サーバ証明書を取得する話

DNS屋さんの観点から

山口崇徳@IIJ

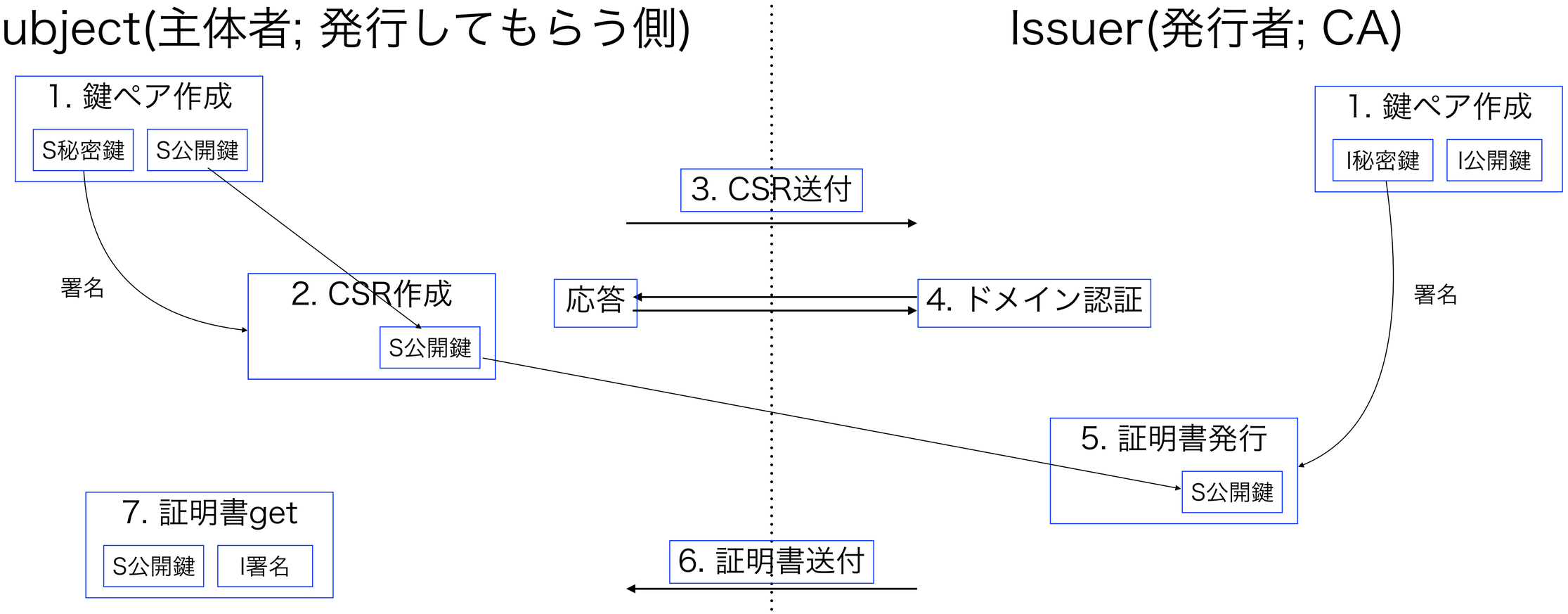
2022/06/24 DNS Summer Day 2022

はじめに

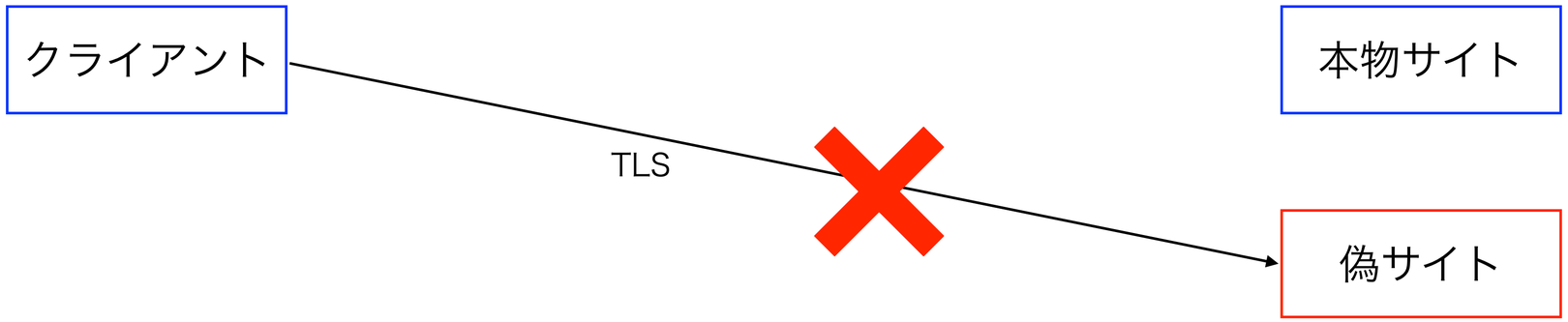
- HTTPSはもはや常識
- DNSにもDoH/DoTがやってきた

- ということで、DNS屋さんの視点でTLS、というかPKIとくに証明書の発行プロセスについて考えるよ
- 念のため、PKIは門外漢です

復習: 証明書取得の手順

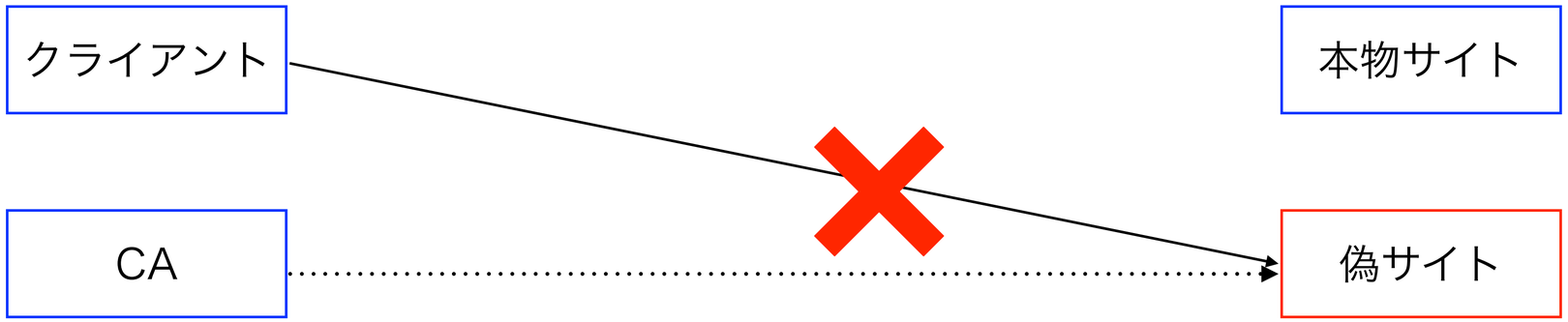

