



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

重要インフラにおける安全基準等の 継続的改善状況等の調査について (2018年度)

2019年4月18日

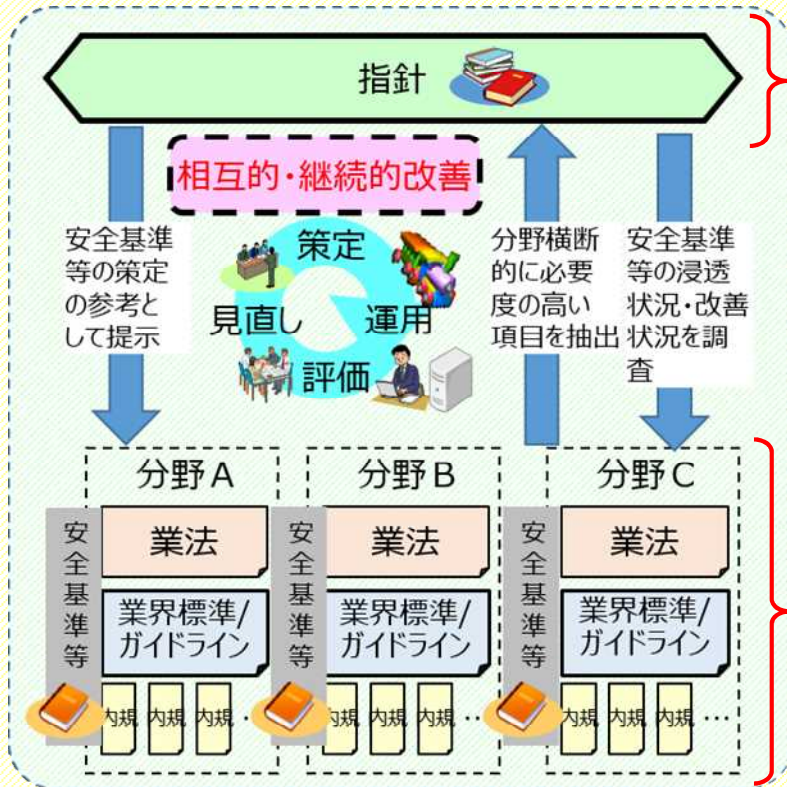
内閣官房 内閣サイバーセキュリティセンター(NISC)

目次

調査目的	P. 2
調査対象一覧	P. 3
調査結果一覧	P. 4
調査結果（概要）	P. 5
調査結果（詳細）	P. 6 - P.17

調査目的

- 重要インフラ防護能力の維持・向上を目的に、情報セキュリティ対策のP D C Aサイクルを踏まえた「指針」及び「安全基準等」の相互的・継続的改善を目指す。このことから「安全基準等」の改善状況を年度ごとに調査し、重要インフラ専門調査会に報告するもの。



<指針>

「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」の略称

<安全基準等とは>

以下の総称

- 業法に基づき国が定める「強制基準」
- 業法に準じて国が定める「推奨基準」及び「ガイドライン」
- 業法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」
- 業法や国民・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

* 指針は含まない

【調査ポイント】

- ① P D C Aサイクルに基づく安全基準等の改善要否を判断するための分析・検証作業の取組状況の把握
- ② 分析・検証の結果に基づく安全基準等の改定状況の把握
- ③ 指針の継続的改善に繋がる安全基準等の具体的な改定事例の抽出

調査対象一覧

分野		安全基準等名称
情報通信	電気通信	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版） 電気通信事業法／電気通信事業法施行規則／事業用電気通信設備規則
	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	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<初版>
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 第9版 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		航空運送事業者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）
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1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3版）
電力		電力制御システムセキュリティガイドライン 電気設備の技術基準の解釈 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 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		製造・供給に係る制御系システムのセキュリティ対策ガイドライン
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
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3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

