Vol.2009-CSEC-46 No.38
2009/7/3

企業におけるセキュリティ管理者と従業員のセキュリティ対策への認識に関する現状調査報告

柴田賢介[†1]　沼田晋作[†1]
岡崎聖人[†1]　高橋克巳[†1]

現在多くの企業において様々なセキュリティ対策が導入されているが，情報漏洩等のインシデントは未だ後を絶たない．本研究ではこのような現状をふまえ，現在企業において実施されているセキュリティ対策の課題抽出を目的とし，企業におけるセキュリティ対策の現状調査を行なった．本調査ではまずリスクの特定からセキュリティ対策を実行するまでの過程のモデル化を行ない，モデル上の個々のフェーズにおけるセキュリティ管理者と従業員の現状認識について，既存のセキュリティ調査を対象とした分析およびヒアリングを実施した．本論文では調査の内容について述べるとともに，調査の結果得られた管理者と従業員との間での認識のギャップについて考察する．

A study on Security Recognition of Current Situation in the Business Organization

Kensuke Shibata,[†1] Shinsaku Numata,[†1]
Masato Okazaki[†1] and Katsumi Takahashi[†1]

In recent years, many companies implement security controls, but security incidents have increased. In this study, we have conducted a survey on security recognition of current situation to clarify the problems about security controls. The survey found that the gap of recognition exists between security administrators and employees. In this paper, we explain about the survey and consideration about the gap.

†1 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories

1. はじめに

現在，企業においては多くのセキュリティ対策が導入されている．企業において想定しなければならないセキュリティインシデントは，社外からのネットワークを介した攻撃や，社内からの情報漏洩など多岐にわたっており，これに対応する形で様々なセキュリティ対策製品が提案されている．

しかし，企業からの機密情報漏洩を例とすると，文献 1) に示されるように，2008 年度のインシデントの発生件数は前年に比べて増加する傾向にあり，現状のセキュリティ対策には課題があると考えられる．

そこで本研究では，企業におけるセキュリティ対策に関する課題を明確にすることを目的とし，その第一歩として現状の調査を行なった．調査に先立って，JIS Q 27001:2006[2)] において定められている ISMS(Information Security Management System) を参考に，企業におけるリスクの特定からこれに対応するセキュリティ対策の実行までの過程のモデル化を行なった．これを元に，モデル上の個々のフェーズにおける企業内のプレイヤの現状認識について，既存のセキュリティ調査の分析およびヒアリングという 2 種類の手法を用いて調査を行なった．

本論文では，まず 2 章においてリスク特定からセキュリティ対策の実行までの過程のモデル化について述べるとともに，今回の調査対象について言及する．3 章において調査方法，4 章で調査結果を示し，5 章において結果から得られた考察について述べる．考察では，セキュリティ管理者と従業員との認識のギャップについて言及する．6 章において今後の課題について述べ，まとめとする．

2. 調査の方針

本章では，今回実施した調査に用いた，企業におけるリスクの特定からこれに対応するセキュリティ対策の実行までの過程のモデルに関する説明と，本モデルを用いて行なう調査の対象について述べる．

2.1 企業におけるセキュリティ対策の過程モデル

1 章において述べたとおり，JIS Q 2700:2006[2)] において定められている ISMS では，セキュリティ対策を実行する際には，まず想定されるリスクを特定するために，守るべき対象となる情報資産を評価し，この資産に対しての脅威，そして脅威に結びつく脆弱性を特定する．以上から特定されたリスクに従い，これらのリスクを低減するためのセキュリティ対

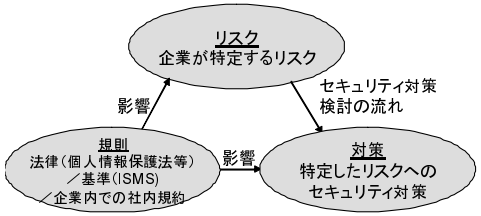

図 1 企業における規則-リスク-対策の関係
Fig. 1 Tripartite Relationship(Rules, Risks, and Security Controls)

