社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2007－DPS－130 (37)
2007－CSEC－ 36 (37)
2007／3／1

利便性とセキュリティの動的移行による ユーザ要求の自動交渉方式の検討

加藤 弘一　　勅使河原 可海

創価大学大学院工学研究科

〒192-8577 東京都八王子市丹木町 1-236

E-mail: {kokatou, teshiga}@soka.ac.jp

あらまし 一般に，組織のネットワークにおいて，ユーザが通常利用できないサービスを特別に利用するためには書類等により申請を行う．しかし，管理者による審査の妥当性を証明することは難しい．本稿では，ユーザと管理者が利便性とセキュリティの両観点から特別利用の実施可否を交渉する方式を検討する．特別利用のために対策レベルを低下させるとリスク発生確率が増加するため，多層防御の概念に基づき，他対策を強化してリスク発生確率を抑制する．しかし，他対策を強化するとユーザは新たな制約を受けて利便性が低下する．そこで，フォルトツリー解析を用いてリスク発生確率とユーザの利便性を定量的に算出し，管理者はリスク発生確率を，ユーザは新たな制約をそれぞれ許容できるかどうかで特別利用の実施可否を決定する．本交渉方式により，ユーザの状況に応じて利便性とセキュリティを動的に移行し，利便性とセキュリティの両立を実現する．

キーワード 利便性とセキュリティ，交渉，多層防御，フォルトツリー解析，リスクマネジメント

A Study on an Automatic Negotiation Method for Users' Requests Based on Dynamic Changes between Usability and Security

Koichi KATO　　Yoshimi TESHIGAWARA

Graduate School of Engineering, Soka University

1-236 Tangi-cho, Hachioji, Tokyo, 192-8577 Japan

E-mail: {kokatou, teshiga}@soka.ac.jp

Abstract Generally, in the network of the organization, a user must submit an application by papers if the user wants to use specially some services which the user cannot use usually. However, it is difficult to prove the appropriateness of the administrator's judgment. In this paper, we study on a negotiation method to decide whether the user's request can be allowed considering usability and security. Because the probability of risks increases, when the level of safeguards becomes lower in order to achieve the user's request, the probability of risks should be made smaller by reinforcing other safeguards based on the concept of Defense In Depth. On the other hand, the user is forced new restrictions by their reinforcement. Therefore, our method calculate quantitatively the probability of risks and the usability for users by means of Fault Tree Analysis, then decide the result of negotiation when the administrator and the user accept the risk probability and usability each other. We can achieve a good balance between usability and security by changing them dynamically as the user's situation.

Keywords Usability and Security, Negotiation, Defense In Depth, Fault Tree Analysis, Risk Management

1. はじめに

近年，ホームネットワーク，企業や大学など組織のネットワーク，公共空間における高速無線アクセスポイントなど，インターネットを利用できる環境が整備されつつある．それに伴い，複数のネットワーク環境を利用するユーザも増加傾向にある．今後，ユビキタスネットワークが確立され，いつでもどこでもネットワークが利用できるようになった場合，ユーザは当然のように多くのネットワーク環境

を利用するようになると考えられる．

この際，どのようなネットワーク環境においても，ユーザが望む端末・サービスを自由に利用できる十分な利便性と，ユーザや組織が保有する情報資産を保護できる十分なセキュリティを確保し，両立することが重要となる．しかし，一般に利便性とセキュリティはトレードオフの関係にあり，過度のセキュリティは利便性を損ない，一方で利便性を重視しすぎるとセキュリティが不十分となるため，適切なバランスを維持し，両立することは非常に困難である．さらに，ネットワークの運用形態や，求められる利便性とセキュリティのバランスは環境や組織によって異なるため，利便性とセキュリティの両立が可能なネットワークを構築するための汎用的な手法は確立されていない．

