情報処理学会論文誌　Vol. 49　No. 9　3209–3222 (Sep. 2008)

ネットワーク特別利用時におけるセキュリティと利便性を考慮した最適対策決定手法の提案

加　藤　弘　一[†1]　　勅使河原　可海[†1]

組織のネットワークにおいて，ユーザは通常利用できないサービスを一時的に利用したい場合があり，その際には書類などにより申請を行う．管理者は特別利用を実施した場合に発生しうるリスクを考慮して申請を許可するか判断し，できる限りリスクを抑制できるように適切な対策を追加的に施す必要がある．しかし，管理者がすべてのリスクを網羅して妥当な判断をすることは難しい．さらに，追加した対策によりユーザは利用上の新たな制約を受ける可能性もある．本論文では，多層防御の概念から適切な対策制御によりリスクを抑制できることに着目し，フォルトツリー解析を利用して管理者とユーザが交渉を行うことで特別利用のための対策を決定する手法を提案する．そして，本手法の適用実験を行い，管理者の知識・経験に基づく対策決定手法と本手法の比較・評価から，セキュリティと利便性を維持した特別利用が可能な対策組合せを決定できることを示す．

A Proposal of Selecting Optimal Countermeasures with Security and Usability in a Special Network Use

Koichi Kato[†1] and Yoshimi Teshigawara[†1]

In the network of companies or organizations, a user sometimes wants to use special services temporarily which the user cannot use usually. At that time, the user must submit an application by papers. An administrator judges whether the user's request can be allowed considering potential risks by the user's special use. Then, he should implement additional countermeasures properly to reduce risks. However, it is difficult for the administrator to judge appropriately with all risks in mind. On the other hand, the user may be forced by new restrictions because of added countermeasures. This paper proposes a method of selecting optimal countermeasures for the user's request through a negotiation by the administrator and the user, using the Fault Tree Analysis, based on the concept of Defense In Depth to reduce the probability of risks with effective countermeasure control. Under the experimental deployment to a network example, we evaluate our method by comparing it with an experience-based countermeasures selecting method, and it is confirmed that our method can decide optimal countermeasures for a special network use in keeping security and usability level high.

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．それにともない，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，ユーザが自由にサービスを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，両立させることが重要となる[1)]．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することは非常に困難である．さらに，要求さ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いまだに確立されていない．

本研究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，特に本論文ではセキュリティに対する要求が厳しい環境として組織のネットワークに焦点を当て，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し，3 章で先行研究との差異を述べる．続いて，4 章で資産・脅威・対策の関係と多層防御の概念を利用したセキュリティを維持するための方針を述べ，5 章でフォルトツリー解析を利用したリスクと利便性の定量化，および最適な対策を決定するための交渉方法について述べる．そして，6 章で本手法の適用実験を行い，7 章で評価する．最後に，8 章で今後の課題を述べ，9 章でまとめる．

†1 創価大学大学院工学研究科
Graduate School of Engineering, Soka University

© 2008 Information Processing Society of Japan

2. ネットワーク利用の現状と課題

2.1 ISMS の構築と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[2]．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，組織において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の確保もまた重要である[3]．

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・管理方針や具体的な実施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，許可された範囲内でのみ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 特別利用によるセキュリティレベルの低下と申請に対する審査の困難さ

セキュリティポリシーには，通常時に従うべき事項に加え，例外措置が規定されていることが多い．ユーザは本来，前者に従ってネットワークを利用しなければならないが，実際には企業における業務遂行のため，また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がある．一般に，ユーザが特別利用を望む場合には，管理者へ書類などにより申請を行い，管理者が審査して申請内容の実施可否を決定する．なお，本論文で扱う特別利用とは，例外措置としてのセキュリティポリシーの許容範囲内での利用を意味する．

ところが，この特別利用のために何らかの対策を取り除いた場合，従来維持されていたセキュリティが損なわれる可能性がある．そのため，この審査では申請内容の実施時にセキュリティ上の問題が起きないかどうかが重要な観点であり，適切な判断をするためには管理者にネットワークやセキュリティに関する多くの知識や経験が要求される．さらに，セキュリティへの影響を把握して適切な対策を選択することは容易ではなく，審査結果の妥当性の客観的な証明は困難である．

2.3 安全な特別利用と交渉による対策決定手法

2.2 節で述べた特別利用を安全に実施するためには，特別利用のために対策を変更してもセキュリティを維持できる仕組みが必要である（要求 a）．また，審査上の問題に対し，セキュリティへの影響の程度を定量化し，発生しうる問題を網羅して申請内容の実施可否を判断する仕組みが必要である（要求 b）．さらに，ネットワーク利用時のセキュリティと利便性を両立させるためには，特別利用を行うその時点において管理者とユーザの望むセキュリティと利便性を確保できる柔軟性が必要である（要求 c）．

本研究では，要求 a を満たすため，1 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を採用する．つまり，現在実施している対策を特別利用のために弱化させる代わりに，他の対策を強化することでリスクを抑制する．ただし，他対策の強化によりユーザのネットワーク利用に関して新たな利便性低下が発生しうることに注意する．

一方，要求 b に対しては，リスクが顕在化する確率（以下，事故発生確率と呼ぶ）をセキュリティへの影響度ととらえてフォルトツリー解析（FTA: Fault Tree Analysis）を用いて定量化する．また，要求 a へのアプローチで述べた利便性低下が問題となりうるため，利便性も FTA を用いて定量化する．そして，管理者とユーザの間で，特別利用や対策制御にともない変化する事故発生確率と利便性を基に交渉を行い，両者の満足する対策を模索する．この交渉により対策が見いだせれば特別利用の実施を可決し，見いだせなければ否決する．

さらに要求 c について，リスクには端末への不正アクセス，外部への機密情報の漏洩など様々なものがあり，一時的であれば許容されるリスクがある場合や，特別利用を許可する代わりにリスクへの許容度が厳しくなる場合がある．同様に，利便性にもホームページ閲覧，メール送受信など様々な観点での利便性が考えられ，特別利用ができれば他の利便性が低下してもよい場合や，業務遂行のために利便性を低下させることができないサービスが存在する場合がある．つまり，管理者やユーザが各事故発生確率や各利便性に対して求める度合いは状況に応じて異なる．この状況の違いに対応するためには，要求 b で述べたリスクの網羅だけでなく，影響を受ける利便性を網羅して対策を決定する必要がある．さらに，管理者とユーザのそのときの状況に応じた意思を正確に反映させるためには，対策変更によって影響を受けるリスクや利便性を認識して対策を選択できなければならない．一方で，管理者やユーザがすべてのリスクと利便性を何度も見直しながら対策を選択することは容易ではない．そこで要求 c に対しては，要求 b へのアプローチの中で，事故発生確率はリスクごとに，利便性はサービスごとに細分化して値を求め，最適対策組合せを導出する．これにより，影響を受けるリスクや利便性を認識でき，各値を比較しながらそのときの状況における最適な対策を効率良く選択できる．

なお，リスクは資産価値，影響度，発生確率などを考慮した「リスク値」として考えるこ

© 2008 Information Processing Society of Japan

とが一般的だが，本論文では特別利用をする際にリスクが顕在化しやすくなること自体が問題であると考え，事故発生確率を基準としている．また，すでにリスク分析，リスクアセスメント，リスク対応は実施されていることを前提とし，各対策におけるリスク抑制の効果や利便性への影響度は定量化できるものとする．

3. 関 連 研 究

2.3 節の要求 b，c へのアプローチは対策を選定する問題に相当し，中村ら，佐々木らによる研究がなされている[4),5)]．中村らは，資産・脅威・対策の関係をモデル化し，セキュリティ対策選定問題を離散最適化問題として定式化している．この手法ではセキュリティ面から適切な対策を決定可能であるが，利便性については考慮しておらず，ユーザの意見を反映させることが困難である．

