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33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［2022年度］

令和５年６月２日

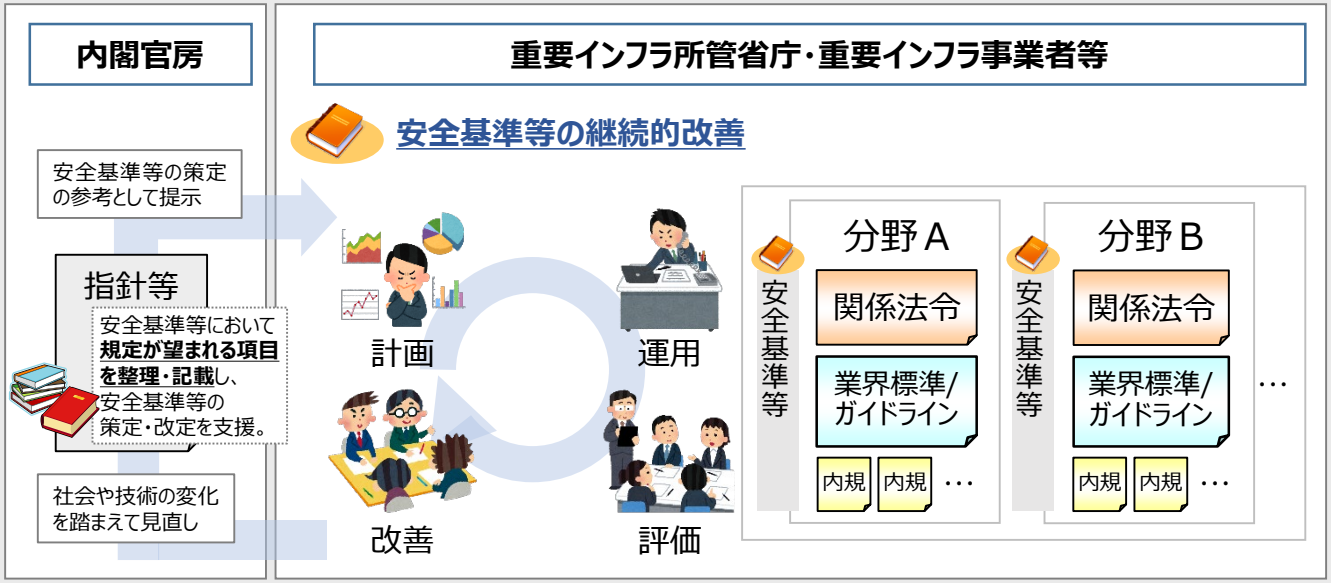
内閣サイバーセキュリティセンター
重要インフラグループ

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。
- 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改定状況、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

調査項目

① 各安全基準等の**改定**の状況

② 各安全基準等の**指針への対応**の状況

【参考：本調査の実施背景】

○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）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。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。

調査対象一覧（14分野32件）

分野		安全基準等の名称　※2021年度調査からの追加は下線部
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4.2版）
	放送	• 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	• 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 資金決済	• 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		• 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		• 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		• 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		• 医療法施行規則 • 医療情報システムの安全管理に関するガイドライン（第5.2版）
水道		• 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		• 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

- 2022年度は、医療機関に対するサイバー攻撃の増加等に伴う医療法施行規則の改定等、10件の安全基準等に係る改定・策定が実施された。
- また、連続して通信障害が発生していることを踏まえた構造的問題の検証等、改定に向けた検討がなされた。
- 安全基準等の指針への対応状況については、「経営層とのコミュニケーション」「任務保証の考え方に基づくリスクアセスメント等の実施」「コンティンジェンシープランの策定」「バックアップリカバリー検査の実施」等に関する充実化の余地がある。改定指針等を踏まえた更なる改善が期待される。

主な改定の概要

□ サイバー攻撃の増加等に伴う改定

○ 医療法施行規則

昨今、医療機関に対するサイバー攻撃が増加しており、サイバー攻撃により診療が長期に停止する事案が発生したこと等を踏まえ、「病院、診療所又は助産所の管理者はサイバーセキュリティの確保のために必要な措置を講じなければならない」旨を規定。

