

「悪」と戦うためにやった 2 つのこと

2022/11/08

株式会社インターネットイニシアティブ(IIJ)
ネットワーク本部 アプリケーションサービス部 運用技術課
課長 古賀 勇

Ongoing Innovation

想定時間 5分






(1) PPAP 廃止しました

みんなでやめましょう



(1) PPAP 廃止しました、みんなでやめましょう

第1回 (2018年) JPAAWG で似たような話をしました

<p>確実にメールを届けたい情シス担当者様に最低限の心得を5分で伝授します</p> <p>暗号化 ZIP は危ない</p>  <p>- 13 -</p>	<p>確実にメールを届けたい情シス担当者様に最低限の心得を5分で伝授します</p> <p>誤送信対策?</p> <p>- 14 -</p>
<p>確実にメールを届けたい情シス担当者様に最低限の心得を5分で伝授します</p> <p>悪い人から見た暗号化 ZIP</p> <p>△ 誤送信対策</p> <p>◎ ウィルススキャン回避</p> <p>- 15 -</p>	<p>確実にメールを届けたい情シス担当者様に最低限の心得を5分で伝授します</p> <p>悪い人から見た暗号化 ZIP</p> <p>△ 誤送信対策 (と知っているのは日本だけの文化)</p> <p>◎ ウィルススキャン回避</p> <p>- 16 -</p>

(1) PPAP 廃止しました、みんなでやめましょう

IIJ の方針表明、2022年 1月 26日に パスワード付き ZIP 運用を全面廃止



IIJ Internet Initiative Japan

法人のお客様 個人のお客様 IIJについて IIJの技術 IR情報 サステナビリティ CONNECTED via IPv6

ホーム > PPAPに対する当社運用の変更について

パスワード付きzipファイルが添付されたメールおよび別送のパスワード記載メール (PPAP) に対する当社運用の変更について

メールにファイルを添付して送信する際、「パスワード付きのzipファイルと、そのパスワードを別送する」という手順で行われている情報セキュリティ対策手法、いわゆる「PPAP」につきまして、当社は2022年1月26日より、社外の方からのIIJアドレスへのメール送信における対応を、原則として以下のように変更いたします。

2022年1月25日以前	従来通り、パスワード付きzipファイルが添付されたメールを受信する
2022年1月26日以降	パスワード付きzipファイルをフィルタにより削除し、メール本文のみ受信する

また、IIJより社外の方へパスワード付きファイルを添付し送信する場合においても、今後順次別の手段へ変更いたします。

上記の変更にもとない、ファイルを共有するための別の手段を用意し、移行いたします。その利用につきましては、お客様、お取引先様に、個別にご連絡を申し上げます。

変更に至った背景

メールにパスワード付きのzipファイルを添付して送信し、そのパスワードを後送する「PPAP」は、日本において多く見られる情報セキュリティ対策の一つですが、効果が薄く、ウィルススキャンをすり抜けてしまうことから、米国のサイバーセキュリティ・インフラセキュリティ庁においてもブロックすることが推奨されています。この仕組みを悪用したマルウェアは今後も発生することが予想されることから、当社だけでなく、お客様、お取引先様よりお預かりする情報を守るためにも、対応が必要との考えに至りました。

当社のお客様、お取引先様におかれましては、何卒、ご理解・ご協力のほど、よろしくお願い申し上げます。

<https://www.iij.ad.jp/ppap/>



パスワード付き (暗号化) ZIP廃止の考え方と対策

2020年11月30日 月曜日

【この記事を書いた人】
古賀 勇

IIJ ネットワーク本部アプリケーションサービス部・(兼)エンタープライズサービス部・(兼)社長室所属。メールサービスの運用業務に従事し、日々世界の悪と戦う一兵の父親。社内 Power Automate エンジニア(自務)、M3AAWG / openSUSE / WIDE Project メンバー。趣味は大昔利。はがき職人。



