想定所要時間 25分

Internet Week ショーケース in 静岡 / C13
15:00～15:50

IIJ Internet Initiative Japan

メールセキュリティ 2026 キャッチアップ

DMARC・STARTTLS(経路暗号化)

2026/06/30(火)

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
運用技術課 課長　古賀 勇

Ongoing Innovation

自己紹介

法人系メールセキュリティサービスの運用と PKI

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

- PKI・サーバ証明書

古賀 勇 (Isamu Koga)

株式会社インターネットイニシアティブ (IIJ)
アプリケーションサービス2部 運用技術課・課長
(兼)証明書技術課・課長

「静岡県出身」

WIDE Project

M3AAWG

openSUSE (趣味)

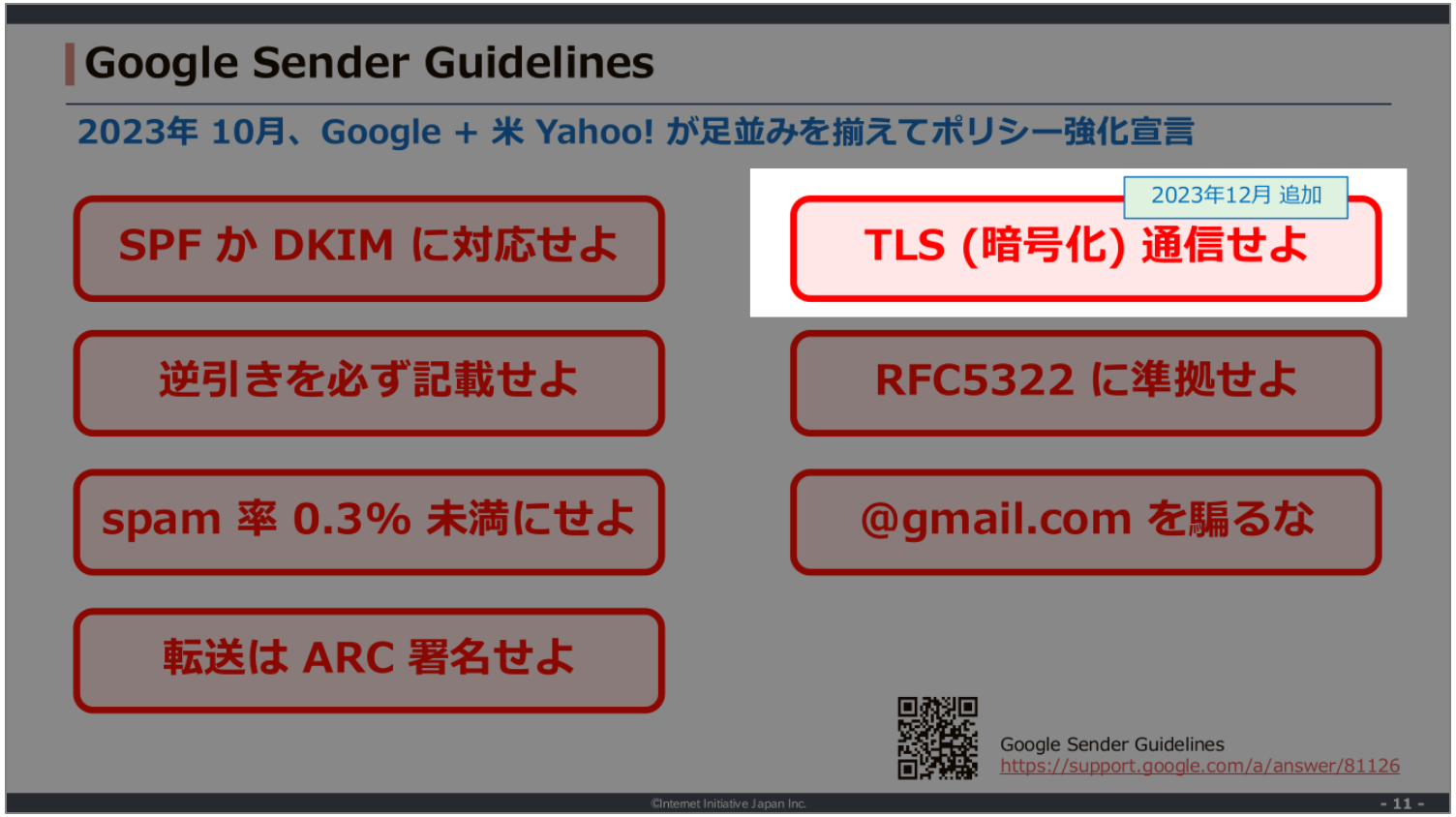
経路暗号化(STARTTLS)と証明書管理の課題

(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

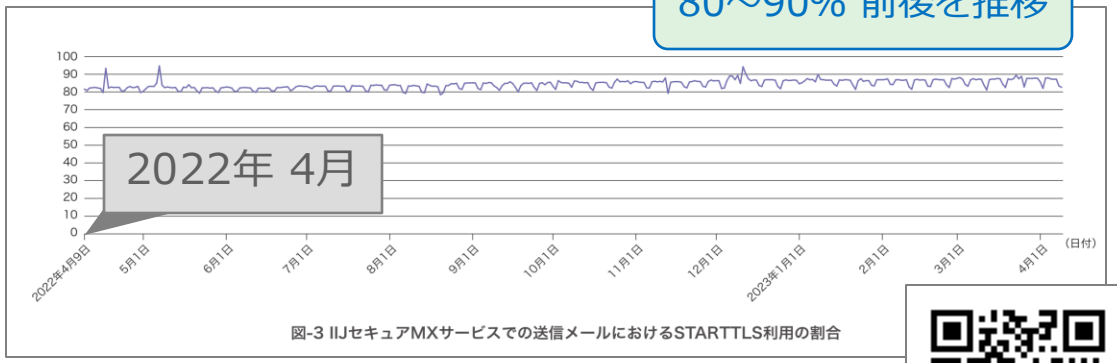


図-3 IIJセキュアMXサービスでの送信メールにおけるSTARTTLS利用の割合

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

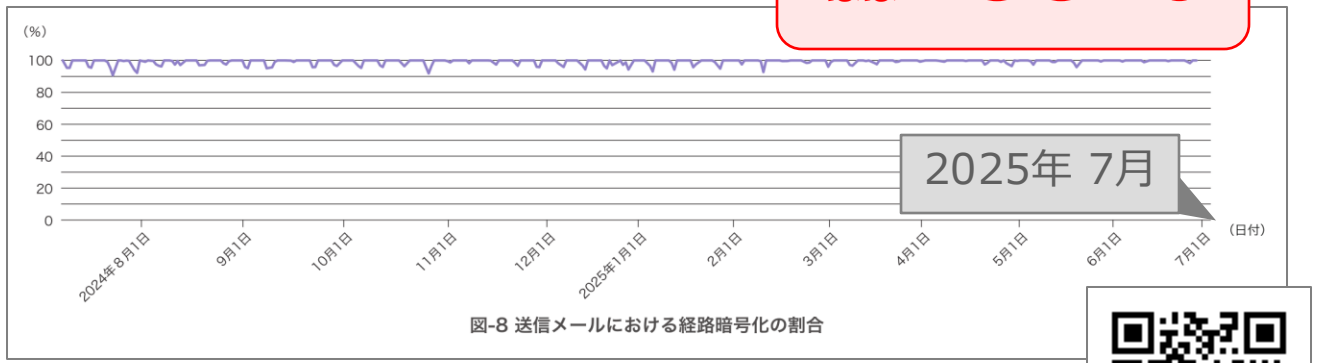
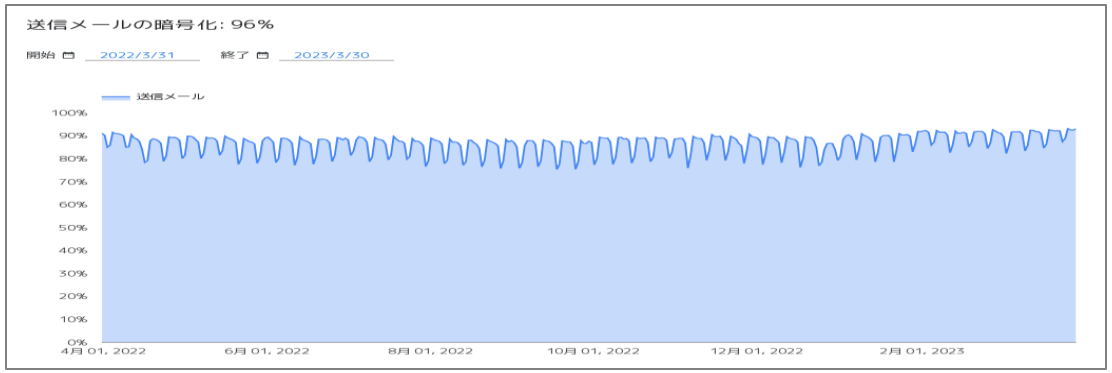


