脆弱性対応のための
適切な資産管理手法へのチャレンジ

ICSセキュリティ担当者コミュニティーメンバー

日本精工株式会社
デジタル変革本部 ITガバナンス部
担当課長 田中 哲也 氏

パナソニック オートモーティブシステムズ株式会社
開発本部 プラットフォーム開発センター セキュリティ開発部
係長 越智 直紀 氏

一般社団法人JPCERTコーディネーションセンター
国内コーディネーショングループ
制御システムセキュリティ シニアアナリスト 河野 一之

1. はじめに

- 脆弱性対策の重要性の認識と促進を阻む「情報活用の課題」 -

制御システムセキュリティの重要性の認識は向上したが…

- 制御システムユーザー組織のセキュリティ施策において

脆弱性対策を進めることは重要？	Yes	No
その重要な一手は脆弱性情報の収集？	Yes	No
脆弱性情報を収集していますか？	Yes	No

では、収集した脆弱性情報は対策に活用できていますか・・・？

収集しても活用が進まない一因（課題）は・・・？

活用が進まない「課題」に取り組んだメンバーと共同発表

■ **講演&パネラー：ICSセキュリティ担当者コミュニティーメンバー**

— 日本精工株式会社
デジタル変革本部 ITガバナンス部
担当課長 田中 哲也 氏

— パナソニック オートモーティブシステムズ株式会社
開発本部 プラットフォーム開発センター セキュリティ開発部
係長 越智 直紀 氏

これ以降は、今回、課題に取り組んだコミュニティーメンバーから上記のお二人にご登壇いただき共同で発表いたします

■ **講演&ファシリテーター：**

— 一般社団法人JPCERTコーディネーションセンター
国内コーディネーショングループ シニアアナリスト 河野 一之

アジェンダ

1. はじめに - 脆弱性対策の重要性の認識と促進を阻む「情報活用の課題」 -

2. 「情報活用の課題」の解決へのチャレンジ

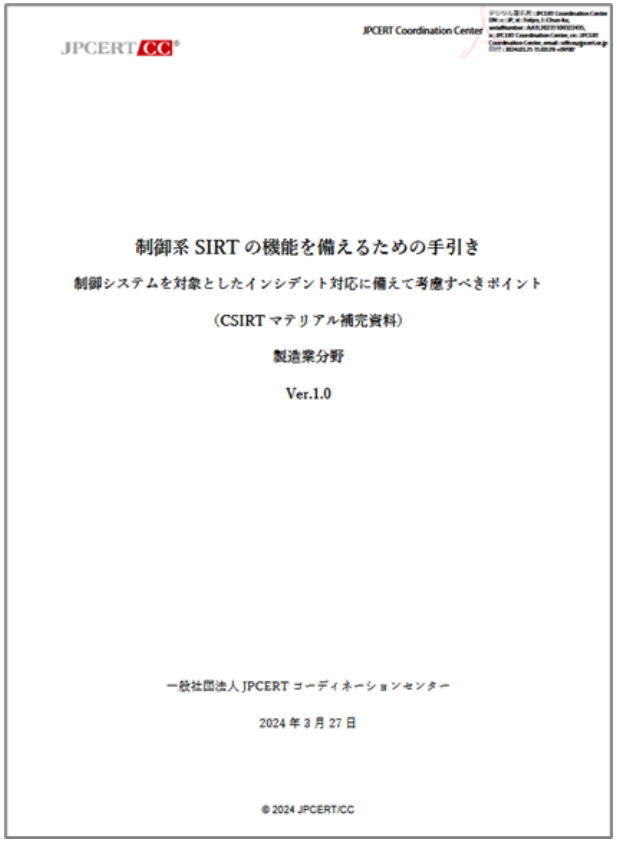
a. 背景・課題
b. 制御システムでの資産管理の難しさ
c. 整理プロセスの全体像
d. 具体的な整理プロセス例 : プロセスⅠ、 Ⅱ、 Ⅲ、 Ⅳ
e. まとめ

3. パネルディスカッション

2. 「情報活用の課題」の解決へのチャレンジ

- a. 背景・課題 -

制御システムセキュリティに関するさまざまな取り組み（例）



JPCERT CC

JPCERT Coordination Center

制御系 SIRT の機能を備えるための手引き

制御システムを対象としたインシデント対応に備えて考慮すべきポイント

（CSIRT マテリアル補完資料）

製造業分野

Ver.1.0

一般社団法人 JPCERT コーディネーションセンター

2024 年 3 月 27 日

© 2024 JPCERT/CC

（左記文書の pp.3～4より）

2. 本書について
2.1. 本書の作成背景
…**「制御系SIRT」が備えるべき能力およびそのために必要なその他の考慮すべき事項等に関する要件**が求められていた。

