インターネット官報データ提供サービスにおけるディジタル証拠性の保証

梅澤 淳子[†,††] 上野 裕之[††] 宮田 幸夫[††]
佐井川 泰治[††] 江並 孝之[††]
吉岡 克成[†] 松本 勉[†]

1999 年 11 月以来，国立印刷局はインターネットを通して官報ディジタルデータを提供している．官報ディジタルデータには，(1) 記事内容が改変されていないことが確認できること，(2) 製造者が確認できること，(3) 閲覧方法が至便であること，という要件がある．これらの要件を実現させるために，国立印刷局は 2003 年 7 月に官報ディジタルデータに，ディジタル署名とタイムスタンプの適用を開始した．また，多くの国がインターネットを通して官報ディジタルデータをはじめとした電子文書を提供している．しかしながら，我々が知っている限り今回の事例が，法令の公布に用いられる重要な文書である官報のディジタルデータに対してディジタル署名とタイムスタンプを使う初めての例である．この論文では，それぞれのセキュリティ技術が現行の官報データ提供サービスでどのように適用されているかを概説し，また，それによって達成できることについて議論する☆．

Digital Evidence Enhancement for the Japanese Official Gazette Data Providing Services

Atsuko Umezawa,[†,††] Hiroyuki Ueno,[††] Yukio Miyata,[††]
Yasuharu Saikawa,[††] Takayuki Enami,[††] Katsunari Yoshioka[†]
and Tsutomu Matsumoto[†]

Since November 1999 the National Printing Bureau of Japan has been providing the Japanese Official Gazette digital data via the Internet. The Official Gazette digital data has the following requirements: (1) the integrity of the data is verifiable, (2) the manufacturer should be identifiable, and (3) viewing should be convenient. In order to fulfill these requirements, the National Printing Bureau started adopting digital signature and time stamping schemes to the Official Gazette digital data in July 2003. Many countries have also been providing their documents data via the Internet. However, as far as we know, it is the first example of employing digital signature and time stamp to the Official Gazette digital data, which are important official documents used for proclamation of statutes to take a simple example. This paper outlines how individual security technologies are applied in the current version of the Official Gazette Data Providing Services and also discusses their achievements.

1. はじめに

近年，電子署名および認証業務に関する法律（電子署名法）や書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律（IT 書面一括法）の施行により，電子文書を紙文書と同等に扱うことが認められる場面が増えている．また，様々な取引や手続を電子文書により行うために，電子データのセキュリティ確保が求められている．

あわせて，行政機関への様々な届出・申請手続をインターネット上で行えるよう，平成 14（2002）年度内には政府認証基盤の各府省認証局が整備され，2004 年 2 月から名古屋国税局管内で，2004 年 6 月からは全国で電子申告・納税システムの運用が開始される等，すでに一部の手続は電子的に実行可能になっている．

一方，多くの省庁・自治体が情報公開等の目的で

† 横浜国立大学大学院環境情報研究院
Graduate School of Environment and Information Sciences, Yokohama National University
†† 独立行政法人国立印刷局
National Printing Bureau, Incorporated Administrative Agency, Japan

☆ 本稿は，文献 1) の内容を含み，さらに充実させたものである．

Web サイトに電子文書を公開しているが，個々の文書については改ざんやなりすましへの対策が施されていないというのが現状である．

本稿では，国が発行する機関紙である官報について，紙面の印刷物の頒布に加えて 1999 年から実施している，インターネットを通じた電子データの提供について述べ，提供する電子データのセキュリティを高めるため，平成 15（2003）年 7 月よりディジタル署名およびタイムスタンプ方式の適用を開始した事例について報告する．

本稿の構成は以下のとおりである：2 章では，従来の紙の官報について説明する．3 章では，従来版の官報データ提供サービスについて述べる．4 章では，官報が満たす性質と官報ディジタルデータの要件について説明する．5 章では，従来版の官報データ提供サービスのセキュリティについて考察する．6 章では，官報ディジタルデータのディジタル証拠性の保証について説明する．7 章では，官報データへのディジタル署名とタイムスタンプの適用について詳説する．8 章では，ディジタル署名とタイムスタンプの適用の有効性と，他国における官報データ提供サービスとの比較について論じる．

2. 官報について

官報[2] は，法律，政令，条約等の公布をはじめとして，国の機関の諸報告や資料を公表する「国の広報紙」「国民の公告紙」としての使命を持ち，さらに，法令の規定に基づく各種の公告を掲載する等，国が発行する機関紙として重要な役割を果たしている．官報の編集および印刷は，国立印刷局[3] が行っている．

「法令の公布」とは，憲法，詔書，法律，政令，条約，省令，告示等の成立した成文の法を公表して，一般国民が知ることのできる状態に置くことをいう．法令が現実に拘束力を発生するためには，一般に公布の用件を満たすことが必要とされている．大日本帝国憲法下では，明治 40（1907）年の公式令第一二条により，法令の公布は官報によって行うことが明確に定められていた．だが，日本国憲法下では公式令が廃止され，現行法上このような一般規定はない．しかし，他に適当な公布の方法や媒体がないため，従来と同じように法令の公布は官報によって行うことが最高裁判所の判例（最高裁昭和 32（1957）年 12 月 28 日大法廷判決）で是認されている[4),5)]．

また，「広報」として，国会事項，人事異動，叙位，叙勲，褒章，皇室事項，官庁報告（国家試験，公聴会，地価公示等）および資料（閣議決定事項，国際収支状況等）等を掲載して，広く国民に公表している．

図 1 官報紙面イメージ
Fig. 1 The Official Gazette.

さらに，官報には様々な「公告」が掲載される．公告とは，ある事項を一般に知らせること等をいい，掲載される公告には，

- WTO に基づく政府調達
- 押収物還付，国有財産売払等（官庁の公告）
- 日本銀行営業毎旬報告等（特殊法人の公告）
- 公債抽選，行旅死亡人等（地方公共団体の公告）
- 破産，会社更生関係等（裁判所の公告）
- 合併公告，決算公告等（会社の公告）

等がある．

官報の体裁は，日本工業規格 A4 判の紙面，第 1 ページ右上に題字，各ページに日付，号数，種別（本紙，号外，特別号外，資料版等の区別）をヘッダとして記載，段組形式，8 ポイント活字，というような形式の冊子体とされている（**図 1**）．

官報の種類には，毎日発行される本紙，本紙に掲載しきれない記事がある場合に必要に応じて発行される号外，政府調達公告を掲載する政府調達版，緊急を要する記事を掲載するために発行される特別号外，週に一度発行される資料版，月に一度発行される官報目録がある．

