いかにしてメールセキュリティ問題をとくか（なりすまし・フィッシング・etc）

株式会社TwoFive

目次

- TwoFive について
- なりすましメール（DMARC/DKIM/BIMI）トレンド
- フィッシングサイトトレンド
- なりすましメールとフィッシングサイトの関係性
- まとめ・今後の対策を考える
- 質疑応答

3名の紹介

- 加瀬　正樹
- 佐々木　智彦
- 藤田　善光

TwoFive 事業内容

電子メールの信頼性と安全性の向上の鍵となる
3本のソリューションをご提供しています。

メッセージング
システム

メッセージング
セキュリティ

twofive
3本の柱

スレット
インテリジェンス

いかにして問題をとくか

- まずは問題をよく理解する
- 理解した上で、計画を立てて実行する
- 実行した結果を振り返り、次につなげる

G. Polya, 1975

いかにしてメールセキュリティ問題をとくか

- まずは **メールセキュリティ問題** をよく理解する
- 理解した上で、計画を立てて 実行 **実態調査** する
- 実態調査した結果を振り返り、次（**対策の開発**）につなげる

メールセキュリティ問題をよく理解する

攻撃手法・リスク	対策	対応技術（抜粋）
ウイルス・スパム・マルウェアの受信	コンテンツフィルタ・送信元チェック	コンテンツフィルタ
フィッシング	コンテンツフィルタ・出口対策	Passive DNS, Spamhaus, OSINT
なりすましメールの受信	DMARC・SPF・DKIM・BIMI	OpenDMARC, 他milter
ホモグラフドメイン攻撃	コンテンツフィルタ・モニタリング	Passive DNS, OSINT
EAC（アカウント不正利用）	認証強化・ピッチコントロール	2FA, 機械学習
不正転送	認証強化・ユーザ通知	2FA
RBL（ブロックリスト）への過剰登録	ピッチコントロール・宛先クリーニング	ー
データ漏洩	TLS・MTA-STS・S/MIME	サーバ証明書, クライアント証明書
大量通信・大量メール送受信	SMTP認証・ピッチコントロール	IP Warm-up, ピッチコントロール
メールドメイン乗っ取り	認証強化・モニタリング	2FA, ネームサーバ監視
BEC（ビジネスメール詐欺）	ビジネスフロー整備・教育	出口対策, メール訓練

メールセキュリティ問題をよく理解する

攻撃手法・リスク	対策	対応技術（抜粋）
ウイルス・スパム・マルウェアの受信	コンテンツフィルタ・送信元チェック	コンテンツフィルタ
フィッシング	コンテンツフィルタ・出口対策	Passive DNS, Spamhaus, OSINT
なりすましメールの受信	DMARC・SPF・DKIM・BIMI	OpenDMARC, 他milter
ホモグラフドメイン攻撃	コンテンツフィルタ・モニタリング	Passive DNS, OSINT
EAC（アカウント不正利用）	認証強化・ピッチコントロール	2FA, 機械学習
不正転送	認証強化・ユーザ通知	2FA
RBL（ブロックリスト）への過剰登録	ピッチコントロール・宛先クリーニング	ー
データ漏洩	TLS・MTA-STS・S/MIME	サーバ証明書, クライアント証明書
大量通信・大量メール送受信	SMTP認証・ピッチコントロール	IP Warm-up, ピッチコントロール
メールドメイン乗っ取り	認証強化・モニタリング	2FA, ネームサーバ監視
BEC（ビジネスメール詐欺）	ビジネスフロー整備・教育	出口対策, メール訓練

いかにしてメールセキュリティ問題をとくか

- まずは **メールセキュリティ問題** をよく理解する
- 理解した上で、計画を立てて 実行 **実態調査** する
- 実態調査した結果を振り返り、次（**対策の開発**）につなげる

フィッシング詐欺
なりすましメール
を調査

いかにしてメールセキュリティ問題をとくか

- まずは **メールセキュリティ問題** をよく理解する
- 理解した上で、計画を立てて 実行 **実態調査** する
- 実態調査した結果を振り返り、次（**対策の開発**）につなげる

フィッシング詐欺
なりすましメール
に対抗する方法を考える

フィッシング詐欺とは

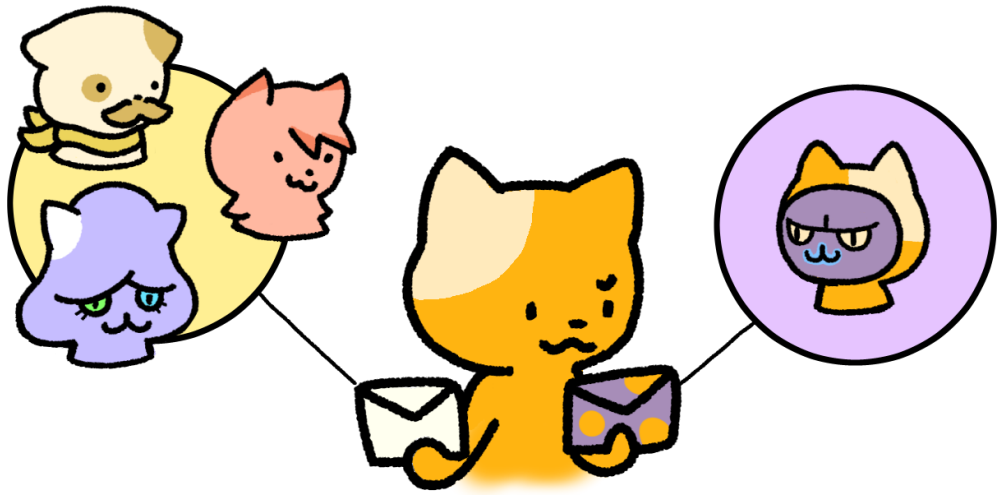
- 有名ブランドを装ったメッセージで**フィッシングサイトへ誘導**し、
  認証情報・決済情報や個人情報を詐取する。
  - ログイン画面や決済画面を装い情報を入力させる
  - アプリのインストールを促しマルウェア感染させる

- 詐取された情報は不正利用・悪用され**金銭的な被害等が発生**する。
  - ID盗用
  - クレジットカード不正利用
  - 電話帳盗み出し、SMS送信

なりすましメールとは

- 差出人情報を使って**他者・組織を装いメールを送信**する。
  - エンベロープFrom
  - ヘッダーFrom
  - 表示名（ディスプレイネーム）

- 個人向けだけでなくビジネスシーンでも**悪用され金銭的な被害等が発生**する。
  - 請求書詐欺
  - ID盗用
  - クレジットカード不正利用



c.f. アカウント乗っ取り（ID 盗用）

- フィッシング詐欺やなりすましメールを悪用して取得した認証情報（ID やパスワード情報）で**他者・組織のシステムを乗っ取る**
  - データ漏洩
  - なりすましメール送信
  - etc

- 今回はスコープとしない

なりすましメール（DMARC/DKIM/BIMI）トレンド

DMARC

認証

IPアドレス(SPF)や
電子署名(DKIM)を使って
なりすましメールか
どうかを認証する

ポリシー

ドメイン所有者が
認証に失敗したメールの
取り扱い方法を
受信側に宣言する

レポート

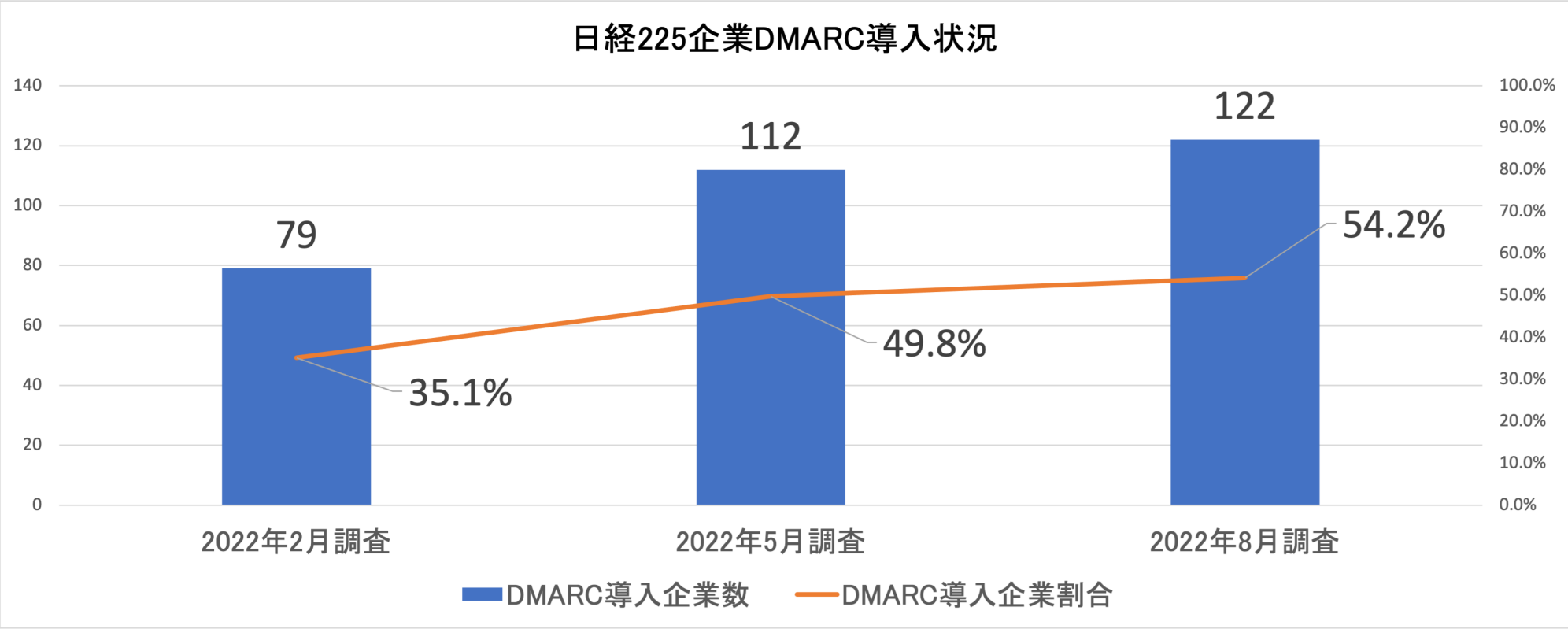
サーバに届いたメールの
認証結果を
ドメイン所有者に
レポート送信する

twofive

- 2016年政府サービス義務化
- 2017年政府ドメイン義務化
- 2020年6月 フィッシング対策協議会
  フィッシングレポート2020記載
- 2020年7月 NISC
  サイバーセキュリティ 2020記載
- 2022年8月 日経225銘柄 (TwoFive調査)
  DMARC 導入企業は 54.2 %

国内企業の DMARC 導入状況

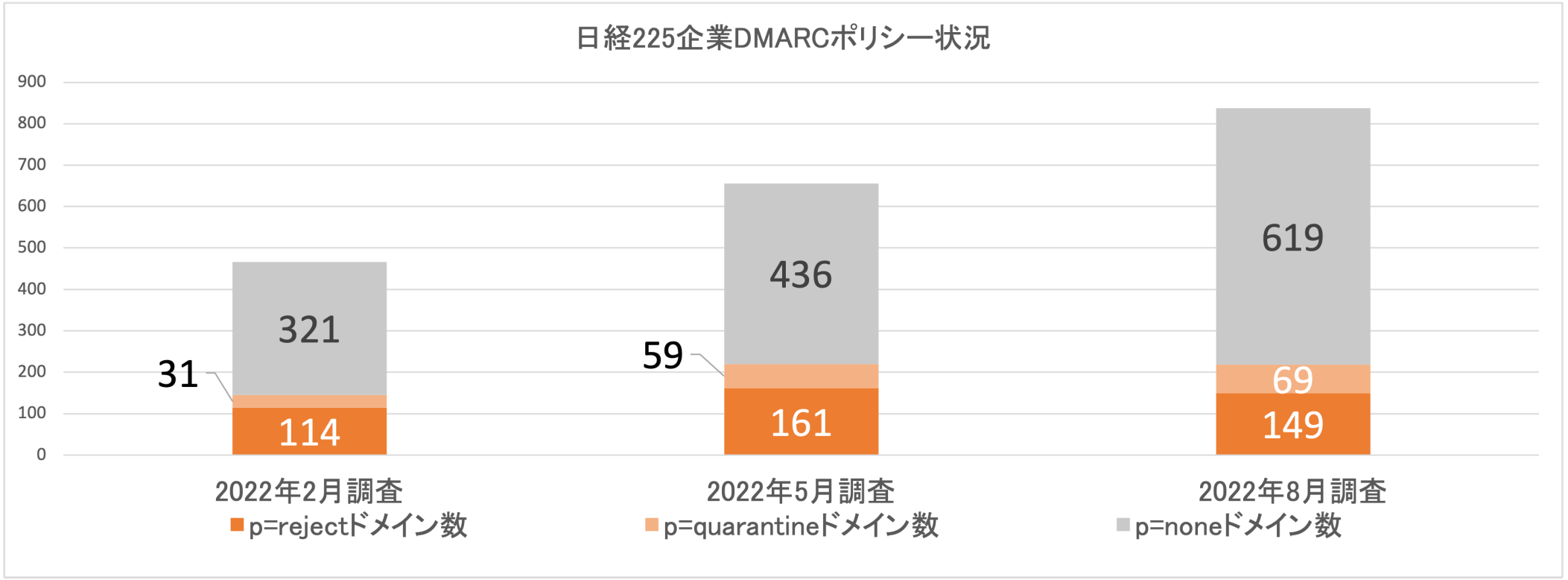
- 日経225銘柄が所有するドメインのDMARC導入率は 50% を超えた
- 2022年2～5月と比較すると、やや伸びは小さいが依然として上昇傾向



