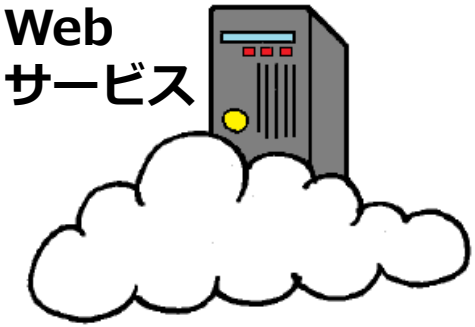
ユーザ

認証局

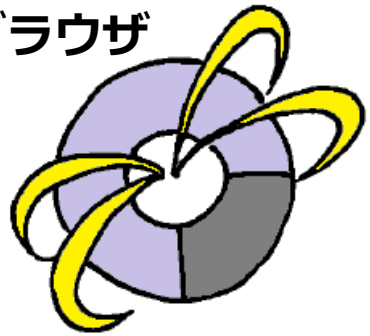
TLSとWebブラウザの表示のいまとこれから
～URLバーの表示はどうなるのか～

2019/5/31
NTTセキュアプラットフォーム研究所
奥田 哲矢



Web
サービス

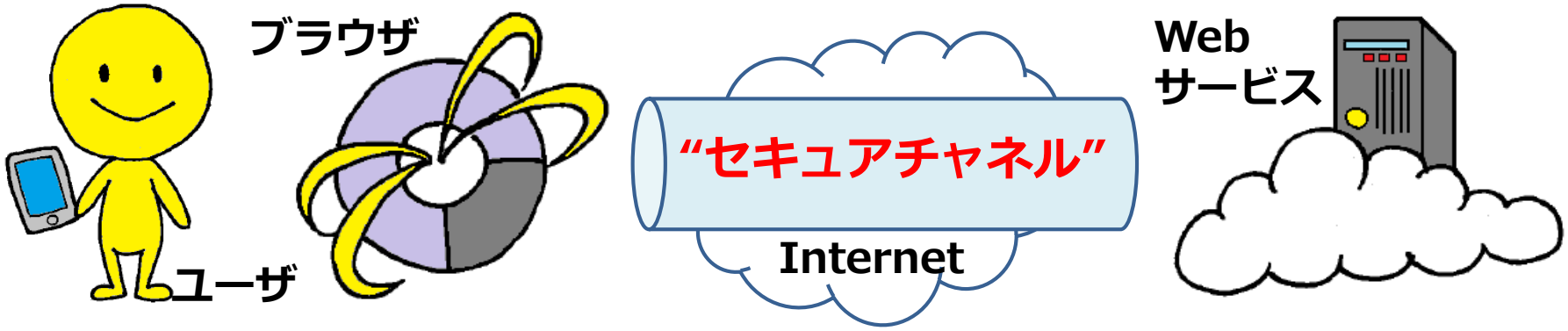
ブラウザ



はじめに

SSL/TLSとは？

→相手の顔が見えないインターネット上で安全な通信を実現する仕組み



- SSL/TLSの目的は、2者間通信に ”セキュアチャネル” を提供すること
- ”セキュアチャネル” は下記機能を提供する。
  - エンドポイント認証：サーバ認証は必須、クライアント認証は任意
    （※サーバの運営元の信頼性は必ずしも保証されない → 詳細は本編で）
  - データ機密性：通信内容をエンドポイント間で秘匿
  - データ完全性：攻撃者による通信内容の改ざんの検知

本編に入る前に

今年のSSL/TLS分野の話題といえば・・・

ＴＳＨＲ

皆さん、もちろんキャッチアップ出来てますよね？

（答えは次ページで）

本編に入る前に

Taisho
Showa
Heisei
Reiwa

New!!

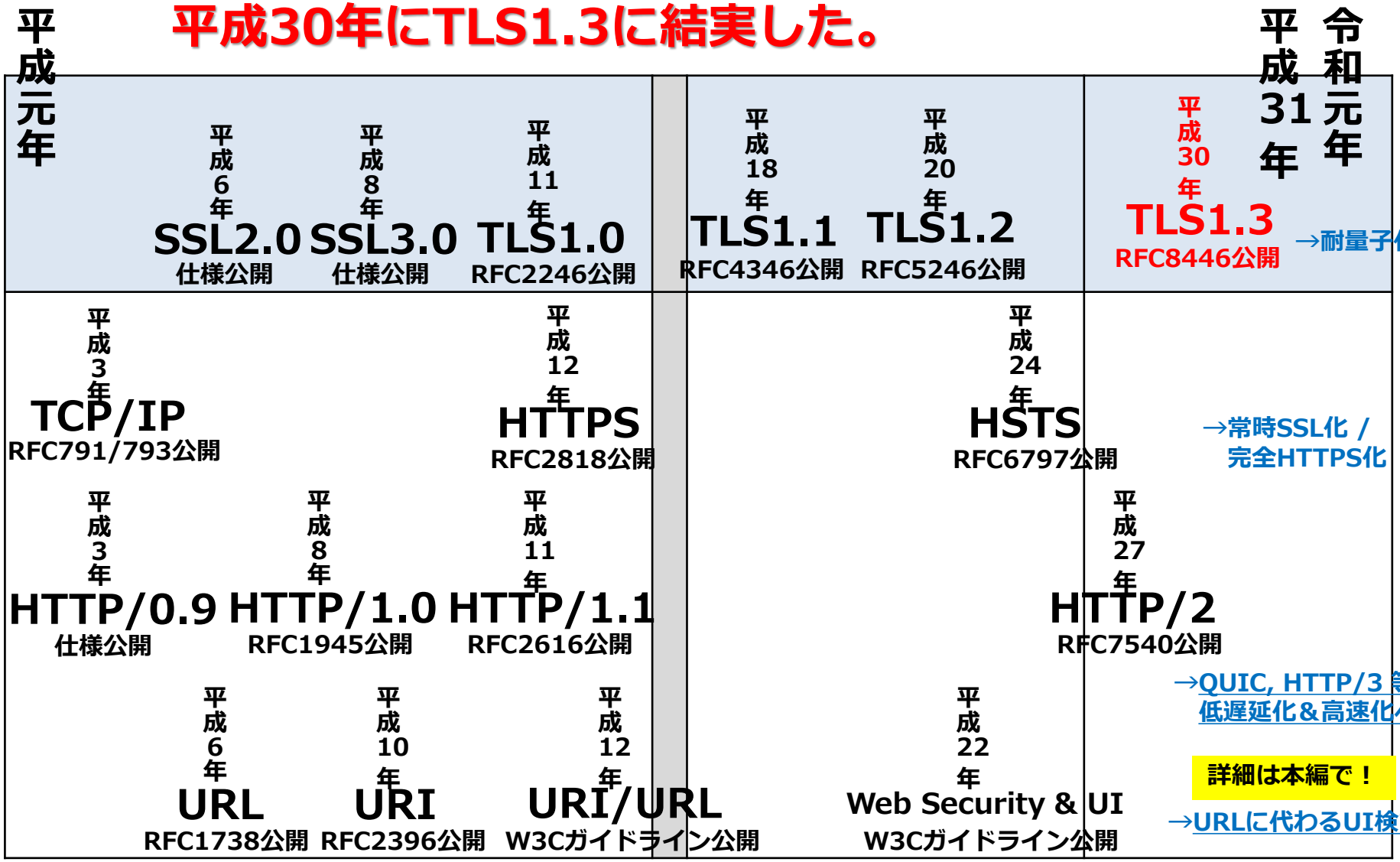
本編に入る前に

IWSC事務局の方から、
「TLS1.3時代の新常識（2018.11.27 大津様）」の内容を一部盛り込むようリクエスト頂きましたので、

本編に入る前に、
「あえて平成年号で振り返るTLSの30年」と題して、お話しさせて頂きます。

あえて平成年号で振り返るTLSの30年

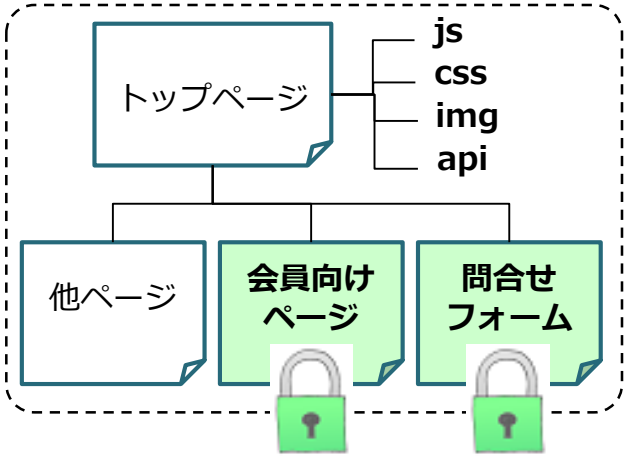
→TLSの歴史は平成に始まり、平成30年にTLS1.3に結実した。



あえて平成年号で振り返るTLSの30年

①誕生と成長の時代

・SSL/TLSの誕生と成長
平成3年：TCP/IP RFC公開、HTTP/0.9 仕様公開
平成6-8年：SSL2.0, SSL3.0, Netscape社により実装＆普及
平成9-11年：TLS1.0, IETFで仕様が標準化される
（Netscape社＆Microsoft社の取組みを反映）
平成12年：HTTPS, IETFで仕様が標準化される



・会員向けページや問合せフォームなど、限定的にSSL/TLSが利用されていた。
・SSL/TLSのバージョンは、大手ベンダの提供するデファクトが使われていた。

あえて平成年号で振り返るTLSの30年

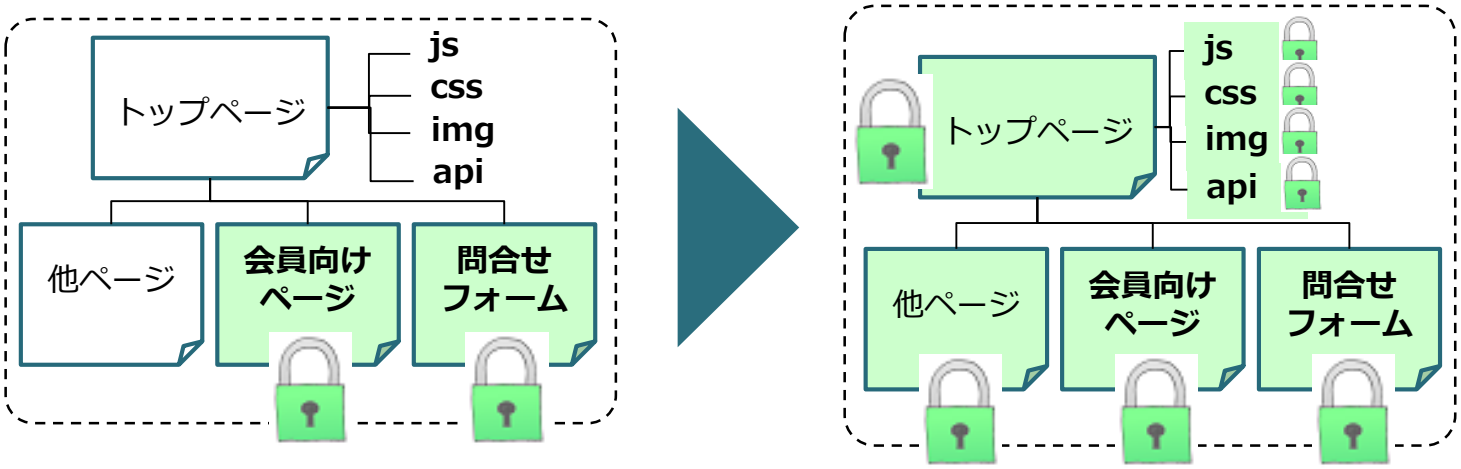
②改良と普及の時代

・SSL/TLSの改良と普及
平成29年頃：常時SSL化/完全HTTPS化の進行
Webサイトのすべてのページおよびコンテンツを
HTTPSに対応させて通信を保護するサイトが国内外で急速に増加

「米国政府の全Webサーバの完全HTTPS化の指示や、日本政府の情報セキュリティ対策のための統一基準群の見直しの中で完全HTTPS化の計画が公表されている。」
（弊社グループも現在対応中）

IPA, SSL/TLS暗号設定ガイドライン第2.0版, **2018 May**.

・Webサイトのすべてのページおよびコンテンツで、
SSL/TLSが利用され始めている。



あえて平成年号で振り返るTLSの30年

②改良と普及の時代

・SSL/TLSの改良と普及
平成11年：TLS1.0 RFC公開
平成18年：TLS1.1 RFC公開
平成20年：TLS1.2 RFC公開

・SSL/TLSのバージョンは、IETF主導で標準化が進められたバージョンが主流に

・平成30年：TLS1.0 & TLS1.1 終了に向けた動き

IETFが, 平成30年にTLS1.0およびTLS1.1を廃止予定とするdraftを公開、
ブラウザベンダ（Apple, Google, Mozilla, Microsoft）が令和2年、
クレジットカード（JCB等）が平成30年5-6月、Yahoo! が平成30年9-10月に、
TLS1.0およびTLS1.1の利用を終了すると発表。 IETF, Deprecating TLSv1.0 and TLSv1.1 (draft), 2018 Jun.
（その他、各社の公式サイトおよび公式ブログを参照）

米国政府関連機関(NIST)が, TLSガイドライン第2版(draft)を公開
政府機関のサーバおよびクライアントは、TLS1.2(FIPSベース暗号設定)を利用すること、
令和6年1月までに、TLS1.3のサポートをすることとしている。
TLS1.3は、TLS1.2の代替ではなく、TLS1.2との共存を意図している。

NIST, SP 800-52 Rev.2 (draft), Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, 2018 Oct.

