「政府機関の情報セキュリティ対策のための統一基準(第３版)」(案)に対する提出意見の概要及び御意見に対する考え方

情報セキュリティ政策会議
平成20年２月４日

意見提出者一覧（五十音順）

IPv6普及・高度化推進協議会事務局
大阪国際大学
株式会社アール・アイ
北陸無線データ通信協議会

該当箇所	ご意見の概要	ご意見に対する考え方
5.4.2 府省庁内通信回線の管理(3)(b) 及び全般	無線LANの利用については、混信、暗号解読、通信傍受等の危険性にかんがみ、政府機関における利用を停止すべきである。 利用停止が受け入れられない場合でも、「政府機関の情報セキュリティ対策のための統一基準」について以下の変更を要望する。 (A)「他の無線通信の混信・妨害を定期的に確認すること」を追加する。 (B)「（イ）通信内容の暗号化」については、「（イ）通信内容の解読が困難な暗号化」とする。 (C)第三者による通信傍受を防止するために、「（キ）無線LAN接続方法の機密性の確保」を削除する。 （北陸無線データ通信協議会）	ご意見のとおり無線LANの利用については情報セキュリティに関して固有の事項がありますが、業務上必要な場合には、適切な情報セキュリティ対策を実施した上でその利用を許容すべきものと考えます。 (A)については、(2)(b)に既に記述されている内容であると考えます。 (B)については、暗号化を行う主旨から現状の記述で十分であると判断します。 (C)について、現行の記述「無線LAN接続方法の機密性の確保」は、許可されていない者の利用を防ぐことを求めるものであり、無線LANへの接続に必要な情報を秘匿することまでは求めておりませんので、現状の記述とさせていただきます。
6.2.3　情報システムへのIPv6技術の導入における対策(2)(a)の解説	適切なポート管理を行う方が、セキュリティを高めるという意味では効果的であるため、「（前略）また、ルータ等の通信回線装置についてもIPv6 通信を監視するか、適切なポート管理を行うことで、意図しないIPv6 通信を制限することが求められる。」に修正する。 （IPv6普及・高度化推進協議会事務局）	6.2.3(2)(a)は通信回線でIPv6通信を想定していない通信回線に関する遵守事項です。 したがって、解説では「（前略）IPv6通信をしないよう設定し、（後略）」としており、ご提案のポート管理を含むより広いものと考えており、ます。また、当該回線におけるIPv6通信有無の監視については、6.2.3(2)(b)に基づき行われるものと考えています。
6.2.3　情報システムへのIPv6技術の導入における対策(2)(b)の解説	根本的な対処として、どの端末から通信が行われているかを確認して、状況にあった対処をすることが求められるため、「（前略）府省庁内通信回線を管理する者は、このような通信の有無を監視して、 IPv6 通信が検知された場合は、当該通信の遮断や、端末の特定による対処等の措置を講ずる必要がある。」に修正する。 （IPv6普及・高度化推進協議会事務局）	6.2.3(2)(b)の解説には「（前略）当該通信の遮断等の措置（後略）」であり、「端末の特定」という表現ではありませんが、同項本文に「（前略）通信している装置を特定し、IPv6通信を遮断するための措置（後略）」と記載しており、「装置」に「端末」を含んでいます。
6.3.2　業務継続計画との整合的運用の確保 (2)(c)(イ)の解説	内閣府やその他省庁が発表している災害時の事業継続計画のガイドラインでは、データの保存についてより詳細に明記されているものがある。そこで、「対策として、例えば、情報システムは、運用場所と併せて事態発生時に同時に被災しない複数の遠隔地施設に、リアルタイムまたは最低でも日々バックアップデータを暗号化して保存することが望ましい。また、施設の災害性確保、非常用電源の確保、人手による業務処理や郵送・電話の利用を含む情報システム以外の通信手段の利用等があり、事態発生時の対応体制及び担当者の指名も整備対象となり得る。」に修正する。 （株式会社アール・アイ）	6.3.2(2)(c)は政府機関を対象とした業務継続ガイドラインである内閣府の「中央省庁業務継続ガイドライン」に基づいて府省庁が定めた業務継続計画と整合的運用が可能となるように事態発生時の規定を整備することを求めているものです。そのため、解説では当該規定に含める事項の例を示し、ご提案の具体的な対策の記述は府省庁において本項に基づいて整備される規定に必要に応じて記載される事を想定しています。
その他	政府の電子申請で用いられるJavaに関する脆弱性があるにも係わらずそれを無視するような内容の文章や取り組みを国民に見せてしまった場合、国民が悪い方向に教育されてしまうというような事が懸念される。それを未然に防いだり、万が一そのような事態に陥った場合の政府機関の対応（国民に正しい情報を提供し正しい方向に導くこと)に関する定め等が「政府機関の情報セキュリティ対策のための統一基準」に含まれていないように見える。 また、公開しているPDF文書の閲覧ソフトで表示されるページ番号と、目次に表示されるページ番号が異なっており、ページ番号が一致するように閲覧者の利便性を計っていただくよう要望する。 （大阪国際大学）	6.3.1項で、府省庁外の情報セキュリティ水準の低下を招く行為の防止を全般的に求めています。例えばJavaに関する脆弱性があった場合の対処は本項に基づく対策に該当し、ご指摘の点については6.3.1(1)(a)の解説に記載しています。 「政府機関の情報セキュリティ対策のための統一基準」においては特定の技術に固有の表現にならないようにしていますが、「政府機関の情報セキュリティ対策のための統一基準」に基づいて定められる各府省庁基準にて整備する対策手順書などでは、ご指摘の事項についても具体的に対策を講じることとなります。 また、PDFのページ番号のご指摘については、今後の文書の作成の参考にさせていただきます。
－	特定個人の活動に関するご意見 （北陸無線データ通信協議会）	今回の「政府機関の情報セキュリティ対策のための統一基準」改訂に関係しない意見と考えています。