WebPKIの最新動向と今後の見通し

セコム株式会社　伊藤忠彦

自己紹介

伊藤　忠彦

セコム株式会社　IS研究所　暗号・トラストグループ　上級研究員

- 主な研究分野：
  - **暗号鍵管理**全般
  - **ルート認証局**のポリシー管理・運用
  - 暗号システムの**移行**・制度設計

- 主な活動領域：標準化やルール整備
  - **IETF** (鍵管理関連規格提案：RFC 8813, RFC 9295, RFC 9336など)
  - **CA/BForum** (WebTrust向けの証明書に関するルール整備)
  - **IPA**　非常勤 研究員（暗号鍵管理のドキュメント整備）

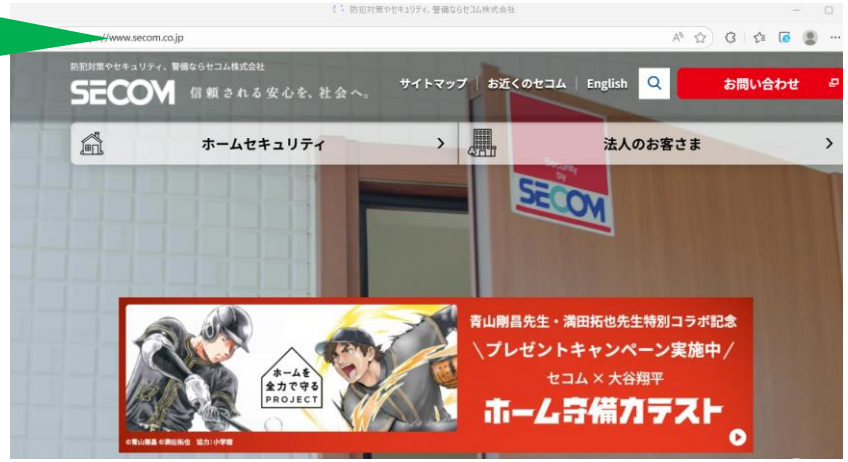
目次

- CA/BForum関連同行
- PQC移行の見通し

CA/BForumとは

CA/BROWSER FORUM

信頼できるか
判断するための
仕組み



- 認証局及びブラウザベンダの業界団体
  - Apple, Cisco, Google, Microsoft, Mozilla等のブラウザベンダ
  - 世界各国の50＋の認証局事業者

- 活動
  - TLS向け、SMIME向け、コードサイン向け等の「Public Trusted」証明書のルール/ガバナンス整備
    - 8つの隔週のミーティング
    - 毎年3回の対面会合
    - Ballot（投票）により意思決定

■2025年3月25日～27日：CA/BForum　F2F 64東京開催

■20年以上の歴史で、日本開催は2度目（前回はChromeがホスト）

CA/BForumにおける重要な変更

ドメイン確認（DCV）の手段のアップデート

- DCV関連の主なアイテム
  - MPIC（Multi-Perspective Issuance Corroboration）
  - DNSSECの扱い変更
  - 電話やメールベースのDCV段階的廃止

- 懸念：BGPハイジャッキング
- 認証局は、DCVにおいて、複数の観測地点から名前解決をする。
- 既に導入済み、観測地点数が徐々に増えていきます。
  - 最低2か所（2024年9月15日） ⇒ 最低5か所（2026年12月15日）

DNSSECの扱い変更

- 今まで:
  - DNSSEC（が設定してあり、そ）の設定が失敗していた場合も、CAは証明書を発行できた（発行するかはCAのポリシ依存）。
- 2026年3月～
  - 適切にDNSSECが設定されていないと、証明書を発行できなくなります。
- ポイント
  - DNSSECの設定がちゃんとされているか、確認をお願いいたします。

