# JANOG サイバーセキュリティBoF 参加者向け用語集

本BoF参加者向けの用語集です。ISP・ホスティング事業者で特有に用いられる業界的な解釈も含みます。一般的な解釈と異なる場合がありますのでその点ご留意ください。

※各用語（）内は読み方

※赤字は2020/1/22 BoF終了後に追記

## ■Abuse関連

| | |
|---|---|
| Abuse（あびゅーず） | 不正使用や乱用などを意味し、インターネット上での迷惑行為やその行為を通報する事業者に設置された窓口のこと。<br><br>本BoFでは、事業者がAbuse（迷惑行為）の通報を第三者から受付けること、またはその迷惑行為自体を示すことがある。 |
| Abuse業務（あびゅーずぎょうむ） | Abuse窓口/部署で第三者からのAbuse通報を受付けて対応する業務のこと。<br><br>対応内容には、対象ユーザの特定、対象ユーザへ通知（警告）、対象ユーザのサービスを一次的に停止する、通報者対応などがある。 |
| 不正申込み（ふせいもうしこみ） | フィッシングサイトの開設やスパムメールの配信など不正に利用することを目的にサービスを申込み（契約）する行為のこと。<br><br>虚偽情報（氏名、住所、TELなど）を用いて申込みされることが多い。 |
| 架電（かでん） | 電話をかけること。ここでは本人確認の手法として申込時に記入された連絡先電話番号に電話をおこない、実際に申込者につながる電話なのかを確認したり、申し込みの意思を確認したりすること。 |

## ■インターネット資源関連

| | |
|---|---|
| ドメイン | インターネット上に存在するコンピューターやネットワークを識別するための名前。 |
| レジストリ | 登録ドメイン名のデータベースを維持管理する機関。 |
| レジストラ | ドメイン登録を希望する者からドメイン名の登録申請を受け付け、その登録データをレジストリのデータベースに登録する機関。 |

## ■通信技術

| | |
|---|---|
| ポート番号（ポートばんごう） | インターネットで通信する際にIPアドレスとセットで使われる識別番号。 |

| | |
|---|---|
| | よく知られている「80:http」「25:SMTP」というのはサーバに接続する際の「宛先(DST, Destinationの略)ポート番号」であるが、送信側も「送信(SRC, Sourceの略)ポート番号(一般に1024以上が使われる)」を使って通信している。 |
| NAT(なっと) | Network Address Translationの略。アドレスを変換する技術。大抵はポート番号とセットで「1つのグローバルIPアドレス」に対して「複数のプライベートIPアドレス」を紐づける技術を指す。その場合正式にはNAPT(Network Address Port Translation) と呼ばれるが、これもNATということが多い。 |
| CGN(しーじーえぬ) | Carrier Grade NATの略。キャリア(通信事業者)の規模で行うNAT(NAPT)。<br><br>NAT(NAPT)は家庭やオフィスなど限られた範囲で使われることが多い技術であるが、インターネットに接続される端末が増加するにつれて新たに割り振られるIPアドレス(IPv4アドレス)が枯渇、少ないグローバルIPアドレスを有効に使うためにキャリアの規模で利用されるNAT(NAPT)の事を特にCGNと呼ぶ。<br><br>スマートフォンなどモバイル回線では多くの事業者が以前からCGNを用いてインターネット接続をを提供している。加えて固定回線でも「IPv4 over IPv6」サービスでもCGNを導入する事業者が多くなっている。 |
| NGN(えぬじーえぬ) | NTTが進めている次世代ネットワークのこと。一般には「フレッツ 光ネクスト」の名称でインターネットに接続するのに使われたり、「ビジネスイーサワイド」の名称で企業ネットワークの構築に使われている。 |
| PPP(ぴーぴーぴー) | PPP(Point-to-Point Protocol)は電話回線などを通しパソコンなどの端末をネットワークにつなげるプロトコル。認証(IDとパスワードで接続を許可すること)を行う方式として、インターネットの接続では広く使われてきた。 |
| IPv6 PPPoE(あいぴーぶいろくぴーぴーぴーおーいー) /IPv6 IPoE(あいぴーぶいろくあいぴーおーい) | IPoE(IP over Ether)とPPPoE(PPP over Ether)は、狭義的には、NTT東西提供のNGN(フレッツネクスト)上でIPv6通信を行う際の方式。NGNはIPv6で構築されており、そこで提供されるIPv6通信は、IPv6用網終端装置を経由しPPP方式で認証を行い通信を行う「IPv6 PPPoE方式」と、NGNのIPv6通信網を直接使い通信する「IPv6 IPoE方式」の2種類がある。 |
| IPv4 over IPv6 (あいぴーぶいよんおーばーあいぴーぶいろく) | IPv6通信上でIPv4通信を流通させる技術。<br><br>IPv6は広大なアドレス空間を持ち事実上IPアドレスを無限に利用することができる。IPv4とIPv6はそのままでは互換性がないが、ネットワークをIPv6で構成し、その上にカプセル化やヘッダ変換したIPv4パケットを通信することで、既存のIPv4通信も可能にしている。<br><br>「v6プラス」「v6アルファ」「transix」等の名称で、NTT東西提供のNGN(フレッツネクスト)のIPoEサービス上で提供している。 |
| SIMカード(しむかーど) | 携帯電話端末に入っている加入者識別符号・電話番号などが記録されたカード。最近ではnano-SIM(幅12.3mm×高さ8.8mm)が多く利用されている。物理的なSIMカードを使わず、内部のチップに情報を書き込むe-SIMと呼ばれる技術も利用され始めている。 |
| MVNO(えむぶいえぬおー) | 仮想移動体通信事業者(Mobile Virtual Network Operator)のこと。いわゆるキャリア(ドコモ・au・SBB等)から携帯電話回線の提供(卸)を受け、エンドユーザ向けに再販を行う事業者を指す。主なサービスには楽天モバイル、UQモバイル、mineo、OCNモバイルONE、IIJ mio、LINE |