佐々木らは，リスクに関係する関与者間でリスク，対策コスト，利便性などを考慮して対策組合せに関する合意形成を行う多重リスクコミュニケータについて研究している．この中では，本論文と同様に FTA を利用したリスクの定量化，および複数人による対策決定を行っており，関与者が皆納得のいく対策を決定することができる．また，利便性についても各対策に割り当てた値を合算したものとして定量化し，対策決定の一要素として扱っている．しかし，ひとまとめにした値では具体的に利便性が低下するサービスをユーザが認識できず，この認識のためにはユーザが各対策を確認しながら影響を受けるサービスを判断しなければならない．さらに，見落としなどの可能性を考慮すると，ユーザは必ずしも利便性を網羅した判断ができるとは限らない．そのため，2.3 節の要求 c で述べた，状況により変化するユーザの利便性への要望に柔軟に対応することは難しい．

さらに，中村ら，佐々木らの両者が組織のシステムや特定の問題に対する「対策導入」時点についての取組みであるのに対し，本論文は対策が導入されたシステム利用時の特別利用という「運用」時点についての取組みであり，セキュリティと利便性の維持という運用時点に独特の問題を扱っている．

これに対し，榊らは，リスク，利便性，コストを考慮した，システム運用時における状況に応じた対策立案方式を提案している[6)]．この方式では，資産価値や対策間の関係を考慮して対策変更にともなうリスク値，利便性低下度，コストを算出し，本論文と同様に運用時における対策見直しが可能である．また，リスクを脅威別に分析しているため，セキュリティの観点からは 2.3 節の要求 c に対応できていると考えられる．しかし，佐々木らと同様に利便性は総合値で扱っており，対策変更によって利便性に影響を受けるサービスを認識して対策を選択することができず，状況に応じてユーザの望む利便性を正確に反映することは難しい．

以上から，運用時点における対策見直しの際に 2.3 節の要求 a，b，c をすべて満たす手法は存在していない．我々の手法では，これらの既存研究で取り組まれてきたリスクに対する詳細な分析と定量化に加え，利便性もネットワークで利用するサービスごとに詳細に分析して定量化する．これにより，要求 a，b，c をすべて満たし，その時点における管理者とユーザのリスクや利便性に対する要望を反映させて，特別利用のための最適な対策を決定することが可能となる．

4. 対策制御によるセキュリティの維持

セキュリティを維持した特別利用のためには，対策を適切に制御する必要があり，そのためにはリスクと対策の関係を明確にしなければならない．そこで，資産・脅威・対策の関係および多層防御の概念について述べる．

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．そのため，資産・脅威・対策の関係は**図 1** のように表現できる[4)]．なお，リスク分析における「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．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，脆弱性と結び付かない脅威は脅威ではないとの考えから，図 1 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．

一方，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と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[7),8)]．たとえば，ネットワークにファイアウォール（FW: Firewall）を設置し，端末にパーソナルファイアウォール（PFW: Personal Firewall）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

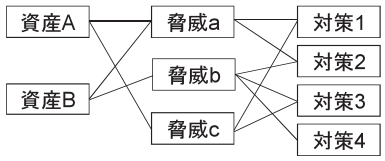

図 1　資産・脅威・対策の関係
Fig. 1　Relation among assets, threats and countermeasures.

© 2008 Information Processing Society of Japan

らの対策の 1 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．

図 1 のようにモデル化されたリスク（資産と脅威の組）と対策の関係と多層防御の概念をあわせることで，対策の弱化による影響を他対策の強化により抑制できる．たとえば，特別利用のために対策 3 を弱化させた場合，資産 B に対する脅威 b（リスク B-b），資産 A に対する脅威 c（リスク A-c）が顕在化しやすくなる．そこで，リスク B-b に対しては対策 2，4 の 1 つ以上を，リスク A-c に対しては対策 1 をそれぞれ強化することで各リスクの顕在化を抑制する．このように，特別利用時において，適切な対策制御を行うことでセキュリティを維持することが可能となる．

5. 交渉による最適対策の決定

5.1 事故発生確率と利便性の定量化

適切な対策制御および対策制御の妥当性の証明のためには，対策の変化にともなう事故発生確率と利便性の変動を定量化する必要がある．このとき，セキュリティや利便性など達成したい事項（目標事項）が明確である場合，無数に存在する対策がどの目標事項に影響するかを分析するよりも，目標事項に必要な対策を考えるトップダウンアプローチによる分析の方が効率が良い．そこで本論文では，目標事項の達成の妨げとなる要因の分析や，各要因を抑制可能な対策の整理，必要箇所への的確な対策の決定が可能であるという特徴を持つ FTA を定量化手法として用いる[9]．

FTA による分析は，結果として起きる事象を頂上事象とし，頂上事象の発生原因を論理ゲート（AND，OR など）でつないで木を作成する．そして，頂上事象が発生する必要最小限の基本事象の組の集合（最小カットセット）を見つけ，発生確率を計算する．この結果から，どこに対策を施すべきか判断することができる．

まず事故発生確率を算出するために，リスクに関するフォルトツリー（FT: Fault Tree）を作成する．一般に，リスクは顕在化するまでにいくつかのフェーズが存在し，各フェーズが成立しないように対策をとることでリスクの顕在化を防ぐことができる．これはまさに多層防御の概念であり，4 章で述べた対策制御方法が適用可能であることを裏付けている．そこで，頂上事象に顕在化が望まれないリスクを置き，攻撃フェーズごとに分解して FT を展開していく．

一方，ユーザによるサービス利用についても，複数のフェーズを経て利用が実現する．しかし，セキュリティ対策により特定のフェーズの達成が妨げられ，十分なサービス利用ができなくなる場合がある．そこで，利便性を算出するための FT は，利用サービスを頂上事象に置き，利用フェーズごとに分解して展開していく．なお本論文での利便性は，まったく対策が影響せずいっさい支障のないサービス利用を基準に，どの程度便利に使えるかの割合を利便性として扱っている．

ここで，3 章で述べた利便性を総合値で扱う従来の方法では，対策変更により数値的には許容できたとしても，実際には達成が妨げられたフェーズを回復できずサービス利用に支障が残る場合がある．たとえばファイルサーバの利用について，ある対策強化によりファイルサーバへのアクセス自体が妨げられてしまった場合を考える．総合値を用いた場合，対策強化による利便性の低下が算出でき，他の対策の変更により利便性低下度を抑えることはできる．しかし，この「他の対策の変更」がファイル利用に対する利便性を増加するものである場合，ファイルサーバへのアクセスそのものに支障が残り，数値上は利便性低下度が抑制されるがファイルサーバの利用は不便なままという状態となり，実際のサービス利用時の利便性と数値が一致しないことになる．これに対し，本論文のようにフェーズに基づく分析では，ファイルを利用すること自体に問題がない場合に，ファイル利用を回復する対策を選択しても効果は薄く，利便性は大きな増加を見せない．つまり，妨害されたフェーズを回復する対策は他のフェーズに関係する対策に比べて利便性の値が大きく向上するため，利便性を大きく向上させる対策を比較的優先して求めることができ，実際のサービス利用に合致した効果的な対策が抽出可能となる．

これらの FT から事故発生確率と利便性を定量的に算出するために，立式を行う．FT における頂上事象の発生確率は，最小カットセットを基に求められる．カットセット c，カットセット集合 C，1 つのカットセットに含まれる基本事象 e とその集合 E_c，基本事象の発生確率 P_e，対策 i の実施の有無 $X_i \in \{0, 1\}$，対策 i を実施したときの基本事象 e に対するリスク低減効果 $\Delta P_{e,i}$ とすると，頂上事象の発生確率 P_{top} は式 (1) で表される．

$$P_{top} = 1 - \prod_{c \in C} \left\{ 1 - \prod_{e \in E_c} P_e \prod_i (1 - X_i \, \Delta P_{e,i}) \right\} \tag{1}$$

