「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５版）」（案）に対する意見募集の結果一覧

意見募集期間：平成30年１月25日（木）から同年２月15日（木）まで　18件

No	箇所	頁	団体名	御意見	御意見に対する考え方	修正有無 （修正後の頁番号）
1	－	－	匿名団体	ユーザー企業で活躍の広まりがない「情報処理安全確保支援士」の活躍機会となればと考えます。「情報処理安全確保支援士」の配置義務あるいは活用推奨を記載していただきたい。同試験の合格者は、ある一定のレベルの知識・スキルを持ち合わせている。関係各位と様々な対策強化に関する議論が深まると思います。	ご指摘の点を踏まえ、関係部分を以下のとおり修正いたします。 ----- （２）人材育成及び意識啓発 「特に、情報セキュリティ対策の推進役となるセキュリティ人材の育成においては、政府機関の人材育成プログラムやセキュリティベンダーが提供するトレーニング等の活用や、関係主体等と連携した演習・訓練（※4.2.1.（３）参照）への参加、「情報処理安全確保支援士」等の資格取得等も期待される。」	17
2	Ⅱ.4.1.3.(２)(ウ)	12, 36	パスロジ株式会社	p12：4.1.3(2)(ウ)アクセス制御 ●情報システム等のアクセス制御 および p36：【別紙４】対策項目の具体例等の参照先 4.1.3（2)(ウ)アクセス制御 ●情報システム等のアクセス制御 【内容】 主体認証機能について言及されていますが、主体認証機能についての詳細な表記が「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」の6.1.1にされております。 こちらを参照先として掲載することを提案させていただきます。	ご指摘の点を踏まえ、左記ガイドラインを【別紙４】に追加いたします。	37～39
3	Ⅱ.4.1.4.(２)	17	個人	P17の（２）人材育成及び意識啓発　について 『情報セキュリティ対策の推進役となるセキュリティ人材について、重要インフラサービスの安全かつ持続的な提供に必要不可欠な能力や人数等を確保・維持する観点から、これらのセキュリティ人材の重要インフラ事業者内のキャリアパス及び賃金政策をあらかじめ検討しておくことが重要となる。』とあるが、人材のスキル評価に関する記述が欠けていると感じた。 経済産業省「サイバーセキュリティ経営ガイドライン」P9の注釈には下記の記述がある。 『セキュリティ人材が有するスキルを測る指標の一つとして、民間企業が提供する専門資格や IPA が実施している情報処理安全確保支援士制度などを活用することも有効である。』 本件にも同様の記述を本文中に追加し、人材の育成が達成されているかの客観的な評価・確認を推進するべきであると考える。	ご指摘の点を踏まえ、関係部分を以下のとおり修正いたします。 ----- （２）人材育成及び意識啓発 「特に、情報セキュリティ対策の推進役となるセキュリティ人材の育成においては、政府機関の人材育成プログラムやセキュリティベンダーが提供するトレーニング等の活用や、関係主体等と連携した演習・訓練（※4.2.1.（３）参照）への参加、「情報処理安全確保支援士」等の資格取得等も期待される。これらの取組は人材育成の達成状況を客観的に評価・確認する際にも有効となる。」	17

4	－	－	個人	「重要インフラにおける情報セキュリティ確保・中略・（第５版）(案)」を拝読しましたが、全体を通じて性善説に依存しており、且つ法の助力もなく、有効性が疑わしいと判ぜざるを得ません。本案は、重要インフラに関わった企業と、情報を盗みたい第三者が金融機関と結託した場合、つまり過去にも起きた企業買収により公然と行われた情報漏洩の懸念を教訓としておらず、全く不十分です。この案を逆に解せば、悪意を持ちながらも案に沿って行動しさえすれば情報は入手出来てしまうと示されたことになります。勿論これは仮定の話ではなく、実際に進行中の話です。なお、実際には企業を買収する必要すらありません。