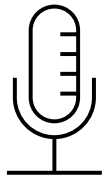
Internet Week 2023

PKIのこのごろ

2023.11.21



@Eurekaberry
(Microsoft Corp.)

@hitok_
(Trend Micro Inc.(米国))

ゆりかとひとけーの二人で、Public Key Infrastructure(PKI)について、やわらかい話題からかたい話題まで雑談を交えながら紹介するポッドキャスト「ひとくちPKI」を配信しています。

このポッドキャストは二人とも個人の取り組みとして実施しているものですが、今日の講演では自分の所属の成果物を引用する都合上、所属を名乗っています。

本講演の内容は個人の意見であり、所属を代表する意見ではありません。

情報の取扱い

- すでに公開されている情報をベースに、一般的な内容をまとめています
- SNS 投稿 OK !

WebPKI の動向

①

信頼できるCA、信頼できる証明書の維持に対する取り組み

WebPKI における信頼できるルートCAの取り扱い

各ルートプログラムに含まれているCAのリストは、それぞれのベンダーが管理し、異なるポリシーで運用されている

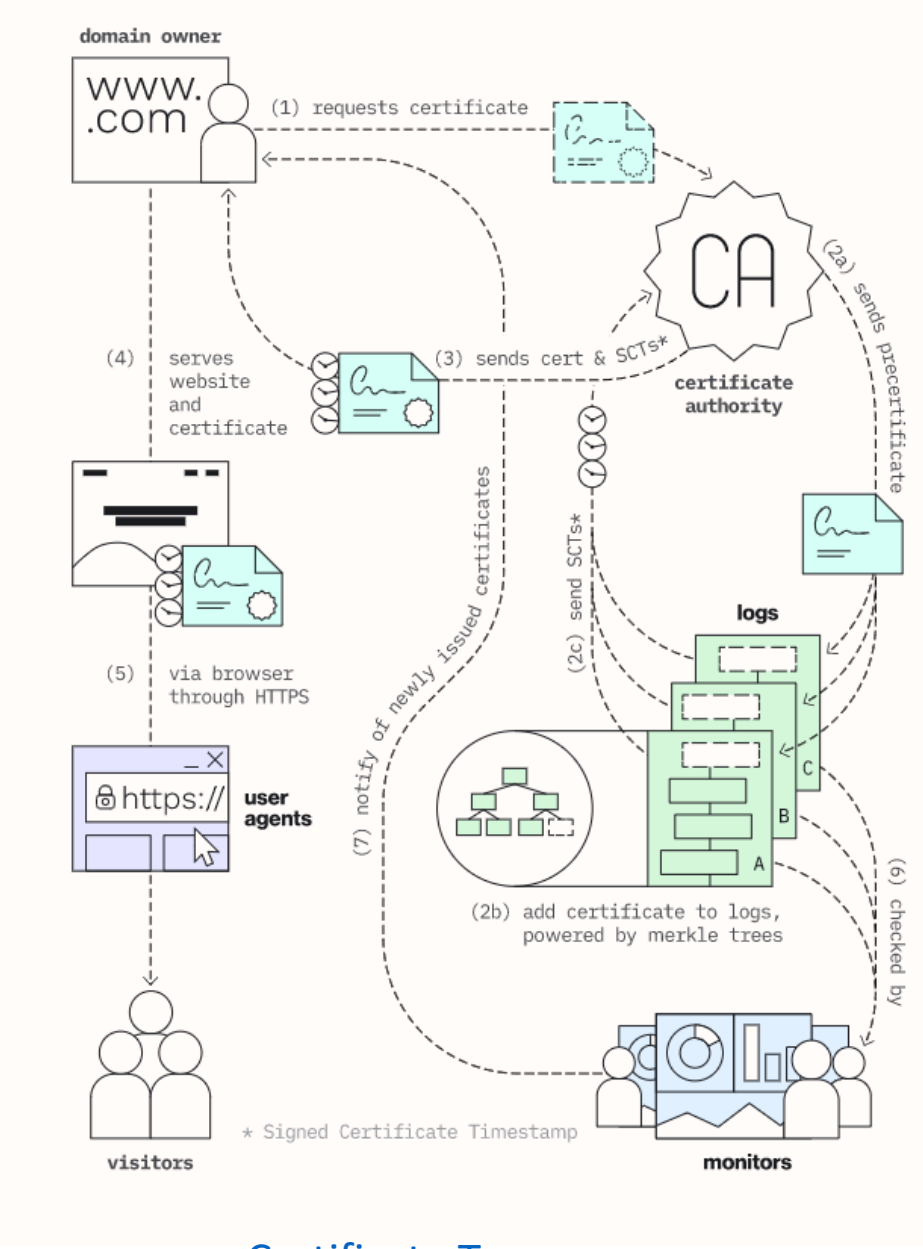
- 問題が発生したCAの信頼をとりやめる指針や時期が異なる
- ルートプログラムのポリシーがデファクトスタンダードに
  - Google 90日の有効期限化を提案*
  - 独占的であるとの議論も**

