2022年6月21日 IWショーケース徳島

# ドメイン名と証明書とTLS
# ～ 署名のカクゴ / 検証のカクゴ ～

我々は何をしようとしているのか

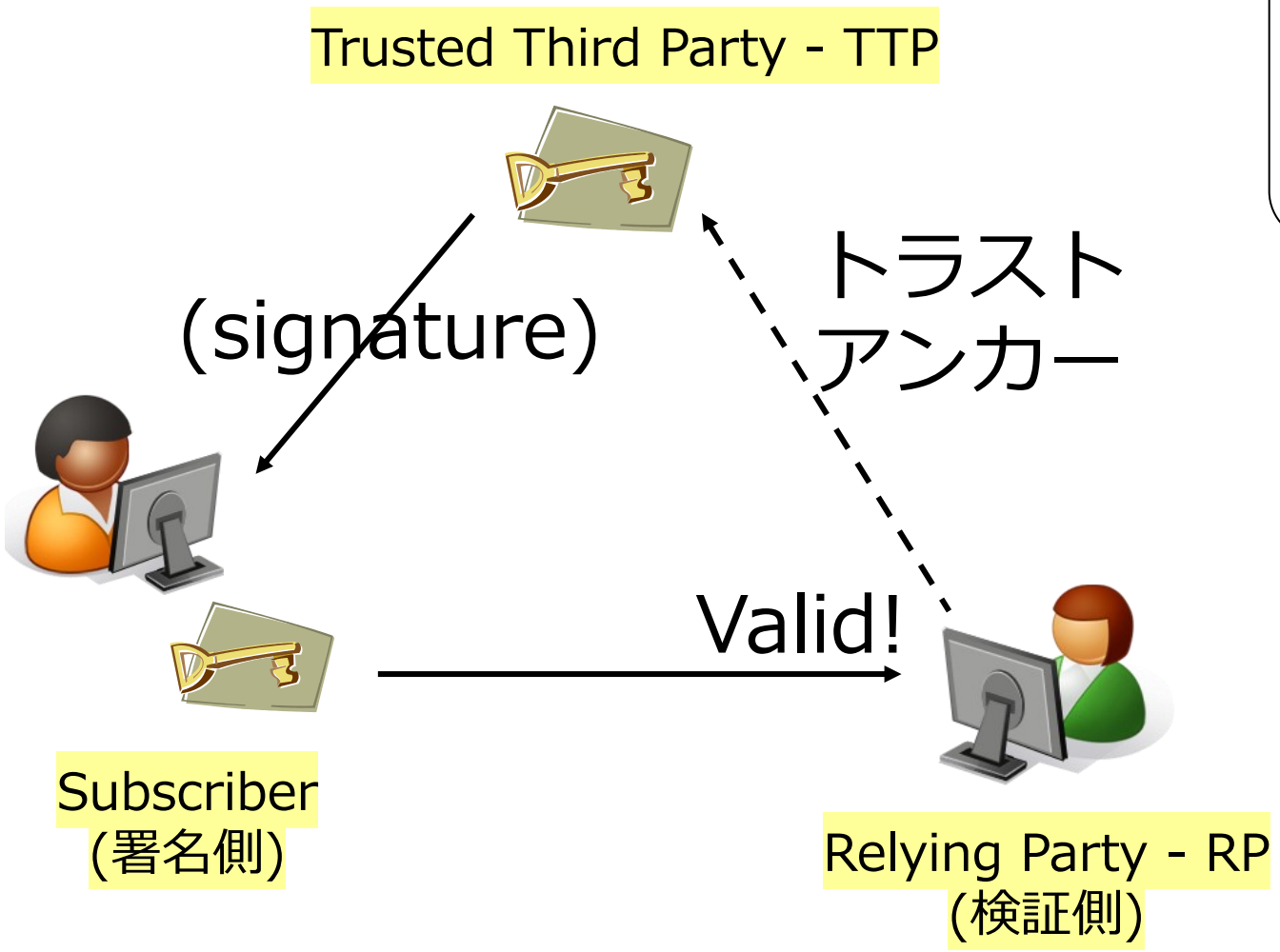
木村泰司

JPNIC 一般社団法人 日本ネットワークインフォメーションセンター

# 内容

- カクゴ
- WebのPKIとDANE
- ドメイン名と証明書とTLS
- DV, OV, EV
- 我々は何をしようとしているのか「DNSSEC」

