社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

情報通信システムセキュリティ研究会
Information and Communication System Security
ICSS2008-06 (2008-09)

アクセス制御の違いによるネットワークシステムの特性変化に関する考察

金岡 晃† 加藤 雅彦†† 藤堂 伸勝† 岡本 栄司†

† 筑波大学大学院システム情報工学研究科 〒305–8573 茨城県つくば市天王台 1–1–1
†† アイアイジェイ テクノロジー 〒101–0051 東京都千代田区神田神保町 1-105 神保町三井ビルディング
E-mail: †{kanaoka,okamoto}@risk.tsukuba.ac.jp, ††masa@iij-tech.co.jp, †††toudou@cipher.risk.tsukuba.ac.jp

あらまし モデル化されたネットワークシステムのアクセス制御解析を網羅的に行なった。その結果、アクセス制御が適切にされていないケースと適切にされているケースでは出線数分布に大きな差異が見つけられ、さらに適切なアクセス制御状態においては利用されるネットワーク機器にかかわらず出線数分布がほぼ一定になることが判明した。
キーワード ネットワークシステム、アクセス制御

A study on a property difference in networked systems from access control view

Akira KANAOKA†, Masahiko KATO††, Nobukatsu TOUDOU†, and Eiji OKAMOTO†

† University of Tsukuba 1–1–1, Tennodai, Tsukuba, 305-8573, Ibaraki, Japan
†† IIJ Technology, Inc. 1–105 Kanda Jinbo-cho, Chiyoda-ku, 101–0051, Tokyo, Japan
E-mail: †{kanaoka,okamoto}@risk.tsukuba.ac.jp, ††masa@iij-tech.co.jp, †††toudou@cipher.risk.tsukuba.ac.jp

Abstract Integration of a networked system (NS), which consists of various network equipment and uses LAN technology to provide a service, has become increasingly important. However, there have been few studies in on the integration of secure NSs. In this paper, we analyze the characteristics of NS using NS expression model. The obtained results suggest that a well-designed NS from an access control viewpoint has a fixed link distribution, regardless of connection restriction.
Key words Networked System, Access Control

1. まえがき

インターネットを通じてサービスを提供するシステムでは、1 台のサーバのみでサービスを提供していることは稀であり、多くはルータやスイッチ、ファイアウォール、サーバなど機器が多岐にわたり、さらにはサーバ自身も Web サーバ、アプリケーションサーバ、そしてデータベースなど、さまざまなネットワーク機器を組み合わせ、LAN 技術を利用することで 1 つのサービスが提供されている。このようなシステムをネットワークシステム（Networked System:NS）と呼ぶこととする。

近年のインターネットを通じたビジネスの拡大により、NS の重要性は高くなっており、そこにはコスト、冗長性、拡張性、そしてセキュリティなど多くの性質が求められている。これら性質を満たすために、単純な NS でさえその構築は複雑なものとなる。しかし NS の構築や運用はその重要性にもかかわらず、いまだに経験を多く積んだ技術者の経験に依存したものとなっており、そこには学術的視点からみた構築・運用方法論や理論などはほとんどなされていない。

システムやネットワークの設計に関してはこれまで多くの研究がなされていたが、それらのほとんどは単一機能に絞られた複数システムの協調などに焦点が当てられている。しかし NS は、さまざまな機器がさまざまな機能を提供しているものであり、単一機能での効率化や最適化を図る既存研究を直接適用することは難しい。またそれら複数機能を 1 つの表現上に集約可能とするモデルも検討されていなかったが、金岡らにより提案された NS の表現モデルにより、複数機能を 1 つの表現上に集約することを可能とした [1]。

本研究では金岡らのモデル（NSQ モデル）を用いて NS のアクセス制御状態の特性を解析した。解析は各ノードから出るリンク数の分布（次数分布）を対象に行った。その結果、アクセス制御が適切に施されている NS では次数分布がある一定の分布形状を見せることがわかり、その特徴は NS の各機器（モ

ジュール）の接続制限にかかわらずに現れることが判明した。

2 章ではこれまでの研究を述べ、3 章において解析対象となる NS 群の生成方法を解説する。そして 4 章において次数分布の解析を行い、特徴の変化を見る。最後に 5 章においてまとめる。

