金融分野における サイバーセキュリティ対策の勘所

東証コンピュータシステム リスクマネジメント室
情報セキュリティスペシャリスト、CISSP、システム監査技術者
菅原　昭伸

1．はじめに

セキュリティ（security）の語源はラテン語のsecuritas（se＝free from：……からの自由、curita＜cura＝care：不安、心配）で、個人、社会などの不安を解消することが本来の意味であろう。ちなみに、金融用語では、言うまでもないが、有価証券（国債、株券）や担保のことを指す。

サイバー空間が、陸・海・空、そして宇宙空間につづく、第五の戦場と呼ばれてすでに久しいが、さきの米国大統領選挙にロシアの介入が疑われたという。

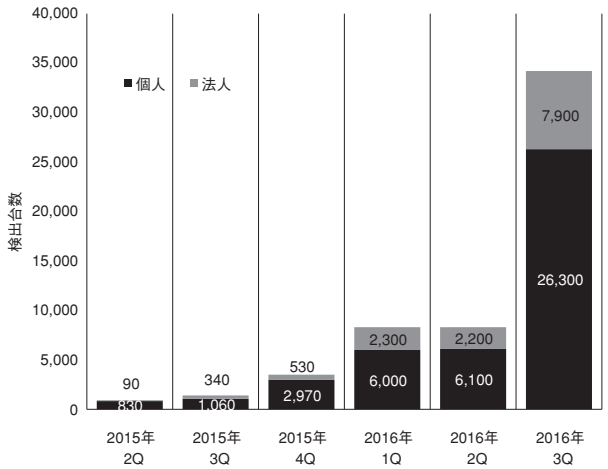
この種の報道には、どこまでが真実なのか、一般の我々には判然としないことが多いのだが、サイバーセキュリティに関する国や金融庁の取組みを概括したうえで、サイバーセキュリティ対策の勘所を、特にITガバナンスの観点も含めて、述べてみたい。

〈目　次〉

2．昨今のサイバーセキュリティ事情

昨今のサイバーセキュリティ事情として、先ず取り上げるべきは、ランサムウェアであろう。ランサムウェアとは『ransom』（身代金）と『software』を組み合わせた造語で、パソコン内のファイルを勝手に暗号化し自分のファイルを読めなくしてしまうウイルスの総称である。それらの復旧を条件に身代金を支払うように促す脅迫メッセージを表示させることから、ランサムウェアと呼ばれている。

（図－１）国内ランサムウェア検出台数



（出典）「2016年第３四半期セキュリティラウンドアップ」トレンドマイクロ社のデータより、著者が作図

情報処理推進機構（以下、IPAと略す）が今年の１月に公表した、『情報セキュリティ10大脅威 2017』でも、組織への脅威を対象とした分野で昨年の７位から２位にランクが上昇している（注１）。また、図－１はトレンドマイクロ社のデータだが、2016年から飛躍的に伸びている。特に、従来、個人を狙ったものが多かったのだが、最近では法人が狙われていることを示している。

このランサムウェアだが、最近はますます悪質になってきている。例えば、何時までであれば、この程度の身代金で良いが、それを過ぎたら10倍の身代金になるというふうに、早く何とかしなければ、と被害者に思わせるような巧みな攻撃が最近では多くなってきている。

なぜこんなに増えているのか。最近はクラウド上でのランサムウェアを提供するランサムウェア as a serviceといったサービスもあり、あまり知識がなくても、攻撃が可能な状況が整ってきていることが背景にある。

つまり、標的型攻撃メールのように、狙った企業のネットワーク内に長く潜んで、丹念に情報を探さなくても良い。あるいは、盗んだ情報の買い手を探さなくても良く、手軽にお金を手に入れることができる。犯罪者にとって投資対効果の高いビジネスモデルとして確立されてきたことが要因である。

二つ目のセキュリティ事情は、Business E-mail Compromise、いわゆるビジネスメール詐欺と呼ばれるものを紹介しよう。この詐欺は通常、企業幹部などのEメールアドレスに侵入して、そのアカウントを悪用する『なりすまし詐欺』から始まる。サイバー犯罪者は企業の幹部社員を装って何も知らない従業員にメールで連絡して、海外取引先の口座等

