資料 8-4

○重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針　　新旧対照表（案）

改定案	現行
重要インフラにおける情報セキュリティ確保に係る 安全基準等策定指針 （第５版） 平成３０年４月４日 ○○○年○月○日改定 サイバーセキュリティ戦略本部	重要インフラにおける情報セキュリティ確保に係る 安全基準等策定指針 （第５版） 平成３０年４月４日 サイバーセキュリティ戦略本部
（略）	（略）
（脚注） 7 健康（Health）、安全（Safety）及び環境（Environment）を指す。産業用オートメーション及び制御システムを対象としたサイバーセキュリティのマネジメントシステムである CSMS 認証基準（Ver.2.0）では、物理的リスクのアセスメントの結果、HSE 上のリスクのアセスメントの結果及びサイバーセキュリティリスクのアセスメントの結果の統合を要求している。	（脚注） 7 健康（Health）、安全（Safety）及び環境（Environment）を指す。産業用オートメーション及び制御システムを対象としたサイバーセキュリティのマネジメントシステムである CSMS 認証基準（Ver.1.0）では、物理的リスクのアセスメントの結果、HSE 上のリスクのアセスメントの結果及びサイバーセキュリティリスクのアセスメントの結果の統合を要求している。
（略）	（略）
4.1.3.　「計画」の観点 （１）情報セキュリティリスクアセスメント	4.1.3.　「計画」の観点 （１）情報セキュリティリスクアセスメント
（略）	（略）
（２）情報セキュリティリスク対応の決定	（２）情報セキュリティリスク対応の決定
（略）	（略）

改定案	現行
（イ）資産の管理 ●資産に対する責任 （略） **●情報分類と取扱い** 重要インフラ事業者等の取り扱う情報について、その重要性や法的要求、国民の安心感への影響等に応じて、機密性、完全性、可用性の観点から情報の格付け及び情報媒体（紙、電子）へのラベル付けを行う。 また、作成、入手、利用、保存、運搬、送信、提供、消去といった情報のライフサイクルを踏まえ、必要な取扱制限（例：複製禁止、持出禁止、配布禁止）を定め、実施する。 **●データ管理** システムのリスク評価に応じてデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行う。 また、事業環境の変化を捉え、インターネットを介したサービス（クラウドサービス等）を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意する。 （略） **（オ）物理的及び環境的セキュリティ** **●セキュリティ確保が求められる領域** 重要インフラサービスの提供に係る情報システムや情報のある領域（情報セキュリティや安全等の確保が求められる領域）を保護するため、物理的なセキュリティ境界を設けるとともに、物理環境のモニタリングや、認可された従業	（イ）資産の管理 ●資産に対する責任 （略） **●情報分類と取扱い** 重要インフラ事業者等の取り扱う情報について、その重要性や法的要求、国民の安心感への影響等に応じて、機密性、完全性、可用性の観点から情報の格付け及び情報媒体（紙、電子）へのラベル付けを行う。 また、作成、入手、利用、保存、移送、提供、消去といった情報のライフサイクルを踏まえ、必要な取扱制限（例：複製禁止、持出禁止、配布禁止）を定め、実施する。 （新設） （略） **（オ）物理的及び環境的セキュリティ** **●セキュリティ確保が求められる領域** 重要インフラサービスの提供に係る情報システムや情報のある領域（情報セキュリティや安全等の確保が求められる領域）を保護するため、物理的なセキュリティ境界を設けるとともに、物理環境のモニタリングや、認可された従業

改定案	現行
員や委託先だけにアクセスを許すための適切な入退管理の仕組みを構築する。 　また、悪意ある活動を防止する観点から、当該領域への認可されていない物品の持ち込みを制限する。加えて、複数の作業要員を確保できる重要インフラ事業者等においては、単独での作業を制限するといった対応も有効である。	員や委託先だけにアクセスを許すための適切な入退管理の仕組みを構築する。 　また、悪意ある活動を防止する観点から、当該領域への認可されていない物品の持ち込みを制限する。加えて、複数の作業要員を確保できる重要インフラ事業者等においては、単独での作業を制限するといった対応も有効である。
●災害による障害の発生しにくい設備の設置及び管理 　重要インフラサービスの提供に係る情報システム、データセンター等の設備については、各種災害による障害が発生しにくい適切な場所を設置の際に検討するとともに、災害が発生した場合であっても被害を低減できるような防止対策を事前に検討・実施する等、適切な設備の設置及び管理を行う仕組みを構築する。	（新設）
●装置の管理 （略）	**●装置の管理** （略）

