Vol.2014-SPT-8 No.33
2014/3/28

IT システム運用時におけるインシデント分類に関する一考察

安藤 玲未[†1]　芦野 佑樹[†1]　島 成佳[†1]

IT システムの運用中に発生するトラブルの 1 つに，情報セキュリティインシデントがある．情報セキュリティインシデントに対しては，技術的な対策を立てることが多く，その有効性も検証されている．しかし，ヒューマンエラーに対する対策の立て方にはまだ改善の余地があると考えられる．本研究では，医療や航空などの分野で用いられている複数のヒューマンエラーの未然防止手法を IT 分野に適用し，比較検証を行ったので報告する．

A study of a Classification about Security Incident for IT System Operation

REMI ANDO[†1]　YUKI ASHINO[†1]
SHIGEYOSHI SHIMA[†1]

Information security is revealed the necessity of consideration for human factor. If human factor is relating and causing the incidents, traditional physical and technical countermeasures will not be sufficient. Therefore, it is became our challenge to tackle human factor. This paper describes case studies of applying the human error analysis and the measures plan techniques that have been chiefly used in the medical, aerospace and power and energy field.

1. はじめに

近年，医療システムや航空管制等の重要インフラサービスにおいて，IT システムへの依存度が高くなっている[1]．そのため，IT システムの運用中のトラブルは，国内外の経済活動へ影響を与える．

IT システムの運用中に発生するトラブルの 1 つに，情報漏えいを代表とする情報セキュリティインシデント(以下，インシデント)が挙げられる．インシデントの発生頻度は低減させる必要があり，その対策は情報セキュリティ対策と呼ばれる．情報セキュリティ対策は，過去に発生したインシデントをなぜなぜ分析[2]などの根本原因分析[3]を用いて，再発・未然防止策を立てることが推奨されている[4]．再発・未然防止策を実施しても同様のインシデントが発生する場合は，PDCA サイクル[5]を回すことにより，更なる対策を立てる．情報セキュリティ対策は，(a)物理的セキュリティ対策，(b)システムセキュリティ対策，(c)人的セキュリティ対策，に分類できることが知られている[6] ．(a) は，入退管理や自然災害対策，(b)はアクセス制御やポリシー策定等の情報システム自体に施される対策，(c)は教育・訓練に挙げられるような人の操作ミス等を抑止するための対策がそれにあたる．

人的セキュリティ対策が必要な情報セキュリティインシデント要因の 1 つとして，人の不注意による「うっかりミス」が挙げられる．図 1 は，過去にインターネット上に公開された個人情報漏えい事故を年別，漏えい原因別に表したグラフである[7]．漏えい原因のうち，「誤操作」「管理ミス」「設定ミス」等は人の不注意によるミスであり，2009 年以降はこれらの 3 項目で約 70%を占めている．前述した(a)～(c)の対策が行われているにも関わらず，人の不注意が原因で発生するインシデントの割合が未だ大きい．人の不注意によるインシデントが一向に減少しない現状を踏まえると，(c)人的セキュリティ対策の立て方にはまだ改善の余地があると考えられる．

人的セキュリティ対策の立て方は再発防止と未然防止の 2 つに分類できる．前者は，過去に発生したインシデントと同様もしくは同類のインシデントを防止するための対策である．後者は，インシデントにつながる要因を未然に防止するための対策である．これらは両方とも実施することによって，インシデント発生頻度の低減につなげることができる．しかし，現在の人的対策は，インシデントレポートの共有や，複数人で作業を行う確認作業の多重化などを実施することが多い．このような対策は，直接的な原因にしかつながらず，背後要因の分析が難しいため，主に再発防止策となってしまう．

未然防止策は，医療の現場や，航空宇宙開発の分野等では複数の手法が確立されているため，本論文では IT 分野にも応用することを検討する．JSSA で公開されているヒューマンエラー[8]を例に試験的に分析し，各手法の有効性や改善点等を洗い出したので報告する．

