想定所要時間 35分

Internet Week 2025 / C11
10:00～11:30

メールセキュリティ 2025 アップデート

DMARC・STARTTLS(経路暗号化)・大量配信

2025/11/26(水)

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2部 アプリケーションサービス運営課
課長　古賀 勇

Ongoing Innovation

自己紹介

古賀 勇 (Isamu Koga)

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2部
アプリケーションサービス運営課・課長

Power Automate エバンジェリスト (自称) **「自動化は正義」**

法人系メールセキュリティサービスの運用

SecureMX

- ウイルス対策
- 迷惑メール対策
- Sandbox
- 送信ドメイン認証
- 顧客サポート
- 執筆活動・公演活動・エンジニアブログ・技報

WIDE Project

M3AAWG

openSUSE (趣味)

自己紹介

法人系メールセキュリティサービスの運用と ID とサーバ証明書

IIJ ID
- IDaaS・ガバナンス管理
- サーバ証明書

SecureMX
- ウイルス対策
- 迷惑メール対策
- Sandbox
- 送信ドメイン認証
- 顧客サポート
- 執筆活動・公演活動・エンジニアブログ・技報

古賀 勇 (Isamu Koga)

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2部
アプリケーションサービス運営課・課長

Power Automate エバンジェリスト (自称) **「自動化は正義」**

WIDE Project

M3AAWG (Messaging Malware Mobile Anti-Abuse Working Group)

openSUSE (趣味)

メールセキュリティ 2025 アップデート

(1) 送信ドメイン認証 DMARC ポリシー強化

(2) 経路暗号化(STARTTLS)と証明書管理の課題

(3) メール大量配信時の注意点

メールセキュリティ 2025 アップデート

- **(1) 送信ドメイン認証 DMARC ポリシー強化**

(2) 経路暗号化(STARTTLS)と証明書管理の課題

(3) メール大量配信時の注意点

別紙

（公印及び契印省略）

総基用第 76 号
令和７年９月１日

一般社団法人電気通信事業者協会会長　島田　明　殿
一般社団法人テレコムサービス協会会長　是枝　周樹　殿
一般社団法人日本インターネットプロバイダー協会会長　久保　真　殿
一般社団法人日本ケーブルテレビ連盟会長　塩冶　憲司　殿

総務省総合通信基盤局長
湯本　博信

フィッシングメール対策の強化について（要請）

平素より、情報通信行政に御理解と御協力をいただいておりますことに、厚く御礼申し上げます。

フィッシングメール対策について、政府は、「国民を詐欺から守るための総合対策 2.0（令和７年４月 22 日犯罪対策閣僚会議決定）」において、「詐欺メール、詐欺 SMS による被害防止等のための取組」として、「送信ドメイン認証技術（DMARC 等）への更なる対応促進」を掲げているところです。

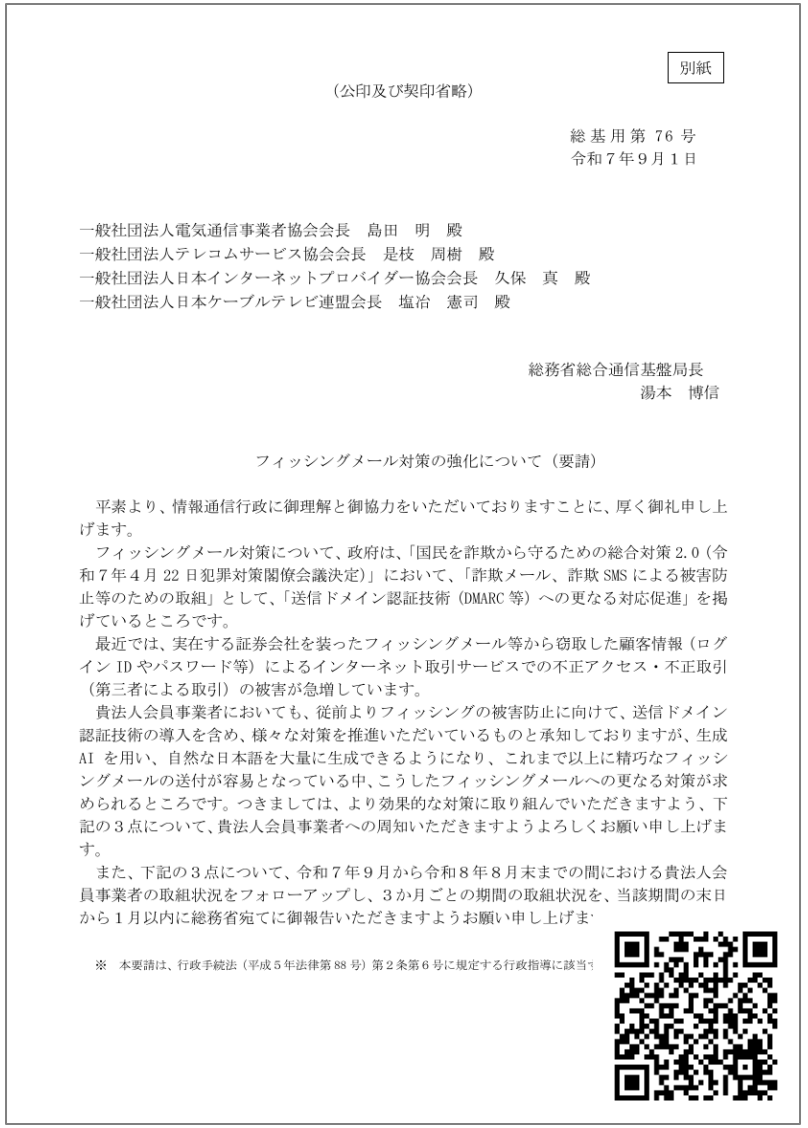
最近では、実在する証券会社を装ったフィッシングメール等から窃取した顧客情報（ログイン ID やパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増しています。

貴法人会員事業者においても、従前よりフィッシングの被害防止に向けて、送信ドメイン認証技術の導入を含め、様々な対策を推進いただいているものと承知しておりますが、生成 AI を用い、自然な日本語を大量に生成できるようになり、これまで以上に精巧なフィッシングメールの送付が容易となっている中、こうしたフィッシングメールへの更なる対策が求められるところです。つきましては、より効果的な対策に取り組んでいただきますよう、下

https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000260.html

総務省「フィッシングメール対策の強化について（要請）」

事業者団体を通じて電気通信事業者への要請文章



別紙

（公印及び契印省略）

総基用第 76 号
令和７年９月１日

一般社団法人電気通信事業者協会会長　島田　明　殿
一般社団法人テレコムサービス協会会長　是枝　周樹　殿
一般社団法人日本インターネットプロバイダー協会会長　久保　真　殿
一般社団法人日本ケーブルテレビ連盟会長　塩冶　憲司　殿

総務省総合通信基盤局長
湯本　博信

フィッシングメール対策の強化について（要請）

平素より、情報通信行政に御理解と御協力をいただいておりますことに、厚く御礼申し上げます。

フィッシングメール対策について、政府は、「国民を詐欺から守るための総合対策 2.0（令和７年４月 22 日犯罪対策閣僚会議決定）」において、「詐欺メール、詐欺 SMS による被害防止等のための取組」として、「送信ドメイン認証技術（DMARC 等）への更なる対応促進」を掲げているところです。

最近では、実在する証券会社を装ったフィッシングメール等から窃取した顧客情報（ログイン ID やパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増しています。

貴法人会員事業者においても、従前よりフィッシングの被害防止に向けて、送信ドメイン認証技術の導入を含め、様々な対策を推進いただいているものと承知しておりますが、生成 AI を用い、自然な日本語を大量に生成できるようになり、これまで以上に精巧なフィッシングメールの送付が容易となっている中、こうしたフィッシングメールへの更なる対策が求められるところです。つきましては、より効果的な対策に取り組んでいただきますよう、下記の３点について、貴法人会員事業者への周知いただきますようよろしくお願い申し上げます。

また、下記の３点について、令和７年９月から令和８年８月末までの間における貴法人会員事業者の取組状況をフォローアップし、３か月ごとの期間の取組状況を、当該期間の末日から１月以内に総務省宛てに御報告いただきますようお願い申し上げま