同様に，基本事象 e の利便性 U_e，対策 i を実施した場合の利便性の低下度を $\Delta U_{e,i}$ とすると，頂上事象の利便性 U_{top} は式 (2) で表される．

$$U_{top} = 1 - \prod_{c \in C} \left\{ 1 - \prod_{e \in E_c} U_e \prod_i (1 - X_i \, \Delta U_{e,i}) \right\} \tag{2}$$

式 (1)，(2) から通常のネットワーク利用時，また対策変更時の事故発生確率と利便性を求めることができ，これらの値を対策の決定に利用する．このとき，リスクやサービスごと

© 2008 Information Processing Society of Japan

に分析して定量化することで，対策変更により影響を受けるリスクやサービスが明確となり，対策を選択する際に管理者とユーザの意思をより正確に反映することが可能となる．

5.2　対策決定手順

安全な特別利用のための対策制御は，セキュリティおよび利便性に関係し，状況の変化に対応するために管理者とユーザが関与して次の手順により決定する．

(1)　特別利用時における事故発生確率の算出

特別利用のために対策を弱化させる必要がある場合，すべての事故発生確率を算出して影響のあるリスクを確認する．もし管理者がこれらの事故発生確率を許容できれば他対策の強化は不要であり，ユーザは特別利用が可能となる．許容できない場合は次の段階へ進む．

(2)　計算による理論上の最適対策組合せの導出

手順 (1) において管理者が事故発生確率を許容できないため，他対策を強化した場合の各リスクの事故発生確率を求める．また，他対策の強化により利便性が低下する場合があるため，同時にすべてのサービスに関する利便性も算出する．この中から管理者は事故発生確率を，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，この選択は容易ではない．さらに，事故発生確率の抑制や利便性の維持のための「適切な」対策制御といっても，何が適切なのかは状況により変化する．そこで，事故発生確率，利便性，対策に対し，その状況において必要な目的関数や制約条件を決め，最適対策組合せを導出する．

たとえば，目的関数として (a) 全事故発生確率の最大値最小化，(b) 全事故発生確率の平均値最小化，(c) 全利便性の最小値最大化などがあり，制約条件として (i) 特定の対策は決められた実施方法しか許可しない，(ii) 特定のリスクは事故発生確率を一定値以下にするなどがあげられる．これらは，P_{top} の集合を P，U_{top} の集合を U としたとき，次のようになる．

目的関数として

(a) minimize　$\max(P)$

(b) minimize　$\mathrm{average}(P)$

(c) maximize　$\min(U)$

制約条件として

(i) 特定の対策 i について $X_i = Z$（Z は一定）

(ii) 特定のリスクについて $P_{top} \leqq P_M$（P_M は一定）

このように，その環境に応じた目的関数，制約条件のもと，X_i を変数とした対策組合せの離散最適化問題を解き，管理者とユーザにとっての理論上の最適対策組合せを決定する．

(3)　交渉による状況に応じた最適対策組合せの決定

手順 (2) により求められた対策組合せは事故発生確率や利便性の数値の点では最適といえても，実際には状況に応じて管理者やユーザが求めるセキュリティや利便性は変化するため，必ずしも最適とは限らない．そこで，管理者とユーザの意思を反映できるよう，計算上の最適対策組合せをそのまま許容できるのか，許容できない場合にはどの対策の変更を必要とするかなどについて管理者とユーザが意見を交換し，この交渉を通して両者が許容できる対策組合せを決定する．この対策組合せが，管理者およびユーザのそのときの状況において最適な対策組合せである．最終的に両者の納得できる対策組合せを見いだせれば特別利用が許可される．もし対策組合せが決定しなかった場合には，交渉不成立となり，特別利用は許可できないことになる．

6.　本手法の適用実験

本章では，特別利用のための一般的な審査時に行われる管理者の知識・経験に基づく対策決定手法との比較を通して，本手法が 2.3 節の要求 a，b，c を満たし，管理者とユーザのリスクや利便性に関する要望をより正確に反映した対策決定が可能であるかを検証する．同時に，本手法では事故発生確率と利便性を細分化して算出するため，対策決定のために考慮すべき事項が増加すると考えられることから，本手法が対策決定にどの程度の時間や労力を要するかも検証する．

この検証のため，簡単なネットワークをモデルとして，管理者とユーザが両手法により対策組合せを決定する実験を行った．本章では実験の環境，方法，結果について述べる．

6.1　前提環境の準備

本論文では 2.3 節で述べた環境を前提としているが，実際のリスク分析結果や対策のリスク抑制効果などは組織のセキュリティ情報であるため入手することが困難である．そこで，まず前提とする環境を揃えるため，簡易的にリスク分析を行い，対策とその効果を整理し，実施する対策を決定する．その際，実運用されているネットワークでは資産・脅威・対策数が膨大になるため，**図 2** のような簡単なネットワークを想定する．ファイルサーバは業務に必要なデータを保持しており，機密性の高いデータも多く存在する．ユーザはユーザ端末を使用して Web 閲覧やメール送受信，ファイル操作などの一般業務を行う．また，DMZ には外部に公開された Web サーバ，メールサーバが設置されている．

まず，ハードウェア，ソフトウェア，デジタルデータなどの資産と，資産に関係する脅威を洗い出す．そして，各リスク（資産と脅威の組）に対して攻撃フェーズを明確にし，FT

© 2008 Information Processing Society of Japan

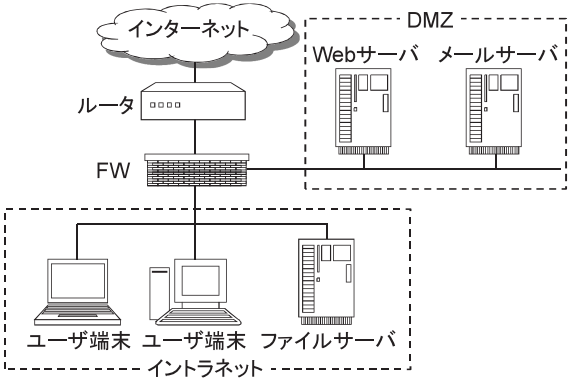

図 2　想定ネットワーク
Fig. 2　Assumed network.

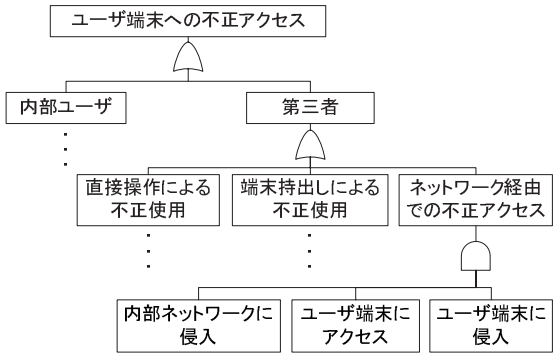

図 3　ユーザ端末への不正アクセスのフォルトツリー
Fig. 3　Fault tree for unauthorized access to a user's PC.

を作成する．たとえば**図 3** の「ユーザ端末への不正アクセス」というリスクについて，第三者がネットワーク経由でユーザ端末に不正アクセスする場合の攻撃フェーズは，(1) 攻撃者が内部ネットワークに侵入し，(2) ユーザ端末にアクセスし，(3) ユーザ端末に侵入するという流れである．

次に，作成した FT の各基本事象に対し，対策を列挙する．ここで，実際にとりうる対策は多種多様であり，すべてを網羅することは困難であるので，リスクの分類や技術・運用上の対策がまとめられた国際標準 ISO/IEC TR 13335 [10] を基に約 100 個の対策を決定した．前述のリスクへの対策は，各攻撃フェーズと対応して，(1) FW による内部ネットワークへのアクセス制限，(2) ユーザ端末上の PFW による端末へのアクセス制限，(3) ログイン時のユーザ認証や OS 更新ファイルの適用などがあげられる（**表 1**）．

表 1　リスクと対策の分析
Table 1　Analysis of risks and countermeasures.

