参考資料

重要インフラのサイバーセキュリティに係る安全基準等策定指針との対応状況

総 務 省

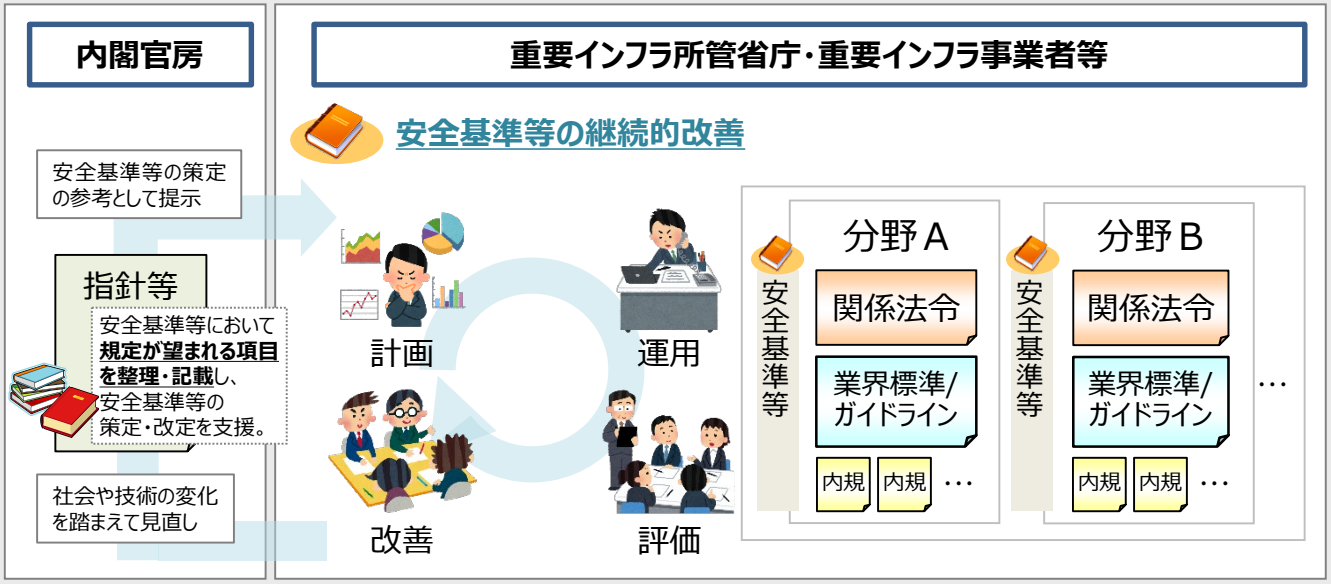
令和６年７月22日

総務省自治行政局

デジタル基盤推進室

「重要インフラのサイバーセキュリティに係る安全基準等策定指針」について

- ✓ 内閣官房（NISC）では、我が国の重要インフラ防護能力の維持・向上を目的に、**<u>各重要インフラ分野に共通し、重要インフラサービスの安全かつ持続的な提供を実現する観点から安全基準等において規定されることが望まれる項目</u>**を「重要インフラのサイバーセキュリティに係る安全基準等策定指針」（2023年７月4日サイバーセキュリティ戦略本部決定）として取りまとめている。
- ✓ 重要インフラ所管省庁は、安全基準等（ガイドライン等）を策定、改善することとされ、重要インフラ事業者等に対し、安全基準等の浸透に向けた取組を実施することなどが規定されている。
- ✓ 総務省は安全基準等として、「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」を策定し、各地方公共団体に助言を行っている。



※NISC資料より作成

【安全基準等とは】

- **<u>関係法令に基づき国が定める「強制基準」</u>**
- 関係法令に準じて国が定める「推奨基準」及び「ガイドライン」
- 関係法令や国民からの期待に応えるべく業界団体等が定める**<u>業界横断的な</u>**「業界標準」及び「**<u>ガイドライン</u>**」
- 関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」　　等

○重要インフラのサイバーセキュリティに係る行動計画

IV.2.2 安全基準等の継続的改善

（略）<u>内閣官房は、重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表</u>する。また、必要に応じ、重要インフラ所管省庁の策定する安全基準等に関し助言を行う。

