CRIC CSF

OTセキュリティ人材スキル定義リファレンスガイド

～NIST SP800-53およびSP800-82を活用したリファレンス～

初版（ver 1.0）

産業横断サイバーセキュリティ人材育成検討会

第二期 OTセキュリティ人材定義WG (WG2)

2019/07/31

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅰ．目次

I.　目次

II.　はじめに

1.　OTセキュリティ人材スキル定義リファレンス
2.　産業横断サイバーセキュリティ人材育成検討会の活動の経緯
3.　公開中の成果物の例

III.「 OT人材定義リファレンス」の考え方

1.　OTセキュリティに関する検証の全体像
2.　OT領域を整理するための3つの事業モデル
3.　共通言語についての検討と方向性
4.　NIST SP800-53および82、並びにIEC62443
5.　ネットワーク構成図（構成イメージ）

IV. 事業モデルに基づく検証

1.　事業モデル毎の主要なパターン
2.　「OT人材定義リファレンス」のパターン組み合わせ
3.　「OT人材定義リファレンス」の留意すべきポイント
4.　セキュリティ・リスクアセスメントの考え方

V.　「OT人材定義リファレンス」の活用法

1.　「OT人材定義リファレンス」の活用
2. Pattern A-1：各役割(Role)の特定・レベル設定
3. Pattern A-2：各役割(Role)の特定・レベル設定
4. Pattern B-1：各役割(Role)の特定・レベル設定
5. Pattern B-2：各役割(Role)の特定・レベル設定
6. Pattern C　：各役割(Role)の特定・レベル設定

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅱ．はじめに

- OTセキュリティ人材スキル定義リファレンス
  - 「OTセキュリティ人材スキル定義リファレンス」（以下「OT人材定義リファレンス」）は、産業横断サイバーセキュリティ人材育成検討会（CRIC CSF）において第二期より検討を進めてきた 「OT領域」 に求められるセキュリティ人材のあり方を「モデル化」する取り組みの一部を公開するものです。
  - 本資料は、会員向け資料を公開用として再編集したものです。

- 対象者
  - 下記の方々にお読み頂くことを想定して作成されています。
    - CISO等
    - セキュリティ部門責任者
    - システム部門責任者
    - 事業部門責任者
    - セキュリティ部門担当者
    - OT領域における様々なIT導入を推進される方
    - その他、事業のリスクマネジメントを検討されている方々

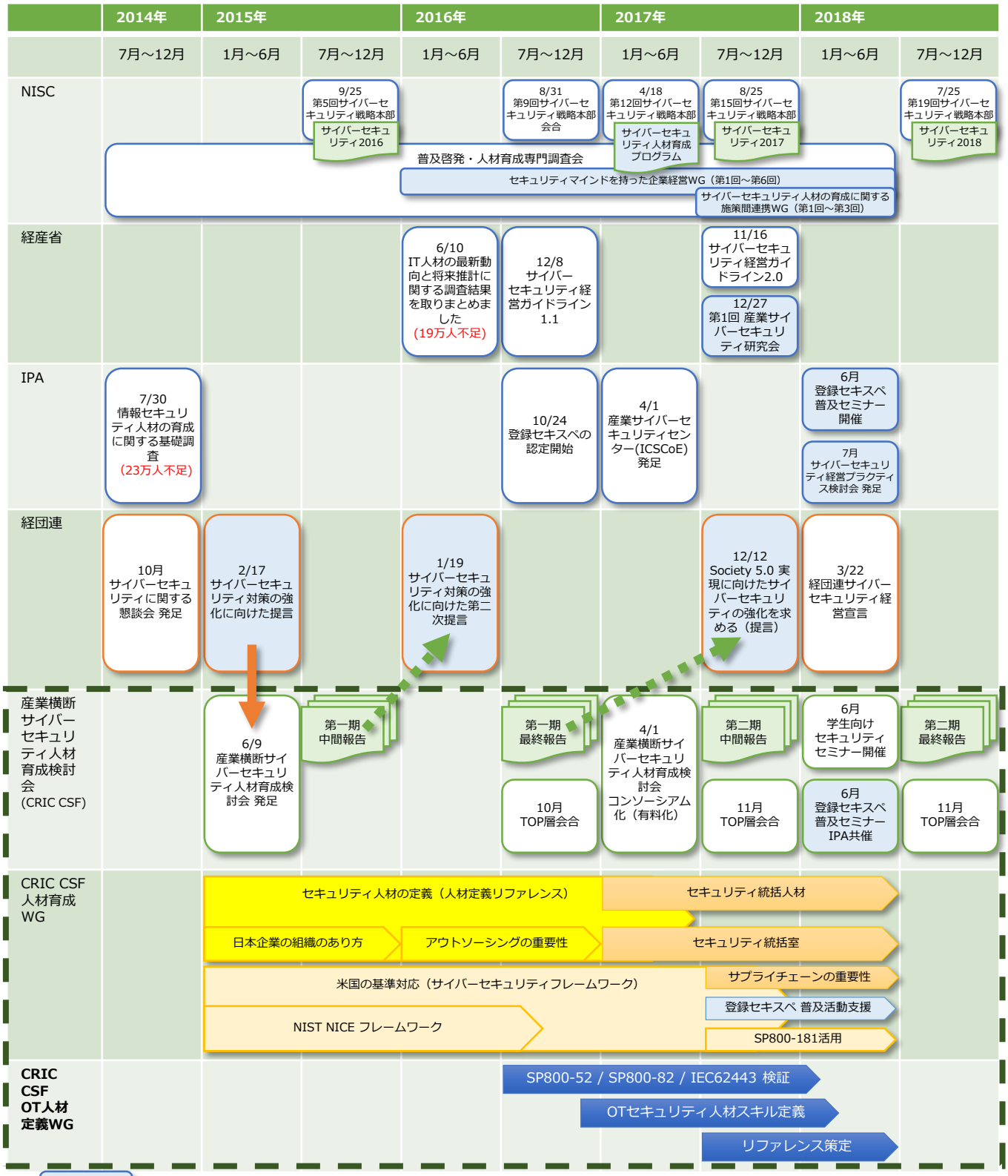
- 著作権
  - 「OTセキュリティ人材スキル定義リファレンス」の著作権は、「一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ人材育成検討会」（CRIC CSF）に帰属します。

- お問合せ先
  - 一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ人材育成検討会 事務局　office@cric-csf.jp

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅱ．はじめに

- 産業横断サイバーセキュリティ人材育成検討会の活動の経緯



：CRIC CSF による活動協力、情報連携、会合参加、並びに資料等の相互参照関係を示す。

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅲ．「OT人材定義リファレンス」の解説

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅲ-1．OTセキュリティに関する検証の全体像

- 議論の経過
  - CRIC CSFでは、重要インフラ事業者を中心としたユーザ企業の団体として、今後必要性が高まる「OT領域」のセキュリティのあり方について議論を重ねてきた。
  - また、ITとOTの違いを様々な角度で整理し「OT領域」におけるセキュリティを向上させるために必要な取り組みとはどのようなものかについて、参加企業各社の実態、最新のトレンド、様々なガイドライン等を踏まえて、幅広い議論を重ねた。
- OT セキュリティ人材
  - ユーザ企業のビジネスを変革し、高度化、効率化を図るためには、事業本体の「ものづくり」を担う制御システムなどのセキュリティ、つまり、「OT セキュリティ」が重要であり、その重要性が増している。
  - 「OT セキュリティ」においては事業の「ものづくり」を最重要と捉え、その仕組みを熟知していることが必要であることとから、一般的な IT セキュリティの導入時の判断とは異なる考えが必要なことから、IT 人材とは異なったモデル、育成が必要と考えられる。
  - 第二期においては、OT セキュリティ人材定義 WG において、ユーザ企業において OT セキュリティを担う人材について検討を行った。
- 「OT人材定義リファレンス」パターン
  - IT システムは、社内情報システムや顧客向けウェブサービスなど、セキュリティの観点から一つの共通モデルを作ることができ、それを支えるセキュリティ人材についても一つの共通モデルを基本として考えることができた。
  - 一方で、ユーザ企業の事業を支える制御システムは、業態や企業規模などによって大きく異なり、本検討会では一つの標準モデルを作ることが難しい、という結論に至った。また、セーフティ (安全計装) に留意する必要があるという点でも IT とは異なる。
  - そこで本検討会では各企業の業態を踏まえ、その業務プロセスを分析し 3つの主要パターン (サービス・インフラの構築・運用/サービス・インフラの利用・製造/サービスの提供) に分類した。さらにサービス・インフラの構築・運用とサービス・インフラの利用・製造を、それぞれ 2つの視点に分けて合計 5つのパターンとした。

