

サイバー・フィジカル・セキュリティ対策 フレームワーク（CPSF）改訂 CPSFの改訂概要

令和8年10月23日

経済産業省 商務情報政策局
サイバーセキュリティ課・情報経済課

0. アジェンダ

1. 本資料参照時のポイント
2. CPSFの改訂背景等
3. 対策要件IDの新旧対応表
4. CPSF本文の改訂について
5. 添付Bの改訂について
6. 添付Cの改訂について
7. 添付Dの改訂について
8. 添付Eの改訂について

1. 本資料参照時のポイント

① 本資料の位置付け

- 本資料は、CPSF Ver.1.0からVer.1.1への改訂背景及び改訂概要を把握するための資料である。

② CPSFの改訂背景等（P.3～7）

- 2019年に策定したCPSF Ver.1.0を改訂するに至った背景や今後の改訂方針等を示している。

③ 対策要件IDの新旧対応表（P.8～36）

- 当該対応表では、CPSF Ver.1.0の各対策要件が、Ver.1.1のどの対策要件に統合・対応しているかの確認が可能である。
- 変更履歴付きのCPSF Ver.1.1（Word版）では、対策要件改訂箇所を確認できる一方、新旧の対応関係までは示していないため、Ver.1.0との差分を確認する場合は本資料を参照されたい。

④ CPSF本文の改訂について（P.37）

- 今年度のCPSF本文の改訂は、第Ⅲ部の対策要件に関する部分が中心であり、その他の部分については大幅な修正を行っていない。このため、対策要件以外の具体的な改訂箇所については、変更履歴付きのCPSF Ver.1.1を参照されたい。

⑤ 添付Bの改訂について（P.38）

- 添付Bは、インシデント及びリスク源と対策要件の紐付けを示すものであるが、本年度は対策要件のみを改訂しているため、添付BについてVer.1.0とVer.1.1の新旧対応表等を示す必要性は低いと判断し、改訂イメージのみを示している。

⑥ 添付Cの改訂について（P.39～42）

- 添付Cの改訂内容は、対策要件・対策例・参照ガイドラインの主に3区分に分けられる。本資料では、このうち特に新規性の高い、新たに追加した対策例を後続頁に示している。対策要件の改訂内容については、前述の新旧対応表を、参照ガイドラインの改訂内容については、各発行元が公表する概要資料等を参照されたい。

⑦ 添付Dの改訂について（P.43）

- 添付Dにおいては、CPSF Ver.1.0で参照していた海外規格自体が改訂されていることから、Ver.1.0とVer.1.1の新旧対応表等を示す必要性は低いと判断し、改訂イメージのみを示している。

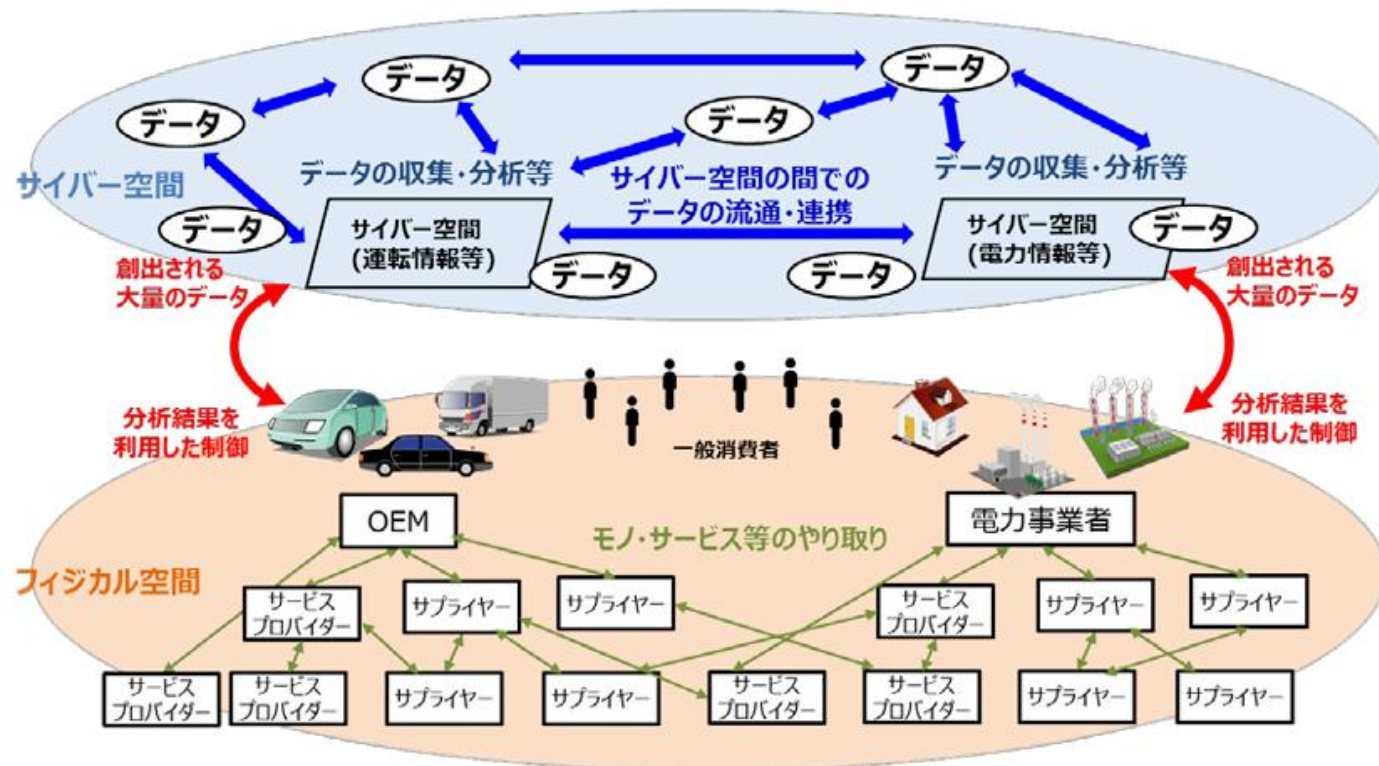
⑧ 添付Eの改訂について（P.44）

- 添付Eの改訂は、各用語の参照先としている規格等の更新が中心であるため、変更履歴付きの用語集を参照されたい。

2. CPSFの策定背景

- 第5期科学技術基本計画（平成28年1月22日閣議決定）にて提唱された「Society5.0」へ向けた歩みの中で、経済産業省は2019年に『サイバー・フィジカル・セキュリティ対策フレームワーク』（CPSF）を策定し、新たな産業社会において付加価値を創造する活動が直面するリスクを適切に捉えるためのモデルを構築し、リスク源を明らかにしつつ、産業界が自らのセキュリティ対応に活用できる対策等を取りまとめた。
- 2019年のCPSF策定後も、IoT・デジタルツイン、データスペース、ひいてはフィジカルAIの進展などを通じて、CPSFが提示するリスクや対策等に係る枠組みはますます汎用性と重要性を増していると考えられる。

