内部不正による情報セキュリティインシデントにおける内部者の意識と対策に関する分析と考察

島 成佳 †

† 独立行政法人情報処理推進機構
113-6591 東京都文京区本駒込 2-28-8
s-shima@ipa.go.jp

あらまし 組織では，内部者の不正行為によって情報漏洩等のインシデントが発生している．しかし，内部者の不正行為は風評被害等の理由から表に出ることが稀であり，対策を講じるための情報共有も難しいことから，情報セキュリティの隠れた問題となっている．内部不正の特徴の 1 つは，正規のアクセス権を持つ者が不正行為を行うため，技術面や制度面からの対策のみでは防止が困難だということである．そのため，内部不正を行う気持ちを低減させる心理的な面からの対策も必要となる．本論文では，事例調査やアンケート調査から内部不正の実態解明の活動の一環として，職種における内部不正への意識と対策について分析・考察した結果を報告する．

A Study on Insiders' attitudes and Countermeasures about Information Security Incidents by internal illicit

Shigeyoshi Shima†

†Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, TOKYO, 113-6591 JAPAN
s-shima@ipa.go.jp

Abstract Information security incidents such as the information leakage occur by internal illicits in organizations. However, it is rare that information of internal illicits are disclosed because the organizations are afraid of damages such as bad reputation. Information sharing for countermeasures of internal illicits is difficult between organizations. Thus, internal illicit is one of the serious problems in the information security. One of the characteristics of the internal illicit is illicit of user with regular access right. Prevention of internal illicit is difficult only by the measures of technical aspect and management aspect, and measures of psychological aspect are necessary. In the paper, We report results that analysis and consideration about insiders' attitudes and countermeasures about internal illicit from case studies and a questionnaire survey.

1 はじめに

組織では，組織内部者の不正行為による情報漏洩等のインシデントが発生しており，企業や組織が対策に取り組むべき重要な課題の 1 つとなっている [1].

組織内部者による不正行為によって引き起こされるインシデントは，外部からの攻撃によるインシデントと比較すると発生頻度は低くあまり注目されていない．Verizon Business の報告

によると，2011 年の全データ漏洩/ 侵害事例で，外部からの攻撃によるものの割合が 95%であるのに対し，内部者によるものはわずか 3%しかない [2]．また，米国 CERT の報告によると，2010 年に発生したサイバー犯罪のうち，外部からの攻撃によるものが 73%であるのに対し，内部者の不正行為によるものが 23%であった [3]．しかし，外部からの攻撃によるものと，内部者の不正行為によるものについて，どちらの被害額が大きいかという質問では，外部からの攻撃が 38%であり，内部者による不正行為が 33%，わからないが 29%となっており，外部からの攻撃と内部者の不正行為による被害額への意識に大差がない [3]．内部者の不正行為では，組織内部者が価値のある情報や組織の機密情報，情報システム等の情報資産の場所を把握しており，それら情報資産へのアクセス権限を有していることから不正行為が発生すると被害が大きくなってしまうと推測される．このように組織では外部からの攻撃への対策のみでなく，内部者の不正行為にも対策していくことが重要である．

組織内部者の不正行為では，報道や判例で公開されている事件以外の裁判に至らない事件や組織のルール違反等の事件の情報は「風評被害が発生する恐れ」や「利害関係者との調整がつかない」等の理由から公開されることが稀であり，発生件数や傾向等の実態を掴むことが困難である．情報公開が困難なことは，独立行政法人情報処理推進機構の調査で，社員の不正行為によるインシデントを中立機関に情報提供可能かとの企業の経営者・管理者に対する問に，公開しないが 32%で，公開するがわずか 9%であったことから明らかである [4] (AppendixA 図-3)．また，経済産業省の産業構造審議会知的財産政策部会技術情報の保護等のあり方に関する小委員会からの報告において，内部者による営業秘密侵害行為に関する裁判で営業秘密を公開しなければならず，企業が告訴を断念してしまうケースが記述されており，ここからも情報公開が困難であることが伺える [5]．このように情報が少ないために実態が掴めておらず，情報共有も困難なことから，不正行為が発生する環境や効果的な対策等を十分に検討できないため，組織内部者の不正行為の防止は情報セキュリティの隠れた課題となっている．

