

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	1. 本フレームワークの必要性	3
32	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)	3
33	1-1-1 CPSF 概論	3
34	1-1-2 第 2 層の位置づけ	3
35	1-2 本フレームワークの目的	5
36	2. 本フレームワークの想定読者	6
37	3. 本フレームワークの基本構成	7
38	3-1 基本構成の背景にある考え方	7
39	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	7
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	8
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)	9
42	3-2-3 フィジカル・サイバー間をつなげる機器・システムのカテゴリライズ	10
43	3-3 求められるセキュリティ・セーフティ要求の整理	11
44	3-3-1 第 1 の観点:運用前(設計・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	
45	確認要求	12
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	13
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	13
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	13
49	4. 本フレームワークの活用方法	14
50	5. リファレンス	15
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、これらの基点を中心に経済社会全体のセキュ
78 リティ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、例えば前記の転写機能を担うセンサや
84 アクチュエータなどから構成される、いわゆる IoT のシステムによって成立している。IoT のよう
85 なフィジカル空間とサイバー空間をつなぐ機器・システムは、それをを用いるヒトやソシキの企業活
86 動・経済活動に利益をもたらす一方、インシデントが発生した場合には、それをを用いるヒトやソシ

87 キが損失や責任を負うことになる。したがって、IoT 機器・システム¹のセキュリティを確保するこ
88 とが、第 2 層におけるセキュリティ対策の中核となる。なお、本フレームワークにおいて機器だけ
89 でなくシステムも対象としているのは、セキュリティ対策を検討する際には当該機器・システムが
90 利用者に提供する付加価値に着目することが重要であるところ、センサやアクチュエータを搭載
91 する機器単独で付加価値を提供する場合もある一方、当該機器がシステムに組み込まれて初
92 めて付加価値を提供する場合があるためである。

93 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
94 に複数の事例が示されている。

- 95 ・ 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
96 に誤ったデータがサイバー空間へ提供され、データを活用して実施されるオペレーション
97 に対する信頼を喪失
- 98 ・ 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
99 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
100 上の問題が発生
- 101 ・ サイバー攻撃等によって IoT 機器・システムの機能が停止

102 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
103 ても以下のように触れている。

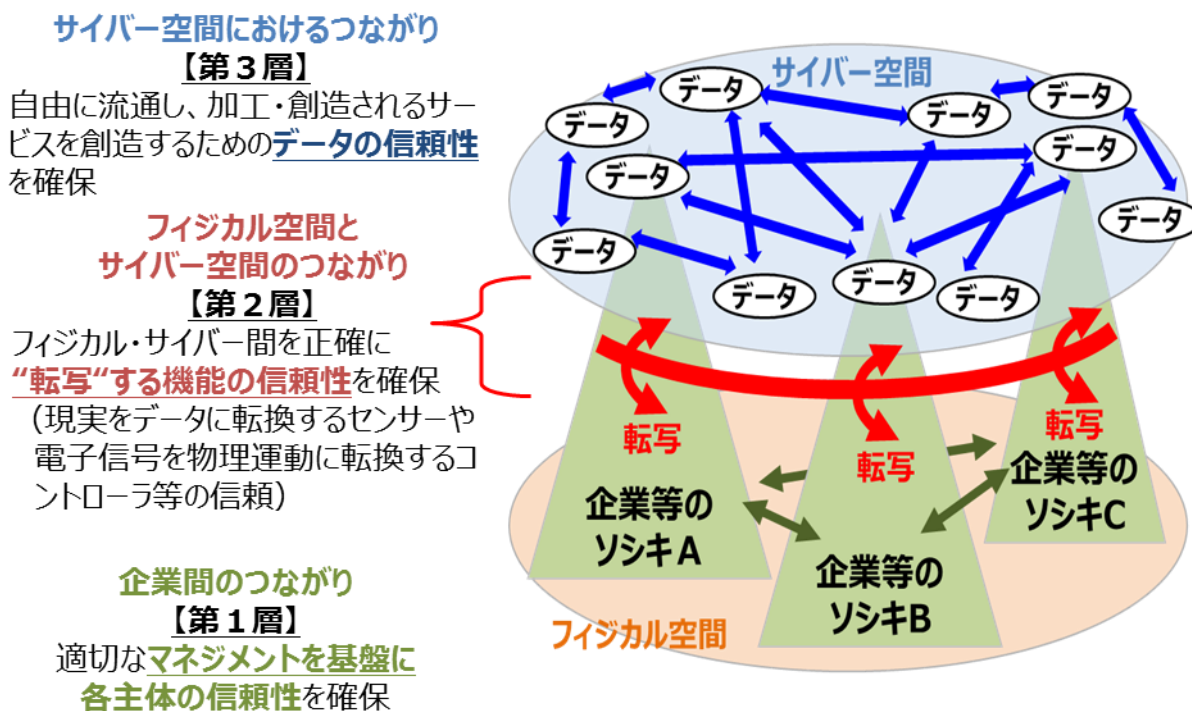
- 104 ・ 組織等において、IoT 機器の担う役割の重要性に応じて、設置区域管理やモニタリングの
105 実施等の多層的な対策の検討が必要。
- 106 ・ 個人によって家庭などに設置される IoT 機器には、組織等による管理が行き届きにくいも
107 のが存在するため、盗難、紛失等のリスクを考慮した対策の実施が必要。

