資料１

サイバーセキュリティ戦略本部
普及啓発・人材育成専門調査会
セキュリティマインドを持った企業経営ワーキンググループ
第１回会合　議事概要

１　日時
平成 28 年 4 月 28 日（木）　13:30～15:30

２　場所
内閣府庁舎別館９階会議室

３　出席者（敬称略）

（主査）	林　紘一郎	情報セキュリティ大学院大学　教授
（委員）	引頭　麻実	株式会社大和総研　専務理事
	大杉　謙一	中央大学　法科大学院　教授
	岡村　久道	英知法律事務所　弁護士
	落合　正人	SOMPO リスケアマネジメント株式会社 ERM 事業部　部長
	野口　和彦	横浜国立大学　大学院　環境情報研究院　教授
	橋本　伊知郎	野村ホールディングス株式会社　参事　Co-CIO 兼 IT 統括部長 野村證券株式会社　経営役
	丸山　満彦	デロイト トーマツ リスクサービス株式会社 代表取締役社長

（事務局）	谷脇 康彦	内閣審議官
	三角 育生	内閣参事官
	阿蘇 隆之	内閣参事官
	八剱　洋一郎	指導専門官

（オブザーバー）　金融庁
経済産業省

4 議事概要

（1）谷脇内閣審議官挨拶

（2）セキュリティマインドを持った企業経営ワーキンググループ（WG）について

事務局から、資料 1、資料 2、資料 3 に沿って説明。

その後、林委員を主査に互選。

（3）セキュリティマインドを持った企業経営に係る検討について

事務局から、資料 4、資料 5 に沿って説明。

その後、委員による自由討議が行われた。委員から以下のような意見が述べられ、それに対し事務局が説明を行った。

委員からの発言の概要は以下のとおり

（引頭委員）

・資本市場からみると、サイバーセキュリティにはあまり関心がないというのが現在の実情。しかし、サイバーセキュリティのリスクは、大企業だけではなく中小企業も高く、中小企業の対策も必要と見られる。例えば、大企業を中心とした、いわゆるバリューチェーンあるいはサプライチェーンにおいて、ネットで繋がっている各取引先に対して、サイバーセキュリティに関する指導を大企業に積極的に取り組んでいただくという仕組みを考えていく必要があるのでないか。

・また、日本のビジネスフィールドの意識改革として、サイバーセキュリティへの対応というのは、日本で仕事をするための入場料、すなわち必要投資という考え方もあるのでないか。

・東京証券取引所で、コーポレートガバナンス・コードが昨年から採用された。その中で、取締役あるいは監査役へのトレーニングという項目がある。これは、外部環境の変化に応じて、経営者が様々なトレーニングを取り入れ、それを経営に生かしなさいということだ。これを踏まえれば、新しい経営環境の重要な要素としてサイバーセキュリティを位置づけ、これをトレーニングしていることについて開示してもらうというのも方策の 1 つでないか。

（大杉委員）

・日本企業と外国企業を比較した場合、日本企業はメンバーシップ型で、会社に就職して、会社の文化とか帰属意識を持ち、OJT を通じてローテーションして、自己の能力を磨いて出世していくシステムであり、経営者は自分が今までやってきたこと、経験してきたことの延長線上で物事を考える傾向にある。一方で、外国企業はジョブ型といって、自分の能力と時間を企業に売って給料を稼ぐシ

ステムであり、経営層は資源の配分者であり、理論上起こりうる問題に対して備えるべきとした考えがある。こうした、日本の経営者の特性も考慮した上で、サイバーセキュリティに対する経営者の考え方についても検討する必要があり、単純に教科書的なアメリカの経営者像をそのまま当てはめることは難しいのでないか。

・コーポレートガバナンスから考えると、自社の経営資源でなるべく高い利益を上げるだけではなくて、社会的責任はきちんと果たすことは世界共通であると考える。サイバーセキュリティに関しても、ネットワーク外部性のある話であり、個社にとっての最適な水準ではなく、社会的に最適水準の情報セキュリティへの投資額を考えていくということは、大企業の経営者として、当然負う責務としての社会的責任という形で訴えかける方がいいのでないか。

（岡村委員）

・経営者層自体がセキュリティ以前の問題として、経営における IT、ICT 自体の重要性をどこまで理解しているのかどうかということが非常に心もとない。今後は、世界各地から集まるデータやノウハウを集約して、それを分析してサービス化できるかどうかということが重要になってくる。そうしたサービスの重要性がわかる IT、ICT に強い経営者は、当然セキュリティは重要であることがわかっており、そうした経営者の育成が必要。

・サイバーセキュリティ＝個人情報漏洩対応対策　としたステレオタイプ的な認識を変えなければならない。

・中小企業のセキュリティ対策というのが後手後手に回っている。ISMS は中小企業には重すぎると感じているので、中小企業でも取り組めるようなベーシックなレベルから始めて、最終的には国際標準に適合していけるような仕組み作りが必要でないか。例えば囲碁における昇段制度のような仕組みで、最終的には最上位が ISMS に相当するような制度があってもいいのではないか。

