

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

IoT セキュリティ・セーフティ・フレームワーク  
～フィジカル空間とサイバー空間のつながりの信頼性の確保～

(案)

## 30 目次

31	<b>1. 本フレームワークの必要性</b> .....	3
32	<b>1-1 CPSFにおける第2層（フィジカル空間とサイバー空間のつながり）</b> .....	3
33	1-1-1 CPSF 概論 .....	3
34	1-1-2 第2層の位置づけ .....	3
35	<b>1-2 本フレームワークの目的</b> .....	5
36	<b>2. 本フレームワークの想定読者</b> .....	5
37	<b>3. 本フレームワークの基本構成</b> .....	6
38	<b>3-1 基本構成の背景にある考え方</b> .....	6
39	<b>3-2 フィジカル・サイバー間をつなげる機器・システムに潜むリスクの整理</b> .....	6
40	3-2-1 第1軸：発生したインシデントの影響の回復困難性の度合い .....	7
41	3-2-2 第2軸：発生したインシデントの経済的影響の度合い（金銭的価値への換算） .....	8
42	3-2-3 フィジカル・サイバー間をつなげる機器・システムのカテゴライズ .....	9
43	<b>3-3 求められるセキュリティ・セーフティ要求の整理</b> .....	10
44	3-3-1 第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求 .....	11
45	.....	
46	3-3-2 第2の観点：運用中のフィジカル・サイバー間をつなぐ機器・システムの確認要求 .....	12
47	3-3-3 第3の観点：機器・システムの運用・管理を行う者の能力に関する確認要求 .....	12
48	3-3-4 第4の観点：その他、社会的なサポート等の仕組みの要求 .....	12
49	<b>4. 本フレームワークの活用方法</b> .....	13
50		
51		
52		
53		
54		
55		
56		
57		
58		
59		

## 60 1. 本フレームワークの必要性

### 61 1-1 CPSF における第 2 層(フィジカル空間とサイバー空間のつながり)

#### 62 1-1-1 CPSF 概論

63 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いては、製品・サービスという  
64 価値を生み出す工程(サプライチェーン)が従来の定型的・直線的なものから、多様なつながり  
65 による非定型的なものへと変化している。このような新たな価値創造過程(バリュークリエイショ  
66 ンプロセス)のセキュリティ上の課題とその対策を整理することによって、新たな産業社会のセキ  
67 ュリティを確保していく考え方をまとめたものが、サイバー・フィジカル・セキュリティ対策フレーム  
68 ワーク(CPSF)である。CPSF では、「バリュークリエイションプロセスのセキュリティ確保に当たっ  
69 ては、従来のサプライチェーンで想定されているマネジメントの信頼できる企業間のつながりに  
70 よって付加価値が創造される領域を越えて、フィジカル空間の情報が IoT によってデジタル化さ  
71 れ、データとしてサイバー空間に取り込まれ、そうしたデータがサイバー空間で自由に流通する  
72 ことで、多様なデータが新たなデータを生み出して付加価値を創出することや、新たに創出され  
73 たデータが IoT によってフィジカル空間にフィードバックされることで新たな製品やサービスを創  
74 出するという、新たな付加価値を創造するための一連の新たな活動を視野に入れる必要があ  
75 る」とし、企業間のつながりに信頼性の基点を置く第 1 層、フィジカル空間とサイバー空間のつ  
76 ながりに信頼性の基点を置く第 2 層、サイバー空間におけるつながりに信頼性の基点を置く第  
77 3 層という異なる 3 つの信頼性の基点を設定し、この基点を中心に経済社会全体のセキュリティ  
78 上の課題の洗い出しとその対策をまとめている。

79

#### 80 1-1-2 第 2 層の位置づけ

81 第 2 層は、サイバー空間とフィジカル空間の境界であり、その境界において情報が正確に変  
82 換されること、つまり転写機能の正確性を確保することを、第 2 層における信頼性の基点として  
83 いる。一般に、サイバー空間とフィジカル空間の境界は、例えばセンサやアクチュエータなどか  
84 ら構成される、いわゆる IoT のシステムによって成立している。したがって、IoT 機器・システム  
85 のセキュリティを確保することが、第 2 層におけるセキュリティ対策の中核となる。

