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

2006－CSEC－34（9）
2006／7／20

環境の変化に対応した動的なリスク分析の検討

川西 英明　加藤 弘一　高橋 達明

ラミレス カセレス ギジェルモ オラシオ　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: {e06m5111, kokatou, ttakaha, guillerm, teshiga}@soka.ac.jp

あらまし

情報セキュリティマネジメントにおけるリスクは，環境の変化に伴い変化するものである．そのため，環境の変化によるリスクの変化を考慮しなければ，正確なリスク分析を行うことはできない．そこで本稿では，まず資産・脅威・脆弱性を識別するパラメータを定義する．そして，新たなリスク分析モデルを作成し，各パラメータから損害の発生の大きさと発生確率を求め，損害の大きさと発生確率からリスク評価を行う方法について検討を行う．また，時間の経過による資産価値の変化，時間帯の違いによる資産の可用性に対する影響，資産価値と脆弱性の認知度の違いによる脅威の発生確率への影響に対し，本モデルを使用した分析手法が有効であることを示す．その結果として本リスク分析手法が環境の変化に動的に対応可能であることを示す．

キーワード リスク分析，情報セキュリティ，リスクマネジメント，ISO/IEC TR 13335

A Study on Dynamic Risk Analysis Corresponding to Environmental Changes

Hideaki KAWANISHI　Koichi KATO　Tatsuaki TAKAHASHI

Guillermo Horacio RAMIREZ CACERES　Yoshimi TESHIGAWARA

Graduate School of Engineering, Soka University

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

E-mail: {e06m5111, kokatou, ttakaha, guillerm, teshiga}@soka.ac.jp

Abstract

A risk changes with an environmental change. If change of the risk by environmental change is not taken into consideration, exact risk analysis cannot be performed. In this paper, the discernment method of the size of generating damage and occurrence probability of clarified in consideration of the parameters, which identifies asset, threat, and vulnerabilities. A new risk assessment model is created based on the size and occurrence probability of damage. In addition, by using this assessment model, the change of the time in an environment is considered. Value of asset changes with progress of time, and the influence to availability of asset changes with differences in a time period. It is shown that value of asset and vulnerabilities recognition affect threat occurrence probability and the relationship between the environment change and the risk change .

Keyword Risk Analysis, Information Security, Risk Management, ISO/IEC TR 13335

1. はじめに

近年，企業において外部からの不正アクセス，予期せぬシステム障害，内部ユーザの意識低下による個人情報漏洩等，企業活動の中で様々な問題が多発している．それに伴い，組織の持つ情報資産のセキュリティを適切に維持・管理するための仕組みである情報セキュリティマネジメントを実施する企業が増加している．この情報セキュリティマネジメントに関する指標として，ISO/IEC 17799，ISO/IEC TR 13335 等の国際標準が存在し，現在ではこれらの国際標準を ISO 27000

シリーズとして体系的な規格群にするための検討・審議が行われている[1] - [3]．上記の ISO/IEC 17799 は新たに ISO/IEC 27002 の番号付与が決定されており，今後は ISO/IEC TR 13335 も ISO 27000 シリーズに移行される予定である．一方，国内においては，組織の実施する情報セキュリティマネジメントを第三者が評価・認証する情報セキュリティマネジメントシステム（ISMS）適合性評価制度が創設されており，ISMS 認証取得事業者数は年々増加している[4][5]．このように，情報セキュリティマネジメントに関する指標や制度が整備されてきており，組織において情報セキュリティマネジメントが一層重要なものとなっている．

この情報セキュリティマネジメントを実施する際に重要な工程となるのが，リスク分析である．リスク分析では，資産に対するリスクを特定し，そのリスクが資産にどの程度影響を与えるかを判断する．このリスク分析を実施することで，早急に対応しなければならないリスクとそうでないリスクが識別され，優先的・重点的に対策を実施する必要のあるリスクが明確になる．しかし，リスク分析が不十分であると，資産に過剰な対策を実施したり，強固な対策が必要であるのに十分な対策が実施されなかったりするというように，不適切な対策になってしまう可能性がある．