資産	脅威	基本事象	発生確率	対策	低減効果	実施
ユーザ端末	第三者のネットワーク経由での不正アクセス	内部ネットワークに侵入	0.7	FW：FTP（外→内）の禁止	0.3	1
				FW：WEB（外→内）の禁止	0.3	1
				FW：SMTP（外→内）の禁止	0.3	1
				FW：POP（外→内）の禁止	0.3	1
				FW：その他（外→内）の禁止	0.9	1
				外部からのアクセス認証	0.9	0
				ネットワークアクセスログの取得	0.3	1
		ユーザ端末にアクセス	0.7	ユーザ端末　PFW：inbound制限	0.7	0
				ユーザ端末　アクセスログ取得	0.1	0
				内部ネットワークログの取得	0.3	0
		ユーザ端末に侵入	0.4	ユーザ端末　ログイン時の認証	0.9	1
				ユーザ端末　ログイン失敗時のアカウントロック	0.7	0
				ユーザ端末　アクセスログ取得	0.1	0
				ユーザ端末　OS，アプリケーションのパッチ適用	0.9	1
				ユーザ端末　ウィルス対策ソフト	0.7	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮

一方，利便性についても同様に，ネットワークで利用するサービスを洗い出し，利用フェーズに基づいて利便性の FT を作成する．そして，各基本事象に影響する対策を整理する．たとえば，**図 4** の「ファイルサーバの利用」を行う際には，(1) ファイルサーバにアクセスし，(2) ファイルサーバにログインし，(3) ファイルにアクセスし，(4) ファイルを使用するという流れが存在し，各フェーズに影響する対策は**表 2** のようになる．なお，図 4 は実際の利用時の動作を各事象の表現としてそのまま使用できるよう，望ましい事象を頂上事象とした信頼性を表す木として構成されており，厳密には FT ではない．しかし，頂上事象が成立する要因の分析，成立確率の定量的評価が可能という性質は同じであり，計算も同様に行えるため，便宜上 FT と表記している．各事象の意味の反転，AND と OR の論理ゲートの反転により，FT への変換が可能である．

さらに，基本事象の発生確率，各対策のリスク低減効果と利便性低下度を割り当てる．各

© 2008 Information Processing Society of Japan

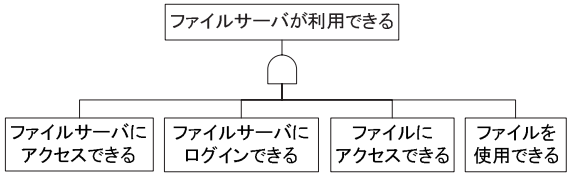

図 4　ファイルサーバ利用のフォルトツリー
Fig. 4　Fault tree for the use of a file server.

表 2　利便性と対策の分析
Table 2　Analysis of usability and countermeasures.

利用内容	基本事象	利便性	影響する対策	低下度	実施
ファイルサーバの利用	ファイルサーバにアクセス	1	ユーザ端末　ファイル共有の禁止	0.9	0
			ユーザ端末　PFW:inbound制限	0.9	0
	ファイルサーバにログイン	1	ファイルサーバ　ログイン時の認証	0.1	1
			ファイルサーバ　ログイン失敗時のアカウントロック	0.1	1
	ファイルにアクセス	1	ファイルサーバ　アカウントのグループ	0.1	1
			ファイルサーバ　ファイルアクセス権限	0.1	1
			ファイルサーバ　ファイル暗号化	0.3	0
			ファイルサーバ　ファイルパスワード	0.3	0
			ファイルサーバ　不要ファイルの削除	0.1	1
	ファイル使用	1	ファイルサーバ　ファイルアクセス権限	0.1	1
			ファイルサーバ　ファイル暗号化	0.5	0
			ファイルサーバ　ファイルパスワード	0.3	0
			ユーザ端末　ウィルス対策ソフト	0.1	1
⋮	⋮	⋮	⋮	⋮	⋮

基本事象の発生確率についてはISMSユーザーズガイド[11]を参考に3段階（0.1，0.4，0.7），対策効果については5段階（0.1，0.3，0.5，0.7，0.9）とした．一方，利便性については基本事象の利便性を基準値1とし，利便性低下度は5段階（0.1，0.3，0.5，0.7，0.9）とした．そして，対策の未実施を0，実施を1とし，各対策を通常時に実施するかどうかを決定した．表1，2は分析結果の一部であり，それぞれ図3，4と対応している．

なお，ユーザ端末のIPアドレスとポート番号を対応づけてFWを設定できるなど，対策変更は交渉を行うユーザのみに影響し，他のユーザや機器には影響を与えないことを前提とする．

6.2　実験概要

6.1節の前提環境下で，従来手法（管理者の知識・経験に基づく対策決定手法）と本手法でそれぞれ実験を行う．実験は本研究室でリスクマネジメント関係の研究に携わる修士の学生2名がそれぞれ管理者とユーザの役割を担当して実施した．

本実験で扱う特別利用は，「通常時には使用できないポートを利用した通信」，「通常時には使用できないリムーバブルメディアの使用」の2つである．特定ポートを使用するためには，弊害となっているFWのポートを開放する必要がある．一方，リムーバブルメディアを使用するためには，リムーバブルメディアの使用を制限する機能の一時的な無効化が必要である．

なお，管理者とユーザによる想定環境の理解，ユーザから管理者への要求の提示，要求実施のために弱化すべき対策の確認は事前に済ませておき，特別利用のために強化すべき対策を決定する過程のみを比較する．また，実験は対象の特別利用ごとに従来手法，本手法の順で行う．両手法の実験手順は次のとおりである．

従来手法の実験手順

(1)　特別利用のために対策を弱化させた場合にセキュリティ上の問題が発生しないかどうかを，知識・経験に基づき検討する．

(2)　セキュリティ上の問題があると判断した場合，対策リストの中から強化すべき対策を知識・経験に基づき選択する．この対策リストは，とりうるすべての対策が記載されており，現在その対策が実施済みか未実施かも明記してある．

(3)　(2)で選択した対策組合せを管理者からユーザに提示し，ユーザは許容できるか判断する．

(4)　管理者とユーザがその対策組合せを許容できれば交渉が成立する．許容できない場合は，(2)へ戻り管理者が対策を再検討し，両者が納得できる対策組合せが発見できるまで繰り返す．ただし，両者が許容できる対策組合せを見いだせなければ，交渉不成立となる．

本手法の実験手順

(1)　特別利用のために対策を弱化させた場合における，すべてのリスクの事故発生確率を求める．

(2)　事故発生確率が閾値（後述）を超えたリスクがある場合，すべての事故発生確率が閾値以下になるような，理論上の最適対策組合せを導き出す．また，管理者は必要に応じて対策を追加・変更する．

© 2008 Information Processing Society of Japan

(3)　(2) で導出した対策組合せと，通常時と対策実施時の各利便性の値を管理者からユーザに提示し，ユーザは許容できるか判断する．

(4)　管理者とユーザがその対策組合せを許容できれば交渉が成立する．許容できない場合は，(2) へ戻り条件を変更して理論上の最適対策組合せを再導出し，両者が納得できる対策組合せが発見できるまで繰り返す．ただし，すべての対策組合せで両者が許容できなければ，交渉不成立となる．

ここで，従来手法の実験手順 (3) において，3 章で述べた文献 5)，6) のような利便性の総合値を扱っていない．利便性の総合値が示されてもユーザは影響を受けるサービスを認識できず，対策を確認しながら各サービスへの影響を判断する必要がある．つまり，管理者から対策を提示された際，利便性の総合値ではユーザの各利便性に対する要望を反映した対策選択ができないため，利便性の総合値を扱わないこととした．

