氏名（本籍）	蒋　成栄　（中華人民共和国）
学位の種類	博士（工学）
学位記番号	甲第204号
学位授与の日付	平成29年3月22日
学位授与の要件	学位規則第4条第1項該当
学位論文題目	情報システム開発におけるリスクマネジメント方法に関する研究
論文審査委員	（主査）教　授　森　雅俊
	（副査）教　授　秋葉　知昭
	教　授　谷本　茂明
	教　授　鴻巣　努
	准教授　滝　聖子

学位論文の要旨

情報システム開発におけるリスクマネジメント方法に関する研究

本研究では，情報システム開発において生じるリスクに注目しリスク分析手法及び評価を提案することを研究目的とする．

近年，情報化が進むにつれて，企業は情報システムへの依存度が高くなっている．企業の情報化が進む中，1980年代から日本企業は情報システム開発人材不足とコスト高騰を抑えるために，海外でのソフト開発を拡大している．現在，日本から海外への発注総額は世界三位になっている．日本の情報システムオフショア開発には，一般的な製品生産と異なって，特有なリスクが存在している．日本企業が情報システムオフショア開発におけるリスクを把握するため，リスクマネジメント方法を研究し，リスクマネジメントの適用化も図りたい．

情報システム開発プロジェクトにおけて，組織がプロセスをより適切に管理できるため，能力成熟度モデル統合(CMMI)を遵守する．本研究はCMMIのリスクマネジメント手法の上に，コンジョイント分析方法を加えたリスクの分析方法を検討する．

また，企業や組織の運営において，情報セキュリティのリスクが存在している．情報セキュリティリスクの発生は，企業や組織に大きな被害をもたらす．情報システムの活用がますます増えており，情報セキュリティは企業経営の中で非常に重要な問題となっている．情報システム運用開始後に情報システムの脆弱性を修正するには多大なコストがかかる．未然防止のため，情報システムの開発時から情報セキュリティリスクを管理し，対策を取りすべきと思われる．

従来，一般に実施しているリスクマネジメントのリスク分析手法としては，PMBOK で記載しているマトリックス分析が主なものである．この方法はリスク発生確率と評価したリスク影響値を乗じて，リスク値を決める．しかし，情報セキュリティリスクを分析する場合，分析要因は情報資産，脅威と脆弱性の 3 つであるが，脆弱性と脅威の間に依頼関係がある．各脆弱性の間の連鎖関係がリスク値に影響が与えるため，既存のマトリックス手法ではリスク分析する際に不十分である．つまり，脅威が複数の脆弱性を原因として，リスクを招いているが，脆弱性も互いに影響を及ぼす．従来手法でリスクを分析する方法は各脆弱性間の関係が考えられてない．また，脆弱性は相互の影響が存在しているので，一つ脆弱性に対して対策すれば，他の関連ある脆弱性の発生確率は変わる．従来の手法ではこの変化を表することができない．このため，連鎖的な因果関係を表現できるリスク分析手法が必要である．そこで本研究では，ベイジアンネットワークを用いて情報システム開発におけるセキュリティリスク分析手法をモデル化し連鎖的な因果関係を表現できるリスク分析手法を提案した．

本論文では次のような構成をとる．第 1 章では研究背景を詳述し，本研究の目的と意義について述べる．その中に，本論の新規性及び立ち位置について闡明する．第 2 章では情報システム開発におけるリスクマネジメントを考察し，現状と既存課題を分析する．第 3 章ではオフショア開発プロジェクトリスク分析手法に対する研究を行う．コンジョイント分析に基づきオフショア開発プロジェクトリスク分析手法を提案する．第 4 章では情報セキュリティリスクとリスクマネジメントを考察し，現状と既存課題を分析する．第 5 章ではベイジアンネットワークに基づきリスク分析モデルを提案する．最後本論の終章，第 6 章で，研究結果をまとめて，コンジョイント分析に基づきオフショア開発プロジェクトリスク分析手法及びベイジアンネットワークを利用したリスク分析の手順を整理し新たなリスク分析手法を提案する．

