博士論文

組織の情報セキュリティリスク対応を支援するモデルの提案とその適用可能性の検討

—ISO/IEC 27001:2013 及び ISO/IEC 27002:2013 適合モデルとその運用手法について—

川崎　律子
Ritsuko KAWASAKI

情報セキュリティ大学院大学
情報セキュリティ研究科
情報セキュリティ専攻

2015 年 3 月

目次

1. 序章

1.1 背景

(1) 情報セキュリティとリスクマネジメント

情報セキュリティ分野におけるリスクマネジメントは，組織が情報セキュリティを適切に確保する上で欠かせない活動として，一般に広く認識されている。それは次のような背景による。

高度に情報通信技術（以降，ICT と略）が発達している現代では，ICT は多くの社会活動やビジネス活動と深いかかわりを持っている。そして多くの組織が ICT を活用しており，ICT の無い状況はもはや想定しがたい。ICT 活用の機会が増えることは，組織における情報セキュリティリスクの増加につながる。なぜならば，「情報の機密性，完全性，及び可用性を維持すること」と定義される[1]情報セキュリティは，ICT の発達により，組織の情報がファイルサーバ，データベース，クライアント PC，モバイルデバイスなどさまざまなデバイス・場所に格納されるようになり，保護対象の増加や，保護手段の多様化及び複雑化が生じた結果，その重要性が高まっているためである。増加する情報セキュリティリスクを適切に把握，特定し，それらへ適切に対応することは，組織にとって今後ますます欠かせないものとなる。情報セキュリティリスクの特定，評価，及びそれらへの対応は，情報セキュリティリスクマネジメントにおいて実施される。

環境（外的なもの及び組織の内的なものいずれも含む）や事業の内容が異なると，想定されるリスクは一般に異なる。リスクの種類も異なることが想定されるし，また，リスクレベルの評価値も異なることが想定される。例えば，顧客の個人情報を保有し，業務においてそれを活用している組織（教育サービスの提供会社など）は，個人情報の機密性又は完全性侵害を発生するリスクに直面しており，それらのリスクレベルを高く評価し，手厚い対策をとることを心がけるであろう。これに対して，従業員以外の個人情報を保有しない組織の場合は，従業員の個人情報を保有しているため，個人情報の機密性あるいは完全性侵害を発生するリスクには直面しているが，それらのリスクレベルはあまり高く評価されないであろう。モバイルバンキングサービスを提供する組織では，そのサービスに関する機密性及び完全性を脅かすリスクを特定し，高く評価するであろうが，同時に可用性を脅かすリスクについても，特定し，高く評価するであろう。このように，情報セキュリティリスク及びそのレベルは，組織ごとに異なる。このため，組織は，情報セキュリティリスクアセスメント活動を実施することで，自分の組織が直面する情報セキュリティリスクを特定し，評価しなければならない。さらに，特定し評価した情報セキュリティリスクは，リスク対応の取り組みをとおして組織が許容できるものへと修正する必要がある。従って，情報セキュリティにおけるリスクアセスメント及びリスク対応は，情報セキュリティリスクマネジメントに含まれる主要な活動であるといえる。

さらに，現代は，ICT に限らず社会全般にわたって，著しい変化や進展の中にある。その変化や進展の速いスピードに呼応して，情報セキュリティリスクも日々変化している。インターネットやオープンなネットワーク環境を利用したビジネスは拡大しつづけており，仮想通貨やモバイルバンキングといったサービスが開始され，運用管理の効率化や高度化のために従来スタンドアローンで運用されていた制

御系のシステムがオープンネットワークと接続される，といった状況が発生している。また，そういった場で用いられる技術もオープン化が進んでいる。こうした状況は，攻撃者が攻撃する機会を増やしている。というのも、適用技術に関する情報が入手しやすかったり，攻撃対象がオープンな環境からアクセスできる場所にあったり，新たな攻撃手法を容易く発表したり，配布する環境ができつつあるからである。その結果，日々，システムのぜい弱性が暴かれたり，それらをターゲットにした攻撃手法が開発され，使用され，あるいは一般に情報提供されるということが発生している。さらに，ビジネスモデルや ICT の進展は，攻撃の機会だけではなく，内部の関係者のミスやシステムエラーといった意図しないリスク発生の機会も増加させている。すなわち，情報セキュリティの状況は日々変わっていると言える。組織は情報セキュリティに関する継続的な取り組みを行うことが必要となり，またそれらを改善していくことが重要となる。このため，組織は，刻々と変化する情報セキュリティリスクへ対応し続けなければならず，これを実現するためは，継続的改善の概念に基づいた，情報セキュリティリスクマネジメントの取り組みが必要となる。

(2) 情報セキュリティリスクマネジメントに関する国際及び国内の規格類

情報セキュリティ分野におけるリスクマネジメントの重要性及び必要性は，(1)に記した背景などにより，比較的古くから認識されてきた。そして，情報セキュリティのリスクマネジメントについて記述した，国際及び国内の規格等が多く発行されている。情報セキュリティリスクマネジメントに関する記述を有する，現在発行中の主要な国際規格としては， ISO/IEC 27001 [2]及び ISO/IEC 27005 [3]がある。

ISO/IEC 27001 [2]は，情報セキュリティマネジメントシステム（以降，ISMS と略）認証のための要求事項を示す規格である。ISMS 認証は，2012 年の調査によると，全世界で 19,577 事業者が認証を取得している [4]。また，国内においては 2014 年 11 月 27 日時点で，一般財団法人日本経済社会推進協会（以降、JIPDEC と略）を認定機関として 4,548 事業者が認証を取得している [5]。このようなことから，ISO/IEC 27001 [1]は，国内及び海外において広く普及している規格であると言える。この規格は，情報セキュリティリスクアセスメントの結果に基づいて，アクセス制御やウィルス対策といった情報セキュリティの各種対策を選択して実装することを，組織に対して要求する。広く普及している国際規格が，リスクマネジメントを情報セキュリティマネジメントの中核的活動として扱ったことも，リスクマネジメントが情報セキュリティにおいて欠かせない活動として，広く認識されることに貢献したと言える。

ISO/IEC 27005 [3]は，情報セキュリティのリスクマネジメントに関するガイドライン規格である。要求事項を示す ISO/IEC 27001 [2]では記述できない内容を，ガイドラインとして示している。また，その他関連する国際規格として，ISO/IEC 27000 [6]がある。この中では，ISO/IEC 27001 [2]や ISO/IEC 27005 [3]などの ISMS ファミリ規格で共通的に使用する用語が定義されている。それら共通用語には，リスクマネジメントに関するものが多く含まれている。なお，これら国際規格のうち，ISO/IEC 27000 [6]，ISO/IEC 27001 [2]及び ISO/IEC 27002 [7]については，翻訳され，それぞれ JIS Q 27000 [1]，JIS Q 27001 [8]及び JIS Q 27002 [9]として，日本規格としても発行されている。

また，情報セキュリティリスクマネジメントプロセスのうち，リスク対応プロセスによってリスクを修正するための，具体的対策の候補に関するガイドライン規格として，ISO/IEC 27002 [7]がある。対策の候補は, 113 個の管理策として, ISO/IEC 27001 [2]の Annex A に一覧が示されており, ISO/IEC 27002 [7]は，これら管理策の実施の手引や関連情報を提供している。ISO/IEC 27002 [7]も翻訳され JIS Q 27002 [9]として国内規格となっている。

国内の規格としては，JIS Q 13335-1 [10]がある。これは国際規格 ISO/IEC 13335-1 [11]を翻訳し，国内規格として発行したものであるが，もとの国際規格は 2010 年に廃止されている。これは，情報通信技術セキュリティマネジメント全般について記述した規格であり，その中でリスクマネジメントについても記述がある。ISO/IEC 13335-1 [11]の前身は，マルチパートの標準情報 ISO/IEC TR 13335-1 [12]～ISO/IEC TR 13335-5 [13]として 1996 年から 2001 年の期間に発行された文書群である。タイトルの Guidelines for the Management for IT Security から GMITS と呼ばれ，広く参照されていた。また，これらは翻訳され，TR X 0036-1 [14]～TR X 0036-5 [15]として国内標準情報としても発行された。現在は，ISO/IEC TR 13335 シリーズ，TR X 0036 シリーズとも廃止されているが，その内容は別規格等に引き継がれている。ISO/IEC TR 13335-1 [12]及び ISO/IEC TR 13335-2 [16]の内容は, ISO/IEC 13335-1 [11]に引き継がれて，JIS Q 13335-1 [10]として発行された。ISO/IEC TR 13335-3 [17]は，リスクアセスメント手法を記しており，この中で資産に関しては機密性，完全性，及び可用性それぞれの観点をもってリスクを特定及び評価すること，また，リスクに関しては，資産に対する脅威及びぜい弱性から特定及び評価することが記されていた。ISO/IEC TR 13335-4 [18]には，セーフガードの選択に関する内容が記されていた。セーフガードは，管理策と類似の概念であり，特定及び評価されたリスクに対してセーフガードを適用してリスクを修正する活動，すなわちリスク対応について記されていた。これら ISO/IEC TR 13335-3 [17]及び ISO/IEC TR 13335-4 [18]の内容は，情報セキュリティリスクマネジメントに関する内容として ISO/IEC 27005 [3]に引き継がれている。ISO/IEC TR 13335-5 [13]の内容は ISO/IEC 18028-1 [19]（IT ネットワークセキュリティに関するマルチパート規格のひとつであって，ネットワークセキュリティマネジメントについて規定するもの）に引き継がれている。先に述べたとおり，ISO/IEC TR 13335 シリーズ，TR X 0036 シリーズ，及び ISO/IEC 13335-1 [11]はいずれも既に廃止されており，現在では JIS Q 13335-1 [10]のみが発行されている。

国際及び国内の規格や標準情報以外にも，情報セキュリティのリスクマネジメントについて記した文書として，ISMS ユーザーズガイド [20]がある。これは，国内における ISMS 認定機関である JIPDEC が発行している文書であり，ISMS 認証基準（JIS Q 27001 [8]）の要求事項について一定の範囲でその意味するところを説明している。ISMS ユーザーズガイドの別冊として，リスクマネジメント編 [21]もある。これは，ISMS ユーザーズガイドを補足し，リスクマネジメント，特にリスクアセスメント及びリスク対応について，例を挙げて解説する文書である。これらのガイドは，いずれも前述の国際及び国内規格を参照して記述されている。

一方，リスクマネジメントの重要性は情報セキュリティ以外の分野においても認識されてきており，

2009 年には，組織が保有する全てのリスクを対象とするリスクマネジメントに関するガイドライン規格[22]が発行された。そして 2010 年には翻訳され，JIS Q 31000 [23]として国内規格としても発行された。また，リスクマネジメントの用語について規定した ISO Guide 73 [24]は 2002 年に発行された初版が，2009 年，ISO 31000 [22]の発行と併せて改訂された。また，翻訳され，JIS Q 0073 [25]として国内規格としても発行された。なお，前述の ISO/IEC 27001 [2]は，組織のリスクマネジメントを規定する際に，これら汎用的リスクマネジメントに関する規格を参照し，これに適合している。その他，汎用的リスクマネジメントを対象とする国際規格としては，IEC 31010 [26]，ISO/TR 31004 [27]も発行されており，このうち前者は JIS Q 31010 [28]として国内規格としても発行されている。

(3) 情報セキュリティリスクマネジメントの保有する課題

情報セキュリティリスクマネジメントについて規定あるいは説明する規格類や文書が多くあるにもかかわらず，情報セキュリティリスクマネジメントを組織に実装する際には，それらを参照しても解消できない課題が多く残される。それら課題のうち，代表的なものについて，課題とされている理由とともに以下に述べる。

課題 1　リスク基準（リスク評価基準）の適用において，評価実施者の主観を排除できないこと

課題のひとつめは，リスク基準の適用において，評価実施者の主観を排除できないことである。主観を排除できないということは，評価を実施する者によって，評価の結果が異なることを意味する。ISO/IEC 27001[2] には，「6.1.2 b）繰り返し実施した情報セキュリティリスクアセスメントが，一貫性及び妥当性があり，かつ比較可能な結果を生み出すことを確実にする」という要求事項があるが，これを満たさないことにもなる。一貫性及び妥当性あるリスクアセスメントを実現するためには，主観をできるだけ排除することが必要となる。

リスクマネジメントにおいて必要とされるリスク基準には，主要なものとして，「リスクアセスメントを実施するための基準」と「リスク受容基準」がある。このうち「リスクアセスメントを実施するための基準」は，リスクアセスメントを実施する者によって，結果に大きな違いが出ないようにすることを目的に設定される。これには，リスクレベルを決定するために参照する尺度となるリスク評価基準が含まれる。リスクレベルを評価する手法には，定量化手法と定性化手法がある。定量化手法とは，リスクレベルを金額等の絶対的数値で示す手法であり，定性化手法とはリスクレベルを大・中・小といった相対的尺度で評価する手法である。「リスク受容基準」は組織が受容するリスクレベルを決めるための基準であり，一般にリスク受容値を決定する。

現在，広く用いられている評価手法として，GMITS や ISMS ユーザーズガイドで示される手法がある。リスクレベルを決定する際には，次の手順をとる。まず，資産を特定し，その機密性，完全性，可用性が損なわれた場合の影響を評価する。次に，資産に対する脅威及びぜい弱性を特定し，それぞれ評価す

る。最後に，資産，脅威及びぜい弱性の評価結果からリスク値を算出する。このとき，資産，脅威及びぜい弱性の評価は，多くの場合，相対評価で 3～5 段階にレベル分けする手法をとるため，この手法は，定性的手法に分類される。相対評価によるレベル分けには，実施者の主観が含まれやすい。

次に，リスク値を金額で示す定量化手法を適用する場合を考える。この場合にも，リスク値を評価するためには，リスクの顕在化による影響やリスクの発生可能性などを評価することが必要になる。金額として定量化するためには，リスク顕在化による影響を金額で示さなければならない。この場合，影響をどの範囲と見るかによって金額は変わる。たとえば，リスクの顕在化により発生した直接的な影響だけを見る場合と，それにより派生的に発生した間接的影響（風評被害などによるビジネス機会の喪失など）も考慮する場合とでは，想定する金額は大きく異なる。また，直接的な影響だけを影響範囲とすると決めた場合でも，直接的な影響と間接的な影響を明確に区分けできない場合なども容易に想定できるため，影響に対する金額設定においては，主観を完全に排除することは難しいと言える。また，定量化するためには，リスクの発生可能性についても定量的な評価が必要となる。リスクが，システムの停止や従業員によるミス又は災害といった過去のデータに基づいて発生可能性を設定できる場合については問題ないであろう。しかし，攻撃者の意図的な攻撃によるリスクの顕在化などの場合には，発生可能性を定量化することが極めて困難である。ひとつのアプローチとして，攻撃対象の資産に大きな価値があるとか，攻撃しやすい環境にあるなど，攻撃者にとって高いモチベーションがある場合に，発生可能性を高く評価するという手法もあるとはいえ，この手法では発生可能性の評価に主観が含まれる。このように，定量化手法をとる場合であっても，リスクアセスメントにおいて評価実施者の主観を排除することは難しい。

課題 2　リスク対応の選択肢からの選択に関する手法が限定的

リスク対応とは，リスクアセスメントで特定及び評価されたリスクに対して，どのような措置をとるかを検討し，対応を決定するプロセスである。ISMS の場合を例に見てみると，ISO/IEC 27000 [6]ではリスク対応が「リスクを修正するプロセス」と定義されており，さらに定義に付された注記 1 において，リスク対応としてとるべき措置として 7 つの選択肢が示されている。従って, ISO/IEC 27001 [2]の「6.1.3 a) リスクアセスメントの結果を考慮して，適切な情報セキュリティリスク対応の選択肢を選定する」という要求事項は，前述，注記 1 の 7 つの選択肢から当該リスクに対して適切なものを選択することとみなせる。さらに，ISO/IEC 27001 [2]では，6.1.3 b)において，選定した情報セキュリティリスク対応の選択肢の実施に必要な管理策の特定も要求する。ここで，特定する管理策は，ISO/IEC 27001 [2]の Annex A 及び ISO/IEC 27002 [7]で示される 113 個の管理策と対照付けることが, ISO/IEC 27001 [2]の 6.1.3 c)で要求されているため，単純には，リスク対応を 113 個の管理策から選択することと見なすことができる。このように，リスク対応においてどのような活動を行うかについては，ISO/IEC 27001 [2]の要求事項をみても明確な記述がある。しかし，一方，特定されたリスクに対して，どの選択肢が適切であると判断し選定するか，さらに，その実現のために，どのような管理策を選択するべきかについての具体的な決定方法について記述している文書はほとんどない。一部，環境や想定するリスクが限定された場合

に限って，選択の仕方を示した文献がある程度にとどまる。（詳細は，1.3 で述べる）

リスクマネジメントを行う対象が非常に限られる場合や，想定されるリスクが限定的である場合には，上記の課題は，あまり大きな問題にはならない。なぜならば，リスク評価結果に，評価実施者の主観が含まれていたとしても，どのように判断を行ったかについて記録することで，次の見直しに向けて，主観も含めて評価結果を引き継ぐことができるためである。また，リスクの数が限られていれば，個々のリスクを詳細に検討することで，どのような対策を行えばよいかを具体的に検討することができる。従って，ここで記したような選択に関する手法が無くても，具体論に基づいて検討することで，リスク対応の選択肢や管理策の選択が容易になる。しかし，組織全体のリスクを把握して，適切なリスクマネジメントを行う場合を想定すると，リスクマネジメントを実践的活動とするためには，リスクは，ある程度大きな粒度をもって捉えざるをえない。そのような抽象度を含むレベルで，リスクアセスメントから主観を排除することや，リスク対応の選択肢や管理策の選択の具体的な方法を導くことは難しい。

本研究では，上記 2 つの課題のうち，具体的な手法の提案が少ない課題 2 に焦点をあてることにする。

1.2 本研究の目的

本研究の目的は，情報セキュリティリスクマネジメントのうち，特に情報セキュリティリスク対応を支援するモデルを提案することによって，情報セキュリティリスク対応に伴う組織における意思決定を支援することである。

リスク対応とは，リスクアセスメントの結果，特定及び評価されたリスクに対して実施し，リスク対応の選択肢，及び管理策を選択するプロセスである。また，投資対効果を考慮し，どのレベルのリスクを修正し，どのレベルのリスクは残留を受容するかについての判断も行われる。この判断は，組織のリスク受容基準と対照することで実施される。本研究では，これらリスク対応における活動を支援するモデルを提案する。

モデルの適用対象は，組織全体である。経営者が，組織の情報セキュリティにまつわるリスク全般を把握した上で，リスク対応を適用するシーンを想定し，組織の予算の制約のもと，どのリスクにどの程度の費用を配分して対策することで，どの程度の情報セキュリティレベルを達成するかに関する意思決定，すなわち，組織の情報セキュリティ対策方針の決定を支援することが目的であるためである。このことは，組織が継続的に管理できる粒度やレベルでのリスク対応の進め方を提案することを意味する。

尚，本研究においては，リスク対応の前プロセスとしてリスクアセスメントが実施され，リスクが特定・評価されていることを前提としている。すなわち，リスクアセスメントに関しては，特定や評価に関する手法を提案していない。リスクアセスメントに関しては，モデルを適用し検証するために必要なサンプルデータの作成，及び実際のデータからモデルに合うリスクアセスメント結果を作成する方法に

ついて示すのみである。

情報セキュリティリスクマネジメント及び関連する概念については，現在広く普及している ISMS に関する以下の国際規格（及び対応する国内規格）並びに関連文書を参照し，そこに記されている内容に基づくこととする。

- ISO/IEC 27000:2014 [6]（JIS Q 27000:2014 [1]）
- ISO/IEC 27001:2013 [2]（JIS Q 27001:2014 [8]）
- ISO/IEC 27002:2013 [7]（JIS Q 27002:2014 [9]）
- ISO/IEC 27005:2011 [3]
- JIPDEC ISMS ユーザーズガイド [20]
- JIPDEC ISMS ユーザーズガイド - リスクマネジメント編 [21]

ここで，これらの規格類に基づくこととしたのは，ISMS 構築において活用できるモデルを提案するためではない。これらが，規格及びそれに基づく文書という性質を持ち，組織レベルの情報セキュリティリスクマネジメントに関する記述を有し，さらに広く普及していることに着目し，これら規格類に基づく内容とすることで，モデルが一定レベルの品質を保ち，且つ多くの組織から受け入れられやすいものとなるであろうと想定してのことである。実際，ISMS 認証取得を目指す場合，ISMS 適用範囲は，組織の一部である場合も多く，そのような限られた範囲に対しては，本モデルの適用は適さない。本モデルは，目的の冒頭で記したとおり，組織におけるリスク対応に関する意思決定を支援することを目的とするものである。

なお，リスク対応の中心的な活動である情報セキュリティ対策の選択は，ISMS の場合には 113 個の管理策を選択することによって実施されるものの，組織全体を対象にリスクマネジメントを行う場合，それを実践的な取り組みとするには，113 個の管理策では詳細すぎる場合がある。詳細な対策を選択するためには，リスクの特定及び評価も同等レベルの詳細度をもって実施する必要があるからである。組織全体を対象としてリスクマネジメント行う場合に，リスクを詳細に特定すると，リスクアセスメントの実施にかかる工数は莫大になり，リスクアセスメント結果を見直し，適切に修正，維持していく，というその後の継続的活動も困難なものとなる。従って，リスクの特定や評価は，ある程度大きな粒度で実施することになる。大きな粒度で特定及び評価したリスクに対して，リスク対応で詳細な対策を適用しても，工数を費やすだけであまり意味がない。リスクと同程度の粒度の対策の適用を検討することが望ましい。この場合のリスクマネジメントの目的は，組織全体の情報セキュリティリスクの全体像を把握し，リスク対応により対策の方針を決定することにある。より詳細なリスクアセスメントやリスク対応は，全体方針のもとで，部署単位など，限定した範囲で実施すればよい。本研究では，組織全体を対象とすることから，リスク対応において選択する対策は，113 個の管理策よりも大きな粒度の対策の選択候補を用いる方が適切である。

以上のことから，本研究では，次について提案する。

- 組織全体を対象とする場合を想定した，組織の情報セキュリティリスク全般に対する対策の候補一覧を作成する方法
- 上記の各対策と各リスクとの関係を定量化する方法
- 情報セキュリティ対策に対する組織の予算という制約条件のもとで，次の機能を有するモデル
  - ・最適な情報セキュリティ対策の選択及び各対策への費用分配を支援する
  - ・達成可能なリスク受容値の決定を支援する

1.3 先行研究

先行研究をみると，リスク対応に関する手法を具体的に示した研究は限られる。また，それについて記述したものの多くは，資産を特定及び評価し，それに対する脅威などを特定及び評価するリスクアセスメントを前提とするものになっている。こうしたリスクアセスメントは，情報セキュリティ分野で従来広く使用されてきた。しかし，ISO/IEC 27001:2013 [2]におけるリスクアセスメントでは資産ベースでの実施は要求されていないことから，今後は，情報セキュリティ分野のリスクアセスメントでも資産や脅威を特定しない手法が扱われるケースが増えることが想定できる。情報セキュリティリスクマネジメントのリスク対応では，リスクに対する対策を選定することが主たる活動となるが，対策の選定の具体的な手法について提案した研究は非常に限られている。以下に，それらに関連する内容を提案する研究について示す。

(1) 資産・脅威・対策案の関係のモデル化により，対策の最適な組み合わせを求める手法の提案

資産・脅威・対策案の関係をモデル化し，対策の最適な組み合わせを論理的に求める手法の提案により，対策の選定を離散最適化問題として定式化する研究がある [29] [30] [31]。これらの研究の手法は，組織の保有する情報セキュリティリスクに対する対策の選定としては，もっとも実用的な提案になっているものの，次の課題がある。

第一に，対策を選定するためには，リスクの特定及び評価の過程において，資産及び脅威が特定され評価されていることが前提となっている点である。従来，情報セキュリティの分野では，組織が保護すべき資産，それに対する脅威及びぜい弱性を特定及び評価することにより，リスクを特定・評価する手法が一般的に行われてきた。このため， [29] [30]及び [31]のモデルは，こうした従来型の手法には適合する。確かに，ISO/IEC 27001 [2]の旧版である 2005 年版では，資産，脅威及びぜい弱性を特定及び評価することで，リスクを特定及び評価する方法が要求事項となっていた。しかし，改訂された ISO/IEC 27001:2013 [2]では，ISO 31000 [22]との整合性の観点から，資産，脅威及びぜい弱性の特定及び評価する要求事項を削除している。従って，今後は，情報セキュリティの分野においても，資産，脅威及びぜい弱性を特定・評価することなくリスクを特定・評価する手法が使われていくと想定されるため，資産

や脅威の特定を前提としなくとも，対策を選定できるモデルが必要となる。

次に，情報セキュリティ対策の候補の一覧は，抜け漏れのない対策を実現するために，ある程度の網羅性を持つものが用意される必要がある。こうした一覧を作成するためには，情報セキュリティに関する豊富な知識や経験が必要であったり，抜け漏れのないリストとするための工夫が必要である。しかし，対策候補の一覧の作成方法については，「電子商取引推進協議会（ECOM）情報セキュリティマネジメント標準（JIS X 5080:ISO/IEC 17799） [32] の解説をもとに現状考えうるものを列挙した。また，組織的な活動により実現できる対策は優先的に実施されているものとして削除した。」との記述しかなく，リストの作成方法と十分性に疑問が残る。特に， [29]及び [30]では，ノウハウが無いものについてもモデルを適用することで最適な対策の選定が行えることを提唱しているため，作成方法についての説明が不足していると考えられる。

(2) 資産・脅威・対策案の関係のモデルの，教育によるセキュリティ対策効果追加による拡張

文献 [33]及び [34]は，セキュリティ対策の効果が教育レベルによって変動することに着目することで，1.3(1)の [29] [30]及び [31]の資産・脅威・対策案の関係のモデルの拡張を提案する研究である。具体的に，文献 [33]及び [34]は教育による対策効果及びそれによるコストを追加したモデルを提案している。要員の人的なミスや認識不足により生じるリスクが一般に多いことを考えると，特に人手による運用業務が多い組織などでは，教育による対策を切り出してモデル化することに意味があると考えられる。しかし，一方，教育によりルールや運用方法を周知徹底すること，罰則の周知により悪意ある行動を抑止することなどは，情報セキュリティ対策にもともと含まれる内容である。文献 [33]及び [34]において教育による効果を別に検討できたのは，対策候補の一覧作成時に，「組織的な活動により実現できる対策は優先的に実施されているものとして削除した」とした前提を拡張前のモデルから引き続き使用しているためである。削除の根拠が「優先的に実施されている」ことであるならば，それに相当する「教育」をあらためて重要な対策としてモデルに加えることには矛盾を感じる。また，「組織的な活動により実現できる対策」には，「教育」以外のものもあると考えられ，教育以外のそうした対策はモデルから排除されることにも疑問が残る。「教育」も含めた対策全般を同一レベルで捕らえ，資産・脅威・対策案の関係のモデル化を想定するほうが望ましいように思われる。

(3) リスク顕在化に伴う賠償費用を軽減する対策を考慮する研究

文献 [35]及び [36]は，ISO/IEC 27001 Annex A の管理策で示されている，インシデント発生を抑止するための対策などの，いわゆる情報セキュリティの対策に加えて，発生した場合の損害賠償費用を軽減するための対策を想定し，個々の情報セキュリティリスクに対して，両方の対策群から損害とコストが最小になるような対策選定を行うモデルを提案している。このような 2 種の対策群を設定し，情報セキュリティリスクに加え，賠償リスクにも着目して，損害とコストを算定するこの手法は，プライバシ

一性の強い情報を扱う組織や業務についてリスクマネジメントを行う場合など，高い賠償リスクが想定される場合には有効と思われる。一方，リスクによる影響は，損害賠償費用だけには限らない。直接的な費用としては，例えば，リスク顕在化によりシステムが停止した場合のそれに伴う損害や修復や復旧に係る費用といったものが想定できる。風評被害によるビジネス機会の喪失に伴う逸失利益といったものを間接費用として想定する場合もある。賠償リスクは，情報セキュリティリスクの顕在化に伴い発生するリスクであるから損害賠償費用は，風評被害による逸失利益と同様に，間接的費用とみなすことができる。従って，汎用的な手法の検討においては，情報セキュリティリスクに加えて，賠償リスクについても考慮するのであれば，風評被害リスクのような，その他の 2 次的リスクについても検討するべきである。

(4) 限定範囲に対する詳細な脅威分析に基づき対策を選定する手法

脅威に対する必要最低限の対策候補を導出し，さらに必要コストを最小化する最適対策目標を析出する手法を提案しているのが文献 [37]である。各脅威の因果関係を示す Fault Tree の作成とミニマルパスセット探索アルゴリズムの適用により，脅威対抗に必要最小な対策目標候補集合群を導出する方法を提案している。さらに，文献 [38]は不正コピーにリスクを限定し，文献 [37]の手法を拡張しつつ適用したものである。文献 [39]は Fault Tree による解析を Fault Tree のサイズを縮小することで実践的なものとすることを提案している。

文献 [39]で, Fault Tree のサイズの縮小化が提案されてはいるものの, 組織を対象とした脅威の Fault Tree 作成は，いまだ非常に複雑になることが想定される。例えば，文献 [37]では，まず脅威として「端末利用によるユーザデータへの不正アクセス」「端末利用による暗号鍵への不正アクセス」といったレベルのものが一覧として示されることを前提としている。さらに，これらの脅威を基本事象に分解し，脅威毎に Fault Tree を作成する。そして，各 Fault Tree の頂上事象として設定されている各脅威の発生を抑止するのに必要十分な対策すべき基本事象の組み合わせをミニマルパスセットとして導出する。対策は，このミニマルパスセットに含まれる基本事象を修正するためのものである。すなわち，ここで想定される対策も具体的なレベルのものである。さらに [37] [38] [39]のいずれの文献においても，情報セキュリティ対策のリストに相当するものは示されていない。

このように具体論で検討する手法は, 組織に適用する場合には, 実用性の観点で問題があると言える。Fault Tree の分析は，主に範囲の限定される製品やサービスに適していると考えられる。

2　モデルの提案

2.1 モデルの目的と概要

(1) モデルの目的

本研究で提案するモデル（以降，本モデルと略）は，組織における情報セキュリティリスクマネジメントの中のリスク対応プロセスを支援することを目的としている。ここで，リスク対応とは，前プロセスであるリスクアセスメントにおいて，特定，分析及び評価された情報セキュリティリスクに対して，組織として受容するリスクのレベルを定め，受容できないリスクに対しては各種の対策を適用することで，リスクを受容できるレベルに変更する一連の活動を指すこととする。

特定された情報セキュリティリスクに対して，組織が潤沢に費用をあてて対策を取ることができる場合には，情報セキュリティ対策の選択はあまり重要な意味をもたない。しかし，一般に，組織が情報セキュリティ対策に充てられる費用には上限があり，組織は限られた予算の中でできるだけ効果をあげたいと考えている。この場合には，情報セキュリティ対策をいかに選択するかが，重要な問題になってくる。本モデルは，特定されたリスク及びそれらのリスク値に対して，組織のリスク受容値を定めると，それを満たす最適な情報セキュリティ対策の選択のひとつを解として示す。また，組織の予算の中で最大効果を見込めるリスク受容値を見つけたり，逆に，組織が達成したいリスク受容値に対してどの程度の予算が必要となるかを知る，といった追加的な使い方も提供する。このように，本モデルは，組織が経験や勘によらずに最適な情報セキュリティ対策の選択を行ったり，組織の予算やリスク受容値を決定したりすることを支援する。

