企業における内部者の故意による情報セキュリティインシデントへの対策に関する一考察

沼田 晋作 †　　柴田賢介 †　　岡崎聖人 †　　高橋克巳 †

†NTT 情報流通プラットフォーム研究所
180-8585 東京都武蔵野市緑町 3-9-11

あらまし　企業において情報セキュリティ対策の実施は，今もなお重要事項であると考えられる．特に近年では，内部者の故意による情報漏洩が発生し，それらへの対策が求められていると考えられる．本論文では，情報セキュリティに関して実施した定性的，定量的調査から，内部者の故意による情報セキュリティインシデント対策を実施している管理者の，90%以上がリスクアセスメントを実施している一方で，39%もの管理者がインシデントを経験している実態を報告し，その原因がリスクアセスメントの方法や内容と考えられる事を述べ，企業における情報セキュリティの課題と原因について考察する．

A study of information security controls in enterprise for incident on which internal person depends by intention

Shinsaku Numata †　　Kensuke Shibata †　　Masato Okazaki †　　Katsumi Takahashi †

†NTT Information Sharing Platform Laboratories
3-9-11 Midori-Cho Musashino-Shi Tokyo 180-8585 Japan

Abstract　The execution of the information security measures is still thought to be matters of weight for the enterprise in the enterprise of the information leakage measures etc. Especially, the leak of information etc. on which an internal person depends by intention are generated, and it is thought that measures against them are requested in recent years. In this thesis, it reports on the realities of the information security of the enterprise that those internal people confront by intention from a qualitative of execute for the information security quantitative survey,and while 90% or more manager is executing the information security incident mesures but,39% manager is experiencing the incident,and it is thought that cause is a method and a content of the risk assessment, and the problem of the information security in the enterprise is described.

1　はじめに

近年社会問題となっている情報漏洩等の情報セキュリティインシデントは，情報を取り扱う内部の人間の過失や情報を取り扱う内部の人間の故意等の様々な原因によって発生している．内部の人間の故意を原因とした情報セキュリティインシデントには，定められているルールを知りつつも業務上やむを得ずにルールを破った結果のインシデントや，自分の利益のためにルールを破る内部犯行や内部不正のようなインシデントが考えられる．

JNSA が毎年発表している情報セキュリティインシデントに関する調査報告書 [1] では，個人情報漏洩インシデントの漏えい原因，漏洩経路，漏洩人数等が報告されている．同報告書によると，内部者の故意が原因である「内部犯罪・内部不正行為」による個人情報漏洩インシデントは，インシデント 1 件あたりの平均漏洩人数が 2005 年から 2007 年の 3 年連続で 1 位であることから，その規模が大きいことが考えられる．

企業では，これら内部者の故意によって発生する情報セキュリティインシデントに対して，各種対策を実施している．同報告書では，2008 年に発生した「内部犯罪・内部不正行為」による個人情報漏洩事件の漏洩人数が 2007 年までと比較して大幅に減少している事が述べられ，減少の理由を内部の権限管理等の対策が取られ，内部犯罪や不正

行為が困難になっていることと推測している[1].

しかし，同報告書のデータを分析すると，2005年から2008年にかけて，内部犯罪・内部不正行為による個人情報漏洩事件の発生件数は横ばいで推移している．また，漏洩人数が大幅に減少したとはいえ，インシデント1件あたりの平均漏洩人数が2008年は2位であり，依然としてその規模は大きいままである．これらの事から，内部者の故意による情報セキュリティインシデントに対して現在実施されている対策は，漏洩規模を以前よりも小さくするという効果は出ているが，発生件数を減らすことは出来ず，依然として課題が残されていることが考えられる．

このため本研究では，企業における内部者の故意を原因とした情報セキュリティインシデントへの対策について，現状調査を実施した．定量的調査と定性的調査によって，それら対策における課題とその原因を考察する．

