C11
メールセキュリティ2025アップデート

スピーカー

- 古賀 勇(株式会社インターネットイニシアティブ)
- 加瀬 正樹(株式会社TwoFive)

本日のアジェンダ

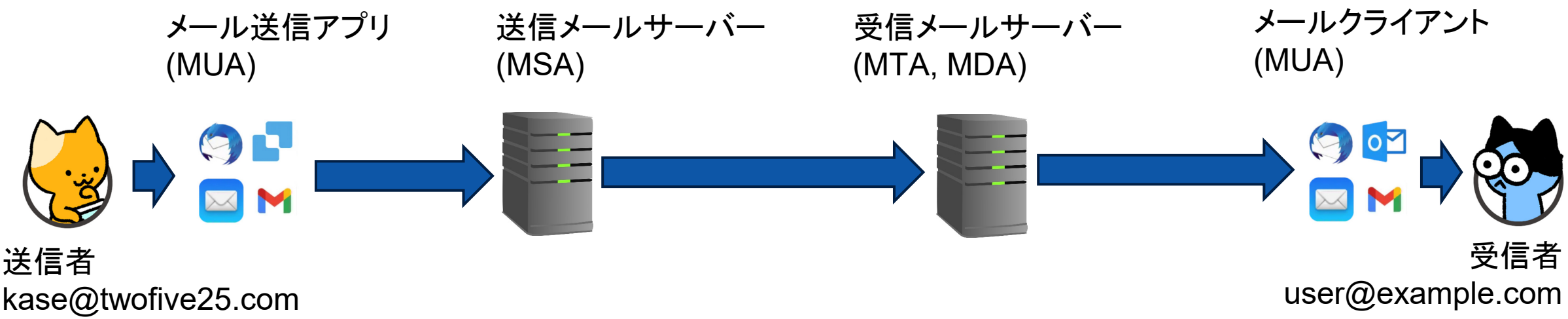
- メール基礎
- メール運用アップデート – DMARC
- メール運用アップデート – 証明書管理
- メール運用アップデート – 大量配信
- メール運用アンチパターン

- Open mic

メール基礎

基本的なメールの流れ

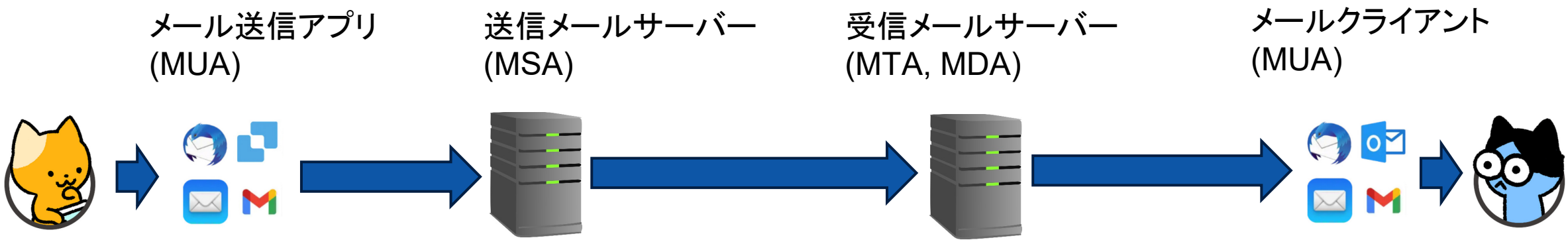
一般的なメールでは、送信者が MUA を使ってメッセージを送信して、
MSA と MTA を経由して、MDA に配送される。
最終的に、受信者が MUA を使ってメッセージを受信する。



MUA (Mail User Agent)	メールソフト、メールアプリ、Webメールなど
MSA (Mail Submission Agent)	Postfix、Amazon SES、Salesforce など
MTA (Mail Transport Agent)	Postfix、セキュリティゲートウェイなど
MDA (Mail Delivery Agent)	Dovecot、ISP メールサービスなど

基本的なメールの流れ

MUA -> MSA -> MTA -> MDA -> MUA の配送経路の中で付属情報としてヘッダー情報を付与する。差出人情報のなりすまし対策として、DKIM 電子署名や認証結果をヘッダーに付与する。



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)

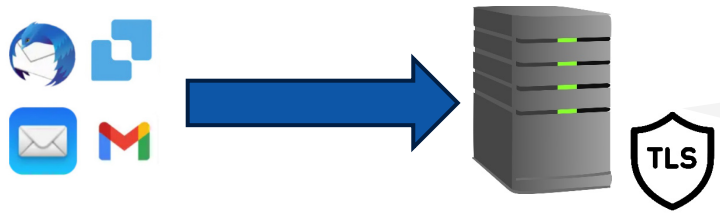
4. 差出人(From)
   宛先(To,Cc)
   件名(Subject)
   認証結果

Well-known ポート

メールシステムでは、いくつかの受付用ポート番号が割り当てられている。

メール送信アプリ
(MUA)