86 一方、第 2 層におけるセキュリティ上の課題は一様ではない。CPSF においても、以下のよう  
87 に複数の事例が示されている。

- 88 ・ センサの機能に対するサイバー攻撃の結果、フィジカル空間のデータが正しく転写できず  
89 に誤ったデータがサイバー空間へ提供され、データを利活用して実施されるオペレーション  
90 に対する信頼を喪失

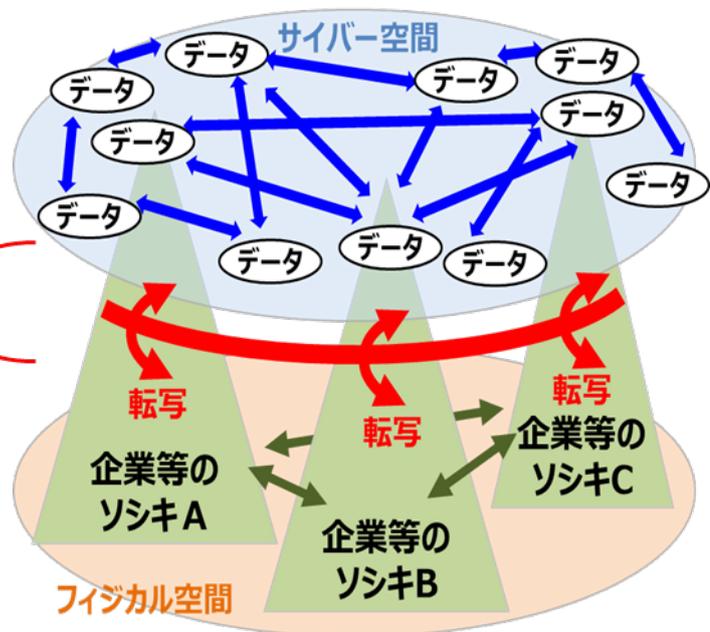
- 91 ・ サイバー空間からの間違った指示や IoT 機器への攻撃により、フィジカル空間において機  
92 器の制御が誤った形で実施され、従業員等への物理的な危害、機器の損壊等による安全  
93 上の問題が発生
- 94 ・ サイバー攻撃等によって IoT 機器・システムの機能が停止  
95 また、サイバー空間とフィジカル空間をつなぐ IoT 機器・システムの管理における課題につい  
96 ても以下のように触れている。
- 97 ・ 組織等において、IoT 機器の担う役割の重要性に応じて、設置区域管理やモニタリングの  
98 実施等の多層的な対策の検討が必要。
- 99 ・ 個人によって家庭などに設置される IoT 機器には、組織等による管理が行き届きにくいも  
100 のが存在するため、盗難、紛失のリスクを考慮した対策の実施が必要。

101 このように、第 2 層におけるセキュリティ対策には、IoT 機器・システムに関連する課題の多  
102 様性だけでなく、その利用される環境の多様性も踏まえた対応が必要である。こうした多様性に  
103 対し、CPSF では、3 層構造アプローチを通じてリスク源と対策要件を整理し、対策要件に対応し  
104 たセキュリティ対策例を示している。その際には、セーフティの確保を大前提として、機能安全の  
105 観点からの対策やサイバーセキュリティ対策を組み合わせる必要があるとして  
106 いる。

**サイバー空間におけるつながり**  
**【第3層】**  
 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**  
 を確保

**フィジカル空間と  
 サイバー空間のつながり**  
**【第2層】**  
 フィジカル・サイバー間を正確に  
**“転写”する機能の信頼性**を確保  
 (現実をデータに転換するセンサーや  
 電子信号を物理運動に転換するコ  
 ントローラ等の信頼)

