情報処理学会論文誌 Vol.60 No.1 250–259 (Jan. 2019)

「関係の合成」の概念を用いた ISMSとITSMSにおけるリスクアセスメントの統合

松村 宣顕[1,a)] 長谷川 孝博[1]

受付日 2018年4月9日, 採録日 2018年10月2日

概要：本論文では，情報セキュリティマネジメントシステム（ISMS：Information Security Management System）とITサービスマネジメントシステム（ITSMS：IT Service Management System）の新しい統合リスクアセスメント方法を提案する．一般的に，組織がISMSとITSMSのような複数のISO（International Organization for Standardization）マネジメントシステムを運用する場合，作業量は増大する．筆者らは，複数のISOマネジメントシステムを，現実的に十分機能させるためには，運用の省力化が課題であると考える．提案方法は，ISMSのリスクアセスメントで特定した「リスクと資産の関係」と「資産とITサービスの関係」とを合成することにより，ISMSとITSMSのリスクアセスメントを統合する．構成員約12,000名の国立大学の情報系センターにおいて提案方法を適用した．結果，提案方法は，ISMSとITSMSの要求事項に適合した．そして，両マネジメントシステムに対する共通のリスクアセスメントアプローチの採用により，提案方法はリスクアセスメントの所要時間を従来方法と比較して約24%削減した．提案方法は，組織の人員や予算などのリソースが限られるなかで，ISMSとITSMSのリスクアセスメントに関する業務効率の向上と，運用の省力化に貢献すると考えられる．

キーワード：ISMS，ITSMS，リスクアセスメント，統合マネジメントシステム，リスクマトリックス法，関係の合成

Integration of the Risk Assessment for an Information Security Management System and that for an IT Service Management System Using Composition of Relations

Noriaki Matsumura[1,a)] Takahiro Hasegawa[1]

Received: April 9, 2018, Accepted: October 2, 2018

Abstract: Generally, when an organization operates multiple ISO (International Organization for Standardization) management systems such as an information security management system (ISMS) as specified in ISO/IEC 27001 and an IT service management system (ITSMS) as specified in ISO/IEC 20000-1, workloads relating to management systems operation will increase. Here, we describe a novel risk assessment method that composes the relation from risks to assets and the relation from assets to IT services. By utilizing this composition method, we can reduce the workloads relating to the risk assessments for both management systems. We applied the method to the information system department at a national university with approximately 12,000 members. The result shows that it satisfies the requirements specified in both management systems and can reduces approximately 24% of time required for the risk assessment.

Keywords: ISMS, ITSMS, risk assessment, integrated management system, risk matrix technique, composition of relations

1. はじめに

情報技術（IT：Information Technology）は社会基盤となり，技術革新は日進月歩である．社会では多様なITサー

[1] 静岡大学情報基盤センター
Center for Information Infrastructure, Shizuoka University, Hamamatsu, Shizuoka 432–8561, Japan
[a)] matsumura.noriaki@shizuoka.ac.jp

ビスが提供され，ユーザの利活用方法も進化している．ITに関する環境が大きく変化し続けるなかで，組織はセキュリティやITサービスを適切に管理する必要がある．国際標準化機構（ISO：International Organization for Standardization）は，このための枠組みを提供している．情報セキュリティマネジメントシステム（ISMS：Information Security Management System）は，組織における情報セキュリティを管理するための枠組みである．ITサービスマネジメントシステム（ITSMS：IT Service Management System）はITサービスを効果的に管理するための枠組みである．情報セキュリティリスクを最小限に抑えることを目的とするISMSとITサービスの品質やユーザ満足度の向上に貢献するITSMSは，ITサービス事業者などの組織にとり，情報戦略における「守り」と「攻め」の両輪であるといえる．

一般財団法人日本情報経済社会推進協会（JIPDEC）によれば，2018年03月01日現在，日本国内におけるISMS認証取得組織は5,488組織である[1]．また，ITSMS認証取得組織は210組織である[2]．ISMSとITSMSは，営利組織が認証取得することが多いが，近年では，非営利組織が認証取得する事例も増えてきており，両マネジメントシステムを認証取得する組織が多様化してきている．たとえば，非営利組織である学術組織による認証も増えている．文部科学省による平成29年度の学校基本調査の結果によると日本の大学数は780校であり，国立大学は86校である[3]．JIPDECの認証取得組織検索システム[4]によれば，ISMSを認証取得している国立大学は14校あり，このうち2校はITSMSもあわせて認証取得している．

ISMSとITSMSのような複数のISOマネジメントシステムを認証取得し運用する場合，個別のISOマネジメントシステムを認証取得し運用する場合と比較して，運用に関わる作業量は増大する．ここで，マネジメントシステム間の整合性をとらないと，多重に管理手順が発生し，業務効率が悪化する．人員や予算などのリソースが限られるなかで，複数のISOマネジメントシステムを現実的に十分機能させるためには，筆者らは，ISOマネジメントシステム運用の省力化が課題であると考えている．

ISMSとITSMSについては，ISO/IEC 27013:2015情報技術—セキュリティ技術—ISO/IEC 27001およびISO/IEC 20000-1の統合実装に関するガイダンス[5]が発行されており，ISO/IEC 27013:2015の4.4で，情報セキュリティマネジメントとサービスマネジメントは，非常に類似したプロセスおよび活動に取り組む旨指摘している．そして共有部分としてリスクアセスメント，情報セキュリティ管理，サービス継続および可用性管理などをあげている．

そこで，本論文では，ISMSとITSMSの運用省力化のために，統合リスクアセスメント方法（以下，提案方法）を提案する．提案方法は，ISMSのリスクアセスメントとITSMSのリスクアセスメントを統合し，両マネジメントシステムのリスクアセスメントに関する業務効率を向上し，運用を省力化する．

本論文の構成は，以下のとおりである．2章ではISOマネジメントシステムにおける統合マネジメントおよびリスクアセスメントについて概観し，3章で関連研究について述べる．4章で提案方法の詳細について述べ，5章で提案方法を実装したプロトタイプシステムについて説明する．6章では，提案方法を構成員約12,000名の国立大学の情報系センター（以下，センター）において適用した結果を示し，考察する．最後に7章で本論文をまとめ，今後の展望を述べる．