役員を送り込む、或いは盗聴用の通信インフラ等を使わざるを得ないよう仕向けるだけで、情報セキュリティ管理責任者が関知する間もなく情報は横取りが可能です。重要インフラ案件に関わった企業が経営に行き詰まり、経営者が経営資金や金融機関に対する信用を対価に情報を漏洩する誘惑に駆られた場合、現行の法制度ではその実行を阻止出来ません。また経営幹部によって為された情報漏洩は発見が困難になるか、発覚まで非常に時間を要する結果になり得ます。経営に行き詰まるなどしてモラルの低下した経営者に厳格なリーダーシップやPDCAの遂行は期待できるのでしょうか。経済状況が変われば人は変わります。企業側へ無駄な努力を押し付けるのではなく、厳罰を主体とした法制度により組織的・計画的情報漏洩を防がなけば、高いセキュリティ意識も絵に描いた餅に過ぎません。	貴重なご意見をいただき、ありがとうございました。 今後の検討の参考とさせていただきます。	修正なし
5	Ⅱ.4.1.1.(２)	7	電気事業連合会	Ⅱ.4.1.1.(2) サプライヤーや委託先からの「要求事項」という表現を使うでしょうか？サプライヤー、委託先からの「制限事項」「制約事項」という表現ではないでしょうか？	ご指摘の点を踏まえ、関係部分を以下のとおり修正いたします。 ----- （２）関係主体等の要求事項の理解 「重要インフラ事業者等の情報セキュリティ対策の取組（重要インフラサービス障害発生時の初動対応や復旧対応等も含む）に対する、関係主体、顧客、サプライヤー、委託先等からの要求事項を整理する。要求事項には、各事業分野の関係法令や契約等に規定された義務や、サプライヤーや委託先が提示する制限事項等も含まれる。」	7
6	Ⅱ.4.1.2.(1)	7	電気事業連合会	Ⅱ.4.1.2.(1) 経営上の重要会議での意思決定は重要であるものの、サイバーセキュリティ経営ガイドラインVer.2.0の記載（「経営会議などで対策の内容に見合った適切な費用かどうかを評価」））に合わせるべきではないでしょうか？	本指針の「重要インフラ事業者等の経営層の在り方」を認識いただくとともに、「サイバーセキュリティ経営ガイドライン」等も参考としていただくことを期待しております。	修正なし
7	Ⅱ.4.1.3.(1)	10	電気事業連合会	Ⅱ.4.1.3.(1) 「リスク選好」という言葉はそれほど一般的ではないのではないでしょうか？　これまでのＮＩＳＣの資料や引用されているＩＰＡの資料の中にも記載がない言葉です。参考資料に「組織に追求する又は保有する意思があるリスクの量及び種類。」との用語説明がありますが、分かりづらいため、解説を補充するか、言葉を削除してはどうでしょうか。	ご指摘の点を踏まえ、「リスク選好」を「リスクに対する態度」という言葉に変更するとともに、脚注に補足説明を追加いたします。 ----- リスクに対する態度 「リスクのアセスメントを行い、最終的にリスクを保有する、取る又は避ける、という組織の取組みのこと。リスクに対する態度を明らかにするとは、例えば「20%未満のサービスレベル低下を伴う重要インフラサービス障害の発生は年間３回以下とする」といったように、重要インフラ事業者等がどの程度のリスクを	10

8	Ⅱ.4.1.3.(2)(オ)	13	電気事業連合会	Ⅱ.4.1.3.(2)(オ) 要員面の制約により、複数の作業要員を確保できないケースもあり、単独作業を制限することは現実的ではないと考えられるため、削除してはどうでしょうか。	ご指摘の点を踏まえ、関係部分を以下のとおり修正いたします。 --- ●セキュリティ確保が求められる領域 「また、悪意ある活動を防止する観点から、当該領域への認可されていない物品の持ち込みを制限する。加えて、複数の作業要員を確保できる重要インフラ事業者等においては、単独での作業を制限するといった対応も有効である。」	13