（参考）重要インフラ分野

✓ 「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の対象の中に、地方公共団体が含まれている。

- 重要インフラの対象事業者　（「重要インフラのサイバーセキュリティに係る行動計画」 別紙1より）

別紙１　対象となる重要インフラ事業者等と重要システム例

重要インフラ分野	対象となる重要インフラ事業者等(注1)	対象となる重要システム例(注2)
情報通信	・主要な電気通信事業者 ・主要な地上基幹放送事業者 ・主要なケーブルテレビ事業者	・ネットワークシステム ・オペレーションサポートシステム ・編成・運行システム
金融　銀行等 生命保険 損害保険 証券 資金決済	・銀行、信用金庫、信用組合、労働金庫、農業協同組合等 ・資金清算機関 ・電子債権記録機関 ・生命保険 ・損害保険 ・証券会社 ・金融商品取引所 ・振替機関 ・金融商品取引清算機関 ・主要な資金移動業者 ・主要な前払式支払手段(第三者型)発行者　等	・勘定系システム ・資金証券系システム ・国際系システム ・対外接続系システム ・金融機関相互ネットワークシステム ・電子債権記録機関システム ・保険業務システム ・証券取引システム ・取引所システム ・振替システム ・清算システム
航空	・主たる定期航空運送事業者	・運航システム ・予約・搭乗システム ・整備システム ・貨物システム
空港	・主要な空港・空港ビル事業者	・警戒警備・監視システム ・フライトインフォメーションシステム ・バゲージハンドリングシステム
鉄道	・ＪＲ各社及び大手民間鉄道事業者等の主要な鉄道事業者	・列車運行管理システム ・電力管理システム ・座席予約システム
電力	・一般送配電事業者、主要な発電事業者　等	・電力制御システム ・スマートメーターシステム
ガス	・主要なガス事業者	・プラント制御システム ・遠隔監視・制御システム
政府・行政サービス	・地方公共団体	・地方公共団体の情報システム
医療	・医療機関 （ただし、小規模なものを除く。）	・診療録等管理システム ・診療業務支援システム ・地域医療支援システム
水道	・水道事業者及び水道用水供給事業者 （ただし、小規模なものを除く。）	・水道施設や水道水の監視システム ・水道施設の制御システム
物流	・大手物流事業者	・集配管理システム ・貨物追跡システム ・倉庫管理システム
化学	・主要な石油化学事業者	・プラント制御システム
クレジット	・主要なクレジットカード会社 ・主要な決済代行業者 ・指定信用情報機関　等	・クレジット(包括信用購入あっせん及び二月払購入あっせん)に係る決済システム ・信用情報提供・収集システム
石油	・主要な石油精製・元売事業者	・受発注システム ・生産管理システム ・生産出荷システム
港湾	・主要な港湾運送事業者・港湾管理者等	・ターミナルオペレーションシステム（TOS）

注１　ここに掲げているものは、重点的に対策を実施すべき重要インフラ事業者等であり、行動計画の見直しの際に、事業環境の変化及びITへの依存度の進展等を踏まえ、対象とするものの見直しを行う。
注２　ここに掲げているものは、例であり全てではない。

「重要インフラのサイバーセキュリティに係る安全基準等策定指針」

- ✓ 令和５年度に改定された「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の項目と「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(令和5年3月版)」の対応状況を、以下の確認項目に沿って整理。
- ✓ 「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(令和5 年3 月版)」は「3.7 情報開示」を除く項目については規定済み。

安全基準等策定指針の指針項目
2.総則
2.1.策定目的
2.2.対象範囲
2.3.関係主体の役割
3.組織統治におけるサイバーセキュリティ
3.1.組織方針
3.1.1.組織方針とサイバーセキュリティ
3.1.2.サイバーセキュリティ方針
3.2.組織内外のコミュニケーション
3.3.経営リスクとしてのサイバーセキュリティリスクの管理
3.5.資源の確保
3.6.監査・モニタリング
3.7.情報開示
3.8.継続的改善
4.リスクマネジメントの活用と危機管理
4.1.組織状況の理解
4.2.リスクアセスメント
4.3.サイバーセキュリティリスク対応
4.3.1.リスク対応の決定
4.3.2.個別方針の策定
4.3.3.リスク対応計画の策定
4.4.サプライチェーン・リスクマネジメント
4.5.事業継続計画等
4.6.人材育成・意識啓発
4.7.CSIRT等の整備
4.8.平時の運用
4.8.1.セキュリティ対策の導入、運用プロセスの確立・実行
4.8.2.情報共有
4.9.危機管理
4.10.演習・訓練

