フィッシング対策協議会
Council of Anti-Phishing Japan

詐欺サイト
被害対応机上演習

version 20231030.04

フィッシング対策協議会　詐欺サイト対処机上演習WG
林憲明

配布資料確認

文書名			概要
事前アンケート			オンラインにて実施 ※事前アンケートは回答をとおして、参加者のスキルを揃える目的も兼ねています。必ず回答しください。
進行用資料（本スライド）	シナリオ1	状況付与	・シナリオ毎に「6つのフェーズ」と「議論を促す質問」により構成されています。 ・「状況付与」は、コントローラーの役割を担う人へ判断を迷わせる追加すべき状況を付与することを目的としています。
	シナリオ2	状況付与	
	シナリオ3	状況付与	
仮想企業設定集（株式会社CAPJランウェイ）			本机上演習では、参加者は「仮想企業設定集」にて示す企業に勤務する従業員として演じていただきます。
ステータスレポート			「被害事案発生時に把握すべき影響項目」と「測定すべきKPI」のテンプレート
事後アンケート			オンラインにて実施

※各配付資料のヘッダ部（左上）に資料の文書名を記載してあります。

黙読タイム（事前アンケート 回答時間）

https://forms.gle/zd2aBUKUggmBbWu67

事前アンケートにご回答ください。
参加者のスキルを揃えるための情報提供をかねています。

フィッシング対策協議会
Council of Anti-Phishing Japan

机上演習（TTXs）の目的

- 「詐欺サイト」（フィッシング詐欺、偽サイト、なりすまし）などサイバー空間においてブランドが無断で騙って行われる犯罪行為について、事業部門を含むすべてのステイクホルダーの危機意識を高める。
- 自組織のブランドを騙る犯罪者が確認された際の備えについて、サイバーセキュリティの観点から評価を行う。
- サイバーセキュリティ・インシデントの情報共有、エスカレーション基準、関連する行動指針を検討する。
- サイバーセキュリティ・インシデント管理構造を検討する。
- サイバーリソースの要求と管理プロセスを検討する。

- **「ステータスレポート」を使って、組織の対象サービス責任者が経営者へ報告することができる。**

机上演習の前提条件

- 参加者が実際の緊急事態に対応しているかのように、既存の計画、ポリシー、手順を評価します。
- 特定された目的を評価・検証するために、もっともらしく現実的なシナリオを作成することに真摯に取り組んでください。
- 個人のパフォーマンスをテストしたり検査したりするものではありません。
- 隠された意図はなく、騙すような質問もありません。
- 参加者の所属部署はご自身で選択し、他の参加者に対して宣言してください。

グランドルール

1. シナリオを批判してはいけない
   - シナリオの穴や矛盾点を見つけようとすることは、混乱を招くだけです。
2. 自分の過去の経験を振り返る
   - 参加者全員で、対応や復旧に向けてどのように協力していくのかについての知識・経験を深めてください。
3. 情報を決めつけない
   - 提供された資料では答えられない質問がある場合は、進行役に尋ねてください。
4. 参加を奨励する
   - 自由に話し、他の人が話しているときはその人を尊重する
   - インシデントが発生しているかのように、自分の役割を意識して参加する。
   - 詳細よりもプロセスと意思決定が重要である。
5. 進行役の仕事は、あなたが解決策を生み出す手助けをすること
6. シナリオは一般的なもので、一般的な部門を使用する
   - あなたの組織に特定の部門がない場合でも、あなたがこの演習から利益を得られると思う部門で代用する。

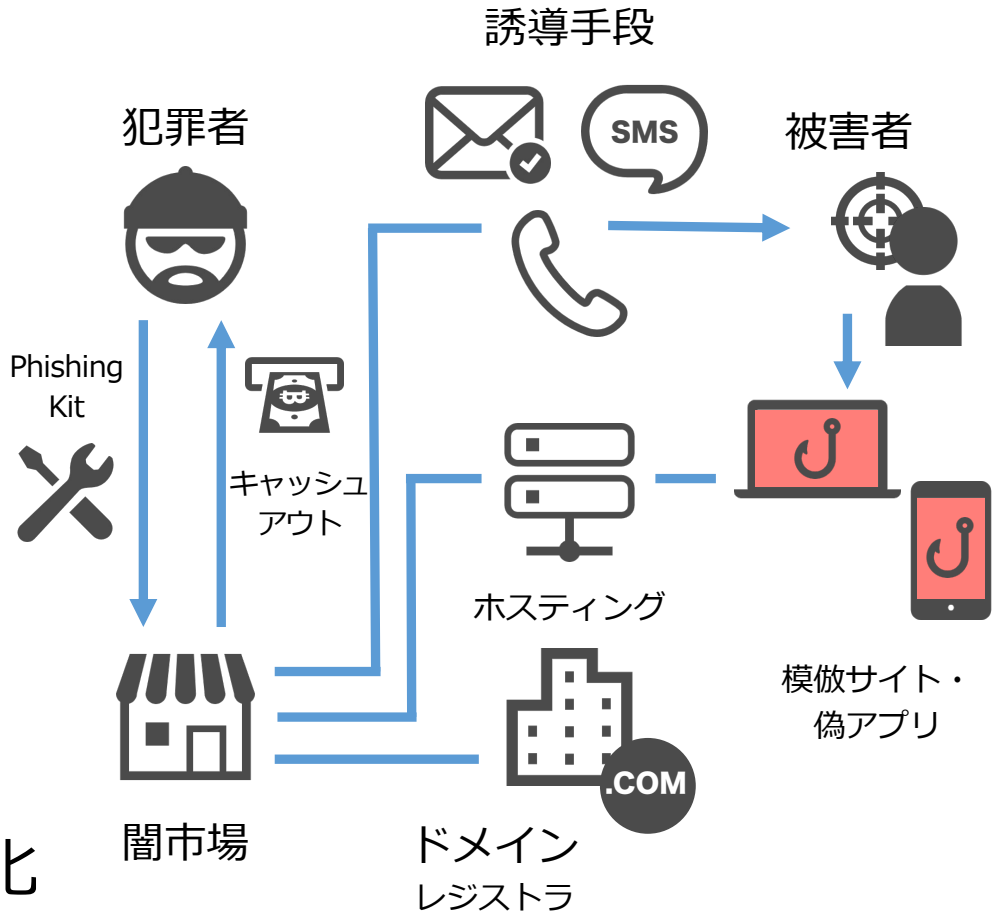
フィッシング対策協議会
Council of Anti-Phishing Japan

脅威の状況

脅威の状況

拡大を続けるフィッシング詐欺被害

- **フィッシングサイトの件数**
  全世界で4,744,699件観測, 年率150%以上*1
- **利用者情報の違法取引が拡大**
  闇市場で最も活性な商品は盗難アカウント
  600フォーラムで4,954,825スレッドを観測*2
- **合理的かつ効率的な利益追求**
  サービス, 配信, マネタイズ 役割の分業, 複雑化



フィッシング詐欺の全体的なプロセス理解が必要不可欠

*1 “Phishing Activity Trends Report, 4th Quarter 2022”. https://docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf
*2 ”Shifts in Underground Markets”. https://documents.trendmicro.com/assets/white_papers/wp-shifts-in-the-underground.pdf

