資料12－2

総務省「不適正利用対策に関するワーキンググループ」 第12回目会合

「敵」を知る
生成AIにより崩壊した言語壁と日本を狙う詐欺メールの急増

2025年11月

日本プルーフポイント チーフエバンジェリスト
警察大学校講師

そうた　ゆきみ
増田 幸美

年末から相次ぐ日本への異様なDDoS攻撃

公表された国内DDoS被害 (国内46以上の企業/団体が標的に)	
2024/12/26	日本航空
2024/12/26	三菱UFJ銀行
2024/12/30	PayPay銀行
2024/12/30 2025/1/7	りそなホールディングス傘下4行
2024/12/31	みずほ銀行
2025/1/2	NTTドコモ
2025/1/5-15	日本気象協会
2025/1/6	三井住友カード

- **攻撃ボリュームは過去最大規模**
- レイヤ3/4 (Syn/Ack/UDP/GRE Fllod) と
  レイヤ7 (HTTP/HTTPS) の**DDoSが時間によって切り替わる**
- 経路にCDNがないIPアドレス直打ちで**オリジンサーバーを直接攻撃**
- **攻撃元は世界中に分散**（英国、香港、日本、シンガポールなど）
  （参考：アカマイテクノロジーズ社）
- レイヤ3/4については**Miraiボットネット活用**の疑い
  (参考：トレンドマイクロ社)

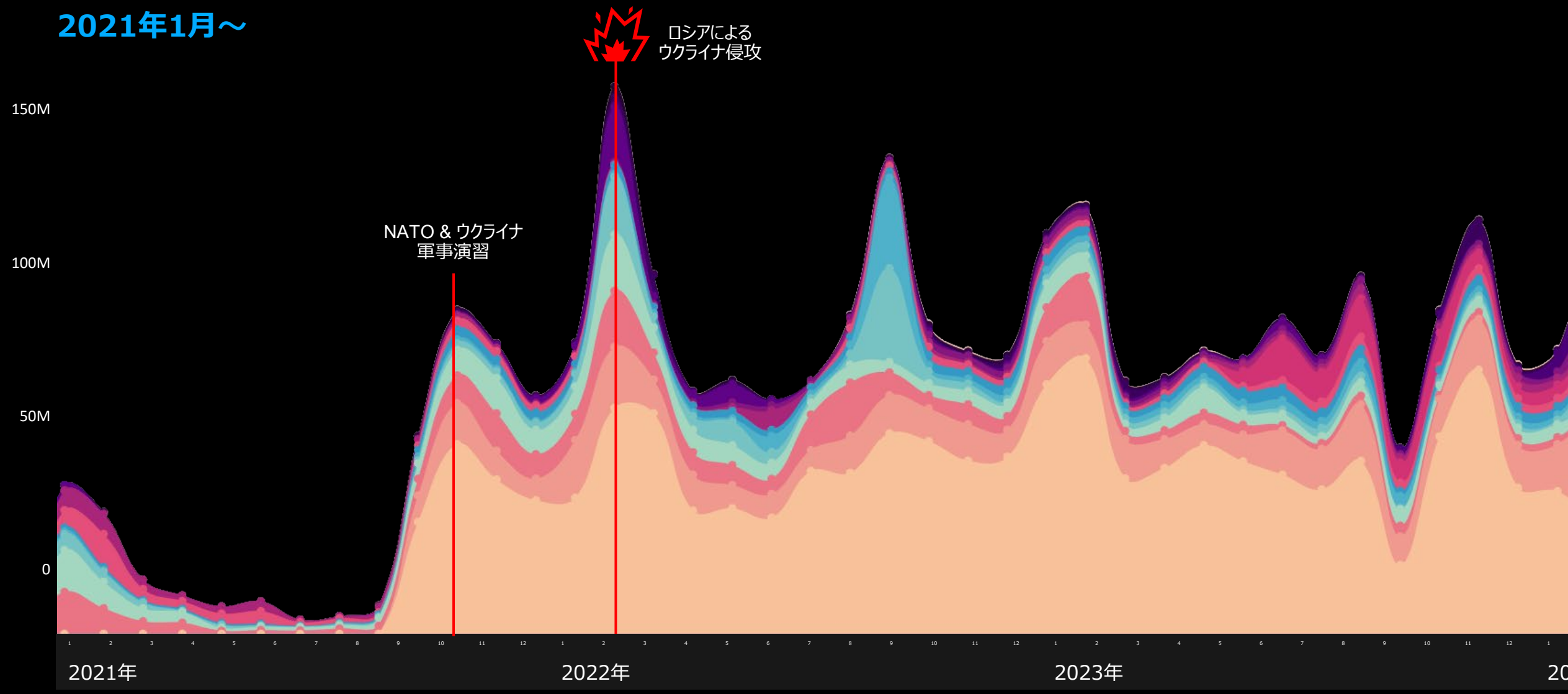
通常のリフレクションDDoSと比較すると
コストをかけた柔軟性の高い洗練されたDDoS攻撃
しかも犯行声明がない

日本へのスキャンも急増

© 2025 Yukimi Sohta. All rights reserved

全世界の新種メール脅威動向

2021年1月～



proofpoint.

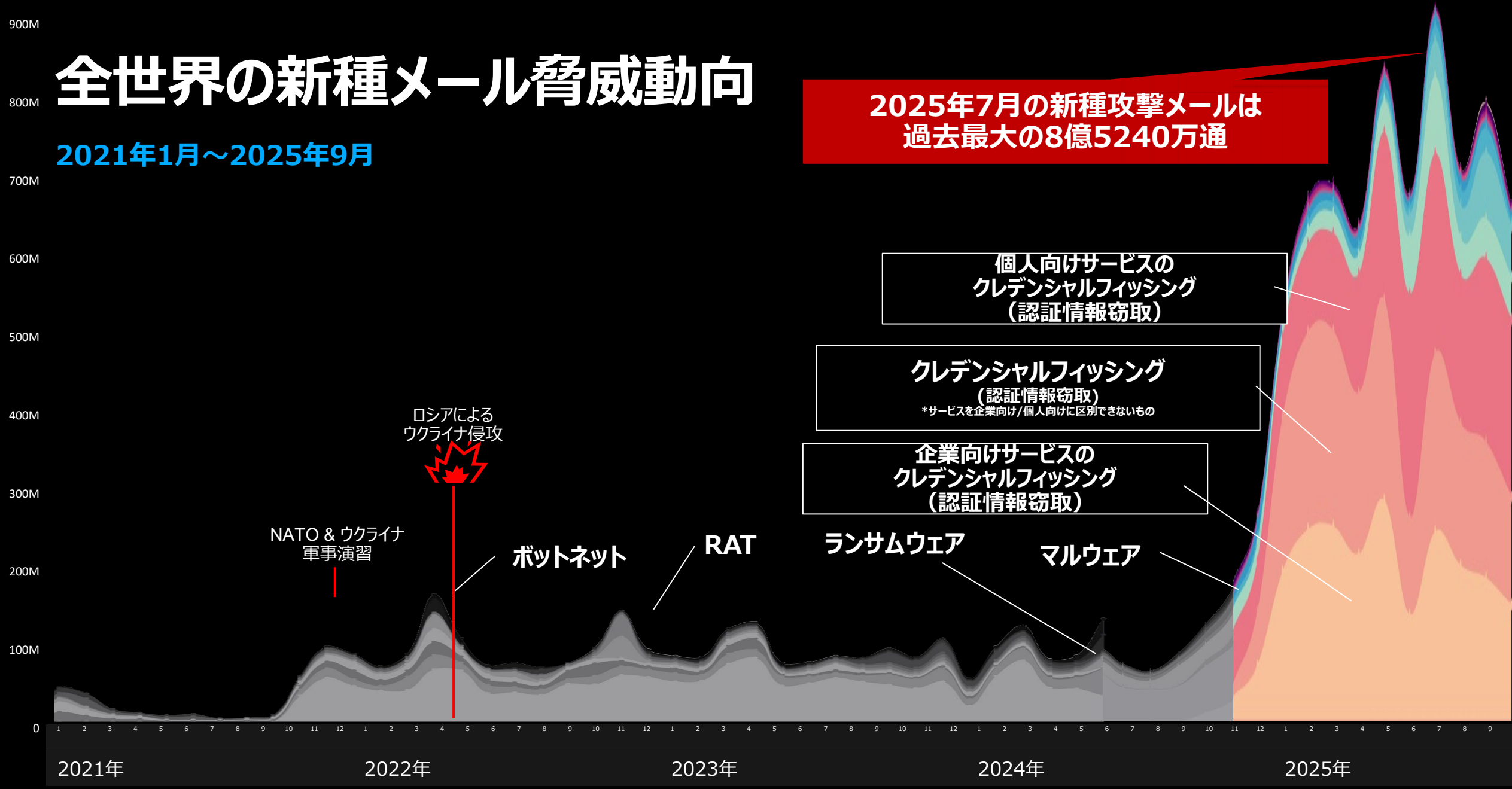
出典：プルーフポイント

© 2025 Proofpoint. All rights reserved

全世界の新種メール脅威動向

2021年1月～2025年9月

2025年7月の新種攻撃メールは過去最大の8億5240万通



proofpoint.

