RN-002

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
A countermeasure of Human error for protecting personal information disclosure

新原 功一† 原田 要之助†
Koichi NIIHARA Yonosuke HARADA

1. はじめに

情報セキュリティインシデントは当事者の過失，即ちヒューマンエラーに起因するものが多く存在する．一方組織の情報セキュリティ対策は技術的対策に偏りがちである．本論文は医療分野にて実績があるヒューマンエラー対策を応用して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を提案する．更に当該対策の実施手順を実組織の情報セキュリティインシデントに適用して有効性を検証した．

2. 背景

2.1 情報セキュリティインシデントの原因

「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 Ver.1.2」[1]によれば過去に公表された個人情報漏えい事故の漏洩原因のうち「誤操作」，「管理ミス」の割合が増加傾向[1]にある．詳細を図 1に示す．

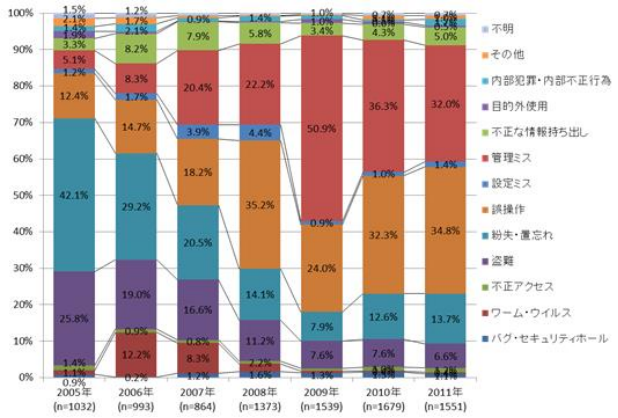

図 1 漏洩原因比率の経年変化(件数)

図 1では，2011 年の漏洩原因のうち「誤操作」が 34.8%，「管理ミス」が 32.0%，「紛失・置忘れ」が 13.7%，「盗難」が 6.6%であり 4 項目の合計は 87.1%を占めた．これらの 4 項目はいずれも当事者に不正行為（情報を外部に漏洩する）を犯す意志がないが，結果として事故を引き起こしており過失[2] による事故と考える．つまり，当事者の意図に反してヒューマンエラーに起因する情報セキュリティインシデントが多く発生していることが分かる．

2.2 関連法令

個人情報漏洩に関する法令として個人情報保護法が包括的な法律として制定され，更に事業分野毎のガイドラインが制定されている．経済産業省が定める事業全般向けのガイドライン[2]には，個人情報漏洩事故発生時の対処内容として「影響を受ける可能性のある本人への連絡」や「事実関係，再発防止策等の公表」等を求めている．個人情報に係る漏洩事故発生の際は当該情報に「高度な暗号化等の秘匿化」がされていてもこれらの対応が免除されないケース[3] がある．

2.3 コーポレートレピュテーション

コーポレートレピュテーションとは企業が社会から受ける評判や評価のことである．松田ら[3]は，企業価値を高めるコーポレートレピュテーションのことを正のコーポレートレピュテーションと定義した．例えば，ステークホルダーのインセンティブが向上し，企業への愛着や親しみが増大して企業の生産性やブランド価値の向上により企業価値の向上が期待できる．逆に，不祥事等により企業価値を落とす場合を負のコーポレートレピュテーションと定義している．情報漏洩事故の発生は負のコーポレートレピュテーションを高めて顧客離れや顧客損失の要因になるため適切な管理を施す必要がある．

2.4 先行研究

情報セキュリティの分野では川越[4]がヒューマンファクタ全般の調査及び情報セキュリティへの適用を考察した．石丸[8]はヒューマンエラーによる情報漏洩防止策として，本論文が採用するヒューマンエラー分析手法のひとつである m-SHEL モデルを紹介した．また，ヒューマンエラー分析手法を情報セキュリティに適用した事例として，村上[5]がコンピュータウィルスの蔓延に伴うネットワーク障害に対し，富樫ら[6]がメール誤送信に対して机上による分析を行った．江崎ら[7]は情報漏洩事故に係る組織管理の在り方として，ヒューマンエラーや日常的な逸脱を誘発する因子が放置すると，次第に情報漏洩事故として顕在化する可能性があるため，適切かつ継続的な管理が必要と指摘している．

しかし，情報セキュリティ分野においてヒューマンエラー分析手法の有効性を実環境にて検証した研究は無い．

2.5 本論文の概要

3 章ではヒューマンファクタの概要，ヒューマンエラー分析手法の選定について述べる．4 章では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実施手

†情報セキュリティ大学院大学 INSTITUTE of INFORMATION SECURITY.

