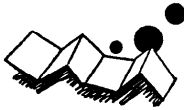


解説

認証とデジタル署名†



小山 謙 二†

1. はじめに

電子送金 (EFT), 電子郵便, オフィス・オートメーション (OA) など, 通信とコンピュータを融合したシステムが広く社会に普及しつつある。これらのシステムが社会に浸透すればするほど, システムの安全性と信頼性を確保することが重要となる。特に, 最近のコンピュータ犯罪の急増に伴い, セキュリティに対する関心と要求が高まっている^{1), 2)}。システムの不正使用, 例えば, 盗聴, 無断コピー, ニセデータ入力, 改ざん, 偽装などを防止し, セキュリティを向上させる技術的対策が, 最近広範に取り組み始めた。盗聴, 無断コピーへの対策として暗号化技術があり, ニセデータ入力, 改ざん, 偽装への対策として認証技術がある。認証すべき対象として重要なものは個人と情報の内容である。ニセモノとホンモノを区別し, 認証することは昔から重要な問題であり続けているが, 特に, 最近ではデータ通信の進展に伴い, 個人や情報の内容の真偽を自動的 (機械的) に認証することが必要となってきた。さらに, デジタル化された情報の内容の認証は新たな課題として提起されている。

本稿では, これらの課題への技術的アプローチとして, 個人を認証するための個人照合技術と, 個人と情報の内容を認証する, 暗号を用いたデジタル署名について解説する。

2. 個人の認証

犯罪防止, 機密保持のために, 個人を認証してアクセス制御を行う方法が広く用いられている。個人の認証 (authentication) の方法は識別 (identification) と照合 (verification) に大別される⁴⁾。個人識別と個人照合はいずれもあらかじめ認証すべき個人のパターン (パスワード, 指紋など) を登録しておくことが前提となる。個人識別は個人のパターンのみ入力し, 入力

パターンが誰のパターンに一致するか, または, 似ているかを判定するものである。一方, 個人照合は個人のパターンと個人識別名 (ID: identifier) を入力し, 入力パターンが名乗った本人のパターンとみなせるか否かを判定するものである。

犯罪捜査では, 例えば遺留指紋から犯人を同定するように, 主に個人識別が行われているが, アクセス資格検査では, 個人識別より処理が容易で確実なので, 個人照合が通常行われる。したがって, データ通信での個人の認証法は個人照合技術が用いられている。そこで, 2.1 節で, 個人照合技術の特徴と動向を, 2.2 節で照合による個人認証の応用例を述べる。

2.1 個人照合技術

個人照合の方法をその手段, すなわち, 入力パターンの性質で分類すると, 記憶内容によるもの, 所有物によるもの, 個人特性によるものの3つに大別される。一方, セキュリティの指標として, 信頼性 (reliability) と安全性 (safety) がある。信頼性が高いとは, 正規の者が受け入れられない確率が小さいことを意味し, 安全性が高いとは, 正規でない者が受け入れられる確率が小さいことを意味する。個人照合の手段とその特徴を表-1 に示す。個人特性による個人照合法が最もセキュリティが高いことが分かる。しかし, 個人特性による照合は処理が複雑となり, 判定の正確さが

表-1 個人照合の手段と特徴

項目 \ 手段	記憶内容	所有物	個人特性
具体例	パスワード, 暗証番号, 暗号鍵, 電話番号	磁気カード, ICカード, 物理的鍵, 印鑑	指紋, 手形, 筆跡, 音声, 顔
信頼性	△ (忘却の可能性あり)	△ (紛失・破壊の可能性あり)	○ (経年変化するものもある)
安全性	△ (推定, メモの盗難, 有資格者による盗聴の可能性あり)	△ (盗難の可能性あり)	○
データ量と照合処理時間	○ (少)	○ (少)	△ (多)
研究実用化	実用化段階	実用化段階	研究段階

† Authentication and Digital Signature by Kenji KOYAMA (Musashino Electrical Communication Laboratory, N.T.T.).

†† 日本電信電話公社武蔵野電気通信研究所

表-2 個人特性による照合技術

項目 手段	有効な個人性パラメータ	情報量	処理時間	識別率	実用化例	研究機関別
指 紋	隆線の分岐点・端点の位置	200バイト	2.5秒	$P_1=99.63\%$ $P_2=99.97\%$	米 Finger matrix 社 ^(*) 5,000~6,000ドル/台	FBI, 警察庁
手 形	指の長さ	4バイト	数秒	$P=99.72\%$	米 Identimat 社 ^(*)	米国空軍
筆 跡	筆の速度・加速度, 筆圧 (オンライン)	50バイト	数秒	$P_1=99\%$ $P_2=98.5\%$	米 Sycon 社 ^(*) 1,000~2,000ドル/台	名大, 通研 SRI
音 声	鼻音のスペクトル (ケブストラム) 高次ホルムント周波数	600バイト	12秒	$P_1=97\%$ $P_2=98\%$	—	IBM 社, ベル研 TI 社, 通研 ^(*)
顔	目, 鼻, 口の相対位置, 横顔の輪郭	100バイト	数秒	$P=86\sim 100\%$	—	Case Western Reserve 大 ^(*) ベル研, 京大, 通研