電話やメールベースでのDCV段階的廃止

- **2025年7月15日～**
  - Whois に記載されたメールアドレス等を用いたDCV禁止
- **フェーズアウト提案（SC090）**
  - 2026年3月15日：
    - “IP Address”(3.2.2.4.8)廃止、emailや電話番号に依存する方法を非推奨
  - 2027年3月15日
    - Phone Contact with DNS TXT Record Phone Contact (3.2.2.4.16)廃止
    - Phone Contact with DNS CAA Phone Contact (3.2.2.4.17)廃止
    - Email, Fax, SMS, or Postal Mail to IP Address Contact (3.2.2.5.2)廃止
    - Phone Contact with IP Address Contact (3.2.2.5.5)廃止
  - 2028年3月15日：
    - Constructed Email to Domain Contact (3.2.2.4.4)廃止
    - Email to DNS CAA Contact (3.2.2.4.13)廃止
    - Email to DNS TXT Contact (3.2.2.4.14)廃止

- ポイント：証明書更新の自動化をご検討ください。

証明書の有効期間短縮

	証明書有効期間	DCV再利用可能期間
現在	398日	398日
2026年3月15日	200日	200日
2027年3月15日	100日	100日
2029年3月15日	47日	10日

■ポイント

- ■証明書の更新間隔が1年に1回　⇒　1か月に1回
- ■（実質的に）証明書更新の自動化が必須となります

- 自動化が実質的に必須となります。

- どうしても自動化が無理なケースがありましたら、教えてください。

TLS証明書からClientAuth除外（Chromeのポリシー）

- 今まで
  - サーバ認証用の証明書（Key UsageにServerAuthが設定された証明書）にClientAuthも設定できた。

- 新規Root以下は2025年6月以降、既存ルートも2026年6月以降
  - TLS用証明書に、ClientAuthの設定することを禁止（Chromeのポリシー）

- 対策
  - ClientAuthが必要な用途は、「Public Trusted」でないCA（プライベートCA等）を利用する。
  - どうしても無理なケースがあればご相談ください。

失効検証関係

- OCSP
  - プライバシ上の懸念あり
  - 2023年よりBRではOptional（2024年より全てのRoot ProgramでOptional）
  - 一部事業者はOCSPサービスの提供を停止(CRLは提供)
- CRL
  - 「サービスが落ちて使えない」ということが発生しにくい
  - 大量失効時に通信量が大幅に増加
- 対策技術：
  - Partitioned CRL (CRLを分割する方法、X.509)
  - OneCRL（CA証明書, firefox）
  - CRLite (EE証明書, firefox)
  - CRLset （EE証明書とCA証明書向, Chrome）

大量失効

- 大量失効に備える体制を構築中しております。
  - CAは大量失効の訓練も行います。

- ポイント
  - サブスクライバの証明書が、訓練でいきなり失効することないはずです。
  - インシデント等が発生した場合に、大量失効が発生する可能性についてはご留意ください。

