用語集

■ .exe(エグゼ)

Microsoft が開発したファイル拡張子。Windows上で実行できるプログラムのファイル形式の1つ。Windowsが普及した結果、見た目に「.exe」を付け、利用者の目をごまかし、実際は不正なプログラムを潜り込ませるといった悪質な犯罪行為があるので注意が必要

......126

■ 00000JAPAN(ファイブゼロ ジャパン)

2011年3月11日の東日本大震災をきっかけに、日本国内での通信回線を、非常時に利用できる仕組みを整備し、緊急時におけるがよう確保を目的に取り組みが始まったプロジェクト。2016年4月14日の熊本地震で初めて利用された。00000JAPANは、非常サソーンのでいるになる。利用時のSSID(無線LANの名前)が「00000」で始まっていることから、この名称となっている。

■ 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担保する

■ BCP(ビー・シー・ピー)

Business Continuity Planning の略。事業継続計画の意味で、災害時などの被害を最小限に抑えて事業を継続するために、あらかじめ人・モノ・金などのポイントから計画を立て、また、これを訓練することが望まれる。中小企業庁に詳細なウェブサイトがある

■ BEC(ベック)

Business Email Compromise の略。ビジネスメール詐欺。攻撃者がビジネス用のメールを装い、企業の担当者をだまして、不正送金や機密情報の流出などが行われる攻撃

■ 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

......89

■ BYOD(ビー・ワイ・オー・ ディー)

Bring Your Own Device の 略。社 員が個人の所有機材を会社の業務 で使用すること

■ CDN(シー・ディー・エヌ)

Content Delivery Network (コンテ ンツ デリバリー ネットワーク)の 略。CDNをサービスとしているグ ローバル企業もある。写真や動画 など、データサイズが大きなもの をインターネットで通信すると、 通信が遅延してしまう問題が発生 してしまうため、遅延を解消する 目的で作られた。CDNサービスで は、世界各地にデータセンターが 展開されていて、データセンター のサーバーには一時的にファイル のコピーが保存されている。例え ば、動画を配信する事業者がCDN を利用することで、事業者にとっ ては自社のサーバーへのアクセス を軽減でき、動画を視聴したいユー ザーにとっては地理的に近いCDN サービスのサーバーからコンテン ツを配信され、遅延なく安定的に 動画を視聴できるメリットがある

■ DDoS攻撃(ディードスこうげき)

Distributed Denial of Service Attack。攻撃者などが不正に操作した多数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

.....21,55,58,62,72,94,159

■ DMZ(ディーエムゼット)

DeMilitarized Zone。非武装地帯の 意味。インターネットにつながる LAN 用ルータに接続した機器のう ち、LAN 側ではなくインターネッ ト側に設置したかたちにする仮想 的なエリア。自前の公開用サーバ やインターネット側から参照する 監視カメラなどを設置する。DMZ にあるIT機器はインターネットか ら直接見えるため攻撃されやすい

......95

■ FIDO(ファイド)

FIDO (Fast Identity Online:ファイド)は、新しい認証手段としまれている技術の1つ。多にかったアプリの認証手段にからないではないではないではないではないではない。2022年12月にはないる。2022年12月にがいるの大手IT企業がFIDOをもったが、現地には、使用のはないでは、使用ができたがではないではないではないではないではないが特徴を持たせてユーザの認証をが特徴

■ GDPR(ジー・ディー・ピー・ アール)

GDPR (General Data Protection Regulation) とは、個人情報の保護やその取扱について、詳細に定められた EU 域内の各国に適用される法令。2018 年 5 月 25 日施行された。EU 域内とはなっているが、インターネットの場合、国境の壁がないため、EU 圏内のユーザからのアクセスを対象としたサービスやアプリの場合、GDPRの対象となることに注意

......162

■ 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

......39,42,70,79,81,90

■ https://(エイチ・ティー・ ティー・ピー・エス)

ホームページ(ウェブページ)にアクセスするためのURLの冒頭に記述される文字列。検索大手企業のGoogleが2014年ごろから積極的に安全なホームページへのアクセスを推奨し始め、2018年7月24日以降、https://でアクセスできるホームページ以外(http://ではじまるページ)については、警告を出すようにしました。詳しくは常時SSL化を参照

■ 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

18,22,30,31,33,35,36,40,55,56,75,89,99,101,104,105,108,118,121,133,139,141,145,153,156,158

■ IoT(アイ・オー・ティー)

Internet of Things。「モノのインターネット」ともいわれるが、あらゆるものをネットにつなげる考え方。しかし、IoT機器製造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…… 17,18,19,30,31,51,58,94,95,100,115

■ 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し、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……………37,38

■ LTE(エル・ティー・イー)

Long Term Evolution。携帯電話の通信規格。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

......90,93,110

■ 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 を小型化したもの

.....44,86,87

■ NAS(ナス)

Network Attached Storage の略称であり、パソコンやサーバーをつないでいる既存のネットワーク (LAN) に直接接続するストレージのこと。ネットワーク上のファイルサーバーとしての機能を果たすが、1台のサーバに直接接続されるのではなく、複数のパソコンやサーバーに接続することが想定される。

■ 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

.....24,27,59,108,146,147,164

■ 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

......29

■ OS(オー・エス)

Operating System (オペレーティングシステム)の略。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「macOS」、iPhoneの「iOS」、Androidスマホの「Android」などが代表的。ほかにも「Linux」(リナックス)という、サーバや工業機器、IOT機器などに搭載されているOSや、「UNIX」(ユニックス)、「Ubuntu」(ウブントゥ)などがある25,27,29,30,38,44,50,88,89,115,128,129,146

■ PGP(ピー・ジー・ピー)

Pretty Good Privacy の略。米国の Philip Zimmermann が開発した暗 号化ソフトウェアの名称。公開鍵 の交換を事前に当事者間で行い、 その間で電子署名や暗号化された メールのやりとりを可能にする仕 組み

■ 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。複数回入力画面がロカカ運延や入力画面がかかるなどの規制がかかるものを指する「ワイプ」機能であるものもら、本書では機器やサ以上の数字で打ち込むもので、入して変義

33,34,42,43,46,81,83,99,100,101, 129,141

■ 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

■ QRコード決済

インターネット上で普及した電子マネーを、物理店舗での購買にも利用するための仕組み。使用する電子決済サービスごとに用意されたQRコードを利用し、スマホのカメラでそのQRコードを映し、電子マネーの支払い・受け取りを行う