2 調査概要

本章では，本研究で実施した定量的調査と定性的調査の概要について述べる．

2.1 定量的調査

2.1.1 調査方式

調査方式はWebアンケート方式を採用した．回答者はWebブラウザでインターネット上のWebサーバにアクセスし，表示される設問に対し回答する形式とした．

2.1.2 調査対象者

定量的調査は，企業で情報セキュリティ管理者の立場にある回答者を対象とした調査である．毎日PCを使用する業務を行い，現在の企業に3年以上勤務し，情報セキュリティ対策製品の導入を行ったことがある管理者を対象とした．

2.1.3 質問項目

Webアンケートは，回答者自身の勤務する企業の情報セキュリティ対策製品の導入とその実施状況についての質問項目とした．質問内容は表1の通りである．質問項目の詳細を以下に述べる．

Q1 情報セキュリティ対策製品　回答者が実際に導入した情報セキュリティ製品を調査する質問項目である．情報セキュリティ対策製品の一覧を選択肢で表示し，回答者に実際に導入した情報セキュリティ対策製品を1つ選択させる形式とした．

[1]2008年情報セキュリティインシデントに関する調査報告書 p.32

表 1: 定量的調査質問項目

質問番号	質問内容
Q1	情報セキュリティ対策製品
Q2	情報セキュリティ対策製品が防止しているインシデント
Q3	インシデントを発生させる脅威
Q4	対策実施状況把握の有無
Q5	発生インシデント把握の有無
Q6	想定インシデント発生の有無
Q7	想定外インシデント発生の有無
Q8	従業員からの意見の有無
Q9	従業員からの意見の内容
Q10	情報資産認定ルールの有無
Q11	情報資産管理ルールの有無
Q12	脆弱性の特定

Q2 情報セキュリティ製品が防止しているインシデント　Q1の回答である対策製品が，どの様な情報セキュリティインシデントを防止するために導入されたのかを調査する質問項目である．

Q3 インシデントを発生させる脅威　Q2の回答である情報セキュリティインシデントを発生させる脅威を調査する質問項目である．以下の選択肢から1つを選び回答する．

- 内部の人間の過失による操作・行動
- 内部の人間の故意による操作・行動
- 外部の関係者の過失による操作・行動
- 外部の関係者の故意による操作・行動
- 第三者の過失による操作・行動
- 第三者の故意による操作・行動
- ワーム・ウィルス等の悪意のあるプログラムの動作
- プログラムのバグによる誤動作
- その他（経年劣化や自然災害などによる故障等）
- わからない

Q4 対策実施状況把握の有無　Q1の回答である対策製品を導入した後，実際に使用されているかどうかを，管理者が把握する仕組みを構築しているかを調査する質問項目である．

Q5 インシデント発生把握の有無　Q1の回答である対策製品の導入時に，回答者が想定していた情報セキュリティインシデントの発生を，管理者が把握する仕組みを構築しているかを調査する質問項目である．

Q6 想定インシデント発生の有無　Q1の回答である対策製品の導入時に，回答者が想定していた情報セキュリティインシデントが，実際に発生したかどうかを調査する質問項目である．

Q7 想定外インシデント発生の有無　Q1 の回答である対策製品の導入時に，回答者が想定していなかった情報セキュリティインシデントが，実際に発生したかどうかを調査する質問項目である．

Q8 従業員からの意見の有無　Q1 の回答である対策製品の導入後に，回答者がその対策について従業員から意見を受けたかどうかについて調査する質問項目である．

Q9 従業員からの意見の内容　Q8 で調査した管理者が従業員からから受けた意見について，その内容を調査する質問項目である．「その他に守るべき情報がある」「その他に注意すべき脆弱性が有る」「その他に注意すべき脅威がある」「その他に注意すべきインシデントがある」「業務に影響がある」「その他」という選択肢から複数を選択する形式とした．