3. 従来の官報データ提供サービス

本章では，従来の官報データ提供サービスの概要，データ形式，個々のサービス内容について説明する．

3.1 概　　要

国立印刷局では，従来より官報紙面の編集および印刷を行っているが，加えて，近年電子情報に関する技

術および機器が急速に進展し，インターネットによる官報の閲覧に対する国民のニーズの高まり等をふまえ，官報紙面の補完的な役割を担うものとして，1999年11月より，インターネットでのデータ提供（インターネット版『官報』[6]）を開始した．さらに2001年9月より，データ収録期間を広げ，検索を可能にして利便性を向上したサービス（官報情報検索サービス[7]・有料会員制）を開始した．以下，本稿では，インターネット版『官報』をサービスB（Basic service：基本版官報データ提供サービス），官報情報検索サービスをサービスA（Advanced service：拡張版官報データ提供サービス）と呼ぶ．

3.2 提供データ形式

サービスBで提供するデータ形式は，ページ単位PDF（Portable Document Format）データである．ページ単位PDFデータとは，官報データの各ページをPDFファイルとして作成したものである．サービスBのデータベースには直近1週間以内のページ単位PDFデータが収録されている．

サービスAで提供するデータ形式は，ページ単位PDFデータ，記事単位PDFデータ，記事単位HTMLデータ，ページ単位JPEGデータである．記事単位PDF/HTMLデータとは，官報データの各記事をPDF/HTMLファイルとして作成したものである．ページ単位JPEGデータとは，官報を1ページごとにスキャナで読み込み，JPEG形式で保存したものである．サービスAのデータベースには1947年5月3日から当日分までの官報データが収録されている．データの日付によって形式が異なっており，記事単位HTMLデータはすべての期間において収録されているが，ページ単位JPEGデータは1947年5月3日〜1999年3月31日，ページ単位/記事単位PDFデータは1999年4月1日〜当日の期間収録されている．

両サービスで共通するデータ形式は，PDFである．PDFは，官報のような縦書・段組の複雑な文書を体裁どおりに表示することができ，またアドビシステムズ株式会社から無償で提供されるAcrobat Readerを利用することにより，様々なプラットフォームで閲覧できる．

3.3 サービス内容

サービスBでは，利用者は1週間以内に発行された官報のページ単位PDFデータを閲覧できる．閲覧したいページを探すためには，まず日付と官報種別（本紙，号外等）を選択し，その官報の目次を表示する．目次から，閲覧したい記事が掲載されているページを選択する．

サービスAでは，利用者は，日付検索と記事検索の2種類の検索方法が利用できる．日付検索では，サービスBのように日付と官報種別を指定し，表示される目次から閲覧したい記事を探し，その記事を表示する．記事検索では，日付，官報種別，記事種別，キーワード等を指定し，条件に合った記事を表示する．検索した官報データの表示方法は，テキスト表示とイメージ表示の2種類がある．日付検索・記事検索ともにテキスト表示では記事単位HTMLを表示する．1999年3月31日以前の日付を指定した場合，日付検索・記事検索ともにイメージ表示ではページ単位JPEGデータを表示する．1999年4月1日以降の日付を指定した場合，日付検索のイメージ表示ではページ単位PDFデータを表示し，記事検索のイメージ表示では記事単位PDFデータを表示する．

この論文では,「官報」という場合は紙の官報を指し,「官報データ」という場合は紙の官報の内容を電子データ化したもののことを指す．さらに,「官報データ」とは，ページ単位PDFデータ，記事単位PDFデータ，記事単位HTMLデータ，ページ単位JPEGデータを指すものとし，サービスBで表示される目次データや，両サービスにおける案内画面・ログイン画面等のHTMLデータを含まない．

通信時のサーバ認証は，サービスBでは行っていないが，サービスAでは日本ベリサイン株式会社発行によるサーバ証明書を取得しており，サーバ認証を行っている．サービスAでは，ユーザIDとパスワードを用いてユーザ認証を行っている．

表1に，サービスBとサービスAの内容を比較したものを示す．

4. 官報と官報データの性質

本章では，官報の性質と官報データの要件について述べる．

4.1 官　　報

2章で述べたように，官報は，法令の公布，広報および公告という2つの大きな役割を担っている．法令の公布という観点では，法令の内容を正確に国民に伝達する必要がある．広報および公告という観点では，合併公告，資本減少公告等の公告は，会社の合併による変更の登記申請，金融機関の合併や分割の認可申請等を行う際に添付書類として提出を求められることもあるため，偽造品でないことが必要である．また，官報に掲載される内容は社会生活に大きな影響を及ぼすものが多く，国民が必要なときに手軽に閲覧できることが望ましい．

表 1 官報データ提供サービス
Table 1 The Official Gazette Data Providing Services.

	サービス B	サービス A
収録期間	直近 1 週間	1947.5.3〜当日
データの種類	ページ単位 PDF	記事単位 HTML(全期間)，ページ単位 JPEG(1947.5.3〜1999.3.31)，ページ単位／記事単位 PDF(1999.4.1〜当日)
利用対象	インターネット利用可能な人全て	契約会員のみ
利用方法	目次から希望記事の掲載ページを探す 印刷・テキスト選択は不可	日付，官報種別，記事種別，キーワード検索 検索した記事を印刷可能
ユーザ認証	なし	ユーザ ID とパスワードによる認証
サーバ認証	なし	サーバ証明書による検証可

以上のことをふまえ，官報は次の性質を満たしているといえる．

(1) 記事内容が改変されていないことが確認できること
(2) 製造者が確認できること
(3) 閲覧方法が至便であること

4.2 官報データ

官報データをインターネット配信することで，目的の記事へ容易にアクセスできるようになり，4.1 節で述べた官報の性質 (3) の点で利便性が大きく向上している．一方，紙文書に比べ，ディジタルデータは複写および改ざんを容易に行うことができ，その痕跡が残りにくいため，官報データが性質 (1) と (2) を満たしているかどうかを考慮する必要がある．我々は，従来版の官報データは性質 (1) と (2) を十分満たしているとはいえないと考える．詳細については，5 章で説明する．

5. 従来版サービスの情報セキュリティの検討

本章では，サービス B・サービス A の情報セキュリティについて述べる．

インターネットで官報データを配信することにより，特に紙の輸送に時間を要する地域において，紙の官報よりも迅速な提供が可能になる．しかし，ネットワークは必ずしも安全なものではなく，盗聴，不正アクセス，なりすまし，改ざん，否認等の様々な脅威が存在する[8]．