また，最適な情報セキュリティ対策の選択を実現するためには，選択元となる情報セキュリティ対策のリストの品質が重要となる。例えば，想定できる対策は漏れなくリストに含まれている必要がある。仮にリストに抜け漏れがあれば，それは選択結果にも抜け漏れを生じされる場合があるため，選択結果が最適であるとは言い切れなくなってしまう。このため，本モデルでは，想定される情報セキュリティの対策をある程度のレベルで包括的に含むリストについて提案することも目的の一つとした。なお，日々変化する情報セキュリティ環境において，完全に包括的なリストの作成は現実的ではないため，ここでは「ある程度の」という表現を用いている。

(2) モデルの概要

本モデルは，次の要素からなる。

a) 情報セキュリティリスクのリスト，及び各リスクレベルの評価値
b) 情報セキュリティ対策のリスト，及び各対策を実施するために必要な費用
c) 各情報セキュリティ対策の各情報セキュリティリスクに対する影響値
d) リスク受容値，及び
e) 情報セキュリティ対策に対する組織の予算（費用の上限）

a)は,組織において想定される情報セキュリティリスクの包括的なリストである。また,本モデルでは,各リスクレベルを数値化した評価値も必要となる。これらは，一般にリスク対応の前プロセスであるリスクアセスメントプロセスのアウトプットとして想定されるものである。本モデルでは，情報セキュリティリスクセスメントの実施を前提とするため，これらのアウトプットは既に得られていることが前提となる。

b)は，情報セキュリティ対策として想定できるものの包括的なリストである。本モデルは，14 個の対策で構成されるリストを使用する。これは，情報セキュリティ対策の汎用的なリストとして，本研究において提案するものである。また，本モデルは，このリストの 14 個の情報セキュリティ対策を，組織において実装する際にかかる費用の情報も必要とするが，これらの値は，組織の規模，事業の内容，組織の内外部の環境などによって一般に異なるため，組織ごとに算出することを想定している。この算出方法については，汎用的な手法は示せてないものの，5 章において，実データを用いた算出方法の例を示している。

c)は，a)の各情報セキュリティリスクに対して，b)の各情報セキュリティ対策がどれだけ影響を持つかを示す値である。組織で特定されたリスクに対して，汎用的な情報セキュリティ対策がどの程度影響を持つかを定量化した値である。本モデルでは，各対策の各リスクに対する影響値を，0 から 1 の範囲で数値化する方法について提案する。本モデルは，b)で述べた 14 個の情報セキュリティ対策で構成される汎用的リストを用いることを提案するが，情報セキュリティリスクのリストについては一意に特定していないため，様々な情報セキュリティリスクのリストが使用されることを想定し，それらに対する影響値を求める手法を示している。詳細な算出手法は 2.2 で述べる。

d)のリスク受容値は,組織として受容できるリスクの大きさの最大値を示すものである。これを超える大きさのリスクについては，組織として何らかの対策が必要であることを意味する。従って，リスク受容値は,a)のリスク評価値を求める際に使用した評価基準を用いて,その中の値として設定する。例えば，後節では，リスクを 0 から 9 の離散数値で評価する例を示している。この場合には，リスク受容値は 0 から 9 のいずれかの数値で設定することになる。なお，この例では，リスクが大きい場合により大きなリスク値を設定することとしているため,例えばリスク受容値を 4 とすると，5 以上の値を持つリスクが受容できないことを意味する。組織において特定されたリスクは，リスク対応プロセスの中で，原則リスク受容値以下に修正される。本モデルにおいても，リスク受容値は，リスクを修正する際のリスク値の上限であり，制約条件を示す要素として用いられる。

e)の情報セキュリティ対策に対する組織の予算は,組織が情報セキュリティ対策に対して割り当てる費用の総額のことである。情報セキュリティ対策に対して費やせる上限額とも言える。すなわち，この値もまた，本モデルにおいて制約条件を示す要素である。

要素のうち a)から c)は，本モデルが解を求める際の固定値である。これに対して，d)及び e)の値は本

モデルに対する入力値となるため，いろいろ異なる数値を割り当てることができる。

本モデルは，最適な情報セキュリティ対策の選択について示すことを目的としている。本モデルの解，すなわち選択結果は，b)の 14 個の情報セキュリティ対策が，各々何パーセント選択されたかを示す 14 個の割合値の組として示される。すなわち，ある対策の結果が 0%の場合は，その対策が選択されないことを意味し，50%の場合には，その対策内容のうち半分が，100%の場合にはすべてが選択されることを意味する。本モデルは，また，選択された管理策の実装に必要な費用の合計値についても算出する。これは e)の組織の予算以下の値となる。

d)及び e)の値を入力すると，モデルは情報セキュリティ対策の最適な選択結果のひとつを示す。さらに，d)及び e)の値をいろいろ変化させることで，組織にとって適切なリスク受容値や予算額を見つけることも可能になる。こうしたモデルの基本的な使い方については 3 章で述べる。

モデルは， ソルバーアドイン機能を追加した Excel 2010 を用いて実装した。Excel 2010 における実装イメージを図 1 に示す。

情報セキュリティ対策 ＼ リスク		a) R_1	R_2	R_3	R_4	R_5	R_6	R_7	選択結果: 情報セキュリティ対策の適用率(%)（出力値）
リスク値	対策費用	7	6	8	7	9	8	6	
b) H_1	500	c) 0.01	0.01	0.01	0.01	0.01	0.01	0.01	f)
H_2	1000	0.06	0.06	0.06	0.06	0.06	0.05	0.02	
H_3	1000	0.04	0.03	0.00	0.02	0.02	0.00	0.00	
H_4	1500	0.10	0.10	0.09	0.10	0.10	0.09	0.04	
H_5	2500	0.13	0.13	0.12	0.12	0.12	0.11	0.00	
H_6	1000	0.02	0.02	0.02	0.02	0.02	0.02	0.00	
H_7	5000	0.13	0.13	0.12	0.13	0.13	0.10	0.07	
H_8	1500	0.11	0.11	0.08	0.11	0.11	0.07	0.03	
H_9	1500	0.06	0.06	0.06	0.06	0.06	0.06	0.06	
H_{10}	2000	0.11	0.12	0.10	0.10	0.11	0.10	0.08	
H_{11}	3000	0.02	0.03	0.02	0.02	0.03	0.02	0.02	
H_{12}	1500	0.05	0.05	0.05	0.05	0.05	0.05	0.05	
H_{13}	2000	0.04	0.04	0.04	0.04	0.04	0.04	0.04	
H_{14}	1000	0.06	0.06	0.04	0.06	0.06	0.04	0.04	
選定された情報セキュリティ対策実装にかかる費用合計 （出力値）									
情報セキュリティ対策のための組織の予算 （入力値）									e)
リスク受容値 （入力値）									d)

図 1 モデル実装画面，モデルの各要素，及びモデルによる解のイメージ

2.2 モデルの要素

(1) 情報セキュリティリスクのリスト

これは，組織において想定される情報セキュリティリスクの包括的なリストである。情報セキュリティリスクマネジメントにおいて，リスク対応の前プロセスにあたるリスクアセスメントのアウトプットとして特定される。本モデルでは，組織が情報セキュリティリスクアセスメントを実施し，このリストを得ていることを前提とする。尚，本モデルは，リストに含まれるリスクの数としては，10 個程度を想定している。つまり，組織が，10 前後のリスクからなるリストをリスクアセスメントのアウトプットとしてもつことを想定する。これは，数 10 や 100 を超える数のリスクを，組織レベルで適切に継続・管理していくことは現実的でないという考えに基づいている。扱うリスクの数が多いということは，その分個々のリスクの具体性が増すということである。それによりリスクを特定したり，特定したリスクに対する対策を検討したりするリスクマネジメントの活動がより具体的になるとはいえ，その結果，組織全体を俯瞰するという観点からは煩雑すぎたり，かかる工数が大変大きなものとなったりするため，現実的とはいえない。リストに含まれるリスクの粒度を大きく捕らえることで，リスクの総数を適当な値に調整できる。組織レベルのリスクアセスメント活動では，このような考えのもとで特定するリスクの数を抑制することは，妥当な行為である。

一方で，情報セキュリティリスクのリストには，組織において想定される情報セキュリティリスクが漏れなく含まれていなければならない。特定されないリスクは，その後の対応を検討することができないためである。本研究では，提案するモデルの検証を進めるために情報セキュリティリスクのリストを必要とするため，包括的であり且つその数が 10 前後である情報セキュリティリスクのリストを検証用サンプルとして作成することにした。リスクの数が少なく，かつ包括的であるという一見矛盾するようなリストを策定するために，情報セキュリティリスクをいくつかの属性を用いて分類し，分類のひとつひとつをそれぞれひとつのリスクとみなすことによって，リストを作成する手法をとることにした。以下では，実際にリスト作成において取った手法を説明する。情報セキュリティを分類するための属性として，リスク顕在化の原因となるエンティティ，及びそのエンティティの動機の 2 つを取り上げる。エンティティは，組織の雇用者，契約者，外部者，及び人以外の 4 つに分類できる。また，リスクを顕在化させるに至るエンティティの動機は，意図的なものと，意図しない偶発的なものとに分類できる。このような属性及び分類をもちいることで，情報セキュリティリスクは 7 つに分類できる。なお，人以外によって顕在化するリスクは意図的なものを含まないため，想定しなかった。このため，各々4 個及び 2 個の要素からなる 2 つの属性を用いた分類の数は 7 個となる。（表 1 参照）これらの各分類を各々ひとつのリスクと捉えることで，7 個のリスク R_1，〜，R_7 で構成されるリストが得られる。分類という手法を用いていることから，情報セキュリティリスクを具体的に想定した場合にも，いずれのリスクも 7 個のうちいずれかに含まれると考えられるため，このリストは包括的とみなすことができる。

表 1　情報セキュリティリスクのリストの例(1)

－ 基本モデルで使用 －

リスク	属性 1 エンティティ	属性 2 動機	具体的リスクの例
R_1	雇用者	意図的	権限を悪用しての情報の漏えいや改ざん，機器やシステムの破壊など
R_2	契約者	意図的	同上
R_3	外部者	意図的	不正侵入による情報漏えいや改ざん，機器やシステムの破壊など
R_4	雇用者	偶発的	誤用や不注意による情報の漏えいや改ざん，機器やシステムの破壊など
R_5	契約者	偶発的	同上
R_6	外部者	偶発的	誤用や不注意によるデータ（情報），機器，及びシステムの破壊など
R_7	人以外	偶発的	機器の故障，停電など

基本モデルでは，表 1 のリストを用いる。しかし，これは情報セキュリティリスクのリストの 1 例である。4 章では，モデルの更なる検証のために，経済産業省による情報処理実態調査 [40]のデータを用いている。そこではリスクのリストとして表 2 を用いている。表 2 のリストは， [40]の内容に沿って作成したものである。このように，情報セキュリティリスクのリストは，モデルを適用するデータによって異なる場合がある。

表 2　情報セキュリティリスクのリストの例(2)

－ 情報処理実態調査データによるモデル検証で使用 －

リスク	内容	具体的リスクの例
R_1	システムの停止	内部要因／外部要因（地震，火災等の問題による）によるシステムの停止など
R_2	その他のシステムトラブル	DoS 攻撃，スパムメールや DoS 攻撃の中継利用，ホームページやファイル，データの改ざんなど
R_3	不正アクセス	IP・メールアドレス詐称，リソースの不正利用，内部関係者による不正アクセスなど
R_4	コンピュータウィルス	（USB 経由，スパムメール，ホームページ，標的型サイバー攻撃などの経路による）ウィルスなどの感染，トロイの木馬など
R_5	重要情報の漏えい	コンピュータウィルス，ファイル共有ソフトに起因する情報漏えい，不正アクセスによる情報漏えい，標的型サイバー攻撃による情報漏えい，内部者による情報漏えい，委託先による情報漏えい，ノートパソコン及び携帯記憶媒体等の盗難・紛失など
R_6	その他	ホームページ上での誹謗中傷，その他

尚，ここで，上で示した情報セキュリティリスクは，いずれも情報資産や脅威によって特定されることを必要しないことに留意されたい。本モデルでは，組織が継続的に管理できる 10 前後のリスクが特定され，そのリスクに対して(2)で説明するリスク値を設定できるだけでよい。1.3 で検討した先行研究のうち，文献 [29] [30] [31]は，組織に適用できる手法を提案するが，情報資産・脅威・対策案の関係のモデ

ル化を前提としていた。本研究において参照している ISO/IEC 27001 [2]が，2013 年の改訂において，情報資産，脅威及びぜい弱性の特定と評価に基づくリスクアセスメントに関する要求事項を修正し，より自由度の高い内容に変更されたことを考えると，情報資産や脅威を特定しない手法は，今後必要性が高まると思われる。さらに，組織を対象としたリスクアセスメントにおいては，そのような具体性を手法から排除することも，適用組織の規模などを想定した場合には必要となろう。

(2) 各情報セキュリティリスクの定量的評価値

本モデルは，定量化されたリスク値を必要とする。この値もまた，情報セキュリティリスクアセスメントのアウトプットに含まれるものであり，本モデルは，そのアウトプットから得られる値の使用を前提とする。

(1)で作成したモデル検証用の情報セキュリティリスクのリスト（表 1）についても，各リスクのリスク値が必要となる。このリスク値の設定方法については，ISO/IEC 27005 [3]や ISMS ユーザーズガイド [20] [21]をはじめ，多くの書籍で紹介されている。その多くの場合，リスク値は相対的評価により数段階に評価されている。従って， 表 1 の各リスクには，0 から 9 の 10 段階の離散的数値をリスク値として割当て，相対的評価結果として表 3 の数値を用いることとする。なお，ここでは，値が大きいほうがリスクが大きいとする。すなわち，0 がリスクが最小の場合を表し，9 がリスクが最大の場合を表す。

表 3　リスク値の設定例(1)

－ 基本モデルで使用 －

リスク	R_1	R_2	R_3	R_4	R_5	R_6	R_7
リスク値	7	6	8	7	9	8	6

4 章の情報処理実態調査 [40]のデータによるモデルの評価においては，表 4 の数値を用いた。これらは，[40]の概評 5-1-1 及び表 5-2-1-1-1 にリスクの重要度や発生状況に関するデータが示されているため，それらを用いて算出した。

表 4　リスク値の設定例(2)

－ 情報処理実態調査データによるモデル検証で使用 －

リスク	R_1	R_2	R_3	R_4	R_5	R_6
リスク値	9	4	5	8	6	4

(3) 情報セキュリティ対策のリスト及び各対策を実施するために必要な費用

リスク対応のプロセスでは，特定された情報セキュリティリスクのうち，組織が受容できないものについては，何らかの情報セキュリティ対策を行い，リスクを受容できるレベルまで修正する。リスクの修正が適切に行われるためには，想定される情報セキュリティ対策の包括的なリストが用意されていることが望ましい。包括的なリストがあれば，そこから必要な対策を選択することで，実際に行うべき情報セキュリティ対策がリストにないために選択されず，その結果として対応漏れが生ずることを防げるであろう。従って，ここでは，汎用的に用いることができる，包括的な情報セキュリティ対策のリストの作成について提案する。

尚，先行研究においては，このような情報セキュリティ対策のリストの作成方法について示すものは無かった。資産・脅威・対策案の関係のモデル化により，対策の最適な組み合わせを求める手法を提案する，文献 [29] [30] [31]の研究では，情報セキュリティ対策のリストの作成方法に関する記述としては，文献 [29]に「電子商取引推進協議会（ECOM）情報セキュリティマネジメント標準（JIS X 5080:ISO/IEC 17799）の解説 [32]をもとに現状考えうるものを列挙した。また，組織的な活動により実現できる対策は優先的に実施されているものとして削除した」とあるにすぎない。文献 [29]及び [30]では，ノウハウが無いものについてもそれらの中で提案されるモデルを適用することで，最適な対策の選定が行えることを提唱しているため，情報セキュリティ対策のリストの作成方法いついて明確な記述が無いことは，内容として不足しているとみなせる。限定範囲に対する詳細な脅威分析に基づき対策を選定する手法を提案する文献 [37] [38] [39]の研究では，文献 [37]に「対策目標の候補集合」という表現はあるものの，その作成方法に関する記述は無かった。文献 [38]では，脅威が不正コピーに限定されており，これに対する対策のカテゴライゼーションは示されていたが，内容が特化されすぎていた。また文献 [39]では，対策候補のリストに相当する概念が記されていなかった。

包括的な情報セキュリティ対策のリストを作成するために，ISO/IEC 27002 [7]を参照する。この国際規格は，情報セキュリティリスクを修正するために選択する対策を管理策という単位で掲載しているガイドライン規格であり，管理策は管理目的ごとにまとめられている。また類似の管理目的は集められて，ひとつの箇条として構成されている。この国際規格は，14 の箇条で構成され，文書全体で管理目的は 35 個，管理策は 114 個ある。各箇条には 1 つ以上の管理目的が含まれ，各管理目的は 1 個以上の管理策で構成されている。各箇条が保有する管理目的，各管理目的に含まれる管理策の数は表 5 のとおりである。なお，表 5 の表現は，JIS Q 27001 [9]の表現である。

表 5　JIS Q 27002:2014（ISO/IEC 27002:2014）の箇条，管理目的及び管理策の構成

箇条	箇条タイトル	管理目的のタイトル	管理策数
5	情報セキュリティのための方針群	情報セキュリティのための経営陣の方向性	2
6	情報セキュリティのための組織	内部組織	5
		モバイル機器及びテレワーキング	2
7	人的資源のセキュリティ	雇用前	2
		雇用期間中	3
		雇用の終了及び変更	1
8	資産の管理	資産に対する責任	4
		情報分類	3
		媒体の取扱い	3
9	アクセス制御	アクセス制御に対する業務上の要求事項	2
		利用者アクセスの管理	6
		利用者の責任	1
		システム及びアプリケーションのアクセス制御	5
10	暗号	暗号による管理策	2
11	物理的及び環境的セキュリティ	セキュリティを保つべき領域	6
		装置	9
12	運用のセキュリティ	運用の手順及び責任	4
		マルウェアからの保護	1
		バックアップ	1
		ログ取得及び監視	4
		運用ソフトウェアの管理	1
		技術的ぜい弱性管理	2
		情報システムの監査に対する考慮事項	1
13	通信のセキュリティ	ネットワークセキュリティ管理	3
		情報の転送	4
14	システムの取得，開発及び保守	情報システムのセキュリティ要求事項	3
		開発及びサポートプロセスにおけるセキュリティ	9
		試験データ	1
15	供給者関係	供給者関係における情報セキュリティ	3
		供給者のサービス提供の管理	2
16	情報セキュリティインシデント管理	情報セキュリティインシデントの管理及びその改善	7
17	事業継続マネジメントにおける情報セキュリティの側面	情報セキュリティ継続	3
		冗長性	1
18	順守	法的及び契約上の要求事項の順守	5
		情報セキュリティのレビュー	3

ISO/IEC 27002 [7]を参照した理由は，主に 2 つある。ひとつは，この国際規格が ICT や情報セキュリティの分野で広く参照されていることである。ISMS 認証を取得している事業者だけを見ても，既に全世界で 20,000 に近い事業者が ISO/IEC 27002:2013 の管理目的及び管理策ベースで，組織の情報セキュリティ対策を計画及び実装している [4]。また，認証取得はしていなくとも，情報セキュリティの具体的な

対策を実装するために，この国際規格を参照する組織は多い。また，国内では，経済産業省による情報セキュリティ監査制度において，情報セキュリティ監査にあたっての判断の尺度を示した「情報セキュリティ管理基準」が，この国際規格を参照して作成されている。また、内閣官房情報セキュリティセンター（NISC）が発行する「政府機関の情報セキュリティ対策のための統一基準」では，基準として示されている順守事項とこの国際規格の項目を対応付ける文書が発行されており，この国際規格の活用がなされている。このように広く参照，活用されているのは，この国際規格が，汎用的には，情報セキュリティの対策をある程度網羅的に含むと見なされているからであると言える。本モデルにおいて，情報セキュリティ対策のリストを作成するためにこの国際規格を参照したもう一つの理由にもあたる。

一方，情報セキュリティのリストと同様に，組織全体を俯瞰する情報セキュリティリスク対応を行うためには，リスト化される情報セキュリティ対策の数は多すぎてはならない。継続的な管理が実現できるような数となるよう配慮し，ISO/IEC 27002 [7]の箇条単位でリスト化することとした。その結果，14個の情報セキュリティ対策のリストを作成した。なお，ここで 14 個のリストに含まれる情報セキュリティ対策を以降，リスクヘッジ策と呼ぶことにする。情報セキュリティ対策は，一般的な表現であるため，リストに含まれる対策なのか一般的な意味での対策なのか区別がつけにくいため，ここではリスクヘッジ策という固有の表現を充てることにした。また，管理策は情報セキュリティ分野では，ISO/IEC 27002 [7]で示される特定の情報セキュリティ対策を意味するため，この表現も避けた。（表 6 参照）

表 6　情報セキュリティ対策（リスクヘッジ策）のリスト

リスクヘッジ策	対策の内容
H_1	情報セキュリティのための方針群
H_2	情報セキュリティのための組織
H_3	人的資源のセキュリティ
H_4	資産の管理
H_5	アクセス制御
H_6	暗号
H_7	物理的及び環境的セキュリティ
H_8	運用のセキュリティ
H_9	通信のセキュリティ
H_{10}	システムの取得，開発及び保守
H_{11}	供給者関係
H_{12}	情報セキュリティインシデント管理
H_{13}	事業継続マネジメントにおける情報セキュリティの側面
H_{14}	順守

本モデルにおいては，14 個のリスクヘッジ策を組織において実装する際にかかる費用の情報も必要である。これら 14 個のリスクヘッジ策自体は，組織の特性などに拠らない汎用的なものであると言えるが，これらを各組織に実装する場合にかかる費用は，組織ごとに異なるため，本モデルにおいては，リスク

ヘッジ策の実装に係る費用は，各組織が算出することを想定している。表 7 は，モデル検証用に仮に設定した，各リスクヘッジ策を実装するために必要な費用である。

表 7　各リスクヘッジ策実装にかかる費用

リスクヘッジ策	リスクヘッジ策実装にかかる費用
H_1	500
H_2	1000
H_3	1000
H_4	1500
H_5	2500
H_6	1000
H_7	5000
H_8	1500
H_9	1500
H_{10}	2000
H_{11}	3000
H_{12}	1500
H_{13}	2000
H_{14}	1000
費用計	25000

14 個のリスクヘッジ策は，いずれも，その作成方法から明らかなように，具体的な対策を多く含む粒度の大きい情報セキュリティ対策である。ISO/IEC 27002 [7]の箇条がひとつのリスクヘッジ策に相当するため，その箇条に含まれる管理策や，管理策の実施の手引きに記述された内容はすべて，そのリスクヘッジ策に含まれることになるためである。そこで，各リスクヘッジ策の傾向や特徴を分かりやすくするために，管理策や管理策の実施の手引きの記述に対して，表 8 に示す観点を適用し，それぞれの観点に相当する具体的な対策内容が書かれている数をカウントすることで分析を行った。表 8 は， [41]に示されている分類をベースに，外部委託先の管理など，一部含まれていないものについて追加する形で作成した。

表 8　分析の観点

観点	各観点に含まれる対策内容
物理的セキュリティ対策	・不正な立入り、損傷及び妨害から保護するための適切な設備の設置、 ・出入管理 ・執務室にあるパソコン等の盗難対策　　等
技術的セキュリティ対策	・コンピュータ及びネットワークの管理 ・アクセス制御 ・システム開発、導入、保守等 ・コンピュータウィルス対策 ・セキュリティ情報の収集　　等
運用的セキュリティ対策	・情報システムの監視及びポリシーの遵守状況の確認（以下「運用管理」という。） ・運用管理における留意点 ・侵害時の対応策 ・外部委託による運用契約　　等
人的セキュリティ対策	・役割・責任、免責事項 ・教育・訓練 ・事故、欠陥に対する報告 ・パスワードの管理 ・非常勤及び臨時職員等の雇用及び契約　　等

分析した結果，得られたのが表 9 である。

表 9　各リスクヘッジ策の分析結果

リスクヘッジ策	4 つの観点ごとの具体的対策の数				具体的対策数の合計
	物理的	技術的	運用的	人的	
H_1	2	0	0	1	3
H_2	2	2	7	5	16
H_3	0	0	4	5	9
H_4	5	5	10	4	24
H_5	5	13	14	1	33
H_6	0	2	2	0	4
H_7	15	8	15	2	40
H_8	3	10	14	3	30
H_9	2	4	7	3	16
H_{10}	3	9	13	4	29
H_{11}	0	0	5	3	8
H_{12}	0	2	7	4	13
H_{13}	2	2	4	1	9
H_{14}	2	3	8	3	16
観点別にカウントした具体的対策数の合計					250

表 9 の結果は，リスクヘッジ策 H_1～H_{14} の傾向を知るだけでなく，それらを組織に実装する場合の費用を想定する際にも使用することができる。大枠での費用概算の想定方法として，例えば，物理的対策，技術的対策，人的対策，及び運用的対策をそれぞれ 1 つ実施するのにかかる費用を単位費用として設定し，リスクヘッジ策に含まれる各々の対策数と単位費用の積を取り，4 つの観点の合計値をリスクヘッジ策ごとにかかる費用とするなどの方法をとることができる。尚，この手法をさらに単純化し，物理的対策，技術的対策，人的対策，及び運用的対策の各対策を 1 つ実施するのにかかる費用はいずれも同じであるという仮定を置いて，具体的対策の単位費用を求め，そこから各リスクヘッジ策実装にかかる費用を求めるという算出方法の例を，5 章において，算出方法の例として示している。

14 個のリスクヘッジ策は，粒度が大きく，その中に複数の具体的対策を含むことは既に述べたとおりである。このことは，リスクヘッジ策の選択にも影響する。各リスクヘッジ策が，そうした複合的なものであるのに，その選択を「選択する」又は「選択しない」の 2 拓とすることは適切とはいえない。従って，本モデルでは，各情報セキュリティ対策の選択は，パーセンテージを用いて割合をもって選択することとした。例えば，あるリスクヘッジ策の選択結果が 0%の場合は，その対策が選択されなかったことを意味し，50%の場合には，その対策内容のうち半分が，100%の場合にはすべてが選択されたことを意味する。なお，本モデルでは，単純化のために，各リスクヘッジ策において，リスクヘッジ策の適用率とそれに係る費用は正比例の関係にあるとの前提を置いた。すなわち，リスクヘッジ策 H_i（i は 1～14 のいずれかの数）の実装に係る費用を 100 万円と想定した場合，H_i が 30%選択されれば，そのための費用は 30 万円となる。

(4) 各情報セキュリティ対策の各情報セキュリティリスクに対する影響値

特定された情報セキュリティリスクに，適切な情報セキュリティ対策を適用するためには，各情報セキュリティ対策が各情報セキュリティリスクに対してどのように効果があるのかという関係を明らかにする必要がある。このため，本モデルでは，表 6 で示した各リスクヘッジ策が，特定した情報セキュリティリスクに対しどの程度影響を持つかを定量化する手法について提案する。そのために，表 9 を求めたのと同様に，表 8 の観点を用いつつ，各リスクヘッジ策に含まれる管理策及び管理策の実施の手引きの内容を参照することから始める。リスクヘッジ策 H_3 の，表 1 の各情報セキュリティリスクに対しての影響値を算出する場合を例に，以下でその方法を示す。

まず，第 1 ステップとして，H_3 には，「箇条 7 人的資源のセキュリティ」が対応するため，箇条 7 に含まれる各管理策が，情報セキュリティリスク各々に影響するかどうかを評価する。JIS Q 27002 [9]（ISO/IEC 27002 [7]）の各管理策及び管理策の実施の手引きの記述内容を参照し，各情報セキュリティリスクに影響する対策が示されているかを確認する。管理策及び管理策の実施の手引きに含まれる具体的な対策を特定するにあたっては，表 8 の 4 つの観点（物理的，技術的，人的，及び運用的）を適用し，それぞれの観点ごとに該当する記述があるかを確認する。関係を定量化するために，該当する記述がある場合には 1 を，無い場合には 0 を設定する。例えば，管理策 7.1.1 では，従業員の雇用前の選考に関す

る具体的対策が示されている。しかし，契約者や外部者によるリスクに対する対策は記されていない。また，人以外によるリスクに対する対策も記されていない。さらに，選考に関する管理策であるため，物理的観点の対策や技術的観点の対策に関する記述はない。管理策には，雇用や契約時の留意事項について記述されているものの，これは表 8 によれば，運用的対策には相当せず，人的対策に相当する。以上をまとめると，管理策 7.1.1 については，内部者による情報セキュリティリスク R_1 及び R_2 に対して影響を持つ人的対策のみが記されていることが確認でき，その結果，表 10 に示すとおり，7.1.1 については，R_1 と H の交差するセル，及び R_2 と H の交差するセルの値のみ 1 となり，他セルは 0 となる。他の管理策についても同様にして表 10 の結果を得る。

尚，セルの値が 0 であるか 1 であるかの判断は，各管理策及び管理策の実施の手引きの記述内容を参照し，各情報セキュリティリスクに影響する対策が示されているか否かを確認するという活動に基づくため，実施者の主観を排除することは難しい。そこで，今回は，なぜ 0 又は 1 と判断したかの根拠をメモとして残すことで透明性及び客観性を確保することとした。これにより，例えば，次の見直しのタイミングで，前回の結果を再検討する場合や，実施者が変更となった場合に，既存の判断の妥当性を検討することができる。また，判断に誤りが見つかった場合や，異なる判断を取る決断をした場合に，値を変更することができる。尚，この際にも，変更の理由や新たな根拠をコメントとして残すことを推奨する。

次に，第 1 ステップで特定した値を集計する。すなわち，情報セキュリティリスク毎に，全ての管理策について観点毎に設定された値（0 又は 1）の和をとる。また，影響値を割合として表すため，求めた和を 250 で割り，その値を影響値とする。ここで，250 は，観点別にカウントした管理策の延べ数である（表 9 参照）。

残りのリスクヘッジ策についても同様にして，各リスクヘッジ策の各情報セキュリティリスクに対する影響値を求めることができる。尚，情報セキュリティリスクのリストとして，表 2 やその他のリストを用いる場合にも同様の手法で影響値を求めることができる。表 1 の情報セキュリティリストに対する影響値を表 11 に，表 2 の情報セキュリティリストに対する影響値を表 12 に示す。尚，上記手順に沿って各影響値を算出した際の記録を，付録 A に記す。

表 10　表 1 の情報セキュリティリスクに対するリスクヘッジ策 H_3 の影響値算出

管理策	観点	情報セキュリティリスク						
		R_1	R_2	R_3	R_4	R_5	R_6	R_7
箇条 7								
7.1 雇用前								
7.1.1	物理的対策	0	0	0	0	0	0	0
	技術的対策	0	0	0	0	0	0	0
	人的対策	0	0	0	0	0	0	0
	運用的対策	1	1	0	0	0	0	0
7.1.2	物理的対策	0	0	0	0	0	0	0
	技術的対策	0	0	0	0	0	0	0
	人的対策	1	1	0	0	0	0	0
	運用的対策	1	1	0	0	0	0	0
7.2 雇用期間中								
7.2.1	物理的対策	0	0	0	0	0	0	0
	技術的対策	0	0	0	0	0	0	0
	人的対策	1	1	0	1	1	0	0
	運用的対策	0	0	0	0	0	0	0
7.2.2	物理的対策	0	0	0	0	0	0	0
	技術的対策	0	0	0	0	0	0	0
	人的対策	0	0	0	0	0	0	0
	運用的対策	1	1	0	1	1	0	0
7.2.3	物理的対策	0	0	0	0	0	0	0
	技術的対策	0	0	0	0	0	0	0
	人的対策	1	0	0	0	0	0	0
	運用的対策	1	0	0	0	0	0	0
7.3 雇用の終了及び変更								
7.3.1	物理的対策	0	0	0	0	0	0	0
	技術的対策	0	0	0	0	0	0	0
	人的対策	1	1	0	1	1	0	0
	運用的対策	1	1	0	1	1	0	0
合計(*1)		9	7	0	4	4	0	0
影響値（合計/250 (*2)）		0.04	0.03	0	0.02	0.02	0	0