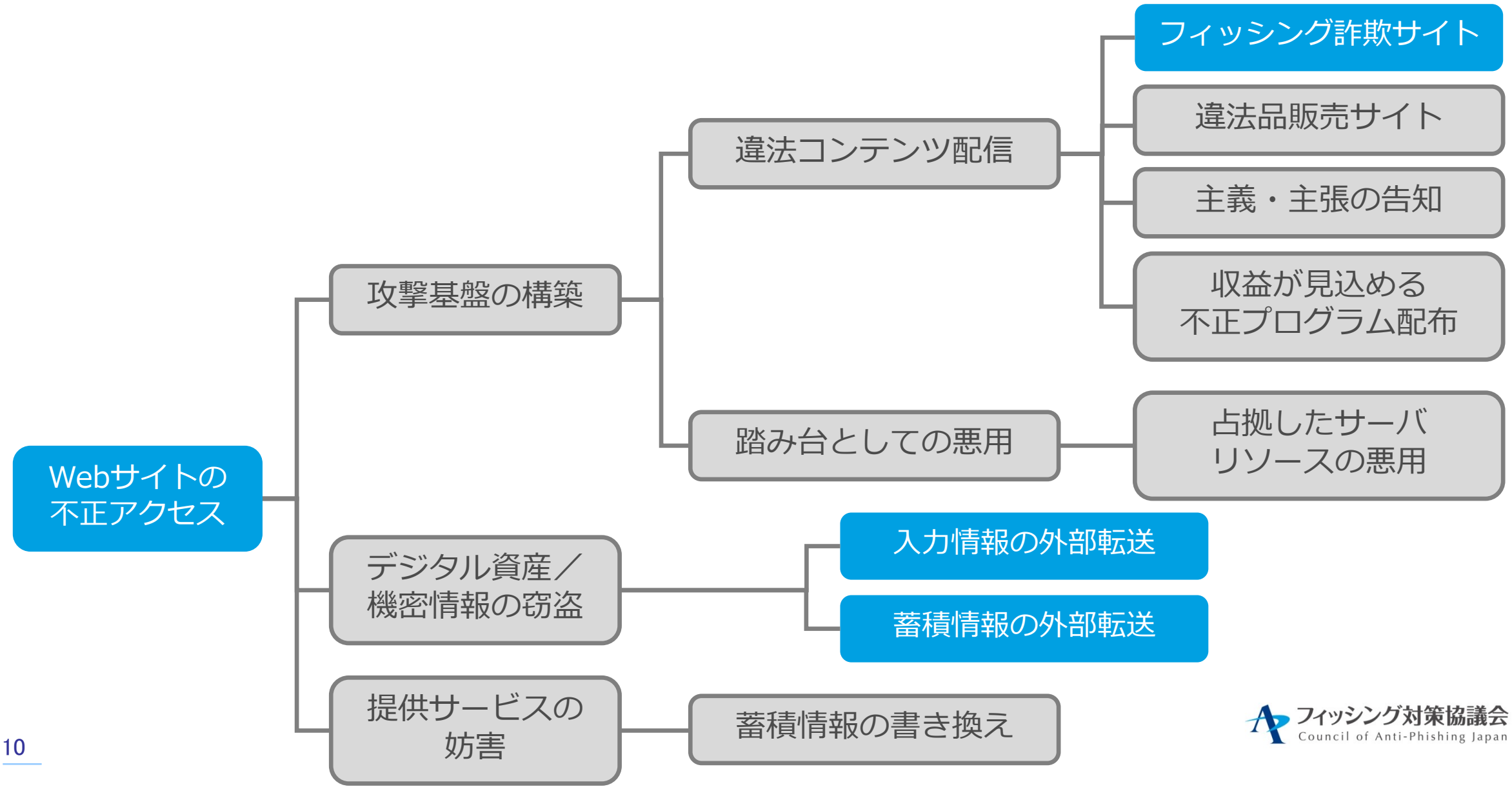
フィッシング対策協議会 Council of Anti-Phishing Japan

ブランドを誤認させる手口を知る

犯罪者は、誤認の恐れがあるブランドを悪意を持って占拠（スクワッティング）し正当な権利者に対し不利益をもたらそうとしている。

手口	詳細
転用	期限切れドメインの取得（ドロップキャッチ） 先取得（新TLD狙い、国際化ドメイン名） 正規サイトのコンテンツを転用（ロゴマーク等のコピー）
転送	インターネット検索エンジンの結果を悪用（ブラックハットSEO） 第三者の正規サイトに無断でコンテンツを蔵置 ソーシャルメディアによる悪意ある広告の拡散 短縮URLで転送先を隠ぺい
外観	タイプミスを狙ったURL（タイポスクワッティング） アルファベットの字形類似（ホモグラフ攻撃） 空白文字の挿入（URLパディング）
概念	例：「KING」を「王」と表記
呼称	英単語のローマ字綴り（例：「COPY」と「KOPI」） ブランド名と文字列のコンビネーション

犯罪者の動機を分析

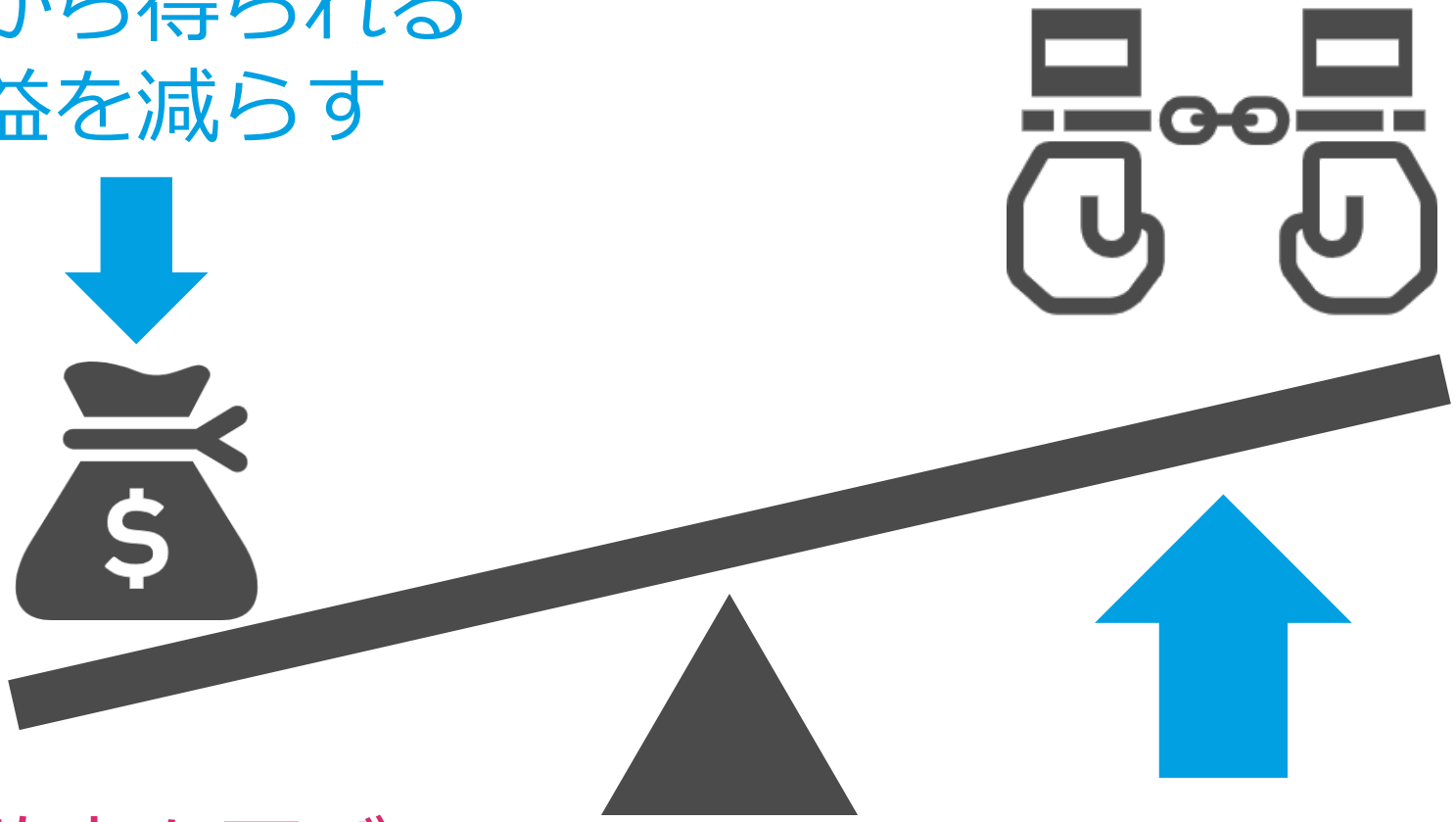

Webサイトの
不正アクセス
攻撃基盤の構築
違法コンテンツ配信
フィッシング詐欺サイト
違法品販売サイト
主義・主張の告知
収益が見込める
不正プログラム配布
踏み台としての悪用
占拠したサーバ
リソースの悪用
デジタル資産／
機密情報の窃盗
入力情報の外部転送
蓄積情報の外部転送
提供サービスの
妨害
蓄積情報の書き換え

フィッシング詐欺の全体的なプロセス

犯罪者は効率的に利益を得るために様々な手法を組み合わせる

犯罪抑止：便益を減らし損出を増やす

犯罪から得られる
便益を減らす



成功確率を下げる

露見時の
損失を増やす

フィッシング対策協議会
Council of Anti-Phishing Japan

フィッシング対策協議会
Council of Anti-Phishing Japan

詐欺サイト対処机上演習

詐欺サイト対処机上演習

「シナリオ」に対して、「ステータスレポート」（「被害発生時に把握すべき影響項目」と「測定すべきKPI」）をまとめ、経営責任者へ報告する対処能力を強化する机上演習

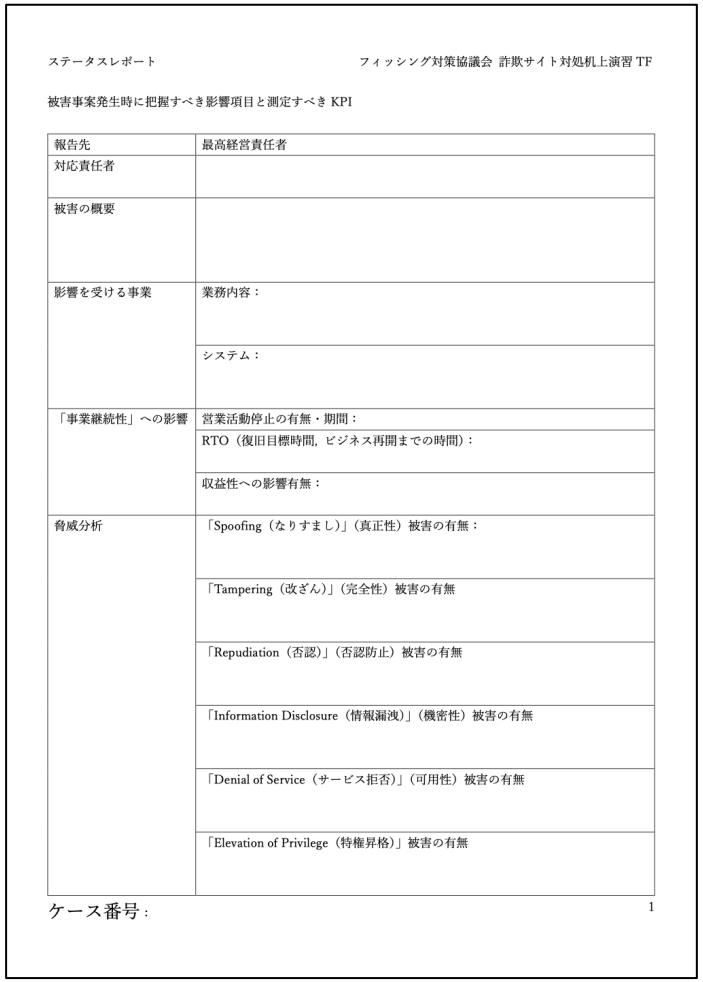
https://www.antiphishing.jp/news/info/tabletopexercise_20230601.html