第 1 に，従来のサービス B とサービス A で提供している官報ディジタルデータの PDF ファイルは，作成時にマスタパスワードを設定し，PDF の文書セキュリティ設定で文書の変更等を不可にしている．したがって，ページ単位 PDF データと記事単位 PDF データは，内容の改ざんはできない．しかし，攻撃者によりマスタパスワードが破られれば，内容が改ざんされてしまい，そのことを検知することはできない．したがって，従来のサービスで提供されている官報データは，4.1 節で述べた性質 (1) を十分に満たしているとはいえない．

第 2 に，従来のサービス B ではサーバ認証を行っていないため，利用者は官報データを本当に国立印刷局のサーバからダウンロードしているのかどうかを確認することができない．サービス A では，利用者は日本ベリサイン株式会社発行のサーバ証明書により，配信サーバの確認ができる．しかし，利用者が国立印刷局でない他者から入手した官報データについて確認したいというような場合には，問題が生じる．確認するためには，利用者は国立印刷局の配信サーバにアクセスしてオリジナルの官報データをダウンロードし，所有しているデータと比較する，もしくは別途紙の官報を入手して比較する等，確認を行う時点で何らかの問合せ行為が必要となり，煩雑さをともなう．したがって，サービス B・サービス A で提供されている官報データは，4.1 節で述べた性質 (2) を十分に満たしているとはいえない．

6. 官報データの証拠性の強化

ディジタル証拠性とは，誰がいつどこでどんなデータを作成したかを，事後的に検証できる性質と定義する．ディジタル証拠性が達成されているシステムから提供されるデータは，4.1 節で述べた性質 (1) 記事内容が改変されていないことが確認できること，(2) 製造者が確認できること，を満たしているといえる．

ディジタル証拠性を達成する技術として，ディジタル署名とタイムスタンプがあげられる．ディジタル署

名とは，公開鍵暗号方式の応用によって，データの作成者証明と，データの一貫性証明を可能にする技術である．タイムスタンプとは，データの存在証明と，データの一貫性証明を可能にする技術である．ディジタル署名とタイムスタンプのメカニズムについては，付録 1 と付録 2 に示す概要を参照されたい．

データの作成者証明とは，そのデータを誰が作成したのかを第三者に証明することである．データの存在証明とは，タイムスタンプによって示される時刻にデータが存在していたことを第三者に証明することである．データの一貫性証明とは，ディジタル署名もしくはタイムスタンプ適用後に，そのデータが改ざんされていないことを第三者に証明することである．

2003 年 7 月より，国立印刷局は官報データ提供サービスで配信しているページ単位 PDF データにディジタル署名とタイムスタンプの適用を開始した．

体裁を含めた内容が官報紙面と同一であるのはページ単位 PDF のみであるという考え方に基づき，ページ単位 PDF にのみ証拠性の強化を行っている．記事単位 HTML テキスト，記事単位 PDF については，記事ごとに分割されているため，官報紙面と同じ体裁であるとはいえない．

ディジタル署名の適用により，官報データの作成者証明と，一貫性証明を行うことができ，官報データは性質 (1) と (2) を満たすことができる．

ディジタル署名の適用により，官報データは新たに以下のような特徴を持つ：

- 利用者が直接国立印刷局のサーバからダウンロードした官報データでなくても，データの一貫性が検証できる．
- 検証手順が簡単である．

タイムスタンプを適用することにより，タイムスタンプの示している信頼できる時刻に，その官報データが存在していたことが確認できる．官報データへのディジタル署名とタイムスタンプは，発行日に 1 ページずつ連続処理を行って生成･付与するという運用を行うこととする．Adobe Acrobat で，官報データ PDF ファイルを開き，ディジタル署名 → タイムスタンプの順に生成・付与し，官報データ PDF ファイルを閉じる，という動作を連続して行う．この処理に要している時間は，1 ファイルあたり約 5.5 秒（実測値）である．タイムスタンプは遡った日付・時刻で発行することができないので，ある 1 ページの官報データのタイムスタンプが示す時刻を，そのデータの前後に処理を行ったページの官報データのタイムスタンプが示す時刻と比較し，その時刻差が，ディジタル署名とタイムスタンプ生成・付与の連続処理を行うための所要時間の範囲内であれば，官報データ作成の運用状況を第三者が事後的に確認することができるといえる．加えて，外部のタイムスタンプ局のような第三者を介入させることにより，内部不正が困難になりシステムの信頼性が高まる．

また，タイムスタンプにより，タイムスタンプの示す信頼できる時刻以降の官報データの一貫性を検証できる．

さらに，ディジタル署名に加えてタイムスタンプを適用することにより，ディジタル署名の有効期限が切れてしまった場合でも，タイムスタンプの検証が可能であれば，データの一貫性を検証できる手段が増える．

7. ディジタル署名とタイムスタンプにより証拠性を高めた官報データ提供サービス

本章では，ディジタル証拠性保証のための，官報データへのディジタル署名とタイムスタンプの適用について述べる．

7.1 サービス概要

6 章で述べたように，ページ単位 PDF データにのみディジタル署名とタイムスタンプを適用した．サービス B では，ディジタル署名を生成し，ページ単位 PDF データに埋め込む．サービス A では，ディジタル署名とタイムスタンプを生成し，ページ単位 PDF データに埋め込む．以下，ディジタル署名を適用したインターネット版『官報』をサービス B-S（Basic service with digital Signature：ディジタル署名付基本版官報データ提供サービス），ディジタル署名とタイムスタンプを適用した官報情報検索サービスをサービス A-ST（Advanced service with digital Signature and Time stamp：ディジタル署名・タイムスタンプ付拡張版官報データ提供サービス）と呼ぶ．サービス B-S では 2003 年 7 月 15 日以降の日付のページ単位 PDF データにディジタル署名が適用されており，一方，サービス A-ST では 2003 年 7 月 15 日以降の日付のページ単位 PDF データにディジタル署名とタイムスタンプの両方が適用されている．**表 2** に，ディジ

表 2 ページ単位 PDF データへのディジタル署名とタイムスタンプの適用期間
Table 2 Applicable periods of digital signature and time stamp for the paginal PDF data.

	サービス B-S	サービス A-ST
データ提供期間	直近 1 週間	1999.4.1 付-当日付
ディジタル署名適用期間	2003.7.15 付-当日付	2003.7.15 付-当日付
タイムスタンプ適用期間	なし	2003.7.15 付-当日付

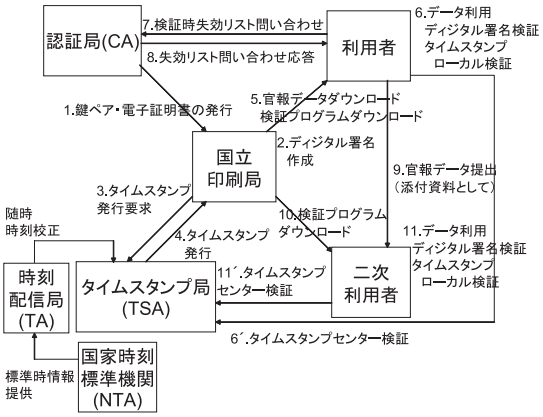

図 2 サービス A-ST システムの概要
Fig. 2 Outline of Official Gazette Data Providing Services with digital signature and time stamp.

