Vol.2009-DPS-141 No.18
Vol.2009-GN-73 No.18
Vol.2009-EIP-46 No.18
2009/11/27

情報セキュリティ対策における コミュニケーションツールの活用に関する一考察

沼田　晋作[†1]　　岡崎　聖人[†1]　　高橋　克巳[†1]

企業にとって情報セキュリティ対策は，依然として重要事項である．企業ではそれら情報セキュリティ対策の実施における周知等に，メールや Web などのコミュニケーションツールを活用していることが考えられる．本論文では，情報セキュリティ対策の現状調査から，コミュニケーションツールを活用している情報セキュリティ管理者の対策実施状況について分析し，情報資産認定ルールの策定（84.3%実施) インシデント把握体制の確立 (80.0%実施) 対策製品使用割合の把握体制確立 (80.4%実施) 等を高い割合で実施している一方で，従業員意見収集体制確立 (38.2%の実施)，実インシデント発生件数把握 (32.6%の実施) 等となっており，従業員からの情報収集については，実施がされていないことを述べる．そして，それらの結果がコミュニケーションツールの活用における課題であることを考察した上で，関連する論文を参考として，解決の可能性について述べる．

A study of using communications tool in information security controls

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

The information security controls are still matters of weight for the enterprise. The communications tools such as mails and Web, have been used to inform for execution of those information security controls in the enterprise. In this thesis, analysis of the current situation survey of the information security controls shows that current situation of the information security controls in using the communication tools, the information security manager using the communication tools are, measures execution condition of the system of information asset recognition (84.3% execution) , incident grasp (80.0% execution) ,grasp of using the controls (80.4% execution) . While, a mechanism of the opinion taking up from the employee (execution of 38.2%), and the incident realities grasp (execution of 32.6%). It has been understood that execution is not done about the information gathering from the employee. It is considered that those results are problems in the use of the communications tool, using the relative thesis about a communications tools, it is descrived how to solve the problem.

1. はじめに

近年，インターネット等への情報流出事件等，様々な情報セキュリティインシデントが発生し，社会問題となっていると考えられる．このため，企業では情報資産を情報セキュリティインシデントから守るために，各種情報セキュリティ対策が実施されている．そして，その情報セキュリティ対策の実施において，企業の情報セキュリティ管理者は，対策製品の導入だけでなく，それら対策製品の利用方法の周知や利用実態の把握，インシデント発生時の連絡体制構築，社内のルール策定や従業員教育など，多岐に渡る業務を行う必要があると考えられる．[1)2)]

それらの業務では，管理者と従業員の間で様々な情報伝達が行われる必要がある．策定されたルールは，周知がされなければ従業員がそれを知ることが困難であるし，発生したインシデントは管理者に報告されることが望ましい．そして，それら管理者と従業員の間での情報伝達には，回覧・Web・メールなどのツールを使用していることが考えられる．

本論文では，これら情報セキュリティ管理者と従業員の間で情報伝達に使用されるツールを，コミュニケーションツールとして定義する．そして，それらコミュニケーションツールを用いて実施されている情報セキュリティ対策の実施状況を調査し，情報セキュリティ対策の実施におけるコミュニケーションツール活用の課題点を明らかにする．

2. 調査概要

本章では，本研究で分析を行った調査の概要を述べる．

2.1 調査方式

調査方式は Web アンケート方式とした．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．回答は選択肢の選択，数値の入力，自由記述のいずれかで行う．選択肢の選択はマウスを用いて行い，数値の入力や自由記述はキーボードを使用して回答を行えるように Web ページを作成した．

†1 NTT 情報流通プラットフォーム研究所

Vol.2009-DPS-141 No.18
Vol.2009-GN-73 No.18
Vol.2009-EIP-46 No.18
2009/11/27

表 1 情報セキュリティ対策の実施状況把握のための質問項目

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使用に関する周知方法
Q3	情報資産認定ルールの策定
Q4	対策製品使用割合の把握体制確立
Q5	インシデント発生把握体制確立
Q6	従業員意見収集体制確立
Q7	実インシデント発生件数把握
Q8	従業員意見の提示・受付経験
Q9	従業員意見の採用率

2.2 調査対象者

本調査では，企業における情報セキュリティ対策の管理者と従業員を対象に，Web アンケート調査を実施した．企業における情報セキュリティ管理者は，以下の条件を満たす回答者とした．