(*1) 情報セキュリティリスク毎の，観点別管理策との関係値（0 又は 1）の和
(*2) 観点別にカウントした管理策の延べ数（表 9 参照）

表 11　各情報セキュリティリスクに対する各リスクヘッジ策の影響値(1)

－ 基本モデルで使用 －

情報セキュリティ リスク / リスクヘッジ策	R_1 内部者の意図的な	R_2 契約者の意図的な	R_3 外部者の意図的な	R_4 内部者の偶発的な	R_5 契約者の偶発的な	R_6 外部者の偶発的な	R_7 人以外の偶発的な
H_1	0.01	0.01	0.01	0.01	0.01	0.01	0.01
H_2	0.06	0.06	0.06	0.06	0.06	0.06	0.03
H_3	0.04	0.03	0.00	0.02	0.02	0.00	0.00
H_4	0.10	0.10	0.09	0.10	0.10	0.09	0.02
H_5	0.13	0.13	0.12	0.12	0.12	0.11	0.00
H_6	0.02	0.02	0.02	0.02	0.02	0.02	0.00
H_7	0.13	0.13	0.12	0.13	0.13	0.11	0.06
H_8	0.11	0.11	0.08	0.11	0.11	0.07	0.02
H_9	0.06	0.06	0.06	0.06	0.06	0.06	0.06
H_{10}	0.11	0.12	0.10	0.10	0.11	0.10	0.08
H_{11}	0.02	0.03	0.02	0.02	0.03	0.02	0.02
H_{12}	0.05	0.05	0.05	0.05	0.05	0.05	0.05
H_{13}	0.04	0.04	0.04	0.04	0.04	0.04	0.04
H_{14}	0.06	0.06	0.04	0.06	0.06	0.04	0.04

表 12　各情報セキュリティリスクに対する各リスクヘッジ策の影響値(2)

－ 情報処理実態調査データによるモデル検証で使用 －

情報セキュリティ リスク / リスクヘッジ策	R_1 システムの停止	R_2 その他のシステムトラブル	R_3 不正アクセス	R_4 コンピュータウィルス	R_5 重要情報の漏えい	R_6 その他
H_1	0.01	0.01	0.01	0.01	0.01	0.01
H_2	0.02	0.02	0.03	0.03	0.03	0.02
H_3	0.02	0.02	0.02	0.02	0.02	0.02
H_4	0.00	0.04	0.04	0.03	0.05	0.00
H_5	0.00	0.01	0.07	0.00	0.01	0.00
H_6	0.00	0.01	0.01	0.00	0.01	0.00
H_7	0.06	0.02	0.03	0.01	0.04	0.05
H_8	0.04	0.05	0.04	0.03	0.03	0.02
H_9	0.01	0.03	0.02	0.03	0.03	0.02
H_{10}	0.05	0.05	0.05	0.05	0.06	0.05
H_{11}	0.02	0.01	0.01	0.01	0.01	0.02
H_{12}	0.03	0.03	0.03	0.03	0.03	0.03
H_{13}	0.02	0.00	0.00	0.00	0.00	0.02
H_{14}	0.01	0.01	0.02	0.02	0.03	0.03

2.3 モデルの定式化及びモデルの解

各リスクヘッジ策の選択割合の組（x_1，x_2，…，x_{14}）を変数とし，これの最適解を導くようにモデルを定式化する。選択割合はパーセンテージで示されるため，$0 \leqq x_i \leqq 100$（$1 \leqq i \leqq 14$，i：整数）である。また，本モデルにおいて入力値として扱われるリスク受容値，及び情報セキュリティ対策に対する組織の予算はいずれも制約条件となる。（x_1，x_2，…，x_{14}）が最適解となる条件は，本モデルでは，次のように設定する。

a) リスク受容値以上のリスク値をもつ情報セキュリティリスクは，いずれもリスク値がリスク受容値以下に修正される。

b) 最適解で選択された割合でリスクヘッジ策を実装するためにかかる総費用は，情報セキュリティ対策に対する組織の予算以下である。

c) 最適解は，修正されたリスクとリスク受容値との乖離を最少化する。

a)及びb)の条件は，制約条件から導かれる。c)の条件は，修正されたリスクとリスク受容値との乖離が大きいほど費用を余分に使うことを意味するため，これをできるだけ小さく押えるべきであるという考え方に基づいている。これらの条件を定式化すると次のようになる。

情報セキュリティリスク R_jの修正前のリスク値を r_j，修正後のリスク値を r_j’とすると，a)の条件は，(1)式で表現できる。ただし，リスク受容値を R_{accept}，リスクヘッジ策 H_iの情報セキュリティリスク R_jに対する影響値を e_{ij}とする。

$$r_j^{'} = r_j \bullet (1 - \frac{\sum_{i=1}^{14} e_{ij} \bullet x_i}{\sum_{i=1}^{14} e_{ij}} \bullet \frac{1}{100}) \leq R_{accpet} \tag{0}$$

b)の条件は，リスクヘッジ策 H_i を実装するためにかかる費用を c_i，及び情報セキュリティに対する組織の予算をBとするとき，(2)式で表現できる。

$$\sum_{i=1}^{14} c_i \bullet x_i \leq B \tag{0}$$

c)の条件は，最適解を導く目的関数を示す。これは，(3)式として表現できる。

$$Min.\{ f(x_i) = \sum_{j=1}^{7} (R_{accpet} - r_j^{'}) \} \tag{0}$$

本モデルでは，最適解で選択された割合でリスクヘッジ策を実装するためにかかる総費用もモデルの解とみなす。すなわち，(3)式を満たす（x_1，x_2，…，x_{14}），及び(2)式の左辺 $\sum_{i=1}^{14} c_i g x_i$ の値の組みが，本モデルの解となる。

本モデルは，ソルバーアドオン機能を追加したExcel 2010を用いて実装しているため，(3)式を満たす最小値のひとつが導かれる。実際には最適解は複数存在する場合もある。その場合は最適解のうちのひとつが導かれることになる。また，リスク受容値や，情報セキュリティ対策に対する組織の予算として入力した値によっては，最適解を導けない場合もあり得る。本モデルのExcel 2010上での実装に伴う各種設定を付録Bに示す。尚，多目的線形計画法のモデルへの適用検討に際しては，[42] 及び [43]を参照した。また，0章で示す基本モデル，3章のサンプルデータを用いた基本モデルの検証は [44]にも示されている。

尚，先に述べたとおり，先行研究においては，情報セキュリティ対策を選択するもとになる情報セキュリティ対策のリストについて，その作成方法に言及したものは無く，従って，その中から如何にして適切な情報セキュリティ対策を選択するかについても記述したものは少なかった。文献 [29]のリスクアセスメントにおいて特定した資産及び脅威に基づいて，対策を選択する手法，文献 [37]の脅威を基本事象に分け，これに対する対策を選択する手法があるが，いずれもリスクアセスメントを具体的に実施し，具体的な内容に沿って対策を検討するという手法にすぎない。

3　サンプルデータによる基本モデルの検証

3.1 基本モデル

基本モデルにおける各要素のうち，モデルにおいて固定値として扱われるものの設定は次のとおりである。

a-1) 情報セキュリティリスクのリスト：表 1 のリストを使用
a-2) 各リスクレベルの評価値：表 3 の設定例を使用
b-1) 情報セキュリティ対策のリスト：表 6 のリストを使用
b-2) 各対策を実施するために必要な費用：表 7 の値を使用，
c-1) 各情報セキュリティ対策の各情報セキュリティリスクに対する影響値：表 11 の値を使用

モデル分析では，リスク受容値及び情報セキュリティ対策に対する組織の予算（費用の上限）は，変数として扱い，入力値に対して，解の組み（各リスクヘッジ策の採用割合（パーセンテージ）及びそれらの実装にかかる費用の合計値）が得られる。本章では，基本モデルに，まず，解が自明であるような変数値を設定し，想定する解が得られるかをみることで，モデルの基本動作を確認する。次に，変数の値をいろいろ変えることによって，より効果的な解を導くことができるようなモデルの使い方を提案する。

3.2 基本動作の確認

(1)　入力値：リスク受容値=9 及び組織の予算＝25000

まず，入力値を，リスク受容値を 9，組織の予算を 25000 とする。基本モデルでは，リスク値として 0～9 の離散値を設定し，数が大きいほうがリスクが大きいことを表すため，リスク受容値を 9 とすることは，全てのリスクをそのままの状態で受容することを意味する。一方，25000 は，表 7 に示されるとおり，H_1～H_{14} のリスクヘッジ策を全て 100 パーセント実装した場合に係る費用の合計である。従って，「リスク受容値=9，及び組織の予算＝25000」という設定は，リスクヘッジ策の選択において，リスク受容値，組織の予算とも何の制約も与えないということを意味する。また，リスク受容値=9 として，全てのリスクをそのままの状態で受容するのであるから，予算が与えられているとしても，組織においてリスクを修正するための取り組みは必要ないということを意味する。

この入力値に対してモデルを適用すると，表 13 のとおり，十分な予算が与えられているにもかかわらず，いずれのリスクヘッジ策も選拓されず（すべて 0%），実装にかかる費用も発生しないという解が得られる。これは，想定どおりの結果である。

表 13　基本動作の確認(1)：リスク受容値=9 及び組織の予算＝25000

種別	項目		値
入力	リスク受容値		9
	情報セキュリティ対策に対する組織の予算		25000
解	選定されたリスクヘッジ策実装にかかる費用		0
	リスクヘッジ策の選定結果（%）	H_1	0
		H_2	0
		H_3	0
		H_4	0
		H_5	0
		H_6	0
		H_7	0
		H_8	0
		H_9	0
		H_{10}	0
		H_{11}	0
		H_{12}	0
		H_{13}	0
		H_{14}	0

(2) 入力値：リスク受容値=0 及び組織の予算＝25000

次に，リスク受容値を 0，組織の予算を 25000 とする。リスク受容値が 0 とは，全てのリスクを最小限のレベルにまで修正することを意味する。これに対して，組織の予算は，全てのリスクヘッジ策を 100%実装し得るだけの値となっている。従って，全てのリスクヘッジ策が 100%選択される結果となることが想定される。

モデルを適用すると，表 14 の結果となり，想定どおりすべてのリスクヘッジ策が 100%選択される結果となった。

表 14 基本動作の確認(2)：リスク受容値=0 及び組織の予算＝25000

種別	項目		値
入力	リスク受容値		0
	情報セキュリティ対策に対する組織の予算		25000
解	選定されたリスクヘッジ策実装にかかる費用		25000
	リスクヘッジ策の選定結果（%）	H_1	100
		H_2	100
		H_3	100
		H_4	100
		H_5	100
		H_6	100
		H_7	100
		H_8	100
		H_9	100
		H_{10}	100
		H_{11}	100
		H_{12}	100
		H_{13}	100
		H_{14}	100

3.3 モデルの活用方法の検討

(1) 与えられたリスク需要値に対する組織の予算の最小値の導出

次に，2 つの変数，リスク需要値と組織の予算に，入力する値を工夫することで，組織にとって最適な結果を得るようなモデルの使い方について示す。

変数のうち，リスク需要値を固定し，組織の予算の値を変化させ，結果を比較してみる。基本モデルを使用し，リスク需要値を 5 とする。まず，組織の予算を 8000 とすると，モデルの適用により，表 15 の(I)列に示す解が得られる。組織の予算を 7000 とすると，表 15 の(II)列に示す解が得られる。組織の予算を 6000 とした場合には，モデルは解を見つけることができない。これは，リスク需要値 5 の達成するには，組織の予算 6000 は十分ではないことを意味する。このことから，リスク需要値 5 に対して，これを実現する組織の予算の最小値は，6000 より大きく 7000 以下であることが分かる。

表 15　リスク需要値 5 に対して異なる組織の予算を設定した場合の解(1)

種別	項目		値		
			(I)	(II)	(III)
入力	リスク受容値		5	5	5
	情報セキュリティ対策に対する組織の予算		8000	7000	6000
解	選定されたリスクヘッジ策実装にかかる費用		8000	7000	－
	リスクヘッジ策の選定結果（%）	H_1	0	0	－
		H_2	0	18	－
		H_3	100	32	－
		H_4	100	100	－
		H_5	100	100	－
		H_6	0	0	－
		H_7	0	0	－
		H_8	100	100	－
		H_9	0	0	－
		H_{10}	0	0	－
		H_{11}	20	0	－
		H_{12}	0	0	－
		H_{13}	0	0	－
		H_{14}	91	100	－

組織の予算の最小値を，より精密に知りたい場合には，組織の予算に，6000 より大きく，7000 以下である値をさらに入力する。たとえば，中間値である 6500 を組織に予算に設定すると，表 16 の(IV)列で示される解を得る。解が得られたことから，さらに少ない組織の予算を入力して，6400 とした場合には表 16 の(V)列の解が得られる。6300 とすると，モデルは解を見つけることができない。このため，予算の最小値は，6300 より大きく，6400 以下であることが分かる。

表 16　リスク需要値 5 に対して異なる組織の予算を設定した場合の解(2)

種別	項目		値		
			(IV)	(V)	(VI)
入力	リスク受容値		5	5	5
	情報セキュリティ対策に対する組織の予算		6500	6400	6300
解	選定されたリスクヘッジ策実装にかかる費用		6500	6400	－
	リスクヘッジ策の選定結果（%）	H_1	0	0	－
		H_2	100	100	－
		H_3	0	0	－
		H_4	100	100	－
		H_5	47	12	－
		H_6	0	0	－
		H_7	0	0	－
		H_8	100	100	－
		H_9	0	0	－
		H_{10}	16	55	－
		H_{11}	0	0	－
		H_{12}	0	0	－
		H_{13}	0	0	－
		H_{14}	100	100	－

本モデルを使用すると，上の例のようにして，ある与えられたリスク受容値に対し，それを達成する組織の予算の最小値の近似解を得ることができる。このようなモデルの使い方をすることで，組織は，設定したリスク受容基準に対して，どの程度の予算が必要であるか知ることができる。また，リスク受容基準に対し，多すぎる予算を割り当てることもなくなるであろう。尚，予算が潤沢にある場合には，さらに高いリスク受容値を設定することも組織の選択に入ってくる。組織の予算に適したリスク受容値の設定を行うためのモデル活用方法についてを，以下に記す。

(2) 与えられた組織の予算に対する最小リスク受容値の導出

あらかじめ情報セキュリティ対策に対する組織の予算が確定している場合，その予算を最大限に活用するためには，達成できるリスク受容値はなるべく小さくしたい。なぜならば，リスク受容値が小さければ小さいほど，組織に残留するリスクが減るためである。そこで，モデルを用いて，与えられた組織の予算に対して達成可能なリスク受容値の最小値を，見つける方法を示す。

モデルの変数のうち，組織の予算を固定し，リスク受容値を変化させ，それぞれの場合の解を比較してみる。たとえば，組織の予算は 12000 とし，リスク受容値は，5 から順に減らしていく。それら入力の結果として，表 17 を得る。

リスク受容値を 5 とした場合，表 17 の(VII)列の解が得られる。しかし，この場合，各リスクヘッジ策を選定結果に沿って実装した場合にかかる費用の合計は 10757 であり，組織の予算 12000 を下回る。このことは，組織の予算 12000 に対して，リスク受容値 5 が十分なレベルではない可能性を意味する。すなわち，より小さなリスク受容値を達成できるかもしれない，ということである。次に，リスク受容値を 4 とすると，表 17 の(VIII)列の解が得られる。この場合は，実際にかかる費用も 12000 となり，組織の予算に対して釣り合いの取れたリスク受容値であることが分かる。さらに，リスク受容値 3 としてみる。この場合も，表 17 の(IX)列の解が得られ，実際にかかる費用は 12000 となる。リスク受容値 4 の場合も，組織の予算を満額使用して達成されるとはいえ，リスクヘッジ策の選択を変えることによって，同じ予算でリスク受容値 3 も達成できることが分かる。さらにリスク受容値を減らし，2 を設定すると，この場合にはモデルは解を見つけられない。従って，この例においては，組織の予算 12000 に対する，リスク受容値の最小値は 3 であることが分かる。

表 17　組織の予算 12000 に対して異なるリスク受容値を設定した場合の解

種別	項目		値			
			(VII)	(VIII)	(IX)	(X)
入力	リスク受容値		5	4	3	2
	情報セキュリティ対策に対する組織の予算		12000	12000	12000	12000
解	選定されたリスクヘッジ策実装にかかる費用		10755	12000	12000	－
	リスクヘッジ策の選定結果（%）	H_1	0	0	0	－
		H_2	0	100	100	－
		H_3	100	100	0	－
		H_4	100	100	100	－
		H_5	100	89	100	－
		H_6	100	0	0	－
		H_7	0	15	25	－
		H_8	100	100	100	－
		H_9	0	0	2	－
		H_{10}	0	2	100	－
		H_{11}	100	100	40	－
		H_{12}	0	0	0	－
		H_{13}	0	0	0	－
		H_{14}	26	100	100	－

上に示したようにモデルを活用することで，組織は，限られた予算の中で，どのレベルのリスク受容値を目指すことができるのか，あるいは，目指すリスク受容値を達成するためには，どのくらいの予算確保が必要かの目安を知ることが可能になる。

4　統計データによるモデルの検証

4.1 統計データの概要

組織における情報セキュリティリスクアセスメントや，情報セキュリティリスク対応の内容は，セキュリティ上の理由から一般には公表されない。従って，ここでは，公表されている統計データの情報を用いてモデルの検証を進めることとする。統計データは，経済産業省による平成 25 年度版情報処理実態調査 [40]の結果を用いた。このデータを使用した理由は，調査事項の中に，情報セキュリティの状況があり，情報セキュリティトラブルの発生状況，発生したトラブルに対する重要性の組織における認識，情報セキュリティ対策状況と対策費用など，モデルの要素として必要な値を得るためのデータが提供されていると考えたことによる。モデルがインプットとして必要な値を，このデータを用いて算出した具体的な方法については，以下に示す。

4.2 統計データを用いたモデル各要素の算出

(1) 情報セキュリティリスクのリスト及び各リスクレベルの評価値

情報セキュリティリスクのリストは，[40]の「集計表（概要)」の概表 5-1-1 を参照して，「トラブルの種類」で示されるカテゴリをリスクと見なすことで作成した。尚，トラブルのうち「システムトラブル」は，「システムの停止」と「その他のシステムトラブル」にカテゴリが細分されているものの，それぞれの詳細項目を見ると，前者は「内部要因によるシステムの停止」及び「外部要因（地震，火災等の問題）によるシステムの停止」を含み，後者が「DoS 攻撃」，「スパムメールや DoS 攻撃の中継利用等」及び「ホームページやファイル，データの改ざん」を含むことから，これら 2 つのトラブルは，性質が異なると判断した。その結果，「システムトラブル」は，「システムの停止」と「その他のシステムトラブル」の 2 つのリスクと見なすことにした。また，「コンピュータウィルス」については，大きく「ウィルスなどによる感染」と「トロイの木馬」に分けられているが，このうち「ウィルスなどによる感染」については，「USB 経由による感染」「スパムメール等による感染」「ホームページ等による感染」及び「標的型サイバー攻撃による感染」といったように感染経路別に回答数が示されており，各々の数も多いことから，感染経路別のリストを詳細項目として扱うことにした。

以上の考え方でまとめたトラブルとリスクの対応付けを表 18 に示す。

表 18　トラブルとリスクの対応付け

トラブルの種類(*1)		モデルで使用するリスク名
カテゴリ	詳細項目	
システムトラブル	－	－
システムの停止	内部要因によるシステムの停止 外部要因（地震，火災等の問題）によるシステムの停止	R_1
その他のシステムトラブル	DoS 攻撃 スパムメールや DoS 攻撃の中継利用等 ホームページやファイル、データの改ざん	R_2
不正アクセス	IP・メールアドレス詐称 リソースの不正使用 内部関係者による不正アクセス	R_3
コンピュータウィルス	USB 経由によるウィルスなどの感染 スパムメール等によるウィルスなどの感染 ホームページ等によるウィルスなどの感染 標的型サイバー攻撃によるウィルスなどの感染 その他の経路によるウィルスなどの感染 トロイの木馬	R_4
重要情報の漏えい	コンピュータウィルス､ファイル共有ソフトに起因する情報漏えい 不正アクセスによる情報漏えい 標的型サイバー攻撃による情報漏えい 内部者による情報漏えい 委託先による情報漏えい ノートパソコン及び携帯記憶媒体等の盗難・紛失	R_5
その他	ホームページ上での誹謗中傷等 その他	R_6

(*1) [40]のデータ
(注)表 2 は，詳細項目の内容を具体的リスクの例として示したものであり，内容的には本表と同等

リスクレベルの評価値の決定は，各トラブルの発生割合と重要性のレベルを評価し，各レベル値を設定，さらにそれらを総合評価することで算出した。トラブルの発生割合のレベル値の決定では，まず [40]の「集計表（概要)」の概表 5-1-1 を参照して，表 18 のトラブルの「詳細項目」単位で，当該トラブルが発生したと回答した企業数を，回答した企業数で割ることでトラブル発生割合を算出した。次に，算出結果を表 19 に示すように 5 段階にレベル分けした。

表 19　リスク（トラブル）の発生割合の算出

トラブルの種類(*1)		(I) 回答企業数（社）(*1)	(II) 発生した件数（社）(*2)	(I)/(II) トラブル発生割合(%)	レベル値 (*3)
カテゴリ	詳細項目				
システムトラブル	―	4782	―	―	―
システムの停止	内部要因によるシステムの停止		550	11.50	5
	外部要因（地震，火災等の問題）によるシステムの停止		128	2.68	2
その他のシステムトラブル	DoS 攻撃		65	1.36	1
	スパムメールや DoS 攻撃の中継利用等		90	1.88	1
	ホームページやファイル、データの改ざん		30	0.63	1
不正アクセス	IP・メールアドレス詐称		20	0.42	1
	リソースの不正使用		11	0.23	1
	内部関係者による不正アクセス		19	0.40	1
コンピュータウィルス	USB 経由によるウィルスなどの感染		345	7.21	4
	スパムメール等によるウィルスなどの感染		244	5.10	3
	ホームページ等によるウィルスなどの感染		203	4.25	3
	標的型サイバー攻撃によるウィルスなどの感染		29	0.61	1
	その他の経路によるウィルスなどの感染		136	2.84	2
	トロイの木馬		145	3.03	2
重要情報の漏えい	コンピュータウィルス、ファイル共有ソフトに起因する情報漏えい		3	0.06	1
	不正アクセスによる情報漏えい		9	0.19	1
	標的型サイバー攻撃による情報漏えい		4	0.08	1
	内部者による情報漏えい		34	0.71	1
	委託先による情報漏えい		29	0.61	1
	ノートパソコン及び携帯記憶媒体等の盗難・紛失		224	4.68	3
その他	ホームページ上での誹謗中傷等		28	0.59	1
	その他		34	0.71	1

(*1) 情報セキュリティトラブルの発生に関する問いに回答した企業数
(*2) 各トラブルが発生したと回答した企業
(*3) トラブル発生割合(%) = （ 発生したトラブル（ある）の件数 ／ 回答企業数 ）*100
(*4) 次の尺度で 5 段階にレベル分け：
2%未満→1，　2%以上 4%未満→2，　4%以上 6%未満→3，6%以上 8%未満→4，8%以上→5

次に，トラブルの重要性レベルは，[40]の「集計表（概要）」の概表 5-1-3 で示される「各企業のトラブルの重要性に対する認識」に関するデータを用いて設定した。このデータでは，各企業がトラブルの重要性について「非常に重要」「どちらかといえば重要」「重要ではない」「わからない」のいずれと考えているかを回答した結果が示されている。これを用いてトラブルの重要性をレベル分けするために，前

述の 4 つの回答に対して，表 20 のとおり重要性レベル値を割り当てた。さらに，各重要性レベル値と各回答企業数とから，重要性レベル値の平均値を求め，これを重要性レベル値とした。ここで，重要性レベル値は，トラブルの詳細項目単位で算出している。このとき小数点以下は四捨五入し，結果が整数値となるようにした。(表 21 参照)

表 20 トラブルの重要性に対する認識と重要性レベル値

トラブルの重要性に対する認識	非常に重要	どちらかといえば重要	重要ではない	わからない
重要性レベル値	5	3	1	0

表 21　トラブルの重要性レベルの設定（詳細項目単位）

トラブルの種類(*1)		トラブルの重要性に対する認識					重要レベル値 (*1)
カテゴリ	詳細項目	(I) 回答企業数(社)	(II) 非常に重要	(III) どちらかといえば重要	(IV) 重要ではない	(V) わからない	
システムトラブル	－	－	－	－	－	－	－
システムの停止	内部要因によるシステムの停止	4,735	4,050	590	42	53	5
	外部要因（地震，火災等の問題）によるシステムの停止	4,728	3,750	882	37	59	5
その他のシステムトラブル	DoS 攻撃	4,683	2,739	1,468	210	266	4
	スパムメールや DoS 攻撃の中継利用等	4,697	2,875	1,428	164	230	4
	ホームページやファイル、データの改ざん	4,706	3,228	1,205	139	134	4
不正アクセス	IP・メールアドレス詐称	4,707	3,093	1,318	157	139	4
	リソースの不正使用	4,696	2,966	1,371	170	189	4
	内部関係者による不正アクセス	4,710	3,456	1,050	100	104	4
コンピュータウィルス	USB 経由によるウィルスなどの感染	4,721	3,522	1,097	44	58	4
	スパムメール等によるウィルスなどの感染	4,717	3,345	1,220	70	82	4
	ホームページ等によるウィルスなどの感染	4,717	3,294	1,222	117	84	4
	標的型サイバー攻撃によるウィルスなどの感染	4,714	3,347	1,164	106	97	4
	その他の経路によるウィルスなどの感染	4,712	3,227	1,300	81	104	4
	トロイの木馬	4,701	3,165	1,317	90	129	4
重要情報の漏えい	コンピュータウィルス、ファイル共有ソフトに起因する情報漏えい	4,716	3,959	640	50	67	5
	不正アクセスによる情報漏えい	4,718	3,910	670	66	72	5
	標的型サイバー攻撃による情報漏えい	4,705	3,651	843	109	102	4
	内部者による情報漏えい	4,717	4,018	595	47	57	5
	委託先による情報漏えい	4,696	3,710	778	111	97	4
	ノートパソコン及び携帯記憶媒体等の盗難・紛失	4,709	3,689	866	88	66	4
その他	ホームページ上での誹謗中傷等	4,682	2,212	1,845	427	198	4
	その他	3,370	1,002	995	276	1,097	2

(*1) 重要性レベル値は，
表 20 のレベル値を用いて次の式で算出：

重要性レベル ＝(5*(II)+3*(III)+1*(IV)+0*(V)) / (I)

表 20 及び表 21 で算出した「トラブルの発生割合」と「トラブルの重要レベル値」に表 22 を適用することで，トラブルの詳細項目単位で，1～9 の 9 段階のリスク値を決定した。

表 22　リスク値の算出表

トラブルの重要レベル値＼トラブル発生割合	1	2	3	4	5
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8
5	5	6	7	8	9

尚，詳細項目単位で決定したリスク値のうち，トラブルの各カテゴリ内の最大値をとって，そのカテゴリのリスク値とした。各カテゴリは，表 18 において，モデルにおけるリスクと定義づけたので，これにより，モデルで使用するリスクのリスト及び各リスクのリスク値を決定できる（表 23 参照)。

表 23　トラブルに関するデータをもとに設定及び算出したリスクの一覧とリスク値

リスク名	トラブルの種類		トラブルの発生割合	トラブルの重要レベル値	リスク値(*1)	
	カテゴリ	詳細項目				
－	システムトラブル	－	－	－	－	－
R_1	システムの停止	内部要因によるシステムの停止	5	5	9	9
		外部要因（地震，火災等の問題）によるシステムの停止	2	5	6	
R_2	その他のシステムトラブル	DoS 攻撃	1	4	4	4
		スパムメールや DoS 攻撃の中継利用等	1	4	4	
		ホームページやファイル、データの改ざん	1	4	4	
R_3	不正アクセス	IP・メールアドレス詐称	1	4	4	4
		リソースの不正使用	1	4	4	
		内部関係者による不正アクセス	1	4	4	
R_4	コンピュータウィルス	USB 経由によるウィルスなどの感染	4	4	7	7
		スパムメール等によるウィルスなどの感染	3	4	6	
		ホームページ等によるウィルスなどの感染	3	4	6	
		標的型サイバー攻撃によるウィルスなどの感染	1	4	4	
		その他の経路によるウィルスなどの感染	2	4	5	
		トロイの木馬	2	4	5	
R_5	重要情報の漏えい	コンピュータウィルス、ファイル共有ソフトに起因する情報漏えい	1	5	5	6
		不正アクセスによる情報漏えい	1	5	5	
		標的型サイバー攻撃による情報漏えい	1	4	4	
		内部者による情報漏えい	1	5	5	
		委託先による情報漏えい	1	4	4	
		ノートパソコン及び携帯記憶媒体等の盗難・紛失	3	4	6	
R_6	その他	ホームページ上での誹謗中傷等	1	4	4	4
		その他	1	2	2	

(*1) リスク値の左列は，トラブルの詳細項目単位で 表 22 を適用してリスク値を算出した値。右列は，トラブルの詳細項目のリスク値のうち，カテゴリ内の最大値をとって，そのカテゴリのリスク値として設定した値。トラブルのカテゴリはモデルで使用するリスクに対照付く。

(2) 情報セキュリティ対策（リスクヘッジ策）のリスト

本検討においても，基本モデルと同様に，モデルでは表 6 のリスクヘッジ策のリストを使用することとする。一方，[40]では，概表 5-2-1-1「情報セキュリティの対策状況」において，情報セキュリティの対策のリストが示されているものの，これは「組織的対策」「技術的対策」「監視体制」「評価」という 4

つのカテゴリで整理されたリストとなっており，リスクヘッジ策とは別の構成となっている。モデルによる解を検証する際には，これら概表 5-2-1-1 の情報セキュリティの対策の対策状況を参照する必要がある，そこで，この情報セキュリティ対策と，モデルで使用するリスクヘッジ策との対応付けを行い表 24 の結果を得た。

表 24　情報セキュリティの対策とリスクヘッジ策の対照

[40]による情報セキュリティ対策の種類		リスクヘッジ策	対照する管理策，対照しない理由等
＜組織的対策の実施＞	リスク分析	－	ISMS マネジメントサイクルの活動であり，リスクヘッジ策には含まれない
	セキュリティポリシーの策定	H_1 (Clause 5)	5.1.1 と対照
	セキュリティポリシーに基づいた具体的な対策の検討	－	ISMS マネジメントサイクルの活動であり，リスクヘッジ策には含まれない
	情報セキュリティ報告書の作成	－	同上
	事業継続計画（BCP）の作成	H_{13} (Clause 17)	17.1.1 と対照
	全社的なセキュリティ管理者の配置	H_2 (Clause 6)	6.1.1 と対照
	部門ごとのセキュリティ管理者の配置	H_2 (Clause 6)	6.1.1 と対照
	従業員に対する情報セキュリティ教育	H_3 (Clause 7)	7.2.2 と対照
	取引（委託、外注を含む）相手における情報セキュリティ対策実施状況の確認	H_{11} (Clause 15)	15.2.1 及び 15.2.2 と対照
	内部統制の整備強化	H_{14} (Clause 18)	18.1.1 と対照
＜技術的対策の実施＞	重要なコンピュータ室への入退室管理	H_7 (Clause 11)	11.1.2 と対照
	重要なシステムへの内部でのアクセス管理	H_5 (Clause 9)	9.1.1，9.1.2，9.2.1～9.2.6，9.4.1～9.4.5 と対照
	データの暗号化（PKI を含む）	H_6 (Clause 10)	10.1.1～10.1.2 と対照
	クレジットカード情報の暗号化	H_6 (Clause 10)	同上
	個人情報の暗号化	H_6 (Clause 10)	同上
	外部接続へのファイアウォールの配置	H_9 (Clause 13)	13.1.1 と対照
	ISO/IEC15408 認証取得製品の導入	－	
	シンクライアントの導入	H_7 (Clause 11)	11.2.6 と対照
	生体認証の導入	H_5 (Clause 9)	9.4.1 と対照
	電子署名の導入	H_9，H_{10} (Clause 13, 14)	13.2.3，14.1.3 と対照
＜監視体制＞	セキュリティ監視ソフトの導入	H_{12} (Clause 16)	インシデントの管理とその改善を目的に監視は行われるため，H12 と対照すると判断。16.1.2～16.1.7 と対照
	外部専門家による常時セキュリティ監視	H_{12} (Clause 16)	同上
	情報セキュリティ対策ベンチマークの活用	－	
＜評価の実施＞	外部専門家による定期的なシステム監査	－	システム監査は，ISO/IEC 27002 に含まれない
	内部による定期的なシステム監査	－	同上
	外部専門家による定期的な情報セキュリティ監査	－	情報セキュリティ監査は ISMS マネジメントサイクルの活動であり，リスクヘッジ策には含まれない
	内部による定期的な情報セキュリティ監査	H_{14} (Clause 18)	18.1.1，18.2.1 と対照
	定期的なぜい弱性診断の実施	H_{12} (Clause 16)	12.1.1 と対照
	定期的なぜい弱性情報の取得	H_{12} (Clause 16)	同上
	定期的なアクセスログの分析	H_8 (Clause 12)	12.1.1 と対照
	情報セキュリティマネジメントシステム（ISO/IEC27001）認証の取得	－	ISMS 認証の取得は，ISO/IEC 27002 に含まれない
対応なし		H_4 (Clause 8)	
		H_{10} (Clause 14)	