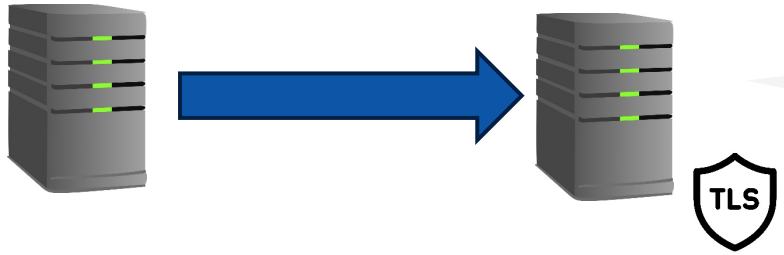
送信メールサーバー
(MSA)



TCP Port	用途
465	TLS 通信でのメール送信(SMTPS)
587	STARTTLS によるメール送信(SMTP)
25	非暗号通信でのメール送信(SMTP)

送信メールサーバー
(MSA)

受信メールサーバー
(MTA, MDA)



TCP Port	用途
25	STARTTLS によるメール送信(SMTP)

Well-known ポート

メールシステムでは、いくつかの受付用ポート番号が割り当てられている。

受信メールサーバー
(MTA, MDA)

メールクライアント
(MUA)

TCP Port	用途
110	非暗号通信でのメール取込(POP3)
143	非暗号通信でのメール操作(IMAP4)
993	TLS 通信でのメール取込(POP3S)
995	TLS 通信でのメール操作(IMAPS)

SMTP プロトコル例

S: 220 foo.com Simple Mail Transfer Service Ready
C: EHLO bar.com
S: 250-foo.com greets bar.com
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
C: MAIL FROM:<Smith@bar.com>
S: 250 OK
C: RCPT TO:<Jones@foo.com>
S: 250 OK
C: RCPT TO:<Green@foo.com>
S: 550 No such user here
C: RCPT TO:<Brown@foo.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: From: :<Smith@bar.com>
C: Blah blah blah...
C: ...etc. etc. etc.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel

メッセージ
(RFC5322)

https://tools.ietf.org/html/rfc5321#section-10 一部改

[補足] SMTP AUTH over STARTTLS 例

S: 220 foo.com Simple Mail Transfer Service Ready
C: EHLO bar.com
S: 250-foo.com greets bar.com
S: 250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250-STARTTLS
S: 250 HELP
C: STARTTLS
S: 220 2.0.0 Ready to start TLS

(TLS 1.3 connect)

C: AUTH PLAIN
S: 334
C: dXNlcj1rYXNlQHNvZnRlc3Q・・・5TN2F2Sy1IbmpRMDIwNgEB
S: 235 2.7.0 Accepted
.....

以降、TLS によって
通信が暗号化されている

https://tools.ietf.org/html/rfc5321#section-10 一部改

IMAP4 プロトコル例

S: * OK IMAP4rev1 Service Ready
C: a001 capability
S: * CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ STARTTLS AUTH=PLAIN
S: a001 OK CAPABILITY completed.
C: a002 STARTTLS
S: a002 OK STARTLS completed

(TLS 1.3 connect)

C: b001 login mrc secret
S: b001 OK LOGIN completed
C: b002 select inbox
S: * 18 EXISTS
S: * FLAGS (¥Answered ¥Flagged ¥Deleted ¥Seen ¥Draft)
S: * 2 RECENT
S: * OK [UNSEEN 17] Message 17 is the first unseen message
S: * OK [UIDVALIDITY 3857529045] UIDs valid
S: b002 OK [READ-WRITE] SELECT completed
.....
C: b006 logout
S: * BYE IMAP4rev1 server terminating connection
S: b006 OK LOGOUT completed

以降、TLS によって
通信が暗号化されている

https://tools.ietf.org/html/rfc3501#section-8 一部改

IMAP4 プロトコル例

C: a003 fetch 12 full
S: * 12 FETCH (FLAGS (¥Seen) INTERNALDATE "17-Jul-1996 02:44:25 -0700"
RFC822.SIZE 4286 ENVELOPE ("Wed, 17 Jul 1996 02:23:25 -0700 (PDT)"
"IMAP4rev1 WG mtg summary and minutes"
(("Terry Gray" NIL "gray" "cac.washington.edu"))
(("Terry Gray" NIL "gray" "cac.washington.edu"))
(("Terry Gray" NIL "gray" "cac.washington.edu"))
((NIL NIL "imap" "cac.washington.edu"))
((NIL NIL "minutes" "CNRI.Reston.VA.US")
("John Klensin" NIL "KLENSIN" "MIT.EDU")) NIL NIL
"<B27397-0100000@cac.washington.edu>")
BODY ("TEXT" "PLAIN" ("CHARSET" "US-ASCII") NIL NIL "7BIT" 3028
92))
S: a003 OK FETCH completed

https://tools.ietf.org/html/rfc3501#section-8 一部改

RFC5322 (rfc822)

赤字は必須ヘッダー

ヘッダー名	内容	使い方
Date	オリジナルの日付	MTA で存在性を確認 MUA で「送信日時」として表示
From	差出人情報	MTA で存在性を確認 MUA で「送信者」として表示
Message-ID	メッセージ識別子	MTA で存在性や一意性を確認
Received	配送経路情報	MSA, MTA によって付与 場合によっては、MTA でホップ数を確認 （通信暗号化の情報も含む）
Return-Path	リバースアドレス	MTA でエラーメールの返答先として利用
DKIM-Signature	DKIM 署名情報	MSA で真正性や改ざん検知のために付与
Authentication-Results	さまざまな認証結果	MTA, MUA でなりすましメール確認として利用

メール運用アップデート
- DMARC

古賀 勇

メール運用アップデート
- 証明書管理

古賀 勇

メール運用アップデート
- 大量送信

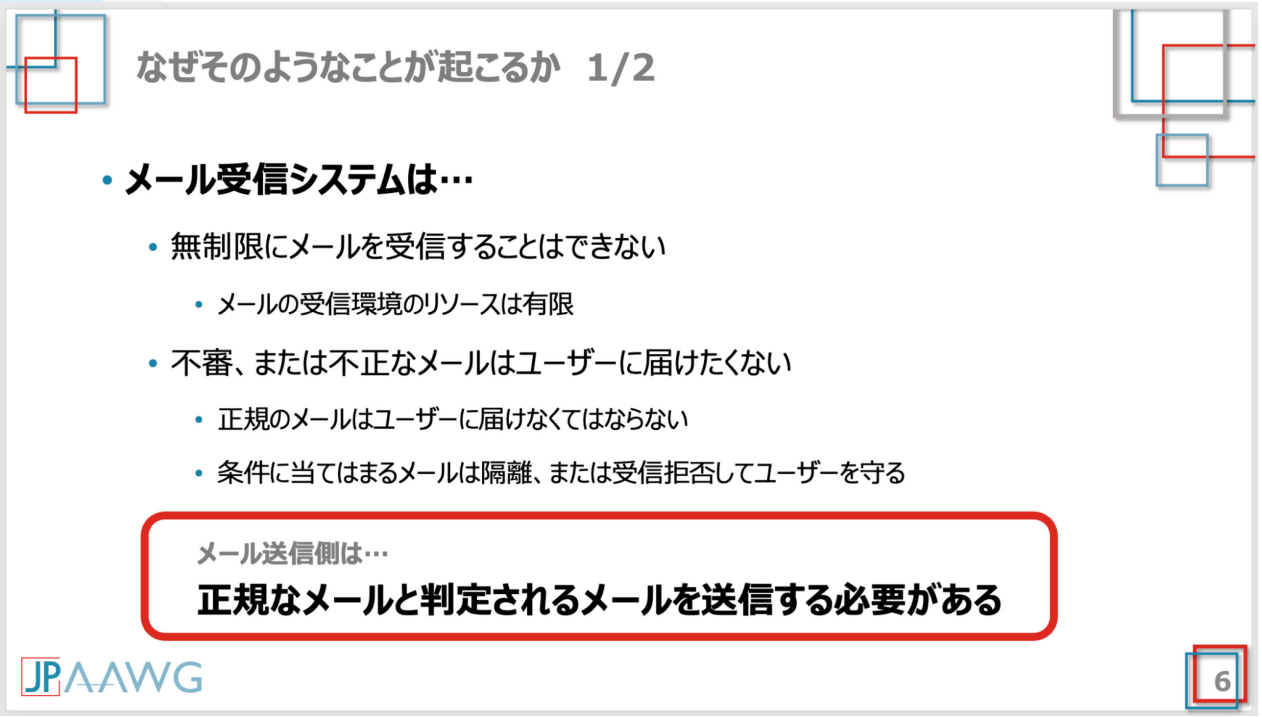
大量送信（バルク送信）のとある事例

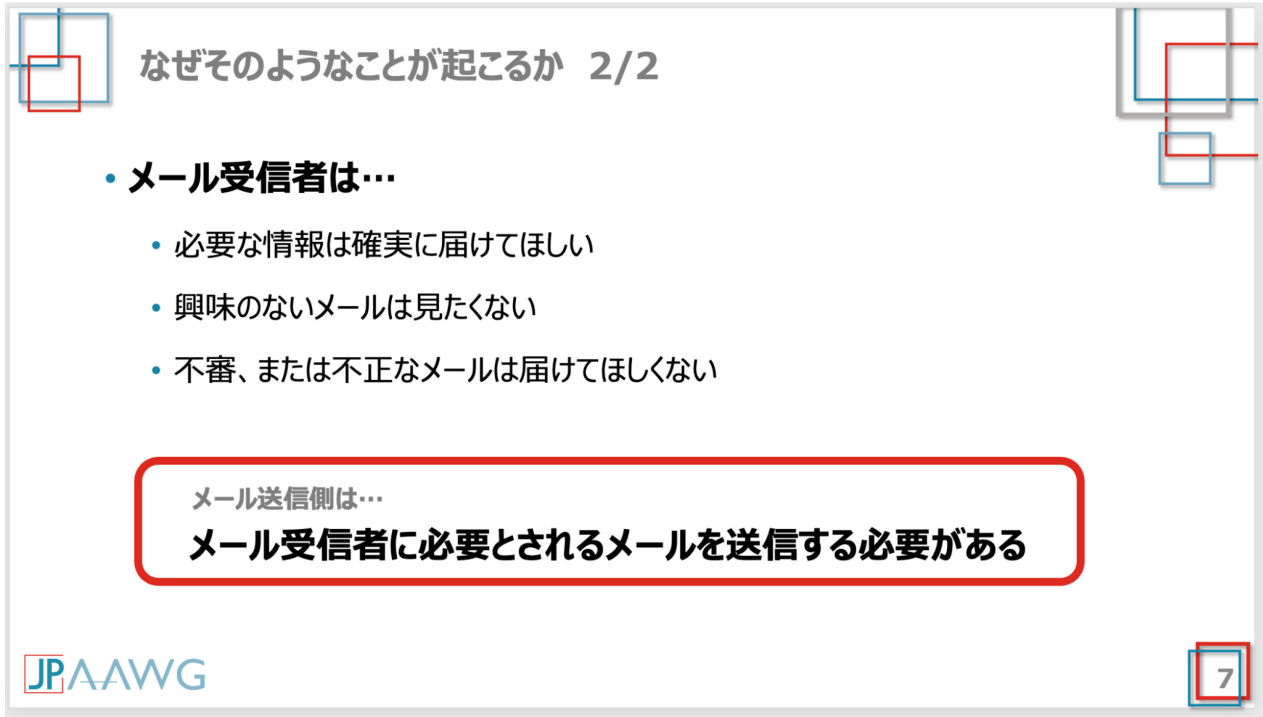
- 2025年10月、認証コードが届かないトラブルが大きく取り上げられた

時期	事業者	概要
2025.10	放送サービス関連	IDの新規登録開始直後、メール認証コードが届かない・大幅遅延の報告が相次ぎました。アプリ内お知らせで「登録集中でメール配信が遅れています」と謝罪。
2024.5	ネットバンキング	申し込みが殺到し、口座開設を申し込んだユーザーに届くはずの案内メールが遅延。
2024.1	地方自治体関連	高校入試のオンライン出願システムで、登録時に手続きメールが届かない問題が発生。出願期限直前に混乱。

https://xtech.nikkei.com/atcl/nxt/column/18/01157/110600146/
https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/041800013/101600083/
https://www.itmedia.co.jp/news/articles/2405/14/news167.html

[参考] JPAAWG (2025.2.27)



