情報処理学会論文誌 Vol.60 No.9 1518–1527 (Sep. 2019)

制御システム向け事業レベルでのリスク分析手法の提案

熊谷 洋子[1,a)] 松原 佑生子[1] 内山 宏樹[1] 鍛 忠司[1] 藤田 淳也[1] 中野 利彦[1]

受付日 2018年11月26日, 採録日 2019年6月11日

概要：電力，鉄道，水道，ガスといった社会インフラを支える制御システムは，システムのオープン化等にともない，情報システムと同様のセキュリティ対策が求められてきている．制御システムを運営する事業者は，事業全体に対するサイバーセキュリティリスクを正しく認識したうえで適切なセキュリティ対策を実施する必要がある．しかしながら，社会インフラシステムは事業規模が大きいため，事業全体のリスクを網羅的に把握するのが困難である．また，制御システムと情報システムとでは保護対象や想定脅威が異なるため，制御システムの特徴を考慮した分析が必要である．このような課題を受け，本論文では事業レベルでのリスク分析手法として，事業全体のリスクを効率的に抽出し，それらを俯瞰したうえで優先的に対策すべき業務/システムを把握する手法を示す．本手法では，入力，出力，人，システム，装置，規格・計画の構成要素を活用し，汎用的な事業モデルを定義することで，事業全体を把握可能であることを示す．また，制御システムで考慮すべき H&SEB（Health, Safety, Environment and Business）の観点で事業上のリスクを解析的に抽出し，重大なリスクに関係の深い業務/システムを特定可能であることを示す．さらに，本提案手法と従来手法のリスク抽出および評価手法について比較，評価することで，本手法が活用可能であることを示す．

キーワード：社会インフラシステム，制御システム，サイバーフィジカルシステム，セキュリティ設計，リスク分析

Proposal of a High-level Risk Analysis Method for Industrial Control Systems

Yoko Kumagai[1,a)] Yukiko Matsubara[1] Hiroki Uchiyama[1]
Tadashi Kaji[1] Junya Fujita[1] Toshihiko Nakano[1]

Received: November 26, 2018, Accepted: June 11, 2019

Abstract: In the industrial control system supporting social infrastructure such as electric power, railway, water supply, and gas, security measures similar to those of the information system are required. Business operators operating the industrial control system need to correctly recognize cyber security risks for the entire business and implement appropriate security measures. However, the social infrastructure system has a large business scale, so it is difficult to understand the overall risk of the entire business. Also, it is necessary to analyze considering the characteristics of the industrial control system. In response to these issues, this paper proposes a risk analysis method at the business level. This method efficiently extracts the risks of the entire business, understands the business/system that should be taken preferentially after overlooking them. In this method, general-purpose business models are defined using inputs, outputs, people, systems, equipment, standards and plan components. Also analyze business risks analytically from the viewpoint of HSE & B (Health, Safety, Environment, and Business) to be considered in the industrial control system. Furthermore, we show that our method can be utilized by comparing and evaluating risk extraction and evaluation method of this proposed method and conventional method.

Keywords: social infrastructure system, industrial control system, cyber physical system, security design, risk analysis

1. はじめに

鉄道，電力，水道，ガスといった社会インフラを支える制御システムは，ネットワークや装置への汎用技術の取込みや，情報システムとの接続の増加にともない，情報システムと同様のセキュリティ対策が求められてきている．近年，制御システムを狙ったサイバー攻撃の報告件数は，国内外において増加傾向にあり [1]，2020 年の東京オリンピック・パラリンピックの開催に向けサイバー攻撃がますます高度化することが予想される．社会インフラシステムにおいて何らかの障害が発生した場合，死亡事故や環境汚染といった大きな影響を及ぼす恐れがあるため，セキュリティ対策の実施は不可欠なものと考えられる．

このような状況を受けて，社会インフラシステムを支える産業制御システム向けセキュリティ標準規格 IEC62443-2-1 [2] では，上位レベル（事業レベル）で想定すべきリスクを認識し，対策が必要と判断したシステムに関して詳細なリスク分析および対策立案を実施することが定められている．また，NISC 重要インフラ第 4 次行動計画 [3] において，リスクマネジメントをふまえた対処態勢整備の推進として，リスク分析や事業継続計画の策定が要求されている．

制御システムを運営する事業者は，上記標準規格やガイドラインに準拠するために，事業全体に対するサイバーセキュリティリスクを正しく認識し，重要な業務/システムを特定したうえで適切なセキュリティ対策を実施する必要がある．しかしながら，IEC62443-2-1 では，「上位レベルのリスクアセスメントの実行」が要求事項として記述されているものの，リスク分析方法に関しては具体的な方法は定義されていない．また，事業継続計画の策定の中でも，システム停止時の業務影響を正確に把握するリスク分析としてビジネスインパクト分析（BIA：Business Impact Analysis）が求められているが，具体的な手法については定義されていない．このため，分析者によるランク付け等，分析者のノウハウに依存した分析結果となってしまう恐れがある．

また，社会インフラシステムは事業規模が大きく，事業を構成する業務/システムも多種多様であるため，事業全体のリスクを網羅的に把握するのが困難である．さらには，社会インフラ事業は多数の事業と連携するため，他事業との依存関係を考慮したリスクの把握が必要であるが，他事業との複雑な依存関係の把握も困難である．

