資料5－1

ウェブサイト認証(SSLサーバ証明書)の現状と課題

総務省：トラストサービス検討WG

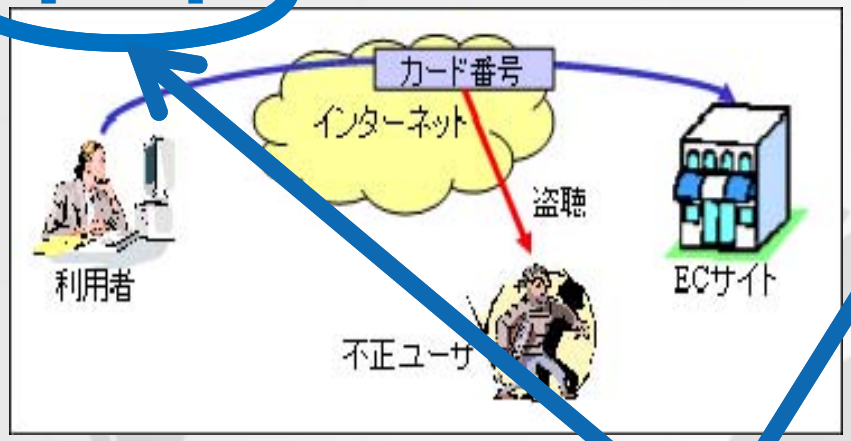
稲葉 厚志 - 2019年4月15日
atsushi.inaba@globalsign.com

GlobalSign®
GMO INTERNET GROUP

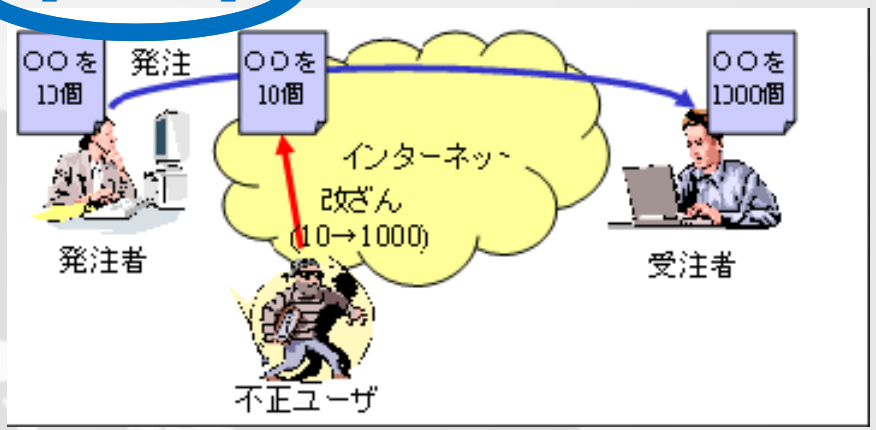
目次

1.1 サーバ証明書の必要性：脅威への対策

[盗聴]

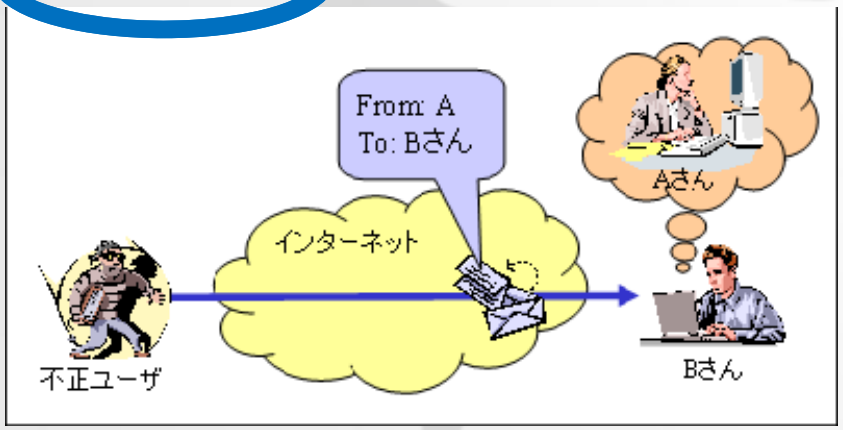


[改ざん]