ベンダー	ルートストアが利用されるシナリオ	参照リソース
Apple	MacOS, iOSでの証明書検証	Root Certificate Program - Apple
Mozilla	Firefox 、 Network Security Services (NSS) での証明書検証	Mozilla Root Store Policy — Mozilla
Google	Windows, ChromeOS, Linux, macOS 上のChromeでの証明書検証 (* 順次切り替え中) [Google, 2022]	Chrome Root Program Policy, Version 1.2 (chromium.org)
Microsoft	Windows 上での証明書検証が実施された場合	プログラムの要件 - Microsoft の信頼されたルート証明書プログラム | Microsoft Docs

* Moving Forward, Together
** https://www.european-signature-dialog.eu/Google_returns_to_anti-competitive_behavior-ESD_26042023.pdf

インシデント防止のための Certificate Transparency が存在感を増している

- CTはCA によって発行された証明書のログ
- 発行ログを確認することで不適切な証明書の発行を監視する
- ブラウザで、CT(Certificate Transparency)対応が必須化
  - Chrome: 2018.4以降発行の全ての証明書
  - Safari 2018.10以降発行の全ての証明書



Certificate Transparency.org

Certificate Transparency の効果

- 不適切な証明書のエコシステムでの監視が役立った事例が出始めている
  - Let’s Encrypt から不適切な証明書が発行されていることが発見される (2023.6) [1]
  - Certificate Transparencyのデータを使って大量の証明書からRSA鍵を取り出して調べたら因数が重複しているものが見つかった[2]
- 自組織を騙る不正な証明書が発行されていないかの活用も

- 一方で、課題も
  - 少数のログプロバイダにCTエコシステムが依存
  - CT に問題があると WebPKI のクリティカル問題に
    - Google の CTログサーバーの撤去が、CTエラー (2022.5) [3]
    - CTv3 移行でエラーが多発 (2023.2) [4]
    - CTログのビット反転問題 (2023.5) [5]
  - PQCの鍵の場合はログが肥大化が予想される

1. https://www.agwa.name/blog/post/last_weeks_lets_encrypt_downtime
2. https://bora.uib.no/bora-xmlui/bitstream/handle/11250/3001128/Masters_thesis__for_University_of_Bergen.pdf
3. https://bora.uib.no/bora-xmlui/bitstream/handle/11250/3001128/Masters_thesis__for_University_of_Bergen.pdf
4. https://groups.google.com/a/chromium.org/g/ct-policy/c/P3_hj9QmsLc/m/S9xohdAHAQAJ?pli=1
5. https://www.theregister.com/2023/02/16/google_delays_certificate_transparency_log/
6. https://groups.google.com/a/chromium.org/g/ct-policy/c/R27Zy9U5NjM?fbclid=IwAR38qhmIaFWyROlCTP6RxG3CBfWxDYu8UAJ7h8MfpieuXEvKLLtOXT1tmac&pli=1