本研究では，ネットワーク利用時における利便性とセキュリティの両立を目的とし，特に本稿では組織のネットワークにおけるネットワークサービスの利用に焦点を当て，セキュリティを維持しつつユーザがサービスを自由に利用できるようにするための手法について述べる．まず2章で，ネットワーク利用の現状と課題，我々のアプローチを明確にする．3章では，セキュリティの確保において重要である資産・脅威・対策の関係と多層防御の概念，リスク発生確率やユーザの利便性を算出するためのフォルトツリー解析について述べる．そして4章で，リスク発生確率と利便性の変動をもとにユーザの望むサービスが利用可能かどうかを交渉する方式と，利便性とセキュリティの両立の展望について述べる．最後に，5章でまとめる．

2. ネットワーク利用の現状と課題

2.1 セキュリティポリシーの遵守

現在，組織のシステムを適切に運用・管理するための情報セキュリティマネジメントシステム（ISMS）の構築が重要視されている．国内ではISMS適合性評価制度が存在し，ISMS認証取得事業者数も年々増加している[1]．

ISMSを構築し，ネットワークのセキュリティを確実なものとするためには，組織が保有する守るべき資産を明確にし，脅威や脆弱性を洗い出し，適切な対策を選択することが重要である．その一方で，組織の目的達成に必要な利便性を確保することもまた重要である[2]．そして，多くの組織では利便性とセキュリティのバランスを考慮し，ネットワークの利用・運用・管理方針や具体的手順を定めたセキュリティポリシーを策定している．ユーザはセキュリティポリシーの遵守が原則であり，利用が許可された範囲内でネットワークを利用することができる．そのため，ユーザは利用できることと利用できないことが明確に分かれる一方で，その組織が目指すセキュリティは確保される．

2.2 特別な利用の申請・審査と課題

セキュリティポリシーの遵守がユーザに求められているが，実際には企業における業務遂行のため，または大学における研究活動のためなど，通常時には利用できないサービスを特別に利用したい場合もある．一般に，ユーザが特別な利用を実施したい場合には管理者へ書類等により申請を行い，管理者（厳密には経営者などの意思決定者かもしれない）が審査することで申請内容の実施可否を決定する．しかし，管理者が申請内容を審査するためには多くの知識や経験が必要であり，容易に判断することはできない．さらに，審査結果の妥当性を客観的に証明することは困難である．

我々は，ユーザが自由にネットワークを利用するためには，通常利用できるサービスに加え，通常時には利用できないサービスも許可を得ることで自由に利用できることが重要であると考える．ただし，そのためにはセキュリティ上の問題が発生しないように，十分なセキュリティを維持することが求められる．そして，これら自由な利用とセキュリティの維持を実現するためには，特別な利用の実施可否を客観的に審査する仕組みが必要である．

2.3 利便性とセキュリティを考慮した交渉方式

本研究ではこれまで，ユーザと管理者が利便性とセキュリティの両観点から特別な利用の実施可否を交渉する方式について検討してきた[3]．この方式では，一つの脅威に対して様々な箇所で対策を施すことで堅牢なセキュリティを確保するという多層防御の概念に基づき，特別な利用を実施するために現在のある対策の強度を低下させる代わりに，他の対策を強化することでリスクの発生を抑制する．しかし，他対策を強化した場合にはユーザに新たな利用上の制約が発生することになる．そこで，管理者はリスクの抑制ができるかどうか，ユーザは新たに発生する制約を許容できるかどうかのそれぞれの観点から交渉を行い，特別な利用の実施可否を判断する．しかし，この方式では対策の変化に伴うリスク発生確率やユーザの利便性の変動がどの程度であるかが不明瞭であり，どの対策を強化することが妥当か判断することができなかった．

そこで本稿では，フォルトツリー解析を利用して対策の変化によるリスク発生確率と利便性の変動を定量的に算出し，特別な利用を実施するために強化すべき対策の組合せを導き出す．そして，ユーザと管理者の両者が許容できる組合せを選択することにより特別な利用の実施可否を交渉する方法を述べる．本交渉方式により客観性かつ妥当性のある交渉を可能とし，ユーザの利用状況に応じて利便性とセキュリティを動的に移行させることで利便性とセキュリティを両立することを目指す．

