Vol.2010-CSEC-51 No.7
2010/12/10

モチベーションマネジメントの情報セキュリティマネジメント分野への適用の提案

頼永　忍†

数々の情報セキュリティインシデントの報告資料から読み取れるのは,情報セキュリティ分野における喫緊の課題が従業員による内部要因であるということである.情報セキュリティや内部統制の管理策は原則としてシステム化すべきであるが,経済面等,様々な理由により,教育により従業員の行動を統制する選択をすることが多い.しかし直接的に利益につながるわけではない情報セキュリティ分野の取り組みについては,従業員におけるモチベーションが低下しがちである.本論文では,これまで製造業等で用いられてきたモチベーションマネジメントの,情報セキュリティ分野における有効性を論じ,その適用を提案する.

Proposal to apply motivation management to the information security management field

Shinobu Yorinaga†

Several reports about information security incidents say urgent problems of information security are caused by internal factors by employees. The countermeasures of the information security and the internal control should be systematized. The employee's behavior is often managed by the education because of various reasons like the economic situation etc. However, motivation in the employees tends to decrease about the approach in the information security field not connected with the immediate profit of the company. Up to now, the motivation management has been applied by manufacturing field. This paper discusses the effectiveness of the motivation management in the information security field, and I propose the application for that field.

1. はじめに，研究の背景

情報漏洩をはじめとした情報セキュリティインシデントの発生は,組織の懸案となり続けており,対策に頭を悩ませているところである.セキュリティインシデントには外部要因（外部からのアタック等）と内部要因（置き忘れ,操作ミス等）がありる.企業及び自治体に調査を行った「「2008 年 国内における情報セキュリティ事象被害状況調査 」報告書(N = 2,317)」[1]によると,「機関内部の不正者による重要情報の流出」「委託先の不正者による重要情報の流出」共に 1%強の企業で発生している.

また,情報セキュリティ対策についてはシステム化するなどの,ミスに対するフェイルセーフ機構を導入することが望ましいが,導入はあまり進んでおらず,最も進んでいる「ウェブ閲覧のフィルタリング」で 40.7%という状態である.また,「「2009 年度情報セキュリティの脅威に対する意識調査」報告書」[2]では,情報セキュリティ対策を実施しない理由の上位に「費用がかかる」が挙げられており,また組織の情報セキュリティ対策は現実として従業員の自身のモラル向上,ポリシーの教育・啓蒙に多くを頼っている,あるいは頼らざるを得ない状態であるということができよう.しかし,教育の効果には限界があると言われて久しい.まして情報セキュリティ分野は直接利益を生む分野ではないため,セキュリティ教育がいわゆる「不便の押し付け」「やらされている」と感じられてしまい,モラルハザードを促進し,セキュリティインシデントの引き金になってしまう可能性すらあり得る.

そんな中,近年モチベーションマネジメントの考え方が改めて注目されているところである.モチベーションとはつまり「動機付け」であり,自発的な行動を促す要素であるが,先述の通り情報セキュリティは「やらされ感」を感じさせやすい分野であり,また各個人の行動がセキュリティインシデントに直結する分野であることから,モチベーションマネジメントとの相性がよいと考えた.

セキュリティ対策においてシステム化できなかった部分をどのように補完するかは,非常に多くの組織が頭を悩ませているところであるが,情報セキュリティ分野へのモチベーションマネジメント手法を確立し,適用することで,従業員の負担感を軽減しながら,またセキュリティインシデントの低減へ貢献できるのではと考え,本提案に至ったところである.

2. モチベーションマネジメント

2.1 歴史

モチベーションマネジメントの歴史は新しいようで相当に古い.

†情報セキュリティ大学院大学
Institute of Information Security

ピラミッドは奴隷によって建立されたと言われていたが,最近では公共事業であったとの説が有力視されている.加えて,この 20 年でピラミッド建設に携わった労働者の墓がピラミッド近辺で発見されるなど,労働者への待遇が決して悪い物ではなかったことの裏付けが示されはじめている.

ギザの大ピラミッドで言えば,完成時の高さ 146.6m,完成までの歳月は 20 年以上という,いろいろな意味での超巨大プロジェクトである.このプロジェクトを遂行する中で,プロジェクトマネージャは人心を掌握し,モチベーションを長い間高く保つ必要があったはずである.これはまさにモチベーションマネジメントであったといえよう.

ギザのピラミッドの建立は紀元前 2540 年頃と言われ,先述の仮説が正しい物であるならば,実に 4500 年以上前からモチベーションマネジメントの必要性がプロジェクトマネージャに意識されていたことになる.

