社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2006－ＤＤ－56（２）
2006／7／28

データ管理にXMLを用いたWebベースのネットワーク利用者情報管理システムの構築

小野寺克昌†　瀬川　典久†　杉野　栄二†　澤本　潤一†　阿部　芳彦†

† 岩手県立大学ソフトウェア情報学部　〒020-0173 岩手県岩手郡滝沢村滝沢字巣子 152-52
E-mail: †g031b029@edu.soft.iwate-pu.ac.jp, ††{sega,sugino,sawamoto,yoshi}@iwate-pu.ac.jp

あらまし　企業や大学等の組織において構成される内部ネットワークには固定された端末だけでなく、個人持ち込みのPC等の様々な端末も接続される。情報漏洩やウイルスによる被害を防ぐためにも端末の管理を行うことは非常に重要である。土屋はこの問題に対し、ネットワーク監視ソフトと連携したWebベースのネットワーク利用者情報管理システムを構築した。本稿では土屋が提案したネットワーク利用者情報管理システムを拡張再構築し、複数のネットワーク間での連携を行うシステムを提案する。
キーワード　XML, ネットワーク

Construction of the Web based network user information management system using XML for data management

Katsuyoshi ONODERA†, Norihisa SEGAWA†, Eiji SUGINO†, Junichi SAWAMOTO†, and Yoshihiko ABE†

† Faculty of Software and Information Science, Iwate Prefectural University　Takizawa aza Sugo 152-52, Iwate-gun Takizawa-mura, IWATE, 020-0173 Japan
E-mail: †g031b029@edu.soft.iwate-pu.ac.jp, ††{sega,sugino,sawamoto,yoshi}@iwate-pu.ac.jp

Abstract　Not only the fixed terminal but various terminals are connected to internal network of the organization of a company, a university, etc. It is very important to manage a terminal, also in order to prevent the damage by an information leak or the virus. In this paper, the user information management system which manages the terminal connected to the network safely and easily is proposed.
Key words　XML, Network

1. はじめに

近年ネットワークの普及により企業や大学等の組織においても内部ネットワークが構築されるようになった。ネットワークにはサーバマシンや個人PC等が接続され、同じネットワーク上に存在するリソースを利用することができる。このようなネットワークは通常、外部からの攻撃を防ぐためにファイアウォール等の対策がとられている。しかし内部ネットワークに接続された端末からの情報漏えいやウイルスの拡散等が近年問題になっている。そのため、内部ネットワークに接続された端末及び端末の利用者を管理することは非常に重要である。[1]

1.1 端末管理の現状

現在多くの組織ではネットワークの管理は組織の一部署で集中管理されていることが多い。岩手県立大学においては中央監視センターが学内の内部ネットワークを管理している。内部ネットワークのリソースはDHCPによる割り当てと研究室毎に割り当てられているIPアドレス空間を用いる方法の2つに大別される。

DHCPによるIPアドレス割り当てではまず、ネットワークの利用を希望する学生及び職員がネットワーク接続申請を行い、接続許可が下りた段階でネットワークへ接続が可能になる。この際、IPアドレスの割り当てに認証DHCPの機構を用いている。しかし、割り当てられたIPアドレスを第三者が何らかの手段を持って手に入れた場合、利用許可を与えられていない端末が不正に接続することを防ぐことができない。また、申請から許可までに3日程の時間がかかるため、端末の入れ替わりが頻繁に行われる組織においてこの方法は不向きであると言える。

あらかじめ研究室に割り当てたIPアドレス空間を用いる場

合には、接続を行うために研究室のネットワーク管理者に対してアドレスを割り当ててもらい、ネットワークへの接続を行う。割り当て可能なIPアドレス空間はあらかじめ範囲が指定されており、管理者はその中から未使用のIPアドレスを利用者へ割り当てる。中央監視センターへの手続きが不要であるため即時ネットワークの利用が可能となる反面、管理者を介さずに利用者自身が直接端末へIPアドレスを割り当てることも可能であり、その場合ネットワーク管理者は現在使用されているIPアドレスの把握が困難になる。そのため、不正接続を防ぎ、且つ容易にネットワークの利用者情報を管理するシステムが必要であるといえる。これに対して土屋伸二はネットワーク監視ソフトと連携したWebベースの利用者情報管理システムを構築した。[2]

1.2 先行研究

土屋が構築したシステムは既存のネットワーク監視ソフトと連携を行う利用者情報管理システムにより、不正接続端末の検知と利用者情報の管理を行う。ネットワーク利用希望者はシステムの管理者に対して接続希望の申請を行い、管理者がシステムに利用者情報の登録を行う。登録されたネットワーク利用希望者の端末は正規の端末と見なされ、ネットワークへの接続が許可される。

このシステムはWebベースであることと、管理対象を比較的小規模なネットワークとすることで、容易に利用者情報を管理することができる。

2. システムの提案

先の研究[2]では管理対象のネットワークを一つのサブネットとし、利用者情報の管理を行っている。利用者情報はデータベースに格納され、Web上での参照が可能となっている。しかし、個々のシステムが独立して存在しているため、サブネット間を移動してネットワークを利用する場合それぞれのシステムに対して接続希望の申請を行う必要がある。ネットワーク移動毎の登録申請は利用者にとって不便であり、登録作業を行うネットワーク管理者にとっても手間がかかる。