Subject(主体者; 発行してもらう側)
Issuer(発行者; CA)
1. 鍵ペア作成
S秘密鍵
S公開鍵
署名
2. CSR作成
S公開鍵
3. CSR送付
応答
4. ドメイン認証
1. 鍵ペア作成
I秘密鍵
I公開鍵
署名
5. 証明書発行
S公開鍵
6. 証明書送付
7. 証明書get
S公開鍵
I署名

TLSの理想



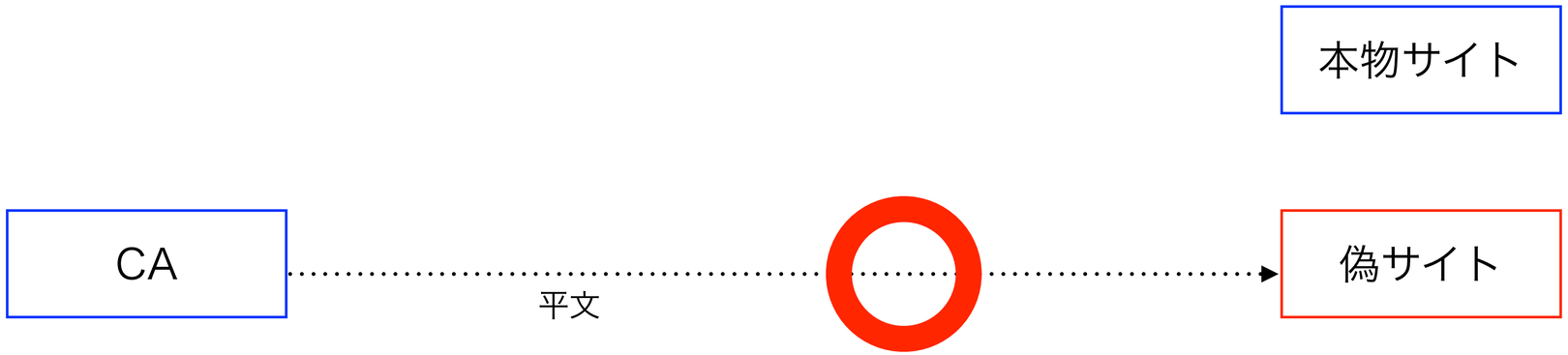
- なりすました偽サイトが出現しても、TLSがあればそれを検知できる
  - ブラウザが警告してくれる
  - TLSで検知できるからDNSSECなんかなくても大丈夫

