重要インフラ専門委員会
第 39 回会合議事

1　日時　平成 26 年 12 月 18 日（木）15:00～17:00

2　場所　中央合同庁舎第４号館　共用第 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）
安部　俊史　委員　（日本通運株式会社）
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（代理人出席）　（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（代理人出席）　（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）
菊池　篤郎　委員　（明治安田生命保険相互会社）
阪上　啓二　委員　（野村ホールディングス株式会社）
鈴木　栄一　委員　（一般社団法人日本損害保険協会）
高橋　泰宏　委員　（石油連盟）
竹原　　達　委員　（電気事業連合会）
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　（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）
筆島　　一　委員　（全日本空輸株式会社）
細川　　猛　委員　（石油化学工業協会）
松田　栄之　委員　（ＮＴＴデータ先端技術株式会社）
盛合　志帆　委員　（独立行政法人情報通信研究機構）
矢野　一博　委員　（日本医師会総合政策研究機構）
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	自治行政局地域政策課地域情報政策室
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医療技術情報推進室
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
警察庁	長官官房総務課
警察庁	警備局警備企画課
警察庁	情報通信局情報技術解析課
外務省	大臣官房情報通信課
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）委員長挨拶

（３）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。

〇指針の改訂について（資料２～資料５）

②委員からの意見等は次のとおり。

〇指針が改訂されれば、安全基準等作成のガイドラインを分野内でも改訂していくとともに、分野内の中小事業者に対して、手引書を参考として活用していきたい。

〇対策編の P9 に「ＩＴ障害発生時の体制の整備」として、「ＩＴ障害時の所管省庁への連絡体制」あるが、所管省庁のみならず、重要インフラ事業者等同士の連絡体制等も必要ではないか。

〇対策編の P11 に「外部委託における対策」とあるが、実際には再委託も頻繁に行われており、「再委託の制限」という記載に加え、委託先への注意喚起等について具体的に記載できないか。

〇分野内で事業者の規模が様々であり、今回の手引書等を通じて意識の向上が図られるため歓迎する。PDCA についても、小規模な事業者は、一度作ったらなかなか見直さない傾向があるので、その点についても記載されており参考にしていきたい。

〇サイバーセキュリティ基本法が施行されるタイミングで、経営層に期待する在り方や具体的な取組を含む指針・手引書ができることは評価したい。

〇内部権限者による機密情報の故意の漏えいについては、セキュリティ人材の育成というより、情報を守るためにふさわしい人をいかに配置してどう評価するかという問題である。データを管理する者の責任として、対策編の P19 に「適切な作業環境の整備」や「適切な労働政策の策定」といった旨の追記ができないか。[※１]

〇分野内でも事業者の管理レベルは多様だが、指針等が改訂されれば、特に提供サービスの安全が侵されるような事故の防止に向けて、必要な対策を行いたい。

〇情報の作成・入手から消去までの情報のライフサイクルにおいての安全対策が求められ

ており、今回の指針は非常に役に立つと期待している。ただ、第３次行動計画を含めて、内容を各分野に噛み砕いて伝えられる人材の育成も必要である。

○経営者の中には、どのくらいの人が真剣に取組んでいるかということで、事の重大さを感じるタイプもいるので、分野横断的演習等の機会も活用してアピールすることも有効である。

○指針の改訂は、セキュリティ対策に新たに取り組んだり、既存の社内規程を見直したりする観点で、優先順位付けの考え方が示されており、大変参考になる。また、手引書の最初の章に「経営層のあり方」が追加され、社内での取組が円滑に進む工夫が盛り込まれており非常にありがたい。事業者が所管省庁へ報告を行うレベルについても、各分野の特徴を踏まえた上で記載されるとよい。

○次のステップかもしれないが、システムはベンダー頼りになってしまう状況を踏まえ、より強固な体制化の観点から、社外の専門機関への出向等といった、外部ノウハウの吸収を経営層に積極的に訴求できないか。

○手引書でモニタリングが充実した記載となっており、作り上げた後の運用は、なかなか経営者の目が行かない場合があるので、意識させるためにはありがたい。

○安全基準等の策定においてこの指針等を大いに活用していきたい。

○指針の改訂内容については、政府からの重要インフラ事業者等への要求事項と捉え、業界内で活用していきたい。

○セキュリティはコストが必要だという認識が少しずつ理解され始めている環境にあり、今回の指針改訂を活用していきたい。

○指針の P9 で、Plan の項に Check・Act からの継続を前提とした記載に違和感がある。[※２]

○手引書の P5 の図表や P28 で、モニタリングとある部分にはレビューも入るのではないか。また、図表の矢印が状況の設定に戻るのではなく各項目に戻っているのは特定の考えがあってのものなのか。[※３]

○手引書の P7 の図表で、優先順位付けをするのは良いが、リスクを特定していない状況でリスク評価をすることになってしまっていないか。[※４]