2. 既存研究

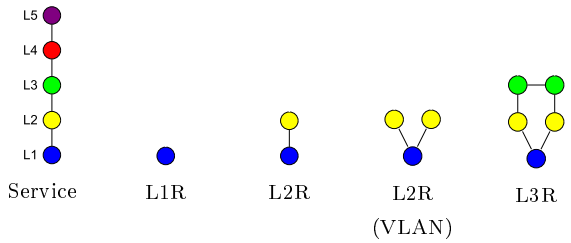
金岡らによる NS 表現モデル [1] は、複数機器の特徴を失うことなく NS を表現可能にした。本論文では金岡らによるモデルを NSQ モデルと呼ぶこととする。

NSQ モデルでは、機器やサーバなど機能を提供する実体をモジュールと定義し、モジュールは各レイヤにおいてノードを持つことで各レイヤでのサービス（通信の始点・終点・中継点）をそれぞれ表現している。レイヤ定義は表 1 に示すように定義されている。またモジュールの例を図 1 に示す。ここで L1R、L2R、L3R はそれぞれのレイヤでの中継モジュールを表している。例えば L1R は Hub、L2R は L2 スイッチなどがそれにあたる。

表 1　レイヤ定義

Layer 5	Abstracted service (WWW, DNS, etc.)
Layer 4	Services by port number (80, 53, etc)
Layer 3	IP
Layer 2	MAC address space
Layer 1	Physical object

図 1　モジュール例



それぞれのノードはリンクにより接続される。リンクには 2 つの種類があり、1 つは異なるモジュールを同じレイヤで接続するリンクであり、もう 1 つは同じモジュール内で異なるレイヤを接続するリンクである。前者は当該レイヤ上での直接通信が可能であるかを表現するものであり、後者はモジュール内のノード間の関係を示すものである。

これによりさまざまなモジュールを含んだ NS を、機能の特徴を失うことなく同一モデル上に展開できることが可能になった。図 2 は従来の表現方法としての NS の例であり、図 3 は同一 NS を NSQ モデルに適用し可視化したものである。

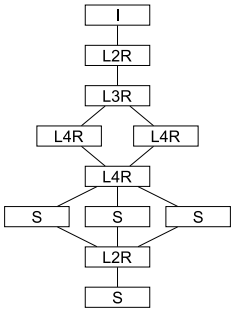


図 2　従来の NS 表現例

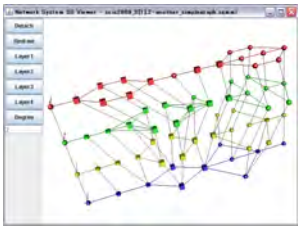


図 3　NSQ モデルによる NS 表現例

3. ネットワークシステムの構築

NSQ モデルにより表現された NS がどのような特徴を持つかを知るために、すべての NS の種類を網羅して解析を行うことが理想的である。しかし、すべての NS の種類を網羅することは種類数の多さから現実的ではなく、さらに現実の構築では設計され得ない NS の種類を含んでしまうことなどからその解析結果が決して最適な NS 設計に適したものとはならない。そこで本研究では各モジュールの接続制限を加えることにより、解析対象となる NS の範囲を絞った。

本節では、接続制限の方法と、解析対象となった NS 群の構築方法について解説をする。

3.1 接続の制限

解析対象となる NS 群を洗い出すために、まず NS がどれだけの種類を持つかを調査した。NS はモジュールの集まりであり、各モジュールは基本的に 1 つの L1 ノードを持つ。そこでモジュール間接続自体がどれだけの種類を持つかとして、L1 ネットワークの種類数を調査した。表 2 はノード数ごとのネットワーク種類数である。ノード数 n の L1 ネットワーク群の種類数を求めるには、ノード数 $n-1$ の L1 ネットワーク群にあらたに 1 つのノードを加えることで求める。しかしそれでは同型が発生するために同型判定を行う。表 2 ではノード数 8 以上は同型判定後の種類数を記載していないが、おおむね判定前の 6 割程度の値となっているためその数の多さは類推可能であろう。

表 2　Number of L1 networks: Edge Nodes

# of node	Before iso. check	After iso. check
2	1	1
3	6	6
4	42	27
5	474	294
6	12,606	7,121
7	470,742	283,482
8	26,364,210	N/A
9	2,181,981,354	N/A
10	292,914,780,702	N/A

モジュール間としての接続数でこれだけの膨大な数になり、さらにモジュール間においてどのレイヤで通信が行われるか・各モジュールが各レイヤでいくつのノードを持つか、などその数はさらに膨大なものとなり、解析を行う対象として現実的で

