「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定指針（第４版）(案)」に対する意見募集の結果の概要

資料４－２

■ **実施方法：** NISCのWebページ及び電子政府の総合窓口（e-gov）に掲載して公募

■ **実施期間：** 平成27年２月３日（火）～２月24日（火）

■ **提出意見：** ７者から10件

内訳　７者（個人２、企業･団体４、無記名１）
10件（個人２、企業･団体７、無記名１）

※その他、参考意見１件

■ **意見に対する考え方：**

- 指針本編の修正を要するもの　３件
- 第３次行動計画の考え方を改めて御説明するもの　３件
- 今後の施策の参考とさせていただくもの　４件

■ **その他：**

- 指針本編について、サイバーセキュリティ基本法の施行及び第３次行動計画の改訂に伴う修正のほか、誤植等を修正（指針対策編･指針手引書についても併せて修正）
- 指針手引書について、仮称であった名称を変更
- 指針本編については、重要インフラ専門調査会での審議を経て、サイバーセキュリティ戦略本部にて決定
- 指針対策編･指針手引書については、重要インフラ専門調査会にて決定（決定日は指針本編の決定日）

「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定指針（第4版）（案）」に関する意見の募集の結果について

意見募集期間：平成27年2月3日(火)から同年2月24日(火)まで

別紙

通番	提出者	枝番	該当箇所（該当ページ）	概要	御意見に対する考え方
1	一般社団法人全国銀行協会	1	Ⅱ.「安全基準等」で規定が望まれる項目 6. 対策項目 6.1「Plan(準備)」の観点 6.1.2「規定」の観点 (2)IT-BCP等の策定・見直し (p9(意見募集時p10))	＜意見＞ 「事業継続に必要なデータが東京に一極集中している状況等についても考慮する」を「事業継続に必要なデータが地域的に集中している状況等についても考慮する」等に修正いただきたい。 ＜理由＞ 事業継続に必要なデータが東京以外の都市に集中している場合も考慮する必要があるため。	御意見の趣旨を踏まえ、修正いたします。
2	株式会社アズム	1	Ⅱ.「安全基準等」で規定が望まれる項目 6. 対策項目 6.1「Plan(準備)」の観点 6.1.2「規定」の観点 (3)情報の取扱いについての規定化 (p9(意見募集時p10))	重要インフラの情報セキュリティ対策拝見させていただきました。重要インフラの継続性に関して大変共感を覚え賛同いたすところであります。 一方で昨今の情報漏洩などの見地からデータの保護という観点からのセキュリティに関していくつか気になる点がありますのでコメント差し上げます。 “6.1「Plan(準備)」の観点の 6.1.2「規定」の観点 (3)情報の取扱いについての規定化” について「取り扱う情報の重要度に応じて、機密性、完全性、可用性の観点から情報の格付け(ランク付け)を行うとともに、作成、入手、利用、保存、移送、提供、消去等と いった情報のライフサイクルの各段階における遵守事項、情報セキュリティ対策を規定する。」とあります。また「なお、個人データについては、国民の安心感への影響に鑑みた取扱いを規定する。」とありますが、上記の表記にある機密性は注書き10を参照するといわゆるアクセス制限について言及されていると思われ、何らかの事象があり漏洩しても影響を及ばさないとの観点で「データの秘匿性」等を追加すべきと考えます。	御意見の趣旨を踏まえ、機密性に関する注意書きにおいて、秘匿性の確保の観点が含まれることを明記します。
3	株式会社アズム	2	Ⅱ.「安全基準等」で規定が望まれる項目 6. 対策項目 6.1「Plan(準備)」の観点 6.1.5「構築」の観点 (1)情報セキュリティ要件の明確化・変更 (p10(意見募集時p11))	“6.1「Plan(準備)」の観点の 6.1.5「構築」の観点 (1) 情報セキュリティ要件の明確化・変更” では「重要インフラ事業者等が有する情報システムへの情報セキュリティ対策の実装に向け、機密性、完全性、可用性等の観点から、導入を要する情報セキュリティ機能を明示する。」とありますがこちらも上記同様に秘匿性等を追加すべきと考えます。 様々な災害やサイバー攻撃にあったとしても、漏洩されたデータが例えば暗号化で保護されていれば悪用されたりすることもなく「国民の安心感」につながります。また昨今の情報セキュリティのレポートによる内部犯行の増加を考えた場合にも、盗んでも利用できないという秘匿性があればそもそも盗難などの抑止になり、Plan(予防・抑止)にも沿っていると考えます。 さらに詳細なガイドラインには暗号化など具体的な解決策が記載されることを希望しますが、重要なことはまずは情報単体でも保護すべきであり、それを秘匿性という言葉を盛り込むことによってデータそのものの保護をメッセージとして追加していただけますよう強く推奨させていただきます。	