本論文では，組織内部者の不正行為の効果的な対策を検討していくうえで必要となる実態を明らかにする基礎的なデータの提供を目的とし，独立行政法人情報処理推進機構の「組織内部者の不正行為によるインシデント調査報告書 [4]」のアンケート調査の Raw データを用い，職種ごとの不正行為やその対策への意識について分析・考察した結果について述べる．

2 既存の調査研究

国内外では，サイバー犯罪 (情報技術を悪用した犯罪) に係る内部犯行を事例をもとに，人的な面からの調査や研究が主になされている．

米国の CERT の Insider Threat Study Team[1]が，1996 年から 2002 年までに内部犯行の事例として 150 例を収集し，いくつかの部門の事例について分析を行い，内部犯行の予兆の検知，犯罪に対する防護のためのベストプラクティスに関して報告書を公表している [6]．この報告書では，内部犯行者の定義と内部犯行の分類を以下のように定義している．

■ 内部犯行者

- 現在もしくは過去の社員，その他の被雇用者もしくはビジネスパートナー
- 組織の IT システム (ネットワーク，システム，データ) への正規に認められたアクセス権を持っている，もしくは持っていた者
- 意図的にそのアクセス権を用い，組織の情報の機密性，完全性，可用性に対して負の影響をもたらした者

■ 内部犯行の 3 つの分類

- システム悪用 (Employee Fraud)
- 情報流出・情報アクセス (Information Theft)
- 情報破壊・システム破壊 (Sabotage)

[1]Insider Thread Center: http://www.cert.org/insider_threat/

また，国内でも財団法人社会安全研究財団がCERTの報告書を参照し，警察機関の有する事件資料30件の事例を類型化・分析して得られた知見による対策に関して報告書を公表している[8]．この報告書では，内部犯行の30の事例を多次元尺度法(Multi Dimensional Scaling)によって類型化し，CERTの「情報流出・情報アクセス」をさらに2つに分け，以下のように内部犯行を4つに分類している．

■ 内部犯行の4つの分類

- システム悪用
  組織の財やサービスをごまかし(deception)やぺてん(trickery)で手に入れる不正行為
- 情報流出I(道具的な犯行)
  情報セキュリティの違反行為が金銭的な利得を得るための不正，換金のための情報及びその他の情報や情報資産を獲得する不正行為
- 情報流出II(表出的犯行)
  蓄積した不満の発散や嫌がらせによる不正，情報の把握，持ち出し，公開等を行うことで心理的な優位性を保つなど，心理的満足のための不正行為
- 情報破壊・システム破壊
  特定個人，組織(含む組織のデータ，システム，日常業務)に損失を与えるという意志に基づいた悪意ある行為

本論文では，既存の調査研究のこれらの定義を参照して事例調査やアンケート調査を実施した．

3　本論文の内部不正

既存の調査研究は，法律によって禁じられた行為である犯罪によるインシデントを対象としている．

インシデント(情報セキュリティの事故)は，ハインリッヒの法則に当てはめることが可能である[9]．ハインリッヒの法則では，「1件の重大な事故・災害の背景には，29件の軽微な事故・災害が発生しており，300件のヒヤリ・ハット[2]が発生している」と言われており，重大な事故・災害を防止するために事故・災害のヒヤリ・ハットにも対処する必要がある．