はなくなる。

さらに、これらの中には現実的には構築され得ない NS が存在する。たとえば 2 つの経路を持つ冗長構成系において、片方がルータ（L3R）を含むのに対し、もう片方はハブ（L1R）のみを含むケースなどがそれに当たる。

そこで、接続制限を加え、解析対象となる NS を絞ることとした。

3.1.1 モジュール間接続制限

実際に構築されている NS では、ファイアウォールやルータなどのネットワーク機器に、直接サーバが接続されていることは少なく、多くは L2 の中継器（L2R）であるスイッチを介した接続がなされている。また直接接続されているケースでも、そのネットワーク機器がスイッチの機能を持っていることがあるなど、仮想的に 2 台の機器となっていると考えると、すべての機器はスイッチ（L2R）と接続されているという接続制限は非現実的な接続制限ではない。そこで解析対象の NS に「L2R 以外のモジュールはかならず L2R と隣接しており、L2R は直列しない」という接続制限を加えることとした。

3.1.2 接続制限下での L1 ネットワーク種類数

接続制限を加えたときの L1 ネットワーク種類数は表 3 に示した通りであり、表 2 と比較して大幅な対象数の減少を実現している。

表 3　接続制限下での L1 ネットワーク種類数

ノード数	種類数
2	0
3	1
4	1
5	6
6	21
7	121
8	1,061
9	10,782
10	N/A

3.2 抽象サービスノードにおける部分ネットワーク

表 3 では、L1 ノード数 9 までの NS 種類数が求められたが、現実の NS では機器の数が 100 以上に達するものは珍しくなく、さらなるノード数での網羅が求められる。そこで、さらなる種類数の減少を実現するために、NS の機能要件を利用した。

顧客が NS 構築を依頼した場合を考慮するとき、そこには顧客より NS の機能要件が与えられ、それを基に設計が行われる。例えば、フロント Web サーバ、アプリケーションサーバ、データベース等が要件より選択され、そこにそれら機能の関連付けを行う。NSQ モデルにおける L5 レイヤのノードはそれら機能要件により現れた機器そのものであり、L5 ネットワークはそれら機能の関連を示したネットワークである。

さらに実際に構築されている NS を見ると、機器の配置や構成は、それら機能要件に基づいて部分ネットワークに分割されていると考えることができる。そこで機能要件である L5 ノードが、その最下位レイヤ L1 で部分的なネットワークを持つと考えた（図 4）。そして L5 ノードの接続に応じて L1 ノード同士が接続をされるという接続制限をさらに課した。

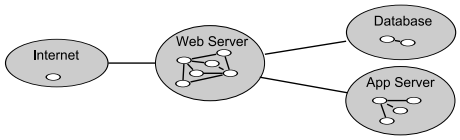


図 4　4 つの L5 ノードと、各内部 L1 ネットワーク

これにより更なるノード数の絞込みが可能になった。表 4 は、L5 ノード数が 4 の場合の各 L1 部分ネットワークのノード数とその合計種類数の一部を示したものである。

表 4　L1 部分ネットワークを利用した L1 ネットワーク種類数（抜粋）

# of L5 nodes	L1 nodes of each func.	# of patterns
3	1-5-5	3660
	...	
	5-5-5	128235
4	...	
	1-1-5-5	7520
	1-3-3-5	140
	1-3-4-5	205
	1-3-5-5	18020
	1-4-4-5	140
	1-4-5-5	18170
	...	

3.3 各レイヤのネットワーク構築

前節までにおいて、L5 のネットワークに応じた L1 ネットワークが決定された。本節ではその他のレイヤネットワークの構築について述べる。

L2 ネットワークはアクセス制御のルール等に関係なく、L1 のネットワーク形態により決まる。基本的には 2 つの L1 ノード a, b がリンクを持つ場合、それらのノードの上位にある 2 つの L2 ノード x, y が接続される。しかし L1R や L2R の中継モジュールが NS に存在する場合は異なる。L1R が存在する場合、L1R で接続された L1 ノード群の上位ノード群はそれぞれが接続され、部分的な完全グラフを形成する。

L1 ネットワークから L2 ネットワークを求めるアルゴリズムを Algorithm 1 に示す。各関数の詳細なアルゴリズムは省略する。

Algorithm 1 L2 構築アルゴリズム

Require: L1 link set L

Ensure: L1 and L2 link set L'

1: $L' \leftarrow L$
2: $L' \leftarrow L' \cup linkByL1R(L')$
3: $L' \leftarrow L' \cup linkByL2R(L')$
4: $L' \leftarrow L' \cup linkByOverL3R(L')$

