ORION2001における主認証システムの構築と運用

大野 人侍†

2002年3月に稼動を開始したORION2001の構築にあわせて、それまでのキャンパス・ネットワークの構築と運用の経験を生かし、管理性の向上と情報セキュリティの高度化を目指し、ORION2001主認証システムを構築した。

主認証システムは、エージェントソフトウェアを必要としないMACアドレスにもとづいた端末のネットワークへの接続管理とIPアドレスの配布、統合されたユーザ認証データベースの提供と認証実施点への認証データの自動配布及び階層化された管理機能と使いやすいWebインターフェースの提供などが大きな特徴となっている。

本論文では、主認証システムの設計と構築について述べる。

Construction and Management of ORION2001 Main Authentication System

OONO, Hitoshi†

ORION2001 Main Authentication System (ORION2001-MAS) was introduced into the same time as constructing ORION2001 in March, 2002. It is made based on the construction of ORION and the experience of operation and designing the improvement of management and the upgrade of information security.

ORION2001-MAS has the important feature such as connection management to network of station based on MAC address and distribution of IP address that doesn't need agent software, offer of integrated user authentication DB, automatic distribution of the authentication data to authentication execution point, role-based access control and easy web interface.

In this paper, we describe the design and construction of ORION2001-MAS.

1. はじめに

大学共同利用機関法人自然科学研究機構岡崎3機関等☆1（以下「岡崎3機関等」）では、キャンパス・ネットワークとしてORION☆2を構築・運用している。ORIONは、FDDIを用いた旧ORION(1994-2002.03)、ATM交換機及びATM LANE Ver.1.0を用いVLANで構成された新ORION[1)]（1996.03-2002.03）を経て、基幹部にGigabit Ethernetを用いユーザへのサービス用情報コンセントへの回線として10/100Mbps Ethernetを用いたFull-Switchedネットワークである現在稼働中のORION2001（2002.03-）へ至っている。ORION2001では、新ORIONで導入したVLANをIEEE802.1Qを用いて全体的に構築し、物理ネットワーク構成に囚われない柔軟な論理ネットワークを運用している。

ORION2001では、新ORIONの構築と運用で得られた経験をもとにし、管理面に重点を置いた設計及び構築を行った。特に、VLANの全面的な導入による管理の複雑さや、セキュリティ上の大きな脅威となっていた情報コンセントへ

† 大学共同利用機関法人自然科学研究機構岡崎情報ネットワーク管理室
Center of Information and Communication, National Institutes of Natural Sciences

☆1 旧岡崎国立共同研究機構、2004年4月1日に改組。

☆2 Okazaki Research Institutes Organization Network

のネットワーク機器の接続を制御するという大きな課題に対する 1 つの解答として ORION2001 主認証システム（以下「主認証システム」）を構築し、運用を行ってきた。

今回、主認証システムの構築から 1 年以上たち、その間、1 回のマイナーバージョンアップを経て、岡崎 3 機関等内での定着とその間の稼動が安定している事から、主認証システムの構築・運用について発表する事とした。

2. 主認証システム構築の背景と基本方針

ORION2001 構築に向け検討を始めた 2000 年度末までには、新 ORION の構築と運用経験をふまえ、ネットワーク管理や情報セキュリティの面で改善しなければならない課題として大きく以下の 3 点が上がっていた。

1. IP アドレスによる管理の限界
2. 情報コンセントへのネットワーク機器接続制御などのセキュリティ対策
3. 接続申請データベースの整備と活用

これらの課題に関して、以下に項目ごとに背景について詳細を述べると共に構築の基本方針についても述べる。

2.1. IP アドレスによる管理の限界

IP アドレスによる管理の限界とは、現在の VLAN ネットワーク環境ではデータリンク層（以下「L2」）における管理がより本質的で重要であると言う事を示している。非 VLAN 環境におけるネットワーク管理は、ネットワーク層における経路制御管理と、ネットワークに参加する機器及び機器間の接続等の物理的管理に大きく分けられる。非 VLAN 環境では、物理的な位置と IP アドレスの管理及び経路制御を意識しておけば良いと言う事になる。しかしながら、VLAN 環境下のネットワークでは、ネットワーク層上で障害を発見しても、実際の障害箇所（場所）が特定できるわけでもない。逆に、物理的な機器の位置から参加している IP ネットワークが分かるわけでもない。VLAN 環境下では、物理ネットワーク構成に囚われる事なく、論理ネットワーク（L2 Broadcast Domain）を定義出来、その論理ネットワーク上に IP ネットワーク（Layer3 Network）を柔軟に構築できる。しかしながら、従来の IP アドレスによる IP ネットワーク管理システムでは、どの IP ネットワークで障害が起こっているかは分かっても、VLNA で重要な L2 での管理が行えないため L2 での経路や物理的にどの機器で障害が起こっているのか把握しづらいという問題がある。この問題は、新 ORION での VLAN 導入直後から管理運用上の問題点として挙げられていた。更に、ORION2001 では、VLAN の利用を拡大し、建屋間や分散したキャンパス間をもまたぐ、広域・分散化した VLAN の運用を行う事が検討されており、この保守・管理上の問題を解決する必要があった。

