2019.07.01

情報セキュリティニュース ＜2019 No.1＞

経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク」の概要

【要旨】
■経済産業省は、サイバー・フィジカル・セキュリティ対策フレームワーク（以下、CPSF）を策定、2019 年 4 月 18 日に公開した。
■サイバー空間と現実（フィジカル）空間が高度に融合する「Society5.0」における産業社会では、ネットワーク化されたサプライチェーン上にサイバー攻撃の起点が拡散するとともに、攻撃の影響がフィジカル空間にまで及び、被害が影響する範囲も広くなることが懸念される。
■CPSF では、新たなサプライチェーン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）をサイバーセキュリティの観点から整理、このモデルを活用したリスク源の整理と対策要件、具体的な対策例を提示している。
■本レポートでは、CPSF の概要を整理するとともに活用のポイントを解説する。

1. CPSF策定に至った背景と経緯

IoT（Internet of Things）技術の進展で、工場設備の稼働状況、自動車の走行時の記録、人の健康状態など現実（フィジカル）空間の情報は、センサーなどを介してデータとしてサイバー空間に送信・蓄積できるようになり、蓄積されたデータは人工知能（AI）による解析によって新たな価値が付加されてフィジカル空間にフィードバックされる。

日本においては、2016 年 1 月 22 日に閣議決定された「第 5 期科学技術基本計画」において、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society 5.0」を提唱している。さらに、「Society 5.0」へ向けて、ヒト・モノ・データ・技術・企業など様々なつながりによって新たな付加価値を創出する「Connected Industries」の実現に向けた産業構造の構築が求められている。

「Society5.0」では、価値の源泉となるデータが多種多様な場所で生成されることから、製品・サービスを生み出す工程＝サプライチェーンは、従来の上流から下流へとつながる定型的・直線的なものではなく、データの生成と流通の流れを交えた複雑なものとなる。このような「Society5.0」におけるサプライチェーンを「価値創造過程（バリュークリエイションプロセス）」と称している。

サイバー空間とフィジカル空間が高度に融合する「Society5.0」における産業社会では、ネットワーク化されたサプライチェーン上にサイバー攻撃の起点が拡散するとともに、攻撃の影響がフィジカル空間にまで及び、被害が影響する範囲も広くなることが懸念される。

従来のサイバーセキュリティは、システム自体や生成されるデータ自体にフォーカスした対策が多くあるが、「Society 5.0」時代において直面する新たなサイバーセキュリティリスクに対応するために「サイバー・フィジカル・セキュリティ対策フレームワーク（以下 CPSF）」が策定された。

２．CPSFの構成

CPSF は、バリュークリエイションプロセスにおけるサイバーセキュリティの観点からリスク源を的確に捉え、それに対応していく指針としての役割を担っていくべく、全体を三部構成としている。これに添付Ａ．～Ｅ．の 5 種類の文書が付属する。

（1）第Ⅰ部「コンセプト」

サイバーセキュリティの観点から、バリュークリエイ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。

（２）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。

（３）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。

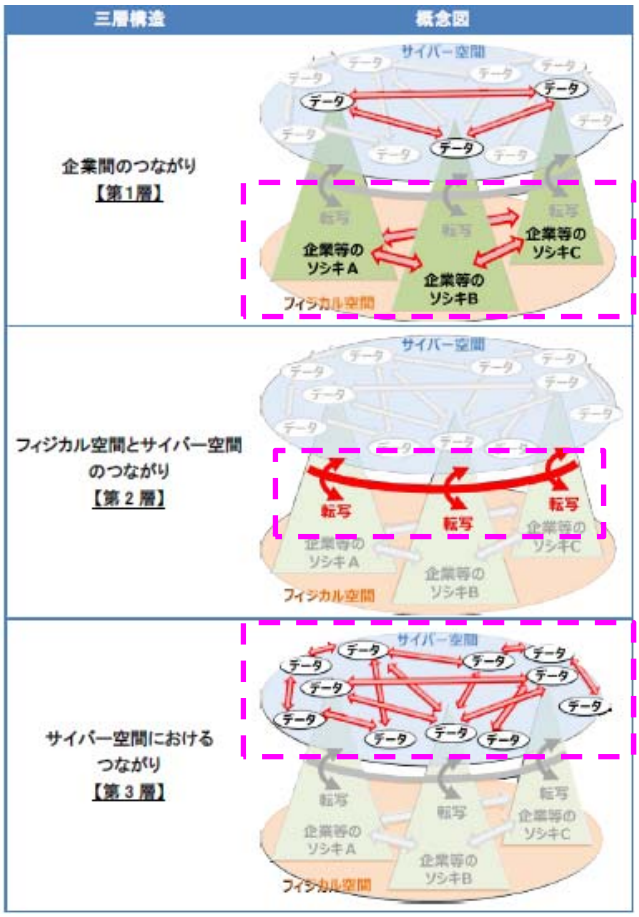
（添付）

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（添付Ａ）、各層におけるリスク源と対策要件の対応関係（添付Ｂ）、対策要件に応じたセキュリティ対策例（添付Ｃ）、海外の主要規格との対応関係（添付Ｄ）、用語集（添付Ｅ）