へ多額の送金を指示するといったものである。こういった指示を出すのはCEOだったりするのだが、例えばそのCEOが海外へ出張しているタイミングとか、あるいはこの案件は秘密に進めている海外企業の買収のために使う費用なので誰にも相談せずに処理しろとか、言葉巧みに操って、実行させるというものだ。

FBIの調査によると（注２）2013年10月から2016年の５月までで、15,668の企業が被害に遭っており、被害総額は約30億ドルと言われている。一方、トレンドマイクロ社の調査（注３）では、昨年の上半期の被害法人数は、米国では2,496法人、日本は４番目で218法人となっている。この手法はメールに侵入するところを除けば、後はソーシャルエンジニアリングの手口と言ってよい。したがって、何かツールを入れて防げるというものではなく、あくまでも人を言葉巧み操って、目的の行為をさせるというものになっている。情報セキュリティの世界では、人が最大のセキュリティ・ホールだという言葉があるが、まさにその典型的な犯罪だと言ってよい。

日本での発生件数は、日本語の問題があるからだとみえて、まだまだ少ないが、今後ますます増えてくることが予想され、要注意である。

３．国及び金融庁の動向

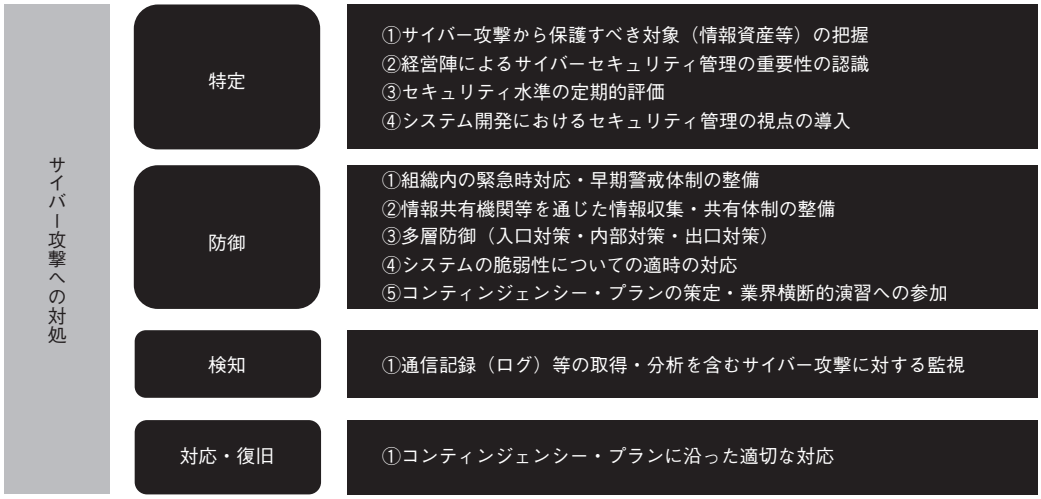
次に、こうしたサイバーセキュリティの状況に対するNISC（内閣サイバーセキュリティセンター）や金融庁に代表される動きについて見ておこう。まずは、2014年11月のサイバーセキュリティ基本法制定以降の動きに絞れば、2015年４月には、金融検査マニュアルが改正され、システムリスク管理態勢が大幅に加筆されている。同じく金融庁は７月に『金融分野におけるサイバーセキュリティ強化に向けた取組方針』（注４）を公表している。その中で、五つの方針として、

- ❏ サイバーセキュリティに係わる金融機関との建設的な対話と一斉把握
- ❏ 金融機関同士の情報共有の枠組みの実効性向上
- ❏ 業界横断的演習の継続的な実施
- ❏ 金融分野のサイバーセキュリティ強化に向けた人材育成
- ❏ 金融庁としての態勢構築

を掲げている。なんといっても、最初の金融機関との建設的な対話と一斉把握の中で金融庁が重視している対策が透けて見えてくる。サイバー攻撃への対処という中では、特定・防御・検知・対応と復旧という四つの項目が掲げられている（図－２参照）。図－２には記してないが、顧客保護の観点でいうと、サービスの提供状況・顧客への働きかけといった２項目が対象として挙げられている。

一方で、2015年12月には経済産業省が、経営者向けに『サイバーセキュリティ経営ガイ

（図ー２）金融庁　サイバーセキュリティ対策重点項目



ドライン』(注５)を公表している。また、昨年８月には、NISCが『企業経営のためのサイバーセキュリティの考え方』(注６)のなかで、サイバーセキュリティ対策は、より積極的な経営への投資であることを強調している。