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅲ-1．OTセキュリティに関する検証の全体像

- OT人材定義リファレンス
  - このような想定を踏まえ、製造業（BtoC）を想定したモデルを定め、事業のフェーズ毎に何を確認すべきかという点を踏まえて「OT人材定義リファレンス」を策定。
  - また、個別のセキュリティに関する取り組みについては、米国NISTのSP800の中の53および82を参考とし、サイバーセキュリティフレームワーク1.1を活用した各種ガイドラインの読み替えを実施している。
- <u>参考）製造業（BtoC）のモデル化</u>

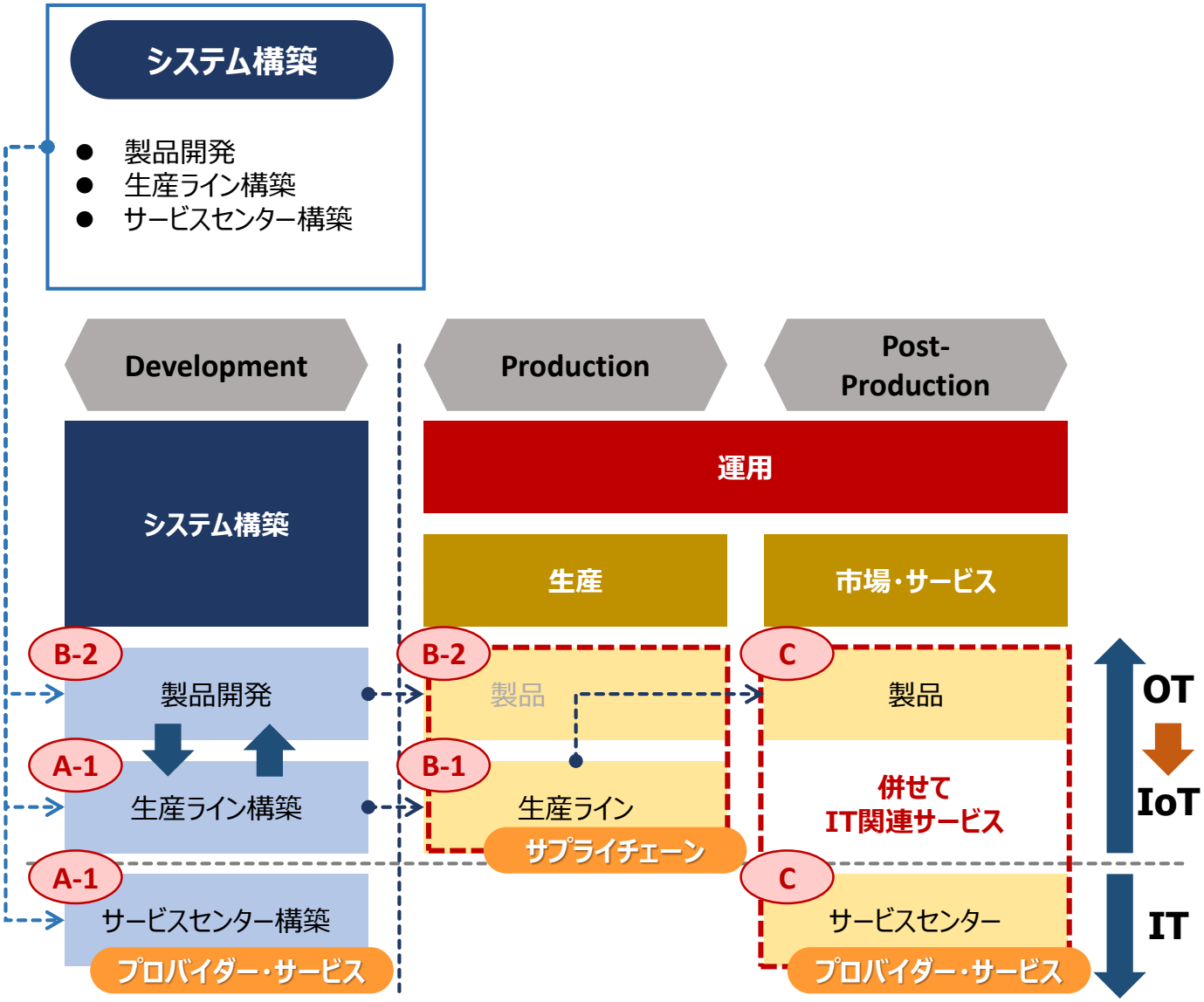


図3-1．製造業（BtoC）のモデル

※ 本モデル図においては、「A-2」 に該当するプロセスが存在せず、記載されておりません。

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅲ-2. OT領域を整理するための3つの事業モデル

- モデル化の議論に基づく事業モデル化
  - 前ページにある「参考）製造業（BtoC）のモデル化」のような議論を重ねることにより、主要パターンの整理（A～C）を行っている。

- OT領域に関する各事業モデルの特徴
  - CRIC CSFの議論においては、事業活動（収益を得るための活動）に直接的に関連するシステムと仮定し、事業活動全体におけるシステムの構成要素を抽出した上で、特に「OT領域」であるとされる部分についての議論を行っている。

  - 尚、事業活動に関連するシステムという表現については、IT技術によるサービス提供等について含まれることも想定しているが、それは、パターンCの一部または、今後の議論のテーマとしている。

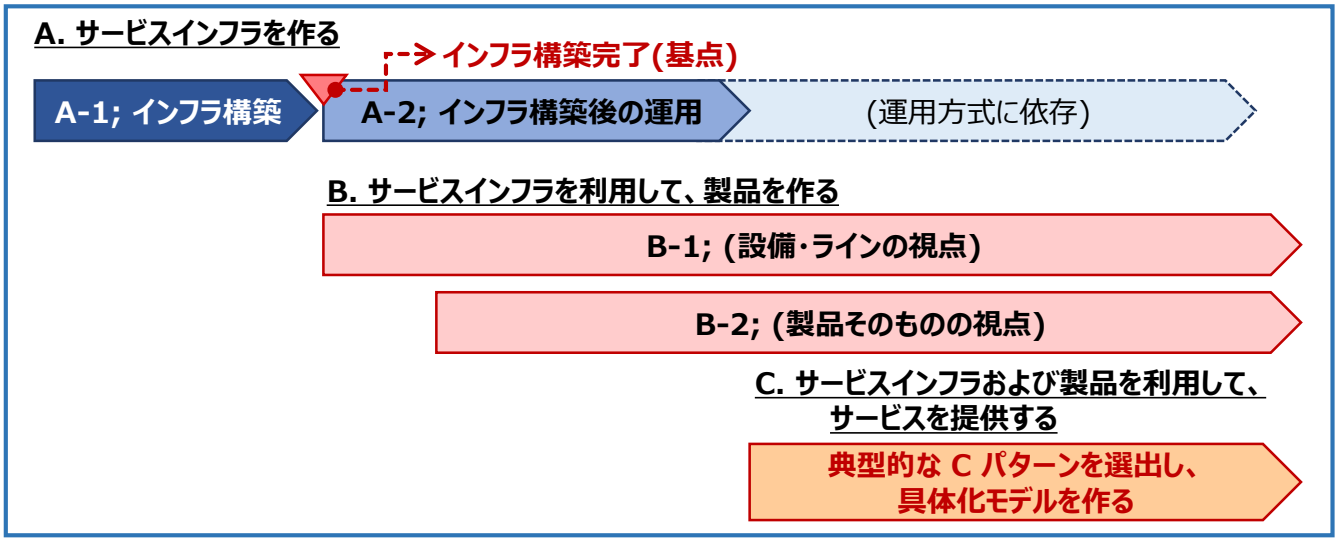


図3-2-1. 主要パターン間の関係性イメージ

- OT領域とは
  - OT領域とは、プロダクション領域であり、製品・サービスを提供するための一連の事業領域に関連する領域を指す。

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅲ-2. OT領域を整理するための3つの事業モデル

- 3つの事業モデル化の後も残る重要な課題
  - OTセキュリティ人材に関するリファレンスを検討していく中で、パターン化と並行して重視しなければならない課題は「用語の取扱い」である。ここでは「用語の統一」ではなく、あくまでも取扱いの重要性に関する課題意識を持つところに留めている。