調査結果一覧

分野	安全基準等名称	2018年度内の取組状況	
		分析・検証	改定
情報通信	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版） 電気通信事業法／電気通信事業法施行規則／事業用電気通信設備規則	実施した 実施した 実施中	実施した 実施した 実施していない
	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	実施していない 実施していない	実施していない 実施していない
	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<初版>	実施した	実施していない
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 第9版 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	実施していない 実施した 実施していない	実施していない 実施していない 実施していない
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）	実施した	実施した
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）	実施した	実施した
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）	実施した	実施した
電力	電力制御システムセキュリティガイドライン 電気設備の技術基準の解釈 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 スマートメーターシステムセキュリティガイドライン	実施中 実施していない 実施していない 実施中	実施していない 実施していない 実施していない 実施していない
ガス	製造・供給に係る制御系システムのセキュリティ対策ガイドライン	実施中	実施していない
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	実施した	実施した
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版）	実施していない	実施していない
水道	水道分野における情報セキュリティガイドライン	実施した	実施した
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）	実施した	実施した
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	実施した	実施中
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	実施した	実施した
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	実施した	実施中

調査結果（概要）

○安全基準等の継続的改善における2018年度の取組状況及び改定状況については以下のとおり。

分析・検証後、改定を実施済：9件

分析・検証後、改定を実施中：2件

分析・検証を実施中：5件

（上記以外に昨年度に改定不要と判断したため、今年度は分析・検証を実施しなかった等が8件）

○安全基準等の分析・検証を行うに至った主な契機は以下のとおり。

- ・ 指針の改定
- ・ ITに係る環境変化の調査・分析からの課題発見
- ・ 定期的に検証することとしている

（上記以外にも、ユーザからの要望やIoTの普及や仮想化技術の進展などネットワークの環境変化に対応等もあった。）

○重要インフラの情報セキュリティ対策に係る第4次行動計画と指針に記載されている「機能保証の考え方」、「経営層の在り方」、「制御系セキュリティ」について、下記のことを考えられる。

- ・ 指針の改訂に伴い、第5版で新たに記載された「機能保証の考え方」等の内容を踏まえた安全基準等の改善が見受けられ、リスクアセスメントの取組が一步進んだ。
- ・ 経営層の積極的関与や在り方についての記載が充実化されている安全基準等も存在し、経営層に対するアプローチの重要性が認識されてきていることが認められる。
- ・ OT（制御系）とIT（情報系）を含めた内容の記載のある安全基準等もあることから、制御系を含めた意識醸成がされ始めていることが確認できる。

調査結果（詳細） 1 / 12

分野	情報通信（電気通信）	情報通信（電気通信）	
名称	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版）	
発行主体等	総務省	一般社団法人電気通信事業者協会	
最新改定／新規作成年月	2015年4月	2018年10月	
分析・ 検証 状況	分析検証の実施状況	2018年度中に実施済	2018年度に実施済
	分析検証の実施契機	その他状況の変化等（平成29年8月にGoogleを起因とする大規模なインターネット障害が発生したことを踏まえ、その対象について分析・検証を実施。）	安全基準等策定指針の改定（第5版への改定） / ITに係る環境変化の調査・分析からの課題発見 / サイバー攻撃動向を受けて
	分析・検証プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	（1）2017年12月～2018年9月 （2）情報通信審議会 情報通信技術分科会 IPネットワーク設備委員会 （3）同委員会は、近年のIoTの普及に伴う通信ネットワークの高度化や利用形態の多様化を踏まえ、「IoTの普及に対応した電気通信設備に係る技術的条件」について検討（合計8回）。同委員会の検討結果について、情報通信審議会情報通信技術分科会で審議が行われ、一部答申を受けたため、改定を行うことが正式決定。	（1）2018年4月～2019年3月 （2）一般社団法人電気通信事業者協会 安全・信頼性協議会 安全基準検討ワーキンググループ （3）同ワーキンググループで分析・検証し、改定が必要な場合は同WGで改定案を作成・検討し、策定する。
改定 状況	改定の実施状況	2018年度中に実施済	2018年度に実施済
	改定プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	（1）2019年3月 （2）総務省総合通信基盤局電気通信事業部電気通信技術システム課安全・信頼性対策室 （3）2018年12月下旬から1か月間、改定案について意見募集を実施し、その結果に基づき、2019年3月末までに改定を実施する予定。	（1）2018年10月 （2）一般社団法人電気通信事業者協会 安全・信頼性協議会 安全基準検討ワーキンググループ （3）同ワーキンググループで改定案を作成・検討し、策定。
	改定内容	大規模インターネット障害に関し、事業者等に推奨する対策の追加	主として、NISC指針第5版で記載されたリスクアセスメントのうち、「機能保証の考え方」を踏まえた継続的な改善に取り組む必要性、経営層の積極的な関与・在り方についての記載充実化・明確化、「サイバー攻撃リスクの特性」「対策の考慮事項」の整理、OT(制御系)含めたCSIRTの構築や人材育成、の4点を反映した。
記載項目を包括的に確認し、安全基準等に必要項目を漏れなく記載していますか	はい（第5版の記載項目、第4版の記載項目）	はい（第5版の記載項目、第4版の記載項目）	
独自記載項目	なし	ISO/IEC27001:・27002:2013の要素を取り入れるとともに、ISO/IEC27017:2015（クラウドサービスのための実践規範）を取り入れた。	

