6ZC-02

業務の電子化における網羅的なリスク特定手法の提案*

稲田　陽一†　　後藤　厚宏†
情報セキュリティ大学院大学†

1.　はじめに

現代の企業において情報システムは幅広く利用されており，旧来人手で行ってきた業務を大幅に代替するに至っている．業務の電子化にあたっては電子化による新たなリスクが発生することがあり，ひとたびリスクが顕在化した場合には業務の停止や機密情報の漏洩など，大きな被害が発生することも珍しくない．一方，業務電子化の企画は往々にしてリスクおよび情報システムの非専門家である業務を所管する部署により行われることが多く，電子化の企画におけるリスク特定が網羅性を欠くために企画時において特定されていないリスクが顕在化して対策などで多くの工数が発生することがある．
本稿ではリスクおよび情報システムの非専門家でも実施可能かつ，網羅性の高いリスク特定手法を提案することにより，未特定リスクの減少を図る．

2.　業務の電子化におけるリスク特定の課題

近年，多くの企業においてはシステムリスクを包含するリスクマネジメント体制が整備されており，リスクの特定から対応に至るまでのプロセスが整備されている［1]．しかしながら近年地方公共団体の災害拠点病院が公表したランサムウェア感染事案の報告書［2]において，「サイバー攻撃による事業継続リスクが存在するという認識（中略）はなかった．」と述べられるなど，リスクマネジメント体制を有する組織でも，必ずしもシステムリスクの特定が十分に行われているとは言い難い現状がある．これは企業において行われるリスク特定の手法がリスクや情報システムの非専門家によるブレーンストームのような非体系的なものにとどまり，体系的かつ網羅的なリスク特定が行われていないことに要因があると考えられ，非専門家でも実施が可能かつ体系的，網羅的なシステムリスク特定手法が必要である．

3.　提案手法

リスク特定手法はJIS　Q31010　[3]等で多くの種類が挙げられている．本研究においてはこの中で HAZOP に着目して非専門家でも可能なシステムリスク特定手法を考察する．これは HAZOP が元々化学プラントなど複数のシステム間でのプロセスを持つ産業で利用されているリスク特定手法であり，「多い/少ない」「早い/遅い」等のガイドワードからプロセス間の相互作用における「意図した動作とのズレ」を導き出し次いでそのズレを引き起こすハザードを特定する手法であるために，相互に作用する要素を有する情報システムにおけるリスク特定に適すると考えられるためである．
本提案手法においてもリスク特定を「意図した動作とのズレ」の特定とそれを引き起こすハザードの特定という2段階で行うこととし（図　1），「意図した動作とのズレ」の特定には土井，内田［4]が提案した機密性/完全性/可

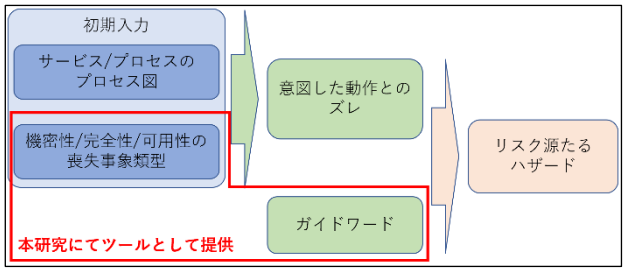

図　1：提案手法の段階

用性を軸とする手法を一部取り入れ，ハザード特定にはWinther ら［5]の提案した HAZOP 拡張手法における Post-Guideword および Attribute を利用することとした．
具体的には，非専門家によるリスク特定を可能とするために 9 つの動作類型を定義して，「意図した動作とのズレ」を特定する段階ではその動作ごとの機密性/完全性/可用性の喪失類型を提示することとし（図　2），ハザードの特定においては Post- Guideword および Attribute の組み合わせ（図　3）のうち，重複が認められるものおよ