このリスク分析を実際に行うために，様々なリスク分析手法が存在するが，それらの多くは，組織のある時点におけるリスクを分析する定点的なものである．しかし，組織を取り巻く環境は常に変化しているものである．この環境の変化は資産・脅威・脆弱性に影響を与え，リスクの大きさにも変化を与える．そのため，リスク分析結果の中には，時間の経過とともに有効性を失い，現状にそぐわず不適切となってしまうものも存在する．その結果，現在のリスク分析手法では，リスク分析直後のセキュリティ対策の導入時には効果を発揮するが，対策の導入と並び重要である運用・改善においては対応しきれないという問題がある．

この問題に対し，環境の変化に対応するものとして，IT システムの脆弱性の変化に注目した脆弱性診断ツールが存在する[6]．しかし，本来は脆弱性だけではなく，資産や脅威も変化するものであるため，資産・脅威・脆弱性の変化に対応できることが必要である．

そこで，本研究ではこれまで，脅威の変化に注目し，企業の業務時間内，時間外での環境の変化による脅威の変化を考慮したリスク分析手法を検討してきた[7]．この手法では，資産・脅威・脆弱性の評価を個々に行いリスクを評価していた．しかし，資産・脅威・脆弱性の大きさは互いに影響し合うものであり，この点を考慮に入れなければ十分なリスク分析を行うことができないことが明らかとなった．そこで本稿では，環境の変化による資産・脅威・脆弱性の変化を考慮に入れた動的なリスク分析手法について検討を行う．具体的には，資産・脅威・脆弱性の互いの影響関係を明らかにし，この影響関係を総合的に捉えたリスク分析手法について検討する．また，より細かく資産・脅威・脆弱性を識別するため，資産・脅威・脆弱性を識別するための要素の再検討も行う．

2. 既存のリスク分析手法の概要と問題点

2.1 リスク分析とは

リスクを抑制するのか許容するのかを識別する作業がリスク分析であり，セキュリティ対策の導入・改善において，期間やコストを左右する非常に大きな要素となるものである．ISO/IEC TR 13335 では，リスク分析の際には，脅威や脆弱性はリスク因子と呼ばれ，リスクとの関係を図示すると図 1 のようになる．

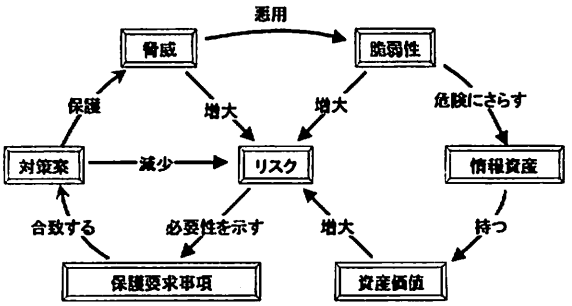

図 1　リスク因子とリスクの関係

図 1 では，資産価値，脅威，脆弱性のいずれかが増加するとリスクが増大することを示している．また，資産価値，脅威，脆弱性を識別することで，リスクに対する保護要求事項が明確になり，対応する対策案を適切に講じることにより，リスクが減少することを示している．しかし，脅威と脆弱性がそれぞれ個別に存在しているだけでは損失は発生せず，脅威が脆弱性を利用して資産に対して悪影響を与えたときに損失が発生する．また，脆弱性には様々な種類がある．このように，資産・脅威・脆弱性はそれぞれが複雑に絡み合っている．それらの関係を明らかにしていくことがリスク分析の作業になる．

2.2 リスク分析のアプローチ方法

ISO/IEC TR 13335 では，リスク分析のアプローチとして以下の 4 つの方法が示されている[2]．

1) ベースラインアプローチ

あらかじめ一定の確保すべきセキュリティレベルを設定し，実装が必要な対策を選択し，対象となるシステムに一律に対策を適用するアプローチである．リスクそのものを評価するわけではなく，ガイドライン

や業界間で出版されている規定や指示書などを参照して，未導入の管理策があれば，それを補強していくアプローチである．後述の詳細リスク分析のような資源が不要であり，対策の選択に費やす時間及び労力を低減できる．しかし，通常各資産に必要な対策レベルは異なるため，資産によっては，過度な対策もしくは不十分な対策になることがある．