CPSF 1.0 策定後の動き



データスペースの進展、
大規模言語モデル(LLM)等の高度化に伴う
セキュリティリスクの増大

IoT製品に対するセキュリティ制度の策定、
フィジカルAIの発展等に伴う
セキュリティリスクの増大

サプライチェーンのさらなる複雑化、
セキュリティ管理の重要性向上

2. CPSFの策定背景

- CPSFは、新たな産業社会におけるバリュークリエーションプロセス(※)全てを適用範囲として、各事業者が実施するセキュリティ対策のオペレーションレベルで活用できる、グローバルハーモナイゼーションの実現に貢献するものとして策定された。

フレームワークを策定 する目的と適用範囲

- 本フレームワークにおけるリスク源の洗い出しやセキュリティ対策の適用範囲は、新たな産業社会におけるバリュークリエーションプロセス(※)全てである。
※サイバー空間とフィジカル空間の両空間を跨いで、様々なモノやデータが動的につながって構成される付加価値の創造活動（「Society5.0」型のサプライチェーン）

フレームワークの 想定読者

- CISO（最高情報セキュリティ責任者）
- サプライチェーンマネジメントに関わる戦略・企画部門の担当者（主に第Ⅰ部）
- バリュークリエーションプロセスに関わる企業・団体等のセキュリティ担当者
- 情報関連機器、制御系機器の開発・品質保証、システム設計・構築・検証担当者
- データマネジメントの担当者
- 各産業分野におけるセキュリティ対策のガイドライン等を策定する業界団体等の担当者

フレームワークの特徴

- 各事業者が実施するセキュリティ対策のオペレーションレベルで活用できる。
- セキュリティ対策の必要性和適切な水準の対策例を示すことでコストの関係を把握できるようにする。
- グローバルハーモナイゼーションの実現に貢献する。

2. CPSFの改訂背景

- CPSFでは、全体を三部構成として、頻繁に見直しを行うべき部分（第Ⅲ部及び添付）と安定した基本コンセプトを示してフレームワークとしての信頼性を確保する部分（第Ⅰ部）を分けた構造としている。

CPSFの構成

第Ⅰ部【コンセプト】

サイバーセキュリティの観点から、バリュークリエーションプロセスにおけるリスク源を整理するためのモデル（三層構造と6つの構成要素）を整理。

安定した基本コンセプトを示して
フレームワークとしての信頼性を
確保する部分

第Ⅱ部【ポリシー】

第Ⅰ部で示したモデルを活用したリスク源の整理と、リスク源に対応する対策要件を提示。

第Ⅲ部【メソッド】

第Ⅱ部で示した対策要件に対応するセキュリティ対策例を提示。

添付

三層構造モデルを代表的な産業に適用した場合のユースケース
リスク源と対策要件の対応関係
対策要件に応じたセキュリティ対策例
海外の主要規格との対応関係
用語集

ISOやNIST CSF、NIST SPシリーズなどの
様々な国際標準を踏まえ、
頻繁に見直しを行うべき部分

2. CPSFの改訂背景

【CPSF1.0の策定経緯及び生じている主な課題】

- CPSFの策定時から約7年が経過し、以下の課題が生じている。
 - ① 対策要件及び対策例が、最新のセキュリティ動向を反映できていない。
 - NIST CSF 2.0への改訂をはじめ、SP 800-53 Rev.5、SP 800-171 Rev.3、ISO/IEC 27001:2022等、CPSF1.0の策定に用いた主要規格が相次いで更新されている。
(対策例についても、参照すべき基準が多岐にわたり、ユーザーにとって掘りどころとすべき文書が不明瞭な状態にある。)
 - ② AIによる新たなリスクへの対応が必要。
 - AIエージェントに関するセキュリティ対応技術の未成熟や、AIの能力高度化に伴う攻撃の激化・大規模化など、AIは新たなリスクをもたらすことが予想される。
 - 一方で、AIセキュリティに関する国際的なフレームワークは策定途上の段階にあり、現時点で未成熟な内容をCPSFに取り込むことは時期尚早ではないかと考えられる。



【改訂方針】

- **本年度：**課題①への対応として、最新の主要規格を基に第Ⅲ部(Methods)及び添付の改訂を実施する。
- **次年度以降：**課題②への対応に向けた準備として、AIセキュリティに関する国際的なフレームワークの策定動向や、AIがCPSに与えるリスクの調査及びその結果を踏まえ、必要に応じて第Ⅱ部(ポリシー)及び第Ⅲ部(メソッド)等を改訂する。
- **将来：**第2段階の成果を踏まえ、AIセキュリティに関する国際的なフレームワークが成熟した段階で、第Ⅰ部(コンセプト)の「バリューチェーンプロセスが展開する三層構造」及び「6つの構成要素」等の改訂を行うとともに、必要に応じて第Ⅱ部(ポリシー)及び第Ⅲ部(メソッド)等を改訂する。

2. CPSFの改訂背景

- CPSFの構成要素のうち、本年度は第Ⅲ部及び添付B～Eのみの更新を行う想定である。(第Ⅰ部・第Ⅱ部・添付Aは将来的に改訂予定)