□ システム障害の発生等に伴う改定

○ 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

昨今の金融機関等におけるシステム障害等を踏まえ、障害時・災害時に備えた教育・訓練、関係者への連絡手段の明確化等に関する改定を実施。

□ 指針・ガイドライン等の改定に伴う改定

○ クレジットCEPTOARにおける情報セキュリティガイドライン

指針を踏まえ、経営陣の関与とリーダーシップに関する事項やサプライチェーンマネジメントの強化について改定を実施。

□ デジタル化の進展等に伴う改定

○ 事業用電気通信設備規則

音声伝送番号の指定を受けるMVNOの電気通信回線設備以外の設備に対し、携帯電話用設備と同等の基準を規定。

○ 電気設備に関する技術基準を定める省令

電気工作物におけるサイバーセキュリティの確保義務について、配電事業の用に供する電気工作物を対象に追加。

○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

地方公共団体情報システム標準化基本方針（令和４年10月閣議決定）を踏まえ、情報システムの標準化・共通化の動向に対応できるよう改定。

改定に向けた主な検討状況の概要

□ システム障害の発生等に伴う検討

○ 事業用電気通信設備規則

連続して通信障害が発生していることを踏まえ、適切なモニタリングのルール等に関する見直しを検討。

□ 環境変化に伴う検討

○ 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

業務継続に対する社会の関心が大きく高まっていることから、金融機関等の業務継続を脅かすリスク要因として、自然災害に加えて、大規模システム障害、サイバー攻撃、感染症についても主たるリスクと位置づけ、手引書の構成を見直すこと等を検討。

○ 医療情報システムの安全管理に関するガイドライン

外部委託、外部サービスの利用に関する整理、新技術、制度・規格の変更への対応等について見直しを検討。

□ 指針・ガイドライン等の改定に伴う検討

○ 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、他

各ガイドライン・法令・規則等におけるセキュリティに関する改正、指針改定に向けた検討状況等を踏まえ、見直しを検討。

資料２別紙

重要インフラのサイバーセキュリティに係る
安全基準等の概要と改善状況（2022 年度）

目次

1. 情報通信分野

1.1 電気通信

総務省令においてサイバーセキュリティの確保に関する規定が設けられており、さらに、総務省及び業界団体がガイドラインを策定している。

○ 事業用電気通信設備規則（昭和六十年郵政省令第三十号）

> （事業用電気通信設備の防護措置）
> 第六条　事業用電気通信設備は、利用者又は他の電気通信事業者の電気通信設備から受信したプログラムによつて当該事業用電気通信設備が当該事業用電気通信設備を設置する電気通信事業者の意図に反する動作を行うことその他の事由により電気通信役務の提供に重大な支障を及ぼすことがないよう当該プログラムの機能の制限その他の必要な防護措置が講じられなければならない。

※その他、災害対策、代替手段等に関する規定あり。

- MVNO による多様な付加価値サービスの創出・提供を実現するため、MVNO に音声伝送携帯電話番号の指定ができるようにした上で、音声伝送番号の指定を受ける MVNO の電気通信回線設備以外の設備を「特定携帯電話用設備」として定義し、携帯電話用設備と同等の基準を規定（2023 年２月改正）。
- 「電気通信事故に係る構造的な問題の検証に関する報告書（令和５年３月）」を踏まえた改正を予定（2023 年度）。

○ 情報通信ネットワーク安全･信頼性基準（総務省，2023 年２月（初版制定:1987 年２月））

- 事業用電気通信設備規則の改正を踏まえて改正した（2023 年２月改正）。
- 「電気通信事故に係る構造的な問題の検証に関する報告書（2023 年３月）」を踏まえた改正を予定（2023 年度）。

○ 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）（一般社団法人電気通信事業者連合会，2021 年 12 月（初版制定:2006 年９月））

