電子メールにおける信頼できる情報とは

株式会社TwoFive　加瀬 正樹

会社概要

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	● メッセージングテクノロジー ● ITセキュリティ ● モバイルテクノロジー
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
販売パートナー	● 株式会社日立ソリューションズ ● NECソリューションイノベータ株式会社 ● 東芝デジタルソリューションズ 株式会社 ● 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 ● SB C&S株式会社 ● スターネット株式会社 ● 株式会社QTnet
主要取引銀行	三井住友銀行（プロパー）

事業内容

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

twofive

メッセージングテクノロジー

電子メールに関する
多彩な製品と教育・コンサルティング

ITセキュリティ

ITシステムに関する
セキュリティソリューションとコンサルティング

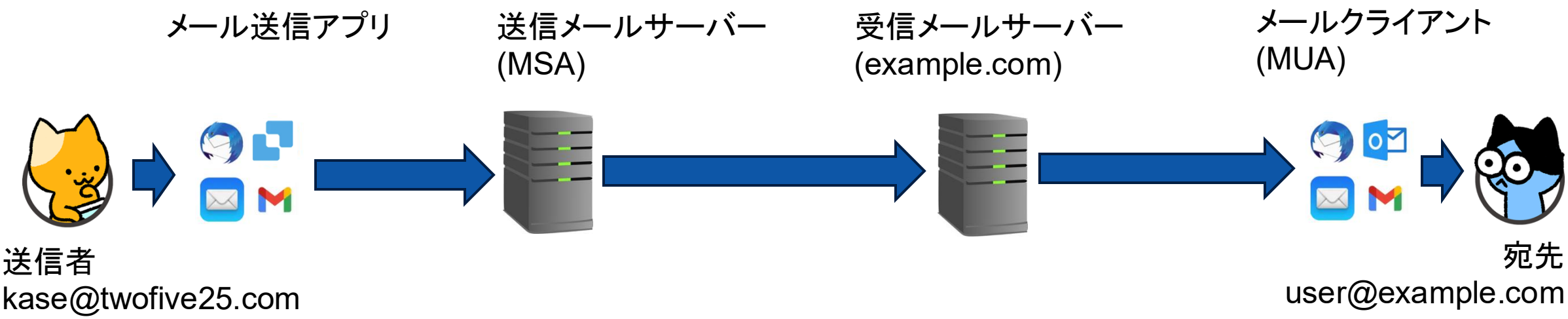
モバイルテクノロジー

最新のモバイルネットワークやセキュリティを
提供するためのプラットフォームとサービス

メールヘッダーと
メールクライアント

メールの流れとメールヘッダー

一般的なメールでは、経由したメールサーバー（MSA, MTA）でヘッダーを追加し、場合によっては内容を改変することがあります。

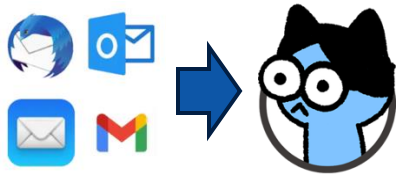


1. 差出人(From)
   宛先(To,Cc)
   件名(Subject)
   その他(Dateなど)
2. 配送経路(Received)
3. 配送経路(Received)
   送信元(Return-Path)
   配送先(Delivered-To)
4. 差出人(From)
   宛先(To,Cc)
   件名(Subject)

実際のメールクライアントでの表示

一般的なメールでは、経由したメールサーバー（MSA, MTA）でヘッダーを追加し、場合によっては内容を改変することがあります。
メールクライアント（MUA）では、そのヘッダー情報を表示します。

メールクライアント
(MUA)