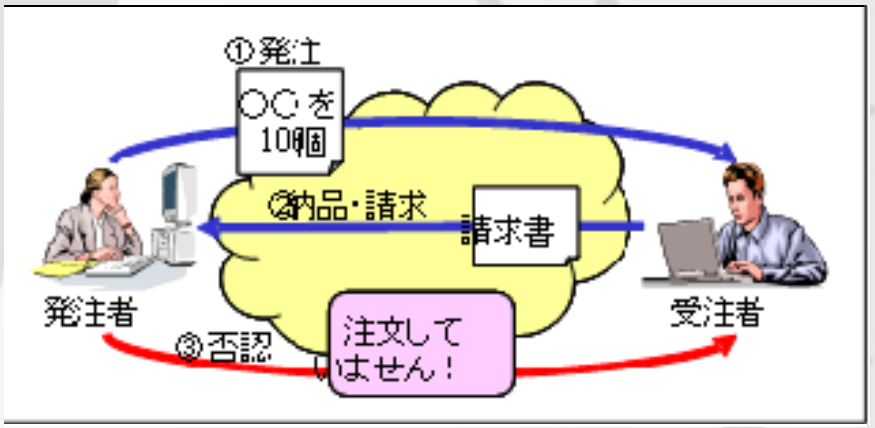


サーバ証明書が有効

[なりすまし]



[否認]

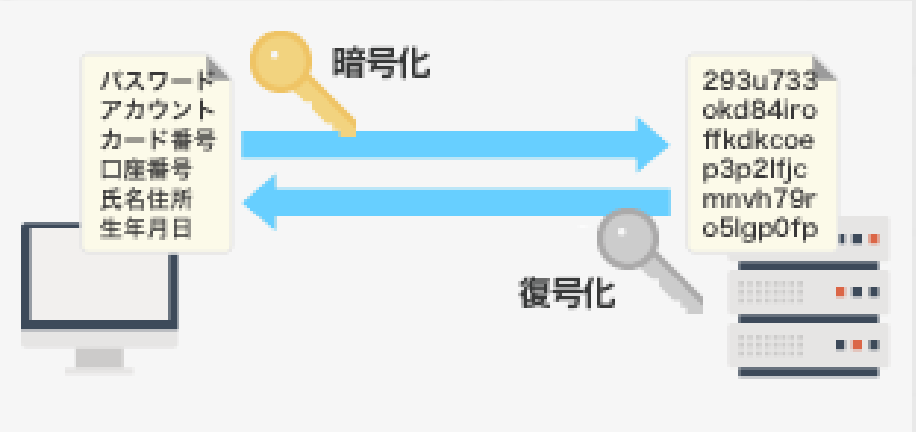


IPA(情報処理推進機構)ウェブサイトより引用

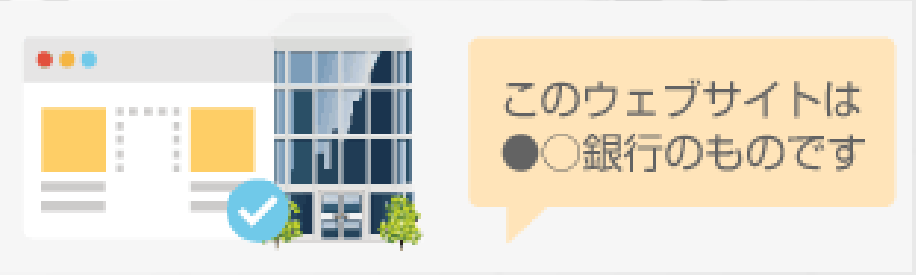
1.2 SSLサーバ証明書の役割

暗号化通信と実在証明の2つの役割をもつ

暗号化通信：
SSLサーバ証明書に記載される証明書所有主体の公開鍵と2つの暗号方式(共通鍵暗号方式・公開鍵暗号方式)を用いて、ブラウザ⇔サーバ間で送受信される個人情報や決済情報などの通信データを暗号化する。暗号化されたデータは、SSLサーバ証明書を導入したサーバで保持する秘密鍵のみでしか解読することができず、悪意ある第三者からの盗聴を防ぐ。



