

メールサービスの運用開発こぼれ話 正しい送信ドメイン認証規格を目指して歩んだ道



株式会社インターネットイニシアティブ
山下 隼平

Ongoing Innovation

自己紹介

自己紹介

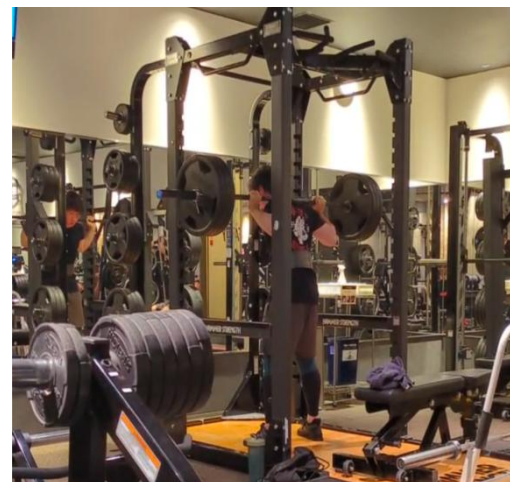
山下 隼平

お仕事

メールサービスの開発業務に従事

趣味

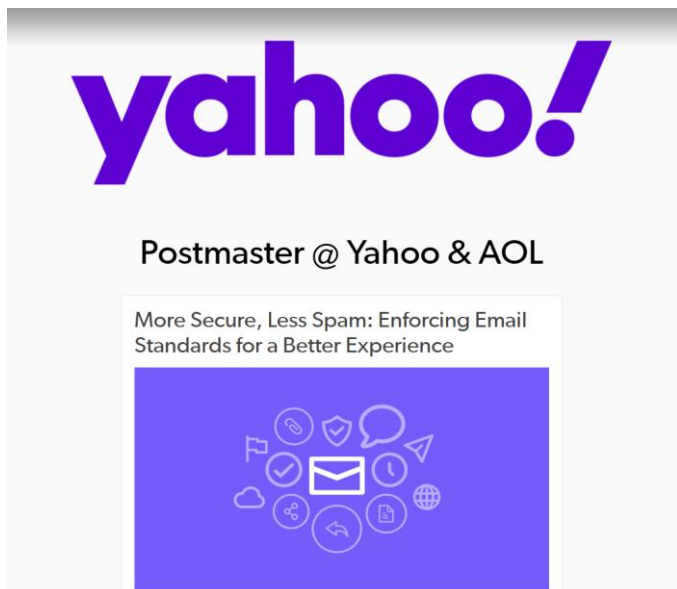
- 筋トレ
 - スクワット170kg、ベンチプレス105kg、デッドリフト190kg
- ボルダリング
 - b-pump 秋葉原に生息



あらすじ

あらすじ

2023年にGoogle、Yahooが送信ドメイン認証必須化発表



<https://blog.postmaster.yahooinc.com/post/730172167494483968/more-secure-less-spam>

メール送信者のガイドライン

この記事のガイドラインに沿った対応を行うことで、個人用 Gmail アカウントにメールが正常に送信、配信されるようになります。2024 年以降は、Gmail 個人用アカウントにメールを送信する場合に、こちらに記載の要件を満たす必要があります。個人用 Gmail アカウントとは、末尾が @gmail.com または @googlemail.com のアカウントを指します。

送信者の要件に関する最新情報については、[メール送信者のガイドラインに関するよくある質問](#)をご覧ください。

Google Workspace の送信者: Google Workspace を使用して大量のメールを送信する場合は、[Gmail での迷惑メールや不正行為に関する規定](#) [☑](#) をご確認ください。この規定は [Google Workspace 利用規定](#) [☑](#) の一部です。

<https://support.google.com/a/answer/81126?sjid=4803819380708520790-NC>

発表を受けIIJでは元々対応していたが、改めて他社との送信ドメイン認証の互換性の確認を開始

あらすじ

何かおかしい(arc=failが発生!)



Gmail → SMX(転送) → Live!mail(M社)でやってみたんですが、Live!mailで arc=fail になりますね。
Gmail の DKIM で救われて dmarc=pass になっている感がある。なんでだろう (後で調べる)

```
ARC-Seal: i=2; a=rsa-sha256; s=arcselector9901; d=██████████; cv=fail; b=nf/fD(略) ARC-Message-
Signature: i=2; a=rsa-sha256; c=relaxed/relaxed; d=██████████; s=arcselector9901;
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:
██████████; bh=1V02(略)
ARC-Authentication-Results: i=2; mx.██████████ 1; spf=softfail (sender ip
is 210.130.202.147) smtp.rcpttodomain=live.jp smtp.mailfrom=gmail.com;
dmarc=pass (p=none sp=quarantine pct=100) action=none header.from=gmail.com;
dkim=pass (signature was verified) header.d=gmail.com; arc=fail (47) ARC-Seal: i=1;a=rsa-
sha256;d=securemx.jp;s=arc20190303;t=1700484843;cv=none;b=a9qF(略) ARC-Message-Signature: i=1;a=rsa-
sha256;c=relaxed/simple;d=securemx.jp;h=
DKIM-Signature:MIME-Version:From:Date:Message-
ID:Subject:To:Content-Type;s=
arc20190303;t=1700484843;x=1701089643;bh=1V02f86F7zmLwQuYtpfZn7iDsSww3dH430
g90KLOV1s;byNzP9An(略) ARC-Authentication-
Results: i=1; mx.securemx.jp; spf=pass smtp.mailfrom=██████████@gmail.com; dkim=pass
header.i=@gmail.com; dmarc=pass header.from=gmail.com; x-country-code=IE;
arc=none smtp.remote-ip="2a00:1450:4864:20::632"
```



