Let’s Encryptのルート認証局移行問題の解説

オープンソースカンファレンス2021北海道
2021年6月26日(土) 11:00-11:45 A会場

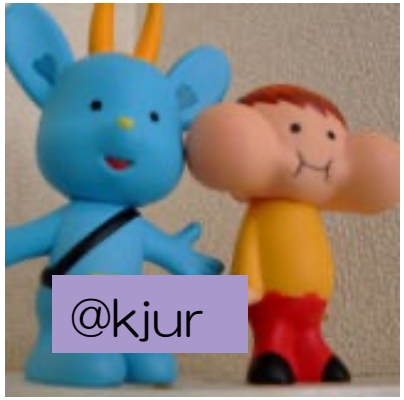
改訂: 2021.06.29 17:12 誤記等修正

漆嶌賢二, CISSP (うるしまけんじ @kjur)

自己紹介: 漆嶌 賢二(うるしま), CISSP

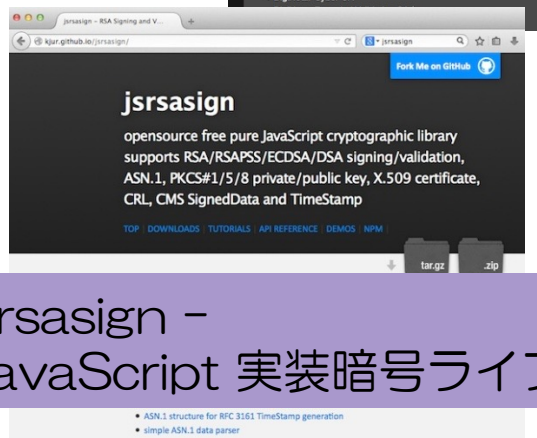
- 経歴
  - PKIベンダー(2019-)、
  - 製造業(2010-)、PKIベンダー(2002-)
- 興味：

  PKI, TLS, 電子署名, SSO, 認証, 暗号,
  CSIRT, 脆弱性検査, フォレンジック,
  スマホ, プログラミング, ビットコイン
- 別名
  - 証明書ハンター
  - (TLS)暗号スイートウォッチャー
- 委員、標準化、認定基準、実証実験、普及啓蒙
  - JNSA, CRYPTREC, 日本データ通信協会
    IPAセキュキャン講師
  - 旧ECOM, PKI-J, 欧州ETSI
  - PKI, TLS, 長期署名, タイムスタンプ



Twitterでフォローすべきサイバーセキュリティの専門家リストを日本で選ぶなら
https://yamdas.hatenablog.com/entry/20210420/top-cybersecurity-experts

ブログ：自堕落な技術者の日記



jsrsasign –
JavaScript 実装暗号ライブラリ

オープンソース開発：github/kjur/jsrsasign (2010年6月～)

- JavaScript実装の暗号、PKI、署名フォーマット等のセキュリティライブラリ
- 依存関係もなく、マニュアル等、ドキュメントも充実してて割と使いやすい
- npmパッケージは月間60～70万くらいダウンロード
- 商用商品にも組み込まれている

Google Open Source Peer Bonus

September 16, 2020

Dear Kenji Urushima,

On behalf of Google Open Source, I would like to thank you for your contribution to jsrsasign.

We are honored to present you with a Google Open Source Peer Bonus. Inside the company, Googlers can give a similar bonus to each other for going above and beyond, so this is just a small way of saying thank you for your hard work and contributions to open source.

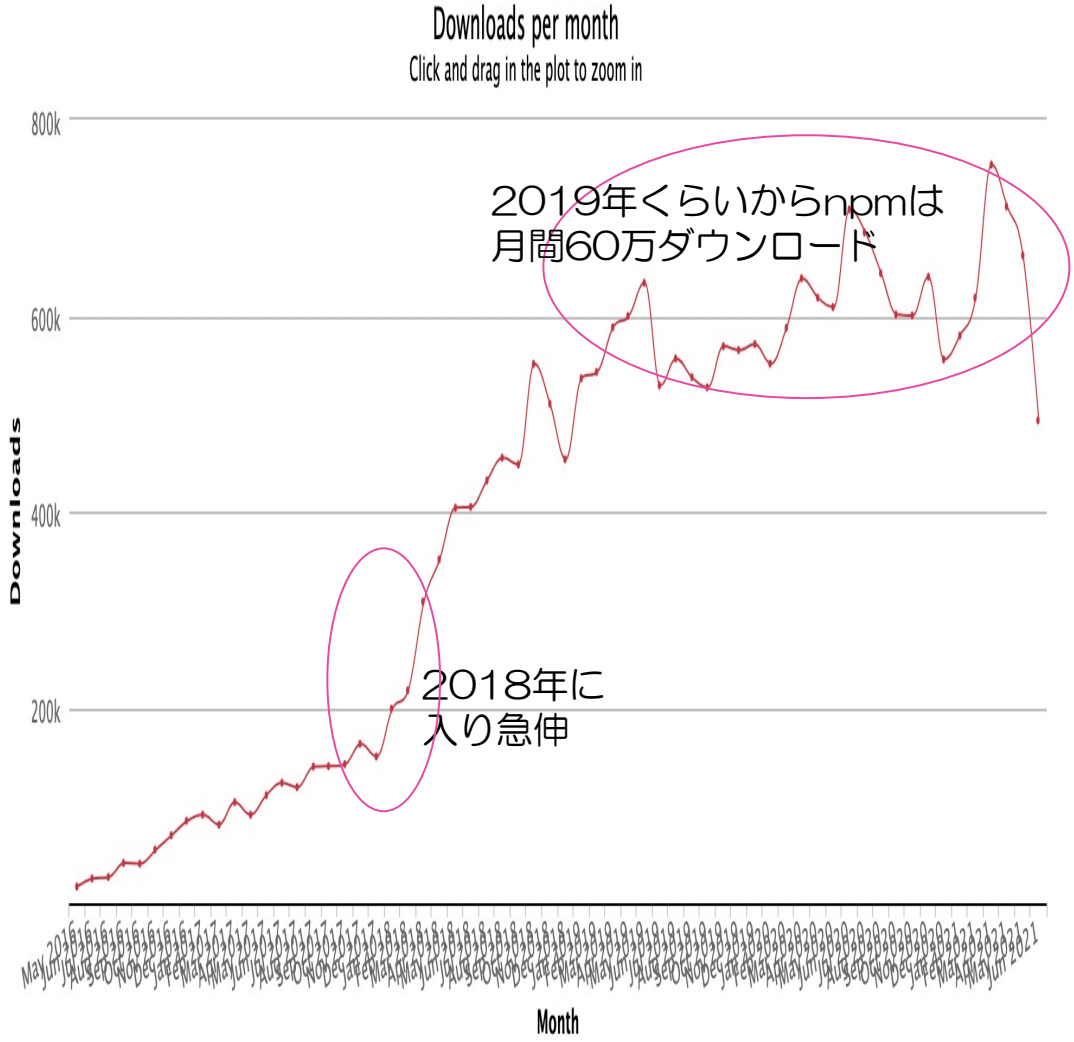
We hope you enjoy this gift from all of us at Google and Eiji Kitamura who nominated you.

Thank you again for supporting open source! We look forward to your continued contributions.