2.2. 本書の目的
…ICSに関わるセキュリティ担当者が**「制御系SIRT」の新規構築の要件を検討する際の参考として活用し、適切な構築につながる一助としていただくこと**を目的としている。…

出典：JPCERT/CC「制御系SIRTの機能を備えるための手引き - 制御システムを対象としたインシデント対応に備えて考慮すべきポイント -（CSIRTマテリアル補完資料）製造業分野 / Ver.1.0」
https://www.jpcert.or.jp/ics/sirt-for-ics_guide.html

再掲：制御システムセキュリティの重要性の認識は向上したが…

- 制御システムユーザー組織のセキュリティ施策において

脆弱性対策を進めることは重要？	Yes	No
その重要な一手は脆弱性情報の収集？	Yes	No
脆弱性情報を収集していますか？	Yes	No

では、収集した脆弱性情報は対策に活用できていますか・・・？

収集しても活用が進まない一因（課題）は・・・？

ガイダンス等で「やるべきこと」の記載はあるが・・・

■ **（一例）「制御系SIRTの機能を備えるための手引き」 pp.10～11より**

a） 脆弱性の管理と対応

- 利用している**ICS関連製品の棚卸し**
- 棚卸し結果をもとにした**資産管理表の作成**
- 公開されるICS関連の**脆弱性情報の入手**
- 資産管理表において入手した脆弱性情報の**該当の有無を確認**
- 該当があった場合の当該脆弱性の**対応要否の検討**

（中略）

■ 脆弱性に関する3つの対応方針

- アップデートやパッチの適用等による当該脆弱性の**解消（根本的な対処）**
- ワークアラウンドの実施による当該脆弱性におけるリスクの**低減（低減対処）**
- いずれの対処も行わず当該脆弱性の**把握にとどめる（リスクの受容）**

出典： JPCERT/CC「制御系SIRTの機能を備えるための手引き - 制御システムを対象としたインシデント対応に備えて考慮すべきポイント -（CSIRTマテリアル補完資料）製造業分野 / Ver.1.0」
https://www.jpcert.or.jp/ics/sirt-for-ics_guide.html

なぜ制御システムでは脆弱性対応が進まないのか？

- ガイダンス等で「やるべきこと」の記載はあるが・・・

実際に伺ったご意見

対象品を見つけたとして、
対応すべきなのか？
（どうやって判断する？）

対象品を所有
しているのか？

そもそも、システム内に
何台あるのか？

脆弱性対応をして大丈夫なのか？
（更新して、動くのか？）

対象品は、物理的に
どこにあるのか？

どうやってファームウェアや
バージョンを調べる？

更新（脆弱性対応）して、
サポートは切れないのか？

どうやって対象品に
アクセスすれば良いのか？

装置内のどこに、
対象があるのか？

どんな手順で検出して、
対応すればよいのか？

対象品は、論理的に
どこにあるのか？

なぜ制御システムでは脆弱性対応が進まないのか？

- ガイダンス等で「やるべきこと」の記載はあるが・・・

実際に伺ったご意見 → よく見ると、そもそも対象を探すことが難題

対象品を見つけたとして、
対応すべきなのか？
（どうやって判断する？）

対象品を所有
しているのか？

そもそも、システム内に
何台あるのか？

脆弱性対応をして大丈夫なのか？
（更新して、動くのか？）

対象品は、物理的に
どこにあるのか？

どうやってファームウェアや
バージョンを調べる？

更新（脆弱性対応）して、
サポートは切れないのか？

どうやって対象品に
アクセスすれば良いのか？

装置内のどこに、
対象があるのか？

どんな手順で検出して、
対応すればよいのか？

対象品は、論理的に
どこにあるのか？

そもそも対象を探して整理することが難題

■ **（一例）「制御系SIRTの機能を備えるための手引き」 pp.10～11より**

a） 脆弱性の管理と対応

- 利用している**ICS関連製品の棚卸し**
- 棚卸し結果をもとにした**資産管理表の作成**

資産管理

- 公開されるICS関連の**脆弱性情報の入手**
- 資産管理表において入手した脆弱性情報の**該当の有無を確認**
- 該当があった場合の当該脆弱性の**対応要否の検討**

脆弱性調査

（中略）

■ 脆弱性に関する3つの対応方針

- アップデートやパッチの適用等による当該脆弱性の**解消（根本的な対処）**
- ワークアラウンドの実施による当該脆弱性におけるリスクの**低減（低減対処）**
- いずれの対処も行わず当該脆弱性の**把握にとどめる（リスクの受容）**

