

見出し	表（ワード）	裏（解説）	対策、注意点等
A～Z	D o S 攻撃 / D D o S 攻撃	大量にアクセスするなどしてサーバに負荷をかけてサービスを停止させるサイバー攻撃	犯罪です（電子計算機損壊等業務妨害等に該当し、5年以下の拘禁刑等に処される可能性があります。） 当該企業のほか、社会にも大きな迷惑をかける可能性があります。絶対にしてはいけません。
	Hello, World!	print("Hello, World!")で出力される文字	Python等のプログラミング言語で「Hello, World!」と表示させるコードです。プログラミング言語や通信記録（ログ）が読み解く能力は、セキュリティ対策に活用できます。
	I P アドレス	スマホ等の各機器に割り当てられ、「インターネット上の住所」と例えられている情報	インターネットで通信をした際にはどこからアクセスされたかのログ（記録）が残ります。 「匿名だからバレない」ということはありません。
	V P N	データを安全にやり取りするための暗号化通信技術で「仮想トンネル」などに例えられる	V P N機器の脆弱性を放置することでサイバー攻撃の標的とされることがあります。常に最新の状態を保ち、多要素認証を取り入れる等、認証を厳格に行いましょう。
あ	アップデート	スマホ等の不具合を修正したり機能を追加して、最新の状態にする作業	多くはセキュリティ強化や不具合の修正、新機能の追加の際に行われます。更新の通知があれば、設定画面やアプリストアから更新を行いましょう。
	ウイルス対策ソフト	スマホ等を悪意のあるプログラムから保護するセキュリティツール	フィッシング対策など様々な機能を有したものがあります。必要性や自身にあったものかどうか、検討をしてみましょう。 ただし導入をしたからといって全ての被害を防げるものではないため、自身の被害防止対策を怠らないようにしましょう。
	炎上	S N S等の投稿に対し、不特定多数の人から批判や非難のコメントが殺到し、収拾がつかなくなる状態	不適切な投稿は、ちょっとしたきっかけで大きく炎上します。 S N Sの利用にはリスクと責任が伴います。正しい使い方について、よく考えて利用しましょう。
	オフラインバックアップ	ネットワークに接続されていない記録媒体にデータを保存する手法	ランサムウェアによる暗号化やサイバー攻撃の波及を防ぐためにはオフラインバックアップが重要です。
	オンラインゲーム	離れた場所にいるプレイヤーと一緒にできるゲームの総称	悪意のある人と繋がってしまうことで犯罪被害に巻き込まれることもあります。うっかり個人情報を流出させてしまうことがないよう、十分に注意しましょう。
さ	生成A I	指示に従って文章や画像などを作り出す人工知能	利用者が入力したデータを学習データとして利用することがあります。学習されて困るものはオプトアウト（学習拒否）を行いましょう。
た	チートツール	ゲームのデータを不正に改ざんして攻略しやすくするソフトウェア	使用すると、アカウントの停止だけでなく、ウイルス感染のおそれもあります。 また、運営会社の業務を妨害したとして逮捕されたり、損害賠償請求されることもあります。
	チケット詐欺	S N Sなどで「チケット売ります」などとだまして、お金をだまし取る手口	チケット譲渡や売買は公式のチケットトレードサイトを利用しましょう。 また、悪用のおそれもあるので、むやみに自分の個人情報や身分証明書の画像を送らないようにしましょう。
	著作権	小説、音楽、写真などの「著作物」を創作した人に法律で自動的に与えられる権利	著作権者の許可なく著作物（映像、写真、画像、音楽等）をインターネット上に流通させる等をしてはいけません。 フリー素材にも著作権が存在します。利用のルールや条件をよく確認しましょう。
	デジタルタトゥー	インターネットに一度でも流れた情報は完全には消せないこと	少しの間だから、友達しか見れないから、は命取り！一度ネットに出た情報を完全に消すことは困難です。

見出し	表（ワード）	裏（解説）	対策、注意点等
な	偽・誤情報	人を欺く意図的なウソの情報や、勘違い・誤解による誤った情報	インターネットの中は正しい情報ばかりではありません。 偽・誤情報に惑わされないように、情報の確認をしっかりと行いましょう。
	ネットいじめ	ネット、SNSなどを悪用し、誹謗中傷や仲間外れをして心を傷つける行為	SNS等への軽い気持ちの投稿が、相手を深く傷つけてしまったり、罪に問われることがあります。 見た人、受け取った人の気持ちをよく考えて利用しましょう。