以上のように，本研究では情報システム開発におけるオフショア開発プロジェクトリスクと情報セキュリティリスク分析手法の改善に有用な結果が得られた．

審 査 結 果 の 要 旨

本論文は、「情報システム開発におけるリスクマネジメント方法に関する研究」をテーマにしており、情報システム開発におけるリスクマネジメントに注目し、その中でリスク分析の方法を提案している。特に、オフショア開発に焦点を絞り、オフショアによるシステム開発のリスク分析を研究した。

１．　研究対象と範囲

本論文の研究対象は、オフショアによる情報システム開発において、日本の企業が発注元となり、発注先が中国系企業の開発するプロジェクトのビジネス形態を対象としている。対象範囲として、情報システム開発のモデルは、ウオーターフォール型開発であり、システ

ムの種類は、企業の業務系アプリケーションシステムである。特に、経理会計システムを開発するプロジェクトチームにアンケートを依頼した関係でこの分野の特色が反映された。

2．　課題と研究目的

研究課題としては、情報システムのオフショア開発におけて，発注側と受注側は各自の利益や立場から考えると，リスクに対する分析の結果が異なる可能性が高い．問題点としては，オフショア開発プロジェクトのリスクを評価する際に，リスクの大きさは，リスク影響度とリスク発生確率により求めるが,オフショア開発プロジェクトにおける各リスク項目の影響度を定量的な数値で表すことが難しい．つまり、オフショア開発プロジェクトにおける複数のリスク影響度を定量的な数値で表すことが難しい.そこでこれらの課題を解決するために「研究目的１：コンジョイント分析を用いたプロジェクト・リスク分析を研究する．」を定めた。

研究目的２としては、情報セキュリティの脆弱性を確定する場合，各脆弱性間の関係が考えられてない．脆弱性は相互の影響が存在しているので，一つ脆弱性に対して対策をすれば，他の関連ある脆弱性の発生確率は変わる．

従って，問題点を解決するために，「研究目的２：ベイジアンネットワークを用いて，現在のリスクマネジメント手法を改善する」を設定した。

3．　研究方法

１）オフショア開発の問題点を解決するために，コンジョイント分析を用いたプロジェクト・リスク分析を研究する．

情報システムのオフショア開発における各リスク項目を分析する際に，コンジョイント分析の流れは下記の通りである．

① プロジェクトのリスク要因とリスク項目を特定する．

② 複数の評価用プロジェクトのプロファイル(Profiles)を作成する．

③ 調査対象者にこれらのプロジェクトのプロファイルを評価してもらう．

④ それぞれのリスク項目が回答者に与える効用を数値化したもの(効用値と呼ばれる)を表する．

効用値を用いて，リスク値を確定するため，CMMI－DEVのリスクマネジメントのプロセスにコンジョイント分析をツールとして導入することを考慮し，既存プロセスを改善する．

２）ベイジアンネットワークを利用した

情報セキュリティのリスクの分析方法を述べる．ここでベイジアンネットワークについて解説し，情報セキュリティマネジメント中のリスク分析手法での適用をする．適用の研究について，ベイジアンネットワークによりリスク分析モデルの構築を行う．まず，本研究での情報セキュリティリスクは情報システム開発におけるリスクを対象とする．次にモデルの構築手順を論述し，新たなリスク分析手法を提案する．

4．　提案

研究目的１として，提案の 1 つ目は，コンジョイント分析を用いて，リスクの影響度を基づきリスク値評価方法を定量化し，この定量的なリスク影響度を算出するため，コンジョイント分析を CMMI-DEV のリスクマネジメント・プロセスに追加し，組み合わせたリスクマネジメント・プロセス改善案を提案した．研究目的２として，ベイジアンネットワー

クは相互影響が存在している各リスクの間に因果関係を図で表示できるために，情報セキュリティの情報資産・脅威・脆弱性を示すことにより，便利性があることが明らかになった．ベイジアンネットワークの CPT で確率を算出する方法があることから，リスク分析する際に，適切な方法であると考え，ベイジアンネットワークを用いた情報システム開発における情報セキュリティのリスク分析手法を提案した．

5．まとめ

本研究は，情報システム開発におけるリスクマネジメント方法いついて，研究したものである．コンジョイント分析を用いて，リスクの影響度を基づきリスク評価方法と，ベイジアンネットワークを用いた情報システム開発における情報セキュリティのリスク分析手法について重要な知見を得たものとして価値ある集積であると認める．従って，学位申請者の蒋成栄は博士(工学)の学位を得る資格があると認める．