- ISO/IEC 規格（27001,27002 等）の改定や電気通信分野固有の各ガイドライン・法令・規則等におけるセキュリティに関する改正、また現在進められている「重要インフラのサイバーセキュリティに係る行動計画」に沿った安全基準等策定指針・手引書等の策定に伴い、それらを反映した改版を 2023 年度中に実施予定。

1.2. 放送・ケーブルテレビ

総務省令においてサイバーセキュリティの確保に関する規定が設けられており、さらに、業界団体がガイドラインを策定している。

○ 放送法施行規則（昭和二十五年電波監理委員会規則第十号）

（サイバーセキュリティの確保） 第百十五条の二　放送設備及び当該放送設備を維持又は運用するために必要な設備は、当該放送設備によつて行われる放送の業務に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。以下同じ。）の確保のために必要な措置が講じられていなければならない。

※「放送設備」には、ケーブルテレビに係る設備が含まれる。

○ 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（一般社団法人 ICT-ISAC, 2020 年９月（初版制定:2005 年 10 月））

・ 「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」の改定状況を踏まえて、改定を検討する。

○ 放送設備サイバー攻撃対策ガイドライン（一般社団法人 ICT-ISAC, 2020 年２月（初版制定:2018 年６月））

・ 放送設備の IP 化に伴う安全・信頼性に関する技術条件等の変更、「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」の改定状況を踏まえて、改定を検討する。

○ 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）（一般社団法人日本ケーブルテレビ連盟, 2021 年９月（初版制定:2012 年 11 月））

・ 「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」の改定状況を踏まえて、改定を検討する。

2. 金融分野

関係法令において態勢整備について規定されており、例えば、銀行については、銀行法施行規則に基づき健全かつ適切な業務の運営を確保するための措置に関する社内規則等を定めるとともに従業員に対する研修その他の当該社内規則等に基づいて業務が運営されるための十分な体制を整備しなければならないこととされている。また、それを具体化した監督指針に基づきサイバーセキュリティ管理態勢の整備が求められている。さらに、業界団体がガイドラインを策定している。

○ 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（公益財団法人　金融情報システムセンター（FISC），2022 年 12 月（1985 年 12 月））

・ 第 10 版 2022 年 12 月改訂（2022 年 12 月発刊）

(1) サイバーセキュリティに関する改訂

金融機関等がサイバー攻撃に対するより実効性のある対応態勢の整備を進め、そのレベルアップを継続的に実施する取組みを支援することを目的として、内閣サイバーセキュリティセンター(NISC)、金融庁、経済産業省等より公表された文書、及び海外の代表的なガイドライン等の内容を分析し、侵入されることを前提とした対応策を事前に検討しておくこと、リスクの洗い出しと影響度の評価を行い定期的に見直すこと、また、ランサムウェア対策のひとつとして、バックアップからの復旧ができることの確認等について、安全対策基準への取込みを行った。

(2) 個人情報保護法改正に関する改訂

個人情報保護法の改正（令和２年改正法、令和３年改正法）について、法令、個人情報保護委員会・金融庁より公表されたガイドライン等の改正内容を分析し、安全対策基準への取込みを行った。

(3) システム障害事例に関する改訂

2021 年２月から３月にかけて複数件発生した都市銀行のシステム障害について原因を分析し、障害時・災害時に備えた教育・訓練、関係者への連絡手段の明確化等について、安全対策基準への取込みを行った。

・ 第 10 版（2022 年７月発刊）

(1) 設備基準の全面見直し

金融情報システムの設備を巡る技術や法令などの変化を鑑みたうえで、設備基準の全ての基準や解説を総点検し、記載内容を全般的に見直した。

(2) システム障害等への対応

昨今の金融機関等における大規模なシステム障害や、社会情勢・技術動向等の変化を踏まえ、各種ガイドラインやレポート等と安全対策基準とのギャップ分析を通じて対応策を検討し、その内容を反映した。

