参考文献

2010/7/30現在

指針対策編項目	参考文献	その他参考文献等
Ⅱ　対策項目の具体化の例示		
（1）4つの柱		
ア　組織・体制及び資源の確保		【情報セキュリティガバナンス導入ガイダンス】
（ア）組織・体制及び人的資源の確保	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 5 セキュリティ基本方針 A. 5. 1 情報セキュリティ基本方針 A. 6　情報セキュリティのための対策 A. 6. 1 内部組織 A. 8　人的資源のセキュリティ A. 8. 1 雇用前 A. 8. 2 雇用中 A. 8. 3 雇用の終了又は変更 【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）】 第1. 2部 組織と体制の整備 1. 2. 1　導入 1. 2. 2. 1 情報セキュリティ対策の教育 1. 2. 2. 2 障害・事故等の対処 1. 2. 3. 1 情報セキュリティ対策の自己点検 1. 2. 3. 2 情報セキュリティ対策の監査 1. 2. 4　見直し	【情報セキュリティ管理基準（平成20年改正版）】 Ⅳ.管理策基準 1 セキュリティ基本方針 1. 1 情報セキュリティ基本方針 2 情報セキュリティのための組織 2. 1 内部組織 4 人的資源のセキュリティ 4. 1 雇用前 4. 2 雇用中 4. 3 雇用の終了又は変更 【ITサービス継続ガイドライン】 4 ITサービス継続マネジメント 4. 3 ITサービス継続計画 4. 4 ITサービス継続体制の実装、運用、維持及び監査
（イ）情報セキュリティ人材の育成等	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 5 経営陣の責任 5. 2. 2 教育・訓練, 意識向上及び力量	【情報セキュリティ管理基準（平成20年度改正版）】 Ⅲ.マネジメント基準 2 情報セキュリティマネジメントの導入と運用 2. 4 教育、訓練、意識向上及び力量
（ウ）監査等によるセキュリティ対策の評価	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 15 順守 A. 15. 3 情報システムの監査に対する考慮事項	【情報セキュリティ管理基準（平成20年度改正版）】 Ⅳ.管理策基準 11 順守 11. 3 情報システムの監査に対する考慮事項

参考文献

2010/7/30現在

指針対策編項目	参考文献	その他参考文献等
イ 情報についての対策	個人情報の保護に関する法律／施行例 個人情報の保護に関するｶﾞｲﾄﾞﾗｲﾝ（各重要ｲﾝﾌﾗ所管省庁作成） 【JIS Q 15001:2006対応】	
（ア）情報の格付け （イ）情報の取り扱い	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 7 資産の管理 A. 7. 1 資産に対する責任 A. 7. 2 情報の分類 【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）】 第1. 3部 情報についての対策 1. 3. 1 情報の取扱い	【情報セキュリティ管理基準（平成20年改正版）】 Ⅳ.管理策基準 3 資産の管理 3. 1 資産に対する責任 3. 2 情報の分類
ウ 情報セキュリティ要件の明確化に基づく対策		
（ア）情報セキュリティ確保のために求められる機能	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 10 通信及び運用管理 A. 10. 6 ネットワークセキュリティ管理 A. 11 アクセス制御 A. 11. 1 アクセス制御に対する業務上の要求事項 A. 11. 2 利用者アクセスの管理 A. 11. 3 利用者の責任 A. 11. 4 ネットワークのアクセス制御 A. 11. 5 オペレーティングシステムのアクセス制御 A. 11. 6 業務用ソフトウェア及び情報のアクセス制御 A. 11. 7 モバイルコンピューティング及びテレワーキング 【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）】 第2. 1部 情報セキュリティ要件の明確化に基づく対策 2. 1. 1 情報セキュリティについての機能	【情報セキュリティ管理基準（平成20年改正版）】 Ⅳ.管理策基準 6 通信及び運用管理 6. 6 ネットワークセキュリティ管理 7 アクセス制御 7. 1 アクセス制御に対する業務上の要求事項 7. 2 利用者アクセスの管理 7. 3 利用者の責任 7. 4 ネットワークのアクセス制御 7. 5 オペレーティングシステムのアクセス制御 7. 6 業務用ソフトウェア及び情報のアクセス制御 7. 7 モバイルコンピューティング及びテレワーキング
（イ）情報セキュリティについての脅威	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 10 通信及び運用管理 A. 10. 6 ネットワークセキュリティ管理 A. 12 情報システムの取得, 開発及び保守 A. 12. 6 技術的ぜい弱性管理 【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）】 第2. 1部 情報セキュリティ要件の明確化に基づく対策 2. 1. 2 情報セキュリティについての脅威	【情報セキュリティ管理基準（平成20年改正版）】 Ⅳ.管理策基準 6 通信及び運用管理 6. 6 ネットワークセキュリティ管理 8 情報システムの取得、開発及び保守 8. 6 技術的ぜい弱性管理

