JANOG48 Meeting

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

スミッシングについて本気出して考えてみた

フィッシング対策協議会 学術研究WG
唐沢勇輔

本日のねらい

- **スミッシングについて知っていただく**
- **スミッシングの対策についてアイデアをいただく**

アイデア　　求む！

アジェンダ

- 自己紹介 & フィッシング対策協議会の紹介
- ウォームアップ
- SMSとは
- スミッシング（SMSフィッシング）とは
- 学術研究WGで整理した分析手法の紹介
- スミッシングのビジネスプロセス分析
- Q&A
- 対策？

アジェンダ

- **自己紹介＆フィッシング対策協議会の紹介**
- ウォームアップ
- SMSとは
- スミッシング（SMSフィッシング）とは
- 学術研究WGで整理した分析手法の紹介
- スミッシングのビジネスプロセス分析
- Q&A
- 対策？

自己紹介

唐沢 勇輔（からさわ ゆうすけ）

- **フィッシング対策協議会 副運営委員長（本日の肩書）**
- Japan Digital Design, Inc　Vice President of Security（本業）
- 某ソフトウェアベンダー　セキュリティスペシャリスト（副業）
- JNSA社会活動部会 副部会長
- OpenID ファウンデーション・ジャパン 理事

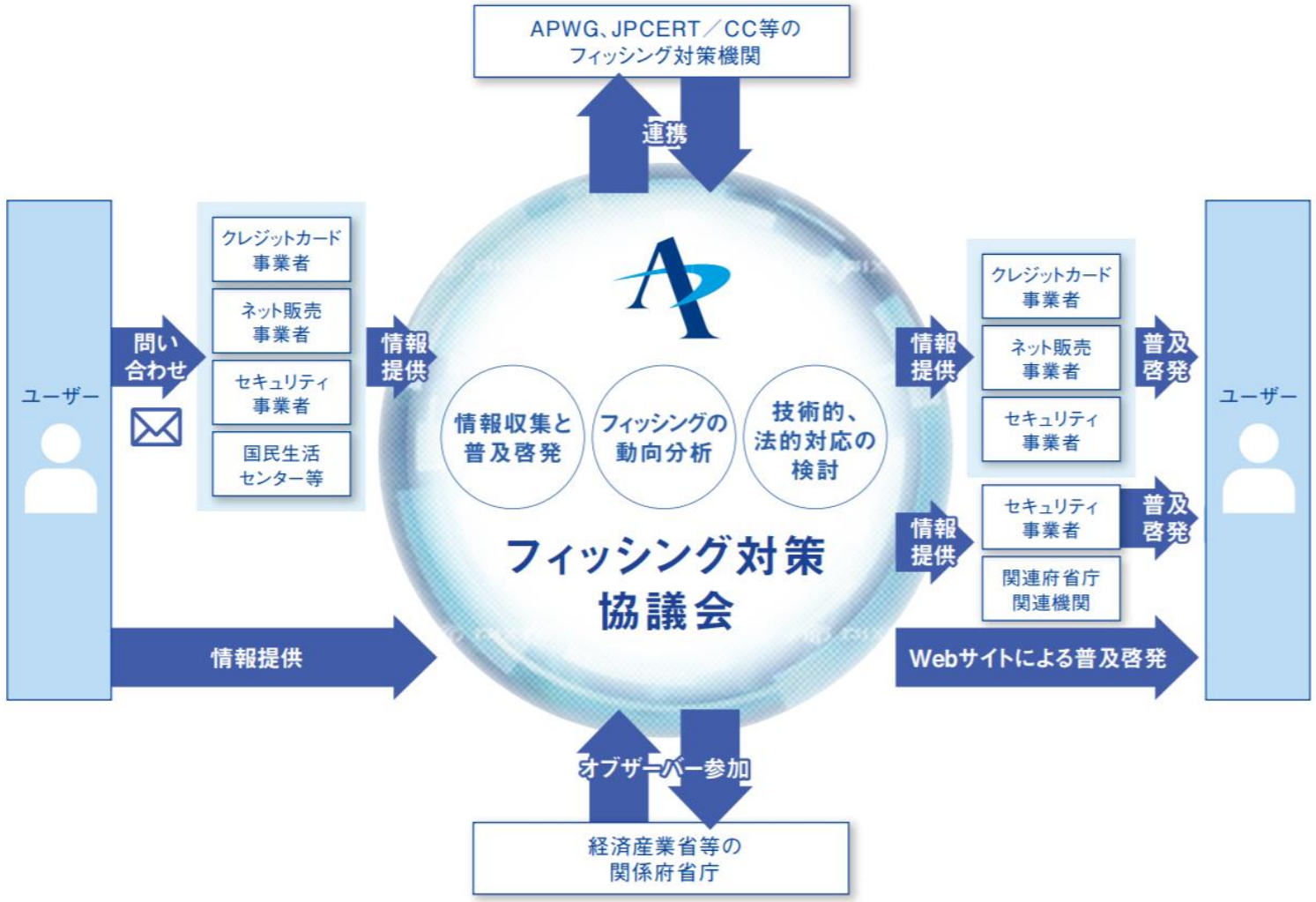
フィッシング対策協議会について

概要

- 設立　2005年4月
- 名称　フィッシング対策協議会 / Council of Anti-Phishing Japan
- 目的　フィッシング 詐欺に関する事例情報、技術情報の収集及び提供を中心に行うことで、日本国内におけるフィッシング詐欺被害の抑制を目的として活動
- 会員+オブザーバー 104
  - 正会員：77、リサーチパートナー：６、関連団体：１４
  - オブザーバー：7
  - 金融機関、信販会社、オンラインサービス、セキュリティベンダーなど

フィッシング対策協議会について

活動内容



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

学術研究
- フィッシングサイト早期検知
- フィッシング詐欺の全容解明

会員間の情報交流
- 総会／情報交換会
- 勉強会
- ワーキンググループ活動 等

啓発活動
- フィッシング対策セミナー
- STOP.THINK.CONNECT.