注) 1. 各項目の数値などは * 印のついた実用化例または研究例による。

2. P_1 は本人を正しく受理する確率, P_2 は他人を正しく棄却する確率を表わし, P はその平均を表わす。

完全とはいえない。したがって、現在は、正確さ、照合時間、価格の点から、記憶内容と所有物による自動的個人照合の手法が実用化されている。将来の個人照合技術では、個人特性による照合を併用することが必要と思われる。個人特性による照合技術を実用化するには、個人の特性を表わすパラメータの選定、類似度の定義、個人パターンの特徴抽出法のアルゴリズムと実現技術、類似度のしきい値による比較判定のアルゴリズムがポイントとなる。

表-2 に個人特性による照合の代表的な手段について、有効な個人性パラメータ、情報量、処理時間、識別率、および、研究機関、実用化例を示す。

2.2 個人の認証の応用例

金融機関の CD (現金自動支払機) や ATM (現金自動預入支払機) には暗証番号と磁気カードが使われている。コンピュータ室など機密性のある部屋への入室管理には通常、磁気カードが使われ、暗証番号や手形によるチェックが併用されている例もある。大型計算機の利用資格検査ではパスワードが使われている。銀行・信販・百貨店・スーパーの会員制のクレジットカードは磁気帯のない単なるプラスチックカードが多く使われている。しかし、総合信販の GC カードでは本社のホスト・コンピュータと加盟店の端末がオンラインで接続され、磁気カードと暗証番号で個人照合が行われている。さらに、これで会員の信用チェックと売り上げ処理をする点でわが国では最も進んだクレジットカードシステムといえる³²⁾。

また、磁気カードの発展形として、従来のカードと同じ形状で、LSI メモリとマイコンが内蔵された IC カードが出現している。この IC カードは大量の記憶容量と演算機能をもつので、セキュリティ・チェック

の高度化、ホストコンピュータの負荷軽減に役立つ。現在、フランスの一部の金融機関や米国の軍で実用に供せられており、将来性のある技術である。

電電公社が提供している二重番号サービスやポケットベルのデュアルコールサービスも、記憶内容によって送信者を認証している応用例である。すなわち、1 台の電話 (ポケットベル) に、2 種類の電話番号をつけ、片方の電話番号を特定の人にだけ知らせておき、受信した電話番号の違いにより、着信拒否したり、鳴音が異なるようにして呼出元を識別している。また、発信者の電話番号が着信電話に表示される装置の実用化は高度情報通信システム (INS) の実現目標の 1 つである²⁸⁾。

3. デジタル署名の目的と原理

3.1 デジタル署名の目的

従来の署名は紙の上に書かれた個人特有の筆跡 (アナログ的なパターン) により文書の内容と筆者が正しいものであることの認証が行われてきた。しかし、従来の署名をオンラインのデータ通信にそのまま適用しようとする、認証機能を果たすことができない。例えば、ファクシミリで送られた文書は、複写機でコピーされた文書と同様に、署名部分 (アナログ的なパターン) を容易に偽造できるので、法的に正式文書とみなされていない。まして、デジタル情報の通信と蓄積を行うデータ通信においては署名部分のデジタル情報はさらに容易にコピーできるので、従来の署名法は使うことができない。

そこで、デジタル情報に対しても従来の署名と同様の機能を果たすことができる手法の開発が要請されており、その解決策がデジタル署名と呼ばれている

ものである⁹⁾。

デジタル署名の目的はデジタル化された通信情報(メッセージ)と蓄積情報(ファイル)に対し、それぞれ、情報の送信者(筆者)の身元の確認と、情報の内容が改ざんされていないことの確認を受信者(読者)が行うことにある(以下、署名の対象となる情報をメッセージと呼ぶ)。

デジタル署名が上記の目的を果たすためには、次の3つの性質をもつ署名付きメッセージを生成できることが必要である¹⁰⁾。

- ① 署名付きメッセージが第三者によって偽造できないこと、
- ② 署名付きメッセージが受信者によって偽造できないこと、
- ③ 署名付きメッセージを送った事実を送信者が後で否定できないこと。

上記の3つの条件をデジタル署名の3条件と呼ぶ。

3.2 認証の原理

メッセージの認証を行うためには、送りたい狭義のメッセージ M に対して、送信者の個人識別名($S-ID$)、受信者の個人識別名($R-ID$)、メッセージの通し番号($SEQ-NO$)および日時(T)などの情報を付加する必要がある。この付属情報を

$$m = \langle S-ID, R-ID, SEQ-NO, T \rangle$$

とする。したがって、認証の対象は広義のメッセージ

$$M' = \langle m, M \rangle$$

となる。

デジタル署名を行うためには暗号が用いられる。署名に用いる暗号は慣用暗号と公開鍵暗号に大別される。慣用暗号は転置と換字を基本原理としており、暗号化鍵と復号化鍵が同じでそれぞれ秘密にしておくのが特徴である。代表例として、データ暗号化規格DES¹¹⁾がある。一方、公開鍵暗号は落し戸式一方性関数を基本原理としており、対となっている暗号化鍵と復号化鍵が異なり、暗号化鍵を公開し、復号化鍵を秘密にしておくのが特徴である。代表例としてRSA¹⁴⁾法がある。