Best regards,

Chris DiBona
Director of Google Open Source

2020年9月にGoogle Open Source Peer Bonus Award 2020Q3を受賞



Qiitaの記事
Let’s Encryptのルート認証局移行についてちょっと調べてみた

https://qiita.com/kjur/items/2fd72b6707497c7fc6c5

HTTPSと証明書とLet’s Encrypt

HTTPSとは

出典：首相官邸ホームページ

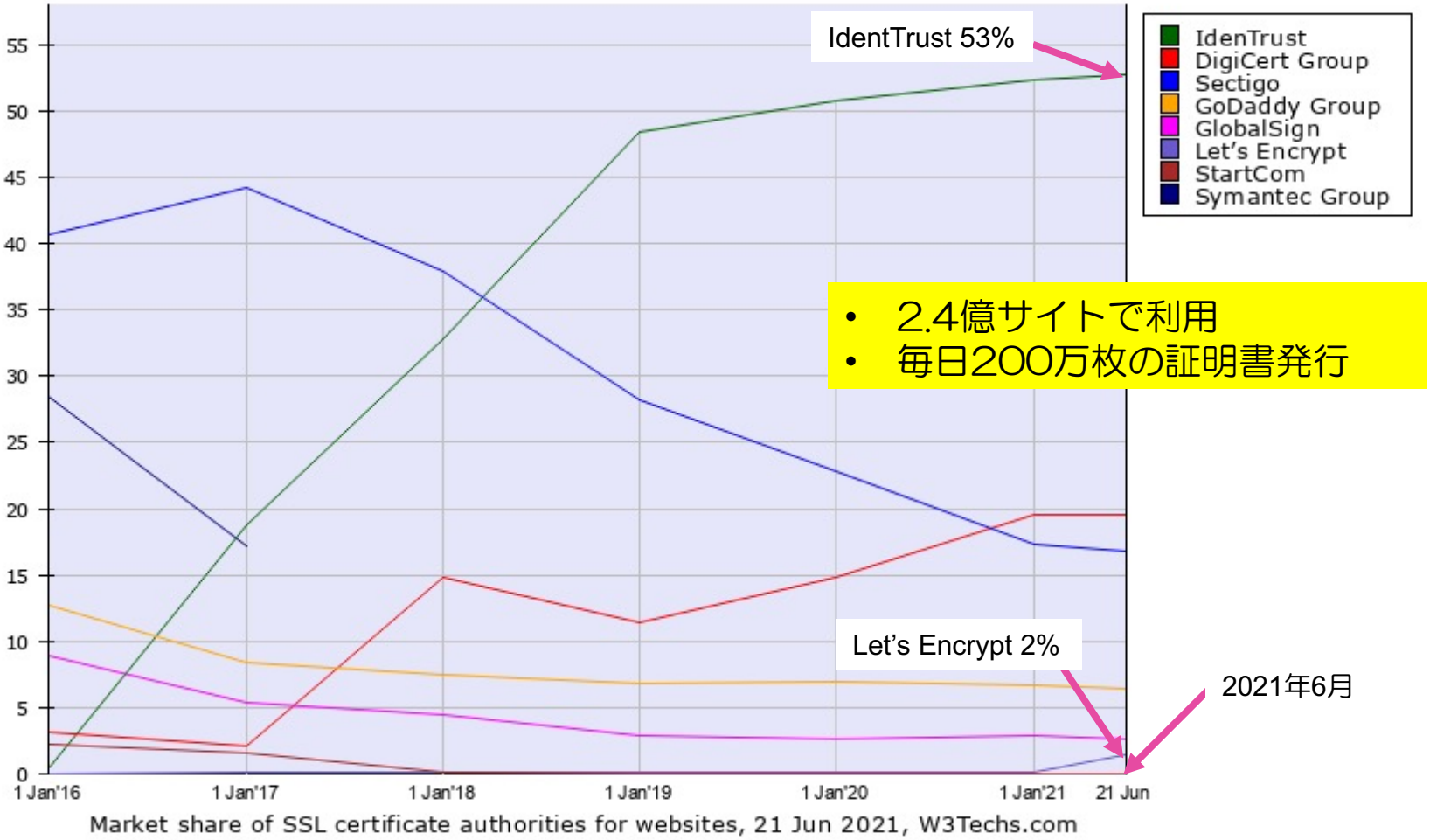
デジタル証明書

Let's Encrypt(LE)とは何か

- 2016年4月から正式スタートした無料TLSサーバー証明書サービス
- 2013年5月設立の米カリフォルニア州公益法人ISRGによる無料証明書発行プロジェクト
- プライバシー保護、セキュリティのために全通信を暗号化したい
- プライバシー保護団体EFF、ミネソタ大、Mozilla、Cisco、Akamaiが創設スポンサー
- サービス維持の資金を、企業、個人による「寄付」で賄う
- certbot、ACMEといった仕組みにより証明書の審査と発行を自動化
- 一日、200万枚の証明書を発行している
- 一日、2億枚の証明書発行が可能
- 2.4億のサイト(ドメイン)がLEを使っている

ウェブサイトにおけるLE証明書のシェア(w3techより)

- IdenTrustは、ほとんどがLet's EncryptのDST Root X3の使用率
- Let's Encryptと表示されているのは自前ISRG Root X1を手動設定してる
- Let's Encryptの使用率：53%+2%=55%

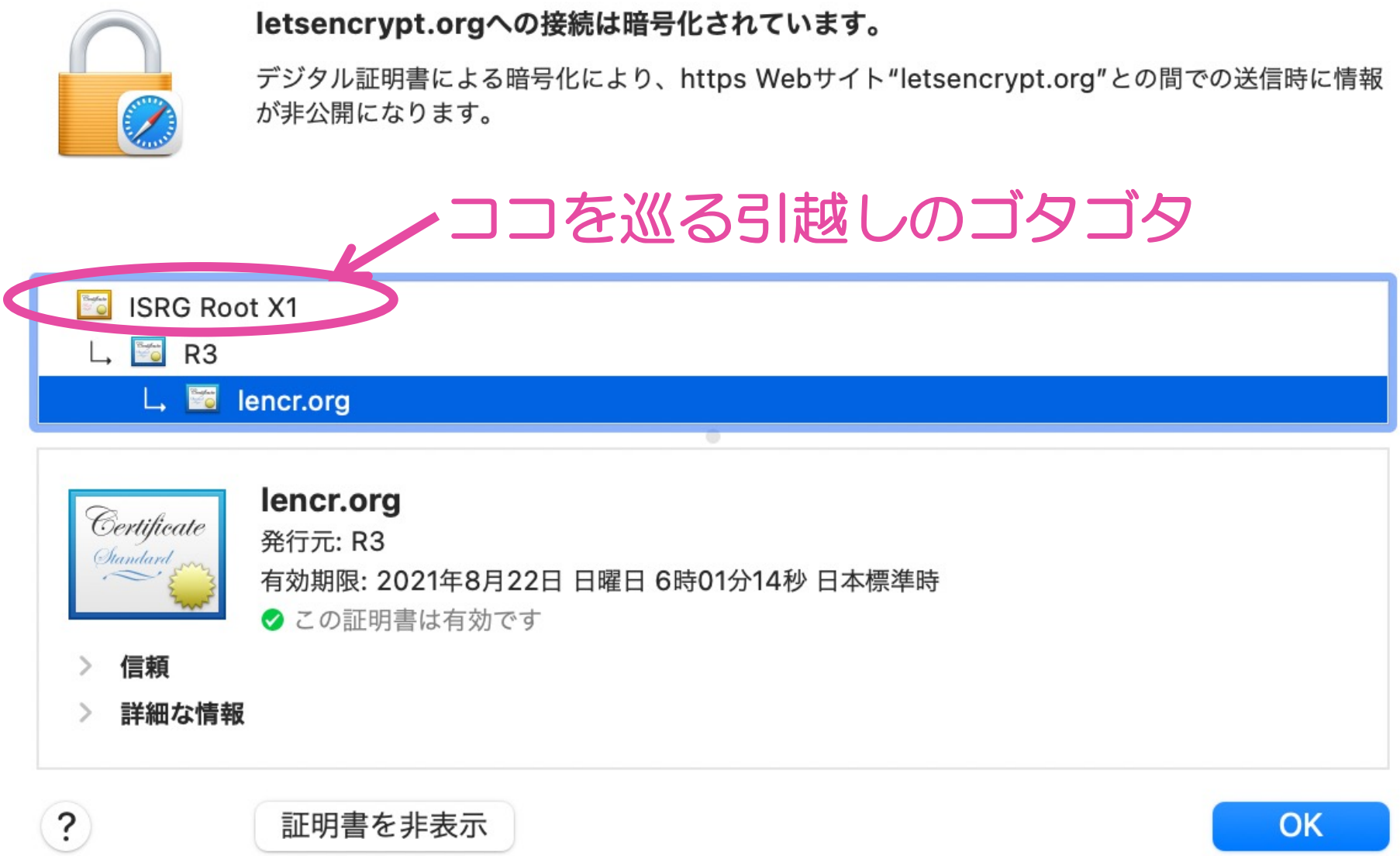


- 2.4億サイトで利用
- 毎日200万枚の証明書発行

出典: W3Techs Market share yearly trends for SSL certificate authority (2021年6月時点)
https://w3techs.com/technologies/history_overview/ssl_certificate/ms/y

Let’s Encryptの
ルート認証局移行、
証明書チェーン移行問題とは

Let's Encryptの発行する証明書のチェーン(繋がり)



Let’s Encryptのルート認証局移行問題を例えるなら

① 新居を建ててみたが、老人にはわかりづらく

② 老人でも着くように当面は廃止の決まってる他社の送迎バスを案内していた

③ その後、スマホを使える老人には送迎なしで新居がわかるようになったので

④ 他社送迎バスの運行をやめようと思ったが

⑤ ガラケーしか使わない老人にはやはり新居にたどりつけないことがわかり

⑥ 拝み倒してガラケー専用の他社送迎バスを新たに運行してもらった

⑦ 案内が二転三転(以上)したのでみんなが混乱した

Let's Encryptの実際四転した証明書チェーン変更のアナウンス

- 2015年6月、ISRGルートX1 CA、Let's Encrypt X1中間CA構築
- 2015年10月、 Let's Encrypt X1中間CAがIdenTrust社ルートと相互認証
- 2016年4月、サービス開始

