Vol.2014-SPT-12 No.17
Vol.2014-EIP-66 No.17
2014/11/21

人の行動に注目した情報セキュリティ対策について —ヒヤリ・ハット情報の収集及びその活用について—

佐々木崇裕† 原田要之助†

近年，情報システムは組織にとって欠かせないものとなり，それへの依存も高まっている．その結果，情報システムの事故やトラブルが社会に大きな影響を与えるようになった．人の行動は，情報システムの事故等の一因となっている．人の行動による事故等に対して，航空や医療の分野ではヒヤリ・ハット事例収集の取組みが構築され，航空や医療分野の安全に貢献している．情報セキュリティ分野における，同様な取組みの構築について実現可能性を示す．

Information Security Measures for Focusing Human Behavior -The Collection and Application of a near miss(Hiyari-Hatto) incident-

TAKAHIRO SASAKI† YONOSUKE HARADA†

In these days, information system is indispensable for an organization. Dependence on information system increases. As a result, accidents or troubles of the information system have made a big influence on the society. The human behavior is one cause of an accident and the trouble of the information system. In the medical field, the system to collect and analyze near miss incident information caused by human error has been implemented, in order to support medical safety. In this paper, the feasibility of application to near miss incident of information system is discussed.

1. 情報セキュリティ事故の現状

1.1 はじめに

組織において,情報システムへの依存度は高まっており，一つの事故・トラブルが組織にさらには社会に大きな影響を与えるようになってきている．情報システムに関連した事故・トラブルの中には，ヒューマンエラーや規則違反といった人の行動に起因しているものがある．

本研究では，人の行動により発生する事故やトラブルを減らすため，人の行動により発生する事故やトラブルの事例収集の必要性，事例収集の形態及びその実施の実現可能性について考察する．

1.2 人の行動が原因の情報漏えい事故の発生状況

情報セキュリティ事故の一形態である，個人情報漏えい事故について，NPO 日本ネットワークセキュリティ協会及び情報セキュリティ大学院大学が調査・公表した，「2012 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～　第 1.2 版」 [1]がある．同報告書の中で図 1 の情報漏えいの事故の傾向が示されている．それによると，『2012 年は「管理ミス」，「誤操作」，「紛失・置き忘れ」で約 90%を占めた.』とある．「誤操作」，「紛失・置き忘れ」は，人が介在して発生した事故であり，また同報告書によれば『「誤操作」および「紛失・置き忘れ」はヒューマンエラーである.』と述べている．なお，この傾向は 2012 年以前の調査でも指摘されている．

つまり，情報漏えい事故は人の行動が多く絡んでいることがわかる．

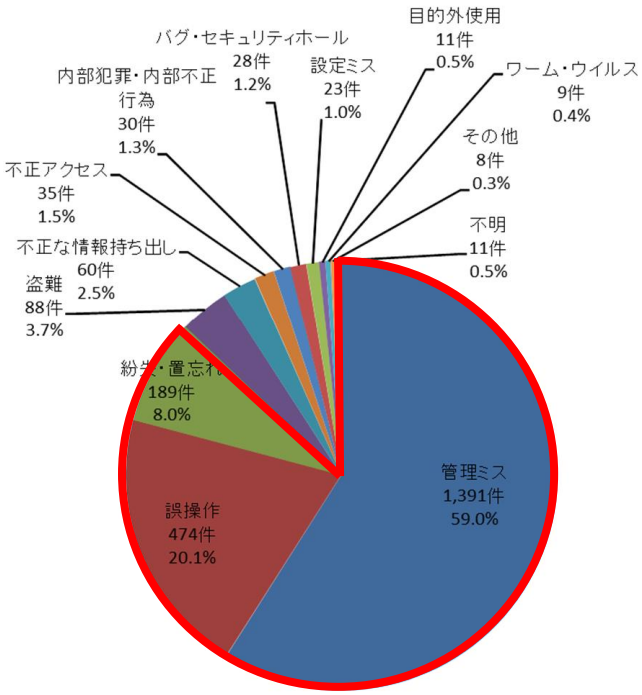

図 1　漏えい原因比率(件数)

出典: 2012 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～　第 1.2 版に加筆[1]

