

メールサービスの運用開発こぼれ話 ARCとRFCの解釈における注意点



株式会社インターネットイニシアティブ
清水泰雅

Ongoing Innovation

自己紹介

自己紹介

清水泰雅

社会人経歴:

2022年: 新卒で某メーカーに就職

2024年: IIJに転職

業務:

メールサービスの開発業務

趣味:

ゲーム

ゲームコミュニティ用のウェブアプリの開発/保守



送信ドメイン認証について

送信ドメイン認証について

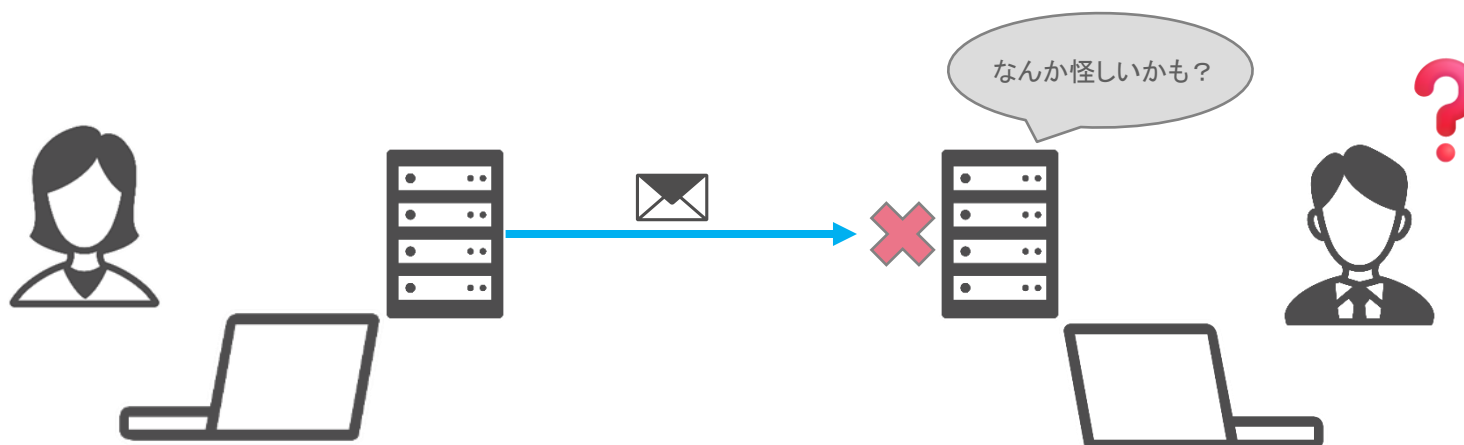
送信ドメイン認証はなぜ必要か

昔のメールは限られた良い人だけが使っていた

昔はなりすましメールの危険性は低かった
性善説によるプロトコル
現在もメールの枠組み自体に認証機能は無い

今は良い人も悪い人もみんなが使うサービスに

なりすましメールの詐欺によるビジネス
本当にそのメールが本人から来たのか受信者は不安
認証できてないメールは怖いので受け取りたくない
送信者は受け取ってもらうために送信ドメイン認証



送信ドメイン認証について

セキュアMX

内製でMTAを開発している

柔軟な機能拡張を担保するために独自にMTAを開発している
送信ドメイン認証も独自に開発している



- 2006年 4月 SPFがRFCになる
Category: Experimental
- 2006年10月 セキュアMXがSPFにした状態でサービス開始
- 2007年 5月 DKIMがRFCになる
Category: Standards Track
- 2009年 4月 セキュアMXがDKIMに対応
- 2014年 8月 セキュアMXがDMARCに対応
- 2015年 3月 DMARCがRFCになる
Category: Informational
- 2019年 3月 セキュアMXがARCに対応
- 2019年 7月 ARCがRFCになる
Category: Experimental

内製 MTA

- IIJ の積極的な開発方針を支えるには、ベンダ製 MTA は自由がなさすぎる
- ベンダ製 MTA で痛い目を見ている
 - 全体を委ねるのはリスクが大きすぎる
- アンチウイルスやアンチスパムエンジンには大抵組み込み用の製品がある
 - ライブラリ
 - daemon + ネットワーク API
- 莫大な開発コスト
- 楽しそう

