暗号アルゴリズムの 2010 年問題について

■暗号アルゴリズムの 2010 年問題とは

【背景】
電子認証や署名には、暗号技術が使われています。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。
具体的な暗号技術と致しまして、下記になります。

〇公開鍵：1,024 ビット RSA
〇ハッシュアルゴリズム：SHA-1

【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。

【暗号技術の移行にあたって】
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。しかしながら、特に携帯電話等、デバイス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。従いまして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ます。

これら暗号技術の移行に伴う問題につき、「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：1,024 ビット RSA について)

暗号技術の移行につき、市場環境も鑑みた移行が必要であるとの見解から、下記の通り証明書発行を致します。

○ セコムパスポート forWeb SR2.0：
2010 年 7 月 1 日より 2,048 ビット RSA のみの発行です。
1,024 ビット RSA の CSR では、申請画面からお申し込みが出来なくなります。

○ セコムパスポート forWeb EV：
EV ガイドラインの規定により、従来通り 2,048 ビット RSA のみの発行です。

○ 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、1,024 ビット RSA 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、 1,024 ビット RSA の鍵長を採用した本証明書の最長有効期間は、2013 年 12 月 31 日迄となる見込みです。
それに伴い、セコムパスポートforWebの 2 年証明書は、2011 年 11 月 30 日をもちまして申し込み受付を終了いたします。
セコムパスポートforWebの 1 年証明書は従来通り、 2013 年 12 月 31 日までの証明書有効期間内において 1,024 ビット RSAでのCSR受付および発行を継続する予定です。

詳細につきましては下図を参照下さい。

	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	2,048bitRSA	2,048bit	1,024bitRSA
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	2,048bitRSA	2,048bitRSA	1,024bitRSA
中間証明書 ハッシュ関数	SHA-1	SHA-1	SHA-1
サーバ証明書 公開鍵鍵長	2,048bitRSA のみ	2,048bitRSA のみ	1,024bitRSA まで対応
サーバ証明書 ハッシュ関数	SHA-1	SHA-1	SHA-1

2,048 ビット RSA の公開鍵に対応していないアプリケーションとして、具体的に下記があります。

・古い携帯電話

現況、市場において 2,048 ビット RSA に対応していない携帯電話が占める割合は極めて少ないかと存じますが、これら 2,048 ビット RSA 非対応携帯電話からのアクセスを重要視されない場合、セコムパスポート forWeb SR2.0、若しくは EV にて 2,048 ビット RSA での証明書発行を推奨致します。セコムパスポート forWeb SR2.0 及び EV につき、ルート証明書、中間証明書ともに 2,048 ビット RSA を使用しておりますので、サーバ証明書を 2,048 ビット RSA にて発行頂ければ、万一 1,024 ビット RSA が危殆化しても、問題なくご利用頂けます。※現況 1,024 ビット RSA につき、危殆化しておらず、危殆化する時期につきましても不明です。

■2010 年問題への弊社の対応(ハッシュアルゴリズム：SHA-1 について)

次世代暗号技術のスタンダードとなる「SHA-2」ハッシュ関数アルゴリズムを採用したルート認証局を構築しました。
ルート証明書名：「Security Communication RootCA2」

SHA-2 ハッシュ関数につきまして、PC 環境においては Windows XP SP2 以前は対応しておりません。また、携帯電話につきましては 2009 年冬春モデルの一部より対応が開始した状況です。従いまして、現行のサービスにつきまして、従来通り「Security Communication RootCA1」より発行致します。セコム「SHA-2」対応　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、セコム「SHA-2」対応 次世代ルート証明書を採用した証明書サービスを提供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、「SHA256」ハッシュ関数アルゴリズムを採用したルート証明書「Security Communication RootCA2」の搭載アプローチを実施し、これらの環境にて普及した段階で、新たなルート認証局を採用したサービスを提供する予定です。

セコム「SHA-2」対応　次世代ルート証明書につきまして、下記をご参照下さい。
参照：セコム　「SHA-2」対応 次世代ルート証明書