2) 非形式的アプローチ

厳密に分析の手順や評価の方法が定められた構造化された手法ではなく，組織や担当者の経験や判断によってリスクを評価するアプローチである．改めて技術を習得する必要がなく，迅速にリスク分析を実施できる．しかし，構造化された手法ではないためリスクを見落とす可能性があり，分析結果も担当者の主観的なものになるため，信頼性のある分析を行うことが困難である．

3) 詳細リスク分析

対象とするシステムについて詳細なリスク分析を行うアプローチである．まず，情報資産を特定し，資産価値を評価する．そして，資産に対する脅威及び資産の脆弱性を評価することで，関連するリスクの特定及びその大きさの評価を行う．また，潜在的にビジネスを妨げるような事象に対し，その影響やそれらが発生する頻度を識別する．詳細リスク分析の問題点については 2.3 節で述べる．

4) 組み合わせアプローチ

ベースラインアプローチと詳細リスク分析を組み合わせたアプローチである．基本的には，ベースラインアプローチで分析を行い，重要またリスクが高いとされた資産にのみ詳細リスク分析を行う．ISO/IEC TR 13335 では，この組合せアプローチを推奨している．この理由として，ベースラインアプローチだけでは，他の資産よりセキュリティの高い対策が施されるべきシステムについて対応策が不十分になる可能性があること，また詳細リスク分析をすべてのシステムに適用することは効率の観点から現実的ではないことがあげられる．

2.3 既存のリスク分析の問題点

ISO/IEC TR 13335 で推奨されている組み合わせアプローチでは，初めに危険または重要な資産を特定し，事前に定めた必要なセキュリティ水準に基づき，詳細リスク分析が必要な資産とベースライン保護で十分な資産に分類する．そのため，重要な資産に対しては詳細リスク分析を行うことになる．本研究では，組織にとって重要な資産に対して適切な対策をとることが重要であると考えるため，詳細リスク分析を対象に研究を進めている．本節では，詳細リスク分析の特徴と問題点，及び本研究のアプローチについて述べる．

詳細リスク分析を行うことで，資産それぞれに必要なセキュリティレベルが特定できる．また，対策の実施後のリスクが特定できるため，現在の対策の有効性や新たな対策の必要性などが明確になる．しかし，詳細リスク分析を行う場合には，それぞれの資産に対して，存在する脆弱性と想定される脅威の洗い出しを行い，評価しなければいけないため，明確な結果を得るのに，相当な時間，労力，専門知識が必要となる．

ここで，環境の変化は資産・脅威・脆弱性に影響を与える．例えば，ウィルスの流行が発生した場合には，特定のウィルスの発生確率が高くなり，セキュリティパッチが公開されると対策としてパッチが利用できるようになるのと同時に，脆弱性の存在が広く認知されるようになる．その結果，環境が変化するとリスクも変化してしまう．つまり，リスクを正しく分析するためには，環境の変化を考慮する必要がある．しかし，環境の変化が起こるたびに詳細リスク分析を行うことは現実的とは言えない．

これに対し，本研究のリスク分析手法では，資産・脅威・脆弱性を識別するパラメータが明確になっている．そのため，環境が変化した場合には，パラメータを変化させることで環境の変化に対応可能な動的なリスク分析を行うことが可能となる．

3. 想定環境

本手法でリスク分析を行うにあたり，あらかじめ組織の所有している資産の洗い出しが行われており，資産に対する脆弱性・脅威についても洗い出しが行われているものとする．

また，詳細リスク分析では，基本的に資産・脅威・脆弱性・対策を考慮してリスク分析を行うが，本稿では対策の実施によるリスクの緩和が行われる前のリスク分析を想定しているため，対策によるリスクの緩和については対象としていない．

ISO/IEC TR 13335 は，資産の価値を評価する際に，機密性・完全性・可用性に加えて，責任追跡性，真正性及び信頼性を考慮することを推奨している．しかし，責任追跡性，真正性及び信頼性は，ISO/IEC TR 13335 においても明確な定義がされていない．そのため，資産に対しこれらを評価することは困難なため，責任追跡性，真正性及び信頼性の評価は今後の課題とする．

