情報処理学会論文誌 Vol.56 No.12 2337–2345 (Dec. 2015)

情報セキュリティ分野における ヒヤリ・ハット情報の収集について

佐々木 崇裕[1,a)] 原田 要之助[1]

受付日 2015年2月28日, 採録日 2015年9月2日

概要：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情報漏えいが社会に大きな影響を与えるようになった．これらの事故・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．人の行動に起因する事故を減らすために航空や医療の分野では，事故という結果に至らなかったヒヤリ・ハット情報を収集・分析・公表する取り組みが行われており，安全に貢献している．本研究では，そのような取り組みが情報セキュリティ分野に導入できないか，取り組みの必要性，事例収集の形態について考察を行った．また，アンケート調査を通じて，その取り組みの導入を実現する可能性があること，情報を収集する際は収集目的を明確に示すことが重要であることが分かった．最後に，情報セキュリティ分野におけるヒヤリ・ハット情報収集の具体的な方法を提案する．

キーワード：情報セキュリティ，ヒューマンエラー，ヒヤリ・ハット情報収集，ハインリッヒの法則

Study on the Collection of an Information Security Near Miss (Hiyari-Hatto) Incident Cases

Takahiro Sasaki[1,a)] Yonosuke Harada[1]

Received: February 28, 2015, Accepted: September 2, 2015

Abstract: With the dependence increases more and more today, the information system has become indispensable for organization operation. As a result, an accident and a trouble of the information system came to have a big influence on the society. The human behavior, such as human error and the rule violation, is one cause of an accident and the trouble of the information system. Action to collect "near miss incident information" caused by human error, and to analyze it, and to announce to the public has been implemented in the aviation and the medical field to support safety. In this research, an information collection method capable of collecting information required for support safety is considered, to introduce the similar system into the information system field. And, the major findings from questionnaire survey are, the participant organization of this activity might increase if the condition matched, and the most important point is to show clearer collection purpose of information. Finally the collection of a near miss (Hiyari-Hatto) incident in the field of information security is analyzed to complete a concrete method.

Keywords: information security, human error, the collection of Hiyari-Hatto incident, Heinrich's law

1. はじめに

1.1 情報セキュリティ事故の原因

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の原因は，「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] によると，「誤操作」，「管理ミス」，「紛失・置き忘れ」といった，人の行動に強く関係したもので多くの割合が占められている．その傾向は 2005 年以降続いており，2012 年の漏えい原因では，「誤操作」が 20.1%，「管理ミス」が 59.0%，「紛失・置き忘れ」が 8.0%であり，これらを合計すると約

[1] 情報セキュリティ大学院大学
Institute of Information Security, Yokohama, Kanagawa 221–0835, Japan
[a)] mgs135504@iisec.ac.jp

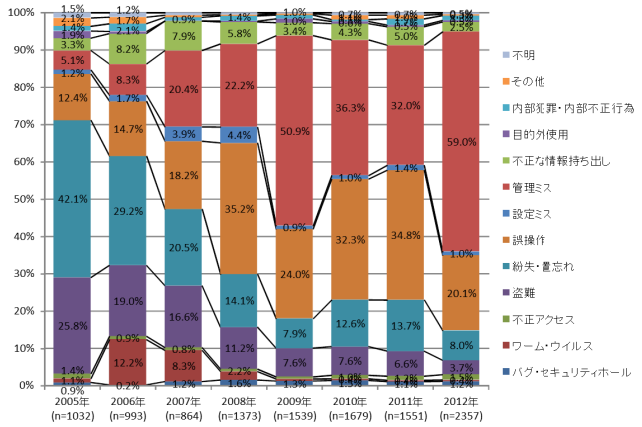


図 1 漏えい原因比率の経年変化 [1]

Fig. 1 Annual changes of number of information breach incident (breakdown by causes).

90%を占めていることが分かる．詳細を**図 1** に示す．

また，同報告書では，『「誤操作」および「紛失・置き忘れ」はヒューマンエラーである』と指摘している．なお，本報告書は，企業が個人情報を漏えいした場合に公表する事故情報を集めて分析したものである．企業は個人情報を漏えいした場合に個人情報保護法により，情報漏えいを報告する義務があるからである．すなわち，事故情報を公開したものを収集してデータベース化したものである．情報漏えいに至らなかった情報セキュリティにおけるヒヤリ・ハット（2 章で定義する）に関する情報は公開されておらず不明のままである．

1.2 論文の構成

2 章では情報セキュリティ分野[*1]におけるヒヤリ・ハットについて定義するとともにヒヤリ・ハット情報収集の先行事例について述べる．3 章では情報セキュリティ分野におけるヒヤリ・ハット情報収集の必要性，実現可能性を検討する．そのうえで 4 章において，情報セキュリティ分野におけるヒヤリ・ハット情報収集の方法を提案する．5 章では総括および今後の課題を述べる．