あえて平成年号で振り返るTLSの30年

③再発明の時代

・**平成30年:TLS1.3 RFC公開**

・より低遅延＆高速に

※0-RTT利用時はリプレイに注意

・0-RTT：セッション再開時など、ClientHello後にデータ送信可

・1-RTT：ClientHello/ServerHello等の一往復後にデータ送受信可

※TLS1.2以前は2-RTTが必要であった

→ハイレベルのWebサービス管理者が嬉しい
（最速のユーザ体験を追求できる！）

・より安全に運用しやすく

・鍵交換は Forward Secrecy 対応のみ

・暗号化は 認証付き暗号のみ

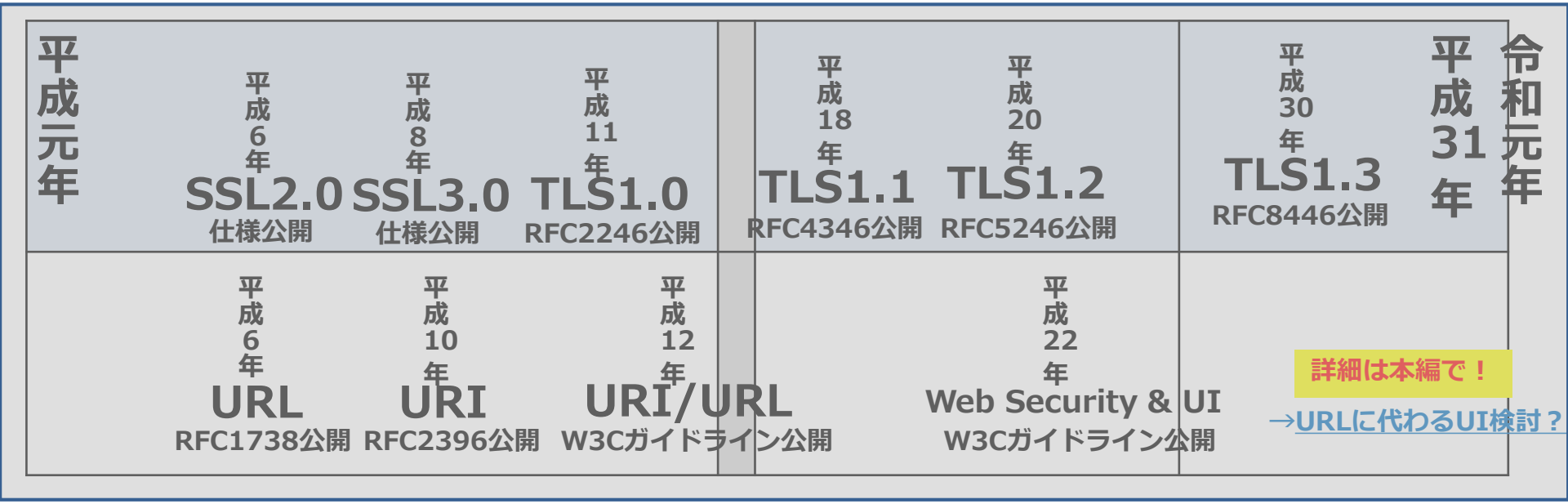
※PSKのみ利用時は例外

・ハンドシェイク通信を暗号化

※ClientHello/ServerHello 以後

→すべてのWebサービス管理者が嬉しい
（SSL/TLS設定時に陥りやすい落とし穴が減った！！）

あえて平成年号で振り返るTLSの30年



平成30年、TLS1.3公開により平和が訪れた矢先、
平成31年、新たに巻き起こる議論

『1月下旬に開かれたセキュリティカンファレンス「Enigma 2019」で、Chromeのセキュリティ対策チームを率いるエミリー・スタークが語った内容が論争を巻き起こした。』
『グーグルのChromeセキュリティ対策チームは2018年9月、大胆な構想を打ち出した。あのURLをなくしてしまおうというのだ。』
『長くなるばかりの理解不能なURLの文字列と格闘せずに済むようになる。URLの複雑さにつけ込んで次々に現れる詐欺行為にも対抗できるはずだ。（中略）現状、意味不明の文字が際限なく並ぶURLは、ハッカーによる詐欺行為の格好の隠れみのになっている。』

詳細は本編（第2章）で！

(原文) Emily Stark, Google, @ USENIX / Enigma 2019 “The URLephant in the Room”, **2019 Jan**.

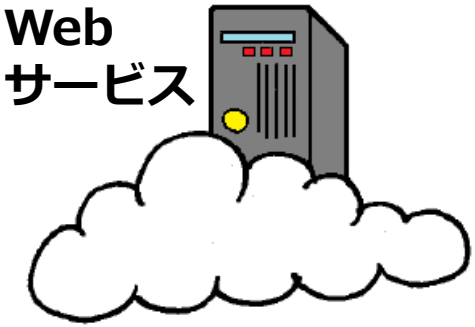
(解説記事) WIRED,『グーグルは、こうして「URLがない世界」への第一歩を踏み出す』, **2019 Feb**.

ユーザ

認証局

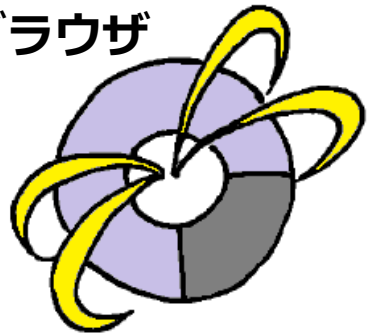
TLSとWebブラウザの表示のいまとこれから
～URLバーの表示はどうなるのか～

2019/5/31
NTTセキュアプラットフォーム研究所
奥田 哲矢



Web
サービス

ブラウザ



講演概要

Webサイトの常時SSL化が進んでいる中で、一部ブラウザベンダは
SSL/TLSに関する警告表示等のユーザインタフェースの変更を進めています。
その多くは、ボランティアユーザによるトライアルを経て、
変更方針が国際会議で発表され、ブラウザにデプロイされる流れで進行しています。
本講演では、ブラウザベンダの動向や国際会議の動向に従って、
SSL/TLSに関するWebブラウザの表示がどのように変化しているかを解説します。

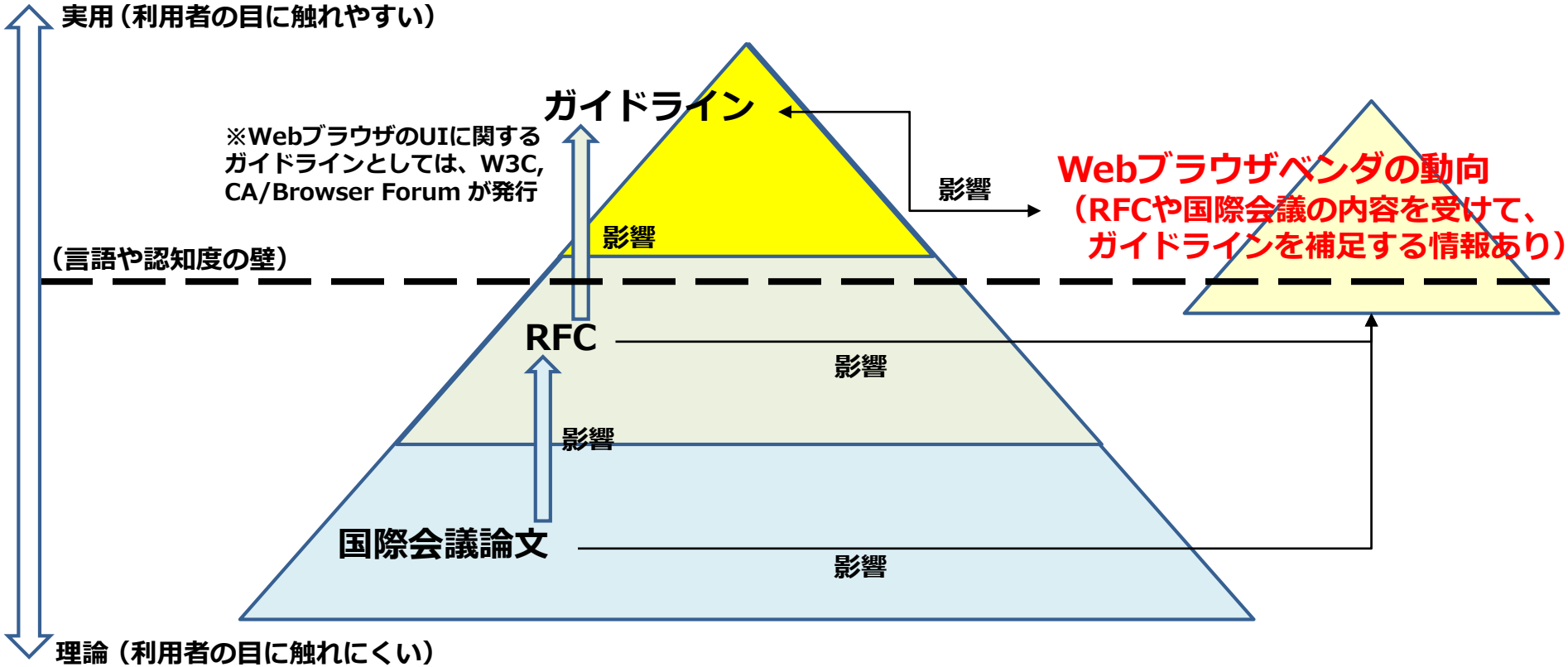
特に、2018年に入ってから、一部ブラウザにおいて
EV証明書の社名の表示が変更され始めている事が一時話題になりました。
これは、今後のユーザのインターネットへの向き合い方に
大きな影響を及ぼす取り組みであると言えます。

相手の顔の見えないインターネットを安全に利用するためには、
Webサイトの信頼性の判断材料として、ユーザ認知に合った表示と情報提供が必要です。
URLやドメイン名のみでは、正しいドメイン名と誤認してしまうような
ドメイン名が悪用されている既知の問題があり、一定の危うさを抱えていると言えます。
そのため、例えばEV証明書の社名の表示に代表されるような、
人間の認知に合った信頼判断の仕組みが、将来的に必要になると考えられます。
本発表では、これらに関する現状と今後を読み解いていきます。

本講演の目的

Q. なぜ「TLSとWebブラウザの表示」について知るべきなのか？
A. Webブラウザベンダの動向が、RFCや国際会議の動向を反映しており、Webサイト管理において関連する情報源となっているため。

各情報源の間には力学が存在し、相互に影響を与えている。



自己紹介

前職 NTTレゾナントでWebサービス開発に従事。
→**担当サービスの常時SSL化対応**を経験。

goo地図の実験的サービスとして、
Webブラウザで利用可能な
商業施設の3Dマップなどの開発をやっていました。

goo 地図 goo ラボ

Webブラウザの表示の最近の話題(1/3)

一部ブラウザで、非HTTPS時の警告アイコン表示が徐々に強化されている

2018年2月-5月発表

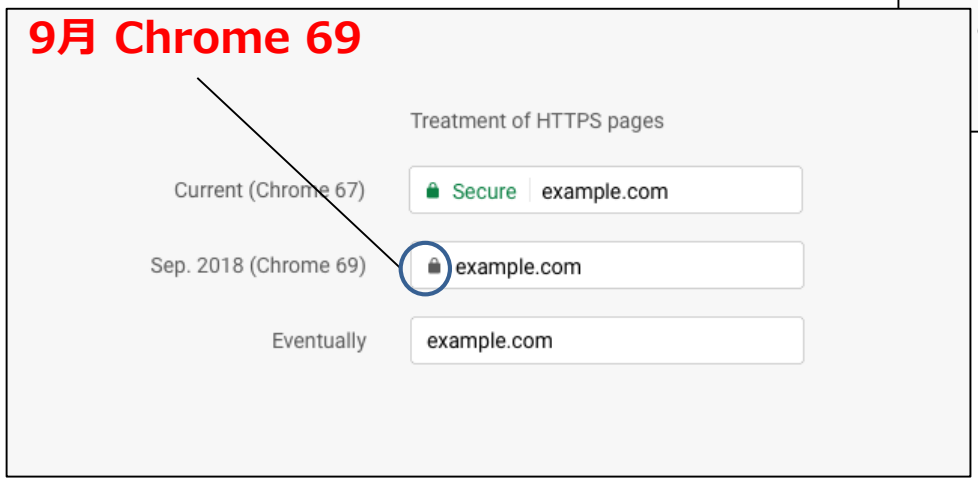
HTTP

7月 Chrome 68

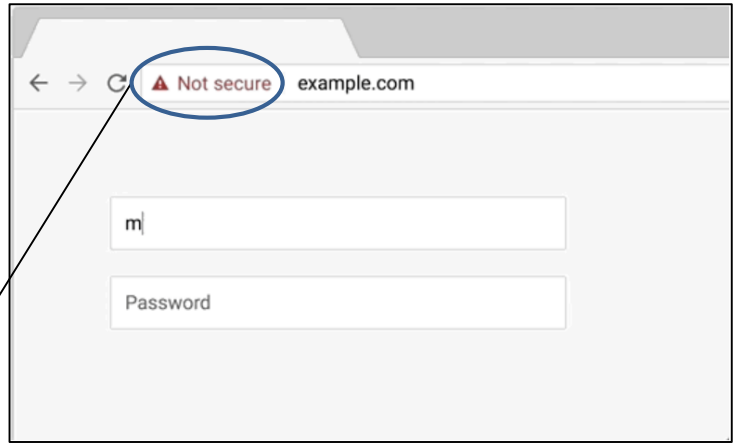
※日本語表記は
「保護されていない通信」

HTTPS

9月 Chrome 69



HTTP



10月 Chrome 70

©Googleセキュリティブログ「A Secure Web is Here to Stay」2018.2
©Chromiumブログ「Evolving Chrome's Security Indicators」2018.5

