Vol.2019-IOT-47 No.8
Vol.2019-SPT-35 No.8
2019/9/19

# 秘匿性の高い個人情報を扱う業務時のヒューマンエラーに基づく情報漏えいインシデント低減に関する一考察

植草皓[†1]　谷本茂明[†1]　畑島隆[†2]　金井敦[†3]

**概要**: 個人情報漏洩は重大な情報セキュリティインシデントであり解決すべき重要な課題である. 例えば, JNSA（Japan Network Security Association）は，年間平均約 500 万人分以上の個人情報が漏洩していると報告している．その要因は組織外からの攻撃と組織内の不正に大別できる．一般に，前者の組織外からの攻撃に対する対策は進んでいるが，後者の組織内の内部不正やヒューマンエラーに対する対策の検討は十分ではない．本論文は，組織内の不正やヒューマンエラーに着目し，特に秘匿性の高い個人情報を扱う業務における情報漏洩の原因を明らかにし，これらを要因とするセキュリティインシデント対策を提案する．具体的には，リスクマネジメント手法により情報漏洩に至るリスク要因を網羅的に抽出し，その要因を詳細に分析することによりインシデント低減策を新たに提案する．

**キーワード**:

# A Study on Information Leakage Incident Mitigation based on Human Error in Business Handling Highly Confidential Personal Information

HIKARU UEKUSA[†1]　SHIGEAKI TANIMOTO[†1]
TAKASHI HATASHIMA[†2]　ATSUSHI KANAI[†3]

## 1. はじめに

現在，ICT（Information and Communication Technology）は，国内のみならず世界のインフラとして急速に発展し，重要なポジションを担っている．2017 年の世界のインターネットユーザは約 40 億人となり，総人口の 53%に相当するといわれている．また，国内のインターネットユーザは総人口の 80.9%となり, 広く普及している. 個人の主な ICT の利用目的としては，電子メールの送受信，天気予報の利用，地図・交通情報の提供サービスなどが挙げられる．企業などの組織体においても，SNS を用いた商品の広告，クラウドサービスを用いた情報の共有など，さまざまな場面で ICT の利用が行われている [1][2].

上述したように，一般生活から経済活動まで幅広い分野において利便性を向上させている ICT であるが，同時に情報セキュリティインシデントを発生させる危険も持つ．とりわけ個人情報漏洩は，今日のセキュリティインシデントにおける重要な課題の一つである．そのため国内のほぼすべての企業は，このセキュリティインシデントへの様々な対策を行っている．その要因は組織外からの攻撃と組織内の不正に大別できる．それぞれへの具体的な対策として，前者に対してはアンチウイルスソフトの導入や更新，OS の自動アップデート，多要素認証システムや生体認証システムによるアクセスの厳格化が行われ，後者に対しては従業員へのセキュリティ教育などの啓蒙活動などが行われている．しかし JNSA の調査によると，2018 年の個人情報漏えい人数は 561 万人となり，前年に比べて増加している．また発生件数においても前年と比べて増加している [3]. このように，依然としてセキュリティインシデントは発生している．

本稿では，秘匿性の高い個人情報を扱う業務として代表的な公務を対象に，これらの情報セキュリティインシデントの発生傾向について検討する．業種ごとに持つ個人情報にはさまざまな種類があるが，とりわけ公務活動で利用される個人情報は秘匿性の高いものが多いと考えられる．例えば住所やマイナンバー，収入や納税額，家族構成や生年月日などさまざまであるが，いずれも個人や周辺の人物を特定するには容易な情報といえる．公務におけるインシデント発生件数は慢性的に多く，過去 5 年間の平均では，国内の情報セキュリティインシデント全体の 35.4%が公務活動によって起こっているものとなっている [3]．公務活動におけるセキュリティインシデント発生の原因として，最

†1 千葉工業大学
Chiba Institute of Technology
†2 NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories
†3 法政大学
Hosei University

も多く挙げられているのは誤操作である．誤操作とは「あて先を間違えたり、操作ボタンを間違えて押したりするなどの人間のオペレーションによって情報が漏えいした場合」とされている [4]．つまり，公務における情報漏洩の多くは，人の失敗，すなわちヒューマンエラーが原因である．設備投資やソフトウェアインストールのような外部攻撃への対策をしているにもかかわらず，内部の操作者の失敗により，毎年最低でも 20 万人分，多いときではその十倍以上の件数の個人情報が漏洩しているのである．

