フィッシング対策活動と
スミッシング動向

2024/11/11

JC3 Japan Cybercrime Control Center

アジェンダ

- **JC3の紹介**
- **フィッシングサイトのテイクダウン活動**
  - フィッシングサイト撲滅チャレンジカップ
  - Abuse報告の支援ツール
  - 開催結果
- **スミッシングの動向**
  - 配信基盤となっているマルウェア
  - 観測の概要
  - 最近の動向

JC3の紹介

法人名

✓ **一般財団法人日本サイバー犯罪対策センター**

（英語名：Japan Cybercrime Control Center）　※2014年11月13日に業務開始

創設の背景

✓ **サイバー空間の脅威が深刻化する中、個別具体の脅威に対して、事後的に防護措置を講ずる受け身の対応**

→サイバー空間全体を俯瞰し、産学官(警察)それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を組織内外で共有し、サイバー空間の脅威を特定、軽減及び無効化するための活動に貢献する。

警察庁の有識者会議等を経て、「世界一安全な日本」創造戦略（平成25年12月閣議決定）でも言及

～米国のモデル～

米国ではサイバー空間における脅威への対処を目的として1997年、非営利法人**ＮＣＦＴＡ**を創設。FBIをはじめとする法執行機関、大学等の学術機関及び民間企業連携の組織として機能しており、迅速な情報収集、情報の分析、分析した情報に基づく迅速な捜査等を遂行するためのトレーニングを提供している。

（ＮＣＦＴＡ=National Cyber-Forensics & Training Alliance)

フィッシングサイトのテイクダウン活動

フィッシングサイトのテイクダウン活動

フィッシングサイト撲滅チャレンジカップ

- 都道府県警察のサイバー防犯ボランティアが参加
- コンテスト形式で開催（テイクダウン活動を数値化）
- 成績優秀な団体や個人を表彰
- Abuse報告の支援ツールを活用

第１回

開催日程

- 期間：2月13日（火）～2月20日（火）

参加者

- 都道府県警察数：20道府県警察本部
- ボランティア団体：27団体
- 参加人数：125名

結果

- Abuse数 9,319件
- テイクダウン数 268件
- 内訳
  - ドメイン事業者Abuse報告数　5,464件　　テイクダウン数　264件
  - ホスティング事業者Abuse報告数　3,855件　　テイクダウン数　4件

第２回

開催日程

- 期間：7月22日（月）～７月29日（月）

参加者

- 都道府県警察数：31道府県警察本部
- ボランティア団体：46団体
- 参加人数：359名

結果

- Abuse数　12,072件
- テイクダウン数　2,201件
- 内訳
  - ドメイン事業者Abuse報告数　9,837件　　テイクダウン数　2,004件
  - ホスティング事業者Abuse報告数　2,235件　　テイクダウン数　197件

