平成１５年１０月２日

電 子 署 名 法 概 説

弁護士　藤　　本　　博　　史

第１　背景及び技術論

１，インターネット上の通信メッセージの偽造変造の容易性

インターネット上の通信メッセージは，

（１）当該通信メッセージの発信者へのなりすましが容易である。

（２）当該通信メッセージの改ざんが容易である。

という性質を有する（添付資料ＣＤ「振興事業」フォルダー参照[*1]）。

２，前項の偽造変造を防止するために各種の暗号技術が用いられることがある。

暗号技術は，現在，大まかに分類すると次の二種がある。

共通鍵暗号方式と公開鍵暗号方式

（１）共通鍵暗号方式（「*PKI* 解説」内「共通鍵暗号方式」参照）

暗号化と復号に同じ鍵（解読規則と鍵と呼ばれるデータ〝ビット列〟）を用いる暗号方式を共通鍵暗号方式と呼ぶ。秘密鍵暗号の原理は比較的単純で，基本的には換字（字面の順を変える）と置換（文字を別の文字に置き換える）を組み合わせである。

共通鍵方式は公開鍵方式と比較すると鍵そのものをどうやって相手方に安全に送るかという難点がある。また，通信相手の数だけ鍵を保有しなくてはならないので，大勢を相手とする場合には適しない。

（２）公開鍵暗号方式（概説は添付資料２「公開鍵暗号「ＲＳＡ暗号」」，詳細は資料３[*2]　「ＲＳＡ暗号方式の基礎編，同応用編」参照）

共通鍵暗号方式とは異なり，対になっているふたつの鍵を用いる方式

対になっている鍵の一方を秘密鍵（秘密とは鍵の保有者のみが秘匿しているべきという意味），他方を公開鍵（対世的に公開しておくべき鍵という意味）と言うが，片方の鍵（Ａの鍵，秘密鍵）で暗号化した情報はもう片方の鍵（Ｂの鍵，公開鍵）でないと復号できないという性質を持っている。

すなわち，公開鍵で復号できた情報は必ずその対になった秘密鍵で暗号化されているということができるので，情報出所の確からしさ（秘密鍵の持ち主から来た情報だ）の確認と改ざんの恐れを防止することができる。

但し，公開鍵で復号できる情報のままでは情報の内容は秘密にできないから，情報を送

---

1 情報処理振興事業協会セキュリティセンター作成　*PKI* 関連技術解説（以下「*PKI* 解説」と言う）

2 ベリサイン社（*RSA* 製品の発売元）のサイト情報

るべき相手方の公開鍵で更にこの暗号情報を暗号化すれば，相手方を除きこの情報を正しく復号化できるものはいないから内容の秘密も保てることになる。

なお，公開鍵方式にはいくつかの種類があるが最も有名なのがＲＳＡ方式で，大きな整数の素因数分解が困難であるという仮定に基づいて鍵を作成するところに特徴がある。

なお，ＲＳＡを典型とする公開鍵暗号方式はロジックが比較的複雑なので，暗号化の計算時間は秘密鍵暗号と比べて長くかかるという問題がある。

３，電子署名(添付資料４[*3]　詳しくは資料３「４．３ＲＳＡ署名方式」)

電子署名とは，この公開鍵暗号方式とセキュアハッシュ関数を利用した技術で，メッセージ（及び電子署名）の改ざんを検出する技術である。

（前述のとおり公開鍵暗号方式は復号化に時間を要したりするので）送信情報全体について暗号化する必要（解読不能とする必要）がないけれども，送信情報の偽造変造を防止をしようとする場合に用いられる技術である。

セキュアハッシュ関数（「*PKI* 解説」内「２．３セキュアハッシュ関数」参照）は、以下のような性質を有する可変長の入力データから固定長（*20* バイト程度）のビット列を出力（出力されたビット長をダイジェストと言う）するもの（プログラム関数）である。

(*1*)　入力データの長さが異なっても、決められた長さのダイジェストを出力する。

(*2*)　入力メッセージが少しでも異なっていれば、出力されるダイジェストは大きく異なる。

(*3*)　ダイジェストから元のメッセージを算出することができない。

(*4*)　同じダイジェストを出力する *2* つの入力データを見つけるのが困難である。

セキュアハッシュ関数にも，いろいろ種類があるが，現在，よく利用されているのがＳＨＡ－１方式[*4]である。

電子署名は，この公開鍵暗号方式とセキュアハッシュ関数を次のように利用する。

デジタル署名の生成は次のとおり。

(*1*)　署名したいメッセージから、ハッシュ関数を使ってダイジェストを生成する。

(*2*)　生成したダイジェストを自分の秘密鍵で暗号化する。

(*3*)　メッセージと生成した署名を受信者に送信する。

デジタル署名付の情報の受信者の検証は，次のとおり。

(*4*)　受信したメッセージから、ハッシュ関数を使ってダイジェストを生成する。

(*5*)　受信したデジタル署名を、デジタル署名の生成者の公開鍵を使って復号する。

3　同資料脚注記載の個人のサイト情報

4　詳しくは添付のＣＤ媒体中「ハッシュ」フォルダー内のファイル参照

(6)（4）において生成したダイジェストと（5）で復号したダイジェストを比較し、完全に一致するかどうかを確認することによって，メッセージとデジタル署名の改変を判別することができる。