※　本要請は、行政手続法（平成５年法律第 88 号）第２条第６号に規定する行政指導に該当

https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000260.html

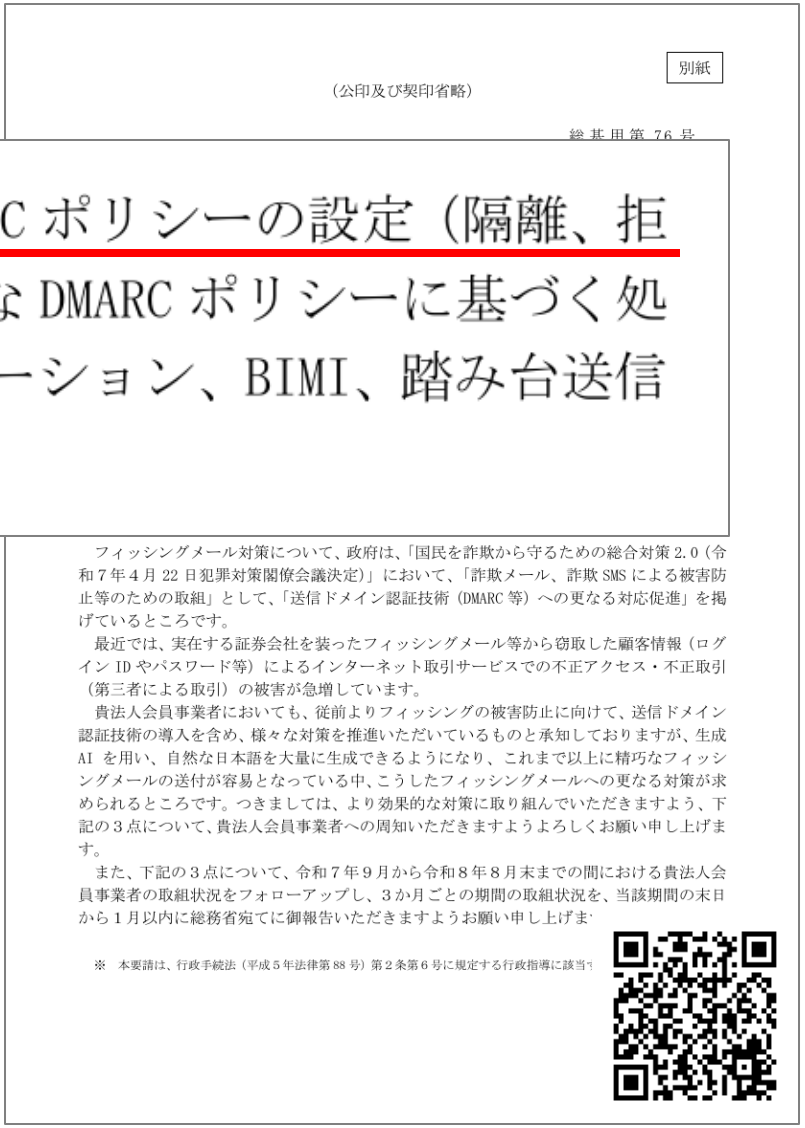
総務省「フィッシングメール対策の強化について（要請）」

事業者団体を通じて電気通信事業者への要請文章

（２）なりすましメール対策として有効な DMARC の導入や DMARC ポリシーの設定（隔離、拒否）を行うこと。送信側だけでなく受信側についても、適切な DMARC ポリシーに基づく処理やレポート送信を設定すること。また、ドメインレピュテーション、BIMI、踏み台送信対策等の更なる対策の導入を積極的に検討していくこと。

DMARC ポリシーの設定（**隔離、拒否**）を行うこと

p=quarantine/reject の話だ！



別紙

（公印及び契印省略）

総基用第 76 号

フィッシングメール対策について、政府は、「国民を詐欺から守るための総合対策 2.0（令和７年４月 22 日犯罪対策閣僚会議決定）」において、「詐欺メール、詐欺 SMS による被害防止等のための取組」として、「送信ドメイン認証技術（DMARC 等）への更なる対応促進」を掲げているところです。

最近では、実在する証券会社を装ったフィッシングメール等から窃取した顧客情報（ログイン ID やパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増しています。

貴法人会員事業者においても、従前よりフィッシングの被害防止に向けて、送信ドメイン認証技術の導入を含め、様々な対策を推進いただいているものと承知しておりますが、生成 AI を用い、自然な日本語を大量に生成できるようになり、これまで以上に精巧なフィッシングメールの送付が容易となっている中、こうしたフィッシングメールへの更なる対策が求められるところです。つきましては、より効果的な対策に取り組んでいただきますよう、下記の３点について、貴法人会員事業者への周知いただきますようよろしくお願い申し上げます。

また、下記の３点について、令和７年９月から令和８年８月末までの間における貴法人会員事業者の取組状況をフォローアップし、３か月ごとの期間の取組状況を、当該期間の末日から１月以内に総務省宛てに御報告いただきますようお願い申し上げま

※　本要請は、行政手続法（平成５年法律第 88 号）第２条第６号に規定する行政指導に該当

https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000260.html

(参考)
日本国内 4 キャリアで見る DMARC ポリシー

(参考) 日本国内 4 キャリアの DMARC ポリシー

(参考) 日本国内 4 キャリアの DMARC ポリシー

全社 p=quarantine/reject 設定済み

```
$ dig _dmarc.docomo.ne.jp txt +short
"v=DMARC1; p=quarantine; sp=quarantine;
   pct=100; rua=mailto:docomo00001-ra@dmarc25.jp"
```

p=quarantine (隔離)

```
$ dig _dmarc.ezweb.ne.jp txt +short
"v=DMARC1; p=reject;
   rua=mailto:kddi00001-ra@dmarc25.jp,
   mailto:report_dmarc_rua.ez@ezweb.ne.jp"
```

p=reject (拒否)

```
$ dig _dmarc.i.softbank.jp txt +short
"v=DMARC1; p=quarantine;
   rua=mailto:softbankmail00001-ra@dmarc25.jp"
```

p=quarantine (隔離)

```
$ dig _dmarc.rakumail.jp txt +short
"v=DMARC1; p=reject;
   rua=mailto:dmarc-report-a@rx.rakuten.co.jp"
```

p=reject (拒否)

NTT ドコモさんの見解 2024

次のSTEPであるなりすましメールの排除へ

p=quarantine/rejectへ進む時です

	具体例	第三者チェック	なりすましメールの排除	DMARC ※header fromの認証	SPF ※envelope fromの認証
	ドコモメール公式アカウント	○	○		
	BIMI	○	○		
新しい基準	p=quarantine/reject	×	○		
	p=none	×	×		
古い基準	DMARC未導入	×	×		
	認証失敗	×	×		

