〔公　開〕

ＴＲ－Ｃ－０１１１

ネットワークセキュリティ参照モデル

力石　徹也
Tetsuya　CHIKARAISHI

１９９４　３．３１

ＡＴＲ通信システム研究所

ネットワークセキュリティ参照モデル

The Network Security Reference Model

力石　徹也
Tetsuya Chikaraishi

ATR通信システム研究所
ATR Communication Systems Research Laboratories

１９９５年３月３１日

目次

概要

本報告では、ネットワークセキュリティに関する共通の認識や共有できる課題，対策技術の獲得を目的とする、ネットワークセキュリティ参照モデルを説明する。ネットワークセキュリティ参照モデルにより、通信ネットワークでのセキュリティ問題の発生箇所やその対策の実施箇所が特定でき、ネットワークで発生するセキュリティ問題とその解決技術との関係を規定できる。さらにネットワークセキュリティの統一的な説明やその体系的な検討が可能となる。またこの論文ではネットワークセキュリティ問題を分類する分類基準を示し、それに従ってネットワークセキュリティ問題を分類することにより、通信ネットワークのセキュリティ課題の内容を明らかにする。さらにセキュリティ課題の解決に必要となるセキュリティ機能、論理的実現法，セキュリティ要素技術の内容を明らかにする。

通信ネットワークの発達に伴い、通信ネットワークのセキュリティの保証が重要な課題となっている。そのため暗号や認証などのセキュリティ技術が多くの研究者によって研究されている。しかし通信ネットワーク自体を対象として、そこで発生するセキュリティ問題や通信ネットワークが備えるべきセキュリティの機能という観点からの研究はあまり行われていなかった。この意味からも、ネットワークセキュリティ参照モデルは、ネットワークセキュリティを検討する上での重要なモデルであると言える。

Abstract

This paper proposes a model called the Network Security Reference Model. The Network Security Reference Model enables common concepts concerning network security to be obtained and security issues and technologies to be shared. It can clearly determine points causing network security problems and implementing the countermeasures. And it can also specify relations between specific network security problems and technologies to solve them. Consequently, the Network Security Reference Model makes the systematic consideration of network security possible.

This paper describes criteria for classifying most specific security problems of communications networks, and by classifying network security problems according to this criteria, the Network Security Reference Model identifies some contents of Security Subjects in communications networks. The Security Subject describe those security problems in terms of certain common concepts. Furthermore, the Network Security Reference Model describes some contents of Security Functions, Logical Implementation Methods and Security Element Technologies.

As communications networks have progressed, it has become more important to guarantee the security of information processing and communication systems that make use of these networks. Consequently, security technologies such as cryptography and authentication have been researched by many researchers. However, little research from a broad perspective has been conducted concerning solutions to security problems that may occur in the whole network itself, or the functions and technologies that the network should accommodate to guarantee the security. Because of this, the Network Security Reference Model had been a necessary scheme to consider issues of network security.

１．はじめに

本論文では「ネットワークセキュリティ参照モデル」を提案する。［１］［２］［３］ネットワークセキュリティ参照モデルは、通信ネットワーク自体を検討対象とした上で、ネットワークセキュリティ研究の共通の認識や共有できる課題，対策技術などの獲得を目的としており、対策だけでなくネットワークに発生するセキュリティ問題も検討の対象に含めて、ネットワークセキュリティに関わる全ての問題や対策技術を、包括的に検討，説明するために導入されたモデルである。

情報化社会が進展するにつれ情報を伝える通信はますます重要になっている。この通信を支える基盤が通信ネットワークである。今日、通信ネットワークは移動体通信やインタネットさらにはマルチメディアの実現などにより、その機能やサービスが高度化され、ますます便利なものになろうとしている。

しかしこのような通信ネットワークの発達に伴い、従来は考えられなかったセキュリティ問題の発生が明らかになり始めている。特にインタネットに実現に伴う通信ネットワークを介したコンピュータに対する不正やネットワークのオープン化に伴うネットワーク機器に対する不正の問題の発生が懸念されている。このためネットワークセキュリティの確保が重要な課題となっている。

このようなセキュリティ問題を解決するために、従来から暗号や認証などの多くのセキュリティ技術が研究開発されている。しかし従来のセキュリティ技術の主な目的は、通信データの秘匿化や端末のセキュリティの保護などであった。また解決方法は、個々の具体的なセキュリティ問題を個別に解決する方法であった。このため通信ネットワーク自体を対象として、統一的な観点からのネットワークセキュリティ研究はあまり行われていなかった。

国際標準化機構（ISO : International Organization for Standardization）からセキュリティ技術を標準化するために、OSIセキュリティアーキテクチャ（OSI : Open System Interconnection）が提案されている。［４］これはOSI参照モデルの枠組みの中で、セキュリティサービスとそれを実現するためのセキュリティメカニズムを標準化し、またセキュリティサービスを実現するプロトコルのOSI参照モデル上での階層を規定するものである。またこれを応用したシステムとして、CISS（Conprehensive Integrated Security Sysyem）が提案されている。［５］しかしOSIセキュリティアーキテクチャは、OSI参照モデルのプロトコル上でのセキュリティサービスの実現というセキュリティ対策に対象を限定して、セキュリティ技術を標準化したものである。このためネットワークに発生するセキュリティ問題から、その解決に必要となるセキュリティ技術までを全体的に検討の対象としたモデルではなかった。

ネットワークセキュリティ参照モデルでは、通信ネットワークの構造に基づいた「複数ネットワーク層，単一ネットワーク層，機器層，データ層」からなる階層構造を規定しており、また具体的なセキュリティ問題からその解決方法までの関係を「セキュリティ課題，セキュリティ機能，論理的実現法，セキュリティ要素技術」という項目として規定している。このモデルにより通信ネットワークでのセキュリティ問題の発生箇所やその対策の実施箇所が特定でき、またネットワークで発生するセキュリティ問題とその解決技術との関係を規定することが可能となる。このモデルによりネットワークセキュリティの統一的な説明やその体系的な検討を実現する。

またこの論文ではネットワークセキュリティ問題を分類する分類基準を示し、それに従ってネットワークセキュリティ問題を分類することにより通信ネットワークのセキュリティ課題の内容を明らかする。さらにセキュリティ課題の解決に必要となるセキュリティ機能、論理的実現法，セキュリティ要素技術の内容を明らかにする。

本論文の内容は、第２章で本論文が対象としている新しいネットワークセキュリティの考え方を示し、第３章ではネットワークセキュリティ参照モデルの概要を説明する。第４章ではネットワークセキュリティ参照モデルの概要に基づき、モデルの詳細な内容を明らかにしする。

２．ネットワークセキュリティの考え方

本章では従来から検討されているネットワークセキュリティの考え方と比較することにより、本論文が対象とするネットワークセキュリティの考え方を明らかにする。

（１）従来のネットワークセキュリティの考え方

ワークステーションなどのコンピュータを端末として伝送路で接続されたシステムは、コンピュータネットワークと呼ばれる。従来のネットワークセキュリティの考え方では、一方の端末からこのコンピュータネットワークを介してUNIXなどのOSのセキュリティ上の不備を突くことにより他方の端末の内部へ不正に侵入し、内部のシステムやデータに被害を与える問題が主な検討対象となっている。［６］［７］その際、通信ネットワークの存在は明確に認識されておらず、端末間に介在し信号を伝送するためだけの単なる「針金」とみなされている。これより従来のネットワークセキュリティのモデルは図１に示すように端末間が直接伝送路で接続されたものであり、その検討対象は通信ネットワークではなく、端末やその内部に存在するデータのセキュリティで場合ことが多い。また解決のためのセキュリティ機能も端末自体に備わっている場合が多い。このように通信ネットワークで発生するセキュリティ問題や通信ネットワークが備えるべきセキュリティ機能に関する検討は、従来あまり行われなかった。