(3) 各リスクヘッジ策の各情報セキュリティリスクに対する影響値

本検討においては，基本モデルとは，扱う情報セキュリティリスクのリストが異なるため，各リスクヘッジ策の各情報セキュリティリスクに対する影響値を改めて算出する必要が生じる。そこで，2.2(4)と同様の手順で影響値を算出し表 12 の値を得た。各影響値を算出した詳細結果は付録A(2)を参照せよ。

(4) 情報セキュリティ対策を実施するために必要な費用

各リスクヘッジ策を組織において実装する際にかかる費用を算出するために，各リスクヘッジ策の各情報セキュリティリスクに対する影響値算出の過程で得られた表 25 の数値を用いる。費用算出を単純化するために，ひとつの観点に相当する対策を実施するための費用は，管理策や観点の種類に因らず一定であると仮定した。例を用いて説明すると，5.1.1 の管理策は，人的対策も運用的対策も含むが，5.1.1 の人的対策実施に係る費用も，運用的対策にかかる費用も同じと見なすということである。さらには，別の管理策 8.2.2 は，物理的，技術的，人的，運用的すべての対策を含むものの，これらに係る費用もすべて同じであり，またそれらと 5.1.1 の各対策とも同一費用であると見なすということである。あるひとつの観点に相当する対策を実施するための費用を U とする。すると，表 25 の観点別の管理策数のリスクヘッジ策ごとの合計値を用いて，各リスクヘッジ策を組織において実装する際にかかる費用は U を用いて表現できる。例えば，H_1 に実装にかかる費用は 3U，H_2 に実装にかかる費用は 16U となる。

表 25　リスクヘッジ策に含まれる各観点の対策を含む管理策の数

リスクヘッジ策	物理的	技術的	人的	運用的	管理策延べ数計
H_1	0	0	1	2	3
H_2	2	2	5	7	16
H_3	0	0	5	4	9
H_4	5	5	4	10	24
H_5	5	13	1	14	33
H_6	0	2	0	2	4
H_7	15	8	2	15	40
H_8	3	10	3	14	30
H_9	2	4	3	7	16
H_{10}	3	9	4	13	29
H_{11}	0	0	3	5	8
H12	0	2	4	7	13
H13	2	2	1	4	9
H14	2	3	3	8	16
計	39	60	39	112	250

モデルが有効な解を導くようにするためには，組織の規模等に見合った U の値を設定することが肝要である。U の値を決めるために，ここでは，まず組織が情報セキュリティ対策に費やした総費用を参照することにした。なぜなら，そのような費用には，通常，組織の規模感などの状況が反映されているためである。

組織が情報セキュリティ対策に費やした総費用は，概表 5-2-3-1 の値を用いて算出した。概表 5-2-3-1 は，各企業が使用した情報セキュリティの対策費用を，金額によって 14 段階に分割，さらにそれに「わからない」「発生しなかった」の 2 項目を加えた 16 個の分類を作成し，各分類に属する回答した企業数を示している。このデータを用いて，実際にかかった情報セキュリティ対策費用の平均値を求め，それをある企業の情報セキュリティ対策の総費用とみなすこととした。

平均値は，各レンジに含まれる組織は，そのレンジの中間値をその組織の予算として持つと想定して算出した。表 26 のとおり，同じ対策費用のカテゴリの(I)中間値と(II)件数を用いて，情報セキュリティ対策費用の平均を求めると，834.22 万円という値を得た。

表 26　情報セキュリティ対策費用

情報セキュリティ対策費用	(I) 中間値	(II) 件数
50 万円未満	25 万円	978 社
50～100 万円	75 万円	532 社
100～150 万円	125 万円	288 社
150～200 万円	175 万円	179 社
200～400 万円	300 万円	283 社
400～600 万円	500 万円	171 社
600～800 万円	700 万円	66 社
800～1,000 万円	900 万円	89 社
1,000～1,500 万円	1,250 万円	108 社
1,500～2,000 万円	1,750 万円	53 社
2,000～3,000 万円	2,500 万円	73 社
3,000～5,000 万円	4,000 万円	66 社
5,000～1 億円	7,500 万円	63 社
1 億円以上	2 億円	67 社
わからない	－	1,070 社
発生しなかった	－	392 社
(III) 回答企業数（わからないと回答した企業を除く）		3408 社
情報セキュリティ対策費用の平均値（$\sum_1^{14}$(I)*(II) / (III) ）		834.22 万円

次に，この平均値から，U の値を導くことを検討する。この検討には，表 24 の対照表を用いた。 [40] の情報セキュリティ対策は，表 24 によれば 31 個ある。この中には，リスク分析やシステム監査など，

管理策には含まれない対策も含まれている。表 24 では，それらも特定されており，31 個中 9 個がそれにあたる。情報セキュリティ対策にかかる総費用は，834.22 万円であるが，このうち 9/31 は管理策の実施には該当しないため，該当しない分を減じることで，管理策に対照付く情報セキュリティ対策のみにかかる総費用を算出できると考えた。単純に，834.22 万円から 9/31 分の費用を減じて，592.03 万円という費用を得る。31 の情報セキュリティ対策に対照付けられる管理策は，表 24 によれば 35 個ある。すなわち，31 個の情報セキュリティ対策の実施により，113 個の管理策のうち，35 個を実施したと考えることができる。上で求めた 592.03 万円は，これら 35 個の管理策を実装するための総費用と考えられる。単純な比率の問題として捉えて，113 個すべての管理策実装にかかる費用として，1911.4 万円（= 592.303*113/35）を得る。すべての管理策実装にかかる費用は 250U であるから，U=76456 となる。U の値が得られたことで，表 25 とから，各リスクヘッジ策の実装にかかる費用が表 27 のとおり求められた。

表 27　各リスクヘッジ策実装いかかる費用

リスクヘッジ策	管理策実装にかかる費用	
	U を用いた表現	費用（円）
H_1	3U	229,368
H_2	16U	1,223,296
H_3	9U	688,104
H_4	24U	1,834,944
H_5	33U	2,523,048
H_6	4U	305,824
H_7	40U	3,058,240
H_8	30U	2,293,680
H_9	16U	1,223,296
H_{10}	29U	2,217,224
H_{11}	8U	611,648
H_{12}	13U	993,928
H_{13}	9U	688,104
H_{14}	16U	1,223,296
計	250U	229,368

以上により，モデルを使用するために必要なすべての要素がそろったことになる。

4.3 モデルの検証及び結果

4.2 で求めた要素からなるモデルを用いて解を導くためには，さらに情報セキュリティ対策のための組織の予算とリスク受容値の入力が必要である。情報セキュリティ対策のための組織の予算は，リスクヘッジ策を選択して実施する際にかかる費用の上限である。4.2(4)で算出した，組織が情報セキュリティ対策に費やした費用のうち，管理策に対照付く費用として算出した 592.03 万円は，組織の予算に近い値と

考えることができる。そこで，端数を切り上げ 600 万円を組織の予算とした。リスク受容値は，1～9 の 9 段階の値を順に入力し結果をみてみよう。

表 28 に，組織の予算として 600 万円を入力した場合に得られた解の一覧を示す。(I)でリスク受容値を 6 とした場合は，それを満たすために必要な組織の費用は 485 万円程度という結果になっている。そこで，(II)でリスク受容値を 5 とすると，組織の費用 600 万円を使ってそれを達成できるという結果が得られる。さらに(III)でリスク受容値 4 を入力すると，解が得られず，リスク受容値 4 を達成するには，組織の予算 600 万円では不十分であるということが分かる。

表 28　モデルが導いた解の一覧(1)

種別	項目		値		
			(I)	(II)	(III)
入力	リスク受容値		6	5	4
	情報セキュリティ対策に対する組織の予算		6000000	6000000	6000000
解	選定されたリスクヘッジ策実装にかかる費用		4857010	6000000	－
	リスクヘッジ策の選定結果（%）	H_1	0	0	－
		H_2	0	0	－
		H_3	0	100	－
		H_4	0	0	－
		H_5	100	64	－
		H_6	0	0	－
		H_7	31	0	－
		H_8	0	76	－
		H_9	0	0	－
		H_{10}	62	0	－
		H_{11}	0	45	－
		H_{12}	0	100	－
		H_{13}	0	100	－
		H_{14}	100	0	－

次に，600 万円の予算でリスク値 5 を達成することが組織にとって最適と言えるかどうかを検討してみよう。3.3(1)で示した，あるリスク受容値に対する組織の予算の最小値を導出する手法を用いて，表 29 の結果を得た。(IV)から(VII)の結果はいずれも，与えられた組織の予算をすべて費やしてリスク受容値 5 を達成している。しかし，同じリスク受容値を達成するのであれば，費用は少ないほど良いという一般的な考え方によれば，この中では(VII)が最適解となる。より正確に言うと，リスク受容値 5 を達成する最小費用は，540 万円より大きく 550 万円以下であることが分かる。従って，(VII)の結果をほぼ最適解と想定してよいと言えよう。このとき，リスクヘッジ策は，「H_1：情報セキュリティのための方針群（箇条 5)」が 100%，「H_2：情報セキュリティのための組織（箇条 6)」が 8%，「H_3：人的資源のセキュリティ（箇条 7)」が 100%，「H_5：アクセス制御（箇条 9)」が 71%，「H_8：運用のセキュリティ（箇条 12)」

が 17%,「H_{11} : 供給者関係（箇条 15)」が 100%,「H_{12} : 情報セキュリティインシデント管理（箇条 16)」が 100%，及び「H_{13} : 事業継続マネジメントにおける情報セキュリティの側面（箇条 17)」が 100%選択される。

ここで，表 29 の解を比較してみる。いずれもリスク受容値 5 を達成しているものの，リスクヘッジ策実装にかかる費用がそれぞれ異なっており，いずれも与えられた組織の予算を使い切る解となっている。リスクヘッジ策 H_3，H_5，H_{11}，H_{12} 及び H_{13} は，組織の予算値が変わっても同じか，ほとんど変わらない内容で選択されている。一方，H_1 は，組織の予算が減るごとに，選択割合が増加していき，反対に H_8 は，組織の予算が減るごとに，選択割合が減少する。このことは，このケースの場合には，H_1 と H_8 が，リスクレベルの修正に関して類似の効果をもつことを意味する。H_1 は，情報セキュリティに関する経営陣の方向性支持が，具体的な情報セキュリティ対策活動の中で展開され，従業員や関係者に確実に伝達されることを目的とした管理策を含むリスクヘッジ策である。ここで言う方針にはいろいろな階層があり，最上位のものは，組織全体の情報セキュリティの取り組みに関する方針であろうが，より低いレベルの方針としては，アクセス制御，情報分類，クリアデスク・クリアスクリーンのような特定のトピックスを対象とした個別方針がある。また，H_1 には，これら方針群のレビューも含まれる。H_8 は，情報セキュリティを保った運用を実現するための管理策を含むリスクヘッジ策である。操作手順書の作成と徹底，運用の変更管理，容量・能力の管理，開発環境，試験環境運用環境の分離，マルウェア対策，情報のバックアップ，ログ取得保護，ログの正確性担保のためのクロック同期など，運用に関わる各種具体的な対策が含まれている。いずれのリスクヘッジ策も対象となる対策の領域は広いところは共通しているとはいえ，H_1 が，方針やルールを作成し，それを従業員や関係者に周知することで情報セキュリティを実現しようとするのに対して，H_8 は，運用に関して，運用的人的観点のみでなくて，物理面技術面の具体的対策を実装することで実現しようとするものであると考えられる。

先に，一般的には，同じリスク受容値を達成するのであれば，費用は少ないほど良いと述べたが，組織の具体的な状況と照らすことで, 最小費用ではない解を選ぶ場合があってもよい。例えば, 表 29 では, (VII)の解の代わりに, 費用は 20 万円多くかかるが, (V)の解を選んでも良い。組織があまり大きくなく，きめ細かい方針の策定で，従業員などの活動が管理できるような場合には，最小費用の(VII)で十分と思われる。しかし、大きな組織がであって，管理者に対して運用担当者の割合が多いような業務形態の場合には，費用が少々余計にかかっても(V)を選択し，運用手順等の中に確実に情報セキュリティ対策の活動を埋め込む方が確実な場合がある。モデルの導く解は，リスク受容値に対する最小費用の場合の解が，最適解の最有力の候補には違いないが，近隣の解を比較することで，このように組織にとってより良い解を見つけることができる場合もある。いまの場合は，費用を少し増すことで，組織により良い解を得られる可能性を見ることができたが，別の場合として，リスク受容値を高くすることで費用を格段に節約でき，それが組織に適しているようなケースもあるかもしれない。

本モデルは，モデルが導く解を単純に受け入れるという使い方でだけではなくて，このように，入力値を変更して得られる複数の解を比較したり，組織の環境やリスクの状況と照らして，組織にとって最適なものを探すことに活用する使い方もできることに大きな利点がある。

表 29　モデルが導いた解の一覧(2)

種別	項目		値				
			(IV)	(V)	(VI)	(VII)	(VIII)
入力	リスク受容値		5	5	5	5	5
	情報セキュリティ対策に対する組織の予算		5800000	5700000	5600000	5500000	5400000
解	選定されたリスクヘッジ策実装にかかる費用		5800000	5700000	5600000	5500000	－
	リスクヘッジ策の選定結果（%）	H_1	0	14	68	100	－
		H_2	0	0	0	8	－
		H_3	100	100	100	100	－
		H_4	0	0	0	0	－
		H_5	66	67	68	71	－
		H_6	0	0	0	0	－
		H_7	0	0	0	0	－
		H_8	54	43	33	17	－
		H_9	0	0	0	0	－
		H_{10}	0	0	0	0	－
		H_{11}	85	100	100	100	－
		H_{12}	100	100	100	100	－
		H_{13}	100	100	100	100	－
		H_{14}	0	0	0	0	－

「H_1：情報セキュリティのための方針群（箇条 5)」には [40]の概表 5-2-1-1 の対策「セキュリティポリシーの策定」に対応することは先に述べた（表 24 参照)。この対策は，概表 5-2-1-1 を参照すると 37.6%の企業で既に実施されており，実施しているかしていないかを別にすると，90%を超える企業が必要性を認識している（表 30 の概表 5-2-1-1 の該当部分の抜粋を参照)。一方で，H_1 はいわゆる組織のトップレベルの情報セキュリティポリシーについてだけ述べているのではなくて，個別方針レベルに対する対応も含んでいる。すなわち，リスクアセスメントの結果，組織が管理対象とすることを決定したリスクについて，運用的かつ人的観点の対策を，方針をもって進めることを確実にすることを意味する。先にも述べたとおり，対策費用を最小化するためには，このリスクヘッジ策を 100%採用することがモデルにより提案されていると考えられるが，これは妥当と言えるであろう。なぜならば，H_1 は，いずれのリスクへの対応も，運用的人的対策についてはカバーする内容となっているためである。

表 30 「セキュリティポリシーの策定」の実施状況（ [40]の概表 5-2-1-1 の抜粋）と必要性の認識度

項目		対策の実施状況											
		(I)	(II)		(III)		(IV)		(V)		((II)+(III)+(IV)+(V))/(I)	
		対策の実施状況・回答企業数（社）※3	既に実施している		実施を検討している		必要性を感じるが、未実施		必要性を感じず、未実施		必要性を感じる（対策済み，検討中，未実施）	
対策の種類			件数(社)	構成比(%)	件数(社)	構成比(%)	件数(社)	構成比(%)	件数(社)	構成比(%)	件数(社)	構成比(%)
＜組織的対策＞	リスク分析	4,311	1,621	37.6	671	15.6	1,606	37.3	413	9.6	3,898	90.4
	セキュリティポリシーの策定	4,356	2,295	52.7	581	13.3	1,150	26.4	330	7.6	4,026	92.4
	・・・											
・・・以降略・・・												

「H_2：情報セキュリティのための組織（箇条 6)」は，表 29 の(IV)までは選択されず，(VII)で初めて 8%選択されている。この結果は，H_8 の運用への情報セキュリティの具体的な実装の度合いが下がり，H_1 の方針作成が充実化することに伴い，組織体制の在り方を充実させることで，具体的な実装が軽減されることをカバーしているように考えられる。実際，H_2 には情報セキュリティの役割及び責任の設定や職務の分離などが含まれている。H_1 で作成した方針を周知するにあたり，各員の情報セキュリティの役割責任の明示が行われれば，方針に沿った活動の確実な実施を強化できるため，運用への実装が具体的でない場合にも，それに代わる効果を見込めると考えられる。このように考えると，(VII)で H_8 が選択されたことは，意味があると結論付けられる。

「H_3：人的資源のセキュリティ（箇条 7)」は，従業員や契約者の雇用前の選考や雇用条件について，雇用期間中は，情報セキュリティに対する意識向上や教育・訓練の実施，違反に伴う懲戒手続などを含む。概表 5-1-1 の情報セキュリティトラブル発生状況を見ると，システムの停止は，外部要因よりも内部要因によるものの方が圧倒的に多いこと，発生した不正アクセスの半数近くが内部関係者によるものであること，重要情報の漏えい発生の理由は，内部者委託者による情報漏えいとノートパソコン携帯記憶媒体等の盗難・紛失がほとんどであることなど，内部関係者が関係するトラブルの割合の多さが見て取れる（表 31 の概表 5-1-1 の抜粋を参照)。このようなリスクの状況から，H_3 を充実して実施することは理解しやすい対応と考えられる。

表 31　情報セキュリティトラブルの発生状況（ [40]の概表 5-1-1 の抜粋）

トラブルの種類		発生件数（件）
システムの停止	内部要因によるシステムの停止	550
	外部要因（地震、火災等の問題）によるシステムの停止	128
不正アクセス	IP・メールアドレス詐称	20
	リソースの不正使用	11
	内部関係者による不正アクセス	19
重要情報の漏えい	コンピュータウィルス、ファイル共有ソフトに起因する情報漏えい	3
	不正アクセスによる情報漏えい	9
	標的型サイバー攻撃による情報漏えい	4
	内部者による情報漏えい	34
	委託先による情報漏えい	29
	ノートパソコン及び携帯記憶媒体等の盗難・紛失	224

「H_5：アクセス制御（箇条 9)」には，ネットワークネットワークサービスへのアクセス制御，システムアプリケーションのアクセス制御，利用者のアクセス権管理利用者の責任といった対策が含まれる。概表 5-1-1 によれば，不正アクセスそのものの件数は限られているものの，「ホームページやファイル、データの改ざん」や「不正アクセスによる情報漏えい」など，不正アクセスはその他のトラブルの前提となるとも考えられる。また，外部者によるものだけでなくて，内部者や契約者によるものも有り得るであろう。71%の選択結果は，このように，対象リスクが多いことを考えると理解できる。

「H_8：運用のセキュリティ（箇条 12)」は，具体的な情報セキュリティを運用に実装する各種対策を含むリスクヘッジ策である。特定されたリスクへ対応するために，運用への実装は欠かせないが，先に述べたとおり，方針の充実化と関係者への周知などで代替えすることもあり得る。17%の選択結果は，方針作成の方にウェイトをおいた解と考えられる。

「H_{11}：供給者関係（箇条 15)」における供給者とは，IT サービス，物流サービス，金融サービス，IT 基盤の構成要素などの供給者を意味する。また，サービス及び製品の ICT サプライチェーンの供給者も意味する。一般に，企業はいくつもの供給者をもつため，それに関するリスクヘッジ策が 100%選択されることは理解しやすい。

「H_{12}：情報セキュリティインシデント管理（箇条 16)」が 100%選択されている。概表 5-1-1 のトラブルのうち，インシデント管理で対応すべきものは「DoS 攻撃」「スパムメールや DoS 攻撃の中継利用等」「ホームページやファイル，データの改ざん」といったシステムトラブル，コンピュータウィルスなどであり，これらの発生件数が非常に多いため，H_{12} が 100%選択されたことは納得的である。

「H_{13}：事業継続マネジメントにおける情報セキュリティの側面（箇条 17)」は，困難な状況においても，情報セキュリティ及び情報セキュリティマネジメントを継続できるように，情報セキュリティ継続を事業継続に組みこむための各種対策を含む。概表 5-1-1 によると「外的要因によるシステム停止」は 128 件発生しており，「内部要因によるシステム停止」「各種ウィルスなどの感染」「ノートパソコン及び携帯記憶媒体等の盗難・紛失」に次ぐ多さである。また，このリスクは，発生可能性は低いものの，発生した場合にはその影響が大きいため，リスクの重要度レベルは高い。その結果，リスク値も高くなる。こうしたことから，H_{13} は 100%選択されたと考えられる。

4.4 検証結果のまとめ

統計データは，実際の企業で想定されるリスクや予算とは違い，複数企業のデータを基に平均値などをとって算出した値であるため，モデルの解の有効性や妥当性を検討することは難しい。しかし，3 章では，リスク値やリスクヘッジ策実装にかかる費用を，特別な根拠なく作成したものを用いてモデルを検証したのに比べ，平均値などを用いたとはいえ，実在する数値を用いてモデルの解を導けたことには意味があると言えるであろう。また，いわゆるリスクアセスメント結果が得られていない場合に，類似の情報からモデルが必要とする要素を作成する方法についても示せた。具体的には，リスクアセスメント結果（情報セキュリティリスクのリスト及びリスク値）を推定する方法，影響値算出に用いた観点を活用した各リスクヘッジ策の実施に係る費用の推定方法，及び組織の予算の推定方法を，実際のデータを用いて，具体例を以って示した。

また，入力値である組織の予算やリスク受容値をさまざまに変えて入力し，その解を比較し，結果の意味を考察することで，組織にとっての最適解をみつけるアプローチの取り方についても，統計データの検討の中で見つけることができたことは，このモデルの有用性を示していると言えよう。ここでは，あるリスク受容値に対し，最小費用となる解が必ずしも最適ではないというアプローチ方法を得た。例えば，費用が少し余計にかかったとしても，組織にとって，より効果のある対策が選択されている解を，その組織の最適解とするという場合があることが分かった。また，本モデルは，そのような解の候補を示せること，組織はそれらの中から，自組織に合ったものを選択できることを示せた。

しかしながら，先にも述べたとおり，検証で用いたリスク及びリスク値と，リスクヘッジ策と紐付いた対策の発生件数の間には，直接的なつながりはないし，同一調査の中の結果を用いてはいるとはいえ，リスクレベル決定において参照した回答企業群とリスクの発生件数決定において参照した回答企業群とは，重複しているものもあるであろうが，同じものとはいえない。このことは，モデルの解の妥当性及び有効性の検討にも影響すると思われる。従って，5 章では，実在する組織のデータを用いて検討を進める。

5　実データによるモデルの検証

5.1 実データの概要

本章では，実在する組織において実施された情報セキュリティリスクマネジメントのデータを用いてモデルを検証する。本章で用いるデータは，ある組織（A 社とする）の 1 部門が，ISMS 認証取得をめざした際に実施した情報セキュリティリスクマネジメントに関するものである。この取り組みでは，リスクアセスメント及びリスク対応は表 32 に示すとおり ISO/IEC 27001 [2]で規定されるプロセスに沿った内容で実施された。また，その結果として，表 36 及び表 37 のアウトプットが得られた。本検討では，これらのアウトプットを基に，モデルが必要とする各種データを作成，インプットし，それによって得られるモデル適用の結果を，実際の管理策選択結果やリスク受容基準と比較することで，モデルの有効性を検証した。モデルがインプットとして必要な値を，与えられたアウトプットからどのように算出したかについては 5.2 で示す。

尚，本活動の具体的な内容は，A 社において一般には開示していない情報のため，本稿では具体的な内容を示さず，結果だけを記すものとする。

表 32　実施されたプロセスと ISO/IEC 27001 要求事項の対照及びアウトプット

#	ISO/IEC 27001 の要求事項	実施されたプロセス	アウトプット
1	情報セキュリティリスクアセスメントプロセスの決定（6.1.2）	・リスクアセスメント手順の作成	・リスク評価・リスク管理手順書 ・リスクアセスメント結果
1-1	リスク基準の確立・維持	・リスク評価基準の作成 ・リスク受容基準の作成	
1-2	情報セキュリティリスクの特定	・情報資産の特定 ・脅威及びぜい弱性の特定 ・上記に基づくリスクの特定	
1-3	情報セキュリティリスクの分析・評価	・情報資産の価値評価 ・脅威及びぜい弱性の特定及び評価 ・リスク値の算出	
2	情報セキュリティリスク対応プロセスの決定（6.1.3）	・リスク対応手順の作成	・リスク評価・リスク管理手順書
2-1	情報セキュリティリスク対応の選択肢の選定及び管理策の決定	・管理策選択方針の作成 ・管理策の選択 ・残留リスクの受容	・管理策選択方針 ・リスク管理結果 ・残留リスクサマリ
2-2	リスク対応計画の作成	・リスク対応計画の作成	・リスク対応計画

5.2 実データのモデルの各要素への対照

(1)　情報セキュリティリスクのリスト及び各リスクレベルの評価値

A 社の取り組みでは，情報セキュリティリスクは，情報資産に対する脅威を特定するという立場から

特定された。脅威は，脅威の要因（偶発的又は故意的）と，脅威の実施者（内部者，外部者（契約者又はそれ以外），又は人以外）とに分類され，それぞれに該当するものがあるかどうかが検討された。該当する脅威があると判断された場合には，その情報資産とその脅威の組み合わせをひとつのリスクとして見なして，そのリスクに対して，相対的に 10 段階のランク分けが施され，リスク値が決定された。

一方，基本モデルにおけるリスクは，エージェントと動機という 2 つの観点からカテゴライズされた 7 個のリスクである。エージェントとしては，内部者，契約者，外部者，又は人以外を想定している。また，動機としては意図的なものと意図しない偶発的なものとしており，A 社の脅威分類とほぼ一致している。このため，資産と脅威の組み合わせで特定された A 社のリスク群を，脅威分類を用いてグループ分けし，各リスクグループをひとつのリスクと見なした（表 33 参照)。つまり，各々リスクとして見なされることになったリスクグループには，脅威の要因と実施者を同じくする情報資産がすべて含まれる。

一方，相対的な 10 段階のリスク値は，情報資産単位で割り当てられているおり，各リスクグループには，それに含まれる情報資産の数だけリスク値が割り当てられている。各リスクグループを 1 つのリスクとみなしてモデルのインプットとするためには，リスクグループに対して 1 つのリスクレベルを決める必要がある。そこで，単純に，グループに含まれるリスク値の最大値を，そのリスクグループのリスク値とみなすことにした。その結果として，表 33 のリスク値を得た。

表 33　A 社の保有する情報セキュリティリスクのリスト

リスク（リスクグループ）	内容	リスク値
R_1	内部者の故意によるリスク	8
R_2	契約者の故意によるリスク	9
R_3	外部者の故意によるリスク	8
R_4	内部者の意図しない行為によるリスク	9
R_5	契約者の意図しない行為によるリス	9
R_6	外部者の意図しない行為によるリス	9
R_7	人以外の原因によるリスク	8

表 34　リスクグループ（1 つのリスクとみなす）のリスク値の決定例

リスク（リスクグループ）	対象情報資産(*1)			リスク値
	#	資産名	リスク値(*2)	
R_1	1	顧客情報（データ）	7	8(*3)
	2	顧客情報（紙）	7	
		・・・中略・・・		
	7	基準書（紙）	8	
	8	基準書（2）（データ）	3	
	9	手順書（データ）	4	
		・・・以降略・・・		

(*1) R_1のリスクを保有する情報資産の一覧。
(*2) R_1に対するリスク値
(*3) R_1の対象情報資産のR_1に対するリスク値の最大値

(2) 情報セキュリティ対策（リスクヘッジ策）のリスト

A 社のリスク対応の取り組みにおいては，ISO/IEC 27002 [7]の管理策の選択が行われた。このことから，情報セキュリティ対策のリストは，基本モデルと同じ表 6 のリスクヘッジ策のリストを使用することとした。ただし，A 社の管理策は ISO/IEC 27002 [7]の 2005 年版相当のものであるため，現行版（2014 年版）の管理策との対応付けが必要になった（付録 C 参照）。

(3) 各リスクヘッジ策の各情報セキュリティリスクに対する影響値

情報セキュリティリスクのリスト及び情報セキュリティ対策（リスクヘッジ策）のリストとも，基本モデルと同じリストを適用するため，影響値についても基本モデルと同じ値を使用した。

(4) リスクヘッジ策を実施するために必要な費用

リスクヘッジ策を，組織において実装する際にかかる費用の算出は，統計データの検証で用いた，各リスクヘッジ策が含む 4 つの観点毎の管理策数（表 25 参照）の情報と，実際にかかった費用をもとに実施した。A 社は ISMS 認証取得を目指していたことから，要求事項の内容の組織内ルール化とそれに基づく運用の実装を行っていた。その活動を進める中で，ISO/IEC 27002 [7]の管理策のうち，運用的観点に相当するものについては，ほぼ全て実装していた。また，ルール作成及びその運用への実装にかかった費用は，その活動内容から人件費を含めておよそ 670 万円と見積もられた。一方，表 25 を見ると，運用的対策を含む管理策の合計数は 112 である。運用的対策全てにかかった費用を約 670 万円と見なすことで，U を約 6 万円（≒670 万円÷112）と想定することができる。この U は運用的対策に基づき算出したもであるものの，今回は，前述のとおり，他の観点の対策でも同じ一律の値を使用した。これにより表 35 の値を得た。

表 35　各リスクヘッジ策実施にかかる費用（A 社の場合）

リスクヘッジ策	対策数計	費用（円）
H_1	3	180,000
H_2	16	960,000
H_3	9	540,000
H_4	24	1,440,000
H_5	33	1,980,000
H_6	4	240,000
H_7	40	2,400,000
H_8	30	1,800,000
H_9	16	960,000
H_{10}	29	1,740,000
H_{11}	8	480,000
H_{12}	13	780,000
H_{13}	9	540,000
H_{14}	16	960,000
計	250	180,000

5.3 モデルの検証及び結果

5.2 では，モデルが使用する各種固定値を算出した。これらに加えて，モデルを用いて結果を算出するためには，リスクヘッジ策実施のための組織の予算（費用の上限値）及びリスク受容基準を入力する必要がある。A 社の実際の取り組みから，これらの値を決定する。まず，リスクヘッジ策実施のための組織の予算としては，実際にかかった費用を予算として設定することにする。5.2(4)で記したとおり，運用的対策の実施費用は 670 万円であった。これにその他の観点の対策を加えると，実際にかかった費用は 700 万円程度になった。そこで，組織の予算を 700 万円とした。リスク受容基準は，A 社においてはリスク値 7 と設定したため，これを初期値とした。ただし，リスク値については，組織の予算 700 万円に対して解が得られる値まで，順次減らして入力し解を求めた。