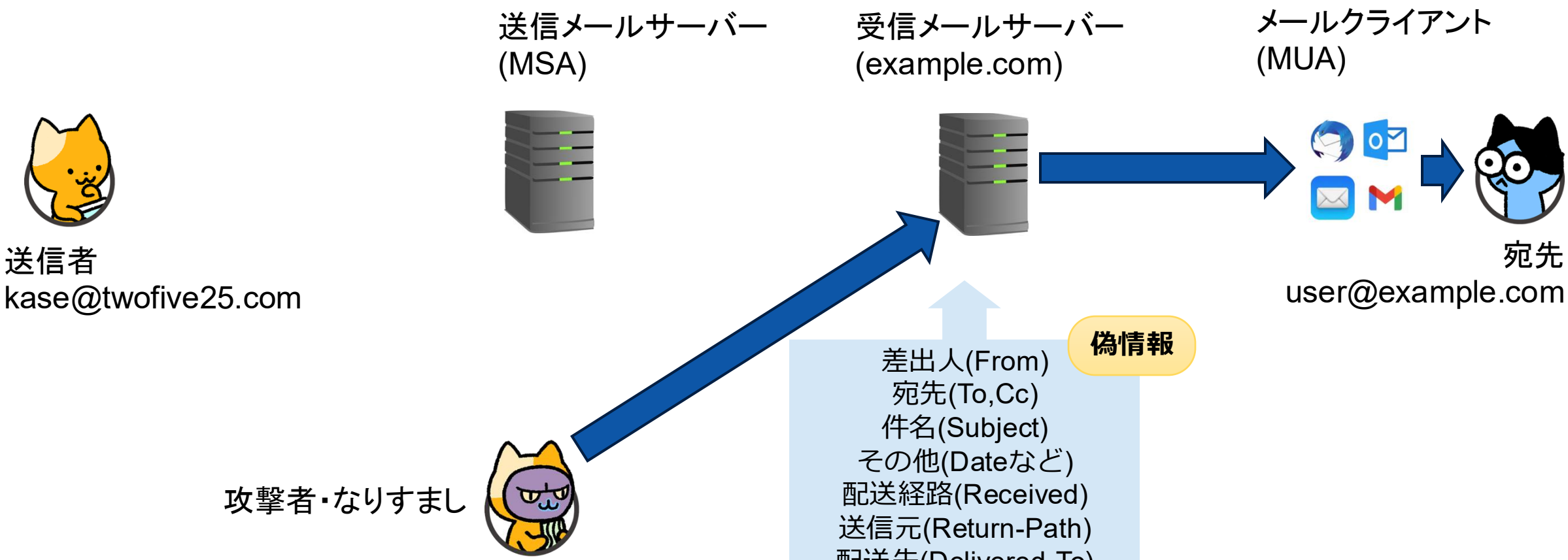


宛先
user@example.com

メールの流れとメールヘッダー(攻撃者のなりすまし)

攻撃者は騙す目的でメールヘッダーを加工・追加・改ざんができてしまいます。

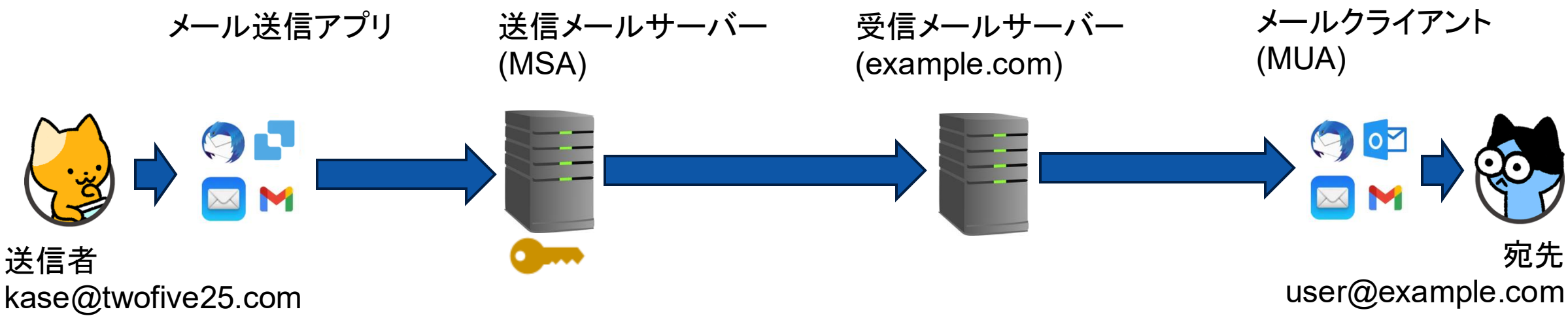
メールクライアントが表示する情報はそのままでは信頼できません（Untrusted）。



