調査報告書

人的エラーによる情報漏洩事故とその防止策に関する研究

2009 年 3 月

中央大学理工学部経営システム工学科

大室　巧・早乙女　慧

目次

謝辞

本研究を進めるに当たり、貴重な時間を割き、調査に御協力下さいました情報セキュリティマネジメントシステム管理責任者の方々にこの場をお借りして、心より厚く御礼申し上げます。

要　旨

人的エラーによる情報漏洩事故とその防止策に関する研究

中央大学理工学部経営システム工学科
大室　巧・早乙女　慧

1. 研究目的

近年高度化する社会において、情報漏洩事故の件数は年々増加する傾向にある。これらの事故を調べてみると、度忘れ、見間違いなどの人の意図しないエラーによるものが多い。

本研究では、企業・組織が行っている意図しないエラーの防止対策の分析を行い、情報漏洩事故を防止するためにはどのようにしたらよいか明らかにすることを目的とする。

2. 情報漏洩事故の事例分析

過去の情報漏洩事故の事例を１００件調査し、どのような原因で起こったのかを分析した〔2〕。結果を図１に示す。

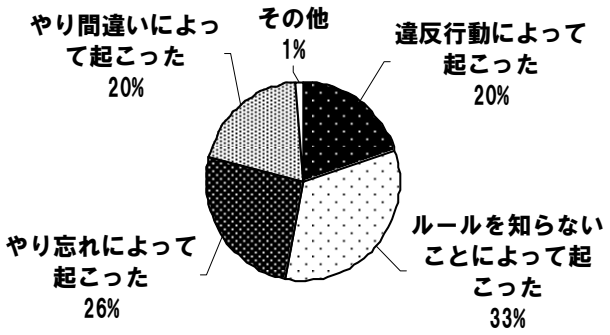

図１　各事故原因の割合

図１より以下のことが分かった。

（1）事故要因は大きく４つに分けられる。

（2）意図しないエラー、すなわちセキュリティに関するルールを知っており、守るつもりでいながら、ついうっかり度忘れ、見間違い、聞き違い、勘違いしたことが原因の事例が多い。

（3）セキュリティに関するルールを知らないことに起因するものも多い。

3. ISMS 認証企業に対する調査

ISMS 認証企業の中で所在地が東京都内である企業の中から無作為に抽出した２００社にアンケートを郵送し、調査を行った（回答社数９社)。調査項目は以下の５項目である。

（1）ISMS がカバーしている業務内容

（2）情報漏洩事故の発生の状況

（3）情報を取り扱う作業における意図しないエラーの発生の有無及び防止対策の実施状況

（4）対策を推進するための組織の取り組み（意図しないエラーに関する情報の収集・分析、リスク予測、対策案の作成・選定・実施）

（5）意図しないエラー以外の原因による情報漏洩事故を防止するための取り組み

なお、（3）では、過去に発生した情報漏洩事故の事例を基に、業務別（情報を受け取る、情報を処理する、情報システムを運用・管理するなど）に起こりうるエラーを示し各々のエラーの発生率を４段階で聞いた。また、対策については、エラープルーフ化の原理〔1〕を用いて作成し、各々の対策を行っているかどうかを聞いた。

4. 意図しないエラーの発生状況と対策の実施状況

得られたアンケートの回答を基に、業務別のエラーの発生率及び行われている対策の現状について以下の３項目に分けて解析を行った。

a)エラー発生率

過去５年間によく発生したもの（◎）を３点、まれに発生したもの（○）を２点、発生していないが起こりそうなもの（△）を１点とし、エラーごと、業務ごとに平均を求めた。

b)対策の実施率

対策の実施率を、対策ごと、意図しないエラーごと、業務ごとに求めた。

c)対策を行うための組織としての活動の把握

①誰が、②どのような頻度で、③どのような方法で対策を推進する取り組みを行っているかを表にまとめ、類似の回答をグルーピングし、集計を行った。

表１　意図しないエラーの発生率（一部）

業務	エラー発生率	意図しないエラー	エラー発生率
情報システムを運用･管理する	0.88	不要になったアカウントの削除を忘れる	1.38
情報を受け取る	0.57	個人情報を含む書類･媒体･PC などを移動中に置き忘れる	1.5
情報を保管する	1.14	破棄すべき書類･媒体･PC などを放置する	0.71
情報を破棄する	0.71	ウイルスメールなどを気づかずに開いてしまう	0.57
情報を処理する	0.67	情報を送る相手先を間違える	1.29

表２　行われている対策（一部）

業務	対策の実施率	意図しないエラー	対策の実施率
情報システムを運用･管理する	23%	不要になったアカウントの削除を忘れる	25%
情報を受け取る	42%	破棄すべき書類･媒体･PC などを放置する	15%
情報を保管する	5%	個人情報を含む書類･媒体･PC などを移動中に置き忘れる	5%
情報を破棄する	9%	ウイルスメールなどを気づかずに開いてしまう	42%
情報を処理する	13%	情報を送る相手先を間違える	17%

得られた結果の一部を表１と表２に示す。この解析より以下のことが分かった。

（１）１社を除いて、取り上げた業務が全て行われている。

（２）取り上げた意図しないエラーの内７５％で実際にエラーが発生している。

（３）業務の種類によってエラーの発生率が異なり、「情報を保管・管理する」におけるエラーの発生率が最も高く、「情報を受け取る」におけるエラーの発生率が最も低い。

（４）同じ業務でも意図しないエラーの発生率はエラーごとに様々である。「情報を保管する」という業務の中でも「秘密にすべき情報を一般の情報を保管する場所に誤って保管する」というエラーが最も発生率が高い（５０％）。

（５）対策が行われている業務とされていない業務がはっきりしている。「情報を受け取る」における対策の実施率が最も高く、「情報を持ち出す」における対策の実施率が最も低い。

（６）エラーの発生率と対策の実施率の関係については、①発生率が高く、実施率が高い、②発生率が低く、実施率が高い、③発生率が高く、実施率が低いの３つに分けられる。③の例としては「個人情報を含む書類･媒体･PC などを移動中に置き忘れる」エラーがある。

（７）情報の収集に関しては、部門関係者が発生時に報告書形式で行い、情報の分析に関しては、セキュリティ関係者が発生時に報告書形式で行うのがよい。また、リスクの予測・評価に関しては、部門関係者が決められた時期ごとに報告書形式または会議・委員会形式で行い、対策の作成・選択・実施に関しては、ＩＳＭＳ関係者が決められた時期ごとに報告書形式で行うのがよい。さらに、効果の確認に関しては、内部監査員が決められた時期ごとに報告書形式で行うのがよい。

５. 結論と今後の課題

多くの業務において、意図しないエラーによる情報漏洩の危険が少なからずあること、エラーの発生頻度が高いにも関わらず、対策の実施率が低いものがあることがわかった。

今後の課題としては、発生しやすいエラーに対する対策を組織的に推進する方法を明らかにし、情報漏洩事故の未然防止に繋げていくことが残されている。

参考文献

［1］中條武志，尾辻正則，松倉辰雄：ポカミス防止実践マニュアルー実務に役立つシリーズー，品質月刊委員会

［2］IT 保険ドットコム：個人情報漏洩事件一覧，(http://www.it-hoken.com/cat_aeieoieioeie.html)

第１章
研究目的

１．研究目的

近年高度化する情報化社会において、情報漏洩事故が頻繁に発生している。企業・組織の扱う情報には様々なものが含まれており、中には許可された者以外の目に触れない状態に保持することが求められるものもある。仮に、これらの情報が外部に漏れた場合、社会的な信用の低下だけでなく、顧客等の実際の不利益につながる恐れもあり、万全の対策を講じなくてはならない。

本研究では、情報の操作や情報システムの管理に携わる人の意図しないエラーを防ぐための対策を行うことが、情報漏洩事故の件数を減らす上で不可欠であると考え、企業・組織が行っている意図しないエラーの防止対策、その推進のための活動の現状の調査・分析を行い、意図しないエラーによる情報漏洩事故を防止するにはどうしたらよいかについて明らかにすることを目的とする。

第２章
情報漏洩事故の事例調査

２．情報漏洩事故の事例調査

過去にどのような情報漏洩事件が発生しているかについて把握するために、発生した情報漏洩事故１００件を調査した〔2〕。各々の事故について、企業名、発生日、原因、流出内容、被害人数、影響度などについてまとめた。なお、情報漏洩事故の原因及び情報漏洩の被害は以下のように分類した。

Ａ．情報漏洩事故の原因コード

（1）意図的な不遵守が原因で起こった

・悪意のある違反行為によって起こった

・悪意のない違反行為によって起こった

（2）ルールを知らないことによって起こった

（3）意図しないエラーによって起こった

・やり忘れによって起こった

・やり間違いによって起こった

Ｂ．情報漏洩事故の被害の影響度

（1）９９９９９人～

（2）９９９９人～１０００人

（3）９９９人～１００人

（4）～９９人

ただし、「意図しないエラー」「ルールを知らなかった」「意図的な不遵守」「セキュリティに関するルールが不十分・間違っていた」については、それぞれ以下のように定義した。

（1）**意図しないエラー**：セキュリティに関するルールを知っており、守るつもりでいながら、ついうっかり度忘れ、見間違い、聞き違い、勘違いした。

（2）**ルールを知らなかった**：新人、交代者、応援者等のために職場で設定されたセキュリティに関するルールを守らなかった。

（3）**意図的な不遵守**：セキュリティに関するルールを知っていたにも関わらず、急いでいた、面倒などの理由で意図的にルールを守らなかった。

（4）**セキュリティに関するルールが不十分・間違っていた**：セキュリティに関するルールは守られていたが、事故・未遂事故が発生した。

表２．１に原因コードと被害の影響度のクロス集計表を示す。また、図２．１に原因コードによる事故の比率を示す。これらの図表より以下のことが分かる。

（1）影響度が 9999 人以下の情報漏洩事故が頻繁に発生している。

（2）ルールを知らなかったことによることが原因で、影響が 99 人以下である情報漏洩事故が最も発生している。(14 件)

（3）やり忘れによって発生した、やり間違いなどの意図しないエラーにより発生した事故が約５０％を占めている。

（4）悪意のある違反行為によって発生した事故はほとんど発生していない。

（5）被害人数の多い事故の原因は、主に悪意のない違反行為によって起こったもの、ルールを知らなかったことによって起こったものの 2 つに集中している。

表２．１　情報漏洩事故の原因コードと影響度のクロス表

	99 人以下	999 人～100 人	9999 人～1000 人	99999 人以上	不明	合計
悪意のある違反行動によって起こった	1	0	0	0	0	1
悪意のない違反行為のよって起こった	3	7	7	2	4	23
ルールを知らないことによって起こった	14	3	7	0	3	27
やり忘れによって起こった	13	7	1	5	1	27
やり間違いによって起こった	7	4	4	1	5	21
その他	1	0	0	0	0	1
合計	39	21	19	8	13	100