ところで，公務員の懲戒の指針[5]では 2016 年まで故意による情報漏洩のみを対象としていたが，過失による漏えいについても懲戒の対象となるようになった．また，2018 年 9 月に，地方公共団体へ向けたセキュリティ対策やセキュリティポリシーの具体例の記載されたガイドライン[6]が改訂されたが，前述のように当年のセキュリティインシデント発生件数が増加している[7]ことから，現在の対策では不十分であるといえる．特に，物理的な入退室の管理やサイバー環境における二段階認証システムによる対策だけでなく，ヒューマンエラーによるインシデントを減少させるために，業務や従業員への対策が必要となっている ．本稿ではこれらを問題意識として情報セキュリティインシデントを軽減する方法を検討した結果を報告する．具体的には，まず RBS 手法を用いてヒューマンエラーによる IT リスクを特定した．その後特定したリスク要因をヒューマンエラーの種類を基に分類を実施し考察を行った．

以降 2 章ではヒューマンエラーと IT リスクとの関係を調査について述べ，3 章で具体的なリスク要因の特定と分類を行った結果と考察，それらを基にした低減策を述べる．最後に 4 章で,本稿をまとめる．

## 2. ヒューマンエラーと IT リスク

### 2.1 ヒューマンエラー

ヒューマンエラーとは人が何かしらのオペレーションを行う際に起こす失敗のことである．ヒューマンエラーの起こる背景には，人間の意図とそれによって引き起こされる行動がある．Reason[8]はヒューマンエラーを“スリップ（slip）とラプス（laps)”，および“ミステイク（mistake)”の二つに大別し，さらにそれぞれの発生する 3 つのパフォーマンスレベルと合わせて 3 種類に分類している．

表 1 に挙げたように，スリップとラプスは，もともと計画していた行動が何らかの要因，主に外的要因によってその計画から外れ, 意図しない行動をすることを指す. また，ミステイクは，ある目的を達成するための行動の計画した際に，計画そのものが間違っていた場合を指す．3 つのパフォーマンスレベルは，スキルベースレベル，ルールベースレベル，知識ベースレベルに分けられる．スキルベースレベルではルーチン行動が行われ，その実行中にエラーとしてスリップとラプスが発生する．ルールベースレベル，および知識ベースレベルでは問題発生時にその問題を解決するための計画と行動が行われ，エラーとしてミステイクが発生する．

表 1 エラー区分と特性のまとめ [8]

| パフォーマンスレベル (エラータイプ) | スキルベース (スリップとラプス) | ルールベース (ミステイク) | 知識ベース (ミステイク) |
|---|---|---|---|
| 活動のタイプ | ルーチン行動 | 問題解決の行動 | |
| 注意の集中先 ＝エラーの原因 | 実行中タスク以外の何か | 問題に関連する事項 | |
| 制御モード ＝あらかじめ行動に決まりがあるか | 主に自動的処理 (＝処理ルールの決まりがある) | | 限定された 意識的な処理 |
| エラータイプの予測可能性 | かなり予測可能な 「強力だが的外れ」な ルーチン適用によるエラー | | さまざま |
| 機会に対するエラーの比率 | 絶対数は多いが, 対機会発生比率は小さい | | 絶対数は少ないが, 対機会発生比率は大きい |
| 状況要因の影響 | 内発的要因が圧倒的影響を及ぼすと思われる | | 外発的要因が主体と思われる |
| 検出の容易さ | 検出はふつう かなり素早く効果的 | 検出は困難であり，しばしば 外部からの介入によってのみ可能 | |

### 2.2 IT リスクの現状と課題

現在の IT リスクの課題として情報漏えいが挙げられるが，この情報漏えいが発生する原因は，外部攻撃と内部不正の 2 つに大別することができる．2014 年の米国 CERT の調査[9]によると，サイバー犯罪の 30%近くが内部者による不正である．また，同様の調査において外部者による攻撃と内部者による不正の影響度はどちらもほぼ同等であるとの結果も出ている（図 1）．また，図 2 に示すように国内の 2018 年におけるセキュリティインシデント発生要因では，「紛失・置忘れ」,「誤操作」,「管理ミス」，といった内部者の失敗やミス，つまりヒューマンエラーが原因となる不正が 70%以上を占めている [3].

