

ディレクトリサービス情報とネットワークトラフィックを用いた 内部分離ネットワーク構築手法

長谷川 皓一† 山口 由紀子†† 嶋田 創†† 高倉 弘喜‡

†名古屋大学 大学院情報科学研究科
464-8601 愛知県名古屋市千種区不老町
hasegawa@net.itc.nagoya-u.ac.jp

††名古屋大学 情報基盤センター
464-8601 愛知県名古屋市千種区不老町
{yamaguchi,shimada}@itc.nagoya-u.ac.jp

‡国立情報学研究所
101-8430 東京都千代田区一ツ橋 2-1-2
takakura@nii.ac.jp

あらまし 近年の巧妙化するサイバー攻撃に対し、ネットワークの内部分離設計は有効な対策の1つである。ネットワークを複数のセグメントに分割し緻密なアクセス制御を行うことで、マルウェアの活動抑制、感染端末の検知や隔離などを行い易くする。しかし、内部分離設計を行うには莫大な手間と運用コストが必要であるため、一般的な企業では適切なセグメント化とアクセス制御が行われていない。そこで本研究では、ディレクトリサービスから取得する人事情報やアクセス権限を基にネットワークを分割し、ネットワークトラフィックから不必要な通信可能区間を判別し、アクセス制御を行うことにより容易に内部分離設計を構築する手法を提案する。

A Construction Method of Separated Internal Network using Directory Service Information and Network Traffic Data

Hirokazu Hasegawa† Yukiko Yamaguchi†† Hajime Shimada††
Hiroki Takakura‡

†Graduate School of Information Science, Nagoya University
Furo-cho, Chikusa-ku, Nagoya, 464-8601, JAPAN
hasegawa@net.itc.nagoya-u.ac.jp

††Information Technology Center, Nagoya University
Furo-cho, Chikusa-ku, Nagoya, 464-8601, JAPAN
{yamaguchi,shimada}@itc.nagoya-u.ac.jp

‡National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, JAPAN
takakura@nii.ac.jp

Abstract Separating network and controlling access among separated sub-networks are effective countermeasure against cyber attacks. Such countermeasure can prevent unintended communication by malware. Furthermore we can quickly sense infected hosts, estimate their influence and isolate them from the network. However, enormous effort and operational cost are required to construct such a separated network and proper access control. As a solution, we propose a construction method of separated internal network that refers directory service to obtain employee information and his/her access authority for the separation. Furthermore, we use network traffic data to determine unnecessary communication among separated sub-networks.

1 はじめに

近年、サイバー攻撃の巧妙化により、個人情報漏洩などといった深刻な被害が後を絶たない。特に標的型攻撃と呼ばれるサイバー攻撃の場合には、特定の企業や国家機関などの攻撃対象に対して情報窃取や破壊活動を目的として行われるため、事前の調査活動により攻撃対象に特化した専用のマルウェアが使用される場合が多い。このようなマルウェアは施されているセキュリティ対策をすり抜け、他の通信に紛れて活動するため、その検知や対策が難しくなっている。このような巧妙化するサイバー攻撃に対し、企業内ネットワークを複数のセグメントに分割し、セグメント間の緻密なアクセス制御を行うネットワーク内部分離設計は有効な対策の1つである。適切なネットワークの分離とアクセス制御を行うことにより、マルウェアの活動抑制、感染端末の検知や隔離などが行い易くなる。しかし、内部分離設計を行うには莫大な手間と運用コストが必要であるため、適切なセグメント化とアクセス制御が行えていない企業が多い。本稿では、ディレクトリサービスから取得する人事情報やアクセス権限を基にネットワークを分割し、分割したセグメントについてネットワークトラフィックから不必要な通信可能区間を判別し、アクセス制御を追加することにより容易に内部分離設計を構築する手法を提案する。