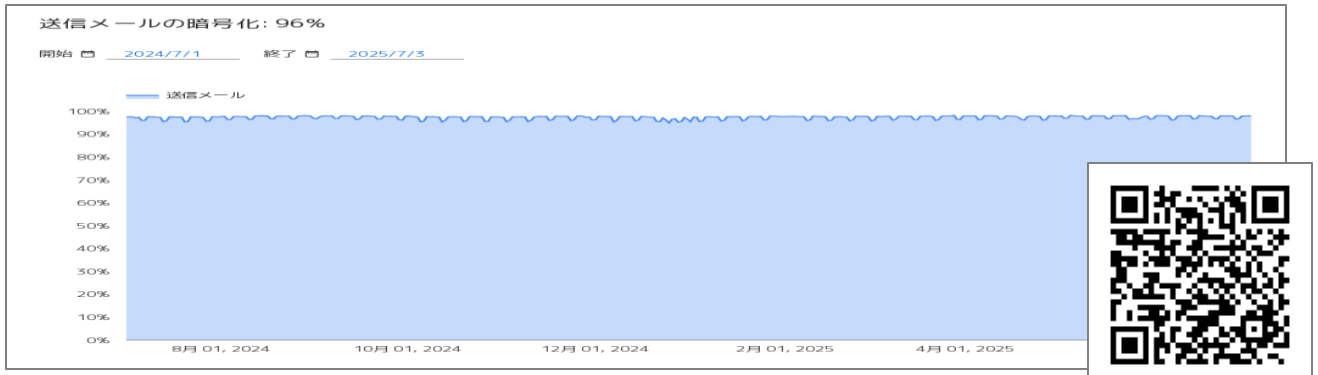
図-8 送信メールにおける経路暗号化の割合

▲ 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

図-3 IIJセキュアMXサービスでの送信メールにおけるSTART

メールにおける経路暗号化の割合

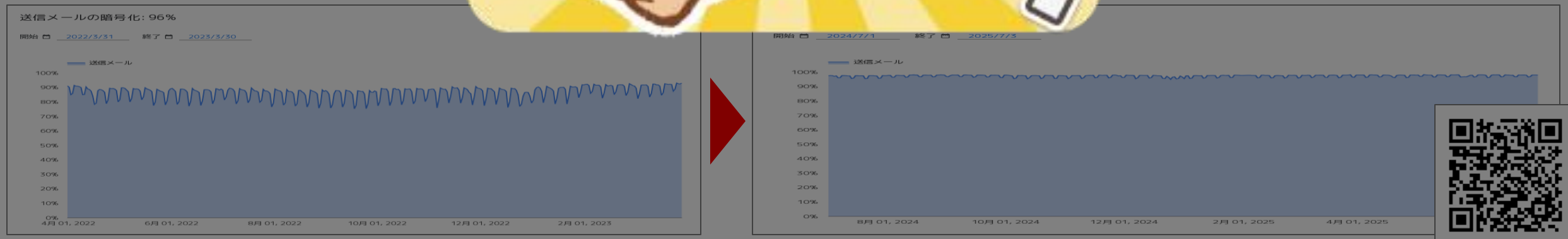
▲ Internet Infrastructure Review (IIR) Vol.59 IIR) Vol.67