デジタル署名に暗号を用いて認証する方式としてメッセージ復元法と認証子法がある。

メッセージ復元法においては、送信者がメッセージに暗号処理をして署名付きメッセージに変換し、受信者に送る。受信者は送られてきた署名付きメッセージに暗号処理の逆操作を施して元のメッセージを復元す

る。復元されたメッセージに含まれている付属情報が意味のあるものならば、受信者はメッセージの送信者と内容が正しいと認証する。

メッセージ復元法には慣用暗号と公開鍵暗号が適用できる。慣用暗号では前もって秘密の認証用の暗号鍵を共有しておく必要がある。公開鍵暗号では送信者は自分しか知らない秘密鍵で暗号処理し、受信者は公開の鍵で暗号処理の逆操作を施すことができるので、秘密の鍵の配送は不必要である。

一方、認証子法は検証(validation)とも呼ばれている方法である。送信者はメッセージに暗号処理をして署名付きメッセージの一種である認証子(authenticator)に変換し、生のままのメッセージとともに受信者に送る。受信者は送られてきた生のメッセージとともに新たに認証子に変換する。受信者は送られてきた認証子と自ら求めた認証子が一致するかどうかを判定し、もし一致したなら、メッセージの送信者と内容が正しいと認証する。

認証子法に適用できる暗号処理は、入力メッセージと鍵に依存した乱数発生法でよい。すなわち、慣用暗号や公開鍵暗号のように、暗号処理の逆操作が保証されている必要はない。しかし、通常、慣用暗号が用いられている。

3.3 認証機能をもつ公開鍵暗号アルゴリズム

メッセージ M に対して、暗号化鍵 k^e を用いた暗号化操作を $E(k^e, M)$ とし、復号化鍵 k^d を用いた復号化操作を $D(k^d, M)$ とすると、公開鍵暗号アルゴリズムは、まず、次の2つの条件を満たすことが必要である。

(1) k^e が分かっても、これから k^d を求めることは計算量の点で困難である。

(2) k^e と k^d の対を生成することは容易である。

次に、公開鍵暗号を用いて秘密通信ができる条件は上記の(1)、(2)に加えて、次の(3)の条件が成立することが必要である。

(3) すべてのメッセージ M に対し、

$$E(k^e, M) \text{ が定義でき、}$$

$$D(k^d, E(k^e, M)) = M$$

が成立する。

一方、公開鍵暗号を用いてデジタル署名通信ができる条件は上記の(1)、(2)に加えて、次の(4)の条件が成立することが必要である。

* k^p , k^s はそれぞれ公開鍵(public key), 秘密鍵(secret key)を意味し、 p , s の添字はべき指数でなく、鍵の特性を表わす。

(4) すべてのメッセージ M に対し, $D(k^*, M)$ が定義でき,

$$E(k^*, D(k^*, M)) = M$$

が成立する。

公開鍵暗号では, 公開鍵を用いる処理を暗号化, 秘密鍵を用いる処理を復号化という。秘密通信では暗号化・復号化の順に行うが, デジタル署名では復号化・暗号化の順に行う。すなわち, 復号化の入力は平文メッセージであってもよい。

(3), (4)の条件を写像の用語に換言すると, (3)の条件は E が単射で, D が全射であることが必要であり, (4)の条件は, E が全射で, D が単射であることが必要である*。

現在までに提案されている公開鍵暗号の具体的アルゴリズムは Rivest・Shamir・Adleman の RSA 法¹⁴⁾, Merkle・Hellman の MH 法¹⁵⁾, Rabin の R 法¹⁶⁾, Shamir の S 法¹⁷⁾ が有名である。各アルゴリズムの詳しい解説^{11), 12)}は本稿では省略する。RSA 法と R 法は素因数分解の困難さを基にし, MH 法と S 法は「ナップザック問題」の解法の困難さを基にした落し戸式一方向性関数を用いる。表-3 に各法の写像の性質を示す。表-3 より明らかなように, RSA 法は E と D が全単射であるので, 秘密通信とデジタル署名が可能である。MH 法は秘密通信は可能であるが, 一部のメッセージにしかデジタル署名ができない。R 法は 4:1 の写像なので秘密通信においては 1 つのメッセージを暗号化して復号化すると 4 種類のメッセージが復元されるので, その中から意味のある 1 つのメッセージを選択することが必要となり, デジタル署名においては, 全メッセージ空間の 1/4 のメッセージがデジタル署名可能となる。S 法はナップザック問題による方法を秘密通信は不可能だが, デジタル署名は可能のように改訂したものである。

表-3 公開鍵暗号のアルゴリズムの写像

アルゴリズム	暗号化関数 E		復号化関数 D	
	全 射	単 射	全 射	単 射
RSA 法	○	○	○	○
MH 法	×	○	○	×
R 法	×	×	×	×
S 法	○	×	×	○