† 情報セキュリティ大学院大学
Institute of Information Security

Vol.2014-SPT-12 No.17
Vol.2014-EIP-66 No.17
2014/11/21

1.3 情報漏えい事故以外の人の行動が原因の情報システムの事故事例

情報漏えい事故以外にも，情報システムにおいては人の行動に起因した事故・トラブルが発生している．

人命にかかわる事例としては，2012 年 11 月に不適切な情報システムの運用により住民基本台帳の情報が流出し，その住所を元にストーカーにより女性が殺害された逗子ストーカー殺人事件が発生している[2]．不適切な情報システムの運用は，人により行われたものであるから、人の不適切な行動とも解釈することが出来る．

また，社会的な損失にかかわる事例としては，2005 年 12 月の東証におけるみずほ証券誤発注事件[3]や，2012 年 7 月にレンタルサーバー事業のファーストサーバ社のデータ消失事故[4]などが発生しており，それらはヒューマンエラーにより発生したとされている．

なお，ヒューマンエラーに関しては，一般的な失敗にみられる法則として中尾が『「人間は必ず失敗する動物である．しかも同じような失敗を繰り返す．ゆえに失敗は数が多くとも，互いに類似する．」』[5]と述べている．また，リーズンは『ヒューマンエラーは普遍的なものであり，避けられないものでもある』[6]と述べ，エラーは人間の特性であるとしている．つまり，エラーはある特定の人が引き起こす特別のことではなく，誰しもがいつでも同じようなエラーを起こしうるものであるということができる．

2. 医療分野における人の行動による事故等に対する取り組み

1 章では，情報システムにおける事故は人の行動により引き起こされるものがあり，さらに情報漏えい事故では高い確率でヒューマンエラーが原因であることを述べた．

ヒューマンエラーに対する対策については，医療及び航空の分野が進んでいる．医療及び航空分野においては，事故事例や，事故には至らないがヒヤリとしたり，ハットしたりして気づいた事象，いわゆるヒヤリ・ハットの事例を集めてその原因を追究し対策をとることで安全に貢献している．

一方，情報システム分野においては，ヒューマンエラーが原因の事故事例及びヒヤリ･ハットは集められておらず，容易に分析ができる環境にはなっていない．

どのようにすれば，情報システム分野においても事故事例及びヒヤリ・ハットを集められるようになるかを，本稿では医療分野の情報収集例を参考として考える．医療分野を参考とした理由は，公開事例が多いこと，日本国内において約 10 年前に体制が構築された体制であり，日本国内においては適用しやすいと推測したためである．

医療分野の情報収集例を見る前に，事故事例のみならず，ヒヤリ・ハットを集める必要性を検証する．

2.1 ヒヤリ・ハット

人の行動が原因となって事故が起きた場合，事故を端緒に，事故が起きるまでのストーリーに気付くことは可能である．しかし，事故が起きなくとも事故につながりそうなミスや事象にヒヤリとしたり，ハッとしたりして気づく，いわゆるヒヤリ・ハット[a]により，事故が未然に回避されることも多い．

ヒヤリ・ハットの収集の根拠として，ハインリッヒの法則（図 2，別名：1:29:300 の法則） があげられる．これは，アメリカの安全技師であったハインリッヒが，労働災害 5000 件以上を統計学的に調べた結果見いだしたものである．内容は，「1 件の重傷を伴う事故の背景には，同じ要因で 29 件の軽傷事故が発生しており，さらにけがはないものの同じ要因で発生した 300 件もの事象がある．」というものである．

図 2 のハインリッヒの法則が述べるところは，「事故の発生は確率的なものである」というものである．この法則は，従来「大事故を防止するには小さなトラブルをひとつひとつつぶすことが必要である」とも解釈されて，ヒヤリ・ハットとした事例を収集する活動であるヒヤリ・ハット活動推進の原動力となっている[7]．

