コンピュータセキュリティ　18－16
(2002. 7. 18)

# セキュリティ品質の一検討

村上　英世† 坂本　弘章‡ 幸　徳雄†

†東和大学工学部 〒815-8510 福岡市南区筑紫丘 1-1-1
‡(株)ＮＴＴデータ　ビジネス開発事業本部　セキュリティ事業部
〒212-0058　神奈川県川崎市南区鹿島田 890-12　WEST15F
E-mail: †{mura79, yuki}@tohwa-u.ac.jp, ‡ sakamotohra@nttdata.co.jp

あらまし　高度情報化社会における情報は、その障害によっては個人・企業のみならず人類全体に波及する被害もあり得る、重要かつかけがえのない財産である。セキュリティ品質の尺度・目標値案に関する別資料による提案に続き、その設計法について、①サービスシステムの規模別目標値、②システム機能・運用へのセキュリティ品質配分、③規模別セキュリティ品質設計の考え方、などについての一案を述べた。

キーワード　セキュリティ，品質，設計，品質目標

# Consideration on Security Quality

Hideyo MURAKAMI†, Hiroaki SAKAMOTO‡ and Norio YUKI†

† Department of Multimedia, Tohwa University , Fukuoka, 815-8510
‡ IT Security Center, NTT DATA CORPORATION, 890-12-16F kasimada Minami-ku kawasaki-si, 212-0058
E-mail: †{mura79, yuki}@tohwa-u.ac.jp, ‡ sakamotohra@nttdata.co.jp

**Abstract**　In advanced information society, information .trouble effects on not only one person or company but also human continuation. Information is important property. On the basis of the previous paper proposal, this describes consideration on security quality design method that includes quality objectives for each scale of a service system, quality allocation for both of system function (soft ware and hardware) and operation people, design concept of security quality.

**Keyword**　Security, Quality, Design, Objective

## 1. はじめに

高度情報化社会における情報は、その障害によっては個人・企業のみならず人類全体に波及する被害もあり得る、重要かつかけがえのない財産である。情報のセキュリティを確保するために、既に多くのセキュリティ技術の研究が進められている(1)(2)(3)。一方、各種情報サービスにおけるセキュリティ品質の目標値、設計法については研究があまり進んでいない。そこで、まずセキュリティの品質コンセプト、品質尺度、などについてのコンセンサスを醸成し、それに基づいて我が国におけるセキュリティ品質基準の策定および一定レベルのセキュリティ品質の実現が望まれる。そこでセキュリティ品質の技術基盤を構築することをねらい、セキュリティ品質の研究の必要性を著者らは、資料(4)で提案し、主に装置で実現されるセキュリティ機能の品質について考察した。本文では、運用におけるセキュリティ品質まで拡張し、設計法について検討している。

ここでのセキュリティ品質の対象としては、全ての情報サービスシステムを前提としている。従ってここで検討しているセキュリティ品質は、情報サービスシステムを計画・構築・運用する際に、提供する官庁・企業や提供サービスに依存しないでセキュリティ品質を相互に比較・設計できるため、セキュリティ品質の基盤技術として有用であろう。

既にセキュリティ品質の尺度として、「セキュリティ障害時に及ぼす社会的な迷惑度合い」を提案した(4)。本文では、提案に基づく設計法についての研究経過を報告する。

## 2. セキュリティ品質の尺度と目標値

セキュリティ品質の研究は、表１に示すように、情報サービスシステムに関する広い適用範囲と効用をねらっている。

このような適用範囲を考慮すると、セキュリティ品質は、２つの側面（①サービス提供者から見たセキュリティ品質、②サービスユーザから見たセキュリティ品質）を持つと思われる。

### 2.1. セキュリティ品質の尺度

まずはサービス提供者(サービスシステムの経営者、管理者、運用者など)から見たセキュリティ品質について述べる。セキュリティ品質の尺度は、表２に示すような条件を考慮して、主観的な「セキュリティ障害時に及ぼす社会的な迷惑度合い」として、既に資料(4)で提案している。

