「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（第３版） 対策編」（改定案）に対する提出意見の概要及びご意見に対する考え方

重要インフラ専門委員会
平成２５年３月２６日

意見提出者一覧（五十音順）

株式会社クルウィット　2件
日本ユニシス株式会社　7件
特定非営利活動法人　日本ネットワークセキュリティ協会　社会活動部会　16件

その他個人　3件

合計　28件

「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（第3版）対策編」（改定案）に対する提出意見の概要及びご意見に対する考え方（案）

No.	該当箇所	ご意見の概要	ご意見に対する考え方
1	3ページ 〇組織・体制の確立	「・人的資源確保（雇用条件の明示、守秘契約の締結、懲戒手続等）」を「・人的資源確保（雇用条件の明示、守秘契約の締結、人材育成、情報セキュリティ関連資格の推奨・評価等）」に変更する。 （この項の趣旨は情報セキュリティ対策人材の確保であると考えられる。懲戒手続は内部不正の抑制の趣旨と想定されるが、人材確保目的としてはそぐわない。人材育成や、そのための自体的施策である「情報セキュリティ関連資格の推奨・評価」を明示すべきと考える。）	情報セキュリティ対策人材の育成については、3ページ「（イ） 情報セキュリティ人材の育成等【参考事項】」の中の「・情報セキュリティ人材の育成・活用・管理に関する規程の整備（情報処理技術者試験、情報システムユーザースキル標準等を活用し、社内人材育成マップ等の作成とこれに基づく社内教育コースの整備等を記載）」に記載しております。 「懲戒手続」については、人的資源確保にあたって用意しておくべき仕組みの1つと認識しております。
2	3ページ （イ）情報セキュリティ人材の育成等【参考事項】	「育成マップ等の作成とこれに基づく社内教育コースの整備」の後に「、情報セキュリティ関連資格の推奨と教育機会の提供」を追加 （情報セキュリティ人材は高度な知識やスキルを必要とする領域であり、社内教育だけで必ずしも十分な資質が得られない可能性がある。情報セキュリティスペシャリストをはじめ、民間の運営によるものでも世界的に評価される資格が多数あり、このような資格取得を通じての人材育成は重要な手段と考える。よって、資格への言及を明記することで人材育成の具体策の例示を行うべきと考える。）	ご指摘の内容については、重要インフラにおける情報セキュリティ対策全体の中で、追加が適当か否か検討する必要があるため、今後の改定時の検討材料とさせていただきます。
3	5ページ 〇情報の消去	「可搬型記録媒体の物理的破壊や電磁的記録の確実な消去を行うためのプログラムの導入もしくは外部サービスの利用」を追加 （現状の記述では実施のための手続き事項を述べているに過ぎず、具体的対策手段の例示がない。したがって具体的対策手段の例示を追加する。）	情報の消去の手段については、多様であると認識しております。 ご指摘の内容については、重要インフラにおける情報セキュリティ対策全体の中で、追加が適当か否か検討する必要があるため、今後の改定時の検討材料とさせていただきます。
4	6ページ 〇権限管理	システム管理・運用者に付与する特権IDの適切な管理 （情報セキュリティ確保のためには利用者IDの管理以上に特権IDの管理が重要であるので、明示的に示すべきである。）	「・権限管理機能の導入」の中に特権IDの管理機能も含まれているという認識です。ご指摘の内容を踏まえ、導入だけでなく管理も重要であるとの観点から、当該対策について「・権限管理機能の導入実施」とさせていただきます。
5	6ページ 〇冗長化	ネットワークやハードウェアだけでなく、情報システムにも可用性が必要なため、情報システムの冗長化について記述が必要と思われます。	冗長化は、ハードウェア（電子計算機）、ネットワーク（通信回線及び通信回線装置）については記載していますが、アプリケーションを含めた情報システム全体については記載しておりませんでした。 ご指摘の内容を踏まえ、「（アプリケーションを含めた）情報システムの冗長対策」を追加させていただきます。
6	6ページ 〇セキュリティホール	「・不正アクセスの監視・検出（IDSの使用）」を「・不正アクセスの監視・検出・防止（IDS/IPSの使用）」に変更 （今日、IDSは多くの場合IPS機能も備えており、状況に応じて使い分け、もしくは組み合わせての使用が望ましいことから、IPSを追加する。）	不正アクセスについては、IPSだけでなく、ネットワークやアプリケーションにおける防止機能もあります。 ご指摘の内容については、重要インフラにおける情報セキュリティ対策全体の中で、追加が適当か否か検討する必要があるため、今後の改定時の検討材料とさせていただきます。
7	6ページ 〇セキュリティホール	「・標的型攻撃を通じてのマルウェア侵入を防止するための従業者教育の徹底」を追加 （今日外部からの侵入を許す要因の多くが標的型攻撃に誘導されて従業者がマルウェアを引き込むことによっている。標的型攻撃対策には有効な技術的対策が限られることから、従業者の意識を高め騙されないようにする対策は必須である。よってこの項を追加すべきと考える。）	ご指摘の内容については、3ページの「〇教育訓練の実施」の中の項目に含まれますので、原文の通りとさせていただきます。

