Sec01-02-56\_各種ガイドブックの内容要約\_重要インフラ・政府機関向け【独法を含む】【SK3】

ドキュメントを参照: [Sec01-02-50\_サイバーセキュリティ関連\_各種ガイドブックの内容要約.mmap](file:///D:\Cloud_Storage\OneDrive%20-%20ＮＰO知的資源イニシアティブ（ＩＲＩ）\git_repository_Duo\Sharing_Knowledge3\MindManager3\Sec01-02-50_サイバーセキュリティ関連_各種ガイドブックの内容要約.mmap)

1. 重要インフラ・政府機関向け【独法を含む】
2. サイバーセキュリティ基本法（2016年4月15日改正）
   1. 目的
      1. サイバーセキュリティに関する施策を総合的かつ効果的に推進し、 もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、 国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。
3. 【未整理】サイバーセキュリティ2018【2018年7月25日NISC】

ドキュメントを参照: [cs2018.pdf](https://www.nisc.go.jp/active/kihon/pdf/cs2018.pdf)

1. サイバーセキュリティ2017【2017年８月25日NISC】

ドキュメントを参照: [cs2017.pdf](https://www.nisc.go.jp/active/kihon/pdf/cs2017.pdf)

1. 重要インフラの情報セキュリティ対策に係る第4次行動計画【2017年4月18日NISC】

ドキュメントを参照: [infra\_rt4.pdf](https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf)

* 1. 重要インフラの情報セキュリティ対策に係る第４次行動計画（案）の概要

ドキュメントを参照: [pubcom\_ap4\_abst.pdf](https://www.nisc.go.jp/active/infra/pdf/pubcom_ap4_abst.pdf)

1. サイバーセキュリティ戦略【2015年９月４日閣議決定】

ドキュメントを参照: [cs-senryaku-kakugikettei.pdf](https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf)

1. 政府機関の情報セキュリティ対策のための統一規範

ドキュメントを参照: [kihan28.pdf](http://www.nisc.go.jp/active/general/pdf/kihan28.pdf)

1. 政府機関等の情報セキュリティ対策の運用等に関する指針

ドキュメントを参照: [shishin28.pdf](http://www.nisc.go.jp/active/general/pdf/shishin28.pdf)

1.  政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）

ドキュメントを参照: [guide30.pdf](https://www.nisc.go.jp/active/general/pdf/guide30.pdf)

