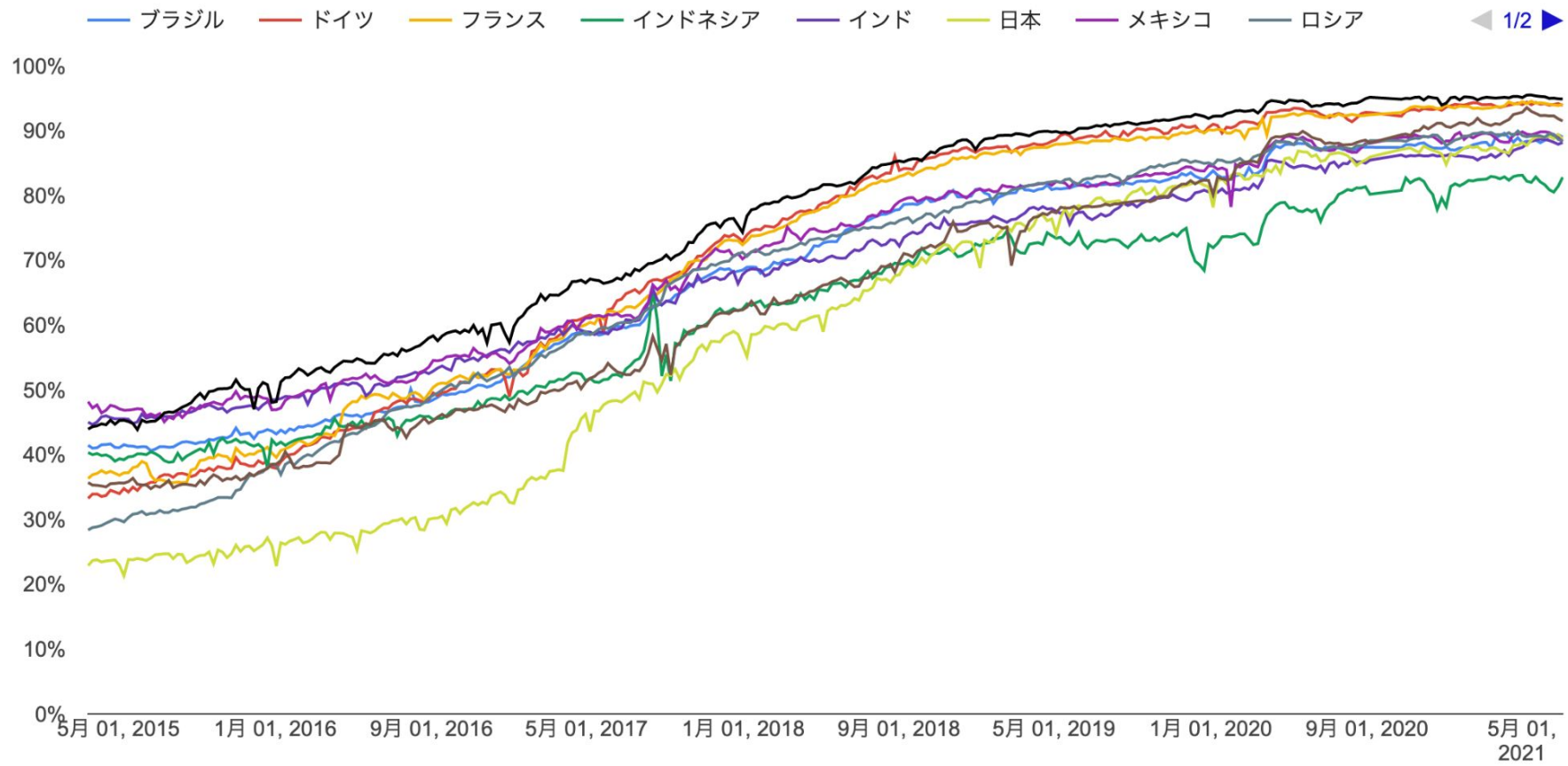
UPKI電子証明書発行サービスについて

NII 学術情報基盤 オープンフォーラム 2021

2021年7月8日 認証トラック1

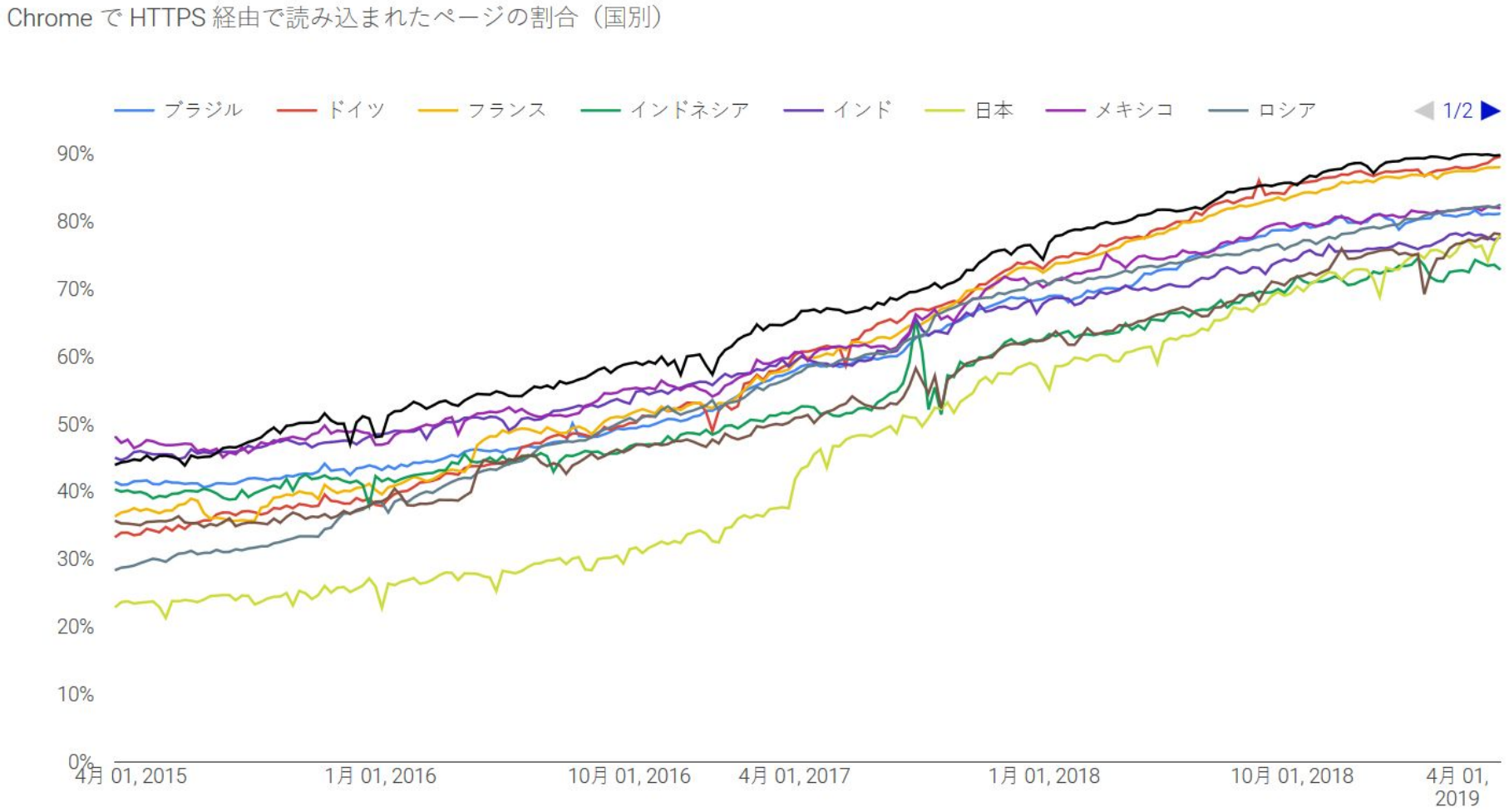
HTTPS経由で読み込まれたページの割合（2021年）

Chrome で HTTPS 経由で読み込まれたページの割合（国 / 地域別）



Google, 2021,「ウェブ上でのHTTPS暗号化」, Google 透明性レポート,（2021年7月6日取得, https://transparencyreport.google.com/https/overview?hl=ja

HTTPS経由で読み込まれたページの割合（2019年）



Google, 2019,「ウェブ上でのHTTPS暗号化」, Google 透明性レポート,（2019年5月23日取得, https://transparencyreport.google.com/https/overview?hl=ja

サーバ証明書中間認証局切り替え

中間認証局の切り替えについて

- UPKIの証明書を各機関に継続して利用いただくために、下記の対応を実施しました
  - 1. UPKI電子証明書発行サービスの証明書を発行する中間認証局を、外部監査を受けたものに切り替えました
  - 2. サービス利用機関には、現在有効なサーバ証明書とクライアント証明書を監査を受けた中間認証局から再発行し、置き換えを実施いただきました
    - サーバ証明書の置き換え作業期間は当初予定より短縮し、期限を2021年4月26日（中間認証局失効は27日）としました

