# DMARCは導入したんだけど・・・
# 現場のつぶやき
# ～ BIMI？何それ美味しいの？

HORNETSECURITY

HornetSecurity
プリンシパルメッセージングエンジニア
平野 善隆

JPAAWG 8th General Meeting 2025-11-05

# 自己紹介

名前　　平野 善隆

所属　　Hornetsecurity株式会社 (旧Vade Japan)
Principal Messaging Engineer

好きな技術　　メール、DNS、Python、Go
AWS、Serverless

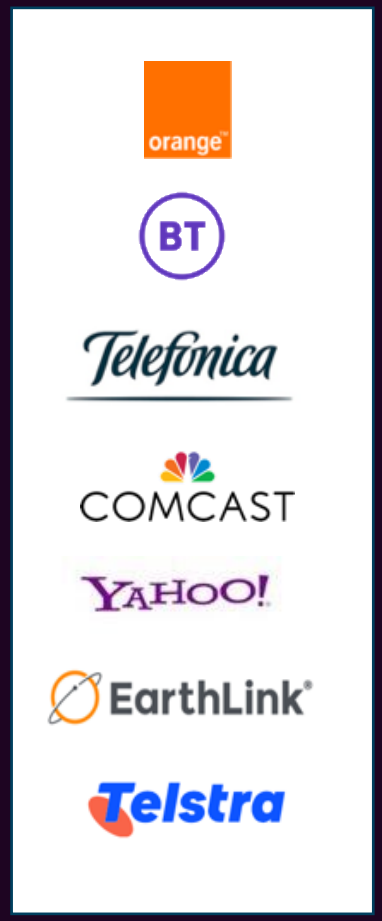
趣味　　長距離の自転車大会(1,200kmとか、2,000kmとか)
バンド演奏

主な活動　　M³AAWG
JPAAWG
迷惑メール対策推進協議会
Audax Randonneurs Nihonbashi

# HONET SECURITY (VADE JAPAN)とは

| | |
|---|---|
| **設　立** | 2009年、フランス共和国リールにて設立<br>2024年 3月 ドイツ Hornetsecurityのグループとなる |
| **拠　点** | ドイツ、フランス、アメリカ、カナダ、スペイン、イギリス、イタリア、北マケドニア、マルタ、日本 |
| **社員数** | 約700名 ※Hornetsecurityグループ |
| **国　内** | 2017年に日本市場に参入。日本国内にスレッドセンター設立 |
| **顧客数** | エンドユーザ 約75,000社　／ パートナー 12,000社 |

# 保護しているメールボックス数




14億

全世界

1.5億

日本

HORNETSECURITY

# 本日のトピック

- メールの仕組みのおさらい
- DMARCって何？
- メールが届かなくなる？
- DMARCのポリシー
- DMARCの対応状況　世界、日本、JPAAWG
- DMARCの設定・よくある間違い
- DMARCレポートの使い方
- BIMIって美味しいの?

HORNETSECURITY

HORNETSECURITY

# メールは古い

# メールはここから始まった RFC821, RFC822

RFC 821

SIMPLE MAIL TRANSFER PROTOCOL

Jonathan B. Postel

August 1982

Information Sciences Institute
University of Southern California
4676 Admiralty Way
Marina del Rey, California 90291

(213) 822-1511

RFC # 822

Obsoletes: RFC #733 (NIC #41952)

**STANDARD FOR THE FORMAT OF**

ARPA INTERNET TEXT MESSAGES

August 13, 1982

Revised by

David H. Crocker

Dept. of Electrical Engineering
University of Delaware, Newark, DE 19711
Network: DCrocker @ UDel-Relay

HORNETSECURITY

# RFC821, RFC822

RFC 821

SIMPLE MAIL TRANSFER PROTOCOL

Jonathan B. Postel

August 1982

August 1982

Information Sciences Institute
University of Southern California
4676 Admiralty Way
Marina del Rey, California 90291

(213) 822-1511

RFC # 822

Obsoletes: RFC #733 (NIC #41952)

RFC733を廃止

RFC733は1977年

**STANDARD FOR THE FORMAT OF**

ARPA INTERNET TEXT MESSAGES

August 13, 1982

August 13, 1982

Revised by

David H. Crocker

Dept. of Electrical Engineering
University of Delaware, Newark, DE 19711
Network: DCrocker @ UDel-Relay

