IPアドレスリースとAbuseの現状

～事例を通じた課題共有と調整への提言～

JPCERTコーディネーションセンター
インシデントレスポンスグループ
中井 尚子

JPCERT/CCとは

■ 一般社団法人JPCERTコーディネーションセンター

Japan Computer Emergency Response Team / Coordination Center

- コンピューターセキュリティインシデントへの対応、国内外にセンサーを置いたインターネット定点観測、ソフトウェアや情報システム・制御システム機器等の脆弱性への対応など**国内の「セキュリティ向上を推進する活動」**を実施
- **サービス対象：国内のインターネット利用者やセキュリティ管理担当者、ソフトウェア製品開発者等（主に、情報セキュリティ担当者）**
- インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、**日本の窓口となる「CSIRT」**
  ※各国に同様の窓口となるCSIRTが存在する
  （例：米国のCISA、CERT/CC、中国のCNCERT/CC、韓国のKrCERT/CC）

■ 経済産業省からの委託事業として**サイバー攻撃等国際連携対応調整事業を実施**

JPCERT/CCの活動

インシデント予防 → インシデントの予測と捕捉 → 発生したインシデントへの対応

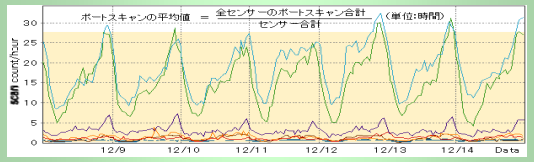
脆弱性情報ハンドリング

- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

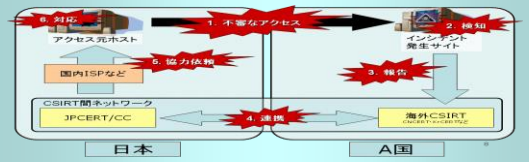
情報収集・分析・発信
定点観測（TSUBAME）

- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング
（インシデント対応調整支援）

- マルウェアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
脆弱性情報ハンドリング	ソフトウェア製品等の脆弱性情報に関わる開発者等との調整・公表
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
アーティファクト分析	マルウェア（不正プログラム）等の攻撃手法の分析、解析
制御システムセキュリティ	制御システムに関するインシデントハンドリング/情報収集,分析発信
国内外関係者との連携	フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