表1　セキュリティ品質の対象範囲と設計の効用

| | |
|---|---|
| 対象範囲 | 情報サービスシステム |
| | ソフトウェア、ハードウェアと関連する人間 |
| | 時間空間に分布したサービスシステム |
| 設計の効用 | セキュリティ品質が設計・運用可能 |
| | 他企業・他サービス間のセキュリティ品質の比較 |
| | セキュリティ品質バランスのとれたサービスシステム構築 |

表2　セキュリティ品質の尺度・測度の条件

| | |
|---|---|
| 尺度の条件 | 障害の社会への影響度を表現<br>・時空間の広がりをカバー　・ハードソフトシステムと人間を含む |
| | あらゆる情報サービスに対して適用 |
| | 主観に結びつく |
| 測度の条件 | 障害の社会への影響度：頻度、強さ・広さ、時間長さ |
| | 実測可能、測定点がある、相加則があること |
| | セキュリティ機能技術に依存せずに適用可能 |

表3　セキュリティ品質の測度の提案

| | |
|---|---|
| 測度1 | 障害の発生頻度<br>（回/年） |
| 測度2 | 被害の規模<br>（人・円） |
| 測度3 | 障害の影響からの回復期間<br>（時間） |

サービス提供者から見た場合、サービスシステムの設計・管理・運用を実施するために可能であれば、セキュリティ品質を客観化し数値化する必要がある。かつ数値化されたセキュリティ品質度合いを持つ機能素子を組み合わせて、サービス全体や運用のセキュリティ品質度合いを求められるようにする必要がある。

そこでセキュリティ品質を客観化・数値化するために、セキュリティ品質測度を、表３に示すように、３つの測度で具体化した。前記の条件をこれらの３つの測度では満たしている。これらの測度で、「測度１で、障害発生の時間的発生状況」、「測度２で、障害の大きさ」「測度３で、障害発生からの回復のしかた」を規定している。

これらの３測度以外の候補として、「障害発生の密度」、「障害発生の回数」、「障害の金額」、「障害の被害人数」、「障害発生からの回復時間」、などいくつか考えられる。ここでは、できる限り、独立した測度を選び、測度数をしぼることを前提に、上記の３測度とした。

一方、サービスユーザから見た場合には、「情報セキュリティ障害が及ぼす社会的な迷惑」をどのように考えれば良いのだろうか？ユーザにとって障害でサービスが利用できない自体も問題ではあるが、個人情報の漏洩が最重要問題であろう。

また、サービスユーザも個人と企業・団体が活動の手段として使用する場合がある。この場合の企業・団体については間接的な管理・運用者であり、サービスユーザは団体内の個々の使用者である。このときの企業・団体に対しては、セキュリティ品質の尺度は、「情報セキュリティ障害が及ぼす社会的な迷惑」を用いても良いかもしれない。

しかし、サービスを利用するサービスユーザ個人にとっては、「情報セキュリティ障害は及ぼす個人的な迷惑」である。情報の価値が個人にとって大きく異なるため、情報障害の被害程度を統一的に取り扱えない。すなわち、個人ユーザにとってどのような障害でも規模は１件であり、回復時間は、個人情報の漏洩であれば無限時間の可能性もある。このように考えるとユーザにとっては一生に一度も起きないことが唯一の要求条件であるかもしれない。少なくとも全ての個人ユーザにとって重要な測度は、表３に示されるセキュリティ品質尺度に要求される条件では、①条件；測度１のみである。つまり、１案として、セキュリティ障害の発生頻度を測度とすることを提案する。（個々個人にとって取り返しがきかないセキュリティ障害の発生頻度を１００年に一度以下とすれば、十分であろう。社会的コンセンサスや実態値での確認が必要。）このようにすることで、２つの側面（①サービス提供者から見たセキュリティ品質、②サービスユーザから見たセキュリティ品質）のセキュリティ品質を、唯一の尺度・測度で表現できる。

