JANOG42.5 Interim Meeting, Tokyo, October 18th, 2018

マンション証明書と一戸建て証明書

Internet Initiative Japan

wizSafe

セキュリティ本部セキュリティ情報統括室
須賀祐治
2018-10-18

Ongoing Innovation

最初の「お作法」

- 本発表について
  開示すべき利益相反状態はありません.

- 本発表はすべて筆者の個人的見解であって所属組織とは無関係です.

自己紹介代わりに

https://www.iij.ad.jp/news/iijnews/

- 今日発行されました！

須賀執筆のIIRネタ(抜粋)

https://www.iij.ad.jp/dev/report/iir/

- Vol.39 (2018-06) ROCA(RSA実装問題)
- Vol.33 (2016-12) TLS1.3
- Vol.31 (2016-06) 耐量子暗号
- Vol.30 (2016-03) Let's Encrypt
- Vol.26 (2015-02) ID管理技術
- Vol.25 (2014-11) POODLE attack
- Vol.21 (2013-11) 仮想通貨 Bitcoin
- Vol.18 (2013-02)
  暗号技術を用いたプロトコル・実装に
  多発している問題の整理とあるべき姿

再掲

マンション証明書と一戸建て証明書

Internet Initiative Japan

wizSafe

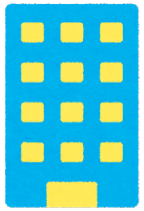
セキュリティ本部セキュリティ情報統括室
須賀祐治
2018-10-18

Ongoing Innovation

タイトルからはこういうイメージ？

今回の発表方針とか

- Terminology 思いついたので言ってみる
  - 「一番先言うたで」というスナップショット

- VPS等でのサーバ証明書配備を調査してみるとある観点での分類ができそうなことに気がつく
  - マンション証明書  一戸建て証明書 
- メリットとかリスクとかの分析はまだできていない
  - 議論のきっかけになればいいなと
  - 忌憚なきご意見お待ちしております

マンション証明書

Subject Alternative Name

- 異なるドメイン名がSANに共存している証明書

Subject DN OU=Domain Control Validated, OU=PositiveSSL Multi-Domain, CN=sni178105.cloudflaressl.com

Issuer DN C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2

Serial 374962007578661058562359913471005634O8

Validity 2018-02-22 00:00:00 **to** 2018-08-31 23:59:59 (190 days, 23:59:59)

Names
*.angrycpu.com
*.baeb71i.ga
*.blockcoiners.com
*.cediplus.org
*.cellos-consortium.org
*.choinkidomacyno.gq
*.deuz39i.cf
*.faab52i.cf
*.game2cloud.com
*.genesequencing.gq
*.hellosmooth.com
*.jiez97i.cf
*.kentonchamber.org
*.lanicchiadelsole.altervista.org
*.leav11i.cf
*.leiq89i.ga
*.manhoodlose.ga
*.multansultan.com.pk
*.noem25i.ga
*.qwpfilmlink.ga
*.ratanfire.in
*.softwarebombde.tk
*.sotrue.cc
*.soulbible.ga

VPSでお隣のVMに入居してる人の顔を知らない状況とよく似てる

https://censys.io/certificates/2843400699468ff9439c3ec89c3ee475d8d6ae9d1ca4107cad94d54b112c5e8f

一戸建て証明書

- 同組織のFQDNのみが同居する証明書
  - 居候とか内縁とかヤヤコシイツッコミはやめてね

Subject DN	C=US, ST=California, L=Mountain View, O=Google LLC, CN=*.google.com
Issuer DN	C=US, O=Google Trust Services, CN=Google Internet Authority G3
Serial	1721922324728960956
Validity	2018-10-09 13:09:00 **to** 2019-01-01 13:09:00 (84 days, 0:00:00)
Names	*.android.com *.appengine.google.com *.cloud.google.com *.g.co *.gcp.gvt2.com *.ggpht.cn *.google-analytics.com *.google.ca *.google.cl *.google.co.in *.google.co.jp *.google.co.uk *.google.com *.google.com.ar

https://censys.io/certificates/2b51048cefd7a7aee614d2c2f90cf4121384ab63986787bac37737185f01e768

