デジタル署名付文書の長期的安全性に関する考察

佐々木良一＊　東京電機大学工学部　吉浦裕　電気通信大学
洲崎誠一　宮崎邦彦　日立製作所システム開発研究所
＊　郵便番号101-8457 東京都千代田区神田錦町2－2　sasaki@im.dendai.ac.jp

あらまし：電子商取引や電子政府の進展に伴い、デジタル署名の利用範囲が拡大してきている。しかし、デジタル署名を付与した電子文書を長期的に利用･保管する場合の安全性については、ほとんど検討がなされてこなかった。そこで、長期利用上の問題を、デジタル署名のベースとなる公開鍵暗号の危殆化の影響を中心に検討を行い、公開鍵暗号の危殆化のパターンや、代替暗号があるかどうかなどのパターンごとに必要となる対策課題の分析を行った。次にそれらの課題に対する対策案を示すとともにそれらを評価したので、その結果を報告する。

キーワード：デジタル署名、署名検証、秘密鍵漏洩、公開鍵暗号危殆化、署名付文書長期保管

Consideration on Long Term Security of Digital Document with Digital Signature

Ryoichi Sasaki*, School of Engineering, Tokyo Denki University
Hiroshi Yoshiura Denki Tsushin University
Seiichi Susaki,　Kunihiko Miyazaki Hitachi Ltd.
* 2-2 Kanda Nishiki-Cho Chiyoda-Ku Tokyo, 101-8457 Japan, sasaki@im.dendai.ac.jp

Abstract: The usage of a digital signature is being increased with progress of electronic commerce or the electronic government. However, the security in the case of keeping the digital document with the digital signature for the long time has been hardly examined.　First of all, we show that biggest problem to use digital document with digital signature for long time is the public key cipher weakened for these period. Next, required countermeasures are analyzed for every patterns of a public key cipher weakness. Lastly, these countermeasures are evaluated, and the result is reported.

Keywords: Digital Signature, Signature Verification, Secret Key Leakage, Weakened　Public Key Cipher, Long Term Storage of Signed Document

1. はじめに

電子商取引や電子政府の進展に伴い、デジタル署名の利用範囲が拡大してきている。しかし、デジタル署名の長期的安全性についてはほとんど研究されておらず、最近になって、検討が部分的に始まったところである[1)－4)]。なかには、デジタル署名の安全性は公開鍵証明書の有効期間(1-2年)が終了した時点で必要なくなると考えおり、デジタル署名の長期的安全性の検討は必要ないという人までいる。

しかし、紙の世界で印鑑証明の有効期間中に対応する印鑑を用いて作成した取引文書(例えば土地の売買契約書)は、印鑑証明の有効期間が過ぎても有効でなければならないように、デジタル署名を施した電子文書は公開鍵証明書の有効期間が過ぎても有効でなければならない。そのためには、デジタル署名は、対象となる電子文書の有効期間にわたり、安全でなければならない。しかし、この電子文書の有効期間が長くなると、デジタル署名のベースとなる公開鍵暗号が危殆化(脆弱化)するなどの理由により、安全性が脅かされる可能性が増大する。

公開鍵暗号が危殆化することがわかったとしても、デジタル署名つき文書の安全性を何とか確保する必要がある。本報告では、公開鍵暗号の危殆化のパターンや、代替暗号があるかどうかなどのケースごとに分析を行い、必要となる対策課題を明確化する。次にそれらの課題に対する対策案についての評価結果を行う。

2. デジタル署名の長期利用と問題点

デジタル署名の利用形態としては次のようなものが考えられる。

(1) 一般ユーザでの署名

(a) エンティティ認証のための署名(SSLでのサーバ認証など)

(b) 短期利用文書への署名(電子申請書への署名)

(c) プログラムへの署名(JAVAアプレットへの署名)

(d) 長期利用文書への署名

(2) 認証局での利用(証明期間:1年程度)

(a) 公開鍵証明書への署名

(b) 下位認証局公開鍵証明書の公開鍵証明書への署名

(3) 公証局での署名

(a) 時刻データへの署名　　－＞証明期間が長期になり勝ち

(b) 証明依頼文書への署名　－＞証明期間が長期になり勝ち

このうち、その利用期間が長期(ここでは数年から数十年を想定)になるものとしては、(1)の(d)、(3)の(a)(b)が考えられるが、本論文では一般ユーザが使う署名である(1)の(d)を対象とする。長期に利用する署名付文書はまだあまり無いという意見もあるが、**図1**に示すように電子カルテや、電子アーカイブなどはすでに使われ始めている。