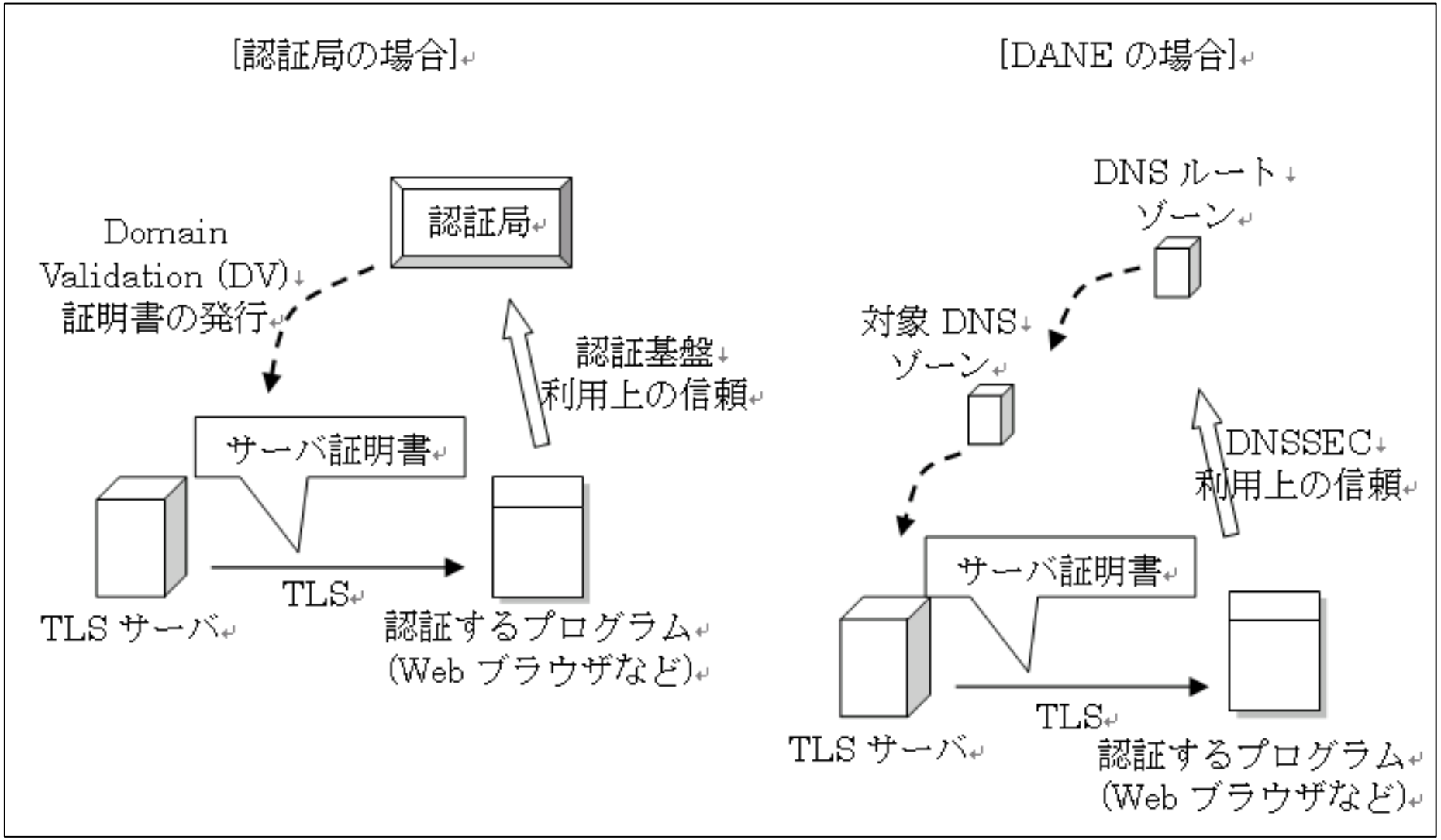
# カクゴ　－鍵に対する期待と検証結果への対応－




□公開鍵暗号基盤で行われていること
第三者を設け、鍵保有等に関する信頼性を担保。鍵使用の結果が期待される条件を満たすようにする。

- 署名側のカクゴ
  鍵使用の結果が「正しい」
  - エンティティの認証
  - データの認証
- 検証側のカクゴ
  Relying(依拠)して判断
  - “条件を満たす”対象
  - 判断の結果の扱い

