



内閣サイバーセキュリティセンター
National center of Incident readiness and
Strategy for Cybersecurity

資料 2

サイバーセキュリティ戦略本部 重要インフラ専門調査会（第29回）

重要インフラにおける 安全基準等の継続的改善状況等に関する調査について [2021年度]

令和 4 年 5 月 30 日

内閣サイバーセキュリティセンター
重要インフラグループ

- 内閣官房では、**我が国の重要インフラ防護能力の維持・向上を目的に**、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を「**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）**」（サイバーセキュリティ戦略本部 平成30年4月決定・令和元年5月改定。以下「指針」という。）**として取りまとめている。**
- 内閣官房が各重要インフラ分野の安全基準等の現状を把握し、安全基準等の継続的な改善を促していくため、**本調査では、重要インフラ所管省庁等における安全基準等の分析・検証や改定の状況、指針への対応状況等を確認する。**

安全基準等の継続的改善

- 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



【安全基準等とは】

- 関係法令に基づき国が定める「強制基準」
- 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業界横断的な「業界標準」及び「ガイドライン」
- 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

調査対象

- 重要インフラ所管省庁及び重要インフラ事業者の業界団体が制定する安全基準等（全14分野31件）

※ 調査対象は2ページ参照

調査項目

- ① 各安全基準等の**分析・検証**の状況
- ② 各安全基準等の**改定**の状況
- ③ 各安全基準等の**指針への対応**の状況

【参考：本調査の実施根拠】

○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

- Ⅲ. 1. 1.2 安全基準等の継続的改善
重要インフラ事業者等及び重要インフラ所管省庁は、重要インフラ全体の防護能力の維持・向上を目的とし、各重要インフラ事業者等の対策の経験から得た知見等をもとに、継続的に安全基準等を改善する。

（中略）

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、その結果を公表する。

分野		安全基準等の名称
情報通信	電気通信	<ul style="list-style-type: none"> ・ 事業用電気通信設備規則 ・ 情報通信ネットワーク安全・信頼性基準 ・ 電気通信分野における情報セキュリティ確保に係る安全基準（第4.2版）
	放送	<ul style="list-style-type: none"> ・ 放送法施行規則 ・ 放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン ・ 放送設備サイバー攻撃対策ガイドライン
	ケーブルテレビ	<ul style="list-style-type: none"> ・ 放送法施行規則 ※再掲 ・ ケーブルテレビにおける情報セキュリティ確保に係る安全基準等（第2版） ・ 電気通信分野における情報セキュリティ確保に係る安全基準（第4.2版） ※再掲 ・ 放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン ※再掲
金融	銀行等 生命保険 損害保険 証券	<ul style="list-style-type: none"> ・ 金融機関等コンピュータシステムの安全対策基準・解説書 ・ 金融機関等におけるセキュリティポリシー策定のための手引書 ・ 金融機関等におけるコンティンジェンシープラン策定のための手引書
航空		<ul style="list-style-type: none"> ・ 航空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（第5版）
空港		<ul style="list-style-type: none"> ・ 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（第2版）
鉄道		<ul style="list-style-type: none"> ・ 鉄道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（第4版）
電力		<ul style="list-style-type: none"> ・ 電気設備に関する技術基準を定める省令 ・ 電気事業法施行規則第50条第2項の解釈適用に当たっての考え方 ・ 電気設備の技術基準の解釈 ・ 電力制御システムセキュリティガイドライン ・ スマートメーターシステムセキュリティガイドライン
ガス		<ul style="list-style-type: none"> ・ ガス事業法施行規則 ・ 都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説
政府・行政サービス		<ul style="list-style-type: none"> ・ 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
医療		<ul style="list-style-type: none"> ・ 医療情報システムの安全管理に関するガイドライン（第5.1版）
水道		<ul style="list-style-type: none"> ・ 水道施設の技術的基準を定める省令 ・ 水道分野における情報セキュリティガイドライン（第4版）
物流		<ul style="list-style-type: none"> ・ 物流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（第4版）
化学		<ul style="list-style-type: none"> ・ 石油化学分野における情報セキュリティ確保に係る安全基準
クレジット		<ul style="list-style-type: none"> ・ クレジットCEPTOARにおける情報セキュリティガイドライン
石油		<ul style="list-style-type: none"> ・ 石油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

