NISC NEWS

第１８号（２００８年２月２１日発行）
内閣官房情報セキュリティセンター
National Information Security Center (NISC)

★目次

１．情報セキュリティ施策紹介

【 政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針（案）について 】

１ はじめに

電子申請、電子入札等の電子政府システムを始めとした政府機関の情報システムにおいては、データの改ざん、盗聴、なりすまし等を防止するため、様々な技術が使用されていますが、その一つに、暗号技術があります。

政府機関において使用されている暗号技術については、基本的に「電子政府推奨暗号リスト」（http://www.cryptrec.jp/images/cryptrec_01.pdf）に記載されたアルゴリズムから選択することとなっておりますが、一般的に暗号アルゴリズムは、電子計算機の能力の向上などにより、時間の経過とともに安全性が低下していくため、これらについては、暗号技術検討会（※１）において、安全性の監視等が行われております。このような中、近年、暗号技術検討会などで、本リストに含まれる、SHA-1（※２）及び RSA1024（※３）と呼ばれる一部の暗号アルゴリズムの安全性低下が報告され、これらを使用した情報システムにおいて、近い将来に現実的な問題が生じる可能性について指摘されております。

政府機関の情報システムの安全性及び信頼性を確保し続けるためには、これらの暗号アルゴリズムについて、情報システムのライフサイクル等を踏まえつつ、適切な時期に、より安全なものに移行する必要があります。その際には、関係する情報システム間における相互運用性を確保する観点や政府機関全体の情報セキュリティ向上の観点から、政府統一的な対応が必要です。

そこで、情報セキュリティ政策会議においては、政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 について、より安全な暗号アルゴリズムに移行するための指針をとりまとめることとし、現在、パブリックコメントを受け付けております（受付期間２月４日～３月７日）。

具体的な指針案について、以下に概要をご説明します。

２ 指針案の内容

(1) 技術的な対応
- 新たな暗号方式として、SHA-256（※４）及び RSA2048（※５）を採用。
- 移行完了前に安全性低下の影響が発生する場合に備え、緊急避難的な対応も想定。

(2) 制度的な対応
- 各府省庁において、システムの移行時期を踏まえ、必要な対応の取りまとめ、移行手順書の整備を実施。

(3) スケジュール
- 2008 年度中に新たな暗号方式へ切り替える時期を検討。
- 2010 年度から 2013 年度までの間に、各府省庁における情報システムの対応を完了。

・ 総務省及び経済産業省は暗号の安全性に係る状況を監視し、内閣官房は必要な情報を速やかに各府省庁に提供。

3 参考

米国では期限を決めて対応する方法を採用し、2010 年末以降、政府機関において、SHA-1 の新規使用を停止する方針です。しかし、SHA-1 の安全性が保てなくなる時期については専門家の間でも意見がわかれているところです。このため日本では、暗号の安全性低下の状況を監視しながら対応する方法を選択し、政府が暗号の安全性を監視し、安全性低下が早まった場合は、緊急避難的な対応を実施することとしております。

パブリックコメントを受け付けている移行指針案については、ホームページで公表しております。ご興味のある方は、是非次の URL で御覧ください。(http://www.nisc.go.jp/active/general/niscrypt.html)

※1:総務省大臣官房技術総括審議官及び経済産業省商務情報政策局長の私的研究会
※2:ハッシュ関数 SHA の一つで、与えられたデータから 160 ビットの固定長の値を生成する
※3:公開鍵暗号方式の一つで、暗号アルゴリズムを RSA、鍵の長さを 1024 ビットとしたもの
※4:ハッシュ関数 SHA の一つで、与えられたデータから 256 ビットの固定長の値を生成する
※5:公開鍵暗号方式の一つで、暗号アルゴリズムを RSA、鍵の長さを 2048 ビットとしたもの

2. 誰でもわかる情報セキュリティ用語

【 WPA / WPA2 】

無線 LAN は、ケーブルの取り回しを気にしなくてよいという利便性に加えて、十分な通信速度が確保できるようになり、また低価格化も進んだために、あらゆる場面で用いられています。しかし、電波で通信している以上、第三者に傍受されてもそれに気付くことは困難であり、通信内容を盗聴される危険性があります。

一般的に普及している無線 LAN 規格 IEEE 802.11 シリーズには、WEP(wired equivalent privacy)、WPA(Wi-Fi protected access)、WPA2(Wi-Fi protected access 2)という、通信暗号化のための3種類のセキュリティ規格があります。WEP は3つの中では、現在最も多く利用されている規格で、データの受信側と送信側とが共通のキーを持つことで、データの暗号化/複号化、および改ざんされていないことの検証を行います。ところが、WEP で用いられる RC4 という暗号化アルゴリズムに脆弱性があること、またキーの長さが十分でないことなどから、フレームをキャプチャして解析用のツールを用いれば、短時間で WEP キーを解読できることが報告されています。