| | |
|---|---|
| | モバイルなどがある。キャリアから回線の卸を受け、さらに別の事業者に再販を行う事業者はMVNE(Mobile Virtual Network Enabler)と呼ばれる。 |
| VNE（ぶいえぬいー） | Virtual Network Enablerの略。NGN網(フレッツ光ネクストサービス)上でIPv6接続機能を提供する事業者。ユーザはISPと契約するとVNEよりネットワーク接続提供されることもある。<br><br>2020年1月現在、BBIX、JPNE、インターネットマルチフィード、ビッグローブ、朝日ネット、NTTコミュニケーションズ、フリービット、アルテリアネットワークスの8社がVNEとしてNGN網に接続している。 |
| SMS認証（えすえむえすにんしょう） | サービスを申し込む際登録電話番号と契約者を紐づけるため、登録電話番号にSMS(ショートメッセージサービス)で認証番号を送り、申込ウェブ上で認証番号を入力させること。電話番号を申込者本人が使っていることを確認するための仕組みではあるが、「SMS認証代行アルバイト」等というもので他人がSMS認証を代行するような例があったり、そもそもSMS用SIMは携帯電話不正利用防止法で本人確認が必要とはされていないサービスのため、厳密な本人性確認とは言えない部分もある。 |
| IPジオロケーション（あいぴーじおろけーしょん） | サービスに接続した際のIPアドレスを元に、接続してきたユーザの位置情報を判定する技術。接続元情報を元にたとえば検索結果を変化させることや、サービスの利用を許可・制限することに利用されたりしている。 |