本論文では，ハインリッヒの法則を参照して，犯罪によって発生したインシデントを重大な事故・災害とし，犯罪に至らないルール違反等の不正行為によるインシデントを軽微な事故・災害，ヒヤリ・ハットとして捉え，犯罪に加えてルール違反等の犯罪に至らない不正行為も対象とする．既存の調査研究では犯罪となる不正行為を「内部犯行」としていたため，本論文では犯罪以外のルール違反等を含む不正行為を「内部不正」と定義する．

内部不正の分類は，内部犯行を内部不正の中の大きな事故と捉えることから，小さな事故も同様の分類が可能であると考え，2節の「内部犯行の4つの分類」を流用し，「システム悪用」「情報流出I(道具的な犯行)」「情報流出II(表出的な犯行)」「情報破壊・システム破壊(破壊行為)」に分類する．

また，本調査では，2節の既存の調査研究の定義を参考に内部不正者の定義を以下のようにする．2節の内部犯行者の定義との違いは下線の部分である．事例調査において，パスワードの窃取による内部不正が見られたため，下線部のアクセス権のないものも含めている．

■ 内部不正者

- 現在もしくは過去の社員，その他の被雇用者もしくはビジネスパートナー
- 組織のITシステム(ネットワーク，システム，データ)への正規に認められたアクセス権を持っている者，及びアクセス権を持っていない者[3]
- 意図的にそのアクセス権を用い，組織の情報の機密性，完全性，可用性に対して負の影響をもたらした者

[2]重大な事故や災害に至らないが，重大事故につながりかねない事故寸前の危険な事例のこと

[3]アクセス権を持っているもの／持っていない者の両方であるため，定義する必要がないが，2節の定義と比較するために示す

4　事例調査

本論文では，内部不正の実態を把握するための事例調査として，判例調査とインタビュー調査の2つを実施した．判例調査では，判例データベースを利用して「営業秘密」「電気計算機」「流出」「アクセス」「背任」「詐欺」といったキーワードから内部犯行に該当するものを検索し，検索結果から最新の事例10件を抽出した．また，インタビュー調査では，インシデントの調査に関わったことのあるデジタル・フォレンジックの調査員，企業の情報セキュリティ担当者，法律家等へのインタビューから19件の事例を得た．

まず，判例調査とインタビュー調査で内部不正の分類ごとの件数比較を表1に示す．判例調査では，10件すべてが情報流出I(道具的な犯行)であった[4]．一方，インタビュー調査では，分類した4つすべての内部不正が見られる．判例調査と同様に情報流出Iが9件と一番多いが，割合は5割以下である．

表 1: 内部不正の分類ごとの件数

	システム悪用	情報流出 I	情報流出 II	破壊行為	分類不能
判例調査	0 件	10 件	1 件	0 件	0 件
インタビュー調査	1 件	9 件	6 件	1 件	2 件

インタビュー調査では，社員の属性として「一般社員」「システム管理者」「開発者」「管理職」「その他」が挙がっていたことからこの5つに社員を分類し，社員を軸に「対象物」「動機」「監視性」に関して整理したものを図2に示し，以下に傾向を述べる．

対象物とは内部不正で狙われた情報資産であり5つに分類した．また，動機とは犯行に至る原因となるものであり4つに分類した．監視性は業務に対する監視者が設定されていたかどうかを意味している．

判例調査では，開発者が5件で一番多く，次いで一般社員が3件であった．一方，インタビュー調査では，一般社員が10件と一番多く，次いで開発者とシステム管理者が3件であった．このことから一般社員や開発者によって発生する内部不正の割合が高い．

一般社員と開発者に注目すると，一般社員は顧客情報の持ち出しが多く，動機として判例では転職，インタビュー調査では不満や金銭が多い．一方，開発者は開発情報の持ち出しが多く，動機として転職が多い．一般社員と開発者では，「対象」や「動機」の傾向が異なっている．傾向の違いは扱う情報や社内での役割や立場の違いによるものと考えられる．そのため，一般社員や開発者では，効果的な対策が異なると推測される．

本論文では，職種の違いに注目し，事例調査の考察結果を考慮してアンケート調査に用いるシナリオを作成し，一般社員や開発者の意識の違いや，期待される対策に関するアンケート調査を実施した．

5　アンケート調査

本節では，事例調査をもとにシナリオと質問項目を設計し，アンケート結果をもとに分析した内容について述べる．

5.1　アンケート調査の概要

本アンケート調査は，アンケート調査会社に委託し，このアンケート調査会社の保有するモニター会員をアンケート参加者として実施したものである．

・サンプル数：3,000 件
・対象：社員 (非正規, 元社員, 経営者を含む)
・形式：Web アンケート
・期間：2012 年 1 月 13 日〜2012 年 1 月 18 日

本アンケート調査では，事例調査の結果から道具的な犯行に注目したシナリオとして，以下の技術職による開発情報の漏洩 (シナリオ I) と，営業職による個人情報の漏洩 (シナリオ II) の2つのシナリオに基づき，アンケート項目を作成した．

[4] 1 件は情報流出 I と情報流出 II(表出的犯行) の 2 つの要因を含んでいた

表 2: 判例調査結果 (n=10)

	対象物					動機				監視性	
	社内情報	顧客情報	ID・パスワード	開発情報	物理装置	不満	情報窃取	転職	金銭目的	高い	低い
一般社員	0	3	0	0	0	0	0	3	0	0	3
システム管理者	0	0	0	0	0	0	0	0	0	0	0
開発者	0	0	0	5	0	1	0	5	0	0	5
管理職	0	1	0	0	0	0	0	1	0	0	1
その他	0	1	0	0	0	0	0	0	1	0	1

表 3: インタビュー調査結果 (n=19)

	対象物					動機				監視性	
	社内情報	顧客情報	ID・パスワード	開発情報	物理装置	不満	情報窃取	転職	金銭目的	高い	低い
一般社員	2	3	3	0	1	6	0	0	4	3	7
システム管理者	1	2	0	0	0	0	2	0	1	1	2
開発者	0	1	0	2	0	0	1	2	0	1	2
管理職	0	1	0	0	0	0	0	0	1	0	1
その他	0	2	0	0	0	2	0	0	0	0	2

シナリオ I

情報システム企業 X 社に勤める A さんは，システム開発 2 課の主任になって 3 年になる．現在，A さんは，プロジェクトの開発を担当し，このプロジェクトを順調に進めていることを周囲から評価されていた．ある時，A さんは，上司に呼び出され，長時間の面談が行われた．その後，1 週間程度，同様の面談が頻繁に行われ，後日，A さんはプロジェクトから外れ，その月に任意退社した．後日，A さんが，自らが作成した開発物（ソースコード等）を一般公開されている Web サイト（掲示板等）に掲載したことが発覚した．その後，システム開発 2 課を含むシステム開発系部門では，開発物に関する管理規定が見直された．

■シナリオ I の質問項目

- 自らが作成した開発物を (ソースコード等) Web サイト (掲示板) に掲載するという行為にどの程度共感できますか (3 問，1. 非常にあてはまる〜5. 全くあてはまらないの 5 件法)
  Q1: 自分で開発したものであれば掲載しても良いと思う
  Q2: 見つからなければ掲載しても良いと思う
  Q3: A さんの行為に悪意は無いと思う
- A さんが開発物 (ソースコード等) を X 社の許可なしに一般公開することを防ぐための効果的な対策は何だと思いますか (20 問，1. 大変効果的である〜5. まったく効果的でないの 5 件法)

シナリオ II

B さんは，服飾系代理店である Y 社の営業系事務として，10 年以上勤務している．B さんは人当たりが良く，Y 社の営業職員や取引先の企業からも頼りにされることが多く，それに応えることに仕事のやりがいを感じている．周囲からは，仕事ぶりに華やかさはないがコツコツと地道にやっていくタイプだと見られている．そんな中，B さんを高く評価してくれている他社から転職の誘いがあり，転職を決意した．その後，B さんが Y 社の顧客情報を持ち出したことが発覚した．