5.対策項目
5.1.組織的対策
5.1.1.資産の管理
5.1.1.1.資産に対する責任
5.1.1.2.情報分類と取扱い
5.1.1.3.データ管理
5.1.1.3.データ管理
5.1.2.供給者管理
5.1.3.運用の管理
5.1.3.1.運用の手順及び責任
5.1.3.2.マルウェアからの保護
5.1.3.3.バックアップ
5.1.3.4.ログ取得
5.1.3.5.運用ソフトウェアの管理
5.1.3.6.脆弱性の管理
5.1.4.システムの取得・開発・保守
5.1.5.インシデント管理
5.2.人的対策
5.2.1.従業員の管理
5.2.2.委託先管理
5.2.3.テレワーク・遠隔制御
5.2.4.エスカレーション
5.3.物理的対策
5.3.1.セキュリティ確保が求められる領域
5.3.2.災害による障害の発生しにくい設備の設置及び管理
5.3.3.装置の管理

5.4.技術的対策
5.4.1.利用者アクセスの管理
5.4.2.情報システム等のアクセス制御
5.4.3.暗号を活用した情報管理
5.4.4.通信のセキュリティ
5.4.5.多層防御
5.5.動向を踏まえた対策
5.5.1.ランサムウェア対策
5.5.2.クラウドサービス利用時の対策

重要インフラのサイバーセキュリティに係る安全基準等策定指針　3.7 情報開示

「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の中の「情報開示」に係る項目について、NISCが調査票において、ベースライン（○：最低限実施すべき事項）　）と推奨事項（◎：実施が望ましい事項）を規定。

指針区分	○：ベースライン(最低限実施すべき事項)　◎：推奨事項（実施が望ましい事項）	
○	3.7.情報開示	国民の安心感の醸成を図る観点から、組織内の既存の情報開示体制を活用し、可能な範囲でサイバーセキュリティに関する取組の開示
◎	3.7.情報開示	組織方針・サイバーセキュリティ方針
◎	3.7.情報開示	維持するサービス範囲・水準
◎	3.7.情報開示	リスク管理体制に関する記載
◎	3.7.情報開示	サイバーセキュリティに関する責任者の知見
◎	3.7.情報開示	資源の確保
◎	3.7.情報開示	リスクの把握と対応計画策定
◎	3.7.情報開示	緊急対応体制・復旧体制
◎	3.7.情報開示	インシデントの発生状況

- ✓　**今般の地方自治法の改正により、各地方公共団体は、サイバーセキュリティを確保するための方針を定め、公表することが義務付けられた**ため、**ベースラインの「組織内の既存の情報開示体制を活用し、可能な範囲でサイバーセキュリティに関する取組の開示」については法的に担保された**といえる。
- ✓　なお、地方公共団体については、情報公開条例に則って情報開示を行っており、インシデントに関しては、住民情報の漏洩など、個人情報に係る事案については報道、公表されている。

（参考）地方自治法

✓ 地制調答申において、**地方公共団体のサイバーセキュリティ対策の実効性を担保**することが必要との提言があったことを踏まえ、以下のサイバーセキュリティの確保の方針の策定・実施・公表義務を課す改正を実施。

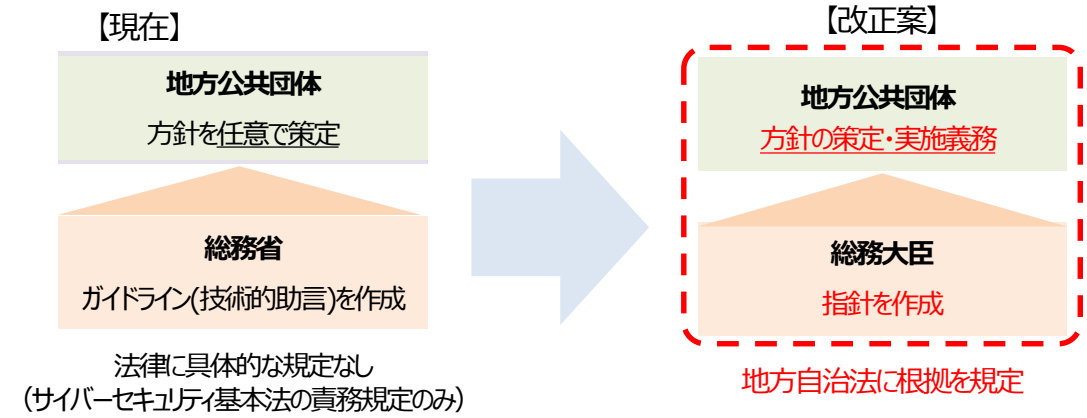
（**サイバーセキュリティを確保するための方針等**）

第二百四十四条の六　**普通地方公共団体の議会及び長その他の執行機関は**、その事務の処理に係る情報システムの利用に当たつての**サイバーセキュリティを確保するための方針を定め、及びこれに基づき必要な措置を講じなければならない**。