調査結果（詳細） 2 / 1 2

分野	情報通信（電気通信）	情報通信（放送）	
名称	事業用電気通信設備規則 ※電気通信事業法、電気通信事業法施行規則は改定なし	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	
発行主体等	総務省	放送セクター（日本放送協会（NHK）、一般社団法人日本民間放送連盟）	
最新改定／新規作成年月	2015年11月27日	2016年10月	
分析・検証状況	分析検証の実施状況	実施中	2018年度に実施予定なし (理由：放送設備サイバー攻撃対策ガイドラインの現場への浸透を進めているため、本ガイドラインの分析・検証は2019年度以降に実施予定)
	分析検証の実施契機	その他状況の変化等（IoTの普及や仮想化技術の進展などネットワークの環境変化に対応して、設備の維持・管理に求められる知識、能力の確保の在り方や将来にわたっての人材の確保・育成の方策等について検討する必要があるため。）	—
	分析・検証プロセス (1) 実施時期 (2) 実施主体 (3) 実施の流れ	(1) 2018年10月～ (2) 情報通信審議会（情報通信技術分科会 I P ネットワーク設備委員会） (3) 2019年5～6月頃に一部答申を予定。	—
改定状況	改定の実施状況	—	—
	改定プロセス (1) 実施時期 (2) 実施主体 (3) 実施の流れ	—	—
	改定内容	—	—
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか	いいえ（本件は、事業用電気通信設備の技術基準に特化した内容であるため）	はい（第4版の記載項目）	
独自記載項目	なし	なし	

調査結果（詳細） 3 / 1 2

分野	情報通信（放送）	情報通信（ケーブルテレビ）	
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<初版>	
発行主体等	一般社団法人ICT-ISAC放送設備サイバー攻撃対策WG	一般社団法人日本ケーブルテレビ連盟（通信・放送制度委員会）	
最新改定／新規作成年月	2018年6月	2012年11月	
分析・検証状況	分析検証の実施状況	2018年度に実施予定なし（理由：2018年6月に作成）	2018年度に実施済
	分析検証の実施契機	—	定期的に検証することとしている
	分析・検証プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	—	（1）毎年4～5月 （2）通信・放送制度委員会 （3）通信・放送制度委員会配下のセキュリティWGにて改訂の必要性を検討→通信・放送制度委員会で承認を行う。
改定状況	改定の実施状況	—	実施不要と判断（理由：既存内容を確認した結果、大きな変更は必要ないと判断し、次回は2019年度に検討を行うと判断した。）
	改定プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	—	—
	改定内容	—	—
記載項目を包括的に確認し、安全基準等に必要項目を漏れなく記載していますか	いいえ（本ドキュメントは、放送設備のサイバー攻撃の対策に特化しており、該当部分のみを参照した）	いいえ（各ケーブルテレビ事業者に対して災害や事業環境変化による経営危機に備えるために経営戦略と連動したBCPの策定を促進させている。本ガイドラインは業界におけるセキュリティ対策の留意点をまとめたものであり、BCPの一部として位置付けている。）	
独自記載項目	なし	なし	

調査結果（詳細） 4 / 1 2

分野	金融	金融	
名称	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 第9版	
発行主体等	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）	
最新改定／新規作成年月	2008年6月	2018年3月	
分析・検証状況	分析検証の実施状況	2018年度に実施予定なし（理由：次年度以降に改訂の可否含め検討予定）	2018年度中に実施済
	分析検証の実施契機	—	ITに係る環境変化の調査・分析からの課題発見
	分析・検証プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	—	（1）2018年7月～2019年3月 （2）安全対策専門委員会、安全対策に関する検討部会 （3）金融機関、ITベンダー等から構成される安全対策専門委員会等を2018年12月から開催し、会員意見を踏まえ2019年3月までに改訂内容を決定する予定。
改定状況	改定の実施状況	—	—
	改定プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	—	—
	改定内容	—	—
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか	はい（第5版の記載項目）	はい（第5版の記載項目）	
独自記載項目	金融機関における固有業務や設備設置に係る基準等	金融機関における固有業務や設備設置に係る基準等	

