資料２

高度情報通信ネットワーク社会推進戦略本部情報セキュリティ政策会議
重要インフラ専門委員会
第 33 回会合議事要旨（案）

１　日時　平成 25 年 10 月 4 日（金）14:00～15:45

２　場所　内閣府本府　仮設庁舎講堂

３　出席者

（委員）

浅野　正一郎　委員長　（情報・システム研究機構　国立情報学研究所　教授）
稲垣　隆一　委員　（弁護士）
太田　英雄　委員　（公益社団法人　日本水道協会）
大高　利夫　委員　（神奈川県藤沢市）
大林　厚臣　委員　（慶應義塾大学　教授）
木内　　舞　委員（代理人出席）　（一般財団法人　電力中央研究所）
岸野　広也　委員　（一般社団法人　日本ガス協会）
小出　哲也　委員　（第一生命保険株式会社）
小林　圭治　委員　（一般社団法人　日本民営鉄道協会）
阪上　啓二　委員　（野村ホールディングス株式会社）
佐藤　昌志　委員　（電気事業連合会）
神保　　謙　委員　（慶應義塾大学　准教授）
鈴木　　毅　委員（代理人出席）　（一般社団法人　日本損害保険協会）
関沢　雅士　委員　（株式会社東京証券取引所）
谷合　通宏　委員　（株式会社みずほ銀行）
寺内　利晃　委員　（東日本旅客鉄道株式会社）
長島　雅夫　委員　（日本電信電話株式会社）
西村　敏信　委員　（公益財団法人　金融情報システムセンター）
土生　　尚　委員　（日本放送協会）
早貸　淳子　委員　（一般社団法人　JPCERT コーディネーションセンター）
松崎　吉伸　委員　（株式会社インターネットイニシアティブ）
松田　栄之　委員　（新日本有限責任監査法人）
吉岡　克成　委員　（横浜国立大学　准教授）
渡辺　研司　委員　（名古屋工業大学大学　教授）

（政府）

内閣官房副長官補
内閣審議官
内閣参事官
金融庁　　総務企画局政策課
総務省　　情報流通行政局情報流通振興課情報セキュリティ対策室
総務省　　自治行政局地域情報政策室
厚生労働省　政策統括官付情報政策担当参事官室
厚生労働省　医政局研究開発振興課
厚生労働省　健康局水道課
経済産業省　商務情報政策局情報セキュリティ政策室
国土交通省　総合政策局情報政策課情報危機管理室
国土交通省　総合政策局情報政策課企画室
国土交通省　鉄道局総務課危機管理室

4　議事概要

（1）内閣官房副長官補挨拶

（2）委員長挨拶

（3）議事内容

①議事次第に基づき、以下の議題について事務局より資料に基づき説明。

○討議：次期行動計画の検討状況について（資料 3～資料 4、参考資料 2）

②委員意見開陳

〈討議〉

○資料 3 の P15 のシステムベンダー、セキュリティベンダー、プラットフォームベンダーの位置付け、追加を検討するという所は、様々なベンダー、規模の大小、国内外での活動や情報提供サービスする顧客層に相違があるなど様々な対応をしている。

このため、各ベンダーへの早期警戒情報等の提供を公開する際には、提供する情報の内容によって提供内容が異なることやベンダーによっては情報提供出来ない条件等の留保を付けるといったことが読み取れる表現を残しておく方が良いとの印象を持った。

○資料 3 の P8、9 について。防衛産業は、重要な技術基盤を持っている一方で、中小企業もあり、非常に裾野が広い側面を持つ。国民生活への影響や分野間の波及という観点では(重要インフラ分野等と)繋がっていない面もあるが、これらの中小企業におけるセキュリティ対策も重要であると考えている。重要インフラに入れるというよりも今後、何らかの形で連携を深めていくことを盛り込んで頂きたい。