https://www.iij.ad.jp/dev/report/iir/059/01.h r/067/02.html

ほぼ100%

■ 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

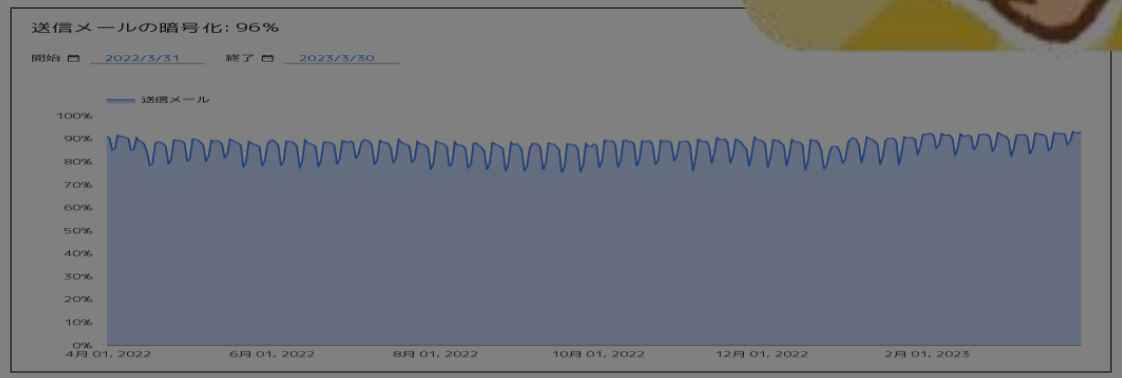
ほぼ100%

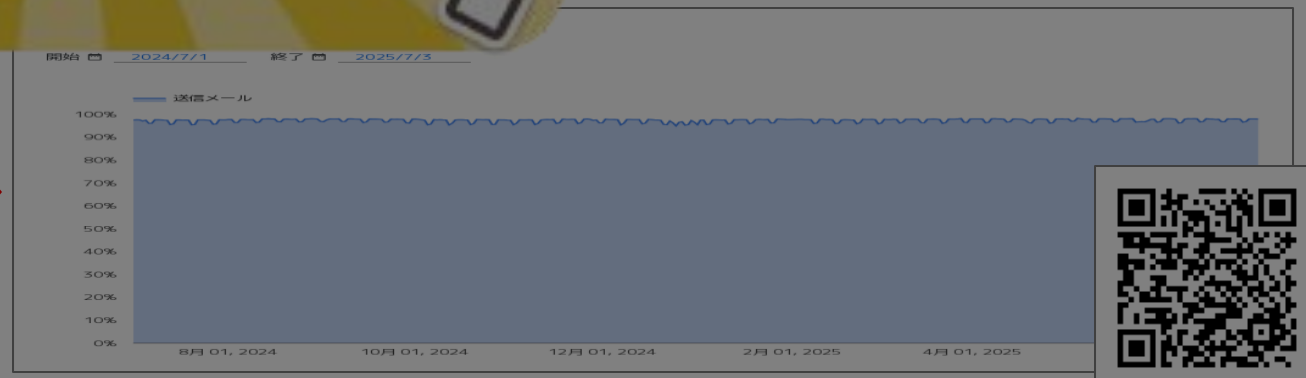
▲ Internet In
https://www.

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
2026/03/14 以前	最大 398 日間
ココ 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**

■ 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)

■ 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限
2026/03/14 以前	最大 398 日間
ココ 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]
2026/03/14 以前	最[illegible]
ココ 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[illegible]**

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

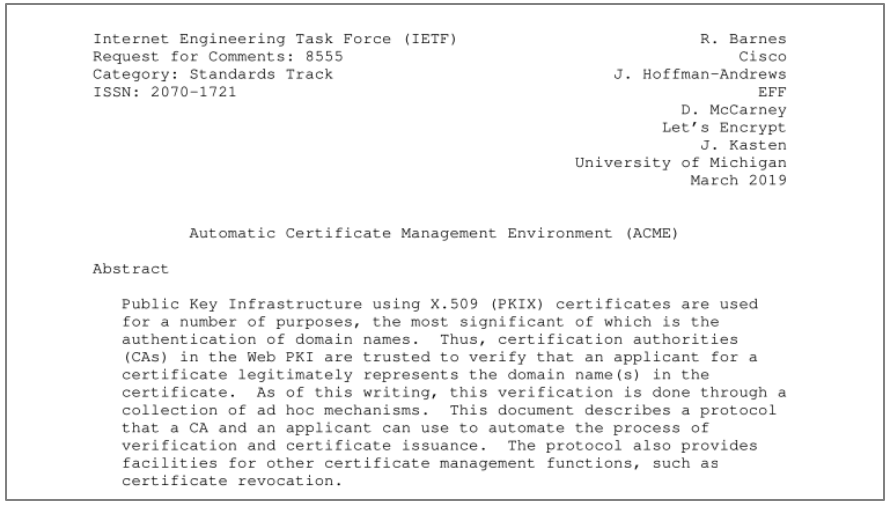
証明書更新の自動化プロトコル (ACME)