9	Ⅱ.4.1.3.(2)(カ)	13	電気事業連合会	Ⅱ.4.1.3.(2)(カ) ソフトウェアバージョンの更新によりシステムの可用性を損なうケースも存在することから、全てのシステムにおいてソフトウェアをサポート対象バージョンに更新出来るわけではありません。このような場合に代替手段（ネットワーク上で攻撃を防止する装置の導入など）を講じるケースもあることから、ソフトウェア更新以外の手段も可能とする表現が望ましいと考えます。	ご指摘の点を踏まえ、関係部分を以下のとおり修正いたします。 --- ●運用ソフトウェアの管理 「また、重要インフラサービス障害が発生した際やサイバー攻撃等の予兆を認識した際に、ソフトウェアベンダ等のサポートを速やかに受けることを可能にするため、サポート対象バージョンへの更新を計画的に実施する。なお、サポート対象バージョンへの更新が困難である場合においては、重要インフラサービス障害やサイバー攻撃を防止するための補完的な措置を講じる。」	14
10	Ⅱ.4.1.4.(3)	17	電気事業連合会	Ⅱ.4.1.4.(3) 経営層と実務者層のギャップが生じないようにするためには、定期的な対話の機会よりも、自社だけでなく、業界によらず発生しているセキュリティインシデントに関する話題など、日頃からコミュニケーションを図ることが重要ではないでしょうか。	ご指摘の点を踏まえ、関係部分を以下のとおり修正いたします。 --- （３）コミュニケーション 「情報セキュリティリスクへの対応に責任を持つ経営層と、経営層による管理（指示、モニタ、評価等）の下で情報セキュリティ対策を推進する実務者層との間で、定期的な対話の機会等を設け、コミュニケーションを活性化することが重要である。」	17
11	Ⅱ.4.1.4.(3)	17	電気事業連合会	Ⅱ.4.1.4.(3) 一つの手段であると思われるので、語尾を見直してはどうでしょうか。	ご指摘の点を踏まえ、関係部分を以下のとおり修正いたします。 --- （３）コミュニケーション 「また、自組織が所属する重要インフラ分野全体で重要インフラサービスの安全かつ持続的な提供を実現するという観点から、他の重要インフラ事業者や所管省庁等の関係主体と各々の役割や責任分担、情報共有や報告の体制等について意見交換を行うことも有効である。」	17
12	－	－	株式会社ＩＣＳ研究所	従来の安全基準等の策定指針に比して、重要インフラの機能保証を維持継続するために、ＰＤＰＤで終わりがちなＰＤＣＡにやるべき要素が明確に示されていると思います。 あと、工事や現場サポートでベンダや業者が持ち込むＰＣやデバイス、ソフトウェアにウイルスやマルウェアがあって、現場の設備につなぐことで感染し、試運転や操業開始時に緊急停止する件数が１企業で年間十数件から数十件起きている企業が少なくありません。それによって操業時間が減ることで機能保証が減少している事実にも対策が必要と考えます。	ご指摘の点を踏まえ、関係部分を以下のとおり修正いたします。 --- ●マルウェアからの保護 「標的型攻撃メールやUSBメモリ等から情報システムに感染するマルウェアが重要インフラサービス障害を引き起こす可能性が考えられるため、マルウェアを検出及び予防する仕組みをあらかじめ整備しておくとともに、万が一マルウェアに感染した場合でも早期回復を図るための対策及び手順を確立する。なお、重要インフラ事業者等が直接管理することが困難である、委託先等が持ち込むPCやデバイスがマルウェア感染している可能性も考慮する。」	13

13	【別紙３】	30	匿名団体	「サイバー攻撃リスクの特性②：攻撃手口の高度化」に関して、新しい手口の攻撃が発生した場合には、一定期間、監視機能・体制を強化するという対応も有効ではないか。	ご指摘の点を踏まえ、該当の頁に以下の項目を追加いたします。 -------- 「・ 新たな攻撃手口の情報を入手した場合は、自組織の対策の状況とその有効性及び被害の有無を早急に確認するとともに、自組織への攻撃到達に備え、一定期間、監視機能・体制を強化する。」	31
14	【別紙３】	31	匿名団体	「サイバー攻撃リスクの特性③：急速な被害拡大に繋がる攻撃が行われる可能性」に関して、対策のひとつとしてEDR（Endpoint Detection and Response）製品を加えてはどうか。	ご指摘の点を踏まえ、関係部分を以下のとおり修正いたします。 ----- 【修正前】 「・ 攻撃を受けたシステムからネットワークを介して他のシステムに対して更なる攻撃が行われることを防止する対策（システムの機能や重要性に基づいたネットワークセグメントの分割や、IPS、プロキシサーバ等での不審な通信の制限等）の導入を必要に応じて検討する。」 【修正後】 「・攻撃の拡散に備えた対策の導入を必要に応じて検討する。対策の例として、ネットワークセグメント分割（重要システムの隔離）、IPS/プロキシサーバ（不審な通信の遮断）、EDR（影響範囲の特定と被害端末の隔離）等がある。」	32
15	Ⅱ.4.1.3.(2)(イ)	12	匿名団体	「（イ）資産の管理　●資産に対する責任」に資産目録の記載項目例を書いてはどうか。また、「資産利用の許容範囲」という表現が分かり辛い。	ご指摘の点を踏まえ、関係部分を以下のとおり修正いたします。 ----- ●資産に対する責任 「重要インフラサービスの提供に係る情報システムやソフトウェア、情報等の資産を特定した上、各資産の管理責任者や利用制限（利用が許される範囲）等を明確化した資産目録を作成し、維持管理する。」	12
16	Ⅱ.4.1.3.(2)(カ)	13	匿名団体	「（カ）運用時のセキュリティ管理　●マルウェアからの保護」で、「ホワイトリスト型のマルウェア無効化機能」によってマルウェアの検出率が高まるように読めてしまう。ホワイトリスト型の優位点は未知の脅威に対応できることではないか。	ご指摘の点を踏まえ、関係部分を以下のとおり修正いたします。 ----- ●マルウェアからの保護 「また、優先度の高い重要システムにおいては、マルウェアの検知率向上が期待されるマルチエンジン型のマルウェア検知ソフトや、システム負荷を抑えつつ、未知の脅威に対応できることを特徴とするホワイトリスト型のマルウェア無効化機能の活用も検討することが期待される。」	14

17	－	－	匿名団体	平時においてもサイバー空間関連事業者（特にセキュリティベンダー）を含めた体制を構築する必要性について言及すべきではないか。障害時のみサイバー空間関連事業者に頼る運用では、サイバー空間関連事業者の状況によっては十分な支援が得られず、被害拡大に繋がる恐れがある。	ご指摘の点を踏まえ、関係部分を以下のとおり修正いたします。 ----- （イ）ＣＳＩＲＴ等の整備、関連部門との役割分担等の合意 「サイバー攻撃リスクの特性を考慮したコンティンジェンシープラン及び事業継続計画の実行に必要な組織体制のひとつとして、ＣＳＩＲＴ（又は同等機能を持つ組織）を重要インフラ事業者等の内部に整備する。ＣＳＩＲＴ等の組織は、役割分担や対応手順等について、あらかじめ関連部門と合意しておくことが重要である。 特に、制御システム等の運用環境を保有する重要インフラ事業者等においては、重要インフラサービス障害発生時の対応にＯＴ関連部門の専門知識が要求される可能性を十分に認識しておく必要がある。 また、サイバー攻撃に迅速に対処する観点から、情報セキュリティの専門知識を持つ組織を含めた対処態勢を平時から整備しておく必要性を検討することが期待される。例えば、サイバー空間関連事業者及び情報セキュリティ関係機関との提携が有効である。」	19
18	Ⅱ.4.1.3.(2)(カ)	14	匿名団体	「（カ）運用時のセキュリティ管理　●運用ソフトウェアの管理」に関連して、攻撃者が脆弱なサービスや設定を悪用できないようにするため、セキュアな設定で構築・運用する必要があると考える。（Secure Configurationの考え方）	ご指摘の点を踏まえ、関係部分を以下のとおり修正いたします。 ----- ●運用ソフトウェアの管理 「重要インフラサービスの提供に係る情報システムで利用するソフトウェアは、脆弱な設定状態を悪用した攻撃の可能性が想定されるため、個々の設定について可能な限り把握・理解し、安全性の確保に努める。」	14