## ■ソフトウェア/コマンド/システム管理関連

| | |
|---|---|
| WordPress<br>（わーどぷれす） | PHP製のCMSの一つ。すべてのCMSの中でシェアはトップを占めており、多くのWebサイトで使用されている。サードパティ製のプラグインやテーマの開発も活発である。一方で多くのユーザをもつことから、WordPressもしくはプラグイン・テーマの脆弱性を狙った攻撃も観測されており、Web改ざんなどの被害が発生している。 |
| CMS（しーえむえす） | Contents Management System の略。ウェブサイトのコンテンツ管理を容易にするウェブアプリケーションの総称で、WordPressもCMSの一種。 |
| root（るーと） | Unix系OSの管理者ユーザー。高い権限を持ちあらゆる操作が可能。 |
| curl（かーる） | HTTP, HTTPSに対応するコマンドラインクライアント。<br>正式には cURLと表記し、シーユーアールエルと読む。 |
| whois（ふーいず） | IPアドレス・ドメイン・AS番号の3つのインターネット資源について利用者を登録したデータベース、またそのデータベースにwhoisプロトコルを用いて問い合わせるコマンドを指して言う。 |
| netstat<br>（ねっとすたっと） | ネットワークの状態を確認するコマンド。Windowsにも存在する。<br>RedHat Enterprise Linux 7系以後のLinux OSでは netstat に代えて ssコマンド, ipコマンドを使用する場合が多い。 |
| RDP（あーるでぃーぴー） | Microsoftt Windows に付属する リモートデスクトップ接続プロトコル。<br>3389番ポートを使用する。 |

## ■不正利用/攻撃手法関連

| | |
|---|---|
| フィッシングサイト | メール等で偽のWebサイトに誘導し、ユーザ情報（認証情報やクレジットカード情報等）を搾取するサイトのこと。 |
| スパムメール | 所謂迷惑メールのこと。<br><br>ウイルスに感染した端末やレンタルサーバを不正に利用して不特定多数に大量に送信されることがある。厳密にはフィッシングメールは含まないが、文脈によっては含む場合もある。 |
| 標的型メール（ひょうてきがためーる） | 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。（引用：NISC インターネットの安全・安心ハンドブック） |
| Bot（ボット） | 自動的・自律的に実行されるソフトウェアやシステムのこと。<br><br>本BoFにおいて脆弱なデバイスが攻撃者によって乗っ取られ、不正なプログラムが仕込まれることをBot化という。 |
| ボットネット | Bot化された大量のデバイスによって構成される集合体。コントロール用Botからの命令でDDoS攻撃等の不正行為に利用されることがある。 |
| 辞書攻撃（じしょこうげき） | 「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。（引用：NISC インターネットの安全・安心ハンドブック） |
| パスワードリスト攻撃/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。（引用：NISC インターネットの安全・安心ハンドブック）<br><br>辞書攻撃と比べて攻撃精度が高い。 |
| 踏み台（ふみだい） | 攻撃者によって脆弱なホスト（IoTデバイス、サーバ、NW機器等）を不正に乗っ取られ、DDoS攻撃用のボットやマルウェア配布サイト等に利用されること。 |

## ■防御技術関連

| | |
|---|---|
| フィルタリング | コンテンツフィルタリング、オプトアウト（解除）可能。スマートフォンや携帯など通信接続元の機器内に設けたフィルタリング機構で処理する場合もあれば、通信事業者の通信設備で処理する場合もある。 |
| ブロッキング | インターネットブロッキング、オプトアウト（解除）不可能。通信事業者の通信設備で処理する場合、通信事業者は通秘への侵害について考慮する必要がある。【参考】「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」 |

| | |
|---|---|
| FW(ふぁいやーうぉーる) | コンピュータやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システムなどのこと。(引用:IT用語辞典 e-Words) |
| WAF(わふ) | Web Application Firewallの略。Webサーバへの外部からの攻撃を検知、防御するシステム。Webサーバとインターネットなど外部との中間に設置され、サーバと外部との通信を監視して、攻撃とみなしたアクセスをブロックする装置のこと。(引用:IT用語辞典 e-Words) |
| IDS/IPS(あいでぃーえす/あいぴーえす) | 不正侵入検知(Intrusion Detection System)と不正侵入防御(Intrusion Prevention System)のこと。<br><br>攻撃パターンマッチング(シグネチャ)でFWで防げない脅威も検知、防御が可能でFWに続けて導入されることが多い。 |
| EDR(いーでぃあーる) | Endpoint Detection and Responseの略。エンドポイント(端末)での検出と対応を主眼においたセキュリティソリューションで標的型攻撃やランサムウェアなどによるサイバー攻撃を検出して対応する。 |
| ATP(えーてーぴー) | Advanced Threat Protectionの略。未知のスパム, マルウェア, ウイルスに対抗することを謳うセキュリティソリューションの一種。 |
| SIEM(しーむ) | Security Information and Event Managementの略。<br><br>セキュリティソフトの一つで、様々な機器やソフトウェアの動作状況の記録(ログ)を一元的に蓄積・管理し、保安上の脅威となる事象をいち早く検知・分析するもの。(引用:IT用語辞典 e-Words) |
| パッチ | ソフトウェア上の脆弱性等の不具合を解消するためのプログラム。 |
| CAPTCHA(キャプチャ) | completely automated public Turing test to tell computers and humans apartの略。人間とコンピュータを判別するテストのことで、文字を変形させた画像を表示させそこに記載されている文字を入力させたり、複数の画像を表示させ特定のものが写っている画像を選択させたり、パズルのーピースをと特定のところにはめるように指示するものなど、機械的な申込を選別するような仕組みを指す。 |