脆弱性対応

出典： JPCERT/CC「制御系SIRTの機能を備えるための手引き - 制御システムを対象としたインシデント対応に備えて考慮すべきポイント -（CSIRTマテリアル補完資料）製造業分野 / Ver.1.0」
https://www.jpcert.or.jp/ics/sirt-for-ics_guide.html

まず取り組むべき課題は・・・

- ここまでの流れで見えてきたことは・・・

脆弱性対応に至るために、まずは、資産管理に取り組むことが必要

では、脆弱性対応に至るための「適切な資産管理」とは・・・

具体的に、何を取得・理解・整理し、何を作り、どう使うべきなのか？

2. 「情報活用の課題」の解決へのチャレンジ

- b. 制御システムでの資産管理の難しさ-

難しい理由（例）

現状
（資産管理）

「対処すべきもの」＝最初のステップである資産管理自体が難しい

1. （脆弱性対応に）必要な情報や項目が、明確になっているか？
2. 必要な情報の調べ方が、明確になっているか？
   （物理的単位での重要装置の台帳管理は、できていることが多い）
3. 装置や機材が非常に多く、適切な単位ですべて捕捉できているか？

どのように進めれば良いか？

現状
（資産管理）

「対処すべきもの」＝最初のステップである資産管理自体が難しい

1. （脆弱性対応に）必要な情報や項目が、明確になっているか？
2. 必要な情報の調べ方が、明確になっているか？
   （物理的単位での重要装置の台帳管理は、できていることが多い）
3. **装置や機材が非常に多く、**適切な単位で**すべて捕捉できているか？**

