOS パスワード ・・・・・・・ 104,154
DDoS 攻撃 ・・・・・18,48,49,126,140,154
EC サイト ・・・・・・・・・・ 135,154
GPS ・・・98,105,108,119,131,133,137,145,146,154
IMAP ・・・・・・・・・・・・・ 84,154
IoT ・・・・・・・ 17,30,32,34,49,57,154
JailBreak ・・・・・・・・・・ 32,154
microSD ・・・・・・・・・・101,102,155
Office 製品 ・・・・・・・・・・ 29,155
PIN コード ・・・ 35,36,40,56-59,62,91,98,99,108,125,129,134,155
POP ・・・・・・・・・・・・・ 84,155
POS レジ ・・・・・・・・・・ 17,155
RMT ・・・・・・・・・・・ 125,155
root 化 ・・・・・・・・・・・ 32,155
SIM ・・60,75,133,135,136,137,142,143,155
SIM 認証 ・・・・・・・・・ 72,74,75,155
SIM フリー ・・・・・・・・・136,137,155
SMS ・・・・・・ 18,22,31,36,41,42,59,60,136,137,141,155
SSL 証明書 ・・・・・・・・ 79-82,87,156
Stuxnet ・・・・・・・・・・・・・ 92
TKIP ・・・・・・・・・・・72,75,156
TPM ・・・・・・・・・・・ 105,156
UPnP ・・・・・・・・・・・・ 74,156
USB (カー)チャージャー ・・136,141,157
VPN ・・・・・・・・50,76-84,142,145,157
WEP ・・・・・・・・・ 65,71,72,75,157
Wi-Fi ・・・・・ 17,56,70,71,73,82,91,95,135,145,157
WPA,WPA2,WPA3 ・・・65,71,72,74,75,157

あ行

アオリ行為 ・・・・・・・・・・ 121,157
悪意のボット ・・・・・・・・ 16,18,46,48
アクセスポイント ・・・・ 48,70-72,74-79,82,83,100,110,134,157
アクティベーションコード ・・・・ 47,157
アタッカー ・・・・・・・・・・・ 15,157
アップデートファイル ・・・・・・ 30,158
アバター ・・・・・・・・・・・ 151,158
アプリ連携 ・・・・・・ 63,64,110,111,158
アンインストール ・・・・・・ 33,111,158
暗号(化)キー ・・・・・ 47,48,56-59,64,65,71-75,90,91,100,105,134,158
インターネットバンキング ・・・・ 47,82,93,158
インターフェース ・・・・・・・・ 26,158
ウイルス ・・・・・ 16,28,29,32,70,90,127
ウイルス定義ファイル ・・・・・・ 29,158
ウェブブラウザ ・・・29,30,33,35,61,63,66,67,73,76,78-83,87,96,109,158
ウォードライビング ・・・・・・・・・ 48
エアギャップ ・・・・・・・・・・ 92,93
炎上 ・・・・・・・・・・・・117,118,121
オシント ・・・・・・・・・・・・・・ 54
オフラインアタック ・・・・・・・58,62,158
オレオレ証明書 ・・・・・・・・・ 81,159
オンラインアタック ・・・・・・・ 58,159
オンライン(授業)(会議) ・・ 21-24,47,93

か行

キーロガー ・・・・・・・・・・・ 16,135
ギブアンドテイク ・・・・・・・・ 20,159
共通鍵暗号方式 ・・・・・・・・・・ 91
クラウド(サーバ)(サービス),(ストレージサービス) ・・・35,61,62,63,90,96,101,102,106,117,130,143,159
クラッカー ・・・・・・ 15,16,43,152,159
クラッキング ・・・・・ 33,61,62,126,159
検体 ・・・・・・・・・・・・・・ 31,159
公開鍵暗号方式 ・・・・・・・・・ 85,91
虹彩 ・・・・・・・・・・・・・・36,59,159
公衆無線 LAN ・・・・・ 70-72,74-77,82,95,100,135,159

さ行

サービス連携・・・・・・・63,64,111,159
シギント・・・・・・・・・・・・・・・54
辞書攻撃・・・・・・・・・34,57-59,96,159
ショルダーハッキング・・・・・・・40,58
スタンドアロン・・・・・・・35,61,92,159
ステルス状態・・・・・・・・・・105,160
スパムメール・・40,41,44,50,86,88,89,160
スマートウォッチ・・60,66,67,98,136,160
スマート家電・・・・・・・・30,32,49,160
スマートテレビ・・・・・・・・・・17,132
スマート冷蔵庫・・・・・・・・・17,32,49
生体認証・・・・・・・36,38,58-60,67,68,98,104,108
セキュリティアプリ・・・・・・・30,32,160
セキュリティキー・・・26,36,56,60,69,160
セキュリティパック・・・・・26,32,38,160
セキュリティパッチ・・・・・27,33,38,160
セキュリティホール・・・17,20,26-30,33,36,38,49,83,109-111,160
セクスティング・・・・・・・・・・19,118
ゼロデイ攻撃・・・・・28,33,41,49,83,86,110,160
総当たり攻撃・・・・・34,35,56-59,65,160
ソーシャルエンジニアリング・・・20,27,39,40,43,160
ソーシャルログイン・・・・・・63,64,160
ソフトウェアトークン・26,36,59,60,66,161
ゾンビ化・・・・・・・・・・・・・48,126