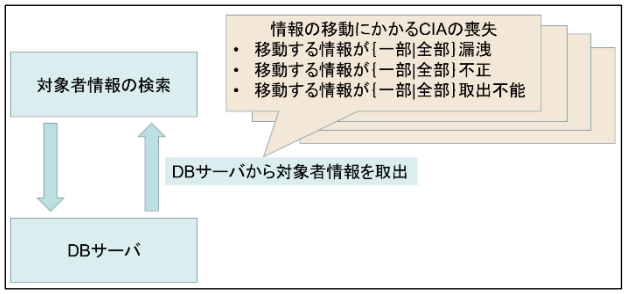

図　2：動作類型毎の CIA 喪失例

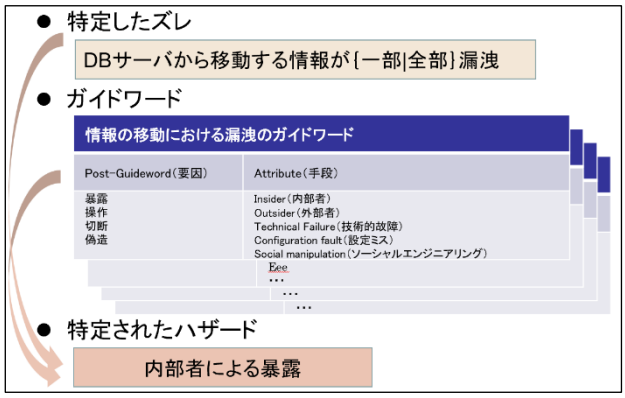

図　3：Post-Guideword と Attribute の組み合わせによるハザード特定例

びシステムの構成によって論理的に発生し得ないものをあらかじめ排除し，残ったものを当該システムで発生し得るハザードとしてリスク特定者に提示することとした．

*Proposal of Comprehensive Risk Identification Method in Digitalization of Business
†Yoichi Inada, Atsuhiro Goto
†Institute of Information Security

また，ハザードを抑止する要因の有無により当該システムで発生しないハザードを排除するとともに軽微なシステムにおいて過大なリスク特定が行われないよう，システムで扱う情報の種別およびバックアップの有無によっても特定されるハザード数を絞ることとした．

4. 網羅的なリスク特定を可能とするツール

本提案手法をリスクおよび情報システムの非専門家が実施できるよう Excel ワークシートを利用して提案手法のツール化を行った．
ワークシートにおいては，対象システムにおける①発生する動作，②ハザードを抑止する要因の有無，③システムの重要度を決定する要因の有無を所定の欄に入力することで，対象システムにおいて発生し得る意図した動作とのズレおよびハザード，また各ハザードが起こしうる意図した動作とのズレの対応を表示することとした．なお，対象システムで起こり得るハザードおよびリスクの判定にはExcelの関数を利用し，Excelのフィルタ機能を利用して表示を絞り込むことで起こり得る「意図した動作とのズレ」及びハザードが表示されるようにした．

5. 企業における検証と結果

前項で作成したツールを利用し，企業内研修への従業員のアサインを電子化するというモデルケースを想定して，従来手法（ブレーンストーミング）でのリスク特定及び社内リスク専門家によるリスク特定との比較を行った．
従来手法と本提案手法においては著者所属企業の研修所管部署および調達部署の協力を得て各部署から 2 名ずつの要員派遣を受け各部署 1 名ずつのチームを 2 つ組み，従来手法と本ツール利用を 1 チームずつ振り分けてリスク特定を実施した．
結果として，従来手法では意図した動作とのズレおよびハザードがそれぞれ 13 件特定されたのに対し，ツールを利用した場合には意図した動作とのズレが 19 件，ハザードが 108 件特定された．専門家によるリスク特定では「意図した動作とのズレ」が 17 件特定され，ハザードについては 35 件が特定された．従来手法において特定されたAttribute8 件およびPost-Guideword8 件のうちツールでも特定されたものが Attribute7 件，Post-Guideword8 件であり，ツールで特定された Attribute13 件および Post-Guideword13 件のうち，従来手法で特定されたものがAttribute7件，Post-Guideword6 件であった．
専門家により特定された Attribute15 件および Post-Guideword8 件のうち，ツール利用において特定されたものはAttribute9 件，Post-Guideword6 件であり，ツール利用において特定されたうち，専門家によるリスク特定において特定された Attribute は 4 件，Post-Guideword は7件であった．
本ツールを利用したチームはハザードの発見において従来手法と比してより多くの Attribute および Post-Guidewordを発見することができ，本提案手法によってリスク特定者の知識不足を補完し，現在手法より網羅的にリスク特定を行い得ることが示唆された．