引用: TwoFive 調査, https://www.twofive25.com/news/20220519_dmarc_report.html

国内企業の DMARC ポリシー設定状況

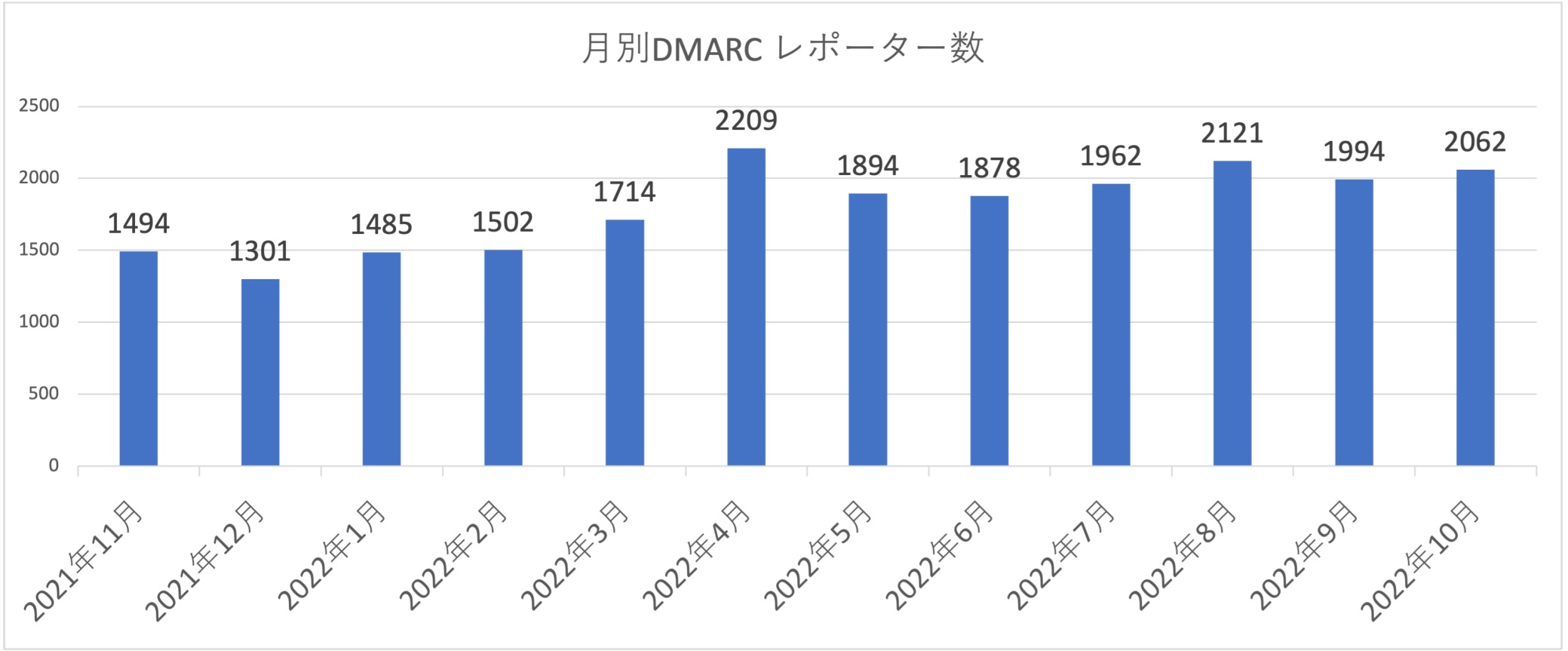
- 日経225銘柄の DMARC ポリシー設定は月によって変動あり
- p=quarantine, p=reject のメールドメイン数は増加傾向



引用: TwoFive 調査, https://www.twofive25.com/news/20220519_dmarc_report.html

受信側の DMARC 対応状況

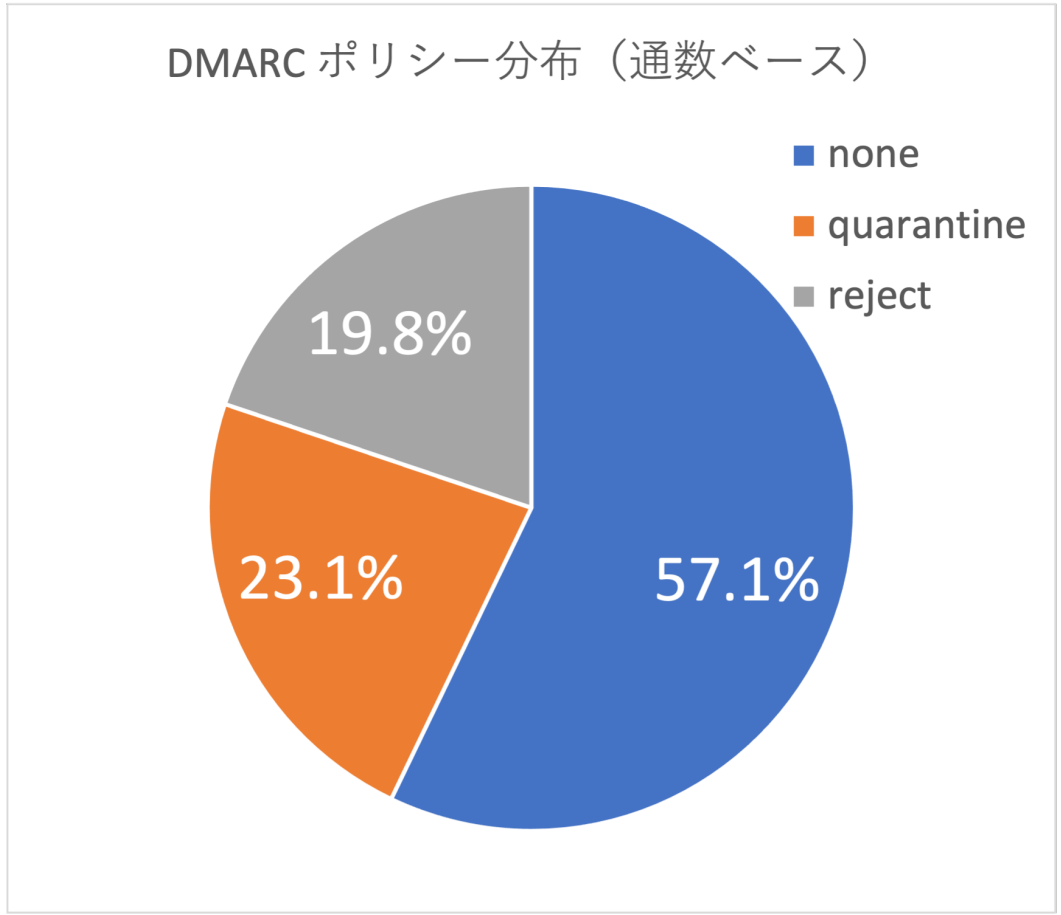
- DMARCレポート送信サーバ・組織は 2,000 に拡大中
- レポート送信数 TOP5 は Google, Microsoft, nifty, Yahoo.com, Amazon