- 2018年8月、主要全ブラウザにISRGルートX1証明書が搭載された(移行判断)
- 2019年4月、新証明書チェーンの切替を2019年7月に計画告知
- 2020年5月、新証明書チェーンの切替を2020年7月に延期告知
- 2020年6月、新証明書チェーンの切替を2020年9月に延期告知
- 2020年9月、新証明書チェーンの切替を2021年1月に延期告知
- 2020年11月、新証明書チェーンが古いAndroid非対応が発覚
- 2020年12月、古いAndroidを救うウルトラCな方法の実施計画を公表
- 2021年5月、ようやく新証明書チェーンに切替を実施告知
- 2021年9月、古いDST Root X3の期限切れ

結局 2019年7月予定→2021年5月実施
Let's Encryptのアナウンスはあまりあてにならない ☺

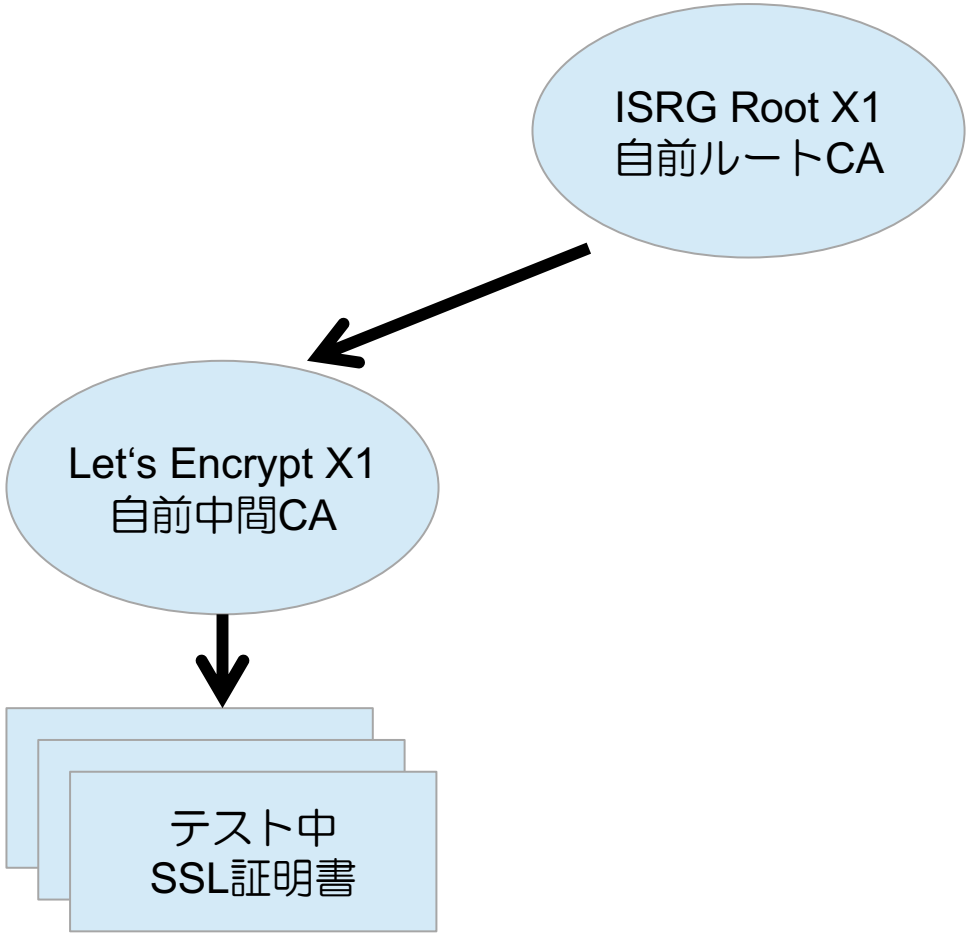
(参考) Let's Encryptの本番サービス開始の度重なる延期

- 2015年6月、自前ルートCA(ISRG X1)構築と2015年9月サービス開始告知
- 2015年8月、サービス開始を2015年11月に延期
- 2016年4月、ベータテスト終了と本番サービス開始告知

結局 2015年9月予定→2016年4月実施
Let's Encryptのアナウンスは過去も当てにならなかった(笑)

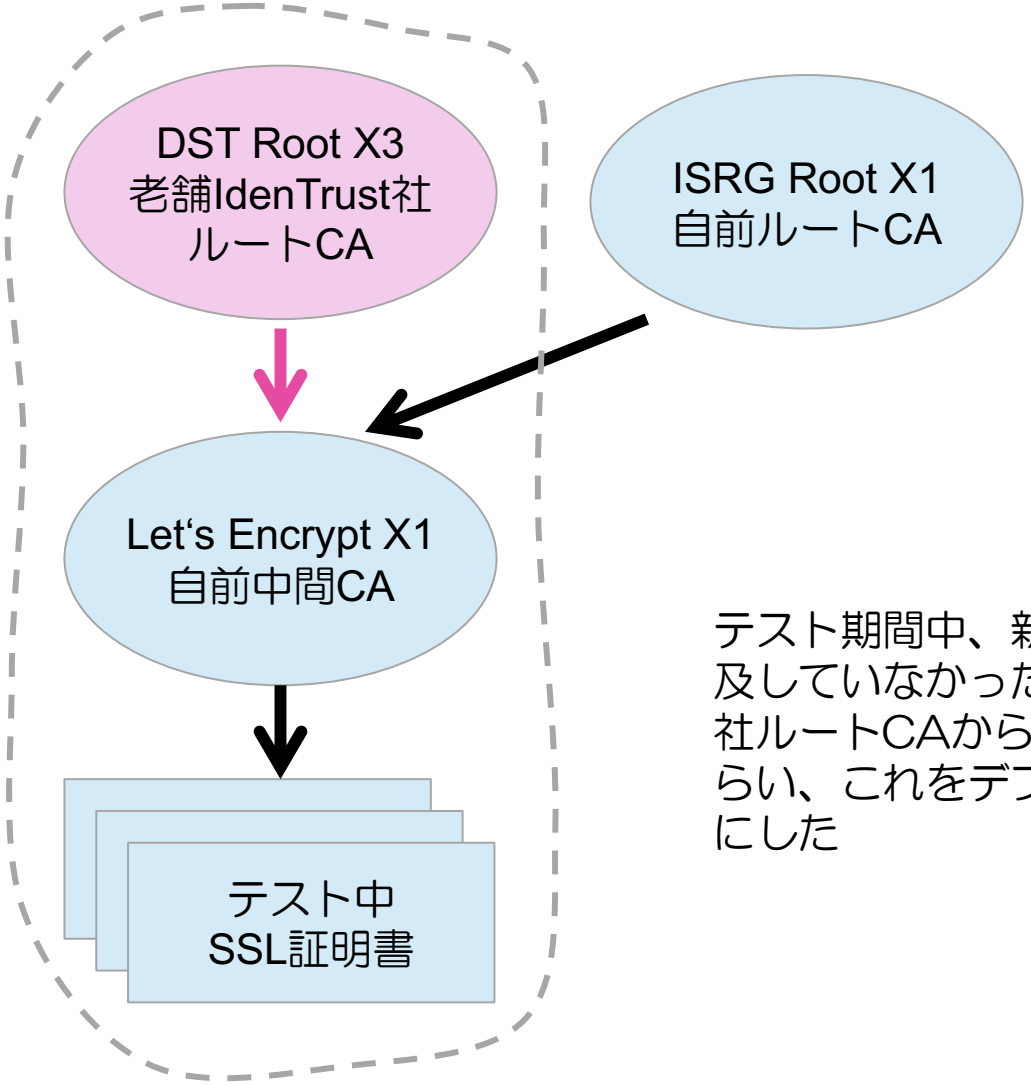
Let's Encrypt証明書チェーンの推移(1/1)
2015年6月~8月 ルート中間構築、ベータテスト中