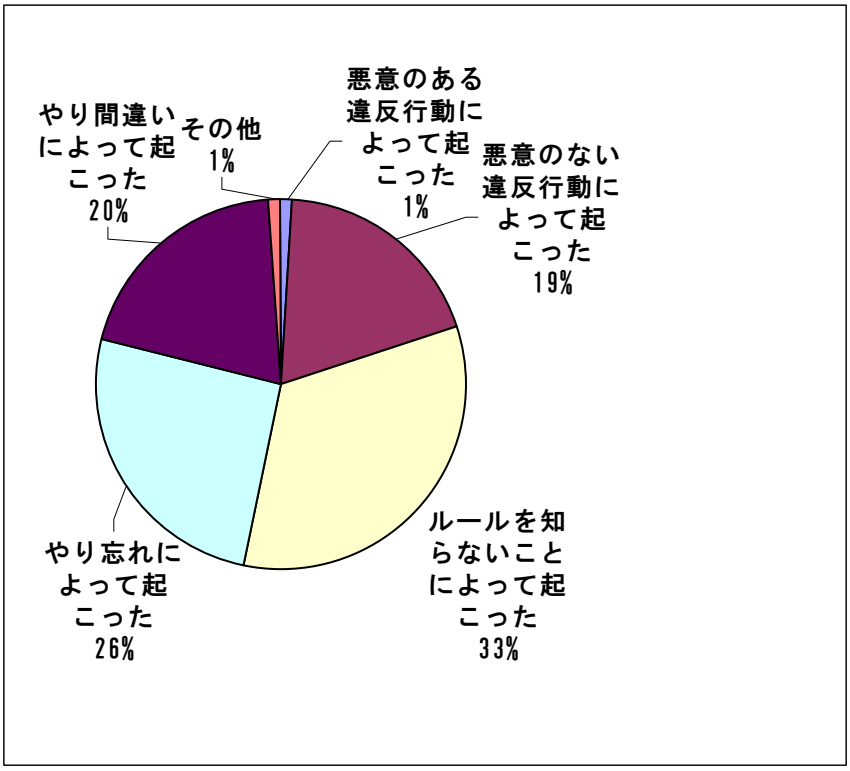

図２．１　情報漏洩事故の原因コード別比率

第３章
意図しないエラーに対する対策の考案

３．意図しないエラーに対する対策の考案

３．１　作業の分類

実際の職場で行われている、主に情報を取り扱う作業を、２章で調査した過去の事故事例を基に分類した。結果を表３．１に示す。

表３．１　情報を取り扱う主な作業

	情報を取り扱う業務	作業例
1	情報を送る	メールを送信する
2	情報を持ち出す	USB メモリなどに保存し、持ち出す
3	情報を保管する	書類を保管する
4	情報を処理する	書類を分類し保管する
5	情報を受け取る	メールを受信する
6	情報を持ち込む	外部から、USB メモリなどに保存した情報を持ち込む
7	情報を破棄する	書類などを破棄する
8	情報システムを運用・管理する	会員のアカウント情報などを管理する

３．２　起こりうるエラーの選定

表３．１の８つの作業ごとに、実際に発生し得るエラーを、2 章で調査した過去の事故事例を基に、考案した。結果を表３．２に示す。

表３．２　各作業における起こり得るエラー

業務	起こり得る意図しないエラー
情報を送る	送る情報の中に個人情報が含まれていることに気付かない
	情報を送る相手先を間違える
	送り先の住所変更・アドレス変更を見逃し、違う送り先に送付してしまう
	送信方法を間違える（メールで bcc にせずに送信してしまうなど）
情報を受け取る	ウイルスメールなどを気づかずに開くことにより、情報が流出してしまう
情報を持ち出す	作業後に回収すべき書類・媒体・PC などを、回収し忘れてしまう
	作業中に個人情報を含む書類・媒体・PC などから目を離してしまう
	移動中に個人情報を含む書類・媒体・PC などを置き忘れてしまう
	個人情報の入った過般型情報媒体などを使用後、うっかり持って帰ってしまう
情報を持ち込む	持ち込む際にウイルスなどの感染チェックを忘れる
情報を受け取る	施錠を忘れることにより、情報が誰の手にも渡る状況にしてしまう
	秘密にすべき情報を、一般の情報を保管する場所に誤って保管する
情報を破棄する	破棄すべき書類・媒体・PC などを放置する
	不要書類・媒体・PC などの破棄を行う際に秘密にすべき情報の処置を忘れる
情報を処理する	重要な情報の暗号化を行い忘れる
	フォルダやファイルを間違える
	セキュリティの確保されていないPC（P2P ソフトなど）とは気づかずに使用する
情報を運用・管理する	セキュリティソフト等のアップデートをし忘れる
	不要になったアカウントの削除を忘れる
	ホームページの設定を間違えて、情報の閲覧が可能になってしまう

３．３　エラー対策の列挙

表３．２で整理した２０の意図しないエラーに対する対策を、エラープルーフ化の原理[１]を用いて、考案した。なお、エラープルーフ化とは、意図しないエラーを防止するための作業方法（機器、手順、帳票、情報など）の工夫であり、エラープルーフ化の原理はこのような工夫を行うための基本的な考え方を整理したものである。エラープルーフ化の原理を表３．３に示す。

表３．３　エラープルーフ化の原理

排除	作業の必要になる条件や作業に付随する危険を取り除き、エラーしやすい作業や注意を不要にする
代替化	人の手によって行わなければならない作業の中で、エラーの起こりやすいものを機械等に置き換える
容易化	人の手による作業を確実に行えるように、作業を人のやりやすい、容易なものにする
異常検出	エラーに起因する異常が引き続くプロセス中に発見され、是正措置がとられるようにする
影響緩和	作業を並列化したり、制限や保護を設けることで、エラーの影響を緩和・吸収するようにする

表３．２に示した各エラーに表３．３のエラープルーフ化の原理を当てはめ、それぞれの原理に対応する対策を考案した。結果の一部を表３．４に示す。なお、考案した対策の全容については、巻末に添付する。

表３．４　意図しないエラーに対する対策（一部）

意図しないエラー	エラープルーフ化の原理	エラー対策
送る情報の中に個人情報が含まれていることに気付かない	排除	個人情報の入っている書類・媒体・ファイルを送らない
	代替化	送る情報の作成を人手によらず、コンピュータで一括して行う
	容易化	色などを用いて個人情報であることが明確になるようにする
	容易化	個人情報とそうでない情報を分けて保管する
	異常検出	送る情報を自動的にチェックし、個人情報が含まれていると警
	影響緩和	第三者が見ても個人情報であることがすぐに分からないように
	影響緩和	送った情報が着信側で一定期間後に自動的に削除されるよう

第４章
ＩＳＭＳ認証企業に対する調査の計画と実施

４．ＩＳＭＳ認証企業に対する調査の計画と実施

４．１　調査の計画と実施

ＩＳＭＳ（情報セキュリティマネジメントシステム）認証企業の中から、所在地が東京都または埼玉県内に属する２００社を選び、郵送調査を行った。アンケート項目は以下の５項目である。なお、今回の調査で用いた調査票は巻末に添付する。

（１）ＩＳＭＳがカバーしている主な業務内容、また当該業務に関わっている従業員構成。業務内容については、こちらでリストアップした業種の中から選択式で回答してもらった。従業員構成については、主な従業員数と、それを構成する正社員、パート・アルバイト・派遣社員の割合を 10 パーセント刻みで回答してもらった。

（２）ＩＳＭＳがカバーしている業務内での情報漏洩事故および情報漏洩の未遂事故の発生経験の有無とそれぞれの原因比率。情報漏洩事故や情報漏洩の未遂事故の経験があるのかどうか、それらが発生した原因（意図しないエラー、ルールを知らなかった、意図的な不遵守、セキュリティに関するルールが不十分・間違っていたなど）がどのくらいの割合かについて回答してもらった。

（３）ＩＳＭＳがカバーする業務の内容と意図しないエラーの発生状況。表３．１で挙げた業務が含まれているかどうか、表３．２で挙げた意図しないエラーがどのような頻度で発生しているか回答してもらった。頻度については、過去５年間によく発生したものに◎、まれに発生したものに○、発生していないが起こりそうなものに△を付けてもらった。

（４）意図しないエラーに対する対策の実施状況。表３．４で挙げた意図しないエラーの対策としてどの対策が行われているのか、さらに挙げた対策の他にどのような対策が行われているのか、について調査した。意図しないエラーに対する対策を一覧表にし、その中で該当するものに○を点けてもらう形で回答してもらった。

（５）意図しないエラーに対する対策を推進するための組織の取り組み。意図しないエラーに関する情報の収集・分析、リスク予測、対策案の作成・選定・実施のそれぞれについて、「誰が」「どのくらいの頻度で」「どのような方法で」という項目に分けて、自由書式で回答してもらった。

（６）意図しないエラー以外の原因に対する取り組み。意図的な不遵守やルールを知らなかったことが原因で起こる情報漏洩事故を防ぐために、どのような取り組みを行っているかについて自由書式で回答してもらった

４．２　回答企業の概要

調査に回答いただいた企業は全部で１９社であった（回収率 9.5%）。図４．１および図４．２に、回答いただいた企業の ISMS がカバーする事業（業種）と当該 ISMS にかかわる従業員数（規模）について示す。これらの図より以下のことが分かった。

（１）情報・システム業から最も多くの回答が得られたが、ソフトウェア業、マーケティング業、販売業、サービス業、コンサルティング業、金融業などの様々な業種からの回答が得られた。