調査結果（詳細） 5 / 1 2

分野	金融	航空	
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	
発行主体等	公益財団法人 金融情報システムセンター（FISC）	国土交通省	
最新改定／新規作成年月	2017年5月	2019年（平成31年）3月29日	
分析・検証状況	分析検証の実施状況	2018年度に実施予定なし（理由：2016年度に分析・検証実施済）	2018年度に実施済
	分析検証の実施契機	—	安全基準等策定指針の改定（第5版への改定）
	分析・検証プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	—	（1）2018年（平成29年）4月～2018年（平成30年）12月 （2）国土交通省、航空運送事業者、定期航空協会 （3）「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月改定）を踏まえるとともに「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」（平成30年7月改定）を参考。
改定状況	改定の実施状況	2019年度以降に先送り（理由：2017年度にサイバー攻撃対応に係る改訂を実施し、2017年5月に第3版追補3を発刊したため）	2018年度に実施済
	改定プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	—	（1）2018年4月～2019年3月末 （2）国土交通省 （3）「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月改定）（以下「策定指針」という。）を踏まえるとともに「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」（平成30年7月改定）を参考にしながら、重要インフラ事業者等と調整の上、改訂。
	改定内容	—	・策定指針の改定を踏まえた見直し（「機能保証」の考え方、経営層の在り方、コンティンジェンシープラン及び事業継続計画等の整備、CSIRT等の整備、関連部門との役割分担等の合意など） ・政府統一基準の考え方を踏まえた見直し（クラウドサービスの利用など） ・ガイドライン名称の見直し ・全体構成や表現の見直し
記載項目を包括的に確認し、安全基準等に必要項目を漏れなく記載していますか	はい（第5版の記載項目）	はい（第5版の記載項目、第4版の記載項目）	
独自記載項目	金融機関における固有業務や設備設置に係る基準等	政府統一基準群を参考にして追加している項目がある。 なお、今後、安全基準等策定指針の改定に際して、以下の意見を提出いたします。 策定指針中、【「安全基準等」で規程が望まれる項目】は概念的な記述が多く、また、制御系については広く浅い言及にとどまっているという印象です。一方、政府統一基準群では、安全基準等策定指針より詳細な記載もあり、セキュリティ対策について網羅的に記載され、政府で保有する制御系システムについても当該基準を基に対策を講じております。 政府統一基準群は公表資料であるため民間企業でも参考にされており、さらに同じNISC内で策定されているものであることから、これを活用して策定指針のブラッシュアップを図っていただくことで、我が国のサイバーセキュリティ対策を同じ方向性をもって取り組むことが可能となるものと考えます。 政府統一基準群は網羅的に記載されているが故に制御系システムに特化した記述はありませんが、制御系システムを有する重要インフラ分野が多いことを踏まえ、策定指針のブラッシュアップの際には、制御系システムを念頭においた項目をさらに盛り込んでいただきたいと思います。 なお、そのようなすることで、策定指針は、国の整備する制御系システムの安全対策にも役立つものになると考えます。	