「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（第3版）対策編」（改定案）に対する
提出意見の概要及びご意見に対する考え方（案）

No.	該当箇所	ご意見の概要	ご意見に対する考え方
8	6ページ 〇セキュリティホール	「・不正アクセスの管理・検出（IDSの使用）」だけなく、他の検出方式も用いるべき。 様々な脅威に対して全てを未然に防ぐことは難しくなるため、マルウェアに感染する可能性もあることを前提にした対策も盛り込む必要がある。例えば、不正アクセスの管理・検出には「ダークネット」(未使用の IP アドレス) を用いた不正アクセスの管理・検出も有効。ダークネットの併記を検討していただきたい。 （ダークネットを勧める理由） 昨今 APT 攻撃を受けて、マルウェアに感染した場合 IDS では検知ができない。マルウェアに感染した場合、感染を広げるために内偵調査が行われるが、その際にダークネットにも通信が発生するため、不正アクセスの検出が可能になる。	ご指摘の内容については、重要インフラにおける情報セキュリティ対策全体の中で、追加が適当か否か検討する必要があるため、今後の改定時の検討材料とさせていただきます。
9	8ページ 〇電力供給の途絶・通信の途絶・水道供給の途絶への対応	「・自家発電装置、無停電電源装置、予備電源」の後ろに（給電回路の冗長化設計、発電装置燃料の優先供給・複数社契約等）を追加 （電源構成の冗長化を行っていても、その配線構造で一箇所だけ冗長構成になっていないために停電が発生したデータセンターの例があり、また東日本大震災に際しては非常用電源設備の燃料供給で危機的状況も発生しており、それらへの対応にまで言及しておくべきと考える。）	ご指摘の内容については、重要インフラにおける情報セキュリティ対策全体の中で、追加が適当か否か検討する必要があるため、今後の改定時の検討材料とさせていただきます。
10	8ページ 〇電力供給の途絶・通信の途絶・水道供給の途絶への対応	新項目として「非常用予備設備の定期点検（試験運転を含む）」を追加 （非常用予備装置は通常時には稼動していないために非常時にいきなり使用してうまく機能するかについて不確実性がある。これを避けるために、定期的点検と、いざというときの稼動確認を常に行っておく必要がある。）	ご指摘の内容については、9ページの「・障害時、緊急時を想定した訓練（復旧テスト等）の実施」に含まれますので、原文の通りとさせていただきます。
11	9ページ 〇運用時（保守時含む）	システム管理・運用者に付与する特権IDの適切な管理 （電子計算機の運用における情報セキュリティ確保のためには利用者IDの管理以上に特権IDの管理が重要であるので、明示的に示すべきである。）	ご指摘の内容については、No.13における修正で対応させていただきます。
12	9ページ 〇運用時（保守時含む）	「最新バージョンまたは適切なぜい弱性回避策の適用」を「・セキュリティホール対策（検査、対応）」の次辺りの位置に追加 （セキュリティホール対策も同趣旨と思えるが、「検査、対応」では実施事項として具体的イメージが弱いので具体的に最新バージョンまたは適切なぜい弱性回避策の適用を記すべきと考える。）	ご指摘の内容については、9ページ「・利用ソフトウェアのアップデート、脆弱性に関する情報収集」に同趣旨の対策を記載しております。
13	11ページ 〇運用時（保守時含む）	バックアップだけできても無意味であり、リストアできなければリカバリできない、また、定期的なリストアテストが肝要であると考えるため、「・データバックアップ、バックアップ媒体の安全管理」の部分は、「・データバックアップ、データリストア、バックアップ媒体の安全管理」としてはいかがでしょうか。	ご指摘の内容については、情報セキュリティ対策の全体像を見ながら追記の検討をする必要があるため、今後の改定時の検討材料とさせていただきます。
14	11ページ 〇運用終了時	運用を終了した機器に残存する取り扱いに慎重を要する情報は回復不能にする必要がある（JIS Q 27002「10.7.2 媒体の処分」より）ため、電磁的記録（媒体）の「情報抹消」は、「情報の完全消去」に修正してはいかがでしょうか。	「抹消」には、「完全に消す」という意味も含まれると認識しておりますので、原文の通りとさせていただきます。
15	13ページ 〇未然防止措置	「・情報システムの多重化、通信回線の冗長化、代替手段の整備」の部分は、「・情報システムの冗長化、通信回線の冗長化、代替手段の整備」としてはいかがでしょうか。 障害対策の理論からすると、多重化ではなく冗長化が正しいです。	ご指摘の内容を踏まえ、「・情報システム・通信回線の冗長化、代替手段の整備」とさせていただきます。
16	16ページ 〇PCや外部記録媒体の盗難、紛失を防止するための措置	「盗難、紛失の防止」を重点項目の一つ(行頭〇の粒度)への昇格を検討していただければ幸いです。 「盗難、紛失の防止」に対する興味は高く、重点項目の一つ(行頭〇の粒度)でも良いのではと考えました。 ※「盗難、紛失の防止」を「人為的過誤の防止」と捉えた場合、「不正アクセスの防止」以外の対策にも関連する粒度の大きな問題であると考えます。	「盗難、紛失の防止」については、16ページ「（ウ） 不正アクセスによる脅威への対策 【要検討事項】」の項に、「〇PCや外部記録媒体の盗難、紛失を防止するための措置」があります。

