



A-3:
まだ間に合う？
今日から始める送信ドメイン認証

株式会社NTTドコモ

正見 健一郎



本日の目的

送信ドメイン認証が行われることが日本のメール環境で当たり前になること

各章のねらい

	項目	想定するゴール
1	はじめに	・特にフィッシング詐欺対策で送信ドメイン認証が必要なことがわかる
2	そもそもドメイン認証とは	・送信ドメイン認証とはメールサーバに対する認証であることがわかる
3	SPF,DKIM,DMARCとは	・SPF,DKIM,DMARCが何を用いて検証しているかわかる
4	お客さまへの影響について	・送信ドメイン認証を行うメリット、行わないデメリットがわかる

基本

←比較的容易なスライドに基本マークを付与しています
これがあるスライドの内容は是非覚えてください！

Copyright © 2024 NTT DOCOMO, INC. - All Rights Reserved



はじめに



名前

正見 健一郎

部署

株式会社NTTドコモ第一プロダクトデザイン部

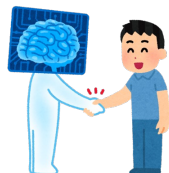
担当業務

- ・ ドコモメールの迷惑メール対策の開発、運用
- ・ 迷惑メールの傾向分析、インシデント対応
- ・ DMARCの普及活動
- ・ ドコモメール公式アカウントの普及活動
- ・ Eメールの疎通関連の窓口対応

あんしんセキュリティ

取り組み事例の共有

2019



- ・ AIを活用した迷惑メールの分析基盤の構築
- ・ デイリーでの迷惑メール傾向の見える化

2021



公式アカウントマーク

- ・ ドコモメール公式アカウントの提供開始

2023



警告



WARNING

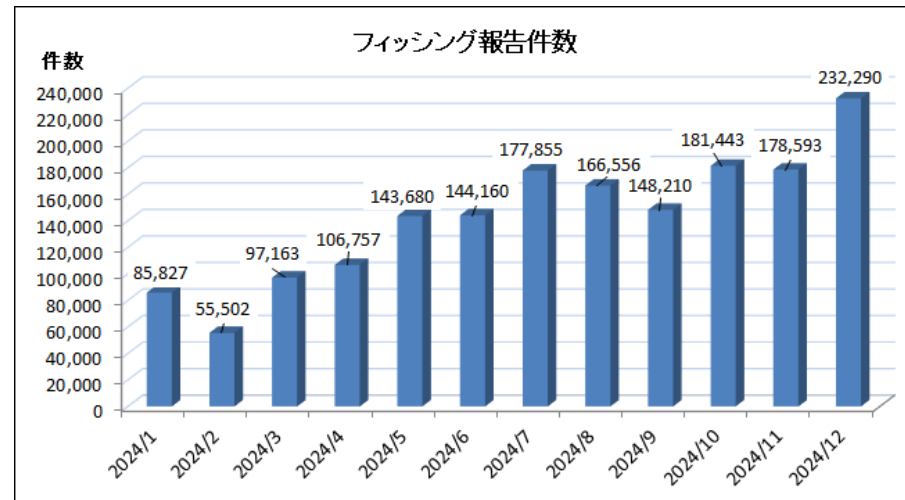
- ・ DMARCによるメールフィルタリングの提供開始
- ・ なりすましメールの警告表示の提供開始

2025



- ・ 迷惑メールフォルダの提供開始

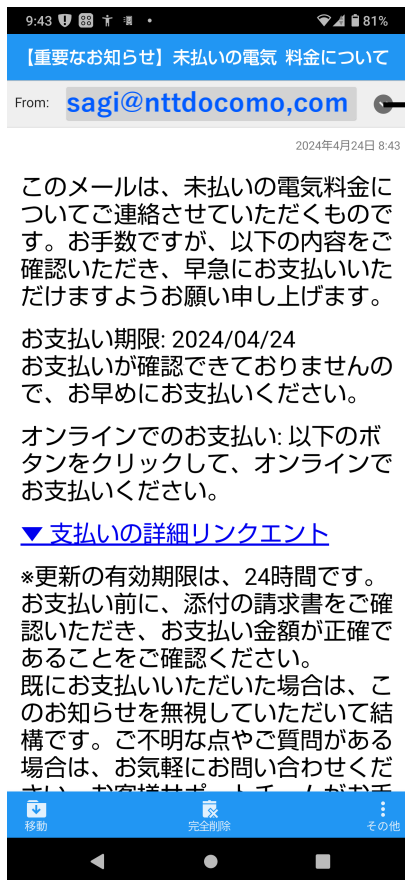
昨今迷惑メールはフィッシング詐欺の文脈で語られます



引用：フィッシング対策協議会月次報告書
<https://www.antiphishing.jp/report/monthly/202412.html>

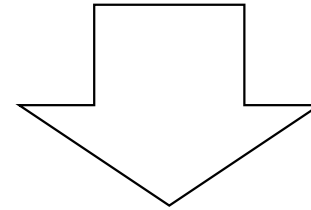
送信ドメイン認証は、迷惑メール対策のうち、
フィッシング詐欺に有用な技術です

フィッシング詐欺はメールアドレスを詐称します



メールアドレスまたはディスプレイネームを詐称して攻撃が行われる場合が多いです

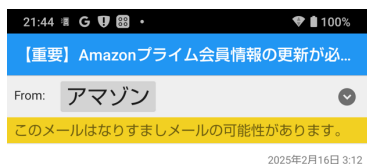
- ・ユーザの視認性を目的とした攻撃
- ・スパムフィルタ除け（受信リスト設定）を目的とした攻撃



メールアドレスの正当性の確認が必要

ドコモメールではドメイン認証を活用してUIを工夫

なりすましメールには警告を表示



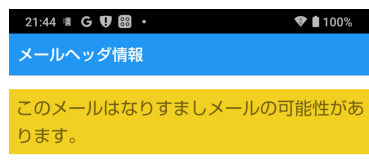
平素よりAmazonプライムをご利用いただき、誠にありがとうございます。

お客様の会員情報の一部が更新が必要な状態になっております。引き続きAmazonプライムの特典を利用いただくために、以下の手順で情報を更新してください。

情報更新の手順:

1. 下記のリンクをクリックしてください。
2. Amazonアカウントにログインしてください。
3. 表示される指示に従い、情報を確認・更新してください。

[会員情報を更新する](#)



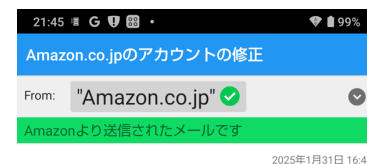
このメールが「tsite.jp」の所有者から送信されているかどうか、ドコモメールのサーバにて検証しました。

技術名	認証結果	対象ドメイン
DMARC	NG	tsite.jp
SPF	NG	tsite.jp
DKIM	NG	tsite.jp

詳細なメールヘッダは[こちら](#)をご覧ください。



正当なメールにはあんしん安全を訴求



amazon.co.jp

Amazon.co.jp をご利用いただき、ありがとうございます。お客様のリクエストに沿って、アカウント情報を変更いたしましたのでお知らせします。変更後のアカウント名：セキサン太郎2

アカウントサービスでは、登録内容の変更のほか、注文内容の確認および変更ができます。

当サイトにお問い合わせの際は、アカウントにご登録のお名前およびEメールアドレスでお問い合わせください。他のEメールアドレスや別のお名前でお問い合わせいただいた場合、ご注文内容や登録内容についてお答えできませんので、ご了承ください。