2　普通地方公共団体の議会及び長その他の執行機関は、**前項の方針を定め、又はこれを変更したときは**、遅滞なく、**これを公表しなければならない**。

3　総務大臣は、普通地方公共団体に対し、第一項の方針（政令で定める執行機関が定めるものを除く。）の策定又は変更について、指針を示すとともに、必要な助言を行うものとする。

4　総務大臣は、前項の指針を定め、又は変更しようとするときは、国の関係行政機関の長に協議しなければならない。



（参考）安全基準等策定指針と総務省ガイドラインとの比較状況

重要インフラのサイバーセキュリティに係る安全基準等策定指針			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(令和5 年3 月版)	
2.総則	ー	2.1.策定目的	基本方針	1. 目的 3. 対象とする脅威
		2.2.対象範囲	基本方針	4. 適用範囲
		2.3.関係主体の役割	対策基準	1. 組織体制 8. 業務委託と外部サービスの利用 8.1 業務委託 8.2.外部サービスの利用（機密性２以上の情報を取り扱う場合） 8.3.外部サービスの利用（機密性２以上の情報を取り扱わない場
3.組織統治におけるサイバーセキュリティ	3.1.組織方針	3.1.1.組織方針とサイバーセキュリティ	基本方針	6. 情報セキュリティ対策 9. 情報セキュリティ対策基準の策定 10. 情報セキュリティ実施手順の策定
			対策基準	1. 組織体制
		3.1.2.サイバーセキュリティ方針	基本方針	6. 情報セキュリティ対策 9. 情報セキュリティ対策基準の策定 10. 情報セキュリティ実施手順の策定
		3.2.組織内外のコミュニケーション	対策基準	1.組織体制 （９)CSIRTの設置・役割 5.人的セキュリティ 5.3.情報セキュリティインシデントの報告
		3.3.経営リスクとしてのサイバーセキュリティリスクの管理	対策基準	1.組織体制
		3.4.責任及び権限の割当て	対策基準	1.組織体制
		3.5.資源の確保	対策基準	1.組織体制
		3.6.監査・モニタリング	対策基準	6.技術的セキュリティ 6.6. セキュリティ情報の収集 9.評価・見直し 9.1.監査 9.2.自己点検
		3.7.情報開示	基本方針	（地方自治法で規定）

（参考）安全基準等策定指針と総務省ガイドラインとの比較状況

重要インフラのサイバーセキュリティに係る安全基準等策定指針			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(令和5 年3 月版)	
3.組織統治におけるサイバーセキュリティ	ー	3.8.継続的改善	対策基準	5.人的セキュリティ 5.2.研修・訓練 9.評価・見直し 9.1.監査 9.2.自己点検 9.3.情報セキュリティポリシー及び関係規程等の見直し
4.リスクマネジメントの活用と危機管理	ー	4.1.組織状況の理解	基本方針	６．情報セキュリティ対策 （１）組織体制
		4.2.リスクアセスメント	基本方針	６．情報セキュリティ対策 （２）情報資産の分類と管理
	4.3.サイバーセキュリティリスク対応	4.3.1.リスク対応の決定	対策基準	9.評価・見直し 9.3.情報セキュリティポリシー及び関係規程等の見直し
		4.3.2.個別方針の策定	対策基準	9.評価・見直し 9.3.情報セキュリティポリシー及び関係規程等の見直し
		4.3.3.リスク対応計画の策定	対策基準	9.評価・見直し 9.3.情報セキュリティポリシー及び関係規程等の見直し
	ー	4.4.サプライチェーン・リスクマネジメント	基本方針	６．情報セキュリティ対策 （８）業務委託と外部サービスの利用
	ー	4.5.事業継続計画等	基本方針	６．情報セキュリティ対策 （７）運用
	ー	4.6.人材育成・意識啓発	基本方針	６．情報セキュリティ対策 （５）人的セキュリティ
	ー	4.7.CSIRT等の整備	対策基準	1.組織体制 （９）CSIRTの設置・役割
	4.8.平時の運用	4.8.1.セキュリティ対策の導入、運用プロセスの確立・実行	対策基準	1.組織体制 （９）CSIRTの設置・役割
		4.8.2.情報共有	対策基準	1.組織体制 （９）CSIRTの設置・役割