[1] 集計対象は 2002～2011 年

[2] 盗難は，悪意ある第三者による「故意」と捉えることもできる．一方，被害者は罪を犯す意思がなく，盗難防止対策を講じれば盗難に遭う確率を低減できるため，本論文では盗難を当事者による「過失」に分類する

[3] 暗号化による免除規定は各省庁のガイドライン毎に異なり，免除されない場合がある

順を示す．5 章では，当該対策の有効性を検証するため，実組織に適用して対策前後のインシデント発生に対する効果測定について述べる．6 章では総括を行い 7 章にて今後の課題を述べる．

3. ヒューマンエラー分析手法

3.1 ヒューマンファクタ

人間と機械などで構成されるシステムの弱点を分析する学問や技術の領域は，ヒューマンファクタと呼ばれる．細かな定義の違いは学者や国により多数存在するが，篠原[9]は，ヒューマンファクタを「人間に関するさまざまな学問領域（行動科学，社会科学，工学，生理学など）からの学際的な知見を活用し，人間と機械が協調的に働く必要のあるシステムに応用することによって，エラーの減少，人間能力の最適化と健康・生活の向上，生産性・安全性の向上を目指す応用科学」と定義している．

David Lacey の「Managing the Human Factor in Information Security」[10]は，ipad 等のようにマニュアルレスを製品が増えてきた一方で，人に覚えて慣れて実行してもらうためにポリシーを延々と追加した製品も存在するが，このようなポリシーは誰も見ないと指摘している．心理学的な面でのマニュアルや操作面での対応を考えることでヒューマンエラーの低減を考察している．

ISACA[4] の「An Introduction to the Business Model for information Security」[11]は，情報セキュリティのビジネスモデルを提案している．その概要を図 2に示す．

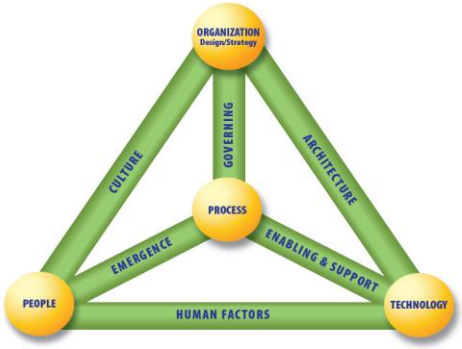

図 2　情報セキュリティのビジネスモデル

図 2は，4 つの要素を 6 つの関係でつないだピラミッド型の構造になっている．このモデルの全ての要素は，相互に作用しており，どれか一つでも変更が加えられたり，適切に管理されなかったりするだけで，このモデルのバランスが保たれず，常に潜在的なリスクにさらされる．このモデルでは，人的要素（PEOPLE）が重要な要素の一つとして，考慮されている．

3.2 ヒューマンエラー分析手法

3.2.1 分析手法の選定

ヒューマンファクタの分析手法には，IRAS[12]，VTA[5]，4M4E 分析等がある．これらの中で，専門的な知識がなくても比較的容易に実践可能であるため，医療分野で広く用いられているヒューマンエラー分析手法のひとつの Medical SAFER[13]を採用した．

3.2.2 Medical SAFER

Medical SAFER は，原子力発電所に勤務する運転員が自分たちの経験したヒヤリ・ハットを分析することを目的に開発した H2-SAFER を医療用に使いやすくしたモデルである．特徴としては，現場で実際に働いている人が使えるように工夫され，分析を容易に実施するためのツールが提供されている．

4. ヒューマンエラー対策実施手順

Medical SAFER は医療用に開発されており，情報セキュリティ分野に適用するには一部修正する必要があった．修正点の詳細は 4.4.2 章に記す．

本論文では Medical SAFER の考え方をベースとして修正した分析手法を元に，情報セキュリティインシデントに関するヒューマンエラー対策を提案する．

対策の流れを以下に記す．

① 時系列事象関連図の作成
② 問題点の抽出
③ 問題点の背後要因の探索
④ 考えられる対策の列挙
⑤ 実施可能な対策の決定
⑥ 対策の実施
⑦ 実施した対策の評価