改定案

【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
(略)		
航空	(略)	(略)
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	(略)	(略)
(略)		

(略)

【別紙２】重要インフラサービスの説明と重要インフラサービス障害の例

(平成 31 年○月時点)(注4)

重要インフラ分野		重要インフラサービス（手続を含む）(注1) 呼称	重要インフラサービス（手続を含む）の説明（関連する法令）	システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注2)）
(略)					
金融	銀行等	・預金 ・貸付 ・為替	(略)		
		・資金清算	・資金清算（資金決済に関する法律第２条第10項）	(略)	
		・電子記録等	(略)		
	生命保険	(略)			
(略)					
航空		(略)			
空港		・空港におけるセキュリティの確保 ・空港における利便性の向上	・警戒警備等による空港のセキュリティ確保 ・空港利用者等への正確・迅速な情報提供 ・航空機への受託手荷物の検査及び搬送	・警戒警備等に支障が発生することによる空港のセキュリティの低下 ・情報提供等に支障が発生することによる利便性の低下 ・航空機への受託手荷物の検査及び搬送の遅延・停止	・空港分野における情報セキュリティ確保に係る安全ガイドライン
鉄道		(略)			
(略)					

注１　ＩＴを全く利用していないサービスについては対象外。

注２　重要インフラサービス障害に係る基準がない分野については、システムの不具合が引き起こす重要インフラサービス障害が生じないことをサービス維持レベルとみなしている。

注３　改正割賦販売法（施行は、公布（2016年12月９日）から１年６か月以内の政令で定める日）においては、法第２条第３項第１号及び第２号、第35条の16第１項第２号及び第２項。

現行

【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
(略)		
航空	(略)	(略)
新設		
鉄道	(略)	(略)
(略)		

(略)

【別紙２】重要インフラサービスの説明と重要インフラサービス障害の例

(平成 30 年３月時点)(注4)

重要インフラ分野		重要インフラサービス（手続を含む）(注1) 呼称	重要インフラサービス（手続を含む）の説明（関連する法令）	システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル(注2)）
(略)					
金融	銀行等	・預金 ・貸付 ・為替	(略)		
		・資金清算	・資金清算（資金決済に関する法律第２条第５項）	(略)	
		・電子記録等	(略)		
	生命保険	(略)			
(略)					
航空		(略)			
新設					
鉄道		(略)			
(略)					

注１　ＩＴを全く利用していないサービスについては対象外。

注２　重要インフラサービス障害に係る基準がない分野については、システムの不具合が引き起こす重要インフラサービス障害が生じないことをサービス維持レベルとみなしている。

注３　改正割賦販売法（施行は、公布（2016年12月９日）から１年６か月以内の政令で定める日）においては、法第２条第３項第１号及び第２号、第35条の16第１項第２号及び第２項。

改定案

注４　別紙２に記載された内容は平成31年〇月現在のものである。法令等の最新の状況については、必要に応じて、所管省庁等へ確認すること。

（略）

【別紙４】対策項目の具体例等の参照先

対策項目	具体例等の参照先
（略）	（略）
（ア）人的資源のセキュリティ（外部委託）	－
●委託前の対応事項（選定・契約条件）	•「JIS Q 27002:2014」 7.1.1, 7.1.2, 7.2.1, 7.2.2, 7.3.1 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 4.1.1 •「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）」 4.1.1 •「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」 3.1, 3.2
●委託期間中の対応事項	
（イ）資産の管理	－
●資産に対する責任	•「JIS Q 27002:2014」 8.1.1 ～ 8.1.4
●情報分類と取扱い	•「JIS Q 27002:2014」 8.2.1 ～ 8.2.3 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 3.1.1 •「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）」 3.1.1
●データ管理	•「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 4.1.4, 7.2.4 •「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）」 4.1.4, 7.2.4
（ウ）アクセス制御	－
●利用者アクセスの管理	•「JIS Q 27002:2014」 9.2.1 ～ 9.2.6 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 6.1.3 •「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）」 6.1.3
●情報システム等のアクセス制御	•「JIS Q 27002:2014」 9.4.1 ～ 9.4.3 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 6.1.1, 6.1.2 •「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）」 6.1.1, 6.1.2