* 集合 X から Y への写像 E について, Y の任意の元 y に対し, $y = E(x)$ なる $x \in X$ が存在するなら, E を X から Y への全射 (surjection) といい, X の任意の 2 元 x_1, x_2 に対し, $f(x_1) \neq f(x_2)$ が成り立つとき, E を X から Y への単射 (injection) という。

ところで, RSA 法では, 複数個 (l 個) の個別鍵 (k_i^*, k_i') , ($1 \leq i \leq l$) に共通に代替できる。すなわち, 次式を満たす真のマスタ鍵 $(\bar{k}^*, \bar{k}')$ が提案され, さらに, このマスタ鍵の導出法が明らかにされている。

$$\begin{aligned} E(k_i^*, M) &= E(\bar{k}^*, M) \\ D(k_i', M) &= D(\bar{k}', M) \end{aligned} \quad (1 \leq i \leq l)$$

このマスタ鍵を用いてもデジタル署名ができるので¹⁸⁾, 正規の受信者集合へ放送 (同報) 形態で機密保護つきデジタル署名通信ができる¹⁹⁾。

3.4 データ圧縮による検証

ところで, 広義のメッセージ M' をそのまま暗号処理して検証を行うと, 認証子の長さは元のメッセージ M' と同一の長さとなり, 効率が良くない。安全性を損わない範囲で署名付きメッセージの長さを圧縮して, 検証を効率化する方法が提案されている。

ANSI (米国規格協会) と ISO (国際標準化機構) で標準化が進められている認証方式²⁰⁾は, DES を用いた検証方式であり, その概要を説明する。

64 ビットのランダムベクトル RV^* と付属情報 m および狭義のメッセージ M を含んだ広義のメッセージが $64n$ ビットの大ききとすると, 64 ビットごとに n 個のブロックに分割する。

$$\begin{aligned} M' &= \langle RV, m, M \rangle \\ &= \langle M_1, M_2, \dots, M_n \rangle \end{aligned}$$

送信者は受信者と前もって共有している検証用の暗号鍵 k で, 以下の暗号文の系列 $C_i (1 \leq i \leq n)$ を生成する。

$$\begin{aligned} C_1 &= E(k, M_1) \\ C_2 &= E(k, M_2 \oplus C_1) \\ C_3 &= E(k, M_3 \oplus C_2) \\ &\dots\dots\dots \\ C_n &= E(k, M_n \oplus C_{n-1}) \end{aligned} \quad (1)$$

ただし, $\oplus$ は排他的論理和 (exclusive OR) を表わす。最終的に得られた C_n の上位 32 ビットを認証子として, 生のままの M' とともに受信者に送る。受信者は M' に検証用の鍵 k で式 (1) と同じ操作を施す。もし, 同一の認証子が得られたならば, メッセージの内容と送信者を認証できる。この方式は DES を CBC (Cipher Block Chaining) モードで利用したものであり, 流れ図を図-1 に示す。

この方式による認証子は M' のすべてのビットに依

* メッセージの最初の部分によく現われるビットパターンや繰り返し送られるメッセージを偽装するために固定長の乱数を広義のメッセージに含める。

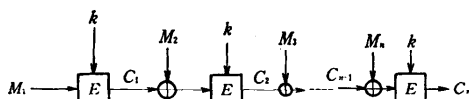


図-1

存して生成されるので、メッセージを途中で変えられても、受信者が認証子との対応の違いからメッセージの改ざんや誤りを見つけることができる。また、検証鍵は送信者と受信者が秘密に持っているため、第三者は認証子を作ることができない。

以上の方式は送信者または受信者が信頼できて、もめごとが起こらないシステムに有効である。例えば、ホストコンピュータ側が信頼できて、端末との通信を認証する場合に適用できる。この方式はオンラインの入力データの責任者を明確にするために、米国の金融機関を中心に実用化され始めている。暗号化関数 E として、DES を採用しているのは米国のチェスマンハッタン銀行、シティ銀行、ファーストインターステート銀行などがあり¹³⁾、独自の暗号アルゴリズムを採用した例としてスウェーデン銀行などがある。

4. デジタル署名の手順 (プロトコル)

前章で署名に用いる暗号として慣用暗号と公開鍵暗号があることを述べた。一方、署名の構成法としては、直接署名と調停署名に大別できる。直接署名では受信者が直接、メッセージの正当性を認証する。もめごとが起こった場合のみ判定者 (judge) が呼ばれ、送信者と受信者のいずれが正しいかの判断を下す。一方、調停署名では、すべての署名は調停者 (arbitrator) を介して行われ、調停者がメッセージの正当性を認証し、その結果を受信者に知らせる。したがって、調停署名は調停者の信頼性に大きく依存している。