（２）ISMS に関わる従業員数は１００人以下のところが多い。

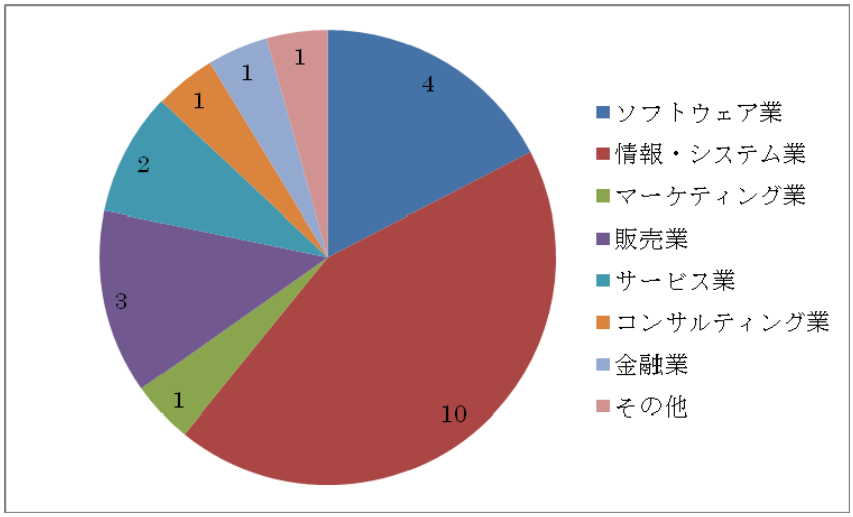

図４．１　回答企業の ISMS がカバーする事業（業種）

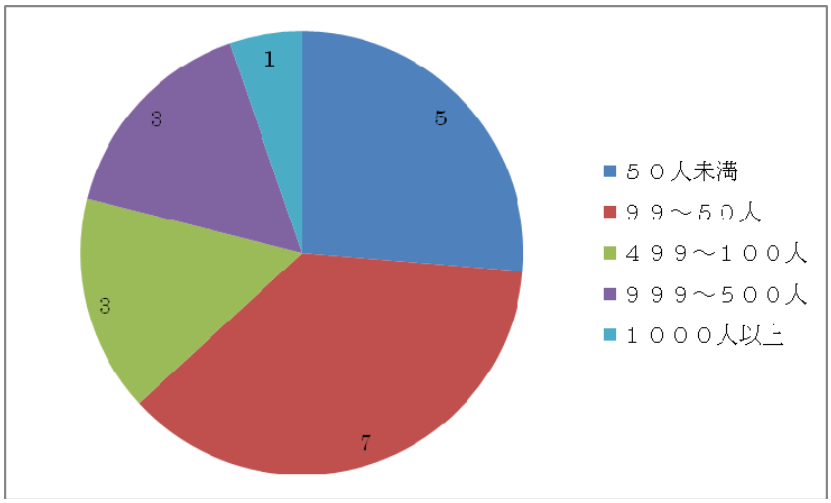

図４．２　回答企業の ISMS にかかわる従業員数（規模）

第５章
意図しないエラーの発生状況

５．意図しないエラーの発生状況

どのような意図しないエラーが発生しやすいかについての調査結果を表５．１に示す。なお、発生度に関しては、過去５年間によく発生したもの（◎）を３点、まれに発生したもの（○）を２点、発生していないが起こりそうなもの（△）を１点とし、エラーごと、業務ごとに平均を求めた。この表から以下のことが分かった。

（１）多少のバラつきはあるが、いずれの意図しないエラーも発生している。

（２）発生度でみると、「情報を送る相手を間違える」が最も大きい。「秘密にすべき情報を、一般の情報を保管する場所に誤って保管する」「不要になったアカウントの削除を忘れる」「移動中に個人情報を含む書類・媒体・PC などを置き忘れてしまう」も多く発生している。

（３）「ウイルスメールを気付かずに開くことにより、情報が流出してしまう」という意図しないエラーは実際の発生は少ないものの、起こりやすそうなものとして多くの企業が挙げられている。

（４）業務ごとの平均で見ると「情報を保管する」という業務が最もエラーの発生度率が高い。

表５．１　業務ごとの意図しないエラーの発生度

業務	意図しないエラー	◎	○	△	平均	平均
情報を送る	送る情報の中に個人情報が含まれていることに気付かない	0	4	8	1.00	1.13
	情報を送る相手先を間違える	1	9	5	1.53	
	送り先の住所変更・アドレス変更を見逃し、違う送り先に送付してしまう	1	4	7	1.00	
	送信方法を間違える（メールで bcc にせずに送信してしまうなど）	0	4	8	1.00	
情報を受け取る	ウイルスメールなどを気づかずに開くことにより、情報が流出してしまう	1	1	10	0.87	0.87
情報を持ち出す	作業後に回収すべき書類・媒体・PC などを、回収し忘れてしまう	0	1	6	0.73	1.07
	作業中に個人情報を含む書類・媒体・PC などから目を離してしまう	0	3	6	1.00	
	移動中に個人情報を含む書類・媒体・PC などを置き忘れてしまう	0	6	6	1.45	
	個人情報の入った過般型情報媒体などを使用後、うっかり持って帰ってしまう	0	4	5	1.09	
情報を持ち込む	持ち込む際にウイルスなどの感染チェックを忘れる	1	0	9	0.79	0.79
情報を保管する	施錠を忘れることにより、情報が誰の手にも渡る状況にしてしまう	2	3	8	1.29	1.39
	秘密にすべき情報を、一般の情報を保管する場所に誤って保管する	0	7	7	1.50	
情報を破棄する	破棄すべき書類・媒体・PC などを放置する	2	0	9	1.00	0.89
	不要書類・媒体・PC などの破棄を行う際に秘密にすべき情報の処置を忘れる	0	2	9	0.79	
情報を処理する	重要な情報の暗号化を行い忘れる	0	1	8	0.60	0.76
	フォルダやファイルを間違える	1	3	8	1.07	
	セキュリティの確保されていないＰＣ（P2P ソフトなど）とは気づかずに使用する	0	2	5	0.60	
情報システムを運用・管理する	セキュリティソフト等のアップデートをし忘れる	0	3	8	0.88	0.88
	不要になったアカウントの削除を忘れる	3	3	7	1.38	
	ホームページの設定を間違えて、情報の閲覧が可能になってしまう	0	0	6	0.38	

第６章
エラー対策の実施状況

６．エラー対策の実施状況

６．１　「情報を送る」業務に関するエラー対策の実施率

「情報を送る」業務に関して、どのようなエラー対策が実施されているかについての調査結果をまとめたものを表６．１に示す。なお、実施率に関しては、実施している場合（○）を１点、実施していない場合を０点とし、エラー防止策ごと、エラーごとに平均を求めた。この表から以下のことが分かった。

（１）「情報を送る」業務の中で起こり得る意図しないエラーに対する、エラー対策の実施率は約２０％である。

（２）「情報を送る相手先を間違える」、「送り先の住所変更・アドレス変更を見逃し、違う送り先に送付してしまう」、「**送る情報の中に個人情報が含まれていることに気付かない**」エラーに対する対策の実施率は、「送信方法を間違える」エラーに対する対策の実施率に比べて高い。

（３）「個人情報の入っている書類・媒体・ファイルを送らない」「個人情報とそうでない情報を分けて保管する」「中身を暗号化し、第三者に分からないようにする」対策は半分近い企業で行われている。

表６．１　「情報を送る」業務に関するエラー対策の実施率

業務	意図しないエラー	エラー対策	実施率	エラーごとの実施率	業務ごとのの実施率
情報を送る	送る情報の中に個人情報が含まれていることに気付かない	個人情報の入っている書類・媒体・ファイルを送らない	62.50%	19.60%	17.10%
		送る情報の作成を人手によらず、コンピュータで一括して行う	0%		
		色などを用いて個人情報であることが明確になるようにする	0%		
		個人情報とそうでない情報を分けて保管する	56.30%		
		送る情報を自動的にチェックし、個人情報が含まれていると警告する	0%		
		第三者が見ても個人情報であることがすぐに分からないようにする	18.80%		
		送った情報が着信側で一定期間後に自動的に削除されるようにする	0%		
	情報を送る相手先を間違える	個人情報を郵送・ＦＡＸ・メール等で送らない	43.80%	22.90%	
		宛先などを記す・入力する処理を人手によらずコンピュータで行う	6.30%		
		アドレス帳などを誰が見ても分かりやすいものにする	12.50%		
		アドレス帳などで類似の住所・名前が隣同士に並ばないようにする	18.80%		
		送る中身と送り先を自動的にチェックし、異なると警告するようにする	0.00%		
		万一誤っても大丈夫なように、中身を暗号化する	56.30%		
	送り先の住所変更・アドレス変更を見逃し、違う送り先に送付してしまう	個人情報を郵送・ＦＡＸ・メール等で送らない	31.30%	21.30%	
		住所変更・アドレス変更が人手でなく自動的に行われるようにする	0.00%		
		変更の届出があった場合、その場で即座に変更する	25.00%		
		変更の届出とアドレス帳の照合を行わないと送れないようにする	0.00%		
		中身を暗号化し、第三者に分からないようにする	50.00%		
	送信方法を間違える（メールで bcc にせずに送信してしまうなど）	メールを同時送信できないようにする	6.30%	2.50%	
		自動的にＢＣＣで送信されるように設定する	0.00%		
		CC とＢＣＣの入力欄を離し・色分けし、紛らわしくないようにする	6.30%		
		送るべきではない方法を用いた場合、エラー表示が出るようにする	0.00%		
		万一間違っても大丈夫なように、アドレスを一定期間ごとに変更する	0.00%		

６．２　「情報を受け取る」業務に関するエラー対策の実施率

「情報を受け取る」業務に関するエラー対策の実施率を表６．２に示す。この表より、以下のことが分かった。

（１）「情報を受け取る」業務に関するエラー対策の実施率は約５０％であり、高い。

（２）「ウイルスメール等を自動的に検出・処理する」「定期的にウイルスの感染をチェックし、早期に発見する」など、セキュリティソフトなどを用いて自動的に行えるエラー対策は多くの企業で行われている。

表６．２　「情報を受け取る」業務に関するエラー対策の実施率

業務	意図しないエラー	エラー対策	実施率	エラーごとの実施率	業務ごとの実施率
情報を受け取る	ウイルスメールなどを気づかずに、情報が流出してしまう	知らない人からのメールは受け取らない	43.80%	44.80%	44.80%
		ウイルスメール等を自動的に検出・処理するようにする	87.50%		
		知らない人から送られたメールの受信フォルダを分ける	6.30%		
		怪しいメールはセキュリティレベルなどを表示し分かり易くする	6.30%		
		定期的にウイルスの感染をチェックし、早期に発見する	75.00%		
		メールを受け取るＰＣに重要な情報を保管しない	50.00%		

６．３　「情報を持ち出す」業務に関するエラー対策の実施率

「情報を持ち出す」業務に関するエラー対策の実施率を表６．３に示す。この表より、以下のことが分かった。

（１）「情報を受け取る」業務に関するエラー対策の実施率は約１０％であり、低い。

（２）特に、「個人情報の入った過般型情報媒体などを使用後、うっかり持って帰ってしまう」エラーに対するエラー対策の実施率は低い。

（３）情報を持ち出すことを許可している場合は「中身を第三者に読み取られないように暗号化する」ケースが多く、意図しないエラーを防ぐために、「外部に持ち出すことを禁止する」ケースも同程度に行われている。