■ 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ストー 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

......37,38

■ RSS(アール・エス・エス)

Really Simple Syndication もしくは Rich Site Summary の略。ウェブサイトの見えない部分で更新情報を掲載し、RSS リーダーで複数のサイトの更新情報を集約して見る事ができる。更新情報やタイトルだけで無く、仕様によっては要

約文が提供される場合もある

■ S/MIME(エスマイム)

Secure / Multipurpose Internet

| Mail Extensionsの略。電子メールのセキュリティの確保を目的とした暗号方式の1つ。電子証明書を用いてメールの暗号化とメールへ | SSID(エス・エス・アイ・ディー) SSID(Service Selt Identifier) は、 | 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 |
|--|--|--|
| デジタル署名を行える 124,125,130 | 無線LAN接続の際に利用するネットワーク名のこと。無線LAN接続 では、接続する無線LANアクセス | ි90 |
| ■ SIM(シム) | ポイントそれぞれを識別するため | ■ UPnP(ユニバーサルプラグア |
| スマホなどで携帯電話回線を利用 | に、最大32文字の英数字の名称 | ンドプレイ) |
| するために挿入する小型のカード。 | を付ける | Universal Plug and Play。ルータ |
| 電子的なeSIMもある | 111,112,113,114,115,122 | に内蔵されている機能で、家や会 |
| 81,102,114,115 | | 社のLAN側にある機器を、難しい |
| | ■ SSL(エス・エス・エル) | 設定抜きでインターネット側から |
| ■ SIM 認証(シムにんしょう) | →SSL/TLS | アクセス可能にする。LAN内の機 |
| 公衆無線LANなどで、「暗号キー」 | 115 | 器がインターネット側からアクセ |
| を他人と共用しないように、それ | | スされ、「踏み台」にされることも |
| ぞれの利用者によって異なるSIM | ■ SSL/TLS(エス・エス・エル/ | あるので、利用しない方が安全 |
| の情報を使って認証を行う方式 | ティ・エル・エス) | 95,113 |
| 112 | Secure Socket Layer / Transport | |
| | Layer Security。データを暗号化 | ■ URL(ユー・アール・エル) |
| ■ SMS(エス・エム・エス、 | して送受信する方法で、SSLの方 | Uniform Resource Locator の 略。 |
| ショートメッセージ) | が古く、これを改訂して進化させ | http://やhttps://などから始まる |
| Short Message Serviceの略。スマ | たものが TLS。SSL が TLS の元に | インターネットのウェブサイトの |
| ホなどで電話番号宛てで送受信で | なったこともあり、未だにSSLと | 住所を示す文字列 |
| きるテキストメッセージ。携帯電 | 呼ばれたり、SSL/TLSと書かれた | 37,52,63,84,114,118,120, |
| 話回線契約があればデータ通信契 | りするが、古い資料やバージョン | 121,122,156 |
| 約が無い状態でも送受信できる。 | を明記しているものを除けば同義 | |
| 一方、電話番号が無い場合や、デー | の意味と考えてよい | ■ USB(ユー・エス・ビー) |
| タ通信専用SIMでSMSが提供され | 115,118,123,124 | Universal Serial Bus。パソコンな |
| ていない契約では送受信できない。 | | どに周辺機器を簡単に接続するた |
| SMSがオプションとして提供され | ■ SSL証明書(エス・エス・エル | めの規格 |
| ている場合もある | しょうめいしょ) | 44.89.91.100.129.140.144.151. |

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

......44,90,92,100

的高価だが高速

■ 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、さまざまな形態が

.. 34,36,38,41,62,101,102,140,156

.... 20,23,24,32,35,36,39,40,43,49, 50,52,56,58,60,61,64,65,66,67,68 ,69,70,71,73,74,75,76,77,78,79, 80,84,86,87,88, 93,96,97,98,104, 105,114,126,127,128,133,134, 142,145,146,147,157,158,160

■ 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記憶 装置であるハードディスク(HDD)

Temporal Key Integrity Protocol.

EV-SSL証明書も存在する

■ TKIP(ティーキップ)

暗号化方式の1つ。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

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

......98,119,120,122,125

■ TPMチップ(ティー・ピー・エ ムチップ)

Trusted Platform Module の 略。 TCG (Trusted Computing Group)

と呼ばれる団体によって定義され たセキュリティの仕様に準拠した 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 敬慧を困難にする。 内華司絵

160,161

■ USBセキュリティキー(ユー・ エス・ビー・セキュリティキー)

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ことを 証明する物理的な鍵の役割を果た すもの、およびそこから認証用の ワンタイムパスワードなどを送信 するもの。BluetoothやNFCに使 うタイプも存在する

......34,91,101,102,109,158

■ 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

.... 40,59,98,115,116,117,118,119, 123,139,150

■ WEP(ウェップ)

Wired Equivalent Privacy。暗号化方式の1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)

ルータに無線LAN アクセスポイン ト機能を付けたもの。無線LAN ア クセスルータ。→ルータ

......110

■ WPA(ダブリュー・ピー・エー)

Wi-Fi Protected Access。無線 LAN の 暗号化方式の1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とされる。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ぜい弱性 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 …………112,114,115

■ ZIPファイル(ジップファイル)

パソコンなどに保存されるさまざまなデータ(ファイルやフォルダ)を1つのまとまりにしたもの。ZIPと呼ばれる形式のため、ZIPファイルと呼ぶ。まとめることを圧縮、ふたたび分けることを解凍と呼ぶ。また、ZIPファイルに圧縮する際に、パスワードを設定して認証を必要とさせることも可能

......99,100,126,127

■ アウトソース

企業や組織において、プロジェクトの遂行やサービスの運用を内部の人材だけで対応するのが難しい場合、外部の人材、組織を利用することがある。これをアウトソース(人材の外部調達)と呼ぶ。インターネット関連のビジネスでは、サーバの運用そのものをアウトソースする場合が増えており、その際に利用されるものにクラウドサービスがある