以上のような背景から，本論文では社会インフラシステム等の制御システムを対象とした事業レベルでのリスク分析手法を提案する．これまでは未定義であった事業レベルでのリスク分析手順を具体的に定義することで，分析者のノウハウや前提知識に依存せず，分析漏れを最小限とし，事業に大きな影響を及ぼすリスクの特定を可能とする．

本手法を活用することにより，事業全体のリスクを効率的に抽出し，それらを俯瞰したうえで優先的に対策すべき業務/システムを把握することが可能となる．

本論文の構成は以下のとおりである．2 章で事業レベルでのリスク分析における課題を述べ，3 章では課題を解決する事業レベルでのリスク分析手法を示す．4 章では 3 章で提案した事業レベルでのリスク分析手法の評価結果を示し，5 章でまとめを述べる．

2. 事業レベルでのリスク分析における課題

2.1 制御システム向け事業レベルでのリスク分析の概要

IEC62443-2-1 では，産業制御システムにおいてサイバーインシデントが発生した場合の財務的（Business）および HSE（Health, Safety and Environment）に対する影響を把握するために，上位レベルのリスクアセスメントの実行が要求されている．このため，本論文で提案する制御システム向け事業レベルでのリスク分析とは，サイバーインシデントが発生した場合の事業の H&SEB への影響の性質や規模に基づき，リスクを認識するためのものである．

事業を構成する各業務/システムにどのようなリスクが存在するのかを事業者が認識し，リスクが大きい業務/システムから優先的にセキュリティ対策を実施することで，効果的なセキュリティ投資が可能となる．たとえば，事業レベルでのリスク分析の結果，事業を構成する一部のシステムにおいて，サイバー攻撃によるシステム停止の影響が周辺住民の人命に関わる甚大な影響があると判明した場合は，当該システムに対する詳細なリスク分析を行い，適切なセキュリティ対策を実施する必要がある．

2.2 関連研究

IEC62443-2-1 では，「上位レベルのリスクアセスメントの実行」が要求事項として記述されているが，リスク分析方法に関しては具体的な方法は定義されていない．また，事業継続計画の策定の中でも，システム停止時の業務影響を正確に把握するリスク分析として BIA が求められているが，具体的な手法については定義されていない．

BIA の具体的な手順に関する先行研究として，益田らが提案する手法 [4] が存在する．本手法は，金融事業を対象とした BIA の手順として，リスクの洗い出し，リスク潜在場所（重要システム）の絞り込み，リスクシナリオの特定，優先業務の特定，ボトルネックの判定，といった BIA 全体の具体的な手順を示している．

具体的には，分析対象の事業内部の各部署へのアンケートにより業務とその業務停止時の影響をリストアップし，業務とシステムとの関係をマトリクス状に整理し，多くの業務が関わるシステムを重要システムとして設定する．

[1] 株式会社日立製作所
Hitachi Ltd., Yokohama, Kanagawa 244–0817, Japan
[a)] yoko.kumagai.su@hitachi.com

次に，重要システムに関わる複数業務に対して，業務停止時の影響を定性的に評価することで優先順位付けし，優先業務を特定する．最後に特定した各優先業務に対して，HAZOP を活用し脅威や影響を分析する手法である．

益田らの手法のうち，「リスクの洗い出し」から「優先業務の特定」までの手順が，本手法と同じスコープを対象とした分析手法であると考えられるため，益田らの上記部分の手順を既存技術として設定した．

2.3 事業レベルでのリスク分析における課題

益田らの手法は，金融の情報システムを対象としたものであり，制御システムに適用するには課題がある．益田らの手法では，多くの業務が関連するシステムを重要システムに設定することで，ビジネス上の影響範囲の広さを基準にリスクの大きさを識別しているが，ビジネス以外の観点でのリスク抽出が困難であるといえる．たとえば，制御システムにおいては，単一の業務で使われるシステムであっても人命等に関わる場合はリスクが大きいため重要システムとして設定すべきである．また，益田らの手法では，重要業務の優先順位付けを業務停止時の影響を定性的評価により実施しているが，この場合評価結果が評価者のノウハウに依存するという課題がある．

また，社会インフラ事業は，社内外の複数事業が関連しているケースが多く，分析対象事業内の業務/システムを原因としたリスクだけでなく，他事業のリスクが対象事業に及ぼすリスクも考慮する必要がある．しかしながら，益田らの手法では事業内部の業務のみを対象としており，他事業のリスクが対象事業に影響を及ぼすリスクの抽出が困難であるという課題がある．たとえば，電力事業者から電力を購入して事業活動を実施している場合，他事業である電力事業が停止した場合に対象事業においても大きな影響を及ぼすというリスクがある．

