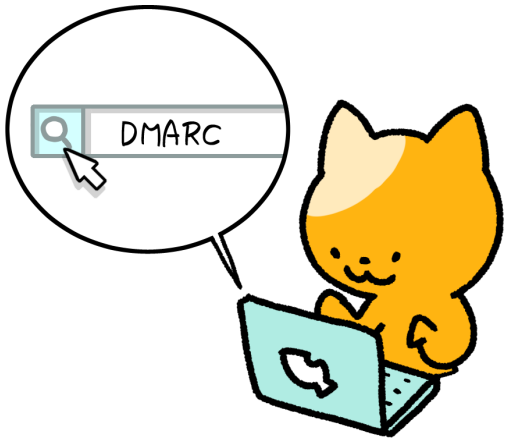
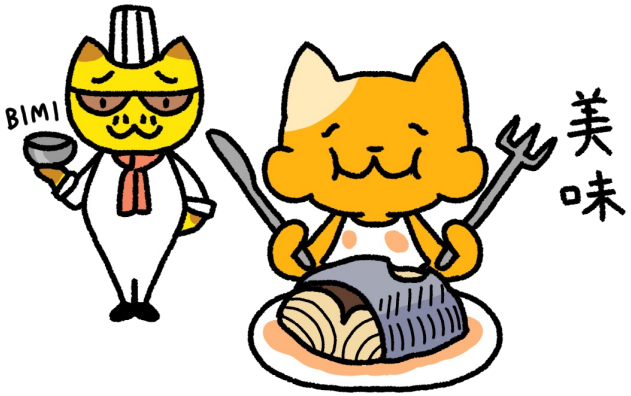
なりすましメール対策DMARCを導入することの効用

株式会社TwoFive
加瀬　正樹

目次



- TwoFive について
- なりすましメールの実際とその対策
- 送信ドメイン認証 SPF/DKIM/DMARC 解説
- DMARC 活用事例
- その他注意すること



会社紹介

TwoFiveは、メールから新時代のメッセージングまで
コミュニケーションのセキュリティ課題に挑むリーディングカンパニーです。

社名	株式会社TwoFive（TwoFive,Inc.）
設立	2014年5月
代表者	末政 延浩
事業内容	- メッセージングシステム - メッセージングセキュリティ - スレットインテリジェンス
所在地	本社 〒103-0027　東京都中央区日本橋3-1-4 画廊ビル3F ベトナム支社 TT01-37 Mon City, Ham Nghi, My Dinh 2, Nam Tu Liem, Hanoi, Vietnam
主要取引先	- NECソリューションイノベータ株式会社 - 株式会社日立ソリューションズ - 東芝デジタルソリューションズ株式会社 - 日本ヒューレット・パッカード合同会社 - 株式会社ブロードバンドセキュリティ - 株式会社インターネットイニシアティブ