また従来のセキュリティ問題の解決手法は、発生した個々のセキュリティ問題に対して、それを解決する暗号や認証などのセキュリティ技術を個別に適用するという対症療法的な方法であった。このため、新しいセキュリティ問題が発生するたびに、新たにそれに合ったセキュリティ技術を開発する必要があり、結果的に多くの時間や高い技術コストが必要となっていた。

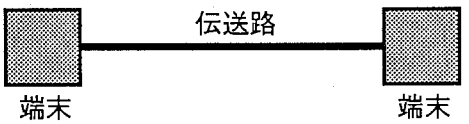

図１　従来のネットワークセキュリティのモデル

（２）新しいネットワークセキュリティの考え方

将来、通信ネットワークがユーザに対してオープン化された結果、通信ネットワークにおいてもセキュリティ問題が発生することが予想される。このため通信ネットワーク自体のセキュリティを保証することが重要な課題となっている。これより本論文のネットワークセキュリティの考え方では、端末間を接続する通信ネットワークの存在を十分に認識した上で、その通信ネットワークのセキュリティを検討の対象としている。その

モデルは図２に示すようになる。例えばその通信ネットワークは、公衆網のようなネットワークや、または複数のネットワーク間を接続したインタネットなどのコンピュータネットワークである場合がある。これより本論文で言うネットワークセキュリティの検討対象は、通信ネットワーク全体に渡っており、例えば通信ネットワークを構成する個々のネットワークや交換機，伝送装置，管理制御機器，伝送路などの機器，通信ソフトウェア，データ，さらにはネットワーク内に形成される論理的な通信経路（パス）、通信ネットワークの持つ機能やサービスなどがある。

またセキュリティ技術の再利用などを可能とする系統的なセキュリティ問題の解決を実現するためには、従来のように個々の問題を個別の解決するのではなく、ネットワークセキュリティを体系的に扱い検討する必要がある。その上で通信ネットワークで発生するセキュリティ問題の解決やそれが備えるべきセキュリティ機能の明確化などを実現する。

本論文ではこの新しいネットワークセキュリティの考え方に基づき、ネットワークセキュリティ参照モデルの提案を行う。

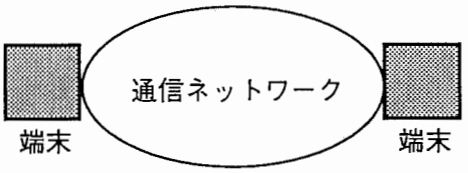

図２　新しいネットワークセキュリティのモデル

３．ネットワークセキュリティ参照モデルの概要

本論文では、ネットワークセキュリティ研究の基盤となるモデルとして、図３に示す「ネットワークセキュリティ参照モデル」（以下、モデルとも言う）提案する。まず本章ではモデルの概要として、モデルの必要性やその目的，モデル化の対象である通信ネットワークの構造，モデルの枠組み，そして性質を述べる。

（１）モデルの必要性と目的

従来のネットワークセキュリティ研究では、各研究者の間にネットワークセキュリティに対する考え方の違いがあり、必ずしも同一の基盤の上で議論が行われているとは言い難かった。またネットワークセキュリティ問題自体も、通信ネットワークが複雑化するのに伴い、より複雑になっている。ネットワークセキュリティを取り巻くこのような状況の中で、複雑な通信ネットワークを対象として、共通な認識の下でのネットワークセキュリティの体系的な検討を実現するためには、ネットワークセキュリティ研究の

セキュリティ課題	セキュリティ機能	論理的実現法	セキュリティ要素技術
	複数ネットワーク層		
	単一ネットワーク層		
	機器層		
	データ層		

図３　ネットワークセキュリティ参照モデル（枠組み）

基盤となるモデルが必要となる。このモデルによりネットワークセキュリティに関する共通の認識や共有できる課題，対策技術が獲得でき、さらにネットワークセキュリティの統一的な説明や問題やその体系的な検討が可能となる。

（2）モデルの対象と通信ネットワークの構造

本節ではこのモデルの対象である通信ネットワークの構造を規定する。モデルの対象は通信ネットワークである。通信ネットワークは端末を含まない。その通信ネットワークの構造は次の様に考えることができる。（図4参照）

通信ネットワークは物理的または論理的に異なる個々のネットワークが相互に接続した大きなネットワークであり、これを「複数ネットワーク」と呼ぶ。複数ネットワークの中には物理的または論理的にそれぞれ異なる個々のネットワークが存在する。これを「単一ネットワーク」と呼ぶ。単一ネットワークの中には、それを構成する「機器」が存在する。機器は伝送路と伝送路以外の交換機や管理制御機器などのノードに分けられる。さらに機器の中にはプログラムやいわゆる数値データである「データ」が存在する。データは通信ネットワークの伝送路上を伝送されている「動的データ」とノード内に蓄積されている「静的データ」に分けられる。

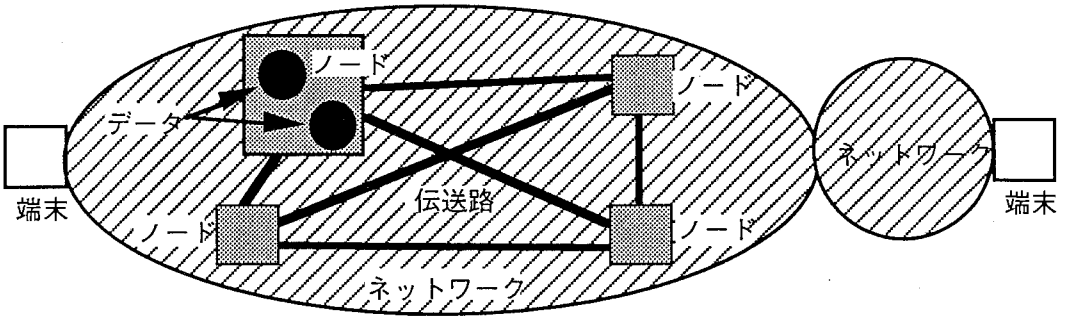

図4　通信ネットワークの構成

（3）モデルの枠組み

ネットワークセキュリティ参照モデルは、（2）で述べた通信ネットワークの構造に従ってその枠組みが構成されている。モデルでは縦軸として「複数ネットワーク層，単一ネットワーク層，機器層，データ層」という階層構造が規定されている（図3参照）。各階層は次の様に定義される（図5参照）。

複数ネットワーク層

物理的または論理的に構成が異なる個別の通信ネットワークが複数接続した、より大きなネットワークの階層。複数のネットワーク間で発生するセキュリティ問題がこの階層での検討対象となる。

