情報流通　電子行政　HSM

R&D ホットコーナー ソリューション

# セキュア情報流通基盤技術の電子行政分野への適用

NTTサービスインテグレーション基盤研究所†1 / NTT情報流通プラットフォーム研究所†2

岸　晃司†1 /高橋　誠治†1 /村井　健二†1 /柏木　巧†1 /吉田　芳浩†1 /
阿部　裕文†2 /池田　高志†2

NTT研究所では，ITシステムにおいて情報を安全・確実に流通させるための技術「セキュア情報流通基盤技術」を検討・開発しています．今回，本技術の電子行政分野への適用を検討し，電子行政基盤のプロトタイプシステムを開発しましたので紹介します．

## セキュア情報流通基盤技術とは

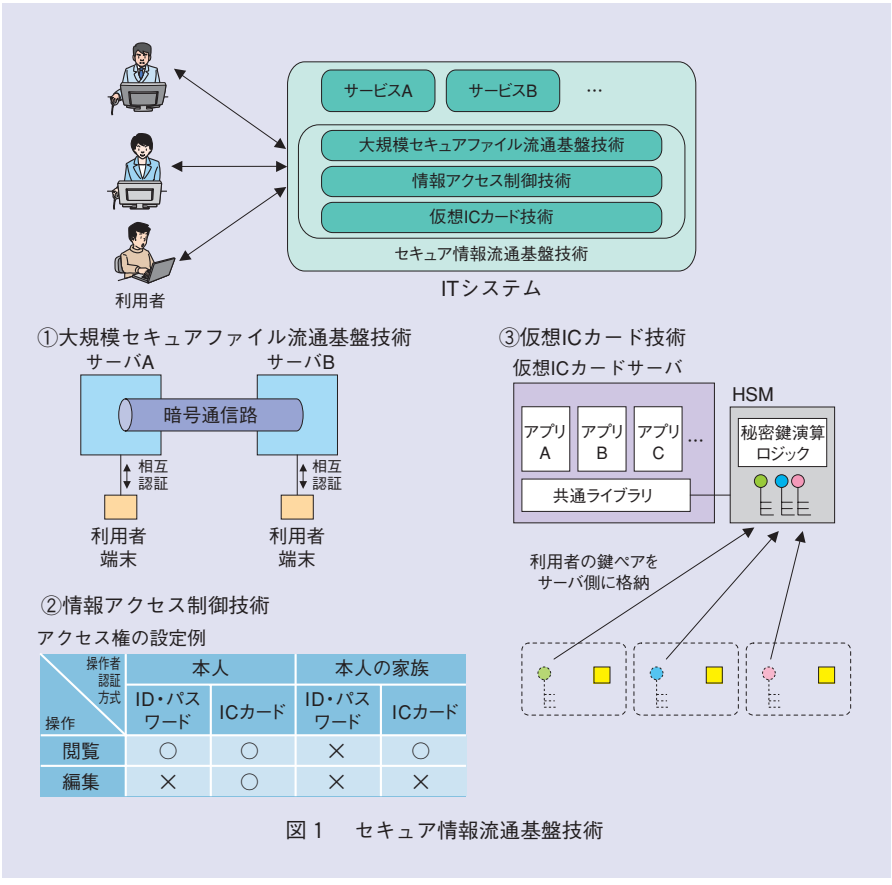
近年，私たちの生活に関連するさまざまな分野においてIT化が進んでいます．そのようなITシステムにおいては，情報を安全・確実に流通させるための仕組みが必要です．我々は，そのような要求にこたえるため，情報の改ざんや，意図しない人への情報の漏洩を防止するための技術として「セキュア情報流通基盤技術」の検討・開発を行っています（**図1**）．セキュア情報流通基盤技術は，具体的には以下に示すような技術要素を含んでいます．

