Vol.2010-IOT-9 No.12
2010/5/14

# 遠隔ネットワーク性能・機能診断システムの構想

佐藤 聡[†1] 高田真吾[†1]
中井 央[†2] 新城 靖[†1]

我々は，個人が利用する端末のファイアウォール設定やネットワーク性能を遠隔から診断するために，認証連携により利用可能となった遠隔にある計算機資源を使うことを考えている．ネットワーク機能・性能診断を行うには，診断を行う主体の組織，診断対象のネットワーク管理組織，診断装置自体の管理組織のそれぞれのポリシーに従って診断内容についての承認する必要がある．本論文では診断システムおよび承認機構の構想について述べる．

# A conception of a diagnosis system for network fucntion and perfomance from remote

Akira SATO,[†1] Shingo TAKADA,[†1] Hisashi NAKAI[†2] and Yasushi SHINJO[†1]

We think about using the remote computer resources that became available by certification cooperation to diagnose firewall setting and the network performance of the user terminal. To perform network function and performance diagnosis, it is necessary to approve diagnosis content according to policies described by a manager of the organization of user and a network administrator. We discuss a diagnosis system and a design of the approval method in this paper.

†1 筑波大学大学院システム情報工学研究科コンピュータサイエンス専攻
Department of Computer Science, Graduate School of Systems and Information Engineering, University of Tsukuba
†2 筑波大学大学院図書館情報メディア研究科
Graduate School of Libraty, Information and Media Studies, University of Tsukuba

## 1. はじめに

近年，インターネットにサービス提供するサーバの構築，ブロードバンドルータを用いたネットワークの構築，パソコン上のファイアウォール機能の設定など，個人ユーザがネットワークのアクセス制限に関する設定を行う機会が増大している．また，ネットワークの利用のされ方がより複雑になってきたのに伴い，ネットワークのアクセス制限の設定もさらに複雑になってきている．そのため，ネットワークのアクセス制限の設定が正しく設定されているかの確認をしたいという要望は非常に大きなものとなっている．また，ネットワークの回線帯域が自由に選択できる環境が整備されたことに伴い，選択のためにネットワーク帯域の調査を行いたいといった要望も高まってきている．

ネットワークのアクセス制限の設定が正常になされているかを診断するためには遠隔からアクセスを試みる必要がある．この試みは，時と場合によっては，ネットワークに対する攻撃として判断される可能性がある．そのため，遠隔から診断を行う場合には，診断対象となる計算機の管理者と診断を行う計算機の管理者とで診断を行う行為に対してあらかじめ調整を行う必要がある．さらに，ネットワーク構成によっては，その診断行為が結果的には経路中にあるネットワーク機器の診断を行うことになる場合がある．そのような場合にはその経路中のネットワーク機器の管理者との調整も必要となる．

一方で，近年組織を越えた認証基盤の構築が進んでいる．これは，Web を用いたサービスでの認証が容易に実現できる環境がが整備されてきたと捉えることができる．これを遠隔からのネットワーク機能・性能の診断に対して適用すると，診断対象となる計算機の管理者と診断を行う計算機の管理者との間の信頼関係があらかじめ構築しやすくなる．

本論文では，認証基盤を使って認証を行い，遠隔からのネットワーク機能・性能の診断を容易に実現するためのシステムついて構想する．ただし，ここで容易に実現できるというのは，診断を実施した行為自体が，経路となるネットワークの管理者や認証に用いた認証サーバの管理者等に迷惑をかけることなく実施できるという意味も含めている．

## 2. ネットワーク機能・性能の診断における問題点

サーバへのアクセス拒否機能が正常に動作しているかを診断するためには遠隔からアクセスを試みる必要がある．これらのアクセス拒否機能は，本来，サービスに提供するために実施するために動作させている．したがって，拒否されるべきアクセスが頻繁に行われる場合には，ネットワーク攻撃として判断される可能性がある．本研究で開発を進めているシス

テムおいては，ネットワーク攻撃として判断されると，そのサービスを継続できなくなる．したがって，本研究では間違って攻撃と判断されることを防ぐことが重要な課題となる．