出典：プルーフポイント

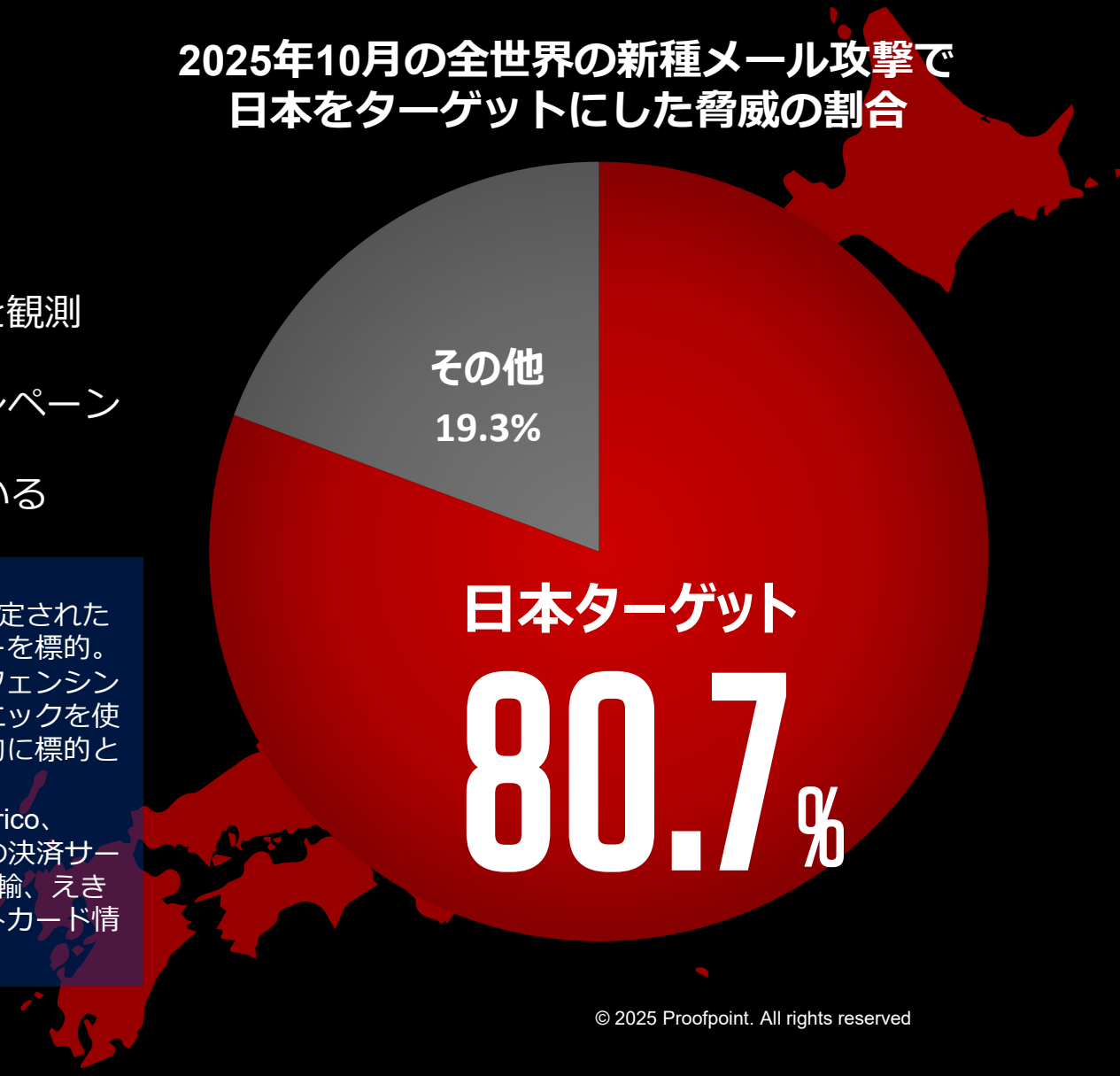
© 2025 Proofpoint. All rights reserved

2025年10月：
全世界のメール攻撃のうち80%が日本をターゲットに

- グローバルで**合計712の新種のメール攻撃キャンペーン**を観測
- うち136の攻撃キャンペーンが日本をターゲット
  ボリューム数TOP10のうち8つが日本を標的にしたキャンペーン
- CoGUIフィッシングキットを用いた攻撃が急増
- 多要素認証をすり抜けるAiTMであるEvilginxも使われている

CoGUIフィッシングキットとは：
CoGUI “フィッシング・キットは、プルーフポイントのリサーチャーによって特定された高度な検知回避機能を持つフィッシング・フレームワーク。主に日本のユーザーを標的。他に少数だがオーストラリア、ニュージーランド、カナダ、米国を標的。ジオフェンシング、ヘッダーフェンシング、フィンガープリンティングなどの高度な回避テクニックを使用することにより、セキュリティ対策を回避しながら特定の地理的地域を選択的に標的とすることが可能。標的とされた国のユーザーにとって重大な脅威となっている。
Amazon, 楽天、Apple、ヨドバシなどのショッピングサイト、イオンカード、Orico、VISA、 TS Cubic、セゾンカード、Orico、EPOSカード、Paypay、SMBCなどの決済サービス、SBI証券、大和証券松井証券などの証券会社ほか、NTTドコモ、ヤマト運輸、えきネットなどのサービスになりすまし、ログイン認証権限、個人情報、クレジットカード情報などを窃取する

2025年10月の全世界の新種メール攻撃で日本をターゲットにした脅威の割合



proofpoint.