現在のセキュリティ対策はほとんどが外部攻撃への事前対策である．しかし，外部攻撃への対策は，攻撃者の技術向上に伴い無力化され，さらに新たな対策が必要となる，いわばイタチごっこのような様相を示す [10]．そのため，常に一定以上のリスクを伴うことが考えられる．一方，内部者のヒューマンエラーによるリスクは，外部者からの攻撃と比較すると顕在化しやすく，かつ対策が無力化されることは少ない．しかし，内部者に対するセキュリティ対策はあまり行われていない [11]．企業で実施されている内部者への対策は,「社員教育」,「セキュリティポリシーの策定」などが行われている（図 3）が，外部攻撃への対策に比べると圧倒的に数が少なく[3]，対策の内容についても具体的とはいいがたい．そのため，対策に関する検討も十分でないと考えられる．

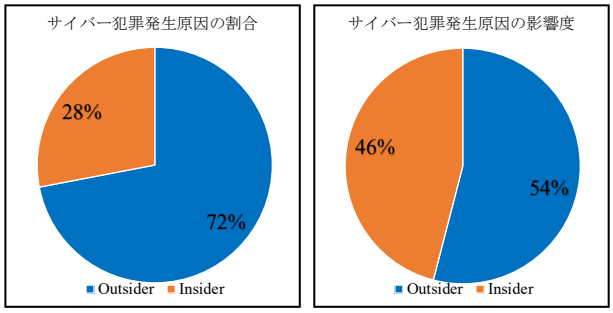


図 1 サイバー犯罪原因の割合と影響度 [6]

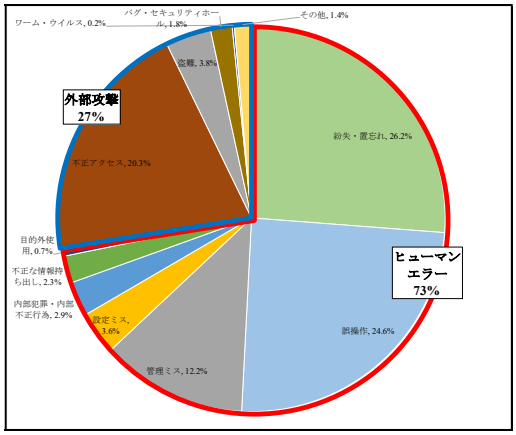


図 2 セキュリティインシデント発生要因割合[3]

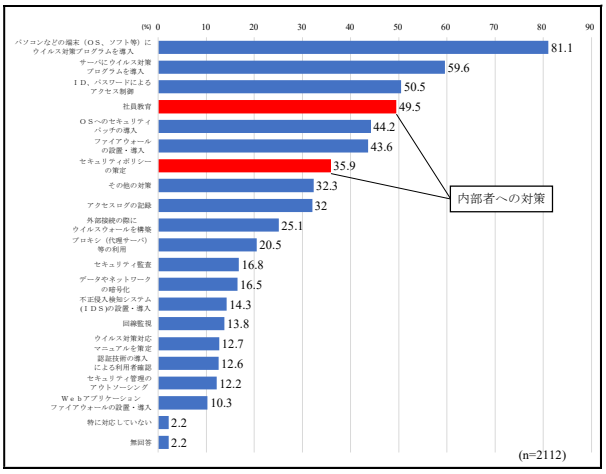


図 3 企業で行われているセキュリティ対策と施策割合[3]

### 2.3 セキュリティポリシーと IT リスク

一般に，多くの企業や組織では個人情報や秘匿情報の取り扱いについて，セキュリティポリシーを定めている．セキュリティポリシーとは，組織における情報セキュリティに対する基本方針や対策基準を示したものである．具体的な対策実施手順や運用規則等は，このポリシーによって策定され運用される．

現在，さまざまな業種や組織に向けた，セキュリティポリシーのガイドラインが多く公表されている [6][12]．これらはセキュリティポリシーのガイドラインである一方，そのポリシーを満たすための具体的な対策を例として記述しているものが多い．この中には，組織内部者に関する人的管理の記述も多くある．しかし，上述したように内部者の問題や失敗によるセキュリティインシデントは数多く発生している．IPA の調査[13]によると，内部不正経験者の内，58%は「ルールを知らずに違反した」，あるいは「ルールを知っていたが、うっかり違反した」といった過失によって発生していることが示されている（図 4）．