通常，資産は情報資産，ソフトウェア資産，物理的資産，及びサービスなど多くのものが含まれる．一般的に組織イメージなども資産に含まれるが，損害の発生による影響の特定が困難であるため，本研究では組織イメージや評判などは検討対象としない．

また，一般に資産の価値には依存関係が存在する．例えば，PC の価値は，単純に PC 購入に必要なコスト

だけでなく，その PC に保存されている情報の価値の大きさに影響を受けるといったことである．しかし，資産間の依存関係を考慮すると，後述の分析プロセスが複雑になるため，本稿ではすでに資産間の依存関係を考慮して資産の価値が識別されているものとする．

4. 本手法の分析プロセス

本手法では，まず資産・脅威・脆弱性を識別するパラメータを定義する．そして，それらのパラメータを用いて損害の発生確率，資産に対する損害の影響を評価することで，リスクの評価を行う．リスクの算出の流れは図 2 のようになる．

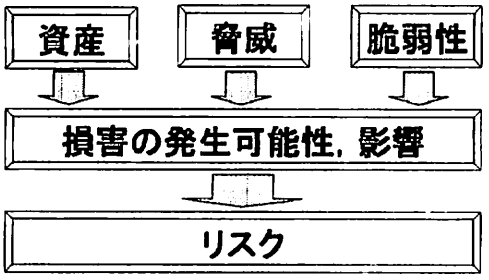

図 2 リスクの算出の流れ

4.1 リスク分析の構成要素

本研究で扱うリスク，及びリスク分析を構成するパラメータは，ISO/IEC TR 13335 に基づき定義した．「リスクは，好ましくない偶発事故の発生確率およびその影響という二つの要因の組み合わせによって特徴づけられる．」と述べられていることから，リスクを好ましくない偶発事故の発生確率及びその影響と定義した．パラメータについては，「リスクは，リスクに対する資産の価値，ビジネスへの潜在的悪影響を及ぼす脅威の発生可能性，特定された脅威による脆弱性の利用の容易さ，及びリスクを低減させる可能性のある既存又は計画中のセーフガードなどの関数である．」と述べられていることから，本研究では資産・脅威・脆弱性からリスクが顕在化する可能性や損害の種類，損害の大きさを明確にすることでリスクを特定する．第 3 章で述べたとおり，既に実施済みの対策によるリスクへの影響については，本稿では扱わないこととする．

1) 資産

組織が直接価値を認めているものであって，組織がその保護を必要としているシステム全体の構成要素又はその一部である．資産は情報資産，ソフトウェア資産，物理的資産など多くのものが含まれる．

以下に本手法で用いる資産のパラメータを示す．

a) 価値

組織の事業活動にとっての資産の重要度を表したものであり，言い換えれば，損害が発生した際の事業活動への影響の大きさである．

b) 機密性・完全性・可用性の重要性

資産において，機密性・完全性・可用性を維持することの重要性である．重要性が大きいほど，それが失われたときの影響も大きくなる．

ISO/IEC TR 13335 では資産を評価する際に，資産の価値を特定することが望ましいとされ，「その資産の入手及び保守に要する費用，及び，機密性，完全性，可用性，責任追跡性，真正性並びに信頼性の損失によるビジネスへの潜在的な悪影響に関連付けることが望ましい．」と述べている．第 3 章で述べたとおり，本稿では責任追跡性・真正性・信頼性は対象外とし，機密性・完全性・可用性の重要性を扱う．

c) 種類

情報資産やソフトウェア資産など，資産の形態の違いによる種類である．

ISO/IEC TR 13335 では，「すべての資産が洗い出されたことを確認するために，資産を情報資産，ソフトウェア資産，物理的資産，及びサービスなどのタイプ別にグループ分けすることが有用である．」と述べている．そこで，本研究では，情報資産やソフトウェア資産など，資産の形態の違いにより分類したものを資産の種類と定義する．このように資産をグループ分けすることは，資産の種類ごとに存在する固有の脅威や脆弱性の洗い出しに有効である．

