NISC 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25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［2020年度］

令和３年５月31日

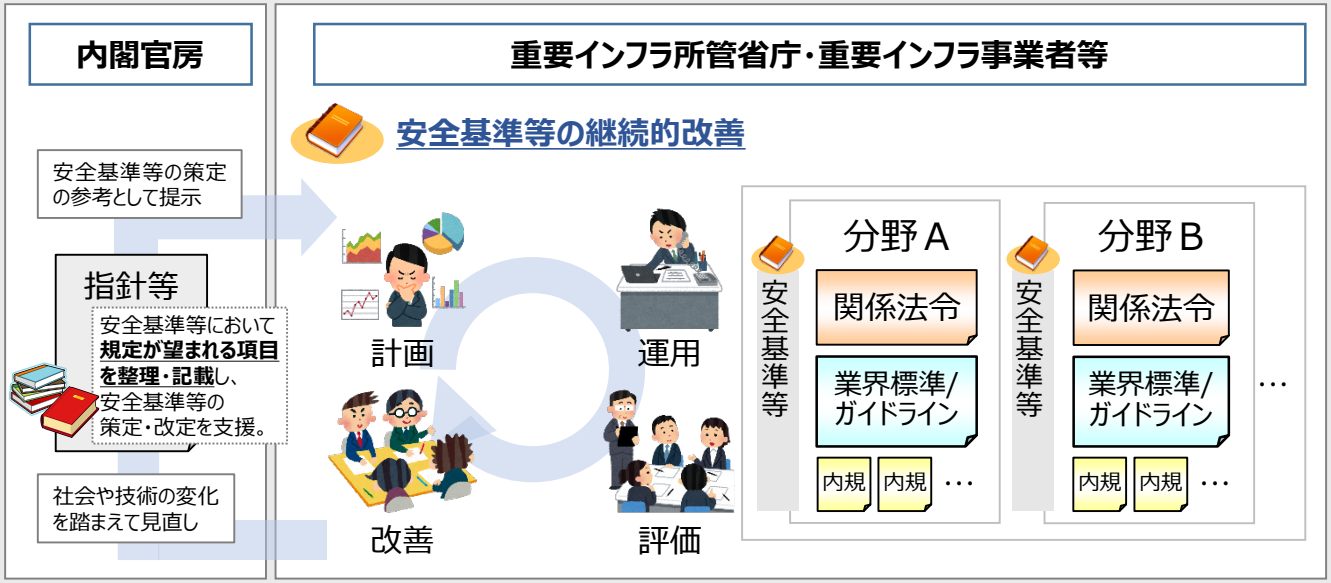
内閣サイバーセキュリティセンター
重要インフラグループ

調査概要

- 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26件）

※ 調査対象は02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】
〇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。

調査対象一覧（全14分野26件）

分野		安全基準等の名称
情報通信	電気通信	• 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4.1版）
	放送	• 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	• ケーブルテレビの情報セキュリティ確保に係る「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（第4.1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	• 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コンティンジェンシープラン策定のための手引書
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）
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）
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）
電力		• 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		• 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		• 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		• 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		• 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		• 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		• 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		• 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		• 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

調査結果

- 2020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**８件の改定が実施**（※）された。　※ うち１件は2021年４月１日の改定
- 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】
- 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
- 業務のデジタル化等の進展
- 新型コロナウイルス感染症の拡大　等

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**安全基準等を改定が行われている**（※）ことを確認 。

（※）分析・検証の結果、自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**
  - 事業用電気通信設備規則
  - 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
- **社会的・技術的な環境の変化を踏まえた改定**
  - 情報通信ネットワーク安全・信頼性基準
  - 電気設備の技術基準の解釈
  - 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）
- **その他**
  - 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
  - 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

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）2020年度における各安全基準等の改善状況

（目次）

各安全基準等の改善状況 [1/12]

