PKI day 2012
「我が国における信頼基盤の連携に向けて」
「PKIへの攻撃とその対応」

セコム株式会社　IS 研究所
松本　泰・島岡　政基

今年度のJNSA PKI相互運用技術WGが主催するPKI day 2012は、2012年12月13日に100名弱の参加者のもと開催されました。会場の参加者のほか、PKI dayでは、昨年同様、Ustreamによるライブ中継を行い、会場外から参加する方もいらっしゃいました。

毎年、恒例となっているPKI dayですが、ここ数年は、PKIの社会基盤的な側面から、その役割と課題をテーマとして取り上げてきました。PKI day 2012でも、こうした社会基盤としてのTRUSTのあるべき姿をイメージし、午前と午後でふたつのテーマ（午前の部「我が国における信頼基盤の連携に向けて」、午後の部　「PKIへの攻撃とその対応」）で講演とパネルディスカッションを行い、それぞれ密度の濃い議論が展開されました。

午前の部

我が国における信頼基盤の連携に向けて

午前の部の「我が国における信頼基盤の連携に向けて」は、以下のようなテーマ設定を行いました。

> PKIは現在、様々な情報通信基盤の信頼の要として利用されています。例えば、インターネット上の通信におけるTLS/SSLや、電子政府の電子申請等で利用される電子署名法に準拠した証明書による電子署名、e文書法等で要求される時刻証明のためのタイムスタンプ等があります。我が国において、これらのPKIは、それぞれ別々の目的や成り立ちがあり、現在は、似て非なるフレームワークで、構築、運用されています。しかし、今後は様々な分野において情報連携が求められており、この情報連携を実現するうえで整合性の取れた信頼基盤構築のフレームワークが重要になると考え、そのため、これらのPKIにおいても制度的に整合性をもったフレームワーク作りが望まれます。
>
> 本セッションでは、PKIに関連した団体の活動を紹介すると共に、パネルディスカションでは日本社会における信頼基盤の連携を確立するため、各団体でどのような連携を図っていくか議論します。

講演者と講演、およびパネルディスカッションの登壇者は、以下のとおりです。

【講演】「我が国における信頼基盤の連携に向けて」
講師：セコム株式会社 IS研究所　松本　泰 氏

【講演】「電子認証局会議の活動」
講師：日本電子認証株式会社　高橋　章 氏

【講演】「タイムビジネス協議会の活動」
講師：アマノビジネスソリューションズ株式会社　市川 桂介 氏

【講演】「電子記録応用基盤フォーラム（eRAP）の活動」
講師：三菱電機株式会社　宮崎 一哉 氏

【パネルディスカッション】
＜モデレータ＞
セコム株式会社 IS研究所／
PKI相互運用技術WGリーダー　松本　泰 氏
＜パネリスト＞
高橋　章 氏　日本電子認証株式会社
市川 桂介 氏　アマノビジネスソリューションズ株式会社
宮崎 一哉 氏　三菱電機株式会社
秋山 卓司 氏　クロストラスト株式会社
宮内　宏 氏　宮内宏法律事務所

講演、およびパネルディスカッションの講演資料と動画のアーカイブが公開されていることもありますので、ここでは、パネルディスカッションでの議論の背景をもう少し補足して説明します。

PKI相互運用技術WGは、元々、WGの名前のとおりPKIの相互運用技術に注目した活動でした。繋がる事だけを目的とした「相互運用技術」とは違い、セキュリティ技術、暗号技術、更には信頼（TRUST）の形成まで目的とした「相互運用技術」は、別次元の難しさがあります。しかし、TRUSTに係わる「相互運用技術」に取り組む程に、「相互運用技術」では解決できないポリシーの不整合等の問題に突き当たるということが

ありました。これは、簡単に表現することが難しいのですが、IT社会における信頼（TRUST）であっても、社会基盤に組み込まれるほどに、既存の制度、慣習との整合が求められます。しかし、元々「紙文書」を前提に構築されてきた既存の社会の仕組み（TRUSTの仕組み）は、「デジタル」な技術を前提としたIT社会の信頼（TRUST）には適合しにくい面があります。そこで、従来の制度の延長線上だけではない新たな枠組みが必要になります。これらの課題をうまく表現した「絵」が三菱電機の宮崎氏の発表資料（図1）にあります。

このパネルディスカッションでの「密度の濃い議論」は、短い紙面では書ききれません。「密度の濃い議論」に関しては、公開されている講演資料及び動画のアーカイブを参照して頂ければ幸いです。