４．金融庁が重視するセキュリティ対策

まずサイバー攻撃への対処として、「特定」の分野では、一つ目に「サイバー攻撃から保護すべき対象（情報資産等）の把握」と書かれている。何を守るのか、を明確にさせることはセキュリティの基本だが、ここでは情報資産の把握だけに言及している。ただし、本当に大切なのはその後のリスク評価となる。自社がどのようなリスクを抱えているかをしっかり分析して、対策を立案し、計画的に実行していくことが何よりも大切である。金融庁は、決して、サイバーセキュリティ対策の正解を言ってはくれない。

「特定」の二つ目には、「経営陣によるサイバーセキュリティ管理の重要性の認識」と書かれている。具体的にどんな行動をとっていれば、経営陣が主体的にサイバーセキュリティに関与していると言えるのか。ここでは私が考える例を挙げよう。①セキュリティ対策の中期計画の進捗状況について取締役会等でちゃんと報告を受けて確認している。②自社における情報セキュリティに関する事故について、例えば携帯電話を紛失してしまった程度の軽微なインシデント、あるいは標的型攻撃メールを何件ぐらい受けているといった発生状況と対策について、定期的に取締役会等で報告している。③他社で発生した事故に関

する調査報告書（例えば、年金機構の事例）が出た時に、その中で対策の不備が記載されていたときに、その対策が自社ではどうなっているかということを振り返って必要な手を打つ。そんな状態であれば、経営陣がサイバーセキュリティに関与していると言えるであろう。また、仮に情報漏洩で訴訟に巻き込まれる場合もあることを考えると、善管注意義務の観点から、取締役会の議事録の作成等の証拠作りも忘れてはならない。

「特定」の三つ目は「セキュリティ水準の定期的評価」である。①セキュリティの状況を客観的に第三者等によって評価をし、世間一般及び業界内のレベルと比較しておく。それも定期的に実施して、システム環境が変化したり、周りの環境が変わった時に改めて評価をして、状況の推移を見ておくことが大切である。ここでは、第三者による、というところがポイントである。②システム開発におけるセキュリティ管理の視点の導入である。作った後からセキュリティを考えるのではなくて、設計の段階からしっかり考えてモノ作りをしなさいと言っているわけだ。IoT機器等では特に重要な項目となる。

次は「防御」項目だ。一つ目に、「組織内の緊急時対応・早期警戒体制の整備」が挙げられている。CSIRT（Computer Security Incident Response Team）は、コンピュータセキュリティに係るインシデントに対処するための組織の総称である。CSIRTというのは、情報システム部だけではなく、広報部、法務部など、関連部署がチームをつくり、そして当然ながら経営者が陣頭指揮をとる。これも侵入されることを前提として体制を取れということである。

続いて「防御」の二つ目だが、「情報共有機関等を通じた情報収集、共有体制の整備」だ。情報共有の意味は、例えばある証券会社がこんな標的型攻撃を受けたということを、間に入っている機関を通して業界内に広める。そうすることによって、未然防止の措置をとることが可能となる。そういう点で情報共有は大変意味があると言われている。金融業界の場合、金融ISACという団体が中心になってそうした活動をしている。2017年２月現在271社が正会員として活動している。

各業界を所管する省庁が縦割りのせいだと思うが、経済産業省傘下には電力業界、石油業界や自動車業界など幾つか業界団体があり、ほかにも医療関係については厚生労働省であるとか、交通インフラについては国土交通省とか、それぞれの分野ごとに活動をしている。国として情報共有を進めているのは主に重要インフラ（日本では13分野）と指定されている分野に限られている。分野間の情報共有も勧めるためには、ここらの縦割りの構造の解消は今後の課題であろう。

「防御」のところで、三つ目が「多層防御」ということが言われている。セキュリティというのはもともと初期の侵入を防ぐという入口対策だけをやってきたが、攻撃がますます巧妙になってくるので、初期の侵入を止める

ことができなくなってきている。そこで内部対策として、内部のネットワークを相手が偵察している状況とか、外に情報を持ち出す時の出口対策とか、こういうことをちゃんとやっていかないと防げないということで最近、多層防御ということがしきりに言われている。