タル署名とタイムスタンプの適用期間を示す．

図 2 にサービス A-ST のシステムについて示す．まず認証局が国立印刷局に対し，鍵ペアと電子証明書を発行する．電子証明書は，ディジタル署名を検証するために必要な公開鍵とその所有者を証明するもので，署名者の情報と署名者の公開鍵に，認証局のディジタル署名が付与されている．国立印刷局は発行された秘密鍵を用いて官報データにディジタル署名をした後，タイムスタンプ局にタイムスタンプ発行要求をする．タイムスタンプ局はタイムスタンプを発行し，国立印刷局に送り返す．タイムスタンプ局は，時刻配信局から随時時刻校正を受けている．時刻配信局は，国家時刻標準機関から標準時情報の提供を受けている．

データの利用者は，国立印刷局からディジタル署名とタイムスタンプ付データをダウンロードする．利用者はディジタル署名とタイムスタンプの検証を行うことができる．利用者はディジタル署名検証用プログラムとタイムスタンプ検証用プログラムを国立印刷局からダウンロードし，インストールする．ディジタル署名検証時に，利用者は認証局のリポジトリに証明書失効リストの問合せを行う．タイムスタンプの検証は基本的に利用者のパソコン内で行うが，タイムスタンプ作成ソフトのユーザはタイムスタンプ局に問合せを行うセンター検証を行うこともできる．将来，利用者がダウンロードした官報データは，添付資料として二次利用者に提出されるという利用法も考えられる．そのような場合にも，二次利用者は検証用プログラムを国立印刷局からダウンロードし，ディジタル署名とタイムスタンプの検証を行うことができる．

7.2 電子証明書の発行とタイムスタンプ局

7.1 節で述べたサービスを実現するために，以下の 2 つのサービス提供者を選択した：

- ディジタル署名生成のための鍵と電子証明書を発行する認証局（CA：Certification Authority）
- タイムスタンプ生成と検証のためのタイムスタンプ局（TSA：Time Stamp Authority）

CA としては，日本認証サービス株式会社（以下，JCSI）の「SecureSign パブリックサービス」[9] を利用することとした．TSA としては，検討時に国内で利用可能であったアマノ株式会社（以下，アマノ）の「デジタルタイムスタンプサービス」[10]，セイコーインスツルメンツ株式会社の「Chronotrust」[11]，株式会社 NTT データの「SecureSeal」[12] の 3 つのサービスのうち，「デジタルタイムスタンプサービス」を利用することとした．宇根らによる可用性および安全性の観点からみたタイムスタンプ方式の評価[13] によると，上述の 3 つのタイムスタンプサービスのうち，Chronotrust やデジタルタイムスタンプサービスが含まれる方式群の方が，SecureSeal が含まれる方式群よりも安全性上望ましいとされている．その理由は，ローカル環境での検証手続に起因している．Chronotrust やデジタルタイムスタンプサービスが含まれる方式群（個別型方式 I）では，タイムスタンプの検証者が，他のエンティティから検証に用いるデータを入手できない場合でも，ハッシュ値の比較とディジタル署名の検証という既定の検証処理を実行することができるのに対し，SecureSeal が含まれる方式群（連鎖型方式 L）では，タイムスタンプの検証者が，他のエンティティから検証に用いるデータを入手できない場合，実行可能な検証処理がハッシュ値の比較のみとなってしまう．しかし，データを改ざんし，そのハッシュ値を元のハッシュ値と置き換えることは攻撃者にとって容易であるので，こちらの方式群では，ローカル環境での検証は十分なものではなく，データの一貫性を検証するためには TSA の存在が不可欠となる．

サービス B-S・サービス A-ST では，PDF ファイルとの親和性，サービス運用実績，TSA 構築・運営のコスト等を勘案し，SecureSign パブリックサービスとデジタルタイムスタンプサービスを採用した．

7.3 ディジタル署名

PDF ファイルにディジタル署名をする方法を**図 3** に，有効性検証方法を**図 4** に示す．

署名は国立印刷局内に設置された署名サーバで行う．まず，JCSI により事前に発行された電子証明書を PDF データに付加する．電子証明書には，公開鍵自体が含まれている．次に，Acrobat のセキュリティ設定で PDF データの暗号化とファイル内容変更不可

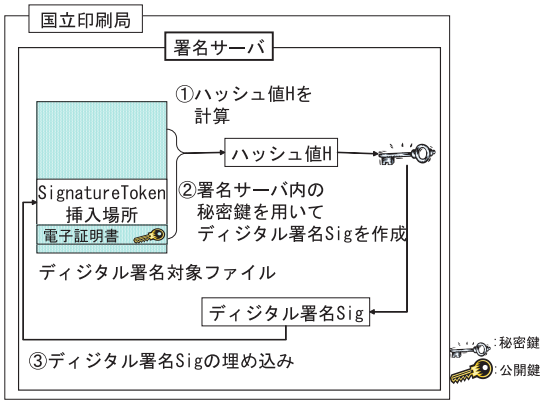

図 3 ディジタル署名の付与
Fig. 3 Embedding of digital signature.

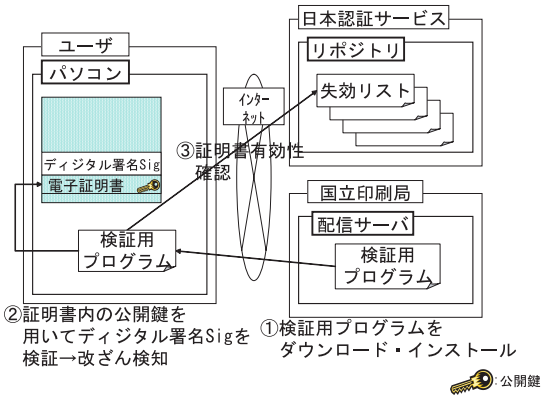

図 4 ディジタル署名の検証
Fig. 4 Verification of digital signature.