以上より，社会インフラ等の制御システムに対する事業レベルでのリスク分析においては，以下の課題がある．

【課題 1】

社会インフラ等の制御システムに適した（H&S，E，B の観点や複数事業の連携を考慮した）リスク抽出手法が存在しない．

【課題 2】

社会インフラ等の制御システムに適したリスク評価手法が存在しない．

3. 制御システム向け事業レベルでのリスク分析手法の提案

一般的に，リスク分析は以下のステップで行う．

[Step1] 対象事業モデル化

保護対象となる事業をモデル化する．

[Step2] 事業リスク抽出

保護対象に対するリスクを抽出する．

[Step3] リスクレベル見積り

抽出したリスクに対して，その影響の大きさを評価する．

[Step4] 事業リスク要因検討

事業リスクと業務/システムとの関係性を明確化し，詳細分析を行うべき業務/システムを明らかにする．

本論文では，2.3 節であげた課題を解決するため，以下のようなアプローチに従って検討を実施した．本アプローチに従い検討した結果を，制御システム向け事業レベルでのリスク分析手法として提案する．

【課題 1 へのアプローチ】

関連する他事業との依存関係や事業内の業務間の依存関係を明確化するため，Step1 において事業の入出力や構成要素に着目した汎用的な事業モデルの構築方式を検討する．Step2 では，そのモデルを活用した H&SEB の観点でのリスク抽出方式を検討する．

【課題 2 へのアプローチ】

Step3 において，事業への H&SEB の影響の大きさを元にリスクレベルを見積もる手法を検討する．

3.1 [Step1] 対象事業のモデル化

本ステップは，リスク抽出およびレベル見積りに必要な対象事業の情報を整理することを目的とする．重要インフラ事業には様々な種類があるが，品質マネジメントの技法である 4M（Man, Machine, Material, Method）を参考に，入出力や構成要素を抽象化して事業を表現すると，**図 1** のモデル図として表現できる．図に示すように，事業は事業者外からの入力（原料等のモノ，情報等）を用いて，出力（製品・サービス，廃棄物等）を他者に対して提供する．また，事業は入力と出力のほかに，事業を実施するうえで必要な人，IT/OT システム群，物理装置群や，事業を実施するうえで従うべき規格・計画から構成される．車両製造事業をモデル図で表した例を**図 2** に示す．

また，本事業モデルに基づき様々な事業をモデル化した場合，事業には大きく 2 つの分類があることが分かった．1 つは入力になんらかの処理を加えて変換することで製品やサービスを出力する「変換系事業」と，もう 1 つは入力は

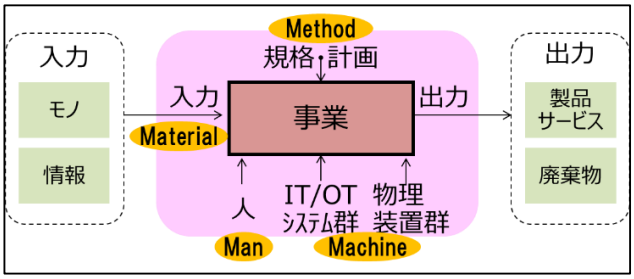

図 1 事業モデル
Fig. 1 Business model.

そのままの形で別の場所等に移動させて出力する「フロー系事業」である．

さらに，図 3 に示すようなターゲット事業と周辺事業の依存関係を示す事業外モデルを立案した．このような事業外モデルは，サプライチェーンのモデルとして既存研究でも考慮されており，たとえば西川らのリスク解析手法 [5] ではサプライチェーンの連結タイプとして直列型，並列型，併用型が定義されている．しかしながら，具体的にどのような事業がどのような型で連結しているのかを明らかにするための手法については述べられていなかった．

本手法では，事業の各構成要素は他の事業の出力から導かれると想定し，事業外モデルを構築する手法を考案した．事業外モデルは，ターゲット事業の各入力要素（入力，人，IT/OT システム群，物理装置群，規格・計画）をさかのぼってたどることで構築する．各構成要素は，他の変換系業務である周辺事業の出力であり，運輸や伝達を行うフロー系事業を通じてやりとりされる．車両製造事業の事業外モデルの例を図 4 に示す．

さらに，図 5 に示すようにターゲット事業の内部には複数の業務を保有しており，この業務も事業と同様のモデルで表現可能である．本モデルに基づき，分析対象事業の入出力や，事業を構成する業務/システムを整理することで，対象事業の特徴が明らかとなる．車両製造事業の事業内モデルの例を図 6 に示す．

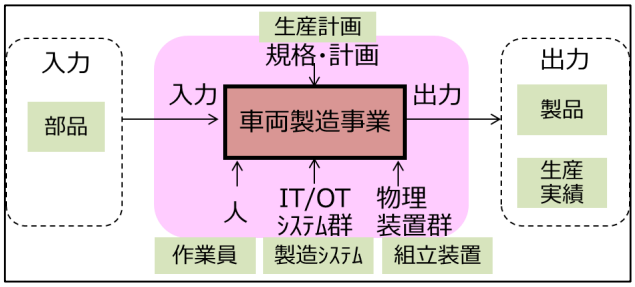

図 2 車両製造事業の事業モデルの例

Fig. 2 Example of business model of vehicle manufacturing business.