2.2 先人の研究

モチベーションマネジメントが体系立って研究され始めたのは,先進国において第二次産業から第三次産業への転換が始まった 20 世紀中頃からである.その中で

- アブラハム・マズロー:「自己実現理論（欲求段階説）」[3]
- マクレランド:「マクレランドの欲求理論」[4]
- フレデリック・ハーズバーグ:「動機づけ衛生理論」[5]
- アルダーファー:「ERG 理論」[6]

等,数々の理論が打ち立てられた.多くの理論が「自己実現理論」（図 1）をベースとしており,生存欲求から社会的（外的）欲求,自己実現（内的）欲求へと進んでいく構成と解釈できる.

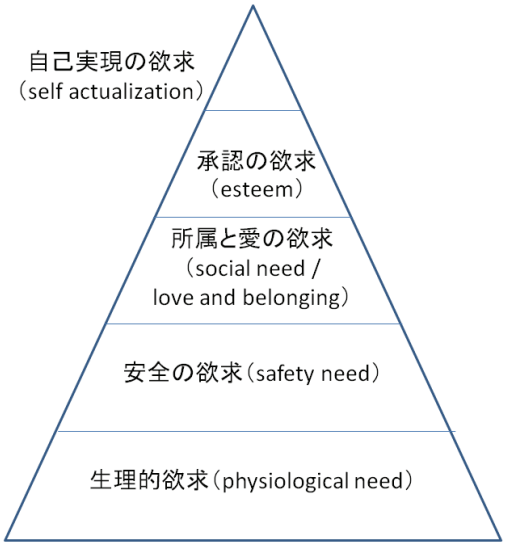

図 1　アブラハム・マズローの欲求段階説

2.3 モチベーション 3.0

ダニエル・ピンクは 2009 年（日本では 2010 年）,「Drive!」を刊行[7].「Motivation 3.0」という考え方を披露した.その中で「モチベーション OS」という考え方に触れ,それぞれの OS を

- 【モチベーション 1.0】: 生存を目的としていた人類最初の OS.
- 【モチベーション 2.0】: アメとムチ＝信賞必罰（ある種の行動に対して褒美を出せば,その行動が増え,ある種の行動を罰すれば,その行動が減る）に基づく与えられた動機づけによる OS.
- 【モチベーション 3.0】: 自分の内面から湧き出る「やる気」に基づく OS.

と解説している.これもまたマズローの自己実現理論に近い考え方である.

しかしダニエル・ピンクは必ずしもモチベーション 3.0 がすべてに適用しうるとは述べておらず,信賞必罰的なモチベーション 2.0 がフィットする場合もあると強調し,またモチベーション 3.0 と 2.0 を使い分ける条件は「本人の欲求の充足度」ではなく「従事している業務の種類」であるとし,この点でもマズローとの差違がある.

3. 情報セキュリティ

3.1 インシデントの内部要因分析

IPA「情報漏えいインシデント対応方策に関する調査」[8]（2007 年 8 月）によると組織のセキュリティインシデントのうち「紛失・盗難」「P2P による漏洩」「誤送信」「内部犯行」の合計で全体の 8 割以上を占めており,外部からの不正アクセス等は 1 割強に過ぎない.（図 2）

これらの内容を「ミス」と「意図的犯行」に分けると,「ミス」が 46%,「意図的犯行」が 40%となり,「ミス」の方が高頻度であることがわかる.これらを総合すると,組織のセキュリティインシデントの低減に向け重要なことは「ミスの低減」であると言える.

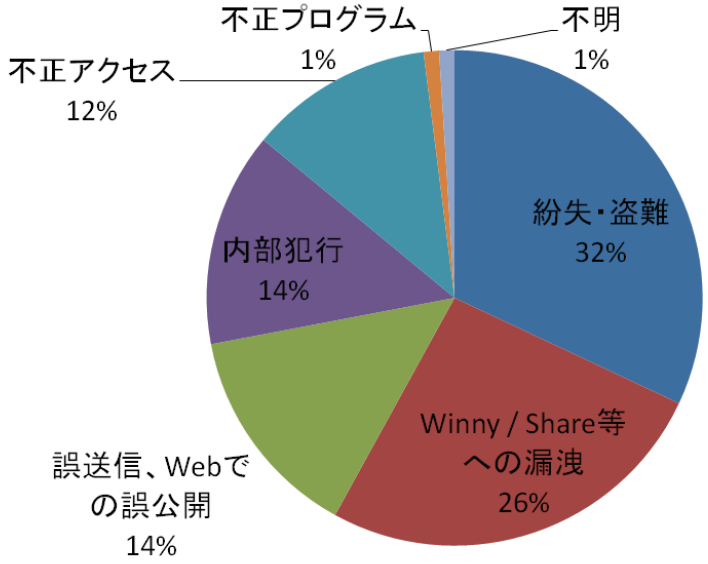

図 2 インシデントと内部要因

3.2 インシデント低減策の現状

日本において,企業の 99%以上,従業員数の 70%以上を中小企業が占めている.[9]中小企業におけるインシデント低減策については,IPA 発行「中小企業における情報セキュリティ対策の実施状況等調査報告書」にまとめられている.