2 近年のサイバー攻撃と企業内ネットワーク

巧妙化する攻撃に対し、従来からの企業内ネットワークの運用形態では特に対応が難しい。従来の企業内ネットワークでは、単一のセグメントでの運用形態が多く用いられてきた。これは社員が利用するパソコンやOA機器、重要な情報が保管されたサーバなどがすべて同じセグメントに接続され各端末同士が自由に通信を行うことが可能な状態である。また、セキュリティ対策は内部ネットワークとインターネットとの境界部にファイアウォールやIDS(Intrusion Detection

System, 侵入検知システム)を設置することで不正通信の遮断を行うといった、外部からの攻撃の侵入を防ぐための対策が行われる。

先述のように、標的に特化したマルウェアはセキュリティ対策をすり抜けてしまう場合が多く、侵入を防ぐための対策のみでは侵入を許してしまう。その場合、従来の運用形態のネットワークや適切なセグメント化やアクセス制御が行われないネットワークでは、マルウェアが自由に通信が行えるため、活動を行い易い環境であると言える。そのため、マルウェアによる感染の察知やその影響範囲の特定が難しく、感染端末の隔離などの感染拡大の防止も困難である。結果として、マルウェアがネットワークに侵入した場合には検知できない、もしくは対策が取れないまま情報漏洩などの被害を受けてしまう。または侵入を検知したが感染範囲や活動内容の特定が行えないため、インターネットから内部ネットワークを切り離すことにより被害を防止するが業務に深刻な影響を与えてしまう。

3 ネットワーク内部分離設計

3.1 概要

ネットワークの内部分離設計は、標的型攻撃への有効な対策の1つである。単一セグメントのネットワークを複数のセグメントに分割し、セグメント間の不必要な通信を遮断するといった緻密なアクセス制御を行う。これにより、マルウェアが行う悪意ある通信を抑制することが可能である。また、禁止されている通信区間でマルウェアが通信を行おうとする挙動を察知しやすくなり、感染端末の早期発見につながる。感染端末の通信可能区間からマルウェアによる影響範囲の特定が可能なため隔離すべき端末の迅速な判断が行え、またアクセス制御により端末の隔離も容易に行うことが可能となる [1]。昨今ではこのようなネットワーク設計が推奨されている [2]。

適切な内部分離設計が困難な理由として、構築のための膨大な手間と運用コストが挙げられる。細かいネットワークの分割およびアクセス制御を行うためには、分割のための詳細な基準

を決定し、各端末の利用者がどのような通信が必要であるか等の判断が必要となる。これらを決定するためには、利用者ごとの担当業務を含む人事情報や各業務内容に応じてどのような通信が必要であるかといった様々な情報を利用する必要がある。ネットワーク管理者のみがこれらの必要な情報をすべて収集し、アクセス制御の判断を下すのは困難である。その上、企業内では人事異動等によりネットワーク構成が変更される場合が多々あるため、その都度ネットワークを再度分割し直し、アクセス制御を設定することは非常に手間がかかる。

3.2 関連研究

安全なネットワークを構築するための仕組みは様々なものが研究、開発されている [3][4]。また、VLAN を容易に構築可能な株式会社イガの VLAN .Config といった製品なども存在する。京都大学のキャンパスネットワークでは、ネットワーク設計システムを自動化し、20000 ポート、4000VLAN という規模の管理運用が可能となっている [5]。しかしながら、細かいアクセス制御などを設計するためにはすべての VLAN ごとに細かいセキュリティポリシーを定義する必要があるなど、ネットワーク管理者の負担も残る。

我々は内部分離設計の構築から、インシデント発生時の分析や対策の補助を行うための仕組みを提案してきた [6]。これまでの研究では、ネットワーク管理者が業務内容と各業務で用いる情報のネットワーク内での流れをワークフローとして入力し、その情報を基にネットワークを部署単位などに大まかに分割する。さらに、構築したネットワーク上のトラフィックから通信が行われていないセグメント間のアクセス制御を行う。このネットワークトラフィックからの不必要な通信の特定を繰り返し行うことで、アクセス制御を徐々に追加していくものであった。