このメールが「amazon.co.jp」の所有者から送信されているかどうか、ドコモメールのサーバにて検証しました。

Amazon
より送信されたメールです

本メールはドメイン所有者の認証済みメール(BIMI)です。

技術名	認証結果	対象ドメイン
DMARC	OK	amazon.co.jp
SPF	OK	bounces.amazon.co.jp

・公式アカウント
・BIMI(ブランドロゴ)
を表示し安全さを明示





そもそも
送信ドメイン認証って？



ドメイン認証は認証と送受信の2つの意味を持っています

認証

誰からのメールかを確認、検証する

DMARC

DKIM

SPF

送受信

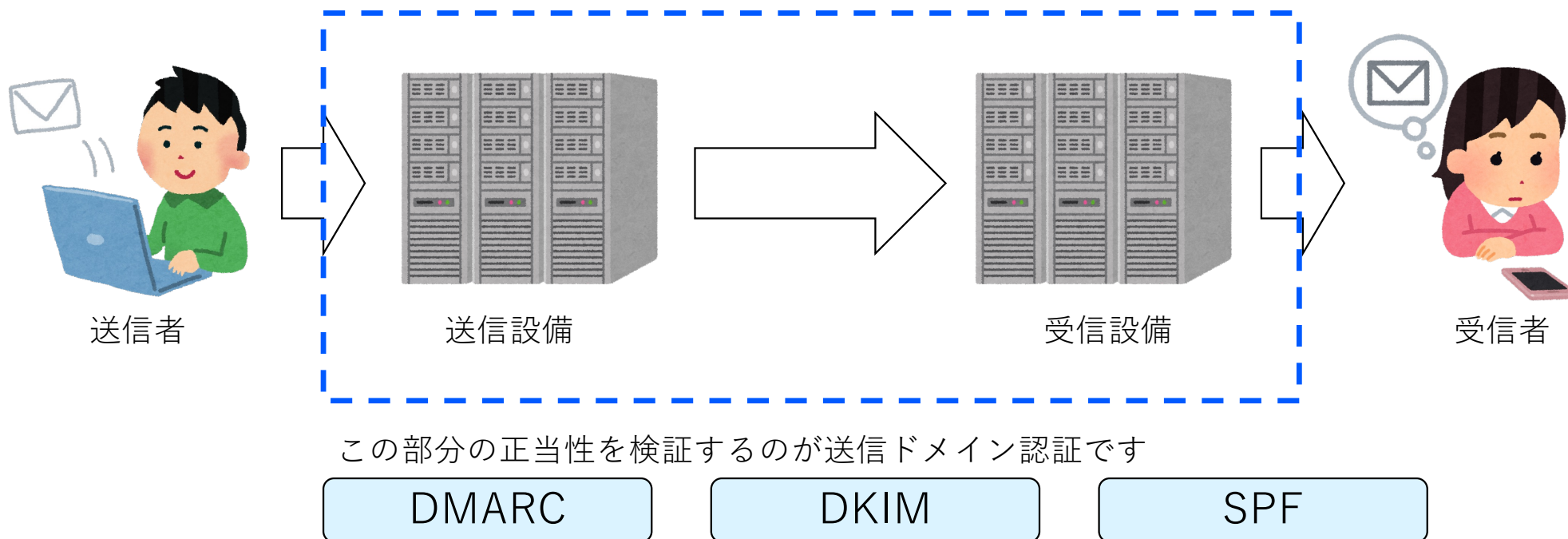