JPAAWG

第7回 JPAAWG General Meeting
https://meetings.jpaawg.org/program/

まとめ

・DMARCの**p=noneは順調**に普及！

・**次はp=quarantine/reject**を導入すべき！

・並行して、**正規メールのPR**も！

JPAAWG

16

KDDI さんの見解 2024

第7回 JPAAWG General Meeting
https://meetings.jpaawg.org/program/

auが発信するメールへのDMARC対応

au系ドメイン：通信／金融／各種サービスのサブドメイン多数

2023/10 全社横断でDMARC(p=reject)推進で方針決定
2024/02 p=reject化完遂へ

DMARC導入の背景と課題

DMARCレポート分析	お客様からの迷惑メール情報分析
詐称ドメイン多数・・・	DMARCすり抜けメール増加傾向

DMARC(p=reject)／BIMI導入

au主要ドメイン：au.com/ezweb.ne.jp/auone.jp
サブドメインを含め、全ドメインでDMARC reject化完了！

JPAAWG

6th General-Meeting資料抜粋

金融やEC系業界等を中
当社のau PAYなども

まとめ

・キャリアメールは国内1億人のDMARC対応メール

・DMARC みんなでReject 目指しましょう！（字余り

・Reject化は（少し大変だけど）怖くない！
結構あっさり実現できます！

・Reject化終われば次はBIMIで正規メールアピールを！

by KDDI
（懐かしい

JPAAWG

28

ソフトバンクさんの見解 2024

p＝reject

絶大な効果あり！！

DMARCポリシーをrejectに変更した
なりすましメールのブロック件数急増
さらに、**なりすましメール通数自体が減**

JPAAWG

第7回 JPAAWG General Meeting
https://meetings.jpaawg.org/program/

まとめ

①なりすましドメインとして実在するサービスのドメインが悪用されている

・金融、宅配、決済可能なキャリアや企業のドメインが悪用されていたが、
フリマ系、某大手倉庫店のドメインを悪用するパターンも増加傾向

②キャリアでDMARCフィルタ導入

・**国内3キャリアはデフォルトON！1億ユーザーが適用中！！**
・**DMARCポリシーを「reject」に変更するだけで大きな効果**

ここ重要！！

③転送メールサービスはARC署名で対策！？

・受信側ARCに対応する企業は増えるのか？

JPAAWG

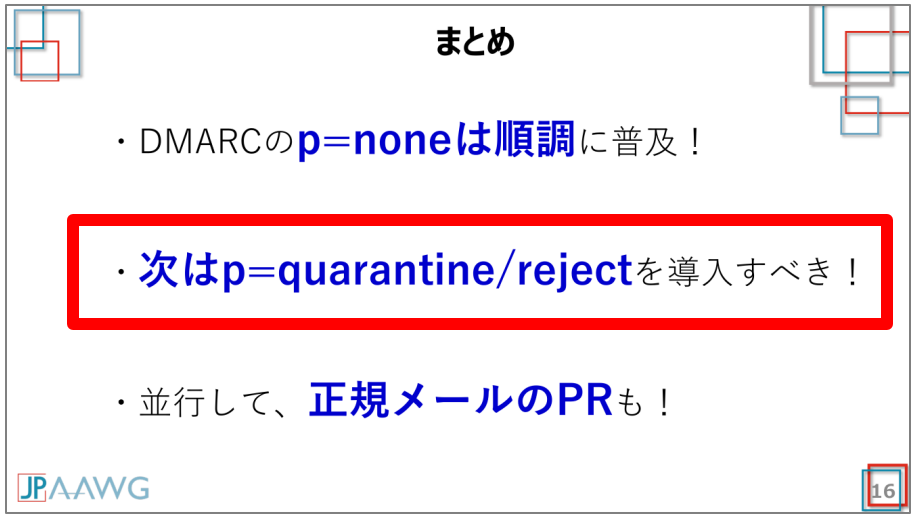
38

(IIJ 古賀の予想) DMARC p=reject の時代がきます

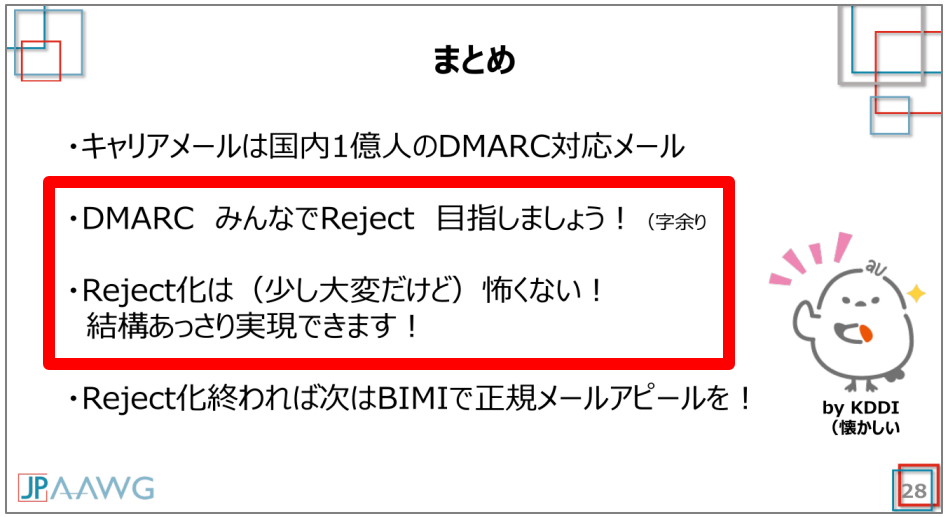
国内 3キャリアが声を揃えて p=reject 共同声明

第7回 JPAAWG General Meeting
https://meetings.jpaawg.org/program/

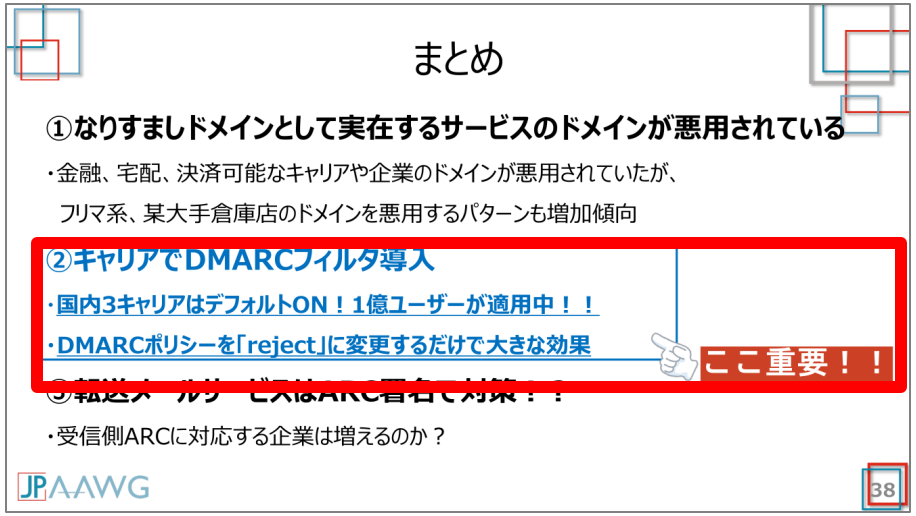
NTT ドコモ



KDDI



ソフトバンク



p=reject にしないと
届かない時代へ突入間近

(準備がまだなら急いで)

Yahoo! Japan も追従

Yahoo!メール
ドメイン認証技術「DMARC」について

DMARCとは

DMARC（Domain-based Message Authentication, Reporting, and Conformance）とは、なりすましメール対策の技術で、電子メールの送信元のドメインを認証する技術の一つです。
Yahoo!メールでは以前からSPF（※1）、DKIM（※2）というなりすましメール対策技術を導入しています。
これらがYahoo!メール側でなりすましを判断する技術であるのに対して、2020年3月より順次導入されるDMARCは「なりすまされたメールの扱い（ブロック、迷惑メール判定など）を設定」することで、ユーザーの皆様になりすまされたメールが届かないようにするための技術となります。
これによって今まで以上になりすましメール対策が強化され、より安心・安全なメールとしてお使いいただけるようになります。

メール送信事業者様へ

DMARC導入によって貴社になりすましたメールを自発的に防ぐことができるようになります。
※DMARCレポートの送信については、現在Yahoo!メールでは対応しておりません。

DMARCの仕組み

DNSサーバ

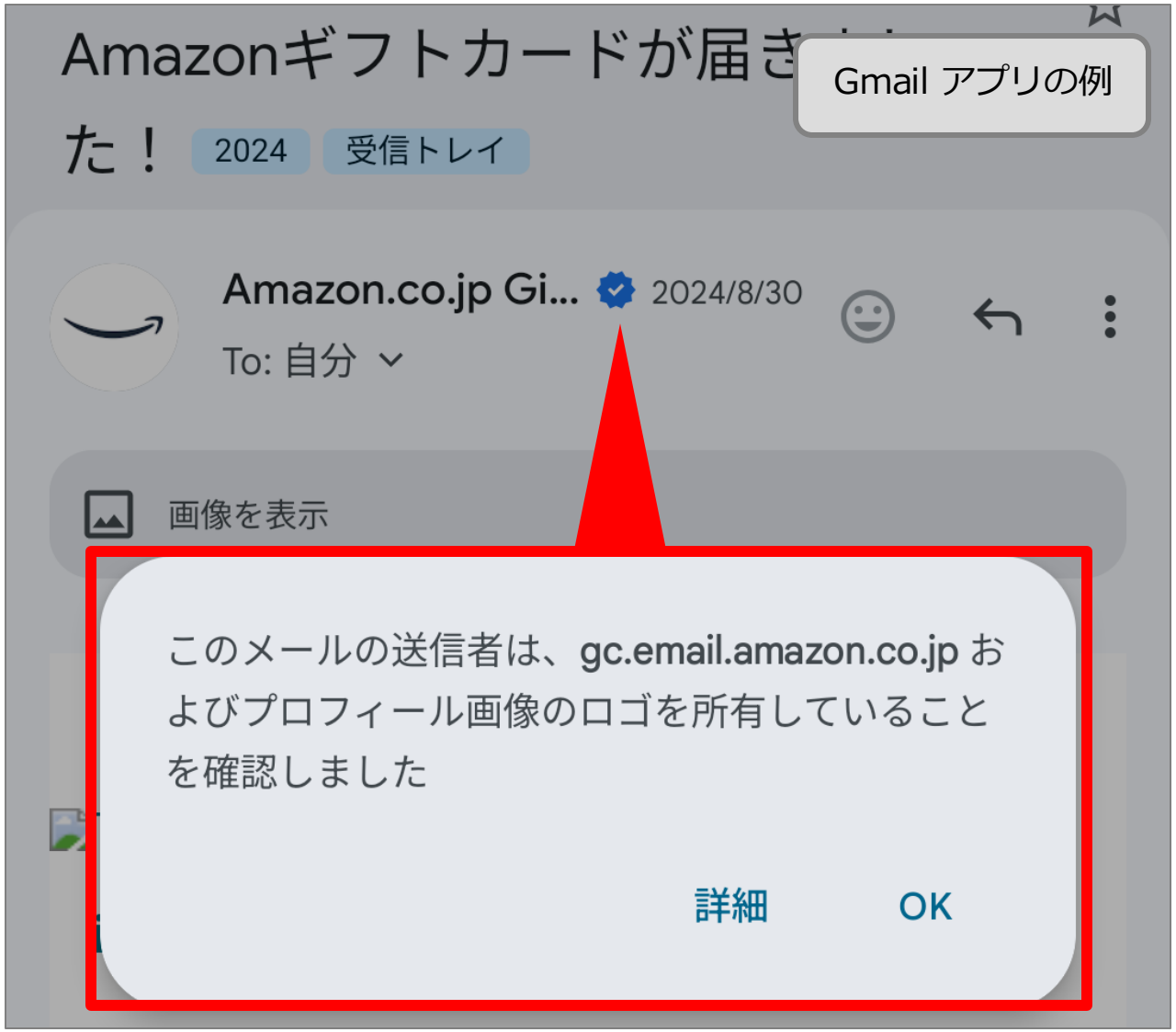
```
$ dig _dmarc.yahoo.co.jp txt +short
"v=DMARC1; p=quarantine;
   rua=mailto:ymail_dmarc_report@yahoo.co.jp"
```

Yahoo!メール ドメイン認証技術「DMARC」について
https://mail.yahoo.co.jp/antispam/dmarc.html

(補足) BIMI は ← このマークが超重要 (Gmail の場合)

BIMI(VMC)認証されたことを示す証拠

- **マークの示し方は各社それぞれ**
  - 利用しているアプリ・Web メールの案内を参照
  - UI/UX 設計者は、非認証メールと誤認しないよう注意しながら、利用者の学習コストが小さくなるようにする
- **Gmail の場合、アバターとの違いに注意**
  - アバターの場合は マークがない
  - ただし CMC 証明書で BIMI 認証された場合、ロゴは表示されるが マークがない
  - (このあたりがちょっとややこしい)
- **やはり DMARC p=reject が最重要**
  - なりすましメールを受信者に届かせない世界が最も大切



※ VMC = Verified Mark Certificate (厳しい認証条件あり)
※ CMC = Common Mark Certificate (VMC より取りやすい認証条件)

(緊急告知) Google Sender Guidelines 2025/11 アップデート

2025年 11月より、規制をさらに強化することを発表

Gmail > Gmail の制限とポリシー > 一括送信メールを送信する > メール送信者のガイドラインに関するよくある質問

メール送信者のガイドラインに関するよくある質問

重要: Gmail では 2024 年 2 月以降、Gmail アカウントに 1 日あたり 5,000 件以上のメールを送信する送信者に対し、1. 送信メールを認証すること、2. 未承諾のメールまたは迷惑メールを送信しないようにすること、3. 受信者がメールの配信登録を容易に解除できるようにすること、の 3 つが義務付けられます。詳しくは、1 日あたり 5,000 件以上のメールを送信する場合の要件をご覧ください。

2025 年 11 月より、Gmail では非準拠のトラフィックに対する違反措置の強化を進めていきます。メール送信者の要件を満たしていない送信元からのメールは配信が中断され、一時的な拒否や永続的な拒否などの措置が講じられることがあります。

2025 年 11 月より、Gmail では非準拠のトラフィックに対する違反措置の強化を進めていきます。メール送信者の要件を満たしていない送信元からのメールは配信が中断され、一時的な拒否や永続的な拒否などの措置が講じられることがあります。

▲ メール送信者のガイドラインに関するよくある質問 (日本語)
https://support.google.com/a/answer/14229414?hl=ja