**企業間につながり**  
**【第1層】**  
 適切な**マネジメントを基盤に**  
**各主体の信頼性**を確保



107 図1 CPSF における 3 層構造モデルと各層における信頼性  
 108

## 109 1-2 本フレームワークの目的

110 IoT セキュリティガイドライン<sup>1</sup>でも触れられているように、簡易な情報サービスの分野に使用さ  
111 れるIoT 機器と、工場や社会インフラシステム等の安全に関わる分野で使用されるIoT 機器で  
112 は、求められるセキュリティレベル、セキュリティ対策の目的、優先度が異なる。今後、IoT の活用  
113 の拡大に伴い、それぞれの分野の特殊性・多様性を踏まえて、使用分野ごとに個別・具体的な  
114 IoT 機器・システムに対して実際のセキュリティ対応が進んでいくことになると考えられる。その過  
115 程において、サイバー空間とフィジカル空間をつなぐ機器・システムのセキュリティ・セーフティに関  
116 して、包括的に課題を捉える統一的な手法が欠如しているため、それぞれの分野/業界において  
117 別々の検討プロセスを経て、独自のセキュリティ・セーフティ対策等が設定されることが懸念され  
118 る。それぞれの対応策に不整合が生じれば、社会として新たな仕組みを受容・管理していくための  
119 コストが増大する恐れがある。

120

121 本フレームワークは、上記のような事態を避けるため、サイバー空間とフィジカル空間をつなぐ  
122 新たな仕組みによってもたらされる新たなリスクに着目し、リスク形態及びそうしたリスクに対応す  
123 るセキュリティ・セーフティ対策の類型化の手法を提示するものである。すなわち、異なる分野/業  
124 界のプレイヤーがサイバー空間とフィジカル空間をつなぐ機器・システム、つまりIoT 機器・システ  
125 ムにおけるセキュリティ・セーフティの検討に資する枠組みを共有するための「基本的共通基盤」を  
126 提供し、IoT という新たな仕組みを社会として効果的に受容できるようにすることを目的とする。

127

## 128 2. 本フレームワークの想定読者

129 サイバー空間とフィジカル空間をつなぐ仕組みを構築し、新たな仕組み・サービスを実現していこ  
130 うとする者は、その仕組み・サービスが様々な形態で実現されることによって、そのセキュリティ上  
131 の課題も多様なものにならざるをえないことを認識し、そうした多様性を踏まえた適切なセキュリテ  
132 ィ対策を講じていかなければならない。新たな仕組み・サービスの革新性が高ければ高いほど、  
133 社会で受容していくためには、予想される様々な課題に対応した包括的な対策を講じることが求  
134 められることになる。

135 したがって、本フレームワークは、新たな仕組み・サービスを実現する主体が、新たなリスクに  
136 対するセキュリティ対策を講じようとする際に、また、そのような仕組み・サービスを利用する主体  
137 が本フレームワークの理解を通じてそのリスクを自ら認識した上でそうした仕組み・サービスを利

---

<sup>1</sup> IoT 推進コンソーシアム、総務省、経済産業省、平成 28 年 7 月策定

138 用する際に、それぞれ参照されることを想定しており、例えば、以下に示すような者を読者として  
139 想定している。

- 140 ・ IoT を活用してサイバー空間とフィジカル空間をつなぐ新たな仕組み・サービスを実現しよう  
141 とする者
- 142 ・ そのような新たな仕組み・サービスで活用される IoT 機器・システムの開発を行う者
- 143 ・ そのような新たな仕組み・サービスを適切に管理していく制度・環境を実現していこうとする  
144 者
- 145 ・ IoT による新たな仕組み・サービスを受ける者

146

### 147 3. 本フレームワークの基本構成

#### 148 3-1 基本構成の背景にある考え方

149 サイバー空間とフィジカル空間をつなぐ新たな仕組みには様々な形態及びそれに伴うセキュリティ  
150 上の課題があり、更に、実際にインシデントが発生した場合の被害の態様も極めて多様である。  
151 そのような仕組みを構成する機器・システムに対して一律のセキュリティ要求を設定した場合、仮  
152 にその要求が満たされていても、それでは多様なセキュリティ上の課題に十分に対応することは  
153 できない。すなわち、利用者等が適切に守られる状況であるとはいえない。

154 第 2 層のセキュリティ対策を検討する際のポイントは、この多様性に対してどのようにアプローチ  
155 するのか、ということである。

156 本フレームワークでは、サイバー空間とフィジカル空間をつなぐ新たな仕組み・サービスの“多様  
157 性”という論点にアプローチするための手段として、この仕組みを構成する機器・システム(これ以  
158 降「フィジカル・サイバー間をつなげる機器・システム」という。)について、リスクの捉え方とその対  
159 応に係る基本的な考え方を集約した 3 つの軸を活用し、カテゴライズするとともに、適切な対策の  
160 内容を整理して比較・検討できるようにすることを提案している。

161

#### 162 3-2 フィジカル・サイバー間をつなげる機器・システムに潜むリスクの整理

163 フィジカル・サイバー間をつなげる機器・システムのセキュリティ上の課題が実際にインシデント  
164 の発生へとつながった場合に影響が出る事象は、人命に関わるようなケースもあれば、プライバ  
165 シーに関わるケース、資産の毀損に関わるケース、生活環境に関わるケースなど、極めて多様で  
166 ある。つまり、フィジカル・サイバー間をつなげる機器・システムに潜むリスクは多様なものである。

167 しかしながら、インシデント発生によって影響を受ける事象ごとに整理を行うことは、フィジカル・  
168 サイバー間をつなげる機器・システムのセキュリティ対策を検討する上で、その考え方を逆に複雑

169 なものにしてしまうことになる。したがって、影響を受ける事象から何らかの共通項を抽出すること  
170 によって抽象化した少数の基準に絞り込み、フィジカル・サイバー間をつなげる機器・システムに  
171 潜むリスクをシンプルな形で整理できるようにする必要がある。

172 そのため、本フレームワークでは、様々な人命/身体、プライバシー/名誉、資産、生活環境、経  
173 済活動への影響、風評等の影響を受ける様々な事象を以下の2つの基準に抽象化して整理し  
174 て、フィジカル・サイバー間をつなぐ機器・システムに潜むリスクのカテゴリ化を行う2つの軸とし  
175 て設定することとした。

### 176 177 3-2-1 第1軸:発生したインシデントの影響の回復困難性の度合い

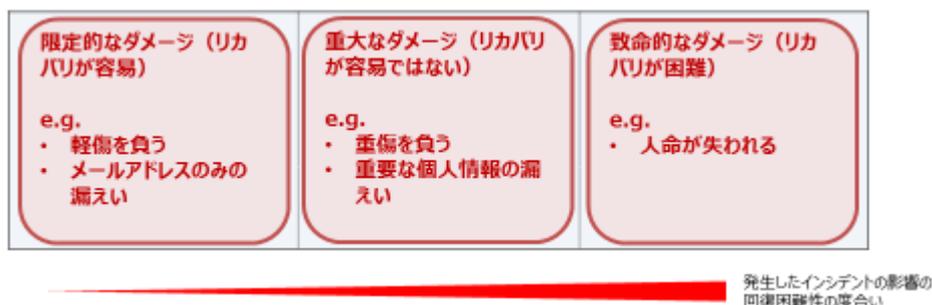
178 この第1軸はインシデントの影響の回復の困難性からリスクを捉えるものである。回復の困  
179 難性については、まず、何よりも人命/身体に関する影響から考えることが必要である。言うまで  
180 もないが、人命が失われればそれが回復されることはない。また、インシデントの発生の結果、  
181 重度の身体障害が発生した場合、完全に回復できるとはいえないケースが少なくない。回復が  
182 できるものであったとしても、早期に回復できるケースもあれば、回復に時間を要するケースも  
183 ある。こうした、インシデントによる影響が回復できるものか否か、また、回復ができるものにつ  
184 いては早期の回復ができるか否か、という判断軸を第1軸として設定した。

185 この第1軸は、製品安全、労働安全などの分野で法体系によって強制的に要求される安全  
186 対策や禁止行為を設定する規制の仕組みの基本的な考え方と同じ立場に立っており、既存の  
187 制度体系とも整合性を確保したものである。

188 第1軸では、上記のように、まずは人命/身体の回復不可能な状況を回避するという論点か  
189 ら考え方の整理を進めたが、個人のプライバシー/名誉に関わる情報の中には、一度明らかにな  
190 ってしまうと、本人に回復することができないダメージを与えるような機微な情報も含まれて  
191 おり、こうした本人に回復不可能なダメージを与える情報の保護に関わるような事象も第1軸で  
192 捉えられる課題に整理されるものである。

193 なお、「リスク」については、インシデントによる影響の度合いと、インシデントの発生確率を用  
194 いて捉えることがあるが、本フレームワークでは、フィジカル・サイバー間をつなぐ機器・システム  
195 の多様性を踏まえたカテゴリ化が容易に行えるように、算出が比較的難しい発生確率は考慮