	ネットリテラシー	インターネットを安全に使うことが出来る能力や知識	インターネットの特性、危険性を正しく理解し、上手に使うことができる知識・能力を身につけましょう。
は	フィッシング	偽のサイトに個人情報などを入力させて情報をだまし取る手口	本物と偽物の区別は困難なため、事前に登録しておいたブックマークや公式アプリからの接続を習慣づけましょう。
	フィルターバブル	ネット検索履歴などから自分の関心のある情報だけが表示される現象	偏った情報ばかりが表示されるため、思考に偏りができたり、偽情報などを誤信してしまう危険性があります。表示されているものがパーソナライズされた情報であることを認識しましょう。
	不正アクセス	第三者が正規の使用者になりすましてログインすること	パスワードの強化や多要素認証の設定などで、被害を防止しましょう。 また、興味本位でも他人のアカウント等に不正にアクセスすれば犯罪となります。絶対にしてはいけません。
	プロバイダ	インターネットに接続する役割を担う事業者	ネット上の書き込み等で権利の侵害を受けた被害者は、プロバイダ等に対して発信者情報の開示を求めることができます。
ま	マルウェア	スマホ等に被害をもたらす、悪意のあるソフトウェア	メールのリンクや添付ファイルはむやみに開かないようにしましょう。感染するとデータ流出や金銭被害等につながります。
や	闇バイト	SNSなどで「簡単なアルバイト高額報酬」などとだまして、犯罪等に加担させる行為	闇バイトは犯罪です。 「簡単に高額を稼げる」等の甘い言葉に注意しましょう。 少しでも怪しいと思ったら、周りの人や警察に相談しましょう。
ら	リアルマネートレード	ゲームのアカウントやアイテムなどを現実のお金などで売り買いする行為	多くの場合、運営の利用規約等でリアルマネートレードは禁止されています。 取引の際、詐欺被害に遭ったり、アカウントが乗っ取られる等の被害も発生しています。
わ	ワンクリック詐欺	ページにアクセスしただけで契約が成立したと見せかけ、お金をだまし取る手口	利用規約や利用料金、契約内容の確認と同意がない場合、支払い義務はありません。突然料金請求画面が表示されても、支払うことなく、表示された電話番号にも電話をしないでください。

見出し	表（ワード）	裏（解説）	対策、注意点等
A～Z	I o T	家電、車、センサーなどをインターネットに接続し、相互にデータをやり取りする仕組み	家庭用IoT機器がマルウェアに感染し、知らぬ前に犯罪行為の踏み台とされることがあります。初期設定の見直し、こまめなアップデートを行いましょう。
	S E Oポイズニング	悪意のあるサイトをネット検索結果の上位に表示させるサイバー攻撃	クリックする前にドメイン等に不審点がないか、よく確認しましょう。偽ショッピングサイトでは、不自然に安い値段設定をしている場合が多いです。よく利用するサービスは、あらかじめブックマーク登録をしておきましょう。
	S N S型投資・ロマンス詐欺	S N Sを介して投資目的や出会い目的から金銭をだまし取る手口	実際に会ったことのない人からお金の話が出たら詐欺を疑いましょう。また、送金、入金前には家族や周囲の人に相談しましょう。
あ	暗号資産	インターネット上でやり取りできる物理的な実体がない電子的な財産的価値	暗号資産交換業者は金融庁への登録が義務付けられています。無登録の業者でないか、よく確認しましょう。
	インフォスティーラー	インターネットブラウザに保存された I Dやパスワードを盗み取る手口	WEBブラウザに認証情報を保存しないようにしたり、多要素認証を取り入れる等して被害を防ぎましょう。
	エコーチェンバー現象	自分と似た意見の人とばかりつながり、それが正しいと思いこんでしまうこと	人間は「自分が欲しいと思う情報を求めたがる特性」があります。S N S等から得られる情報だけで決めつけず、自分が見ている情報が世の中の全てではないことを意識しましょう。
か	拡張子	ファイル名の末尾についている「.（ドット）」から始まる文字列で、ファイルの種類や形式をP C等に伝える役割がある部分	拡張子を偽装しマルウェアに感染させる手口があります。メールに添付ファイルがある場合には、拡張子の確認はもちろん、身に覚えのないものでないか、送信元等もよく確認しましょう。
	クイッシング	偽の二次元コード(Q Rコードなど)から、悪意のあるサイトへ誘導する手口	正規な二次元コードの上に偽の二次元コードが書かれたシールが貼られていることも。読み取ったコードの接続先U R Lに不審点がないか、確認しましょう。