■シナリオ II の質問項目

- 企業の許可なく顧客情報を持ち出すという行為にどの程度共感できますか (3 問，1. 非常にあてはまる〜5. 全くあてはまらないの 5 件法)
  Q4: 自分が収集したものであれば，持ち出してよいと思う
  Q5: 見つからなければ，持ち出してもよいと思う
  Q6: B さんの行動に悪意はないと思う
- B さんが Y 社の許可なく顧客情報を持ち出すことを防ぐための効果的な対策は何だと思いますか (20 問，1. 大変効果的である〜5. まったく効果的でないの 5 件法)

5.2 アンケート調査結果の分析と考察

アンケート調査結果から参加者の職種ごとに内部不正や対策への意識について分析する．

本論文では，技術職 (シナリオ I) と営業職 (シナリオ II) に関するシナリオを用いていることから，アンケート参加者の所属部門に関する属性情報をもとに，参加者を表 4 のように職種を営業職，技術職[5]，その他の 3 つに分類してアンケート結果を分析した．

表 4: アンケート参加者の 3 つの分類

職集	人数
営業職	904 人
技術職	1010 人
その他	1086 人
全体	3000 人

5.2.1 内部不正に関する意識

5.1 節のシナリオの共感に関する問 (Q1〜Q6) において，各職種の共感度合の平均値を表 5 に示す．技術職，営業職はその他の職種と比較して共感度合の値が低いことから共感度合が強いことが示唆された[6]．また，技術職と営業職のシナリオに注目すると，持ち出してもよいとする問 (Q1 と Q4, Q2 と Q5) において，技術職はシナリオ I (技術職) に営業職はシナリオ II(営業職) での値が低いことからより共感が強いことが示唆された．しかし，悪意はないとする問では，シナリオ I(技術職) で営業職の方が共感度合の値が低く，シナリオ II(営業職) で技術職の方が共感度合が低いという結果であった．

表 5: 各職種の共感の平均

	シナリオ I			シナリオ II		
	Q1	Q2	Q3	Q4	Q5	Q6
技術職	3.95	4.32	3.40	3.98	4.21	3.57
営業職	3.97	4.37	3.39	3.93	4.18	3.68
その他	4.12	4.41	3.51	4.05	4.29	3.75
平均	4.02	4.37	3.44	3.99	4.23	3.67

次に，各質問項目において，職種ごとで平均値の差が統計的に有意な差であるかどうかを u 検定 (Mann-Whitney 検定) によって確認し，検定結果を表 6 に示す．表 6 では，職種の頭文字で表した 2 つの職種ごとで検定している．ここでは 5%未満であれば統計的に有意差があるとし，「*」の印があれば 2 群において有意差あることを示している．以下で表 5 の結果とともに考察する．

表 6: 各職種ごとの 2 群における U 検定結果

	シナリオ I			シナリオ II		
	Q1	Q2	Q3	Q4	Q5	Q6
技ーそ	0.1 **	1.4 **	1.4 **	20.4	13.8	0.0 ***
営ーそ	0.2 **	24.0	1.4 *	3.2 *	2.5 *	17.1
営ー技	80.9	23.2	99.9	37.6	44.4	3.6 *

※ 表内の数値：(%)
Note:(有意確率) $***P < 0.1\%$ $**P < 1\%$ $*P < 5\%$

シナリオ I の Q2 とシナリオ II の Q5 に注目すると，Q2 において技術職は他の職種との間で差が見られた．技術職は他の職種と比較して表 5 の Q2 の共感度合の値が低いことから，見つからなければ開発物を Web の掲載してもよ