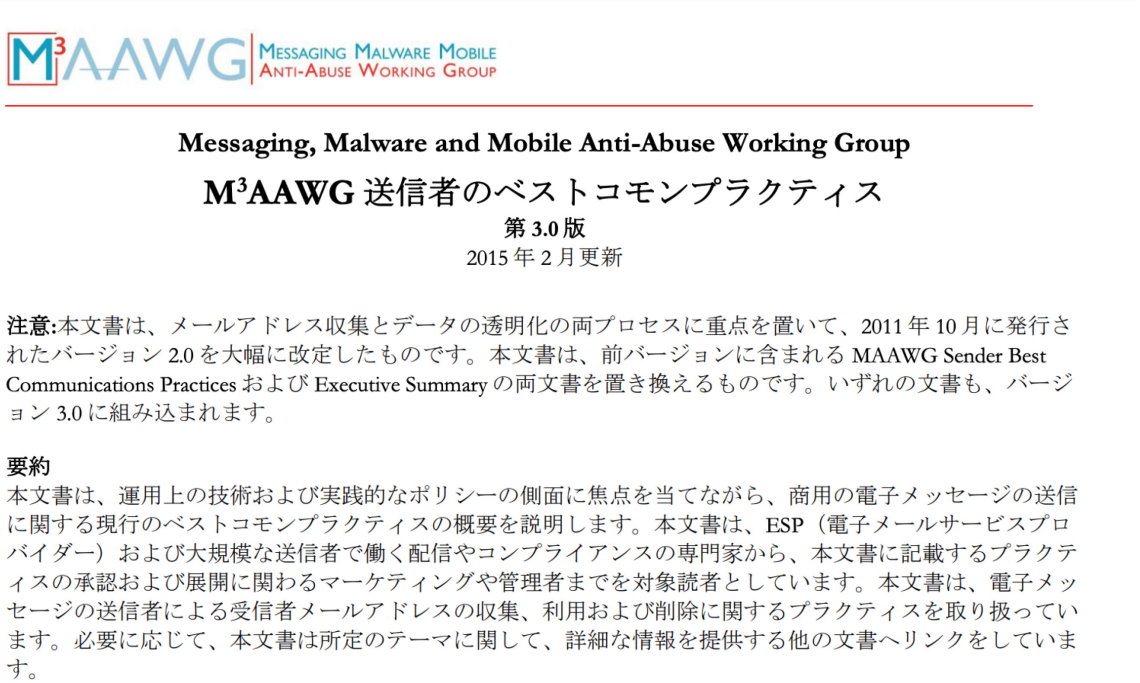


https://www.jpaawg.org/docs/event/2025training/20250227_jpaawg_a4.pdf

M³AAWG “Sender BCP”

M³AAWG(Messaging Malware Mobile Anti-Abuse Working Group)が公開している「メール送信に関するベストコモンプラクティス」

- 簡便なオプトアウト
- 通知メールと広告の区別
- 送信ドメイン認証の対応
- 送信サーバの適正化
- 宛先のクリーニング



M³AAWG Messaging Malware Mobile Anti-Abuse Working Group

Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG 送信者のベストコモンプラクティス

第 3.0 版

2015 年 2 月更新

注意:本文書は、メールアドレス収集とデータの透明化の両プロセスに重点を置いて、2011 年 10 月に発行されたバージョン 2.0 を大幅に改定したものです。本文書は、前バージョンに含まれる MAAWG Sender Best Communications Practices および Executive Summary の両文書を置き換えるものです。いずれの文書も、バージョン 3.0 に組み込まれます。