No.	CPSFの構成	改訂の有無	改訂内容
1	第Ⅰ部 コンセプト： サイバー空間とフィジカル空間が高度に融合した産業社会における産業分野のサイバーセキュリティの在り方	—	✓ 最新のセキュリティ基準を反映することが今年度のスコープであることから、第Ⅰ部は今年度の改訂の対象外とする。 ✓ なお、今後策定されると想定されるAIに関する国際的なセキュリティフレームワークや、CPSFの国際標準化であるISO/IEC TS 5689等の内容を踏まえ、将来的に改訂予定。
2	第Ⅱ部 ポリシー： リスク源の洗い出しと対策要件の特定	—	✓ 同上。
3	第Ⅲ部 メソッド： セキュリティ対策要件と対策例集	○	✓ CPSF Ver.1.0で参照している国際的なフレームワーク(例：NIST CSF)の改訂内容を踏まえ、対策要件を改訂する。
4	添付A ユースケース	—	✓ 第Ⅰ部及び第Ⅱ部の内容を踏まえ、将来的に改訂予定。
5	添付B リスク源と対策要件の対応関係	○	✓ 第Ⅲ部で改訂した対策要件を踏まえ、リスク源との対応表を改訂する。
6	添付C 対策要件に応じたセキュリティ対策例	○	✓ 第Ⅲ部で改訂した対策要件を踏まえ、SCS評価制度の★3,★4の評価基準等を対策例として振り分けるとともに、参照ガイドラインを最新版に改訂する。
7	添付D 海外の主要規格との対応関係	○	✓ CPSF1.0で用いた主要規格(NIST CSF、NIST SP 800、ISO/IEC 27001)の最新版を参照の上、対策要件との対応表を改訂する。
8	添付E 用語集	○	✓ 各用語の参照元となる文書の最新版に基づき、既存用語の定義を更新するとともに、新たな用語を追加する。

3. 対策要件IDの新旧対応表（統治機能）

- CPSF Ver.1.1への改訂に伴い、第Ⅲ部対策要件における改訂内容の把握に資するため、対策要件IDの新旧対応表を作成した。

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
1	統治 (CPS.GV)	CPS.GV.OC-01	組織は、自組織のミッションを理解し、サイバーセキュリティリスクマネジメントにおける判断に用いる。	-	-
2		CPS.GV.OC-02	組織は、サイバーセキュリティに関する法的要求事項や、規制上の要件、契約上の要求事項（プライバシー及び市民的自由の義務を含む）、及び業界のガイドライン等を理解した上で、それらを考慮した社内ルールを策定する。	CPS.GV-2	個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。
				CPS.DP-2	監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する。
3		CPS.GV.OC-03	組織は、自組織が事業を継続する上で、自組織及び関係する他組織における依存関係と重要な機能を特定し、共有する。	CPS.BE-3	自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。
4		CPS.GV.RM-01	組織は、リスクマネジメントの目的を定め、関係するステークホルダーとの間で合意する。	-	-
5		CPS.GV.RM-02	組織は、サイバーセキュリティリスクマネジメントを適切に行うために、サイバーセキュリティ戦略を策定する。	CPS.GV-4	セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う。

3. 対策要件IDの新旧対応表（統治機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
6	統治 (CPS.GV)	CPS.GV.RM-03	組織は、自組織におけるリスク選好度及びリスク許容度を定め、組織内に周知する。	CPS.RM-2	リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。
7		CPS.GV.RM-04	組織は、サイバーセキュリティリスクマネジメントの活動及びその結果を、組織のリスクマネジメントプロセスに組み込み、当該プロセスの中でサイバーセキュリティリスクを管理する。	-	-
8		CPS.GV.RM-05	組織は、リスク対応における選択肢及びその運用に係る方針を策定し、組織内に共有する。	-	-
9		CPS.GV.RM-06	組織は、取引先及びその他の第三者によるリスクを含むサイバーセキュリティリスクについて、組織全体にわたるコミュニティシステムを明確にし、運用する。	-	-
10		CPS.GV.RM-07	組織は、サイバーセキュリティリスクの評価、文書化、分類及び優先順位付けに関する標準的な方法を整備し、組織内に共有する。	CPS.RM-1	自組織内におけるサイバーセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に係る自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。

3. 対策要件IDの新旧対応表（統治機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
11	統治 (CPS.GV)	CPS.GV.RM-08	組織は、戦略的機会（組織にとってプラスに働くリスク）を特定し、その特性を整理した上で、組織のサイバーセキュリティリスクに関する議論に含める。	-	-
12		CPS.GV.RR-01	組織の経営層は、サイバーセキュリティリスクに対する責任及び説明責任を負い、当該リスクを認識した上で、倫理的かつ継続的に改善する文化を醸成する。	-	-
13		CPS.GV.RR-02	組織は、自組織のサイバーセキュリティリスクマネジメントに関する役割、責任及び権限を定め、組織内へ周知する。	CPS.BE-1	サプライチェーンにおいて、自組織が担う役割を特定し共有する。
				CPS.AM-7	自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める。
14		CPS.GV.RR-03	組織は、セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を設置し、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	CPS.AE-2	セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える。
15		CPS.GV.RR-04	組織は、サイバーセキュリティ戦略、役割、責任及びポリシーに応じて、必要なリソースを確保する。	-	-

3. 対策要件IDの新旧対応表（統治機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
16	統治 (CPS.GV)	CPS.GV.RR-05	組織は、人の異動に伴い生じる役割の変更に 対応した対策に、セキュリティに関する事項 （例：アクセス権限の無効化、 従業員に対 する審査）を含める。	CPS.IP-9	人の異動に伴い生じる役割の変更に 対応した対策に、セキュリティに関する事項（例：ア クセス権限の無効化、 従業員に対する審 査）を含める。
17		CPS.GV.PO-01	組織は、自組織の状況、サイバーセキュリ ティ戦略、優先順位等に基づいてセキュリ ティポリシーを策定し、組織内及び自組織の 取引に関係する者（必要に応じてサプライ ヤー、第三者プロバイダ等を含む）に伝達し、 実施する。	CPS.GV-1	セキュリティポリシーを策定し、自組織及び 関係する他組織のセキュリティ上の役割と責 任、情報の共有方法等を明確にする。
				CPS.BE-2	あらかじめ定められた自組織の優先事業、優 先業務と整合したセキュリティポリシー・対 策基準を明確化し、 自組織の取引に関係す る者（サプライヤー、第三者プロバイダ等を 含む）に共有する。
18		CPS.GV.PO-02	組織は、要件、脅威、技術及び自組織のミッ ションの変化を踏まえ、セキュリティポリ シーを定期的にレビューし、必要に応じて更 新する。	-	-
19		CPS.GV.OV-01	組織は、サイバーセキュリティ戦略の成果を レビューし、当該結果及び内外の環境変化等 を踏まえ、サイバーセキュリティ戦略並びに 組織全体の戦略及び方向性を必要に応じて見 直す。	-	-