等の設定をする．電子証明書の付加と Acrobat のセキュリティ設定の後に，署名対象ファイルのハッシュ値 H を計算する．ハッシュ対象となる部分は，作成されたディジタル署名 Sig を埋め込む領域を除いた部分すべて（図 3 の網掛け部分）である．ファイル内のハッシュする領域は，PDF の署名フィールドと呼ばれる項目の中で指定される．ハッシュ値 H と，JCSI により発行され，署名サーバ内にセットされた官職署名用の秘密鍵を用いて，ディジタル署名 Sig を作成する．作成されたディジタル署名は対象ファイルの署名挿入場所（対象ファイル白抜き部分）に署名トークンとして埋め込まれる．

署名検証を行う際には，まず，ユーザは国立印刷局の配信サーバからインターネットを通じて署名検証用プログラムをダウンロードし，官報ディジタルデータを閲覧するパソコンにインストールする．今回の場合，検証用プログラムは，Adobe Acrobat5.05 または Adobe Acrobat Reader5.1 のプラグインである．署名検証動作を行うと，PDF ファイル内の電子証明書に含まれるディジタル署名検証用公開鍵を用いて，ディジタル署名 Sig の復号を行い，別途計算した検証対象 PDF ファイルのハッシュ値と比較し，文書が改ざんされていないかどうかを検査する．また，HTTP 通信により JCSI のリポジトリにアクセスし，PDF ファイルに含まれている電子証明書の有効性を確認する．

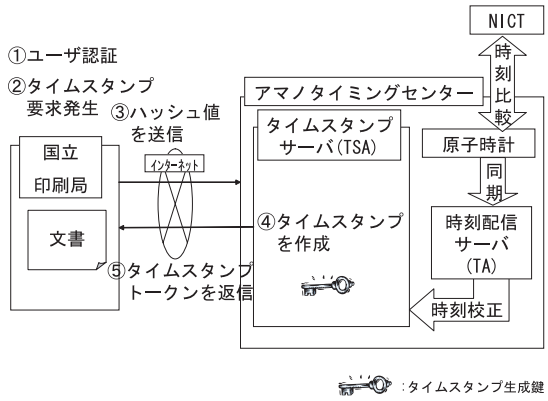

図 5 アマノデジタルタイムスタンプ
Fig. 5 Issuing process of time stamp.

なお，2003 年 7 月に開始したサービス B-S・サービス A-ST では，ハッシュ関数は SHA-1，署名方式は鍵長 1024 ビットの RSA 署名方式を用いている．

7.4 タイムスタンプ

アマノデジタルタイムスタンプ発行の流れを**図 5** に示す．この方式では，タイムスタンプの生成に RSA 署名方式を用いている．

タイムスタンプの発行には，国立印刷局とアマノタイミングセンターの 2 つのエンティティが関わっている．アマノタイミングセンターには，原子時計，タイムスタンプサーバ，時刻配信サーバが設置されている．タイムスタンプサーバ内には，タイムスタンプ生成用の秘密鍵がセットされ，タイムスタンプトークンの生成を行う．すなわち，タイムスタンプサーバはタイムスタンプ局の役割を果たしている．時刻配信サーバは時刻配信局の役割を果たしている．

タイムスタンプサーバの時刻源となる原子時計および時刻配信サーバは，タイムスタンプサービス開始時から 2003 年 12 月 31 日までの間は，NIST（National Institute of Standards and Technology：米国商務省国立標準技術研究所）から遠隔監視・校正を受けており，協定世界時（UTC（NIST））とのトレーサビリティを確保していた．2004 年 1 月 1 日以降は，コモンビュー法を用いて，NICT（National Institute of Information and Communications Technology：独

立行政法人情報通信研究機構）が提供する協定世界時（UTC（NICT））との時刻校正を行い，トレーサビリティを確保している．NICT は，日本で唯一の国家時刻標準機関であり，日本標準時を提供している．NICT とアマノタイミングセンターは，それぞれで保有する原子時計の時刻を GPS 時刻と比較し，時刻比較データを公開することにより，トレーサビリティを確保している．

事前準備として，アマノタイミングセンターではタイムスタンプ発行時の公開鍵暗号通信を行うための公開鍵・秘密鍵ペアを生成し，公開鍵を含めたユーザ固有のライセンスファイルを国立印刷局に渡す．国立印刷局は，受領した公開鍵を用いて，アマノタイミングセンターとの暗号化通信を行う．通信に用いる公開鍵・秘密鍵ペアは 1 年に 1 度更新される．国立印刷局は，アマノタイミングセンターが管理する Web サイトから，更新された公開鍵をダウンロードする．

タイムスタンプ発行の流れを以下に説明する．

〈国立印刷局での処理〉

(1) 国立印刷局はタイムスタンプを押してもらいたい官報データ（すでにディジタル署名済み）のハッシュ値を計算する．

(2) 国立印刷局は共通鍵暗号方式（3DES）の鍵をランダムに生成する．

(3) 国立印刷局は (2) で生成した共通鍵を使って (1) で得たハッシュ値を暗号化する．

(4) 国立印刷局は事前準備においてアマノタイミングセンターから受け取った公開鍵を用いて，(2) で生成した共通鍵を暗号化する．

(5) 国立印刷局は (3)，(4) で得た 2 つの暗号文をアマノタイミングセンターに送る（リクエスト送信）．

〈アマノタイミングセンターでの処理〉

(6) タイミングセンターでは，受信した 2 つの暗号文のうち，(4) で生成した暗号文について自らの持つ秘密鍵で復号し，共通鍵を得る．

(7) (6) で得た共通鍵を用いて，受信した 2 つの暗号文のうち，(3) で生成した暗号文について復号し，ハッシュ値を得る．

(8) このハッシュ値に対するタイムスタンプトークンを生成する．

(9) (8) で得たタイムスタンプトークンを (6) で得た共通鍵を用いて暗号化する．

(10) (9) で得た暗号文を国立印刷局に送る．

〈国立印刷局での処理〉

(11) 国立印刷局は受信した暗号文を，共通鍵を使って復号し，タイムスタンプトークンを得，文書に埋め込む．

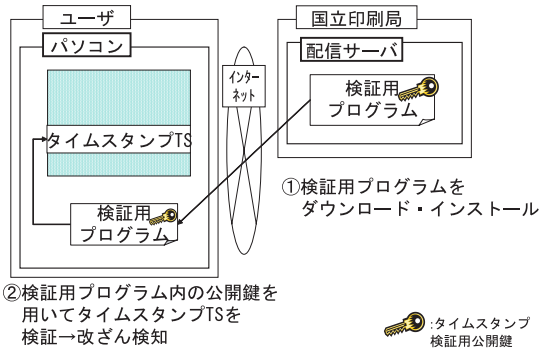

図 6 タイムスタンプの検証（ローカル検証）
Fig. 6 Local verification of time stamp.