3. 本方式で用いる技術

2.3 節で述べたように，セキュリティを維持しつつユーザが通常時には利用できないサービスを特別に利用するためには，様々な対策を変化させる必要がある．そのためには，対策とリスクの関係を明確にすることが必要である．そこで，まず資産・脅威・対策の関係を整理する．また，様々な箇所で対策を実施することでリスクを抑制する多層防御の概念について述べる．

さらに，対策レベルの変化に伴うリスク発生確率と利便性の変動を定量的に求めることが必要である．そこで，定量化手法として用いるフォルトツリー解析（FTA：Fault Tree Analysis）の概要を述べる．

3.1 資産・脅威・対策の関係

一般に，資産と脅威は多対多，脅威と対策も多対多の関係にある．中村氏らは，この関係をモデル化し，セキュリティ対策選定問題の定式化を行っている[4]．このモデルでは，リスクアセスメントおよびリスク対応の結果を図1のように表現している．

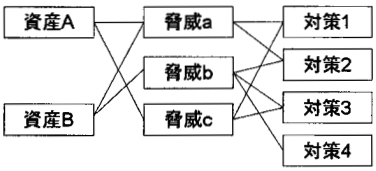


図1 資産・脅威・対策の関係

リスクアセスメントにおける「脆弱性」が図1には明記されていないが，これは脆弱性を考慮していないということではない．ある資産にとって，脆弱性を突く脅威のみが本当の脅威であり，脆弱性と結びつかない脅威は脅威ではないとの考えから，このモデルにおいて資産と脅威が線で結ばれるかどうかに脆弱性の考えを置いている．

本交渉方式では，この関係を利用することで，特別な利用の実施のために対策を変化させた場合にどの資産・脅威に影響が発生するか，またその影響を抑制するためにどのような他の対策があるかを明確にすることができる．

3.2 多層防御の概念と拡張モデル

多層防御とは，データ，アプリケーション，マシン，ネットワーク，外部ネットワークとの境界といった様々な箇所で対策を取ることで資産に対する脅威の発生を防ぐという概念である．Microsoft 社はセキュリティ対策には多層防御が効果的であると述べ，多層防御セキュリティモデルを示している[5, 6]．例えば，ネットワークにファイアウォール（FW）を設置し，端末にパーソナルファイアウォール（PFW）やウィルス対策ソフトを導入することでウィルスやワームの感染を防ぐことができ，もしこれらの対策の一つが損なわれても他の対策により感染する可能性を抑制することができる．意識しているかどうかにかかわらず，多くのネットワークにおいて多層防御は当然のように実施されている．特別な利用を実施するためにある対策のレベルを低下させても他の対策を強化すればリスクの発生を抑制することができるという本研究の考えは，この多層防御の概念に基づいている．

また，Microsoft 社の多層防御セキュリティモデルでは各層における対策の実施を表現できるが，本来は守るべき資産がどの層に位置づけられるか，脅威がどの層からどの層へ向けて発生するのかも考慮すべきであり，また脅威が層から層へと移る際に効果を発揮する対策もあると考えられる．そこで本研究では，Microsoft 社の多層防御セキュリティモデルを拡張し，資産の位置づけ，脅威の発着点，層間の対策も表現できるようにした[3]．本研究の拡張多層防御セキュリティモデルを図2に示す．なお，詳細な使用方法については4.2節で述べる．



図2 拡張多層防御セキュリティモデル

3.3 フォルトツリー解析（FTA）

信頼性・安全性工学の分野において古くから使われている代表的な信頼性分析手法である[7, 8]．望ましくない故障（不安全事象）を定義し，その故障が発生し得る原因を下位へ枝状に分解して木（フォルトツリー）を作成し，論理的・定量的に故障評価を行う，トップダウンアプローチによる分析手法である．まず，リスクを頂上事象とし，頂上事象の発生原因を論理ゲート（AND，OR など）で繋ぎ木を作成する．そして，最も重要な基本事象の組（最小カットセット）を見つけ，不信頼度（発生確率）を計算する．この結果をもとに，どの部分に対策を施せばよいかを判断することができる．フォルトツリーを利用したリスクマネジメントとして，佐々木氏らは経営者，従業員，顧客といった意思決定者の間で合意を形成するためのリスクコミュニケーションを実現する多重リスクコミュニケータについて研究しており，その中で FTA を用いてリスクの定量化などを行っている[9]．また，対策の最適組合せを決定するために FTA を利用し，離散型最適化問題として定式化している[10]．

