「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』策定にあたっての指針(案)」への提出意見に対する考え方

番号	該当箇所	ご意見の概要	ご意見に対する考え方
1	Ⅱ 2. 「安全基準の公開」 (P.4)	「この際、公開することにより脅威の増大等が想定される項目等については、当該項目が非公開であることを明示するとともに、何故公開すべきでないのかを明記することが望ましい」という記述を削除されるよう求めます。	ご指摘の点については、本文にお示ししたとおり、重要インフラの国民生活への影響や社会的責任の大きさ等に鑑みれば、国民に対し安全・安心に取り組む姿勢を表明する観点から、「安全基準等」に示された対策項目の内容が可能な限り公開されることは望ましいと考えます。 しかしながら、分野によっては対策項目の内容を公開することにより、ご指摘いただいたような脅威の増大につながる場合も考えられることから、そのような場合には、脅威の増大につながらないよう、理由を付した上で、非公開項目として明示することにより、具体的な対策内容を示さず対策実施の有無のみを明らかにすることとしているものです。 また、特定の対策項目の内容を非公開とする場合には、当該対策項目の明示の仕方や非公開とする理由の提示の方法を工夫することによって、脅威の増大を回避することは十分可能であると考えます。 なお、「公開」「非公開」の判断基準は各重要インフラ分野の特性に応じ、決められるべきものであり、一律の設定は困難であると考えます。
2－1	Ⅱ 1. 「安全基準等」の対象範囲及び対象とする脅威 (P.3)	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。	ご指摘の点については、「(1)サイバー攻撃によるIT障害」の例にあるとおり、意図的に行われる外部からの行為だけでなく、内部からの行為も含んでいます。
2－2	Ⅱ 1.(2) 非意図的要因によるIT障害 (P.4)	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。	ご指摘を踏まえ、以下のように修正を加えます。 「システムの仕様やプログラム上の欠陥(バグ)、・・・」
2－3	Ⅱ 3.(4) 対策項目 (P.5)	「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。	ご指摘の点については、今後の政策の推進に当たっての参考の一つとさせていただきます。
2－4	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 (P.6)	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。	ご指摘の点については、本指針(案)の4ページⅡ3.(2)の「対象範囲と想定する脅威」に含んでいます。
2－5	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 (P.8)	「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。	ご指摘の点は重要と認識しており、「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」においても、「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」である旨示しているとおりです。 また、外部委託先の選定基準を規定する際には、国際規格を踏まえた既存の取り組み等を参考に検討すべきという点についても、「(ア)委託先管理の仕組み」に明示しています。
3	Ⅰ 目的及び位置づけ (P.1)	指針の目的が重要インフラの情報セキュリティ対策であるならば、その対象範囲をIT障害に限定するのでは部分的な情報セキュリティ対策にしかならない。 IT障害だけでなく、紙などの現物や他の情報媒体を含め、媒体を問わず情報及びドキュメンテーション全体をその対象範囲を捉えたうえでの指針の内容にしていただきたい。 実際、官民を問わず情報資産は様々な媒体で構成されマネジメントされているのである。 さらに、情報資産の安全確保はその先に情報活用の仕組みがあって始めて真に役立つものとなる。情報活用についてのガイドライン等も示されればなお有効な指針となるであろう。	ご指摘の点については、「Ⅱ『安全基準等』で規定が望まれる項目」の「1.『安全基準等』の対象範囲及び対象とする脅威」にお示ししたとおり、保護対象には、情報資産、情報システム間でやりとりされるトランザクション又はビジネスプロセス及び情報システムの運用が想定されており、重要インフラ事業者等の事業継続性に密接に関連するものであれば、媒体を問わず情報及びドキュメンテーション、さらにはそれらの運用等も含まれるものです。
4－1	Ⅰ 目的及び位置づけ と Ⅰ 2.「安全基準等」の必要性 (P.1)	各重要インフラ事業者が自主的な取組みのもと、その「安全基準等」を満たすべく努力し、また満たしているか否かを自ら検証するとしているが、検証のみにとどめるのではなく、検証に基づくサービスの保証(SLA)を明らかにさせ、国民に選択させる必要がある。 またそのためには内閣官房、重要インフラ所管省庁による「安全基準等」の継続的検証、助言、経済的支援が必要である。	ご指摘の点については、今後の政策の推進に当たっての参考の一つとさせていただきます。