なお，この実施手順は過去に発生したインシデントの原因を把握して対策案を見出して活用する流れになる．

4.1 時系列事象関連図の作成

インシデント発生に至るまでに起こった事象や行動を整理し，事実を把握するために「時系列事象関連図」を作成する．過去の情報セキュリティインシデントに対して関係者，機器，設備等を横軸，時間経過を縦軸として何がどのように起こったのか記載する．

車上荒らしによる PC 紛失の「時系列事象関連図」の例を図 3に示す．

4.2 問題点の抽出

「時系列事象関連図」からインシデントにつながったと想定される事象，関係者，機器，設備等やこれらの相互関係に含まれる問題点を抽出する．

4.3 問題点の背後要因の探索

抽出した問題点に潜む背後要因やエラーの誘発要因を特定，分析し「背後要因関連図」を作成する．

4.4 考えられる対策の列挙

4.4.1 背後要因からの検討

問題点から探索された背後要因の対策案を列挙する．この段階では，実行可能性を考慮せず，背後要因関連図を見ながら，対策を思いつくままに列挙する．車上荒らしによる PC 紛失の「背後要因関連図」の例を図 4に示す．

[4] Information Systems Audit and Control Association
[5] Variation Tree Analysis

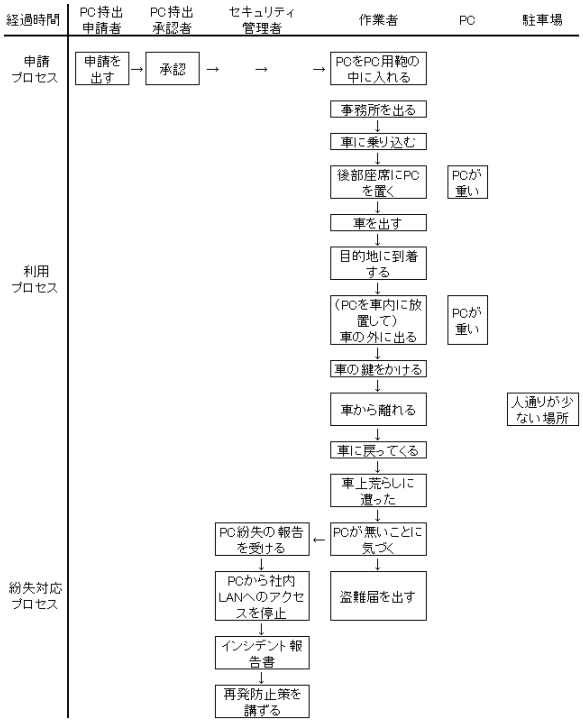

図 3　時系列事象関連図（例）

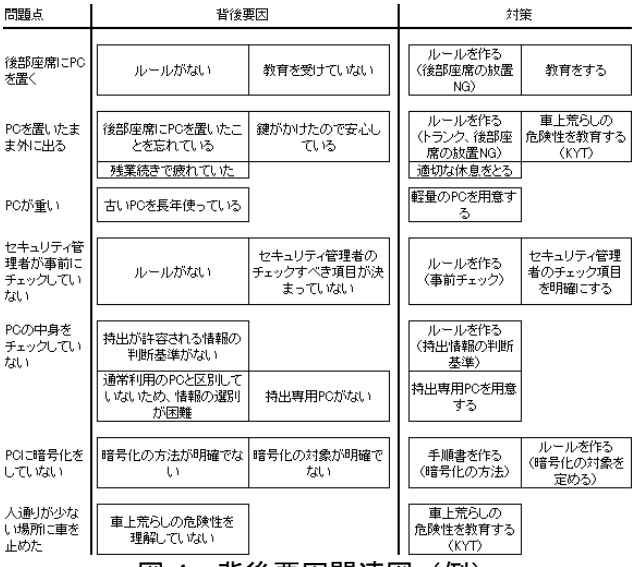

図 4　背後要因関連図（例）

4.4.2 網羅性の検証

4.4.1にて検討した対策の他に講ずるべき対策の検討漏れ等が無いか確認するため，以下の手順にて対策の網羅性を検証する．

①m-SHEL モデル

ヒューマンエラーの先行研究である Edwards の SHEL モデル[14]，これを修正した Hawkins の SHEL モデル[15]，河野が発展させた m-SHEL モデル[13]がある．本論文では m-SHEL モデルを採用する．m-SHEL モデルの各要素の定義を表 1に示す．なお，表 1 の定義は情報セキュリティのヒューマンエラー対策に応用するため，m-SHEL モデルを情報セキュリティに則した内容に定義を修正した．