本研究ではこの FTA を利用して，リスク発生確率やユーザの利便性を定量化する．リスク発生確率を算出するためのフォルトツリーは，頂上事象に発生が望ましくないリスクを置き，対策実施の有無によってリスクが発生する確率が変化すると捉えて対策を基本事象とする．一方，ユーザの利便性を算出するためのフォルトツリーは，ユーザが利用するサービスを頂上事象に置き，対策実施の有無によって利便性の大きさが変化すると捉えて対策を基本事象とする．これにより，リスク発生確率とユーザの利便性を定量的に求めることができる．

4. 利便性とセキュリティを考慮した交渉方式

4.1 交渉手順

まず前提として，すでにリスクアセスメント・リスク対応は実施されているものとし，各対策におけるリスク抑制の効果や利便性への影響は定量化されているものとする．

初めに，リスクの発生に関するフォルトツリーを作成する．リスクの発生に結びつくまでには，いくつかの攻撃ステップが存在する．そして，各攻撃ステップが成立しないように対策を取ることで，リスクの発生を防ぐことができる．したがって，リスクに対するフォルトツリーは図３のように作成することができる．一攻撃ステップへの対策は，一つでも実施すればよい場合や，複数個実施しないと防げない場合など様々考えられるため，適切な論理ゲートを選択する必要がある．また，攻撃ステップの一つでも防ぐことができればリスクは発生しないと考え，各攻撃ステップの対策を最終的にまとめる論理ゲートは AND としている．

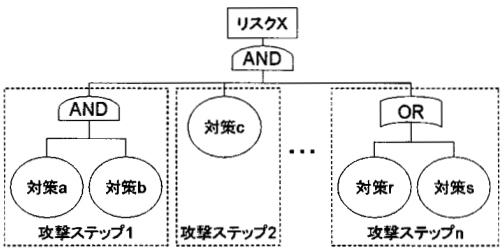


図３　攻撃ステップに基づくリスクのフォルトツリー

次に，ユーザの利便性に関するフォルトツリーを作成する．リスク発生の考え方と同様，ユーザがサービスを利用するためには，いくつかの利用ステップが存在する．しかし，対策を実施することで十分な利用ができないステップが発生する．したがって，ユーザの利便性に対するフォルトツリーは図４のように作成することができる．各利用ステップに影響する対策は，適切な論理ゲートを選択する必要がある．また，利用ステップのいずれか一つでも妨げられると利便性が低下すると考え，各利用ステップの対策を最終的にまとめる論理ゲートは OR としている．

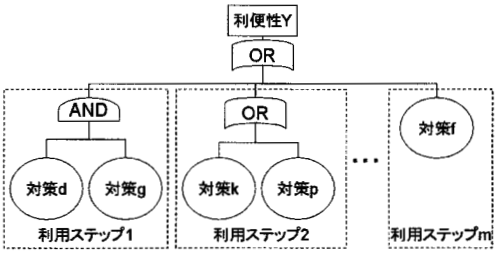


図４　利用ステップに基づく利便性のフォルトツリー

特別なサービスをユーザが利用するために対策を変化させる場合にはリスクに関するフォルトツリーを利用し，影響するすべてのリスクの発生確率を算出する．もし管理者がこの発生確率を許容できればユーザは特別なサービスを利用することが可能となるが，管理者が許容できない場合には他の対策を強化した際の各リスクの発生確率を求める．同時に，対策を強化した場合の各利便性も算出する．この中から管理者はリスク発生確率を，ユーザは利便性をそれぞれ許容できるような対策組合せを選択できればよい．しかし，実際には強化すべき対策の組合せ数は膨大であり，選択することは容易ではないため，リスク発生確率や利便性に対する制約条件を決め，強化すべき対策の組合せを絞り込む．そして，管理者とユーザの両者が許容できる対策組合せが選択できれば，ユーザが特別なサービスを利用することが許可される．

