報道関係者各位
プレスリリース

2011 年 10 月 14 日
ジェイサート株式会社

ジェイサート「スターフィールド SSL では、偽証明書の発行はこうして防ぐ！」を報告
他社「偽証明書」はどのようにして発行されたのでしょうか？（その２）

ジェイサート株式会社(本社：東京都千代田区、代表取締役：石原　章年　以下、ジェイサート)は、「スターフィールド SSL」の発行元で世界最大の認証局である米国 Go Daddy 社が、いかにして「偽証明書」の発行回避に万全を期しているのかにつき、続報を報告致します。

2011 年 8 月、今年春先にハッキングされたとの報道あった米国コモド社（Comodo）に続き、オランダの認証局 DigiNotor 社が第三国の何者かにハッキングされ、またも Google や Microsoft、twitter, facebook, Skype, Mozilla など世界的に著名なサイトのログインページ等に利用される、500 枚を超える「偽証明書（なりすまし証明書）」が発行されたとの報道があり、その後 Microsoft Internet Explorer や Mozilla Firefox、Google Chrome や Apple Mac OS X など主要なブラウザベンダにより DigiNotar 社が発行した SSL サーバ証明書の一切を無効化するという迅速かつ断固とした措置が取られたことから、同社は 4000 万ドル前後（30 億円前後）の負債を抱え自己破産した、と伝えられております。

なぜ、「認証局に対するハッキング」が後を絶たないのでしょうか？

SSL サーバ証明書は、通販サイトや金融サービス等のログインページなど、インターネット上に個人情報やカード番号等の機密情報が流れる際に「封書」効果を施すべく暗号化する機能を持っていますが、同時に通販サイトや金融サービスのログインページが「偽サイト」「偽ログインページ」ではないことを業界団体（CA Brower Forum（注 1））が定め、推奨する手続きにより実在確認を行った上でサイトやログインページに発行されることが前提となっております。

CA Browser Forum が定め、推奨するサイトやログインページの実在確認手続きは、法務局が発行する登記簿や WHOIS などの信頼に足る第三者情報との照合やサイト運営組織への電話による在職確認など、実用レベルに耐える精度が担保されているものと考えられますが、他方、サイトやログインページの実在確認を行い、証明書を発行する認証局そのも

の（ビジネスモデル）に以下に列記されるような「脇の甘さ」が疑われる手抜かりが、一連の「認証局に対するハッキング」により明らかになったものと受け止めております。

１）　証明書発行権限を、WebTrust（注 2）等の第三者監査機関の認証を取得していない、複数の外部協力会社に付与していたのではないか。

２）　外部協力会社による証明書発行業務を、事前承諾するのではなく、事後追認に留めてきたのではないか。

３）　外部協力会社の中には、認証局のルート認証局に直接アクセスし証明書を発行できるところがあったのではないか。

これに対し、「スターフィールド SSL」の発行元である Go Daddy 社では、世界最大規模の証明書を発行（年間 60 万枚以上、世界シェア 1 位）しており、SSL サーバ証明書サービスへの信頼維持・向上には細心の注意を払って来ておりますが、次のような同社のビジネスモデルが、高い精度で「偽証明書」の発行を未然に防ぐ管理体制の構築を可能にして来たものと考えております。

１）　証明書発行業務の一切を外部委託せずその全てを、WebTrust 監査認証を取得済の米国アリゾナ州の同社本社において一元的に実施、世界中の市場に対しマルチリンガル管理（日本語含め）しております。

２）　証明書発行に至るまでに、複数階層の社内部署に発行承認権限を分散、発行前承認の精度を高めております。　特に、同社が併営するドメイン管理事業（管理ドメイン数 4,800 万、世界シェア 1 位）により作成される世界の不正サイトに関わるブラックリストによる検証機能は他社に例を見ないものです。

３）　万が一「偽証明書」が発行されるような事態が起こっても、ルート認証局へのハッキングを回避するため、すべてのエンド証明書は中間認証局から発行されております。

今回の「偽証明書」発行事故を受け、CA Browser Forum では、証明書発行業務の外部委託について何らかの規制を打ち出すのものと想定しており、同時に認証局各社による証明書発行業務の見直しにより、インターネット上の信頼基盤の一翼を担う SSL サーバ証明書サービスの品質の向上が一層進められるものと確信しております。

（注1）　CA Browser Forum（CABF）とは、世界の主要な認証局と Microsoft 等ブランザベンダーによって米国に設立された団体で、EV SSL 証明書の技術仕様および認証基準の標準化を行うとともに、SSL/TSL 技術がインターネットの信頼基盤として広く安心して利用されるよう業界調整を行うことを目的としています。（http://www.cabf.org/）

（注2）　WebTrust（ウェブトラスト）とは、国際監査法人により毎年実施される、電子証明書を発行する認証機関として具備すべき、業務手順やシステム運用規

定に関わる監査プログラムであり、マイクロソフト等世界で広く利用されている各種ウェブ・ブラウザにおいて「信頼されたルート証明機関」として登録されるための要件ともなっています。

【Go Daddy Group, Inc.　会社概要】
代表　　：CEO ＆ Founder　Bob Parsons
本社　　：米国アリゾナ州スコッツデール
年商　　：850 億円(2010 年実績)
URL　　：http://www.godaddy.com
事業概要：
1.ドメインレジストラ事業(世界最大 4,800 万ドメイン)
2.ホスティング事業(世界最大 500 万アカウント)
3.SSL 証明書事業(世界最大 60 万ライセンス シェア 30%)

【ジェイサート株式会社　会社概要】
代表　：代表取締役　石原 章年
本社　：〒102-0082 東京都千代田区一番町 4 番 22 号 プレイアデー番町 6 階
資本金：7,600 万円
URL　：http://www.jcert.co.jp