18

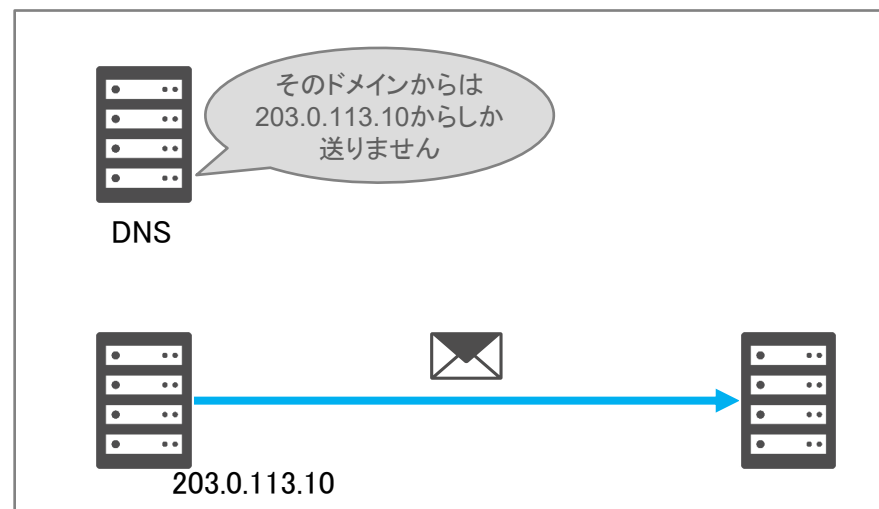
引用:
IIJ Technical NIGHT vol.7
Session3 : 高トランザクションシステムとしてのメールシステム
<https://eng-blog.ij.ad.jp/archives/3029>