3.2 [Step2] 事業リスク抽出

本ステップは，H&SEB の観点で対象事業のリスクを洗い出すことを目的とする．事業リスクには，事業外リスクと事業内リスクに分けられると考え，両方の観点でリスクを抽出する．

事業外リスクとは，事業の結果生成される出力によって他者，他組織，環境等に対して悪影響を及ぼすリスクを示す．事業内リスクとは，事業を構成する要素（人，システム，装置等）に対して悪影響を及ぼすリスクを示す（図 7）．

事業リスクの抽出は，各要素に対して HAZOP のガイドワード（なし/不正/過剰/不足）をベースに意図しない状況を抽出し，その状況により事業外や事業内にどのような悪影響を及ぼすのかを抽出する．具体的には，事業外リスクの抽出は，Step1 で整理した出力項目の各要素に対して HAZOP のガイドワードをベースに意図しない状況（発生事象）を洗い出す．そして各発生事象により顧客や他組織，環境等に対して H&S，E，B の観点でどのような影響を及ぼすかを事業外リスクとして抽出する．同様に事業内リスクの抽出は，Step1 で整理した人，IT/OT システム，物理装置の各構成要素を対象に，上記と同様の手順で事業内リスクを抽出する．

以上のような手順に基づき事業外/事業内リスクを抽出することで，ターゲット事業におけるリスクを網羅的に抽出することができる．事業リスクの抽出結果例を表 1 に示す．

3.3 [Step3] リスクレベル見積り

本ステップは，抽出した事業リスクに対して，その影響

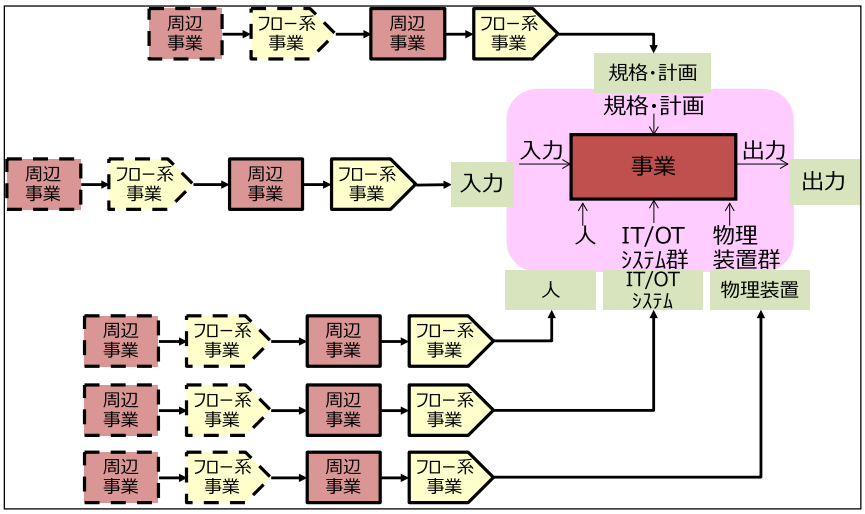

図 3 事業外モデル

Fig. 3 Outside business model.

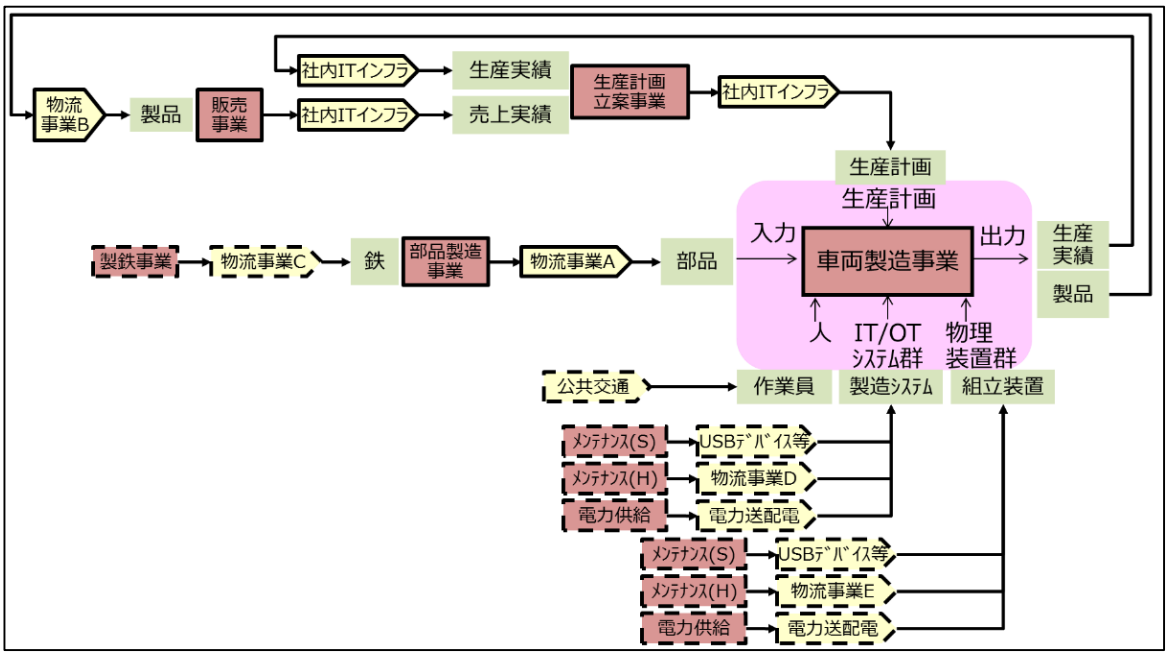

図 4 車両製造事業の事業外モデルの例

Fig. 4 Example of outside business model of vehicle manufacturing business.