実在証明：
「実在する運営者(組織)によって運営されている本物のウェブサイト」であることが認証局によって認証され、ユーザは自分がアクセスしたウェブサイトが、安心して利用できるウェブサイトであることが確認できる。



1.3 SSLサーバ証明書の種類

SSLサーバ証明書には3つの種類がある

種類	ドメイン認証型	実在認証型	EV SSL
英語表記	Domain Validation	Organization Validation	Extended Validation
略称	DV	OV	EV
利用シーン	個人ブログ、掲示板、イントラネット内の Web サイト、メールサーバ、FTP サーバ	コーポレートサイト、ニュース・情報検索・ナビゲーションサイト、動画・音楽視聴サイト、ソーシャルメディアサイト、金銭のやり取りがない Web サービスサイト	ネットショッピングサイト、インターネットバンキングサイト、オンライン証券サイト、フィッシング詐欺に狙われやすいブランドのコーポレートサイト

2.1 CA/Browser Forum 設立までの経緯(1/2)

CA/Browser Forum 設立までの経緯

■サーバ証明書事業者が登場し始めた頃(1990年代半ば～2000年)
・ルート証明書のブラウザへの搭載要件の変遷
①当初WebTrust ETSIといった第三者機関監査は必須とされておらず基本的に申請すれば搭載された：ブラウザは鍵マークを表示
②Microsoftが認証局・電子証明書サービスの信頼性維持の為2000年頃WebTrust監査を要件化(新規・搭載済ルート証明書共に適用された為搭載されているルート証明書に監査受審済のものと未受審のものが一時期混在していた)
③各ブラウザベンダが個々にルート証明書搭載プログラム(技術・運用要件、申請手続き)を策定し始めた：Microsoft、Mozilla、Google、Apple、SunMicro/Java 等

■Domain Validation SSL(DV SSL)を提供する事業者が登場(2001年)
・それまではOrganization Validation SSLのみ
・DVは、低価格ということもあり普及は進んだものの認証レベルが低い為容易にフィッシングサイトに使用されることがあった：ブラウザはOV、DV共に同じ鍵マークを表示する為ユーザが証明書種別を容易に認識できなかった

2.1 CA/Browser Forum 設立までの経緯(2/2)

■CA/Browser Forumの設立(2005年)

・Microsoft及び主要な商用認証局が協議を行い、https採用サイトのユーザへのわかりやすさ向上を図る為、新たな規格に基づくサーバ証明書仕様を関連業界(ブラウザ、認証局、監査機関等々)が一堂に会して策定していくことを趣旨としCA/Browser Forumが設立された

・「新たな規格に基づくサーバ証明書」として認証プロセスを厳格化したEV-SSLについてガイドラインを策定、ブラウザもEV-SSLであることをユーザに明示する(グリーンのアドレスバー等)ことを目指した

・EV-SSLガイドラインに基づき認証局がEV-SSL証明書を市場へ提供し始めて以降、既存のOV、DVといったサーバ証明書タイプについてもCA/Browser Forumとしてガイドラインを策定しようという機運がForumメンバー内に高まり、認証局各社が個々のルールで既にビジネスを展開していた状況下、新たに業界としてルールを整理する形でBaseline Requirementsを策定し、これ以降パブリック証明書のルール設定機構として認知される存在となった

2.2 CA/Browser Forum構成メンバー

国	CAメンバー
アメリカ	Amazon Trust Services
	DigiCert
	Entrust
	GoDaddy
	Let's Encrypt
	Network Solutions
	OATI
	SecureTrust
	Sectigo (旧Comodo)
	SSL.com
	Visa
	Wells Fargo
イスラエル	ComSign
イタリア	Actalis
インド	eMudhra
エストニア	AS Sertifitseerimiskeskus
オランダ	Digidentity
	ESG de Electronische Signatuur BV
	KPN
	Logius
ギリシャ	HARICA
サウジアラビア	National Center for Digital Certification
スイス	Swisscom
	SwissSign
スペイン	ANF
	Camerfirma

