資料３－３

「政府機関の情報セキュリティ対策のための統一基準（第４版）（案）」に対する意見提出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21年２月３日

意見提出者一覧（五十音順）

株式会社ラック
社団法人情報処理学会
データベース・セキュリティ・コンソーシアム
トレンドマイクロ株式会社
日本ネットワークセキュリティ協会
日本ユニシス株式会社
富士通株式会社
三菱電機プラントエンジニアリング株式会社

その他個人3件

	該当箇所	ご意見の概要	ご意見に対する考え方
1	1.1.1.2(6)評価の方法　及び　1.2.3評価	対策が正しく実施できているかの評価について、自己申告のレベルでは足りない分野があるのではないか。情報セキュリティ監査などを利用して、より詳細な評価を行うとともに、これらの報告書そのものを評価する機構を設置する必要がある。 内容がセキュリティであることから国民への内容公開は極めて難しいと考えられるが、CIO補佐官の連絡会議のように情報共有や一部共有できる情報の公開などをしていただけると、信頼感が高まるのではないかと考えるため、検討していただきたい。情報セキュリティ白書のようなサマリー文書が公開されるとよいと考える。 （日本ネットワークセキュリティ協会）	「政府機関の情報セキュリティ対策のための統一基準」（以下、「政府機関統一基準」という。）では、各省庁が1.2.3.1の自己点検を実施した後、1.2.3.2の監査を実施した上で、それを1.1.1.2(6)によりNISCが検査、評価してから情報セキュリティ政策会議に報告しています。この仕組みの中で、自己申告のレベルで不十分となる点については省庁自身が監査し、さらにNISCが検査、評価しています。 今後、第２次情報セキュリティ基本計画に基づき策定する情報セキュリティ報告書の評価方法を検討する際に、ご意見を参考にさせていただきます。
2	1.2.1.1　組織・体制の整備	1-2-1-1 (8)に最高情報セキュリティアドバイザーの設置とあるが、これにあたる人材像はどのように想定しているか。第2次情報セキュリティ基本計画においては人材の見える化ということでスキルセットを定義することになっている。統一基準においても、この点を重視して、スキルセットなどを明確にする必要があるのではないか。 また、最高情報セキュリティアドバイザーの命を受けて実際に計画や対策の実施、監査などを行う人材についても同様にスキルセットを明確にしていく必要があると考える。これらをもとに民間においても情報セキュリティ関連の人材像やキャリアパスなどを設定できると期待している。 （日本ネットワークセキュリティ協会）	1.2.1.1(8)(b)において、最高情報セキュリティ責任者は、最高情報セキュリティアドバイザーが行う業務の内容について定めることとしており、同項解説において、業務内容の例示がされています。御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
3	1.2.1.2役割の割当て(1)(a)（ア）	1.2.1.2 (1)(a)(ア)では、「承認又は許可事案の申請者とその承認権限者又は許可権限者（以下、「承認権限者等」という。）」とある。ここでいう「許可権限者」は、後ろの「1.2.1.3 違反と例外措置(2)(a)」で初めて定義されています。また、承認権限者がどこにも定義されていません。承認権限者と許可権限者の明確な定義を記載していただきたい。 （日本ユニシス株式会社）	御指摘を踏まえ、以下のとおり２点修正いたします。 ・1.2.1.2(1)(a)(ア) 「承認又は許可事案の申請者とその承認又は許可を行う者（以下、本項において「承認権限者等」という。）」 なお、1.2.1.2(1)(a)(ア)の承認権限者及び許可権限者はいずれも、承認事案の承認をする権限者及び許可事案の許可をする権限者の意味であり、特定の業務を対象とする権限者ではありません。 ・1.2.1.3(2)(a) 「～例外措置の適用の申請を審査する者（以下、本項において「許可権限者等」という。）」
4	1.2.1.2役割の割当て(2)(a)	「承認権限者等が有する職務上の権限等から、当該承認権限者等が承認又は許可の可否の判断を行うことが不適切と認められる場合」とは、具体的にどのような場合なのか記載していただきたい。また、「上司が許可権限者の役割を代わりに果たす。」というような記述を追加し、「1.2.1.3 違反と例外措置(2)(a)について」の(c)や (e) で定義されている許可権限者が守るべき基本遵守事項が、そのような場合にも間違いなく守られるようにしていただきたい。 （日本ユニシス株式会社）	政府機関統一基準において、事務に係る承認等の多くは課室情報セキュリティ責任者から承認等を得ることとして定めています。課室情報セキュリティ責任者よりも上位の管理職についても同様としています。しかし、上位の管理職が取り扱う情報や情報システムの種類によっては、それよりも下位となる課室情報セキュリティ責任者から承認等を得ることが不適切である場合があると考えています。そのような場合には、課室情報セキュリティ責任者の上司から承認等を得ることを求める記述です。 このとき代行者が、代行処理に係る対策を遵守することについては、1.2.1.2(2)(b)に規定しています。