参考文献

2010/7/30現在

指針対策編項目	参考文献	その他参考文献等
エ 情報システムについての対策	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 10 通信及び運用管理 A. 10. 3 システムの計画作成及び受入れ A. 10. 10 監視 A. 15 順守 A. 15. 1 法的要求事項の順守 A. 15. 2 セキュリティ方針及び標準の順守，並びに技術的順守 【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)】 第1. 5部 情報システムについての基本的な対策 1. 5. 1 情報システムのセキュリティ要件 1. 5. 2 情報システムに係る規定の整備と遵守	【情報セキュリティ管理基準(平成20年改正版)】 Ⅳ.管理策基準 6 通信及び運用管理 6. 3 システムの計画作成及び受入れ 6. 10 監視 11 順守 11. 1 法的要求事項の順守 11. 2 セキュリティ方針及び標準の順守並びに技術的順守
(ア)施設と環境	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 9 物理的及び環境的セキュリティ A. 9. 1 セキュリティを保つべき領域 【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)】 第2. 2部 情報システムの構成要素についての対策 2. 2. 1 施設と環境	【情報セキュリティ管理基準(平成20年改正版)】 Ⅳ.管理策基準 5 物理的及び環境的セキュリティ 5. 1 セキュリティを保つべき領域
(イ)電子計算機	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 9 物理的及び環境的セキュリティ A. 9. 2 装置のセキュリティ 【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)】 第2. 2部 情報システムの構成要素についての対策 2. 2. 2 電子計算機	【情報セキュリティ管理基準(平成20年改正版)】 Ⅳ.管理策基準 5 物理的及び環境的セキュリティ 5. 2 装置のセキュリティ

参考文献

2010/7/30現在

指針対策編項目	参考文献	その他参考文献等
(ウ)アプリケーションソフトウェア	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 10 通信及び運用管理 A. 10. 4 悪意のあるコード及びモバイルコードからの保護 A. 10. 5 バックアップ A. 12 情報システムの取得, 開発及び保守 A. 12. 1 情報システムのセキュリティ要求事項 A. 12. 2 業務用ソフトウェアでの正確な処理 A. 12. 3 暗号による管理策 A. 12. 4 システムファイルのセキュリティ A. 12. 5 開発及びサポートプロセスにおけるセキュリティ A. 12. 6 技術性ぜい弱性管理 【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)】 第2. 2部 情報システムの構成要素についての対策 2. 2. 3 アプリケーションソフトウェア	【情報セキュリティ管理基準(平成20年改正版)】 Ⅳ.管理策基準 6 通信及び運用管理 6. 4 悪意のあるコード及びモバイルコードからの保護 6. 5 バックアップ 8 情報システムの取得、開発及び保守 8. 1 情報システムのセキュリティ要求事項 8. 2業務用ソフトウェアでの正確な処理 8. 3 暗号による管理策 8. 4 システムファイルのセキュリティ 8. 5 開発及びサポートプロセスにおけるセキュリティ 8. 6 技術的ぜい弱性管理 【情報システムの信頼性向上に関するガイドライン(第2版)】 【情報システムの信頼性向上に関する評価指標(第1版)】
(エ)通信回線及び通信回線装置	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 10 通信及び運用管理 A. 10. 1 運用の手順及び責任 A. 10. 6 ネットワークセキュリティ管理 A. 10. 8 情報の交換 A. 10. 9 電子商取引サービス 【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)】 第2. 2部 情報システムの構成要素についての対策 2. 2. 4 通信回線	【情報セキュリティ管理基準(平成20年改正版)】 Ⅳ.管理策基準 6 通信及び運用管理 6. 1 運用の手順及び責任 6. 6 ネットワークセキュリティ管理 6. 8 情報の交換 6. 9 電子商取引サービス 【情報システムに係る政府調達への SLA導入ガイドライン】 【SaaS向けSLAガイドライン】

