SSLの脆弱性を検証するシステム XPIA（エクスピア）

野島 良
（のじま りょう）
ネットワークセキュリティ研究所
セキュリティ基盤研究室
主任研究員

2006年、NICTに入所。ネットワークセキュリティ、特に公開鍵暗号、暗号プロトコルの設計に従事。博士（工学）。

黒川 貴司
（くろかわ たかし）
ネットワークセキュリティ研究所
セキュリティ基盤研究室
有期技術員

2010年、NICTに入所。暗号技術の安全性評価に関する研究開発に従事。

盛合 志帆
（もりあい しほ）
ネットワークセキュリティ研究所
セキュリティ基盤研究室
室長

1993年、大学卒業。日本電信電話（株）、ソニー（株）を経て2012年、NICT入所。暗号技術の設計及び安全性評価に関する研究や国際標準化に従事。博士（工学）。

概要

NICTでは、情報通信ネットワークを安心・安全に利用するために必要なセキュリティ技術の研究開発を行っており、特にインターネット上で最も利用されている暗号通信規格SSL（Secure Socket Layer）の信頼性向上のための研究を行っています。このたび、SSLの脆弱性を検証するシステムXPIA（エクスピア）を開発しましたのでご紹介します。

背景

電子商取引、インターネットショッピングなどのオンラインサービスが広く普及したことにより、膨大な量の情報がネットワークを介して行き交うようになっています。このようなサービスを提供する多くのWebサイトでは、SSLと組み合わせたプロトコルHTTPSを使うことが主流となっています。SSLはインターネット上で安全な通信を行うために最も広く利用されている規格の1つです。その一方、軽微なものまで含めると、何らかの攻撃に悪用される可能性のある仕様上や実装上の問題点を含む多くの脆弱性がこれまで報告されてきました。

2012年、カリフォルニア大学とミシガン大学の研究チームによりSSLに対する新たな脅威が報告され、世界中のSSLサーバの0.4%に当たる2万台にも及ぶSSLサーバについてそのRSA秘密鍵が暴かれる可能性があり、SSLサーバ証明書の偽造などが可能となる危険な状態になっていることが明らかになりました。この新たな脅威によりどのSSLサーバが危険な状態にあるかなど、その実態を把握することが喫緊の課題となっていました。

RSA暗号に対する新たな脅威

報告されたSSLの脆弱性は、SSLの生命線であるRSA暗号に関わるものでした。RSA暗号は、ユーザとサーバ間の秘密通信を支える技術であり、素因数分解が難しいことを利用した暗号技術です。RSA暗号における素因数分解問題とは、pとqを素数とすると、N=pqが与えられたときに、pとqを求める問題です。RSA暗号では、Nは公開鍵と呼ばれ、平文の暗号化に用いる公開できる情報ですが、素数p、qは暗号文の復号に用いる秘密にしなければならない情報です。このため暗号解読を目的とする攻撃者は、秘密情報p、qを入手すると、ユーザとサーバ間の全ての通信を解読することが可能となります。各サーバはSSLを運用するためにRSA公開鍵Nを保管しており、ユーザはSSLを使った通信に先立ち、この公開鍵Nをサーバからダウンロードします（図1）。各サーバの公開鍵は安全性を担保するために、サーバごとに異なるものとなるよう、各サーバで独立に生成した公開鍵を利用します。理論的には素数は十分に多いため、全サーバで異なる公開鍵を利用することが期待されます。しかし、先の報告によると、サーバAにおいては公開鍵$N_A = pq_A$を、別のサーバBにおいては公開鍵$N_B = pq_B$といったように、共通のpを使用している事例が多数存在することが報告されたのです。素数が重複する2つの公開鍵N_A、N_Bの最大公約数を計算することにより、p、q_A、q_Bを得ることは容易であるため、攻撃者はサーバAとサーバBが関わる通信を盗聴することが可能となります。NICTでは、この新たな攻撃手法による実際の脅威がどのようなものか、どのSSLサーバが危険な状態にあるかなどを明らかにするためのシステムXPIAを構築しました。