108 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
109 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
110 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
111 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

¹本フレームワークでは、IoT について、ISO/IEC 20924:2018 も参考に、フィジカル空間とサイバー空間からの情
報を処理し、反応するサービスと相互接続されたエンティティ、ヒト、システムおよび情報資源のインフラストラク
チャであると定義し、そのような機能を提供するシステムを IoT システム、そのシステムにおいてセンシング、あ
るいはアクチュエーティングを通じてフィジカル空間と相互作用し、通信するエンティティを IoT 機器であるとし
た。本フレームワークにおいては、IoT を用いて利用者に提供する付加価値に着目することが重要であることか
ら、IoT 機器と IoT システムを区別せず、付加価値を提供する単位を指して「IoT 機器・システム」と表現してい
る。

112 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
113 いる。

114



115

図1 CPSF における 3 層構造モデルと各層における信頼性

116

117 1-2 本フレームワークの目的

118 IoT セキュリティガイドライン²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れ
119 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 機器では、
120 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 の活用の拡
121 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IoT 機
122 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。その過程にお
123 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・セーフティに関して、
124 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/業界において別々
125 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る。そ
126 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コスト
127 が増大する恐れがある。

128

² 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

129 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
130 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
131 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
132 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
133 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
134 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。IoT
135 機器・システムに対する具体的な要求の一律の規定を目的に定めるものではない。

136 なお、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機器・システムの代表例と
137 して IoT、すなわち “Internet of Things” を捉えているが、本フレームワークはサイバー空間とフィ
138 ジカル空間をつなぐ機器・システム全般に言えることである。

139

140 2. 本フレームワークの想定読者

141 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
142 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
143 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
144 イ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、
145 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
146 められることになる。

147 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
148 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
149 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
150 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
151 想定している。

- 152 ・ 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
153 とする者
- 154 ・ 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
- 155 ・ 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
156 者
- 157 ・ そのような新たな仕組み・サービスを受ける者

158

159 3. 本フレームワークの基本構成

160 3-1 基本構成の背景にある考え方

161 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
162 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。
163 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
164 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
165 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。

166 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
167 するのか、ということである。

168 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
169 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
170 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
171 応に係る基本的な考え方を集約した3つの軸を活用し、カテゴリ化するとともに、適切な対策の
172 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。

173

174 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

175 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
176 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
177 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
178 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。

179 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・
180 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
181 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
182 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
183 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。

184 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
185 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、
186 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カテ
187 ゴライズし、マッピングする 2つの軸として設定することとした。

188

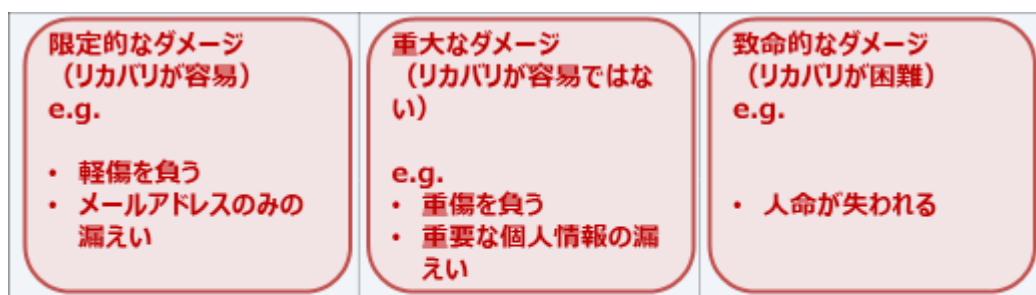
3-2-1 第1軸:発生したインシデントの影響の回復困難性の度合い

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、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。

