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

SSL サーバー証明書に関する
事業者ならびに利用者向けアンケート調査結果

2017 年 9 月

フィッシング対策協議会
証明書普及促進ワーキンググループ
https://www.antiphishing.jp/

目次

1. はじめに

フィッシング対策協議会 証明書普及促進ワーキンググループは、電子証明書を活用した実在証明書の有効性を普及啓発し、インターネットを安心安全に利用できるよう推進しています。

WEB サイトは SEO 対策の観点から、小規模事業者も含め SSL サーバー証明書を導入（*1）し、また常時 SSL/TLS 化を行う WEB サイトが増える傾向にあります。しかし、上位 30 万サイトにおける SSL 対応率は 13%（*2）と低いのが現状です。

インターネット利用者はオンライン詐欺（フィッシングやなりすましサイト）に対し脆弱な状況であり、DV SSL サーバー証明書（ドメイン認証による審査発行されるサーバー証明書）がオンライン詐欺サイトに利用されているケースも多く見受けられます。この状況下において、サーバー証明書が果たしている役割や効果を利用者ならびに事業者に正しく理解していただき、健全なサイトを利用および運営することが望ましいと考えます。

電子証明書の技術によって利用者を保護できるように、各種アンケート調査、ケーススタディの公開等、普及啓発に努めてまいります。

*1. http://httparchive.org/trends.php#perHttps

*2. http://googlewebmastercentral-ja.blogspot.jp/2014/08/https-as-ranking-signal.html

2. 「SSL サーバー証明書に関する事業者ならびに利用者向けアンケート調査」の概要

2.1. 調査目的

本アンケート調査では、EC サイト、ネットバンキング等のＷＥＢサイト（システム）の管理、運用者（以下、事業者）と EC サイト、ネットバンキング等のＷＥＢサイト利用者（以下、利用者）を調査対象者として、SSL サーバー証明書に対する意識を調査し、今後の継続調査ならびに当協議会における活動、サーバー証明書の適正な普及啓発、促進を目的としています。

2.2. 調査概要

予備調査により、事業者に対して「SSL サーバー証明書がどのようなものか知っているか」について、また利用者に対して「インターネット上での商品購入・サービス利用の際に意識して注意していること何か」についてアンケート調査を行いました。本調査の事業者向けでは、SSL サーバー証明書について認知されている方を対象に、利用者向けでは、EC サイトやネットバンク等を利用されている方を対象に SSL サーバー証明書に対する意識調査を行いました。

2.3. 実施時期

- 予備調査
  - 事業者向け：2017 年 2 月 14 日～15 日
  - 利用者向け：2017 年 2 月 10 日～13 日
- 本調査
  - 事業者向け：2017 年 2 月 16 日～17 日
  - 利用者向け：2017 年 2 月 16 日

2.4. 調査方法

当協議会独自に調査項目を作成し、外部調査システムを利用し Web システムでアンケート調査を実施した。

2.5. 実施対象者

事業者向け：20 歳以上の EC サイト、ネットバンキング等のＷＥＢサイト（システム）の管理、運用者
利用者向け：20 歳以上の EC サイトやネットバンキング等の利用者

2.6. 回答数

事業者向け：218 件
利用者向け：222 件

3. 調査結果

3.1. 事業者向け

事業者向けアンケート

A) SSLサーバー証明書の認知度などに関するセクション

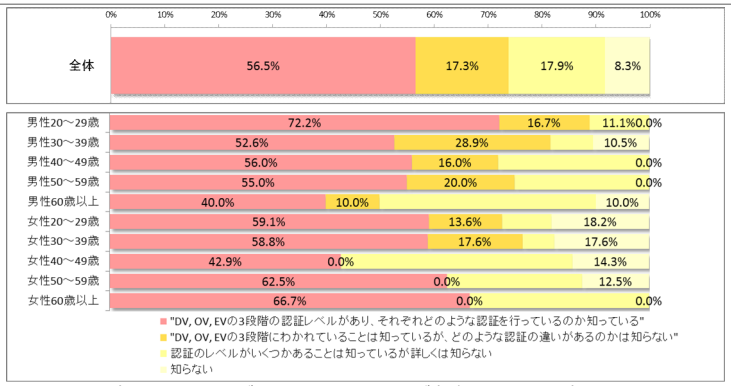
1

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

事業者向けアンケート結果(1/13)

Q1 SSLサーバー証明書の認知に関する質問

あなたは、SSLサーバー証明書は認証のレベルが3段階にわかれていることを知っていますか？



解説・考察

- レベルの違いを詳しく知っている人が半数おり、レベルが存在することを知っている人も35%おり、認証レベルの認知度は高いと言える。
- 実際、Q2の結果を見るとよく知られている通信暗号化、https化、錠前マークは3/4以上が、EVのアドレスバー緑色変色や組織認証は1/3が認知しており、回答内容が正確であることが伺える。

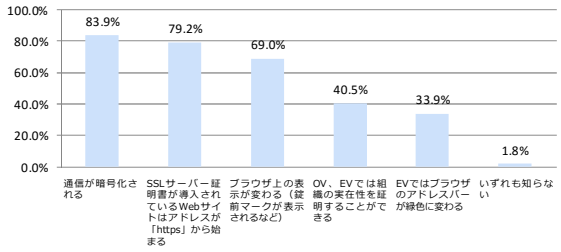
2

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

事業者向けアンケート結果(2/13)

Q2 SSLサーバー証明書の認知に関する質問

SSLサーバー証明書を導入することで、以下の選択肢のような効果が生じます。あなたが、知っていることを全て選択してください。



解説・考察

- 通信の暗号化とhttps/錠前マークの表示はよく知られている。これはインターネットバンキング・ショッピングなどのHPで説明を見かけ、周知の機会が多いことが認知度が高い要因と思われる。
- 逆に組織認証やアドレスバー変色は、認知度が低い傾向である。