196 せず、インシデントが発生した場合の影響の度合いからカテゴリ化を行うアプローチを採って  
197 いる。



198 図 2 発生したインシデントの影響の回復困難性の度合いのイメージ

199  
200 3-2-2 第 2 軸: 発生したインシデントの経済的影響の度合い(金銭的価値への換算)

201 第 2 軸は、インシデントによる影響の回復の可能性・困難性という観点を除き、インシデントに  
202 による影響の大きさを金銭的価値に換算した場合の大きさ・度合いを基準としたものである。

203 この基準は、3-2-1 で議論した人命/身体や深刻なプライバシー/名誉に関わるようなケース  
204 におけるインシデントによる影響の回復困難性を考慮したものではなく、その影響の回復につい  
205 ては金銭的価値に換算して捉えることが可能なものと仮定し、資産の毀損、経済活動や社会へ  
206 の影響等の事象を第 2 軸に写像して捉えることとした。

207 第 2 軸は第 1 軸とは独立して考えるべき基準であり、第 1 軸における整理において回復困  
208 難性の度合いが低いものとして捉えられたフィジカル・サイバー間をつなぐ機器・システムであっ  
209 ても、第 2 軸では経済的影響の度合いが非常に高いものとして整理されることは十分にある。  
210 一方で、第 1 軸における整理において回復困難性の度合いが高いものとして捉えられたフィジ  
211 カル・サイバー間をつなぐ機器・システムは、実際には賠償金等の形で金銭的価値に換算され  
212 る中で相応の水準に該当することになる可能性が高い。

213



図 3 発生したインシデントの経済的影響の度合いのイメージ

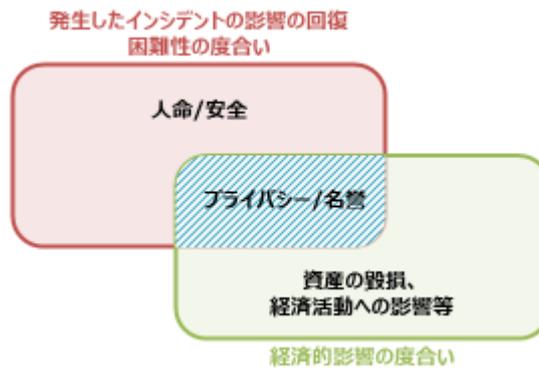


図 4 第 1 軸にも整理されうるプライバシー/名誉の整理

### 3-2-3 フィジカル・サイバー間をつなげる機器・システムのカテゴライズ

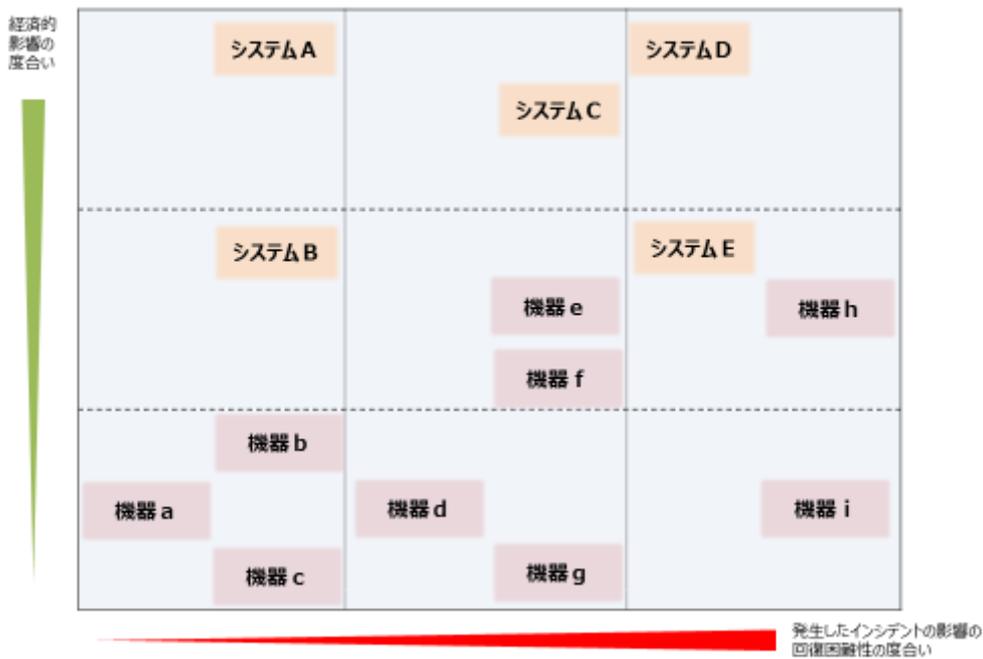
上述の 2 つの軸に基づいて、フィジカル・サイバー間をつなぐ機器・システムを、当該機器・システムに潜むリスクに基づいてマッピングすることができる。