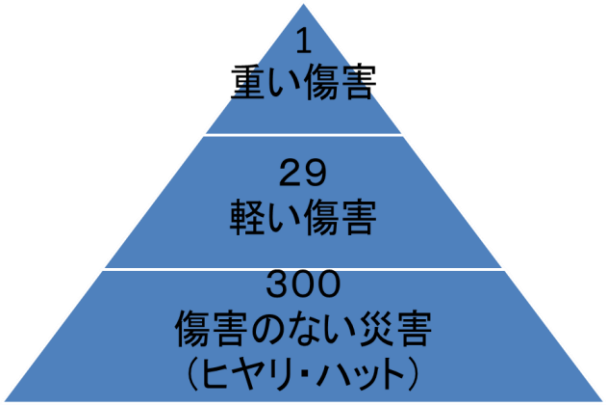

図 2　ハインリッヒの法則
出典: 交通心理学[7]を修正

なお，ファーストサーバ社は事故後，組織を挙げて抜本的な再発防止策を取り組んだ際，その中でも効果が大きかったのはヒヤリ・ハット活動であり，現場の意識を変えるきっかけとなったとしている[8]．具体的には，常駐する協力会社の社員を含む全従業員に対してシートを配布し，どんな気づきでも自由に記載させた．社員が挙げたヒヤリ・

a) ヒヤリ・ハットという言葉は、使う者や環境によってその解釈が異なる。医療分野においては、『平成 15 年 8 月 28 日　医政発第 0828004 号・医食発第 0828006 号　医療安全対策ネットワーク整備事業（ヒヤリ・ハット事例の収集、分析及び情報提供）の実施について』によりヒヤリ・ハット事例として
①誤った医療行為等が、患者に実施される前に発見された事例
②誤った医療行為等が実施されたが、結果として患者に影響を及ぼすに至らなかった事例
が定義されている。本稿では、この定義を応用して、次のように定義する。
① 誤った行為等が、実施される前に発見された事例
② 誤った行為等が実施されたが、結果として社会に影響を及ぼすに至らなかった事例

ハットは 580 件近くあり，それを整理し緊急に対策を打つべき課題を 16 件にまとめた．また，ヒヤリ・ハット情報は全社員で共有し、これをもとに対策を実施した．これらの活動により，課題や疑問を会議などで指摘できる雰囲気に変わったといった効果である．

2.2 医療分野におけるヒヤリ・ハット事例等収集構築の経緯

医療分野における，ヒヤリ・ハット事例の収集が始まった経緯は以下のとおりである．

平成 11 年に死亡医療事故が立て続けに 2 件発生し，医療事故防止の面から医療安全対策を求める社会的要請が高まった．その後，平成 13 年 10 月に，「医療安全対策ネットワーク整備事業（ヒヤリ・ハット事例収集等事業)」を開始した．更に，3 年後の平成 16 年には，医療事故情報収集事業が始まった[9][10] ．

2.3. ヒヤリ・ハット事例等収集の体制

次に，医療分野におけるヒヤリ・ハット事例等収集の体制について述べる．

2.2 で述べた通り，医療分野にはヒヤリ・ハット事例を報告する体制と医療事故情報を報告する体制との，2 種類の情報を収集する体制が構築されている．

ヒヤリ・ハット事例収集等事業への医療機関の参加は任意である．医療事故情報収集事業については，任意の参加を認めるとともに，国立高度専門医療研究センター，国立病院機構の病院，大学病院等一定の病院にあっては，医療法等の法令により参加が義務付けられている．

ヒヤリ・ハット事例収集等事業にあっては報告する情報が「発生件数情報」と「事例情報」とがあり，参加している医療機関は，「発生件数情報」のみの報告か，「発生件数情報」と「事例情報」との両方を報告するかを選択することができる．また，医療機関から当該機構への報告は，Web 上の情報報告画面への直接入力による報告方法，又は，指定フォーマット（XML ファイル）を作成し Web にアップロードする報告方法が準備されており，報告しやすい環境を整えている．

なお，ヒヤリ・ハット事例収集等事業及び医療事故情報収集事業は，日本医療機能評価機構が，中立的第三者機関として実施している．同機構は，収集された情報やその集計・分析結果は，報告書や年報，Web により広く社会に公表し，医療安全の推進に貢献している．

3. 情報システム分野におけるヒヤリ･ハット事例収集の提案

本章では，情報システム分野におけるヒヤリ・ハット事例収集の必要性を考察し，収集方法を提案する．なお，情報収集の対象をヒヤリ・ハットに限定して考察を進めていく．その理由としては，医療の分野での情報収集は，先にヒヤリ・ハット事例の収集が始まり，その後医療事故の情報収集が始まったことから，情報システム分野においても，まずはヒヤリ・ハット事例を収集する体制の構築を試みるべきと考えたからである．