要素	定義
m(マネジメント)	組織・管理・体制・職場の雰囲気，セーフティカルチャー（安全文化）の醸成
S(ソフトウェア)	行動規範，マニュアル，手順書，セキュリティ教育，訓練，セキュリティアプリケーション，セキュリティソリューション，暗号化
H(ハードウェア)	機器の設計，機器の配置，マンマシンインターフェース
E(環境)	作業特性（緊急作業等），物品管理
L(本人:ライブウェア)	身体的・心理的・精神的状況，能力（技能・知識）
L(周りの人:ライブウェア)	コミュニケーション，リーダシップ，チームワーク

表 1　河野の m-SHEL モデルを一部修正

②戦略的エラー対策の 4M

河野[13]は，ヒューマンエラー対策を「発生防止」と「拡大防止」に分けている．

「発生防止」とは，ヒューマンエラーの絶対数を出来るだけ少なくするステップであり，危険を伴う作業遭遇数を減らす「機会最小（Minimum encounter）」と各作業のエラー確率を小さくする「最小確率（Minimum probability）」の２つで構成される．

「拡大防止」とは，ヒューマンエラーの発生はある程度避けられないという前提に立ち，多重のエラー検出策を設ける「多重検出（Multiple detection）」と被害を最小とするために備える「被害極限（Minimum damage）」により，エラーが最終的な事故やトラブルに結びつかないようにする．これらの 4 つステップを「戦略的エラー対策の 4M」という．

③エラー対策の思考手順

河野[13]は「戦略的エラー対策の 4M」をベースに実行レベルまで 11 段階に分解した「エラー対策の思考手順」を提案している．この手順は，エラー対策を段階的に捉えているため，対策を考えやすいという特徴がある．この手順を情報セキュリティに応用する．ただ，情報セキュリティ分野に応用するためには「多重検出」，「被害局限」の段階で食い止めれば情報漏洩事故の発生に至らないため「エラー対策の思考手順」の「拡大防止」を「顕在化防止」に修正した．これを「情報セキュリティ対策の思考手順（以下，「思考手順」とする）」とし，図 5に示す．

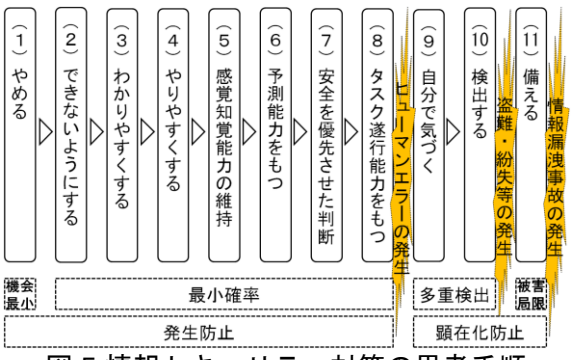

図 5 情報セキュリティ対策の思考手順

④発想手順マトリクス

河野[13] は「エラー対策の思考手順」と m-SHEL モデルを組み合わせ，「エラー対策の発想手順マトリクス」を考案している．本論文では，m-SHEL モデルと「情報セキュリティ対策の思考手順」を組み合わせ，「情報セキュリティ対策の発想手順マトリクス」（以下，「発想手順マトリクス」とする）を作成した．これを表 2に示す．

⑤網羅性の検証

4.4.1 にて検討した対策を「発想手順マトリクス」の項目にあてはめる．例えば，「適切な休息をとる」という対策では，m-SHEL モデルでは「L（本人）」に該当し，「思考手順」の 11 段階では，「⑤知覚能力を持たせる」に当てはまる．実際に「発想手順マトリクス」に記載したものを図 6に記す．

		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（ﾏﾈｼﾞﾒﾝﾄ）											
	S（ｿﾌﾄｳｪｱ）											
	H（ﾊｰﾄﾞｳｪｱ）											
	E（環境）											
	L（本人）											
	L（周りの人）											