パスワードの入力

ファイル: 誰も知らない怪人学級授業.docx... はパスワードで保護されています。パスワードを入力してください。

パスワード: ●●●●●●

OK ファイルのスキップ(⌘) キャンセル

パスワード付き ZIP 問題

BI ブックマーク 18 いいね 42 ツイート

CONTENTS

1. なぜパスワード付き ZIP を廃止するのか
2. なぜパスワード付き ZIP がダメなのか
3. どのようなときにパスワード付き ZIP を使うべきか
4. 国内企業の動き
5. IIJ がオススメする誤送信対策

<https://eng-blog.iij.ad.jp/archives/7963>

(1) PPAP 廃止しました、みんなでやめましょう

パスワード付き ZIP 廃止までの流れ

約 1 年間

情報システム部門から危機管理部門・経営層への説明

経営層から社内へのリスク説明・方針説明

情報システム部門での対策実現のための検討

情報セキュリティ担当部門での統制ルール検討

各部門への説明とスケジュールの展開

お客様・取引先への説明

ポリシーの変更

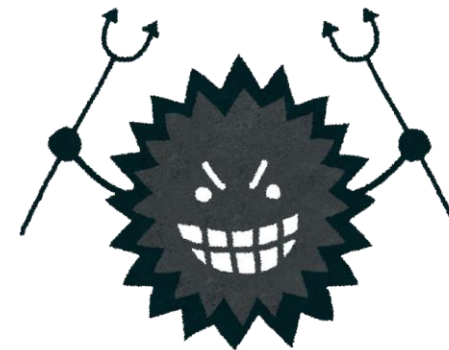
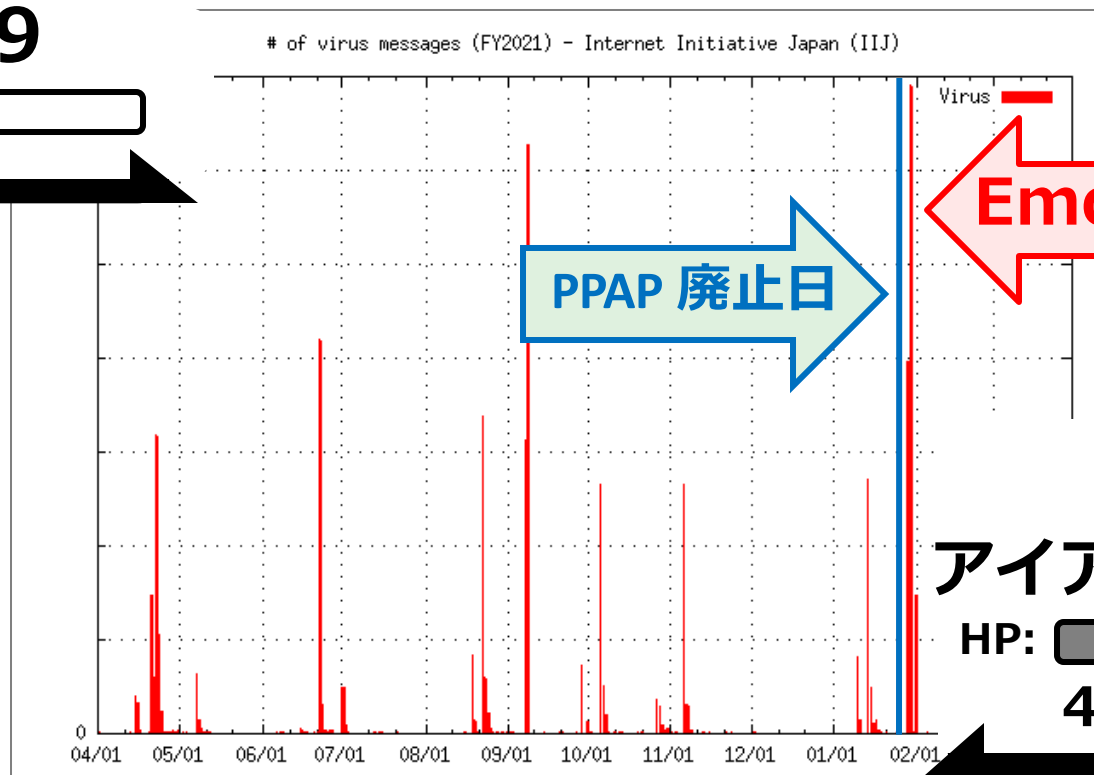
社内の意思決定と
色んな所への説明