6. 今後の課題

本提案手法におけるコンセプトにおいては，①リスク特定対象システムの要件の理解及び特定された「意図した動作とのズレ」およびハザードの理解が必要であり，情報システムに関する一定の知識を要することおよび，②2段階の特定ではハザードと「意図した動作とのズレ」の紐づけにおいて 1 つのハザードに対して多くの「意図した動作とのズレ」が紐づけられ，特に大規模なシステムにおいてはシステム内で発生する動作が多くなることからハザードとリスクの対応の把握と優先度付けが困難になること，③提案で利用した HAZOP の手法において，ガイドワードによるリスク特定においてはガイドワードに記載されていない事柄に関する特定が手薄になると考えられ，専門家によるリスク特定手法であるデルファイ法やリスク特定者が各種想定を行うシナリオ分析などのリスク特定手法と比して非網羅的なリスク特定となることが課題として考えられる．
また，手法においては，④今回のリスク特定においては「意図した動作とのズレ」の特定軸に機密性/完全性/可用性を採用したものの，専門家によるリスク特定において特定された「共有サーバの更新（バージョンアップ、脆弱性対応）が遅れる」のように，CIAに直接分類することが困難な「意図した動作とのズレ」が特定されず，網羅性について欠けがあることおよび，⑤独自に定義したシステム動作類型に重複が見られる（情報の移動は情報の書込みと削除，作成及び保存を含んでいるなど）こと，⑥提案手法において用いた Winther らによるガイドワードは要因と手段を具体的に表していることから，他のHAZOP拡張ガイドワードと比して特定され得るハザードの大枠が限定されたものとなっており，ネガティブワードを組み込むことが困難であるほか，Wintherらのガイドワードに含まれない組織的な要因によるハザードが特定されないことが課題として考えられる．
このうち①についてはリスク特定組織においてシステム開発に要する前提知識の定義を行うことにより，③および⑥についてはガイドワードの取捨選択を行うことにより課題の低減が考えられる．また，⑤については Kilov ら [6]による CRUD の利用などが考えられ，今後その他の課題も含め解決に取り組みたい．

参照文献

1. **横田絵里 ， 妹尾剛好.** 日本企業におけるマネジメント・コントロール・システムの実態：質問票調査の結果報告. 三田商学研究 / 53 (2010) / 53(6) 201102, 2011/2.
2. **つるぎ町立半田病院.** コンピュータウイルス感染事案有識者会議調査報告書.
3. **日本産業標準調査会.** リスクマネジメントーリスクアセスメント技法（JIS Q31010）.
4. **土井智朗 ， 内田勝也.** 情報セキュリティ意識向上に向けた効果的なリスクアセスメント手法の提案. 情報処理学会研究報告 2008 (122)43-48 (Dec. 2008).
5. **WintherRune, JohnsenOle-Arnt , GranAxelBjørn.** Security Assessments of Safety Critical Systems Using HAZOPs. SAFECOMP 2001: Computer Safety, Reliability and Security pp 14-24, 2001/9.
6. **KilovHaim.** From semantic to object-oriented data modeling. Systems Integration'90. Proceedings of the First International Conference on Systems Integration, 1990.