Firefoxも表示変更を推進。Mozillaセキュリティブログ
「Communicating the Dangers of Non-Secure HTTP」2017.1

Webブラウザの表示の最近の話題(2/3)

一部ブラウザで、EV(Extended Validation)証明書の表示が変更されている

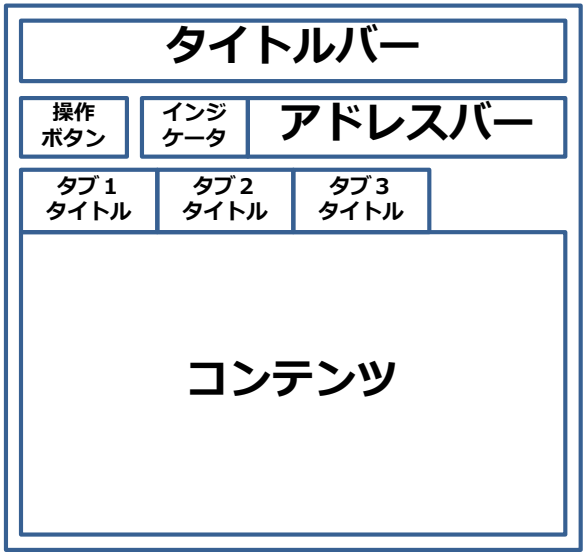
※EV証明書については後述

・2018.9 Chrome（デスクトップ版），
緑色→グレー色表示

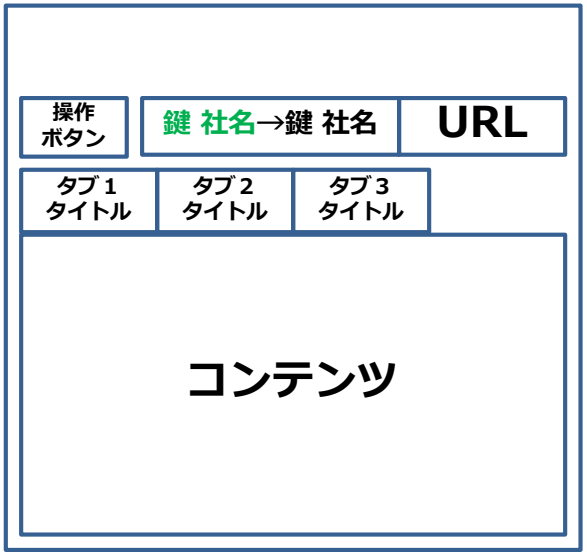
他、表示変更に関して実験中の様子

森下様, @ Twitter, 2018.9, 他
“As part of an experiment, Chrome temporarily shows only the lock icon in the address bar. Your SSL certificate with Extended Validation is still valid.”

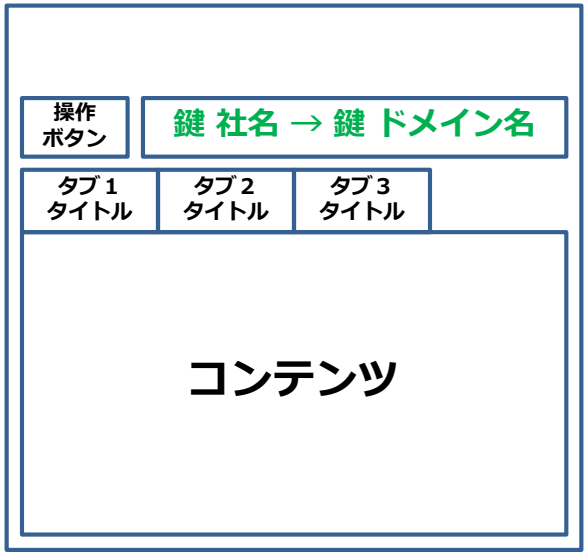
・2018.9 一部ブラウザ, **社名→ドメイン名表示** @ CA / Browser Forum, 2018.6



凡例



Chrome（デスクトップ版）
ver.68→ver.69



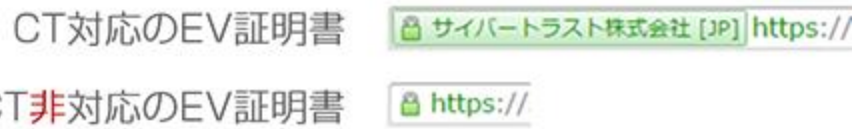
一部ブラウザ 旧版→最新版

Webブラウザの表示の最近の話題(3/3)

一部ブラウザで、CT(Certificate Transparency)対応が必須化されている

※CTについては後述

- **Chrome**
  2015.1以降、EV証明書の発行時にCT対応を必須化
  （CT非対応の場合は社名→ドメイン名表示）



  2016.9以降、一部の認証局の証明書で
  CT対応を必須化（非対応時は警告画面表示）
→その後、2018.4以降に発行される、
全ての証明書で必須化、対応する認証局が増加

©グローバルサイン
「Certificate Transparencyの最新状況」
©サイバートラスト
「Chrome 53 から Certificate Transparency の何が変わる？」
©DigiCert
「Certificate Transparency Required for EV Certificates to Show Green Address Bar in Chrome」

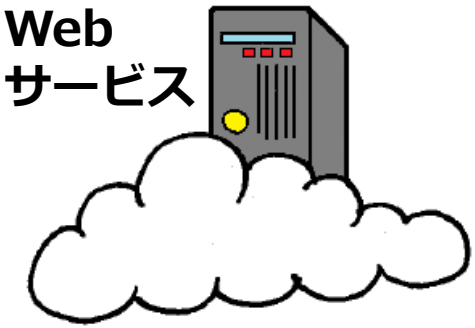
- **Safari**
  2018.10以降に発行される、
  全ての証明書でCT対応を必須化

©Apple Inc. 「Apple’s Certificate Transparency policy」

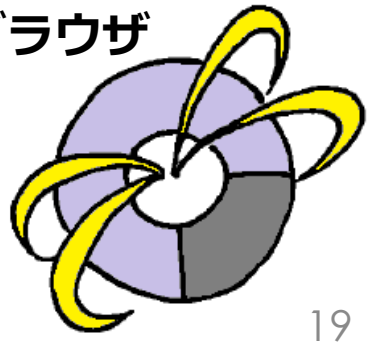
ユーザ

認証局

TLSとWebブラウザの表示のいまとこれから



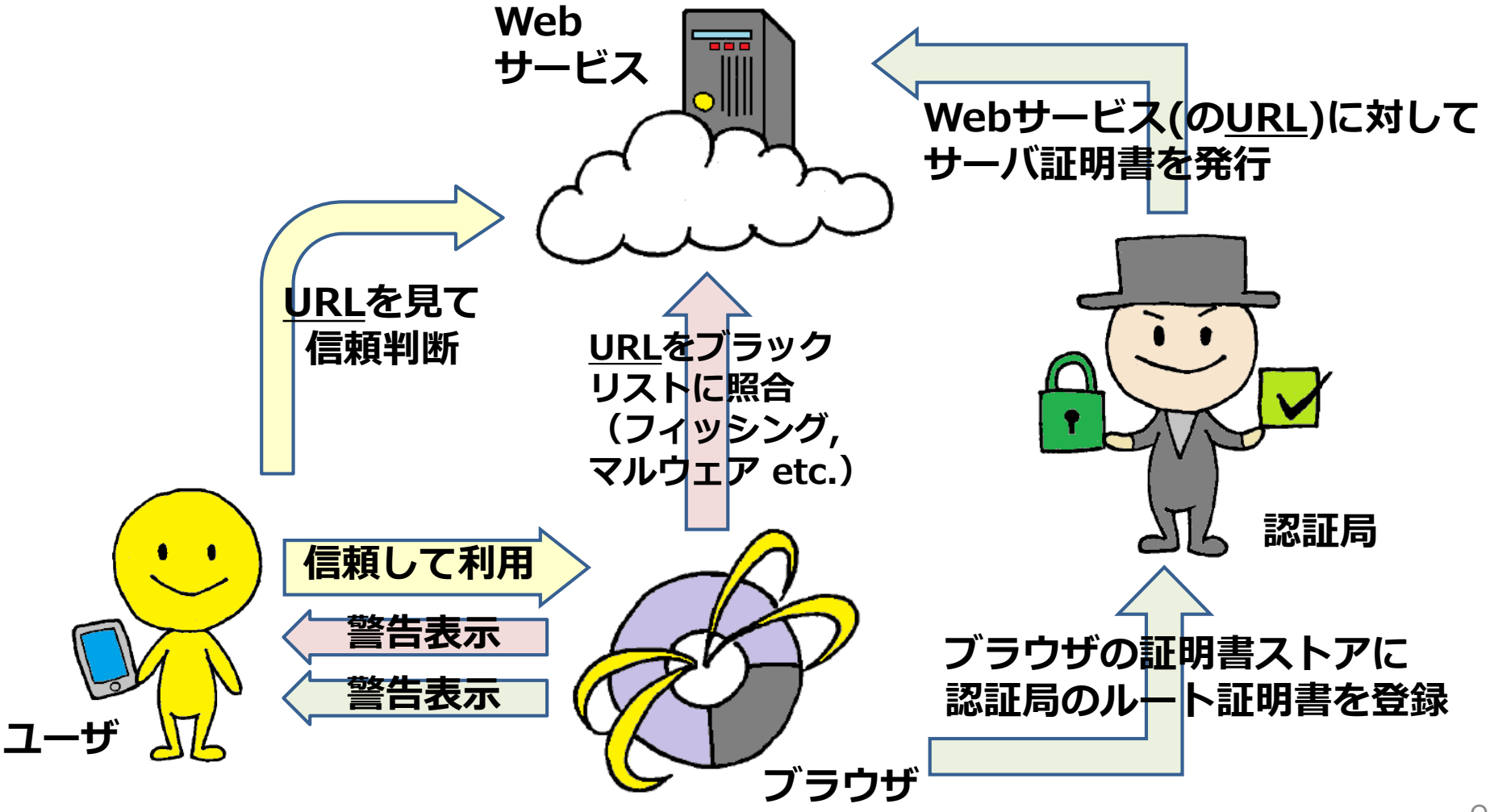
Web
サービス



ブラウザ

公開鍵基盤(PKI)の登場人物の紹介

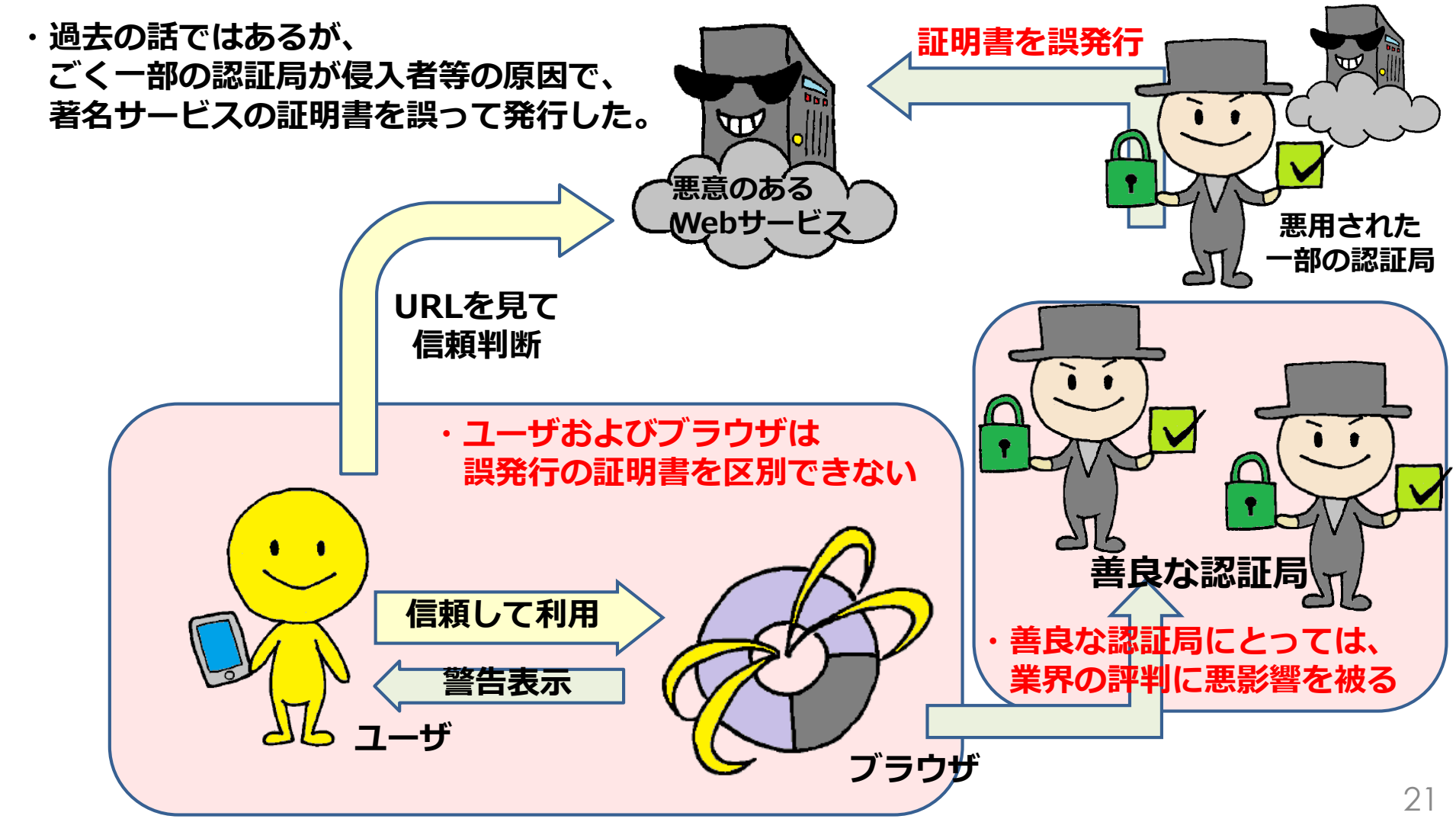
・ユーザ, ブラウザ, 認証局は、URLでWebサービスの信頼可否を判断する。
・ブラウザは、信頼形成時に異常が検知されれば、ユーザに警告を表示する。



