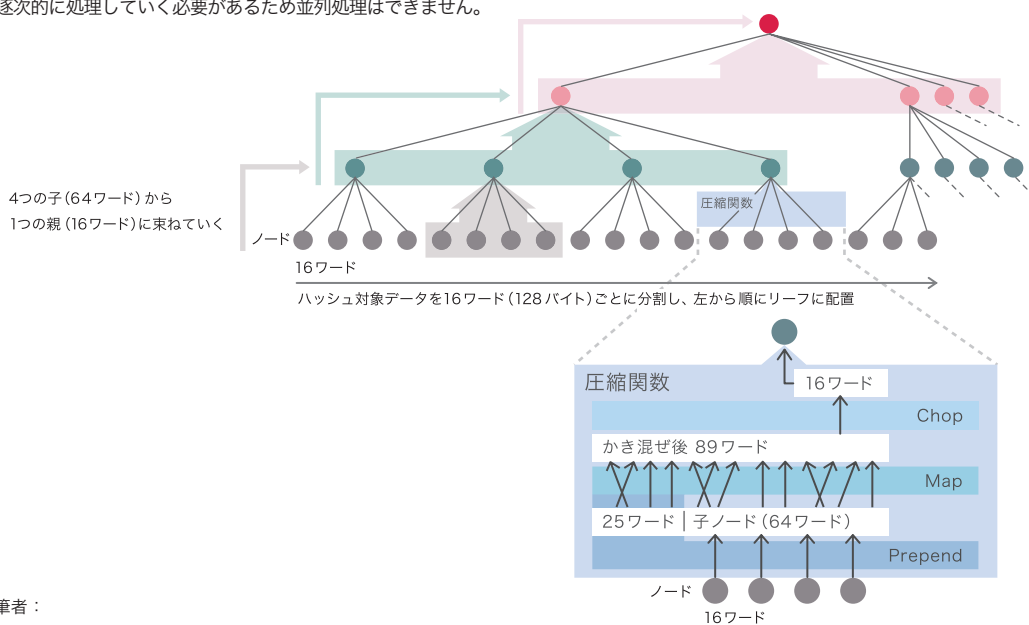


## インターネットトピック：MD6とは？

今年8月、IACR主催の暗号に関する国際学会「CRYPTO 2008」のInvited Talkにおいて、Ron Rivest (RSA暗号の設計者の一人) からMD6の概要が発表されました。勘のいい方はお気づきかと思いますが、MD6は同じくRivestによって設計されたセキュアハッシュ関数MD5の次世代版です。2004年のWangらによる攻撃<sup>\*1</sup>が発表されて以来、APOPパスワードが現実的な時間内で解読できる、X.509公開鍵証明書が偽造できる等、身近な利用場面での攻撃が発表され、MD5は使いものにならない、危ないというレッテルを貼られるようになりました。MD5よりも10年以上後に発表され、現在最も使われているSHA-1でさえ危殆化により日本政府機関の情報システムにおいては2013年を目途に排除されることが決まっています。HMAC等、使い方によってはまだ安全に利用できる用途もありますが、発表から17年経ったMD5はその役目を終えたと言えるでしょう。MD6はMD5の次世代版という位置付けですが、設計思想はまったく異なります。MD6は図のように、入力メッセージをリーフとしたtree hashの構造を持ちます。それぞれのノードは16ワード(1ワード=64ビット)のデータに相当します。圧縮関数は4つの子を1つの親に束ねていく再帰的な構造を持つため、並列処理が可能です。一方で、MD5、SHA-1/2らが採用しているMerkle-Damgaard (MD) 構成法はメッセージの頭から逐次的に処理していく必要があるため並列処理はできません。

次に圧縮関数を見ていきましょう。入力である子ノードの64ワード(4つのノード)に対し、固定データや鍵情報(MD6ではオプションで鍵情報を入力できます)等を含む25ワードを先頭につけ(Prepend)、ワードごとに変換を行い(Map)、後ろ16ワードのみを出力する(Chop)という3つの処理を行っています。Map処理に使われる演算子はXOR、AND、shiftのみで非常にシンプルな構成ですが、64ビットCPUでのソフトウェア評価でSHA-256と比較すると3倍程度遅いという結果が出ています。これは逆に、4チップのマルチコアを利用すればSHA-256以上の速度性能が出るということを示しています。

現在MD6の実装に必要な具体的な仕様は公開されていませんが、AHS<sup>\*2</sup>コンペティションの応募締切が10月末であることから、11月にはMD6の全貌が明らかになります。また同時期にMD構成法とは異なる設計思想を持つハッシュ関数が数多く登場すると考えられます。今後、ハッシュ関数の差し替えによるIPsecやTLS等のセキュリティプロトコルの新バージョン移行をスムーズに行える体制を確立する必要があります。IIJとしては今後もハッシュ関数の標準化動向を追い、最新情報を提供していきます。



執筆者：  
須賀 祐治  
IIJ サービス事業統括本部 セキュリティ情報統括部

\*1 CRYPTO2004のランブセッションにて、IBM P690による約1時間の計算でMD5のコリジョン(異なる入力に対して同じハッシュ値を持つこと)を見つげられることが発表された(<http://eprint.iacr.org/2004/199>)。この結果の詳細は翌年のEUROCRYPT2005にて2本の論文に分けて公開されている。

\*2 AHS (Advanced Hash Standard)。米国商務省配下の技術部門であるNIST (National Institute of Standards and Technology) による公募中の次世代ハッシュ関数。通称「SHA-3」。