３．CPSFの特徴

従来のサプライチェーンでは、サプライチェーンの各当事者がセキュリティ対策をしっかり行っていれば、サプライチェーン全体のセキュリティが確保されるという考え方が成立していた。これに対し、「Society5.0」時代のサプライチェーン＝バリュークリエイションプロセスでは、データの連携主体が多様化し、なかには IoT 機器のように無機的にデータを提供する主体も含まれることから、当事者によるセキュリティ対策の実施だけで信頼性を確保することは困難である。

CPSF では、従来のサプライチェーンにおける当事者のつながりに加え、データの生成・流通の領域におけるつながりまでを対策の範囲としており、これを「三層構造」と表現している。



【図 1】バリュークリエイションプロセスが展開する産業社会の三層構造

（出典：CPSF）

また、対策を講じる上で最適な最小単位としてバリュークリエイションプロセスに関与する構成要素を 6 つに整理している。

【表 1】バリュークリエイションプロセスに関わる 6 つの構成要素

構成要素	定義
ソシキ	バリュークリエイションプロセスに参加する企業・団体・組織
ヒト	ソシキに属する人、及び価値創造過程に直接参加する人
モノ	ハードウェア、ソフトウェア、及びそれらの部品 操作する機器を含む
データ	フィジカル空間にて収集された情報、及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	定義された目的を達成するための一連の活動の手続き
システム	目的を実現するためにモノで構成される仕組み・インフラ

（出典：CPSF）

「三層構造」モデルにおける各層で守るべきものとリスク源を抽出し、6 つの構成要素について各リスク源に対する対策要件及び具体的な対策例を示すのが、CPSF の基本構成である。各層の信頼性の基点となる構成要素のセキュリティを各主体がそれぞれ確保することによって、バリュークリエイションプロセス全体のセキュリティ確保が実現される。

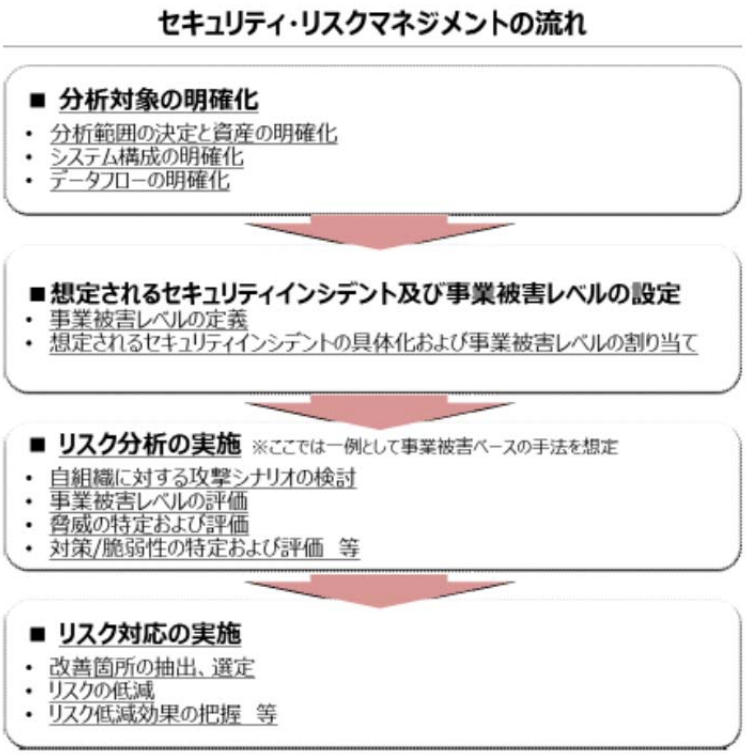
【表 2】各層におけるセキュリティ対策の概要

	第 1 層 企業間のつながり （従来のサプライチェーン）	第 2 層 フィジカル空間とサイバー空間のつながり （データの生成）	第 3 層 サイバー空間におけるつながり （データの流通）
確保すべき信頼性の基点	適切なマネジメントを基盤とした各主体の信頼性	フィジカル・サイバー間を正確に“転写“する機能の信頼性	自由に流通し、加工・創造されるサービスを創造するためのデータの信頼性
機能 （守るべきもの）	・ 平時および緊急時のリスク管理・対応体制の構築と運用 ・ 企業内および企業間のリスク管理・対応体制の構築と運用	・ フィジカル空間とサイバー空間の境界における情報の正確な転写および正確な転写の証明	・ データの加工・分析 ・ データの保管 ・ データの送受信
セキュリティインシデント	・ 保護すべき資産の棄損 ・ 他組織のセキュリティ事象発生に起因する事業停止	・ 不正確なデータの送信 ・ 安全に支障をきたす動作	・ 保護すべきデータの漏えい ・ なりすまし等による不正な組織からのデータ受信
リスク源 （構成要素ごとに整理）	・ セキュリティリスクに対するガバナンスの欠如 ・ 他組織との連携状況の未把握	・ 不正な IoT 機器との接続 ・ 許容範囲外の入力データ	・ 通信経路が保護されていない ・ 通信相手を識別していない
対策	各組織・関係者に求められるセキュリティ対策 （セキュリティポリシー） ・ マネジメントルールの徹底 ・ 関係者との役割分担	転写機能を考慮した、モノ（ハード・ソフト）に求められるセキュリティ対策 ・ 接続相手の認証 ・ 安全な IoT 機器の導入	組織を越えてデータを利活用する際のセキュリティ対策 ・ 暗号化によるデータ保護 ・ データの提供者の信頼性確認

