2026-03-24

DMARCは「p=rejectがゴール」ではない
none放置もreject即設定も危険！

～ 判断できる企業だけが実現する戦略的DMARC運用 ～

Hornetsecurity株式会社
プリンシパルメッセージングエンジニア
平野 善隆

本日のトピック

- 自己紹介
- メールの仕組みのおさらい
- DMARCって何？
- p=rejectのやり方
- DMARCレポートの見方
- DMARC Managerがすべて解決

HORNETSECURITY
BY proofpoint.

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

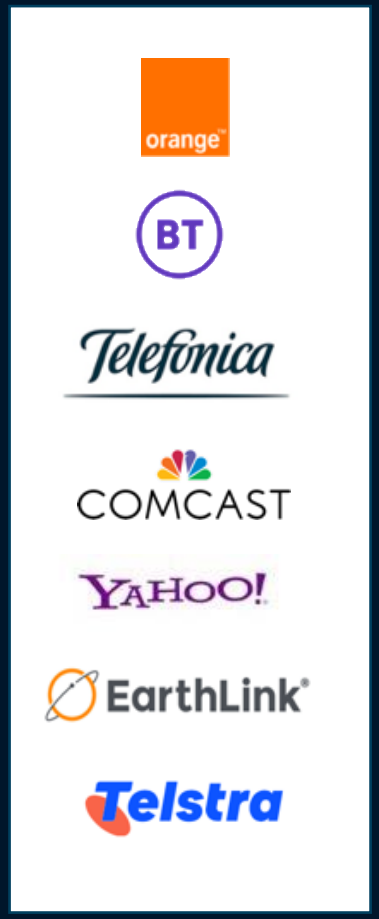
趣味　　長距離の自転車大会(1,200kmとか、2,000kmとか)
バンド演奏

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

HORNET SECURITY (VADE JAPAN)とは

設　立	2009年、フランス共和国リールにて設立 2024年 3月 ドイツ Hornetsecurityのグループとなる 2025年 12月 Proofpoint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、日本など
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
BY proofpoint.

継続サービス

ワンストップ・プロテクション　機能のラインナップ

メールセキュリティ

- スパム＆マルウェアフィルター
- メール暗号化
- 署名、免責事項の追加
- アドバンスド脅威保護
- メールアーカイブ
- 継続性確保サービス
- Webフィルター

M365 API経由で未知の脅威を検知するメールフィルター

バックアップ

- M365データの自動バックアップ
- セルフサービスでの詳細な復旧
- 定額料金でストレージ容量無制限
- VMバックアップ

コンプライアンス、セキュリティ意識向上

- セキュリティ意識向上
- パーミッション管理
- DMARCレポート管理
- フィッシング攻撃シミュレーション
- パーミッションアラート
- メールのレピュテーション改善、配信
- ESI®レポート
- パーミッション監査
- 容易なDNS管理、最適化

POWERED BY AI CYBER ASSISTANT

- AI誤送信防止
- Teams保護
- AI メールセキュリティアナリスト
- コミュニケーションパターン分析
- チャット型脅威のモニタリング
- AIユーザーレポート分析
- センシティブデータのチェック
- Ai フィッシング検知、レスポンス
- AI レスポンスとユーザー意識向上

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
BY proofpoint.