†1 NEC クラウドシステム研究所
NEC Cloud System Research Laboratories

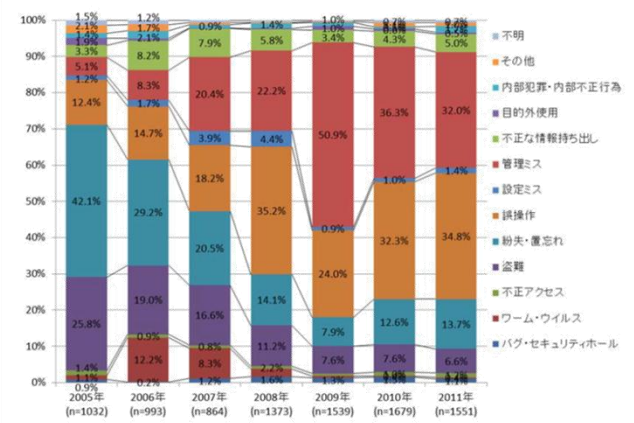

図 1　漏えい原因比率の経年変化(件数)

2. ヒューマンエラー

2.1 取扱い領域

人間と機械などで構成されるシステムにおいて，人間の優れた特性を活かし，マイナス面を適切にカバーすることにより，安全性，信頼性，および効率の向上を目指す学術領域をヒューマンファクタと呼ぶ[9].

ヒューマンエラーとは，ヒューマンファクタのマイナス面の結果を表しており,「達成しようとした目標から意図せずに逸脱することとなった，期待に反した人間行動」と定義されている[10]．ヒューマンエラーは人的ミス，人為ミス等と呼ばれることもあるが，単に人が起こしたエラーではなく，人の不注意や思い込みによるミスをさす．本研究では，IT システム運用中に起こり得るヒューマンエラーを対象とし，検討を進める．

2.2 関連研究

ヒューマンエラーを防ぐ既存研究としては，医療，航空，鉄道，電力等の分野において，エラー要因分析や対策立案を行う手法が確立されている[8][11][12][13].

また, これらの分野の手法を IT 分野に適用した事例もあるが[14]，再発防止策の立案に近くなっている．本論文では，これらの再発防止策の立案手法を更に深堀することにより，ヒューマンエラーの未然防止策の立案に適用する．

2.3 課題の定義

2.2 で述べた再発防止策の立案手法の課題は，インシデントが発生しないと対策案が作られないことである．多層防御[16]の観点では，仮に各対策が完璧なものではなかったとしても，対策を多重化することによりインシデントを防ぐことができる．しかし，ヒューマンエラーをはじめとするインシデントは発生してしまっている．

このようなモデルはスイスチーズモデル[17]として表現されている．そこで本論文での課題をスイスチーズモデルを例に述べる．スイスチーズモデルとは,「インシデントは多重防御壁の穴を全て貫通した時に生じる」という理論である．インシデントを防止するために，リスク管理の観点から多くの防御壁が設けられており，1 つの防御壁が破られても次の防御壁によって事故に至ることを防げる仕組みになっている．しかし，いずれの防御壁にもスライスしたスイスチーズのように，潜在的原因，もしくは即発的なエラーによる大小の穴が開いており，偶然ある状況下で全ての防御壁の穴の位置が重なると，インシデントに至るというモデルである. 本論文では, 防御壁を対策案と置き換え，検討した．

インシデントの発生を防ぐために立てた対策案には，スイスチーズの穴のような想定外の穴が存在している可能性がある．この想定外の穴が重なりヒューマンエラーが発生した際，ヒューマンエラーに直結する対策案の穴しか見えないため，そこに新たな対策が立てられる．しかし，ヒューマンエラーの発生に至ったいくつもの穴を予測しないことには未然防止策を立てることができない．

また，具体的なヒューマンエラーは[8]のような事例が挙げられるが，ヒューマンエラーには企業機密が含まれていることも多いため，通常公開されないことが多く，ノウハウが蓄積されにくい．いかに 1 つのインシデントから複数のヒューマンエラーを防止できるかが大事である．