「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（第3版）対策編」（改定案）に対する
提出意見の概要及びご意見に対する考え方（案）

No.	該当箇所	ご意見の概要	ご意見に対する考え方
17	16ページ 〇PCや外部記録媒体の盗難、紛失を防止するための措置	いまや業務端末としてスマートデバイスを使用することが多くあるため、端末の種別としてPCのみでなく、スマートデバイス（スマートフォンやタブレット含む）を追加してはいかがでしょうか。	ご指摘の内容については、重要インフラにおける情報セキュリティ対策全体の中で、追加が適当か否か検討する必要があるため、今後の改定時の検討材料とさせていただきます。
18	16ページ 〇情報の保存 17ページ 〇アプリケーションからの情報漏えいを防止するための措置	17ページの「〇アプリケーションからの情報漏えいを防止するための措置」の下にある「データの書き換えを検出する設定、定期的な改ざんの有無の検査」をこの項（16ページの〇情報の保存）の下に移動 （上記内容はデータそのものの完全性の保護策であり、機密性対策である「アプリケーションからの情報漏えいを防止」にはそぐわず、また「・ネットワーク上からの不正アクセス対策」としてもそぐわないため）	「データの書き換えを検出する設定、定期的な改ざんの有無の検査」は、不正侵入発見の手段でもあるので、原文の通りとさせていただきます。
19	17ページ 〇アプリケーションからの情報漏えいを防止するための措置	「・ネットワーク上からの不正アクセス対策」についても、他の対策を用いるべき。 不正アクセス対策に「ダークネット」(未使用の IP アドレス) を用いた対策も有効であるため、ダークネットの併記を検討していただきたい。	ご指摘の内容については、重要インフラにおける情報セキュリティ対策全体の中で、追加が適当か否か検討する必要があるため、今後の改定時の検討材料とさせていただきます。
20	17～18ページ 〇内部関係者による情報漏えいを抑止するための措置	全体に、この項における対策項目は整理が必要と考える。 (1)「個人データ」が2ヵ所出てくるが、（個人情報保護法における定義による個人データと推定）この項として保護対象とする情報は、企業等が秘密として管理する対象となる情報全般と考えられる。（P4では情報の格付けについても記述されている。）個人データに限定した場合、その趣旨が分かりにくくなる恐れがある。 (2)「外部での情報処理」「事業者外での」（P18上から2行目）の「外」は組織の設備の外、つまり物理的概念と想定されるが、外部委託との解釈も可能であり、用語が曖昧。 (3)「IDアクセスの不正使用防止機能」の意味が不明。おそらく特権IDや他者のIDの盗用・成りすましの防止の趣旨と考えられるが、用語が不適切と感じられる。 (4)「退職後の個人情報保護規定」の趣旨が不明。 (5)「端末への資料の保管」の端末が意味するものが曖昧。可搬型PCやタブレット端末が推定されるが、この項目の趣旨と合わせて明確化が必要。 (6)なお、データの破壊・改ざんやシステムの悪用による情報窃取防止には「難読化」も有効であり、対策として追加を検討されることをお勧めする。 (7)電子メールの監視、フィルタリング、アーカイブ等の対策が盛り込まれていない。	(1)(2)(5)(6)ご指摘の内容については、重要インフラにおける情報セキュリティ対策全体の中で、追加・修正等が適当か否か検討する必要があるため、今後の改定時の検討材料とさせていただきます。 (3)ご指摘の内容を踏まえ、「IDの不正使用防止機能」とさせていただきます。 (4)当該対策は、退職後の個人情報漏えいを抑止するための措置を意図したものです。 (7)ご指摘の内容については、18ページの「〇情報漏えいの追跡性確保のための措置」における「・証跡管理」の中に含まれております。
21	18ページ 〇情報漏えいの追跡性確保のための措置	・検知策（不正アクセスの監視機能、不正な取引の検知機能、異例取引の監視機能）の「取引」は「トラフィック」ではないかと思われる。 そのように変更した方がわかりやすい。 （内部不正による情報漏えい対策としては、通信トラフィック監視は欠かせない一方「取引」の監視は余り意味がないと考えられるため。）	当該対策は、内部不正の追跡を行う観点から記載したもので、「取引」の検知・監視が有効であると認識しております。 「通信トラフイックの検知・監視」については、「・証跡管理」の中に含まれております。
22	18ページ 〇情報漏えいの追跡性確保のための措置	「電子メールの監視、フィルタリング、アーカイブ等」を追加 （電子メールの通信を記録しておくことは、情報セキュリティ管理の基本であり、情報漏えい発生時の追跡にも必須の要素である。）	ご指摘の内容については、18ページの「〇情報漏えいの追跡性確保のための措置」における「・証跡管理」の中に含まれております。
23	18ページ 〇情報漏えいの追跡性確保のための措置	「・早期回復対策（障害時の縮退・再構成機能、取引制限機能、リカバリ機能）」の削除 （早期回復対策が情報漏えいの追跡性確保のために有効と考えにくい。）	情報漏えいの追跡性確保のためには、事業継続・早期回復の観点も必要であるため、原文通りとさせていただきます。
24	18ページ 〇取扱いミスを低減させるための措置	情報を格納したPC、外部記憶媒体、携帯端末等の紛失、盗難、置き忘れ等を予防するための措置（教育、ストラップ、専用携帯具等）や、暗号化、いわゆるリモートロック・リモートワイプ等の対策を追記する （紛失、盗難、置き忘れは当協会のインシデント調査でも常に上位を占める情報漏えい要因であるので、その対策を明記することが望ましい。なお、ここでは「取扱いミス」ということで、人為ミスによる脅威の対策に言及しているが、「指針」第3版P5における「安全基準等」の対象とする脅威には、非意図的要因として人為ミスが指摘されていない。これは欠落と思われるので補われることが望ましい。）	ご指摘の内容については、重要インフラにおける情報セキュリティ対策全体の中で、追加が適当か否か検討する必要があるため、今後の改定時の検討材料とさせていただきます。

「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（第3版）対策編」（改定案）に対する
提出意見の概要及びご意見に対する考え方（案）