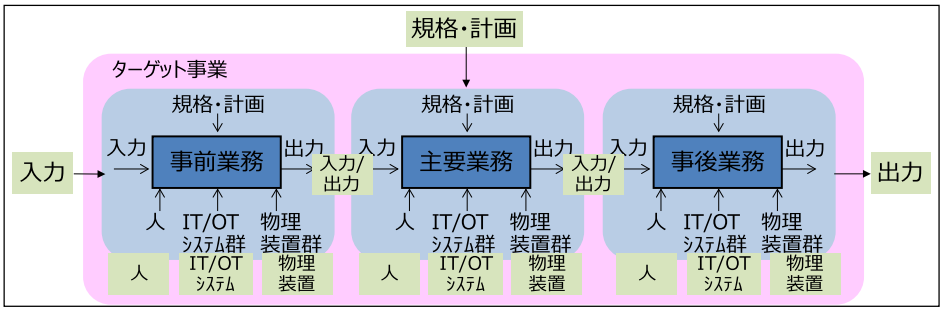

図 5 事業内モデル

Fig. 5 Inside business model.

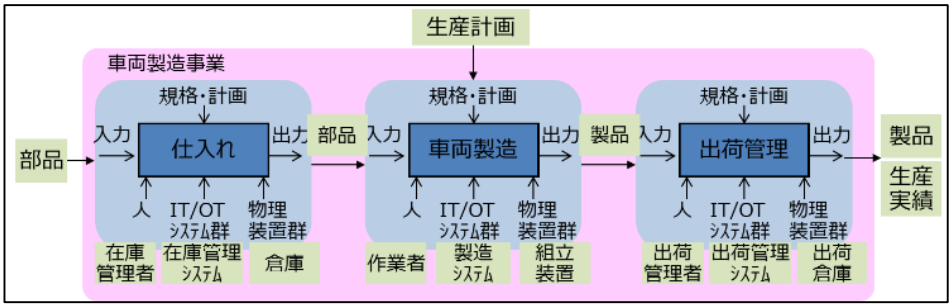

図 6 車両製造事業の事業内モデルの例

Fig. 6 Example of inside business model of vehicle manufacturing business.

の大きさを評価することを目的とする．

ここで，情報システムと制御システムでは，**表 2** に示すように保護対象や想定脅威が異なるため，同じ評価指標でリスクの大きさを把握することはできない．具体的には，情報システムでは保護対象が「情報」であり，CIA（Confidentiality, Integrity, Availability）が損なわれることが想定脅威となる．これに対して制御システムにおける保護対象は「物理プロセス」であり，H&SEB が損なわれることが想定脅威となる．このため，情報システムにおける評価指標をそのまま活用するのではなく，制御システムに適したリスク評価指標が必要となる．

本手法では，**表 3** に示すように H&SEB の観点で影響のレベルを定義し，これらの観点での影響レベルからリスクレベルを見積もる方式を考案した．リスクレベルの見積

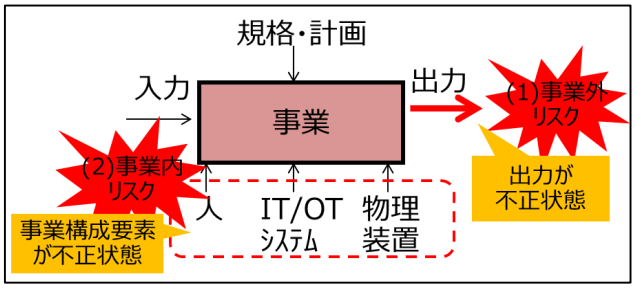

図 7 事業リスクの種類
Fig. 7 Types of business risk.

表 1 事業リスク抽出例
Table 1 Example of the extraction of business risk.

出力項目	ｶﾞｲﾄﾞﾜｰﾄﾞ	発生事象	観点	事業外リスク
製品	不正	不正な製品が製造される	H&S, B	不正な製品が製造され，その顧客(利用者)が負傷する
⋮				
構成要素	ｶﾞｲﾄﾞﾜｰﾄﾞ	発生事象	観点	事業内リスク
製造システム	不正	システムが停止する	B	システムの停止により製造ラインが停止し，顧客の信頼失墜
⋮				

表 2 情報と制御の違い
Table 2 Difference between information systems and control systems.

項目	リスクの種類	定義
保護対象	情報	物理プロセス
リスク顕在化時の影響	情報漏えい，金銭的被害	危険状態に陥る
想定脅威	CIA が損なわれること	H&SEB が損なわれること
要求される稼動率	95-99%	99.9－99.999%
ライフサイクル	3〜5 年	10〜20 年

り方式は，情報システムの脆弱性評価手法である CVSS [6] の影響度算出ロジックを活用し，制御システムに適したリスクレベルの見積り方法とした．

なお，H&SEB のうち H と S は，その性質上合わせて検討される場合が多いため（たとえば IEC62443-2-1 や EHS ガイドライン [7]），本手法においても H&S として合わせて分析することとした．

CVSS では，脆弱性の深刻度を「悪用の可能性」と「影響度」からスコア化している．事業リスクの評価においても，その事業リスクがどの程度深刻なものかをスコア化することで，各事業リスクの大きさ（レベル）を表現できると考え，CVSS の考え方を事業リスクの評価に活用することとした．ただし，本手法の対象は事業上のリスクであり，悪用の可能性にかかわらず，影響が大きいものは対象とすべきと考え，CVSS の「影響度」をリスクレベルとして活用することを検討した．

CVSS の影響度は，C（Confidentiality），I（Integrity），A（Availability）の影響レベルを掛け合わせることで算出するため，この考え方を活用し，本手法におけるリスクレベルは H&S，E，B の影響レベルを掛け合わせることで見積もることとした．具体例としては，**表 4** に示すような基準で，リスクレベルを決定する．

表 3 影響レベルの定義例
Table 3 Example of definition of impact level.