CAを騙す



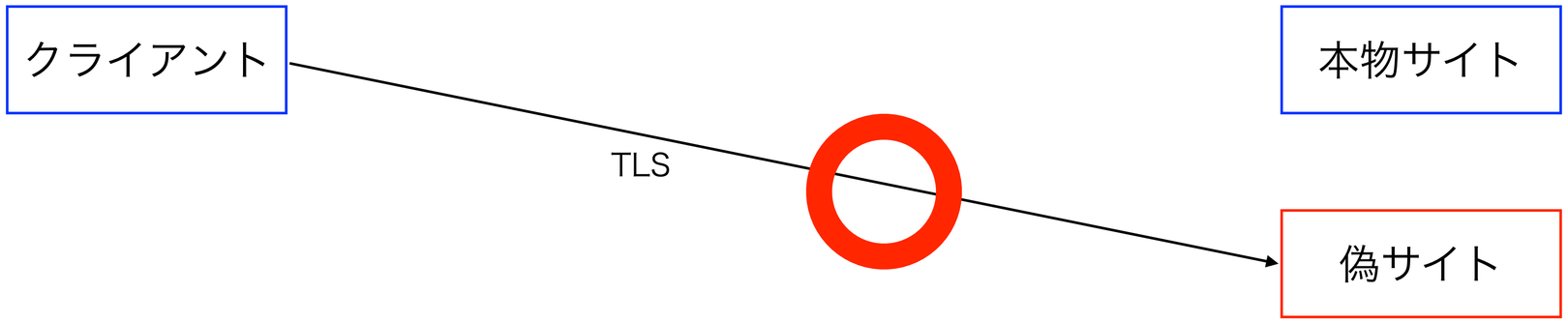
- (TLSで検知できるとはいえ)クライアントからのアクセスを偽サイトにねじ曲げることができる攻撃者であれば、CAからのアクセスもねじ曲げることができる可能性が高い
  - CAが検知できるのであれば何の問題もない

CAは騙される



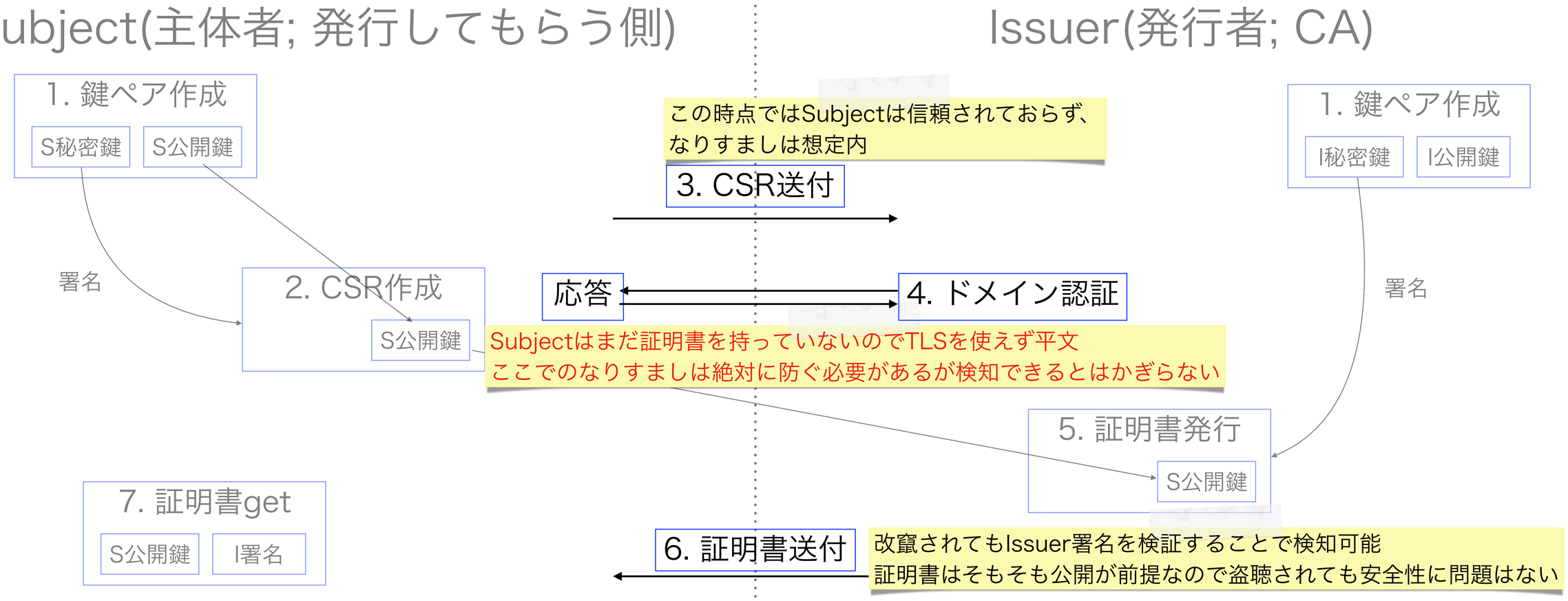
- 証明書発行プロセスにおいて、CAからのアクセスはTLSで保護されない
  - つまり、CAはなりすましを見破れるとはかぎらない
  - 攻撃者は正当な証明書を誤発行させることができる(かもしれない)