# 認証局を使う場合とDANEを使う場合

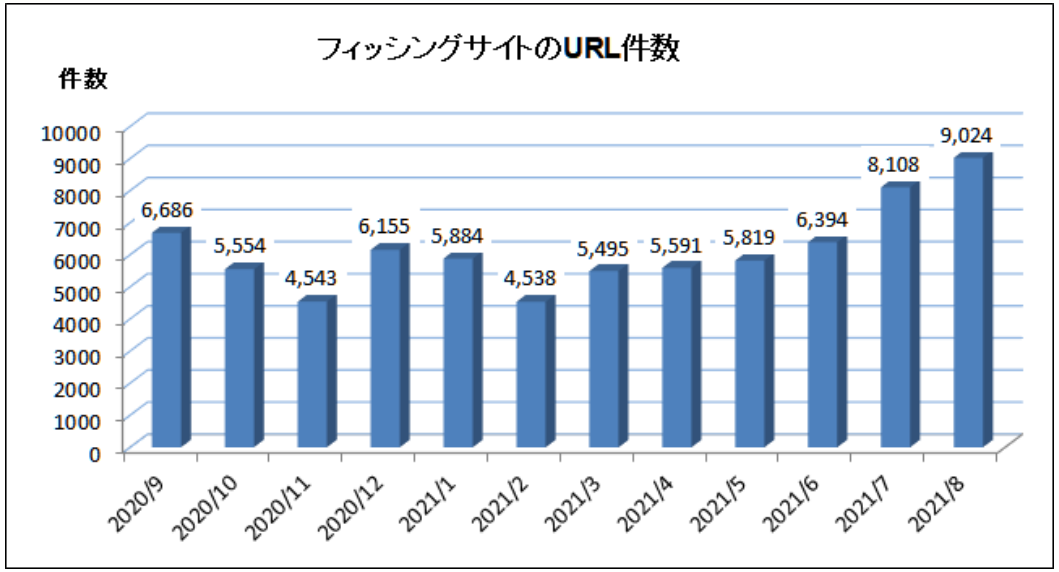



情報セキュリティ技術動向調査（2011 年上期）：IPA 独立行政法人 情報処理推進機構　「4. DNSを用いた公開鍵の配送技術 – DANE」より
https://www.ipa.go.jp/security/fy23/reports/tech1-tg/a_04.html

# ドメイン名と証明書とTLS (1/2)

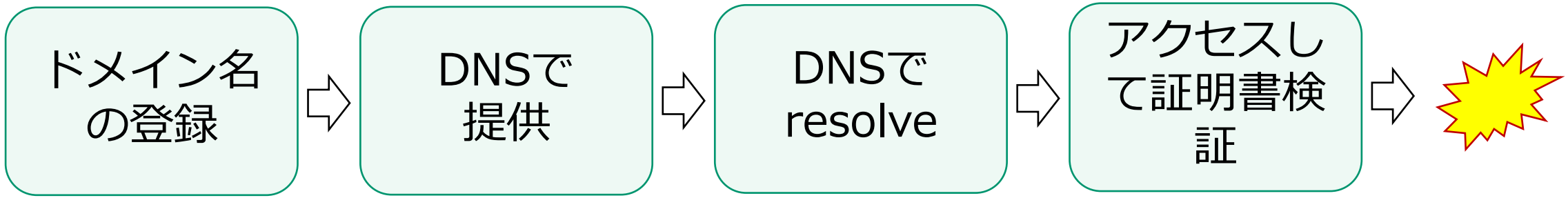
- **“トリプルプレー”**
  - 偽のBGP経路情報を流す。
  - 偽のDNS応答を返す。
  - 偽のサーバ証明書を返す。

トリプルプレーまででではなくても....




2021/08 フィッシング報告状況, フィッシング対策協議会
https://www.antiphishing.jp/report/monthly/202108.html

例




紛らわしいドメイン名　偽のDNS応答　偽のresolve結果　正しく検証できるサーバ証明書

# ドメイン名と証明書とTLS (2/2)

| DV | OV | EV |
| --- | --- | --- |
| Domain Validation | Organization Validation | Extended Validation |
| ドメイン名の確認 | 組織の確認 | 組織の確認 (登記簿等とオンラインでない手段) |

# 我々は何をしようとしているのか

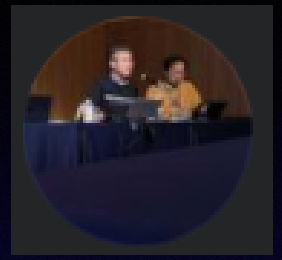
- **ドメイン名の設定(DNSSEC)**
  - リソースレコードの改ざん検知　／　権威サーバのなりすまし検知
    ⇒ 元来はDNSの委任構造に従ってリソースレコードを守るもの。特に手で指定されるようなドメイン名を守るなら。SERV FAILはこわい。でも様々なTXTレコードが。。