- 毎日 PC を使用する業務を行う
- 現在の企業に 3 年以上勤務している
- 現在勤めている企業に情報セキュリティ対策製品の導入を行ったことがある

同様に，企業における従業員は，以下の条件を満たす回答者とした．

- 毎日 PC を使用する業務を行う
- 現在の企業に 3 年以上勤務している
- 現在勤めている企業に導入された情報セキュリティ対策製品を使用している

2.3 調査項目概要

アンケートの調査項目は，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にまつわる，各種情報セキュリティ対策の実施状況に関する質問とした．用いた質問項目を表 1 に示す．表 1 に示したそれぞれの質問項目について，管理者と従業員それぞれについて，実施していると答えた割合をアンケートによって調査し，その結果を情報セキュリティ対策の実施率として利用することとした．

2.4 調査項目詳細

本節では，2.3 節で述べた質問項目について詳細な説明を行う．

2.4.1 Q1 情報セキュリティ対策製品

本調査では，企業に導入された情報セキュリティ対策製品を調査する質問項目を設けた．回答者に情報セキュリティ対策製品の一覧を表示し，管理者にはその中から実際に導入した情報セキュリティ対策製品を１つ回答してもらうこととした．従業員には，実際に導入されて回答者自身が使用している情報セキュリティ対策製品を１つ回答してもらうこととした．この際に，特定の情報セキュリティ対策製品に回答者の選択結果が偏ることが考えられた．選択結果に偏りが生じた場合，調査結果に特定の情報セキュリティ対策製品の影響が出てしまうことが考えられた．このため，表 2 のような製品分類を行い，製品分類毎に回答者数が平均的になる様に，回答者の選定（スクリーニング）を実施した．

表 2 製品分類

製品分類	製品例
メール関係	メールフィルタ，メールアーカイヴ，メール暗号化
Web 関係	Web フィルタ，オンラインストレージ
電子ファイル関係	電子ファイルアクセス制御 (DRM/持ち出し制御)，コンテンツフィンガープリンティング，ファイル暗号化，機密情報検索
記録媒体関係	HDD 暗号化，セキュアな外部記録媒体，データ完全消去
システムユーザ ID 関係	ID 管理，ユーザ認証強化（PKI），ユーザ認証強化（PKI 以外），証跡管理
ネットワークセキュリティ関係	社内 NW セキュリティ（検疫 NW,NBAND, 脆弱性診断），社外 NW セキュリティ(Firewall,UTM,WAF)
ストレージ関係	データバックアップ
物理セキュリティ関係	入退室管理，持ち出し管理

2.4.2 Q2 情報セキュリティ対策製品使用に関する周知方法

Q1 の回答である対策製品を使用して実施した情報セキュリティ対策の周知に，コミュニケーションツールが使用されているかどうかを調査した．本調査では，コミュニケーションツールとして，掲示板やメール・イントラネット上の Web など，管理者と従業員の間で情報伝達に使用される道具を想定した．そして，それらを用いて周知を実施した管理者を，情報セキュリティ対策にコミュニケーションツールを利用している管理者と判断した．また，コミュニケーションツールを使用して周知を受けた従業員を，コミュニケーションツールを利用している従業員と判断した．本論文においては，このコミュニケーションツールを利用している管理者と従業員を対象として分析を実施した．

2.4.3 Q3 情報資産認定ルールの策定

Q1 の回答である対策製品によって，各種情報セキュリティインシデントから守られている情報資産について，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．

2.4.4 Q4 対策製品使用割合の把握体制確立

Q1 の回答である対策製品を導入した後，実際にその対策製品を従業員が使用しているか

Vol.2009-DPS-141 No.18
Vol.2009-GN-73 No.18
Vol.2009-EIP-46 No.18
2009/11/27

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．

2.4.5 Q5 インシデント発生把握体制の有無

Q1 の回答である対策製品の導入によって防がれている，情報セキュリティインシデントが発生した時に，従業員からインシデントの発生を管理者へ連絡し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．

2.4.6 Q6 従業員意見収集体制確立

Q1 の回答である対策製品の導入後に，従業員から管理者へ意見を上げる仕組みを構築されているかを調査する質問項目である．

2.4.7 Q7 実インシデント発生件数把握

Q1 の回答である対策製品の導入によって防がれていた，情報セキュリティインシデントの実発生件数について，回答者が把握しているかを調査する質問項目である．管理者には自分が管理している組織の発生件数を把握しているか，従業員には自分が所属する組織の発生件数を把握しているかを回答してもらった．