- テスト開始時点では、自前のルートCAがブラウザ/OSに搭載されてない



Let's Encrypt証明書チェーンの推移(2/1)
2015年8月～2016年4月 ベータテスト２

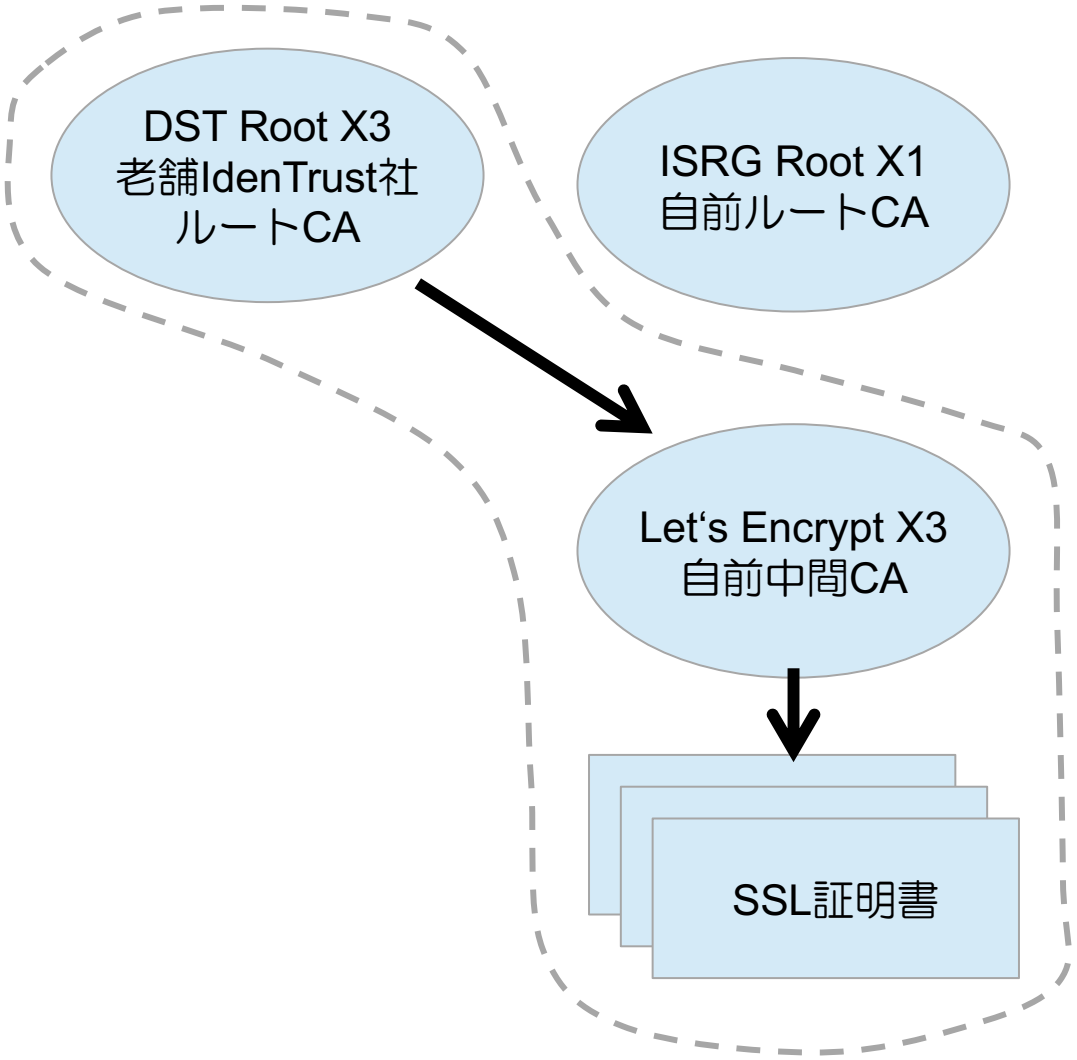
- 自前ルートは普及してないので老舗のIdenTrust社のルートから追加発行



テスト期間中、新しい自前ルートCAはまだ普及していなかったため、老舗CAのIdenTrust社ルートCAから中間CAに証明書を発行してもらい、これをデフォルトのチェーンとすることにした

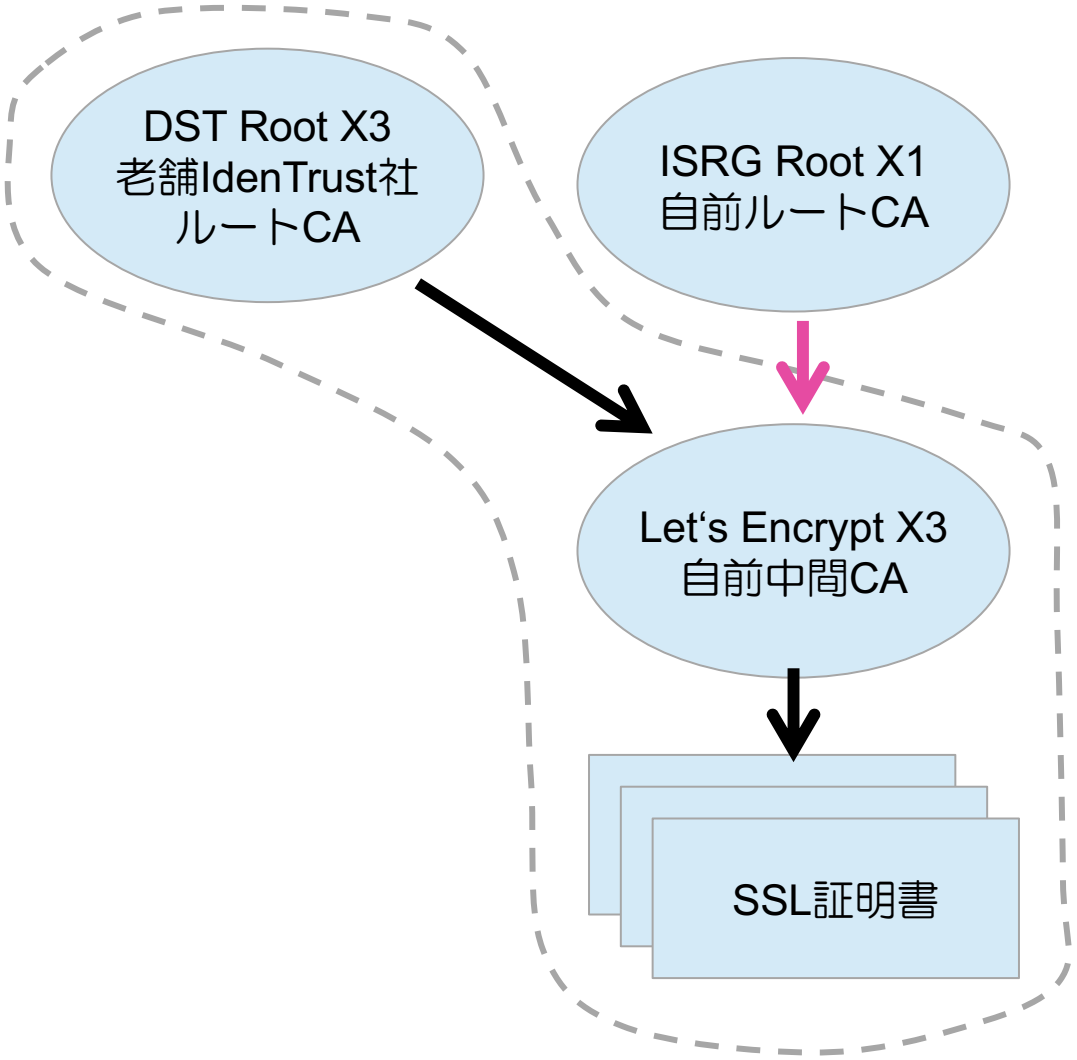
Let's Encrypt証明書チェーンの推移(3/1)
2016年4月～ サービス正式開始

- 本番中間CAの運用開始、最初はIdenTrustからののみ



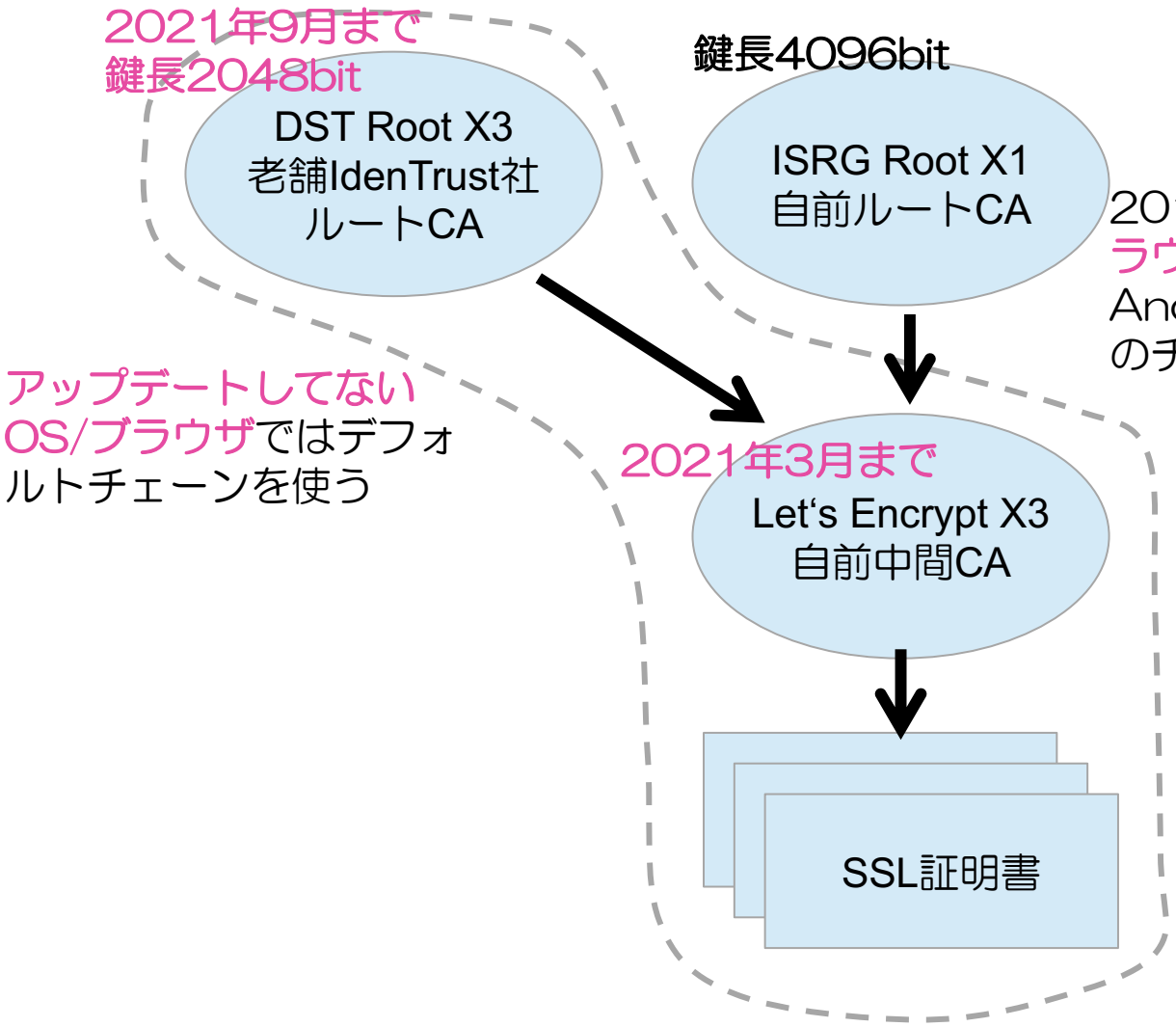
Let's Encrypt証明書チェーンの推移(3/1)
2016年10月～ 後追いで自前ルートからも発行