送信ドメイン認証について

送信ドメイン認証技術の代表例

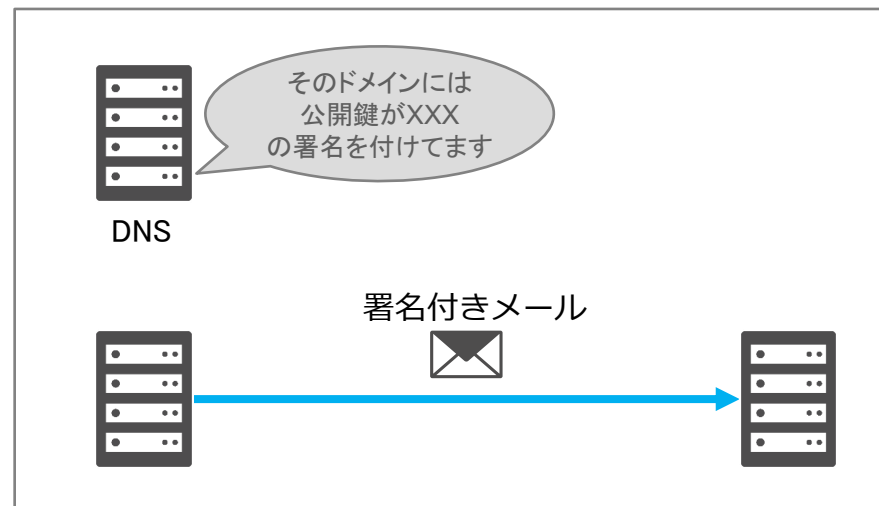
SPF

送信者のメールサーバのIPアドレスをDNSで宣言
違うIPアドレスからのメールは詐称とみなす



DKIM

公開鍵基盤による送信者の署名
公開鍵をDNSレコードで記載
本文や一部ヘッダに対して署名して受信者が検証



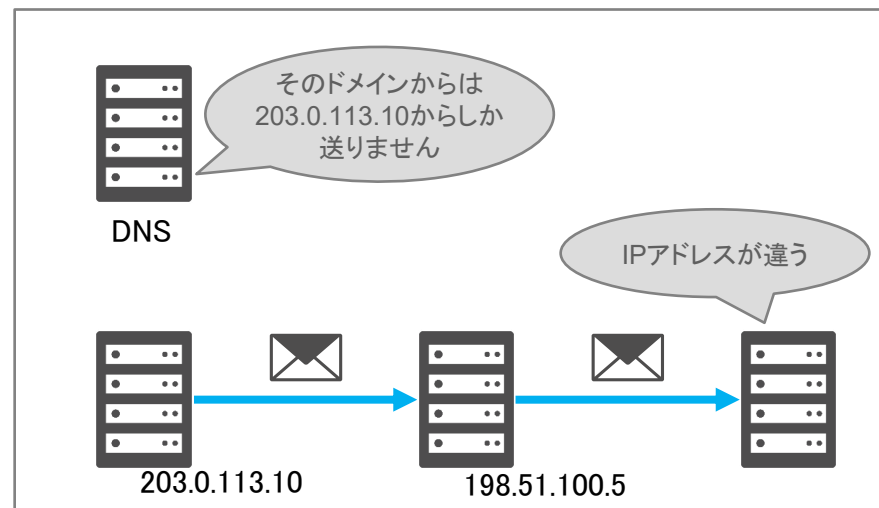
送信ドメイン認証について

送信ドメイン認証技術の代表例

SPF

送信者のメールサーバのIPアドレスをDNSで宣言
違うIPアドレスからのメールは詐称とみなす

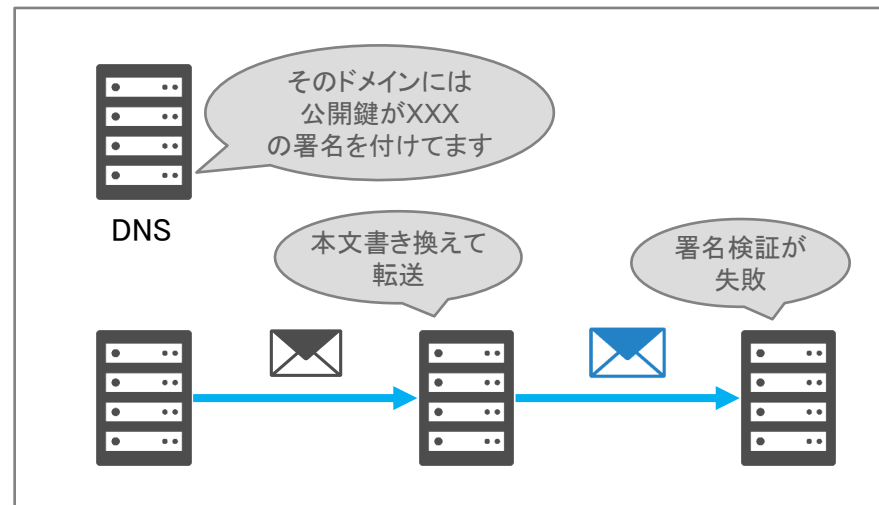
→転送すると受信者から見たIPアドレスが書き変わる
認証失敗！



DKIM

公開鍵基盤による送信者の署名
公開鍵をDNSレコードで記載
本文や一部ヘッダに対して署名して受信者が検証

→メール転送時に本文が書き変わると署名が壊れる
認証失敗！



メーリングリスト等でメール転送したときに
送信ドメイン認証が失敗する！

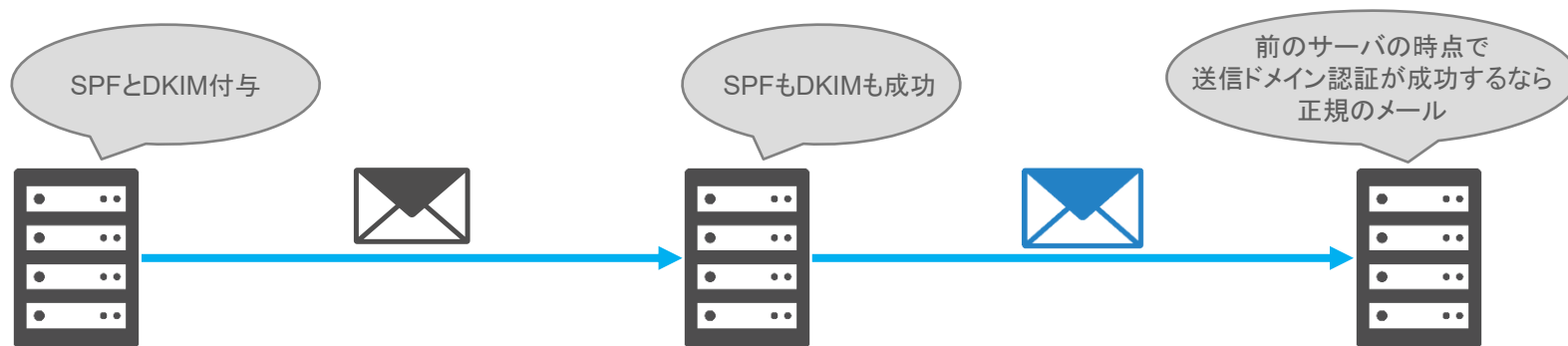
ARC

ARC

ARCとは

ARC: Authenticated Received Chain

メール転送時に認証結果に対して署名を付けて転送することで信頼の輪を作成
後段に送信ドメイン認証の結果を伝達する仕組み



ARC

ARCとは

ARCの用語

AAR(ARC-Authentication-Results)

