NTT DATA
Trusted Global Innovator

注目されているセキュリティ事故・事件に関する情報 ＜2018年9月版 (第26号)＞(選り抜き版)

2018年9月28日
ＮＴＴデータ先端技術株式会社
セキュリティ事業部

今回のサマリー

「Symantec系SSL証明書の無効化へ」
2017年9月、Googleは自社のブログで、Symantec傘下の認証局から発行されたSSL証明書(以下、Symantec証明書)をGoogle Chromeで段階的に無効化することを公表しました。本記事では、方針決定に至った背景と、企業が公開しているWebサーバの証明書が無効化対象である場合に取るべき企業の対応について解説します。

Symantec系SSL証明書の無効化へ

1. 段階的な証明書無効化 (1/4)

■**ChromeとFirefoxでSymantec証明書の無効化を実施**

2017年9月、業界標準となっているCA Browser Forumの「**Baseline Requirements**」を遵守した認証局としての運用をしていないとして、Symantec傘下の認証局が発行したルート証明書をGoogle Chrome の「信頼されたルート証明書」から段階的に除外することを公表しました。以下にタイムラインを記載します。

時期	組織	動き	詳細
2009年～2017年	Google社 Mozilla	Symantec社に対して再三に渡り問題を指摘 →証明書の誤発行 →業界標準に準拠していない証明書発行	合計17件の指摘(※引用元参照)が行われました．主な指摘は以下です。 2015年10月　不正なテスト証明書発行 2017年1月　業界標準の監査プロセスに従わず、不正に証明書を発行。 不正発行の指摘後の情報開示が適切に実施されない。
2017年3月24日	Google社	Symantec証明書の無効化を提案	Google社からSymantec社に証明書発行プロセスの是正を求め、Google Chromeにおいて同社のルート証明書を「信頼されたルート証明書」から段階的に除外していくことが提案されました。 正式決定した場合、Symantec社が無効化を解除されるためには、業界標準に則った認証局の新規構築が必要となります。
2017年8月3日	Symantec社 Digicert社	Symantec社がPKI事業をDigicert社に売却することを発表	Digicert社がSymantec社のWebサイトセキュリティ事業、ならびに関連するPKIソリューションを買収すると発表。 Symantec社は認証局の新規構築の代わりに事業の売却を選択することを決断しました。
2017年9月11日	Google社	Symantec証明書の無効化を正式決定	2017年1月に発生した不正発行を受け、Symantec傘下の認証局のルート証明書をGoogle Chrome の「信頼されたルート証明書」から段階的に除外することを公表。
2017年12月1日	Digicert社	Symantec社から移管された認証局事業を運用開始	-
2018月3月12日	Mozilla	Symantec証明書の無効化を正式決定	Googleに追随する形でMozillaが段階的に無効化する計画を公表。

※引用元：　CA:Symantec Issues
https://wiki.mozilla.org/CA:Symantec_Issues

1. 段階的な証明書無効化 (2/4)

主要ブラウザでは証明書の発行日に応じた無効化が実施されます。

① 証明書の発行日が 2016年5月31日 以前
② 証明書の発行日が 2016年6月1日 以降

Google ChromeとFirefoxの無効化スケジュールを以下の表に記載します。

対象	ブラウザ / バージョン	リリース日(予定日)		
		Dev 版	Beta 版	安定版
①	Chrome 66	2018年2月9日	2018年3月19日	2018年4月17日
	Firefox 60	2018年1月22日	2018年3月12日	2018年5月9日
②	Chrome 70	2018年8月3日	2018年9月13日	2018年10月16日
	Firefox 63	2018年6月25日	2018年9月4日	2018年10月23日

・Dev版　… 開発者向けのリリースです。最新機能を利用できます。主に検証やバグFix目的で利用されます。
・Beta版　… Dev版と同じく開発者向けのリリースです。次期バージョンをテストするための目的で利用されます。
・安定版　… 一般ユーザ向けのリリースです。すべてのテストが完了したものがリリースされます。

Google ChromeとFirefox以外にも、Apple社などのOSベンダや他ブラウザベンダが追随して無効化する動きを見せています。(※)

(※) https://support.apple.com/en-us/HT208860

1. 段階的な証明書無効化 (3/4)