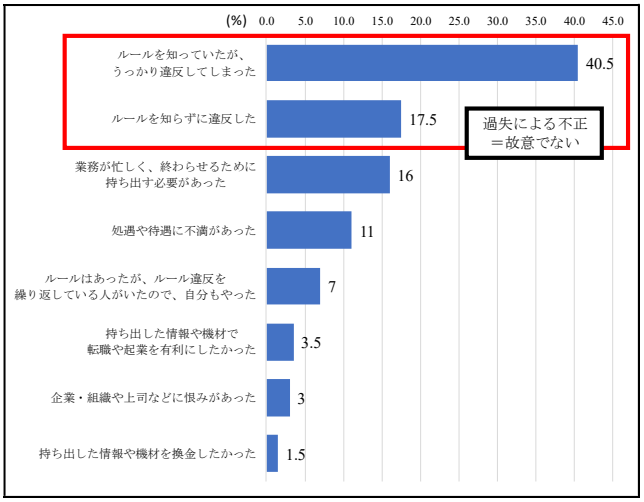


図 4 内部不正経験者の不正理由割合[13]

### 2.4 公務における個人情報保護

本稿では秘匿性の高い情報を多く扱う業務の代表として，公務を例に検討を行う．一般に，公務では，氏名や住所，生年月日，職業，財産などの様々な情報を多数保持している．行政機関の保有する個人情報ファイル（電算処理ファイル，マニュアルファイル）の総数は 2018 年 3 月において 72,175 ファイルとなっており，1 年間で 676 ファイルが新たに作成されている．公務では特に，これらの情報の開示や訂正を行っている [14]．そのため，民間企業を対象としている個人情報保護法とは別に，行政機関個人情報保護法，あるいは独立行政法人等個人情報保護法といった法律を遵守することで管理体制を築いている．また，2016 年からマイナンバー制度の運用が開始され，特定個人情報の管理，マイナンバーカードの受け渡しなども業務に含まれるようになり，個人情報のより厳重な管理が求められるようになっている [15]．

しかし，公務における個人情報漏えい被害は依然として発生しており，2018 年の日本国内のセキュリティインシデントの 3 割近くを占めている（図 5） [3]．2017 年の行政機関による情報の漏えいや毀損の発生およびその可能性があった事案は 949 件あり，そのうちの 860 件が国民等の情報である[14]．また，マイナンバーに関する事例については，2019 年の国民健康保険関係書類の誤送付[16]や 2017 年の特定個人情報の誤送付事件[17][18]，など，マイナンバー法等による厳重な管理が求められているにもかかわらず多数発生している．

ところで，公務においてもセキュリティポリシーの策定が行われ，そのためのガイドラインも公表されている．特に，地方公共団体に向けたセキュリティポリシーのガイドラインは 2018 年に改訂され，システムの強靭性の向上，マイナンバー利用事務の多要素認証の実施必要性，CSIRT（Computer Security Incident Response Team）の設置と役割について追記されている．しかし，公務におけるセキュリティインシデントは，誤操作を原因とするものが多く[19][20]，ポリシーの運用や啓蒙活動，及びシステム強度の向上だけではなく，人間の内面にアプローチをかける対策の考案が必要である．

## 3. ヒューマンエラーを防止する IT リスク管理

### 3.1 ヒューマンエラーと情報漏えいの関連研究

2 章で述べたように，ヒューマンエラーによる情報漏えいは数多く発生しており，エラー防止を図ることは重要な課題である．川越ら[21]はヒューマンエラーを防止するための技術的要素は HCI（Human Computer Interaction）の改善やフェール・セーフ，フール・プルーフなどにより充実しているが，これらによりヒューマンエラー低減の効果が上がっているか明確ではないと述べている．また，新原ら[22]や村上ら[23]などによってヒューマンエラーによる情報セキュリティインシデントの分析手法は検討，提案がなされているが，具体的な対策方法の検討や提案に関する研究は十分ではないと言える．