- 2021年度は、指針や関係法令・ガイドラインの改定等を契機として、**各重要インフラ分野で安全基準等の分析・検証が行われ**、それらの結果を踏まえ**7件の改定が実施**された。
- また、各安全基準等のそれぞれの制定主体において、**各重要インフラ分野の安全基準等の指針への対応について確認**が行われている。

分析・検証の主な契機・内容等

- 指針や関係法令・ガイドラインの改定等に伴う安全基準等への影響を踏まえた分析・検証及び見直し
- 近年の社会的・技術的な環境の変化を踏まえた安全基準等の分析・検証及び見直し

【社会的・技術的な環境の変化の例】

- ・ ランサムウェア等によるサイバー攻撃の増加
- ・ サイバーセキュリティを巡る脅威の巧妙化・複雑化
- ・ 関与するステークホルダーの増加・サービスの複雑化
- ・ ネットワーク及びシステムのソフトウェア化・仮想化の進展
- ・ クラウドサービスの利用の拡大
- ・ 重要インフラサービスの安全かつ継続的な提供に影響を与える自然災害の増加
- ・ テレワークやBYOD(私有端末の持込み利用)等の進展

指針への対応

- 各安全基準等の制定主体において**指針の内容が分析・検証**され、必要に応じて**安全基準等の改定が行われている**（※）ことを確認。

（※）分析・検証の結果、自分分野の安全基準等に反映の必要がないとした項目は除く。

主な改定

- **指針や関係法令・ガイドラインの改定に伴う改定**
 - 電気通信分野における情報セキュリティ確保に係る安全基準（第4.2版）
 - 電気設備の技術基準の解釈
- **社会的・技術的な環境の変化を踏まえた改定**
 - 金融機関等コンピュータシステムの安全対策基準・解説書
 - 医療情報システムの安全管理に関するガイドライン（第5.1版）
 - 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
- **その他**
 - 情報通信ネットワーク安全・信頼性基準
 - ケーブルテレビにおける情報セキュリティ確保に係る安全基準等（第2版）

重要インフラ所管省庁及び重要インフラ事業者等で構成される業界団体において、各安全基準等の分析・検証や改定が行われ、**安全基準等の継続的な改善が着実に実施**されていることを確認。

(参考) 2021年度における各安全基準等の改善状況

(目次)

情報通信 (電気通信)

- 事業用電気通信設備規則 … 5
- 情報通信ネットワーク安全・信頼性基準 … 5
- 電気通信分野における情報セキュリティ確保に係る安全基準 (第4.2版) … 6

情報通信 (放送)

- 放送法施行規則 … 6
- 放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン … 7
- 放送設備サイバー攻撃対策ガイドライン … 7

情報通信 (ケーブルテレビ)

- 放送法施行規則 … 8
- ケーブルテレビにおける情報セキュリティ確保に係る安全基準等 (第2版) … 8

金融

- 金融機関等コンピュータシステムの安全対策基準・解説書 … 9
- 金融機関等におけるセキュリティポリシー策定のための手引書 … 9
- 金融機関等におけるコンティンジェンシープラン策定のための手引書 … 10

航空

- 航空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 (第5版) … 10

空港

- 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 (第2版) … 11

鉄道

- 鉄道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 (第4版) … 11

電力

- 電気設備に関する技術基準を定める省令 … 12
- 電気事業法施行規則第50条第2項の解釈適用に当たっての考え方 … 12
- 電気設備の技術基準の解釈 … 13
- 電力制御システムセキュリティガイドライン … 13
- スマートメーターシステムセキュリティガイドライン … 14