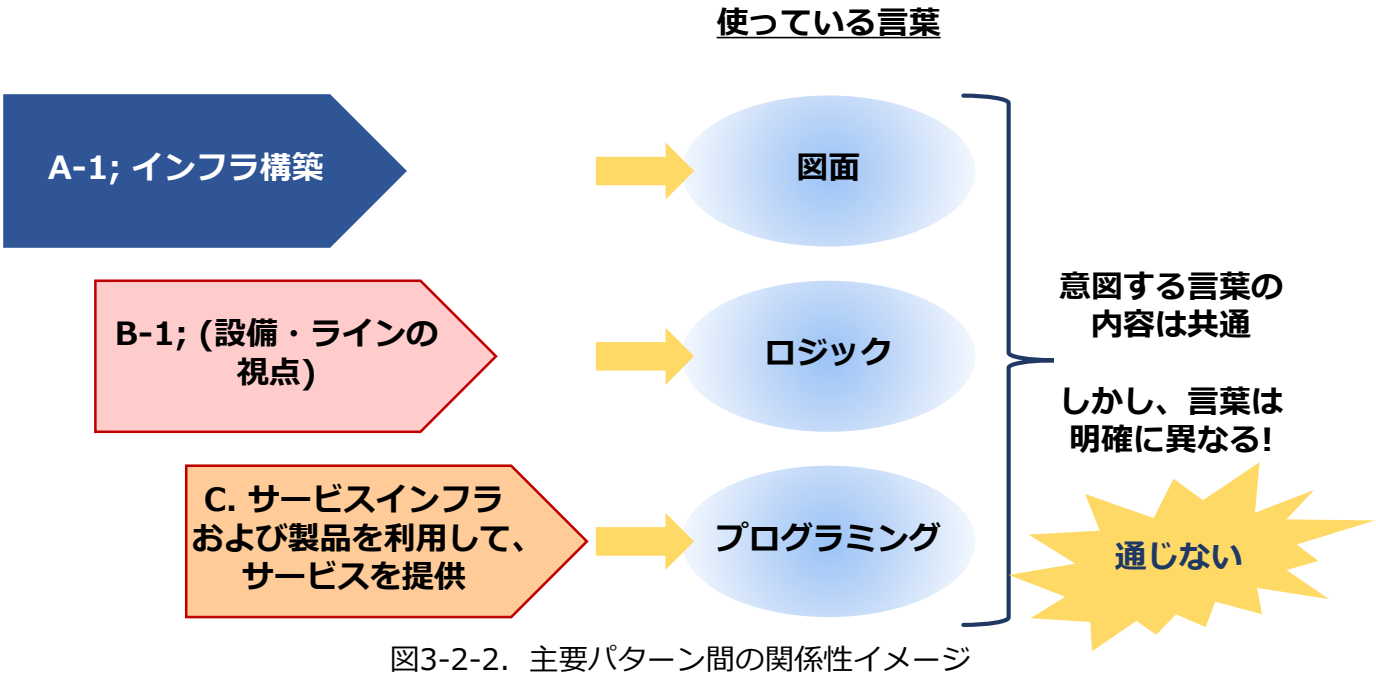


図3-2-2. 主要パターン間の関係性イメージ

- 言葉使いが、各パターン(属する業界)において異なっていることが非常に多い。
- 使っている言葉が、そもそも異なるので、お互いを理解し合うこと自体とても難しい。

IEC 62443 (制御システム)　A, B
NIST SP-800　C
→ **NIST Cyber Security Framework を使って、相互に読み替えていく必要あり。**

- 他のガイドライン等との関係性の整理
  - METI サイバーフィジカルセキュリティフレームワークとの関係性については、現在（2019年5月現在）確認中である。

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅲ-3. 共通言語についての検討と方向性

- OT領域とIT領域をつなぐ「言葉」
  - CRIC CSFでは、OT領域におけるセキュリティのあり方を議論する過程で、事業領域や業種・職種の違いによって、同一のシステムおよびシステム環境等に対して複数の呼び名が存在するなど、セキュリティの取り組みを推進する上で、課題となるものが存在することを確認している。

  - CRIC CSFでは、サイバーセキュリティフレームワーク1.1の参考情報に基づき、SP800-53およびIEC62443それぞれに対応表が存在するため、用語を統合するのではなく、CSFを活用した取り組みの紐づけを実施した。

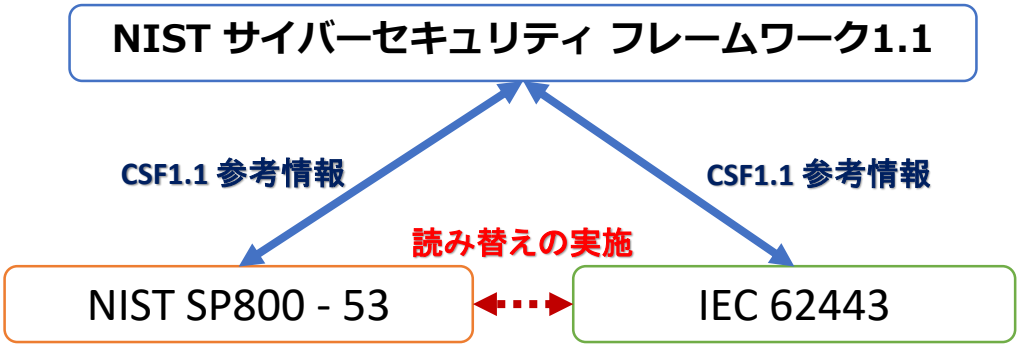


図3-2-3. CSFによる読み替え

- 米国NIST サイバーセキュリティフレームワーク1.1 カテゴリー及び参考情報（例）

カテゴリー	サブカテゴリー	参考情報
	ID.AM-1: 自組織内の物理デバイスとシステムが、目録作成されている。	・ **CIS CSC** 1 ・ **COBIT 5** BAI09.01, BAI09.02 ・ **ISA 62443-2-1:2009** 4.2.3.4 ・ **ISA 62443-3-3:2013** SR 7.8 ・ **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 ・ **NIST SP 800-53 Rev. 4** CM-8, PM-5
	ID.AM-2: 自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。	・ **CIS CSC** 2 ・ **COBIT 5** BAI09.01, BAI09.02, BAI09.05 ・ **ISA 62443-2-1:2009** 4.2.3.4 ・ **ISA 62443-3-3:2013** SR 7.8 ・ **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 ・ **NIST SP 800-53 Rev. 4** CM-8, PM-5
		・ **CIS CSC** 12 ・ **COBIT 5** DSS05.02

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅲ-4. NIST SP800-53および82、並びにIEC62443

- **「OT人材定義リファレンス」**
  - **米国 NIST SP800-53 、82および IEC 62443** に基づき策定されている。
  - 特に、「IT領域」と「OT領域」のバランスをどのように取るべきかの議論を重ね、双方から読み替えて活用できる「モデル」のあり方を整理し、公開することとした。
- **NIST SP800-53**
  - **『連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策』**
    - 連邦政府の情報システムにとって必要なセキュリティおよびプライバシーに対する施策の要件がまとめられたもの
- **NIST SP800-82**
  - **『産業用制御システム(ICS)セキュリティガイドSCADA、DCS、PLC、その他の制御システムの設定』**
    - 産業制御システムの典型的なシステム形態、脅威と脆弱性及び回避策等がまとめられたもの。
- **IEC（ISA）62443**
  - 本規格は4つに区分され、管理から技術までを網羅。
  - 制御システム運用者、システム・インテグレータ、製品ベンダが実現すべきセキュリティ要件を規定している。
- **OT人材定義リファレンスにおける Excel資料ではSP800-53rev5（Draft）**の項目分類を先取りして使用した。

