フィッシング対策協議会
Council of Anti-Phishing Japan

S/MIMEの普及啓発における活動について

フィッシング対策協議会
証明書普及促進WG 主査
田上 利博（サイバートラスト株式会社）

証明書普及促進WG の活動

技術による利用者の保護

●Webサイト 常時SSL/TLS化 時代突入
- 常時SSL対応率：87.2%*

●身元証明に対するニーズの高まり
- 利用者は、いまだフィッシング詐欺に対して安全ではない状態

価値を正しく訴求する

●複雑な証明書技術
- 主要ブラウザのTLS1.0/1.1無効化
- DV / OV / EV サーバー証明書の違い

●証明書が果たしている役割を明らかに
- 証明書が果たすメリットを正しく理解いただき健全なウェブサイト運営維持
- メール送信者の実在性証明

コンセプト

電子証明書を活用した実在証明の有効性を啓発

それが、みんなにとっての安全につながる

業界を横断する啓発活動

業界団体としての啓発が重要

サイバートラスト株式会社
GMOグローバルサイン株式会社
セコムトラストシステムズ株式会社
デジサート・ジャパン合同会社
トッパン・フォームズ株式会社
キヤノンマーケティングジャパン株式会社
一財）日本情報経済社会推進協会（JIPDEC）
株式会社日本レジストリサービス（JPRS）
一般社団法人JPCERTコーディネーションセンター

実現に向けた行動

ベストプラクティスの集積
- IPA『SSL/TLS 暗号設定ガイドライン』
- NIST SP800シリーズなど

ケーススタディの公開

利用者：信頼できる安全なウェブサイトは
アドレスバーが『社名』
事業者：安全安心で本物のウェブサイトは
アドレスバーが『社名』

達成目標

無関心層へのアプローチ方法確立

<ガイドライン / 啓発情報の公開>
- 事業者に証明書の有用性について啓発
- 安全なウェブサイト運営に必要となる証明書の活用方法を啓発
- メール送信者の実在性証明についての啓発

* https://www.feedtailor.jp/report_aossl/

証明書普及促進WG の役割

- フィッシング対策においては、利用者に対して事業者が高い信頼性を示すことが重要
- 技術策としての証明書の有用性について事業者へ理解を促すことで普及促進を図る
- 安全なウェブサイト運営に必要となる証明書の活用方法を周知する
- メール送信者の実在性証明について普及啓発する

利用者向け啓発コンテンツ

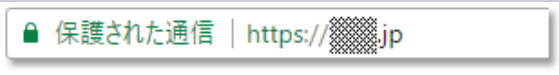
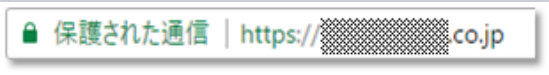
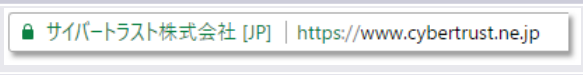
■ ブラウザ毎のサーバー証明書の表示の違い

ブラウザ	証明書なし	DV証明書	OV証明書	EV証明書
Google Chrome (Windows) Ver. 65.0.3325.162	▒▒▒▒▒▒.co.jp	保護された通信 | https://▒▒▒.jp	保護された通信 | https://▒▒▒▒▒▒.co.jp	サイバートラスト株式会社 [JP] | https://www.cybertrust.ne.jp
Google Chrome (Android) Ver. 65.0.3325.109	▒▒▒▒▒▒.co.jp	https://▒▒▒.jp	https://▒▒▒▒▒▒.co.jp	https://www.cybertrust.ne.jp
Microsoft Edge Ver. 41.16299.15.0	▒▒▒.co.jp	▒▒▒.jp	▒▒▒.co.jp	サイバートラスト株式会社 [JP] cybertrust.ne.jp
FireFox Ver. 59.0.1	▒▒▒▒▒▒.co.jp	https://▒▒▒.jp	https://▒▒▒▒▒▒.co.jp	GMO GlobalSign, Inc. (US) | https://jp.globalsign.com
Safari (Mac) Ver. 11.0.3	▒▒▒.co.jp	▒▒▒.jp	▒▒▒.co.jp	GMO GlobalSign, Inc.
Safari (iOS) Ver. 11.0.3	▒▒▒▒▒▒.co.jp	▒▒▒.jp	▒▒▒.co.jp	GMO GlobalSign, Inc.