2. ヒヤリ・ハットとその情報収集についての先行事例

2.1 ヒヤリ・ハットについて

ISO31000:2009 Risk management – Principles and guidelines（以下，ISO31000 という）は，リスクマネジメントのガイドラインであり，この定義を情報セキュリティ分野にあてはめると，リスク源（Risk Source：リスクにつながる要素で脅威や脆弱性が含まれる）が，情報セキュリティの機密性（Confidentiality），完全性（Integrity），可用性（Availability）を脅かすことで引き起こされる事象（event）が起きて，経営に影響するなどの結果（Consequence）につながることになる．なお，ISO31000 では，『事象の発生を結果として顕在化した「情報セキュリティにおける事故」』と『結果にまで至らない事象の発生を「情報セキュリティにおけるヒヤリ・ハット」』と定義している．佐藤ら [2] は，この ISO31000 の定義をベースにして，さらに，事故とヒヤリ・ハットを含むものとして「情報セキュリティの失敗」を定義している．すなわち，失敗に対する対策を実施するため，機械工学の分野の失敗学の概念を導入し，失敗事例を原因に基づき類型化し，新たな設計に生かす考え方を情報セキュリティ分野に導入し，その対策の有用性を示している．

表 1 事故とヒヤリ・ハットの分類

Table 1 Classification with incident and near-miss.

分類	情報セキュリティにおける失敗	
	事故	ヒヤリ・ハット
内容	CIAを損なう結果の発生	結果にまで至らない事象の発生
具体例	・メールの宛先間違いによる誤送信 ・障害を起こすコマンドの実行 ・個人情報の記録されたUSBメモリの紛失	・メール送信前の宛先間違いへの気づき ・ダブルチェックによる，コマンドミスの回避 ・情報の入っていないUSBメモリの紛失

本稿では，佐藤らの定義に基づき情報セキュリティ事故をとらえ，これに至らない事象の発生をヒヤリ・ハットとする．これらの分類とその具体例を**表 1** に示す．

さらに，佐藤らは，一般に情報セキュリティの事故情報は公表されにくく，その収集が難しいと述べている．その理由としては，情報セキュリティ事故の事例情報そのものを効果的に収集する方法についての研究がなされていないからと述べている．

一方，ヒューマンエラー[*2]に対するヒヤリ・ハットへの対策が進んでいる分野として航空や医療の分野があげられる．これらの分野において，ヒューマンエラーへの対策の 1 つとして，事故やヒヤリ・ハット情報を収集・分析し，その分野の安全に貢献している．本章では，ヒヤリ・ハットについて考察した後に，各分野のヒヤリ・ハット情報の収集について述べる．

2.2 ヒヤリ・ハットとヒューマンファクタ

一般に，事故が起きた場合，その原因を追究して対策をとることになる．ヒューマンファクタが起因となって事故が起きた場合，その事故を端緒に，事故が起きるまでのストーリーに気づくことは可能である．しかし，事故が起き

[*1] 本稿では，情報システムを扱う人の行動に注目することから，情報システムとその運用も含めた分野として，情報セキュリティ分野という言葉を用いる．

[*2] 本稿では，『計画された知的または物理的な活動で，意図した結果が得られなかったときで，これらの失敗がほかの出来事によるものでないときの，すべての場合を包含する本質的な項目として，エラーを考える』という定義を用いる．Reason, J.：ヒューマンエラー—認知科学的アプローチ—，海文堂出版 (1994).

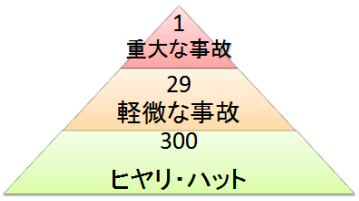


図 2 ハインリッヒの法則
Fig. 2 Heinrich's law.

なくて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こともある．いわゆるヒヤリ・ハットといわれるものである．

ヒヤリ・ハットの関連として，アメリカの安全技師であったハインリッヒは，潜在的有傷災害の頻度に関するデータから，同じ人間の起こした同じ種類の 330 件の災害のうち，300 件は無傷で，29 件は軽い障害をともない，1 件は報告を要する重い障害をともなっていることを判明させた [3]．ハインリッヒの法則（**図 2**，別名：1 : 29 : 300 の法則）として知られているものであり，300 件の無傷の事象が，いわゆるヒヤリ・ハットに該当する．

こ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．つまり，小さなトラブルはたまたま小さなトラブルで済んだだけであり，大事故になった可能性もありうる．これから大事故を防止するには小さなトラブルを 1 つ 1 つ潰すことが必要であるとも解釈することもできる．

