「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)」への意見提出者一覧
（五十音順）

ＡＲＭＡ　International東京支部
株式会社　ＮＴＴデータ
有限責任中間法人　ＪＰＣＥＲＴ／ＣＣ
社団法人　情報サービス産業協会
独立行政法人　情報処理推進機構
電気事業連合会
財団法人　日本情報処理開発協会
特定非営利活動法人　日本セキュリティ監査協会
日本放送協会
株式会社　日立製作所

※　五十音順にて記載しております。下記提出意見の意見番号との関連はありません。

提出意見一覧

（意見　1）

該当箇所	「指針」（案）4ページ10～12行目
意見内容	「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。
理　由	当該項目が非公開であることとその理由を明記すること自体が、システム構成や運用実務を推測できる材料を提供することとなり、結果として業務の根幹に関わるITシステムを危険にさらす場合が少なくないから。

（意見　2－1）

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。

（意見　2－2）

該当箇所	P4 II－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。

（意見　2－3）

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。

（意見　2－4）

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。

（意見　2－5）

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。 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。

（意見　3）

該当箇所	重要インフラの定義と情報セキュリティ確保の対象について ・　「指針」全体にかかるが特に1．目的、位置づけ部分 ・「重要インフラの情報セキュリティ対策に係る行動計画」の1．目的と範囲及び重要インフラの定義と対象
意見内容	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。

理　由	官民を問わず、組織における重要な情報資産は電子媒体はもとより、紙やマイクロフィルム等様々な媒体により構成されマネジメントされている。従ってその情報セキュリティ対策の対象範囲は IT 障害に限定してはならない。実際、過去に重要情報インフラに係る記録の改ざん等の事件が発生し、社会問題になってきたこともある。 一方、新会社法や今後作られる日本版 SOX 法が組織の内部統制の強化を求めている。内部統制の手段の1つのテーマとして危機管理が重要な課題となってきている。危機管理の基盤には情報管理がある。優れた情報管理の仕組みづくりが喫緊の課題である。欧米に比べると日本のこの分野は法及び規制環境は整備されていない。この度の指針がこうした課題を考える上で1つの方向性を示してくれることを願っている。 昨年7月に制定発行された「情報とドキュメンテーションの記録管理 JIS X 0902-1」が記録管理の指針として役立つことを紹介したい。

(意見　4－1)

該当箇所	Ⅰ　目的及び位置づけ 2.「安全基準等」の必要性　1 ページ
意見内容	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。
理　由	重要インフラにおける情報セキュリティの確保は、国民生活や社会経済活動の基盤となるものであり、自主的な検証だけでなく、政府等の評価、助言、経済的支援により必要な水準を確保するため。

(意見　4－2)

該当箇所	Ⅰ　目的及び位置づけ 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　3 ページ
意見内容	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。
理　由	「安全基準等」を策定するに際して、どういう形でベストプラクティス等を積極活用したかを示すため。

(意見　4－3)

該当箇所	Ⅰ　目的及び位置づけ 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 3 ページ
意見内容	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。
理　由	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参照するだけではなく、世界的なセキュリティ標準である ISO/IEC 27001 や 17799 を積極的に取り入れることにより、グローバルでかつ高度な情報セキュリティ水準の実現を目指すため。

（意見　4－4）

該当箇所	Ⅱ　「安全基準等」で規定が望まれる項目 3．具体的項目 (4) 対策項目　6 ページ
意見内容	「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。
理　由	標題及び前文では「対策」に焦点が当てられているにもかかわらず、(ア)「情報セキュリティ確保のために求められる機能」及び (イ)「情報セキュリティについての脅威」に記載されていることは、導入すべきセキュリティ要件の明示であり、対策を示すことを求めていないため。

（意見　4－5）

該当箇所	Ⅱ　「安全基準等」で規定が望まれる項目 3．具体的項目 (4) 対策項目　8 ページ
意見内容	「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。
理　由	外部委託可能な範囲の明確化や委託先の選定基準、委託先に求める情報セキュリティ対策項目や事業者としての管理方法等を規定するのであれば、外部委託先の情報セキュリティ対策の水準を把握する必要があるが、これにはＩＳＭＳ制度等の第三者評価の活用が有効であるため。