© 2025 Proofpoint. All rights reserved

CoGUIターゲットのプロファイリング

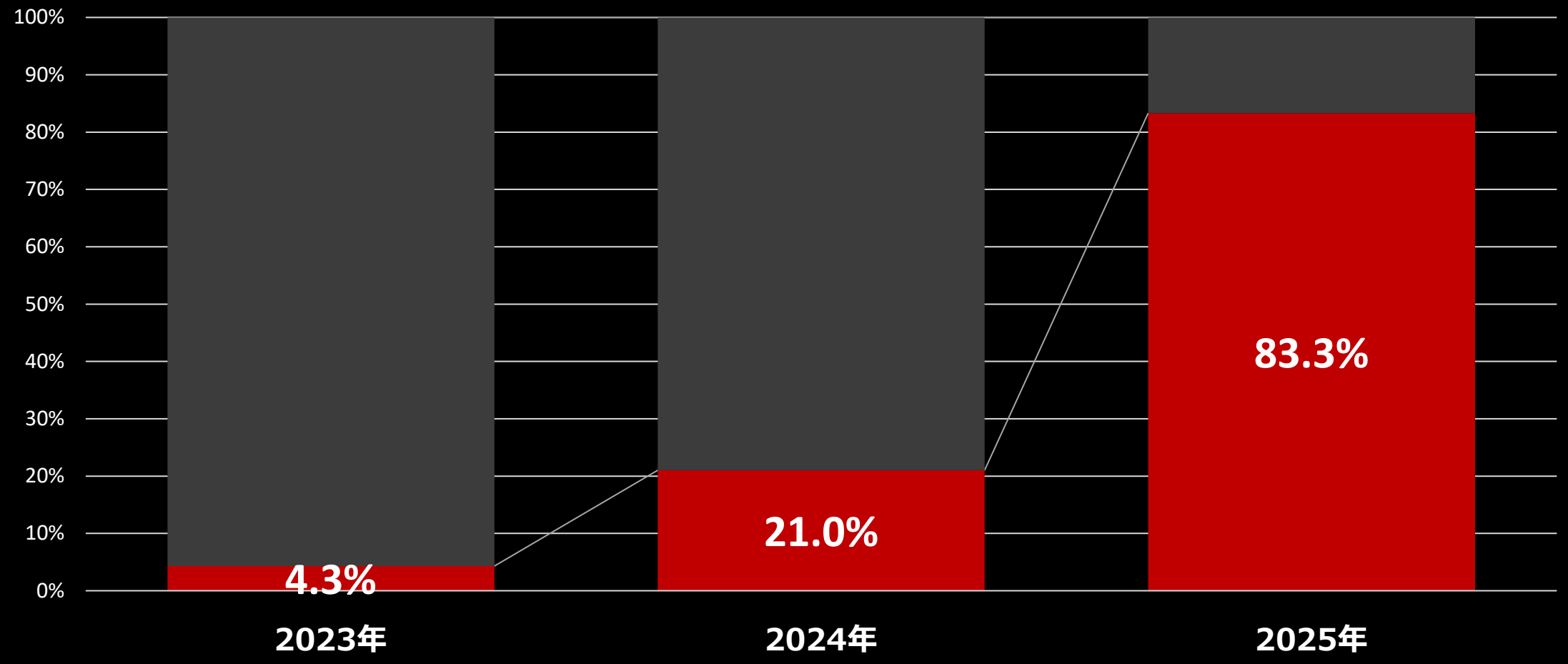
- GeoIP（IPアドレスの地理的ロケーション）
- ブラウザの言語設定
- ブラウザの種類（例：Chrome）
- ブラウザのバージョン
- モニターの高さと幅
- OSプラットフォーム（例：win32）
- ブラウザがモバイルデバイス上で実行されているかどうか

© 2025 Proofpoint. All rights reserved

日本への攻撃の割合が増加

2023年1月～2025年10月までの統計

全世界の新種メール攻撃の中で日本が標的にされている比率



出典：プルーフポイント

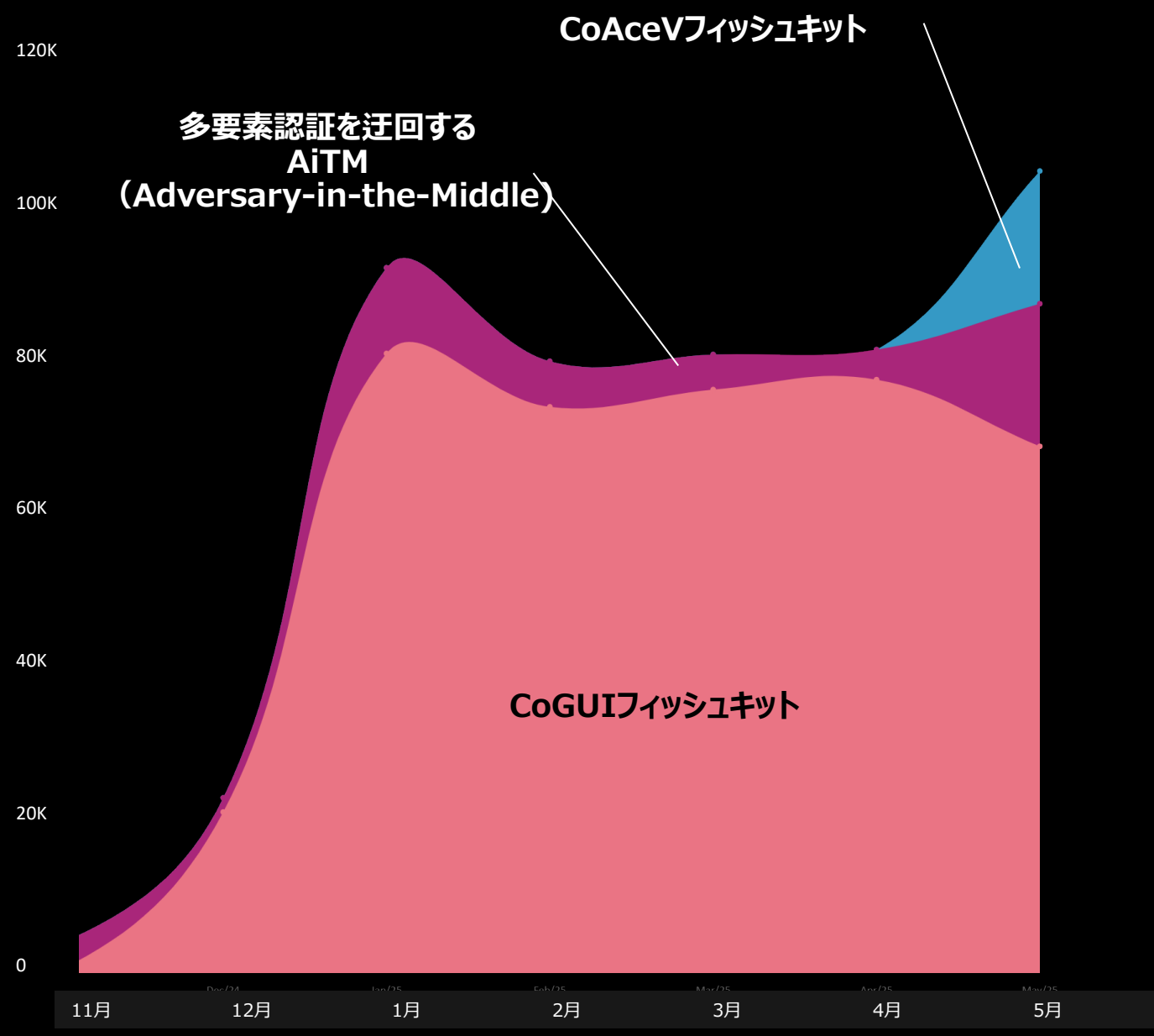
proofpoint.

© 2025 Proofpoint. All rights reserved

多要素認証導入の影響で攻撃者が戦術を変更

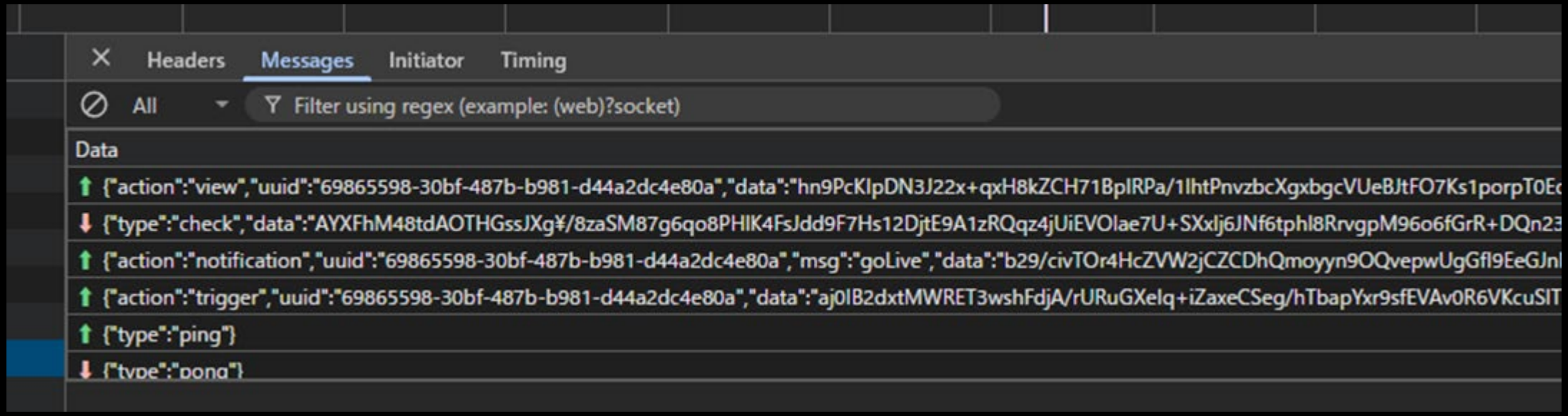
CoAceV フィッシング・キットの登場

- CoGUIでは、情報送信時にAPIエンドポイントを用いていたが、新種のCoAceVではWorksocket APIを使うように
- さらにCoAceVとも異なる新種も現れており、JSコードは似通っているものの、ユーザープロファイルのために、ネットワーク通信方式が変更されている(6/4現在)