2. 統合マネジメントおよびリスクアセスメント

2.1 統合マネジメント

ISMSは2013年に大きく改正され，ISO/IEC 27001:2013[6]が発行された．この改正の趣旨は次のとおりである．

- 基本的には，ISO/IEC 27001:2005を継承する．
- ISO/IEC専門業務用指針第1部及び統合版ISO補足指針[7]の附属書SL（以下，附属書SL）を適用し，附属書SLのAppendix2「上位構造，共通の中核となるテキスト，共通用語及び中核となる定義」に基づき改正した．附属書SLを適用した他のISOマネジメントシステムとの整合性を確保する．
- 汎用的なリスクマネジメントに関する国際規格であるISO 31000:2009[8]を適用する．
- 通信分野，金融分野，クラウドコンピューティングサービス事業などの分野別ISMS認証制度の要請に対応できるように，要求事項を修正する．

ISO/IEC 27001:2013は，附属書SLを適用したため，附属書SLを適用した他のISOマネジメントシステムとの統合マネジメントシステムの実装と運用について考慮されている．一方，ITSMSの要求事項を定義するISO/IEC 20000-1:2011[9]は，附属書SLを適用していない．しかしながら，サービスマネジメントシステム要求事項（0.2）でISO/IEC 27001に基づく情報セキュリティマネジメントシステムと統合することができると例示している．さらに，前述のように，ISO/IEC 27013:2015情報技術—セキュリティ技術—ISO/IEC 27001およびISO/IEC 20000-1の統合実装に関するガイダンスが発行されており，ISO/IEC 27001:2013とISO/IEC 20000-1:2011の統合マネジメントシステムの実装と運用は可能である．

2.2 リスクアセスメント

ISO/IEC 27001:2013は，主な用語の定義をISO/IEC 27000:2014[10]に求めており，ISO/IEC 27000:2014ではリスクアセスメントを「リスク特定，リスク分析およびリス

表 1 用語の比較：リスクアセスメント
Table 1 Comparison of the term: Risk assessment.

ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
2.7.1 overall process (2.61) of risk identification (2.75), risk analysis (2.70) and risk evaluation (2.74) [ISO Guide 73:2009]	Not defined	References in ISO/IEC 20000-1 are to the risk assessment related to services. For example: Clause 4.5.3: (Implement and operate the SMS(Do)) includes "…d) identification, assessment and management of risks to the services:" Clause 5.2 (Plan new or changed services) includes f) identification, assessment and management of risks; Clause 6.6.1: "d) ensure that information security risk assessments are conducted at planned intervals;"

ク評価のプロセス全体」と定義している．これは，リスクマネジメントに関する用語を定義する ISO Guide73:2009 [11] に基づいている．ISO/IEC 27001:2013 の 6.1.2 は，情報セキュリティリスクアセスメントの要求事項を示している．ISO/IEC 27001:2013 の 6.1.2 c) 1) では，「ISMS の適用範囲内における情報の機密性，完全性及び可用性の喪失に伴うリスクを特定する」ことを要求している．そして，特定されたリスクに対して，ISO/IEC 27001:2013 の 6.1.2 d) と 6.1.2 e) でリスク分析とリスク評価を要求している．ISO/IEC 27001:2013 の 6.1.2 は，記述レベルを ISO 31000:2009 に合わせたため，ISO/IEC 27001:2005 の資産，脅威，脆弱性などによる詳細なリスクアセスメントプロセスの記述ではなくなっている．

ISO/IEC 20000-1:2011 は，リスクアセスメントを明確に定義していない．関連する記述として，ISO/IEC 27013:2015 の附属書 B は次をあげている．

- 4.5.3 SMS（Service Management System）の導入及び運用（Do）
  d) サービスに対するリスクの特定，アセスメント及び管理
- 5.2 新規サービス又はサービス変更の計画
  f) リスクの特定，アセスメント及び管理
- 6.6.1 情報セキュリティ基本方針
  d) 情報セキュリティリスクアセスメントを，あらかじめ定めた間隔で実施することを確実にする．

表 1 に ISO/IEC 27013:2015 の附属書 B における，ISO/IEC 27000:2014 と ISO/IEC 20000-1:2011 のリスクアセスメントの比較表 [12] を示す．

3. 関連研究

IT 分野における ISO マネジメントシステムの統合に関連した先行研究としては，ISMS と ITSMS の統合化に向けた効果的な情報共有方法の提案 [13]，ISMS と事業継続マネジメントシステム（BCMS：Business Continuity Management Systems）の統合手法の提案 [14] などがある．しかしながら，これまでに ISMS と ITSMS の統合リスクアセスメント方法についての研究は報告されていない．

個別のリスクアセスメント方法自体については，定性的，半定量的または定量的の多くの方法が提案，実用されている．たとえば，年間予想損失額を求める ALE（Annual Loss Expectancy）法 [15]，リスクマトリックス法 [16], [17]，事業影響度分析法 [18] などがあげられる．汎用的なリスクマネジメントに関する国際規格である ISO 31000:2009 の支援規格 IEC/ISO 31010:2009 [19] の附属書には，31 種類のリスクアセスメント技法が説明されている．

JIPDEC は，ISMS におけるリスクアセスメント方法として，前述した個別のリスクアセスメント方法のうちリスクマトリックス法に基づいた方法を ISMS ユーザーズガイド-JIS Q 27001:2014（ISO/IEC 27001:2013）対応（以下，ISMS ユーザーズガイド）で説明している [20], [21], [22]．ここで，リスク源は「情報及び情報に関連する資産（以下，資産として総称），脅威，脆弱性」としている．提案方法は，この ISMS ユーザーズガイドの方法を基に「関係の合成」の概念を用いて ISMS と ITSMS におけるリスクアセスメントを統合する．

1 章および 2 章で示した ISO/IEC 27013:2015 は，重複を避けるために，ISO/IEC 27001 と ISO/IEC 20000-1 の両マネジメントシステムに対して，リスクアセスメントを含む共通のリスクマネジメントアプローチを採用することは効率的である旨指摘している [23]．本章で示したように，ISMS と ITSMS の統合リスクアセスメント方法の研究はこれまでに報告されていない．そこで，本論文では，ISMS ユーザーズガイドのリスクアセスメント方法を基に，ISMS と ITSMS の両マネジメントシステムを認証取得している組織を対象とした，統合リスクアセスメント方法を提案する．