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

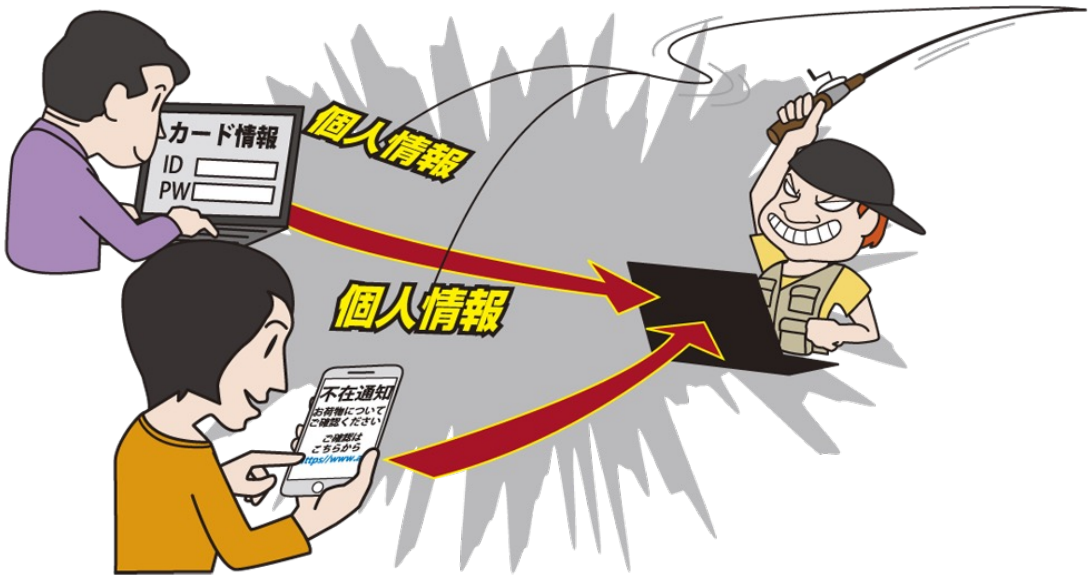
スレット
インテリジェンス

なりすましメールの実際とその対策

2022年度もメールに関連する脅威が目立つ

情報セキュリティ10大脅威 2023（※）でも、メールを悪用した被害が注目。

ビジネスメール詐欺による被害
（組織**第7位**）



フィッシングによる個人情報等の
詐取（個人**第1位**）

(※) https://www.ipa.go.jp/security/vuln/10threats2023.html

なりすましメールがフィッシングの入口に・・・

事例: なりすましフィッシングメールの大量配信

【VISAカード】利用いただき、ありがとうございます。
このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、
誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。

つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。
お客様にはご迷惑、ご心配をお掛けし、誠に申し訳ございません。
何卒ご理解いただきたくお願い申しあげます。
ご回答をいただけない場合、カードのご利用制限が継続されることもございますので、予めご了承下さい。

■ご利用確認はこちら　　の部分のリンク
<http://www.●●●●.com.cn/ic6oXx7P3s/page1.php> など

ご不便とご心配をおかけしまして誠に申し訳ございませんが、
何とぞご理解賜りたくお願い申しあげます。

■発行者■
VISAカード
東京都中野区中野4-3-2

©Copyright 1996-2022. All Rights Reserved.
無断転載および再配布を禁じます。

メール文面の例

- ほぼ同一文面で、ブランド名と署名欄だけ変更
- 2020年頃から使われている。

- 今まで確認されたブランド
  - 三井住友銀行
  - 三菱UFJ銀行
  - PayPay銀行
  - イオン銀行
  - 鹿児島銀行
  - 三井住友カード
  - 三菱UFJニコス
  - JCB
  - JACCS
  - オリコ
  - アプラス
  - エムアイカード
  - エポスカード
  - イオンカード
  - UC カード
  - UCSカード
  - ビューカード
  - 楽天
  - 楽天カード
  - ライフカード
  - VISA
  - Mastercard
  - au PAY
  - えきねっと など
    （順不同）

フィッシング対策協議会
クレジットカードの利用確認を装うフィッシング (2022/06/24)
https://www.antiphishing.jp/news/alert/creditcard_20220624.html

- このタイプは配信量が非常に多く、報告が多い
- 本物と同じドメインを使った**なりすまし送信率**が高い
- **2022年5月以降に増えた大量のURLを使用したフィッシングもこのタイプ**

(※) https://www.janog.gr.jp/meeting/janog51/wp-content/uploads/2022/12/JANOG51_DMARC_%E5%B9%B3%E5%A1%9A%E3%81%95%E3%82%93-1.pdf

なりすましメールの手口（ドメインなりすまし）

DMARC（ディーマーク）：2つの機能

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
どうかを認証する技術

分析

サーバに届いたメールの
認証結果を
ドメインの管理者に
集計レポートする技術

認証＋集計レポートによって
正しいメールを届けて
なりすましメールを削除できます

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
- 2023年2月 経産省/総務省/警察庁
  カード会社などへ DMARC 導入要請

c.f. 経産省などから DMARC 導入要請（2023年2月）

HOME | 脅威 | 脆弱性 | 情報漏えい | インシデント | 不正アクセス | 報告書 | 講演 | 業界

› Scan PREMIUM とは › 脅威 › 脆弱性 › インシデント › 情報漏えい › 著作権侵害 › 製品・サービス

› 製品・サービス・業界動向 › 業界動向 › 記事

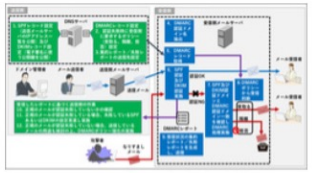
製品・サービス・業界動向 ／ 業界動向

2023年2月3日（金） 08時00分

総務省ら、クレジットカード会社等にDMARCの導入を要請

総務省、警察庁、経済産業省は、「クレジットカード会社等に対するフィッシング対策強化の要請」を発表した。

総務省、警察庁、経済産業省は2月1日、「クレジットカード会社等に対するフィッシング対策強化の要請」を発表した。クレジットカード番号等の不正利用の原因の一つであるフィッシング被害が増加していることを受けたもの。



