1999.8.31

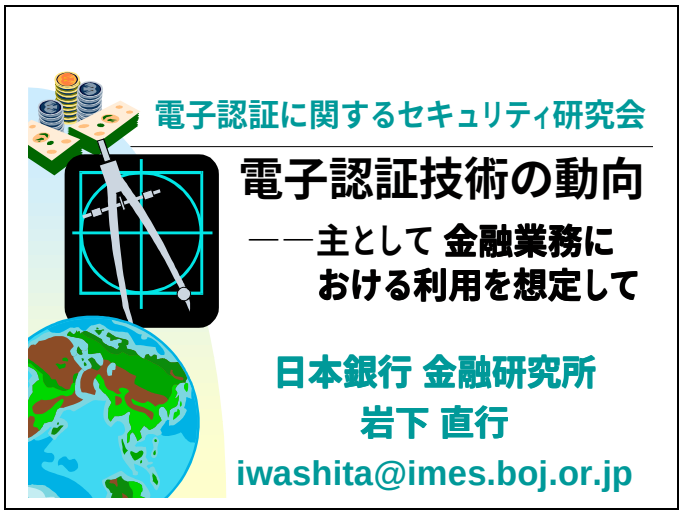
通産省 電子認証に関するセキュリティ研究会

電子認証技術の動向

――主として 金融業務における利用を想定して

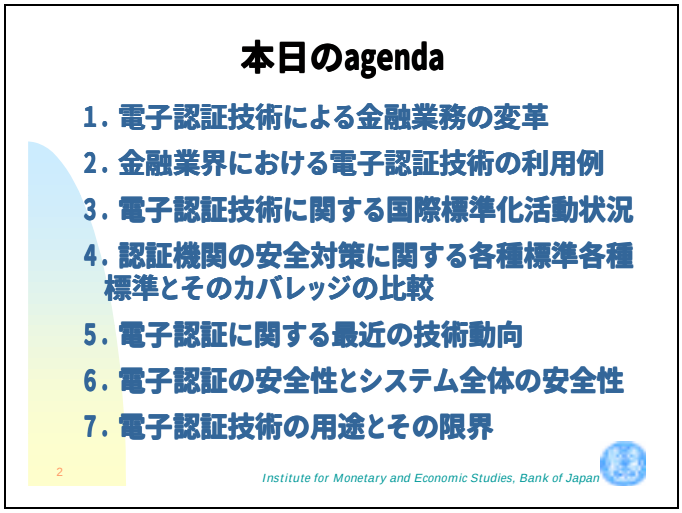
日本銀行 金融研究所 岩下 直行

■タイトル画面（画面１）



日本銀行 金融研究所では、情報セキュリティ技術の金融業務への適用に関する研究を行っています。また、ISO/TC68という、金融分野で利用される情報技術の国際標準化委員会の日本における事務局も務めています。こうした立場から、電子認証技術についても、主として金融業務における利用を想定して調査・研究していますし、金融機関が認証業務を行う場合のセキュリティ対策に関する国際標準の策定作業に参加しています。本会合では、時間も限られていることから、多少論点を絞らせて頂き、電子認証技術の「ユーザー」の視点から、電子認証におけるセキュリティ確保のための様々な技術をどのように利用していくべきか、というテーマでお話をさせて頂きたいと思います。