5	1.2.1.1組織・体制の整備(6)(c)	意見 情報システムセキュリティ責任者からの報告は、統括情報セキュリティ責任者だけでなく、情報セキュリティ責任者にも報告するように記載していただきたい。 理由 情報システムセキュリティ責任者の設置は、情報セキュリティ責任者の役割となっていることから、統括情報セキュリティ責任者への報告だけでは十分ではないと考えます。 （日本ユニシス株式会社）	政府機関統一基準では、1.2.1.1については、統括情報セキュリティ責任者に報告を集約するようにしています。 なお、情報セキュリティ責任者にも同時に報告する、又は情報セキュリティ責任者を介して統括情報セキュリティ責任者に報告をするという形態も有り得ると考えております。
6	1.2.5.1 外部委託 (4)(e)	再請負を許可する場合の条件として明示、または例示が必要と考える。 （株式会社ラック）	再請負については、御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
7	1.3.1.4 情報の移送 &1.3.1.5 情報の提供	府省庁内部での複製、配布でも責任者の許可、記録が必要と考える。 （株式会社ラック）	1.3.1.2(5)(c)(d)(f)において、要機密情報の複製、配布、保存等について規定するとともに、「複製要許可」「配布要許可」や「複製要記録」などの取扱制限を指定することも想定しています。
8	1.5 情報システムについての基本的な対策	情報システムの導入などについて、米国ではSCAPやFDCCなどの規格に基づき、詳細まで要件が決定されておりセキュリティの水準が明確になっている。しかしながら、国内においてはこれらが明確にされている文書がなく、各省庁の自由裁量となっているのではないかと懸念される。統一基準に具体的な要件を書くのは難しいと思うが、水準となる情報システム要件などについてどこかで明確にする必要があると考える。これらについて統一基準の中に盛り込んでいただきたい。さらにそれが調達基準として活用されるとよい。また、検討においては民間をうまく利用して最新技術などを盛り込んでいただけるとなお良いと考える。 （日本ネットワークセキュリティ協会）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。

	該当箇所	ご意見の概要	ご意見に対する考え方
9	1.5.1.1　情報システムのセキュリティ要件(1)(e)	意見 解説を下記のとおり修正 「監視機能の例・ウイルス感染や踏み台に利用されること等による府省庁「内」外への不正な通信を監視する機能」 理由 外部からの不正通信だけではなく、内部から外部に出る通信、および内部間を行き交う不正通信を監視することで被害の最小化を図る。また、内部の端末を特定しやすいため、事故発生時の原因究明時間が最小化される。特に新たな不正プログラムについて従来方式に比して効果的と考えられるため。 （個人）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
10	1.5.1.1 情報システムのセキュリティ要件（4）	情報システムのセキュリティ対策を見直す対象として、新たに計画されるシステム以外に、過去に構築したシステムを対象とする必要があると考える。 （株式会社ラック）	過去に構築したシステムであっても、対策を行うことが必要であると認識しており、対策が現在未導入である場合は、各省庁において例外措置の適用を行うことにより代替策を含め検討することとしております。
11	1.5.2.1 情報システムの文書整備	情報システムの文書は、定期的に見直しを行うことを明記する必要があると考える。 （株式会社ラック）	御指摘の点については、1.5.2.1以外の文書等についても見直すことが求められると考えています。作成され見直しされ適宜更新することについて、整備するという表現をしています。 また、1.5.2.1(1)(a)の解説では「所管する情報システムに変更があった場合、また想定しているリスクが時間の経過により変化した場合等、整備した文書の見直しが必要になる。」としています。
12	1.5.2.3 ソフトウェア開発	案にあるような規定は2008年において大きな問題になっているソフトウェア脆弱性問題を解決する上で重要と考えます、しかし、案にあるような規定を定めるだけでは、開発における脅威や脆弱性の排除の実効性としては十分ではなく、セキュリティに特化した開発規定項目の具体化が必要ではないでしょうか。 （富士通株式会社）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