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、既存の制度体系とも整合性を確保したものである。

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、一度明らかになってしまえば、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軸で捉えられる課題に整理されるものである。

ここで、「リスク」については、インシデントによる影響の度合いと、インシデントの起りやすさを用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・システムの多様性を踏まえたカテゴライズが容易に行えるように、算出が比較的難しい起りやすさは考慮せず、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ライズを行うアプローチを採っている。なお、本フレームワークに基づき、産業界での議論等を踏まえた上で具体的な要求を整理する際には、起りやすさについても考慮することが適切であることに留意されたい。



発生したインシデントの影響の
回復困難性の度合い

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

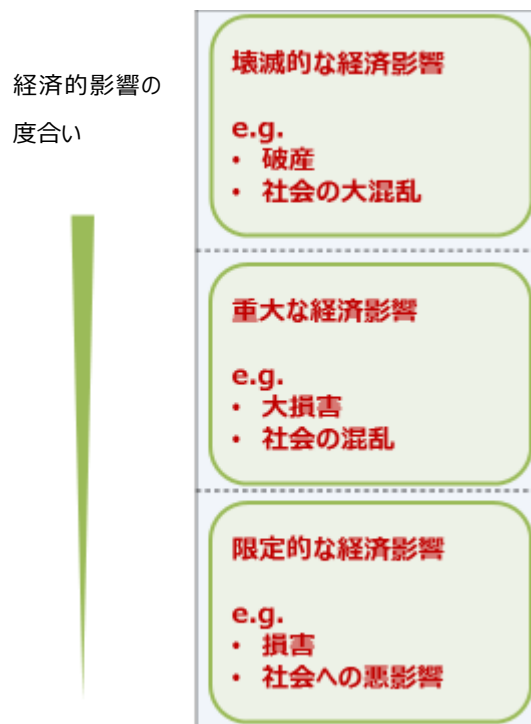
213

214 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)

215 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
216 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。

217 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
218 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
219 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
220 の影響等の事象を第2軸に写像して捉えることとした。

221 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
222 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・システムであつ
223 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。
224 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
225 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
226 る中で相応の水準に該当することになる可能性が高い。