IPアドレスリースとAbuse

IPアドレスリースとは

- 本プレゼンテーションでは、IPアドレスを企業に対して一定期間貸し出すサービスを「IPアドレスリース」と定義する

アジェンダ

1. IPアドレスリースとフィッシングサイト
2. IPアドレスリースとAbuseの課題
3. 提言

1 IPアドレスリースとフィッシングサイト

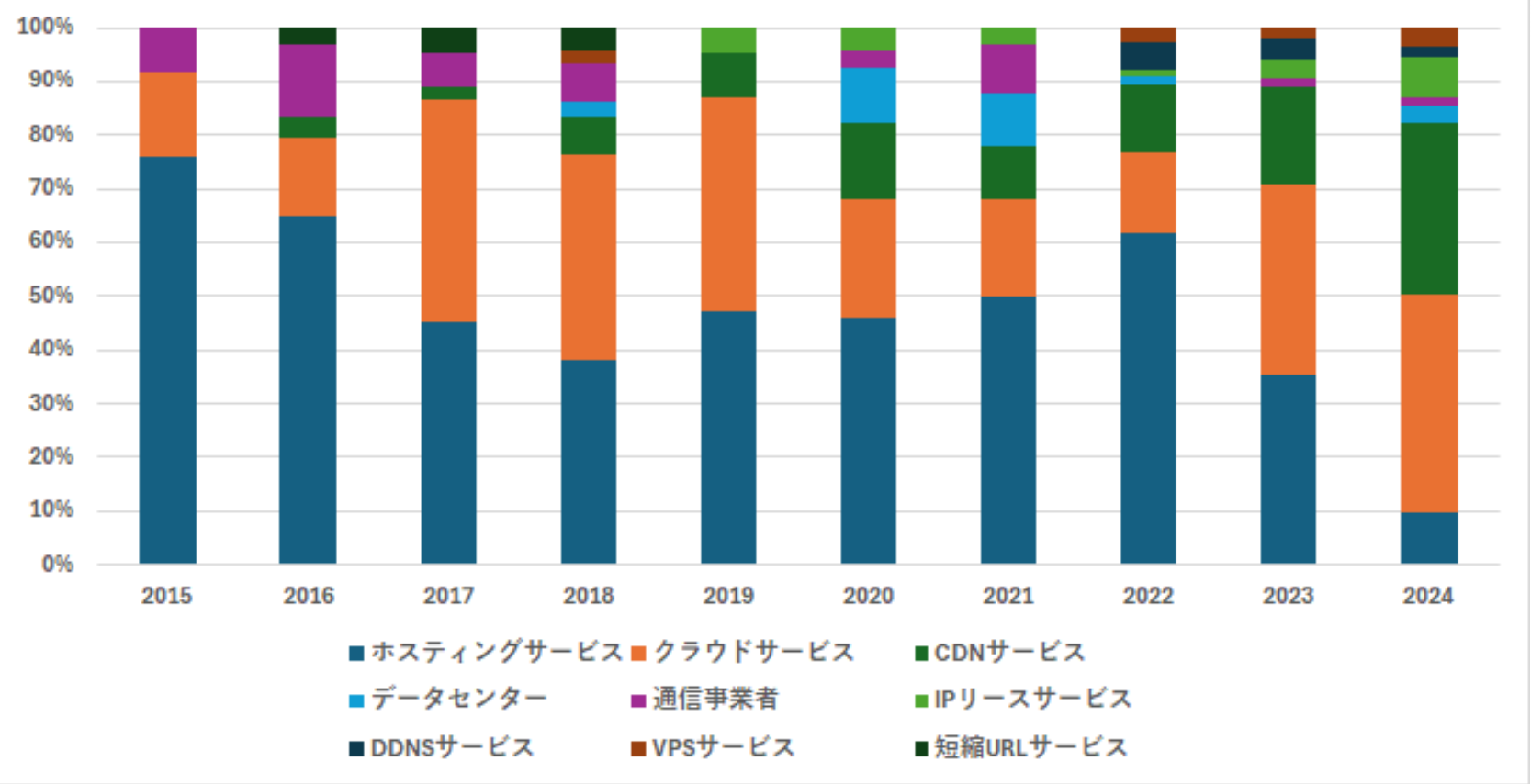
2 IPアドレスリースとAbuseの課題

3 提言

JPCERT/CCが調整するセキュリティインシデント

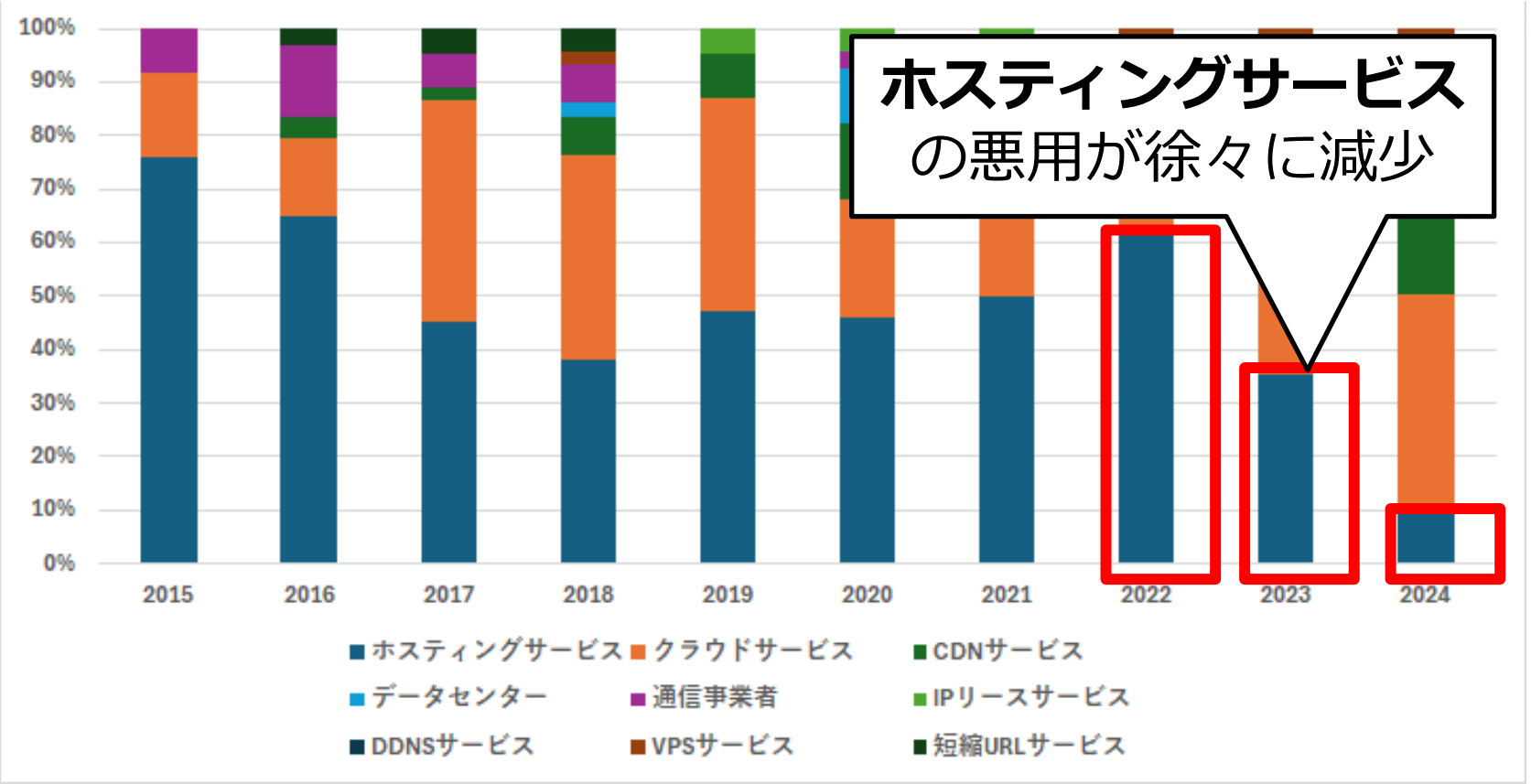
- フィッシングサイト
- マルウェア設置サイト
- 改ざんサイト
- DDoS／DoS／スキャン
- 標的型攻撃
- ランサムウェア