Google ChromeとFirefoxのSymantec証明書の無効化スケジュールは前ページの通りとなります。これにより2018年10月中旬には、安定バージョンのブラウザでSymantec証明書を利用したWebサイトへアクセスした場合、ブラウザ上に証明書エラーの警告が表示されることとなります。

無効化の対象となる証明書は以下のブランドを含むSymantec傘下の認証局から発行された証明書です。

1. 段階的な証明書無効化 (4/4)

前ページ記載のSymantec傘下の認証局以外に、過去にも認証局のルート証明書を「信頼されたルート証明書」から除外した事例が発生しています。事例を以下の表に記載します。

項番	発生年	事業者名	事象の概要	無効化の原因
1	2011年	DigiNotar (オランダ)	攻撃者が外部からのハッキングにより、同社の認証局内部のサーバに侵入した。政府機関やGoogleなどの著名なサイトの証明書が不正発行され、攻撃者により暗号化通信が傍受された。	• 証明書不正発行のセキュリティ影響が甚大であったため • 攻撃者の侵入を検知した後、不正発行された一部の証明書を失効させて外部に情報開示を行わなかったため
2	2015年	CNNIC (中国) MCS Holdings (エジプト)	CNNICは、MCS Holdings に事前申請したドメイン向けの中間証明書を発行する契約を行った。しかしMCS Holdingsは入手した中間証明書を使用して、Googleの複数のドメインの証明書を発行した。	• CNNICが適切ではない組織に対して権限を委譲したため • 発行されたSSL証明書がパスワードを盗む目的で作成され利用された可能性があったため
3	2016年	WoSign (中国) StartCom (イスラエル)	WoSignとStartComは使用の廃止が決まっているハッシュ関数「SHA-1」を使った証明書の日付を意図的に古く偽装するなど不正な運用を行った。	• 証明書の発行日付を64件に渡り偽装して発行したため • 業界標準の「**Baseline Requirements**」に違反した運用が行われていたことが確認されたため等

次ページでは具体的な事例として「項番１」の2011年に発生したDigiNotar社のインシデントを説明します。

2. 過去の事例 (DigiNotar社インシデント)

2011年、オランダの認証局を運営する組織であるDigiNotar社の公開Webサーバに攻撃者が侵入しました。それを足がかりに同社が運営する認証局サーバ本体へ攻撃者の侵入し、攻撃者が認証局や政府機関を含む著名なWebサイト等の531通の証明書を不正入手してしまうインシデントが発生しました。

この結果、約１ヶ月間に渡りGoogle社を始めとしたWebサイトとユーザ間の暗号化通信が、攻撃者による中間者攻撃により傍受していたとされています。

当時のGoogle Chromeに実装されていた公開鍵ピンニング(HPKP)機能による警告をユーザが報告したことで、インシデントが発覚しました。攻撃の発覚後、2日程度でMicrosoft社やGoogle社が、DigiNotar社が発行したルート証明書を「信頼されたルート証明書」から除外するアップデートを提供することで、事態の収束が図られました。

結果として、DigiNotar社は2011年9月に廃業に追い込まれることとなりました。

3. 認証局が果たす役割 (1/2)

過去事例としてご紹介したDigiNotar社や今回のSymantec社の事例から分かるとおり、認証局のルート証明書をブラウザベンダが「信頼されたルート証明書」から除外することは、認証局事業に多大な影響を及ぼします。それにもかかわらず、なぜブラウザベンダはこのような強硬な対応を取るのでしょうか。

それは現在のインターネットで利用されているPKIでは、ブラウザと正しいWebサーバ間で行われる安全な暗号化通信が、**認証局を無条件に信頼することを前提**に運用されているからです。

ブラウザが暗号化通信の開始時に接続先Webサーバが本物であるかを確認するためにWebサーバから提示される証明書を複数の観点で検証します。この際、証明書に含まれている情報から「あらかじめブラウザが信頼している認証局が発行した証明書であるか」等を確認することで、正しい接続先Webサーバであるとブラウザが判断します。

インターネットPKIの詳細はJPNIC(※2)やIPA(※3)の資料をご参照ください。

(※1)インターネット10分講座：PKI
https://www.nic.ad.jp/ja/newsletter/No23/080.html
(※2) PKI 関連技術情報
https://www.ipa.go.jp/security/pki/index.html