単一ネットワーク層

複数ネットワークを構成する個別の（単一の）ネットワークの階層。個々のネットワーク内で発生するセキュリティ問題がこの階層での検討対象となる。

機器層

単一ネットワークを構成する機器の階層。端末で発生するセキュリティ問題がこの階層での検討対象となる。

データ層

機器と蓄積または伝送されているデータ、そして通信の事実や通信ネットワークの状

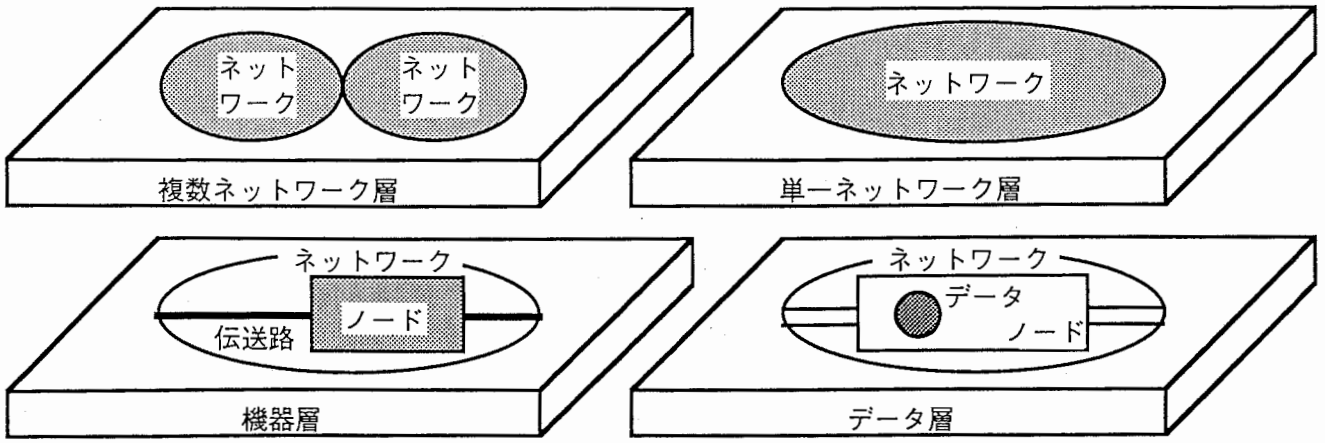

図5　ネットワークセキュリティ参照モデルの階層

況や振る舞い、さらにそれらから推論することにより間接的に得られる情報などの階層。データやプログラム，情報などに発生するセキュリティ問題がこの階層での検討対象となる。

通信ネットワークの具体的なセキュリティ問題は、複数の複雑な要因が組合わさることにより発生している。この様な階層化したモデルを導入することより、これらのセキュリティ問題は、モデルの各階層のセキュリティ問題に分解して考えることが可能となる。これによりセキュリティ問題の発生箇所や対策の実施箇所を明確に特定することが可能となる。

次にモデルでは横軸として「セキュリティ課題，セキュリティ機能，論理的実現法，セキュリティ要素技術」という項目が規定されている（図3参照）。各項目は次の様に定義される。

セキュリティ課題

通信ネットワークで発生する具体的なセキュリティ問題を分類しグループ化することにより得られる類似したセキュリティ問題の集合で、通信ネットワークに普遍的に存在するセキュリティ上の課題。

セキュリティ機能

セキュリティ課題を解決するために端末や通信ネットワークが備えるべきセキュリティ上の基本的な機能。一つのセキュリティ課題の解決に複数のセキュリティ機能が必要となることもある。

論理的実現法

セキュリティ機能を実現するための論理的なセキュリティ技術。一つのセキュリティ機能の実現に対して複数の論理的実現法が必要となることもある。

セキュリティ要素技術

論理的実現法を実現するための個々の具体的なセキュリティ技術。一つの論理的実現法に対して複数存在することもある。

このようにモデル上でネットワークのセキュリティ問題とその対策技術を「セキュリティ課題，セキュリティ機能，論理的実現法，セキュリティ要素技術」として規定することにより、通信ネットワークの具体的なセキュリティ問題とその問題を解決するために必要となる具体的なセキュリティ技術との関係を明らかにすることができる。またセキュリティ問題の解決に必要となるセキュリティ技術の特定が容易になる。

（4）モデルの性質

ネットワークセキュリティ参照モデルの性質を以下に示す。

1）このモデルの各階層の関係は互いに独立した関係となる。つまり上位の階層の内容は下位の階層の内容を含まず、また下位の階層で発生した問題は上位の階層の問題とはならない。

2）論理的実現法は類似したセキュリティ要素技術の集合としても規定することができる。

つまり論理的実現法はセキュリティ技術の進歩にも対応するためのものであり、セキュリティ要素技術が技術の進歩と共に変化しても変わらない、普遍的なセキュリティ技術として考えることができる。これによりセキュリティ機能の実現には常に適切な論理的実現法を利用すればよく、セキュリティ要素技術は状況に応じて変更または使い分けられてもかまわない。

3）機器の破壊や伝送路に盗聴装置を取り付けるなど、機器に対して物理的に直接不正を実行する問題や、人為的な要因はこのモデルの検討対象ではない。

4．ネットワークセキュリティ参照モデルの内容

本章では3で述べたモデルの概要に基づき、ネットワークセキュリティ参照モデルの項目である「セキュリティ課題，セキュリティ機能，論理的実現法，セキュリティ要素技術」の検討を行い、モデルの具体的な内容を明らかにする。

4－1　セキュリティ課題

通信ネットワークの具体的なセキュリティ問題の例をモデルの各階層の問題に分解し、それをネットワークセキュリティ問題の分類基準に従って分類することにより、その結果からセキュリティ課題の内容を明らかにする。またセキュリティ課題と分類基準の関係について考察する。

（1）ネットワークセキュリティ問題の例

今回の検討に用いた具体的なネットワークセキュリティ問題の例を以下に示す。

1）送受信者による電子メールの送受信事実またはその内容の否認［8］

2）分散ネットワークシステムにおいて「なりすまし」を行った不当な依頼者によるネットワークを介した他のコンピュータへの不正な委託［9］

3）電子メールを送る際に途中で中継を行う不適切なネットワークや端末などでの電子メールの漏洩，改ざん，破壊［10］

4）複数のClosed User Group（CUG）に所属できるユーザを介したCUG内の情報の他のCUGへの漏洩［11］

5）交換機の誤動作などを原因とするVirtual Private Network（VPN）間での不適切な回線の接続

6）ファクシミリ通信でのダイヤル誤りによる不適切なFAX端末への誤接続，誤配送

7）インタネットにおいて他機器のIPアドレスを利用して正当な受信機器に“なりすます”ことにより送信機器から送られたデータを不正に受信する

8）通信ネットワーク内のデータ伝送量や伝送先などの不正な解析

9）通信ネットワークへ不必要なデータを大量に送出したり、多数のユーザが同時に電話をかけることによる通信の妨害

１０）通信ネットワークを介したコンピュータやデータベースへの不正なアクセス
１１）移動体通信での端末の移動経路や現在位置の発覚
１２）電子メールを利用したコンピュータウイルスの不当な送信［１２］
１３）無線伝送路からの通信内容の盗聴