そこで策定されたのが、WPA と WPA2 です。2003 年から対応製品が登場した WPA は、WEP には無かったユーザ認証機能を備え、暗号化プロトコルは WEP の改良版である TKIP(temporal key integrity protocol)を採用していますが、WEP との互換性を持っています。これは、ファームウエアやドライバを更新すれば、WEP を利用していた従来機器でも WPA に対応できるようにするための配慮です。もう一つの WPA2 は、WEP との互換性はありませんが、より強力な暗号プロトコルと暗号アルゴリズムを採用しています。

ネットワーク機器やソフトウェアの設定というのは、最初に接続する際にやって上手くつながってしまうと、その後で見直すことは少ないのではないでしょうか。ですので、皆さんが家庭や職場で利用されている無線 LAN 機器も、WAP/WAP2 に対応しているにもかかわらず、WEP のまま使われているかも知れません。不安な方は、是非一度確認してみることをお勧めします。

3. NISCOLUMN (ニスコラム)

【 ゴールが見えないセキュリティの道を進むためには 】

インターネットが広く普及してから十年くらいの時が流れました。これを読んでいる皆さまも日々様々なホームページを見ていることと思います。私は、インターネットによって大きく変わったと感じる点の一つが、個人がブログや日記などのホームページを立ち上げて、個人の意見を表明する場が増えたことではないかと思います。私

はインターネットに点在する個性豊かなサイトが好きで、Web ブラウザのブックマークにお気に入りや情報源となるサイトを登録して、日々巡回にいそしんでいます。

その反面、最近は更新が途絶えたり、閉鎖されたりするホームページもよく見かけます。何年か前に面白いと思ってブックマークしておいたホームページを見直そうとしてアクセスしたら、閉鎖している場合も多くなってきました。個人に限らず大抵のホームページは自主的に立ち上げている場合が多いので、公開するのも閉鎖するのも自由です。しかし、自分の経験を振り返りながらその理由を考えてみると、以下のようなことが浮かびました。

・就職、転勤、転居など環境が変わった
・仕事が忙しい時期に入った
・別の趣味に多く時間をかけるようになった
・更新するネタが無くなった
・ホームページの更新に飽きた

ホームページの更新以外の優先事項ができる場合など外的な要因がある一方で、外からの刺激が無い場合は逆に淡々と続けていくのにも飽きが来ます。適度な刺激を受けながら、また、他の日常生活や仕事と両立するというバランスを保つのは結構大変です。

今書いてきたことを情報セキュリティに当てはめて見ると、実は凄く大変であることが分かります。情報セキュリティへの取り組みは情報を扱う限り終わりが来ることはないので、ずっと継続し続けなければならないことになります。仕事が忙しい時も情報セキュリティについてさぼることはできませんし、環境が変わったらその新しい環境に合わせるためにかえってやるべきことが増えてしまいます。IT の世界では、技術の進展や不正アクセスやウイルスなどの脅威の変化が早く、状況の変化については事欠かないので刺激は心配ありませんが、逆に刺激がありすぎて力尽き果ててしまうかも知れません。情報セキュリティについては今まさに IT 化と共に現在進行中で、新たな対策を打ちながら、実施している対策を維持し続けている状況であり、ゴールが見えない深く、長いイバラの道です。

その道を途絶えることなく進めていくためには様々な工夫が必要かと思います。一つ思いつくのがドキュメント化して共有することです。ノウハウなどは属人的になってしまいがちで、ある特定の人しかできないことになっている場合があると思います（逆にそのノウハウが人の強みになりますが）。それ以外にも情報はたくさんあるが、どこかに埋もれてしまい必要なときに出てこないという場合も良くあります。

そのノウハウや情報を、マニュアル、チェックリストあるいは簡単なレポートなどの形で集めて、蓄積して、まとめて共有することで、属人的になっていた作業が分担でき、様々な情報が効果的に活用できるなどの効率化が図れるばかりでなく、ミスや漏れを未然に防止する効果があるのではないかと思います。ドキュメント化をするのが大変ですが、後になって驚くような効果を上げるようなこともあります。

ちなみに、NISC は人が定期的に交代する職場なので、うまく引き継ぎをしないとそれまでに蓄積した記憶やノウハウが無くなってしまう恐れがあります。いつか私も異動になり、引き継ぎをする時が来るはずなので、その時の自分への備忘録という意味も込めてこのコラムに書き残したいと思います。

（さくら・桜・佐倉）

＜バックナンバー・配信先変更・配信中止＞

本メールマガジンにおけるバックナンバーの取得及び配信先の変更、配信の中止等は下記の URL から可能です。

http://www.nisc.go.jp/nisc-news/

＜御意見、御感想＞

http://www.nisc.go.jp/mail.html