## ■インシデントレスポンス関連

| | |
|---|---|
| インシデント | 望まない、又は予期しない事象で事業者の正常なサービス運営やユーザの情報セキュリティを脅かす可能性が高い事象のこと。<br><br>【インシデントの例】・プローブやスキャンなどの不審なアクセス(Scan) ・送信ヘッダを詐称した電子メールの配送(Forged) ・システムへの侵入(Intrusion) ・フィッシング詐欺(Phishing) ・分散型サービス運用妨害(DDoS) ・コンピュータウィルスの感染(Virus) ・迷惑メール(Spam) ・先進的で執拗な脅威(APT) (引用:JPCERT/CC CSIRTガイド) |

| | |
|---|---|
| インシデントレスポンス | インシデントを検知し、あるいはその報告を受けることにより認知し、影響の拡大を防ぐとともに、情報を収集して分析を加え、インシデントの全体像や原因に ついて把握し、復旧措置や再発防止のための措置を取る一連の活動。（引用：JPCERT/CC CSIRTガイド）<br><br>本BoFではAbuse通報を受領したユーザ側の一連の対応（認知～復旧～再発防止）について示すことが多い。 |
| JPCERT/CC（じぇいぴーさーと・こーでぃねーしょん・せんたー） | JPCERTコーディネーションセンターは、インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内に関するインシデント等の報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっている。特定の政府機関や企業からは独立した中立の組織である。（参考：JPCERT/CCサイト） |
| SIRT（さーと） | Security Incident Response Teamの略。<br>企業や行政機関などに設置される組織の一種で、コンピュータシステムやネットワークに保安上の問題に繋がる事象（インシデント）が発生した際に対応する組織。<br><br>（引用：IT用語辞典 e-Words） |
| CSIRT（しーさーと） | Computer Security Incident Response Teamの略。<br>意味はSIRTと同じ。 |
| SOC（そっく） | Security Operation Center(セキュリティ・オペレーション・センター)の略で、企業などにおいて情報システムへの脅威の監視や分析などを行う、役割や専門組織。（引用：JPNIC インターネット用語1分解説） |
| NCA（えぬしーえー） | Nippon CSIRT Association(にぽん しーさーと あそしえいしょん)の略。<br>日本で活動するCSIRT間の情報共有及び連携を図るとともに、組織内 CSIRT の構築を促進、支援するコミュニティ。（引用：Wikipedia） |
| T-ISAC（てれこむ・あいざっく） | 一般財団法人日本データ通信協会 テレコム・アイザック推進会議のこと。<br>通信サービスの安全かつ安心な運用の確立のため、会員が関連情報を共有・分析する仕組みを構築し、事業者単独では手に負えないサイバー脅威に対してタイムリーな対策をとることを目的に設立。（引用：T-ISAC-J HP） |
| ICT-ISAC （あいしーてぃ・あいざっく） | T-ISACを母体としてネットワークのセキュリティ確保のために、ISPを含む通信事業者、放送事業者、ソフトウェアベンダー、情報提供サービス事業者、情報関連機器製造事業者を含む幅広い分野の事業者が情報収集・分析および対応について情報共有し、業界の枠を超えて連携・協調する組織として脅威に対処する目的で2016年7月に設立。（参考：ICT-ISAC HP） |
| NISC（にすく） | National center of Incident readiness and Strategy for Cybersecurityの略。<br>内閣サイバーセキュリティセンターのこと。<br>サイバーセキュリティ基本法に基づき、2015年1月、内閣官房に設置された。 |
| NOTICE（のーてぃす） | 総務省、国立研究開発法人情報通信研究機構（NICT）及びインターネットプロバイダが連携し、IoT機器へのアクセスによる、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行う取組みのこと。 |
| 認定送信型対電気通信設備サイバー攻撃対処協会（にんていそうしんがたたいでんきつうしんせつびさいばーこうげきたいしょきょうかい） | 総務省が平成30年5月23日に公布された改正電気通信事業法において、電気通信事業者がDDoS攻撃等のサイバー攻撃への対応を共同して行うため、サイバー攻撃の送信元情報の共有やC&Cサーバの調査研究等の業務を行う第三者機関（認定送信型対電気通信設備サイバー攻撃対処協会）を総務大臣が認定する制度を創設。<br>認定送信型対電気通信設備サイバー攻撃対処協会としてICT-ISACが認定されている。<br>（参考：総務省 報道資料）<br>長くて覚えていない・舌が回らない・会話を急ぎたい時に「認定協会」さらに「認協」と略す事が |