組織・機能		
Management(M) / Technology(T)		
計画	**PL**	計画作成
	RA	リスク評価
	CP	緊急時対応計画
設計・構築	**IA**	識別および認証
	AC	アクセス制御
	CM	構成管理
	MP	メディアの保護
	PE	物理的および環境的な保護
	PM	プログラム管理
	SA	システムおよびサービスの調達
	SC	システムと通信の保護
	SI	システムおよび情報の完全性
	PS	人的セキュリティ
	CA	セキュリティ評価および運用認可
	IP	個人参加の原則
	PA	プライバシーの承認
	AU	監査および責任追跡性
事後	**IR**	インシデント対応
	MA	保守
	AT	意識向上およびトレーニング

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅲ-5. ネットワーク構成図（構成イメージ）

- OT人材定義リファレンスにおいて想定するネットワーク構成図
  - CRIC CSFにおける議論では、様々なOT環境におけるネットワーク構成が確認されたが、本リファレンスにおける議論を行うために標準モデル（理想形）を活用した。

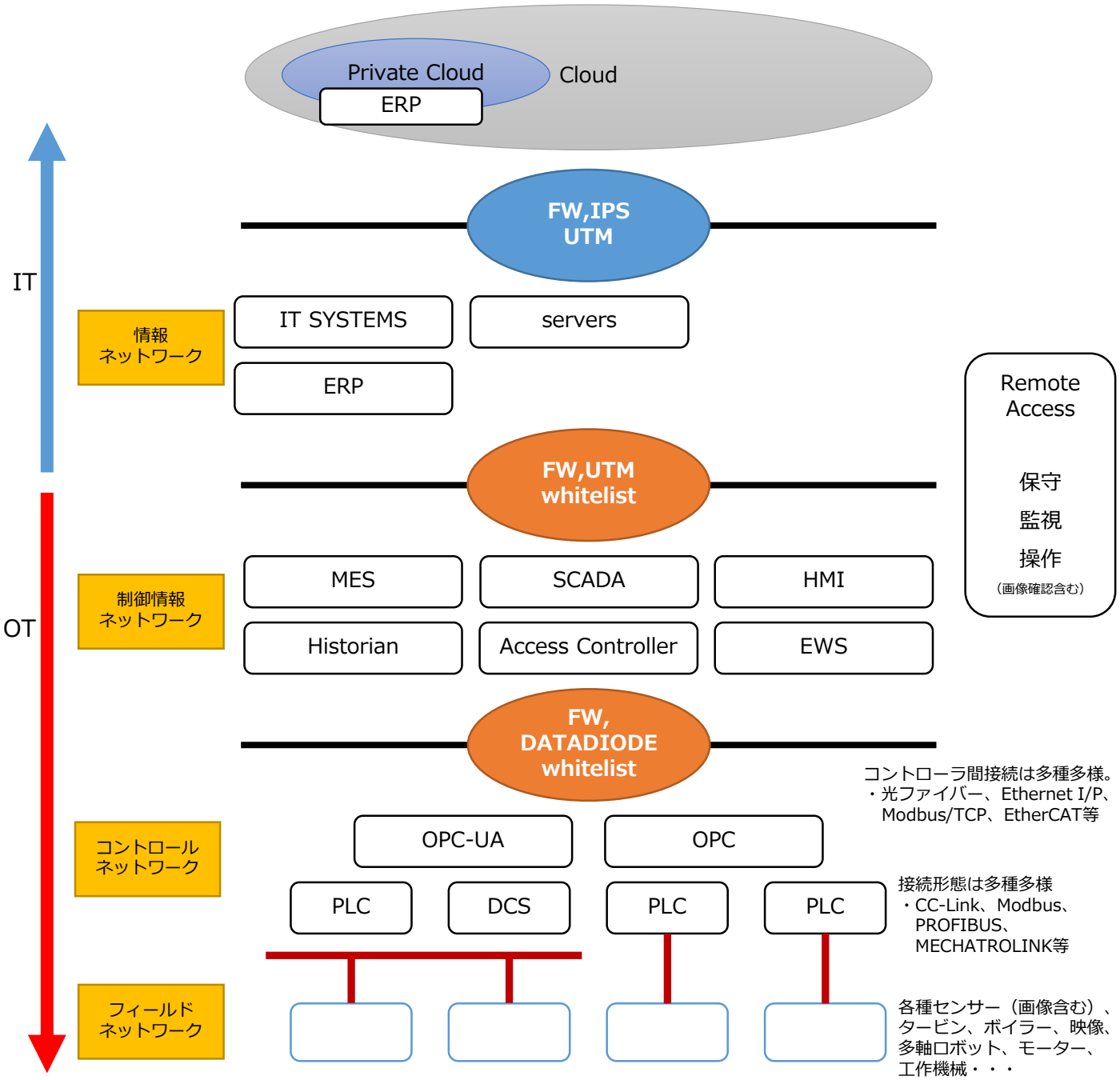


図3-5. OT領域のネットワーク構成イメージ

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅳ．事業モデルに基づく検証

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅳ-1. 事業モデル毎の主要なパターン

事業モデル毎(インフラ構築、製品製造、サービス提供)の主要なパターン

- 自組織の事業分野、または対象となる製品やサービスの分野を以下のA～Cに分類し定義し、各社の事業やサービスはA-Cのパターン、およびA-Cの組み合わせで構成されていると分類・整理した。

- **A: サービスインフラを作る**
  - 「**インフラ構築時**」 を基点に、時間軸で「**構築までの期間**」と「**構築後の運用期間**」に分ける。
  - **A-1**: (～構築)　サービスインフラの構築までを指す。「インフラ構築側」 の視点で定義・設定。
  - **A-2**: (構築後～運用)　但し、「インフラ構築側」 の視点で、役割を定義、レベルを設定。

- **B: サービスインフラを利用して、製品を作る**
  - ものづくりの観点で、「**設備・ラインを運営する視点**」と「**製品そのものを作る視点**」に分ける。
  - **B-1**: (設備・ラインの視点)　「インフラ活用側」 の視点で、役割を定義、レベルを設定。
  - **B-2**: (製品そのものの視点)　「製品そのもの」 を見る視点で、上記同様に定義・設定。