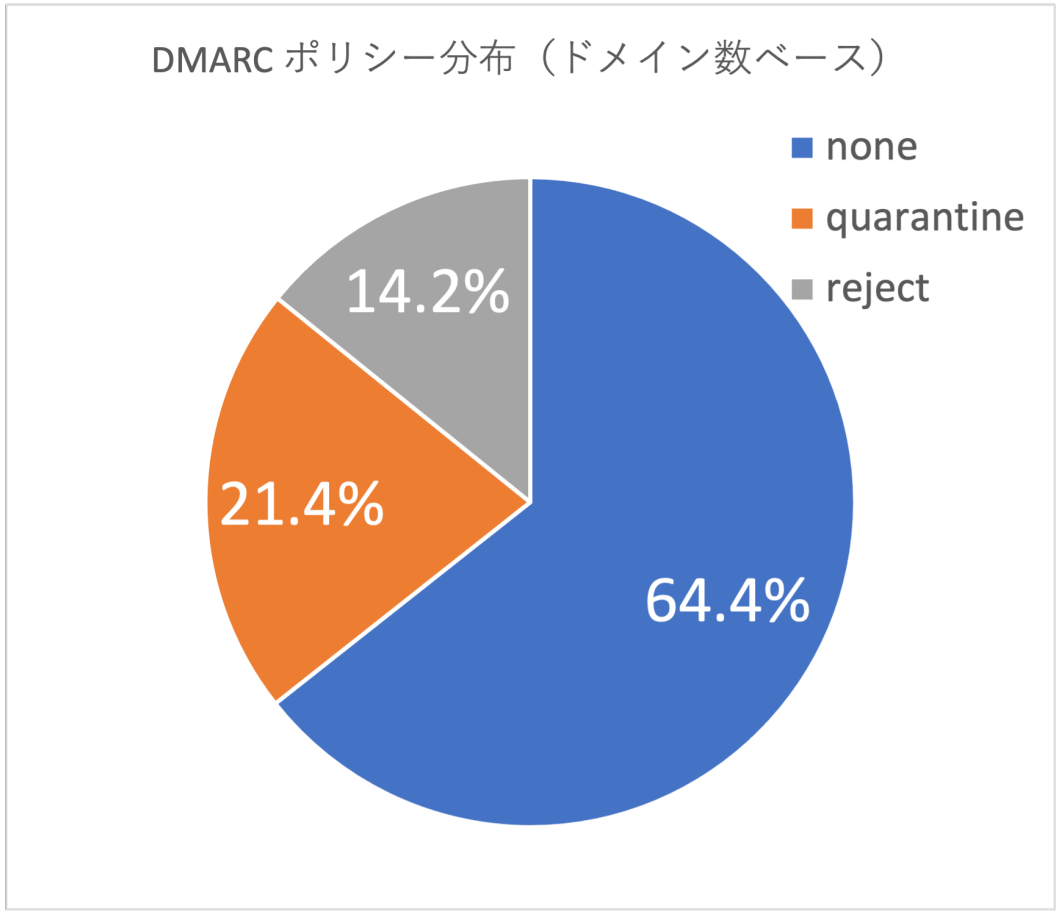


DMARC/25 Analyze 調査

受信側で観測された DMARC ポリシーの割合

- ある ISP における受信メール統計（2022年10月某日）
- 3割以上が p=quarantine または p=reject

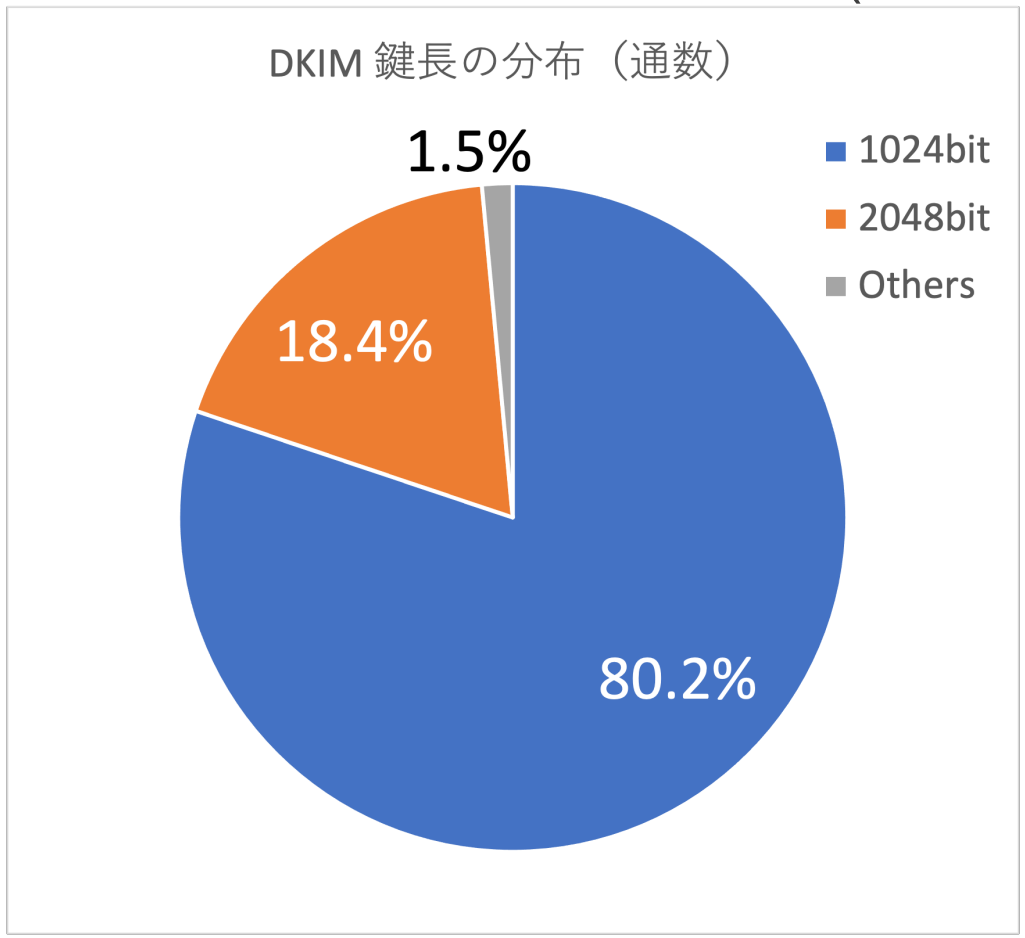


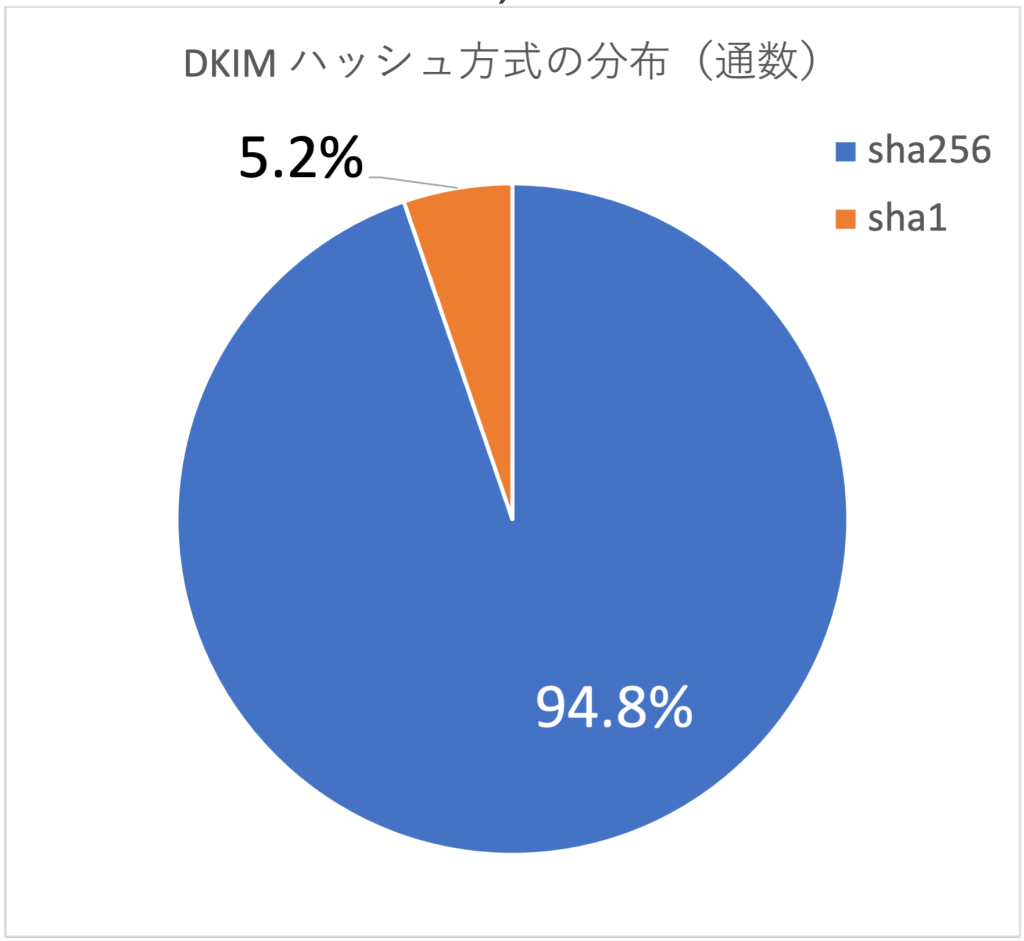


DMARC/25 Reporter 調査

受信側で観測された DKIM 署名方式の割合

- 鍵長は 1024bit が大半だが 2048bit も増加傾向。
- ハッシュは sha256 に移行 (sha1は非推奨だが残っている)

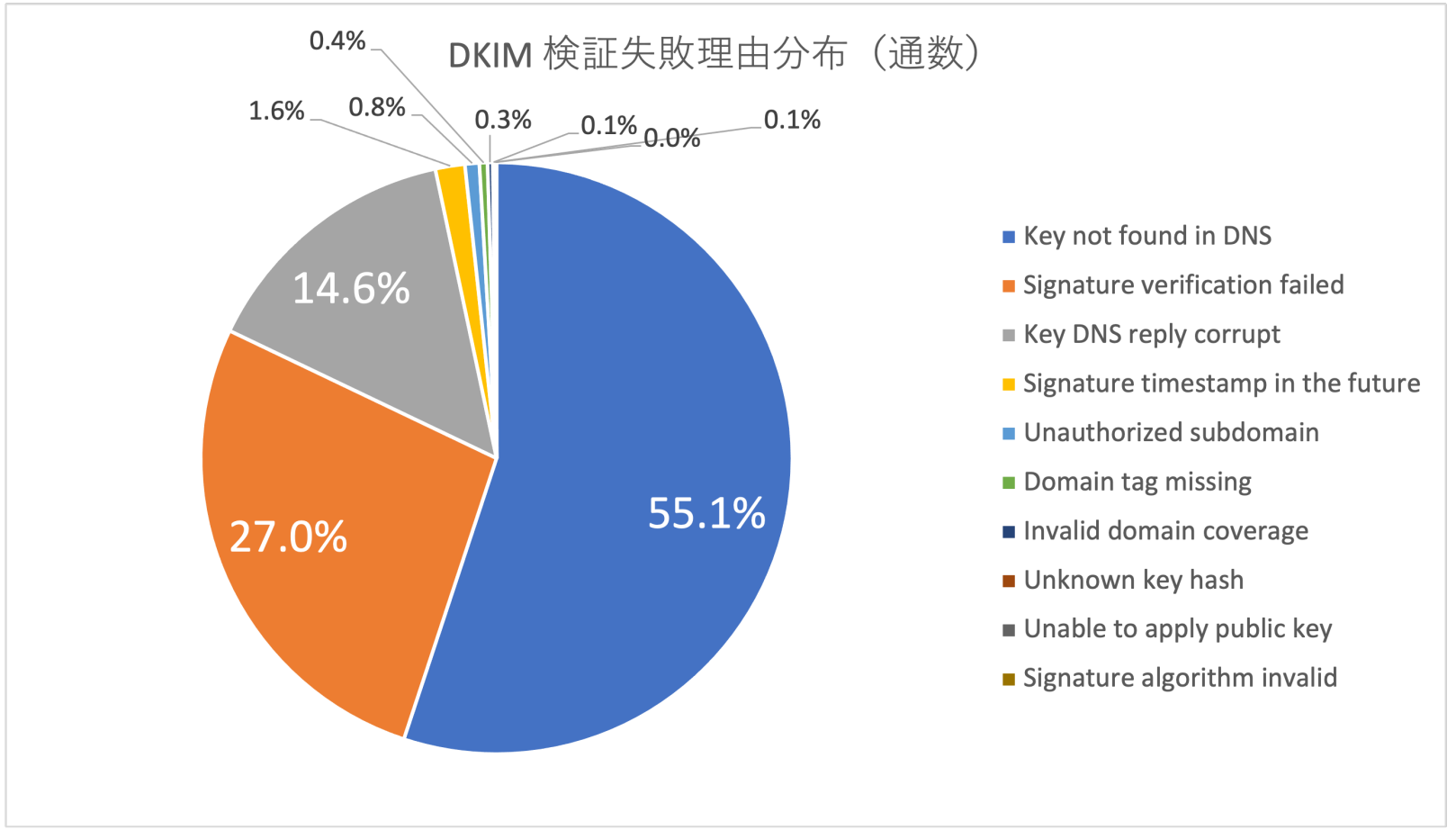




DMARC/25 Reporter 調査

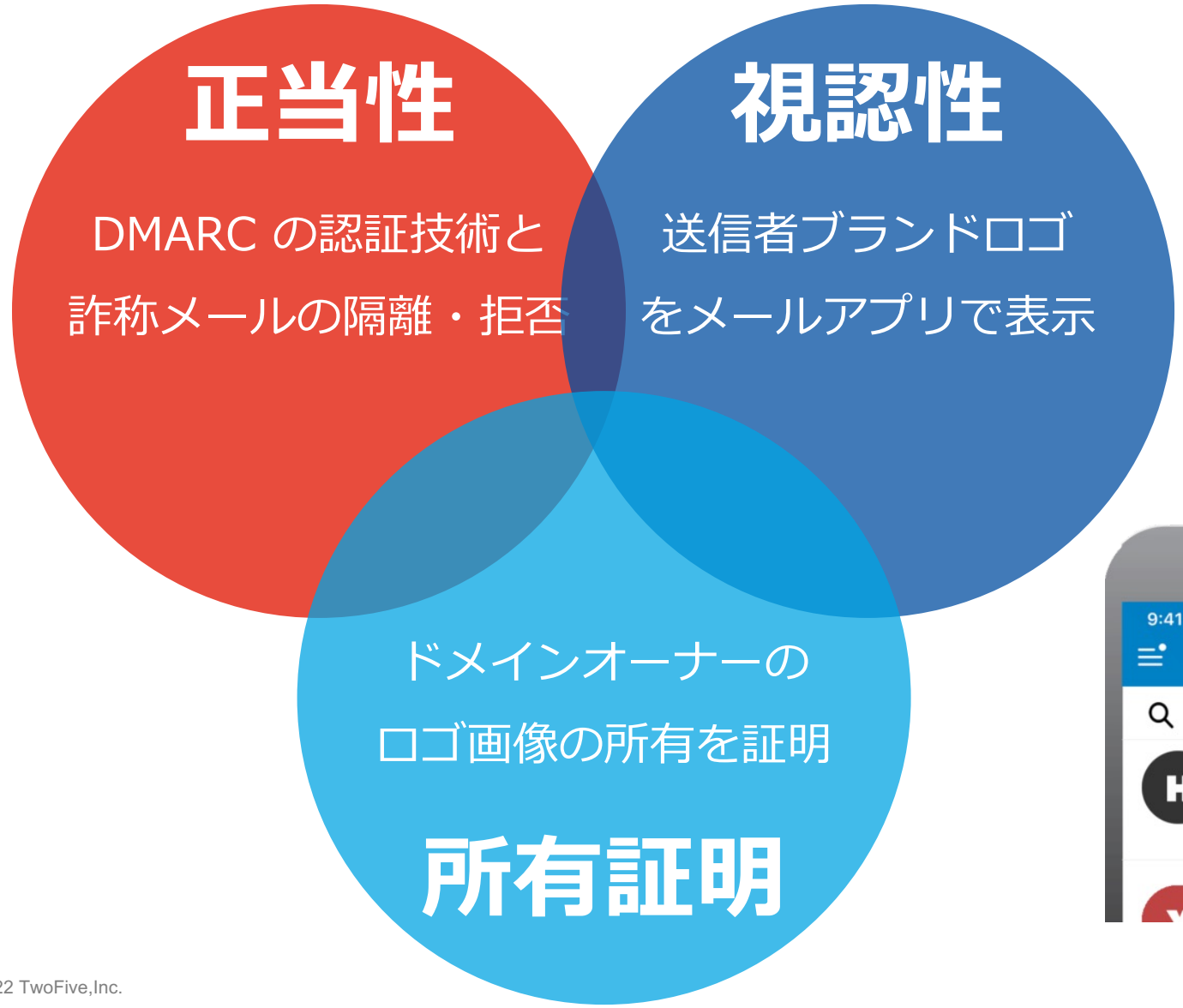
受信側で観測された DKIM 署名検証失敗理由

- DNS 公開鍵未設定が 50% 以上
  - 攻撃者が “default” をセレクター指定する場合も多いと思われる(レコード不在)



DMARC/25 Reporter 調査

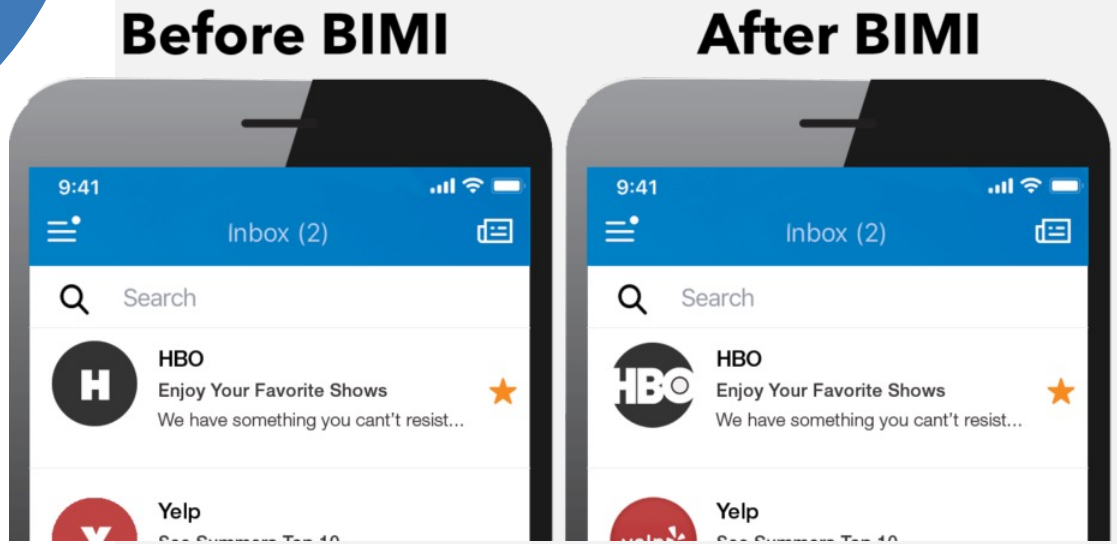
BIMI – 3つの可視化



twofive

様々なプラットフォームが WG 参画
DMARC やそのポリシー強化の推進のため
BIMI 規格を策定

Fastmail　Google
mailchimp　proofpoint　TWILIO SendGrid
validity　VALIMAIL TRUST YOUR EMAIL　verizon media