- デフォルトのチェーンはIdenTrust社のまま



Let's Encrypt証明書チェーンの推移(3/1)
2016年8月～2018年8月 自前ルートの普及

- 2018年8月には、主要すべての最新ブラウザ/OSで自前ルートが搭載された

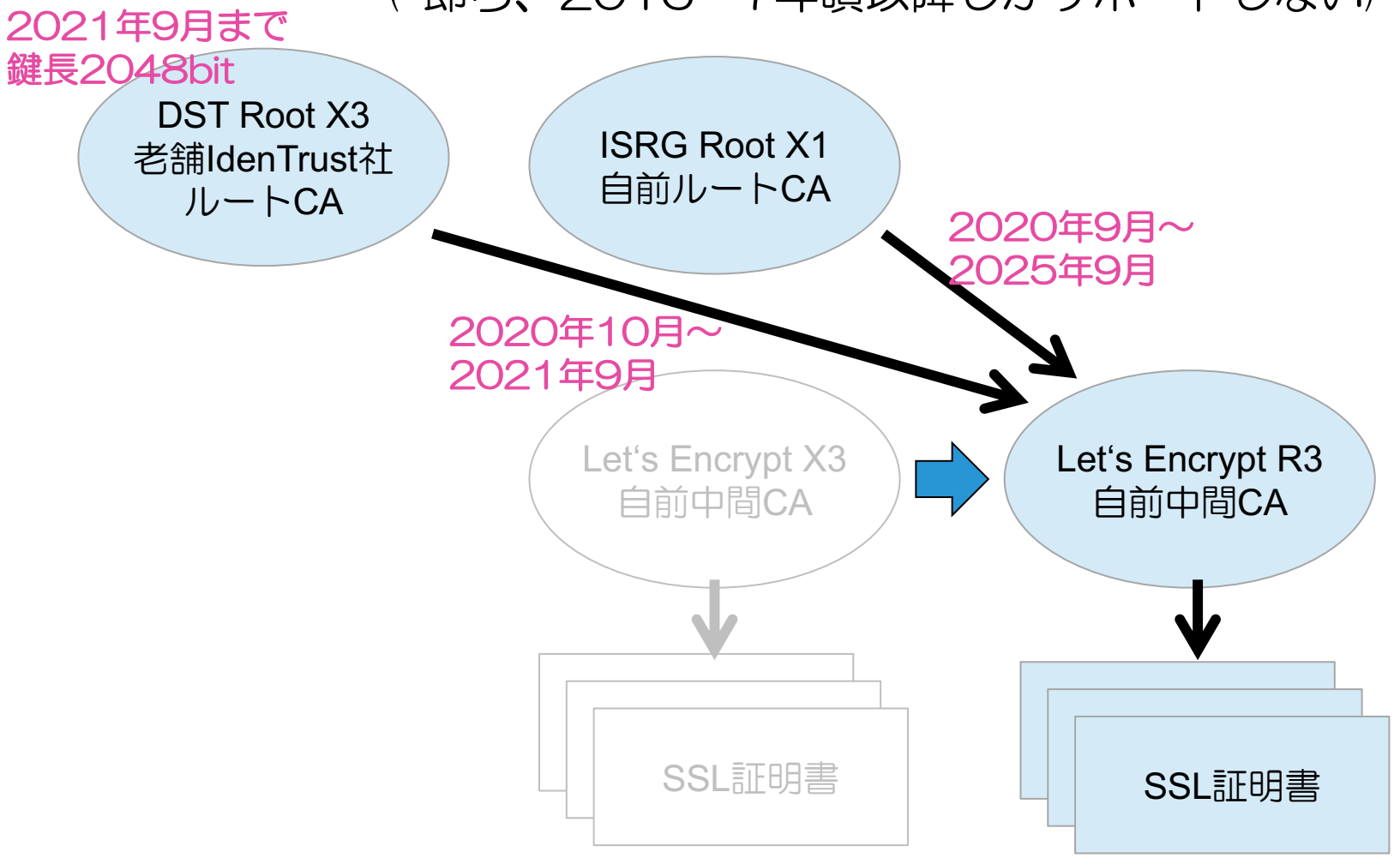


自前ルートも普及したし、IdenTrustルート、自前中間X3も有効期限が近づいてきたので移行計画を立てる必要がある

Let's Encrypt証明書チェーンの推移(1/1)

(案) 2020年10月からの移行案

- 古いブラウザ/OSは2021年9月までしかサポートしないと発表
  (=即ち、2016~7年頃以降しかサポートしない)



ISRG Root X1を搭載するブラウザ/OS

- 概ね2016-2017年以降リリースされたブラウザ/OSならばISRG Root X1を搭載
- 即ち2021年9月以降でも問題なくLet's EncryptのSSLサーバー証明書を使ったサイトを閲覧できる

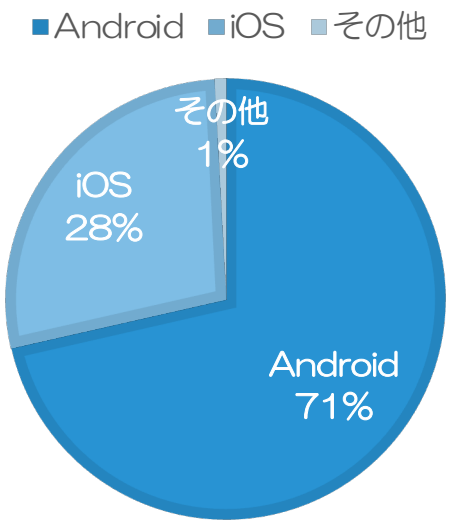
- Windows：　XP SP3以降 (=2008年4月以降)
- macOS：　10.12.1 Sierra以降 (=2016年9月以降)
- iOS：　iOS 10以降 (=
- iPhone：　iPhone4より後 (iPhone4はソフト更新不能)
- Android：　7.1.1以降 (=2016年10月以降)
- Mozilla Firefox：50.0以降 (=2016年11月以降)
- Ubuntu：　Xenial 16.04LTS以降 (2016年4月以降)
- Java8：　8u141以降 (=2017年6月以降)
- Java7：　7u151以降 (=2017年6月以降)
- NSS：　3.26以降 (=2016年8月以降)

Android関係者、利用者から大きなクレームがあった

Let's Encryptの当初ルートチェーン変更案のAndroidへの影響

- 当初の移行案では2021年9月以降、33.8%のAndroid端末(=全スマホの23%)でLet's Encrypt証明書のサイトが閲覧できなくなる (Android製品はOSアップデートがし辛い)

世界スマホ/タブレットOSシェア(2021年5月)



データ元：statcounter GlobalStats gs.statcounter.com

Android Platform/API Version Distribution

ANDROID PLATFORM VERSION	API LEVEL	CUMULATIVE DISTRIBUTION
4.0 Ice Cream Sandwich	15	
4.1 Jelly Bean	16	99.8%
4.2 Jelly Bean	17	99.2%
4.3 Jelly Bean	18	98.4%
4.4 KitKat	19	98.1%
5.0 Lollipop	21	94.1%
5.1 Lollipop	22	92.3%
6.0 Marshmallow	23	84.9%
7.0 Nougat	24	73.7%
7.1 Nougat	25	66.2%
8.0 Oreo	26	60.8%
8.1 Oreo	27	53.5%
9.0 Pie	28	39.5%
10. Android 10	29	8.2%