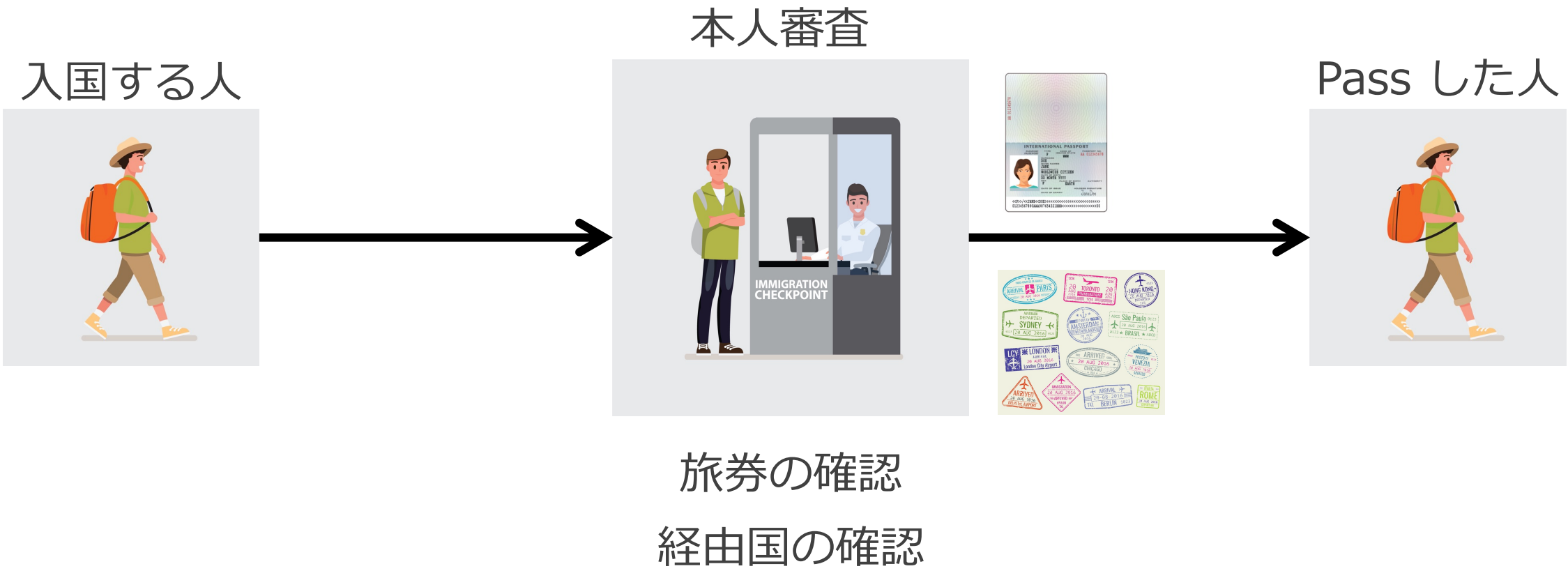
DMARCの仕組み

https://scan.netsecurity.ne.jp/article/2023/02/03/48863.html

送信ドメイン認証 SPF/DKIM/DMARC 解説

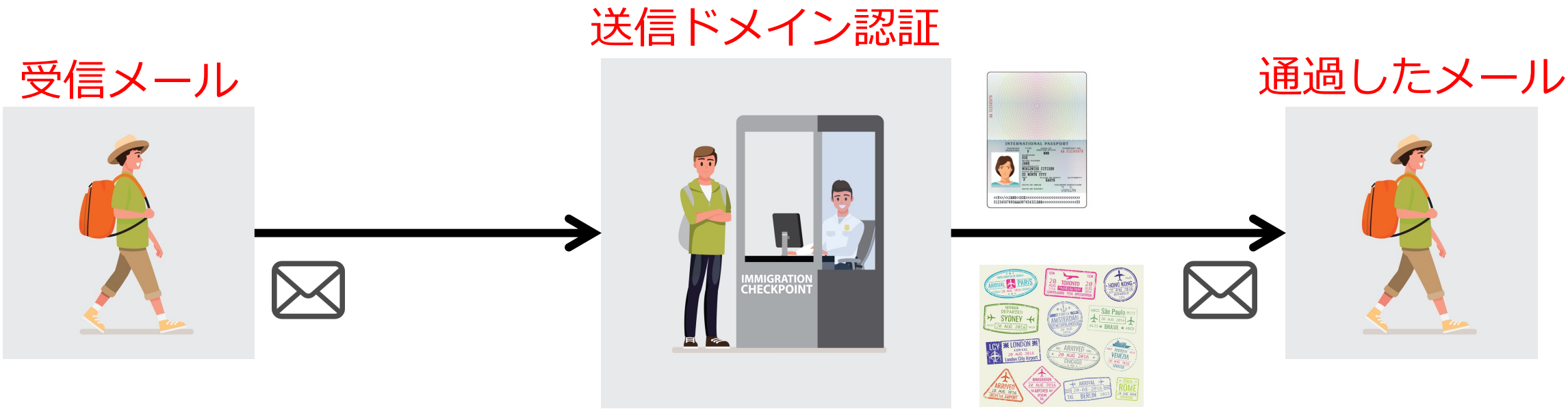
送信ドメイン認証技術

- 例えるならば、入国管理と同じ・・・



送信ドメイン認証技術

- 認証結果をパスポートに**記録する**（だけ）



DKIM の確認

SPF の確認

送信ドメイン認証技術

- ドメイン単位で送信者が名乗っている情報(メールアドレス)が**正しいか確認する**技術

SPF	規格	DKIM
RFC 7208	ドキュメント	RFC 6376 (STD 76)
IPアドレスで判定	認証方法	電子署名で判定
