メールドメイン認証を実装してみた

2023 年 5 月 19 日
ENOG 78 Meeting
上 越 市 ミ ュ ゼ 雪 小 町

Masato Nakakura
masato.nakakura@global-netcore.jp
masato.nakakura@nkkr.jp

自己紹介

GLOBAL NET CORE

中　倉　雅　人

なかくら　まさと

ENOGは昨年の新潟で初参加し、
柏崎 ⇒ 長岡 ⇒ 三条 と参加してきて、
今回で１年経過しました！

以前、自宅サーバを構築して
いたものの廃止してしまったため、
あらたにVPS上にメールサーバを構築してメール送信ドメイン認証に対応させましたので、そのあたりのお話をまとめてみました！

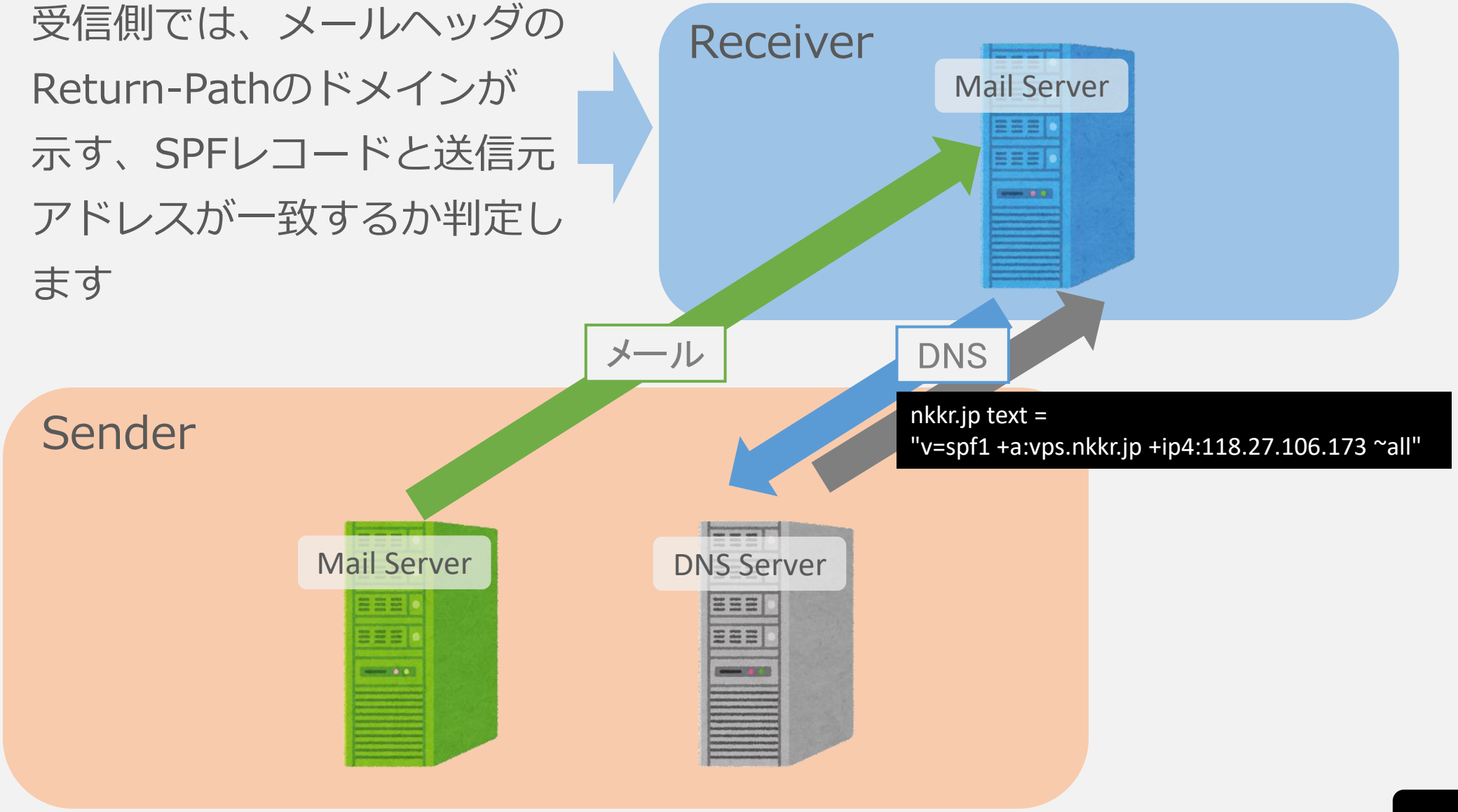
目次

SPF とは

SPF(Sender Policy Framework)は、
メールの送信ドメイン認証のひとつで、
メールが正規のサーバ（＝そのドメインからの送信が許可されているサーバ）
