2012 年 12 月
セコムトラストシステムズ株式会社

暗号アルゴリズムの 2010 年問題と弊社の対応について

■　暗号アルゴリズムの2010年問題とは

電子認証や署名には暗号技術が使われていますが、コンピュータの性能や解読技術の向上により、暗号技術の安全性は徐々に低下していきます。暗号の安全性だけを考えると、より安全な暗号技術への移行が望ましいと考えられます。

【米国国立標準技術研究所(NIST)の見解】

現在利用されている米国政府使用の暗号技術を、2010年末までにより安全なアルゴリズムへ移行させる方針を打ち出しています。

【日本の内閣官房情報セキュリティセンター(NISC)や総務省の見解】

電子署名法関係における対応として、より安全性の高い暗号化技術を採用し、「2014年度早期までにより安全性の高い暗号技術による電子署名に係る特定認証業務を開始する」との対応を予定しています。

※安全性の低下が懸念されている具体的な暗号技術

○公開鍵：1,024bit

○ハッシュアルゴリズム：SHA-1

しかしながら、デバイス（特に携帯電話など）においては新たに暗号技術を実装すること自体が難しく、またデバイス以外のシステムにつきましても、新しい暗号技術への対応につき、改修にかかるコストが発生し企業の負担になります。また、急激な暗号技術の切り替えは情報システムの安全性・可用性を損なう危険性があります。

NIST、NISCは上記の見解ですが、あくまでもガイドラインであり、市場環境も鑑みた移行が必要であると考えられています。これら暗号技術の移行に伴う問題が「暗号アルゴリズムの2010年問題」と呼ばれています。

■ 2010年問題への弊社の対応

公開鍵：1,024bit について

暗号技術の移行につき、市場環境も鑑みた対応を行って参りましたが、マイクロソフト等のブラウザベンダーによる将来的な暗号強度の信頼性低下に備えた方針に則り、 1,024bit の鍵長を採用した証明書の最長有効期間は、2013年12月31日迄となります。

○セコムパスポート forWeb SR2.0：

2010年7月1日より鍵長2,048bitのみ発行しております。

2010年6月以前に発行された鍵長1,024bitの5年証明書については、無償にて鍵長2,048bit証明書への再発行を受付ておりますので、お早めの手続きをお願い致します。

○セコムパスポート forWeb EV：

EVガイドラインの規定により、鍵長2,048bitのみ発行しております。

○セコムパスポート forWeb：

携帯電話の旧機種への対応を考慮し、鍵長1,024bitでのCSR受付および発行を継続して参りましたが、マイクロソフト等のブラウザベンダーによる将来的な暗号強度の信頼性低下に備えた方針に則り、セコムパスポートforWebの2年証明書は2011年11月30日、1年証明書は2012年11月30日をもちまして申込み受付を終了いたしました。

詳細につき、下図を参照下さい。

	セコムパスポート forWeb EV	セコムパスポート forWeb SR2.0	セコムパスポート forWeb
ルート証明書 公開鍵鍵長	2,048bit	2,048bit	1,024bit
ルート証明書 ハッシュ関数	SHA-1	SHA-1	MD5
中間証明書 公開鍵鍵長	2,048bit	2,048bit	1,024bit
中間証明書 ハッシュ関数	SHA-1	SHA-1	SHA-1
サーバー証明書 公開鍵鍵長	2,048bit のみ	2,048bit まで対応 ※2,048bit 推奨	1,024bit まで対応 ※1,024bit 推奨
サーバー証明書 ハッシュ関数	SHA-1	SHA-1	SHA-1

ハッシュアルゴリズム： SHA-2 について

NISTでは、より安全性の高い暗号技術への移行を推奨しています。移行対象の暗号技術のうち、SSLサーバー証明書の署名で用いられるハッシュ関数アルゴリズムについては、現在のデファクトスタンダード「SHA-1」から、今後はより強固な「SHA-2」ファミリーへの移行対応が行われることとなります。

それに伴い、弊社では次世代暗号技術のスタンダードとなる「SHA-2」を採用したルート認証局を構築(注1)いたしました。

セコム「SHA-2」対応の次世代ルート証明書名 ： Security Communication RootCA2

※ハッシュ関数アルゴリズム SHA256、 公開鍵 2,048bit

ドコモの2009年度冬春モデルを皮切りに、PCや携帯/スマートフォンブラウザをはじめ、各種組込み機器に対して、次世代ルート証明書を搭載しております。

PC環境において、次世代ルート証明書はWindows XP SP2以前には対応しておりません。また、携帯電話においても現時点では、対応機種一覧の中の多くの機種が対応しておりません。
従いまして、現行のサービスにつきましては従来通り「Security Communication RootCA1」より発行いたします。

次世代ルート証明書は、将来を見越した対応の一環であり、現サービスに影響は御座いません。
現時点では、次世代ルート証明書を採用することは市場環境により出来ませんが、ブラウザ等各アプリケーション、「SHA-2」対応の携帯電話等デバイスに対して、次世代ルート証明書の搭載アプローチを継続的に実施し、これらの環境にて普及した段階で、次世代ルート証明書を採用した新たなサービスを提供する予定です。
新たなサービス提供については、今後の各アプリケーションの対応状況も鑑み、別途ご案内いたします。

(注1) SSLサーバー証明書の信頼の拠り所となる認証局。ルート認証局の証明書は、ブラウザ等に搭載され、Webサイトとの通信が安全かどうかを確認するときに使われます。

以上