https://www.antiphishing.jp/news/info/_ssl_20191021.html

事業者向け啓発コンテンツ

- SSL / TLS サーバー証明書のユースケースついて
- 各サーバー証明書の利用指針、利用例等のユースケースについて情報公開

	DV（ドメイン認証）	OV（組織認証型）	EV（Extended Validation）
証明書の説明	• ドメイン名の登録権のみを確認して発行する証明書 • 組織の実在性は確認されませんが、通信内容の暗号化は OV・EV 同様に行わる	• ドメイン名の登録権の他に、Web サイトの運営組織が実際に存在するかどうか、証明書の申請者がその組織に所属するかを審査した上で発行する証明書 • Web サイトの運営者が誰なのかがわかるので、Web サイトの信頼性が向上します	• OV 証明書よりも厳格な審査 (組織の法的な登録の確認など) の基に発行する証明書 • EV 証明書に対応する Web ブラウザでは DV / OV とは異なりアドレスバーが緑色に変色するため、Web サイトの閲覧者に一目で安全性をアピールできます
表示例			
利用指針	• 個人情報やクレジットカード番号などの重要情報を入力しない Web サイト • 誰が運営しているかを確認する必要のない、重要ではない Web サイト • インターネットに公開せず特定の人しか閲覧しない内部ネットワークにある Web サイト	• クレジットカード番号や口座番号など金銭のやり取りに必要な情報を入力しない Web サイト • 公開する情報に信頼性を持たせる必要のある Web サイト • 個人情報など一般公開したくない情報の入力が必要な Web サイト	• クレジットカード番号や口座番号など金銭のやり取りに必要な情報を入力する Web サイト • Web サイトのブランドや安全性をよりアピールしたい Web サイト
利用例	• 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

https://www.antiphishing.jp/news/info/_sslusecase_20180329.html

S/MIME署名の利活用に関する普及啓発

- 電子署名付き電子メールの普及啓発
  - S/MIME署名対応メールソフトの調査、公開
  - フィッシング対策ガイドラインの要件として明記
    - 利用者が正規メールとフィッシングメールを判別可能とする対策【要件１】
      - 利用者が確認できるように利用環境と分かりやすい説明に配慮した上で、どのように確認すればいいのかを分かりやすく端的に説明すること。
  - （今後）事業者および利用者向けS/MIME署名に関する啓発
  - （今後）DMARC（SPF/DKIM含む）とS/MIMEとの違い、それぞれの利用用途やメリット、デメリットに関する啓発

S/MIMEのメーラー別対応状況の調査結果

- メーラー別のS/MIME対応状況の調査結果公表
- S/MIME未対応メーラーを狙った攻撃事例の啓発

メーラー名	OS	メーラーのバージョン/ Webブラウザのバージョン	S/MIME電子署名		S/MIME暗号化	
			受信(検証)	送信	受信(復号)	送信
Outlook（アプリ）	Windows10 Pro	2008	○	○	○	○
Outlook（Webブラウザ）	Windows10 Pro	（edgeのバージョン:91.0.864.59）	○	○	○	○
Outlook（アプリ）	iOS 14.6	4.2124.0	○	○	○	○
Outlook（アプリ）	Android 11	4.2123.2	○	○	○	○
Thunderbird（アプリ）	Windows10 Pro	78.11.0	○	○	○	○
Gmail（Webブラウザ）無料版	Windows10 Pro	（Chromeバージョン:91.0.4472.114） （Firefoxのバージョン:89.0.2）	○	×	×	×
Gmail（アプリ）無料版	iOS 14.6	6.0.210530	○	×	×	×
Gmail（アプリ）無料版	Android 11	2021.05.16.380255809	○	×	×	×
Yahoo!メール（アプリ）	Android 11	4.11.2	×	×	×	×
Yahoo!メール（アプリ）	iOS 14.6	8.6.0	×	×	×	×
Yahoo!メール（Webブラウザ）	Windows10 Pro	（Firefoxのバージョン：89.0.2）	×	×	×	×
iPhone標準メール（アプリ）	iOS 14.6	ー	○	○	○	○
		対応数	9	6	6	6
		対応割合	75.0%	50.0%	50.0%	50.0%

フィッシング対策協議会
Council of Anti-Phishing Japan

ご清聴ありがとうございました

フィッシング対策協議会
@antiphishing_jp
フィッシング対策協議会は2005年4月に発足いたしました。海外、特に米国を中心として大きな被害を生んでいるフィッシング詐欺に関する事例情報、技術情報の収集及び提供を中心に行うことで、日本国内におけるフィッシング詐欺被害の抑制を目的として活動しております。
http://www.antiphishing.jp/

- フィッシング対策協議会　事務局 (JPCERT/CC内)
  - Email：antiphishing-sec@jpcert.or.jp