DKIM 署名による保護

DKIM (DomainKeys Identified Mail)

公開鍵方式で電子署名を作成、該当ドメインの DNS TXT レコードに公開された公開鍵をもとにして電子署名を検証し、結果として正規のメールサーバー（署名メールサーバー）から送信されたことを確認します（信頼します）。



1. 差出人(From)
   宛先(To,Cc)
   件名(Subject)
   その他(Dateなど)

2. 電子署名(DKIM-Signature)
   配送経路(Received)

3. 認証結果(Authentication-Resuls)
   配送経路(Received)
   送信元(Return-Path)
   配送先(Delivered-To)

4. 差出人(From)
   宛先(To,Cc)
   件名(Subject)
   認証結果

DKIM 署名

送信メールサーバー
(MSA)

送信者
kase@twofive25.com

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=twofive25.com; s=20230601; t=1758685612; x=1759290412;
h=from:to:cc:subject:date:message-id:reply-to;
bh=koWKRuRtbuq・・・・・Vs28366ut+JQ==

2

ヘッダー（from, to, cc, subject,・・・）とメール本文を使って
ハッシュ値を計算（koWKRuRtbuq・・・・・Vs28366ut+JQ==）
なお、DKIM 鍵は 20230601 を利用しており、この電子署名の有効期限は
205/10/01 12:46:52 まで

From: "Masaki Kase" <kase@twofive25.com>
Date: Wed, 24 Sep 2025 12:46:40 +0900
Message-ID: <CAOr0XRHc3mY1EWiw86xxxxxxxxxxxxxxxxx@xxxxxxxxx.com>
Subject: DKIM テストメール
To: "foo bar" <foobar@example.com>

・・・

DKIM 検証

受信メールサーバー
(example.com)

Authentication-Results: example.com;
dmarc=pass header.from=twofive25.com;
dkim=pass header.d=twofive25.com header.s=selector;
spf=pass smtp.mailfrom=twofive25.com;

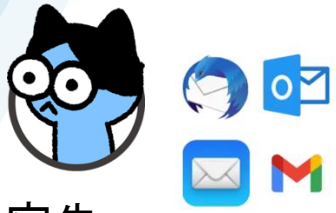
3 DKIM-Signature ヘッダーのハッシュ値が正しいため DKIM は pass

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=twofive25.com; s=20230601; t=1758685612; x=1759290412;
h=from:to:cc:subject:date:message-id:reply-to;
bh=koWKRuRtbuq・・・・Vs28366ut+JQ==
From: "Masaki Kase" <kase@twofive25.com>
Date: Wed, 24 Sep 2025 12:46:40 +0900
Message-ID: <CAOr0XRHc3mY1EWiw86xxxxxxxxxxxxxxxxx@xxxxxxxxx.com>
Subject: DKIM テストメール
To: "foo bar" <foobar@example.com>