Q10 情報資産認定ルールの有無　業務で取り扱っている重要な情報を，ルールを定めて情報資産と認定しているかを調査する質問項目である．

Q11 情報資産管理ルールの有無　業務で取り扱っている重要な情報を，ルールを定めて管理しているかを調査する質問項目である．

Q12 脆弱性の特定　業務で取り扱っている重要な情報に，どの様な情報セキュリティ上の欠陥があるかを特定しているかを調査する質問項目である．

2.2　定性的調査

2.2.1　調査方式

定性的調査はグループインタビュー方式とした．1 グループ 6 人で 5 つのグループを作成した．インタビュー中の発言を録音し，テキストデータに書き起こした．テキストデータには発言した順番，誰への発言かなどの情報を含んでいる．インタビューは回答者 6 人に議事の進行をスムーズにするための司会者を加えた計 7 人として，各グループ 2 時間で実施した．

2.2.2　調査対象者

定性的調査は，情報システムを利用する立場にある従業員を対象とした調査である．日常業務で PC を使用し，情報システムに対し何らかの不満を感じている従業員を対象とした．

2.2.3　質問項目概要

グループインタビューでは，参加者が実際に使用している情報セキュリティ対策と，その対策に関する不満，望ましい情報セキュリティ対策の方法について意見を述べて貰い，それらについて参加者同士が議論をする形で調査を行った．

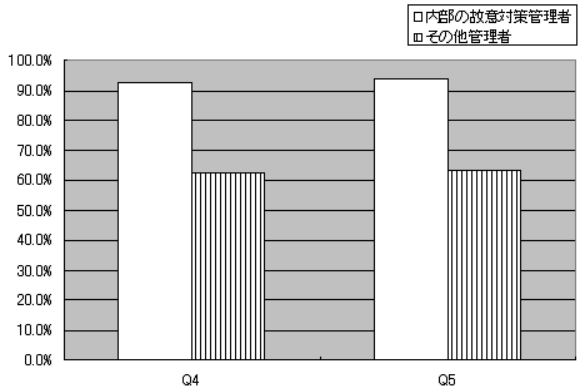

図 1: 対策の実施とインシデント発生の把握状況

3　調査結果

本章では定量的調査と定性的調査の調査結果について述べる．

3.1　定量的調査

本節では定量的調査の調査結果について述べる

アンケートでは 1741 人へ回答を依頼し，357 人から有効回答を得ることが出来た．この有効回答の中で，インシデントを発生させる脅威について「内部者の故意による操作・行動」と回答した回答者は 52 人であり，その他の脅威を選択した回答者は，305 人であった．以後は，前者を内部者の故意による情報セキュリティインシデントへの対策を実施した管理者として扱う．（以後「内部者の故意対策管理者」と記述する）そして，後者からインシデントを発生させる脅威について「わからない」を選択した管理者を除いた 263 人を，内部者の故意以外による情報セキュリティインシデントへの対策を実施した管理者として分析する．（「その他管理者」と記述する．）

定量的調査結果を図 1 に示す．対策実施把握の有無 (Q4) について，内部者の故意対策管理者が 92.3%が実施していると回答したのに対し，その他対策管理者は 62.3%の管理者が実施していると回答している．情報セキュリティインシデント発生把握の有無 (Q5) については，内部犯行対策の管理者の 94.1%が実施していると回答したのに対し，その他対策管理者は 63.3%が実施していると回答するという結果となった．これらの結果から内部者の故意対策管理者は，対策の実施状況の把握や，情報セキュリティインシデントの発生状況の把握を高い割合で実施していることが分かった．

しかし，そのように内部の故意対策管理者が力を入れて対策を実施している一方で，対策が守っている情報資産にインシデントが発生してしまっている状況が確認できた．図 2 に示すとおり，想定

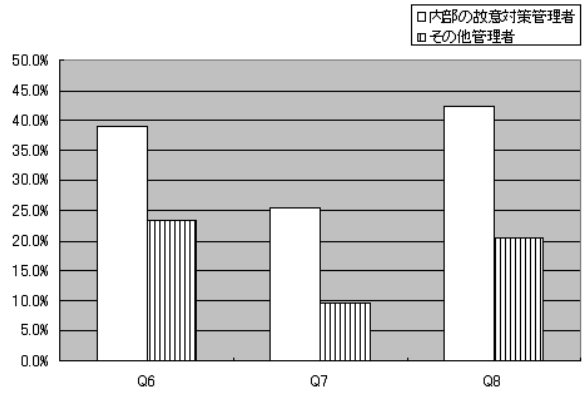

図 2: インシデント経験と従業員からの意見を受けた経験

インシデント発生の有無 (Q6) について，インシデントを経験したと答えた管理者の割合は 39.0%であり，想定外インシデント発生の有無 (Q7) については，25.5%の管理者が想定外インシデントを経験していた．

