サイバーセキュリティ経営を支援する ITC にとって必要になる知見とは

2017年3月31日

企業内 ITC・IT ガバナンス研究会

序

2015 年 12 月に経済産業省と独立行政法人 情報処理推進機構（ IPA ）が、大企業及び中小企業（小規模事業者除く）のうち、ＩＴに関するシステムやサービス等を供給する企業及び経営戦略上ＩＴの利活用が不可欠である企業の経営者を対象に、「サイバーセキュリティ経営ガイドライン」を策定し、公表した。

また 2016 年 12 月には、IPA から「サイバーセキュリティ経営ガイドライン解説書」を、更に 2017 年 1 月に「中小企業の情報セキュリティ対策ガイドライン（第 2.1 版）」を策定し、公表している。

これまで、中堅中小企業は大企業に比べ、セキュリティ対策に積極的ではなく、大企業の問題とされてきた状況があったが、2015 年以降こうした状況が大きく変わりつつある。情報セキュリティ対策を疎かにしたために秘密情報や個人情報の漏えいを発生させ、経営を揺るがしかねない高額な賠償金を支払った企業もある。

中小企業の IT 経営を支援する立場の ITC は、中小企業経営者が適切なリーダーシップを発揮し、意識改革や人材育成などができるよう、担当者への丸投げではなく、経営者が自社の情報セキュリティについて明確な方針を示すとともに自ら実行していくように指導していくことが必要である。そのために、ITC には「サイバーセキュリティ経営」に関する深い理解と、その実現を支援するための新たな知見の獲得が必要になる。

本論文では経営者に対して、「わかっているのに、なぜ対策がおろそかになるか」をしっかり理解頂き、適切な情報セキュリティ対策が提案できる施策を論述させて頂く。

２０１７年３月

執筆者　一同

執筆メンバー　ITガバナンス研究会

久住　昭之（元 IT コーディネータ）

坂本　徳明（0064952006C）

瀬戸　昭彦（0065252006C）

滝沢　　康（0012552001C）

千枝　和行（0029302004C）

古川　正紀（0005462001C）

牧田　一雄（0052712005C）

山﨑　直和（0035252003C）

1. はじめに

経済産業省と情報処理推進機構（IPA）は 2015 年 12 月 28 日、企業の経営者を対象とした指針「サイバーセキュリティ経営ガイドライン Ver 1.0」を公表した。ここではサイバー攻撃から企業を守る観点で、経営者が認識すべき「3 原則」と、経営者が情報セキュリティ対策の担当幹部（CISO：最高情報セキュリティ責任者）に指示すべき「重要 10 項目」をまとめている。

対象となるのは、大企業および中小企業（小規模事業者除く）のうち、IT に関するシステムやサービスを供給する企業、または経営戦略上 IT の利活用が不可欠な企業の経営者。経営者のリーダーシップの下で、企業がサイバーセキュリティ対策を推進するための指針として策定されている。

2015 年には標的型攻撃によって日本年金機構から 101 万人分の個人情報が流出するなど、サイバー攻撃は件数の増大に加えて手口が高度化し、被害の件数や規模の拡大が続いている。一方で、企業にとってセキュリティ対策のための投資は、利益を生み出すわけではないため費用対効果を計りにくく、ほかの投資案件と比べて後回しになりやすい状況は続いている。

ガイドラインは、各種アンケート調査のグローバル比較から、日本企業の経営層のセキュリティ意識が相対的に低いことを指摘。経営判断に基づくトップダウンで企業のセキュリティ投資を促すことを目的としている。

ガイドラインの柱となるのは、経営者が認識すべき「3 原則」と、経営者が情報セキュリティ対策の担当幹部に指示すべき「重要 10 項目」からなっている。

3 原則では、サイバー攻撃によるリスクを経営リスクに位置付けて対策を講じること、系列企業や取引先、システム委託先を含めた対策が必要なこと、平時から顧客や株主にリスクや対策の情報を開示して信頼を醸成し緊急時の不信感を抑えることが挙げられている。

セキュリティ担当幹部に指示すべき 10 項目としては、リーダーシップの表明と体制の構築、リスク管理の枠組み決定、攻撃を防ぐための事前対策、攻撃を受けた場合に備えた準備が掲げられている。10 個の項目ごとに、対策を怠った場合のシナリオと対策例も同時に示されているという形式である。

更に、付録として、担当幹部向けの「(A) サイバーセキュリティ経営チェックシート」と、セキュリティ担当者向けの「(B) 望ましい技術対策と参考文献」「(B-2) 技術対策の例」「(C) 国際規格 ISO/IEC27001 及び 27002 との関係」「(D) 用語の定義」を付け、対策に着手しやすいようにされている。

そしてちょうど 1 年後の 2016 年 12 月に「サイバーセキュリティ経営ガイドライン」 の普及と実践に向けて、ガイドラインの内容を補足し、実施方法を具体的に解説する「サイバーセキュリティ経営ガイドライン解説書」が公開され、本解説書を

活用することにより、経営者のサイバーセキュリティの確保に向けた取り組みが推進されることを期待していることが明記されている。

さらにその 1 ヶ月後の 2017 年 1 月、「中小企業の情報セキュリティ対策ガイドライン（第 2.1 版）」が公表され、2009 年に策定された「中小企業の情報セキュリティ対策ガイドライン」について、新たな脅威などを踏まえて内容を刷新するとともに、経営者観点での情報セキュリティの必要性や管理者が組織的な対策を講じる際の具体的な手引きなどを追記している。（「サイバーセキュリティ経営ガイドライン」の内容を踏まえ、中小企業に焦点を絞ったものになっている。）

中小企業にとって重要な情報を漏えいや改ざん、喪失などの脅威から保護することを目的とする情報セキュリティ対策の考え方や実践方法について、ここでは説明され、本編 2 部構成と付録より構成されている。

このように現在は「うちは中小企業だからサイバー攻撃を受けないのでは…？」は通用しない時代に入っている。中小企業経営者はこのことを十分理解し、「サイバー攻撃を受けたら企業にどのような損害があるのか…？」、「ウィルス対策ソフトを導入しているから予防対策は万全かどうか…？」、「サイバー攻撃を受けたらどうしたらよいのか…？」などに明確な答えを持って頂かねばならない。

そこで以下の章では、まず「サイバーセキュリティ経営ガイドライン」を通して、現在の脅威の実態を理解頂き（第 2 章）、次に中小企業と「サイバーセキュリティ経営ガイドライン」の接点、中小企業にとってもいかにサイバーセキュリティ経営が重要であるかを述べ（第 3 章）、その後サイバーセキュリティの実践について、4 章では一般的な視点で、5 章ではそれをうけて ITC にフォーカスして論述する。

2. サイバーセキュリティ経営ガイドライン

本章では、経済産業省が公表した「サイバーセキュリティ経営ガイドライン」（本章においては以下「本ガイドライン」と記載）そのものについて考察する。

本ガイドラインは、経済産業省が独立行政法人情報処理推進機構の協力のもと、「経営者のリーダーシップの下でサイバーセキュリティ対策が推進されること」を期待して策定したものであり、「策定の背景」および「概要」については、次のように明記されている。

【策定の背景】
様々なビジネスの現場において、ＩＴの利活用は企業の収益性向上に不可欠なものとなっている一方で、企業が保有する顧客の個人情報や重要な技術情報等を狙うサイバー攻撃は増加傾向にあり、その手口は巧妙化しています。そこで、企業戦略として、ＩＴに対する投資やセキュリティに対する投資等をどの程度行うかなど、経営者による判断が必要となっています。

【概要】
経済産業省では、独立行政法人情報処理推進機構（ＩＰＡ）とともに、大企業及び中小企業（小規模事業者除く）のうち、ＩＴに関するシステムやサービス等を供給する企業及び経営戦略上ＩＴの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため、「サイバーセキュリティ経営ガイドライン」を策定しました。
サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「３原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に指示すべき「重要１０項目」をまとめています。

まずは、何故このタイミングで本ガイドラインの策定が必要になったのか、策定の背景にある「増加傾向にある手口が巧妙化しているサイバー攻撃とは一体どんなものなのか」を簡単に再確認してみることとしたい。

2-1. サイバー攻撃とは

サイバー攻撃の定義については、いろいろな書物で様々な説明がなされているが、ざっくりまとめると「外部からインターネット等を通じて特定のコンピュータに侵入し、システムそのものを破壊したり、保存データを改ざんしたりすること」である。具体的には、いくつかの種類や手口で分類することができ、代表的なものとしては、標的型攻撃、不正アクセス攻撃、マルウェア攻撃等が有名である。

【標的型攻撃】
特定の組織（企業、官公庁等）を狙い打ちし、ウィルス添付メール等を送信して相手を困らせる攻撃である。この攻撃に対しては、システム的な対策を講ずることも必要であるが、従業員それぞれが、不審メールは絶対開かない、といったような高いセキュリティ意識を有していることが肝要である。

【不正アクセス攻撃】

外部から不正に特定のコンピュータ（Webサイト等）へアクセスし、機能停止に陥らせたり、内容の改ざん等を行う攻撃である。有名なものとしてDos攻撃、DDos攻撃、クロスサイトスクリプティング等が挙げられる。特徴として、誰（どこ）から、誰を狙った攻撃なのか、が特定しづらく一般的に対策が講じにくい。