そこで、サービスシステムの設計・管理・運用のためのセキュリティ品質を、上記３つの測度を使用して研究するなかで、サービスユーザから見た場合について検討していき、重要な問題がでれば見なおすこととする。

### 2.2. セキュリティ品質目標値案

セキュリティ品質目標値の案を、セキュリティ障害の影響回復時間が短期である場合について、表４、図１および図２に示す。セキュリティ品質目標値は、その実態を考慮せずに、障害の影響が及ぼす度合いを念頭に著者の１案として示している。今後セキュリティ品質の実態調査・把握を進め、多くの方々からのご意見や情報をいただき、セキュリティ品質目標値の案を見直す考えである。

表4　セキュリティ品質の目標例

| 規模 | 発生頻度目標値 | 備考 |
|---|---|---|
| 100億円・人<br>（レベル1） | ≦ 0.001/年 | 中企業・市の運営に影響<br>（100万円・1万人） |
| 10,000億円・人<br>（レベル2） | ≦ 0.0001/年 | 大企業・県の運営に影響<br>（100万円・100万人） |
| 1,000,000億円・人<br>（レベル3） | ≦ 0.00001/年 | 国家の運営に影響<br>（100万円・1億人） |
| 100,000,000億円・人<br>（レベル4） | ≦ 0.000001/年 | 地球・人類の存続に影響<br>（100万円・100億人） |

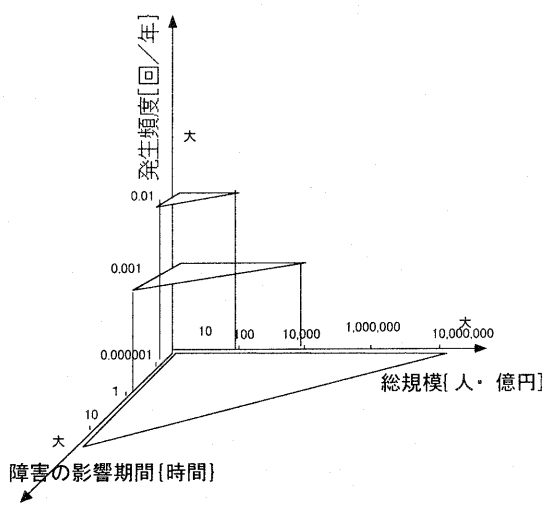


図1　セキュリティ品質目標値（例）

## 3．　セキュリティ障害

### 3.1　セキュリティ機能

本文では、セキュリティ機能を、①サービスを運用している人間が果たすセキュリティ機能（以下では運用と略す）と②サービスシステム（装置類）に盛り込まれたセキュリティ機能（システムのソフトウェアとハードウェアの機能・手順であるが、以下ではシステム機能と略す）に大別する。運用については、以下の節で述べる。

システム機能については、その主要なセキュリティ機能の例を、表５に示す。

### 3.2　セキュリティ品質の劣化要因

(1) セキュリティのシステム機能

サービスシステムのセキュリティ障害が生じる要因としては、本文では、全て外部からの悪意による行為を前提とする。従って、表５に示すセキュリティ機能が劣化する頻度は、悪意の度合いや技術の進展に依存し、時々刻々変化する。それらのセキュリティ障害が生じる頻度は、調査が進んでおらず、実態値が不明である。（本文では以下の節で必要であるため、著者のかってな想定値を、付表１に示す。）

(2) セキュリティの運用

サービスシステムの運用者、管理者、サービス利用者は、セキュリティの運用を果たしている。例えば、サービスシステムの運用者は、パスワードを自分以外にもれないようにして、「認証におけるパスワードの秘密保持」を実施している。