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

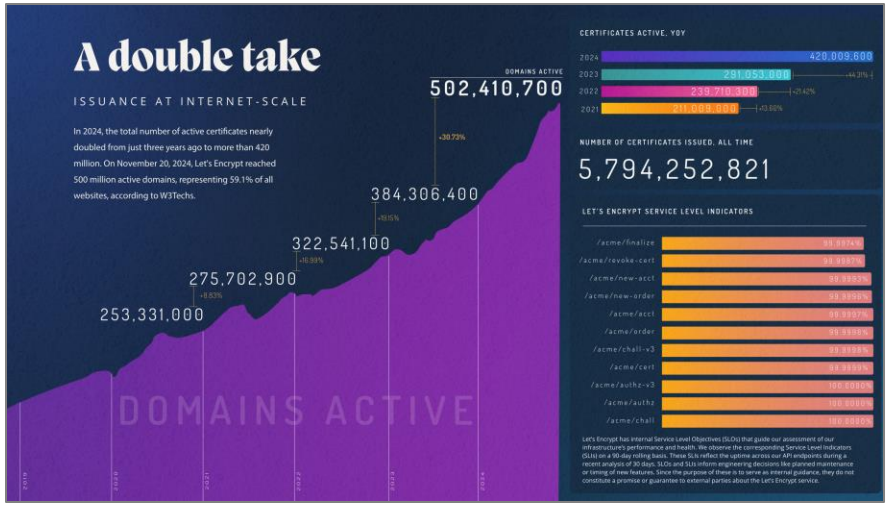
R. Barnes
Cisco
J. Hoffman-Andrews
EFF
D. McCarney
Let's Encrypt
J. Kasten
University of Michigan
March 2019

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

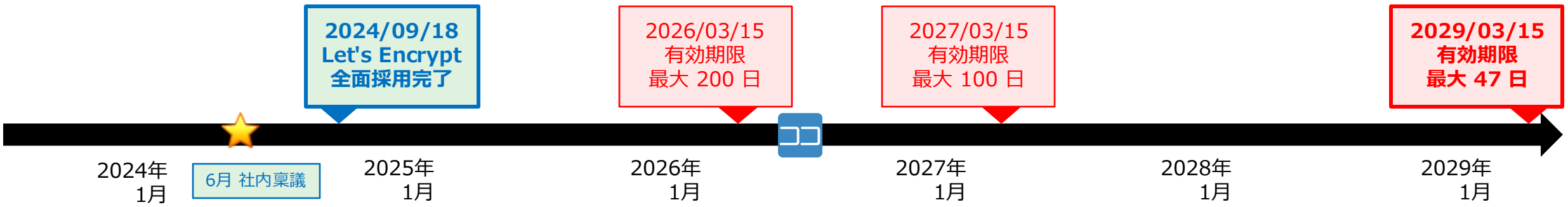
※1 “Moving Forward, Together” — Chrome Root Program Policy
https://chromium.googlesource.com/website/+/5943ad5e004c1cde2f869f1d67008a729e9ec12e/site/Home/chromium-security/root-ca-policy/moving-forward-together/index.md

■ 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 100 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**

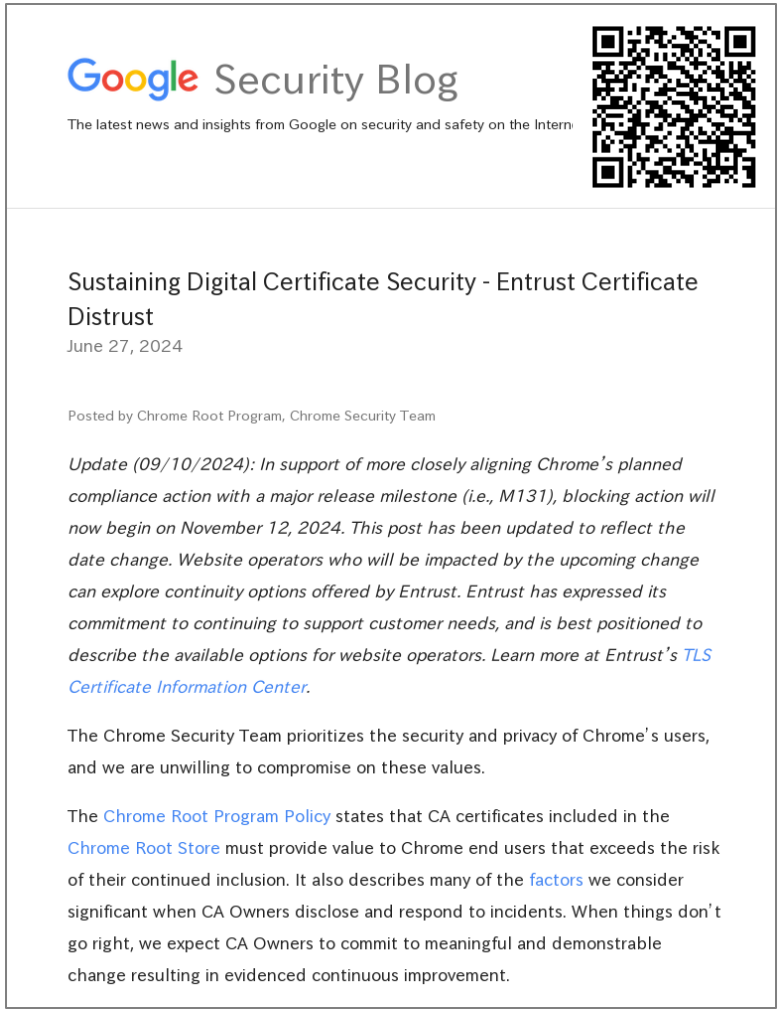
2016年	Distrusting WoSign and StartCom Certificates
2018年	Chrome's Plan to Distrust Symantec Certificates
2022年	TrustCor Certificate Distrust