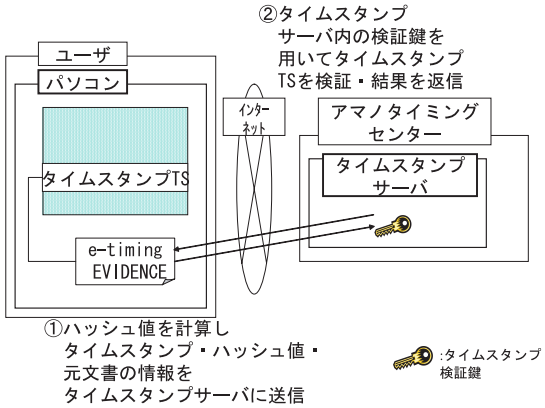

図 7 タイムスタンプの検証（センター検証）
Fig. 7 Central verification of time stamp.

ハッシュ値を送り始めてからタイムスタンプトークンが返送されるまでのターンアラウンド時間は 0.5 秒程度（動作環境により変化）である．また，サービス A-ST で提供する官報データへの適用に関する運用状況から，6 章で述べたとおり，1 つのファイルに対してディジタル署名・タイムスタンプ付与の処理を行うのに要する時間は，連続して処理された 2 つのデータのタイムスタンプが表す時刻差に相当し，実測値で 5〜6 秒程度である．ターンアラウンド時間の動作環境による変化が，連続したディジタル署名・タイムスタンプ生成・付与処理において無視できるほどであれば，連続処理によって生成されたタイムスタンプトークンの表す時刻差には影響を与えないといえる．

アマノデジタルタイムスタンプの検証方法には，ローカル検証とセンター検証がある．ローカル検証の方法を**図 6** に，センター検証の方法を**図 7** に示す．

ローカル検証では，ユーザは国立印刷局の配信サー

バからタイムスタンプ検証用プログラムをダウンロードし，官報ディジタルデータを閲覧するパソコンにインストールする．検証用プログラムは，Adobe Acrobat5.05 または Adobe Acrobat Reader5.1 のプラグインである．検証動作を行うと，プログラム内の検証鍵を用いてタイムスタンプ TS の復号と検証対象 PDF ファイルのハッシュ値の計算を行い，値を比較して文書が改ざんされていないか，時刻情報が有効であるかを検査する．

タイムスタンプ生成用のクライアントソフト製品である「e-timing EVIDENCE for Adobe Acrobat」の利用者は，センター検証を行うことができる．検証動作を行うと，プログラムが検証対象ファイルのハッシュ値を計算し，タイムスタンプ，ハッシュ値等の情報をタイミングセンターに送信する．タイミングセンターでは，タイムスタンプ検証鍵を用いて送信されたタイムスタンプを復号し，送られたハッシュ値と比較を行い，検証結果をインターネット経由でユーザに返信する．

なお，2003 年 7 月に開始したサービス A-ST で利用している，アマノデジタルタイムスタンプサービスでは，ハッシュ関数は SHA-1，署名方式は鍵長 2048 ビットの RSA 署名方式を用いている．

アマノデジタルタイムスタンプサービスでは，タイムスタンプ生成鍵および検証鍵を自身で生成・管理し，有効性検証手段までを一貫して自己責任の範囲内に収めている．すなわち，公開鍵暗号方式を利用したタイムスタンプ方式における CA，TA，TSA の役割を一元的に果たしている．

7.5 ディジタル署名・タイムスタンプ付官報データの利用

ディジタル署名とタイムスタンプを適用したサービス A-ST のページ単位 PDF データを画面表示すると**図 8** のようになる．PDF ファイル表示の左側，署名フィールドにはディジタル署名とタイムスタンプが表示されている．

図 8 で示される，ディジタル署名とタイムタイムスタンプが適用された PDF データには，サービス A-ST にログインし，日付検索で希望の日付と官報種別を設定し，表示された目次の中から希望のページを指定し，イメージ表示を選択することでアクセスすることができる．利用者は，閲覧を希望する記事が掲載されている日付や官報種別が分かっていない場合が多いので，記事検索から希望の記事を表示させることが多い．そのため，記事検索から表示させた記事が含まれる，ディジタル署名・タイムスタンプ付ページ単位 PDF

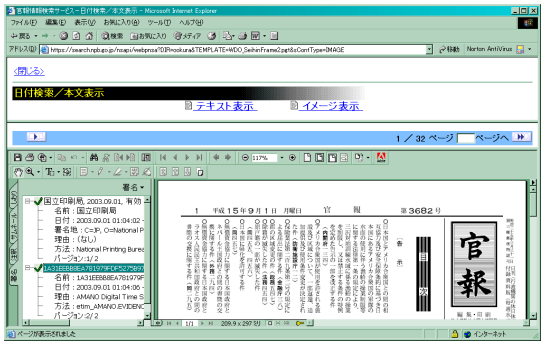

図 8 官報情報検索サービス利用イメージ
Fig. 8 Screen image of the Official Gazette Data Providing Services with digital signature and time stamp.

データを表示させるには，日付検索に戻って希望の官報種別とページを指定する必要がある．日付検索と記事検索で表示させる官報データを，もっと円滑に切り替えられるようになると，記事検索から表示した記事を含む，ディジタル署名・タイムスタンプ付ページ単位 PDF データを表示させるのが簡単になり，より使い勝手が向上するのではないかという意見が寄せられている．

8. 考　　察

以上，国立印刷局による官報データ提供サービスへのディジタル署名とタイムスタンプの適用について述べてきた．今回の適用による達成事項について以下に考察する：

- 官報データの利用者は，官報データのディジタル署名を検証することにより，官報データの作成者とデータの一貫性を検証することができる．また，ディジタル署名の有効性は，官報データの入手経路には依存しない．
- 官報データの利用者は，官報データのタイムスタンプを検証することにより，タイムスタンプの示す信頼できる時刻に，その官報データが存在していたことを確認することができ，また，タイムスタンプの示す信頼できる時刻以降の官報データの一貫性を検証することができる．
- もし，ある 1 ページの官報データを事後に作成し直したとしても，同一日付のほかのデータを作成した日時まで遡ったタイムスタンプを発行することはできない．したがって，官報データの利用者は，同一日付の複数個の官報データのタイムスタンプを確認することにより，官報データの作り直し・差し替え等が利用者に無断で行われていないかどうかという運用状況について確認することが

できる．

- 官報データの利用者は，ディジタル署名の有効期限内であれば，ディジタル署名の検証とタイムスタンプの検証という 2 つの手段によって，官報データの一貫性を検証することができる．ディジタル署名の有効期限後には，ディジタル署名の検証はできなくなるが，タイムスタンプの検証によって，官報データの一貫性を検証することができる．
- タイムスタンプ局のような第三者を介在させることにより，内部不正等に対するサービスの信頼性が向上する．