4. 統合リスクアセスメント方法

本章では，提案方法について詳しく説明する．提案方法は，「関係の合成」の概念を ISMS と ITSMS の統合リスクアセスメントに応用する．

4.1 前提

文献 [24] には，「ISMS 全般の内，ITSMS に関連する組織や活動を ITSMS のインフラとして位置付け，その上位に各サービスに必要なプロセスを適切に管理しながら ITSMS を構築していくことが，効果的」とある．提案方法では，IT サービスは ISMS の適用範囲内にある資産によってのみ構成し，ISMS の資産価値の算定基準に ITSMS の資産価値算定の考え方を織り込むため ISMS と ITSMS の資産

価値の算定基準は同一であるという前提をおく．

4.2 関係の合成

数学における「関係の合成」は，与えられた関係から新たな関係を構成する概念であり，次のように説明される．

A，B，C を集合とし，R を A から B への関係，S を B から C への関係とする．すなわち，R は $A \times B$ の部分集合，S は $B \times C$ の部分集合である．このとき，R と S から $R \circ S$ によって表される A から C への関係が次のように定められる：

ある $b \in B$ に対して aRb かつ bSc ならば $a(R \circ S)c$

すなわち，

$$R \circ S = \{(a,c) \mid \text{ある } b \in B \text{ が存在して } (a,b) \in R \text{ かつ } (b,c) \in S\}$$

この関係 $R \circ S$ は R と S の合成（composition）とよばれる [25]．

4.3 概念

ここでは，従来方法と提案方法の概念について説明する．資産を a_i（$i = 0,\ldots,n-1$），IT サービスを s_j（$j = 0,\ldots,m-1$），リスクを $r_{i,k}$（$i = 0,\ldots,n-1$；$k = 0,\ldots,\ell-1$）とする．ここで，n は資産の数，m は IT サービスの数，ℓ は i 番目の資産に関係するリスクの数を表す．概念説明のため，組織は適用範囲に，資産の集合 A，IT サービスの集合 S を保有運用していることにする．ここで，集合 A，S をそれぞれ，

$$A = \{a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\},$$
$$S = \{s_0, s_1, s_2\}$$

とする．

従来方法では，ISMS は資産（a_i）ベースのリスクアセスメント方法（RAM_0）を実施する．ITSMS は IT サービス（s_j）ベースのリスクアセスメント方法（RAM_1）を実施する．RAM_0 は資産（a_i）を，RAM_1 は IT サービス（s_j）に着目するリスクアセスメント方法であるため，原理的な整合性はない．または，それぞれの結果をふまえて，整合性に問題がないかレビューする必要がある．

提案方法は，まず，1）従来方法と同じ資産（a_i）ベースのリスクアセスメント方法（RAM_0）を行う．提案方法では，RAM_0 として，ISMS ユーザーズガイドのリスクマトリックス法に基づくリスクアセスメントを行う．このとき，リスク特定により，リスク（$r_{i,k}$）と資産（a_i）の関係が定義される．次に，2）IT サービス（s_j）ベースのリスクアセスメント方法（RAM_1）は行わず，A と S を関係 L（*LINK*，リンク）で定義する．このとき，「関係の合成」が得られ，リスク（$r_{i,k}$）から IT サービス（s_j）への関係が定められる．リスクアセスメント方法には RAM_0 のみを用いるため，従来方法のような整合性のレビューを必要としない．

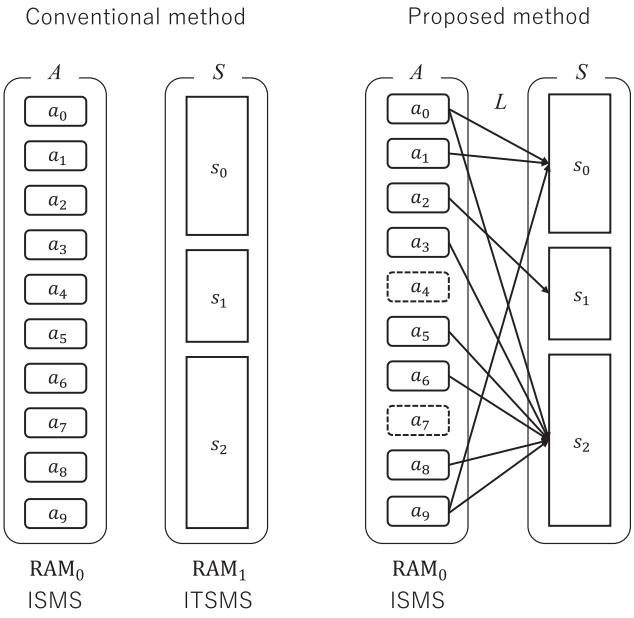


図 1 従来方法と提案方法の概念比較図

Fig. 1 Concept comparison diagram of conventional method and proposed method.

図 1 に従来方法と提案方法の概念比較図を示す．提案方法における a_4 と a_7 は IT サービス（s_j）と関係が定義されていない資産（a_i）であり，ITSMS 上は重要でなくとも，ISMS 上は無視できない資産（a_i）であることを示す．a_2 は s_1 との関係のみ定義されており，「資産 a_2 のみで 1 つの IT サービス s_1 を構成している」または「IT サービス s_1 は資産 a_2 のみで提供されている」ことを表す．s_2 は最も多くの資産（a_i）と関係が定義されているため，個別資産（a_i）の障害の影響を受けやすい IT サービス（s_j）である．複数の資産（a_i）を運用するためのコストに注意を払うべきである．a_0 と a_9 は複数の IT サービス（s_j）と関係が定義されている．個別資産（a_i）の障害が，複数の IT サービス（s_j）に影響を及ぼすため，特に注意を要する資産（a_i）である．

4.4 リスク特定

提案方法では，まず，1）RAM_0 を実施する．資産（a_i）を特定し，脅威・脆弱性を明確化する．そしてリスク（$r_{i,k}$）を特定する．資産の集合 A に関係して特定されたリスク（$r_{i,k}$）の集合を R とすると，

$$R = \{r_{0,k}, r_{1,k}, r_{2,k}, r_{3,k}, r_{4,k}, r_{5,k}, r_{6,k}, r_{7,k}, r_{8,k}, r_{9,k}\}$$