3.1 情報システム分野におけるヒヤリ・ハット事例収集の必要性

情報システム分野でのヒヤリ・ハット事例収集の必要性については，ここでは人命にかかわる問題とガバナンスとの視点から考察する．

(1) 人命にかかわる問題としての必要性

医療分野においては，人の不適切な行動（ヒューマンエラー）が，最悪の場合，人命損失や後遺症としてその後の人生に直接影響を与えることから，ヒヤリ・ハット事例収集の体制が構築された．

一方，情報システム分野においては，最悪の場合，人命損失や後遺症としてその後の人生に直接影響を与えるということは意識されてこなかった．しかしながら，逗子ストーカー殺人事件では，人の不適切な行動が殺人事件につながるという結果を引き起こしており，情報システム分野でも人の不適切な行動が人命に直接影響を与えうるということを示した．このことは，情報システム分野においても，医療分野と同様にヒヤリ・ハット事例収集が必要になる根拠となると考える．

(2) ガバナンスの視点から見た必要性

ガバナンスの視点，特に情報セキュリティガバナンスの視点で考える．情報セキュリティガバナンスの規格，ISO/IEC27014:2013[11]では，6 つの原則が示されている．その中の一つ『原則 5：セキュリティに積極的な環境を醸成する』において，情報セキュリティガバナンスは，人間の行動に基づいて構築することが望ましいとしている．

人間の行動について，情報セキュリティマネジメント活動の有効性を評価するモニターは難しい．しかし，組織内部でヒヤリ・ハットの事例を収集・分析し，その分野のヒヤリ・ハットの発生件数等を比較することで，その活動に関連する効果を客観的に評価することができるようになる．

このように，ヒヤリ・ハット情報事例収集は情報セキュリティガバナンスの観点からも必要であると考える．

3.2 情報システム分野におけるヒヤリ・ハット事例収集方法の提案

情報収集方法については本稿で触れてきた医療分野における収集方法を参考にして，次の三つを提案する．

①2.1 で述べたファーストサーバ社が取り組んだヒヤリ・ハット活動のように，自組織内の情報を自組織内で収集し，分析・活用する方法．

②医療分野で行っているヒヤリ・ハット事例収集等事業のように，組織がヒヤリ・ハット事例を中立的な第三者機関に任意で提供し，第三者機関が集計・分析結果を公表する方法．

③医療分野で行っている医療事故情報収集事業のように，

法律等により（特定の）組織に対して報告を義務付け，報告のあった情報を集計・分析し公表する方法．

なお，③の方法に近い制度としては，個人情報保護法第20条で個人データの安全管理措置を求めており，各省庁のガイドラインにおいては，個人情報の漏えい等が発生した場合，事業者に対し事実関係・再発防止策等の公表，主務大臣等へ事実関係を報告するよう示されている[12][13]. また，プライバシーマーク制度においては，プライバシーマーク付与を受けている事業者に対して事故等が発生した場合に事故報告書の提出を義務付けている[14]．しかし，ファーストサーバ社のデータ消失事故のような，個人情報漏えいとは関係ない事例も実際には発生しており，より広い範囲において集める必要があると考える．

3.2.1 自組織のみで行う方法

自組織のみで行う情報システムに関する事例情報収集についてインターネットで調べてみると，すでに取り組みをはじめ，その内容や成果を開示している組織も確認できる[b]．この方法については，当該組織がヒヤリ・ハット事例収集により得るメリットが，収集するために費やす手間や時間といったコストを上回ると判断すれば，導入は難しいものではないと考えられる．

しかし，単一組織のみであり，収集できる情報には限りがある．また，発生頻度が低いものについては収集できない可能性がある．

なお,自組織のみで行う方法のさらに進んだ事例として，データ消失事故を起こしたファーストサーバ社の事故の情報及び第三者調査委員会による調査報告書の自主公開があげられる[4]．公表の義務のない公開された情報を元に，事故原因やヒヤリ・ハットを含む取り組んだ対策についての記事等が掲載されるなど[8][15][16]，社会に対して事故を議論する機会を与えたことは評価すべき正しい取組みであると考える．

3.2.2 第三者機関に任意で提供する方法

情報システム分野において，組織が任意でヒヤリ・ハット事例を第三者機関に提供する方法は存在していない．

情報システム分野における情報共有の参考になる取組みとしては，独立行政法人情報処理推進機構（以下，IPA）が第三者機関として活動する，サイバー情報共有イニシアティブ（J-CSIP[c]）があげられる．J-CSIP は，標的型攻撃といったサイバー攻撃による被害拡大を防止するため，サイバー攻撃に関する情報の共有と早期対応の場として発足した[17]．2013 年度は，IPA への情報提供件数は，385 件，参加組織への情報共有実施件数は 180 件であった．IPA は共有した情報からいわゆる「やり取り型」の手口の分析を行った上で，その情報を参加組織に共有する実績をあげている[18].