2) 脅威

資産の全てもしくは一部に損害を発生させる可能性があるものであり，脅威が発生した場合は好ましくない事故や事件の原因となる．

脅威については，「偶発的及び意図的な脅威を理解し，脅威のレベル及びその振る舞いを評価しなければならない．」及び，「偶然又は計画的な脅威の原因を特定し，その発生の可能性が評価されることが望ましい．」と述べられている．そこで，本研究では原因・振る舞い・レベル・発生可能性を，脅威のパラメータとして定義する．

a) 発生原因

資産に対する損害の発生源であり，脅威が内部から発生したのか外部から発生したのか，偶発的な脅威なのか意図的な脅威なのか，人に端を発しているものなのか自然に端を発生しているものなのかを特定するパラメータである．

b) 動作

資産に対して脅威が行う攻撃方法である．例えば，成りすまし，破壊，改ざんといったようなものであり，

発生する損害の種類は動作によって異なる．

c) 強度

脅威の発生源の強さであり，脅威の発生源である人間の持っている能力や地震の強さなどによって決まる．この強度が大きいほど，資産への影響も大きくなる．

d) 発生可能性

脅威が資産に対して攻撃を行う可能性であり，ウィルスの流行の推移，攻撃ツールの登場，地震の頻発といったことにより変化する．発生可能性の大きさは，資産が損害を受ける可能性に影響を与える．

3) 脆弱性

脆弱性は，物理的なレイアウト，手続き，管理，ハードウェア，ソフトウェア，または情報における弱点である．資産に影響を与える脅威と合わさることにより資産に損害を与える．

脆弱性の識別の際は，「脅威によって利用可能性のある脆弱性を特定し，その弱点の成功しそうなレベル，すなわち利用の容易さを評価する．」とされている．また，脆弱性が一般に知られているかを表す認知度を考慮することも推奨されている．そのため，本研究では脆弱性を識別するパラメータとして，脆弱性の種類，認知度，利用の容易さを用いる．

a) 種類

資産固有の弱点やセキュリティホールのことである．

b) 利用の容易さ

脅威が脆弱性を利用する際の，脆弱性に対する攻撃の行いやすさである．

c) 認知度

脆弱性が脅威の発生源によってどの程度知られているかを表す．脆弱性の存在の公表具合などにより変化する．

4) 損害の種類

1)で述べたように，資産はその資産自体の価値，機密性・完全性・可用性の重要性という要素を持つ．一方，脅威は，脆弱性を利用することにより資産の価値に損害を発生させるが，必ずしも機密性，完全性，可用性のすべてに影響を与えるわけではない．そこで，脅威の発生により資産の価値，機密性，完全性，可用性のいずれへ影響を与えるのかを損害の種類として定義する．

5) 損害の大きさ

資産の価値と機密性・完全性・可用性の重要性に対して与える影響の大きさである．脅威ごとに動作やその強度が異なるため，資産に及ぼす損害の程度は脅威ごとに異なる．また，資産の価値も資産ごとに様々である．そのため，資産と脅威の組み合わせにより損害が発生した際の損害の大きさは異なる．

6) 損害の発生確率

脅威が脆弱性を利用して，資産に損害を与える可能性である．損害は，脅威が脆弱性を利用することにより発生するが，脅威が発生したとしても，脆弱性を利用することができなければ損害は発生しない．そのため，脅威の発生確率と脆弱性の利用の容易さの組み合わせにより，損害の発生確率は異なる．

7) リスク

資産に対する損害の影響と発生確率を組み合わせた，資産が損害を受ける危険性である．例えば，一回の損害の発生による影響は小規模でも，発生確率が高いものはリスクが高くなる．

4.2 資産・脅威・脆弱性間の影響関係

一般に，リスク分析では，資産，脅威，脆弱性を個々に評価してリスクを求めるが，これらは互いに影響し合うものであり，総合的に捉えなければ十分なリスク分析を行うことはできない．本稿では，資産・脅威・脆弱性の影響関係を明確化するために，資産・脅威・脆弱性のパラメータ間の影響関係の検討を行った．図3にパラメータ間の影響関係を示す．