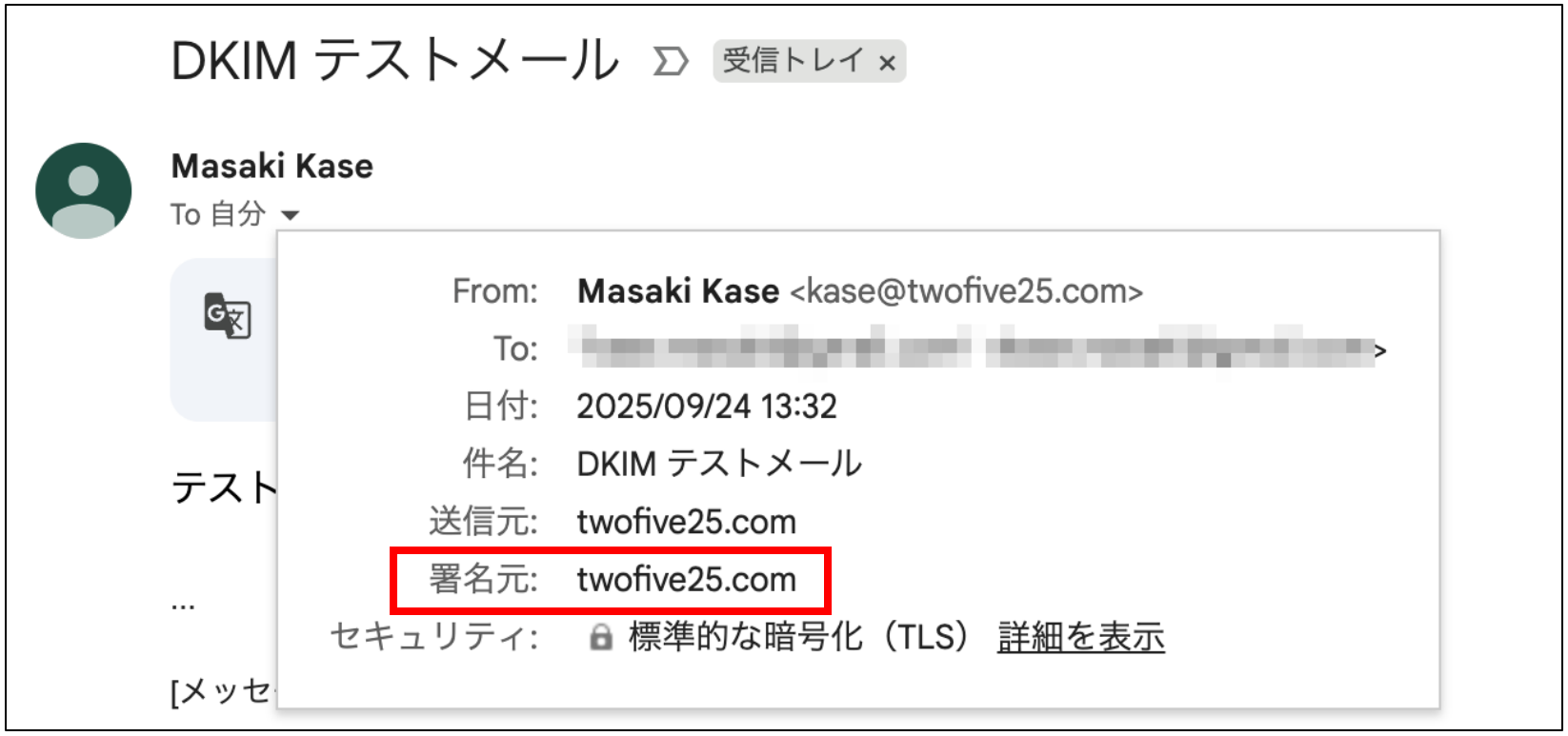
・・・

送信メールサーバー
(MSA)

DKIM 検証結果の表示



宛先
user@example.com



4

受信メールサーバー
(example.com)

Authentication-Results: example.com;
dmarc=pass header.from=twofive25.com;
dkim=pass header.d=twofive25.com header.s=selector;
spf=pass smtp.mailfrom=twofive25.com;