（４）情報を持ち出す場合の管理は、チェックリストで行われているケースが多い。

表６．３　「情報を持ち出す」業務に関するエラー対策の実施率

業務	意図しないエラー	エラー対策	実施率	エラーごとの実施率	業務ごと実施率
情報を持ち出す	作業後に回収すべき書類・媒体・PC などを、回収し忘れてしまう	個人情報の入った過般型情報媒体などを使用後、うっかり持って帰ってしまう	12.50%	12.50%	11.00%
		必要な情報の送付・回収を自動的に行うようにする	0.00%		
		書類・媒体・PC などをまとめて持ち出す	6.30%		
		書類・媒体・PC を持ち出す際に、社員証などを預ける	6.30%		
		暗号化し、第三者に読み取れないようにする	37.50%		
	作業中に個人情報を含む書類・媒体・PC などから目を離してしまう	仕事の掛け持ちを禁止する	0.00%	16.30%	
		席を立つと自動的に情報がロックされるようにする	43.80%		
		色分けなどで、重要な書類・媒体・PC であることを明確にする	25.00%		
		一定期間放置するとアラームが鳴るようにする	0.00%		
		第三者から見て重要なものと分からないようにする	12.50%		
	移動中に個人情報を含む書類・媒体・PC などを置き忘れてしまう	外部に持ち出しすることを禁止する	37.50%	15.20%	
		情報のやり取りをメール等の機械によって行うようにする	0.00%		
		常に一定の方法で持ち歩く	6.30%		
		カバン等に入れ、別に持たない	25.00%		
		ある一定の距離を離れたらアラームが鳴るようにする	0.00%		
		シンクライアント方式の採用	0.00%		
		暗号化し、第三者に読み取れないようにする	37.50%		
	個人情報の入った過般型情報媒体などを使用後、うっかり持って帰ってしまう	過般型情報媒体の使用禁止	6.30%	8.90%	
		過般型情報媒体を返却する場所・タイミングを標準化する	12.50%		
		携帯していることを認識しやすい形状・大きさにする	0.00%		
		チェックリストを作成し、過般型情報媒体の管理を行う	37.50%		
		過般型情報媒体を会社から持ち出すと、アラームが鳴る	0.00%		
		過般型情報媒体を会社から持ち出すと、アラームが鳴る	6.30%		

６．４　「情報を持ち込む」業務に関するエラー対策の実施率

「情報を持ち込む」業務に関するエラー対策の実施率を表６．４に示す。この表より、以下のことが分かった。

（１）「情報を持ち込む」業務に関するエラー対策の実施率は約２０％である。

（２）ウイルス対策としてセキュリティソフトを導入し、管理しているケースが多く見られる。

（３）人の手による管理はあまり行われていなく、自動的に処理できるようなエラー防止策が多く取られている。

表６．４　「情報を持ち込む」業務に関するエラー対策の実施率

業務	意図しないエラー	エラー対策	実施率	エラーごとの実施率	業務ごと実施率
情報を持ち込む	持ち込む際にウイルスなどの感染チェックを忘れる	外部からのデータを持ち込むことを禁止する	0.00%	20.00%	20.00%
		情報の受信をメールで行い、自動的にチェックする	25.00%		
		出勤時の打刻など、必ず行う作業と一緒に行う	0.00%		
		チェックされていない媒体・ファイルを使用するとアラームが鳴る	0.00%		
		万一持ち込まれても大丈夫なようにウイルス対策を整えておく	75.00%		

６．５　「情報を保管する」業務に関するエラー対策の実施率

「情報を保管する」業務に関するエラー対策の実施率を表６．５に示す。この表より、以下のことが分かった。

（１）「情報を保管する」業務に関するエラー対策の実施率は約２０％である。

（２）多く行われているエラー対策としては「色分けなどで情報と保管場所のセキュリティレベルを明確にする」、「中身を暗号化し、第三者が読み取れないものにしておく」がある。

（３）自動的に防止できるようなシステムは対策として行われていない。

表６．５　「情報を保管する」業務に関するエラー対策の実施率

業務	意図しないエラー	エラー対策	実施率	エラーごとの実施率	業務ごとの実施率
情報を保管する	施錠を忘れることにより、情報が誰の手にも渡る状況にしてしまう	秘密にすべき情報を持たないようにする	18.80%	11.30%	17.00%
		鍵をオートロックにする	0.00%		
		施錠状態をランプ等で知らせる	0.00%		
		施錠を怠った場合、アラームなどで知らせるようにする	6.30%		
		中身を暗号化し、第三者が読み取れないものにしておく	31.30%		
	秘密にすべき情報を、一般の情報を保管する場所に誤って保管する	秘密にすべき情報を持たないようにする	18.80%	21.90%	
		タイプを識別し、適切な場所に自動的に保管されるようにする	18.80%		
		色分けなどで情報と保管場所のセキュリティレベルを明確にする	43.80%		
		秘密にすべき情報は一般の保管場所に入らないようにする	18.80%		
		誤った場所に保管すると、アラームなどが鳴るようにする	0.00%		
		中身を暗号化し、第三者が読み取れないものにしておく	31.30%		

６．６　「情報を破棄する」業務に関するエラー対策の実施率

「情報を破棄する」業務に関するエラー対策の実施率を表６．６に示す。この表より、以下のことが分かった。

（1）「情報を破棄する」業務に関するエラー対策の実施率は約２０％である。

（2）「不要書類・媒体・PC などの破棄を行う際に秘密にすべき情報の処置を忘れる」エラーに対する対策の実施率は低い。

（3）「不要な書類・媒体・ＰＣを持たない」という対策が半数の職場で取られている。

（4）他の業務の対策と同様に、重要な情報は暗号化を用いるという対策が多く取られていて、破棄すべき情報も第三者に読み取られることのないようにされている。

表６．６　「情報を破棄する」業務に関するエラー対策の実施率

業務	意図しないエラー	エラー対策	実施率	エラーごとの実施率	業務ごとの実施率
情報を破棄する	破棄すべき書類・媒体・PC などを放置する	不要な書類・媒体・PC を持たない	50.00%	26.30%	18.10%
		設定した時期が来たら、自動的に破棄されるようにする	6.30%		
		不要になったらすぐに破棄する	43.80%		
		一定期間放置すると、アラームなどで知らせるようにする	0.00%		
		秘密にすべき情報は暗号化して保存するようにする	31.30%		
	不要書類・媒体・PC などの破棄を行う際に秘密にすべき情報の処置を忘れる	廃棄をしない	0.00%	10.00%	
		秘密にすべき情報が含まれていないか自動的にチェックする	0.00%		
		色などで書類・媒体・PC などのセキュリティレベルを明確にする	18.80%		
		処置を忘れて破棄するとアラームなどで知らせるようにする	0.00%		
		秘密にすべき情報は暗号化して保存するようにする	31.30%		

６．７　「情報を処理する」業務に関するエラー対策の実施率

「情報を処理する」業務に関するエラー対策の実施率を表６．７に示す。この表より、以下のことが分かった。

（1）「情報を処理する」業務に関するエラー対策の実施率は約２０％である。

（2）「重要な情報の暗号化を行い忘れる」エラーに対する対策の実施率は低い。

（3）「不要なファイル・フォルダを作成しない」、「セキュリティの確保されていないＰＣを無くす」といった、エラープルーフ化の原理の「排除」に近い対策が多く行われている。

（4）Ｐ２ＰソフトなどがインストールされたＰＣへの対策が多く行われていて、他の意図しないエラーごとの対策に比べ、実施率が高い。

表６．７　「情報を処理する」業務に関するエラー対策の実施率

業務	意図しないエラー	エラー対策	実施率	エラーごとの実施率	業務ごとの実施率
情報を処理する	重要な情報の暗号化を行い忘れる	暗号方式を用いない	0.00%	12.50%	22.10%
		自動的に暗号化が行われるようにしておく	12.50%		
		常に一定のやり方で暗号化するようにする	31.30%		
		暗号化が行われているかどうかが一目でわかるようにする	18.80%		
		暗号化が行われていないとエラー表示されるようにする	6.30%		
		記述の方法を第三者にわかりにくいものにしておく	6.30%		
	フォルダやファイルを間違える	不要なファイル・フォルダを作成しない	50.00%	25.00%	
		ファイルやフォルダの処理を自動化する	6.30%		
		ファイルやフォルダに似た名前をつけない	25.00%		
		間違った操作ができないようにする	12.50%		
		万一間違えても大丈夫なように、暗号化しておく	31.30%		
	セキュリティの確保されていないＰＣ（P2P ソフトなど）とは気づかずに使用する	セキュリティの確保されていないＰＣを無くす	68.80%	29.20%	
		起動・ログイン時にセキュリティレベルを通知する	12.50%		
		個人が使用するＰＣを予め決め、他の人が使わないようにする	43.80%		
		セキュリティレベルをランク付けし、色分けなどで明確にする	18.80%		
		セキュリティレベルの低い PC で情報を操作すると警告がでる	0.00%		
		万一間違えても大丈夫なように、暗号化しておく	31.30%		

６．８　「情報システムを運用・管理する」業務に関するエラー対策の実施率

「情報システムを運用・管理する」業務に関するエラー対策の実施率を表６．８に示す。この表より、以下のことが分かった。

（1）「情報システムを運用・管理する」業務に関するエラー対策の実施率は約３０％であり、高い。

（2）特に「セキュリティソフト等のアップデートをし忘れる」エラーに対する対策の実施率は高い。

（3）セキュリティソフトのアップロードし忘れの対策として、「自動でアップデートされる」という対策が８割以上の職場で行われている。

（4）「不要になったアカウントをすぐに削除する」、「重要な情報はホームページに載せない」といった対策も、他の各対策と比べ、多く実施されている。

表６．８　「情報システムを運用・管理する」業務に関するエラー対策の実施率

業務	意図しないエラー	エラー対策	実施率	エラーごとの実施率	業務ごとの実施率
情報システムを運用・管理する	セキュリティソフト等のアップデートをし忘れる	自動でアップデートされるように設定する	87.50%	43.80%	30.30%
		アップデートの時期を決め、いつも同じ時に行うようにする	25.00%		
		一定期間アップデートされていないと、アラームなどで知らせる	18.80%		
	不要になったアカウントの削除を忘れる	自動でアカウントを削除できるようにする	6.30%	33.80%	
		簡単にアカウントの削除を行えるようにする	25.00%		
		不要になった時にすぐにアカウントを削除する	81.30%		
		アカウントの削除を忘れていると、アラームなどで知らせる	0.00%		
		アカウントの権限をできるだけ制限しておく	56.30%		
	ホームページの設定を間違えて、情報の閲覧が可能になってしまう	ホームページを使用しない	6.30%	18.80%	
		ホームページの設定を自動で行うようにする	0.00%		
		ホームページの設定の手順を単純なものにしておく	12.50%		
		設定が適切でない時に警告で知らせるようにする	6.30%		
		重要な情報はホームページに載せない	68.80%		

６．９　業務ごとのエラー防止策の実施率

業務ごとのエラー防止策の実施率をまとめた結果を表６．９に示す。また、エラープルーフの原理（排除、代替化、容易化、異常検出、影響緩和）ごとのエラー防止策の実施率をまとめた結果を表６．１０に示す。これらの表から以下のことが分かった。