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）	2020年６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**	**実施**
	分析・検証の内容や主な理由・契機	◆ 加入電話のアクセス区間の一部を無線で代替するワイヤレス固定電話の実現に向け、通信品質や重要通信の確保をはじめとする適切な技術的条件について検討を実施。 ◆ 通信ネットワークの本格的なソフトウェア化・仮想化の進展に対応した技術基準等の在り方について検討を実施。	◆ 通信ネットワーク内のソフトウェアの不具合や外部連携先の作業ミス等による事故が増加傾向にあること、仮想化技術の導入により同一のソフトウェアを利用するシステムが共倒れするなど被害が広範囲に及ぶこと、仮想化技術の導入やクラウド利用の進展に伴う故障箇所や原因の特定が困難になること、台風によって商用電源からの電力供給が長時間途絶して重要通信が維持できなかったこと等を踏まえ、その対策について分析・検証を実施。 ✓ 他社が提供する設備を利用する際のサービス全体の品質管理の在り方 ✓ 通信ネットワークの標準的なソフトウェアの評価・検証手法 ✓ 通信ネットワークのソフトウェア故障やクラウド故障が発生した際のサービス早期復旧に向けた手順等 ✓ 固定通信局舎や携帯電話基地局の商用電源の供給が途絶した場合における通信インフラの維持・管理方策
	改定の実施状況	**実施**	**実施**
	改定の主な内容	◆ 分析・検証の結果を踏まえ、事業用電気通信設備としてワイヤレス固定電話用設備を新たに定義し、同設備の技術基準として電気通信設備の損壊又は故障の対策、秘密の保持、他の電気通信設備の損傷又は機能の障害の防止等に関する項目を追加。	◆ 設備等基準及び管理基準として以下の対策項目を追加。 ✓ 電気通信事業者が他社のクラウド設備等を利用する場合でも通信ネットワーク全体として従来と同等の品質を確保するように取り組むこと ✓ 交換機等の制御等に用いられる重要なソフトウェアについて、その安全・信頼性を確保するため、電気通信事業者がソフトウェアを導入・更新する際に共通的に取り組むべき最低限の項目の検証を行うこと ✓ 防災上必要な通信を確保するために、都道府県庁、市役所又は町村役場の災害時における重要な対策拠点をカバーする通信設備の予備電源については、少なくとも「24時間」にわたる停電対策に取り組むこと ✓ 事前準備が可能である台風等の災害の場合は、各電気通信事業者による応急復旧対策として、移動電源車や予備ケーブル等の応急復旧資機材を被災が予想される地域の近くにあらかじめ配備することや、その運用に必要な人員の確保・配備に積極的に取り組むこと　　等
	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

各安全基準等の改善状況 [2/12]

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４.１版）	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
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	一般社団法人ICT-ISAC
最終改正（初版制定）年月			2020年３月（初版制定：2006年９月）	2020年９月（初版制定：2005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**	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	◆ 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。 ✓ 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）	◆ 指針の改定の反映、情報通信（ケーブルテレビ）分野の「ケーブルテレビの情報セキュリティ確保に係る『安全基準等』策定ガイドライン」の放送事業に係る部分と統合等のため分析・検証を実施。
	改定の実施状況		なし	**実施**
		改定の主な内容	（分析・検証の結果を踏まえ、2021年度中に改定を実施する予定。）	◆ 指針の改定を踏まえ、「データ管理」及び「災害による障害の発生しにくい設備設置及び管理」の項目を追加。 ◆ 情報通信（ケーブルテレビ）分野の「ケーブルテレビの情報セキュリティ確保に係る『安全基準等』策定ガイドライン」の放送事業に係る部分を統合し、更新。
		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

各安全基準等の改善状況 [3/12]

安全基準等の名称			放送設備サイバー攻撃対策ガイドライン	ケーブルテレビの情報セキュリティ確保に係る「安全基準等」策定ガイドライン
重要インフラ分野			情報通信（放送）	情報通信（ケーブルテレビ）
制定主体			一般社団法人ICT-ISAC	ケーブルテレビセプター
最終改正（初版制定）年月			2020年２月（初版制定：2018年６月）	2012年11月（初版）
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	**実施**
		分析・検証の内容や主な理由・契機	（2020年２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。）	◆ 放送事業について、本ガイドラインと情報通信（放送）分野の「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」を統合するため、分析・検証を実施。 ◆ 電気通信事業については、情報通信（電気通信）分野の「電気通信分野における情報セキュリティ対策に係る安全基準」を本ガイドラインの参照先とするため、分析・検証を実施。
	改定の実施状況		なし	なし
		改定の主な内容	—	◆ 放送事業に係る内容については、情報通信（放送）分野の「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」と統合。 ◆ 電気通信事業に係る内容については、情報通信（電気通信）分野の「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4.1版）」を参照。 （本ガイドラインについては、今回の統合等を踏まえて2021年度に改定を行い、引き続きケーブルテレビ分野の安全基準等として維持する予定。）
		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

各安全基準等の改善状況 [4/12]