エンベロープ From ドメイン	保護する対象	署名ドメイン
DNS に設定を記述	対応の難しさ	サーバーに実装
Authentication-Results ヘッダー	確認方法	Authentication-Results ヘッダー
転送に弱い **ヘッダー From 詐称が可能**	**問題点**	メーリングリストに弱い **ヘッダー From 詐称が可能**

DMARC – ポリシー機能

Domain-based Message Authentication, Reporting and Conformance

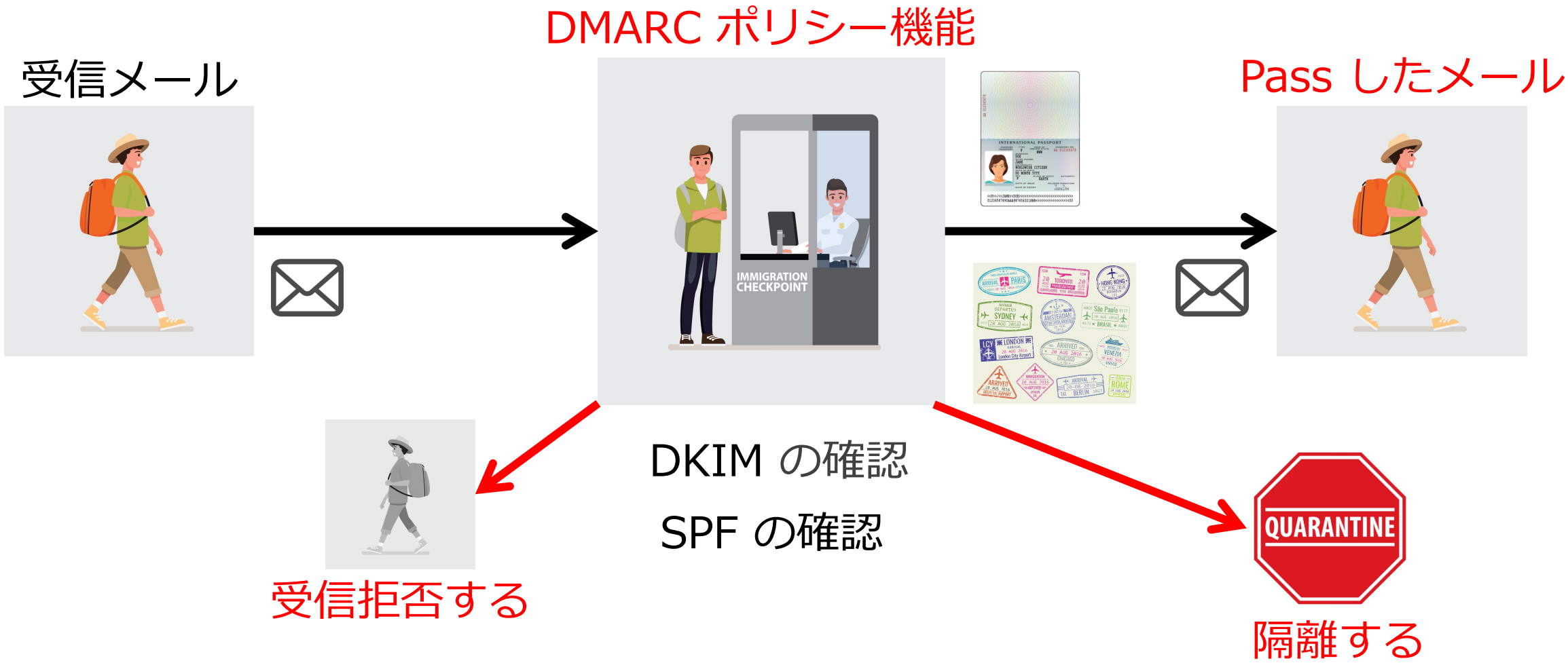
- 2012年1月 電子メール関連企業・組織により DMARC.org 設立
  - PayPal, Bank of America, LinkedIn, Facebook
  - Comcast, Google, Yahoo, Microsoft など