© 2025 Proofpoint. All rights reserved

Websocketで暗号データを送信する仕組みへ変更



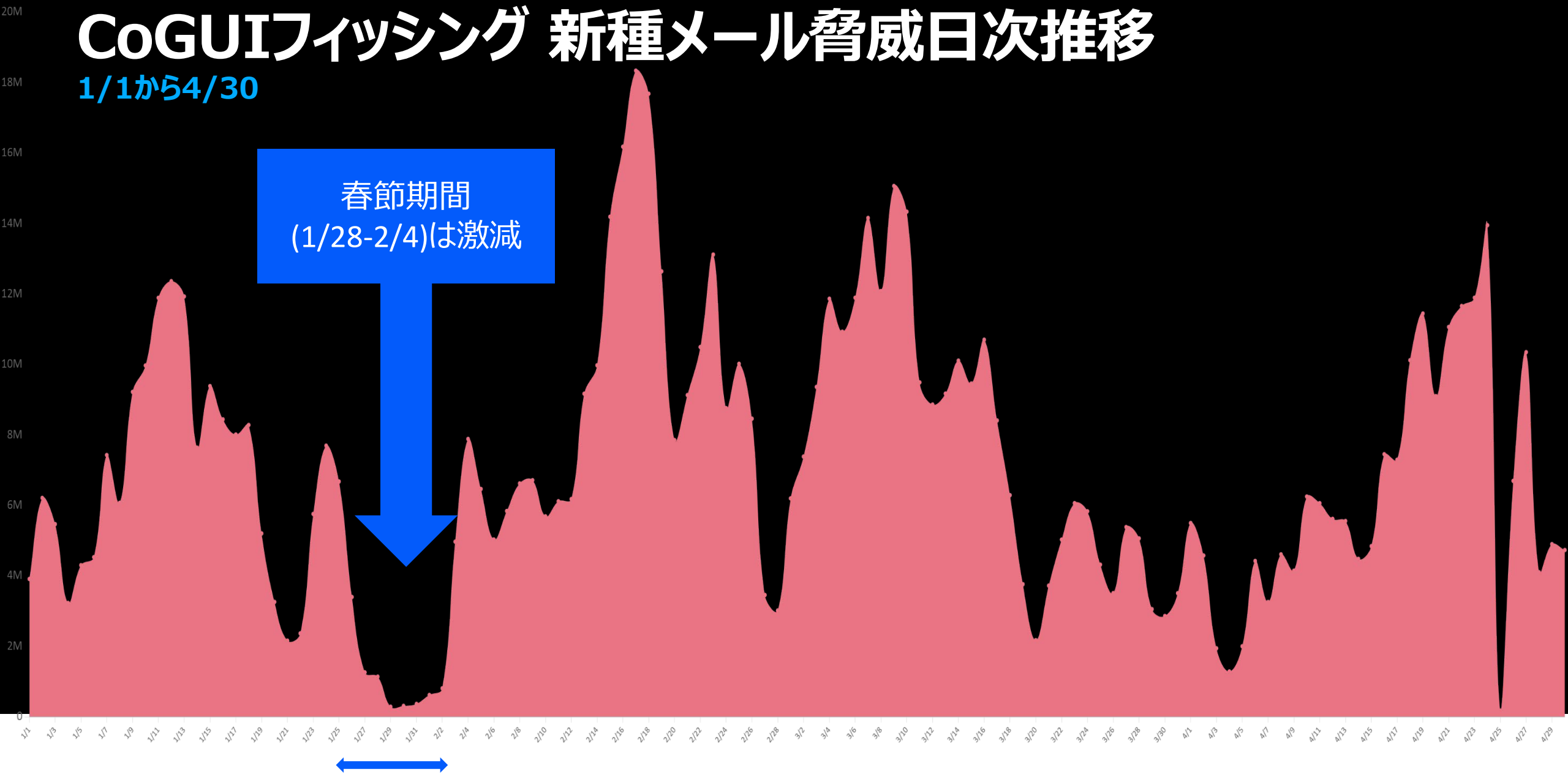
operator_admin_name	operator_admin_id	_0xb7c3l
dalaoniubi01	16	sagawaExp_jp_card
lvjian04	9	anaco_jp_card
qiangzi001	20	sagawaExp_jp_card
baoan222	3	anaco_jp_card
dahu888	2	sbisec_jp_creditcards
a	42	kuronekoyamato_jp
a3	7	tokyogas_jp_card
a2	6	tokyogas_jp_card
baoan111	2	anaco_jp_card
nuli03	7	tepco_jp_card

proofpoint.

© 2025 Proofpoint. All rights reserved

CoGUIフィッシング 新種メール脅威日次推移

1/1から4/30



proofpoint.

出典：プルーフポイント

© 2025 Proofpoint. All rights reserved

楽天証券をテーマとしたCoGUIフィッシングキャンペーン

From 楽天証券からのお知らせ <Rakuten.love-kirarin@uwwxlf.com>
To user.name@organizationname.tld
18/04/2025, 15:51
Subject 【緊急対応】関税危機へのAI投資戦略：トップアナリスト木野内栄治氏監修ツール限定公開

AI投資戦略委員会
平素より格別のご高配を賜り、厚く御礼申し上げます。
現在、世界的な関税政策の影響により市場が激しく変動しております。このたび当協会は、元ゴールドマン・サックス主席ストラテジストで20年の市場経験を持つトップアナリスト・木野内栄治氏と連携し、危機対応型「AI市場診断システム」を緊急開発いたしました。

ご利用確認はこちら

【本システムの3大特徴】
✅ 0.5秒でリスク回避戦略を生成：AIが関税敏感セクターの資金流動をリアルタイム分析
✅ 独占的危機予測モデル：過去10年の経済周期データを統合（予測精度91%）
✅ 期間限定無料開放：登録者全員に『関税戦争サバイバルガイド』（翌日の行動リスト付き）を進呈
※免責事項：本ツールの分析結果は過去のデータとアルゴリズムに基づいたものであり、将来の投資成果を保証するものではありません。投資判断はご自身の責任にてお願いいたします。

▼「楽天の証券取引約款」等の一部改定について
https://www.rakuten-sec.co.jp/web/info/info20240209-01.html
▼サイトご利用にあたってのご留意事項
https://www.rakuten-sec.co.jp/web/info/info20160426-01.html

当社では本お知らせとは別に、定期的にログイン後の画面にてお客様情報の確認をお願いすることがございます。画面の案内に従ってご確認・ご回答をお願い致します。

【1】このメールアドレスは、楽天証券（株）からの発信専用とさせていただいております。このメールの送信元のアドレス宛てに返信することはできません。
【2】銘柄の選択など、投資の最終決定はご自身の判断でなさるようにお願いいたします。
【3】このメールの内容は、お客様限りでご使用ください。メールの内容については楽天証券（株）が著作権を有し、よってそのいかなる部分も、電子的または機械的な方法を問わず、いかなる目的であれ、複製または転送などを行わないようお願いいたします。
【4】送信上の誤処理により、受信される予定でない方に配信されました場合は、送信者までお知らせいただき、受信されましたメール内容は削除していただきますようお願いいたします。
【5】メールによる残高照会などのお問い合わせ、ご伝言などを承ることはできませんので、ご了承ください。

