L-001

ヒューマンエラーの観点を取り入れた、情報システムのリスク特定手法に関する提案

Proposal on Risk Identification Method for Information System Considering a Viewpoint of Human Error

山本 英朗† 五郎丸 秀樹†
Hideaki Yamamoto Hideki Goromaru

1. はじめに

著者らは、情報システムを対象に、最上流工程でのセキュリティ対策を意識したリスクマネジメント手法を検討してきた[1][2][3]。情報システムを用いた業務には人間の行動が伴うため、ヒューマンエラーに起因するインシデントを未然防止するよう業務要件に盛り込むことが重要である。そこで、情報システムを用いた業務に従事する人間に着目したリスクマネジメント手法の検討の一環として、ヒューマンエラーの観点を取り入れたリスク特定手法を提案する。

本稿では、構成要素に着目したリスク特定のみではヒューマンエラー起因リスクの特定に漏れが生じること、及び、本提案が当該特定漏れの低減に大きく寄与することを、IoT システムを例に挙げて報告する。

2. ヒューマンエラーの観点を取り入れる背景

人間(サービス提供者・サービス利用者)が介在する情報システムでは、ヒューマンエラーを要因とする重大なインシデントの低減が重要課題である。とりわけ、IoT(Internet of Things)の進展に伴い、IoT の特徴に起因した下記の要因が加わり、ヒューマンエラーを低減化するリスクマネジメントの重要性が益々高まっている。

① 多数のデバイスが存在し長期間動作するため、人手による管理上のミスを起こしやすい
② ひとつのシステムにステークホルダが多数存在し、全体像が見えにくい
③ 利用されるデバイスは多岐に渡り、前例のないサービスであることが多い

3. 提案手法

3.1 人間の失敗原因と作業項目とのマトリクス

JIS Q 31000 において、リスク特定は、「リスクを発見、認識及び記述するプロセス」と定義されており、リスクは、「リスク源・事象・結果の組合せ」が注記として示されている[4]。著者らは、事象・結果の背後要因である「リスク源」に着目した対応が、リスクを低減させる手段として最も効果があると考える。本検討では、人間が介在する情報システムにリスク特定を行うため、人間が失敗する原因に着目した。

人間の失敗に関する先行文献として「失敗まんだら(原因/行動/結果)」が知られている。これは、失敗事例を分析して教訓を抽出し、知識として活用する活動として「失敗の原因→行動→結果」を分類して体系化したものである[5]。「失敗まんだら(原因/行動/結果)」のうち、「失敗まんだら(原因)」では、失敗原因が体系化されている。

著者らは、情報システムの業務を複数の作業項目に細分化し、これらの作業項目に対して、前記失敗原因の観点でリスクを特定する手法を考案した。このリスク特定に用いる様式を表 1 に示す。表 1 の様式の行に作業項目を記述し、当該作業で想定されるリスクを、各列に記載された失敗要因(小項目数 27)に照らしながら記述する。

表 1　本提案にかかるリスク特定様式 [1]

原因	個人に起因する原因														個人・組織のいずれにも責任にもできない原因	組織に起因する原因									誰の責任でもない原因	
	無知		不注意			手順の不遵守		誤判断			調査・検討の不足			環境化への対応不良	企画不良			価値観不良		組織運営不良			未知	
作業番号及び項目	知識不足	伝承無視	理解不足	注意・用心不足	疲労・体調不良	連絡不足	手順無視	狭い視野	誤った理解	誤認知	状況に対する誤判断	仮想演習不足	事前検討不足	環境調査不足	使用環境変化	経済環境変化	権利構築不良	組織構成不良	戦略・企画不良	異文化	組織文化不良	安全意識不良	運営の硬直化	管理不良	構成員不良	未知の事象発生	異常事象発生
1																											
2																											
3																											
・・・																											

3.2 提案手法の試行

本提案手法の有効性を検証する目的で、IoT ゲートウェイを用いた IoT システムの業務を対象に、構成要素(IoT ゲートウェイ、IoT システム内に持ち込まれた作業用 PC など)に着目したリスク特定の試行(以下、試行 A)、及び 3.1 章に提案した手法によるリスク特定の試行(以下、試行 B)を実施した。試行対象の主要業務を表 2 に示す。

表 2　リスク特定の試行対象とした業務

ステークホルダ	主要業務
IoT ゲートウェイの製造者	●IoT ゲートウェイの製造・販売・不具合対応 ●エンドユーザの登録 ●アプリケーションの審査・登録・販売
システムインテグレータ	●IoT ゲートウェイの導入、運用請負(受託)
アプリケーション開発者	●アプリケーションの開発 ●製造者へのアプリケーションの登録
エンドユーザ	●IoT システムの運用 ●アプリケーションの購入・インストール ●IoT ゲートウェイの移設・廃止
廃棄業者	●IoT ゲートウェイの廃棄

当該業務における前提は、下記①・②のとおりである。

① エンドユーザへの IoT ゲートウェイの納品は、IoT ゲートウェイの製造者(以下、製造者)から出荷された IoT ゲートウェイにシステムインテグレータが初期設定を行った状態でなされる。

† 日本電信電話株式会社

[1]参考文献[6]を基に著者らが加筆して構成した。

Copyright © 2018 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

② この IoT システムでは、製造者以外の業者(アプリケーション開発者)も IoT ゲートウェイで動作するアプリケーションを開発可能である。エンドユーザは製造者を介して、製造者の審査に合格したアプリケーションをオンラインサイトから購入・利用できる。

