特集2

IPアドレス管理業務における、電子証明書を用いた申請者認証の開始について

■ 電子証明書を用いた申請者認証の開始

2008年9月29日、JPNICのIPアドレス管理指定事業者（以下IP指定事業者）が、IPアドレスに関する各種申請を行う際のユーザー認証の方式として、電子証明書をご利用いただけるようになりました。2005年9月以降、利用実験が行われてきましたが、9月29日より正式に提供されることとなりました。

既存のIP指定事業者においては、申請業務を行うためのWeb申請システムにログインする際、パスワードに加えて電子証明書をご利用いただくことが可能になります。

本稿では、認証方式がどのように変わるのかを解説し、電子証明書を使う認証方式が導入された背景について述べます。また最後に今後の展開について紹介します。

■ 三つのポイント

電子証明書を用いた申請者認証のポイントを図1にまとめます。

一つ目のポイントは、IPアドレスの各種申請におけるユーザー認証の方式としてパスワードに加えて電子証明書が使えるようになることです。今後、新たにIP指定事業者になる方には、契約締結とあわせて電子証明書の発行手続きが行われます。

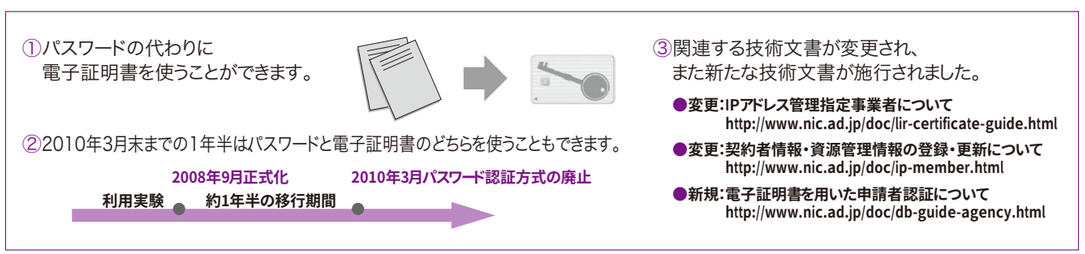
一方、これまでパスワードを使って申請業務をされてきたIP指定事業者は、電子証明書の申し込みが必要です。ただし、次に述べる移行期間では、従来のパスワードを使い続けることができます。

二つ目のポイントは、移行期間です。各種申請業務で使われてきた資源管理パスワードおよび資源業務パスワードは、2009年度末に廃止される予定です。それまでの約1年半の間は、電子証明書に移行するための期間です。パスワードを記入する形で、電子メールを使った申請業務が行われている場合や、IP指定事業者側に申請を自動化するためのシステムがある場合は、JPNICとそのIP指定事業者で、対応を進めます。

三つ目のポイントは、電子証明書を用いた認証方式は、2008年9月29日に施行された技術文書※1に則って行われる点です。これまで、電子証明書の利用は実験的に行われていたため、実験参加のお申し込みがあった際に配られる「資源管理証明書（クライアント証明書）利用規約」に則って行われていました。今後は、図1の③に示す三つの技術文書が適用されます。

またJPNICが定める文書に一部変更がございますので※1、ご確認いただきますようお願いします。

図1：電子証明書を用いた申請者認証の三つのポイント



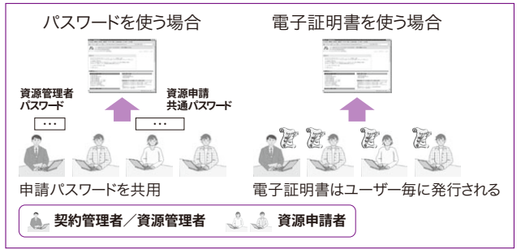
■ 認証方式はどのように変わるのか

電子証明書を利用した申請者認証が導入されることにより、ユーザー認証の方式がどのように変わるのかについて説明します。

これまでの各種申請業務では、「資源管理パスワード」と「資源業務パスワード」の2種類のパスワードが使われてきました。資源管理パスワードは、IP指定事業者の契約に関する情報や、管理する資源に関する情報の確認・変更を行うときに使われます。また、資源業務パスワードは、IPアドレス割り当て業務を行うときなどに使われます。

電子証明書は、これらのパスワードと同様に2種類発行されます（図2）。

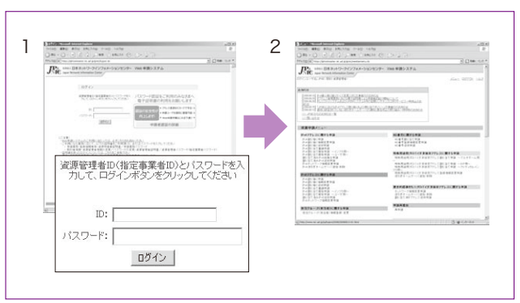
図2：パスワードと電子証明書の違い



電子証明書は、やはりパスワードと同様にWeb申請システムへのログインに使われます。いったん、ログインした後のWeb申請システムの操作方法は、パスワードでログインした場合と変わりません。