表 36 に得られた解の一覧を示す。これを見ると，(I)の結果から，A 社が定めたリスク受容基準 8 と組織の予算 700 万円は，釣り合っていないことが分かる。リスク受容基準 7 を達成するためには，320 万円強の費用で十分であるという結果になっている。そして，結果(III)及び(IV)に因れば，700 万円の予算で，リスク受容基準 5 まで達成できることが分かる。このような実際の結果との差が発生した原因は，A 社が管理策を選択した方法にあったと考えられる。すなわち，ひとつには，リスク対応において管理策を選択する際に，A 社は，リスク評価結果に基づいた選択を行う一方で，組織に情報セキュリティのマネジメントを実装する観点で，リスク結果には直接基づかずに「箇条 5 情報セキュリティのための方針群（H_1 に相当）」「箇条 6 情報セキュリティのための組織（H_2 に相当）」「箇条 7 人的資源のセキュリティ（H_3 に相当）」「箇条 8 資産の管理（H_4 に相当）」「箇条 16 情報セキュリティインシデント管理（H_{12} に相当）」「箇条 17 事業継続マネジメントにおける情報セキュリティの側面（H_{13} に相当）」「箇条 18 順

守（H_{14}に相当）」といった箇条に含まれる多くの管理策を全て選択している。また，ふたつめとして，リスク評価結果に基づく選択についても，当該リスクに関係のある対策が記述された管理策は全て選択する手法をとっており，リスク低減度合に応じた必要十分な選択を行っていない。その結果，ほぼ全ての管理策が選択された。さらに，認証取得を目指す短期的な取り組みの中では，物理的対策や技術的対策の実施が難しいことから，運用的対策の実施が中心となった。こうした状況から，予算の多くは，管理策の運用的対策を実施することに費やされることになった。また，物理的対策や技術的対策の実装を含む，短期で実施できない対策は，短期対応では行わず，中期的に実施を検討するという判断により，リスク低減が難しい状況が発生し，その結果，リスク受容基準も高い数値である 8 とする状況になったと考えられる。

表 36　モデルの算出した解の一覧（A 社の場合）(1)

種別	項目		値			
			(I)	(II)	(III)	(IV)
入力	リスク受容値		7	6	5	4
	情報セキュリティ対策に対する組織の予算		7000000	7000000	7000000	7000000
解	選定されたリスクヘッジ策実装にかかる費用		3213943	4803725	6411374	－
	リスクヘッジ策の選定結果（%）	H_1	0	0	0	－
		H_2	0	100	100	－
		H_3	28	24	0	－
		H_4	100	100	100	－
		H_5	25	26	32	－
		H_6	100	100	100	－
		H_7	0	0	0	－
		H_8	6	12	54	－
		H_9	0	0	34	－
		H_{10}	0	0	23	－
		H_{11}	33	69	100	－
		H_{12}	0	0	0	－
		H_{13}	0	0	0	－
		H_{14}	64	100	100	－

モデルを適用すると，700 万円の予算に対して，受容リスク値を 5 とすることができることが分かる。この場合にも，選定されたリスクヘッジ策を実装するためにかかる費用を算出すると 640 万円程度となり，700 万円の予算は十分すぎるという結果になっている。

そこで，次に，受容リスク値 5 に対して，最小となる組織の予算をさがす。統計データの検証の場合と同様に，3.3(2)の手法を用いると，表 37 の結果を得た。同じリスク受容値を達成するのであれば，費用は少ないほど良いという一般的な考え方によれば，リスク受容値 5 を達成する費用は，630 万円より大きく 640 万円以下であることが分かった。すなわち，(VI)の結果をほぼ最適解と想定してよいと言える。このとき，リスクヘッジ策は，「H_2：情報セキュリティのための組織（箇条 6）」が 100%，「H_4：資

産の管理（箇条 8)」が 100%,「H_5 : アクセス制御（箇条 9)」が 34%,「H_6 : 暗号（箇条 10)」が 100%,「H_8 : 運用のセキュリティ（箇条 12)」が 44%,「H_9 : 通信のセキュリティ（箇条 13)」が 8%,「H_{10} : システムの取得，開発保守（箇条 14)」が 50%,「H_{11} : 供給者関係（箇条 15)」が 79%,「H_{14} : 順守（箇条 18)」が 100%選択される。

表 37　モデルの算出した解の一覧（A 社の場合）(2)

種別	項目		値		
			(V)	(VI)	(VII)
入力	リスク受容値		5	5	5
	情報セキュリティ対策に対する組織の予算		6500000	6400000	6300000
解	選定されたリスクヘッジ策実装にかかる費用		6411373	6400000	－
	リスクヘッジ策の選定結果（%）	H_1	0	0	－
		H_2	100	100	－
		H_3	0	0	－
		H_4	100	100	－
		H_5	32	34	－
		H_6	100	100	－
		H_7	0	0	－
		H_8	54	44	－
		H_9	34	8	－
		H_{10}	23	50	－
		H_{11}	100	79	－
		H_{12}	0	0	－
		H_{13}	0	0	－
		H_{14}	100	100	－

上記の結果を受けて，次に，選択されたリスクヘッジ策それぞれについて，組織の状況や特定されたリスクの状況を参照することで，その選択が妥当であるかどうかを検討してみよう。妥当であることが確認できれば，モデルを実データに適用した場合に，意味のある解を導いたと見なせるであろう。

「H_2 : 情報セキュリティのための組織（箇条 6)」は，情報セキュリティの役割及び責任，職務の分離，プロジェクトマネジメントにおける情報セキュリティの他，関係当局及び専門組織との連絡など，組織内の情報セキュリティの実施及び運用を統制するための管理上の枠組みの確立に関する管理策が含まれている。A 社のリスク評価結果を見ると，ぜい弱性の評価において管理面の対策が存在しない，あるいは不十分であるとする記述が多くみられる。H_2 に含まれる，管理上の枠組みの確立に関する管理策は，こうしたリスクの低減に寄与する。こうした状況から，H_2 が 100%選択されることによるリスクの低減効果は大きいと想定できる。

「H_4：資産の管理（箇条 8)」には，資産目録の作成，資産の管理責任の明確化，利用範囲の決定，返却手続など資産の取り扱いに関する管理策，情報の分類とラベル付けに関する管理策，及び媒体の取り扱いに関する管理策が含まれる。A 社は，情報セキュリティリスクアセスメントを資産ベースで実施しており，資産を起点にリスクを想定し，その対応を検討しているため，このリスクヘッジ策に含まれる資産の管理に関する管理策は，リスク低減に大きく貢献すると考えられる。媒体に関するリスクも数は少ないとはいえ，記録媒体や入退館カードなどに対するリスクランクはいずれも高く，対策の必要性が感じられる。従って，100%選択されたことは，A 社のリスク対応の方向性に沿った結果であると考える。

「H_5：アクセス制御（箇条 9)」は，ネットワーク及びネットワークサービスへのアクセス制御のルール化及び実装，利用者のアクセス管理に関するもの，システムやアプリケーションのアクセス管理に関するもの，及び利用者の責任に関する管理策を含む。A 社の当該部門の業務は，社内及びグループ会社への，外部接続を含む通信，及び通信上の各種サービスの提供であるため，アクセス制御は，情報セキュリティ対策の中でも中心的対策のひとつと考えられる。また，リスクアセスメントの結果をみると，既にアクセス管理をしていることが分かる。加えて，社内規則，運用マニュアル及び手順書も既に存在することが分かる。これらのことから，A 社では，既にアクセス制御に関してある程度の対策を実施していると想定できる。一方で，リスクアセスメントの結果は，契約者又は外部者による不正アクセスで，高いリスク値をもつものが存在することを示している。ただし，全体のリスクから見てその数は多くない。従って，アクセス制御はすでに対策されているものの，追加対策が必要であるが，残留リスクからみてそれほど多くは無いと考えられる。H_5 が 34%選択されたことは，妥当に見える。

「H_6：暗号（箇条 10)」は，管理策として暗号による管理策の実装と鍵管理の確実な実装を含む。包含する管理策の内容が少ないことから，暗号化適用が必要な場合には，100%選択されることは自然である。A 社の場合には，外部者による機密性侵害において，リスクランクが 8 以上に相当するものが複数あるため，それらに対して暗号化対策をとるか検討することは容易に想定できる。

「H_8：運用のセキュリティ（箇条 12)」には，情報セキュリティを保った運用を実現するための管理策として，操作手順書の作成と徹底，運用の変更管理，容量・能力の管理，並びに開発環境，試験環境及び運用環境の分離といった内容のものが含まれる。また，その他にも，マルウェアに対する管理策，情報のバックアップに関するもの，ログ取得及び保護に関するもの，ログの正確性担保のためのクロック同期に関するもの，運用システムに関わるソフトウェアの導入に関するもの，技術的ぜい弱性管理に関するもの，さらに情報システムの監査に対する管理策など，運用に関わる管理策が数多く含まれる。A 社のリスクアセスメント結果を見ると，既にバックアップを多くの情報に対して実施していることや，社内規則，運用マニュアル及び手順書類が存在することが分かる。また，マルウェアに対する管理策の一環として，バージョンアップ及びパッチの適用などが実施されている。すなわち，A 社では，既に運用のセキュリティに相当する対策をいくつも実施していることがわかる。一方で，リスクアセスメントの結果を見ると，運用マニュアルや手順などの内容に不足があることが多くのリスクで認識されている。こうした状況から，H_8 の選択が 44%であることは，A 社にとって妥当な内容であると考えられよう。

「H_9：通信のセキュリティ（箇条 13)」は，ネットワーク上の情報やネットワークを支える情報処理施設の保護を確実にするための管理策を含む。すなわち，ネットワークサービスにおける情報セキュリティの要求事項の特定やネットワークの分離，情報転送に係る方針や手順，転送に関する合意，電子的メッセージ通信の保護，秘密保持契約又は守秘義務契約などが含まれる。A 社では，リスクアセスメントの結果から，技術的な対策としてはアクセス管理の実施や，ファイアウールの導入，ID・パスワード管理などが既に実施されている。さらにネットワーク経由でのリスクのレベルは，あまり高くない。従って，リスク受容値が 5 である場合に，管理の対象となるリスクの数も限られる。こうした状況からみて，H_9 の選択が 9%であることは，妥当な内容と考えられる。

「H_{10} : システムの取得，開発及び保守（箇条 14)」は，情報セキュリティ要求事項の分析及び仕様化，公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮，アプリケーションサービスのトランザクションの保護といった管理策を含む。また，情報システム開発の中で，情報セキュリティを確実に設計し，実施することに関する管理策，試験データの保護に関する管理策も含む。一方，ISMS 認証取得を目指す部門の適用宣言書をみると，A 社の当該部門の業務は，社内及びグループ会社への，外部接続を含むネットワーク接続，及びネットワークサービスの提供であり，そこで使用する情報システム運用が主たる業務である。情報システムの開発及び保守などは別部門の業務となる。当該部門が，システムの取得，開発及び保守に関して関わるのは，主に情報システムの受け入れにおいてだけである。一方，システムの取得や開発が開発部門主導で行われ，取得や開発時点での直接の関与ができないことから，運用側にとってシステムの受け入れ時の確認は通常より重要な意味合いを持つ。このような状況を考慮すると，対象範囲は限定的だが，そこでの対応は充実させる必要があるため，H_{10} が 50%選択されたことは，A 社の状況に即した内容であると見なせる。

「H_{11}：供給者関係（箇条 15)」は，各種供給者から，組織の資産を確実に保護することを目的とした管理策を含む。すなわち，供給者との関係に関する情報セキュリティの方針の策定，供給者との合意や ICT サプライチェーンの中でのセキュリティの取扱い，供給者のサービス提供の管理に関する管理策を含む。A 社の場合をみると，当該部門は，業務を遂行する上で，多くの組織との連携を必要としていることが分かる。例えば，運用に用いられる情報システムの開発・保守は別部門あるいは別組織で行われるため，運用を考慮したハードウェアの選定，セキュリティ要件の作りこみなどの実現には，供給者との密な連携が欠かせない。一方で，リスクアセスメントの結果から，アクセス状況の管理など一部対応している内容も見られる。ただし，供給者との合意など主たる対応内容については確認できない。こうした状況を考慮すると，H_{11} が 100%選択されたことは，A 社の状況に沿っていると考えられる。

「H_{14}：順守（箇条 18)」は，法的及び契約上の要求事項の順守及び情報セキュリティのレビューに関する管理策を含む。A 社は，社内及びグループ会社への通信及び通信環環境における各種サービスの提供を業務とするため，供給者だけでなく，社内及び関連会社とのさまざまな契約及び／又は合意を保持する。このような状況では，契約上の要求事項に違反があった場合の影響は大きく，確実な順守は欠かせない。従って，H_{14} が 100%選択されたことも A 社にとっては妥当な内容と言える。

以上の検討をまとめると，モデル適用により選択されたリスクヘッジ策は，A 社の当該部門が実際に実施した管理策とは内容が異なる結果となったとはいえ，A 社で行われたリスクアセスメントの結果と，モデルが示した解を比較すると，モデルの解は A 社の状況に沿った内容を示していることが見て取れる。

5.4 検証結果のまとめ

5 章では，ある組織が ISMS 認証取得の取り組みの中で実施した情報セキュリティリスクアセスメント及びリスク対応の記録を参照し，モデルの要素に合うように修正は加えたものの，実際のデータをモデルに適用することで解を導くことができた。

モデルが導いた結果は，組織が実際に選択したリスク対応結果とは隔たりがあるものであったが，なぜ差分が発生したかを検討することで，組織のリスク対応において望ましくなかった点や，なぜそのようなことが発生したかをつきとめることができた。また，モデルの適用により，組織にとってより良い対応，すなわち，組織にとってより適切な情報セキュリティ対策のための予算や，より適切なリスク受容値を導けることを示せた。また，このことをとおして，本モデルが実データに対して意味のある解を導くことを確認できた。

さらには，与えられた実データを用いて，各リスクヘッジ策実装にかかる費用を算出した。この算出には，表 38 の ISO/IEC27002 [2]の 114 の管理策に，物理的，技術的，人的及び運用的 4 つの観点をあてて 250 個の具体的対策としたものを用いた。これは，算出方法の 1 例にすぎないが，表 39 を用いることが，各リスクヘッジ策実装にかかる費用の算出いおいて有効であることを示せたとはいえよう。

6　結論

6.1 本研究で得られた結果

本研究では，情報セキュリティリスクマネジメントのプロセスのうち，情報セキュリティリスク対応に焦点をあて，その実施に伴う組織の意思決定支援を目的としたモデルを提案した。本モデルは，次の要素をもつ：

a) 情報セキュリティリスクのリスト，及び各リスクレベルの評価値
b) 情報セキュリティ対策のリスト，及び各対策を実施するために必要な費用
c) 各情報セキュリティ対策の各情報セキュリティリスクに対する影響値
d) リスク受容値，及び
e) 情報セキュリティ対策に対する組織の予算（費用の上限）

a)～c)は本モデルが解を導くために必要であり，本モデルにおいては固定値として扱われる。d)及び e)は本モデルの入力値である。これらの値を入力し，本モデルを実行することで次の解が示される。
本モデルの示す解：
・各リスクヘッジ策（H_i，i=1～14）の適用率適用率（P_i：$0 \leqq P_i \leqq 100$，単位%）
・選択されたリスクヘッジ策実装にかかる費用

本研究では，まず a)～c)の作成方法について示した。

a)のリスク一覧に含まれるリスクの数は，本モデルでは 10 程度とした。これは，組織全体を俯瞰する活動を，実践的な規模の取り組みとするための制限である。一方，情報セキュリティリスクアセスメントは，多くの組織で，情報資産を特定し，これに関連するリスクを特定する手法で実施されているため，リスクの数は 10 程度ではなく，より多くの数となっている場合が多い。そこで，本研究では，4 章及び 5 章で，数多いリスクが特定・評価されたリスクアセスメントの結果から，本モデル要素できるリスク一覧を作成する方法について，具体例を以って示した。

b)の情報セキュリティ対策のリストについては，ISO/IEC 27002 [7]の管理策のカテゴリを用いて作成することを提案し，リスクヘッジ策と呼ぶ 14 個の要素からなるリストを示した。ISO/IEC 27002 [7]を参照することで，リスク対策のリストにある程度の網羅性を確保することを実現した。各リスクヘッジ策の実装にかかる費用の算出については，4 章及び 5 章において想定方法の具体例を示した。

c)の各リスクヘッジ策の各情報セキュリティリスクに対する影響値は，ISO/IEC 27002 [7]の記述を参照して算出する手法を提案した。また，4 章及び 5 章において使用した影響値について，算出した過程の記録を付録 A に示した。本影響値算出の手法も，その判断に定性評価を含むため，実施者の主観が含まれるが，付録 A として過程を示すことで，他者が本モデルを使用する際に，自身の判断で影響値の見直しができる。また，本研究で使用した以外のリスクの一覧を使用する場合にも，2.2(4)で示した内容と付録 A を参照して影響値を算出することができる。

次に，サンプルデータ，情報セキュリティリスクマネジメント実施に関する統計データ，及び実際の情報セキュリティリスクマネジメントの実施データを用いて，モデルの有効性及び活用方法の検証を行った。

3 章のサンプルデータの適用では，リスク受容値が決定されている場合に，それを実現する組織の予算の最小値の近似値を見つけるために本モデルを使用できること，また，逆に，組織の予算が決められている場合に達成できるリスク受容値の最小値を見つけることにも本モデルを活用できることを示した。尚，このアプローチは，4 章及び 5 章でも応用的に用いている。

4 章の統計データを用いた検証では，いわゆるリスクアセスメント結果が得られていない場合に，類似の情報からリスクアセスメント結果を推定する方法，影響値算出に用いた観点を活用した各リスクヘッジ策の実施に係る費用の推定方法，及び組織の予算の推定方法を，経済産業省による情報処理実態調査[40]のデータを用いて，具体例を以って示した。また，モデルが導いた各リスクヘッジ策の選択結果については，リスク受容値や組織の予算を変更して得たいくつかの結果を比較することで，解の妥当性が確認できること，また組織にとっての最適解を探すことができることを，具体例で示した。各リスクヘッジ策の選択結果についても，それぞれ組織の環境やリスクの状況を考慮し，選択された理由を推察することで，選択結果の妥当性，有用性について確認できた。

5 章では，ある組織が ISMS 認証取得の取り組みの中で実施した情報セキュリティリスクアセスメント及びリスク対応の記録を参照し，実際に本モデルを適用することで，モデルの有効性を確認した。実際のリスク対応結果とモデルの解とでは差が生じたが，差分が生じた理由の明確化，本モデルによる解が妥当であることの確認をとおして，本モデルが組織にとって有効なリスク対応の解を導くことを示した。

6.2 今後の課題

本研究では，モデルの単純化のために，リスクヘッジ策に関する次の点でさまざまな限定条件を置いた。

a) リスクヘッジ策の実装にかかる費用の算出方法
b) リスクヘッジ策の選択割合と実装費用

a)については，組織の環境や業態などにより，リスクヘッジ策の実装にかかる費用は異なるため，この算出方法を示すことは重要である。本研究では，影響値算出において得られた各リスクヘッジ策がもつ物理的，技術的，人的及び運用的対策の数を用いて，1つの対策にかかる費用は一律であるという仮定を置き，その単価を決めることで各リスクヘッジ策の費用を算出する手法を示し，実際に4章及び5章の検討で用いた。しかし，より実際に近い値を設定するためには，本費用の算出方法の改善が必要となる。例えば，影響値算出手法において，リスクヘッジ策に含まれる対策の数の数え方が，管理策単位では4つ

の観点が有るか無いかだけの判断となっており，ひとつの管理策の中で複数個の運用対策が実施されている場合などに，その数は反映されていないといったことがある。また，物理的対策と人的対策をそれぞれ1つ実施する場合にかかる費用は同じでよいか，組織の業態や体制などにより特徴があるかなど，精緻化のアイディアの候補はいくつかあるが，いずれも手法をかなり複雑にすることが想定されるため，実現性をよく考慮して検討する必要がある。

b)については，本研究では，リスクヘッジ策の選択割合と実装費用は正比例の関係にあると仮定した。しかし，リスクヘッジ策が複数の管理策から構成されており，また各管理策も物理的，技術的，人的及び運用的といったさまざまな対策で構成されていることを考えると，より精緻な結果を得るためには，適用率と費用の関係を詳細化する必要がある。物理的，技術的，人的及び運用的を包含する程度でリスクヘッジ策をパターン分けし，パターン毎に選択割合と費用の関係を示す関数を設定するなどのアイディアはあるものの，包含の程度の算定は複雑になることが想定され，また適当な関数を見つけられるかといった課題もある。複雑化にかかる工数と効果をよく判断し，詳細化は検討する必要がある。

さらに，基本モデルに重みづけの概念を追加したモデルも検討中の状況である。具体的に，リスクに重みづけを行う場合と，リスクヘッジ策に重みづけを行う場合とが考えられる。

リスクへの重みづけについては[45]で検討している。そこでは，コンピュータウィルスの被害が急増したり，情報漏えいが頻発したりといった，リスクのトレンドをモデルに反映させることを目的とし，各リスクへの重みづけをモデルへのインプットとして追加した拡張モデルを提案している。しかし，そうしたリスクのトレンドは，リスクの重みを追加してモデルを拡張するのではなく，リスク値を評価するときにそれに含める方法も考えられる。また，リスクの重みを結果に反映させるためには，どの程度の重みを付加するかについて，さらなる検討が必要な状況にある。

リスクヘッジ策への重みづけについては，組織として重点的に実施したい対策がある場合に，それが優先的に選択されるような解を導くモデルが考えられる。重点的に実施したいリスクヘッジ策に重みを付加し，モデルが解を導く場合に，それらの選択が，設定した重みを反映して実施されるようにする拡張モデルである。このような拡張モデルを用いるケースとしては，組織が既に，情報セキュリティ対策の実装につながるような計画を持っている場合などが考えられる。例えば，事務所移動に伴う物理対策の実施を計画中といった状況が具体例として考えられる。しかし，リスクヘッジ策へ重みづけの導入は，現在のEXCELソルバーを用いたモデルでの実現は難しいため，実装方法の変更も視野に検討する必要がある。

7　謝辞

本研究を行うにあたりご指導を賜りました，廣松 毅教授に深く感謝いたします。研究に関するご指導から論文の作成に至るまで，多大なるご助言及びご指導をいただきました。特に，研究を進めるのに迷った際にいただいた，発想の転換を促すアドバイスには，いつも感銘を受けました。

論文執筆にあたっては，原田 要之助教授から，情報セキュリティマネジメントの観点から多くの具体的なご助言と，ご指導をいただきました。また，本論文の審査に加わっていただきました，田中 英彦教授，佐藤 直教授には，本論文を完成させるにあたり，貴重なご指導と再考の機会をいただきました。ここに深く感謝いたします。

付録A 影響値の算出

(1) 表 1の情報セキュリティリストに対する影響値の算出

表 6の各リスクヘッジ策の，表 1の各情報セキュリティリスクに対する影響値を算出するにあたって，2.2(4)に記した手順を適用した結果を下表に示す。

表 40 影響値の算出（基本モデル及び実データ検討で使用）

管理策	観点	情報セキュリティリスク							判断の根拠	備考
		R_1	R_2	R_3	R_4	R_5	R_6	R_7		
箇条 5 (H_1) 情報セキュリティのための方針群										
5.1. 情報セキュリティのための経営陣の方向性										
5.1.1 情報セキュリティのための方針群	物理的	0	0	0	0	0	0	0	「脅威環境から生じる要求事項を扱う」こと，及び「ISMに関する責任の割り当てをする」ことが行われる管理策であるため，全リスクに対する運用的及び人的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
5.1.2 情報セキュリティのための方針群のレビュー	物理的	0	0	0	0	0	0	0	「組織で選択した管理策のレビューをする」管理策であるため，全リスクに対する運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
H_1 合計		3	3	3	3	3	3	3		
H_1 影響値（合計/250）		0.01	0.01	0.01	0.01	0.01	0.01	0.01		
箇条 6 (H_2) 情報セキュリティのための組織										
6.1 内部組織										
6.1.1 情報セキュリティの役割及び責任	物理的	0	0	0	0	0	0	0	全ての情報セキュリティ責任を定め，割り当てること，及びそのルール化に関する管理策であるため，全リスク対する人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
6.1.2 職務の分離	物理的	0	0	0	0	0	0	0	職務上の権限悪用又はミスなどがリスクのため内部・契約者によるリスクが対象。職務の分離，そのルール化のため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	0	1	1	0	0		
6.1.3 関係当局との連絡	物理的	0	0	0	0	0	0	0	いずれのリスクも当局への連絡が発生する場合があるため，全てのリスクが対象の運用的対策に相当。いつ誰が連絡するかという内容も含むため人的対策にも相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
6.1.4 専門組織との連絡	物理的	0	0	0	0	0	0	0	いずれのリスクも専門組織との連絡体制の維持は望ましいため，全てのリスクが対象。組織単位の連絡体制であるため，運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
6.1.5 PM における情報セキュリティ	物理的	0	0	0	0	0	0	0	プロジェクトマネジメントにおいて，情報セキュリティリスクを特定・対処する管理策であるため，全てのリスクが対象の運用的及び人的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		

6.2 モバイル機器及びテレワーキング										
6.2.1 モバイル機器の方針	物理的	1	1	1	1	1	1	0	記載されている脅威は，マルウェア，認可されないアクセス，漏洩，盗難・紛失のため人によるリスク全般。すべての対策にあてはまる	
	技術的	1	1	1	1	1	1	0		
	人的	1	1	1	1	1	1	0		
	運用的	1	1	1	1	1	1	0		
6.2.2 テレワーキング	物理的	1	1	1	1	1	1	0	テレワーキング場所でのアクセス，処理及び保存される情報の保護が目的のため，人によるリスク全般。管理策の内容は人的対策以外全て。	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
H_2 合計		16	16	14	16	16	14	7		
H_2 影響値（合計/250）		0.06	0.06	0.06	0.06	0.06	0.06	0.03		
箇条 7 (H_3)　人的資源のセキュリティ										
7.1 雇用前										
7.1.1 選考	物理的	0	0	0	0	0	0	0	内部者・契約者が意図的に発生するリスクが対象。雇用や契約に関する対策は人的対策のため，人的対策のみに相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	0	0	0	0	0		
7.1.2 雇用条件	物理的	0	0	0	0	0	0	0	内部者・契約者が意図的に発生するリスクが対象。雇用や契約に関する組織でのルール化も含むため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	0	0	0	0	0		
	運用的	1	1	0	0	0	0	0		
7.2 雇用期間中										
7.2.1 経営陣の責任	物理的	0	0	0	0	0	0	0	内部者・契約者が発生するリスクが対象。雇用や契約に関する組織でのルール化も含むため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	0	1	1	0	0		
	運用的	0	0	0	0	0	0	0		
7.2.2 情報セキュリティの意識向上，教育及び訓練	物理的	0	0	0	0	0	0	0	内部者・契約者が発生するリスクが対象。教育や訓練に関する対策及びそれらのルール化のため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	0	1	1	0	0		
7.2.3 懲戒手続	物理的	0	0	0	0	0	0	0	内部者が発生するリスクが対象。懲戒手続きのルール化と実装についてなので人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	0	0	0	0	0	0		
	運用的	1	0	0	0	0	0	0		
7.3 雇用の終了及び変更										
7.3.1 雇用の終了又は変更に関する責任	物理的	0	0	0	0	0	0	0	内部者・契約者が発生するリスクが対象。雇用の終了及び変更に関するルール化と実装についてなので人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	0	1	1	0	0		
	運用的	1	1	0	1	1	0	0		
H_3 合計		9	7	0	4	4	0	0		
H_3 影響値（合計/250）		0.04	0.03	0	0.02	0.02	0	0		

箇条 8 (H_4)　資産の管理										
8.1 資産に対する責任										
8.1.1 資産目録	物理的	0	0	0	0	0	0	0	資産を脅かすリスクが対象のため，全てのリスクが対象。資産目録の作成及び維持なので運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
8.1.2 資産の管理責任	物理的	0	0	0	0	0	0	0	資産を脅かすリスクが対象のため，全てのリスクが対象。管理責任者を割り当て管理することであるため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
8.1.3 資産利用の許容範囲	物理的	0	0	0	0	0	0	0	資産を脅かすリスクが対象のため，全てのリスクが対象。ルール化，利用者の責任の明言から，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	0		
	運用的	1	1	1	1	1	1	0		
8.1.4 資産の返却	物理的	0	0	0	0	0	0	0	契約等終了に伴うリスクのため内部者・契約者が対象。資産利用についての文書化・実装は運用的対策，意識付けなどは運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	0	1	1	0	0		
	運用的	1	1	0	1	1	0	0		
8.2 情報分類										
8.2.1 情報の分類	物理的	0	0	0	0	0	0	0	資産を脅かすリスクが対象のため，全てのリスクが対象。分類することのルール化と実装に関することのため運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
8.2.2 情報のラベル付け	物理的	1	1	1	1	1	1	0	ラベル付けが効力を発揮するため，人によるリスクが対象。物理的／技術的ラベル付け，そのルール化と実装，従業員他への周知のため，全ての対策に相当。	
	技術的	1	1	1	1	1	1	0		
	人的	1	1	1	1	1	1	0		
	運用的	1	1	1	1	1	1	0		
8.2.3 資産の取扱い	物理的	1	1	1	1	1	1	0	ラベル付けが効力を発揮するため，人によるリスクが対象。資産の取り扱いに関する物理的／技術的内容，ルール化のため人的対策以外に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
8.3 媒体の取扱い										
8.3.1 取外し可能な媒体の管理	物理的	1	1	1	1	1	1	0	媒体内情報の認可されない開示，変更，除去又は破壊がリスクのため，人によるリスクが対象。物理／技術的内容，ルール化を含むため物理的，技術的，運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
8.3.2 媒体の処分	物理的	1	1	1	1	1	1	0	媒体内情報の認可されない開示，変更，除去又は破壊がリスクのため，人によるリスクが対象。物理的／技術的内容，ルール化を含むため物理的，技術的，運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
8.3.3 物理的媒体の輸送	物理的	1	1	1	1	1	1	0	媒体内情報の認可されない開示，変更，除去又は破壊がリスクのため，人によるリスクが対象。物理的／技術的内容，ルール化を含むため物理的，技術的，運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		