通番	提出者	枝番	該当箇所 （該当ページ）	概要	御意見に対する考え方
4	個人	1	Ⅰ．目的及び位置付け 2.「安全基準等」の必要性 （p1～2(意見募集時p2～3)）	特に重要なこととして「重要インフラ事業者等が自らの状況を正しく認識し、自らの情報セキュリティ対策の水準を規範等に照らした上で、PDCAサイクルに沿って適切かつ定期的に自らの情報セキュリティ対策を実施・改善すること」と記載されています。 理想論としてはその通りかもしれません。 しかし現実問題として、重要インフラ事業者が当該インフラの構築や保守等を外注先に、いわゆる「丸投げ」している場合、上記のことを実効的に実施する能力を持っているのは事業者ではなくアウトソーシーのほうです。その場合、本来の姿としては、重要インフラ事業者がアウトソーシーの協力を得て一連の「正しく認識、実施・改善」に取り組むのが、あるべき姿かもしれませんが、それを正しく行うには、当然ながらアウトソーシーに費用を支払う必要が生じます。 重要インフラ事業者も企業であり、コスト削減が求められるという事情に鑑みると、アウトソーシーに費用を支払ってまで真正面から「正しく認識、実施・改善」に取り組むよりも、実効性はさておいて、書類上の辻褄を合わせる程度の取り組みを重要インフラ事業者の内部で行うに留めるほうが合理的ということになります。すなわち形骸化であり、そうなったのでは意味がありません。 もちろん、すべての重要インフラ事業者が「丸投げ」しているわけではないでしょうが、「丸投げ」していなければ重要インフラ事業者自身、「丸投げ」しているのであればアウトソーシーというように、関係者のうち少なくとも誰かが確実に一連の「正しく認識、実施・改善」を責任をもって行うという仕組みを確立することが必要で、これが実現しない限り、どれほど優れた安全基準も指針も、残念ながら、形骸化を免れないと思います。	「正しく認識、実施・改善」を責任をもって行うという仕組みを確立することが必要であるとの御意見については御認識のとおりです。 本件指針案の上位に位置付けられる「重要インフラの情報セキュリティ対策に係る第3次行動計画」（平成26年5月19日情報セキュリティ政策会議決定。以下「第3次行動計画」という。）において、「情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施するものである。」とされており、この考えの下で、業務の一部を外部委託することは妨げられるものではありません。 なお、その際の外部委託における対策は本件指針案のⅡ.6.1.4(3)に記載したとおりです。
5	日本ユニシス株式会社	2	Ⅱ．「安全基準等」で規定が望まれる項目 3.「安全基準等」において対象とする原因 （p6～7(意見募集時p7～8)）	＜意見＞ 安全基準等の対象とする原因に比較的軽微な物理的テロを追加していただきたい。 ＜理由＞ P7の「意図的な原因」にはサイバーテロが含まれていると思いますが、安全保障上の観点から物理テロを含む攻撃を想定した情報セキュリティ対策も追加すべきと考えます。 例えば、データセンターに対し郵便による炭疽菌の送付や爆発物（火炎瓶等）持参による突入などの物理的テロは比較的簡単に実行が可能と思われます。 一般企業にはこれら対策への知見があまりないので、安全基準にはこれら軽微な物理的テロも対象として記載すべきと考えます。	対象とする原因については、重要インフラサービスの安定的供給や事業継続等への影響がないように、顕在化する可能性が高いIT障害を想定した上で、そのIT障害の原因を各重要インフラ分野及び各重要インフラ事業者等の特性等を可能な限り具体的に考慮し、「安全基準等」に規定されることを期待しております。 また、例示する原因については、本件指針案の上位に位置付けられる第3次行動計画の別紙3において記載する「情報連絡における事象と原因の類型」に基づいております。 なお、その具体的な対策については、参考資料として添付した「重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定指針（第4版）対策編(案)」に「〇情報システム施設における安全区画の確保」、「〇情報システム施設に係る入退出管理（物理的な不正侵入の防止）」等を記載することとしています。
6	無記名	1	指定なし （指定なし）	「重要インフラ」が13分野として定義されているが　そもそもこのようなカテゴリで規定することに意味があるのか。そもそも　ここで記されていることは　「重要インフラ」に限らず　すべての情報システムにあてはまる内容である。 策定指針とあるので　今後具体化されるものと考えるが書かれていることも　あまりに抽象的である。 利用者からみて　もっとも重要な個人情報の保護という観点が抜けている。 あいまいな定義で　あいまいに運用される恐れがある。 対象や対策をより具体的に規定すべきである。	「重要インフラ」については本件指針案の上位に位置付けられる第3次行動計画において規定されており、これに基づいて本件指針案を策定しております。 なお、第3次行動計画において、指針は「安全基準等の策定・改訂に資することを目的として、情報セキュリティ対策において、必要度が高いと考えられる項目及び先進的な取組として参考とすることが望ましい項目を、横断的に重要インフラ分野を俯瞰して収録したもの。」とされています。 また、個人情報については、本件指針案のⅡ.6.1.2(3)に規定しています。