現行

注４　別紙２に記載された内容は平成30年３月現在のものである。法令等の最新の状況については、必要に応じて、所管省庁等へ確認すること。

（略）

【別紙４】対策項目の具体例等の参照先

対策項目	具体例等の参照先
（略）	（略）
（ア）人的資源のセキュリティ（外部委託）	－
●委託前の対応事項（選定・契約条件）	•「JIS Q 27002:2014」 7.1.1, 7.1.2, 7.2.1, 7.2.2, 7.3.1 •「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）」 4.1.1 •「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）」 4.1.1 •「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」 3.1, 3.2
●委託期間中の対応事項	
（イ）資産の管理	－
●資産に対する責任	•「JIS Q 27002:2014」 8.1.1 ～ 8.1.4
●情報分類と取扱い	•「JIS Q 27002:2014」 8.2.1 ～ 8.2.3 •「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）」 3.1.1 •「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）」 3.1.1
（新設）	
（ウ）アクセス制御	－
●利用者アクセスの管理	•「JIS Q 27002:2014」 9.2.1 ～ 9.2.6 •「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）」 6.1.3 •「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）」 6.1.3
●情報システム等のアクセス制御	•「JIS Q 27002:2014」 9.4.1 ～ 9.4.3 •「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）」 6.1.1, 6.1.2 •「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）」 6.1.1, 6.1.2

改定案	
（エ）暗号	－
●暗号を活用した情報管理	•「JIS Q 27002:2014」 10.1.1, 10.1.2, 18.1.5 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 6.1.5 •「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）」 6.1.5 •「輸出貿易管理令別表第1第9項(7) 暗号装置又はその部分品」
（オ）物理的及び環境的セキュリティ	－
●セキュリティ確保が求められる領域	•「JIS Q 27002:2014」 11.1.1 ～ 11.1.6 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 3.2.1 •「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）」 3.2.1 •「IoTセキュリティガイドライン ver.1.0」 要点2
●災害による障害の発生しにくい設備の設置及び管理	•「JIS Q 27002:2014」 11.1.4 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 3.2.1 •「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）」 3.2.1
●装置の管理	•「JIS Q 27002:2014」 11.2.1, 11.2.3, 11.2.5 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 7.1.1, 7.1.2 •「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）」 7.1.1, 7.1.2 •「IoTセキュリティガイドライン ver.1.0」 要点2
（カ）運用時のセキュリティ管理	－
（略）	（略）
●ログ取得	•「JIS Q 27002:2014」 12.4.1 ～ 12.4.4 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 6.1.4 •「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）」 6.1.4 •「高度サイバー攻撃への対処におけるログの活用と分析方法」 •「IoTセキュリティガイドライン ver.1.0」 要点2
●運用ソフトウェアの管理	•「JIS Q 27002:2014」 12.5.1 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 5.2.3, 6.2.1 •「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）」 5.2.3, 6.2.1
●技術的脆弱性管理	•「JIS Q 27002:2014」 12.6.1 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 6.2.1 •「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）」 6.2.1 •「IoTセキュリティガイドライン ver.1.0」 要点17, 18, 21

現行	
（エ）暗号	－
●暗号を活用した情報管理	•「JIS Q 27002:2014」 10.1.1, 10.1.2, 18.1.5 •「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）」 6.1.5 •「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）」 6.1.5 •「輸出貿易管理令別表第1第9項(7) 暗号装置又はその部分品」
（オ）物理的及び環境的セキュリティ	－
●セキュリティ確保が求められる領域	•「JIS Q 27002:2014」 11.1.1 ～ 11.1.6 •「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）」 3.2.1 •「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）」 3.2.1 •「IoTセキュリティガイドライン ver.1.0」 要点2
（新設）	
●装置の管理	•「JIS Q 27002:2014」 11.2.1, 11.2.3, 11.2.5 •「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）」 7.1.1, 7.1.2 •「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）」 7.1.1, 7.1.2 •「IoTセキュリティガイドライン ver.1.0」 要点2
（カ）運用時のセキュリティ管理	－
（略）	（略）
●ログ取得	•「JIS Q 27002:2014」 12.4.1 ～ 12.4.4 •「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）」 6.1.4 •「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）」 6.1.4 •「高度サイバー攻撃への対処におけるログの活用と分析方法」 •「IoTセキュリティガイドライン ver.1.0」 要点2
●運用ソフトウェアの管理	•「JIS Q 27002:2014」 12.5.1 •「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）」 5.2.3, 6.2.1 •「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）」 5.2.3, 6.2.1
●技術的脆弱性管理	•「JIS Q 27002:2014」 12.6.1 •「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）」 6.2.1 •「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）」 6.2.1 •「IoTセキュリティガイドライン ver.1.0」 要点17, 18, 21