HORNETSECURITY

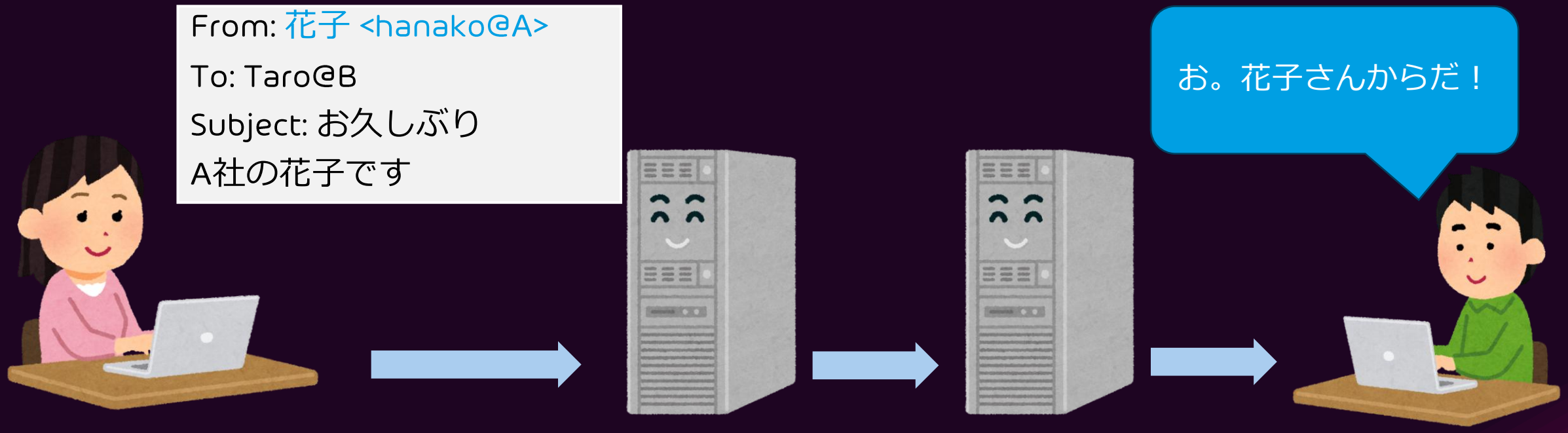
# DAVID H. CROCKER


HORNETSECURITY

HORNETSECURITY

# メールは
# なりすませるのか

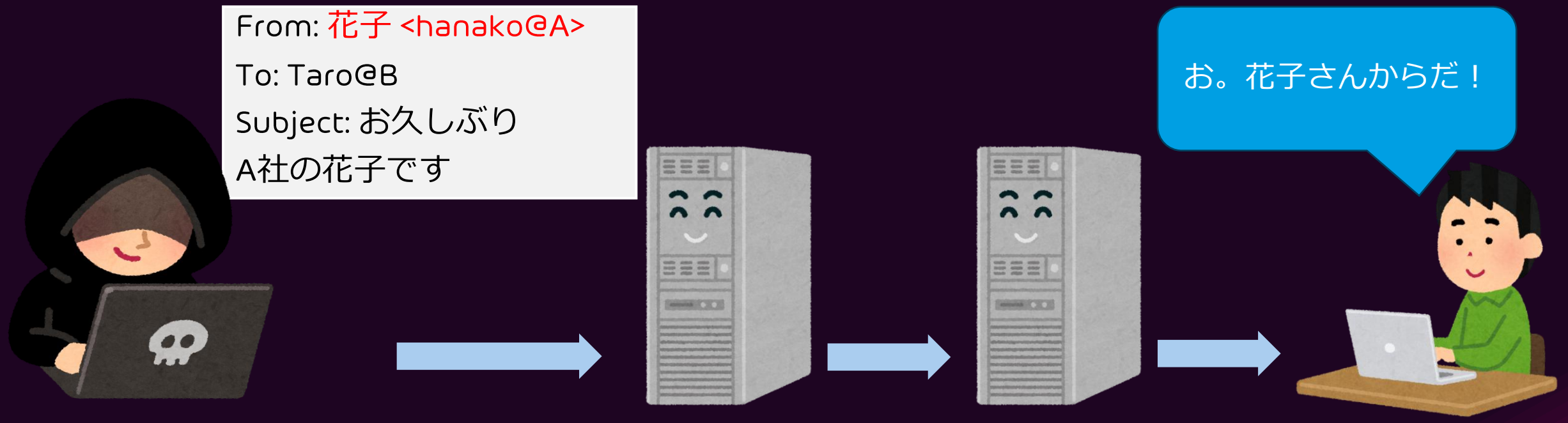
# メール配信の仕組み



# 表示名のなりすまし


自分のメールアドレスで
表示名だけなりすます

# メールアドレスもなりすまし

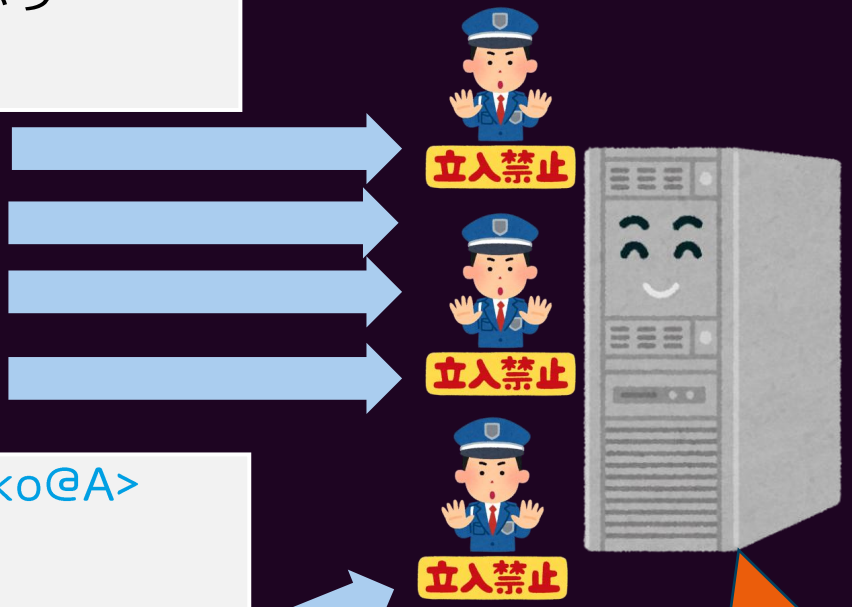



メールアドレスも
なりすます

# なりすまされた結果

C組織の悪い人

From: 花子 <hanako@A>
To: Taro@B
Subject: お久しぶり
金出せ、金




最近、花子さんから
来ないなぁ。

B社の太郎さん

A社の花子さん

From: 花子 <hanako@A>
To: Taro@B
Subject: お久しぶり
A社の花子です

A社からはスパム
ばっかりやな。
ブロックや！

HORNETSECURITY

何もしなければ

メールはなりすまし放題

メールも届かなくなる

HORNETSECURITY

HORNETSECURITY

# DMARCが必要

# DMARCがないと?

- 自社のメールアドレスがなりすまされる
  - 怪しいメールを受けた人から問い合わせが来る
  - 周りに迷惑をかける

- 本物のメールも信用してもらえない
  - メールを受け取ってもらえない
  - ログイン認証や発注確認のメールが届かず システムが機能しない

HORNETSECURITY

# 取引先の安藤さん(仮名)にメールが届く

**「取引口座の変更のお知らせ」**

取引先の安藤様

いつもお世話になっております。
Hornetsecurityの平野です。
Vade Japanから社名が変わりましたので
9月末締めの分を至急新しい口座に振り
込んでください。

受信者
取引先の
安藤さん(仮名)


ドメインが
hornetsecurity.com
なので本物だな。
よしよし。

※ この話は**フィクションです**。実在の人物や団体などとは関係ありません。

HORNETSECURITY

# 1カ月後

Hornetsecurity
新井原さん (仮名)

Hornetsecurity
平野 (仮名)

取引先から
先月分
振り込まれてないよ

ひどいっすね。
確認します。

HORNETSECURITY

# 取引先の安藤さん(仮名)に確認

先月分、
振り込まれて
ないんですけど。

**「取引口座の変更のお知らせ」**

取引先の安藤様

いつもお世話になっております。
Hornetsecurityの平野です。
Vade Japanから社名が変わりましたので
6月末締めの分を至急新しい口座に振り込んでください。

あ、先月、平野さんから
言われた新しい口座に
振りこんでおきましたよ。

HORNETSECURITY

# DMARCがないと

送信者
つまり攻撃者


送信者（Hornet 平野）を詐称

hirano@horetsecurity.com

これはメールプロトコル上では
問題ない

**「取引口座の変更のお知らせ」**

取引先の安藤様

Hornetの平野です。
お金ください。

受信者
取引先の
安藤さん

HORNETSECURITY

# DMARCがあると

送信者
つまり攻撃者


送信者（Hornet 平野）を詐称

hirano@horetsecurity.com

これはメールプロトコル上では
問題ない

HornetのDNS

「インターネットの皆様へ

弊社を名乗るメールで、DMARC認証に失敗したメールは、受信拒否して(p=reject)」

**のお知らせ」**

取引先の安藤様

Hornetの平野です


取引先のメールサーバ

「Hornetさんの宣言に従い、DMARCに失敗したのでこのメールは受信拒否します。」

HORNETSECURITY

# DMARCがないと受け取ってもらえない

# 2023年10月3日
# 米Yahoo, Gmailが大量送信者に厳しくすると発表

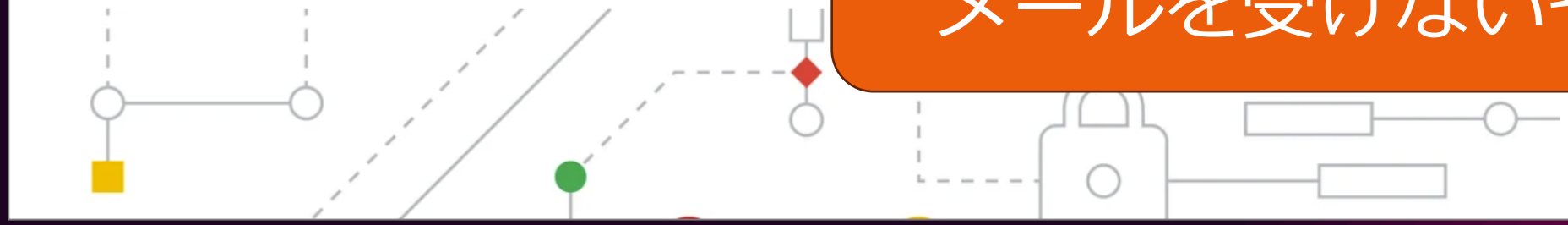
GMAIL

## New Gmail protections for a safer, less spammy inbox

Starting in 2024, we'll require bulk senders to authenticate their emails, allow for easy unsubscription and stay under a reported spam threshold.

Oct 03, 2023 · 2 min read

N **Neil Kumaran**
Group Product Manager, Gmail Security & Trust



DMARCを書いていないと
メールを受けないぞ！

HORNETSECURITY

# Microsoftも追随　2025年５月

TECH+ Powered by マイナビニュース

検索する

企業IT　テクノロジー　導入事例

TECH+ ＞ 企業IT ＞ 開発/エンジニア ＞ Microsoft、5月5日よりSPF、DKIM、DMARCに準拠しないメールの受信拒否

## Microsoft、5月5日よりSPF、DKIM、DMARCに準拠しないメールの受信拒否

掲載日 2025/04/14 11:46　更新日 2025/04/23 18:34　著者：杉山貴章

サイバーセキュリティ

Microsoftは2025年5月5日より、outlook.com、hotmail.comおよびlive.comのメール認証基準を強化し、SPF、DKIM、DMARC設定の要件に準拠しないメッセージを迷惑メールとして排除する。これはGmailやYahoo!メールが採用した基準と同等のもので、1日に5,000通を超えるメールを送信するドメインに対して適用される。ユーザーの安全性と信頼性を向上させることが目的で、スパム（迷惑メール）やフィッシングによる被害の軽減につながる。

詳細は、Microsoft Defender for Office 365 Blogの次の記事にまとめられている。

- Strengthening Email Ecosystem: Outlook's New Requirements for High - Volume Senders | Microsoft Community Hub