（意見　4－6）

該当箇所	III　フォローアップ （2）「安全基準等」の継続的検証 ②「安全基準等」に対する準拠状況の評価　10 ページ
意見内容	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。
理　由	各重要インフラ分野における「安全基準等」に対する準拠状況の評価については、情報セキュリティ政策会議あるいは内閣官房、重要インフラ所管省庁の協力による専門家の継続的検証・評価・助言が必要であり、これに基づくサービスの保証（SLA）の変更などは、国民に知らせる必要があるため。

（意見　5－1）

該当箇所	P6　エ　情報システムについての対策
意見内容	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、<u>情報セキュリティに係る国際規格を利用した取組等を</u>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。
理　由	客観的に評価されただけでは不十分であり、安全性等について評価することが必要と考えます。また、情報セキュリティの評価は、その評価基準により安全性等のレベルは変わりますから、実績のある国際規格（例えば、ISO/IEC15408）などに基づく取組を踏まえる必要があると考えます。

（意見　5－2）

該当箇所	P8　（ウ）　不正アクセスによる脅威への対策

意見内容	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。
理由	情報の漏えいを防止するための措置を明示するだけでは不十分であると考えます。情報の漏えいを防止するための対策が取られ、かつ国際規格などの実績のある評価基準で評価されたものを使用することでその安全性等が確保されますので、このことを具体的に示すべきであると考えます。

(意見　5－3)

該当箇所	P8　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	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。
理由	重要インフラは国民の日々の生活に直接影響を与えるので、その事業継続性の確保は最重要事項です。また、重要インフラはその事業規模が大きく様々な外部委託者が関与してその事業活動が行われています。従って委託先に係る対策について、信頼性の高いガイドライン、国際規格、ベストプラクティスを参考にする必要がありますし、これら情報は政府が責任を持って提供する必要があると考えます。

(意見　6)

該当箇所	P4　2.「安全基準等」の公開

意見内容	● 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。
理　由	● 安全･安心に取り組む姿勢を国民に表明する際、分かりやすい内容で表明する必要があると考えます。専門用語等を用いた「安全基準等」の公開を手段とせず、別の分かりやすい内容･手段で姿勢を表明する必要があると考えます。 ○ 安全基準等を公開することは、守るべきセキュリティ情報が攻撃者等にも伝わることとなり、脅威の増大等が想定されるところです。 ○ また、非公開項目を明示し、その理由を明記したとしても、同様に脅威の増大等が懸念されるところです。 ○ このようなことから、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。

（意見　7）

該当箇所	P10 **III.** (2) ①「安全基準等」の見直し
意見内容	「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。
理　由	意見内容と同じ

（意見　8－1）

該当箇所	２ページ「3．安全基準等とは何か」

意見内容	「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
理　由	「理解可能な状況」という言葉はあいまいで分かりにくい

（意見　8－2）

該当箇所	2 ページ「4．本指針の位置づけ」
意見内容	「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
理　由	「もっとも困難」なのは、「何をすべきか」ではなく、「何をどのような優先順位で行なうか」だと思われる

（意見　8－3）

該当箇所	5 ページ「(イ) 情報の取扱い」
意見内容	「複製」、「更新」を加えるべき
理　由	情報の「複製」、「更新」も「取扱い」の重要な例である。

（意見　8－4）

該当箇所	6 ページ「エ 情報システムについての対策」
意見内容	「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
理　由	具体的に何を指しているのかが分かりにくいため

（意見　8－5）

該当箇所	7 ページ「(ア) 事業継続性確保のための個別対策の実施」
意見内容	「措置」を「手順」に変更すべき
理　由	インシデント発生時は、誰でも分かる平易な手順(書)が必要であるため、より具体的に明示すべきものとして「措置」ではなく「手順」と表記すべきと考えられるため

（意見　8－6）

該当箇所	10 ページ「安全基準等に対する準拠状況の評価」
意見内容	「評価基準を策定し、その基準を公開する」旨、記載すべき
理　由	評価の基準がなければ、「自己」点検も不可能 また評価基準が公開されれば、「自己」点検であっても、その信頼性がある程度は担保される

（意見　9－1）

該当箇所	II「安全基準等」で規定が望まれる項目 ２.「安全基準等」の公開
意見内容	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。

理　　由	保護対象や想定する脅威に関する情報を公開することは、攻撃者に対してヒントを与えることに繋がるのではないか、と一般的には懸念されます。このため、「公開」「非公開」とすべき項目や、その判断基準があって初めて、実際の「安全基準等」の公開が促進され得るのでは、と思われます。 合せて、「安全基準等」の公開を促進する為の取組みとして、重要インフラ分野の事業者が、特定の条件の下で開示する（匿名の請求者には開示しないなど）など幾通りかの「公開」の形態を選択できる仕組み作り等も必要では、と考えます。