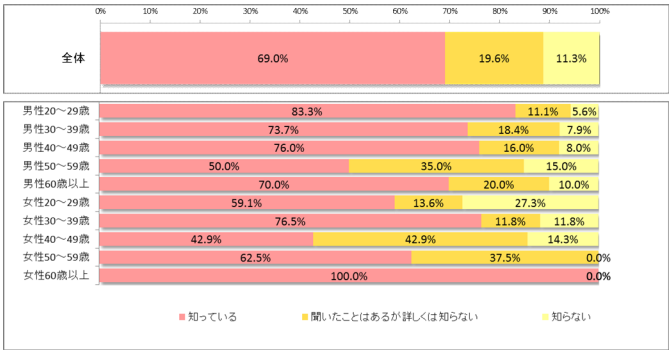
3

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

事業者向けアンケート結果(3/13)

Q3 SSLサーバー証明書の認知に関する質問

あなたは、無料でSSLサーバー証明書が発行可能なサービスがあることを知っていますか？（例：Let's Encryptなど）



解説・考察

- IT系ニュースでも取り上げられたこと、無料という響きからかよく知られており、興味の高さが伺える。
- 認知度の高さから今後利用される可能性が高いとも考えられるため、実際に利用するうえでの注意事項などは情報提供する必要がある。

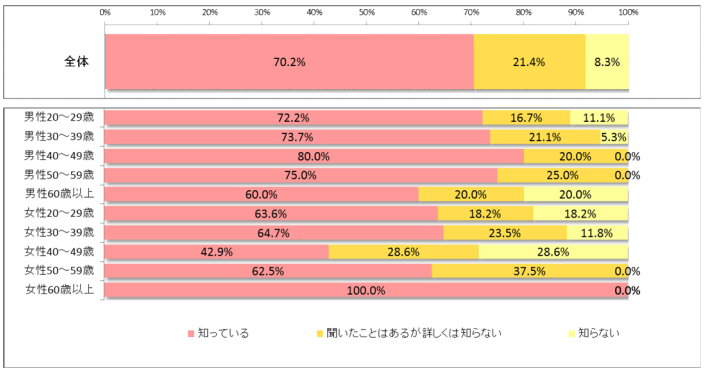
1

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

事業者向けアンケート結果(4/13)

Q4 SSLサーバー証明書の認知に関する質問

SSLサーバー証明書は認証局という組織から発行されます。あなたは、認証局という組織の役割を知っていますか？



解説・考察

- 予想した以上の人が知っていると回答されている。
- サーバー証明書が単に購入するだけのものではなく、審査など事務手続きが必要であることから認知度が高いと思われる。

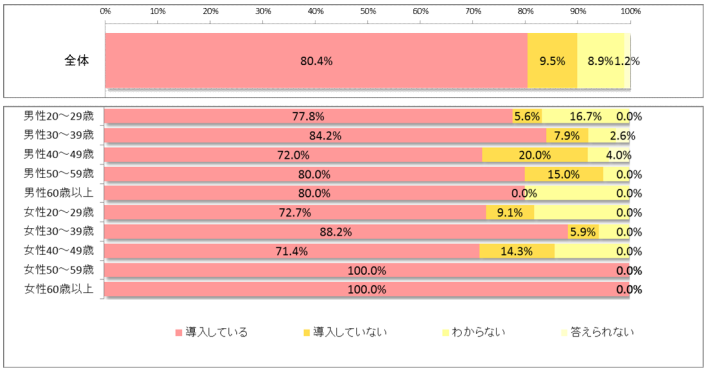
5

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

事業者向けアンケート結果(5/13)

Q5 SSLサーバー証明書の認知に関する質問

自社のWebサイトやWebサービスへSSLサーバー証明書を導入していますか？※注：一部でも導入している場合は「導入している」と選択してください。



解説・考察

- 一般の普及率(50%以下)から見ると、今回のアンケート対象であるECサイト、ネットバンキングの管理・運用者は導入率が高い。
- 取り扱う情報の機密性の高さを認識されていることが伺える。

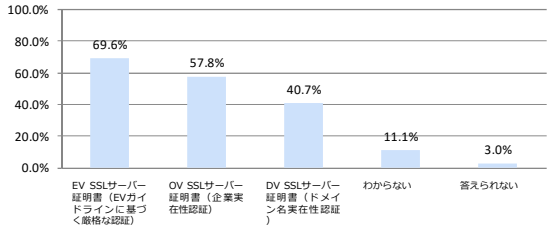
6

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

事業者向けアンケート結果(6/13)

Q6 SSLサーバー証明書の導入状況に関する質問

自社で導入しているSSLサーバー証明書の種類はどれですか？該当するサーバー証明書の種類をすべて選択してください。



解説・考察

- EVの利用率が多い。ECサイトでありアドレスバーが緑色になることを意識している。
- Q2で緑色になることを知っている人が少ない結果から、アドレスバーの変色ではなくEVであること自体を認識して導入していることが伺える。

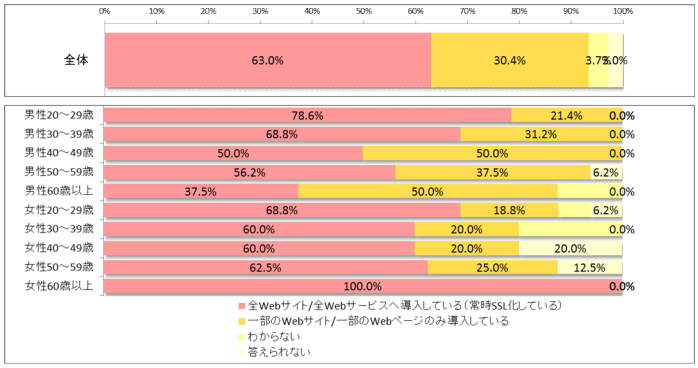
7

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

事業者向けアンケート結果(7/13)