以上述べたように、デジタル署名の手順は暗号の種類と構成法の違いにより4通りの方式が考えられる。次節で各方式の手順 (プロトコル) と特徴について述べる。

4.1 慣用暗号による直接署名

歴史的には、初期のデジタル署名はこの分類に属している。この署名法の有名な例は Lamport⁹⁾ と Rabin²¹⁾ によって提案されている。

まず、Lamport の手法を説明する。

step 1 n ビット長の広義のメッセージ M' を署名する場合、送信者 S はランダムに $2n$ 個の鍵

$$K = \{k_{10}, k_{11}, k_{20}, k_{21}, \dots, k_{n0}, k_{n1}\}$$

を生成し、秘密に保管しておく。さらに、 S は $2n$ 個の検証パラメータ

$$U = \langle u_{10}, u_{11}, u_{20}, u_{21}, \dots, u_{n0}, u_{n1} \rangle$$

をランダムに生成し、 u_{ij} を鍵 k_{ij} ($1 \leq i \leq n$, $0 \leq j \leq 1$) で暗号化した値

$$V = \langle E(k_{10}, u_{10}), E(k_{11}, u_{11})$$

$$\dots, E(k_{n0}, u_{n0}), E(k_{n1}, u_{n1}) \rangle$$

$$= \langle v_{10}, v_{11}, v_{20}, v_{21}, \dots, v_{n0}, v_{n1} \rangle$$

を求める。署名に先立って、 S は受信者 R と判定者 J に U と V を秘密に送る。

step 2 メッセージ M' の署名を行うには、 M' の第 i 番目のビットが 0 のとき $k_i^* = k_{i0}$ とし、1 のとき、 $k_i^* = k_{i1}$ とする。

S は R と J へ全部で n 個の鍵

$$K^* = \langle k_{1^*}, k_{2^*}, \dots, k_{n^*} \rangle$$

を署名として送る。 M' は生のまま送る。

step 3 R は、受信した M' と K^* をもとに、認証する。具体的には、 M' の第 i 番目 ($1 \leq i \leq n$) のビットが 0 ならば、 $v_{i0} = E(k_{i^*}, u_{i0})$ が成立し、1 ならば、 $v_{i1} = E(k_{i^*}, u_{i1})$ が成立することを確認する。

この方式では署名 K^* の長さが (1 個の鍵の長さ) $\times$ (メッセージ長) となる。DES の場合 K^* は 56 n ビットの署名長となり、検証パラメータ U と V の全情報量は $256n$ ($=64 \times 2 \times 2 \times n$) ビットとなる。

次に、Rabin の手法を説明する。

step 1 送信者 S はランダムに l 個の鍵 (l はメッセージ長に無関係)

$$K = \langle k_1, k_2, \dots, k_l \rangle$$

と l 個の検証パラメータ

$$U = \langle u_1, u_2, \dots, u_l \rangle$$

を選ぶ。次に、 u_i を k_i で暗号化した値

$$V = \langle E(k_1, u_1), \dots, E(k_l, u_l) \rangle$$

$$= \langle v_1, v_2, \dots, v_l \rangle$$

を求める。 S は受信者 R と判定者 J に署名に先立って、 U と V を送る。

step 2 S はメッセージ M' を k_i で暗号化した値

$$W = \{E(k_1, M'), \dots, E(k_l, M')\}$$

$$= \{\omega_1, \omega_2, \dots, \omega_l\}$$

を署名として R と J に送る。

step 3 R は l 個の鍵のうち r 個 ($r \leq l$) の任意の鍵

$$K^* = \{k_{1^*}, k_{2^*}, \dots, k_{r^*}\}$$

を指定して、 S より送ってもらう。

R はこれらの r 個の鍵で

$$v_i^* = E(k_i^*, u_i^*)$$

$$\omega_i^* = E(k_i^*, M)$$

の両式が成立することを確認して認証する。

この方式の安全性は l と r の数に依存しており、確率的な認証方式といえる。

以上の2つの方式は、デジタル署名の3条件を満たすことができる。すなわち

①' 第三者は M' を改ざんしても、 K^* を意味のあるように改ざんすることができない。

②' 送信者と判定者は、 U, V, K を保管しているので、受信者は改ざんできない。

③' 受信者と判定者は U, V, K^* を保管しているので、送信者はメッセージを送った事実を否定できない。

この署名法では、送信者と受信者間で真偽のもめごとが起こる場合の対策として、送信者は V と U を判定者に送っておく。判定者は、もめごとが起こった場合どちらが正しいかを容易に判定できる。