策を策定し，これを運用することによって対策を実行していく．なお，リスクの特定からセキュリティ対策の実行までの一連の過程において，規則が影響を及ぼすことが考えられる．規則には，個人情報保護法等の法律や，プライバシーマークや ISMS 等の基準のほかに，当該企業において定められている社内規定といったものも含まれる．

以上から本研究では「規則」「リスク」および「対策」の三者の関係を図 1 のように示し，本調査においては特に「リスク」と「対策」に着目した調査を実施する．リスクと対策との間に生じうる課題としては，以下の三点が挙げられる．

(1) リスクを正しく特定できていない (リスク特定単独での課題)
(2) 特定したリスクに対応する対策になっていない (リスクー対策間の課題)
(3) 策定された対策を実行できていない (対策単独での課題)

ここで，リスク特定からセキュリティ対策実行までの一連の過程を図 2 のようなモデルとして表すこととする．図 2 は，上述したリスク特定を「情報資産の評価」「インシデントの発生確率の見積り」そしてその結果としての「リスクの特定」に分割し，特定されたリスクに従って,「必要と考える対策」を検討し,「実行する」という 5 つのフェーズから成る過程モデルとなっている．

規則に加えて，経営者や役員の一声，他社のインシデント発生状況などの他社動向といった要素も過程モデル上の個々のフェーズに影響を及ぼすと考えられるため，規則に加えてこれらの要因を外部要因として整理することとする．

本論文では，本節において定義したこのモデルを「リスク-対策過程モデル」とし (以後過程モデルと呼ぶ)，本モデルに示された 5 つの個々のフェーズにおける企業内のプレイヤの現状認識を調査することにより，リスク特定からセキュリティ対策実行までの間に生じている課題を明らかにする．

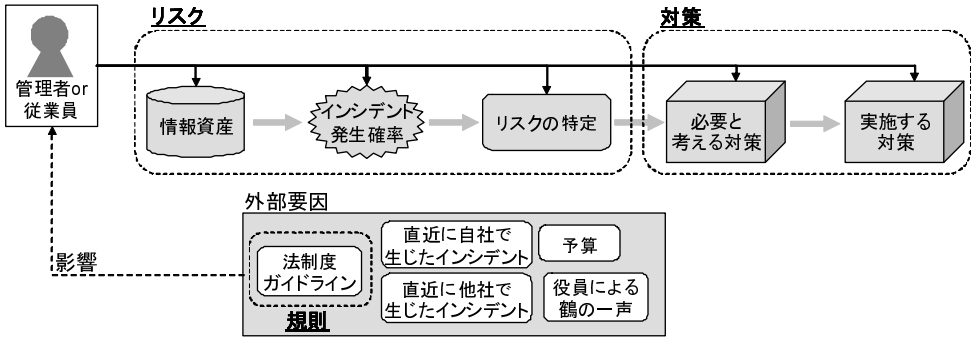

図 2 リスク-対策過程モデル
Fig. 2 Risk - Security Control Process Model

2.2 調 査 対 象

本節では 2.1 節において定義した過程モデルに従って企業内のプレイヤへの調査を実施する際に，調査対象となるプレイヤについて述べる．

企業においてセキュリティ対策が実施される際には，経営者やセキュリティ管理者，従業員など，企業内の様々なプレイヤが関わっていると考えられる．これを図にしたものが図 3 である．本調査では，図中のプレイヤの中でリスク特定から対策実行までの一連の過程を主体的に実行するプレイヤとして,「管理者」と「従業員」の 2 プレイヤを調査対象とした．

企業におけるセキュリティ管理者は，情報システム部門といった専門の部署に所属している人や，通常業務と兼任という形で，他の従業員に向けてセキュリティ対策を指導する立場の人など，企業によって様々な形態が考えられるが，当該企業において，セキュリティ対策を主導的な立場で実施している人を管理者とした．