メールを受信するかどうか判断する

DMARC

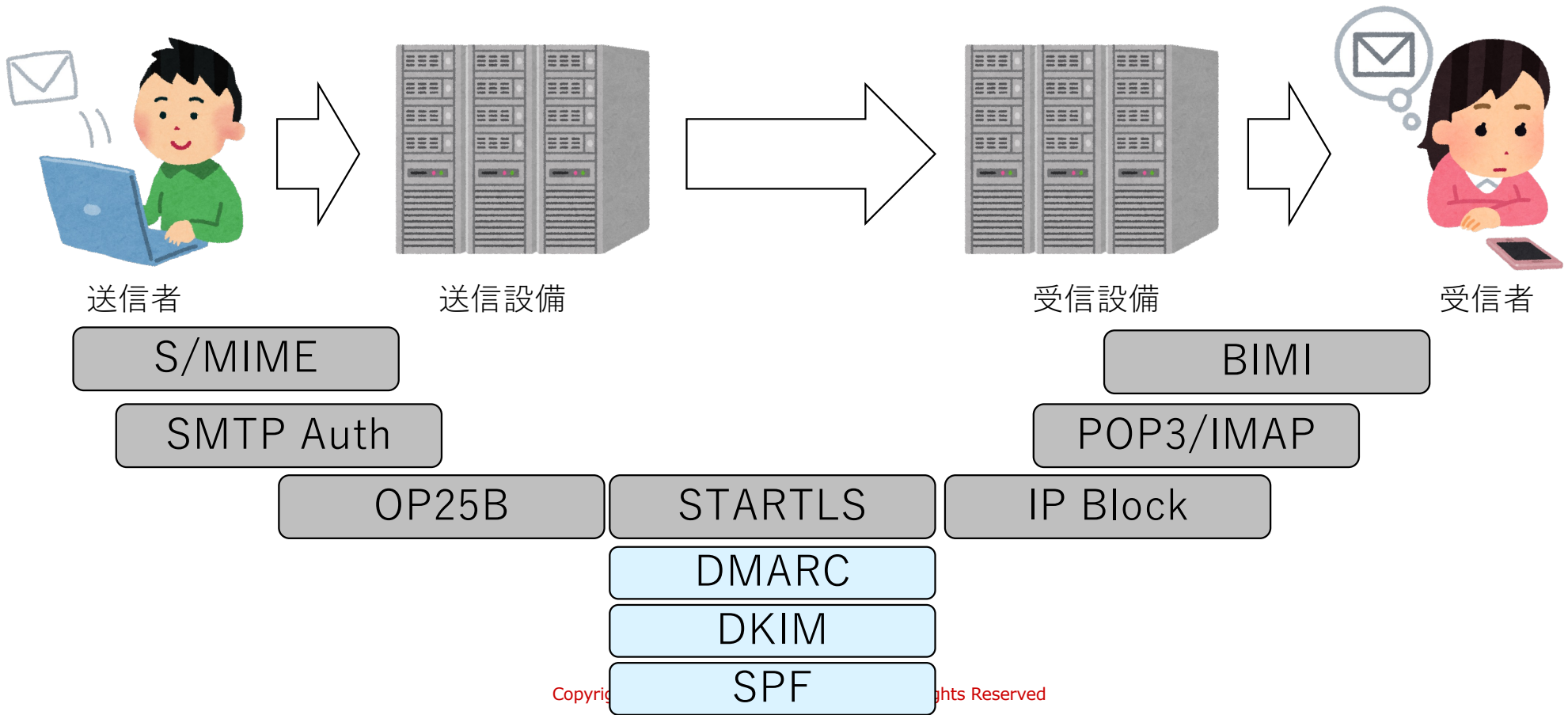
スパムフィルタ

検証によって正当性を確認できない場合、受信側では受け取ってもらえない可能性があります

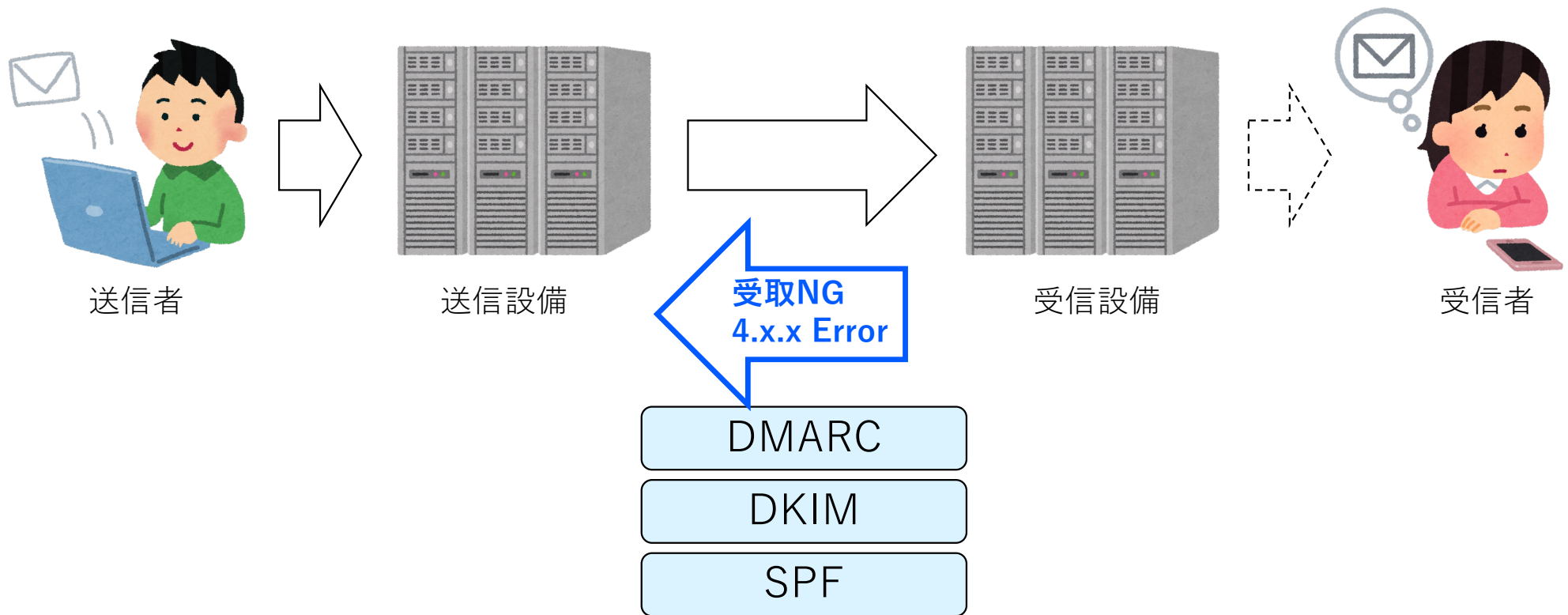
送信ドメイン認証とはメール設備の認証です



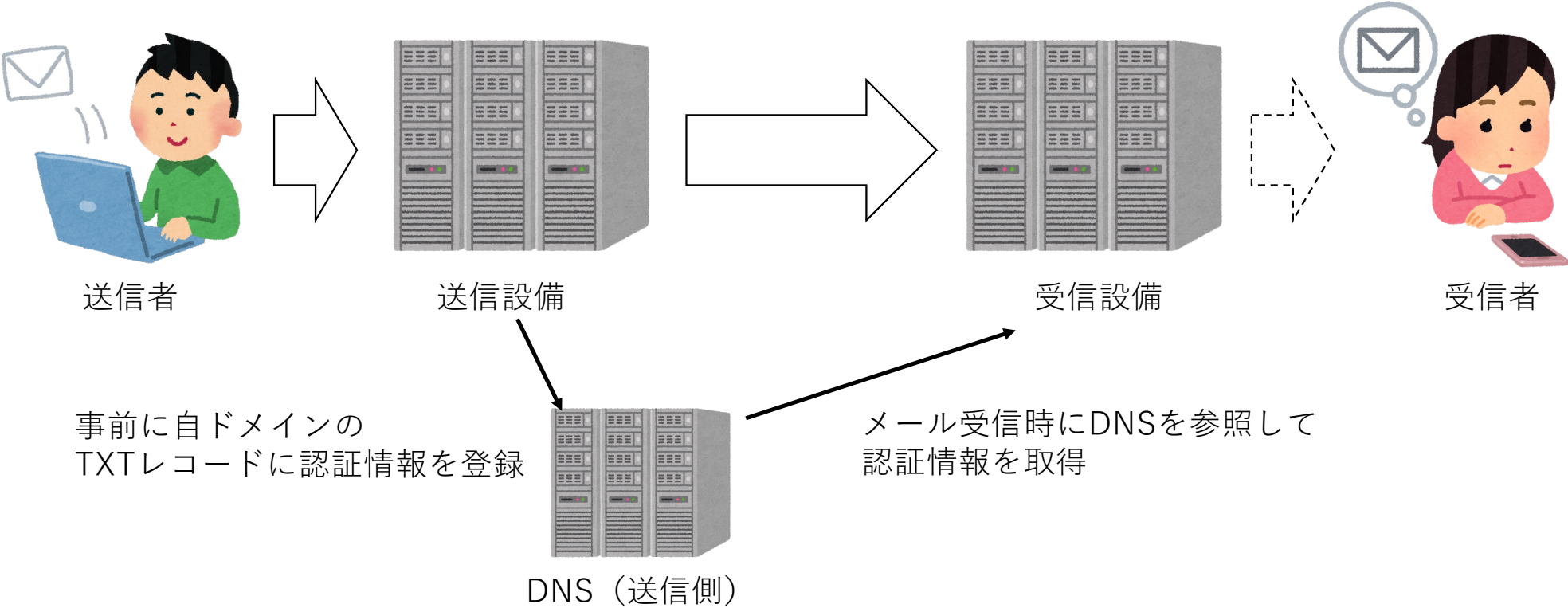
セキュリティは他にも色々ありますが今日は無視します



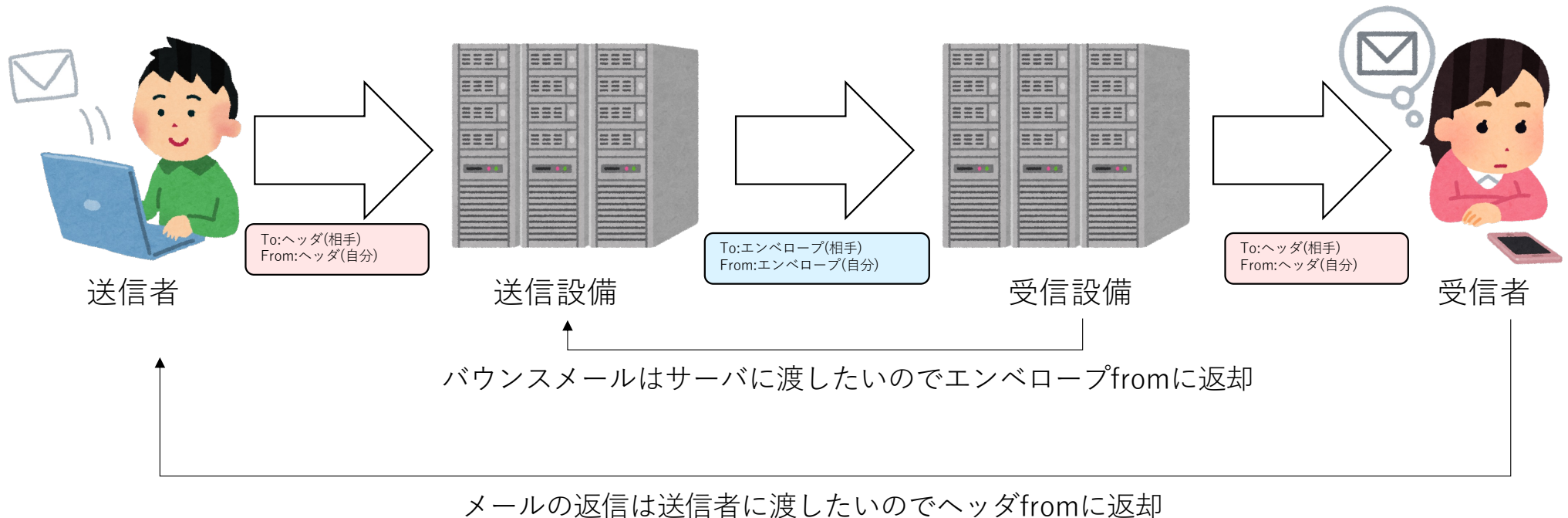
大事なことは、送信ドメイン認証の結果によっては
受信設備側からErrorが返却されることです