となる．また，この作業より，R と A の関係 L' が定義される．関係 L' は，

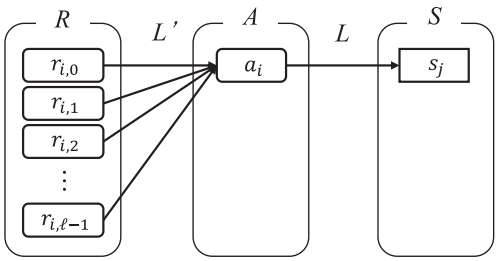


図 2 リスク（$r_{i,k}$），資産（a_i），IT サービス（s_j）の関係図
Fig. 2 Arrow diagram of risks ($r_{i,k}$), assets (a_i), and IT services (s_j).

$$L' = \{(r_{0,k}, a_0), (r_{1,k}, a_1), (r_{2,k}, a_2), (r_{3,k}, a_3), (r_{4,k}, a_4), (r_{5,k}, a_5), (r_{6,k}, a_6), (r_{7,k}, a_7), (r_{8,k}, a_8), (r_{9,k}, a_9)\}$$

である．

次に，2）A と S の関係 L を定義する．関係 L は図 1 より，

$$L = \{(a_0, s_0), (a_0, s_2), (a_1, s_0), (a_2, s_1), (a_3, s_2), (a_5, s_2), (a_6, s_2), (a_8, s_2), (a_9, s_0), (a_9, s_2)\}$$

となる．

このとき，関係 L' と L の合成 $L' \circ L$ が得られる．

$$L' \circ L = \{(r_{0,k}, s_0), (r_{0,k}, s_2), (r_{1,k}, s_0), (r_{2,k}, s_1), (r_{3,k}, s_2), (r_{5,k}, s_2), (r_{6,k}, s_2), (r_{8,k}, s_2), (r_{9,k}, s_0), (r_{9,k}, s_2)\}$$

ここで，関係 L' と L の合成により，資産（a_i）のリスク（$r_{i,k}$）は，資産（a_i）が関係する IT サービス（s_j）のリスクと定められる．

図 1 における IT サービス（s_0，s_1，s_2）のリスク（$r_{i,k}$）の集合を，それぞれ R_0，R_1，R_2 とすると，R_0，R_1，R_2 は R の部分集合であり，

$$R_0 = \{r_{0,k}, r_{1,k}, r_{9,k}\}$$
$$R_1 = \{r_{2,k}\}$$
$$R_2 = \{r_{0,k}, r_{3,k}, r_{5,k}, r_{6,k}, r_{8,k}, r_{9,k}\}$$

となる．

リスク（$r_{i,k}$）から資産（a_i）への関係，資産（a_i）から IT サービス（s_j）への関係の概念図を**図 2** に示す．

4.5 リスク分析

提案方法では，RAM_0 を実施し，特定されたリスク（$r_{i,k}$）のアセスメントを行い，リスクレベルを決定する．ここでは，資産（a_i）が有する機密性，完全性，可用性のそれぞれのリスクレベルを計算する．リスク特定で明確になった，資産価値，脅威の大きさ，脆弱性の度合いを用いて，リスクレベルを次式で算定する．

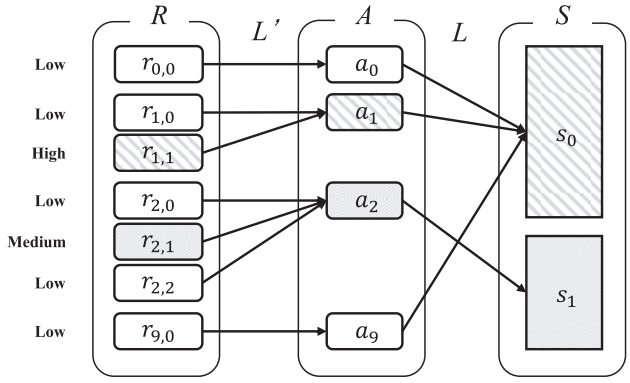


図 3 リスク（$r_{i,k}$），資産（a_i），IT サービス（s_j）のリスク評価例
Fig. 3 An example of risk evaluation for risks ($r_{i,k}$), assets (a_i), and IT services (s_j).

$$RL = AV \times TL \times VL \quad (1)$$

ここで，RL はリスクレベル，AV は資産価値，TL は資産に対する脅威レベル（脅威の大きさ），VL は資産が有する脅威に対する脆弱性レベル（脆弱性の度合い）であり，AV は以下の条件により定まる．

リスク区分 = 機密性（C：Confidentiality） なら
　AV = 機密性に関する資産価値
リスク区分 = 完全性（I：Integrity） なら
　AV = 完全性に関する資産価値
リスク区分 = 可用性（A：Availability） なら
　AV = 可用性に関する資産価値

とする．

4.6 リスク評価

提案方法では，まず，1）RAM_0 を実施する．リスク分析で，式 (1) を用いて算定したリスク（$r_{i,k}$）のリスクレベルと事前に確立したリスク受容基準を比較する．ここで，リスク受容基準はリスクレベルで体現するため，リスク評価は絶対評価である．リスク対応のために，分析したリスク（$r_{i,k}$）の優先順位付けを行う．次に，2）IT サービス（s_j）のリスク評価を実施する．ここで，IT サービス（s_j）のリスク評価は次の評価法に基づく．

(i) 特定された資産（a_i）のリスク（$r_{i,k}$）のうち，最もリスクが高い評価を資産（a_i）のリスク評価とする．
(ii) IT サービス（s_j）と関係 L で定義された資産（a_i）のリスク評価のうち，最もリスクが高い評価を IT サービス（s_j）のリスク評価とする．

図 3 にリスク評価例を示す．a_0 と関係が定義された $r_{0,0}$ はリスクレベル算定およびリスク評価の結果「低（Low）」とする．よって，a_0 は「低（Low）」となる．a_1 と関係が定義された $r_{1,0}$ はリスクレベル算定およびリスク評価の結果「低（Low）」とし，$r_{1,1}$ は「高（High）」とする．よっ

図 4 トップ画面の例．RISKMS：ISMS・ITSMS 統合管理システム

Fig. 4 An example of “Top” screen. RISKMS: The integrated management system for ISMS and ITSMS.