フィッシングサイトテイクダウン調整先の変遷



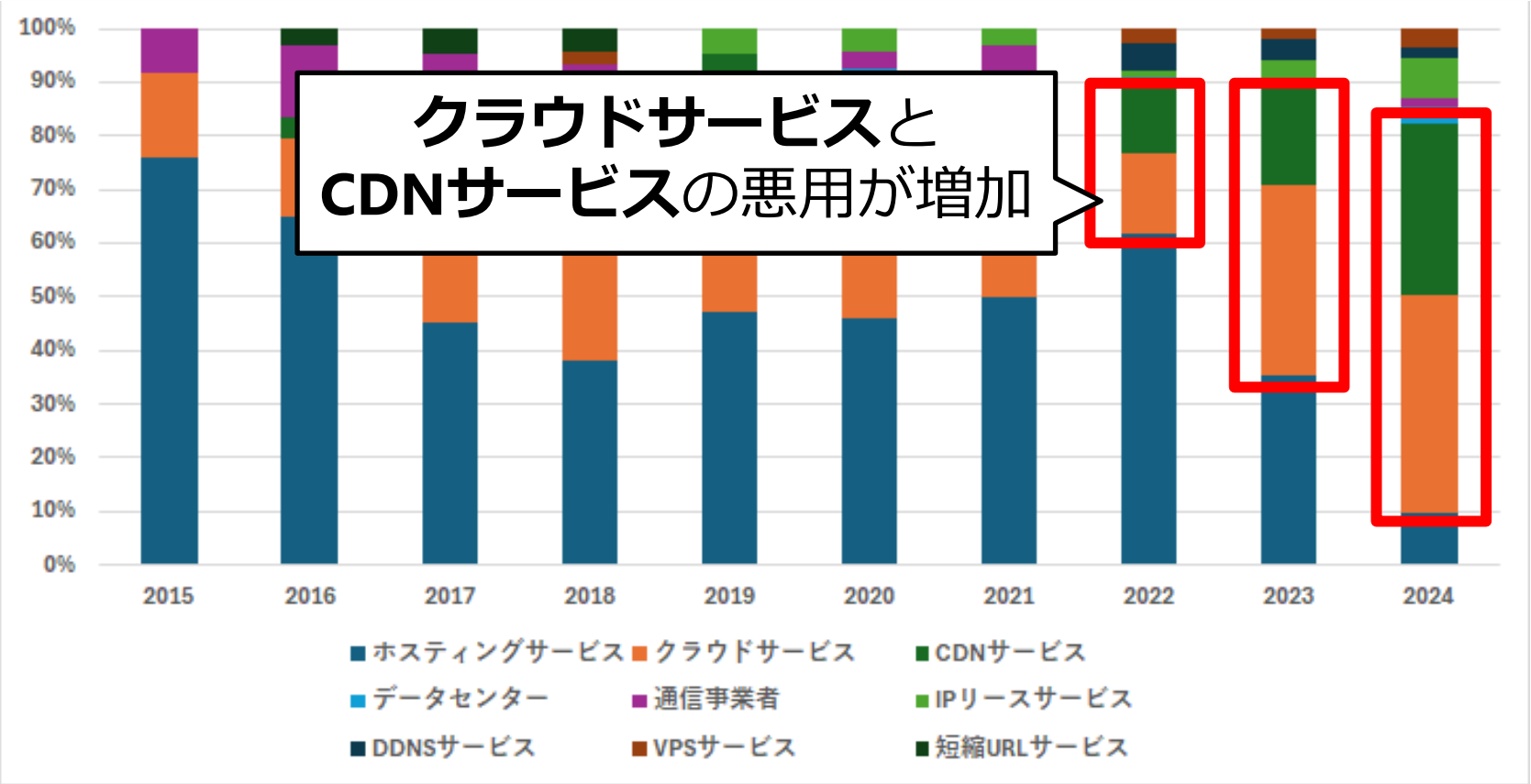
JPCERT/CCのデータをもとに筆者作成

フィッシングサイトテイクダウン調整先の変遷



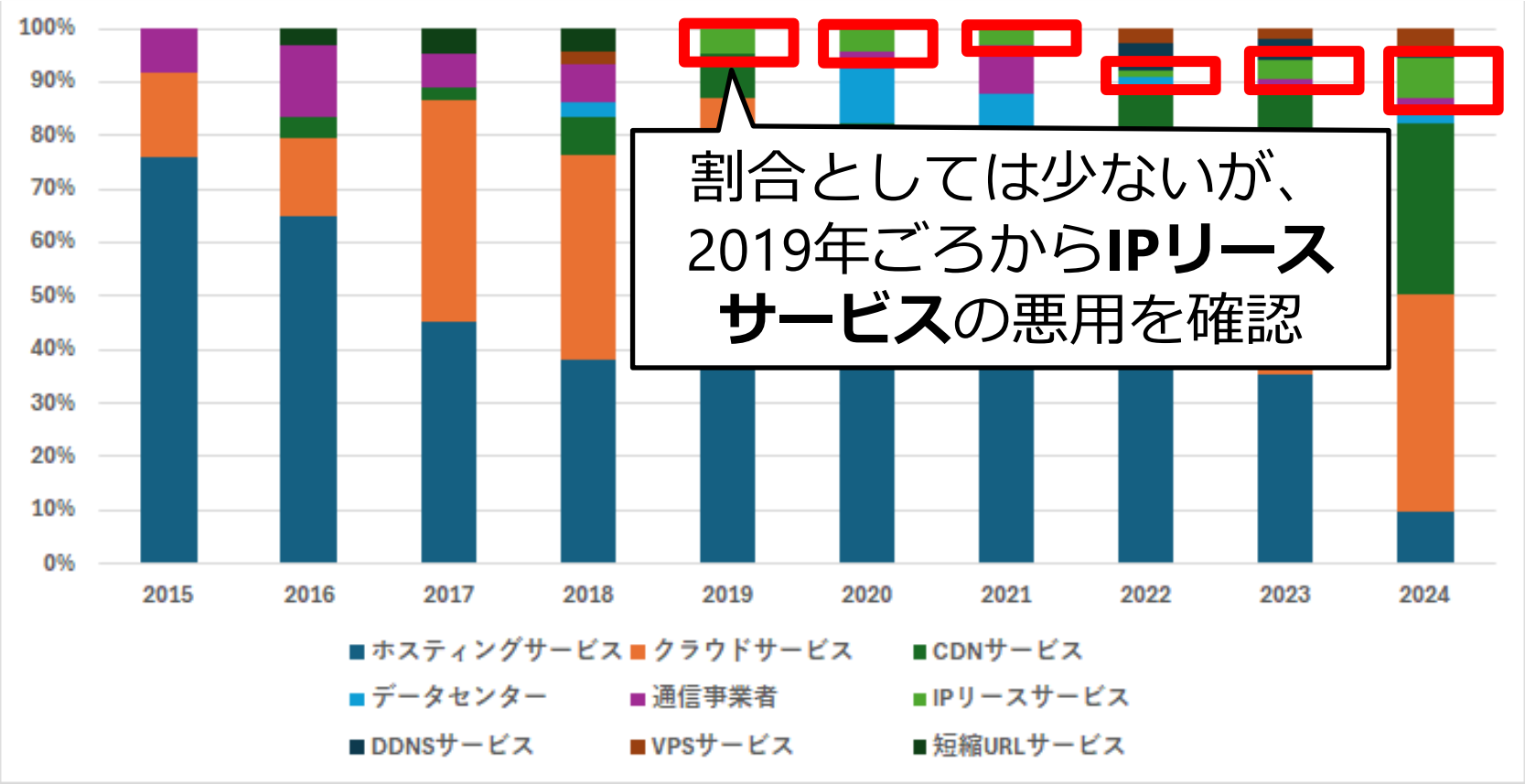
JPCERT/CCのデータをもとに筆者作成

フィッシングサイトテイクダウン調整先の変遷



JPCERT/CCのデータをもとに筆者作成

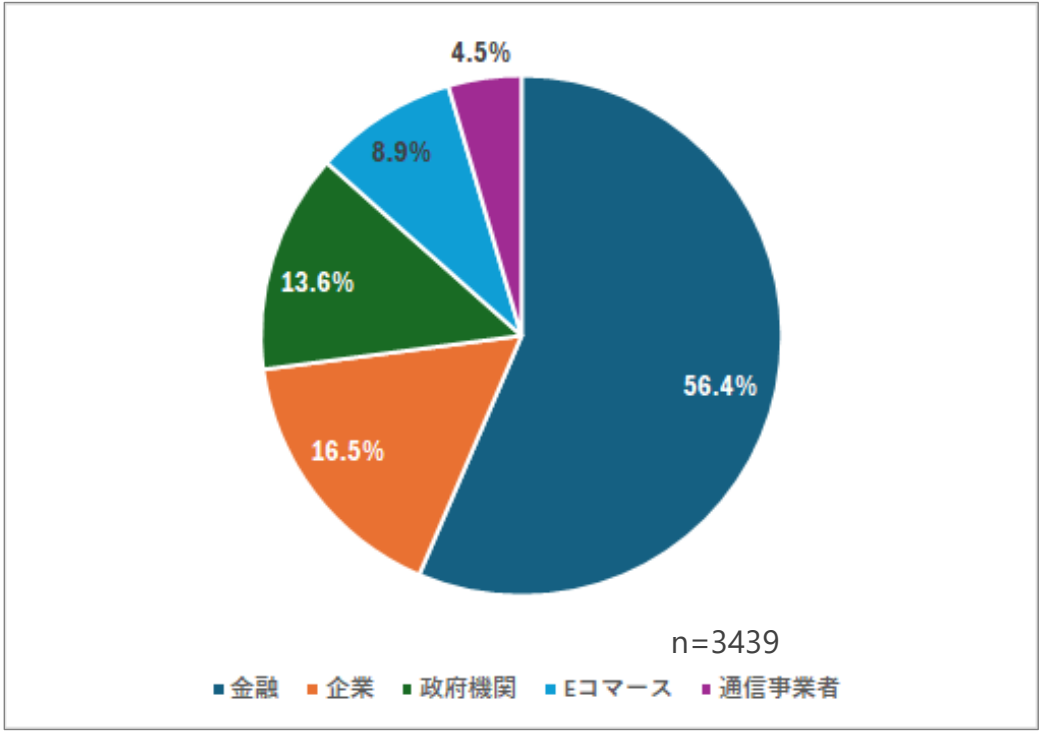
フィッシングサイトテイクダウン調整先の変遷



JPCERT/CCのデータをもとに筆者作成

IPアドレスリースされたIPアドレスで稼働していたフィッシングサイト

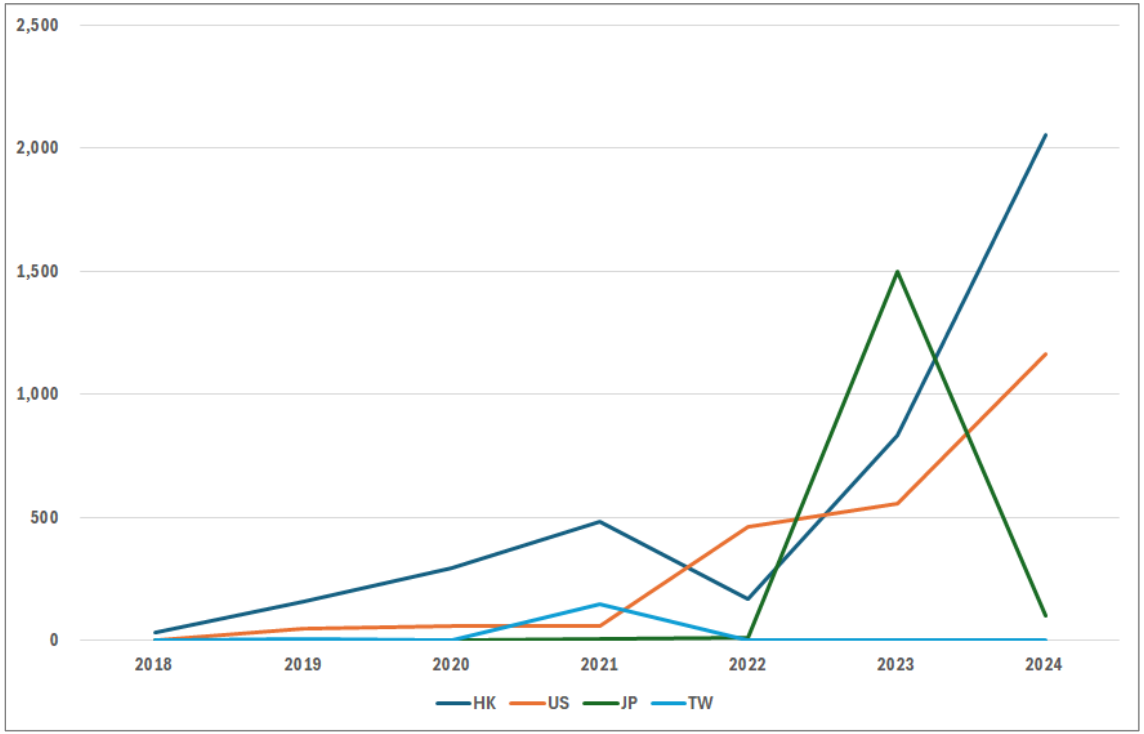