そこで本研究では，1 件のヒューマンエラーから，今後起こり得るインシデントをできるだけ多く予測することを目的とし, 他分野で利用されている手法の比較検討を行う．

3. ヒューマンエラー分析手法の検討

ヒューマンエラーの分析には，医療，電力，航空の分野にて代表的な分析手法である Medical SAFER[14], FTA[18], FMEA[15]を用いた．Medical SAFER 及び FMEA は，分析対象を情報セキュリティにおけるヒューマンエラーを対象とするよう，分析方法を多少変更する必要があるが，既存研究を参考に適宜変更して説明する[14][15].

今回は，システム監査学会(JSSA)が「ヒューマンエラーの事例と影響」として公開しているヒューマンエラー54 件のうち，筆者が独自に IT システムの操作ミスと分類した 14 件を対象に分析を行う．表 1 に示す事例はそのうちの 1 件である．この事例を用いて実際に 3 つの分析手法を用いて分析し，ヒヤリハットの洗い出しの可能性について比較を行った．

事例 : 情報管理室でサーバの管理を担当している A さんは，ウスのドラッグ操作で，サーバ内のフォルダを再編中に，取扱い限定の顧客リストを誤って共有フォルダに格納してしまった．

表 1　ヒューマンエラー事例

3.1 分析手法

3.1.1 Medical SAFER

インシデント発生に至るまでを時系列順に書き出し，問題点やその背後要因をなくすための対策を網羅的に考える手法である．Medical SAFER は元々，実際に医療現場で働

いている人がインシデント分析できるように開発されたため，分析手法に関して専門知識がなくても使えるようなツールが用意されている．分析手順は以下である．

① 事象の整理
② 問題点の抽出
③ 背後要因の探索
④ 考えられる対策案の列挙
⑤ 実施する対策の決定
⑥ 対策の実施
⑦ 実施した対策の効果の評価

以下に各手順の概要を示す．

(1) ①事象の整理，②問題点の抽出

図 2 のような，横軸が関係者や設備，縦軸が時間経過とする時系列事象関連図を作成し，インシデントに至ったと想定される関係者や設備等の相互関係に含まれる問題点を抽出する．

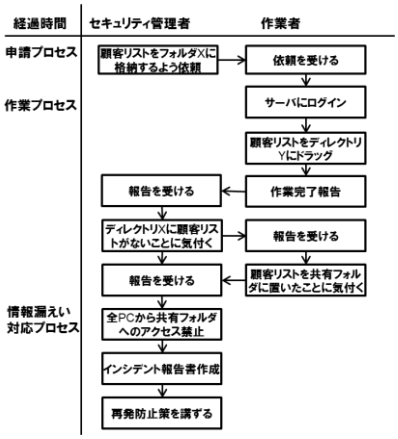

図 2　時系列事象関連図の作成

(2) ③背後要因の探索

図 3 のような，問題点の背後にある背後要因と，背後要因に対する対策を立てる．

	問題点	背後要因	対策
(1)	ドラッグでファイルを移動する	ファイル移動に関するルールがない	右クリックでファイルのコピー・貼り付けをする
(2)	顧客リストのファイルが暗号化されていない	暗号化の方法が明確でない	暗号化についての手順書を作る

図 3　背後要因関連図の作成

(3) ④考えられる対策案の列挙

手順③で検討した対策を図 4 に示す発想手順マトリクスの項目に当てはめ，全ての項目に対し，項目の有無を確認することで網羅性を検証する．発想手順マトリクスは，m-SHELL モデル及び戦略的エラー対策の 4M[19]を組み合わせたものである．

(4) ⑤実施する対策の決定，⑥対策の実施，⑦実施した対策の効果の評価

上記手順④で検討した対策案を 1 つずつ検討・評価し，実施可能かどうかという観点も含め，実施する対策案を決定する．採用した対策を実施した後，アンケート調査やインシデント発生数の推移等により対策を評価する．