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

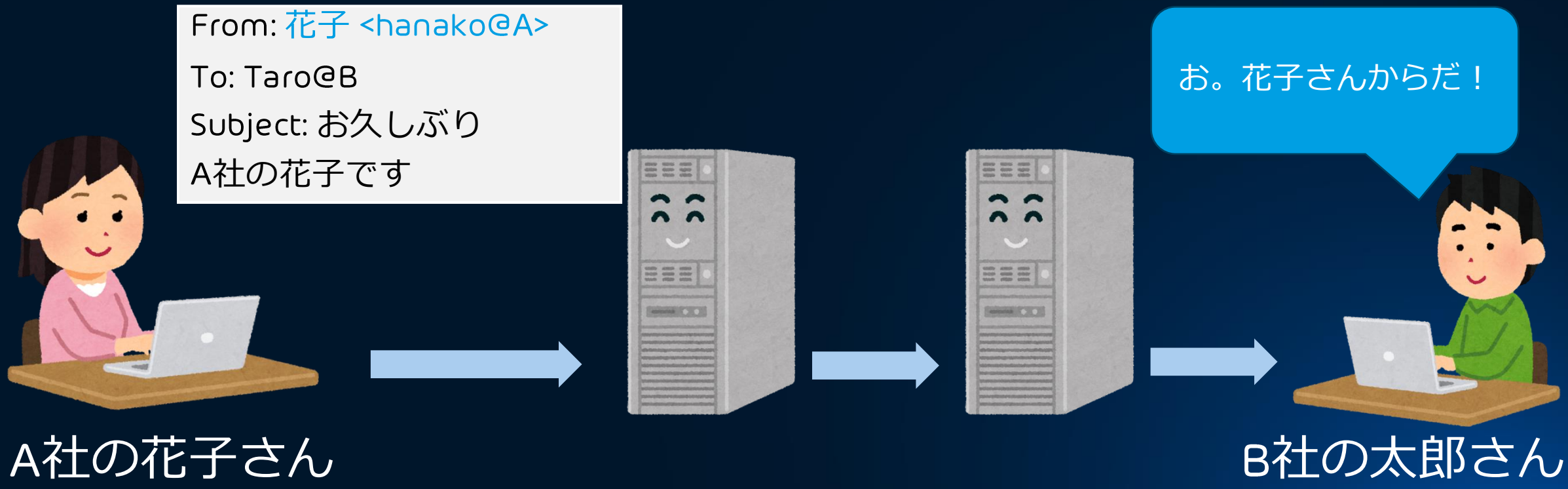
Revised by

David H. Crocker

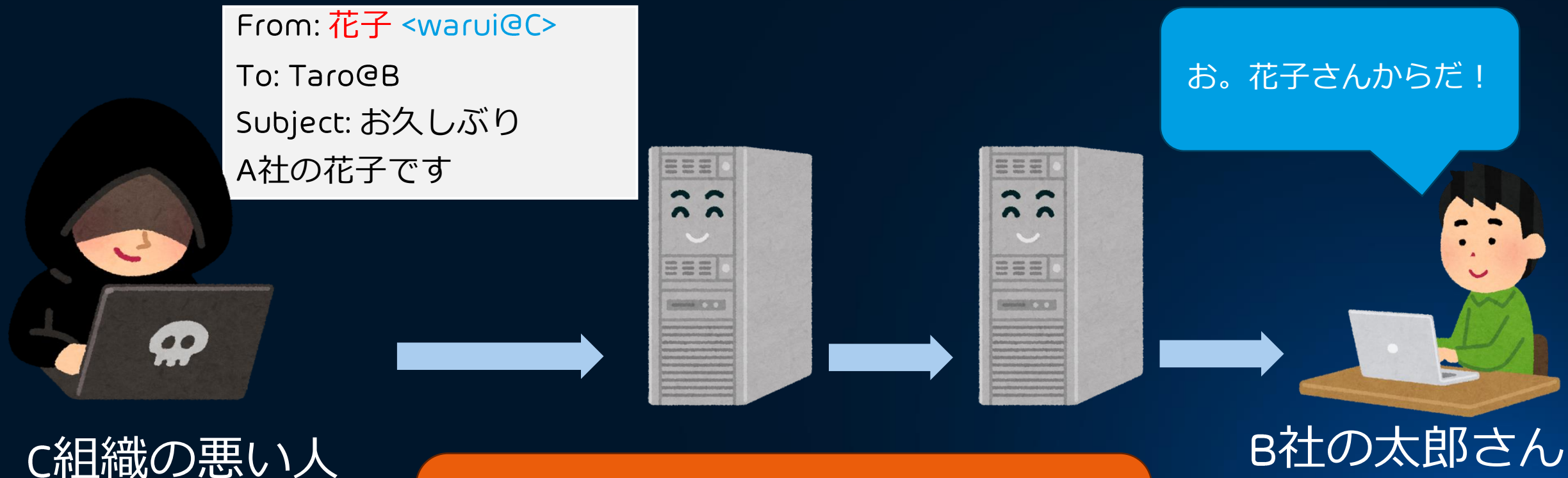
Dept. of Electrical Engineering
University of Delaware, Newark, DE 19711
Network: DCrocker @ UDel-Relay

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



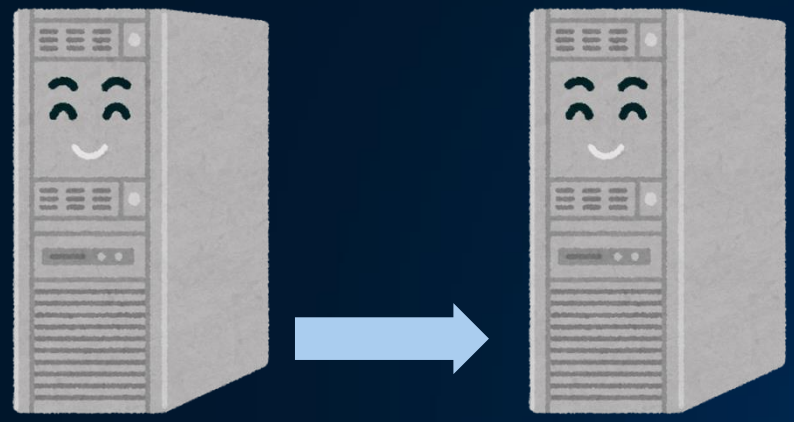
自分のメールアドレスで
表示名だけなりすます

HORNETSECURITY
BY proofpoint.

メールアドレスもなりすまし

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

C組織の悪い人



お。花子さんからだ！

B社の太郎さん

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

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

最近、花子さんから
来ないなぁ。

B社の太郎さん

A社からはスパム
ばっかりやな。
ブロックや！

HORNETSECURITY
BY proofpoint.

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
BY proofpoint.

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
BY proofpoint.

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
1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
BY proofpoint.

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
BY proofpoint.

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
1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。

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
BY proofpoint.

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。」

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

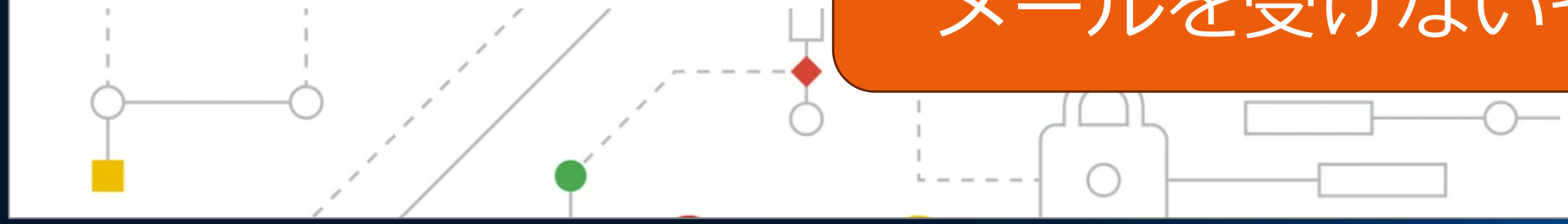
GMAIL

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
BY proofpoint.

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をまずp=noneで設定し、
なりすましメールが届かないように
p=rejectをめざす

HORNETSECURITY
BY proofpoint.