午後の部

PKI への攻撃とその対応

午後の部の「PKIへの攻撃とその対応」は、以下のようなテーマ設定を行いました。

近年、PKIへの攻撃が顕著になっています。例えば、以下の事例があります。

- 2011年3月Comodo事件：9件の証明書が不正発行
- 2011年8月DigiNotar事件：500以上の証明書が不正発行
- 2012年5月に発覚したFlame Malware

これらの事例では、不正な証明書発行やX.509証明書の偽造等、PKIへの攻撃が行われています。こうして

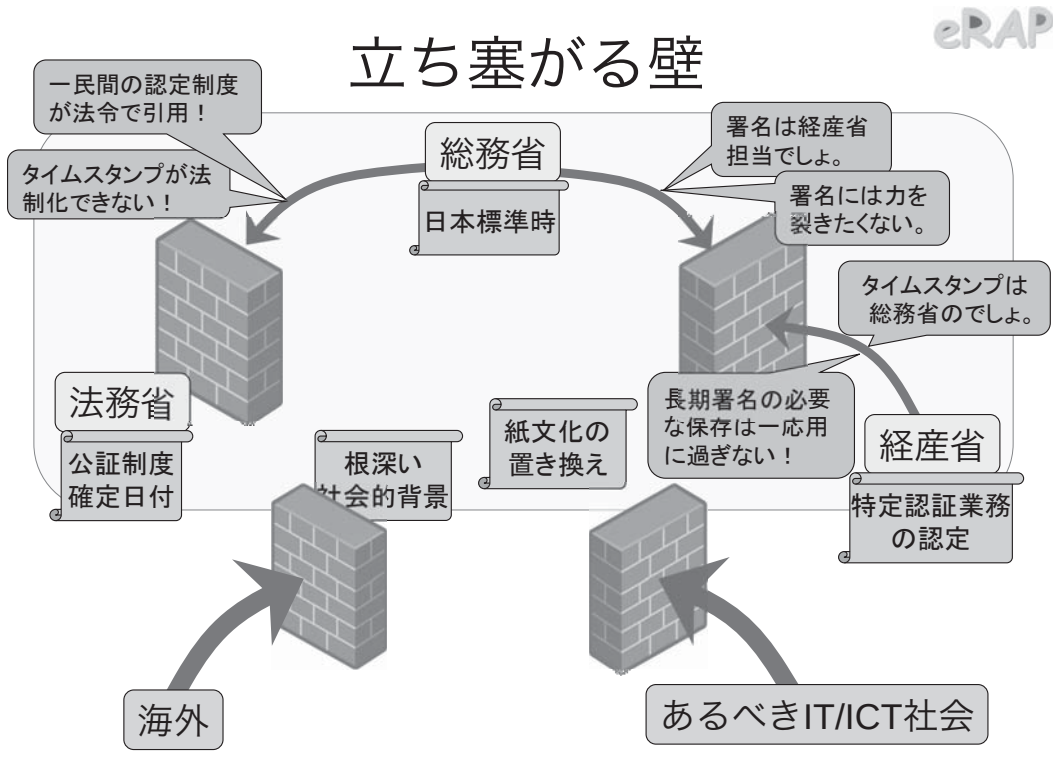

図 1 「立ち塞がる壁」
三菱電機 宮崎氏　講演資料より抜粋

不正に取得された証明書は、Flameで見られるように複雑で高度な攻撃を行うために使われています。これらの事例はたまたま発覚されたに過ぎず、水面下ではもっと多くの攻撃が準備されている可能性もあります。

また、SSL/TLS、SSHなどのセキュリティプロトコルで利用されている証明書を広く収集して様々な分析が行われています。2012年8月にはUSENIX Security SymposiumおよびCRYPTOにて収集された公開鍵の多くが意図せず他のサイトと秘密鍵を共有している問題が指摘されました。この問題は正しく鍵生成を行っていないことに起因し、もちろん攻撃の糸口に利用される可能性があります。

PKIが攻撃されるのは、現在の世の中において、PKIの仕組みが、世の中の信頼の起点として組み込まれていることに他なりません。PKIは、情報化社会の基盤技術ですが、このPKIを代替する技術は考えられず、今後の社会においても信頼の起点であり続ける必要があります。そのためには今後の攻撃に耐えうる技術・運用方法を確立する必要があります。