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

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

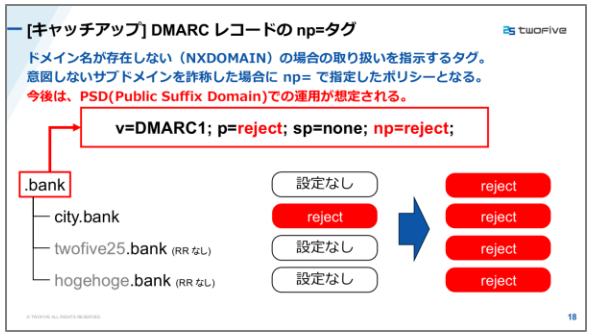
ここまでのまとめ

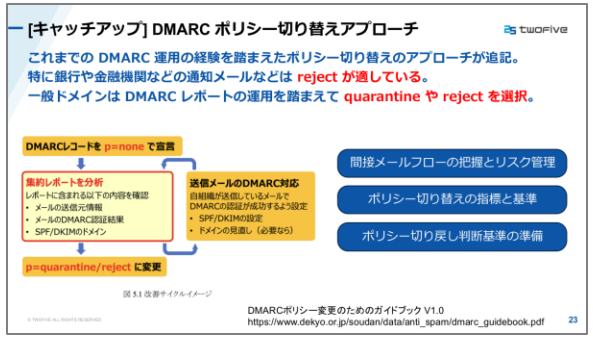
2026 年のメールセキュリティをアップデートしましょう

なりすまし対策に DMARC が必須

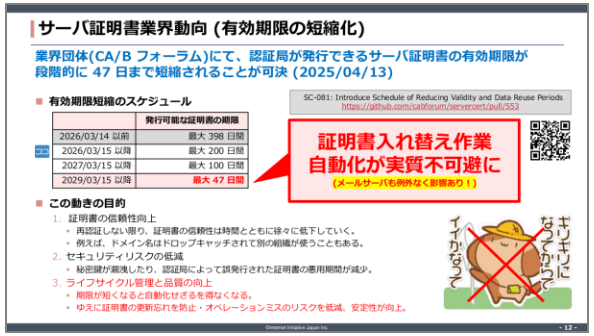
証明書期限短縮 今から備えて

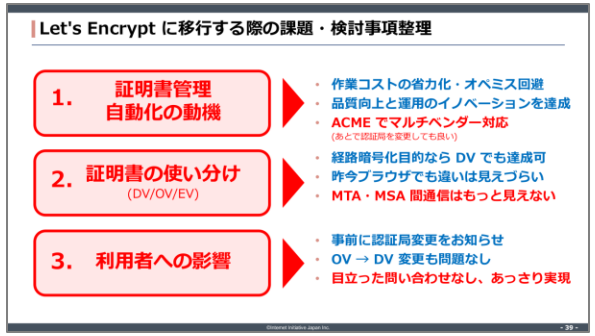
正しく設定して、しっかり守る、p=reject まで





メールも常時 TLS 時代、証明書自動更新が鍵



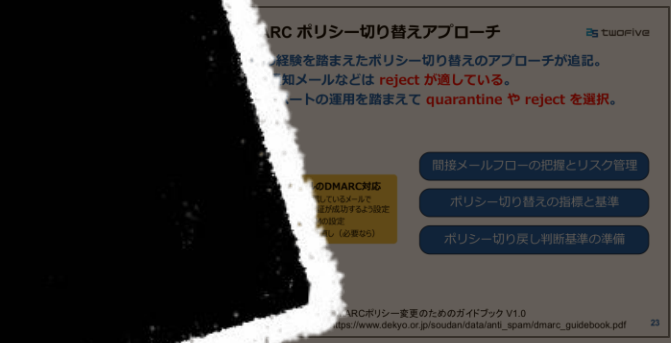


