SHA-1 脆弱化（衝突困難性の脆弱化）に関する公開情報について

2005.11.24

タイムビジネス推進協議会

ガイドライン分科会

2005 年 2 月に報告された SHA-1 脆弱化（衝突困難性の脆弱化）に関する公開情報を収集し、状況整理を行った。2005 年 11 月現在、SHA-1 の衝突困難性が、総当り攻撃による 2 の 80 乗よりも少ない 2 の 63 乗でブレイク可能であるとの報告がなされている。しかしながら、第三者による追試・追認がなされたという報告は見られない。また、NIST の SHA-1 リプレイス計画(2010 年までには、SHA-1 から SHA-2 シリーズへ移行)にも変更は無い状況である。今後も更なる情報収集・分析が必要であると思われる。

現状の国内外の公開情報（学術論文などを除く）

#	日時	公開者	概要
1	2005.2.15	Bruce Schneier	著名な暗号学者である Bruce Schneier が、ブログ(Weblog)上で公開。「Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu からなる暗号チーム」の「SHA-1 の脆弱化(衝突困難性の脆弱化)の論文(一般公開されていない)」の結論を紹介。 ・内容は、新しい攻撃方法により、SHA-1 の衝突困難性が、総当り攻撃による 2 の 80 乗よりも少ないオペレーション（2 の 69 乗）でブレイク可能であると報告。
2	2005.2.17	ECRYPT	Recent Collision Attacks on Hash Functions: ECRYPT Position Paper ECRYPT Network of Excellence www.ecrypt.eu.org 17. February 2005

			Revision 1.1 http://www.ecrypt.eu.org/documents/STVL-ERICS-2-HASH_STMT-1.1.pdf SHA-1 の脆弱化 (2 の 69 乗)について説明しており、ECRYPT としての勧告を示している。勧告の内容は、以下の通り。 1. In general, hash functions with outputs shorter than 160 bits, are not recommended unless the consequences of an attack resistance less than 2^80 operations have been fully considered. 2. We see no immediate need to be concerned about the security of the HMAC construction used with either MD5 or SHA-1. However, cryptanalytic advances on MD5 suggest that it might be prudent to replace HMAC-MD5 with HMAC-SHA-1, or preferably HMAC-h for some still ¥collision resistant" hash function h, as soon as convenient. 3. Even though new attacks cannot currently produce highly controlled message collisions, ECRYPT does not recommend the continued use of MD5 in signature applications with medium to high security requirements. In light of the recently announced attacks on SHA-1, though we have no information on the severity/impact of the collisions that may be obtained, we also recommend to be cautious with new deployments of SHA-1, in particular since it cannot be excluded that the announced attacks will be improved in the near future. It seems unlikely that already existing SHA-1 based signatures are threatened.

			4. ECRYPT sees no immediate need to replace RIPEMD-160 for current and near term (3-5 years) applications. 5. In the longer term, ECRYPT recommends, where possible, that the newer family of hash functions specified in FIPS 180-2, or alternatives such as Whirlpool [16], be considered.
3	2005.2.22	NIST	NIST の速報。 2005.2.22 公開、ドキュメント日付 2005.2.18 「NIST Brief Comments on Recent Cryptanalytic Attacks on SHA-1」 http://csrc.nist.gov/news-highlights/NIST-Brief-Comments-on-SHA1-attack.pdf ・攻撃の技術的詳細は不明。継続して情報収集・分析することを意向表明。 ・影響度に関しては、「タイムスタンプ、公証サービス」に影響があるのではとの指摘。 ・SHA-1 を 2010 年までに廃棄し、SHA-224/256/384/512 に以降する従来どおりの計画に関しては見直し無し。
4	2005.3.5	Eric Rescorla， RTFM, Inc.	62nd IETF ミーティング(ミネアポリス)の Open Security Area Directorate WG (SAAG)にて、「SHA-1 と MD5 についての状況」のプレゼンテーションあり。 （Eric Rescorla，RTFM, Inc.） http://www3.ietf.org/proceedings/05mar/slides/saag-3.pdf
5	2005.03.11	RSA 社	2005.03.11 公開 「Hash Function Update Due to Potential Weakness Found in SHA-1」 http://www.rsasecurity.com/rsalabs/node.asp?id=2834