机上演習の構成

- **「PICERL」サイクル**に基づくフェーズ毎にシナリオを提示
- **ヒント.** 参加者へ議論（当該フェーズにて予め備えるべき項目）を促す質問を提示
- **ヒント.** 「詐欺サイト対処プレイブック」を参照
- 上級編としてさらに成熟度を高めるには何を備えるべきなのかを促す質問を提示
- **ヒント.** 脅威を分析するためのフレームワークとして**「STRIDE」**の項目分析を示唆
- フェーズ毎に内容を検討し、**「ステータスレポート」**を埋めていく。すべてのフェーズを終えたときにレポートの完成を目指す。
- **ゴール. CEO, 最高経営責任者に報告できる状態にすること。**

ステータスレポート

- 「被害事案発生時に把握すべき影響項目と測定すべきKPI」を示したフォーマット

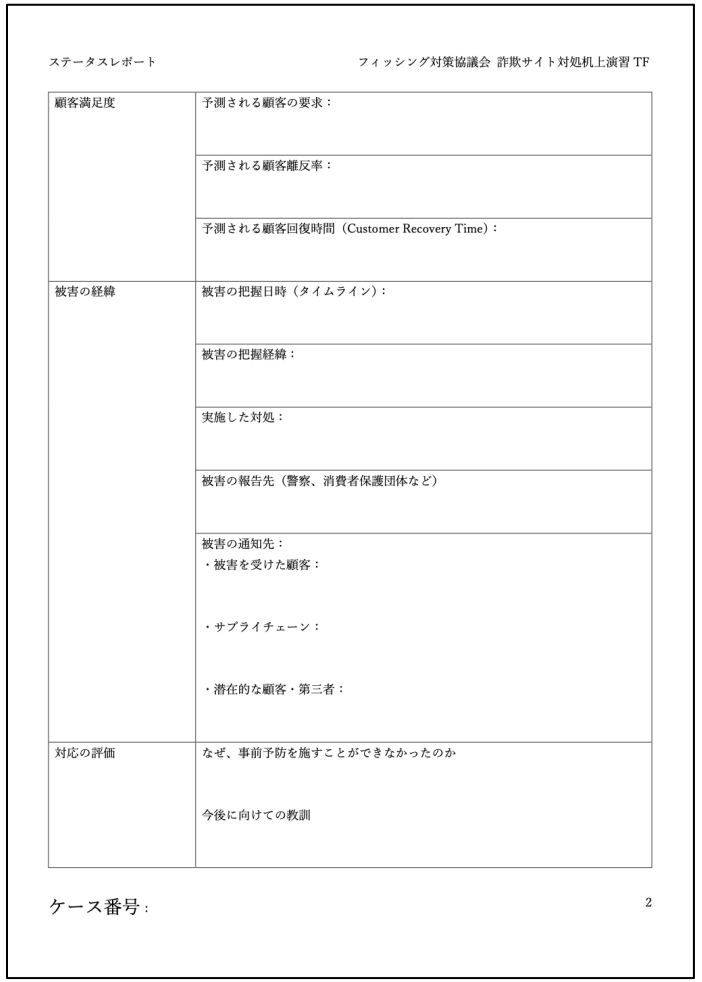


ステータスレポート　フィッシング対策協議会 詐欺サイト対処机上演習 TF

被害事案発生時に把握すべき影響項目と測定すべき KPI

報告先	最高経営責任者
対応責任者	
被害の概要	
影響を受ける事業	業務内容：
	システム：
「事業継続性」への影響	営業活動停止の有無・期間：
	RTO（復旧目標時間，ビジネス再開までの時間）：
	収益性への影響有無：
脅威分析	「Spoofing（なりすまし）」（真正性）被害の有無：
	「Tampering（改ざん）」（完全性）被害の有無
	「Repudiation（否認）」（否認防止）被害の有無
	「Information Disclosure（情報漏洩）」（機密性）被害の有無
	「Denial of Service（サービス拒否）」（可用性）被害の有無
	「Elevation of Privilege（特権昇格）」被害の有無

ケース番号：　1



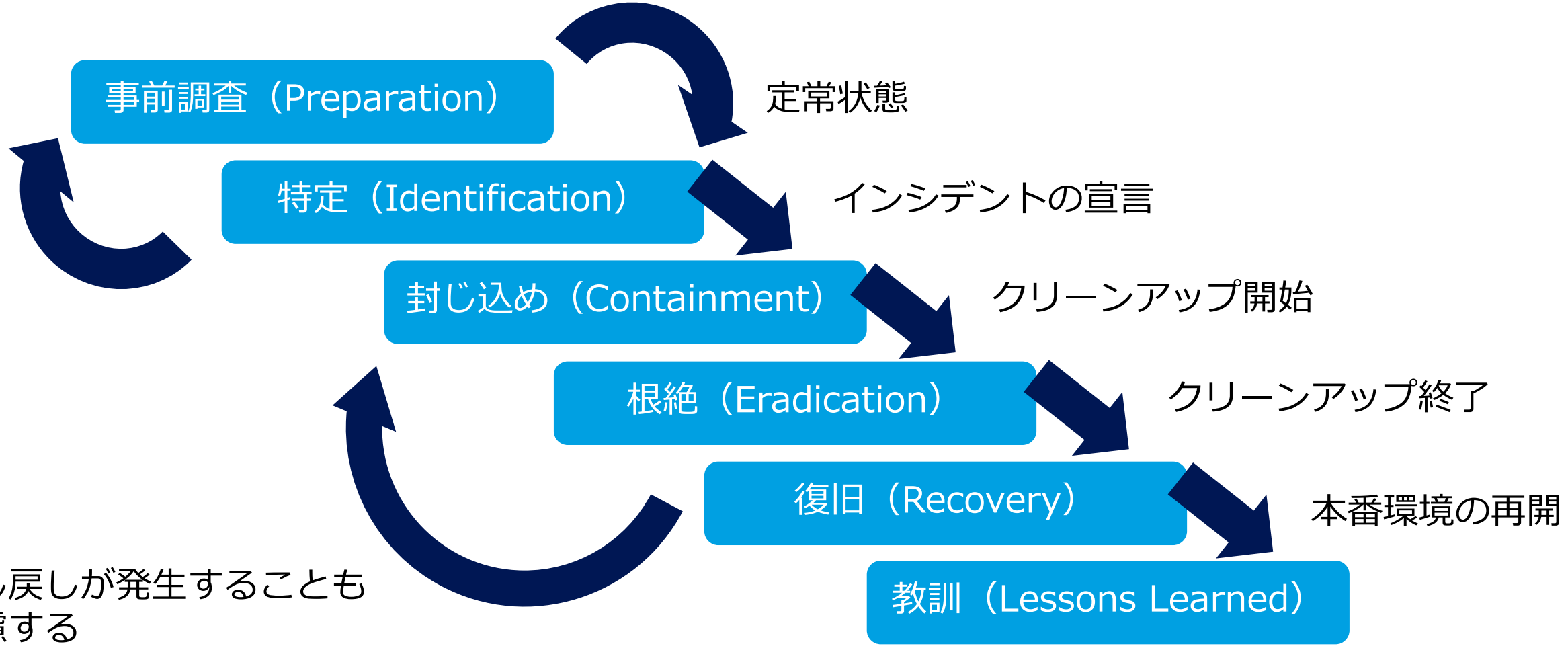
ステータスレポート　フィッシング対策協議会 詐欺サイト対処机上演習 TF

顧客満足度	予測される顧客の要求：
	予測される顧客離反率：
	予測される顧客回復時間（Customer Recovery Time）：
被害の経緯	被害の把握日時（タイムライン）：
	被害の把握経緯：
	実施した対処：
	被害の報告先（警察、消費者保護団体など）
	被害の通知先： ・被害を受けた顧客： ・サプライチェーン： ・潜在的な顧客・第三者：
対応の評価	なぜ、事前予防を施すことができなかったのか 今後に向けての教訓

