INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

算術演算をベースとする
ハッシュ関数安全性評価手法に関する調査
概要版報告書

2008 年 5 月

独立行政法人　情報処理推進機構

算術演算をベースとするハッシュ関数安全性評価手法に関する調査　概要

富士通株式会社

1. 背景

近年、暗号プリミティブの解析技術が著しく進歩するに従い、DES 暗号や一部のハッシュ関数に関し、その危殆化が懸念されており、特に電子政府システム、電子商取引システムなどのデジタル署名に用いられるハッシュ関数の利用に対し、注意が必要となっている。とりわけハッシュ関数 SHA-1 の安全性に対しては、米国標準技術研究所（NIST : National Institute of Standards and Technology）でも注意喚起を行っており、次世代ハッシュ関数 AHS の公募が計画されている。

次世代のハッシュ関数としては、従来のハッシュ関数とは異なる理論に基づいて構成される可能性もあるが、現用の SHA-1 や MD5 といった算術演算をベースとしたもの、あるいは AES の設計思想に基づく S-box をベースとしたもの等、これまでに知られている安全性根拠に基づいて構成される可能性も高い。特に現在広く用いられている SHA-1 や MD5 といった算術演算をベースとしたハッシュ関数の安全性評価手法については、より一層緻密な評価技術の開発が期待されている。

そこで、本報告では、次世代ハッシュ関数の安全性を評価するための手法として、現在研究開発が進められているハッシュ関数の動向を調査し、特に SHA-1 等の算術演算に基づくハッシュ関数の安全性評価手法のツール化を検討し、その適用可能性、実現性、課題を抽出する。

2. 算術演算をベースとするハッシュ関数の脆弱性に関する調査

本章では、算術演算をベースとした MD5, SHA-1 等のハッシュ関数について、ここ数年で指摘された差分解読法の実現可能性と、それが実現した際の、各種暗号プロトコルやアプリケーションへの影響について調査する。

2.1. Fingerprint

ハッシュ関数の最も基本的な応用として fingerprint が挙げられる。多くの通信プロトコルやアプリケーションでは、扱うドキュメントや画像、音声等あらゆる電子データに対して、各々異なる識別子(固定ビット長)を付与し、データを区別する必要がある。この電子データ固有の識別子を電子データに対する fingerprint と呼ぶ。

fingerprint は SSL などでの証明書の正当性の保証, PGP の公開鍵の本人性保証等で利用されており、改竄検知やなりすまし防止に役立てられている。fingerprint で利用されるハッシュ関数としては、MD5 や SHA-1 等が多く用いられているが、その一方で、MD5 等で指摘されている脆弱性を利用することで、さまざまな fingerprint の偽造が可能であることが示されている。

2.2. APOP

APOP は、電子メールクライアントとサーバ間のパスワード暗号化プロトコルであり、処理の内部でハッシュ関数 MD5 を用いることが規定されている。APOP は，電子メールのクライアントとサーバの間で、チャ

レンジ・レスポンス方式に基づいた通信を行い、クライアントを認証するプロトコルであり、パスワードが通信路上を直接流れないようにしたものである。

APOP は、クライアントとサーバの経路上に攻撃者によって偽造されたメールサーバが存在し、クライアントと正当なサーバとの間の認証処理を偽造サーバが複数回なりすまし可能な場合に、現実的な計算量でパスワードが漏洩することが示されている。

2.3. HMAC,NMAC

HMAC および NMAC は 1996 年に提案されたハッシュ関数をベースとしたメッセージ認証コード (MAC) である。HMAC は TLS, SSH, IPsec 等に実装され、広く使われている方法である。HMAC および NMAC は、ある条件の元で安全であることが証明されているが、その一方で、MD4 を用いた HMAC-MD4 ならびに NMAC-MD4 、MD5 を用いた NMAC-MD5 についてディスティングイッシュ攻撃、更にはキーリカバリ攻撃が可能であることが示されている。

2.4. X.509

X.509 は ITU や RFC 等で標準化された公開鍵証明書フォーマットであり、S/MIME や SSL/TLS、などの多くのセキュリティプロトコルが X.509 をベースにしている。X.509 証明書に MD5 等脆弱なハッシュ関数が利用されている場合、所有者と公開鍵が異なる以外、全て同じ X.509 証明書の組を作成することができることが示されている。MD5 の場合 X.509 の偽造にかかる計算量は 2^{50} 回程度であると述べられており、コリジョン探索計算量が少なければ、現実的な計算量での偽造が可能となる。特に SHA-1 を用いた X.509 証明書プロトコルは、あらゆる用途で使われており、本偽造が成功するとその社会的影響は甚大であることから、SHA-1 の詳細なコリジョン探索計算量評価が急務である。