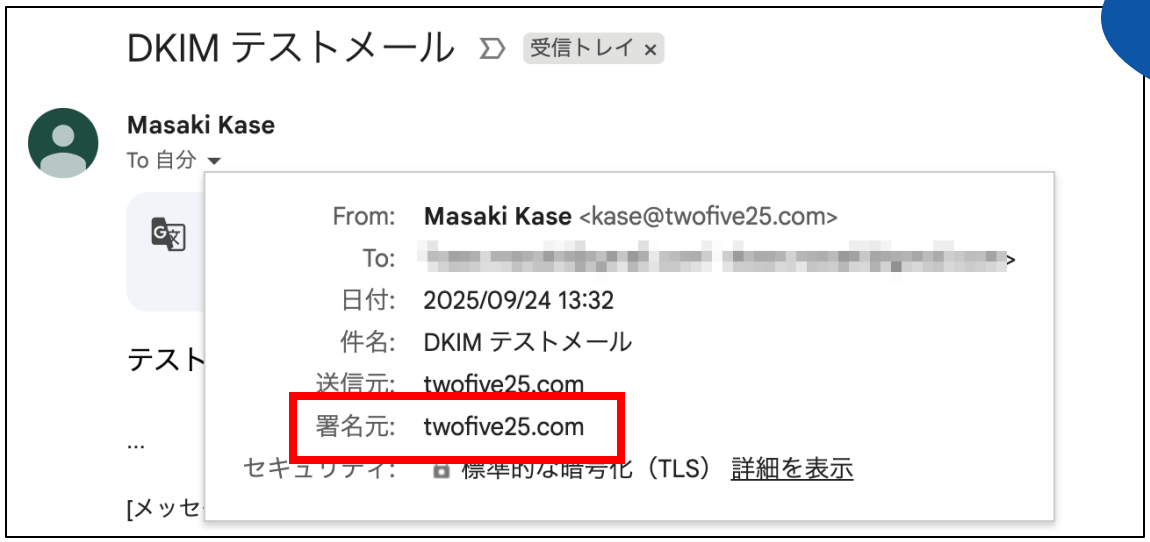
認証結果ヘッダー

Authentication-Results ヘッダー

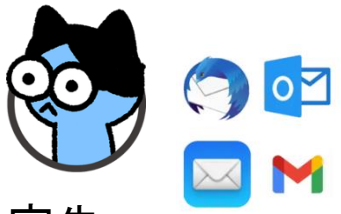
認証結果ヘッダーには、受信メールサーバー（MTA）が処理した SPF/DKIM/DMARC などの評価・結果を記録しています。

受信メールサーバー
(example.com)

Authentication-Results: example.com;
dmarc=pass header.from=twofive25.com;
dkim=pass header.d=twofive25.com header.s=selector;
spf=pass smtp.mailfrom=twofive25.com;
...



example.com
の認証結果は
信頼できる



宛先
user@example.com

Authentication-Results ヘッダー

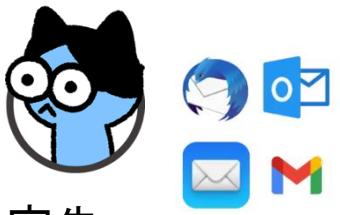
メールクライアント（MUA）は直前のヘッダーのみを信頼して、それ以外の（中間サーバーが付与した） Authentication-Results ヘッダーは信頼しません。

受信メールサーバー
(example.com)

Authentication-Results: example.com;
dmarc=fail header.from=twofive25.com;
dkim=fail header.d=twofive25.com header.s=selector;
spf=fail smtp.mailfrom=twofive25.com;
...
Authentication-Results: list.example.jp;
dmarc=pass header.from=twofive25.com;
dkim=pass;
spf=pass;
...

example.com
の認証結果は
信頼できる

list.example.jp
の認証結果は
信頼できない



宛先
user@example.com

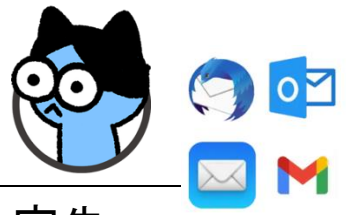
ARC-Authentication-Results ヘッダー

ARC は中間サーバーの認証結果ヘッダーを（連鎖的に）信頼できるようにして、その結果を ARC-Authentication-Results ヘッダーを通じて引き継ぐことができます。