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をまずp=noneで設定し、
なりすましメールが届かないように
p=rejectをめざす

HORNETSECURITY
BY proofpoint.

HORNETSECURITY
BY proofpoint.

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

p=noneは何のため?

- DMARC p=noneはDMARCがないのと変わらない
- レポート分析でrejectに進めるか判断する期間

レポート分析でわかること

- 自社のメールがどこから出ているのか = 棚卸し
- 正規メールがDMARCで失敗していないか
- 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

HORNETSECURITY
BY proofpoint.

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
BY proofpoint.

HORNETSECURITY
BY proofpoint.

p=reject
にするには

p=rejectにする方法

- 1. とりあえず、えいやっとp=rejectにする
- 2. きっちり分析をしてrejectにする
- 3. 何が起こるか怖いので、p=noneのまま

p=rejectにする方法

- p=noneでレポートを受信
  - 失敗しているものを調べる
    - 正規のメールとなりすましメールの分離
    - 設定漏れがあれば修正

- 問題なければp=quarantineでレポートを受信
  - 失敗しているものを調べる
    - 正規のメールとなりすましメールの分離
    - 設定漏れがあれば修正

- 問題なければp=rejectでレポートを受信

課題

- レポートの見方が分からない
- レポートを見たけど、情報がなさ過ぎる
- レポートは分析したけど、意味が分からない
- メーリングリストや転送があるので
  どうしようもない
- 「設定漏れがあれば修正」と言われても
  修正できない環境もある

HORNETSECURITY
BY proofpoint.

課題

- レポートの見方が分からない
- レポートを見たけど、情報がなさ過ぎる
- レポートは分析したけど、意味が分からない
- メーリングリストや転送があるので
  どうしようもない
- 「設定漏れがあれば修正」と言われても
  修正できない環境もある

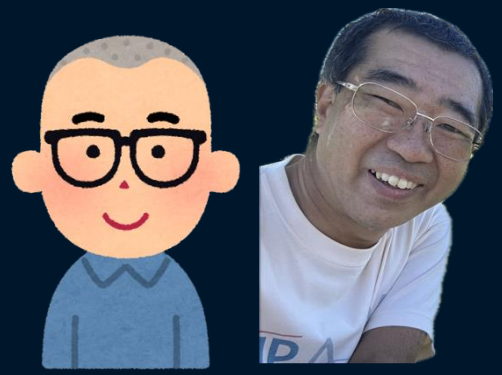
HORNETSECURITY
BY proofpoint.

HORNETSECURITY
BY proofpoint.

DMARC レポート

DMARCレポートの流れ

hornetsecurity.com



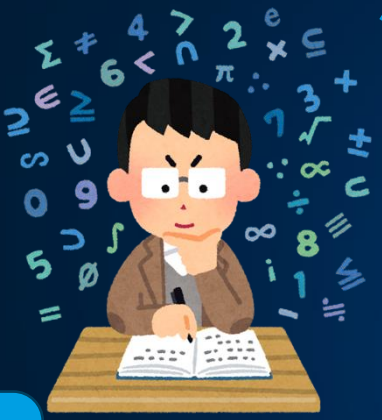
新井原さん

受信事業者

例えばGoogle, Microsoft

A社の花子さん

hornetsecurity.comから
メールが100通来ましたよ



集計

B社の太郎さん

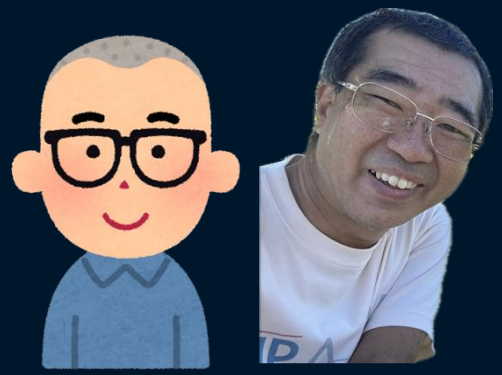
分析する人

メールは社外からも配信

悪い人

配信業者

hornetsecurity.com



新井原さん

受信事業者

例えばGoogle, Microsoft

Web Hosting

集計

分析する人

hornetsecurity.comから
なんかいろいろ来てますよ

DMARCレポートの種類

- Aggregate Report
  - 集計されたレポート
  - rua=で送信先を設定

- Failure Report
  - 個々のメール毎の失敗レポート
  - ruf=で送信先を設定
  - ほとんど誰も送っていない

HORNETSECURITY
BY proofpoint

DMARC
レポートの見方

DMARCレポートとして欲しい情報は? (希望)

- DMARCの結果
- Fromのメールアドレス
- メールの送り先
- メールの件名
- メールの送信元
- p=rejectにしたときにも届くか
- 届かないなら何が悪いのか

HORNETSECURITY
BY proofpoint.

DMARCレポートの受け取り

- 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

HORNETSECURITY
BY proofpoint.

集計レポートの構造

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <version>1.0</version>
  <report_metadata>
    ....
  </report_metadata>
  <policy_published>
    ....
  </policy_published>
  <record>
    ....
  </record>
  <record>
    ....
  </record>
  ....
</feedback>
```

レポート全体の情報

公開されてるポリシー

メールの情報が続く

HORNETSECURITY
BY proofpoint.

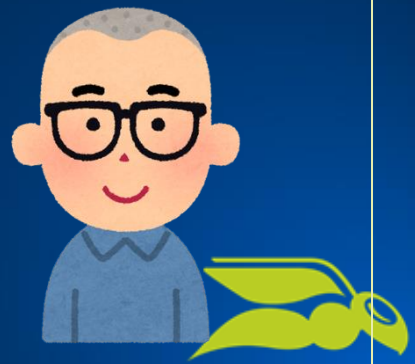
report_metadata