（参考）安全基準等策定指針と総務省ガイドラインとの比較状況

重要インフラのサイバーセキュリティに係る安全基準等策定指針			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(令和5 年3 月版)	
4.リスクマネジメントの活用と危機管理	ー	4.9.危機管理	基本方針	5.人的セキュリティ 5.3.情報セキュリティインシデントの報告 （３）情報セキュリティインシデント原因の究明・記録、再発防止等 7.運用 7.3.侵害時の対応等 （１）緊急時対応計画の策定
		4.10.演習・訓練	対策基準	5.人的セキュリティ 5.2.研修・訓練 （3）緊急時対応訓練
5.対策項目	5.1.組織的対策	5.1.1.資産の管理 5.1.1.1.資産に対する責任	対策基準	2.情報資産の分類と管理 (2)情報資産の管理
		5.1.1.資産の管理 5.1.1.2.情報分類と取扱い	対策基準	2.情報資産の分類と管理 (1)情報資産の分類
		5.1.1.資産の管理 5.1.1.3.データ管理	対策基準	2.情報資産の分類と管理 (2)情報資産の管理 4.物理的セキュリティ 4.2.管理区域（情報システム室等）の管理 (1)管理区域の構造等 8.業務委託と外部サービスの利用 8.2.外部サービスの利用（機密性２以上の情報を取り扱う場合） （２）外部サービスの選定
		5.1.2.供給者管理	対策基準	8.業務委託と外部サービスの利用 8.1.業務委託 （2）契約項目 （3）確認・措置等 8.業務委託と外部サービスの利用 8.2.外部サービスの利用（機密性２以上の情報を取り扱う場合） （３）外部サービスの利用に係る調達・契約 （５）外部サービスを利用した情報システムの導入・構築時の対策

（参考）安全基準等策定指針と総務省ガイドラインとの比較状況

重要インフラのサイバーセキュリティに係る安全基準等策定指針			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(令和5 年3 月版)	
5.対策項目	5.1.組織的対策	5.1.3.運用の管理 5.1.3.1.運用の手順及び責任	対策基準	6.技術的セキュリティ 6.3.システム開発、導入、保守等 （4） システム開発・保守に関連する資料等の整備・保管 7.運用 7.1.情報システムの監視 8.業務委託と外部サービスの利用 8.1.業務委託 （3） 確認・措置等
		5.1.3.運用の管理 5.1.3.2.マルウェアからの保護	対策基準	6.技術的セキュリティ 6.4.不正プログラム対策 （1） 統括情報セキュリティ責任者の措置事項
		5.1.3.運用の管理 5.1.3.3.バックアップ	対策基準	6.技術的セキュリティ 6.1.コンピュータ及びネットワークの管理 （2） バックアップの実施
3.組織統治におけるサイバーセキュリティ	3.1.組織方針	5.1.3.運用の管理 5.1.3.4.ログ取得	対策基準	6.技術的セキュリティ 6.1.コンピュータ及びネットワークの管理 （6） ログの取得等
		5.1.3.運用の管理 5.1.3.5.運用ソフトウェアの管理	対策基準	6.技術的セキュリティ 6.3.システム開発、導入、保守等 （2） 情報システムの開発 （3） 情報システムの導入 6.4.不正プログラム対策 （1） 統括情報セキュリティ責任者の措置事項
		5.1.3.運用の管理 5.1.3.6.脆弱性の管理	対策基準	6.技術的セキュリティ 6.3.システム開発、導入、保守等 （7） 開発・保守用のソフトウェアの更新等 6.6.セキュリティ情報の収集 （1） セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等
		5.1.4.システムの取得・開発・保守	対策基準	6.技術的セキュリティ 6.3.システム開発、導入、保守等 （1） 情報システムの調達 8.業務委託と外部サービスの利用 8.1.業務委託 （3） 確認・措置等