ケース番号：　2

フィッシング対策協議会
Council of Anti-Phishing Japan

PICERL サイクル フレームワーク



詐欺サイト対処プレイブック

詐欺サイト対処プレイブック　　9月21日 編集　共有

事前調査（Preparation... 10	特定（Identification） 10	封じ込め（Containmen... 5	根絶（Eradication） 4	復旧（Recovery） 2	教訓（Lessons Learned...
利用者へのメール送信における、制作・送信に関するガイドライン（差出人、件名の書き方、表現や用語の統一、問い合わせ先や配信停止などの定型フッター様式、配信時間帯など）が策定され、それに則った運用はおこなわれていますか。	添付ファイルが含まれている場合、メタ情報は収集できていますか。	フィッシングサイトのソースコードについてコンテンツのソースがどのように構成されているのか分析していますか。画像データなどは詐欺サイトローカルに蔵置されていますか。正規サイトからリアルタイムで取得していますか。	「ブランド保護サービス」や事業者特有の文字列を含むドメインの登録状況の監視などフィッシング詐欺検知に有効なサービスの活用は行っていますか。	フィッシング詐欺キャンペーンが発生していることを警告するページはどのタイミングで自社サイトから取り下げますか。もしくは恒久的に掲示するに十分な内容になっていますか。	一連のインシデントに関して は必要ですか。必要な場合、 ムとの連携は行われていま
送信ドメイン認証「DMARC」による、なりすましメールに対する受信制御ポリシー（Quarantine, reject）の有効性と問題点について技術部門・営業部門・マーケティング部門間にて情報を共有できていますか。	PhishTank / VirusTotal にて誘導先のサイトは登録されていますか。 https://www.phishtank.com/https://www.virustotal.com/gui/home/url	フィッシングサイトのソースコードについてデータ転送の観点で分析していますか。どのようなデータが収集対象となっていますか。どのようなプラットフォーム（PHPなど）で構築されていますか。フィッシャーに対してデータはどのように転送が行われていますか。	自社サイトに対する不審なアクセス（favicon.ico や ロゴ/バナー画像に対するダイレクトアクセス、バウンスメールなど）を監視し、詐欺サイトの検知に役立っていますか。	不正なページ（詐欺サイト）や詐欺師のメールアドレスがダウンしていることを確認できますか。	積極的な脅威情報の収集に を担っている部門が担うべき いて組織内にて認知されてい
組織を介さずに発生する脅威・リスク（風評被害、偽サイトなど）について監視・通知する体制を持っていますか。	誘導サイトが存在する場合、タイムスタンプ付きのコピーを取得しましたか（HTTrack ツールなどが使えます）各ページのスクリーンショットを取得しましたか。	詐欺サイトに関連したドメイン管理業者 / ISP・VPS業者 / サーバー証明書認証局 を特定する方法は把握していますか。	積極的な脅威情報の収集（デコイアカウントの作成・監視、アクティブな対抗手段の準備など）について責任を担っている部門はありますか。	＋ 新規	詐欺サイト被害に対する対応 レイブックに関して過去1年 直しは行われていますか。
インシデントを通知すべき機関（所轄官庁、ISP、CSIRT、セキュリティベンダー、法執行機関など）に対する要件やプロセスは整備されていますか。	誘導メールには添付ファイルが含まれていますか。	顧客対応部門（コールセンターなど）に入電した問い合わせに対して、トークスクリプトを用意、展開する手段は用意していますか。	脅威インテリジェンスパートナーから情報を受け取る体制は構築されていますか。		利用者に対して詐欺サイトに 意の「アウェアネス（意識 高めるために継続的に実施し 組はありますか。
利用者または任意の第三者が詐欺サイト被害を認知した際に報告することができる窓口は用意されていますか。	誘導メールにはURLが含まれていますか。	自組織のブランドが騙られた場合、その注意を広域（自社サービス利用者と自社サービスを利用していない人の双方）に対して促す手段を用意していますか。	＋ 新規		
あらゆる部門の従業員が自組織を騙る詐欺サイト被害がくすぶっていることを認知した際に組織の関係者へ通知する手段を持っていますか。	過去24時間の報告内容から、同じ傾向の件名をもつ誘導メールを受け取った宛先メールアドレスの数を数え、影響を受けたユーザーの数を推定していますか。	＋ 新規			
使用するドメインの登録、利用、廃止にあたってガイドラインが策定され、それに則った運用はおこなわれていま	過去24時間の報告内容から、同じ送信元から受け取った宛先メールアドレスの数を数え、影響を受けたユーザーの数を推定していますか。				
	詐欺サイトへ誘導するフィッシングメール/SMSは入手できていますか。				
	詐欺サイト被害を認知した際に誰がそのアクションに対して責任を有しているのか従業員は把握できていますか。				

http://bit.ly/3EVP4NS

フィッシング対策協議会
Council of Anti-Phishing Japan

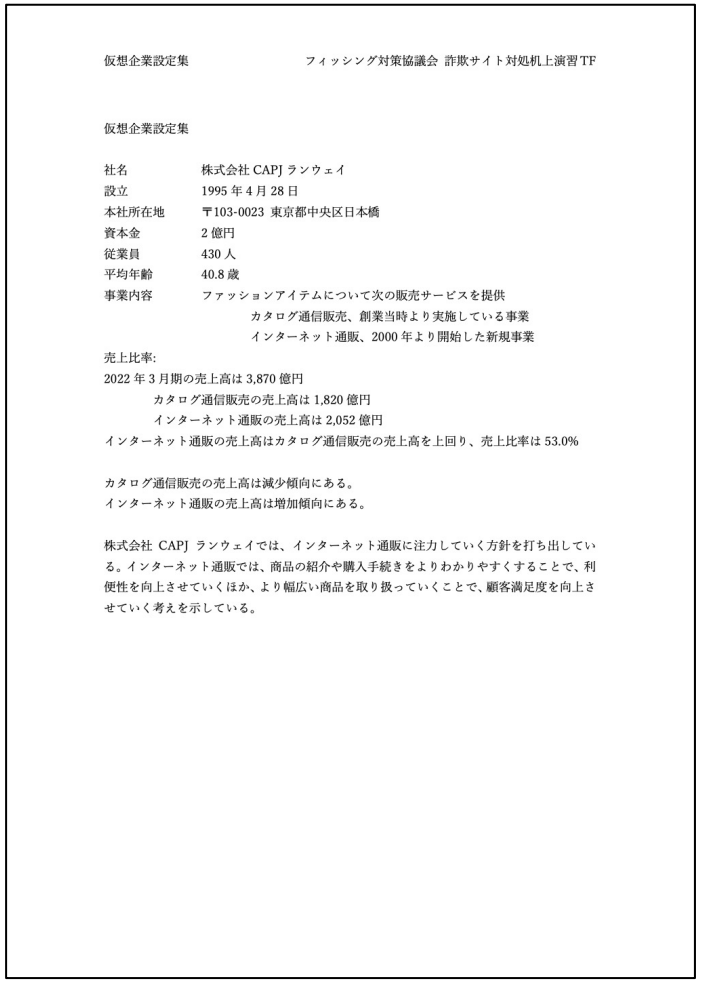
最高経営責任者への報告とは

- **CEOに対して何を知っておいて欲しいのかまとめる**
  - CEOが外部にて当該事件が問われた際に何を発言できるようにすべきなのかレクチャーする
- **CEOに対して何を要求するのかまとめる**
  - 事件の解決には「経営資源」の投入が不可欠
    - 知覚可能：ヒト、モノ（有体物/無体物）、カネ…
    - 知覚不可能：ブランド、組織力、文化形成…