```
<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>16454783335537556531</report_id>
  <date_range>
    <begin>1771891200</begin>
    <end>1771977599</end>
  </date_range>
</report_metadata>
```

レポート作成者の情報

レポートの対象期間

なんや?
この数字は?!



HORNETSECURITY
BY proofpoint.

Epoch Time

- 1970年1月1日 0時0分0秒(UTC) からの秒数

```
<date_range>
  <begin>1771891200</begin>
  <end>1771977599</end>
</date_range>
```

```
% date -d @1771891200
Tue Feb 24 09:00:00 JST 2026
```

```
% date -d @1771977599
Wed Feb 25 08:59:59 JST 2026
```

policy_published

```
<policy_published>
  <domain>hirano.cc</domain>
  <adkim>r</adkim>
  <aspf>r</aspf>
  <p>reject</p>
  <sp>reject</sp>
  <pct>100</pct>
  <np>reject</np>
</policy_published>
```

DNSで公開しているポリシー

```
v=DMARC1; p=reject; fo=1;
 rua=mailto:...;
 ruf=mailto:...;
 np=reject; psd=n
```

GoogleはすでにDMARCbis対応！

HORNETSECURITY
BY proofpoint.

record (前半)

```
<record>
  <row>
    <source_ip>192.0.2.1</source_ip>
    <count>4</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>pass</dkim>
      <spf>pass</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>hirano.cc</header_from>
  </identifiers>
  ... 続く ...
```

送信元IP x 結果 で
グループ化されている感じ

メール送信元のIP

通数

メールをどう扱ったか
none / quarantine / reject
DMARCの判定結果ではない

DMARCのDKIMの結果
pass / fail

DMARCのSPFの結果
pass / fail

認証に使われたドメイン

DMARCの結果が
載ってないなんて

HORNETSECURITY
BY proofpoint.

record (後半)

```
<record>
    ....
    <auth_results>
      <dkim>
        <domain>hirano.cc</domain>
        <result>pass</result>
        <selector>20231227</selector>
      </dkim>
      <spf>
        <domain>hirano.cc</domain>
        <result>pass</result>
      </spf>
    </auth_results>
 </record>
```

DKIMの結果 (DMARCは関係ない)

SPFの結果 (DMARCは関係ない)

auth_resultsは何に使うのか?

- policy_evaluatedだけでは
  何が悪いのかわからない

```
<row>
  <policy_evaluated>
    <disposition>none</disposition>
    <dkim>fail</dkim>
    <spf>pass</spf>
  </policy_evaluated>
</row>
<identifiers><header_from>example.co.jp</header_from></identifiers>
```

DKIMが失敗！
しかし
何を調べたらいいか
わからない

HORNETSECURITY
BY proofpoint.

auth_resultsは何に使うのか?

- どこが間違えているのかのヒント