しかし、ワークフローの入力を行うための情報収集は依然ネットワーク管理者の負担となるうえ、大まかに分割されたネットワークではその後のアクセス制御の改良を繰り返しても限界がある。また、ネットワークの構成変更の際にはワークフローを再度入力し内部分離設計を構

築し直す必要がある。そこで本稿では、これらの問題を解決するために企業内ネットワークで利用されるディレクトリサービスの情報によるネットワークセグメントの細分化と、ネットワークトラフィックを利用したアクセス制御の更新による内部分離設計構築手法を提案する。

4 提案手法

4.1 提案手法の概要

提案手法は、ネットワーク内のディレクトリサービスより取得する情報を基にネットワークの分割を行うことにより、ネットワーク管理者によるワークフロー等の情報の入力の手間を省き、より細かいネットワーク分割を可能とする。ディレクトリサービスとは、ネットワーク上で利用可能なリソースを管理するための仕組みで、企業内ネットワークなどで用いられる。本稿ではディレクトリサービスとして、一般的に利用される Microsoft 社の Windows Server で提供される Active Directory(以降、AD) を想定する。分割されたネットワークにおいて、ネットワークトラフィックにより不必要な通信可能区間を判別し、アクセス制御の追加を行う。

4.2 提案手法の構成

提案手法の構成を図 1 に示す。提案手法は、

- ネットワーク設計生成モジュール
- 人事情報取得モジュール
- 抽出モジュール
- 設定モジュール
- 人事情報データベース
- ネットワーク構成情報データベース
- トラフィック統計データベース

から成り、ネットワーク設計生成モジュールは提案手法の主な機能となるネットワークセパレーティング、ネットワークリファインメント、ネットワークリコンストラクションの 3 つの機能を

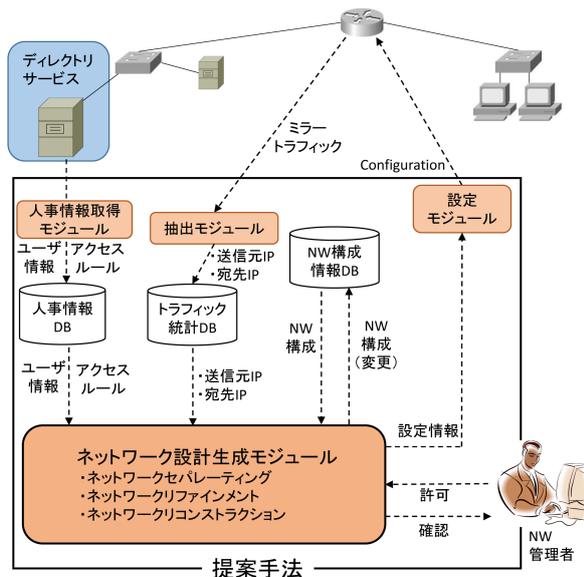


図 1: 提案手法の構成図

有する．ネットワーク内においてディレクトリサービスからのデータ取得および、ネットワーク機器からのトラフィック収集，機器設定を行う．

4.3 ネットワーク内のデータ取得

提案手法では，あらかじめネットワーク内の情報をデータベース内に保持しておく．従業員に関する情報として人事情報データベースを用意する．このデータベースでは，各従業員の所属，役職，ユーザアカウントおよび，共有ファイルへのアクセスルールを保持する．これらの情報は AD において管理を行い，人事情報取得モジュールが AD より取得する．アクセスルールに関しては，4.5 節にて後述する．

ネットワーク内の機器からミラートラフィックを取得し，抽出モジュールによって送信元 IP アドレス，宛先 IP アドレスのみを抽出し，トラフィック統計データベースにおいて保持する．