13	1.5.2.3　ソフトウェア開発	（ク）データに関する記述 上記にも関連しますが，「データのセキュリティ」という視点だけでセキュリティをカバーするのが難しくなっています．「データベース」の視点も含めて言及すべきではないでしょうか． （富士通株式会社）	当該遵守事項において、「データベース」についても、データのセキュリティとして注意すべき対策に含まれると考えています。御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
14	1.5.2.7不正プログラム感染防止のための日常的実施事項(1)(a)	当該項目の追加 （キ）行政事務従事者は、アンチウイルスソフトウエアでは検知不能な不正プログラムの侵入を想定し、必要な対策に努めること。 （ク）行政事務従事者は、アンチウイルスソフトウェア等により不正プログラムをダウンロードさせるサイトとして検知されたWebサイトへアクセスした場合は、当該電子計算機の接続を速やかに中止し、不正プログラムの有無を確認すること。また、当該Webサイトに関して情報セキュリティ責任者へ報告を行うこと。 （トレンドマイクロ株式会社）	・（キ）の追加について 御指摘を踏まえ、以下のとおり修正いたします。 1.5.2.7(1)(a) (カ）行政事務従者は、不正プログラム感染の予防に努めること。 解説：不正プログラム感染の予防に役立つ措置の実施を求める事項である。アンチウイルスソフトウェア等がすべての不正プログラムを検知できるとは限らないことに注意して、例えば、アプリケーションでマクロの自動実行を無効にすることによりマクロウイルスの実行を防ぐことや、ソフトウェアのセキュリティ設定により読み込まれるプログラムやスクリプトの実行を無効にすること、安全性が確実ではないプログラムをダウンロードしたり実行したりしないことなどがある。 ・（ク）の追加について 御指摘を踏まえ、以下のとおり修正いたします。 1.5.2.7(1)(a) (キ）行政事務従事者は、不正プログラムに感染した恐れのある場合には、感染した電子計算機の通信回線への接続を速やかに切断し、必要な措置を講じること。 解説：不正プログラムに感染した恐れがある電子計算機については、他の電子計算機への感染などの被害の拡大を防ぐために、当該電子計算機が通信回線に接続している場合には、それを切断して、必要な措置を講じることを求める事項である。切断後に必要となる措置としては、例えば、不正プログラムの有無を検知して駆除することや、「1.2.2.2 障害・事故等の対処」に定められた連絡等をすることがあげられる。
15	1.5.2.7不正プログラム感染防止のための日常的実施事項(1)(a)（ア）	「アンチウイルスソフトウェア等がすべての現存する不正プログラムを検知できるとは限らないことに留意し、あわせて必要な予防措置を行う。」と修正。 （トレンドマイクロ株式会社）	御指摘を踏まえ、以下のとおり修正いたします。 1.5.2.7(1)(a) (カ）行政事務従者は、不正プログラム感染の予防に努めること。 解説：不正プログラム感染の予防に役立つ措置の実施を求める事項である。アンチウイルスソフトウェア等がすべての不正プログラムを検知できるとは限らないことに注意して、例えば、アプリケーションでマクロの自動実行を無効にすることによりマクロウイルスの実行を防ぐことや、ソフトウェアのセキュリティ設定により読み込まれるプログラムやスクリプトの実行を無効にすること、安全性が確実ではないプログラムをダウンロードしたり実行したりしないことなどがある。

	該当箇所	ご意見の概要	ご意見に対する考え方
16	1.5.2.7 不正プログラム感染防止のための日常的実施事項 (1)(a)(ア)	意見 「不審なプログラムファイル（実行ファイル）は、不必要に実行しない、開かない」と明記する必要があると考える。 理由 「アンチウイルスソフトウェア等により不正プログラムとして検知された実行ファイルを実行せず、～」とあるが、アンチウイルスソフトでも検知できない不正プログラムを電子メールで受信する場合も考えられる。アンチウイルスソフトウェアのみを信頼せず「不必要に実行しない、開かないよう」にするのが良いのではないか。（解説版を見ると留意されているようであるが、本文にも明記したほうが良い）。 （株式会社ラック）	御指摘を踏まえ検討した結果、解説をより具体的に追記しました。以下のとおり修正いたします。 1.5.2.7(1)(a) (カ) 行政事務従事者は、不正プログラム感染の予防に努めること。 解説：不正プログラム感染の予防に役立つ措置の実施を求める事項である。アンチウイルスソフトウェア等がすべての不正プログラムを検知できるとは限らないことに注意して、例えば、アプリケーションでマクロの自動実行を無効にすることによりマクロウイルスの実行を防ぐことや、ソフトウェアのセキュリティ設定により読み込まれるプログラムやスクリプトの実行を無効にすること、安全性が確実ではないプログラムをダウンロードしたり実行したりしないことなどがある。