続いて「防御」の四つ目、「システムの脆弱性についての適時の対応」。規模の大きな組織だと、WSUS等を利用してセキュリティパッチを配信されているケースが多いと思う。一方、小規模の組織の場合、個人にWindows Updateを手動で実施させる方法もあるかと思うが、やりっ放しにしてはいけない。確実に実施していることの確認が必要で、『やれ』と指示を出しただけではなくて、少なくとも『やりました』という返事ぐらいはもらっておかなければいけない。時には抜き打ちで本当にやっているかどうかをチェックしてみるといった行動が必要だろう。

また、webサイトを保有している企業が多いと思うが、それにコンテンツ・マネジメント・システム（CMS）を利用している場合、そのCMSとプラグインの脆弱性もしっかり把握しておく必要がある。相変わらず、Webサイトからの情報漏洩や改ざんは続いており、これについて2016年９月に、IPAより『CMSを用いたウェブサイトにおける情報セキュリティ対策のポイント』（注７）という文書が公開されている。大いに参考にすべき資料だと考える。

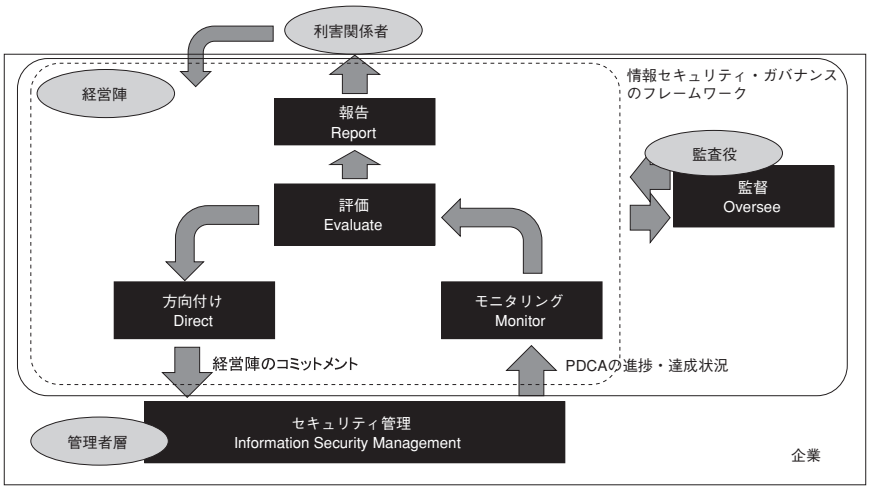
「防御」の五つ目は、「コンティンジェンシープランの策定・業界横断的演習への参加」で、いわゆるBCP、事業継続計画をちゃんと作っておきなさいということになる。特にシステムの関係でいうと、先ほどお話ししたようにランサムウェアがこれほど流行っていると、ランサムウェアにかかってしまうとお金を払う以外の手段として、あとはもうバックアップから戻すしかない。これが唯一の手段となるので、バックアップは大変に重要となる。

「防御」の六つ目は、「業界横断的演習」で、これは昨年10月後半に金融庁で実施し、全部で77の金融機関が参加したと言われている。金融庁は各社の結果から浮かび上がった問題点を洗い出して、今回の演習に参加していない金融機関にも分析結果を知らせると言っているが、2017年２月15日時点ではまだ公表されていない。もう少し時間がかかるものと思われる。

続いて「検知」の項目だが、「通信記録（ログ）等の取得・分析を含むサイバー攻撃に対する監視等」とある。ログの監視というのは、問題の早期解決だけではなくて、取引先や顧客に対する説明責任や証拠確保の面からもログは大変重要となる。現実的には、ログは何かあったときのために取得はしているものの、日常的は監視まではできていないという企業が多いと思われる。

以上が昨年に出たサイバーセキュリティ強化に向けた取組方針の中で述べている、これ

（図ー３）サイバーセキュリティ・ガバナンスの枠組み



だけはやりなさいと金融庁が言った内容となる。次に、2016年９月に、取組みを過去１年間やってきて振り返った時の状況を金融庁の金融レポート（注８）の中で、次のように書かれている。一部の金融機関においては、経営陣の積極的な関与の下、おおむねサイバーセキュリティ対策の態勢整備が進んでいるものの、以下三つのことができていないと言っている。①従来目線でのリスク評価のみにとどまり、サイバーセキュリティに着眼したリスク評価が未実施である。②ログ分析が不十分である。③実効性のあるコンティンジェンシープランが未整備である。この３点を挙げている。特に態勢整備が遅れている根本的な要因について、経営陣の関与が受動的であるといったことが共通していると述べている。