またいずれの場合もDNSを参照して検証を行っています
今後宣言とか許可した、とかはDNSの登録内容を指します



今後ヘッダfromとエンベロープfromという単語が出ます。
 ちょっと誤解があるかも知ですが、以下でご認識ください





SPF,DKIM,DMARCとは



上から順にやっていくことになると思われます

- ✓ SPF(Sender Policy Framework)
- ✓ SenderID/SPF
- ✓ DKIM(DomainKeys Identified Mail)
- ✓ DMARC(Domain based Message Authentication)



✓ **SPF**(Sender Policy Framework)

✓ **SenderID/SPF**

✓ DKIM(DomainKeys Identified Mail)

✓ DMARC(Domain based Message Authentication)

✓ SPF (Sender Policy Framework)

ドメイン所有者が許可したIPアドレスから送信されているか検証します

検証対象ドメイン

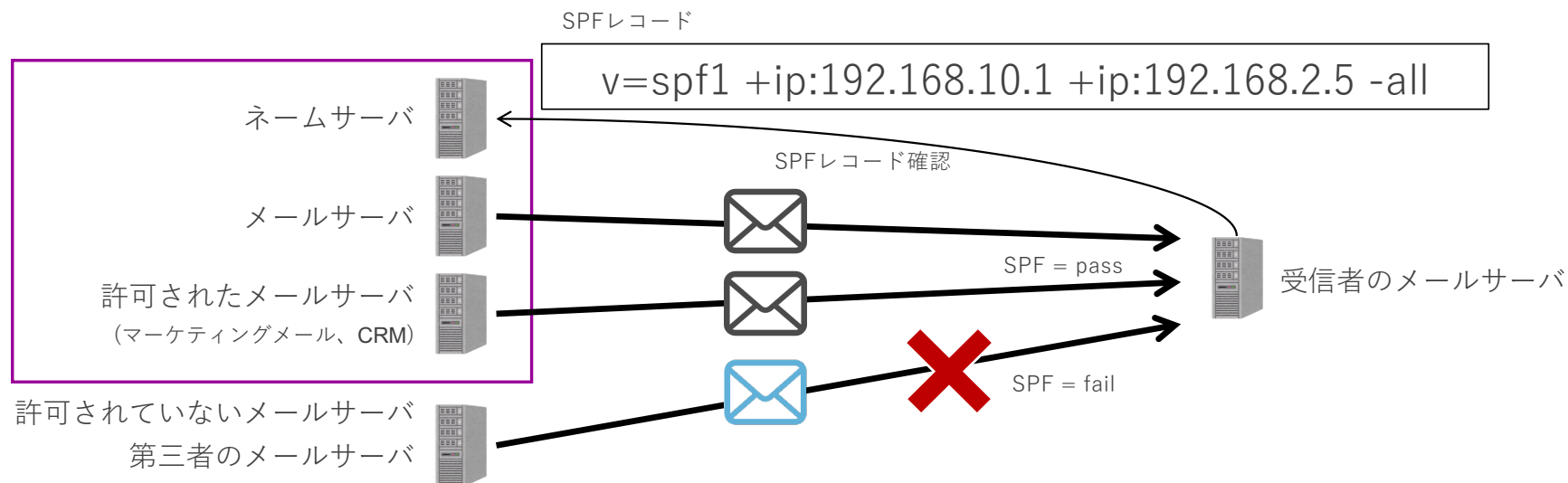
エンベロープfrom ドメイン

送信者がやること

DNSにIPアドレスリストを登録する

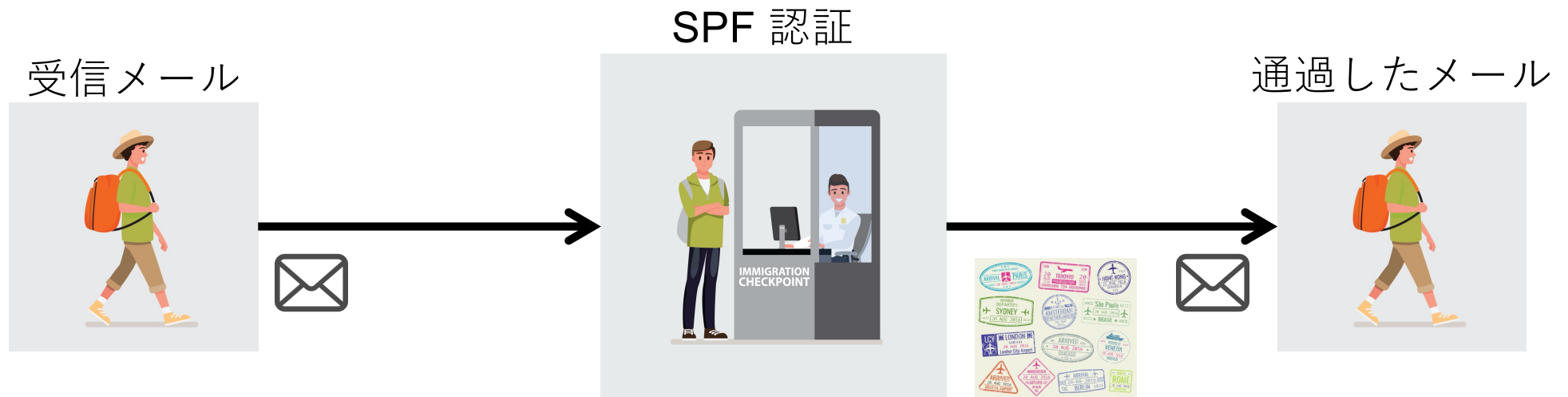
受信者側の処理

DNSのIPアドレスリストからのメールであれば認証成功とする



✓ SPF (Sender Policy Framework)

入国審査で例える



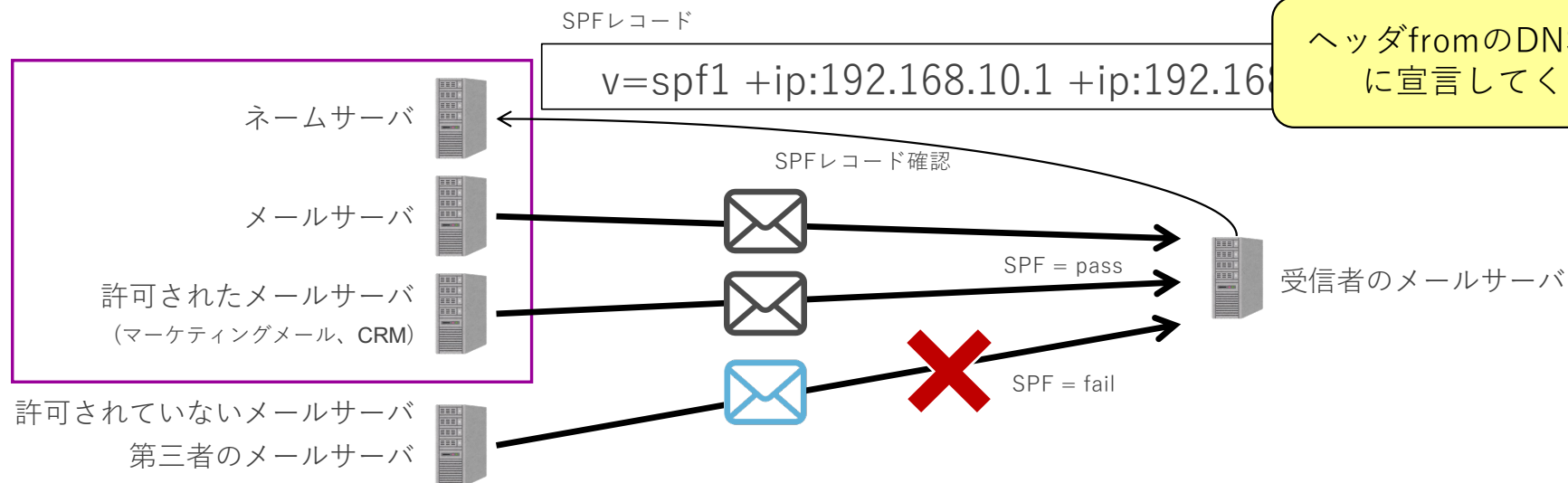
IP アドレス の確認

国籍と出国情報が
一致しているか

✓ SenderID/SPF

SPFとの違いは検証対象ドメインがヘッダfromドメインになっていることです

検証対象ドメイン	ヘッダfromドメイン
送信者がやること	DNSにIPアドレスリストを登録する
受信者側の処理	DNSのIPアドレスリストからのメールであれば認証成功とする