また，別の視点からみると，ヒヤリ・ハットは何らかの気づきによって事故を回避した状況でもある．何らかの気づきとは，人が事前に危険に気づいたり，機器やセンサからのアラートであったりなどである．これらの気づきが得られるのは，それがコントロールされている状況にあったからであり，逆にいえばすべてのコントロールが機能しなかった場合が事故となるとも解釈することができる．

情報セキュリティ分野におけるヒヤリ・ハットを考えるうえで参考となる先行分野の情報収集について述べる．

2.3 航空分野におけるヒヤリ・ハット情報収集

航空分野におけるヒヤリ・ハット情報などを収集する体制について述べる．

(1) 事故および重大インシデント情報[*3]の収集

航空分野においては，航空法第 76 条および同法第 76 条の 2 により，機長に対して事故や重大インシデントが発生した場合および発生する恐れがあると認められる場合，国土交通大臣への報告を義務付けている．また，航空法第 111 条の 4 により，本邦航空運送事業者に対し，航空機の

[*3] 航空法第 76 条の 2 および航空法施行規則第 166 条の 4 に定められている航空事故が発生するおそれがあると認められる事態であり，「閉鎖中の又は他の航空機が使用中の滑走路からの離陸又はその中止」，「航空機から脱落した部品が人と衝突した事態」など 16 の事態が定められている．

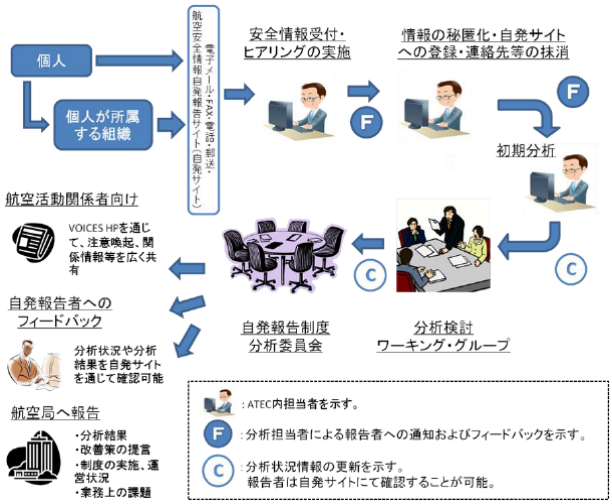


図 3 VOICES における分析業務フロー [5]
Fig. 3 Flow of VOICES.

正常な運航に安全上の支障を及ぼす事態が発生したときに，国土交通大臣への報告を義務付けている．

(2) ヒヤリ・ハット情報の収集

一方，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に，国土交通省航空局により，国際民間航空条約第 19 附属書安全管理の規定に従った，航空安全情報自発報告制度（略称：VOICES）が運用されている．

自発報告制度の考え方は，『航空安全プログラム』[4] 第 4 章 2 に記述されており，それを受けて VOICES の運営は，公平性を担保するために第三者機関である公益財団法人航空輸送技術研究センター（略称：ATEC）に委譲されている．

情報収集の方法について以下に述べる [5]．航空分野の報告者は，航空活動に自ら直接携わる個人となっており，個人が直接 ATEC に報告することになっている（個人が所属する組織経由で報告する場合もある）．これは，航空業界に関与する者が専門的な教育を受けているなど，航空分野特有の事情があるからと考えられる．報告手段には，「電子メール」，「ファックス」，「電話」，「郵送による報告」，「航空安全情報自発報告サイト（WEB ページ）」の 5 種類の報告方法が準備されており，報告しやすい環境が構築されている．

ヒヤリ・ハット情報の流れとしては，報告の受付，分析担当者によるヒアリング，情報の秘匿化，自発サイトへの登録，連絡先などの抹消，分析検討およびフィードバックに分かれている（**図 3** 参照）．

以下に作業の概略を示す．報告の受付・ヒアリングの実施では，本報告制度の対象となるかを確認して，情報を受理する．受理できない場合は，ATEC 内分析担当者（以下，分析担当者という）から報告者に連絡する．また，不足している情報があれば分析担当者により電話や電子メールで

ヒアリングを行って，内容を確定させる．

報告内容が確定したヒヤリ・ハット情報については，報告手段にかかわらずすべての報告に対して，個人または会社などが特定される可能性のある情報を消去または伏せ字にするなど，匿名化がなされる．その後，航空安全情報自発報告サイト以外の手段で提供された情報は，分析担当者が当該サイトに代理登録する．その際，報告者が自分の報告内容やその分析状況などを当該サイトで確認する際に必要となる「受付番号」と「パスワード」を報告者に伝える．これらの一連の作業を実施後に，分析担当者は報告者の連絡先などを抹消する．つまり，この段階まで進むと，報告者は自分の報告内容や分析状況を確認できるが，本人以外のいかなる人も報告者を特定できず，またコンタクトできない．