ガス

- ガス事業法施行規則 … 14
- 都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説 … 15

政府・行政サービス

- 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 … 15

医療

- 医療情報システムの安全管理に関するガイドライン (第5.1版) … 16

水道

- 水道施設の技術的基準を定める省令 … 16
- 水道分野における情報セキュリティガイドライン (第4版) … 17

物流

- 物流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 (第4版) … 17

化学

- 石油化学分野における情報セキュリティ確保に係る安全基準 … 18

クレジット

- クレジットCEPTOARにおける情報セキュリティガイドライン … 18

石油

- 石油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 … 19

安全基準等の名称	事業用電気通信設備規則	情報通信ネットワーク安全・信頼性基準	
重要インフラ分野	情報通信（電気通信）	情報通信（電気通信）	
制定主体	総務省	総務省	
最終改正（初版制定）年月	2021年4月（初版制定：1985年4月）	2021年4月（初版制定：1987年2月）	
安全基準等の位置付け	関係法令に基づき国が定める 強制基準	関係法令に準じて国が定める 推奨基準・ガイドライン	
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	実施	
	分析・検証の内容や主な理由・契機	<ul style="list-style-type: none"> ◆ 通信ネットワークの仮想化技術の進展とともに、関与するステークホルダーの増加、電気通信サービスの提供構造の複雑化等が見られ、電気通信サービスの停止のリスクが高まっていることから、電気通信事業法上の設備規律等が、電気通信サービスの安定的な提供を維持する上で将来的にも有効に機能するかどうかという観点から検証を実施。電気通信サービスの主な用途が音声通話からデータ通信へとシフトしている現状を踏まえ、引き続き検討を実施予定。 	—
	改定の実施状況	なし	実施
	改定の主な内容	—	<ul style="list-style-type: none"> ◆ 電気通信事業法及び日本電信電話株式会社等に関する法律の一部を改正する法律（令和2年法律第30号）の施行に伴う条ずれ等の改正。
	改定の際に参考としている基準・規格（指針除く）	—	—
(2) 指針との対応	確認済み	確認済み	

安全基準等の名称		電気通信分野における情報セキュリティ確保に係る安全基準（第4.2版）	放送法施行規則
重要インフラ分野		情報通信（電気通信）	情報通信（放送）
制定主体		一般社団法人電気通信事業者協会	総務省
最終改正（初版制定）年月		2021年12月（初版制定：2006年9月）	2021年12月（初版制定：1950年6月）
安全基準等の位置付け		業界団体等が定める業界横断的な 業界標準・ガイドライン	関係法令に基づき国が定める 強制基準
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	実施	なし
	分析・検証の内容や主な理由・契機	<ul style="list-style-type: none"> ◆ 以下の関連する法令・ガイドライン等の改定の確認、分析・検証等を実施。 <ul style="list-style-type: none"> ✓ NISC重要インフラ行動計画・指針 ✓ ISO/IEC (27001 27002 27017) ✓ 電気通信分野の関係法令（電気通信事業法等） ✓ 個人情報保護関連ガイドライン等（GDPR等含む） ✓ その他（ISMAP等） 	—
	改定の実施状況	実施	なし（サイバーセキュリティに関する箇所に限る）
	改定の主な内容	<ul style="list-style-type: none"> ◆ 「政府機関等のサイバーセキュリティ対策のための統一基準」を踏まえた改版 <ul style="list-style-type: none"> ✓ 「情報の抹消」に「暗号化消去」を追記 ✓ 情報自体の消去の他に、暗号化に使用した暗号鍵の消去等を追記 ◆ 「既存の法令・ガイドライン等」を更新 <ul style="list-style-type: none"> ✓ 外国の個人情報保護に関する法律・ガイドライン等（新規） ✓ 帯域制御の運用基準に関するガイドライン（更新） ✓ 政府情報システムのためのセキュリティ評価制度（新規） 等 	—
改定の際に参考としている基準・規格（指針除く）	<ul style="list-style-type: none"> • NISC「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」 • ISO/IEC (27001:2013 27002:2013 27017:2015) • 電気通信事業法・規則・施行令等 • NISC「政府機関等のサイバーセキュリティ対策のための統一基準」 	—	
(2) 指針との対応		確認済み	確認済み