```
<row>
  <policy_evaluated>
    <disposition>none</disposition>
    <dkim>fail</dkim>
    <spf>pass</spf>
  </policy_evaluated>
</row>
<identifiers><header_from>example.co.jp</header_from></identifiers>
<auth_results>
  <dkim>
    <domain>example-co-jp.onmicrosoft.com</domain>
    <result>pass</result>
    <selector>20231227</selector>
  </dkim>
  ....
</auth_results>
```

署名ドメインが
一致していない

DKIM単体ではPASS

HORNETSECURITY
BY proofpoint.

DMARCレポートから得られる情報

- 受信サーバー
- 送信元IPアドレス

- DMARCの適用結果
- DMARCのSPFの結果
- DMARCのDKIMの結果

- 素のSPFの結果
- 素のDKIMの結果

HORNETSECURITY
BY proofpoint.

欲しい情報はあるのか? (現実)

- DMARCの結果
  - ➔ △ DKIM, SPFの結果から計算
- Fromのメールアドレス
  - ➔ × ない (ドメインはわかる)
- メールの送り先
  - ➔ × ない (受信事業者はわかる)
- メールの件名
  - ➔ × ない

HORNETSECURITY
BY proofpoint.

欲しい情報はあるのか? (現実) (2)

- メールの送信元
  - ➔ △ IPアドレス
- p=rejectにしたときにも届くか
  - ➔ △ p=noneのときはDKIM, SPFから計算
    - ○ p=quarantine以上のときはdisposition
- 届かないなら何が悪いのか
  - ➔ ○ 素のSPFやDKIMの結果から判断

HORNETSECURITY
BY proofpoint.

課題

- レポートの見方が分からない
- レポートを見たけど、情報がなさ過ぎる
- レポートは分析したけど、意味が分からない
- メーリングリストや転送があるので
  どうしようもない
- 「設定漏れがあれば修正」と言われても
  修正できない環境もある

HORNETSECURITY
BY proofpoint.

情報の補完

DMARCレポートにはDMARCの結果はない

- DMARCがfailでもdispositionはnoneになり得る
- DMARCがpassでもdispositionはrejectになり得る

- DMARCの結果は自分で計算

spf=pass	➔ DMARC=pass
dkim=pass	➔ DMARC=pass
spf, dkim 両方 fail	➔ DMARC=fail

HORNETSECURITY
BY proofpoint.

IPアドレスから得られる情報

- IPアドレスの保有事業者
- 国・地域
- IPブラックリスト
- 逆引きホスト名
- ドメインの保有事業者
- AS番号
- ASの保有事業者
- などなど

HORNETSECURITY
BY proofpoint.

課題

- レポートの見方が分からない
- レポートを見たけど、情報がなさ過ぎる
- レポートは分析したけど、意味が分からない
- メーリングリストや転送があるので
  どうしようもない
- 「設定漏れがあれば修正」と言われても
  修正できない環境もある

意味の分からないレポート分析結果

- 送信元: 自社では使用していないISP
- DMARCの結果: 配送
  - SPF: 失敗
  - DKIM: 成功

- 送信元: 自社では使用していないISP
- DMARCの結果: 拒否
  - SPF: 失敗
  - DKIM: 失敗 (自社のドメイン)

転送や
メーリングリスト

転送されたメール

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

A社の花子さん

B社のメールサーバー

メールはgmailに
転送して読んでるよ

B社の太郎さん

転送

SPF: 失敗

DKIM: OK

DMARC: OK

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

DKIMがなければ届かない

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

A社の花子さん

B社のメールサーバー

転送

SPF: 失敗

DKIM: 失敗

DMARC: 失敗

メールはgmailに
転送して読んでるよ

B社の太郎さん

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

DKIMがあってもメーリングリストでは

From: 花子 <hanako@A>
To: Ochakai@ML
Subject: 案内です
DKIM署名: A社花子
A社の花子です

A社の花子さん

メーリングリストサーバー

転送

SPF: 失敗

DKIM: 失敗

DMARC: 失敗

最近花子さんのお茶会案内来ないなぁ

B社の太郎さん

From: 花子 <hanako@A>