⑴　大規模セキュアファイル流通基盤技術

本技術は，大容量の電子ファイル群を安全・確実に送信するための技術です(1)．Camellia暗号を利用したデータ暗号化やPKI（Public Key Infrastructure）による利用者・サーバ間の相互認証に加え，時刻認証局と連携することにより配達証明書の発行も可能なので，電子ファイルが確実に相手に届いたことを確認できます．また，ネットワーク障害等による送信中断が発生した場合でも，送信再開を確実に行えるための仕組みを持っています．

⑵　情報アクセス制御技術

本技術は，サーバに存在する個々の情報に関して，「誰にどのような操作を認めるか」を制御するものです．「誰に」に関しては，ある個人を指定してもいいですし，情報の所有者との関係性によって指定することもできます．また，「操作」とは，その情報に対する閲覧，編集等




| 操作 ＼ 操作者認証方式 | 本人 | | 本人の家族 | |
|---|---|---|---|---|
| | ID・パスワード | ICカード | ID・パスワード | ICカード |
| 閲覧 | ○ | ○ | × | ○ |
| 編集 | × | ○ | × | × |

図1　セキュア情報流通基盤技術

を意味します．例えば，Aさんの情報に関しては，Aさんの家族は閲覧可能，Aさん自身は編集可能である，という設定が可能です．また，そのようなアクセス権の設定を，あらかじめ事前に行っておくこともできますし，閲覧等の操作の都度に行うことも可能です．さらに，本技術では，利用者のできる操作を，利用者の認証方式によって変えることも可能です．例えば，「ICカードによる認証を行った場合は情報の編集が可能だが，ID・パスワードによる認証を行った場合は，閲覧のみが可能である」という設定が可能です．

⑶ 仮想ICカード技術

本技術は，ICカードの機能をサーバ上で実現するものです．ICカードは，情報システムの利用において，利用者による電子署名や，商品購入時のチャージ残高減算など，さまざまな処理を行います．その機能の一部あるいはすべてをサーバ上で実現することにより，サーバと実際のICカードとの機能分担が可能となり，実際のICカードの機能の複雑さや，ICカードの発行や配布等の運用の複雑さを抑制することができます．

なお，利用者の鍵ペアは機密性の高い情報のため，HSM（Hardware Security Module：耐タンパ装置）に格納します．また，本技術においては，マルチアプリケーション型のICカードのように，サーバ上の仮想ICカードにアプリケーションを後から追加することも可能です．

## 電子行政分野への適用の検討

電子行政とは，ITを活用した行政の仕組みのことで，行政の効率化や，国民にとって真に使いやすい行政サービスの提供を目指すものであり，近年その必要性が認識されつつあります．ただし，実現するうえでは解くべき課題がいくつか存在します．今回，セキュア情報流通基盤技術を電子行政分野に適用することを検討しました．その結果，電子行政を実現するうえでの以下の課題に対応できるのではないかと考えました（**図2**）．

⑴ 課題1：個人情報の安全な流通

電子行政分野では，行政機関から国民に対して，その人に関連する情報を安全に届ける必要があります．また，国民が行政機関に対して何らかの申請を行う場面もあります．ネットワークを利用し，それらを安全に行うためには，文書の暗号化技術や，相互認証技術が必要となります．また，特に重要な情報の伝達に関しては，情報が確実に相手に届いたかどうかを確認できる配達証明機能も必要となります．これらの要求に関しては，大規模セキュアファイル流通基盤技術の利用が考えられます．本技術により，安全・確実な情報の伝達が可能となります．さらに，仮想ICカード技術を組み合わせることにより，PKI機能を搭載した高機能ICカードを利用者に配布しなくても，利用者の鍵ペアを利用した認証やデータ暗号化等の高いセキュリティが実現可能となります．