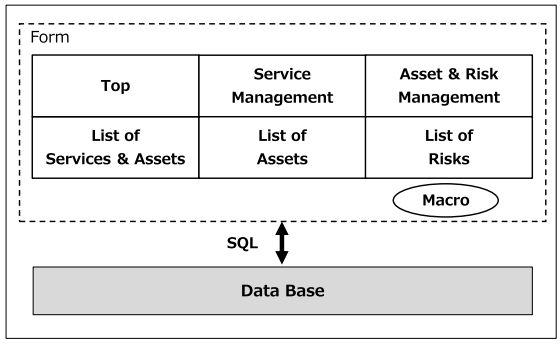


図 5 概略図．RISKMS：ISMS・ITSMS 統合管理システム

Fig. 5 Schematic diagram. RISKMS: The integrated management system for ISMS and ITSMS.

て，a_1 は $r_{1,0}$，$r_{1,1}$ のリスク評価のうちリスクが高い評価とし「高（High）」となる．同様の処理を行い，a_2 は「中（Medium）」，a_9 は「低（Low）」となる．s_0 は，a_0，a_1，a_9 でサービスが提供されている．関係が定義された資産（a_i）のリスク評価のうち，最もリスクが高い評価を IT サービス（s_j）のリスク評価とするため，s_0 は「高（High）」となる．同様に，s_1 は「中（Medium）」となる．

5. プロトタイプ実装

本章では，提案方法を実現する ISMS・ITSMS 統合管理システムのプロトタイプ（以下，RISKMS）について説明する．RISKMS の実装には，コッドが考案した関係モデル [26] に基づいた関係データベースを用いる．

5.1 システム概要

関係データベース管理システムを使用し，RISKMS を実装した．**図 4** に RISKMS のトップ画面の例を示す．トップ画面は，ISMS と ITSMS に関するリスク（$r_{i,k}$）のサマリ情報を表示する．「IT サービス一覧」では，IT サービス（s_j）名，IT サービス（s_j）と関係が定義された資産（a_i）数，IT サービス（s_j）のリスク評価などを表示する．「リスク情報」には，リスク特定で明確化した，資産価値，脅威・脆弱性などのリスク情報を表示する．

RISKMS は，トップ画面を含めて，主に 6 画面で構成する．次に 6 画面の機能概要を示す．

- トップ画面［Top］
  ISMS と ITSMS に関するリスク（$r_{i,k}$）のサマリ情報を表示する．
- サービス管理画面［Service Management］
  IT サービス（s_j）の情報を入力し，資産（a_i）と IT サービス（s_j）の関係を定義する．
  〈A と S の関係 L の定義〉
- 資産リスク管理画面［Asset & Risk Management］
  資産（a_i）情報を入力し，資産（a_i）に関係する脅威・脆弱性を明確化し入力する．
  〈R と A の関係 L' の定義〉
- サービス資産一覧画面［List of Services & Assets］
  関係 L で定義された IT サービス（s_j）と資産（a_i）のリンク情報を表示する．
- 資産一覧画面［List of Assets］
  特定した資産（a_i）を資産目録として表示する．
- リスク一覧画面［List of Risks］
  すべてのリスク（$r_{i,k}$）を一覧表示する．

RISKMS の実装には，Microsoft Access を使用した．フォーム（Form）で画面をデザインし，クエリ（Query）で SQL (Structured Query Language) を実行する．また，画面表示に関連してマクロ（Macro）を使用している．RISKMS のシステム概略図を**図 5** に示す．

表 2 リスク受容基準

Table 2 Risk acceptance criteria.

Risk Evaluation	C	I	A
High	>24	>24	>16
Medium	>=12	>=12	>=8
Low	<12	<12	<8

5.2 リスク基準確立

ISO/IEC 27001:2013 は，リスクアセスメントの実施にあたり，リスク受容基準の確立を求めている．RISKMS では，センターの ISMS・ITSMS 統合マニュアルに基づきリスク受容基準を設定した．リスク受容基準を**表 2** に示す．ここで，C は機密性（C：Confidentiality），I は完全性（I：Integrity），A は可用性（A：Availability）を表しており，表内の数値はそれぞれのリスクレベルである．なお，組織体の公共性と研究・教育の継続性を通して社会に果たすべき責務に鑑み，特に可用性を重視し，機密性，完全性の基準よりも可用性の基準は約 30%増の強化基準とした．

5.3 リスク特定

提案方法では，まず，1）RAM_0 を実施する．資産（a_i）

図 6 資産リスク管理画面の例．RISKMS：ISMS・ITSMS 統合管理システム

Fig. 6 An example of “Asset & Risk Management” screen. RISKMS: The integrated management system for ISMS and ITSMS.

を特定し，脅威・脆弱性を明確化する．そしてリスク（$r_{i,k}$）を特定する．この作業より，R と A の関係 L' が定義される．次に，2）A と S の関係 L を定義する．関係 L' と L の合成により，資産（a_i）のリスク（$r_{i,k}$）は，資産（a_i）が関係する IT サービス（s_j）のリスクとなる．

RISKMS では，まず，RISKMS 資産リスク管理画面の「資産データ入力フォーム」で資産（a_i）情報を入力し，機密性，完全性，可用性の 3 要素に関する資産価値を評価する．「リスクデータ入力フォーム」では資産（a_i）に関係する脅威・脆弱性を明確化し入力する．この作業より，R と A の関係 L' が定義される．**図 6** に RISKMS 資産リスク管理画面の例を示す．図 6 では，「資産データ入力フォーム」でセンターの ISMS・ITSMS 統合マニュアルに基づき，特定した資産（a_i）の機密性，完全性，可用性の 3 要素に関する資産価値を評価し，管理者や資産形態などの情報を入力している．「リスクデータ入力フォーム」には特定した複数のリスク（$r_{i,k}$）を入力している．ここで特定し入力したリスク（$r_{i,k}$）は，トップ画面の「リスク情報」に表示する．リスク（$r_{i,k}$）は RISKMS リスク一覧画面においても確認できる．特定した資産（a_i）は，RISKMS 資産一覧画面に資産目録として表示する．

次に，RISKMS サービス管理画面で A と S の関係 L を定義する．**図 7** に RISKMS サービス管理画面の例を示す．「サービスデータ入力フォーム」にはサービス名などの IT サービス（s_j）の情報を入力する．「関係資産データ入力フォーム」では，RAM_0 で特定した資産（a_i）の一覧から IT サービス（s_j）に関係する資産（a_i）を選択できる．ここで，IT サービス（s_j）に関係する資産（a_i）を設定することで，A と S の関係 L を定義する．図 7 では，「関係資産データ入力フォーム」で IT サービス（s_j）に関係する複数の資産（a_i）を定義している．関係 L で定義された IT サービス（s_j）と資産（a_i）のリンク情報は，RISKMS