eIDAS 2.0 がもたらすリスクの議論

- eIDAS: EU 加盟国の電子商取引のための、電子識別およびトラストサービスの枠組みを確立するための EU 規制 No 910/2014 の通称
- 次期バージョンとなるeIDAS 2.0 最初のドラフトは 2018 年に作成され、それ以降議論が続けられており、2021年6月に最終ドラフトが欧州議会に立法提案
- eIDAS 2.0 Web サイト認証用の認定証明書(QWACs) の要件の条項　Article 45 に対して、WebPKI を担う組織や専門家から、懸念が表明されている
  - QWACはブラウザーによって認識されるものとし、これらの目的のために、Web ブラウザーは、いずれかの方法を使用して提供された ID データがユーザーフレンドリーな方法で表示されることを保証するものとする、
- QWACが認識されて表示されるためには、そのQWACのルートCA証明書は、ブラウザ（又はOS）で、信頼できるCAとして認識される必要があります。すなわち、いずれかのEU加盟国によってトラストリストに掲載されたQTSPのルートCA証明書を、ブラウザーは信頼できるCAとして受け入れる必要があります。
- QWACが満たす必要のある要件は、European Standards Organization: European Telecommunications Standards Institute (ETSI) によるもののみ
  - Certificate Transparency (CT) への対応は、ETSIでは求められていません
- ブラウザーが維持しているルートCAプログラムの基準を満たさない信頼度の低いCAが信頼されるCAとして登録される可能性が生じるとして懸念が表明されている

参照
Mozilla: Last Chance to fix eIDAS: Secret EU law threatens Internet security https://last-chance-for-eidas.org/
Security Risk Ahead https://securityriskahead.eu/

WebPKIの動向

②

ウェブサイトの安全性に関する表示の変化

WebPKIの動向②
ウェブサイトの安全性に関する表示の変化

「信頼できるサイト」に表示を

- EV 証明書の “緑のアドレスバー”

- TLS 証明書の鍵アイコン

EV 表示はユーザーに心理的影響やセキュリティ行動に寄与しない という議論

- “Stripe社” 同一の組織名によるフィッシングサイト立ち上げの実証
- Google 社のEV表示のフィールド実験*

HTTPS 対応サイトは増加

Let’s Encrypt : Internet Security Research Groupが2015年10月に開始した 証明書無償発行サービス

HTTPS 対応サイトは増加

80% はHTTPS (5年前は 50%) *

*The Web's Identity Crisis: Understanding the Effectiveness of Website Identity Indicators | USENIX

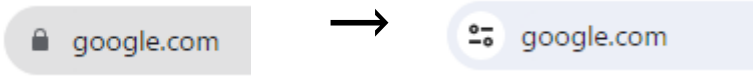
WebPKIの動向②
ウェブサイトの安全性に関する表示の変化

「信頼できるサイト」に表示を

- EV 証明書の “緑のアドレスバー”
- TLS 証明書の鍵アイコン

「信頼のできないサイト」に警告を

- HTTPS ではないサイトの場合は警告表示
- ブラウザでのHTTPS ONLY を開始
  - Chrome 94, Edge 92, Safari 15
- 鍵アイコンの廃止(Chrome)



- HTTP→ HTTPS自動リダイレクト(Chrome)