要約

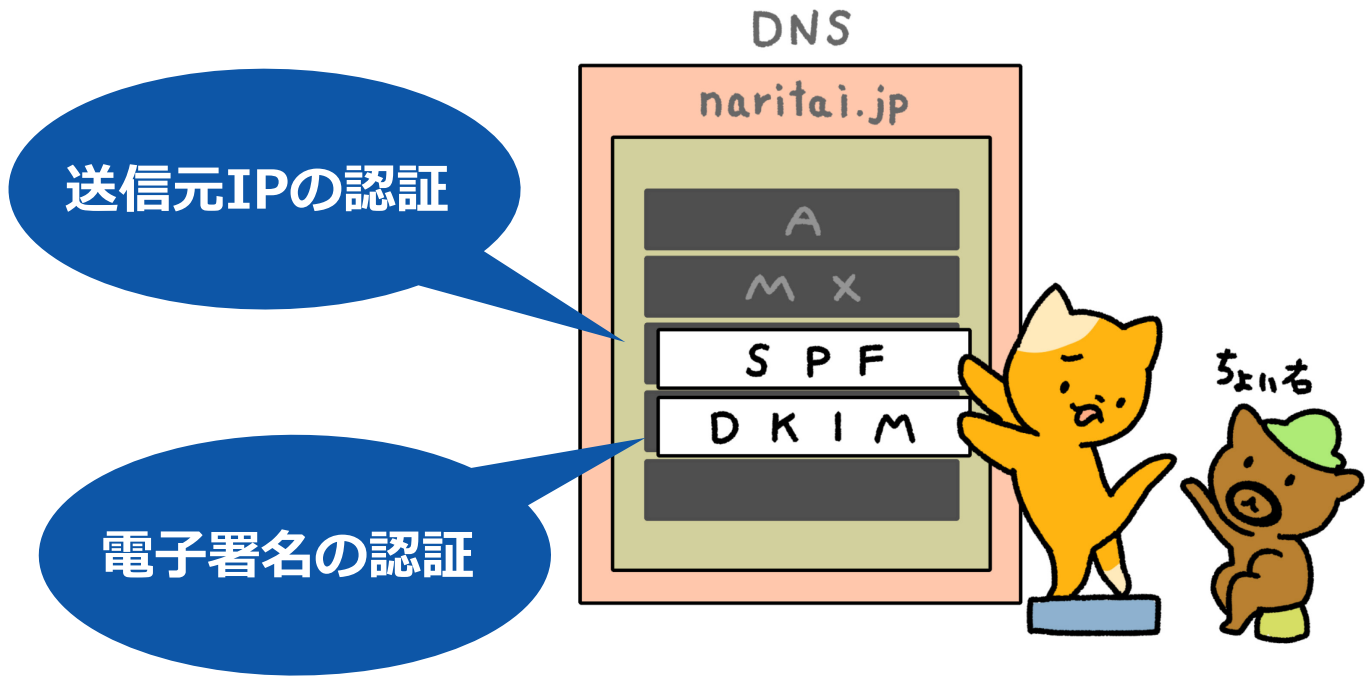
本文書は、運用上の技術および実践的なポリシーの側面に焦点を当てながら、商用の電子メッセージの送信に関する現行のベストコモンプラクティスの概要を説明します。本文書は、ESP（電子メールサービスプロバイダー）および大規模な送信者で働く配信やコンプライアンスの専門家から、本文書に記載するプラクティスの承認および展開に関わるマーケティングや管理者までを対象読者としています。本文書は、電子メッセージの送信者による受信者メールアドレスの収集、利用および削除に関するプラクティスを取り扱っています。必要に応じて、本文書は所定のテーマに関して、詳細な情報を提供する他の文書へリンクをしています。

https://www.m3aawg.org/sites/default/files/m3aawg_senders_bcp_ver3-2015-02-japanese.pdf

M³AAWG “Sender BCP”

M³AAWG(Messaging Malware Mobile Anti-Abuse Working Group)が公開している「メール送信に関するベストコモンプラクティス」