転送するメールサーバが
メールを受信したときに検証結果を付与する
ヘッダフィールド
この結果を後段MTAに伝えるのが目的

AMS(ARC-Message-Signature)

転送するメールサーバが
メール本文や一部ヘッダを使用して
メールに対して署名した結果を付与する
ヘッダフィールド
隣同士のMTAの真正性を保証

AS(ARC-Seal)

転送するメールサーバが
ここまでの全てのARC関連のヘッダに対して
署名した結果を付与する
ヘッダフィールド
ARC全体の枠組みの真正性を保証

ARC-Seal: i=2;a=rsa-sha256;d=securemx.jp;s=arc20250414;t=1761288770;cv=pass;b=miXyJXkS416kp2Xyei8etEBcYUJPyQOn7rtc37IIakcPFoNEd7uILPsQOOm2orKg8AMYkeNbJfJQ
QMqD5gwuiwr9/JbFhVn+CUerucnx9gv2FWbrh6b4ApCQAOhRmRSwVqnISEN9cZ6+wgGD5RCNMrg
xLc5pLN0dnKUtdBD/I3yWC3Vh4+99z/NXJD0YqVklG17wNKAV00IGIaHqnHkGkCMH34QJaptzzMT
xiq3i02PMLqHbuGhmv89qeRJ/gbDtl+fRUYe/kvUYcME5g7XVXmLwcMaKIKI4OguZVtCHFk1+mR
+okHek/pUbWlurBVBV+E0fcqVjkporxLSV+6RHmAA==

ARC-Message-Signature: i=2;a=rsa-sha256;c=relaxed/relaxed;d=securemx.jp;h=
Content-Type:MIME-Version:Subject:Message-Id:To:From:Date:DKIM-Signature;s=
arc20250414;t=1761288770;x=1761893570;bh=YJWMysPI36audKpPjWIG/TOL/JVGuKuq1l
4/HEAjb8=;b=RIVg6c/iK3d7PbO/9dm8nsq49eLj1iMKQkMIR3jJ6/YDzk43TpR+05GctPsBDd
MnOGUudCdVj3PlfqNMywNImvoUhT7rqx3B7R+hn7jn9BNyRaUhpY69jkzy71fyjvrLu6CvV+FbN
O1pAf9vTpLoQOQ/b0/R08uVcKnGnA7Or4E4ZBkvJ7lwlSdK04TRpp6bZEu9WTKnt7FJc4LNI3RW
pFip8isJw5Pn1ZdBLw7uydxV+IEFH/88gEgxWy9CdT9Bz+to5pHYEK+XXlIt6zzmcccoU24LOfG
DvOtb/v33DEavMPebmWLIxQA0YzFKP43a7Z9jt2PcM37WgxyG79Ammw==

ARC-Authentication-Results: i=2; mx.securemx.jp; spf=hardfail
smtp.mailfrom=user001@example.com; dkim=pass
header.i=user001@example.com; dmarc=pass
header.from=example.com;
arc=pass header.oldest-pass=0 smtp.remote-ip=<IPアドレス>