○ 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（FISC，2008 年６月（初版制定:1999 年１月））

・ 改定していない。

○ 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（FISC，2017 年５月（初版制定:1994 年１月））

・ 最後の改訂から 6 年が経過し、その間、大規模システム障害による顧客サービス停止、新型コロナウイルス禍での社会活動停滞、高度なサイバー攻撃による業務妨害などを経験し、業務継続に対する社会の関心が大きく高まっていることから、下記を主な改訂ポイントとして検討を実施しており、2023 年度中を目途に改訂予定。

１．金融機関等の業務継続を脅かすリスク要因として、自然災害に加えて、大規模システム障害、サイバー攻撃、感染症についても主たるリスクと位置づけ、手引書の構成を見直す。

２．改訂された業務継続に関するガイドライン等の内容を取り込む。特に以下のテーマについては、内容の更新に加え、考慮すべき事項の充実を図る。

(1)大規模システム障害

(2)サイバー攻撃

(3)感染症

（参考）銀行法施行規則（昭和五十七年大蔵省令第十号）（抄）

（社内規則等）

第十三条の七　銀行は、その営む業務の内容及び方法に応じ、顧客の知識、経験、財産の状況及び取引を行う目的を踏まえた重要な事項の顧客に対する説明その他の健全かつ適切な業務の運営を確保するための措置（書面の交付その他の適切な方法による商品又は取引の内容及びリスク並びに当該銀行が講ずる法第十二条の三第一項に定める措置の内容の説明並びに犯罪を防止するための措置を含む。）に関する社内規則等（社内規則その他これに準ずるものをいう。以下同じ。）を定めるとともに、従業員に対する研修その他の当該社内規則等に基づいて業務が運営されるための十分な体制を整備しなければならない。

（参考）主要行等向けの総合的な監督指針（金融庁，令和５年４月）（抄）

III －３－７　システムリスク

III －３－７－１　システムリスク

III －３－７－１－２　主な着眼点

(1)システムリスクに対する認識等

①システムリスクについて代表取締役をはじめ、役職員がその重要性を十分認識し、定期

的なレビューを行うとともに、全行的なリスク管理の基本方針が策定されているか。

②代表取締役は、システム障害やサイバーセキュリティ事案（以下「システム障害等」という。）の未然防止と発生時の迅速な復旧対応について、経営上の重大な課題と認識し、態勢を整備しているか。

③取締役会は、システムリスクの重要性を十分に認識した上で、システムに関する十分な知識・経験を有し業務を適切に遂行できる者を、システムを統括管理する役員として定めているか。

④代表取締役及び取締役（委員会設置会社にあっては執行役）は、システム障害等発生の危機時において、果たすべき責任やとるべき対応について具体的に定めているか。

また、自らが指揮を執る訓練を行い、その実効性を確保しているか。

3. 航空分野

国土交通省がガイドラインを策定している。

○ 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)(国土交通省, 2019 年３月（初版制定:2006 年９月))

・ 「重要インフラのサイバーセキュリティに係る行動計画」等の改訂を踏まえ、国土交通省において、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」の改善に向けた検討を行った。

4. 空港分野

国土交通省がガイドラインを策定している。

○ 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)(国土交通省, 2019 年３月（初版制定:2018 年４月))

・ 「重要インフラのサイバーセキュリティに係る行動計画」等の改訂を踏まえ、国土交通省において、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」の改善に向けた検討を行った。

5. 鉄道分野

国土交通省がガイドラインを策定している。

○ 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)(国土交通省, 2019 年３月（初版制定:2006 年９月))

・ 「重要インフラのサイバーセキュリティに係る行動計画」等の改訂を踏まえ、国土交通省において、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」の改善に向けた検討を行った。

6. 電力分野

関係法令において、保安規定を定める旨や、サイバーセキュリティを確保する旨を規定している。また、関係法令の解釈において、技術的内容を具体的に示しており、サイバーセキュリティの確保については日本電気技術規格委員会規格による旨を規定している。