観点	リスクの種類	影響レベル	定義
H&S	人的安全性	甚大	死亡事故の発生
		軽微	疾病の発生
E	環境的安全性	甚大	広範囲，長期間の汚染
		軽微	地域行政への報告が必要な汚染
B	事業継続性	甚大	広範囲での事業停止
		軽微	限定範囲での事業停止
	公衆の信頼	甚大	ブランドイメージの喪失
		軽微	顧客信頼の喪失
	法的制裁	甚大	重い刑事犯罪
		軽微	軽い刑事犯罪

表 4 リスクレベル基準例
Table 4 Examples of risk level criteria.

				H&S		
				なし	軽微	甚大
B	なし	E	なし	低	低	中
			軽微	低	中	中
			甚大	中	中	高
	軽微		なし	低	中	中
			軽微	中	中	高
			甚大	中	高	高
	甚大		なし	中	中	高
			軽微	中	高	高
			甚大	高	高	高

表 5 リスクレベル評価例
Table 5 Example of estimation result of risk level.

出力内容	ｶﾞｲﾄﾞﾜｰﾄﾞ	発生事象	影響レベル	事業外リスク	ﾘｽｸﾚﾍﾞﾙ
製品	不正	不正な製品が製造される	H&S：甚大 B：甚大	不正な製品が製造され，その顧客(利用者)が負傷する	高
⋮					
構成要素	ｶﾞｲﾄﾞﾜｰﾄﾞ	発生事象	観点	事業内リスク	ﾘｽｸﾚﾍﾞﾙ
製造システム	不正	システムが停止する	B：甚大	システムの停止により製造ラインが停止し、顧客の信頼失墜	中
⋮					

表 6 事業リスクと構成要素の関係特定
Table 6 Identifying the relationship between business risks and components.

対象事業リスク / 構成要素	事業外リスク		…
	不正な製品が製造され，その顧客(利用者)が負傷する	想定外の廃棄物が発生し，広範囲が汚染される	
入力	○	○	
人	○	○	
IT/OT システム	○	○	
物理装置		○	
規格・計画			

前節で抽出した事業外リスクに対し，上記ロジックに従いリスクレベルを評価した結果を**表 5** に示す．3.2 節のステップで抽出したすべての事業リスクに対してリスクレベルを見積もった結果から，リスクレベル「高」のものを「対象事業リスク」として選定し，次のステップに進める．

3.4 [Step4] 事業リスク要因の検討

本ステップは，3.1 節で整理した事業モデルを活用し，3.3 節で特定した対象事業リスクと周辺事業や事業内業務との関係性を明確化することを目的とする．これにより，詳細分析を行うべき業務/システムを明らかにできる．

まず，各対象事業リスクに対して，3.1 節で整理した事業モデルの各構成要素との対応関係を明確化する．前節までで例示した対象事業リスクに対して各構成要素との対応関係を明確化した例を**表 6** に示す．具体的には，各対象事業リスクのうち発生事象（表 6 の下線部分）に着目し，この発生事象の要因につながる構成要素をピックアップする．

次に，3.1 節で整理した事業外モデルを活用し，各構成要素に関連する周辺事業をピックアップする．車両製造事業における例を**表 7** に示す．

さらに，3.1 節で整理した事業内モデルを活用し，各構成要素に関連する事業内業務をピックアップする．車両製造事業における例を**表 8** に示す．

以上で整理した表 7，表 8 の対応表をベースに，対象事

表 7 事業リスクと周辺事業の関係特定
Table 7 Identify relationship between business risk and peripheral business.

対象事業リスク / 構成要素	周辺事業	事業外リスク：不正な製品が製造され，その顧客(利用者)が負傷する	事業外リスク：想定外の廃棄物が発生し，広範囲が汚染される	…
入力	・物流事業 A ・部品製造事業	○	○	
人	－	○	○	
IT/OT システム	－	○	○	
物理装置	－		○	
規格・計画	・通信事業 ・生産計画立案事業 ・販売事業 ・物流事業 B			

表 8 事業リスクと事業内業務の関係特定
Table 8 Identifying relationship between business risk and business.

対象事業リスク / 構成要素	事業内業務	事業外リスク：不正な製品が製造され，その顧客(利用者)が負傷する	事業外リスク：想定外の廃棄物が発生し，広範囲が汚染される	…
入力	・仕入れ業務 ・車両製造業務	○	○	
人	・車両製造業務	○	○	
IT/OT システム	・車両製造業務	○	○	
物理装置	・車両製造業務		○	
規格・計画	・車両製造業務			

表 9 事業リスクの要因抽出例
Table 9 Example of extraction of the factor of business risk.