なお，対策組合せ数が膨大になったため，対策変更にともなう事故発生確率や利便性の算出，および計算による最適対策組合せの導出は，本実験用に開発したツールを利用した．

6.3　目的関数と制約条件の設定

6.2 節での本手法の実験手順 (2) で最適対策組合せを導出するためには，目的関数と制約条件を設定する必要がある．本実験ではセキュリティの維持と利便性の確保が可能な対策を決定できるか検証するため，金銭・労力などの対策コストは扱わないこととする．まず，特別利用時にセキュリティレベルを維持するためには，各事故発生確率を通常時の値（閾値）以下にするという条件が付く．つまり，リスク n の通常時および対策変更後の事故発生確率を $P_{\mathrm{MAX}n}$，P_n とすると，

すべてのリスクについて $P_n \leqq P_{\mathrm{MAX}n}$

を満たすことが制約条件となる．これは，5.2 節で述べた制約条件 (ii) における対象をすべてのリスクに拡張したものである．

次に，この制約条件だけでは必要以上の対策を実施する組合せも多く存在するため，本実験では通常時の事故発生確率を維持する最低限の対策を選択できればよいとして，閾値の上限に近づけることとした．本来はすべての事故発生確率を閾値の上限に近づけるような目的関数とすべきだが，計算が複雑になるため，ここでは事故発生確率が増加したリスクの中から最低限の対策でよいリスク m を決め，「従来の事故発生確率を維持する対策のうち，リスク m への対策は最低限のもの」を求める．したがって，本実験の最適化問題は，すべてのリスクの集合を N として，次のようになる．

$$\text{maximize} \quad P_m$$

$$\text{subject to} \quad P_n \leqq P_{\mathrm{MAX}n} \quad ({}^{\forall}n \in N)$$

この目的関数は 5.2 節の例と異なるが，制約条件と組み合わせることで，近似的に「従来の事故発生確率を維持する必要最低限の対策を決定する」ことになる．

表 3　従来手法と本手法による対策選択結果
Table 3　Results of selecting countermeasures by existing method and our method.

	従来手法	本手法
FWの開放のポート	ユーザ端末 アクセスログ取得 ネットワーク 外部からのアクセス認証 ユーザ端末 ファイル暗号化 ユーザ端末 バックアップ ※ 特別利用は否決された	ユーザ端末 ログイン失敗時のアカウントロック ユーザ端末 PFW：inboundの制限 ユーザ端末 アクセスログ取得 ユーザ端末 スクリーンセーバー時にロック ユーザ端末 HTMLメールの禁止
のルリ使メムー用ディバアブ	ユーザ端末 ファイルパスワード ユーザ端末 アクセスログ取得 メール本文チェック メール添付ファイルの利用禁止 Web フィルタリング	ユーザ端末 ログイン失敗時のアカウントロック ユーザ端末 ファイルパスワード ユーザ端末 メーラパスワード ユーザ端末 HTMLメールの禁止

6.4　実 験 結 果

両手法により最終的に選択された対策を**表 3** に示す．また，本節では両手法での実験の過程，管理者とユーザのコメント，対策決定に要した時間について述べる．

(1)　通常時には使用できないポートを利用した通信

（従来手法の実験過程）

まず管理者は，FW のポート開放により生じる問題を検討した．そして，管理者が追加的に必要と考えた対策は，(a) ユーザ端末でのアクセスログの取得，(b) 外部からのネットワークアクセスへの認証，(c) ユーザ端末でのファイル暗号化，(d) ユーザ端末でのデータバックアップの 4 つであった．

これに対し，ユーザは対策の追加によりどのような利用に影響があるかを検討した．その結果，一時的な利用であるのに端末内の全データをバックアップすることは労力が大きすぎると判断したため，(d) の対策を許容できなかった．そこでユーザは管理者に対し (d) を除外した別の対策組合せを求めた．

しかし，管理者は (d) の対策は必須であり，この対策を実施できないならば特別利用は許可できないと返答した．ユーザは，(d) の実施は特別利用に見合わないと結論づけ，最終的に特別利用は否決された．

© 2008 Information Processing Society of Japan

表 4　通常時，FW 開放時，対策導入時の事故発生確率と利便性
Table 4　Probability and usability at normal time, at FW port opening time and at countermeasures implemented time.

×：通常時より大きい

識別子	リスク	事故発生確率		
		通常時	要求実施時	対策導入時
R_1	ユーザ端末への不正アクセス	1.12E−1	× 1.15E−1	3.04E−2
$R_{1\text{-}1}$	内部ユーザによる不正アクセス	1.02E−1	1.02E−1	2.38E−2
$R_{1\text{-}1\text{-}1}$	直接操作による不正使用	7.21E−2	7.21E−2	2.01E−2
$R_{1\text{-}1\text{-}2}$	端末持出しによる不正使用	4.00E−3	4.00E−3	2.50E−3
$R_{1\text{-}1\text{-}3}$	ネットワーク経由の不正アクセス	2.80E−2	2.80E−2	1.24E−3
$R_{1\text{-}2}$	第三者による不正アクセス	1.13E−2	× 1.42E−2	6.78E−3
$R_{1\text{-}2\text{-}1}$	直接操作による不正使用	9.16E−4	9.16E−4	2.44E−4
$R_{1\text{-}2\text{-}2}$	端末持出しによる不正使用	1.01E−2	1.01E−2	6.35E−3
$R_{1\text{-}2\text{-}3}$	ネットワーク経由の不正アクセス	3.29E−4	× 3.29E−3	1.87E−4
R_2	ユーザ端末内のデータの漏洩	1.70E−1	× 1.70E−1	1.38E−1
$R_{2\text{-}1}$	端末利用者による漏洩	1.09E−1	× 1.10E−1	9.18E−2
$R_{2\text{-}1\text{-}1}$	直接操作による漏洩	4.76E−2	× 4.82E−2	3.98E−2
$R_{2\text{-}1\text{-}2}$	端末持出しによる漏洩	6.47E−2	6.47E−2	5.42E−2
$R_{2\text{-}2}$	内部ユーザによる漏洩	3.39E−2	× 3.40E−2	1.81E−2
$R_{2\text{-}2\text{-}1}$	直接操作による漏洩	1.92E−2	× 1.93E−2	4.39E−3
$R_{2\text{-}2\text{-}2}$	端末持出しによる漏洩	1.48E−2	1.48E−2	1.37E−2
$R_{2\text{-}2\text{-}3}$	ネットワークアクセスによる漏洩	1.75E−3	× 1.76E−4	1.04E−5
$R_{2\text{-}3}$	第三者による漏洩	3.51E−2	× 3.52E−2	3.36E−2
$R_{2\text{-}3\text{-}1}$	直接操作による漏洩	1.51E−4	× 1.53E−4	3.35E−5
$R_{2\text{-}3\text{-}2}$	端末持出しによる漏洩	3.50E−2	3.50E−2	3.36E−2
$R_{2\text{-}3\text{-}3}$	ネットワークアクセスによる漏洩	1.47E−5	× 1.47E−4	8.13E−6
⋮	⋮	⋮	⋮	⋮

○：通常時より大きい　×：通常時未満

識別子	利用内容	利便性		
		通常時	要求実施時	対策導入時
U_1	ログイン	8.10E−1	8.10E−1	× 4.59E−1
U_2	ファイル利用	4.59E−1	4.59E−1	4.59E−1
U_3	ファイルサーバの利用	4.78E−2	4.78E−2	× 4.78E−3
U_4	Web 利用	8.10E−1	8.10E−1	8.10E−1
U_5	メール受信	5.91E−1	5.91E−1	× 4.13E−1
U_6	メール送信	5.91E−1	5.91E−1	× 5.31E−1
U_7	データ持出し	9.47E−1	○ 9.94E−1	○ 9.93E−1
⋮	⋮	⋮	⋮	⋮

（本手法の実験過程）

まず管理者は，ツールを用いて，FW のポート開放により事故発生確率が通常時より大きくなるリスクを調べた．**表 4** での要求実施時に×印の付いているものが，該当するリスクである．

