JPNIC 情報サービスへの認証技術の適用（アクセスコントロール）について

＊宇井隆晴、小幡広昭、奥山　徹**
（社）日本ネットワークインフォメーションセンター
** 豊橋技術科学大学

概要

日本ネットワークインフォメーションセンター（以下、「JPNIC」とする）では、インターネット上の種々の情報を収集し whois データベースとして公開している。このような、インターネット上の公開情報はインターネットを維持・管理していく上で重要なものとなっている。しかしながら、これらの情報を正しく管理するには多くの労力を必要とする。JPNIC では whois データベースのインターネット上での情報の正確性・最新性の維持、及び安全な提供手段の確立について、利用者の認証問題を含めて検討している。基本的には認証局による本人認証とそれを利用したデータベースへのアクセスコントロールの導入を考えている。本論文では JPNIC が考えている認証の方法と広域情報提供サービスへの応用のあり方について議論する。

Authentication and Access Control on the Information Services in JPNIC.

＊Takaharu Ui, Hiroaki Obata and Tohru Okuyama**
Japan Network Information Center
** Toyohashi University of Technology

Abstract

Recently, applying authentication technologies to JPNIC whois database has been tried for access control. JPNIC whois database is collective catalog on whole information of IP networks and domain names in Japan. It has to provide the correct data sets of them for internet management. In JPNIC, the management of it is one of the time- and labour-consuming works. We would like to expect to reduce the management works by using the authentication processes. In this paper, fundamental policies in JPNIC related with this problem are described.

1．はじめに

JPNIC における情報提供サービスは、広義には jp トップドメインの DNS サーバの管理から WWW 等による通常の情報提供サービスまでを含むが、狭義には whois データベース[1]の維持管理が中心となる。whois データベースはインターネットに接続されているネットワークのアドレスやドメイン名に関する種々の情報を収集し、インターネットの発展のために提供されているデータベースである。

whois データベースを正しく管理・運用することは日本のインターネットの発展のために重要な事であり、JPNIC は whois データベースの管理・運用のために多くの時間と労力を割いている。しかしながら、現実には登録されたデータの内容をすべてチェックできるわけではなく、データの信頼性の維持はもっぱらユーザサイドに委ねられている。

JPNIC は、このような状態は必ずしも適切なものであると考えていない。それどころかきちんとしたデータの管理体制がない状況は、データの改ざんを含めた重大な危機をまねく恐れがある。しかしながら、日々寄せられる大量のデータベース更新を確認するためにこれ以上の労力を割くことはできず、なんらかの形でユーザを認証し、信用モデルに基づいたデータベース更新を行っていく必要がある。

そこで JPNIC では、公開鍵証明書を用いてユーザを識別・認証し、その情報を元にデータベースの登録・更新に関するアクセスコントロールを行うことを計画している。

このような政策は whois のデータの所有者（「オーナー」と呼ぶ）をはっきりさせるとともに、オーナーあるいはオーナーから権限委譲された更新責任者（これを、「メンテナー」と呼ぶ）による責任あるデータ登録・更新体制の確立を目指している。このようなモデルは、オーナーやメンテナーを全面的に信用する信用モデルが成り立つと仮定しており、この信用モデルに対する監査体制の確立も必要であるが、この論文ではそこまで踏み込んだ議論はしていない。

本論文では、次の第 2 章において、JPNIC の whois データベースについて紹介し、どの段階で認証を必要とするかについて議論する。第 3 章では、JPNIC の考えるデータ提供サービスに対する認証の基本的な考え方を議論し、第 4 章において whois データベースへのアクセスコントロールモデルについて述べる。ここでは、データベースのアクセスコントロールに適用する前段階として実施した、実験的なデータの提供サービスについて述べ、その後、whois データベースに対するアクセスコントロールの基本的な考え方を示す。第 5 章においてまとめる。

2. JPNIC の whois データベース

JPNIC の whois データベースは、日本におけるインターネット上のドメイン名と IP アドレスに関する情報を収集し公開している。データベースには、

- ネットワーク情報：IP アドレスの割り当てに関する情報
- ドメイン情報：JP ドメインの登録に関する情報
- ホスト情報：DNS サーバに関する情報
- 個人情報：登録担当者や技術連絡担当者等の各個人の情報
- 接続情報：ネットワークの接続に関する情報

などの情報が格納されている。1999 年 3 月 1 日現在のデータベース中のレコード数は表 1 のようになっている。

表 1　whois データベースのレコード数
(1999 年 3 月 1 日現在)

[ドメイン情報]	64678 (*46504)
[ネットワーク情報]	48902
[ホスト情報]	32507
[個人情報]	106150
[接続情報]	263 (*2)

*JPNIC の都合により登録したものを含む

全体のレコード総数は約 24 万件であり、月平均 1 万件ずつ増加している。また、更新・

削除を含めたデータベースへの書き込みトランザクションは平均 23,000/月に達しており（1 日平均 700 件以上)、最終的にはこれらのチェックは目視に頼っているのが現状である。書き込みトランザクションの量は増加の一途をたどっており、現状の体制では破綻する。