CA階層を単用途に

- 方針
  - 用途毎（サーバ認証、SMIME、コードサイン等）にPKI階層を（ルートから）分離する
  - 各ルート証明書は、単用途のものとなる

- 理由
  - クロスプロトコルアタック対策

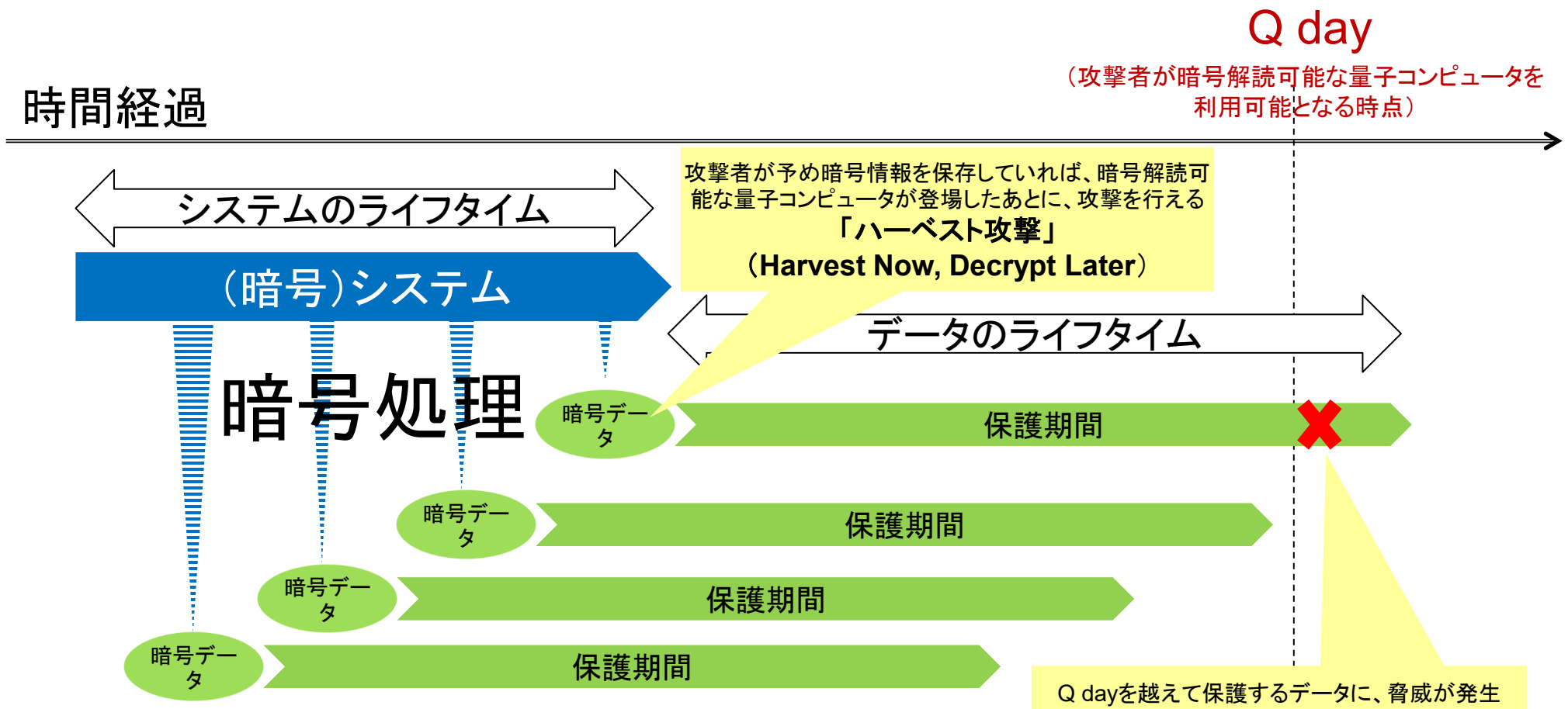
  - 単一のPKI階層が、異なるポリシーをサポートすると、「悪いとこどり」になりうる。
    - e.g.)TLS用の証明書とCodeSign用の証明書は、発行枚数も利用期間も大きく異なる。
      異なるPKI階層を持たせた方が、ポリシ管理を効果的にできる。
    - クロスサイン等の扱いが難しくなる