（1）「情報を受け取る」業務で最も多く対策が行われている。「情報を送る」業務に比べ、「情報を受け取る」業務は、数において２倍近い企業で、対策が行われている。

（2）最もエラー対策の実施率が低いのは「情報を持ち出す」業務である。

（3）実施率が最も高い業務でも４４．８％であり、対策率が５０％以上の業務は無かった。

（4）「影響緩和」の対策の実施率が最も高い。

（5）「異常検出」の対策の実施率は他の原理に比べて極端に低い。

表６．９　　業務ごとのエラー対策の実施率

業務	エラー対策の実施率
情報を送る	17.1%
情報を受け取る	44.8%
情報を持ち出す	13.6%
情報を持ち込む	20.0%
情報を保管する	17.0%
情報を破棄する	18.1%
情報を処理する	22.1%
情報システムを運用・管理する	30.3%

表６．１０　エラープルーフの原理ごとのエラー対策の実施率

エラープルーフの原理	実施率
排除	**25.3%**
代替化	**15.5%**
容易化	**23.6%**
異常検出	**6.6%**
影響緩和	**31.5%**

６．１０　エラーの発生度とエラー対策の実施率の関係

意図しないエラー毎の発生度と対策実施率の散布図を図６．１に示す。この図より、エラーの発生度と当該のエラーに対する対策の実施率から見ると、両者の関係は大きく３つにタイプ分けできることが分かった。

（1）エラーの発生度が高く、対応する対策の実施率も高いケース。このケースでは、発生度が高く、対策も多く実施されていることから、各企業で意図しないエラーについて十分に把握しており、対策も防止すべきエラーを的確に捉えた上で行われていると思われる。例えば、「情報の送る相手先を間違える」エラーに対しては、仮に間違えてしまった時のことを想定し、「情報を暗号化して第三者に読み取られないようにする」対策が大半の企業で行われている。このケースでは、完全に起こらないように対策を行うというよりも、起こった場合、被害を最小限に抑えるという抑止策としてのニュアンスが強いように思われる。

（2）エラーの発生率が低く、対応する対策の実施率が高いケース。このケースは、「ウイルスメールに気付かずに開いてしまい、情報が漏洩してしまう」といった意図しないエラーに見られる。このケースは、仮にウイルスにネットワークが感染してしまった場合、被害を受けるのは情報漏洩だけでなく、システム全体に及ぶ可能性がある。仮に、そうなってしまったとするならば、会社の運営全体に危険が及んでしまうと思われる。よって、このケースでは意図しないエラーが発生する前に、未然に防ぐという意味合いが大きいのではないかと推測される。

（3）エラーの発生率が高いにも関わらず、対応する対策の実施率が低いケース。このケースでは、例を挙げると、「情報を保管する」という業務に属する「施錠を忘れることにより、情報が誰の手にも渡る状況にしてしまう」という意図しないエラーは、発生しやすい状況にあるにも関わらず、対策の実施率を他の対策と比較すると、比較的低いことが言える。この状況が最も問題すべき点であり、早急に善処しなくてはならないと思われる。意図しないエラーが発生しやすいにも関わらず、対策が十分に行われていないということは、情報漏洩が発生しやすい環境が形成されやすいことに繋がり得る。よって、今後このようなケースを中心に対策を効果的な対策を講じていく必要性があると思われる。

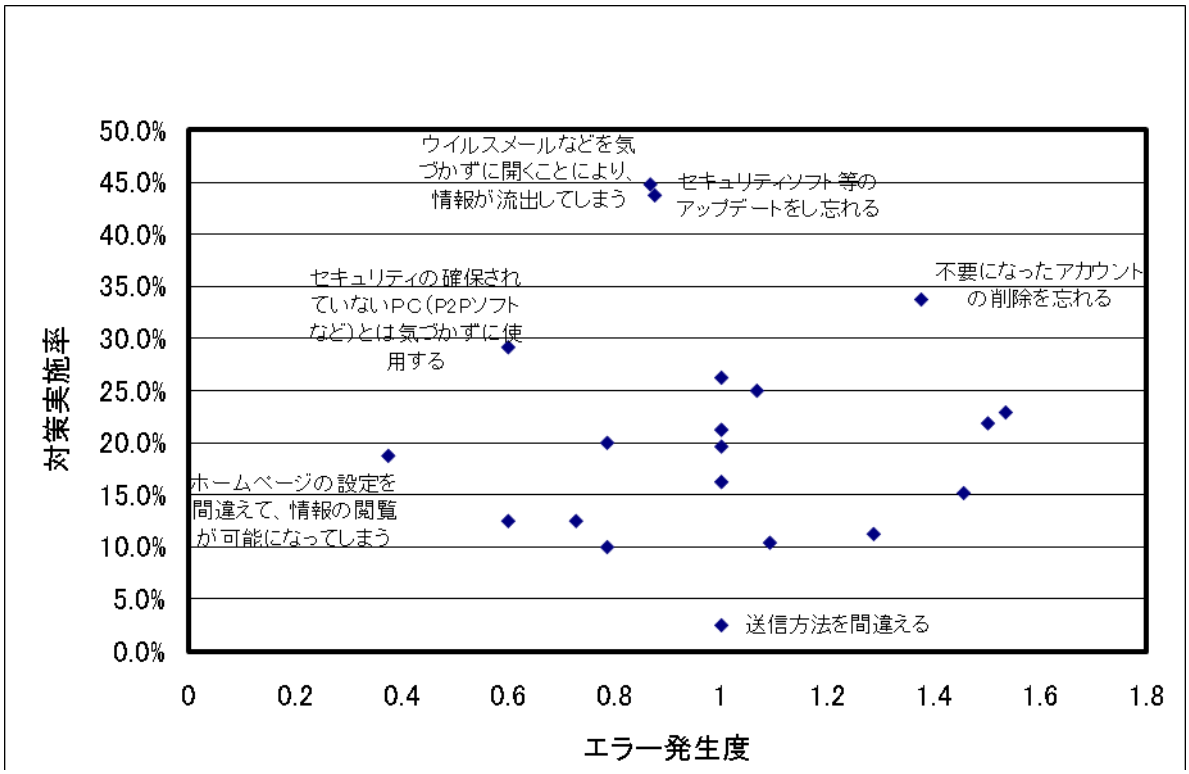

図６．１　エラーの発生度とエラー対策の実施率の関係

第７章
意図しないエラーに対する対策を推進するための取り組みの状況

７．意図しないエラーに対する対策を推進するための取り組みの状況

７．１　情報の収集に関する取り組み状況

エラー対策を推進する場合、意図しないエラーやエラーに起因する事故・トラブルに関する情報を収集し、これをエラー対策に活用することが重要となる。このような情報収集を、①誰が行うか（行う人）、②いつ行うか（頻度）、③どのように行うか（方法）を調べた結果を、それぞれ分類した。結果を図７．１～図７．３に示す。また、①行う人、②頻度、③方法の３つの組合せを整理した結果を表７．１に示す。これらの図表より以下のことがわかった。

（１）部門関係者が情報の収集を行っているところが最も多い。これに ISMS 関係者、セキュリティ関係者が行っているところを含めると約９０％を占める。

（２）事故の発生の都度、情報の収集を行っているところが最も多い。

（３）方法としては、報告書形式で提出してもらっているところが最も多い。

（４）組合せとしては、部門関係者が事故発生時に報告書形式で事故の報告を行っているところが最も多い。ただし、ISMS 関係者が決められた時期ごとに報告書形式で事故の報告を行っているところも他に比べて多い。

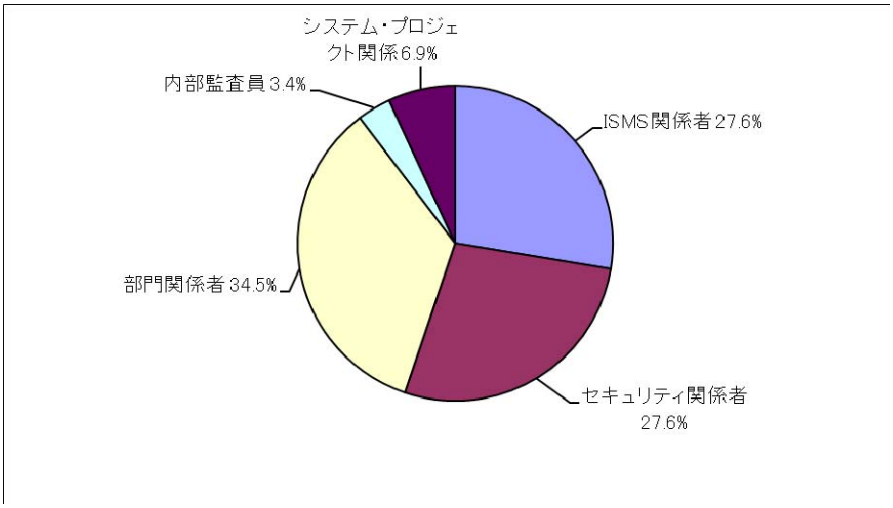

図７．１　　情報の収集を行う人

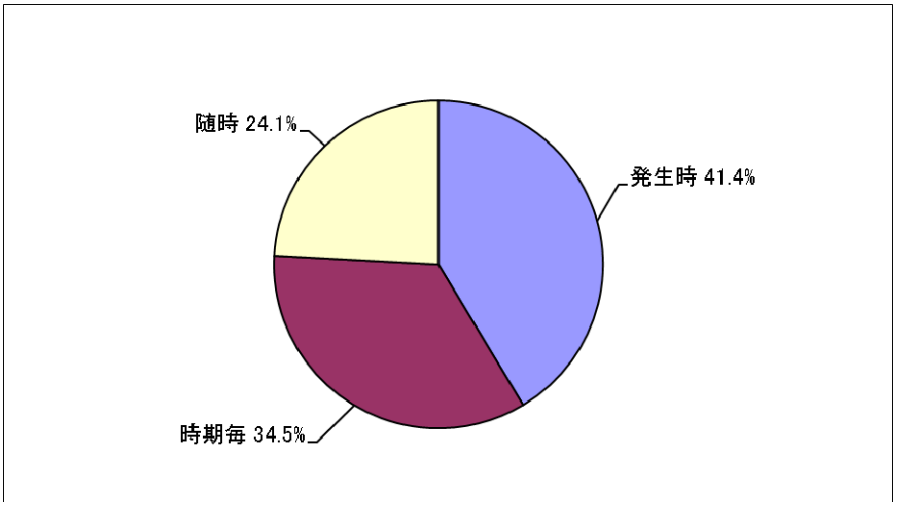

図７．２　　情報の収集を行う頻度

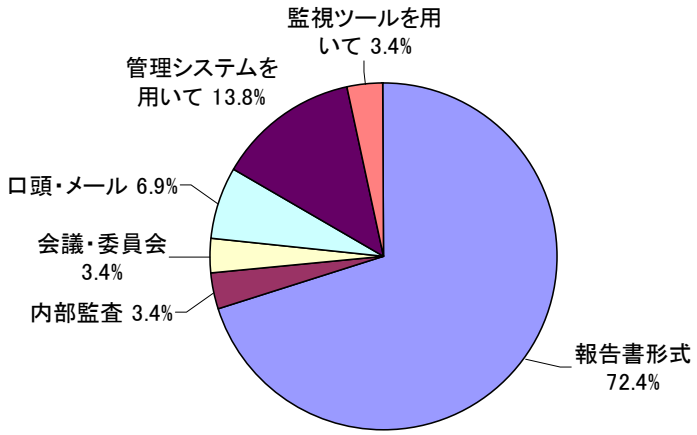

図７．３　　情報の収集を行う方法

表７．１　情報の収集に関する取り組みの組合せ

行う人	頻度	方法	割合
ISMS 関係者	発生時	報告書形式	10.3%
	時期毎	報告書形式	10.3%
		内部監査	3.4%
	随時	報告書形式	3.4%
セキュリティ関係者	発生時	報告書形式	13.8%
		口頭・メール	3.4%
	時期毎	報告書形式	6.9%
	随時	管理システムを用いて	3.4%
部門関係者	発生時	報告書形式	10.3%
		管理システムを用いて	3.4%
	時期毎	報告書形式	6.9%
		会議・委員会	3.4%
	随時	報告書形式	3.4%
		口頭・メール	3.4%
		監視ツールを用いて	3.4%
内部監査員	時期毎	報告書形式	3.4%
システム・プロジェクト関係者	随時	管理システムを用いて	6.9%