4.2 具体例

簡単な例により，本交渉方式の利用方法について述べる．まず，組織におけるリスクアセスメント・リスク対応の結果が図５のようであるとする．

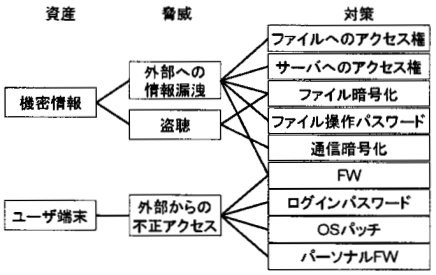


図５　リスクアセスメント・リスク対応の結果

ここで，ユーザが FW の FTP ポート開放を要求したとする．もし要求を許可した場合，機密情報の外部への漏洩，ユーザ端末への外部からの不正アクセスというリスクが増加する．そこで，まず情報漏洩に注目して攻撃ステップを整理する．3.2 節で述べた拡張多層防御セキュリティモデルでは，情報漏洩に関する資産の位置・脅威（各攻撃ステップ）の発着点・対策箇所を図６のように表現する．

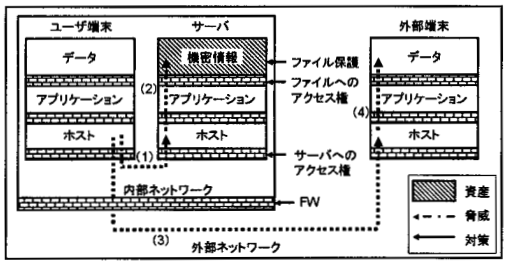


図６　情報漏洩に関する資産・脅威・対策の関係

情報漏洩に対する攻撃ステップは，(1)内部マシンから機密情報を保持するサーバへアクセスし，(2)サーバ内のファイルへアクセスし，(3)ファイルを FTP 経由で外部へ持ち出し，(4)外部のマシンでファイルを開くという流れである．(1)への対策はサーバへのアクセス権制御があり，具体的にはユーザアカウントによるアクセス制御，ユーザの利用するマシンの IP アドレスや MAC アドレスなどによる制御といった方法がある．(2)に対してはファイルへのアクセス権制御があり，ファイルそのものへアクセスできなくする，ファイルの操作権限を制御するなどの対策がある．(3)に対してはFWによる制御がある．(4)に対してはファイル自体を保護する対策が考えられ，具体的にはファイル操作のためのパスワードやファイル暗号化といった対策がある．これらの対策をもとに，情報漏洩リスクに関するフォルトツリーを図７のように作成する．

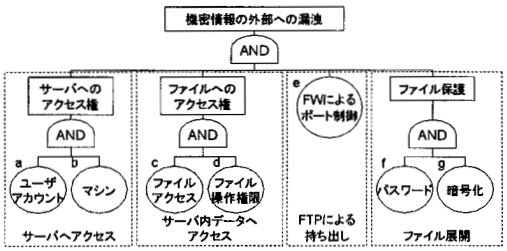


図７　情報漏洩リスクに関するフォルトツリー

同様に，機密情報の盗聴，ユーザ端末への外部からの不正アクセスのそれぞれのリスクについても，攻撃ステップをもとにフォルトツリーを作成する．

一方，利便性に関するフォルトツリーも作成する．この例では，図５の対策に関係する利便性のみを考えればよく，ファイルサーバの利用，サーバ内ファイルの利用，マシン利用，ネットワーク利用などが挙げられる．例として，サーバ内ファイルの利用という利便性についてのフォルトツリーを図８に示す．