以下に，システムの一部が正しく機能しない場合の分析を示す：

- 官報データが 4.1 節と 4.2 節で示した 3 つの要件をすべて満たすためには，国立印刷局，認証局，時刻配信局，タイムスタンプ局のすべてが信頼できる必要がある．
- 認証局が正しく機能しない場合，官報データ作成者の確認ができなくなる．
- 時刻配信局とタイムスタンプ局が正しく機能しない場合，国立印刷局が一度配信した官報データを差し替えていないかどうかを確認できなくなる．
- 利用者がサーバへの接続を確立できない場合でも，ディジタル署名とタイムスタンプの検証を行うことはできる．しかし，公開鍵証明書の検証と，タイムスタンプのセンター検証を行うことはできない．

今回構築したシステムでは，ディジタル署名とタイムスタンプは独立して適用されているため，ディジタル署名の公開鍵証明書の有効期限後には，タイムスタンプの検証によるデータの一貫性の検証のみ行うことができる．なお，長期署名フォーマットとして，RFC3126[14] で規定されている，ディジタル署名に，署名再検証に必要な情報（認証パス上の公開鍵証明書，公開鍵証明書の失効情報等）を追加し，ディジタル署名と追加情報に対するタイムスタンプを取得してディジタル署名に添付するという形式がある．このような長期署名に対する技術を適切に利用していくことも，今後の検討課題である．

一方，諸外国の状況に目を向けると[15]，米国の Federal Register，英国の London Gazette，欧州連合（EU）の Official Journal of the European Union 等，諸外国も官報紙面のほかにディジタルデータのインターネット配信を行っている．採用されているデータ形式はいずれも PDF である．2004 年 3 月現在，配信データにディジタル署名やタイムスタンプを適用している事例はない．

政府機関がインターネット配信している PDF データにディジタル署名を適用している例としては，英国の The UK online annual report[16] があげられる．これは，2000 年 12 月から運用されている行政ポータルサイト「UK online」[17] の年次報告書であり，「e-Envoy」（e 政策担当特使）のサイトからダウンロードできる．2002 年度版には Adobe Acrobat のデフォルト署名ハンドラである Self-Sign を用いた e-Envoy のディジタル署名が適用されている．Self-Sign 方式は，証明書の共有にサードパーティの認証機関を介さず直接ユーザ同士で認証を行う方式である．e-Envoy の証明書のフィンガープリントは，UK online のサイト上に掲示されていて，署名検証を行うユーザは目視で値を比較し確認する．

官報は，電子申請・届出のような 1 対 1 の双方向な文書流通モデルとは異なり，発行されたものを多くの国民が利用する 1 対多の一方向な文書流通モデルである．このような文書流通モデルにおけるディジタルデータのセキュリティについて今後も整理・検討を行い，官報ディジタルデータを紙面の官報と同等に扱うための要件について検討を進めていきたい．

参 考 文 献

1) 梅澤淳子，上野裕之，宮田幸夫，佐井川泰治，江並孝之，松本 勉：インターネット配信される官報ディジタルデータへのディジタル署名・タイムスタンプ方式の適用，コンピュータセキュリティシンポジウム 2003 予稿集，pp.55–60 (2003).
2) 大蔵省印刷局：官報百年のあゆみ (1983).
3) 国立印刷局：http://www.npb.go.jp/(last visit: 26 Nov. 2003).
4) 吉国一郎，角田礼次郎，茂串 俊，味村 治，工藤敦夫，大出峻郎，大森政輔，津野 修：法令用語辞典（第八次改訂版），学陽書房 (2001).
5) 牧 潤二：官報の徹底活用法，サンドケー出版局 (1994).
6) 国立印刷局：インターネット版『官報』，http://kanpou.npb.go.jp/ (last visit: 26 Nov. 2003).
7) 国立印刷局：官報情報検索サービス，https://search.npb.go.jp/ (last visit: 26 Nov. 2003).
8) 情報処理振興事業協会セキュリティセンター：PKI 関連技術解説，http://www.ipa.go.jp/security/pki/ (last visit: 26 Nov. 2003).
9) 日本認証サービス：SecureSign パブリックサービス，http://www.jcsinc.co.jp/service/s_sign.html (last visit: 26 Nov. 2003)
10) アマノ：デジタルタイムスタンプサービス，

http://www.e-timing.ne.jp/tsa/ (last visit: 26 Nov. 2003).
11) セイコーインスツルメンツ：Chronotrust, http://www.sii.co.jp/ni/tss/s090054.html (last visit: 26 Nov. 2003).
12) NTT データ：SecureSeal〈テクニカル情報〉, http://210.144.76.11/technical/tech01.html (last visit: 26 Nov. 2003).
13) 宇根正志，松本　勉：可用性および安全性の観点からみた各タイムスタンプ方式間の関係，情報処理学会論文誌，vol43, No.8, pp.2644–2658 (2002).
14) Pinkas, D., Ross, J. and Pope, N.: RFC3126 Electronic Signature Formats for long term electronic signatures. http://www.ietf.org/rfc/rfc3126.txt
15) 国立国会図書館：法令議会資料室議会・法令リンク集，http://www.ndl.go.jp/horei_jp/Links/link.htm (last visit: 26 Nov. 2003).
16) The UK online annual report, http://www.e-envoy.gov.uk/assetRoot/04/00/04/01/04000401.pdf (last visit: 26 Nov. 2003).
17) UK online, http://www.ukonline.gov.uk/ (last visit: 26 Nov. 2003).

付　　録

A.1　ディジタル署名について

公開鍵暗号方式を用いたディジタル署名とその検証の概要を**図 9** に示す．

認証局は署名生成者に対し，電子証明書の発行を行う．認証局は発行した電子証明書と失効情報をリポジトリに登録し，公開する．電子証明書には，署名生成者の公開鍵と署名生成者の情報が含まれており，認証局のディジタル署名がされている．署名生成者は秘密鍵を用いて，ディジタル署名を作成する．署名生成者からディジタル署名付データを取得した署名検証者は，署名付データの中に含まれる電子証明書内の公開鍵を用いて，ディジタル署名の検証を行う．その際，認証局のリポジトリに問い合わせ，その電子証明書が有効であるかどうかの確認を行う．

A.2　タイムスタンプについて

タイムスタンプの生成方式として，他のタイムスタンプを構成するデータを用いて生成する連鎖型方式 L と，他のタイムスタンプを構成するデータを使わずに生成する個別型方式 I に分類する．個別型方式 I は，シンプルプロトコルとも呼ばれる．