Q7 SSLサーバー証明書の導入状況に関する質問

自社でSSLサーバー証明書を導入している範囲を教えてください。



解説・考察

- 常時SSL化したところが予想よりも多い。
- 常時SSLの啓発活動の成果か、一部SSL化のメリットが低下して相対的に上昇している。

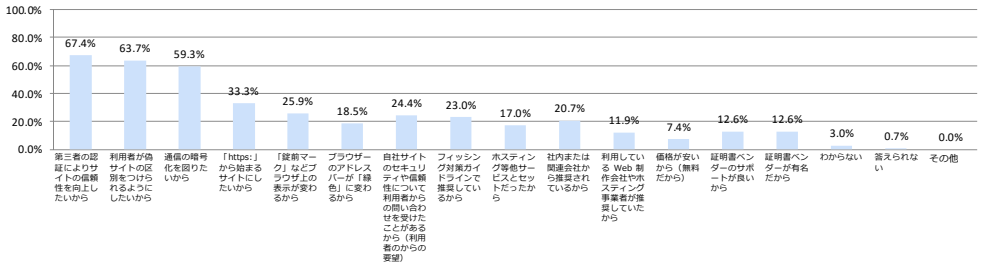
8

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

事業者向けアンケート結果(8/13)

Q8 SSLサーバー証明書の導入状況に関する質問

自社でSSLサーバー証明書を導入している理由について、該当するものを全て選択してください。



解説・考察

- 証明書の役割として信頼性向上と通信暗号化についての認知度が高い。
- 他の質問の傾向を見るとEVについて知っている人の割合は多いが、アドレスバーが緑色になることは余り意識されていない模様。
- 漠然とした役割を理解されている状態で、具体的な表示については認識が低い。

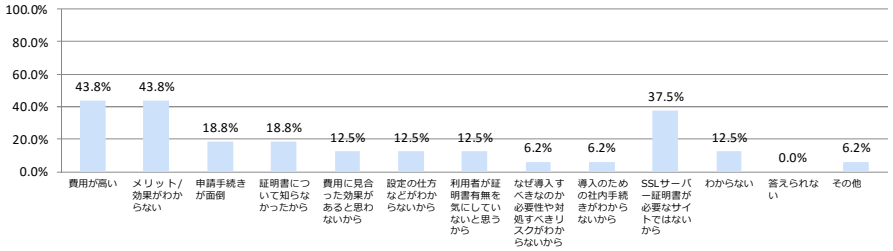
9

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

事業者向けアンケート結果(9/13)

Q9 SSLサーバー証明書の導入状況に関する質問

自社のWebサイトやWebサービスにSSLサーバー証明書を導入していない理由を教えてください。



解説・考察

- 費用が高いが、44%、メリットが分からないが44%。
- メリットがわからないについては啓発活動の必要性があり、申請・審査手続きの面倒さなどは認証局ベンダーの課題か。

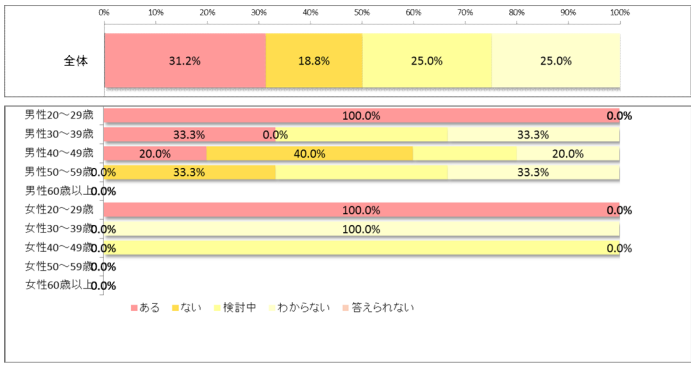
10

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

事業者向けアンケート結果(10/13)

Q10 SSLサーバー証明書の導入状況に関する質問

自社のWebサイトやWebサービスへSSLサーバー証明書を今後導入する予定の有無を教えてください。



解説・考察

- あるが31%、ないが19%。
- 予定がある・検討中を合せると50%以上となり、証明書をまったく利用しないところは少ないといえる。

11

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

事業者向けアンケート

B) アンケート回答事業者に関するセクション

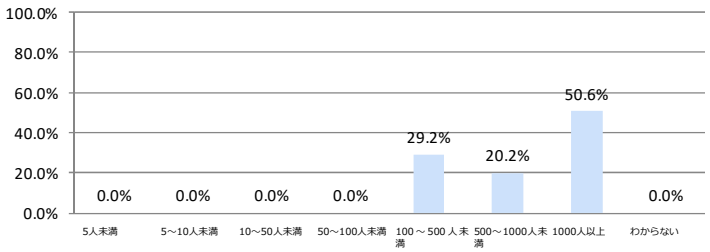
12

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

事業者向けアンケート結果(11/13)

Q11 アンケート回答事業者に関する質問

あなたのお勤め先の企業の規模（従業員数）を教えてください。



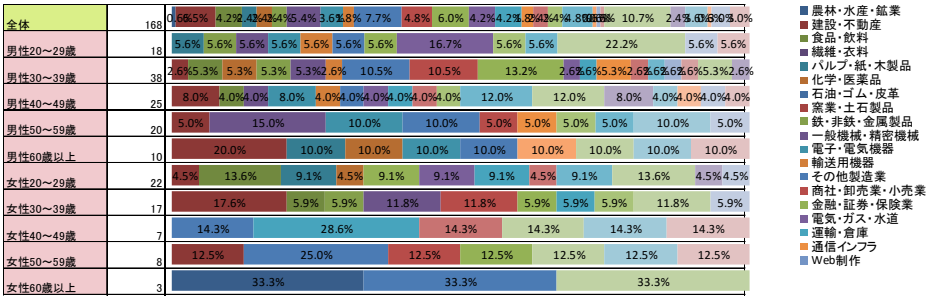
13

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

事業者向けアンケート結果(12/13)