[5] ノウハウ等の技術的な情報を扱う製造，開発，研究部門の者を対象とした．

[6] 5.1 節の共感度に関する質問では，回答した値が小さいほど共感度が高い

いと感じていると推測される．同様に Q5 において，営業職は他の職種との間で差が見られた．営業職は他の職種と比較して表 5 の Q5 の共感度合の値が低いことから，見つからなければ顧客情報を持ち出してもよいと感じていると推測される．これらから社員は付いている職種の内部不正に対して甘くなるのではないかと考えられる．

シナリオ II の Q6 の結果に注目すると，技術職は他の職種と差が見られた．技術職は他の職種と比較して表 5 の Q6 の共感度合の値が低いことから，他の職種と比較して情報を持ち出して転職先で使うことに悪意を感じていないと推測される．

5.2.2 各職種の対策への意識

本論文では，5.1 節のシナリオの対策に関する問の 20 項目から，各職種の対策への意識について，図 1 (シナリオ I) と図 2(シナリオ II) に示し，考察する．

図 1 と図 2 ともにすべての対策項目において，3 つの職種とも効果の意識は同じ傾向である．ただし，技術職は他の職種と比較して，すべての対策項目の平均値が高いことから対策効果が低いと感じていることが示唆された[7]．営業職とその他の平均値は変わりない．

ここで，シナリオ I とシナリオ II で効果的な対策の 3 位までを表 7 と表 8 に示す．内部不正防止には，技術面の対策として情報システムの操作のログを記録し，ルール違反等を検出可能なシステムの導入が有効であると考えられる．また，運用面から，情報資産へのアクセスや持ち出しに関する運用をしっかりと行うことが有効であると考えられる．ただし，事例調査において対策を厳しくしたために業務に支障が出て内部不正が発生した事例もあり，厳しすぎる運用は逆効果にもなることに注意する必要がある．

[7]5.1 節の効果的な対策に関する質問では，回答した値が小さいほど効果が高いと感じている

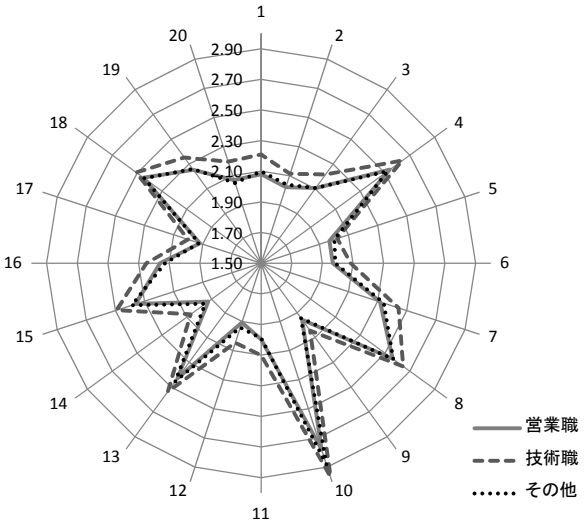

図 1: シナリオ I の対策に関する各職種の意識

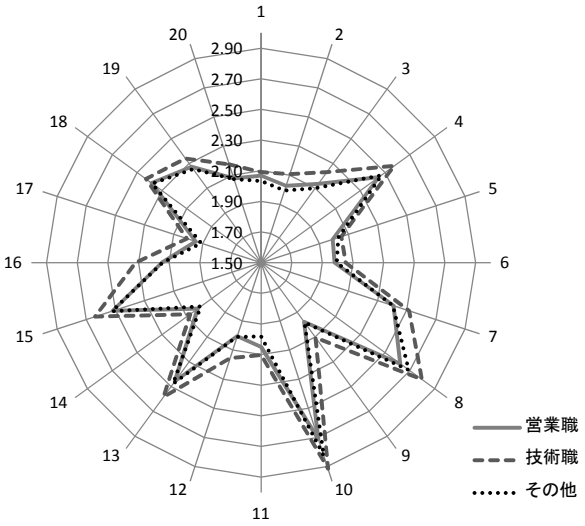

図 2: シナリオ II の対策に関する各職種の意識

表 7: シナリオ I の効果的な対策の順位

順位	アンケート内容	平均値
1 位	社内システムで行ったルール違反の痕跡を消すことが難しい (図 1 の 17)	1.95
2 位	退職者のアカウントは即日削除される (図 1 の 12)	1.97
3 位	社内システムにログインするための ID やパスワードの管理を徹底する (図 1 の 9)	1.98
3 位	CD や USB メモリ等の外部記憶媒体への書き出しや持ち出しが制限されている (図 1 の 14)	1.98