■ 悪意のハッカー

■ 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

.... 57,84,96,110,111,112,113,114, 115,116,117,118,119,122

■ 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

→本書では「攻撃者」と同義。ハッカーやクラッカーなどとの使い分けはイントロダクション2 (P.15) 参照

■ 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 トを行うためのインストールファイルを「アップデートファイル」と呼ぶこともある。セキュリティの向上を含む場合もあるが、単に機能向上の場合もある。セキュリティ向上のみを行う場合は、セキュリティパッチと呼ばれる場合が多い…17,25,27,29,30,38,45,50,61,91,94,95,96,114,145,147,155,158

■ 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……25,27,30,32,33,34,36,37,38,39,41,43,44,58,59,61,63,66,70,79,80,83,84,86,87,93,95,97,101,102,103,104,105,106,109,115,116,118,121,122,123,124,126,131,140,141,147,149

■ 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り、攻撃者のサイバー攻撃の手口になるため利用は非推奨96,97,105

30,31,100

■ 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29,61,97

■ 暗号化

■ 暗号鍵

暗号化処理(別項)において、データを暗号または復号する際に必要となる、短い符号のこと。暗号化処理で使用されるため、このような名前が付いている。暗号化処理の方法によって、共通鍵、公開鍵、秘密鍵といった種類がある

......99

■ 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、意図せずれ有すると、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

......99,111,115

■ 暗号化処理

パソコンやスマホでやりとりする データに処理を加えることで、外 部から判読できないようすること。 インターネットでのコミュニケー ションが一般化している今、重要 な情報を扱うデータには暗号化処 理が必須となっている

.....90

■ 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

......90,129

■ 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

.. 84,85,106,107,111,112,113,114, 115,116,123,129

■ 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

......129

■ 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→暗号化キー

... 56,57,84,85,90,99,100,101,106, 107,111,112,113,114,115,129, 130

■ 位置情報共有アプリ

現在、ほとんどのスマホに搭載されている位置情報特定機能を利用して、そのスマホのある物理的な場所(位置情報)を共有できるアプリ。家族や恋人、仲のよい友人間で、お互いの現在地を共有したい場合に利用される。最近では、こどもの通学時の安全確認といった利用方法にまで広がって

いる

■ 違法アップロード・ダウンロード

イラストや写真、文章、ソフトウェアなど、著作権が発生する著作物を、著作者、著作権者に無断で利用したり複製し、インターネットを通じてアクセスできる状況に不正にアップロードすること。また、そのようにアップロードされた著作物を不正にダウンロードすること。その行為を行った場合、著作権法違反として刑罰の対象となる…………………………………………………………71

■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

...... 17,22, 27,29,37,38,42,50,59, 61,95,97,121,125,126,155,157

■ 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

■ 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

......29

■ ウェブ

ウェブサイト、ホームページの略称。そもそもはインターネット上のウェブサイトを指す、World Wide Web(WWW,W3)の略

.... 18,21,31,32,33,34,35,38,39,41, 47,48,49,56,57,61,62,71,87,94,97,99,100,101,102,103,104,105,110,119,120,122,123,125,126,127,128,131,141,146,147,151,153,158

■ 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

............ 18,61,93,117,118,137,159

■ ウェブサイト

ネット上で文章ファイル風に情報 を表示する場所。主としてウェブ ブラウザなどで閲覧する。ウェブ サーバ上で運営される

......18,37,41 ,47,59,60,61,75,79,84,93,103,110, 111,114,117,118,119,120,121,122 ,123,125,126,131,135,139,140,14 3,147,153,155,156,157,158,159

■ ウェブブラウザ

ネット上で公開されているウェブ サイトを閲覧するためのソフトウェ アやアプリ

... 29,30,33,61,93,95,103,108,113, 115,118,119,120,121,122, 125,133,156

■炎上

SNSの投稿をきっかけに、想定外の情報拡散、また、不特定多数への反応が大きくなること。と、場で使われる用語は投稿者あるいは投稿者あるいは投稿された人物や企業・一大名の誹謗中傷につながり、一大は組織の計論を表上の範囲が大きまると、その対象者・対象企業を対象組織の社会的立場を失わせるまでの事件にも発展する

■ 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

■ 鍵マーク

パソコンのブラウザでホームページにアクセスすると、上部にそのホームページのURLが表示される(https://の部分)。このとき、アクセスしたホームページが常時SSL化されていると、URLの頭に鍵マークが付く。つまり、このマークが付いているホームページは常時SSL化対応済み、と認識できる…………………119,120,122,125

■ 拡散

インターネットやSNSにおける拡散とは、掲載された情報やSNSで投稿された内容が周囲に広がっていくこと。拡散の使われ方として、大切な情報や募金などの慈善行為を広げるための好意的な場合と、フェイクニュースや特定事物を攻撃する誹謗中傷をおもしろおかし

く広げる、悪意が含まれる場合の 2通りがある ………………20,23,39,41,47,58, 60,68,69,73,74,75,97

■ 拡張子

パソコンやスマホで利用するファイルの種類を識別するために使われる、ファイル末尾にある文字列。.(ドット)の後ろにある1~4の文字列のこと。例えば、テキストファイルなら.xlsxとなる

......126

■ 管理者用パスワード

インターネット上のサービスや企業・組織内のサーバを管理するための権限を持つアカウントのためのパスワード。これを知っていると、該当するサービス・サーバのすべての作業が行える。なお、サーバ以外にも個人のパソコンやスマホでの設定もできる場合がある

.....58,95

■ 記憶装置

パソコンやスマホの中にあるプログラムやデータを保存するメモリ。CPUに直結されデータをやりとりするメインメモリが主記憶装置、何らかの結線を使って接続しデータをやりとりするものが補助記憶装置という。ハードディスクやSSDなどはこれにあたる。総括して記憶装置

... 44,45,90,91,92,97,100,103,110, 111,129,160,161

■ 機械学習

大量のデータをコンピューターに 読み込ませ、データ内に潜むパターンを学習させることで、未知のデータを判断するためのルールを獲得することを可能にするデータ解析技術。最近では、人工知能技術の一部に位置付けられている。なお、機械学習に含まれる技術のうち、さらに精度・自動化向上等を目指す技術として、「ディープラーニング」などが挙げられる。

