重要インフラ専門委員会
第 37 回会合議事

1　日時　平成 26 年 6 月 19 日（木）10:00～12:10

2　場所　中央合同庁舎第４号館　共用 1208 号特別会議室

3　出席者

（委員）

渡辺　研司　委員長　（名古屋工業大学　教授）
有村　浩一　委員　（一般社団法人ＪＰＣＥＲＴコーディネーションセンター）
伊澤　雅和　委員　（一般社団法人日本ケーブルテレビ連盟）
稲垣　隆一　委員　（稲垣隆一法律事務所　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）
金子　　功　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）
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）
鈴木　栄一　委員　（一般社団法人日本損害保険協会）
手塚　　悟　委員　（東京工科大学　教授）
寺内　敏晃　委員　（東日本旅客鉄道株式会社）
中尾　康二　委員　（ＫＤＤＩ株式会社 兼 独立行政法人情報通信研究機構）
長島　雅夫　委員　（日本電信電話株式会社）
中山　広樹　委員　（株式会社三井住友銀行）
西村　敏信　委員（代理人出席）　（公益財団法人金融情報システムセンター）
野口　和彦　委員　（横浜国立大学　教授）
土生　　尚　委員　（日本放送協会）
福留　義之　委員（代理人出席）　（日本通運株式会社）
筆島　　一　委員　（全日本空輸株式会社）
逸見　行男　委員　（石油連盟）
松野　　靖　委員　（石油化学工業協会）
盛合　志帆　委員　（独立行政法人情報通信研究機構）
與口　真三　委員　（一般社団法人日本クレジット協会）

（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企画室
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	航空局安全企画課
国土交通省	鉄道局総務課危機管理室
内閣府	政策統括官（防災担当）付参事官（調査・企画担当）付
警察庁	長官官房参事官(サイバーセキュリティ担当)付
警察庁	警備企画課
警察庁	情報技術解析課
外務省	情報通信課
防衛省	運用企画局情報通信・研究課
防衛省	運用企画局情報通信・研究課　サイバー攻撃対処・情報保証企画室

４　議事概要

（１）内閣官房副長官補挨拶

（２）委員長互選

○参考資料１「重要インフラ専門委員会の設置について」に基づき、委員の互選により渡辺委員を委員長とすることに決した。

○渡部新委員長より挨拶。

（３）報告事項

①次の報告事項について事務局より資料に基づき説明。

○第３次行動計画について（資料２）

②委員からの意見等は次のとおり。

○リスクマネジメントの部分（P10）に関して３点述べる。

１点目は、情報セキュリティのリスクマネジメントと重要インフラのリスクマネジメントの相互の観点からである。重要インフラのリスクマネジメントについての目的は行動計画に記載がありとてもよいが、情報セキュリティにおけるリスク

の重大性の判定をどのように行うのか明確な記載ない。情報セキュリティのリスクを重要インフラのリスクとしてどう位置付けるかの決め方が重要である。別の言い方をすれば、情報セキュリティの在り方をリスクマネジメントの中に位置付け、重要インフラの経営層を引き込まないと、情報セキュリティはうまくいかない。

２点目は、図がリスクアセスメントだけを描いており、リスクへどう対策するか、更に対策の効果をどう見るかというリスク対応の観点が抜けているようにみえる。

３点目は、リスクマネジメントの施策と他の施策との関わりにおいて、他の施策の中で、リスクマネジメントの結果をどう受け取るのか、紐付けを記載できると良い。

○（事務局）１点目について、資料はNISC等における取組みに注視した書き方になっているため、リスクマネジメントの全体像がわかる記載に改めたい。２点目について、その対策等のプロセスがわかる記載を考えたい。３点目について、個々の資料に入れるには細かくなるので、記載振りは検討したい。

○この資料の記載は従来の工学的なリスク手法（ハザード特定）になっている。３．１１以降は原因系からのアプローチではなく結果系からのアプローチが潮流であり、この視点からの取組を進めてほしい。

○重要インフラ防護の目的は、重要インフラサービスの提供による安寧な国民生活の確保であり、これはマネジメント・ガバナンスの目的でもある。これはこれまでの議論・施策の積み上げによるもので、その上で、行動計画は、経営との関係、省庁との関係を含め、目的を情報システムではなく国民の生活に置き、ＣＳＲの観点でまとめられたものとなっている。この行動計画を基に新しい取り組みを進めていくことを期待する。