報告書によると,中小企業の多くは,ルールの策定,教育による徹底が中心であるか,あるいはルールの策定自体すら十分にされていない状態である.

大企業は比較的情報管理がしっかりしているものの,その業務の委託を受ける中小企業の情報管理の状態が不十分であっては,結果的に委託先の中小企業から情報漏洩が起こることになる.

中小企業の情報セキュリティインシデント対策に対するニーズはどのようなものであるのだろうか.

3.3 セキュリティ対策のニーズ

3.2 に上述した調査で実施されたヒアリング調査の回答内容を下記に示す.

> ・IT投資そのものは行うつもりであるが,セキュリティについては,コストのかからない,社員の教育や啓蒙といった部分の対応を考えて行きたい.
> ・現場や上層部とコンセンサスがとれていない.投資に関して,セキュリティのみでの投資には上層部も積極的ではない.
> ・システムの投資は難しい.売上に貢献しないセキュリティ投資は後回しの可能性があるために,投資してセキュリティレベルを上げるというより,まずは意識付けからやっていきたい.

「情報セキュリティについての重要性,課題について」の回答内容

「教育」「啓蒙」「意識付け」の言葉が並んでいる.

こと中小企業においては,業務を運営していくことが最優先であり,セキュリティに関しては「できるだけ低いコストでリスクを低減したい」というニーズが非常に強いことが伺える.

3.4 システム化以外のセキュリティ対策

費用を掛けないセキュリティ対策として取られる対策,統制は,主として「教育・啓蒙による逸脱行動の抑止」である.

具体的な伝達内容は以下の要素がある.

- ルール・ポリシー
- 操作手順

- 過去のネガティブ事例（事故例等）
- ペナルティの内容
- ペナルティの実施による草の根伝達（一罰百戒）
-

3.5 教育の限界,ミスの要因

教育・啓蒙により,従業員を統制しようという活動は全国的,全世界的に行われているが,必ずしも組織が望むようにインシデントが低減しているとは言い難い状態である.

この理由の一つが,「ミスの自発的な低減には限界がある」と言うことである.自発的にミスを犯す従業員がほとんど居ないことは自明であるが,ミスをゼロにすることは不可能に近いこともまた自明である.ミスの要因として集中力の低下,モチベーションの低下等が言われている.先述の通り,セキュリティ教育は売り上げに直接貢献しづらく,また多くの場合は業務効率の低下につながっている.そのため従業員側に「やらされ感」が芽生え,ポリシー,ルールに従うモチベーションが低下し,操作ミスによる誤送信や置き忘れ等が発生すると考えられる.

4. モチベーションマネジメントの導入

4.1 モチベーション OS と情報セキュリティ

ダニエル・ピンクの提唱するモチベーション OS の考え方は,非常に明快で,「「ルーチン業務」には信賞必罰（アメとムチ）の OS 2.0 を適用し,「クリエイティブ業務」には OS 3.0 を適用すべし」というものである.

情報セキュリティの運用における「やらされ感」は特に日々の運用である「マニュアル通り実施する」というルーチン業務に対するメリットが無いことにも由来していると考えられる.ではアメを与えればよいかというと,その効果は回を追うごとに低減していくと言うことも同時に言われており,セキュリティ運用のように恒久的に継続する取り組みについては,別の角度から,より長期的な展望を持つアプローチを選択する必要がある.