17	2.1.1 情報セキュリティについての機能	機密性、完全性、可用性についての取り組みは理解できるものが多く、引き続き推進していただきたい。ただし、もう少し具体的な内容として、権限における認証についても特化して記述することはできないか。政府だけではなく、民間においてもどのような認証システムを取り入れるかの方針などを示していただきたい。また、認証基盤の構築についても官民連携で実施していただきたい。 （日本ネットワークセキュリティ協会）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
18	2.1.1.1 主体認証機能(2)識別コードの管理 (3)主体認証情報の管理	意見 開発環境、テスト環境の情報システムで利用した識別コード、主体認証情報を利用しないようにすることを明示する必要があると考える。 理由 本番環境でもテスト環境と同様の設定を利用した場合、開発者もしくはその関係者による不正アクセスが行える可能性があるため。 （株式会社ラック）	御指摘を踏まえ、以下のとおり修正いたします。 1.5.2.3(1)(a)(エ)解説 「運用中の情報システムを利用してソフトウェアの作成及び試験を行うことにより、運用中の情報システムに悪影響が及ぶことを回避することを求める事項である。これは運用中の情報システム全体ではなく一部だけの場合も同様である。例えば、開発中のソフトウェアの動作確認のために、運用中の情報システムの要機密情報をテストデータとして、試験を行う情報システムにおいて使用しないようにすること等も含まれる。」
19	2.1.2.2 不正プログラム対策(1)	項目追加 (e) 情報システムセキュリティ責任者は、当該電子計算機で動作可能なアンチウイルスソフト等が存在しない場合は、少なくとも同電子計算機に接続する通信回線において不正プログラムを検知する仕組みを設置すること。 （トレンドマイクロ株式会社）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
20	2.1.2.2 不正プログラム対策(1)(c)	「情報システム～異なる業者のアンチウイルスソフトウェア等を組み合わせ、導入すること。」を「情報システム～複数の製品や技術のアンチウイルスソフトウェア等を組み合わせ、導入すること。」という内容に修正。 （トレンドマイクロ株式会社）	御指摘を踏まえ、以下のとおり修正いたします。 2.1.2.2(1)(c) (c) 情報システムセキュリティ責任者は、想定される不正プログラムの感染経路において、複数の種類のアンチウイルスソフトウェア等を組み合わせ、導入すること。 解説：複数の種類のアンチウイルスソフトウェア等を導入することにより～　（中略）～感染経路において異なる製品や技術を組み合わせ、～
21	2.1.2.2 不正プログラム対策(2)	項目追加 (c) 情報システムセキュリティ責任者は、府省庁内の不正プログラムの感染状況を把握するための手段を講じ、記録や予見を行い、その見直しを行うこと。また定期的に確認・報告を行える手段・体制を構築する。 （トレンドマイクロ株式会社）	2.1.2.2(2)(b)において、対策状況の把握と見直しについて規定しております。御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
22	2.1.2.2 不正プログラム対策(2)(a)	情報システムセキュリティ管理者は、不正プログラムに関する情報を不正プログラム対策の専門家との直接窓口から、情報の収集に努め当該情報について対処の要否を決定し、特段の対処が必要な場合には、行政事務従事者にその対処の実施に関する指示を行うこと。 （トレンドマイクロ株式会社）	2.1.2.2(2)(a)に記載の「不正プログラムに関する情報の収集に努め」とは、御指摘にあるような不正プログラム対策の専門家から情報収集する場合も含めた表現として考えております。
23	2.2.2.3　サーバ装置（1）(c)	意見 サーバアプリケーション導入時に標準で設定されている設定値をそのまま利用しないこと（デフォルト設定値の排除）を明記する必要があると考える。 理由 ソフトウエアをデフォルト設定値のまま運用することは、製品を精通した攻撃者に対して脆弱であるため。 （株式会社ラック）	御指摘を踏まえ、以下のとおり修正いたします。 2.2.2.3(1)(c)解説 「不要なサーバアプリケーションの停止及び不要な機能の無効化により、サーバ装置から潜在的な脅威を排除するための事項である。なお、ソフトウェアの設定は初期状態が安全であるとは限らないことについても留意して確認すること。」
24	2.2.3 アプリケーションソフトウェア	2.2.3.4節として、要保護情報が格納されるデータベース管理システムに関する対策を追記することを提案します。対策内容の例としては、私どもが無償で公開しているデータベースセキュリティガイドラインが参考になれば幸いです。 (データベース・セキュリティ・コンソーシアム)	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。

	該当箇所	ご意見の概要	ご意見に対する考え方