国	CAメンバー
スペイン	Firmaprofesional
	Izenpe
スロバキア	Disig
台湾	Chunghwa Telecom
	TAIWAN-CA
中国	CFCA
	CNNIC
	GDCA
	SHE-CA
チェコ	Prvni certifikacni autorita
ドイツ	D-TRUST
トルコ	E-TUGRA
	Kamu Sertifikasyon Merkezi
	TURKTRUST
日本	GMO GlobalSign
	SECOM Trust Systems
ノルウェー	Buypass
パナマ	TrustCor
バーミューダ	QuoVadis
フランス	CERTIGNA
	Certinomis
	DocuSign
ポーランド	Certum
UAE	Dark Matter
ルーマニア	certSIGN
リトアニア	SSC

Browserメンバー
Apple
Cisco
Comodo Security Solutions
Google
Microsoft
Mozilla Foundation
Opera Software AS
360

協力機関
American Bar Association（アメリカ法曹協会）
AICPA（アメリカ公認会計士協会）
CICA（カナダ勅許会計士協会）
ETSI（欧州電気通信標準化機構）
tScheme（英国トラストサービス標準化・認定組織）

※掲載URL

https://cabforum.org/members/

2.3 CA/Browser Forum 運営と意思決定のプロセス

議論・コミュニケーションの手段

- 電子メール
- ウェブサイト
- 電話会議
- Face to Face ミーティング

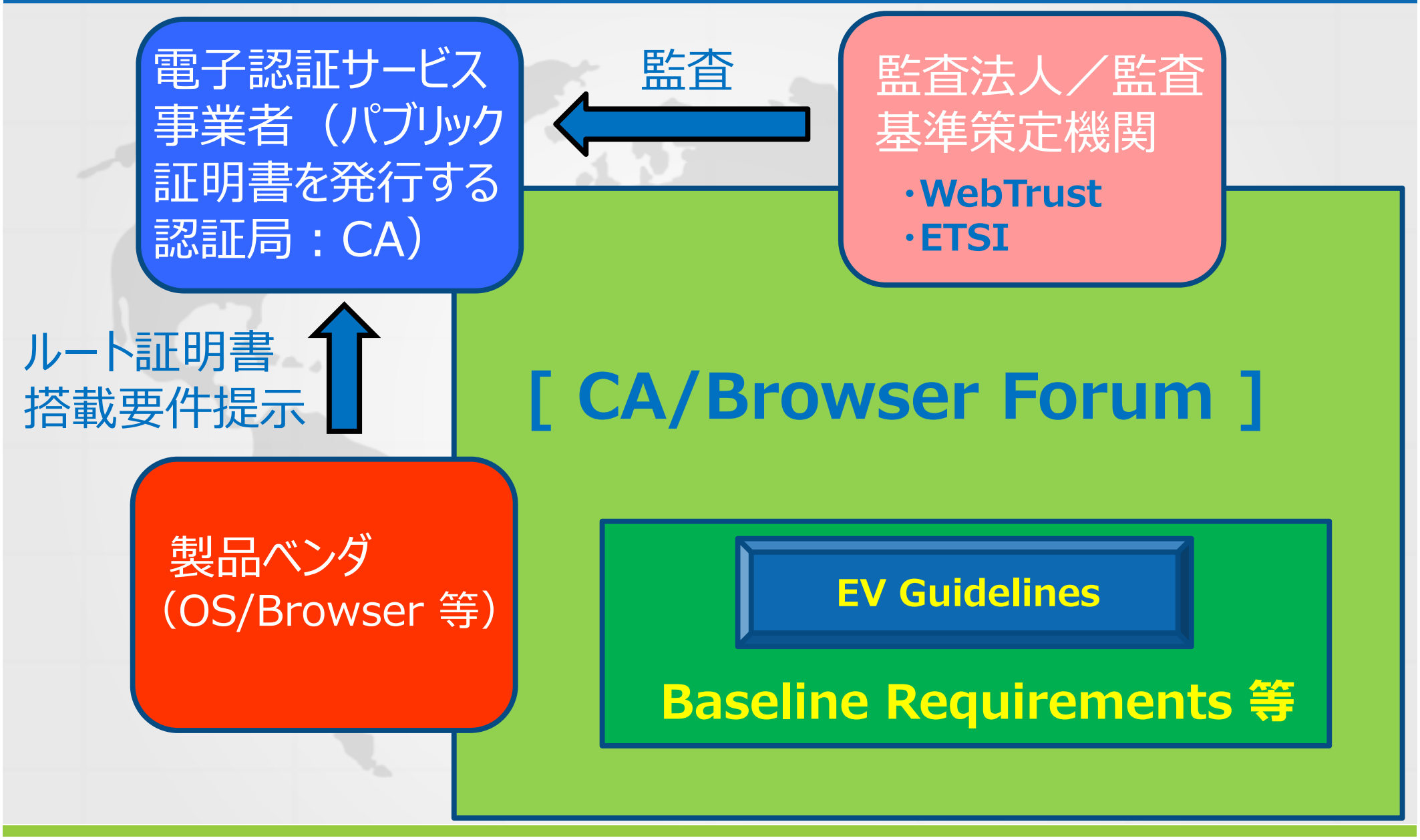
意思決定のプロセス

2.4 CA/Browser Forum 策定ガイドライン

策定したガイドライン等

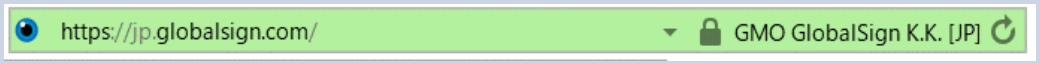
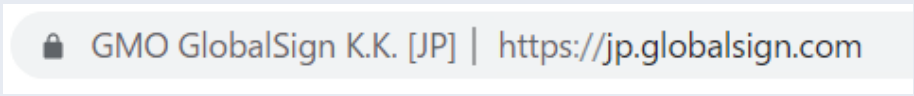
- EV SSL Certificate Guidelines （2007年～）
  - 認証局CP/CPSの書式として用いられるRFC3647に準拠した記載項目