【マルウェア攻撃】

マルウェアと呼ばれる悪意のある活動を行うソフトウェア等を攻撃先のシステムにインストールさせ、遠隔で情報操作や破壊活動を行う攻撃である。バックドア、ワームソフト、トロイの木馬、・・・等、様々なマルウェアが存在する。

以上のように、ざっくりレベルであれば軽く説明することもできるが、実際のところは、手口や方法も千差万別であり、しかも日々攻撃手段は進化を遂げている。本書では、これ以上の技術的な説明を記載するつもりはないため、詳細については専門の解説書等に任せることとしたいが、詳細解説を記載している文書においては、同じ内容（文面）ではおそらく１年ももたないだろう。それだけ攻撃手段の多様化は凄まじく、日々生き物のように進化を遂げている、というのが現状である。

そのような攻撃側が多種多様化している状況において、守る側はどうやって自分の身を守るべきか、何を、どこまで、どのようにサイバーセキュリティ対策を講じるべきか、重要な情報を抱える立場の者はしっかりと戦略をもって考える必要がある。

2-2. サイバー攻撃に対する経営者の心構え

2-1 で述べたように、現在は攻撃が多様化しており、いたちごっこの状況になっている。そこで、そろそろ攻撃から情報を守る段階から、「サイバー攻撃を完全に防ぐことは不可能」という前提に立った対応が必要な時期に来ている。つまり、事前の攻撃防止（Pre-Attack-Management）から、攻撃を受けた時の被害の最小化を図る事後対策（Post-Attack-Management）に重点を移すということである。

被害想定をしたうえで、現実的に想定した被害を被った時にどのような対処を行う必要があるかを整理しておくことは、その被害により影響を受ける自社のお客様や業務への対応を適切かつ迅速に行うためには必須事項になる。サイバー攻撃を受けてその事後対策がおぼつかなければ、お客様の信頼を失い、ひいては事業自体が大きな影響を受けることになる。そのようなことにならないためにも、事前対策は

一定のレベルまでやっておくとしても、事後対策を疎かにしてはならない。

一例を示すと、最近はウィルス感染の中でも「ランサムウェア」感染も日常茶飯事となり、情報の漏えいだけでなく、必要なデータのバックアップを適切に行っていないと日常の業務が停止し、最悪の場合には事業継続の危機につながってしまうこともある。身代金を支払ってデータが回復できれば良いが、もしそれが出来なかった場合には、それまで蓄積してきた情報資産がすべて消え去ってしまい、その事業影響は相当なものになるものと思われる。

中小企業の経営者は、自らの事業を守り社員の生活を守る責任を負っている。それを改めて認識したうえで、自社のシステムのどこが狙われるのかをきちんと分析し、万が一攻撃を受けたとしても、事業を安定的に継続するために必要な措置をきちっと整理して日頃から備えておくことが重要である。

サイバーセキュリティ経営ガイドラインの期待するところは、まさにこのようなサイバー攻撃に対するリスクマネジメントを経営者自らが行う点にあると考えられる。

3.「サイバーセキュリティ経営ガイドライン」が主張していること

次に、経営者の情報セキュリティに対するガバナンスの重要性について述べてみたい。

2014年11月に制定されたサイバーセキュリティ基本法に基づき2015年9月にサーバーセキュリティ戦略が閣議決定された。

それを基に経営責任としてサイバーセキュリティ（情報セキュリティ）対策の必要性を経営者向けにしめした「サイバーセキュリティ経営ガイドライン」が制定された。この中で　経営者が認識する必要がある３原則、サイバーセキュリティ（情報セキュリティ）対策を実施する上でCISO（情報セキュリティ対策責任者）に指示すべき10項目が定義されている。

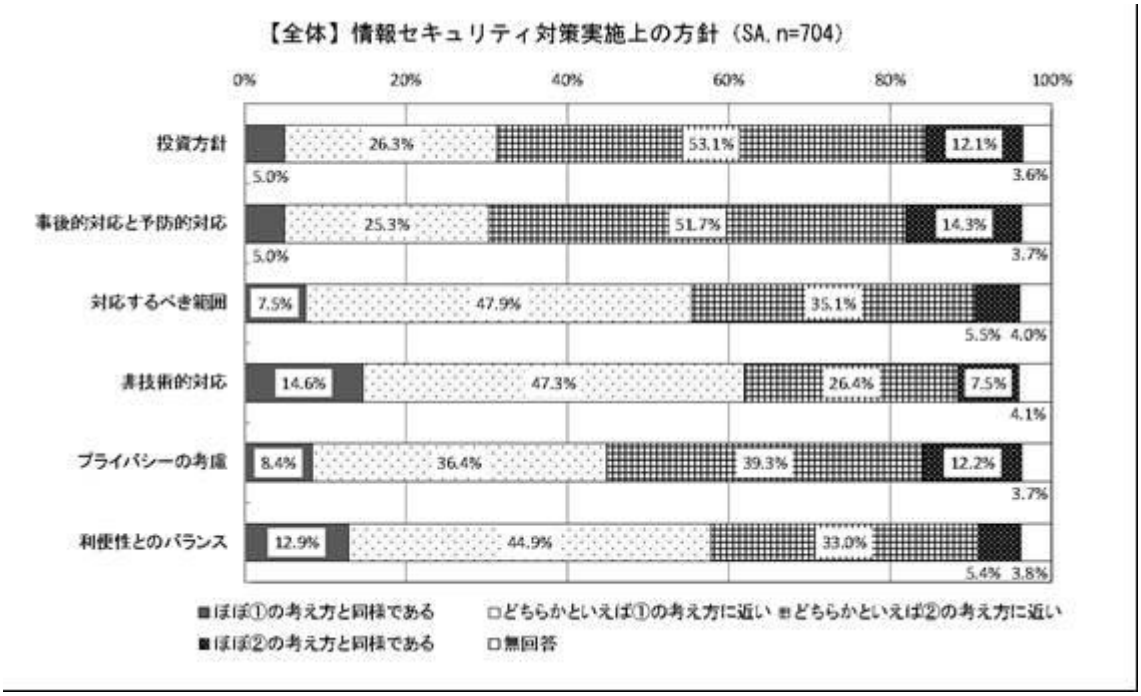
3-1.　「不正アクセス行為対策等の実態調査」による経営者の認識

警察庁が公開している「不正アクセス行為対策等の実態調査」によると、『多くの社・団体において１人１台以上の端末が整備されているほか、外部からのセキュリティ対策、ログ管理などの各種セキュリティ対策への取り組みが行われており、その意識は高い。』とされているが、その一方で『セキュリティ対策にかかるコス

トが高すぎることや費用対効果が見えないなどの費用や投資に関する問題が多く挙げられる』との問題提起も行われている。

また、2016年度は過去に受けたことがある被害状況(137件/704組織)について「ランサムウェア」が35.8%で新しく一躍トップに躍り出て、昨年度トップだった「ホームページの改ざん」(2015年度35.9%⇒2016年度34.3%)を抜いており、既知の被害に加え年々未知の被害が増加し、今後もその傾向が増大してゆくことが推測される。

情報セキュリティ対策を実施する上での「投資方針」については「②積極的」(65.2%)が「①必要最低限」(31.3%)と大幅に上回り、「事後的対応と予防対応」についても「②予防的対応」(67.0%)が「①問題発生への適切な対応」(30.3%)とする回答を大幅に上回っている。



出典：警察庁「不正アクセス行為対策等の実態調査」（平成28年度）
https://www.npa.go.jp/cyber/research/

一方で来年度(2017年度)情報セキュリティ対策の投資計画については、「ほぼ同額とする計画」(70.3%/704組織)が大半を占めており、今年度(2016年度)(67.2%/793組織)と比べてあまり変化が無い。

さらに、情報セキュリティ対策への投資に関する問題点については「どこまで行えばよいのか基準が示されていない」(51.3%)、「費用対効果が見えない」(47.3%)、「コストがかかり過ぎる」(42.5%)となっている。

以上の様な調査結果から,情報セキュリティ対策については**総論賛成各論反対**といった現状の姿が見えてきているのではないだろうか。

「投資方針」は積極的と言っているものの「投資計画」は現状維持（昨年度並み）となっていることから、大部分の経営者は情報セキュリティ対策の必要性や昨今の報道や情勢も踏まえ重要性の認識はあるもののあくまで「投資」ではなく「コスト」として捉えていると思われる。

3-2. 経営者の基本的行動スタイル及び陥りやすい錯覚

経営判断の原則は、日本においては、取締役のなす経営判断には広い裁量が認められ、結果的に会社に損害を与えても取締役には法的責任が生じない、という考え方である。明文の規定があるわけではないが、裁判所の判例にその考え方は用いられていると理解されている。具体的には、判断時の状況を前提とし、関連業界の通常の経営者を基準として、判断の前提たる事実認識を不注意で誤ったか、あるいは、事実に基づく判断が著しく不合理であった場合でなければ、取締役の善管注意義務違反を認めない、という法理として一般化されている。

一方では、会社法上　役員（取締役，執行役，会計参与(監査法人等)，監査役）は，善管注意義務（会社法第330条，民法第644条）又は忠実義務（会社法第355条）に違反する任務懈怠により会社に損害を与えた場合には損害賠償責任を会社に対して負う（会社法第423条）ことが定められている。