✓ SPF (Sender Policy Framework)

SPFレコードの書き方はややこしいので実際に書くときに調べてみてください

Sample 1: ホストのIPアドレスで記述メールを外部に送出するメールサーバのIPアドレスを直接指定する。送信メールサーバ数があまり多くない場合は、記述ミスを防ぐためや、受信側でのDNSクエリを抑制するため、この記述方を強く推奨する。

```
example.org. IN TXT "v=spf1 ip4:x.x.x.x ip4:y.y.y.y ip4:z.z.z.z -all"
```

Sample 2: ホスト名で記述メールを外部に送出するメールサーバのホスト名を指定する。上のIPアドレス直接指定に比べてメンテナンスが簡単であるが、受信側の認証処理においてDNSへの負荷が少し増える可能性はある。ホスト名は必ずFQDNで指定する。

```
example.org. IN TXT "v=spf1 a:mx01.example.org a:mx02.exmaple.org a:ns.example.org -all"
```



- ✓ SPF (Sender Policy Framework)
- ✓ SenderID/SPF
- ✓ **DKIM (DomainKeys Identified Mail)**
- ✓ DMARC (Domain based Message Authentication)

✓ DKIM(DomainKeys Identified Mail)

電子署名を用いて検証する技術です。対象ドメインを自由に設定可能です

検証対象ドメイン

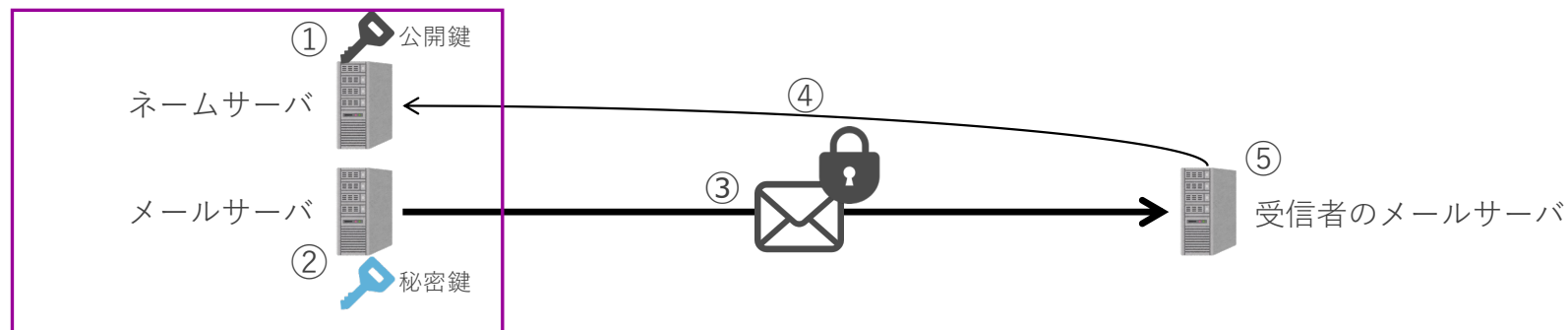
送信者が指定した任意のドメイン

送信者がやること

- ①メールの送信設備で電子署名を実施（秘密鍵）
- ②DNSに公開鍵を登録する

受信者側の処理

公開鍵で署名を検証し、ハッシュが一致すれば認証成功とする



✓ DKIM(DomainKeys Identified Mail)

入国審査で例える



✓ DKIM(DomainKeys Identified Mail)

やはりややこしいのでやるときに調べてみてください

署名の処理イメージ

図 DKIM-Signatureヘッダ例

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=example.jp;
s=fife.dkim; t=1257184337; bh=pPfbzXX9GdGASjXoTuUHQohBpWhrAlGhKFWK
SOHLIY=;

DomainKeysヘッダ

署名の対象に含まれるヘッダのリスト。このリストによって明示的に署名対象にしたヘッダを宣言しておくことで、他のヘッダの予期せぬ追加による認証情報の破壊を防ぐ

h=Subject:Mime-Version:Content-Type:From:In-Reply-To:Date
Cc:Content-Transfer-Encoding:Message-Id:References:To;
b=hTE38v7jP+8xFUIdm8Zv0skfAluZ/ELWgfflpUm/XjNAkS+8kuByB7Cef9qnAZLb5
IBfBhHG+Ta00artNJQerWbAXWfBqzPFXPcZcIaI8xb8ZmvvnNnAA0rFGkXo8B/3+k2
edgwQACP4IxcFJLlnatyTjqvQkIdja8uk41lGKI=

電子署名

Subject: =?iso-2022-jp?B?UmU6IEpUcbJEIKSIRJGyhc?=
Mime-Version: 1.0
Content-Type: text/plain; charset=iso-2022-jp; format=flowed; delp=yes
From: Hanako Yamada <yamada@example.jp>
Date: Tue, 3 Nov 2009 02:52:05 +0900
Content-Transfer-Encoding: 7bit
To: Taro Suzuki <suzuki@example.com>

鈴木様

お世話になっております。

.....

DNS登録のイメージ

<セクタ>._domainkey.<ドメイン名>

にTXTレコードとして公開

(例)

Selector._domainkey.example.com

```
tf0001._domainkey.twofive25.com text =
```

```
"v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC9Y4Yc8MUut6E1b  
ynuQTz4d3hwZB8GISuWlvWyH189ygRwa+HJpT2BAMojUd3n16G4VP4GDpXe70t8cnmhH8UoiRrzP/ark  
J16CnZUKDN2s8X5iwYdpeC8pX3BSXIisVTuYxaBDsAsb5Hgqg+Hf50VcEN6WIKtL2BpXchWQtwvbwIDA  
QAB"
```

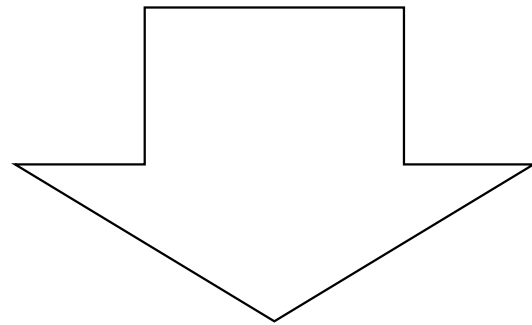


DMARCの前にいったんまとめます



項目	SPF	SenderID/SPF	DKIM
RFC	7208	4406	6376
検証方法	IPアドレス	IPアドレス	電子署名
対象 ドメイン	エンベロープfromドメイン	ヘッダfromドメイン	送信者の指定したドメイン
簡単さ	DNSに記載するだけ	DNSに記載するだけ	署名の実装が必要
問題点	・ 転送に弱い ・ ヘッダfromドメインの詐称が可能	・ 普及率が低い	・ 改変に弱い（メーリス等） ・ ヘッダfromドメインの詐称が可能