おお！？なんか違和感ありますね

この検体ですが、M社(Vade:arc=none) -> officemail(arc=pass) -> M社(IIJ:arc=fail)です
最後はarc=failになってるからM社側の動きなのかなとも思いつつ分からない(これだけ見るとIIJ側の実装が
まずい可能性も現時点では捨てられないが・・・)。

興味ですがlive -> SMX(転送) -> gmailだとどうなりますか(IIJの後ろでarcがどうなるかを知りたいところ)

あらすじ

何かおかしい(arc=failが発生!)

一部抜粋

```
ARC-Authentication-Results: i=2; mx.〇〇.com 1; spf=fail (sender ip is ...)  
smtp.rcpttodomain=iijsmxstg.onmicrosoft.com  
smtp.mailfrom=iij.ad.jp; dmarc=pass (p=reject sp=reject pct=100)  
action=none  
header.from=iij.ad.jp; dkim=pass (signature was verified)  
header.d=iij.ad.jp;  
arc=fail (47)
```



あらすじ

詳細な調査を始める

原因の切り分けのためにM社以外のプロバイダでも検証を行った



転送経路	i=1	i=2	i=3	ARC結果
IJ office → SecureMX → Google → M社	IJ-office	SecureMX	Google	pass
IJ office → SecureMX → Fastmail	IJ-office	SecureMX	-	pass
IJ office → SecureMX → M社	IJ-office	SecureMX	-	fail

IJ office: IJ社内で業務利用 しているメールシステム。SecureMXとは異なるメールシステム

SecureMX: IJセキュアMXサービス

Fastmail: オーストラリアのメールプロバイダ

あらすじ

詳細な調査を始める

RFC 6376およびRFC 8617準拠のPythonライブラリ「dkimpy」を用いて署名検証

```
>>> import dkim
>>> dkim.ARC(open("iijsmx-forward-365-arc-fail-
20231127.eml", "br").read()).verify()
(b'fail', [{ 'instance': ..., ...; spf=... smtp.rcpttodomain=...
smtp.mailfrom=...; dmarc=... action=... header.from=...; dkim=...
header.d=...; arc=fail (47)¥r¥n', 'ams-domain': ..., 'ams-selector': ...,
'ams-valid': True, 'as-domain': ..., 'as-selector': ..., 'cv': ..., 'as-
valid': ...}], "x= ...")
```

ARC-Message-Signature (AMS) のverifyに成功することを確認



あらすじ

詳細な調査を始める

RFC 6376およびRFC 8617準拠のPythonライブラリ「dkimpy」を用いて署名検証

```
>>> import dkim
>>> dkim.ARC(open("iijsmx-forward-365-arc-fail-
20231127.eml", "br").read()).verify()
(b'fail', [{ 'instance': ..., ...; spf=... smtp.rcpttodomain=...
smtp.mailfrom=...; dmarc=... action=... header.from=...; dkim=...
header.d=...; arc=fail (47)¥r¥n', 'ams-domain': ..., 'ams-selector': ...,
'ams-valid': True, 'as-domain': ..., 'as-selector': ..., 'cv': ..., 'as-
valid': ...}], "x= ...")
```

ARC-Message-Signature (AMS) のverifyに成功することを確認

M社側の不具合疑惑が出たため調査依頼



調査依頼(1回目)

調査依頼(1回目)

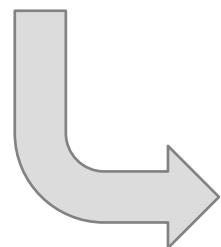
IIJ側で調査した内容を基にM社側でも調査を行うよう依頼

調査依頼(1回目)

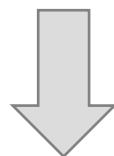
IIJ側で調査した内容を基にM社側でも調査を行うよう依頼

M社からの回答

ARC 署名の検証を行った際のハッシュ値が一致しないため
arc = failとなっており、署名を行った時点から改変され
た可能性がある



IIJ側の設備の問題の可能性を指摘された



IIJでは正規化のアルゴリズムにsimpleアルゴリズムを使用
M社では relaxed アルゴリズムを使用していた

正規化

正規化とは、メールの内容を一定の形式に変換する処理

- ARCはDKIMの標準であるRFC 6376に準拠
- RFC 6376では、ヘッダーと本文の正規化アルゴリズムとして「simple」と「relaxed」の2種類が定義されている

To satisfy all requirements, two canonicalization algorithms are defined for each of the header and the body: a "simple" algorithm that tolerates almost no modification and a "relaxed" algorithm that tolerates common modifications such as whitespace replacement and header field line rewrapping.

