NISC National Information Security Center

「政府機関の情報セキュリティ対策のための統一基準群」平成24年度版（案）の概要

2012年3月

内閣官房情報セキュリティセンター

Ⅰ. 政府機関統一基準群　平成24年度版（案）のポイント

1. 標的型攻撃への対応	• 情報システムの構築・運用段階での標的型攻撃対策、被害の拡大防止措置を求める。 • 適切な管理者権限管理のための規定を追記。 • 各府省庁に組織内CSIRTの体制整備を求める。
2. 東日本大震災の教訓の反映	• 各府省庁におけるIT-BCPの策定と省庁基準への反映を求める。
3. 運用の実効性の向上	• 調達の際のセキュリティ要件の決定にSBDマニュアルの活用を明文化。 • 「基本遵守事項」と「強化遵守事項」の区分を廃止して、「遵守事項」に一本化。
4. NISCの役割の明確化	• NISCは、各府省の障害・事故等への対応の中核となることを明記。
5. 情報技術、利用環境の変化への対応	• 複数府省庁で共通的に使用する基盤となる情報システムについての情報セキュリティ対策の進め方を記載。 • 「情報取扱区域」の概念を新たに定め、クラス別の物理空間の管理を行う。 • IPv6技術の利用のための対策を追加。 • スマートフォン、タブレット端末を含む「モバイル端末」を定義。

Ⅱ. 政府機関統一基準群　平成24年度版(案)の概要

1. 標的型攻撃への対応

○標的型攻撃への対応

経緯

・昨今の政府機関等を対象とした標的型攻撃の増加への対応として、標的型攻撃対策や被害の拡大防止措置、適切な管理者権限の管理、組織内CSIRT体制整備等の規定を明記。

改定案

■標的型攻撃対策、被害の拡大防止措置の実施

・標的型攻撃対策に関する節を設け、侵入及び感染拡大防止に関する遵守事項を追加。

■適切な管理者権限の管理

・複数の識別コードを付与されている場合に共通の主体認証情報を用いないこと等、適切な管理者権限の管理を行うための規定を追加。

■障害・事故等発生時の体制整備

・障害・事故等の発生時における体制や他の組織との情報共有に関する規定を追加。

2. 東日本大震災の教訓の反映

○東日本大震災を踏まえた情報システム運用継続計画(IT-BCP)に係る見直し

経緯

・NISCが平成23年3月に策定した「情報システム運用継続計画(IT-BCP)ガイドライン」に基づき、各府省庁のIT-BCPの策定及び省庁対策基準への反映を求めるとともに、東日本大震災によって明らかとなった脅威等を踏まえ、大規模災害時の情報システム運用継続のために行うべき対策を追加。

改定案

■省庁対策基準と情報システム運用継続計画の整合的運用の確保

・平成23年3月にNISCが策定した「情報システム運用継続ガイドライン」に基づく各府省庁の情報システム運用継続計画と省庁対策基準の、整合的運用の確保のための検討を行う。

■東日本大震災を踏まえた大規模災害時の情報システム運用継続のための対策を追加

・東日本大震災によって明らかとなった脅威及び被害状況調査分析等を踏まえて、行うべき対策を追加。

3. 運用の実効性の向上

○SBDマニュアルの活用の推進

経緯

・NISCが平成23年3月に策定した「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(SBDマニュアル)に基づき、システムの企画段階からのセキュリティ要件策定による適切な情報セキュリティ対策を講じるため、各府省庁におけるSBDマニュアルの活用を推進。

改定案

■情報システムのセキュリティ要件策定に係るSBDの活用

・情報システムのセキュリティ要件を決定するにあたっては、「SBDマニュアルの活用又はそれと同等以上の検討を行った上でセキュリティ要件を決定する」こととする。

○「強化遵守事項」「基本遵守事項」の枠組みに関する見直し

経緯

・これまでの統一基準上の「基本遵守事項」「強化遵守事項」の区分を廃止し、今後は各府省庁が省庁対策基準において全ての遵守事項を採ることで、自己点検による確認を図り、全ての遵守事項の必要性の有無に関する検討を、確実に行うこととする。

改定案

■「基本遵守事項」と「強化遵守事項」の区分を廃止し、「遵守事項」へ統合。

・「基本遵守事項」と「強化遵守事項」の区分を廃止し、全ての項目を「遵守事項」とする。

4. NISCの役割の明確化

○NISCの役割の明確化

経緯

・標的型攻撃増加への対策として、各府省庁における障害・事故等の発生に備えた体制の整備や、情報共有による被害拡大防止の必要性が増加していることから、障害・事故等発生時のNISCの役割を明確化。

改定案

■障害・事故等発生時のNISCの役割を規定

・NISCは、各府省庁の障害・事故等への対応の中核となる機関として、各府省庁への技術的な支援及び助言を行うとともに、各府省庁間の情報共有の結節点として、各府省庁間の連携・調整を行う。各府省庁は、障害・事故等が発生又はそのおそれがある場合には、NISC及び府省庁内外の関係部門との情報共有により、被害の拡大防止及び再発防止を図る。

5．情報技術、利用環境の変化への対応

○複数の府省庁で共通的に使用する基盤となる情報システムに係る規定

経緯

・複数の府省庁で共通的に使用する情報システムの導入の増加が見込まれることを踏まえて、複数の府省庁で共通的に使用する基盤となる情報システムにおける情報セキュリティ対策の進め方を規定。

改定案

■複数の府省庁で共通的に使用する基盤となる情報システムの情報セキュリティ対策の進め方

・運用指針において、各府省庁の責任と役割分担の在り方の検討、責任分界や平常時・非常時の協力体制の整理、適切な情報セキュリティマネジメント等の規定を追加。

○安全区域の考え方の見直し（「情報取扱区域」の規定）

経緯

・従来の「安全区域」の考え方を見直し、「区域情報セキュリティ責任者」を設置し、各府省庁で情報を取り扱う区域（情報取扱区域）のクラス区分を定め、クラスに応じて適切な物理的セキュリティ対策を取ることとする。

改定案

■各府省庁における「区域情報セキュリティ責任者」の設置、情報取扱区域のクラス区分・対策の決定

・各府省庁は、「区域情報セキュリティ責任者」を設置するとともに、情報取扱区域のクラス区分並びにクラスに応じた管理及び利用制限に関する対策を決定し、実施するものとする。

5. 情報技術、利用環境の変化への対応

○IPv6移行に係るセキュリティ対応

経緯

・今後の政府機関の情報システムのIPv6移行を踏まえ、IPv6アドレスへの移行に係るセキュリティ対策の内容を追加。

改定案

■情報システムへのIPv6技術の導入におけるセキュリティ対策の追加

・準拠製品の導入やフィルタリング機能の適切な設定等、IPv6技術の導入に伴うセキュリティ対策を追加。

○スマートフォン・無線LAN等の利用の増加に係る対応

経緯

・政府機関等におけるスマートフォンやタブレット端末、無線LAN等の今後の利用増加が見込まれることを踏まえ、スマートフォン、タブレット端末に係る定義の追加、無線LAN等に係るセキュリティ対策を追加。

改定案

■無線LANに関するセキュリティ対策の解説の追加

・従来の無線LANの構築時の遵守事項につき、対策内容に係る解説を追加。

■スマートフォン、タブレット端末に関する定義の追加

・統一基準上の「モバイルPC」の定義を、スマートフォン、タブレット端末を含むものとなるよう、「モバイル端末」と修正。(スマートフォン・タブレット端末等の利用に係るマニュアルを、別途作成予定。)