一方、IP アドレスによる管理の限界には、各種 OS のネットワークサポート状況の大幅な改善が影響している側面もある。旧来の OS でネットワーク設定を行うのは、一般ユーザでは敷居が高く、一部の管理者によって設定作業が行われる事が普通であり、管理という面では管理者が現状を十分把握する事が可能であった。

しかしながら、OS のネットワーク設定の簡易化やネットワーク自動設定機能の普及や DHCP サーバ機能や機器が一般化するとともに、IP アドレスの使い回しや不正な DHCP サーバなどが目立つようになり、管理者が必ずしも十分にネットワークの現状を把握する事が出来なくなっていた。特に VLAN 環境下で IP アドレスから、機器を特定する作業は、管理者の作業負担となっていた。

2.2. 情報コンセントへのネットワーク機器接続制御などのセキュリティ対策

新 ORION 構築時の 1996 年前後の時期から、ファイヤーウォール導入の議論が組織内部で行われていたが、その当時の中心的な話題は、組織内部のネットワークを如何に外部ネットワークから守るかと言うものであった。しかしながら、筆者としては情報コンセントがキャンパス・ネットワーク全体で整備された事による、内部ネットワークの不正利用による外部ネットワークへの攻撃やそれに伴う責任問題、特に不正を働いた者を特定できなかった場合の管理者の責任を問われる事の方がより脅威であると感じていた。それは、情報コンセントがキャンパス内の至る所に設置されていたにもかかわらず、物理的な入室管理等が必ずしも十分に行われていなかったからである。

その後、岡崎 3 機関等でも 1998 年以降、ファ

イヤーウォールを設置し、外部ネットワークからの攻撃に対する備えを行っているが、内部ネットワークのセキュリティはガイドライン等の整備のみで行われていた。しかしながら、2000 年以降、ウィルス等に感染した端末の無許可持込などにより、内部ネットワークでセキュリティ上の問題が起こるという事態が頻発し、何らかの接続制御が必要となった。

2.3. 接続申請データベースの整備と活用

旧 ORION 以来、岡崎 3 機関等では、機器のネットワーク接続や電子メールアドレス発行などについて、紙による申請及び管理を行ってきた。しかしながら、紙による申請では、利用者にとって不便であり、訂正や追加、削除などが十分に行われず実態と申請の間で食い違いが発生しがちであった。また、管理者側でも情報の管理が十分行えず、特に情報の運用面では問題となっていた。更に、申請そのものが形骸化し始めていたため、利用者、管理者双方に優しい方式への転換が求められていた。そこで、各種ネットワークに関係する申請を電子化・データベース（以下「DB」）化する事が考えられた。

2.4. 構築の基本方針

ここまで述べてきた課題は、相互に関連しており、ネットワーク層アドレスである IP アドレスによる管理に替え、VLAN の基本となるデータリンク層アドレスである MAC アドレスによる管理を行うと、その MAC アドレスを用いてフィルタリングが行え、ネットワークへの機器接続制御が可能となる。また、その制御に必要な情報は各種申請を電子化・DB 化すれば、一元管理可能となる。そこで、当初は、MAC アドレスによる機器管理、MAC アドレスによるフィルタリング、接続申請 DB の電子化及び統合運用を基本に機器・接続管理セキュリティシステムの構築を目指した。

MAC アドレスによる管理及びフィルタリングを行う場合には、MAC アドレスに設置機器（正確には NIC）、設置場所、設置機器責任者及び IP アドレスなどの管理情報を紐付けする必要があるが、岡崎 3 機関等の機器設置状況を見ると、職員 1 人に 1 台以上の占有端末が当たり前となっており、職員全てが管理 DB に登録される事になる。岡崎 3 機関等では、人事異動が激しく、それに伴うネットワーク管理者の管理作業、例えば、メールアドレスの変更や転送設定、ファイルサーバなどのユーザ ID 管理等が頻繁に発生し、管理者の負担となっていた。そこで、ネットワーク接続管理情報に、電子メールアドレスやファイルサーバなどのユーザ ID、所属や内線番号などの個人情報も加え、ネットワークサービス用の個人認証情報も備えた単なる接続管理用 DB としてではなく、岡崎 3 機関等における統合認証 DB として整備する事とした。