4. 結果及び考察

4.1 提案手法の有効性

同一業務を対象に試行 A・試行 B によって特定したリスクの記述を俯瞰し、

① 構成要素の観点でのみ特定できたリスク
② 構成要素・ヒューマンエラー要因のどちらの観点で試行しても特定できたリスク
③ ヒューマンエラー要因の観点でのみ特定できたリスク

に分類すると、図 1 に示すようになった。

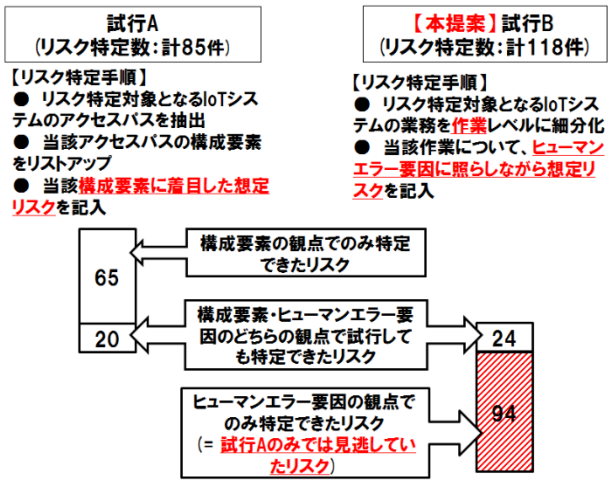

図 1　試行によって特定できたリスクの内訳

試行 A でもヒューマンエラー起因リスクを特定できたものの、試行 B で特定したリスクのうち「94 件」は試行 A では見逃していたこととなる。人間が介在する情報システムのリスクマネジメントにおいて、試行 A のみに頼ったリスク特定では、ヒューマンエラー起因リスクの漏れが生じる点で不十分であることがわかった。試行 A・試行 B の結果の分析を通じて、本提案がヒューマンエラー起因リスクをより網羅的に特定できる点で有効であることを確認した。

4.2 リスク特定対象の業務とヒューマンエラー要因との関連

試行 B で特定したリスクについて、各業務の性質とヒューマンエラー要因との関連について考察する。

試行 B において最も多く特定できた要因は「注意・用心不足」「疲労・体調不良」に属するリスクであった。これらのリスクは「～を設定する」「～を出荷する」「～をシステムに登録する」など比較的定型的な作業において特定できたほか、比較的高度な判断を伴う作業においても特定できた。

これに次いで多く特定できた要因は「連絡不足」「手順無視」「理解不足」であった。これは、対象業務におけるステークホルダ間でのモノ・情報の授受に関する作業が多いことによるものと考える。

また、本試行では、「知識不足」「狭い視野」に属するリスクも特定できた。今回の試行には、修理や不具合対応時に不可欠な原因切り分け業務が含まれている。技術的知識の欠如や判断誤りによる原因切り分け業務の遅延が、エンドユーザの業務の正常化に支障を来たすことになる。

この分析から、ヒューマンエラー要因について、下記①～③の傾向を確認できた。

① 「不注意」は、業務の性質に依存せず、さまざまな業務において特定されやすい。
② 「手順の不順守」は、ステークホルダ間での情報伝達を伴う業務において特定されやすい。
③ 「無知」「誤判断」は、障害切り分けや審査など、比較的高度な判断を伴う業務において特定されやすい。

本提案では、リスク特定対象の作業項目数とヒューマンエラー小項目数との積のカラム(本試行では約 4000)から構成される表を用いるため、リスク特定作業が煩雑となる。本提案によるリスク特定を効率良く実施するには、リスク特定対象の業務が、どの失敗要因に該当するかの予測をつけておくのが有効で、当該業務がそれぞれ前記傾向(①～③)のどれに該当するのかを事前に把握しておくのが望ましいという知見を得た。

5. おわりに

著者らは、情報システムのセキュリティ設計をより網羅的に行う目的で、当該システムの業務に関与する人間に着目し、ヒューマンエラーの観点を取り入れた、情報システムのリスク特定手法を提案した。

著者らは、IoT ゲートウェイを用いた IoT システムに 2 つのアプローチによるリスク特定を試行し、構成要素に主眼をおいたリスク分析は、ヒューマンエラー要因のリスク特定漏れが生じる点で望ましくないことを例示した。そのうえで、ヒューマンエラーの観点を取り入れたリスク特定が、ヒューマンエラー起因リスクをより網羅的に特定できる点で有効であることを明らかにした。さらに、業務の特性とヒューマンエラー要因との間にはある程度の相関があることがわかり、リスク特定対象の業務の性質を予め把握しておくと、重点的に着目すべきヒューマンエラー要因を予測できるため、本提案を用いたリスク特定の効率化に寄与すると考える。

参考文献

[1] 山本英朗, 佐伯拓也, 亀石久美子, 二又俊仁, “情報システムにおけるセキュリティ設計手法の提案”, 2016 信学総大予稿集, pp.182 (2016).
[2] 佐伯拓也, 山本英朗, 亀石久美子, 二又俊仁, “情報システムにおけるセキュリティ設計手法の実践”, 2016 信学総大予稿集, pp.183 (2016).
[3] 石倉禅, 山本英朗, 仁佐瀬剛美, 間形文彦, “IoT システムのセキュリティ設計に関する考察”, 4E2-1, 2018 年 暗号と情報セキュリティシンポジウム予稿集(2018).
[4] JIS Q 31000 :2010, “リスクマネジメント−原則及び指針”
[5] “失敗知識データベースの構造と表現”, http://www.sozogaku.com/fkd/inf/mandara.html (参照 2018-06-29).
[6] 畑村洋太郎, 中尾政之, 飯野謙次, “失敗知識データベース構築の試み”, IPSJ Magazine, Vol.44, No.7 (2003).

Copyright © 2018 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.