IPアドレスリースを使用したフィッシングサイトにおいてかたられた業種別割合



JPCERT/CCのデータをもとに筆者作成

IPアドレスリースされたIPアドレスで稼働していたフィッシングサイト

IPアドレスリースを使用したフィッシングサイトの通知先国



JPCERT/CCのデータをもとに筆者作成

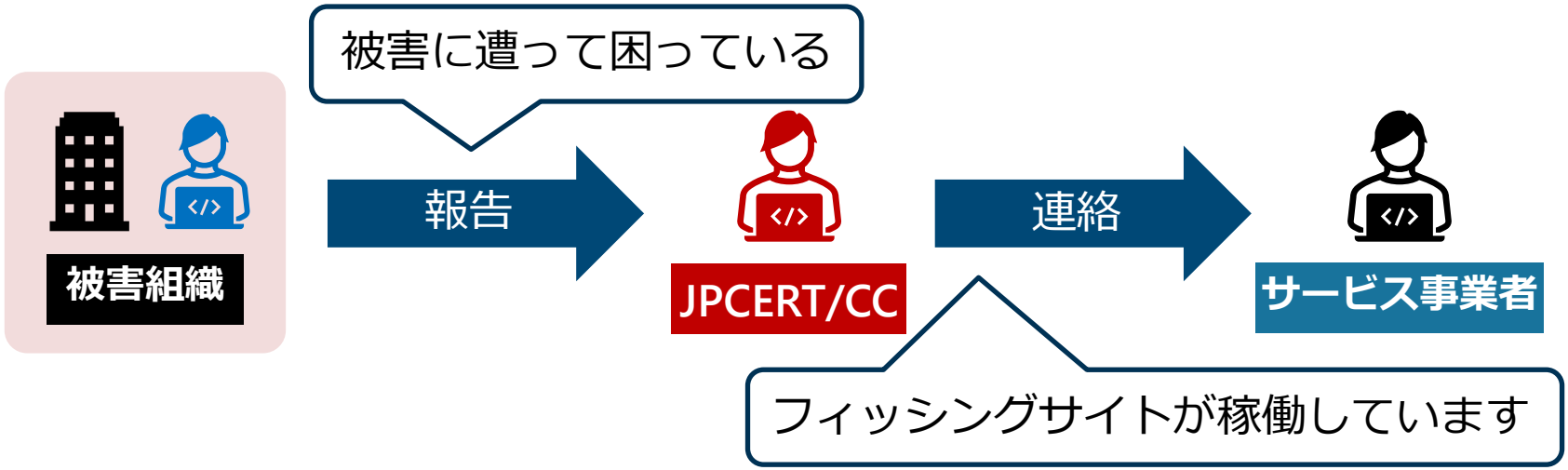
1 IPアドレスリースとフィッシングサイト

2 IPアドレスリースとAbuseの課題

3 提言

JPCERT/CCの調整活動

フィッシングサイトが稼働する当該IPアドレスを管理しているサービス事業者と調整し、フィッシングサイトを停止させる



どの情報をもとに通知先を決定するのか？

どの情報をもとに通知先を決定するのか？

WHOIS

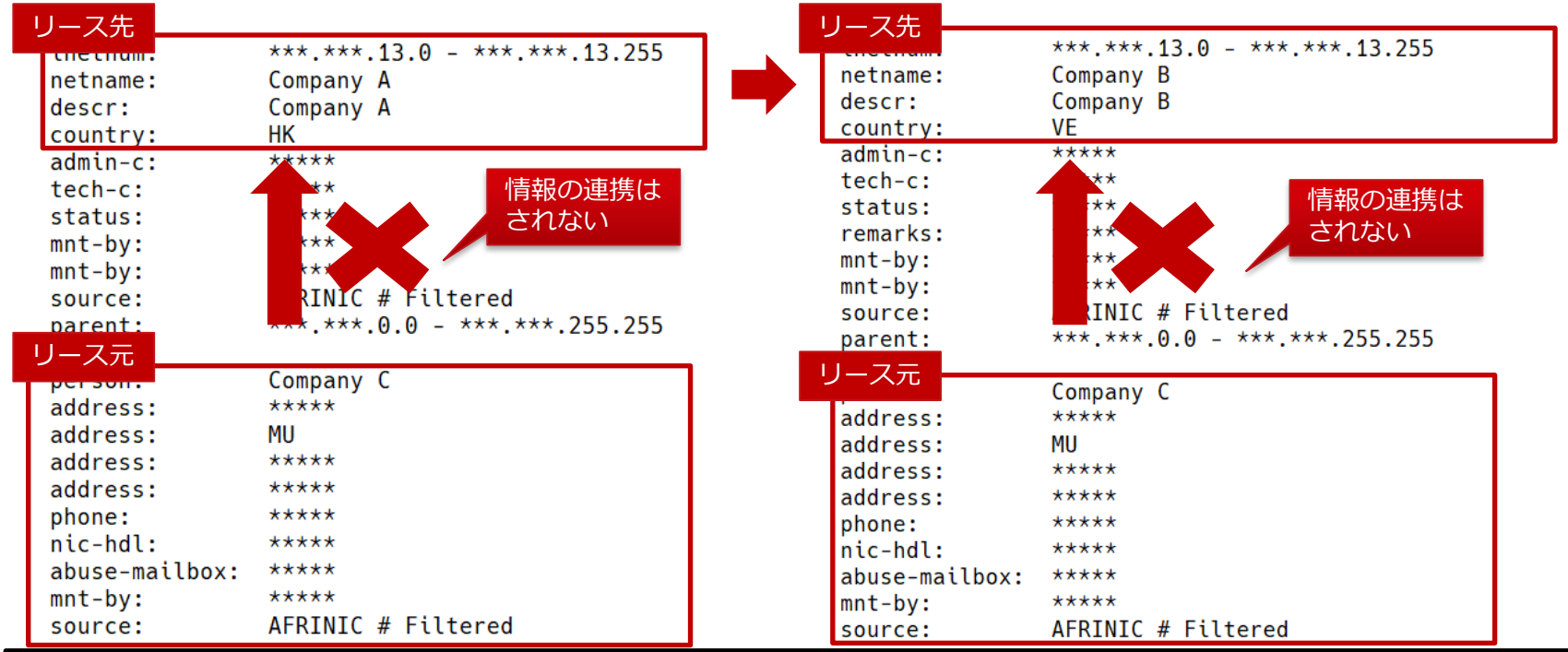
どの情報をもとに通知先を決定するのか？