また、読み出しトランザクションは表 2 に示すように、1 日平均 5 万件を越えており、こちらは、データベースの分散などにより負荷分散を図ることで対処しようとしている。

表 2　whois データベースの平均検索件数
(1999 年 02 月 01 日　02 月 28 日)

総検索件数：	1,508,650 件
一日平均：	53,880 件
一時間平均：	2,245 件
分平均：	37.4 件
秒平均：	0.62 件
平均間隔：	1.60 秒

このように、whois データベースの管理・運用体制は重大な岐路に立たされている。

3．認証の基本的な考え方

本章の具体的な記述に入る前に述べておかなければならないことは、JPNIC においても認証に関するポリシは流動的であり、ここでは本論文執筆時点での著者らの考えを中心とした展開となっているということである。したがって、この論文に記されていることが全て JPNIC において採用されるとは限らないことをあらかじめ明記しておく。

現在、JPNIC が進めているユーザ認証の対象は、あくまでもデータベースに対する登録・更新者に関するものである。すなわち、第 2 章で述べたような日々増大する whois データベースへの書き込みトランザクションの内部処理の軽減と、認証されたユーザに対する信用モデルに基づくデータベース書き込み権限の委譲を実現するである。

そのためには、対象者の本人認証を含めた認証システムの確立が必要である。ところが、このような認証を検討する上で、InterNIC を含めた多くの NIC で採用されている電子メールによる登録・更新の受付が、一つの重大な問題と考えられている。電子メールを改ざんすることは、手慣れた人にとってはそれほど難しくない。そのため、InterNIC などでは PGP[2]を使った電子署名がよく使われる。しかし、PGP の公開鍵は認証している相手を信頼する信頼の鎖モデルに依存しているため、whois データベースの登録・更新のような重大な局面で使用するには不安が残る。

そこで、JPNIC では X.509 を中心にすえた公開鍵証明書を用いた認証技術の適用を検討している。公開鍵証明書を発行する機関として認証局が必要であるが、当面は JPNIC 内のプライベート認証局において実験を行い、いずれはパブリックなサービスへ移行することを考えている。

JPNIC が現在考えている認証対象は、あくまでもデータベースの登録・更新に責任を持つ人たちの有限集合であり、適当な確認手段で相手を特定できることを原則としている。このようにして本人確認された「人」に対して、認証局が公開鍵証明書を発行する予定である。

なお、細かな認証局の運用規程については暫定的なサービスについて策定したものがあるので、次の章で示す。

4．認証とアクセスコントロール

さて、前の章で示した通り、今回はデータベースの登録･更新の権限を持つ人を認証し、公開鍵証明書を発行する。データベース側では提示された証明書を見て、登録・更新権限者かどうかを判断し、データベースへのアクセスを許可するか否かを判断する。このような部分は実際には認証問題とは別の問題であり、基本的にはデータベースへのアクセスコントロールと定義できる。

アクセスコントロールをどのように実現するかは実装系の問題であり、どのようにデータベースに実装するかは現在議論の途中である。そこで、ここでは JPNIC のデータベースに対するアクセスコントロールに関する基本的な考え方を示す。

アクセスコントロールは基本的に 3 つのカテゴリーに分類される。つまり、

(1) JPNIC 内部のデータベース管理者
(2) 各レコードごとのオーナーとメンテナー
(3) データベースの検索を行うユーザ

データベース管理者は、whois データベースに対するすべてのアクセス権限を持つとする。オーナーとメンテナーの関係は第 2 章での述べたとおりであり、各レコードごとに設定され、レコードの書き込み権限を持つものとする。最後のユーザは単にデータベースの読み出し権限を有し、データベースを検索することのみが許されるものとする。したがって、(1)と(2)のデータベース管理者とオーナー及びメ

JP ドメインリスト・IP リスト配布に関わる JPNIC 認証局運用規定（抜粋）

社団法人　日本ネットワーク・
インフォメーション・センター

1. 本運用規定の目的および対象

1.1 本運用規定の目的

本運用規定は、社団法人日本ネットワーク・インフォメーション・センター（以下、「JPNIC」と呼ぶ）が設置する認証局（以下、「JPNIC 認証局」と呼ぶ）の目的、機能及び運用に関する規定を定めたものである。

1.2 本運用規定の対象

本運用規定は、JPNIC 認証局運用担当者、本認証局から公開鍵証明書の発行を受ける全て組織または個人（以下、「認証局利用者」と呼ぶ）、その他、JPNIC 認証局が発行した公開鍵証明書を使用する全ての組織または個人を対象とする。