2.4.8 Q8 従業員意見の提示・受付経験

Q1 の回答である対策製品の導入後に，従業員がその対策について意見を上げ，管理者が受けたかどうかについて調査する質問項目である．

2.4.9 Q9 従業員意見採用率

Q8 にて，意見を受けた事が有ると答えた管理者と，意見を上げたことがあると答えた従業員に対して実施した質問である．管理者には，従業員から受け付けた意見について，その意見を採用してその後の情報セキュリティ対策に意見の内容を反映したかどうかを答えて貰い，従業員には，管理者へ上げた意見について，その意見が採用されてその後の情報セキュリティ対策に意見の内容を反映されたかを答えて貰った．

3. 調 査 結 果

本章では 2.3 節と 2.4 節で説明した調査の結果について述べる．

3.1 管 理 者

本節では，管理者の回答結果について述べる．

3.1.1 回 収 数

アンケートでは 1741 人の管理者へ回答を依頼し，357 人から有効回答を回収した．その有効回答に対し，製品分布が均一になる様にスクリーニングを実施し 250 人の回答を調査対象データとした．この調査対象データの中で，掲示板や電子メールなどのコミュニケーションツールを用いたと回答した管理者は 102 人であった．以後はこの回答者を情報セキュリティ対策にコミュニケーションツールを用いた管理者として扱い分析を実施する．(以後，ツール利用管理者と記述する)

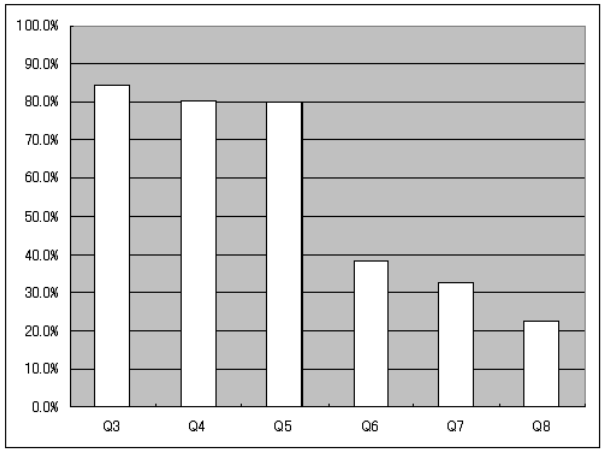

図 1 ツール利用管理者の情報セキュリティ対策実施状況 (管理者,n=102)

3.1.2 情報セキュリティ対策実施状況

ツール利用管理者について，調査から得られた情報セキュリティ対策実施状況を図 1 に示す．

各質問項目で確認した情報セキュリティ対策の実施状況について，次の様な結果となった．情報資産認定ルールの策定 (Q3) は 84.3%の実施率であり，対策製品利用割合の把握体制確立 (Q4) については，80.4%，インシデント発生把握体制確立 (Q5) についても 80.0%の実施率となっており，それぞれ高い実施率となった．この結果は，ツール利用管理者が情報セキュリティ対策の実施において対策製品の導入にとどまらず，その対策製品が守る情報の認定や，実施した対策の実施率，その対策製品の導入の結果であるインシデント発生件数についても，その連絡体制を確立して情報収集を実施しようとしている事が分かる．

しかしその一方で，実施率が 5 割を切るような結果も見られた．実インシデント発生件数把握 (Q7) を行っている管理者は 32.6%という低い結果となった．また，従業員意見収集体制確立 (Q6) については，38.2%が仕組みの構築を行っているが，従業員意見の提示・受付経験 (Q8) があるツール利用管理者は 22.5%という低い値となった．

Vol.2009-DPS-141 No.18
Vol.2009-GN-73 No.18
Vol.2009-EIP-46 No.18
2009/11/27

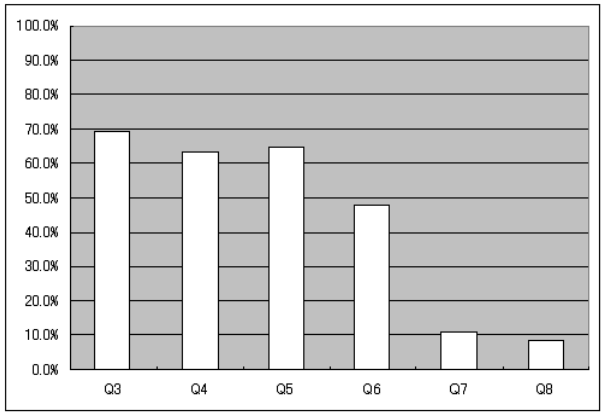

図 2 ツール利用従業員の情報セキュリティ対策実施状況 (従業員,n=117)