従業員は，上記管理者の指導のもと，指示された対策を実際に実行したり，守るべき情報を取り扱う主体である．セキュリティ対策を策定する主導的な立場にはないため，リスクの特定や導入すべきセキュリティ対策の検討を実際に行なうわけではないが，個々の従業員においてもリスクの認識や，とるべき対策への認識はあると考えられ，過程モデル上で管理者と同様の調査を行なえると考えた．

3. 調 査 内 容

本章では，2 章において述べた調査方針に従って実施した調査の内容について述べる．図

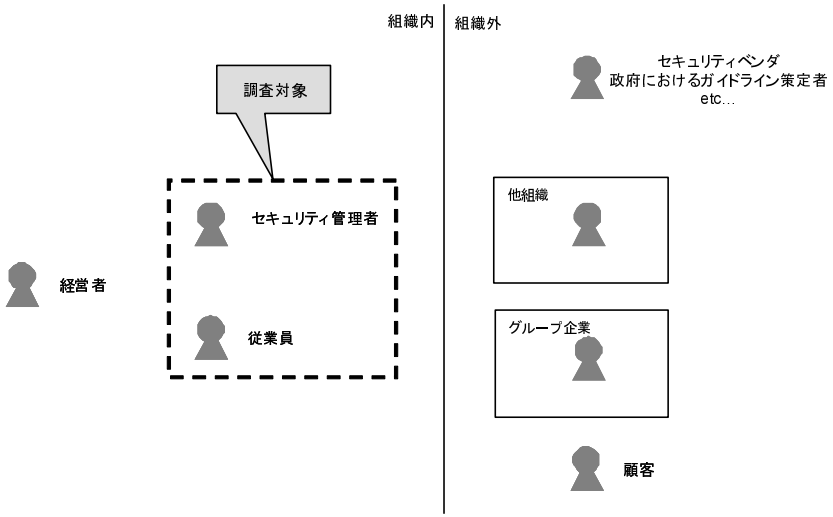

図 3 本調査の対象
Fig. 3 Scope of the Survey

2 に示す過程モデル上の各フェーズにおける管理者と従業員の現状認識を調査するため，今回は 2 種類の方法を用いた．

3.1 調査内容 1：既存調査分析

調査 1 として，2007 年から 2008 年にかけて行なわれた，企業におけるセキュリティに関する既存の調査報告について，本研究の観点で分析を行なった．分析対象は以下の 2 種類，6 件の調査である．

- 国内の公的機関が実施している調査
  - 「国内における情報セキュリティ事象被害状況調査」[3)]
    - 情報セキュリティ関連の被害実態及び対策の実施状況把握を目的とし，企業・自治体を対象として実施されたアンケート調査．
  - 「不正アクセス行為対策等の実態調査」[4)]
    - インターネット及び企業内ネットワーク上での不正アクセス行為の現状把握を目的とし，企業・行政機関等を対象として実施されたアンケート調査．
- セキュリティベンダーにおいて実施している調査
  - 「情報セキュリティに関するインターネット利用者意識調査」[5)]
    - 情報セキュリティに関するインターネット利用者の意識や行動の実態を明らかにすることを目的とし，一般利用者を対象として実施されたアンケート調査．
  - 「企業における情報セキュリティ実態調査」[6)]
    - 企業における脅威の認知，対策の実施状況把握を目的とし，情報システム・セキュリティ担当者を対象として実施されたアンケート調査．
  - 「メール誤送信に関する実態調査」[7)]
    - メール誤送信に関する実態把握を目的とし，仕事で電子メールを利用している人を対象として実施された調査．
  - 「組織でのインターネット管理実態調査」[8)]
    - 企業における Web アクセス管理の実態把握を目的とし，システム管理者を対象として実施されたアンケート調査．

表 1 管理者ヒアリングの対象企業
Table 1 Company List on the Security Administrator Hearing

企業番号	ヒアリング対象企業
1	ISMS 認証取得企業である IT 系事業者
2	企業グループ (電気メーカー) の親会社
3	企業グループ (食品会社) の子会社

上記調査の内容から，管理者と従業員のセキュリティ対策に関する認識について述べている部分をそれぞれ抽出し，2 章において述べた過程モデル上にこれをプロットする．

3.2 調査内容 2：ヒアリング調査

調査 2 では，ヒアリングによる調査を実施した．まず管理者に対するヒアリング調査としては，国内の企業 (表 1 に示す 3 社) に勤務し，管理者として業務を行なっている方 3 名に対し，現在導入されているセキュリティ対策とその効果についてのヒアリングを行なった．

今回ヒアリング対象となる企業を選定する際には，2.1 節において述べた外部要因の存在を考慮し，表 1 に示す企業を選択した．本調査では規則や他社動向のような，セキュリティ対策の検討に影響を及ぼす要素を外部要因として整理している．企業番号 1 の企業は外部要因として規則の影響を強く受けていると想定され，企業番号 2，3 の企業についてはグループ内の他の企業の動向を受けると想定されることから，これら 3 社を対象とした．

従業員へのヒアリングは，事前に Web アンケートを実施し，表 2 に示す条件を満たす 30 名を集め，表 3 に示すグループ構成にて，インタビュー形式での 2 時間のヒアリングを行なった．

Vol.2009-CSEC-46 No.38
2009/7/3

表 2 Web アンケートにおいて抽出した従業員の属性
Table 2 Provision of Employees' Attributes by the Screening

項目	条件	備考
年齢	25 歳以上 60 歳未満	入社後ある程度の年数が経過している従業員を抽出
業種	建設，製造，電気・ガス・水道，情報通信，運輸，卸売・小売，金融・保険，不動産，商社，印刷・出版	通常業務で情報システムを利用する可能性が高い人を抽出
規模	従業員が 30 人〜300 人以上を中小企業，300 人以上を大企業とし，これらの企業に勤務する従業員を抽出	〃
職種	営業，販売，研究，開発・設計，経理，総務，人事	〃
日常業務の形態	毎日 PC を使う	業務においてある程度の PC 利用経験がある人を抽出
リテラシ	メールや HP 閲覧，文章執筆に支障がないレベル以上	〃
ISMS 取得	勤務している企業が ISMS 認証を取得している	グルーピングに利用
インシデント経験	過去に自身もしくは身近でセキュリティインシデントを経験したことがある	〃
マネージャ経験	過去 5 年以内にセキュリティ対策を主導する立場にいたことがある	〃
対策への不満度	大変満足／満足／どちらでもない／不満／大変不満のいずれかを選択	〃
不満な理由	対策が厳しい／対策が見当違いである／対策が不足のいずれかを選択	〃

表 3 従業員ヒアリングでのグルーピング
Table 3 Group List on the Employee Hearing

番号	グループ名	グルーピングの目的
1	対策不満 (1)	対策が過剰だと感じている従業員の認識と抱えている課題を抽出
2	対策不満 (2)	対策が見当違いだと感じている従業員の認識と抱えている課題を抽出
3	マネージャ経験有	管理者と従業員の両面の立場から認識しているセキュリティ対策への課題を抽出
4	インシデント経験有	インシデントの経験前後での認識の差異を抽出
5	ISMS 取得企業	外部要因の 1 つである規則の影響を抽出

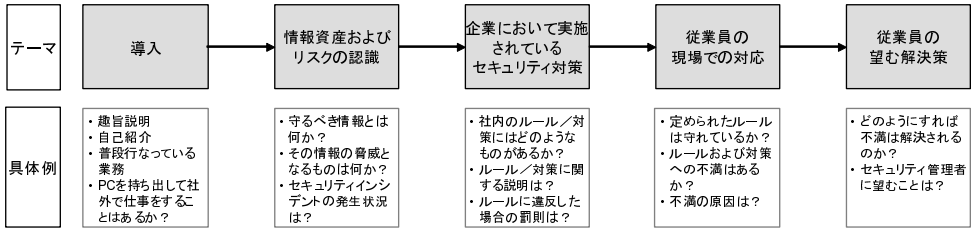

図 4 従業員へのヒアリングにおけるシナリオ
Fig. 4 Scenario of the Employee Hearing

後者の従業員に対するヒアリングについては，2 章において述べた過程モデルの流れを考慮し，図 4 に示すようなシナリオに従って，インタビュアーがそれぞれの参加者に対してヒアリングを行なうとともに，話の流れに応じてグループ内でフリーにディスカッションをしてもらう，といった形式での進行とした．発言がシナリオ中のどの時点のものであるかを記録し，得られた意見を過程モデル上へプロットした．

4. 調 査 結 果

4.1 調査 1：既存調査分析の結果

調査 1 として実施した，既存調査分析の結果を図 5 として示す．図中において先頭に「1)」と記載している部分が調査 1 によって得られた結果であり，個々の結果の末尾には文献番号を記している．調査結果から得られる代表的な知見としては，以下のようなものが挙げられる．

- 管理者側
  - 外部要因の中でも規則に対しての意識の高さが窺える一方で，「どの対策をどの程度までやるべきかが分からない」と考えている管理者も多く，具体的な対策を講じる上で，規則がその拠り所となっていない現状が窺える．
  - 管理者が定めたルールをその企業内へ浸透させる，もしくは導入した対策を企業内において適切に運用させることへの障壁が高いと言える．
- 従業員側
  - 企業内において定められたルールの存在を知らない，もしくはリテラシが低いといった理由で対策を適切に運用できていないケースが存在 (無知)．
  - ルールの存在を知っていながら，業務効率の低下などを理由にこれを遵守しない