７．２　情報の分析に関する取り組み状況

集めた情報の分析を、①誰が行うか（行う人）、②いつ行うか（頻度）、③どのように行うか（方法）を調べた結果を、それぞれ分類した。結果を図７．４～図７．６に示す。また、①行う人、②頻度、③方法の３つの組合せを整理した結果を表７．２に示す。これらの図表より以下のことがわかった。

（１）ISMS 関係者が情報の分析を行うことが最も多い。

（２）決められた時期ごとに情報の分析を行うことが最も多い。

（３）報告書形式で情報の収集を行うことが最も多い。

（４）ISMS 関係者が決められた時期ごとに報告書形式で分析を行う割合が最も高い。セキュリティ関係者が決められた時期ごとに報告書形式で分析を行う割合、セキュリティ関係者が決められた時期ごとに会議・委員会で分析を行う割合も他の組合せに比べて高い。

（５）ISMS 関係者が分析を行う組合せの種類が一番多い。

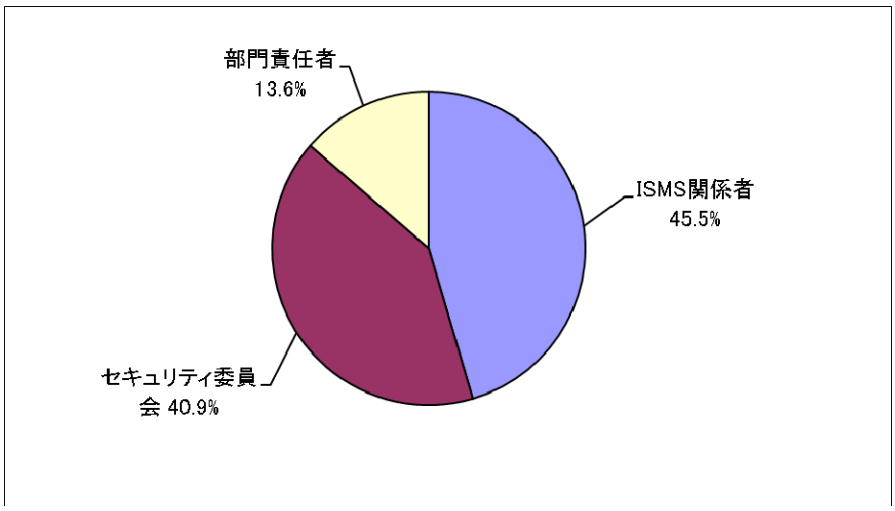

図７．４　　情報の分析を行う人

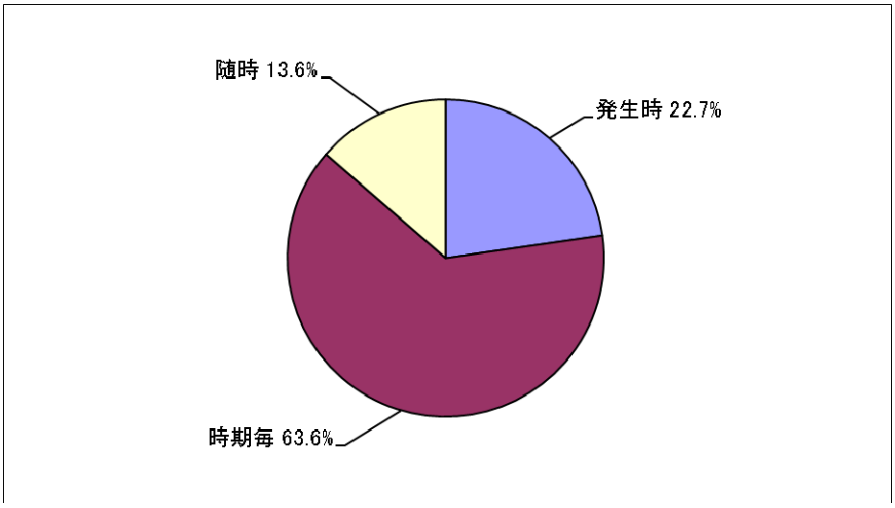

図７．５　　情報の分析を行う頻度

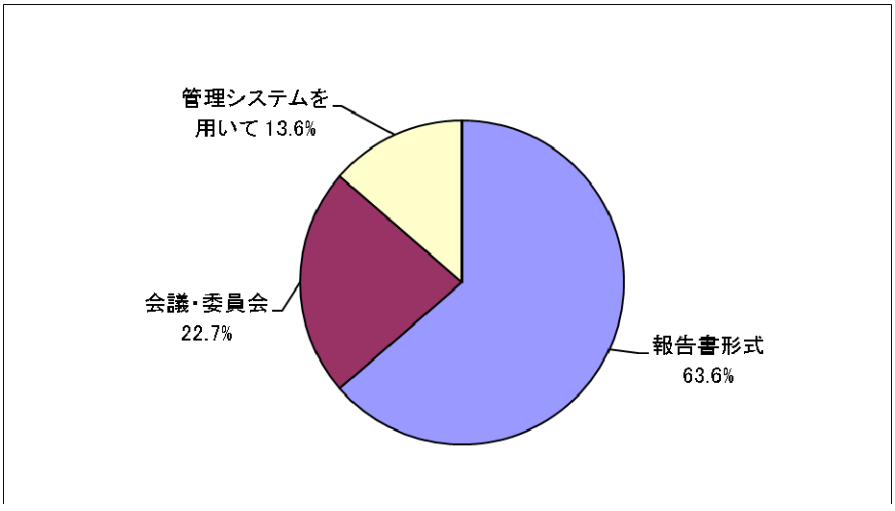

図７．６　　情報の分析を行う方法

表７．２　情報の分析に関する取り組みの組合せ

行う人	頻度	方法	割合
ISMS 関係者	発生時	管理システムを用いて	4.5%
	時期毎	報告書形式	22.7%
		会議･委員会	4.5%
		管理システムを用いて	4.5%
	随時	報告書形式	4.5%
		会議･委員会	4.5%
セキュリティ関係者	発生時	報告書形式	9.1%
	時期毎	報告書形式	13.6%
		会議･委員会	13.6%
	随時	報告書形式	4.5%
部門責任者	発生時	報告書形式	4.5%
		管理システムを用いて	4.5%
	時期毎	報告書形式	4.5%

７．３　リスクの予測・評価に関する取り組み状況

意図しないエラーの防止のためには、発生したものの情報を集めたり、分析したりするだけでなく、得られた情報をもとに、業務に潜在しているまだ発生していないエラーやエラーによる事故のリスクを洗い出すことが重要となる。リスクの予測・評価を、①誰が行うか（行う人）、②いつ行うか（頻度）、③どのように行うか（方法）を調べた結果を、それぞれ分類した。結果を図７．７～図７．９に示す。また、①行う人、②頻度、③方法の３つの組合せを整理した結果を表７．３に示す。これらの図表より以下のことがわかった。

（１）部門関係者がリスクの予測・評価を行うことが最も多い。

（２）決められた時期ごとにリスクの予測・評価を行うことが最も多い。

（３）報告書形式でリスクの予測・評価を行うことが最も多い。

（４）①ＩＳＭＳ関係者が決められた時期ごとに報告書形式で、②セキュリティ関係者が決められた時期ごとに報告書形式で、③部門関係者が決められた時期ごとに報告書形式で、リスクの予測・評価を行う割合が最も高い。