参考文献

2010/7/30現在

指針対策編項目	参考文献	その他参考文献等
(2)5つの重点項目		
ア IT障害の観点から見た事業継続性確保のための対策	【中央省庁業務継続ガイドライン第1版】	【ITサービス継続ガイドライン】
(ア)事業継続性確保のための個別対策の実施	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 13 情報セキュリティインシデントの管理 A. 13. 1 情報セキュリティの事象及び弱点の報告 A. 13. 2 情報セキュリティインシデントの管理及びその改善	【情報セキュリティ管理基準(平成20年改正版)】 Ⅳ.管理策基準 9 情報セキュリティインシデントの管理 9. 1 情報セキュリティの事象及び弱点の報告 9. 2 情報セキュリティインシデントの管理及びその改善
(イ)事業継続計画との整合性の確保	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 14 事業継続管理 A. 14. 1 事業継続管理における情報セキュリティの側面 【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)】 第1. 2部 組織と体制の整備 1. 2. 2. 2 障害・事故等の対処 1. 2. 5. 2 業務継続計画との整合的運用の確保	【情報セキュリティ管理基準(平成20年改正版)】 Ⅳ.管理策基準 10 事業継続管理 10. 1 事業継続管理における情報セキュリティの側面

参考文献

2010/7/30現在

指針対策編項目	参考文献	その他参考文献等
イ 情報漏えい防止のための対策		個人情報の保護に関する法律／施行令 個人情報の保護に関するｶﾞｲﾄﾞﾗｲﾝ（各重要ｲﾝﾌﾗ所管省庁作成） 【JIS Q 15001:2006対応】
（ア）保護すべき情報の類型化		
（イ）保護すべき情報の管理	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 10 通信及び運用管理 A. 10. 7 媒体の取扱い A. 15 順守 A. 15. 1 法的要求事項の順守 A. 15. 1. 4 個人データ及び個人情報の保護 【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）】 第1. 3部 情報についての対策 1. 3. 1 情報の取扱い	【情報セキュリティ管理基準（平成20年改正版）】 Ⅳ.管理策基準 6 通信及び運用管理 6. 7 媒体の取扱い 11 順守 11. 1 法的要求事項の順守 11. 1. 4 個人データ及び個人情報の保護は、関連する法令、規制、及び適用がある場合には、契約条項の中の要求に従って確実にする
（ウ）不正アクセスによる脅威への対応	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A. 9 物理的及び環境的セキュリティ A. 9. 2 装置のセキュリティ A. 10 通信及び運用管理 A. 10. 6 ネットワークセキュリティ管理 A. 10. 7 媒体の取扱い A. 11 アクセス制御 A. 11. 1 アクセス制御に対する業務上の要求事項 A. 11. 2 利用者アクセスの管理 A. 11. 3 利用者の責任 A. 11. 4 ネットワークのアクセス制御 A. 11. 5 オペレーティングシステムのアクセス制御 A. 11. 6 業務用ソフトウェア及び情報のアクセス制御 A. 11. 7 モバイルコンピューティング及びテレワーキング	【情報セキュリティ管理基準（平成20年改正版）】 Ⅳ.管理策基準 5 物理的及び環境的セキュリティ 5. 2 装置のセキュリティ 6 通信及び運用管理 6. 6 ネットワークセキュリティ管理 6. 7 媒体の取扱い 7 アクセス制御 7. 1 アクセス制御に対する業務上の要求事項 7. 2 利用者アクセスの管理 7. 3 利用者の責任 7. 4 ネットワークのアクセス制御 7. 5 オペレーティングシステムのアクセス制御 7. 6 業務用ソフトウェア及び情報のアクセス制御 7. 7 モバイルコンピューティング及びテレワーキング