L3 と L4 のネットワークでは、各ノード間の接続はアクセス制御のルールにより接続の可否が定められる。

アクセス制御のルールがなく、すべての通信が許可されてい

Algorithm 2 Loose ケース構築アルゴリズム

Require: Link set L, Node set S
Ensure: Link set L'
1: $L' \leftarrow L$
2: **for all** L3 node $x \in S$ **do**
3: $y \leftarrow$ L2 node such that $(x, y) \in L$
4: $V \leftarrow findL3connectable(y, L)$
5: $L' \leftarrow L' \cup compGraph(V, L)$
6: **end for**
7: **for all** L4 node $x \in S$ **do**
8: $y \leftarrow$ L3 node such that $(x, y) \in L$
9: $V \leftarrow findL4connectable(y, L)$
10: $L \leftarrow compGraph(V, L)$
11: **end for**

るケース（以後 Loose ケースと呼ぶ）では、各セグメント内にあるモジュール間はすべて通信可能、つまり L3 あるいは L4 ネットワークにおいて部分的な完全グラフを形成する。Loose ケースを実現する L3-4 接続アルゴリズムを Algorithm 2 に示す。

Algorithm 3 接続可能 L3 ノード抽出アルゴリズム: $findL3connectable()$

Require: L2 node x, Link set L
Ensure: L3 node set S
1: $S \leftarrow \phi$
2: $V \leftarrow$ L2 nodes p such that $(x, p) \in L$
3: **for all** L2 node $i \in V$ **do**
4: **if** i is a node of L2R **then**
5: $S \leftarrow S \cup findL3connectable(i, L)$
6: **else**
7: $S \leftarrow S \cup \{$ one of L3 node y such that $(i, y) \in L\}$
8: **end if**
9: **end for**

次にアクセス制御が適切になされている場合を考える。ここでは、アクセス制御における最適を「各モジュールが必要最低限のアクセスパスで接続されている」とした。NSQ モデル上で言えば、L3 あるいは L4 ノードが同一レイヤネットワーク内で孤立することなく、最小のリンク数で接続されている状態を言う。

実際にはその最適性には議論の余地があり、他の要件を加えた上での最適性を定義することもできよう。例えばコストや冗長性を加えることでのアクセス制御の最適性などが考えられる。しかし本稿ではアクセス制御だけに焦点を当て上記の定義とした。

サービスを実現する最小のリンク数を実現するアルゴリズムを求めることは大きな課題ではあるが、本稿ではアルゴリズムの開発を行うことに焦点は置いていないため、リンク数を減少させる単純なアルゴリズムを Algorhtim4 に提案するに留める。以後このアルゴリズムを用いて構築された NS を Efficient ケースと呼ぶこととする。

Algorithm 4 Efficient ケース構築アルゴリズム

Require: Link Set L
Ensure: Link Set L'
1: $L' \leftarrow L$
2: **for all** L5 nodes x, y such that $(x, y) \in L$ **do**
3: $S_A \leftarrow candidateL4nodes(x, L)$
4: $S_B \leftarrow candidateL4nodes(y, L)$
5: $L' \leftarrow L' \cup connect(S_A, S_B)$
6: **end for**
7: **for all** L4 nodes x, y such that $(x, y) \in L'$ **do**
8: $p \leftarrow$ L2 node such that (p, k) and $(k, x) \in L'$ for some L3 node k
9: $q \leftarrow$ L2 node such that (q, l) and $(l, y) \in L'$ for some L3 node l
10: $V \leftarrow searchRoute(p, q)$
11: $L' \leftarrow connectRoute(x, y, V)$
12: **end for**

Algorithm 5 L2 ノード x, y 間のパス探索アルゴリズム: $searchRoute()$

Require: x,y, Link set L
Ensure: Node set V
1: $V \leftarrow \phi$
2: **if** $(x, y) \in L$ **then**
3: $V \leftarrow V \cup \{x, y\}$
4: **else**
5: $V \leftarrow V \cup \{x\}$
6: **for all** L2 or L3 node i **do**
7: **if** $(x, i) \in L$ and $searchRoute(i, y) \neq \phi$ **then**
8: $V \leftarrow V \cup searchRoute(i, y)$
9: return
10: **end if**
11: **end for**
12: $V \leftarrow V/\{x\}$
13: **end if**