  - 認証局に関わる技術・運用、証明書プロファイル、証明書ライフサイクル、認証プロセス、設備、監査等についての要件
  - EV SSL証明書の発行・管理を行う認証局に求められる要件
- Baseline Requirements (2011年～)
  - 書式及び記載項目構成はEV SSL Certificate Guidelinesと同様RFC3647準拠
  - SSL証明書の発行・管理を行う認証局に求められる要件
- Network Security Requirements (2012年～)
  - EV SSL Certificate Guidelines及びBaseline Requirements を補完する目的で認証局のネットワーク管理、証明書発行管理システムの構成、操作者の権限管理、システムへのアクセスコントロールに関する要件を規定
- EV Code Signing Certificate Guidelines (2012年～)
  - 書式及び記載項目構成はRFC3647準拠
  - EV Code Signing 証明書の発行・管理を行う認証局に求められる要件

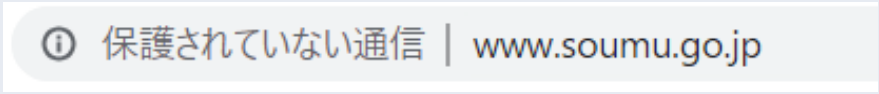
2.5 パブリック認証局とその周辺を取り巻く業界構造



2.6 ブラウザベンダのポリティカルパワー

SSLサーバ証明書を利用に関する検証の手段は主にブラウザ

	EV SSLのアドレスバーの表示
Internet Explorer	
Google Chrome	

	サーバ証明書が未設定のアドレスバーの表示
Internet Explorer	
Google Chrome	

ビジネス推進に認証局ルート証明書のブラウザ製品への搭載が必須の為、ブラウザベンダの発言・発案に対し認証局が真っ向から抗うのが難しい状況がある。このため、ブラウザベンダと認証局は対等とは言えず、認証局はブラウザベンダからのルール改定案に対し、認証局ビジネスや顧客への影響も考慮に入れハードな折衝を強いられているのが現状。

3.1 常時SSL

常時SSL（Always On SSL）は、ウェブサイト内のログインページやフォームなど特定のページだけでなく、その他すべてのページをSSL化することを指す。
常時SSL化はセキュリティ強化だけでなく、ユーザとウェブサイト運営者の双方にさまざまなメリットがある。