各運用者の情報アクセス権限は一定の範囲（レベルa）に限定されており、その限界を超えるレベルｂの情報にアクセスする時に、上位運用者の認証などを必要とする場合を考える。このとき、レベルｂの情報は、セキュリティの運用すなわち「認証におけるパスワードの秘密保持」が２重に設置されていることになる。これは、「システムにおける２重の認証機能」とは、異なる。つまり１人の運用者が、２つのパスワードを使って運用するのとは異なる。このような、運用人間によるセキュリティ機能の主要なものを表６に示す。

本文では、「システムの認証機能」と、「認証におけるパスワードの秘密保持」とを区別して取り扱っている。この例から想定されるように、セキュリティの運用は複雑に構成でき、構成によってセキュリティ障害の発生頻度は大きく異なる。本文では、悪意によるセキュリティ障害を想定しているため、運用者の意思に反してセキュリティ障害を起こす場合を考慮する必要があるとしている。運用者がセキュリティ障害を起こす要因としては、表７に示すものを想定すべきであろう。

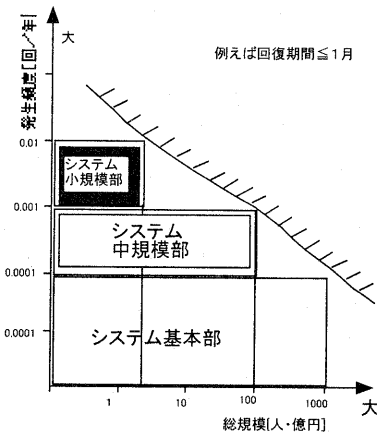


図2　セキュリティ品質目標値（例）

表5　システム機能・装置における主要なセキュリティ機能の例

| 不正行為 | セキュリティ機能・対策 |
|---|---|
| 盗聴・漏洩 | ファイアワール、データの暗号化 |
| 改竄 | ディジタル署名 |
| なりすまし | 端末・端末間の認証：ディジタル署名、<br>端末・本人間認証：指紋、網膜、ﾊﾟｽﾜｰﾄﾞ |
| 事後否認 | ディジタル署名 |

表6　運用における主要なセキュリティ機能例

| セキュリティ機能 | 備考 |
|---|---|
| 運用人間数とその機能関数 | ・例、２人のﾊﾟｽﾜｰﾄﾞで運用 |
| 運用人間の機能関数の秘密保持 | ・ﾊﾟｽﾜｰﾄﾞ担当名を秘密 |
| ﾊﾟｽﾜｰﾄﾞの秘密保持 | |
| IDカード・指紋・網膜の秘密保持 | |

表7　運用者がセキュリティ障害を起こす要因例

| セキュリティ機能障害要因 | 備考 |
|---|---|
| 脅迫 | ・未確定の人は脅迫されない<br>３人以上は脅迫されない。 |
| 買収 | ・経営者は買収されない。<br>３人以上は買収されない。 |
| 秘密の漏洩 | ・ﾊﾟｽﾜｰﾄﾞとうの秘密 |
| 運用人間の倫理 | ・運用人間が障害を起こす |

## 4. サービスシステムの機能モデル

サービスシステムの機能ブロックモデルの考え方として、①実態システム機能構成を模擬する、②システム機能と運用と分離する、③多数の低処理機能と少数の高処理機能で構成する、ことを前提とした。一例として、サービスシステムの機能ブロックモデルを図3に示す。

対象としたサービスシステムは、1個のデータ記憶・処理装置、管理用の端末 T0 とそのアクセス制御装置 A0, 支店内設置の n1 個の端末 T1,1...T1,n1、その通信ネットワークとアクセス制御装置 A1、支店外設置の n2 個の端末 T2,1...T2,n2、その通信ネットワークとアクセス制御装置 A2 から構成される。

データ記憶・処理装置は、本社などに設置されたサービスシステムにおける唯一の大型処理装置で、サービス全体を運用している。

T1,i は、各支店などに設置されたサービスシステムにおける中型処理装置を介した端末で、各支店毎の運用をしている。アクセス制御装置 A1 は、各支店などに設置された T1,i を通信ネットワーク経由で n1 個収容してアクセス制御している。