最終的には、

- MAC アドレスによる機器管理
- MAC アドレスによるフィルタリング
- 統合ユーザ認証
- 統合認証 DB

の基本的な機能を持つ ORION のセキュリティ向上の為の端末管理とネットワークへの接続管理及びユーザ管理を統合的に行う主認証システムの基本整備方針を決定した。

3. 設計と実装

2 章で述べた主認証システムの基本方針に従い、実際のシステムの設計を行うに当たって、

1. 運用可能なシステム
2. 集中管理・分散処理

の 2 点を指針とした。

3.1. 運用可能なシステム

厳密な情報セキュリティを追求するあまり使い勝手が著しく悪くなると、ユーザの反発を買いシステムを運用できなくなる恐れがある。従って、ユーザの受入れ易さと現実的な情報セキュリティ確保のバランスを取る事を優先した設計とした。ユーザ負荷を軽くする為に認証エージェントソフトウェアの採用も検討したが、多岐に渡るユーザ使用機器を網羅する事は出来ないと判断した。また、認証に複数の方法を組み合わせる事も検討したが、操作方法が統一されていないとユーザが混乱を起こし、認証システムが形骸化する恐れもあると判断した。

そこで、以前から行われていた紙による利用申請の延長という形で必要な情報を事前登録させ、事前登録情報のみを用いて接続制御や認証に使用する事とした。例えば、事前登録した MAC アドレスに対して DHCP を使用し IP アドレ

スを配布するとともに、未登録 MAC アドレスに対しては、通信を遮断しネットワーク接続制御を行う事にした。この方式では、利用者個人ベースではなく端末単位の接続認証となるが、サーバ以外基本は1ユーザ1端末である事を考慮すると、十分な制御と考えられる。

3.2. 集中管理・分散処理

主認証システムで扱う情報は、セキュリティ上重要であるとともに、個人情報に該当すると思われるものも一部ある為、慎重に管理しなければならない。また、保守対象となる機器は少ない方が良い。一方、認証機能は高負荷が予想される。

そこで、認証情報を管理する主認証サーバ（以下「MAS」）と実際に認証を実行する機器を分け、MAS を中央に配置し、各部局機器で認証を分散実行する集中管理・分散処理型の機能・機器配置とした（図 1、図 2 参照）。

3.3. 実装

ORION2001 は、主基幹ノード装置（以下「CS」）を中心とした多段スター型であり、CS に部局内を束ねる部局基幹ノード装置（以下「DS」）がつながり、部局内は、DS からスター型に情報コンセント接続用支線ノード装置（以下「ES」）がつながるという構成である。また、各部局向けの各種サーバも DS に接続されている（図 1 参照）。DS は、部局内唯一のルータとして振舞い部局内ルーティングを行い、CS は部局間及び対外ルーティングを担当する。

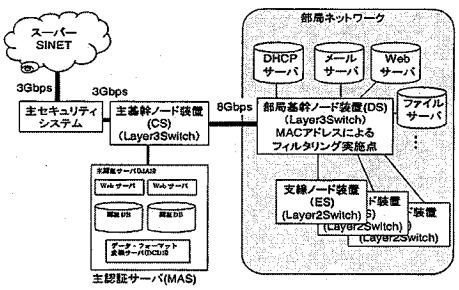

図1．ネットワーク構成概要図

MAS は、Web アプリケーションとて実装し、Model-View-Controller (MVC) モデルを採用した、Web サーバ、RDB サーバに、認証を実施する各機器用にデータを変換・配布するデータ変換・配布サーバ（以下「DCDS」）加えた構成と成っている。当然、ユーザ環境を限定しないために、サーバ側での処理を基本とした。MAS から各認証実施機器には、DCDS を通して認証情報が配布され、各認証実施機器で認証が行われる（図 2 参照）。