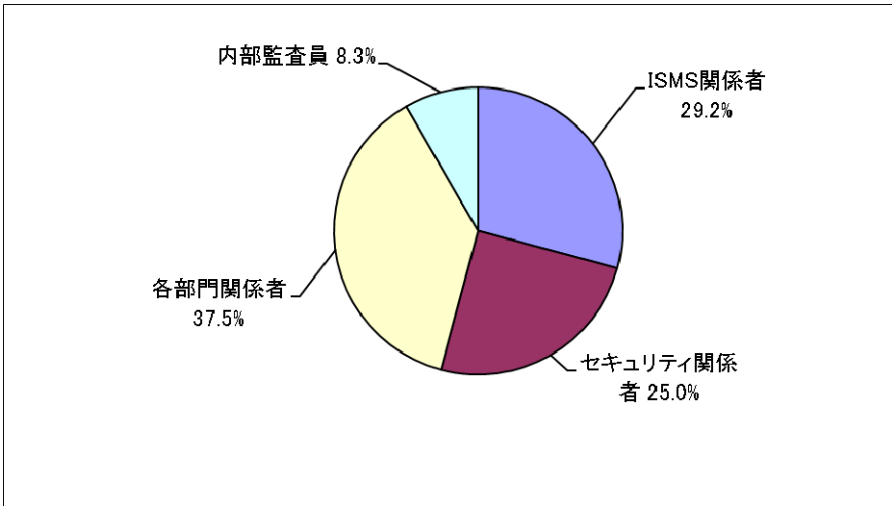

図７．７　　リスクの予測・評価を行う人

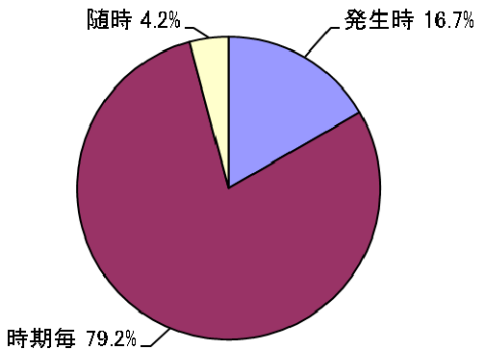

図７．８　　リスクの予測・評価を行う頻度

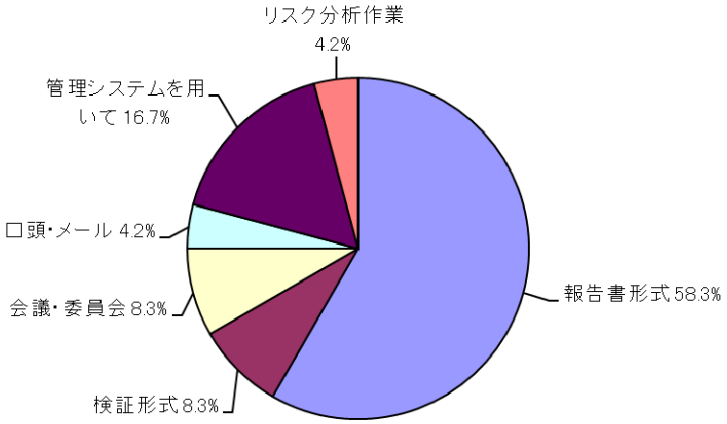

図７．９　　リスクの予測・評価を行う方法

表７．３　リスクの予測・評価に関する取り組みの組合せ

行う人	頻度	方法	割合
ISMS 関係者	発生時	管理システムを用いて	4.2%
	時期毎	報告書形式	12.5%
		検証形式	8.3%
		管理システムを用いて	4.2%
セキュリティ関係者	発生時	報告書形式	8.3%
	時期毎	報告書形式	12.5%
		リスク分析作業	4.2%
部門関係者	発生時	報告書形式	4.2%
	時期毎	報告書形式	12.5%
		会議･委員会	8.3%
		口頭･メール	4.2%
		管理システムを用いて	4.2%
	随時	報告書形式	4.2%
内部監査員	時期毎	報告書形式	4.2%
		管理システムを用いて	4.2%

７．４　対策の作成・選定・実施に関する取り組み状況

洗い出したリスクに対する対策の作成・選定・実施を、①誰が行うか（行う人）、②いつ行うか（頻度）、③どのように行うか（方法）を調べた結果を、それぞれ分類した。結果を図７．１０～図７．１２に示す。また、①行う人、②頻度、③方法の３つの組合せを整理した結果を表７．４に示す。これらの図表より以下のことがわかった。

（１）セキュリティ関係者がリスクに対する対策の作成・選定・実施を行うことが最も多い。

（２）決められた時期ごとにリスクに対する対策の作成・選定・実施を行うことが最も多い。

（３）報告書形式で対策の作成・選定・実施を行うことが最も多い。

（４）部門関係者が事故発生時に報告書形式で対策の作成・選定・実施を行う割合が最も高い。ISMS関係者が決められた時期ごとに報告書形式で対策の作成・選定・実施を行う割合も他の組合せに比べて高い。

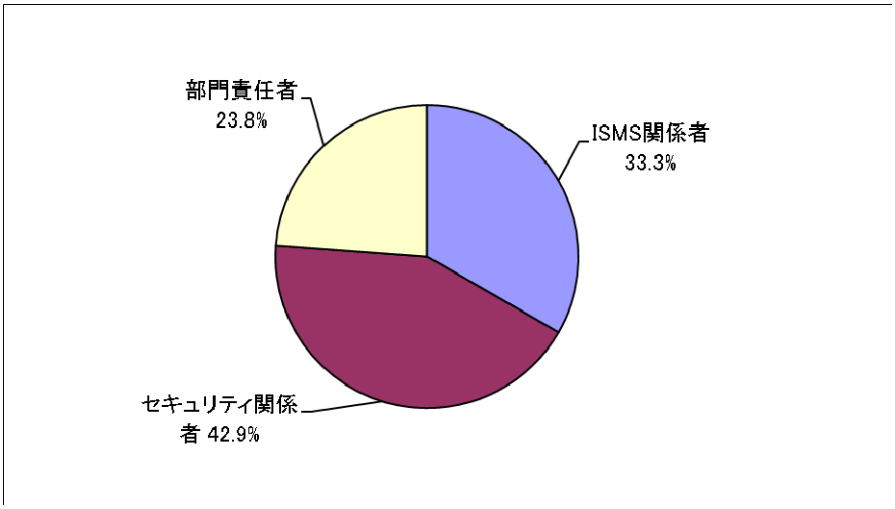

図７．１０　　対策の作成・選定・実施を行う人

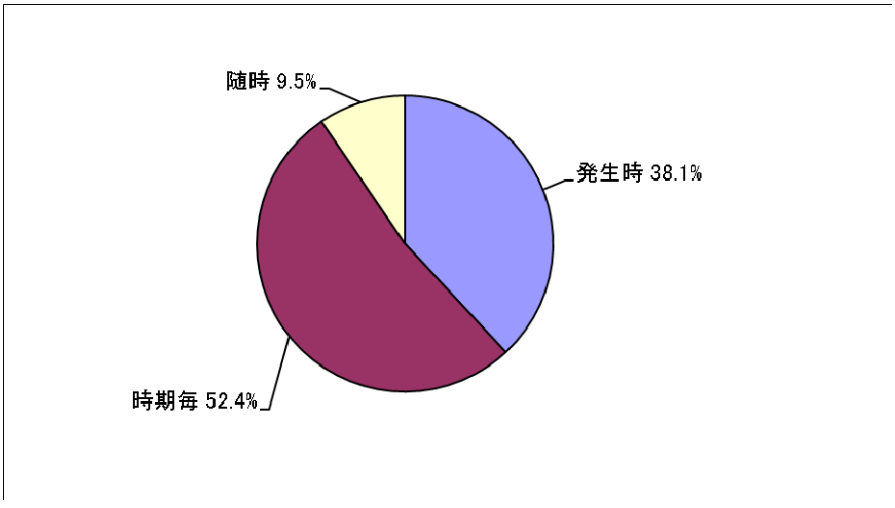

図７．１１　　対策の作成・選定・実施を行う頻度

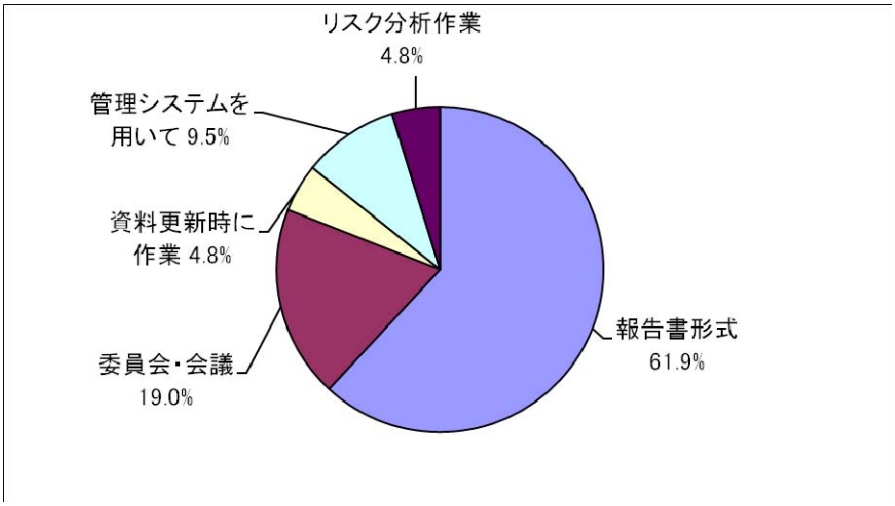

図７．１２　対策の作成・選定・実施を行う方法

表７．４　対策の作成・選定・実施に関する取り組みの組合せ

行う人	頻度	方法	割合
ISMS 関係者	発生時	報告書形式	4.8%
		委員会・会議	4.8%
	時期毎	報告書形式	14.3%
		委員会・会議	4.8%
		資料更新時に作業	4.8%
セキュリティ関係者	発生時	報告書形式	9.5%
	時期毎	報告書形式	9.5%
		委員会・会議	4.8%
		管理システムを用いて	4.8%
		リスク分析作業	4.8%
	随時	報告書形式	4.8%
		委員会・会議	4.8%
部門関係者	発生時	報告書形式	19.0%
	時期毎	管理システムを用いて	4.8%

７．５　効果の把握に関する取り組み状況

行った対策の効果の把握を、①誰が行うか（行う人）、②いつ行うか（頻度）、③どのように行うか（方法）を調べた結果を、それぞれ分類した。結果を図７．１３～図７．１５に示す。また、①行う人、②頻度、③方法の３つの組合せを整理した結果を表７．５に示す。これらの図表より以下のことがわかった。

（１）ISMS 関係者が対策の効果の把握を行うことが最も多い。

（２）決められた時期ごとに効果の把握を行うことが最も多い。

（３）報告書形式で効果の把握を行うことが最も多い。

（４）ＩＳＭＳ関係者が決められた時期ごとに報告書形式で対策の効果の把握を行う割合が最も高い。

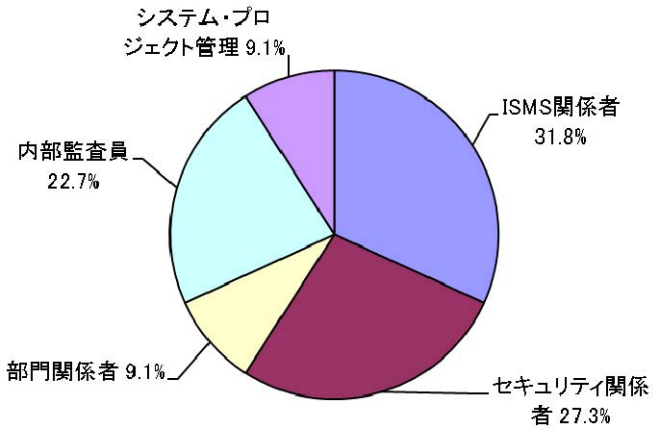

図７．１３　　効果の把握を行う人

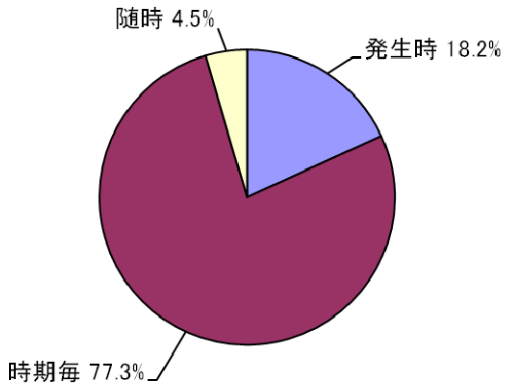

図７．１４　　効果の把握を行う頻度

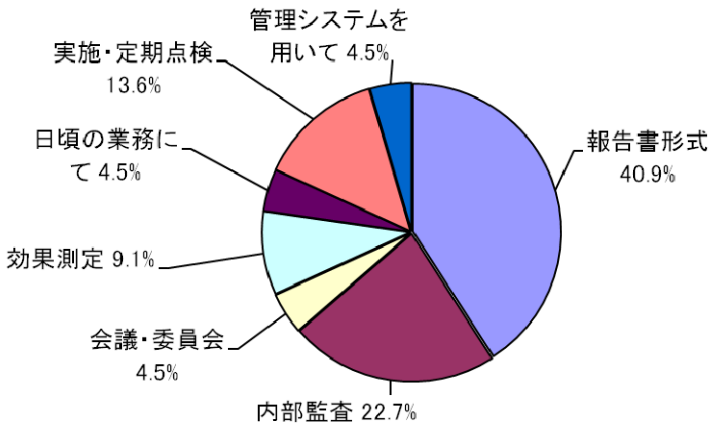

図７．１５　効果の把握を行う方法

表７．５　効果の把握に関する取り組みの組合せ

行う人	頻度	方法	割合
ISMS 関係者	時期毎	報告書形式	13.6%
		内部監査	9.1%
		効果測定	4.5%
	随時	日頃の業務にて	4.5%
セキュリティ関係者	発生時	報告書形式	9.1%
		会議・委員会	4.5%
	時期毎	効果測定	4.5%
		実施・定期点検	4.5%
		管理システムを用いて	4.5%
部門関係者	発生時	報告書形式	4.5%
	時期毎	報告書形式	4.5%
内部監査員	時期毎	報告書形式	9.1%
		内部監査	13.6%
システム・プロジェクト管理	時期毎	実施・定期点検	9.1%