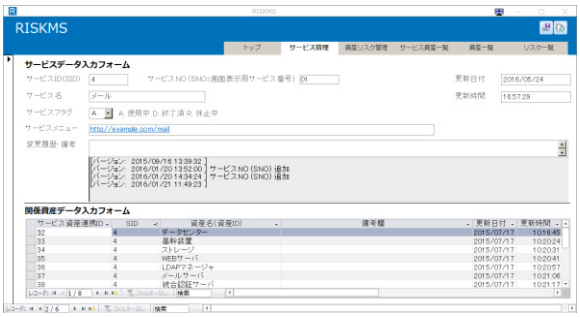
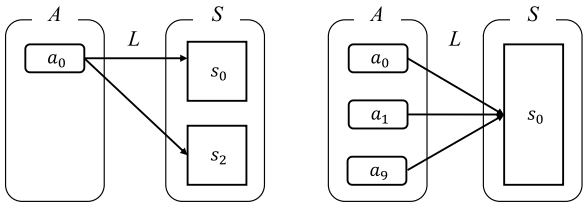


図 7 サービス管理画面の例．RISKMS：ISMS・ITSMS 統合管理システム

Fig. 7 An example of “Service Management” screen. RISKMS: The integrated management system for ISMS and ITSMS.



(a) Link data extraction about a_i. (b) Link data extraction about s_j.

図 8 リンク情報抽出の概念図．(a) 資産（a_i）に関するリンク情報抽出，(b) IT サービス（s_j）に関するリンク情報抽出

Fig. 8 Conceptual diagram of link data extraction. (a) Link data extraction about an asset (a_i), (b) Link data extraction about an IT service (s_j).

サービス資産一覧画面で抽出し，関係を確認できる．ここで，RISKMS サービス資産一覧画面は，

(a)：資産（a_i）が関係する IT サービス（s_j）
(b)：IT サービス（s_j）に関係する資産（a_i）

の 2 通りのリンク情報を抽出できる．**図 8** にリンク情報抽出の概念図を示す．

5.4 リスク分析

提案方法では，RAM_0 を実施し，特定されたリスク（$r_{i,k}$）のアセスメントを行い，リスクレベルを決定する．ここでは，資産（a_i）が有する機密性，完全性，可用性のそれぞれのリスクレベルを計算する．リスク特定で明確になった，資産価値，脅威の大きさ，脆弱性の度合いを用いて，リスクレベルを式 (1) で算定する．

RISKMS では，RISKMS 資産リスク管理画面で入力された機密性，完全性，可用性の 3 要素に関する資産価値と資産（a_i）に関係する脅威・脆弱性を基に，クエリで式 (1) を実装し，リスクレベルを算定する．

5.5 リスク評価

提案方法では，まず，1）RAM_0 を実施する．リスク分

析において，式 (1) を用いて算定したリスク（$r_{i,k}$）のリスクレベルと事前に確立したリスク受容基準を比較する．リスク対応のために，分析したリスク（$r_{i,k}$）の優先順位付けを行う．次に，2）IT サービス（s_j）のリスク評価を実施する．

RISKMS では，リスク分析において式 (1) を用いて算定したリスク（$r_{i,k}$）のリスクレベル，リスクレベルとリスク受容基準の比較結果などのリスク評価をトップ画面の「リスク情報」に表示する．ここで，リスクレベルがリスク受容基準を超えているリスク「高（High）」については赤色表示する．また，リスク情報はリスクレベルの降順で表示する．IT サービス（s_j）のリスク評価は，提案方法の評価法に基づき計算処理し，RISKMS トップ画面の「IT サービス一覧」に表示する．

6. 結果と考察

センターは，ISMS を 2003 年に，ITSMS を 2012 年に認証取得し，以後継続して運用している．提案方法については，2014 年から適用した．本章では，ISO/IEC 27001:2013 および ISO/IEC 20000-1:2011 の要求事項充足性の観点から，提案方法の妥当性を示す．また，センターにおける従来方法と提案方法の所要時間の見積りを比較することによって，提案方法が課題解決のために有効であることを示す．さらに，提案方法の適用が，資産（a_i）ベースのリスクアセスメント方法（RAM_0）におけるリスク評価の改善にも寄与することを述べる．

6.1 要求事項充足

提案方法は，ISMS と ITSMS の統合リスクアセスメントとして次の 1），2）を実施する．

1） 資産（a_i）ベースのリスクアセスメント方法（RAM_0）として，ISMS ユーザーズガイドのリスクマトリックス法に基づくリスクアセスメントを実施する．このとき，リスクの集合 R と資産の集合 A の関係 L' が定義される．

2） 資産の集合 A と IT サービスの集合 S を関係 L で定義する．このとき，関係 L' と L の合成 $L' \circ L$ が得られる．

ISMS のリスクアセスメントについては，2.2 節で示したように，ISO/IEC 27001:2013 の 6.1.2 が要求事項を示している．ISO/IEC 27001:2013 の 6.1.2 c) から 6.1.2 e) で，ISMS の適用範囲内における情報の機密性，完全性及び可用性の喪失に伴うリスクを特定し，特定されたリスクに対して，リスク分析とリスク評価することを要求している．提案方法は，1）で ISMS ユーザーズガイドのリスクマトリックス法に基づくリスクアセスメントを実施する．ここで，リスク源を「情報及び情報に関連する資産，脅威，脆弱性」としている．このため，ISO/IEC 27001:2013 の 6.1.2 の要求事項を満たしている．

ITSMS の要求事項を定義する ISO/IEC 20000-1:2011 は，2.2 節で示したように，リスクアセスメントを明確に定義していない．関連する記述として，ISO/IEC 27013:2015 の附属書 B は，表 1 の 3 項目をあげている．ここでは，提案方法が表 1 の 3 項目を満たしているか考察する．

ISO/IEC 20000-1:2011

- 4.5.3 SMS の導入及び運用（Do）
  d) サービスに対するリスクの特定，アセスメント及び管理
- 5.2 新規サービス又はサービス変更の計画
  f) リスクの特定，アセスメント及び管理