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

アジェンダ

- 自己紹介＆フィッシング対策協議会の紹介
- **ウォームアップ**
- SMSとは
- スミッシング（SMSフィッシング）とは
- 学術研究WGで整理した分析手法の紹介
- スミッシングのビジネスプロセス分析
- Q&A
- 対策？

Q1

「フィッシング」または「フィッシング詐欺」をどの程度ご存知ですか？

1. 全く知らない
2. 言葉は知っている
3. 説明できる
4. やったことがある (∩´∀｀)∩

Q2

「スミッシング」という言葉をご存知ですか？

1. 全く知らない
2. 言葉は知っている
3. 説明できる
4. やったことがある (∩´∀｀)∩

Q3

フィッシング詐欺メールやSMS(ショートメッセージ)を受け取ったことはありますか？

1. ある
2. ない

Q4

フィッシングに対するあなたの立場として、以下のどれが最も近いですか？

1. フィッシング対策をする立場　（対策ベンダー、啓発をしている、フィッシングハンターetc）
2. フィッシングのターゲットになりそうなブランドの立場
3. 対策製品を使う立場（企業や一般消費者）

Q5

フィッシング対策協議会をご存知ですか？

1. 協議会の会員です
2. 会員ではないが、知っています
3. 知りません

アジェンダ

- 自己紹介＆フィッシング対策協議会の紹介
- ウォームアップ
- **SMSとは**
- スミッシング（SMSフィッシング）とは
- 学術研究WGで整理した分析手法の紹介
- スミッシングのビジネスプロセス分析
- Q&A
- 対策？

SMSの生みの親

SMSの父
Friedhelm Hillebrand (中央),
Finn Trosby (右)
Kevin Holley (左)

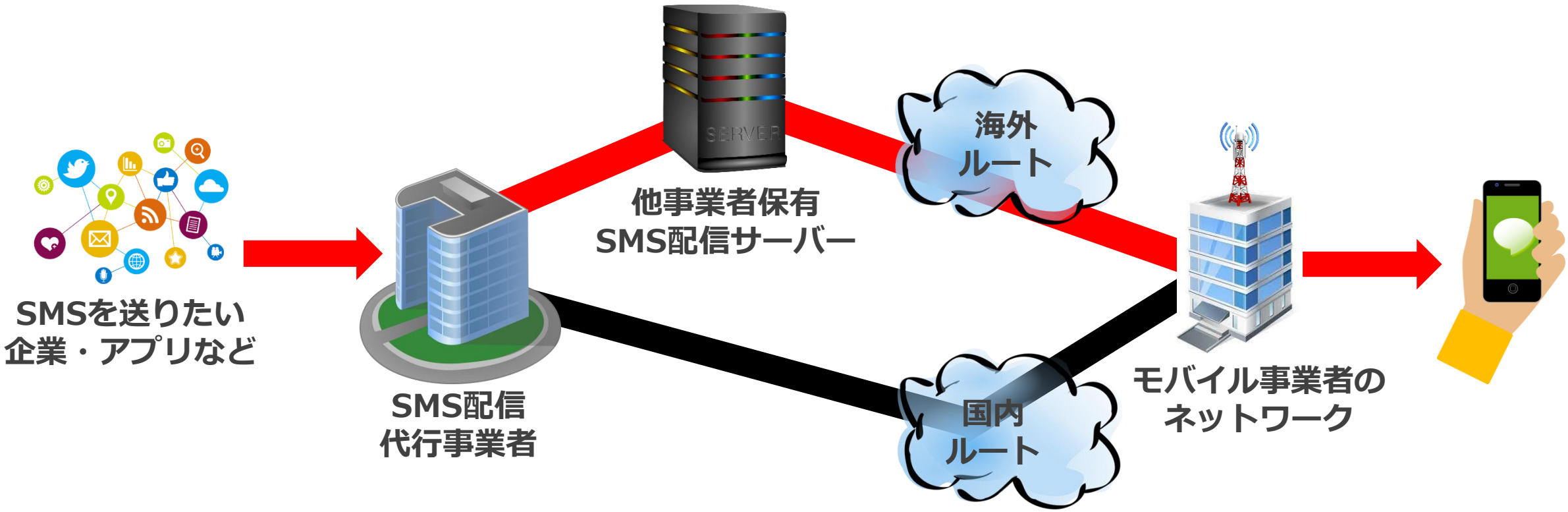
1980年代
ヨーロッパのエンジニアたちが発明し
世界標準として規格を作り上げました。

1990年代
第二世代(GSM)で基本搭載され
ケータイ黎明期のキラーサービスに

コミュニケーションや認証要素として

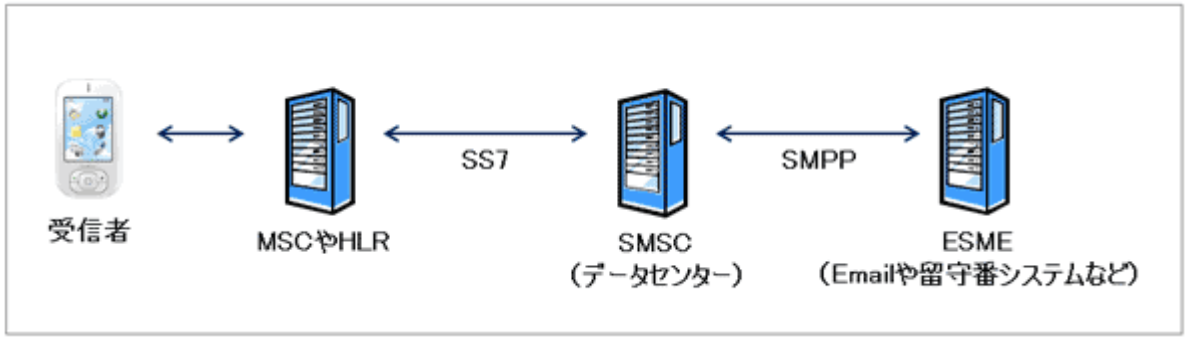
フィッシング対策協議会
Council of Anti-Phishing Japan

SMS送信ルートは様々



SMSの仕組み

- 電子メールのようなパケットネットワークではなく、回線交換ネットワーク上を通る
- 回線交換ネットワーク
  - 音声を運ぶトラフィックチャネル
  - 制御するシグナリングチャネル　→　ここでテキストを流す
- 送信したメッセージはSMSC（ショートメッセージサービスセンター）に一時的に保管され、転送される