メールセキュリティ 2025 アップデート

(1) 送信ドメイン認証 DMARC ポリシー強化

▶ **(2) 経路暗号化(STARTTLS)と証明書管理の課題**

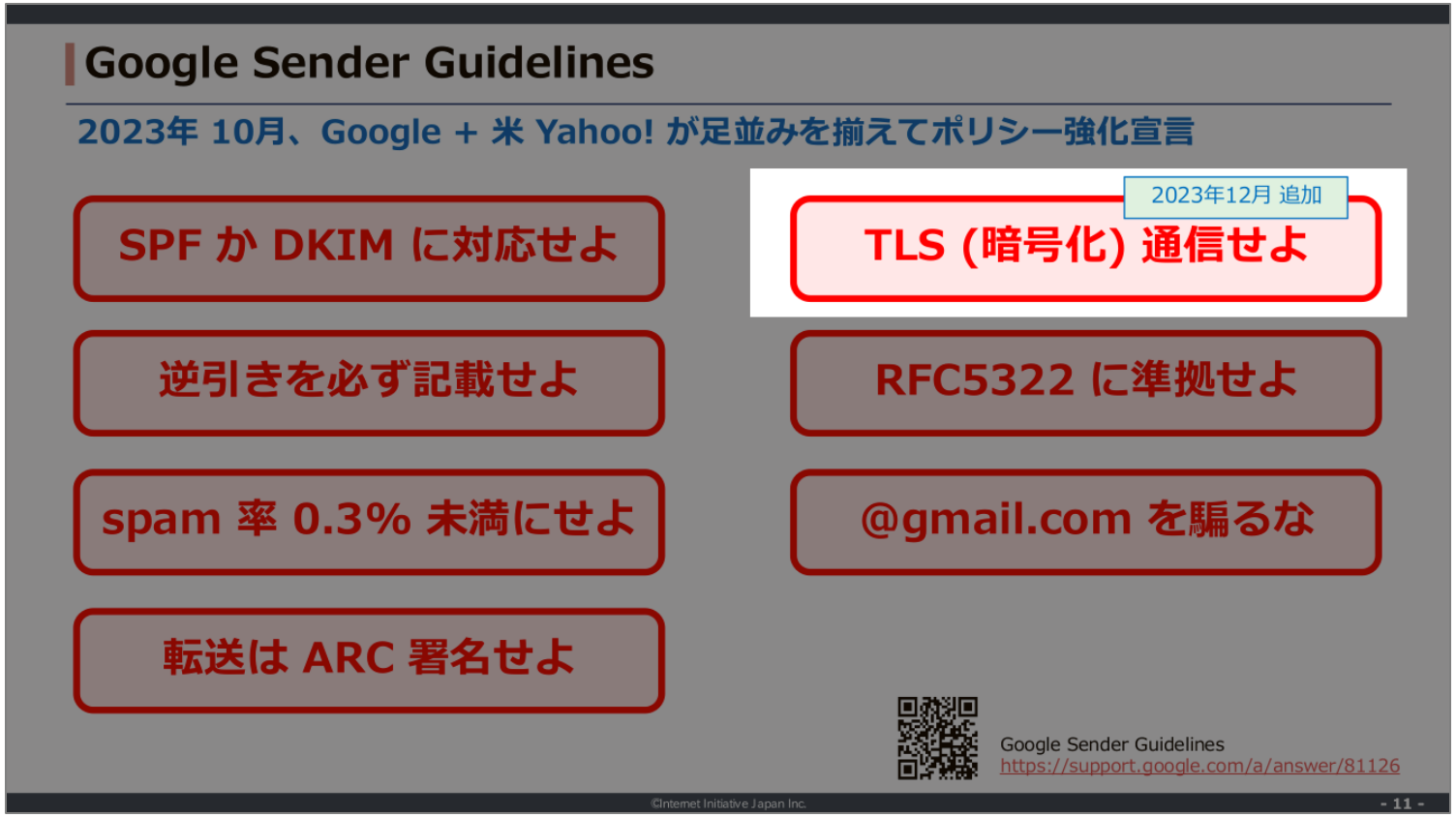
(3) メール大量配信時の注意点

(復習) Google Sender Guidelines

2023年 12月、ガイドラインのアップデートで TLS 通信が追加要求された

- **STARTTLS 対応が加速**
  - 従来から受信メールが経路暗号化されていると 🔒 マークの表示はされていた。

  - 「ガイドラインに準拠しないと届かなくなる」
  - 一気に普及



▲ C7 2024年のメール運用と DMARC (Internet Week 2024)
https://www.nic.ad.jp/ja/materials/iw/2024/proceedings/c7/

経路暗号化(STARTTLS)の普及状況

経路暗号化ほぼ 100% を達成、メールも常時 TLS の時代へ

IIJ による定点観測

80～90% 前後を推移

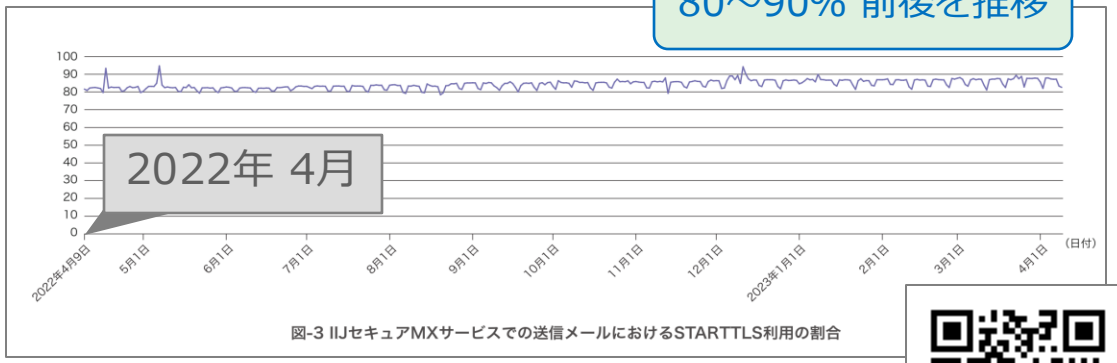


図-3 IIJセキュアMXサービスでの送信メールにおけるSTARTTLS利用の割合

▲ Internet Infrastructure Review (IIR) Vol.59
https://www.iij.ad.jp/dev/report/iir/059/01.html

ほぼ100%

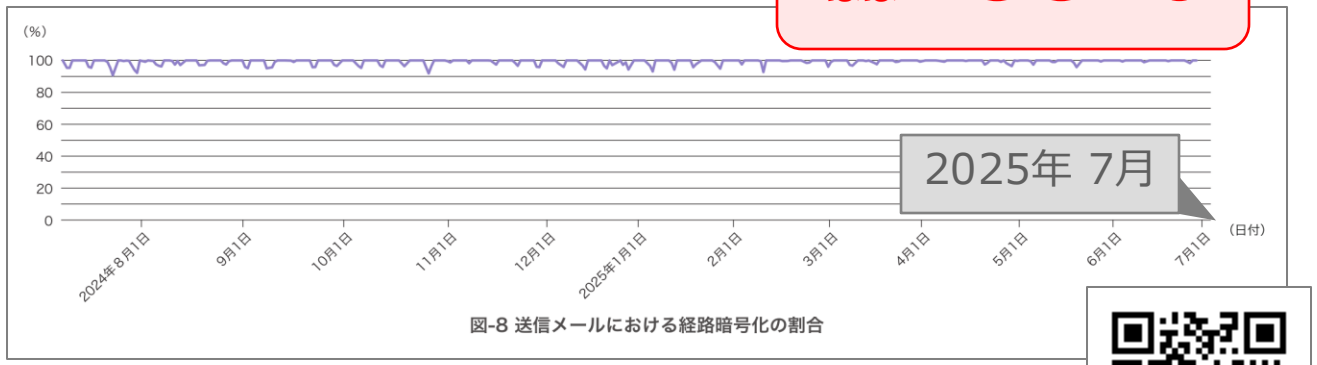
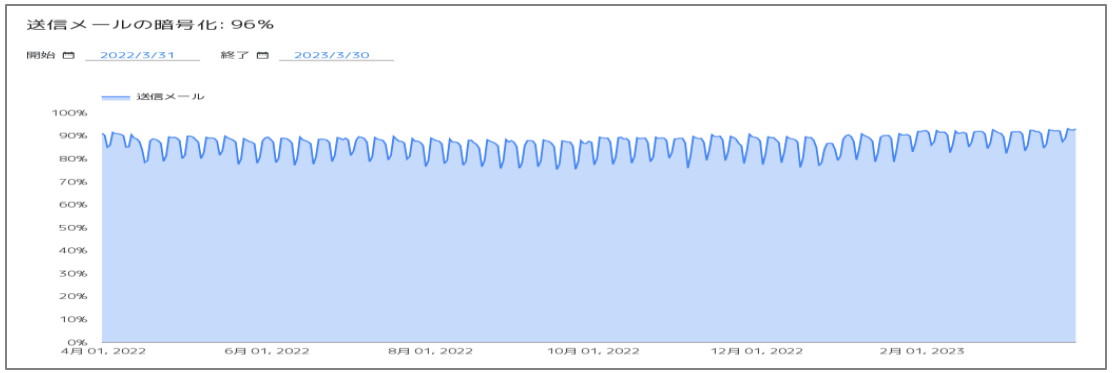