3. 対策要件IDの新旧対応表（統治機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
20	統治 (CPS.GV)	CPS.GV.OV-02	組織は、自組織のサイバーセキュリティリスクマネジメントの実施状況をレビューし、必要に応じて見直す。	-	-
21		CPS.GV.SC-01	組織は、サプライチェーンに係るリスクマネジメントに関するプログラム、戦略、目的、ポリシー及びプロセスを明確にし、組織のステークホルダーと合意の上、運用する。	-	-
22		CPS.GV.SC-02	組織は、取引先及びパートナーに対するサイバーセキュリティの役割と責任を定め、組織内外へ周知するとともに、必要に応じて内容の調整を行う。	CPS.AM-7	自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める。
				CPS.DP-1	セキュリティ事象の説明責任を果たせるよう、セキュリティ事象検知における自組織とサービスプロバイダが担う役割と負う責任を明確にする。
23		CPS.GV.SC-03	組織は、サイバーセキュリティサプライチェーンリスクマネジメントを、サイバーセキュリティ及び事業体のリスクマネジメント、リスクアセスメント、改善プロセスに統合する。	-	-
24	CPS.GV.SC-04	組織は、自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをする。	CPS.SC-2	自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	

3. 対策要件IDの新旧対応表（統治機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
25	統治 (CPS.GV)	CPS.GV.SC-05	組織は、取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について契約等を通じて取引先と合意する。	CPS.SC-1	取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。
				CPS.SC-5	取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。
				CPS.DS-1	組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取り決める。
26		CPS.GV.SC-06	組織は、サプライヤー及びその他の第三者との契約を締結する前に、当該サプライヤー等のサイバーセキュリティ管理態勢を評価し、必要に応じてリスク軽減に必要な措置を講ずる。	CPS.SC-3	外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。
27		CPS.GV.SC-07	組織は、取引先等の関係する他組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して、関係する他組織が提供する製品・サービスが適合していることを確認する。	CPS.SC-4	外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。

3. 対策要件IDの新旧対応表（統治機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
28	統治 (CPS.GV)	CPS.GV.SC-08	組織は、取引先等の関係する他組織が契約上の義務を果たしていることを確認するために、監査、テスト結果、又は他の形式の評価を使用して定期的に評価する。	CPS.SC-6	取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。
29		CPS.GV.SC-09	組織は、取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロセスを策定し、運用する。	CPS.SC-7	取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロセスを策定し、運用する。
30		CPS.GV.SC-10	組織は、技術製品及びサービスのライフサイクル全体を通じて、サプライチェーンに係るセキュリティ対策の実施状況を監視する。	-	-
31		CPS.GV.SC-11	組織は、取引先等との契約終了時に実施すべきプロセスを策定し、運用する。	CPS.SC-10	取引先等の関係する他組織との契約が終了する際（例：契約期間の満了、サポートの終了）に実施すべきプロセスを策定し、運用する。
32		CPS.GV.SC-12	組織は、自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8	自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。

3. 対策要件IDの新旧対応表（識別機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
33	識別 (CPS.ID)	CPS.ID.AM-01	組織は、システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1	システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。
34		CPS.ID.AM-02	組織は、組織内の通信ネットワーク構成図及びデータフロー図を作成し、適切に管理する。	CPS.AE-1	ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。
				CPS.AM-4	組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する。
35		CPS.ID.AM-03	組織は、自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.AM-5	自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。
36		CPS.ID.AM-04	組織は、リソース（例：モノ、データ、システム）を機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.AM-6	リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。

3. 対策要件IDの新旧対応表（識別機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
37	識別 (CPS.ID)	CPS.ID.AM-05	組織は、保有するデータ及びメタデータの一覧を作成し、適切に管理する。	-	-
38		CPS.ID.AM-06	組織は、システム、ハードウェア、ソフトウェア、サービス及びデータを、取得から廃棄に至るライフサイクル全体を通じて管理する。	-	-
39		CPS.ID.AM-07	組織は、自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める。	CPS.AM-2	自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める。
40		CPS.ID.AM-08	組織は、重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する。	CPS.AM-3	重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する。
41		CPS.ID.RA-01	組織は、自組織の資産の脆弱性を特定し、対応する資産と紐づけて管理する。	CPS.RA-1	自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。
42		CPS.ID.RA-02	組織は、組織内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2	セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。

3. 対策要件IDの新旧対応表（識別機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
43	識別 (CPS.ID)	CPS.ID.RA-03	・ 組織は、自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。 ・ IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.RA-3	自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。
				CPS.RA-4	・ 構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。 ・ IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。
44		CPS.ID.RA-04	組織は、構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施することにより、脆弱性を悪用する脅威の潜在的な影響と起こりやすさを識別する。	CPS.RA-4	・ 構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。 ・ IoT機器及びIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。
				CPS.RA-5	リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。

3. 対策要件IDの新旧対応表（識別機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
45	識別 (CPS.ID)	CPS.ID.RA-05	・組織は、保護技術の有効性について、適切なパートナーとの間で情報を共有する。	CPS.IP-8	保護技術の有効性について、適切なパートナーとの間で情報を共有する。
46		CPS.ID.RA-06	・組織は、リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化するとともに、その実施状況を把握し、関係者に共有する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。 ・IoT機器及びIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。
47		CPS.ID.RA-07	組織は、自組織における重要な変更及びセキュリティ要件の例外について、それらがもたらすリスクの影響度をアセスメントし、その結果を記録し、管理する。	-	-
48		CPS.ID.IM-01	組織は、CPS.ID.IM-02以降に示す観点を含め、自組織における平時又は有事のサイバーセキュリティ管理態勢を継続的に改善する。	-	-
49		CPS.ID.IM-02	組織は、サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。	CPS.SC-11	サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。

3. 対策要件IDの新旧対応表（識別機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
50	識別 (CPS.ID)	CPS.ID.IM-03	組織は、自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を継続的に改善する。	CPS.AT-3	自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。
51		CPS.ID.IM-04	組織は、セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを継続的に改善する。	CPS.IP-7	セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。
52		CPS.ID.IM-05	組織は、アラートやログ等の検知イベントの分析結果から教訓を導き出し、セキュリティ事象の検知プロセスを継続的に改善する。	CPS.DP-4	セキュリティ事象の検知プロセスを継続的に改善する。
53		CPS.ID.IM-06	組織は、セキュリティインシデントへの対応から教訓を導き出し、インシデント対応計画を継続的に改善する。	CPS.IM-1	セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する。
54		CPS.ID.IM-07	組織は、セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又は緊急時対応計画を継続的に改善する。	CPS.IM-2	セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又は緊急事対応計画を継続的に改善する。