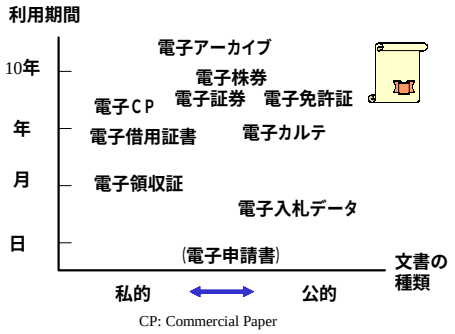

図1 長期利用署名つき電子文書の例[1]

一般ユーザがデジタル署名を長期にわたって用いる手順と問題点を、**図2**を用いて説明する。

(1) まず、一般ユーザは自分の公開鍵に対する証明書を認証局よりもらった後、借用書などの取引文書に対し署名を生成し、公開鍵証明書とともに取引相手に送る。

(2) 受け取った取引相手は、公開鍵証明書から署名生成者の公開鍵を取り出し、取引文書に対する署名が確かに本人のものであることを検証する。この過程で、相手の公開鍵が無効化されていないことを認証局に対し、ＣＲＬ(Certificate Revocation List)やＯＣＳＰ(Online Certificate Status Protocol)を用いて確認する。この確認は証明書の有効期間(通常1-2年)ならば比較的容易に実施できる。

(3) しかし、この期間をすぎると次のような2つの

問題が発生する。

(a) 証明書情報や失効情報がどのようなものであったかわからない。

(b) 時間がたつにつれて、公開鍵暗号の秘密鍵が漏洩し、署名つきの偽文書が偽造される可能性が増える。

(a) については、署名再検証技術が研究されており、最初の署名検証時に署名ポリシーや、CRL情報、タイムスタンプなどを収集し、それを署名付文書とともに安全に保管することにより、再検証時に備えようというものである[4]。本報告では、(b) の問題を対象とする。

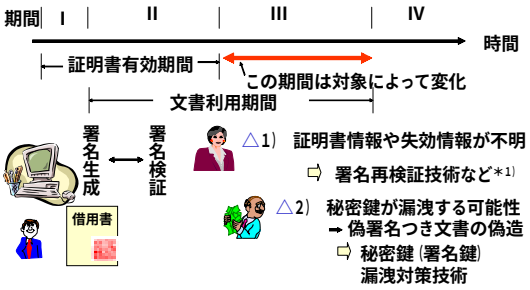

図2 長期利用上の問題点

公開鍵暗号の秘密鍵の漏洩の原因としては、図3に示すような5つのものが考えられる。**図3**において上に行くほど影響の範囲が狭く、下に行くほど広くなる。分類5の「利用者の不注意」による鍵の漏洩の影響範囲は、その人の利用したデジタル署名にとどまるが、分類1の「公開鍵暗号の危殆化」は、その暗号を使うすべてのデジタル署名に影響する。

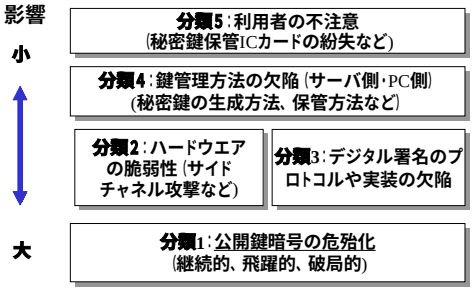

図3 秘密鍵の漏洩原因の分類

本報告では、鍵の漏洩の原因として従来あまり検討が行われてこなかったことや、影響が最も大きいという理由から分類1の「公開鍵暗号の危殆化」を対象とする。

3. 公開鍵暗号危殆化と対応課題

公開鍵暗号の危殆化のパターンとしては、**表1**に示すようなものが考えられる。危殆化が、継続的か、飛躍的か、破局的かによる分類と、代替暗号があるかないかによる分類で構成される6つのパターンである。

ここで、継続的危殆化というのは攻撃側の計算機能力の向上などによるもので、例えば、10年で100倍になるであろうなど、比較的予測がつきやすいものである。飛躍的危殆化というのは、新しい攻撃方法が発見され、秘密鍵が解読されるまでの時間が大幅に短縮される場合を言う。次に、破局的危殆化というのは、新しいタイプの計算機の出現や数学上の発見により、暗号の安全性を支える理論が破綻する場合である。