安全基準等の名称	放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン	放送設備サイバー攻撃対策ガイドライン
重要インフラ分野	情報通信（放送）	情報通信（放送）
制定主体	一般社団法人ICT-ISAC	一般社団法人ICT-ISAC
最終改正（初版制定）年月	2020年9月（初版制定：2005年10月）	2020年2月（初版制定：2018年6月）
安全基準等の位置付け	業界団体等が定める業界横断的な 業界標準・ガイドライン	業界団体等が定める業界横断的な 業界標準・ガイドライン
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	なし
	分析・検証の内容や主な理由・契機	（2020年9月に改定を行っており、改定が必要となる環境変化等はないと判断したため。今後必要に応じて分析・検証を実施。）
	改定の実施状況	なし
	改定の主な内容	—
	改定の際に参考としている基準・規格（指針除く）	—
(2) 指針との対応	確認済み	確認済み

安全基準等の名称		放送法施行規則	ケーブルテレビにおける情報セキュリティ確保に係る安全基準等（第2版）
重要インフラ分野		情報通信（ケーブルテレビ）	情報通信（ケーブルテレビ）
制定主体		総務省	ケーブルテレビセプター
最終改正（初版制定）年月		2021年12月（初版制定：1950年6月）	2021年9月（初版制定：2012年11月）
安全基準等の位置付け		関係法令に基づき国が定める 強制基準	業界団体等が定める業界横断的な 業界標準・ガイドライン
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	なし	実施
	分析・検証の内容や主な理由・契機	—	<ul style="list-style-type: none"> ◆ 安全基準等策定指針（第5版）との対応をとるべく検討を実施。ケーブルテレビ事業者は放送事業に加え、電気通信事業を提供していることから、関連セプターと協議を実施。
	改定の実施状況	なし（サイバーセキュリティに関係する箇所に限る）	実施
	改定の主な内容	—	<ul style="list-style-type: none"> ◆ 目次やPDCAを考慮した内容等を指針に準じた内容に改定しつつ、ケーブルテレビ事業者の事業内容、組織、システム等に関して具体化。 ◆ 電気通信事業及び放送事業に係る安全基準を掲載し、提供する事業分野に応じた参照を推奨する旨を記載。
	改定の際に参考としている基準・規格（指針除く）	—	<ul style="list-style-type: none"> ・ 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 ・ 放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン ・ 電気通信分野における情報セキュリティ確保に係る安全基準
(2) 指針との対応	確認済み	確認済み	

安全基準等の名称		金融機関等コンピュータシステムの安全対策基準・解説書	金融機関等におけるセキュリティポリシー策定のための手引書
重要インフラ分野		金融	金融
制定主体		公益財団法人金融情報システムセンター（FISC）	公益財団法人金融情報システムセンター（FISC）
最終改正（初版制定）年月		2021年12月（初版制定：1985年12月）	2008年6月（初版制定：1999年1月）
安全基準等の位置付け		業界団体等が定める業界横断的な 業界標準・ガイドライン	業界団体等が定める業界横断的な 業界標準・ガイドライン
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	実施	実施
	分析・検証の内容や主な理由・契機	<ul style="list-style-type: none"> ◆ ①新型コロナウイルス感染拡大に伴い、就業形態としてテレワークが急速に普及したことによるセキュリティリスクが増大していること、②金融機関と資金移動業者が連携して提供するサービスにおいて、口座振替による不正出金の事案が多発したこと、③新技術の開発、新たなサイバー攻撃手口の出現に伴い、従来の対策では不十分とみられる事象が常に出現している可能性があることを踏まえ、以下の分析・検証を実施。 <ul style="list-style-type: none"> ✓ 金融機関等でのテレワーク普及に鑑み、テレワークにおけるサイバーセキュリティに関する課題を調査。 ✓ 口座振替による不正出金事案発生に伴い、同事案が発生した原因を調査。 ✓ 金融機関等で発生したサイバー攻撃に関する事案をもとに、新たな安全対策の過不足を確認。 ✓ 関連するガイドラインやセキュリティインシデント事案を踏まえ、サイバーセキュリティに関する態勢や対策の整備状況を分析。 	<ul style="list-style-type: none"> ◆ ①新型コロナウイルス感染拡大に伴い、就業形態としてテレワークが急速に普及したことによるセキュリティリスクが増大していること、②金融機関と資金移動業者が連携して提供するサービスにおいて、口座振替による不正出金の事案が多発したこと、③新技術の開発、新たなサイバー攻撃手口の出現に伴い、従来の対策では不十分とみられる事象が常に出現している可能性があることを踏まえ、以下の分析・検証を実施。 <ul style="list-style-type: none"> ✓ 金融機関等でのテレワーク普及に鑑み、テレワークにおけるサイバーセキュリティに関する課題を調査。 ✓ 口座振替による不正出金事案発生に伴い、同事案が発生した原因を調査。 ✓ 金融機関等で発生したサイバー攻撃に関する事案をもとに、新たな安全対策の過不足を確認。 ✓ 関連するガイドラインやセキュリティインシデント事案を踏まえ、サイバーセキュリティに関する態勢や対策の整備状況を分析。
	改定の実施状況	実施	なし
	改定の主な内容	<ul style="list-style-type: none"> ◆ テレワークの普及による改正 <ul style="list-style-type: none"> ✓ ハードウェアの管理、アクセス制御、暗号化等の対策の実施 ✓ 物理的及びWeb会議における情報漏えい防止措置 ✓ スマートデバイスの取扱いに関する対策の追記 ◆ 資金移動業者との連携に関する改正 <ul style="list-style-type: none"> ✓ FinTech企業等との連携に関する固有のリスクを把握した安全対策の実施 ✓ QRコード決済における安全対策の実施 ✓ 本人確認機能における注意事項の追記 	—
改定の際に参考としている基準・規格（指針除く）	—	—	
(2) 指針との対応		確認済み	確認済み

安全基準等の名称		金融機関等におけるコンティンジェンシープラン策定のための手引書	航空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（第5版）
重要インフラ分野		金融	航空
制定主体		公益財団法人金融情報システムセンター（FISC）	国土交通省
最終改正（初版制定）年月		2017年5月（初版制定：1994年1月）	2019年3月（初版制定：2006年9月）
安全基準等の位置付け		業界団体等が定める業界横断的な 業界標準・ガイドライン	関係法令に準じて国が定める 推奨基準・ガイドライン
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	実施	実施
	分析・検証の内容や主な理由・契機	<ul style="list-style-type: none"> ◆ ①新型コロナウイルス感染拡大に伴い、就業形態としてテレワークが急速に普及したことによるセキュリティリスクが増大していること、②金融機関と資金移動業者が連携して提供するサービスにおいて、口座振替による不正出金の事案が多発したこと、③新技術の開発、新たなサイバー攻撃手口の出現に伴い、従来の対策では不十分とみられる事象が常に出現している可能性があることを踏まえ、以下の分析・検証を実施。 <ul style="list-style-type: none"> ✓ 金融機関等でのテレワーク普及に鑑み、テレワークにおけるサイバーセキュリティに関する課題を調査。 ✓ 口座振替による不正出金事案発生に伴い、同事案が発生した原因を調査。 ✓ 金融機関等で発生したサイバー攻撃に関する事案をもとに、新たな安全対策の過不足を確認。 ✓ 関連するガイドラインやセキュリティインシデント事案を踏まえ、サイバーセキュリティに関する態勢や対策の整備状況を分析。 	<ul style="list-style-type: none"> ◆ 新たなデジタル技術に対応する内容を分析・検証し、見直した項目について事業者へ意見要望等を聴取したうえで改定案を検討した。（次期行動計画等が策定される2022年度内に改定する予定。）
	改定の実施状況	なし	なし
	改定の主な内容	—	—
	改定の際に参考としている基準・規格（指針除く）	—	・ 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（サイバーセキュリティ戦略本部）
(2) 指針との対応		確認済み	確認済み