スミッシングの動向

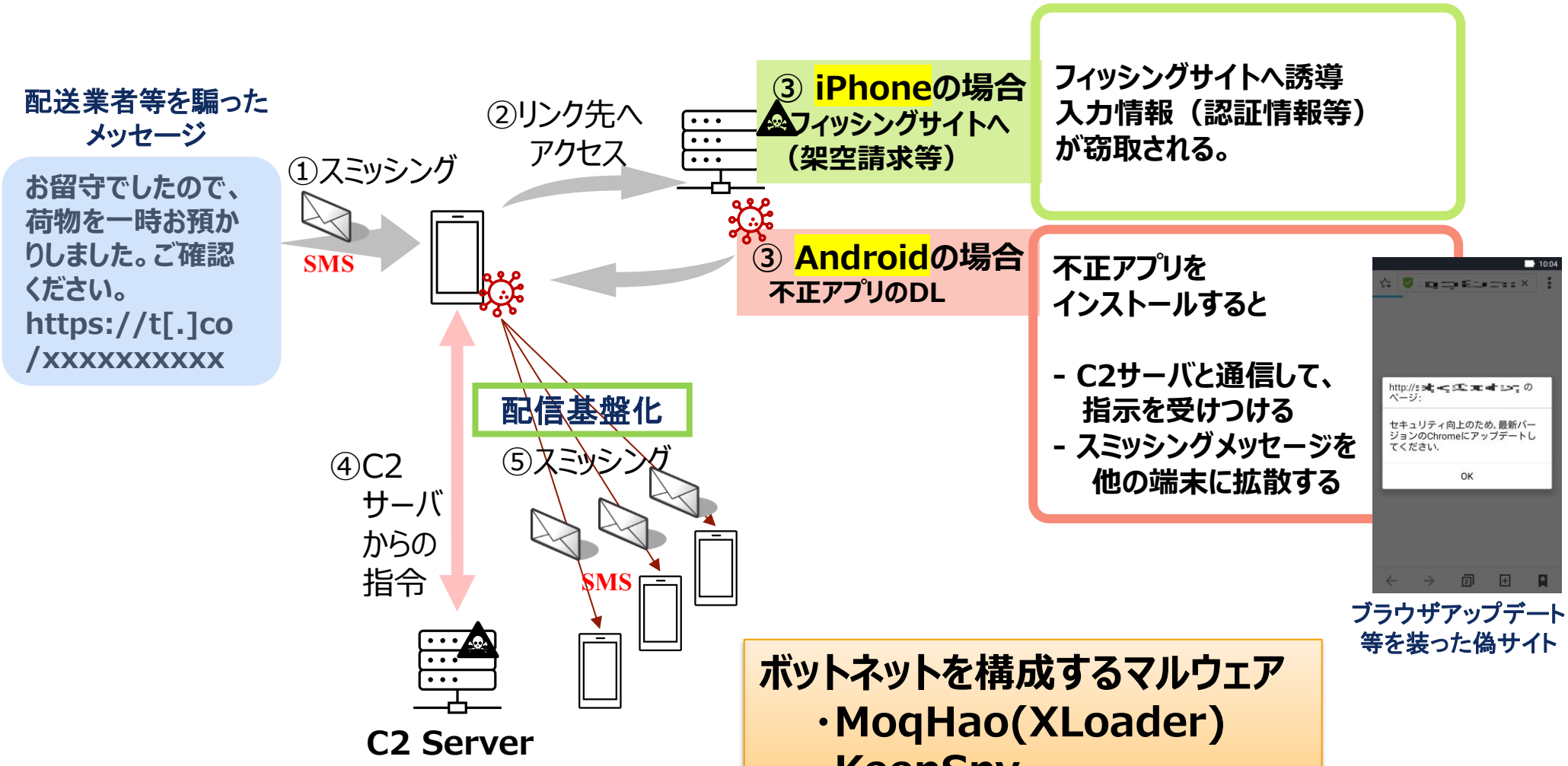
はじめに

このようなSMS（ショートメッセージサービス）
受け取ったことありますか？

お留守でしたので、荷物を一時お預かりしました。ご確認ください。
https://t[.]co/xxxxxxxxxx

【 ●●銀行 】お客様の口座の取引を一時的に規制しています、再開手続きをお願いします。
https://t[.]co/xxxxxxxxxx

脅威の流れ

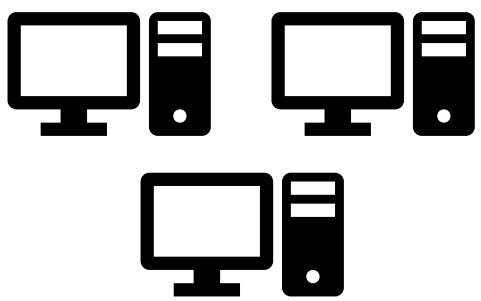


脅威の観測イメージ

ボットネットを構成するモバイルマルウェア

KeepSpy　Moqhao (Xloader)