から送信されているのかどうかをアドレスベースで判断する仕組みです。

SPF のおおまかな流れ

受信側では、メールヘッダのReturn-Pathのドメインが示す、SPFレコードと送信元アドレスが一致するか判定します



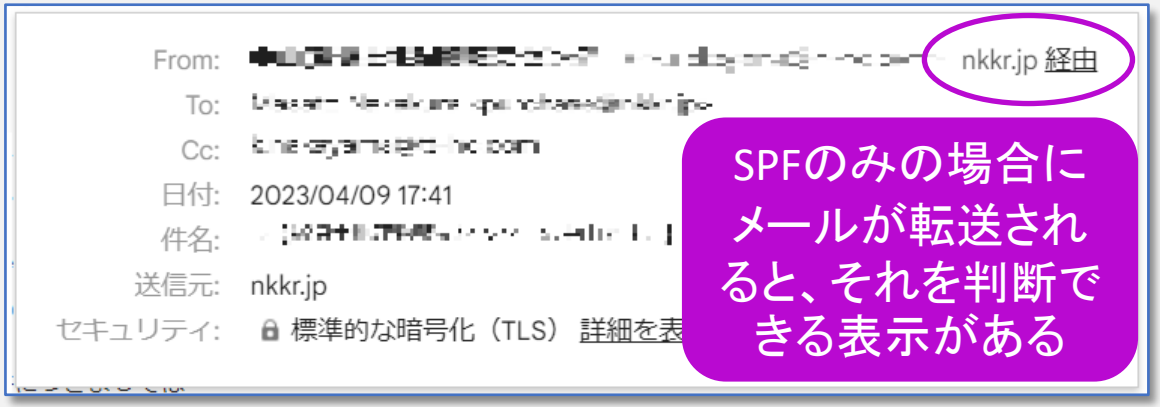
SPF の特徴

```
nkkr.jp text =
"v=spf1 +a:vps.nkkr.jp +ip4:118.27.106.173 ~all"
```

v : (SPFバージョン)
+a:～(許可ドメイン名)▶+ip4:～(許可IPアドレス)▶~all (soft fail)

Return-Pathのドメインに
TXTレコードを
問い合わせすると
SPFレコードが取得できます

SPFは、アドレス(DNS応答)によってメール送信元の正当性を保証することはできるが、メールの改ざんを検知することはできず、メール内容の正当性を保証することはできない。