H_4 合計		24	24	22	24	24	22	4		
H_4 影響値（合計/250）		0.10	0.10	0.09	0.10	0.10	0.09	0.02		
箇条 9 (H_5)　アクセス制御										
9.1 アクセス制御に対する業務上の要求事項										
9.1.1 アクセス制御方針	物理的	0	0	0	0	0	0	0	人による情報へのアクセスに対するリスクが対象。アクセス制御方針の文書化及び維持なので運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
9.1.2 ネットワーク及びネットワークサービスへのアクセス	物理的	0	0	0	0	0	0	0	人による情報及び情報処理施設へのｱｸｾｽに対するﾘｽｸが対象。ﾈｯﾄﾜｰｸ及びﾈｯﾄﾜｰｸｻｰﾋﾞｽのｱｸｾｽ制御の技術的対応とﾙｰﾙ化なので技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
9.2 利用者アクセスの管理										
9.2.1 利用者登録及び登録削除	物理的	0	0	0	0	0	0	0	人によるシステム及びサービスへの認可されないアクセスが対象リスク。利用者IDの登録・削除の技術的対応内容とルール化なので，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
9.2.2 利用者アクセスの提供	物理的	0	0	0	0	0	0	0	人によるシステム及びサービスへの認可されないアクセスが対象リスク。利用者 ID へのアクセス権割り当てに関する技術的対応とルール化なので，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
9.2.3 特権的アクセス権の管理	物理的	0	0	0	0	0	0	0	人によるシステム及びサービスへの認可されないアクセスが対象リスク。特権的アクセス権に対する技術的対応とルール化なので，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
9.2.4 利用者の秘密認証情報の管理	物理的	1	1	1	1	1	1	0	人によるシステム及びサービスへの認可されないアクセスが対象リスク。秘密認証情報の割当に関する技術的対応とルール化なので，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
9.2.5 利用者アクセス権のレビュー	物理的	0	0	0	0	0	0	0	人によるシステム及びサービスへの認可されないアクセスが対象リスク。利用者アクセス権のレビューに関する技術的対応(ログ取得など)とルール化なので，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
9.2.6 アクセス権の削除又は修正	物理的	1	1	1	1	1	1	0	人によるシステム及びサービスへの認可されないアクセスがリスク対象。アクセス権削除･修正に関する物理的／技術的対応，及びルール化なので，物理的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
9.3 利用者の責任										
9.3.1 秘密認証情報の利用	物理的	1	1	0	1	1	0	0	利用者認証情報の不適切な管理がリスクのため内部・契約者が対象。利用者認証情報管理への物理的／技術的対応，ルール化及び利用者への要求のため，全ての対策に相当	
	技術的	1	1	0	1	1	0	0		
	人的	1	1	0	1	1	0	0		
	運用的	1	1	0	1	1	0	0		

9.4 システム及びアプリケーションのアクセス制御										
9.4.1 情報へのアクセス制限	物理的	1	1	1	1	1	1	0	人によるシステム及びアプリケーションへの認可されないアクセスが対象リスク。物理的／技術的アクセス制御とルール化についてなので，物理的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
9.4.2 セキュリティに配慮したログオン手順	物理的	0	0	0	0	0	0	0	認可されないシステム及びアプリケーションへの意図的アクセスが対象リスク。セキュリティに配慮したログオン手順に関する技術的対応とルール化のため，技術的及び運用的対策に相当	
	技術的	1	1	1	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	0	0	0	0		
9.4.3 パスワード管理システム	物理的	0	0	0	0	0	0	0	人によるシステム及びアプリケーションへの認可されないアクセスが対象リスク。パスワード管理システムの満たすべき条件のルール化と実装のため，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
9.4.4 特権的なユーティリティプログラムの使用	物理的	0	0	0	0	0	0	0	人によるシステム及びアプリケーションへの認可されないアクセスが対象リスク。特権的ユーティリティプログラムの管理についての技術的対応とルール化のため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
9.4.5 プログラムソースコードへのアクセス制御	物理的	1	1	1	1	1	1	0	人によるｼｽﾃﾑ及びｱﾌﾟﾘｹｰｼｮﾝへの認可されないｱｸｾｽが対象リスク。ﾌﾟﾛｸﾞﾗﾑｿｰｽｺｰﾄﾞの管理への物理的／技術的対応とﾙｰﾙ化のため，物理的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
H_5 合計		33	33	29	31	31	27	0		
H_5 影響値（合計/250）		0.13	0.13	0.12	0.12	0.12	0.11	0.00		
箇条 10 (H_6)　暗号										
10.1. 暗号による管理策										
10.1.1 暗号による管理策	物理的	0	0	0	0	0	0	0	人による意図的・偶発的な情報の侵害が対象リスク。暗号管理についての方針作成，及び暗号方針実施に関する技術的対応のため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
10.1.2 鍵管理	物理的	0	0	0	0	0	0	0	人による意図的・偶発的な情報の侵害が対象リスク。鍵管理の方法とルール化なので技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
H_6 合計		4	4	4	4	4	4	0		
H_6 影響値（合計/250）		0.02	0.02	0.02	0.02	0.02	0.02	0		
箇条 11 (H_7)　物理的及び環境的セキュリティ										
11.1 セキュリティを保つべき領域										
11.1.1 物理的セキュリティ境界	物理的	1	1	1	1	1	1	1	物理的アクセス，損傷及び妨害全般のため全リスクが対象。物理的境界の設定，侵入検知システム導入とルール化のため技術的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		

11.1.2 物理的入退管理策	物理的	1	1	1	1	1	1	0	物理的入退リスクのため人によるリスクが対象。侵入を管理する物理対策，及び物理対策を補助／補強する技術対策とルール化のため物理的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
11.1.3 オフィス，部屋及び施設のセキュリティ	物理的	1	1	1	1	1	1	0	人による認可されない物理的アクセス，損傷及び妨害が対象リスク。オフィス，部屋及び施設への物理的対策とそのルール化のため，物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1			
11.1.4 外部及び環境の脅威からの保護	物理的	0	0	1	0	0	0	1	外部者及び人以外によるリスクが対象。専門家から助言を得た物理的対策とそのルール化のため，物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	0	0	1	0	0	1	1		
11.1.5 セキュリティを保つべき領域での作業	物理的	1	1	1	1	1	0	0	セキュリティを保つべき領域での人によるリスクが対象のため，外部者の意図しないリスクは対象外。物理的対応とそのルール化なので物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	0	0		
11.1.6 受渡場所	物理的	1	1	1	1	1	1	0	人による認可されない物理的アクセス，損傷及び妨害が対象リスク。外部者が立ち入る受渡場所に対する物理的対応とそのルール化なので物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
11.2 装置										
11.2.1 装置の設置及び保護	物理的	1	1	1	1	1	1	0	人による装置及び関連資産の損失，損傷，盗難又は劣化，及び組織の業務の妨害がリスク。装置の設置や保護とそのルール化なので，物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
11.2.2 サポートユーティリティ	物理的	0	0	0	0	0	0	1	ｻﾎﾟｰﾄﾕｰﾃｨﾘﾃｨ(電気，通信ｻｰﾋﾞｽ，給水，ｶﾞｽ，空調など)の不具合による装置の故障がﾘｽｸ(人以外のﾘｽｸ)。ｻﾎﾟｰﾄﾕｰﾃｨﾘﾃｨへの条件に相当する物理的，技術的，及び運用的対策	
	技術的	0	0	0	0	0	0	1		
	人的	0	0	0	0	0	0	0		
	運用的	0	0	0	0	0	0	1		
11.2.3 ケーブル配線のセキュリティ	物理的	1	1	1	1	1	1	0	人による情報の傍受，情報及び関連する資産の損傷，及び組織の業務の妨害がリスク。ケーブル配線の物理的保護とその運用のため，物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
11.2.4 装置の保守	物理的	0	0	0	0	0	0	1	装置の完全性及び可用性の侵害がリスク。装置の保守に関する物理／技術対応とその運用についてなので，物理的，技術的，及び運用的対策に相当	
	技術的	0	0	0	0	0	0	1		
	人的	0	0	0	0	0	0	0		
	運用的	0	0	0	0	0	0	1		
11.2.5 資産の移動	物理的	1	1	0	1	1	0	0	移動に伴う，装置及び関連する資産の損失，損傷や組織の業務の妨害などがリスクのため，内部・契約者が対象。装置の移動の保護とその運用のため，物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	0	1	1	0	0		

11.2.6 構外にある装置及び資産のセキュリティ	物理的	1	1	1	1	1	1	0	人による装置の損失，盗難，及び装置に関連する傍受が対象リスク。構外の装置に対する物理的／技術的対策，及び運用なので物理的，技術的，及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
11.2.7 装置のセキュリティを保った処分又は再利用	物理的	1	1	0	1	1	0	0	処分等に伴う装置に格納されたデータやソフトウェアの漏洩がリスクのため内部・契約者が対象。処分に伴う物理／技術対応，その運用なので，物理的，技術的，及び運用的対策に相当	
	技術的	1	1	0	1	1	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	0	1	1	0	0		
11.2.8 無人状態にある利用者装置	物理的	1	1	1	1	1	1	1	無人状態の利用者装置，それ経由でｱｸｾｽできる資産に対するﾘｽｸ全般が対象。装置への対策，その他資産への対策，その運用，及び利用者への助言等のため，全ての対策に相当。	
	技術的	1	1	1	1	1	1	1		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
11.2.9 クリアデスク・クリアスクリーン方針	物理的	1	1	1	1	1	1	0	書類や媒体類の机上放置によるﾘｽｸ，及び情報をｽｸﾘｰﾝ上に放置することによるﾘｽｸのため人によるﾘｽｸが対象。物理，技術，その運用，利用者への徹底など全ての対策に相当。	
	技術的	1	1	1	1	1	1	0		
	人的	1	1	1	1	1	1	0		
	運用的	1	1	1	1	1	1	0		
H_7 合計		32	32	29	32	32	27	15		
H_7 影響値（合計/250）		0.13	0.13	0.12	0.13	0.13	0.11	0.06		
箇条 12 (H_8)　運用のセキュリティ										
12.1 運用の手順及び責任										
12.1.1 操作手順書	物理的	0	0	0	0	0	0	0	情報処理設備が正しく使用されないことに起因するリスク全般。運用に関する対策全般であるため，運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
12.1.2 変更管理	物理的	0	0	0	0	0	0	0	組織，業務プロセス，情報処理設備及びシステムの変更に起因するリスクのため，内部・契約者が対象。変更管理に関する対策のため運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	0	1	1	0	0		
12.1.3 容量・能力の管理	物理的	0	0	0	0	0	0	0	システム性能不足に起因するリスク全般が対象。調整，能力予測などが該当するため運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
12.1.4 開発環境，試験環境及び運用環境の分離	物理的	1	1	0	1	1	0	0	ﾌｧｲﾙ/ｼｽﾃﾑ環境の不正な変更，ｼｽﾃﾑ不具合，運用環境への不正なｺｰﾄﾞの挿入，運用ﾃﾞｰﾀの不正な変更，要員の不正による情報漏えいなど内部契約者によるﾘｽｸが対象。すべての対策に相当	
	技術的	1	1	0	1	1	0	0		
	人的	1	1	0	1	1	0	0		
	運用的	1	1	0	1	1	0	0		
12.2 マルウェアからの保護										
12.2.1 マルウェアに対する管理策	物理的	0	0	0	0	0	0	0	マルウェアの侵入によるリスクのため，人によるリスクが対象。技術的対応と運用，人員への徹底のため，技術的，運用的及び人的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	1	1	1	1	1	1	0		
	運用的	1	1	1	1	1	1	0		

12.3 バックアップ										
12.3.1 情報のバックアップ	物理的	1	1	1	1	1	1	1	データの消失に関するリスク全般が対象。バックアップ方針や運用，バックアップデータの物理的，技術的保護が該当するため，物理的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
12.4 イベントログ取得										
12.4.1 イベントログ取得	物理的	0	0	0	0	0	0	0	各種活動や事象等の不記録により，不正の原因・証拠，ｲﾝｼﾃﾞﾝﾄを特定できないなど人によるﾘｽｸが対象。ﾛｸﾞ取得の設定及び運用のため，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
12.4.2 ログ情報の保護	物理的	0	0	0	0	0	0	0	ログ情報の改ざん及び不正アクセスなど人によるリスクが対象。技術的保護とその運用が対策として該当するから技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
12.4.3 実務管理者及び運用担当者の作業ログ	物理的	0	0	0	0	0	0	0	利用者の自己の特権の不正使用がリスクのため，内部・契約者が対象。作業ログの保護とレビューが対策のため，技術的及び運用的対策に相当	
	技術的	1	1	0	1	1	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	0	1	1	0	0		
12.4.4 クロックの同期	物理的	0	0	0	0	0	0	0	不正確な監査ﾛｸﾞにより，証拠の信頼性を損なう，ｲﾝｼﾃﾞﾝﾄを特定できない等の人によるﾘｽｸが対象。ｸﾛｯｸ同期を要求事項として文書化，その技術的保護のため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
12.5 運用ソフトウェアの管理										
12.5.1 運用システムに関わるソフトウェアの導入	物理的	1	1	1	1	1	1	0	人による運用システムの完全性侵害が対象リスク。運用システムに関わるソフトウェアの変更管理，ソフトウェアの物理的保管のため，物理的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
12.6 技術的ぜい弱性管理										
12.6.1 技術的ぜい弱性の管理	物理的	0	0	0	0	0	0	0	技術的ぜい弱性の悪用がリスクであり，人による意図的なリスクが対象。ぜい弱性管理及び技術的対応のため，技術的及び運用的対策に相当	
	技術的	1	1	1	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	0	0	0	0		
12.6.2 ソフトウェアのインストールの制限	物理的	0	0	0	0	0	0	0	ｿﾌﾄｳｪｱのｲﾝｽﾄｰﾙ制限不足によりぜい弱性対策が不十分になることがﾘｽｸのため，内部・契約者が対象。ｲﾝｽﾄｰﾙ制限のﾙｰﾙ化と利用者への徹底のため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	0	1	1	0	0		
	運用的	1	1	0	1	1	0	0		
12.7 情報システムの監査に対する考慮事項										
12.7.1 情報システムの監査に対する管理策	物理的	0	0	0	0	0	0	0	運用システム監査による業務プロセスの中断という内部・契約者による意図しないリスクが対象。監査方法への同意，監査用アクセスログ取得など技術的及び運用的対策に相当	
	技術的	0	0	0	1	1	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	0	0	0	1	1	0	0		
H_8 合計		28	28	19	28	28	17	5		
H_8 影響値（合計/250）		0.11	0.11	0.08	0.11	0.11	0.07	0.02		

箇条 13 (H_9)　通信のセキュリティ										
13.1 ネットワークセキュリティ管理										
13.1.1 ネットワーク管理策	物理的	0	0	0	0	0	0	0	ネットワーク上の情報，及びネットワーク関連施設が適切に保護できないリスク全般が対象。ネットワーク及び施設の技術的保護及びその運用のため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
13.1.2 ネットワークサービスのセキュリティ	物理的	0	0	0	0	0	0	0	ネットワークサービスの対策不十分による，ネットワーク上の情報，及びネットワーク関連施設の不十分な保護全般がリスク。ネットワークサービスを正しく保つ運用のため，運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
13.1.3 ネットワークの分離	物理的	1	1	1	1	1	1	1	ネットワーク上の情報，及びネットワーク関連施設が適切に保護できないこと全般がリスク。ネットワークの分離とその運用のため，物理的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
13.2 情報の転送										
13.2.1 情報転送の方針及び手順	物理的	1	1	1	1	1	1	1	組織の内外部に転送した情報が適切に保護されないリスク全般が対象。手順化，責任の割り当て，暗号技術の適用，装置への物理アクセス制限のため，全ての対策が相当	
	技術的	1	1	1	1	1	1	1		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
13.2.2 情報転送に関する合意	物理的	0	0	0	0	0	0	0	外部関係者との合意に因らない情報転送により情報セキュリティリスクが顕在化するリスク全般。合意を事前に取ることが該当するため，運用的対策に相当。	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
13.2.3 電子的メッセージ通信	物理的	0	0	0	0	0	0	0	電子的ﾒｯｾｯｰｼﾞ通信内の情報が脅かされるリスク全般が対象。認証強化，通信の保護，送付先指定の確実化，外部ｻｰﾋﾞｽ使用時の承認手続き化のため，技術的，人的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
13.2.4 秘密保持契約又は守秘義務契約	物理的	0	0	0	0	0	0	0	外部関係者及び従業員により秘密情報が脅かされるリスク。契約に掲載すべき要求事項の特定と文書化，それによる人員管理のため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	0		
	運用的	1	1	1	1	1	1	0		
H_9 合計		16	16	16	16	16	16	14		
H_9 影響値（合計/250）		0.06	0.06	0.06	0.06	0.06	0.06	0.06		
箇条 14 (H_{10})　システムの取得，開発及び保守										
14.1 情報システムのセキュリティ要求事項										
14.1.1 情報セキュリティ要求事項の分析及び仕様化	物理的	0	0	0	0	0	0	0	情報システムの情報セキュリティ要求事項の仕様化が不十分なことによるリスク全般が対象。要求事項の仕様化，及び供給者との契約への反映のため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
14.1.2 公衆ﾈｯﾄﾜｰｸ上のｱﾌﾟﾘｹｰｼｮﾝｻｰﾋﾞｽのｾｷｭﾘﾃｨの考慮	物理的	0	0	0	0	0	0	0	公衆ネットワークを経由するｱﾌﾟﾘｹｰｼｮﾝｻｰﾋﾞｽに含まれる情報に対する不正行為，契約紛争，及び認可されない開示・変更など意図的なリスクが対象。要求事項の考慮なので運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	0	0	0	0		

14.1.3 ｱﾌﾟﾘｹｰｼｮﾝｻｰﾋﾞｽのﾄﾗﾝｻﾞｸｼｮﾝの保護	物理的	0	0	0	0	0	0	0	ｱﾌﾟﾘｹｰｼｮﾝｻｰﾋﾞｽのﾄﾗﾝｻﾞｸｼｮﾝに含まれる情報の不完全な通信，認可されない変更等，人によるﾘｽｸが対象。ﾄﾗﾝｻﾞｸｼｮﾝの技術的保護と運用のため，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	0		
14.2 開発及びサポートプロセスにおけるセキュリティ										
14.2.1 セキュリティに配慮した開発のための方針	物理的	0	0	0	0	0	0	0	情報システムの開発サイクルにおいて適切に情報セキュリティが設計，実施されないことによるリスク全般が対象。方針の作成とその徹底であるため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
14.2.2 システムの変更管理手順	物理的	0	0	0	0	0	0	0	開発ライフサイクルにおけるシステムの変更が適切に管理されないことに伴うリスク全般が対象。手順の作成とその徹底であるため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
14.2.3 ｵﾍﾟﾚｰﾃｨﾝｸﾞﾌﾟﾗｯﾄﾌｫｰﾑ変更後のｱﾌﾟﾘｹｰｼｮﾝの技術的ﾚﾋﾞｭｰ	物理的	0	0	0	0	0	0	0	ｵﾍﾟﾚｰﾃｨﾝｸﾞﾌﾟﾗｯﾄﾌｫｰﾑの変更に伴い，ｱﾌﾟﾘｹｰｼｮﾝの機能及び処理の完全性が損なわれるﾘｽｸ全般が対象。変更に伴う技術ﾚﾋﾞｭｰの実施のため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
14.2.4 パッケージソフトウェアの変更に対する制限	物理的	0	0	0	0	0	0	0	ﾊﾟｯｹｰｼﾞｿﾌﾄの変更による機能や処理の完全性失墜，業者の保障が得られなくなるﾘｽｸ全般が対象。変更手続のﾙｰﾙ化，十分な技術的検証のため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
14.2.5 セキュリティに配慮したシステム構築の原則	物理的	1	1	1	1	1	1	1	システム構築で適切なセキュリティの配慮がなされないことに伴うリスク全般が対象。システム構築手順の確立とその実装のため，物理的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
14.2.6 セキュリティに配慮した開発環境	物理的	1	1	0	1	1	0	0	ｼｽﾃﾑ開発環境（要員，ﾌﾟﾛｾｽ，技術を含む）が適切に保たれないことに伴うﾘｽｸ全般が対象。開発環境の保護ﾚﾍﾞﾙの決定と構築，文書化，要員への徹底のため全ての対策に相当	
	技術的	1	1	0	1	1	0	0		
	人的	1	1	0	1	1	0	0		
	運用的	1	1	0	1	1	0	0		
14.2.7 外部委託による開発	物理的	0	0	0	0	0	0	0	外部委託先の開発活動で発生するリスク及び不適切なシステムが開発されるリスク全般が対象。外部委託契約，受入れ試験，証拠の提出要求のため技術的及び運用的対策に相当	
	技術的	0	1	1	0	1	1	0		
	人的	0	0	0	0	0	0	0		
	運用的	0	1	1	0	1	1	0		
14.2.8 システムセキュリティの試験	物理的	0	0	0	0	0	0	0	システムセキュリティ試験の不備によりシステムにおいて顕在化する可能性のあるリスク全般が対象。試験実施のためのルール及び試験の実施であるから，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
14.2.9 システムの受入れ試験	物理的	0	0	0	0	0	0	0	システム受入れ時のチェックの不備によりシステムにおいて顕在化する可能性のあるリスク全般が対象。受入れ試験実施のルール化及び試験の実施のため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		

14.3 試験データ										
14.3.1 試験データの保護	物理的	1	1	1	1	1	1	1	適切な試験データが用いられないことによる情報漏えい全般がリスク。運用ルール作成と技術的／物理的保護のため物理的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
H_{10} 合計		27	29	25	26	28	24	20		
H_{10} 影響値（合計/250）		0.11	0.12	0.10	0.10	0.11	0.10	0.08		
箇条 15 (H_{11})　供給者関係										
15.1 供給者関係における情報セキュリティ										
15.1.1 供給者関係のための情報セキュリティの方針	物理的	0	0	0	0	0	0	0	供給者による不適切な資産へのアクセスにより生じるリスクであるため契約者が対象。文書化及び供給者との合意であるため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	1	0	0	1	0	0		
	運用的	0	1	0	0	1	0	0		
15.1.2 供給者との合意におけるセキュリティの取扱い	物理的	0	0	0	0	0	0	0	供給者による不適切な行為により生じるリスクであり，契約者が対象。文書化及び供給者との合意であるため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
15.1.3 ICT サプライチェーン	物理的	0	0	0	0	0	0	0	ICT サービス及び製品のサプライチェーンに関するリスクへの対応不足によるリスクであり，契約者及び外部者が対象。文書化及び供給者との合意であるため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	1	1	0	1	1	1		
	運用的	0	1	1	0	1	1	1		
15.2 供給者のサービス提供の管理										
15.2.1 供給者のサービス提供の監視及びレビュー	物理的	0	0	0	0	0	0	0	供給者サービスの不備により顕在化する可能性のあるリスク全般が対象。監視しレビューすることであるから運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
15.2.2 供給者のサービス提供の変更に対する管理	物理的	0	0	0	0	0	0	0	供給者サービスの変更時の検討の不備により顕在化する可能性のあるリスク全般が対象。変更内容の検討であるため運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
H_{11} 合計		4	8	6	4	8	6	6		
H_{11} 影響値（合計/250）		0.02	0.03	0.02	0.02	0.03	0.02	0.02		
箇条 16 (H_{12})　情報セキュリティインシデント管理										
16.1 情報セキュリティインシデントの管理及びその改善										
16.1.1 責任及び手順	物理的	0	0	0	0	0	0	0	情報セキュリティインシデント全般がリスク。手順化と責務の明確化・周知のため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
16.1.2 情報セキュリティ事象の報告	物理的	0	0	0	0	0	0	0	情報セキュリティインシデント及びその報告が遅れることに伴うリスク全般が対象。手順化と責務の明確化・周知のため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		

16.1.3 情報セキュリティ弱点の報告	物理的	0	0	0	0	0	0	0	情報セキュリティインシデントがリスクであり，R_1～R_6。弱点発見時の運用及びその周知のため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
16.1.4 情報セキュリティ事象の評価及び決定	物理的	0	0	0	0	0	0	0	情報セキュリティインシデント全般がリスク。情報セキュリティインシデントの定義に関するルール化であるため運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
16.1.5 情報セキュリティインシデントへの対応	物理的	0	0	0	0	0	0	0	情報セキュリティインシデント全般がリスク。手順の文書化，インシデント発生後の分析であるため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
16.1.6 情報セキュリティインシデントからの学習	物理的	0	0	0	0	0	0	0	情報セキュリティインシデント全般がリスク。発生したインシデントを記録，分析すること，意識向上訓練につなげることであり，技術的，人的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
16.1.7 証拠の収集	物理的	0	0	0	0	0	0	0	情報セキュリティインシデント全般がリスク。証拠の収集のルール化と実装のため運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
H_{12} 合計		13	13	13	13	13	13	13		
H_{12} 影響値（合計/250）		0.05	0.05	0.05	0.05	0.05	0.05	0.05		
箇条 17 (H_{13})　事業継続マネジメントにおける情報セキュリティの側面										
17.1 情報セキュリティ継続										
17.1.1 情報セキュリティ継続の計画	物理的	0	0	0	0	0	0	0	事業継続をさまたげるリスク全般が対象。事業継続計画の策定であるため運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
17.1.2 情報セキュリティ継続の実施	物理的	1	1	1	1	1	1	1	事業継続をさまたげるリスク全般が対象。事業継続計画の実施であり，インシデント管理及びツールによる管理も含むため全ての対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
17.1.3 情報ｾｷｭﾘﾃｨ継続の検証，ﾚﾋﾞｭｰ及び評価	物理的	0	0	0	0	0	0	0	事業継続をさまたげるリスク全般が対象。事業継続計画の検証，レビュー及び評価であるため運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
17.2 冗長性										
17.2.1 情報処理施設の可用性	物理的	1	1	1	1	1	1	1	情報処理施設の可用性をさまたげるリスク全般が対象。情報処理施設の物理的／技術的冗長化及び運用であるため物理的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
H_{13} 合計		9	9	9	9	9	9	9		
H_{13} 影響値（合計/250）		0.04	0.04	0.04	0.04	0.04	0.04	0.04		

箇条 18 (H_{14})　順守										
18.1 法的及び契約上の要求事項の順守										
18.1.1 適用法令及び契約上の要求事項の特定	物理的	0	0	0	0	0	0	0	法的，規制又は契約上の義務に関する違反，及びセキュリティ上の要求事項に対する違反であり，内部・契約者が対象。要求事項の特定，文書化，順守であるため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	0	1	1	0	0		
	運用的	1	1	0	1	1	0	0		
18.1.2 知的財産権	物理的	0	0	0	0	0	0	0	知的財産権の侵害がリスクであり，内部・契約者が対象。知的財産権の特定，文書化，順守であるため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	1	1	0	1	1	0	0		
	運用的	1	1	0	1	1	0	0		
18.1.3 記録の保護	物理的	1	1	1	1	1	1	1	記録の消失，破壊，改ざん，許可されていないアクセス及び不正な流出全般が対象リスク。記録の物理的／技術的保護，ルール化のため，物理的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
18.1.4 プライバシー及び個人を特定できる情報（PII）の保護	物理的	1	1	1	1	1	1	1	プライバシーの侵害全般がリスク。ルール化と実装（技術的／物理的），順守であるため全ての対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	1	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1	1		
18.1.5 暗号化機能に対する規制	物理的	0	0	0	0	0	0	0	暗号化機能に関する協定，法令及び規制の不履行であり，内部・契約者が対象。規制の順守であるため運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	0	1	1	0	0		
18.2 情報セキュリティのレビュー										
18.2.1 情報セキュリティの独立したレビュー	物理的	0	0	0	0	0	0	0	確実な運用のためのレビューであるため，全てのリスクが対象。レビューなので運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
18.2.2 情報ｾｷｭﾘﾃｨのための方針群及び標準の順守	物理的	0	0	0	0	0	0	0	方針群及び基準のレビューであるため，全てのリスクが対象。レビューなので運用的対策に相当	
	技術的	0	0	0	0	0	0	0		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
18.2.3 技術的順守のレビュー	物理的	0	0	0	0	0	0	0	情報システムのレビューであり，全てのリスクが対象。技術的レビューも含まれるため，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1	1		
	人的	0	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1	1		
H_{18} 合計		16	16	11	16	16	11	11		
H_{18} 影響値（合計/250）		0.06	0.06	0.04	0.06	0.06	0.04	0.04		

(2) 表 2 の情報セキュリティリストに対する影響値の算出

表 6 の各リスクヘッジ策の, 表 2 の各情報セキュリティリスクに対する影響値を算出するにあたって, 2.2(4)に記した手順を適用した結果を下表に示す。

表 41　影響値の算出（統計データ検討で使用）

管理策	観点	情報セキュリティリスク						判断の根拠	備考
		R_1	R_2	R_3	R_4	R_5	R_6		
箇条 5 (H_1)　情報セキュリティのための方針群									
5.1. 情報セキュリティのための経営陣の方向性									
5.1.1 情報セキュリティのための方針群	物理的	0	0	0	0	0	0	「脅威環境から生じる要求事項を扱う」こと，及び「ISMに関する責任の割り当てをする」ことが行われる管理策であるため，全リスクに対する運用的及び人的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
5.1.2 情報セキュリティのための方針群のレビュー	物理的	0	0	0	0	0	0	「組織で選択した管理策のレビューをする」管理策であるため，全リスクに対する運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
H_1 合計		3	3	3	3	3	3		
H_1 影響値（合計/250）		0.01	0.01	0.01	0.01	0.01	0.01		
箇条 6 (H_2)　情報セキュリティのための組織									
6.1 内部組織									
6.1.1 情報セキュリティの役割及び責任	物理的	0	0	0	0	0	0	全ての情報セキュリティ責任を定め，割り当てること，及びそのルール化に関する管理策であるため，全リスク対する人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
6.1.2 職務の分離	物理的	0	0	0	0	0	0	認可のない／意図しない資産の変更又は不正使用が対象リスク。職務を分離すること，そのルール化が内容のため，R1からR5に対する人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	0		
	運用的	1	1	1	1	1	0		
6.1.3 関係当局との連絡	物理的	0	0	0	0	0	0	いずれのリスクも当局への連絡が発生する場合があるため，全てのリスクが対象の運用的対策に相当。いつ誰が連絡するかという内容も含むため人的対策にも相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
6.1.4 専門組織との連絡	物理的	0	0	0	0	0	0	いずれのリスクも専門組織との連絡体制の維持は望ましいため，全てのリスクが対象。組織単位の連絡体制であるため，運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
6.1.5 PM における情報セキュリティ	物理的	0	0	0	0	0	0	プロジェクトマネジメントにおいて，情報セキュリティリスクを特定・対処する管理策であるため，全てのリスクが対象の運用的及び人的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
6.2 モバイル機器及びテレワーキング									

6.2.1 モバイル機器の方針	物理的	0	0	1	1	1	1	記載されている脅威は，マルウェア，認可されないアクセス，漏洩，盗難・紛失のためR3～R6が対象。物理的／論理的／人的／運用的すべてにあてはまる	
	技術的	0	0	1	1	1	1		
	人的	0	0	1	1	1	1		
	運用的	0	0	1	1	1	1		
6.2.2 テレワーキング	物理的	0	1	1	1	1	0	テレワーキング場所でのアクセス，処理及び保存される情報の保護が目的のため，想定リスクはR2～R5。管理策の内容は人的対策にあたるもののみ無い	
	技術的	0	1	1	1	1	0		
	人的	0	0	0	0	0	0		
	運用的	0	1	1	1	1	0		
H_2 合計		9	12	16	16	16	11		
H_2 影響値（合計/250）		0.02	0.02	0.03	0.03	0.03	0.02		
箇条 7 (H_3)　人的資源のセキュリティ									
7.1 雇用前									
7.1.1 選考	物理的	0	0	0	0	0	0	内部者・契約者が発生しうるリスクが対象なので，R1～R6すべてが対象。雇用や契約に関する対策は人的対策のため，人的対策のみに相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	0	0	0	0	0	0		
7.1.2 雇用条件	物理的	0	0	0	0	0	0	内部者・契約者が発生しうるリスクが対象なので，R1～R6すべてが対象。雇用や契約に関する組織でのルール化も含むため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
7.2 雇用期間中									
7.2.1 経営陣の責任	物理的	0	0	0	0	0	0	内部者・契約者が発生しうるリスクが対象なので，R1～R6すべてが対象。雇用や契約に関する組織でのルール化も含むため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	0	0	0	0	0	0		
7.2.2 情報セキュリティの意識向上，教育及び訓練	物理的	0	0	0	0	0	0	内部者・契約者が発生しうるリスクが対象なので，R1～R6すべてが対象。教育や訓練に関する対策及びそれらのルール化のため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
7.2.3 懲戒手続	物理的	0	0	0	0	0	0	内部者・契約者が発生しうるリスクが対象なので，R1～R6すべてが対象。懲戒手続きのルール化と実装についてなので人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
7.3 雇用の終了及び変更									
7.3.1 雇用の終了又は変更に関する責任	物理的	0	0	0	0	0	0	内部者・契約者が発生しうるリスクが対象なので，R1～R6すべてが対象。雇用の終了及び変更に関するルール化と実装についてなので人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
H_3 合計		9	9	9	9	9	9		
H_3 影響値（合計/250）		0.02	0.02	0.02	0.02	0.02	0.02		