そこで、本研究ではネットワーク利用者情報管理システム間で連携を行う複数ネットワーク対応のシステムを提案する。これを実現するため、具体的には以下の情報が必要となる。

- 不正接続端末の情報
- 連携する管理システムの情報

これらの情報をシステムが管理することで、他システムに対して問い合わせを行い正規端末であるかどうかを検証する。他システムに登録されている場合は一時的に接続を認め、正規の接続とする。システムに登録されていなかった場合、又は他システムからの接続を認めない場合は不正接続とする。これによってあるシステムで登録された端末は他システムにおいて接続申請を行うことなく接続を行うことができる。また、ネットワーク管理者の作業を減らすことも可能である。

本システムは基本的に先行研究で開発された土屋のシステムを踏襲する。特徴としては次の3つが挙げられる。

（1） Web上で動作することで管理を容易なものとする

（2） ネットワークへの不正接続を防止する

（3） 組織に応じた情報の管理を可能とする

(1)はWebブラウザ上からシステムの操作を可能とすることで端末を限定しないという利点がある。(2)はネットワーク監視ソフトとの連携により実現する。(3)については例として大学での運用を仮定し、システムの構築を行う。

本システムの利用者情報のデータ形式は土屋によるシステムとは違って、XMLを用いる。これによってデータの変更、Web上でのインターフェース拡張が容易なものになると期待できる。

システムを扱うクライアントはPC以外にも場所を問わずにWeb上で行える利点からPDAも想定する。PDA用Webブラウザでも情報の管理がスムーズに行えるようにシステムのインターフェースはWeb上で動的に生成を行う。XMLは独自の変換仕様であるXSLT(XML Style Sheet Language Transformation)を持っているため、様々なクライアントに対し柔軟にインターフェース変更が可能である。管理される利用者情報のXMLはテキストデータとして生成するため、利用者情報管理システム導入が容易である。

3. システム構成

本研究で提案するシステムは単独で動作するネットワーク利用者情報管理システムと、システム間を連携する機能から成る。単独で動作するシステムが持つ必要な機能は以下の通りである。

- ネットワーク監視システムとの連携機能
- 利用者情報管理システムを利用するためのインターフェース提供機能
- 利用者情報管理機能
- 不正接続端末閲覧機能

さらにこれらの機能を持つ単独システムを連携させるシステム間連携機能により、他システムとの連携が可能となる。図1にシステムの全体図を示す.

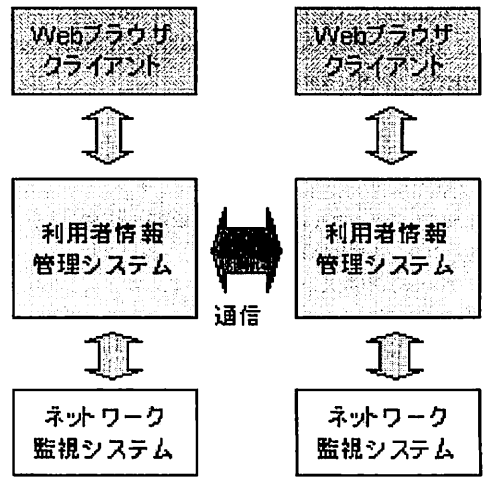

図1 システムの全体図

3.1 ネットワーク監視システムとの連携機能

不正接続を防ぐために既存のネットワーク監視システムを利用する。ネットワーク監視システムと連携するために、ネットワーク監視システムのデータベースにアクセス（データの登録、削除）を行う。ネットワーク監視システムには（株）サイバーソリューションズの NetSkateKoban を用いる。このシステムはネットワーク内を流れる ARP パケットを常時監視し、ネットワークに接続されている端末を検出することが可能である。

3.2 利用者情報管理システムを利用するためのインターフェース提供機能

Web 上から利用者情報の管理を行うために、インターフェースを提供する。インターフェースの提供には利用者情報 XML に対して動的に変換を行う XSLT を用いる。XSLT は XML 文書変換のための仕様であり、W3C(World Wide Web Consortium) により標準化されている。PC や PDA といったユーザクライアントを判定し、ユーザクライアントに適したスタイル情報を動的に XML 文書に適応させることで、適当なインターフェースを提供することが可能となる。図 3 に XML ファイルの変換イメージを示す。