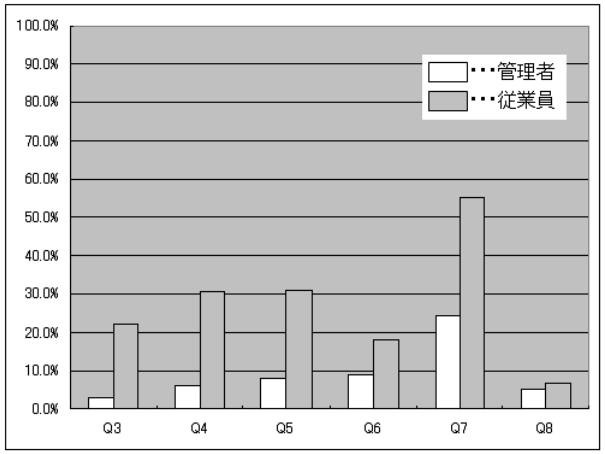

図 3 各設問において「わからない」と回答した回答者の割合

3.2 従 業 員

本節では，従業員の回答結果について述べる．

3.2.1 回 収 数

アンケートでは 4282 人の従業員へ回答を依頼し，417 人から有効回答を得ることが出来た．その 417 人の有効回答に対し，情報セキュリティ対策製品に偏りが出ない様にスクリーニングを実施し，250 人の回答を調査対象データとした．この調査対象データの中で，掲示板や電子メールなどのコミュニケーションツールを用いて周知を受けたと回答した従業員は 117 人であった．以後はこの 117 人の回答を情報セキュリティ対策において，コミュニケーションツールを用いられている従業員として扱う（以後，ツール利用従業員と記述する）．

3.2.2 情報セキュリティ対策実施状況

ツール利用従業員について調査結果から得られた情報セキュリティ対策実施状況を図 2 に示す．

従業員の回答結果も，管理者の回答結果と似た傾向が見られた．「情報資産認定ルールの策定 (Q3)」「対策製品使用割合の把握体制確立 (Q4)」「インシデント発生件数把握体制確立 (Q5)」については高い実施率となったが，「従業員意見収集体制確立 (Q6)」「実インシデント発生件数把握 (Q7)」「従業員意見の提示・受付経験 (Q8)」については低い実施率となった．

情報資産認定ルールの策定 (Q3) について 69.2%の実施率となった，対策製品利用割合の把握体制確立 (Q4) については 63.2%，インシデント発生件数把握体制確立 (Q5) の実施率については 64.5% という結果となった．

そして，従業員意見収集体制確立 (Q6) については，実施率が 47.9%であり，実インシデント発生件数の把握 (Q7) については，11.2%の実施率，従業員意見の提示・受付 (Q8) 従業員は 8.5%であった．

3.3 管理者と従業員に見られる実施率の差

従業員の回答結果を管理者の回答結果と比較したときに，従業員の結果の方が全体的に実施率が低くなっている．これは，回答者の中で選択肢「わからない」を選択した割合の高さが影響していると考えられる．各質問について「わからない」と答えた回答者の割合を図 3 に示す．従業員の立場にいる回答者にとって，情報セキュリティ対策の実施は，本来業務の手段であって目的ではないため，管理者よりも「分からない」という回答が多いと考えられ，本調査にて実施したスクリーニングが，管理者と従業員を分ける事が出来たために発生していると考えられる．

管理者が「わからない」と回答した割合は，多くの質問で 10%を切る割合であったが，従業員が「わからない」と回答した割合は，多くの質問で 20%を超える結果となった．

4. 考　　察

本章では，得られた調査結果から，情報セキュリティ対策実施状況におけるコミュニケー

Vol.2009-DPS-141 No.18
Vol.2009-GN-73 No.18
Vol.2009-EIP-46 No.18
2009/11/27

ションツールの利用状況を考察し，その利用状況に見られる情報セキュリティの面からの課題点，そしてその課題点に対して，関連研究で述べられている内容を情報セキュリティに適用する．