例えば、第 1 軸では、回復困難性の観点から、限定的なダメージ(回復が容易)、重大なダメージ(回復が容易ではない)、致命的なダメージ(回復が困難)という形で整理し、第 2 軸では、経済的影響の観点から、限定的な経済的影響、重大な経済的影響、壊滅的な経済的影響という形で整理を行うことで、リスクに応じて 9 つの象限(カテゴリ)にカテゴライズすることが可能となる。

それぞれの機器・システムについて適切な対策を検討するに際し、このカテゴリを利用することができる。前述したとおり、フィジカル・サイバー間をつなぐ機器・システムのセキュリティ上の

228 課題は多様であるため、それぞれの機器・システムにおける適切な対策も一様ではない。しかし  
 229 ながら、このカテゴリに基づいて検討を行うことで、一般に右上にカテゴリ化されるものほどイ  
 230 ンシデントによる影響が大きい傾向があるため、より重厚な対策が必要であると考えられる一  
 231 方、左下にカテゴリ化されるものほど、軽微な対策で十分な可能性がある整理することが可  
 232 能となる。詳細は 3-3 で記載する。

233 なお、ここでは例として機器・システムのマッピングを行ったが、サービスを構成する機器・シ  
 234 ステムが提供する機能に着目してマッピングを行うことも考えられる。機器・システムの単位につ  
 235 いても、マッピングを行う際に任意に設定できるものである。また、同じ機器であったとしても、ど  
 236 ういうシステムで使われるか、システムにおいてどういう役割を持つのか、どのようなスキルを持  
 237 つ者が使うのか等、その用途により、その重要性や課題、インシデントによる影響等は大きく異  
 238 なる。そのため、同じ機器でも使用形態などによってマッピング先が異なり得ることに留意する  
 239 必要がある。



240 図 5 フィジカル・サイバー間をつなげる機器・システムのカテゴリ化のイメージ

241 (※ 同じ機器でも使用形態などによってマッピング先が異なり得る。

242 例えば、機器gと機器hが同じ機器で異なる使用形態である場合などがあり得る。)