出典) https://www.ex-sms.com/related/signal-line/

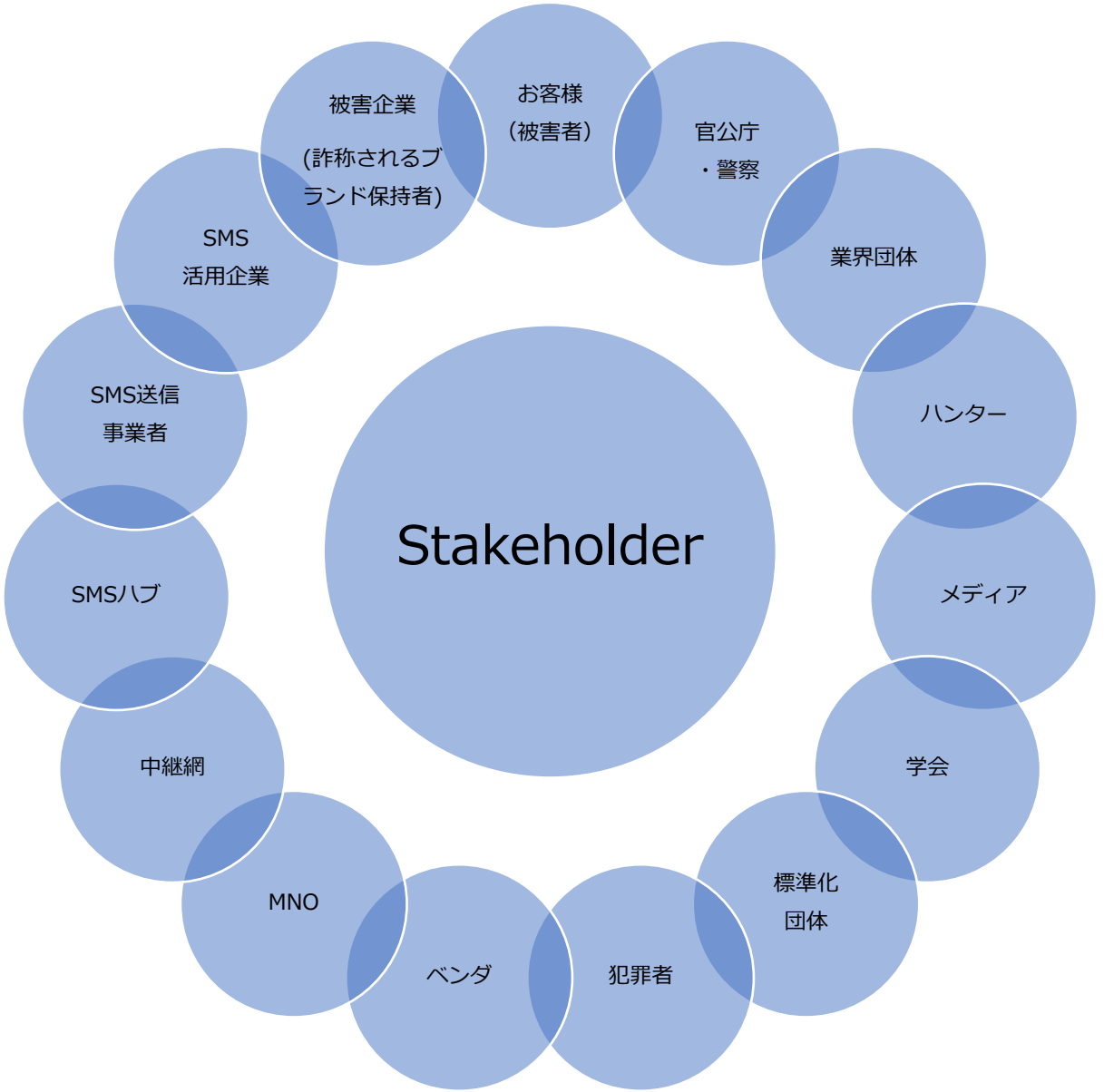
SMSの特徴

SMSは電話番号と紐づいており確実に届き、開封率が高いと言われる

	電子メール	SMS
配信方式	プル方式	プッシュ方式　(強制受信)
発信者ID	メールアドレス	自由に設定できる（余地が大きい）
受信者	メールアドレス	電話番号
迷惑メールフィルタ	受信者の許諾を得ることで送信元や内容で判定OK（一般利用可）	通信の秘密の取り扱いについて未整理のため文面判定NG（一般利用不可、海外SMS拒否は可）
送信料金	無料	有料
メッセージ長・形式	長さは自由 形式はテキスト or HTML	長さは160bytesまで 形式はプレーンテキストのみ

出典） マクニカ社の発表資料を基に筆者が一部改変
https://www.macnica.net/news/mnc_20200909.html/

多くの(多すぎる?)ステークホルダー



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

アジェンダ

- 自己紹介＆フィッシング対策協議会の紹介
- ウォームアップ
- SMSとは
- **スミッシング（SMSフィッシング）とは**
- 学術研究WGで整理した分析手法の紹介
- スミッシングのビジネスプロセス分析
- Q&A
- 対策？