目次

- CA/BForum関連同行
- PQC移行の見通し（私見）

- PQC対応の状況
  - 通信暗号化に関するもの
  - TLSにおける認証に関するもの

暗号化に対する脅威の概観：長期間ライフサイクルにおける脅威



保護期間が長いデータは、既に「手遅れ」かもしれない

デジタル署名に関する脅威

■例えば、PKIのルート証明書のように、単一の鍵ペアが広く・長く利用されるケースが存在

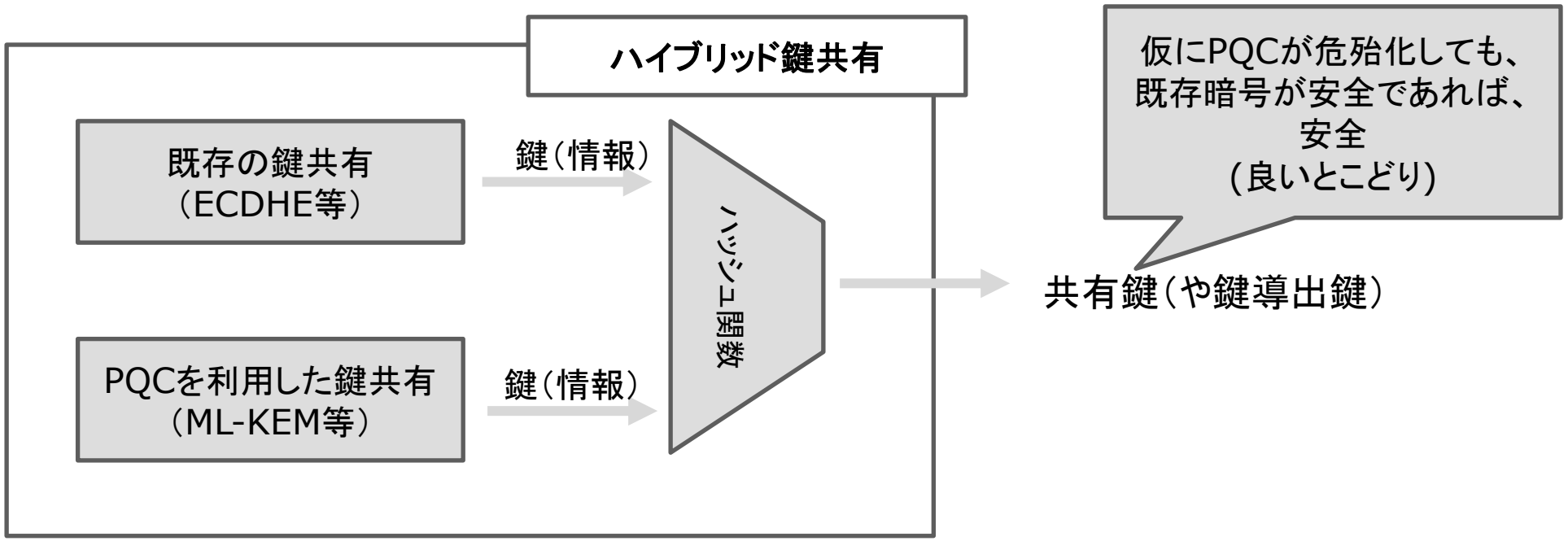
– 「広く・長く使われる」証明書は、切り替えにより時間がかかる
　ハードコードされている場合は、切り替不可能な場合もある
　古いコードサイン用途などが該当