収集したヒヤリ・ハット情報は，ATEC 内で各業務分野に精通した担当者で構成された専門チームにより，民間航空の安全を阻害しうる要因を特定すべく予防的な観点から分析が実施される．専門チームの分析結果は，業務分野別に設定する分析検討ワーキング・グループで各分野の専門家からの意見収集を行った後，学識経験者などで構成される自発報告制度分析委員会で，最終的な分析結果をとりまとめて，必要なヒヤリ・ハット情報とその分析結果を VOICES ポータルサイトに掲載する．また，ATEC はこれらのヒヤリ・ハット情報に基づく分析結果の報告と改善策の提案を航空局に行っている．なお，ATEC から発信されるすべての情報や報告・提言では，報告者を特定できる情報が含まれないようにしている．

なお，日本の VOICES と同様の取り組みは，すでに，アメリカ，イギリス，ブラジル，台湾，中国，南アフリカなど，12 の国や地域で運用され，一部のヒヤリ・ハット情報が相互交換されている．

2.4 医療分野におけるヒヤリ・ハット情報収集

2.4.1 医療分野におけるヒヤリ・ハット情報収集体制構築の背景

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

1999 年に重大な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，2001 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）」が開始された．さらに，3 年後の 2004 年には，医療事故情報を収集する「医療事故情報収集事業」が始まった．

2.4.2 医療分野におけるヒヤリ・ハット情報収集の体制

次に，医療分野におけるヒヤリ・ハット情報などを収集する体制について述べる [6], [7].

(1) 医療事故情報の収集

医療分野では，医療事故情報収集・分析・提供事業として事故情報の収集が行われている．この事業では，民間の医療機関の任意の参加を認めるとともに，医療法などの法令により，国立高度専門医療研究センター，国立病院機構の病院，大学病院など一定の病院の参加が義務付けられている．医療事故情報の報告先は中立的第三者機関である，日本医療機能評価機構である．

(2) ヒヤリ・ハット情報の収集

ヒヤリ・ハット情報の収集は，医療事故情報の報告とは別のヒヤリ・ハット事例収集・分析・提供事業として行われている．この制度にあっては，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．報告先は，日本医療機能評価機構であり，医療機関から同機構への報告は，Web 上の情報報告画面への直接入力による報告方法，または，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．

また，同機構では，報告された情報を専門家により分析し，Web ページに掲載するなどして，公表している．

2.5 その他分野におけるヒヤリ・ハット情報の収集

航空や医療分野以外の分野においても事故情報の収集やヒヤリ・ハット情報の収集が行われている．

特に，トラック事業 [8]，保育園 [9]，消防 [10] など複数の分野においてもヒヤリ・ハット情報の収集が広く行われている．これらは，航空分野や医療分野に比べ規模は小さいが，ヒヤリ・ハット情報が収集され分析されて，将来の事故の予防などに役立てられている．さらに，単一組織においてヒヤリ・ハット情報を集めている組織も多数見受けられる．たとえば，京都大学 [11]・三重大学 [12] など複数の大学組織において，それぞれヒヤリ・ハット情報を収集し，将来の事故回避などに役立てている．

ヒヤリ・ハット情報収集の仕方や公開・活用の仕方は，それぞれの分野で異なっているが，共通する点として，ヒヤリ・ハット情報の報告者の匿名化がなされていることがあげられる．

2.6 小括

様々な分野において，ヒヤリ・ハット情報収集は取り組まれており，航空，医療の分野では海外でもその取り組みが行われている．複数の分野でヒヤリ・ハット情報収集が行われているのは，この取り組みが事故を減らす対策として効果が認められているからと考えられる．

各分野の事故とヒヤリ・ハットの情報収集状況および情報収集の根拠または事業などを**表 2** に示す．

表 2 から分かることは，情報セキュリティ分野のヒヤリ・ハット情報収集と活用がなされていないことである．

表 2 各分野の事例収集の状況
Table 2 The collection situation of the incident and the near miss of each field.

分野	事故	ヒヤリ・ハット	備考
航空	○ 航空法 等	○ VOICES	海外においても実施
医療	○ 医療法 医療事故情報収集事業等	○ ヒヤリ・ハット事例収集等事業	海外においても実施
トラック事業	○ 道路運送車両法 自動車事故報告規則等	○ ドライブレコーダ映像を活用したヒヤリハット集	
情報セキュリティ	△ （個人情報について**のみ存在**） 個人情報保護法 各省庁の個人情報保護に関するガイドライン等	× **存在せず**	標的型攻撃，不正アクセスについては報告制度が存在

（○は実施済み，△は一部実施，×は未実施を表す.）

3. 情報セキュリティ分野におけるヒヤリ・ハット情報収集にかかる検討

本章では，情報セキュリティ分野におけるヒヤリ・ハット情報収集の必要性を考察し，具体的な収集方法を考察する．なお，本章では情報セキュリティ分野のヒヤリ・ハットの情報収集に限定して考察を進めていく．