227

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

228

229

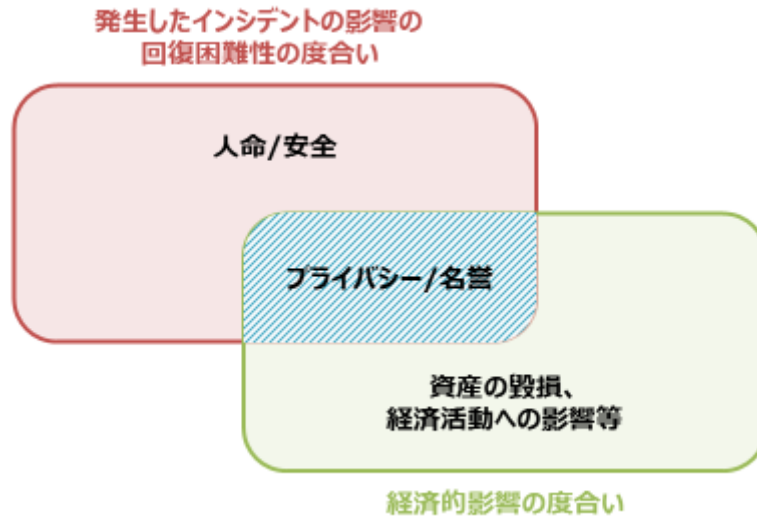


図4 第1軸にも整理されうるプライバシー/名誉の整理

230

231

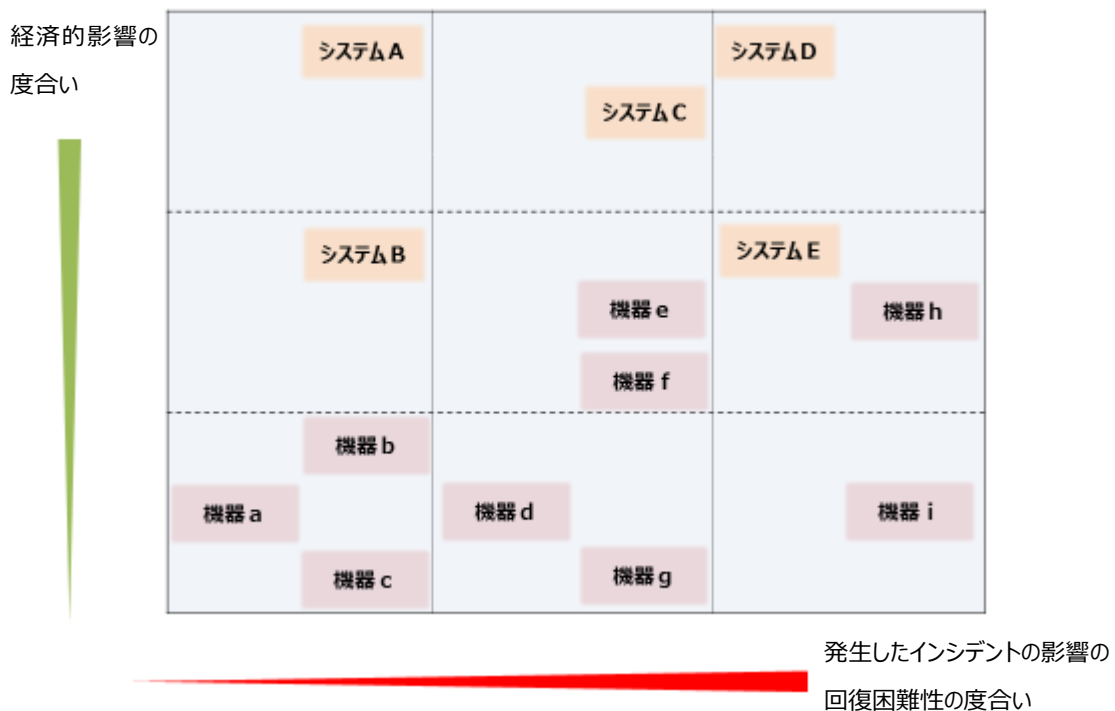
232 3-2-3 フィジカル・サイバー間をつなげる機器・システムの Kategorizatsiya

233 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
234 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。

235 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
236 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、
237 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
238 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 Kategorizatsiya することが可能と
239 なる。

240 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
241 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
242 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
243 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 Kategorizatsiya されるものほどイ
244 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
245 方、左下に Kategorizatsiya 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
246 能となる。詳細は3-3で記載する。

247 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
 248 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
 249 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・システムであったと
 250 しても、どういう環境で使われるか、当該環境においてどういう役割を持つのか、どのようなスキ
 251 ルを持つ者が使うのか等、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
 252 く異なる。そのため、同じ機器・システムでも使用形態などによってマッピング先が異なり得る
 253 ことに留意する必要がある。



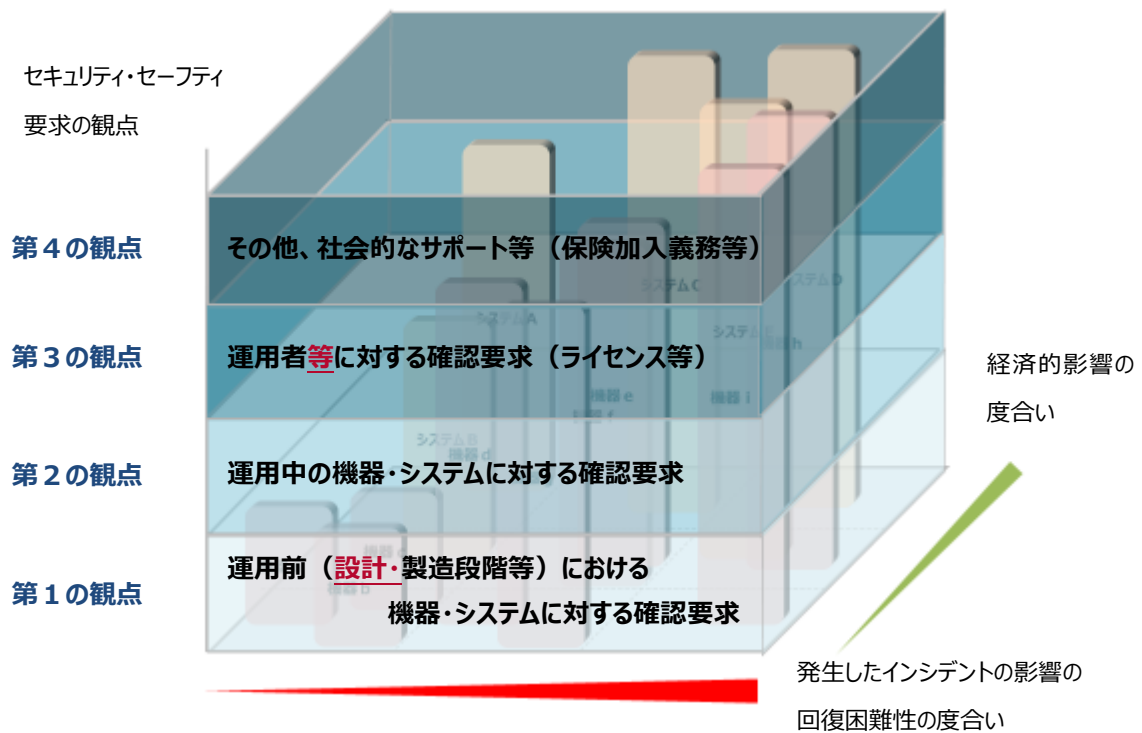
254 図 5 フィジカル・サイバー間をつなげる機器・システムの Kategorize のイメージ
 255 (※ 同じ機器・システムでも使用形態などによってマッピング先が異なり得る。
 256 例えば、機器gと機器hが同じ機器で異なる使用形態である場合などがあり得る。)