Register　Sign In

MICROSOFT DEFENDER FOR OFFICE 365 BLOG　5 MIN READ

## Strengthening Email Ecosystem: Outlook's New Requirements for High-Volume Senders

Puneeth MICROSOFT
Apr 03, 2025

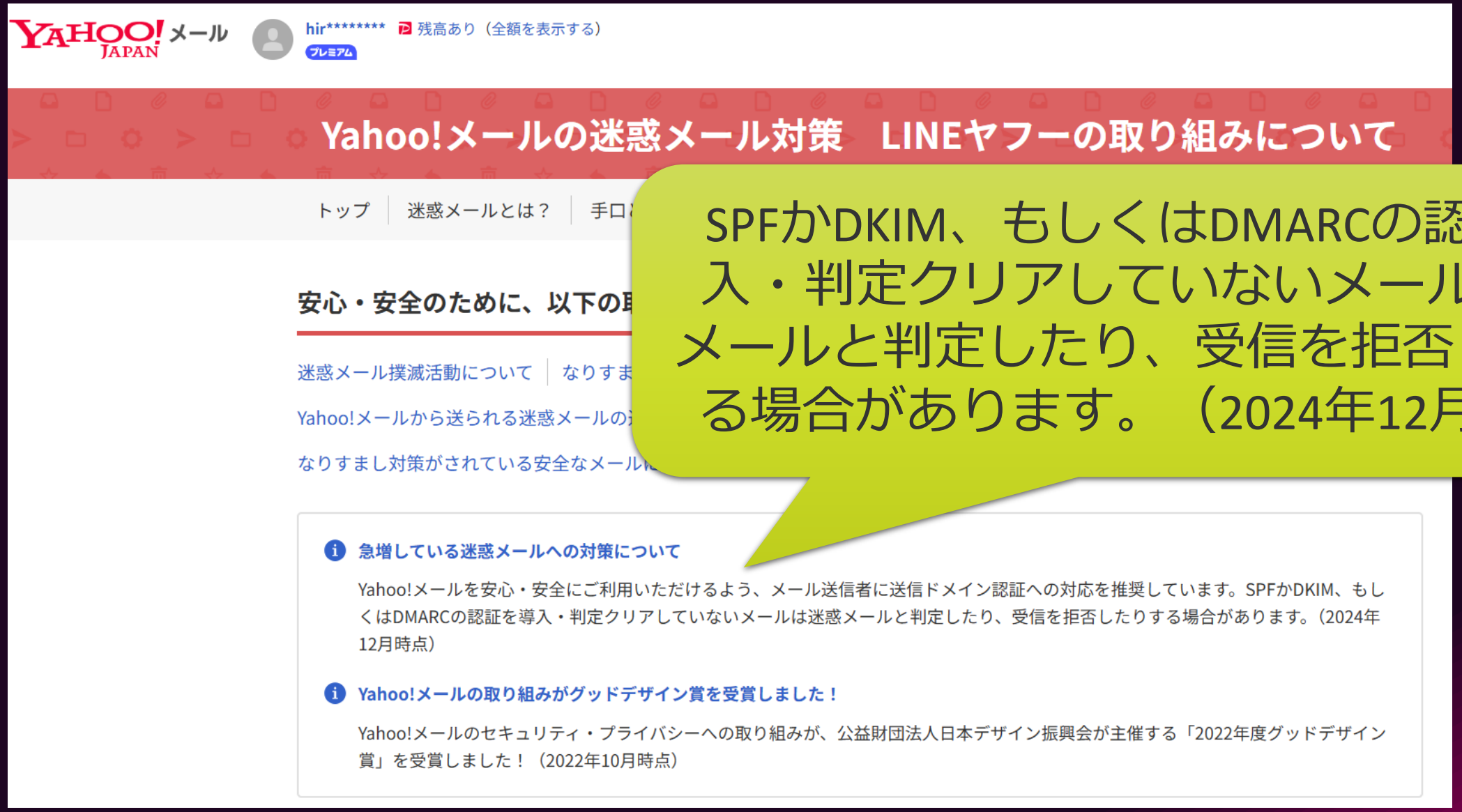
This applies to Outlook.com - our consumer service, which is supporting hotmail.com live.com and outlook.com consumer domain addresses.

***April 29th Update - Changes have been made to the action take on messages that do not meet requirements, please see details below.***

Google, Yahooとおおよそ同じ

HORNETSECURITY

# Yahoo! JAPANメール の対策




HORNETSECURITY

# ドコモメールの警告表示

## ドコモメールへメールを送信する際の注意事項

### メール送受信する際の注意事項

メールの送信方法が適切でないために、着信遅延や不達などが
ここでは、メールを効率よく円滑に送信いただくために、送信
す。
iモード・spモードのメールサービスは、複数の要因により、着
緊急を要する情報（速報、警報など）を送信される場合には、
段をご検討いただくことをお勧めします。

### 1. 送信ドメイン認証DMARCを導入してください

DMARCの認証に成功していない場合ドコモメールに警告が表示されます。
また、認証に成功していない場合はメールが届かない場合があります。

#### 対処策

送信ドメイン認証を正しく導入し、認証が成功するよう設定をお願いいたします。

DMARCの認証に成功していない場合
ドコモメールに警告が表示されます。
また、認証に成功していない場合は
メールが届かない場合があります。
（2025年1月）

HORNETSECURITY

# 対策は?

A. ドメインをホワイトリストに入れてください
と告知する

B. DMARCでp=rejectを設定し
なりすましメールは届かないようにする

HORNETSECURITY

# 対策は?

A. ドメインをホワイトリストに入れてください
と告知する

B. DMARCでp=rejectを設定し
なりすましメールは届かないようにする

HORNETSECURITY

HORNETSECURITY

# DMARCのポリシー

# DMARCのポリシー

- p=reject
  - うちのドメインのなりすましメールは捨ててね

- p=quarantine
  - うちのドメインのなりすましメールは隔離してね

- p=none
  - うちのドメインをなりすましたメールも、
    いつも通り届けてね

HORNETSECURITY

# p=noneは何のため?

- DMARC p=noneはDMARCがないのと変わらない
- 本来はレポートを分析しモニタリングするため

  - 自社のメールがどこから出ているのか棚卸しする
  - p=rejectにしたときに、届くべきメールが届くか

  - なりすましがどこから配送されているか
  - 受信者が転送しているか

# なぜDMARC p=rejectが必要なのか

- 攻撃者はDMARCの設定が弱いところをなりすましてメールを送る。

会社のメールが届かなくなる

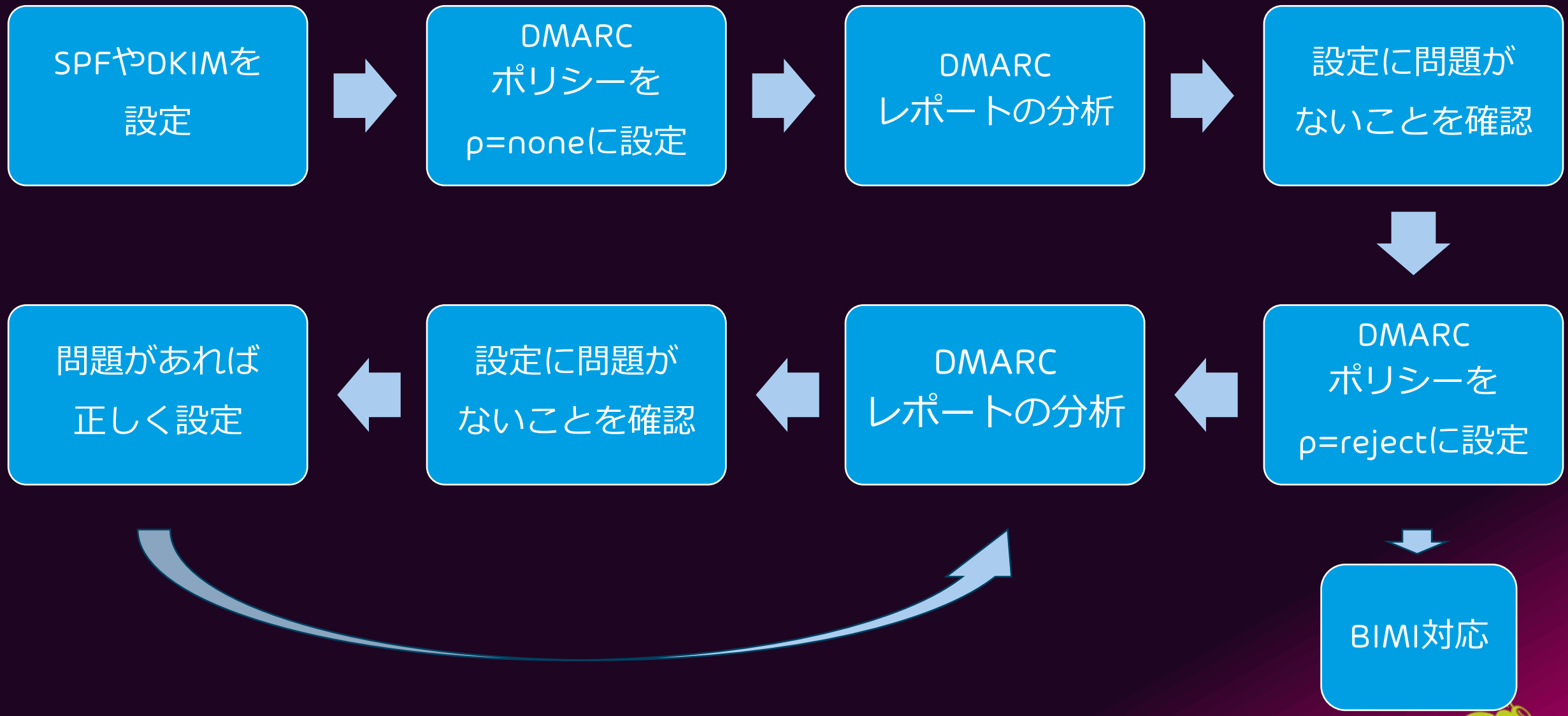
会社のブランドイメージが毀損する

会社に問い合わせが来る

p=none
では不十分

HORNETSECURITY

# DMARC安定運用までの流れ




HORNETSECURITY

HORNETSECURITY

# DMARCの普及状況

# 日本は周回遅れで滅びる！(2020年)


https://weekly-economist.mainichi.jp/articles/20201103/se1/00m/020/061000c

HORNETSECURITY

# オランダの場合

Meting Informatieveiligheidstandaarden overheid maart 2020
(政府情報セキュリティ基準の測定2020年3月)

| Implementatie-deadline | Betreffende standaarden |
|---|---|
| uiterlijk EIND 2017 | TLS/HTTPS: beveiligde verbindingen van (transactie)websites<br>DNSSEC: domeinnaambeveiliging<br>SPF: anti-phishing van email<br>DKIM: anti-phishing van email<br>DMARC: anti-phishing van email |
| uiterlijk EIND 2018 | HTTPS, HSTS en TLS conform de NCSC richtlijn (externe link): beveiligde verbindingen van alle websites |
| uiterlijk EIND 2019 | STARTTLS en DANE: encryptie van mailverkeer<br>SPF en DMARC: het instellen van strikte policies voor deze emailstandaarden |