７．６　取り組みの組合せとエラー対策の実施率との関係

回答企業を対策実施率の高低により２つのグループに分類し、７．１～７．５節で述べた、

（１） 情報の収集

（２） 情報の分析

（３） リスクの予測・評価

（４） 対策の作成・選定・実施

（５） 効果の把握

の①行う人、②頻度、③方法の組合せがどのように異なっているか調べた。結果を表７．６～７．１０に示す。これらの表から以下のことが分かった。

（１）情報の収集について見ると、対策実施率の高い企業は、低い企業に比べると、①ＩＳＭＳ関係者が決められた時期ごとに報告書形式で、②部門関係者が発生時に報告書形式で取り組みを行っているところが多い。

（２）情報の分析について見ると、対策実施率の高い企業は、低い企業に比べると、セキュリティ関係者が発生時に報告書形式で取り組みを行っているところが多い。

（３）リスクの予測・評価について見ると、対策実施率の高い企業は、低い企業に比べて、部門関係者が決められた時期ごとに報告書形式または会議・委員会形式で取り組みを行っているところが多い。

（４）対策の作成・選定・実施について見ると、対策実施率の高い企業は、低い企業に比べて、ＩＳＭＳ関係者が決められた時期ごとに報告書形式で取り組みを行っているところが多い。

（５）効果の把握について見ると、対策実施率の高い企業は、低い企業に比べて、①内部監査員が決められた時期ごとに報告書形式で、②ＩＳＭＳ関係者が決められた時期ごとに内部監査形式で取り組みを行っているところが多い。

表７．６　対策実施率の高い企業と低い企業の比較（情報の収集に関する取り組み）

行う人	頻度	方法	実施率の高い企業	実施率の低い企業
ISMS 関係者	発生時	報告書形式	3.4%	6.9%
	時期毎	報告書形式	6.9%	3.4%
		内部監査	0.0%	3.4%
	随時	報告書形式	3.4%	0.0%
セキュリティ委員会	発生時	報告書形式	6.9%	6.9%
		口頭・メール	0.0%	3.4%
	時期毎	報告書形式	3.4%	3.4%
	随時	管理システムを用いて	3.4%	0.0%
部門関係者	発生時	報告書形式	6.9%	3.4%
		管理システムを用いて	0.0%	3.4%
	時期毎	報告書形式	3.4%	3.4%
		会議・委員会	3.4%	0.0%
	随時時	報告書形式	3.4%	0.0%
		口頭・メール	3.4%	0.0%
		監視ツールを用いて	3.4%	0.0%
内部監査員	時期毎	報告書形式	3.4%	0.0%
システム・プロジェクト管理	随時	管理システムを用いて	3.4%	3.4%

表７．７　対策実施率の高い企業と低い企業の比較（情報の分析に関する取り組み）

行う人	頻度	方法	実施率の高い企業	実施率の低い企業
ISMS 関係者	発生時	管理システムを用いて	0.0%	4.5%
	時期毎	報告書形式	9.1%	13.6%
		会議・委員会	4.5%	0.0%
		管理システムを用いて	0.0%	4.5%
	随時	報告書形式	4.5%	0.0%
		会議・委員会	4.5%	0.0%
セキュリティ委員会	発生時	報告書形式	9.1%	0.0%
	時期毎	報告書形式	4.5%	9.1%
		会議・委員会	4.5%	9.1%
	随時	報告書形式	4.5%	0.0%
部門責任者	発生時	報告書形式	4.5%	0.0%
		管理システムを用いて	4.5%	0.0%
	時期毎	報告書形式	0.0%	4.5%

表７．８　対策実施率の高い企業と低い企業の比較（リスクの予測・評価に関する取り組み）

行う人	頻度	方法	実施率の高い企業	実施率の低い企業
ISMS 関係者	発生時	管理システムを用いて	0.0%	4.2%
	時期毎	報告書形式	4.2%	8.3%
		検証形式	4.2%	4.2%
		管理システムを用いて	4.2%	0.0%
セキュリティ委員会	発生時	報告書形式	4.2%	4.2%
	時期毎	報告書形式	4.2%	8.3%
		リスク分析作業	4.2%	0.0%
各部門関係者	発生時	報告書形式	0.0%	4.2%
	時期毎	報告書形式	12.5%	0.0%
		会議・委員会	8.3%	0.0%
		口頭・メール	4.2%	0.0%
		管理システムを用いて	0.0%	4.2%
	随時	報告書形式	4.2%	0.0%
内部監査員	時期毎	報告書形式	4.2%	0.0%
		管理システムを用いて	0.0%	4.2%

表７．９　対策実施率の高い企業と低い企業の比較（対策の作成・選択・実施に関する取り組み）

行う人	頻度	方法	実施率の高い企業	実施率の低い企業
ISMS 関係者	発生時	報告書形式	4.8%	0.0%
		委員会・会議	0.0%	4.8%
	時期毎	報告書形式	9.5%	4.8%
		委員会・会議	4.8%	0.0%
		資料更新時に作業	4.8%	0.0%
セキュリティ委員会	発生時	報告書形式	4.8%	4.8%
	時期毎	報告書形式	4.8%	4.8%
		委員会・会議	0.0%	4.8%
		管理システムを用いて	4.8%	0.0%
		リスク分析作業	4.8%	0.0%
	随時	報告書形式	0.0%	4.8%
		委員会・会議	4.8%	0.0%
部門関係者	発生時	報告書形式	4.8%	14.3%
	時期毎	管理システムを用いて	4.8%	0.0%

表７．１０　対策実施率の高い企業と低い企業の比較（効果の確認に関する取り組み）

行う人	頻度	方法	実施率の高い企業	実施率の低い企業
ISMS 関係者	時期毎	報告書形式	0.0%	13.6%
		内部監査	9.1%	0.0%
		効果測定	4.5%	0.0%
	随時	日頃の業務にて	4.5%	0.0%
セキュリティ委員会	発生時	報告書形式	4.5%	4.5%
		会議・委員会	0.0%	0.0%
	時期毎	効果測定	4.5%	0.0%
		実施・定期点検	0.0%	4.5%
		管理システムを用いて	4.5%	0.0%
部門関係者	発生時	報告書形式	0.0%	4.5%
	時期毎	報告書形式	4.5%	0.0%
内部監査員	時期毎	報告書形式	13.6%	0.0%
		内部監査	4.5%	9.1%
システム・プロジェクト管理	時期毎	実施・定期点検	0.0%	9.1%

第８章
考察

８．考察

５章～７章の結果を総合して考えると、情報漏洩事故を防止するためには、意図しないエラーに対する対策を推進していくことが必要であるといえる。対策を行うべきところは、エラー発生率が高く対策実施率が低い業務やエラーであると考えられる。具体的には、

（1）「情報を持ち出す」業務

（2）「情報を保管する」業務

（3）「施錠を忘れることにより、情報が誰の手にも渡る状況にしてしまう」意図しないエラー

（4）「送信方法を間違える（メールで bcc にせずに送信してしまうなど)」意図しないエラー

（5）「個人情報の入った過般型情報媒体などを使用後、うっかり持って帰ってしまう」意図しないエラー

（6）「施錠を忘れることにより、情報が誰の手にも渡る状況にしてしまう」意図しないエラー

などが挙げられる。

また、上で挙げた対策をどのような体制で推進するべきかに関しては、

（1）情報の収集に関しては、①ＩＳＭＳ関係者が決められた時期ごとに報告書形式で、または②部門関係者が発生時に報告書形式で行う

（2）情報の分析に関しては、セキュリティ関係者が発生時に報告書形式で行う

（3）リスクの予測・評価に関しては、部門関係者が決められた時期ごとに報告書形式または会議・委員会形式で行う

（4）対策の作成・選択・実施に関しては、ＩＳＭＳ関係者が決められた時期ごとに報告書形式で行う

（5）効果の確認に関しては、①内部監査員が決められた時期ごとに報告書形式で、または②ＩＳＭＳ関係者が決められた時期ごとに内部監査形式で行う

のがよいと考えられる。

第９章
結論と今後の課題

９．結論と今後の課題

本研究では、過去の情報漏洩事故の事例を基に、どのような人的エラーが原因で情報漏洩事故が発生しやすいのか、また職場では、意図しないエラーに対して、どのような対策を行い、推進活動を講じているのかについて調査・解析を行った。結果として、現在の意図しないエラーの発生状況と、対策の実施率との関係性や、組織として意図しないエラーをどのように捉えているのかについて明らかにすることができた。今現在も、増加の一途を辿っている情報漏洩事故の背景として、今もまだ顕在化されていない意図しないエラーが存在していることが原因ではないかと考えられる。

今後の課題としては、そのような表にまだ出ていない、意図しないエラーを明らかにし、それに対する対策を策定・実施し、一件でも情報漏洩に繋がり得るファクターを減らしていくことが挙げられる。

参考文献

[1]　中條武志，尾辻正則，松倉辰雄：ポカミス防止実践マニュアルー実務に役立つシリーズー，品質月刊委員会

[2]　IT 保険ドットコム：個人情報漏洩事件一覧，(http://www.it-hoken.com/cat_aeieoieioeie.html)

[3]　日本ネットワークセキュリティ協会，２００７年情報セキュリティインシデントに関する調査報告書（http://www.jnsa.org/result/2007/pol/incident/2007incidentsurvey_v1_5.pdf）

[4]　財団法人　日本情報処理開発協会情報マネジメント推進センター：ISMS 適合性評価制度，（http://www.isms.jipdec.jp/isms.html）