パスワードの場合、図3に示すように、Webブラウザでログインページを表示させた後、IDとパスワードを入力します。

図3：パスワード認証方式



一方、電子証明書の場合には、利用する電子証明書をWebブラウザのダイアログボックスで選択し、続いて電子証明書を使うためのパスワードを入力します（図4）。このパスワードはWebブラウザで処理されるもので、サーバ側に送られることはありません。たとえWeb申請システムに成りすました、偽のWebサーバに接続していても、パスワードなどの認証情報が偽のサーバに送られることはありません。

図4：電子証明書を用いた認証方式

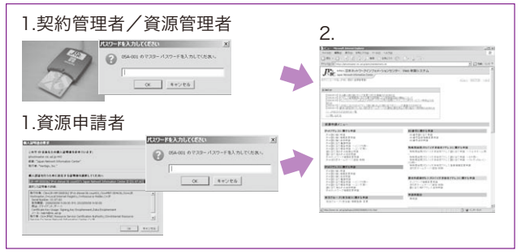


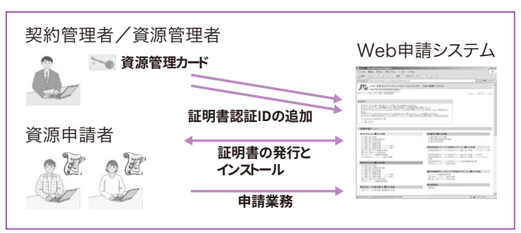
図4の左上にあるように、契約情報や割り振り先組織に関する情報の変更を行うユーザー（以下、資源管理者）は、後述する「資源管理カード」を利用します。そして、資源申請を行うユーザー（以下、資源申請者）は、電子証明書をWebブラウザにインストールして利用します。

ユーザーの切り替えのために、いったんWebブラウザを終了させるなどの操作が必要ですが、1台のパソコン（Webブラウザ）で、両方の電子証明書を使い分けることができます。

■ 新たに行われる資源申請者のID管理

パスワード認証方式では、複数の資源申請者の間でパスワードが共通であるため、資源申請者ごとに異なるユーザーIDは存在していませんでした。一方、電子証明書の場合には、ユーザーごとに発行や失効を行うため、“証明書認証ID”と呼ばれるユーザーIDの管理が行われるようになります（図5）。

図5：資源管理者による資源申請者証明書の管理

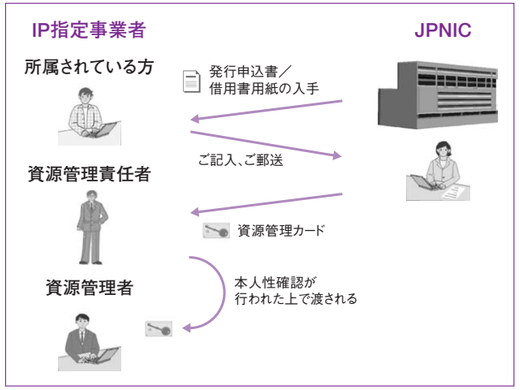


特集2 IPアドレス管理業務における、電子証明書を用いた申請者認証の開始について

証明書認証IDの管理には、Web申請システムを利用します。資源管理カードの発行を受けた資源管理者の方は、Web申請システムの「資源管理者パスワード変更」から「申請業務パスワード」の右側の「>>>証明書」をクリックすると管理画面に移ることができます。

なお、資源管理カードは図6に示す手順で入手します。はじめに、JPNICの技術文書※1を通じて、発行申込書等の申込書類を入手します。申込書にご記入の上、JPNICへ送付しますと、資源管理カードが「資源管理責任者」に送られます。資源管理責任者は、IP指定事業者において実際に業務を行う、各資源管理者の本人性確認を行った上で、資源管理者に資源管理カードを渡します。

図6：資源管理カードの発行



上記の本人性確認手順の円滑化や、不正な申請を防止するため、資源管理責任者には、資源管理カードを発送するタイミングで、資源管理カード発送のお知らせが送られます。このお知らせは、JPNICの資源管理情報に登録された電子メールアドレスに宛てて送られます。これらの手続きについては、「電子証明書を用いた申請者認証について」※2をご覧ください。