- 簡便なオプトアウト
- 通知メールと広告の区別
- 送信ドメイン認証の対応
- 送信サーバの適正化
- 宛先のクリーニング

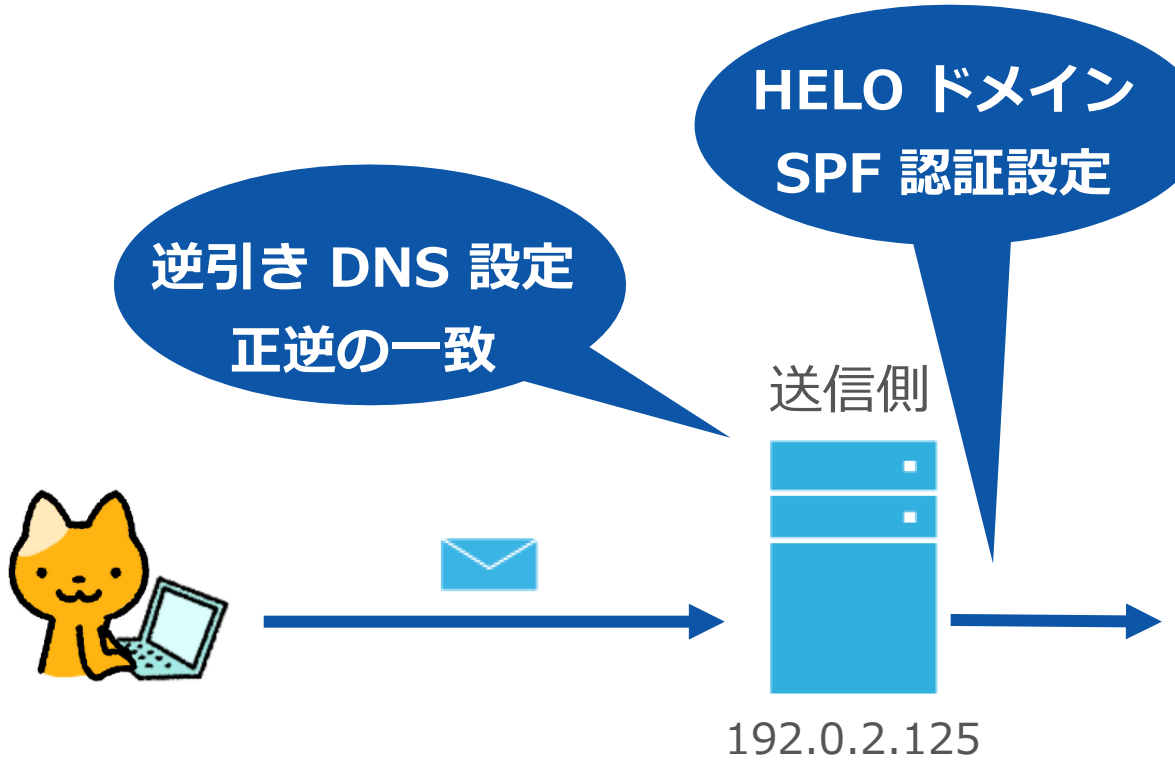


https://www.m3aawg.org/sites/default/files/m3aawg_senders_bcp_ver3-2015-02-japanese.pdf

M³AAWG “Sender BCP”

M³AAWG(Messaging Malware Mobile Anti-Abuse Working Group)が公開している「メール送信に関するベストコモンプラクティス」

- 簡便なオプトアウト
- 通知メールと広告の区別
- 送信ドメイン認証の対応
- 送信サーバの適正化
- 宛先のクリーニング



https://www.m3aawg.org/sites/default/files/m3aawg_senders_bcp_ver3-2015-02-japanese.pdf

M³AAWG “Sending Domains BCP”

M³AAWG(Messaging Malware Mobile Anti-Abuse Working Group)が公開している「送信ドメインのベストコモンプラクティス」

- 適切なサブドメイン
- ウォームアップ
- ランプアップ
- 送信ドメイン認証の対応
- DNS 設定

M³AAWG Messaging Malware Mobile Anti-Abuse Working Group

Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Sending Domains Best Common Practices

October 2019

The URL to reference this document is: https://www.m3aawg.org/SendingDomsBCP

Abstract

When preparing for bulk or transactional email sending, two items require special attention: outbound IP addresses, and the domain names to be used for these communications. For the latter, ESPs (Email Service Providers) go through this set-up process frequently and have to review the same readiness checklist each time. This process may involve individual client preferences and constraints, both legal and technical.

This document provides the best common practices related to choosing, setting and using a domain name when sending bulk or transactional emails. Senders, receivers and anti-spam organizations participated in writing and assessing these best practices.

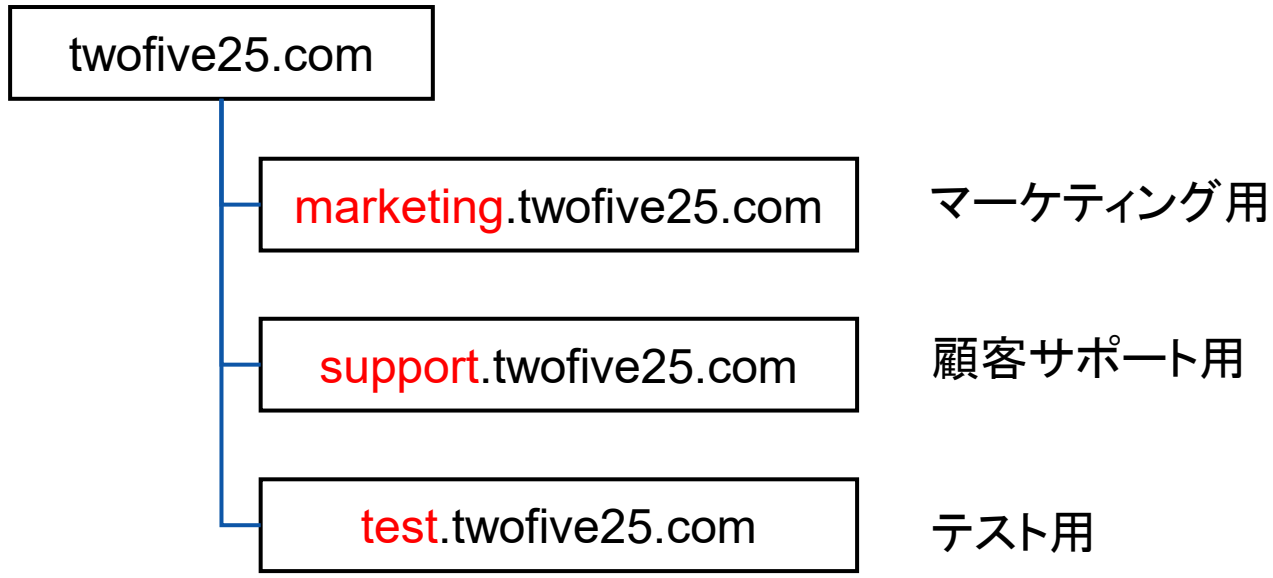
The intended audience is primarily senders—both traditional ESPs and other, smaller senders.

