RFC4270　インターネットプロトコルにおける暗号技術的ハッシュ関数についての攻撃

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	インターネットプロトコルのコミュニティは、SHA-1 および MD5（特に MD5 ）から段階的に、よりセキュアなハッシュアルゴリズムに移行する必要があります。				
	あらゆる大きさの 2 つの異なるメッセージも、メッセージ間の類似性の程度に関わらず、同一のハッシュ値となる可能性が極めて低い必要があります。				
	さらに、以前のいくつかの作業（特に、[PKIX-MD5-construction] ）によって示されたように、「どの主体が、そのハッシュ化されたオブジェクトの先頭にある素材を予測できるか？」を考慮することも重要です。				
	「現在の『衝突攻撃』は、少なくとも、2 つのメッセージの一方に『メッセージのビット中に一定の構造をもつこと』を要求すること」				
	「『両者が同一のハッシュ値をもち』かつ『現実世界の攻撃において使える』ような 2 つのメッセージを発見することは、単に同一のハッシュ値をもつ 2 つのメッセージを発見することより困難であること」				
	そのメッセージが署名されており、そのメッセージの受信者が「その署名者が、本当にそのメッセージを作成したこと」を証明するために、その署名を後で利用できる場合、メッセージは、否認防止のために使われます。				
	これらのプロトコルは、暗号化されていないチャネル上を送られるとき、その値を隠すようにするために、公開の大きな乱数と組み合わせています。				
	「公開の値を使う代わりに、そのメッセージは、ハッシュ化される前に、共有された秘密と組み合わされること」				
	複数の鍵における用途で、データを乱雑な文字列となるように撹拌するために、ハッシュアルゴリズムを繰り返し使います。				
	「共有された秘密（shared secret）」によるメッセージ認証において、「その秘密は、両者に知られている」という事実も、あらゆる知覚しうる攻撃を防ぐと信じられています。				
	換言すれば、人間が署名されたメッセージを認可として使っている場合、否認防止プロトコルにおいて、ハッシュ衝突攻撃を防ぐために、その署名者は、自身が署名した元のメッセージのコピーを保持する必要があります。				
	「その受け入れる主体が、『その証明書が正しく、その証明書によって識別される人もしくはシステムを識別すること』を信頼できること」				
	「ひとつの身元を使っている人は、ひとつの公開鍵によって、ひとつのデジタル証明書を入手できるが、『それは、異なる公開鍵による（ただし、同一の身元と有効期限等をもつ）』ふりができること」				
	「衝突攻撃は、証明書上の（公開鍵のように）人間が読める情報が無い部分のみに影響を与えること」				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	PKIX 証明書を発行する TTP が上記の攻撃を避けることを望む場合、彼らは、その攻撃によって得られる、いかなる優位性をも根絶するために、その証明書の他の署名された部分を十分に乱雑にすることによって、攻撃を防ぐことができます。示唆されたアイディアは、下記の事項を含みます。: ＊証明書のシリアル番号の部分を攻撃者が予測できないようにする ＊任意に選択されたコンポーネントを身元に追加する ＊有効期限の文字を前後に歪めることによって、攻撃者が予測不能にする				
	「すべてのインターネットプロトコルが、異なるハッシュアルゴリズムを、より長いハッシュ値と共に使えるようにする作業が行われる必要があること」				
	本書の著者陣は、開発中の新しいプロトコルについて、同じように感じています。: Bruce は、「それらは、最初から SHA-256 を使い始める必要がある」と考えており、Paul は、「それらは、その新しいプロトコルが衝突攻撃の影響を受けないかぎり、SHA-1 を使う必要がある」と考えています。あらゆる新しいプロトコルは、そのハッシュアルゴリズムのみならず、そのすべての暗号アルゴリズムを変更することが可能でなければなりません。				