| | |
|---|---|
| | 多い。 |
| パブモニ | パブリックモニタリングの略。<br>一般的に公開されている情報を情報源にして調査を行うこと。Open Source Intelligence の一種。 |
| テイクダウン | サイバー攻撃を行うサイト・ホスト・ドメイン・ネットワーク等を停止すること。 |

## ■法規関連

| | |
|---|---|
| 通秘（つうひ） | 通信の秘密のこと。憲法第21条は、公権力による積極的知得行為の禁止と通信業務従事者による漏洩行為の禁止という二つの面を定めたもの。<br><br>何人も通信の秘密を侵害することは電気通信事業法で禁止され刑罰が規定されており、加えて電気通信事業者の取扱中に係る場合はより厳しい罰則となっている。なお、通信の秘密を侵害してもよいのは「通信当事者による有効な同意」もしくは違法性阻却事由（「正当業務行為」「緊急避難」「正当防衛」）に当てはまる場合に限られるというのが一般的な認識である。 |
| プロ責（ぷろせき） | プロバイダ責任制限法、正式名称「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」の略称。インターネット上の掲示板などで行われた名誉棄損や著作権侵害といった行為で権利侵害を被った被害者が、コンテンツ事業者やISPに対し発信情報の削除や加害者(情報発信者)の情報開示を求めることができると定められた法律。 |
| NDA（えぬでぃーえー） | 秘密保持契約のこと。取引を行う上で知った相手方の営業秘密や顧客の個人情報などを、取引の目的以外に利用したり、他人に開示・漏洩することを、禁止する契約のこと。 |
| 照会（しょうかい） | 公的機関が、業務遂行のために必要な事項について他の役所や民間企業や団体に報告を求めることができるという規定を元に行う問合せのこと。<br><br>サイバーセキュリティ関連では警察が刑事訴訟法197条2項に基づいて発付する「捜査関係事項照会書」の数が多いため、特に断りなく「照会」と述べる場合これを指す。 |
| 差押え（さしおさえ） | 国家権力によって特定の有体物または権利について、私人の事実上・法律上の処分を禁止し、確保すること。<br><br>差押えには民事・行政・刑事の種類があり、サイバーセキュリティ関連では刑事手続において裁判官の発する差押令状に基づく「通信記録の差押え」を指すことが多い。 |

## ■その他

| | |
|---|---|
| 脆弱性(ぜいじゃくせい) | OSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のこと。 |
| BoF（ぼふ） | Birds of Feather の略。JANOGでは「同じ関心を持つ者同志であつまって、ディスカッションをしましょう！」というプログラムを BoF と呼ぶ。<br>みんなぜひBoFに参加してディスカッションをしましょう！ |