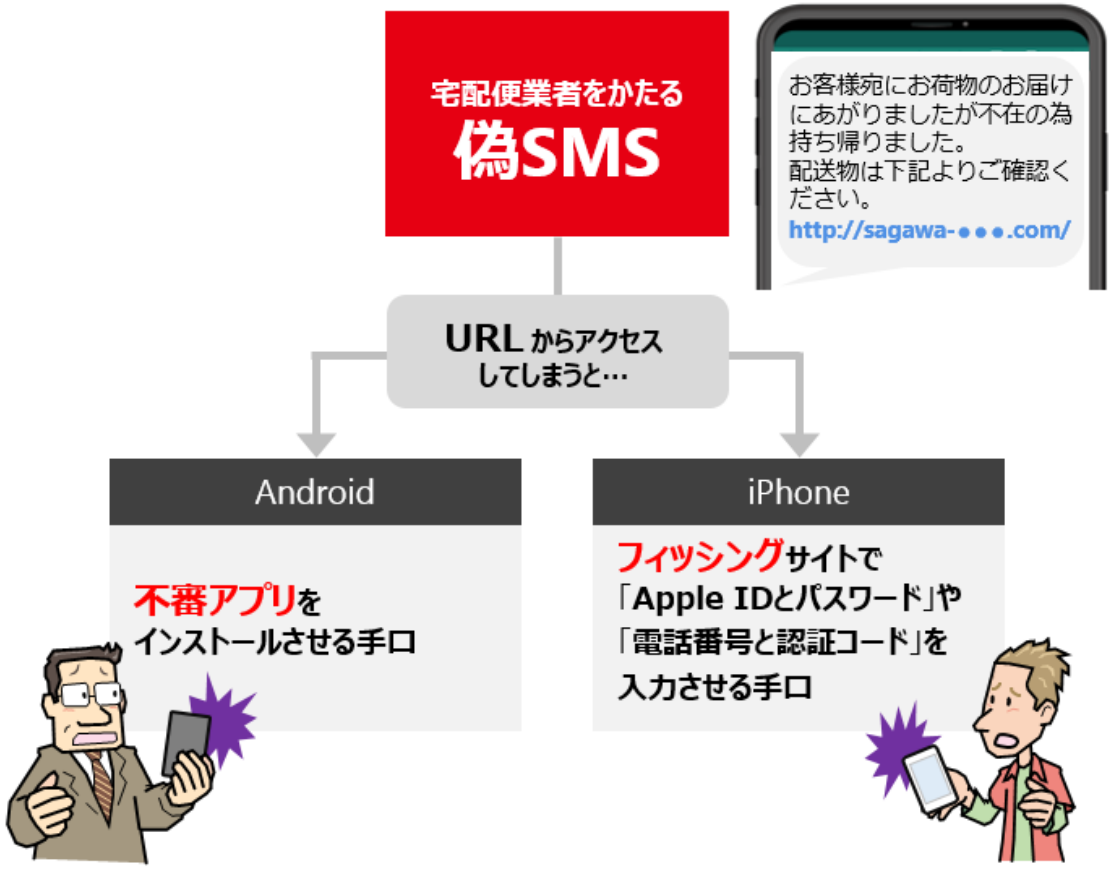
スミッシングとは

SMSを使ったフィッシング詐欺
Smishing＝SMS ＋ phishing

出典：フィッシング対策協議会

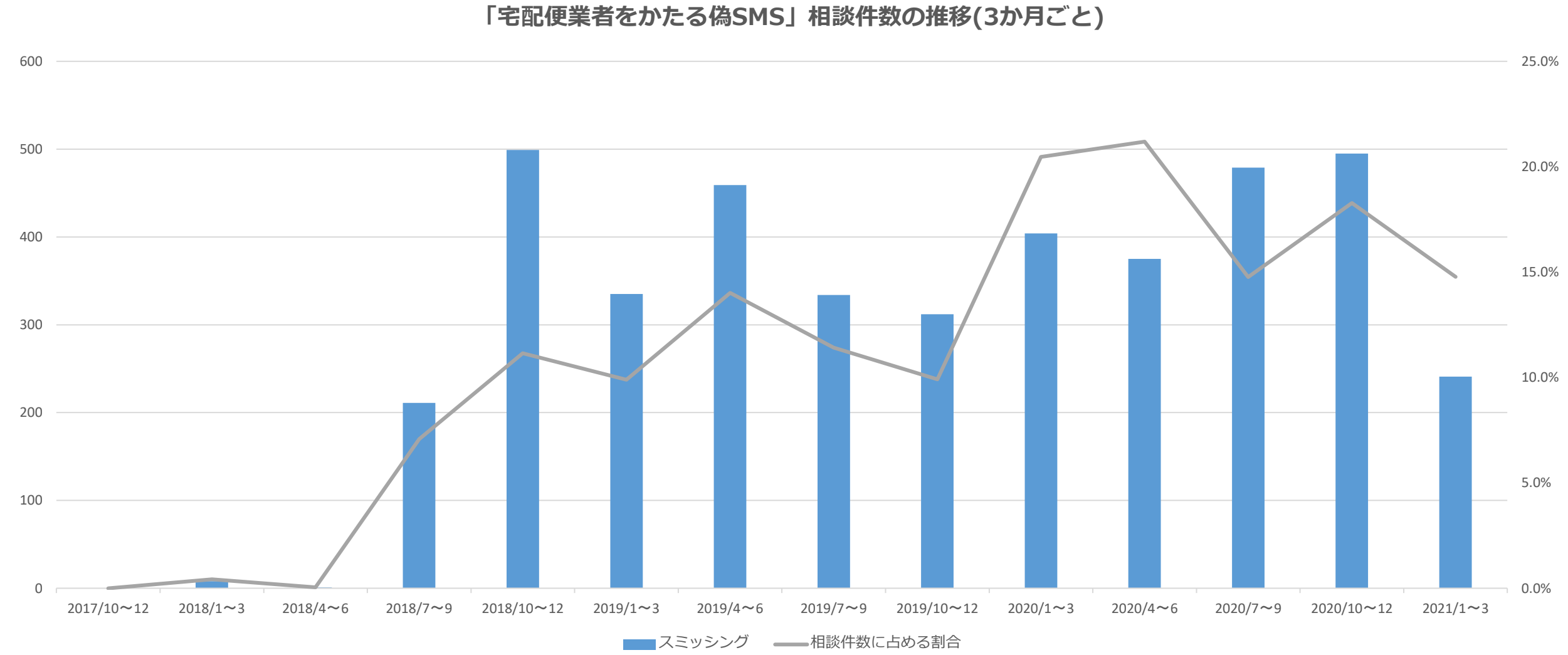
フィッシング対策協議会
Council of Anti-Phishing Japan