4.2 情報セキュリティマネジメントフレームワークへの適用

情報セキュリティマネジメントのフレームワークとして,ISO/IEC 27001[11]がよく知られている.この中のリスクマネジメントプロセスには,先述した,決定された対策に従って行動する「ルーチン業務」に加え,リスクを分析し,その対策を立案するという「クリエイティブ業務」が混在していると考えられる.（図 3）

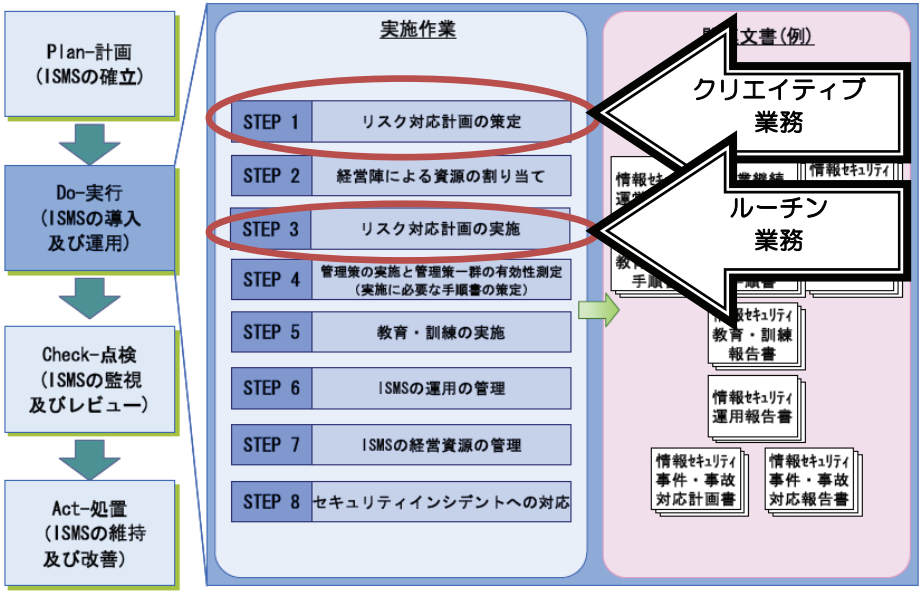

図 3 「ISMS の導入及び運用」の手順と業務の種類
(ISMS ユーザーズガイド[12]より引用)

言い換えると,一つのプロセス中に,OS 2.0 的業務と OS 3.0 的業務が混在している.リスク分析によって洗い出された組織のリスクに対し、リソースをどのように配分し、最適な対策を立てていくかを検討する業務は、非常に「クリエイティブな業務」であり、決してルーチン的な業務ではない。しかし、図 3 STEP 3 に見られるような「リスク対応計画の実施」は「決まった対策を粛々と実行していく業務 ＝ ルーチン業務」と見なされがちである。

このようなことから、情報セキュリティ分野、こと実施・運用フェーズにおいては「やらされ感」「希薄なメリット」などによるモチベーション低下が見られる.これはモチベーション 2.0 的な動機付け要因が不足していることが一因とも考えられる.

また,リスク対応計画の策定とそれを実行する人員が分かれてしまっていることも「やらされ感」を受ける一因であろう.

4.3 プロセス,モチベーション OS の一本化

しかし,情報セキュリティの運用フェーズにおいて,信賞必罰の「賞」を与えることにはどうしても限界があり,モチベーション 2.0 的な動機付け要因を満たすことが難しい.

そこで,リスクマネジメントプロセスの「リスク対応計画の策定」,「リスク対応計画の実施～ISMS の運用の管理」を一つのクリエイティブ業務を行うプロセスとして取り扱い,モチベーション 3.0 的なモチベーションマネジメント手法を導入することを提案する（図 4）.