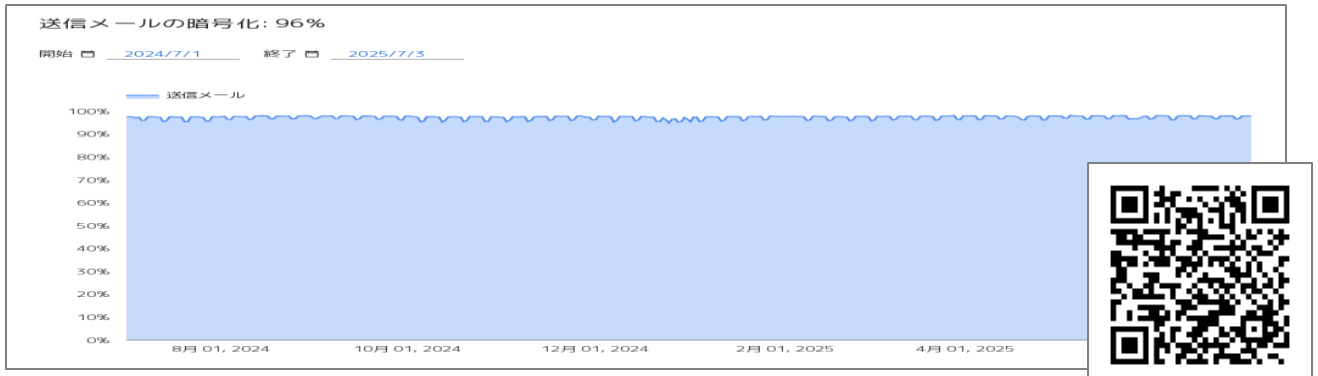
図-8 送信メールにおける経路暗号化の割合

▲ Internet Infrastructure Review (IIR) Vol.67
https://www.iij.ad.jp/dev/report/iir/067/02.html

Google 透明性レポート

https://transparencyreport.google.com/safer-email/overview





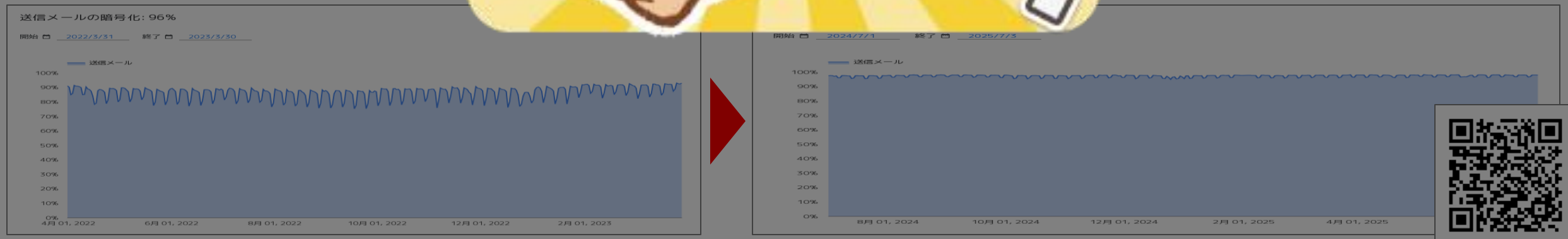
経路暗号化(STARTTLS)の普及状況

経路暗号化ほぼ 100% を達成、メールも常時 TLS の時代へ

■ IIJ による定点観測

▲ Internet Infrastructure Review (IIR) Vol.59 IIR) Vol.67
https://www.iij.ad.jp/dev/report/iir/059/01.h r/067/02.html

■ Google 透明性レポート
https://transparencyreport.google.com/safer-e



経路暗号化(STARTTLS)の普及状況

経路暗号化ほぼ 100% を達成、メールも常時 TLS の時代へ

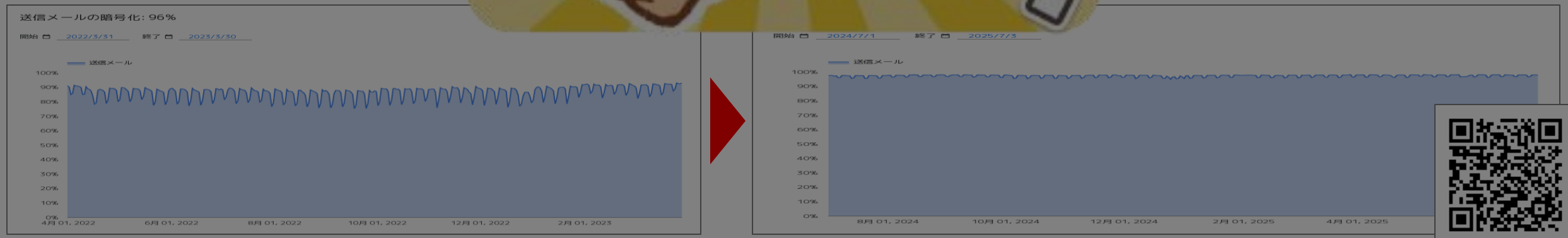
■ IIJ による定点観測

▲ Internet In
https://www.

ところが...

■ Google 透明性レポート

https://transparencyreport.google.com/safer-e



サーバ証明書業界動向 (有効期限の短縮化)

業界団体(CA/B フォーラム)にて、認証局が発行できるサーバ証明書の有効期限が段階的に 47 日まで短縮されることが可決 (2025/04/13)

SC-081: Introduce Schedule of Reducing Validity and Data Reuse Periods
https://github.com/cabforum/servercert/pull/553

■ 有効期限短縮のスケジュール

	発行可能な証明書の期限
現在	最大 398 日間
2026/03/15 以降	最大 200 日間
2027/03/15 以降	最大 100 日間
2029/03/15 以降	**最大 47 日間**

ココ

■ この動きの目的

1. 証明書の信頼性向上
   - 再認証しない限り、証明書の信頼性は時間とともに徐々に低下していく。
   - 例えば、ドメイン名はドロップキャッチされて別の組織が使うこともある。
2. セキュリティリスクの低減
   - 秘密鍵が漏洩したり、認証局によって誤発行された証明書の悪用期間が減少。

サーバ証明書 有効期限短縮に伴う課題

サービス運営のリスク・品質低下・破綻に繋がりかねない

作業工数の増加

作業リスクの増加

にも関わらず、この作業自体に生産性はない、機能追加など顧客へのメリットもない

サーバ証明書 有効期限短縮に伴う課題

サービス運営のリスク・品質低下・破綻に繋がりかねない

作業工数の増加

作業リスクの増加

にも関わらず、この作業自体に生産性はない、機能追加など顧客へのメリットもない

■ サーバ証明書 三大失敗あるある

1. 入替そのものを失念して証明書の有効期限が失効
2. 中間証明書の入替を失念・ミスしてチェインが辿れない
3. 上記作業に伴うオペミス・設定間違い

・ブラウザは他サイトで得た中間証明書をキャッシュする
・Web サイトを閲覧するだけのテストでは発見しづらい

必ず openssl コマンドで確認する!!

```
$ openssl s_client -connect mx.example.jp:25 -starttls smtp
```

サーバ証明書 有効期限短縮に伴う課題

サービス運営のリスク・品質低下・破綻に繋がりかねない

作業工数の増加

作業リスクの増加

にも関わらず、この作業自体に生産性はない、機能追加など顧客へのメリットもない

■ **サーバ証明書 三大失敗あるある**

1. 入替そのものを失念して証明書の有効期限が失効
2. 中間証明書の入替を失念・ミスしてチェインが辿れない
3. 上記作業に伴うオペミス・設定間違い

全部やらかしたことがあります。本当にごめんなさい。

サーバ証明書業界動向 (有効期限の短縮化)

業界団体(CA/B フォーラム)にて、認証局が発行できるサーバ証明書の有効期限が段階的に 47 日まで短縮されることが可決 (2025/04/13)

SC-081: Introduce Schedule of Reducing Validity and Data Reuse Periods
https://github.com/cabforum/servercert/pull/553

■ 有効期限短縮のスケジュール

	発行可能な証明書の期限
ココ 現在	最大 398 日間
2026/03/15 以降	最大 200 日間
2027/03/15 以降	最大 100 日間
2029/03/15 以降	**最大 47 日間**

証明書入れ替え作業
自動化が実質不可避に
(メールサーバも例外なく影響あり！)

■ この動きの目的

1. 証明書の信頼性向上
   - 再認証しない限り、証明書の信頼性は時間とともに徐々に低下していく。
   - 例えば、ドメイン名はドロップキャッチされて別の組織が使うこともある。
2. セキュリティリスクの低減
   - 秘密鍵が漏洩したり、認証局によって誤発行された証明書の悪用期間が減少。
3. ライフサイクル管理と品質の向上
   - 期限が短くなると自動化せざるを得なくなる。
   - ゆえに証明書の更新忘れを防止・オペレーションミスのリスクを低減、安定性が向上。

サーバ証明書業界動向 (有効期限の短縮化)

業界団体(CA/B フォーラム)にて、認証局が発行できるサーバ証明書の有効期限が段階的に 47 日まで短縮さ[illegible]とが可決 (2025/04/13)

■ **有効期限短縮のスケジュール**

Schedule of Reducing Validity and Data Reuse Periods
[illegible]com/cabforum/servercert/pull/553

	発行可能な証[illegible]
ココ 現在	最[illegible]
2026/03/15 以降	最[illegible]
2027/03/15 以降	最大 10[illegible]
2029/03/15 以降	**最大 47 日間**

入れ替え作業
[illegible]化が実質不可避に
(メールサ[illegible]例外なく影響あり！)

■ **この動きの目的**

1. 証明書の信頼性向上
   - 再認証[illegible]
   - 例えば[illegible]
2. セキュリ[illegible]
   - 秘密鍵[illegible]
3. ライフサ[illegible]
   - 期限が[illegible]
   - ゆえに証明書の更新忘れを防止・オペレーションミスのリスクを低減、安定性が向上。