3. 認証局が果たす役割 (2/2)

認証局のオペレーションミスにより誤って不適切な証明書が発行された場合や、認証局へ攻撃者が侵入され証明書が不正に発行された場合、Webサーバ運営組織やユーザはその事実に気づくことができません。なぜならその証明書は、私たちが信頼する認証局によって発行された「本物」の証明書であるからです。

このため、現状のPKIの問題への対策として以下のものが提案/運用されています。

- 「**Baseline Requirements**」 の遵守の要請
  - ✓ CA Browser Forumが策定した認証局の運用規定
- インターネットPKIを改善するための技術の提案/運用
  - ✓ 公開鍵ピンニング(HPKP)
  - ✓ Certificate Transparency(CT)
  - ✓ DNS-Based Authentication of Named Entities(DANE)

ここまで認証局が果たす役割について説明してきました。次ページでは、今回のSymantec証明書の無効化に対して、企業に必要な対応についてご説明します。

4. 企業側はどのような対応が必要か (1/3)

今回のSymantec証明書の無効化に対して、公開するWebサーバを運用する企業では以下の対応が必要となります。

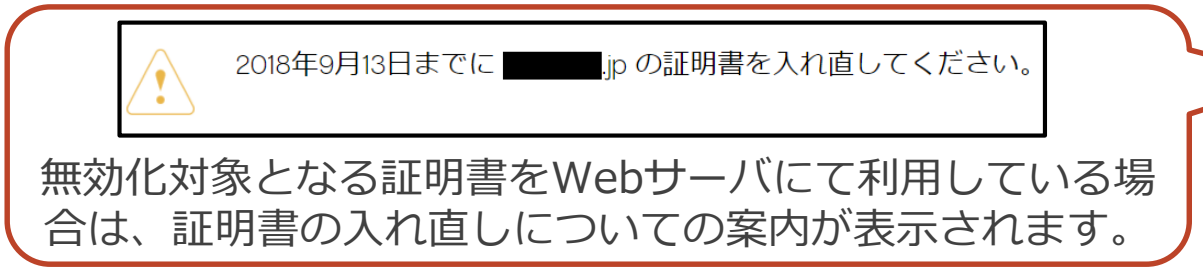
1. 運用しているWebサーバの証明書が無効化対象かを確認する
2. 無効化対象である場合は、早急に証明書の更新手続きを行う

1. 運用しているWebサーバの証明書が無効化対象かを確認する

公開Webサーバの場合、Symantec社が公開している確認サイト(※)を利用した確認方法があります。

① 確認サイトを開く
② URL入力欄に確認対象のWebサイトのURLを入力
③ 確認実行ボタンを押下
④ 表示内容を確認する

確認実行ボタン押下後の確認サイトの画面



無効化対象となる証明書をWebサーバにて利用している場合は、証明書の入れ直しについての案内が表示されます。

(※) https://www.websecurity.symantec.com/ja/jp/support/ssl-checker

4. 企業側はどのような対応が必要か (2/3)

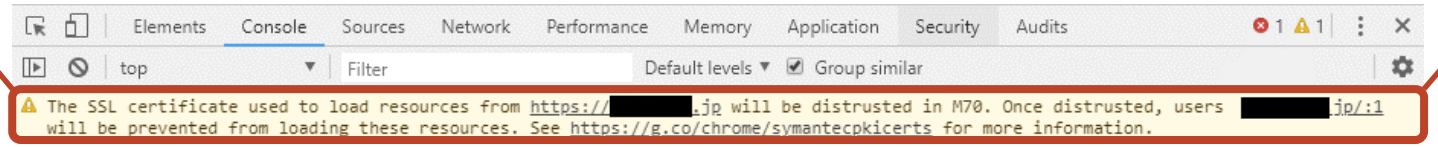
1. 運用しているWebサーバの証明書が無効化対象であるかを確認する (続き)

非公開Webサーバの場合は、Google Chomeのデベロッパーツールを用いた確認方法があります。

① 対象のWebサイトへアクセスし [Ctrl+Shift+I] を押下して、デベロッパーツールを表示
② 表示されたデベロッパーツール内の「Console」タブをクリック
③ 次の警告が表示されていないことを確認

The SSL certificate used to load resources from **<対象サイトのURL>** will be distrusted in M70. See https://g.co/chrome/symantecpkicerts for more information.