スミッシング被害の流れ



出典：https://www.ipa.go.jp/security/anshin/mgdayori20200220.html

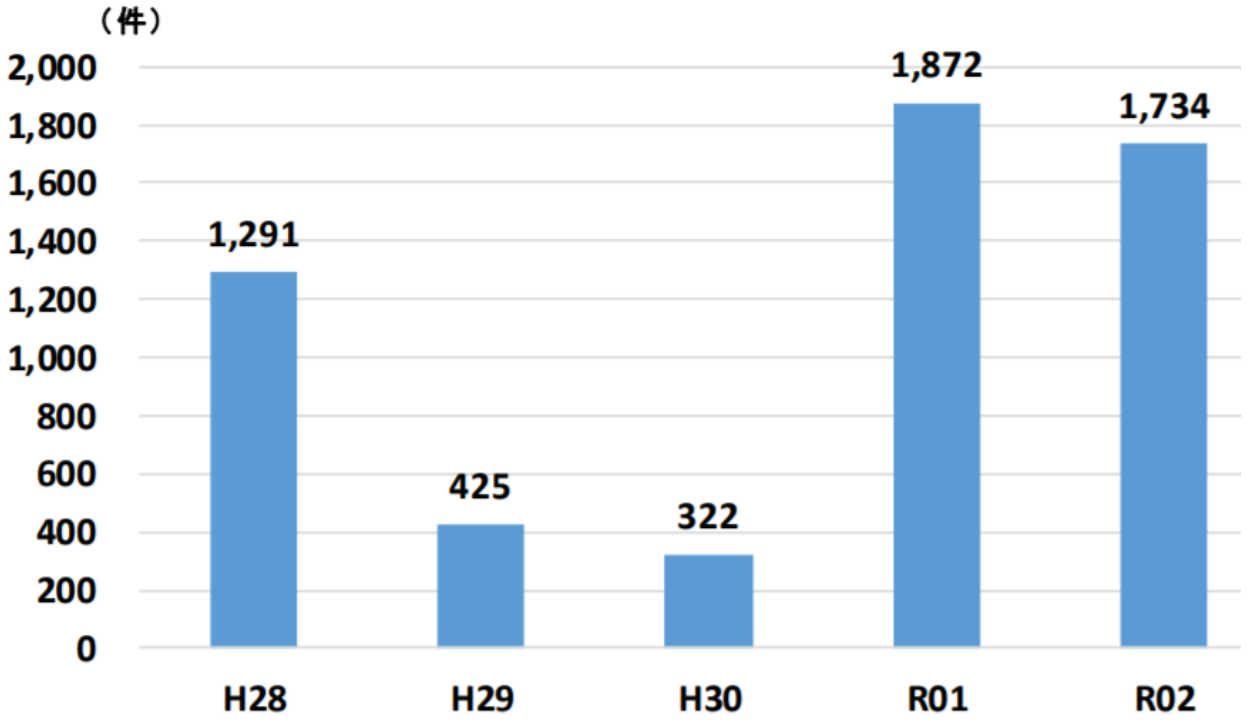
スミッシングによる被害件数



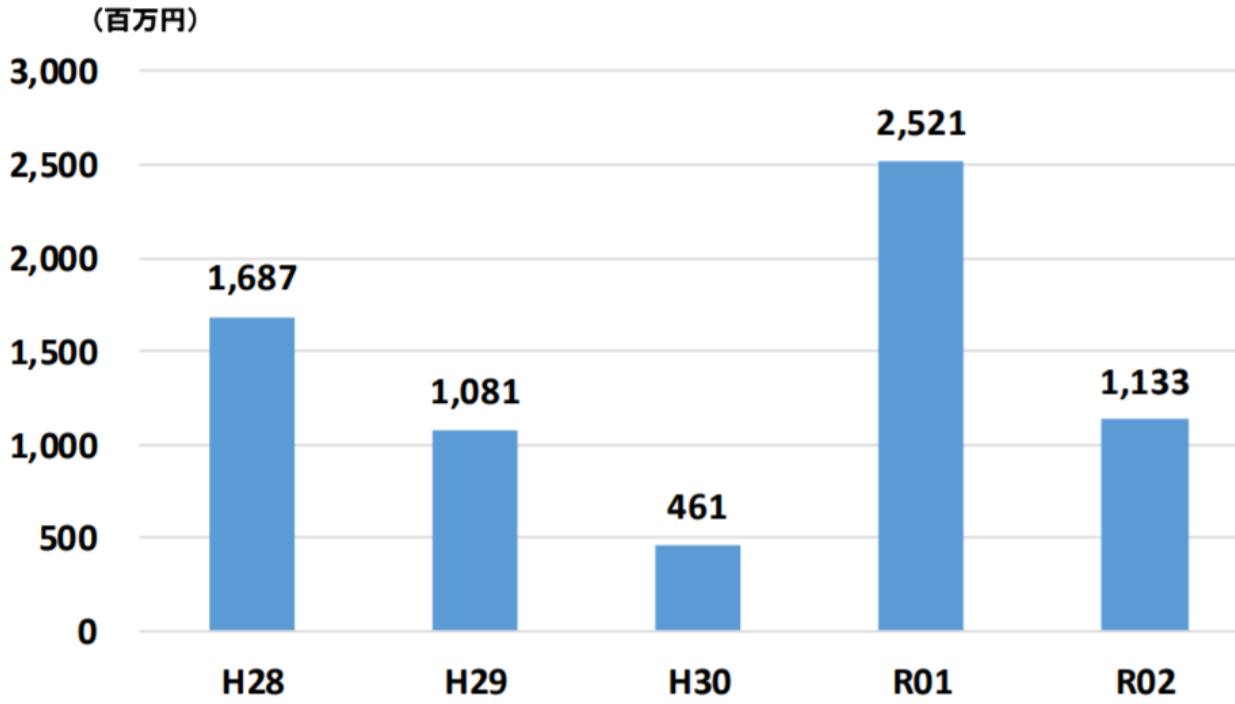
出典) https://www.ipa.go.jp/security/txt/2021/q1outline.html、https://www.ipa.go.jp/security/txt/2019/q4outline.html、
https://www.ipa.go.jp/security/txt/2018/q4outline.html