3.1 情報セキュリティ分野におけるヒヤリ・ハット情報収集の必要性

サイバーセキュリティ基本法では，国に対して電力やガス，交通，金融，情報通信など 13 分野の重要インフラ事業者におけるサイバーセキュリティに関する取り組みの促進などの施策を講ずることを定め，その取り組みの中に情報の共有があげられている．また，内閣官房情報セキュリティセンターの担当者は，「実害に至らないヒヤリ，ハットの事例でも，情報共有が必要で，今後の課題になる」と述べている [13]．このことは，重要インフラ分野における，ヒヤリ・ハット情報収集の必要性を示すものである．

さらに，重要インフラ以外の情報セキュリティ分野でのヒヤリ・ハット情報収集の必要性については，次の 2 つの観点からその必要性があると考えられる．

3.1.1 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，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・ハット情報収集の体制が構築された．

一方，情報セキュリティ分野においては，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 [14]，情報セキュリティ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，情報セキュリティ分野においても，医療分野と同様にヒヤリ・ハット情報の収集が必要となる根拠になると考える．

3.1.2 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，JIS Q 27014:2015 [15] では，6 つの原則が示されている．その中の 1 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，経営者が実施すべき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のモニタは難しい．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・ハットの発生件数などを比較することで，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 情報セキュリティ分野におけるヒヤリ・ハット情報収集方法の提案

情報収集方法については本稿で触れてきた航空や医療，その他の分野における収集方法を参考にして，次の 3 つが考えられる．

① 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 航空や医療分野などで行われているヒヤリ・ハット情報収集のように，組織がヒヤリ・ハット情報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 航空や医療分野で行っているように法律などにより（特定の）組織に対して事故情報の報告を義務付け，報告のあった情報を集計・分析し公表する方法．情報セキュリティ分野では，表 2 中に示した個人情報漏えいの場合がこれにあたる．

3.2.1 自組織のみで行う方法

自組織のみで行う情報セキュリティに関する事故情報やヒヤリ・ハット情報収集については，すでに取り組みをはじめ，その内容や成果をインターネットで開示している組織を確認できる[*4]．すなわち，当該組織がヒヤリ・ハット

[*4] 株式会社インプレス，http://www.imprex.co.jp/managementsystem/security.html（参照 2014-04-28）．
株式会社リコー，http://www.ricoh.com/ja/security/management/activity/accident.html（参照 2014-04-28）．

情報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，単一組織のみの取り組みだけでは，収集できる情報の範囲と種類には限界がある．また，発生頻度が低いものについては顕在化しないと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およ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 [16]．公表の義務のない公開された情報をもとに，事故原因やヒヤリ・ハットを含めて取り組んだ対策についての記事が掲載されるなど [17]，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り組みであるといえる．

3.2.2 第三者機関に任意で提供する方法

現在，情報セキュリティ分野において，組織が任意でヒヤリ・ハット情報の収集や活用を第三者機関に提供する方法は存在していない．

しかし，2 章で述べたように，航空，医療，その他の分野において実施されており，情報セキュリティ分野にも導入するのは難しくないと考えられる．ただし，情報システムは組織の機密情報を扱うこともあり，このような情報が外部に漏れることは組織としては避けたいという意識が働く．このような意識をなくすために組織に関する情報や機密情報の匿名化が必要となる．

3.2.3 報告を義務付ける方法

航空分野にあっては，事故および重大インシデント情報の報告については，法律で義務付けられている．一方，ヒヤリ・ハット情報の報告については義務を課さず，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 [4]．航空分野でヒヤリ・ハット情報の報告が任意となっているのは，報告者の信頼を得ることを最優先にしているからである [18]．

航空というヒューマンエラーの対策が進んだ分野においても，ヒヤリ・ハット情報の報告を義務とせず，報告者の信頼を得ることを最優先にして，成功している現状をかんがみるに，情報セキュリティ分野においても報告を義務とせず，信頼を得ることを最優先にすべきであり，報告を義務付けるべきではないと考える．

したがって，③ の方法は検討から外す．

3.3 情報セキュリティ分野におけるヒヤリ・ハット情報収集の実現可能性

3.3.1 ヒヤリ・ハット情報収集についての現状調査

3.2 節において，ヒヤリ・ハット情報収集の方法について考察を行った．その結果，

① 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 組織がヒヤリ・ハット情報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，

の 2 つが情報セキュリティ分野におけるヒヤリ・ハット情報収集が可能な方法と考えられる．

そこで組織が人的ミスの情報収集を行っているか，それらの情報を第三者機関に提供するとするならばどのような条件であればよいか，アンケートによる現状調査を行った．

3.3.2 アンケート調査の概要

アンケート調査の実施概要は次のとおりである．

2014 年 8 月に「情報セキュリティ調査」アンケートを郵送で実施した．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%（437 組織）であった．