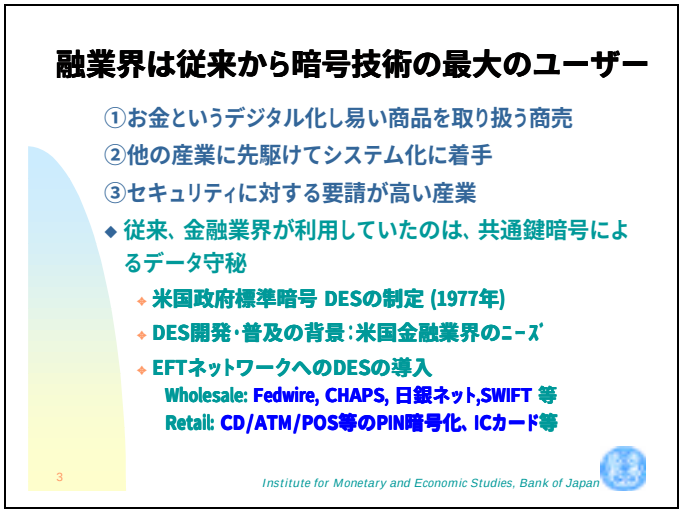
■本日のアジェンダ（画面２）



（アジェンダの説明）

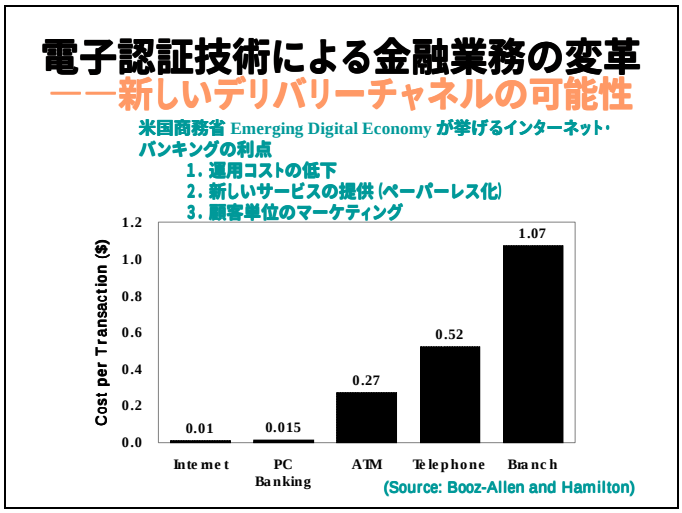
（配布資料の説明）

■金融業界は従来から暗号技術の最大のユーザー　（画面３）



さて、金融業界は、①お金というデジタル化し易い商品を取り扱う商売であり、また、②他の産業に先駆けてシステム化を進めてきたこと、そして何より、③セキュリティに対する要請が高い産業であることから、従来から暗号技術の大手のユーザーでした。しかし、従来金融業界が利用していたのは、基本的には共通鍵暗号によるデータ守秘でした。電子認証技術、すなわち公開鍵方式によるデジタル署名を用いて通信メッセージの真正性等を確認する技術は、その原理が考案されてから既に 20 年以上経っており、理論的には良く知られていたものの、金融業界において本格的に実務に利用されるようになったのは比較的最近のことです。電子認証技術はオープンな環境で不特定多数の利用者による情報通信に利用される際に、その威力を発揮します。しかし、金融業務においては、つい最近までは、金融機関同士とか、大手企業といった特定のユーザーの間で、クローズドなネットワークを構築して取引を行うことが多く、わざわざ電子認証技術を導入しなくても、ネットワークの安全性を確保することができたのです。

■電子認証技術による金融業務の変革―新しいデリバリーチャネルの可能性（画面４）



しかし、インターネットの普及が全てを変えました。金融機関は、その顧客との間のデリバリーチャネルとして、インターネットのようなオープンなネットワークを利用することにより、大幅に取引コストを削減できると考えられるようになったのです。例えば、あるコンサルティング会社の調査によれば、欧米の金融機関の多くは、今

後 10 年間において最も重要な顧客とのインターフェイスとしてインターネットを挙げています(Booz-Allen and Hamilton)。現在のように、各地に支店網を置いて顧客を開拓するのに比べ、コストが２桁も安いと試算されているからです。わが国の銀行や証券会社も、相次いでインターネット・バンキング、インターネット・トレーディングに乗り出しています。このように、金融業界は、電子認証技術の発達により、特に大きなインパクトを受けている業界と言えるでしょう。