TLSの現実



- 正当な証明書を持っている偽サイトは、TLSで検知できない
  - ブラウザは警告しない
  - 証明書を取得する段階でのなりすましを防がないと、TLSの意味がない

証明書発行プロセスにおける通信



もっと端的に言うと

- 「いまどきはHTTPSが常識だよね、HTTPとかありえなくない?」
- …というならば、Let's Encryptのhttp-01チャレンジはありえないのでは?

  `http://example.jp/.well-known/acme-challenge/<TOKEN>`

- こんな非常識な方法でドメイン認証していて証明書は安全なの?

なりすまし、できる?

- なりすましや中間者攻撃を成功させるのが困難なのは間違いない
- が、100%できないと断言できるのであれば、そもそもTLSが不要
- 仮にできたとしても、盗聴や改竄は防ぐためのものがTLS
  - 「困難」と「不可能」の間の可能性を埋める技術
  - つまり、TLSを考える上で、なりすましは「できる」ことが前提
  - 「可能性が低いから考慮しなくていい」は絶対に不可

EV証明書ならば…!

- DV→OV→EVの順にドメイン認証や実在性確認の厳格性が増す
- が、EVでもDVでも、「CAがお墨つきを与えた」ということでは同じ
  - 以前はブラウザがEVを特別扱いしてURLバーの表示を変えていたが、今ではやめてしまって見た目の違いはない
  - 「そのサイトはEV証明書を使っている」という事前知識がなければ、「DV証明書を使ってる! おかしい!」と気がつくこともない
  - EV証明書を使っているはずのサイトであっても、攻撃者にとってはDV証明書を誤発行させることができれば十分
- EV証明書の厳格な審査はなりすまし対策にはならない

Certificate Transparency

- 証明書発行を記録、公開、監視、検証する仕組み
  - 発行した証明書を公開ログに登録する → 登録されていない証明書を不正とみなす
- ドメイン所有者が関知しない証明書が発行されたことを検知できる
  - 監視していないと検知できない(どっかから勝手に通知が飛んできたりはしない)
  - ブラウザからは検知できない(証明書とログの整合性は検証できるが、誤発行でも整合性はあう)
- 誤発行そのものを防ぐ仕組みではない
  - 発行→検知→対処までの間に被害が出る可能性はある

どうやって対策する?

- PKIの信頼モデルは証明書が正しく発行されていることが大前提だが、発行プロセスが平文でおこなわれるので正当性を保証できない
  - のはずだけど、保証してる扱いになってるような???
- TLSを使わずになりすましを完璧に検知できるような都合のいい方法はない
  - そんな方法があるならTLSなんかに頼らずはじめからそれだけ使ってりゃいいんです
- しかし、どんなケースにも対応できる完全な方法ではないけれど、特定の攻撃手法によるなりすましを防ぐ方法ならば、ある

RPKI

- IPアドレスやらAS番号やらのリソースを証明・検証するための仕組み
- BGP経路広告の正当性を検証することができる = 経路ハイジャックによるなりすましを検知できる
- あんまり普及していない

- ISPが実施するもので、ドメイン所有者やCAの意思では実施できない
  - ISPのみなさん頑張ってください
  - <宣伝>IIJ、RPKIはじめました → https://eng-blog.iij.ad.jp/archives/9320</宣伝>