ネットワーク構成情報データベースでは，ネットワークに接続される PC 等の端末，サーバ，ネットワーク機器や IP アドレスなどのネットワーク構成を管理する．各端末については，使用者のユーザアカウント，MAC アドレス，所属先ネットワークアドレスを保持する．各サーバやネットワーク機器に関しては，IP アドレス，

MAC アドレスを保持する．それに加え，ネットワークアドレスの一覧と，各機器間の接続関係を管理する．これらの情報は，一般的な企業ネットワークにおいてはエージェントや DHCP サーバから情報収集を行う資産管理用のソフトウェアなどにより管理サーバ等に保持されている．本稿ではこのような管理機構が存在しない場合は想定せず，管理サーバ等から情報を取得することとする．

4.4 ネットワークセパレーティング

この機能では，はじめにネットワークを部署ごとに大まかに分割し，分割されたネットワーク内で不必要な通信区間を特定しアクセス制御を行う．ネットワークセパレーティングの構成を図 2 に示す．

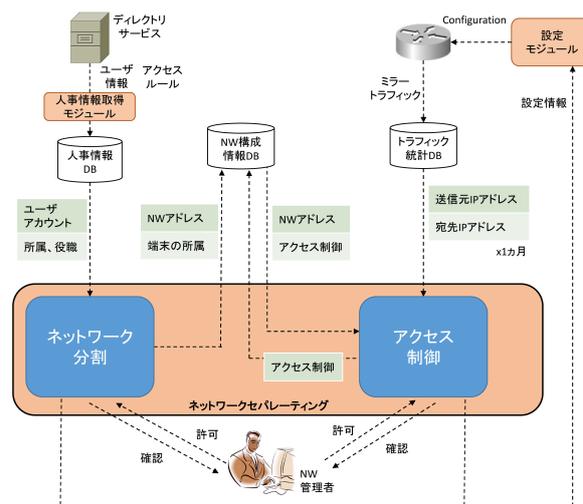


図 2: ネットワークセパレーティング

4.4.1 部署によるネットワーク分割

ネットワーク分割コンポーネントが人事情報データベースより，各ユーザのアカウントと所属を取得する．また，ネットワーク構成情報データベースより，現在のセグメントのネットワークアドレスの一覧を取得する．取得した情報から，部署ごとにセグメントを作成し，異なるネットワークアドレスを割り当てる．また，各ユー

ザの使用端末から、各端末がどのセグメントに属するか決定する。

ネットワーク内のファイルサーバや DHCP サーバ等、サーバは1つのセグメントにまとめ、それぞれ IP アドレスを静的に割り当てる。サーバの一覧はネットワーク構成情報データベースより取得し、サーバセグメント用のネットワークアドレスを割り当てた上で各サーバの IP アドレスを決定する。

これらの変更内容についてネットワーク管理者に対して確認を行い、許可を受ける。その後、ネットワーク構成情報データベースが保持しているネットワークアドレスに作成した各部署のネットワークアドレスを追加する。また、各ユーザのアカウントと紐付けされた端末の所属先ネットワークアドレスを更新する。サーバの場合には、静的に割り当てた IP アドレスを更新する。ネットワーク構成情報データベースの更新内容に基づき、設定モジュールがネットワーク機器に反映させる。DHCP サーバの設定を更新することで、MAC アドレスベースに各端末の IP アドレスの変更を行う。ただし、各端末の IP アドレスは即座に変更されないため、各端末上で割り当てられている IP アドレスの解放を行うなどの必要がある。

4.4.2 アクセス制御

分割されたネットワークにおけるトラフィックを収集し、それらを基にセグメント間の不必要な通信可能区間を特定し、アクセス制御を行う。アクセス制御コンポーネントがトラフィック統計データベースからネットワーク分割後1ヶ月等の一定の長期間の送信元 IP アドレス、宛先 IP アドレスを取得する。また、ネットワーク構成情報データベースからネットワークアドレスの一覧と、現在適用されているアクセス制御の一覧を取得する。取得した情報を用いて、同セグメントの端末同士の通信、セグメント内でのブロードキャスト、外部ネットワークとの通信を排除し、セグメントを跨ぐ通信のみを抽出する。抽出した結果から、アクセスが許可されているにもかかわらずトラフィックが観測されない区間を特定し、不必要な通信可能区間の候