参考: https://bimigroup.org/

BIMI – アイコン表示の条件

- DMARC ポリシーは p=quarantine 以上
  - 組織ドメインで p=reject あるいは (p=quarantine かつ pct=100)
  - sp=none の場合は対象外
- アイコン画像は SVG フォーマット
  - スクリプトを含まない画像（ SVG Tiny PS ）
- VMC (Verified Mark Certificate) の発行
  - アイコン画像を証明するため。商標登録チェックもある。
  - Gmail で表示させるためには必要
- アイコン画像、VMC証明書の場所をBIMIレコードで宣言

BIMI – 設定方法

- DNS の TXT レコード（default._bimi.example.jp）で宣言をする
- ロゴを出し分けるためにセレクターを指定可能（デフォルトは “default”）

v=BIMI1; l=https://example.jp/xxx.svg; a=https://example.jp/xxx.pem

バージョン

アイコンの URL

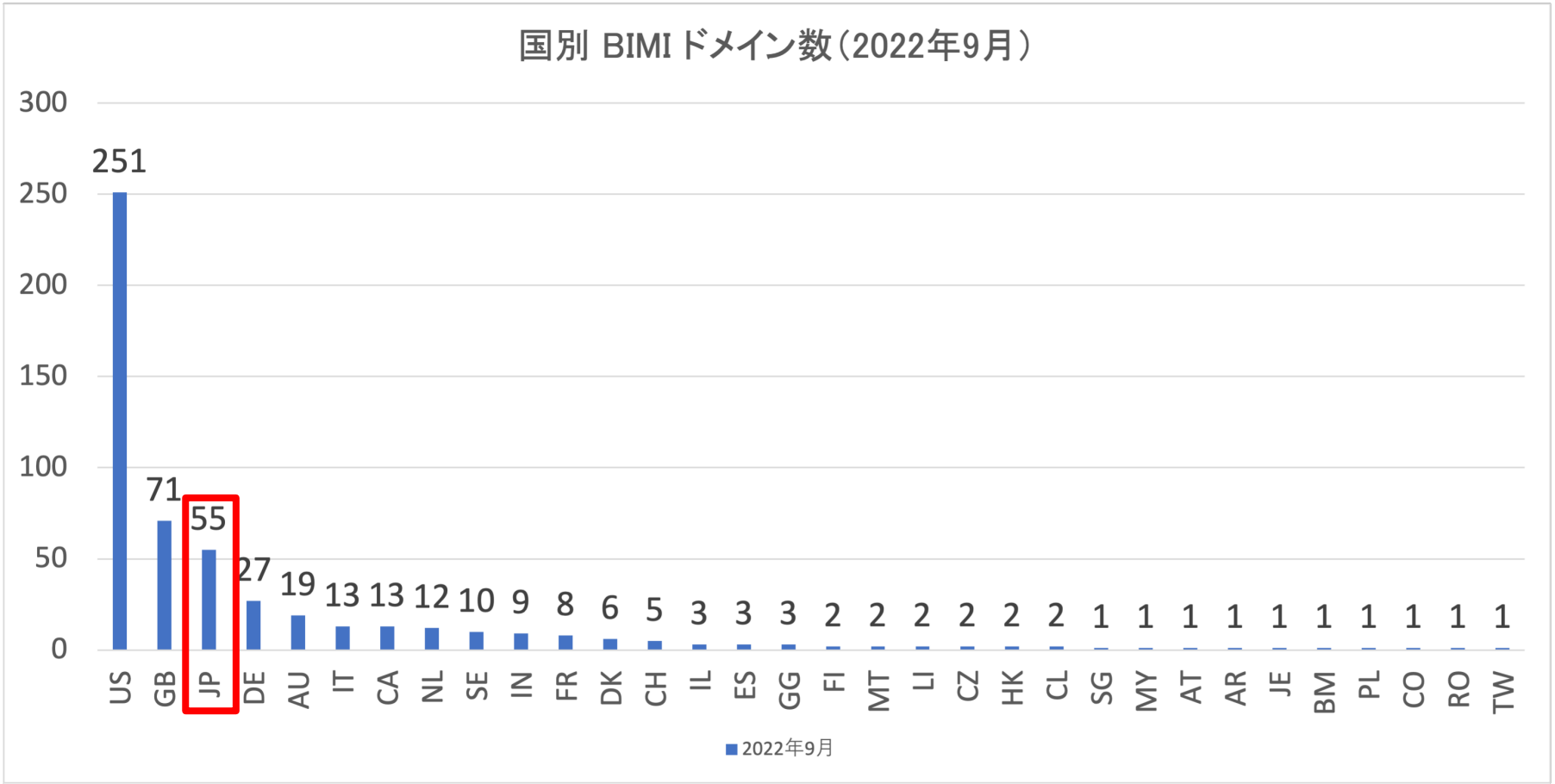
l=タグは
HTTPS サーバに配置

VMC の URL

a=タグは
HTTPS サーバに配置

BIMI対応ドメイン数

- 2022年9月調査では、メールドメインで BIMI 対応は 2,466 ドメイン
- VMC が設定されていたのは 578 ドメイン（日本では 55 ドメイン）



TwoFive 調査

BIMI対応ドメインの例（2022年9月）

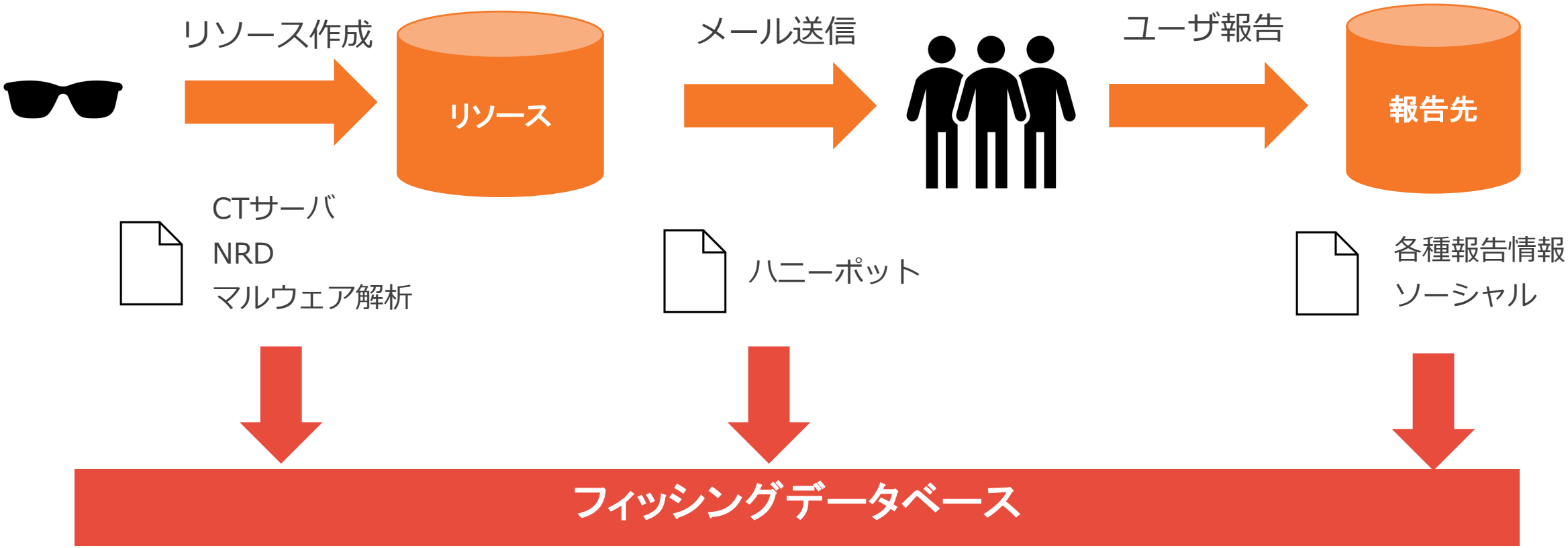
amazon.co.jp 他
v=BIMI1;l=https://d3frv9g52qce38.cloudfront.net/amazon_web_services_196911883.svg; a=https://d3frv9g52qce38.cloudfront.net/amazon_web_services_196911883.pem
rakuten.co.jp 他
v=BIMI1; l=https://r.r10s.jp/com/bimi/r_crimsonred/r_crimsonred.svg; a=https://r.r10s.jp/com/bimi/r_crimsonred/r_crimsonred_177085657.pem
disneyplus.com
v=BIMI1; l=https://d3cmxxs15s2e2m.cloudfront.net/DPlus_square_SVG_PS.svg; a=https://d3cmxxs15s2e2m.cloudfront.net/dPlus_VMC_2021.pem
nvidia.com
v=BIMI1; l=https://www.nvidia.com/content/dam/logos/nvidia_corporation.svg; a=https://www.nvidia.com/content/dam/logos/nvidia_corporation.pem;
mail.yahoo.co.jp
v=BIMI1; l=https://bimi.west.edge.storage-yahoo.jp/yahoo_japan_corporation_224791083.svg; a=https://bimi.west.edge.storage-yahoo.jp/yahoo_japan_corporation_224791083.pem