本セッションでは、

- これらの事件の内容を、その背景も含め正確に理解し
- 今後の考えられる攻撃を考察し
- 今後の中長期的な対策

について議論します。

講演者と講演、およびパネルディスカッションの登壇者は、以下のとおりです。

【講演】「サイバー攻撃ツールとしての公開鍵証明書の役割～信頼の起点にカモフラージュされた攻撃の起点～」

講師：(独) 情報処理推進機構 セキュリティセンター 暗号グループ 研究員　神田 雅透 氏

【講演】「公開鍵の多くが意図せず他のサイトと秘密鍵を共有している問題～いつのまにか他人と秘密鍵を共有してませんか？～」

講師：株式会社インターネットイニシアティブ セキュリティ情報統括室 シニアエンジニア 須賀 祐治 氏

【パネルディスカッション】

＜モデレータ＞

株式会社インターネットイニシアティブ セキュリティ情報統括室 シニアエンジニア 須賀 祐治 氏

＜パネリスト＞

神田 雅透 氏　(独) 情報処理推進機構 セキュリティセンター 暗号グループ　研究員

島岡 政基 氏 セコム株式会社　IS研究所

高橋 正和 氏 日本マイクロソフト株式会社 チーフセキュリティアドバイザー

佐藤 直之 氏 日本ベリサイン株式会社　主席研究員

■ 講演の概要

午後のセッションは、はじめにIPA神田氏から概略として最近の認証局に対する一連の攻撃について解説が行われました。

攻撃の対象となっているのはもっぱらトラストアンカとなるルート認証局であり、これらトラストアンカは様々なアプリケーションに予め組み込まれるものであるために、これを攻撃されるとユーザは何ら気づくことなく騙され続けてしまいます。

現在、PKIが攻撃されるケースは、大きく3つの要因に分類されます。一点目は認証局へのハッキング、二点目は暗号技術に対する攻撃、三点目は運用の問題です。三点目については次のセッションでIIJ須賀氏が解説されるため、神田氏からは前者二点について説明されました。

認証局へのハッキングは、ComodoおよびDigiNotar事件が知られています。特に後者のDigiNotar事件は、少なくとも531枚以上という大量の不正な証明書発行が行われ、実際にイランで不正な証明書を悪用した盗聴行為が行われた可能性が高く、最終的にこの

事件の影響によりDigiNotar社が1998年からの歴史に幕を閉じることになった（つまり倒産した）、という点で認証局業界にとってインパクトの高い事件でした。

これまでは、不正発行された証明書を悪用するためには、DNSサーバを改ざんするか、いわゆる中間者攻撃（Man-in-the-middle）を行う必要があり、不正発行だけで実害を発生させることは難しいとされてきたわけですが、DigiNotar事件では、これがいとも簡単に覆されてしまいました。このように証明書の不正発行とDNSサーバの改ざんといった複数の攻撃が同時に成立した背景には、大規模な組織的支援つまり政府機関の関与があったのではないかと推測されています。続いて暗号技術に対する攻撃事例としてFlame事件の解説が行われました。これもやはり政府機関の関与が指摘されていますが、特徴的なのはやはり暗号アルゴリズムに対する攻撃を成功させた点であり、従来の想定を覆す計算能力と解読技術を有する攻撃者の存在を知らしめたことでしょう。このように、認証局に対する攻撃は年々本格化しており、政府レベルの関与や世界トップレベルの暗号解読能力にもとづく攻撃が行われる可能性を無視できなくなりつつあることが再認識されました。

午後二本目のセッションは、IIJ須賀氏から公開鍵使いまわし問題について解説が行われました。本問題は、2012年8月に複数の暗号研究者からほぼ同時期に発表されたもので、インターネット上に存在するSSL/TLSやSSHなどの公開鍵（それぞれ約1,000万件以上）を収集・分析した結果、いずれも6割以上という多くのノードで私有鍵（又は秘密情報の一部）が重複していることを指摘したものです。こうした私有鍵の重複は一概に危険であるとは言えず、例えば負荷分散のための冗長構成で同じ鍵を利用しているケースなどもあると推測されます。しかしながら、機器出荷時の初期鍵をそのまま利用しているケースが5%以上(67万件以上)のホストで確認されており、これらについては盗聴やなりすましの危険性が懸念されています。

典型的な公開鍵暗号であるRSAは、二つの巨大な素数p, qを用いて構成されますが、この二つの素数のうちいずれかを他のユーザが用いていれば、公開鍵から私有鍵を解読するのは容易になります。これらの素数は、擬似乱数生成(PRNG)モジュールによって鍵ペア生成時にランダムに選択されますが、ここで十分な乱雑性が確保されなければ、pまたはqの重複や最悪の場合は鍵ペアそのものの重複が生じます。