この典型的な例が量子コンピュータの出現であり、量子コンピュータが現れれば、暗号解読の困難性の根拠となっている大きな数の素因数分解や離散対数問題の求解が、多項式オーダで可能となるといわれており、簡単に秘密鍵が解読されてしまうことが予想される。もちろん、量子コンピュータの出現までには10年以上かかるであろうといわれており、すぐに問題になるわけではないが、現在作成したデジタル署名、および署名つきの文書が、量子コンピュータの出現時点で無効になってしまうので、今から対策を考えておく必要がある。

表1で代替暗号というのは標準的に使われている暗号に対し、それに取って代りうる暗号である。例えば、現在使われているのが通常のRSA暗号(鍵長1024ビット)だとすると、代替暗号としては、(1) 鍵長2048ビットなど鍵長を長くしたもの、(2) RSA－PSS(Probabilistic Signature Scheme)など類似の方式で安全性を強化したもの、(3) 楕円曲線暗号など安全性の根拠が素因数分解の困難性から楕円曲線上の離散対数問題求解の困難性へと少し変わるもの、(4) 計算量的安全性ではなく情報論的安全性に基づく暗号のようにその安全性の根拠が大幅に異なるもの

などいろいろなものが考えられる。

表1のそれぞれのパターンについて分析したが、パターン3（飛躍的危殆化で代替暗号ありの場合）と、パターン6（破局的危殆化で代替暗号なしの場合）について、分析した結果を報告する。

表1　公開鍵暗号危殆化のパターン

危殆化	原因	例	代替暗号	No
継続的	攻撃側の計算機能力の向上など	計算能力10年で100倍	あり	1
			なし	2
飛躍的	新しい攻撃方法の発見	楕円曲線法	あり	3
			なし	4
破局的	新しい計算機の出現や数学上の発見などにより暗号を支える理論が破綻	量子コンピュータの出現	あり	5
			なし	6

[8]

パターン3の場合は、以下のような対応が必要となる（**図4**参照）。

（1）総務省と経済産業省で設置した暗号技術検討会（CRYPTREC）は、暗号解読の技術動向を監視することになっており、標準的に用いられている暗号が、近く解読される可能性があると判断した場合には、電子政府推奨暗号リストから削除することになっている。

（2）このリストの変更を受けて、システム構築者は、そのリストに代替暗号があればそれらのうちの1つを選び、対応するソフトを、デジタル署名応用システムを構成するサーバやクライアントに送付する。CRYPTERECは、電子政府で使う暗号の検討を行う組織であるが、現在の日本の最高レベルの暗号学者が集まっているので、ここでの検討結果は、民間のシステム構築者も利用するようになると予想される。

（3）一方、認証局ではシステム構築者が選定した代替暗号に対応できるようになっていなければ、新ソフトを追加する。そして、従来用いられていた暗号に対応して登録された公開鍵証明書をいつ無効化するかを宣言する。危殆化の状態によって直ちに無効化する必要がある場合と、少し、時間的余裕がある場合がある。

（4）デジタル署名を使って署名したいと考えている人は、新しい暗号に対応したソフトを導入し、ICカードやPCなどの中で、新しい鍵のペアを生成し、これを認証局に登録し、新しい公開鍵証明書を入手する。

（5）デジタル署名の検証者側でも、新しい暗号ソフトに置き換え、新しい暗号方式に対応した署名の検証を可能とする。

古い公開鍵証明書の無効化の時期が宣言された時点で問題となるのは、古い暗号方式に基づき作成した署名付文書の扱いである。この点については従来ほとんど検討されておらず、最大の課題となる（課題1）。また、従来の暗号ソフトから新しい暗号ソフトへの確実で容易な一斉の置き換えも現実には大きな課題である(課題2)。さらに、検証者側や認証局では複数の暗号を取り扱うことになり、容易に行えるようにするとともに、複数の暗号を取り扱えるようにすることがセキュリティホールの作りこみにつながらないようにすることも必要である（課題3）。

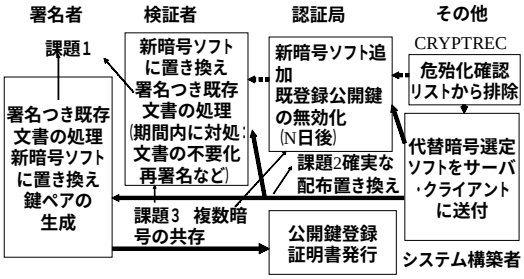

図4　飛躍的危殆化・代替暗号あり時の対応

[9]