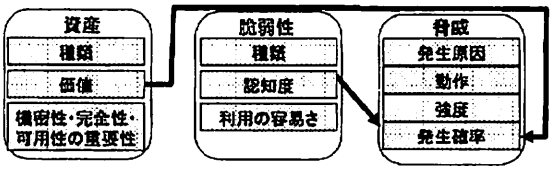

図3 パラメータ間の影響関係

1) 資産価値による影響

一般に，発生原因が人間による故意の脅威の場合には，資産の魅力により脅威の発生可能性が影響を受ける．つまり，攻撃者がPCを盗む場合には，より価値の高いPCを盗むといったように，攻撃者は攻撃を行う場合に見返りの大きな資産を狙う．そのため，脅威の発生確率に対する，資産価値の影響を考慮する必要がある．

2) 脆弱性の認知度による影響

脅威の発生原因が意図的である場合には，攻撃者は資産に対して攻撃を行うに当たり，資産の脆弱性の存在を確認しなければならない．そのため，広く一般に認知されている脆弱性は，多くの脅威から攻撃を受ける危険性を保有している．つまり，セキュリティパッチが公開された場合には，対策としてパッチが利用できるようになるのと同時に，脆弱性の存在が広く認知されるようになり，脆弱性に対して未対策の資産を狙う脅威が増加する．このことから，脅威の発生確率に対する，脆弱性の認知度の影響を考慮する必要がある．

4.3 損害の種類・大きさ・発生確率の特定

損害の種類・大きさ・発生確率は，資産・脅威・脆弱性からリスクを評価する際に特定されるものであり，資産・脅威・脆弱性を識別することにより特定することができる．本研究では，資産・脅威・脆弱性を識別する各パラメータのどのパラメータが損害の種類・大きさ・発生確率にどのように影響するのかを検討した．各パラメータと損害の種類・大きさ・発生確率の関係は図4のようになる．

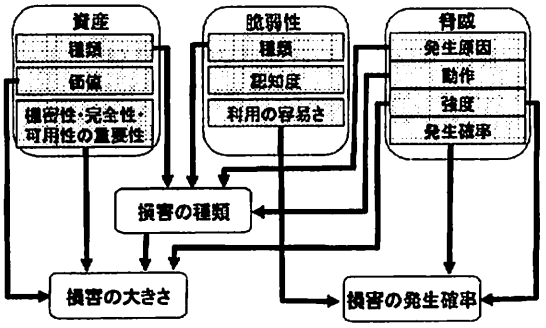

図4 各パラメータと損害の種類・大きさ・発生確率の関係

1) 損害の種類の特定

脅威が資産の脆弱性を突いて資産に損害を発生させる場合に，脅威が資産の何に損害を発生させるのかを特定する．つまり，損害の発生により，資産価値，資産の機密性，完全性，可用性のどれに影響を及ぼすかを特定する．脅威によって発生する損害の種類は，ひとつの要素のみで決まるものではなく，資産がどのようなものであるのか，どのような原因で発生した脅威がどのような方法でどの脆弱性を利用したのかによって決まる．そこで本研究では，識別された資産の種類，脅威の発生原因，脅威の動作，脆弱性の種類から，発生する損害の種類を特定する．

2) 損害の大きさの特定

特定された資産に対する損害の種類の大きさを評価する．同様の脅威であっても，資産の価値は資産ごとに異なるため，資産に対する損害の程度は異なる．また，同様の発生原因による，同様の資産に対する脅威であっても，攻撃者の持っている能力や，強度の違いにより，損害の大きさは異なる．そのため，損害の大きさを特定する際には，特定された損害の種類，資産の価値，脅威の強度を基に大きさを特定する．

3) 損害の発生確率

資産に対して脅威が発生し，脅威が資産の脆弱性を利用した時に損害は発生するものである．脅威が発生しなければ損害は発生せず，脅威が発生したとしても脆弱性を利用することができなければ損害は発生しない．また，攻撃者の能力が高い場合には脆弱性を容易に利用できるというように，脆弱性を利用して損害を発生させることができるかどうかを評価する際には，脅威の強度を考慮に入れる必要がある．本研究では，損害の発生確率を算出する際に，脅威の発生可能性，脅威の強度，脆弱性の利用の容易さを特定する．