		情報セキュリティ対策の思考手順										
		①やめる（なくす）	②できないようにする	③わかりやすくする	④やりやすくする	⑤知覚能力を持たせる	⑥認知・予測させる	⑦安全を優先させる	⑧できる能力を持たせる	⑨自分で気づかせる	⑩検出する	⑪備える
m-SHELモデル	m（マネジメント）											
	S（ソフトウェア）											
	H（ハードウェア）											
	E（環境）											
	L（本人）											
	L（周りの人）											

図 4　発想手順マトリクスの作成

3.1.2 FTA(Fault Tree Analysis)

FTA は原子力プラントの安全性評価等に用いられている手法である．分析対象となる脅威を頂上事象とし，脅威の発生過程における因果関係を表現した故障木とよばれる樹形図を用いて分析する手法である．FTA は，潜在的な原因および頂上事象までの経路を特定すると共に，各原因事象の発生確率が判明している時に，頂上事象の発生確率を計算する定量的手法として利用される．

FTA の具体例を図 5 に示す．FTA は，頂上事象である脅威に対して，その直接的もしくは間接的原因となり得る要因を特定し，AND 論理または OR 論理でツリー構造を作成する．同様に，各要因に対して原因となる事象を特定し，ツリー構造を作成する．末端の原因事象がこれ以上分割不能である，または，発生確率を算出可能となるまで，作業を続ける．

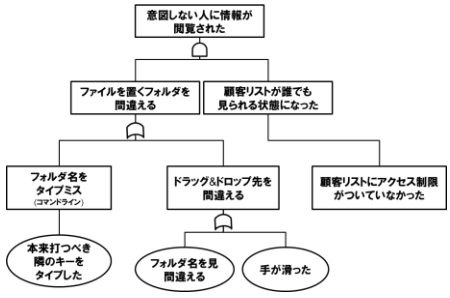

図 5　FT 図

3.1.3 FMEA(Failure Mode and Effects Analysis)

システムやプロセスの構成要素に起こり得る故障モードを予測し，考えられる問題点を摘出し，事前対策を行う手法である．FMEA では，故障モードという概念を用いてインシデント予測を進める．故障モードとは，システムやプロセスの構成要素があるべき姿からかい離した状態である．

FTA が予めシステムやプロセスの事故や故障などの起こしてはならない重大な事象を頂上事象としてとらえ，その発生要因を逐次展開していくのに対し，FMEA はシステムやプロセスの構成要素に着目し，故障モードシステムやプロセス全体への影響ならびに故障モードを検討する手法である．

FMEA は信頼性工学手法であり，航空宇宙開発の分野等において製品の潜在的な故障の危険性を設計段階で洗い出し，その未然防止を図るために用いられていたが，医療分野でもヒューマンエラー防止に FMEA が用いられている[15]．信頼性工学においては，例えば機械の設計書等を元に, 部品を故障モード予測の解析アイテムとして捉えるが，ヒューマンエラーでは作業プロセスを幾つかのサブプロセスに分解し，サブプロセスを故障モード予測の解析アイテムと捉える．手順は以下の通りである．

① 作業プロセスを分析し，サブプロセスに分解する．
② 各サブプロセスで起こり得るエラーを列挙する．
③ 列挙されたエラーについて，発生頻度，影響度などを評価し，リスクの高いエラーを特定する．
④ 特定されたリスクの高いエラーについて，対策案を考え，実施する．

ヒューマンエラーにおける FMEA の表は図 6 の通りである．

番号	サブプロセス	失敗モード	最悪の影響	影響解析			重要度	対策
				発生頻度	影響度	検知難易度		
1	ドラッグでファイルを移動する	ドラッグ先を間違える	意図していない人にまで公開されてしまう	4~5	5	4	5	ファイルの移動は右クリックで行う