https://www.m3aawg.org/sites/default/files/m3aawg-sendingdomains10102019nk-2.pdf

M³AAWG “Sending Domains BCP”

M³AAWG(Messaging Malware Mobile Anti-Abuse Working Group) が公開している「送信ドメインのベストコモンプラクティス」

- 適切なサブドメイン
- ウォームアップ
- ランプアップ
- 送信ドメイン認証の対応
- DNS 設定



https://www.m3aawg.org/sites/default/files/m3aawg-sendingdomains10102019nk-2.pdf

M³AAWG “Sending Domains BCP”

M³AAWG(Messaging Malware Mobile Anti-Abuse Working Group)が公開している「送信ドメインのベストコモンプラクティス」

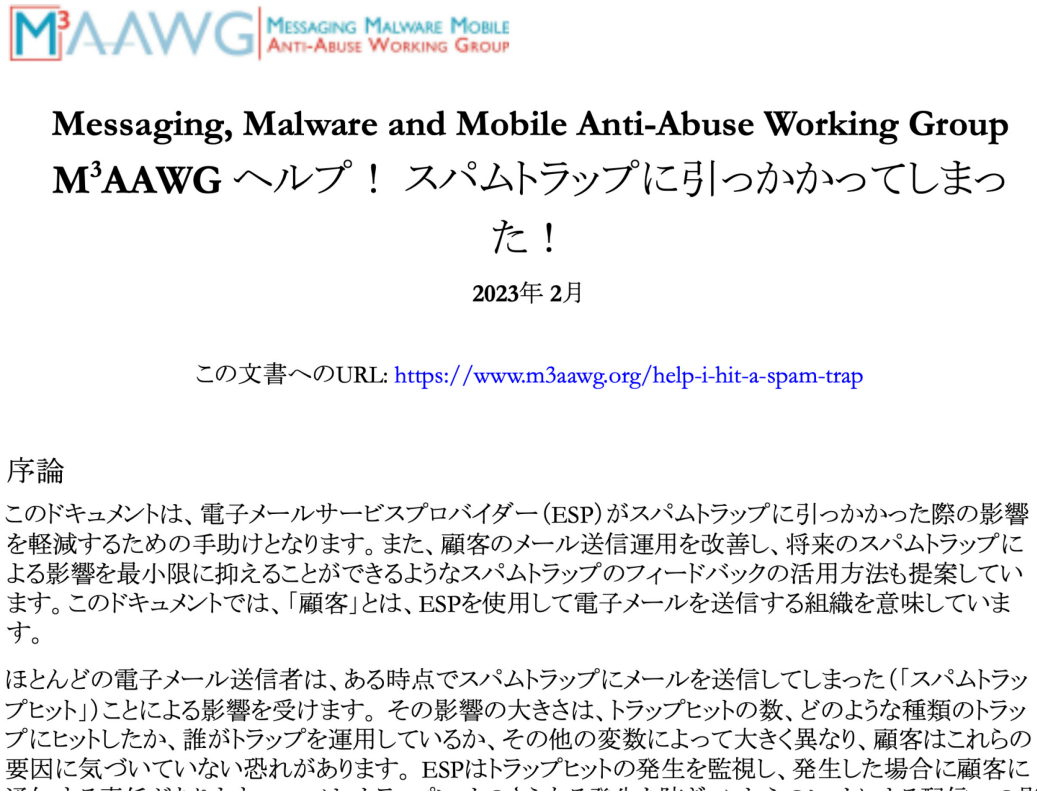
- 適切なサブドメイン
- ウォームアップ
- ランプアップ
- 送信ドメイン認証の対応
- DNS 設定

https://www.m3aawg.org/sites/default/files/m3aawg-sendingdomains10102019nk-2.pdf

[参考] M³AAWG “Help! I Hit A Spam Trap”

M³AAWG(Messaging Malware Mobile Anti-Abuse Working Group)が公開している「スパムトラップとその付き合い方」