※注意※　「ステータスレポート」を埋めることがゴールではありません。

仮想企業設定集

- 企業規模、事業内容、売り上げ比率、企業戦略
- 主要な部署名と役割、本社とコールセンター（2拠点）の所在地



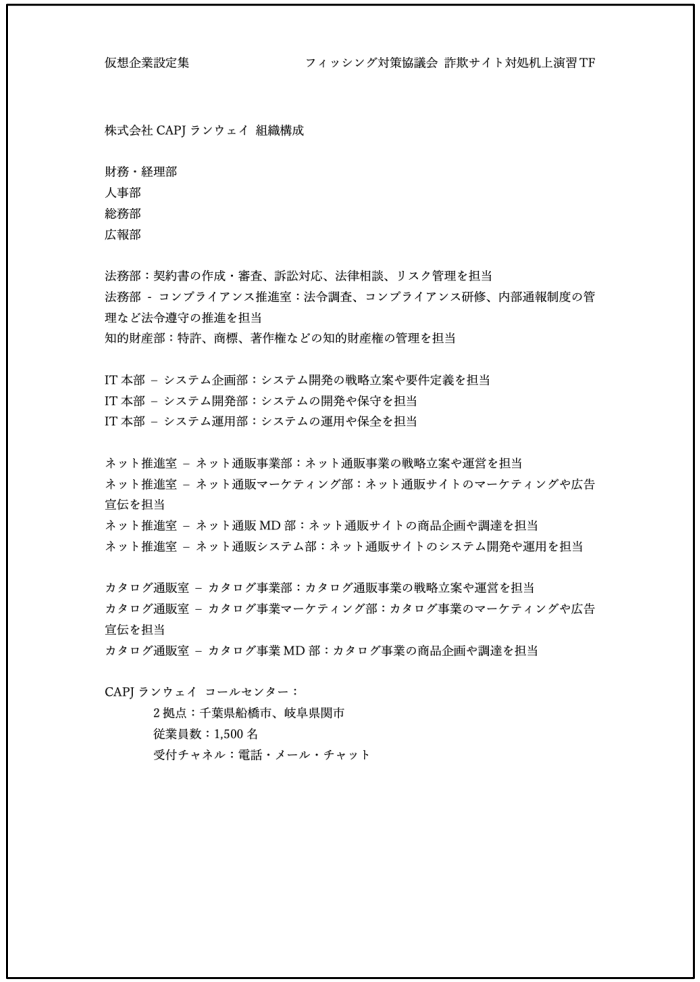
仮想企業設定集　　フィッシング対策協議会 詐欺サイト対処机上演習TF

仮想企業設定集

社名　　株式会社 CAPJ ランウェイ
設立　　1995 年 4 月 28 日
本社所在地　　〒103-0023 東京都中央区日本橋
資本金　　2 億円
従業員　　430 人
平均年齢　　40.8 歳
事業内容　　ファッションアイテムについて次の販売サービスを提供
　　カタログ通信販売、創業当時より実施している事業
　　インターネット通販、2000 年より開始した新規事業
売上比率:
2022 年 3 月期の売上高は 3,870 億円
　　カタログ通信販売の売上高は 1,820 億円
　　インターネット通販の売上高は 2,052 億円
インターネット通販の売上高はカタログ通信販売の売上高を上回り、売上比率は 53.0%

カタログ通信販売の売上高は減少傾向にある。
インターネット通販の売上高は増加傾向にある。

株式会社 CAPJ ランウェイでは、インターネット通販に注力していく方針を打ち出している。インターネット通販では、商品の紹介や購入手続きをよりわかりやすくすることで、利便性を向上させていくほか、より幅広い商品を取り扱っていくことで、顧客満足度を向上させていく考えを示している。



仮想企業設定集　　フィッシング対策協議会 詐欺サイト対処机上演習TF

株式会社 CAPJ ランウェイ 組織構成

財務・経理部
人事部
総務部
広報部

法務部：契約書の作成・審査、訴訟対応、法律相談、リスク管理を担当
法務部 - コンプライアンス推進室：法令調査、コンプライアンス研修、内部通報制度の管理など法令遵守の推進を担当
知的財産部：特許、商標、著作権などの知的財産権の管理を担当

IT 本部 – システム企画部：システム開発の戦略立案や要件定義を担当
IT 本部 – システム開発部：システムの開発や保守を担当
IT 本部 – システム運用部：システムの運用や保全を担当

ネット推進室 – ネット通販事業部：ネット通販事業の戦略立案や運営を担当
ネット推進室 – ネット通販マーケティング部：ネット通販サイトのマーケティングや広告宣伝を担当
ネット推進室 – ネット通販 MD 部：ネット通販サイトの商品企画や調達を担当
ネット推進室 – ネット通販システム部：ネット通販サイトのシステム開発や運用を担当

カタログ通販室 – カタログ事業部：カタログ通販事業の戦略立案や運営を担当
カタログ通販室 – カタログ事業マーケティング部：カタログ事業のマーケティングや広告宣伝を担当
カタログ通販室 – カタログ事業 MD 部：カタログ事業の商品企画や調達を担当

CAPJ ランウェイ コールセンター：
　　2 拠点：千葉県船橋市、岐阜県関市
　　従業員数：1,500 名
　　受付チャネル：電話・メール・チャット

フィッシング対策協議会
Council of Anti-Phishing Japan

シナリオ 1

フィッシング対策協議会
Council of Anti-Phishing Japan

フェーズ 1.

フェーズ 1. – Day 1: コールセンター

11:00

ネット推進室、カタログ通販室の双方に対して、コールセンターより、「Abandoned Rate (放棄率)」（オペレーターにコールがつながる前に何らかの理由で切れてしまったコール率）が異常値を示しているとの報告を受けています。

着信内容を確認したところ、いずれのコールもSMSによる通知に従ってフォームへ情報を入力したところ、エラーメッセージが表示され先に進まないとの報告でした。

※コールセンターは2拠点あり。役割に違いはなし。負荷分散が目的。センターと本社機能は物理的に離れている。

フェーズ 1. 議論を促す質問 1/2

1. コールセンターにおいて異常値が発生した場合の連絡経路は整っていますか。

2. セキュリティ事故と判断する基準を持っていますか。
   a) 疑わしき事象が発生したときに取るべき行動を知っていますか。
   b) サイバーセキュリティインシデントを報告するためのプロセスはありますか。
   c) 経過について報告するための連絡先は設定されていますか。

3. 自社の「なりすまし」が疑われる通知（電子メール、SMSなど）によるインシデントの重大度について基準を持っていますか。

フェーズ 1. 議論を促す質問 2/2

4. 所属組織にて、すべてのITユーザ（管理者及び上級管理者を含む）に対して、基本的なサイバーセキュリティ及び／又はITセキュリティ意識向上トレーニングを実施していますか。

   a) トレーニングはどのくらいの頻度で提供されていますか。
   b) トレーニングは次の項目を包含していますか。
      i. 参加者は部門を横断しているか。
      ii. 業務の責任者や責任範囲が明確化されているか（RACIチャートは配備されているか）。
      iii. 疑わしい行為についての連絡先や報告方法が定義されているか。

参考資料：RACIチャート

名前	日本語訳	説明
Responsible	実行責任者	タスクの実行者。複数いることを許容。Accountableと兼ねることもあり。
Accountable	説明責任者	タスクの説明責任者。承認者とも置き換えられる。責任の所在を曖昧にせず、原則1つのタスクに1人（1部門）のみ。
Consulted	協業先	タスクを進める際の相談者。タスクを進める際に、双方向のやり取りを行う。
Informed	報告先	タスクの進捗状況の報告先。タスクを進める際に、一方向的なやり取りとなる。

フェーズ 1. 上級編

1. 所属組織では、次のロールに対してどのようなセキュリティ関連のトレーニングを行っていますか。

   a) システム及びネットワーク管理者
   b) ベンダー、外部の助言者、所轄官庁（該当する場合）
   c) 広報（メディアとのコミュニケーション）
   d) 一般従業員

2. 組織を介さずに発生する脅威・リスク（風評被害、偽サイトなど）について監視・通知する体制を持っていますか。

フィッシング対策協議会
Council of Anti-Phishing Japan

フェーズ 2.

フェーズ 2. – Day 1: スミッシング

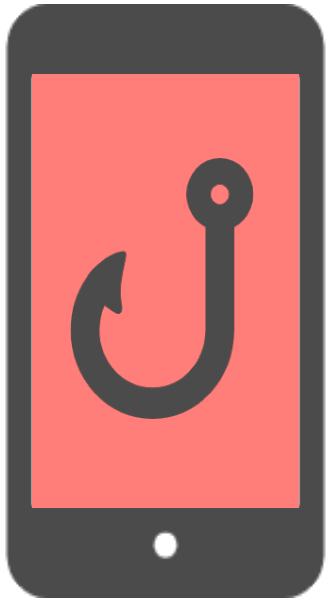
15:00

調査の結果、中部地区のみにおいてスミッシングメールが配信されていることが判明しました。

配信先は当社のユーザーではない方も含まれています。

このSMSは、ユーザー名とパスワードを取得するために作られた偽サイトへの誘導を目的としているようです。

また、指示に従って進めていくとアプリのインストールが要求されていることが分かりました。



フィッシング対策協議会
Council of Anti-Phishing Japan

フェーズ 2. 議論を促す質問 1/2

1. 複数のなりすましメール/SMSが報告された場合、このインシデントの重大度レベルをどう評価すべきですか。可能性と重篤度を変更すべき基準は何ですか。

2. 所属組織では、どのような修復および保護措置をとりますか。
   a) 誰がそれらのアクションに対して責任を負うのか。
   b) アクションの計画は文書化されているか（プレイブックはあるのか）
   c) アクションの発動はどのタイミングによって行われるのか。

3. 経過報告に関する一次、二次、三次の連絡先は整備されていますか。

フェーズ 2. 議論を促す質問 2/2

4. インシデントを分析するためにどんなリソースや能力が利用できますか。
   a) 内部におけるリソース。
   b) 外部におけるリソース。

5. インシデントを通知すべき機関（所轄官庁、ISP、CSIRT、セキュリティベンダー、法執行機関など）の要件やプロセスは整備されていますか。

6. 組織内および組織外へ脅威情報を共有する際に、どのような仕組みを使用することができますか（例：PGP公開鍵を外部公開している）。

フェーズ 2. 上級編

1. 組織内および組織外へ脅威情報を共有する際に、どのような仕組みを使用することができますか（例：PGP公開鍵を外部公開している）。

フェーズ 3.