発生頻度:
5:日常的にある
4:1年に数回ある
3:1年に1度くらいある
2:1年に1度以下である
1:絶対にない

影響度:
5:ユーザ影響がある
4:ユーザの信用を失う

検知難易度:
5:最終確認で発見できない
4:最終確認までに発見可能
3:その場で発見できる

図 6　FMEA

3.2 分析手法の比較

いくつかの事例を 3.1 で述べた 3 つの手法を用いて筆者が試験的に分析し，手法の有効性を検討した結果を表 2 に示す．今回の評価軸は以下の 2 点である．

1. 手法の有効性
2. 手法の使いやすさ

まず，1．手法の有効性については，

a) ヒヤリハット事例の洗い出しやすさ
b) 洗い出したヒヤリハット事例に対して対策の立案がしやすいこと

2．手法の使いやすさについては，

c) 分析手法に対して専門的な知識がない人にとって使いやすいこと
d) 同様なインシデントにも当てはめることができる対策案を立案することができること

を中心に評価を行った．今回は，1．手法の有効性を重視するが, 現場の人が分析できるよう, 使いやすさや同類インシデントへ対策案が応用できるかについても検討した．この評価軸は[3]を参考にしている．

以下，各評価軸について詳細を述べる．

a) ヒヤリハット事例の洗い出しやすさ

1 つのヒューマンエラーに至るまでの各過程においてエラーの要因となり得る事象を洗い出せることが重要である．FTA はこれ以上分割できない所まで事象を洗い出すため, ヒヤリハット事例を洗い出しやすい．FMEA も，万が一ある要素が故障したら，といったインシデントにつながる可能性がある事項を列挙できるため, ヒヤリハットを洗い出しやすい. Medical SAFER は事実を人別・時系列順に記述していくだけなので, ヒヤリハットも含めて記述することが難しい.

b) 対策立案へのつながりやすさ

対策を立てる際は，1 つのインシデント要因に対し，多面的に対策案を立てることが重要である．Medical SAFER は，m-SHEL モデル及び戦略的エラー対策の 4M を用いたマトリクスを用いて対策案を検討するため，網羅的な対策案を立てやすい．FMEA も各構成要素の故障モードに対して対策案を立てるため, 比較的対策案を立てやすい．一方 FTA は，ツリー構造のどこに焦点を当てて対策案を検討するかが難しい.

c) 使いやすさ

分析手法に対して専門的な知識がない人にとって使いやすいことが大事である．使いやすければ，分析者間で結果のばらつきも少なる．

Medical SAFER は時系列に沿ってヒューマンエラーに至るまでを記述していくものであり, FMEA はフォーマットに従い, 要素を記述していくものであるため, 初めて使う人にも使いやすい手法であると言える. 一方 FTA は，頂上事象をどう定めるかによりその下のツリーが変わってしまう点や, 起こり得る事象を多方面から検討し, 列挙する必要があるため初心者には適していないと考えられる．

d) 分析結果の応用度合い

分析した結果が 1 つのインシデントに対しての対策案だと再発防止策になってしまうため, 立案した対策案が他のヒューマンエラーにも応用できるものかどうかが大事である．FTA は同じ頂上現象が発生する場合でも，基本現象は多数あるため，他のヒューマンエラーにも応用可能だと考えられる．一方，Medical SAFER や FMEA は 1 つのインシデントを具体的な内容に分解して分析し, 対策を立てるので再発防止策となりやすい.

	Medical SAFER	FTA	FMEA
a) ヒヤリハット事例の洗い出しやすさ	△	◎	○
b) 対策立案へのつながりやすさ	◎	△	◎
c) 使いやすさ	◎	△	○
d) 分析結果の応用度合い	△	◎	△

◎:要件を十分に充足している、○充足している、△充足していない

表 2　分析手法の検討結果

3.3 考察

3.3.1 対策の有効性

インシデント分析の際は，ヒヤリハットを洗い出した後，対策案を立てる．ヒヤリハットを洗い出す際には，なぜなぜ分析のように 1 つのインシデント要因を深堀していく手法が良い．そのため，FTA のように，1 つの頂上現象から複数の末端事象まで深堀していく手法が適していると考える．対策案を立てる際は，ここで洗い出した末端事象全てに対策を立てるのは非効率なため，その末端事象の起こりやすさを元に，Medical SAFER の発想手順のマトリクスを用いて多面的に対策案を立てる手法が良い．