ネットバンク不正送金の発生数

【図表12：インターネットバンキングに係る不正送金事犯の発生件数の推移】



【図表13：インターネットバンキングに係る不正送金事犯の被害額の推移】



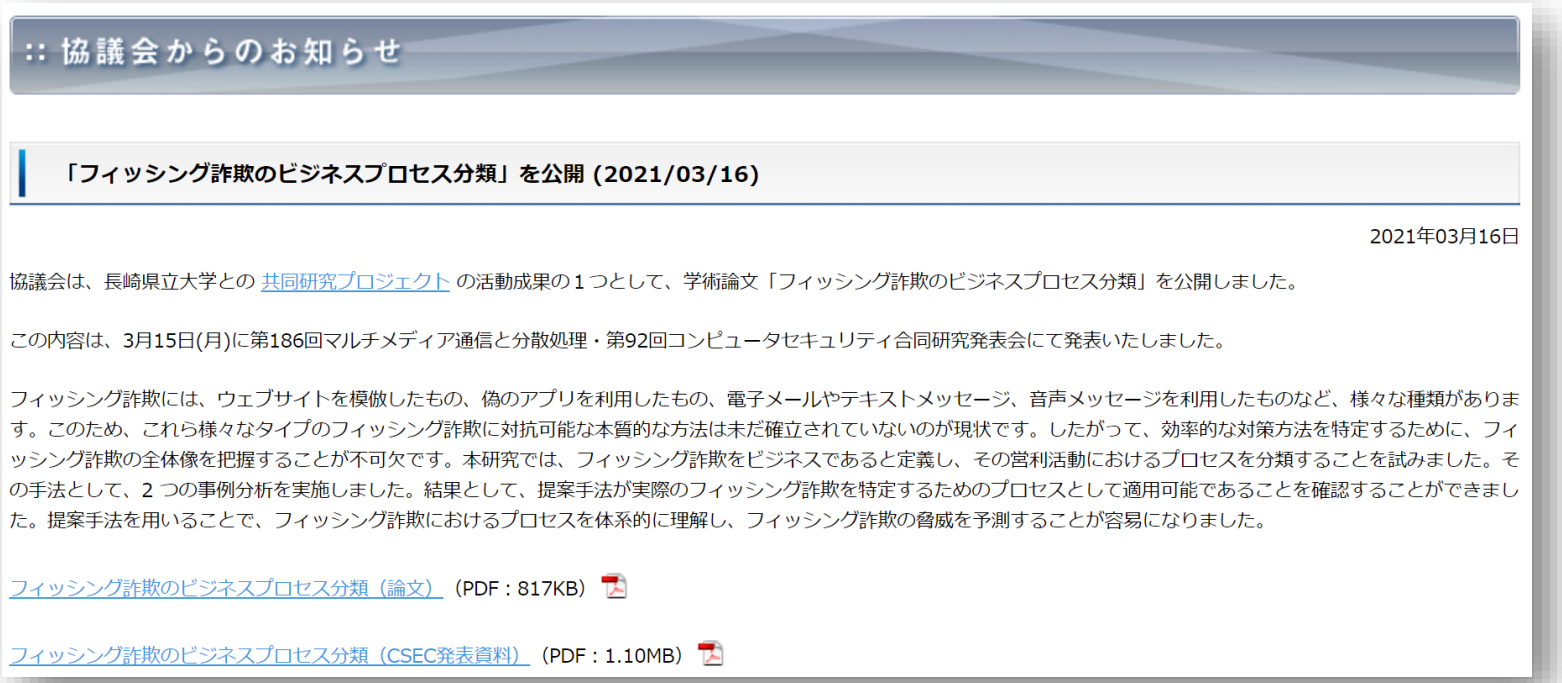
出典：　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_cyber_jousei.pdf

アジェンダ

- 自己紹介＆フィッシング対策協議会の紹介
- ウォームアップ
- SMSとは
- スミッシング（SMSフィッシング）とは
- **学術研究WGで整理した分析手法の紹介**
- スミッシングのビジネスプロセス分析
- Q&A
- 対策？

学術研究WGで整理した分析手法の紹介

- 2021年3月に協議会・学術研究WGより「フィッシング詐欺のビジネスプロセス分類」を公開
- さまざまなフィッシング手法を汎用的に分析する方法を提案したもの
- 今回、この手法でスミッシングを分析



:: 協議会からのお知らせ

「フィッシング詐欺のビジネスプロセス分類」を公開 (2021/03/16)

2021年03月16日

協議会は、長崎県立大学との 共同研究プロジェクト の活動成果の１つとして、学術論文「フィッシング詐欺のビジネスプロセス分類」を公開しました。

この内容は、3月15日(月)に第186回マルチメディア通信と分散処理・第92回コンピュータセキュリティ合同研究発表会にて発表いたしました。

フィッシング詐欺には、ウェブサイトを模倣したもの、偽のアプリを利用したもの、電子メールやテキストメッセージ、音声メッセージを利用したものなど、様々な種類があります。このため、これら様々なタイプのフィッシング詐欺に対抗可能な本質的な方法は未だ確立されていないのが現状です。したがって、効率的な対策方法を特定するために、フィッシング詐欺の全体像を把握することが不可欠です。本研究では、フィッシング詐欺をビジネスであると定義し、その営利活動におけるプロセスを分類することを試みました。その手法として、2 つの事例分析を実施しました。結果として、提案手法が実際のフィッシング詐欺を特定するためのプロセスとして適用可能であることを確認することができました。提案手法を用いることで、フィッシング詐欺におけるプロセスを体系的に理解し、フィッシング詐欺の脅威を予測することが容易になりました。

フィッシング詐欺のビジネスプロセス分類（論文） (PDF : 817KB)

フィッシング詐欺のビジネスプロセス分類（CSEC発表資料） (PDF : 1.10MB)