このとき，診断依頼の発信元となる IP アドレスに対してのみ診断を行うことという制限を設けることにより，診断依頼元と異なる計算機を診断し，間違ってネットワーク攻撃と判断されることを防ぐことが可能である．

しかしながら，これだけでは，間違ってネットワーク攻撃と判断される問題全ては解決できない．ネットワーク攻撃の判断を行うのは，診断対象となる計算機の管理者であり，利用者ではない．管理者が診断を行うことを知らないことにより，ネットワーク攻撃と判断される場合がある．

また，計算機と診断実施する計算機との間のネットワーク構成によっては，その診断行為が経路中にあるネットワーク機器の診断を行うことになる場合がある．例えば，その経路上にファイヤウォール装置や NAT 装置がある場合には，診断行為自身が，その経路中のネットワーク機器への攻撃と判断される場合もある．通常，ネットワークまたは計算機の管理者がネットワーク上の攻撃と判断した場合，その通信の発信のネットワーク管理者に対して対処要求が行われる．

## 3. 提案するネットワーク機能・性能診断システム

本論文では，関係する管理者に余計な手間をかけることなく，遠隔からネットワークの性能や機能についての診断を容易に実現できるシステムについての構想について述べる．，本研究で提案する遠隔からのネットワーク機能・性能の診断システムの概要を**図 1** に示す．

提案システムは，遠隔診断を行う**装置**，診断対象となる**端末**，認証を行う**認証サーバ**から構成される．またそれらについては各々管理者がいるものとする．具体的には，装置を管理する**装置管理者**，端末が接続されているネットワークを管理する**ネットワーク管理者**，認証サーバの認証情報を管理している**認証サーバ管理者**である．

提案システムの利用の流れを以下に示す．

(1) システムを利用する**利用者**は診断対象となる端末から認証サーバに接続し認証を受ける．
(2) 利用者は，同じ端末から装置に診断要求を出す．
(3) 装置は，利用者の認証情報を含む端末からの診断要求をポリシーに基づいて承認し，承認された場合のみ診断を実施する．

提案システムにおいて，認証連携を用いる点および記述されたポリシーを用いた承認をする点に特徴がある．

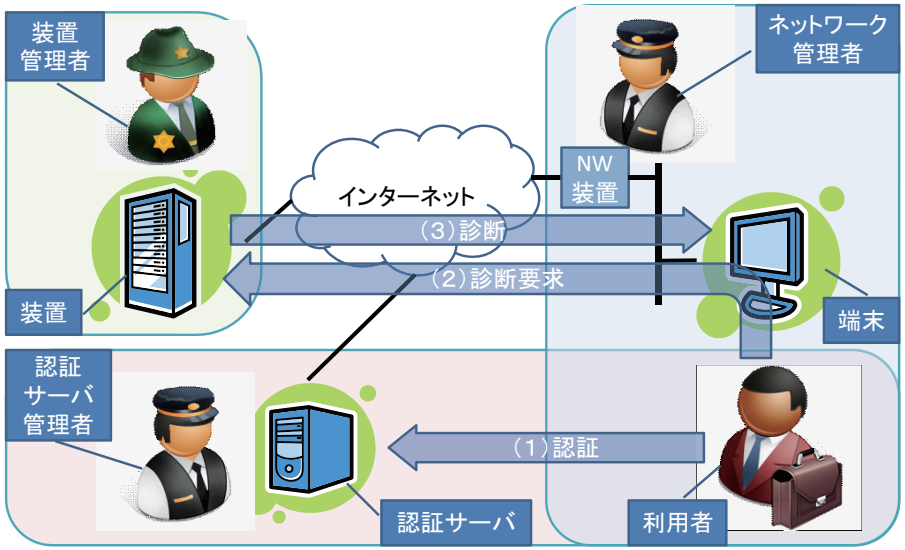


**図 1** 提案するシステムの概要
Fig. 1 Overview of proposed system

認証連携を用いることにより，診断要求をする利用者について認証することが可能となる．これにより，仮に診断行為がネットワーク攻撃と判断されても，誰が診断を要求したのかという証跡が装置管理者によって可能となる．