257
 258 **3-3 求められるセキュリティ・セーフティ要求の整理**

259 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
 260 について、そのリスクを踏まえて Kategorize することが可能となるが、これだけでは、新たな仕組
 261 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
 262 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
 263 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。

264 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
265 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
266 を示す役割を果たすものである。

267 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
268 る。



269 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

270
271 3-3-1 第1の観点:運用前(設計・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・
272 システムの確認要求

273 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
274 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
275 該機器・システム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
276 力条件等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。

277 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に
278 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
279 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
280 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。

281

282 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

283 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
284 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
285 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
286 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
287 である。

288 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
289 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
290 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
291 施を求めていくためには各ステークホルダーにおいて役割や責任分界点を明確化するなど、よ
292 り社会的な仕組みを用意することが必要となる。なお、ここにおける検査についても、自主検査
293 や第三者による検査など様々な形態を取り得る。

294

295 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

296 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
297 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
298 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
299 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
300 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
301 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
302 る。

303 なお、ここでいう運用者には、サービス提供者のようなシステムを直接操作するわけではない
304 ものも含まれる。

305

306 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

307 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
308 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
309 どの社会的なセーフティネットを講じることを求めるものである。

310 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
311 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
312 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
313 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。

314

315 なお、第3軸における4つの観点は、それぞれが必ずしも完全に独立したものではない。例え
316 ば、使用者による誤使用や誤操作によるインシデントの発生を回避するためには、第3の観点で
317 運用・管理を行う者の能力の確認によって実現するのが適当か、又は第1の観点で販売前に使
318 用者に対して使用方法等の情報を提供することを義務化することが適当か、その機器・システム
319 の特徴を踏まえて検討することが必要である。使用方法等の情報を提供するには、どのように
320 してその情報へのアクセシビリティを向上させるかも検討する必要がある。また、必ずしも全ての
321 観点での要求が求められるものではなく、例えば第2の観点到に係る要求が無くとも、第1や第3
322 の観点到に係る要求により対策を構成することも考え得る。この例のように、複数のステークホルダ
323 ーが関係するリスクへの対処は、複数の観点から行えることから、関係するステークホルダーにお
324 ける負担について、各ステークホルダーが機器・システムのリスクに関連する情報を可視化・共有
325 する等の方法を通じて、総合的に検討し、ステークホルダー間で合意する必要がある。したがっ
326 て、単独のステークホルダーが全ての要求に対処する必要はなく、また、ある観点内であらゆるケ
327 ースで必須に求められる具体的な要求の規定を一律に求めることは困難である。

328 さらに、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
329 れたものであり、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
330 様ではない。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、
331 第2の観点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
332 の全てのセキュリティ・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
333 ストが必ず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。なお、対策の実施はコストに直
334 結することから、求められるセキュリティ・セーフティ要求に対しどのような対策を取るかは、インシ
335 デントの起こりやすさ等も踏まえた上で決定されることが適当である。