この結果から，FW のポートを開放した場合，いくつかの事故発生確率が増加することが分かる．これらの事故発生を抑制するために，実施・未実施を義務づけた固定的な対策を除いた 30 個の対策から適切な組合せを決定する．この固定的な対策は，5.2 節の制約条件 (i) に相当する．本実験での最適化問題は，リスク R_1（表 4 参照）よりも R_2 の方が顕在化による影響が小さく，さらに R_2 の中でも行動を把握されやすい申請者が不正を行う可能性は低いと考え，最低限の対策でよい対象として $R_{2\text{-}1\text{-}1}$ を目的関数に選択し，実施，未実施を義務づけた対策の集合をそれぞれ S，T として，次のように定めた．

$$
\begin{aligned}
&\text{maximize} \quad P_{2\text{-}1\text{-}1} \\
&\text{subject to} \quad P_n \leqq P_{\mathrm{MAX}n} \quad ({}^{\forall}n \in N) \\
&\qquad\qquad\quad X_s = 1 \quad ({}^{\forall}s \in S) \\
&\qquad\qquad\quad X_t = 0 \quad ({}^{\forall}t \in T)
\end{aligned}
$$

ツールにより導出された対策組合せは (e) ログイン失敗時のロックアウト，(f) 不要ファイルの削除，(g) PFW：inbound 制限の 3 個であった．しかし，管理者が対策 (f) は不適当と判断し，(f) を除外して再計算したところ，(e)，(g)，(h) ユーザ端末でのアクセスログ取得の 3 個となった．さらに管理者は，安全のためにもう少し対策を加えたいと考え，第 2，3，8 最適解の中から (i) スクリーンセイバーロック，(j) HTML メールの禁止，(k) PFW：メール通信の制御を加え，この結果をユーザに伝えた．同時に，通常時と対策導入時の各利便性の値についてもユーザに提示した．

これに対し，ユーザは利便性の値から，メール送信，メール受信，ファイルサーバ利用の利便性が著しく低下することが分かり（いずれも通常時の約 10 分の 1．他のサービスの利便性は表 4 の対策導入時と同じ値），対策 (k) がメール送受信の通信を阻害すると判断した．ユーザは，ファイルサーバは一時的に利用できなくてもよいが，メールが使用できないと業務に支障が生じると考え，対策 (k) を除外してほしいと要望した．

管理者は，対策 (k) を除外した場合でも，表 4 のように事故発生確率が通常時以下になっていることを確認し，これを許容した．結果として，両者の納得する対策 (e)，(g)，(h)，(i)，(j) を追加することで FW の特定ポート開放が許可された．

(2)　リムーバブルメディアの使用

(1) と同様に，両手法において，管理者とユーザが意見を交換しながら対策選定を行った．影響するリスク，利便性，対策は (1) と異なるが，対策選定の過程はほぼ同じであるので詳細は省略し，決定された対策の結果のみを表 3 に示す．また本手法において，影響を受けたリスクは R_2，$R_{2\text{-}1}$，$R_{2\text{-}1\text{-}1}$，$R_{2\text{-}1\text{-}2}$，$R_{2\text{-}2}$，$R_{2\text{-}2\text{-}1}$，$R_{2\text{-}2\text{-}3}$，$R_{2\text{-}3}$，$R_{2\text{-}3\text{-}1}$ であり，第三者がリムーバブルメディアを使用して申請者の端末から情報を漏洩させることは少ないと考

© 2008 Information Processing Society of Japan

え，目的関数を次のように設定した．

maximize　$P_{2\text{-}3\text{-}1}$

なお，両手法ともに管理者とユーザの満足する対策組合せが決定でき，最終的にリムーバブルメディアの特別利用が許可された．

(3)　管理者とユーザのコメント

実験終了後に，両手法による対策決定に至る経緯や対策結果に関して管理者とユーザからコメントを得た．

まず管理者から得たコメントをまとめる．

- 従来手法では，FW 開放については外部からの不正を，リムーバブルメディア使用については申請者が不正を行うことを多く考慮した．また，不正アクセスよりもデータの漏洩をより危惧した．
- 本手法において，通常時の事故発生確率以下ならばよいという閾値の設定は問題ではないか．特別利用を許可する分，通常時よりも強く守るべきであり，ユーザはある程度の負荷，手間を許容すべきだと思う．対策選択の際に，第 2 最適解以降からも対策を選択したのはこのためである．
- 従来手法では，特別利用を許可した場合にだれが，どこから，どのような手段で不正を行う可能性があるのかなど，様々なパターンを一度に考える必要があった．また，本当にこの対策組合せでよいのかという不安から何度も検討し直すこともあった．そのため，対策選択までに非常に時間と労力を要した．本手法では，対策変更に関係するリスクが一目で分かり，必要な対策候補が自動的に提示されるため，効率良く対策を選択できた．また，従来手法では気づかなかった対策組合せが存在することが分かり，対策を選択する幅が広がった．

一方，ユーザからは次のようなコメントを得た．

- 両手法の実験で，管理者から対策を提示されたときに，特別利用のために利便性が低下してもよいサービス，使用できなくては支障があるサービス，特別利用に見合わない対策などをふまえて検討した．従来手法では，管理者から提示された対策を追加した場合に利便性が下がるだろうという感覚はあるが，どのような利用に対する利便性が低下するのか不明瞭であり，管理者に何が利用できなくなるのかをしばしば尋ねた．一方，本手法ではサービスごとに値が提示され，どの利便性が低下するか分かり，判断に役立った．ただし，数値だけでは具体的に何ができなくなるかは曖昧であり，提示された対策とあわせて判断する必要があった．
- 従来手法では管理者に再検討を依頼した際に，対策全体としての組合せを検討し直す柔軟さに欠けていたと思う．本手法では，管理者が対策を選択する際に事故発生確率という指標があり，その中で比較的柔軟に対応してくれた．

(4)　対策決定までに要した時間

従来手法では，ユーザが要求を提示してから対策が決定するまでに，1 つの申請に対して 30 分から 1 時間程度の時間を要した．一方，本手法では対策決定に至るまでに 10 分から 15 分程度の時間を要した．

7. 評価・考察

本章では，6.4 節の結果から，本手法が 2.3 節の要求 a，b，c を満たしているかどうかを評価・考察する．

7.1　特別利用時におけるセキュリティの維持

表 3 の対策を実施した場合の事故発生確率と利便性の値を**表 5**，**表 6** に示す．なお，従来手法の各値は本章の評価のために算出した値であり，実験時には管理者やユーザに提示していない．

表 3 に示された両手法の対策選択結果をそれぞれ実施した場合の事故発生確率を確認する．表 5，6 から，FW の特定ポート開放，リムーバブルメディアの特別利用のために決定された対策を実施した場合，両手法とも事故発生確率はすべて通常時以下となっていた．表 5，6 は結果の一部のみの掲載であるが，事故発生確率はすべて通常時以下であった．両手法ともに，特別利用によるセキュリティの低下を考慮して新たに追加すべき対策を決定しており，このことから多層防御の概念に基づく他対策の強化という本論文でのアプローチが，特別利用時のセキュリティ維持に効果的であるといえる．

7.2　リスクを網羅した特別利用の実施可否の判断

従来手法では，特別利用に関係するリスクの整理，必要な対策の検討，見逃しに対する不安による確認や再検討と，管理者による対策選択に多大な時間と労力が費やされた．さらに，対策案を提示されたユーザが対策の変更を要求した際，再検討にも多くの時間が必要であった．

一方，本手法においては，複数のリスクの事故発生確率を 1 度に計算して管理者に提示するため，リスクの整理が容易であった．また，ツールにより導出された対策組合せは事故発生確率の条件を満たしており，管理者がコメントした「事故発生確率の基準値」の問題を除き，対策組合せの有効性に関する不安もほとんど生じなかった．さらに，ツールによる最適

© 2008 Information Processing Society of Japan

表 5　両手法における事故発生確率と利便性（FW のポート開放）
Table 5　Probability and usability of each method at FW port opening time.