				事業外リスク		
	周辺事業／事業内業務 ＼ 対象事業リスク			不正な製品が製造され、その利用者が負傷する	想定外の廃棄物が発生し、広範囲が汚染される	…
				H&S:甚大、B:甚大	E:甚大、B:軽微	
	分類	事業/業務名	構成要素	リスクレベル：高	リスクレベル：高	
本手法のリスク発生源	周辺事業	生産計画立案事業		小	小	…
		社内 IT インフラ事業		中	小	
		⋮				
従来手法のリスク発生源	事業内業務	仕入れ	入力(原料・情報)	中（可能性あり）	中	
			人	小	小	
			IT/OT システム	小	小	
			物理装置	中（可能性あり）	中（可能性あり）	
			規格・計画	小	小	
		部品製造	入力(原料・情報)	中（可能性あり）	中（可能性あり）	
			人	中（可能性あり）	中（可能性あり）	
			IT/OT システム	大（システムに大きく依存）	中（可能性あり）	
			物理装置	中（可能性あり）	大（有毒ガス使用）	
			規格・計画	大（部品仕様に大きく依存）	小	
		⋮				

業リスクと，対象事業を構成する周辺事業や事業内業務のマトリクスを作成し，事業リスクの要因となるか否かの判断と，その大きさの指標（大，中，小）を割り当てる（**表 9**）．

この結果，「大」の指標が多く割り当てられた業務/システムが，事業リスクの要因となる可能性が高いと判断できる．たとえば，表 9 の例では「部品製造業務」が様々な事業リスクと強く関連していると判断できる．

4. 提案手法の評価

本章では，提案手法により 2 章で整理した課題を解決していることを評価するために，以下の観点で従来手法である益田らの手法との比較を実施する．

(1) 観点 1：網羅的な事業リスク抽出

社会インフラ等の制御システムに適したリスク抽出手法として，H&SEB の観点や複数事業の連携を考慮し，網羅的にリスクを抽出可能か評価する．

(2) 観点 2：評価者のノウハウに依存しないリスク評価

社会インフラ等の制御システムに適したリスク評価手法として，H&SEB の観点を考慮し，評価者のノウハウに依存しないリスク評価手法であるかを評価する．

4.1 網羅的な事業リスク抽出の観点での評価

提案手法と従来手法において，事業リスクとして抽出可能な範囲を**表 10** に整理する．リスクは，リスク発生原，事象およびそれらの原因，起こりうる結果（リスク顕在時の影響）から構成される [8] ため，事業リスク抽出の網羅性をこれらの観点で評価した．

従来手法は，リスク発生源としては内部業務のみを対象としている．また，事業継続計画におけるビジネスインパクト分析手法であるため，発生事象の原因については「業務停止」に着目した分析を実施している．リスク顕在時の影響については，金融の情報システムを対象事業としているため，主にビジネス上の影響のみを抽出している．

表 10 網羅的な事業リスク抽出に関する比較
Table 10 Comparison on comprehensive business risk extraction.

観点		従来手法	提案手法
リスク発生源	内部業務	○	○
	周辺事業	×	○
発生事象の原因	なし（業務停止）	○	○
	不正	×	○
	過剰	×	○
	不足	×	○
リスク顕在化時の影響	H&S	×	○
	E	×	○
	B	○	○

これに対して，提案手法では事業内/外モデルを整理することで，リスク発生源として内部業務だけでなく周辺業務についても考慮している．具体的には，車両製造事業に対するリスク抽出の例において，従来手法では「不正な製品が製造され，その利用者が負傷する」というリスクの発生原因として，事業内業務に対してのみ考慮していた（表 9 の「従来手法のリスク発生源」）．これに対して，本手法では事業外モデルから周辺事業も考慮可能であるため，「社内 IT インフラ」が停止したり不正な状況になることが，上記リスクの発生原因となることを明確化できる（表 9 の「本手法のリスク発生源」）．

また，発生事象の原因として業務停止以外の観点につい

表 11 リスク評価の観点での評価
Table 11 Evaluation from the perspective of risk assessment.

観点	従来手法	提案手法
影響度の判断基準が明確	×	○
複数観点を統合した評価が可能	×	△

ても抽出可能である．具体的には，HAZOP のガイドワードを活用することで，なし（業務停止），不正，過剰，不足の観点について広く抽出可能である．

リスク顕在化時の影響については，制御システムで考慮すべき H&SEB のすべての観点で抽出可能である．

以上より，提案手法はすべての観点について事業リスクを抽出するフレームワークとなっており，網羅的に事業リスクを抽出可能であるといえる．

4.2 評価者のノウハウに依存しないリスク評価の観点での評価

提案手法と従来手法において，事業リスクの評価方法の比較を**表 11** に整理する．リスク評価手法の評価観点として，評価者に依存しない結果を導きだすために，「影響度の判断基準が明確であること」，「複数の観点を統合した評価が可能であること」の観点で整理した．

従来手法では，影響度の判断基準については特に述べられておらず，評価者が業務停止時の影響を定性的に評価することとなる．また，従来手法では B の観点でのみ分析を実施しているため，複数の観点での影響度評価については述べられていない．