- **ポリシー機能**によるメール取り扱い指定
  - DMARCの認証結果が失敗した場合、受信者にどのように処理してほしいか宣言する。

  - **none** (何もしない)
    ✓受信箱へ入れる
  - **quarantine** (隔離する)
    ✓迷惑メール判定する、迷惑メールフォルダーへ入れる
  - **reject** (受信拒否する)
    ✓送信者へエラーを返す、受信して破棄する

DMARC – ポリシー機能

- DMARC は結果に応じて**制限ができる**



DMARC – レポート機能

Domain-based Message Authentication, Reporting and Conformance

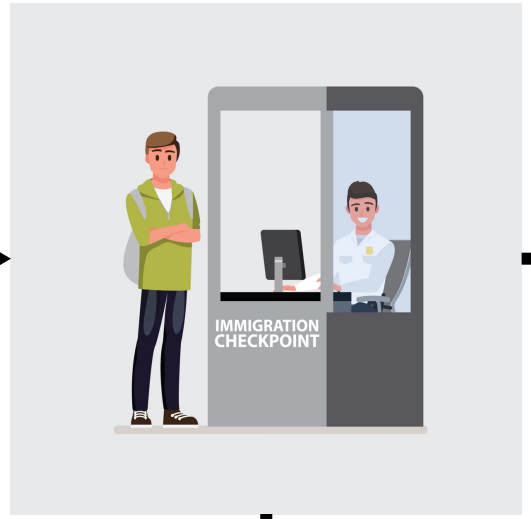
- 2012年1月 電子メール関連企業・組織により DMARC.org 設立
  - PayPal, Bank of America, LinkedIn, Facebook
  - Comcast, Google, Yahoo, Microsoft など
- ポリシー機能によるメール取り扱い指定
  - DMARCの認証結果が失敗した場合、受信者にどのように処理してほしいか宣言する。
- **レポート機能**によるフィードバック
  - DMARC/SPF/DKIM認証結果、送信元情報

DMARC – レポート機能

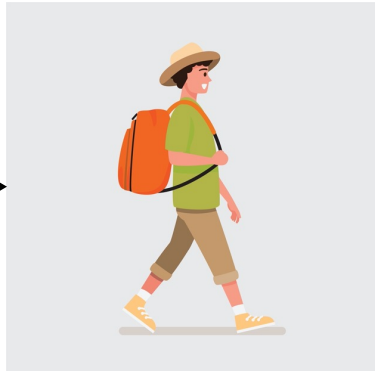
- DMARC は結果が**フィードバック**される

DMARC レポート機能

受信メール



Pass したメール



ドメイン管理者

DKIM/SPF認証結果・送信元情報など

DMARC – 認証仕様

Domain-based Message Authentication, Reporting and Conformance

- 2012年1月 電子メール関連企業・組織により DMARC.org 設立
  - PayPal, Bank of America, LinkedIn, Facebook
  - Comcast, Google, Yahoo, Microsoft など
- ポリシー機能によるメール取り扱い指定
  - DMARCの認証結果が失敗した場合、受信者にどのように処理してほしいか宣言する。
- レポート機能によるフィードバック
  - DMARC/SPF/DKIM認証結果、送信元情報
- **SPF、DKIM いずれかで認証 Pass** すればよい
- **ヘッダー From**を保護できる