CT (Certificate Transparency)とは？

Q. CT (Certificate Transparency)とは？
A. 過去の証明書誤発行の問題への対策

・過去の話ではあるが、
ごく一部の認証局が侵入者等の原因で、
著名サービスの証明書を誤って発行した。

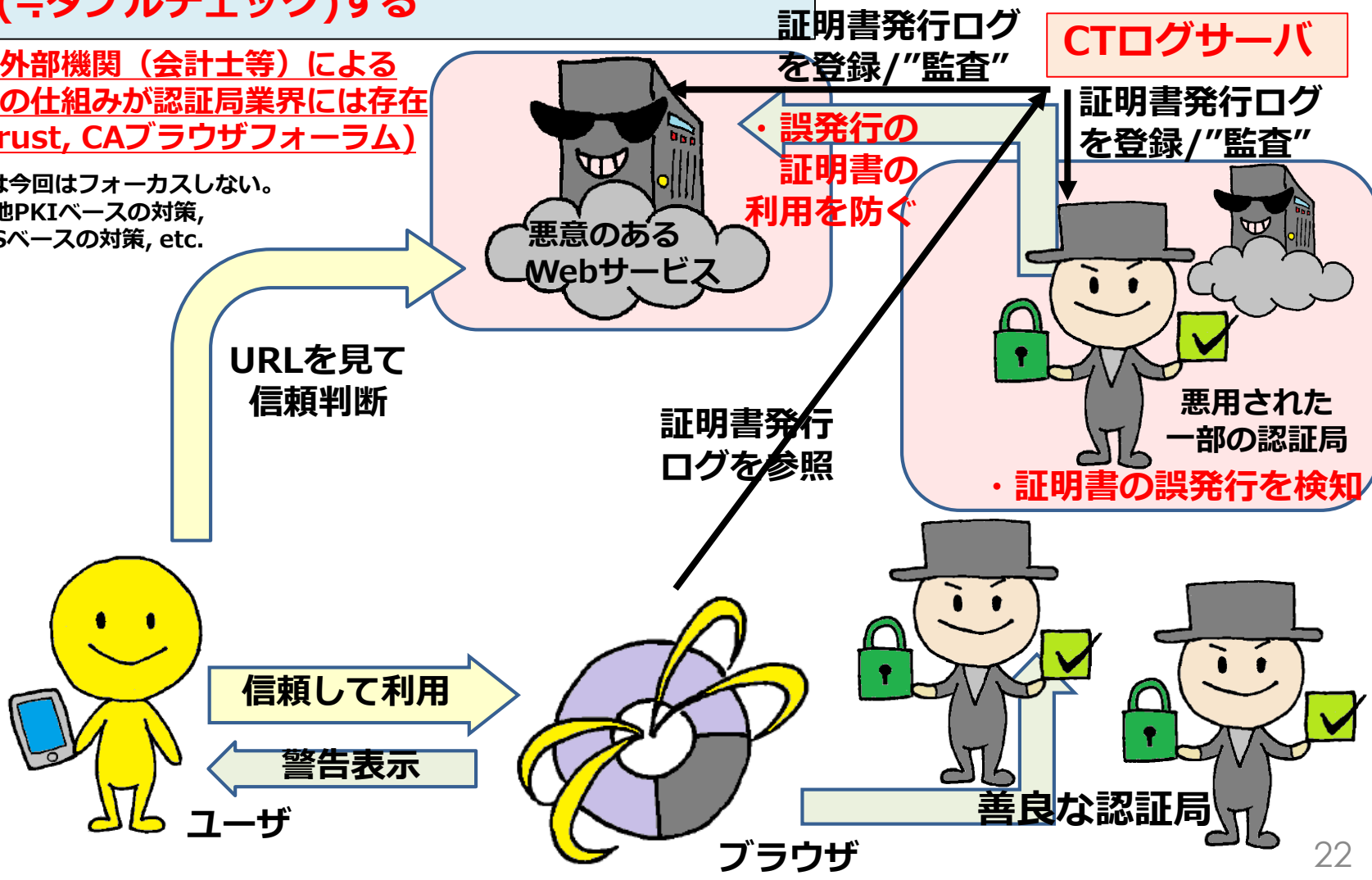


CT (Certificate Transparency)とは？

・誤発行された証明書をユーザは見分けることが困難
・CTログサーバで、認証局による誤発行が無いことを“監査”(≒ダブルチェック)する

※実際には、外部機関（会計士等）による厳正な監査の仕組みが認証局業界には存在 (cf. WebTrust, CAブラウザフォーラム)

※他の対策技術は今回はフォーカスしない。
CRL, OCSP, 他PKIベースの対策,
DANE, 他DNSベースの対策, etc.

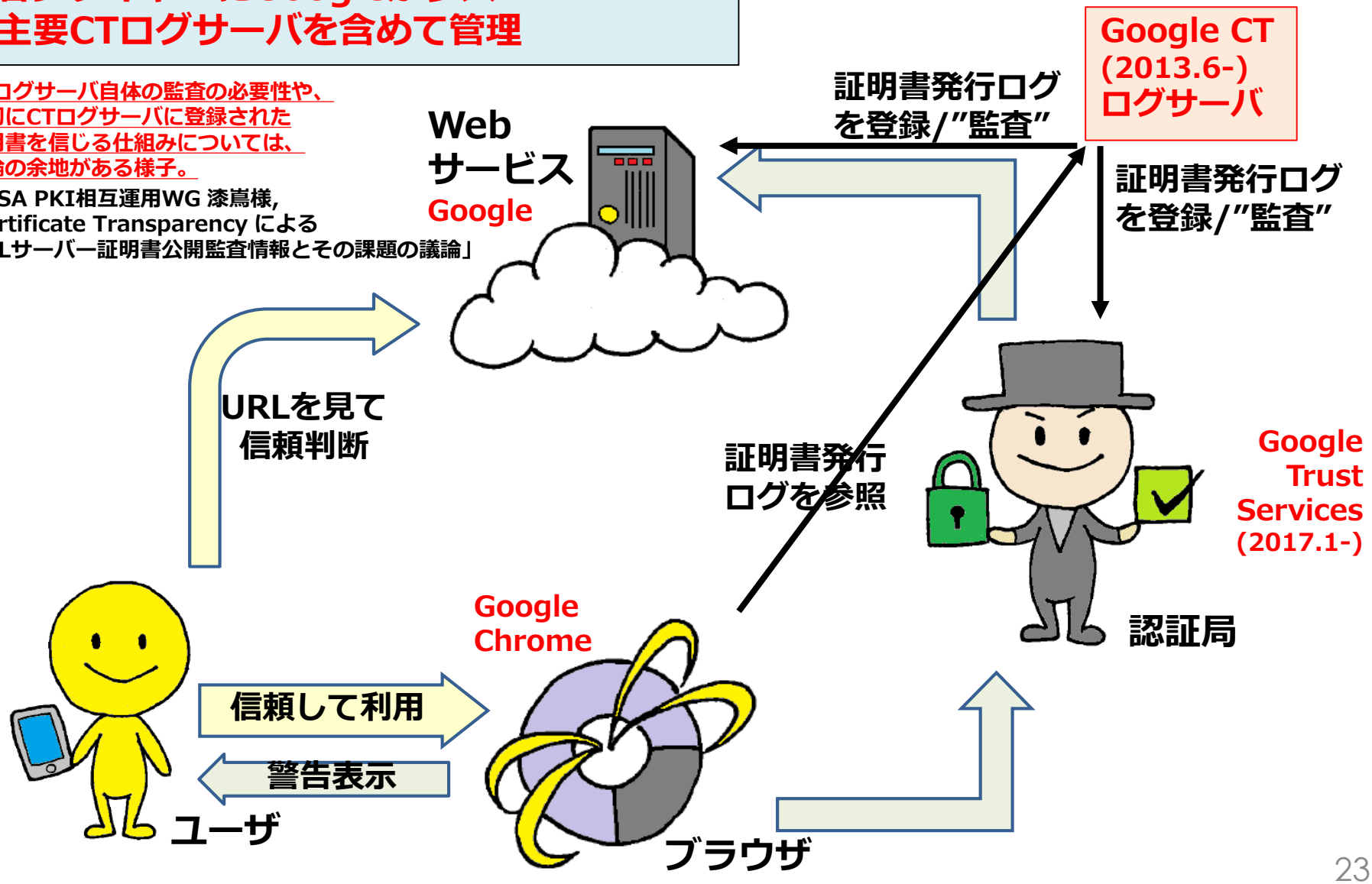


公開鍵基盤(PKI)の登場人物のいま

・各プレイヤーにGoogleが参入
主要CTログサーバを含めて管理

※CTログサーバ自体の監査の必要性や、最初にCTログサーバに登録された証明書を信じる仕組みについては、議論の余地がある様子。

©JNSA PKI相互運用WG 漆嶌様,
「Certificate Transparency による
SSLサーバー証明書公開監査情報とその課題の議論」

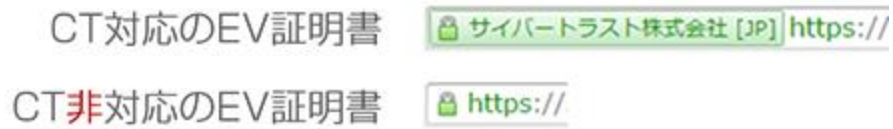


Webブラウザの表示の最近の話題(3/3) 再掲

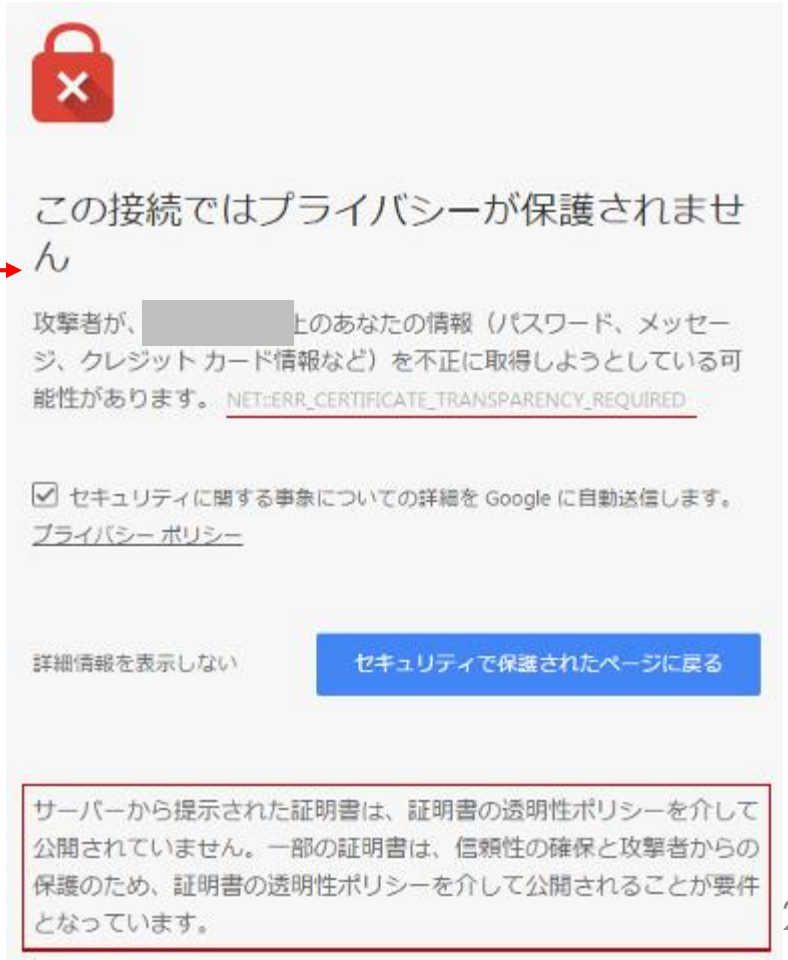
一部ブラウザで、CT(Certificate Transparency)対応が必須化されている

→認証局のCT対応が（事実上）必須に

- **Chrome**
  2015.1以降、EV証明書の発行時にCT対応を必須化
  （CT非対応の場合は社名→ドメイン名表示）



  2016.9以降、一部の認証局の証明書で
  CT対応を必須化（非対応時は警告画面表示）
→その後、2018.4以降に発行される、
全ての証明書で必須化、対応する認証局が増加



©グローバルサイン
「Certificate Transparencyの最新状況」
©サイバートラスト
「Chrome 53 から Certificate Transparency の何が変わる？」
©DigiCert
「Certificate Transparency Required for EV Certificates to Show Green Address Bar in Chrome」