WHOIS

WHOIS情報の正確性こそが、
セキュリティインシデントにおける調整活動の生命線

異なる国・事業者へ入れ替わり

- 2024年：HK　→　2025年：VE



IPアドレスリース事業者からリース先事業者へのAbuse報告連携はない

IPアドレスリースのAbuseにおける問題

IPアドレスリース事業者の問題

IPアドレスリース事業者がリース先の詳細な状況を
把握していない

IPアドレスリース事業者が貸出先に是正を促さない
（連絡しない）

セキュリティインシデントの継続

IPアドレスリースのAbuseにおける問題

IPアドレスリース先の問題

WHOIS情報を正しく登録しない
（Abuse窓口を設置しない）

IPアドレスリース先の事業者に連絡できない

セキュリティインシデントの継続

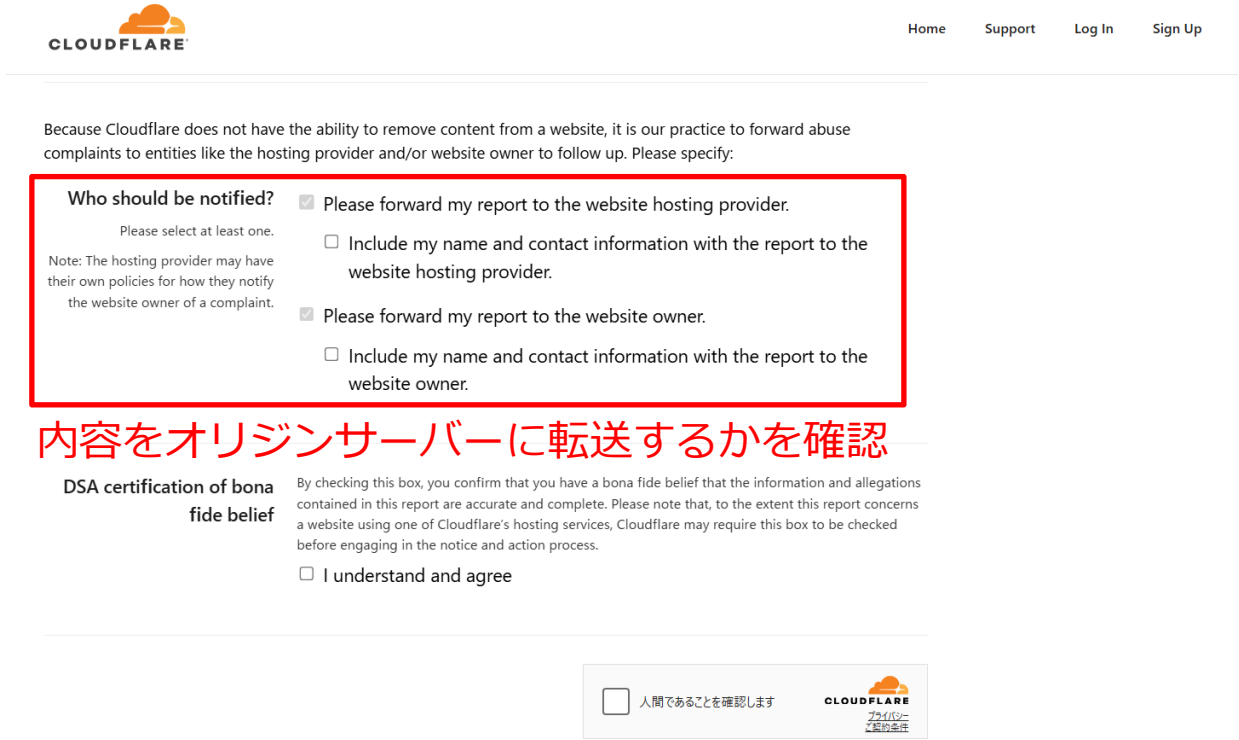