○資料 3 の骨子案全般で、５項のリスクマネジメントに関し、幾つかの会社の中で経営

者等リスクマネジメントを現実にやっている立場から見ると、骨子案全体として論理的・重要度に応じた体系化を図る必要があるのではないか。

１項から６項までの並びを見ると、ISO27000 の何を為すべきかという各論の並びに沿っているとの印象。課題・今後何をすべきかについて「誰が」ということが一番大事で、この「誰が」という視点をもっと鮮明にすべき。

リスクマネジメントについて、「各事業者が」「国が」という概念の大括りのレベルのものとなっており細分化されていないから、何時になっても前進しない。リスクマネジメントの主体の位置付けをはっきりさせて、「経営管理における」「事業における」というオペレーションまで意識した書き方が望ましい。

全体の構成として、５項は最初に持ってくる。その際に主体の位置付けをはっきりさせる必要がある。

○また、ISO27000 に倣うのではなく、各省庁が事業者に対するもの、例えば金融庁の検査マニュアル等では、情報セキュリティ関係で組織内における主体の責任体制とかオペレーションまでのこと細かに書かれ、非常に実践的である。従前の規範・ルールを配慮、評価した上で、検査マニュアル等を参照しながら、その位置付けを検討してはどうか。

○さらに、金融庁の検査マニュアル改訂版にある経営管理態勢の重要性についての検討を踏まえて頂きたい。

一般的なリスクマネジメントの ISO27000 等を考えると、経営層、経営各層の役割について経営層と一緒くたに書かれているため、現場と情報セキュリティ構築部門との関係・役割が明確にされていない。主体の責任を明確にしておかないといけないので、検査マニュアルの経営管理態勢以下の体系を参考にして欲しい。

○資料 3 リスクマネジメントに関する P22 辺りの所であるが、ISO はあくまで単体組織に対する認証。全体最適とは違うので、(事業者が)リスクマネジメントを最適化して行く際、これを余り前面に出すと、全体最適と個別最適には違いがあるので、参照程度に止めては如何か。

リスクマネジメントというと、ISO31000 が全体のフレームワークとしてあり、その中の「情報システム」として ISO27000 がある。事が起こる前か後かによっても、もし事が起こった後は情報共有等が主となるなら、これはリスクマネジメントというよりも事業継続マネジメントということになる。

単体の組織に対して導入する ISO の枠組みを全体のセキュリティ防護のためにということで ISO27000 を全面的に持ってくるというのはミスリードの可能性がある。

○国際連携の所であるが、欧米の金融分野では、DHS,FSA が連携して演習をしており、Industry の国際連携、レイヤー毎に国際連携し、政府レベル、Industry レベル及び学会

レベルの 3 分野の者、産官学の連携の下行われている。
　ここは、国際連携を進めながらプロフェッショナルを育成し、ネットワークしていくことをイメージした方が良いと思う。

○情報共有体制の強化、安全基準等の整備・浸透、障害体制の所で、主体の書き方として二層構造を設けてはどうか。全て主体は「事業者は」になっている。今の表現は例えば「セキュリティ部担当部門」「担当取締役」というようにある部門等というように限定的に書かれているが、「経営陣」等が主体となる表現、経営者層の責任構造を明確にする記載がない。ここは経営層における一定の情報交換の仕組みなどを構築する努力を促し、経営責任を明確化するためにも「経営陣は」、「代表取締役会は」等の主語を入れて明示できないか。

○委員の指摘については、「経営者」等が主語として記載されて良いように思う。行動計画のどの章に入れるのが良いか。第 6 章に書くと弱いのでは。是非検討願いたい。

○経営者が読んだ時に、会社の責務として「何がうちの会社に必要か？」ということではなく、経営者の責務として「自分が何をやらないといけないのか？」ということを検討すべき。

○この問題は、セブターカウンシル、色々な企業の方がいるのでこの場で企業の方々に議論して貰った方が良い。

（4）その他
○　委員の意見を踏まえ、骨子案は次期行動計画の本文に近い形で次回会合に付議する。
○　次回の会合を 11 月下旬頃に予定する。

（以　上）