- **Safari**
  2018.10以降に発行される、
  全ての証明書でCT対応を必須化

©Apple Inc. 「Apple’s Certificate Transparency policy」

ユーザ

認証局

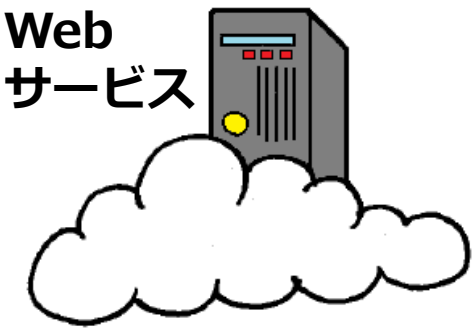
TLSとWebブラウザの表示のいまとこれから

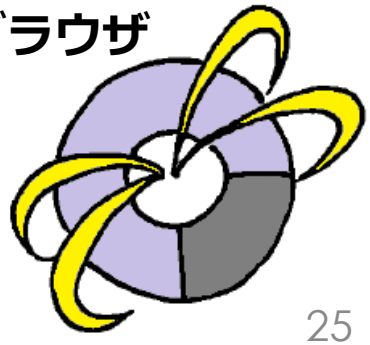
1章：公開鍵基盤(PKI)のいま

2章：EV証明書の本当の価値

3章：Webブラウザの表示のいまとこれから

Web
サービス



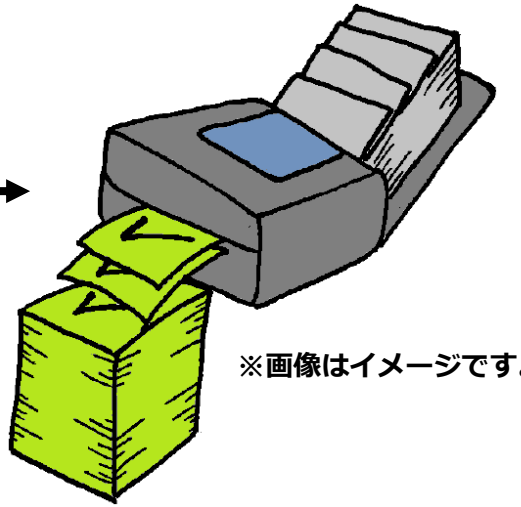


ブラウザ

EV証明書とは？

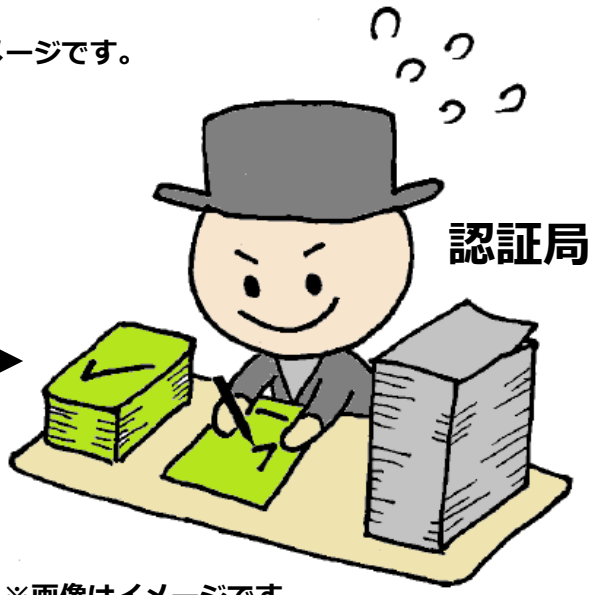
・DV(Domain Validated)証明書：対象ドメインの管理権限のみを確認
・EV(Extended Validated)証明書：上記＋対象ドメインの管理組織の実在を確認

・DV証明書は、
確認作業を自動化できるため、
自動発行の認証局が存在。



※画像はイメージです。

・EV証明書は、
確認作業の自動化が困難なため、
一定の人手が必要となる。



※画像はイメージです。

EV証明書のブラウザ表示例

・EV証明書の表示：社名／所在地をアドレスバーに表示

Webサービス

Webサービス(のURL)に対して
サーバ証明書を発行

認証局

URLと緑色の社名／所在地を見て
信頼判断

信頼して利用

警告表示

ユーザ

ブラウザ

ブラウザの証明書ストアに
認証局のルート証明書を登録

EV証明書に関する動向１

CT対応しなければEV社名表示を変更する旨、一部ブラウザベンダが宣言
→各認証局がCT対応を進める方向に

Google等
CTログサーバ
（普及中）

EV証明書に関する
動向１

Webサービス(のURL)に対して
サーバ証明書を発行

Web
サービス

URLと緑色の社名／所在地を見て
信頼判断

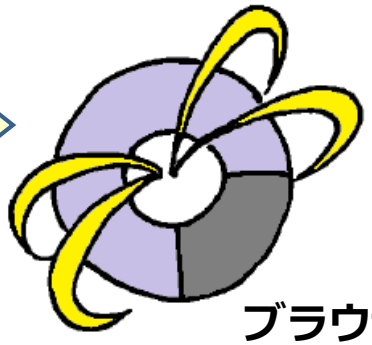
収益＄

認証局

信頼して利用

警告表示

ユーザ



ブラウザ

ブラウザの証明書ストアに
認証局のルート証明書を登録

EV証明書に関する動向２

その後、CT普及率は向上 →
~~CT対応しなければ~~EV社名表示を変更する試行を一部ブラウザベンダが実施

Google等
CTログサーバ
（普及済み）

EV証明書に関する
動向２

Web
サービス

Webサービス(のURL)に対して
サーバ証明書を発行

収益＄

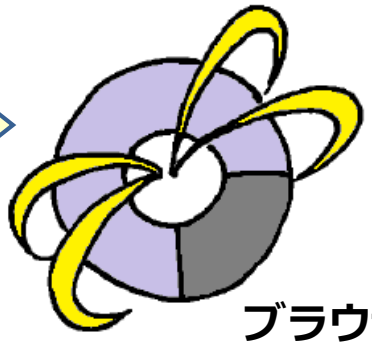
認証局

URLと緑色
の社名／所
在地を見て
信頼判断

ユーザ

信頼して利用

警告表示



ブラウザ

ブラウザの証明書ストアに
認証局のルート証明書を登録

Webブラウザの表示の最近の話題(2/3) 再掲

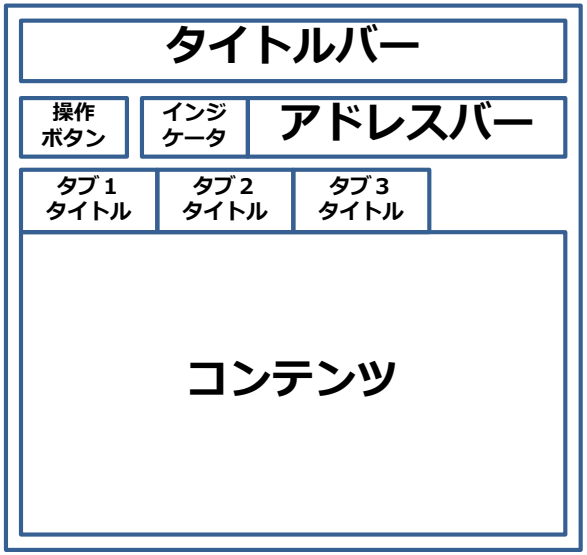
一部ブラウザで、EV(Extended Validation)証明書の表示が変更されている

・2018.9 Chrome（デスクトップ版）,
緑色→グレー色表示

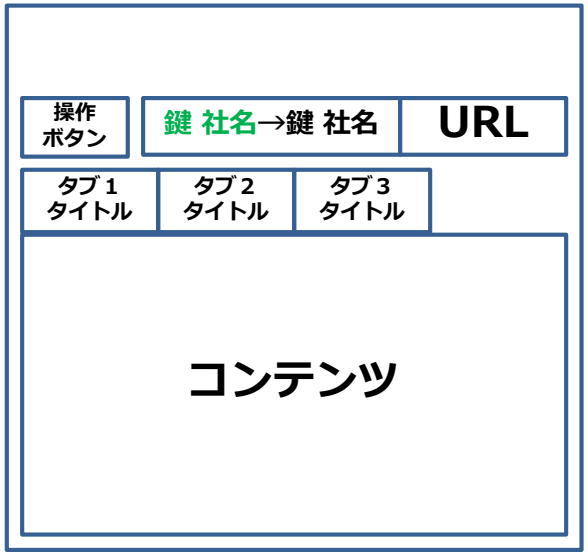
他、表示変更に関して実験中の様子

森下様, @ Twitter, 2018.9, 他
“As part of an experiment, Chrome temporarily shows only the lock icon in the address bar. Your SSL certificate with Extended Validation is still valid.”

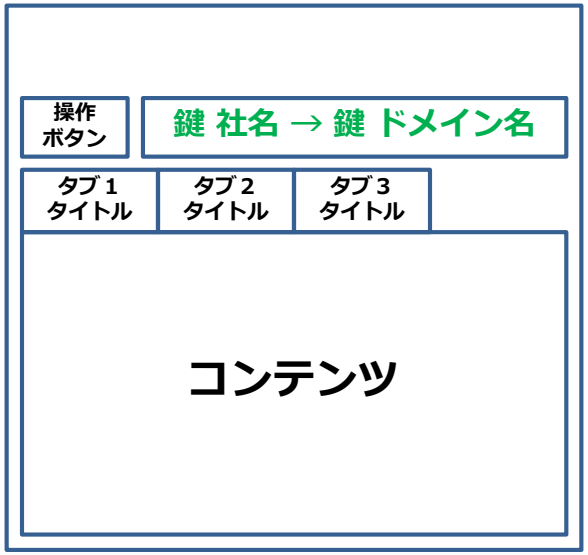
・2018.9 一部ブラウザ, **社名→ドメイン名表示** @ CA / Browser Forum, 2018.6



凡例



Chrome（デスクトップ版）
ver.68→ver.69



一部ブラウザ 旧版→最新版

なぜ EV表示の変更が検討されるのか

一部ブラウザベンダは(現状の)EV表示に積極的ではなかった様子が見受けられる。

・Google所属著者の2016年発行の論文で、EV表示について下記の言及があった。
「Webサイトはアイデンティティ保証のため、認証局に代金を支払っている。」
「EVはフィッシング対策であるが、著名サイト／主要ブラウザのサポートが十分でなく、
その利用は限定的である。デスクトップの主要ブラウザではEV表示が行われるが、
Android版のChrome/Opera等のモバイルブラウザはEV表示を行っていない。」
「先行研究では、EVの表示方法に改善が必要である旨、示唆されている。
ただ、本研究では、EVの表示方法の改善はスコープ外とした。」
→2016年時点では改善検討のスコープ外にしたということ。以降は推測であるが、
2018年現在に改善検討（社名表示の変更を含めて）を実施しているということか。

[SOUPS2016] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. Embre, E. Morant, and S. Consolvo, Rethinking Connection Security Indicators, SOUPS, 2016 Jun.

・ユーザビリティの観点では、モバイルは表示スペースが小さいことが課題
→一部モバイルブラウザでは、元々EV証明書の社名を初期表示していない [SOUPS2016]

Chrome（デスクトップ版）

Chrome（モバイル版）

・CA/ブラウザフォーラムのガイドラインでは、
EV証明書は「may be displayed in a special manner」
「recommended that the application's behavior differ」
・W3Cのガイドラインでは、EV証明書は
「can therefore be treated more favorably
in terms of the primary security indicators /
may need to be specially marked」

[CABF2018] Guidelines for the Issuance and Management of Extended Validation Certificates, **CA / Browser Forum**, 2018 Mar.
[CABF2014] Recommendations for Processing EV SSL Certificates, **CA / Browser Forum**, 2014 Jan.
[W3C2010] T. Roessler, A. Sladhana, Web Security Context: User Interface Guidelines, **W3C Recommendation**, 2010 Aug.

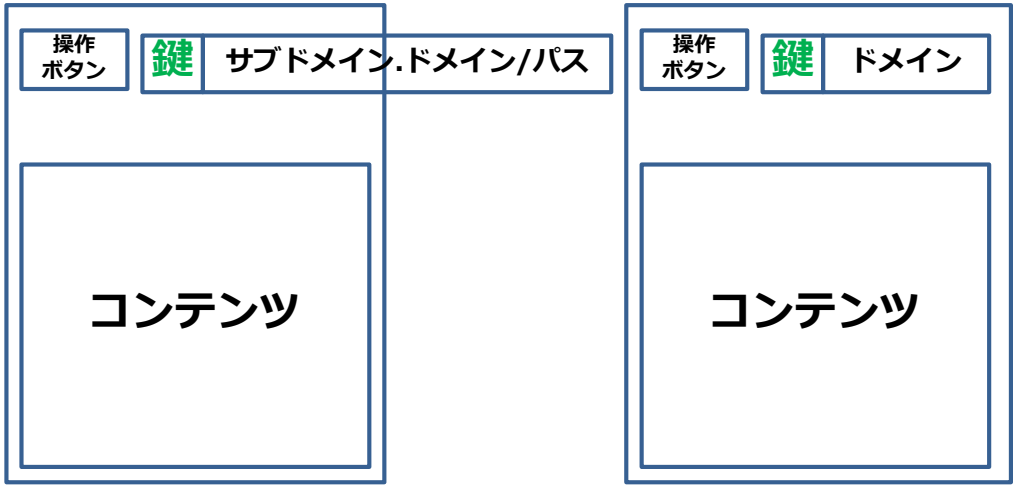
なぜ EV表示の変更が検討されるのか

・ユーザビリティの観点では、モバイルは表示スペースが小さいことが課題
→一部モバイルブラウザでは、URLさえも短縮表示して、
Webサイトの信頼判断に重要とされる「ドメイン名」のみを表示している。

・多くのユーザは、Webページのコンテンツに注目して、
見た目や内容で、Webサイトの正当性を判断している場合がある。
（が、コンテンツはフィッシングサイト側が複製できるため、判断誤りである。）
→対策として、ドメイン名を、それ以外のURL要素と分離する、
URLを複雑にする要素を削減する等、より明瞭に注目を集めるように表示する方法がある

[CHI2011] University of Calgary, Canada,
Does Domain Highlighting Help People Identify Phishing Sites?, ACM CHI, 2011 May.