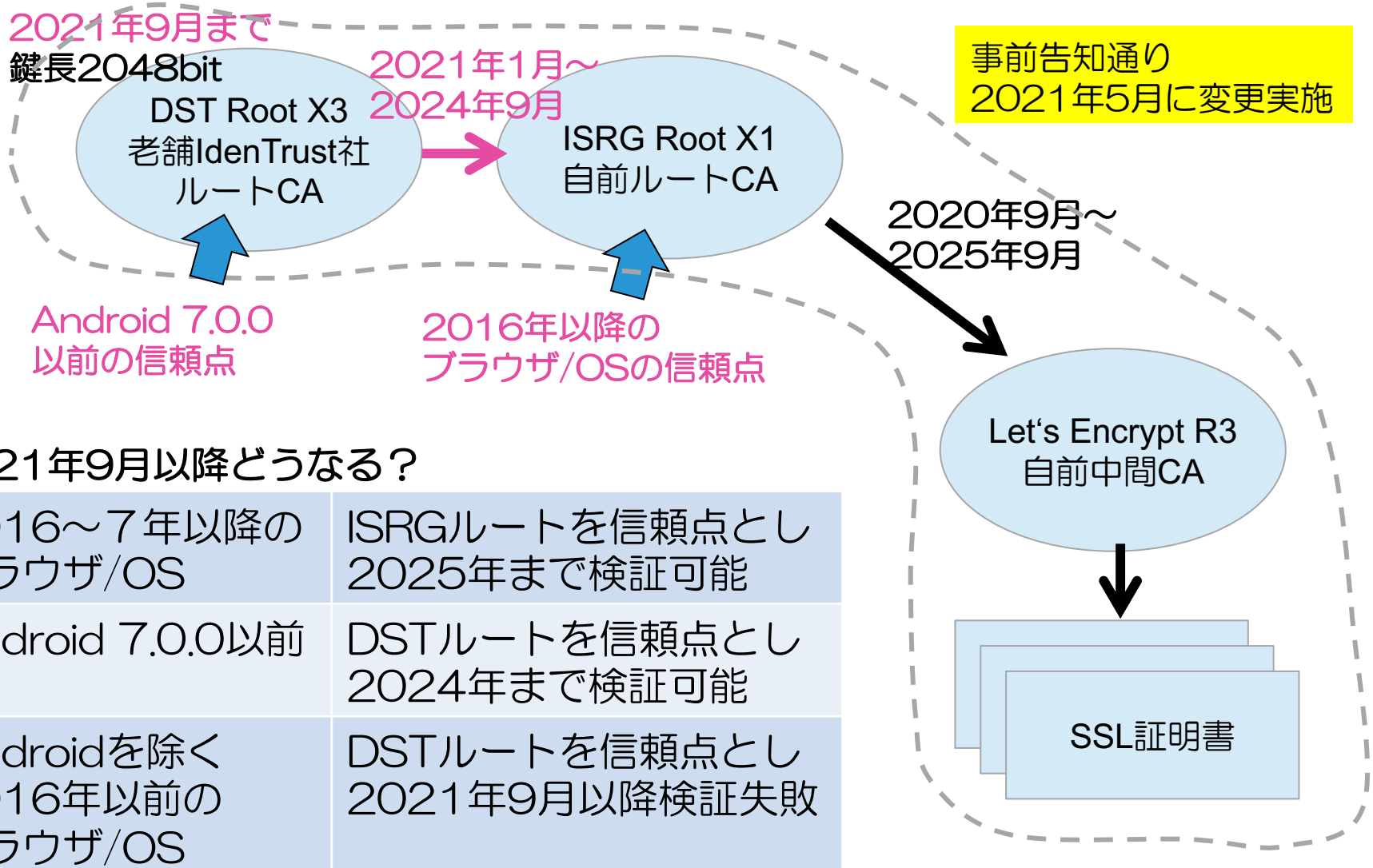
Android Studioのダイアログより

2.3.6～7.0.0まで33.8%の端末が2021年9月以降、LE証明書サイトを見れない

7.1.1～最新は、2021年9月以降もLE証明書サイトを見れる

Let's Encrypt証明書チェーンの推移(1/1)
(案) 2020年12月発表の古いAndroidのみの救済案

- 退役予定のIdenTrustルートからISRG Rootへ期限超えの証明書を発行



2021年9月以降どうなる？

2016～7年以降のブラウザ/OS	ISRGルートを信頼点とし2025年まで検証可能
Android 7.0.0以前	DSTルートを信頼点とし2024年まで検証可能
Androidを除く2016年以前のブラウザ/OS	DSTルートを信頼点とし2021年9月以降検証失敗

なぜ、古いAndroidは大丈夫で
他の古いブラウザ/OSはダメなのか？

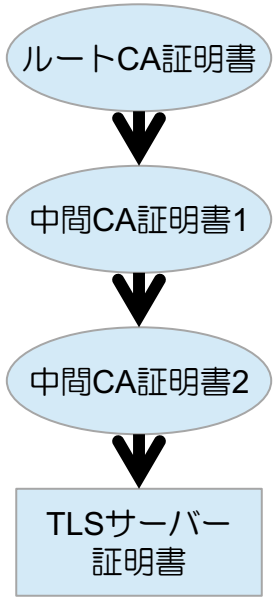
(参考)SSL/TLSのハンドシェイクで送られくる証明書チェーン

- certificate_listフィールドによりサーバーを検証するための証明書チェーンが、サーバーから送られ、クライアントはこれを検証する
- TLSのバージョンにより少し違う

TLS 1.2以前

- サーバー証明書は先頭で、順に認証の連鎖になるよう
- ルートは入れなくても可
- 実際には多くのクライアント今回のLEのような世代交代用の中間CA群が入ってても処理できる

配列[3]	ルートCA (オプション)
配列[2]	中間CA1
配列[1]	中間CA2
配列[0]	サーバー証明書



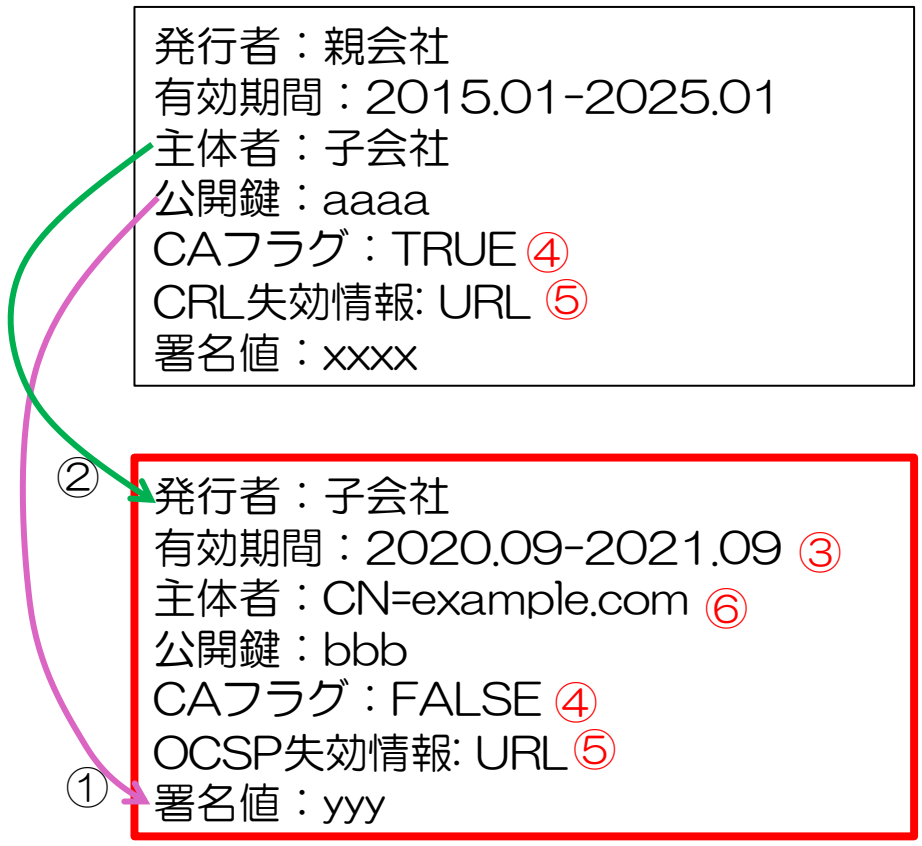
TLS 1.3

- サーバー証明書は先頭
- その他は順序は任意で、世代交代用の中間CA群等、検証に必要な(余分な)証明書も入れて良い
- でも順序は後方互換性に配慮
- ルートについて書いてない

配列[3]	ルートCA (記載なし)
配列[2]	中間CA2
配列[1]	中間CA1
配列[0]	サーバー証明書

証明書の構造と証明書チェーンの検証(1/2) ルート

- RFC 5280 6章に検証アルゴリズム例が記載(=結果が同じなら良い)