TwoFive 調査

フィッシングトレンド

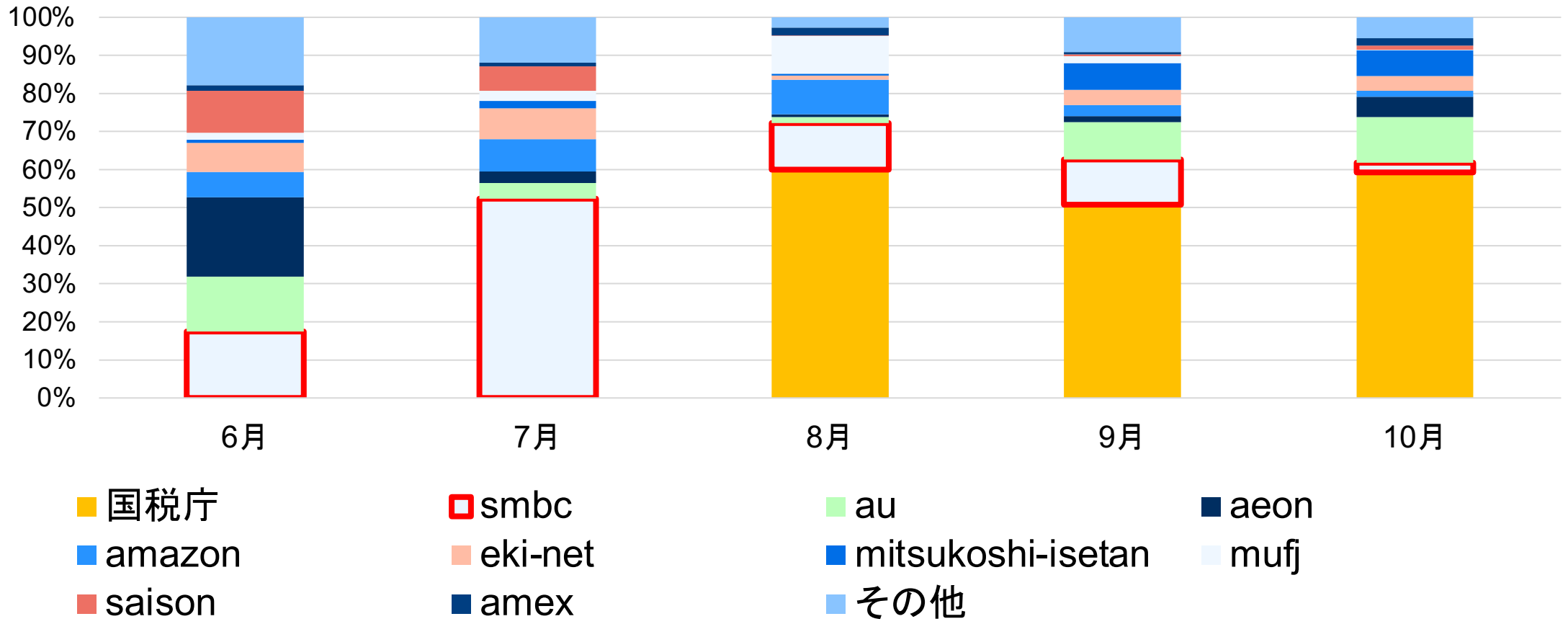
調査したデータ

- フィッシング情報取得元
  - 取得できるところから多角的に取得
  - 先勝ちデータを利用



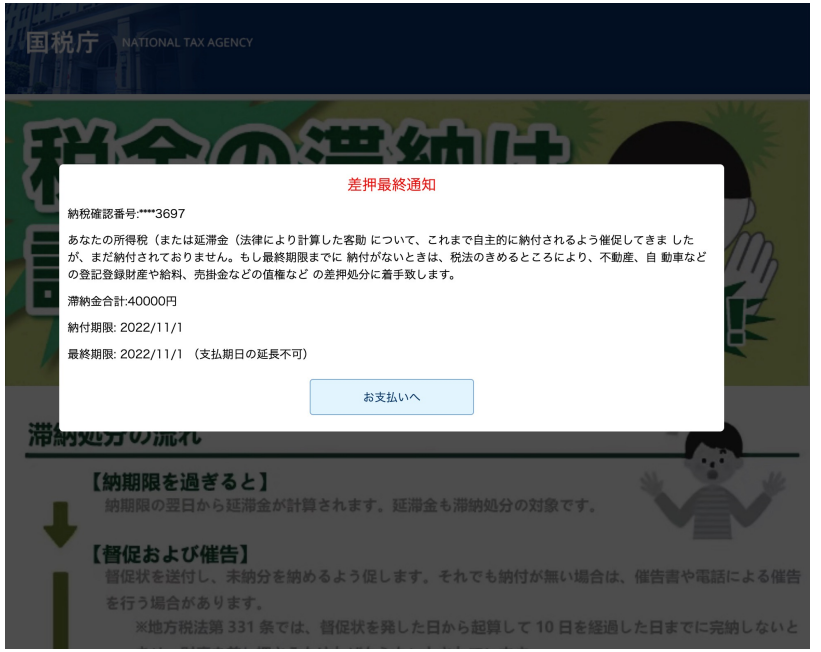
ブランド情報

- 国税庁への攻撃が多くいまだに続いている
  - ８月から開始されている



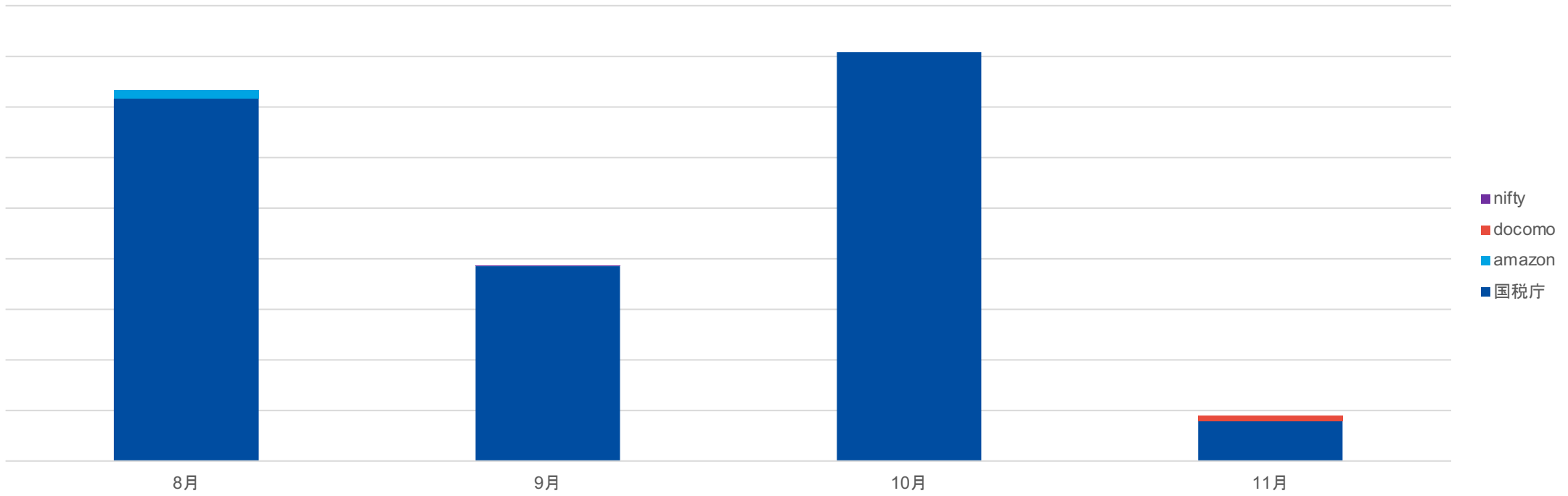
国税庁のフィッシングサイト

- 所得税の延滞金の支払いを催促
  - 支払いは電子マネー
- 特徴
  - 単一証明書で複数のサブジェクト代替名使用
  - duckdnsを利用
  - 漢字が一部中国語(所得税, 滞納 etc)



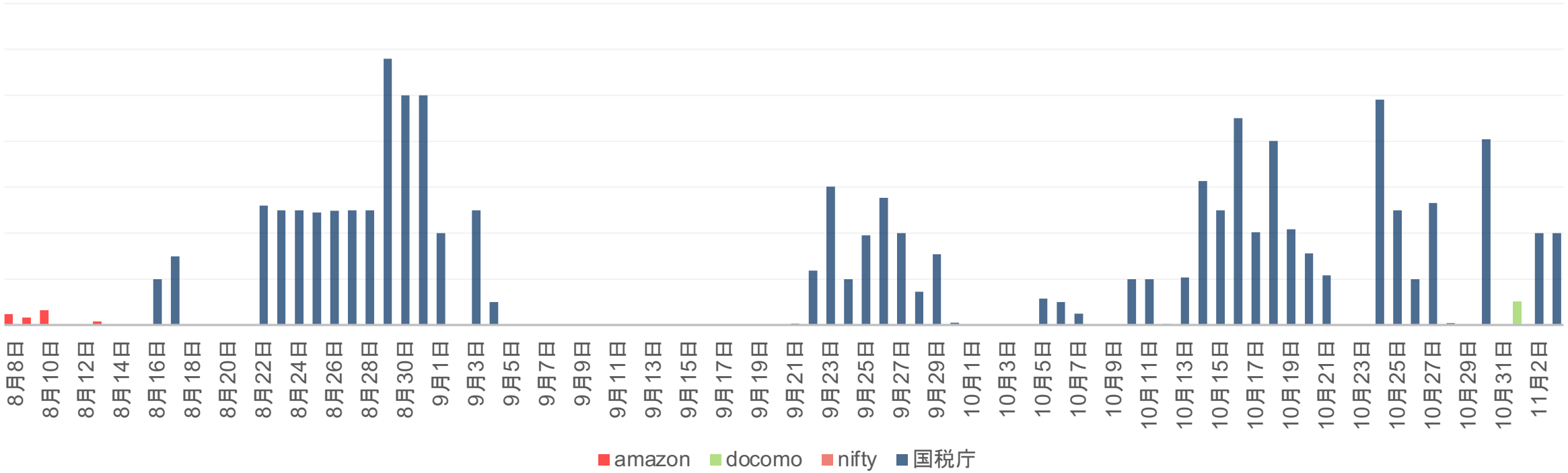
duckdns

- 無料のダイナミックDNSサービス
  - 簡易的にduckdns.org下のサブドメインが取れるのでフィッシングに利用される
- 6,7月は落ち着いて8月から大量に使用されている