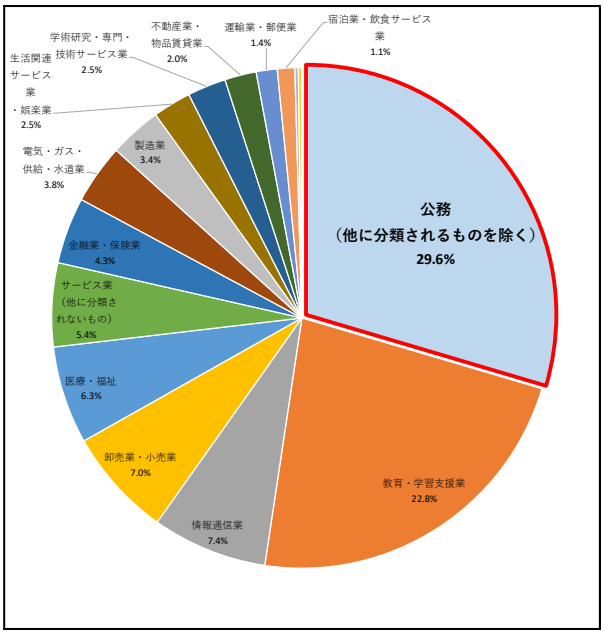


図 5 2018 年の業種別セキュリティインシデント件数[3]

### 3.2 ヒューマンエラーによる情報漏えいの要因特定

上述したように，ヒューマンエラーはパフォーマンスレベルの違いによって，エラーの傾向もさまざまとなる．それぞれのパフォーマンスレベルによって発生するエラーの要因を，Reason[8]は表 2 のように失敗モードの主要語としてまとめている．我々は過去のリスク事例や文献調査を踏まえ，この表を基に，RBS（Risk Breakdown Structure）手法[24]を用いてリスク要因の特定を行った．

まず，秘匿性の高い個人情報として特定個人情報に関する事例の調査を行ったところ，2.4 節で挙げたような特定個人情報を含む個人情報を誤送付する事件が散見された．さらに，公務における情報漏えいの要因が誤操作によるものが多いことを考慮すると，スキルベースにおけるスリップとラプス，つまり，ルーチン行動中のヒューマンエラーを原因とするリスク要因が重要であることが考えられる．事実，上述した事例についても[16]-[18]，送付先の誤登録や個人情報訂正時のミスによる誤送が原因となっている．そこで，メールや郵便の誤送付における，スキルベースのパフォーマンスによるエラー原因の特定を行った．

具体的には，事例を基に [16]-[18]，特定個人情報を含む書類及びデータを送付する業務フロー(図 6)を作成した．その後，それぞれのプロセスで入力・確認される個人情報をブレインストーミングによって洗い出し，漏えい原因となる「受取人の取違」や「情報の未更新」リスク要因を抽出した．抽出したリスク要因を，表 2 を基に作成した RBS によって分類し，リスク要因の傾向を明らかにした．

Vol.2019-IOT-47 No.8
Vol.2019-SPT-35 No.8
2019/9/19

表 2 各パフォーマンスレベルにおける
失敗モードの主要語（[8]から筆者が作成）

| パフォーマンスレベル | エラーの種類 | 失敗モード | | |
|---|---|---|---|---|
| | | 第一分類 | 第二分類 | 第三分類 |
| スキルベース | スリップ・ラプス | 不注意 | 二重補足スリップ | |
| | | | 中断に伴う抜け落ち | |
| | | | 意図の鮮度低下 | |
| | | | 知覚の混同 | |
| | | | 干渉によるエラー | |
| | | 注意過剰 | オミッション | |
| | | | 繰り返し | |
| | | | 逆戻り | |
| ルールベース | ミステイク | 良いルールの誤適用 | 1つ目の例外 | |
| | | | サイン・カウンターサインとノンサイン | |
| | | | 情報の過負荷 | |
| | | | ルールの強度 | |
| | | | 一般的なルールは強くなりがち | |
| | | | むだと重複 | |
| | | | 硬さ | |
| | | 悪いルールの適用 | ルール符号化の欠陥 | |
| | | | ルールアクション部に欠陥 | 間違ったルール |
| | | | | エレガントでないルール |
| | | | | 得策でないルール |
| 知識ベース | ミステイク | 選択性 | | |
| | | 作業領域の限界 | | |
| | | 見えないものは気付かない | | |
| | | 確証バイアス | | |
| | | 自信過剰 | | |
| | | 偏見つき再吟味 | | |
| | | 錯誤相関 | | |
| | | ハロー効果 | | |
| | | 因果関係についての問題 | | |
| | | 複雑性に伴う問題 | フィードバック遅れに伴う問題 | |
| | | | 時間軸を含めたプロセス考察が不十分 | |
| | | | 指数関数的進行の取り扱いが苦手 | |
| | | | 原因から結果へのつながりをネットワークでなく順番に続くものと考える | |
| | | | 取り組み課題の放浪性 | |
| | | | 包囊化 | |