ISO/IEC 20000-1:2011 の 4.5.3 d) と 5.2 f) については，提案方法のリスク特定において，関係 L' と L の合成により，資産（a_i）のリスク（$r_{i,k}$）を，資産（a_i）が関係する IT サービス（s_j）のリスクとして特定し，リスクアセスメントを実施することから要求事項を満たす．

ISO/IEC 20000-1:2011

- 6.6.1 情報セキュリティ基本方針
  d) 情報セキュリティリスクアセスメントを，あらかじめ定めた間隔で実施することを確実にする．

ISO/IEC 20000-1:2011 の 6.6.1 d) については，組織の年間計画に基づき，提案方法を実施することで要求事項を満たす．

以上より，提案方法は，ISO/IEC 27001:2013 および ISO/IEC 20000-1:2011 の要求事項を充足すると判断できる．

6.2 省力化

センターにおける ISMS と ITSMS の運用実績値を用いて，従来方法と提案方法の所要時間を見積り，提案方法の効果を明らかにする．

センターにおける ISMS と ITSMS の運用実績値：

- グルーピングした 67 の資産（a_i）を保有し，32 の IT サービス（s_j）を運用している．
- 1 つの資産（a_i）または IT サービス（s_j）のリスクアセスメントの所要時間はほぼ等しく，概算見積り値 60 分（1 時間）が得られた．この値は，PMBOK（Project Management Body of Knowledge）の 3 点見積り（ベータ分布）[27] を用いて算定した．このとき，運用実績から仮定された値の分布は，楽観値 10 分，最可能値 50 分，悲観値 150 分である．
- 資産の集合 A と IT サービスの集合 S の関係 L（*LINK*，リンク）の定義に要する時間は，運用実績値の 3 点見積り（楽観値 1 分，最可能値 3 分，悲観値 5 分）から資産（a_i）のリスクアセスメントの所要時間の 5%（3 分）とした．
- 関係 L（*LINK*，リンク）における実際のリンク総数

は 158 である．

運用実績値を用いて，従来方法と提案方法のリスクアセスメントの中心部分の所要時間を概算した結果を次に示す．

$$\text{従来方法} = (67 + 32) \times 1 = 99$$

$$\text{提案方法} = (67 \times 1) + (158 \times 1 \times 0.05) = 74.9$$

従来方法では，RAM_0 と RAM_1 の合計所要時間が 99 時間と算定された．提案方法では，RAM_0 と関係 L の定義の合計所要時間が 74.9 時間と算定された．提案方法により，リスクアセスメントの中心部分の所要時間は，従来方法と比較して 24.1 時間（約 24%）削減でき，省力化できていると判断できる．

提案方法は，リスクアセスメントの中心部分の所要時間を削減できることに加えて，副次的な省力化の効果も期待できる．すなわち，RAM_0 と RAM_1 実施結果の整合性レビューの削減である．従来方法では，RAM_0 と RAM_1 の実施結果に論理的な矛盾がないことの確認が重要であった．論理的な矛盾とは，たとえば，RAM_0 で高いリスク（$r_{i,k}$）が存在すると評価された資産（a_i）で提供される IT サービス（s_j）であるにもかかわらず，RAM_1 におけるその IT サービス（s_j）のリスク評価が低い場合である．リスクアセスメントは，ISO マネジメントシステムにおいて，論理性の高い要求事項の 1 つであるため，認証機関による審査でこの種の矛盾を指摘される機会は多い．提案方法では，RAM_0 のみを用いるため，従来方法のような整合性レビューを必要としない．論理的な矛盾は入り込む余地がなく，簡便な運用を可能としている．さらに，省力化の効果は文書管理にも現れる．文書化要求の強い ISO マネジメントシステムにおいて，提案方法は，RAM_1 に関する文書は RAM_0 に関する文書を参照することで代替でき，RAM_0 の文書化と管理を行うだけでよい．

以上より，人員や予算などのリソースが限られる組織において，提案方法は省力化の課題解決のために有効であると判断できる．提案方法の効果は，センターにおける ISMS と ITSMS の円滑な運用を導き，同時にスタッフの心理的負担の軽減にも寄与した．

6.3 リスク評価の改善

リスク評価は，リスクアセスメント完了後に続くリスク対応のために，分析したリスク（$r_{i,k}$）の優先順位付けを行う．基本的には，リスクレベルとリスク受容基準に基づきリスク評価する．ここで，リスクレベルが同じリスク（$r_{i,k}$）が存在した場合，それらのうち，どのリスク（$r_{i,k}$）を優先的に対応するか，さらに決定する必要がある．

提案方法は，関係 L' と L の合成により，資産（a_i）のリスク（$r_{i,k}$）は，資産（a_i）が関係する IT サービス（s_j）のリスクとなる．リスクレベルが同じリスク（$r_{i,k}$）が存在した場合，関係する IT サービス（s_j）数を基に，さらに優先順位付けできる．資産（a_i）が関係する IT サービス（s_j）のリンク情報抽出の概念については，図 8 (a) を参照されたい．センターにおいて，ネットワーク装置に関係するリスク（$r_{i,k}$）と電子掲示板に関係するリスク（$r_{i,k}$）のリスクレベルが同じものがあった．ネットワーク装置は 7 サービスに関係しており，電子掲示板は 1 サービスにのみ関係していた．この場合，IT サービス（s_j）数を基に，より広範な IT サービス（s_j）への影響を考慮して，ネットワーク装置に関係するリスク（$r_{i,k}$）の優先順位を上げた．すなわち，提案方法では，リスクレベルが同じリスク（$r_{i,k}$）が存在した場合でも，リスク（$r_{i,k}$）が関係する IT サービス（s_j）数が多い方がリスク対応を優先すべきリスク（$r_{i,k}$）と判断できる．提案方法の適用により，資産（a_i）ベースのリスクアセスメント方法（RAM_0）として実施した，ISMS ユーザーズガイドに基づくリスク評価に加えて，リスクレベルが同じリスク（$r_{i,k}$）が存在した場合，IT サービス（s_j）数に基づく，さらなる半定量的リスク評価ができる．

7. まとめと今後の展望

本論文では，「関係の合成」の概念を用いた ISMS と ITSMS の新しい統合リスクアセスメント方法を提案した．関係データベース管理システムを使用し，提案方法を実現する RISKMS を実装した．提案方法を，センターにて 2014 年から適用した結果，リスクアセスメントの所要時間を削減し，ISMS と ITSMS のリスクアセスメントに関する業務効率の向上と，運用の省力化に有効であった．