To: Ochakai@ML
Subject: [お茶会]案内です
DKIM署名: A社花子
A社の花子です

気の利いたメーリングリスト

From: 花子 <hanako@A>
To: Ochakai@ML
Subject: 次回会合
DKIM署名: A社花子
A社の花子です

A社の花子さん

メーリングリストサーバー

Fromを書き換えて転送

SPF: OK

DKIM: OK

DMARC: OK

From: 花子via ML <ocha@ML>
To: Ochakai@ML
Subject: [お茶会]次回会合
DKIM署名: お茶会ML
A社の花子です

お、花子さんから
お茶会だ。

B社の太郎さん

Fromアドレスを書き換える条件

転送サービスやメーリングリストによりますが、

- p=noneでは書き換えない
- p=quarantine以上で書き換える

p=noneでは結果が悪く見える

p=noneでは、転送やメーリングリストの影響はわからない

⬇

p=quarantineで確認！

HORNETSECURITY BY proofpoint.

課題

- レポートの見方が分からない
- レポートを見たけど、情報がなさ過ぎる
- レポートは分析したけど、意味が分からない
- メーリングリストや転送があるので
  どうしようもない
- 「設定漏れがあれば修正」と言われても
  修正できない環境もある

HORNETSECURITY
BY proofpoint.

DMARCbis

DMARCbisとは

- 現在のDMARCの仕様を置き換える予定の規格
- 現時点では「Proposed Standard」

DKIM必須

- 卒業生向けメール転送サービス
- 部署名のエイリアス
- メーリングリスト

- 中継するメールサーバーが
  ヘッダFromアドレスを書き換えない場合

- SPFに依存してはならない(MUST NOT)
- 有効なDKIM署名が必要 (MUST)

HORNETSECURITY
BY proofpoint.

インターネット上のMLをよく使う場合

- 一般ユーザーが日常的にメールを送るようなドメインで
- インターネット上のメーリングリストに送るような場合

p=rejectにするべきではない (SHOULD NOT)

- p=rejectにする場合は
  - 1ケ月間p=noneでレポートを分析
  - さらに1ケ月間p=quarantineでレポートを分析、noneの時と比較する
  - p=rejectにする場合は、ユーザーに以下を周知すべき (SHOULD)
    - メーリングリストに投稿しないようにする
    - メーリングリストの参加が妨げられる可能性がある

あれ? ARCは?

- ここ10年でメーリングリストソフトはすでにbob@example.comをbob=example.com@user.somelist.exampleのように書き換えるような修正をおこなった
- 理想とはほど遠いがメーリングリスト業者は受け入れている
- ARCも解決策のひとつで研究は現在も進行中であるが、この文書の発行時点では、広く普及するには至っていない
- 将来、広く採用されるようになった場合には、本文書は更新される

draft-ietf-dmarc-dmarcbis-41 §7.4 より

- To avoid any future confusion, it is therefore requested that ARC (RFC8617) be marked “Obsolete” by the publication of this Internet-Draft.
- 将来的な混乱を避けるため、本インターネットドラフトの公開をもって、ARC（RFC8617）を「Obsolete（廃止）」と位置付けることを求める。

draft-adams-arc-experiment-conclusion-00 より

p=reject にするには (現実)

p=rejectにするリスク

- 自社をなりすましたメールが届かない
  = 正しく認証されたメールのみが届く
    - ➔ 設定ミスしたメールは届かない
    - ➔ 受信者が転送したメールが届かない(かも)
    - ➔ メーリングリスト宛のメールが届かない(かも)

レポートを分析して、rejectにするかどうかの判断が重要

rejectにしたあとも継続的にモニタリングが必要

HORNETSECURITY
BY proofpoint.

レポート分析の流れ (p=noneの場合)

- レポートを受け取る
- 集計する
- 送信元IPから様々な情報を集めて
- 自社のメールがFailしていないか確認
- Failしていれば、SPFやDKIMを設定

いろいろ失敗

失敗なし

転送やMLのみ失敗

p=quarantineへ

レポート分析の流れ (p=quarantineの場合)

- レポートを受け取る
- 集計する
- 送信元IPから様々な情報を集めて
- 自社のメールがFailしていないか確認
- Failしていれば、SPFやDKIMを設定

いろいろ失敗

失敗なし

転送やMLのみ失敗

積極的none
積極的quarantine

p=rejectへ

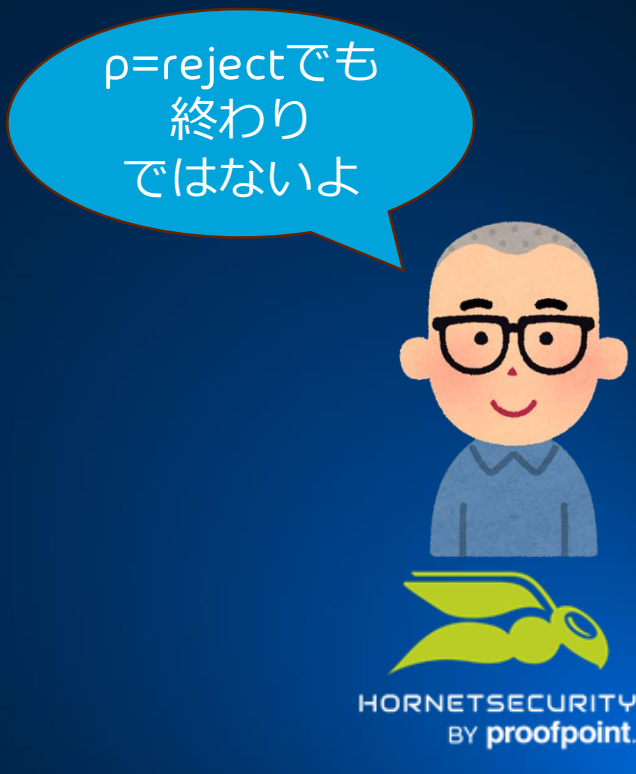
quarantineのまま据え置くか
noneに戻す

HORNETSECURITY
BY proofpoint.