DMARC – 導入方法

- SPF と同じようにDNS の TXT レコード（_dmarc.example.com）に上記のような宣言をする
- 親ドメインに設定することで、配下のサブドメイン全てに適用が可能
- 認証結果をメール受信側からレポート受信先へフィードバックがある

v=DMARC1; p=none; rua=mailto:rua@example.com

バージョン

必須

ポリシー

none: そのまま受信
quarantine: 隔離
reject: 拒否

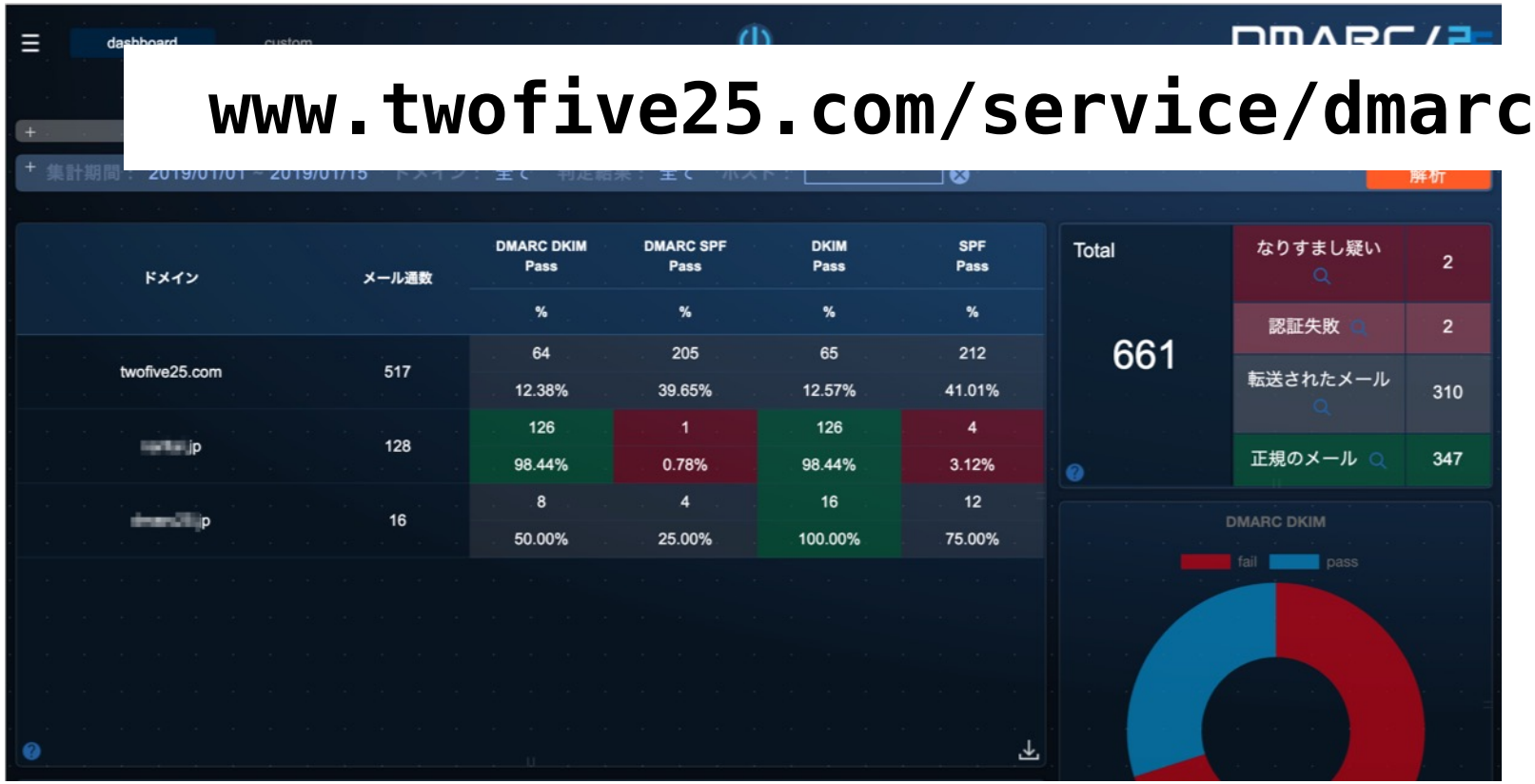
レポート受信先

任意だが設定すべき

DMARC 活用事例

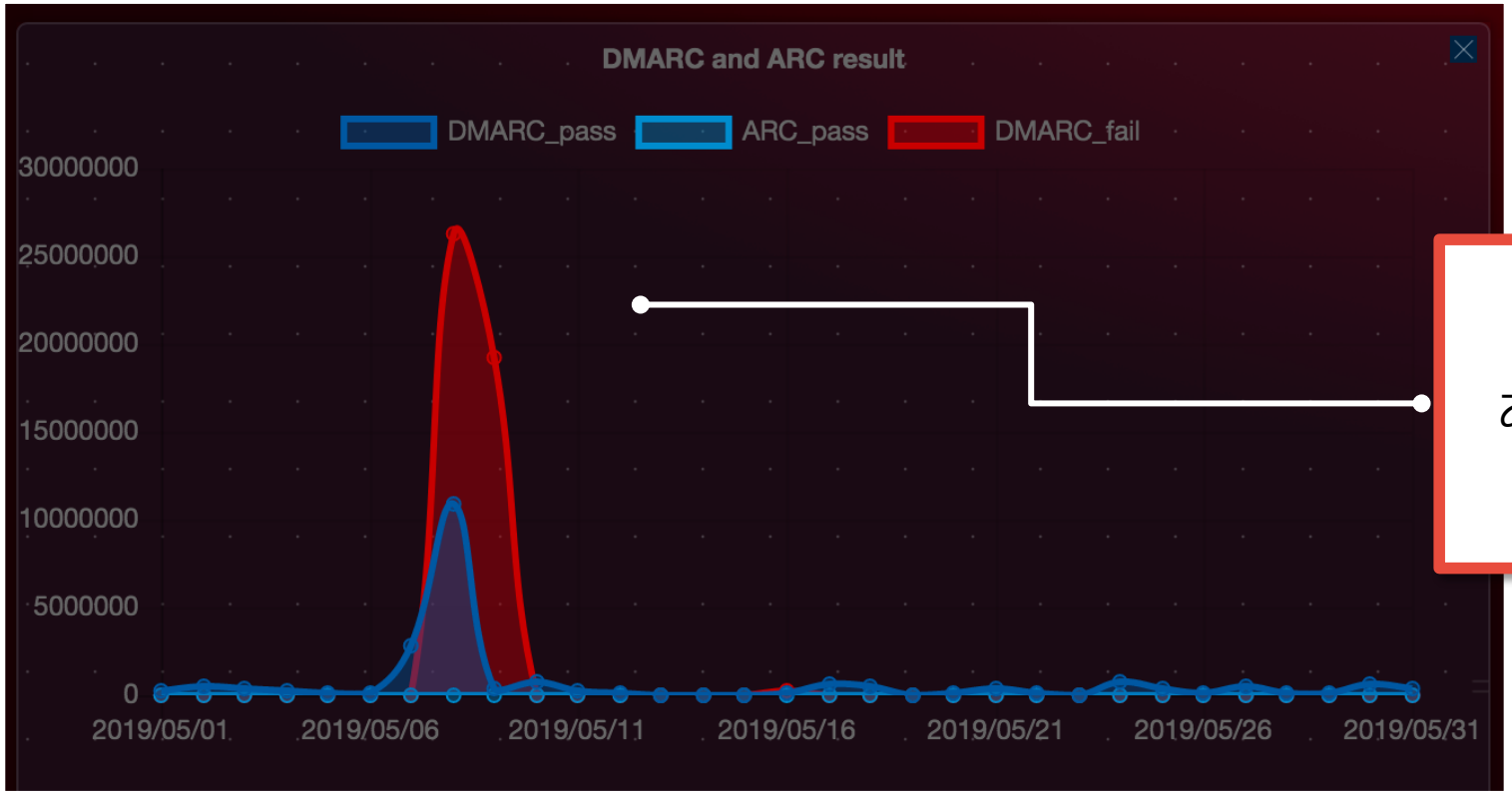
[紹介] クラウド型分析ツール DMARC/25 Analyze

DMARCの集計レポートを分析し、可視化し、なりすましの検知を支援するクラウドサービスです。



効用1. 実際のなりすましメールの流通がわかる

- 認証結果を集計すれば、**なりすましメールの流通状況**を把握でき、取引先へのアナウンス、不正利用通報、DMARC ポリシー強化につながる



XX月XX日に
あなたのドメインを騙った
メールが流通していた！

効用2. 正規メールサーバが可視化される

- 認証結果を集計すれば、**送信元メールサーバの一覧**がわかり、把握していないメールサーバ（シャドー IT）が見つかる

IPアドレス / ホスト	分類	国名	メール通数	DMARC DKIM Pass %	DMARC SPF Pass %	DKIM Pass %	SPF Pass %	ARC Pass %
[redacted]118.87		Japan	145	0	0	0	0	0