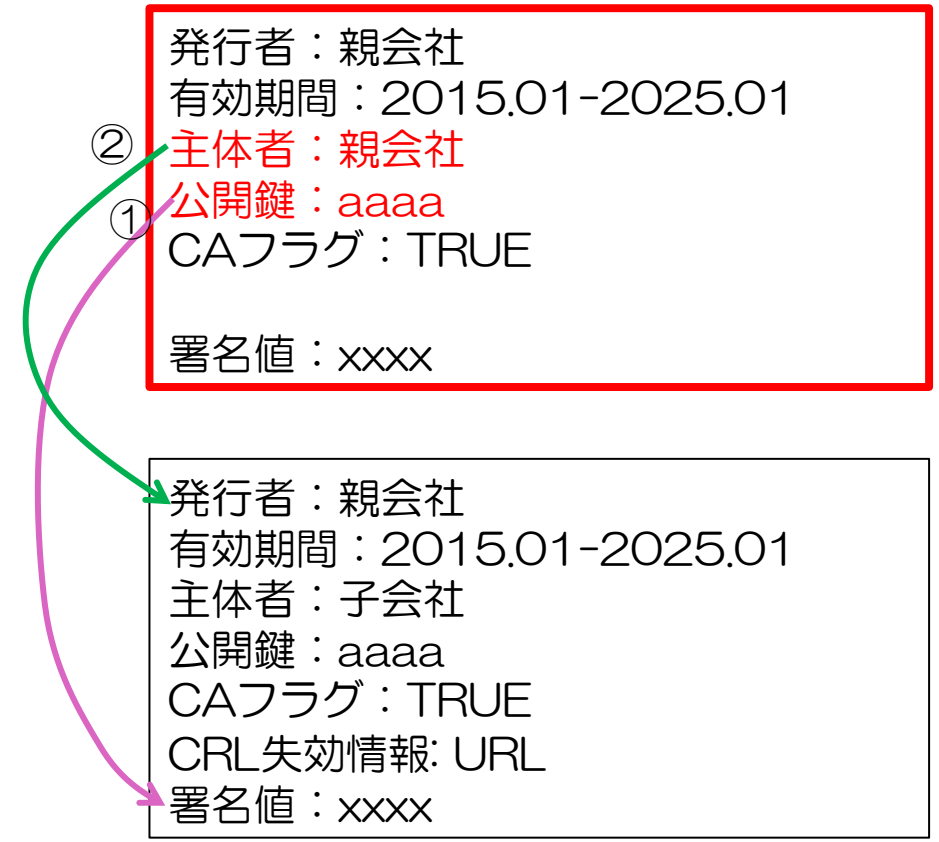
主な確認項目（他にもあるけど）

① 署名の連鎖
② 名前の連鎖
③ 有効期間内か?
④ 基本制約(CA用か?)
⑤ 失効検証(失効申請されてないか?)
⑥ アプリ用途毎の検証
  - TLSサーバー証明書用
  - S/MIME証明書用など

証明書の構造と証明書チェーンの検証(2/2) ルート証明書の扱い

- RFC 5280 6章の定義では、(実際にルート証明書の形で保持してたとしても)公開鍵と主体者名しか検証では使わないことになっている
- つまり、(仕様上は)ルート証明書の有効期間や拡張領域は見なくていい

信頼点(=トラストアンカ)、一般にはルート証明書

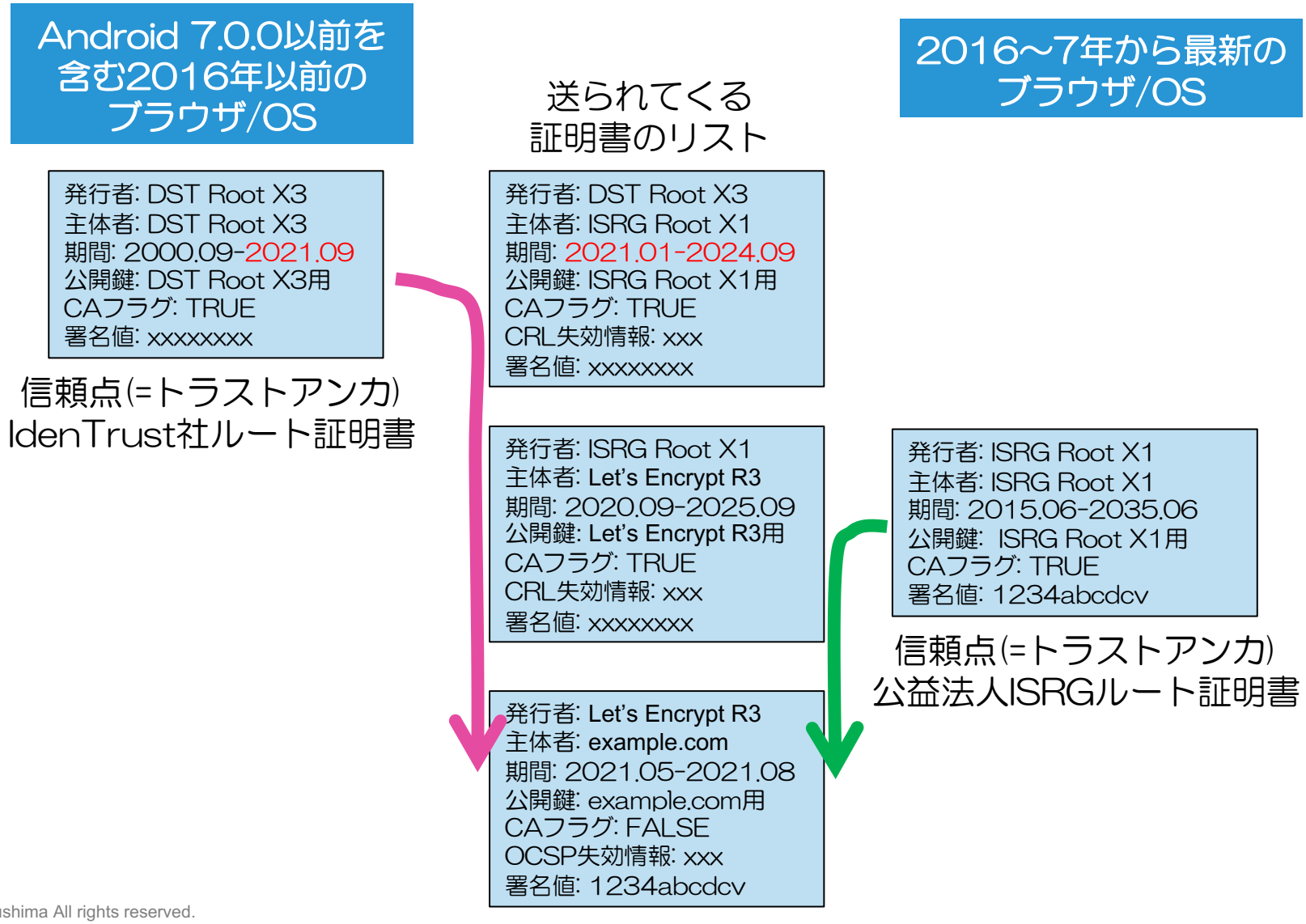


主な確認項目（他にもあるけど）

① 署名の連鎖
② 名前の連鎖
③ 有効期間内か?
④ 基本制約(CA用か?)
⑤ 失効検証(失効申請されてないか?)
⑥ アプリ用途毎の検証
  - TLSサーバー証明書用
  - S/MIME証明書用など

certbotコマンドで2021年5月以降、設定された証明書チェーン

- certbotで設定したウェブサーバーの返すcertificate_listフィールドのチェーン
- DST Root X3ルート証明書は送らずクライアントに入っているものを使う



2016年以前のOS/ブラウザでAndroid7.1.1以前と他の違い

- Android(2.3.6-7.0.0)は標準通り、信頼点は公開鍵と主体者名しか使わない
- 他のOS/ブラウザはすべて有効期間、拡張領域などをチェックする

信頼点(=トラストアンカ)、一般にはルート証明書

発行者：DST Root X3
有効期間：2000.09-2021.09
② 主体者：DST Root X3
① 公開鍵：aaaa
CAフラグ：TRUE

署名値：xxxx

Androidのみこれを無視するから9月以降も動く

発行者：DST Root X3
有効期間：2021.01-2024.09
主体者：ISRG Root X1
公開鍵：aaaa
CAフラグ：TRUE
CRL失効情報: URL
署名値：xxxx