* 1. 【2018年7月25日NISC】
  2. 第 1 部 総則
     1. 1.1 目的
     2. 1.2 対策基準の策定手順
     3. 1.3 本ガイドラインの改定
     4. 1.4 統一基準、 本ガイドライン及び実施手順の関係
     5. 1.5 統一基準で定義されている用語
        1. (1) 情報の格付の区分
        2. (2) 情報の取扱制限
        3. (3) 統一基準 1.3「用語定義」において定義されている用語
     6. 1.6 一般用語の解説
     7. 1.7 基本対策事項及び解説の読み方
  3. 第 2 部 情報セキュリティ対策の基本的枠組み
     1. 2.1 導入・計画
        1. 2.1.1 組織・体制の整備
        2. (1) 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置
        3. (2) 情報セキュリティ委員会の設置
        4. (3) 情報セキュリティ監査責任者の設置
        5. (4) 統括情報セキュリティ責任者・情報セキュリティ責任者等の設置
        6. (5) 最高情報セキュリティアドバイザーの設置
        7. (6) 情報セキュリティ対策推進体制の整備
        8. (7) 情報セキュリティインシデントに備えた体制の整備
        9. (8) 兼務を禁止する役割
        10. 2.1.2 対策基準・対策推進計画の策定
        11. (1) 対策基準の策定
        12. (2) 対策推進計画の策定
     2. 2.2 運用
        1. 2.2.1 情報セキュリティ関係規程の運用
           1. (1) 情報セキュリティ対策の運用
           2. (2) 違反への対処
        2. 2.2.2 例外措置
           1. (1) 例外措置手続の整備
           2. (2) 例外措置の運用
        3. 2.2.3 教育
           1. (1) 教育体制の整備・教育実施計画の策定
           2. (2) 教育の実施
        4. 2.2.4 情報セキュリティインシデントへの対処
           1. (1) 情報セキュリティインシデントに備えた事前準備
           2. (2) 情報セキュリティインシデントへの対処
           3. (3) 情報セキュリティインシデントの再発防止・教訓の共有
     3. 2.3 点検
        1. 2.3.1 情報セキュリティ対策の自己点検
           1. (1) 自己点検計画の策定・手順の準備
           2. (2) 自己点検の実施
           3. (3) 自己点検結果の評価・改善
        2. 2.3.2 情報セキュリティ監査
           1. (1) 監査実施計画の策定
           2. (2) 監査の実施
           3. (3) 監査結果に応じた対処
     4. 2.4 見直し
        1. 2.4.1 情報セキュリティ対策の見直し
           1. (1) 情報セキュリティ関係規程の見直し
           2. (2) 対策推進計画の見直し
  4. 第 3 部 情報の取扱い
     1. 3.1 情報の取扱い
        1. 3.1.1 情報の取扱い
           1. (1) 情報の取扱いに係る規定の整備
           2. (2) 情報の目的外での利用等の禁止
           3. (3) 情報の格付及び取扱制限の決定・明示等
           4. (4) 情報の利用・保存
           5. (5) 情報の提供・公表
           6. (6) 情報の運搬・送信
           7. (7) 情報の消去
           8. (8) 情報のバックアップ
     2. 3.2 情報を取り扱う区域の管理
        1. 3.2.1 情報を取り扱う区域の管理
           1. (1) 要管理対策区域における対策の基準の決定
           2. (2) 区域ごとの対策の決定
           3. (3) 要管理対策区域における対策の実施
  5. 第 4 部 外部委託
     1. 4.1 外部委託
        1. 4.1.1 外部委託
           1. (1) 外部委託に係る規定の整備
           2. (2) 外部委託に係る契約
           3. (3) 外部委託における対策の実施
           4. (4) 外部委託における情報の取扱い
        2. 4.1.2 約款による外部サービスの利用
           1. (1) 約款による外部サービスの利用に係る規定の整備
           2. (2) 約款による外部サービスの利用における対策の実施
        3. 4.1.3 ソーシャルメディアサービスによる情報発信
           1. (1) ソーシャルメディアサービスによる情報発信時の対策
        4. 4.1.4 クラウドサービスの利用
           1. (1) クラウドサービスの利用における対策
  6. 第 5 部 情報システムのライフサイクル
     1. 5.1 情報システムに係る文書等の整備
        1. 5.1.1 情報システムに係る台帳等の整備
           1. (1) 情報システム台帳の整備
           2. (2) 情報システム関連文書の整備
        2. 5.1.2 機器等の調達に係る規定の整備
           1. (1) 機器等の調達に係る規定の整備
     2. 5.2 情報システムのライフサイクルの各段階における対策
        1. 5.2.1 情報システムの企画・要件定義
           1. (1) 実施体制の確保
           2. (2) 情報システムのセキュリティ要件の策定
           3. (3) 情報システムの構築を外部委託する場合の対策
           4. (4) 情報システムの運用・保守を外部委託する場合の対策
        2. 5.2.2 情報システムの調達・構築
           1. (1) 機器等の選定時の対策
           2. (2) 情報システムの構築時の対策
           3. (3) 納品検査時の対策
        3. 5.2.3 情報システムの運用・保守
           1. (1) 情報システムの運用・保守時の対策
        4. 5.2.4 情報システムの更改・廃棄
           1. (1) 情報システムの更改・廃棄時の対策
        5. 5.2.5 情報システムについての対策の見直し
           1. (1) 情報システムについての対策の見直し
     3. 5.3 情報システムの運用継続計画
        1. 5.3.1 情報システムの運用継続計画の整備・整合的運用の確保
           1. (1) 情報システムの運用継続計画の整備・整合的運用の確保
  7. 第 6 部 情報システムのセキュリティ要件
     1. 6.1 情報システムのセキュリティ機能
        1. 6.1.1 主体認証機能
           1. (1) 主体認証機能の導入
           2. (2) 識別コード及び主体認証情報の管理
        2. 6.1.2 アクセス制御機能
           1. (1) アクセス制御機能の導入
        3. 6.1.3 権限の管理
           1. (1) 権限の管理
        4. 6.1.4 ログの取得・管理
           1. (1) ログの取得・管理
        5. 6.1.5 暗号・電子署名
           1. (1) 暗号化機能・電子署名機能の導入
           2. (2) 暗号化・電子署名に係る管理
     2. 6.2 情報セキュリティの脅威への対策
        1. 6.2.1 ソフトウェアに関する脆弱性対策
           1. (1) ソフトウェアに関する脆弱性対策の実施
        2. 6.2.2 不正プログラム対策
           1. (1) 不正プログラム対策の実施
        3. 6.2.3 サービス不能攻撃対策
           1. (1) サービス不能攻撃対策の実施
        4. 6.2.4 標的型攻撃対策
           1. (1) 標的型攻撃対策の実施
     3. 6.3 アプリケーション・コンテンツの作成・提供
        1. 6.3.1 アプリケーション・コンテンツの作成時の対策
           1. (1) アプリケーション・コンテンツの作成に係る規定の整備
           2. (2) アプリケーション・コンテンツのセキュリティ要件の策定
        2. 6.3.2 アプリケーション・コンテンツ提供時の対策
           1. (1) 政府ドメイン名の使用
           2. (2) 不正なウェブサイトへの誘導防止
           3. (3) アプリケーション・コンテンツの告知
  8. 第 7 部 情報システムの構成要素
     1. 7.1 端末・サーバ装置等
        1. 7.1.1 端末
           1. (1) 端末の導入時の対策
           2. (2) 端末の運用時の対策
           3. (3) 端末の運用終了時の対策
           4. (4) 要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末の導入及び利用時の対策
        2. 7.1.2 サーバ装置
           1. (1) サーバ装置の導入時の対策
           2. (2) サーバ装置の運用時の対策
           3. (3) サーバ装置の運用終了時の対策
        3. 7.1.3 複合機・特定用途機器
           1. (1) 複合機
           2. (2) IoT 機器を含む特定用途機器
     2. 7.2 電子メール・ウェブ等
        1. 7.2.1 電子メール
           1. (1) 電子メールの導入時の対策
        2. 7.2.2 ウェブ
           1. (1) ウェブサーバの導入・運用時の対策
           2. (2) ウェブアプリケーションの開発時・運用時の対策
        3. 7.2.3 ドメインネームシステム（DNS）
           1. (1) DNS の導入時の対策
           2. (2) DNS の運用時の対策
        4. 7.2.4 データベース
           1. (1) データベースの導入・運用時の対策
     3. 7.3 通信回線
        1. 7.3.1 通信回線
           1. (1) 通信回線の導入時の対策
           2. (2) 通信回線の運用時の対策
           3. (3) 通信回線の運用終了時の対策
           4. (4) リモートアクセス環境導入時の対策
           5. (5) 無線 LAN 環境導入時の対策
        2. 7.3.2 IPv6 通信回線
           1. (1) IPv6 通信を行う情報システムに係る対策
           2. (2) 意図しない IPv6 通信の抑止・監視
  9. 第 8 部 情報システムの利用
     1. 8.1 情報システムの利用
        1. 8.1.1 情報システムの利用
           1. (1) 情報システムの利用に係る規定の整備
           2. (2) 情報システム利用者の規定の遵守を支援するための対策
           3. (3) 情報システムの利用時の基本的対策
           4. (4) 電子メール・ウェブの利用時の対策
           5. (5) 識別コード・主体認証情報の取扱い
           6. (6) 暗号・電子署名の利用時の対策
           7. (7) 不正プログラム感染防止
     2. 8.2 機関等支給以外の端末の利用
        1. 8.2.1 機関等支給以外の端末の利用
           1. (1) 機関等支給以外の端末の利用可否の判断
           2. (2) 機関等支給以外の端末の利用規定の整備・管理
           3. (3) 機関等支給以外の端末の利用時の対策
  10. 付録