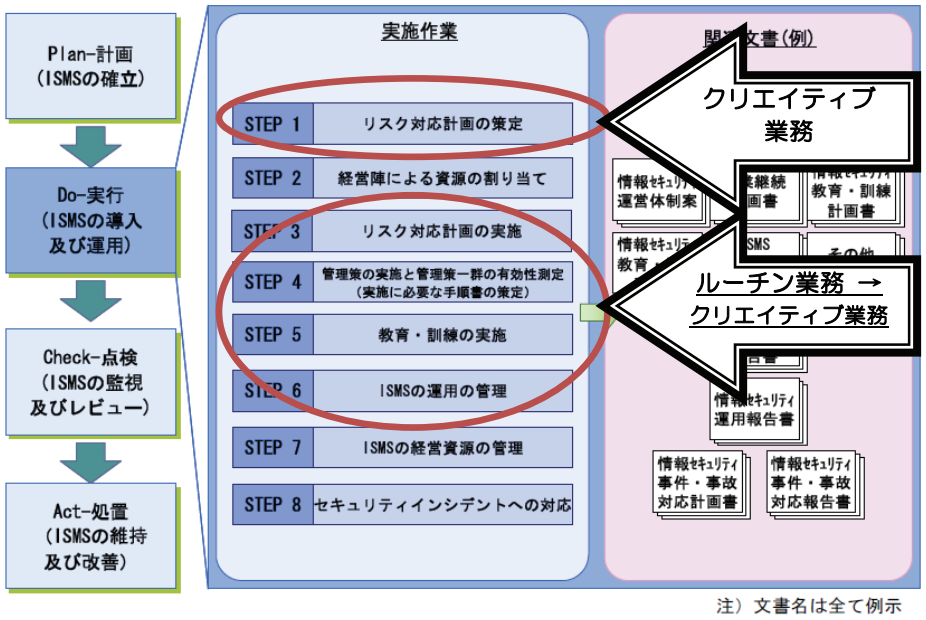

図 4 「リスク対応計画～運用の管理」をクリエイティブ業務化
(図は ISMS ユーザーズガイドより引用)

この手法を導入することで情報セキュリティインシデント,特に「ミス」に由来するインシデントを低減させることを狙う.

4.4 ポイントと期待

この提案は,「自律」「熟達」「目的」の観点をリスクマネジメントプロセスに導入するものである.提案のポイントは以下の点である.

(ア) 自律
- リスク対応計画の作成と,ISMS の運用の管理を同一部門にする
- リスク対応計画の立案,実施,管理主幹を原則として現業部門が持つ

(イ) 熟達
- 立案するセキュリティ施策が組織に合致することを目指す
- 監査等からのフィードバックを受け止め,更なる向上を目指す
- 自身の状況を見極め,その状況に最適な施策を立案,実行する

(ウ) 目的
- セキュリティ方針を従業員一人一人の目的,意義とマッチングさせ,ベクトルを合わせる

当然最低限のベースライン（組織全体のポリシー）は必要であるが,その上にどのようなセキュリティレベルを確保していくかについて,出来る限り現業部門に任せ,自律的に実施することとする.

従業員が自ら進んでリスクマネジメントプロセスに関与し,現業部門で自律した統制が行われることで,

- 「やらされ感」等を低減できる
- 実態を知るものが立案するため,実効性ある対策が立案,実行できる
- モチベーションマネジメントにより,「モチベーション低下によるミス」に起因するインシデントが低減される
- 自身の部門が文書の編集・承認権限を持つため,組織の状況が変わった際にも実態に合わなくなったルールを自分たちの権限で素早く修正できる

等の効果が期待できる.

5. おわりに

本稿ではセキュリティマネジメントのフレームワークのリスクマネジメントのプロセスについて,その捉え方を転換した上で,モチベーションマネジメントの考え方を取り入れることについて提案をした.本方式は実施した結果にインセンティブを感じ（させ）ることが難しい取り組みについて,その汎用的な実施のヒントを含んでいる物

Vol.2010-CSEC-51 No.7
2010/12/10

と考えている.

今後は本提案を実際の組織に適用することを目指し,実際の組織への適用方針,導入手法,効果測定について検討を進める.

例えば,組織形態,組織規模,業界等による情報セキュリティへの取り組み,統制方法の差違等を考察した上で,どのようなアプローチでこの手法を企業に適用させられるかの具体的な導入手法の検討である.これはフィールドワークの準備にもなる.また効果を客観的に確認するための測定手法も併せた検討も必要と考えている.

以上

参考文献

1) 情報処理推進機構:「2008 年 国内における情報セキュリティ事象被害状況調査」報告書(2009)
2) 情報処理推進機構: 「2009 年度 情報セキュリティの脅威に対する意識調査」 報告書(2010)
3) A. H. Maslow: A Theory of Human Motivation,Psychological Review 50(4)(1944)
4) David Mcclelland, John Atkinson, Russell Clark, Edgar Lowell: The achievement motive, Appleton-Century-Crofts(1953)
5) Herzberg, Frederick: The Motivation to Work, New York: John Wiley and Sons(1959)
6) Alderfer, Clayton P.: Existence, Relatedness, and Growth; Human Needs in Organizational Settings, New York: Free Press(1972)
7) Daniel. H. Pink: Drive: The Surprising Truth About What Motivates Us(2009)
8) 情報処理推進機構: 情報漏えいインシデント対応方策に関する調査(2008)
9) 中小事業庁: 中小企業／小規模企業者数, http://www.chusho.meti.go.jp/koukai/chousa/chu_placement/index.htm
10) 情報処理推進機構: 中小企業における情報セキュリティ対策の実施状況等調査報告書 (2009)
11) International Organization for Standardization: ISO/IEC 27001:2005
12) 日本情報処理開発協会, ISMS ユーザーズガイド-JIS Q 27001:2006(ISO/IEC 27001:2005)対応 -(2008)