ここまでは、認証方式がどのように変わるのかについて述べました。ここからは、認証方式の変更に関わる背景と今後の展望について述べます。

■ IPアドレス資源の保護強化に向けて

電子証明書を用いた認証方式は、2002年度後半から調査研究※3が行われ、2005年9月以降に利用実験が行われてきました。

ここでは、電子証明書を用いた認証方式を導入する背景となった、三つの事柄をご紹介します。

1. IPアドレスハイジャック

国内外のレジストリにおける登録情報の安全性について行われた調査研究の過程で、“IPアドレスハイジャック”と呼ばれる行為が問題となっており、多くのIPアドレスが不適切に利用されていることがわかってきました。

IPアドレスハイジャックとは、IPアドレスに関する登録情報を改ざんし、本来の割り振り先／割り当て先とは異なる第三者が、自身をあたかも正しい割り振り先／割り当て先であるかのように変更することを意味します。登録情報が書き換えられているため、WHOISを使っても正しい情報は得られません。IPアドレスハイジャックの中には、レジストリの認証手順の弱さをついて行われているものがありました。

2. 申請業務パスワード利用の実態

二つ目は申請業務におけるパスワード利用の実態です。IP指定事業者における申請業務で、申請業務パスワードが漏洩しやすい状況があることがわかってきました。例えば、申請用のメールがメーリングリストに流れているようなケースです。

Web申請システムで使われる場合には、資源申請を行う担当者の間でパスワードが共有される必要があります。担当者が固定的であれば問題にならないケースが多いようですが、異動などによって担当者が気づかないうちにパスワードが漏洩してしまうリスクがあることがわかりました。

3. RIRにおける電子証明書の導入

RIPE NCC、ARIN、APNIC等のRIRでは、電子証明書を用いたユーザー認証の方式の導入が2002年頃より進められてきています。JPNICでは2005年度から実験を開始しましたが、同じ時期にRIPE NCC、ARIN、APNICでは、パスワードと並ぶ正式な認証手順として導入されていました（表1）。

表1：RIRにおける導入の状況

	JPNIC	APNIC	ARIN	RIPE NCC	AfriNIC	LACNIC
認証サービスの有無	△	○	○	○	×	×
認証強化開始時期	2005/9	2002/9	2004/4	2003/5	準備中	未実施

IP指定事業者で、Web申請システムのご利用が難しい場合や、申請業務を効率化するためのシステムがある場合には、ぜひお問い合わせ窓口までお知らせください。今後の対応方法や連携方式について、ご相談させていただければ幸いです。

■ 今後の応用

JPNICではセキュリティに関する調査研究を継続しています。2007年度以降は、IPアドレスを管理するレジストリとして、特にインターネット経路制御のセキュリティに注目しています。

その一環として、IP指定事業者に発行される電子証明書を応用し、IPアドレスの割り振り先／割り当て先における、インターネットの接続性向上に役立てるシステム「経路情報の登録認可機構」を実験的に構築しました。

経路情報の登録認可機構は、JPIRR※4に登録されるIPアドレスの情報を、JPNICの割り振り情報と照合し、不適切なインターネット経路の情報がJPIRRに登録されないようにするシステムです。

図7：許可リスト

図7は許可リストと呼ばれるWebインタフェースで、IP指定事業者が自身に割り振られたIPアドレスをJPIRRに登録する、“メンテナー”を指定するために使われます。許可リストに登録されたIPアドレスは、第三者によってJPIRRに登録されることがなくなるため、自身や顧客のIPアドレスがインターネットで不正に使われている場合に、JPIRRを使ったチェックが、より正確にできるようになります。

この許可リストは、資源申請者に発行される電子証明書を使ってアクセスするようになっており、利用実験に参加することで、本機構が組み込まれたIRRを利用できます。

今後、この機構の実験運用を継続し、JPNICの登録情報がインターネットの運用に役立つような仕組み作りを行いたいと考えています。利用実験へのご参加をお待ちしております。

■ まとめ

2008年9月29日より、電子証明書を用いた申請者認証が開始されました。今後、約1年半の移行期間を経て、2009年度末にパスワード認証方式が廃止される予定です。

IPアドレスに関する登録情報のセキュリティ向上のため、IP指定事業者におかれましては、お早めに電子証明書への移行を進めていただきますよう、よろしくお願いいたします。

お問い合わせ窓口：IPアドレス担当
ip-service@nir.nic.ad.jp

（JPNIC 技術部/インターネット推進部 木村泰司）

※1 2008年9月29日から有効となったJPNIC公開文書
http://www.nic.ad.jp/ja/ip/doc/20080929.html

※2 電子証明書を用いた申請者認証について
http://www.nic.ad.jp/doc/lir-certificate-guide.html

※3 経済産業省との「情報セキュリティ基盤整備（IPアドレス認証局のあり方に関する調査研究）に関する委託契約」に基づく調査研究
http://www.nic.ad.jp/ja/research/200303-CA/index.html

※4 JPIRR登録者・利用者向けページ
http://www.nic.ad.jp/ja/ip/irr/