Q12 アンケート回答事業者に関する質問

あなたのお仕事の業種を教えてください。



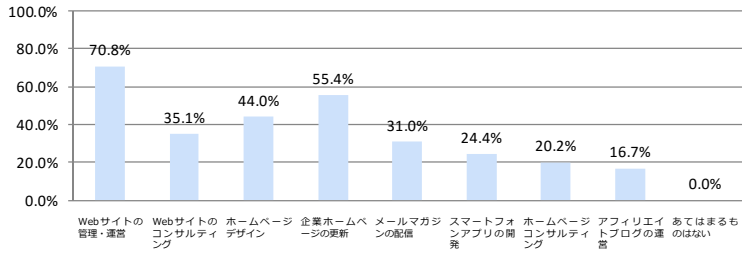
14

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

事業者向けアンケート結果(13/13)

Q13 アンケート回答事業者に関する質問

あなたが現在、携わっているお仕事をお答えください。



15

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

3.2. 利用者向け

利用者向けアンケート

A) SSLサーバー証明書の認知度などに関するセクション

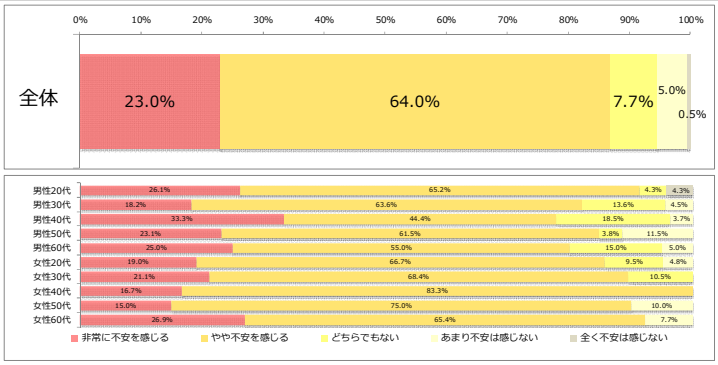
1

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

利用者向けアンケート結果(1/9)

Q1 インターネット利用時のセキュリティ意識に関する質問

インターネット上の様々なサービスを利用する際、あなたは、個人情報の漏洩について不安を感じることはありますか？



解説・考察

- インターネット利用者において、性別年齢を問わず、個人情報の漏洩に対する脅威（「不安」や「やや不安」を感じる）と感じている傾向」にある。

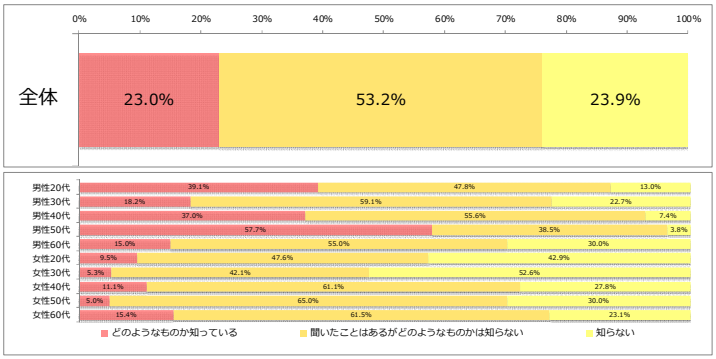
2

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

利用者向けアンケート結果(2/9)

Q2 SSLサーバー証明書の認知度に関する質問

あなたは、SSLサーバー証明書とはどのようなものか知っていますか？



解説・考察

- SSLサーバー証明書の認知は、利用者の半数が聞いたことはある程度に留まり、約1/4は認知もされていないことから、SSLサーバー証明書の認知は決して高いものとは言えない。
- ネットバンキング経験者でも「どのようなものか知っている」と回答したのは30.6%に留まっている。

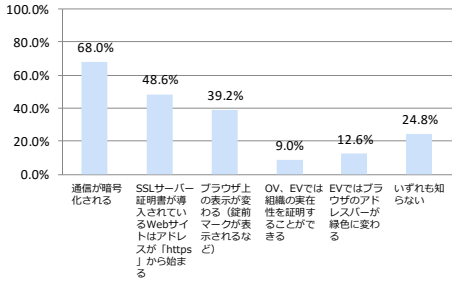
3

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

利用者向けアンケート結果(3/9)

Q3 SSLサーバー証明書の効果に関する質問

SSLサーバー証明書が導入されているサイトでは、以下の選択肢のような効果が生じます。あなたが知っていることを全て選択してください。（複数回答）



解説・考察

- SSLサーバー証明書の効果に対しては、通信暗号化などの理解が約7割と高かったが、その証明書の種類（OV,EV等）の違いへの関心は低く、認知者は全体の1割に留まる。

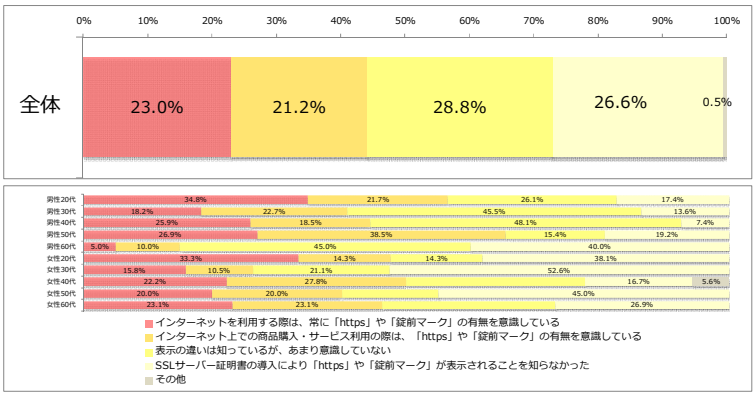
4

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

利用者向けアンケート結果(4/9)