調査結果（詳細） 6 / 1 2

分野	空港	鉄道
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
発行主体等	国土交通省	国土交通省
最新改定／新規作成年月	2019年（平成31年）3月29日	2019年（平成31年）3月29日
分析・検証状況	分析検証の実施状況	2018年度に実施済
	分析検証の実施契機	安全基準等策定指針の改定（第5版への改定）
	分析・検証プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	（1）2018年（平成29年）4月～2018年（平成30年）12月 （2）国土交通省、主要な空港・空港ビル事業者 （3）「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月改定）を踏まえるとともに「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」（平成30年7月改定）を参考。
改定状況	改定の実施状況	2018年度に実施済
	改定プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	（1）2018年4月～2019年3月末 （2）国土交通省 （3）「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月改定）（以下「策定指針」という。）を踏まえるとともに「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」（平成30年7月改定）を参考にしながら、重要インフラ事業者等と調整の上、改訂。
	改定内容	<ul style="list-style-type: none"> 策定指針の改定を踏まえた見直し（「機能保証」の考え方、経営層の在り方、コンティジェンシープラン及び事業継続計画等の整備、CSIRT等の整備、関連部門との役割分担等の合意など） 政府統一基準の考え方を踏まえた見直し（クラウドサービスの利用など） 全体構成や表現の見直し
記載項目を包括的に確認し、安全基準等に必要項目を漏れなく記載していますか	はい（第5版の記載項目、第4版の記載項目）	はい（第5版の記載項目、第4版の記載項目）
独自記載項目	<p>政府統一基準群を参考にして追加している項目がある。</p> <p>なお、今後、安全基準等策定指針の改定に際して、以下の意見を提出いたします。</p> <p>策定指針中、【「安全基準等」で規程が望まれる項目】は概念的な記述が多く、また、制御系については広く浅い言及にとどまっているという印象です。一方、政府統一基準群では、安全基準等策定指針より詳細な記載もあり、セキュリティ対策について網羅的に記載され、政府で保有する制御系システムについても当該基準を基に対策を講じております。</p> <p>政府統一基準群は公表資料であるため民間企業でも参考にされており、さらに同じNISC内で策定されているものでもあることから、これを活用して策定指針のブラッシュアップを図っていただくことで、我が国のサイバーセキュリティ対策を同じ方向性をもって取り組むことが可能となるものと考えます。</p> <p>政府統一基準群は網羅的に記載されているが故に制御系システムに特化した記述はありませんが、制御系システムを有する重要インフラ分野が多いことを踏まえ、策定指針のブラッシュアップの際には、制御系システムを念頭においた項目をさらに盛り込んでいただきたいと思います。</p> <p>なお、そのようにすることで、策定指針は、国の整備する制御系システムの安全対策にも役立つものになると考えます。</p>	<p>政府統一基準群を参考にして追加している項目がある。</p> <p>なお、今後、安全基準等策定指針の改定に際して、以下の意見を提出いたします。</p> <p>策定指針中、【「安全基準等」で規程が望まれる項目】は概念的な記述が多く、また、制御系については広く浅い言及にとどまっているという印象です。一方、政府統一基準群では、安全基準等策定指針より詳細な記載もあり、セキュリティ対策について網羅的に記載され、政府で保有する制御系システムについても当該基準を基に対策を講じております。</p> <p>政府統一基準群は公表資料であるため民間企業でも参考にされており、さらに同じNISC内で策定されているものでもあることから、これを活用して策定指針のブラッシュアップを図っていただくことで、我が国のサイバーセキュリティ対策を同じ方向性をもって取り組むことが可能となるものと考えます。</p> <p>政府統一基準群は網羅的に記載されているが故に制御系システムに特化した記述はありませんが、制御系システムを有する重要インフラ分野が多いことを踏まえ、策定指針のブラッシュアップの際には、制御系システムを念頭においた項目をさらに盛り込んでいただきたいと思います。</p> <p>なお、そのようにすることで、策定指針は、国の整備する制御系システムの安全対策にも役立つものになると考えます。</p>

調査結果（詳細） 7 / 1 2

分野	電力	電力	
名称	電力制御システムセキュリティガイドライン	電気設備の技術基準の解釈	
発行主体等	一般社団法人 日本電気協会	経済産業省	
最新改定／新規作成年月	2016年5月	2018年10月	
分析・ 検証 状況	分析検証の実施状況	実施中	2018年度に実施予定なし（理由：引用している民間規格が改定手続き中で、改定が次年度になるため）
	分析検証の実施契機	その他状況の変化等（ユーザーからの要望による）	—
	分析・検証プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	（1）2018年12月～2019年10月 （2）情報専門部会 （3）電気事業者主体の分科会・作業会で、分析・検証を実施。改定案も含めて検討し、上位の会議体で審議。	—
改定 状況	改定の実施状況	—	—
	改定プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	—	—
	改定内容	—	—
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか	はい（第5版の記載項目）	はい（第5版の記載項目）	
独自記載項目	電力制御システムに特化する内容は安全基準等策定指針には含まれていないことがある。	電力制御システムやスマートメーターに特化する内容は安全基準等策定指針には含まれていないことがある。	