DKIM とは

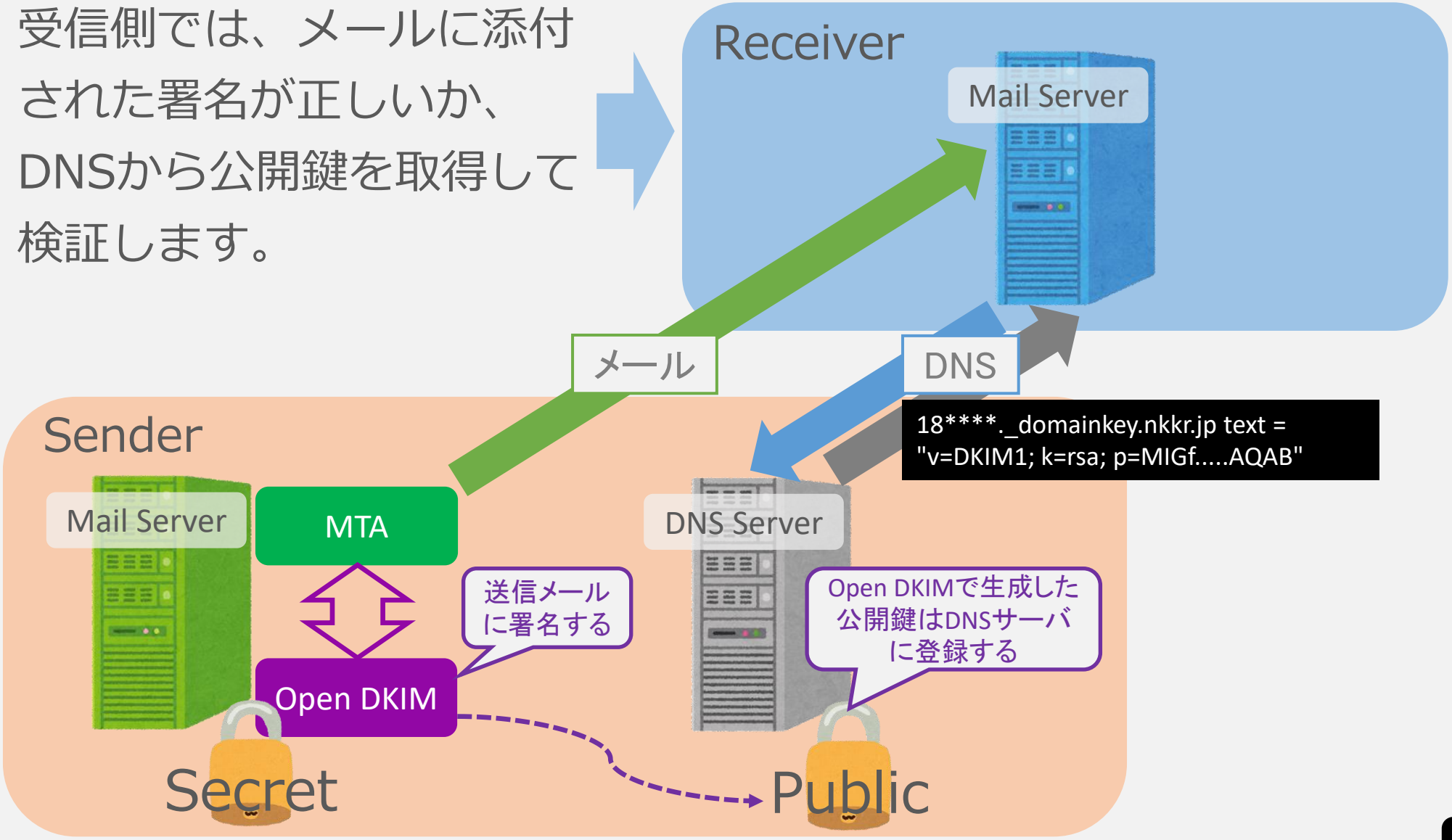
DKIM(DomainKeys Identified Mail)は、特定のドメインから送信されたメールを検証することで第三者によってメールの内容が改ざんされていないことを確認できる仕組みです。

