SKY Perfect JSAT Corporation

News Release

2011 年 8 月 9 日

スカパーJSAT 株式会社

衛星時刻配信サービス「TimeShower」において、時刻配信業務認定事業者として国内初となるセキュリティ強度の高い暗号アルゴリズム SHA-2(*1)対応を完了

スカパーJSAT 株式会社（本社：東京都港区、代表取締役　執行役員社長：高田真治、以下、スカパーJSAT）は、財団法人日本データ通信協会の認定による時刻配信業務認定事業者（以下、TA 局）として、自らが運用する通信衛星を利用した画期的な時刻配信サービス「TimeShower」を 2009 年 10 月に開始し、タイムスタンプ(*2)サービスに必要不可欠な正確な時刻情報をタイムスタンプ事業者（以下、TSA 局）向けに提供致しております。

今般、時刻配信業務認定の更新にあたり、スカパーJSAT が独自に開発した衛星時刻配信・監査システムの暗号アルゴリズムを従来より格段にセキュリティ強度の高い SHA-2 に更新し、かつ、GMO グローバルサイン株式会社の SHA-2 対応の時刻配信局証明書（GlobalsignTA証明書）(*3)を採用し、本年 7 月より、国内で初めて、SHA-2 対応が可能な時刻配信サービスを提供することとなりましたのでお知らせします。

これにより、TSA 局による SHA-2 対応のタイムスタンプサービス提供の環境が整うことになりました。今後、電子的な書面のやりとりが増大してゆく中で、セキュリティを強化したタイムスタンプは、電子契約、電子カルテ、官公庁向け電子申請等に益々活用され、その重要度が高まってゆくものと期待されています。

スカパーJSATは TimeShower サービスを通じて、電子文書の改ざん等を防ぎ、原本性確保の確実な実行に資するべく今後もサービス強化に努めてまいります。

*1: SHA とは、Secure Hash Algorithm の略で、通例「シャー」と読まれ、米国家安全保障局（NSA)が設計し、米国立標準技術研究所(NIST)が規格化した米国政府標準ハッシュ関数（与えられたデータから固定ビット長の値を生成する関数）のこと。
SHA-1 は現在のところ幅広く利用されている暗号アルゴリズムで、与えられたデータから 160 ビットの値を生成する。
SHA-2 は、SHA-224、SHA-256、SHA-384、SHA-512 の総称で、例えば、SHA-256 の場合、与えられたデータから 256 ビットの値を生成する。SHA-1 よりも強度が強く、次世代の暗号アルゴリズムとされる。

*2:タイムスタンプとは、信頼の置ける時刻と文書などのデジタル情報に対し、変更、改ざんがあったかどうかを検知できる情報もしくはそれを指し示す情報を付与し、それ以降、内容や時刻に変更・改ざんがあったかどうかを証明する技術。国際標準規格（ISO/IEC18014、RFC3161）、JIS 規格（JISX5063-1）に準拠しており、国内においては、財団法人日本データ通信協会が認定した TSA(Time Stamp Authority)局により提供されている。TA(Time Authority)局は、TSA 局に対して日本標準時を適正に提供する機関（時刻配信サービスの提供者）として、TSA局と同様に財団法人日本データ通信協会からの認定を受けている。

*3:時刻配信局証明書とは、TA 局を運営する企業の実在性を認証し、TA 局が運用する時刻配信サーバに対して、認証局が発行するサーバ証明書。TA 局の業務認定において必須とされている。

（参考）
衛星時刻配信サービス「TimeShower」の詳細については、下記 URL をご参照ください。
http://www.sptvjsat.com/service/satellite/timeshower/timeshower_whats.html

【経緯】
スカパーJSATが時刻配信サービス「TimeShower」を提供するにあたり、財団法人 日本データ通信協会 タイムビジネス認定センターの認定(TA0005)を受けております。同センターは、2010年 7 月 8 日に、「デジタル署名を利用するTSA 及びTA 業務に対する暗号アルゴリズム移行への検討開始のお知らせ」(*4)を公表し、2012年3月末までを目標として、TSA 局及び TA 局において利用する暗号アルゴリズムをより強度の強いものへ移行させる指針を示しました。具体的には、TSA局及びTA局ではこれまで、SHA-1の技術を用いておりましたが、今後、目標とされる期限までにSHA-2に対応することを求められることとなります。スカパーJSATでは、この状況を鑑み、お客様に対し、より安全なサービスを継続してご提供するために、いち早くSHA-2に切り替えることを検討しておりました。
*4: http://www.dekyo.or.jp/tb/data/100708.pdf

【技術的背景】
「各府省の情報システム調達における暗号の利用方針」（2002年2月28日）(*5)において、各府省の情報システム調達に使用すべき暗号リスト（総務省／経済産業省「電子政府推奨暗号リスト」）が公表され、SHA-1、SHA-256、SHA-384、SHA-512がそれぞれ推奨されているものの、256ビット以上のハッシュ関数を選択することが望ましいとされている。
また、「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」（2008年4月22日情報セキュリティ政策会議決定）(*6)においては、政府機関の情報システムにおける暗号アルゴリズムについて、現在、SHA-1を使用している場合には、その安全性の低下が指摘されてきている状況を踏まえて、2013年度までにSHA-256にも対応するよう決定されている。
*5: http://www.cryptrec.go.jp/images/cryptrec_02.pdf
*6: http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf