「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』策定のための指針（案）」に関する意見の募集

意見提出フォーマット

内閣官房情報セキュリティセンター（重要インフラ対策担当）あて

Ｈ１８．１．１３

| | | | |
|---|---|---|---|
| 所　属 | 社団法人<br>情報サービス産業協会 | （ふりがな）<br>氏　名（※） | 棚橋　康郎（たなはしやすろう） |
| （ふりがな）<br>住　所（※） | 135-8073<br>東京都江東区青海2-45 タイム24 ビル17 階 | | |
| 連絡先 | （ふりがな）<br>連絡担当者氏名：調査企画部　鈴木律郎（すずきりつお）<br>電話：03-5500-2610<br>FAX：03-5500-2630<br>e-mail：rsuzuki@jisa.or.jp | | |

※ 法人又は団体の場合は、名称、代表者の氏名及び主たる事務所の所在地を御記入ください。

（注）上記の住所・連絡先は手続き上必要な連絡のためにのみ使用します。

| | |
|---|---|
| 該当箇所 | Ｐ3　Ⅱ－1　「安全基準等」の対象範囲及び対象とする脅威 |
| 意見内容 | 対象とする脅威として、（1）サイバー攻撃によるIT障害、（2）非意図要因によるIT障害、（3）災害によるIT障害の3点が記載されているが、対象とする脅威として、「意図的要因によるIT障害（内部犯罪）」を追記すべきである。 |
| 理　由 | 職員等の内部関係者の性善説だけでは、情報セキュリティ事故、事件を防ぐことはできない。すでに国内の情報漏えい事故で、内部関係者による意図的な犯罪が発生している。この指針案のＰ７　Ⅱ－３－（４）－②－イ－（エ）でも、意図的犯罪を意識した対策として「内部関係者による情報漏えいを抑止するための措置、・・・」が記載されている。 |

| | |
|---|---|
| 該当箇所 | Ｐ４ＩＩ－１－（２） 非意図的要因によるIT障害 |
| 意見内容 | 例として「プログラム上の欠陥（バグ）、操作ミス」などが例示されているが、「仕様上の問題、想定外のトランザクションの集中」、といった項目も例示すべきである。 |
| 理　由 | これまでの非意図的要因によるIT障害発生の原因として代表的なものは列挙すべきである。特に、情報システムにおいては、上記2つは大きな要因である。 |

| | |
|---|---|
| 該当箇所 | Ｐ５　ＩＩ－３－（４） 対策項目 |
| 意見内容 | 「4つの柱と3つの重点項目を盛り込むことが望ましい」とあるが、この中に「監査」という項目を追記すべきである。 |
| 理　由 | 監査については、Ｐ１０　ＩＩＩ－（２）－①で「安全基準等に明示することを検討する」とだけ記載されているが、本記載のみでは不十分であると考えられる。安全基準に監査を盛り込むことにより、ＰＤＣＡサイクル（Ｐ５　ＩＩ－３－（４）－①－ア）を機能させることを明確にすべきである。重要インフラの事業特性を鑑みても、監査についての指針を先延ばしにはできないと考える。 |

| | |
|---|---|
| 該当箇所 | Ｐ6　Ⅱ－3－(4)－①－ウ　情報セキュリティ要件の明確化に基づく対策 |
| 意見内容 | 本要件の中に「リスク分析」または「リスク評価」の重要性について追記すべきである。 |
| 理　由 | ＩＳＭＳでも定められている通り、情報セキュリティ要件を明確化するためには、「リスク分析」「リスク評価」が大変重要であり、本指針にそれらの重要なキーワードが漏れていることは、ミニマムスタンダードとして考えても不十分であると考えられる。 |

| | |
|---|---|
| 該当箇所 | Ｐ8　Ⅱ－3－(4)－②－ウ　外部委託における情報セキュリティ確保のための対策 |
| 意見内容 | 「委託先と連携した情報セキュリティレベルの向上が必須」とあるが、外部委託先にＩＳＭＳやＰマーク取得を一方的に強制させるだけではなく、外部委託先への支援等も含めた「連携」が重要であることを明記すべきである。 |
| 理　由 | 受託を受ける側が自主努力によってセキュリティレベルを向上させる必要があるのは言うまでもないが、発注者－受注者という取引関係上、必要以上の認定取得を発注条件に盛り込まれるケースも見受けられる。<br>指針でも述べている通り、発注者と受注者のパートナーシップが重要であり、外部委託先のセキュリティレベル向上のためには、発注者である重要インフラ事業者側の支援、インセンティブの付与なども検討すべきケースがあることを認識すべきである。 |