1. 政府機関向け「アマゾン ウェブ サービス」対応セキュリティリファレンス

ドキュメントを参照: [aws\_security.html](http://dc.jp.nttdata.com/service/cloud/aws_security.html)

* 1. NISC「政府機関等の情報セキュリティ対策のための統一基準群（平成28年度版）」の最新基準に対応したAWS利用のためのリファレンス
  2. 【参考】政府機関の情報セキュリティ対策のための統一基準（平成28年度版）

ドキュメントを参照: [kijyun28.pdf](http://www.nisc.go.jp/active/general/pdf/kijyun28.pdf)

* 1. 【参考】府省庁対策基準策定のためのガイドライン（平成28年度版）

ドキュメントを参照: [guide28.pdf](http://www.nisc.go.jp/active/general/pdf/guide28.pdf)

1. 「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」の策定について【2015年5月NISC】

ドキュメントを参照: [sbd\_sakutei.html](http://www.nisc.go.jp/active/general/sbd_sakutei.html)

* 1. 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 ◦「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」

ドキュメントを参照: [SBD\_manual.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_manual.pdf)

* 1. 「同　マニュアル　付録A.対策要件集」

ドキュメントを参照: [SBD\_manual\_annex\_a.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_manual_annex_a.pdf)

* 1. 「同　マニュアル　付録B.政府機関統一基準群対応表」

ドキュメントを参照: [SBD\_manual\_annex\_b.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_manual_annex_b.pdf)

* 1. 「同　マニュアル　付録D.用語解説」

ドキュメントを参照: [SBD\_manual\_annex\_d.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_manual_annex_d.pdf)

* + 1. 「同　マニュアル活用ワークシート」(MS-Excel形式)

ドキュメントを参照: [SBD\_manual\_worksheet.xlsx](http://www.nisc.go.jp/active/general/xls/SBD_manual_worksheet.xlsx)

* + 1. 「同　マニュアル活用ワークシート」（活用例）

ドキュメントを参照: [SBD\_manual\_worksheet\_example.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_manual_worksheet_example.pdf)

* 1. 「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」概要

ドキュメントを参照: [SBD\_overview.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_overview.pdf)

* 1. 情報セキュリティを企画・設計段階から確保するための方策に係る検討会　報告書

ドキュメントを参照: [SBD\_report.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_report.pdf)

1. 地方公共団体における情報セキュリティポリシーに関するガイドライン【2015年3月総務省】

ドキュメントを参照: [000348656.pdf](http://www.soumu.go.jp/main_content/000348656.pdf)