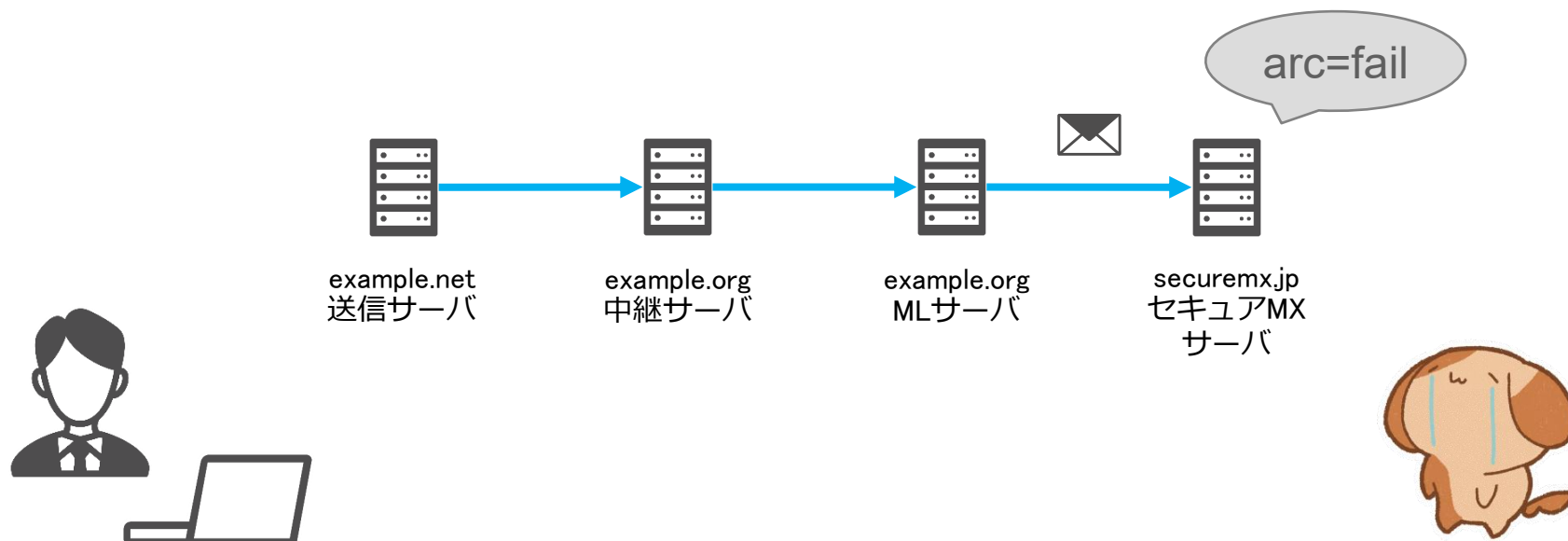
ARCのRFCを読み違えた事例 その1

ARCのRFCを読み違えた事例①

特定の外部メーリングリストでARCが失敗

相手(sender@example.net)が
mailing-list@example.org というセキュアMX上のメールアドレスを含む外部メーリングリスト宛にメールを送ると
セキュアMX側でARCがfail