ただし,情報システム分野における情報共有については，標的型攻撃に対するセキュリティマネジメントモデルについて研究した村山が，標的型攻撃に関する情報は『複数組織で得られたより多くの情報を対策に活用することで，更に有効になる．しかし，組織の機密情報が添付されているメールなどの場合，そのままの状態で情報を外部に提供することは難しく，組織間の情報共有を行うことは重要と考えていても，抵抗感がどうしてもでてくる可能性がある.』[19]とし情報共有のむずかしさを指摘している．

しかし，J-CSIP は情報システム分野において，情報共有を機能させ，実績を出している．機能している理由は，第三者機関である IPA が①各参加組織や参加組織を束ねる業界団体と間で秘密保持契約を結ぶ，②情報提供元に関する情報や機微情報の匿名化を行う，③IPA の分析情報を付加した情報であっても情報提供元の承認を得る，といった，匿名化の仕組みが整えられているからと考える．

ヒヤリ・ハット事例収集にあっても，情報システムがその組織の固有の情報を取り扱う場面があることから，組織の秘密情報が含まれることがあると考えられる．そういった場合，情報を共有，公開することに抵抗感が生じると考えられ，J-CSIP のような仕組みが必要であると考える．

3.2.3 報告を義務付ける方法

医療分野においては，人命にかかわるような特定の事象等が発生した場合は，法律で報告するよう義務付けられている．しかし，ヒヤリ・ハット事例収集等事業への参加は，任意となっている．

航空分野にあっても，人命にかかわる事象は，法律で報告を義務付けられている．しかし，ヒヤリ・ハット事例については，報告の義務を課さず，自主報告としている．その理由としては,『義務報告では捕捉しにくい，民間航空の安全に関する情報を幅広く収集するため』としている[20].

両分野でヒヤリ・ハット事例の報告が任意となっているのは，発表した途端責任追及されるとなると，報告されなくなる可能性が高いからと考えられる．

医療や航空といったヒューマンファクターの対策が進んだ分野においても，ヒヤリ・ハット事例の報告を義務としていないことから，情報システム分野においても報告を義務にする必要性の論理を構成するのは難しい．

3.3 仮説

3.2.1 から 3.2.3 において，ヒヤリ・ハット事例収集の方法について考察を行った．これをもとに，以下の仮説を設定した．

仮説 1

組織は,ヒヤリ･ハット事例収集により得るメリットが，収集するために費やすコストや手間を上回ると判断すれば，

b) 株式会社インプレス,
http://www.imprex.co.jp/managementsystem/security.html, (2014 年 4 月 28 日閲覧).
株式会社リコー,
http://www.ricoh.com/ja/security/management/activity/accident.html, (2014 年 4 月 28 日閲覧).
c) Initiative for Cyber Security Information sharing Partnership of Japan

Vol.2014-SPT-12 No.17
Vol.2014-EIP-66 No.17
2014/11/21

ヒヤリ・ハット事例収集を行う．

仮説 2

組織は，組織に関する情報や機微情報の匿名化が担保されていれば，任意にヒヤリ・ハット事例を第三者機関に提供する可能性がある．

4. アンケート結果

3 章において設定した仮説に対して，アンケート調査を行った．

4.1 アンケート概要

原田研究室では 2014 年 8 月に「情報セキュリティ調査」アンケートを郵送にて実施した．対象は，日本国内のプライバシーマーク取得組織，ISMS 認証取得組織，官公庁，教育機関などから，ランダムに選んだ 4,500 組織（送達確認できたのは 4,374 組織）である．回答率は約 10%であった．