フェーズ 3. – Day 2: 被害者が加害者に

09:30

調査の結果、SMSにて誘導されるURL（偽サイト）として35件特定できました。しかし、その数は時間経過と共に増え続けているようです。

また、偽サイトからダウンロードできるスマートフォン偽アプリを誤ってインストールした場合、スマートフォンのアドレス帳が読み取られ、誘導SMSを配信する機能（マスメーリング機能）が含まれていることを確認しました。

被害者が新たな加害者となっています。

フェーズ 3. 議論を促す質問 1/2

1. インシデントに関する追加の通知・行動指針は定義されていますか。
   a) 追加の通知に関する連絡先は特定できていますか。
   b) どの時点でどのような行動を、誰が行いますか。

2. 自組織のブランドが騙られた場合、その注意を広域に対して促す手段を用意していますか。
   a) それは自社サービス利用者と自社サービスを利用していない人への注意を促すことが可能ですか。
   b) コールセンターに入電する問い合わせに対してトークスクリプトの用意、展開を行う手段は用意していますか。

フェーズ 3. 議論を促す質問 2/2

2. 自組織のブランドを騙るサイトを封鎖するための連絡先を把握していますか。
   a) 「フィッシング対策協議会」への報告先は把握していますか。
   b) PhishTank、Google Safe Browsingへの通報方法は把握していますか。
   c) ドメイン管理業者を特定する方法は把握していますか。
   d) ISP/VPS事業者を特定する方法は把握していますか。
   e) サーバー証明書認証局を特定する方法は把握していますか。

参考資料：例文

To whom it may concern,
[簡潔な企業プロファイル].

The website is located at the following address:
＜当該フィッシングサイトのURI＞
For your information, the fraudulent website appears to be a forgery of this legitimate website:
＜正規サイトのURI＞

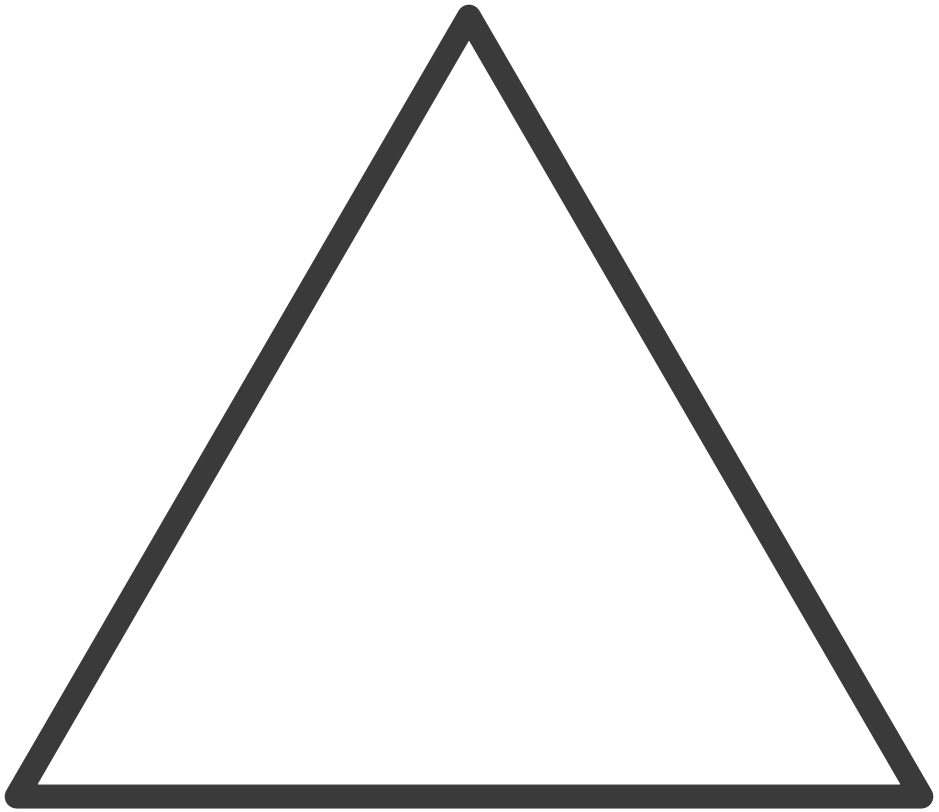
Please take all necessary measures to suspend services of this fraudulent site.
We highly appreciate your cooperation on this matter.

Thank you very much. Sincerely,
--
[担当者、送信者の名前]
[担当者、送信者の所属部署]
[企業名]
[国際電話番号]
[担当者、送信者のメールアドレス

Subject：フィッシングメールに関する情報提供
タイトル：緊急のお知らせ
差出人名：john@xxbank.example.co.jp
送信日時：2008 年3 月XX 日
概要：○○銀行を装ってリンクを含んだメールを送ってきた。
--
○○ ○○（報告者氏名、匿名での報告も可）

CIAトライアド

機密性
Confidentiality



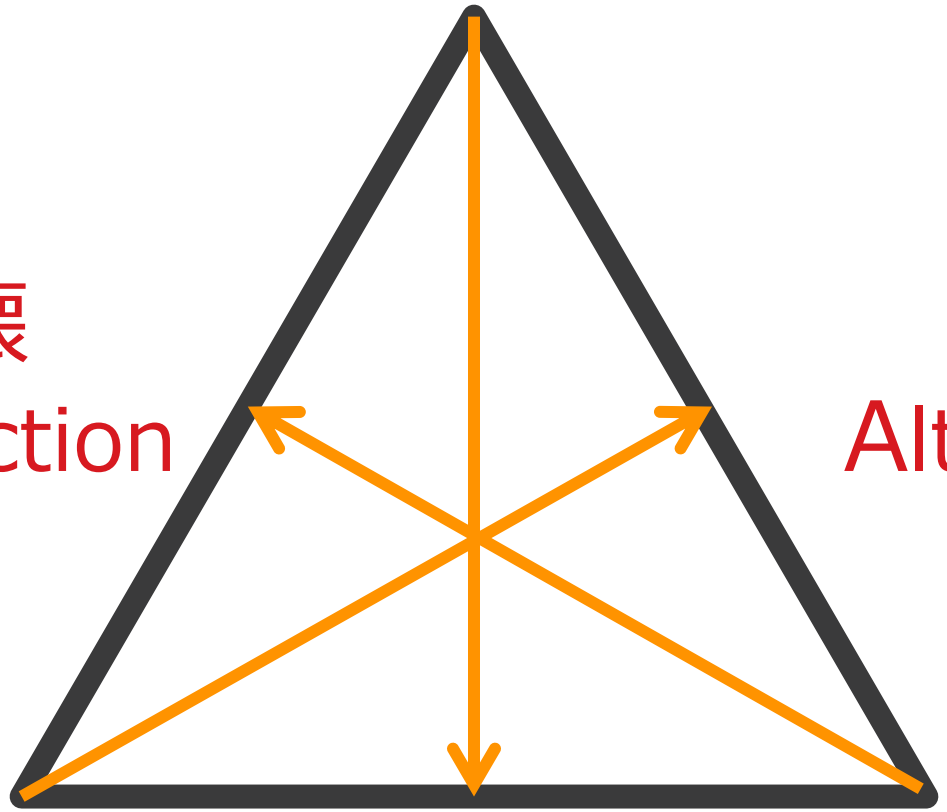
完全性
Integrity

可用性
Availability

フィッシング対策協議会
Council of Anti-Phishing Japan

論理的に表裏を考える

機密性
Confidentiality



破壊
Destruction

変更
Alteration

完全性
Integrity

可用性
Availability

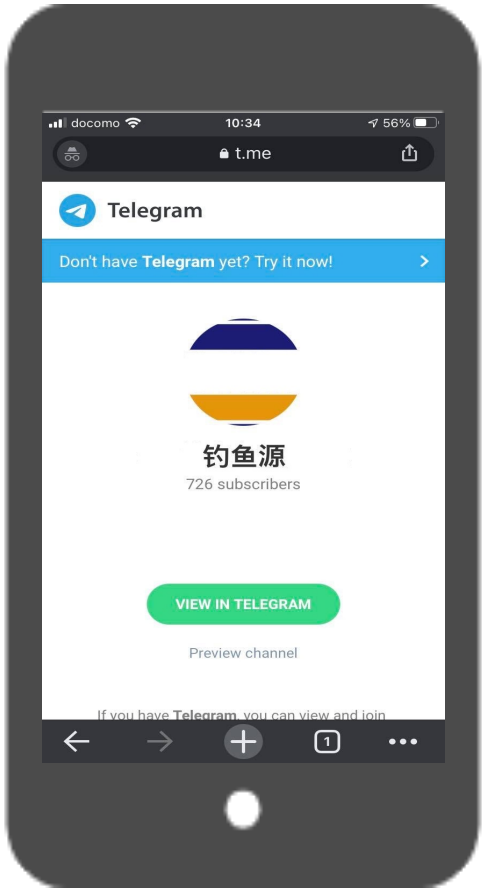
開示 Disclosure

フェーズ 4.