【常時SSLの目的（メリット）】

- なりすまし対策
- Cookie情報の盗聴防止
- SEOの順位向上
- 流入元情報解析

上記が主な目的としてあげられる

世の中の潮流が、特定のページへのSSLサーバ証明書の適用から、常時SSLになっている

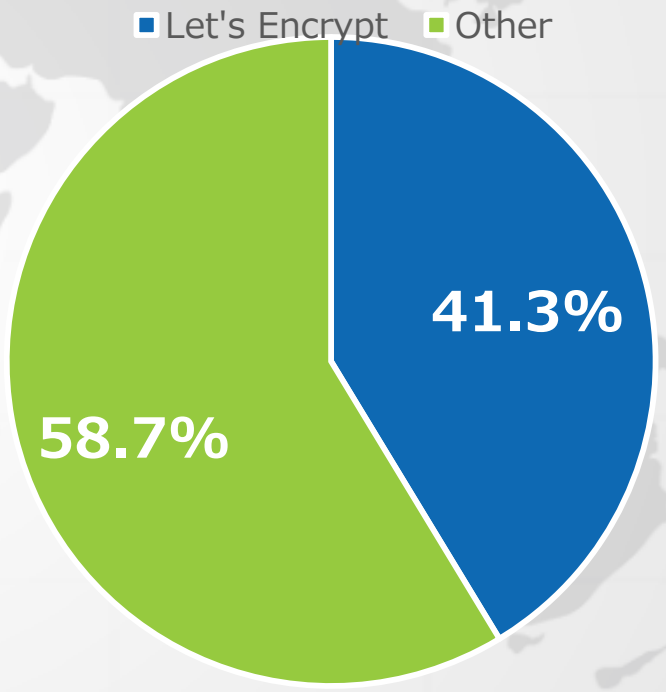
3.2 無償の証明書の台頭

2016年4月、アメリカの非営利団体が運営する認証局(Let's Encrypt)により無償でのSSLサーバ証明書(DV)提供サービスが開始された。

Let's Encryptのサービスは証明書発行プロセスの完全自動化を特徴とし短期間で世界的に導入シェアを拡大した。日本では企業ウェブサイトでの利用が進んできている。グラフはJIPDECが2018年9月に調査をした、「企業等がホームページに設定している Let's Encrypt SSLサーバ証明書の割合」を示したもので、その利用率は41.3%という結果が出ている。

SSLサーバ証明書が設定されたhttpsサイトの増加に貢献する一方で、Let's Encryptの証明書が世界的にフィッシング詐欺サイトに多く利用されているという状況を示すデータも報告されている。（スライド15に掲載）