また，従業員からの意見の有無 (Q8) についても，従業員から意見を受けた事がある管理者の割合が高い事が分かった．図 2 に示すとおり，内部者の故意対策管理者の 42.3%が，実施した情報セキュリティ対策製品に関して従業員からの意見を受けていた．

そしてその意見の内訳 (Q9. 従業員からの意見の内訳) は，意見を受けた管理者の 45.5%が「その他に守るべき情報資産がある」「その他に配慮すべき情報セキュリティの欠陥がある」「業務への影響が高い」という 3 つについて，意見を受けたと回答した．

3.2 定性的調査

本節では定性的調査によって得られた調査結果を述べる．定性的調査では，各参加者から実施されている情報セキュリティ対策と，その情報セキュリティ対策への不満，望ましい情報セキュリティ対策についての発言を得ることが出来た．全体的に，情報セキュリティ対策製品の必要性は認めている一方で，それらが業務を阻害していることに不満を感じており，改善を望む傾向が見られた．

定性的調査結果全てを本論文に掲載することは困難であるため，得られた発言の一部を示す．表 2 に実際に使用している対策とその対策への不満，表 3 に情報セキュリティ対策全般への不満と望ましい対策方法を示す．

表 2: 情報セキュリティ対策と不満

項番	対策	不満
1	情報のラベル付け	ルールを見たことがない
2	情報のラベル付け	ルールの運用が困難
3	情報のラベル付け	ルールがわからない
4	セキュリティの試験	試験のための試験
5	ビデオ研修後の試験	研修の内容の丸暗記
6	対策などの周知 (管理者時の経験)	周知しても誰も読まない

表 3: 情報セキュリティ対策全般の不満と望ましい対策方法

項番	情報セキュリティ対策全般への不満	望ましい情報セキュリティ対策
1	無意味なチェック	管理者とのリスクの議論
2	多様な業務に応じていない	従業員からの意見収集の機能
3	トップダウンで決まる無意味なルール	何が必要で何が出来るのかの管理者との議論
4	難解なルール	具体的な事例の提示
5	世間に追従した対策導入	業務を止めない対策
6	いつの間にか作られるルール	全社員への通知
7	ルールを自分で探し出さなければならない	問い合わせ先の設置

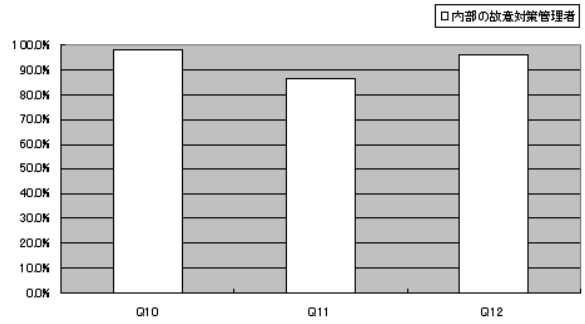

図 3: 情報資産の認定と管理実施状況

4 考察

4.1 定量的調査からの考察

定量的調査の結果から，内部者の故意対策管理者は，情報セキュリティ対策製品の導入だけで終わることなく，その対策実施の確認や，インシデント発生の把握までを高い割合で実施しているが，情報セキュリティインシデントが発生してしまっているという課題が有ることが分かった．

そして，対策についての従業員の意見から「他に守るべき情報がある」「その他に注意すべき脆弱性がある」という内容が見られている．これは，実施されている対策は，守られるべき情報と対処すべき脆弱性に漏れがあることを従業員が感じていると考えられる．この事から，対策における課題の原因は「情報資産の認定と管理」「脆弱性の特定」であることが考えられた．

そこで内部者の故意対策管理者の，情報資産の認定と管理および脆弱性の特定の実施割合を図 3 に示す．情報資産の認定 (Q10) を実施していると答えた管理者は，内部犯行の管理者の 98.1%であり，情報資産の管理 (Q11) は，86.5%が実施していると回答した．また，脆弱性の特定 (Q12) についても 96.2%が実施していると答えている．

この結果から,「情報資産の認定と管理」「脆弱性の特定」は，高い割合で実施されており，課題の原因は「情報資産の認定と管理」「脆弱性の特定」が実施されていない事ではなく，実施されている内容や方法であることが考えられた．

4.2 定性的調査からの考察

4.1 節では，定量的調査結果から内部者の故意対策にはインシデントの発生という課題があり，その課題の原因は「情報資産の認定と管理」「脆弱性の特定」の実施内容と実施方法であるという考察を述べた．

そこで本節では，それら定量的調査の結果に関連づけて，定性的調査の結果から，一般的な情報セキュリティ対策における「情報資産の認定と管理」「脆弱性の特定」の実施内容や実施方法の現状を分析し，課題の原因についての考察を述べる．

まず，情報資産の認定と管理について考察する．定性的調査結果から情報資産の認定と管理についての発言を確認することが出来た．それらからは，従業員には定められたルールに従う事が困難な状況であるという事が分かった．表 2 中の 1,2,3 の発言に示すとおり，情報資産の認定と管理のための対策「情報資産のラベル付け」について，そのルールを見つけ出すことが困難 (表 2 項番 1)，解釈が困難 (表 2 項番 2)，遵守が困難 (表 2 項番 3) であるという発言が確認できた．

これらから，情報資産の認定と管理の実施に当たって，まずルールを見つけることが出来ず，見つけたとしてもルールの内容を理解することが難しく，理解できたとしてもそのルールを遵守が困難であるという状況が考えられる．その結果として，管理者がルールを定めることで情報資産の認定と管理が実施されていると考えていても，実際にはそのルールは運用が困難であるため，守るべき情報資産に適切な管理が施されず，インシデント発生の原因となってしまう可能性が考えられた．

次に，脆弱性の特定について考察する．定性的調査の結果からは脆弱性の特定についての発言を見る事が出来なかった．しかし，脆弱性の特定を含むリスクアセスメントについての発言が見られた．それらからは，従業員の視点を含まないリスクアセスメントがされている現状が考えられた．表 3 の望ましい情報セキュリティ対策に示すように，リスクの議論 (表 3 項番 1) を望む発言や，何が必要で何が出来るのかの議論 (表 3 項番 3) というような，リスクアセスメントへの参加を望む発言が見られた．また,「世間に追従した対策導入」(表 3 項番 5) の様に，自組織のリスクアセスメントの結果ではない対策が導入されている現状を示す発言を見ることもできた．

これらの発言から，リスクアセスメントに従業員が参加しておらず，従業員の視点を含まないリスクアセスメントがされており，その結果として情報資産に関する脆弱性の中で特定されない脆弱性が存在してしまったり，優先して対処すべき脆弱性の対処が後回しにされるなどの状況が発生し，結果としてそれら未対処の脆弱性がインシデント発生の原因となっている可能性が考えられた．

4.3 従業員に望まれている解決策

4.2 節にて課題の原因が，ルール運用の困難さと，従業員の視点を含まないリスクアセスメントであるという考察を事を述べた．本節では，それ

ら原因について，従業員はどの様な解決策を望んでいるのか，ルール運用とリスクアセスメントそれぞれについて，定性的調査結果から考察する．

ルール運用　定性的調査結果から，情報資産の認定と管理のルールに限らず，ルール運用全般に関してその周知方法についての発言が見られた．具体的には「知らない間にルールが出来ている」(表 3 項番 6)「ルールを自分で探さねばならない」(表 3 項番 7)「ルールの場所を周知しても読まれない (管理者時の経験)」(表 2 項番 6) というような発言も見られたことから，いつ策定されているのか分からないルールを従業員が探し出す必要があるという状況であることが分かった．このルールの周知について,「30 分程度の試験がある」(表 2 項番 4)「ビデオ研修」(表 2 項番 5) の発言に見られるように，ルール策定に合わせてのテストや研修などで確認や周知を行っている発言が確認できた．しかし，それらの内容については「試験に通るために覚えてるので役に立たない」(表 2 項番 4)「研修の内容がそのまま出るだけで無意味」(表 2 項番 5)「具体的な事例があると理解しやすい」(表 3 項番 4) という発言があり，試験や研修によってルールの確認や周知を実施する際に，ルールを暗記させるような形式ではなく，従業員にとって具体的な事例を用いた方法を望んでいると考えられる．