調査結果（詳細） 8 / 12

分野	電力	電力	
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	スマートメーターシステムセキュリティガイドライン	
発行主体等	経済産業省	一般社団法人 日本電気協会	
最新改定／新規作成年月	2016年9月	2016年3月	
分析・検証状況	分析検証の実施状況	2018年度に実施予定なし（理由：2016年度に改定されたところであり、環境変化がないため。）	実施中
	分析検証の実施契機	—	安全基準等策定指針の改定（第5版への改定）/その他状況の変化等（ユーザーからの要望による）
	分析・検証プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	—	（1）2018年12月～2019年10月 （2）情報専門部会 （3）電気事業者主体の分科会・作業会で、分析・検証を実施。改定案も含めて検討し、上位の会議体で審議。
改定状況	改定の実施状況	—	—
	改定プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	—	—
	改定内容	—	—
記載項目を包括的に確認し、安全基準等に必要項目を漏れなく記載していますか	いいえ（本ドキュメントは保安規程の記載事項に特化した内容のため、該当部分のみを参照。）	はい（第5版の記載項目）	
独自記載項目	なし	スマートメーターシステムに特化している内容は安全基準等策定指針に含まれていないことがある	

調査結果（詳細） 9 / 12

分野	ガス	政府・行政サービス
名称	製造・供給に係る制御系システムのセキュリティ対策ガイドライン	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
発行主体等	一般社団法人 日本ガス協会	総務省自治行政局地域情報政策室
最新改定／新規作成年月	2016年7月	2018年9月
分析・検証状況	分析検証の実施状況	実施中 2018年度に実施予定なし（理由：2017年以前に分析・検証実施済）
	分析検証の実施契機	— その他状況の変化等（2018年3月METIガス安全小委員会を踏まえ、都市ガス業界におけるサイバーセキュリティ保安規程化が決定したため）
	分析・検証プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	— （1）2018年4月～2019年3月（予定） （2）JGAシステムセキュリティWG （3）保安規程化の決定を踏まえ、要領改訂内容についてシステムセキュリティWGにて検討中。その結果を、上位組織の保安対策小委員会に報告し、改訂を行うことを正式決定予定。
改定状況	改定の実施状況	— 2018年度に実施済
	改定プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	— （1）平成29年12月～平成30年9月 （2）総務省自治行政局地域情報政策室（調査研究受託事業者：日本電気株式会社） （3）①改定項目の整理→②有識者へのヒアリング→③改定案の作成→④有識者検討会議の開催→⑤パブコメ→⑥改定
	改定内容	— 「政府機関の情報セキュリティ対策の統一基準」等の反映
記載項目を包括的に確認し、安全基準等に必要項目を漏れなく記載していますか	はい（第5版の記載項目、第4版の記載項目）	はい（第4版の記載項目）
独自記載項目	なし	なし

調査結果（詳細） 10/12

分野	医療	水道
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版）	水道分野における情報セキュリティガイドライン
発行主体等	厚生労働省	厚生労働省 医薬・生活衛生局水道課
最新改定／新規作成年月	2017年5月	2013年6月
分析・検証状況	分析検証の実施状況	2018年度に実施予定なし（理由：2017年以前に分析・検証実施済のため）
	分析検証の実施契機	—
	分析・検証プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	—
改定状況	改定の実施状況	2018年度に実施済
	改定プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	—
	改定内容	—
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか	いいえ（安全基準等策定指針よりも国内の法令や現場の実態に沿った要件を重視したため）	はい（第5版の記載項目、第4版の記載項目）
独自記載項目	なし	なし