[redacted]znlc.jp				0.00%	0.00%	0.00%	0.00%	0.00%
[redacted]112.100		Japan	27	27	0	27	0	
[redacted]				100.00%	0.00%	100.00%	0.00%	
[redacted]		Japan	23	23	0	23	23	
[redacted]				100.00%	0.00%	100.00%	100.00%	
[redacted]159.89		United States	11	0	0	11	11	
[redacted]mail.sendgrid.net				0.00%	0.00%	100.00%	100.00%	0.00%

マーケティング部門が
CRM を使っているけど
SPF も DKIM も未設定！

効用3. 設定不備がわかる

- 認証結果を集計すれば、SPF の設定不備や把握していない**サブドメイン**を検出でき、それらを改善をすることでメール到達性を向上できる

ドメイン	メール通数	DMARC DKIM Pass	DMARC SPF Pass	DKIM Pass	SPF Pass
		%			
[redacted]jp	2,692	2,317			
		86.07%			
[redacted]	851	86			
		10.11%	78.14%	15.04%	83.08%
[redacted]	122	0	0	0	113
		0.00%	0.00%	0.00%	92.62%
id.[redacted]	71	0	0	28	49
		0.00%	0.00%	39.44%	69.01%

知らないところで
こんなサブドメインをメールで
使っていたのか！

c.f. BIMI