ヘッダfromドメインの詐称が可能の問題点が残る

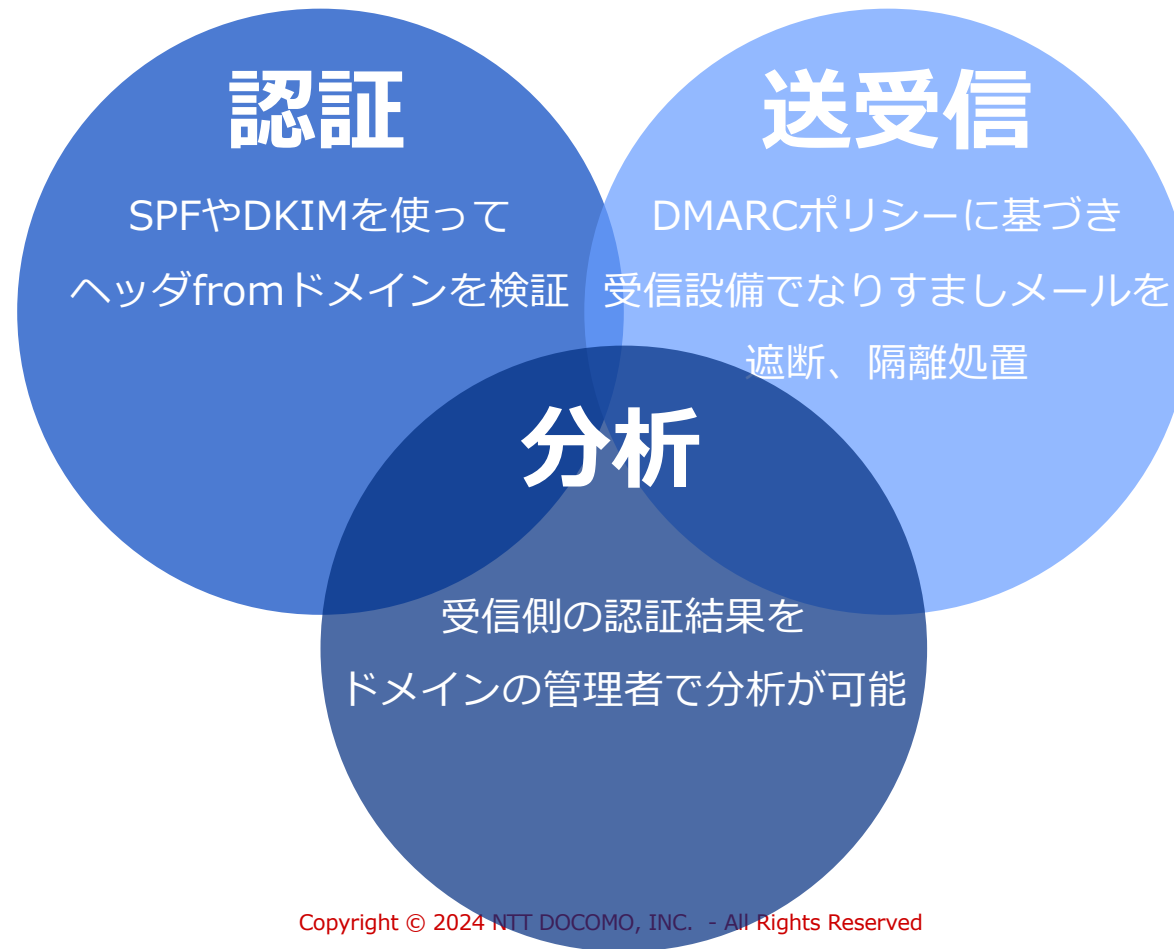


DMARCは詐称ができません



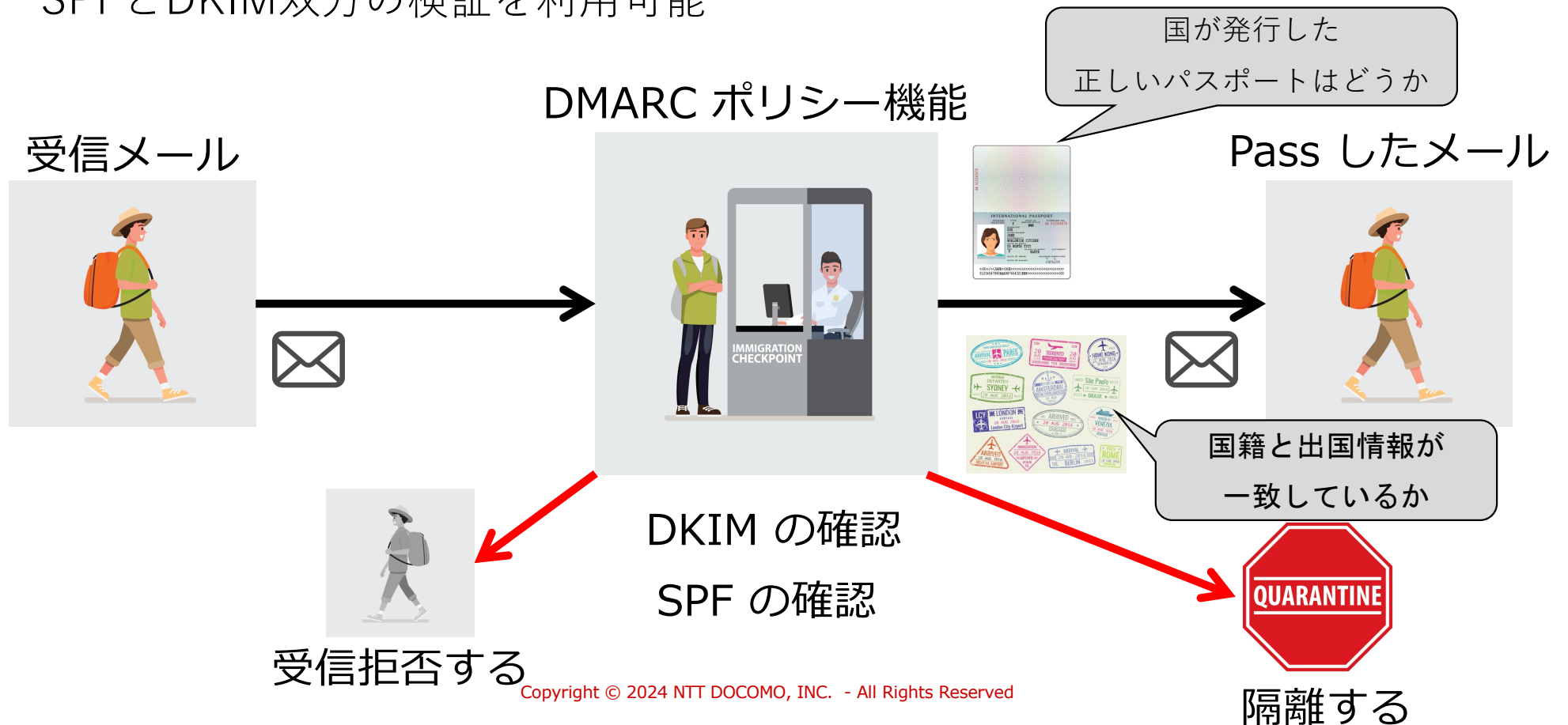
- ✓ SPF(Sender Policy Framework)
- ✓ SenderID/SPF
- ✓ DKIM(DomainKeys Identified Mail)
- ✓ **DMARC(Domain based Message Authentication)**

✓ DMARC(Domain based Message Authentication)



✓ DMARC(Domain based Message Authentication)

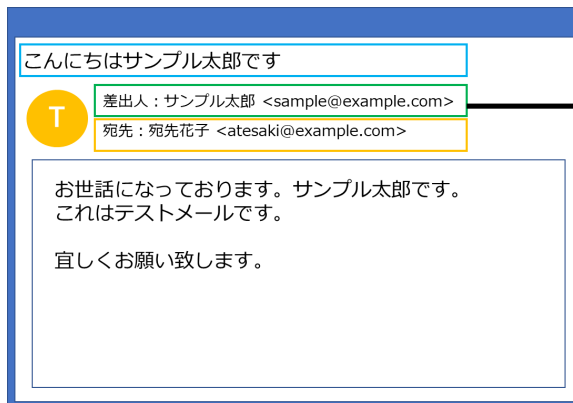
SPFとDKIM双方の検証を利用可能



✓ DMARC(Domain based Message Authentication)

SPF or DKIMを用いて検証する技術です。まずは認証側の処理です

検証対象ドメイン	ヘッダfromドメイン
送信者がやること	①DNSにDMARC宣言を登録する (noneで可) ①ヘッダfromドメインと同じドメインでSPFを実施 ②ヘッダfromドメインと同じドメインでDKIMを実施
受信者側の処理	ヘッダfromドメインと同じ、または同じ組織ドメインでSPFまたはDKIMが成功したら認証成功とする