<table>
<tr><td></td><td></td><td></td><td>・報告された攻撃(2 の 69 乗)は、非常に大きな計算機パワーを必要とするため、現時点では、影響はないと思われる。ただし、攻撃方法がより向上する可能性はある。</td></tr>
<tr><td>6</td><td>2005.4.8</td><td>IPA</td><td>IPA 調査研究報告書(実施者：三菱総合研究所)
2005.4.8 公開

「暗号の危殆化に関する調査」
http://www.ipa.go.jp/security/fy16/reports/crypt_compromize/index.html

・ 暗号の危殆化のレベル分け(レベル 0 からレベル 4)を提案(P.65 図 6.1)
表：「暗号の危殆化に関する調査」P.65 図 6.1 より一部抜粋
<table>
<tr><th></th><th></th><th>レベルの要件</th></tr>
<tr><td>レベル 0</td><td>安全</td><td>・攻撃手法が報告されていない</td></tr>
<tr><td>レベル 1</td><td>確認</td><td>・ ある攻撃手法が報告されている
・ 暗号監視機関により、上の攻撃手法に関する事実確認と継続的調査が必要との判断が示されている
（暗号監視機関により状況報告として公表されている）</td></tr>
<tr><td>レベル 2</td><td>注意</td><td>・ ある攻撃手法について信頼のおける情報源から検証結果が提示されている
・ 暗号監視機関により、上の検証結果に基づき主に理論的観点からその攻撃手法が近い将来に脅威となり得るとの判断が示</td></tr>
</table>
</td></tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td>
<table>
<tr><td></td><td></td><td>されている
（暗号監視機関により注意喚起として公表されている）</td></tr>
<tr><td>…</td><td>…</td><td>・ ….</td></tr>
</table>
・ 各レベルの標準的な対策を提示(P.66 図 6.2)
表：「暗号の危殆化に関する調査」P.65 図 6.2 に基づき作成
<table>
<tr><th></th><th>対策</th></tr>
<tr><td>レベル 0</td><td>暗号危殆化判断用ガイドライン、暗号危殆化対処用ガイドライン作成</td></tr>
<tr><td>レベル 1</td><td>情報収集、及び影響分析</td></tr>
<tr><td>レベル 2</td><td>リスク分析、代替暗号検討、改修・移行に関する見積</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>
【TBF 注釈】
今回の SHA-1 の脆弱化(衝突困難性の脆弱化)の現状ステータスは、上記の報告書のレベルでいうと、「1」である。「対策レベルとしては、情報収集・影響分析レベル」。
</td>
</tr>
<tr>
<td>7</td>
<td>2005.4.20</td>
<td>IPA CRYPTREC</td>
<td>IPA の報告。
「ハッシュ関数に関する研究動向について」
http://www.ipa.go.jp/security/enc/CRYPTREC/fy17/cryptrec20050420_report01.html

・攻撃の技術的詳細は未確認。継続して情報収集・分析することを意向表明。
・「電子政府推奨暗号リスト」の観点からは、従来どおり、新規の電子政府用システムを構築する際に利用するハッシュ関数は、ハッシュ値が 256 ビット以上を推奨。</td>
</tr>
</table>