3. 対策要件IDの新旧対応表（防御機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
55	防御 (CPS.PR)	CPS.PR.AA-01	組織は、承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1	承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。
56		CPS.PR.AA-02	組織は、IoT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で、信頼性の高い方式（例：多要素認証）を用いて認証・認可する。	CPS.AC-3	無線接続先（ユーザーやIoT機器、サーバ等）を正しく認証する。
				CPS.AC-6	特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。
				CPS.AC-8	IOT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。
				CPS.AC-9	IOT機器やユーザーによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。

3. 対策要件IDの新旧対応表（防御機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
57	防御 (CPS.PR)	CPS.PR.AA-03	組織は、一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ。	CPS.AC-4	一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ。
58		CPS.PR.AA-04	組織は、認証された主体に関する情報（IDアサーション）を保護し、送受信し、検証する。	-	-
59		CPS.PR.AA-05	組織は、アクセス権限の付与に関する規定をセキュリティポリシーに定義し、最小特権と職務分離の原則を組み込む。	CPS.AC-5	職務及び責任範囲（例：ユーザー／システム管理者）を適切に分離する。
60		CPS.PR.AA-06	組織は、アクセス権限の付与状況について、定期的に見直しを行い、不要又は過剰な権限を是正する。	-	-
61		CPS.PR.AA-07	組織は、IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2	IOT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。

3. 対策要件IDの新旧対応表（防御機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
62	防御 (CPS.PR)	CPS.PR.AT-01	組織は、自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1	自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。
63		CPS.PR.AT-02	組織は、自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	CPS.AT-2	自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。
64		CPS.PR.DS-01	組織は、各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3	各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。

3. 対策要件IDの新旧対応表（防御機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
65	防御 (CPS.PR)	CPS.PR.DS-02	組織は、保存しているデータの機密性、完全性、及び可用性を保護する。	CPS.DS-2	情報を適切な強度の方式で暗号化して保管する。
				CPS.DS-5	送受信、保管データの暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。
				CPS.DS-11	送受信・保管する情報に完全性チェックメカニズムを使用する。
66		CPS.PR.DS-03	組織は、伝送中のデータの機密性、完全性、及び可用性を保護する。	CPS.DS-3	IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。
				CPS.DS-4	情報を送受信する際に、情報そのものを暗号化して送受信する。
				CPS.DS-5	送受信、保管データの暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。
				CPS.DS-11	送受信・保管する情報に完全性チェックメカニズムを使用する。
67		CPS.PR.DS-04	組織は、使用中のデータの機密性、完全性、及び可用性を保護する。	-	-

3. 対策要件IDの新旧対応表（防御機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
68	防御 (CPS.PR)	CPS.PR.DS-05	組織は、データの取得元、加工履歴等をライフサイクル全体に渡って維持・更新・管理する。	CPS.DS-14	データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する。
69		CPS.PR.DS-06	組織は、データ（例：構成要素の設定情報、業務データ等を含む）に対し、定期的なバックアップを実施し、バックアップデータの保護及び復旧のテストを行う。	CPS.IP-4	構成要素（IoT機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする。
70		CPS.PR.PS-01	組織は、ハードウェア及びソフトウェアの真正性と完全性を、取得及び使用前に評価するとともに、稼働中もハードウェア及びソフトウェアの完全性を検証する。	CPS.DS-12	ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する。
				CPS.DS-13	IoT機器やソフトウェアが正規品であることを定期的（起動時等）に確認する。
71		CPS.PR.PS-02	組織は、保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。	CPS.DS-8	保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。
72		CPS.PR.PS-03	組織は、計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、適切なセキュリティ対策を実装した製品を利用する。	CPS.DS-15	計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する。

3. 対策要件IDの新旧対応表（防御機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
73	防御 (CPS.PR)	CPS.PR.PS-04	組織は、ネットワークにつながることを踏まえた安全性を実装するIoT機器を導入する。	CPS.PT-3	ネットワークにつながることを踏まえた安全性を実装するIoT機器を導入する。
74		CPS.PR.PS-05	組織は、セキュアなソフトウェア開発プラクティス（例：設計段階でのセキュリティレビュー、セキュアコーディング規約の適用、リリース前の脆弱性診断）をシステム開発ライフサイクルに統合し、その実施状況を確認する。	CPS.IP-3	システムを管理するためのシステム開発ライフサイクルを導入する。
75		CPS.PR.PS-06	組織は、IoT機器、サーバ等のハードウェア及びソフトウェアに対する構成管理の対策（不要なネットワークポート、USB、シリアルポート等の物理的または論理的な閉塞による機能の必要最小化を含む）を確立し、適用する。	CPS.IP-1	IOT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。
				CPS.IP-2	IOT機器、サーバ等の導入後に、追加するソフトウェアを制限する。
				CPS.PT-2	IOT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。

3. 対策要件IDの新旧対応表（防御機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
76	防御 (CPS.PR)	CPS.PR.PS-07	組織は、不正なソフトウェアのインストール及び実行を防止する。	CPS.DS-10	IoT機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。
				CPS.DS-13	IoT機器やソフトウェアが正規品であることを定期的（起動時等）に確認する。
77		CPS.PR.PS-08	組織は、脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.IP-10	脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。
78		CPS.PR.PS-09	組織は、IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.MA-1	・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 ・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。
79		CPS.PR.PS-10	組織は、自組織のIoT機器、サーバ等に対する保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.MA-2	自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。

3. 対策要件IDの新旧対応表（防御機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
80	防御 (CPS.PR)	CPS.PR.PS-11	組織は、セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、継続的にログを記録し、レビューする。	CPS.PT-1	セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。
81		CPS.PR.PS-12	組織は、IoT機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規IoT機器、サーバ等を一意に識別するID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする。	CPS.IP-6	IOT機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規IoT機器、サーバ等を一意に識別するID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする。
82		CPS.PR.IR-01	組織は、ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等して、認可されていないアクセス及び使用からネットワーク及び環境を保護する。	CPS.AC-7	データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。
				CPS.DS-9	自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。