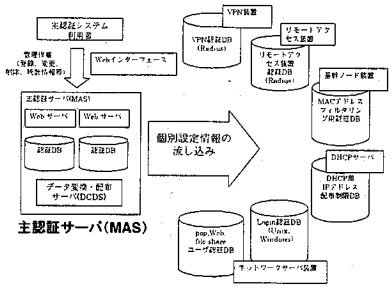

図 2. 設計概念図

MAC アドレスフィルタリング処理を例にとり、処理の流れを図 3 に示す。

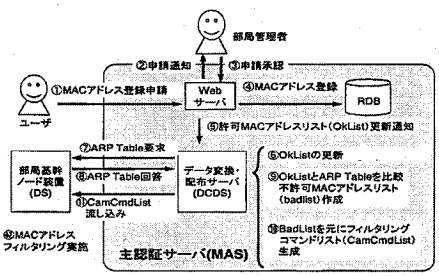

図 3. MAC アドレスフィルタリング処理流れ図

ユーザからの端末登録申請（図 3.①）により MAC アドレスが MAS 登録されると、Web サーバから DCDS に許可 MAC アドレスリスト（以下「OkList」）更新通知が出る（図 3.⑤）。DCDS は、保持している OkList を更新（図 3.⑥）後、対象 DS から ARP Table を取得する（図 3.⑦、⑧）。OkList と取得した ARP Table の差分を VLAN 単位に取り、VLAN 毎に不許可 MAC アドレスリスト（以下「BadList」）を作成し（図 3.⑨）、そこから対象 DS 用にフィルタリング用コマンドリスト（以下「CamCmdList」）を作成し（図 3.⑩）、DS に CamCmdList を配布する（図 3.⑪）。この方法は、OkList では無く BadList を使用している為、Web サーバからの指示以外に、図 3.⑥～⑪の処理を定期的（60 秒間隔）に行い不許可端末の排除を行っている。

DCDS と DS との情報のやり取りは、SSH を用

いた暗号化された通信路上で、コマンドラインコンソール上での標準入出力をエミュレートする事によって実現させている。

MAS で実装した主な機能は、

- MAC アドレス（端末）管理
- ネットワーク接続管理
- 情報コンセント管理
- ユーザ情報管理
- MAC アドレス、ネットワーク接続及びユーザの紐付け管理
- MAC アドレスベース・フィルタリング情報の生成と機器への配布
- DHCP 及び DNS 情報の生成と機器への配布
- ユーザ認証情報の生成と機器への配布
- システムで使用する通信の暗号化
- 登録情報の検索とレポート
- 外部システムとの連携機能
- ユーザの役割に応じた主認証システムへのアクセス制御

などである。

4. 運用

主認証システムの利用は、全て Web ブラウザを通して行う（図 4 参照）。

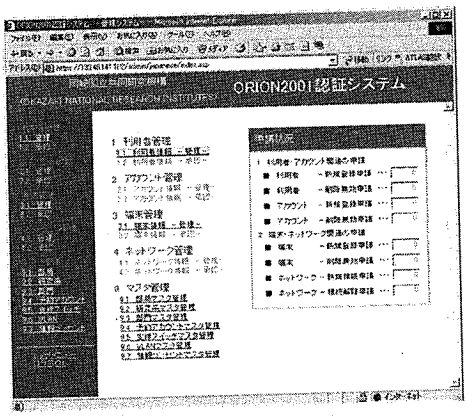

図 4. 主認証システム管理トップ画面

実際の利用の流れは、まず、研究部門の担当者が新規ユーザ登録をアカウント管理画面を使用して行う。次に端末管理画面を使用し、端末 MAC アドレス情報などを登録後、その端末の使用場所（情報コンセント）情報をネットワーク管理画面から申請する。ユーザからの申請があると、管理者に対して電子メールで通知があり、ユーザからの申請を許可するかどうか判断する。申請を許可すると、MAS が登録情報をもとに、必要な情報を生成し、各機器に情報を配布するとともに、ユーザに許可を通知する。その後、実際に端末を接続し、ネットワークを利用する事が出来る。管理者による登録・申請内容の確認は各段階で行え、修正、許可、不許可及び差戻しなどが選択できる。また、結果は申請者やユーザに通知される。

5. 評価と課題

5.1. MAC アドレスによる管理

MAC アドレスによる管理は、VALN 環境に適していると同時に、端末の管理と言う点でも適している。IP アドレスによる管理では、リソースとしての IP アドレスは管理できても、情報セキュリティの基本である端末（NIC）の管理は行えない。情報セキュリティや VLAN 等を考慮しなければならないネットワークに関しては、IP アドレスによる管理より、MAC アドレスによる管理が遥かに優れている。

5.2. 初期フィルタリング漏れ

3.3. で述べた様に未登録 MAC アドレスの検知と実際のフィルタリング処理は、現状で最大 60 秒間の遅延が発生し、その間は、不正通信を許してしまう。60 秒と言う検知・処理間隔を短くする事は可能であるが、DS や DCDS の負荷や仕様上、リアルタイムに処理を行う事は不可能である。