・Chromeは、ドメインのみ黒字で表示、他はグレー字で表示
一部サブドメイン非表示(www, m, etc.)のトライアルを実施している様子(2018.9～)
・一部ブラウザでは、ドメインのみ表示、パスは非表示
・W3Cのガイドラインでは、URLは ”MAY shorten ~ by displaying only a suffix(末尾)” [W3C2010]



Chrome（モバイル版）
URL全体を表示する場合

一部モバイルブラウザで、
ドメインのみ表示する場合

Chrome(PC版)のURL表示例
（ドメインハイライト）

グレー字　黒字　グレー字

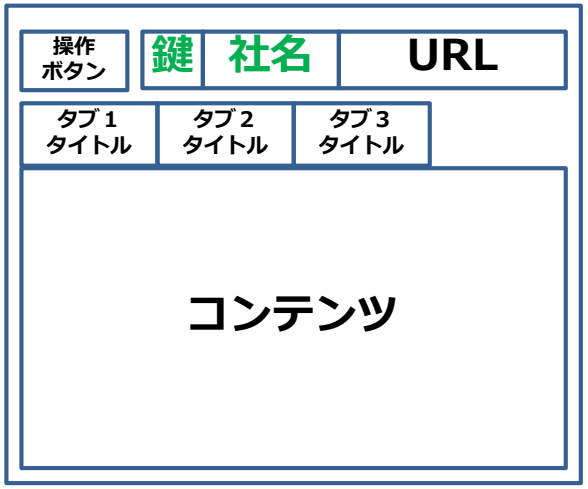
なぜ EV表示の変更が検討されるのか

・現在はモバイルユーザが増加（PCユーザに比較して）
→モバイルブラウザの表示に統一する、という考え方が一つの要因か

・デスクトップブラウザとモバイルブラウザの間で、表示に差異がありユーザは混乱する

C. Amrutkar, P. Traynor, P. C. Oorschot, An Empirical Evaluation of Security Indicators in Mobile Web Browsers, IEEE Transactions on Mobile Computing, 2015 May.
（※ブラウザベンダ所属の著者では無い）

・一部モバイルブラウザでは、フィッシング対策のために
「緑色の社名/所在地を確認しよう」とユーザに教育することが出来ない場合がある。
（「緑色のカギマークを確認しよう」がユーザに浸透してきた状況とは異なる。）



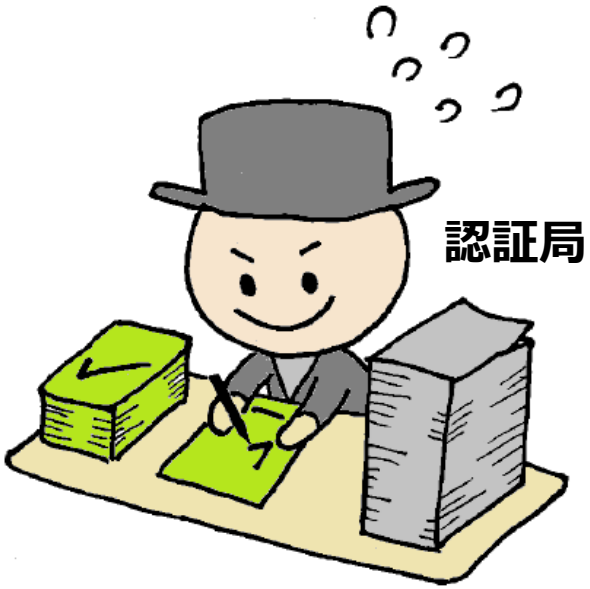
Chrome（デスクトップ版）

一部モバイルブラウザで、
ドメインのみ表示する場合

デスクトップブラウザと
モバイルブラウザの間で、
表示に差異がある。

EV表示のこれからは？

・本当にURLのみの表示で良いのか？



URL表示に関する課題

・モバイルは表示スペースが小さい
→URL表示の悪用への対策がより重要

※下記一覧は、ブラウザベンダにより
既に対策が出来ている課題を含む

Table 1: List of the 27 attack building blocks (ABBs) used to evaluate security of mobile browsers

Class	Test#	Explanation	Prior Work	Potential Attacks
Event Routing	1–6	Do cross-origin, overlapping elements receive events when they are not the topmost ones? (Different tests for combinations of overlapped images and buttons, links, forms, and other images)	[3, 6]	Clickjacking, CSRF
URL	7–9	When presented with a long URL (long subdomain, longfi lepath, or a combination of both), does a browser render that URL in a way that could be abused for spoofing attacks?	[30, 38]	Phishing, malware/scam delivery
	10	When presented with an Internationalized Domain Name (IDN), will a browser display the IDN format?		
Address Bar	11	Is the address bar hidden if the top-level frame is navigated by a child frame?	[3, 6]	Phishing, malware/scam delivery
	12	Does a browser show a page's title instead of its URL?		
	13	Is the address bar hidden if the visited website has a lot of content?		
	14	Is the address bar hidden when switching the device to "landscape" mode?		
	15–16	Is the address bar hidden upon manual/automatic page scrolling?	[30, 32]	Phishing, malware/scam delivery
	17–18	Is the address bar hidden when typing in a textbox and tapping on a button?	[15, 38]	Phishing, malware/scam delivery
	19	Is the address bar hidden when typing to a fake (e.g., canvas-created) textbox?	Novel	Phishing, malware/scam delivery
Security Indicators	20	Is the favicon placed next to padlock icon?	[4, 5, 14, 37]	MITM attack, Phishing
	21–22	When rendering an HTTPS page, is the address bar displayed the same in the presence of mixed content (image and JavaScript) as in its absence?	[9]	MITM attack
	23	Is a webpage with self-signed certificate rendered without warnings?	[4, 5, 14, 37]	MITM attack, Phishing
Content	24	Can an iframe expand its size past the one defined by its parent frame?	[3, 6]	Phishing
	25	Is a mixed-content image resource loaded?	[9]	MITM attack
	26	Is a mixed-content JavaScript script executed?	[9]	MITM attack
	27	Is JavaScript code included in a self-signed website executed before the warning is accepted?	Novel	Phishing, MITM attack

長いURLやIDNの表示不備を狙ったなりすまし

アドレスバーやURLの非表示時を狙ったなりすまし

M. Luo, O. Starov, N. Honarmand, N. Nikiforakis, Hindsight: Understanding the Evolution of UI Vulnerabilities in Mobile Browsers, ACM CCS, **2017 Oct-Nov**.

EV表示のこれからは？

URLのみの表示では、対策が難しい課題が残る
→EV表示には、将来的に見出すべき価値があるか

・URL表示の悪用の事例（長くて見間違えやすいURL, 文字が似て見間違えやすいURL etc.）
・Google所属著者の2018年発行の論文で、下記の言及があった。
「フィッシング攻撃は**ユーザが大変慎重に注意してURLバーの内容を確認**することで、
しばしば防ぎ得る**（が、これで常に十分という訳ではない。）**」

[CHI2018] R. W. Reeder, **A. P. Felt**, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman
An Experience Sampling Study of User Reactions to Browser Warnings in the Field, ACM CHI, **2018 Apr**.

→URL／ドメイン名によるサーバ認証では、対策が困難な事例が存在する。
本質的な解決には、よりユーザ認知に合った方法でサーバ認証をすべき（To Be Continued . . . ）

→本発表では、解決策に代わり、W3Cのガイドラインにおける検討（一部, 抜粋, 意訳）を紹介する。
「**人間が理解できる名前を、ドメイン名(URL)と紐づけること**　[W3C2010]
（Binding “human readable” names to domain names）」
「ユーザにとって重要なことは、**ドメイン名(URL)と実世界の存在を紐づけること**である。
例えば、あるドメイン名(URL)が、どこの国のどの会社であるか、知ることは有用である。
実世界の存在確認を行った証明書であれば、上記目的を果たすことが出来る。」

※本資料 P38「（参考）URL as UI 」を併せて参照

→EV表示に例示されるような、URLを補完する、
人間の認知に合った信頼判断の仕組みは、いずれ必要になると考える。

（To Be Continued . . . ）

ユーザ

認証局

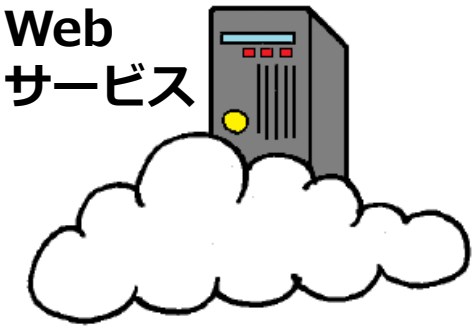
TLSとWebブラウザの表示のいまとこれから

1章：公開鍵基盤(PKI)のいま

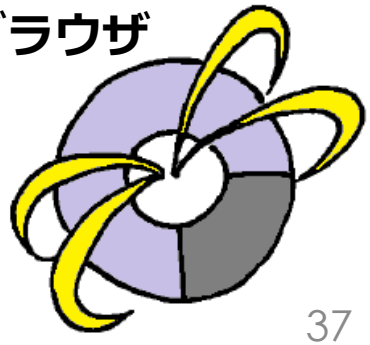
2章：EV証明書の本当の価値

3章：Webブラウザの表示のいまとこれから

Web
サービス



ブラウザ



Webブラウザの表示は今後どうなるのか？

・一部ブラウザベンダがPKIに関するトレンド発信を積極的に行っている。
→今後、Webブラウザの表示はどうなるのか、各種文献から読み解く。

・キープレイヤー：A. P. Felt 氏
下記のUI改善を進めた中心人物の様子
・Androidのプライバシーポリシー
・Chromeのセキュリティ警告表示(TLS, Malware, Phishing)

→現在進行形で、A. P. Felt 氏が関わる研究成果が続々と公表され、
Chromeにデプロイが進んでいる様子。

[USENIX2017] A. P. Felt, R. Barnes, A. King, C. Palmer, C. Bentzel, P. Tabriz, Measuring **HTTPS Adoption** on the Web, USENIX Security Symposium, **2017 Aug**.

[SOUPS2016] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. Embre, E. Morant, and S. Consolvo, **Rethinking Connection Security Indicators**, SOUPS, **2016 Jun**.

[CHI2018] R. W. Reeder, A. P. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman An Experience Sampling Study of **User Reactions to Browser Warnings** in the Field, ACM CHI, **2018 Apr**.

[CCS2017] M. E. Acer, E. Stark, A. P. Felt, S. Fahl, R. Bhargava, B. Dev, M. Braithwaite, R.Sleevi, and P. Tabriz. Where the Wild Warnings Are: Root Causes of **Chrome HTTPS Certificate Errors**. ACM CCS, **2017 Oct-Nov**.

[CHI2014] A. P. Felt, R. W. Reeder, H. Almuhimedi, S. Consolvo, Experimenting At Scale With **Google Chrome's SSL Warning**, SOUPS, **2014 Jul**.

[SOUPS2014] H. Almuhimedi, A. P. Felt, R. W. Reeder, S. Consolvo, Your Reputation Precedes You: History, Reputation, and **the Chrome Malware Warning**, SOUPS, **2014 Jul**.

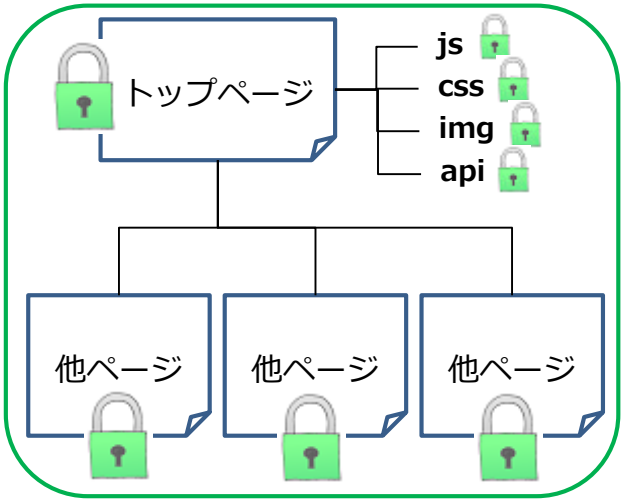
[USENIX2013] D. Akhawe and A. P. Felt. Alice in Warningland: A Large-Scale Field Study of **Browser Security Warning Effectiveness**. USENIX Security Symposium, **2013 Aug**.

Webブラウザの表示は今後どうなるのか？

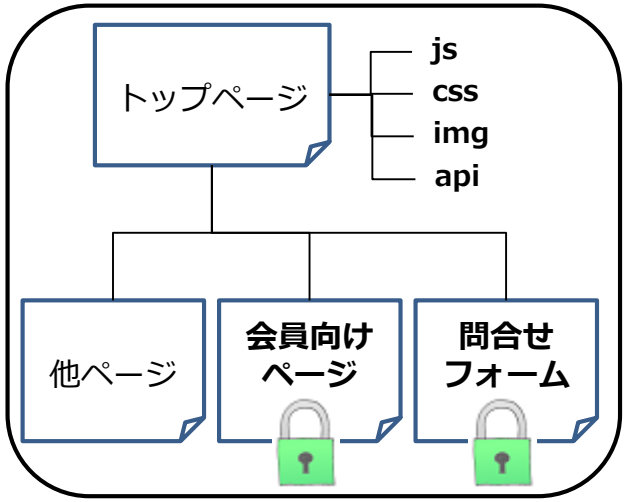
・背景：常時SSL化の進行

・常時SSL化（完全HTTPS化）とは、
トップページを含むWebサイト全体をHTTPS化すること

常時SSL化対応済み



一部ページのみSSL化



・各国政府が対応方針を策定

「米国政府の全Webサーバの完全HTTPS化の指示や、日本政府の情報セキュリティ対策のための統一基準群の見直しの中で完全HTTPS化の計画が公表されている。」
（弊社グループも現在対応中）

IPA, SSL/TLS暗号設定ガイドライン第2.0版, **2018 May**.