T2,j は、小さな支店や街角などに設置されたサービスシステムにおける小型処理装置を介した端末である。アクセス制御装置 A2 は、各支店などに設置された T2,j を通信ネットワーク経由で n2 個収容してアクセス制御している。

T0 はそのアクセス制御装置 A0 を介して、管理者が使用してサービス全体の管理をしている。T0 からの情報処理は、1処理で全データ領域を対象にでき、かつデータ値にも上限がない。従って T0 を介したセキュリティ障害が生じた場合、全サービスにわたる被害・影響が出ることが想定され、影響額は 100 億円と仮定する。

T1,i からの情報処理は、従業員の運用者が実施し、定形入出力で、1処理で中規模の特定領域のデータ記憶領域を対象にでき、かつサンプル値に一定の上限：M1 がある。従って T1,i を介したセキュリティ障害が生じた場合、特定のサービスにわたる被害・影響が出ることが想定され、影響額は 10 億円とする。

T2,j からの情報処理は、サービスユーザが利用し、定形入出力で、1処理で小規模の特定領域のデータ記憶領域を対象にでき、かつサンプル値に上限：M2 がある。従って T2,j を介したセキュリティ障害が生じた場合、特定のサービスにわたる被害・影響が出ることが想定され、影響額は 1 億円とする。

サービスシステムモデルをシステム機能と運用の面からモデル化すると、図4のように表わせる。図4では、セキュリティ機能 Fa0 と Fm0 は、データ記憶・処理装置の全領域に並列に接続されている。従ってセキュリティ品質の観点からは、どちらの機能を介しても全領域のデータを処理できることを示している。

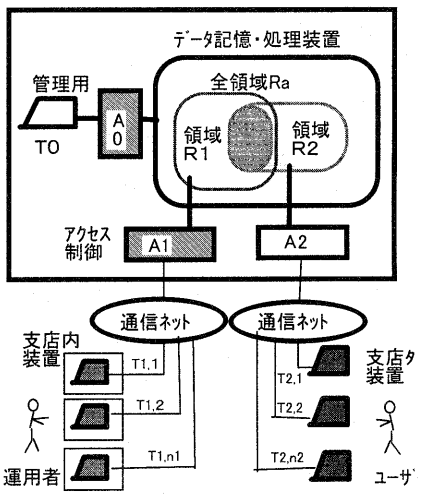


図3　サービスシステムの機能ブロックモデル

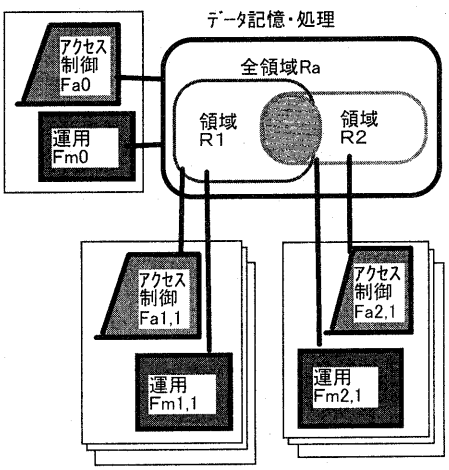


図4 サービスシステムのセキュリティ機能モデル

言い換えると、装置のセキュリティ機能をいくら性能良くしても、運用者が買収されることがないようにしたり、１人の運用者が買収されても障害を起こさないように運用のセキュリティ品質を良くしないとダメである。ただし、ここで述べている運用セキュリティは、運用上の倫理や運用マニュアルの整理などではなく、節 3.2 で述べた運用人間の処理機能・手順である。従って容易に、しかけとして利用でき、そのセキュリティ性能を演算できるものである。