○指針の P12 について、平時の状況やしきい値と異なることを指して「予兆の把握」としているが、それほど単純なものではないので記載を見直した方がよい。

○指針は、PDCA で整理されて非常にわかりやすくなった。IT-BCP についてはＩＴ特有的なことだけではなく、2020 に向け、パンデミックや自然災害等も考慮が必要。また、PDCA も 2020 に向け何度回せるかも大きな課題になってくるのではないか。

○指針の改訂は中小事業者の底上げに資するもの。また、リスクマネジメントの中で事案の対策を考える際、事案情報の共有が大事である。

○改訂指針等を参考にして、基準の改訂を行っているところ。いったん基準を作っても、新たな攻撃を受けるため、情報共有や基準の反映をいかにタイムリーに行うかという仕組み作りも重要である。

○情報通信システムを守ることが特別な行為ではなく、社会や組織の中におけるマネジメントの一つとして位置付けられることが重要である。その点で、情報セキュリティ対策とリスクマネジメントの整合性が図られているのは良いが、担当者の業務視点での対応だけでなく経営層が当たり前に関与していくことを明記できないか。

○規程の整備において、モニタリングの必要性を感じていたところ、今回盛り込まれており、生きたものになるのではないか。
○改訂指針は事業者の特徴に応じたドライブをかけた上で推進していきたい。
○事業者等の規模は様々であるので、中小規模でも使えるものとなってありがたい。
○指針対策編の P25 で、ログに係る対策項目の「取得、確認、保管」のうち「確認」については、ログを取得すること自体を確認するのではなく、ログの内容を確認することであるということを明示できないか。
○指針の P3 で、「レビューや検証等のモニタリングを組み込む」という表現が、手引書の用語定義に照らすと違和感がある。
○対策編の P30 で、「電子政府推奨暗号リスト」は、解読のリスクが高い暗号である運用監視暗号リストにも注目して欲しいため、「CRYPTREC 暗号リスト」に修正してほしい。
○分野内での安全基準等を中小事業者にも広げていく必要があり、その際に、この指針等は活用できる。

③事務局からの回答等は次のとおり。
○（事務局）[※１]については、対策編の P19 は「構築の視点」の項目で技術的・システム的な記述の部分であり、御指摘の点は P9 の「体制の観点」で記載しているところだが、その中で修正すべき点があれば検討したい。
○故意の情報漏えいへの対策として、人材の確保ではなく、経営層の仕事である労働政策、職員・リソースの配置が重要であるということを入れたいという趣旨。
○（事務局）全体の並びや読みやすさも含めて検討したい。他委員から頂戴した御指摘についても、全体構成を見た上で検討したいが、具体的な修文案があればお願いしたい。
○（事務局）[※２]については、現に事業をやっている者が指針等を読むと考えており、既に何らかの取組があった上で、途中から始める想定で記載している。
○（事務局）[※３]の矢印については、中小事業者等も含めて、できるところから段階的に実施するという趣旨があり、途中でフィードバックをかける等の柔軟な対応がとれるようにしたもの。[※４]の御指摘についても、中小事業者等に理解しやすいように端的に記載したものだが、違和感があるようであれば見直していきたい。
○手引書の P5 の図表でモニタリングの結果を各ステップに戻すのは、状況の設定まで戻らなくても他のステップに問題があることもあり、これでよいと思う。ただ、各ステップのモニタリングをすることもリスクマネジメントとして必要ではないか。
○手引書の P7 は、リスクを特定しないままリスク評価をするのはわかりにくいので、特に必要なものだけでもリスク特定をする表現としておけばよいのではないか。
○手引書の P5 の図表は、独自の考えがあるなら、きちんとモニタリングの章に記載する必要がある。
○そのモニタリングやレビューについて、人によって受け止め方に違いがあると思われるため、現状に適した日本語で再定義することで、取組も定着していくのではないか。
○指針対策編の P11 で、再委託については「再委託の制限」とだけ記載されているが、ＩＴサービスは多様な関係者が関わっており、具体的にどのような配慮をすればよいのか非常に悩んでいる。具体的に明記できればありがたい。

④欠席委員には会議資料送付の上、追加意見があれば、12 月 24 日までに事務局宛提出の旨を事務連絡。

⑤委員長から、パブリックコメント案については委員長一任の提案があり了承。

⑥パブリックコメントの方法について、資料３の指針本編のみがパブリックコメントの対象とすると、内容が概要的でコメントしにくいのではないかとの質問があり、これに対して事務局から、対象は指針本編のみだが、指針対策編及び手引書も参考資料として添付する予定である旨を回答。

（４）その他

①事務局より参考資料２について説明。

②次のとおり事務連絡の後、閉会。

〇パブリックコメントについては、１月から２月頃までを目処として予定。

〇サイバーセキュリティ戦略本部の設置を１月９日に予定しており、これに伴い情報セキュリティ政策会議重要インフラ専門委員会としては、本回が最終会合となる予定。

〇サイバーセキュリティ戦略本部下での重要インフラ防護に関する活動については、年度内に初回会合の開催を予定。任命手続等を含めて詳細は別途連絡。

（以　上）