- ①SPF認証はexample.comで成功しているか？
(エンベロップfromはexample.comか？)
- ②DKIM認証はexample.comで成功しているか？
(DKIM署名はexample.comか？)



✓ DMARC(Domain based Message Authentication)

SPF,DKIMの設定が完了していたらDNSに1行書くだけです

_dmarc.<ドメイン名>にTXTレコードとして公開

(例)

_dmarc.example.com text =

"v=DMARC1; p=reject; rua=mailto:dmarc-ra@example.com; ruf=mailto:dmarc-ra@example.com"

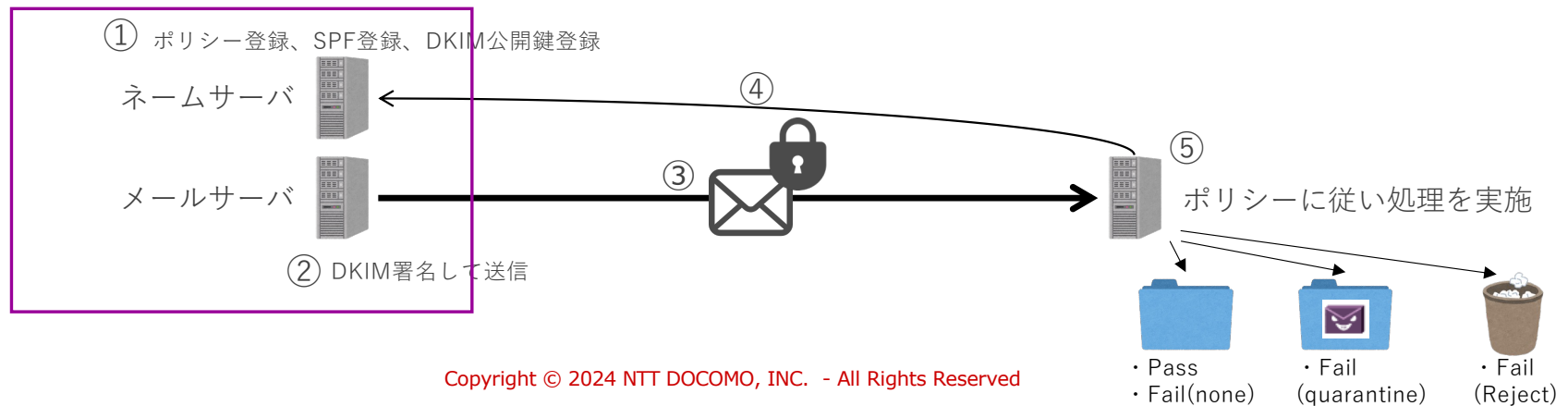
_dmarcとつけてください

rua,rufはなくても問題ありません

✓ DMARC(Domain based Message Authentication)

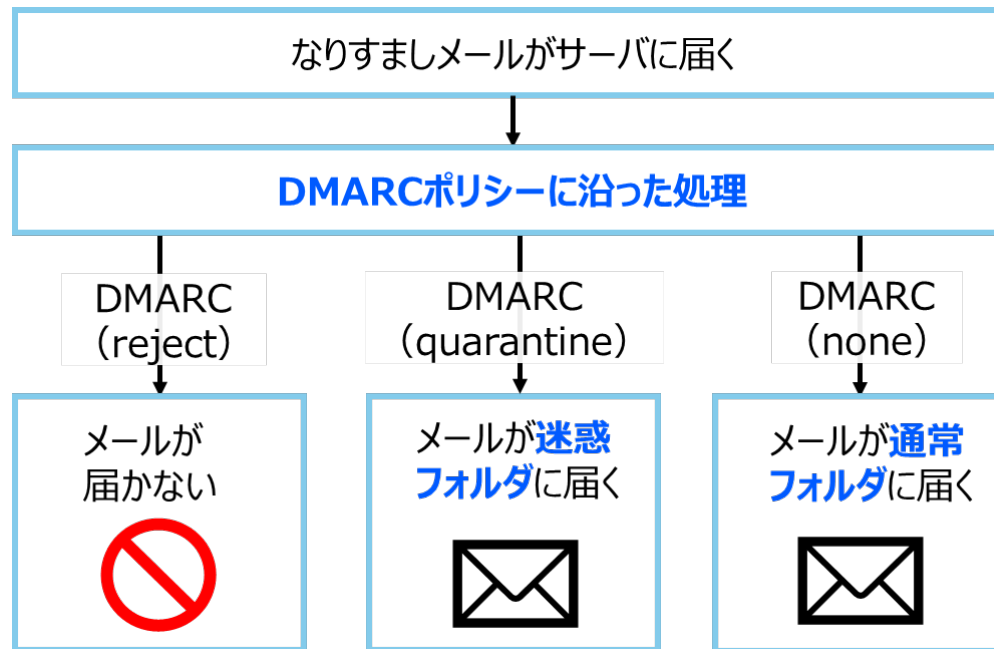
SPF or DKIMを用いて検証する技術です。次に送受信の処理です

検証対象ドメイン	ヘッダfromドメイン
送信者がやること	DNSにポリシーを登録する(quarantine,reject)
受信者側の処理	ヘッダfromドメインと同じ、または同じ組織ドメインでSPFまたはDKIMが成功したら認証成功とする



✓ DMARC(Domain based Message Authentication)

p=xxxという宣言によって受信側の挙動を指定できます



送信側が規定するポリシー

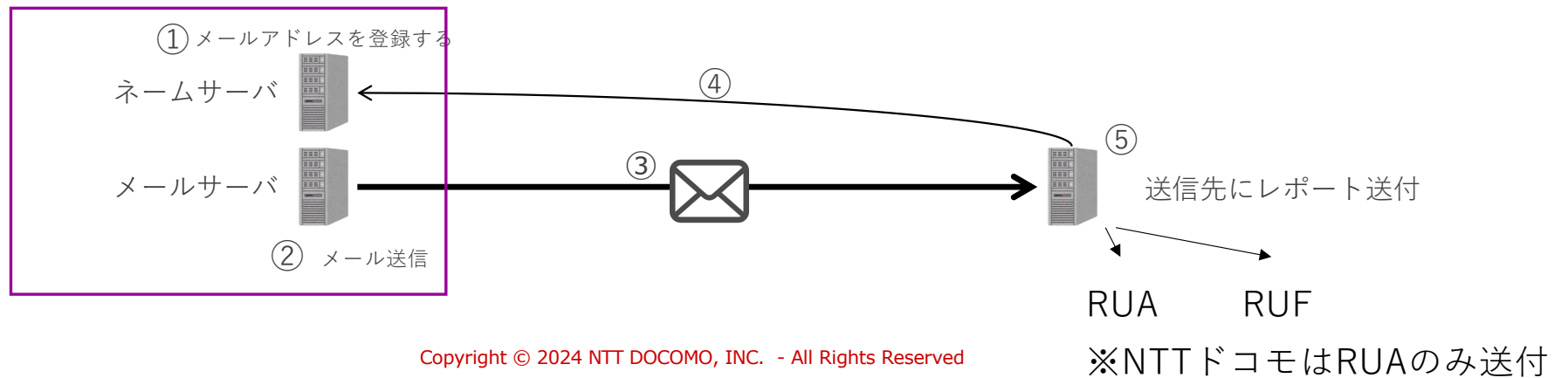
p= None	なりすましメールに対して何も行わない
p= Quarantine	なりすましメールを迷惑メールフォルダに隔離する
p= Reject	なりすましメールを受け取らない

導入時に認証が正しく成功しているか確認する際はp=noneを宣言し、その後にp=quarantine,rejectへ移行が必要

✓ DMARC(Domain based Message Authentication)

SPF or DKIMを用いて検証する技術です。次に分析の処理です

検証対象ドメイン	ヘッダfromドメイン
送信者がやること	DNSにレポートの送信先メールアドレスを登録する
受信者側の処理	指定されたメールアドレスにRUA,RUFを送信する