モデルの中で、通信プロトコル１～７におけるセキュリティ機能（ノード間・端末相互間での暗号や折り返し確認など）は、１つのアクセス制御によるセキュリティ機能 Fa0、Fa1,i、Fa2,j として表示した。

運用として、管理者の機能を運用 Fm0、Fma1,i、Fm2,j として記述した。

このモデルの特徴は、データ記憶処理領域が、①各アクセス端末で異なること、②システム機能と運用は、セキュリティ品質の観点からは並列機能となっていること、である。この並列機能となっている点は、どちらかの機能を介すれば、データにアクセスできることを意味している。

## 5. セキュリティ品質設計法

### 5.1 セキュリティ品質設計の考え方

セキュリティ品質の目標値は、法律もしくは企業内規として、既に存在するとするものとする。セキュリティ品質は、上記３つの測度を用いて目標値を満たすように設計される。複数の測度を用いた設計は、面倒ではあるが、コンピュータを用いた設計は、同時に３つの測度による目標を満たすように設計することは容易であると考える。

また、セキュリティ品質がいくら良くても使いがってが悪いと使用されない。このため、設計は、原則的に、「日常的に何度も運用されるものは、一定のセキュリティ品質を確保しつつ使い易く」、「１ヶ月に一度とか、まれに運用されるもの（かつデータ領域が広く・データ値が高いもの）は、使い勝手が悪くても高度のセキュリティ品質を確保する」方向で対処する。このため、サービスシステムを規模別にセキュリティ品質レベルを分ける。すなわち、日常的に何度も運用されるものは小規模に構築し、セキュリティ品質は低いが使い易くし、まれに行う全システム保守などは使いにくいが高セキュリティ品質にすることが可能となる。

また、測度１のセキュリティ品質障害の影響期間が、障害発生頻度に比較して同程度もしくは長い場合は継続研究するものとして、ここでは、セキュリティ品質障害の影響期間が、障害発生頻度に比較して短い場合を考える。

### 5.2 セキュリティ品質設計例

ここでは、100 億円規模の情報サービスで、図３に示すような機能ブロックで構成して、実施している場合を例にとって、セキュリティ品質設計例を述べる。

(1) セキュリティ品質設計のステップ１：

セキュリティ品質設計の対象としているサービスシステムの属性を明確化し、セキュリティ品質の目標値を選定する。サービスシステムの以下の２項目を求める。

①セキュリティ品質障害の発生箇所（種類）：人がアクセスして情報処理する時空間経路や情報蓄積装置など

②セキュリティ品質障害種類毎の影響規模：その時空間経路や情報蓄積装置での情報障害によって生じる影響規模

上記２項目の値に対応したセキュリティ品質障害種類毎の発生頻度目標値を選定する。ただし、セキュリティ品質障害の種類は、悪意による情報障害を対象とする。

(2) セキュリティ品質設計のステップ２：

セキュリティ品質障害の回復期間は、発生頻度目標値に対応する期間に比べ短いことを仮定して、そのサービスでの最大値回復期間の障害を対象に設計する。

サービスシステムは、人間（運用）とサービスシステム装置（システム機能）で構成され、セキュリティ品質障害要因は、この２つに大別する。従って、セキュリティ品質目標値をこれらの障害要因に配分する。ここでは、５０％に等配分することとする。

(3) セキュリティ品質設計のステップ３：

セキュリティ品質障害規模毎に障害発生頻度目標値を、サービスシステム装置に 50%に分けて設計する。サービスシステム装置は、多くのサブ装置で構成されており、障害規模毎の発生頻度目標値の 50%を分配す

る。

①全サービスユーザのセキュリティに関する大規模部分(100 億円規模障害)は、アクセス端末 A0 とデータ記憶・処理装置の基本部分(例えば OS、サービスシステムのデータシステム)である。この部分に対してはレベル 2 発生頻度目標値の 50%を配分する。