保有銘柄・お気に入り銘柄の四半期決算・臨時基準日（臨時株主総会等）が発表されました。
四半期決算・臨時基準日（臨時株主総会等）に伴うお客様の手続きは必要ありません。
http://www.rakuten-sec.co.jp/cgi-bin/CTS/Direct_Login.cgi?homeid=ACC_CA_MAIL
本メールでお送りしているのは、本決算/中間決算以外の四半期決算や臨時基準日の情報になります。
http://www.rakuten-sec.co.jp/cgi-bin/CTS/Direct_Login.cgi?homeid=JP_PRC_SEARCH
本メールは、情報発表時、発表内容変更時、権利落日の5営業日前および1営業日前にお送りしています。
https://www.rakuten-bank.co.jp/rd/fes/mail/ad/register/001.html
■保有銘柄一覧
保有銘柄は、以下の画面にてご確認いただけます。
<PCウェブ>

"codeName":"日本rakuten乐天证券"

© 2025 Proofpoint. All rights reserved

今、日本が狙われる理由

AIによって変わる攻撃先

1. **AIにより言語の壁が消失**したことにより、日本への攻撃が可能に

2. 防御が薄くなった日本企業の**知的財産**は価値が高く、
   日本人の**個人情報はアンダーグラウンドで高値**で売れる

3. 不気味なDDoSのタイミングと合わせると、
   外国政府主導による**軍事的/戦略的**な攻撃である可能性：

   - 中国による台湾有事を見据えての準備攻撃、ロシアへの経済制裁に対する報復・・・
   - 外国政府インシデント対応プロセス、ネットワーク機器やサーバーの冗長構成などの技術詳細、システム切り替えのタイミングの把握する準備活動である可能性

DDoSは単なる陽動作戦であり、DDoSで注意をそらしている間に、
本丸の攻撃（ランサムウェア、内部への侵入）を展開している可能性

proofpoint.

© 2025 Yukimi Sohta. All rights reserved

メールはただの
やりとりのツールではない

今やSSO(シングル・サイン・オン)
のIDとして
あらゆるシステムの入口に

proofpoint.

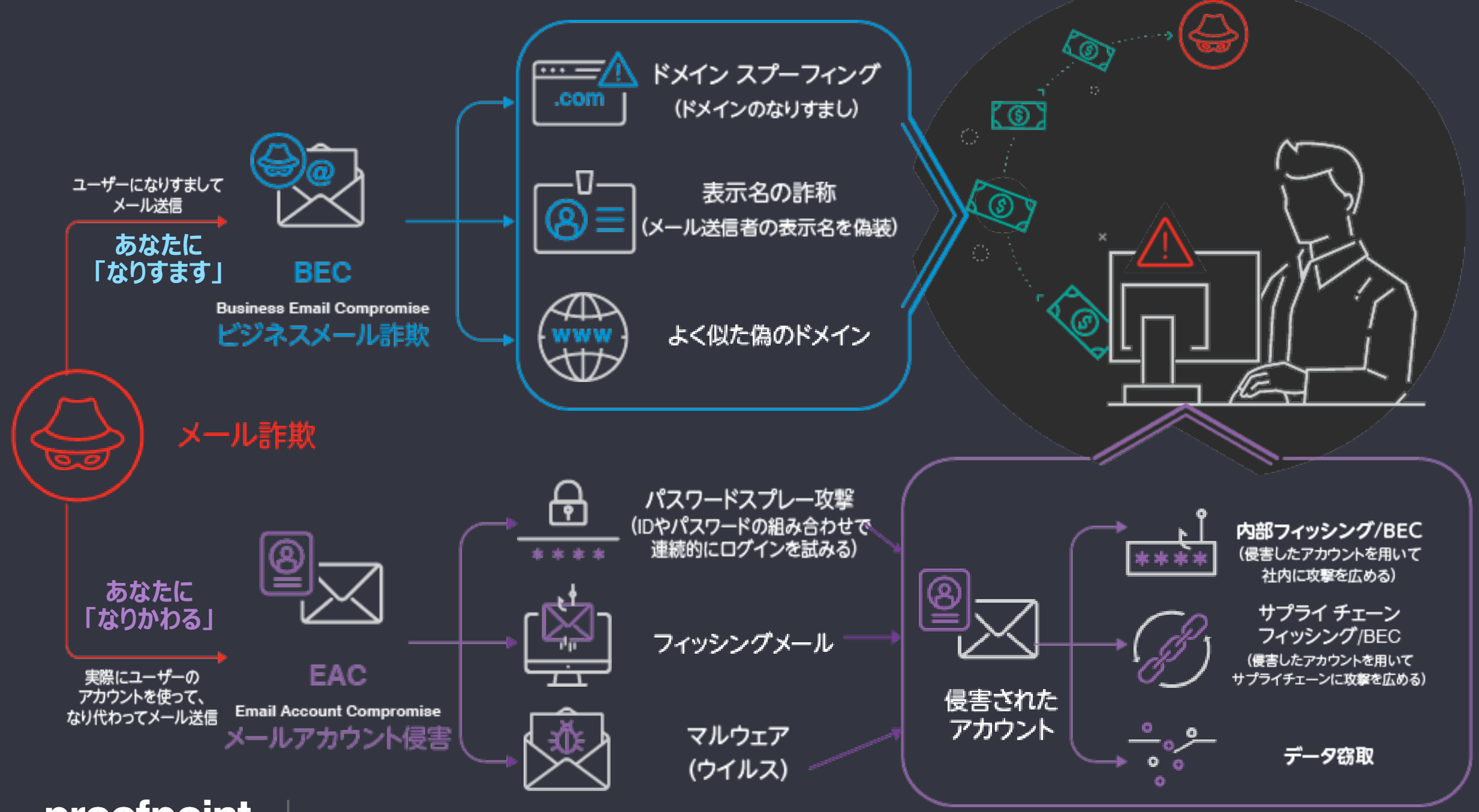
© 2024 Proofpoint. All rights reserved

メール詐欺を解剖する

メール詐欺の仕組みと、その対策

proofpoint

© 2024 Proofpoint. All rights reserved

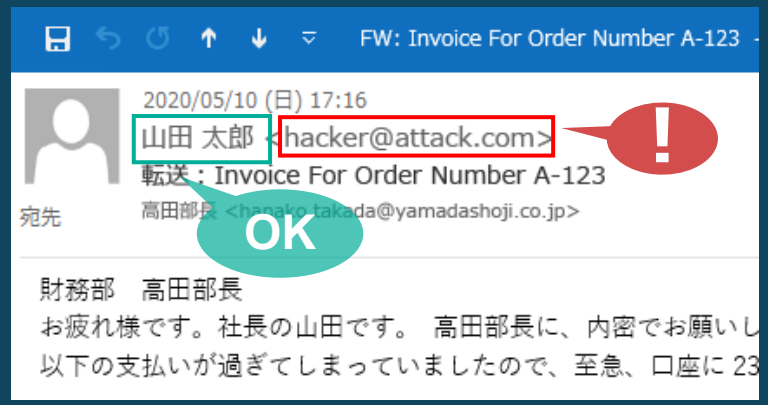


proofpoint

© 2024 Proofpoint. All rights reserved

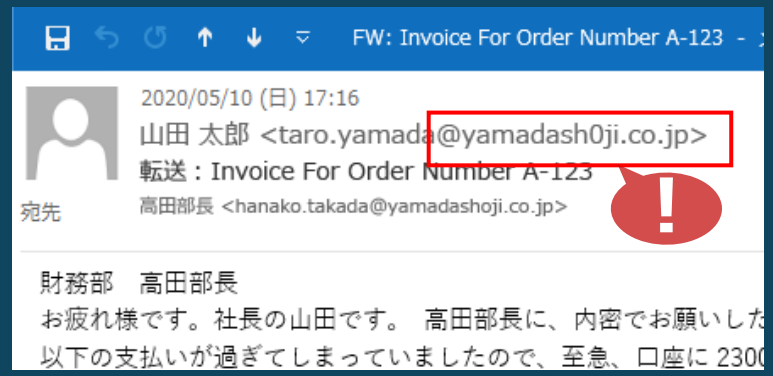
なりすましメールの手口

表示名 詐称
(Display Name詐欺)