遅くとも
2017年末まで

遅くとも
2018年末まで

遅くとも
2019年末まで

DNSSEC

SPF

DKIM

DMARC

STARTTLSとDANE

SPFとDMARC
厳しいポリシー

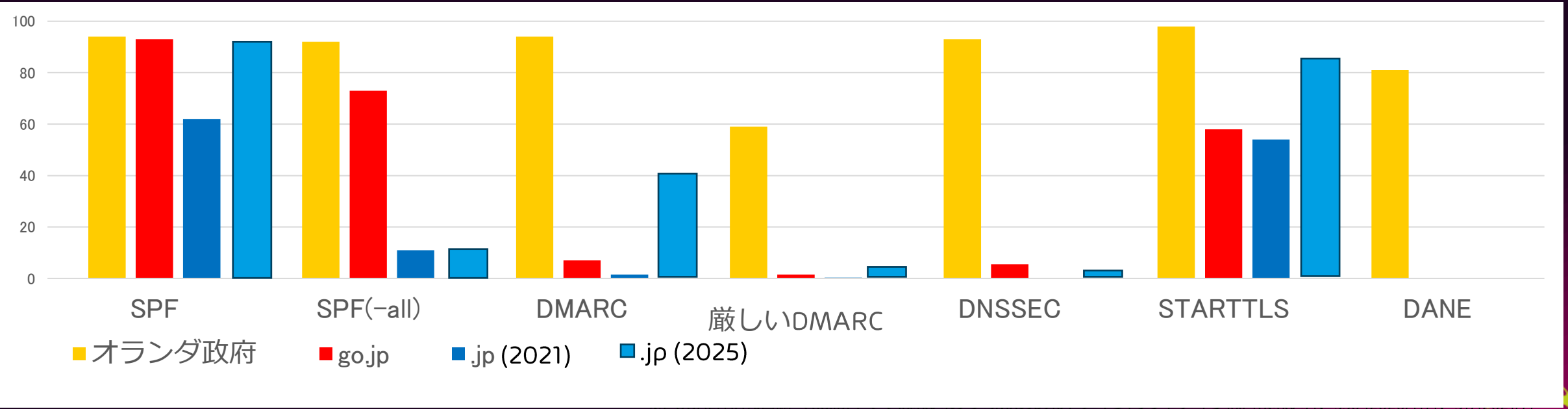
https://magazine.forumstandaardisatie.nl/meting-informatieveiligheidstandaarden-begin-2020

https://www.forumstandaardisatie.nl/sites/bfs/files/rapport-meting-informatieveiligheidstandaarden-maart-2020.pdf (当時)

HORNETSECURITY

# オランダと日本の比較

| | SPF | SPF -all | DMARC | 厳しい DMARC | DNSSEC | START TLS | MTA-STS | DANE |
|---|---|---|---|---|---|---|---|---|
| オランダ政府(2020/3) (※1) | 94% | 92% | 94 % | 59 % | 93 % | 98% | - | 81% |
| go.jp (2021/7) (※2) | 94% | 74% | 7.3% | 0.9% | 6.0 % | 63% | 0% | 0% |
| .jp (2021/7) (※4) | 71% | 14% | 2.3% | 0.3% | 0.10% | 64% | 18件 | 6件 |
| .jp (2025/10) (※4) | 92% | 16% | 41 % | 14 % | 1.4 % | 85% | 250件 | 221件 |



# DMARC普及率

- DMARC設定あり

| Hornet調査の平均 | JPAAWG2024参加者 | アンケート回答者 |
|---|---|---|
| 41% | 84% | 62% |

- DMARC設定なし

| Hornet調査の平均 | JPAAWG2024参加者 | アンケート回答者 |
|---|---|---|
| 59% | 16% | 38% |

Hornet調査の平均
N=約20万ドメイン

JPAAWG2024参加者
N=272ドメイン

アンケート回答者
N=29ドメイン

HORNETSECURITY

# ポリシー別DMARC普及率

| | Hornet調査の平均 | JPAAWG2024参加者 | アンケート回答者 |
|---|---|---|---|
| p=reject | 2% | 16% | 17% |
| p=quarantine | 4% | 22% | 13% |
| p=none | 35% | 46% | 32% |
| DMARCなし | 59% | 16% | 38% |

N=約20万ドメイン

N=272ドメイン

N=29ドメイン

HORNETSECURITY

# 無料で診断します！

リモートの方


１分で
DMARC診断
が可能！

ブースにて
その場で診断書を
お渡しします。

HORNETSECURITY

## hornetsecurity.com様 DMARC診断結果

DMARC（送信ドメイン認証）対応、どこまでできていますか？

| SPF | DMARC | DMARC レポート | DMARC p=reject | BIMI |
|---|---|---|---|---|
| ▲ | ✓ | ✓ | ✓ | ✓ |

### 詳細情報

#### SPF

| 項目 | 結果 | 備考 |
|---|---|---|
| SPF設定 | SPFが設定されています。 | v=spf1 redirect=hornetsecurity.com.spf.hornetdmarc.com |
| レコード数 | OK | |
| バージョン | OK | |

HORNETSECURITY

HORNETSECURITY

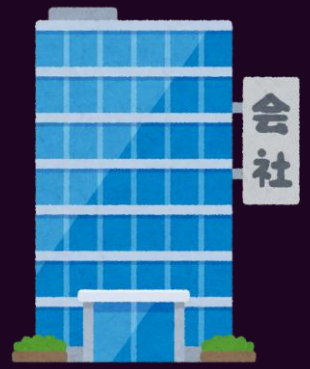
# DMARCの仕組み

# DMARCとは

- SPF・DKIMの検証が両方失敗したときに
  どうして欲しいかを宣言する仕組み

- ただし、ふつうのSPFやDKIMとはちょっと違う

# SPFとは




自社 192.0.2.0/28

① IPアドレスを登録


- 192.0.2.0/28
- _spf.sender.example.jp

悪い人 203.0.113.4

⑤ 送信


④ 確認

② 送信

③ 送信

メール配信業者 _spf.sender.example.jp

HORNETSECURITY

# DKIMとは


① 登録


② 預ける

③ 送信

④ 送信

メール配信業者

送信元も
改ざんされ
ていない

悪い人

⑤ 確認

送信 ⑥

なりすまし
ているかも

ハンコがない

HORNETSECURITY

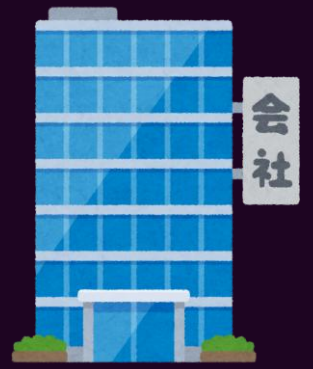
# なぜSPF, DKIMだけではだめなのか

- SPF
  - ヘッダの送信者(メールソフトに表示されるアドレス)は参照しない

- DKIM
  - 署名者は誰でもいい (悪い人でも署名できる)
  - ヘッダの送信者とは関係ない

HORNETSECURITY

# SPFは なりすませる




自社 192.0.2.0/28

登録


- 192.0.2.0/28
- _spf.sender.example.jp

悪い人 203.0.113.4

登録


- 203.0.113.4

送信

確認

確認

送信

メール配信業者 _spf.sender.example.jp

送信

HORNETSECURITY

# DKIMも なりすませる


登録


悪い人


預ける

送信

確認

送信

確認

メール配信業者

送信

送信元も
改ざんされ
ていない

送信元も
改ざんされ
ていない

改ざん ≠ なりすまし

HORNETSECURITY

# DMARCのSPF, DKIM

- DMARCのSPF
  - 通常のSPFに加えて
  - ヘッダFromのドメインがSPFのドメインと同じ

- DMARCのDKIM
  - 通常のDKIMに加えて
  - ヘッダFromのドメインがDKIM署名者と同じ

悪い人は
送信ドメインの
なりすましではきない

HORNETSECURITY

HORNETSECURITY

# 実際の設定

# DMARCの設定は難しい？

- 「何をやったらいいのかさっぱりわからない」
- 「用語だけで頭が爆発しそう」

- 「DNSパパッと書くだけだよ」
- 「ちょっと勉強すればすぐ慣れる感じやね」

- 「ミスするとめんどくさいから、慎重にやった方がいいよ」

HORNETSECURITY

HORNETSECURITY

# SPFの設定

# SPFの設定方法

- DNSのTXTレコードにメール送信サーバーのIPアドレスを記述
- 別のSPFレコードをincludeすることも可能

- 送信サーバー：192.0.2.25
- 配信事業者の指定のSPF: _spf.sender.example.jp

```
example.com.  TXT  "v=spf1 ip4:192.0.2.25 include:_spf.sender.example.jp -all"
```