本稿作成現在，データ集計途中である為，暫定データ[d]を使用して分析した．暫定データであるため，今後の確認作業によっては結果が変わる可能性がある．

回答者の傾向としては，従業員数では，300 人以下の組織が 74%と組織規模が小さい組織の回答が多い（図 3）．

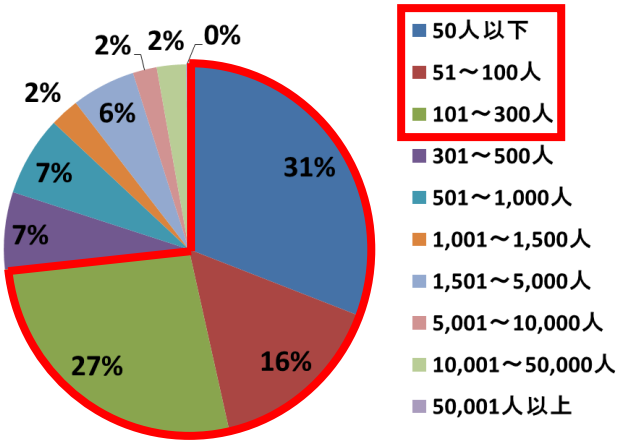

図 3　全従業員数（n=437，択一）

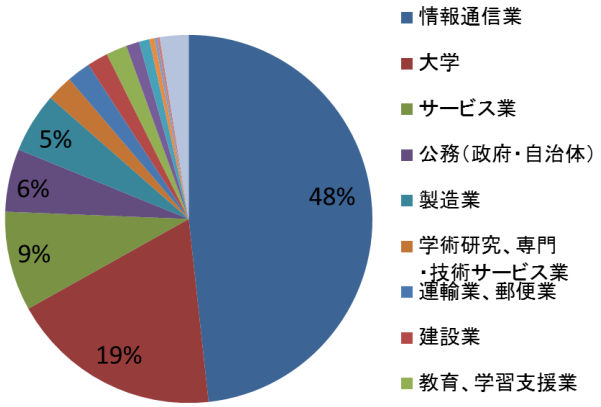

図 4　業種（n=437，択一）

d)暫定データは 2014 年 10 月 9 日に準備できた，回収した全 437 件のアンケートを入力したが，入力誤りの確認を行っていないデータである．

また，業種としては，情報通信業が 48%と約半数を占め，次に大学，サービス業，公務，製造業と続く結果となった．(図 4)

4.2 仮説 1 に対するアンケート結果

仮説 1 に対して，組織にメリットの無いことは行わないという仮定のもと，組織内で人的ミスによる事故・トラブルの情報を集めているか，また，どのような情報を集めているかを調査した．情報の種別としては，内容については，「誤操作」，「紛失・置き忘れ」，「設定ミス」に区別し，影響の度合いでは，事故となって「社会に影響を与えた」場合と「ヒヤリ・ハット」で事故とならなかった場合とを区別して調査した．調査結果を図 5 に示す．

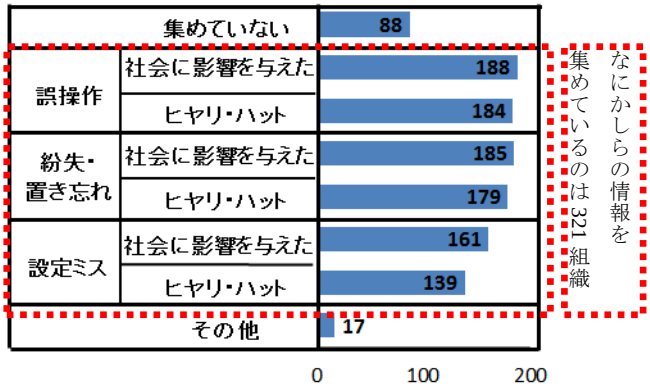

図 5　人的ミスの情報収集状況（n=437，複数選択）

人的ミスだけが原因の場合「集めていない」組織は 88 組織（約 20%）であった．

一方，「なにかしらの情報を集めている」組織はグラフからは直接読みとれないが図 5 中において点線で囲んだ項目を 1 つ以上選択している組織をカウントしたところ，321 組織（約 73%）あった．このことから，現時点では仮説 1 は成り立つと考えられる．

内容別では，「誤操作」，「紛失・置き忘れ」にあっては 180 組織（40%）前後であった．「設定ミス」では，件数の多い「社会に影響を与えた」場合に着目すると約 160 組織（約 37%）であり，わずかであるが他の 2 つの項目より少ない結果となった．