これらの問題の中には、モデルの検討対象ではない端末において発生するネットワークセキュリティ問題も含まれている。しかしそれらの問題は本質的に通信ネットワークの機器においても発生しうる問題であるため、ここでネットワークセキュリティ問題の例に含めることに問題はない。

（２）各階層のセキュリティ問題への分解

これら通信ネットワークの具体的なセキュリティ問題の例を、ネットワークセキュリティ参照モデルの枠組みに写像することにより、各階層のセキュリティ問題に分解する。分解は例えば次の様に行われる。

３）は「電子メールを送る際に不適切なネットワークや端末との間にパスが形成されることにより、そのネットワークや端末において電子メールが漏洩，改ざん，破壊される問題」と考えることができるから、これより各階層の対象となる問題を導き出すと、次の様な各階層毎のセキュリティ問題に分解できる。

複数ネットワーク層：中継を行う不適切なネットワークとの間の電子メールを送るパスの形成
単一ネットワーク層：中継を行う不適切な端末との間の電子メールを送るパスの形成
データ層：電子メールを中継する端末における電子メールの内容の漏洩，改ざん，破壊

同様にして１）～１３）の通信ネットワークの具体的なセキュリティ問題を各階層のセキュリティ問題に分析した結果を示す。「→」は左側の番号の具体的なセキュリティ問題が右側の各階層のセキュリティ問題へ分解できることを示している。

複数ネットワーク層

ａ）３→不適切なネットワークとの間の電子メールを送るパスの形成
ｂ）４→複数のCUG間での不適切な通信経路（パス）の形成
ｃ）５→複数のVPN間での不適切な回線の接続
ｄ）５→パスや回線を介したVPNへの不正な侵入

単一ネットワーク層

ｅ）３→不適切な端末との間の電子メールを送るパスの形成
ｆ）６→不適切なFAX 端末との間の誤接続

機器層

ｇ）２→不当な依頼者による被依託機器への処理の不正な委託
ｈ）７→受信機器によるデータの不正な受信
ｉ）９→交換機の機能の妨害
ｊ）１０→コンピュータやデータベースへの不正な侵入
ｋ）１２→不正な機器からのでたらめなデータや不当なデータの送信

データ層

ｌ）１→電子メールの送受信事実やその内容の否認
ｍ）２→被委託機器で行われた処理結果の漏洩
ｎ）３→端末での電子メールの漏洩，改ざん，破壊

o） 4→CUG内で通信されているデータの隠れパスを介した他のCUGへの漏洩
p） 5→VPN内で通信されているデータの不適切な回線を介した他のVPNへの漏洩
q） 6→誤接続によるFAXの通信内容の漏洩
r） 8→通信ネットワーク内の重要機器の存在や接続関係の発覚
s） １０→コンピュータやデータベースに蓄積されているデータの漏洩，改ざん，破壊
t） １１→移動体通信での端末の移動経路や現在位置の発覚
u） １３→無線伝送路からの通信内容の漏洩

（3）ネットワークセキュリティ問題の分類基準

この様に分解された各階層のセキュリティ問題からセキュリティ課題を得るためには、セキュリティ問題の分類に際して抜けや重複が生じないように明確な基準の下で分類することが必要となる。ここではその分類基準を各階層毎に示す。まず分類のための基本的な考え方を示す。

通信ネットワーク間またはノード間の接続には、「直接的な接続」と「間接的な接続」がある。直接的な接続とはネットワーク間が通信回線によって直接的に接続され通信経路が形成される場合の接続のことで、間接的な接続とはネットワーク間に他のネットワークや端末などの第三者が介在することにより、その第三者をいったん経由して情報が伝搬するような通信経路が形成される場合の接続のことである。またその接続には、「全ての接続が禁止」される場合と「一部の接続が許可」される場合がある。これより接続に関しては「直接－間接」と「禁止－許可」という基本的な考え方を導入する。次に機器やデータに対するアクセスには、情報を受信する，読み出すなどの「Read系」のアクセスと、送信する，委託する，書き込むなどの「Write系」のアクセスがある。これよりアクセスに関しては「Read系－Write系」という基本的な考え方を導入する。またデータには先に述べたように、「動的データ」と「静的データ」が存在する。このためデータに関する基本的な考え方として「動的－静的」という考え方を導入する。

これらの基本的な考え方に基づき、各階層毎にネットワークセキュリティ問題の分類基準を定義する。次にその定義を各階層毎に述べる。

複数ネットワーク層（図６参照）

複数ネットワーク層の具体的なセキュリティ問題は、ネットワーク間の通信経路が「直接的な接続」である場合に発生する問題と、「間接的な接続」である場合に発生する問題に分類できる。さらにそれぞれはネットワーク間の「接続が禁止される」場合に発生する問題と「接続は許されるが個別の通信が制限される」場合に発生する問題に分類できる。「接続は許されるが個別の通信が制限される」場合に発生する問題は、他ネットワークからの「Read系」の問題と他ネットワークへの「Write系」の問題に分類できる。またこの他に「複数ネットワークの機能やサービス」に発生する問題がある。

単一ネットワーク層（図７参照）

単一ネットワーク層の具体的なセキュリティ問題は、単一のネットワーク内のノード間の通信経路が「直接的な接続」である場合に発生する問題と、「間接的な接続」である場合に発生する問題に分類できる。またこの他に「単一ネットワークの機能やサービス」に発生する問題がある。