箇条 8 (H_4)　資産の管理									
8.1 資産に対する責任									
8.1.1 資産目録	物理的	0	0	0	0	0	0	資産を脅かすリスクが対象のため，R2～R5が対象。資産目録の作成及び維持なので運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	1	1	1	1	0		
8.1.2 資産の管理責任	物理的	0	0	0	0	0	0	資産を脅かすリスクが対象のため，R2～R5が対象。管理責任者を割り当て管理することであるため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	1	1	1	1	0		
	運用的	0	1	1	1	1	0		
8.1.3 資産利用の許容範囲	物理的	0	0	0	0	0	0	資産を脅かすリスクが対象のため，R2～R5が対象。ルール化だけでなく利用者に責任を負わせることが明言されているため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	1	1	1	1	0		
	運用的	0	1	1	1	1	0		
8.1.4 資産の返却	物理的	0	0	0	0	0	0	資産を脅かすリスクが対象のため，R2～R5が対象。資産利用の許容範囲の文書化・実装は運用的対策，また従業員及び外部利用者への意識付けなどは運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	1	1	1	1	0		
	運用的	0	1	1	1	1	0		
8.2 情報分類									
8.2.1 情報の分類	物理的	0	0	0	0	0	0	資産を脅かすリスクが対象のため，R2～R5が対象。分類することのルール化と実装に関することのため運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	1	1	1	1	0		
8.2.2 情報のラベル付け	物理的	0	1	1	1	1	0	資産を脅かすリスクが対象のため，R2～R5が対象。物理的／技術的ラベル付け，それについてのルール化と実装，従業員他への周知のため，全ての対策に相当。	
	技術的	0	1	1	1	1	0		
	人的	0	1	1	1	1	0		
	運用的	0	1	1	1	1	0		
8.2.3 資産の取扱い	物理的	0	1	1	1	1	0	資産を脅かすリスクが対象のため，R2～R5が対象。資産の取り扱いに関する物理的／技術的内容，ルール化を含むが，従業員他への周知の記述は無いため人的対策以外に相当	
	技術的	0	1	1	1	1	0		
	人的	0	0	0	0	0	0		
	運用的	0	1	1	1	1	0		
8.3 媒体の取扱い									
8.3.1 取外し可能な媒体の管理	物理的	0	1	1	0	1	0	媒体に保存された情報の認可されない開示，変更，除去又は破壊がリスクのため，R_2，R_3及びR_5。物理的／技術的内容，ルール化を含むため物理的，技術的，運用的対策に相当	
	技術的	0	1	1	0	1	0		
	人的	0	0	0	0	0	0		
	運用的	0	1	1	0	1	0		
8.3.2 媒体の処分	物理的	0	0	0	0	1	0	媒体に保存された情報の認可されない開示がリスクのためR_5。物理的／技術的内容，ルール化を含むため物理的，技術的，運用的対策に相当	
	技術的	0	0	0	0	1	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	0	0	1	0		
8.3.3 物理的媒体の輸送	物理的	0	1	1	0	1	0	媒体に保存された情報の認可されないアクセス，不正使用又は破壊がリスクのため，R_2，R_3及びR_5。物理的／技術的内容，ルール化を含むため物理的，技術的，運用的対策に相当	
	技術的	0	1	1	0	1	0		
	人的	0	0	0	0	0	0		
	運用的	0	1	1	0	1	0		

H_4 合計		0	21	21	15	24	0		
H_4 影響値（合計/250）		0.00	0.04	0.04	0.03	0.05	0.00		
箇条 9 (H_5)　アクセス制御									
9.1 アクセス制御に対する業務上の要求事項									
9.1.1 アクセス制御方針	物理的	0	0	0	0	0	0	情報へのアクセスに対するリスクが対象のためR2，R3及びR5。アクセス制御方針の文書化及び維持なので運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	1	1	0	1	0		
9.1.2 ネットワーク及びネットワークサービスへのアクセス	物理的	0	0	0	0	0	0	情報及び情報処理施設に対するリスクが対象のためR2～R5。ﾈｯﾄﾜｰｸ及びﾈｯﾄﾜｰｸｻｰﾋﾞｽのアクセス制御の技術的対応とルール化なので技術的及び運用的対策に相当	
	技術的	0	1	1	1	1	0		
	人的	0	0	0	0	0	0		
	運用的	0	1	1	1	1	0		
9.2 利用者アクセスの管理									
9.2.1 利用者登録及び登録削除	物理的	0	0	0	0	0	0	システム及びサービスへの認可されないアクセスがリスクのためR3。利用者IDの登録・削除の技術的対応内容とルール化なので，技術的及び運用的対策に相当	
	技術的	0	0	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	1	0	0	0		
9.2.2 利用者アクセスの提供	物理的	0	0	0	0	0	0	システム及びサービスへの認可されないアクセスがリスクのため R3。利用者 ID へのアクセス権割り当てに関する技術的対応とルール化なので，技術的及び運用的対策に相当	
	技術的	0	0	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	1	0	0	0		
9.2.3 特権的アクセス権の管理	物理的	0	0	0	0	0	0	システム及びサービスへの認可されないアクセスがリスクのため，R3。特権的アクセス権に対する技術的対応とルール化なので，技術的及び運用的対策に相当	
	技術的	0	0	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	1	0	0	0		
9.2.4 利用者の秘密認証情報の管理	物理的	0	0	1	0	0	0	システム及びサービスへの認可されないアクセスがリスクのため，R3。秘密認証情報の割当に関する技術的対応とルール化なので，技術的及び運用的対策に相当	
	技術的	0	0	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	1	0	0	0		
9.2.5 利用者アクセス権のレビュー	物理的	0	0	0	0	0	0	システム及びサービスへの認可されないアクセスがリスクのため，R3。利用者アクセス権のレビューに関する技術的対応(ログ取得など)とルール化なので，技術的及び運用的対策に相当	
	技術的	0	0	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	1	0	0	0		
9.2.6 アクセス権の削除又は修正	物理的	0	0	1	0	0	0	システム及びサービスへの認可されないアクセスがリスクのため，R3。アクセス権削除・修正に関する物理的／技術的対応，及びルール化なので，物理的，技術的及び運用的対策に相当	
	技術的	0	0	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	1	0	0	0		
9.3 利用者の責任									
9.3.1 秘密認証情報の利用	物理的	0	0	1	0	0	0	利用者による利用者認証情報の不適切な管理がリスクのため，R3。利用者認証情報管理への物理的／技術的対応，ルール化及び利用者への要求のため，全ての対策に相当	
	技術的	0	0	1	0	0	0		
	人的	0	0	1	0	0	0		
	運用的	0	0	1	0	0	0		

9.4 システム及びアプリケーションのアクセス制御									
9.4.1 情報へのアクセス制限	物理的	0	0	1	0	0	0	システム及びアプリケーションへの認可されないアクセスがリスクのため，R3。物理的／技術的アクセス制御とルール化についてなので，物理的，技術的及び運用的対策に相当	
	技術的	0	0	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	1	0	0	0		
9.4.2 セキュリティに配慮したログオン手順	物理的	0	0	0	0	0	0	システム及びアプリケーションへの認可されないアクセスがリスクのため，R3。セキュリティに配慮したログオン手順に関する技術的対応とルール化のため，技術的及び運用的対策に相当	
	技術的	0	0	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	1	0	0	0		
9.4.3 パスワード管理システム	物理的	0	0	0	0	0	0	システム及びアプリケーションへの認可されないアクセスがリスクのため，R3。パスワード管理システムの満たすべき条件のルール化と実装のため，技術的及び運用的対策に相当	
	技術的	0	0	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	1	0	0	0		
9.4.4 特権的なユーティリティプログラムの使用	物理的	0	0	0	0	0	0	システム及びアプリケーションへの認可されないアクセスがリスクのため，R3。特権的ユーティリティプログラムの管理についての技術的対応とルール化のため技術的及び運用的対策に相当	
	技術的	0	0	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	1	0	0	0		
9.4.5 プログラムソースコードへのアクセス制御	物理的	0	0	1	0	0	0	システム及びアプリケーションへの認可されないアクセスがリスクのため，R3。ﾌﾟﾛｸﾞﾗﾑｿｰｽｺｰﾄﾞの管理への物理的／技術的対応とルール化のため，物理的，技術的及び運用的対策に相当	
	技術的	0	0	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	1	0	0	0		
H_5 合計		0	3	33	2	3	0		
H_5 影響値（合計/250）		0.00	0.01	0.07	0.00	0.01	0.00		
箇条 10 (H_6) 暗号									
10.1. 暗号による管理策									
10.1.1 暗号による管理策	物理的	0	0	0	0	0	0	情報の機密性，真正性及び完全性の侵害がリスクのため，R2，R3，R5 及び R6。暗号管理についての方針作成，及び暗号方針実施に関する技術的対応のため技術的及び運用的対策に相当	
	技術的	0	1	1	0	1	1		
	人的	0	0	0	0	0	0		
	運用的	0	1	1	0	1	1		
10.1.2 鍵管理	物理的	0	0	0	0	0	0	情報の機密性，真正性及び完全性の侵害がリスクのため， R2，R3，R5及びR6。鍵管理の方法とルール化なので技術的及び運用的対策に相当	
	技術的	0	1	1	0	1	1		
	人的	0	0	0	0	0	0		
	運用的	0	1	1	0	1	1		
H_6 合計		0	4	4	0	4	4		
H_6 影響値（合計/250）		0.00	0.01	0.01	0.00	0.01	0.01		
箇条 11 (H_7) 物理的及び環境的セキュリティ									
11.1 セキュリティを保つべき領域									
11.1.1 物理的セキュリティ境界	物理的	1	0	1	0	0	0	認可されない物理アクセス，損傷及び妨害がリスクのためR1及びR3。物理的境界の設定，侵入検知システム導入とルール化のため技術的，技術的及び運用的対策に相当	
	技術的	1	0	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	0	1	0	0	0		

11.1.2 物理的入退管理策管理策	物理的	0	0	1	0	0	0	認可されない物理的アクセスがリスクのため，R3。侵入を管理する物理対策，及び物理対策を補助／補強する技術対策とルール化のため物理的，技術的及び運用的対策に相当	
	技術的	0	0	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	1	0	0	0		
11.1.3 オフィス，部屋及び施設のセキュリティ	物理的	1	0	1	0	0	0	認可されない物理的アクセス，損傷及び妨害リスクのため，R1 及び R3。オフィス，部屋及び施設への物理的対策とそのルール化のため，物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	0	1	0	0	0		
11.1.4 外部及び環境の脅威からの保護	物理的	1	0	0	0	0	0	火災，洪水，地震，爆発，暴力行為といった自然災害及び人的災害がリスクのため，R1。専門家から助言を得た物理的対策とそのルール化のため，物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	0		0	0	0		
11.1.5 セキュリティを保つべき領域での作業	物理的	1	0	1	0	0	0	認可されない物理的アクセス，損傷及び妨害がリスクのため，R1 及び R3。セキュリティを保つべき領域での作業に対する物理的対応とそのルール化なので物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	0	1	0	0	0		
11.1.6 受渡場所	物理的	1	0	1	0	0	0	認可されない物理的アクセス，損傷及び妨害がリスクのため，R1 及び R3。外部者が立ち入る受渡場所に対する物理的対応とそのルール化なので物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	0	1	0	0	0		
11.2 装置									
11.2.1 装置の設置及び保護	物理的	1	1	0	0	1	1	装置及び関連資産の損失，損傷，盗難又は劣化，及び組織の業務の妨害がリスクのため，R_1，R_2，R_5，R_6。装置の設置や保護とそのルール化なので，物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	0	0	1	1		
11.2.2 サポートユーティリティ	物理的	1	0	0	0	0	1	ｻﾎﾟｰﾄﾕｰﾃｨﾘﾃｨ(電気，通信ｻｰﾋﾞｽ，給水，ｶﾞｽ，空調など)の不具合による装置の故障がﾘｽｸのため，R1 及び R6。ｻﾎﾟｰﾄﾕｰﾃｨﾘﾃｨへの条件に相当する物理的，技術的，及び運用的対策	
	技術的	1	0	0	0	0	1		
	人的	0	0	0	0	0	0		
	運用的	1	0	0	0	0	1		
11.2.3 ケーブル配線のセキュリティ	物理的	1	0	0	0	1	1	情報の傍受，情報及び関連する資産の損傷，及び組織の業務の妨害がﾘｽｸのため，R1，R5 及び R6。ｹｰﾌﾞﾙ配線の物理的保護とその運用のため，物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	0	0	0	1	1		
11.2.4 装置の保守	物理的	1	0	0	0	0	1	装置の完全性及び可用性の侵害がリスクのため，R1 及び R6。装置の保守に関する物理／技術対応とその運用についてなので，物理的，技術的，及び運用的対策に相当	
	技術的	1	0	0	0	0	1		
	人的	0	0	0	0	0	0		
	運用的	1	0	0	0	0	1		
11.2.5 資産の移動	物理的	1	1	0	0	1	1	装置及び関連する資産の損失，損傷，盗難又は劣化，及び組織の業務の妨害がリスクのため，R_1，R_2，R_5 及び R_6。装置の移動の保護とその運用のため，物理的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	0	0	1	1		

11.2.6 構外にある装置及び資産のセキュリティ	物理的	0	0	0	1	1	1	対象ﾘｽｸは，装置の損失，盗難，及び装置に関連する傍受なので，R_4，R_5 及び R_6。構外の装置に対する物理的／技術的対策，及び運用なので物理的，技術的，及び運用的対策に相当	
	技術的	0	0	0	1	1	1		
	人的	0	0	0	0	0	0		
	運用的	0	0	0	1	1	1		
11.2.7 装置のセキュリティを保った処分又は再利用	物理的	0	0	0	0	1	1	装置に関連する資産（格納されたﾃﾞｰﾀやｿﾌﾄｳｪｱ）の漏洩がﾘｽｸのため R_5 及び R_6。装置の廃棄に伴う物理／技術対応，その運用なので，物理的，技術的，及び運用的対策に相当	
	技術的	0	0	0	0	1	1		
	人的	0	0	0	0	0	0		
	運用的	0	0	0	0	1	1		
11.2.8 無人状態にある利用者装置	物理的	1	1	1	1	1	0	無人状態の利用者装置，それ経由でｱｸｾｽできる資産に対するﾘｽｸのため，R1～R5。装置への対策，その他資産への対策，その運用，及び利用者への助言等のため，全ての対策に相当。	
	技術的	1	1	1	1	1	0		
	人的	1	1	1	1	1	0		
	運用的	1	1	1	1	1	0		
11.2.9 クリアデスク・クリアスクリーン方針	物理的	0	0	0	0	1	1	書類や取外し可能な記憶媒体の机上放置によるﾘｽｸ，及び情報をｽｸﾘｰﾝ上に放置することによるﾘｽｸのため，R5 及び R6。物理，技術，その運用，利用者への徹底など全ての対策に相当。	
	技術的	0	0	0	0	1	1		
	人的	0	0	0	0	1	1		
	運用的	0	0	0	0	1	1		
H_7 合計		27	8	16	7	20	22		
H_7 影響値（合計/250）		0.06	0.02	0.03	0.01	0.04	0.05		
箇条 12 (H_8)　運用のセキュリティ									
12.1 運用の手順及び責任									
12.1.1 操作手順書	物理的	0	0	0	0	0	0	情報処理設備が正しく使用されないことに起因するリスクなため，R1～R6。運用に関する対策全般であるため，運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
12.1.2 変更管理	物理的	0	0	0	0	0	0	組織，業務プロセス，情報処理設備及びシステムの変更に起因し情報セキュリティに影響するものがリスクのため，R1～R6。変更管理に関する対策のため運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
12.1.3 容量・能力の管理	物理的	0	0	0	0	0	0	システム性能不足に起因するリスクであるため R1。調整，能力予測などが該当するため運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	0	0	0	0	0		
12.1.4 開発環境，試験環境及び運用環境の分離	物理的	1	1	1	1	1	0	ﾌｧｲﾙ/ｼｽﾃﾑ環境の不正な変更，ｼｽﾃﾑ不具合，運用環境への不正なｺｰﾄﾞの挿入，運用ﾃﾞｰﾀの不正な変更，要員の不正による情報漏えいなどがﾘｽｸのため，R1～R5。すべての対策に相当	
	技術的	1	1	1	1	1	0		
	人的	1	1	1	1	1	0		
	運用的	1	1	1	1	1	0		
12.2 マルウェアからの保護									
12.2.1 マルウェアに対する管理策	物理的	0	0	0	0	0	0	マルウェアの侵入によるリスクのため，R1～R5。技術的対応，その運用，人員への徹底のため，技術的，運用的及び人的対策に相当	
	技術的	1	1	1	1	1	0		
	人的	1	1	1	1	1	0		
	運用的	1	1	1	1	1	0		

12.3 バックアップ									
12.3.1 情報のバックアップ	物理的	0	1	0	0	0	1	データの消失がリスクのため，R2及びR6。バックアップ方針や運用，バックアップデータの物理的，技術的保護が該当するため，物理的，技術的及び運用的対策に相当	
	技術的	0	1	0	0	0	1		
	人的	0	0	0	0	0	0		
	運用的	0	1	0	0	0	1		
12.4 イベントログ取得									
12.4.1 イベントログ取得	物理的	0	0	0	0	0	0	各種活動や事象等の不記録により，不正の原因・証拠，ｲﾝｼﾃﾞﾝﾄを特定できないなどがﾘｽｸなので R6。ﾛｸﾞ取得の設定及び運用のため，技術的及び運用的対策に相当	
	技術的	0	0	0	0	0	1		
	人的	0	0	0	0	0	0		
	運用的	0	0	0	0	0	1		
12.4.2 ログ情報の保護	物理的	0	0	0	0	0	0	ログ情報の改ざん及び不正アクセスがﾘｽｸのため，R2 及び R3。技術的保護とその運用が対策として該当するから技術的及び運用的対策に相当	
	技術的	0	1	1	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	1	1	0	0	0		
12.4.3 実務管理者及び運用担当者の作業ログ	物理的	0	0	0	0	0	0	利用者の自己の特権の不正使用がリスクのため，R1～R4 及び R5。作業ログの保護とレビューが対策のため，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	0		
12.4.4 クロックの同期	物理的	0	0	0	0	0	0	不正確な監査ﾛｸﾞにより，証拠の信頼性を損なう，ｲﾝｼﾃﾞﾝﾄを特定できないなどがﾘｽｸのため R6。ｸﾛｯｸ同期を要求事項として文書化，その技術的保護のため技術的及び運用的対策に相当	
	技術的	0	0	0	0	0	1		
	人的	0	0	0	0	0	0		
	運用的	0	0	0	0	0	1		
12.5 運用ソフトウェアの管理									
12.5.1 運用システムに関わるソフトウェアの導入	物理的	0	1	0	0	0	0	運用システムの完全性侵害がリスクのため，R2。運用システムに関わるソフトウェアの変更管理，ソフトウェアの物理的保管のため，物理的，技術的及び運用的対策に相当	
	技術的	0	1	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	1	0	0	0	0		
12.6 技術的ぜい弱性管理									
12.6.1 技術的ぜい弱性の管理	物理的	0	0	0	0	0	0	技術的ぜい弱性の悪用がリスクであり，R1，R2，R3，R4 及び R5。ぜい弱性管理及び技術的対応のため，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	0		
12.6.2 ソフトウェアのインストールの制限	物理的	0	0	0	0	0	0	ｿﾌﾄｳｪｱのｲﾝｽﾄｰﾙ制限不足によりぜい弱性対策が不十分になることがﾘｽｸのため，R1，R2，R3，R4 及び R5。ｲﾝｽﾄｰﾙ制限のﾙｰﾙ化と利用者への徹底のため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	0		
	運用的	1	1	1	1	1	0		
12.7 情報システムの監査に対する考慮事項									
12.7.1 情報システムの監査に対する管理策	物理的	0	0	0	0	0	0	運用システム監査による業務プロセスの中断がリスクのため，R1。監査方法についての同意，監査のためのアクセスのログ取得などのため技術的及び運用的対策に相当	
	技術的	1	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	0	0	0	0	0		
H_8 合計		18	23	17	15	15	9		
H_8 影響値（合計/250）		0.04	0.05	0.04	0.03	0.03	0.02		

箇条 13 (H_9)　通信のセキュリティ									
13.1 ネットワークセキュリティ管理									
13.1.1 ネットワーク管理策	物理的	0	0	0	0	0	0	ネットワーク上の情報，及びネットワーク関連施設が適切に保護できないことがリスクのため，R1～R4 及び R5。ネットワーク及び施設の技術的保護及びその運用のため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	0		
13.1.2 ネットワークサービスのセキュリティ	物理的	0	0	0	0	0	0	ネットワークサービスの対策不十分による，ネットワーク上の情報，及びネットワーク関連施設の不十分な保護がリスクのため，R1～R4 及び R5。ネットワークサービスを正しく保つ運用のため，運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	0		
13.1.3 ネットワークの分離	物理的	1	1	1	1	1	0	ネットワーク上の情報，及びネットワーク関連施設が適切に保護できないことがリスクのため，R1～R4 及び R5。ネットワークの分離とその運用のため，物理的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	0		
13.2 情報の転送									
13.2.1 情報転送の方針及び手順	物理的	0	1	0	1	1	1	組織の内外部に転送した情報が適切に保護されないことがリスクのため R_2，R_4～R_6。手順化，責任の割り当て，暗号技術の適用，装置への物理アクセス制限のため，全ての対策が相当	
	技術的	0	1	0	1	1	1		
	人的	0	1	0	1	1	1		
	運用的	0	1	0	1	1	1		
13.2.2 情報転送に関する合意	物理的	0	0	0	0	0	0	対象リスクは，外部関係者との合意に基づかない情報転送により情報セキュリティリスクが顕在化するリスクであるため，R6。合意を事前に取ることが該当するため，0 とみなす。	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	0	0	0	1		
13.2.3 電子的メッセージ通信	物理的	0	0	0	0	0	0	電子的ﾒｯｾｰｼﾞ通信内の情報が脅かされることがリスクで，R2，R4～R6。認証強化，通信の保護，送付先指定の確実化，外部ｻｰﾋﾞｽ使用時の承認手続き化のため，技術的，人的及び運用的対策に相当	
	技術的	0	1	0	1	1	1		
	人的	0	1	0	1	1	1		
	運用的	0	1	0	1	1	1		
13.2.4 秘密保持契約又は守秘義務契約	物理的	0	0	0	0	0	0	外部関係者及び従業員により秘密情報が脅かされるリスクであり，R3，R5 及び R6。契約に掲載すべき要求事項の特定と文書化，それによる人員管理のため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	1	0	1	1		
	運用的	0	0	1	0	1	1		
H_9 合計		6	13	8	13	15	10		
H_9 影響値（合計/250）		0.01	0.03	0.02	0.03	0.03	0.02		
箇条 14 (H_{10})　システムの取得，開発及び保守									
14.1 情報システムのセキュリティ要求事項									
14.1.1 情報セキュリティ要求事項の分析及び仕様化	物理的	0	0	0	0	0	0	情報ｼｽﾃﾑの情報ｾｷｭﾘﾃｨ要求事項の仕様化が不十分なことによるﾘｽｸの顕在化も含めると R_1～R_6。要求事項の仕様化，及び供給者との契約への反映のため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
14.1.2 公衆ﾈｯﾄﾜｰｸ上のｱﾌﾟﾘｹｰｼｮﾝｻｰﾋﾞｽのｾｷｭﾘﾃｨの考慮	物理的	0	0	0	0	0	0	公衆ﾈｯﾄﾜｰｸを経由するｱﾌﾟﾘｹｰｼｮﾝｻｰﾋﾞｽに含まれる情報に対する不正行為，契約紛争，及び認可されない開示・変更がﾘｽｸのため，R2～R6。要求事項の考慮なので運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的		1	1	1	1	1		

14.1.3 ｱﾌﾟﾘｹｰｼｮﾝｻｰﾋﾞｽのﾄﾗﾝｻﾞｸｼｮﾝの保護	物理的	0	0	0	0	0	0	ｱﾌﾟﾘｹｰｼｮﾝｻｰﾋﾞｽのﾄﾗﾝｻﾞｸｼｮﾝに含まれる情報の不完全な通信，認可されない変更等がﾘｽｸのため R_2～R_6。ﾄﾗﾝｻﾞｸｼｮﾝの技術的保護と運用のため，技術的及び運用的対策に相当	
	技術的	0	1	1	0	1	1		
	人的	0	0	0	0	0	0		
	運用的	0	1	1	0	1	1		
14.2 開発及びサポートプロセスにおけるセキュリティ									
14.2.1 セキュリティに配慮した開発のための方針	物理的	0	0	0	0	0	0	情報システムの開発サイクルにおいて適切に情報セキュリティが設計，実施されないことによるリスクのため R_1～R_6。方針の作成とその徹底であるため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
14.2.2 システムの変更管理手順	物理的	0	0	0	0	0	0	開発ライフサイクルにおけるシステムの変更が適切に管理されないことに伴うリスクのため R_1～R_6。手順の作成とその徹底であるため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
14.2.3 ｵﾍﾟﾚｰﾃｨﾝｸﾞﾌﾟﾗｯﾄﾌｫｰﾑ変更後のｱﾌﾟﾘｹｰｼｮﾝの技術的ﾚﾋﾞｭｰ	物理的	0	0	0	0	0	0	ｵﾍﾟﾚｰﾃｨﾝｸﾞﾌﾟﾗｯﾄﾌｫｰﾑの変更に伴い，ｱﾌﾟﾘｹｰｼｮﾝの機能及び処理の完全性が損なわれることがﾘｽｸのため，R_1～R_5。変更に伴う技術ﾚﾋﾞｭｰの実施のため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1			
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	0		
14.2.4 パッケージソフトウェアの変更に対する制限	物理的	0	0	0	0	0	0	ﾊﾟｯｹｰｼﾞｿﾌﾄの変更による機能や処理の完全性失墜，業者の保障が得られなくなることがﾘｽｸであり，R_1～R_6。変更手続のﾙｰﾙ化，十分な技術的検証のため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
14.2.5 セキュリティに配慮したシステム構築の原則	物理的	1	1	1	1	1	1	システム構築で適切なセキュリティの配慮がなされないことに伴うリスクであり，R_1～R_6。システム構築手順の確立とその実装のため，物理的，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
14.2.6 セキュリティに配慮した開発環境	物理的	1	1	1	1	1	1	ｼｽﾃﾑ開発環境（要員，ﾌﾟﾛｾｽ，技術を含む）が適切に保たれないことに伴うﾘｽｸであるため R_1～R_6。開発環境の保護ﾚﾍﾞﾙの決定と構築，文書化，要員への徹底のため全ての対策に相当	
	技術的	1	1	1	1	1	1		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
14.2.7 外部委託による開発	物理的	0	0	0	0	0	0	外部委託先の開発活動で発生するリスク及び不適切なシステムが開発されるリスクであり，R_1～R_6。外部委託契約，受入れ試験，証拠の提出要求のため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
14.2.8 システムセキュリティの試験	物理的	0	0	0	0	0	0	システムセキュリティ試験の不備によりシステムにおいて顕在化する可能性のあるリスクで，R_1～R_6。試験実施のためのルール及び試験の実施であるから，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
14.2.9 システムの受入れ試験	物理的	0	0	0	0	0	0	システム受入れ時のチェックの不備によりシステムにおいて顕在化する可能性のあるリスクで，R_1～R_6。受入れ試験実施のルール化及び試験の実施のため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		

14.3 試験データ									
14.3.1 試験データの保護	物理的	0	0	0	0	1	0	適切な試験データが用いられないことによる情報漏えいがリスクであり，R5。運用ルール作成と技術的／物理的保護のため物理的，技術的及び運用的対策に相当	
	技術的	0	0	0	0	1	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	0	0	1	0		
H_{10} 合計		23	26	26	24	29	24		
H_{10} 影響値（合計/250）		0.05	0.05	0.05	0.05	0.06	0.05		
箇条 15 (H_{11})　供給者関係									
15.1 供給者関係における情報セキュリティ									
15.1.1 供給者関係のための情報セキュリティの方針	物理的	0	0	0	0	0	0	供給者による不適切な資産へのアクセスにより生じるリスクであり，R_1～R_6。文書化及び供給者との合意であるため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
15.1.2 供給者との合意におけるセキュリティの取扱い	物理的	0	0	0	0	0	0	供給者による不適切な行為により生じるリスクであり，R_1～R_6。文書化及び供給者との合意であるため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
15.1.3 ICT サプライチェーン	物理的	0	0	0	0	0	0	ICT サービス及び製品のサプライチェーンに関するリスクへの対応不足によるリスクであり，R_1及び R_6。文書化及び供給者との合意であるため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	0	0	0	0	1		
	運用的	1	0	0	0	0	1		
15.2 供給者のサービス提供の管理									
15.2.1 供給者のサービス提供の監視及びレビュー	物理的	0	0	0	0	0	0	供給者サービスの不備により顕在化する可能性のあるリスクで，R_1～R_6。監視しレビューすることであるから運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
15.2.2 供給者のサービス提供の変更に対する管理	物理的	0	0	0	0	0	0	供給者サービスの変更時の検討の不備により顕在化する可能性のあるリスクで，R_1～R_6。変更内容の検討であるため運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
H_{11} 合計		8	6	6	6	6	8		
H_{11} 影響値（合計/250）		0.02	0.01	0.01	0.01	0.01	0.02		
箇条 16 (H_{12})　情報セキュリティインシデント管理									
16.1 情報セキュリティインシデントの管理及びその改善									
16.1.1 責任及び手順	物理的	0	0	0	0	0	0	情報セキュリティインシデントがリスクであり，R_1～R_6。手順化と責務の明確化・周知のため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
16.1.2 情報セキュリティ事象の報告	物理的	0	0	0	0	0	0	情報セキュリティインシデント及びその報告が遅れることに伴うリスクであり，R_1～R_6。手順化と責務の明確化・周知のため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		

16.1.3 情報セキュリティ弱点の報告	物理的	0	0	0	0	0	0	情報セキュリティインシデントがリスクであり，R_1～R_6。弱点発見時の運用及びその周知のため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
16.1.4 情報セキュリティ事象の評価及び決定	物理的	0	0	0	0	0	0	情報セキュリティインシデントがリスクであり，R_1～R_6。情報セキュリティインシデントの定義に関するルール化であるため運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
16.1.5 情報セキュリティインシデントへの対応	物理的	0	0	0	0	0	0	情報セキュリティインシデントがリスクであり，R_1～R_6。手順の文書化，インシデント発生後の分析であるため技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
16.1.6 情報セキュリティインシデントからの学習	物理的	0	0	0	0	0	0	情報セキュリティインシデントがリスクであり，R_1～R_6。発生したインシデントを記録，分析すること，意識向上訓練につなげることであり，技術的，人的及び運用的対策に相当	
	技術的	1	1	1	1	1	1		
	人的	1	1	1	1	1	1		
	運用的	1	1	1	1	1	1		
16.1.7 証拠の収集	物理的	0	0	0	0	0	0	情報セキュリティインシデントがリスクであり，R_1～R_6。証拠の収集のルール化と実装のため運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
H_{12} 合計		13	13	13	13	13	13		
H_{12} 影響値（合計/250 ）		0.03	0.03	0.03	0.03	0.03	0.03		
箇条 17 (H_{13})　事業継続マネジメントにおける情報セキュリティの側面									
17.1 情報セキュリティ継続									
17.1.1 情報セキュリティ継続の計画	物理的	0	0	0	0	0	0	事業継続をさまたげるリスクであり，R_1 及び R_6。事業継続計画の策定であるため運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	0	0	0	0	1		
17.1.2 情報セキュリティ継続の実施	物理的	1	0	0	0	0	1	事業継続をさまたげるリスクであり，R_1 及び R_6。事業継続計画の実施であり，インシデント管理及びツールによる管理も含むため全ての対策に相当	
	技術的	1	0	0	0	0	1		
	人的	1	0	0	0	0	1		
	運用的	1	0	0	0	0	1		
17.1.3 情報セキュリティ継続の検証，ﾚﾋﾞｭｰ及び評価	物理的	0	0	0	0	0	0	事業継続をさまたげるリスクであり，R_1 及び R_6。事業継続計画の検証，レビュー及び評価であるため運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	0	0	0	0	1		
17.2 冗長性									
17.2.1 情報処理施設の可用性	物理的	1	0	0	0	0	1	情報処理施設の可用性をさまたげるリスクであり，R_1及びR_6。情報処理施設の物理的／技術的冗長化及び運用であるため物理的，技術的及び運用的対策に相当	
	技術的	1	0	0	0	0	1		
	人的	0	0	0	0	0	0		
	運用的	1	0	0	0	0	1		
H_{13} 合計		9	0	0	0	0	9		
H_{13} 影響値（合計/250）		0.02	0.00	0.00	0.00	0.00	0.02		