検証方法としては、送信時にデジタル署名をメールに追加します。

そして、メールが到着すると受信者は公開鍵を、DNSサーバーから取得し、デジタル署名を検証してメール内容の正当性を確認します。

DKIM のおおまかな流れ

受信側では、メールに添付された署名が正しいか、DNSから公開鍵を取得して検証します。



DKIM の特徴

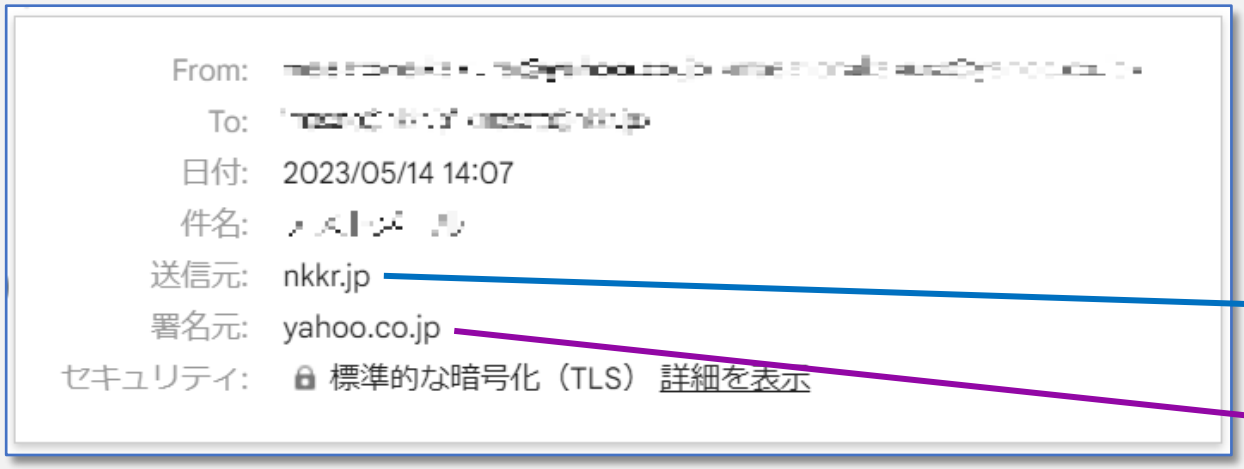
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt;
c=relaxed/relaxed; t=1684040871;
s=yj20******; d=yahoo.co.jp;
h=Date:From:To:Message-ID:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding:References;
bh=vBt0..（本文のハッシュ）..;
b=Jq+B..（メール全体の署名）..

メールヘッダにある DKIM-Signature の
セレクタ名(s=) とドメイン名(d=)
から以下のように、DNSに問合せすると
公開鍵が取得できる

yj20***._domainkey.yahoo.co.jp

yj20***._domainkey.yahoo.co.jp text =
"v=DKIM1; g=*; k=rsa; p=MIGf.... AQAB"

yj20*** : セレクタ名
v : (DKIMバージョン)
k : (キータイプ
p : (公開鍵)



メールが、どこかで転送されたとしても

署名元（送信元）とメール内容を検証できるので、正当性を確認できる

DKIM -ADSPレコード

ADSPレコードは、受信側でDKIMの認証結果をどのように扱ってほしいかを示すためのレコードです。
dkim=の値は「all」「unknown」「discardable」のいずれかを設定します。

```
_adsp._domainkey.＜ドメイン名＞ TXT =
"dkim=unknown"
```

なお、discardableやallを公開すると、署名して送信したメールが配送経路において再署名されるケース（メーリングリストへの投稿等）や、第三者にメールの送信を委託する場合などにおいて、受信側に厳しい対応をとられる可能性が考えられる。そのような状況を考慮する必要のあるメールを送信する場合、discardableやallの公開については十分に注意が必要である。

▲ （引用元）DKIM (Domainkeys Identified Mail)｜迷惑メール対策委員会

Gmailなどで、ADSPレコードが設定されているか参照してみたが設定されていないようだったので、今回は設定しなかった。

DMARC とは

DMARC (Domain-based Message Authentication, Reporting, and Conformance) は、SPF と DKIM の両者を利用したメールのドメイン認証を補強する技術です。