■金融業界における電子認証技術の利用例（画面５）

金融業界における電子認証技術を利用した主なプロジェクトを整理すると、この表のようになります。

この表では、金融業務における電子認証技術の利用目的を、次のように６つに分類しています。

金融業界における電子認証技術の利用例

金融機関・団体名	利用目的	PKI・電子認証を採用するﾌﾟﾛｼﾞｪｸﾄ	利用ﾌﾟﾛﾄｺﾙ	認証ﾍﾞﾝﾀﾞｰ等	備考
住友銀行	①	個人向ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞ	SSL (128bit)	日本ﾍﾞﾘｻｲﾝ社	―
三和銀行	①	個人向ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞ	SECE	日本認証ｻｰﾋﾞｽ社	―
野村證券	①	個人向ｲﾝﾀｰﾈｯﾄﾄﾚｰﾄﾞ	SSL (128bit)	ｻｲﾊﾞｰﾄﾗｽﾄ社	―
日本興業銀行	②	企業向ｸﾞﾛｰﾊﾞﾙｷｬｯｼｭﾏﾈｼﾞﾒﾝﾄｻｰﾋﾞｽ	SSL	ｻｲﾊﾞｰﾄﾗｽﾄ社	暗号鍵や公開鍵証明書はPCカードで保管
JCB	③	個人向ｸﾚｼﾞｯﾄｶｰﾄﾞ決済	SET	―	自社でCA機能を運行
Wells Fargo	④	SureServer ｻｰﾋﾞｽ	―	GTE Cybertrust	一般的な認証ｻｰﾋﾞｽの提供
大和證券	⑤	社内国際ﾈｯﾄﾜｰｸ	SSL (128bit)	日本ﾍﾞﾘｻｲﾝ社	ｲﾝﾀｰﾈｯﾄを利用して国際基幹網を構築
ABAecom	⑥	銀行の Web ﾍﾟｰｼﾞ・ｻｰﾊﾞｰの真正性を確認	―	Digital Signature Trust (DST)	米国銀行のﾙｰﾄCAとなることを展望
GTA	⑥	国際的な CA の相互運用性の確保に向けた認証ｻｰﾋﾞｽの提供	―	―	国際的な金融業務で電子認証を行う銀行のﾙｰﾄ CAとなることを展望
SWIFT	⑥	SWIFT での金融取引に電子認証を提供	―	―	―

①：個人向けインターネット・バンキング、インターネット・トレーディング
②：企業向けインターネット・バンキング
③：個人向けインターネット・ショッピングの決済（クレジットカード、口座振替）
④：電子商取引におけるオンライン店舗サーバーの認証
⑤：金融機関社内ネットワークでの相手認証及びデータの暗号化
⑥：①～⑤における CA に対する認証（ルート CA 等）

①個人向けのインターネットバンキング（預金の振替、残高照会等）やインターネットトレーディング（株式、債券等の売買等）

②企業向けのインターネットバンキング（従来から存在するエレクトロニックバンキングのインターネット対応）

③個人向けのインターネットショッピングの決済（クレジットカード、銀行口座引き落とし等）

④一般的な電子商取引におけるオンライン店舗サーバーの認証

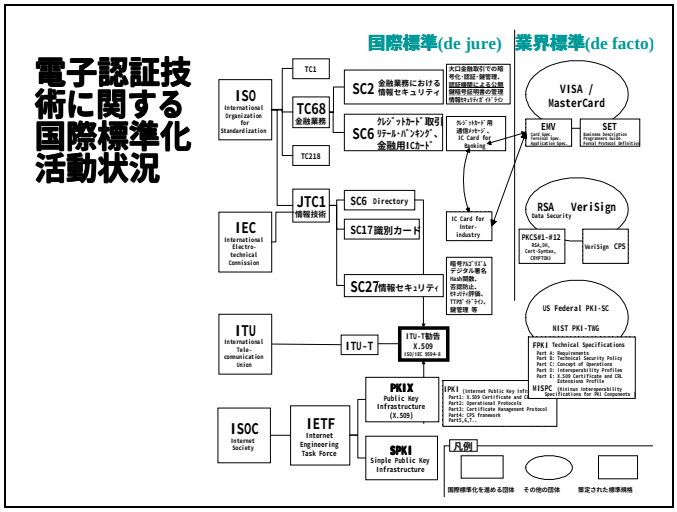
⑤金融機関社内ネットワーク（イントラネット及びエクストラネット）での相手認証及びデータの暗号化