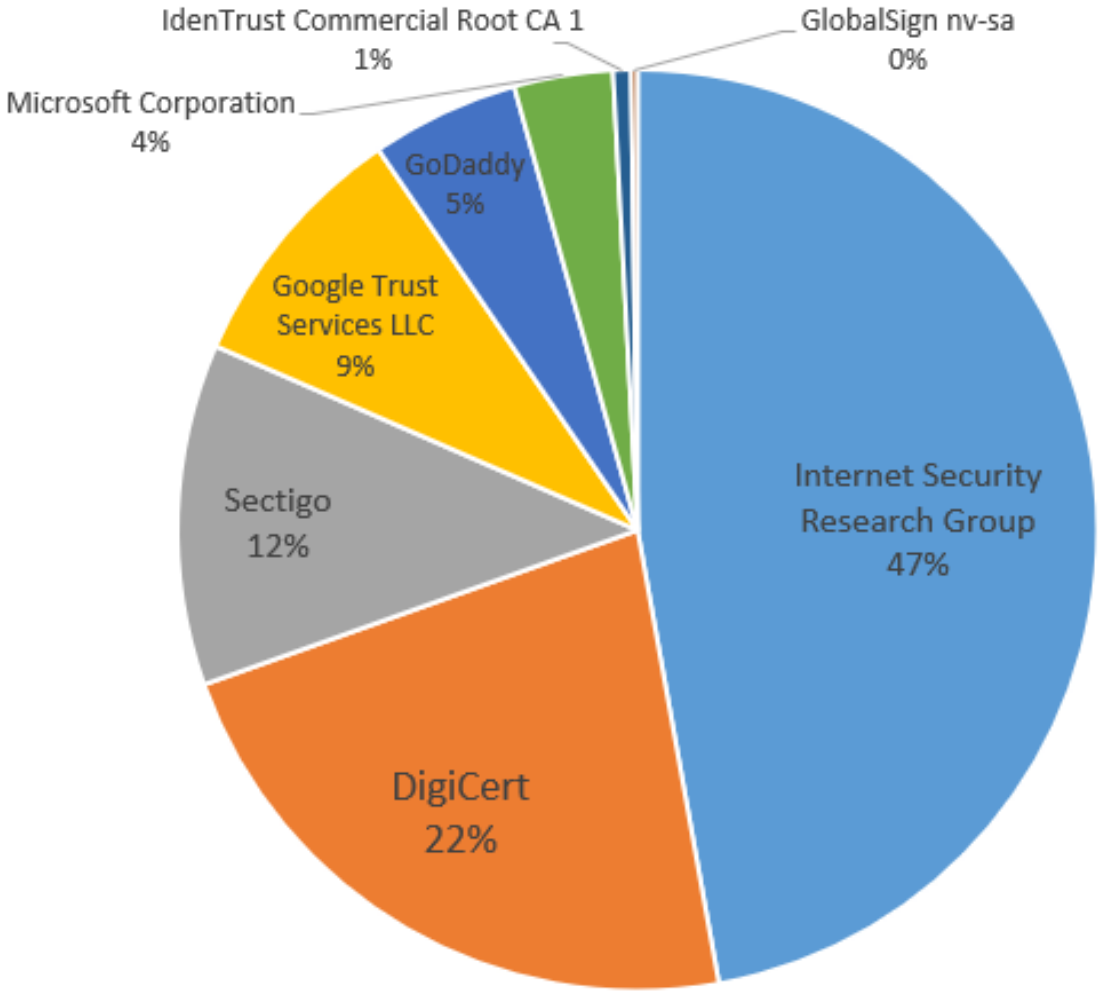
The Web's Identity Crisis: Understanding the Effectiveness of Website Identity Indicators | USENIX

WebPKIの動向

③

WebPKI のキープレーヤーの変化

TLS 証明書のシェア



- Let's Encrypt の占める割合は増加傾向
- 7 つのCAが99%を占める
- クラウドサービスが運営するCA の存在感の高まり
- Contents Delivery Network (CDN) の PKI への取り組み
  - Cloudflare
    - HeartbleedRevisited https://blog.cloudflare.com/heartbleed-revisited/
    - High-reliability OCSP stapling and why it matters https://blog.cloudflare.com/high-reliability-ocsp-stapling/
    - Introducing: Backup Certificates https://blog.cloudflare.com/introducing-backup-certificates/
    - Out now! Auto-renew TLS certificates with DCV Delegation https://blog.cloudflare.com/introducing-dcv-delegation/

参照: Cert.sh (https://crt.sh/cert-populations) から取得したデータを筆者がグラフ化
(データ取得日 2023 年 11　月 3 日、現在有効期間内のPre証明書の発行数)

まとめ

- PKI技術からもたらされる認証や署名・暗号化は強固なものであるが、適切な利用にはサイバー攻撃・運用ミス・脆弱性・計算能力の向上などにより、その時点でどの要素がどこまで危殆化しているかについて継続した観察と対応のループが必要。
- PKIは基盤として様々なテクノロジーで活用されている。専門家だけではなく、幅広く議論されることが望ましい。

@Eurekaberry

@hitok_

https://anchor.fm/hitokuchipki

THANK YOU