図1　SSLサーバから証明書をダウンロードする様子

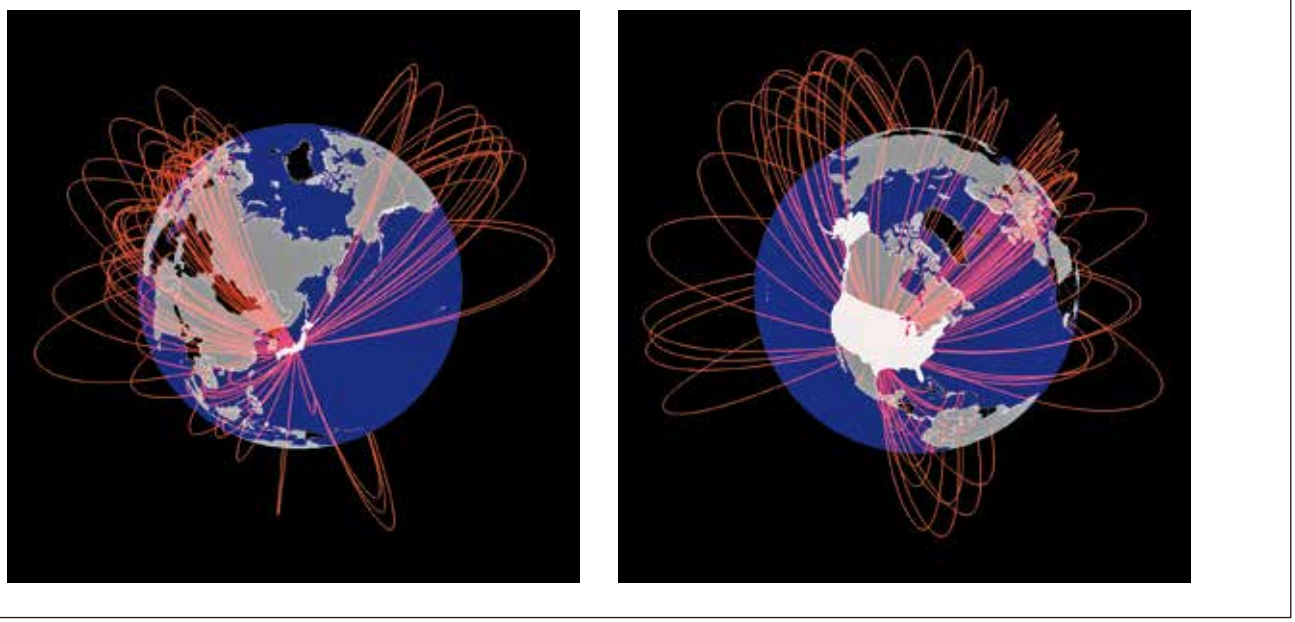

図2　今回開発した「XPIA」による脆弱性分布の表示例

XPIAの構成

1. **公開鍵証明書の収集:** クローラを用いて、世界中のサーバに接続し、公開鍵証明書をダウンロードします。また、今回の調査では、SSL Observatory[*1]が入手した公開鍵証明書も利用しました。
2. **RSA公開鍵の抽出:** 入手した公開鍵証明書からRSA暗号の公開鍵を抽出します。
3. **RSA公開鍵の解析:** 抽出した各サーバのRSA公開鍵について、全ての対の最大公約数を計算します。最大公約数が1でない場合は、互いに共通の素数を使用しているため、RSA公開鍵を素因数分解できることを意味します。本処理により、素因数分解可能なRSA公開鍵とそれに対応する公開鍵証明書及びそれを使用しているSSLサーバのIPアドレスを得ることができます。
4. **図示:** 図2はRSA公開鍵の解析により得られた情報を元に、共通の素数を用いたRSA公開鍵を使用しているSSLサーバの対を赤い線で結んだものです。

解析結果

XPIAを用いて、SSLサーバから収集した公開鍵証明書から抽出したRSA公開鍵の脆弱性を検証したところ、今回の調査範囲では素因数分解可能な脆弱な公開鍵を使用しているインターネットバンキングやオンラインショッピングなどのサービスサイトは見つかりませんでした。しかし、少なくとも世界中で2,600台を超えるSSLサーバが脆弱な公開鍵を2013年10月時点でも利用していることがわかりました（図3）。

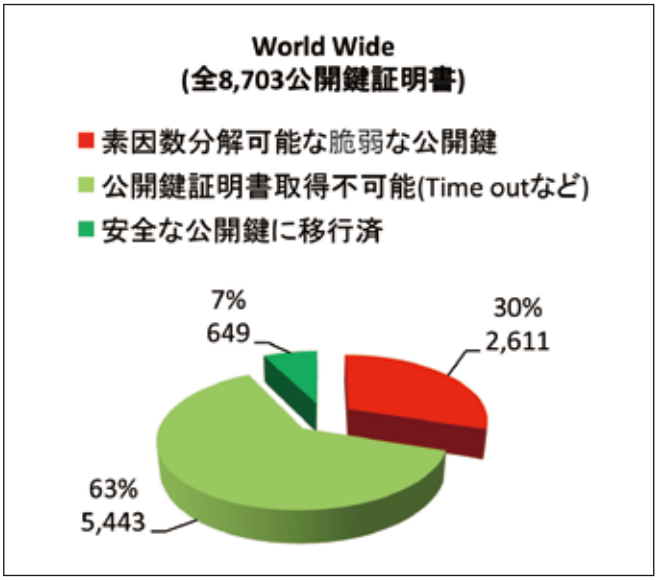

図3　脆弱な公開鍵を持つ公開鍵証明書の最新状況

今後の展望

本システムにより、SSLに対する新たな攻撃手法による実際の脅威を把握しました。NICTでは、本システムをBEAST攻撃[*2]やRC4[*3]への攻撃などにも対応できるよう拡張し、ネットワーク上での安全な通信を確保するための研究開発を進めていきます。

＊1　SSL Observatory
世界中で利用されている公開鍵証明書の状況を調査することを目的として、IPv4アドレス空間において入手可能な公開鍵証明書を収集しているプロジェクト。

＊2　BEAST攻撃
SSLの特定のバージョンにおける暗号利用モードCBC (Cipher Block Chaining)の脆弱性を利用した攻撃。

＊3　RC4
Ronald Rivest によって開発され、SSLや無線LAN規格で採用されたことで世界中で広く利用されている暗号技術の1つ。