出典：　https://www.antiphishing.jp/news/info/collabo_20210316.html

研究目的：全体像把握＆対策の検討

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

インプットをプロセスアクティビティにて処理し，アウトプットに変換する活動，ISO 15288:2015

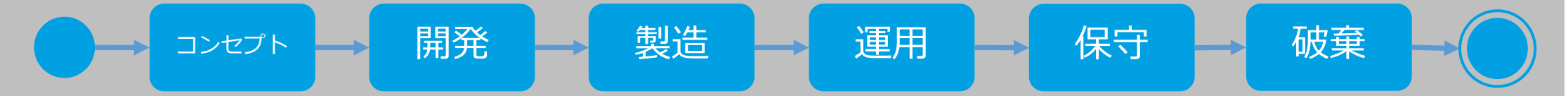


図: 一般的なシステムライフサイクルフェーズ

フィッシング詐欺をビジネスとして捉える．6つの活動を定義

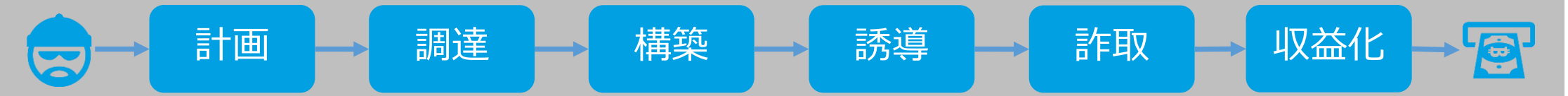


図: フィッシング詐欺ビジネスプロセス

フィッシング詐欺ビジネスプロセスの提案．共通ルールで分析

研究方法：ケーススタディ

フィッシング詐欺ビジネスプロセスを2つの実例に対し照合

- **事例1: 16Shop フィッシングキット**
  同一の**「Phishing as a Service (PHaaS)」提供者**による変遷に注目
- **事例2: LINEを騙るフィッシング詐欺**
  同一の**「標的」を狙う詐欺者**の変遷に注目

	16Shop事例分析	LINE事例分析
観測期間	2018年7月 – 2018年8月	2016年10月 – 2020年5月
調査対象数	115 URLs （無作為に抽出）	1,025 URLs
TLD	22 件	14件
AS番号	39 件	51件

※件数はすべて重複を除く、ユニーク件数

考察

プロセスの体系的な理解により，各段階の主要因子を特定

フィッシング詐欺ビジネスプロセス	16Shop事例分析により判明した因子	LINE事例分析により判明した因子
計画	動機，機会，標的，詐欺の開始時期，詐取を狙うeKYC	動機，機会，標的，誘導試行回数の期待値,詐取を狙うeKYC
調達	調達先の傾向，調達サービスを支えるコミュニティ	調達先の傾向
構築	技術習熟度，帰属情報	構築期間，設置のタイミング
誘導	疑念払拭の手法，作業品質	疑念払拭の手法，作業品質
詐取	被害認知に至るまでの引き延ばし工作	被害認知に至るまでの引き延ばし工作
収益化	換金対象，二次被害	換金対象

主要因子の観測により進行段階の特定，脅威予測/対策を支援する

※補足　**水色**の表記はどちらか一方の事例のみで判明した因子

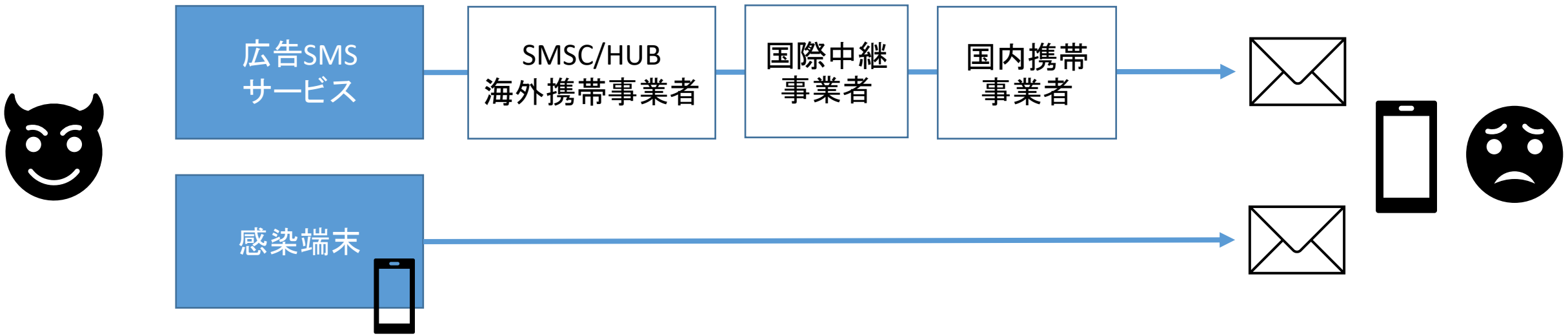
アジェンダ

- 自己紹介＆フィッシング対策協議会の紹介
- ウォームアップ
- SMSとは
- スミッシング（SMSフィッシング）とは
- 学術研究WGで整理した分析手法の紹介
- **スミッシングのビジネスプロセス分析**
- Q&A
- 対策？

スミッシングのビジネスプロセス分析

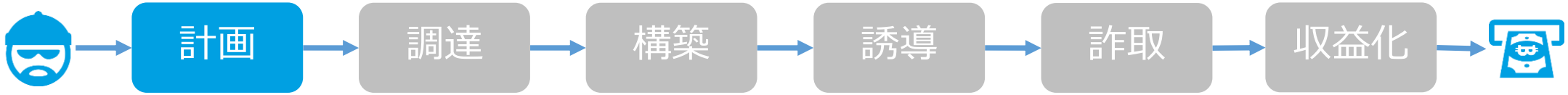
- 主なスミッシングの経路は以下の２つ

【①海外SMS利用】



【②感染端末利用】

①計画



共通

- ターゲットブランド選定、本物SMSの分析
- SMS文面の作成
  - クリックされやすい時事ネタを収集するなど
- 送信先の検討
  - 地銀を狙ったスミッシングの場合、当該地域の番号リストに送付する..等

①海外SMS利用

- SMS送信者IDの検討

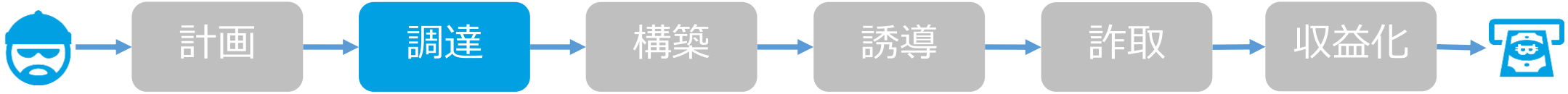
  例えば送信者を「Amazon」「NTT」などと正規ブランドを詐称したい場合、その英数字が送付できるところを選択する（国によっては英字を拒否しているところもある）