Q4 SSLサーバー証明書の表示の違いに対する意識に関する質問

SSLサーバー証明書が導入されているWebサイトはアドレスが「https」から始まるようになり、合わせて錠前マークが表示されるようになっています。インターネット上のさまざまなサービスを利用する際、あなたは、この表示の違いは意識していますか？



解説・考察

- Webサイトのアドレス表記の「https」における錠前マーク表示を知らない利用者が半数近くいる傾向が全世代で出ているものの、年齢が高いほど、錠前マークの存在も知らない傾向にある。

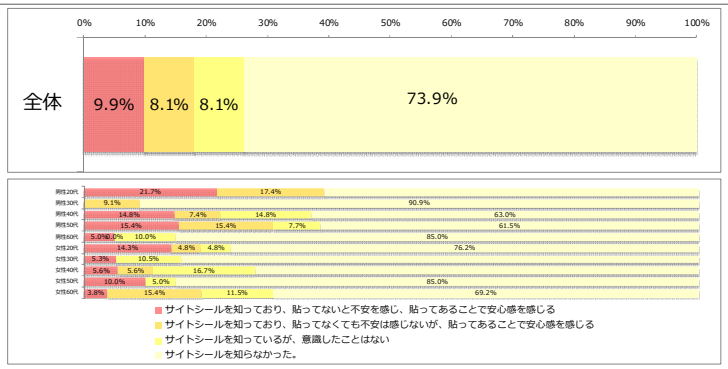
5

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

利用者向けアンケート結果(5/9)

Q5 サイトシールに関する認知度・理解度に関する質問

SSLサーバー証明書が導入されているWebサイトには、証明書が導入されていることを示し、証明書の詳細情報等を見ることができる以下の画像のような「サイトシール」と呼ばれる画像が貼ってあることがあります。サイトシールについて、あなたはどう思いますか？



解説・考察

- 証明書のサイトシールの存在は実に全体の3/4は知らないと回答し、認知度が低い傾向が顕著である。

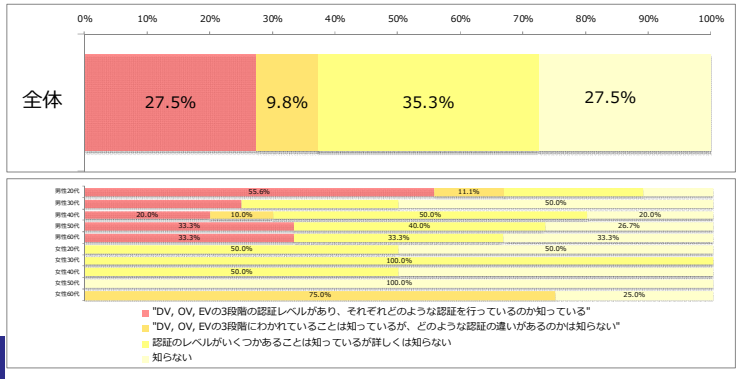
6

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

利用者向けアンケート結果(6/9)

Q6 DV/OV/EVの3段階の認証レベルの認知度に関する質問

SSLサーバー証明書とはどのようなものか知っていると回答した方にお伺いします。あなたは、SSLサーバー証明書は認証のレベルが3段階にわかれていることを知っていますか？



解説・考察

- SSLサーバー証明書の認証レベルが3段階に分かれていることについても、全般的に認知されていなく、比較的男性20代が把握しているに留まっている。

7

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

利用者向けアンケート

B) インターネットの利用状況に関するセクション

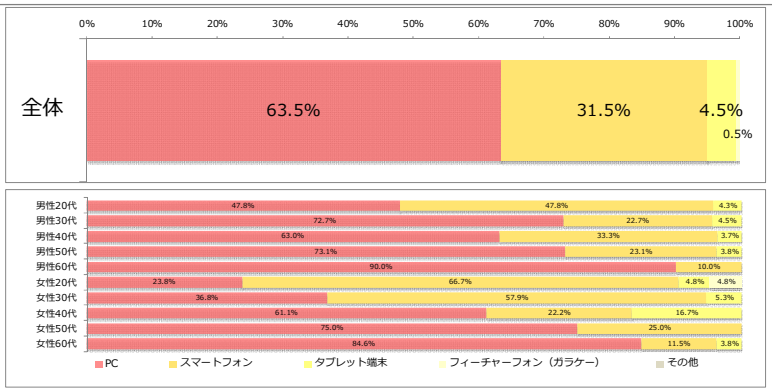
8

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

利用者向けアンケート結果(7/9)

Q7 インターネット利用時の端末に関する質問

あなたが、インターネットを利用する際に主に使う端末はどれですか？



解説・考察

- インターネットを利用する主な端末の傾向は、PCが全体の6割強を占めスマートフォンが全体の3割強であるものの、年代毎に見ると、年齢が高いほどPC利用が高く、年齢が低いほどスマホ利用が高い傾向にある。従って、長期視点で見ると、スマートフォンの比重がより高くなっている傾向と考えられる。

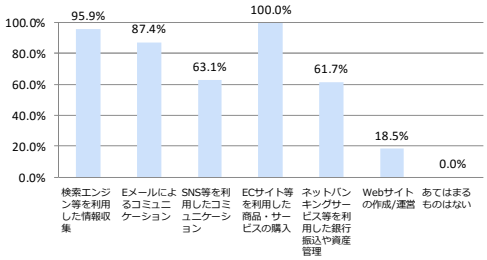
9

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

利用者向けアンケート結果(8/9)