顧客への説明と実行

(1) PPAP 廃止しました、みんなでやめましょう

エモテット: L9999

HP:



アイアイジエイ: L2497

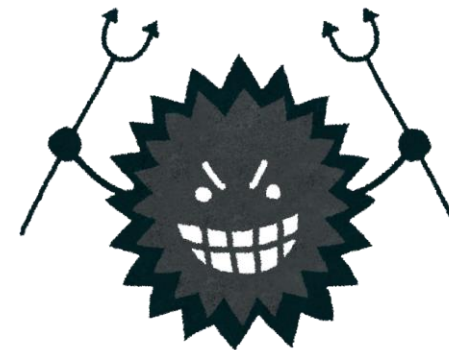
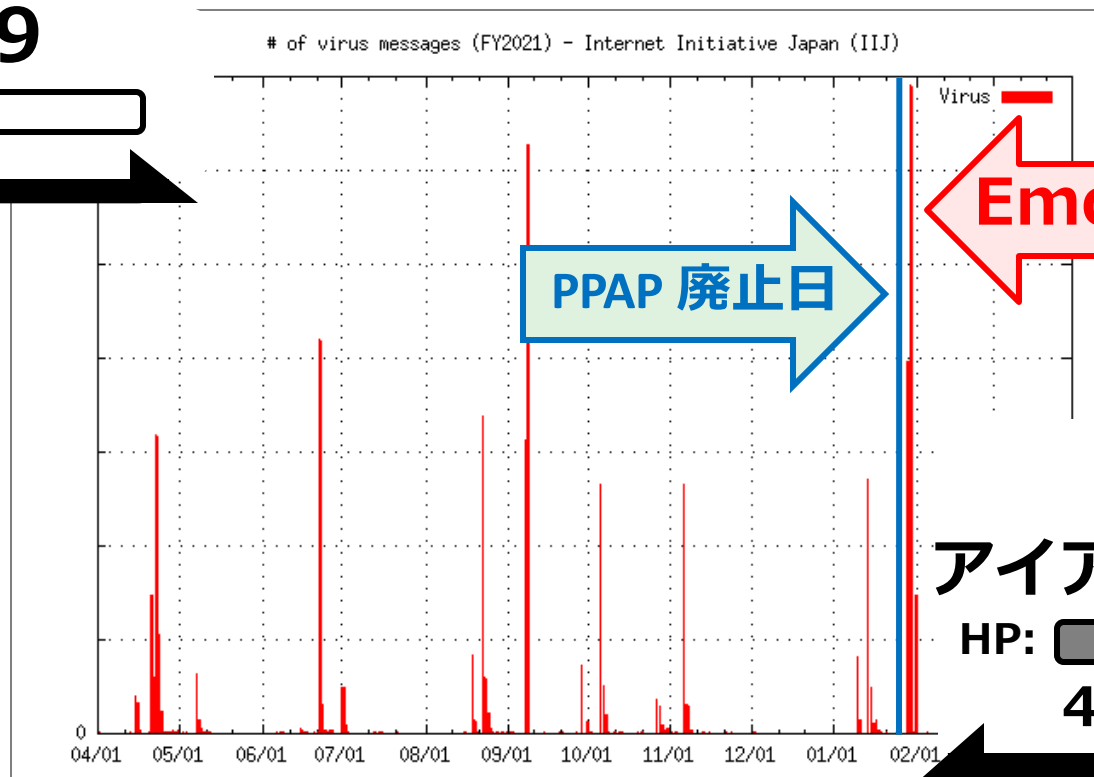
HP:

440 / 440

(1) PPAP 廃止しました、みんなでやめましょう

エモテット: L9999

HP:



Emotet

アイアイジエイ: L2497

HP:

440 / 440

こうかは ばつぐんだ！

あれ?