■ 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

......62

■ 共通鍵暗号方式

通信を暗号化する仕組みにおいて、 暗号化と復号に同一の(共通の)鍵 を用いる暗号方式

......130

■ クライアント証明書認証

インターネットを通じてサーバに アクセスする際に、個人や組織を 認証し発行される電子証明書。利 用者側のパソコンやスマホにイン ストールされるものを指す。これ と、サーバ側に置かれるSSLサー バ証明書が対となって、正しい利 用者かどうかを認証し、不正アク セスを防ぐことができる

■ クラウド

従来手元で保存していたデータな どを、インターネット上に存在し ているサーバに保存し、ネットに つながったどの機器からでも利用 できるサービス。ネットワークの 図の上にインターネットを書く場 合、雲(英語でクラウド)を書くこ とが一般的であったことから、イ ンターネット上で提供されるサー ビスをクラウドサービス(略して クラウド)と呼ぶようになった。 ほかにも「オンラインストレージ サービス」と呼ぶ場合もある 21,33,35,44,45,62,69,76,86,87 ,91,104,129,133,135,137,139,141, 142,143,144,148,149,153,158,164

■ クラウドサーバ

,168,169,173

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。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 …… 33,44,45,86,87,91,133,135,153

■ クラッカー

■ 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

■ 権限

Windows や macOS など、コンピュータ上で動くOSは、ログインする(使用する)ユーザごとに操作権限を指定できる。これをOSの権限と呼ぶ。例えば、管理者権限の場合、対象となるOSすべての操作が可能となり、データをすべて削除したり、OSそのものを再インストール(初期化)することが可能となる

41,105,119,133,136,144,145

■ 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

......50

■ 公開鍵暗号方式

通信を暗号化する仕組みにおいて、暗号化と復号に別個の鍵(手順)を用い、暗号化の鍵を公開できるようにした暗号方式

■ 公開範囲

Facebook や X(旧 Twitter)などの SNSにおいて自身の投稿内容を公 開する範囲。また、クラウドサー ビスやプロジェクト管理ツールな どにおいても、サーバにアップし たファイルやサービス内の情報を 公開する範囲を指す場合もある。 公開範囲の名称はサービスによっ てさまざまだが、インターネット 上すべてに公開する「全体公開」、 「一般公開」、SNS上の友人やフォ ロワーまでの「友人までの公開」、 さらにその友人やフォロワーまで の「友人の友人までの公開」、特定 の人物を指定した「特定範囲での 公開」、「限定公開」などがある。 ただし、公開範囲を限定したから と言って、公開範囲のユーザの行 動によっては、その情報が完全に 秘匿されるわけではないので注意 が必要である

.....67,144

■ 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 カーとも呼ばれる。本書では「ハッ カー」そのものは悪意があるかど うかとは関係が無いので、とくに 攻撃を行うものとして「攻撃者」と する。イントロダクション2(P.15) 参照 =アタッカー。≒クラッカー \cdot 15, 16,17,18,19,20,21,22,27,29,3 1,34,35,36,38,41,45,48,49,55,56, 57,58,61,62,84,88,90,91,94,95,97 ,99,100,101,105,107,108,110,111 ,112,113,114,116,117,118,119,12 0,121,122,123,124,125,126,128,1 29,132,133,135,139,145146,148,1 51,153,154,155,156,157,158,160

■ 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 85,110,111,112,114,115,116,117, 122,132

■ 個人情報

生存する個人に関する情報で、氏 名、生年月日、住所、顔写真など、 特定の個人を識別できる情報を指 す。日本では2005年4月から、個 人情報の有用性を配慮しながら、 個人の権利・利益を守ることを目 的とした「個人情報保護法」が全面 施行され、個人情報の取扱につい て一層厳格になった。また、この 法令に基づき、個人情報の適正な 取扱の確保を図ることを任務とす る「個人情報保護委員会」が存在し

,46,47,49,55,56,67,68,69,84,87,88 ,92,101,105,108,118,120,126,129, 148,151,153,156,160,164,174

■ 個人情報保護委員会

個人情報保護委員会は、個人情報 (特定個人情報を含む)の有用性に 配慮し、個人の権利利益を保護す るため、個人情報の適正な取扱の 確保を図ることを任務とする、独 立性の高い機関。個人情報保護法 及びマイナンバー法に基づき、個 人情報の保護に関する基本方針の 策定・推進や個人情報などの取扱 に関する監視・監督、認定個人情 報保護団体に関する事務などの業 務を行う団体

■ サービス・アプリ連携

インターネット上のサービスやア プリが増えることで、1つのサー ビス、1つのアプリで閉じずに、 他のサービス・アプリと連動して 操作したり、楽しめるケースが増 えている。これを、サービス・ アプリ連携と言う。例えば、X(旧 Twitter)を他のブログサービスと サービス・アプリ連携することで、 Xで投稿した内容を、自動でブロ グサービスの方にも投稿できるよ うになる

■ 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 とく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

.....97,105,133

■ サイバー攻撃

インターネットを通じて、別の企 業や組織、ときに国家を攻撃する 行為の総称。対象は、パソコンや スマホといった個人が利用する1 つの端末から、サーバやデータベー スなどの大規模なものまで、手法 によってさまざまある。ネット社 会となった現代では、インターネッ ト空間をサイバー空間と呼び、そ こでの攻撃、すなわちサイバー攻 撃を舞台とした国家間の争いが起 きている事実がある

14,15,16,17,18,19,20,21,22,23,24 ,28,29.30,31,35, 36,43,44,47,48,5 1,54,55,57,58,60,61,62,63,69,72, 93,95,96,97,115,121,122,125,134 ,135,136,138,139,141,146,147,14 8,149,150,151,152,157,158,159,1 60,163,164,165,167,171,175

■ サイバープロパガンダ

SNSやウェブサイトなどのサイ バー空間においてプロパガンダ(特 定の思想・世論・行動を誘導する 行為)を行うこと。インターネッ トが、人類の生活空間、社会とし て浸透した結果、国家間の争いの 場所にもなった結果、生まれた事 象。フェイクニュースやフェイク サイトを活用した方法など、悪質 かつ狡猾な方法が増えている

......60

■ サプライチェーン

製品の原材料・部品の調達、製造、 在庫管理、配送、販売、消費までの、 製造から流通すべての流れを指す。 大手企業が開発するスマホなどは、 サプライチェーン管理がしっかり されていることが多い反面、その 中の一部でのトラブル(自然災害・ 人工災害)により、製品の供給数へ の影響が大きくなるケースがある 51,148,149,150,152