- **Webサーバ(TLS / QUIC)**
  - 鍵マークが表示されれば安心、ではない。
  - DV・OV・EVの心を…
    ⇒ 検証結果にはSubscriberの”条件”が宿っている、が「見えにくい」。
    ⇒ ユーザにドメイン名を確認して頂く必要があるのが現在。

- **メールサーバ(TLS)**
  - ここで行われている認証は何のためなのか。
    SMTPSの検証結果は誰が見るもの？

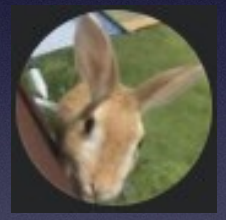
# 我々は何をしようとしているのか

Webサーバの証明書やドメイン名登録や
クラウド事業者の動向を踏まえた上での
「DNSSEC」



石田慶樹さん


小山裕司さん



其田学さん

藤原和典さん

※五十音順

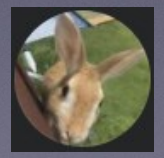
ご発言は個人の見解によるものです。
所属組織を代表するものではありません。

Q1. 権威側の署名はすべき？
カクゴがいるので、こうすればいける！を教えてください。

# Q1. 権威側の署名はすべき？カクゴがいるので、こうすればいける！を教えてください。

改竄されると不味いサービスが乗ってるんであればやるべき。

ただ自前でやるにはハードルが高いんで、対応サービスを利用するべし。



其田学さん

クリティカルなサービスなら入れたほうがよいですよね。

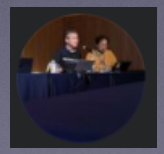
入れておけば防げたのに、とかならないように。

小山さん

小山裕司さん

社会的に重要なドメイン名においては、署名すべき。

別に覚悟とかしなくとも、DNSプロバイダー(CDN事業者含む)で簡単に署名できるようになっているのでは。



石田慶樹さん

IIJとかCloudflareが提供しているDNSSEC対応のDNSサービスを使うといい、、

鍵更新の頻度を下げてゾーンファイルの編集と署名を組み合わせた簡単な手順を考えるとよいです。

藤原和典さん

Q2. リカーシブリゾルバーで
署名検証はすべき？
SERVFAILについてどう考れば？

# Q2. リカーシブリゾルバーで署名検証はすべき？ SERVFAILについてどう考えれば？

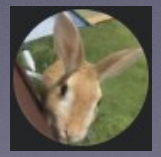
署名検証は簡単なのでするべきです。
SERVFAILになったらそのサイトはアクセスすべきでないです。

WebPKIでサーバ証明書が失効したのにアクセスしたい人なんていませんよね？

藤原和典さん

フルリゾルバで署名検証しないという選択肢はもはや無い。
SERVFAILしたということは、検証が有効に働いたということなので歓迎するべき事象。

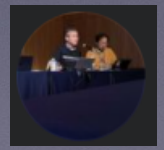
権威側の問題で発生した場合は、毅然として権威側の問題ですと回答するだけ。



其田学さん

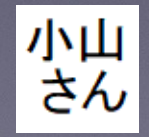
なんで検証しないの？

Integrityの観点からはSERV FAILはやむを得ない。



石田慶樹さん

ntaの運用方法。
使い方が分かれば入れられるかと。




小山裕司さん

Q3. DNSの支える“トラスト” ----
固いDNS運用によって支えられる
インターネットはどんなカタチ？

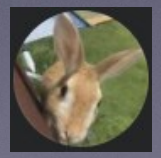
# Q3. DNSの支える“トラスト” ---- 固いDNS運用によって支えられるインターネットはどんなカタチ？

クライアント証明書などにも使えるようにしようというのを念頭に置くと end 2 end のセキュリティが確保できるようになるかも。

小山さん 小山裕司さん

すでにDNSはDNSSEC導入を前提として様々なプロトコルの信頼の起点となっている。

DNSSECが普及することでより安全なプロトコル開発など、インターネット全体の機密性・完全性を向上させることに繋がる。



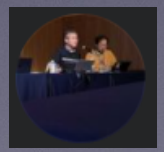
其田学さん

DNSだけが固くてもドメイン名登録はまた別だし、迷惑メールとか偽サイトもまた別問題であまりかわらない。

藤原和典さん

DNSとは、実はDNSに閉じておらず、DNSをシグナリングに使っているあらゆるサービス／アプリに関与。

社会基盤に近いサービスやアプリでは「固い」DNS運用が必要である。一方で、すべてを固くしなくてもよい余地を残せるとこが、インターネットらしさではないか。



石田慶樹さん

# まとめ

# おわり