3. 対策要件IDの新旧対応表（防御機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
83	防御 (CPS.PR)	CPS.PR.IR-02	組織は、無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.IP-5	無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。
84		CPS.PR.IR-03	組織は、平時及び有事において、システム及びサービスの継続稼働に関する要件を達成するための仕組みを実装する。	-	-
85		CPS.PR.IR-04	組織は、サイバー攻撃（例：ランサムウェア、サービス拒否攻撃等）を受けた場合でも、攻撃による影響を最小限に抑え、重要な機能を維持できるよう、十分なリソース（例：ヒト、モノ、システム）を確保する。	CPS.DS-6	サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例：ヒト、モノ、システム）を確保する。
				CPS.DS-7	IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。

3. 対策要件IDの新旧対応表（検知機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
86	検知 (CPS.DE)	CPS.DE.CM-01	組織は、セキュリティ事象を適切に検知できるよう、ネットワーク及びネットワークサービスを監視する。	CPS.CM-1	組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。
87		CPS.DE.CM-02	組織は、セキュリティ事象を適切に検知できるよう、IoT機器、サーバ等のハードウェア及びソフトウェアの稼働状況、並びにネットワーク接続状況等を監視する。	CPS.CM-6	機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。
88		CPS.DE.CM-03	組織は、セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容を監視する。	CPS.CM-5	セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。
89		CPS.DE.CM-04	組織は、セキュリティ事象を適切に検知できるよう、組織内外の要員による構成要素（モノ／システム等）へのアクセスや操作等の活動を監視する。	CPS.CM-6	機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。
90		CPS.DE.CM-05	組織は、IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.CM-2	IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。

3. 対策要件IDの新旧対応表（検知機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
91	検知 (CPS.DE)	CPS.DE.CM-06	組織は、自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.CM-7	自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。
92		CPS.DE.CM-07	組織は、サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	CPS.CM-4	サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。
93		CPS.DE.CM-08	- 組織は、指示された動作内容と実際の動作結果を比較して異常の検知や動作の停止を行うIoT機器を導入する。 - 組織は、サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.CM-3	- 指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行うIoT機器を導入する。 - サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。
94		CPS.DE.CM-09	組織は、監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。	CPS.DP-3	監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。

3. 対策要件IDの新旧対応表（検知機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
95	検知 (CPS.DE)	CPS.DE.AE-01	組織は、潜在的なセキュリティ事象について分析を行い、当該事象の内容を把握する。	-	-
96		CPS.DE.AE-02	組織は、セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。	CPS.AE-3	セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。
97		CPS.DE.AE-03	組織は、関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する。	CPS.AE-4	関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する。
98		CPS.DE.AE-04	組織は、セキュリティ事象がインシデントに該当するか否かの判定基準を定め、当該基準を満たす場合にインシデントの宣言を行う。	CPS.AE-5	セキュリティ事象の危険度の判定基準を定める。

3. 対策要件IDの新旧対応表（対応機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
99	対応 (CPS.RS)	CPS.RS.MA-01	組織は、セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1	セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。
				CPS.SC-9	サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。
100		CPS.RS.MA-02	組織は、セキュリティインシデントとして報告された事象について、誤検知や重複報告でないことを確認し、インシデントとしての妥当性を確認する。	-	-
101		CPS.RS.MA-03	組織は、検知されたセキュリティインシデントを、影響度の大小や侵入経路等に基づき分類し、優先順位を付ける	CPS.AN-3	検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。
				CPS.AE-5	セキュリティ事象の危険度の判定基準を定める。

3. 対策要件IDの新旧対応表（対応機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
102	対応 (CPS.RS)	CPS.RS.MA-04	組織は、セキュリティインシデントが宣言された場合、取引先等の関係する他組織と連携し、あらかじめ定めた対応手順に基づきインシデント対応を実行する。	CPS.RP-2	セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。
103		CPS.RS.MA-05	組織は、セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ（製品）に対して適切な対応を行う。	CPS.RP-4	セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ（製品）に対して適切な対応を行う。
104		CPS.RS.MA-06	組織は、セキュリティインシデントの特性及び復旧活動が業務に与える影響を考慮し、あらかじめ定めた基準に基づき復旧の開始を判断する。	-	-
105		CPS.RS.AN-01	組織は、セキュリティインシデントに関するデータ及びメタデータ（インシデント対応において実施した措置の履歴等を含む）を収集し、それらの完全性を確保するとともに、取得元及び取得時点等が参照可能な状態で保管する。	-	-

3. 対策要件IDの新旧対応表（対応機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
106	対応 (CPS.RS)	CPS.RS.AN-02	組織は、セキュリティインシデント発生後に、根本原因を特定するためのデジタルフォレンジックを実施する。その際、調査過程の記録を改ざんされない形で保管する。	CPS.AN-2	セキュリティインシデント発生後に、デジタルフォレンジックを実施する。
107		CPS.RS.AN-03	組織は、セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。	CPS.AN-1	セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。
108		CPS.RS.CO-01	組織は、セキュリティインシデント発生後の、組織内部及び外部への情報公表に関するルールを策定し、運用する。	-	-
109		CPS.RS.CO-02	組織は、定めたルールに基づき、組織内部の上位意思決定者及び関係する外部組織に対し、必要に応じてエスカレーションを行う。	-	-
110		CPS.RS.MI-01	組織は、セキュリティインシデントによる被害の拡大を最小限に抑え、原因の除去又は影響の低減を行う。	CPS.MI-1	セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う。

3. 対策要件IDの新旧対応表（復旧機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
111	復旧 (CPS.RC)	CPS.RC.RP-01	組織は、自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急時対応計画の中にセキュリティインシデントを位置づける。	CPS.RP-3	自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。
112		CPS.RC.RP-02	組織は、インシデント後の運用方針を定めるにあたり、重要な業務機能及びサイバーセキュリティリスクマネジメントの結果を踏まえる。	-	-
113		CPS.RC.RP-03	組織は、復旧フェーズへの移行が判断された場合、あらかじめ定めた復旧計画に基づき復旧を実行する。	-	-
114		CPS.RC.RP-04	組織は、バックアップ及びその他の復旧資産の完全性を、使用前に検証する。	-	-
115		CPS.RC.RP-05	組織は、復旧した資産の完全性を検証するとともに、システム及びサービスを復旧し、正常な運用状態であることを確認する。	-	-
116		CPS.RC.RP-06	組織は、あらかじめ定めた基準に基づき、インシデント復旧の終了を宣言するとともに、インシデントに関する文書の作成を完了する。	-	-