⑥①～⑤における CA に対する認証（ルート CA 等）

こうした様々な金融関連のプロジェクトにおいて、現実に電子認証技術が利用されている訳ですが、現時点では電子署名等の法的有効性や認証機関のセキュリティ要件について定まったルールがある訳ではないので、各社が自ら安全性を評価して、適当と判断した技術を採用しているようです。そうした評価に際しては、現在策定されている様々な技術標準が参考にされています。

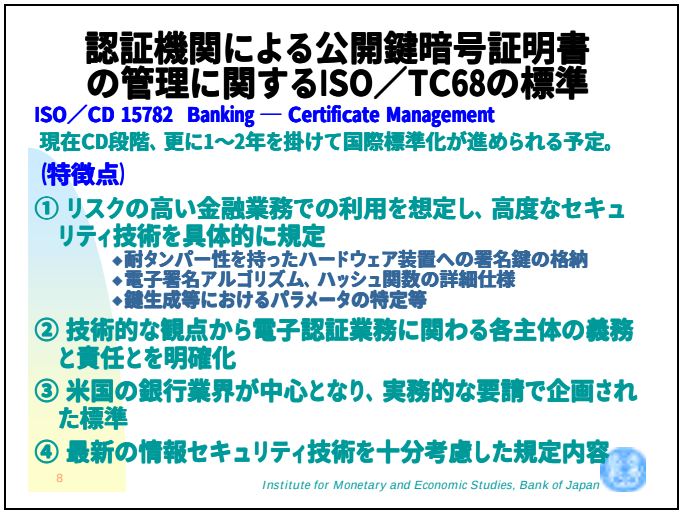
■電子認証技術に関する国際標準化活動状況（画面６）

まず、最初に、現在海外や国内で検討されている様々な技術標準において、特に認証機関のセキュリティを向上させるためにどのような技術の利用が推奨されているか、という点についてご紹介したいと思います。現在、様々な標準が策定されています。



■ISO／TC68 における情報セキュリティ技術の国際標準化（画面７）

■認証機関による公開鍵暗号証明書の管理に関する ISO／TC68 の標準（画面８）

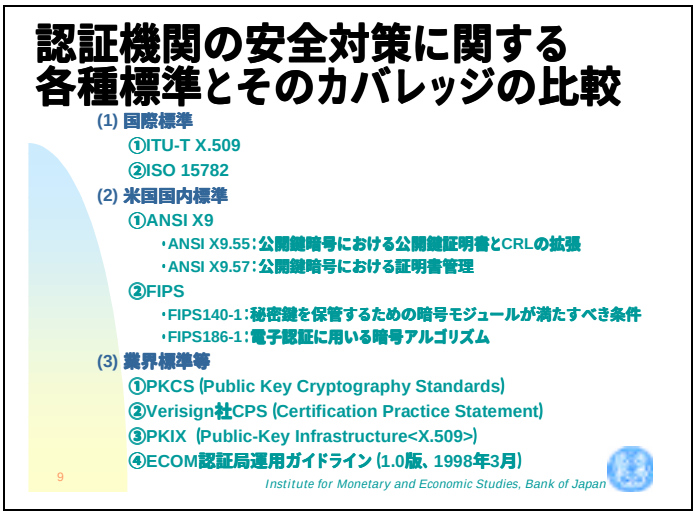


■認証機関の安全対策に関する各種標準各種標準とそのカバレッジの比較（画面９）

(1) 国際標準

①ITU-T X.509：認証書および CRL のフォーマット。現在改訂作業が進んでいる。（AA 関連ほか）

②ISO 15782：公開鍵証明書の管理全般について取り纏められており、公開鍵証明書の管理のために CA や RA が果たすべき機能、公開鍵証明書のライフサイクル、公開鍵証明書の詳細な設定内容等について説明されている。