2.JPNIC 認証局の運用目的

2.1 JPNIC 認証局の運用目的

JPNIC 認証局は、JPNIC の事業の安全かつ効率的な遂行のために、ネットワークを介したデジタル認証を導入する際に、公開鍵証明書の発行を行うことを目的とする。

2.2 公開鍵証明書の使用目的

JPNIC 認証局が発行する秘密鍵、公開鍵及び公開鍵証明書は、認証局利用者が提出する同意書に定められた使用目的のみに使用することとする。

図 1.　JPNIC の暫定サービスに対して作成された認証局の運用規程（抜粋）

ンテナーが認証の対象となる。

実は、オーナーとメンテナーの関係については現在議論の途中であり、実質的にレコードのオーナーという考えを入れないようなものから、オーナーとメンテナーの間に強い階層関係を定義するモデルまで様々なものが考えられる。また、オーナーとメンテナーの関係の記述も、データベースで定義するモデルや、公開鍵証明書に書き込むモデルなどを考えることができ、実装問題と絡めた形で議論している。

いずれにしても、「人」をどのように認証するかおよびアクセスコントロールの方法については、ようやく議論が始まったばかりであり、今後、きちんとまとまった段階で報告するつもりである。

ここでは、whois データベースへのアクセスコントロール導入の前段階で実施された、JP ドメインリストおよび IP アドレスリストの配布に対する認証とアクセスコントロールについて報告する。

JPNIC の whois データベースが日本のインターネットの重要な情報を含むことは既に述べた。さらに、JPNIC はこのような情報を基に、種々の統計データの取得や、JP ドメインや IP アドレスの一覧表を作成している。これらのデータは JP 空間における全インターネットユーザの共有財産であり、しかるべき形で利用可能とすることは重要であると考えている。もちろん、whois データベースはそのための一つの形態である。これらのデータを収集し公開するにあたって JPNIC は、「whois データベースの利用はネットワーク管理に限る」という利用制限を設けている。利用制限を設けている最大の理由は、先に述べたように、これらの情報が JP 空間の共有財産であり、ネットワークの発展に寄与するために使われるべきであり、決して商用主義に走った利用（例えばダイレクトメールの送付先のリストとしての利用）をさせないためである。

JPNIC は whois の異なるビューとして、JP ドメインや IP アドレスのすべてを網羅したリスト（JP ドメインリストと IP アドレスリスト）を公開してきた。しかし、ポートスキャンなどのセキュリティ上の問題[3]や、実際にダイレクトメール発送の為のリストとして使われた事実から、これまでのような完全に自由な提供を見直さざるを得なくなった[4]。そのため、JPNIC ではこれらのリストを必要としている機関と同意書に基づく一種の配布契約関係を結ぶと同時に、利用者に JPNIC のプライベート認証局が発行した証明書を渡し、それを用いたアクセスコントロールを施すこととした。

図 1 は、JPNIC が運用を開始したプライベート認証局の利用規定の抜粋である。認証局の詳細は紙面の都合上割愛するが、今回は Web ベースのデータの提供を予定しており、電子メールベースの whois データベースの登録・更新とはユーザインターフェイスを異にしている。これは、将来 whois データベースの登録・更新業務を Web ベースのオンライン業務に載せるための布石であると位置づけている。今回の認証システムの導入は、whois データベースへのアクセスコントロールへの適用をにらんだものであるが、一挙に対象範囲を広げることは難しいので、比較的小さな集団を相手にしたスモールスタートで実績を積み重ね、実際のデータベースへのアクセスコントロールへの適用を考えていきたい。

5. まとめ

JPNIC のデータベースの正確性と最新性を維持することは、日本のインターネットの健

全な発展のためには不可欠と考えている。しかしながら、現状では完全にそれらを達成することはできず、現状のまま推移すると、より悪い方向に行くと考えられる。

そこで、JPNIC では電子的な認証技術を導入することで、信頼モデルに基づくデータベースの登録・更新業務の抜本的な改善を目指している。ここでは、そのための準備段階として JPNIC が構想しているデータベースへのアクセスコントロールと、そのために必要な認証の問題に関する基本的な考え方を示した。

また、とりあえず手のつく問題から監視すべく、JP ドメインリストと IP アドレスリストの配布という限定された条件での認証と、アクセスコントロールの適用について紹介した。

JPNIC における認証とアクセスコントロールの問題はようやく端緒についたばかりであり、今後十分に議論されなければならない問題（例えば、個人情報の保護問題など）を含んでいる。この論文はそのための第一歩を示したものであり、今後さらなる検討を続けていきたい。

参考文献

[1] http://www.nic.ad.jp/jp/topics/archive/19980120-03.html

[2] Simson Garfinkel, PGP: Pretty Good Privacy, O'Reilly & Associates, Inc. 1996.

[3] http://www.jpcert.or.jp/info/98-0004/

[4] 奥山徹、「DNS ゾーン情報の転送停止と JP ドメインリストの配布停止について」、Internet Magazine, Vol. 6, pp.352, 1999.