一戸建て証明書（表札が一つの姓）

- 同じドメイン名のFQDNのみ同居する証明書
  - 異なるサブドメインがたくさん並ぶ

Subject DN	C=US, ST=Washington, L=Seattle, O=Amazon.com, Inc., CN=amazon-smtp.amazon.com
Issuer DN	C=US, O=DigiCert Inc, CN=DigiCert Global CA G2
Serial	208513026824282538909873398231772048 13
Validity	2018-04-09 00:00:00 **to** 2019-05-07 12:00:00 (393 days, 12:00:00)
Names	amazon-smtp.amazon.com smtp-fw-0101.amazon.com smtp-fw-0102.amazon.com smtp-fw-0103.amazon.com smtp-fw-2101.amazon.com smtp-fw-33001.amazon.com smtp-fw-36001.amazon.com smtp-fw-36002.amazon.com smtp-fw-4101.amazon.com smtp-fw-52001.amazon.com smtp-fw-52002.amazon.com smtp-fw-52003.amazon.com smtp-fw-52004.amazon.com smtp-fw-6001.amazon.com smtp-fw-6002.amazon.com smtp-fw-7002.amazon.com

https://censys.io/certificates/31f39c4ea054b1dbbec53171dcc729f6ad6bb55ae338096c74afe5df88248d02

ぼっち証明書

- たったひとつのFQDNだけに対応した証明書

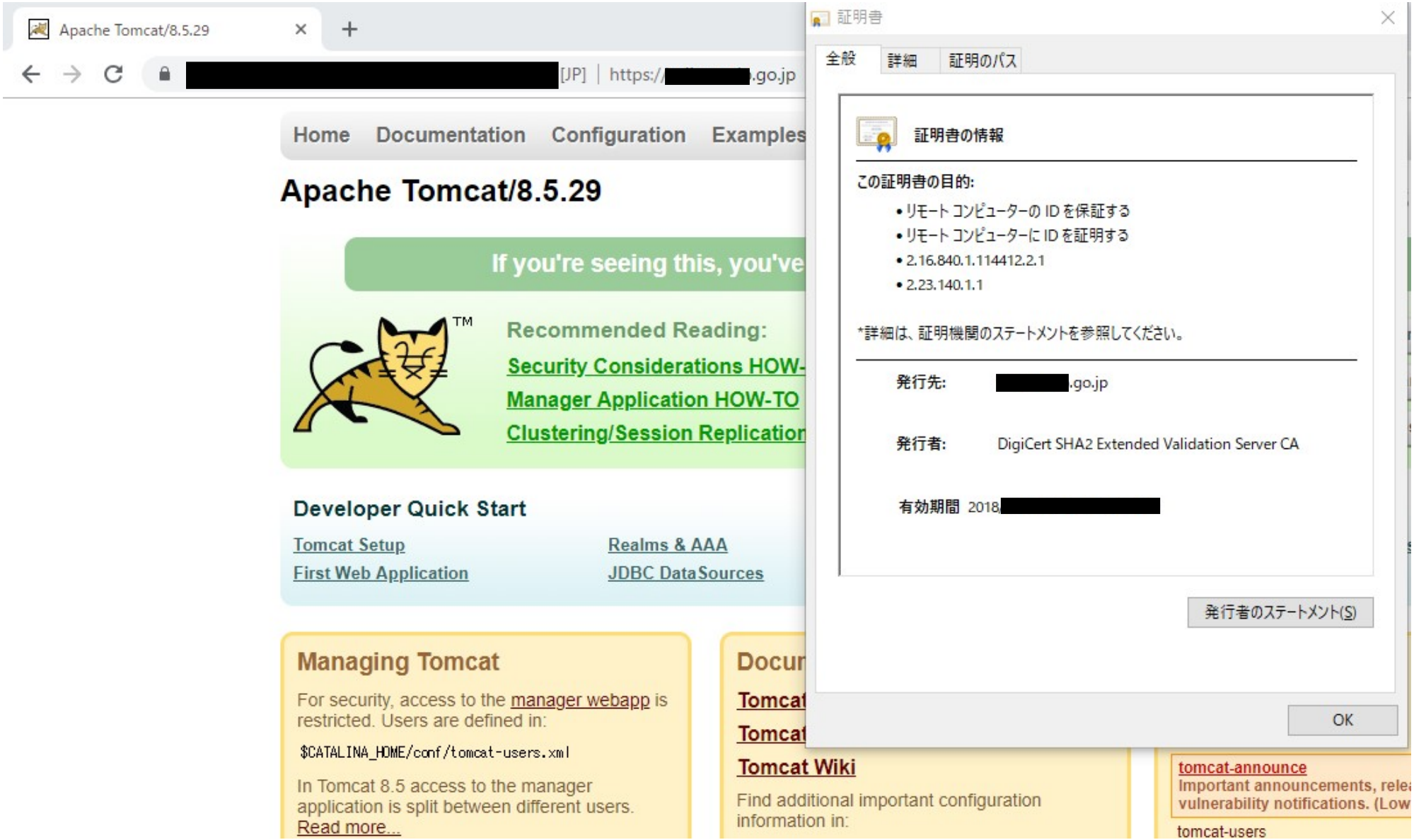
https://censys.io/certificates/692bcd68738efa3d0b92df89164c409533d17855a6ce6e21bb3b04aca5297f82