自動化しましょう

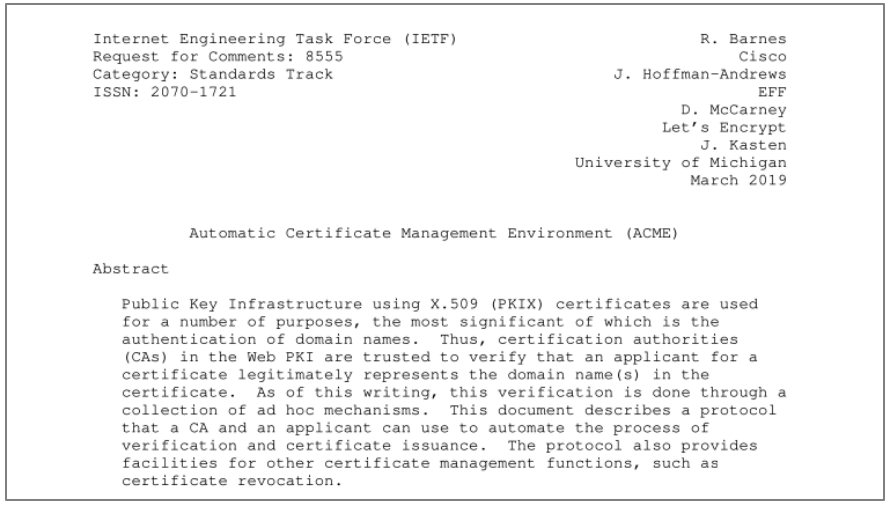
証明書更新の自動化プロトコル (ACME)

ACME に対応した認証局として Let's Encrypt が有名

- **Let's Encrypt**
  - 非営利団体 ISRG により運営・スポンサー多数
  - 2014 年設立、2015 年サービス開始
  - 7 億のサイトで利用中、累計 57 億枚発行
  - 発行に関わるコストは無償

- **ACME 対応クライアントあり**
  - (例) certbot、acme.sh、lego、cert-manager
  - 複数の実装があるので手軽に始められる
  - 仕組みが簡単なので手でも認証・発行できる

- **DV (Domain Validation) のみ対応**
  - 認証プロセスそのものが自動化されているため
  - OV/EV が欲しい場合は他の認証局に問い合わせる



Internet Engineering Task Force (IETF)
Request for Comments: 8555
Category: Standards Track
ISSN: 2070-1721

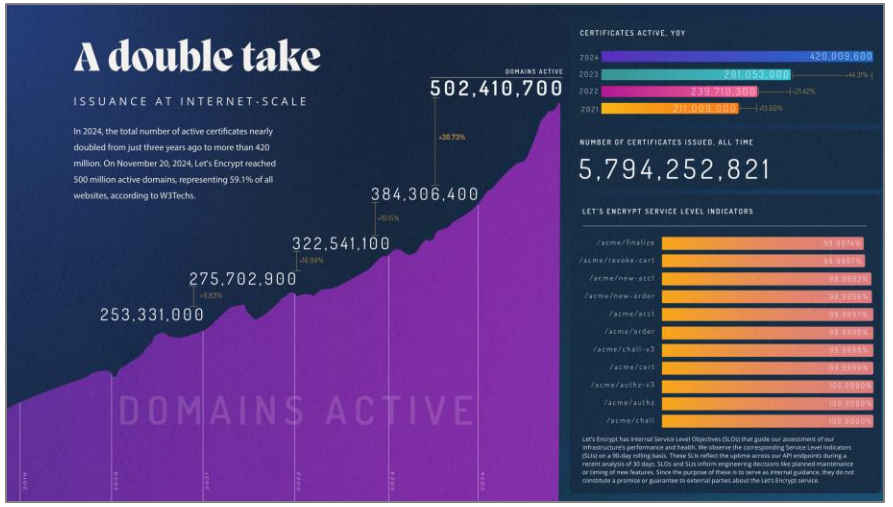
R. Barnes
Cisco
J. Hoffman-Andrews
EFF
D. McCarney
Let's Encrypt
J. Kasten
University of Michigan
March 2019

Automatic Certificate Management Environment (ACME)

Abstract

Public Key Infrastructure using X.509 (PKIX) certificates are used for a number of purposes, the most significant of which is the authentication of domain names. Thus, certification authorities (CAs) in the Web PKI are trusted to verify that an applicant for a certificate legitimately represents the domain name(s) in the certificate. As of this writing, this verification is done through a collection of ad hoc mechanisms. This document describes a protocol that a CA and an applicant can use to automate the process of verification and certificate issuance. The protocol also provides facilities for other certificate management functions, such as certificate revocation.

▲ RFC8555 Automatic Certificate Management Environment (ACME) https://datatracker.ietf.org/doc/html/rfc8555



▲ ISRG Annual Reports 2024 https://www.isrg.org/annual-reports/

(参考) IIJ セキュア MX サービスの事例

2024年 9月、全面的に Let's Encrypt を採用・更新を自動化

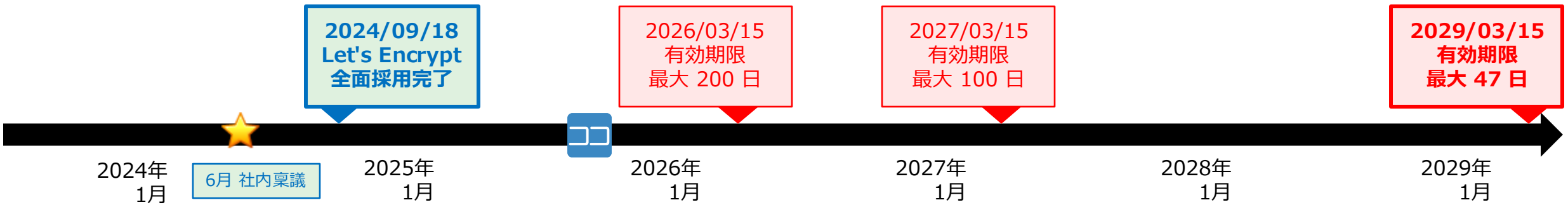
※1 “Moving Forward, Together” — Chrome Root Program Policy
https://chromium.googlesource.com/website/+/5943ad5e004c1cde2f869f1d67008a729e9ec12e/site/Home/chromium-security/root-ca-policy/moving-forward-together/index.md

■ 本取り組みの背景

- 2023年、Google がすべてのサーバ証明書の有効期限を最大 90 日にする方針を発表(※1)
- その後、CA/B フォーラムで有効期限短縮に関する議論が活発化したことから社内検討開始
- 多くの組織で利用されている CentOS 7 が 2024/06/30 に EoL
  - 仮にルート証明書ストアが全く更新されていない環境があったとしてもサポート対象外になった
  - ルート証明書は公開されているので、インストールしてもらえれば継続利用可能なワークアラウンドもある (非推奨)

■ 目的は自動化

- 自動化が達成できれば、本質的にはどの認証局(CA)でも良い
- 特にメール間の通信はユーザに見えないため、実質的に DV/OV/EV の区別はない



(参考) Entrust 認証局 の Distrust

- **Google が Chrome 127 から Entrust を Distrust**
  - 2024/06/27、Chrome ブラウザのルート証明書から外すことを決定
  - Apple、Mozilla も追従、Fortune 1000 の約 20 % (約 57 万枚) が影響

- **過去にも認証局の Distrust は起きている**

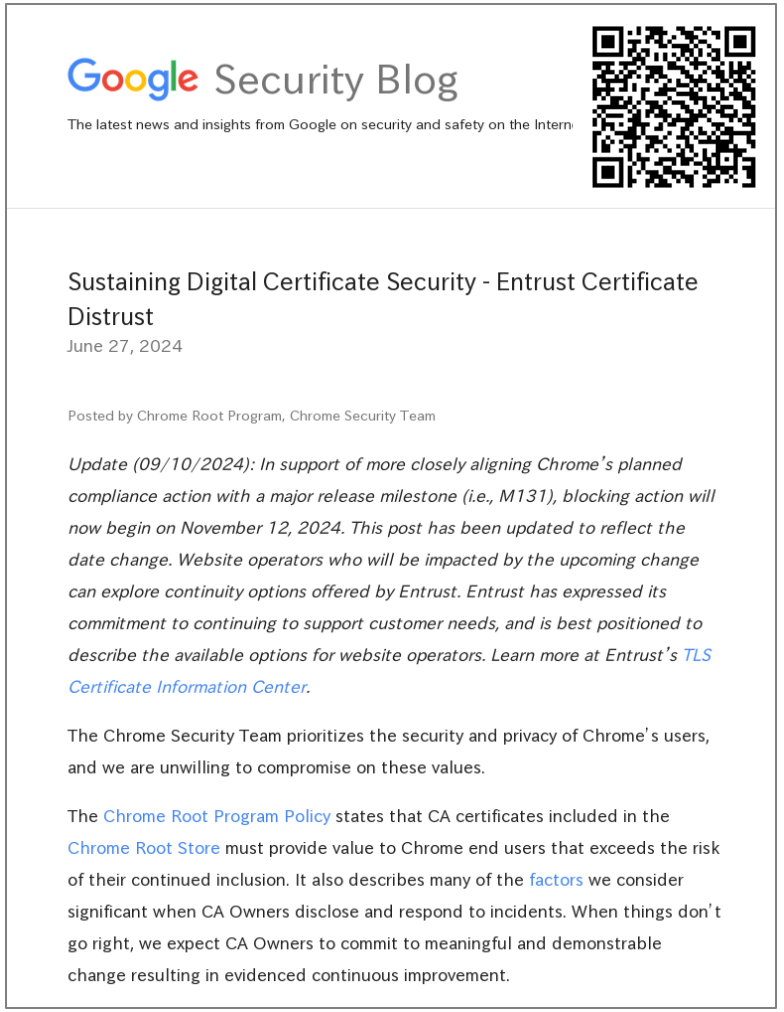
2016年	Distrusting WoSign and StartCom Certificates
2018年	Chrome's Plan to Distrust Symantec Certificates
2022年	TrustCor Certificate Distrust

自組織でない都合で
認証局が利用できなく
なることを想定して
準備・運用しておく

ACME 運用なら

選択肢が増える

容易に変更できる



Google Security Blog

The latest news and insights from Google on security and safety on the Intern

Sustaining Digital Certificate Security - Entrust Certificate Distrust

June 27, 2024

Posted by Chrome Root Program, Chrome Security Team

Update (09/10/2024): In support of more closely aligning Chrome's planned compliance action with a major release milestone (i.e., M131), blocking action will now begin on November 12, 2024. This post has been updated to reflect the date change. Website operators who will be impacted by the upcoming change can explore continuity options offered by Entrust. Entrust has expressed its commitment to continuing to support customer needs, and is best positioned to describe the available options for website operators. Learn more at Entrust's TLS Certificate Information Center.