Algorithm 6 x, y 間の L3 ノード接続アルゴリズム: $connectRoute(x, y, V)$

Require: Node x,y, Node set V
Ensure: Link set L
1: $L \leftarrow \phi$
2: $a \leftarrow x$
3: $b \leftarrow$ null
4: **while** $V \neq \phi$ **do**
5: $b \leftarrow$ first node of V
6: $V \leftarrow V/\{b\}$
7: **if** b is L3 node **then**
8: $L \leftarrow L \cup \{(a, b)\}$
9: $a \leftarrow b$
10: **end if**
11: **end while**

4. ネットワークシステム解析

本節では、前節までで求められた NS 群を対象に各ノードから出るリンクの出線数の分布（次数分布）を解析する。

まず最初にアクセス制御のアルゴリズムにより NS の次数分布がどのように変化するかを調べ、次に特定モジュールの有無が NS の次数分布にどのような影響をあたえるかを調べる。

対象とした NS 群は、L5 ノードは 4 つのものとした。これは NS の典型的機能構成としてインターネット（I）、フロント Web サーバ（W）、アプリケーションサーバ（AP）、データベース（DB）の 4 つからなるものを前提としている。これによる同型を除いた L5 ネットワークの種類数は 27 となる。

また L5 ノードとしての I が持つ L1 ノード数は 1 とし、その他各 L5 ノード内の L1 ノード数は 1 から 5 とし、最大モジュール数を 16 とした。また最大のノード数は 72 であり、最小のノード数は 16 である。

4.1 アクセス制御アルゴリズムによる特徴変化

図 5, 6, 7, 8 はそれぞれ NS のノード数が 51、58、63、66 のときの Loose ケースと Efficient ケースの次数分布を示したものである。

双方に共通することとしては、リンク数 3 を持つノード数が最大となっていることと、リンク数 4 以上のノード数が段階的に減っていることがある。

しかし、Efficient ケースではリンク数 4 以降の分布がなだらかなのに比較して、Loose ケースでは値が上下している。また、Loose ケースは Efficient ケースと比較して低いピーク値を持ち、またピーク値以外では Efficient ケースより大きな値を持つなど、Efficient ケースと比較して平坦な分布になっている。

ここでは 4 種類のノード数における次数分布を取り上げたが、同様の傾向は各ノード数において見られた。

これらの差は、L3 や L4 での部分完全グラフによる影響によりリンク数の多いノードが Efficient ケースにくらべて多くでることが影響していると考えられる。

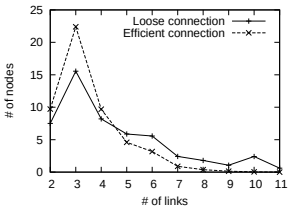


図 5　次数分布（ノード数 51）

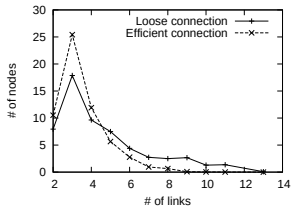


図 6　次数分布（ノード数 58）

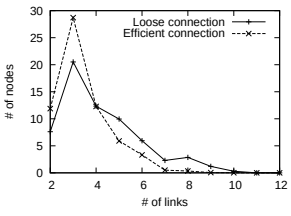


図 7　次数分布（ノード数 63）

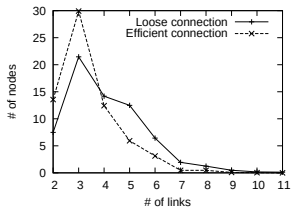


図 8　次数分布（ノード数 66）

4.2 モジュールの有無による特徴変化

次に、各モジュールが NS の次数分布にどのような影響を与えるかを見るために、各モジュールの有無による次数分布の変化を調べる。

まず L1R の有無による NS の次数分布の変化を見る。図 9 はノード数 63 の NS において L1R を持つ NS と持たない NS での Loose ケースにおける次数分布の違いを示したものであり、10 は Efficient ケースでの次数分布の違いを示したものである。

Loose ケースでは、L1R を持つ NS の次数分布は L1R を持たない NS の次数分布と比較してより平坦になっていることがわかる。これは、L1R の存在が、L2 において部分完全グラフを生成させることにより、L2 ノードの平均次数が上がり、さらにそれが L3 以降にも影響しているものと考えられる。