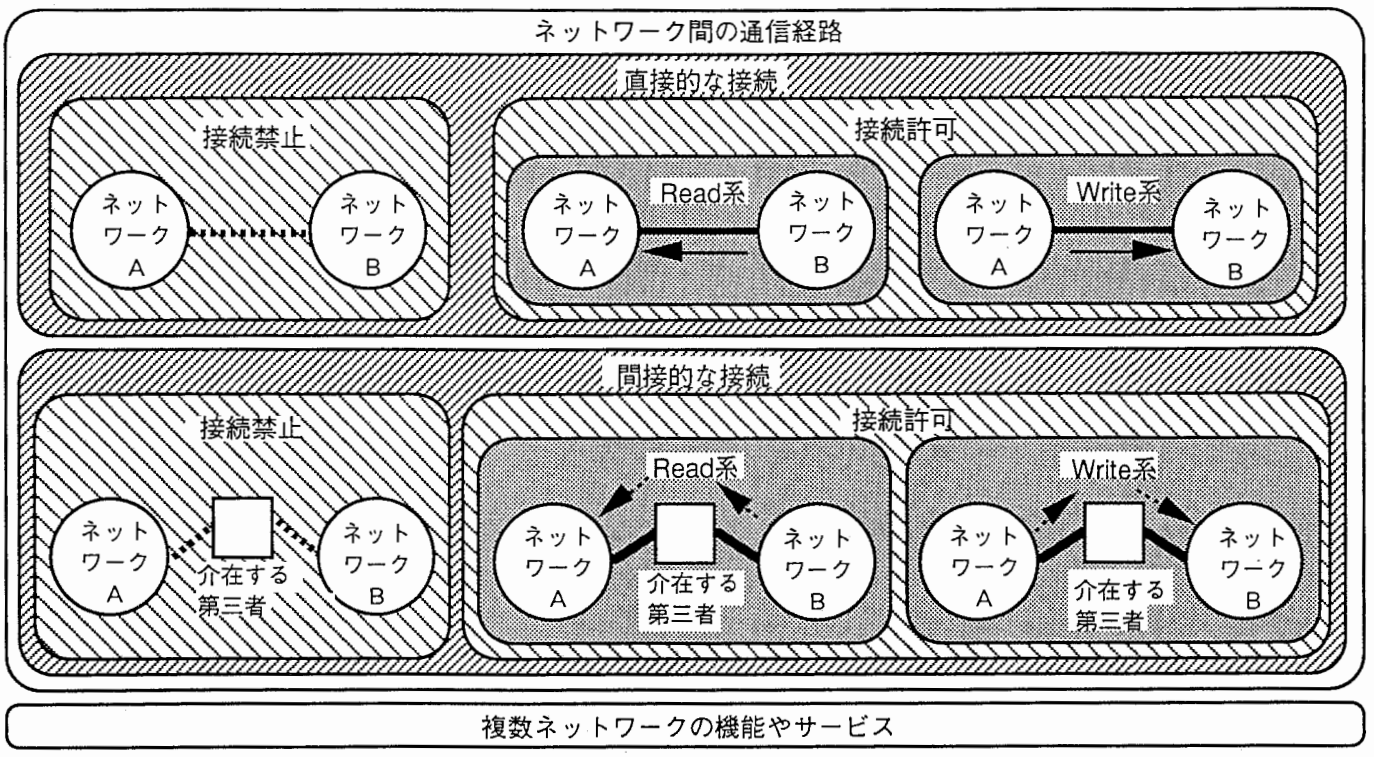

図6　複数ネットワーク層の分類基準

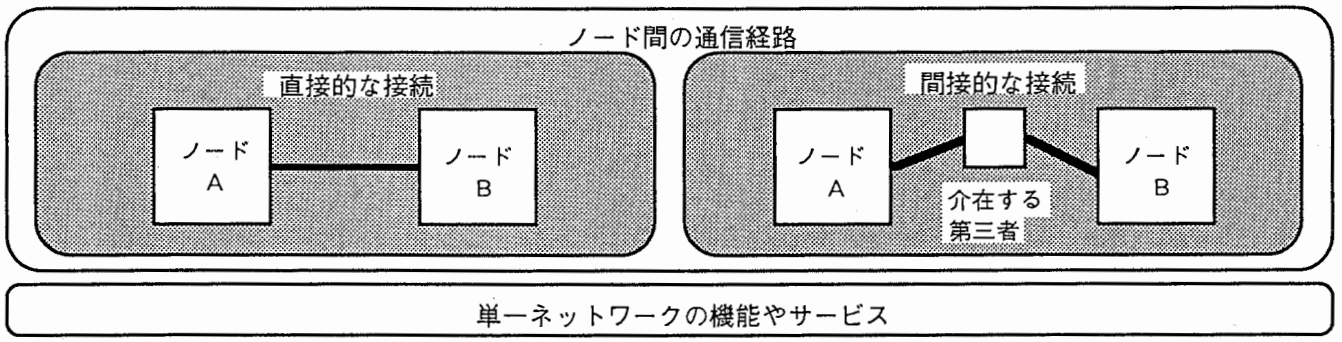

図7　単一ネットワーク層の分類基準

機器層（図8参照）

機器層の具体的なセキュリティ問題は機器に対する「Read系」の問題と「Write系」の問題に分類できる。またこの他に「機器や端末の機能やサービス」に発生する問題がある。

データ層（図9参照）

データ層の具体的なセキュリティ問題は、「データ」に発生する問題と、「推論情報」に発生する問題に分類できる。データとは機器内に存在するデータのことで、直接的に不正が実行される。また推論情報とはデータ以外の情報のことで、通信ネットワークの様々な振る舞いや状況などに関する情報や、またはそれらから推論により間接的に得られる情報などである。データにはノードに伝送路上の「動的データ」とノードに蓄積されている「静的データ」があり、それぞれに対してRead系の問題とWrite系の問題が発生する。