HORNETSECURITY

# Question: どのSPFレコードが正しいですか

1. v=spf1 include:192.0.2.25 -all
2. v=spf1 192.0.2.25 -all
3. v=spf1 ip:192.0.2.25 -all
4. v=spf1 ipv4:192.0.2.25 -all

HORNETSECURITY

# Question: どのSPFレコードが正しいですか

1. v=spf1 include:192.0.2.25 -all
2. v=spf1 192.0.2.25 -all
3. v=spf1 ip:192.0.2.25 -all
4. v=spf1 ipv4:192.0.2.25 -all

v=spf1 ip4:192.0.2.25 -all

HORNETSECURITY

HORNETSECURITY

# よくある
# SPFの間違い

# レコードが複数登録されている

example.jp. TXT “v=spf1 ip4:192.0.2.25 -all”

example.jp. TXT “v=spf1 include:_spf.example.com -all”

SPFレコードは1つしか書けません

# 文法間違い

v=spf1 +ip4:192.0.2.1 +ip4:192.0.2.2+ip4:192.0.2.2 ~all

空白がない

v=spf1 ip4:192.0.2.1 v=spf1 ip4:192.0.2.2 -all

v=spf1が2回ある

v=spf1 ip4=192.0.2.1  mx ~all

= になっている

v=spf1 +ip4:  219.94.128.76 −all

スペースは不要

不要なinclude:

v=spf1 include:spf.protection.outlook.com include:+ip4:192.0.2.1/32 −all

v=spf1 inciube:spf.protection,outlook.com include:spf.example.jp ~all MS=ms12345678

includeのスペルミス

ピリオドではなく
コンマ

別のTXTレコードが
混ざっている

HORNETSECURITY

# SPFのinclude数の制限

- SPFはDNSの参照が10回までしかできない

HORNETSECURITY

# DNSの参照は何回でしょう

v=spf1 ip4:1920.2.1 ip4:192.0.2.2 ip4:192.0.2.3 ip4:192.0.2.4 -all

0回

HORNETSECURITY

# DNSの参照は何回でしょう

```
v=spf1 include:_spf.google.com -all
```

1回?

HORNETSECURITY

# DNSの参照は何回でしょう

①

```
v=spf1  include:_spf.google.com  -all
```

②

```
_spf.google.com.  TXT    "v=spf1 include:_netblocks.google.com
include:_netblocks2.google.com ~all"
```

③

3回

HORNETSECURITY

# 実はつい最近まで

① v=spf1 include:_spf.google.com -all

② _spf.google.com. TXT "v=spf1 include:_netblocks.google.com include:_netblocks2.google.com include:_netblocks3.google.com ~all"

③ ④

4回

HORNETSECURITY

# SPFのincludeができない場合

- SPFはincludeが存在しない場合、エラーになる

```
v=spf1 include:ok1.example.jp include:ng.example.com include:ok2.example.jp -all
```

ok2.example.jpは参照されない

2回までは許容される (default)

# Typosquatting

```
example.jp TXT “v=spf1 include:spf1.example.jp include:spf2.example.com -all”
```

example.jpの書き間違い

- example.comのドメインを購入
- spf2.example.comに自分のサーバーのIPを記述
- example.jpをなりすまして送信

HORNETSECURITY

# SPFを設定したと思っているけど

# 2.5%

期待通り動作していない

HORNETSECURITY

# SecurityDays東京での出展企業
# (SPFを設定したと思っているけど)

# 5.6%

期待通り動作していない

HORNETSECURITY

# 無料で診断します！

リモートの方


１分で
DMARC診断
が可能！

ブースにて
その場で診断書を
お渡しします。

HORNETSECURITY

## hornetsecurity.com様 DMARC診断結果

DMARC（送信ドメイン認証）対応、どこまでできていますか？

| SPF | DMARC | DMARC レポート | DMARC p=reject | BIMI |
|---|---|---|---|---|
| ▲ | ✓ | ✓ | ✓ | ✓ |

### 詳細情報

#### SPF

| 項目 | 結果 | 備考 |
|---|---|---|
| SPF設定 | SPFが設定されています。 | v=spf1 redirect=hornetsecurity.com.spf.hornetdmarc.com |
| レコード数 | OK | |
| バージョン | OK | |

HORNETSECURITY

# こんな感じのレポートです

リモートの方


## SPF

| 項目 | 結果 | 備考 |
|---|---|---|
| SPF設定 | SPFが設定されています。 | v=spf1 redirect=hornetsecurity.com.spf.hornetdmarc.com |
| レコード数 | OK | |
| バージョン | OK | |
| 文法 | OK | |
| DNS参照回数 | DNSの参照回数は10回です。<br>includeなどのDNSの参照回数がすでに上限です。現在は問題ありませんが、上限は10回ですので、次にinclude等を追加するときには注意が必要です。<br>DMARC ManagerのSPFフラット化機能をご利用ください。 | redirect=hornetsecurity.com.spf.hornetdmarc.com<br>└ include:aspmx.pardot.com<br>└ include:et._spf.pardot.com<br>└ include:amazonses.com<br>└ include:emsd1.com<br>└ include:spf.hornetsecurity.com<br>└ include:_spf.salesforce.com<br>└ exists:%{i}._spf.mta.salesforce.com<br>└ include:spf.protection.outlook.com<br>└ include:mail.zendesk.com |
| includeなどの参照可否 | OK | |
| includeのループ | OK | |
| Includeの重複 | OK | |

HORNETSECURITY

HORNETSECURITY

# DMARC
# 安定運用のために

# p=rejectやqurantineにできない理由

- メールが送信できなくなると困る (31%)
  - 怖い
  - クレームになる
  - 影響が分からない
  - 調査できていない
  - 転送やメーリングリストに影響の可能性
- DMARCが未導入だから (24%)
- 検証時間がないから (20%)
- 移行する判断材料がないから (13%)
- 必要性が分からない（p=noneで十分だと考えている）から (10%)
- 社内調整が面倒だから (10%)

アンケート結果より

HORNETSECURITY

HORNETSECURITY

# DMARC Reportの分析

# DMARCレポート受信率

| | Hornet調査の平均 | JPAAWG2024参加者 | アンケート回答者 |
|---|---|---|---|
| p=none | 25% | 75% | 33% |
| p=quarantine | 46% | 85% | 50% |
| p=reject | 62% | 91% | 80% |
| | N=約8.2万ドメイン | N=231ドメイン | N=18ドメイン |

HORNETSECURITY

# レポート分析の目的

## p=noneのとき

- 正しく配送されるべきメールの
  SPFやDKIMの設定漏れを見つける
- 漏れているものを正しく設定する
- 漏れがなければ、p=rejectにしても安心

## p=rejectのとき

- 新規の「漏れ」がないかを定期的にモニタリング

HORNETSECURITY

# DMARCレポートは難しい

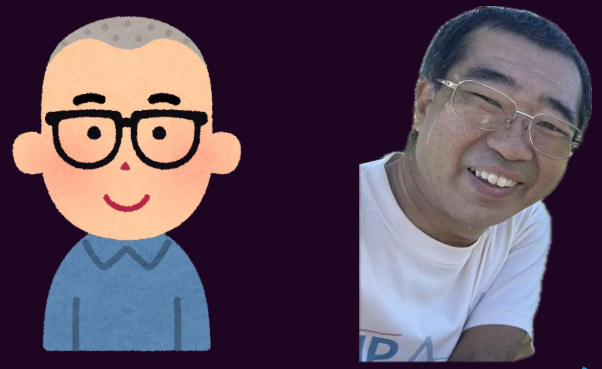
- メールに添付されて送られてくる
- 形式はXML
- gzipやzipで圧縮されている
- あちこちから送られてくる
- あまり欲しい情報が書かれていない
  - 送信メールアドレス、件名などはない。