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			2020年３月（初版制定：1980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	◆ 金融機関と貸資移動業者が連携して提供するサービスで口座振替による不正出金の事案が多発したこと、新型コロナウイルスの感染拡大状況下での対応において、従来のパンデミックを想定したBCPとの相違が明らかになるとともにテレワークの普及によってセキュリティリスクが増大したこと、金融機関等での基幹系システムも含めたクラウドサービスの利用が拡大して同サービスが原因となる重大障害が発生したことを踏まえ、以下の分析・検証を実施。 ✓ 金融機関等で発生した障害事例を踏まえた対策の過不足 ✓ 口座振替による不正出金に関する事案 ✓ 新型コロナウイルス感染症の感染拡大の状況下での金融機関等におけるBCPに基づいた対応の実態及びテレワークにおける課題 ✓ 関連するガイドラインやセキュリティインシデントを踏まえ、サイバーセキュリティに関する態勢や対策の整備状況 ✓ 金融機関等でクラウドサービスを利用する場合の留意点等	◆ 金融機関と貸資移動業者が連携して提供するサービスで口座振替による不正出金の事案が多発したこと、新型コロナウイルスの感染拡大状況下での対応において、従来のパンデミックを想定したBCPとの相違が明らかになるとともにテレワークの普及によってセキュリティリスクが増大したこと、金融機関等での基幹系システムも含めたクラウドサービスの利用が拡大して同サービスが原因となる重大障害が発生したことを踏まえ、以下の分析・検証を実施。 ✓ 金融機関等で発生した障害事例を踏まえた対策の過不足 ✓ 口座振替による不正出金に関する事案 ✓ 新型コロナウイルス感染症の感染拡大の状況下での金融機関等におけるBCPに基づいた対応の実態及びテレワークにおける課題 ✓ 関連するガイドラインやセキュリティインシデントを踏まえ、サイバーセキュリティに関する態勢や対策の整備状況 ✓ 金融機関等でクラウドサービスを利用する場合の留意点等
	改定の実施状況		なし	なし
		改定の主な内容	（口座振替による不正出金に対する金融情報システムへの安全対策等については、2021年度に改定して反映する予定。）	―
		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

各安全基準等の改善状況 [5/12]

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	◆ 金融機関と貸資移動業者が連携して提供するサービスで口座振替による不正出金の事案が多発したこと、新型コロナウイルスの感染拡大状況下での対応において、従来のパンデミックを想定したBCPとの相違が明らかになるとともにテレワークの普及によってセキュリティリスクが増大したこと、金融機関等での基幹系システムも含めたクラウドサービスの利用が拡大して同サービスが原因となる重大障害が発生したことを踏まえ、以下の分析・検証を実施。 ✓ 金融機関等で発生した障害事例を踏まえた対策の過不足 ✓ 口座振替による不正出金に関する事案 ✓ 新型コロナウイルス感染症の感染拡大の状況下での金融機関等におけるBCPに基づいた対応の実態及びテレワークにおける課題 ✓ 関連するガイドラインやセキュリティインシデントを踏まえ、サイバーセキュリティに関する態勢や対策の整備状況 ✓ 金融機関等でクラウドサービスを利用する場合の留意点等	（新たなデジタル技術に対応するため、2021年度中に改定を行うことを目指し、分析・検証の内容、スケジュール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

各安全基準等の改善状況 [6/12]

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ため、2021年度中に改定を行うことを目指し、分析・検証の内容、スケジュール等について検討を実施。）	（新たなデジタル技術に対応するため、2021年度中に改定を行うことを目指し、分析・検証の内容、スケジュール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）	• 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

各安全基準等の改善状況 [7/12]

安全基準等の名称			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
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３月（初版制定：2016年９月）	2020年８月（初版制定：2013年３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	◆ 本安全基準等で引用している規格の改定状況について確認するため、分析・検証を実施。	◆ 2019年９月に関東地方に上陸した台風15号により電力鉄塔や電柱が倒壊する事故が発生したことを受け、事故原因の究明を行うとともに、技術基準の適切性、再発防止策、地域の実情に応じた基準風速の適用等について専門的な見地から分析・検証を実施。 ◆ 水面に設置される太陽電池発電設備が増加したことを受け、それらの事故実績等を踏まえ、水面に設置される太陽電池モジュールの支持物に要求する性能について分析・検証を実施。
	改定の実施状況		**実施**	**実施**
		改定の主な内容	◆ 本安全基準等で引用している日本電気技術規格委員会規格のJESC Z0004（電力制御システムセキュリティガイドライン）及び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）の改定を反映。	◆ 2019年９月に関東地方に上陸した台風15号により電力鉄塔や電柱が倒壊する事故に関する分析・検証の結果を踏まえ、以下の改定を実施。 ✓ 倒壊した電力鉄塔・電柱の技術基準について所要の改定を実施（令和２年５月15日） ✓ 電力鉄塔の強度設計において地域の実情に応じた基準風速の適用を行う改定を実施（令和２年８月12日） ◆ 水面に設置される太陽電池モジュールの支持物に要求する性能を具体的に規定する改定を実施（令和２年６月１日）
		改定の際に参考としている基準・規格（指針除く）	・ 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）	・ JIS C 8955（太陽電池アレイ用支持物の設計用荷重算出方法）
（２）指針との対応			確認済み	確認済み

各安全基準等の改善状況 [8/12]