た行

ダークウェブ・・・・・・・・・・48,88,126
多要素認証・・・26,27,34,36,47,59-61,64,66,68,70,81,82,96,99,106,161
チート行為・・・・・・・・・・・125,161
通知機能・・・・・・・・・・・・・99,161
使い捨てパスワード・・・26,36,64,66,81,83,161
ディクショナリアタック・・・・58,59,161
データローミング・・・・133,135-137,161
テザリング・・・・・・・・・・76,109,161
デジタル遺産相続・・・・・・・・・・129
デジタルイミグラント・・・・・150,161
デジタルタトゥー・・・・・・・・・・115
デジタルネイティブ・・・・・149,150,161
手配書方式・・・・・・・・・・・・・28
テレワーク・・・・・・・・・・・・21,22
ドライブバイダウンロード攻撃・・33,161
トラッシング・・・・・・・・・・40,161
トロイの木馬・・・・・・・・・・・・16

な行

なりすまし・・・19,20,39,47,72,74,86,87,118,121,127
入力遅延・・・・・・・・・・・・57,58
認証局・・・・・・・・・・79-81,85,162
ネームドロップ・・・・・・・・20,40,162
ネチズン・・・・・・・・・・・148,162
ネットいじめ・・・・・・・・・・19,115
ネットワーク暗証番号・・・・・・56,162
ネットワークカメラ・・・・・・17,30,162
ネットワークキー・・・・・・・・56,162
ネットワークルータ・・・・・・・17,162

は行

バージョンアップ・・・・・・・・26,162
バーチャル空間・・・・・・・・151,162
バーチャルリアリティ・・・・・151,162
ハードウェアトークン・・・26,36,59,162
パスコード・・・・・・・・・・・56,162
パスフレーズ・・・・・・・・・・56,68
パスワードリスト攻撃・・・58,59,67,162
パターンロック・・・・・・・・・40,98,162
ハッカー・・・・14,15,43,126,127,152,153
バックアップ・・・・・18,35,50,61,63,96,101-103,106,111,117,133,162
バックドア・・・・・・・・・・103,162
パッチ・・・・・・・・・・・・22,110,163
ハリーアップ・・・・・・・・・20,40,163
秘密の質問・・・・・・・・・・・36,163

ヒューミント・・・・・・・・・・ 54,163
ヒューリスティック分析・・・・・ 28,163
標的型メール・・・・20,27,33,39-41,54,86,88,163
ファームウェア・・・・26,29,30,73,74,163
ファームウェアパスワード・・・ 104,163
ファイアーウォール・・・・・・27,38,163
フィッシング詐欺・・・18,42,46,61,67,144
フィッシングメール・・・・ 41,83,103,163
復号・・・・・・ 50,56,65,71,72,85,91,163
不正アクセス通知・・・・・・・27,38,163
踏み台・・・・・・・・・・ 22,46,48,49,164
フライトモード・・・・・・・・・ 139,164
ブルートフォース攻撃・・・・・・ 56,59
ポート・・・・・・・・・・・ 78,84,85,164
ボット・・・・・・・・・16,18,46,48,53,164
ボットネット・・・・・・18,29,46,48,49,164
ホワイト(ハット)ハッカー・・・・・・ 15

ま行

マネタイズ・・・・・・・・・・・・ 94,164
マルバタイジング・・・・・・・・ 83,164
水飲み場攻撃・・・・・・・・・・ 83,164
無線LAN・・・ 17,30,48,57,58,70-79,82,84,95,100,109,110,134,135,165
無線WAN通信機能 ・・・・・・ 108,165

ら行

ランサムウェア・・・・・16,18,50,52,106,126,165
リカバリメディア・・・・・・・ 104,165
リスト型攻撃・・・・・・ 35,57-59,96,165
リベンジポルノ・・・・・・・・・・ 19,115
リモートワイプ・・・ 90,101,105,108,165
ルータ・・・・ 17,30,32,49,57,70,72,73,74,76,109,165
ローミング・・・ 133,135,136,137,142,165
ログ・・・・・・・・・・・・・・・ 38,165
ログアウト・・・・・・・・・・・ 103,165

内閣サイバーセキュリティセンター (NISC)ウェブサイト：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
NISC「みんなで使おうサイバーセキュリティ・ポータルサイト」：https://security-portal.nisc.go.jp/
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
2019年3月5日　Ver 4.01発行 (誇示脱字修正、用語表記統一修正)
2019年3月18日　Ver.4.02発行 (配色ミス修正、誤字脱字修正、レイアウト統一修正)
2019年3月20日　Ver.4.03発行 (誤字脱字修正)
2020年3月31日　Ver.4.10発行
2021年12月31日　Ver.4.20発行

制作・著作　内閣官房　内閣サイバーセキュリティセンター (NISC)
協力　総務省　経済産業省　独立行政法人情報処理推進機構(IPA)