表 2 発想手順マトリクス

		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（ﾏﾈｼﾞﾒﾝﾄ）											
	S（ｿﾌﾄｳｪｱ）											
	H（ﾊｰﾄﾞｳｪｱ）											
	E（環境）											
	L（本人）					適切な休息をとる						
	L（周りの人）											

図 6「適切な休息をとる」の例

このようにして全ての情報セキュリティ対策を「発想手順マトリクス」マッピングする．次に，対策に不足がないか確認する．例えば，まず m（マネジメント）における「①やめる（なくす）」に該当する対策を検討し，対策があった場合はその対策をマッピングする．この進め方を図 7に示す．

次に m（マネジメント）における「②できないようにする」の対策を確認する．このように m-SHEL モデルの 6 項目と「エラー対策の思考手順」の 11 項目を掛け合わせた全 66 項目に対して対策の有無を確認することで，情報漏洩対策の網羅性を検証する．この網羅性の検証のイメージを図 8に記す．

4.5 実施可能な対策の決定

情報セキュリティの対策案を一つずつ検討・評価し，実施する対策案を決定する．まず，左端に列挙した対策案を並べる．次に，挙げられている対策案を評価するための評価項目を定めて評価する．

4.6 対策の実施

採用した対策を実施する．

4.7 実施した対策の評価

実施された対策について評価する．具体的には組織の社員等へのアンケートやインシデント発生数の推移等を確認する．

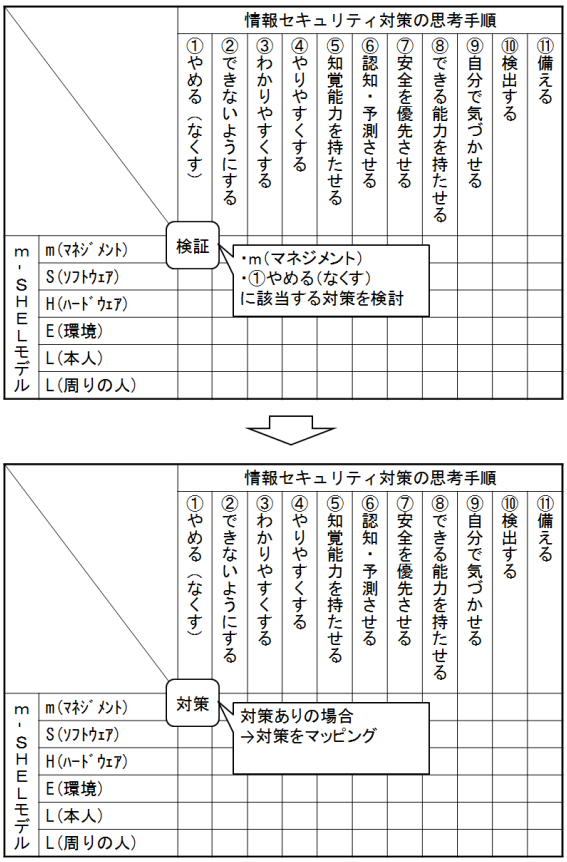

図 7 対策の検討と確認

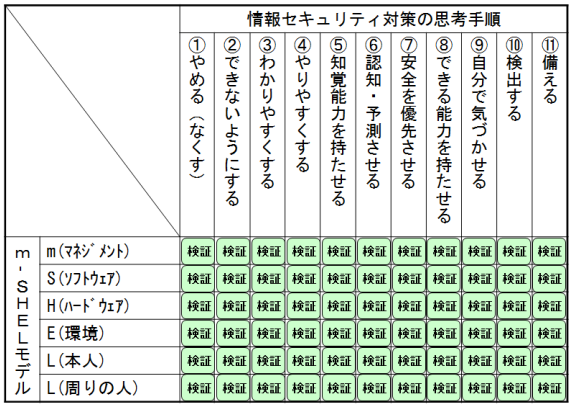

図 8 網羅性の検証のイメージ

4.8 まとめ

4 章の実施手順のうち，特に重要なプロセスは網羅性の検証である．「発想手順マトリクス」による網羅性を検証する過程において，再度「時系列事象関連図」や「背後要因関連図」の事象を見比べながら検証することで，今まで気づかなかったような対策を発想できる．これらの対策を実施することで従来よりも効果的なヒューマンエラー対策を講ずることが出来ると考える．