また，影響の度合いについては，「誤操作」・「紛失・置き忘れ」においては，「社会に影響を与えた」場合と「ヒヤリ・ハット」の場合にさほど差が出ない（%換算で 1.5%以内）という結果となった．一方，「設定ミス」においては，その差が他の 2 つの内容と比べ若干大きく（%換算で約 5%）出た．

今回は暫定データの為，有意性まで確認はしていないが，内容別及び影響度別それぞれにおいて，「設定ミス」のみに特徴が出た．このことから，組織において，「設定ミス」だけ事故やトラブルに対する認識度が違う可能性が考えられる．

Vol.2014-SPT-12 No.17
Vol.2014-EIP-66 No.17
2014/11/21

4.3 仮説 2 に対するアンケート結果

仮説 2 に対して，「国などによりガイドラインが示され，ヒヤリ・ハット事例の収集・分析・公表を担当する公平・中立的で独立した第三者機関が設立された場合」と前提を置いたうえで，どのような条件が整えばヒヤリ・ハット事例を第三者機関に提供するか調査した．前提を置いた理由は，医療分野がヒヤリ・ハット事例収集を事故事例よりも先行して行ったことを参考にしたためである．

調査結果を図 6 に示す．

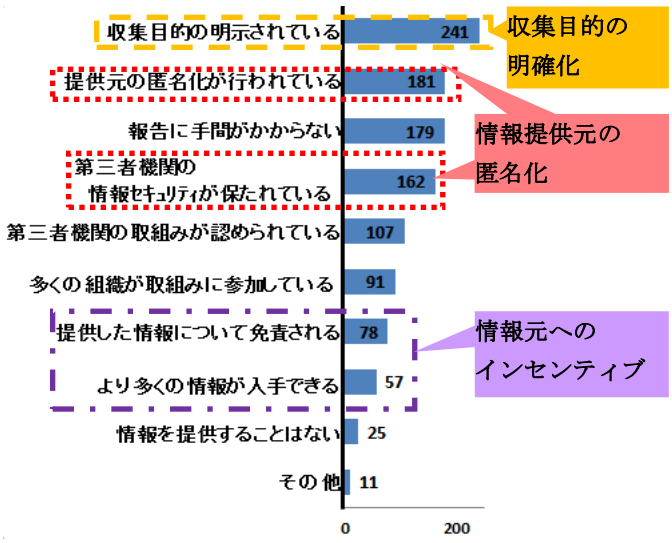

図 6　第三者機関への提供条件 (n=437) 3 つ選択

仮説 2 では，情報提供するには提供元の匿名化が重要としていたが，結果は「収集目的が明示されている」が 241 組織（約 55%）と一番多い結果となった。

匿名化に関する項目については、2 番目に「提供元の匿名化」181 組織（約 41%），4 番目に「第三者機関の情報セキュリティが保たれている」162 組織（約 37%）が入った。

また，「報告に手間がかからない」ことを条件としたのは 179 組織（約 41%）であった．

このことから、ヒヤリ・ハット事例を収集するには，情報提供元の匿名化も重要であるが，収集目的を明確に示すことが重要になると考える．

どのような条件であっても「情報を提供することはない」とする組織は，25 組織（6%弱）と少ない結果となった．

「情報を提供することはない」とする組織が少ないこと，情報提供する条件として「収集目的の明確化」や「情報提供元の匿名化」等を求める組織が存在することから，実際に取組みが行われた際には，条件があえば参加する組織は出てくるのではないかと推測できる．

なお，「情報提供元のインセンティブ」になると考え設定した質問項目「提供した情報について免責される」，「より多くの情報が入手できる」については，それぞれ 78 組織（約 18%），57 組織（約 13%）と少なく，情報提供することに対してインセンティブを求める組織は少ないことが分かった．

5. まとめ

今回，医療分野における人の行動による事故等に対する取り組みを参考に，情報セキュリティ対策として，情報システム分野におけるヒヤリ・ハット事例収集の必要性及びその収集方法を述べた．また，アンケート調査を行い，ヒヤリ・ハット事例収集を行っている組織があること，第三者機関によるヒヤリ・ハット事例収集の実現可能性があることを示した．