・2017年8月、A. P. Feltらが、東アジア（日本および韓国）の進行状況の遅れを指摘。

[USENIX2017]

・2017年に、楽天, クックパッド, アメブロ, Yahoo! Japan, goo 等が対応。

Webブラウザの表示の最近の話題(1/3) 再掲

一部ブラウザで、非HTTPS時の警告アイコン表示が徐々に強化されている

開発者ブログで発信（計3回）

2018年2月-5月発表

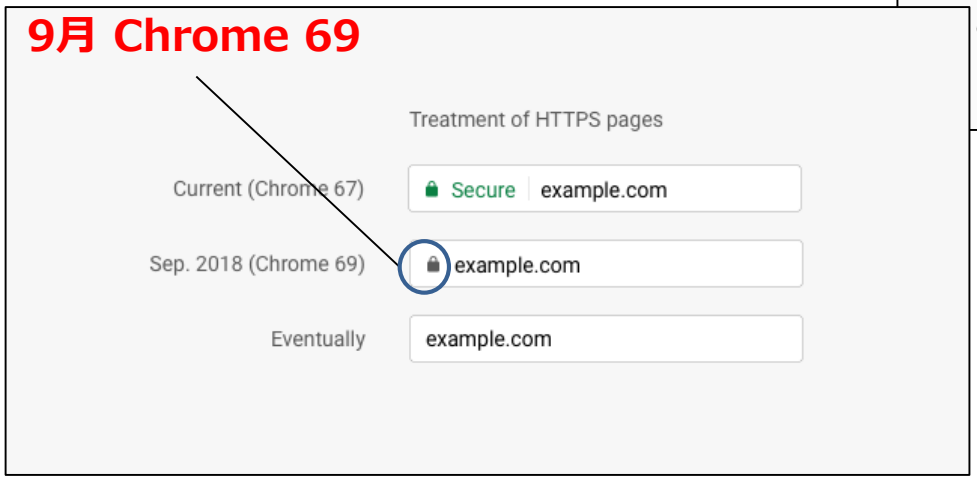
HTTP

7月 Chrome 68

※日本語表記は
「保護されていない通信」

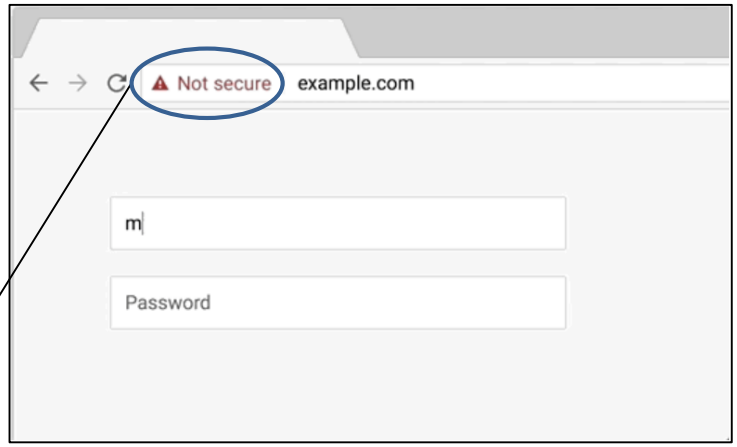
HTTPS

9月 Chrome 69



HTTP

10月 Chrome 70



©Googleセキュリティブログ「A Secure Web is Here to Stay」2018.2
©Chromiumブログ「Evolving Chrome's Security Indicators」2018.5

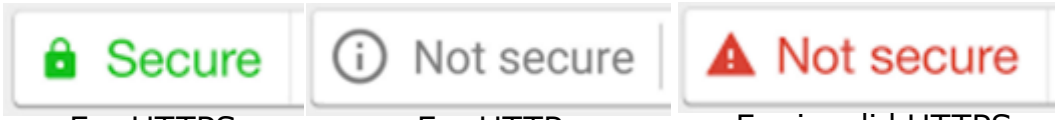
Firefoxも表示変更を推進。Mozillaセキュリティブログ
「Communicating the Dangers of Non-Secure HTTP」2017.1

Webブラウザの表示は今後どうなるのか？

・A. P. Felt 氏の研究紹介１：TLSに関するアイコン表示の変更
2016年時点で、ブラウザ表示変更の基本方針は示されていた。

2016年6月発表
[SOUPS2016]

「TLSに関して表示するアイコン&テキストをユーザテストで決定した」
「2016年9月 Chrome 53 から（次第に）デプロイを始める」



For HTTPS　For HTTP　For invalid HTTPS

2018年2月-5月発表
[開発者ブログ]

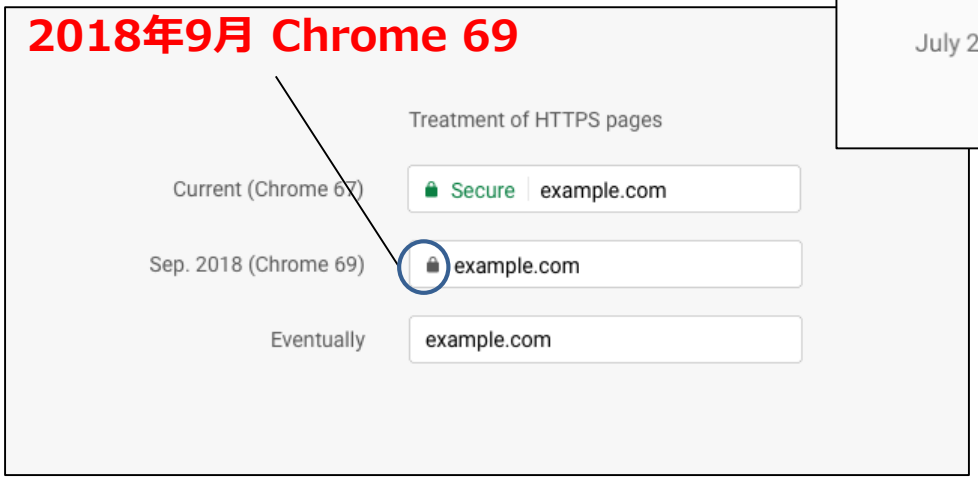
HTTP

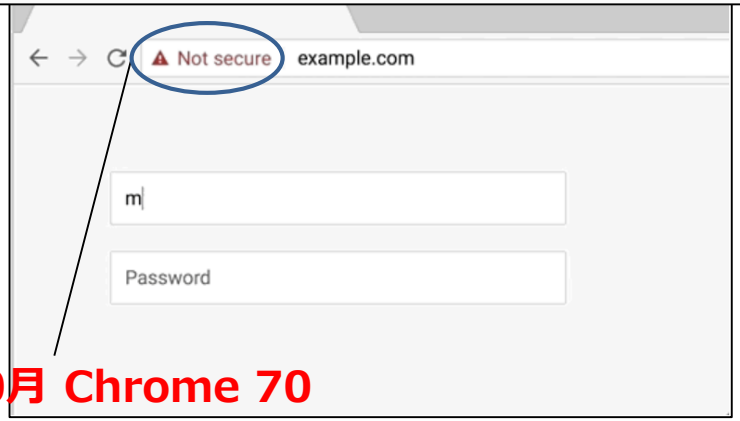
2018年7月 Chrome 68

※日本語表記は
「保護されていない通信」

HTTPS

2018年9月 Chrome 69



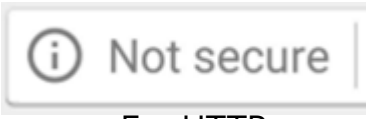


2018年10月 Chrome 70

Webブラウザの表示は今後どうなるのか？

・A. P. Felt 氏の研究紹介１：TLSに関するアイコン表示の変更
「HTTPのアイコン表示変更は徐々に(gradually)進めることにした。」 [SOUPS2016]

・HTTP 警告表示
「HTTP接続のリスクを示すインジケータが無いことは問題である。
クリックすればHTTP接続のリスクが表示されるようなアイコンが必要である。」



For HTTP

「デスクトップは表示スペースがあるため、ユーザ教育のために表示する。」

「HTTPページでは、クレジットカード番号等の入力を避けるよう、ユーザに情報提供する。」

（cf. [W3C2010]「User agents MAY warn users, ~ , if form submissions from a TLS-secured page are directed to an unsecured channel.」）

For invalid HTTPS

・今後の進め方
「人々がインターネットを使うのが恐くならないよう、パニックを与えないよう、
HTTPページの“Not Secure”のラベリングは、プライベートモードから始める等、
徐々に(gradually)進めることにした。」
→開発者ブログの内容から、計画通りに進行されている様子

Webブラウザの表示は今後どうなるのか？

・A. P. Felt 氏の研究紹介１：TLSに関するアイコン表示の変更
HTTPS有無のアイコン表示から、悪意あるサイトの警告アイコン表示へ

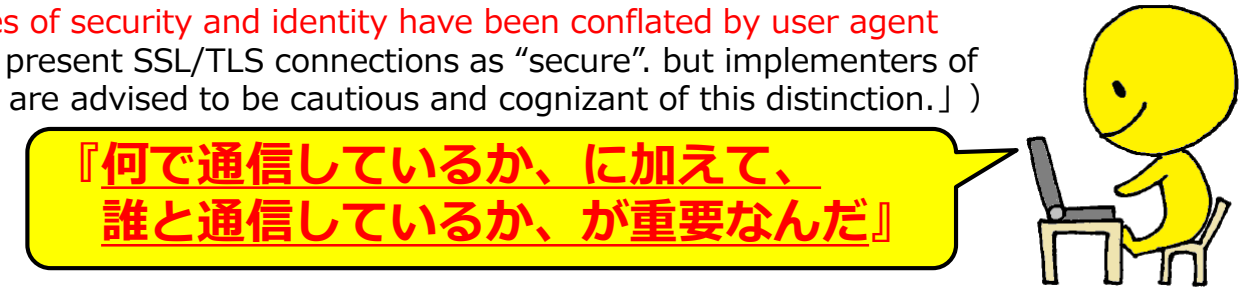
[SOUPS2016]

・HTTPS ”Secure”非表示
「Webサイト自体の信頼性は（もはや）HTTPSか否かでは分からない。
フィッシングサイト等の悪性サイトが HTTPS(主にDV証明書?)を利用している。
一方、ユーザは、緑の鍵マークがサイト自体が悪性でないシグナルと誤認しがちである。
悪性サイトに安全性を強調する緑のカギマークが付いているのは混乱を招く。」

For HTTPS

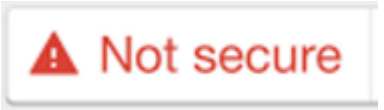
→HTTPSは（単体では）有効なフィッシング対策ではない。
有効な（安全性の）シグナルではない。

（cf. [W3C2010] 「Historically, issues of security and identity have been conflated by user agent interfaces which present SSL/TLS connections as “secure”. but implementers of this specification are advised to be cautious and cognizant of this distinction.」）



・マルウェア＆フィッシングサイトの警告表示
「Edgeは、マルウェア＆フィッシングサイトに警告アイコンを表示している。
Chromeを含め、他ブラウザも同様に警告アイコンを表示すべきと考える。」

→HTTPS有無のアイコン表示から、
悪意あるサイトのブラックリストによる警告表示に向かう可能性



For invalid HTTPS
→For Malicious Site ??