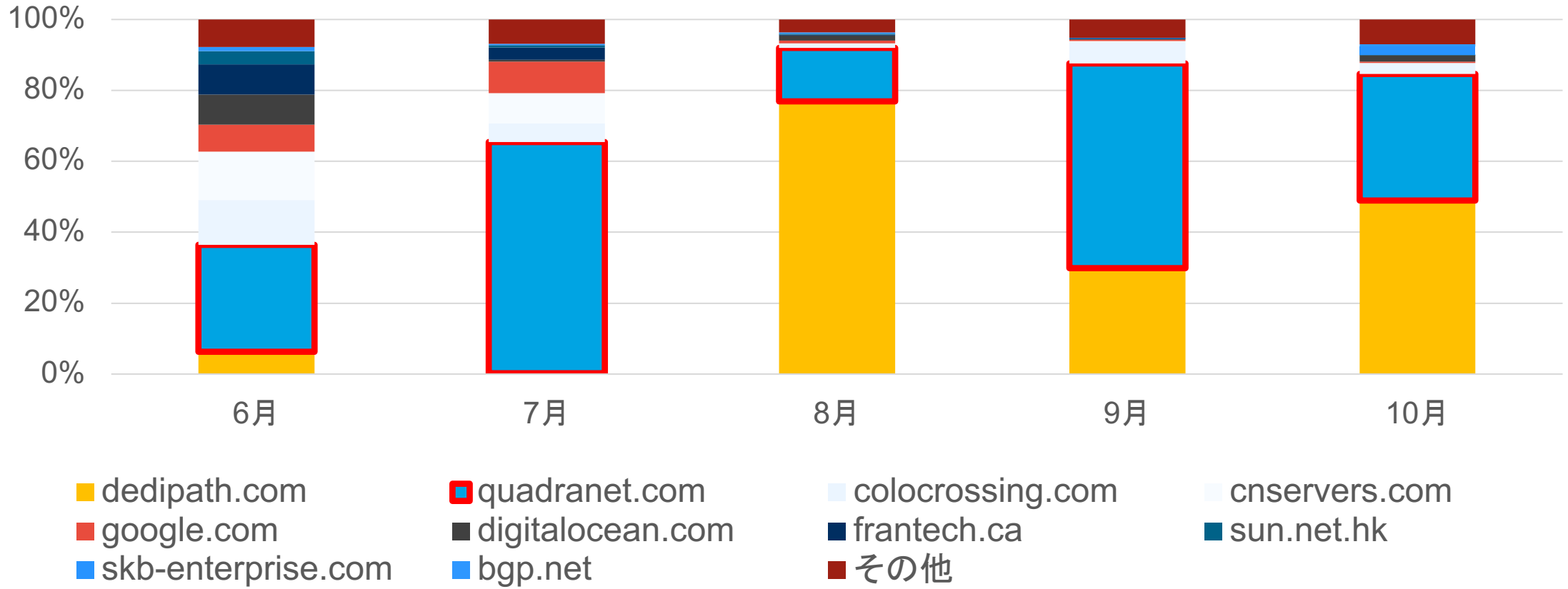
duckdns日付毎の推移

- ブランド毎で日付が被っていない
  - 同一の攻撃者が他ブランドを試している？



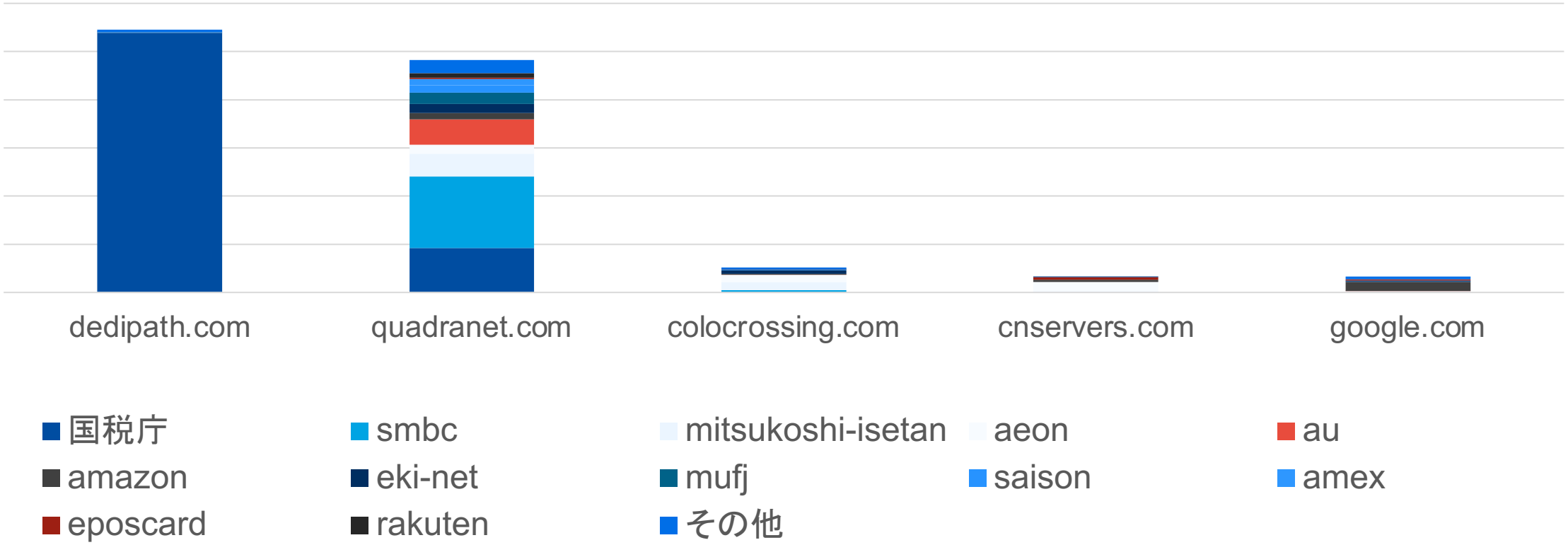
利用されているホスティング事業者

- Quadranetが多い
- 8月からdedipathが大量に使われるように



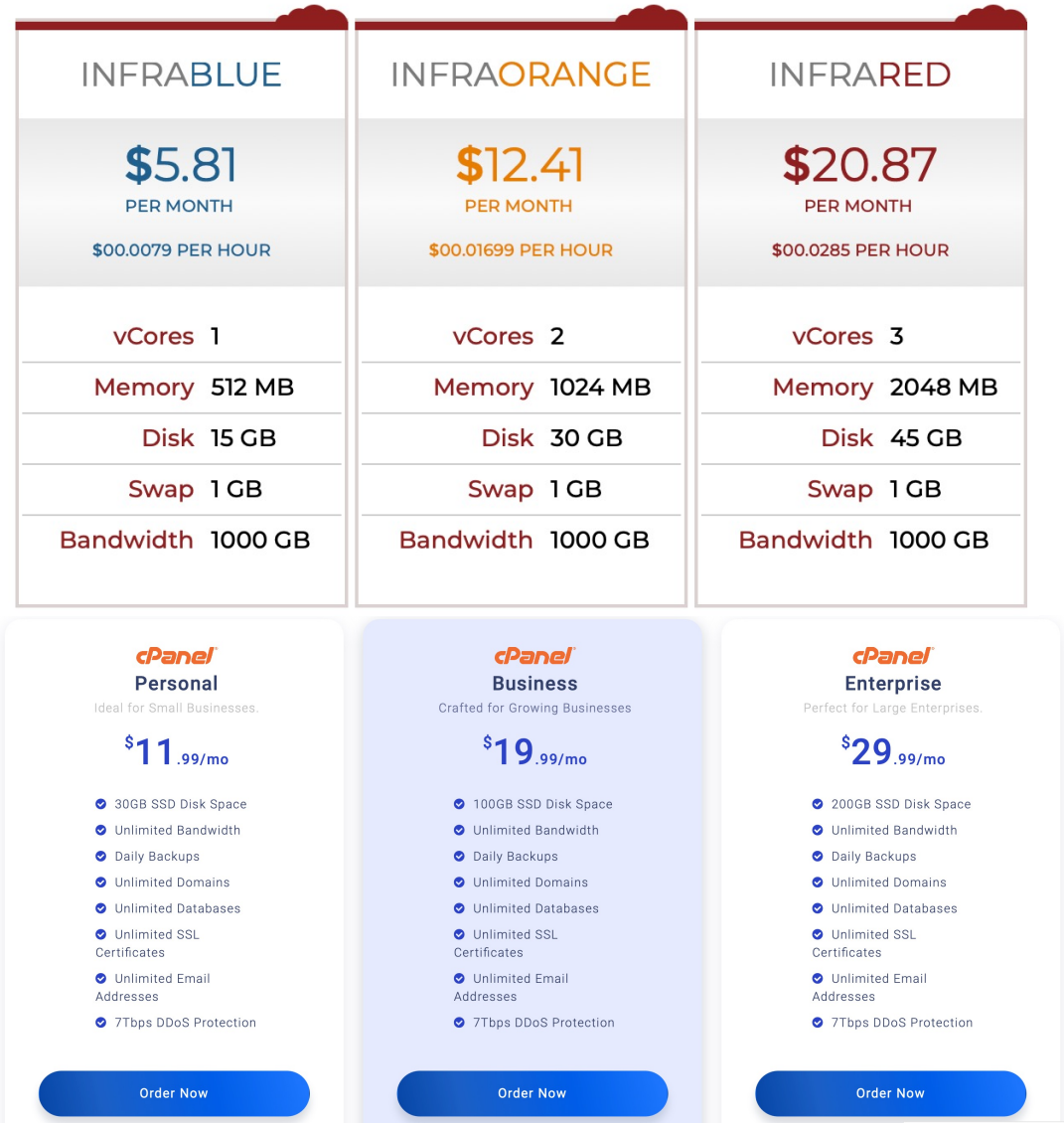
利用ホスティング事業者と攻撃ブランドの関係

- 上位5件のホスティング事業者を調査
  - 海外のホスティング事業者が利用されている
  - 8月から増えたdedipathは国税庁で利用されている



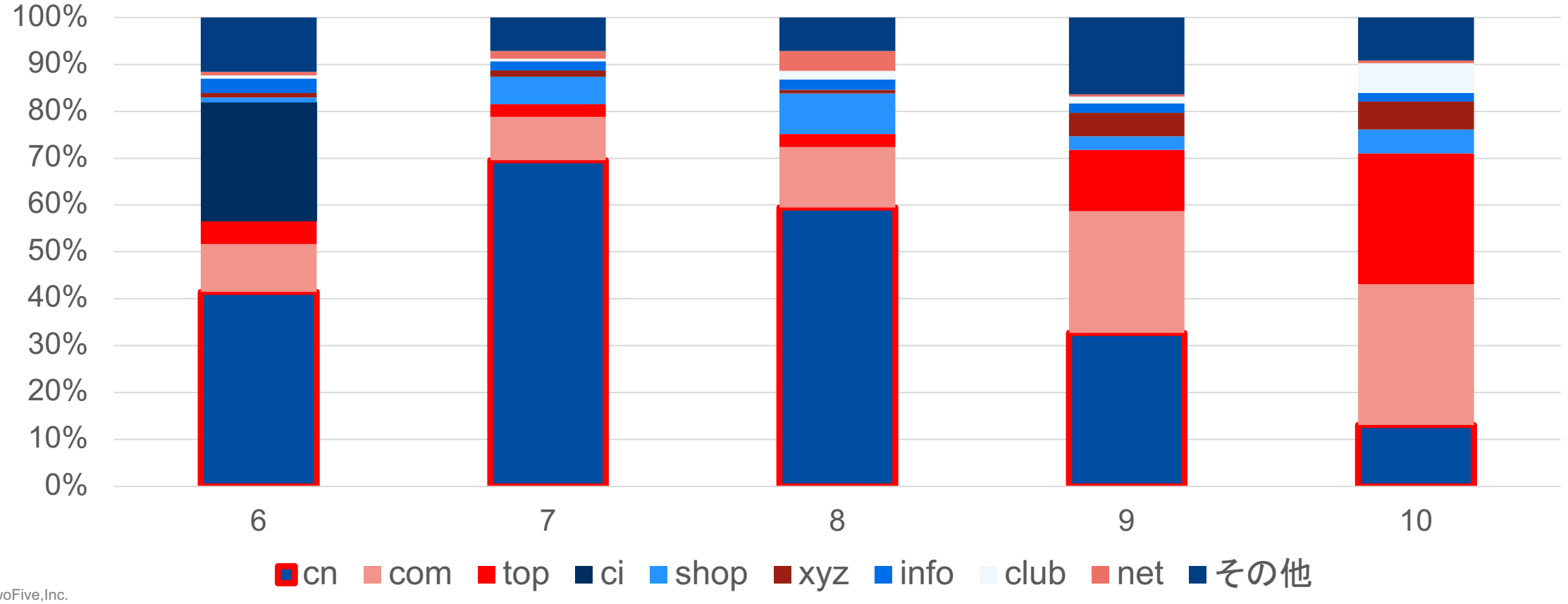
DedipathとQuadranet

- 価格
  - 両方とも安価
  - 若干Quadranetの方が安そう
- ロケーション
  - Dedipath => アメリカ
  - Quadranet => アメリカ、オランダ
- 支払い方法
  - Dedipath => PayPal ,Credit Card , Alipay ,Cryptocurrency , WebPay, Boleto , Rapi Pago , Pago Fácil , PIX , Banco do Brasil , Itaú , Efecty , PSE , OXXO , BCP Peru , Interbank Peru , Red Pagos
  - Quadranet => Credit Card, PayPal, 電信送金



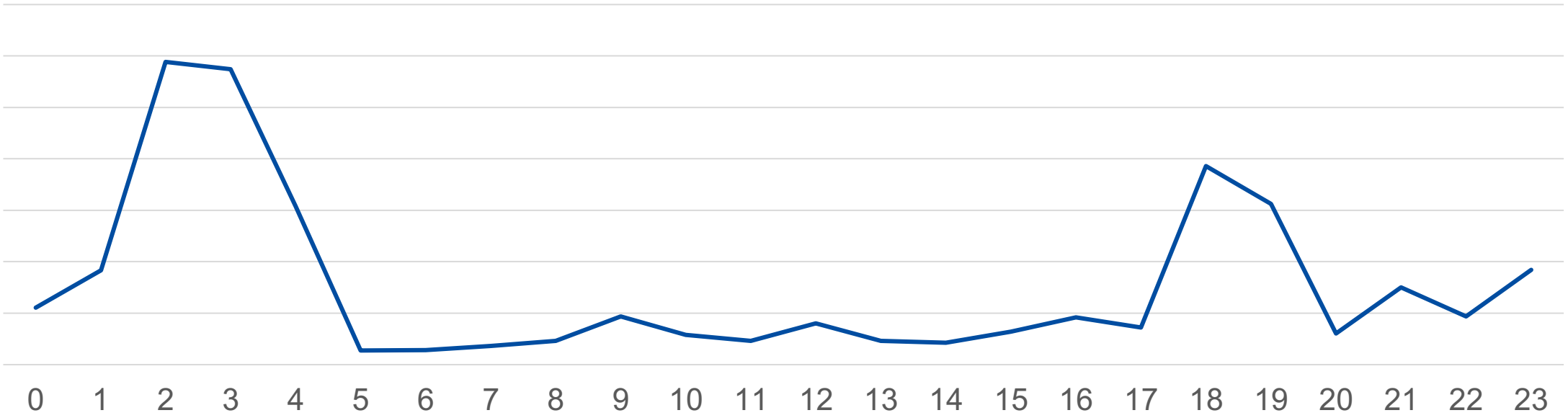
TLD情報

- duckdnsは除く
- ccTLD
  - ci,cn共に減少。グラフには表示されていないがcf, gq,cc等も減少傾向にある
- topとcomが9月から増加傾向にある



CTサーバでの時間帯毎フィッシングサイト検知数

- 深夜帯と18～19時に作られているものが多い
- 傾向的には深夜にサイトを作成して、次の日の日中に配布しているものが多くみられる



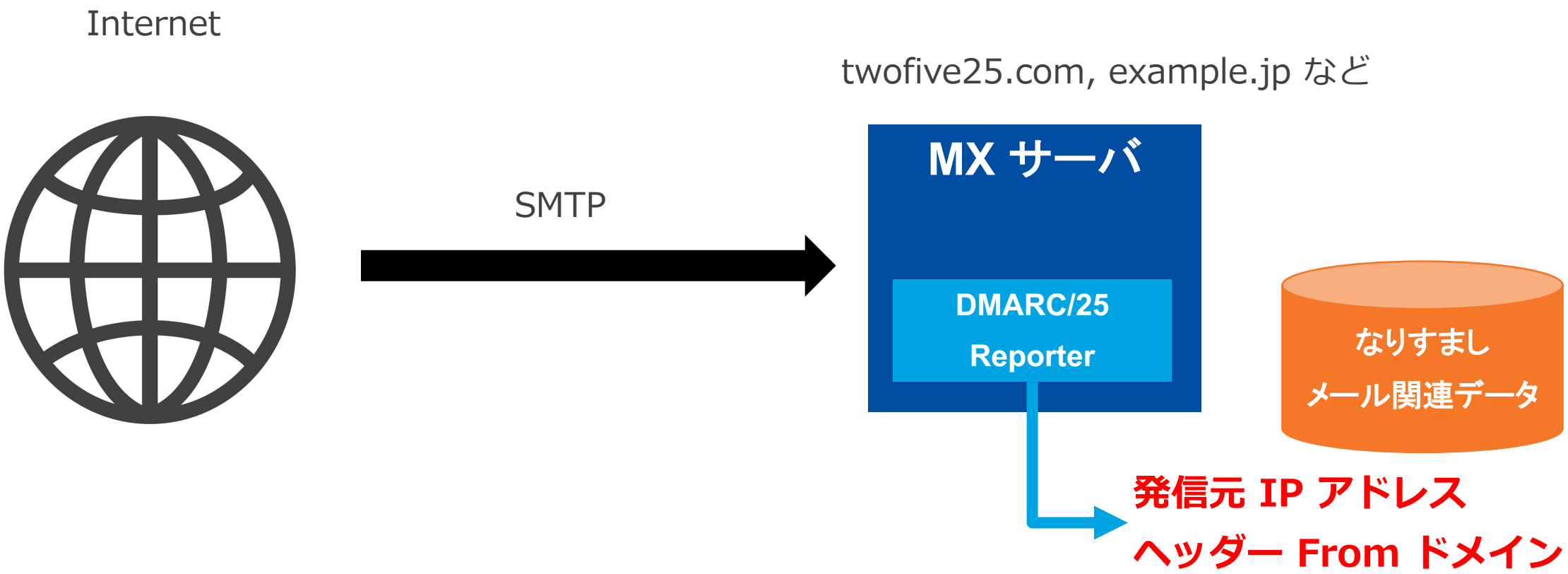
フィッシングメールとフィッシングサイトの関連性

今回の仮説とアプローチ

- 攻撃者は **IP** を使い回しているのではないか
  - DMARC pass したメール発信元とフィッシングサイト IP を突合
  - DMARC fail したメール発信元とフィッシングサイト IP を突合
- 攻撃者は **ドメイン名** を使い回しているのではないか
  - メールドメイン名とフィッシングサイトドメインを突合

調査するデータソース（その1）

- MX サーバに着信したメールの発信元 IP アドレスを調査
  - 2022年10月18日～27日（10日間）
- DMARC/25 Reporter 対応ドメインのみ限定



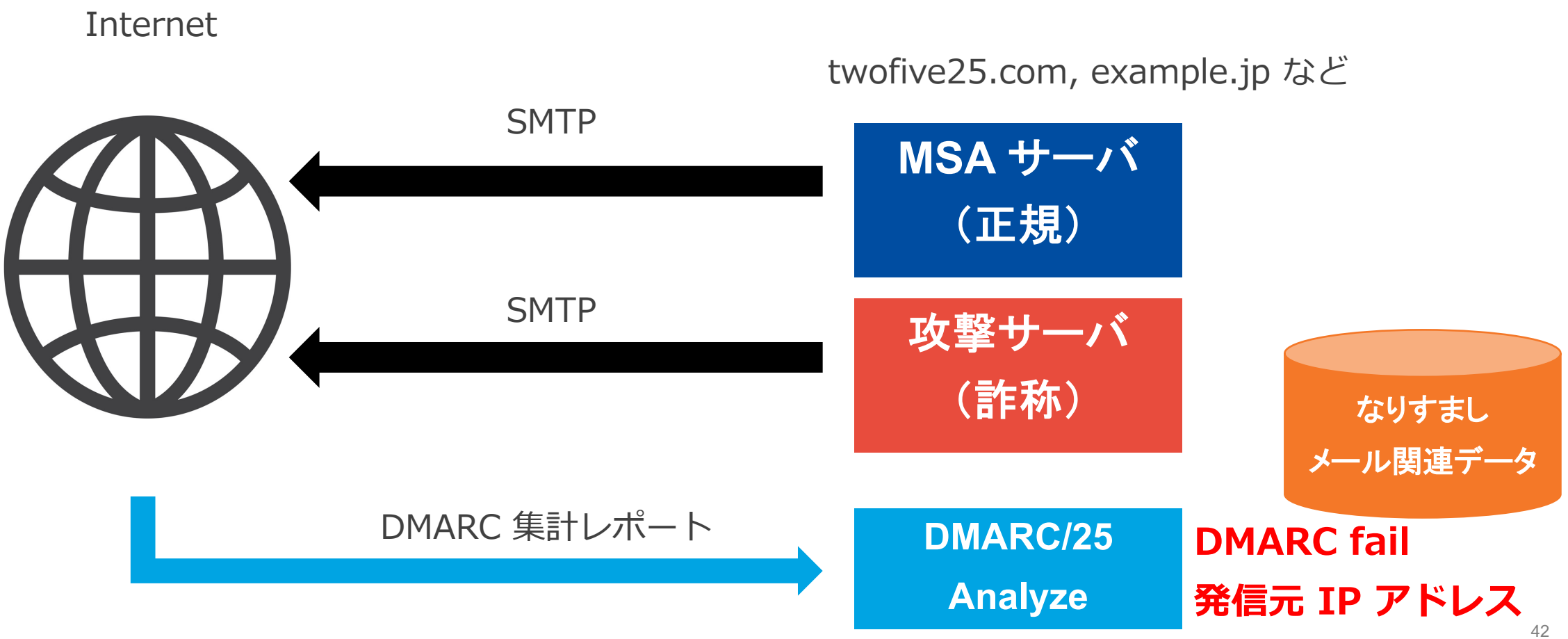
調査するデータソース（その1）

- MX サーバに着信したメールの発信元 IP アドレス・ドメインを調査
  - 2022年10月18日～27日（10日間）
- DMARC/25 Reporter 対応ドメインのみ限定