25	2.2.3 アプリケーションソフトウェア	意見 2.2.3.4節として要保護情報が格納される、データベース管理システムを追加する必要があると考える。 理由 データベース管理システムは、要保護情報を保管するため情報システムの一部として利用されることが多い。例えばSQLインジェクションの脆弱性があるウエブシステムが攻撃された場合、データベースのセキュリティ設定、運用状態によっては被害が拡大することが懸念される。対策内容の例としては、データベース・セキュリティ・コンソーシアムで公開しているデータベースセキュリティガイドラインが参考になる。 （株式会社ラック）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
26	2.2.3.2　ウェブ(2)	意見 項目の追加 （e）改ざんされたホームページを閲覧すること等で発生する、リダイレクトや不正プログラムのダウンロードを防止すること。 理由 不正な目的に利用されるWebサイトへのアクセスを未然に防ぐ必要があります。そこでリアルタイムに更新される全世界のWebサイト情報を利用して、信頼性の低いWebサイトへのアクセスをブロックするなど、Web閲覧にもURLフィルタリングとは異なる対策が必要です。 （トレンドマイクロ株式会社）	2.2.3.2(2)(a)(d)において、ウェブクライアントのセキュリティ設定、及びホームページの閲覧制限について規定しております。御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
27	2.2.3.2 ウェブ（2）	意見 アクセスログを定期的に分析することを強化遵守事項に明記する必要があると考える。 理由 昨今多く発生しているWebアプリケーションの脆弱性を利用した攻撃に備えるため。 （株式会社ラック）	御指摘を踏まえ、以下のとおり修正いたします。 2.2.3.3(2)(e)解説 「～監視の方法としては、アクセスログを定期的に確認することや、侵入検知システム、アンチウイルスソフト又はファイル完全性チェックツール等を利用することができる。」
28	その他	民間企業が活発に情報セキュリティの第三者認証及び格付けの対応を進めるためにも、政府機関が自ら率先してこれらの認証取得や格付け取得などを目指すことを提案します。 （三菱電機プラントエンジニアリング株式会社）	政府機関において認証を取得するには、まず認証機関の準備が必要と考えております。御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
29	-	政府機関統一基準外についてのご意見 （他事振込防止システムの留意点について） （個人）	ご指摘の点については、今回の政府機関統一基準のパブリックコメントの対象ではありませんが、今後の参考とさせていただきます。
30	-	政府機関統一基準の必要性に疑問がある。 （個人）	政府機関における情報セキュリティ確保のために政府機関統一基準は必要であると考えております。
31	-	用語や技術について、ここで統一したものがその後民間などで広く引用される可能性もあるので、統一する用語などについてはより一般的にするか、省庁間での利用を前提としたものであるかが明示的にすることが望まれる。 例えば、「複数要素主体認証（p. 9）」や「不正プログラム定義ファイル(p.10)」はあまり一般的でなく、「マルチモーダル利用者認証」や「シグネチャー」と一般には呼ばれることが多い（変更が必要という意味ではない）。 （社団法人情報処理学会）	政府機関統一基準は原則として政府機関で使用することを想定しています。御意見については、今後の政策の推進に当たっての参考とさせていただきます。
32	-	基本遵守事項の実施状況について 基本遵守事項は必須として実施すべき対策事項として定義されているが、その実施の実情が不十分・不適切なケースはないか。また、適用対象となったものの設計開発結果を、事後に第三者が評価し、基本遵守事項として求められている事項の実現が適切であったかどうかを評価し、どのくらいこの統一基準が実効性のあるものになっているか、実施状況を把握する必要がある。 （社団法人情報処理学会）	今後、第２次情報セキュリティ基本計画に基づき策定する情報セキュリティ報告書の評価方法を検討する際に、ご意見を参考にさせていただきます。
33	-	対策導出の根拠について 本基準は、具体策のカタログとしてまとまっていて一定の有用性があり、民間でも援用しようとする動きがある。しかし、その導出根拠が明示されていないため、個別状況への適用是非を判断できない。可能であれば、対策導出の経緯や根拠の開示が望まれる。 （社団法人情報処理学会）	政府機関統一基準は原則として政府機関で使用することを想定しています。御意見については、今後の政策の推進に当たっての参考とさせていただきます。 なお、御意見に直接関係するものではありませんが、政府機関統一基準を政府機関以外で利用していただく場合の紹介資料をウェブで公表していますので参考にしてください。 http://www.nisc.go.jp/isd/2007/isd_material.html （現時点で公表している資料は第３版以前についての紹介となります。）