安全基準等の名称		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（第2版）	鉄道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（第4版）
重要インフラ分野		空港	鉄道
制定主体		国土交通省	国土交通省
最終改正（初版制定）年月		2019年3月（初版制定：2018年4月）	2019年3月（初版制定：2006年9月）
安全基準等の位置付け		関係法令に準じて国が定める 推奨基準・ガイドライン	関係法令に準じて国が定める 推奨基準・ガイドライン
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	実施	実施
	分析・検証の内容や主な理由・契機	◆ 新たなデジタル技術に対応する内容を分析・検証し、見直した項目について事業者へ意見要望等を聴取したうえで改定案を検討した。 (次期行動計画等が策定される2022年度内に改定する予定。)	◆ 新たなデジタル技術に対応する内容を分析・検証し、見直した項目について事業者へ意見要望等を聴取したうえで改定案を検討した。 (次期行動計画等が策定される2022年度内に改定する予定。)
	改定の実施状況	なし	なし
	改定の主な内容	—	—
	改定の際に参考としている基準・規格（指針除く）	・ 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（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群（サイバーセキュリティ戦略本部）
(2) 指針との対応		確認済み	確認済み

安全基準等の名称	電気設備に関する技術基準を定める省令	電気事業法施行規則第50条第2項の解釈適用に当たっての考え方
重要インフラ分野	電力	電力
制定主体	経済産業省	経済産業省
最終改正（初版制定）年月	2021年4月（初版制定：1997年3月）	2021年3月（初版制定：2016年9月）
安全基準等の位置付け	関係法令に基づき国が定める 強制基準	関係法令に準じて国が定める 推奨基準・ガイドライン
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	なし
	分析・検証の内容や主な理由・契機	<ul style="list-style-type: none"> ◆ 2022年4月の配電事業者制度開始に伴う改正を検討。 ◆ スマート保安技術の導入に伴う自家用電気工作物におけるサイバーセキュリティの確保のための検討を実施。
	改定の実施状況	なし（サイバーセキュリティに関係する箇所に限る）
	改定の主な内容	—
改定の際に参考としている基準・規格（指針除く）	<ul style="list-style-type: none"> ・ 日本産業規格JIS、日本電気技術規格委員会規格JESC等 	<ul style="list-style-type: none"> ・ JESC Z0004（電力制御システムセキュリティガイドライン） ・ JESC Z0003（スマートメーターシステムセキュリティガイドライン）
(2) 指針との対応	確認済み	確認済み

安全基準等の名称	電気設備の技術基準の解釈	電力制御システムセキュリティガイドライン	
重要インフラ分野	電力	電力	
制定主体	経済産業省	一般社団法人日本電気協会	
最終改正（初版制定）年月	2021年5月（初版制定：2013年3月）	2019年7月（初版制定：2016年5月）	
安全基準等の位置付け	関係法令に準じて国が定める 推奨基準・ガイドライン	業界団体等が定める業界横断的な 業界標準・ガイドライン	
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	実施	
	分析・検証の内容や主な理由・契機	<ul style="list-style-type: none"> ◆ 火力発電所の常時監視制御の遠隔化に向けて、常時監視と同等な監視を確実に実行できるよう発電所施設の保安要件の追加を検討。 ◆ その他、電気設備のうち新たに太陽電池発電設備に特化した「発電用太陽電池設備に関する技術基準を定める省令」及び「発電用太陽電池設備の技術基準の解釈」を制定したことに伴う改正の検討、各種規格（JIS、JESC、IEC等）の更新の反映を実施。 	（2019年度に改定を実施。次回改定に向け、規格関連情報を収集）
	改定の実施状況	実施	なし
	改定の主な内容	<ul style="list-style-type: none"> ◆ 火力発電所における遠隔常時監視制御の導入に向けた対応等の改正を実施。（2021年4月） ◆ 各種規格（JIS、JESC、IEC等）の更新に伴う改正を実施。（2021年5月） 	—
改定の際に参考としている基準・規格（指針除く）	・ 日本産業規格JIS、日本電気技術規格委員会規格JESC等	—	
(2) 指針との対応	確認済み	確認済み	