取得日	発信元 IP 数	ヘッダー From ドメイン数
2022/10/18	73,118	32,665
2022/10/19	70,074	33,163
2022/10/20	71,744	32,940
2022/10/21	73,044	32,597
2022/10/22	59,391	24,497
2022/10/23	52,963	21,131
2022/10/24	72,505	28,872
2022/10/25	78,272	31,842
2022/10/26	72,148	32,862
2022/10/27	70,056	34,215

調査するデータソース（その2）

- DMARC レポートに記載された DMARC fail な IP アドレスを調査
  - 2022年10月18日～27日（10日間）
- DMARC/25 Analyze 対応ドメインのみ限定



調査するデータソース（その2）

- DMARC レポートに記載された DMARC fail な IP アドレスを調査
  - 2022年10月18日～27日（10日間）
- DMARC/25 Analyze 対応ドメインのみ限定

取得日	DMARC fail な IP 数
2022/10/18	38,274
2022/10/19	37,044
2022/10/20	32,243
2022/10/21	25,874
2022/10/22	20,423
2022/10/23	28,279
2022/10/24	40,100
2022/10/25	36,277
2022/10/26	28,480
2022/10/27	25,005

IP アドレスの使い回し（堂々と名乗っている）

- 攻撃者は **IP** を使い回しているのではないか
  - DMARC pass したメール発信元とフィッシングサイト IP を突合
  - DMARC fail したメール発信元とフィッシングサイト IP を突合

データソース(その1)

IP アドレス(redacted)	ドメイン・URL・タイトル(redacted)	特徴
135.181.XX.XX	XXカード会員向けサービス「XX」ログイン	ドメイン名はホモグラフドメイン
176.97.XX.XX	Amazonサインイン	ドメイン名はランダムドメイン

IP アドレスの使い回し（なりすましている）

- 攻撃者は **IP** を使い回しているのではないか
  - DMARC pass したメール発信元とフィッシングサイト IP を突合
  - DMARC fail したメール発信元とフィッシングサイト IP を突合

データソース(その2)

IP アドレス(redacted)	ドメイン・URL・タイトル(redacted)	特徴
175.28.XX.XX	「XX」のWEB申込案内	TLD は .xyz
175.28.XX.XX	「XX」のWEB申込案内	TLD は .xyz

ドメイン名の使い回し

- 攻撃者は **ドメイン名** を使い回しているのではないか
  - メールドメインとフィッシングサイトドメインを突合

IP アドレス(redacted)	ドメイン・URL・タイトル(redacted)	特徴
154.209.XX.XX	XXパーソナルID | ケーブルテレビ（CATV）のXX	ドメイン名はホモグラフドメイン
34.84.XX.XX	Amazonサインイン	ドメイン名はランダムドメイン

今回の仮説とその評価

- 攻撃者は **IP** を使い回しているのではないか
  - DMARC pass したメール発信元とフィッシングサイト IP を突合
  - DMARC fail したメール発信元とフィッシングサイト IP を突合
- 攻撃者は **ドメイン名** を使い回しているのではないか
  - メールドメイン名とフィッシングサイトドメインを突合