取締役は会社との関係で受任者の立場にあり、善管注意義務・忠実義務を負っている。取締役は、業務執行の決定または業務執行の決定への関与に関して、一定の裁量を有していると考えられている。元来、経営にあたってはリスクが伴うのが常であり、結果的に会社が損害を負った場合に、事後的に経営者の判断を審査して取締役などの責任を問うことを無限定に認めるならば、取締役の経営判断が不合理に萎縮されるおそれがある。

情報セキュリティ対策についていえば、昨今の「ランサムウェア」の様な急激な新種のマルウェアの対応や標的型サイバー攻撃の進化に代表される様　経営者を取り巻く環境が劇的に変化に対して自社だけでは対応が難しくなったこともあり、その対策の重要性・緊急性を十分理解できていない様に思われる。（進入を防ぐのではなく侵入されるのが前提の対策をとることが重要である。）

そういったことを踏まえ、「サイバーセキュリティ経営ガイドライン」では

１．経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要である。
２．自社はもちろんのこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策が必要である。
３．平時及び緊急時のいずれでも、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要である。

と言う３つの原則を打ち出されたのではないか。

要は

１．経営者が、「サイバーセキュリティ(情報セキュリティ)対策を知らない」、「社内外の担当者に任せている」ではすまなくなってきているので経営判断として対応することが必要である。
２．経営者が、「プロフェッショナル(の委託先)に裏切られた」、「子会社、パートナー(下請け)がやったこと」との釈明が通用しない。
３．経営者が、ステークスホルダーに根拠の無い「大丈夫です」との釈明が通用しない。

と言うことを経営者に理解してもらうことが重要。特に主語が*経営者は*ではなく***経営者が***　となっていることに留意すべきである。

【会社法】

第330条　（株式会社と役員等との関係）
株式会社と役員及び会計監査人との関係は、委任に関する規定に従う。

第355条　（忠実義務）
取締役は、法令及び定款並びに株主総会の決議を遵守し、株式会社のため忠実にその職務を行わなければならない。

第423条　（役員等の株式会社に対する損害賠償責任）
取締役、会計参与、監査役、執行役又は会計監査人（以下この節において「役員等」という。）は、その任務を怠ったときは、株式会社に対し、これによって生じた損害を賠償する責任を負う。

：：

【民法】

第643条　（委任）
委任は、当事者の一方が法律行為をすることを相手方に委託し、相手方がこれを承諾することによって、その効力を生ずる。

第644条　（受任者の注意義務）

受任者は、委任の本旨に従い、善良な管理者の注意をもって、委任事務を処理する義務を負う。

3-3. 経営者のコストへの認識

経営者は現在適切な対策が将来も適切な対策であり続けるとは限らない技術革新(暗号化、脅威の監視→検知→防御、ネットワーク)に伴い最新技術を取り入れながら適切な組み合わせを定期的に変えて行く事が重要である。

going concern　を守り続けるためにも一連の情報セキュリティ対策はコストではなく投資として捉えてゆくことが経営の視点からは必要ではないだろうか。

但し、人・物・金の資源は有限であるとともに、どの様な対策をしても情報セキュリティリスクはゼロにはならない。今後の経営者の必須スキルの１つとして適切なリスクマネジメントと資源の配分を行えることが要求されると思われる。

3-4. そもそもサイバーテロでは何が問題なのか

サイバーテロを100%防ぐことの出来ない現状を考えると、「いつ何をすることが守ることにつながるのか」ということが明確になっていないことが一番の問題である様に思われる。

何を守るかを明確にせずに漫然とシステム面での情報セキュリティ対策を行ったとしても、万が一被害にあった場合の影響度が変わってくるはずである。

ISMSで言うところの情報資産の洗い出しを最初にきちんと行い定期的に見直すことが最重要と思われる。

情報漏えいが発生した場合の影響が風説被害も含め自社(組織)グループ内だけにとどまるのか、外部も巻き込んでしまうのか、各社(組織)での情報/制御システムが１秒たりとも停止してはまずいのか数時間、数日停止しても重大な影響が無いのかや　(外部も含めた)サービス提供に及ぼす影響によっても各社(組織)個別の優先順位付けや防御対策が必要になってくると思われる。

3-5. 何も起こらない(ゼロリスク)なんて有り得ない

万が一にも事案が起こってしまった場合

・インシデント/アクシデントへの適切な判断及び全体統制

・過不足なくインパクトを評価した上での経営層の適切な決断・行動

が必要となる。

但し、判断に迷う状況に陥ったら（未知の脅威であるとか発生時期が株主総会の直前、自社での対応不可等）どうするのか。

かといって　人材の確保も含めた予防体制をどうすべきなのかが経営者が認識し、リーダーシップをとって解決すべき課題。

3-6. 経営層がすべきリスクコミュニケーションの方略

本章の担当者の自宅近くにある落花生を売っている店に、
「なぜか！　下田園の落花生が映画「踊る大捜査線 3」に登場！」
という宣伝の看板が立っておりその前を通る毎にTVでも映画でもよく見たなと思い出される。

看板に載っている「踊る大捜査線 3」のエピソードではないのですが、同じシリーズの「踊る大捜査線 2」で「事件は会議室で起きてるんじゃない！現場で起きてるんだ！」

という有名なセリフがあったかと思う。

組織の観点から見ると、上層部に権限が集中し末端に裁量権が降りてこないため身動きが取れずにいた。しかし、主人公の（現場のことが十分にわかった）上司の勇気ある決断により、現場に自発性と自由裁量を持たせる自律型の持続可能型組織に現場が変わり、全員が、使命を完遂しようと自律的な意思で動くことにより、犯人確保につながった(組織が勝った)というストーリーだったかと思う。

サイバーセキュリティ（情報セキュリティ）対策でも同じ様に経営者とセキュリティの担当者との間で普段から十分なコミュニケーションがとれていないと（特にインシデント発生時に）現場に裁量権が無い為、報告の対応に追われて対策に当てられる時間が不十分になる恐れがあると思われる。

経営者は事前にインシデント発生時に権限の一時的な委譲も含めリスク対応が出来る持続可能型組織を用意することも重要と思う。

映画の中の理想的な組織で現実的ではないとの指摘もあるかと思うとともに、がっ色々あるけれど、現場の気持ちを経営層に伝えるだけでなく、経営層の気持ちもきちんと現場にむけ代弁できる。このつなぎ役がいなければ、持続可能型組織として本当は回らないのではないか。組織に一番必要なのはこのポジションの人材がいないのであれば ITC がそれを補完すればよいのではないかと、強く感じた次第である。

落花生の下田園

http://www.shimodaen.com/

3-7. サイバーセキュリティ経営ガイドラインの限界

「サイバーセキュリティ経営ガイドライン」はあくまでガイドラインであり、法令（法律、政省令、条令、規則）の様な強制力はない。

（法令であれば、前述の取締役の忠実義務の対象になるのであるが…。）

IT と経営の橋渡しを行う ITC としても、この様なガイドラインの必然性を経営層に理解していただくことは、その存在価値を高めるためにも必要である。

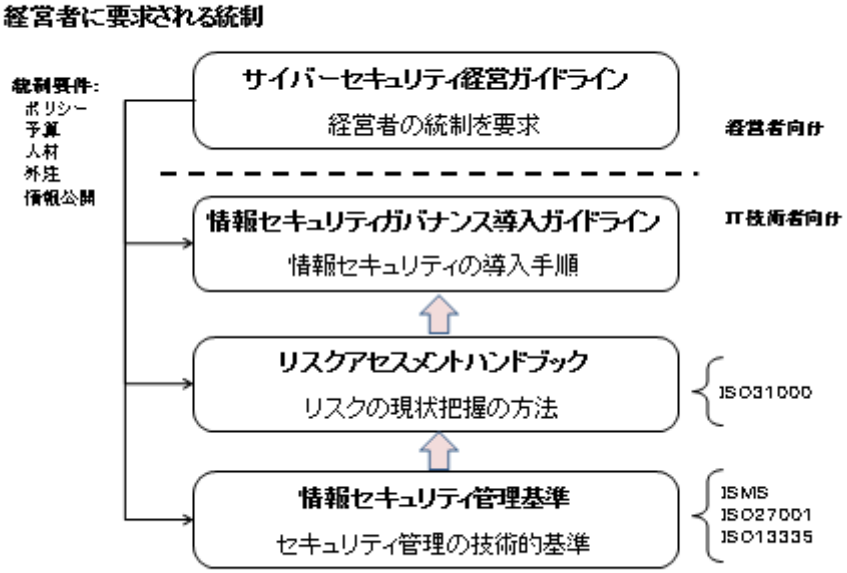
4. リスク対策に対する経営者が陥る心理的錯覚への考察

前章までで、経営者の情報セキュリティに対するガバナンスの重要性について述べた。

しかし、「サイバーセキュリティ経営ガイドライン」のような、経営者向けの指針が出されるのはなぜか。

過去には、技術的管理をするための「情報セキュリティ管理基準」、リスクアセスメントをするための「リスクアセスメントハンドブック」、セキュリティ体制を導入するための「情報セキュリティ導入ガイドライン」等の指針を提示し、情報セキュリティ管理体制の普及に努めてきたはずである（図１）。しかし、一向にセキュリティ事故は無くならない。何故か・・・。