No.	該当箇所	ご意見の概要	ご意見に対する考え方
25	19ページ 〇外部委託可能な範囲の明確化や委託先の選定基準	外部委託先の選定基準に条件「国（海外発注）」が必要か否か検討していただければ幸いです。 カントリーリスクを懸念する。 例：中国→ソース公開要望。韓国→データセンタ情報漏洩等。 本意見とは別に、運用時のカントリーリスクも懸念する。 例：ネットワーク切断(海底テーブルの銅部分を現地の人が売る)、電力不安定、サービス水準合意の不履行等	ご指摘の内容については、重要インフラにおける情報セキュリティ対策全体の中で、追加が適当か否か検討する必要があるため、今後の改定時の検討材料とさせていただきます。
26	全般的内容	電気、ガス、水道などは、「情報」ではなく、しかもハードウェアで制御されている。従って、これらの事業運営には、情報セキュリティは関係ない。そもそも情報セキュリティが問題になるITは、人間が扱う業務であり、ペンなどで紙に書いたもの（情報）をデジタルデータ化し通信回線を使って遠方とやりとりできるようにしたコンピュータ・システム技術である。電気はボイラーで蒸気を作り、タービンを回し三相交流発電機で電気を作る。そして、変圧器で30万ボルトなどという高電圧にしてパイプラインの送電線で送る。家の近くまで来たら、電柱につけた変圧器で、単相三線式の１００ボルトの電気に変換して、その地域の全家庭へあたかも水道管を配管するように供給される。コンピュータは電気をエネルギーとして動く。コンピュータが動くことでITが働く。このITで、光と同じ速度で動くエネルギーである電気を制御することは論理的に不可能である。だから、スマートグリッド（次世代送電網）は、かけ声だけで一向に進まない。また、インターネットが本格的に使われだしたのは、つい最近のこと。個人会員相手のインターネットビジネスにおいて扱う個人情報が盗まれ、悪用されたのが「情報セキュリティ問題」の始まりである。だから、「情報セキュリティ対策」の殆どは、「個人情報保護」である。なお、テレビ放送について言えば、デジタル化したときに地上波で送る仕組みにしてしまったため、東日本大震災では全く使いものにならなかった。これは、国民の利益という「全体最適」ではなく、一部の利権者を守った「部分最適」でデジタル放送政策を遂行したことが原因である。放送や通信インフラを自然災害に強くするには、静止衛星を使ったシステムにすべきと考える。重要インフラ専門委員会の皆様には、よくよく本質をつかんで国民全体に便益を与える「全体最適」で検討されることを期待する。	制御系システムは、現在、稼働監視やリモートメンテナンス等、情報システムを使用して稼働しており、ネットワークや可搬型デバイス等を通じて外部のシステム機器と接続されるケースが相当数存在するという認識です。なお、承ったご意見については、今後の施策において参考にさせていただきます。
27	全般的内容	ISMSとどこが違うのか不明。 また、IT障害の観点から見た事業継続性確保のための対策については、災害時に救命等生命に関わる事業の継続が必要と定め、そうでない事業は休止しても問題ないと思われることから、事業継続のランク付けを国家として行うべきと考える。	ISMSは、企業などの組織が情報を適切に管理し、機密を守るための包括的な枠組みで、コンピュータシステムのセキュリティ対策だけでなく、情報を扱う際の基本的な方針(セキュリティポリシー)や、それに基づいた具体的な計画、計画の実施・運用、一定期間ごとの方針・計画の見直しまで含めた、トータルなリスクマネジメント体系のことです。 　一方、指針は、情報セキュリティ対策について、重要インフラ分野を横断的に俯瞰して必要度が高いと考えられる項目及び先進的な取組みとして参考とすることを期待する項目を記載し、重要インフラ分野及び重要インフラ事業者等が個々の「安全基準等」を策定または改定する際に検討または参考とするものとして策定しています。 　なお、承ったご意見については、今後の施策において参考とさせていただきます。
28	全般的内容	中国、韓国の製品、企業、関係者を使わないことが、セキュリティを守るために重要であると考えます。 なぜ、この2か国の製品や企業、関係者が危険なのかは、これらは、反日国家であることもありますが、すでに、スパイ製品を取り扱い、出入り禁止となっている国があるという、極めて重大な事実があることです。 また、スパイ防止法の存在しない我が国では、両国のスパイが跋扈しておりますが、犯人の検挙が非常に困難なのではありませんでしょうか。 安いからと言って、これらの国々の製品、会社、人員を使えば、確実にセキュリティホールになるということを、明確にしていただきたく思います。 このような国々とのFTA交渉など、とんでもないと思いますが、それは、別の機会に、具申いたします。	今回の改定において、8ページ「（イ）　電子計算機　【要検討事項】」の「〇設置時」の項に、「・サプライチェーンにおける情報セキュリティを考慮した機器の調達（信頼のできるベンダーから調達する等）」を追加しております。