243

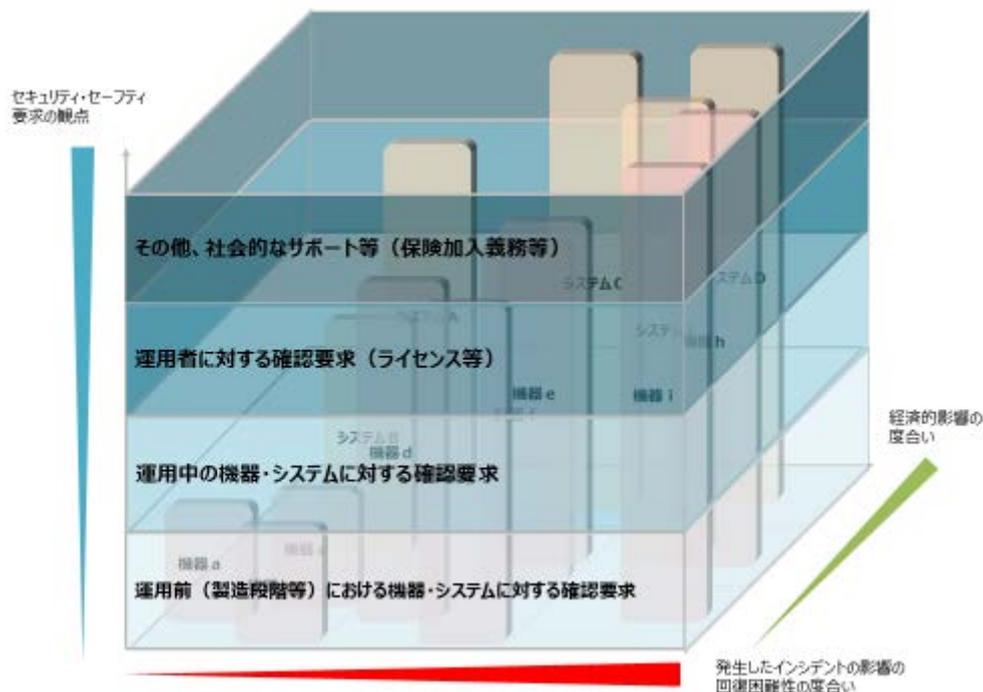
### 244 3-3 求められるセキュリティ・セーフティ要求の整理

245 上記 3-2-3 のとおり、第 1 軸と第 2 軸を活用し、フィジカル・サイバー間をつなぐ機器・システム  
 246 について、そのリスクを踏まえてカテゴリ化することが可能となるが、これだけでは、新たな仕組

247 み・サービスを社会として受容するための具体的な方策を検討することは難しい。そのため本フレ  
248 ームワークでは、フィジカル・サイバー間をつなぐ機器・システムのセキュリティ対策を包括的に整  
249 理するために、求められるセキュリティ・セーフティ要求の観点という第3軸を設定する。

250 第3軸は、第1軸と第2軸で形成される平面に直交する形で、いわば3次元を構成し、第1軸  
251 と第2軸によって整理されたそれぞれのカテゴリに求められるセキュリティ・セーフティ要求の観点  
252 を示す役割を果たすものである。

253 第3軸は、セキュリティ・セーフティを確保するための手法を以下の4つの観点から整理してい  
254 る。



255 図6 カテゴリに応じて求められるセキュリティ・セーフティ要求の観点のイメージ

256

257 3-3-1 第1の観点:運用前(製造段階等)におけるフィジカル・サイバー間をつなぐ機器・シ  
258 ステムの確認要求

259 フィジカル・サイバー間をつなぐ機器・システムが製造され、実際に利用に供される前の段階  
260 で、機器・システムそのものが必要なセキュリティ・セーフティ対策を講じられていること、又は当  
261 該機器等の生産者や供給者、検査者、場合によっては生産設備・工場等が必要な能力条件等  
262 を満たしていることなどを確認することを求めるものである。

263 セキュリティ・セーフティ対策については、その内容を供給者が自ら設定する場合と法令など  
264 によって強制的に設定されている場合がある。また、その内容が満たされていることを確認する方

265 法についても、自己適合宣言や第三者による認証など様々な形態があり、求められる確認レベ  
266 ルの専門性や客観性などを踏まえて実際の確認方法が設定されることになる。

267

268 3-3-2 第2の観点:運用中のフィジカル・サイバー間をつなぐ機器・システムの確認要求

269 機器・システムの運用前にセキュリティ・セーフティ対策の実施状況を確認しても、運用中に発  
270 生する故障や、実施されるソフトウェアのアップデートやメンテナンスなどによって、想定外の問  
271 題が発生する可能性がある。そのような問題が発生していないかを確認するために、運用開始  
272 後に、ライフサイクルやサービス期間も考慮しながら機器・システムを確認することを求めるもの  
273 である。

274 運用中のセキュリティ・セーフティ対策となるため、より高いレベルのセキュリティ・セーフティを  
275 確保することが可能となる。一方で、機器・システムの所有者・運用者が関与するか、機器・シス  
276 テムの所有権・管理権が供給者側に残っているなどの条件が満たされる必要があり、確実な実  
277 施を求めていくためには、より社会的な仕組みを用意することが必要となる。なお、ここにおける  
278 検査についても、自主検査や第三者による検査など様々な形態を取り得る。