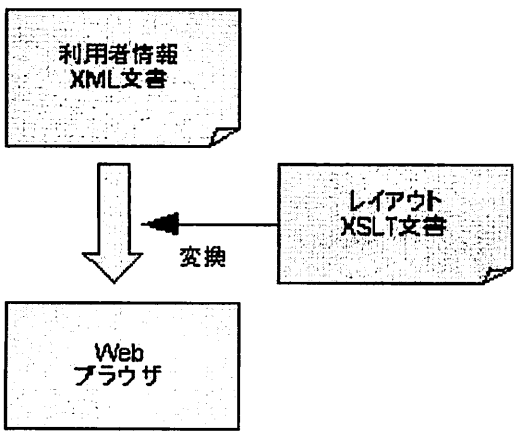

図 2 利用者情報データの変換

3.3 利用者情報管理機能

ネットワーク接続を利用する利用者情報の管理を行う。利用者情報として、ネットワークの利用者の情報と利用者の端末の情報を管理する。Web インターフェースからのフォーム入力を処理し、データの表示、登録、削除、編集、及び検索を行う。データは XML 形式で保存され、インターフェース提供機能によって Web ブラウザ上から操作が可能である。各操作は XML を操作することで実現するが、同時にネットワーク監視システムとの連携機能によりネットワーク監視システムのデータベースに対しても操作を行う。また、他システムに登録されている端末の情報についても閲覧が可能である。

3.4 不正接続端末取得機能

ネットワーク監視システムが検出した不正接続端末の情報を Web 上で閲覧する。ネットワーク監視システムのデータベースに対してアクセスすることで不正接続端末の情報を得る。不正接続端末の情報は XML 形式で保存され、インターフェース提供機能により閲覧が可能となる。不正接続端末の情報は不正接続端末が検出された場合、他システムに問い合わせを行うために必要となる。

4. システム間連携

単独で存在する複数の利用者情報管理システムを連携させるために、システム間で通信を行う。具体的にはあるシステムで登録されている端末が他のシステムに対して登録の処理を行わずとも、正規の端末としてネットワーク接続の許可を与えられるようにする。この際、他のシステムは現在ネットワーク上に接続されている端末の情報と、且つその端末がシステム内に登録されていない端末であるという情報が必要である。

システム内に不正な接続があった場合、不正接続端末取得機能によって不正接続端末の情報を得る。さらに不正接続端末の情報を他システムに対してブロードキャストし、他システムに登録されているかを問い合わせる。この際、問い合わせ対象となる他システムを事前に登録しておくことで、そのネットワークがどの部署であるかの判断が可能となる。問い合わせに対して、他システムに登録されていた場合は正規の端末としてネットワークの接続を許可する。

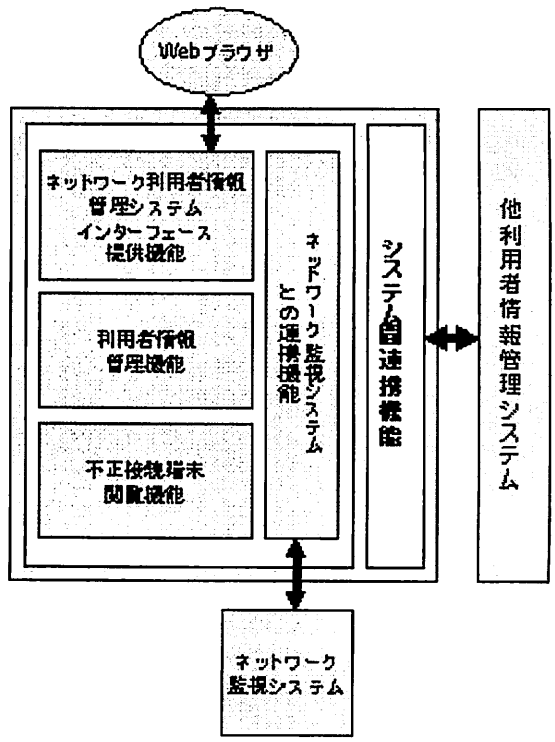

図 3 他利用者情報管理システムとの連携

また、管理ポリシとして他ネットワークからの接続を受け入れないネットワークの存在も考慮する必要がある。その場合は

自システム内に登録されている利用者及び端末を正規の端末とし、それ以外は不正とみなすこととなる。

このシステム間連携が必要となるケースとして、大学内の研究室が想定される。自分が所属する研究室のネットワーク利用者情報管理システムに登録しておくことで、サブネットの異なる他研究室にマシンを持ち込んだ場合登録作業が不要になる。その際は移動元のシステムにおいて正規の端末であるという信頼のもとにネットワークリソースの割り当てを行う。さらに移動先の研究室のサーバが動的 IP アドレス割り当て機構を持っている場合は割り当て作業も自動化される。

5. 今後の課題

本システムは利用者情報システム間での連携部分とネットワーク監視システムとの連携部分を除いてプロトタイプが完成しており、実際に試験運用をしている。今後の課題として、実際に複数のシステムを運用し、評価する必要がある。ネットワークごとの管理ポリシに対応したニーズをシステムに反映させることが必要になってくると考えられる。また、組織に応じた情報を管理するためにシステムが扱う情報に関しても精査することが求められる。

文　献

[1] 稲垣知宏, 隅谷孝洋, 岸場清悟, 入江治行, 岩沢和男, 津久間秀彦, 鈴木俊哉, 新畑道江, 勇木義則, 端末及び利用者情報管理システムと WWW を用いた情報共有, 情報処理学会,2000

[2] 土屋伸二, 根川典久, 杉野栄二, 阿部芳彦, ネットワーク監視ソフトと連携した Web ベースのネットワーク利用者情報管理システムの構築, 岩手県立大学,2006