表 8: シナリオ II の効果的な対策の順位

順位	アンケート内容	平均値
1 位	社内システムで行ったルール違反の痕跡を消すことが難しい (図 2 の 17)	1.96
2 位	顧客情報を持ち出した場合の罰則規定を強化する (図 2 の 6)	2.01
3 位	社内システムにログインするための ID やパスワードの管理を徹底する (図 2 の 9)	2.02
3 位	CD や USB メモリ等の外部記憶媒体への書き出しや持ち出しが制限されている (図 2 の 14)	2.02

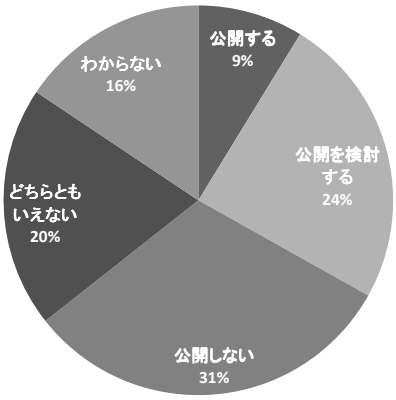

図 3: 公的・中立的機関への情報提供について

6 まとめ

本論文では，内部不正のアンケート調査をもとに，技術職，営業職，その他の 3 つの職種に分けて，内部不正や対策についての意識を分析・考察した．社員は付いている職種の内部不正を許容してしまう傾向があることや，効果的な対策がすべての職種で同じ傾向にあり，情報システムの操作記録をとることが有効な対策であるという等が分析・考察から得られた．

インタビュー調査では，関係者との守秘義務により事例の詳細内容を得ることができなかったため，内部不正の 4 つの分類を参考にさらに分類可能であるかどうかの分析ができなかった．今後，内部不正の実態を明らかにする上で，事例の詳細内容の提供が必要になると考えられる．

内部不正防止対策の活動では，これらの結果を含めた基礎的なデータをもとに，今後内部不正を防止する効果的な対策を明らかにしていきたい．

A 内部不正情報の公開について

発生したインシデント等が内部（社内及び関係者間）で解決できた場合に，公的または中立的な機関に対し,「個人や企業などが特定できない状態での公開」を条件に，有益な対策を検討する事例として情報を公開する可能性があるか (図 3)．

参考文献

[1] 独立行政法人情報処理推進機構: 情報セキュリティ白書 2012, P19-20, 2012.

[2] Verizon Business: 2012 DATA BREACH INVESTIGATIONS REPORT, 2012.

[3] CERT: 2011 CyberSecurity Watch Survey, 2011.

[4] 独立行政法人情報処理推進機構: 組織内部者の不正行為によるインシデント調査 調査報告書, 2012.

[5] 経済産業省: 営業秘密に係る刑事的措置の見直しの方向性について, 2009.

[6] CERT: Common Sense Guide to Prevention and Detection of Insider Threats, 2009.

[7] CERT: Insider Threat Study : Illicit Cyber Activity in the Information Technology and Telecommunications Sector, January 2008.

[8] 財団法人社会安全研究財団: 情報セキュリティにおける人的脅威対策に関する調査研究報告書, 2010.

[9] 内田勝也, 矢竹清一郎, 森貴男: 情報セキュリティ心理学の提案, 情報処理学会研究報告. CSEC 2007(16), 327-331, 2007.