サイバーセキュリティ経営ガイドラインの位置づけ（図1）

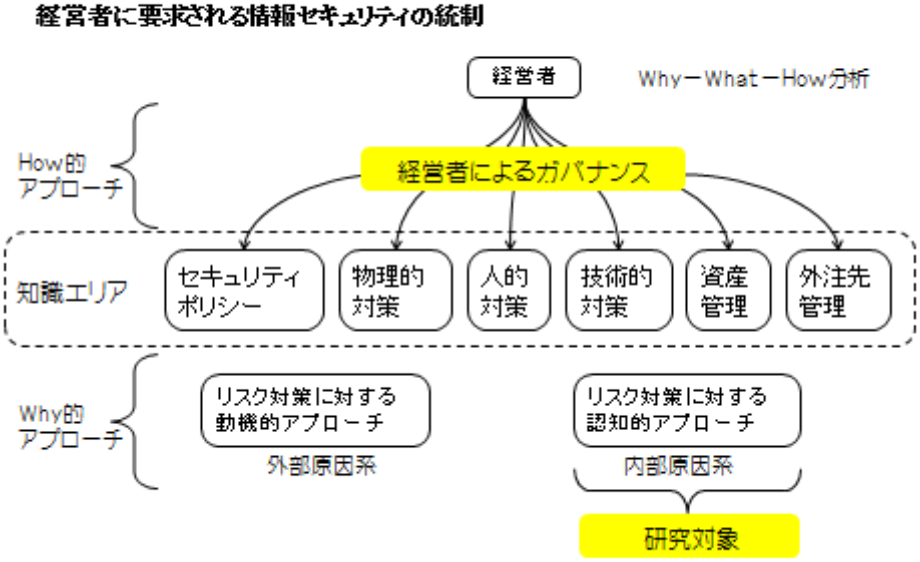


それは、問題の根本が経営者サイドの統制が不十分という問題であって、従来基準のように担当者に対する技術的指針では徹底されないと考えたためではないか。

では、何が原因で経営者は適切な対応をしないのであろうか。実は、分かっていても行動に移されないという現象は、東日本大震災の津波の避難勧告に対する行動に多く見られる。避難勧告に対して、行動に移らなかったり、いったんは避難したが、津波が反復して襲ってくることを甘く考え、家や職場に戻って被害にあった大勢の人達の行動が記録されている。三陸海岸の住人は津波の現象を十分理解していたのに被害に遭遇したのである。

第４章では情報セキュリティの技術的な側面ではなく、この様な現象は人間が陥りやすい心理的錯覚に原因があるのではないかということにたどり着き、心理的面から考察をしてみたいと思う（図２）。

本研究におけるアプローチのポイント（図2）



4-1. コンサルタント会社の意見に見る経営者の認識

経営者の代表的な認識について、普段顧客の会社に接しているコンサルタント会社、PwCサイバーサービス合同会社　最高執行責任者　星澤裕二氏の見解を引用してみる。

「一般的な経営のリスク自体を考えることも難しいのに、それに加えてセキュリティを考えるとなると、余計に難しいのではないかと思います。セキュリティがそのままリスクになるということは、2014～2015年に情報漏えいなどの大きな事件が続いて起こったことによって、だいぶ理解されるようになってきました。実際に、株価が下がったり、数億円に上る巨額を投資しなければならなくなったり、倒産寸前になった企業を見て、セキュリティ対策をしないことは、ものすごいリスクであると理解した経営層も多いと思います。とは言っても、実際に自分の企業で事件が起こっていない企業は、やはり他人事のような意識を持っている経営層がほとんどです。」

また、最高技術顧問　名和利男氏は次のように述べている。

「実際にサイバー攻撃を受けている経営層は、対応しなければならないと考えて、実装段階にありますが、大多数は、世の中がセキュリティの流れになり、担当責任者や部下に指示をしなければならないが、どうやればよいか分からないから勉強し

たいという人たちです。こういう企業の多くは、実装より前の啓発や企画設計の段階だと思います。全体から見ると、後者が大多数なので、セキュリティはまだ進んでいないと思います。」

大まかに表現すれば、「最低限のことはやっているはずである。その上で何をすればいいのかわからない」というふうに読み取れる。大部分の経営者は傍観状態と述べられているので、何らかの心理状態に陥っていると考えられる。

4-2. 人間の基本的行動スタイル

まず最初に、人間の基本的な行動スタイルの傾向に触れてみたい。人間には無意識のうちに、過去の体験に基づく錯覚（思い違い）に基づいた行動を行う傾向がある。

【確証バイアス】

通常、多くの人は日常的な処理についてはあれこれ考えず、手順を定め、手順通りに行動する傾向を持つ。こうすることにより、余分なエネルギーを使わず、コスト的に最適化された行動となると考えているからである。

例えば、何かの質問を受けたとして、それに対する答えは「その人がすぐに思い出せるもの」が、優れた答えだと錯覚する。自分がよく知っていると考える分野だとその傾向が強くなる。

人は個人の経験などから成り立つ信念、理論、仮説などを支持し、先入観を補強する証拠を集める傾向がある。反対に、反証となる証拠の収集を避けたがる傾向がある。これを「確証バイアス」という。典型的な例が喫煙に関する態度で、喫煙者は「喫煙の健康被害はそれほどでもない」という情報や、「税金を納めて国家に貢献している」などの情報を選択的に好み、「肺癌の発生率」や「受動喫煙被害」などの情報を避けたがる。明らかに偏っているのだが、そこに心の安住を求めたがる傾向を持ちたがるのである。

【根本的な帰属の誤り】

状況の影響を過小評価し、個人特性を過大評価して人間の行動を説明する傾向を指す。他人が失敗すればその人の能力のせいにし、自分が失敗すれば環境のせいにして重圧や責任から逃れたがる傾向を示す、などが典型的な例である。

【期待効用論】

人は有利な期待値に従って、合理的に行動すると長い間考えられてきた。しかし、最近の研究では必ずしもそうではないことが分かってきた。ボランティア活動などはその典型である。ボランティア活動の場合、損得勘定よりもう少し高次な精神活

動が関与していると考えられる。

このように、人間は日常的に自己の感情を良好に保ったり、新たなコストや労力の低減のために、無意識のうちに従来のやり方を継続したがる傾向を持ちやすい。最も適切と思われるものを選択するとは限らないのである。こうした傾向が、リスク対策をおろそかにしたり、後回しにする要因の一つになる可能性がある。

4-3. 人が陥る認知上の錯覚

通常、多くの人は重要・緊急と感じない案件は、ヒューリスティックな処理を行いやすい傾向を持つ。

ヒューリスティックとは何か？

それは不確かな状況下で、判断や決定を行う際、通常使用する簡便で直感的な方略のことをいう。これらは、経験に基づくため、経験則と同義で扱われる。判断に至る時間は早いが、必ずしもそれが正しかったり適切だったりするわけではなく、判断結果に一定の偏り（バイアス）を含んでいることが多い。

では、なぜヒューリスティックのような方略に頼るのか？

それは、適切に対応するためには「高い認知コスト」がかかるためである。リスクに対して、発生した時の影響についてその全体像や将来への影響などが瞬時に見えるケースは少なく、通常はよくわからないのが普通である。状況を分析して、正しく認知するには時間や労力などのコストがかかるから、手っ取り早く片付けたいという傾向が、無意識に働くのである。

起きた事象と対応の労力的・コスト的バランスは、経験や情報の蓄積が無いと判断できないのである。そういう点では、経験者や知識のあるものが、情報を示して適切にアドバイスをする必要がある。

4-4. 人が陥る動機づけ上の錯覚

人が行うヒューリスティックな判断によって生まれてくる認識は、一定の偏りを持つ。この偏りを与えるものをバイアスという。バイアスは、人が正常性を保とうとしても、自然と本人の判断に影響を与えてしまう。この項ではその様な人間に認識とそれに対するバイアスについて触れてみる。

【正常性バイアス】

自己や事件、あるいは自然災害など何らかの被害が予想される様な状況下でも、自分にとって都合の悪い情報を無視したり、認知された異常性を、なるべく正常な状態で見ようとする心理的プロセスを指す。日常的によくある出来事の中に押し込

めたがる傾向があり、リスクの過小評価につながる。

【楽観主義バイアス】
自分の周囲で起こる事象を、自分に都合の良いようにゆがめて認知する心理的プロセスを指す。心理的ストレスを回避しようとする傾向で、リスクの過小評価につながる。

【同調性バイアス】
周囲の人のリスク情報への反応に同調して、異常性を押し殺したり、過剰に反応したりする心理的プロセスを指す。リスクの過小評価または過大評価につながる。

このように、セキュリティ事故などの重大事故が発生した場合でも、人は従来から持ち合わせている判断傾向を維持し、新しい事実を受け入れたがらない傾向を持ちたがることを理解しなくてはならない。

サイバーセキュリティに対して、よく分からない、つまり価値判断をする基準が曖昧なので、傍観者になりやすいと考えられる。サイバーセキュリティ対策をやってくれといわれても、ＩＴを運営していく上での他の対策は種々存在する。例えば「社員の裏切りによる情報漏洩」、「誤操作による損失」、「ＳＮＳ炎上」、「ベンダーの裏切り」などである。それらとサイバーテロ対策の価値の比較や優先順位が分からないので、優先的に着手する理由が生まれないのではないだろうか。