無効化対象となる証明書をWebサーバにて利用している場合は、
Webサーバが無効化対象の証明書を利用している警告が表示されます。



アクセス先のWebサーバが無効化対象の証明書を利用している場合の
Google Chrome のデベロッパーツール内の「Console」タブの表示

4. 企業側はどのような対応が必要か (3/3)

2. 無効化対象である場合は、早急に証明書の更新手続きを行う

　確認対象のWebサーバが利用する証明書が無効化対象であると確認された場合は、早急に証明書の入れ替えの対応が必要です。証明書の購入先である代理店などに更新手続きの依頼を行うなど、対応を行ってください。詳細はSymantec社の公式サイト(※)をご確認ください。

(※) https://www.websecurity.symantec.com/ja/jp/blog/replace-your-symantec-ssl-tls-certificates

5. まとめ

本レポートでは、Symantecが発行した証明書が無効化された経緯と背景、ブラウザベンダの対応、認証局の役割を説明し、企業側で求められる対応について解説を行いました。

企業及び個人に安全を提供するための基盤も、人の運用次第では安全の根幹を揺るがすケースがあります。

証明書が無効にされるなど、サービス提供の継続に影響を与えかねない事象が発生した場合、必要な対応やスピードを的確に判断し、サービス提供に影響を与えないように、速やかな情報収集および十分な調査・検証を行える運用体制を構築することが重要となります。

6. 参考URL (1/2)

- CA:Symantec Issues – MozillaWiki
  https://wiki.mozilla.org/CA:Symantec_Issues
- Distrust of Symantec TLS Certificates | Mozilla Security Blog
  https://blog.mozilla.org/security/2018/03/12/distrust-symantec-tls-certificates/
- Google Online Security Blog: Chrome’s Plan to Distrust Symantec Certificates
  https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html
- Google Online Security Blog: Sustaining Digital Certificate Security
  https://security.googleblog.com/2015/10/sustaining-digital-certificate-security.html
- Chrome Releases: Stable Update
  https://chromereleases.googleblog.com/2011/08/stable-update.html
- rapport-fox-it-operation-black-tulip-v1-0
  https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf
- black-tulip-update
  https://cryptosense.com/wp-content/uploads/2014/11/black-tulip-update.pdf
- Distrusting New CNNIC Certificates
  https://blog.mozilla.org/security/2015/04/02/distrusting-new-cnnic-certificates/
- Distrusting New WoSign and StartCom Certificates
  https://blog.mozilla.org/security/2016/10/24/distrusting-new-wosign-and-startcom-certificates/
- アドバイザリ 2607712 更新 – DigiNotar 社のデジタル証明書を削除する更新プログラムを公開 - 日本のセキュリティチーム
  https://blogs.technet.microsoft.com/jpsecurity/2011/09/06/2607712-diginotar-12/

6. 参考URL (2/2)

- シマンテックの SSL/TLS サーバ証明書の入れ替えについて | DigiCert & Symantec
  https://www.websecurity.symantec.com/ja/jp/blog/replace-your-symantec-ssl-tls-certificates
- Baseline Requirements - CAB Forum
  https://cabforum.org/baseline-requirements/
- Google Online Security Blog: Sustaining Digital Certificate Security
  https://security.googleblog.com/2015/10/sustaining-digital-certificate-security.html
- Google Online Security Blog: Chrome’s Plan to Distrust Symantec Certificates
  https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html
- Google Online 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
- Firefox Release Calendar - MozillaWiki
  https://wiki.mozilla.org/Release_Management/Calendar
- Is This MITM Attack to Gmail's SSL ? - Google プロダクト フォーラム
  https://productforums.google.com/forum/#!topic/gmail/3J3r2JqFNTw
- Protection against fraudulent DigiNotar certificates
  https://www.mozilla.org/en-US/security/advisories/mfsa2011-34/
- Misissued/Suspicious Symantec Certificates
  https://groups.google.com/forum/#!msg/mozilla.dev.security.policy/fyJ3EK2YOP8/yvjS5leYCAAJ

NTT DATA

Trusted Global Innovator