これに対して，提案手法では H&SEB の各観点における影響レベルをあらかじめ定義することで，影響度の判断基準を明確化している．また，H&S，E，B の 3 つの観点での影響度を掛け合わせることで，複数観点を統合的に評価可能としている．しかしながら，今回提示した手法では，H&S，E，B の各観点を同じ重み付けで評価しているが，業界や事業者の特性に応じていずれかの観点に重み付けをすることが必要となる場合が考えられる．現状ではこのような場合への柔軟な対応ができないため，「△」とした．

5. まとめと今後の課題

本論文では，社会インフラ等の制御システム事業において，事業全体のリスクを抽出しそれらを俯瞰したうえで優先的に対策すべき業務/システムの把握を可能とする，事業レベルでのリスク分析手法を提案した．事業の入出力および構成要素に着目した汎用的な事業モデルおよび周辺事業との依存関係や事業内の業務間の関係を明確化する事業内・外モデルを立案し，H&SEB の観点で事業リスクの網羅的な抽出と評価を実施することで，高い事業リスクに関連する業務/システムの特定を可能とした．

今後は，より多くの実事業への適用を通じて，手法の実現性評価や課題抽出を実施し，手法の改良を実施する予定である．たとえば，現状のリスクレベル見積り手順では，H&S，E，B の 3 つの観点に対して同じ重み付けで評価したが，業界や事業者の特性に応じて H&S，E，B のいずれかの観点に重み付けをしたり，観点そのものを変更したりすることが必要となる場合が考えられる．このような分析対象ごとのカスタマイズに関しても今後検討をしていく．

また，本論文で提案した事業レベルでのリスク分析手法では，現段階では定量評価を導入できていない．今後より客観的な分析とするために，まずは [Step3] リスクレベル見積りの部分で定量評価を導入していく予定である．将来的には，[Step1]～[Step4] の手順全体において定量評価を取り入れることを今後検討していく．

謝辞 本研究は，総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人：NEDO）によって実施されています．

参考文献

[1] ICS-CERT, ICS-CERT Incident Response 2016 (2016), available from ⟨https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf⟩.
[2] IEC: Industrial communication networks – Network and system security – Part2-1: Establishing an industrial automation and control system security program (2013).
[3] NISC：重要インフラの情報セキュリティ対策に係る第 4 次行動計画 (2017)，入手先 ⟨https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf⟩.
[4] 益田美貴, 高野研一：ビジネスインパクト分析への HAZOP 手法の適用，安全工学，Vol.50, No.5, pp.292–301 (2011).
[5] 西川 智，福島誠一郎，矢代晴実：サプライチェーンを考慮した地震時事業継続のためのリスク解析手法の提案，日本建築学会環境系論文集，Vol.73, No.630, pp.1053–1060 (2008).
[6] IPA：共通脆弱性評価システム CVSS 概説, 入手先 ⟨https://www.ipa.go.jp/security/vuln/CVSS.html⟩.
[7] International Finance Corporation: General Environmental, Health, and Safety Guidelines (2007).
[8] 日本規格境界：ISO/IEC 27001:2013 情報セキュリティマネジメントシステムの国際規格 (2014).

熊谷 洋子 （正会員）

2000 年東京農工大学大学院生物システム応用科学研究科修了．同年（株）日立製作所入社．現在，同社研究開発グループシステムイノベーションセンタ主任研究員．情報セキュリティ技術，制御セキュリティ技術等の研究開発に従事．

松原 佑生子 （正会員）

2007 年津田塾大学学芸学部情報数理科学科卒業．2009 年お茶の水女子大学大学院人間文化創成科学研究科理学専攻修了．同年（株）日立製作所入社．現在，同社研究開発グループシステムイノベーションセンタ研究員．情報セキュリティ技術，制御セキュリティ技術等の研究開発に従事．

内山 宏樹 （正会員）

2001 年京都大学工学部電気電子工学科卒業．2003 年京都大学大学院情報学研究科通信情報システム専攻修了．同年（株）日立製作所入社．現在，同社研究開発グループシステムイノベーションセンタ主任研究員．情報セキュリティ技術，制御セキュリティ技術等の研究開発に従事．電気学会会員．博士（情報学）．CISSP．

鍛 忠司 （正会員）

1996 年大阪大学大学院基礎工学研究科物理系専攻情報工学分野博士前期課程修了．同年（株）日立製作所入社．入社以来，情報セキュリティ，制御システムセキュリティ技術の研究開発・標準化等に従事．博士（情報科学）．IEEE CS 会員．

藤田 淳也

2011 年東京大学大学院工学系研究科修士課程修了．同年（株）日立製作所入社．現在，同社研究開発グループにて制御用組込みシステム開発技術，制御システムおよび制御機器向けサイバーセキュリティ技術の研究開発に従事．IEEE，国際計測制御学会（ISA）各会員．技術士（情報工学部門），CISSP，CISA．

中野 利彦

1980 年日立製作所入社，情報制御システムの人工知能技術やセキュリティ技術の開発を経て，現在，社会インフラシステムおよび IoT システムにおけるセキュリティソリューション開発に従事するとともに，政府関連委員会の委員等を務める．博士（工学）．