（落合委員）

・サイバーセキュリティの保険では、個人情報及び企業情報のいわゆる漏えい対応やシステム停止対応について、それぞれの対処費用や賠償対応、システム停止による事業中断の利益損失、さらには収入が入らない間、継続してテナント等を維持するための営業継続費用、こういったものをカバーすることになっていることが多い。付保すべき保険金を検討する際に、個人情報漏洩の際の調査に係る費用、賠償額などはある程度目安がつくが、それが企業情報、営業秘密の値段は幾らになるのか、また、システム復旧目標時間というものの蓋然性といったことやカバー対象となる事案の全てが複合発生する場合についてまで考えている企業はあまりないのが現状。

・経営陣にセキュリティの重要性をわかってもらうには、それはどれぐらいの影響があって、財務的にどんなインパクトがあるのかという話が伝わらないといけない。それから考えると、橋渡し人材は、経営陣に近い経営企画や社長室、リスク管理部門、内部監査部門などが担うのがいいのでないか。

（野口委員）
・リスクマネジメントとリスク管理という２つの概念を明確に仕分けるべき。リスクマネジメントは、マネジメントの判断を支援するものという位置づけが世界標準になっている。安全管理とか、セキュリティ管理とか、管理という言葉を使ってしまうがゆえに、経営者の人たちは、この仕事は担当管理者の責任だということで、全部部下に落としてしまう。経営者にとっては、サイバー空間や IoT という新しいものの中で、企業経営で重要なリスクへの対応をいかに自主的にやるかというマインドがとても大切であり、リスクマネジメントをしなくてはいけない。
・担当者は、セキュリティは他の何よりも重要なのに経営者は理解してくれない、という考えになりがちだが、今の経営の中で、何をどう判断して、情報セキュリティをどう位置づけるかを、経営者の判断に必要な情報を提供するという観点で整理が必要なのではないか。
・情報セキュリティについては、個人情報が盗まれるのが非常に大変と思っている経営者が多いが、今の情報セキュリティというのはそういうレベルのものでない。制御系のセキュリティも含めて、情報セキュリティとは何かということをきっちりと経営者に届けないといけないのでないか。
・日本での安全対応はほとんど再発防止であり、先取りして対応するリスクマネジメントはほとんどない。

（橋本委員）
・サイバーセキュリティについて理解してほしいのは、経営者はもちろんのこと、予算全体を取り纏める財務部門、PL で負担をかけるビジネス部門等と幅広い。そのため、必要な活動について経営者の理解を得ることに加え、実務上は、例えば全てのマネージャーが集まるミーティングで経営からセキュリティへの取り組みの重要性に言及してもらうなどして、関連部門に活動を是認してもらうことの意味も大きい。
・これだけサービス化が進むと、自社所有のシステムだけでなく、プロバイダーから提供される共用型のソフトウェアやクラウドも同一の安全がないといけない。しかし、現状は、ユーザーとサービスプロバイダー間のサービスレベルに関する条件が折り合いにくく、お互いリスクを感じながらなんとか契約に漕ぎ着けている状況。業界全体で直視すべき課題。

・同じサイバー攻撃でも、DDOS 等による業務停止、不正ログインによる情報搾取、不正送金による金銭詐取など、多種多様。個別事案の対処も重要であるが、一方で常に全範囲の安全を確保しなければならない。また、大規模システム障害や地震のような大規模災害とサイバーセキュリティは、似た点も多いが、決定的に違うのは、犯人がいるというところ。したがって、産も官も学も手を取り合って犯行グループに立ち向かう枠組みが不可欠。
・一般事業会社では、社内で IT 人材の育成が難しい場合が多く、IT 業界などから専門家を招き入れることも多い。その際、IT やセキュリティの専門家と、社内のビジネスや成り立ちを理解している人材とをうまく組み合わせる必要がある。

（丸山委員）
・事務局の方でタイプ別に３つに分けられたが、①のグローバル企業においては、欧米の進んでいる状況に対応しつつある、②の IT・セキュリティを基盤として考える企業については、やる気はあるので、方法さえ示してやればあとは自分でやると思う。問題は③の自ら対策を行えない企業で、社会的にセキュリティの対策ができていないがゆえに、踏み台になったり、社会全体のセキュリティが下がるということになっていくので、政策的な手を打って、経営者の意識改革、ベースの底上げを行っていく必要がある。
・また、サプライチェーンは非常に重要で、他社ともネットワークがつながっているので、その分野のセキュリティが弱いと、自分たちの仕事にも影響がでてくることになるので、お互いに助けあって行く必要がある。
・橋渡し人材としては CISO 的な人になると思うが、現状では、その CISO を育てる人がいないため、内部で育てるのは難しいのでないか。

以　上