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

■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。 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。 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。 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。

■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。 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。フィッシングメールもスパムメールに含まれることがある。
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。 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）
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。 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。 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。

■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。 【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） 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。 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。 （引用：IT用語辞典 e-Words）
CSIRT（しーさーと）	Computer Security Incident Response Teamの略。 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(にっぽん しーさーと あそしえいしょん)の略。 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。 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（えぬあいえすてぃー）	National center of Incident readiness and Strategy for Cybersecurityの略。 内閣サイバーセキュリティセンターのこと。 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	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。 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。 （参考：総務省 報道資料）
パブモニ	パブリックモニタリングの略。 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。

■法規関連

通秘（つうひ）	通信の秘密’（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。 電気通信事業者の取扱中に係る通信の秘密については電気通信事業法等で罰則が規定されている。（要約：Wikipedia「通信の秘密」）
プロ責（ぷろせき）	プロバイダ責任制限法・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。
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。

■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。