2.5. IPSEC

IPsec(IP Security) は、IETF(Internet Engineering Task)において，IP(Internet Protocol)レベルの暗号化機能として標準化されたものであり、認証や暗号のプロトコル，鍵交換のプロトコル，ヘッダー構造など，複数のプロトコルを総称するものである。IPsec ならびに IKE では暗号化機能を実現するための部品として暗号学的ハッシュ関数を利用しているが、ここ数年の間に相次いで発表されたハッシュ関数の脆弱性発見に関する対応について、2007 年 5 月に、IKE（Internet Key Exchange）および IPsec におけるハッシュアルゴリズムの使用に関する文書が RFC 4894 として承認されている。RFC 4894 では IKEv1 と IKEv2、IPsec プロトコルがどのようにハッシュ機能を使うかについて述べられており、また、MD5 および SHA-1 アルゴリズムの劣化した衝突耐性について、こうしたプロトコルの脆弱性がどのような水準にあるのかについても説明している。

2.6. PKCS

PKCS(Public Key Cryptography Standards) は RSA Laboratories によって策定されている RSA 公開鍵暗号ベースの暗号化および認証プロトコルである。PKCS は #1 から #15 までである。調査報告書では 2008 年 2 月現在のカレントバージョンならびにこれらにおけるハッシュ関数の利用状況についてまとめる。

2.7. SSL/TLS

SSL(Secure Socket Layer), TLS (Transport Layer Security)の RSA 暗号を用いた公開鍵暗号規約において、公開鍵に対する証明書の形式としては、X.509 公開鍵証明書を用いることが規定されている。

この X.509 証明書については、前述の MD5 に対するターゲットコリジョンを用いた偽造により、改竄される危険性が指摘されている。従って SSL/TLS の公開鍵証明書に MD5 等脆弱なハッシュ関数を用いると、サーバの偽造が可能となる場合がある。ただし、本攻撃法による SSL/TLS サーバの改竄が成功するには、公開鍵証明書発行時点で、二種類の X.509 公開鍵証明書を準備する必要がある。

2.8. タイムスタンプ

タイムスタンププロトコルは、ある時点でのドキュメントの存在を保証する暗号スキームであり、RFC3161 で規定されている。タイムスタンププロトコルの内部において、X.509 規格に基づく RSA 公開鍵証明書を用いているため、脆弱なハッシュ関数を用いた場合には、X.509 に対する攻撃法と同様の方法で証明書の偽造が可能となる可能性があり、MD5 等、脆弱なハッシュ関数を用いた場合には、ドキュメントの時刻情報を改竄されるおそれがある。ただし、日本国内においてタイムスタンププロトコルに基づく認証業務を行う際、SHA 系ハッシュ関数を使う場合には SHA-256 以上のビット長を持つハッシュ関数を用いることが規定されており、MD5, SHA-1 は含まれていない。

3. 算術演算をベースとするハッシュ関数の安全性評価ツール仕様検討

3.1 ハッシュ関数の安全性評価

ハッシュ関数を設計する場合、そのハッシュ関数が既存の攻撃に対してどの程度の耐性があるのかを見積もることは大変重要である。この「耐性」の客観的な評価指標の一つとして、コリジョン探索の手間について見積もった概算計算量が挙げられる。本報告書では、算術演算をベースとするハッシュ関数を対象とし、差分攻撃をベースとしたコリジョン探索を適用した際の探索計算量を評価するための安全性評価ツールの仕様検討を実施した。

コリジョン探索で必要となる計算量の概算値は数式 1 で与えられることが知られている。

数式 1. コリジョン探索計算量

（コリジョン探索計算量）$=2^{(N-n)}\times B$

N = 満たすべき全てのコンディションの数

n = メッセージモディフィケーションが適用可能なコンディションの数

B = マルチブロックコリジョンにおけるブロック数

3.2. 安全性算出モジュール

数式 1 より「コリジョン探索計算量」を見積もるためには、内部状態が満たすべき「コンディション」と「メッセージモディフィケーションが適用可能なコンディション」をそれぞれ導出すればよいことになる。ところでメッセージモディフィケーションには、「ベーシックメッセージモディフィケーション」と「アドバンストメッセージモディフィケーション」があり、数式 1 における「メッセージモディフィケーションが

適用可能なコンディションの数」とは、両者のうちのいずれかが適用可能であるコンディションの数のことを言う。攻撃者の立場でのコリジョン探索計算量の概算見積もりにおいては、メッセージ拡大非適用ステップに存在する全ての「コンディション」には「ベーシックメッセージモディフィケーション」が適用可能と仮定しても大きな問題はない。そこで今回のツールの検討においては、メッセージ拡大適用ステップに存在するコンディションのみを安全性算出の対象とし、これらのコンディションの総数と、アドバンストメッセージモディフィケーションが適用可能なコンディションの数とを考慮して安全性を算出することにした。本考え方に従い下記構成モジュールに基づく安全性評価ツールの仕様を検討した。