でも自動で **PPAP** するサービスあったよね...?

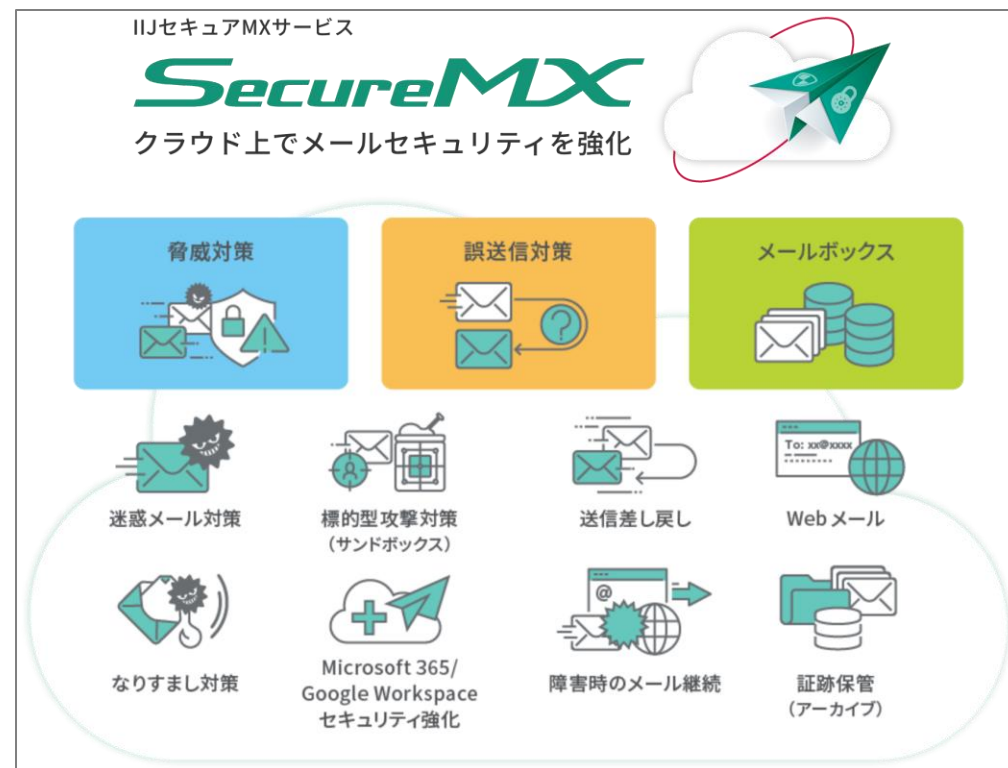
うちのサービスだ！

SecureMX

(1) PPAP 廃止しました、みんなでやめましょう

サービス説明ページからも消しました

添付ファイル暗号化機能※の利用はおすすめしません



※ 2009年リリース。当時、顧客の要望が大きく本機能の開発を決断した。

(1) PPAP 廃止しました、みんなでやめましょう

Emotet にやられないように対策しましょう

**(1) PPAP
みんなでやめましょう**



IIJ IIR

検索

詳細は IIR vol.55 へ!