5. 有効性の検証

4 章の実施手順の有効性を検証するため実企業での適用を行った．以下に適用事例を記す．

ヒューマンエラー対策の主旨に賛同した IT 関連の企業 A 社（以下，A 社とする）にて有効性を検証した．検証プロセスのバイアスを低減させるため，ヒューマンエラー対策の実施手順(4 章)を元に「情報セキュリティインシデントに関するヒューマンエラー対策実施手順書」を作成した後，A 社の改善実施担当者に提示した．以降のプロセスは A 社が単独で実施した．筆者らは独立性を保つため A 社には立ち入っていない．

5.1 改善対象インシデントの選定

改善対象インシデントの特定に際して以下の点を留意した．

- 数値化できるもの
- 実施可能な範囲のもの
- 実際に問題となっている事象

これらの条件に合致するインシデントのうち，A 社のセキュリティポリシー上，社外秘のものを除外した結果，「セキュリティエリアの入退室扉における非常開錠装置の誤操作」を対象に選定した．A 社は入室時及び退室時に認証による開錠をする仕組みを採用している．一方，緊急時は生命の安全を優先させるために各フロアの施錠された退室扉を「1 つの動作で開錠」する仕組みを講ずることを社内規定にて定めている．そのため，扉の退室側には非常開錠装置が設置され，当該装置のプレート部分を手で前方に押すとロックが解除され扉が開錠する．非常開錠装置のイメージを図 9に示す．

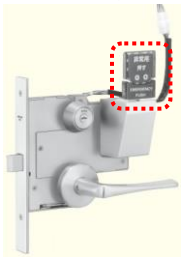

図 9 非常開錠装置のイメージ

A 社は当該装置の開錠動作を全てセキュリティインシデントとして捉えており開錠動作が発生するとビル管理センタの監視メンバーが駆けつける．一方，簡単に開錠できる仕組みを有するために入居者のヒューマンエラーに起因する誤操作によって毎月数件の誤開錠が発生していた．監視メンバーは発生の都度，緊急出動しており誤開錠を抑制する仕組みを検討する必要があった．

5.2 適用対象

ヒューマンエラー対策の有効性を測定するため，改善前の一定期間における改善対象インシデントの発生数の実績値を測定した．なお，改善実施担当者と実績値の測定担当者は別組織とした．

5.3 検証手順及び結果

A 社は「情報セキュリティインシデントに関するヒューマンエラー対策実施手順書」に基づき対策を実施した．

① 時系列事象関連図の作成

申請プロセスから入室時の人の動き，扉や装置との関連を細かく時系列にして「時系列事象関連図」を作成した．この段階で事象の全体の流れ，人，物，動作等の関わりを明確にした．

② 問題点の抽出

「時系列事象関連図」の中で問題点となりそうなポイントにフラグをつけた．

③ 問題点の抽出

「時系列事象関連図」から選択された問題点について，その背後要因を列挙して「背後要因関連図」を作成した．

④ 考えられる対策の列挙

背後要因に対する問題点，根本原因に対する対策案を列挙した．なお，対策は実現可能かどうか，関係なく考えられるものを挙げた．更に「発想手順マトリクス」に対策を転記した．この段階でブランク領域（対策が存在しない領域）は再度，問題点と対策，さらに「時系列事象関連図」まで戻り，該当する対策が無いか検討した．この網羅性の検証プロセスを「発想手順マトリクス」の 66 項目全てに対して実施した．

以下に網羅性の検証を経て発想された主な対策の例を記す．

- 張り紙を貼る（③わかりやすくする・ソフトウェア）
- 違反状況を全員に知らせる（⑪備える・マネジメント）
- 扉の開錠手順書を作成する（④やりやすくする・ソフトウェア）
- レバーを押すと警報が鳴るので触らないことを教育する（⑥認知・予測させる・本人）

⑤ 実施可能な対策の決定

最終的に絞り込まれた対策案に関して，効果，即効性，コスト，制約，労力の観点で評価を行った．評価の結果，一番評価の高かった対策は，「誤動作防止板」の設置である．この対策は「発想手順マトリクス」上では「②できないようにする」の「ハードウェア」に該当する．