参考文献

2010/7/30現在

指針対策編項目	参考文献	その他参考文献等
(エ)内部関係者による脅威への対策	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 5 経営陣の責任 5.2.2 教育・訓練, 意識向上及び力量 A.7 資産の管理 A.7.1 資産に対する責任 A.7.2 情報の分類 A.10 通信及び運用管理 A.10.6 ネットワークセキュリティ管理 A.10.7 媒体の取扱い A.10.10 監視 A.11 アクセス制御 A.11.1 アクセス制御に対する業務上の要求事項 A.11.2 利用者アクセスの管理 A.11.3 利用者の責任 A.11.4 ネットワークのアクセス制御 A.11.5 オペレーティングシステムのアクセス制御 A.11.6 業務用ソフトウェア及び情報のアクセス制御 A.11.7 モバイルコンピューティング及びテレワーキング	【情報セキュリティ管理基準(平成20年改正版)】 Ⅲ.マネジメント基準 2 情報セキュリティマネジメントの導入と運用 2.4 教育、訓練、意識向上及び力量 Ⅳ.管理策基準 3 資産の管理 3.1 資産に対する責任 3.2 情報の分類 6 通信及び運用管理 6.6 ネットワークセキュリティ管理 6.7 媒体の取扱い 6.10 監視 7 アクセス制御 7.1 アクセス制御に対する業務上の要求事項 7.2 利用者アクセスの管理 7.3 利用者の責任 7.4 ネットワークのアクセス制御 7.5 オペレーティングシステムのアクセス制御 7.6 業務用ソフトウェア及び情報のアクセス制御 7.7 モバイルコンピューティング及びテレワーキング
(オ)情報漏えい発生時の対応策の整備	【ISO／IEC 27001 ／ JIS Q 27001:2006対応】 A.13 情報セキュリティインシデントの管理 A.13.1 情報セキュリティの事象及び弱点の報告 A.13.2 情報セキュリティインシデントの管理及びその改善 【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)】 第1.2部 組織と体制の整備 1.2.2.2 障害・事故等の対処	【情報セキュリティ管理基準(平成20年改正版)】 Ⅳ.管理策基準 9 情報セキュリティインシデントの管理 9.1 情報セキュリティの事象及び弱点の報告 9.2 情報セキュリティインシデントの管理及びその改善

参考文献

2010/7/30現在

指針対策編項目	参考文献	その他参考文献等
ウ　外部委託における情報セキュリティ確保のための対策		【アウトソーシングに関する情報セキュリティ対策ガイダンス】
(ア)委託先管理の仕組み (イ)外部委託実施における情報セキュリティ確保対策の徹底 (ウ)IT障害発生時の対応策の整備	【ISO／IEC　27001　／　JIS　Q　27001:2006対応】 A. 6　　情報セキュリティのための対策 A. 6. 2　外部組織 A. 10　通信及び運用管理 A. 10. 2　第三者が提供するサービスの管理 【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)】 第1. 2部　組織と体制の整備 1. 2. 5. 1　その他／外部委託	(ア)(イ)(ウ)共通 【情報セキュリティ管理基準(平成20年改正版)】 Ⅳ.管理策基準 2　情報セキュリティのための組織 2. 2　外部組織 6　通信及び運用管理 6. 2　第三者が提供するサービスの管理 【医療情報を受託管理する情報処理事業者向けガイドライン】 (イ)外部委託実施における情報セキュリティ確保対策の徹底 【情報システム・モデル取引・契約書(第1版)】 【情報システム・モデル取引・契約書(追補版)】
エ　IT障害発生時の利用者の対応のための情報の提供等の対策		
(ア)IT障害による重要インフラサービスの停止等の情報の提供 (イ)IT障害防止のための取組みに関する情報の提供	【重要インフラの情報セキュリティ対策に係る第2次行動計画】 Ⅲ. 2. (6). ア). ⑤「安全基準等の整備及び浸透」に関する対策	(イ)IT障害防止のための取組みに関する情報の提供 【情報セキュリティ報告書モデル】
オ　ITに係る環境変化に伴う脅威のための対策	【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)】 第2. 3部　個別事項についての対策 2. 3. 1　その他 2. 3. 1. 1　情報システムへのIPv6技術の導入における対策	