⇒　Q day までに入れ替えが間に合わないと、攻撃されるかもしれない
（プライベート鍵が漏洩するかもしれない）

⇒ 「広く・長く使われる」証明書のプライベート鍵が漏洩すると、影響も大きい

※一方で、デジタル署名に対するハーベスト攻撃は気にしなくて良い
（ハーベスト攻撃が成立しない or 類似攻撃が成立するとしても他の手段で防御可能）

暗号化通信への量子耐性付与



Chromeブラウザ等、TLS1.3では、既に利用可能
オンラインアップデートが可能な用途では、着実に普及が進んでいる

余談：Chromeブラウザのアジリティ
（ソフトウェアだからできるという面もあるが、それにしても早い）

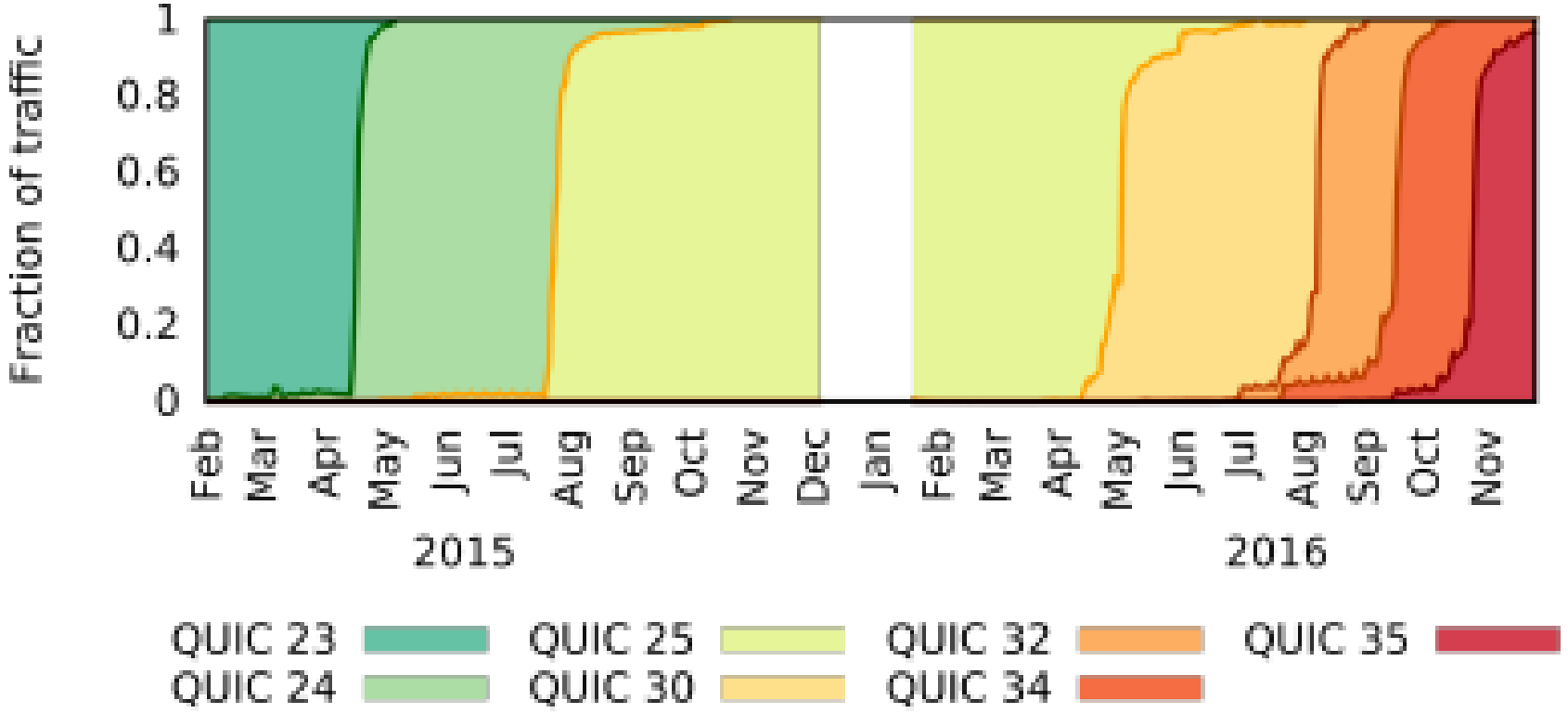


Figure 14: Incoming QUIC requests to our servers, by QUIC version.

The QUIC Transport Protocol: Design and Internet-Scale Deployment (2017)

（Webでのサーバ）認証における現状と課題

PQC移行前のCT対応

- 背景：
  - CT Logは WebPKIのガバナンスに多大な貢献をしているが…
    - 最近、CTログに負荷が掛かっている
      - 平均して、毎秒200枚超※1の登録（10TB/半年※2）、
        世界各地からの参照（約10TB/日※2）
    - PQCを利用すると、CTログのサイズがさらに大きくなる
    - CTログの最適化が急務であり、PQC移行はその後の方が効率が良さそう
      - 具体策としては、Static CT（試験運用中、未標準化）や
        Photosynthesis（標準化中）

上記のようなアプローチが採択可能なのは、
Web PKIが相当の「クリプトアジリティ」を既に確保しているため

- 10年以下でのTLS向けルート認証局入れ替え
- EE証明書の有効期間短縮（2029年に47日）

※1 https://radar.cloudflare.com/certificate-transparency
※2 https://datatracker.ietf.org/meeting/124/materials/slides-124-plants-certificate-transparency-today-00

最後に：PQC移行を行う上での考慮点

- 何もしないと、機会損失が発生することは意識した方が良い

- 暗号化については、「手遅れ」にならないことを意識
  - ハーベスト攻撃が脅威である場合は、対応を急いだほうが良い

- PKIのルート証明書等、ライフサイクルが長く、影響が広いものは注意が必要
  - スムーズな暗号移行ができる体制を整えることが重要（≒クリプトアジリティの確保）
    - 体制が整う前に暗号移行を行うと、移行が長期化しうる
    - 長期化した移行の途上で、さらに別の暗号への移行が要求する可能性に配慮

- 攻撃の蓋然性が低いシステムは優先度を下げても良いかもしれない
  - 攻撃の旨味が少ない・システムの利用期間が短い・データの価値が低い等
  - 暗号システムは広く普及しており、全てを対応するのは非効率かもしれない