受信メールサーバー
(example.com)

Authentication-Results: example.com;
arc=pass (as.1.example.com=pass);
dmarc=fail header.from=twofive25.com; dkim=fail;
spf=pass smtp.mailfrom=twofive25.com;
...
ARC-Authentication-Results: i=1; example.com;
dmarc=pass header.from=twofive25.com;
dkim=pass;
spf=pass smtp.mailfrom=twofive25.com;
...
Authentication-Results: list.example.jp;
dmarc=pass header.from=twofive25.com; dkim=pass;
spf=pass smtp.mailfrom=twofive25.com;
...

example.com
の認証結果は
信頼できる



宛先
user@example.com

https://datatracker.ietf.org/doc/html/rfc8617#appendix-B

おまけ
DMARC と BIMI

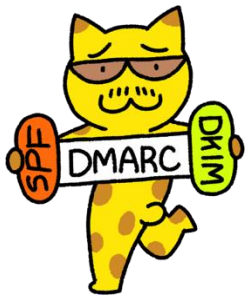
DMARC による認証

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

2012年
電子メール関連企業・組織により
DMARC.org 設立

2016年
2016年政府サービス義務化

2017年
2017年政府ドメイン義務化

2020年
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

2024年
2024年2月 Google/Yahoo.com
DMARC をメール送信ガイドラインに追加

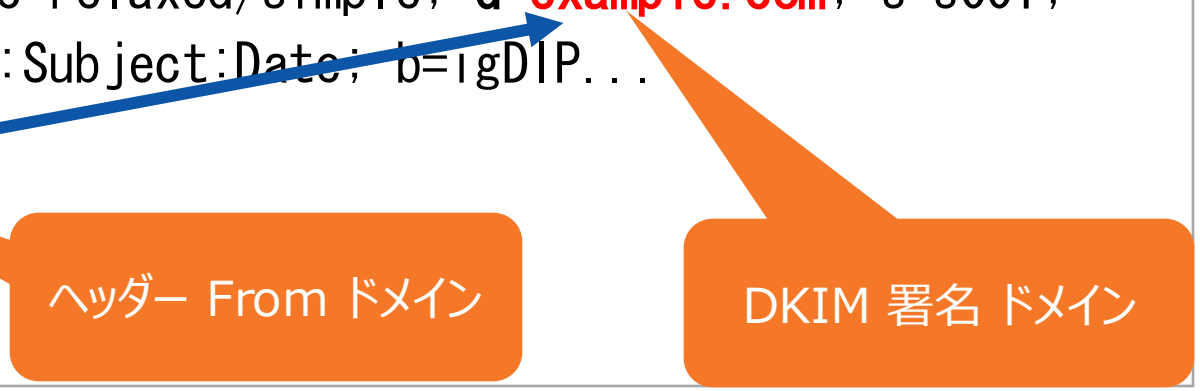
2025年
2025年1月 国内大手メールサービス
DMARC 必須化

DMARC による認証 – DKIM アラインメント

DKIM 署名がされており（信頼できて）、ヘッダー From ドメインと一致すれば、
DMARC 認証も pass（From ヘッダードメインがなりすましではない**）と評価します。**

※なりすましではない ≠ スパムではない

```
Return-Path: <taro@example.com>
Authentication-Results: example.com; spf=pass ... dkim=pass ... dmarc=pass ...
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=example.com; s=s001;
    t=154...; bh=A4I2Z...; h=To:From:Subject:Date; b=igDIP...
From: "Taro" <taro@example.com>
To: "Hanako" <hanako@twofive25.com>
Subject: Hello
```



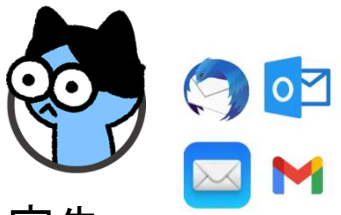
BIMI によるブランドアイコン表示

Gmail をはじめとしたメールサービスではなりすましメール対策の結果を評価して、あらかじめ設定された認証済みブランドアイコンを表示して、その信頼を可視化しています。