主な確認項目（他にもあるけど）

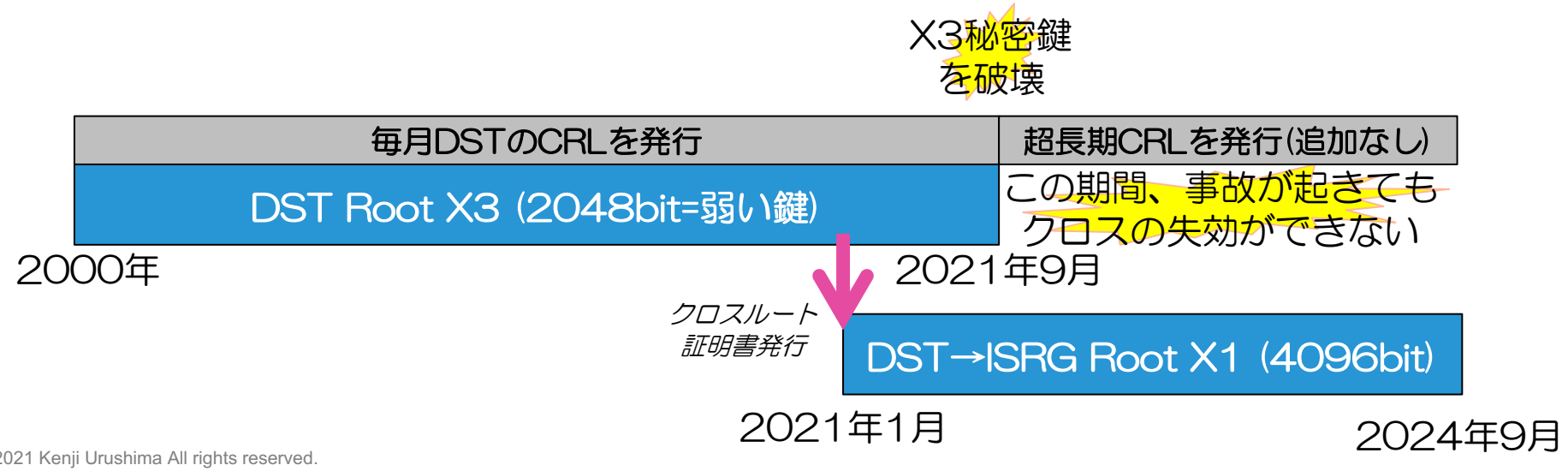
① 署名の連鎖
② 名前の連鎖
③ 有効期間内か?
④ 基本制約(CA用か?)
⑤ 失効検証(失効申請されてないか?)
⑥ アプリ用途毎の検証
- TLSサーバー証明書用
- S/MIME証明書用など

LEはブログで、「Androidは信頼点として公開鍵と名前しか格納してないので大丈夫」と説明したが、ルート証明書を格納しているのでそれはウソ

認証局の運用として
問題はないのか？

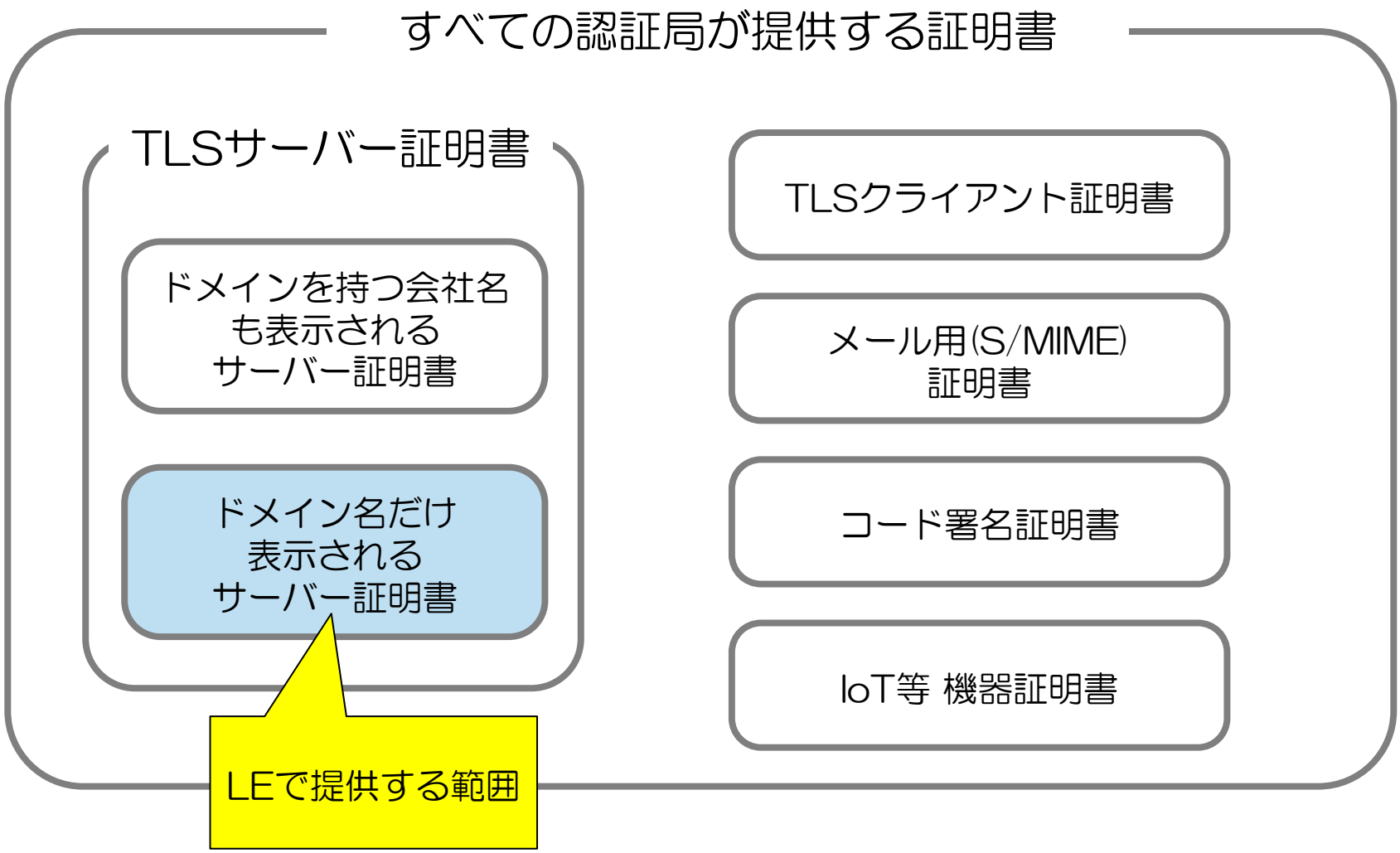
2021年9月以降何が起こるか？

- 通常はDST Root X3の子孫証明書の有効期限は9月を超えさせない
- 通常はルートは有効期限終了後、「ルートを不正使用されないよう」直ちに秘密鍵を破壊する
- 2021年9月まではDST X3は1ヶ月おきにCRLを発行していたが、それができなくなり、鍵破壊をするなら、9月期限切れ前に「超長期(2021.09-2024.09)」CRLを発行するだろう
- 9月以降、事故が起きた時に子孫を無効化できないリスクを負う
- そのような、リスクのあるクロスルートの発行、鍵破壊、CRL発行について、DSTとISRGのCA監査を共通にしている「Schellman & Company」が「問題無い」言ったとLEは言っている。CABF BR、各ルートプログラム的に問題なかったか？



LEさえあれば他の認証局はいらないの？

- LEの提供する証明書はドメイン名しか記載されないTLSサーバー証明書のみ
- 他の証明書は発行が自動化できないので有料になり他の認証局が必要



いろいろ問題はあったが

- かなりユーザの残っていた古いAndroid(2.3.6-7.0.0)を救ったのは大きい
- 「Let's Encryptにまかせておけば、何とか多くのユーザを救ってくれる」というのを再認識
- 認証局として(監査上、リスク上問題ないのか?)は若干疑問

ご清聴ありがとうございました

参考リンク

- Qiita: Let's Encryptのルート認証局移行についてちょっと調べてみた (2021.05.08)
  https://qiita.com/kjur/items/2fd72b6707497c7fc6c5
- Let’s Encryptブログ
  https://letsencrypt.org/blog/
- LEの証明書チェーン変更の詳細アナウンス
  https://community.letsencrypt.org/t/production-chain-changes/150739
- RFC 5280 6章 認証パス検証(証明書の検証方法)
  https://datatracker.ietf.org/doc/html/rfc5280#section-6
- IdenTrust社 (ISRGルートと相互認証した老舗PKI企業)
  https://www.identrust.com/
- CA Browser Forum Baseline Requirements
  https://cabforum.org/baseline-requirements-documents/
- Android Studio (Androidアプリ統合開発環境、Androidのバージョン毎の普及率の閲覧)
  https://developer.android.com/studio

- engadget: Android 7.1以前の証明書問題が解決。向こう3年間はひきつづき安全なウェブ閲覧が可能に (2020.12.23)
  https://japanese.engadget.com/android-lets-encrypt-101047429.html
- ZDnet: 旧版Androidのルート証明書問題を回避-3年間のクロス署名の発行に合意 (2020.12.24)
- https://japan.zdnet.com/article/35164339/

- 講師ブログ：自堕落な技術者の日記
  http://blog.livedoor.jp/k_urushima/
- 講師ツイッター
  https://twitter.com/kjur
- 講師作OSS ”jsrsasign” JavaScript実装PKI/暗号ライブラリ
  https://github.com/kjur/jsrsasign