RFC 6376 3.4. Canonicalizationより抜粋



simpleアルゴリズムとrelaxedアルゴリズムの違い

simpleアルゴリズムとrelaxedアルゴリズムの違いとは？

- simpleアルゴリズムではほとんど変更を許容しない
- relaxedアルゴリズムでは空白の置換やヘッダーフィールドの行の折り返しなど、一般的な変更を許容

To satisfy all requirements, two canonicalization algorithms are defined for each of the header and the body: a "simple" algorithm that tolerates almost no modification and a "relaxed" algorithm that tolerates common modifications such as whitespace replacement and header field line rewrapping.

RFC 6376 3.4. Canonicalizationより抜粋



調査依頼した結果

relaxedアルゴリズムに変更することで不具合解消する可能性があると考え、SecureMX側もrelaxedアルゴリズムを使用するように変更



relaxedアルゴリズムに変更した結果…

relaxedアルゴリズムに変更した結果…

直らず…



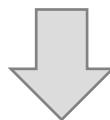
調査依頼(2度目)

前回とは別の切り口で検証

IIJ側の修正後にも不具合が再現したため、再度問い合わせのため検証を再開



他プロバイダへの転送と並行して、メールヘッダーの中の値をより詳細に確認



本文が空であるメールとテキストがあるメールを検体として検証を行ったところ、本文が空の場合bhタグのハッシュ値がIIJ側とM社側で異なっていた

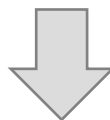


前回とは別の切り口で検証

IIJ側の修正後にも不具合が再現したため、再度問い合わせのため検証を再開



他プロバイダへの転送と並行して、メールヘッダーの中の値をより詳細に確認



本文が空であるメールとテキストがあるメールを検体として検証を行ったところ、**本文が空の場合bhタグのハッシュ値がIIJ側とM社側で異なっていた**



実際のbodyのハッシュ値(抜粋)

本文にテキストがあるメールのbhタグのハッシュ値

```
ARC-Message-Signature:i=3;d=M社;bh=KXMY6AzIdALIOzgkBat5CPcMk0Vqq3IozVvMgC0v4D0=;...
```

```
ARC-Message-Signature:i=2;d=securemx.jp;...;bh=KXMY6AzIdALIOzgkBat5CPcMk0Vqq3IozVvMgC0v4D0=;...
```

```
ARC-Message-Signature:i=1;d=securemx.jp;...;bh=KXMY6AzIdALIOzgkBat5CPcMk0Vqq3IozVvMgC0v4D0=;...
```



実際のbodyのハッシュ値(抜粋)

本文が空のメールのbhタグのハッシュ値

ARC-Message-Signature:i=3;d=M社;bh=47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=;...

ARC-Message-Signature:i=2;d=securemx.jp;...;bh=frcCV1k9oG9oKj3dpUqdJg1PxRT2RSN/XKdLCPjaYaY=;...

ARC-Message-Signature: i=1;d=securemx.jp;...;bh=frcCV1k9oG9oKj3dpUqdJg1PxRT2RSN/XKdLCPjaYaY=;...



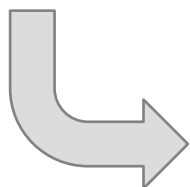
検証した結果を基に再調査依頼

- RFC 6376のセクション3.4.4では、relaxedアルゴリズムにおいても**末尾の改行は除去してはならない**と記述
- 一方、M社では末尾改行を除いた状態でハッシュ値を計算していたため、bhタグの値が一致しなかった

a. Reduce whitespace:

- * Ignore all whitespace at the end of lines. Implementations MUST NOT remove the CRLF at the end of the line.
- * Reduce all sequences of WSP within a line to a single SP character.

RFC 6376 3.4.4. The “relaxed” Body Canonicalization Algorithmより抜粋



検証結果を基に再度調査依頼



無事不具合であることを認めてもらえた

M社側の不具合であると認められ、不具合の修正を行うことも言ってもらえた



不具合の修正はしましたか？

最初の問い合わせから**2年経過**したが、まだ不具合再現...



終わりに

終わりに

- 無事不具合を認めてもらえてよかった
 - サポートはこじ開けるもの
- ARCはあまり普及していないが、正しい送信ドメイン認証規格に修正していく活動は大切
- IJではこれからも正しい送信ドメイン認証規格にする作業を行なっていく





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@iij.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。