箇条 18 (H_{14})　順守									
18.1 法的及び契約上の要求事項の順守									
18.1.1 適用法令及び契約上の要求事項の特定	物理的	0	0	0	0	0	0	法的，規制又は契約上の義務に関する違反，及びセキュリティ上の要求事項に対する違反であり，R_3 ～R_6。要求事項の特定，文書化，順守であるため，人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	1	1	1	1		
	運用的	0	0	1	1	1	1		
18.1.2 知的財産権	物理的	0	0	0	0	0	0	知的財産権の侵害がリスクであり，R_6。知的財産権の特定，文書化，順守であるため人的及び運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	1		
	運用的	0	0	0	0	0	1		
18.1.3 記録の保護	物理的	0	1	1	1	1	0	記録の消失，破壊，改ざん，許可されていないアクセス及び不正な流出がリスクであり，R_2 ～R_5。記録の物理的／技術的保護，ルール化のため，物理的，技術的及び運用的対策に相当	
	技術的	0	1	1	1	1	0		
	人的	0	0	0	0	0	0		
	運用的	0	1	1	1	1	0		
18.1.4 プライバシー及び個人を特定できる情報（PII）の保護	物理的	0	0	0	0	1	1	プライバシーの侵害がリスクであり，R_5 及び R_6。ルール化と実装（技術的／物理的），順守であるため全ての対策に相当	
	技術的	0	0	0	0	1	1		
	人的	0	0	0	0	1	1		
	運用的	0	0	0	0	1	1		
18.1.5 暗号化機能に対する規制	物理的	0	0	0	0	0	0	暗号化機能に関する協定，法令及び規制の不履行であり，R_6。規制の順守であるため運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	0	0	0	0	0	1		
18.2 情報セキュリティのレビュー									
18.2.1 情報セキュリティの独立したレビュー	物理的	0	0	0	0	0	0	確実な運用のためのレビューであるため，全てのリスクが対象。レビューなので運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
18.2.2 情報ｾｷｭﾘﾃｨのための方針群及び標準の順守	物理的	0	0	0	0	0	0	方針群及び基準のレビューであるため，全てのリスクが対象。レビューなので運用的対策に相当	
	技術的	0	0	0	0	0	0		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
18.2.3 技術的順守のレビュー	物理的	0	0	0	0	0	0	情報システムのレビューであり，全てのリスクが対象。技術的レビューも含まれるため，技術的及び運用的対策に相当	
	技術的	1	1	1	1	1	1		
	人的	0	0	0	0	0	0		
	運用的	1	1	1	1	1	1		
H_{14} 合計		4	7	9	9	13	13		
H_{14} 影響値（合計/250）		0.01	0.01	0.02	0.02	0.03	0.03		

付録B 基本モデルのExcel 2010上での実装及び各種設定

(1) 基本モデルの実装

(1-1) 各種セルの説明

EXCEL 2010 上で実装された基本モデルを，各種セルの説明と共に図で示す。

	B	C	D	E	F	G	H	I	J	K	L
2	リスク		R1	R2	R3	R4	R5	R6	R7	ヘッジ策適用率 %	備考
3	リスクヘッジ策	リスクレベル値 / ヘッジコスト	7	6	8	7	9	8	6		
4	H1	500	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0	
5	H2	1000	0.06	0.06	0.06	0.06	0.06	0.06	0.03	0	
6	H3	1000	0.04	0.03	0.00	0.02	0.02	0.00	0.00	100	
7	H4	1500	0.10	0.10	0.09	0.10	0.10	0.09	0.02	100	
8	H5	2500	0.13	0.13	0.12	0.12	0.12	0.11	0.00	100	
9	H6	1000	0.02	0.02	0.02	0.02	0.02	0.02	0.00	100	
10	H7	5000	0.13	0.13	0.12	0.13	0.13	0.11	0.06	0	変化させるセル
11	H8	1500	0.11	0.11	0.08	0.11	0.11	0.07	0.02	100	
12	H9	1500	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0	
13	H10	2000	0.11	0.12	0.10	0.10	0.11	0.10	0.08	0	
14	H11	3000	0.02	0.03	0.02	0.02	0.03	0.02	0.02	100	
15	H12	1500	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0	
16	H13	2000	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0	
17	H14	1000	0.06	0.06	0.04	0.06	0.06	0.04	0.04	26	
18	リスク低減割合		0.45	0.45	0.41	0.44	0.44	0.41	0.17		
19	低減後リスク割合		0.55	0.55	0.59	0.56	0.56	0.59	0.83		
20	低減後リスク値		3.83	3.27	4.69	3.93	5.00	4.73	5.00	←[制約]リスク受容値以下	
21	リスク受容基準との差		1.17	1.73	0.31	1.07	0.00	0.27	0.00		
22	総コスト(組織の予算)		12000			コスト計				10755.05	←[制約]予算値以下
23	リスク受容値									5	
24	Σ(リスク受容基準－各低減後リスクレベル値)									4.55	←[目的]Maxにする

図 2　EXCEL 2010 上で実装された基本モデル

セルの説明：

- モデルで固定的に扱われる値（数値）
- モデルで変数として扱われる値，入力値（数値）
- モデルが導く解，入力値によって変化する（K4～K17：変化させるセル，K22：数式）
- 解を導くために算出される値（数式）
- その他情報提供用（文字列など）

(1-2) ソルバーのパラメータ設定

ソルバーのパラメータ設定画面の各種設定項目の値は次のとおりである。

[目的セルの設定] $K$24

[目標値] 最小値を選択

[変数セルの変更] $K$4:$K$17

[制約条件の対象]

$D$21 >= 0	K4>=0	K11>=0	K4<=100	K11<=100
$E$21 >= 0	K5>=0	K12>=0	K5<100	K12<100
$F$21 >= 0	K6>=0	K13>=0	K6<100	K13<100
$G$21 >= 0	K7>=0	K14>=0	K7<100	K14<100
$H$21 >= 0	K8>=0	K15>=0	K8<100	K15<100
$I$21 >= 0	K9>=0	K16>=0	K9<100	K16<100
$J$21 >= 0	K10>=0	K17>=0	K10<100	K17<100

[解決方法の選択] シンプレックス LP を選択

図 3　ソルバーのパラメータ設定画面

ソルバーパラメータ設定ウィンドウのオプション設定画面の各種設定は次のとおり。

[制約条件の制度] 0.000001（デフォルト値）

「自動サイズ調整を使用する」をチェック

[解決の制限／最大時間（秒）] 100（デフォルト値）

[解決の制限／反復回数] 100（デフォルト値）

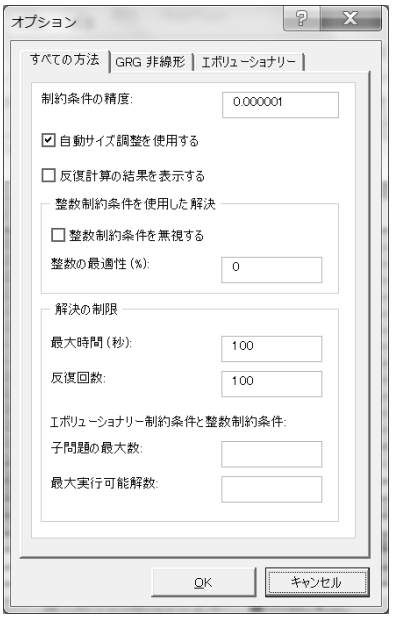


図 4　ソルバーパラメータ設定ウィンドウのオプション設定画面

(2) 数式の設定

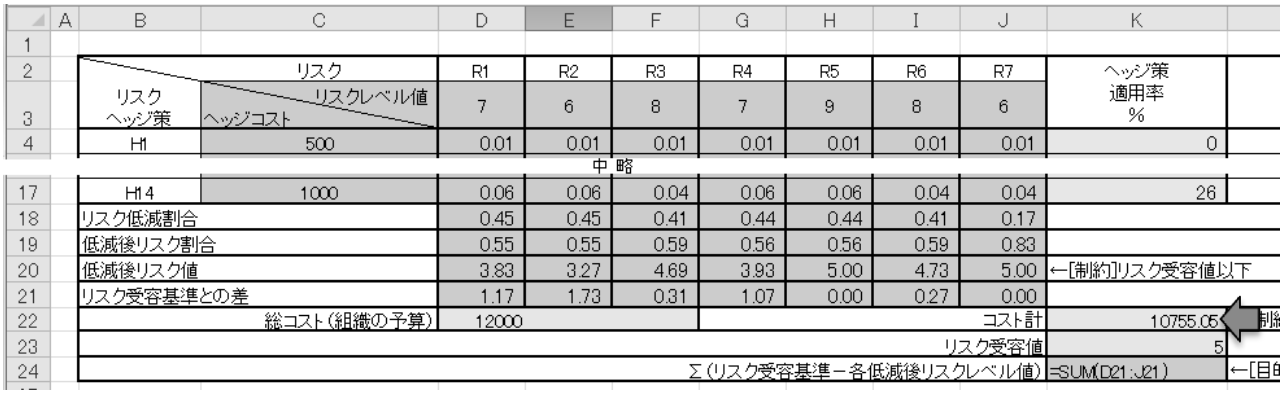
(2-1) 解を導くための各種値の算出式

リスク R_2 を例に，リスク低減割合（E18），低減後リスク割合（E19），低減後リスク値（E20），及び低減後リスク値のリスク受容基準との差（E21）を算出する数式の設定を図 5 において示す。

	A	B	C	D	E	F	G	H	I	J	K	
1												
2			リスク	R1	R2	R3	R4	R5	R6	R7	ヘッジ策適用率 %	
3		リスク ヘッジ策	リスクレベル値 ヘッジコスト	7	6	8	7	9	8	6		
4		H1	500	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0	
					中 略							
17		H14	1000	0.06	0.06	0.04	0.06	0.06	0.04	0.04	26	
18		リスク低減割合		0.45	=SUMPRODUCT(E4:E17,$K$4:$K$17)/(SUM(E4:E17)*100)	0.41	0.44	0.44	0.41	0.17		
19		低減後リスク割合		0.55	=IF(E19>=1,0,(1-E19))	0.59	0.56	0.56	0.59	0.83		
20		低減後リスク値		3.83	=E3*E20	4.69	3.93	5.00	4.73	5.00	←[制約]リスク受容値以	
21		リスク受容基準との差		1.17	=IF((E3-$K$24)<0,0,$K$24-E21)	0.31	1.07	0.00	0.27	0.00		
22		総コスト（組織の予算）		12000						コスト計	10755.05	←[制
23										リスク受容値	5	
24										Σ（リスク受容基準－各低減後リスクレベル値）	2.82	←[目

図 5　解を導くための各種値の算出式

また，ソルバーの目的関数を入力するセル（K24）の数式の設定を図 6 で示す。

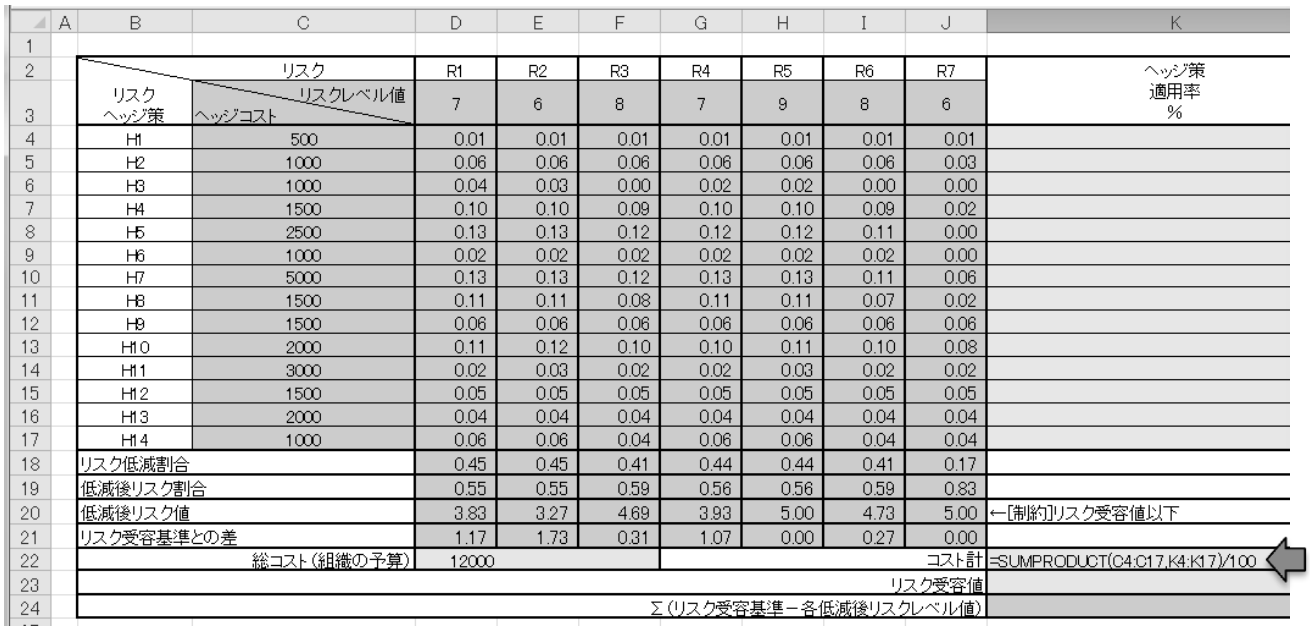


	A	B	C	D	E	F	G	H	I	J	K
1											
2			リスク	R1	R2	R3	R4	R5	R6	R7	ヘッジ策適用率 %
3		リスクヘッジ策	リスクレベル値 / ヘッジコスト	7	6	8	7	9	8	6	
4		H1	500	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0
			中略								
17		H14	1000	0.06	0.06	0.04	0.06	0.06	0.04	0.04	26
18		リスク低減割合		0.45	0.45	0.41	0.44	0.44	0.41	0.17	
19		低減後リスク割合		0.55	0.55	0.59	0.56	0.56	0.59	0.83	
20		低減後リスク値		3.83	3.27	4.69	3.93	5.00	4.73	5.00	←[制約]リスク受容値以下
21		リスク受容基準との差		1.17	1.73	0.31	1.07	0.00	0.27	0.00	
22		総コスト(組織の予算)		12000			コスト計				10755.05
23									リスク受容値		5
24									Σ(リスク受容基準－各低減後リスクレベル値)		=SUM(D21:J21)

図 6　ソルバーの目的関数

(2-2) 解の算出式

K4～K17 は，モデルの解を示すセルである。ソルバーが最適解を見つけるために，入力する数値を与えられた条件のもとで変化させるセルであるため，セルには数式ではなく数値が入力される。K22 は，選択されたリスクヘッジ策が実装される場合にかかる費用を示すセル。図 7 に数式を示す。



	A	B	C	D	E	F	G	H	I	J	K
1											
2			リスク	R1	R2	R3	R4	R5	R6	R7	ヘッジ策適用率 %
3		リスクヘッジ策	リスクレベル値 / ヘッジコスト	7	6	8	7	9	8	6	
4		H1	500	0.01	0.01	0.01	0.01	0.01	0.01	0.01	
5		H2	1000	0.06	0.06	0.06	0.06	0.06	0.06	0.03	
6		H3	1000	0.04	0.03	0.00	0.02	0.02	0.00	0.00	
7		H4	1500	0.10	0.10	0.09	0.10	0.10	0.09	0.02	
8		H5	2500	0.13	0.13	0.12	0.12	0.12	0.11	0.00	
9		H6	1000	0.02	0.02	0.02	0.02	0.02	0.02	0.00	
10		H7	5000	0.13	0.13	0.12	0.13	0.13	0.11	0.06	
11		H8	1500	0.11	0.11	0.08	0.11	0.11	0.07	0.02	
12		H9	1500	0.06	0.06	0.06	0.06	0.06	0.06	0.06	
13		H10	2000	0.11	0.12	0.10	0.10	0.11	0.10	0.08	
14		H11	3000	0.02	0.03	0.02	0.02	0.03	0.02	0.02	
15		H12	1500	0.05	0.05	0.05	0.05	0.05	0.05	0.05	
16		H13	2000	0.04	0.04	0.04	0.04	0.04	0.04	0.04	
17		H14	1000	0.06	0.06	0.04	0.06	0.06	0.04	0.04	
18		リスク低減割合		0.45	0.45	0.41	0.44	0.44	0.41	0.17	
19		低減後リスク割合		0.55	0.55	0.59	0.56	0.56	0.59	0.83	
20		低減後リスク値		3.83	3.27	4.69	3.93	5.00	4.73	5.00	←[制約]リスク受容値以下
21		リスク受容基準との差		1.17	1.73	0.31	1.07	0.00	0.27	0.00	
22		総コスト(組織の予算)		12000			コスト計				=SUMPRODUCT(C4:C17,K4:K17)/100
23									リスク受容値		
24									Σ(リスク受容基準－各低減後リスクレベル値)		

図 7　解の算出式

付録 C 表 6 のリスクヘッジ策と旧版（2005 年版）の ISO/IEC 27002（2006 年版の JIS Q 27002）管理策との対照表

リスクヘッジ策	ISO/IEC 27002:2013（JIS Q 27002:2014）の箇条	ISO/IEC 27002:2005（JIS Q 27002:2006）の管理策	
		管理策番号	項目
H_1	箇条 5	5.1.1	情報セキュリティ基本方針文書
		5.1.2	情報セキュリティ基本方針のレビュー
H_2	箇条 6	6.1.1	情報セキュリティに対する経営陣の責任
		6.1.2	情報セキュリティの調整
		6.1.3	情報セキュリティ責任の割当て
		6.1.4	情報処理設備の認可プロセス
		6.1.6	関係当局との連絡
		6.1.7	専門組織との連絡
		6.2.1	外部組織に関係したリスクの識別
		6.2.2	顧客対応におけるセキュリティ
		10.1.3	職務の分割
		11.7.1	モバイルのコンピューティング及び通信
		11.7.2	テレワーキング
H_3	箇条 7	8.1.1	役割及び責任
		8.1.2	選考
		8.1.3	雇用条件
		8.2.1	経営陣の責任
		8.2.2	情報セキュリティの意識向上、教育及び訓練
		8.2.3	懲戒手続
		8.3.1	雇用の終了関する責任
H_4	箇条 8	7.1.1	資産目録
		7.1.2	資産の管理責任者
		7.1.3	資産利用の許容範囲
		7.2.1	分類の指針
		7.2.2	情報のラベル付け及び取扱い
		8.3.2	資産の返却
		10.7.1	取外し可能な媒体の管理
		10.7.2	媒体の処分
		10.7.3	情報の取扱手順
		10.8.3	配送中の物理的媒体
H_5	箇条 9	8.3.3	アクセス権の削除
		11.1.1	アクセス制御方針
		11.2.1	利用者登録
		11.2.2	特権管理
		11.2.3	利用者パスワードの管理

		11.2.4	利用者アクセス権のレビュー
		11.3.1	パスワードの利用
		11.4.1	ネットワークサービスの利用についての方針
		11.5.1	セキュリティに配慮したログオン手順
		11.5.2	利用者の識別及び認証
		11.5.3	パスワード管理システム
		11.5.4	システムユーティリティの使用
		11.5.5	セッションのタイムアウト
		11.5.6	接続時間の制限
		11.6.1	情報へのアクセス制限
		11.6.2	取扱いに慎重を要するシステムの隔離
		12.4.3	プログラムソースコードへのアクセス制御
H_6	箇条 10	12.3.1	暗号による管理策の利用指針
		12.3.2	かぎ管理
H_7	箇条 11	9.1.1	物理的セキュリティ境界
		9.1.2	物理的入退管理策
		9.1.3	オフィス、部屋及び施設のセキュリティ
		9.1.4	外部及び環境からの保護
		9.1.5	セキュリティを保つべき領域での作業
		9.1.6	一般の人の立寄り場所及び受渡場所
		9.2.1	装置の設置及び保護
		9.2.2	サポートユーティリティ
		9.2.3	ケーブル配線のセキュリティ
		9.2.4	装置の保守
		9.2.5	構外にある装置のセキュリティ
		9.2.6	装置の安全な処分又は再利用
		9.2.7	資産の移動
		11.3.2	無人状態にある利用者装置
		11.3.3	クリアデスク・クリアスクリーン方針
H_8	箇条 12	10.1.1	操作手順書
		10.1.2	変更管理
		10.1.4	開発施設、試験施設及び運用施設の分離
		10.3.1	容量・能力の管理
		10.4.1	悪意のあるコードに対する管理策
		10.4.2	モバイルコードに対する管理策
		10.5.1	情報のバックアップ
		10.10.1	監査ログ取得
		10.10.3	ログ情報の保護
		10.10.4	実務管理者及び運用担当者の作業ログ
		10.10.5	障害のログ取得
		10.10.6	10.10.6 クロックの同期

		12.4.1	運用ソフトウェアの管理
		12.6.1	技術的ぜい弱性の管理
		15.3.1	情報システムの監査に対する管理策
H_9	箇条 13	6.1.5	秘密保持契約
		10.6.1	ネットワーク管理策
		10.6.2	ネットワークサービスのセキュリティ
		10.8.1	情報交換の方針及び手順
		10.8.2	情報交換に関する合意
		10.8.4	電子的メッセージ通信
		11.4.2	外部から接続する利用者の認証
		11.4.3	ネットワークにおける装置の識別
		11.4.4	遠隔診断用及び環境設定用ポートの保護
		11.4.5	ネットワークの領域分割
		11.4.6	ネットワークの接続制御
		11.4.7	ネットワークルーティング制御
H_{10}	箇条 14	10.3.2	システムの受入れ
		10.9.1	電子商取引
		10.9.2	オンライン取引
		10.9.3	公開情報
		12.1.1	セキュリティ要求事項の分析及び仕様化
		12.2.1	入力データの妥当性確認
		12.2.2	内部処理の管理
		12.2.3	メッセージの完全性
		12.2.4	出力データの妥当性確認
		12.4.2	システム試験データの保護
		12.5.1	変更管理手順
		12.5.2	オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー
		12.5.3	パッケージソフトウェアの変更に対する制限
		12.5.4	情報の漏えい
		12.5.6	外部委託によるソフトウェア開発
H_{11}	箇条 15	6.2.3	第三者との契約におけるセキュリティ
		10.2.1	第三者が提供するサービス
		10.2.2	第三者が提供するサービスの監視及びレビュー
		10.2.3	第三者が提供するサービスの変更に対する管理
H_{12}	箇条 16	13.1.1	情報セキュリティ事象の報告
		13.1.2	情報セキュリティ弱点の報告
		13.2.1	責任及び手順
		13.2.2	情報セキュリティインシデントからの学習
		13.2.3	証拠の収集
H_{13}	箇条 17	14.1.1	事業継続管理手続への情報セキュリティの組込み
		14.1.2	事業継続及びリスクアセスメント

		14.1.3	情報セキュリティを組み込んだ事業継続計画の策定及び実施
		14.1.4	事業継続計画策定の枠組み
		14.1.5	事業継続計画の試験、維持及び再評価
H_{18}	箇条 18	6.1.8	情報セキュリティの独立したレビュー
		10.7.4	システム文書のセキュリティ
		10.8.5	業務用情報システム
		10.10.2	システム使用状況の監視
		15.1.1	適用法令の識別
		15.1.2	知的財産権（IPR）
		15.1.3	15.1.3 組織の記録の保護
		15.1.4	個人データ及び個人情報の保護
		15.1.5	情報処理施設の不正使用防止
		15.1.6	暗号化機能に対する規制
		15.2.1	セキュリティ方針及び標準の順守
		15.2.2	技術的順守点検
		15.3.2	情報システムの監査ツールの保護

参考文献

1. JIS Q 27000:2014. 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 用語
2. ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements.
3. ISO/IEC 27005:2011. Information technology - Security techniques - Information security risk management.
4. The ISO Survey of Management System Standard Certifications – 2012, International Organization for Standardization (ISO), 2012, http://www.iso.org/iso/iso_survey_executive-summary.pdf, （参照 2014-06-17）
5. 認証取得組織数推移、認証機関別・県別認証取得組織数, 一般財団法人日本経済社会推進協会（JIPDEC） 情報マネジメントシステム推進センター, http://www.isms.jipdec.or.jp/lst/ind/suii.html, （参照 2014-11-27）
6. ISO/IEC 27000:2014, Information technology - Security techniques - Information security management systems - Overview and vocabulary
7. ISO/IEC 27002:2013, Information technology - Security techniques - Code of practice for information security controls
8. JIS Q 27001:2014, 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項
9. JIS Q 27002:2014 – 情報技術 – セキュリティ技術 – 情報セキュリティ管理策の実践のための規範
10. JIS Q 13335-1:2006, 情報技術 – セキュリティ技術 – 情報通信技術セキュリティマネジメント – 第 1 部：情報通信技術セキュリティマネジメントの概念及びモデル
11. ISO/IEC 13335-1:2004, Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management
12. ISO/IEC TR 13335-1:1996, Information technology - Guidelines for the management of IT Security - Part 1: Concepts and models for IT Security
13. ISO/IEC TR 13335-5:2001, Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security
14. TR X 0036-1:2001, IT セキュリティマネジメントのガイドライン – 第 1 部：IT セキュリティの概念及びモデル（廃止）
15. TR X 0036-5:2003, IT セキュリティマネジメントのガイドライン – 第 5 部：ネットワークセキュリティに関するマネジメントの手引（廃止）
16. ISO/IEC TR 13335-2:1997, Information technology - Guidelines for the management of IT Security - Part 2: Managing and planning IT Security
17. ISO/IEC TR 13335-3:1998, Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security

18. ISO/IEC TR 13335-4:2000, Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards
19. ISO/IEC 18028-1:2006, Information technology - Security techniques - IT network security - Part 1: Network security management
20. ISMS ユーザーズガイド, 2014, JIPDEC ISMS 適合性評価制度技術専門部会, https://contact.jipdec.or.jp/m?f=155 （入手 2014-11-20）
21. 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 –, 2008, http://www.isms.jipdec.or.jp/doc/JIP-ISMS113-21.pdf, （参照 2014-12-20）
22. ISO 31000:2009, Risk management - Principles and guidelines.
23. JIS Q 31000:2010, リスクマネジメント – 原則及び指針
24. ISO Guide 73:2009, Risk management - Vocabulary.
25. JIS Q 0073:2010, リスクマネジメント – 用語
26. IEC 31010:2009, Risk management - Risk assessment techniques
27. ISO/TR 31004:2013, Risk management - Guidance for the implementation of ISO 31000
28. JIS Q 31010:2012, リスクマネジメント – リスクアセスメント技法
29. 兵藤敏之; 中村逸一; 西垣正勝; 曽我正和, セキュリティ対策案選択問題のモデル化, 情報処理学会研究報告, 2003-CSEC-22 (35), 2003, pp.249-256
30. 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, 第 45 巻, No.8, 2003, pp.2022-2033.
31. 中村逸一; 兵藤敏之; 曽我正和; 西垣正勝, セキュリティ対策案選択問題のモデル化とその評価, 情報処理学会シンポジウム論文集, 第 2003 巻, No.15, 2003, pp.331-336
32. 情報セキュリティマネジメント標準（JIS X 5080:ISO/IEC 17799）の解説, 電子商取引推進協議会（ECOM）セキュリティ WG, 2002, http://www.jipdec.or.jp/archives/ecom/results/h13seika/h13results-10.pdf.（参照 2014-12-20）
33. 加藤岳久; 上松晴信; 名坂浩平; 西垣正勝, 教育効果を考慮した情報セキュリティ対策の統合型選定方式の提案, マルチメディア, 分散, 協調とモバイルシンポジウム（DICOMO2012）論文集, 石川県加賀市, 2012-07-04/06, 情報処理学会, 2012, pp.788-797
34. 加藤岳久; 山本匠; 西垣正勝, 教育効果を考慮したセキュリティ対策選定手法の検討, マルチメディア, 分散, 協調とモバイルシンポジウム（DICOMO2011）論文集, 京都府宮津市, 2011-07-06/08, 情報処理学会, 2011, pp.135-140
35. 臼井佑真; 山本匠; 間形文彦; 勅使河原可海; 佐々木良一; 西垣正勝, 訴訟リスクを考慮した情報セキュリティ対策選定方式に関する検討, コンピュータセキュリティシンポジウム 2009（CSS2009）論文集, 富山市, 2009-10-26/28, 情報処理学会　コンピュータセキュリティ研究会（CSEC）, pp.105-110. https://ipsj.ixsq.nii.ac.jp/ej/index.php?active_action=repository_view_main_item_detail&item_id=74884&item_no=1&page_id=13&block_id=8.
36. 西垣正勝; 臼井佑真; 山本匠; 間形文彦; 勅使河原可海; 佐々木良一, 賠償リスクを考慮した情報セキュリティ対策選定方式の提案と評価, 情報処理学会論文誌, 第 52 巻, No.3, 2011, pp.1173-1184

37. 永井康彦; 藤山達也; 佐々木良一, セキュリティ対策目標の最適決定技法の提案, 情報処理学会論文誌, 第 41 巻, No.8, 2000, pp.2264-2271
38. 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, 第 43 巻, No.8, 2002, pp.2435-2446
39. 臼井佑真; 間形文彦; 勅使河原可海; 佐々木良一; 西垣正勝, 事象分割型 FTA を用いたセキュリティ対策評価モデルの提案, 暗号と情報セキュリティシンポジウム（SCIS2008）, 4B1−4, 宮崎市, 2008-01-22/25,
40. 情報処理実態調査 平成 25 年調査関係資料, 経済産業省, 2014, http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/h25jyojitsu.html （参照 2014-06-09）
41. 情報セキュリティポリシーに関するガイドライン, 内閣官房情報セキュリティセンター（NISC), 情報セキュリティ対策推進会議, 2000, http://www.kantei.go.jp/jp/it/security/taisaku/pdfs/ISP_Guideline.pdf （参照 2014-06-09）
42. 中山弘隆; 谷野哲三, 多目的計画法の理論と応用, 計測自動制御学会, コロナ社, 1994
43. 中山弘隆; 三谷克之輔; 吉田太, 多目的計画法による飼料配合支援システム, オペレーションズリサーチ, 第 38 巻, No.9, pp.499-502, 1993
44. Kawasaki (Aiba) Ritsuko, Hiromatsu Takeshi. Proposal of a Model Supporting Decision-Making on Information Security Risk Treatment, International Science Index 88, International Journal of Computer, Information, Systems and Control Engineering. World Academy of Science, Engineering and Technology (WASET), Vol. 8, No.4, pp.545 - 551, 2014
45. Kawasaki (Aiba) Ritsuko; HiromatsuTakeshi, Proposal of a Model Supporting Decision-Making Based On Multi-Objective Optimization Analysis on Information Security Risk Treatment. International Science Index 89, International Journal of Computer, Information, Systems and Control Engineering, World Academy of Science, Engineering and Technology （WASET), Vol.8, No.5, pp.756-762, 2014