1. ローカルコリジョン構成モジュール
2. ディスターバンスベクトル構成モジュール
3. 差分パス構成モジュール
4. メッセージモディフィケーション適用判定モジュール
5. 安全性算出モジュール

3.3. ツールを用いたハッシュ関数の評価検討

本節では、前節までに検討した 5 個の安全性評価ツールが、実際のハッシュ関数の評価に使用可能かどうかを検討する。本検討では具体的に SHA-0、SHA-1、SHA-256 を対象として検討を行った。

- 適用可能性
  ツールを使用するための入力データが対象のハッシュ関数について準備可能かどうかを検討する。
- 実現性
  ツールを実行した際に現実的な時間で出力を得ることが可能かどうかを検討する。
- 課題
  上記 2 検討個目、及びそれ以外の事項において、ツールの実行に関連する課題を整理する。

結果は表 1 から表 5 の通りである。○は容易、△はやや困難、×は困難を意味する。

表 1. ローカルコリジョン構成モジュールの適用性検討結果

検討対象項目	ハッシュ関数名		
	SHA-0	SHA-1	SHA256
適用可能性	○	○	○
実現性	○	○	○
課題	小	小	小

表 2. ディスターバンスベクトル構成モジュールの適用性検討結果

検討対象項目	ハッシュ関数名		
	SHA-0	SHA-1	SHA-256
適用可能性	○	○	○
実現性	○	○	○
課題	小	小	小

表 3. 差分パス構成モジュールの適用性検討結果

検討対象項目	ハッシュ関数名		
	SHA-0	SHA-1	SHA-256
適用可能性	○	○	○
実現性	○	○	○
課題	小	小	小

表 4. メッセージモディフィケーション適用判定モジュールの適用性検討結果

検討対象項目	ハッシュ関数名		
	SHA-0	SHA-1	SHA-256
適用可能性	○	○	○
実現性	△	△	△
課題	中	中	中

表 5. 安全性算出モジュールの適用性検討結果

検討対象項目	ハッシュ関数名		
	SHA-0	SHA-1	SHA-256
適用可能性	○	○	○
実現性	○	○	○
課題	小	小	小

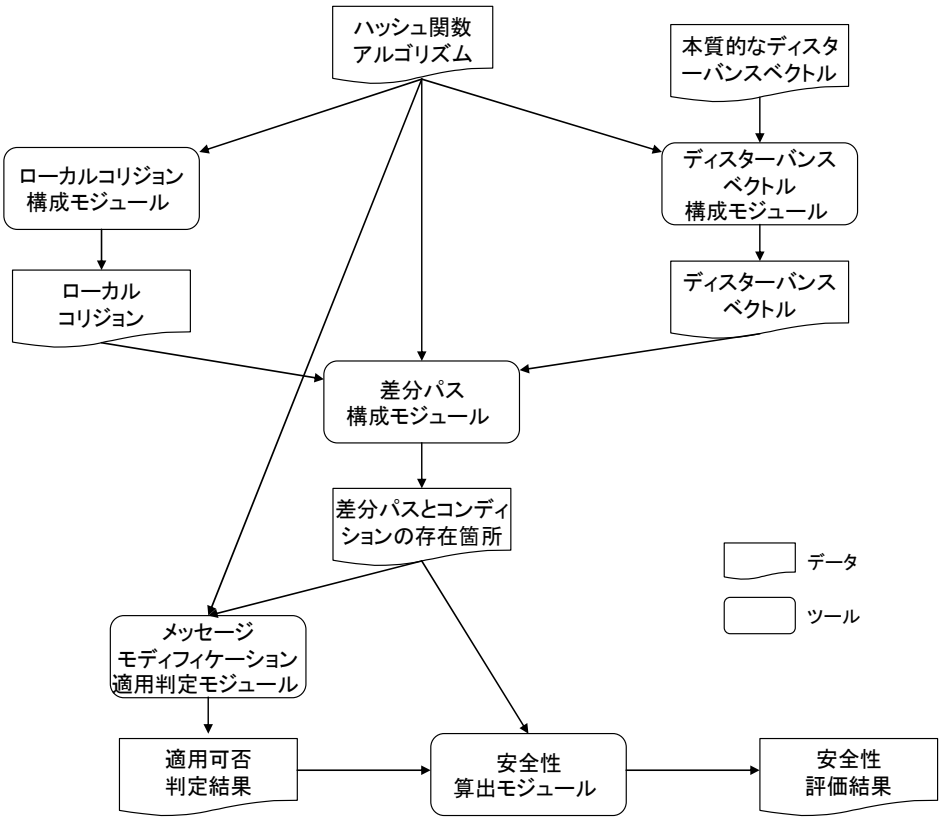

図 1. コリジョン探索計算量評価の処理のフロー
（上記の各モジュールには、上記のほかに制御パラメータなども入出力される）