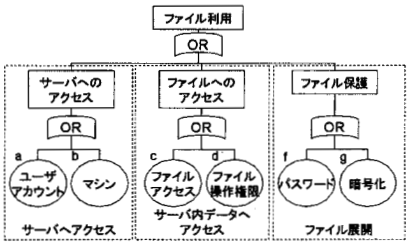


図８　ファイル利用の利便性に関するフォルトツリー

このように，関係するリスクと利便性のフォルトツリーを作成する．さらに，対策の実施または未実施による各リスクの発生確率と利便性の大きさを，すべての対策に対して割り当てる．各対策の実施・未実施によるリスク発生確率と利便性の大きさをそれぞれ表 1，2 に示す．なお，これらの数値は一般的なセキュリティ調査結果や組織における過去の計測結果などをもとに，専門家により決定されるべきである．

表１　対策の実施・未実施とリスク発生確率

リスク	対策		実施	未実施
情報漏洩	ユーザアカウントで禁止	a	0	0.8
	マシンで禁止	b	0.1	0.8
	ファイルへのアクセス権なし	c	0	0.9
	ファイル操作権限なし	d	0	0.9
	FWで制御	e	0	0.8
	ファイルパスワードあり	f	0.5	0.9
	ファイル暗号化あり	g	0.5	0.9
不正アクセス	FWで制御	e	0.1	0.7
	PFWで制御	h	0.2	0.7
	OSパッチを当てる	i	0.1	0.5
	ログインパスワードあり	j	0.3	0.9
盗聴	ファイル暗号化する	g	0.1	0.3
	通信暗号化する	k	0.1	0.3

表２　対策の実施・未実施と利便性の大きさ

利便性	対策		実施	未実施
サーバ利用	ユーザアカウントによる制御	a	0	1
	マシンによる制御	b	0	1
ファイル利用	ユーザアカウントによる制御	a	0	1
	マシンによる制御	b	0	1
	ファイルへのアクセス権	c	0.3	1
	ファイル操作権限	d	0.4	1
	ファイルパスワード	f	0.7	1
	ファイル暗号化	g	0.5	1
マシン利用	PFW	h	0.8	1
	OSパッチ	i	0.6	1
	パスワード	j	0.9	1
ネットワーク利用	FW	e	0.7	1
	PFW	h	0.8	1
	通信暗号化	k	0.6	1

フォルトツリーを利用して，これらの値から通常時，FW の FTP ポートを開放した場合，他対策を様々な組合せで強化した場合のそれぞれについて，リスク発生確率と利便性を求める．その結果の一部を表３に示す．

表3　他対策強化とリスク発生確率・利便性

		通常	FW開放	他対策強化案(一部分)					
ユーザアカウント	a	0	0	0	0	1	0	0	0
マシン制御	b	0	0	0	0	0	0	0	0
ファイルアクセス権	c	0	0	0	0	0	1	0	0
ファイル操作権限	d	0	0	0	0	0	0	0	0
FW	e	1	0	0	0	0	0	0	0
ファイルパスワード	f	0	0	1	1	0	0	0	1
ファイル暗号化	g	0	0	0	1	0	0	1	1
PFW	h	0	0	0	0	0	0	1	1
OSパッチ	i	0	0	0	0	0	0	0	0
ログインパスワード	j	1	1	1	1	1	1	1	1
通信暗号化	k	0	0	0	0	0	0	0	0
リスク									
情報漏洩		0	0.34	0.19	0.10	0	0	0.19	0.10
不正アクセス		0.05	0.32	0.32	0.32	0.32	0.32	0.09	0.09
盗聴		0.09	0.09	0.09	0.03	0.09	0.09	0.03	0.03
利便性									
サーバ利用		1	1	1	1	0	1	1	1
ファイル利用		1	1	0.70	0.35	0	0.30	0.50	0.35
マシン利用		0.90	0.90	0.90	0.90	0.90	0.90	0.72	0.72
ネットワーク利用		0.70	1	1	1	1	1	1	1

このように，ユーザがFWのFTPポート開放を要求した際に他対策の強化によるリスク，利便性の大きさを算出できる．実際には対策組合せ数は膨大であり，すべての組合せの中から管理者とユーザが許容できるものを選択することは現実的ではない．そこで組合せ数を絞り込む必要があるが，何らかの固定的な絞り込み方法では「特別な利用ができるならば他の利便性は損なわれてもよい」「すべての利便性を均等にしてほしい」「特定の利便性を重要視する」といったユーザの状況に対応することが難しい．そのため，リスク発生確率や利便性への閾値の設定，リスクの最大値最小化，利便性の最小値最大化など絞り込む方法を選択できるようにすることで，ユーザの状況に柔軟に対応できると考えられる．