プロセスモデル上のフェーズ	外部要因	情報資産の評価	インシデント発生確率の見積	リスクの特定	必要と考える対策	実施する対策
管理者	1)具体的な管理策が規定されているPCI-DSSをクレジットカード業界以外の企業が採用し始めている[6] 1)他社と比較して，自社の対策がどの程度のレベルにあるのかが気になると答えた管理者が41.3%存在[6] 1)対策立案・実施の動機として「法律に従う必要があるため」が33%[4] 1)情報セキュリティ対策実施上の問題点として，「どこまで行なえば良いのか基準が示されていない」が39.3%[4] 2)PDCAサイクルのC⇒Aについては，モニタリングの仕組みを導入するところまでは実施しているが，モニタリングによって抽出した情報の活用まで至っていない[1:ISMS]	1)対策立案・実施の動機として，「個人情報保護のため」が70%[4] 1)「重要情報」の定義には部門間での差があり，定義自体を部門や従業員に任せているケースも存在[3] 1)個人情報保護法の施行以来，個人情報が守るべき資産の中心となっていたが，今後は機密情報がターゲットになってくると考えている[3]	2)小規模なインシデントは常に発生している状況である．他社で発生した大規模なインシデントについても他人事とは思えない[1:ISMS]		1)情報セキュリティ対策推進にあたって困っていることとして，「対策をどの程度までやるべきなのかが不明」が49.5%[6] 1)情報セキュリティ対策推進にあたって困っていることとして，「有効性の評価方法が不明である」が34.8%[6] 1)持ち出しPCからの情報漏洩の危険性については89.9%の管理者が危惧しているが，持ち出しPCを禁止しているのは13.8%[8] 2)e-learningなどの一方的なセキュリティ教育は従業員にとって受動的なものとなってしまい，効果が薄い．能動的な教育を実施している[2:親会社] 2)アクセス権限の設定および管理を各部門に委譲したことがあったが，現場に混乱が生じた[3:子会社] 2)子会社ならではの悩みについてはそれほど感じていないが，コスト削減は常に意識している[3:子会社]	
従業員		1)電子メールに対する資産の評価が甘く，9割以上が誤送信の影響はないと考えている[7] 2)「守るべき情報は何か？」という問いに対しては，「個人情報もしくは機密情報である」といった回答が多数[全グループ共通]	2)「今後10年以内に自身がインシデントを発生させてしまう可能性があると思うか？」という問いに対して，「確実に1件は経験する」といった回答が多数[4:インシデント経験者]	2)左記，インシデント経験に関して，「10年以内にインシデントを発生させてしまう可能性は高いが，その後のフォローによってお客様からクレームが起きない程度に収めることができる」といった意見あり[4:インシデント経験者]	1)「ノートPCの持ち出しに関する社内ルールがあるか？」との問いに対し，「わからない」との回答が21.0%[5] 1)上記に関連して，持ち出し禁止のルールが存在することを知りながら，ノートPCを持ち出したことがある従業員が2.3%[5] 1)上記に関連して，ルールが存在しない状況下で，「必ず許可を得てからノートPCを持ち出す」との回答が2.3%[5] 1)「自宅においてパソコンを使って仕事を行なうことのデメリットは何か？」との問いに対し，「情報漏洩の可能性が高まる」との回答が62.2%[5] 2)インシデントを起こしてしまった場合，人事制度と連動しており，降格や異動といったケースが存在する[1:対策過剰] 2)厳しい対策を課せられているが，「仕方ない」と概ね受け入れる姿勢がある[1:対策過剰] 2)業務効率がある程度低下しても，セキュリティを重視することはやむをえない[1:対策過剰] 2)もっと現場を見てほしい．全部門に共通の対策を施さなくても良いのでは[2:対策見当違い] 2)パスワードは定期的に変更する等，ルールを完全に遵守しているつもりだが，うっかりメモ帳にパスワード一覧を記入してしまっていたこともある[3:マネージャ経験者] 2)セキュリティ加えて，利便性を高めてくれる他の機能がバインドされていれば受け入れることもある[4:インシデント経験者] 2)自身の会社のために情報資産を守ることが，ひいては自身を守ることにつながる[全グループ共通]	

図 5 調査結果
Fig. 5 Result of the Survey

ケースが存在 (無視).
- 従業員本人はルールを守っているつもりになっているが，実態としては守れていなかった，といったケースが存在 (無意識).

また，調査 1 における全体的な傾向として過程モデル上の上流に位置する情報資産の評価およびインシデントの発生確率の見積もりに関しては，既存調査においては言及されている部分が少ない，といった点も知見として挙げることができる．

4.2 調査 2：ヒアリング調査の結果

本節では，調査 2 として実施した，ヒアリング調査の結果について述べる．調査 2 の結果についても，調査 1 と同様に図 5 に示している．図中において先頭に「2)」と記載している部分が調査 2 によって得られた結果であり，管理者側に記載している内容が管理者ヒアリング，従業員側に記載している内容が従業員へのヒアリングの結果となっている．個々の結果の末尾には，管理者ヒアリングの対象者が所属する企業の種別を示す番号 (表 1) およびインタビュー時のグループ番号 (表 3) をそれぞれ記載している．調査 2 の結果から得られる代表的な知見としては，以下のようなものが挙げられる．

- 管理者側
  - e-learning などの一方的な教育によってルールや適切な運用方法を浸透させることに関しては限界を感じており，新しい教育の方法について模索している．
  - 規模の大小を問わず，インシデントの発生には敏感であり，他社の状況についても意識が高い．
- 従業員側
  - 様々なセキュリティ対策が企業内において施され，ルールも多数存在することにより，業務効率や利便性が低下し，不便を感じてはいるが，基本的には企業において定められたルールは守るべきもの，といった姿勢が窺える．
  - 上記の背景には，インシデントを引き起こすことによる罰則が人事制度と結びついているような厳しいケースや，会社のために情報資産を守ることがひいては自分を守ることになる，といった意識が存在している．
  - 自身が 10 年以内にインシデントを発生させる可能性について質問したところ，多数の回答者が「一度は起こす可能性がある」と答え，インシデント確率については高く見積もる傾向がある．これに対し,「何らかのインシデントを発生させたとしても，お客様からのクレームには結びつかないようなフォローが可能だ」といった根拠のない自信を窺わせる発言があったことから，リスクの認識については未成熟であると考えられ，インシデントの発生確率とリスクの特定には若干の隔たりが見られる．