Q8 インターネット利用経験に関する質問

あなたが、インターネット上で実施された経験があることを全て選択してください。



解説・考察

- インターネット利用経験では、ECサイト利用が全体の100%であり、次いで検索、Eメール、SNS、ネットバンキングとなる。特にECサイトを利用した商品・サービスの購入が全年代で100%を占め、生活に密着した用途としてインターネットが浸透している傾向にある。

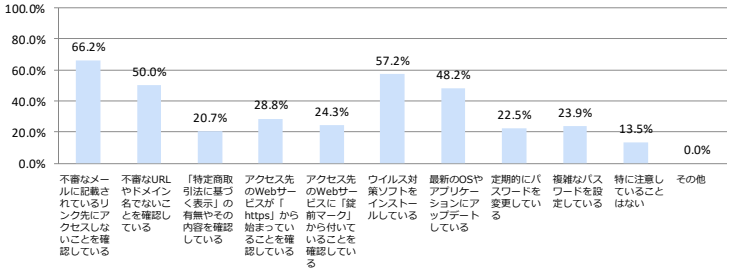
10

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

利用者向けアンケート結果(9/9)

Q9 インターネット利用時の意識に関する質問

インターネット上での商品購入・サービス利用の際に、あなたが意識して注意していることはなんですか？あてはまるもの全てを選択してください。（複数回答）



解説・考察

- インターネット利用時の商品購入やサービス利用の際に留意している点は不審メールや不審なURL等に半数近くが気を配っており、ウィルス対策ソフトやOS/アプリのアップデートなども半数近くの方は定期的に実施する等セキュリティ意識の高さを伺える。
- また、年齢層が高くなるほど意識して注意している項目数が多い傾向にある。インターネット利用経験が短い若い利用者に対する啓発の必要性をあらためて認識した。

11

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

4. まとめ

事業者向けアンケート調査の SSL サーバー証明書の導入によって生じる効果について（Q2）の回答結果では、「通信が暗号化される」（83.9%）、「アドレスが https:から始まる」（79.2%）、「錠前マークが表示される」（69.0%）の順に回答が多かった。
しかし、「EV ではブラウザのアドレスバーが緑色に変わる」（33.9%）という回答結果と、自社で導入している SSL サーバー証明書の種類（Q6）「EV SSL サーバー証明書」（69.6%）にギャップが見られる結果となった。
また、サーバー証明書を導入していない理由（Q9）では、「メリット／効果がわからない」が多く今後の啓発活動の必要性を感じられる結果となった。

利用者向けアンケート調査の SSL サーバー証明書がどのようなものか知っているか（Q2）の回答結果では、半数が聞いたことはある程度にとどまり、約 4 分の 1 には認知されていないことから SSL サーバー証明書の認知は決して高くはなく、またネットバンキング経験者でも「どのようなものか知っている」と回答した利用者が 30.6%にとどまる結果となった。
SSL サーバー証明書の導入によって生じる効果について（Q3）の回答結果では、「通信が暗号化される」（68.0%）、「アドレスが https:から始まる」（48.6%）、「錠前マークが表示される」（39.2%）の順に回答が多かったが、そのサーバー証明書の種類（OV, EV 等）の違いへの関心は低く、認知者は全体の 1 割程度にとどまった。

事業者ならびに利用者に、サーバー証明書が果たす役割や効果を正しく理解していただくための普及啓発活動を実施することで、健全なウェブサイトの運営ならびに利用ができるものと考えています。

5. 付録

5.1. SSL/TLS 入門

5.1.1.SSL/TLS とは

SSL（Secure Sockets Layer）TLS（Transport Layer Security）は、ネットワーク上で送受信されるデータを暗号化する通信技術です。個人情報・口座番号・クレジットカード番号などの重要なデータをインターネット上でやり取りする際に、SSL/TLS にてこれらを暗号化することにより、万が一悪意ある第三者からの盗聴があった場合でも、内容の解読や改ざんを防ぎます。

5.1.2.SSL と TLS の違い

「SSL/TLS」と表記される理由は、この 2 つのプロトコルが開発され、発展してきた歴史にあります。元々、Netscape Navigator という高機能ブラウザを開発したネットスケープコミュニケーションズ社が、SSL（Secure Sockets Layer）を開発しました。SSL1.0 は脆弱性が発見されたため、実装されることはありませんでしたが、改良された SSL2.0 が Netscape Navigator 1.1 に実装されたことで、一般のユーザに SSL が広まりました。

SSL はバージョン 3.0 までが開発されましたが、1999 年には SSL3.0 を元にした「TLS（Transport Layer Security）1.0」が定められました。
SSL3.0 と TLS1.0 は、仕様の違いもごくわずかで仕組みがほぼ同じですが、既にこの時点で SSL という名称が広く使われていたために、「SSL/TLS」「TLS/SSL」のように両者を併記する方法が使われ、「TLS のことも含めて SSL と呼ぶ」という慣習が生まれました。

現在最新バージョンとして広く普及しているのは、2008 年 8 月に制定された TLS1.2 ですが、既に開発から 7 年が経過したバージョンです。
このため、すぐにリリースされる予定ではありませんが、HTTP/2 などの新しいプロトコルの登場などを背景とした TLS 1.3 が提案されています。

5.2. SSL/TLS のこれまでの歩み

SSL 1.0	リリース前に脆弱性が発見され公開されず
SSL 2.0	1994 年リリース
SSL 3.0	1995 年リリース
TLS 1.0	1999 年リリース

TLS 1.1	2006 年リリース
TLS 1.2	2008 年リリース
TLS 1.3	ドラフト策定中 ※2017 年 7 月現在

5.3. SSL/TLS に関する脆弱性の問題

初めて開発された SSL1.0 は、リリース前に脆弱性が発見され公開に至りませんでした。
その後開発された SSL2.0 では、製品に実装された後に脆弱性が発見され、多くのウェブブラウザで SSL2.0 を無効とする初期設定が行われました。