他のメールサービスではARCが成功していた

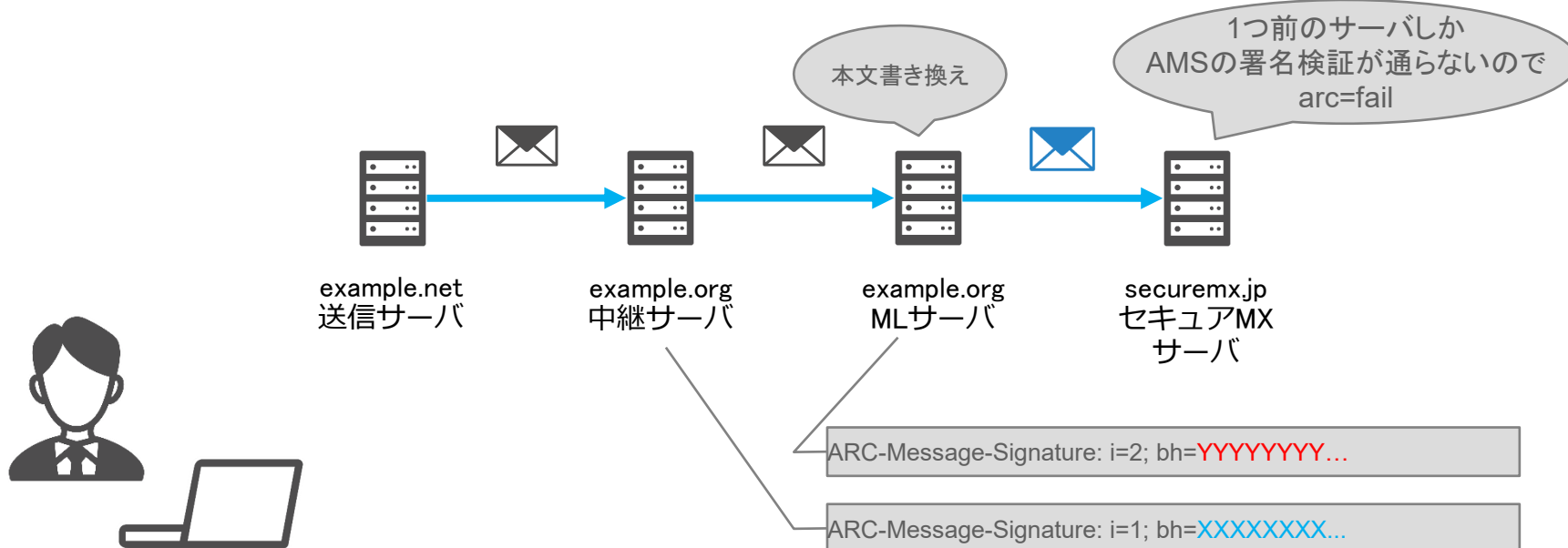


ARCのRFCを読み違えた事例①

特定の外部メーリングリストでARCが失敗

mailing-list@example.org ではメール本文を書き換えていた

セキュアMXで稼働しているMTAは全てのARC Message Signatureを検証していた



ARCのRFCを読み違えた事例①

特定の外部メーリングリストでARCが失敗

ARCでは最新のAMSのみ検証を行う

→ 途中で本文が改変されることを許容する思想

RFC8617 – 5.2 Validator Actions

4. Validate the AMS with the **greatest instance value (most recent)**.
If validation fails, then the Chain Validation Status is "fail",
and the algorithm stops here.

最新のAMSのみ検証

ARC-Message-Signature: i=2; bh=YYYYYYYY...

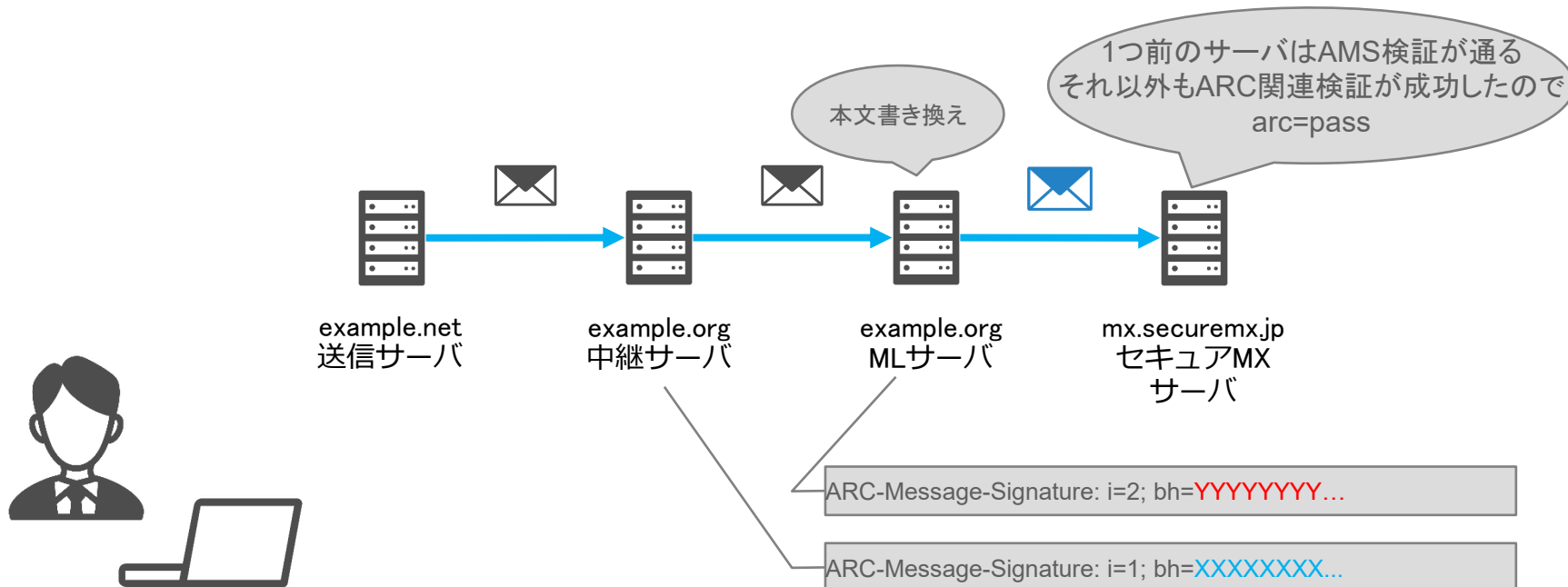
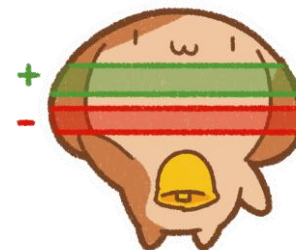
ARC-Message-Signature: i=1; bh=XXXXXXXX...