The Chrome Security Team prioritizes the security and privacy of Chrome's users, and we are unwilling to compromise on these values.

The Chrome Root Program Policy states that CA certificates included in the Chrome Root Store must provide value to Chrome end users that exceeds the risk of their continued inclusion. It also describes many of the factors we consider significant when CA Owners disclose and respond to incidents. When things don't go right, we expect CA Owners to commit to meaningful and demonstrable change resulting in evidenced continuous improvement.

▲ Sustaining Digital Certificate Security - Entrust Certificate Distrust
https://security.googleblog.com/2024/06/sustaining-digital-certificate-security.html

(参考) Entrust 認証局 の Distrust

- **Google が Chrome 127 から Entrust を Distrust**
  - 2024/06/27、Chrome ブラウザのルート証明書から外すことを決定
  - Apple、Mozilla も追従、Fortune 1000 の約 20 % (約 57 万枚) が影響

- **過去にも認証局の Distrust は起きている**

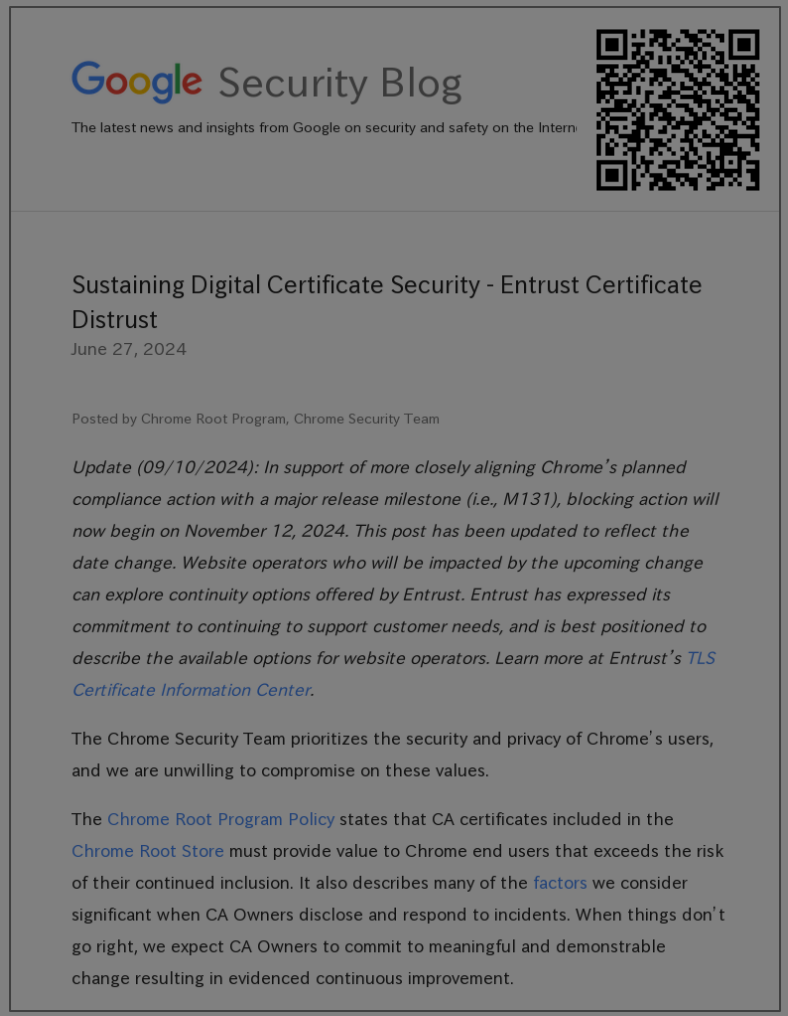
2016年	Distrusting WoSign and StartCom Certificates
2018年	Chrome's Plan to Distrust Symantec Certificates
2022年	TrustCor Certificate Distrust

自組織でない都合で
認証局が利用できなく
なることを想定して
準備・運用しておく

ACME 運用なら

選択肢が増える

容易に変更できる



Google Security Blog

The latest news and insights from Google on security and safety on the Intern

Sustaining Digital Certificate Security - Entrust Certificate Distrust

June 27, 2024

Posted by Chrome Root Program, Chrome Security Team

Update (09/10/2024): In support of more closely aligning Chrome's planned compliance action with a major release milestone (i.e., M131), blocking action will now begin on November 12, 2024. This post has been updated to reflect the date change. Website operators who will be impacted by the upcoming change can explore continuity options offered by Entrust. Entrust has expressed its commitment to continuing to support customer needs, and is best positioned to describe the available options for website operators. Learn more at Entrust's TLS Certificate Information Center.

The Chrome Security Team prioritizes the security and privacy of Chrome's users, and we are unwilling to compromise on these values.

The Chrome Root Program Policy states that CA certificates included in the Chrome Root Store must provide value to Chrome end users that exceeds the risk of their continued inclusion. It also describes many of the factors we consider significant when CA Owners disclose and respond to incidents. When things don't go right, we expect CA Owners to commit to meaningful and demonstrable change resulting in evidenced continuous improvement.

▲ Sustaining Digital Certificate Security - Entrust Certificate Distrust
https://security.googleblog.com/2024/06/sustaining-digital-certificate-security.html

(参考) Entrust 認証局 の Distrust

- Google が Chrome 127 から Entrust を Distrust
  -
  -
- 過

自
認
た
準備・運用しておく

容易に変更できる

ificate

lanned
action will
ect the
g change
d its
tioned to
rust's TLS

e's users,

n the
eds the risk
onsider
hings don't
able

change resulting in evidenced continuous improvement.

▲ Sustaining Digital Certificate Security - Entrust Certificate Distrust
https://security.googleblog.com/2024/06/sustaining-digital-certificate-security.html

(参考) Entrust 認証局 の Distrust

- Google が Chrome 127 から Entrust を Distrust
  -
  -
- 過

自
認
な
準備・運用しておく

容易に変更できる

change resulting in evidenced continuous improvement.

▲ Sustaining Digital Certificate Security - Entrust Certificate Distrust
https://security.googleblog.com/2024/06/sustaining-digital-certificate-security.html

Let's Encrypt に移行する際の課題・検討事項整理

1. 証明書管理
自動化の動機

2. 証明書の使い分け
(DV/OV/EV)

3. 利用者への影響

Let's Encrypt に移行する際の課題・検討事項整理

1. 証明書管理自動化の動機

- 作業コストの省力化・オペミス回避
- 品質向上と運用のイノベーションを達成
- ACME でマルチベンダー対応
  (あとで認証局を変更しても良い)

2. 証明書の使い分け
(DV/OV/EV)

3. 利用者への影響

Let's Encrypt に移行する際の課題・検討事項整理

1. 証明書管理自動化の動機

- 作業コストの省力化・オペミス回避
- 品質向上と運用のイノベーションを達成
- ACME でマルチベンダー対応
  (あとで認証局を変更しても良い)

2. 証明書の使い分け
(DV/OV/EV)

- 経路暗号化目的なら DV でも達成可
- 昨今ブラウザでも違いは見えづらい
- MTA・MSA 間通信はもっと見えない

3. 利用者への影響

Let's Encrypt に移行する際の課題・検討事項整理

1. 証明書管理自動化の動機

- 作業コストの省力化・オペミス回避
- 品質向上と運用のイノベーションを達成
- ACME でマルチベンダー対応
  (あとで認証局を変更しても良い)

2. 証明書の使い分け
(DV/OV/EV)