受信メールサーバー
(example.com)

```
Authentication-Results: example.com;
        dmarc=pass header.from=twofive25.com;
        dkim=pass header.d=twofive25.com header.s=selector;
        spf=pass smtp.mailfrom=twofive25.com;
        bimi=pass header.d=ml.kuronekoyamato.co.jp header.selector=default;
...
```

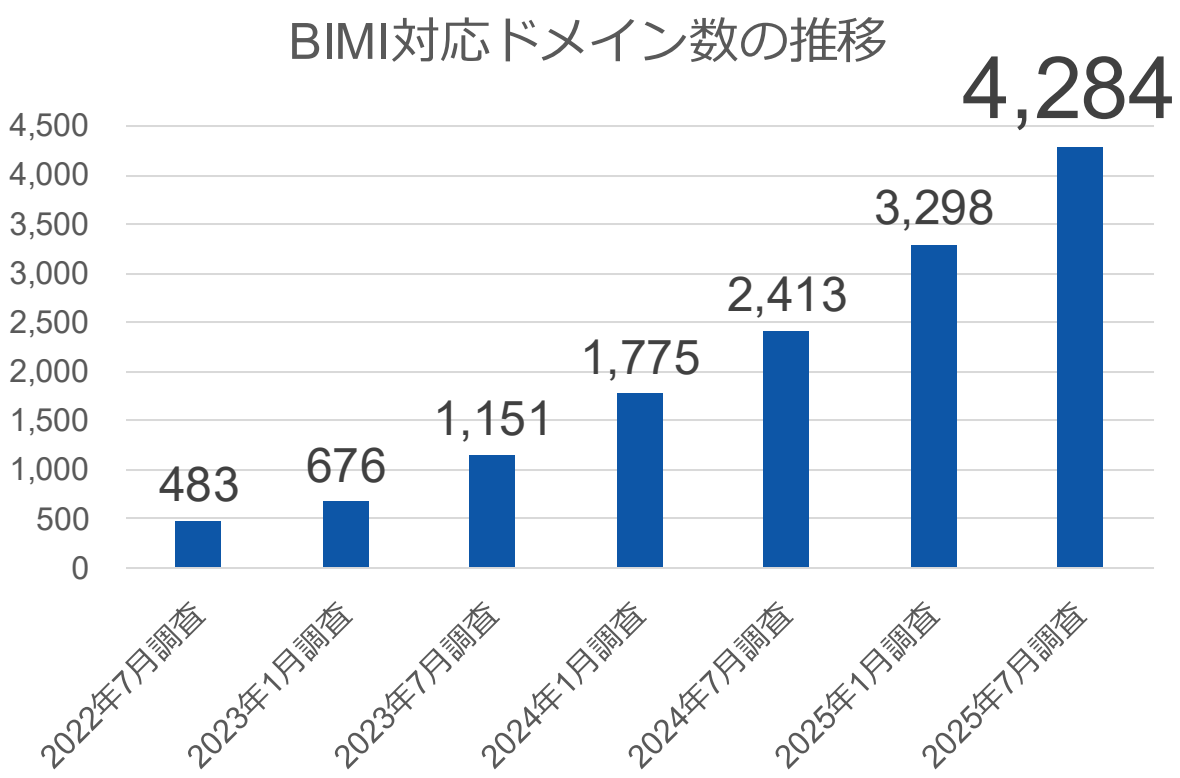
example.com
の認証結果は
信頼できる



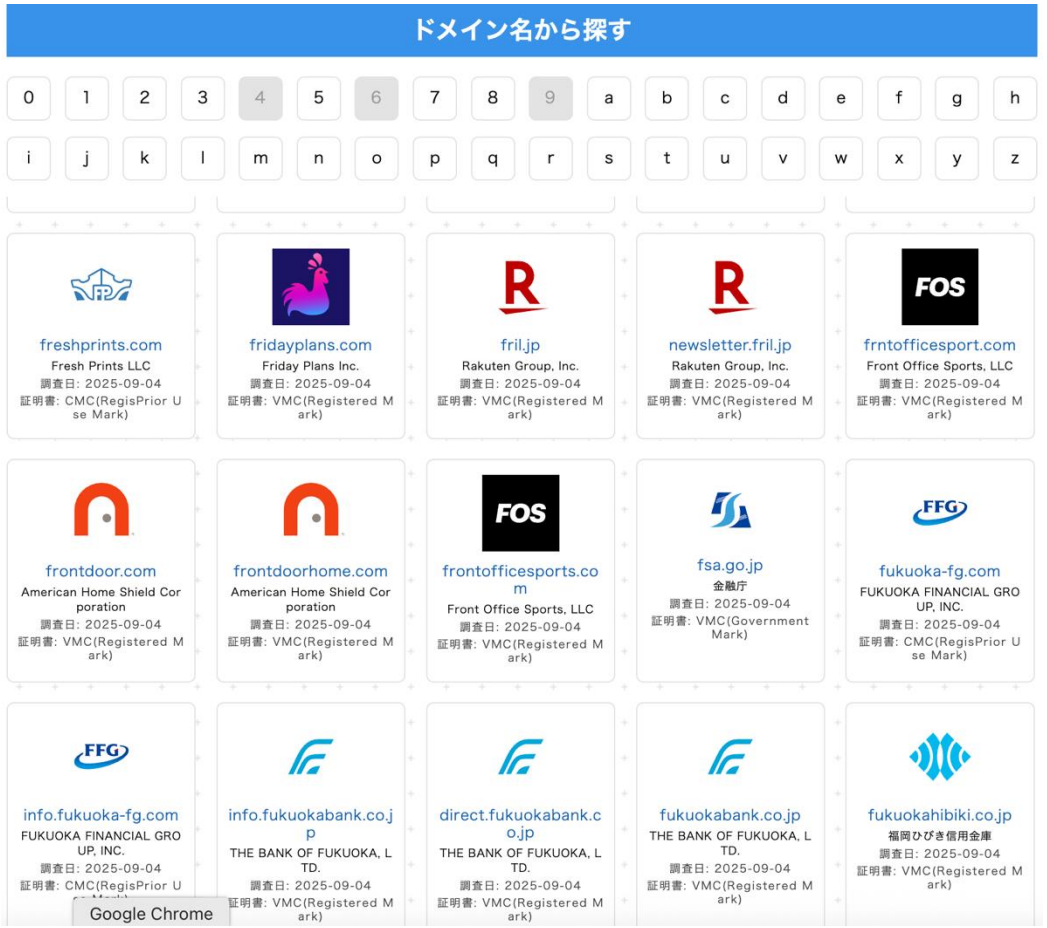
宛先
user@example.com

BIMI によるブランドアイコン表示

BIMI はここ数年で急増しており、直近の3年間で 995 % の成長率を示しています。



TwoFive 独自調べ



ナリタイ: https://naritai.jp/enterprise_bimilist.html

本日のまとめ

- 電子メールのヘッダーは必ずしも信頼はできない
- メールサーバーは DKIM 署名によって正規な送信者かを検証できる
- メールクライアントは Authentiation-Results ヘッダーの結果を表示できる
- DMARC は正規なメールとなりすましメールを見分ける
- BIMI は DMARC の結果をブランドアイコンで表示できる

- メールクライアントは接続先のメールサーバーを信頼できなければならない
- 認証結果の連鎖を信頼できなければならない

- サーバーやドメイン名のレピュテーションが信頼を今後築いていく

メールセキュリティに関しては
お気軽にお問い合わせください。

当社HP	https://www.twofive25.com/
お問い合わせフォーム	https://www.twofive25.com/contact/