一方、Efficient ケースでは L1R の有無による次数分布の差はほとんどみられない。

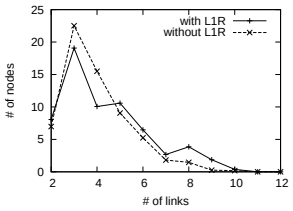


図 9　Loose ケースでの次数分布（ノード数 63）

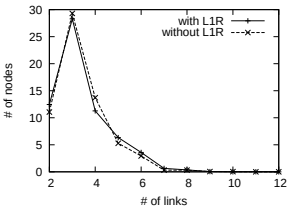


図 10　Efficient ケースでの次数分布（ノード数 63）

次に、L3R の有無による次数分布の違いを見る。図 11 はノード数 63 の NS において L3R を持つ NS と持たない NS での Loose ケースにおける次数分布の違いを示したものであり、図 12 は Efficient ケースでの次数分布の違いを示したものである。

Loose ケースでは、L3R を持たない NS の次数分布が、L3R を持つ NS の次数分布とくらべて平坦になっており、L3R の存在が次数分布の平坦化を抑える効果を持たせ、全体の次数を抑えていることがわかる。しかし Efficient ケースでは L3R の有無による次数分布の差はほとんど見られない。

双方の結果を見ると、Loose ケースの差の図（図 9, 11）では、モジュールの有無による分布の差が現れている一方で、それぞれの Efficient ケース（図 10, 12）ではモジュールの有無による次数分布の差がほとんど見られていないことがわかる。

これにより、本稿で提案した Efficient ケースを実現するアルゴリズム（Algorithm 4）は、モジュールの有無に関係なく、ある一定の次数分布を実現する効果をもつ可能性が示された。これは、アクセス制御として効率的な設計を行うことでその次数分布が一定に抑えらることを伺える結果となっている。

Algorithm 4 は必ずしも最適なアクセス制御を実現するアルゴリズムではないと考えられるが、効率的にリンク数を減らす手法である。Algorithm 4 が最適に近いアクセス制御状態を実現するものであると仮定を置くと、最適アクセス制御状態においてもその次数分布はモジュールに関係なく一定のものになることが言えるであろう。

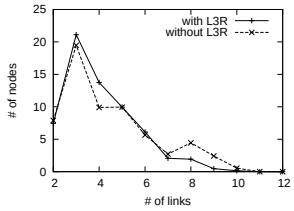


図 11　Loose ケースでの次数分布（ノード数 63）

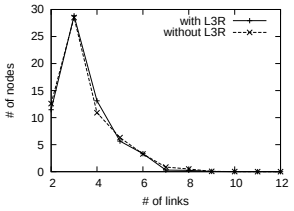


図 12　Efficient ケースでの次数分布（ノード数 63）

5. ま と め

本研究では、金岡らによるネットワークシステム（NS）表現モデル [1] を用いて、NS が持つ特徴をアクセス制御の面より解析した。解析は各ノードが持つ出線数の分布（次数分布）を用いて行われ、アクセス制御が適切に行われている NS とそうでない NS の間での次数分布の差や、ネットワーク機器を示すモジュールの差による次数分布の差を示した。

その結果、アクセス制御が適切に行われている NS では次数分布が一定の分布形状を取ることがわかり、その形状はモジュールの有無にかかわらず現れることがわかった。

これらの結果は、最適アクセス制御状態においてはモジュールや接続制限の差に関係なく次数の分布が一定状態におかれることを示唆しており、それを仮定として置いた場合、一定状態への近似度合いから NS のアクセス制御状態の良否を判断できる指標の構築可能性を示している。

今後の課題として、一定状態を示すパラメータの抽出や、そのパラメータを用いたアクセス制御状態の良否を示す指標を構築することなどがある。

文　献

[1] 金岡晃, 藤堂伸勝, 加藤雅彦, 岡本栄司, ネットワークシステムの安全性定量化に向けた新たな表現モデルとアクセス制御解析, 2008 年暗号と情報セキュリティシンポジウム（SCIS2008）, 宮崎, 2008

[2] A. Hayrapetyan, C. Swamy, E. Tardos, Network Design for Information Networks. Proc. of 16th annual ACM-SIAM symposium on Descrete Algorithms, 933-942 (2005)

[3] N. Sadagopan, M. Singh, B. Krishnamachari, Decentralized Utility-based Sensor Network Design. Mobile Networks and Applications 11, 341-350 (2006)

[4] C. Chekuri, Routing and Network Design with Robustness to Changing or Uncertain Traffic Demands. ASM SIGACT News, 106-129 (2007)

[5] L.C. Lau, J. Naor, M. R. Salavatipour, M. Singh, Survivable Network Design with Degree or Order Constraints. STOC'07, (2007)

[6] T. Wolf, Design of a Network Architecture with Inherent Data Path Security. ANCS'07 (2007)