「政府機関の情報セキュリティ対策のための統一基準（第２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（案）

情報セキュリティ政策会議
平成19年６月〇日

意見提出者一覧（五十音順）

沖電気工業株式会社
オリエント測器コンピュータ株式会社
タイムビジネス協議会
日本ユニシス株式会社
株式会社日立製作所
マイクロソフト株式会社

その他個人２件

該当箇所	ご意見の概要	ご意見に対する考え方
2.3.1 情報セキュリティ対策の自己点検 (2)(3)(4)	自己点検報告の信頼性が保証されることが不可欠であるため、自己点検実施の準備、同実施、同評価に当たっては、自己点検報告が実態を反映するような仕組みが必要である。 (日本ユニシス株式会社)	自己点検の信頼性については監査によって担保されることになります。今般の改訂において、このことを2.3.2(5)(d)で明確化しています。
2.3.2 情報セキュリティ対策の監査	(1)監査計画の策定～(6)情報セキュリティ結果に対する対応について記載されているが、監査対応実施後のフォローアップ監査についても記載する。 (日本ユニシス株式会社)	ご意見の趣旨については、政府機関統一基準解説書2.3.2(1)(a)の解説部分に記載されており、府省庁において必要性を適宜判断して追加の監査等を実施することになります。
3.2.6 情報の消去 (1)(a)	行政事務従事者は電磁的記録媒体を廃棄する場合には、データ抹消ソフトウェア又は消磁装置を使用してすべての情報を復元困難な状態にする（以下、「抹消する」という。）こと。」に修正する。 （オリエント測器コンピュータ株式会社）	抹消方法については、消磁装置の利用を含め政府機関統一基準解説書の解説部分に例示しており、府省庁が適切なものを選択することになります。
3.2.6 情報の消去 (1)(c)	「行政事務従事者は、電磁的記録媒体について、設置環境等から必要があると認められる場合には、当該電磁的媒体の要機密情報を消磁装置にて抹消した後、物理的破壊を実施すること。」に修正する。 （オリエント測器コンピュータ株式会社）	抹消方法については、消磁装置の利用を含め政府機関統一基準解説書の解説部分に例示しており、府省庁が適切なものを選択することになります。
4.1.6 暗号化と電子署名(鍵管理を含む) (2)(g)	「選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装する」に当たり、暗号モジュール内において、複数の暗号アルゴリズムを実装可能とし、選択したアルゴリズムが危殆化した場合、速やかに別の暗号アルゴリズムに変更できることが望ましい。 （株式会社 日立製作所）	ご意見の趣旨については、4.1.6(2)(e)、同(f)で担保されています。
4.1.6 暗号化と電子署名(鍵管理を含む) (1)(b)	「電子署名の実装方式を選択するに当たっては、署名対象文書の保存期間に留意し、必要な期間、電子署名の検証を可能とする標準技術を用いること。」の追記する。 （タイムビジネス協議会）	ご指摘の内容については、政府機関統一基準解説書への反映を含め、今後の施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。
4.1.6 暗号化と電子署名(鍵管理を含む) (3)(a)	「 情報システムセキュリティ責任者は、電子署名の付与を行う必要があると認めた情報システムにおいて、電子署名の正当性を検証するための情報又は手段を必要な期間、署名検証者へ提供すること。」に修正する。 （タイムビジネス協議会）	ご指摘の内容については、政府機関統一基準解説書への反映を含め、今後の施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。
4.3.1 情報システムのセキュリティ要件 (5)(b)	台帳を整備すべき対象である「すべての情報システム」が個々のパソコンという想定でないのであれば、そのことを明確してはいかがか。 (個人)	ご指摘の内容については、政府機関統一基準解説書への反映を含め、今後の施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。
5.2.2 端末 (2)(e) 5.2.3 サーバ装置 (2)(e) 5.4.1 通信回線共通対策(2)(j)	「情報システムにおいて基準となる日本標準時刻に、（端末／サーバ装置／通信回線）の時刻を同期すること。」に修正する。 （タイムビジネス協議会）	ご意見の趣旨については、政府機関統一基準解説書5.2.2(2)(e)、5.2.3(2)(e)、5.4.1(2)(j)の解説部分にそれぞれ記載されております。
5.4.2 府省庁内通信回線の管理 (3)(b)	強化遵守事項として、以下を追加する。 ①管理されている電子計算機以外の電子計算機の無線LANへの接続禁止 ②無線LANに接続するためのアクセスポイントの管理 ③管理されている無線LANのアクセスポイント以外のアクセスポイントの検知 （沖電気工業株式会社）	①については、5.4.1(2)(h)及び5.4.2(3)(b)(ｳ)、②については、通信回線装置の管理として5.4.1等、③については、5.4.1(2)(f)で、それぞれ担保されています。

該当箇所	ご意見の概要	ご意見に対する考え方
6.2.3 情報システムへのIPv6技術の導入における対策 (1)	IPv6を標準的に利用することでIP層での暗号化通信など、セキュリティの向上が図られる点について触れられていない。逆に、IPv6移行が脆弱性をもたらすかのような記述と受け取られる懸念がある。 このため、(a)にIPv6への移行を推進しIP層での暗号化通信などセキュリティの向上を図ることを、(b)に「情報システムセキュリティ責任者は、情報システムにIPv6技術を利用する通信機能を導入する場合には、当該移行組織が他の情報システムに通信上の問題が及ぼすことを防止するために必要な措置を講ずるべきである。」と記載する。 （マイクロソフト株式会社）	6.2.3(1)は、IPv6への移行やIPv6技術の導入の判断を求める対策事項ではなく、情報システムにIPv6を実際に導入することを判断した場合に、他の情報システムに情報セキュリティ上の脅威を及ぼさないよう、OSや機器等において正しい設定が行われるなど、適切な安全管理措置等を求めるものであるため、原案のとおりとします。
全体	電子メールにおけるセキュリティ対策について、 暗号化や認証を用いたメールシステム（アプリケーション）の利用や転送・印刷・コピー&ペースト・スクリーンショット取得の禁止等のセキュリティ機能についても記載する。参照可能な期限の設定等も有効な手段であり、必要に応じて設定することを推奨する。 （マイクロソフト株式会社）	ご指摘の内容については、今後の施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。
その他	機密性１情報について、改訂案では、「機密性２情報、機密性３情報以外」という書かれ方でブラックリスト的に書かれており、このことが、パブリックコメントの意見提出者の個人情報公開という間違った方向を助けている。機密性１情報の定義は、ブラックリスト方式ではなく、ホワイトリストとして定義するのが適切で、その際、「行政機関等個人情報保護法」と矛盾のないようにする。 (個人)	ご指摘の内容については、今後の施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。