補として管理者に通知する。管理者の許可を得た後、その区間の通信を遮断するアクセス制御をネットワーク構成情報データベースに登録すると共に、設定モジュールによりネットワークに反映させる。

4.5 ネットワークリファインメント

ネットワークセパレーティングにより部署ごとのネットワーク分割およびアクセス制御を行った後、より細かくネットワーク分割を行い、アクセス制御を追加する。ネットワークリファインメントでは、以下に述べるネットワークの細分化とアクセス制御の追加を行う。この2つの行程を繰り返し行うことにより、ネットワークの内部分離を徐々に細かくしていくことが可能となる。これに伴い、ネットワークのセキュリティレベルを向上させることが可能となる。

4.5.1 アクセス権限によるネットワークの細分化

ネットワークをより細かく分割するため、人事情報データベースが保持するアクセスルールを利用する。AD では、ダイナミックアクセス制御機能による共有フォルダなどのリソースへのアクセス制御が可能である。ユーザの属性値(例えば、所属 = 経理部、役職 = 部長)に応じたアクセス権限(例えばフルコントロールアクセス可能)をアクセスルールとして定義する。その上で、リソースは AD 上の適切なアクセスルールを選択する。前述の例のようなアクセスルールを選択したリソースには、経理部、部長という属性を持つユーザのみがこのリソースにフルコントロールアクセス可能となる。このアクセスルールは AD が管理するため、これらを人事情報取得モジュールが取得し、人事情報データベースにおいて保持する。

アクセスルールを用いて、ネットワークをより細かく分割する。1回の分割につき1つのアクセスルールを使用し、分割されているセグメント内において属性値によりアクセスルールが適当されるユーザとされないユーザに分類されるかどうかを判定する。例えば先述の例のよう

に、経理部という部署属性と部長という役職属性を使用したアクセスルールの場合、経理部のセグメント内においてこのルールが適用される部長属性を持つユーザと、ルールが適用されないそれ以外のユーザに分類できるはずである。このような場合に、この分類によってセグメントを分割する。

4.5.2 アクセス制御の適用

ネットワークの細分化を行った後、細分化を行う以前の1つのセグメントに対して適用されていたアクセス制御をネットワーク構成情報データベースから取得し、同じアクセス制御を細分化されたそれぞれのセグメントに対して適用する。それに加え、ネットワークセパレーティングと同様に1ヶ月等の長期間のミラートラフィックから送信元/宛先IPアドレスをトラフィック統計データベースに蓄積する。この情報を用いて、長期間通信が行われない区間を不必要な通信可能区間の候補として抽出し、管理者の判断によりアクセス制御を追加適用する。

ただし、アクセス制御について変更が行われない場合が存在する。例えば、先述の例のように経理部内で役職属性を用いるアクセスルールにより、部長属性を持つユーザとそれ以外のユーザを異なるセグメントに分割したとする。この場合、このアクセスルールを適用したリソースと、以前より経理部のユーザが利用していたリソースが経理部の1つのサーバ内に格納されている場合などは、分割された2つのセグメントは共にこの1つのサーバを利用するため、新たにアクセスを遮断する区間は存在しない。このような場合には、このネットワーク分割を解除する。

4.5.3 実行例

ネットワークリファインメントの実行例を図3に示す。経理部には1人の部長と2人の従業員が所属し、サーバセグメント内に経理部が使用するサーバが2台設置されている。この時、経理部サーバ1の共有フォルダには、所属が経理部のユーザにフルアクセスコントロールを許可