- UPKI の旧中間CA証明書は失効されまました
  - RSA: NII Open Domain CA - G5
  - ECDSA: NII Open Domain CA - G6
- Chrome（Chromium Base含む）、Firefox、Appleの失効リストにも掲載済です

プラットフォームごとの旧中間CA失効判定

- ルート認証局での中間CA証明書失効とCRL掲載
  - 4月27日午前
    - NII Open Domain CA - G5　2021-04-27　10:38(JST)
    - NII Open Domain CA - G6　2021-04-27　11:23(JST)
- Chrome(他のChromium base 含む)
  - CRLSet/Blacklist → 4月28日頃より掲載、Chromiumベースのブラウザで失効と判定
- Internet Explorer
  - 中間CAの状態をCRLでチェックする
  - 4月27日から失効と判定
- Mozilla
  - 6月14日にOneCRL掲載
- Apple
  - 4月28日 失効リストに掲載

CA/B Forum BR対応の経緯

- セコムトラストシステムズから、UPKIの中間認証局は、CA/Browser Forum Baseline Requirements 準拠のために以下の2つのうちいずれかの対応をとる必要があるとの指摘がありました
  - 1. 新しい中間認証局を作成し、BRに定められた、準拠性の監査（WebTrust監査といいます）を受ける
  - 2. 技術的に、発行対象の制限を行う
- これを受け、両案の検討を行いました
  - 後者(2)の発行対象制限を行うと、中間CA証明書の容量が肥大化し、下記に例示するような不具合が生じることがわかりました
    - Internet explorer 利用時、サーバ証明書をインストールしたサイトでエラーが表示される（検証に失敗する）
    - 一部OSの証明書ビューアで中間CA証明書を開いたとき、証明書ビューアがハングアップする。
  - 回避する手段はありませんでした。
  - そのため、新しい中間認証局を構築し、年次でWebTrust監査を受けることとしました

移行期間短縮の経緯 1

- UPKIの認証局を運用するセコムトラストシステムズより、下記の通り連絡ありました
  - ブラウザベンダーからセコムトラストシステムズにインシデントに伴う是正のための指摘が入った
  - UPKI含む複数の中間CAで、サーバ証明書を発行する認証局の切り替えに早急に対応しなければならない
  - 最短で1週間以内に旧中間認証局の失効を求められる可能性がある
- インシデントについて（Bugzillaに起票）
  - UPKIとルート認証局を同じくする他の組織の中間認証局のインシデントです
    - スライド3で言う発行対象を制限した中間CAに移行中、SANsにドメイン名が付与されていない値が記された証明書を発行した
    - この調査の過程で中間CAについても精査され、外部監査を受けていないものであることがBugzillaで報告された
  - UPKI のインシデントではありません

移行期間短縮の経緯 2

- セコムトラストシステムズにて、当初の切り替え計画を維持できるようブラウザベンダーに対し理解を求める活動を進めていました
- この交渉の中で、この中で、ルート認証局としての健全性を保つうえでは、やはり旧中間認証局の失効をすみやかに実施する必要があるとの結論に至りました
- セコムトラストシステムズから、国立情報学研究所に旧中間認証局の失効を行いたいとの要請があり、協議のうえ、4月27日に失効を行うことになりました

当初予定より1ヶ月ほど前倒しの中間CA失効となりましたが、総数2万枚近くのサーバ証明書移行作業にご協力いただき、御礼申し上げます。

クライアント証明書認証局
切り替えについて

Mozilla Root Store Policy対応 1

- 中間認証局置き換えについて
  - パブリックなクライアント証明書を発行する認証局は、Mozilla Root Store Policy に準拠しなければなりません
  - クライアント証明書でも、サーバ証明書と同様の対応をとる必要がありますが、やはり監査を受ける以外の対処は不可能でした
  - たとえば下記のような不具合が生じます
    - クライアント証明書を用いた認証（Webサイトやeduroam）が動作しなくなる
  - そのため、外部監査を受けた中間認証局への切り替えが必要です

Mozilla Root Store Policy対応 2

- 必要な対応
  - 旧中間認証局から発行済みの全クライアント証明書を、セコムトラストシステムズが提供する認証局から発行したクライアント証明書に置き換えてください
  - 移行期間は、これまでもお伝えしておりました通り2020年12月25日～2021年12月までの12ヶ月間です

Mozilla Root Store Policy 改訂（2021年5月1日）への対応 1

- Mozilla Root Store Policy が2021年5月1日に改訂され、従来以上に認証局の管理の厳正化がなされました
  - Mozillaによって、セコムトラストシステムズ含む複数社の中間CAに対し是正の指摘がありました
  - 本サービスの旧クライアント証明書中間CAも対象に含まれます