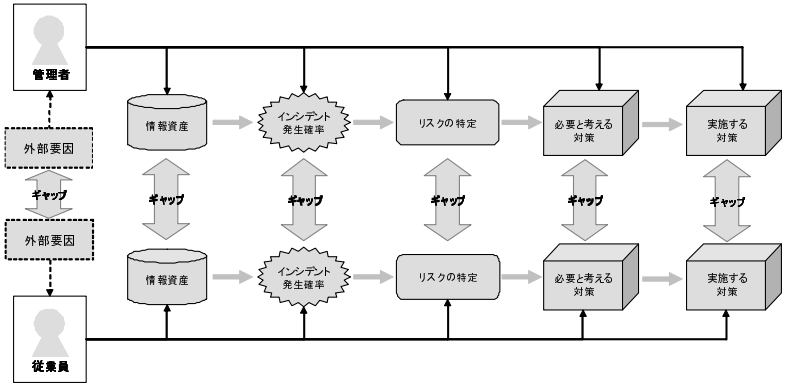

図 6 過程モデル上で表されるギャップ
Fig. 6 Gap on the Process Model

5. 考　　察

本節では，4 章の調査結果によって得られた管理者および従業員の認識について，その間に生じている認識のギャップについて着目し，考察を行なう．今回の調査の結果から，管理者と従業員との間に存在するいくつかの認識のズレを抽出した．本研究ではこれを認識ギャップとして定義する．これらのギャップは，過程モデル上のすべてのフェーズにおいて見られ，モデルとして示すと図 6 のようになる．

抽出した認識ギャップを過程モデル上に整理したものを図 7 として示す．特に興味深いギャップとしては，以下が挙げられる．

- 管理者は個人情報，機密情報等の情報資産に関する定義や，適切な管理を行なうためのランク分けを試みるなど意識の高さが窺えるのに対し，利用者側は電子メールに対する情報資産の認識が低いなど，情報資産の評価に対する認識は未成熟であると言える．
- 管理者は社内におけるインシデントや他社におけるインシデント動向について情報が集まっていることもあり，自社におけるインシデント発生の確率や重大なインシデント発生の可能性に対する認識が高い．これに対し，従業員は自身が原因となるインシデント発生の確率については高く認識しているが，これが重大なインシデントとなる可能性に