■ 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

......31.101

■ 常時SSL化

SSL(Secure Socket Layer)とは、 インターネット上でデータを暗号 化して送受信する仕組みの1つ。 暗号化するだけではなく、電子証 明書の利用により、通信者の本人 性を証明することで、なりすまし などの不正利用を防ぐことができ る。「https://」の項で説明したよ うに、Googleの動きに追従する形 で、今は多くのホームページ(ウェ ブページ)で、常時SSL化が推奨、 一般化してきている

■ 情報モラル教育

インターネット普及がもたらした、 爆発的な情報量の増加、また、イ ンターネット上における年齢や経 験、性別など制限のないコミュニ ケーションにおいて、社会規範を 守るために行われる教育。技術の 進化に合わせて価値観が変化する ため、情報モラル教育自体が変化 しており、それに追従していく必 要がある

■ 初期化

使用しているパソコンやスマホの ハードディスクや保存スペースを、 出荷状態と同じ状況にすること。 その中に保存されているファイル

やアプリはすべて削除される。な お、初期化方法によっては、デー タを復元できる場合がある

..... 59,87,97,99,100,154

■ 初期パスワード

パソコンやスマホなどのログイン が必要な機器で、出荷初期の状態 で設定されているパスワード。初 期パスワードは便宜上使われるた め、利用者は入手後、必ず自身の パスワードに変更する必要がある

......95

■ 署名アルゴリズム

安全な接続を行う際に利用される サーバ証明書を確認するときに使 用するもの。SHA-1/2、DESなど の種類がある。SSL化されたホー ムページヘアクセスした際、その ページの証明書が正しいかどうか、 署名アルゴリズムを見ることで確 認できる

■ ショルダーハッキング

パソコンやスマホを操作してい る人物の背後から肩越し(ショル ダー)に覗いて、無断でその人物 の操作画面を盗み見し、さまざま な情報を盗んでハッキング(クラッ キング)することからその名前が 付いた。物理的な攻撃手法の1つ

■ スクリプトキディ

ハッカーのレベルになく、自分で 作らず購入したマルウェアや簡単 なスクリプトを使って悪事を働く、 初心者攻撃者。「スクリプトを使 うこども」の意

......20

■ 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33,104,160

■ 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

■ スパイ

もともとの意味は、国家間などで 秘密裏に動いて、敵対国や競争相 手の情報を得る人物を指す。イン ターネットにおいては、その意味 を踏襲して、インターネットを通 じて他のOSやアプリのセキュリ ティの不具合(セキュリティホー ル)を利用して、無断で侵入し情 報を抜き取ることを意味する。ま た、そのアプリをスパイアプリ・ スパイウェアと呼ぶ。多くのセ キュリティ対策ソフトでは、既知 のスパイアプリ・スパイウェアの チェックが可能で、侵入されてい る場合、検知可能となる

......14,20,42,48

■ スパムメール

もともと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 りとりできる腕時計型の機器

......42,102

■ スマート家電

単独でネットに接続して、なんら かの情報をやりとりしたり、動作 の指示を受け付けられる家電機器30,58

■スマートフォンを探す

Googleアカウントに用意されて いる、使用しているスマホを探す 機能。対象となるスマホでログ イン中の Google アカウントを インターネット経由で認識し、 そのスマホの位置情報を確認で

■ぜい弱性

狭義ではセキュリティホールと 同義で、「ソフトウェア等にお けるセキュリティ上の弱点」と される。広義では、セキュリティ ホールを含めた、管理体制や人 的ミスなども含めたシステム環 境全体における欠陥とされる

30,59,94,148,150,153,154,158

■ 生成 AI

学習データをもとに、テキストや 画像など新たなデータを生成する AIのこと。これまでのAIが、イン プットされた画像や音声などのデー タについて、おもに推理や判断を 行っていたのに対し、生成AIは自 ら新しいデータを生み出すことが できる。2020年代から、急速に普 及・拡大している。

......22,62,63

■ 生体認証

パソコンやスマホなどを利用する 時の本人確認を、指紋、虹彩、静脈、 顔の形など、本人の生体の一部分 を用いて認証すること

..... 25,27,28,33,34,42, 43,48,83,89,101,102,108,109

■ セキュリティ・バイ・デザイン

インターネットやデジタルの普及、 社会への浸透が進む中、企画・設 計段階からセキュリティ仕様を準 備し、セキュリティ確保を事前に 意識して開発を進めるシステム開 発手法。出来上がったものを守る、 ではなく、あらかじめ堅牢なもの を作る、という思想

■ セキュリティキー

無線LANに関するものの場合→「暗 号キー」、物理的なものの場合→ 「USBセキュリティキー」

.....99,108

■ 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

.... 29,30,48,50,55,59,61,79,91,95, 96,97,121,146,155,157,161,171

■ セキュリティ対策プラン

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

.....48,84

■ 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。アップデー トファイルに含まれる場合もある48,61

■ 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。=ぜい弱性

17,18,21,22,27,29,48,58,61,93,94 ,96,97,121,146,155

■ 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

.....41,58,61,96,125

■ゼロトラスト

基本は「決して信用せず、常に検証せよ」という考え方にもとづき、端末へのアクセスは、常に検証を行い、安全を担保し続けるモデルである。

特定の製品を購入すれば導入できるというものではないため敷居は高いが、興味を持った方は、例えば独立行政法人情報処理推進機構から公開されている文書「ゼロトラストという戦術の使い方」(https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project/zero-trust.html)を参考に、自身の組織で導入できるかどうか検討してみてほしい

■ 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 ブルートフォース攻撃、ブルート フォースアタックともいう

......121

......31,33,99,100,101,107

■ 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心理テクニック。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

...... 21,22,46,49,80,145,151,160

■ 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やウェブサービスのIDを使って、他のSNSやウェブサービスのIDにスにログインして、利用可能にする規格。特定の身分証明書メージを利用できる。所以サービスを利用できる。のpenIDとができる。OpenIDを省くことができる。OpenIDとはぼ同義だが、他にもソーシャをはぼ同義だが、他にもい存在するとはで見える機能は存在する。鍵となるアカウント情報が流出め、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。発生した事象とのものを明確に見たり聞いたり聞いた上で発信しているもでをでいるものを二次ソースという。伝聞など、三次と呼び、次第に信憑性がしているものを二次ソースと呼び、本来の意味とは別のくなったり、本来の可能性が高いなる。なお、プログラムを作るしなの設計ファイルもソース(もしくはソースコード)と呼ばれる