279

280 3-3-3 第3の観点:機器・システムの運用・管理を行う者の能力に関する確認要求

281 機器・システムの誤使用・誤操作などによって発生するインシデントの影響が、セキュリティ・セ  
282ーフティ対策だけでは許容できる水準ではない場合には、機器・システムの運用・管理を行う者  
283 が当該機器・システムを適切に運用・管理するために必要な能力を持っていることを確認するこ  
284 とを要求することになる。例えば、自動車の場合、運転をする者には一定の技術及び知識を持  
285 つことを証明する運転免許の取得を求めており、インシデントが発生した場合の影響が大きいも  
286 のの、社会的に大きな便益をもたらす技術を社会として受容する社会的な仕組みを構築してい  
287 る。

288

289 3-3-4 第4の観点:その他、社会的なサポート等の仕組みの要求

290 インシデントが発生した場合の影響が非常に大きく、当該仕組み等の所有者が個々に賠償等  
291 の対処を実施することが容易ではないケースの場合には、あらかじめ保険加入を義務付けるな  
292 どの社会的なセーフティネットを満たすことを求めるものである。

293 例えば、自動車の場合、自動車を所有して運転をする者に対して運転免許の取得を求めるこ  
294 とに加え、強制保険である自動車損害賠償責任保険に加入することを義務付けている。これに  
295 より、事故を起こした運転者の資力が十分でない場合であっても、被害を受けた者に最低限の  
296 賠償が行われるように社会的なセーフティネットを構築している。

297

298 各観点はセキュリティ・セーフティ要求に関する内容の考え方の違いに基づいて設定されたもの  
299 であり、同じ観点であっても具体的に要求される個々のセキュリティ・セーフティ対策は一様ではな  
300 い。

301 したがって、仮にセキュリティ・セーフティ要求の観点・内容をコストに換算したとき、第 2 の観点  
302 までのセキュリティ・セーフティ要求しか求められていないカテゴリと、第 4 の観点までの全てのセ  
303 キュリティ・セーフティ要求を求められているカテゴリとコストを比較した場合、前者のコストが必ず  
304 低くなるということではないことに留意する必要がある。各分野において、各観点における具体的  
305 なセキュリティ・セーフティ要求事項を詳細に整理することで、本フレームワークをより精緻なもの  
306 にしていくことが可能である。

307

#### 308 4. 本フレームワークの活用方法

309 サイバー空間とフィジカル空間をつなぐことで生み出される新たな仕組み・サービスは今後様々  
310 な形で創出されていくことが予想される。サービスを実現しようとする主体が本フレームワークを活  
311 用することにより、フィジカル・サイバー間をつなぐ機器・システムに潜むリスクを踏まえて、機器・  
312 システムのカテゴライズを行い、カテゴリ毎に求められるセキュリティ・セーフティ要求の観点を把  
313 握し、カテゴリ間で比較することが可能となる。これにより、別々のプロセスで検討した場合であっ  
314 ても、新たな仕組み・サービスに対応したそれぞれの機器・システムに求めるセキュリティ・セーフ  
315 ティ対策の観点・内容の整合性を一定程度確保していくことが可能となる。

316 その際に注意をしなければならないのは、IoT 機器・システムの用途により、インシデントが発生  
317 した場合の影響の内容や大きさが異なるということである。

318 つまり、本フレームワークは、ある特定の機器に対して一義的にセキュリティ・セーフティ要求の  
319 観点を決定するものではなく、実現される仕組み・サービスの利用者側から見てインシデントが発  
320 生した場合の影響を適切に分析し、第 1 軸と第 2 軸に従ってカテゴリズを行い、そのカテゴリに  
321 従って第 3 軸を活用してセキュリティ・セーフティ要求の観点・内容を適切に検討するための枠組  
322 みとなるものである。

323 本フレームワークを有効に活用していくためには、ユースケースの整理を進めていき、第 1 軸と  
324 第 2 軸によるカテゴリズの手法を洗練させていくとともに、ユースケースの蓄積によって第 3 軸  
325 によるセキュリティ・セーフティ要求の観点・内容を比較できる環境を整備していくことが求められ  
326 る。したがって、今後、本フレームワークに基づいて、具体的な仕組み・サービスをユースケースと

327 して整理していくことで、IoT が広く活用されるサイバー空間とフィジカル空間が高度に融合した社  
328 会におけるセキュリティ・セーフティ対策を適切に実施していく制度的対応の整備を進めていくた  
329 めの基礎的条件を整えて行くこととする。

330

331