当該対策の実施について，A 社の管理責任者により最終承認を得た．

⑥ 対策の実施

非常開錠装置のもつ「1 つの動作で開錠」する仕組みを阻害しないため，非常開錠装置全体を覆うことなく，人による誤押，不注意を防止する対策を以下の構造で実現した．

- 非常開錠装置の左右方向からの誤押，不注意により手または指が触れる動作を防止する為に，新たに「誤動作防止板」を非常開錠装置と直角に設置する．

・非常開錠装置の正面方向は，緊急時に前方に押すという動作を妨げないために開放する．
・「誤動作防止板」は，非常開錠装置の表面を横方向から見たときに，押す面より高いが開閉の妨げにならない高さとする

以上の対策によって改善対象インシデントにおける事象のうち，以下のヒューマンエラーを改善できると考えた．

・入室時，扉を押さえる為に手をついた際，誤って「非常開錠装置」を押してしまう．
・退室時，閉まる扉を手で押さえる際，誤って「非常開錠装置」を押してしまう．

⑦ 実施した対策の評価

A 社が入居する事務室のうち，2 フロアを対象として対策を実施した．1 フロア当たり 4 箇所に該当する入退室扉があり，各扉の退室側に非常開錠装置が設置されているため 8 箇所の非常開錠装置に対して「誤動作防止板」を設置した．なお，対象フロアの入居者数は約 1200 名，月間入退室数は延べ約 16 万回である．対策前及び対策後のインシデントの発生数の実績値を図 10に記す．

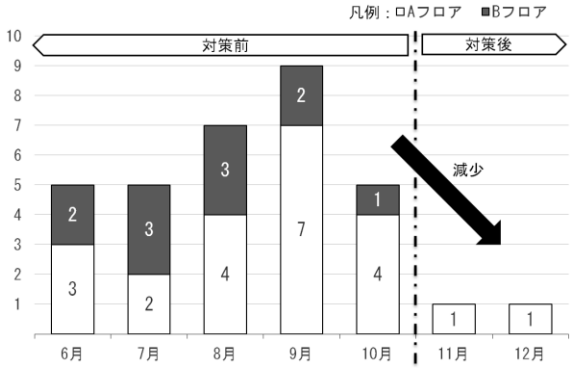

図 10 インシデント発生数の実績値

5.4 考察

「誤動作防止板」が対策として導き出されたのは，時系列事象関連図において以下の点に着目したことが発端である．

・入退室扉は自動的に扉が閉まる．
・閉まる扉をおさえた手で「非常開錠装置」を誤って押してしまう．

背後要因関連図では上記の事象を「おさえた手で押しやすい構造」という問題点として定義し，背後要因を挙げた．具体的には

・「非常開錠装置」と手のつく位置が同じ高さにある．
・「非常開錠装置」の位置，大きさに問題がある．
・「非常開錠装置」が手に当たりやすい面積，形を有している．

といった背後要因が挙げられた．

更にこれらの背後要因への対策として

・「非常開錠装置」の周りにカバーを設置する．
・カバーの高さは「非常開錠装置」よりも高くすることで誤操作を防ぐ．

といった案が出された．これらの案を具体化したものが「非常開錠装置」である．

既存の情報漏洩対策モデル[6]は，個々の情報漏洩事故の原因に特化した対策に係る記載は乏しい．「非常開錠装置」の設置のように具体的な対策までは記載されておらず各組織が独自に対策案を検討する必要がある．本論文にて提案したヒューマンエラー対策の実施手順によって導き出された対策を実施後にインシデント発生件数が大幅に減少しており，当該手順はヒューマンエラーの低減に効果があったと考える．

5.5 A 社の改善実施担当者の意見

最後に，A 社の改善実施担当者から対策実施後に本対策について意見として挙げられた点を以下に記す．

5.5.1 本対策のメリット

・対策案の検討経緯を理論立てて説明しやすい．
・対策案の選定根拠が説明しやすい（最終承認が得られやすい）．
・対策案の検討範囲の見直しがしやすい．
・「発想手順マトリクス」では対策の網羅性が視覚化できる．
・対策の優先順位がつけやすい．
・思いがけない対策案が出る可能性がある．
・複数の対策を組み合わせることで，投資対効果のベスト解が導きやすい．

5.5.2 注意したい点

・「時系列事象関連図」の中で予め問題点となりそうなところを抽出しておくとより分かりやすくなる．
・根本原因にこだわらない点が重要である（この方法しかないという落とし穴に入らない）．
・評価基準の重み付けや評価は意図的になりやすいため，第三者による客観的なレビューが役立つ．