リスクアセスメント　従業員の視点を含んだリスクアセスメントについては，2 つの方法が望まれていた．1 つは従業員から管理者へ意見を上げる仕組みを作ることである．表 3 項番 2 の発言にも見られるように，現在の情報セキュリティ対策に関して，従業員から管理者への情報伝達手段が無いことが考えられる．情報セキュリティ基準 JIS Q 27001:2006[2] では，PDCA サイクルにおいて利害関係者からの意見をインプットとすることが推奨されている．しかし，沼田ら [3] によると，この JIS Q 27001:2006 に準拠して情報セキュリティ対策を実施している企業 (ISMS 適合性評価制度合格企業) ですら，従業員からの意見収集の仕組みを用意している企業は 6 割程度であり，ISMS を取得していない企業では 3 割弱であることが述べられている．この事からも，多くの組織において従業員の意見を採り上げる仕組みが存在していないことが考えられ，それらの仕組みが望まれている．

また，表 4.2 の望ましい情報セキュリティ対策について表 3 項番 1,3 で示す様に，どの様な対策を取ることが可能なのかの議論を望む発言が見られ，具体的な方法として管理者と従業員によるグループディスカッションが上げられていた．これら

5　まとめと今後の予定

定量的調査と定性的調査を実施し，内部者の故意による情報セキュリティインシデントに対する企業の対策について課題と原因を考察した．

定量的調査結果から，内部者の故意による情報セキュリティインシデント対策において，管理者の強い取り組みの姿勢 (対策の実施把握は 92.3%，情報資産の認定は 98.1%，脆弱性の特定は 96.2%が実施) が伺えたが，情報セキュリティインシデントの発生という課題 (39.0%が経験) が見られることを示し，その原因が「情報資産の認定と管理」「脆弱性の特定」の実施内容と実施方法にあると考えられる事を述べた．

次にそれら「情報資産の認定と管理」「脆弱性の特定」が情報セキュリティ対策一般において，どの様な現状にあるかについて定性的調査結果を分析した．情報資産の認定と管理については運用が困難なルールが策定されており，その結果として守るべき情報資産が守られておらず，脆弱性の特定については，従業員の視点を欠いた脆弱性の特定が実施されており，その結果対処すべき脆弱性が未対処のままであると考えられる事を述べた．

さらにそれらの現状に対し従業員が望む解決策を考察した．ルールの周知において，従業員が理解しやすいような事例を用いた研修や試験と，リスクアセスメントにおける従業員の意見を採り上げるルートの構築等を望む発言が見られた．

今後の予定として，まず今回実施した情報セキュリティ対策一般の定性的調査で得られた内容が，内部者の故意による情報セキュリティ対策においても言えることの確認が必要であると考えている．

また，既に従業員の意見を採り上げる仕組みを設けている企業において，その実施の現状とその課題点を明らかにし，本調査で得られた従業員が望む解決策とそれらの現状と課題点を比較し考察することで，課題の原因に対する望ましい解決策を明らかにする事が出来ると考えている．

参考文献

[1] NPO 日本ネットワークセキュリティ協会,2008 年　情報セキュリティインシデント調査報告書 ver.1.2,2009 年 8 月 17 日

[2] JIS Q 27001:2006　情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項, 日本規格協会

[3] 沼田晋作　柴田賢介　岡崎聖人　高橋克巳，企業における情報セキュリティ基準と対策の関係に関する一考察,2008 年 7 月コンピュータセキュリティ研究発表会