⑵ 課題2：個人情報への適切なアクセス制御

電子行政分野では，サーバに存在する，ある個人に関連する情報を本人以外の人が参照したり編集したりする状況があります．例えば，医師は患者の健康保険の情報や受診履歴を確認する必要があるでしょう．また，親が未成年者に代わり行政機関に何らかの申請を行う場面も想定されます．このような状況に関しては，情報アクセス制御技術の利用が考えられます．本技術により，ある個人の情報に対して，誰にどんな操作を許可すべきかをシステムとして制御することが可能となります．それにより，電子行政で想定される上記のような状況に対応することができます．

⑶ 課題3：多様なアクセス端末や個人認証方式への対応

本課題は，国民が電子行政サービス

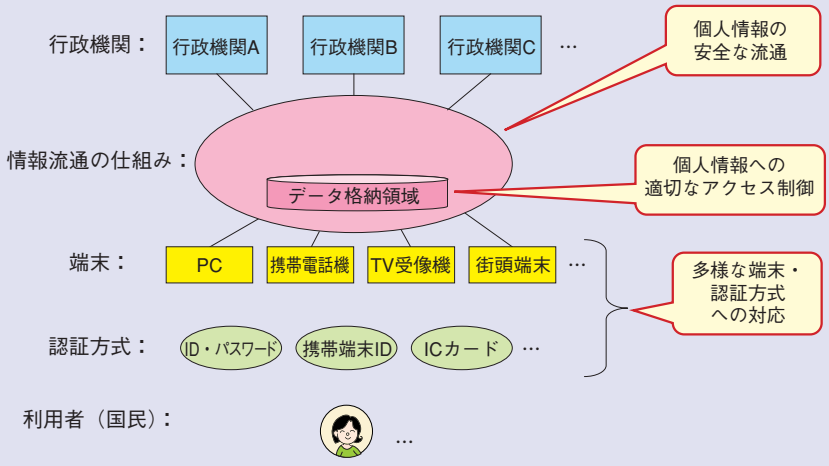



図2　電子行政の課題

を受ける際にさまざまな種類の端末からアクセスする可能性が考えられ，システムとしてそれに対応する必要があるというものです．端末としては，例えばPC，携帯電話機，TV受像機，街頭端末等が考えられます．またそれに伴い，個人認証方式も多様になると考えられます．例えば，ID・パスワードや，携帯電話機の端末IDや，ICカードの利用等です．

個人認証や電子署名を行うために利用者に配布するデバイスとしてはICカードが一般的ですが，「ICカードリーダライタを装着できないような端末からも電子行政サービスを受けられるようにする」という要件が今後はあり得るかもしれません．そのような場合，仮想ICカード技術を利用することにより，ICカードを使わなくても同様のサービスを受けられるようなシステムをつくることが可能となります．

また，電子行政が今後進展するにつれ，官・民を問わずさまざまなサービスが提供されるようになると，それに伴いICカードの発行や配布等の運用の複雑化が問題となる可能性がありますが，それを防ぐためにも本技術は有用であると考えられます．

## 電子行政基盤プロトタイプシステムの開発

前章での検討を踏まえ，電子行政分野へセキュア情報流通基盤技術を適用したシステムとして，電子行政基盤プロトタイプシステムを開発しました．本システムは以下に示すサブシステムから構成されています（**図3**）．

⑴ 基本部

他の各サブシステムと連携し，各処理の制御を行う中核的な位置付けのサブシステムです．大規模セキュアファイル流通基盤技術を利用し，情報保有機関（後述）と情報のやり取りを安全・確実に行います．また，情報保有機関から受け取った情報を格納するデータベースを持ち，その格納領域は利用者ごとに分かれています．このデータベースに格納される情報に対して，アクセス制御技術が利用され，きめ細かなアクセス制御が実現されます．

⑵ 仮想ICカード部

仮想ICカード技術を利用し，ICカードの機能をサーバ上で実現します．HSMを持ち，各利用者の秘密鍵をそこに格納します．利用者認証の成功結果を認証処理部（後述）より受け取ってから，各利用者の秘密鍵を利用した電子署名や暗号化された文書の復号等の処理を行います．