3. 対策要件IDの新旧対応表（復旧機能）

CPSF Ver.1.1				CPSF Ver.1.0	
No.	機能	対策要件ID	対策要件	対策要件ID	対策要件
117	復旧 (CPS.RC)	CPS.RC.CO-01	組織は、セキュリティインシデント発生後の、復旧に向けた情報交換に関するルールを策定し、運用する。	CPS.CO-1	セキュリティインシデント発生後の情報公表時のルールを策定し、運用する。
118		CPS.RC.CO-02	組織は、事業継続計画又は緊急時対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。	CPS.CO-2	事業継続計画又は緊急事対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。
119		CPS.RC.CO-03	組織は、復旧活動について内部及び外部のステークホルダーと役員、そして経営陣に伝達する点を、事業継続計画又は緊急時対応計画の中に位置づける。	CPS.CO-3	復旧活動について内部及び外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急事対応計画の中に位置づける。

4. CPSF本文の改訂について

対策要件以外のCPSF本文における改訂内容については、
変更履歴付きのCPSF Ver.1.1を参照されたい。

5. 添付Bの改訂について

- 添付Bのリスク源と対策要件の対応関係のうち、本年度は「対策要件及び対策要件ID」の列のみ、改訂を行っている。

<本年度の改訂対象>

第Ⅲ部で改訂を行った対策要件を基に、リスク源との紐づけを行っている。

■ 第1層における機能/想定されるセキュリティインシデント/リスク源/対策要件

#	機能	想定されるセキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
1_1	組織として平時のリスク管理体制を構築し、適切に運用すること	自組織で管理している領域から保護すべきデータが漏洩する	・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・入力確認の不備を突いたインジェクション攻撃(例: SQLインジェクション、XSS) ・ネットワーク上の通信の盗聴 ・保護が必要なエリアに対する不正なヒトの物理的な侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・正規ユーザによる内部不正	L1_1_a_ORG	[ソシキ] ・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	・リソース(例: モノ、データ、システム)を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリスクに関わる組織やヒトに伝達する。	CPS.AM-6
				L1_1_a_PEO	[ヒト] ・自身が関わりうるセキュリティやセーフティに関するリスクに対して十分な認識を有していない	・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者(サプライヤー、第三者プロバイダ等を含む)に共有する。	CPS.BE-2
					[ヒト] ・ヒトに関わるセキュリティやセーフティに関するリスクに対するガバナンスが十分でない	・取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。	CPS.SC-1
						・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・システムを管理するためのシステム開発ライフサイクルを導入する。	CPS.IP-3
						・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
						・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	CPS.SC-5
						・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項(例: アクセス権限の無効化、従業員に対する審査)を含める。	CPS.IP-9

<将来的に改訂予定>

本年度は、フレームワークとしての信頼性確保の基点となる第Ⅰ部及び第Ⅱ部は改訂対象外である。したがって、第Ⅱ部で規定された機能・セキュリティインシデント、及び当該インシデントを基に抽出された脅威と脆弱性についても、本年度は改訂を行わない。
ただし、AIがCPSに与えるリスク等の調査結果を踏まえ、将来的には改訂を行う予定。

6. 添付Cの改訂について

- 添付Cの主な構成要素のうち、①対策要件及び③参照ガイドラインについては、第Ⅲ部で改訂した対策要件及び下記ガイドラインの最新版を参照しつつ、それぞれ更新を行っている。
- ②の対策例については、CPSF Ver. 1.0に採用したNIST SP-800等に加え、最新のセキュリティ動向を踏まえた具体的な記述を備えているSCS評価制度の評価基準等も踏まえて改訂している。(次頁以降に、新規追加した対策例を中心とした、機能ごとの改訂概要を示している。また、次頁以降に示すもののほか、必要に応じて軽微な修正を実施している。)

① 第Ⅲ部で改訂した
対策要件に更新

② SCS評価制度や、CSF2.0 実装例、CPGs等を踏まえ、
Basic/Advanced/High-Advancedの3区分に振り分け

③ CPSF1.0に用いた5つの参照ガイドラインを
それぞれ最新版に更新

対策要件ID	対策要件	対応する 脆弱性ID	対策例	対策例を実行 する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS_AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L2_1_a_ORG, L2_3_b_ORG, L2_3_b_SYS	<High-Advanced> - 組織は、自組織の情報システム及び産業用制御システムを構成する資産（IoT機器等を含むハードウェア、ソフトウェア、情報）を一意に特定し、各々の資産に管理責任者を割り当てた上で、資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、定期的又はオペレータ等の求めに応じて、リアルタイムで状況を把握しながら目録を維持・管理する。 - 情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 - 情報システム及び産業用制御システムは、許可されていない資産を自動的に検出し、管理情報から外す・システムから切り離す等を実行するメカニズムを導入、運用している。 ※ 関連する対策要件に、CPS_CM-6がある。 [参考] 重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）のP.44～P.46 に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティリスク分析ガイド 第2版」（IPA, 2018年）のP.21に記載された事業被害の大きさにおける評価を用いる方法等がある	O/S	○ (3.4.2)	○ (下記に加えて、 CM-8(1), CM-8(2), CM-8(3), CM-8(5))	○ (下記に加えて、 A.8.1.3)	-	-
			<Advanced> - 資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 - 組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 - 組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がないとき、このようなデバイスの使用を禁止する。 - 組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。		○				
			<Basic> - 組織は、自組織の情報システムや産業用制御システムを構成する資産（ハードウェア、ソフトウェア、情報）を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。 - 資産は保有するものすべてを一覧化することが望ましいが、対象が膨大な場合、分析対象の統合（グループ化）と分析対象からの除外を通じて、対象とする資産を絞り込むことを検討する。 - 組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。 [参考] 資産目録（情報資産管理台帳）の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）のP.47を参照することが可能である。また、対象の絞り込みに関するより詳細な説明は、「制御システムのセキュリティリスク分析ガイド 第2版」（IPA, 2018年）における 3.1.4. 分析対象とする資産の絞り込み を参照することが可能である。		○ (3.4.1, 3.8.5, 3.8.7, 3.8.8)	○ (CM-8, PM-5)	○ (A.8.1.1, A.8.1.2)	○ (4.2.3.4)	○ (SR 7.8)