この署名法は次のような欠点をもつ。

(a) 送信者と受信者は実際のメッセージの通信の前にかかなり多くの情報、つまり、 V と U を共有しなければならない。

(b) V と U は秘密に通信しなければならない。

(c) V と U はメッセージごとに更新しなければならない。

以上の理由で、この署名法は時間がかかり、非効率と一般に考えられている。

4.2 慣用暗号による調停署名

この分類の署名法はさまざまな実現法が提案されているが、いずれも署名を行う前に、送信者 S と調停者 A は秘密鍵 k_{SA} を共有し、調停者 A と受信者 R は秘密鍵 k_{AR} を共有していることが前提となる。この署名法では慣用暗号をメッセージ復元法または認証子法の両方に適用できる。代表例として前者の手順を示す。

step 1 送信者 S は広義のメッセージ M' を k_{SA} で暗号化した C を調停者 A に送る。

$$C = E(k_{SA}, M')$$

$$S \xrightarrow{C} A$$

step 2 調停者 A は C を k_{SA} で復号化し、 M' を得る。

$$M' = D(k_{SA}, C)$$

M' が意味のあるものかどうかを検査し、もし、正しいと認証したなら、合格証 P と C

と M' を含んださらに広義のメッセージ M''
 $M'' = \langle P, C, M' \rangle$

を k_{AR} で暗号化した C' を受信者 R に送る。

$$C' = E(k_{AR}, M'')$$

$$A \xrightarrow{C'} R$$

step 3 受信者 R は C' を k_{AR} で復号化し、 M'' を得る。

$$M'' = D(k_{AR}, C')$$

M'' が意味のあるものかどうかを検査し、もし、正しいければ、 M' が S から A を経由して送られ、改ざんされていないと認証する。

この手順はデジタル署名の3条件を満たしている。すなわち、①の条件は、第三者が秘密鍵 k_{SA}, k_{AR} を知らないから達成できる。②の条件は、 M'' に C を含めることにより達成している。なぜならば、 k_{AR} を知っているが k_{SA} を知らない受信者が、自分自身に調停者を介さないメッセージを送り、それが送信者 S から来たという主張ができないからである。③の条件は、 C を調停者が保管しておくことにより達成できる。

この署名法は2種類の秘密鍵が安全に保管されている限り、署名の偽造ができないという意味で安全である。この署名法の手順の主な欠点は調停者の信頼性に大きく依存している点である。具体的には

(1) 狭義のメッセージ M の内容が機密性の高いものであっても、 A はその内容を読むことができる。

(2) S は A と組んでメッセージを送信した事実を否定することができ、 R は A と組んであたかも S から送られてきたようにメッセージを偽造できる。

の2つの問題点がある。1番目の問題点に対しては、 M を A に送る前に、 S と R で共有している秘密鍵 k_{SR} で暗号化することにより解決できる。すなわち、 S から A へは $C = E(k_{SA}, \langle m, E(k_{SR}, M) \rangle)$ を送り、 A は m をもとに認証する。次に A から R へは、 $C' = E(k_{AR}, \langle P, C, m, E(k_{SR}, M) \rangle)$ を送り、 R は k_{AR} で復号化して認証し、 k_{SR} で復号化して秘密のメッセージの内容を知る。

2番目の問題点に対する一つの解決策として、調停者の数を増やすことが提案されている²²⁾。(p, q) 調停者法がそれであり、 p は q 以上の数である。送信者は p 人の調停者の集合を選び、受信者はその集合の中から q 人の調停者を選び、メッセージの認証をやってもらう。この方法の安全性は p と q を大きくすれば調停者が不正をはたらく可能性が減少するというこ

に基づいている。しかし、複数の調停者のサービスを受けることは高価になる。

4.3 公開鍵暗号による直接署名

直接署名は公開鍵暗号の性質を用いればうまく実現できる。特に、公開鍵暗号による直接署名は、その特長から「真の署名」とも呼ばれている。

この署名法の手順を以下に示す。

step 1 送信者 S は自分のみが知っている秘密鍵 k_S を用いて広義のメッセージ M' を復号化して C を作成し、受信者 R に送る。

$$C = D(k_S, M')$$

$$S \xrightarrow{C} R$$

step 2 受信者 R は S の公開鍵 k_S を用いて C を暗号化して M' を得る。

$$M' = E(k_S, C)$$

M' が意味のあるものならば、正当性を認証できる。

この手順は、 k_S が一般公開されているので、 C を受信した者はだれでも送信者とメッセージの内容を認証できる。この手順はメッセージの内容の機密性は保たれないが、特定の放送局から不特定多数の受信者に放送する場合の認証に適用できる。

次に機密保護機能付きの署名を行う手順を示す。

step 1 送信者 S は自分のみが知っている秘密鍵 k_S を用いて広義のメッセージ M' を復号化して C を作成する。さらに、 C を受信局 R の公開鍵 k_R を用いて暗号化して Z を作成し、 R に送る。

$$C = D(k_S, M')$$

$$Z = E(k_R, C)$$

$$S \xrightarrow{Z} R$$

step 2 受信者 R は自分のみが知っている秘密鍵 k_R を用いて Z を復号化して C を得る。さらに、送信局 S の公開鍵 k_S を用いて暗号化して M' を得る。

$$C = D(k_R, Z)$$

$$M' = E(k_S, C)$$

M' が意味のあるものならば、正当性を認証できる。

この公開鍵暗号による直接署名は慣用暗号による直接署名の欠点を克服していることは明らかである。送信者 S の秘密鍵 k_S を知っているのは S だけなので、受信者 R はメッセージ M を変更できない。したがっ