4.3　利便性とセキュリティの両立の展望

本交渉方式により，リスクの発生を抑制しつつユーザが特別なサービスを利用できるかどうかを判断することができる．また，リスク発生確率と利便性を考慮して強化すべき対策を選択できるため，利便性とセキュリティを動的に移行することでユーザのそのときの状況に必要な利便性とセキュリティを提供することができる．そのため，ネットワーク利用時におけるユーザの利便性とセキュリティの両立を実現することが可能になると考えられる．

5. まとめと今後の課題

本稿では，ネットワーク利用時における特別なサービス利用を実施するために，利便性とセキュリティを考慮して管理者とユーザが交渉を行う方式について述べた．本方式では，対策の変化によるリスク発生確率と利便性の変化を定量的に算出し，ユーザの状況に応じて強化すべき対策組合せを選択できる．また，本方式の実現により，利便性とセキュリティを動的に移行させ，ユーザが利便性とセキュリティを両立できるという展望について述べた．

今後の課題は，次の通りである．

(1) 対策実施とリスク発生確率・利便性の関係の定量化

現在，表1，2に示した対策実施とリスク発生確率・利便性の関係はリスク分析の際に決定される前提としている．しかし，リスク発生確率には様々な統計情報が必要であり，利便性の捉え方はユーザによって異なることから，これらの数値を客観的に決定することは難しい．そのため，妥当性のある数値化方法について検討が必要である．

(2) 他のユーザに影響しない特別利用の実施方法

他のユーザに影響を与えず，交渉を行ったユーザのみが特別な利用を実施できるようにするためには，ユーザごとに対策を個別制御する必要がある．しかし，個別制御は設定の手間や管理の複雑さなど様々な問題がある．また，個別制御できない対策も存在する．そのため，交渉結果の現実的な実現方法について検討する必要がある．

参考文献

[1] JIPDEC，情報セキュリティマネジメントシステム(ISMS) 適合性評価制度：http://www.isms.jipdec.jp/

[2] 打川和男："市場の失敗事例で学ぶ情報セキュリティポリシーの実践的構築手法"，オーム社，2003.4

[3] 加藤弘一，勅使河原可海："発生リスクを考慮したユーザ要求の自動交渉方式の検討"，マルチメディア・分散・協調とモバイル(DICOMO2006)シンポジウム論文集，pp.65-68，2006.7

[4] 中村逸一，兵藤敏之，曽我正和，水野忠則，西垣正勝："セキュリティ対策選定の実用的な一手法の提案とその評価"，情報処理学会論文誌，Vol.45，No.8，pp.2022-2033，2004.8

[5] Microsoft，Windows 2000 Server セキュリティ運用ガイド：第2章 - セキュリティリスクとは：http://www.microsoft.com/japan/technet/security/prodtech/windows2000/staysecure/secops02.mspx

[6] Microsoft 第3章:クライアント，サーバー，およびネットワークのための対ウイルス防御：http://www.microsoft.com/japan/technet/security/topics/serversecurity/avdind_3.mspx

[7] 塩見弘，島岡淳，石山敬幸："日科技連信頼性工学シリーズ7　FMEA，FTAの活用"，日科技連，1983.9

[8] Rark G. Stewart，Robert E. Melchers 著，酒井信介監訳："技術分野におけるリスクアセスメント"，森北出版，2003.10

[9] 佐々木良一，石井真之，日高悠，矢島敬士，吉浦裕，村山優子："多重リスクコミュニケータの開発構想と試適用"，情報処理学会論文誌，Vol.46，No.8，pp.2120-2128，2005.8

[10] 佐々木良一，吉浦裕，伊藤信治："不正コピー対策の最適組合せに関する考察"，情報処理学会論文誌，Vol.43，No.8，pp.2435-2446，2002.8