今後は，確定したアンケートデータを用い，回答者の組織の規模，業種，職位等でのクロス分析を行って，どのように違いが出てくるかなど，詳細分析及び考察を行っていく．合わせて，収集した情報の活用方法についても検討していく．

謝辞　本研究にご協力いただいた情報セキュリティ大学院大学の教授等関係者，原田研究室の先輩，同僚の皆様に謹んで感謝の意を表する．また，アンケートへの回答を頂きました企業や団体・組織の皆様，アンケートのデータ入力に多大な協力を頂いた神奈川県内特別支援学校の皆様に感謝申し上げます．

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: 2012 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～ 第 1.2 版, http://www.jnsa.org/result/incident/data/2012incident_survey_ver12.pdf (2014 年 10 月 10 日閲覧).
2)　逗子市: 個人情報の外部流出について, http://www.city.zushi.kanagawa.jp/syokan/kouhou/new/p05141.html (2014 年 10 月 10 日閲覧).
3)　日経 BP 社: みずほ証券の誤発注、問われるフェイルセーフ, http://itpro.nikkeibp.co.jp/article/COLUMN/20051227/226805/ (2014 年 10 月 10 日閲覧).
4)　ファーストサーバ株式会社: 2012/6/20 に発生した大規模障害に関するお詫びとお知らせ, http://support.fsv.jp/urgent/fs-report.html (2014 年 10 月 10 日閲覧).
5)　中尾政之: 失敗の「予防学」, p.1, 三笠書房 (2007 年).
6)　ジェームズ・リーズン他: 保守事故, p.133, (2005 年).
7)　蓮花一己,向井希宏: 交通心理学, p.49,119, 放送大学教育振興会 (2012 年).
8)　玄忠雄: “失敗” が鍛えるシステム運用力, 日経コンピュータ 2014.2.20 号, p.81-83, 日経 BP 社, (2014 年).
9)　厚生労働省: 主な医療安全関連の経緯, http://www.mhlw.go.jp/topics/bukyoku/isei/i-anzen/keii/ (2014 年 4 月 22 日閲覧).
10)　後信: 我が国の医療安全対策の歩みと医療事故,ヒヤリ・ハットの収集事業, 日本医療機能評価機構 NEWS LETTER,2012 No.4, p.2-5 (2012 年).
11)　ISO/IEC 27014:2013, Information technology – Security techniques – Governance of information security.
12)　総務省: 電気通信事業における個人情報保護に関するガイドライン, http://www.soumu.go.jp/main_content/000254517.pdf, (2014 年 10 月 15 日閲覧).
13)　経済産業省: 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,
http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf,
(2014 年 10 月 15 日閲覧)
14) 一般財団法人日本情報経済社会推進協会プライバシーマーク推進センター: プライバシーマーク付与に関する規約,
http://privacymark.jp/reference/pdf/pmark_guide/PMK500.pdf, (2014 年 9 月 15 日閲覧).
15) アイティメディア株式会社: マニュアル無視、不十分なバックアップ――ファーストサーバが最終報告書,
http://www.atmarkit.co.jp/news/201208/02/firstserver.html, (2014 年 10 月 15 日閲覧).
16) 株式会社 KADOKAWA: 信頼を失ったファーストサーバが挑んだ事故調査と再発防止, http://ascii.jp/elem/000/000/913/913209/, (2014 年 10 月 15 日閲覧).
17) 情報処理推進機構: サイバー情報共有イニシアティブ (J-CSIP(ジェイシップ)), http://www.ipa.go.jp/security/J-CSIP/ ,(2014 年 10 月 10 日閲覧).
18) 情報処理推進機構: サイバー情報共有イニシアティブ（J-CSIP）2013 年度 活動レポート～ 「やり取り型」攻撃に関する分析情報の共有事例 ～,
http://www.ipa.go.jp/files/000039231.pdf ,(2014 年 10 月 10 日閲覧).
19) 村山厚: 企業における標的型攻撃に対するセキュリティマネジメントモデルに関する考察―標的型攻撃に関する分析情報を起点として―, 2013 年度情報セキュリティ大学院大学修士論文.
20) 国土交通省航空局: 航空安全プログラム,
http://www.mlit.go.jp/common/001033880.pdf , (2014 年 10 月 10 日閲覧).