8	2005.5.12	Eli Biham Computer Science Department	2005 年 5 月 12 日の RSA Conference 2005 Japan での発表。 Recent Advances in Hash Functions: The Way to Go Eli Biham Computer Science Department Technion, Haifa 32000, Israel May 12, 2005 スライドタイトル「Attacks on the MD4/SHA Family」において、SHA-1 の衝突困難性の脆弱化は、2 の 69 乗ではなく、2 の 67 乗と述べている。最初の報告時点(2005/2)よりも解読アルゴリズムが改良されていることが想定される。引用文献は、下記の通り。 SHA-1	an attack for finding collisions with complexity about 2^67(Wang et al., 2005)
9	2005.6.23 〜 6.24	Conference Hash Functions	European Network of Excellence in Cryptology ECRYPT のワークショップの一つ。ハッシュ関数の研究開発に関する国際会議。 招待スピーカーの講演のうち、SHA-1 の衝突困難性の脆弱化(2 の 69 乗)を報告した研究者の発表あり。内容は、これまでの内容を取りまとめたもの。 ・ Xiaoyun Wang What is the potential danger behind the collisions of hash functions? http://www.ecrypt.eu.org/stvl/hfw/Wang.pdf
10	2005.8.14 〜 8.18	CRYPTO 2005	暗号技術に関する国際学会。

			Shamir 氏が、Wang さんの代わりに、最新結果を報告。SHA-1 の衝突困難性が、2 の 63 乗(これが下限ではなく、さらに下がる可能性あり)と報告。 http://www.iacr.org/conferences/crypto2005/rumpSchedule.html の Session 1: Cryptanalysis 19:35 - 19:44 New Collision Search for SHA-1 Xiaoyun Wang, Andrew Yao and Frances Yao (communicated by Adi Shamir) の部分（Shamir 氏が代理で講演） http://www.iacr.org/conferences/crypto2005/r/2.mov http://www.iacr.org/conferences/crypto2005/r/2.pdf
11	2005.10.31 ～11.1	NIST のワークショップ	2005 年の 10 月 31 日から 11 月 1 日の間に開催される「CRYPTOGRAPHIC HASH WORKSHOP」 http://www.csrc.nist.gov/pki/HashWorkshop/index.html 発表資料は、以下のサイトからアクセス可能。 http://www.csrc.nist.gov/pki/HashWorkshop/program.htm キーノート・スピーチでは、Wang さんが、SHA-1 の SHA-1 の衝突困難性が、2 の 63 乗と発表。 Keynote Speech: Cryptanalysis of SHA-1 Hash Function (ppt only) Xiaoyun Wang, Tsinghua University 上記のトップページからリンクされる「NIST の最新の公式表明」は、以下の通り。 http://www.csrc.nist.gov/pki/HashWorkshop/NIST%20Statement/Burr_Mar2005.html **NIST brief comment on recent cryptanalytic attacks on SHA 1 and NIST**

			plans Cryptographic hash functions that compute a fixed size message digest from arbitrary size messages are widely used for many purposes in cryptography, including digital signatures. NIST was recently informed that researchers had discovered a way to "break" the current Federal Information Processing Standard SHA-1 algorithm, which has been in effect since 1994. The researchers have not yet published their complete results, so NIST has not confirmed these findings. However, the researchers are a reputable research team with expertise in this area. Previously, a brute force attack would expect to find a collision in 2 80 hash operations. The researchers assert the “computational complexity” of their new attack would be less than 2 69 hash operations to find a collision. This attack is of particular importance in digital signature applications, such as time stamping and notarization. However, many digital signature applications include contextual information that will make this attack difficult to carry out in practice. Other applications of hash functions, such as Hash-Based Message Authentication Codes (HMACs) and key derivation, are believed unaffected by this attack. Due to advances in computing power, NIST already planned to phase out SHA-1 in favor of the larger and stronger hash functions (SHA-224, SHA-256, SHA-384 and SHA-512) by 2010. New developments should use the larger and stronger hash functions. In addition, agencies are encouraged to develop plans on a timely basis for an orderly transition to the larger hash functions, taking into account system sensitivity in prioritizing their efforts. As the full details of this attack become known, NIST will publish additional guidance. To improve our understanding of the cryptographic strength of hash functions, NIST encourages further

			research in hash functions and their properties. ***NIST will continue to work collaboratively with the cryptographic community in this effort and intends to host a workshop in the Autumn of 2005 on the current state of Hash functions and their analysis to help NIST plan its policies and standards in this area.*** William E. Burr NIST Manager, Security Technology Group 301-975-2914 *Last updated: April 5, 2005* *Page created: December 28, 1997*

-以上-