- 顧客への通知や監査
- 宛先のクリーニング
- 悪意ある顧客の制限
- リスト収集の適正化
- 環境の分離



M³AAWG Messaging Malware Mobile Anti-Abuse Working Group

Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG ヘルプ！ スパムトラップに引っかかってしまった！

2023年 2月

この文書へのURL: https://www.m3aawg.org/help-i-hit-a-spam-trap

序論

このドキュメントは、電子メールサービスプロバイダー（ESP）がスパムトラップに引っかかった際の影響を軽減するための手助けとなります。また、顧客のメール送信運用を改善し、将来のスパムトラップによる影響を最小限に抑えることができるようなスパムトラップのフィードバックの活用方法も提案しています。このドキュメントでは、「顧客」とは、ESPを使用して電子メールを送信する組織を意味しています。

ほとんどの電子メール送信者は、ある時点でスパムトラップにメールを送信してしまった（「スパムトラップヒット」）ことによる影響を受けます。その影響の大きさは、トラップヒットの数、どのような種類のトラップにヒットしたか、誰がトラップを運用しているか、その他の変数によって大きく異なり、顧客はこれらの要因に気づいていない恐れがあります。ESPはトラップヒットの発生を監視し、発生した場合に顧客に

https://www.m3aawg.org/sites/default/files/help_i_hit_a_spam_trap.pdf

海外メールサービス送信者ガイドラインのまとめ

	Google	Yahoo Inc	Apple	Microsoft
ガイドライン対象サービス	Gmail	Yahoo.com, AOL など	iCloudメール	Microsoft 365
DMARC 対応	✅	✅	✅	✅
ARC 対応	メール転送の場合	ー	メール転送の場合	メール転送の場合
関連 RFC 準拠	5322, 8058	5321, 5322, 8058	5321, 5322	2505, 2920, 5321, 5322
送信元サーバの適切な設定	✅	✅	✅	✅
正規メールの可視化	BIMI 表示	BIMI 表示	BIMI 表示	ー
オプトイン	✅	✅	✅	ー
購読解除リンク	✅	✅	✅	✅
アドレスクリーニング	推奨	✅	✅	✅
その他	スパム率 0.3%以下 TLS 対応	スパム率 0.3%以下 CAN-SPAM 対応	広告メールを明確に分離	CAN-SPAM 対応 IPレピュテーションの維持

https://support.google.com/a/answer/81126
https://senders.yahooinc.com/best-practices/
https://support.apple.com/en-us/102322
https://learn.microsoft.com/en-us/defender-office-365/external-senders-policies-practices-guidelines
https://techcommunity.microsoft.com/blog/microsoftdefenderforoffice365blog/strengthening-email-ecosystem-outlook%e2%80%99s-new-requirements-for-high%e2%80%90volume-senders/4399730

海外メールサービス送信者ガイドラインのまとめ

	Google	Yahoo Inc	Apple	Microsoft
ガイドライン対象サービス	Gmail	Yahoo.com, AOL など	iCloudメール	Microsoft 365
DMARC 対応	✅	✅	✅	✅
ARC 対応	メール転送の場合	ー	メール転送の場合	メール転送の場合
関連 RFC 準拠	5322, 8058	5321, 5322, 8058	5321, 5322	2505, 2920, 5321, 5322
送信元サーバの適切な設定	✅	✅	✅	✅
正規メールの可視化	BIMI 表示	BIMI 表示	BIMI 表示	ー
オプトイン	✅	✅	✅	ー
購読解除リンク	✅	✅	✅	✅
アドレスクリーニング	推奨	✅	✅	✅
その他	スパム率 0.3%以下 TLS 対応	スパム率 0.3%以下 CAN-SPAM 対応	広告メールを明確に分離	CAN-SPAM 対応 IPレピュテーションの維持

https://support.google.com/a/answer/81126
https://senders.yahooinc.com/best-practices/
https://support.apple.com/en-us/102322
https://learn.microsoft.com/en-us/defender-office-365/external-senders-policies-practices-guidelines
https://techcommunity.microsoft.com/blog/microsoftdefenderforoffice365blog/strengthening-email-ecosystem-outlook%e2%80%99s-new-requirements-for-high%e2%80%90volume-senders/4399730

メール運用アンチパターン

メール運用で最低限押さえておくアンチパターン

- 大量メール送信のアンチパターン
- SMTP AUTH アンチパターン
- SPF / DKIM アンチパターン
- DMARC アンチパターン

大量メール送信のアンチパターン

- いきなり大規模送信を始める
- 専用 SaaS を利用しない
- 宛先のメンテナンスをしない

Sender BCP を意識した運用

SMTP AUTH のアンチパターン

- 通信の暗号化をしない
- 通信の暗号化を日和見暗号(Opportunistic)にする
- 自由に差出人を設定できてしまう

パスワードを平文や暗号しない通信でやり取りしない

SPF / DKIM のアンチパターン

- DKIM 鍵サイズが 1024 ビット
- DKIM ドメインが第三者ドメイン
- SPF レコードがメンテナンスされていない
- SPF レコードが広すぎる
- SPF RR を使っている

Auth BCP を確認しておかしな設定は見直そう

DMARC のアンチパターン

- DMARC レコードに rua タグを指定しない

自ドメインのなりすまし対策は宣言だけで満足しない

Open mic

本日のまとめ

- メール基礎
- メール運用アップデート – DMARC
- メール運用アップデート – 証明書管理
- メール運用アップデート – 大量送信
- メール運用アンチパターン