......39,66,146,147

■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)

......22,29,33 ,44,45,50,53,55,61,92,97,104,110, 116,118,123,139,158,172

■ ソフトウェアトークン

多要素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

.....14,101,102,108

■ ダークウェブ

ダークウェブとは、日常的に利用されているウェブサイトと異なり、匿名性の高いネットーワーク上に構築された、主として犯罪や国家間の争いに利用されるウェブサイトの総称。Google や Yahoo! などの検索エンジンでは見つけられず、特別な条件でアクセスできる URL やアクセス方法が紹介される

..... 57,72,127,151,153,156,160

■ 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 …… 25,27,34,43,45,56,83,91,101,102,103,108,110,121,133,153,157,158

■ 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

■ 中間者攻撃

インターネット上の通信において 通信している2者の間に入り、両 者がやりとりする情報のすり替え やなりすましにより、情報の盗聴、 不正利用など、通信上で悪意ある 攻撃を行う手法。保護されていな いインターネット回線など、信頼 できない通信経路上で被害に遭う 可能性が高くなる

■ 著作権侵害

......71

| ■ 通信の秘密 | ■ データの移行 | ■ トラッシング |
|-------------------------------------|-------------------------------------|-------------------------------------|
| 個人間の通信の内容およびこれに | スマホの機種変更をはじめ、使用 | ゴミ箱に捨てられた紙などから重 |
| 関連した一切の事項について、公 | している端末を替える際に、それ | 要な情報を探し出すソーシャルエ |
| 権力や通信当事者以外の第三者が | まで使用していた端末に残ってい | ンジニアリングのテクニック |
| これを把握すること、および知り | るデータを、新しい端末へ移すこ | 22 |
| 得たことを他者に漏らすなどを禁 | と。最近のスマホでは、まったく | |
| 止すること。通信の自由の保障と | 同じ状態でのデータ移行がしやす | ■ 内閣サイバーセキュリティセン |
| 対で考える必要がある | くはなっている。ただし、端末に | 9 — |
| 123,124 | 紐づくデータは移行できないもの | 正式名称は「内閣官房内閣サイバー |
| ■ 通知ウインドウ | もある 96.97 | 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 |
| ■ 週知ウインドウ パソコンなどで、なんらかの通知 | 86,87 | 別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 |
| を出す表示のこと | ■ テザリング | を行っている機関。国民へのサイ |
| 43 | パソコンなどで、スマホなどを経 | バーセキュリティ意識の啓発も行 |
| | 由してインターネット接続をする | う。通称 NISC。間違われやすい |
| ■ 通知機能 | 方法。スマホをルータとして利用 | が内閣府ではない |
| エラー発生、メール受信、その他 | する方法など | 27,36,37,164 |
| のアラートなどを利用者に通知す | 93,116 | |
| る機能 | | ■ なりすまし |
| 43 | ■ デジタル署名 | サイバーセキュリティにおける「な |
| | 公開鍵暗号技術を利用して、セキュ | りすまし」とは、悪意ある人物が、 |
| ■使い捨てパスワード | リティ性を担保した署名のこと。 | 別の人物になりすましてパソコン |
| 多要素認証などで用いられる、利 | 暗号技術を利用していることで、 | やスマホ、システムを利用し、不 |
| 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 | 安全性が高く、電子契約サービス と合わせて利用することで法的な | 正な行為を行うことを指す。なり すましをされた人物は、自分がまっ |
| 108 | 対力も持つ | たく意図しない操作やコミュニケー |
| 100 | 125 | ションを行われ、ときに犯罪に巻 |
| ■ 使い捨てメールアドレス | | き込まれる場合がある |
| メールアドレスを利用する場合、 | ■ テレワーク | 19,21,22,49,55,56,68,75,77,84,10 |
| 多くの利用者は自分用として使い | 進化したコンピュータや通信イン | 1,112,114,115,125,133,155,157 |
| 続ける。しかし、最近では、フリー | フラなど情報通信技術を活用した | |
| メールサービスなどで、1回だけ | 働き方の総称。従来は、会社(オ | ■二段階認証 |
| 使うメールアドレスなどが入手し | フィス)へ集まって業務を行うが、 | 利用者認証を2回に分けて行うも |
| やすくなっており、これを使い捨 てメールアドレスと呼ぶことがあ | テレワークの場合、自宅や別の場所がなるという。 | の。多要素認証と異なり、同じ認証の要素で2つの段階につけて認 |
| る。継続的に利用しない場合は便 | 所からインターネットを通じて連携を取って業務を遂行できるため、 | 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 |
| 利だが、使い捨てメールアドレス | 時間や場所を有効活用できる。リ | なる要素を組み合わせて2回認証 |
| を利用したインターネット犯罪も | モートワークと呼ぶ場合もある | を行う場合は二要素認証とも呼ぶ。 |
| 横行しており、注意が必要 | 24,134,137,139,142,164 | 同じ要素2回よりは異なる要素2 |
| 127 | , , , , , , , , , | 回の方がセキュリティレベルは高 |
| | ■ 投資詐欺 | くなる |
| ■ ディクショナリアタック | 株などの金融により、将来に向け | 102 |
| →辞書攻撃 | た資産を増やすために行う投資に | |
| 101 | まつわる勧誘や、実際の架空投資 | ■認証局 |
| | などを行う詐欺。インターネット | 申請に基づきSSL証明書の発行を |
| ■ データ消去機能 パソコンやスマホを買い替えた場 | バンキングやインターネット投資 がしやすくなったことで、投資詐 | 審査する機関 119,120,121,124 |
| インコンやスマホを負い皆えた場 合、古い端末を廃棄したり、転売 | がしやすくなうだことで、投資話が 欺の幅が広くなり、被害件数が増 | 119,120,121,124 |
| することがある。その際、その端 | がいった。 えている | ■ ネームドロップ |
| 末内に含まれているデータが完全 | 66,157 | 業務上の上司や立場が上の人間を |
| に消去されていないと、次に渡っ | - 3 ,- 3 | 装って要求を実行させるソーシャ |
| た相手に不測の使われ方をされる | ■ ドライブバイダウンロード攻撃 | ルエンジニアリングの手法 |
| 危険がある。その場合、端末に含 | いずれかのウェブサイトを訪れた | 22 |
| まれるデータを完全に消去できる | だけで、なんらかのプログラム(こ | |
| のが、データ消去機能である。端 | の場合はマルウェア)のインストー | ■ネットワーク暗証番号 |
| 末にあらかじめ用意されている場 | ルが発生する攻撃 | 通信事業者のサービスを利用する |