安全基準等の名称		スマートメーターシステムセキュリティガイドライン	ガス事業法施行規則
重要インフラ分野		電力	ガス
制定主体		一般社団法人日本電気協会	経済産業省
最終改正（初版制定）年月		2019年7月（初版制定：2016年3月）	2019年4月（初版制定：1970年10月）
安全基準等の位置付け		業界団体等が定める業界横断的な 業界標準・ガイドライン	関係法令に基づき国が定める 強制基準
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	なし	なし
	分析・検証の内容や主な理由・契機	（2019年度に改定を行っており、改定が必要となる環境変化等はないと判断したため。）	—
	改定の実施状況	なし	なし
	改定の主な内容	—	—
	改定の際に参考としている基準・規格（指針除く）	—	—
(2) 指針との対応		確認済み	確認済み

安全基準等の名称		都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説	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
重要インフラ分野		ガス	政府・行政サービス
制定主体		一般社団法人日本ガス協会	総務省
最終改正（初版制定）年月		2021年3月（初版制定：2019年3月）	2022年3月（初版制定：2001年3月）
安全基準等の位置付け		業界団体等が定める業界横断的な 業界標準・ガイドライン	関係法令に準じて国が定める 推奨基準・ガイドライン
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	実施	実施
	分析・検証の内容及び主な理由・契機	<ul style="list-style-type: none"> ◆ 2021年3月の改正において、サイバー事故発生時における当協会連絡先を変更し、その実効性（事業者への浸透状況）を情報連絡訓練や分野横断的演習、セプター訓練により検証を実施した。 ◆ 訓練参加事業者は、安全基準等に基づいた連絡先に情報連絡を行っており、改定した内容が事業者に広く浸透していることを確認 	<ul style="list-style-type: none"> ◆ 2021年度の「政府機関等のサイバーセキュリティ対策のための統一基準群」の改定や、地方公共団体におけるデジタル化の動向を受け、以下について検討・分析を実施。 <ul style="list-style-type: none"> ✓ 外部サービス利用時のライフサイクルに渡るセキュリティ要件や利用承認手続きについて ✓ クラウドサービスの選定における指標・基準としての監査報告書や第三者認証制度の活用について ✓ テレワーク実施場所等の運用面に関するセキュリティ対策について ✓ マイナンバー利用事務系と外部接続先（eLTAX、マイナポータル）との双方向通信について
	改定の実施状況	なし	実施
	改定の主な内容	—	<ul style="list-style-type: none"> ◆ 分析・検証の結果を踏まえ、以下の改定を実施。 <ul style="list-style-type: none"> ✓ 業務委託・外部サービス利用時の情報資産の取扱い ✓ 監視体制やCSIRTとの連携等の組織的な対応の必要性 ✓ テレワークやBYOD利用時の情報セキュリティ対策 ✓ マイナンバー利用事務系の分離の見直し ◆ 2021年度の「政府機関等の情報セキュリティ対策のための統一基準」の改定の内容を反映。
	改定の際に参考としている基準・規格（指針除く）	—	<ul style="list-style-type: none"> • 政府機関等のサイバーセキュリティ対策のための統一基準群 • ISO/IEC 27017（安全なクラウドサービス利用のための分野別ISMS規格） • 政府情報システムのためのセキュリティ評価制度（ISMAP）
(2) 指針との対応		確認済み	確認済み