Brand Indicators for Message Identification

- DMARC やそのポリシー強化を推進するために規格化

- これまではメールサービスが独自（認証と評価基準）でアイコン表示
  - Yahoo!メール
  - ニフティ
  - So-net
  - NTTドコモ

参考: https://bimigroup.org/

c.f. BIMI

- DMARC ポリシーを強化して、正当なロゴマークを表示することが可能

Gmail（Webメールの表示例）

その他注意すること
（DMARC では保護できないフィッシング）

再掲: なりすましメールの手口（ドメインなりすまし）

なりすましメールの手口（類似ドメイン）

なりすましメールの手口（ランダムドメイン）

なりすましメールの手口（スクワッティング）

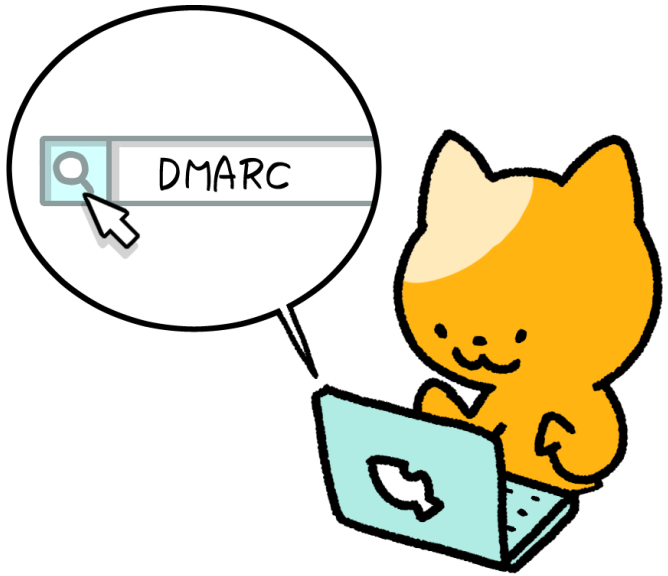
その他 DMARC では対策が難しい手口

- アカウント乗っ取り（踏み台メール送信）
- ソーシャル攻撃
- コンパネ不正利用（DNS ゾーンの不正書き換え）

まとめ

- メールに関連する脅威やその対策に変化が出てきている
- DMARC によってなりすましメールを「認証」し「分析」する
- IPベースの SPF と電子署名ベースの DKIM と合わせた技術
- DMARC による効用と BIMI への対応
- DMARC/25 Analyze でより効果的なりすまし対策の運用を

1ヶ月無料トライアルが可能
DMARC 導入を体感できます



ありがとうございました

DMARC/フィッシング対策は TwoFive におまかせください

https://www.twofive25.com/

sales@twofive25.jp