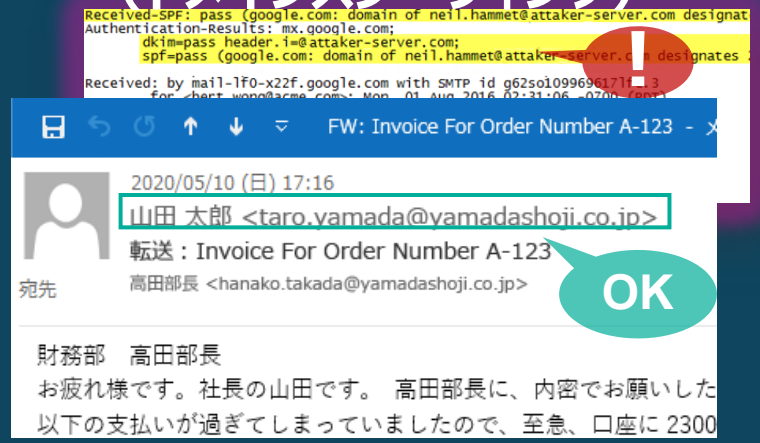
「from」フィールドの表示名は正規の名前だが、実際のアドレスは攻撃者

よく似た類似ドメイン
(タイポスクワッティング)



類似ドメインを装ったドメイン
例) Yamadashoji.co.jp
-> yamadash0ji.co.jp

ドメインのなりすまし
(ドメインスプーフィング)



目に見える「from」フィールドは正規だが、隠れた本当の送信元は攻撃者

※Reply To詐欺の手法も併用されることがあり、返信先に攻撃者のメールアドレスが指定されていることも

教育トレーニング

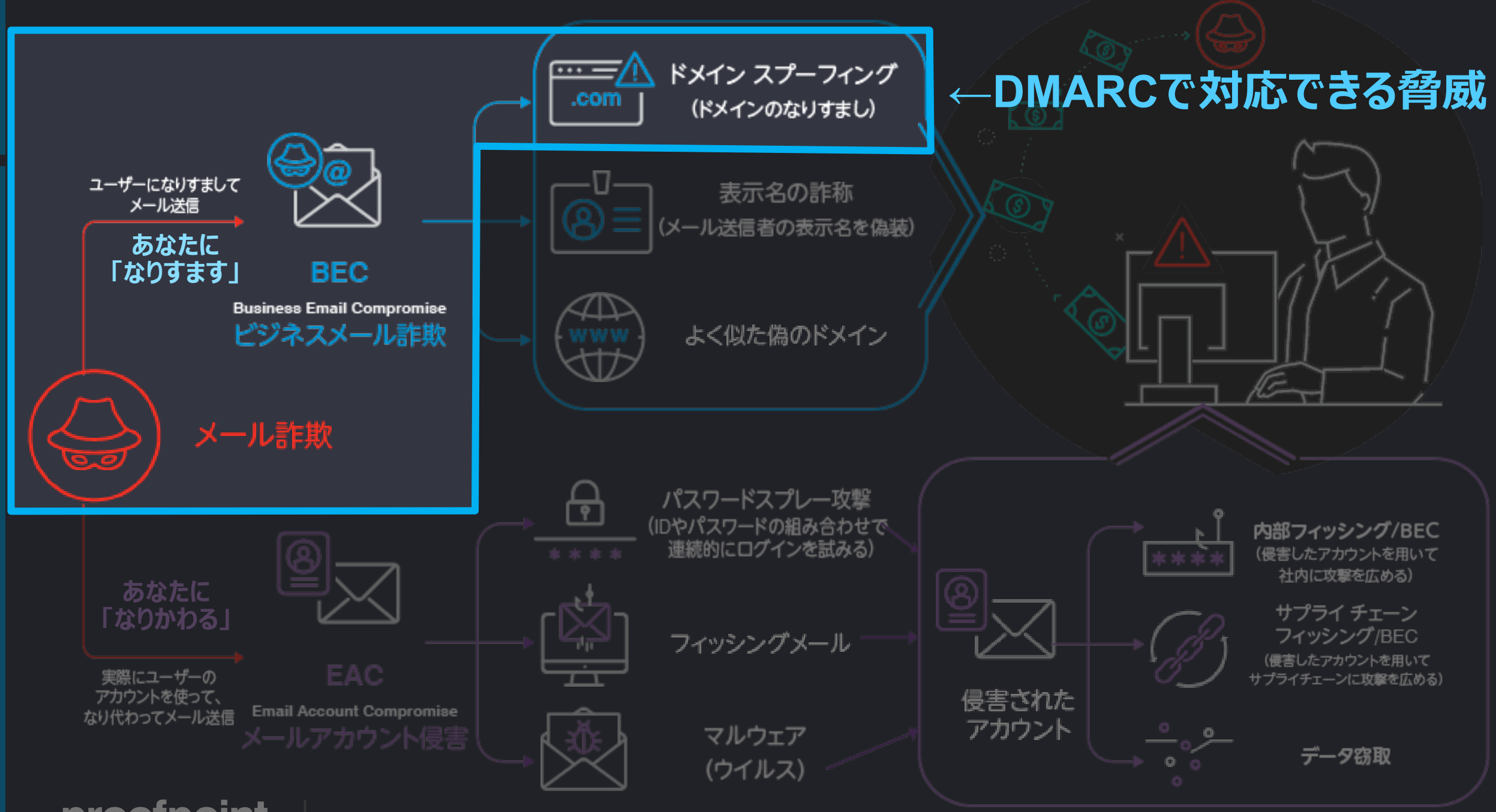
類似ドメインのテイクダウン

DMARCでブロック可能

DMARC + BIMI(VMC) で、なりすましメール全般の見破りが容易に

proofpoint

© 2024 Proofpoint. All rights reserved



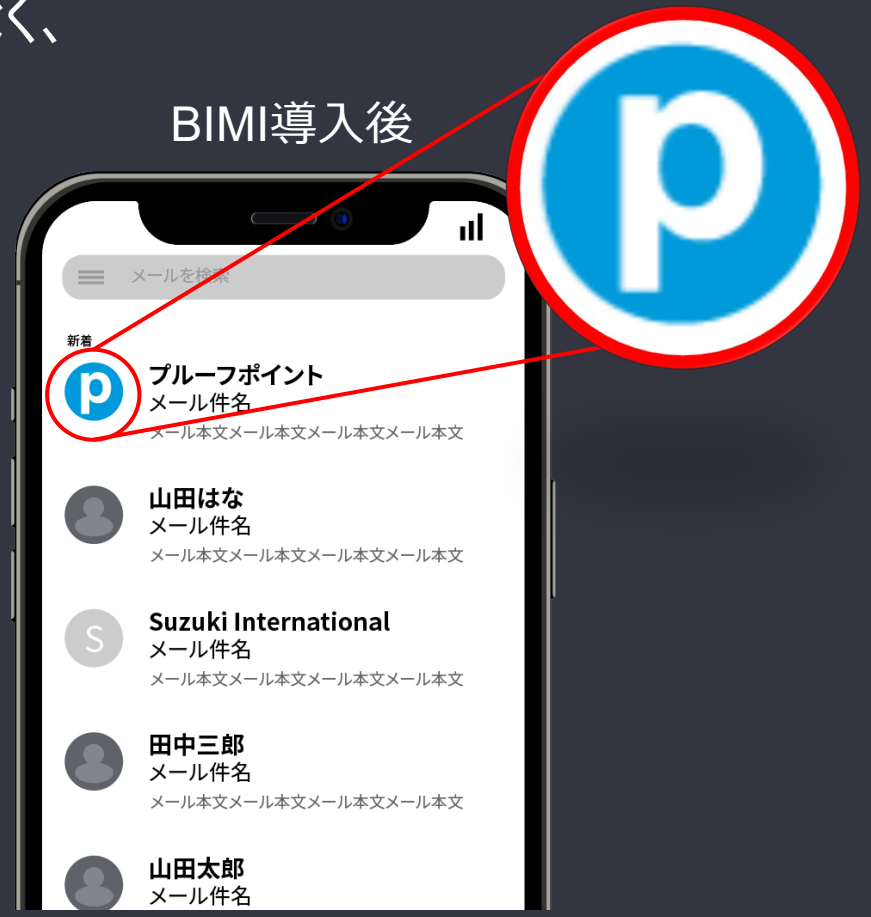
proofpoint
© 2024 Proofpoint. All rights reserved