.....61

際に、利用者が本人であることを

.....99

認証するための暗証番号

合もあるが、ない場合、別の専用

アプリを別途入手する必要がある

.....87

■ 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

......30

■ 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

......99

■ 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

......17

■ 野良 Wi-Fi(のらワイファイ)

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。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時代といない時代をある。暗号化されてのままのものもあるが、攻撃者が情報を詐取するものもある。災間でも観光目的に、運営主体が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。バージョンの整数が上がるものをメジャーアップデート、小数点以下が上がるものをマイナーアップデートなどと呼ぶ

■ ハードウェアトークン

多要素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

......29

......34,101

■パクリ

別の人物が作成したさまざまなコ

ンテンツを真似ること。パクリの表現が使われる場合、多くが無断で真似て、ときにまったく同じ状態で複製し利用する状況となり、元コンテンツに対する著作権侵害となることが多い。ロゴやウェブページの雰囲気(トーン&マナー)など、見た目でわかりやすいものの場合、炎上につながりやすい

■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……………………99

.....71

■パスフレーズ

パソコンやスマホ、あるいはそれらで動くアプリや各種インターネットサービスを利用する際、必要となる認証で利用するパスワードのこと。パスフレーズとは、文字数が多いものを指す

.....99

■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。本書で言う「ログ インパスワード」のみを指す場合 と、暗証番号(PINコード)などや 無線LANを利用する時に入力する 「暗号キー」を含む場合がある。本 書では明確に分けて記述している ···· 11,16,18,21,22,24,25,26,27,30, 31,32,33,34,35,36,40,42,43,48,50 ,55,56,57,58,62,69,75,76,77,83,8 4,86,89,90,95,97,98,99,100,101,1 02, 103, 104, 105, 107, 108, 109, 110, 111,113,115,117,118,119,121,122 ,125,126,127,129,131,133,139,14 1,145,153,161

■ パスワード管理アプリ

インターネット上のさまざまなツールやサービスを利用するにあたり、ログイン情報の管理が煩雑化している。それを解消するのがパスワード管理アプリ(パスワードマネージャー)である。1つのアプリの中で、各ツールのIDとパスワードを理するもので、IDとパスワードを確認するにあたって、生体認証や二段階認証を利用することで、セキュリティを確保する

·· 32,33,102,103,104,105,108,109, 141

■ パスワードの使い回し

パソコンやスマホ、あるいはそれらで動くアプリや各種インターネットサービスを利用する際、必要を使い回すこと。1つのパスワードをさまざまなところで使い回すと、万が一そのパスワードが、悪意べかのアプリで不正利用される危険いのアプリで不正利用される危いしは避けなければいけない

...... 27,35,56,69,77,105,153,158

■ 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

......42,46,83

■ ハッカー

コンピュータに精通し、その方面の高い知識と技術を持つ人を指す尊称で、イコール悪事を行う攻撃者ではない。ハッカー、攻撃者、クラッカーなどの使い分けはイントロダクション 2 (P.15) 参照

.....14,15,16,20

■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。更新された部分だけを追加してバックアップしていく方式は「差分バックアップ」とも呼ばれる

... 18,24,25,26,28,33,44,45,59, 69, 86,87,91,97,103,104,133,150,154 ,159,169

■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ラス方法。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、正規のリリース後それ をわざと残したり忘れたりしてい る場合もある

......148

| ■パッチ |
|------------|
| ≒セキュリティパッチ |
| 61 |

■ 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

......22

■ 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 んど個人情報にまつわるもののた め、正直に答えていると SNS など で探し当てられることもある

■ 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付き合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

...... 17,18,22,28,41,61,125,127, 155,165

■ 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

.....29,30,89,94,113,114

■ 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1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。 \Rightarrow 起動パスワード \Rightarrow BIOSパスワード

......89

■ 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

.....48

■ 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

■ フェイクニュース

SNSが普及してから爆発的に増え た、他人や社会に悪い影響を与え る偽りの情報。最近では、企業や 組織の公式情報、著名人の宣伝、 さらには政治を含めた国家のメッ セージなどでSNSが活用されるこ とが増え、その状況を逆手に取っ て、悪意あるユーザがフェイク ニュースを作成・発信し、自身の 承認欲求を満たしたり、対象となる 人物・企業・組織・国家などに情報 面での攻撃をするケースが増えてい る。フェイクニュースに惑わされ ないよう、日本ではさまざまなレ ベルでのリテラシー教育(情報モ ラル教育)へ注力しはじめている

■ 復元

誤って削除・消去してしまった データや、事故・トラブルによっ て消去されたデータを、再びでき るようにすること。通常、削除・ 消去したデータは復元が難しいが、 最近のパソコンやスマホでは、削

除したデータを一定期間保存して、その期間内であれば復元できる場合がある。なお、パソコンやスマホの本体が故障して消えたデータの復元は、ほぼ不可能となる……25,28,44,86,87,88,92,97,107,130,154

■ 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 59, 99,107,111,112,124,130

■ 不正アクセス

企業や組織で管理されているサーバや、各種インターネットサービスにログイン権限のあるユーザが不正な方法を使ってログインしてアクセスすること。不正アクセスすること。不正アクセスすることが行われると、そのサーバにるが行われるとまざまなデータが行われるさまがデータがが行われるさまがである。日本では、2000年2月に施行された不正アクセス特上等に関する法律(で固く禁止法)により、ことででしている。

...... 19,21,30,34,48,72,75,95,100, 108,129,133,153

■ 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

.....48

■ 不正送金

■ 不正ログイン

パソコンやスマホの起動、また、その後の各種アプリケーションの使用開始時においてID(アカウント)とパスワードを利用してログ

インする際、本人以外の悪意ある 第三者が勝手にログインする行為。 最近では、OSやアプリケーション側でログイン場所やログイン端 末を確認し、通常使用されている 場所や端末と異なる場合に、注意 喚起(アラート)を出すことで、不 正ログインの被害を軽減する仕組 みが用意されている