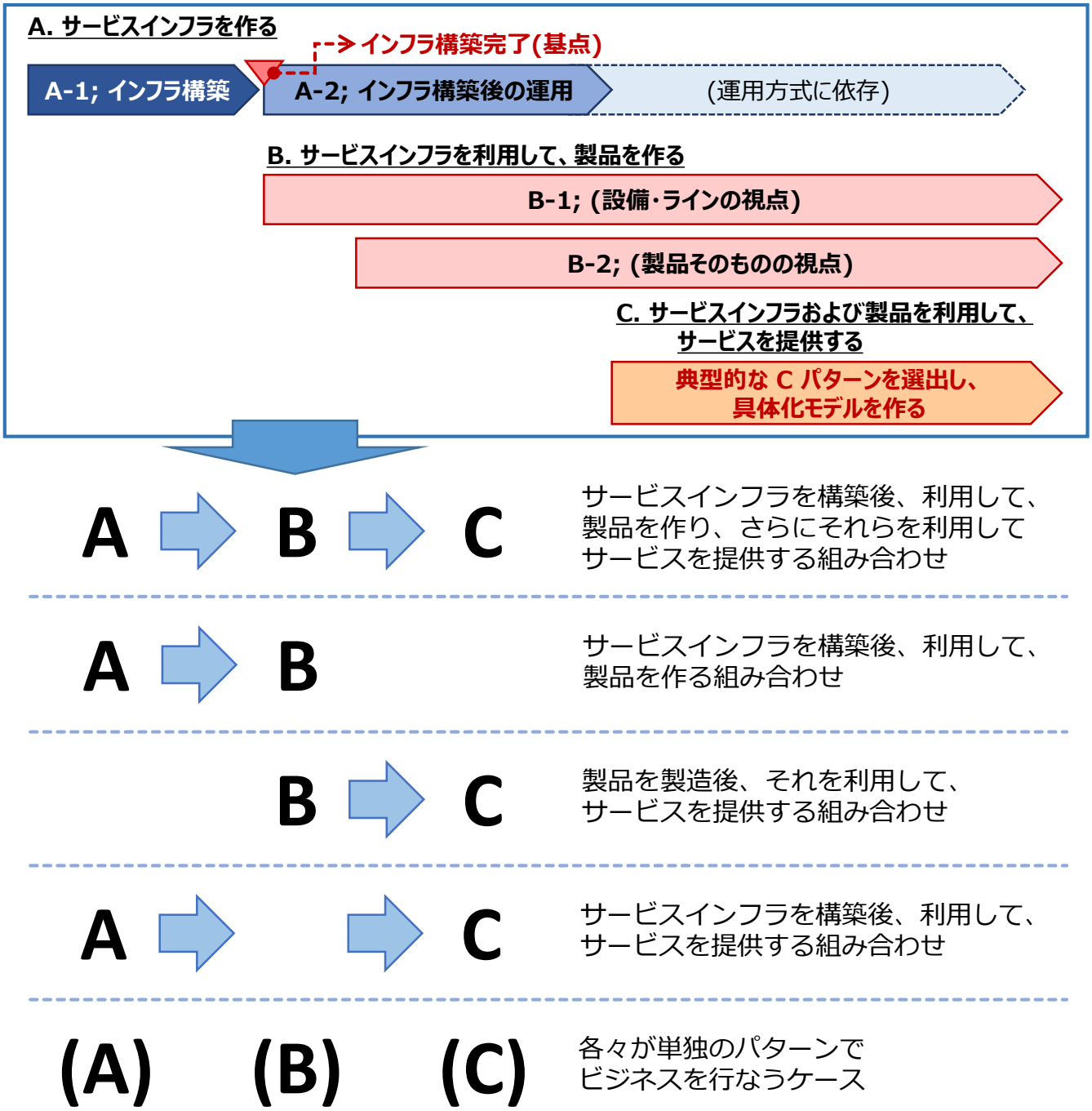
- **C: サービスインフラおよび製品を利用して、サービスを提供する**
  - サービス形態が多様化しているので、イメージしやすい業態やビジネスモデルを選んで、ケースを具体化することが重要。
  - 場合によっては、サービスパターンが幾つかに分類できるかもしれないが、現状では「サービス提供型」として、一つのケースで説明できるリファレンスを目指している。

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅳ-2.　「OT人材定義リファレンス」のパターン組み合わせ

「OT人材定義リファレンス」のパターンによる組み合わせ

- 業種・業態によって、該当するパターンの組み合わせは多様化し、異なるものと想定し、個社別の事情については、各社のカスタマイズにより対応するものと定めた。



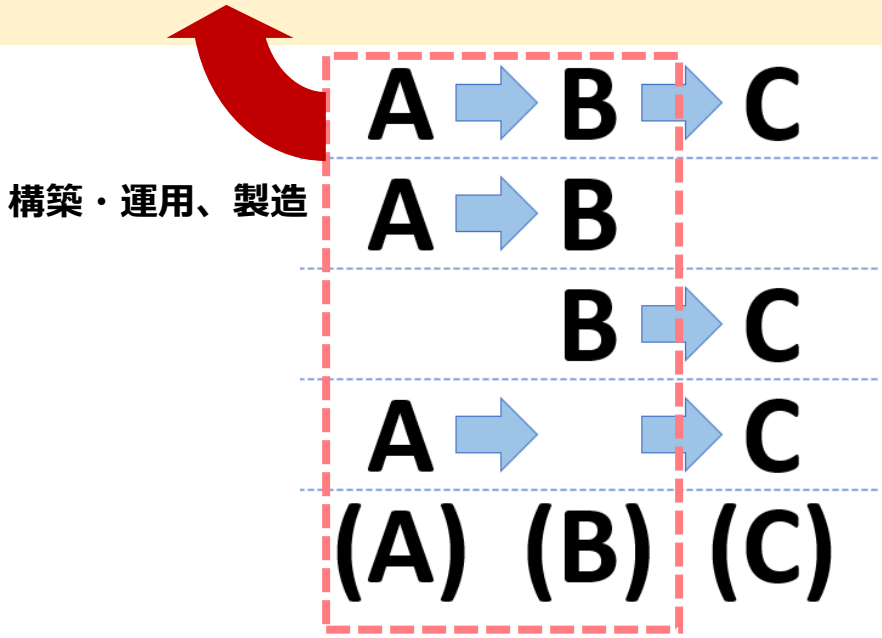
copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅳ-3.　「OT人材定義リファレンス」の留意すべきポイント

「OT人材定義リファレンス」のパターンで留意すべきポイント

- サービスインフラの構築やその運用、そしてインフラを活用した製品製造においては**「セーフティ（安全計装）」**の視点が重要である。

- **安全計装との関係性**
  - ✓ 通常のインシデント（故障）だけを想定するのではなく、セキュリティ・インシデント（サイバー攻撃等）の視点を持ち合わせていることも重要。
- **構築・運用ベンダー教育プログラムへの反映**
  - ✓ 各社各業態の業務プロセスを熟知していないベンダーに対して、その業務プロセスを理解させ、並行して技術的なスキル（セキュリティを含む）を向上させる教育プログラムを組み上げていくことが重要。
- **「設備管理者向け」と「オペレーター向け」の棲み分け、及び両方の共通要素の導出**
  - ✓ 現場に寄れば寄るほど、プロセスに合致した具体的かつ理解されやすい役割の提示が期待される。但し、詳細化される粒度が小さくなりがちなので、両方の要素を取り込んだ上で棲み分けを図りたい。



copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅳ-4. セキュリティ・リスクアセスメントの考え方

- セキュリティ・リスクアセスメント
  - CRIC CSF OTセキュリティ人材定義WG（WG2）では**「セキュリティ・リスクアセスメント」**の考え方として以下の2点を共有している。

■ **ビジネス・リスクアセスメント：**

- ビジネス上で本来、管理・ケアしなければいけないリスクアセスメント

■ **システム・リスクアセスメント（詳細リスクアセスメント）：**

- 各業種・業態のビジネスモデルに基づいて、詳細に管理しなければいけないリスクアセスメント
- 今回の活動で生み出される、リファレンスシートを活用して、Management View (管理視点)・Technology View (技術視点) の両面からアセスメントを実施する。

※ 尚、リスクアセスメントを実施する前に行われる「ビジネスインパクト分析（BIA）」は業種・業界および事業内容により異なるため、今後の検討テーマの1つとし、アセスメントの考え方のみ記している。

- アセスメント実施の際の留意点
  - 「OT人材定義リファレンス」をアセスメント業務に活用する場合、Supply Chain ヒエラルキーが何次にも折り重なる企業集団・ビジネスモデル集団に対して活用することを想定すると、Tier-n企業に該当する各企業向けに「具体的な事例」を用意することが重要。
  - 階層が深いヒエラルキーに位置する企業ほど、具体的な事例を提示しながら対応プロセスを共有していく必要がある。

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ｖ．「OT人材定義リファレンス」の活用法

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅴ-1.　「OT人材定義リファレンス」の活用

- CRIC CSFでは各リファレンス・パターンに対し事業における「経営層」「企画」「設計」といった役割について、NIST SP800-53に準拠した必要なスキルを**技術面**と**管理面**とでレベルを提示した 「**OT人材定義リファレンス**」を策定した。