て、もめごととは容易に解決できる。 k_S の秘密が送信者 S によって完全に守られている限り、この署名法はうまくいく。しかし、もし、送信者が署名付きメッセージを送った事実を否定したくなったら、彼は自分の秘密鍵を失ったり、盗まれたと主張し、だれか第三者がその鍵を用いて署名付きメッセージを送ったに違いないと主張できる²⁵⁾。この解決策は、すべての署名付きメッセージに真の日時を含めておき、送信者が、真偽は別として、彼の秘密鍵の被害にあった日時 t を中央の調停者の届け出ることによって達成できる。受信者は、送信者 S からのメッセージを受けとるたびに、調停者に S の鍵が有効かどうかを確認する。もし、届け出が出ていれば、署名付きメッセージから復元された日時 t' が t より以前かどうかを調べ、署名の有効性を確認する。届け出が出ていなければ、そのまま認証する。

一方、ほんとうに送信者が鍵を盗まれた場合、第三者が t より以前の日時を使って署名付きメッセージを自分自身または他の者へ送ることができる。これらの問題は真の日時を調停者が与える方法を探らなければ解決できない。すなわち、最初から調停者を介入させた署名を用いない限り、解決できないようである。

4.4 公開鍵暗号による調停署名

4.2 節で述べた慣用暗号による調停署名の問題点、および、4.3 節で述べた公開鍵暗号による直接署名の問題点を解決する方法が文献(22), (24)で提案されている。その考え方は、公開鍵暗号による調停署名を行うことにある。送信者 S 、調停者 A 、受信者 R はそれぞれ自分の秘密鍵 k_S 、 k_A 、 k_R を保持し、これらに対応した公開鍵 k_S 、 k_A 、 k_R を他の二者に公開する。 S から R へ送りたい狭義のメッセージを M 、付属情報を m とすると、手順は以下の通りである。

step 1 送信者 S は

$$C_1 = E(k_R, D(k_S, M))$$

を計算する。次に、広義のメッセージ M' を

$$M' = \langle m, C_1 \rangle$$

とし、さらに、

$$C_1' = E(k_A, D(k_S, M'))$$

を計算し、 A に送る。

$$S \xrightarrow{C_1'} A$$

step 2 調停者 A は

$$M' = E(k_S, D(k_A, C_1'))$$

を計算し、 m より、メッセージの認証を行

う。次に、 A は C_1' を受けとった日時 t を m に追加し、 m' とする。 m' と合格スタンプ P と C_1 を含んだ広義のメッセージ $M'' = \langle m', P, C_1 \rangle$ に対し

$$C_1'' = E(k_R, D(k_A, M''))$$

を計算し、 R に送る。

$$R \xrightarrow{C_1''} A$$

step 3 受信者 R は

$$M'' = E(k_A, D(k_R, C_1''))$$

を計算し、 M'' が A で認証されたことを確認する。さらに、 M'' より C_1 を抽出してから

$$M = E(k_S, D(k_R, C_1))$$

を計算し、 M の内容を知る。

この署名法が前節までの署名法の問題点をすべて解決することは容易に分かる。すなわち

(1) 送信者と調停者と受信者の間で、署名付きメッセージの通信に先立って秘密鍵の情報を共有する必要がない。

(2) 秘密鍵が盗難などの危険にさらされても、不正な日時の付いたメッセージが送られることはない。

(3) 送信者と受信者の間で機密性を守りたい狭義のメッセージは調停者にはその内容が見えない。さらに、送信者と調停者、あるいは、受信者と調停者が組んだ不正は防ぐことができる。

4.5 ま と め

4.1節~4.4節で示したように、ディジタル署名の手順(プロトコル)の発展の流れは、不正対策を考慮して直接署名から調停署名へ、認証の手間の軽減を目指して慣用暗号から公開鍵暗号へと変遷していることが分かる。このなかで、公開鍵暗号による直接署名の原理は画期的であり、この考案によりディジタル署名が脚光を浴び始めたともいえる。また、慣用暗号を用いた署名では、認証用の秘密鍵を送信者と受信者で共有する必要があるが、この鍵配送の問題も公開鍵暗号による秘密通信を適用すれば容易に解決できる。

ところで、現在のビジネス社会におけるメッセージの認証はアナログパターン情報をもとにし、個人特性による筆跡や個人の所有物の実印で実現されている。一方、ディジタル信号のメッセージの認証を行うディジタル署名では、個人の記憶による秘密の暗号鍵で実現されることに注意しよう。したがって、ビジネス社会に新たにディジタル署名を導入するには、実現技術の確立、法律や運用体制の整備が必要となろう。

最後に、ディジタル署名を支える暗号の実現技術の現状を簡単にふれる。いかなる暗号アルゴリズムも汎用コンピュータのソフトウェアで容易にインプリメントできるので、現在、ソフトウェアでプロトタイプを実現している例が多い。しかし、実用に供するには、高速・安価な暗号化専用ハードウェアが望まれている。DES は専用 LSI や装置が市販され、RSA 法は専用 LSI が試作されている段階である²⁷⁾。ちなみに、AMD 社から 14 Mbps の DES チップ(現在、市販されている LSI で最高速)が 90 ドルで提供されており、MIT と通研ではそれぞれ、1.2 kbps と 50 kbps の RSA 法チップを試作・検討中である。