調査結果（詳細） 11/12

分野	物流	化学
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
発行主体等	国土交通省	石油化学工業協会
最新改定／新規作成年月	2019年（平成31年）3月29日	2015年3月
分析・検証状況	分析検証の実施状況	2018年度に実施済
	分析検証の実施契機	安全基準等策定指針の改定（第5版への改定）
	分析・検証プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	（1）2018年（平成29年）4月～2018年（平成30年）12月 （2）国土交通省総合政策局物流政策課、重要インフラ事業者及び業界団体（17社6団体） （3）「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月改定）を踏まえるとともに「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」（平成30年7月改定）を参考。
改定状況	改定の実施状況	2018年度に実施済
	改定プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	（1）2018年4月～2019年3月末 （2）国土交通省 （3）「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月改定）（以下「策定指針」という。）を踏まえるとともに「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」（平成30年7月改定）を参考にしながら、重要インフラ事業者等と調整の上、改訂。
	改定内容	・策定指針の改定を踏まえた見直し（「機能保証」の考え方、経営層の在り方、コンティジェンシープラン及び事業継続計画等の整備、CSIRT等の整備、関連部門との役割分担等の合意など） ・政府統一基準の考え方を踏まえた見直し（クラウドサービスの利用など） ・全体構成や表現の見直し
記載項目を包括的に確認し、安全基準等に必要項目を漏れなく記載していますか	はい（第5版の記載項目、第4版の記載項目）	いいえ（この点も含めて、安全基準等の継続的改善のために分析・検証を実施しているところである。）
独自記載項目	政府統一基準群を参考にして追加している項目がある。 なお、今後、安全基準等策定指針の改定に際して、以下の意見を提出いたします。 策定指針中、【「安全基準等」で規程が望まれる項目】は概念的な記述が多く、また、制御系については広く浅い言及にとどまっているという印象です。一方、政府統一基準群では、安全基準等策定指針より詳細な記載もあり、セキュリティ対策について網羅的に記載され、政府で保有する制御系システムについても当該基準を基に対策を講じております。 政府統一基準群は公表資料であるため民間企業でも参考にされており、さらに同じNISC内で策定されているものであることから、これを活用して策定指針のブラッシュアップを図っていただくことで、我が国のサイバーセキュリティ対策を同じ方向性をもって取り組むことが可能となるものと考えます。 政府統一基準群は網羅的に記載されているが故に制御系システムに特化した記述はありませんが、制御系システムを有する重要インフラ分野が多いことを踏まえ、策定指針のブラッシュアップの際には、制御系システムを念頭においた項目をさらに盛り込んでいただきたいと思います。 なお、そのようにすることで、策定指針は、国の整備する制御系システムの安全対策にも役立つものになると考えます。	なし

調査結果（詳細） 12/12

分野	クレジット	石油	
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	
発行主体等	一般社団法人 日本クレジット協会	石油連盟	
最新改定／新規作成年月	2018年4月（最新改定）/2014年12月（新規）	2017年5月26日	
分析・検証状況	分析検証の実施状況	2018年度に実施済	2018年度に実施済
	分析検証の実施契機	ITに係る環境変化の調査・分析からの課題発見	安全基準等策定指針の改定（第5版への改定）
	分析・検証プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	（1）2018年4月に、日本クレジット協会クレジットCEPTOAR運営会議において協議	（1） （2）石油連盟 サイバーセキュリティ専門委員会 （3）指針第5版の改定内容や各社の取り組み状況を踏まえ、ITセキュリティ連絡会にて改定することを決定
改定状況	改定の実施状況	2018年度に実施済	実施中
	改定プロセス （1）実施時期 （2）実施主体 （3）実施の流れ	（1）2018年4月に、日本クレジット協会クレジットCEPTOAR運営会議において協議	（1）未定 （2）石油連盟 サイバーセキュリティ専門委員会、危機管理委員会 （3）サイバーセキュリティ専門委員会にて改定原案作成済。今後、上部組織である危機管理委員会を得て、正式改定となる
	改定内容	障害発生時に重要インフラ事業者が報告を行う際の「インシデント報告書（重要インフラサービス障害）」のフォーマットの変更	『指針第4版』の以下の新たな要請項目について「実施が望ましい項目」として追記 ①経営層の果たすべき役割、経営層による情報セキュリティ対策の運用状況把握 ②抽出した課題に基づくリスク評価の実施 ③基本方針の策定・見直しの実施 ④情報セキュリティ対策に係るロードマップの作成・見直しの実施
記載項目を包括的に確認し、安全基準等に必要な項目を漏れなく記載していますか	はい（第5版の記載項目） ※「クレジットCEPTOARにおける情報セキュリティガイドライン」には記載していないが、重要インフラについては、割販法のもと、PCIDSS準拠が義務付けられている。PCIDSSでは、「安全基準等策定指針」の記載項目をカバーしていることを包括的に確認している。	はい（第5版の記載項目）	
独自記載項目	なし	なし	