×：通常時より大きい

識別子	リスク	事故発生確率		
		通常時	従来手法	本手法
R_1	ユーザ端末への不正アクセス	1.12E−1	9.02E−2	3.04E−2
R_{1-1}	内部ユーザによる不正アクセス	1.02E−1	8.10E−2	2.38E−2
R_{1-2}	第三者による不正アクセス	1.13E−2	1.01E−2	6.78E−3
R_2	ユーザ端末内のデータの漏洩	1.70E−1	8.78E−3	1.38E−1
R_{2-1}	端末利用者による漏洩	1.09E−1	7.36E−3	9.18E−2
R_{2-2}	内部ユーザによる漏洩	3.39E−2	9.56E−4	1.81E−2
R_{2-3}	第三者による漏洩	3.51E−2	4.73E−4	3.36E−2
⋮	⋮	⋮	⋮	⋮

○：通常時より大きい　×：通常時未満

識別子	利用内容	利便性		
		通常時	従来手法	本手法
U_1	ログイン	8.10E−1	8.10E−1	× 4.59E−1
U_2	ファイル利用	4.59E−1	× 1.15E−1	4.59E−1
U_3	ファイルサーバの利用	4.78E−2	4.78E−2	× 4.78E−3
U_4	Web 利用	8.10E−1	8.10E−1	8.10E−1
U_5	メール受信	5.91E−1	5.91E−1	× 4.13E−1
U_6	メール送信	5.91E−1	5.91E−1	× 5.31E−1
U_7	データ持出し	9.47E−1	○ 9.94E−1	○ 9.93E−1
⋮	⋮	⋮	⋮	⋮

表 6　両手法における事故発生確率と利便性（リムーバブルメディアの使用）
Table 6　Probability and usability of each method when using removable media.

×：通常時より大きい

識別子	リスク	事故発生確率		
		通常時	従来手法	本手法
R_1	ユーザ端末への不正アクセス	1.12E−1	9.02E−2	8.84E−2
R_{1-1}	内部ユーザによる不正アクセス	1.02E−1	8.10E−2	8.10E−2
R_{1-2}	第三者による不正アクセス	1.13E−2	1.01E−2	8.01E−3
R_2	ユーザ端末内のデータの漏洩	1.70E−1	3.72E−2	4.56E−2
R_{2-1}	端末利用者による漏洩	1.09E−1	3.04E−2	3.76E−2
R_{2-2}	内部ユーザによる漏洩	3.39E−2	3.64E−3	5.13E−3
R_{2-3}	第三者による漏洩	3.51E−2	3.35E−3	3.22E−3
⋮	⋮	⋮	⋮	⋮

○：通常時より大きい　×：通常時未満

識別子	利用内容	利便性		
		通常時	従来手法	本手法
U_1	ログイン	8.10E−1	8.10E−1	× 6.56E−1
U_2	ファイル利用	4.59E−1	× 1.64E−1	× 1.64E−1
U_3	ファイルサーバの利用	4.78E−2	4.78E−2	4.78E−2
U_4	Web 利用	8.10E−1	× 5.10E−1	8.10E−1
U_5	メール受信	5.91E−1	× 2.03E−1	× 2.07E−1
U_6	メール送信	5.91E−1	× 2.60E−1	× 2.66E−1
U_7	データ持出し	9.47E−1	○ 1.00E+0	○ 1.00E+0
⋮	⋮	⋮	⋮	⋮

解の導出は長くても数分であり，ユーザが対策変更を要求した際には，不要な対策を除外しつつ最適解を導出し直すだけで済み，ほとんど時間を必要としなかった．

ここで，実際の管理者は本実験の被験者よりも知識や経験が豊富であるため，従来手法であっても複数のリスクを考慮して，本実験より短い時間で，不安なく対策を決定できるとも考えられる．しかし，従来手法は管理者の主観的な判断が多く含まれるため，考慮したリスクの網羅性および対策の妥当性の証明は難しい．

また，従来手法での実験による経験や慣れが本手法の実験時間や労力に与える影響について，関係するリスクの整理，最適対策組合せの導出，ユーザの意見を受けての対策の再導出はツールで行うため影響を受けない．また，導出した最適対策組合せに対する追加・変更はすべて第 2 最適解以降から選択されたことから，経験や慣れよりも自動的に最適組合せを導出した効果の方が大きい．さらに，ユーザによる対策の判断において，提示された対策組合せが両手法で大きく異なることから，経験による影響は少ないと考えられる．

したがって，7.1 節から，結果的には両手法ともにリスクを網羅した対策を決定可能であったが，本手法は事故発生確率という客観的指標によりリスクを網羅して特別利用の実施可否を判断したという妥当性を得ることができる．さらに，本手法は従来手法よりも少ない時間や労力で適切な対策を決定できる．また，本手法において通常時の事故発生確率よりも厳しい条件にすべきという管理者のコメントに対しては，目的関数や制約条件をより厳しいものに変更することで解決が可能である．

7.3　状況に応じたセキュリティと利便性の確保

(1)　管理者の望むセキュリティの実現

表 3 から，従来手法は FW のポート開放については外部からの不正への対策，リムーバブルメディアの使用についてはメール本文チェックや Web フィルタリングなど申請者の不正への対策が多く，管理者のコメントどおりの結果となっている．一方，本手法は不正ログイン防止やメーラ使用パスワードなど他のユーザが申請者の端末を悪用することへの対策が多い．この対策結果の違いは，だれを不正者として重視（軽視）したかの違いによるものと思われる．

© 2008 Information Processing Society of Japan

次に，表 5，6 から，選択した対策を実施した場合の事故発生確率について，全体的な傾向として「ユーザ端末への不正アクセス」については本手法の方が低く，一方で「ユーザ端末内のデータの漏洩」に関しては従来手法の方が低かった．従来手法では，管理者は不正アクセスよりもデータの漏洩を危惧して対策を決めたと述べている．一方で本手法では「従来の事故発生確率を維持する最低限の対策」の近似として，軽視するリスク $R_{2\text{-}1\text{-}1}$ や $R_{2\text{-}3\text{-}1}$ を目的関数に設定し，実質は「すべての事故発生確率が通常時以下となる対策のうち，申請者の直接操作（もしくは第三者の直接操作）によるユーザ端末内のデータの漏洩への対策は最低限のもの」を求めている．つまり，どのリスクに対し重点的に対策を施すかの違いが事故発生確率の差に現れたと考えられる．本実験では両手法で結果が異なってしまい，この近似では管理者が重視するリスクを適切に反映できなかった．しかし，管理者がそのときに重視するリスクというものが存在することが分かったため，本手法において重視する不正者やリスクを目的関数や制約条件に反映させることで，その状況において管理者の望むセキュリティを実現することができる．

ここで，本実験では申請者は不正行為を認識されやすく心理的に抑制されると考え，6.1 節のリスク分析の際に申請者が「不正を行おうと思う」という基本事象の発生確率を小さく見積もっていた．しかし，実験において管理者は申請者の不正を重視しており，これは特別利用によって申請者が不正を行う可能性が高くなると判断したということである．このようにリスク分析時の固定的な情報にとらわれず，状況に応じた判断ができる点では従来手法の方が優れている．これに対し，基本事象の発生確率を調整できる仕組みを追加することで，本手法でもある程度の対応は可能であると考えられる．しかし，「不正を行おうと思う」という事象はユーザの立場や不正行為の動機など定性的評価に頼る部分が多く，いずれにしても従来手法のように管理者の経験や勘に基づく判断が必要である．本実験では，この管理者の思考を補うために第 1 最適解以外からの対策の選択やユーザとのやりとりを通じた対策決定などの柔軟性を持たせたが，対策選択結果に十分に反映されていないことから，定性的な要素をより適切に反映できる仕組みが必要である．