パターン6の場合は一番対応が難しい場合で、以下のような対応が必要となる（**図5**参照）。

（1）CRYPTRECで標準的に用いられている暗号が、近く解読される可能性があると判断した場合には、電子政府推奨暗号リストから削除する。この場合は、代替暗号が無いので、別の暗号に置き換えるわけには行かない。そこで、デジタル署名以外の方式に切り替えるよう支持する必要がある。また、同時に、政府は大学などに対し代替暗号開発の緊急促進を依頼する必要があるだろうし、このような状態が生じないようにするために、日ごろから代替暗号の研究開発に資金的援助をしておく必要があると考えられる。

（2）認証局では、既登録の公開鍵証明書の無効化時期を宣言する。破局的危殆化の場合は直ち

に無効化しなければならない場合が多いと推定される。

(3) 従来の署名者や検証者はデジタル署名が利用できなくなるので、デジタル署名以外(例えば、すべて、紙を用いた取引など)へ移行しなければならない。

この場合にもパターン3の場合と同様に、古い暗号方式に基づき作成した署名付文書の扱いが問題となる(課題1)。また、電子署名以外への移行方法の開発と手順の明確化も大切な課題となる(課題4)。さらに、代替暗号の継続的開発も不可欠な課題である(課題5)。

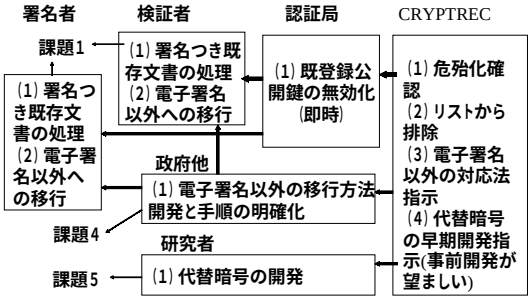

図5 破局的危殆化・代替暗号なし時の対応

11

他のパターンについても分析した結果、解決すべき課題は表2に示すように整理することができる。本報告では、このうち最も重要性が高いと考えられる署名付既存文書の処理方法を中心にその対応方法の整理と評価を行う。

表2 課題とその重要性

No	課題	重要性	備考
1	署名つき既存文書の処理	大大	従来の検討不十分
2	暗号ソフトの確実・迅速な配布置き換え	中	コンピュータの知識が十分でなくとも可能に
3	複数暗号の共存可能化	中	セキュリティホールを作りこまない共存可能化
4	電子署名以外の移行方法開発と手順の明確化	大	従来ほとんど検討なし
5	代替暗号の開発	大	色々な状況下での代替暗号の事前開発

12

4. 重要課題の対策案の検討と評価

ここでは、まず署名つき既存文書の処理方法を以下に記述する。

(1) 公開鍵暗号が危殆化した際に存在する署名つき文書をできるだけ少なくする必要がある。そのためには、署名後の署名付文書の有効期間を必要以上に長くしない工夫をする。例えば、政府が発行するものなら、署名付文書を、定期的に再発行する仕組みにする。免許書などは現在でも数年ごとに再発行しており、電子の世界でも同様に再発行するようにしておけばよい。そうすれば署名つき文書の有効期間が少なくなり、公開鍵暗号が危殆化する確率が下がると考えられる。

(2) 公開鍵暗号が危殆化した際に、署名つき既存文書が存在しても、あらかじめその対応方法を決めておくことにより、トラブルを防止する。例えば、危殆化が生じた後、その署名付文書が無効になる前に、(a) 新しく代替暗号で同じ文書に再署名するとか、(b) 既存の署名つき文書全体に代替暗号で再署名するとか、(c) その署名付文書を不要にする(例えば、近く無効になることがわかった電子証券は必ず現金化するなど)、とかを双方の合意の上で決めておくことが考えられる。そして、そのように事前に決めた対応方法は、署名ポリシーの形で残しておけばよいと考えられる。この署名ポリシーがわからなくなったり、不正に改ざんされたりする可能性もあるので別途対応が必要となる。

(3) 公開鍵暗号が危殆化してしまったとしても、なんらかの形で証拠性を残すことが考えられる。このような方法としては、(a) 信頼できる第三者機関やICカードなどの装置を利用する方法と、(b) 証拠性を残すための特殊なデジタル署名を行う方法がある。

このような証拠性を残す署名方式として、以下のような署名があることが指摘されている[2)]。

(ア) ヒステリシス署名[3) 5) 6)]
(イ) フォワード・セキュア署名[7)]
(ウ) キーインシュレイティド署名
(エ) タグ付署名
(オ) MAC付署名

しかし、これらの署名方式は鍵の漏洩形態によって有効な場合とそうでない場合があり、**表3**に示すように(イ)(ウ)は、不注意による鍵の紛失時などには有効であるが、公開鍵が危殆化するよう