一般的に「緊急案件」は「重要案件」を破ると言われている。サイバー攻撃は頻度が少ないが被害が大きい、それ以外のＩＴ事故は頻度が多いが被害はそれなりで、サイバーテロ対策が重要案件でも他のＩＴ事故の緊急案件に駆逐されてしまう。これらの優先順位や価値判断が明確にならないと対策を進めるような認識は生まれてこないと考えられる。

4-5. コストへの認識

経済産業省は、サイバーテロ対策は「投資である」という位置づけで、普及を図りたい意向の様である。

中小企業のバランスシートは、中小企業庁のホームページ上で公開されている。それによると、規模の小さい企業ほど自己資本が少なくて固定負債が多く、手元流動性が悪い。規模が大きくなるにつれて自己資本比率の割合が多くなり、固定負債の比率が改善され、手元流動性が改善されていく。従業員数数百人の中小企業であれば対策を考慮することは可能であろうが、規模が小さく手元流動債が悪い会社では、現実問題としてお金が無いのである。企業単体での対応は難しく、支援する何らかの制度が必要であると感じる。

サイバーテロ対策手の投資が利益を生むというシナリオが見えない以上、利益を生む製品改善や顧客対策に向けられるのは当然ともいえる。

4-6. そもそもサイバーテロでは何が問題なのか

サイバーテロで問題とされる企業側の被害について触れてみたい。

被害といっても大きく２つに分かれ、一つは自社が被害を被ってしまうという側面、もう一つは自社が踏み台にされた為に起こる加害者としての側面である。

まず。被害者としての側面を述べてみる。

・情報が漏洩した場合

個人情報が漏洩した場合は、漏洩した対象者に損害賠償の義務が発生する。機密情報が漏洩した場合は、ライバル会社に競争で後れを取ってしまう可能性が大きくなる。また、管理体制のずさんさが社会的に問題にされ、取引停止などの信用失墜につながりかねない。

・情報破壊が発生した場合

情報の修復コストや、最初からやり直しのコストなど、労力やコスト面での負担を強いられる。顧客やステークホルダーから預かった情報が破壊された場合は、損害賠償や取引停止などの信用失墜につながりかねない。

次に、加害者としての側面を述べてみる。

・セキュリティの防御策が不十分で加害行為の踏み台にされた場合

被害者であるはずの自社が、加害者の側に立たされてしまう。しかも、「自覚症状が無い」にも係わらずにその様な状況になってしまう。加害行為の証跡によって２次被害を受けた企業からの損害賠償に応じなければならず、社会的信用の失墜を招きかねない。

顧客やステークホルダーに損害を与えた場合、高額な損害賠償費用が発生するケースが多く発生している。

4-7. ゼロリスクなんて有り得ない

ペルリ（リスク事故）の種類は毎年変化し、細かく対応していくにはコストや労力がかかる。しかし、手元流動性の良くない、特に小規模企業にとっては現実問題として資金がなく、フォローしていくのは極めて困難である。

そこで、中規模企業から小規模企業ではダメージコントロールによるアプローチを考えるのが賢明である。第２章でも触れたが、すべての分野・機能に対して防御するのではなく、事後対策（Post-Attack-Management）を重点として対策を組み立てるのである。まず企業の中心となる情報を守り、その情報に対するアクセスを限定的にする。

次のようなシナリオで推進する。

1) ポリシーに基づき組織を作る。
2) 重要情報を識別し、保護する。
3) リスク項目別の目標と手順を確立する。
4) リスクが発生した場合のエスカレーション手順を確立する。
5) やれる部分から定期的に訓練する。(防火・防災訓練などと同じ)。
6) 反省点をチェックし、手順を修正する。

リスク対策やセキュリティ対策は、防火訓練・避難訓練などと同様に定期的に訓練をしていないと、緊急時に体を反応させるのは困難である。頭だけの理解では適切にしかも組織的に行動に移ることは難しい。つまりリスク対策の極意は「習慣化」することであり、これを経営者に提示して理解・実行してもらう必要がある。

また、資金的に可能であれば損害に対する保険などを考えたり、実際にセキュリティ事故が発生した場合に、社外に対する広報手順を確立しておく必要もある。

4-8. リスクコミュニケーションの方略

リスク・セキュリティ対策が重要であるということが分かっていても、なかなか実行されないのが現実である。この章で繰り返し述べてきたように、

・経営上の重要事項は他にもある
・経営上のリスクは情報セキュリティだけではない
・サイバーテロ対策以外にも情報セキュリティ対策が必要なものがある
・対費用効果が見えてこない

等々でなかなか実行してもらえない。このような状況・心理状態の相手に対して、「サイバーテロ対策を行ってください」といっても聞いてもらえないのである。話の持って行きかたに方略が必要である。

この項では、セキュリティ対策を実行してもらうためのコミュニケーションのあり方に触れてみたい。

わざわざリスクコミュニケーションという名称で取り上げるのは、経営者に従来の考え方や行動の在り方を変容して、適切な防御をしてもらうためである。

リスクコミュニケーションとは、「あるリスクについて、直接・間接に関係する人々が、リスクの存在や形態、深刻さ、受け入れ可能性について、情報や意見を交換する相互作用プロセスのこと」である。「情報や意見を交換する相互作用」というところが重要で、説得したり押し付けたりする様な性質のものではない。相手の置かれた状況、心理状態、可用性、対応可能範囲などを調査し、深く考察し、相手次第で適切に推し進めていく必要がある。紋切型ではダメである。

次に、リスクコミュニケーションを進める手順に触れてみたい。通常のＰＤＣＡサイクル的に表現すると以下のようになる。

・経営全体の目的を踏まえたリスクコミュニケーションの目標を設定する。
・リスク事象についての事実・現状を把握する。
・受け手（相手）の特徴や価値観や意見を把握する。
・相手に伝えるメッセージを作成し、プレテストを踏まえて見直す。
・経営者に対しリスクコミュニケーションを実施する。
・リスクコミュニケーションの実施結果を再評価する。

次に、リスクコミュニケーションを適用する上での技術な進め方を紹介する。

【フレーミング効果】

同じ事象であっても表現の仕方（フレーミング）が変わると受け取られる方が異なる。肯定的なフレームで表現された方が相手に好まれる傾向がある。

【恐怖喚起コミュニケーション】

相手に恐怖の感情を引き起こすコミュニケーションのこと。自己効力感を持てるような情報を合わせて伝えることが必要となる。

【一面コミュニケーション】

その事象の安全性やベネフィットだけを伝えるコミュニケーションのこと。比較的教育程度が高くない人に有効とされる。

【両面コミュニケーション】

安全性だけではなく、リスクなど反論も合わせて伝えるコミュニケーションのこと。比較的教育程度が高い人、または反対意見を持つ人に有効とされる。

【結果明示】

送り手が結論を示すプッシュ作戦のことで、相手の行動を促す。

【結果保留】
受け手に結論を出させるプル作戦のこと。比較的教育程度が高い人に有効とされる。

【クライマックス順序】
結論を最後に述べるコミュニケーションのこと。関心が高い人に有効とされる。

【反クライマックス順序】
結論を最初に述べるコミュニケーションのこと。関心が低い人に有効とされる。

他にも方略はあるが、コミュニケーションをとるというのは、必ずしもテクニックではないし、相手は経営者なので適切に選択していく必要がある。効果的な進め方をしたい場合は、リスクコミュニケーションの経験者から指導を受けるのもよい。

リスクコミュニケーションを進める上で一番大切なものは「信頼関係」である。テクニックでは足元を見られてしまう。当然ながら誠意が伝わらないと聞いてもらえない。なかなか難しいのである。まして、飛込的に面接してテクニックを使ったら、難しい局面に立たされる可能性がある。実際のところ外部の専門家は、対策を進言する前に、まず経営者と信頼関係を築かないと、話を聞いてもらえないのである。かといって、一度の失敗でめげてしまっては、何も進まない。心が折れない強さが説明する側には必要である。

もともと、リスク対策は積極的に利益を生み出すものではないので、相手の立場を考えながら進めないと、失敗してしまう可能性が高い。リスクコミュニケーションの方略は使うが、あくまで全体計画の一部としての話で、全体的・長期的なビジョンを示しながら気長に進めていく必要がある。

4-9. リスク対策は持続可能型組織を作ること

リスク・セキュリティ対策がコストと考えるのは、その実行の恩恵が見えないからである。サイバーテロに遭遇する会社の多くは、防御策が不十分というのが直接原因ではあるが、それ以上に会社組織がセキュリティ事故に迅速に対応できていないということがあげられる。組織の成熟度が高く、従業員の訓練が行き届いていれば、被害にあっても迅速に対応できるはずである。

この組織が迅速に行動できるということは、製品づくりやサービス提供でも同様のことが要求されているのであるから、企業としての成熟度が不十分と容易に推察できる。要するに、成熟度が低いのが根本原因であるから、「サイバーテロ対策をきっかけとして、組織の成熟度を上げていきませんか」という方向に進めていくこと

が重要である。成熟度を高め、持続可能型の組織に変容することこそ、サイバーテロを含めたリスクに強い企業となる機会ととらえて推進すべきと考える。

【お断り】この章に紹介されている心理学で使用する用語は、教科書やＷｅｂ上で紹介されている一般的な定義を引用させていただいております。

5. ITC にとって必要になる知見とは

２章および３章では政府や中央官庁・サテライトの技術指導をしている独立行政法人の視点からのサイバーセキュリティの実現性に対するトップダウンの議論、そして４章では個々の企業もしくは経営者の視点に立って、動機づけと現実の実現方法に対する現実的なアプローチに触れてみた。