(2) **米国国内標準**

①ANSI X9

・ANSI X9.30：非可逆型 公開鍵暗号アルゴリズム（DSA、SHA-1）
・ANSI X9.31：可逆型公開鍵暗号を用いたデジタル署名（RSA）
・ANSI X9.55：公開鍵暗号における公開鍵証明書と CRL の拡張
・ANSI X9.57：公開鍵暗号における証明書管理
・ANSI X9.62：楕円曲線暗号

②FIPS

・FIPS140-1：秘密鍵を保管するための暗号モジュールが満たすべき条件
・FIPS186-1：電子認証に用いる暗号アルゴリズム

(3) **業界標準等**

①PKCS（Public Key Cryptography Standards）：RSADSI 社の定める標準。

②Verisign 社 CPS（Certification Practice Statement、バージョン 1.2）：電子認証サービスを提供しているベリサイン社が 1997 年 5 月に作成したものであり、ベリサイン社及びベリサイン社以外の主体が、「ベリサインパブリック証明サービス」における CA として機能するための行動指針が纏められている。本資料は、1 企業が作成した CPS であるが、CA の運用上の注意点として広く参照されている。

③PKIX （Public-Key Infrastructure<X.509>）：PKIX は、IETF の作業部会。なお、PKI Roadmap は、1999 年 3 月に作成したドラフトであり、PKIX の各ドキュメントの内容を実行に移す際の留意点が記述されている、CA にとってのガイドライン的なドキュメントである。

④ECOM 認証局運用ガイドライン（1.0 版）：電子商取引実証推進協議会（ECOM）により、CA を運営するためのガイドラインとして 1998 年 3 月に作成されたものである。その内容は、鍵や公開鍵証明書の管理だけではなく、組織管理やシステム・設備の管理等多岐にわたっている。

■主な標準に記述された CA の業務要件（画面１０）

そこにおける様々な技術のカバレッジはこの表のとおりです。

主な標準に記述された CA の業務要件

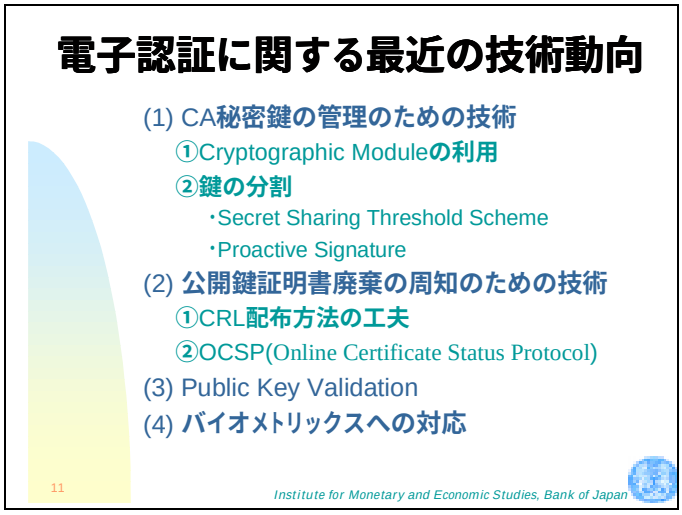
		国際標準		米国国内標準		業界標準等			
		ISO 15782	ITU-T X.509	ANSI X9	FIPS	PKCS	Verisign CPS	PKIX	ECOM
各主体(CA 等)の行動指針		○		○57					○
公開鍵証明書管理	鍵生成	○	△				○	△	△
	公開鍵証明書発行申請	○					○		△
	登録手続	○					○	△	
	公開鍵証明書の発行	○	△	○57			○	△	
	CA 公開鍵配布	○		○57			○		
	公開鍵証明書の配布	○					○		
	公開鍵証明書の使用	○					○		
	公開鍵証明書の廃棄・中断	○	○	○57			○	○	○
	公開鍵証明書の更新	○					○	△	○
データ構造	公開鍵証明書申請データ	△		○57		○#10			
	公開鍵証明書	△	○	○57				○	△
	公開鍵証明書廃棄リスト	△	○	○57				○	△
	公開鍵証明書拡張フィールド	○	○	○55		○#6	△	○	△
	公開鍵証明書廃棄リスト拡張ﾌｨｰﾙﾄﾞ	○	○	○55				○	△
	属性証明書	○	○	○57				○	
属性証明		○							
監査		○							○
アルゴリズム	DSA			○30	○186				
	RSA			○31	△186	○#1			
組織・人事管理									△
情報開示									△
システム・設備要件									△
秘密鍵保管用暗号ﾓｼﾞｭｰﾙのｾｷｭﾘﾃｨ要件					○140				
PKI の構成(CA 間の相互関係)		○	○	○57			○		△
CPS の重要性								○	