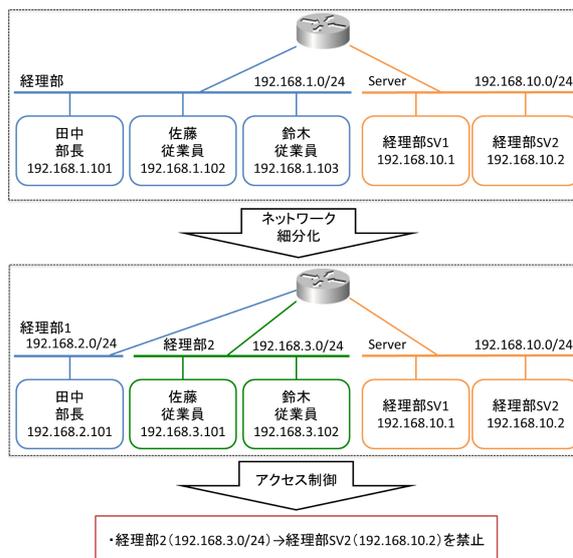


図 3: ネットワークリファインメントの実行例

するアクセスルールが設定されているものとする。また、経理部サーバ2の共有フォルダには、所属が経理部かつ役職が部長のユーザにフルアクセスコントロールを許可するアクセスルールが設定されているものとする。この場合、経理部サーバ1に適用されているアクセスルールは、経理部のユーザ全員に適用されるため、ネットワークリファインメントでは適用されない。経理部サーバ2に適用されているアクセスルールでは、役職に応じたアクセス権が与えられているため、経理部内でアクセス可能なユーザとそうでないユーザが存在することとなる。そこで、経理部セグメントを部長が属するセグメントと、それ以外が属するセグメントに細分化が行われる。

次に、細分化が行われたネットワークにおいて、ミラートラフィックの収集を長期間を行う。その結果、経理部1セグメントからは経理部サーバ1と経理部サーバ2のそれぞれに対してアクセスが存在するのに対して、経理部2セグメントからは経理部サーバ1にのみアクセスが存在する。そこで、経理部2セグメントから経理部サーバ2への通信を不必要な通信可能区間の候補としてネットワーク管理者に確認し、許可を得た後にアクセス制御を追加する。

4.6 ネットワークリコンストラクション

人事異動や、社員の入社などによりネットワークの構成が変更された際には、ネットワークリコンストラクションを行う。ネットワーク管理者の変更通知を受け、現在の人事情報データベースに登録されているユーザアカウントとそれぞれの所属、役職を取得する。その後、人事情報取得モジュールを用いて、AD上の情報により人事情報データベースを更新する。その上で再度人事情報データベースからユーザアカウントとそれぞれの所属、役職を取得し、変更箇所を特定する。以下のように新たに配置されたユーザの種別に応じた変更を行う。

- ユーザが他の部署より異動した場合
引き継ぎ等のため、新たなユーザが以前に所属していた部署や使用していたサーバと通信を行う可能性がある。そのため、新たなセグメントを作成し、新たなユーザはこのセグメントに配置する。その上で、このセグメントへのアクセス制御として、部署内で新たなユーザと同等の役職のユーザが所属するセグメントと同様のアクセス制御を設定し、さらにこのユーザが以前所属していたセグメントで許可されていた通信を可能とするようにアクセス制御を追加する。最終的には、部署内の同等の役職のユーザが所属するセグメントに再配置し、新たに作成したセグメントは削除する必要がある。この基準としては、1ヶ月後などの期間の設定、管理者による通知、トラフィックの分析により一定期間通信がない場合などが考えられる。
また、ユーザが以前に所属していたセグメントについては、そのユーザが単独で分割されていた場合には当該セグメントを削除し、それ以外の場合には変更は行わない。
- 新入社員などの新規ユーザの場合
新規のユーザの場合には、配置された部署内において現在存在するセグメントにユーザを配置する。配置するセグメントは、部署内において最も役職が低いユーザが属す