（4）セキュリティ課題の内容

（1）で分解により得られた各階層のセキュリティ問題を、（2）で示した分類基準

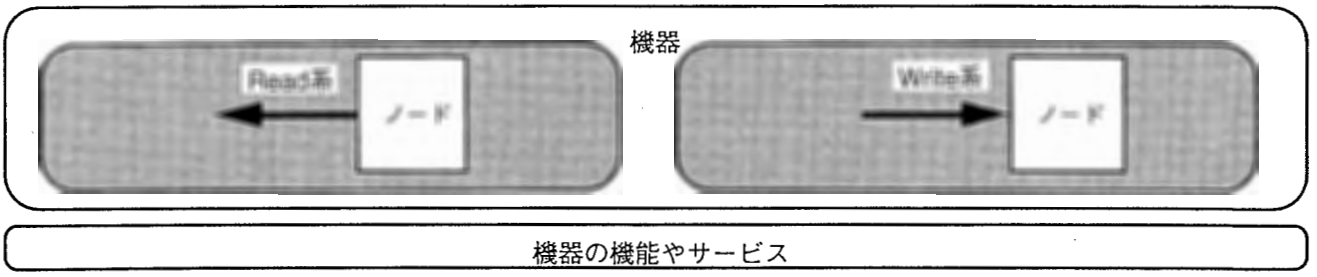

図８　機器層の分類基準

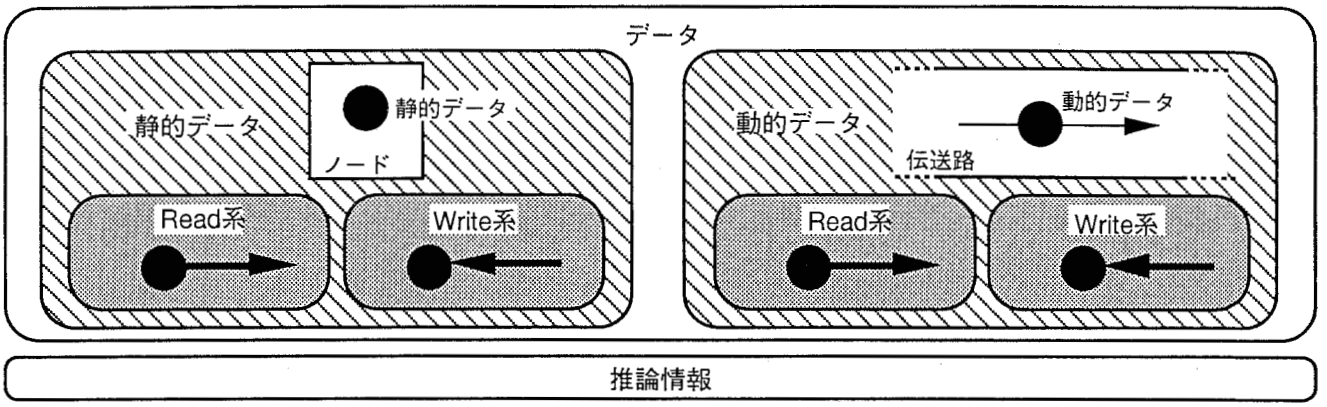

図９　データ層の分類基準

に従って表１（ａ）（ｂ）に示すように分類することにより、モデルのセキュリティ課題を次のように明らかにできる。

複数ネットワーク層

課題１：ネットワーク間の不正接続

課題２：ネットワークへの侵入

課題３：ネットワーク間の隠れパス

単一ネットワーク層

課題４：ノード間の不正接続

課題５：ノード間の隠れパス

機器層

課題６：ノードによる不正な受信

課題７：ノードへの不正な委託，送信，アクセス

課題８：機器の機能やサービスの妨害

データ層

課題９：蓄積データの漏洩

課題１０：蓄積データの改ざん，破壊

課題１１：通信データの漏洩

課題１２：通信データの改ざん，破壊

課題１３：トラヒック解析による情報の漏洩

課題１４：通信事実や通信内容の否認

これらセキュリティ課題は通信ネットワークに普遍的に存在する問題であり、通信ネットワークで発生する具体的なセキュリティ問題を検討する上での基礎となる。

（5）分類基準とセキュリティ課題の関係

表1（a）（b）より全ての分類基準に対してセキュリティ課題が明らかになっているわけではないことがわかる。この理由は、以下の様に考察できる。

1）論理的にはセキュリティ課題の分類基準を規定することはできるが、実際にはその分類基準における具体的なセキュリティ問題の発生が本質的にありえない場合

2）まだ具体的なセキュリティ問題の発生が確認されていない場合

4－2　セキュリティ機能

セキュリティ機能は、セキュリティ課題を解決するために通信ネットワークが備えるべきセキュリティ上の基本的な機能である。ここでは4－1で示した14種類のセキュリティ課題を防止または解決するために、通信ネットワークに必要となる機能を明らかにする。

複数ネットワーク層

セキュリティ課題1：ネットワーク間の不正接続

（1）ネットワーク間の接続要求が正当な要求かそうでないかを確認する機能

（2）確認に基づきネットワーク間の接続を制御する機能が必要となる。

セキュリティ課題2：ネットワークへの侵入

（3）ネットワーク内へのアクセス要求が正当な要求かそうでないかを確認する機能

（4）確認に基づきネットワークへのアクセスを制御する機能

セキュリティ課題3：ネットワーク間の隠れパス

（5）ネットワーク間に存在する隠れパスをあらかじめ解析し発見する機能

単一ネットワーク層

セキュリティ課題4：ノード間の不正接続

（6）ノード間の接続要求が正当な要求かそうでないかを確認する機能

（7）確認に基づきノード間の接続を制御する機能

セキュリティ課題5：ノード間の隠れパス

（8）ノード間に存在する隠れパスをあらかじめ解析し発見する機能

機器層

セキュリティ課題6：ノードによる不正な受信

（9）受信側のノードが正当なノードであるかどうかを確認する機能

セキュリティ課題7：ノードへの不正な委託，送信，アクセス

（10）委託，送信，アクセスなどを要求しているノードが正当なノードであるかどうかを確認する機能

（11）確認に基づき機器へのアクセスを制御する機能

セキュリティ課題8：機器の機能やサービスの妨害

（12）機器に対する妨害が発生した際にそれを排除する機能

（13）妨害により機器に発生する被害を無くすまたは最小限にする機能

データ層

セキュリティ課題9：蓄積データの漏洩

（14）蓄積データへのアクセス要求が正当な要求であるかそうでないかを確認する機能

（15）確認に基づき蓄積データへのアクセスを制御する機能

（１６）蓄積データが漏洩した場合でもデータの内容を理解できなくする機能
（１７）蓄積データの漏洩による被害を最小限にする機能
セキュリティ課題１０：蓄積データの改ざん，破壊
（１８）蓄積データへのアクセスが正当な要求であるかそうでないかを確認する機能
（１９）確認に基づき蓄積データへのアクセスを制御する機能
（２０）蓄積データが改ざん，破壊されたことが容易に発覚するための機能
（２１）改ざん，破壊された蓄積データを元どおりに修復するための機能
セキュリティ課題１１：通信データの漏洩
（２２）通信データが漏洩した場合でもデータの内容を理解できなくする機能
（２３）通信データの漏洩による被害を最小限にする機能
セキュリティ課題１２：通信データの改ざん，破壊
（２４）通信データが改ざん，破壊されたことが容易に発覚するための機能
（２５）改ざん，破壊された蓄積データを元どおりに修復する機能
セキュリティ課題１３：トラヒック解析による情報の漏洩
（２６）通信ネットワーク内のデータの流れの解析を不可能にする機能
セキュリティ課題１４：通信事実や通信内容の否認
（２７）通信事実や通信内容の記録保持し証明する機能

ここで「接続制御」とは、ネットワーク間や機器間に不正な接続が発生しないように制御することで、また「アクセス制御」とはアクセスされるネットワークや機器，データ自体が送信，受信，読み出し，書き込みなどの不正が発生しないように制御することである。

これらセキュリティ課題の解決に必要となる機能は、その内容に応じて次の１０種類のセキュリティ機能に分類される。

Ａ．不正を発見する機能
（５）（８）→隠れパス発見機能
Ｂ．不正を未然に防止する機能
Ｂ－１．不正が実行される前にあらかじめ施しておく機能
（１６）（２２）→データ機密保証機能
（２０）（２４）→データ完全性保証機能
（２６）→トラヒック解析防止機能
（２７）→通信事実内容証明機能
Ｂ－２．不正が実行される際にそれを防止するための機能
（２）（７）→接続制御機能
（４）（１１）（１５）（１９）→アクセス制御機能
（１）（３）（６）（９）（１０）（１４）（１８）→要求確認機能
Ｃ．実行された不正による被害を無くすまたは最小限にする機能
（１２）（１３）→高信頼性化機能
（１７）（２１）（２３）（２５）→データ管理機能

４－３　論理的実現法

論理的実現法はセキュリティ機能を実現するための一般的なセキュリティ技術で、具体的には、暗号や認証などの従来から存在するセキュリティ技術の種類に相当すると考

えられる。ここではそれらセキュリティ技術の種類が、どのセキュリティ機能の実現に利用できるかという観点に基づいて分類する。４－２で示したセキュリティ機能を実現するための論理的実現法をセキュリティ機能毎に示す。

隠れパス発見機能…パス解析
データ機密保証機能…暗号
データ完全性保証機能…暗号，認証
トラヒック解析防止機能…トラヒック管理
通信事実内容証明機能…内容証明
接続制御機能…接続制御
アクセス制御機能…アクセス制御
要求確認機能…認証
高信頼性化機能…通信ネットワーク／機器管理
データ管理機能…データ保守

４－４　セキュリティ要素技術

セキュリティ要素技術は、論理的実現法を実現するための個々の具体的なセキュリティ技術で、具体的には、例えば暗号ならばDESやRSAなどの個々のセキュリティ技術に相当すると考えられる。ここではそれらセキュリティ要素技術が、どの論理的実現法の実現の利用できるかという観点に基づいて分類する。４－３で示した論理的実現法を実現するための現在存在する主なセキュリティ要素技術を論理的実現法毎に示す。［１３］