○：記述されている。　△：簡単に記述されている。

■電子認証に関する最近の技術動向（画面１１）

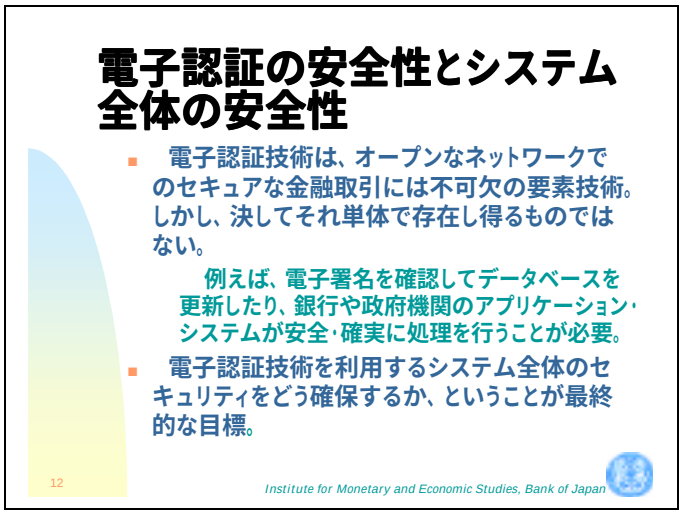
また、より進んだ技術として、次のようなものが考えられています。

(1) CA 秘密鍵の管理のための技術
　①Cryptographic Module の利用
　②鍵の分割
　　・Secret Sharing Threshold Scheme
　　・Proactive Signature
(2) 公開鍵証明書廃棄の周知のための技術
　①CRL 配布方法の工夫
　②OCSP(Online Certificate Status Protocol)
(3) Public Key Validation
(4) バイオメトリックスへの対応



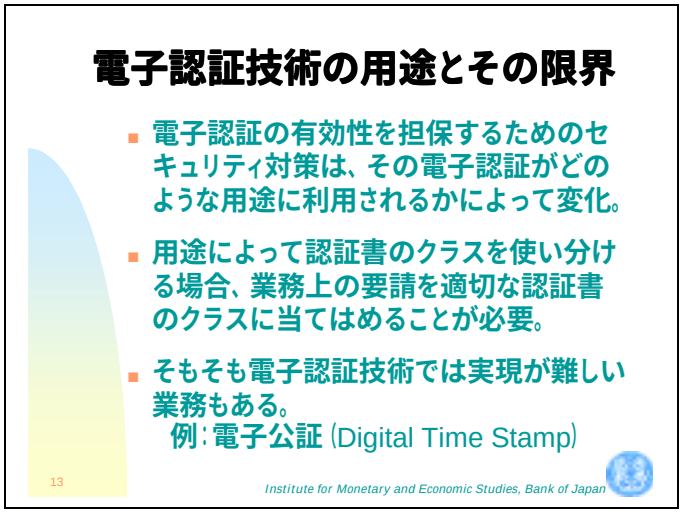
■電子認証の安全性とシステム全体の安全性（画面１２）

ここでは、電子認証技術は、オープンなネットワークでのセキュアな金融取引には不可欠の要素技術ですが、決してそれ単体で存在するものではない、ということを述べておきます。例えば、インターネット・バンキングであれ、電子政府構想などにおける電子的