# DMARCレポートの仕組み

Hornetsecurity

メール受信業者

悪い人



Hornet の社員

受信業者 A

受信業者 B

受信業者 C

受信業者 D


送信元ドメインは
hornet

分析する人


配信業者


Web Hosting

HORNETSECURITY

# レポートの例

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
 <report_metadata>
  <org_name>google.com</org_name>
  <email>noreply-dmarc-support@google.com</email>
  <extra_contact_info>https://support.google.com/a/answer/2466580</extra_contact_info>
  <report_id>15001962018631710439</report_id>
  <date_range>
   <begin>1721347200</begin>
   <end>1721433599</end>
  </date_range>
 </report_metadata>
 <policy_published>
  <domain>orcaland.gr.jp</domain>
  <adkim>r</adkim>
  <aspf>r</aspf>
  <p>reject</p>
  <sp>reject</sp>
  <pct>100</pct>
  <np>reject</np>
 </policy_published>
 <record>
  <row>
   <source_ip>210.158.71.75</source_ip>
   <count>2</count>
   <policy_evaluated>
    <disposition>none</disposition>
    <dkim>fail</dkim>
    <spf>pass</spf>
   </policy_evaluated>
  </row>
  <identifiers>
   <header_from>orcaland.gr.jp</header_from>
  </identifiers>
  <auth_results>
   <spf>
    <domain>orcaland.gr.jp</domain>
    <result>pass</result>
   </spf>
  </auth_results>
 </record>
</feedback>
```

HORNETSECURITY

# DMARCレポートに書かれている情報