4.4 リスク算出

資産・脅威・脆弱性の各パラメータをもとに特定された損害の大きさ・発生確率によりリスクは求まる．

4.3節で述べた，損害の大きさ・発生確率を特定する流れを考慮すると，リスク分析の全体の流れは図5のようになる．

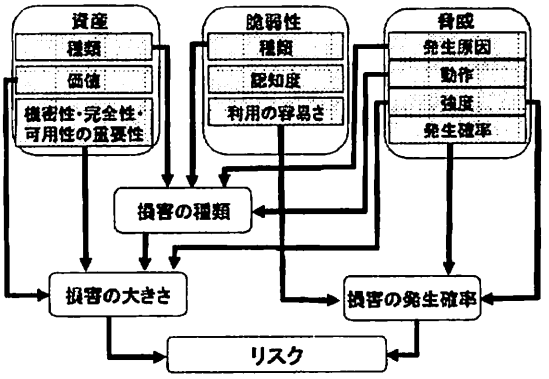

図5 リスク分析全体の流れ

5. 環境の変化によるリスク変化

本手法を用いたリスク分析では，資産・脅威・脆弱性に含まれる様々なパラメータを用いることによりリスクを分析することができる．しかし，同様の資産・脅威・脆弱性であっても環境の変化により図5の各パラメータの値が変化すると考えられるため，リスク分析の結果は環境の変化に対応できなければならない．

これに対し，本手法では，環境の変化に従って各パラメータの値を変化させることにより，環境の変化に対応したリスク分析を行うことができる．

ここで，環境の変化としては，時間・制度・人など，様々な変化が考えられるが，本稿では時間による変化について検討を行ったので，その検討結果について述べる．

5.1 時間の経過による変化

時間の変化による影響としては，時間の経過による影響と時間帯の違いによる影響とが存在する．本稿では，時間の変化及び時間帯の違いを識別できるものとする．

時間の経過によって影響を受けるものの一つとし

て，資産価値があげられる．資産の価値は時間の経過とともに変化するものである．例えば，PC は購入後，時間の経過とともに，PC 自体の消耗や，より性能の高い PC の登場などにより，価値が低下していくものである．

このように，資産の入手からの経過期間に対応して，資産価値は変化する．したがって本手法では，資産の入手からの経過期間によって資産価値を変化させることにより，時間の経過による資産価値の変化に対応することができる．その結果，資産価値の変化に対応している損害の大きさも変化するため，時間の経過によるリスクの変化に対応することができる．

5.2 時間帯の違いによる変化

時間帯の違いによるものの一つとして，資産の可用性に対する損害の大きさがあげられる．例えば，組織内のある IT システムが外部から攻撃され，システムが停止した場合を考える．業務時間内であれば，システム管理者が常駐しているので，システムが停止したことを早期に発見することが可能である．また，損害を受けてから復旧が完了するまでの時間も比較的短くて済む．しかし，業務時間外に同様の損害を受けた場合は，システム管理者が不在であるため，業務時間内と比べて，損害の発見が遅れるとともに，復旧完了までに多くの時間を要する．このように，損害の発生する時間帯の違いにより，可用性に対する損害の大きさは異なる．本手法では，発生する時間帯に応じて，可用性に対する損害の大きさを変化させることにより，時間帯の違いによる可用性への影響の変化に対応できる．その結果，可用性への影響の変化に対応している損害の大きさが変化するため，時間帯の違いによるリスクの変化に対応することができる．

6. 考察

リスク対策は，脅威の発生を抑制するものや，脆弱性を低減するもの，資産に対する損害の影響を制限するものなどがあり，対策の実施により得られる効果は対策ごとに異なる．対策による効果は，本手法の構成要素である脅威の発生確率，脆弱性の利用の容易さ，損害の種類・大きさ・発生確率と結びつけて考えることができる．そのため，本手法を用いることにより，資産・脅威・脆弱性に加えて対策によるリスクの緩和効果を考慮に入れたリスク分析が行えると考えられる．

さらに，本手法では，リスクを評価する際の資産・脅威・脆弱性の関係性が明確になっているため，どのパラメータを抑制したことによりリスクの緩和を実施したのかを明確にすることができる．