SPFおよびDKIMを用いて送信元ドメインを認証して、認証失敗したときの処理は受信者の判断に任せられます。

DMARCは、認証失敗した場合のメール処理ポリシーを送信者がDNS上で表明する仕組みです。

DMARC の導入

送信側での、DMARC導入は簡単で、
SPF と DKIM が正常に動作している
メールサーバ（ドメイン）であれば
DNSにDMARCポリシーレコードを定義
するだけで導入できる。

DMARC の導入

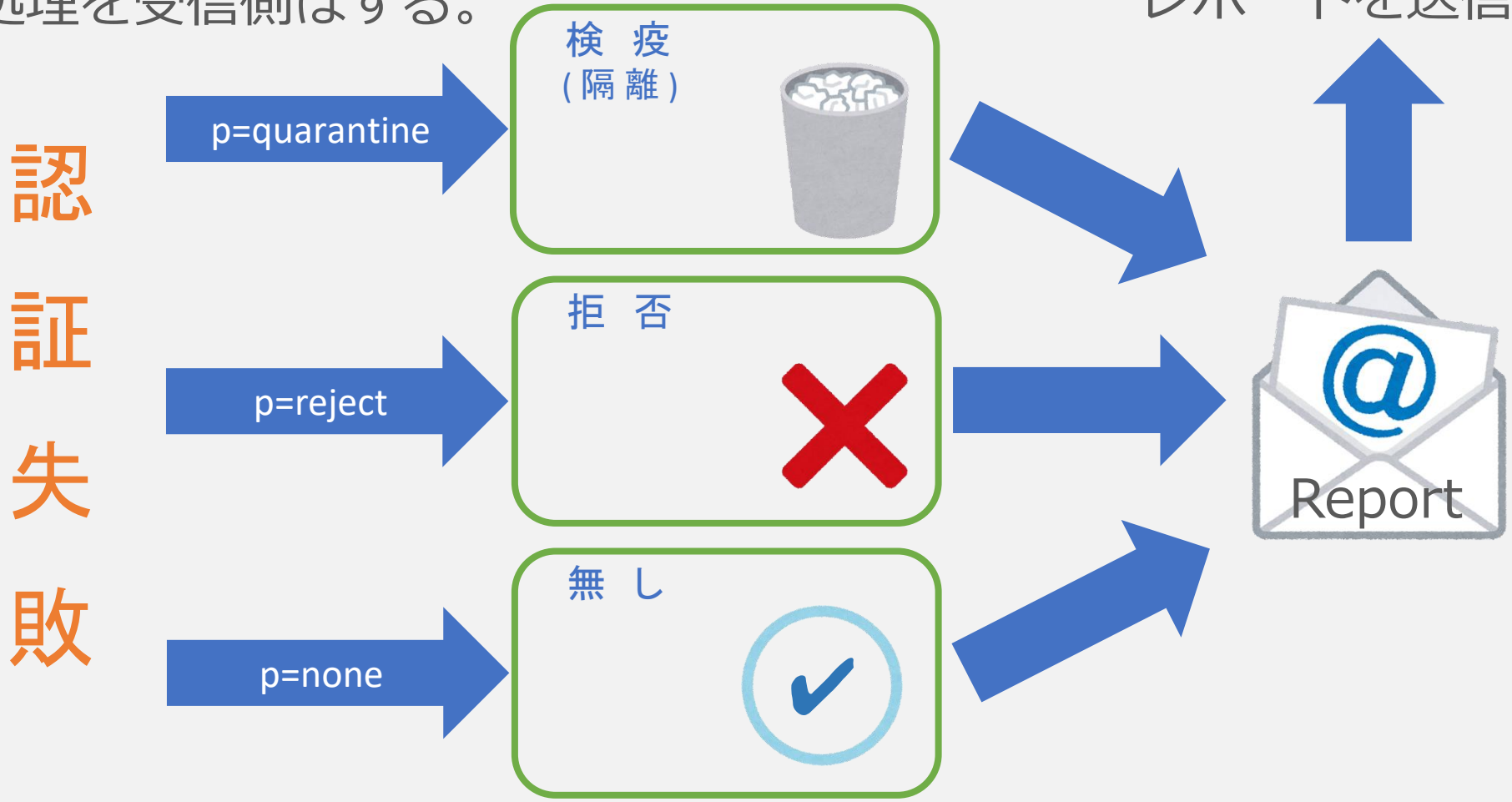
```
_dmarc.nkkr.jp  text =
"v=DMARC1; p=quarantine; rua=mailto:***@nkkr.jp;
ruf=mailto:***@nkkr.jp"
```