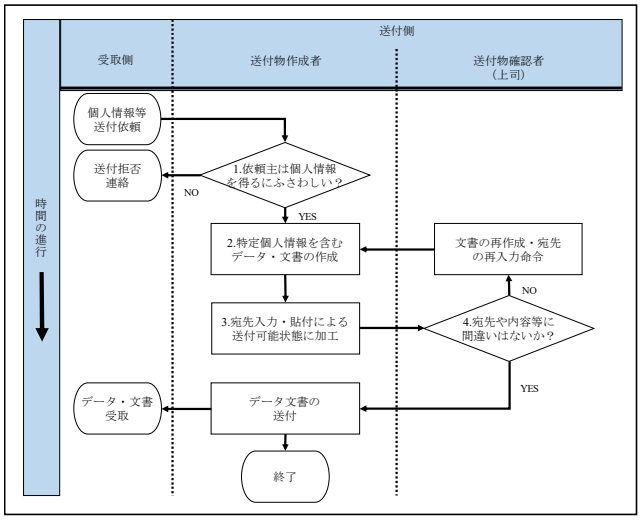


図 6 個人情報送付業務のフローチャート

表 3 プロセスごとに特定したリスク要因

| プロセス及び判断 | 扱う個人情報 | 発生しうるリスク要因 |
|---|---|---|
| 1.受取人は個人情報を得るにふさわしい？ | 受取人氏名 | 1.1 判断違いによる許可 |
| | 受取人連絡先 | 1.2 受取人の取違い |
| | 受取人勤務先 | |
| | 受取人住所 | |
| 2.特定個人情報を含むデータ・文書の作成 | 被送付者氏名 | 2.1 被送付者の取違い |
| | 被送付者連絡先 | 2.2 被送付者情報の入力違い |
| | 被送付者勤務先 | 2.3 被送付者情報の未更新 |
| | 被送付者住所 | 2.4 被送付者以外の情報誤入力 |
| | 被送付者所得情報 | |
| | 被送付者納税情報 | |
| | 被送付者マイナンバー | |
| 3.宛先入力・貼付による送付可能状態に加工 | 受取人氏名 | 3.1 受取人の取違い |
| | 受取人連絡先 | 3.2 受取人情報の入力違い |
| | 受取人勤務先 | 3.3 受取人情報の未更新 |
| | 受取人住所 | 3.4 受取人以外の情報誤入力 |
| 4.宛先や内容等に間違いはないか | 受取人氏名 | 4.1 受取人情報の誤認 |
| | 受取人連絡先 | 4.2 受取人情報の確認漏れ |
| | 受取人勤務先 | 4.3 受取人以外の情報確認漏れ |
| | 受取人住所 | 4.4 被送付者情報の誤認 |
| | 被送付者氏名 | 4.5 被送付者情報の確認漏れ |
| | 被送付者連絡先 | 4.6 被送付者以外の情報確認漏れ |
| | 被送付者勤務先 | |
| | 被送付者住所 | |
| | 被送付者所得情報 | |
| | 被送付者納税情報 | |
| | 被送付者マイナンバー | |

調査した事例を参考に，作成したフローチャート分析した結果，表 3 に示すようなリスク要因を特定した．受取人に対する送付可否の判断において 2 件，特定個人情報を含むデータ・文書の作成中に 4 件，受取人の宛先入力及び貼付中に 4 件，受取人の宛先や作成したデータ・文書の内容確認において 6 件, 全体で 16 件のリスク要因を洗い出した．

### 3.3 失敗モードによるリスク要因の分類

これらのリスク要因を，スキルベースで発生する失敗モードに当てはめた RBS を図 7 に示す. それぞれの失敗モードに特定したリスク要因を分類した結果，二重補足スリップに 4 件，中断に伴う抜け落ちに 2 件，意図の鮮度低下に 2 件，知覚の混同に 2 件，干渉によるエラーに 2 件，オミッションに 4 件のリスクをそれぞれ分類した．また繰り返し，及び逆戻りに分類されるリスク要因は 0 件となった．これらから，個人情報送付業務におけるヒューマンエラーの多くは, データ･文書を作成する際の不注意によるもの，あるいは宛先やデータ・文書を確認する際のオミッションによるものが主であることを明らかにした．