ａ）パス解析
　ブール代数演算に基づく隠れパス解析法

ｂ）暗号
　公開鍵暗号
　　RSA暗号，R暗号，W暗号，MI暗号，MIHM暗号，MH暗号，GS暗号，CR暗号，
　　E暗号，T暗号，S暗号，L暗号，GMY暗号，GMR暗号，OSS暗号，OS暗号
　秘密鍵暗号　Secret-key Cryptosystem
　　バーナム暗号，DES，FEEL
　ストリーム暗号
　　同期式線形フィードバック方式，同期式非線形フィードバック方式
　　自己同期式線形フィードバック方式，自己同期式非線形フィードバック方式
　アナログ暗号
　　スペクトル置換，ビット反転

ｃ）認証
　ユーザ認証
　　パスワード，PIN，指紋照合，声紋照合，筆跡鑑定，ICカード
　　ゼロ知識証明を利用した認証プロトコル，秘密鍵暗号プロトコル
　　公開鍵暗号プロトコル，認証子照合法
　メッセージ認証
　　秘密鍵暗号プロトコル，公開鍵暗号プロトコル，認証子照合法

d）トラヒック管理
　　ダミーデータの伝送
e）内容証明
　　センタ介在型プロトコル，センタ非介在型プロトコル
f）接続制御
　　ルーティング，閉域通信
g）アクセス制御
　　任意アクセス制御
　　　任意アクセス制御モデル
　　強制アクセス制御
　　　BLPモデル
h）通信ネットワーク／機器管理
　　通信ネットワークの多重化，システムの切り換え
　　Telecpmmunication Management Network（TMN）
i）データ保守
　　データの変更無効，データのバックアップ

以上の検討に基づくセキュリティ課題，セキュリティ機能，論理的実現法，セキュリティ要素技術の関係を表２に示す。この検討によりネットワークセキュリティ参照モデルのセキュリティ課題，セキュリティ機能，論理的実現法，セキュリティ要素技術の具体的な内容を明らかにすることができた。

５．まとめ

本論文では、端末を対象として個々の問題を個別に解決するという従来のネットワーて、そのセキュリティの体系的な検討を目的とする新しいネットワークセキュリティの考え方を示した。この考え方に基づきネットワークセキュリティを研究する際の共通の認識や共有できる課題，対策技術の獲得を目的とするネットワークセキュリティ参照モデルを提案を行った。また通信ネットワークの具体的なセキュリティ問題を分類するための分類基準を提案し、それに基づいてセキュリティ問題を分類することにより、通信ネットワークに存在する１４種類のセキュリティ課題を明らかにした。セキュリティ課題を解決するのに必要となる１０種類のセキュリティ機能を示し、それを実現する論理的実現法とセキュリティ要素技術の具体的な内容を明らかにした。

ネットワークセキュリティ参照モデルは、ネットワークセキュリティ研究する上での基盤となるモデルであり、これによりネットワークセキュリティの体系的な検討が実現できる。またこのモデルを利用することにより、ネットワークセキュリティ問題の解決技術の容易な選択や新たに発生したセキュリティ問題に対する従来技術の再利用が可能となり、セキュリティ問題解決の効率化という面において大きな効果が期待できる。この結果、最も適切な従来技術を選択し利用すればよくなり、個別の問題毎に解決技術を開発する必要がなくなるために、経済的には技術のコストダウンが期待できる。さらにネットワークセキュリティ参照モデルは、対象システムにセキュリティ上の問題がないかどうかを評価するシステムなどへの応用が考えられる。

参考文献

［1］力石、T.Hardjono、荒木、太田，“通信ネットワークの持つセキュリティ問題の検討”，1993年暗号と情報セキュリティシンポジウム（SCIS93），SCIS93-8A，1993年1月

［2］太田、力石，“ネットワークセキュリティモデルの一考察”，信学技報，SSE93-33，1993年7月

［3］Tadashi Ohta, Tetsuya Chikaraishi, "Network Security Model", IEEE Singapore International Conference on Networks / International Conference on Information Engineering '93 (SICON/ICIE93), G1-1, Sept. 1993

［4］International Standards Organization，“Information Processing System - OSI RM. Part 2 : Security Architecture”，ISO／TC 97 7498-2，1988

［5］S. Muftich et.al.，“Security Architecture for Open Ditributed Network”，John Wiley & Sons，pp163-253，1993

［6］S.Garfinkel、G.Spafford，“Practical UNIX Security”，O'Reilly&Associates, Inc.,，1991

［7］C.Stoll，“The Cuckoo's Egg：Tracking a Spy through the Maze of Computer Espionage”，Pocket Books，New York，1990

［8］安達、杉村，“電子メイルにおける配達証明・内容証明の実現に関する一考察”，信学技報，COMP93-32（ISEC93-16），1993年7

［9］T.Hardjono、T.Ohta，“Approaches to Secure Delegation in Distributed System”，Proceedins of IEEE Phoenix Conference on Computer and Communication（IPCCC93），1993

［10］S.t.Kent，“Internet Privacy Enhanced Mail”，Communications of the ACM，36.8.pp.48-60，August 1993

［11］力石、荒木、T.Hardjono、竹中，“閉域通信におけるセキュリティ問題の解析”，信学会　暗号と情報セキュリティシンポジウム（SCIS92），SCIS92-9C，1992年4月

［12］“特集ワームストーリー：インターネット・ワーム事件の全容”，Bit，Vol.21 No.14，共立出版，1989年12月

［13］池野，小山，“現代暗号理論”，電子情報通信学会，1986

付録

1．ISO／OSIセキュリティアーキテクチャ

セキュリティ技術のコンピュータネットワークでの体系的な利用を目的として、ISOやITU-T（旧CCITT）などの機関においてセキュリティ技術の標準化が検討されている。その中で最も注目されているのが国際標準化機構（ISO）で標準化されたOSIセキュリティアーキテクチャである。［1］［2］［3］

OSIセキュリティアーキテクチャは、OSIネットワークアーキテクチャをセキュリティに拡張したもので、開放型システム間相互接続（OSI）環境下のコンピュータネットワークで用いるセキュリティ技術を標準化し、そのガイドラインを示している。具体的なセキュリティ技術を規定するものではない。このようにセキュリティ方式を標準化することにより、コンピュータネットワークでのセキュリティ対策をより一般的なものとし、ハードウエアのコストを下げるなどの効果が期待できる。このOSIセキュリティアーキテクチャでは、セキュリティサービスとセキュリティメカニズムが規定されている。

セキュリティサービスとは、コンピュータネットワークのシステムやデータに対して十分なセキュリティを実現するために必要なサービスを規定したもので、次の５種類がある。

ａ）認証…通信相手とデータ発信元を認証するためのサービス
ｂ）アクセス制御…ネットワーク内の資源に対する不正なアクセスを防止するためのサービス
ｃ）データ機密保護…情報漏洩からデータを保護するためのサービス
ｄ）データ完全性保証…改ざんなどに対してデータの完全性を保証するためのサービス
ｅ）拒絶不可保証…送信者がデータを送信したこと、または受信者がデータを受信したことを拒絶できないようにするためのサービス