②感染端末利用

- 固有のものはなし

SMS送信者IDの偽装

②調達



共通

- 偽サイト誘導の準備
  - 偽サイトのドメイン取得
  - DDNSや短縮URLの取得
  - 証明書の準備
- SMS送信先電話番号の購入
  - 観測では、ランダムに送付していることはなさそう
- 受け子の準備

①海外SMS利用

- SMS送信ルートの調達
  - 広告SMSサービスとの契約
  - グレールート接続サービスとの契約(SS7不正接続など)
  - SIM-BOX、SMSデバイスの準備（自力で送信している場合）

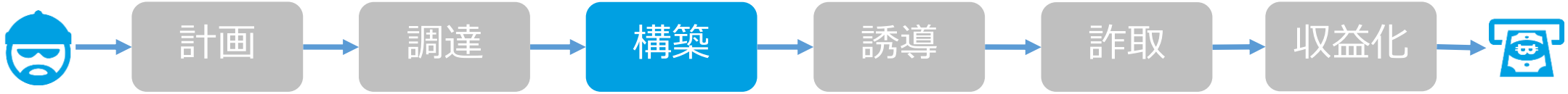
②感染端末利用

- Androidマルウェアの調達

SIM-BOX

出典) https://digital.asahi.com/articles/ASP716JY8P71OIPE00X.html?iref=pc_photo_gallery_bottom

③構築



共通

- フィッシングサイト構築
  - フィッシングキットを用いて構築

①海外SMS利用

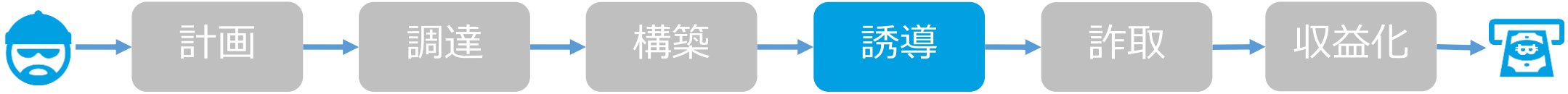
- 固有のものは無し

②感染端末利用

- Androidマルウェア配布サイト構築
- C&Cサーバー準備
  - SMS送信先のリスト配布
  - フィッシングURL記載文面のリスト配布

Pinterestを悪用する例も

④誘導



共通

- フィッシングサイト構築
  - (Android) SMS内のリンクを踏ませて偽サイトへ誘導し、偽アプリインストールさせる
    - 感染後にポップアップを出させる
  - (iOS) SMS内のリンクを踏ませて偽サイトへ誘導

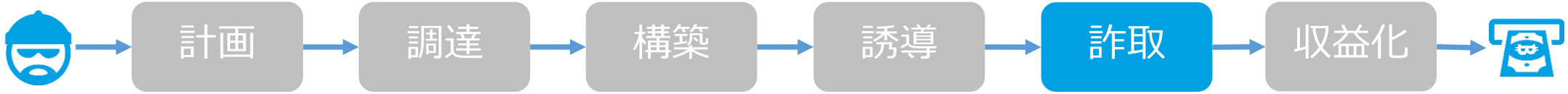
①海外SMS利用

- 固有のものは無し

②感染端末利用

- 固有のものは無し

⑤詐取



共通

- (偽サイト上で)アカウント情報の詐取、乗取り
- (偽サイト上で)クレジットカード情報、有効期限、セキュリティコード、3Dセキュアのパスワードなどを詐取
- (偽サイト上で)個人情報詐取
- オンライン本人確認情報の詐取(免許画像etc)
- キャリア決済先の不正登録、決済時の連絡先変更
- 銀行口座ログイン情報の詐取、二段階認証突破（Androidマルウェアによる OTP詐取など）
- Androidマルウェアによる、端末内の個人情報詐取

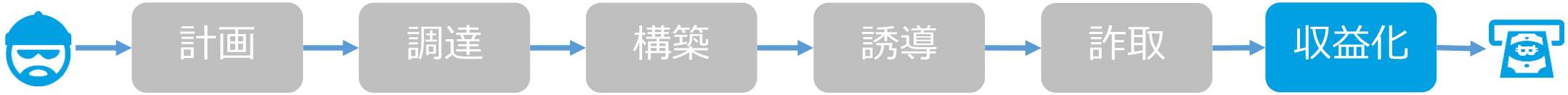
①海外SMS利用

- 固有のものは無し

②感染端末利用

- 固有のものは無し

⑥収益化



共通

- ネットバンクへの不正ログイン、不正送金
- ショッピングサイトに不正ログイン、ギフトカード・物品購入、転売
- ネットゲームに不正ログイン、ゲームアイテムのRMT（リアルマネートレード）
- 詐取情報の転売
- クレジットカードの不正利用

①海外SMS利用

- 固有のものは無し

②感染端末利用

- 固有のものは無し

アジェンダ

- 自己紹介＆フィッシング対策協議会の紹介
- ウォームアップ
- SMSとは
- スミッシング（SMSフィッシング）とは
- 学術研究WGで整理した分析手法の紹介
- スミッシングのビジネスプロセス分析
- **Q&A**
- 対策？

Q&A

内容についてのご質問があれば

Slack

ZoomのQ&A

でいただけますでしょうか？

アジェンダ

- 自己紹介＆フィッシング対策協議会の紹介
- ウォームアップ
- SMSとは
- スミッシング（SMSフィッシング）とは
- 学術研究WGで整理した分析手法の紹介
- スミッシングのビジネスプロセス分析
- Q&A
- **対策？**

対策

- 現在行われている対策は以下の通り

計画	調達	構築	誘導	詐取	収益化
• 類似ドメインの取得を検知してテイクダウン	• なし	• なし	• 報告などから誘導先を発見してテイクダウン • セキュリティアプリによるURLブロック、マルウェア検知	• 一般消費者への啓発	• ショッピングサイトなどでの不正検知

アイデア　　求む！