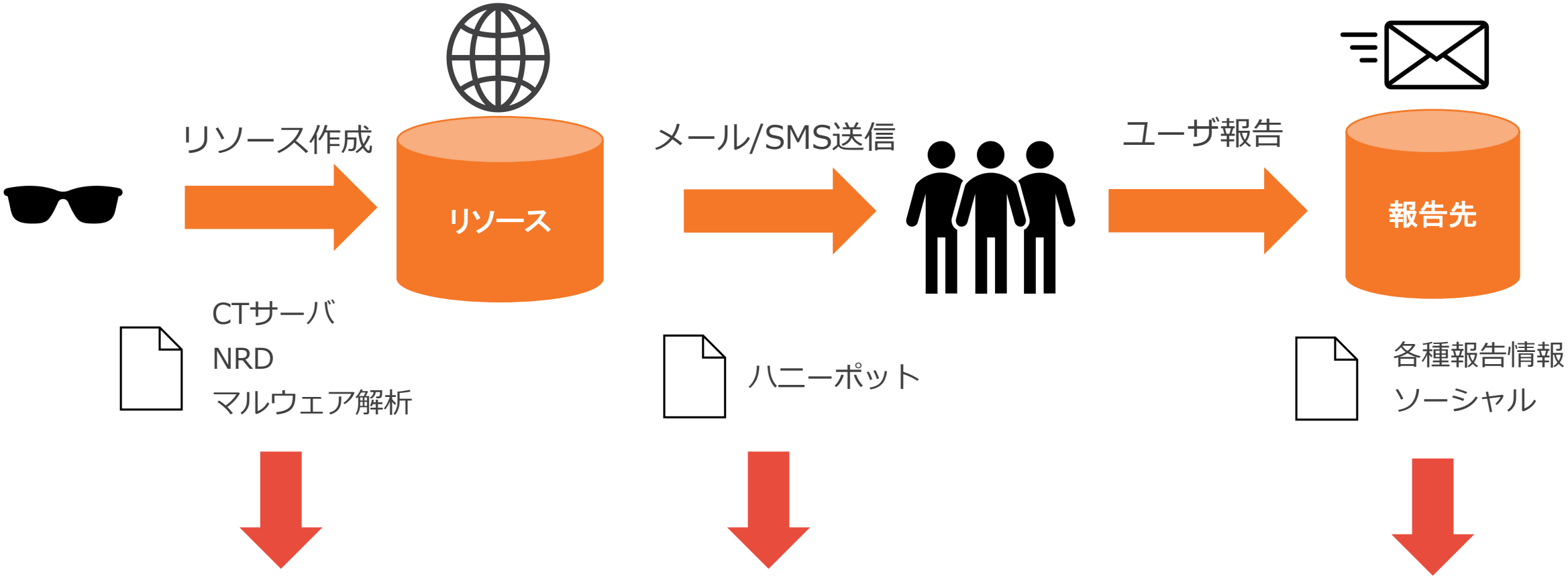
攻撃メール / フィッシングサイトの IP は別物の場合が多い

ドメイン名（ホモグラフ・ランダム・スクワッティング）は流用？

まとめ・今後の対策を考える

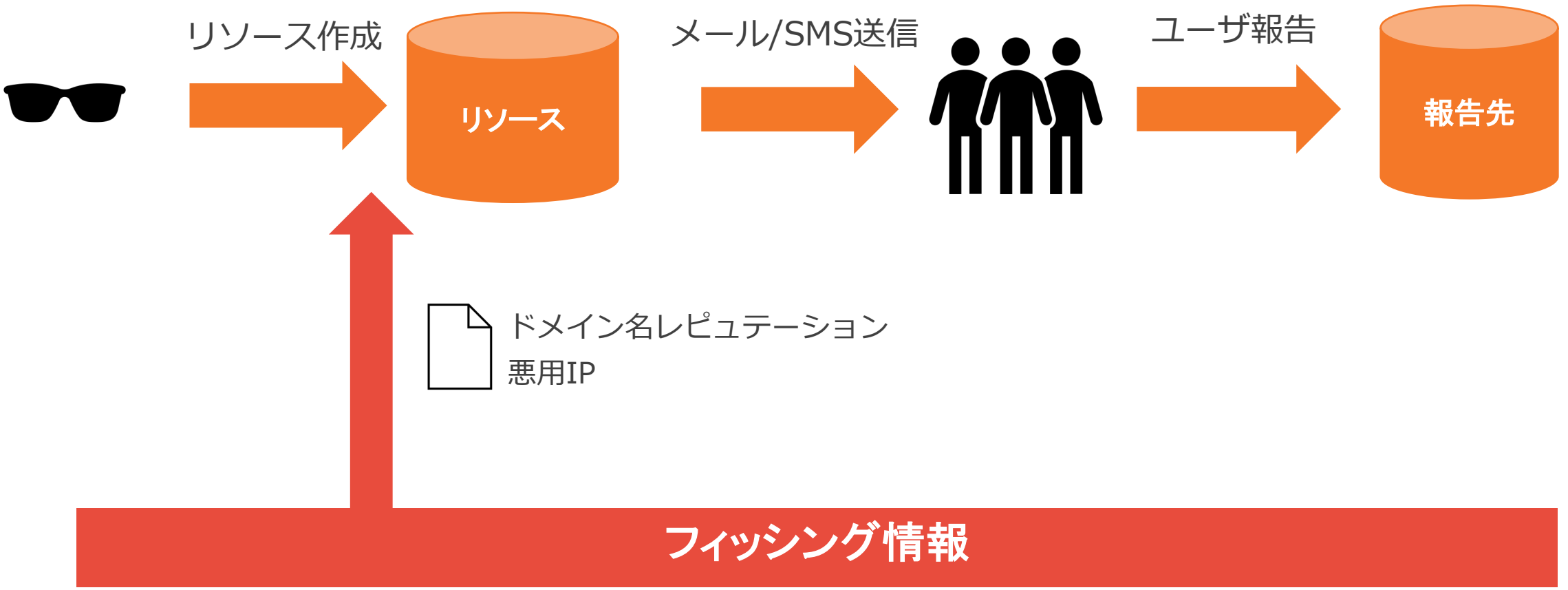
今後も重要なのはさまざまなデータ

- OSINT だけでなくエンドユーザ報告情報も



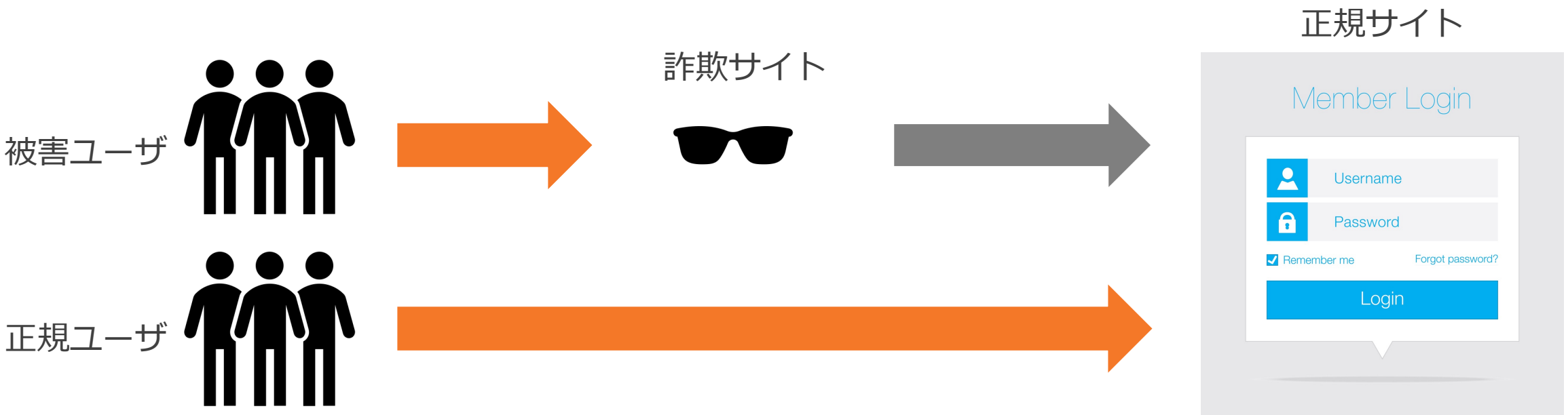
攻撃者のアクションに合わせた対策

- ドメイン取得時やユーザアクセス環境でのレピュテーション
  - レジストラでのドメイン（Cert）取得時
  - 中間者攻撃への対応



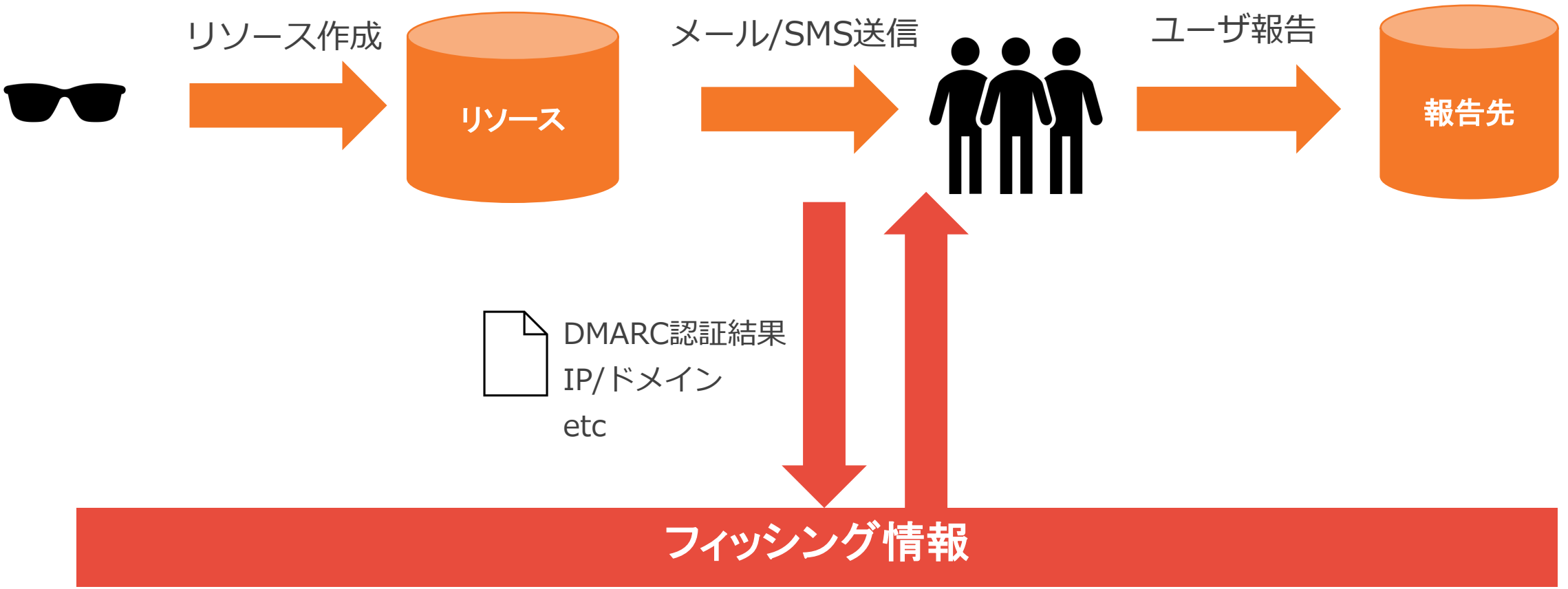
c.f. 事業者向けデータフィード

- データフィードの活用
  - サインインシステムでの IP アドレスブロッキング
  - ドメイン取得時の IP アドレスブロッキング
  - etc



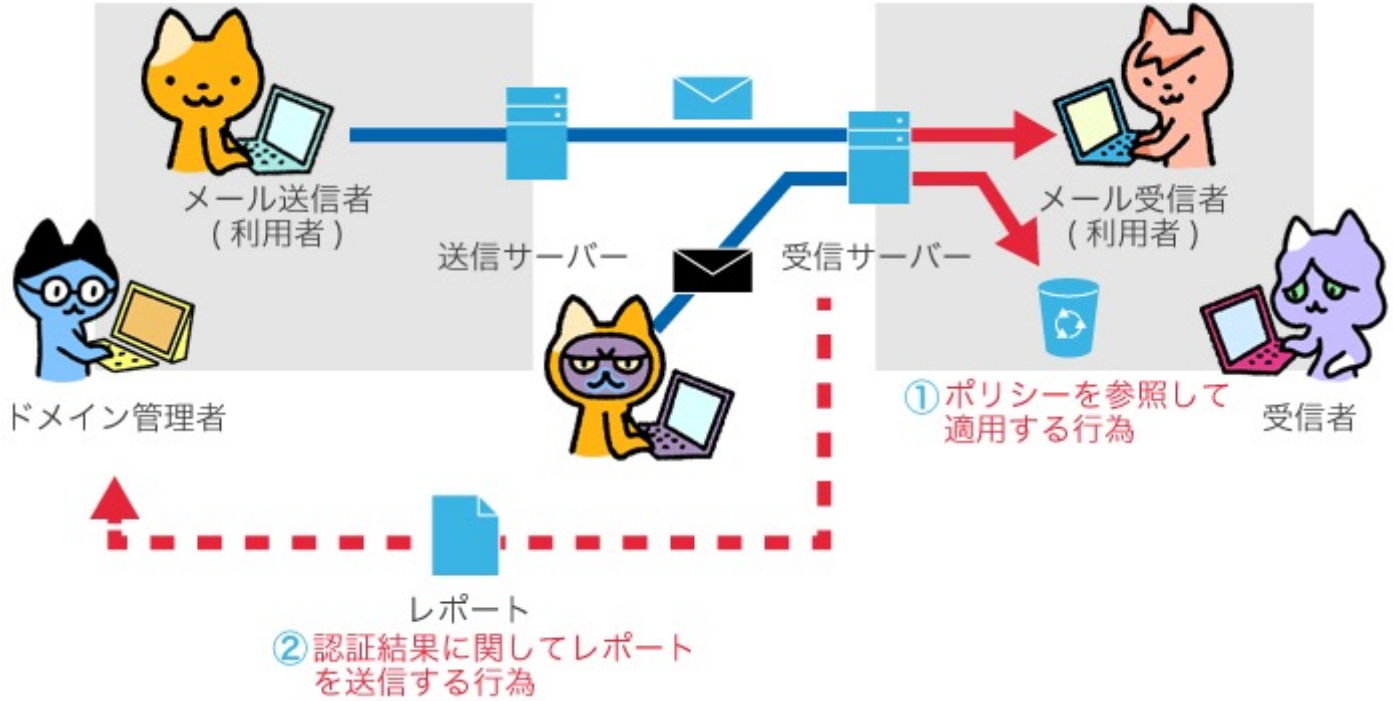
攻撃者のアクションに合わせた対策

- フィルタリング & レポーティング（サーバ側）
  - ドメイン認証（なりすまし対策）
  - ドメインレピュテーション（NRD / ZRD のペナルティ）



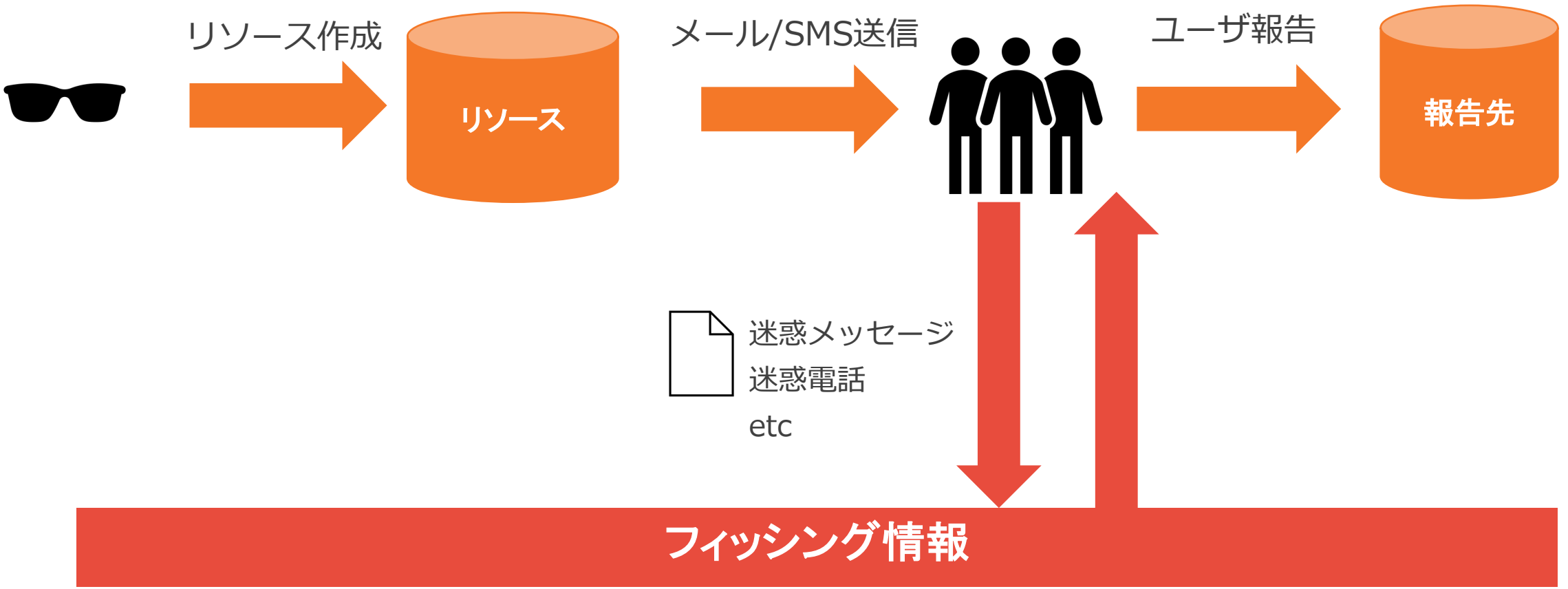
c.f. サーバサイドフィルタリング（DMARC/25）

- フィルタリング機能
  - DMARC 結果に応じた隔離・拒否
  - BIMI ドメインの評価
  - ドメインレピュテーション
- レポーティング機能
  - 集計レポート
  - 失敗レポート（※）
  - 迷惑メール通報データ（※）



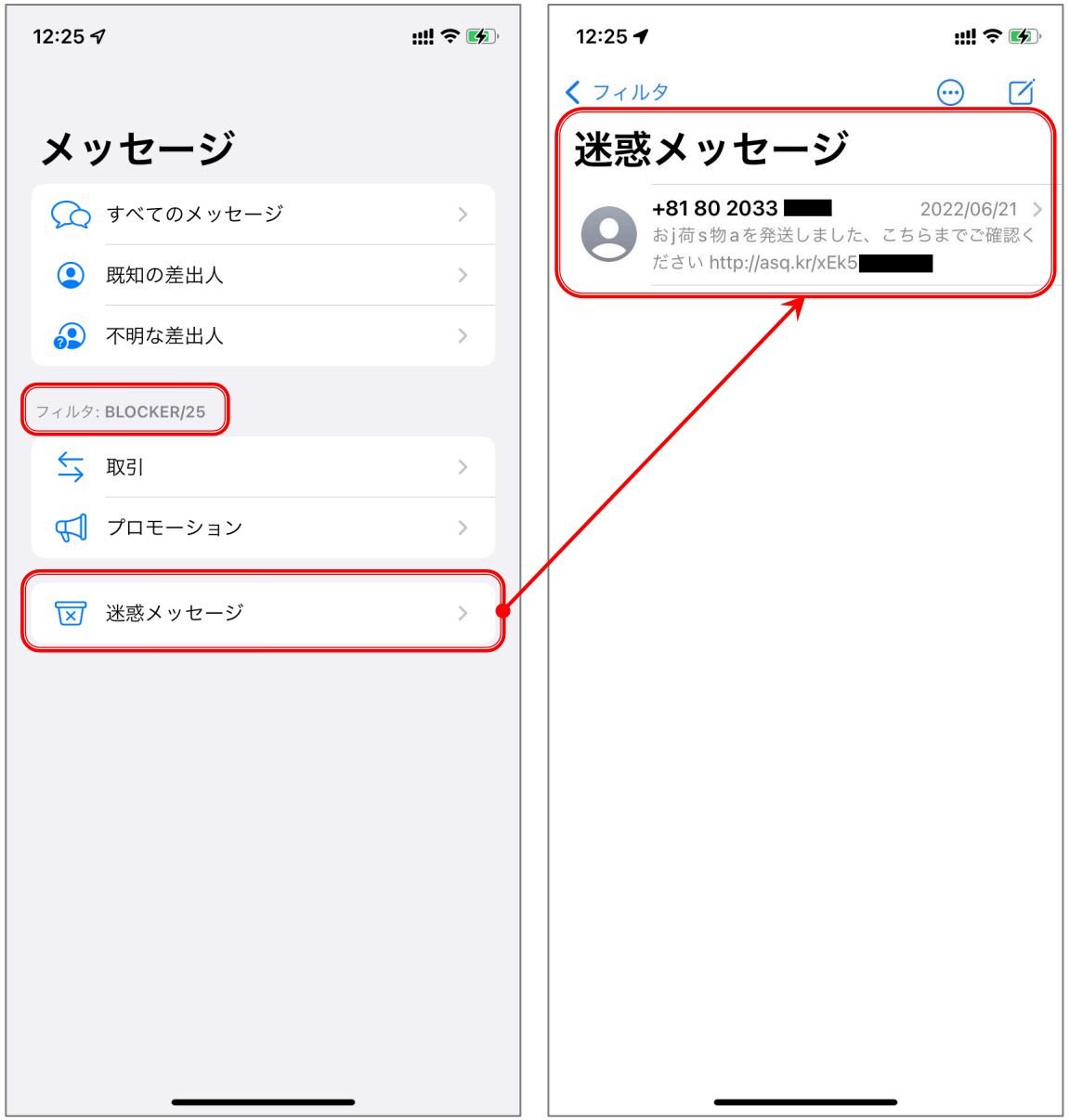
攻撃者のアクションに合わせた対策

- フィルタリング & レポーティング（アプリ側）
  - 迷惑メッセージの拒否
  - エンドユーザーからの報告/通報データの利活用



c.f. SMSフィルタリング（BLOCKER/25）

- フィルタリング機能
  - 未登録番号 / 未返信の SMS　ブロック
  - 通報データベースの活用
- レポーティング機能
  - 迷惑メッセージの通報
  - 救済リスト



質疑応答
ご質問ありませんか

Thanks