ごく最近まで広く使用されていた SSL3.0 は、2014 年に重大な脆弱性である「POODLE(CVE-2014-3566)」が発見されました。このため、現在ではサーバーでの SSL3.0 の利用は非推奨とされ、また多くの主要ブラウザで SSL3.0 が無効となりました。

また POODLE(CVE-2014-3566)においては、実装が不十分な TLS1.0/1.1 の場合も、サーバーとの通信において脆弱性があることが確認され、TLS1.0/1.1 の利用は非推奨となっております。

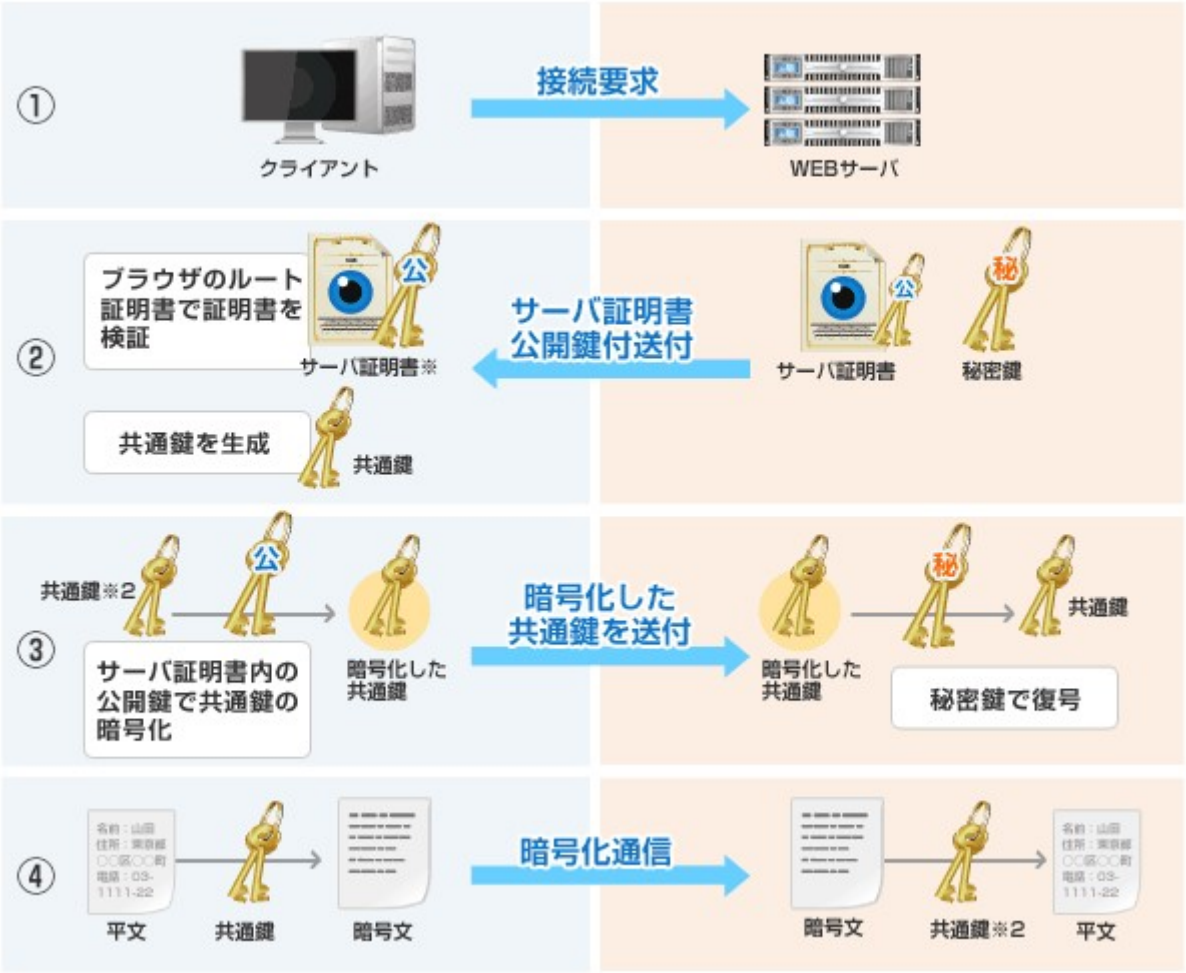
この他、2014 年・2015 年に発覚した OpenSSL の脆弱性「Heartbleed」「FREAK」など、場合によっては OpenSSL のアップグレードやサーバー証明書の入れ替えが必要になるケースもありました。

SSL/TLS 通信を行なっていても「絶対にデータが漏えいしない」とは言えない場合があります。
SSL/TLS の脆弱性についての最新情報の収集や、サーバー証明書の設定状況の確認など、常に「できるだけ安全性の高い通信を行う」「万が一のデータ漏えい、改ざんなどに備える」ということを、心がける必要があります。

Heartbleed（2014 年 4 月）	OpenSSL の暗号ソフトウェアライブラリ上で発見された脆弱性
POODLE（2014 年 10 月）	SSL3.0 と一部の TLS1.0/1.1 の脆弱性
FREAK（2015 年 3 月）	OpenSSL(0.9.8zd 未満・1.0.0p 未満の 1.0.0 バージョン・1.0.1k 未満の 1.0.1 バージョン）と、Apple の SSL/TLS 通信における脆弱性

5.3. SSL/TLS 暗号化通信の仕組み

サーバー証明書を導入することで実現可能な暗号化通信は、クライアント側が共通鍵を使って暗号化したデータをサーバー側に送り、サーバー側は事前にクライアント側から送られた共通鍵を使ってデータを復号します。公開鍵、秘密鍵はクライアント・サーバー間で事前に共通鍵を安全に授受するために使用されます。