この乱雑性は暗号アルゴリズムと無関係に実装に大きく依存しており、例えば某社の実装ではわずか9個の乱数即ち36通り(9C2)の公開鍵しか生成することができなかったことが明らかになっています。これは極端な例ですが、いずれにしてもこうした実装が増えることで「重複しやすい素数」が増えることになり、その素数を用いた「解読しやすい公開鍵」も増えることになります。つまり、RSA暗号の安全性は2つの巨大な素数を衝突することなく選択することに依存していたわけですが、その前提が機能しない場面が見受けられるようになりました。この安全性低下はRSA暗号だけの問題ではなく、例えばDSAも署名時にPRNGを用いて乱数を生成しますが、その乱数が重複していれば私有鍵を容易に解読できてしまうため、やはりRSAと同様に安全性が低下しつつあることが指摘されています。

こうした問題が生じる背景には、多くの暗号アルゴリズムが乱数生成において十分な乱雑性を期待しているのに対して、実装側がその重要性を理解できないままPRNGを実装・使用してしまっていること、また近年増加が著しいアプライアンスも含めた組込み機器にお

いては十分な乱雑性の確保と性能の両立が難しい上に、パッチなどの適用が難しいという問題があるのではないでしょうか。

■ パネルディスカッションの概要

最後に、こうした公開鍵暗号にまつわる様々な攻撃方法が顕在化していく状況を踏まえて、これらの事件・事故の全体像を正しく理解し、今後の対策や提案・提言を検討していくためにはどうしたらよいかというパネルディスカッションが行われました。このパネルに限っては、リアルタイムに可能な限り自由な意見交換を妨げないようにするため、Ustream中継およびTwitterによるtsudaりも禁止という条件で行われました。

パネルでは、最初にマイクロソフトの高橋氏から、昨年10月のWindows UpdateによってRSA1024bit未満の証明書は自動的に使えなくしたこと、これによるお客様対応の事例などについて説明が行われました。次に日本ベリサインの佐藤氏から、DigiNotar認証局事件について昨年末に公開された報告書をもとに解説が行われました。その後セコムIS研究所の島岡氏から、こうしたPKIへの攻撃に対する中長期的な対応の提言とともに、信頼の基盤としてPKIを維持していくことの重要性について説明が行われました。

こうした説明を受けた後のディスカッションでは、PKI業界はこれまであまり攻撃対象として注目されていなかったために対策も甘かったが、今後本格的な攻撃対象となってくるのは明らかなのでより厳格な対策が求められる、特に証明書はコスト構造が利用者から見えにくい面もあるので、コストの割に脆弱と指摘されかねない、など厳しい意見が相次ぎました。

こうした指摘に応えるために、例えばCAブラウザフォーラムでは脆弱性対策に対する要件を明確化してWebTrust for CAの認定要件に追加する動きがあることが報告されるとともに、一方で現状の認証局監査は認定の有無しかわからず、例えば鍵管理や脆弱性対策などの評価項目に対して各認証局がどの程度の水準にあるのかわかるようにしてはどうか、といった監査の透明性を求める意見も出ました。

PKI限界説や、PKIに代わる新しい信頼の基盤が成功する可能性はあるか、といった議論もされましたが、既存の様々な仕組みがサーバ認証やコード署名というPKI特有の技術に依存している現状を考えると切り替えは容易ではないこと、さらに信頼の基盤となるには信頼の起点となるトラストアンカを配布・普及させる必要があり、これは昔よりも組込み機器が多く普及した現在の方が遥かに難しく時間のかかる問題であり、これからも社会はPKIに依存せざるを得ない。つまりPKIの信頼を確保し続けるためにとにかく努力し続ける必要があるという話まで進んだところで残念ながら時間切れとなってしまいました。

■ おわりに

今回のPKI dayは、ここ数年のPKI day と同じくPKIの社会基盤的な側面をテーマとしました。今回は、PKIの既存の制度との不整合の問題、既存の社会基盤化したPKIの課題等、全体として既存のPKIの課題を取り上げたため、PKIの新たな技術の取り組みという点が、不足していたかもしれません。

次の社会基盤と言う観点からは、スマートグリッド、M2M等に組み込まれるPKIの技術研究が欧米では盛んに行われているようであり、今後は、こうした取り組みも取り上げていきたいと考えています。いずれにせよ、今後のIT社会における社会基盤には、デジタル化したTRUSTの構築が不可欠でありPKIの重要性は変わることはないでしょう。それが故に、今回の午後のようなテーマも真剣に議論する必要があると考えています。

◆参考

PKI Day 2012
http://www.jnsa.org/seminar/pki-day/2012/

JNSA/PKI相互運用技術ワーキンググループ
http://www.jnsa.org/result/pki/