ARCのRFCを読み違えた事例①

特定の外部メーリングリストでARCが失敗

セキュアMXの挙動はRFC違反と判断
→修正

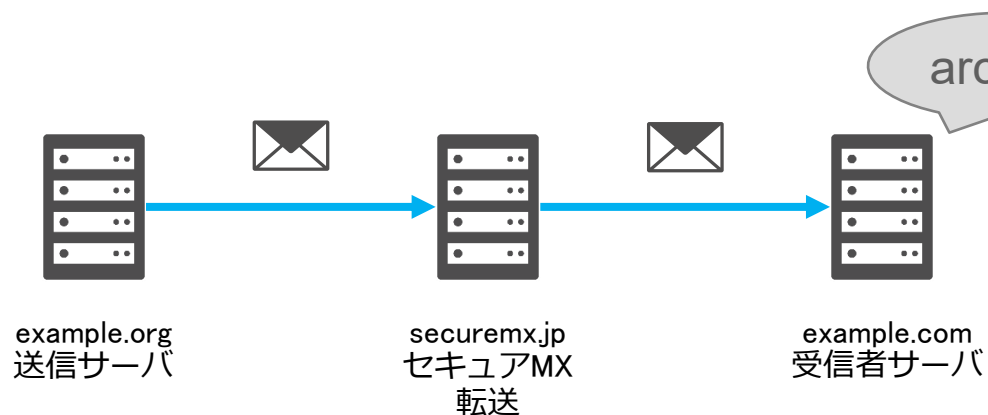


ARCのRFCを読み違えた事例 その2

ARCのRFCを読み違えた事例②

セキュアMXでメール転送するとARCが失敗

メールサービスAからセキュアMXを経由してメールサービスBへメールを転送すると
何故かARCが失敗してしまっていた



ARCのRFCを読み違えた事例

セキュアMXでメール転送するとARCが失敗

同名のヘッダが複数あった場合の処理

セキュアMXの仕様

同名のヘッダをAMSの署名に使う場合は

上から順番に

AMSに入れていた

①

～前略～

Resent-From: <user002@example.com>

～中略～

②

Resent-From: <user001@example.net>

～後略～



ARCのRFCを読み違えた事例②

セキュアMXでメール転送するとARCが失敗

同名のヘッダが複数あった場合の処理

RFCの仕様

同名のヘッダをAMSの署名に使う場合は

下から順番に

AMSに入れなければならない

RFC8617 – 4.1.2 ARC-Message-Signature (AMS)

The AMS header field has the same syntax and semantics as the DKIM-Signature field [[RFC6376](#)], with three (3) differences:

RFC6376 – 5.4.2 Signatures Involving Multiple Instance of a Field

Signers choosing to sign an existing header field that occurs more than once in the message (such as Received) MUST sign the physically last instance of that header field in the header block. Signers wishing to sign multiple instances of such a header field MUST include the header field name multiple times in the "h=" tag of the DKIM-Signature header field and MUST sign such header fields **in order from the bottom of the header field block to the top.**

セキュアMXの挙動はRFC違反
→修正



まとめ

まとめ

RFCの意図を理解しよう

- 時代によって意図は変わる
 - DKIMはそもそも本文書き換えを許していなかった
- トrendを追いながら意図を理解しつつRFCを読む習慣を付けるべき



ご清聴ありがとうございました

お問い合わせ先 IIJインフォメーションセンター
TEL : 03-5205-4466 (9 : 30~17 : 30 土/日/祝日除く)
info@ij.ad.jp

Ongoing Innovation

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。IIJ, Internet Initiative Japan は、株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。本文中では™、®マークは表示していません。©Internet Initiative Japan Inc. All rights reserved. 本サービスの仕様、及び本書に記載されている事柄は、将来予告なしに変更することがあります。