(意見　9－2)

該当箇所	II「安全基準等」で規定が望まれる項目 ３．（４）①　ア　組織・体制及び資源の確保
意見内容	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。
理　　由	重要インフラ分野毎に保護対象となる情報や情報システムは異なっており、適切な脅威分析に基づいて情報セキュリティ対策及びその PDCA サイクルを機能させる仕組み作りが必要となります。したがって、PDCA サイクルを機能させるための資源の確保について、その内容範囲を明確に記載したほうが良い、と考えます。

(意見　9－3)

該当箇所	II「安全基準等」で規定が望まれる項目 ３．（４）①　エ　情報システムについての対策
意見内容	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。

理　　由	情報システムの安全性を考える場合、情報の暗号化は有効な手段と思いますが、システム全体の安全性への寄与度は限定的と、考えています。主旨については賛同するものですが、暗号製品を導入することだけで、情報システムの安全性が確保できるものではありませんし、高度なセキュリティを確保する手段は幾つかあり得ますから、暗号製品の導入の必要性のみを取り上げない方が良いのではないか、と考えます。

(意見　9－4)

該当箇所	III　フォローアップ （1）本指針の見直し
意見内容	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。
理　　由	情報システムにおける定常的なIT障害と一口に言っても様々なレベルのものが考えられますので、重要インフラの維持にダメージを与える「IT障害」について、内閣官房がその発生状況の把握をするという記載に変更したほうが良い、と考えます。

(意見　9－5)

該当箇所	III　フォローアップ ２．①「安全基準等」の見直し
意見内容	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。

理　　由	本指針は、サイバーテロ、災害、非意図的要因などによる IT 障害や情報漏えいを念頭において、重要インフラ事業者が満たすべく情報セキュリティ対策の水準を示す為のものと記載されております。しかし、重要インフラのサービス停止の原因には、他の重要インフラの IT 障害に起因し、副次的・連鎖的に引き起こされるものもあります。こういったインフラ相互間の連鎖的な影響の分析やこれに係る「安全基準等」は、個別の重要インフラ所管省庁や重要インフラ事業者では把握が困難と考えます。 一方、「重要インフラの情報セキュリティ政策に係る行動計画」において、２００６年度に内閣官房にて相互依存性解析の試行を開始とありますので、上記相互依存性の解析に基づく「安全基準等」の見直しに関する情報提供等を内閣官房にて担って頂くのが良い、と考えます。

(意見　10－1)

該当箇所	II　1.「安全基準等」の対象範囲及び対象とする脅威」 (2)非意図的要因による IT 障害　P4
意見内容	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。
理　　由	非意図要因による IT 障害への脅威を特定し、対策を事前に立案していくことは望ましい。しかし、IT システムが期待通りに動作しない要因として、「プログラムが仕様通りに機能しない事態(プログラム上の欠陥（バグ）)」と、「発生事象自体が想定されておらずプログラムが対処できない事態(仕様外の事象によるシステムの不正動作)の区別に対する認識を向上させるためにも、ここで分けて列記しておくべきである。すなわち、前者は品質管理上、後者はリスク管理上の課題として、許容範囲をどう設定するかという視点で対策が検討されるべき、異なる脅威である。 加えて、各種の脅威に対する対策実施責任については、引き続き議論していくことが必要であると考える。

(意見　10－2)

該当箇所	III (1)本指針の見直し P9 ・内閣官房は定常的な IT 障害の発生状況の把握を通じ、各重要インフラ分野に共通する横断的な対策課題の分析・検討を行い、本指針改定のための基礎資料として整備する ・各重要インフラ事業者等における事業継続性確保対策の検討にとって、重要インフラ間の相互依存性の状況やそれに基づくリスク情報は重要と考えられることから、今後、内閣官房が各重要インフラ

	所管省庁及び重要インフラ事業者等の協力を得て相互依存性解析を実施する際には、その結果を本指針や各重要インフラ分野における「安全基準等」の見直しの基礎資料として提供する。
意見内容	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。
理　　由	内閣官房という立場は、各重要インフラ所管省庁及び重要インフラ事業者等の取組みを調整し、わが国全体という立場から重要インフラ相互間の依存について分析を行い、インフラ保護についてより俯瞰的な視野からの対策を立案・提起できる立場にあるので。