るセグメントとする。また、このセグメントのアクセス制御は変更しない。

5 実装に関する検討

5.1 ディレクトリサービス

本稿では、一般的な企業内ネットワークでの利用例が多いADを想定した。AD以外のディレクトリサービスや、ダイナミックアクセス制御機能を有しないWindows Server 2008以前のADを用いた実装を行う場合、アクセスルールのようにユーザのアクセス権限に関する情報をディレクトリサービスから一括して取得することが不可能である。そのため、各ファイルサーバごとに全てリソースに設定されているアクセス権限を取得する必要がある。

5.2 ネットワークの設定

ネットワーク分離設計を生成した後、実際にネットワークに対して設計を反映させるにはいくつかの手法が考えられる。1つは、物理ネットワーク上にIEEE802.1Q等によるVLANを構築し、ルータなどのネットワーク機器のアクセスコントロール機能を用いてアクセス制御を適用する手法である。この場合、既存の製品などを用いてネットワーク内のルータなどを自動的に設定することにより、設計を反映させることが可能である。

また、Software-Defined Network(SDN)の技術により、ソフトウェアによりネットワークを動的に変更する手法がある。ただし、SDNに対応したネットワーク機器(Openflowスイッチ等)の導入のためのコストが必要となる。

6 おわりに

本稿では、巧妙化するサイバー攻撃への有効な対策の1つであるネットワーク内部分離設計を容易に構築するために、ディレクトリサービス情報とネットワークトラフィックを用いた内部分離ネットワーク構築手法を提案した。提案手

法では、ディレクトリサービスから取得できるユーザ情報およびアクセス権限と、ネットワーク上のトラフィックから分析した通信状況を基にネットワークを複数セグメントへと分割を行い、またトラフィックの分析により不必要な通信可能区間を判別しアクセス制御を行うことによって、容易に内部分離ネットワークを実現することが可能となる。

今後、提案手法を実装し、実環境において検証実験を行う。また、ネットワークリファインメントによりセグメントの分割を細分化していった際、不必要に細かい設計はネットワーク機器の負荷増加となり、またVLANを利用する際にはVLAN数の上限の問題がある。そのため、不必要な分割やアクセス制御のない適切な状態をネットワークごとに決定する手法を検討する必要がある。また、本稿ではIPアドレスを用いてアクセス制御を追加する手法を提案したが、今後は社員をベースで分割とアクセス制御を行う方法を検討する必要がある。

謝辞

本研究は平成25年度総務省情報通信技術の研究開発「サイバー攻撃の解析・検知に関する研究開発」の支援を受けた。

参考文献

- [1] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. Computer security incident handling guide. NIST Special Publication 800-61, 2012.
- [2] 独立行政法人情報処理推進機構セキュリティセンター. 「高度標的型攻撃」対策に向けたシステム設計ガイド. 2014.
- [3] James Burns, Aileen Cheng, Proveen Gurgung, S Rajagopalan, P Rao, D Rosenbluth, Alathurai V Surendran, and DM Martin Jr. Automatic management of network security policy. In *DARPA Information Survivability Conference &*
- Exposition II, 2001. DISCEX'01. Proceedings*, Vol. 2, pp. 12–26. IEEE, 2001.
- [4] Leonidas Lymberopoulos, Emil Lupu, and Morris Sloman. An adaptive policy-based framework for network services management. *Journal of Network and Systems Management*, Vol. 11, No. 3, pp. 277–303, 2003.
- [5] 高倉弘喜, 江原康生, 宮崎修一, 沢田篤史, 中村素典, 岡部寿男. 安全なギガビットネットワークシステム kuins-iii の構成とセキュリティ対策. 電子情報通信学会論文誌 B, Vol. 86, No. 8, pp. 1494–1501, 2003.
- [6] Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada, and Hiroki Takakura. Proposal of a network control system to detect, analyze and mitigate targeted cyber attacks. 電子情報通信学会技術研究報告. IA, インターネットアーキテクチャ, Vol. 113, No. 240, pp. 1–6, 2013.