6. まとめ

本論文では，情報セキュリティインシデントに関するヒューマンエラー対策の実施手順を提案した．そして実施手順の有効性を検証するため，実在する企業の協力の元，実証実験を行った．

結果としてインシデント発生が抑制することを確認した．特に「発想手順マトリクス」の網羅性の検証により多くの対策を発想することがインシデント発生数の低減に寄与したと考える．そして本論文が提案するヒューマンエラー対策はヒューマンエラー低減に対して一定の効果があることが分かった．

7. 今後の課題

1.1 章にて述べたとおり，国内にて発生している情報セキュリティインシデントの 87.1%がヒューマンエラーに起因している．組織が公表した情報セキュリティインシデントの情報には多くの場合，発生の経緯や時系列による事象の記録等が記されている．これらの情報に対して本論文が提案したヒューマンエラー対策を適用することで，インシデントの潜在的な背後要因の傾向を把握し，対策案を検討することが出来ると考える．

また，これらのインシデントの原因は紛失，盗難，誤操作，管理ミスであり，更に対象物は PC，外部記録媒体，

[6] JIS Q 27002:2006,PCI DSSver1.2,COBIT4.1,NIST SP800-30 等を調査

電子ファイル，紙など多岐に渡る．入退室扉の誤開錠以外にも様々なヒューマンエラーが発生していると想定される．これらのインシデントに対し，本論文が提案した対策が有効かどうかを実組織にて検証する必要がある．この検証を実組織にて実施した場合，当該組織のセキュリティポリシーによりインシデント発生件数の公表が困難な可能性がある．本提案の有効性を検証した結果を容易に情報共有できるスキームを考案することも今後の課題である．

謝辞

多数の助言を頂いた情報セキュリティ大学院大学 原田研究室のメンバー，検証を実施して頂いた企業 A 社，そして本研究にご協力頂いた皆様に謹んで感謝の意を表する．

参考文献

[1]NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ，情報セキュリティ大学院大学 原田研究室 廣松研究室， "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 Ver. 1.2"，(2011)
[2]経済産業省情報経済課. 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成 16 年 10 月 22 日厚生労働省経済産業省告示第 4 号 ，平成 21 年 10 月 9 日改正）. (2009).
[3]松田貴典，芝隆，辻野武，城順平，金子清美，黒木啓良， "コーポレート・レピュテーション戦略－信頼される企業向けてー"， 工業調査会，(2007)
[4]川越秀人，内田勝也， "情報セキュリティのヒューマンファクタ"， 情報処理学会研究報告. CSEC， [コンピュータセキュリティ]. p. 7-12， (2008)
[5]村上靖，内田勝也， "情報セキュリティ事件・事故の分析と対策に関する考察"， 情報処理学会研究報告. CSEC， [コンピュータセキュリティ]. p. 1-8， (2010)
[6]冨樫由美子，佐藤嘉則，藤井康広， "企業の情報セキュリティ対策におけるヒューマンエラー管理実践に向けた検討"， 情報処理学会研究報告. ソフトウェア工学研究会報告. p. 1-7，(2009)
[7]江崎郁子，大橋毅夫，上野信吾， "個人情報漏洩防止のためのヒューマンエラー対策 (特集 安全と安心の追求)"， 三菱総合研究所所報. p. 66-83， (2005)
[8]石丸英治， "情報管理におけるヒューマン・エラー対策"， 株式会社インターリスク総研，(2011)
[9]篠原一彦， "医療のための安全学入門～事例で学ぶヒューマンファクター"， 丸善株式会社，(2005)
[10]David Lacey， "Managing the Human Factor in Information Security: How to win over staff and influence business manager"，Wiley，(2009)
[11]Information Systems Audit and Control Association， "An Introduction to the Business Model for information Security"，(2009)
[12]宮城雅子， "大事故の予兆をさぐる―事故へ至る道筋を断つために"， 講談社ブルーバックス，(1998)
[13]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)
[14]Earl L.Wiener & David C.Naggel， "Human Factors in Aviation"，Academic press. inc，(1998)
[15]F.H.ホーキンズ著 黒田勲 監修 石川好美監訳， "ヒューマン・ファクター －航空の分野を中心としてー"， 丸山堂書店，(1992)