○ 電気設備に関する技術基準を定める省令（平成九年通商産業省令第五十二号）

（サイバーセキュリティの確保）

第十五条の二　事業用電気工作物（小規模事業用電気工作物を除く。）の運転を管理する電子計算機は、当該電気工作物が人体に危害を及ぼし、又は物件に損傷を与えるおそれ及び一般送配電事業又は配電事業に係る電気の供給に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を確保しなければならない。

- 電気工作物におけるサイバーセキュリティの確保義務について、配電事業者制度開始に伴い、配電事業の用に供する電気工作物にも求めることとした。また、諸外国において製鉄所等の産業施設へのサイバー攻撃により大規模な被害が生じていること、及び中小企業も含む今後の電気保安分野におけるスマート化の進展も踏まえ、サイバーセキュリティの確保義務の対象について、自家用電気工作物を含む事業用電気工作物に拡大した。

○ 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（経済産業省，2023 年３月（初版制定：2016 年９月））

１２．第１５号(その他保安上必要な事項)

十五 その他事業用電気工作物の工事、維持及び運用に関する保安に関し必要な事項

サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を確保するため、次の各号により適切な措置が講じられることが必要である。

一 スマートメーターシステムにおいては、日本電気技術規格委員会規格ＪＥＳＣ Ｚ０００３（２０１９）「スマートメーターシステムセキュリティガイドライン」によること。

二 電力制御システムにおいては、日本電気技術規格委員会規格ＪＥＳＣ Ｚ０００４（２０１９）「電力制御システムセキュリティガイドライン」によること。

また、本号は前に掲げるもののほか、事業用電気工作物の工事、維持及び運用に関する保安を行う上で事業者の判断により必要となるものについて記載することを想定した規定である。

・ 電気工作物におけるサイバーセキュリティの確保義務について、配電事業者制度開始に伴い、配電事業の用に供する電気工作物にも求めることとした。

（参考）電気事業法施行規則第 50 条第３項第９号の解釈適用に当たっての考え方（経済産業省，2023 年３月改正）　（注：電力分野の重要インフラサービスを対象とするものではない）

サイバーセキュリティ（サイバーセキュリティ基本法（平成２６年法律第１０４号）第２条に規定するサイバーセキュリティをいう。）を確保するため、次に掲げる事業用電気工作物の種類ごとにそれぞれに定められたところにより適切な措置が講じられることが必要である。また、次に掲げるもののほか、事業用電気工作物の工事、維持及び運用に関する保安を行う上で設置者の判断により必要となるものについて記載することが必要である。

１．特定送配電事業又は発電事業の用に供する事業用電気工作物

① スマートメーターシステムにおいては、日本電気技術規格委員会規格ＪＥＳＣ Ｚ０００３（２０１９）「スマートメーターシステムセキュリティガイドライン」によること。

② 電力制御システムにおいては、日本電気技術規格委員会規格ＪＥＳＣ Ｚ０００４（２０１９）「電力制御システムセキュリティガイドライン」によること。

２．自家用電気工作物

遠隔監視システム及び制御システムにおいては、「自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）」（令和４年６月１０日付け２０２２０５３０保局第１号）によること。

・ 諸外国においては製鉄所等の産業施設へのサイバー攻撃も発生し、大規模な被害が生じており、また、電気保安分野におけるスマート化の進展にあわせて自家用電気工作物においてもサイバーセキュリティの確保が重要となっている。
・ そのため、2022 年６月 10 日付で「電気事業法施行規則第５０条第３項第９号の解釈適用に当たっての考え方」及び「自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン」を制定し、2022 年 10 月１日から特定送配電事業の用に供する事業用電気工作物及び自家用電気工作物の設置者についてもサイバーセキュリティの確保と保安規程への記載を求めることとした。