次期主認証システム構築時には、この様な点を考慮し、複数の通信遮断方法を組み合わせるなどの工夫を行う事にしている。

5.3. フィルタリング実施点の拡張

主認証システムでは、経路制御を行っている DS のみで MAC アドレスフィルタリングの実施が可能である（図 5 参照）。

現状では、厳密ではないが、十分なフィルタリングの実施が行えていると考えられるが、今後の拡張性の維持や ES の階層化などが進んだ場合、十分なセキュリティを提供できなくなる可能性がある。

それに対応するためには、フィルタリング実施点（装置）を自由に設定できるようにシステムを拡張していく必要がある。

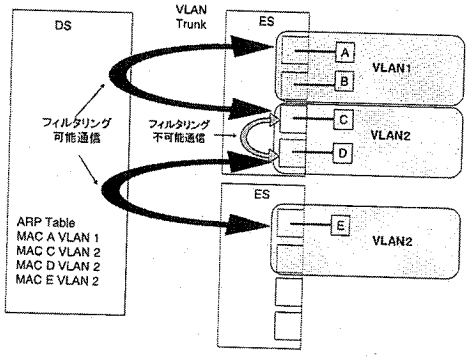

図5. フィルタリング実施点

5.4. DHCPよるIPアドレス配布

1端末で有線LANと無線LANなど複数のインターフェースを持ち、どれを使用したとしても同一のIPアドレスの配布を受けたいというユーザニーズが大変高い。ただし、現在採用しているDHCPサーバでは、

- 異なるMACアドレスへの同一VLAN内での同一IPアドレスの配布

という要求に応えられないため、一方にはDHCPで、片方には手動でと言うような運用によって問題を回避している。

これに対しては、主認証システムの仕様に合わせてDHCPサーバの実装を拡張して行きたいと考えている。

5.5. 情報保持形式

現在の認証情報は、リレーショナルデータベースを用いて表形式で保持しているが、DB内の値がどの様な意味を持つのかそれだけでは分からない。情報の交換方式として今後の拡張性などを考慮すると、現在の単なる値としてデータを保持するのではなく、データに意味を持たせたXML形式で情報を保持する方法も重要な検討課題のひとつである。

5.6. 情報セキュリティ実施手順書との関係

本論文では触れていないが、岡崎3機関等では、2003年度から情報セキュリティ実施手順書（以下「実施手順書」）の運用を開始している。実施手順書では、ORIONの利用資格や接続端末条件（アンチウィルスソフトの装備等）、端末接続手順等を規定している。実施手順書に記載されている手続きを主認証システムがフレームワークとして支え利用者・管理者の負担を軽減している。

5.7. なりすましなどの問題

主認証システムでは、MACアドレス詐称やユーザのなりすましや正規端末の不正サービス提供等の不正を完全に排除する事は出来ない。しかしながら、ある程度の壁を作る事で安易な不正行為を防止している。不正行為を完全に排除する為には、生体認証やより高度な認証ネットワーク、端末のリモート管理等複雑で高度なシステムが必要となる。岡崎3機関等の組織では、全てをネットワークシステムで実装するのは非合理的であると考え、実施手順書の整備や広報、アンチウイルスソフトの配布、セキュリティ情報の提供や啓蒙活動等色々な層で色々な方法を組み合わせる事によって、全体的なセキュリティレベルを保つと言う方針を主認証システム計画段階から採用している。

6. おわりに

5章で述べた様に、主認証システムには、残された課題も存在するが、ユーザ管理や端末の接続管理など統合的に行える様になると共に、障害発生時に障害機器のMACアドレスから、設置場所や設置機器責任者等をすばやく特定でき、復旧時間・復旧作業量の減少や、実施手順書を遵守・実行する為のフレームワークとして十分な機能を一般ユーザ・管理者双方に提供している。更に、実施手順書に準拠しない不正端末のORIONへの接続を拒否する事で、それまでは年に数回発生していたウィルスなどに感染した不正端末による大規模なネットワーク障害などが防止でき、ネットワーク全体が安全に運用できるようになった。

謝辞

主認証システム構築と日ごろの運用に協力していただいている ORION を構成する全ての部局ネットワーク管理者の方々に感謝します。

参考文献

1) 大野人侍:岡崎国立共同研究機構におけるATM ネットワークの構築と運用, 情報処理学会 分散システム運用技術シンポジュウム'98論文集, pp. 41-46 (Feb. 1998)