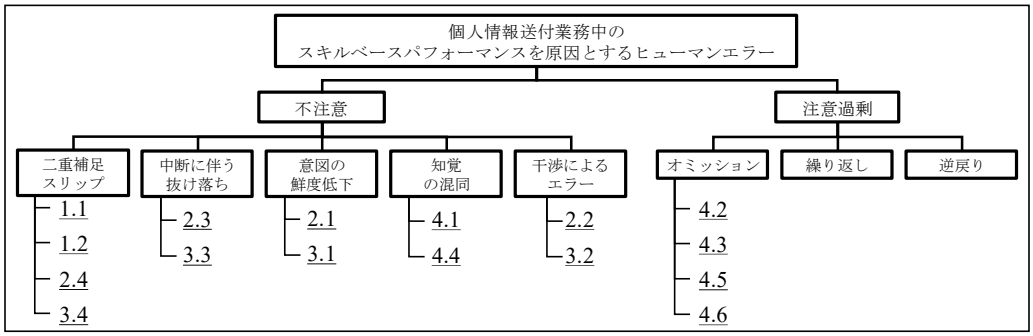


図 7 個人情報送付業務中のスキルベースで起こるリスクの RBS

分類結果を基に提案するリスク低減策の一覧を表 4 に示す．業務フローの 1.および 4.の判断にあたる確認業務は，二重補足スリップ，知覚の混同，オミッションが失敗モードとなる．これらの業務に対するエラーは，主に業務ルーチンの慣れによる油断や，ルーチン化されていない業務および判断が原因となる．そこで，複数人によるマルチチェックの導入ならびに徹底，確認作業の順序・項目の見直しを低減策として提案する．

業務フローの 2.および 3.にあたる作成業務は，二重補足スリップ，中断に伴う抜け落ち，意図の鮮度低下，干渉によるエラーが失敗モードとなる．これらの業務に対するエラーは，業務ルーチンへの慣れによる油断や，業務ルーチン以外への意識の移りが原因となる．そこで，業務の重要度の見直し，それに伴う業務ルーチンの見直し，類似業務の分配を低減策として提案する．

表 4 本稿で提案するリスク低減策の一覧

| 発生しうるエラー | | 失敗モードの分類 | 提案するリスク低減策 |
|---|---|---|---|
| 1.1 | 判断違いによる許可 | 二重補足スリップ | ・業務ルーチンの見直し<br>・複数人によるマルチチェックの徹底 |
| 1.2 | 受取人の取違い | 二重補足スリップ | ・確認事項の追加<br>・複数人によるマルチチェックの徹底 |
| 2.1 | 被送付者の取違い | 意図の鮮度低下 | ・業務の重要度の見直し<br>・作成手順の変更 |
| 2.2 | 被送付者情報の入力違い | 干渉によるエラー | ・類似業務の分配 |
| 2.3 | 被送付者情報の未更新 | 中断に伴う抜け落ち | ・業務の重要度見直し<br>・業務ルーチンの見直し |
| 2.4 | 被送付者以外の情報誤入力 | 二重補足スリップ | ・別業務のルーチンとの分離<br>・予測変換等の利用の停止 |
| 3.1 | 受取人の取違い | 意図の鮮度低下 | ・業務の重要度の見直し<br>・作成手順の変更 |
| 3.2 | 受取人情報の入力違い | 干渉によるエラー | ・類似業務の分配 |
| 3.3 | 受取人情報の未更新 | 中断に伴う抜け落ち | ・業務の重要度見直し<br>・業務ルーチンの見直し |
| 3.4 | 受取人以外の情報誤入力 | 二重補足スリップ | ・別業務のルーチンとの分離<br>・予測変換等の利用の停止 |
| 4.1 | 受取人情報の誤認 | 知覚の混同 | ・類似確認業務の分配 |
| 4.2 | 受取人情報の確認漏れ | オミッション | ・確認順序の統一<br>・複数人によるマルチチェックの徹底 |
| 4.3 | 受取人以外の情報確認漏れ | オミッション | ・確認順序の統一<br>・複数人によるマルチチェックの徹底 |
| 4.4 | 被送付者情報の誤認 | 知覚の混同 | ・類似確認業務の分配 |
| 4.5 | 被送付者情報の確認漏れ | オミッション | ・確認順序の統一<br>・複数人によるマルチチェックの徹底 |
| 4.6 | 被送付者以外の情報確認漏れ | オミッション | ・確認順序の統一<br>・複数人によるマルチチェックの徹底 |