⑶ 認証処理部

利用者の認証を行います．認証方式として，ID・パスワード，ICカードの二通りを用意しました．SAMLの仕組みを利用し，認証結果をポータル部（後述）と仮想ICカード部に送信します．

⑷ ポータル部

情報保有機関から利用者に送付される情報（XML文書）を整形し，利用者に表示する機能を持ちます．また，情報保有機関への申請を利用者から受け付ける機能も有します．利用者認証の成功結果を認証処理部より受け取ってから，利用者に情報を提示します．

⑸ 情報保有機関

各国民の情報を保有している行政機関のシステムに相当する部分です．大規模セキュアファイル流通基盤技術を利用

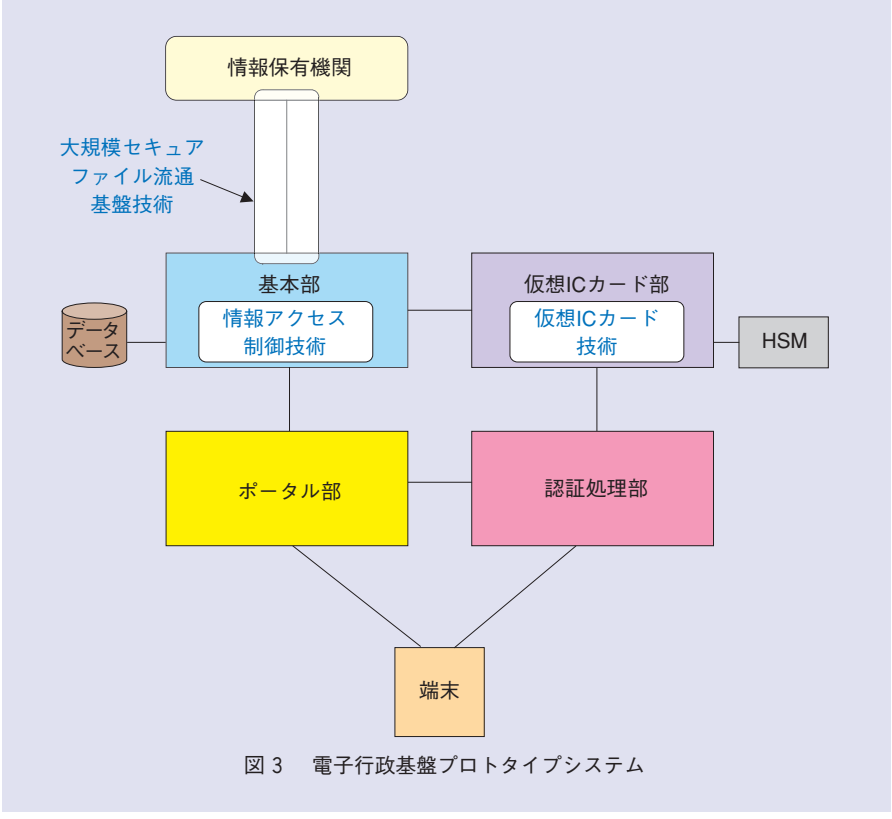



図3　電子行政基盤プロトタイプシステム

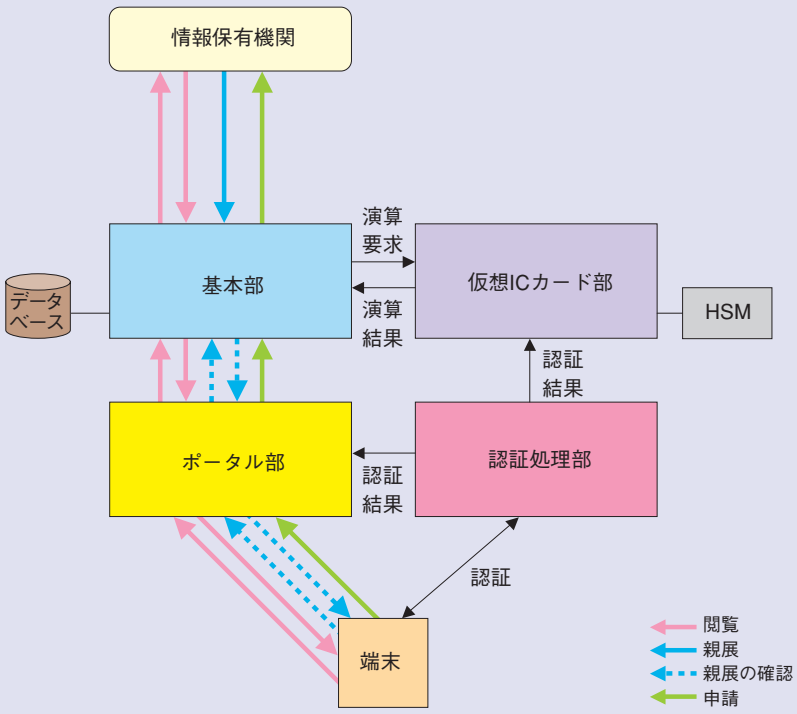



図 4　処理フロー

し，基本部と情報のやり取りを行います．

## 処理フローの確認

本システムを利用し，以下の３つの処理フローを実機で動作させることにより，前章で記した各課題に対する対応策が実現されていることを確認しました（**図 4**）．

⑴　閲　覧

利用者が，情報保有機関に存在する自分に関連する情報を閲覧する処理です．必要に応じて，その情報を基本部の自分のデータ格納領域に保存することができます．

⑵　親　展

情報保有機関が，ある特定の利用者に対してその人に関連する情報を送信する処理です．その情報は，利用者の公開鍵を利用して暗号化されており，その利用者以外の人には復号することができません．復号するには，利用者のICカードもしくは仮想ICカード部に格納されている，利用者の秘密鍵が必要となります．必要に応じて，その情報を基本部の自分のデータ格納領域に保存することができます．