v= (DMARC バージョン)
p= (認証失敗時に受信側で実行してほしいアクション）
rua= (集約レポートの受信アドレス)
ruf= (失敗レポートの受信アドレス)

DMARC の流れ

認証失敗時は、
ポリシーに応じた
処理を受信側はする。

ruf= , rua= の
アドレス宛に
レポートを送信する。



SPF / DKIM / DMARC をみてみると

メール ID	<[redacted]@nkkr.jp>
作成日:	2023年5月15日 9:54（2 秒後に配信済み）
From:	Masato Nakakura <masato.nakakura@nkkr.jp> Becky! ver. 2.81.04 [ja] を使用
To:	masato.nakakura@nkkr.jp
件名:	test
SPF:	PASS（IP: 118.27.106.173）。 詳細
DKIM:	'PASS'（ドメイン: nkkr.jp） 詳細
DMARC:	'PASS' 詳細

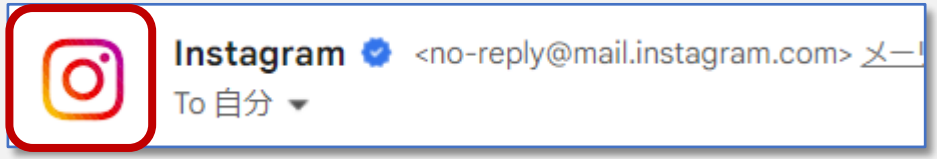
チェックサイトも各種あるようですが、
動作の確認は Gmail へ実際にメールを送信し
て、正常に扱われ(PASS)ているか確認してみました！

BIMI とは

DMARC などの送信ドメイン認証技術によって認証されたドメインは、より分かりやすい形でメール受信者に提示することができれば、ドメイン認証の効果を具体的に知るよい機会になります。

こうした仕組みの一つとして、BIMI (Brand Indicators for Message Identification) が登場しています。

BIMI の特徴



▲BIMIによって表示されたロゴ

```
…
DKIM-Signature: v=1; a=rsa-sha256;
c=relaxed/simple; d=mail.instagram.com; …
…
BIMI-Selector: v=BIMI1; s=fb2021q2v1;
…
```

メールヘッダにある
DKIM-Signature の ドメイン名(d=)
BIMI-Selector の セレクタ名(s=)
から以下のように、DNSに問合せするとURIが取得できる

fb2021q2v1._bimi.mail.instagram.com

v= (BIMI バージョン)
l= (イメージのURI)
a= (VMCのURI)

```
fb2021q2v1._bimi.mail.Instagram.com  text =
 "v=BIMI1; l=https://instagram.com/images/bimi/ig-
logo.svg; a=https://instagram.com/bimi-vmc.pem;"
```

BIMI -VMCとは

VMC（Verified Mark Certificate）は、ロゴの所有権を証明するデジタル証明書です。

VMCを発行するには、事前に商標登録がされている必要があります。

現在、VMCは DigiCert , Entrust が発行しています。

BIMI要件としては、VMCの設定は任意ですが Gmail など多くのメールクライアントでは、VMCを必須としています。（ロゴの不正使用防止のため）

まとめ

SPF / DKIM / DMARC を実装していくことで、受信側は送信元から確実に発信されていることが容易に確認できるようになり、メールの信頼度が増していきます。

BIMIの実装では、より視覚的に送られてきたメールが正規のものであるか判断できます。