4.1 利 用 状 況

本節では得られた調査結果から，情報セキュリティ対策の実施における，コミュニケーションツールの利用状況について考察する．

4.1.1 管理者従業員間のギャップ

3.1.2 節と 3.2.2 節にて示したように，管理者と従業員双方で高い実施率となった質問項目は，情報資産の認定，対策の実施把握，インシデント報告におけるルールの策定と体制の確立であった．そして，低い実施率となった質問項目は，実インシデント発生件数の把握，従業員意見の提示や受付であった．この結果から，情報セキュリティ対策の実施におけるコミュニケーションツールの利用状況について，次の様なことが考えられる．

まず，情報セキュリティ対策の実施において，ルールの策定や体制の確立の様に，管理者から従業員への情報伝達を行う際にはコミュニケーションツールが活用されており，結果として情報セキュリティ対策の実施率が高くなっていると考えられる．

次に，インシデント発生件数の報告や従業員意見の受付の様な，従業員から管理者への情報伝達には，コミュニケーションツールがうまく活用されておらず，情報セキュリティ対策の実施率が低くなっていると考えられる．

特徴的な結果を，管理者の調査結果におけるインシデントの報告体制とその利用状況に見ることが出来る。管理者から従業員への情報発信によって，ツール利用管理者の 80.0%がインシデント報告体制を確立しているが，実際にその体制を利用して，従業員から管理者への実インシデント発生件数の報告を受けそれを把握している管理者の割合は 32.6%である．

4.1.2 従業員から管理者への情報伝達と伝達された情報の扱い

4.1.1 節で述べた通り，従業員が情報セキュリティ対策の実施においてコミュニケーションツールを利用できていない可能性が考えられた．その原因の一つとして考えられる調査結果として，従業員から管理者への情報伝達手段が確立されている割合も低いことが分かった．情報セキュリティに対する従業員の意見受付体制の確立については，管理者の調査結果では 38.2%の実施率であり，従業員の調査結果では 47.9%の実施率であった．さらに，従業員の意見を受け付けたことがある管理者は 25.5%であり，意見を上げたことがある従業員は 8.5%となった．

これらから，情報セキュリティ対策の実施において，従業員から管理者への情報伝達が行いにくい状況が考えられる．そこで，この上げられた意見についてどの程度採用されているのかを調査した (Q9)，調査結果から得られた意見の採用率を図 4 に示す．

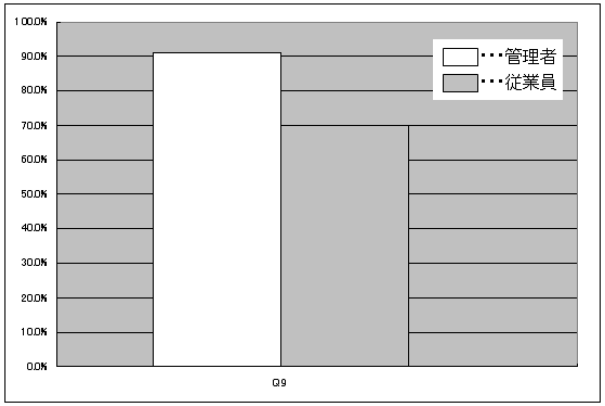

図 4 上げられた意見の採用率 (管理者 n=23, 従業員 n=10)

図 4 に示すとおり，上げられた意見の採用率が管理者は 91.3%であり従業員は 70%となり，高い採用率であることが分かる．つまり，現在の情報セキュリティ対策においては，管理者は従業員からの意見を収集しにくい状況であるが，その状況の中であげられた意見は採用される割合が高いと言うことが分かる．

4.2 利用状況に見られる情報セキュリティの面での課題

4.1 節にて，コミュニケーションツールの利用に関する管理者と従業員の活用状況について述べた．管理者から従業員への情報伝達にはコミュニケーションツールが活用され，情報セキュリティ対策の実施を行う事が出来ているが，それに反して，従業員から管理者への情報伝達にコミュニケーションツールを活用できていないと言うことが考えられた．本節では，そのような状況について情報セキュリティの面からの課題点を述べる．

4.2.1 情報セキュリティ対策の効果測定

4.1 節において，従業員から管理者への情報伝達にコミュニケーションツールがうまく活用できておらず，インシデントの実発生件数の把握について実施率が低いということが本調査結果から考えられると述べた．これは，情報資産を情報セキュリティインシデントから守っているかどうかという効果を挙げているのかどうかを把握できていないということであり，実施した情報セキュリティ対策の効果を把握できていないと言うことである．

Vol.2009-DPS-141 No.18
Vol.2009-GN-73 No.18
Vol.2009-EIP-46 No.18
2009/11/27

情報セキュリティ対策は，企業における情報資産を守ることを目的としており，上記の様な状況においては，自社の持つ情報資産を守れているのかが分からない．このため，効果の上がっていない情報セキュリティ対策を続けてしまうなどの課題が発生する可能性が考えられる

4.2.2 未対応のリスク

4.1.1 節において，従業員がコミュニケーションツールをうまく活用できていないだけでなく，従業員から管理者へ意見を上げる体制そのものが確立されていないことを述べた．これは，リスクアセスメント面での課題点となる．リスクアセスメントとは下記の項目に示す活動によって実施されるものである．

- 組織における情報資産の特定
- 報資産に潜む脆弱性の把握
- 脆弱性を活用する脅威の把握
- 脆弱性と脅威の組み合わせで発生するインシデントの把握
- インシデントの影響であるリスクを把握

そして，この一連の活動には，どの様な情報資産・脆弱性・脅威・インシデント・リスクが存在するのかという情報が必要となる．従業員は，日常の業務においてそれら情報資産を取り扱い業務を行っており，それら情報資産がどの様な情報を含んでいるのか，業務においてどの様に取り扱われていて，どの様な脆弱性や脅威が存在するのかを，管理者とは異なる視点での情報を持っていると考えられる．

従業員から管理者へ意見を上げる体制そのものが確立されていない場合，これら管理者が得にくい情報を従業員から管理者へ伝えることが出来ず，対策が採られるべきリスクであっても，未対策となっている可能性が考えられる．

4.2.3 セキュリティホール

4.1.2 節において，従業員から管理者へ情報伝達が行われにくい状況であり，その中で伝達された情報が高い割合で採用されることを述べた．今回の調査では，どのような意見をあげ，どのようなプロセスを経て採用されたたのかまでは把握できていない．このため，実際に採用された意見がどの程度組織の情報セキュリティ対策に影響を与えるものか，管理者が従業員から意見を受けた後にどのような追加調査や承認行為等を経て採用されているのかについてはわからない．

しかし，追加調査等が行われずに，一部の従業員の意見が採用されている場合，その従業員が悪意をもって意見を上げることによって，実施している情報セキュリティ対策にセキュリティホールが作成されてしまう可能性が考えられる．

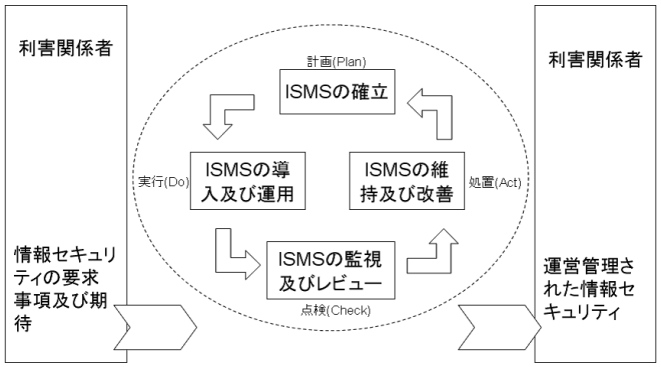

図 5 JIS Q 27001:2006 における PDCA サイクル (出典：JIS Q 27001:2006 *0.2.2* 図 1)

4.2.4 情報セキュリティ基準における従業員からの情報伝達の必要性

企業において情報セキュリティ基準に従って，情報セキュリティ対策を実施している企業は数多く存在する．その中でも，ISMS 適業性評価制度は 2009 年 10 月現在において，3296 の組織が認定を受けている．[3] その ISMS 適合性評価制度おいて利用される情報セキュリティ基準，JIS Q 27001:2006[4] では図 5 に示す様な，情報セキュリティ対策を PDCA サイクルに基づいて実施する事を推奨している．

これは，PDCA サイクルの実施において，利害関係者からの情報セキュリティの要求事項及び期待を受け，PDCA サイクルによって情報セキュリティ対策を実施していくことを推奨している．本調査によって明らかになった従業員からの意見を受け付ける体制がないことは，利害関係者である従業員の要求及び期待をそもそも受け付けられない可能性が考えられる．

情報セキュリティ対策の実施には JIS Q 27001:2006 に則る方法以外にも，様々な方法があるため必ずしもこの基準に記された PDCA サイクルの実施方法に従っている必要はない．しかし，JIS Q 27001:2006 にて述べられている PDCA サイクルの実施方法は，これまでの情報セキュリティ対策の実施における様々な検討結果であるため，その方法に信頼を置くことが出来ると考えられる．また，今後 ISMS 適合性評価制度を受けようと考える組織・企業や，JIS Q 27001:2006 に従った情報セキュリティ対策を実施しようとしている組織・企

Vol.2009-DPS-141 No.18
Vol.2009-GN-73 No.18
Vol.2009-EIP-46 No.18
2009/11/27

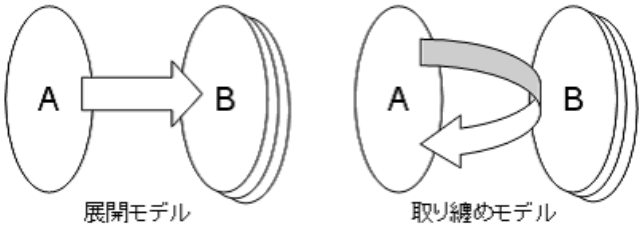

図 6 展開・取り纏めの伝達モデル (研究業務における取り纏め業務の考察[5] より引用)

業が 4.1 節で示した様な状況にある場合，大きな改善が要求されることが予測される．

4.3 関連研究からの知見

従業員から管理者への情報伝達にコミュニケーションツールが活用されていない状況を 4.1 節にて述べ，それが情報セキュリティの面における課題となっていることを 4.2 節にて述べた．本節では，そのような状況を解決するために，関連研究において述べられている内容から解決策を考察する．

4.3.1 展開と取り纏めのモデル

関[5] は，研究組織における本来業務とは異なる組織運営のための情報共有について，電子メール送信履歴の実データに基づいた分析を行った．その中で情報伝達のモデルを「展開モデル」と「取り纏めモデル」の２つを提示した．図 6 に展開モデルと取り纏めモデルの図を示す．図中の A は組織運営のための情報共有と取り纏めを仲介者として実施しており，情報セキュリティ対策の実施においては情報セキュリティ管理者と考えることが出来る．展開モデルは情報の一方的な展開で，返信を求めない物であり，取り纏めモデルは何らかの返信を求める物である．

情報セキュリティ対策の実施における情報共有は，文献[5] に述べられている本来業務とは異なる組織運営のための情報共有であると考え，本論文で取り上げた調査結果を，該当文献の提示したモデルに基づいて分析すると，情報セキュリティ対策の実施における，ルールや体制の構築は展開であり，その結果としてインシデントの発生有無や従業員からの情報収集は取り纏めに分類されると考える．そして，展開について情報セキュリティ管理者は実施できており，取り纏めに関して実施できていないという説明をすることが可能であると考える．

また，文献[5] によると，本務とは異なる業務に関する情報共有や取り纏めが，雑務と感じられやすいこと，このため，出来るだけ本務の支障にはならない様に，新たなインターフェースを構築するよりも，電子メールや社内 Web に限定すべきであると述べており，電子メールを Push 型 (非同期ではあるが強制的に配信される)，Web を Pull 型 (自ら見に行く必要がある) とし，利用者のスキルや情報の展開速度などの特徴があることを述べている．

情報セキュリティ対策も，本務とは異なる業務であり，それらに関する情報共有や取り纏めが雑務と感じられやすい可能性がある．このため，従業員から管理者への情報伝達に Push 型と Pull 型，及びインターフェースの特徴を踏まえたコミュニケーションツールの活用を考える必要がある．

4.3.2 社内 SNS の活用

情報の展開と取り纏めに使用するインターフェースの 1 つとして，社内 Web の一つである blog 等の SNS サービスが考えられる．企業にはそれらを社内 Web で提供し，企業内の情報共有等に役立てている企業が存在する．

古瀬[6] らは，blog から意見文を検索する手法を提案した．4.2.2 に述べた通り，従業員は管理者とは異なる視点でのリスクアセスメントに必要な情報を持っていると考えられる．しかし，それらをリスクアセスメントに必要な情報として従業員に記述させることは，リテラシや作業量の面からも困難である．しかし，blog を用いて自由記述を従業員が行い，その中から情報セキュリティに関する意見を，管理者が検索することは可能であると考える．