```
<record>
  <row>
    <source_ip>210.158.71.75</source_ip>
    <count>2</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>fail</dkim>
      <spf>pass</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>orcaland.gr.jp</header_from>
  </identifiers>
  <auth_results>
    <spf>
      <domain>orcaland.gr.jp</domain>
      <result>pass</result>
    </spf>
  </auth_results>
 </record>
```

送信元IPアドレス

通数

適用されたDMARCのポリシー

DMARCのDKIM, SPFの結果

ヘッダFromのドメイン

SPFの検証に使用したドメイン

SPFの結果

HORNETSECURITY

# レポートから棚卸し

- A: 自社管理のサーバーや送信業者からのメール (DMARC成功)
- B: 自社管理のサーバーや送信業者からのメール (DMARC 失敗)
- C: なりすましメール (DMARC失敗)
- D: 転送されてるかもしれないメール (DKIM成功、SPF失敗)
- E: 転送されてるかもしれないメール (DKIMもSPFも失敗)

BをAになるようにする
Eが多い場合、p=noneで留めることも検討
Eはp=quarantine以上にするとなくなるかもしれない

# どのサーバーかわかるようにする

- 元データと外部データベースを紐づけて、素のDMARCレポートには無かった情報を付与

**素のDMARCレポート**

IP アドレス

**様々なデータを取得**

- IPアドレス
- DNSの逆引き名
- ASN
- IPアドレスの保有事業者名
- ロゴ
- 事業者のタイプ
- ブラックリスト突合
- 国・地域

HORNETSECURITY

# レポート分析ツールの例

送信ISP毎に表示

| 送信元 | IP アドレス | DMARC準拠 | メール数 | パス | 失敗 | 転送 | カテゴリ |
|---|---|---|---|---|---|---|---|
| ITEC HANKYU HANSHIN CO.,LTD. Other | 2 | 99.5% | 209 | 208 | | | ソースの分析中... |
| Hornetsecurity GMBH メールフィルター | 44 | 100.0% | 53 | 0 | 53 | 0 | 承認済 |
| Google, LLC メールボックスプロバイダー | 1 | 100.0% | 24 | 0 | 24 | | しい |
| Register Hosting Italy ホスティング | 3 | 100.0% | 4 | 0 | 4 | 0 | なし |
| ASN-GIGENET Other | 2 | 100.0% | 3 | 0 | 3 | 0 | ソースの分析中... |
| China Unicom ISP | 2 | 100.0% | 2 | 0 | 2 | 0 | なし |
| Strato AG Germany (Gmbh) ホスティング | 2 | 100.0% | 2 | 0 | 2 | 0 | 未承認 |
| T-Online メールボックスプロバイダー | 2 | 100.0% | 2 | 0 | 2 | 0 | 未承認 |

DMARC OK

DMARC だめ

HORNETSECURITY

# 自社管理のメール1

| 送信元 | IP アドレス | DMARC準拠 | メール数 | パス | 失敗 | 転送 | カテゴリ |
|---|---|---|---|---|---|---|---|
| ITEC HANKYU HANSHIN CO.,LTD. Other | 2 | 99.5% | 209 | 208 | 1 | 0 | ソースの分析中... |
| メール | 44 | 100.0% | 53 | 0 | | | 承認済 |
| Goog メー | | 100.0% | 24 | 0 | 24 | 0 | 疑わしい |
| Regis ホスティング | 3 | 100.0% | 4 | 0 | 4 | 0 | なし |
| ASN-GIGENET Other | 2 | 100.0% | 3 | 0 | 3 | 0 | ソースの分析中... |
| China Unicom ISP | 2 | 100.0% | 2 | 0 | 2 | 0 | なし |
| Strato AG Germany (Gmbh) ホスティング | 2 | 100.0% | 2 | 0 | 2 | 0 | 未承認 |
| T-Online メールボックスプロバイダー | 2 | 100.0% | 2 | 0 | 2 | 0 | 未承認 |

ITEC HANKYU HANSHIN には
自社のメールサーバーがある

DMARC OK

HORNETSECURITY

# 自社管理のメール2

| 送信元 | IP アドレス | DMARC準拠 | メール数 | パス | 失敗 | 転送 | カテゴリ |
|---|---|---|---|---|---|---|---|
| ITEC HANKYU HANSHIN CO.,LTD. Other | 2 | 99.5% | 209 | 208 | 1 | 0 | ソースの分析中... |
| Hornetsecurity GMBH メールフィルター | 44 | 100.0% | 53 | 0 | 53 | 0 | 承認済 |
| Google, LLC メールボックス | 1 | 100.0% | 24 | 0 | 24 | 0 | 疑わしい |
| Regis ホス | | 100.0% | 4 | 0 | 4 | 0 | なし |
| ASN- Other | | 100.0% | 3 | 0 | 3 | 0 | ソースの分析中... |
| China Unicom ISP | 2 | 100.0% | 2 | 0 | 2 | 0 | なし |
| Strato AG Germany (Gmbh) ホスティング | 2 | 100.0% | 2 | 0 | 2 | 0 | 未承認 |
| T-Online メールボックスプロバイダー | 2 | 100.0% | 2 | 0 | 2 | 0 | 未承認 |

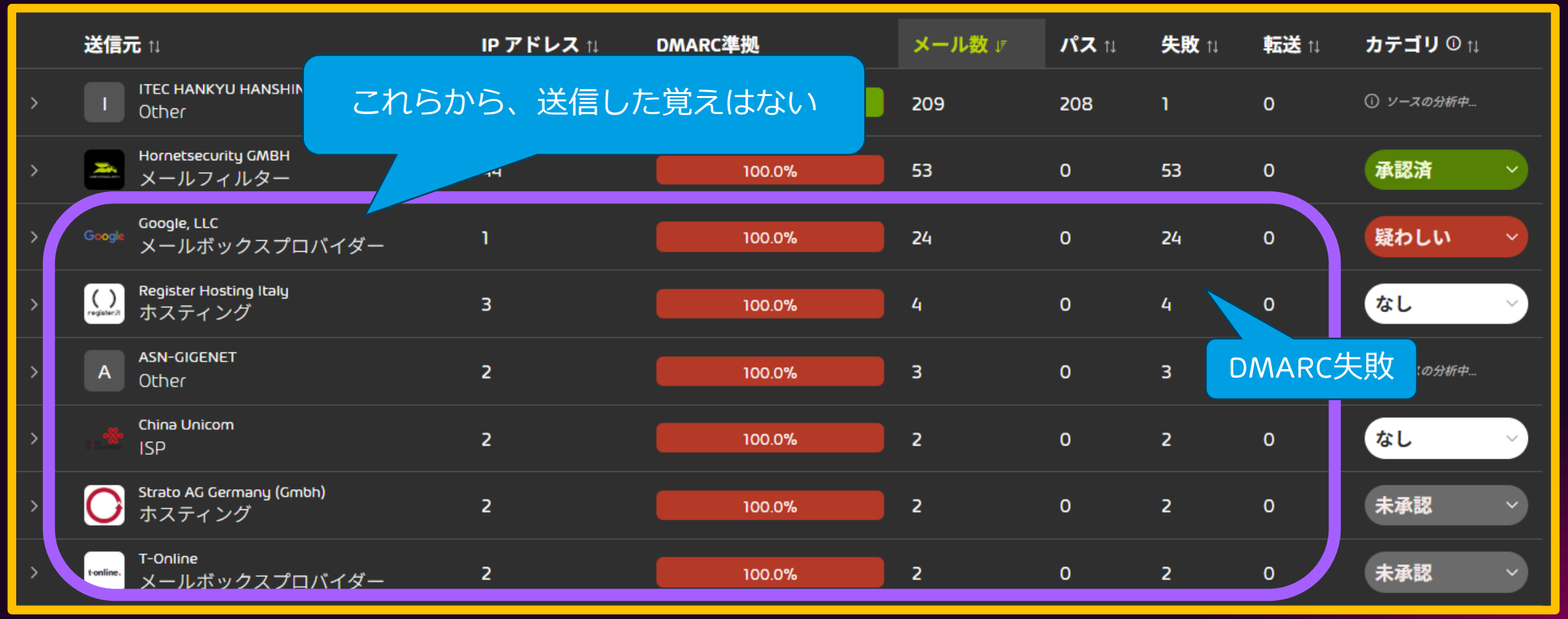
Hornetsecurity からも
自社のメールを送信している

DMARC失敗

SPFやDKIM設定の見直しが必要

HORNETSECURITY

# なりすまし




| 送信元 | IP アドレス | DMARC準拠 | メール数 | パス | 失敗 | 転送 | カテゴリ |
|---|---|---|---|---|---|---|---|
| ITEC HANKYU HANSHIN Other | | | 209 | 208 | 1 | 0 | ソースの分析中... |
| Hornetsecurity GMBH メールフィルター | | 100.0% | 53 | 0 | 53 | 0 | 承認済 |