対策の実施により抑制されるパラメータが明確になることにより，対策の実施，変更，追加を行う際に，どの対策が適切であるかを判断することが容易となる．そのため，本手法は，対策済みの項目に対する重複した対策の実施などの不適切な対策を避け，適切な対策を選択するのに効果的であると考えられる．

7. まとめ

本稿では,環境の変化によりリスクは変化するため，正確なリスク分析を行うためには，環境の変化を考慮したリスク分析を行う必要があることを述べた．本手法では，資産・脅威・脆弱性を識別するパラメータを定義し，環境の変化に応じてパラメータを変化させることで，環境の変化に対応したリスク分析手法について述べた．また，リスク分析を行う際の，資産・脅威・脆弱性の関係性について述べ，資産・脅威・脆弱性は互いに影響関係にあることを示し，それにより資産・脅威・脆弱性の評価が変わることを説明した．そして，対策の実施によるリスクの低減効果を本手法のパラメータに対応させることができ，本手法を用いて対策の実施によるリスクの低減効果を考慮に入れたリスク分析を行える可能性を示した．

8. 今後の課題

8.1 評価尺度の明確化及びリスク算出方法

本稿では，資産・脅威・脆弱性の関係を明らかにし，損害の種類・大きさ・発生確率を特定することにより，リスク分析を行う手法について述べた．しかし，実際にリスク分析を行う際には，資産の価値，脆弱性の利用の容易さ，脅威の発生確率の評価を行わなければならない．そのため，資産・脅威・脆弱性の評価尺度を明確にする必要がある．また，定量的，あるいは定性的な評価方法により評価を行えたとしても，それらの評価を組み合わせて損害の大きさ，損害の発生確率，リスクを算出しなければならない．そのため，本手法を実現するためには，資産・脅威・脆弱性から損害の大きさ，発生確率，リスクを算出する方法を検討する必要がある．

8.2 時間の変化の適応方法

時間の変化について，本手法において各パラメータの値を変化させることで時間の変化に対応するための検討を行った．しかし，現段階では時間の変化及び時間帯を識別する方法が明確になっていない．そのため，時間の変化及び時間帯の違いを識別する方法を明確にする必要がある．

また，他の環境の変化についても，どのような変化があるか，またその識別方法について検討する必要がある．

8.3 対策との関係

本稿では，リスク評価を行う際に，資産・脅威・脆

弱性を考慮してリスク評価を行っている．しかし，リスク評価を行う際には，計画中・計画済みまたは既存の対策によるリスクの緩和を考慮に入れなければ，組織がさらされている現在のリスクを評価することはできない．そのため，資産・脅威・脆弱性に加え，対策を考慮に入れる必要がある．

8.4 脆弱性及び脅威数の考慮

本研究では．資産・脅威・脆弱性の組み合わせごとのリスクを分析している．しかし，一般に資産に対する脆弱性は複数存在し，特定の脆弱性を利用できる脅威も複数存在する．資産は，一つ一つの脅威・脆弱性の組み合わせによる損害の大きさは同じであっても，多くの脆弱性または多く脅威にさらされている資産の方が，リスクは高くなる．そのため，資産に対する脆弱性数，脅威数を考慮にいれたリスクの分析について検討する必要がある．

参考文献

[1] ISO/IEC 17799:2005
Information technology-Security techniques-Code of practice for information security management

[2] ISO/IEC TR 13335-1~5
Information technology-Guidelines for the management of IT Security-

[3] 情報セキュリティマネジメントに関する標準化動向：http://www.itscj.ipsj.or.jp/topics/sc27.html

[4] 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/

[5] ISMS 認証事業者数の推移：
http://www.isms.jipdec.jp/lst/ind/suii.html

[6] nCircle IP360，京セラコミュニケーションシステム株式会社：
http://www.kccs.co.jp/products/ncircle/index.html

[7] 川西英明，ラミレス・カセレス・ギジェルモ・オラシオ，勅使河原可海，"脅威の変化に対応した動的なリスク分析手法の検討"，情報処理学会第68回全国大会講演論文集第4分冊，pp.599-600，Mar.2006