DNSSEC

- DNSの登録情報を署名・検証する仕組み
- DNSの改竄によるなりすましを検知できる
- あんまり普及していない

- RPKIとは異なり、ドメイン所有者の意思で署名でき、CAの意思で検証できる
  - <宣伝>IIJ DNSプラットフォームサービスはDNSSECが簡単です</宣伝>

Multi-Perspective Validation

- Let’s Encrypt独自のなりすまし対策
  - https://letsencrypt.org/2020/02/19/multi-perspective-validation.html
  - http-01やdns-01のチャレンジトークン確認を世界各地の複数拠点からおこなう
  - 複数拠点からの通信を同時に乗っ取る必要があるので攻撃の難度が増す、はず
  - が、無力化できるとの報告が…
    - https://i.blackhat.com/USA21/Wednesday-Handouts/US-21-Shulman-Lets-Attack-Lets_Encrypt.pdf
- 仮にLEの意図どおりの効果があったとしても、攻撃者はこの手法を使っていない別のCAから証明書を発行させるという方法で回避できる

CAAレコード

- 「うちのドメインはこのCAからしか証明書を発行させないよ」とDNSで宣言するためのレコード
  - 「こっちのCAはなりすまし対策が強固だから、対策の弱い別のCAを騙して発行させよう」という攻撃者への対策になる、はず

- あんなの飾りです。偉い人にはそれがわからんのです。
  - なりすまし可能な攻撃者が、CAAレコードを改竄せずに放置しておいてくれるなんて都合がよすぎる妄想
  - CAAが改竄されないよう対策(=DNSSEC署名)されなければ実効性はない

CAの規準

- 「こっちのCAはなりすまし対策が強固だから、対策の弱い別のCAを騙して発行させよう」という攻撃者に対抗するためには、CAが独自に対策するだけではなく、CA全体の最低ラインを引き上げることが必要
- 主な規準
  - WebTrust for CA: アメリカ、カナダの会計士協会による電子商取引規準
  - CA/Browser Forum: CAとブラウザ開発ベンダーで構成される団体による規準
    - Baseline Requirements
    - Network Security Requirements

CAのDNSSEC検証

- WebTrustも、CABFも、どちらもDNSSECやRPKIの検証を必須としていないっぽい
- つまり、「DNSSEC署名していたのにCAが検証しないせいでDNS改竄を見抜けず証明書が誤発行される」という可能性がありうる
  - そんなインシデントが実際に発生するとそのCAの存続にもかかわる大問題になるのは明白なので、ちゃんとDNSSEC検証しているCAが多そう
  - が、すべてのCAがDNSSEC検証している保証はない
- RPKIについてはISPが実施するものなのでCAではどうにもならない…

じゃあDNSSECの効果ないの?

- DNSSECがあればなりすましをかならず検知できるわけではない
  - DNSSEC検証で問題がなくても、Webサーバへの経路をハイジャックできればhttp-01チャレンジは成功する
- しかし、攻撃者の取りうる選択肢は減る
  - 「DNSを改竄しない手法でなりすます」か「検証しないCAを狙う」かどちらか
  - すべてのCAがDNSSEC検証するようになれば後者も選択肢から消える
- 100%完璧な対策以外は無意味というわけではない
  - 多層的な対策を取って実現可能性を少しずつ下げていくことが重要

証明書取得時以外でも…

- 正当なドメイン所有者であることが確認される場面は、TLS証明書取得時だけではない
  - メールの送信ドメイン認証
    - SPF、DKIM、DMARC
  - SaaSサービスを利用するときのドメイン認証
    - “google-site-verification=xxxxx” とか “MS=msxxxxx” とか “facebook-domain-verification=xxxxx” とかのTXTレコード
- 不正に乗っ取られないような対策は十分にしておくべき

まとめ

- WebPKIでは、ドメイン認証をインターネット経由の平文通信で実施するため、なりすましの余地がある
  - 可能性が高いわけではないが、ありえないと断言できるならそもそもTLSは不要
- HTTPSが常識になったからこそ、TLSに頼らないなりすまし対策が重要
  - ドメイン所有者の立場で可能なのは、DNSSEC署名
  - CABFはDNSSEC検証を必須にするようBRを改訂してください…
  - RPKIの普及も進めよう

おまけ

- Q: そんなこと言うならCAに頼らずDNSの仕組みだけで証明書を発行できるようにしたら?

- A: そういう仕組みはすでに存在する(DANE; RFC6698)けど、ブラウザが対応していないので使いものになりません
  - オレオレ証明書扱いになる
  - Webではなくメール方面ではわりと受け入れられている(sendmail、postfix、eximなどで対応済み)