| Google, LLC メールボックスプロバイダー | 1 | 100.0% | 24 | 0 | 24 | 0 | 疑わしい |
| Register Hosting Italy ホスティング | 3 | 100.0% | 4 | 0 | 4 | 0 | なし |
| ASN-GIGENET Other | 2 | 100.0% | 3 | 0 | 3 | | の分析中... |
| China Unicom ISP | 2 | 100.0% | 2 | 0 | 2 | 0 | なし |
| Strato AG Germany (Gmbh) ホスティング | 2 | 100.0% | 2 | 0 | 2 | 0 | 未承認 |
| T-Online メールボックスプロバイダー | 2 | 100.0% | 2 | 0 | 2 | 0 | 未承認 |

HORNETSECURITY

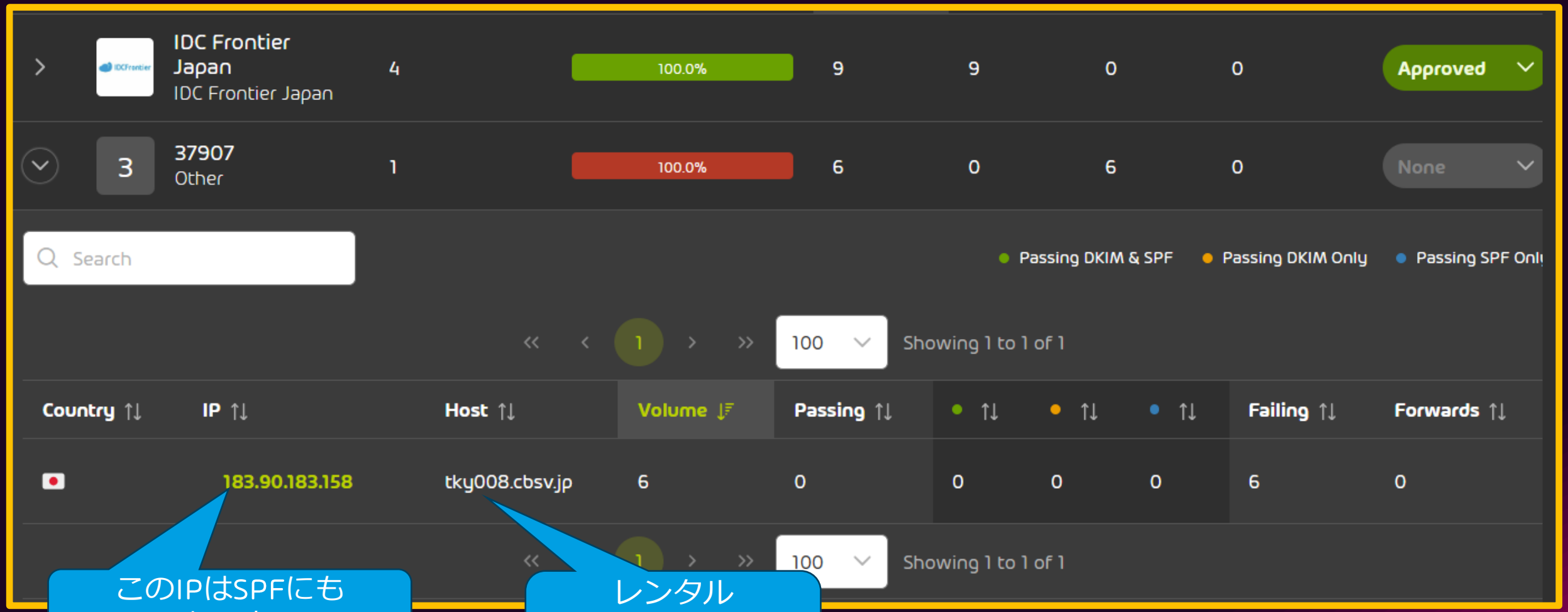
HORNETSECURITY

# 実際の例

# 実際の例 (ar-nihonbashi.org)


HORNETSECURITY

# 失敗してる部分の詳細

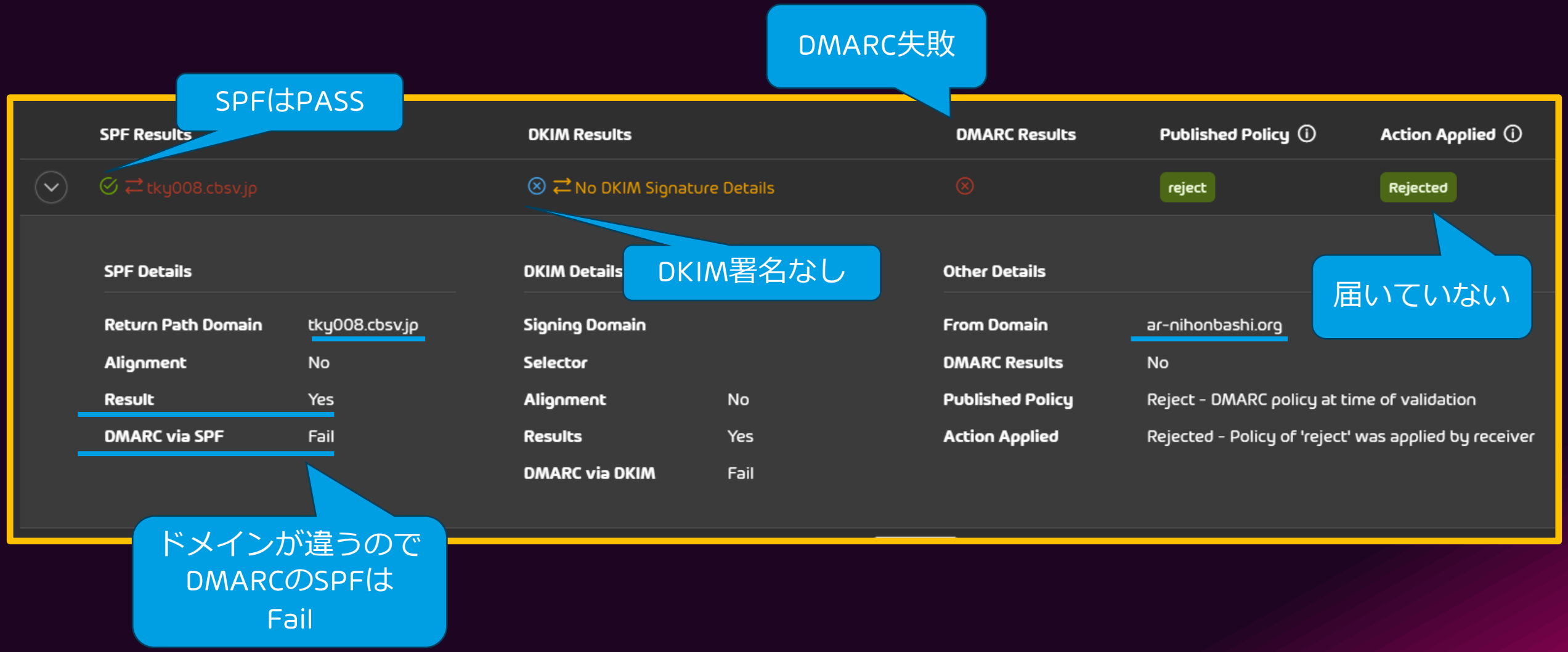



このIPはSPFにも
いれてある

レンタル
Webサーバーの
ホスト名だ

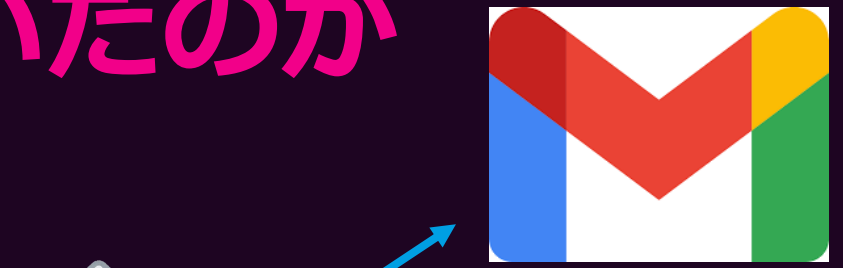
HORNETSECURITY

# さらに詳細




HORNETSECURITY

# 何が起きていたのか



正しいドメインの
SPF, DKIM


ワードプレスの
フォームからの
お知らせメール



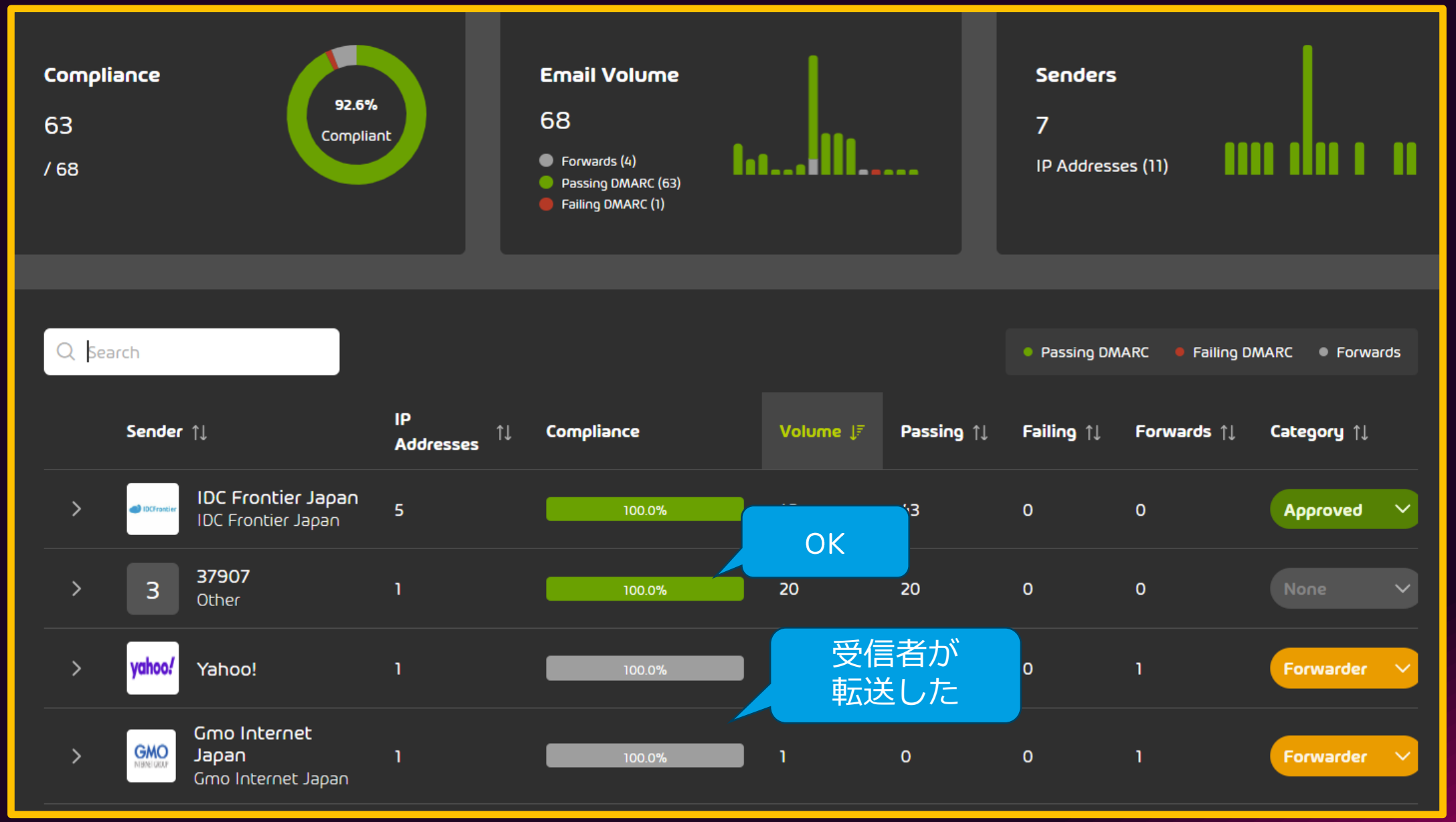
Webレンタルサーバーの
ドメインのSPF

メールサーバー


Webサーバー

HORNETSECURITY

# 無事DMARCがPASSしました




HORNETSECURITY

HORNETSECURITY

# DMARCだけで大丈夫？

# 似たようなドメインでなりすます


会社.com

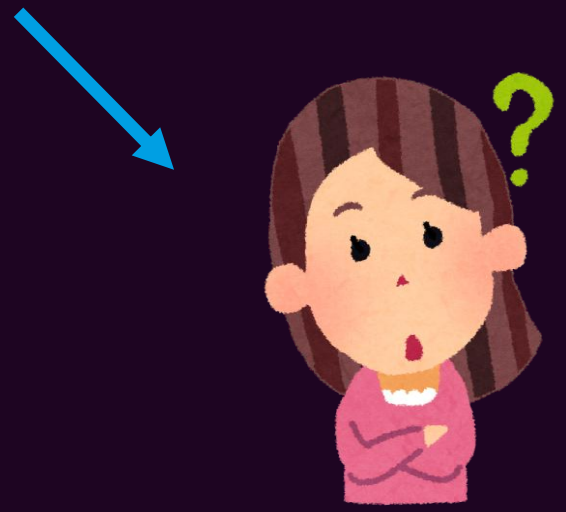
杜

会杜.com

会社.com.悪い人.com

SPFもDKIMもDMARCもバッチリだぜ





会社.com
会杜.com
会社.com.悪い人.com

HORNETSECURITY

# BIMI

- Gmailなどでロゴが表示される
- DMARC p=rejectが必要
- 登録商標が必要
- VMC証明書が必要
  - 会社の存在証明
  - 担当者の存在証明


HORNETSECURITY

# 重要なのはロゴだけではない


ドメインを所有
ロゴを所有
会社が存在
担当者が存在

HORNETSECURITY

# BIMIがあればロゴで判断できる


会社.com

杜

会杜.com

会社.com.悪い人.com

SPFもDKIMもDMARCもバッチリだぜ



- 会社.com
- 会杜.com
- 会社.com.悪い人.com

ロゴを知らなくても、
BIMIがPASSしたドメインの
信頼性はかなり高い

HORNETSECURITY

# BIMIの設定

- DMARCのポリシーを p=rejectにする
- 正方形のロゴを作成する
- ロゴを商標登録する
- ロゴをSVG Tiny P/S形式に変換する
- 証明書を取得
- ロゴをhttpsのサーバで公開する
- 証明書をhttpsのサーバで公開する

default._bimi.example.jp TXT
“v=BIMI1; l=https://../ロゴ.svg; a=https://../証明書”

HORNETSECURITY

# BIMIは美味しいのか?

# BIMIは美味?!


**Yoshitaka Hirano**

I've had BIMI on my DNS for a long time but I've never had BIMI yet. i should try. Is it like a broccoli?

**Dave Crocker**

Yoshitaka, ersatz broccoli.  Looks like it's good for your health, but really isn't.

HORNETSECURITY

HORNETSECURITY

# それでも
# 届かない?!

# 逆引きDNS

送信サーバーのIP:　192.0.2.1
逆引きDNS:　192.0.2.1 → mail.example.jp
正引きDNS:　mail.example.jp → 192.0.2.1

# 逆引きDNS (複数IP)

送信サーバーのIP:　192.0.2.1,　192.0.2.2

逆引きDNS:　192.0.2.1 → mail.example.jp

192.0.2.2 → mail.example.jp

正引きDNS:　mail.example.jp → 192.0.2.1, 192.0.2.2

# フィルタベンダーからのお願い

- 悪い人もDMARCを使います

× いきなりの大量送信
○ 少しずつ送信してIPやドメインの信頼を得る

※ 二要素認証メールなど重要な場合は、
事前に我々まで教えてください

HORNETSECURITY

HORNETSECURITY

# まとめ

# まとめ

- メールは何もしなければなりすましし放題

- 自社のブランドを守るためにも、
  他社に迷惑をかけないためにも、
  DMARCを運用し、
  p=rejectを継続的に維持する
  ことが重要

- 本当に重要なメールを大量に送るときはひと声かけてください。

HORNETSECURITY

# お知らせ

## Postfixが抱える課題を Policy Runnerで すべて解決！！

～ メール基盤に潜む「4つの課題」を解決！ ～

12月16日（火）14時～ 開催予定

- 12月16日(火) 14:00～15:00
- オンラインにて

HORNETSECURITY

# 例えば、同時接続数制限をこんな風に

```
func (p *policy) MailFrom(s *smtp.Session) *smtp.Response {
  // "default": {
  //    "Limit": 5,
  //    "Response": {
  //      "CloseSession": true,
  //      "Reason": "421 4.2.1 Service unavailable - try again later"
  //    },
  //    "Tarpit": "3s"
  // }
  n := smtp.SimultaneousSessions(s.IP.String())
  if r.Enable && n > r.Limit {
      time.Sleep(r.Tarpit.Duration)
      return &r.Response
  }
  ...
```


HORNETSECURITY

# 質疑応答

**Postfixが抱える課題を Policy Runnerで すべて解決！！**

～ メール基盤に潜む「4つの課題」を解決！ ～

12月16日（火）14時～ 開催予定



- 12月16日(火) 14:00～15:00
- オンラインにて

HORNETSECURITY