58のEV証明書のゆくへ

須賀 祐治[1,a)]

概要：ある業界の決済システム等の企画・運営を行っている協会に属する正会員の Web サイトを調査対象として SSL/TLS サーバ設定に関する報告が行われている．広報用に広く公開された FQDN（これを Top FQDN と呼ぶ）で SSL-enable なサイトは 115 であり，このうち脆弱であると認識されてい SSL2.0 が未だに有効となっているサイトは 4.3%，SSL3.0 が有効なサイトは 34.8%も存在した．一方で顧客向けにのみ提供されるログインを必要とするサイトにおける調査では Top FQDN と比較して芳しい結果が得られており組織側の自助努力が垣間見られた．具体的には SSL2.0 有効サイトは無く SSL3.0 有効サイトは 3 サイトのみであった．このとき Top FQDN としては 115 サイトが存在したが，アウトソーシングサービスを利用しているため同じ FQDN に複数の組織のログインサービスが提供されているため，トータルで 58 の FQDN が調査対象となっており 58 全てのサーバにおいて EVSSL 証明書が配備されていた．そのうち 53 の証明書は同一商用認証機関から発行されており，このまま使い続けると近々，ある特定の主要ブラウザにおいて脆弱であると判断され，EV 証明書として本来機能するべきグリーンバーが表示されないことが予想されている．
ブラウザベンダーのアナウンスによると，既に 2018 年 3 月より開発者向けブラウザではエラー表示がされており，2018 年 9 月 13 日にリリース予定の通常版ブラウザでも警告が表記されることとなる．実際に現在も利用されている証明書は有効期限が切れる前に，ブラウザ表記が失効状態と同様の振る舞いとなるため管理者が気が付かないまま運用されてしまう可能性もある．本稿では現在使われている証明書の特徴について分析を行うとともに，2018 年 5 月中旬までの証明書移行の状況について報告する．

Whereabouts of 58 EV certificates

Yuji Suga[1,a)]

2014 年より Alexa Top Sites から .jp ドメインを抽出した URL リストを利用して SSL/TLS サーバのクローリングを行う定点観測を行っており，SSL/TLS バージョンや Export-grade 暗号アルゴリズムの利用率改善に関する調査を行ってきた．特に証明書に着目すると，最近ブラウザのセキュリティインディケータの表記方針が変更になったことから，本来 URL 表記部分に緑のバーが表示される EVSSL 証明書を利用しているにも関わらず安全ではないと判断されるサイトも散見された．これは，本来安全であるにも関わらずコンテンツ不備により安全ではないと表記されてしまう問題であり，コンテンツ管理を適切に行えば改修できる．一方で 2017 年 3 月にブラウザのバグとして取り上げられた問題においてはサーバ証明書の構造に応じて正しい表記になっていない状況が約 1 ヶ月続いていた．証明書ベンダーからサーバ証明書の再発行が可能であることがアナウンスされていたが EVSSL 証明書の差し替えを行っていない，もしくはこの問題に気がついていなかったサイトが多く見られた．

この状況について，ある業界の決済システム等の企画・運営を行っている協会に属する正会員の Web サイトを調査対象として報告が行われている．広報用に広く公開された FQDN（これを Top FQDN と呼ぶ）で SSL-enable なサイトは 115 であり，このうち脆弱であると認識されてい SSL2.0 が未だに有効となっているサイトは 4.3%，SSL3.0 が有効なサイトは 34.8%も存在した．一方で顧客向けにのみ提供されるログインを必要とするサイトにおける調査では Top FQDN と比較して芳しい結果が得られており組織側の自助努力が垣間見られた．具体的には SSL2.0 有効サ

[1] 株式会社インターネットイニシアティブ
[a)] suga@iij.ad.jp

イトは無く SSL3.0 有効サイトは 3 サイトのみであった．このとき Top FQDN としては 115 サイトが存在したが，アウトソーシングサービスを利用しているため同じ FQDN に複数の組織のログインサービスが提供されているため，トータルで 58 の FQDN が調査対象となっており 58 全てのサーバにおいて EVSSL 証明書が配備されていた．そのうち 53 の証明書は同一商用認証機関から発行されており，このまま使い続けると近々，ある特定の主要ブラウザにおいて脆弱であると判断され，EV 証明書として本来機能するべきグリーンバーが表示されないことが予想されている．

ブラウザベンダーのアナウンスによると，既に 3 月より開発者向けブラウザではエラー表示がされており，2018 年 9 月 13 日にリリース予定の通常版ブラウザでも警告が表記されることとなる．実際に現在も利用されている証明書は有効期限が切れる前に，ブラウザ表記が失効状態と同様の振る舞いとなるため管理者が気が付かないまま運用されてしまう可能性もある．本稿では現在使われている証明書の特徴について分析を行うとともに，2018 年 5 月中旬までの証明書移行の状況について報告する．

参考文献

[1] Google Chrome57 のバグにより EV SSL 証明書の組織名がグリーン表示されない事象について, https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?vproductcat=V_C_S&vdomain=VERISIGN.JP&page=content&id=INFO4287&actp=RSS&viewlocale=ja_JP&locale=ja_JP&redirected=true

[2] EV SSL サーバ証明書の Policy OID の変更について, https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?vproductcat=V_C_S&vdomain=VERISIGN.JP&page=content&actp=CROSSLINK&id=ALERT1955&locale=ja_JP&redirected=true

[3] 須賀, ”EVSSL 証明書利用時の表示不備に関する調査”, 第 18 回 インターネットテクノロジーワークショップ, 2017.

[4] Google Security Blog, ”Chrome’s Plan to Distrust Symantec Certificates”, https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

[5] Google Security Blog, ”Distrust of the Symantec PKI: Immediate action needed by site operators”, https://security.googleblog.com/2018/03/distrust-of-symantec-pki-immediate.html

[6] CRYPTREC, SSL/TLS 暗号設定ガイドライン〜安全なウェブサイトのために (暗号設定対策編)〜, https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html