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２回会合　議事概要

１　日時
平成 28 年６月１日（水）　15:00～17:00

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
（外部発表者）	上田　裕子	東京商工会議所　地域振興部　担当部長
	平賀　智	三井住友海上火災株式会社　公務開発部 開発室　課長
（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	情報セキュリティ指導専門官
（オブザーバー）	警察庁	
	金融庁	
	経済産業省	

4 議事概要

（1）セキュリティマインドを持った企業経営に係る発表

資料２－１に沿って八剱指導専門官より発表。

資料２－２に沿って上田部長より発表。

資料２－３に沿って平賀課長より発表。

（2）セキュリティマインドを持った企業経営WG取りまとめ骨子（案）

事務局より資料３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）

・リスク移転の方策として、サイバーリスクに関する保険があるが、サプライチェーンを考えると、大企業と中小企業とでは普及シナリオに差異と課題がある。
・サイバーセキュリティのリスク分析は、日進月歩で進むサイバー攻撃技術の進化を考えると、定期的、継続的に実施していく必要がある。
・中小企業でのサイバーセキュリティの実装ツールは、そこに勤める人々の普段の行動分析も考慮する必要があるのではないか。経営者がリアリティーを持てるものにすることが肝要だ。

（大杉委員）

・日本で経営層が IT やセキュリティのマインドを持ちにくいのには、いくつかの理由が考えられる。１つは、日本では優秀な人材が有名企業に集中してしまい、社会にうまく分散していないこと。もう１つは、企業内のローテーションでジェネラリストを養成し、その中から経営層が生まれる形態が多いため、専門性が高い IT やセキュリティの精通した経営者が現れにくいこと。

（岡村委員）

・もう少し強い表現をしても良いのではないか。１つ目は、サイバー空間は既に実空間と融合しており、ナショナルセキュリティや生命・身体の安全という意味のセキュリティなどとも密接に関係している。このため、国がサイバーセキュリティの確保を促すことは民間企業への余計なお世話ではなく、税金を払うように最低限のことをしないと日本社会がもう持たないという趣旨を発信して欲しい。２つ目は、大企業は IT、ICT が利益の源泉となる経営をしないと、日本経済はこれ以上持たない、というメッセージを強く発信して欲しい。

（落合委員）

・経営層にセキュリティマインドを持ってもらうと云う視点で見ると、サイバー空間では、当たり前に事故が起る「事故前提社会」であることをハッキリとさせた方が良い。また、事故が起ることを前提としても、最低限、取らなければならない対策や責任があることをハッキリと示すべき。

（野口委員）

・【サイバーセキュリティの認識】の項は、もう少しはっきりとした方が良い。例えば、サイバーセキュリティは、利益を生み出し、ビジネスモデルの革新に資するものであると、しっかり書いた方が良い。
・また、社会安全や組織安全の観点では、自分の情報システムが被害者になることを防ぐだけでは不十分。サイバー攻撃の踏み台のように、自分だけではなく、社会に被害を与えることを防ぐという観点が重要。自分だけが被害者では終わらないことを明記した方が良い。

（橋本委員）

・【企業のタイプ別の取組】の項で、企業を３つのタイプに分けてサイバーセキュリティ対策を論じているが、ユーザー視点で自分の企業はどのタイプなのかと考えるときれいに１つに分類できないと思う。むしろ、３つのタイプを観点や視点と捉えて、「うちは２と３に該当する」のように整理した方が良いかもしれない。
・今回の取りまとめがユーザーに使って貰えるようにするには、業態別に踏み込んでセキュリティで必須となるところを述べる必要がある。例えば、「個人情報漏えい」は、金融や証券では、インサイダー情報も同様に大事だし、顧客資産の保全も必須となる。一方で、飛行機・鉄道といった公共交通や、医療分野では、この必須となるものが各々で大きく異なる。業態別に具体化しないと、経営者は実感を持てない。

（丸山委員）

・この報告書の意義の１つは、サイバーセキュリティがビジネスにとって、メリットがあるのか、メリットがないのかの気づきを経営者に与えること。
・２つめは、攻撃の踏み台のように自分のビジネスには影響がなくても、社会には害をまき散らす公害のような状況には、社会として対処する必要があることを経営層に示すこと。
・２つめを考えると、社会に大迷惑がかかるのであれば法規制という方法もあるように思うが、現状でここまでの強いトーンを入れるかどうかは整理の必要がある。

以　上