今ここで、ＩＴＣとして問題にしなければならないのは、トップダウンによる網をかけるような網羅的な対策に適応することでもなく、現実の顧客中小企業の立場での議論でもなく、それらに対する共通の問題認識の浮き彫りと、中小企業の価値を損なわない為の現実を直視すること、そして問題の本質を考えた積極的なアプローチに対する適切な方略を考え、中小企業のセキュリティ対策に対して経営者に適切にアドバイスすることである。

何よりも、サイバーセキュリティ突破のアプローチが年々、しかも急激に変化を遂げていることに注目する必要がある。セキュリティ技術を日常的にフォローしているＩＴＣにとっては理解できていることかもしれないが、仕事に忙殺されていたり、何らかの理由で理解が行き届いていなかったりするＩＴＣにとっては、把握しておかなければいけない重要ポイントであり、前章までに触れた経営者とのリスクコミュニケーションを展開する上でも重要である。

以下、順を追って詳細に説明していく。

5-1.　そのセキュリティ知見はもう危険かもしれませんよ

２章で述べたようなサイバー攻撃は、2000 年頃より目立つようになってきた。当時の攻撃は、攻撃しやすい公開されているサーバ等を狙った攻撃が行われていた。その結果、ウェブサイトの改ざんの被害や、ウィルスの蔓延というような被害が発生していた。これは、単独の攻撃者が攻撃を行っており、いたずら等の目的で行われていた。これらの攻撃に対して、企業ではファイアウォールやウィルス対策ソフトの導入、脆弱性対策など、外部から組織に入り込まれないような対策（入口対策）を行ってきた。

しかし、昨今の攻撃者はサイバー攻撃をビジネスとして行っており、組織的な攻撃となり、ソーシャルエンジニアリングやゼロデイの脆弱性などを利用し、非常に

巧妙で、しかも攻撃が行われていることを発覚させない手口を使用している。その結果、企業の知財や個人情報などの重要な情報が窃取されたり、重要システムを破壊されることになる。しかも、従来であれば入り込まれることはなかった組織深部で管理している重要情報までも窃取される事案が顕在化している。

近年、その中でも特に巧妙に行われているのが、電子メールを使って企業内部の従業員（企業の幹部を含む）の端末に入り込む標的型攻撃メールと呼ばれる手口である。この攻撃はメールに業務上の連絡を装うなど手口が巧妙化・悪質化しており、手口の検知や防御は相対的に困難になっている。

従来、一定のセキュリティ対策を施していれば企業の内部まで入り込まれることはないと考えられていたが、その対策をすり抜けて企業の内部まで入り込まれている。その原因の一つは、対策の多くが外部からの攻撃を入口の部分で防ぐことを目的としているためである。

入口対策として、ファイアウォールや侵入検知システム、ウィルス対策ソフトの導入、パッチ適用による脆弱性対策等が行われているが、例えば、ゼロデイの脆弱性を狙った標的型攻撃のメールにおいては、そのメールに添付されているファイルがウィルスであったとした場合、ウィルス対策ソフトがそのウィルスを検知できない場合はウィルスに感染してしまう。

また、ウィルス対策ソフトについても、全てのウィルスを検知できるとは限らない。攻撃者は検出状況を確認し、検出されないファイルを作成してから攻撃することができるからである。

パッチ適用による脆弱性対策を行っても、ゼロデイの脆弱性を狙われた場合には有効ではない。また、ゼロデイではなくても、攻撃者が企業で使用している多種多様のソフトウェアの脆弱性を狙う可能性があるが、使用している全てのソフトウェアの脆弱性対策を実施することが難しくなってきている。

更に、ウィルスに備わっている通信機能は、Web で使う通信などを使用するため、流れている通信から異常を検知することは困難である。

このように「入口対策」は重要ではあるものの、従来の「入口対策」では防げないのが標的型攻撃メールである。従来の入口対策の知見だけで標的型攻撃メールへの対策を講じるのはもはや危険と言わざるを得ない状況である。本章では標的型攻撃メールに焦点を当て、その対策と ITC に求められる知見について解説する。

5-2. 標的型攻撃メールとは

多くの標的型攻撃メールには、メールの受信者に開封を促す件名や差出人名が付けられ、メール本文には、興味を引く内容と合わせて Web サイトへのリンクや、添付ファイルを開かせるよう巧妙な工夫が施されている。もし、不審なメールを開封し添付ファイルや URL をクリックすると、攻撃を成功させてしまう危険があり、条件が揃えばメールを開くだけでも被害に遭うこともある。攻撃が成功すると、コン

ピュータが強制的にロックされ使用不能になったり、ファイルが強制的に暗号化され、復号鍵と引換えに身代金を要求されたり（ランサムウェア）、コンピュータが外部から操作され（バックドア）、社内ネットワーク上の様々な機密情報の奪取、改ざん、破壊などに遭うなど、企業が事業継続する上で致命的なリスクになる恐れがある。また、「やり取り型（無害なメールのやり取りの後でウィルス付きのメールを送信してくる手口）」と呼ばれる攻撃も増えてきており、標的型攻撃メールの手口はますます巧妙化している。

その対策として、手口に応じて受信を拒否する対策などを施してはいるものの、標的型攻撃メールの受信を完全に拒否するような根本的な防御は困難な状況である。なぜなら、情報技術を駆使して防御策を講じても、攻撃者は次々にその手口を変化させて、防御策を突破してしまうからである。

NRI セキュアテクノロジーズ株式会社（NRI セキュア）は 8 月 18 日、「サイバーセキュリティ傾向分析レポート 2016」を発表した。そのレポートによると、「標的型メール攻撃シミュレーション（標的型メールへの対応訓練）」サービスの結果を分析したところ、およそ従業員の 8 人に 1 人、役員は 5 人に 1 人が標的型メールに添付されたファイルを開いたり、URL をクリックした。この割合は、過去 3 年にわたり大きな改善が見られないという。

このような情報セキュリティリスクを低減させるには、情報技術を駆使した防衛策を強化するだけでなく、人を中心にした対策を講じる必要がある。すなわち、社員一人ひとりがこれまで以上にセキュリティへの意識を高め、被害防止のための有効な手段を講じ、万一攻撃を成功させた場合には早期に被害を極小化できる行動をとることが重要である。

5-3. 標的型攻撃メールへの対策

標的型攻撃メールへの対策は、被害にあうことを前提にしたつぎの４つの対策が基本となる。

１．標的型攻撃の対象にならないようにする。

２．標的型メールが送られてきてもそれを排除できるようにする。

３．標的型メールに仕込まれた攻撃が実行できないようにする。

４．攻撃が実行された場合に被害を最小化できるようにする。

このうち、「３」はすべての標的型攻撃メールの手口に効果を発揮するものではなく、この対策をすり抜けて攻撃を成功させる可能性があることに留意する必要がある。また「４」は攻撃を成功させてしまった際の被害を最小化する対策であることから、標的型攻撃メールへの対策としては、「１」および「２」により攻撃を避けるようにすることが重要である。

特に「２」は、従来のセキュリティ対策の中心であった規則化や手続き化、情報技術の活用によるものではなく、人に依拠した対策になる。したがって、ITC がク

ライアントの標的型攻撃メールへの対策を講じる際には、人中心の、そして被害にあうことを前提にした対策についての知見が求められる。

5-3-1. 標的型攻撃の対象にならないようにする

自分宛に標的型攻撃メールが届くということは、自分のメールアドレスが他人に知られている恐れがあるということである。そのようなメールを減らすには、まず自分のメールアドレスをみだりに公開しないことが重要である。例えば、個人的な商品を購入するためにアマゾンや楽天などの通販サイトや、懸賞に応募する際のアカウント、その他、業務に関係のないメールマガジンやクーポンサイト、Web サイトの会員登録をする際に、会社のメールアドレスを使用すると、それらのサイトやその関連サイトからメールアドレスが不正に取得・利用されてしまう恐れがある。

また、業務と関係のない個人の SNS やブログのプロフィールなどに会社のメールアドレスを公開すると、自分が公開したメールアドレスが、標的型攻撃メールの宛先に使用される危険があることにも注意が必要である。

よって、会社のメールアドレスは業務遂行に利用するものであり、業務以外の利用は控えるべきである。会社のメールアドレスはみだりに公開せず、公私を分けて業務に関係のない利用はやめるよう規則化しそれを周知する必要がある。

5-3-2. 標的型攻撃メールが送られてきてもそれを排除できるようにする

標的型攻撃メールには、「差出人」「件名」「本文」「添付ファイル」などの機能を巧みに利用した仕掛けが仕込まれている。標的型攻撃メールを排除するのはそのメールを受信した「人」であることから、標的型攻撃メールの仕掛けの特徴を「人」つまり経営者を含むメールを利用する社員全員に理解させる必要がある。

メールの「差出人」欄は詐称できることを認識すべきである。「差出人」欄を詐称して知り合いや関係者になりすまし、受信者の警戒心を下げることができる。社内のメールには警戒心が弱いことを逆手にとり、敢えて宛先を間違えたふりをしてターゲットとは別の社員へメールを送り、その社員に不審メールを転送させて本来のターゲットへ到達させる手口もある。