またセキュリティメカニズムとは、セキュリティサービスを実現するために必要となる仕組みを規定したもので、次の８種類がある。

Ａ）暗号…データや伝送情報の機密を保護するためのメカニズム
Ｂ）ディジタル署名…署名者が秘密の個人情報をデータに書き込みそれを照合することにより認証を行うためのメカニズム
Ｃ）アクセス制御…ネットワーク内の各資源へのアクセスを制御するためのメカニズム
Ｄ）データ完全性保証…データの改ざん，削除，挿入，紛失，再送などからデータの完全性を保護するためのメカニズム
Ｅ）認証交換…秘密の個人情報などを交換することにより認証を行うためのメカニズム
Ｆ）トラヒックパッディング…トラヒックの不正解析を防止するためのメカニズム
Ｇ）ルーティング制御…安全なルートの選択や攻撃を避けるルートの選択を実現するためのメカニズム
Ｈ）公証…公正な第三者によってデータの内容や発信元，時間，送信先などの情報を保証するためのメカニズム

2．CISS

S.Muftic氏らは、多くのセキュリティプロジェクトにおいて、同様または類似したセキュリティの方針の下で、セキュリティサービスやセキュリティメカニズムが実行され

ていることによる無駄や、ISO／OSIセキュリティアーキテクチャが、コンピュータ間の通信のセキュリティを対象としているのに対し、Open Distibuted Processing（ODP）環境では対象領域をそれ以外の領域にも拡張し、接続しているコンピュータなどを含む全てのシステムのセキュリティを統一的に検討することが重要であることを指摘した上で、セキュリティサービス，セキュリティメカニズムなどのセキュリティ技術を一般化し統合するシステムであるCISS（Conprehensive Integrated Security Sysyem）を提案している。［3］

CISSではコンピュータやOS，ネットワークなどの環境の違いにかかわらず、OSIやODP環境下のユーザやデータ，プログラム，アプリケーションに対して多様なセキュリティサービスやセキュリティメカニズム，セキュリティ管理機能を能率的かつ使い易く提供する。これを実現するためにCISSでは、類似したまたは同様な複雑さを持ったサービス，メカニズム，機能をモジュール化し、基礎（数学）モジュール，セキュリティメカニズム，セキュリティサービス，セキュリティエージェントとプロトコル，セキュリティ管理とマネジメントツールの５つに階層化したモデルを提案している。各階層の内容は次の様なものである。

ａ）基本層：基礎（数学）モジュール…暗号やゼロ知識証明などを実現する際に、そのアルゴリズムに中で使用される数学的な機能（例えば大きな値の素数の計算や乱数の生成など）のための基本的なモジュールの階層で、セキュリティメカニズムを実現するために使用される。

ｂ）第２層：セキュリティメカニズム…セキュリティメカニズムのモジュールの階層で、セキュリティシステムの個々の機能やセキュリティサービスを実現するために利用される。

ｃ）第３層：セキュリティサービス…OSIセキュリティアーキテクチャで示されているものに加え、その他にもいくつか提案されているセキュリティサービスのモジュールの階層。

ｅ）第４層：セキュリティエージェントとプロトコル…これは主にセキュリティメカニズムとセキュリティサービスの関係とその利用に関するモジュールの階層で、論理的なコンポーネントはエージェントと呼ばれ、その間には特別なプロトコルが規定されている。

ｆ）第５層：セキュリティ管理とマネジメントツール…セキュリティ管理のモジュールの階層で、ISOから勧告されたものや他から提案されているセキュリティ管理に関する全ての機能を備えている。

３．SCSE

中尾氏らは、これまで通信のセキュリティ機能は異なる通信業務毎にそれぞれ独立に検討されており、セキュリティシステム開発の効率やコストの観点から無駄が多く、このため体系的なセキュリティ機能の構築が望まれていることを指摘した上で、OSIネットワークアーキテクチャの環境下でセキュリティ機能を体系的に実現するSCSE（Secure Communication Service Element）の提案を行っている。［4］［5］

SCSEはアプリケーション層の応用サービス要素として、認証，情報秘匿，改ざん防止などのセキュリティ機能を提供するもので、OSI環境下の各種アプリケーションに共通に

利用できる。セキュリティ機能には次の様なものがある。
a）セキュリティ環境設定機能…通信開始時に必要となる暗号のアルゴリズムや暗号鍵などのセキュリティに関する情報を設定する機能
b）相手認証機能…通信開始時に通信相手を認証する機能および通信中に定期的に相手を認証する機能
c）情報秘匿機能…通信情報を暗号化／復号化する機能
d）改ざん防止機能…通信情報に対して改ざん防止のための送信側での検知情報の付与および受信側でのその検査を実行する機能

4．セキュリティアーキテクチャ

先の2つの研究がネットワークセキュリティ問題の解決のためのシステムを検討しているのに対し、原田氏はネットワークセキュリティを検討するためには体系的な枠組みを規定することが必要であることを指摘した上で、その基盤となる「セキュリティアーキテクチャ」を提案している。［6］［7］セキュリティアーキテクチャとは、ネットワークアーキテクチャの持つ「ネットワークの標準部品化，標準部品間の関係とインタフェース点を示す参照モデルを作り、インタフェース点での情報交信法の規定，規格化」の特徴をセキュリティに拡張したものである。

まず原田氏は機能とそれが扱う情報の性質からネットワークを、「ユーザ情報伝達網，制御・管理情報転送，管理・制御システム系」の3つに分類している。その上でこれらのセキュリティアーキテクチャを次の様に規定している。
a）セキュリティアセスメント…潜在的な脅威の洗い出しと体系化を行う
b）セキュリティリクワイヤメント…セキュリティアセスメントにもとづきネットワークセキュリティとしての要求条件の明確にする
c）セキュリティ機能アーキテクチャ…セキュリティリクワイヤメントに従ってネットワークで必要となる機能条件の明確にする
d）セキュリティ実現アーキテクチャ…セキュリティ機能アーキテクチャの現実のネットワークへのマッピング

このセキュリティアーキテクチャを用いることにより、ネットワークのユーザは、ネットワークが提供するセキュリティサービスを把握，選択することが可能となり、ネットワークの設計者は、セキュリティ上の要求に応じて具体的なセキュリティ技術を用いたセキュリティサービスを提供することが可能となる。

さらにセキュリティアーキテクチャに「セキュリティ対策エリア，無対策エリア」という面的な考え方を導入し、ネットワークの一部が侵害されても影響が全体に波及しないような局所化や、またセキュリティ対策によって管理されている「セキュリティ管理ユニット」の階層化の考え方を示している。

付録参考文献

［1］International Standards Organization, “Information Processing Systems - OSI RM. Part 2 : Security Architecture”, ISO／TC 97 7498-2, 1988

［2］中尾, “セキュリティ標準化動向”, 信学技報, ISEC90-7, 1990年7月

［3］S. Muftich et.al., “Security Architecture for Open Ditributed Network”, John Wiley & Sons, 1993

［4］K.Nakao、K.Suzuki, “Proposal on a Secure Communication Service Element (SCSE) in the OSI Application Layer”, IEEETransaction on Communications, Selected Areas in Communications, Vol.7 No.4, May 1989

［5］中尾、田中、鈴木, “OSIセキュリティ通信用SCSEの実装と評価”, 信学会 暗号と情報セキュリティシンポジウム (SCIS92), SCIS92-9D, 1992年4月

［6］原田、中島、吉田, “通信網におけるセキュリティについて”, 信学会, 第三回高度情報通信網の安全・信頼性シンポジウム, 1991年3月

［7］原田、中島、吉田, “通信網のセキュリティアーキテクチャについて”, 1991年信学秋大, SA-7-7