（出典：CPSF に基づきＭＳ＆ＡＤインターリスク総研が作成）

４．CPSF の活用

CPSF・第 II 部では、一般的なリスクマネジメントプロセス（JIS Q 31000:2010 や JISQ 27001:2014 等）に基づいた手順が記載されており、前述の三層構造モデルと 6 つの構成要素を活用し、バリュークリエイションプロセスの特徴をとらえたセキュリティリスクマネジメントを進めることができる。



【図 2】リスクマネジメントの流れ
（出典：CPSF）

なお、添付Ｂでは、各層の機能ごとに想定されるセキュリティインシデントと、それらを引き起こすリスク源（脅威および典型的な脆弱性）を整理しており、加えて、それぞれのリスク源に対応する対策要件も整理されている。

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	対策要件ID
		脅威	脆弱性ID	脆弱性		
下記すべてに関わる • データを加工・分析する機能 • データを保管する機能 • データを送受信する機能	サービス拒否攻撃により、関係する他組織における自組織のデータを取り扱うシステムが停止する	システムを構成するサーバ等の電算機器、通信機器等に対するDoS攻撃	L3_3_b_ORG	[ソシキ] ・データの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない	サービスやシステムの運用において、サービスマネジメントを効率的、効果的に運営管理するサービスサプライヤーを選定する	CPS.SC-2

脆弱性は、６つの構成要素別に記載。
対策要件IDで添付Cの詳細な対策例を参照可能。

【図 3】添付Ｂ：リスク源と対策要件の対応関係
（出典：CPSFに基づきＭＳ＆ＡＤインターリスク総研が作成）

また、添付Ｃでは、添付Ｂで示した「対策要件」に実際に対応するための「対策例」を示しており、ここに記載された「対策例」に沿った対策を実践することで、自組織のセキュリティマネジメントの強化または改善を実現していくことができる。

「対策例」は、自組織のセキュリティマネジメントの「対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）」、「対策を導入・運用する際の相対的コスト」等を考慮して対応すべきレベルを「High-Advanced」「Advanced」「Basic」の三段階のレベルに分けて記載されており、企業は自組織に最適な水準の対策を選択することができる。

加えて、各「対策例」と、主要な国際規格等との対応関係を記載しており、自社・自組織の規程や施策と関連する国際規格の整合性を確認することができる。

【図 4】添付Ｃ：対策要件に応じたセキュリティ対策例

（出典：CPSF に基づきＭＳ＆ＡＤインターリスク総研が作成）

サイバー空間とフィジカル空間がつながり、データの変換や流通が行われる領域では、デバイス、ソフトウェア、通信手段など新たな要素が多数導入され、これらの要素に関わる当事者も増加している。こうした状況では、当事者の多様化がリスクの増大につながるとともに、インシデント発生時の各当事者の責任範囲が不明確になり、対応が混乱することも懸念される。

CPSF は、サイバー空間とフィジカル空間の関係を三層構造で表現し、階層ごとに 6 つの構成要素に落とし込んだ対策を自組織だけでなく関係するサプライチェーン上の取引先にも求めることで、各当事者の責任範囲を明確にしつつ、取引先へのセキュリティガバナンスの強化につなげることが可能と示している。

一方、それぞれの産業分野においては、産業構造や商慣行などの観点から、業界や企業により、守るべき重要な資産、人的・資金的リソース、又は許容できるリスク等が異なっている実態がある。こうした各産業分野の持つ特徴を踏まえつつ、それぞれの組織の状況に応じてセキュリティ対策を選定することが肝要である。

ＭＳ＆ＡＤインターリスク総研㈱　リスクマネジメント第四部
マネージャー・上席コンサルタント　　木村　文彦

ＭＳ＆ＡＤインターリスク総研株式会社は、ＭＳ＆ＡＤインシュアランス グループのリスク関連サービス事業会社として、リスクマネジメントに関するコンサルティングおよび広範な分野での調査研究を行っています。
情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研㈱
リスクマネジメント第四部　事業継続マネジメント第一グループ
千代田区神田淡路町2-105 TEL:03-5296-8918／FAX:03-5296-8941
https://www.irric.co.jp/

本誌は、マスコミ報道など公開されている情報に基づいて作成しております。
また、本誌は、読者の方々に対して企業のＲＭ活動等に役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。

不許複製／Copyright ＭＳ＆ＡＤインターリスク総研 2019