Webブラウザの表示は今後どうなるのか？

・A. P. Felt 氏の研究紹介２：TLSに関する警告画面表示の変更
警告アイコン表示の再考から、警告画面表示の再考へ

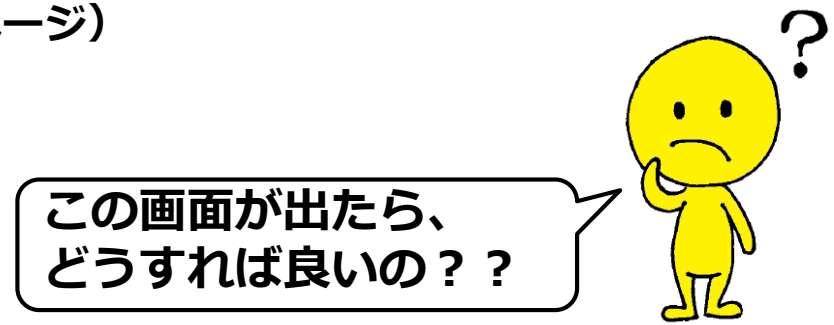
「警告アイコン表示は、ユーザ操作をインタラプトしないため、効果が薄い。」 [CHI2018]
→「多くのブラウザで、ユーザ操作をブロックする警告画面がデフォルトになっている。」
「これまでのブラウザベンダの表示改善により、警告画面の順守率は向上してきた。」
[W3C2010]

「TLSの警告画面は、マルウェア＆フィッシングサイトの警告画面に比べて、
- 非常に多く遭遇する。
- 誤った設定による誤検知が多い。
- （その結果）順守率が低い。」

→「ユーザは”習慣化”して警告画面を無視している。」
[USENIX2013]

→「否。著者らの先行研究はmisleadingであった。
”習慣化”は警告を無視する主要因ではなかった。」
[CHI2018]

（続きは次ページ）

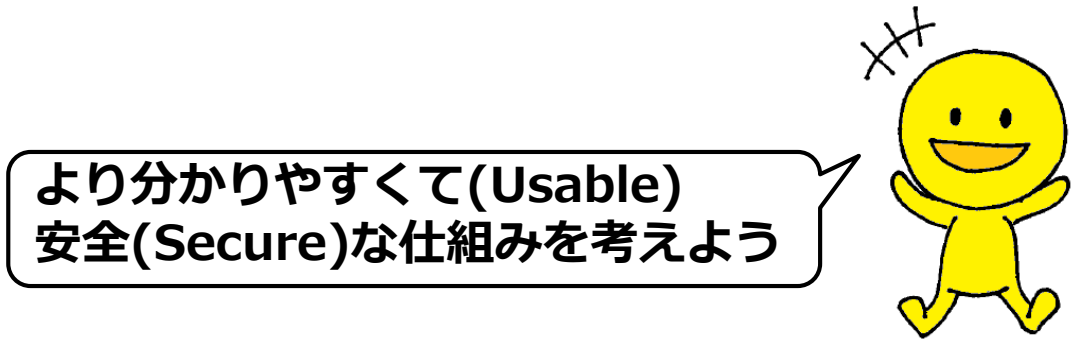


Webブラウザの表示は今後どうなるのか？

・A. P. Felt 氏の研究紹介２：TLSに関する警告画面表示の変更
サイトの証明書リスト&ブラックリストによる警告画面表示へ

「ユーザが警告画面を順守or無視する理由について、 [CHI2018]
”サイトの評判”が警告を無視する主要因であった。
しかし、”サイトの評判が良い”から警告を無視するのは判断誤りである。」
「一度訪問済みのサイトや、普段は評判の良いサイトの警告表示は、
実際の中間者攻撃/危殆化等の危険の兆候の可能性があり、注意が必要である。 [W3C2010]
あるいは、単に設定誤りの場合も多い。」
→（前者の可能性に備えて、CTにより証明書リストを収集していると考えられる。）
→「future workとして、警告画面の再デザインとユーザ教育が必要である。」

「マルウェア警告表示は、TLS警告表示より、重大に捉えられるべきである。 [SOUPS2014]
（誤検知が少ないため＝実際の脅威である可能性が高いため）
ユーザはよく混同するため、上記を区別して警告表示をすべきである。」
→明らかに悪意あるサイトを（ブラックリスト等で）区別して警告表示する方針と考えられる。



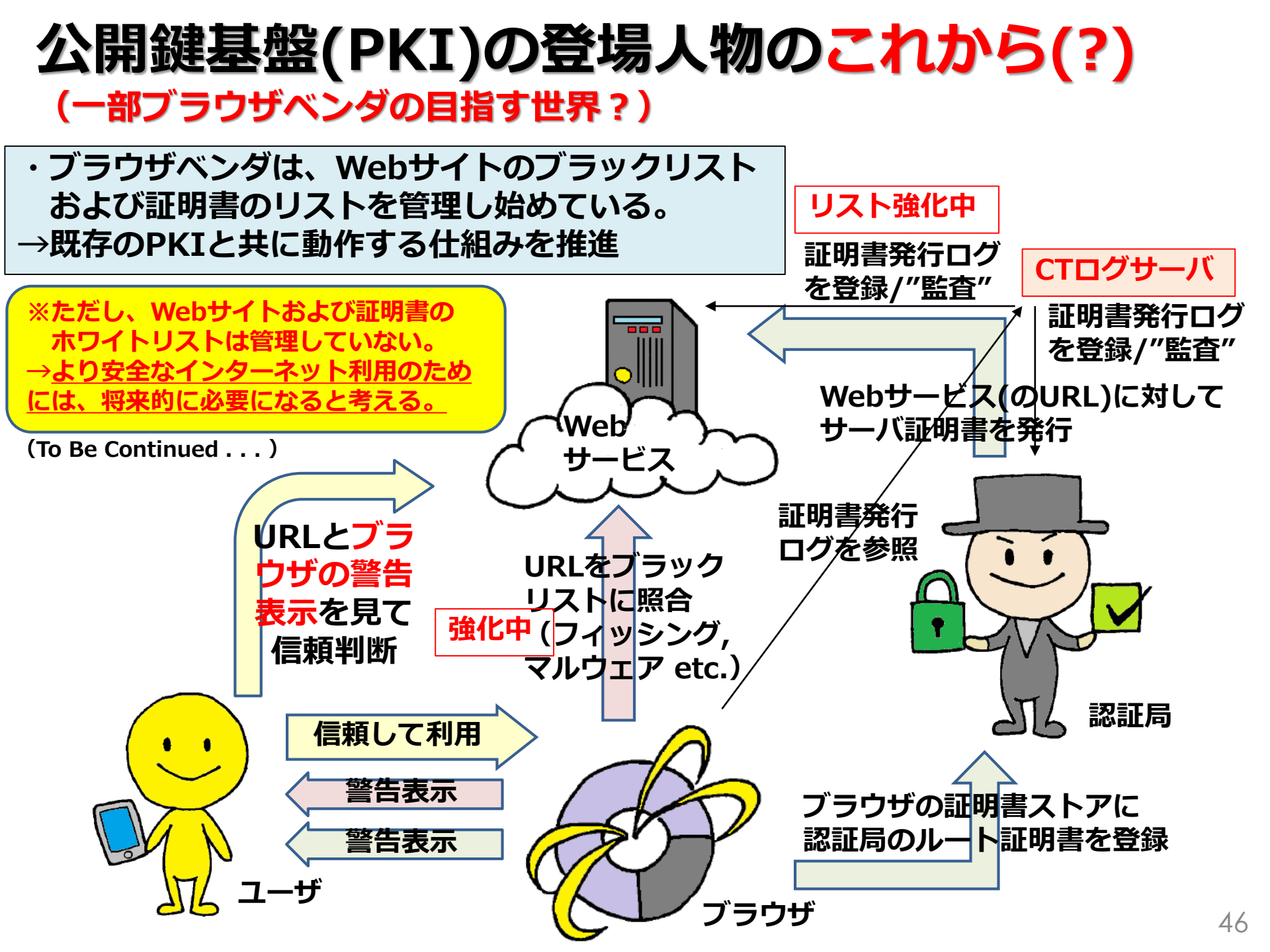
公開鍵基盤(PKI)の登場人物のこれから(?)

（一部ブラウザベンダの目指す世界？）

・ブラウザベンダは、Webサイトのブラックリストおよび証明書のリストを管理し始めている。
→既存のPKIと共に動作する仕組みを推進

※ただし、Webサイトおよび証明書のホワイトリストは管理していない。
→より安全なインターネット利用のためには、将来的に必要になると考える。

(To Be Continued . . .)

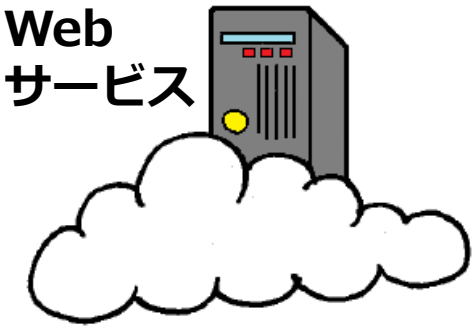


ユーザ

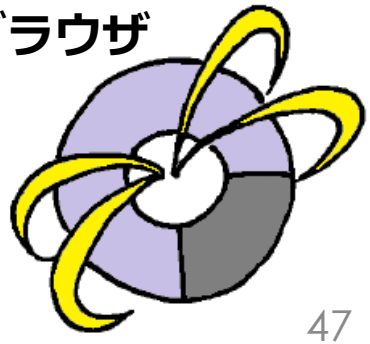
認証局

TLSとWebブラウザの表示のいまとこれから（完）

1章：公開鍵基盤(PKI)のいま
2章：EV証明書の本当の価値
3章：Webブラウザの表示のいまとこれから



Web
サービス

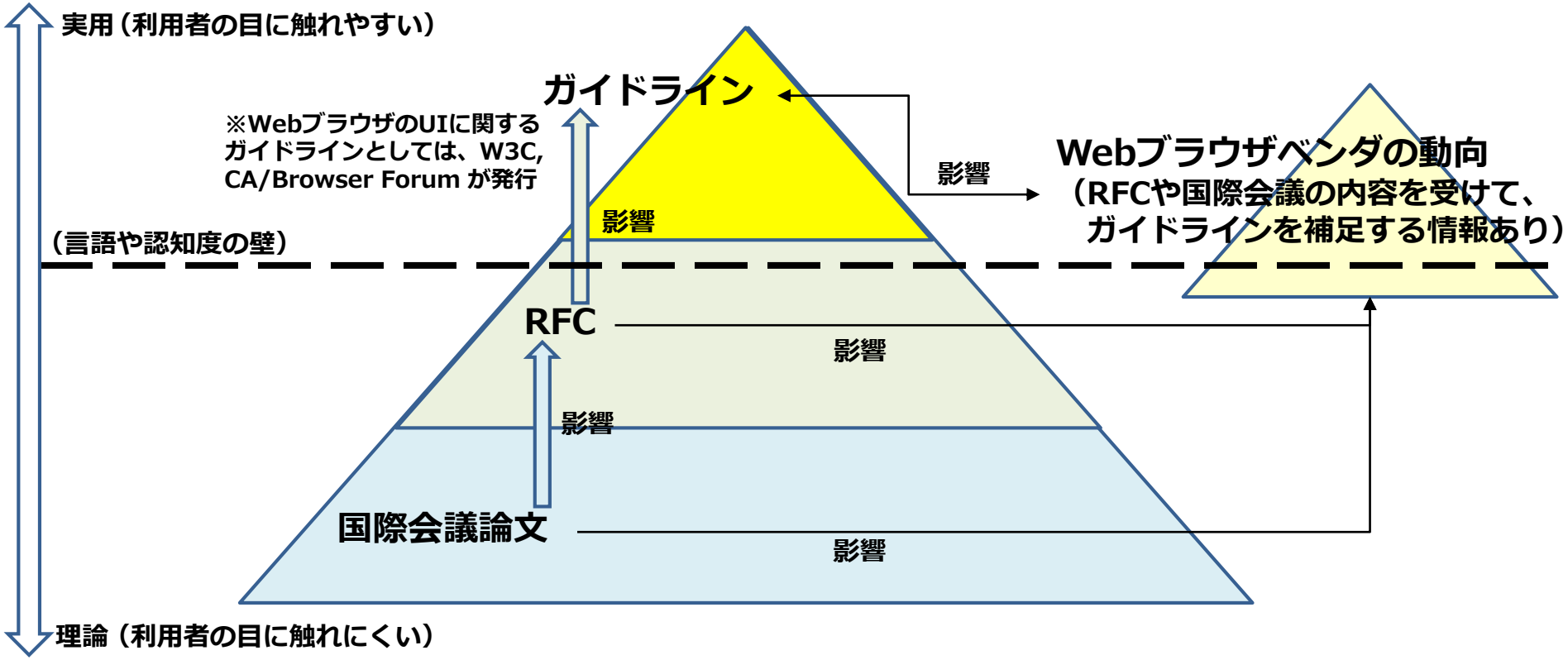


ブラウザ

本講演の目的 再掲

Q. なぜ「TLSとWebブラウザの表示」について知るべきなのか？
A. Webブラウザベンダの動向が、RFCや国際会議の動向を反映しており、Webサイト管理において関連する情報源となっているため。

各情報源の間には力学が存在し、相互に影響を与えている。



・ユーザインタフェース研究は、学術的知見の価値が長いとされる。
→国際会議の動向が、今後のブラウザベンダの動向や、
RFC&ガイドラインに、影響を与えていく可能性がある。
より良いインターネットのために、今後も変化はつづく。

（参考）URL as UI

・ユーザインタフェース研究は、学術的知見の価値が長いとされる。
→1999-2007年の記事に下記の”予言”（一部, 抜粋, 意訳）が述べられている。

©Jakob Nielsen,
URL as UI, 1999 Mar.

・URLは、WebのUIの一部として、もう数年はあり続けるだろう。
そのためには、URLに、UIとして下記が求められる：
短い、覚えやすい、スペルしやすい、タイプしやすい、
サイト構造が分かりやすい、永続性がある、等
・URLは、原理的には、マシン用の仕組みであり、人間が読む必要はない。
（実際には、人間がURL自体を扱うことはよくある。）
・URLは、いずれ使われなくなるだろう（“Domain Names May Die”）
URLが、Webサイト探索に主に使われるのは、あと3-5年か。人間の思考の仕組みに合わない。
ユーザやブラウザの保守性を考慮して、良いURLは、あと10年は重要であり続けるか。

2005年追記：URLはまだ使われている。あと数年は使われるだろう。
しかし、重要性は低下している。ユーザは検索エンジンに
社名/サイト名/ドメイン名を入力することが一般的になっている。
2007年追記：Microsoftの研究で、検索エンジン利用時のアイトラッキングの結果、
ユーザは、利用時間の24%は、検索結果のURLを見ていた。
特にサーチャーは、サイトの信頼性を評価する際、URLを使っている。

→未実現であるが、Nielsen氏の当初主張に共感する。
URLを補完する、人間の認知に合った信頼判断の仕組みは、
いずれ必要になると考える。

（To Be Continued . . .）

Special Thanks

・資料作成のディレクションを頂き、ありがとうございました。
木村様、中島様

・皆様の資料を拝見させて頂きました。ありがとうございました。
島岡様、大津様、漆嶌様、大角様

・サイト利用許可を頂き、ありがとうございました。
NTTレゾナント 広報担当様

・イラスト提供を頂き、ありがとうございました。
長津様

Thank you !