参考：CDN事業者の取り組み

- Cloudflareは、当初Abuse活動に消極的で、
  エンドユーザーに連絡することはなかった

- 現在は、フィッシングサイトなどの通知後、
  早急にアクセスの遮断およびエンドユーザーの通知を
  実施

Cloudflare

- Form　https://abuse.cloudflare.com/phishing



1 IPアドレスリースとフィッシングサイト

2 IPアドレスリースとAbuseの課題

3 提言

調整活動を行う組織としての期待

WHOIS（RDAP）の正確性

- IPアドレスリース事業者は、リース先の情報の正確性と、連絡先の確保
- インシデント対応可能な窓口の登録

Abuse体制の整備

- リース先事業者は、Abuse連絡を受けた場合の対処を整理
- 規約の整備
- ユーザーへの注意喚起方法の整備

参考：IPXOの取り組み

- IPXOは、IPアドレスリース事業者として活動をしている
- IPアドレスリース先の事業者のWHOIS登録をサポートする体制、またAbuse連絡先登録はIPアドレス借り受け時、必須条件としている

Customizing WHOIS records for leased IP addresses is now possible with IPXO

最後に

WHOISデータベースの登録情報は、セキュリティインシデント対応において極めて重要であり、正確性を維持することが求められる

WHOIS情報の迅速な更新が難しい場合は、インシデント調整機関からの連絡が適切な担当者に確実に転送されるよう対応を徹底する必要がある

インシデントの報告は、被害を受けた方からの切実な依頼である場合が多い。そのため、報告内容を適切に確認し、迅速かつ確実な対応をお願いしたい

ご清聴ありがとうございました。