

ガイドワードを利用した、業務の電子化における 網羅的なリスク特定手法の提案

Proposal of Comprehensive Risk Identification Method Using Guidewords in Digitalization of Business

稲田 陽一・マネジメント分科会・情報セキュリティ大学院大学

While many companies are digitizing their business operations, risk identification for digitization is often performed by non-experts in information systems and risk, and therefore often has issues with comprehensiveness. This study proposes an exhaustive risk identification method that can be implemented by non-specialists, thereby preventing the occurrence of unexpected problems when companies computerize their business operations.

1. 業務の電子化におけるリスク特定

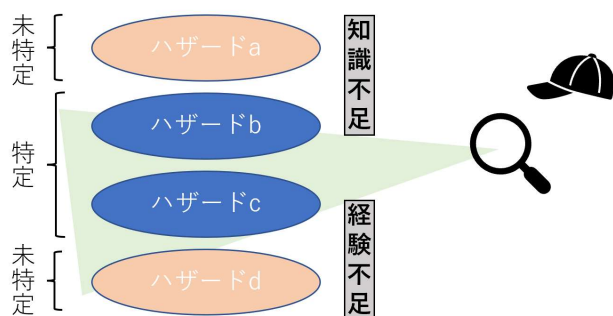
・ 業務の電子化

組織において行われる業務は、RPAなどによって自動化が進められている。実施主体は部や本部など、比較的小規模であることが多い。

・ リスク特定における網羅性の欠如

業務の電子化では、電子化により発生するリスクをあらかじめ想定することが必要だが、部/本部単位の電子化ではリスク特定者は部署内の要員であることが多い。

→リスク特定者の知識や経験不足による、リスク特定の網羅性欠如が発生



2. 非専門家が実施可能かつ網羅的なリスク特定手法

・ 2段階でのハザード特定

①動作類型とCIA喪失類型から「意図した動作とのズレ」を特定

-動作類型:「読み込み」「書き込み」「消去」など9種類

-CIA喪失類型:「機密性の喪失」「完全性の喪失」「可用性の喪失」の3種類
→各動作類型におけるCIA喪失類型を定義し、当該システムにおけるプロセス図に適用。

例)「書き込み」における「機密性の喪失」→「書き込んだデータの意図せぬ開示」

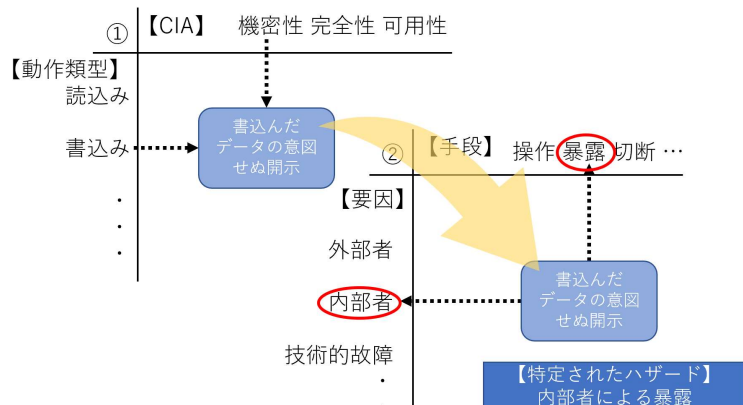
②2種類のガイドワードから「意図した動作とのズレ」を引き起こすハザードを特定

-ガイドワードa: ハザード要因(「内部者」「外部者」「技術故障」など15種類)

-ガイドワードb: 要因が行う手段(「操作」「暴露」「切断」など13種類)

→ガイドワードa,bの組み合わせにより「意図した動作とのズレ」を起こし得るハザードを特定

例)「書き込んだデータの意図せぬ開示」を起こし得るハザード→内部者による暴露



3. 提案手法のツール化

・ リスク特定者負担軽減のためハザード候補を絞り込み

①他と重複するハザードを排除

例)火災による持ち去り→内部者/外部者による持ち去り

②当該の動作で発生しないハザードを排除

例)削除した情報の消去→意図した動作とのズレではない

③ハザード発生を抑制する要因によるハザード候補の排除

例)予備機器がない→予備機器に起因するハザードの排除

・ Excelワークシートにより実装

①システム要件を入力

②起こり得るズレとハザードの表示

4. 提案手法の検証

・ 提案手法×従来手法: 網羅性向上を確認

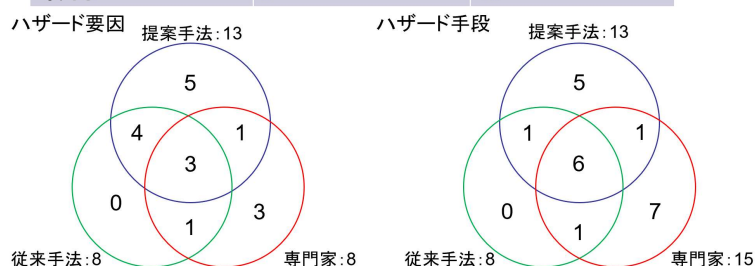
提案手法×専門家: 特定されるハザードに差異

・ 比較対象: 提案手法, 従来手法(ブレンストーミング), 専門家によるリスク特定

・ 評価軸: ハザード要因&手段の網羅性

・ モデルケース: 社内研修への対象者アサインの自動化

特定手法	特定されたハザード要因	特定されたハザード手段
提案手法(業務部署)	13	13
従来手法(業務部署)	8	8
専門家	8	15



※従来手法と提案手法のリスク特定は業務部署役職員により2時間で実施