ポリシーを用いた承認を行うことにより，診断行為が間違ってネットワーク攻撃と判断されることを防いでいる．ポリシーは，認証サーバ管理者，ネットワーク管理者，および，装置管理者が記述する．

### 3.1 診断要求の承認

認証サーバ管理者は，認証をうけた利用者がどの端末の管理者であるかを把握している．したがって，端末の管理者が知らないうちに診断が行われることが防ぐことができるように，特定の利用者が特定の端末に対して特定の診断要求を許可・拒否するか否かのポリシーを記述する．これにより診断行為が間違ってネットワーク攻撃と判断されることを防ぐことが可能となる．

ネットワーク管理者は，装置と端末間のネットワーク構成を把握している．したがって，

診断行為が間違って経路上にあるネットワーク装置の診断を行うことを防ぐことができるように，特定の利用者が特定の端末に対しての特定の診断要求を許可・拒否するかのポリシーを記述する．これにより診断行為が間違ってネットワーク攻撃と判断されることを防ぐことが可能となる．

提案システムでは，認証サーバ管理者は管理している利用者についてのポリシーを記述する．利用者は自分が所属する組織の認証サーバを利用するが，診断要求を行う端末がその利用者が所属する組織の管理下に接続されていない場合もありえる．このような場合に，利用者が利用する端末の管理者となっているかどうかについての判断は認証サーバ管理者ができないため，ポリシー記述ができないという問題がある．また，利用されるであろう端末は，インターネット上の様々なネットワーク上に接続されているため，それらのネットワーク管理者の全てにポリシー記述を依頼することは運用上困難である．ただし，経路上にあるネットワーク装置にネットワーク攻撃がなされて運用上不都合が生じるネットワークにおいては，ポリシー記述が可能であると思われる．

そこで本提案方式ではこれらの問題を解決するために以下のような前提条件を定めた．

- 利用者，端末，診断内容の 3 つ組に対して，ネットワーク攻撃ではないと判断できる場合にはポリシーとして “Permit” 記述する．
- 利用者，端末，診断内容の 3 つ組に対して，ネットワーク攻撃であると判断できる場合にはポリシーとして “Deny” 記述する．
- 利用者，端末，診断内容の 3 つ組に対して，ネットワーク攻撃であるか否かを判断できない場合には，ポリシーを記述しない．

また，診断内容によっては，それがどの利用者であれ，どの端末であれ，ネットワーク攻撃ではないと判断できるものもあるため，装置管理者もポリシーを記述することとした．

これらの前提条件に基づいて，次のような手順により，承認する．

(1) 検索結果集合を空にする．
(2) 診断要求から利用者が認証を受けた認証サーバを特定し，その認証サーバの認証サーバ管理者が記述したポリシー群を検索する．認証サーバ管理者が記述したポリシー群が存在しない場合は検索結果集合に “Not Applicable” を追加する．そのポリシー群に関して，診断要求となる利用者，端末，診断内容の情報を元にポリシーを検索する．検索結果は単数とは限らない．その結果を検索結果集合に追加する．検索結果が空の場合は検索結果集合に “Not Applicable” を追加する．
(3) 診断要求から端末が所属するネットワークを特定し，そのネットワークのネットワーク管理者が記述したポリシー群を検索する．ネットワーク管理者が記述したポリシー群が存在しない場合は検索結果集合に “Not Applicable” を追加する．そのポリシー群に関して，診断要求となる利用者，端末，診断内容の情報を元にポリシーを検索する．検索結果は単数とは限らない．その結果を検索結果集合に追加する．検索結果が空の場合は検索結果集合に “Not Applicable” を追加する．
(4) 装置管理者が記述したポリシー群に関して，診断要求となる利用者，端末，診断内容の情報を元にポリシーを検索する．検索結果は単数とは限らない．その結果を検索結果集合に追加する．検索結果が空の場合は検索結果集合に “Not Applicabl” を追加する．
(5) 以下の条件により，診断要求を承認する．
    - 検索結果集合に 1 つ以上の要素が “Deny” である場合，あるいは，要素全てが “Not Applicable” である場合，承認しない．
    - 検索結果集合の要素全てが “Permit” である場合，あるいは，1 つ以上の要素が “Permit” であり残りの要素全てが “Not Applicable” である場合，承認する．