3.3.3 組織内におけるヒヤリ・ハット収集状況

組織内でヒューマンエラーによるヒヤリ・ハット情報（アンケートでは，人的ミスによる事故・トラブルの情報とした）を集めているか，また，どのような種別の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 4** に示す．

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，調査した項目それぞれで，約 40%の組織が情報収集していることが分かった．さらに，「何かしらの情報を集めている」組織は，図 4 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にあたる 321 組織（約 73%）であった．以上のことから，情報セキュリティ分野におけるヒヤリ・ハット情報を集めている組織が存在していることは確認できた．

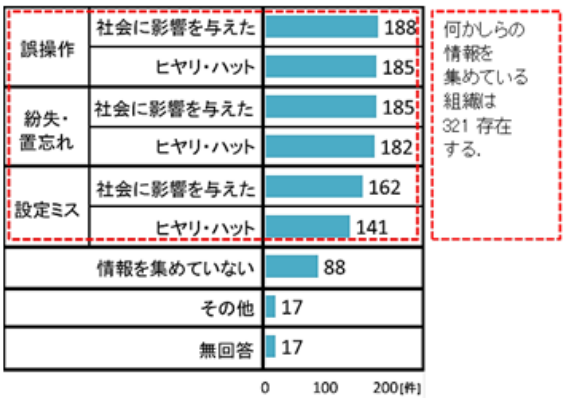


図 4 人的ミスの情報収集状況（$n = 437$，複数選択）

Fig. 4 The collection situation of the human miss information.

3.3.4　第三者機関へ提供する場合の条件

「国などによりガイドラインが示され，ヒヤリ・ハット情報の収集・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」と前提をおいたうえで，どのような条件が整えばヒヤリ・ハット情報を第三者機関に提供するか調査した．調査結果を**図 5** に示す．

調査の結果，「収集目的が明示されている」が 241 組織（約 55%）と一番多かった．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」161 組織（約 37%）が入った．これらは，第三者機関を信頼するための条件とみることもできる．また，3 番目には「報告に手間がかからない」ことが入り，178 組織（約 41%）であった．

一方，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」などを求める組織が存在することから，実際に取り組みが行われた際には，条件があえば，自組織のヒヤリ・ハット情報を第三者機関に提供する意思がある組織が一定以上存在すると考えられる．

3.3.5　アンケート調査の結果

情報セキュリティ分野において「一部の組織がヒヤリ・ハット情報の収集を行っていること」，「条件によっては，ヒヤリ・ハット情報を第三者機関に提供する意思がある」ということが分かった．これは，Reason のいう「報告する文化（Reporting Culture）」が成立していると見なせる [18]．このことから，情報セキュリティ分野においても，航空や医療の分野と同様にヒヤリ・ハット情報収集の体制を導入できると考えられる．

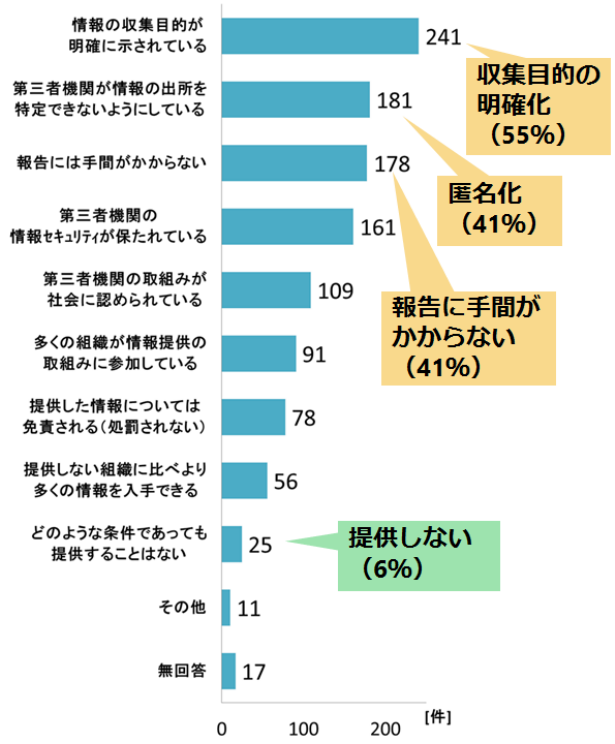


図 5　第三者機関への提供条件（$n = 437$，3 つ選択）

Fig. 5　Offer condition to the third party.