連鎖型方式 L によるタイムスタンプ発行の一例を**図 10** に示す．

この方法は，「ツリー構造のリンキングプロトコル」と呼ばれている．以下，ツリー構造のリンキングプロトコルにおけるタイムスタンプ発行と検証の手続について説明する．

図 10 の方式では，一定時間内（ラウンド）で受け付けた利用者のハッシュ値を結合・ハッシュ化してリンク情報（SRH）を生成し，タイムスタンプ，SRH_{i-1}，中間ハッシュ値（ルートハッシュ値の作成に必要な値）をユーザに返信する．TSA は SRH を定期的に新聞等で公表する．有効性の検証方法は，まず電子文書からハッシュ値 H_1' を再度作成し，タイムスタンプ要求時に TSA から返信されたハッシュ値 H_1 と比較し，内容改ざんの有無を検証する．また，ハッシュ値 H_1' とタイムスタンプ要求時に TSA から返信された中間ハッシュ値からルートハッシュ値 RH_1' を再計算し，RH_1' とサーバに保存されている SRH_{i-1} から SRH_i' を算出する．SRH_i' とサーバに保存されている SRH_i を比較し，値が等しければこのタイムスタンプは有効である．

個別型方式 I によるタイムスタンプ発行の一例を**図 11** に示す．

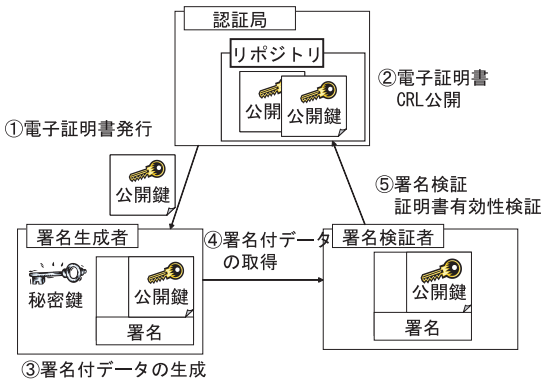

図 9　ディジタル署名の付与
Fig. 9　Outline of digital signature procedures.

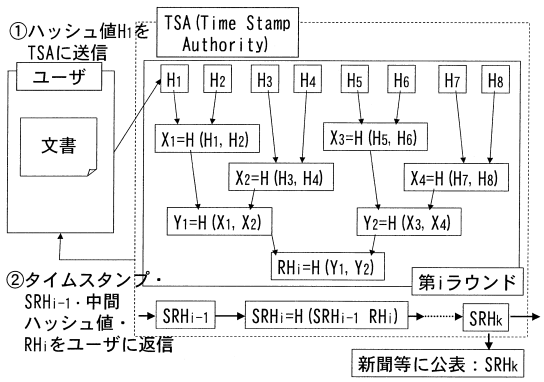

図 10　ツリー構造の連鎖型方式 L
Fig. 10　Tree-structured linked time stamp scheme.

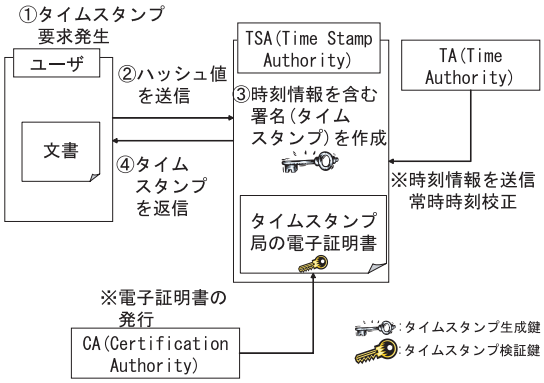

図 11 個別型方式 I の一例
Fig. 11 An example of I scheme.

この方法は，RFC3161 によって仕様が定められており，タイムスタンプは公開鍵暗号方式を用いて発行される．構成要素は，時刻情報を管理する時刻配信局（TA），TA から時刻監査を受け，タイムスタンプを発行するタイムスタンプ局（TSA），タイムスタンプ局の電子証明書を発行する認証局（CA）である．

タイムスタンプ発行者，すなわち TSA に要求者から文書のハッシュ値が送信されると，タイムスタンプ発行者は時刻情報を含むディジタル署名を作成し，タイムスタンプトークンとして要求者に返信する．有効性の検証は，ディジタル署名の検証方法と同様である．

(平成 15 年 11 月 28 日受付)
(平成 16 年 6 月 8 日採録)

梅澤 淳子

2000 年大蔵省印刷局（現，独立行政法人国立印刷局）入局．現在，開発部に所属．インターネット官報データ提供サービスのシステム構築，ディジタル署名・タイムスタンプ機能構築に従事．2003 年 4 月より 2004 年 3 月まで，横浜国立大学大学院環境情報研究院にて，情報セキュリティの研究に従事．

上野 裕之

1985 年大蔵省印刷局（現，独立行政法人国立印刷局）入局．現在，情報製品事業部に所属．インターネット官報データ提供サービスのディジタル署名・タイムスタンプ機能構築に従事．

宮田 幸夫

1983 年大蔵省印刷局（現，独立行政法人国立印刷局）入局．現在，情報製品事業部に所属．インターネット官報データ提供サービスのシステム企画・構築に従事．

佐井川泰治

1994 年大蔵省印刷局（現，独立行政法人国立印刷局）入局．現在，開発部に所属．インターネット官報データ提供サービスのシステム構築，ディジタル署名・タイムスタンプ機能構築に従事．

江並 孝之

1982 年大蔵省印刷局（現，独立行政法人国立印刷局）入局．現在，情報製品事業部に所属．インターネット官報データ提供サービスのシステム構築，ディジタル署名・タイムスタンプ機能構築，販売方法，対外調整等に従事．

吉岡 克成（学生会員）

1977 年生．2000 年横浜国立大学工学部電子情報工学科卒業．2002 年同大学大学院工学研究科博士課程前期修了．現在，同大学院環境情報学府博士課程後期に在学中．情報セキュリティ，特に情報ハイディング技術の研究に従事．

松本 勉（正会員）

1986 年 3 月東京大学大学院博士課程（電子工学）修了，工学博士．同年横浜国立大学工学部専任講師．現在，同大学大学院環境情報研究院教授．1981 年より，暗号・電子署名のアルゴリズムとプロトコル，ディジタル証拠性，耐タンパーソフトウェア，情報ハイディング，ネットワークセキュリティ，認証方式，バイオメトリクス，人工物メトリクス等の各種情報セキュリティ技術の研究教育とその実応用に力を注ぐ．1982 年に「明るい暗号研究会」を数人の仲間とともに創り研究をはじめた．国際暗号学会 IACR 理事．CRYPTREC 暗号モジュール委員会委員長．電子情報通信学会より「情報セキュリティの基礎理論」への貢献に関して業績賞を受賞．