ここまでのまとめ

2026 年のメールセキュリティをアップデー

なりすまし
DMAR

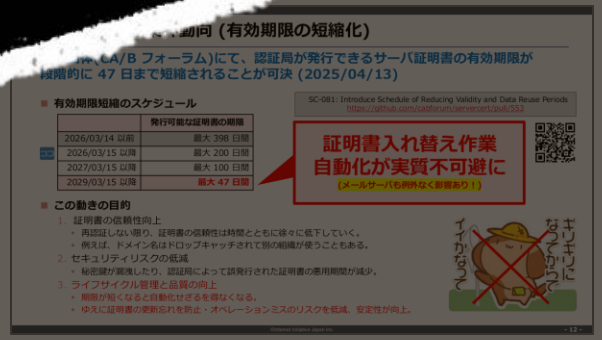
p=reject まで

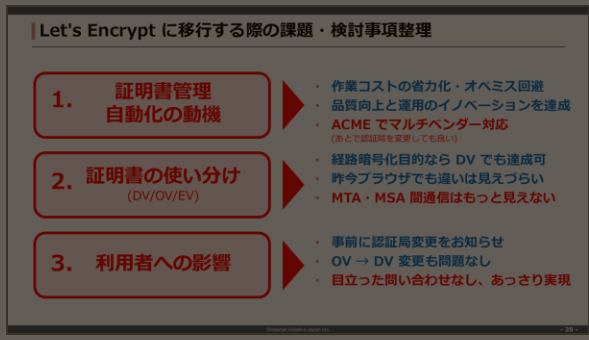


証明

今、

TLS 時代、証明書自動更新が鍵





ここまでのまとめ

2026 年のメールセキュリティをアップデー

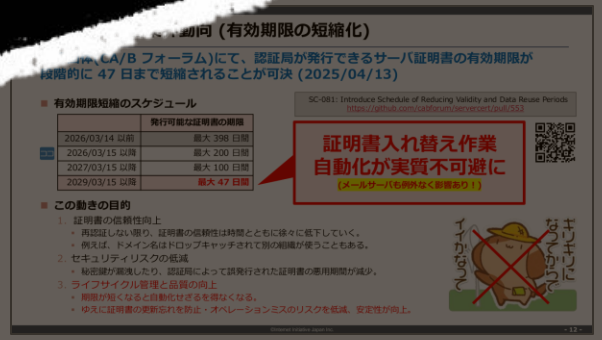
なりすまし
DMAR

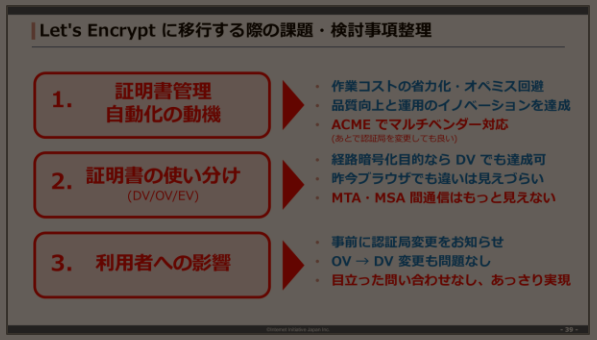
証明
今、

p=reject まで

証明書と掛けまして
2026 年の設備運用と ときます
そのこころは

TLS 時代、証明書自動更新が鍵



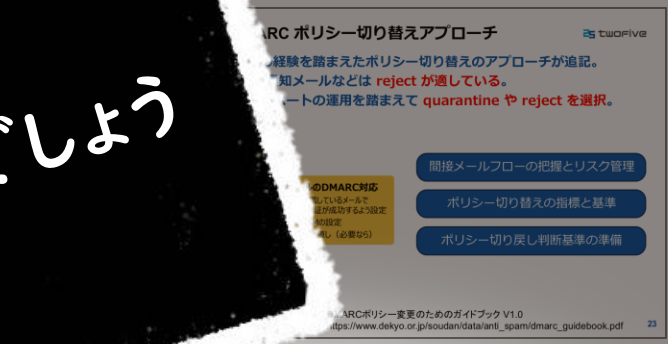


ここまでのまとめ