4.　情報セキュリティ分野におけるヒヤリ・ハット情報収集の体制の提案

4.1　提案する事例収集の体制

情報セキュリティ分野におけるヒヤリ・ハット情報の収集体制の概念図を他分野のヒヤリ・ハット情報の収集体制や 3.3 節のアンケート調査結果をもとに，**図 6** に示す．

基本的な収集体制については Reason の報告する文化が共通することから，2.3 節で述べた，航空分野の VOICES の収集体制が参考となる．また，ほかの分野では航空分野を参考にしていることもあげられる [18]．なお，VOICES と異なる点は，第三者機関による報告システムの提供と外部研究機関[*5]の分析・検討への参画を追加した点である．

なお，情報セキュリティ分野における情報共有例としては，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情報処理推進機構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）がある．J-CSIP は，いわゆる「やりとり型」といわれる攻撃の分析を行ったうえで，その情報を参加組織と共有するといった実績をあげている [19]．本稿は，この活動を試行的にヒューマンエラーへ拡充することを提案し，その活動結果をもって評価検討したいと考えている．

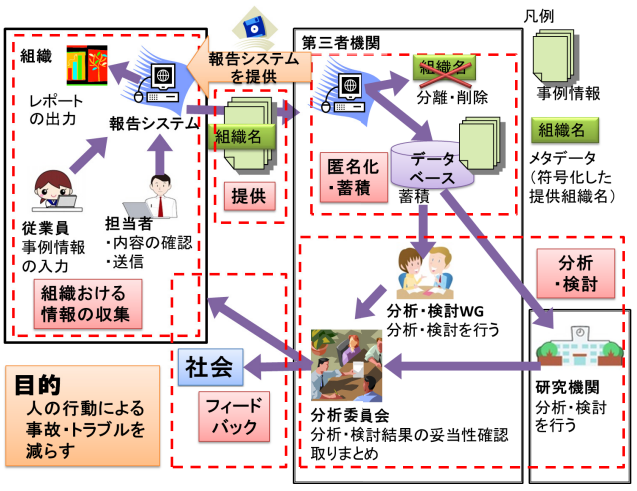


図 6　提案する事例収集体制の概念図

Fig. 6　Suggest for the collection system.

[*5] 大学の付属研究機関などを想定．

4.2 VOICES との相違点およびその理由

4.2.1 第三機関による報告システムの提供

第三者機関がヒヤリ・ハット情報を効率的に収集する場合，報告項目やフォーマットの標準を定めた方が良いと考える．この理由は，現時点でヒヤリ・ハット情報を集めていない組織が，新たにヒヤリ・ハット情報の収集を始める場合，一から組織内の制度や報告フォーマットを作製するのは手間となる．すなわち，新たにヒヤリ・ハット情報収集を始める組織を支援するために，すぐに使える標準的な報告フォーマットが役立つと考える．

さらに，保育園のヒヤリ・ハット情報収集 [9] では，第三者機関がヒヤリ・ハット報告システムを構築し，組織に利用させている．ヒヤリ・ハット報告システムを使えば，だれでも気軽に統一のフォーマットに沿った内容を入力することができる．

情報セキュリティ分野でもこのような取り組みを導入すると，入力しやすくなり提供しやすい環境となる．作成する情報セキュリティ分野のヒヤリ・ハット報告システム（以下，報告システムと略す）には，従業員による事例情報の入力機能，組織の担当者による入力内容の確認機能，第三者機関へのヒヤリ・ハット情報の提供機能，組織内のヒヤリ・ハット情報のレポート作成機能が必要になると考える．

標準化されツールが利用できる報告システムにより，従業員は気軽に事例情報を入力でき，ヒヤリ・ハット情報を報告しやすい環境を作ることができる．また，組織から第三者機関に提供する前には，組織の担当者は報告の中に自組織の特定につながるような情報が含まれていないことを確認する作業を行う必要がある．この作業は，組織に対して負担をかけていることになるので，何らかの補償を行わなければならないと考える．補償の 1 つとしては，入力された組織内のヒヤリ・ハット情報の統計といったレポートを作成出力する機能を報告システムにより提供するなどが考えられる．本稿 3.1.2 項で述べた情報セキュリティガバナンスのモニタに活用できる情報を組織に提供するのが良いのではないかと考える．

4.2.2 研究機関の分析・検討への参画

提案する収集体制では，第三者機関が蓄積した事例情報は，第三者機関だけでなく大学など外部の研究機関にも公開することを想定している．その理由は，情報システムは幅広い業種で活用されており，様々な観点から分析・検討を行わなければならないためである．航空や医療などの専門分野と比べても，情報処理学会がカバーする領域や範囲が広いことからも，同じようにして専門家を集めるだけでは，十分ではないと考える．また，事例情報が研究機関に公開されれば，実際に近い情報を用いて情報セキュリティ事故の対策について研究が広がり，その成果や新しい知見が集積されることが期待される．