4－2	Ⅰ 5. 本指針を踏まえた安全基準等策定若しくは見直しへの期待 (P.3)	5.本指針を踏まえた安全基準等策定若しくは見直しへの期待についての記述の中で、国内外のベストプラクティスを積極的に参考にしていくとともに、「政府機関の情報セキュリティ対策のための統一基準」及び関連文書を適宜参照するとしているが、「安全基準等」策定において、参照した文書や法令等を明示すべきである。	ご指摘の点を踏まえ、以下のように修正し、今後の政策運営に適切に反映してまいります。 「このような観点からは、各種規格をはじめとする国内外のベストプラクティスを積極的に参考としていくとともに、別途決定する『政府機関の・・・・」
4－3	Ⅰ 5. 本指針を踏まえた安全基準等策定若しくは見直しへの期待 (P.3)	本指針に示された項目を満たすだけでなく、一層高度かつ網羅的な安全基準等となるようにするためには、ISO/IEC 27001やISO/IEC 17799を踏まえたベストプラクティスを積極的に参考とする必要がある。	4－2に対する回答に同じです。

４－４	Ⅱ ３．(4) 対策項目 (P.5)	「安全基準等」に盛り込む具体的な対策として4つの柱が示されているが、「ウ　情報セキュリティ要件の明確化に基づく対策」(ア)(イ)については、当該情報システムへ導入すべきセキュリティ要件を明示するだけでは十分ではなく、対策についても明示する必要がある。	ご指摘の点については、ウ本文にも(ア)及び(イ)のセキュリティ要件を明示した上で、各情報システムにおいて講ずべき対策を示すことが重要である旨、明示しています。
４－５	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 (P.8)	「安全基準等」に盛り込む具体的な対策として3つの重点項目が示されており、「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」については、(ア)～(ウ)までの検討事項が記載されているが、外部委託先の情報セキュリティ対策の水準を確保するためには、ISMS認証基準のような客観的な基準に基づく評価等を活用することが必要である。	４－２に対する回答に同じです。
４－６	Ⅲ (2)② 「安全基準等」に対する準拠状況の評価 (P.10)	重要インフラ事業者等は、「安全基準等」に対する準拠状況の評価を実施するに際して、自ら定期的に点検するとともに、内閣官房、重要インフラ所管省庁による評価・検証・助言も受けることが必要であり、その結果についてはサービスの保証(SLA)等を通じて国民に知らせる必要がある。	ご指摘の点については、今後の政策の推進に当たっての参考の一つとさせていただきます。
５－１	Ⅱ ３．(4)①エ 情報システムについての対策 (P.6)	以下の文章を追加すべきと考えます。(下線部は追加事項) 現在、各重要インフラ事業の継続及びサービスの維持は、業務系、制御系を問わず、情報システムへの依存度が高くなっている。 このため、明確化した情報セキュリティ要件に対応した対策項目を、ライフサイクルに応じて装置やシステムごとに規定することが重要である。 また、社外での情報処理の制限や社外の情報セキュリティ水準の低下を招く行為の防止等、個別事象への対応事項として対策すべきと思われる項目も規定されることが重要である。 なお、安全な情報システムの構築を推進するため、情報セキュリティに係る国際規格を利用した取組等を踏まえ、安全性等について客観的に評価された暗号、製品等を導入することを併せて検討することも重要である。	４－２に対する回答に同じです。
５－２	Ⅱ ３．(4)②イ(ウ) 不正アクセスによる脅威への対策 (P.8)	以下の文章を追加すべきと考えます。(下線部は追加事項) 保護すべき情報が保存されたＰＣや外部記録媒体の盗難、紛失及び当該ＰＣや外部記録媒体からの情報漏えいを防止するための措置や、保護すべき情報を処理するウェブやメール等のアプリケーションからの情報の漏えいを防止するための対策が取られ、その安全性等が国際規格で評価されたものを使用すること措置が明示されるべきである。	４－２に対する回答に同じです。
５－３	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 (P.8)	以下の文章を追加すべきと考えます。(下線部は追加事項) 昨今、各重要インフラ分野における重要情報の漏えいが発生している。その漏えい経路は、重要インフラ事業者等の内部からのみでなく、委託先からのものも含まれている場合が多い。また、各重要インフラ分野における事業継続性の確保には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であり、各重要インフラ事業者等による委託先の情報セキュリティ確保に向けた対策を、政府が提供する外部委託に際してのガイドライン、国際規格、ベストプラクティスなどを参考に、併せて規定することが望ましい。	４－２に対する回答に同じです。
６	Ⅱ２． 「安全基準等」の公開 (P.4)	●安全・安心に取り組む姿勢の表明については、「安全基準等」の公開を手段とせず、別の分かりやすい内容・手段で表明する必要があると考えます。 ○「安全基準等」については、公開を前提とすべきではないと考えます。	１に対する回答に同じです。
７	Ⅲ(2)① 「安全基準等」の見直し (P.10)	「監査について『安全基準等』に明示することを検討する」とあるが、IT戦略本部の評価専門調査会報告書で、我が国の情報セキュリティ監査実施率が約４２％に達している状況を鑑みれば、我が国の根幹を支える重要インフラ事業者について、監査をすることは必須と考える。 また、その際、情報セキュリティ監査のための専門性や能力を事業者自らが早急に備えるべきであるが、それが間に合わない或いは困難な場合には、既に世の中に普及してきている外部の専門家、特に監査品質を客観的に担保する制度を有している団体などの監査人による監査を通じて、必要な情報セキュリティ水準が確保されているかを客観的に検証すべきである。	ご指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。

８－１	Ⅰ３． 「安全基準等」とは何か (P.2)	「理解可能な状況となっている」ではなく「明確になっている」とすべき	ご指摘を踏まえ、以下のように修正を加えます。 「･･･一覧することにより、『自らが何をすべきか』が重要インフラ事業者の事業に携わる全ての関係者にとって、理解可能な状況となっていることが望まれる。」
８－２	Ⅰ４． 本方針の位置づけ (P.2)	「何をすべきか」を「何をどの優先順位で行なうか」に修正すべき	「何をすべきか」は、具体的な安全基準等において、情報セキュリティ対策の項目及び水準を示す文書の中で、例えば重要インフラ事業に携わる経営者、従業員等各々の役割と責任をもった関係者ごとに実施すべきものとして明らかにされることになります。
８－３	Ⅱ３．(4)①イ(イ) 情報の取扱い (P.5)	「複製」、「更新」を加えるべき	ご指摘の点については、6つの行為に含まれると考えます。なお、政府統一基準においても当該6つの行為について記述しているものです。
８－４	Ⅱ３．(4)①エ 情報システムについての対策 (P.6)	「社外の情報セキュリティ水準の低下を招く行為」については、例を交えて具体的に示して欲しい	ご指摘の点については、「･･･情報処理の制限や情報セキュリティ水準の低下を招く社外での行為の防止等、･･･」と修正を加えます。 昨今の情報漏えいの事例を想定していますが、具体的例示は相応しくないと考えており、この表記としています。
８－５	Ⅱ３．(4)②ア(ア) 事業継続性確保のための個別対策の実施 (P.7)	「措置」を「手順」に変更すべき	ご指摘の点については、「措置」に包含されるものと考えます。
８－６	Ⅲ(2)② 「安全基準等」に対する準拠状況の評価 (P.10)	「評価基準を策定し、その基準を公開する」旨、記載すべき	ご指摘の点については、今後の政策の推進に当たっての参考の一つとさせていただきます。
９－１	Ⅱ２． 「安全基準等」の公開 (P.4)	主旨については賛同するものですが、実際に「安全基準等」の公開が促進されるためには、「公開」「非公開」の判断基準、対象となる具体的な項目例を示すことが望ましいと考える。 また、条件付き開示等により、重要インフラ分野の事業者が安心して開示できる仕組み作りが必要と考える。	1に対する回答に同じです。
９－２	Ⅱ３．(4)①ア 組織・体制及び資源の確保 (P.5)	情報セキュリティ対策のPDCAサイクルを機能させるために、運用に係る組織及び体制の確立及びこれを支える資源の確保が重要と、記載されていますが、「これを支える資源」が不明確であり、何を示すかを明確にしたほうが良いのではないか、と考える。	ご指摘の点については、なお書きにて例示しているものです。
９－３	Ⅱ３．(4)①エ 情報システムについての対策 (P.6)	安全な情報システムの構築を推進するため、客観的に評価された暗号、製品等を導入することを検討すべきという内容が記載されている。情報の暗号化は有効な手段の1つであると考えますが、これだけを取り上げるのは如何なものか、と考えます。	暗号の導入については、あくまで安全な情報システム構築の推進の一例として例示しているものです。
９－４	Ⅲ(1) 本指針の見直し (P.9)	内閣官房は定常的なIT障害の発生状況を把握等の記載があるが、重要インフラの維持にダメージを与える「IT障害」と記載したほうが良い、と考える。	1ページ脚注にお示ししたとおり「IT障害」とは、重要インフラの情報システムにおける定常的な障害全般を指す用語ではなく、「各事業において発生する障害（サービスの停止や機能の低下等）のうち、ITの機能不全が引き起こす障害」と提示しているところです。
９－５	Ⅲ(2)① 「安全基準等」の見直し (P.10)	内閣官房の役割として、インフラ相互間の連鎖的な影響の分析、これに伴う「安全基準等」の見直しに関する情報の提供等、が必要ではないか。	ご指摘の点については、Ⅲのフォローアップにおいて、内閣官房の取り組みとして記述しているものです。
１０－１	Ⅱ１．(2) 非意図的要因によるIT障害 (P.4)	脅威として、「仕様外の事象によるシステムの不正動作」、を追加すべきである。	２－２に対する回答に同じです。
１０－２	Ⅲ(1) 本指針の見直し (P.9)	相互依存性解析は重要インフラ保護にとって非常に重要なテーマであり、内閣官房が総合的な立場から相互依存性分析により積極的に取組み、早期に相互依存性解析の実施が期待される。	ご指摘の点については、今後の政策の推進に当たっての参考の一つとさせていただきます。