これにより，ネットワーク管理者や認証サーバ管理者が明らかにネットワーク攻撃であると判断できる診断要求を拒否することが可能となる．また，装置管理者，ネットワーク管理者，認証サーバ管理者の全てがポリシーを記述しない場合は，どのような診断要求においても承認されることがないため，ネットワーク攻撃となる可能性のある診断が不用意に行われないようになっている．また，この提案方式では次のような利点もある．

- 全てのネットワーク管理者がポリシーを記述しなくても運用が可能である．記述されていない場合には，装置管理者か認証サーバ管理者が記述したルールが適用される．
- 装置管理者は，利用者がネットワーク攻撃と間違って判断されるような診断を実行した場合には，当該ネットワーク管理者より対策要求を受けることとなる．このとき，当該ネットワークへの診断を禁止するポリシーを記述することによりこの要求を受けないように設定することができる．
- 認証サーバ管理者は，利用者がネットワーク攻撃と間違って判断されるような診断を実行した場合には，その利用者の証跡作業を請け負う可能性がある．悪質な利用者による不適切な診断実行を防ぐために，その利用者の利用を禁止するポリシーを記述することによりこの作業を請け負うことがないように設定することができる．

#### 3.1.1 承認方式の実装

我々は，提案システムの承認方式の実装には XACML[6] を用いることを検討している．

ネットワーク管理者，認証サーバ管理者，装置管理者が記述するポリシーは XACML に基づいた XML ファイルとして格納しておく．ネットワーク管理者および認証サーバ管理者が記述したルールについては，どのネットワークに対するポリシーであるか，どの認証サーバの管理下の利用者であるかというメタ情報も一緒に格納しておく．診断要求があれば，端末の IP アドレスをキーとして必要なファイルを検索する．また，利用者が認証を受けた認証サーバ名をキーとして必要なファイルを検索する．3 つの管理者が記述したファイルからそれぞれ PolicySet タグを根とする部分木を抽出し，その 3 つの部分木を新たに作成した PolicySet タグの配下に格納することで新しいポリシーを作成する．そのポリシーに対して，XACML にて規定されているルール結合アルゴリズムのひとつである Deny-overrides により評価することで実現できる．

### 3.2 認証連携

我々は，提案システムを Web アプリケーションとして設計を進めている．認証の連携については，現在 NII が進めている学術認証フェデレーション（学認：Gakunin) との連携が容易にできる様に Shibboleth[4] の SP として実装することを検討している．

利用者は提案システムに Web ブラウザを用いてアクセスし，検査項目を選択する．提案システムは，Web サーバにアクセスしてきた IP アドレスを診断対象とする．Shibboleth の機能を用いて利用者の属性情報を取得しする．これらの情報を基にして，診断について承認するを判断する．

### 3.3 診断項目

我々は，以下の項目を診断項目として想定している．

**帯域計測** iperf[3] を利用し，装置側がサーバ機能またはクライアント機能として稼働する．

**ポートの開閉状況診断** nmap[1] を利用し，診断要求のあった端末上のサーバソフトウェアが使っているポートなどにアクセス可能かどうかを診断する．

**経路確認** オペレーティングシステムに搭載されている traceroute コマンドを利用し，診断要求のあった端末までの経路を表示する．

**経路情報** 境界ルータが BGP プロトコルにより取得した AS PATH の情報の情報から，診断要求のあった IP アドレスが含まれるネットワークに関する情報だけを提供する．

**Web サーバ動作確認** wget[2] を利用して，診断要求のあった IP アドレス上にて稼働している web サーバにアクセス可能かどうかを判断する．

**メールサーバ確認** SNMP プロトコルを利用して，診断要求のあった IP アドレス上にて稼働しているメールサーバにアクセス可能かどうかを判断する．

これらのうち，ポートの開閉状況診断は，経路中のネットワーク機器に対するネットワーク攻撃と判断される可能性があるが，それ以外については，今のところ，ネットワーク攻撃と判断されることはないと思われる．したがって，装置管理者が記述するポリシーについては，ポート開閉状況診断以外の全ての項目について，全ての利用者，全ての IP アドレスについて “Permit” となるように記述することになる．