⑶　申　請

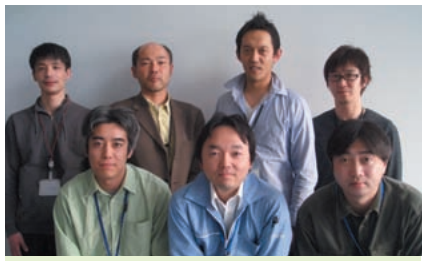
利用者が，情報保有機関に対して申請情報を送信する処理です．申請情報には利用者の秘密鍵を利用して電子署名を付加し，申請内容の改ざんを検出できるようにしています．電子署名を付加するには，利用者のICカードもしくは仮想ICカード部に格納されている，利用者の秘密鍵が必要となります．

## 今後の予定

今回，セキュア情報流通基盤技術の電子行政分野への適用を検討し，電子行政基盤プロトタイプシステムを開発しました．今後は，本システムをベースに，大規模化やバックアップ運用等を検討し，実運用に耐え得る技術，方式を開発していく予定です．また，本技術の電子行政以外の分野への適用も検討していく予定です．

**■参考文献**

⑴　吉田・谷川・高屋・森下・藤原・牛島・武田：“大規模セキュアファイル流通基盤システム（SSS），”NTT技術ジャーナル，Vol.18，No.8，pp.36-39，2006.



（後列左から）高橋　誠治/ 吉田　芳浩/
柏木　　巧/ 池田　高志
（前列左から）岸　　晃司/ 村井　健二/
阿部　裕文

これからのICT社会を支えるための技術を，今後も検討・開発していきたいと考えております．

**◆問い合わせ先**
NTTサービスインテグレーション基盤研究所
パブリックICTソリューションプロジェクト
TEL　0422-59-4913
FAX　0422-59-3983
E-mail　yamamoto.takahiro@lab.ntt.co.jp