「件名」欄は開封を急がせ重要なメールと思わせるキーワードが含まれる傾向にある。興味本位な件名（ゴシップや秘密を連想）で受信者の心を惑わせ、読みたくなる心理を狙う場合もある。

「本文」は特に巧妙化が進んでいる。自然な日本語表示が増え、内部関係者が使う用語や、請求書、クレームなど無視し難い内容など、不審さに気づき難く、また、無視し難くなっている。

メールの添付ファイルが圧縮ファイルの場合、解凍するだけでウィルス感染する危険がある。また Word/Excel ファイルの場合、不正なマクロが実行される危険がある。コンピュータの脆弱性が解消（最新パッチの適用など）されていない場合、PDF

ファイルなどを開いただけでウィルス感染する危険もある。

短縮 URL（http://bit.ly/　https://goo.gl/ など）が使用されている場合、リダイレクト先の URL がウィルス感染を誘導する悪意のある Web サイトになっている危険がある。

最近では、無害なメールを数回やりとりし、 相手の警戒心を下げた後にウィルス付きのメールを送信してくる「やりとり型」と呼ばれる手口が増えている。このように「不審さ」の判断は一層難しくなりつつある。さらにこの手口は電話も併用するなどますます巧妙化している。

標的型攻撃メールを PC 内に保存し続けると、後日、うっかり開封・実行することで突如攻撃を開始することも考えられるため、上記のような不審と思われるメールは削除すべきであるが、その判断が難しく、やむを得ずメールを開く場合にはウィルス感染の危険性を意識する必要がある。

5-3-3.　標的型メールに仕込まれた攻撃が実行できないようにする

受信した電子メールを html 形式で表示（開封）することにはつぎのような危険性がある。

- html 形式で表示（開封）する電子メールは、Web ページのように画像や文字フォントを駆使し、魅力的で美しい見栄えになるが、その反面、Web ページのように悪意のあるスクリプトが仕掛けられた場合、電子メールを開いただけで自動的に攻撃が実行されてしまう危険がある。
- 悪意のあるスクリプトが実行されると、受信者の知らぬ間に不正な Web サイトへ自動接続されウィルスや不正なプログラムが実行されたり、電子メールを受信したコンピュータをリモートから操作できるようにしたり、コンピュータ内にある正規のプログラムを悪用して不正な攻撃命令を実行させ、保存データの破壊や改ざんといった攻撃が成功してしまうことがある。

したがって、電子メールを開封するだけでウィルス感染するリスクを下げるために、Outlook などのメールソフトにテキスト形式で受信メールを開く設定をすることが効果的である。また、特に必要がなければプレビュー機能（受信電子メールを自動的に開封する機能）は無効（オフ）にすることをお薦めする。そうすることで、メールに埋め込まれたプログラムやスクリプトなどが起動しないようにすることができる。

5-3-4.　攻撃が実行された場合に被害を最小化できるようにする

次々に巧妙化する手口を前にして、常に攻撃を回避し続けることはとても難しい状況である。そのため、経営層を含め社員一人ひとりが攻撃を成功させてしまう可能性があることを前提とした対策や早期の対応を確実に実施することで、リスクを低減させることができる。

被害を最小化するための第一歩は、攻撃を受けた「人」の初動である。不審なファイルやURLを開いてしまった場合には、ウィルス感染した危険があることを認識し、コンピュータを社内ネットワークから切り離した後に、ウィルス対策ソフトのフルスキャン機能を実行しウィルスチェックを行う必要がある。また、不審なファイルやURLを開かない場合でも、コンピュータの挙動がいつもに比べて不自然だと感じたら、ウィルス対策ソフトのフルスキャン機能を実行しウィルスチェックを行う必要がることを認識する。

5-4. 標的型攻撃メールの見分け方

前節にて「標的型メールが送られてきてもそれを排除できるようにする」対策について解説したが、これは、標的型攻撃メールを受信した人の判断に依拠した「侵害拡大防止」、及び「監視強化」を目的としている。実際に対策を講じる際は、標的型攻撃メールがどのようなものであるかをより具体的に知ることが重要である。以下は、最近の標的型攻撃メールの特徴をまとめたものである。

(ア) メールのテーマ

① 知らない人からのメールだが、メール本文の URL や添付ファイ ルを開かざるを得ない内容
- (例 1) 新聞社や出版社からの取材申込や講演依頼
- (例 2) 就職活動に関する問い合わせや履歴書送付
- (例 3) 製品やサービスに関する問い合わせ、クレーム
- (例 4) アンケート調査

② 心当たりのないメールだが、興味をそそられる内容
- (例 1) 議事録、演説原稿などの内部文書送付
- (例 2) VIP 訪問に関する情報

③ これまで届いたことがない公的機関からのお知らせ
- (例 1) 情報セキュリティに関する注意喚起
- (例 2) インフルエンザ等の感染症流行情報
- (例 3) 災害情報

④ 組織全体への案内
- (例 1) 人事情報
- (例 2) 新年度の事業方針
- (例 3) 資料の再送、差替え

⑤ 心当たりのない、決裁や配送通知 (英文の場合が多い)
- (例 1) 航空券の予約確認
- (例 2) 荷物の配達通知

⑥ ID やパスワードなどの入力を要求するメール
- (例 1) メールボックスの容量オーバーの警告

（例 2）銀行からの登録情報確認

(イ) 差出人のメール アドレス

① フリーメールアドレスから送信されている

② 差出人のメールアドレスとメール本文の署名に記載されたメー ルアドレスが異なる

(ウ)メールの本文

① 日本語の言い回しが不自然である

② 日本語では使用されない漢字（繁体字、簡体字）が使われている

③ 実在する名称を一部に含む URL が記載されている

④ 表示されている URL（アンカーテキスト）と実際のリンク先の URL が異なる

⑤ 署名の内容が誤っている

（例 1）組織名や電話番号が実在しない

（例 2）電話番号が FAX 番号として記載されている

(エ) 添付ファイル

① ファイルが添付されている

② 実行形式ファイル(exe / scr / cpl など)が添付されている

③ ショートカットファイル(lnk など)が添付されている

④ アイコンが偽装されている

（例 1）実行形式ファイルなのに文書ファイルやフォルダのアイコ ンとなっている

⑤ ファイル拡張子が偽装されている

（例 1）二重拡張子となっている

（例 2）ファイル拡張子の前に大量の空白文字が挿入されている

（例 3）ファイル名に RLO4 が使用されている

標的型攻撃メールの騙しのテクニックは日々進化しており、人に依拠した対策であるため、全ての標的型攻撃メールを見抜けるとは限らない。そのため、経営層を含めメールを受け取る社員への教育は繰り返し実施する必要がある。また、攻撃を見抜けずすり抜けた場合を想定し、OS や各種ソフトウェアのアップデート、セキュリティソフトを最新の状態に保つといった基本的なセキュリティ対策も合わせて実施する必要があることを申し添えておく。

5-5. 標的型攻撃メールによる被害への対応

標的型攻撃メールによる被害が確認された場合には、被害を最小化する対応が求められる。以下に、対応手順を説明する。

5-5-1. 発見

標的型攻撃メールによるウィルスの感染は、多くの場合、ウィルス対策ソフトや

同様のメールを受信した外部からの情報・通知により発覚する。

＜例＞

1 ウィルスに感染し、パソコンを不正操作され、パソコン内の機密情報が悪意のある第三者に窃取された。

2 ウィルスに感染し、会社機密情報が Web サイトに掲載され、不特定多数の人に閲覧可能な状態になった。

5-5-2. 初動

ウィルスの存在が確認された場合は、直ちに当該パソコンの使用を停止し、ウィルスの除去などの対応をおこなう。その場合、ウィルスの種類が特定できる場合は、IPA やウィルス対策ベンダーなどの情報に基づき対処する。

＜例＞

1 ウィルス感染したパソコンの特定

2 ウィルス感染したパソコンのネットワークからの切り離し

つぎに、感染したパソコンに、何の情報がどの程度含まれていたのか、暗号化やアクセス制限の有無を確認する。具体的にはつぎのとおり。

＜事実関係を５Ｗ１Ｈで整理する＞

1 ウィルス感染した当事者は誰か？

2 何(物)がウィルス感染したのか？

3 ウィルス感染により漏えいした情報は何か？

4 いつウィルス感染したのか？

5 どこでウィルス感染したのか？

6 なぜウィルス感染したのか？

7 ウィルス感染が発覚した理由は何なのか？

＜情報について＞

1 誰の情報か？

2 何の情報か？

3 いつ頃の情報か？

4 情報の量（件数）はどのくらいか？

5 どのような形で保存されていたか？ （暗号化／平文、HDD 保護、パスワード 保護など）

5-5-3. 調査

重要なデータをいったん外部メディアにバックアップする。バックアップには不正プログラムが混入している可能性も高いので取扱いに注意する。パソコンに残されたデータやアクセスの履歴から情報漏洩などがないか確認する。情報漏洩が確認された場合には、被害の重要度を判定する。

1 漏えいした情報区分は？（個人情報／公共性の高い情報／一般情報）

2 漏えいした情報の保護策は、何を実施していたか？

3 影響はどこにあるか？（個人／公共インフラ／特定企業）

4 管理上の問題点は？

5-5-4. 通知・報告・公表等

情報漏洩が確認され、漏洩情報に個人情報が含まれる場合には本人に通知しお詫びする。

5-5-5. 抑制措置と復旧

被害にあったパソコンは念のため OS からインストールしなおした方が良い。プログラムもバックアップから戻さず、再インストールしなおした方が良い。バックアップのデータについては、最新のウィルス定義ファイル等を使用して検査し復旧する。