- 経路暗号化目的なら DV でも達成可
- 昨今ブラウザでも違いは見えづらい
- MTA・MSA 間通信はもっと見えない

3. 利用者への影響

- 事前に認証局変更をお知らせ
- OV → DV 変更も問題なし
- 目立った問い合わせなし、あっさり実現

ここまでのまとめ

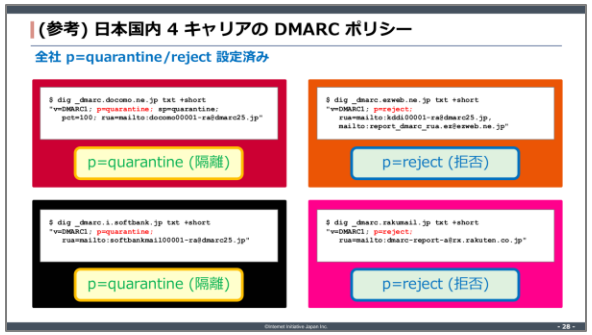
ここまでのまとめ

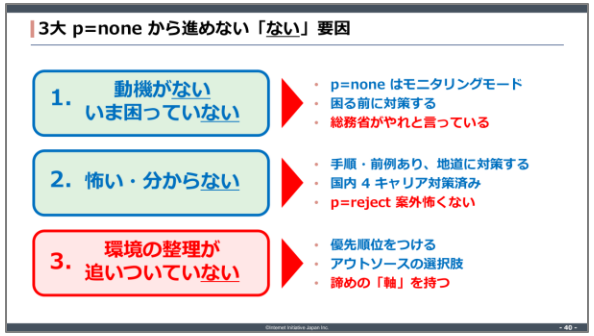
2025年、メールセキュリティをアップデートしましょう

p=reject
意外に怖くない

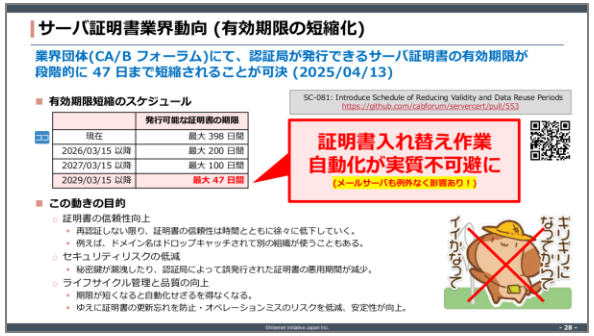
証明書期限短縮
今から備えて

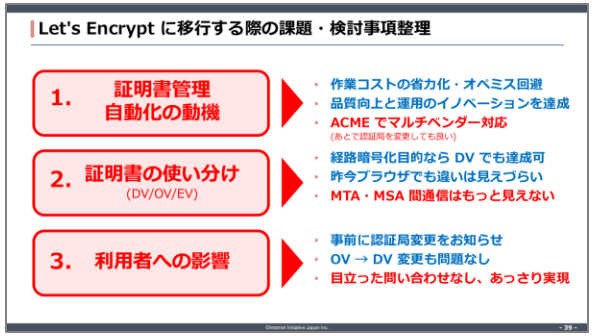
大手キャリアも対応済み、世の中は p=reject へ





メールも常時 TLS 時代へ





ここまでのまとめ

2025年、メールセキュリティをアップデート

p=rei
意外に

証明
今、

は p=reject へ

進めない「ない」要因

- p=none はモニタリングモード
- 困る前に対策する
- 総務省がやれと言っている

- 手順・前例あり、地道に対策する
- 国内 4 キャリア対策済み
- p=reject 案外怖くない

- 優先順位をつける
- アウトソースの選択肢
- 諦めの「軸」を持つ

TLS 時代へ

動向 (有効期限の短縮化)

CA/B フォーラム)にて、認証局が発行できるサーバ証明書の有効期限が段階的に 47 日まで短縮されることが可決 (2025/04/13)

■ 有効期限短縮のスケジュール

SC-081: Introduce Schedule of Reducing Validity and Data Reuse Periods
https://github.com/cabforum/servercert/pull/553

	発行可能な証明書の期間
現在	最大 398 日間
2026/03/15 以降	最大 200 日間
2027/03/15 以降	最大 100 日間
2029/03/15 以降	最大 47 日間

証明書入れ替え作業
自動化が実質不可避に
(メールサーバも例外なく影響あり！)

■ この動きの目的

証明書の信頼性向上
- 再認証しない限り、証明書の信頼性は時間とともに徐々に低下していく。
- 例えば、ドメイン名はドロップキャッチされて別の組織が使うこともある。

セキュリティリスクの低減
- 秘密鍵が漏洩したり、認証局によって誤発行された証明書の悪用期間が減少。

ライフサイクル管理と品質の向上
- 期限が短くなると自動化せざるを得なくなる。
- ゆえに証明書の更新忘れを防止・オペレーションミスのリスクを低減、安定性が向上。

Let's Encrypt に移行する際の課題・検討事項整理

1. 証明書管理 自動化の動機
- 作業コストの省力化・オペミス回避
- 品質向上と運用のイノベーションを達成
- ACME でマルチベンダー対応
(あとで認証局を変更しても良い)

2. 証明書の使い分け (DV/OV/EV)
- 経路暗号化目的なら DV でも達成可
- 昨今ブラウザでも違いは見えづらい
- MTA・MSA 間通信はもっと見えない

3. 利用者への影響
- 事前に認証局変更をお知らせ
- OV → DV 変更も問題なし
- 目立った問い合わせなし、あっさり実現

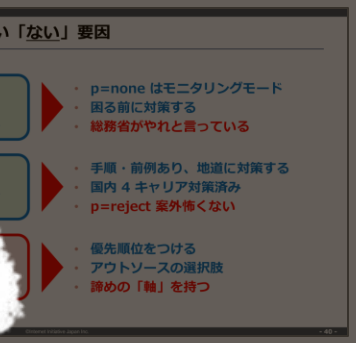
ここまでのまとめ

2025年、メールセキュリティをアップデート

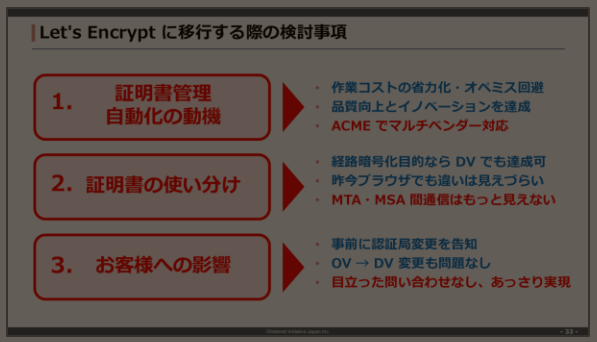
p=rei
意外に

証
今、

は p=reject へ



TLS 時代へ



ここまでのまとめ

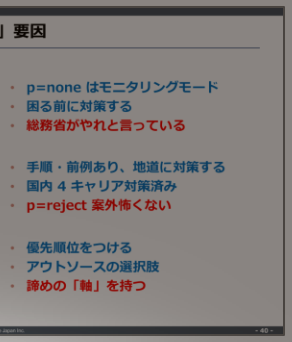
2025年、メールセキュリティをアップデート

p=rei
意外に

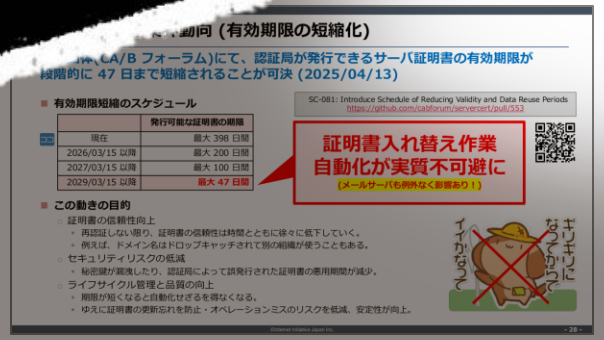
証明
今、

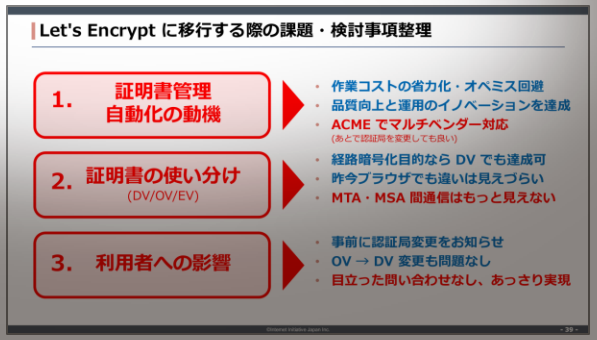
証明書と掛けまして
2025年の設備運用と ときます
そのこころは
どちらも「鍵」と「自動化」が
大切でしょう

は p=reject へ



TLS 時代、証明書自動更新が鍵



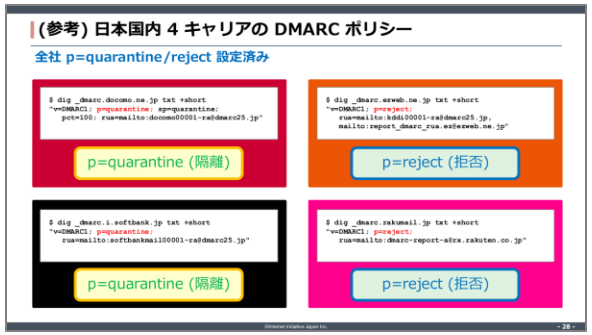


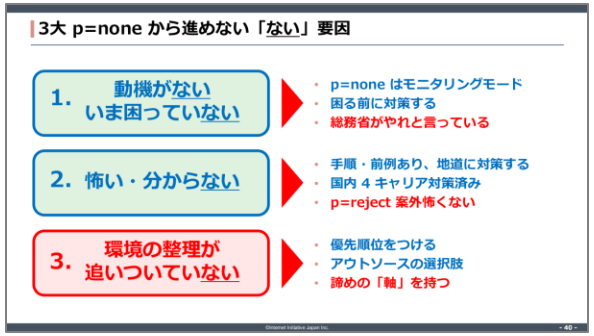
ここまでのまとめ

2025年、メールセキュリティをアップデートしましょう

p=reject
意外に怖くない

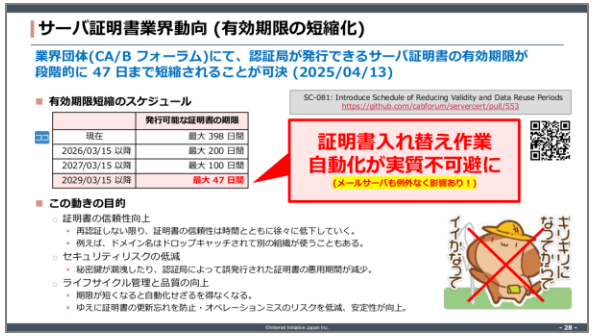
■ 大手キャリアも対応済み、世の中は p=reject へ

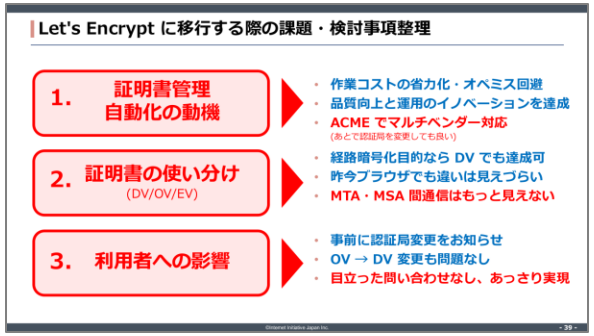




証明書期限短縮
今から備えて

■ メールも常時 TLS 時代、証明書自動更新が鍵





IIJ Internet Initiative Japan

Lead Initiative

日本のインターネットは1992年、IIJとともにはじまりました。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はいつもはじまりであり、未来です。

Ongoing Innovation