また，坂井[7] らは，それら blog に記述された不満表現から，ユーザが潜在的にもっているニーズを把握し，不満の解決策となる商品を結びつける提案を行った．これは，ある不満を解決した blog における単語の共起確率から，不満とその解決策の組合せを作成し，同じ不満が未解決な blog の記述者に対しその解決策を提示するというものである．これを情報セキュリティに適用すると，情報セキュリティに関してリテラシの高い従業員が書いた blog における単語の共起確率を元に，リスクアセスメントの各種情報 (脆弱性・脅威・インシデント等) の組合せを作成し，それをリテラシの低い従業員へ提示し，リテラシの高い従業員が書いた blog から得られた情報セキュリティに関する情報の確認を取る事によって，ある従業員が上げた意見について，情報セキュリティに関するリテラシが異なる従業員に確認を取ることが出来る．

この社内 SNS を活用する手法については，いずれにしても教師データが必要となり，それは情報セキュリティ管理者が実施する必要があり，その作業量が課題である．

Vol.2009-DPS-141 No.18
Vol.2009-GN-73 No.18
Vol.2009-EIP-46 No.18
2009/11/27

5. まとめと今後の予定

本論文では，情報セキュリティ対策の実施におけるコミュニケーションツールの課題について調査した．情報セキュリティ対策の管理者と，その情報セキュリティ対策を利用する従業員それぞれに Web アンケートによる定量的調査を実施した．コミュニケーションツールを活用している管理者，従業員の情報セキュリティ対策実施状況において，高い実施率の項目と，低い実施率の項目が見られた．

コミュニケーションツールを活用している管理者は，情報セキュリティ対策の実施において情報資産の認定を 84.3%の割合で実施しており,，対策製品利用状況の把握について 80.4%，インシデント発生把握方法の実施率について 80.0%という高いものであった．また，コミュニケーションツールの活用がされている従業員も同様に，情報資産の認定について 69.2%，対策実施の把握について 63.2%，インシデント発生把握に潰え 64.5%であった．

しかし，インシデントの発生について，実際に把握を行っている管理者が 32.6%であり，従業員意見受付の仕組みについては，38.2%，従業員の意見を受け付けた経験があるツール利用管理者は 22.5%という低い値となった．従業員も同様に，インシデントの有無を把握している従業員は 11.2%であり，従業員意見の受け付け体制は 47.9%であり，意見を上げた割合は 8.5%であった．

これらの結果から，情報セキュリティ対策の実施において，管理者から従業員への情報伝達は実施されているが，従業員から管理者への情報伝達がされていないというコミュニケーションツールの活用状況が考えられた．

これらコミュニケーションツールの活用状況について，情報セキュリティ的な課題があり，それは実施し対策の効果測定がされていないこと，リスクアセスメントの面で問題があること，情報セキュリティ基準 JIS Q 27001:2006 における PDCA サイクルの実施において必要とされる利害関係者の要求事項や期待をえら得られないなどの課題点を上げた．

そして，関連研究から情報伝達を「展開」と「取り纏め」という 2 つに分けて考えたとき，情報セキュリティ対策におけるコミュニケーションツールの利用が「展開」が出来ている一方で,「取り纏め」がされていないこと，その取り纏めを行うに際し，社内ブログを用いた SNS について効果が上げられる可能性について述べた．

今後は，今回確認された傾向について，被験者を大きくすることでその一般性を確認することである．また，コミュニケーションツールに関して Push 型や Pull 型であることの特性や，一般的に企業で用いられている電子メールと社内 Web について，情報セキュリティ対策におけるコミュニケーションツールとして使用したときの，それぞれの課題を明らかにする必要がある．また，本論文に紹介したモデルや方式について，有効かどうかを確認する予定である．

参 考 文 献

1) 日本ネットワークセキュリティ協会, 人的セキュリティと社内教育, http://www.jnsa.org/ikusei/foundation/educate.html
2) 総務省, 国民のための情報セキュリティサイト, 情報セキュリティポリシーの導入と運用方法, http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin12.htm
3) 財団法人　情報処理開発協会 (JIPDEC),ISMS 認証取得組織推移, http://www.isms.jipdec.jp/lst/ind/suii.html
4) 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
5) 関良明, 研究組織における取り纏め業務の考察, 情報処理学会研究報告,2008-GN-68,p43-48
6) 古瀬蔵, 廣嶋伸彰, 山田節夫, 片岡良治, ブログ記事からの意見文検索, 情報処理学会研究報告 Vol.2006 No.124
7) 坂井俊之, 藤村考, ブログに記述された不満表現からのの潜在ニーズの発見, 情報処理学会研究報告 Vol.2009-GN-72 No.8