Mozilla Root Store Policy 改訂（2021年5月1日）への対応 2

- 本件では、末端のクライアント証明書移行の前倒しは実施しない見込です
  - ただし、Mozillaの是正指摘への対応のため、旧中間CA証明書を同鍵ペアで、また一部パラメータを変更して更新発行いたします
  - 認証などの用途でクライアント証明書をご利用中の場合、この更新発行した中間CA証明書をシステムにインストールしてください
- 移行の期間（2021年12月まで）を延長するものではありません
  - 引き続き、新中間CAから発行したクライアント証明書への移行をお願い申し上げます

タイムスケジュール

- 対象：2020年12月24日までクライアント証明書を発行していた中間CA
  - NII Open Domain CA - G4
  - NII Open Domain S/MIME CA
- 2021年7月（15日頃予定）
  - 同鍵ペアで、EKU:Extended Key Usageを付与した中間CA証明書（更新版）を発行し、リポジトリで公開（UPKI作業）
- 2021年8月27日まで
  - 利用機関の認証サーバ等で使用する中間CA証明書を現行版から更新版に切り替え、テスト等を実施する（利用機関作業）
- 2021年8月31日まで
  - 中間CA証明書現行版を失効（UPKI作業）
- 2021年12月まで
  - クライアント証明書の移行を完了（利用機関・利用者作業）
- 2022年1月
  - 中間CA証明書更新版を失効（UPKI作業）

S/MIME証明書切り替えに関する注意事項

S/MIME証明書移行時の注意

- S/MIME証明書は、歴代で使用したものを利用者各自で保管しておいてください
  - 有効期限切れ・失効したものは署名には使えませんが、暗号化メールの復号に必要です
- 新しいS/MIME証明書を取得したら、署名用の証明書を早期に新しいものに切り替えてください
- メーラーによって動作が異なりますが、署名検証エラーになる場合があります
  - 受信側がThunderbirdの例
    - 送信側が、ある週の金曜日にS/MIME署名メールを送信
    - 翌日 土曜日に送信側のS/MIME証明書の有効期間満了
    - 受信側が翌週 月曜日に当該メールを検証すると署名検証エラー（有効期限切れ）

S/MIME 復号エラー

- S/MIME証明書をインストールしていないPC/メーラーでは、暗号化メールを復号できません

S/MIME証明書プロファイル選定時の注意事項―Gmail

- S/MIME証明書は、現在下記3プロファイルで提供しています
  - 7:S/MIME証明書（sha256WithRSAEncryption）（証明書有効期間:52ヶ月）
  - 15:S/MIME証明書（sha256WithRSAEncryption）（証明書有効期間:13ヶ月）
  - 16:S/MIME証明書（sha256WithRSAEncryption）（証明書有効期間:25ヶ月）
- Gmail では有効期間27ヶ月を超えるS/MIME証明書の署名検証でエラーが表示されます
  - Google Workspaceでの証明書ルールによるものです
  - 「証明書は信頼されていません。」と表示
  - これを回避するには、プロファイル15または16を指定してください

お知らせ

Authority information Access について

- 現在発行されているサーバ証明書には、Authority information Access に CA Issuersとして、中間CA証明書が指定されています
  - この証明書をサーバにインストールしていると、たとえ誤った中間CA証明書をインストールしていた場合、そもそも中間CA証明書をインストールしていない場合でも、クライアント側のアクセス時、ブラウザが自動で正しい中間CA証明書を取得し、証明書検証を行います
    - ブラウザの実装に依存し、例えばFirefoxでは利用できない機能です
- ただし、これが機能するのはサポートしたブラウザのみです
  - 稼働監視を設定している場合、アクセス不能としてアラートが出る場合があります
  - たとえばGCPのMonitoringからはアクセス不能として扱われます

機関所在地とドメイン所有権の確認

- 利用機関の**所在地**確認を特定記録郵便にて実施（書類の到達と返送）

- 対象ドメインの**所有権**確認を、WhoisDB記載の連絡先メールアドレスを対象に実施（メール到達と返信）
  - WhoisDBのメンテナンスをお願い申し上げます

- これらには有効期間があります
  - 2021年8月～9月頃より順次再度の確認を実施いたします
  - 機関によって実施日は異なります

おわりに

- ご連絡・お問い合わせ先
  - 国立情報学研究所　学術基盤課総括・連携基盤チーム（認証担当）
    - お問い合わせフォーム：　https://certs.nii.ac.jp/contact/form
  - 原則，サービス利用機関または利用予定機関の機関責任者・登録担当者・経理担当者からお願いします