ぼっち証明書(⊂一戸建て証明書)の功罪

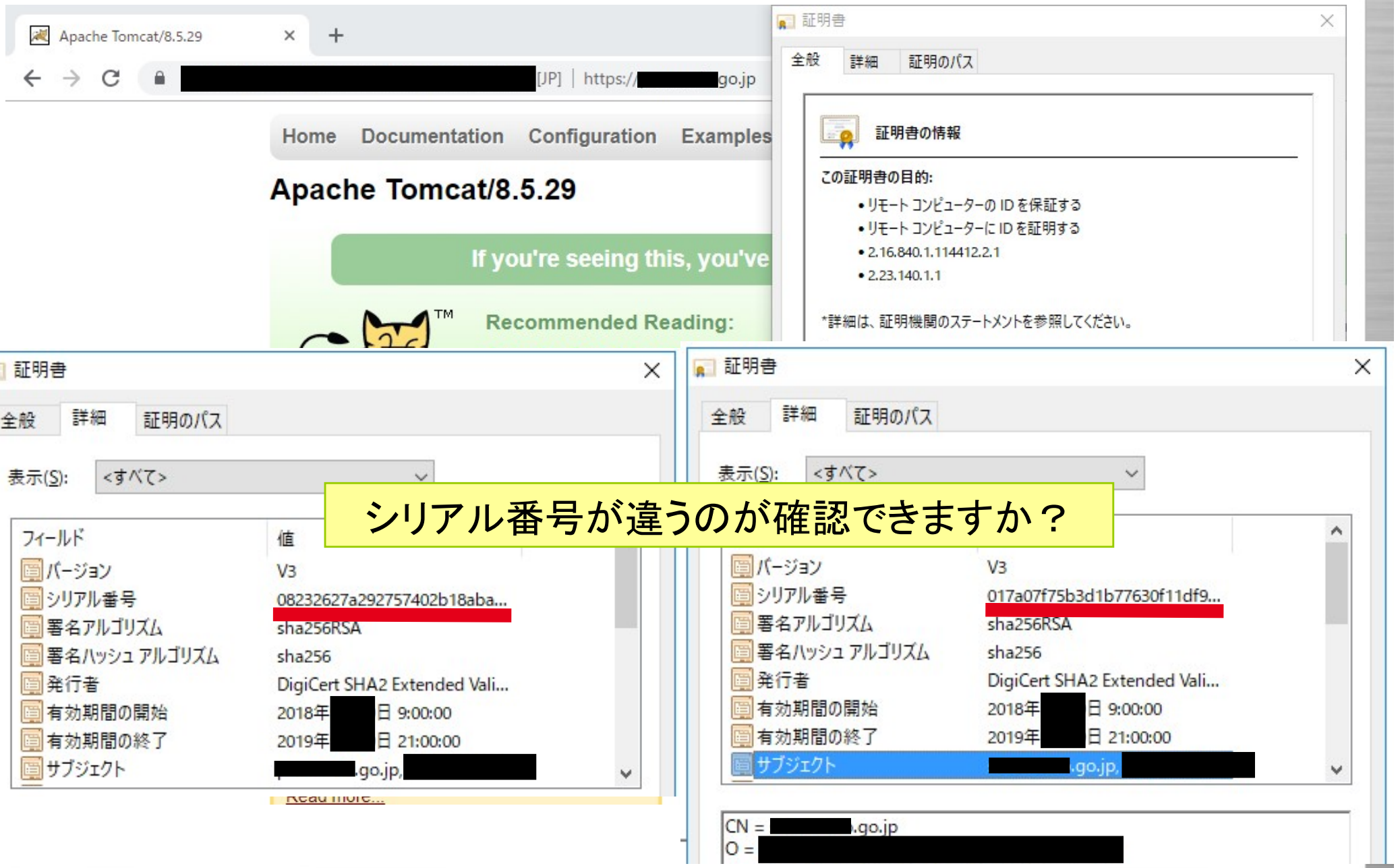
- CTの仕組みにより証明書発行するとFQDNがバレる
  - JANOG40でご紹介した Censys 等で簡単に
    - 事後資料出してないことに今頃気がつく
  - 特にごく最近発行されたものだけをピックアップすると次頁のようなことが判明してしまう
  - https://censys.io/certificates?q=念のため自主規制 念のため自主規制 **parsed.validity.start** 念のため自主規制 **2018-09-01** 念のため自主規制 念のため自主規制 **ev** 念のため自主規制