③報告事項は了承された。

（４）討議事項

①次の討議事項について事務局より資料に基づき説明。

○指針の改訂について（資料３）

②委員からの意見等は次のとおり。

○行動計画においてISO 31000等の最新の考え方を求めることは良いが、リスクマネジメントとは一般的に効果を見るものであって、そもそも情報セキュリティ対策全体を指す概念。リスクマネジメントは目的をどの程度達成できたか又はできていないかというズレを見るものなので、重要インフラに特化する場合は目的を明確にすることが重要である。また、リスクは個々の事業者ごとに異なるため、NISCとして支援する場合には、共通のメソッド・手続きやフレームをガイドすることはできるが、具体的に個々の事業者に踏み込んで示唆することまでは難しいだろう。

○（事務局）リスクマネジメントの位置付けについては、行動計画策定時にも様々

な議論があり現在の形となっている。また、NISC として、個々の事業者のリスクマネジメントに口を出すつもりはなく、またできないと認識している。国全体の対策の底上げのため、対策が進んでいないと思われる中小企業者等をどう支援するかを考え、何が重要かを提示したいという意図である。目的達成の不確かさがリスクであり、それをどのように防ぐことができるかという観点から、指針・対策編において項目を記載し、それをどのように進めるかという観点から、手引書において手順や方法論を記載していきたいと考えている。具体的にどこまで踏み込んで記載するかについては、御意見を踏まえて検討していきたい。

○対策編の項目はこのままの羅列で良いのか。例えば「ポートを閉めろ」と言われても何をすべきかわからない場合もあり、より記載内容を具体化する予定はあるか。

○（事務局）現時点では、対策編はチェックリストであることから、項目は大きく変更する予定はない。対策項目の目的や意味するところは本編の中で記載しており、目的をはき違えることのないようにしたい。

○この場は、重要インフラ事業者等や重要インフラ所管省庁等の、官民の実務者が集まり議論できる唯一の場である。国民に対して提供するサービスレベルをどの程度に設定するのかといった具体的な議論も重要であり、国レベルで共有したい。

○指針・対策編の改訂にあたり時間軸の観点を入れてほしい。調達要件の明確化、開発実施能力の充実、セキュリティ監査の充実など、具体的な業務に落とす際に、各プロセスに対するリスク対策をどのように組み込むのか検討できるようにしてほしい。例えば制御システムにおいて、個別の技術開発は行われているが、システム全体について考え、そこから各機器でどういった対策が必要かという検討が十分でないように思われる。またシステム開発においても、調達段階にまでリスクマネジメントが至っていないように思われる。事業者の現場では既に検討が進んでいるかと思うので、情報共有や議論をしてその結果を指針・対策編に反映することで充実したものになるのではないか。また、昨今、情報セキュリティ対策は、技術面のみならずソーシャルエンジニアリング等の人的側面も求められており、この点についても、事故情報等を集めた反映を検討してはどうか。

○（事務局）各事業者でどこまで取組が進んでいるかについては、安全基準等の浸透状況調査などにおいて把握し、必要な検討を行っていきたい。また、本編のポリシーレベルとして、御意見を踏まえた内容を検討していきたい。

○施策として、個社がそれぞれ対策を進める今のアプローチは必要と考える一方、業界横断的なものがあっても良いのではないか。また、施策の効果測定は重要であり、有効性の効果測定のフレームワークを強化してほしい。

○（事務局）行動計画においてセプターカウンシル等の各主体に期待する内容は記載しており、具体的な運用については、御意見を踏まえたものとなるよう心がけたい。また、効果測定については、PKI が全て設定できるわけではないが、どこま

でできたかという点を意識しながら、各施策で報告を行い改善すべき点を取り入れていきたい。

○各分野がそれぞれ努力をしているかと思うが、各々どのくらいのレベルなのか。この場での官民全体の PDCA と各社での PDCA とが連結し、情報セキュリティ対策の底上げができればよい。

○（事務局）安全基準等の浸透状況調査や情報共有での情報連絡件数などにより、分野ごとのばらつきがあることは理解した上で第３次行動計画を策定しており、比較的対策が遅れている事業者等を見据え、どこまで浸透したかを確認していきたい。

（５）その他

①議事内容全般について各委員からの発言は次のとおり。

○情報共有や分野横断的演習など、各施策の実行の部分を通じて今後とも協力していきたい。

○分野内の事業者の規模は大小あり、セプター参加への条件としている情報セキュリティポリシーの策定が行われていない者もいる。対策レベルの高い事業者は伸ばしながら、低いレベルの事業者を底上げしていきたい。