フェーズ 4. – Day 2

13:30

Telegramグループ「钓鱼源XXX」にて当該詐欺サイトの「構築指南書」が投稿されていることを確認しました。



15:00

正規サイトに対して詐欺サイトに登録しておいたデコイアカウントを使ったアクセスを確認しました。

フィッシング対策協議会
Council of Anti-Phishing Japan

フェーズ 4. 1/2

1. 脅威インテリジェンスパートナーから情報を受け取る体制は構築されていますか。
   a) どこから、どの部門がこの種の情報を受け取ることになりますか。
   b) 善意の協力者からの通報窓口は用意されていますか。
   c) 受信部門はどのようにこの情報を組織内へ展開しますか。

2. 積極的な脅威情報の収集について責任を担っている部門はありますか。
   a) デコイアカウントの作成・監視などアクティブな対抗手段の準備を行うことはできますか。
   b) 詐欺犯の「アトリビューション（帰属）」に繋がる情報を記録できるログを取得していますか。

フェーズ 4. 2/2

3. 詐欺に関する証拠の保存と収集のためのプロセスとリソースは整備されていますか。
   a) 画面キャプチャ
   b) メタデータ（URL, IPアドレス, etc...）

フェーズ 4. 上級編

1. 積極的なスレットハンティングを行う際に、どのような仕組みを使用することができますか。
   a) Certstream, https://certstream.calidog.io/
   b) Certificate Search, https://crt.sh/
   c) DN Pedia, https://dnpedia.com/tlds/search.php
   d) URLScan.io, https://urlscan.io/
   e) DomainWatch, https://domainwat.ch/
   f) SecurityTrails, https://securitytrails.com/
   g) PhishTank, https://www.phishtank.com/

フェーズ 5 - 6.

フェーズ 5 & 6. 1/2

1. 継続的な詐欺サイト対応のためには、どのような「リソース」と「能力」が必要ですか。
   a) スレットハンティングを担う部門に対してどのようなKPIを設定すべきですか。
   b) 利用者に対して偽サイトに対する注意の「アウェアネス（意識付け）」を高めるためにどのような活動をすべきですか。

TTXsで判明した課題

- 参照すべきドキュメントはあったか、アクションに不足は無いか。
- プレイブックには最新の情報が掲載されているか、定期的な更新は行われていたか。
- インシデントに対する対応時間は想定の範囲内であったか。
- 正しい反応はとることができたか。

フィッシング対策協議会
Council of Anti-Phishing Japan

シナリオ 2

フェーズ 1. – Day 1: ブログ記事

11:00

ネット推進室 – ネット通販マーケティング部より、知的財産部に対して、自社が提供する「ファッション サブスクリプションサービス」に関する『課金回避（不正利用）指南』と題した「踏み倒し術」が掲載されたブログ記事を見つけたとの報告を受けました。記事は投稿からすでに3日間経過。1日数千アクセス集めているようです。

また、Twitterなどでもこのサイトの URLが拡散していることを確認しています。

フェーズ 1. 議論を促す質問

1. スライド 14 – 18 の内容を再確認してください。

2. 自社のサブスクリプションサービスの「踏み倒し術」情報の掲載はどの部門との連携が必要となりますか。
   a) 「仮想企業設定集」より組織構成を確認してください。

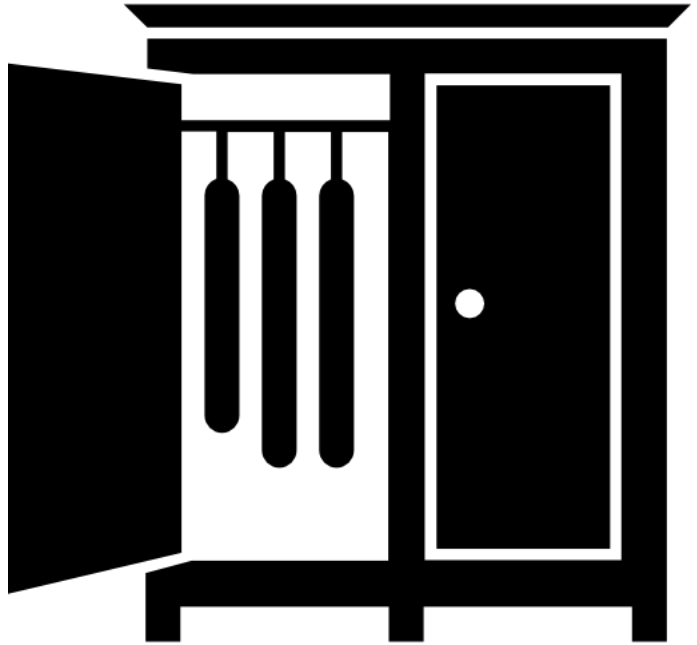
3. 事業部門である[ネット通販事業部]と[カタログ事業部]は、どちらの事業においても影響があり得る被害情報を共有することは可能ですか。
   a) Dev – IT本部, Ops – 事業部, Lgl – 法務部/知的財産部

フェーズ 2. – Day 1: 他社サービスにも波及

15:00

調査の結果、「踏み倒し術」の掲載は当社のサブスクリプションサービスだけでなく、他社の類似サービスについても記載が及んでいることを確認しました。

また、転記ブログも増え、指南された方法を実践した結果成功したとのコメント投稿も見られるようになりました。



フェーズ 2. 議論を促す質問

1. スライド 20 – 22 の内容を再確認してください。

2. 同業他社とコミュニケーション（情報交換）をとる手段はありますか。

3. 自社サービスにて「踏み倒し」の発生有無を調査するには、どの部門との連携が必要となりますか。
4. 詐欺行為が発覚した場合、どのタイミングで、どの機関（法執行機関など）へ通知すべきですか。

フェーズ 3. – Day 2: 実害なし

09:30

調査の結果、すくなくとも当社においてはブログに掲載された「踏み倒し術」を実行した痕跡は1件もありませんでした。

ただし、方法自体は有効であることも確認できました。

方法は、システムに対する不正アクセスなどの攻撃による課金回避ではありません。支払システムの不備による課金回避であることを特定しました。

また、サービスの契約条項上にも不備があり、改訂が必要であると社内の法務部より指摘があります。

フェーズ 4 – 6. 議論を促す質問

1. 一連のインシデントにおいて「まず」何を目指すべきですか。
2. 不正利用に関する規定は整備されていますか。
   a) 規定を整備し、不正利用の防止策を明確化する必要があります。
3. 「踏み倒し術」を指南しただけの人、指南に従って実際に踏み倒し（詐欺行為）を行った人
4. オリジナルの投稿とは別に、再流通した投稿（転記記事）の投稿元や削除などの対策は考慮されていますか。

フィッシング対策協議会
Council of Anti-Phishing Japan

シナリオ 3

フェーズ 1. – Day 1: 参加型キャンペーン

13:00

ネット推進室 – ネット通販マーケティング部は「Instagram」上にて、商品写真の投稿にコメント投稿した人へ抽選で商品をプレゼントするキャンペーンを展開しました。

そのコメント中に当社をなりすました偽アカウントからの投稿が確認されました。

フェーズ 1. 議論を促す質問

1. スライド 14 – 18 の内容を再確認してください。

2. フォロワーを守るために何をすることができますか。
3. なりすまし、偽アカウントに関する注意喚起、ブロック願いはできますか。
4. インスタグラム特有の機能「ストーリーズ」と「フィード」を活用した注意喚起はできますか。
5. 当社が運用しているオンラインサイト、ソーシャルメディアアカウントは他に何がありますか。

フェーズ 1 – 6.

1. フェーズ 1.「事前調査」にて検討すべき事項は何ですか。
2. フェーズ 2.「特定」にて検討すべき事項は何ですか。
3. フェーズ 3.「封じ込め」にて検討すべき事項は何ですか。
4. フェーズ 4.「根絶」にて検討すべき事項は何ですか。
5. フェーズ 5.「復旧」にて検討すべき事項は何ですか。
6. フェーズ 6.「教訓」にて検討すべき事項は何ですか。

事後アンケート

セクション	質問趣旨
1. 参加者の属性情報	匿名化の後、統計処理を行います。
2. 机上演習の実施効果	組織、人材、ツール、プロセス、参加者がそれぞれに対して演習効果を実感いただけたのか聴取します。 参加者がどんな気づきや学びが得られたのか自由記述にて聴取します。
3. 教育的効果	RETAINモデルにしたがい、教育的効果について測定します。
4. 実施時間・配布物	実施時間、配布物に対する改善提案について聴取します。
5. シナリオ評価	3つのシナリオに対して、「全体評価」、「理解度」、「面白さ」（教育的な要素があり、日常に近い内容で、適度に難しい）について聴取します。
6. 全体評価	「机上演習」への参加推薦度を10段階で評価。 9 – 10: 推奨します。 7 – 8: 中立です。 0 – 6: 推薦に対して批判的な立場です。