改定案	
（キ）通信のセキュリティ	－
●ネットワークセキュリティ管理	•「JIS Q 27002:2014」 13.1.1 ～ 13.1.3 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 7.3.1 •「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）」 7.3.1
●情報の転送	•「JIS Q 27002:2014」 13.2.1 ～ 13.2.3 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 7.1.3, 7.2.1 •「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）」 7.1.3, 7.2.1
（ク）システムの取得、開発及び保守	－
●情報セキュリティ要件を踏まえた情報システムの取得	•「JIS Q 27002:2014」 14.1.1 ～ 14.1.3, 14.2.1 ～ 14.2.9, 14.3.1 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 5.2.1, 5.2.2 •「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）」 5.2.1, 5.2.2 •「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」 4.1, 4.2 •「IT製品の調達におけるセキュリティ要件リスト」 •「IT製品の調達におけるセキュリティ要件リスト活用ガイドブック」 •「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」 •「IoTセキュリティガイドライン ver.1.0」 要点8 ～ 16
（ケ）供給者関係	－
●供給者関係における情報セキュリティ	•「JIS Q 27002:2014」 15.1.1 ～ 15.1.3 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 4.1.1, 4.1.4 •「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）」 4.1.1, 4.1.4
●供給者のサービス提供の管理	•「JIS Q 27002:2014」 15.2.1, 15.2.2 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 4.1.1, 4.1.4 •「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）」 4.1.1, 4.1.4
（コ）情報セキュリティインシデント管理	－
●情報セキュリティインシデントの管理及びその改善	•「JIS Q 27002:2014」 16.1.1, 16.1.2, 16.1.6, 16.1.7 •「政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）」 2.2.4 •「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）」 2.2.4
（３）セキュリティ管理策に係る個別方針の策定	•「JIS Q 27002:2014」 5.1.1, 5.1.2
(略)	(略)

現行	
（キ）通信のセキュリティ	－
●ネットワークセキュリティ管理	•「JIS Q 27002:2014」 13.1.1 ～ 13.1.3 •「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）」 7.3.1 •「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）」 7.3.1
●情報の転送	•「JIS Q 27002:2014」 13.2.1 ～ 13.2.3 •「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）」 7.1.3, 7.2.1 •「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）」 7.1.3, 7.2.1
（ク）システムの取得、開発及び保守	－
●情報セキュリティ要件を踏まえた情報システムの取得	•「JIS Q 27002:2014」 14.1.1 ～ 14.1.3, 14.2.1 ～ 14.2.9, 14.3.1 •「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）」 5.2.1, 5.2.2 •「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）」 5.2.1, 5.2.2 •「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」 4.1, 4.2 •「IT製品の調達におけるセキュリティ要件リスト」 •「IT製品の調達におけるセキュリティ要件リスト活用ガイドブック」 •「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」 •「IoTセキュリティガイドライン ver.1.0」 要点8 ～ 16
（ケ）供給者関係	－
●供給者関係における情報セキュリティ	•「JIS Q 27002:2014」 15.1.1 ～ 15.1.3 •「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）」 4.1.1, 4.1.4 •「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）」 4.1.1, 4.1.4
●供給者のサービス提供の管理	•「JIS Q 27002:2014」 15.2.1, 15.2.2 •「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）」 4.1.1, 4.1.4 •「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）」 4.1.1, 4.1.4
（コ）情報セキュリティインシデント管理	－
●情報セキュリティインシデントの管理及びその改善	•「JIS Q 27002:2014」 16.1.1, 16.1.2, 16.1.6, 16.1.7 •「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）」 2.2.4 •「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）」 2.2.4
（３）リスク管理策に係る個別方針の策定	•「JIS Q 27002:2014」 5.1.1, 5.1.2
(略)	(略)

改定案

（略）

定義・用語集

（略）	（略）
重要インフラ分野	重要インフラについて業種ごとに分野と指定しているものであり、具体的には、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」。
（略）	（略）

参考文献

（略）

- サイバーセキュリティ戦略本部. 政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）. 2018-07-25. https://www.nisc.go.jp/active/general/pdf/kijyun28.pdf
- 内閣官房 内閣サイバーセキュリティセンター. 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）. 2018-07-25. https://www.nisc.go.jp/active/general/pdf/guide28.pdf

（略）

現行

（略）

定義・用語集

（略）	（略）
重要インフラ分野	重要インフラについて業種ごとに分野と指定しているものであり、具体的には、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」。
（略）	（略）

参考文献

（略）

- サイバーセキュリティ戦略本部. 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）. 2016-08-31. https://www.nisc.go.jp/active/general/pdf/kijyun28.pdf
- 内閣官房 内閣サイバーセキュリティセンター. 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）. 2016-08-31. https://www.nisc.go.jp/active/general/pdf/guide28.pdf

（略）