5.4. 接続要求

クライアント側 PC のブラウザから、https://～で始まるセキュアなウェブサイトへアクセスします。

5.5. サーバー証明書（公開鍵付き）送付

サーバー側から証明書がクライアントに送付され、クライアントのブラウザに搭載されているルート証明書で署名を確認し、送られてきた証明書を検証します。 もしルート証明書がブラウザに搭載されていない場合は警告が表示されます。（なりすまし防止）

5.6. 暗号化した共通鍵を送付

クライアントは通信データの暗号化に使用可能な暗号の種類をサーバーに通知し、共通鍵暗号方式を選択します。クライアントが暗号用の共通鍵を生成し、サーバーの公開鍵で暗号化して送ります。暗号化された共通鍵はサーバー側の秘密鍵で復号化されます。

5.7. 暗号化通信開始

双方が共通鍵(セッションキー）を用いて、SSL 暗号化通信が行われます。共通鍵には、サーバーとクライアントが使用するブラウザの双方が対応する、最も強度の高い暗号方式・鍵長が使用されます。

5.8. SSL/TLS サーバー証明書とは

5.8.1.SSL/TLS サーバー証明書の役割

サーバー証明書とは、ウェブサイトの所有者の情報、送信情報の暗号化に必要な鍵、発行者の署名データを持った電子証明書です。サーバー証明書の最も基本的な役割は「SSL/TLS 暗号化通信」と「組織の実在性確認」であり、サーバー証明書を導入すると「なりすまし」「盗聴」「改ざん」という 3 つのリスクを防ぎ、ユーザに安心してウェブサイトを利用してもらうことができます。

5.9. SSL/TLS サーバー証明書の役割とリスク防止

5.9.1.SSL/TLS サーバー証明書の　2 つの役割

その１　暗号化通信

ユーザが入力した個人情報や決済情報などを暗号化します。万が一途中で盗聴されても、悪意ある第三者に内容が知られることはありません。

その２　組織の実在性確認

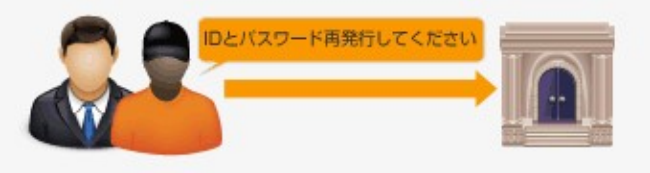
ウェブサイトの運営者・運営組織が実在することを、グローバルサインなどの認証局が確認します。

5.9.2.SSL/TLS サーバー証明書で防ぐ 3 つのリスク

オンラインショッピング・ネットバンキングなどのウェブサービスが普及した昨今、その便利さの反面様々なリスクが伴い、中でも「なりすまし」「盗聴」「改ざん」という 3 つのリスクは「個人情報の漏えい」に直結し、企業の信頼問題にも発展しかねません。
しかし、サーバー証明書を導入することで、この 3 つのリスクを回避することができ、ユーザに安心してウェブサイトを利用してもらうことができます。

なりすまし

なりすましは、第三者が正当な取引主体になりすまして、取引を行うといった行為です。なりすましの事例としては「フィッシング詐欺」が多く話題となっており、本物そっくりに作った銀行やショッピングサイトなどのホームページを使って、個人情報や決済情報などを入手しようとします。
サーバー証明書を導入することで、ウェブサイトを運営している組織がなりすましや架空でない本物の組織であることが認証され、ブラウザに鍵のマークが表示されたり、アドレスバーが緑色になるなど、ユーザが安心してウェブサイトを利用できるようになります。



盗聴

盗聴は、インターネット上でやり取りされる個人情報や決済情報、Cookie など、悪用される危険性のあるデータを第三者が盗み見する行為です。
サーバー証明書を導入することで、重要な個人情報や決済情報は暗号化され、万が一途中で盗聴されても内容は解読されません。
また、フォームやショッピングカート等の特定のページのみならず、ウェブサイト全体に SSL を導入することで、ウェブサイトへの全てのアクセスが暗号化され、Cookie の盗聴を防止することができます。

改ざん

ユーザ登録や注文画面などで入力した内容等が途中で書き換えられるのが「改ざん」です。
例えば、ある商品を 100 個発注したはずが、誰かがデータを書き換えて 1000 個発注したことにしてしまう、というような事態です。
サーバー証明書を導入することで、重要な個人情報や決済情報は暗号化され、万が一途中でデータが盗まれた場合でも、内容が書き換えられないようになっております。

5.10. 参考情報

サイバートラスト：https://www.cybertrust.ne.jp/sureserver/productinfo/sha1ms.html
GMO グローバルサイン：https://jp.globalsign.com/blog/2016/ssl_sha1_sha2_transition.html
シマンテック：https://www.symantec.com/ja/jp/page.jsp?id=ssl-sha2-transition
セコムトラストシステムズ：
https://www.secomtrust.net/service/pfw/news/oshirase20140926.html#01

6. ワーキンググループメンバー

本アンケート調査を行ったフィッシング対策協議会 証明書普及促進ワーキンググループの構成は次のとおりです（2017 年 8 月時点）。

主査	田上利博（サイバートラスト株式会社）
副主査	稲葉厚志（GMO グローバルサイン株式会社）
副主査	駒場一民（一般社団法人 JPCERT コーディネーションセンター）

＜グループメンバー＞
田島悟志（NTT コミュニケーションズ株式会社）
山本健太郎（一般社団法人 JPCERT コーディネーションセンター）
林正人（株式会社シマンテック）
川田晋嗣（セコムトラストシステムズ株式会社）
加藤孝浩（トッパン・フォームズ株式会社）
杉田修（一般財団法人日本情報経済社会推進協会）
新井亮（株式会社日本レジストリサービス）
白岩一光（株式会社日本レジストリサービス）