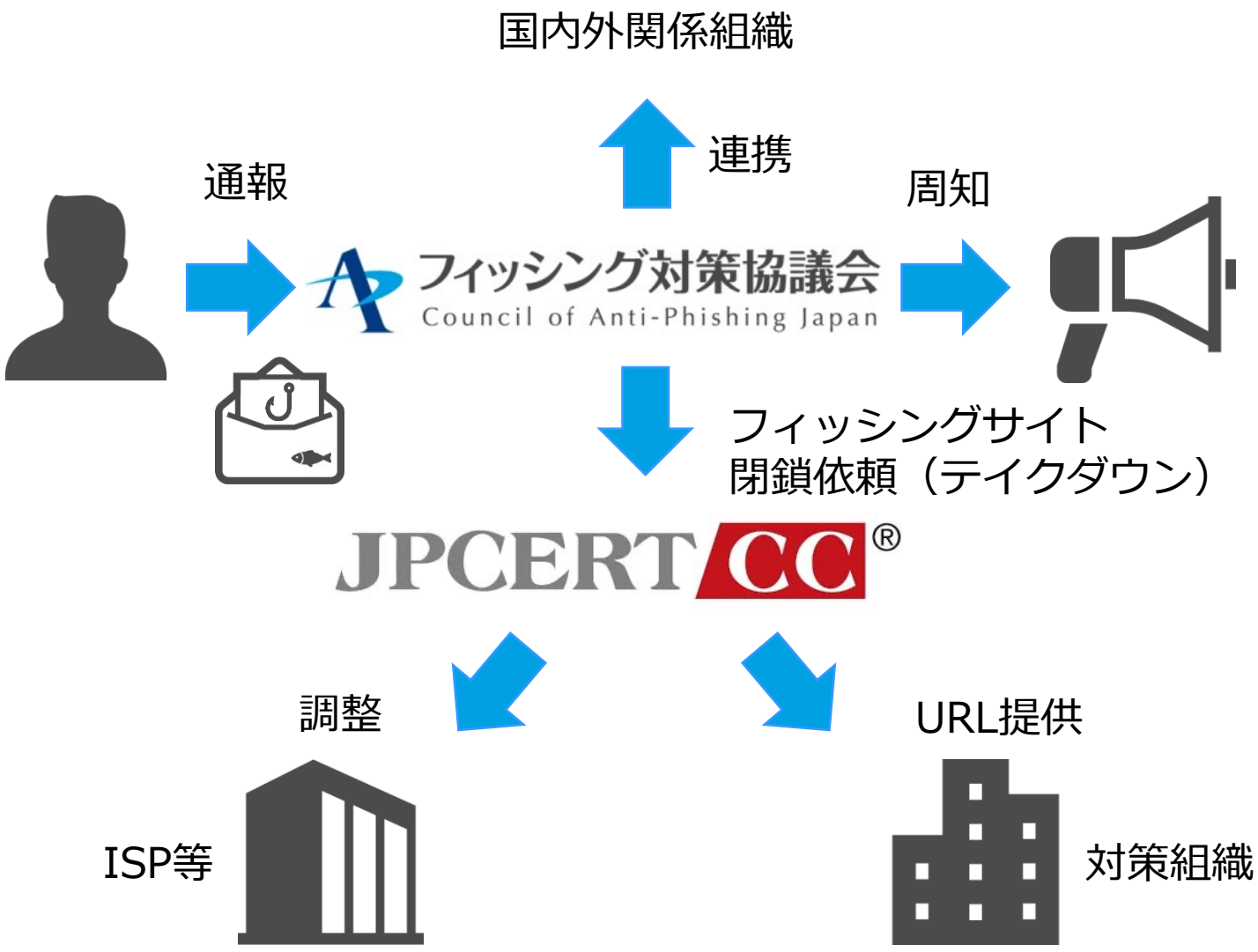
事後アンケート

https://forms.gle/w7yTGcJuMh9t6iGS7

配付資料のデジタル版は事後アンケートの末尾に
ダウンロードURLが記載されています。

フィッシング対策協議会について

フィッシング対策協議会の活動



■情報発信（事業者／一般向け）
・緊急情報
・お知らせ
・ガイドライン改訂(WG活動)
・フィッシングレポート 等

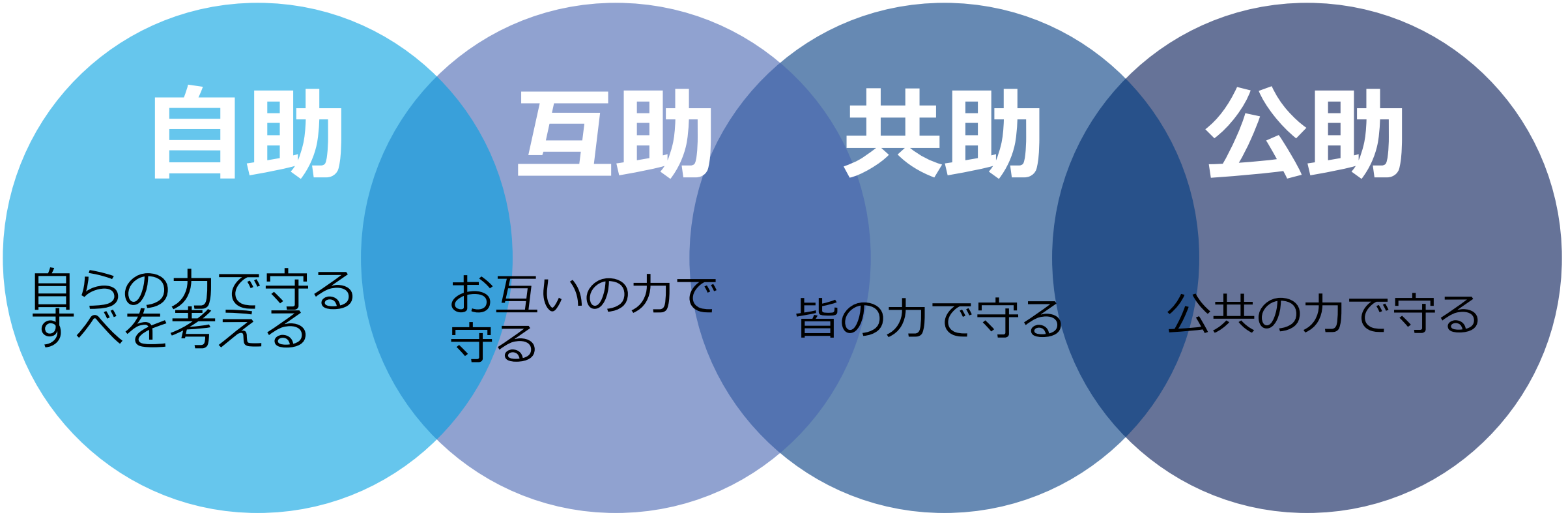
■会員間の情報交流
・総会／情報交換会
・勉強会
・WG活動　等

■啓発
・フィッシング対策セミナー
・「Stop.Think.Connect.」等

■学術研究
・フィッシングサイト早期検知

フィッシング対策協議会
Council of Anti-Phishing Japan

皆さんの参画をお待ちしています。



フィッシング対策協議会
Council of Anti-Phishing Japan

Webフォームによるフィッシングサイト報告

フィッシングの報告

フィッシング対策協議会では、フィッシングメールやフィッシングサイトに関する情報提供を受け付けています。
Webフォームでご報告される場合は**「Webフォームで報告」**、メールでの報告を希望される場合は、**「電子メールで報告」**をご参考にご連絡ください。
なお、ご報告頂いた情報は、法執行機関（警察等）及び関係組織（騙られた被害組織等）へ提供する場合があります。

Webフォームで報告　　電子メールで報告

Webフォームで報告

フィッシングサイトURL

ブランド 必須

選択してください

フィッシングサイトが騙るブランドを選択してください。選択肢にない場合は「その他」を選択してください。

URL 必須

★以下の情報は記載しないでください★
・メールアドレス・メール文面・SMS文面・フィッシングURL以外の情報

[記載例]　※複数の場合は改行で区切ってください。
https://www.abcd.com
https://www.abcd123.co.jp
https://aaa.bbb.ccc.php

フィッシング対策協議会
Council of Anti-Phishing Japan

通報・相談窓口

被害	相談窓口
フィッシングと思わしきメールを受け取った	フィッシング対策協議会, info@antiphishing.jp
ネット犯罪に遭遇	警察庁 サイバー犯罪相談窓口
迷惑メールを受け取った	迷惑メール相談センター
偽装品の販売に遭遇	一般社団法人 ユニオン・デ・ファブリカン
商品やサービスなど消費生活全般に関する苦情や問合せ	独立行政法人 国民生活センター 消費生活センター
自社ブランドになりすました偽サイトを確認	悪質ECサイトホットライン 通報フォーム, 一般社団法人セーファーインターネット協会（SIA）
JPドメイン名の不正登録に関する情報受付窓口	株式会社日本レジストリサービス(JPRS)
サイトに違法情報（銀行口座や飛ばし携帯などの売買）の掲載を確認	インターネットホットラインセンター
法的トラブルに巻き込まれた場合の相談	法テラス

STOP. THINK. CONNECT.

- 知識の習得を目的としたリテラシーの視点
- 習慣付け・意識付けを目指すアウェアネスの視点

STOP 立ち止まる | THINK 考える | CONNECT™ 楽しむ

フィッシング対策協議会
Council of Anti-Phishing Japan

フィッシング詐欺から身を守る方法

決して、メールを見分けようとしない。

大事なのは、差出人や誰宛と書かれていようが「何をさせようとしているのか」との点だけに注目して悪意を判別する。

その上で、公式発表やアクセス履歴、明細を確認することで身を守れる。被害にも早期に検知することが可能。