安全基準等の名称		医療情報システムの安全管理に関するガイドライン（第5.1版）	水道施設の技術的基準を定める省令
重要インフラ分野		医療	水道
制定主体		厚生労働省	厚生労働省
最終改正（初版制定）年月		2022年3月（初版制定：2005年3月）	2020年4月（初版制定：2000年2月）
安全基準等の位置付け		関係法令に準じて国が定める 推奨基準・ガイドライン	関係法令に基づき国が定める 強制基準
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	実施	なし
	分析・検証の内容や主な理由・契機	◆ 2021年1月に改定した第5.1版の改定にあたり、ランサムウェアによる攻撃への対応、外部ネットワーク接続が可能であることを分かりやすく記載することの必要性等について、制度的、技術的な動向や「規制改革実施計画」を踏まえ、改定する項目がないか分析・検証を実施。	—
	改定の実施状況	実施	なし
	改定の主な内容	<ul style="list-style-type: none"> ◆ 医療機関等を対象とするサイバー攻撃の多様化・巧妙化、特にランサムウェアに代表される攻撃への対策に対応するとともに、制度的、技術的な動向等をふまえ、以下の改定を実施。 ✓ ランサムウェア攻撃への対策としてバックアップの在り方、被害に遭った際の対策を速やかに講じられるような体制整備 ✓ 外部サービスとの連携について、アプリケーション間の認証・認可に関する記述 ✓ BYODの利用に関する追記 ✓ 電子署名に関する法的な記載や要件についての記載を整理 ✓ 電子署名に関する暗号アルゴリズムについて、参照規格の変更 等 	—
	改定の際に参考としている基準・規格（指針除く）	・ 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン	—
(2) 指針との対応		確認済み	確認済み

安全基準等の名称	水道分野における情報セキュリティガイドライン（第4版）	物流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（第4版）	
重要インフラ分野	水道	物流	
制定主体	厚生労働省	国土交通省	
最終改正（初版制定）年月	2019年3月（初版制定：2006年10月）	2019年3月（初版制定：2006年9月）	
安全基準等の位置付け	関係法令に準じて国が定める 推奨基準・ガイドライン	関係法令に準じて国が定める 推奨基準・ガイドライン	
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	なし	実施
	分析・検証の内容や主な理由・契機	（2019年度に改定を行っており、改定が必要となる環境変化等はないと判断したため。）	（新たなデジタル技術に対応するため、2022年度中に改定を行うことを目指し、分析・検証の内容、改定案等について検討を実施。）
	改定の実施状況	なし	なし
	改定の主な内容	—	—
	改定の際に参考としている基準・規格（指針除く）	—	・ 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（サイバーセキュリティ戦略本部）
(2) 指針との対応	確認済み	確認済み	

安全基準等の名称	石油化学分野における情報セキュリティ確保に係る安全基準	クレジットCEPTOARにおける情報セキュリティガイドライン
重要インフラ分野	化学	クレジット
制定主体	石油化学工業協会	一般社団法人日本クレジット協会
最終改正（初版制定）年月	2019年5月（初版制定：2015年3月）	2018年4月（初版制定：2014年12月）
安全基準等の位置付け	業界団体等が定める業界横断的な 業界標準・ガイドライン	業界団体等が定める業界横断的な 業界標準・ガイドライン
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	なし
	分析・検証の内容や主な理由・契機	（2019年度に改定を行っており、改定が必要となる環境変化等はないと判断したため。）
	改定の実施状況	なし
	改定の主な内容	—
	改定の際に参考としている基準・規格（指針除く）	—
(2) 指針との対応	確認済み	確認済み

安全基準等の名称		石油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
重要インフラ分野		石油
制定主体		石油連盟
最終改正（初版制定）年月		2020年3月（初版制定：2015年3月）
安全基準等の位置付け		業界団体等が定める業界横断的な 業界標準・ガイドライン
(1) 安全基準等の改善に関する取組	分析・検証の実施状況	なし
	分析・検証の内容や 主な理由・契機	（2019年度末に改定を行い、次回改定は第4次重要インフラ行動計画の改定後の安全基準等策定指針の改定を踏まえて行う予定であり、前倒しての改定が必要となる環境変化等はないと判断したため。）
	改定の実施状況	なし
	改定の主な内容	—
	改定の際に参考としている 基準・規格（指針除く）	—
(2) 指針との対応		確認済み