②中規模部分(10 億円規模障害)は、アクセス端末 T1,i、通信ネットワーク、等である。この部分に対してはレベル 1 発生頻度目標値の 50%を配分する。

③小規模部分(1 億円規模障害)は、アクセス端末 T2,j、通信ネットワーク、等である。この部分に対してはレベル 0(表 4 には未記入)発生頻度目標値の 50%を配分する。

(4) セキュリティ品質設計のステップ 4 :

セキュリティ品質障害規模毎に障害発生頻度を、運用に 50%に分けて設計する。

①アクセス端末 A0 で管理運用する運用 Fm0 は、全サービスユーザのセキュリティを左右できる。この部分に対してはレベル 2 発生頻度目標値の 50%を配分する。

②中規模部分での運用 Fm1,i は、多数のサービスユーザのセキュリティを左右できる。この部分に対してはレベル 1 発生頻度目標値の 50%を配分する。

③小規模部分での運用 Fm2,j は、小数のサービスユーザのセキュリティを左右できる。この部分に対してはレベル 0 発生頻度目標値の 50%を配分する。

(5)セキュリティ品質設計のステップ 5 :

想定している全サービスシステムのセキュリティ機能の障害発生確率をそれぞれ求め、対応する演算で各部の発生確率を順次求めて全体の障害発生確率を得る。但し、各種のセキュリティ機能の障害発生確率は、手順、人間関係などを考慮して、個々に求める必要がある。全体の障害発生確率が目標値を満たさない場合は、再度、各部のセキュリティ機能の障害発生確率を低くするように機能の向上を図る。設計結果の例を、図 5 に示す。

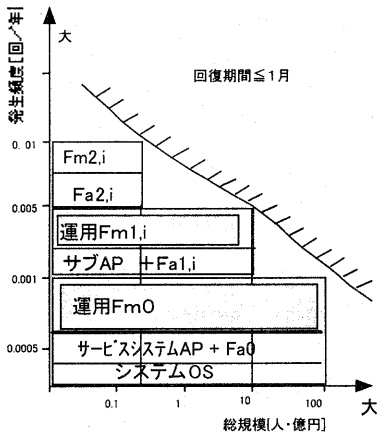


図5 セキュリティ品質設計(例)

## 6. 考察およびまとめ

セキュリティ品質の尺度・目標値案に関する別資料による提案に続き、その設計法について、①サービスシステム構築での規模別目標値例、②システム機能・運用への配分、③運用の障害発生の考え方、などについての一案を述べた。今後、個々のセキュリティ機能障害発生の実態調査、システムにおけるセキュリティ品質の総和関数の具体化、未解決な課題を継続検討する考えである。

### 文 献

[1] 大山永昭、次世代ＩＣカードシステムと暗号技術, 電子情報通信学会誌, vol.83,no.2,pp.91-95, 2000 年 2 月

[2] 前川徹、暗号技術と電子商取引, 電子情報通信学会誌, vol.83,no.2,pp.96-100, 2000 年 2 月

[3] 岡本龍明、電子マニー, 電子情報通信学会誌, vol.83,no.2,pp.101-106, 2000 年 2 月

[4] 村上英世、幸徳雄、セキュリティ品質について、信学技報 CQ2001-59,2001 年 11 月

付録　セキュリティ品質障害発生頻度（仮定値）

この数年で新聞をにぎわす金融・保険関連の使い込みは数軒/年発生し、被害額は犯罪者年収の 10 倍以上の被害額（約 10 億円）である。また、発生件数を、表面に現れる 10 倍とかってな推定すると、30 件/年、程度と仮定する。

また、一部上場の金融・保険関連会社数は、約 140 会社である。支店端末数(または人間運用機能数)を 1,000 個/会社、とすると、発生頻度は、30/(140 x 1,000) ≒2E-4 である。（この実態値 2E-5 は｛10 億円の被害額＋信用失墜の被害額｝が発生する 1 支店での発生頻度で、100 億円の影響であればその目標値例：0.001 を満たす）

（今後継続的に実態調査を実施する）