さ	サイベアーの絵	埼玉県警察サイバー局 公式マスコット サイベアー	埼玉県警察サイバー局の公認キャラクターです。無断掲載、不適切な使用等は著作権法等の法令違反に該当する場合があります。
	サプライチェーン	原材料や部品の調達から、消費者の手元に届くまでの一連の「モノの流れ」	対象の企業等を直接攻撃するのではなく、サプライチェーンのセキュリティ対策が手薄な取引先・子会社などを経由して攻撃をすることを「サプライチェーン攻撃」といいます。自社のセキュリティ対策だけではなく、相手方のセキュリティ対策の確認も重要です。
	サポート詐欺	偽の警告画面を表示させ、ウイルスに感染したと思わせてお金をだまし取る手口	慌てず画面を消して、周囲の人に相談しましょう。画面に表示された電話番号に電話をしてはいけません。
	シャドー I T	従業員が会社や組織の許可ないアプリなどを勝手に仕事で使うこと	情報漏洩等のリスクがあります。企業のガイドラインをよく確認しましょう。
	脆弱性/セキュリティホール	O Sやアプリ、W e bサイトなどに存在する「セキュリティ上の弱点（欠陥）」のこと	放置すると、悪意ある攻撃者による不正アクセス、ウイルスに感染、個人情報流出等のリスクがあります。アップデートの通知や公表があった際は、必ずアップデートを行いましょう。
	ゼロデイ攻撃	脆弱性が発見されてから修正プログラムが出る前に行われるサイバー攻撃	O Sやソフトウェア、周辺機器は最新の状態を保ち、安易にメールのリンク、添付ファイルを開かないようにしましょう。通信内容を監視し、異常や不審な挙動を通知等行うセキュリティ技術の導入することも被害を最小化に繋がります。
	ソーシャルエンジニアリング	人間の心理的な隙を突いて情報を盗み出す手口の総称	「緊急」などの言葉は、利用者を慌てさせる犯人の手口！慌てず落ち着いて対処することが大切です。また、のぞき見防止フィルター等で物理的な対策を取ることも大切です。

見出し	表（ワード）	裏（解説）	対策、注意点等
は	パスワード	パスワードを用いずに端末情報で認証する方法	フィッシングに対して耐性があるとされています。ただし、万能ではないので「メールのリンクを安易に開かない」対策を続けましょう。
	ハルシネーション	生成A I が事実とは異なる情報や存在しない情報を生成する現象	A I により出力された情報をそのまま信用せず、事実確認を確実に行いましょう。
	ビジネスメール詐欺/CEO詐欺	会社の偉い人などに成りすました偽メールを送信して、お金をだまし取る手口	送金に関する指示を受けた場合、送信元アドレスをよく確認し、他の手段（電話等）で取引先担当者に送金内容を確認しましょう。この際、メール記載の電話番号は連絡先偽装のおそれがあるため、名刺等で連絡先を確認してください。
	ファイアウォール	不正な通信を遮断するための防護壁	有効に機能させるため、適切な設定となっているか、ソフトウェアは更新されているか確認しましょう。
	ブルートフォース攻撃/総当たり攻撃	パスワードの可能性のあるすべての組み合わせを総当たりして認証を破るサイバー攻撃	推測されやすい文字列、複数のサービスでの使いまわしは避け、長く複雑なパスワードを設定して被害防止しましょう。
	プロンプトインジェクション	A I を騙し、A I が本来禁止されている動作を強制的に実行させる攻撃手法	重大なセキュリティリスクを伴うほか、多くの場合は利用規約違反となりアカウント凍結の対象となります。A I は利用規約に則って利用し、決して悪用してはいけません。
	ボイスフィッシング/ビッシング	電話や音声通話でメールアドレス等を聞き出し、悪意のあるサイト等に誘導する手口	電話で個人情報を求められた際は、公式サイト等で確認した番号に電話を折り返し、事実を確認しましょう。また、公式サイトを事前にお気に入り登録をしておき、安易にメールのリンクを開かないようにしましょう。
	ポッポくんの絵	埼玉県警察公式マスコットキャラクター ポッポ君	2003年10月に、埼玉県警察のマスコットキャラクターとして県民の鳥「シラコバト」をモチーフに誕生しました。無断掲載、不適切な使用等は著作権法等の法令違反に該当する場合があります。
	ポポ美ちゃんの絵	埼玉県警察公式マスコットキャラクター ポポ美ちゃん	2014年2月、女性警察官の「親しみやすさ」をイメージして誕生しました。無断掲載、不適切な使用等は著作権法等の法令違反に該当する場合があります。
ら	ランサムウェア	P Cをロックしたり暗号化して身代金を要求する手口	O Sやソフトウェア、周辺機器は最新の状態を保ちましょう。万が一に備えてオフラインバックアップを取っておくことも大切です。