3.3.2 手法の使いやすさ

分析を開始するスタート地点が決まると，比較的初心者にとっても分析しやすいことが分かった．FTA のような頂上事象を何とするかにより，その後の分析結果が変わってしまう手法より，Medical SAFER や FMEA のようにプロセスを順に記載する手法の方が使いやすい．

また，ヒヤリハットに対して 1 つずつ対策を立てるのは非効率的なため，1 つの対策案で複数のヒヤリハットに対応したい．Medical SAFER の発想手順のマトリクスは対策案を多面的に検討することができるため，対策案を立てる際の手法に適している．

4. おわりに

本論文では，ヒューマンエラーの未然防止対策の立て方について検証を行った．ヒューマンエラーの未然防止策を立てるには，まずヒヤリハットをできるだけ洗い出せる手法がよく，今回は FTA が適していると考えた．FTA によって洗い出されたヒヤリハットに対して Medical SAFER の発想手順のマトリクスを用いて対策案を立案すると，効率よく未然防止策を立てられると考えている．

本研究は，IT システムの運用中に発生するヒューマンエラーを低減することを最終目標としている．ヒューマンエラーを低減するために，ツールの導入を検討しており，今回の評価にて，ツールの要件には 1.ツール自体の使いやすさ，2.対策案の効果の度合いが重要であることが分かった．より汎用性の高いツールにするため，今後は，今回使用した 3 つの手法をシステム運用者等に使用してもらい，要件を詳細にしていく．

参考文献

1) http://www.nisc.go.jp/inquiry/pdf/it_izon_honbun.pdf
2) 大野 耐一：トヨタ生産方式，ダイヤモンド社，1978
3) 河野龍太郎：根本原因分析，
http://www.jichi.ac.jp/msc/wpgresql/wp-content/uploads/2010/08/ImSAFER-PPT5.pdf，2010
4) http://itpro.nikkeibp.co.jp/article/COLUMN/20131007/509438/
5) PDCA サイクル：
http://www.ipa.go.jp/security/manager/protect/pdca/
6) http://www.utj.co.jp/x-pluspdf/27_security.pdf
7) JNSA：2011 年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～，
http://www.jnsa.org/result/incident/data/2011incident_survey_ver1.3.pdf
8) JSSA 情報セキュリティ研究プロジェクト：ヒューマンエラーの事例と影響，http://www.sysaudit.gr.jp/seika/humanerror.pdf，2007
9) 佐々木良一：IT リスク学，共立出版，2013
10) 日本ヒューマンファクター研究所
11) http://www.sbbit.jp/article/cont1/22926
12) JR東日本研究開発センター 安全研究所：保守用車運転従事者能力向上訓練ツールの開発，2009
13) 東京電力株式会社，「原子力発電所の安全と品質確保のためのヒューマンエラー防止に向けた取り組みについて」，
http://wwwcms.pref.fukushima.jp/download/1/girenH22_7_7.pdf，2010
14) 新原功一：情報セキュリティインシデントに対するヒューマンエラー対策の提案，情報セキュリティ大学院大学，FIT2013
15) 島村瞬：医療機関におけるヒューマンエラーの未然防止に関する研究，中央大学，2007 年
16) 多層防御：
http://itpro.nikkeibp.co.jp/article/COLUMN/20140129/533159/
17) スイスチーズモデル：
http://www.k5.dion.ne.jp/~shikumia/swisscheesemodel.pdf
18) FTA：
http://techon.nikkeibp.co.jp/article/HONSHI/20110927/198652/
19) 河野龍太郎：医療におけるヒューマンエラー―なぜ間違えるどう防ぐ， 医学書院，2004