## 4. 関連研究

参考文献[7] において，サーバソフトウェア，クライアント OS に対応した脆弱性監査システムである．このシステムは Web サーバとして稼働している．指定したドメイン名に対して稼働しているサーバソフトウェアへの通常の問合せによりバージョン情報を取得したり，自組織内の Windows の脆弱性修正プログラムのインストール状況を検査する．Web ブラウザを使う点では提案システムと同じである．ただし自組織に限っているため，認証の仕組みがない．提案システムでは自組織以外のネットワークからの診断を想定している点が異なっている．

参考文献[8] において，専門知識の乏しい管理者でも利用可能なネットワーク資源脆弱性自動検査システムが提案されている．これは Nessus[5] を利用した脆弱性検査を Web サーバ上で実行する方式で実装されている．Nessus は様々な疑似的なネットワーク攻撃を行い，検査対象となる IP アドレスを持つ計算機の脆弱性を調べるシステムである．Web ブラウザを使う点では提案システムと同じである．このシステムでは本論文で議論した様に，ネットワーク構成によっては，経路中のネットワーク装置の脆弱性を検査を行ってしまう可能性がある．提案システムでは，組織外のネットワークから検査を行うことを想定し，認証の仕組みを入れている点で異なっている．

## 5. おわりに

本論文では，関係する管理者に余計な手間をかけることなく，遠隔からネットワークの性能や機能についての診断を容易に実現できるシステムについての構想について述べた．このシステムの特徴は，認証連携を用いている点と認証サーバ管理者，ネットワーク管理者，装置監視者が記述するポリシーを用いて診断要求を承認している点にある．各管理者は適切にポリシーを記述することにより，間違ってネットワーク攻撃と判断されるような診断行為が行われないようにすることができる．

現在は，このシステムは構想段階である．今後実装を行い，実環境上でテストをし，その

Vol.2010-IOT-9 No.12
2010/5/14

有効性を検証していく．

**謝辞** 情報処理学会 IOT 研究会の運営委員の皆様とのフリーディスカッションからこの研究のアイディアをいただきました．ここに謹んで感謝の意を表します．

## 参 考 文 献

1) Gordon Lyon: nmap, http://nmap.org/ (Accessed 2010 Apr 10).
2) Hrvoje Nisksic: GNU wget, http://www.gnu.org/software/wget/ (Accessed 2010 Apr 10).
3) iperf 2.04: http://sourceforge.net/projects/iperf/ (Accessed 2010 Apr 10).
4) Marlena Erdos and Scott Cantor: Shibboleth Architecture v4, http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v04.pdf (Accessed 2010 Apr 10) (20011121).
5) Tenable Network Security: Nessas, http://www.nessus.org/nessus/ (Accessed 2010 Apr 10).
6) Tim Moses, ed.: eXtensible Access Contorl Markup Language (XACML) version 2.0, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml (Accessed 2010 Apr 10).
7) 毛利公美，高橋秀郎，広岡俊彦，曽根直人，森井昌克：ネットワーク資源に対する脆弱性自動監査システムの開発 (オフィスインフォメーションシステム及び一般)，電子情報通信学会技術研究報告. OIS, オフィスインフォメーションシステム， Vol.104, No.69, pp.13–18 (20040514).
8) 蓮井亮二，毛利公美，森井昌克：管理・運用を容易にするネットワーク資源脆弱性自動検査システムの開発 (Web サービスベースのオフィスアプリケーション・ネットワーキング・マネジメント及び一般)，電子情報通信学会技術研究報告. OIS, オフィスインフォメーションシステム， Vol.105, No.529, pp.17–22 (20060113).