プロセスモデル上のフェーズ	外部要因	情報資産の評価	インシデント発生確率の見積	リスクの特定	必要と考える対策	実施する対策
ギャップ	＜ギャップ大＞ ・管理者⇒法制度／他社動向／経営者の鶴の一声といった外部要因を強く意識しており，セキュリティ対策策定の際にもこれらの外部要因の影響を受けている． ・従業員⇒外部要因に関するデータや発言がほとんど観測されなかった．	＜ギャップ大＞ ・管理者⇒情報資産のランク付けなど，意識は高い． ・従業員⇒電子メールに対する情報資産の認識の低さからも，資産の評価に関する認識は未成熟と言える．	＜ギャップ小＞ ・管理者⇒常に自社内のインシデントを経験しており，インシデント発生の確率は高く見積もる傾向がある． ・従業員⇒自身がインシデントを発生させてしまう可能性を認識しており，インシデントの発生確率については管理者同様認識が高いと言える．	＜ギャップ大＞ ・管理者⇒情報資産の評価およびインシデントの発生確率の両方に対しての認識が高いことから，リスクの評価についても認識が高い． ・従業員⇒インシデントの発生確率に関しては高く見積もっているが，「インシデントが起きても重大なものにはならない」といった根拠のない自信も窺うことができ，リスク評価に関する認識は未成熟と言える．	＜ギャップ大＞ ・管理者⇒リスクの評価に高い認識があると同時に，外部要因についても強く意識が働いているため，必要と考える対策については過剰となってしまう傾向がある．また，部門毎の事情に合わせたセキュリティポリシーの策定には消極的であり，全社一律でのセキュリティ対策としてしまう傾向も見られる． ・従業員⇒管理者に比べ，セキュリティ対策が自身の業務に直結するため，特に業務効率の低下や利便性の低下といった観点で不満を抱えるケースが多く見られる．また，各部門での情報資産の取り扱い状況に合わせて，セキュリティポリシーを策定してほしいといった意見も多数得られた．	＜ギャップ小＞ ・管理者⇒必要と考える対策については淡々と実施しているが，教育等によって企業内への浸透を図る方法を模索している． ・従業員⇒「必要と考える対策」には管理者との間に大きなギャップが見られるものの，最終的に対策を実施する段階では「仕方ないから言われたとおりに運用する」といった従順な姿勢が見られる．背景としては，人事制度と連携した厳しい罰則や，他社の動向などからの諦観などが考えられる．

図 7 管理者と従業員の認識ギャップ
Fig. 7 Gap of Security Recognition

ついては認識が低く，リスクの認識においては未成熟であると言える．

上記のような過程モデル上流に存在する認識ギャップは，下流における「必要と考える対策」において観測されているギャップへも強く影響していると考えられる．例えば，上流における認識ギャップの解消のための教育や新たな対策により，現在すでに実施されている対策をより効果的に運用していく，といった可能性も考えられる．このように，ギャップとその発生要因について分析を行なっていくことにより，企業におけるセキュリティの課題を抽出し，効果的な対策を検討する上での一助とできればと考えている．

6. まとめと今後の課題

本論文では，企業において導入されているセキュリティ対策の課題を抽出することを目的とし，企業におけるセキュリティ管理者および従業員のセキュリティ対策への認識について調査報告を行なった．企業内でのリスク特定からセキュリティ対策の実行までの過程をモデル化し，本モデルを元に既存のセキュリティ調査を対象とした分析およびヒアリングによる調査を行なったところ，管理者と従業員との間に認識のギャップが観測された．さらに，セキュリティ対策検討の上流工程と言えるリスク特定のフェーズでのギャップがその後の対策策定／実行に対しても影響しているのではないかとの示唆を得た．

今後の課題としては，まず今回の調査においては管理者および従業員それぞれに対して個別に既存調査分析，ヒアリング等を行なっており，管理者と従業員との間のギャップを言及するための客観的な調査としては不十分な点があると言える．そこでまずは同一企業における管理者と従業員との間での認識のギャップを測る，といった調査が必要になると考えられる．

また，今回はヒアリングによって個別に意見を聞くという形式での定性的な調査となっている．今後は対象を拡大しての定量的な調査を実施し，ギャップの大きさや，上流から下流に向けたギャップの影響度合いといった点についても考察を行なっていきたい．

参 考 文 献

1) 日本ネットワークセキュリティ協会: 2008 年上半期情報セキュリティインシデントに関する調査報告書【速報版】 (2008).
2) 日本工業標準調査会: JIS Q 27001 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 (2006).
3) 情報処理推進機構: 2007 年国内における情報セキュリティ事象被害状況調査 (2008).
4) 警察庁: 不正アクセス行為対策等の実態調査 (2008).
5) NRI セキュア: 情報セキュリティに関するインターネット利用者意識調査 (2008).
6) NRI セキュア: 企業における情報セキュリティ実態調査 2008 (2008).
7) HDE: 「メール誤送信」に関する実態調査 (2008).
8) ネットスター: 第三回「組織でのインターネット管理実態調査」 (2008).