レポート分析の流れ (p=rejectの場合)

- レポートを受け取る
- 集計する
- 送信元IPから様々な情報を集めて
- 自社のメールがFailしていないか確認
- Failしていれば、SPFやDKIMを設定

失敗があれば修正



HORNETSECURITY
BY proofpoint.

2種類のp=none

- 分析の結果p=quarantine以上にできないので
  リスクを分かった上で、あえてnoneにしている

積極的 none

- 何が起こるか怖いので、p=noneのまま

消極的 none

2種類のp=reject

- メール送信の環境はしっかり管理されているし送り先の状況も把握している
  - 全てを把握できている

積極的 reject

- よくわからないけど、p=rejectがいいと言われたのでやってみた

思考停止やん

消極的 reject

DMARCのレポート分析

できそうですか？

HORNETSECURITY
BY proofpoint.

HORNETSECURITY
BY proofpoint.

ツールがあると

データを目で見て分かるように

- 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
BY proofpoint.

レポート分析画面の例

DMARC MANAGER

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 BY proofpoint.

配送状況も確認できます

Sender	IP Addresses	Deliverability	Volume	Delivered	Not Delivered
IDC Frontier Japan IDC Frontier Japan	5	100.0%	44	44	0
37907 Other	1	100.0%	21	21	0
Google, LLC Google Workspace Gmail	1	100.0%	1	1	0
Yahoo!	1	100.0%	1	1	0
ChinaNet Online Holdings ChinaNet	1	100.0%	1	0	1
Gmo Internet Japan Gmo Internet Japan	1	100.0%	1	1	0
Internet Initiative Japan Internet Initiative Japan XSP Mail	1	100.0%	1	1	0

配送された

転送も
配送された

なりすましなので
配送されなかった

HORNETSECURITY
BY proofpoint.

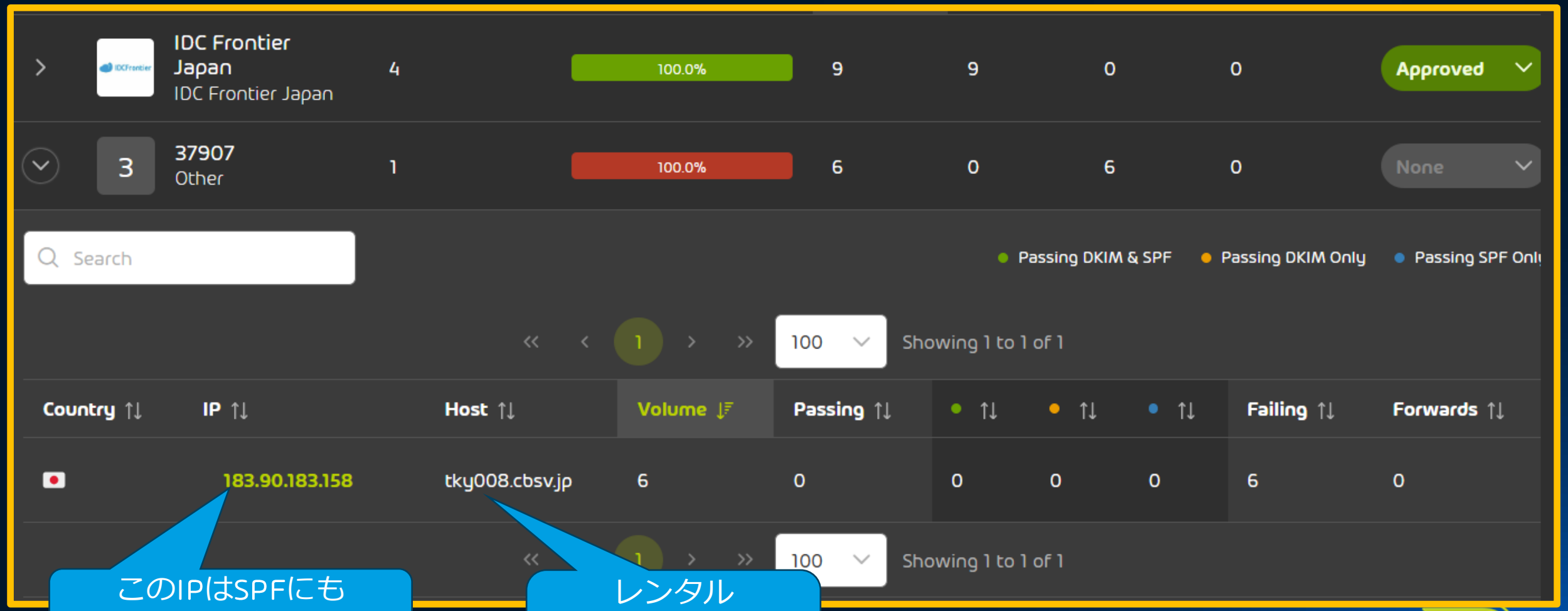
HORNETSECURITY
BY proofpoint.

実際の例

実際の例 (ar-nihonbashi.org)

HORNETSECURITY
BY proofpoint.

失敗してる部分の詳細



このIPはSPFにも
いれてある

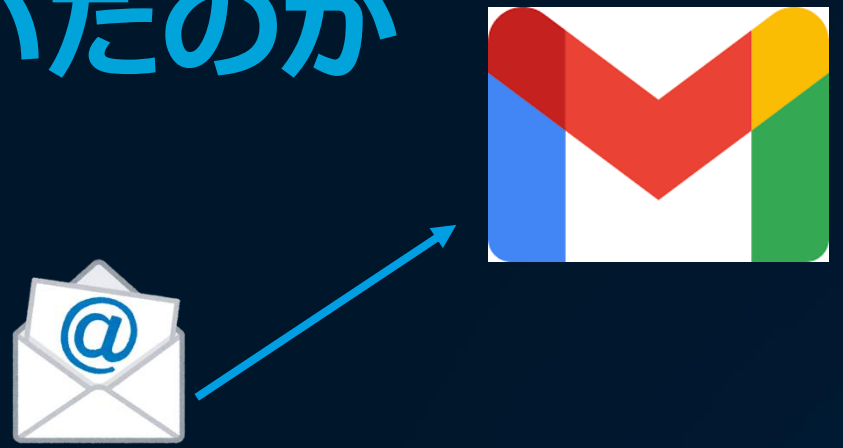
レンタル
Webサーバーの
ホスト名だ

HORNETSECURITY
BY proofpoint.

さらに詳細

HORNETSECURITY
BY proofpoint.

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

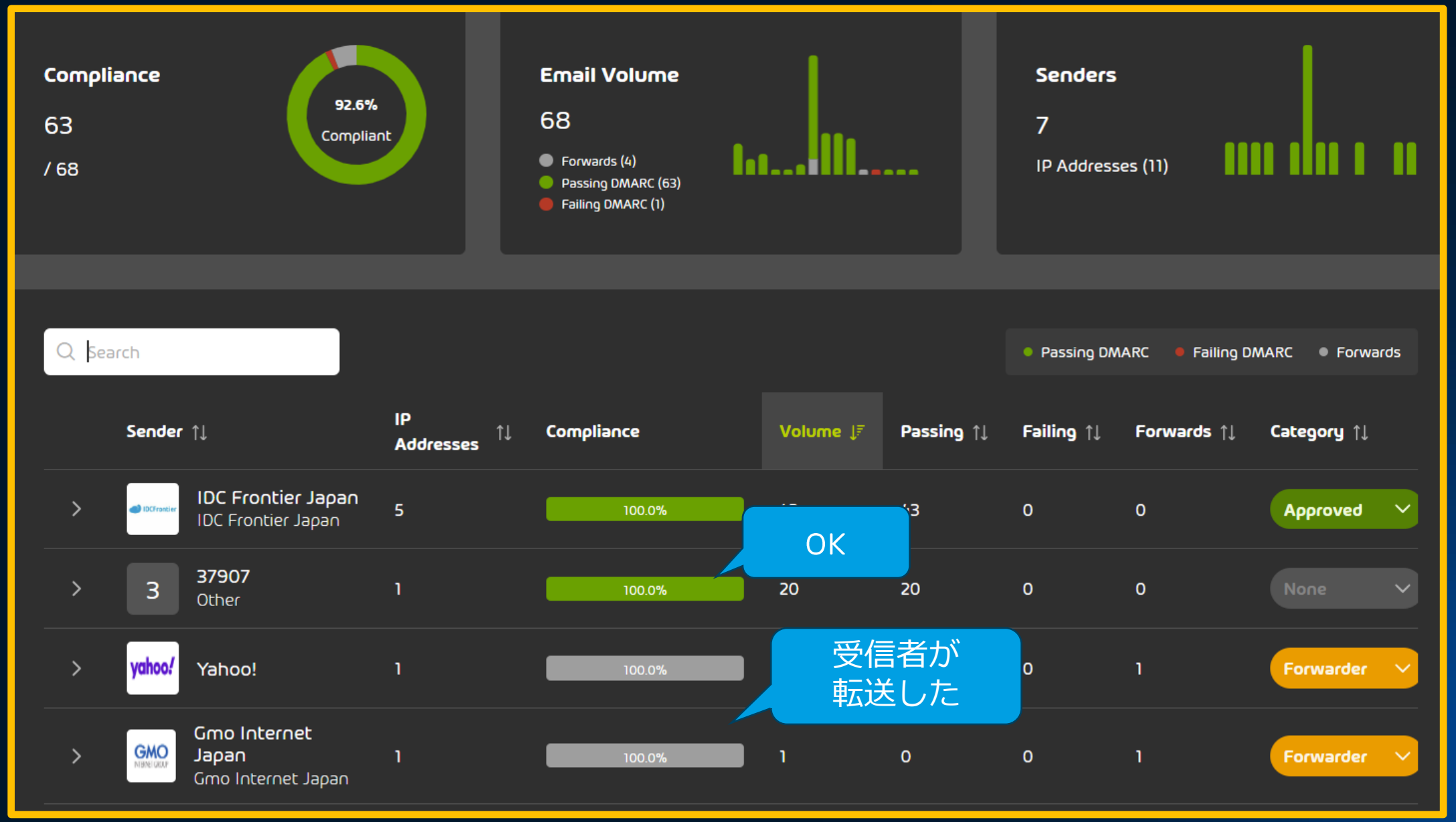
Webレンタルサーバーの
ドメインのSPF

メールサーバー

Webサーバー

HORNETSECURITY
BY proofpoint.

無事DMARCがPASSしました



HORNETSECURITY
BY proofpoint.

HORNETSECURITY
BY proofpoint.

その他の
面倒も見ます

DMARC運用でよく困るところ

- 送信サーバや配信事業者が把握し切れていないので怖くてp=rejectにできない
- DMARCレポートの見方が分からない
- 設定の文法がわからない
- DNSの設定部署が別で、変更に時間がかかる
- SPFのDNS参照が10回を超える

HORNETSECURITY
BY proofpoint.

DMARC Managerが提供する主な機能

日本語対応

DMARC 設定支援

DNSの記述ミスから解放	• 難しいDNSレコードをすべてGUIで設定。記述ミスを完全に排除
SPF10回問題を解決	• SPFフラットニング機能で、SPFのDNS参照回数を10回以下に

DMARC レポート分析支援

簡単。自動収集・描画	• メールアドレスを指定するだけでDMARCレポートを自動で描画
データエンリッチメント	• オリジナルのDMARCレポートに含まれないが分析に有用な情報を外部から自動付与
p=reject シュミレーション	• p=reject にした場合の影響範囲を１クリックで可視化

その他

BIMIの管理	• BIMIのロゴ・証明書のホスティング
MTA-STS管理	• MTA-STSのポリシーのホスティング
TLS-RPTのレポート	• TLS-RPTのレポートの分析

HORNETSECURITY
BY proofpoint.

DMARC
設定支援

DNS設定は大変

DNSの設定・変更

DNSの管理者

設定依頼

メールセキュリティや
ブランドの管理者

SPF