安全基準等の名称			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
重要インフラ分野			電力	電力
制定主体			一般社団法人日本電気協会	一般社団法人日本電気協会
最終改正（初版制定）年月			2019年７月（初版制定：2016年５月）	2019年７月（初版制定：2016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**	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	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。）	（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

各安全基準等の改善状況 [9/12]

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）	2020年12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**（継続中）
		分析・検証の内容や主な理由・契機	◆ ガス分野で実施した情報連絡訓練の参加事業者からの意見を踏まえ、サイバーセキュリティに関する事故が発生した際の情報連絡先について検討を実施。	◆ クラウド・バイ・デフォルト原則、行政手続のオンライン化、働き方改革、サイバー攻撃の増加といった新たな時代の要請に対応するため、以下の点について分析・検証を実施。 ✓ 情報システム機器の廃棄等時におけるセキュリティ要件 ✓ クラウドサービスの利用に係るセキュリティ要件 ✓ LGWAN接続系へのテレワークのセキュリティ要件 ✓ 次期自治体情報セキュリティクラウドの標準要件
	改定の実施状況		**実施**	**実施**
		改定の主な内容	◆ 分析・検証の結果を踏まえ、複数あったサイバーセキュリティに関する事故が発生した際の情報連絡先を一つに集約。	◆ 分析・検証の結果を踏まえ、以下の改定を実施。 ✓ マイナンバー利用事務系の分離の見直し ✓ LGWAN接続系とインターネット接続系の分割の見直し ✓ リモートアクセスのセキュリティ ✓ LGWAN接続系における庁内無線LANの利用 ✓ 情報資産及び機器の廃棄 ✓ クラウドサービスの利用 ✓ 研修、人材育成 ◆ 2018年の「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）	―	• 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 • 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）
（２）指針との対応			確認済み	確認済み

各安全基準等の改善状況 [10/12]

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）	水道分野における情報セキュリティガイドライン（第４版）
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			2021年１月（初版制定：2005年３月）	2019年３月（初版制定：2006年10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**	なし
		分析・検証の内容や主な理由・契機	◆ 2020年3月に公表した本ガイドライン第5.1版改定素案に基づき改定を行うため、「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」（総務省、経済産業省）や「TLS暗号設定ガイドライン」（IPA）との整合性を確認する等、技術動向の変化によって更に改定が必要な項目がないか分析・検証を実施。	（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		**実施**	なし
		改定の主な内容	◆ 医療機関等を対象とするサイバー攻撃の多様化・巧妙化、スマートフォンや各種クラウドサービス等の医療現場での普及、昨今の個人情報に関する状況等に対応するとともに、関連するガイドライン等との整合性を確保するため、以下の改定を実施。 ✓ クラウドサービス利用時の責任分界点の考え方を追記 ✓ リスク分析において、「管理されていない機器」や「ソフトウェア」、「サービス」等の利用等に関するリスクを考慮することを追記 ✓ ネットワーク等の監視等の管理に関する措置やネットワーク構築のあり方、外部からのデータの取り込みにおける対応措置等の必要性を追記 ✓ 暗号鍵の管理に関する内容を追記 ✓ 非常時の体制構築に関する内容、平常時における教育・訓練、サイバー攻撃等が生じた場合の通報に関する規定等を追記 ✓ 外部保存を受託する事業者の選定に関する内容（Cookie等の取扱い、国内法の適用、求められる認証、提供すべきセキュリティ情報等）を追記 ✓ 関連するガイドライン等の改正に伴う修正　　等	—
		改定の際に参考としている基準・規格（指針除く）	• 政府情報システムにおけるクラウドサービスの利用に係る基本方針 • NISTサイバーセキュリティフレームワーク • FIPS 140-2（暗号化モジュールの安全性、機密性に関する要件を定める標準） • IMDRF（国際医療機器規制当局フォーラム） • 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 • TLS暗号設定ガイドライン　　等	—
（２）指針との対応			確認済み	確認済み

各安全基準等の改善状況 [11/12]

安全基準等の名称			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）	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
重要インフラ分野			**物流**	**化学**
制定主体			国土交通省	石油化学工業協会
最終改正（初版制定）年月			2019年３月（初版制定：2006年９月）	2019年５月（初版制定：2015年３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**	なし
		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ため、2021年度中に改定を行うことを目指し、分析・検証の内容、スケジュール等について検討を実施。）	（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）	• 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

各安全基準等の改善状況 [12/12]

安全基準等の名称			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			クレジット	石油
制定主体			一般社団法人日本クレジット協会	石油連盟
最終改正（初版制定）年月			2018年４月（初版制定：2014年12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**	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	なし
		分析・検証の内容や主な理由・契機	（2019年度までにクレジット業界で定めているガイドラインの内容を検証し、問題がないことを確認しているため。）	（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