○ 電気設備の技術基準の解釈（経済産業省，2023 年３月（初版制定:2013 年３月））

【サイバーセキュリティの確保】（省令第 15 条の 2）

第 37 条の 2　省令第 15 条の 2 に規定するサイバーセキュリティの確保は、次の各号によること。

一　スマートメーターシステムにおいては、日本電気技術規格委員会規格　JESC　Z0003 (2019)「スマートメーターシステムセキュリティガイドライン」によること。配電

事業者においても同規格に準じること。

二 電力制御システムにおいては、日本電気技術規格委員会規格 JESC Z0004（2019）「電力制御システムセキュリティガイドライン」によること。配電事業者においても同規格に準じること。

三 自家用電気工作物（発電事業の用に供するもの及び小規模事業用電気工作物を除く。）に係る遠隔監視システム及び制御システムにおいては、「自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）」（20220530 保局第 1 号 令和 4 年 6 月 10 日）によること。

・ 電気工作物におけるサイバーセキュリティの確保義務について、配電事業者制度開始に伴い、配電事業の用に供する電気工作物にも求めることとした。また、諸外国において製鉄所等の産業施設へのサイバー攻撃により大規模な被害が生じていること、及び中小企業も含む今後の電気保安分野におけるスマート化の進展も踏まえ、サイバーセキュリティの確保義務の対象について、自家用電気工作物を含む事業用電気工作物に拡大した。

○ 電力制御システムセキュリティガイドライン（一般社団法人日本電気協会，2019 年７月（初版制定:2016 年３月））

・ 改定していない。

○ スマートメーターシステムセキュリティガイドライン（一般社団法人日本電気協会，2019 年７月（初版制定:2016 年３月））

・ 改定していない。

7. ガス分野

関係法令においてサイバーセキュリティを確保する旨を規定しており、さらに、業界団体がガイドラインを策定している。

○ ガス事業法施行規則（昭和四十五年通商産業省令第九十七号）

（保安規程）

第二十四条　法第二十四条第一項の保安規程は、次の事項（特定ガス発生設備においてガスを発生させ、導管によりこれを供給する小売供給を行う者にあつては、当該供給に係る第八号及び第九号の事項を除く。）について定めるものとする。

一～五　（略）

六　ガス工作物の運転又は操作を管理する電子計算機に係るサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。第九十二条第一項第六号及び第百四十八条第一項第六号において同じ。）の確保に関すること。

七～十三　（略）

○ 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（一般社団法人日本ガス協会，2022 年 12 月（初版制定:2019 年３月））

・ 「重要インフラのサイバーセキュリティに係る行動計画に基づく情報共有の手引書」が改訂されたこと等を受け、セキュリティ事故発生時における情報連絡様式及び情報共有範囲の選択肢を更新した。

8. 政府・行政サービス分野

総務省がガイドラインを策定している。

○ 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（総務省，2023年３月（初版制定:2001 年３月））

・ 地方公共団体情報システム標準化基本方針（令和４年 10 月閣議決定）において、「地方公共団体が利用する標準準拠システム等の整備及び運用に当たっては、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参考にしながら、セキュリティ対策を行うものとする」とされたことから、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の改定等に係る検討会において、地方公共団体がガバメントクラウド等を利用するに当たってのセキュリティ対策等について検討し、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改定した。

9. 医療分野

関係法令においてサイバーセキュリティを確保する旨を規定しており、また、厚生労働省がガイドラインを策定している。

○ 医療法施行規則（昭和二十三年厚生省令第五十号）

第十四条（略） ２　病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）の確保のために必要な措置を講じなければならない。

・ 次のとおり、新規にサイバーセキュリティの確保に関する規定を設けた。

昨今、医療機関に対するサイバー攻撃が増加しており、サイバー攻撃により診療が長期に停止する事案が発生したこと、また、患者の個人情報が窃取される等の甚大な被害がもたらされる可能性があることを踏まえ、医療機関におけるサイバーセキュリティ対策に関する取組の実効性を高める必要が生じている。