.....158

■ 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

......55,57,58,148

■ 不明なアプリ

パソコンやスマホで利用できる OSと、その上で動くアプリに関 しては、OS提供側で許可を得ら れたものを正式なアプリとして利 用できる。しかし、中には許可を 得ずに提供したり利用できるアプリと呼ぶ。なお、スマホの場合、 iOS・Androidとも、世の中に公 開する場合は、それぞれApple・ Googleの審査を通ったものしか 配信できない

......38

■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

.....40

■ブラウザ

→ウェブブラウザ …… 29,33,38,93,109,120,122,139

■ 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

......61,93

■ 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

......123

■ 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

.....89

■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

..... 23,69,84,

111,116,123,125,126,166

■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

......118,123,124

■ ホームページ

=ウェブサイト

■ 補助記憶装置

CPUにケーブルなどを介して接続されデータを記録する記憶装置。 ハードディスクや SSD など。これに対してメインメモリと呼ばれ CPUに直結するものを主記憶装置という。→記憶装置

.....44,100

■ ホスティングサービス

ホームページなどを開設するウェブサーバやメールサーバなど、各種サーバを運用するためのスペースを提供するサービス。ホスティングサービス事業者が運営するサーバを利用することで、自身でサーバの管理をする手間が省ける。個人向け、企業向けなど、用途に応じた種類やプランがある

..... 158,175

■ボット

ロボット(robot)の短縮形。さまざまな作業を自動化したプログラムのことでX(旧 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

...... 16,17,18,55,57

■ 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………………………………………18,21,29,55,57,58,94

■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

......131

■ 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

■ 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

■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)。 「Wi-Fi」とも呼ぶこともある。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

...... 17,30,57,84,85,93,96,100, 101,110,111,112,113,114,117, 118,119,122,123,130,132,145

■ 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 57,110,111,112,114,115,116, 117,118,119

■ 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

.......... 30,93,110,112,113,114,145

■ 迷惑メール

受け手が求めず、勝手に送りつけ られる電子メールの総称。迷惑な 電子メール、ということでその名 が付く。迷惑メールには、広告宣 伝を目的にしたものから、詐欺犯 罪目的の「架空請求メール」や「不 当請求メール」、さらにネット攻 撃を目的とした「ウィルスメール」 など、さまざまなものがある

......37,84,166

■ メッセンジャーアプリ

利用者同士でコミュニケーション (メッセージのやりとり)をするた めのアプリ。メールよりも手軽で、 簡単に会話できるのが特徴。日本 ではLINEを筆頭に、テキストでの コミュニケーションに加え、スタ ンプを利用したメッセージのやり とりが増えている

■ 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

.... 16,17,18,19,21,24,28,44,45,47, 59,62,72,91,108,134,146,150,152, 154,165

■ リカバリ

コンピュータを利用している最中 に、ハードウェア以外の部分、OS やファイルが破損し、データが使 用できなる場合がある。このとき、 リカバリという手法により、OSや ファイルの復旧ができる可能性が ある。最近ではこれらを行うリカ バリツールが存在する。また、企 業などでは重要なデータに関して 「バックアップ」という複製を用意 し、トラブルで破損した場合に、 バックアップからリカバリするこ とが一般化してきている。そのほ か、コンピュータに限定せず「回 復する」、「復旧する」といった意 味・ニュアンスで使用される

......44,83,135

■ 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 攻擊

......31,100,101

■ リモートロック

ノートパソコンやスマホなど持ち 運びで使う端末を、遠隔操作して ロック(操作を受け付けない状態 にする)こと。端末のOSやアプリ ケーションによって操作方法はさ まざま。使用している端末を紛失 した際には、まずリモートロック 機能を利用して、悪意ある操作か ら守ることが必要

......84,85

■ 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

......84,85,90,129

■ リンク

ウェブサイトやメール中にある、 クリックすると所定のウェブサイ トにジャンプする(リンクする)状 態に設定されている文字列をさす。 有意な文字列に設定されている場 合もあれば、リンク先のURLの文 字列に設定されている場合もある。 表示されているURLとは別の場所 へのリンクを設定できるため、表 示されているものがイコールリン ク先だとは思わないこと

18,21,22,25,28,36,37,41,50,58,59, 84,103,121,122,125,126,145,155

■ 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、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-タもある

22,30,58,93,94,95,100,110,113,11 4,115,116

■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

......48,50

■ 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

......87,88

■ 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

...... 25,27,31,32,34,35,43,55,75, 86,89,91,96,100,101,104,105,108, 121,133,145,156

■ 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

 \cdots 33,89,90,99,100,101,104,110, 113,125,133,161

■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 スヘログインできなくなった状態。 また、自らの機器を紛失したとき に、誰かが勝手に操作できないよ うにした状態。これを遠隔操作で 行うことを、リモートロックや遠 隔ロックという

...... 25,28,34,42,46,75,81,83, 84,85,90,99,100,101,129,130,145

■ 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 ------43

■ ワイプ

携帯電話やスマホのデータを消去すること。英語のwipe(拭きとる)という意味から、きれいにすることでそのように使われるようになった。最近のスマホやタブレッするいまでは、遠隔操作でワイプの機能が搭載立れていることが多く、紛失・強力を動きがあった端末のデータを遠隔地から消去することで、データの流出リスクを軽減できる

.....99,100

■ ワンタイムパスワード

=使い捨てパスワード34,101,102

NISC関連ウェブサイト、SNS一覧

回緊鎖回

■ 内閣官房内閣サイバーセキュリティセンター(NISC)公式ウェブサイト



https://www.nisc.go.jp/

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。 国民へのサイバーセキュリティ 意識の啓発も行う。通称「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



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。

https://security-portal.nisc.go.jp/

NISCのSNSによる情報発信

■ X(旧 Twitter) 内閣サイバー(注意・警戒情報)





https://x.com/nisc_forecast

フィッシンング詐欺・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。

■ Facebook





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情報を発信している。

■ X(旧Twitter) 内閣サイバーセキュリティセンター公式アカウント





https://x.com/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。