第２　法律論（制度論）

１，電子署名の法制度化

インターネットを利用した取引や各種公的機関への申請を電子署名によって行うには，当該電子署名者が実存し，かつ，特定の者（法主体）であることが公証される必要があるから，上記に述べた電子署名の「技術」は不可欠であるが，電子署名の技術だけでは足りないものがある。

それは特定の法的主体の実在性とその者と公開鍵の結びつきをどう確保する（公証する）かである。公開鍵暗号方式という技術は，秘密鍵で暗号化した情報は公開鍵でないと復号できないというものに過ぎなく，ある公開鍵が特定の法的主体のものであること（及びその実在性）を保障するものではない。この結びつき等を確保して初めて上記の目的を完成させることができる。この結びつきを確保するのが認証と呼ばれている制度である。

２，認証制度

現在，日本においては電子認証制度がいくつかの法制度に跨って定められていることもあって，我が国には認証機関には様々なものがあり，認証制度にも偏差がある。

（１）電子認証の根拠法（添付資料９）

あ　電子署名及び認証業務に関する法律

い　商業登記に基づく電子認証制度（商業登記法）

う　電子署名に係る地方公共団体の認証業務に関する法律

（２）電子署名及び認証業務に関する法律（添付資料５）

これは主務大臣の認定を受けた民間の認証機関が特定の個人（自然人）の公開鍵について電子証明書を発行する制度である。

（３）商業登記に基づく電子認証制度（商業登記法）（添付ＣＤ「法人の場合」フォルダー参照[*5]）

商業登記に基づく電子認証制度は，電子的な取引社会において用いられる証明として，法人の登記情報に基づいて電子認証登記所が「電子証明書」を発行するものである。電子的な取引社会における登記所が発行する「印鑑証明書・資格証明書」の代わりになるものである。

---

*5 法務省サイト

（４）電子署名に係る地方公共団体の認証業務に関する法律

都道府県知事が，住民基本台帳に記録されている者に対し電子証明書を発行する制度である。

（５）電子認証の制度上の問題点

以上３者については，それぞれ棲み分けがされていて（法文上は棲み分けが分かり辛い），（２）は自然人専用，（３）は法人専用，（３）は自然人専用であるがその発行された電子証明書は国，地方公共団体に対する各種申請（及び（１）の認証機関への登録申請）の際に用いられるものであるが，世界的にみて電子認証に関する法体系としては分かり辛く特異なものとされている（添付資料７）。

電子認証全体の信頼性は最もセキュリティについて脆弱な認証機関のレベルまで下落する危険性があると言われていて，認証機関の利用者の本人確認の方法を含めセキュリティに対するレベルが問題となる。

（６）利用者が認証機関に登録（又は証明申請）する場合の本人確認の方法

あ）電子署名及び認証業務に関する法律

一　住民票の写し、戸籍の謄抄本、外国人登録法に規定する登録原票記載事項証明書又はこれらに準ずるものの提出と以下のいずれかの文書

二　旅券、官公庁が発行した免許証、許可証若しくは資格証明書等、外国人登録法外国人登録証明書、住民基本台帳法に規定する住民基本台帳カード，官公庁又は独立行政法人及び特殊法人がその職員に対して発行した身分を証明するに足りる文書で当該職員の写真をはり付けたもののうちいずれか一以上の提示を求める方法

三　利用の申込書に押印した印鑑に係る印鑑登録証明書の提出を求める方法

四　郵便による確認（省略）

五　その他主務大臣が認めるもの

い）商業登記に基づく電子認証制度（商業登記法）

登録印鑑の申請書への押捺

う）電子署名に係る地方公共団体の認証業務に関する法律

総務省令に定めるところによる（未制定か）

（７）電子署名の応用による電子文書の公証制度

公証人による電子文書に対する公証制度（公証人法）（添付資料８[*6]）

あ）私書証書の認証（文書の真正を更に強めるというものだろう）

い）確定日付の付与

---

6 法務省サイト

う）情報の同一性に関する証明

え）同一の情報の提供

３，裁判実務上電子認証のされた文書の真正が法的に問題とされた場合のいくつか

（１）秘密鍵の保管方法の適否，漏洩の有無

なお，秘密鍵は，ＩＣカード等に格納されて外部からは読出しやコピーが不能となるような措置（将来的には生物学的認証も取り入れたカードになることが予想される）が講ぜられるのが一般になるだろう（添付ＣＤ内 *PKI* 解説「*3.4.2* 秘密鍵のセキュリティ」）。

（２）認証機関への成りすまし登録の可能性

（３）電子署名のある文書の真正の立証方法

（４）認証期間，登録資料保存期間

４，参考資料

辛島　睦　　電子署名法概説　　自由と正義２００１年５月号１４頁

木村　敬　　電子署名に係る地方公共団体の認証業務に関する法律

ジュリスト No1242　２５頁

松本　恒雄　電子署名・認証法の課題

法とコンピュータ No20 July 2002　２１頁

情報処理振興事業協会　　*http://www.ipa.go.jp/security/pki/index.htm* 以下参照