✓ 参考 SPF,DKIM,DMARC認証結果一覧

	None	Neutral	Pass	Fail	SoftFail	TempError	PermError
SPF	SPFレコードなし	“?”条件にマッチ	認証成功	SPFレコードが公開されているが失敗	“～”条件にマッチ	一時的な通信エラーなど	SPFレコードに誤りがあるなど恒常的なエラー
DKIM	署名なし	署名に文法誤りがある	認証成功	認証失敗	N/A	一時的な通信エラーなど	恒常的なエラー
DMARC	DMARCレコードなし	N/A	認証成功	認証失敗	N/A	一時的な通信エラーなど	DMARCレコードに誤りがあるなど恒常的なエラー



✓ SPF/DKIM/DMARCのまとめ

- 各送信ドメインは検証方法と対象が異なる

SPF	エンベロープfromドメイン	IPアドレス
SenderID/SPF	ヘッダfromドメイン	IPアドレス
DKIM	任意のドメイン	電子署名
DMARC	ヘッダfromドメイン	SPForDKIM

→ ヘッダfromドメインの認証が可能な
DMARCまで導入されることが望ましい

- DMARCの導入にはSPF、またはDKIMの導入が必要
- SPF,DMARCはDNS更新のみで可能(DKIMは要設備改修)
※商用のメール配信サービスを利用の場合はDKIMも設定変更のみで実現可能な場合あり
- DMARC導入後はなりすまし対策が必要(p=quarantine,reject))



お客さまへの影響



✓ 実施するメリット

✓ やらない場合のデメリット

✓ メリット① 信用度が上がります

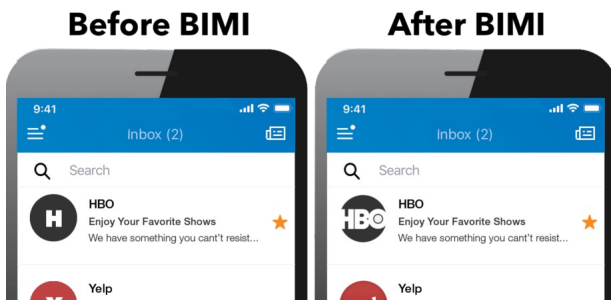
- ・ドメインの正当性が検証でき、受信側の信用度が上がります



✓ メリット② 正当なメールだと明示可能

- ・ 正当なメールであることをお客さまにお伝えできるようになります

BIMI



DMARC

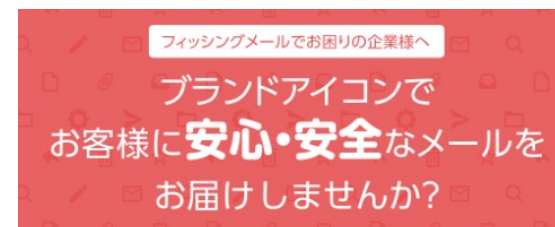
公式アカウント



DMARC

SPF

ブランドアイコン



DKIM

SPF

✓ メリット③ 踏み台攻撃への対処が可能

- ・ DMARC(Reject)を宣言すれば踏み台攻撃を回避可能です

Point①：ドメイン固定で複数の攻撃の踏み台に

Point②：対策されたらすぐに次のドメインへ移行

From:xx@crXXXX.jp

【重要なお知らせ】お客様のお支払い方法が承認されません

残念ながら、Amazon のアカウントを更新できませんでした。
今回は、カードが期限切れになっているか、請求先住所が変更されたなど、さまざまな理由でカードの情報を更新できませんでした。
お客様のアカウントを維持するため Amazon アカウントの情報を確認する必要があります。下からアカウントをログインし、情報を更新してください。

■ご利用確認はこちら

From:xx@crXXXX.jp

今すぐ受け取れる！5000円分の PayPayボーナスとお得なキャンペーン情報

PayPayをご利用いただきありがとうございます。
すぐに5000円分のPayPayボーナスを受け取ることができます。

■詳しくはこちらをご覧ください。

ウェルシアグループアプリから PayPayで支払うと最大全額戻ってくる！

開催期間：2021/8/13（火）～9/9（月）

付与上限：100,000ポイント／回および期間

From:xx@myXXXXmo.com

Amazonプライム会員様への重要なお知らせ

お客様、

Amazon.co.jpをご利用いただきありがとうございます。最近、お客様のアカウント情報が第三者によって変更された可能性があります。アカウントの安全を確保するため、下記のリンクをクリックしてアカウントを検証してください。

hxxps://xxx.html

Amazon セキュリティチーム

From:xx@account.XXXEndo.com

【緊急】dカードが利用停止のお知らせ

誠にありがとうございます。このたび、お客様のdカードアカウントで不審なアクティビティが検出されたため、ご利用を一時的に制限させていただきました。

つきましては、以下のリンクからアカウントの確認と利用再開手続きを行ってください。

hxxps://xxx.cc.

いずれもDMARCの宣言は「none」の日本企業の実在ドメイン

⇒無関係のドメインがいきなり利用されるため、**全ての企業が被害者に**



✓実施するメリット

✓やらない場合のデメリット

✓ デメリット① メールが届かなくなります

・ 某社の送信ガイドライン

送信者ドメイン認証

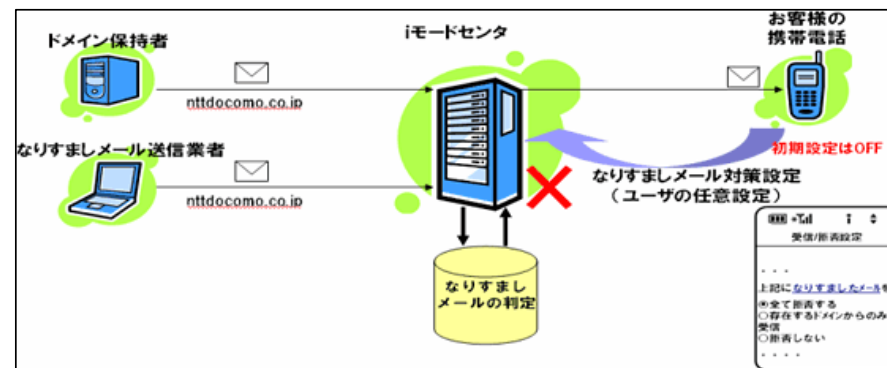
ワンクリック購読解除

TLS化

DNSの適正化

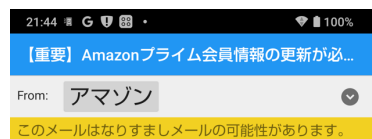
スパム率への考慮

・ 通信キャリアのスパムフィルタ



✓ デメリット② 警告が表示されます (ドコモの場合)

- ・ DMARCが成功していない場合警告が表示されます



平素よりAmazonプライムをご利用いただき、誠にありがとうございます。

お客様の会員情報の一部が更新が必要な状態になっております。引き続きAmazonプライムの特典を利用いただくために、以下の手順で情報を更新してください。

情報更新の手順:

1. 下記のリンクをクリックしてください。
2. Amazonアカウントにログインしてください。
3. 表示される指示に従い、情報を確認・更新してください。

[会員情報を更新する](#)



このメールが「tsite.jp」の所有者から送信されているかどうか、ドコモメールのサーバにて検証しました。

技術名	認証結果	対象ドメイン
DMARC	NG	tsite.jp
SPF	NG	tsite.jp
DKIM	NG	tsite.jp

詳細なメールヘッダは[こちら](#)をご覧ください。



✓ 本日のまとめ

- ① ユーザを脅威から守るために送受信者全員のDMARC対応が必要
- ② 送信ドメイン認証はメールを送信する設備で対応が必要
- ③ 上記のためにはSPF/DKIMそしてDMARCの導入が必要
- ④ 導入にはメリットも多くあり、逆に対応しないと悪影響が発生



ご清聴ありがとうございました