したがって、ディジタル署名を実現するには、郵政省の暗号通信システムのプロトタイプのように、DES と RSA 法を併用することが現実的な解となろう。

5. お わ り に

通信網とコンピュータシステムのセキュリティ向上を図る認証技術として、個人照合技術とディジタル署名の原理と方式を概観した。

一般に、セキュリティに対する投資額は、セキュリティ対策を施さない場合の損失額より低いことが必要である。今後、高度情報通信システムが社会に浸透すればするほど、両者の金額は増加するであろう。また、セキュリティ技術は一見、守りの技術に見えるが、特に、認証技術は、親展サービス、内容証明メールサービスなどの付加価値を生む改めの技術でもある。

今後の課題は、原理的に有望な方式を高速・安価に提供することであろう。

参 考 文 献

- 1) Parker, D.B.: Computer security management, Printice-Hall Co., 1981(邦訳: コンピュータ・セキュリティ犯罪対策と災害対策一, 日本情報処理開発協会/監訳, 企画センター, 1982).
- 2) 鳥居壮行: 検証・日本のコンピュータ犯罪, コンピュータ・エージ社(1982).
- 3) 特集: カード化ですすむコンピュータリゼーション, コンピュートピア(8月号1982年).
- 4) 白井克彦: 個人の識別技術一話者, 筆跡, 指紋, 顔, 計測と制御, Vol. 20, No. 1 (1981).
- 5) 阿部 弘: セキュリティシステムにおける識別技術, 計測と制御, Vol. 20, No. 1 (1981).
- 6) Mier, E. E.: ID verification at your fingertips, Data Communications (July 1982).
- 7) 古井貞照: ケプストラムの統計的特徴による話

- 者認識, 信学論 (A), Vol. J 65-A, No. 2 (1982).
- 8) Harmon, L. D., Kuo, S. C., Ramig, P. F. and Raudkiri, U.: Identification of human face profiles by computer, Pattern Recognition, No. 10 (1978).
- 9) Diffie, W. and Hellman, M.: New directions in cryptography, IEEE Trans Information Theory, IT-22 (Nov. 1976).
- 10) Matyas, S. M.: Digital signature—an overview, Computer Network, Vol. 3 (1979).
- 11) 土居範久, 広瀬 健, 西村恕彦: 公衆暗号系, 情報処理, Vol. 22, No. 1 (Jan. 1981).
- 12) 土居範久, 広瀬 健, 一松 信, 西村和夫: 公衆暗号系の実現可能性と問題点, 情報処理, Vol. 22, No. 1 (Jan. 1981).
- 13) 田中善一郎: コンピュータ犯罪に対する暗号の有効性を探る, 日経エレクトロニクス, 1982年10月11日号.
- 14) Rivest, R., Shamir, A. and Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems, CACM, Vol. 21, No. 2 (1978).
- 15) Merkle, R. and Hellman, M.: Hiding information and receipts in trapdoor knapsacks, IEEE Trans. on Information Theory, IT-24 (1978).
- 16) Rabin, M. O.: Digitalized signatures and public-key functions as intractable as factorization, Tech. Rep. MIT/LCS/TR-212 MIT Lab. Comput. Sci. (1979).
- 17) Shamir, A.: A fast signature scheme, Tech. Rep. MIT/LCS/TM-107, MIT Lab. Comput. Sci. (1978).
- 18) 小山謙二: RSA 公開鍵暗号法のマスター鍵, 信学論 (D), J 65-D, No. 2 (1982).
- 19) 小山謙二: マスター鍵による同報通信の暗号方式, 信学論 (D), J 65-D, No. 9 (1982).
- 20) Test Key, document no. ISO/TC 68/SC 2/WG 2 N 80, ISO (Jan. 1982).
- 21) PeMillo, R. A. et al.: Foundations of secure computation, Academic Press (1978).
- 22) Meijer, H. and Akl, S. G.: Digital signature schemes for computer communication network, Proceedings of the 7th Data Communications, Sympo. (Oct. 1981).
- 23) Akl, S. G.: Digital signatures with blindfolded arbitrators who cannot form alliances, IEEE Symposium on Security and Privacy (Apr. 1982).
- 24) Popek, G. J. and Kline, C. S.: Encryption and secure computer networks, Computing Surveys Vol. 11, No. 4 (Dec. 1979).
- 25) Saltzer, J.: On digital signature ACM. Operating System Review, Vol. 12, No. 2 (Apr. 1978).
- 26) Davis, D. W. and Price, W. L.: The application of digital signatures based on public-key crypto-systems, Proc. of the 5th International Conference on Computer Communication (Oct. 1980).
- 27) Cushman, R. H.: Technology update: Data encryption chips provide security—or is it false security?, EDN, 17 (Feb. 1982).
- 28) 北原安定: 高度情報化社会へ向けての課題, 信学誌, Vol. 65, No. 7 (1982).

(昭和58年2月25日受付)