DKIM

DMARC

DNSサーバー

ちょっと立て込んでるから、来週まで待って

SPFにサーバー追加してよ

で、具体的にどう書けばいいの?

え、DNSわからないんだけど

TXTレコードは書くけど、その中身は分からないよ

えー、じゃ調べるよ

HORNETSECURITY
BY proofpoint.

DNSの設定支援

DNSの管理者

最初に1回だけ
設定

メールセキュリティや
ブランドの管理者

SPF

DKIM

DMARC

DNSサーバー

CNAMEなどで
転送設定

わかりやすいWebUI

DMARC MANAGER

DMARCなどのDNSレコードは
ここで自動生成

HORNETSECURITY
BY proofpoint.

SPFの設定画面

DMARC MANAGER

+ Add New SPF Directive | Import

	Order	Directives
≡	1	Include spf.protection.outlook.com
≡	2	Include _spf.google.com
≡	3	Include _spf.salesforce.com
≡	4	Include the IPv4 address 210.158.71.72

設定ミスしようと
思ってもできない

Edit SPF Directive

Record Type

IPv4 Address/Range

Record Qualifier

+ Allow

Address Value

210.158.71.72

e.g. _spf.example.com

Description

経営管理部の会計サーバー (2025/1/15追加 担当:大野)

コメントも
残せます

SPFのDNSの参照回数制限

example.com

① aspmx.pardot.com → ② et._spf.pardot.com

③ amazonses.com

④ _spf.google.com → ⑤ _netblocks.google.com, ⑥ _netblocks2.google.com, ⑦ _netblocks3.google.com

⑧ mail.zendesk.com

⑨ _spf.salesforce.com → ⑩ %{i}._spf.mta.salesforce.com

⑪ spf.protection.outlook.com

HORNETSECURITY
BY proofpoint.

SPFフラットニング

DMARC MANAGER

example.com

ip4:198.245.81.0/24 ip4:136.147.176.0/24 ip4:13.111.0.0/16 ip4:136.147.182.0/24 p4:136.147.135.0/24 ip4:199.122.123.0/24 ip4:199.255.192.0/22 ip4:199.127.232.0/22 ip4:54.240.0.0/18 ip4:69.169.224.0/20 ip4:23.249.208.0/20 ip4:23.251.224.0/19 ip4:76.223.176.0/20 ip4:54.240.64.0/19 ip4:54.240.96.0/19 ip4:76.223.128.0/19 ip4:216.221.160.0/19 ip4:206.55.144.0/20 .... exists:%{i}._spf.mta.salesforcee.com ip4:40.92.0.0/15 ip4:40.107.0.0/16 ip4:52.100.0.0/15 ip4:52.102.0.0/16 ip4:52.103.0.0/17 ip4:104.47.0.0/17 ip6:2a01:111:f400::/48 ip6:2a01:111:f403::/49 ip6:2a01:111:f403:8000::/51 ip6:2a01:111:f403:c000::/51 ip6:2a01:111:f403:f000::/52

- aspmx.pardot.com
- et._spf.pardot.com
- amazonses.com
- _spf.google.com
- _netblocks.google.com
- _netblocks2.google.com
- _netblocks3.google.com
- mail.zendesk.com
- _spf.salesforce.com
- %{i}._spf.mta.salesforce.com
- spf.protection.outlook.com

DMARC MANAGERがIPアドレスに展開

HORNETSECURITY
BY proofpoint.

まとめ

レポートの分析、ちゃんとできてますか?

- ツールを使って定期的にチームで分析
- 手作業でコツコツと、チームで分析

GOOD

- ○○さんが見てくれてるから大丈夫
- ○○さんがメールは受けてるはずなんだけど
- ruaは書いてあるけど、だれだろ
- ruaも書かれていない

BAD

HORNETSECURITY
BY proofpoint.

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

- メールを正しく届けるためにチームや
  ツールによる継続的なレポート分析が不可欠

HORNETSECURITY
BY proofpoint.

質疑・応答