今回の提案方法と RISKMS の実装における，資産の集合 A と IT サービスの集合 S の関係 L（*LINK*，リンク）の定義において，数段階の重みを定義すれば，機能的にはより高い精度が得られる．そこでは，4.6 節における IT サービス（s_j）のリスク評価法や，6.3 節のリスク評価の改善を，リンクの重みを考慮した評価決定法に進化させることも可能となる．本論文においては，センターにおける 10 年以上にわたる ISO マネジメントシステム運用で，現実的に求められたリスクアセスメントの深さの加減に照らして，リンクの重みを一定に留めた．

ISO マネジメントシステムの規格書は基本的に 5 年に 1 度レビューされる．今後，ISO/IEC 27001 および ISO/IEC 20000-1 が改正される際には，必要に応じて提案方法を要求事項に適合するよう修正する．また，組織の内外の状況に合わせて提案方法を進化させ，マネジメントシステムを効果的に運用していく方針である．

参考文献

[1] 一般財団法人日本情報経済社会推進協会（JIPDEC）：ISMS 認証取得組織数推移，認証機関別・県別認証取得組織数，入手先 ⟨https://isms.jp/lst/ind/suii.html⟩（参照

2018-03-25).
[2] 一般財団法人日本情報経済社会推進協会（JIPDEC）：ITSMS 認証取得組織数推移，認証機関別・県別認証取得組織数，入手先 ⟨https://isms.jp/itsms/lst/ind/suii.html⟩（参照 2018-03-25）.
[3] 文部科学省：学校基本調査—平成 29 年度結果の概要—，入手先 ⟨http://www.mext.go.jp/b_menu/toukei/chousa01/kihon/kekka/k_detail/1388914.htm⟩（参照 2018-01-25）.
[4] 一般財団法人日本情報経済社会推進協会（JIPDEC）：認証取得組織検索，入手先 ⟨https://isms.jp/furiwake-j.html⟩（参照 2018-03-25）.
[5] ISO/IEC 27013:2015: Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1, ISO (2015).
[6] ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems — Requirements, ISO (2013).
[7] ISO: ISO/IEC Directives Part 1 and Consolidated ISO Supplement, available from ⟨https://www.iso.org/directives-and-policies.html⟩ (accessed 2017-11-30).
[8] ISO 31000:2009: Risk management — Principles and guidelines, ISO (2009).
[9] ISO/IEC 20000-1:2011: Information technology — Service management — Part 1: Service management system requirements, ISO (2011).
[10] ISO/IEC 27000:2014: Information technology — Security techniques — Information security management systems — Overview and vocabulary, ISO (2014).
[11] ISO Guide 73:2009: Risk management — Vocabulary, ISO (2009).
[12] ISO/IEC 27013:2015: Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1, p.32, ISO (2015).
[13] 長谷川孝博，中野光義：ISMS から ITSMS への取り組みについて，情報処理学会研究報告，Vol.2012-IOT-16, No.39, pp.1–5 (2012).
[14] 頼永　忍：国際規格に軸足を置いた，情報セキュリティマネジメントと事業継続マネジメントの統合手法の提案，情報処理学会第 75 回全国大会講演論文集，Vol.2013, No.1, pp.503–504 (2013).
[15] Bojanc, R. and Jerman-Blažič, B.: An economic modelling approach to information security risk management, *International Journal of Information Management*, Vol.28, No.5, pp.413–422 (2008).
[16] IEC/ISO 31010:2009: Risk management — Risk assessment techniques, pp.82–86, ISO (2009).
[17] JIS Q 31010: 2012（IEC/ISO 31010:2009）：リスクマネジメント—リスクアセスメント技法，pp.69–72, 日本規格協会 (2012).
[18] IEC/ISO 31010:2009: Risk management — Risk assessment techniques, pp.42–44, ISO (2009).
[19] IEC/ISO 31010:2009: Risk management — Risk assessment techniques, ISO (2009).
[20] 一般財団法人日本情報経済社会推進協会（JIPDEC）：ISMS ユーザーズガイド-JIS Q 27001:2014（ISO/IEC 27001:2013）対応，JIPDEC (2014).
[21] 一般財団法人日本情報経済社会推進協会（JIPDEC）：ISMS ユーザーズガイド—JIS Q 27001:2014（ISO/IEC 27001:2013）対応—リスクマネジメント編，JIPDEC (2015).
[22] 佐々木良一（編著）：IT リスク学，千葉寛之：IT システムにおけるリスクアセスメント，pp.147–150, 共立出版 (2013).
[23] ISO/IEC 27013:2015: Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1, pp.8–9, ISO (2015).
[24] 一般財団法人日本情報経済社会推進協会（JIPDEC）：ITSMS ユーザーズガイド～導入のための基礎～，p.69, JIPDEC (2013).
[25] Lipschutz, S. and Lipson, M.: Schaum's Outline of Theory and Problems of Discrete Mathematics, pp.27–28, McGraw-Hill (2007).
[26] Codd, E.F.: A Relational Model of Data for Large Shared Data Banks, *Comm. ACM*, Vol.13, No.6, pp.377–387 (1970).
[27] Project Management Institute, Inc.：プロジェクトマネジメント知識体系ガイド（PMBOK ガイド）第 5 版，pp.170–171, Project Management Institute, Inc. (2014).

松村 宣顕　（正会員）

民間企業勤務を経て，2008 年独立行政法人国際協力機構（JICA）青年海外協力隊，王立ブータン大学勤務．現在，静岡大学情報基盤センター技術専門職員．情報基盤，ISMS（ISO/IEC 27001），ITSMS（ISO/IEC 20000-1）の運用および情報セキュリティに関する研究に従事．電子情報通信学会会員．

長谷川 孝博　（正会員）

1997 年九州工業大学大学院博士後期課程情報科学専攻修了．博士（情報工）．同年静岡大学工学部システム工学科助手．現在，同大学 CISO，情報基盤センター副センター長，准教授，ISMS（ISO/IEC 27001）ITSMS（ISO/IEC 20000-1）管理責任者．情報基盤，情報セキュリティ，インテリジェンスマイニングに関する研究に従事．スケジューリング学会会員．