観測



観測システム

観測結果

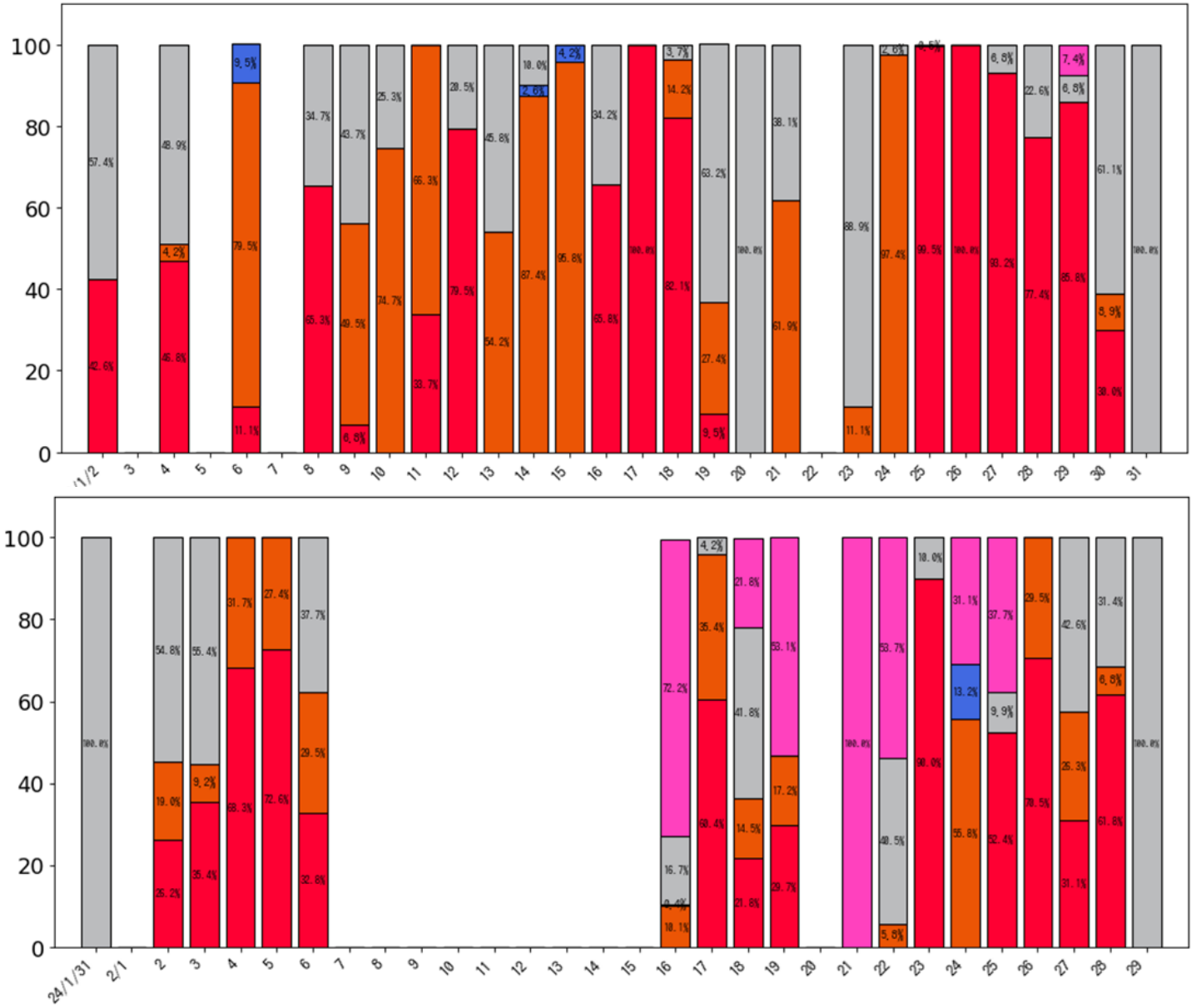
会員へ情報提供

JC3 日本サイバー犯罪対策センター

JC3 : Japan Cybercrime Control Center

観測結果を対策に活用

Moqhao/Xloader – SMS送信先の特徴（2024年1月･2月）



最近の動向（Moqhao/Xloader）

騙り先

- 不在配達連絡の形式

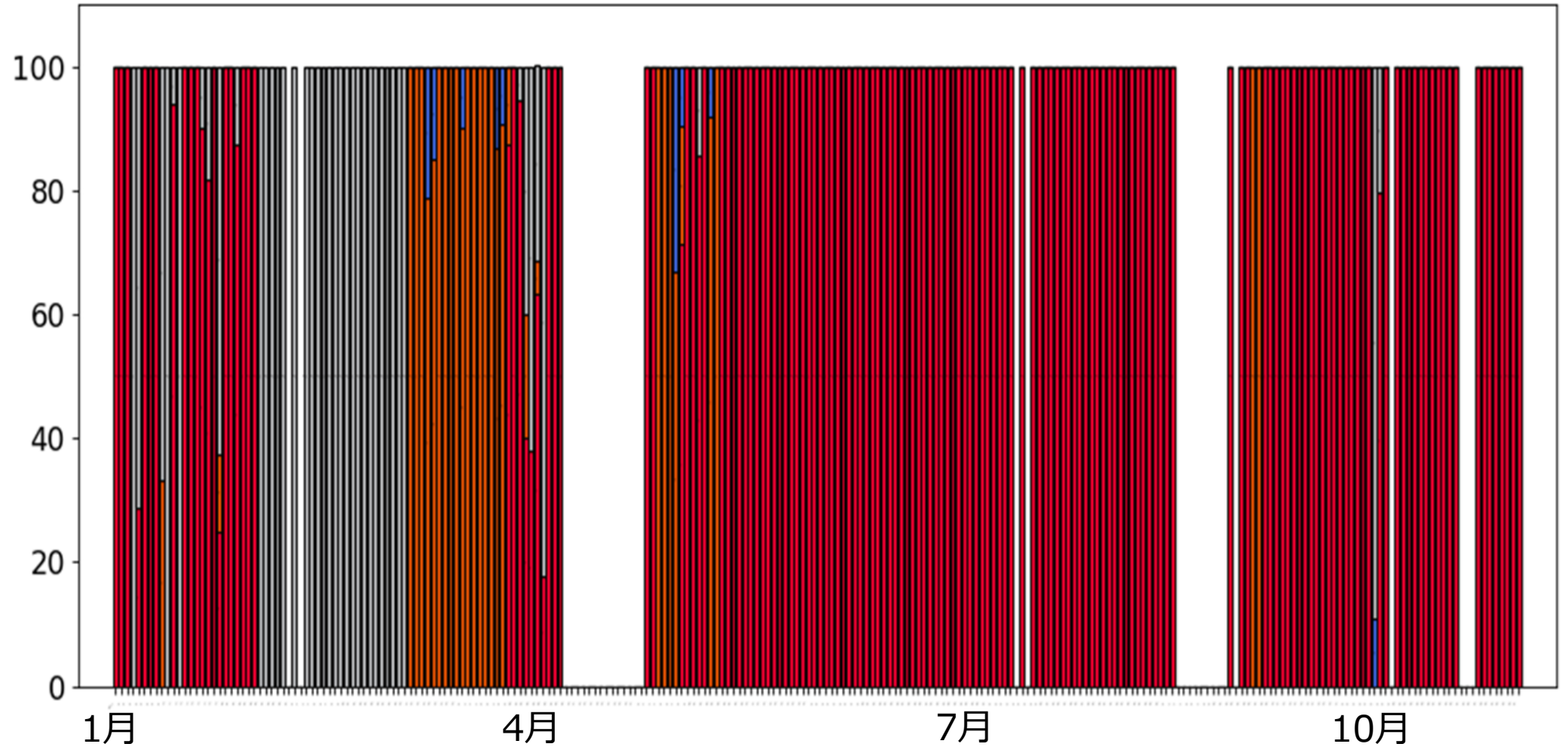
SMS拡散

- 長らく継続していたSMS拡散が、2024年6月末から10月中旬まで停止
- 2月中旬に攻撃が停止する傾向
- お昼時間近辺にSMSが配信される傾向
- 最近は特定の通信キャリアを狙ってSMSを拡散する傾向

その他

- SMS文章の作成に生成AI活用の傾向
- 英文を国外の電話番号宛てに送付したことも…

Keepspy – SMS送信先の特徴（2024年）



最近の動向（Keepspy）

騙り先

- 特定の都市銀行を執拗に狙う傾向
- 最近は土日に地方銀行を狙う傾向

SMS拡散

- ほぼ毎日SMS拡散指示あり
- 拡散時間はばらばら（早朝、夕方、夜分など）
- 特定の通信キャリアや地域を狙ってSMSを拡散する傾向

その他

- 10月、SMS内の誘導先URLに使用する短縮URLを一時的に変更


JC3
Japan Cybercrime Control Center