6. 添付Cの改訂について

- 添付Cの改訂内容のうち、新規追加した主な対策例について、6機能ごとに改訂の観点を整理した。
- 「統治」機能については、経営層の関与の強化や、リスクマネジメントの対象・手段の拡充等の観点から対策例を追加した。
- 「識別」機能については、管理対象の把握・管理や、脅威の把握・特定、セキュリティ態勢の継続的な改善等の観点から対策例を追加した。

No.	対策要件における各機能	対策例の改訂概要（新規追加した主要な対策例を中心に記載）
1	統治（CPS.GV）	以下の対策例を追加した。 - 自組織のサイバーセキュリティ態勢に対する経営層の関与促進に向けた、経営層への当該態勢の報告頻度及び方法の決定と、経営層の関与の下でのサプライチェーンサイバーセキュリティリスクの取扱い。（GV.RM-06、GV.SC-03） - サイバーセキュリティに関するリスクをプラス面とマイナス面の両面から捉えるための、戦略的機会の特定、両面のリスクの算定及び優先順位付け。（GV.RM-08） - サイバーリスクへの対応手段の拡充に向けた、サイバー保険の加入要否の判断。（GV.RM-05）
2	識別（CPS.ID）	以下の対策例を追加した。 - データや製品・サービス等の継続的保護に向けた、組織内に分散する保護対象データの定期的な把握及びデータの取得元・管理責任者等の付帯情報の保護。また、製品・サービス等のライフサイクル全体を通じたセキュリティの確保。（ID.AM-05、ID.AM-06） - 脅威に関する情報の把握及び潜在脅威の特定に向けた、脅威インテリジェンスの活用及び脅威ハンティングの実施。（ID.RA-02、ID.RA-03） - 自組織のセキュリティ態勢の継続的な改善に向けた、ペネトレーションテスト及び第三者評価等の実施。また、サプライヤーと連携した演習及びインシデント発生後の共同振り返りの実施。（ID.IM-01、ID.IM-06）

6. 添付Cの改訂について

- 「防御」機能については、認証・認可の強化や、データセキュリティにおける使用中のデータの保護、システム・サービスの継続稼働等の観点から対策例を追加した。
- 「検知」機能については、セキュリティ事象の監視・検知の強化及びインシデント分類の精緻化等の観点から対策例を追加した。

No.	対策要件における各機能	対策例の改訂概要（新規追加した主要な対策例を中心に記載）
3	防御（CPS.PR）	以下の対策例を追加した。 - 認証・認可の強化に向けた、IDアサーションの保護、アクセス権の定期的な棚卸し及びゼロトラストアーキテクチャの導入。（PR.AA-04、PR.AA-06、PR.IR-01） - 使用中のデータの漏えいや不正利用の防止に向けた、プロセッサやメモリ上に残存するデータの削除及び同一システム上の他のユーザー・プロセスからのアクセスの防止。（PR.DS-04） - システム及びサービスの継続稼働への影響の抑制に向けた、単一障害点の防止及び負荷分散の活用。（PR.IR-03）
4	検知（CPS.DE）	以下の対策例を追加した。 - セキュリティ事象に係る監視対象の拡充に向けた、ハードウェアの改ざん、ソフトウェアの標準設定からの逸脱及びストレージ・電源等の利用状況の監視。（DE.CM-02） - 攻撃活動の検知手法の拡充に向けた、デセプション技術を利用した監視。（DE.CM-04） - インシデントの重要度を対応判断に反映させるための、インシデントレベルに基づく分類の実施。（DE.AE-04）

6. 添付Cの改訂について

- 「対応」機能については、インシデント対応プロセスの強化や、経営層による意思決定の支援等の観点から対策例を追加した。
- 「復旧」機能については、復旧資産の適切性の検証、インシデント対応で得られた教訓の活用及び復旧に関するコミュニケーションの強化等の観点から対策例を追加した。

No.	対策要件における各機能	対策例の改訂概要（新規追加した主要な対策例を中心に記載）
5	対応（CPS.RS）	以下の対策例を追加した。 - インシデントの誤検知や重複報告の防止に向けた、初期段階におけるインシデント報告の妥当性確認。（RS.MA-02） - インシデント対応に係る経営層の意思決定の支援に向けた、経営層へのインシデント状況の報告。（RS.CO-02） - 復旧活動中の業務継続に向けた、当該活動が業務に及ぼす影響の確認。（RS.MA-06）
6	復旧（CPS.RC）	以下の対策例を追加した。 - 復旧後の再侵害の防止に向けた、復旧に用いる資産の使用前における完全性検証。（RC.RP-04） - 復旧した資産の本番環境への適切な移行に向けた、移行前における侵害の痕跡等の検証、及び移行後の性能等の監視。（RC.RP-05） - インシデント対応で得られた教訓の活用に向けた、事後報告書の作成。（RC.RP-06） - 復旧対応に対する関係者の理解及び協力の確保に向けた、復旧状況及び再発防止策の組織内外への周知。（RC.CO-01）

7. 添付Dの改訂について

- 添付Dは、海外の主要規格との対応関係を示す、3種類の対応表（D.1・D.2・D.3）から構成されている。
- CPSF Ver.1.1への改訂にあたり、各対応表で参照する主要規格をそれぞれ最新版に更新するとともに、第Ⅲ部で改訂した対策要件との対応関係を整理した。

構成	CPSF Ver.1.0		CPSF Ver.1.1
D.1	NIST CSF1.1のサブカテゴリと、CPSF Ver.1.0の対策要件の対応表	▶	NIST CSF2.0 のサブカテゴリと、 CPSF Ver.1.1 の対策要件の対応表
D.2	NIST SP 800-171(Rev.1)及びSP 800-53(Rev.4)と、CPSF Ver.1.0の対策要件及び対策例の対応表	▶	NIST SP 800-171(Rev.3)及び800-53(Rev.5)と、 CPSF Ver.1.1 の対策要件及び対策例の対応表
D.3	ISO/IEC 27001:2013 付属書Aと、CPSF Ver.1.0の対策要件及び対策例の対応表	▶	ISO/IEC 27001: 2022 付属書Aと、 CPSF Ver.1.1 の対策要件及び対策例の対応表

8. 添付Eの改訂について

添付Eの改訂内容については、
変更履歴付きの用語集を参照されたい。

END