5. まとめ

本稿では，ヒューマンエラー対策の 1 つとして，複数の分野でヒヤリ・ハット情報収集が行われていることを確認した．情報セキュリティ分野においても，事故を未然に防ぐ観点からヒヤリ・ハット情報収集が必要であること，さらに企業に対するアンケート調査により，ヒヤリ・ハット情報の収集の必要性や期待などから，実現可能性が高いことを示した．最後に，先行事例およびアンケートで得た知見をもとに Reason のいう報告する文化の具体的な展開として，情報セキュリティ分野におけるヒヤリ・ハット情報収集の体制を提案した．

本稿では，ヒヤリ・ハット情報収集の仕組みについて検討し，具体的にどのような種類のヒヤリ・ハット情報を収集するかについては述べていない．これについての検討が残されている．また，実際に情報セキュリティ分野におけるヒヤリ・ハット情報収集のトライアル実験を行い，期待するヒヤリ・ハット情報が収集されるか，情報が集積されるかなどの検証が必要と考える．

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など関係者，原田研究室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いただいた企業や団体・組織の皆様，アンケートのデータ入力に多大な協力をいただ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] 特定非営利活動法人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 (2014).

[2] 佐藤亮太，間形文彦，高橋克巳，桑名栄二：情報セキュリティの失敗事例における原因の類型化とその対策に関する考察，情報処理，Vol.54, No.9, pp.2208–2219 (2013).

[3] 井上威恭（監修）：ハインリッヒ産業災害防止論，海文堂 (1982).

[4] 国土交通省航空局：航空安全プログラム，国土交通省（オンライン），入手先 ⟨http://www.mlit.go.jp/common/001033880.pdf⟩（参照 2014-10-10）.

[5] 公益財団法人航空輸送技術研究センター：航空安全情報自発報告制度 [VOICES]—ご利用の手引き，航空安全情報自発報告制度（オンライン），入手先 ⟨http://www.jihatsu.jp/share/docs/manual.pdf⟩（参照 2015-02-26）.

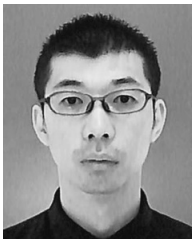
[6] 厚生労働省：主な医療安全関連の経緯，厚生労働省（オンライン），入手先 ⟨http://www.mhlw.go.jp/topics/bukyoku/isei/i-anzen/keii/⟩（参照 2015-01-07）.

[7] 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, pp.2–5 (2012).

[8] 全日本トラック協会：ドライブレコーダ映像を活用したヒヤリハット集，ドライブレコーダ映像を活用したヒヤリハット集（オンライン），入手先 ⟨http://www.jta-hiyari.jp/⟩（参照 2014-12-31）.

[9] 一般財団法人日本保育園保健協議会：保育所・保育園

及び認定こども園における事故予防と安全対策，一般財団法人日本保育園保健協議会（オンライン），入手先 ⟨http://www.nhhk.net/incident/index.html⟩（参照 2014-12-31）．
[10] 東京消防庁：消防ヒヤリハットデータベースとは，入手先 ⟨http://open.fdma.go.jp/hiyarihatto/about/index.html⟩（参照 2014-12-31）．
[11] 京都大学環境安全保健機構：ヒヤリハット事例のオンライン報告，京都大学環境安全保健機構（オンライン），入手先 ⟨http://www.esho.kyoto-u.ac.jp/report/⟩（参照 2014-12-31）．
[12] 三重大学：ヒヤリハット報告について，三重大学（オンライン），入手先 ⟨http://www.mie-u.ac.jp/students/attention/post-2.html⟩（参照 2014-12-31）．
[13] 嘉幡久敬：ライフラインの制御システムサイバー対策欠陥深刻，朝日新聞 2015 年 2 月 16 日朝刊，p.3 (2015).
[14] 朝日新聞：逗子市の端末共有状態，朝日新聞 2013 年 11 月 8 日朝刊，p.38 (2013).
[15] JIS Q 27014:2015，情報技術—セキュリティ技術—情報セキュリティガバナンス (2015).
[16] ファーストサーバ：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，ファーストサーバ（オンライン），入手先 ⟨http://support.fsv.jp/urgent/fs-report.html⟩（参照 2015-02-26）．
[17] 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，pp.81–83, 日経 BP 社 (2014).
[18] ジェームズ・リーズン：組織事故　起こるべくして起こる事故からの脱出，日科技連出版社 (1999).
[19] 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，情報処理推進機構（オンライン），入手先 ⟨http://www.ipa.go.jp/files/000039231.pdf⟩（参照 2014-10-10）．



佐々木 崇裕

2005 年海上保安大学校卒業．2015 年情報セキュリティ大学院大学博士前期課程セキュリティ専攻修了．同年より情報セキュリティ大学院大学客員研究員として情報セキュリティの研究に従事．

原田 要之助　（正会員）

1979 年京都大学大学院工学研究科数理工学専攻を修了，電信電話公社（現，NTT）の研究所を経て，2010 年から情報セキュリティ大学院大学教授．リスクマネジメント・情報セキュリティマネジメントを担当．