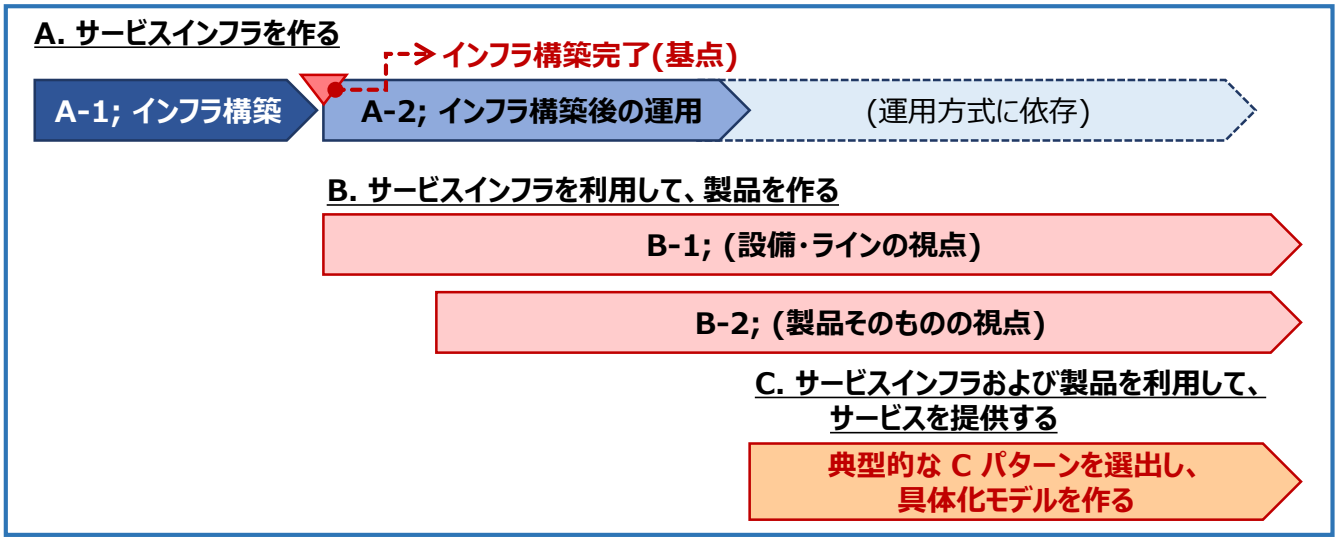


図3-2-2.　主要パターン間の関係性イメージ

- 【凡例】「OT人材定義リファレンス」の読み方
  - 「OT 人材定義リファレンス」ではリファレンス・パターンに対し関わる役割について、それぞれ必要なレベルを実施主体としての主担当は◎、実施主体としての副担当または兼務は○、実施対象者側の関係者・関係部署のレベルは△として定義した。
  - また、★は (理想的には) 経営層からの強い指示・承認を存在することを示し、☆は経営層からの指示・承認が伴うことを示している。
  - 赤くハッチングされている個所は、主たる運営主体者・運営責任者であることを示す。

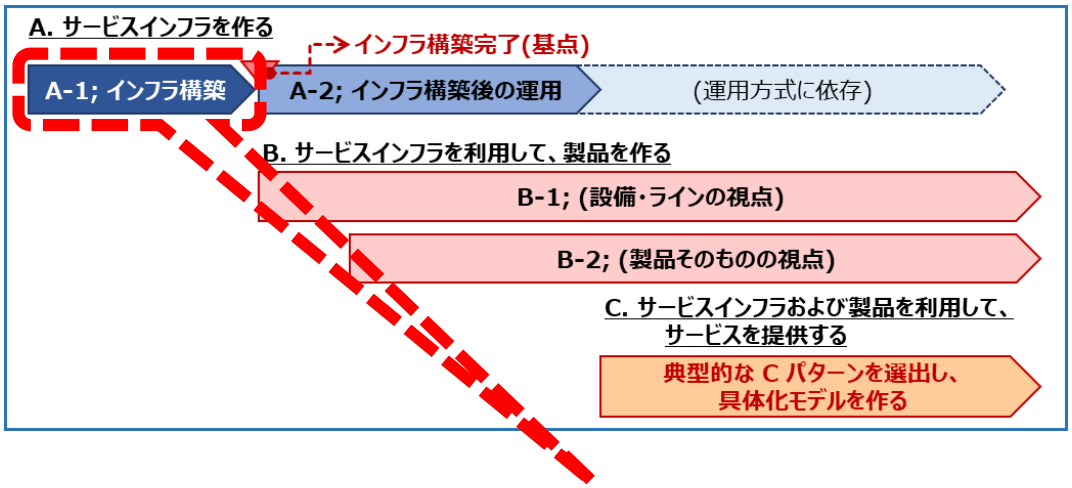
copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

V-2. Pattern A-1：各役割(Role)の特定・レベル設定

OT人材定義リファレンス：Pattern A：各役割(Role)の特定・レベル設定

・[A-1] サービスインフラを作る

1. サービスインフラを構築完了するまでを 「**A-1**」 の役割とし、特定・レベル設定を行なう。



組織・機能			経営層		企画		指示 設計		調達(購買)		工作(構築)	
Management(M) / Technology(T)			M	T	M	T	M	T	M	T	M	T
計画	PL	計画作成	★		◎							
	RA	リスク評価	★				◎				◎	
	CP	緊急時対応計画	★				◎	◎			○	○
設計・構築	IA	識別および認証					◎	◎			◎	○
	AC	アクセス制御					◎	◎			◎	○
	CM	構成管理					◎	◎			◎	◎
	MP	メディアの保護					◎	◎			◎	○
	PE	物理的および環境的な保護			△		◎	◎			◎	○
	PM	プログラム管理					◎	◎			◎	○
	SA	システムおよびサービスの調達					◎	◎	○			
	SC	システムと通信の保護					◎	◎			◎	○
	SI	システムおよび情報の完全性					◎	◎			◎	○
	PS	人的セキュリティ			△		△				△	
	CA	セキュリティ評価および運用認可	★				○	○			△	△
	IP	個人参加の原則	★				△	△			△	△
	PA	プライバシーの承認	★		△		○	○			○	○
	AU	監査および責任追跡性	☆				△	△			△	△
事後	IR	インシデント対応	★				◎	◎			◎	◎
	MA	保守										
	AT	意識向上およびトレーニング	★		△		△	○	△		△	○

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

V-2. Pattern A-1：各役割(Role)の特定・レベル設定

OT人材定義リファレンス：Pattern A：各役割(Role)の特定・レベル設定

■簡単な定義①：

◎（実施主体としての）主担当

○（実施主体としての）副担当、または兼務

△（実施対象者側の）関係者・関係部署

■簡単な定義②：

★ (理想的には) 経営層からの強い指示・承認が存在すること

☆ 経営層からの指示・承認が伴うこと

主たる運営主体者・運営責任者

構築管理/品質管理		IT部門		セキュリティ監査部門		運用		保守		監視モニタリング		PSIRT		人事、総務		法務、広報	
M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T
		◎															
○		○	○	○													
		○	○											△		○	
		○	◎														
		○	◎														
		○	○														
		○	○														
		○	○														
		○	○														
														◎			
		○	○	◎	◎											○	
														◎			
		○	○											◎			
		○	○	◎	◎												
		○	○											△		○	
△		○	◎	△										◎		△	

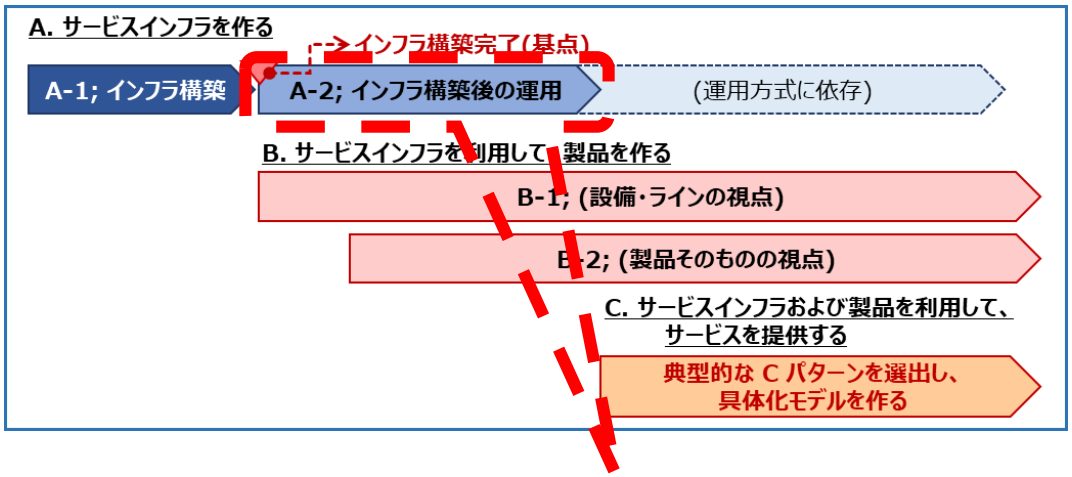
copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