＜二次被害防止策例＞

1 ウィルス名の特定と駆除

2 ぜい弱性の除去

3 漏えいした情報の回収

4 クレジットカード、銀行口座番号、ID パスワードが含まれていた場合、本人に通知し、カード停止、口座停止、ID 停止などを促す

5-6. 人中心のセキュリティ対策を有効に機能させるには

前節では、人中心で、被害にあうことを前提にした標的型攻撃メールへの対策について述べた。本節では、実際に人中心のセキュリティ対策を実施するうえで必要となる知見について述べる。

5-6-1. ヒューリスティックな判断

４章で述べたように、人には重要・緊急と感じない事案については、ヒューリスティックな判断をおこなう傾向がある。ヒューリスティックな判断とは、不確かな状況下で判断や意思決定を行う際に使用する簡便で直感的な思考のことで、自身の経験に基づくため、判断の時間は早いが、必ずしもそれが正しかったり適切だったりするわけではなく、一定の偏り（バイアス）を含んでいることが多い。

さて、経営者や社員にとって情報セキュリティはどの程度重要・緊急な事案と捉えられているであろうか。もし、情報セキュリティに関する事案が重要・緊急でなければ、情報セキュリティ事案に対してヒューリスティックな判断が行われる可能性がある。

そのように考えると、前節で述べたような標的型攻撃メールへの対策を有効化するためには、知識を中心とした教育に加えて、標的型攻撃メール、ひいては情報セキュリティへの意識を高める教育が重要になるといえる。言い換えると、情報セキュリティへの意識が低い「人」に知識ベースの標的型攻撃メール対策を教育しても、

実際の事案に際して知識が活かされることは期待できないということになる。

また、情報セキュリティに関するヒューリスティックな判断はITCに対してもいえると思われる。4章にて「セキュリティ事故などの重大事故が発生した場合でも、人は従来から持ち合わせている判断傾向を維持し、新しい事実を受け入れたがらない傾向を持ちたがることを理解しなくてはならない」と指摘した。ITCにとって標的型攻撃メールが重要・緊急な事案でなければ、ITC自身の経験に基づくヒューリスティックな判断が行われ、標的型攻撃メールに対して有効ではない従来型の対策を講じる危険性があるのではないだろうか。

いずれにしても、標的型攻撃メールへの対策を講じるITCは、このヒューリスティックな判断に関する知見を習得する必要があると考える。

5-6-2. 効果的な意識付け

では、どのようにすれば標的型攻撃メールに対する意識付けができるだろうか。多くの企業で行われている情報セキュリティに対する意識付けは、実際に起こったセキュリティ事故を例に、「もしこのようなセキュリティ事故が自社で発生したらどうなるか」について考えさせる方法がとられているようである。しかし、実際には情報セキュリティの重要さについては認識させることができるものの、「そのような事故が自社で発生する可能性は低い」などのように自己判断する社員が多いようである。これでは情報セキュリティに対する重要性の認識は低く、ヒューリスティックな判断に陥る危険性がある。

そこで、実際に起きたセキュリティ事故と経営者や社員一人ひとりと関連付け、より身近な問題として考えさせるやり方のほうが効果は期待できると思われる。つまり、標的型攻撃メールによるセキュリティ事故は、セキュリティ対策が十分でない企業で、セキュリティ意識の低い人だけが引き起こすのではなく、セキュリティ対策を実施しており、セキュリティ意識がある人でも攻撃を成功させてしまう可能性があることを認識させるのである。標的型攻撃メールを成功させる行為を理解させ、企業のセキュリティシステムを過信させないようにするのである。

また、同じようなセキュリティ教育を繰り返し行うと人は慣れてしまうため、ヒューリスティックな判断を引き起こす要因になることにも留意する必要がある。そのため、常にセキュリティに関する最新の情報を取り入れ、形を変えながら実施することが肝要である。

5-7. セキュリティ知見をたえず更新するために

独立系ITCの場合、サイバーセキュリティ対策のような最新セキュリティ情報に触れる機会が少なく、知見が陳腐化する傾向にあると思われる。また、企業内ITCの場合には、従来のテクノロジー主体の知見に偏る傾向があり、「人中心のセキュリティ対策」への配慮に欠ける傾向にあると思われる。

ＩＴＣは常に最新のサイバー攻撃の実態とその対策に関する情報を収集し、対応能力を向上させる必要がある。そのために活用できる情報源として、ＩＰＡの情報セキュリティサイトを参照することをお勧めする。同サイトには情報セキュリティに関する様々な最新情報が掲載されている。中でも「対策のしおり」にはセキュリティ対策を立案するうえで有用な情報が掲載されている。

本稿執筆時点でつぎのようなしおりが掲載されている。

「IPA 対策のしおりシリーズ」

1.「ウィルス対策のしおり（第 10 版)」
　～コンピュータウィルスからあなたのパソコンを守るには !!～
2.「スパイウェア対策のしおり（第 10 版)」)
　～気付かぬうちにスパイウェアに侵入されていませんか？～
3.「ボット対策のしおり（第 10 版)」
　～あなたのパソコンはボットに感染していませんか？～
4.「不正アクセス対策のしおり（第 6 版)」
　～大丈夫ですか、あなたのパソコン？（パソコン利用者向け）
5.「情報漏えい対策のしおり（第 7 版)」
　～企業（組織）で働くあなたへ 7 つのポイント !!～
6.「インターネット利用時の危険対策のしおり（第 4 版)」
　～インターネットに潜む悪意 こんな手口に騙されないで !!～
7.「電子メール利用時の危険対策のしおり（第 4 版)」
　～電子メールを介したトラブル こんな対策が必要です !!～
8.「スマートフォンのセキュリティ<危険回避>対策のしおり（第 2 版)」
　～便利な道具 スマートフォン　安全・安心利用のためのセキュリティ対策で危険回避 !!～
9.「初めての情報セキュリティ対策のしおり（第 1 版)」
　～新入社員の皆さん「情報セキュリティ対策」って知っていますか？～
10.「標的型攻撃メール<危険回避>対策のしおり（第 1 版)」
　～特定企業・組織への狙い撃ち攻撃 その発端となる最初の攻撃はメールから始まる !!～
11.「無線 LAN<危険回避>対策のしおり（第 1 版)」
　～企業・組織での無線 LAN の導入・運用時の危険回避を考える !!～
12.「暗号化による<情報漏えい>対策のしおり（第 1 版)」
　～暗号化は情報セキュリティ対策の重要なアイテムです。暗号化を理解し、情報漏えいを防ぎましょう !!～

「IPA セキュリティマネジメントのしおりシリーズ」

1.「企業（組織）における最低限の情報セキュリティ対策のしおり」

2.「中小企業における組織的な情報セキュリティ対策ガイドラインチェック項目」

3.「中小企業における組織的な情報セキュリティ対策ガイドライン事例集」

4.「情報セキュリティ対策ベンチマーク」

（企業・組織のためのセキュリティ対策自己診断ツール Ver.4.x）

「姉妹冊子」

1.「クラウドサービス安全利用のすすめ」

～中小企業のみなさん　自社の IT 環境の改善のためにクラウドサービスの導入を検討するときは、安全についての確認もしっかり実施しましょう !! ～

2.「情報漏えい発生時の対応ポイント集」

～情報が漏えいしてしまった時、何をすべきか !!～

6. まとめ

サイバーセキュリティを取り巻く環境は日々変化しており、攻撃手段もより複雑化・悪質化してきている。先にも述べたが、今日まで有効だった対策も、明日には通じなくなっているかも知れない。

セキュリティ事故は、一度起こってしまえば甚大な被害を企業にもたらし、信用を地に落とすため、サイバーセキュリティ管理部門の担当者は、常に最新の対策を徹底することが求められる。

経営者の役割はこの担当者に対して、自身が先頭に立つ強い意思表示と、相応の動機付けとを与えて頂かねばならない。

この経営者の方たちを支援する立場にある、ITC の役割も理解頂けたのではないかと思う。

最後に、本論文が読者諸兄の役に立てれば幸いである。

以上

参考資料：

1．「サイバーセキュリティ経営ガイドライン」（経産省、IPA）
2．「サイバーセキュリティ経営ガイドライン解説書」（IPA）
3．「中小企業の情報セキュリティ対策ガイドライン（第 2.1 版）」（IPA）
4．Japan Security Vision 2017(3 月 2 日開催) NISC(内閣サイバーセキュリティセンター)
講演「わが国におけるサイバーセキュリティに対する取り組み」より
5．総務省 サイバーセキュリティタスクフォース(第１回) 配布資料
6．警察庁「不正アクセス行為対策等の実態調査」（平成 28 年度）
7．奈良由美子氏（2016）「リスクコミュニケーション論」 講義教材
8．IPA 対策のしおりシリーズ（IPA）
9．テクニカルウォッチ「標的型攻撃メールの例と見分け方」（IPA）
10.「新しいタイプの攻撃」の対策に向けた設計・運用ガイド 改訂第２版（IPA）
11. セキュリティの最初の防衛線（NRI）