認証されたメールに企業ロゴを表示するBIMI

DMARC認証が成功した場合は、ロゴを表示することによって
セキュリティが高い企業として信頼性を可視化するだけではなく、
ブランド認知も向上

BIMI導入前

BIMI導入後



© 2023 Proofpoint. All rights reserved

←DMARC+ BIMI(VMC)で対応できる脅威

ユーザーになりすまして
メール送信

あなたに
「なりすます」

BEC

Business Email Compromise
ビジネスメール詐欺

ドメイン スプーフィング
(ドメインのなりすまし)

表示名の詐称
(メール送信者の表示名を偽装)

よく似た偽のドメイン

メール詐欺

あなたに
「なりかわる」

実際にユーザーの
アカウントを使って、
なり代わってメール送信

EAC

Email Account Compromise
メールアカウント侵害

パスワードスプレー攻撃
(IDやパスワードの組み合わせで
連続的にログインを試みる)

フィッシングメール

マルウェア
(ウイルス)

侵害された
アカウント

内部フィッシング/BEC
(侵害したアカウントを用いて
社内に攻撃を広める)

サプライ チェーン
フィッシング/BEC
(侵害したアカウントを用いて
サプライチェーンに攻撃を広める)

データ窃取

proofpoint

© 2024 Proofpoint. All rights reserved

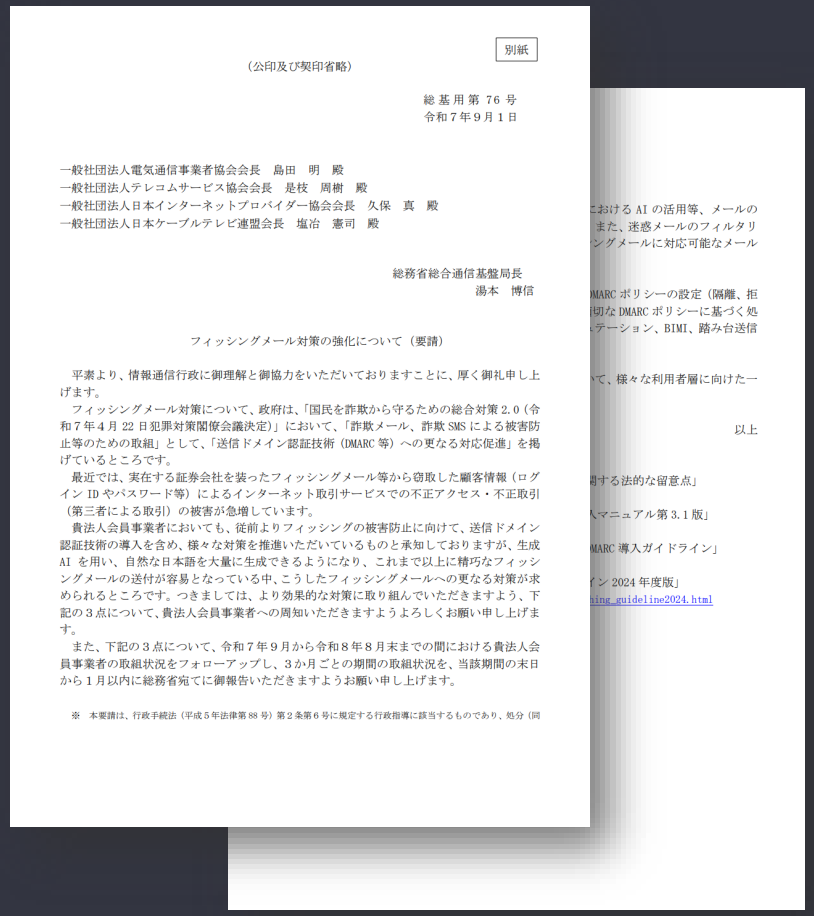
2025年9月　総務省

「フィッシングメール対策の強化」を通信事業者に要請

1. フィルタリングの判定技術の向上や迷惑メール判定における AI の活用等、**メールのフィルタリングの精度の一層の向上**を積極的に図ること。また、迷惑メールのフィルタリ ング強度を適切に設定するなどして、高度化するフィッシングメールに対応可能なメール フィルタリングを目指すこと。

2. なりすましメール対策として有効な DMARC の導入や **DMARC ポリシーの設定（隔離、拒否）** を行うこと。送信側だけでなく受信側についても、適切な DMARC ポリシーに基づく処 理やレポート送信を設定すること。また、**ドメインレピュテーション、BIMI、踏み台送信 対策等の更なる対策**の導入を積極的に検討していくこと。

3. 提供しているフィッシングメール対策サービスについて、様々な利用者層に向けた一 層の**周知・啓発**を行うこと。



別紙

（公印及び契印省略）

総 基 用 第 76 号
令和７年９月１日

一般社団法人電気通信事業者協会会長　島田　明　殿
一般社団法人テレコムサービス協会会長　是枝　周樹　殿
一般社団法人日本インターネットプロバイダー協会会長　久保　真　殿
一般社団法人日本ケーブルテレビ連盟会長　塩冶　憲司　殿

総務省総合通信基盤局長
湯本　博信

フィッシングメール対策の強化について（要請）

平素より、情報通信行政に御理解と御協力をいただいておりますことに、厚く御礼申し上げます。

フィッシングメール対策について、政府は、「国民を詐欺から守るための総合対策 2.0（令和７年４月 22 日犯罪対策閣僚会議決定）」において、「詐欺メール、詐欺 SMS による被害防止等のための取組」として、「送信ドメイン認証技術（DMARC 等）への更なる対応促進」を掲げているところです。

最近では、実在する証券会社を装ったフィッシングメール等から窃取した顧客情報（ログイン ID やパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増しています。

貴法人会員事業者においても、従前よりフィッシングの被害防止に向けて、送信ドメイン認証技術の導入を含め、様々な対策を推進いただいているものと承知しておりますが、生成 AI を用い、自然な日本語を大量に生成できるようになり、これまで以上に精巧なフィッシングメールの送付が容易となっている中、こうしたフィッシングメールへの更なる対策が求められるところです。つきましては、より効果的な対策に取り組んでいただきますよう、下記の３点について、貴法人会員事業者への周知いただきますようよろしくお願い申し上げます。

また、下記の３点について、令和７年９月から令和８年８月末までの間における貴法人会員事業者の取組状況をフォローアップし、３か月ごとの期間の取組状況を、当該期間の末日から１月以内に総務省宛てに御報告いただきますようお願い申し上げます。