V-3. Pattern A-2：各役割(Role)の特定・レベル設定

OT人材定義リファレンス：Pattern A：各役割(Role)の特定・レベル設定

・[A-2] サービスインフラを作る

1. サービスインフラの構築後から運用までを 「**A-2**」 の役割とし、特定・レベル設定を行なう。



組織			経営層		製造企画/製造開発		設計		調達(購買)		工作/運用	
Management(M) / Technology(T)			M	T	M	T	M	T	M	T	M	T
計画	PL	計画作成	★		◎							
計画	RA	リスク評価	★				◎	◎			◎	○
計画	CP	緊急時対応計画	★				◎	◎			○	○
設計・構築	IA	識別および認証					◎	◎			◎	○
設計・構築	AC	アクセス制御					◎	◎			◎	○
設計・構築	CM	構成管理					○	○			○	○
設計・構築	MP	メディアの保護						○	△	△	△	△
設計・構築	PE	物理的および環境的な保護			△			○				○
設計・構築	PM	プログラム管理					◎	◎			◎	○
設計・構築	SA	システムおよびサービスの調達							◎			○
設計・構築	SC	システムと通信の保護					○	○	○			○
設計・構築	SI	システムおよび情報の完全性					○	○			○	○
設計・構築	PS	人的セキュリティ			△		△				△	
設計・構築	CA	セキュリティ評価および運用認可	★				○	○			△	△
設計・構築	IP	個人参加の原則	★				△	△			△	△
設計・構築	PA	プライバシーの承認	★		△		○	○			○	○
設計・構築	AU	監査および責任追跡性	☆				△	△			△	△
事後	IR	インシデント対応	★				○	○			○	○
事後	MA	保守						△				△
事後	AT	意識向上およびトレーニング	★		△		△	○	△		△	○

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

V-3. Pattern A-2：各役割(Role)の特定・レベル設定

OT人材定義リファレンス：Pattern A：各役割(Role)の特定・レベル設定

■簡単な定義①：

◎（実施主体としての）主担当

○（実施主体としての）副担当、または兼務

△（実施対象者側の）関係者・関係部署

■簡単な定義②：

★ (理想的には) 経営層からの強い指示・承認が存在すること

☆ 経営層からの指示・承認が伴うこと

主たる運営主体者・運営責任者

品質管理		IT部門		セキュリティ監査部門		運用		保守		監視モニタリング		PSIRT		人事、総務		法務、広報	
M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T
		◎															
○		○	○	○													
		○	○			△	△	△						△		○	
		○	◎														
		○	◎														
		○	○			◎	◎										
		○	○			◎	◎	○	○								
						◎	◎	○	○								
						○	○	○	○								
						○	◎	○	○								
		○	○			◎	◎										
		○	○			◎	◎	○	○								
						○		△						◎			
		○	○	◎	◎		○		△							○	
						○		△						◎			
		○	○			○		△						◎			
		○	○	◎	◎												
		○	○			◎	◎	○	○					△		○	
		○	○			○	○	◎	◎								
△		○	◎	△										◎		△	

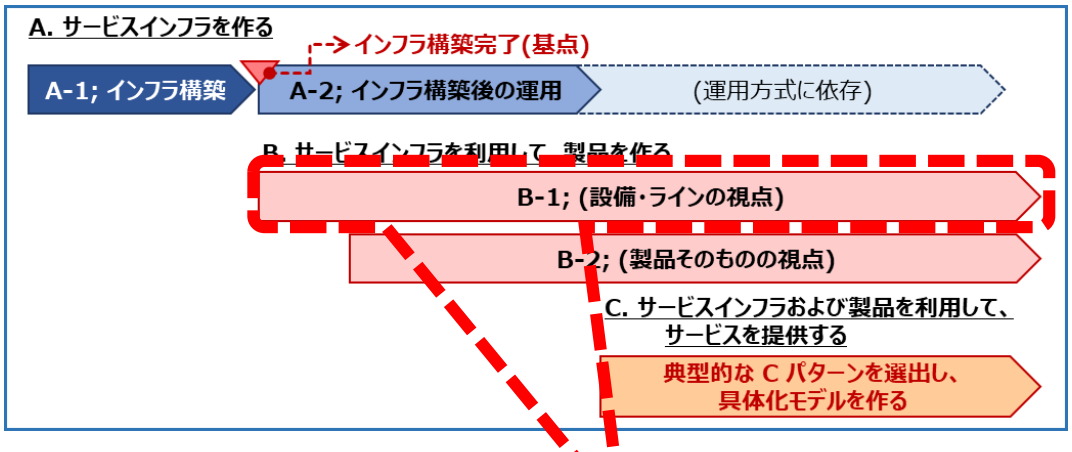
copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

V-4. Pattern B-1：各役割(Role)の特定・レベル設定

OT人材定義リファレンス：Pattern B：各役割(Role)の特定・レベル設定

・[B-1] サービスインフラを利用して製品を作る

1. 設備・ラインの視点（インフラ活用側の視点）を「**B-1**」とし、役割を定義、レベルを設定する。



組織			経営層		製品企画/製品開発		指示 設計		調達(購買)		工作/運用	
Management(M) / Technology(T)			M	T	M	T	M	T	M	T	M	T
計画	PL	計画作成	★		◎							
	RA	リスク評価	★				◎	◎			◎	○
	CP	緊急時対応計画	★				◎	◎			○	○
設計・構築	IA	識別および認証					◎	◎			◎	○
	AC	アクセス制御					◎	◎			◎	○
	CM	構成管理					○	○			○	○
	MP	メディアの保護						○	△	△	△	△
	PE	物理的および環境的な保護			△			○				○
	PM	プログラム管理					◎	◎			◎	○
	SA	システムおよびサービスの調達							◎			○
	SC	システムと通信の保護					○	○	○			○
	SI	システムおよび情報の完全性					○	○			○	○
	PS	人的セキュリティ			△		△				△	
	CA	セキュリティ評価および運用認可	★				○	○			△	△
	IP	個人参加の原則	★				△	△			△	△
	PA	プライバシーの承認	★		△		○	○			○	○
	AU	監査および責任追跡性	☆				△	△			△	△
事後	IR	インシデント対応	★				○	○			○	○
	MA	保守						△				△
	AT	意識向上およびトレーニング	★		△		△	○	△		△	○

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅴ-4. Pattern B-1：各役割(Role)の特定・レベル設定

OT人材定義リファレンス：Pattern B：各役割(Role)の特定・レベル設定

■簡単な定義①：

◎（実施主体としての）主担当

○（実施主体としての）副担当、または兼務

△（実施対象者側の）関係者・関係部署

■簡単な定義②：

★ (理想的には) 経営層からの強い指示・承認が存在すること

☆ 経営層からの指示・承認が伴うこと

主たる運営主体者・運営責任者

品質管理		IT部門		セキュリティ監査部門		運用		保守		監視モニタリング		PSIRT		人事、総務		法務、広報	
M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T
		◎															
		○	○	○													
		○	○			△	△	△						△		○	
		○	◎														
		○	◎														
		○	○			◎	◎										
		○	○			◎	◎	○	○								
						◎	◎	○	○								
						○	○	○	○								
						○	◎	○	○								
		○	○			◎	◎										
		○	○			◎	◎	○	○								
						○		△						◎			
		○	○	◎	◎		○		△							○	
						○		△						◎			
		○	○			○		△						◎			
		○	○	◎	◎												
		○	○			◎	◎	○	○					△		○	
		○	○			○	○	◎	◎								
		○	◎	△										◎		△	