通番	提出者	枝番	該当箇所 （該当ページ）	概要	御意見に対する考え方
7	日本ユニシス株式会社	1	Ⅰ．目的及び位置付け 3.「安全基準等」とは何か （p2(意見募集時p3)）	＜意見＞ 全体を通じてであるが、安全基準等の構成としては、業界をまたがる共通部分を定めたもの（省庁横串の基準）を1つ策定し、そこから逸脱する業界固有のものを各省庁、業界団体が逸脱部分のみを個別に策定するというスキームにしていただきたい。 ＜理由＞ 業法に基づき国が定める「強制基準」、「推奨基準」、「ガイドライン」というように、「業法に基づき」という基準策定の方針は理解できるが、今やビッグデータの時代においては業界をまたがるサービスが種々存在する。 セキュリティ対策を行う企業にとって各省庁毎に作成された基準やガイドラインを全て熟知することは大変な負担である。例えば、個人情報の保護に関するガイドラインは各省庁において27分野39個ものガイドラインが策定されており、それらには共通的な部分が多くある。 共通部分と業界個別部分とを切り離して基準を策定すれば、対策を実施する企業にとっては業界ごとの特性を理解しやすくなり、また基準を策定する側にとっても個別部分のみを検討すればよいので、双方にとって相当な労力削減につながるものと考えます。	本件指針案のI.4において、指針の活用による「安全基準等」の策定・改定に際しての留意点として以下の2点を記載しております。 ○重要インフラ分野又は重要インフラ事業者等によっては、その事業の態様等の理由から指針の記載項目の中に規定する必要がないものを含むことがあり得ること ○重要インフラ分野又は重要インフラ事業者等によっては、その事業の態様等の理由から指針に未記載の項目であっても規定する必要がある場合があり得ること このことに沿って、各重要インフラ分野が「強制基準」、「推奨基準」、「ガイドライン」を定め、各重要インフラ事業者が属する分野の「強制基準」等に基づき「内規」を定められることを期待しております。 御意見については、本件指針案の内容に対するものではないものの、今後の施策の参考とさせていただきます。
8	マカフィー株式会社	1	Ⅰ．目的及び位置付け 3.「安全基準等」とは何か （p2(意見募集時p3)）	ここにあげられている「強制基準」と「ガイドライン」についてだが、重要インフラ事業者に、体制も含めた積極的取組みを促すためにも、最低レベルのセキュリティを確保する「強制基準」とセキュリティレベルを十分なレベルに向上させるための「ガイドライン」を用意することが望ましい。 単に、「ガイドライン」のみの施行では、他の分野でのガイドラインと比べ有効性に乏しいと考える。 その大きな理由として、特に重要インフラ事業者においては、保護すべき部分が、通常の情報システムだけではなく、可用性の高いオペレーションシステム（制御系）を含む場合が多く、通常、事業者内でもこれらのシステムは、異なる部署に属し、関わる人々も異なる文化を持っている。 これらを統合的に保護するためには、事業者内でのトップダウンによる積極的な取り組みが不可欠であるが、ガイドラインでは、社内的なコストの理由を確保するのが難しくなると予想されるためである。 また、「強制基準」にとどまらず、「ガイドライン」を用意する理由としては、強制性を持たせる基準だけでは、あいまいさを排除するために、チェックリスト的なものにならざるをえず、また、あまりきつく縛ると、基準の更新に時間がかかるがゆえに、最新の脅威に適応できない場合が生じると考えられるためである。 したがって、強制性はないが、リスクベースのアプローチに基づいて、重要インフラ資産を守るための手段を提供することで、「強制基準」で最低限レベルのセキュリティを確保しつつ、「ガイドライン」で最新の脅威及び各事業者のリスクに応じたセキュリティを確保するといった取り組みが可能となるようにすべきである。	
9	マカフィー株式会社	2	Ⅰ．目的及び位置付け 4. 指針の位置付け （p2～4(意見募集時p3～5)）	P5の図中にある「情報共有体制の強化」については、重要インフラ事業者をターゲットにした標的型攻撃の存在を考えた場合、単に同一業界内でのインシデントやベストプラクティスの情報共有にとどまらず、インシデントを解析し、その結果をセキュリティ製品で検知するための脅威情報として配信すべきである。 既に、セキュリティベンダーをまたいで脅威情報を共有する仕組みがグローバルで存在している。（IOC、STIXなど） 攻撃者サイドでは、同一業種を狙うツールが即座に流通するなど、密な連携が行われているなかで、守る側が、セキュリティベンダーをまたいだ脅威情報を、業界単位で共有することは有効な対策だと考えられる。	本件指針案は重要インフラ事業者等が適切かつ定期的に情報セキュリティ対策を実施・改善するために必要となる「安全基準等」の策定に資することを目的に策定しております。 このことから、重要インフラ分野そのものや同分野間における取組については記載を控えており、頂戴した御意見については、今後の施策の参考とさせていただきます。
10	個人	1	指定なし （指定なし）	PDCAのサイクルが業界内で回るよう、重要インフラを担う各業界毎に、ノウハウの蓄積と共有がはかられるような場を設けてはどうか。	意見募集の対象外の御意見であり、今後の施策の参考とさせていただきます。 なお、本件指針案は、重要インフラ事業者等が適切かつ定期的に情報セキュリティ対策を実施・改善するために必要となる「安全基準等」の策定に資することを目的に策定しているものです。

その他1件の参考意見の提出あり。