これに関して、第 12 回健康・医療・介護情報利活用検討会（令和４年９月５日開催。以下「検討会」という。）でとりまとめた「医療機関におけるサイバーセキュリティ対策の更なる強化策」において、医療機関の管理者が遵守すべき事項として、サイバーセキュリティ対策を位置付けるための省令改正を令和４年度中に行うこととしたところ。

検討会でのとりまとめを踏まえ、法第 17 条に規定する医療機関の管理者が遵守すべき具体的事項として、サイバーセキュリティの確保に関する基準の遵守を定める必要がある。

以上を踏まえ、規則について所要の改正を行った。

○ 医療情報システムの安全管理に関するガイドライン（第 5.2 版）（厚生労働省, 2022 年 3 月（初版制定:2005 年３月））

・ 次のとおり改定に向けた検討を行い、2023 年度以降に改定予定である。

2023 年４月からの保険医療機関・薬局におけるオンライン資格確認導入の原則義務化により、概ね全ての医療機関等において、本ガイドラインに記載されているネットワーク関連のセキュリティ対策が必要となる。

これを踏まえ、第 5.2 版で中長期的に検討を継続することとした論点※を中心に、全体構成の見直しとともに検討した結果、第 6.0 版への改定を予定している。

※中長期的に検討を継続する論点

・外部委託、外部サービスの利用に関する整理

・情報セキュリティに関する考え方の整理

・新技術、制度・規格の変更への対応

10. 水道分野

関係法令においてサイバーセキュリティを確保する旨を規定しており、また、厚生労働省がガイドラインを策定している。

○ 水道施設の技術的基準を定める省令（平成十二年厚生省令第十五号）

（一般事項）

第一条　水道施設は、次に掲げる要件を備えるものでなければならない。

一～十一（略）

十一の二　施設の運転を管理する電子計算機が水の供給に著しい支障を及ぼすおそれがないように、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を確保するために必要な措置が講じられていること。

十二～十七（略）

○ 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）（厚生労働省, 2019 年３月（初版制定:2006 年 10 月））

・ 改定していない。

11. 物流分野

国土交通省がガイドラインを策定している。

○ 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)(国土交通省, 2019 年３月（初版制定:2006 年９月))

・ 「重要インフラのサイバーセキュリティに係る行動計画」等の改訂を踏まえ、国土交通省において、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」の改善に向けた検討を行った。

12. 化学分野

業界団体がガイドラインを策定している。

○ 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（石油化学工業協会，2019年５月（初版制定:2015年３月））

・ 石油化学工業協会情報通信委員会に新たに安全基準改定サブワーキンググループを設け、改定に向けた検討を開始した。今後予定される「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」の改定を踏まえ、化学分野の対象である制御システムのセキュリティ確保の観点から、2023年度中に改定予定。

13. クレジット分野

業界団体がガイドラインを策定している。

○ クレジット CEPTOAR における情報セキュリティガイドライン（一般社団法人日本クレジット協会, 2023 年２月（初版制定:2014 年 12 月））

・ 環境変化を踏まえつつ、令和元年５月に改定された「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」にて求められている事項への対応状況について、改めて分析・検証を行い、令和５年２月に改正を行った。

・ 具体的には、主にサイバーセキュリティに関し、経営陣の関与とリーダーシップに関する事項やサプライチェーンマネジメントの強化について、より明確に記載した。

14. 石油分野

業界団体がガイドラインを策定している。

（参考）石油精製業は業法が廃止されており、現在は存在しないため、災害対策基本法に基づく指定公共機関としての責務や関係法令等を鑑み、業界団体が業界横断的なガイドラインとして定めている。

○ 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（石油連盟，2020 年３月（初版制定:2015 年３月））

・ 石油連盟サイバーセキュリティ専門委員会において、2022 年度は「重要インフラにおけるサイバーセキュリティ確保に係る安全基準等策定指針」改定に向けた議論の動向や、新指針に盛り込まれる見込みの内容等に関する確認を行った。2023 年度中を目途に「石油分野におけるサイバーセキュリティ（※現行：情報セキュリティ）確保に係る安全ガイドライン」を改定予定。