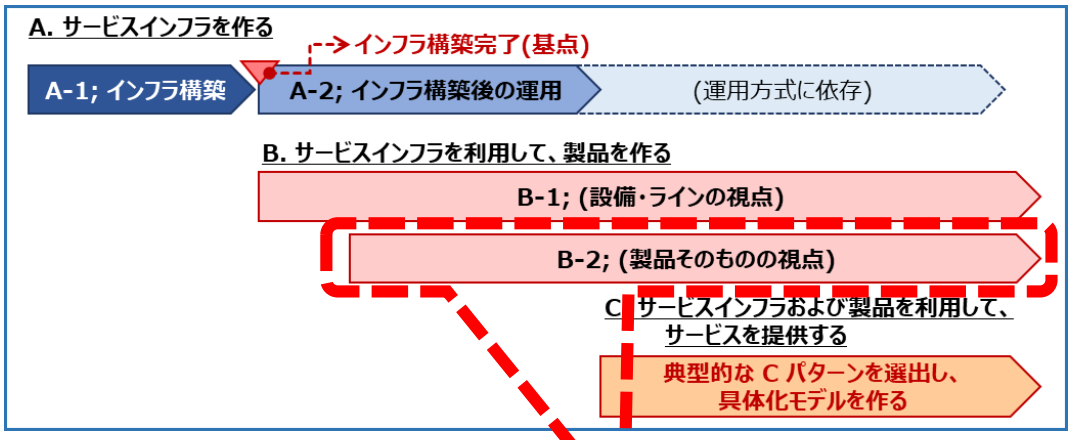
copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

V-5. Pattern B-2：各役割(Role)の特定・レベル設定

OT人材定義リファレンス：Pattern B：各役割(Role)の特定・レベル設定

・[B-2] サービスインフラを利用して製品を作る

1. 製品そのものを見る視点を「**B-2**」とし、役割を定義、レベルを設定する。



組織			経営層		製品企画/製品開発		指示 製品設計		調達(購買)		工作(構築)	
Management(M) / Technology(T)			M	T	M	T	M	T	M	T	M	T
計画	PL	計画作成	★		◎							
	RA	リスク評価	★				◎	◎				
	CP	緊急時対応計画	★				◎	◎				
設計・構築	IA	識別および認証					◎	◎				
	AC	アクセス制御					◎	◎				
	CM	構成管理					○	○				
	MP	メディアの保護						○	△	△		
	PE	物理的および環境的な保護			△			○				
	PM	プログラム管理					◎	◎				
	SA	システムおよびサービスの調達							◎			
	SC	システムと通信の保護					○	○	○			
	SI	システムおよび情報の完全性					○	○				
	PS	人的セキュリティ			△		△					
	CA	セキュリティ評価および運用認可	★				○	○				
	IP	個人参加の原則	★				△	△				
	PA	プライバシーの承認	★		△		○	○				
	AU	監査および責任追跡性	☆				△	△				
事後	IR	インシデント対応	★				○	○				
	MA	保守						△				
	AT	意識向上およびトレーニング	★		△		△	○	△			

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

V-5. Pattern B-2：各役割(Role)の特定・レベル設定

OT人材定義リファレンス：Pattern B：各役割(Role)の特定・レベル設定

■簡単な定義①：

◎（実施主体としての）主担当

○（実施主体としての）副担当、または兼務

△（実施対象者側の）関係者・関係部署

■簡単な定義②：

★ (理想的には) 経営層からの強い指示・承認が存在すること

☆ 経営層からの指示・承認が伴うこと

主たる運営主体者・運営責任者

品質管理		IT部門		セキュリティ監査部門		製造・包装(運用)		保守/修理/アフターケア		監視モニタリング		PSIRT		人事、総務		法務、広報	
M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T
		◎															
		○	○	○								△					
		○	○			○	○	△				○	△	△		○	
		○	◎														
		○	◎														
		○	○			◎	◎					○	△				
		○	○			◎	◎	○	○			○	△				
						◎	◎	○	○			○	△				
						○	○	○	○			○	△				
						○	◎	○	○			○	△				
		○	○			◎	◎					○	△				
		○	○			◎	◎	○	○			○	△				
						○		△						◎			
		○	○	◎	◎		○		△			△				○	
						○		△				△		◎			
		○	○			○		△				△		◎			
		○	○	◎	◎							△					
		○	○			◎	◎	○	○					△		○	
		○	○			○	○	◎	◎								
		○	◎	△										◎		△	

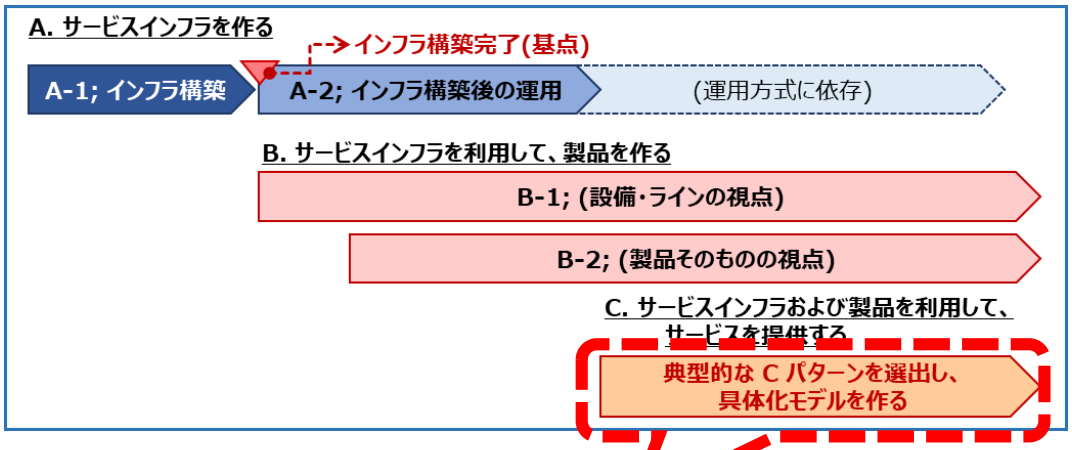
copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

V-6. Pattern C：各役割(Role)の特定・レベル設定

OT人材定義リファレンス：Pattern C：各役割(Role)の特定・レベル設定

・[C] サービスインフラおよび製品を利用してサービスを提供する

1. サービス形態が多様化しているので、イメージしやすい業態やビジネスモデルを選ぶ。
2. その選定されたモデルをより具体化することで、役割を定義、レベルを設定する。



組織			経営層		製品企画/製品開発		指示 設計		調達(購買)		工作(構築)	
Management(M) / Technology(T)			M	T	M	T	M	T	M	T	M	T
計画	PL	計画作成	★		◎							
	RA	リスク評価	★				◎	◎				
	CP	緊急時対応計画	★				◎	◎				
設計・構築	IA	識別および認証					◎	◎				
	AC	アクセス制御					◎	◎				
	CM	構成管理					○	○				
	MP	メディアの保護						○	△	△		
	PE	物理的および環境的な保護			△			○				
	PM	プログラム管理					◎	◎				
	SA	システムおよびサービスの調達							◎			
	SC	システムと通信の保護					○	○	○			
	SI	システムおよび情報の完全性					○	○				
	PS	人的セキュリティ			△		△					
	CA	セキュリティ評価および運用認可	★				○	○				
	IP	個人参加の原則	★				△	△				
	PA	プライバシーの承認	★		△		○	○				
	AU	監査および責任追跡性	☆				△	△				
事後	IR	インシデント対応	★				○	○				
	MA	保守						△				
	AT	意識向上およびトレーニング	★		△		△	○	△			

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

Ⅴ-6. Pattern C：各役割(Role)の特定・レベル設定

OT人材定義リファレンス：Pattern C：各役割(Role)の特定・レベル設定

■簡単な定義①：

◎（実施主体としての）主担当

○（実施主体としての）副担当、または兼務

△（実施対象者側の）関係者・関係部署

■簡単な定義②：

★ (理想的には) 経営層からの強い指示・承認が存在すること

☆ 経営層からの指示・承認が伴うこと

主たる運営主体者・運営責任者

品質管理		IT部門		セキュリティ監査部門		運用		保守		監視モニタリング		PSIRT		人事、総務		法務、広報	
M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T
		◎															
		○	○	○													
		○	○			△	△	△						△		○	
		○	◎														
		○	◎														
		○	○			◎	◎										
		○	○			◎	◎	○	○								
						◎	◎	○	○								
						○	○	○	○								
						○	◎	○	○								
		○	○			◎	◎			○	○						
		○	○			◎	◎	○	○	○	○						
						○		△		○				◎			
		○	○	◎	◎		○		△							○	
						○		△						◎			
		○	○			○		△						◎			
		○	○	◎	◎												
		○	○			◎	◎	○	○	○	△			△		○	
		○	○			○	○	◎	◎								
		○	◎	△						○				◎		△	

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

（裏表紙）

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.