336 各分野において、各観点における具体的なセキュリティ・セーフティ要求事項を詳細に整理する
337 ことで、本フレームワークをより精緻なものにしていくことが可能である。

338

339 4. 本フレームワークの活用方法

340 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
341 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
342 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・
343 システムのカテゴリ分けを行い、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

344 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つ
345 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
346 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。

347 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
348 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。

349 つまり、本フレームワークは、ある特定の機器・システムに対して一義的にセキュリティ・セーフ
350 ティ要求の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
351 デントが発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
352 カテゴリに従って第 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
353 めの枠組みとなるものである。

354 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
355 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
356 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
357 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
358 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
359 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
360 めの基礎的条件を整えて行く必要がある。

361

362 5. リファレンス

363 本フレームワークは、サイバー・フィジカル・セキュリティ対策フレームワーク第 I 部、第 II 部で取
364 りまとめた3層構造に基づき、以下の規格等の文書を参照して作成した。

365

366 ・ サイバー・フィジカル・セキュリティ対策フレームワーク(GPSF) Ver1.0

367 経済産業省 商務情報政策局 サイバーセキュリティ課

368 2019 年 4 月

369

370 ・ ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン 第1版

371 産業サイバーセキュリティ研究会 ワーキンググループ 1(制度・技術・標準化) ビルサブワー

372 キンググループ

373 2019 年 6 月

374

375 ・ IoT セキュリティガイドライン Ver1.0

376 IoT 推進コンソーシアム、総務省、経済産業省

- 377 2016 年 7 月
- 378
- 379 ▪ ISO/IEC 20924:2018
- 380 “Information technology – Internet of Things (IoT) – Vocabulary”
- 381 2018 年 12 月
- 382
- 383 ▪ ISO/IEC 27001:2013
- 384 “Information technology – Security techniques – Information security management systems –
- 385 Requirements”
- 386 2013 年 10 月
- 387
- 388 ▪ IEC 61508:2010
- 389 “Functional safety of electrical/electronic/programmable electronic safety-related systems”
- 390 2010 年 4 月
- 391
- 392 ▪ IEC 62443-2-1:2010
- 393 “Industrial communication networks – Network and system security – Part 2-1: Establishing an
- 394 industrial automation and control system security program”
- 395 2010 年 11 月
- 396
- 397 ▪ IEC 62443-3-3:2013
- 398 “Industrial communication networks – Network and system security – Part 3-3: System
- 399 security requirements and security levels”
- 400 2013 年 8 月
- 401
- 402 ▪ ETSI EN 303 645 V2.1.1
- 403 “CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements”
- 404 ETSI
- 405 2020 年 6 月
- 406
- 407 ▪ REGULATION (EU) 2019/881 (Cybersecurity Act)
- 408 欧州議会及び理事会
- 409 2019 年 4 月
- 410
- 411 ▪ SB-327 “Information privacy: connected devices”
- 412 カリフォルニア州
- 413 2018 年 9 月
- 414

- 415 ▪ Cybersecurity Framework Version1.1
416 NIST
417 2018 年 4 月
418
- 419 ▪ NISTIR 8200
420 “Interagency Report on the Status of International Cybersecurity Standardization for the
421 Internet of Things (IoT)”
422 NIST
423 2018 年 11 月
424
- 425 ▪ NISTIR 8228
426 “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks”
427 NIST
428 2019 年 6 月
429
- 430 ▪ NISTIR 8259
431 “Foundational Cybersecurity Activities for IoT Device Manufacturers”
432 NIST
433 2020 年 5 月
434
- 435 ▪ NISTIR 8267 (Draft)
436 “Security Review of Consumer Home Internet of Things (IoT) Products”
437 NIST
438 2019 年 10 月
439
- 440 ▪ NISTIR 8276 (Draft)
441 “Key Practices in Cyber Supply Chain Risk Management: Observations from Industry”
442 NIST
443 2020 年 2 月
444
- 445 ▪ White Paper “Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software
446 Development Framework (SSDF)”
447 NIST
448 2020 年 4 月
449
- 450 ▪ Code of Practice for Consumer IoT Security
451 英国 Department for Digital, Culture, Media & Sport
452 2018 年 10 月

453

454

▪ Internet of Things (IoT) Security Policy Platform Statement

455

Internet Society (ISOC) IoT Security Policy Platform

456

2019 年 11 月

457