(2) DMARC **p=reject** しました

みんなでやりましょう



|(2) DMARC p=reject しました、みんなでやりましょう

送信ドメイン認証に失敗したメールは受信拒否してくれていい、という強い意志表明

受信者がなりすましメールを見分けられる

※ DMARC p=reject はメーリングリスト等の組み合わせで副作用が出るケースがあります

|(2) DMARC p=reject しました、みんなでやりましょう

送信ドメイン認証に失敗したメールは受信拒否してくれていい、という強い意志表明

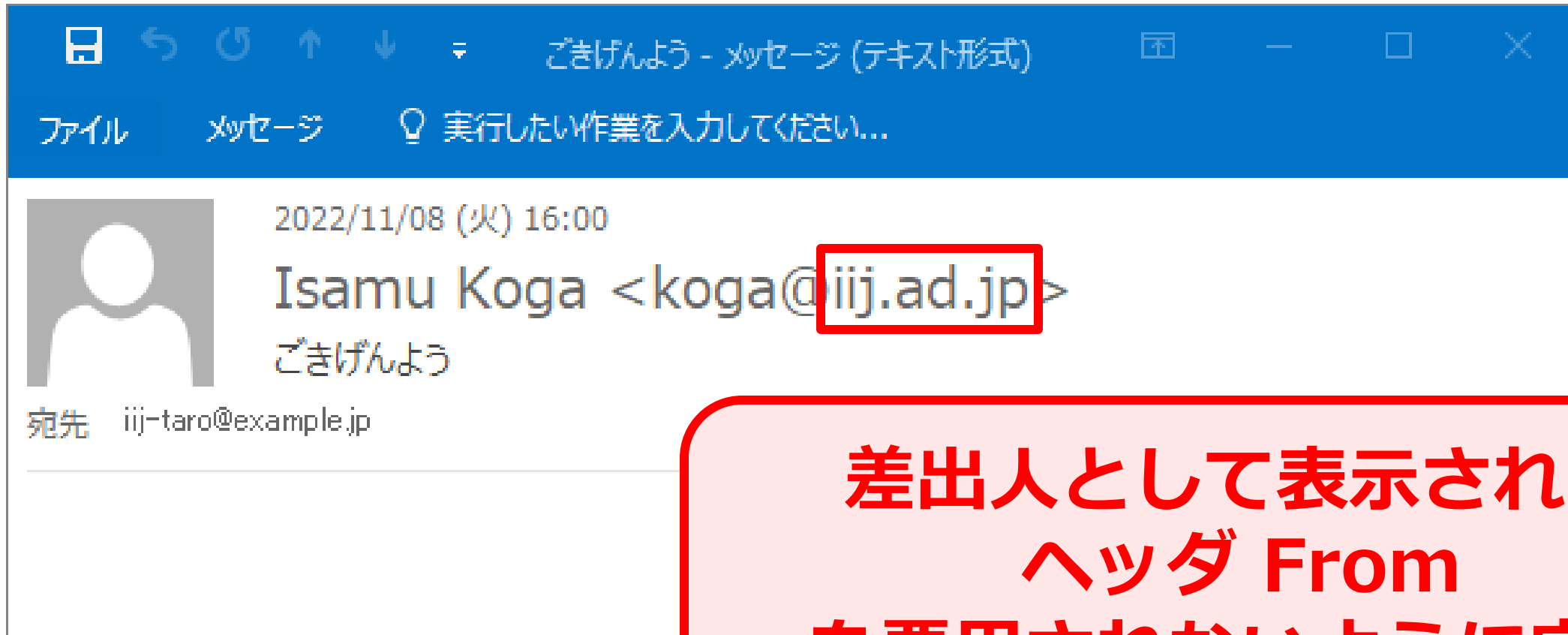
受信者がなりすましメールを見分けられる

送信者のブランドが守られる

※ DMARC p=reject はメーリングリスト等の組み合わせで副作用が出るケースがあります

(2) DMARC p=reject しました、みんなでやりましょう

私たちの守りたい部分

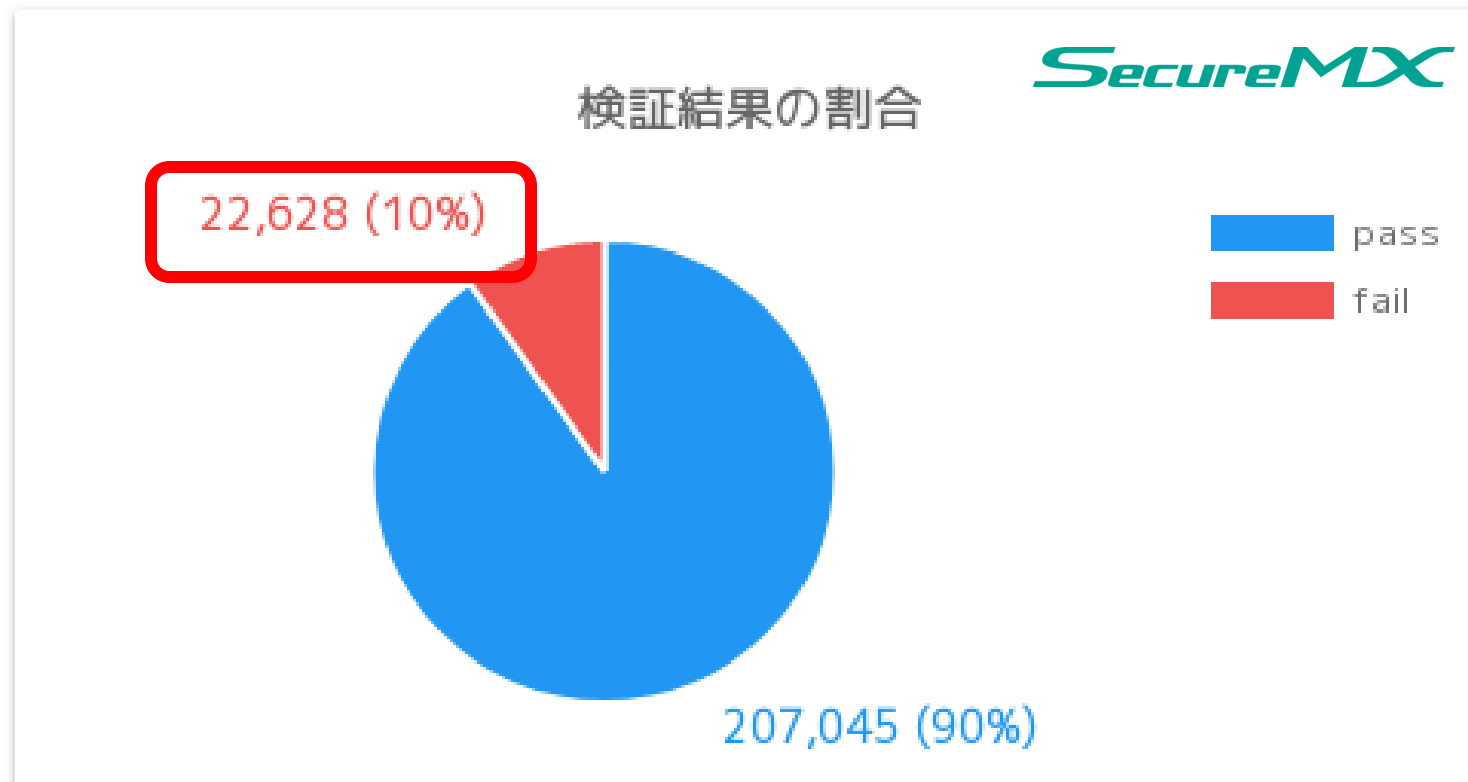


**差出人として表示される
ヘッダ From
を悪用されないように守る**

※ DMARC p=reject はメーリングリスト等の組み合わせで副作用が出るケースがあります

(2) DMARC p=reject しました、みんなでやりましょう

fail したメールは受信拒否されるので、なりすます価値がなくなる



iij.ad.jp おける DMARC レポートの集計結果 (1か月間)

※ DMARC p=reject はメーリングリスト等の組み合わせで副作用が出るケースがあります

まとめ

「悪」の手に掛かる前に対策しましょう

(1) PPAP
みんなでやめましょう

(2) DMARC p=reject
みんなでやりましょう



IIJ IIR

検索

詳細は IIR vol.55 へ!



Lead Initiative

日本のインターネットは1992年、IIJとともに始まりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ

IIJはいつも始まりであり、未来です。

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。