※　本要請は、行政手続法（平成５年法律第 88 号）第２条第６号に規定する行政指導に該当するものであり、処分（同

https://www.soumu.go.jp/main_content/001028028.pdf

proofpoint

© 2024 Proofpoint. All rights reserved

広い業種にて、DMARC対策必須！

ビジネス詐欺メール対策DMARCをご存じですか？

対応が求められている分野

製造/化学/物流
トップ半導体メーカー/自動車メーカーより、取引先条件に追加

外部監査
数社のコンサルティングファームの監査項目に追加

クレジットカード会社
経産省/総務省/警察庁より2024年1月までに対応要請

政府/自治体/独法
令和５年版の政府統一基準にて2024年7月までに対応要請

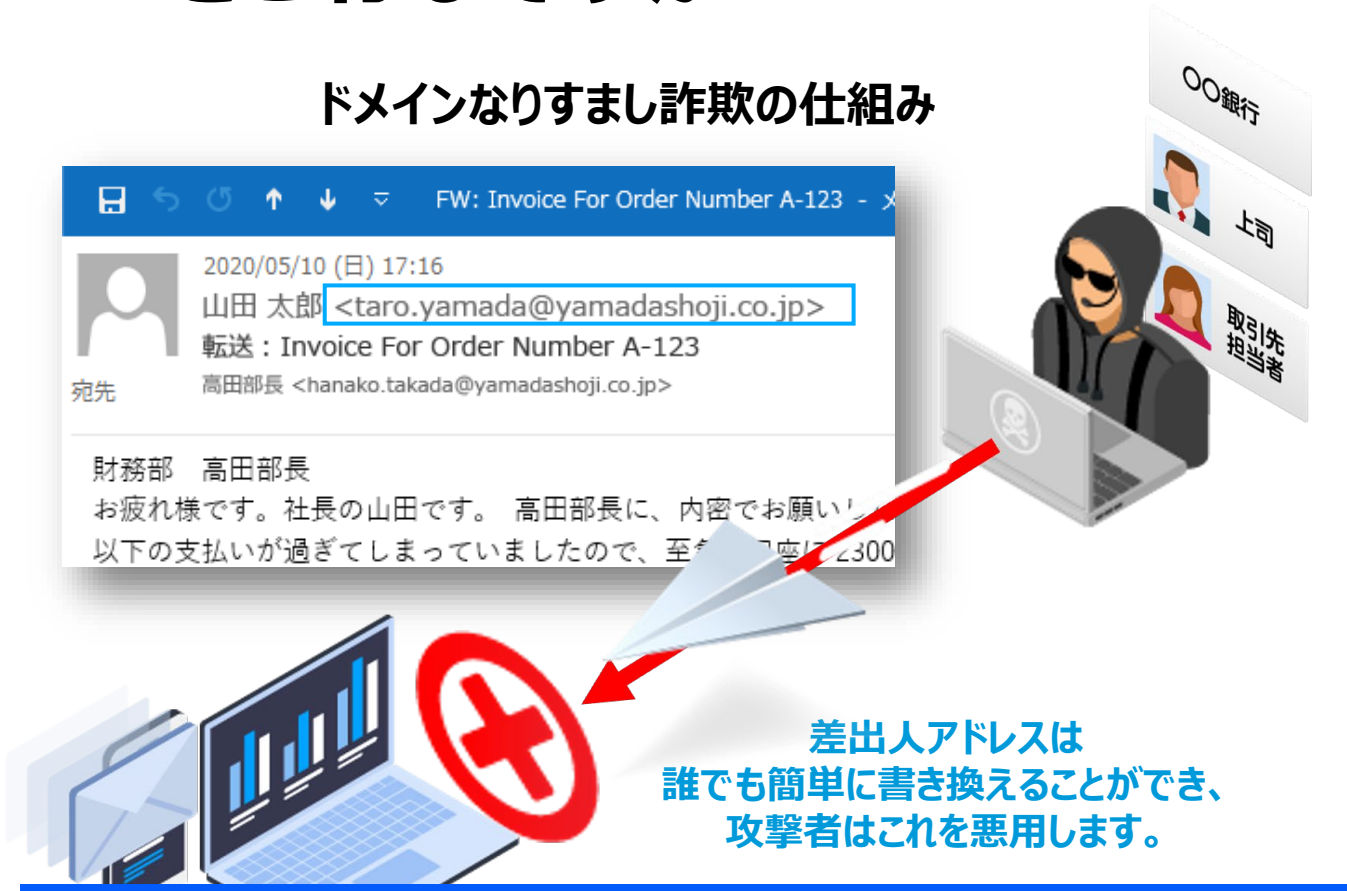
流通小売企業
PCI DSS v4.0にて2025年3月までに対応必要

一定量のメールを送信する企業
Google, 米Yahooの受信側のスパム対策として義務化

金融：
金融庁の2024年10月発表の「金融分野におけるサイバーセキュリティに関するガイドライン」で推奨

電気通信事業者/ISP：
2025年9月に総務省より要請

ドメインなりすまし詐欺の仕組み

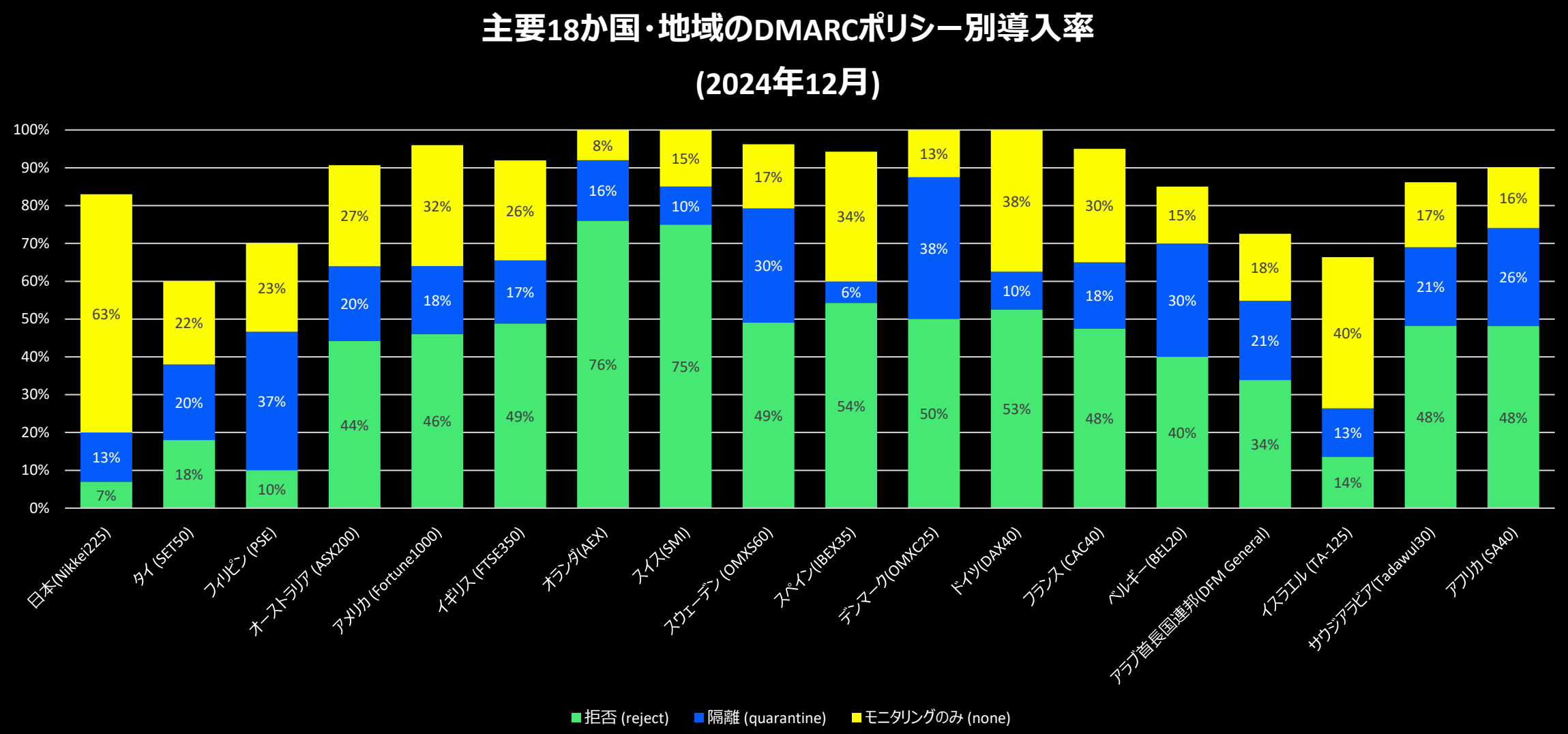


差出人アドレスは
誰でも簡単に書き換えることができ、
攻撃者はこれを悪用します。

**送信ドメイン認証のDMARCを設定することにより、
あなたの組織のドメインを使って
取引先を攻撃する詐欺メールをストップすることができます。**

© 2025 Proofpoint. All rights reserved

DMARC18か国調査



© 2025 Proofpoint. All rights reserved

ご清聴いただき、ありがとうございました。
proofpoint®