## 4. おわりに

本稿では発生が増加しているヒューマンエラーによる情報漏えいを，秘匿性の高い情報を取り扱う業務として公務を例にインシデントを取り上げ，リスク要因を特定，分類しリスク低減策を提案した．具体的には，個人情報誤送付インシデントを例に，個人情報送付業務のフローチャートを作成し，業務中のプロセスと判断部分におけるリスク要因を特定した．また，特定したリスク要因をスキルベースにおけるヒューマンエラーの失敗モードに基づいて分類し，分類に対応したリスク低減策を提案した．

今後の課題としては，提案したリスク低減策の評価，並びに費用対効果の導出である．また，具体的な業務範囲を広げ，本稿で用いたリスク要因の特定，分類方法を一般化し，他業務のヒューマンエラーによる情報漏えいの低減策への拡張である．システム化すべきところと人的対策で行うべきところの分別，システム化すべきところにはどのようにシステム化すべきかの仕様の例示も行うべきであろう．

## 参考文献

[1] “Digital trends 2018: 153 pages of internet, mobile, and social media stats”. https://thenextweb.com/contributors/2018/01/30/worlds-internet-users-pass-the-4-billion-mark/, （参照 2019-07-22）.
[2] “平成 30 年版 情報通信白書”. http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd252120.html, （参照 2019-07-⓪2）
[3] NPO 日本ネットワークセキュリティ協会. 2018 年情報セキュリティインシデントに関する調査結果（速報版）, 2019
[4] NPO 日本ネットワークセキュリティ協会. 情報セキュリティインシデントに関する調査報告書 別紙. 2018
[5] 人事院. “懲戒処分の指針について”. https://www.jinji.go.jp/kisoku/tsuuchi/12_choukai/1202000_H12shokushoku68.html. （参照 2019-07-02）
[6] 総務省. 地方公共団体における情報セキュリティポリシーに関するガイドライン. 2018
[7] NPO 日本ネットワークセキュリティ協会. 2017 年情報セキュリティインシデントに関する調査報告書【速報版】, 2018
[8] ジェームズ・リーズン. ヒューマンエラー. 1990, 十亀洋訳, 海文堂出版
[9] CERT. US State of Cybercrime Survey. 2014, https://resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_298322.pdf,
[10] 真田大志. 最近のセキュリティ脅威と対策の方向性. 2017, UNISYS TECHNOLOGY REVIEW EXTRA EDITION 第 132 号, JUN. 2017.
[11] 植草皓, 谷本茂明, 畑島隆. 内的要因を考慮した新たな IT リスクマネジメントの提案及び評価. プロジェクトマネジメント学会, 2018, 2018 年度秋季研究発表大会予稿集, p.411-417
[12] 文部科学省. 教育情報セキュリティに関するガイドライン. 2017
[13] IPA. 内部不正による情報セキュリティインシデント実態調査 ―調査報告書―. 2016
[14] 総務省. 平成 29 年度における行政機関個人情報保護法の施行の状況について. 2019.
[15] “「個人情報」と「特定個人情報」～正しい理解のために～”, https://www.ppc.go.jp/files/pdf/tadashiirikai_kojin_tokutei.pdf. （参照 2019-8-7）
[16] “国民健康保険関係書類の誤送付による個人情報の漏えい” http://www.city.kobe.lg.jp/information/press/2019/05/20190516500701.html. （参照 2019-8-7）
[17] “平成 29 年度給与所得等に係る市民税・県民税特別徴収税額決定通知書の記載誤りによる特定個人情報の漏えいについて”. https://www.city.nonoichi.lg.jp/uploaded/attachment/6405.pdf. （参照 2019-8-7）
[18] “個人市・県民税特別徴収税額決定通知書の誤送付について（特定個人情報の漏えい）”. https://www.city.chiba.jp/somu/shichokoshitsu/hisho/hodo/documents/170524.pdf. （参照 2019-8-7）
[19] NPO 日本ネットワークセキュリティ協会. 2014 年情報セキュリティインシデントに関する調査結果, 2015

[20] NPO 日本ネットワークセキュリティ協会. 2016 年情報セキュリティインシデントに関する調査結果, 2017
[21] 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, 2008, vol.41, p. 7-12.
[22] 新原功一, 原田要之助. 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の対策の提案. 情報処理学会論文誌, 2014, vol.55, no.10, p.2318-2326.
[23] 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, 2010, vol.48, no.45, p1-8.
[24] 内田吉宣, 尾中章行. 管理対象とアクティビティー二つの観点でリスクを抽出. 日経 BP 社, 日経 systems, 2014-4, p.44-47.