2026 年のメールセキュリティをアップデー

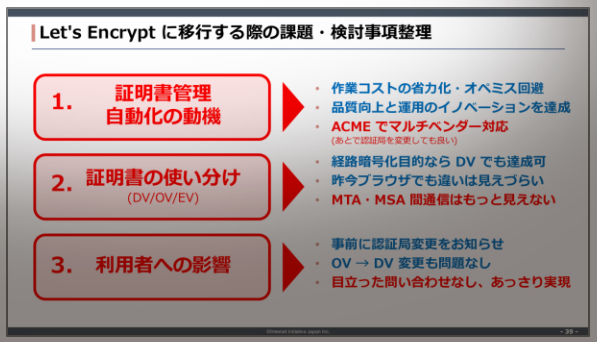
なりすまし
DMAR

p=reject まで



証明
今、

TLS 時代、証明書自動更新が鍵

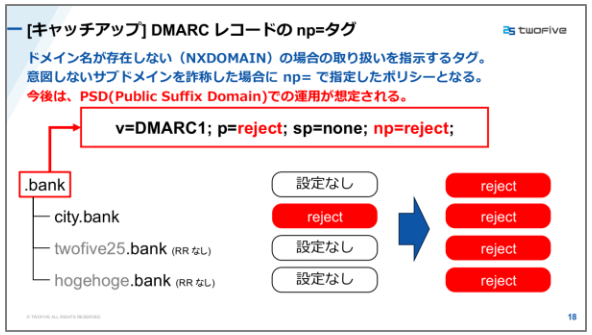


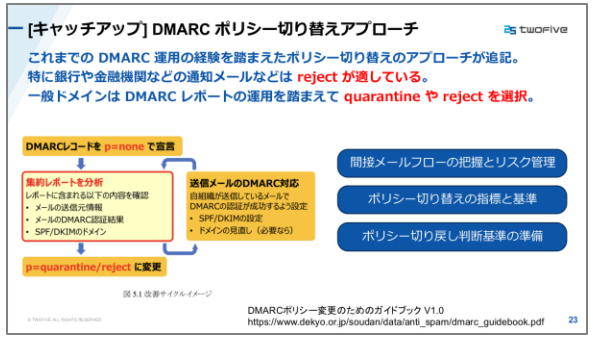
ここまでのまとめ

2026 年のメールセキュリティをアップデートしましょう

なりすまし対策に DMARC が必須

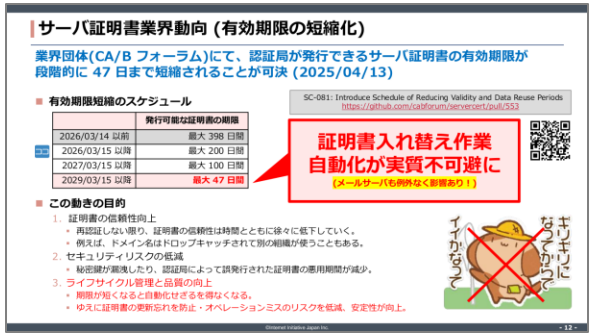
- 正しく設定して、しっかり守る、p=reject まで

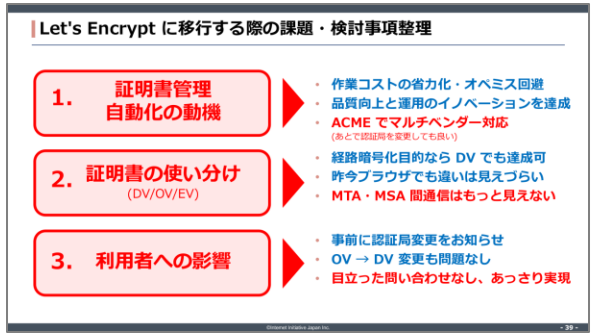




証明書期限短縮 今から備えて

- 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