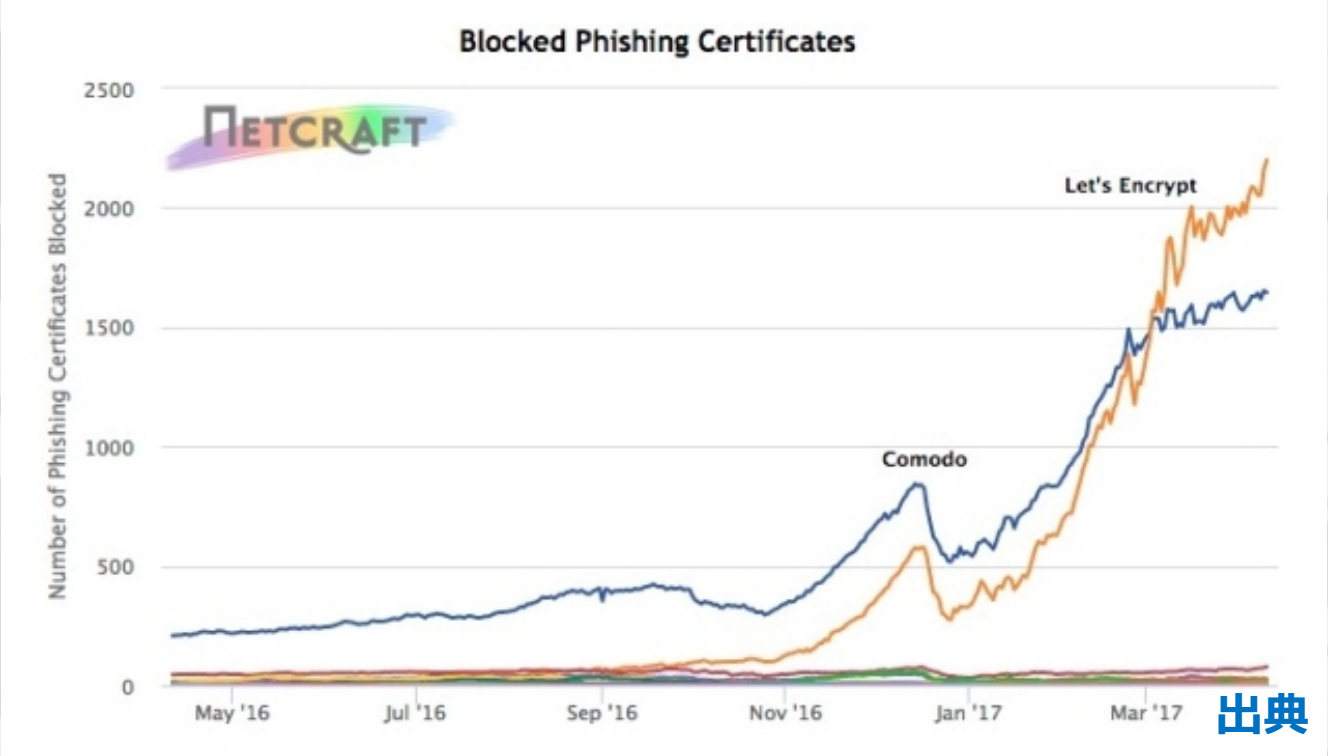
企業等がホームページに設定している
Let's Encryptの割合



JIPDEC2018年9月調査資料

3.3 フィッシング詐欺サイトに利用されるサーバ証明書

フィッシングサイトの約61%はLet's Encryptの証明書が利用されているという結果が出ている。



出典：NetCraft

スライド4に記載した通り、サーバ証明書には「暗号化通信」と「実在証明」の2つの役割がある。
Let's Encryptのサーバ証明書(DV)は暗号化通信はできるものの、実在証明に関してはドメインが登録されていることのみが確認された低レベルで、 証明書を発行する際に認証局が証明書申請組織の実在確認や申請意思確認などを実施するOV/EVと比べ確認プロセスが少ないことからフィッシング詐欺サイトに容易に発行されてしまうため、「なりすまし対策」としての効果がない。

4. eIDAS/Trusted Listと CA/BrowserForumとの位置づけ

Qualified Website Authentication Certificate (QWAC)

- eIDASで規定されたTrust Service のひとつ＝サーバ証明書
- EU Trusted Lists に登録された Qualified Trust Service Provider(QTSP)による厳格な認証プロセスによる証明書発行

CA/Browser Forumの狙い＝EV SSLをQWACと同格化させたい

- QWACは法、EV-SSLは業界スタンダードというギャップが埋めきれず認証プロセスが同レベルにも関わらず”同格”とオーソライズされた状況には至っていないのが現状と認識

現在起きている課題

- EU Trusted List に登録されたQTSPのルート証明書が必ずしも主要ブラウザに搭載されているわけではない＝標準設定のブラウザでQWACウェブサイトへアクセスするとエラーとなる場合がある
- EV SSLにはEVであることを示す識別子が記載されブラウザがEVに対応したユーザインタフェース表示を可能だが、QWACには情報の記載が無いため証明書種類を認識できない
- EV SSLをQualifiedと法的に位置づけられるか及びブラウザでQTSP/QWACをどう扱うかが課題と認識

※補足：アジア地域の動向

・タイのETDA(デジタル経済社会省電子取引開発機構)やインドのCCA(電子情報技術省認証局認定機関)等が参画するAsia PKI Consortiumでは、eIDAS/EUとの認証基盤国際連携フレームワーク実現を検討する為 Legal & Policy Framework WG、Technology & Standards WGが2018年に設置された

ご清聴ありがとうございました

GMOグローバルサイン株式会社
(法人番号：1011001040181)
〒150-8512
東京都渋谷区桜丘町２６－１　セルリアンタワー
https://jp.globalsign.com/

GlobalSign®
GMO INTERNET GROUP