○実際に手を動かす事業者の職員の取組みが重要。セキュリティは技術的に捉えるだけでなく、国民がより安寧で幸せになるということが重要だと考えている。

○重要インフラサービスの提供にはローテクな部分が多いが、電気などが止まるとサービスも止まってしまう。こうした場で各分野との連携を深めながら、小規模な事業者までサービス継続が行えるよう努めていきたい。

○経営層の関与とともに、自分野が重要インフラであることの周知にも取り組んでいきたい。

○大切な視点としてユーザーの影響がある。変化が大きい分野なのでその点も取り入れてほしい。また、国を超えた広がりも検討する必要がある。

○サービスの安定提供が最優先の経営課題である。引き続き他の分野等と連携していきたい。

○分野内の担当者の集まりで、第３次行動計画、特に行動計画の２章（P11,12）を精読するように指示し、活用させて頂いている。分野内の底上げを図るに当たり、指針の改訂に期待している。

○第３次行動計画に、経営層に求めるものを骨子で記載いただいたため、経営層への説明においてわかりやすい資料として活用できた。先進的な分野に比べ対策が遅れがちだが分野全体の底上げを図りたい。

○今後数年で様々な環境変化が想定され、これを見据えて情報セキュリティの確保を検討する必要がある。分野内ガイドラインの見直しも検討しており、指針改訂と整合をとっていきたい。なお、分野間での情報共有については、良いことではあるが、実際には出しにくい部分もある。

○分野内でも事業者の規模は様々であり、底上げの取組に当たり、中小規模事業者を対象とする手引書に期待している。計画はできても、実行する方法がわからないところもあるので、そこに目をつけていただき、期待している。
○分野横断的なアクションの際は、総論で議論が進んだとしても各論で止まってしまうのは常であるが、こうした場で知恵を出し合って乗り越えていきたい。また、国民に対して透明性を持たせ、安心感を与えるという意味でもこの場を活用していきたい。今回の行動計画では、目的として、サービスの持続的な提供という実現可能なものを設定しており、具体的な議論にすぐに入れる。是非各論でも具体的な成果が上がるよう議論していきたい。
○今後とも、所管省庁や分野内の事業者や業界団体とも連携しつつ、自社内での情報セキュリティレベルの向上に努めていきたい。
○海外では、多層防御やスマートメーター、制御システムについても具体的な検討が進んでいる。この場でも、マネジメントフレームワークだけでなく、重要インフラに特化した対策を進化させるような切り口もあってよいのではないか。
○指針の改訂は PDCA ベースでわかりやすくなると期待しているが、その際、ISO27000 等の国際標準等との整合を考慮してほしい。また、脆弱性報告から攻撃開始までの間隔が短くなっており、情報共有のスピード向上についてもその仕掛けを考えてほしい。
○分野内では事業者数も多くレベルも様々である。実事案も発生し、その対策に注力しているが、指針改訂ではこうした点でも貢献していきたい。
○分野内で安全対策基準の見直しを進めてきた。今後とも議論を参考に取組んでいきたい。
○事業を個々の要素に分解して最適化する手法に限界を感じているが、全体最適論は建前だけでなくどこに具体性を盛り込むかが重要である。情報セキュリティを担当者の問題ととらえず、事業者・分野全体をどのように守るかという視点が大切。指針改訂の際にも、情報セキュリティ対策の重要性からではなく、その位置付けから記載してほしい。
○重要インフラ防護は、ユーザーから見えるサービスそのものだけでなく、各種業務システムまで含めてみないと、ユーザーからの信頼の喪失などにつながってしまう。逆にこうした業務システムへの対策を適切に行うことで、ひいては重要インフラサービスの持続的な提供にもつながっていく。今後とも、業界団体とも連携しながら協力していきたい。
○分野内で情報共有について改善すべき点もある。セプター事務局とも連携しながら進めて行きたい。
○分野内では情報システムへの依存度が高く、海外との接点もある。今後とも、所管省庁や業界団体と連携を取りながら取組を進めていきたい。
○サービスの持続的提供が重要な責務であり、そのためにも情報セキュリティの確

保は大事。分野間・分野内での連携を図っていきたい。

〇情報セキュリティの確保は重要であり、引き続きよろしくお願いしたい。

〇CSIRT やセキュリティバイデザイン等に携わってきた経験を活かし、必要な協力を行っていきたい。

〇分野内では、国際的な安全基準等があるが範囲が限られており、他分野の取組みも参考に対策を検討したい。

②次のとおり事務連絡の後、閉会。

〇追加での意見等あれば６月中に事務局宛提出。

〇指針の改訂については、討議事項を踏まえ、次回会合で草案を提示する予定。

〇次回会合の開催予定は９月下旬以降とし、詳細については別途事務局から連絡。

（以　上）