一方で，本手法では管理者の経験だけでは気づきにくい対策組合せを導出できた，管理者が比較的柔軟に対応してくれたとのコメントから，管理者の経験と本手法による定量評価を適切に組み合わせることで，より多彩な対策組合せが選択可能になると期待される．

(2)　ユーザの望む利便性の実現

表 6 から，両手法でそれぞれ利便性の低下するサービスやその値が異なっていたが，影響を受けたサービスを特別利用時にはほとんど使用しないか，その影響が少ないため，両手法ともユーザは対策を許容した．また表 5 においても両手法で結果が異なっていた．ところが，従来手法では管理者が選択した対策のうち「ユーザ端末における定期的なバックアップ」がユーザに受け入れられず，管理者も変更を認めなかったため交渉が成立しなかったが，本手法による対策はユーザが許容したため交渉が成立している．つまり，FW の特定ポート開放に対し，本手法での 4 つのサービス（表 5 中×印）の利便性低下は許容できるが，従来手法でのファイル利用（バックアップ対策が影響）の利便性低下は許容できないということであり，複数のサービスの利便性が低下して総合的に利便性が大きく低下するよりも，特定のサービスの利便性の低下が問題となる場合があるという裏づけとなる．そのため，総合的な利便性でなくサービスごとに利便性を扱う本論文のアプローチが，そのときの状況に応じた利便性の確保に効果的であるといえる．

また対策選択の過程において，従来手法ではユーザは対策をとることで総合的には利便性が低下することを認識できるが，実際には何が利用できなくなったり不便になったりするのかがよく分からず管理者に尋ねる場面も発生しており，対策の利便性への影響の理解に問題があった．これは，利便性をひとまとめにして定量化した際に生じる問題ととらえることができる．一方，本手法では算出された利便性の値を対策案と同時にユーザに提示するため，サービスごとの利便性の低下について理解が容易であった．そのため，サービスごとに利便性を求める本手法により，実際の対策選択の際にユーザの理解を促進することができる．ただし，利便性が低下するサービスについて，具体的にどのような行為ができなくなるのかを数値から判断できないという問題が残った．

7.4　本手法の特徴

以上の評価により，本手法は 2.3 節の要求 a，b，c を満たしている．したがって，本手法は以下の事項が可能であるという特徴を持ち，特別利用のための対策決定に有効であるといえる．

(a)　多層防御の概念に基づく対策制御によるセキュリティレベルの維持
(b)　事故発生確率に基づく対策選択の妥当性の証明
(c)　対策変更による利便性への影響の明確化
(d)　状況に応じたセキュリティと利便性を確保可能な対策の決定

8.　今後の課題

8.1　資産価値や影響度，コストなどの考慮

本論文では事故発生確率をセキュリティレベルの基準としたが，資産価値やリスクの影響度などを考慮したリスク値も重要な考え方である．そのため，リスク値の本手法への導入に

© 2008 Information Processing Society of Japan

関する検討を行う必要がある．

また，実際の組織においては対策導入・実施の費用や労力も大きな要素であり，これらを考慮した対策選択が必要である．これに対しては，最適化問題における目的関数や制約条件に反映させることで，本手法において対応可能であると考えられる．

8.2　新たなリスクの出現への対応

リスク分析，リスクアセスメント，リスク対応がすでに実施され，運用されている環境を前提としているため，対策選択時に扱うリスクや対策は分析時点のものである．そのため，特別利用のために対策を変更することでリスク分析時には想定外であった新たなリスクが発生する場合がある．また，新たな攻撃手法や脆弱性はたえず出現しているため，予期せぬリスクが発生することも予想できる．現時点では本手法はこの新たなリスクの発生には対応できていない．

この新たなリスクについて，一般的な情報セキュリティ対策の実現のうえでも生じる問題であり，ISMS 構築のためには定期的な運用の見直しを実施する PDCA（Plan，Do，Check，Act）サイクル[12] の実現が必要とされている．本手法においては，脅威・脆弱性情報の自動収集などにより新たなリスクにある程度の対応が可能とも考えられるが，最終的には組織のリスクマネジメントに依存する部分が大きく，解決方法について十分に検討しなければならない．

8.3　他のユーザに対する影響の考慮

本論文では，変更される対策は申請したユーザのみに適用でき，他のユーザに影響を与えないとして検討を行った．IP アドレスとポート番号を対応付けた FW の制御，ユーザ端末での対策などはユーザ別に可能であるが，対策によっては他のユーザに影響を与えるものも存在する．複数ユーザを含めた対策制御を行うかどうかは環境や申請内容にも依存するが，他のユーザに影響を与えない範囲内での対策選択や，他のユーザへの影響度などを考慮した対策選択の方法について検討する必要がある．

9. ま と め

本論文では，ネットワーク利用時においてセキュリティと利便性を維持した特別利用を実現するために，多層防御の概念に基づく対策制御および管理者とユーザの交渉による対策決定手法について提案した．まず，多層防御に基づく適切な対策制御により，セキュリティを維持した対策変更が可能であることを示した．そして，対策の変化にともなう事故発生確率と利便性の変化を定量的に算出し，離散最適化問題を解くことで理論上の最適対策組合せを導出し，その中からユーザと管理者が交渉によりそのときの状況において最適な対策組合せを決定する手法について述べた．さらに，適用実験を行い，従来の対策決定手法との比較・評価を行った結果，本手法がセキュリティと利便性を考慮して特別利用のための対策を決定できることを確認した．

また，本手法による環境や状況に応じた適切な対策制御により，セキュリティを維持しつつユーザが自由にネットワークを利用できる可能性を見いだした．今後は 8 章で述べた課題に取り組み，利便性とセキュリティを両立可能なネットワークの実現を目指していく．

参 考 文 献

1) 総務省：何でもどこでもネットワークの実現に向けて，ユビキタスネットワーク技術の将来展望に関する調査研究会. http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/yubikitasu/index.html
2) JIPDEC：ISMS 適合性評価制度．http://www.isms.jipdec.jp/isms.html
3) 打川和男（著），ジェイエムシー（編）：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) 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).
5) 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).
6) 榊　啓，矢野尾一男，小川隆一：多目的最適化によるセキュリティ対策立案方式の提案，コンピュータセキュリティシンポジウム 2007（CSS2007）論文集，Vol.2007, No.10, pp.193–198 (2007).
7) 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
8) 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
9) 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).
10) ISO: ISO/IEC TR 13335 1-5. http://www.iso.org/iso/home.htm
11) JIPDEC：ISMS ユーザーズガイド—JIS Q 27001:2006 (ISO/IEC 27001:2005) 対応—リスクマネジメント編．http://www.isms.jipdec.jp/doc/JIP-ISMS113-20.pdf
12) JIPDEC：ISMS ユーザーズガイド—JIS Q 27001:2006 (ISO/IEC 27001:2005) 対応．http://www.isms.jipdec.jp/doc/uguide/ugall.pdf

(平成 19 年 11 月 30 日受付)
(平成 20 年 6 月 3 日採録)

© 2008 Information Processing Society of Japan

加藤　弘一（学生会員）

2005 年創価大学工学部情報システム学科卒業．2007 年同大学大学院工学研究科博士前期課程修了．現在，同大学院工学研究科博士後期課程在学中．情報セキュリティに関する研究に従事．

勅使河原可海（フェロー）

1970 年東京工業大学大学院理工学研究科制御工学専攻修了．工学博士．同年日本電気入社．コンピュータネットワーク，ネットワークアーキテクチャ，衛星データネットワーク等の開発に従事．1994〜1996 年ハワイ大学アロハシステム客員研究員，1995 年創価大学工学部教授，2003 年より工学研究科長を併任．ユビキタスコンピューティング，グループウェア，e-learning，ネットワークセキュリティ等の研究に従事．情報処理学会，オペレーションズリサーチ学会各フェロー，電子情報通信学会，経営情報学会，IEEE，ACM 各会員．

© 2008 Information Processing Society of Japan