な行政への書類申請事務であれ、認証機関と電子署名が重要な機能を果たすことは事実ですが、それだけでは事務は完結しません。例えば、電子署名を確認してデータベースを更新したり、銀行や行政機関のアプリケーション・システムが安全・確実に処理を行うことが要請されるのです。その意味では、電子認証を支えるCAやEEの秘密鍵の管理が重要なことは言うまでもないのですが、電子認証技術を利用するシステム全体のセキュリティをどう確保するか、ということが最終的な目標となることは、常に意識しておく必要があります。言いかえるならば、どんなに優れた CA を利用しようと、各業務のプロバイダーにおけるセキュリティがお粗末では、意味がないということです。このことは、CA に対して一定の基準の充足を求めようとするときに、考慮すべき点と思われますので、あえて強調しておきます。例えば、インターネット・バンキング全体のセキュリティや電子的な行政手続きのセキュリティは、別途確保する方策が必要ということです。

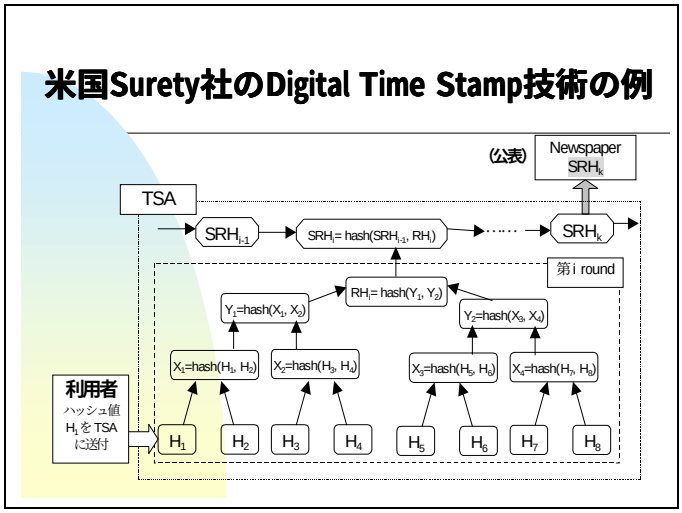
■電子認証技術の用途とその限界（画面１３）



また、同じような視点ですが、「電子認証の有効性を担保するためのセキュリティ対策は、その電子認証がどのような用途に利用されるかによって変化する」ということも重要と思われます。現在でも、用途によって認証書のクラスを使い分ける、といった運用が行われていますが、これはいわば CA の側からのアプローチであって、業務上の要請を適切な認証書のクラスに当てはめることが必要になります。また、そもそもこうしたカテゴリーではカバーしきれない業務もあります。

ひとつの典型的な例は、電子公証と呼ばれる分野でしょう。ある文書がある時点で存在したことを何十年後までも証明したい、というニーズに対して、現在の電子認証技術は解を提供することができません。基本的に、CA とデジタル署名を利用する認証体系は、「何十年」といった長期の要請には応えられないのです。これは、デジタル署名がその実用性や将来にわたっての安全性の担保という面からは、不確実性を抱えており、限界があるのです。

■米国 Surety 社の Digital Time Stamp 技術の例（画面１４）



この問題を解決するために、例えば米国の Surety 社が提供する Digital Time Stamp 技術があります。このスキームでは、秘密鍵の漏洩やデジタル署名アルゴリズムへの攻撃といった将来のリスクを回避するため、ハッシュ関数のみで階層構造を作り、最上位のハッシュ値を公開することにより、証拠性を担保する仕組みを採用しています。このような機能は、現在の紙ベースの書類が果たしているものですが、それをデシタル署名を利用した電子認証技術で実現させることは難しいということを意識すべきでしょう。

電子認証の法的効果をどのように規定するかを検討する際には、例えば紙の技術によって実現している効果と比べて、このような限界が存在することを考慮して、検討していくことも大切なように思われます。

■質疑応答（画面１５）

以上で発表を終了します。ご静聴ありがとうございました。

以　上