５．サイバーセキュリティのガバナンス

コーポレートガバナンスとは、「企業経営において、経営上の意思決定が企業の価値創造にとって有効な判断となるように管理・統制する仕組み」といった理解が一般的であろうが、「株主による経営層の統治」が有効に機能するためには、「経営層による企業内統治」が有効に行われることが前提となると考えられる。

サイバーセキュリティガバナンスのフレームワーク（注９）は、経営戦略やリスク管理の観点から行う「方向付け（Direct）」、ガバナンス活動の状況を指標に基づき可視化する「モニタリング（Monitor）」や結果を判断する「評価（Evaluate）」、これらのプロセスが

（表－１）望まれるモニタリング指標の特性

特性	概要
Specific	主観や判断が入らないように、明確にモニタリング指標が定義されていること
Measurable	本質的に数値ができるモニタリング指標であること
Attainable	予算や技術的な制約の中で、継続的に取得可能な指標であること
Repeatable	測定者や測定場所が異なっても、同じ対象については同じモニタリング結果が得られること
Time Depend	時間と共に変化するモニタリング指標であること。

機能していることを確認する「監督(Oversee)」、結果を利害関係者等に提示する「報告（Report)」の五つの活動から構成されるものと考えられる。

この五つのプロセスはいずれも大切なプロセスではあるが、あえて誤解を恐れずに言えば、五つの活動の中で最も重要なものはモニタリングであるといって良いだろう。これがしっかりできていないと、目が見えない状態で車を運転しているようなものであろう。モニタリングは、適切にリスク管理がなされていることを経営陣が理解できる形で示し、経営陣が評価を行えるようにするために必要な情報を収集する活動であり、有効かつ適切な評価指標が設定されることが必要である。

モニタリング指標は表－１に示す特性を満たすことが望ましい。この指標が適切でないと、活動全体があらぬ方向へ向かってしまうことになるので、慎重に検討する必要がある。

特に、大企業となると、グループ各社の状況をモニタリングすることも念頭に置く必要がある。特に、海外も含む場合には、情報セキュリティに対する意識の共有も含めて、スタート時にしっかり意思疎通を図っておくことが望ましい。さらには、外部委託先なども巻き込んだモニタリングなども検討する必要もある。

金融庁に限らず、最近のサイバーセキュリティに関する国のメッセージはもっぱら経営者に向けたものが多い。経済産業省の『サイバーセキュリティ経営ガイドライン』やNISCの『企業経営のためのサイバーセキュリティの考え方』はその代表である。

サイバーセキュリティ戦略本部が昨年８月に公表した、『サイバーセキュリティ2016』(注10)には、経営層の意識改革として、

「内閣官房及び金融庁において、上場企業におけるサイバー攻撃によるインシデントの可能性等について、米国の証券取引委員会（SEC）における取組等を参考にしつつ、事業等のリスクとして投資家に開示することの可能性を検討し、結論を得る。その際、関連情報の共有など開示するインセンティブを促すための仕組みの在り方についても併せて検討し、結論を得る。」としている。

まさに、経営者にとっては、サイバーセキュリティのガバナンスの枠組みをしっかり作り上げることが求められている、と言ってよい時代になった。

(注1) http://www.ipa.go.jp/security/vuln/10threats2017.html

(注2) https://www.ic3.gov/media/2016/160614.aspx

(注3) TrendMicro Direction2016『被害額は2億円? 情報と事業を破壊するサイバー攻撃の最新事情』より抜粋

(注4) http://www.fsa.go.jp/news/27/20150702-1.html

(注5) http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html

(注6) http://www.nisc.go.jp/conference/cs/jinzai/wg/index.html

(注7) https://www.ipa.go.jp/security/technicalwatch/20160928-1.html

(注8) http://www.fsa.go.jp/news/28/20160915-4.html

(注9) http://www.ipa.go.jp/security/manager/know/meaning/governance.html

(注10) http://www.nisc.go.jp/active/kihon/pdf/cs2016.pdf