な場合には、役に立たないことを知っておく必要がある。その意味で、(ア)のヒステリシス署名の有効な範囲は広いと考えられる。

今後、上記(1)を実施していくとともに、(2)(3)を組み合わせて実施していくことが大切になると考えられる。

このような方式として**図6**に示すようなセキュアストレージという方式が提案されている[4]。ここでは、署名ポリシーをポリシー証明書の形で発行するとともに、署名付文書を信頼できる第三者に保管を依頼し、署名付文書、署名ポリシー証明書、公開鍵証明書、証明書の有効期限が切れる段階でのCRL情報、最初の検証時のタイムスタンプなどを安全なストレージに保管し、裁判時などの再検証に備えようというものである。

これ自体は、合理的なものであるが、長期にわたり本当に信頼できる機関が存在するかという問題や、膨大なコストがかかるという問題がある。このため、安全かつ安価に実現する方式の提案が待たれている。

表3　特殊な署名方式の例と適用分野[2)]

方式	鍵の紛失時	公開鍵危殆化時
1. ヒステリシス署名	○署名履歴により署名があったかどうか類推可能	○署名履歴により署名が危殆化前か類推可能
2. フォアードセキュア署名	○署名鍵を頻繁に変えることにより影響のある文書をある時点以降に局限化	Xすべての署名鍵が危殆化するので通常対応困難
3. キーインシュレーティド署名	○署名鍵を頻繁に変えることにより、影響のある文書を対象署名に局限化	Xすべての署名鍵が危殆化するので通常対応困難
4. タグ付署名	○署名をするハードを限定することにより偽造検知	△署名をするハードを限定することにより偽造検知
5. MAC付署名	○MACを生成できるハードを限定することにより偽造検知	△MACを生成できるハードを限定することにより偽造検知

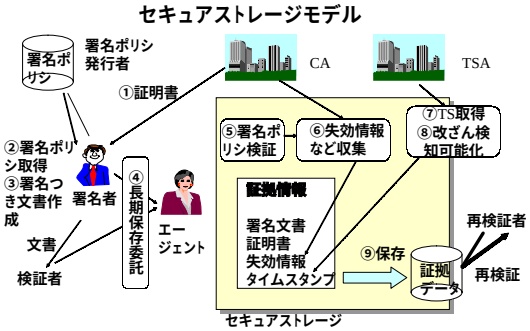

図6　信頼できる機関の利用方式の例

5. おわりに

以上、デジタル署名付文書を長期的に利用する場合の安全性の分析と対策案の評価を行った。今後、具体的対策技術(例えば署名ポリシー証明書とICカード、ヒステリシス署名を組み合わせる方式など)の提案を行って行きたいと考えている。

最後に、このような分析を行うきっかけを与えていただき、貴重な意見をいただいた早稲田大学岩村充教授、横浜国立大学松本勉教授をはじめとする関係者の方々に感謝申し上げる。

参考文献

1) 松本勉、岩下直行、「デジタル署名の長期的利用とその安全性について」日本銀行金融研究所、Discussion Paper No.2003-J-4、2003年3月31日

2) 宇根正志「デジタル署名生成用秘密鍵の漏洩を巡る問題とその対策」日本銀行金融研究所、Discussion Paper No.2002-J-32、2002年

3) 松本勉、岩村充、佐々木良一、松木武、「暗号ブレイク対応電子署名アリバイ実現機構(その1)－コンセプトと概要」情報処理学会研究報告2000-CSEC-8、情報処理学会、2000年3月、pp13－17

4) 米倉早織「電子署名文書長期保存の要件」ビジネスショウ2002　2002年5月22日、http://www.ecom.jp/ecit/tenji/bisinessshow2002/yonekura.pdf

5) 洲崎誠一、松本勉、「電子署名アリバイ実現機構　－ヒステリシス署名と履歴交差」情報処理学会論文誌Vol. 43, No. 8、2002年8月、pp2381－2393

6) 宮崎邦彦、吉浦裕、岩村充、松本勉、佐々木良一「連鎖構造を用いた電子署名技術における信頼性評価方法の提案」電子情報通信学会技術報告、Vol. 102, No. 212, 電子情報通信学会、2002年7月、pp109－115

7) Bellare, Mihir, and Sara K. Miner “ A Forward-Secure Digital Signature Scheme,” Proceedings of CRYPTO’99, LNCS 1666, pp431-448, Springer-Verlag, August 1999