https://www.janog.gr.jp/meeting/janog40/program/censys

よゐこのみんなはやっちゃダメよ

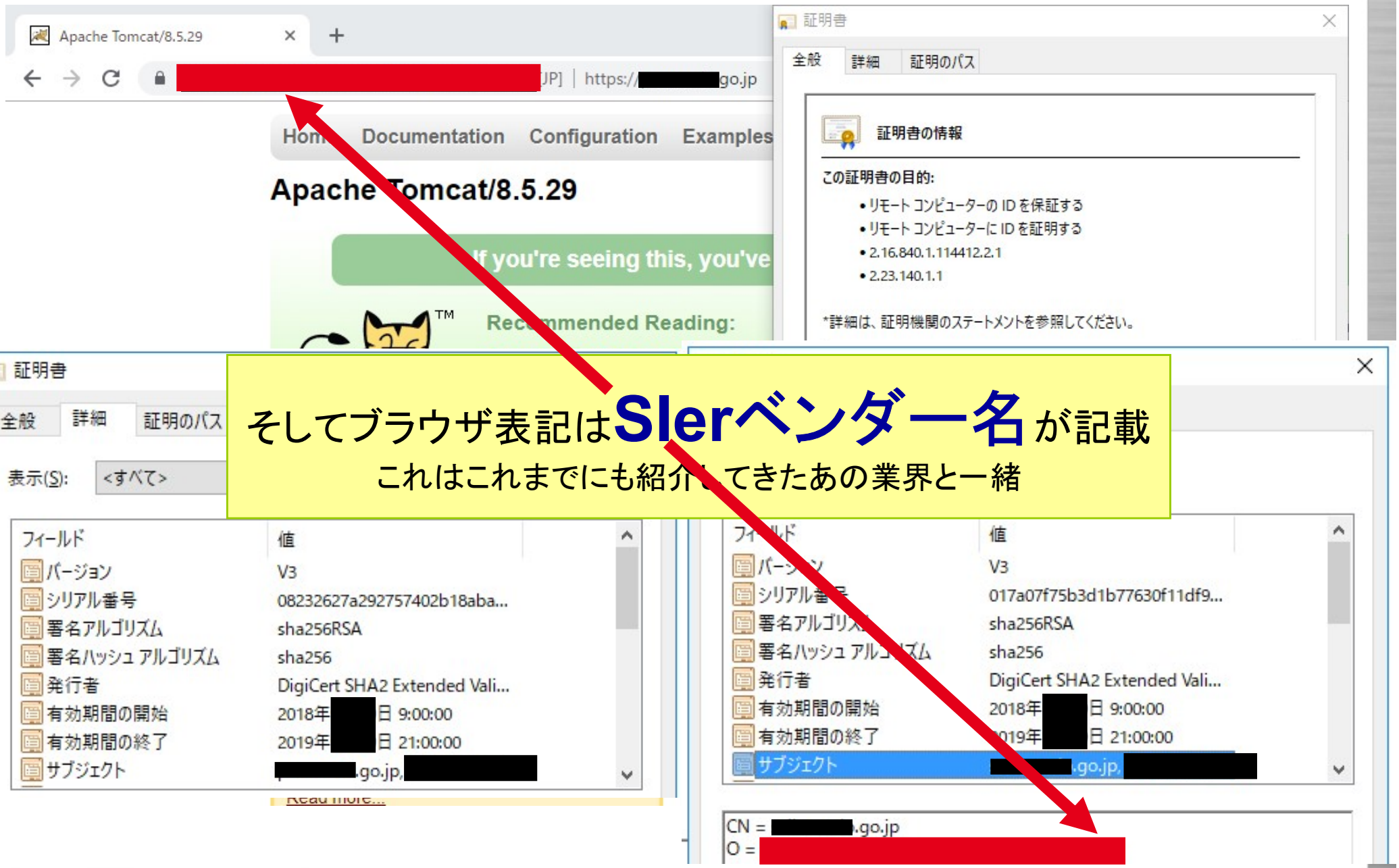


実はもう一枚同日発行されてる



シリアル番号が違うのが確認できますか？

しかもEV証明書の名称がアレゲ



そしてブラウザ表記は**SIerベンダー名**が記載

これはこれまでにも紹介してきたあの業界と一緒

ここから見えてくること

- 案外ワイルドカード証明書もアリなのかな？
- 参考情報：FAMGA

ワイルドカード証明書	Facebook
一戸建て証明書	**A**pple　2人同居=新婚？ **A**mazon　4人同居 **M**icrosoft 7人同居=2世帯くらい **G**oogle　えらいたくさん しかも多国籍
ぼっち証明書	**G**oogle (www.google.com)

マンション証明書のリスク

- 異なる組織が同じ鍵ペアを利用している
  - 理論的にはお隣さんのTLSトラフィック読める？
    - SNIの仕組みとかVMの独立性に依存しそう
  - （そもそも）VPSベンダーが鍵生成してるから…
  - go.jp でもマンション証明書を保持してるFQDNあり
- 自分で調べたサービスは秘密鍵が
  ぶっこ抜けないようになってた
  - （いや，そこは本質じゃない）

リモート鍵とかHSMとかで解決？

- ネットワークトポロジで分類できそう
- リモート：鍵が必要になった時点で問い合わせ
  - レスポンスできる？
  - そもそもVPS借りてる意味は？
- 物理的なHSMを預ければいいのかい？
  - コスト高いわ，物理配送が必要で即時開通できん

そのほか関連情報

- Chrome URL表記 www 端折る問題
  - “Trivial Subdomains” でggrks
- TLS1.0/TLS1.1 死亡のお知らせ
  - https://twitter.com/agl__/status/1051933087699881984
- 2日前のChrome70でレガシー証明書死亡
  - https://www.websecurity.symantec.com/ja/jp/blog/replace-your-symantec-ssl-tls-certificates
- IPアドレス証明書はどう考える？
  - SANに含めた証明書事例：1.1.1.1
    - http://blog.livedoor.jp/k_urushima/archives/cat_30545.html
- GPKIのてんmせdれfrtgyふじこ

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

お問い合わせ先 IIJインフォメーションセンター
TEL 03-5205-4466（9:30～17:30 土/日/祝日除く）
info@iij.ad.jp
http://www.iij.ad.jp/