最初からすべて捕捉を目指すことは、現実的ではない

小範囲から始め
少しずつ広げる

- **小さな範囲から始め、**少しずつ広げていく
  長期的には全体をカバーし、その後も継続的に少しずつ改善する

最初に着手すべき部分の判断はどうあるべきか？

始める基準はどうあるべきか？

セキュリティリスク（CVSSなど）を基準に考えたくなるが
制御システムによる**事業被害の最小化を目指す**ことが必要

経営への影響が大きい事業の資産から順に、セキュリティ対策を進める

小範囲から始め
少しずつ広げる

最初からすべて捕捉を目指すことは、現実的ではない

- **小さな範囲から始め、**少しずつ広げていく
  長期的には全体をカバーし、その後も継続的に少しずつ改善する

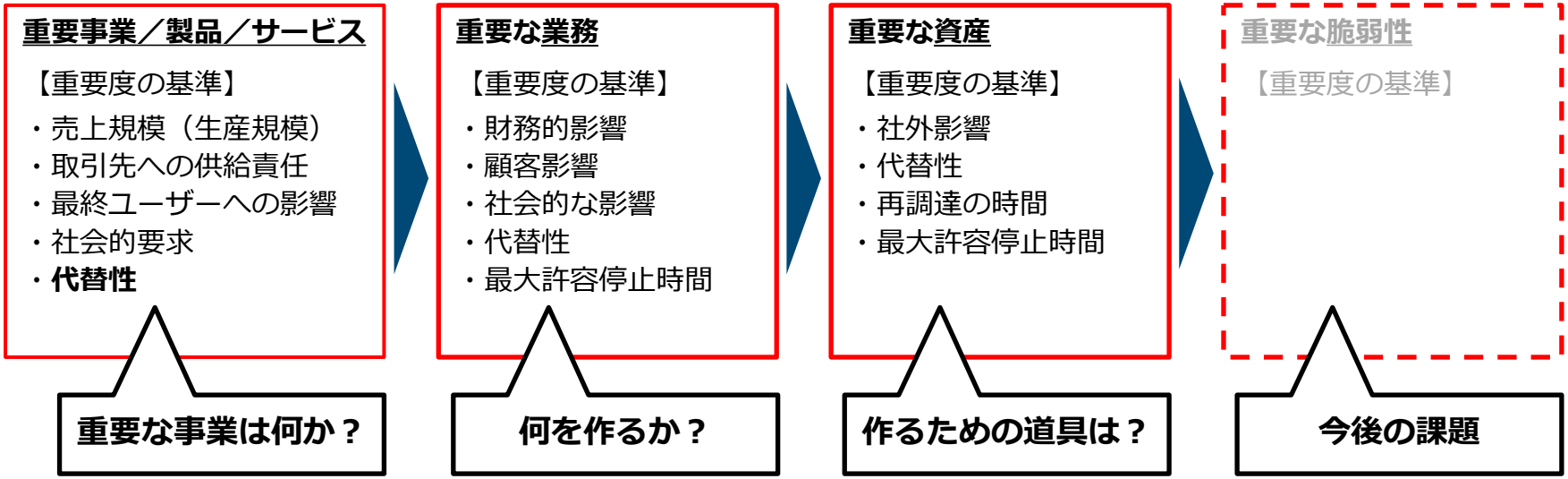
最初に着手すべき部分の判断はどうあるべきか？

同じやるなら効果が高い順にできる基準を

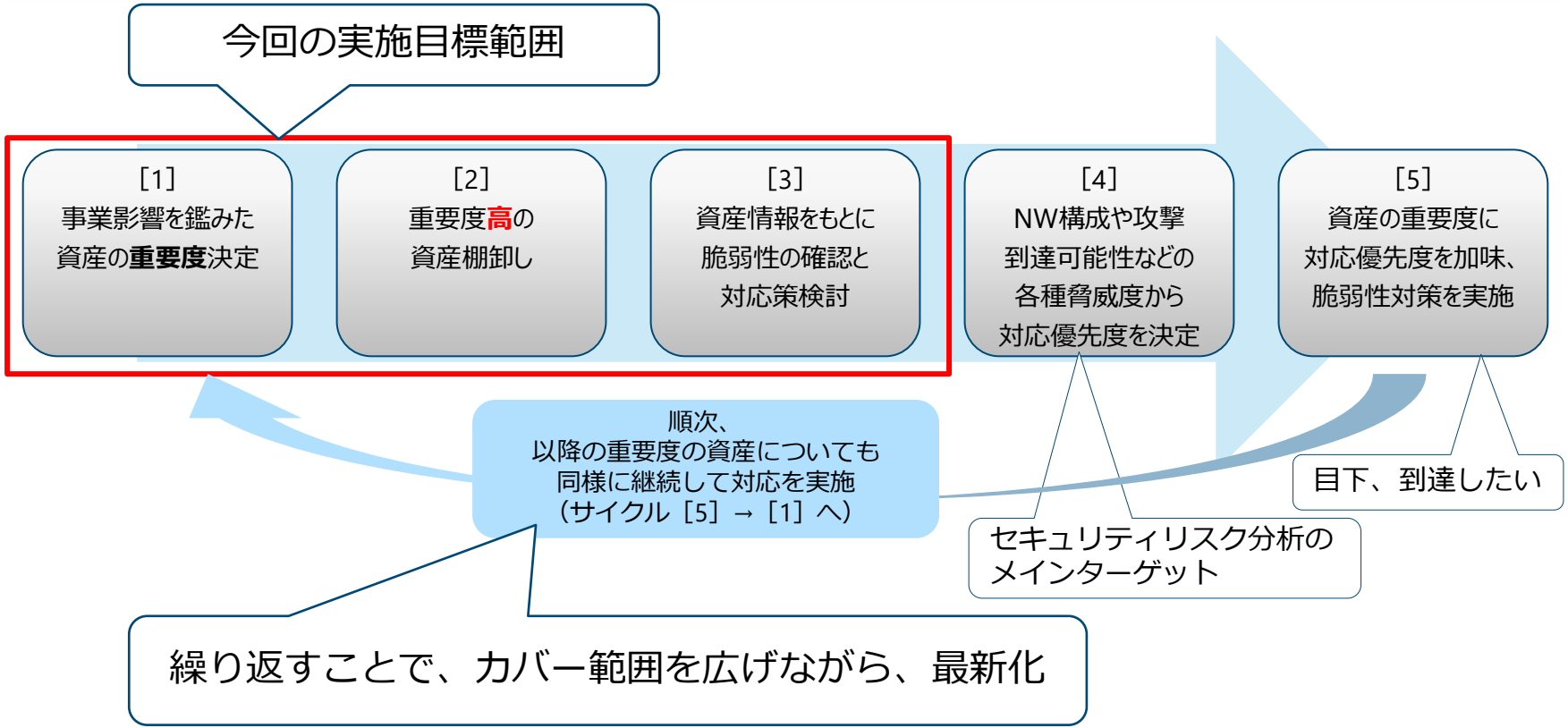
重要度の判断軸検討（例）

（例）ビジネスインパクト分析（BIA）による優先順位付け

BCPなどすでに検討済みなものがあれば、それを活用することも良い



想定する脆弱性対策の概要



この流れを少しでも具体的に

■ **（一例）「制御系SIRTの機能を備えるための手引き」 pp.10～11より**

a） 脆弱性の管理と対応

- 利用している**ICS関連製品の棚卸し**
- 棚卸し結果をもとにした**資産管理表の作成**
- 公開されるICS関連の**脆弱性情報の入手**
- 資産管理表において入手した脆弱性情報の**該当の有無を確認**
- 該当があった場合の当該脆弱性の**対応要否の検討**

（中略）

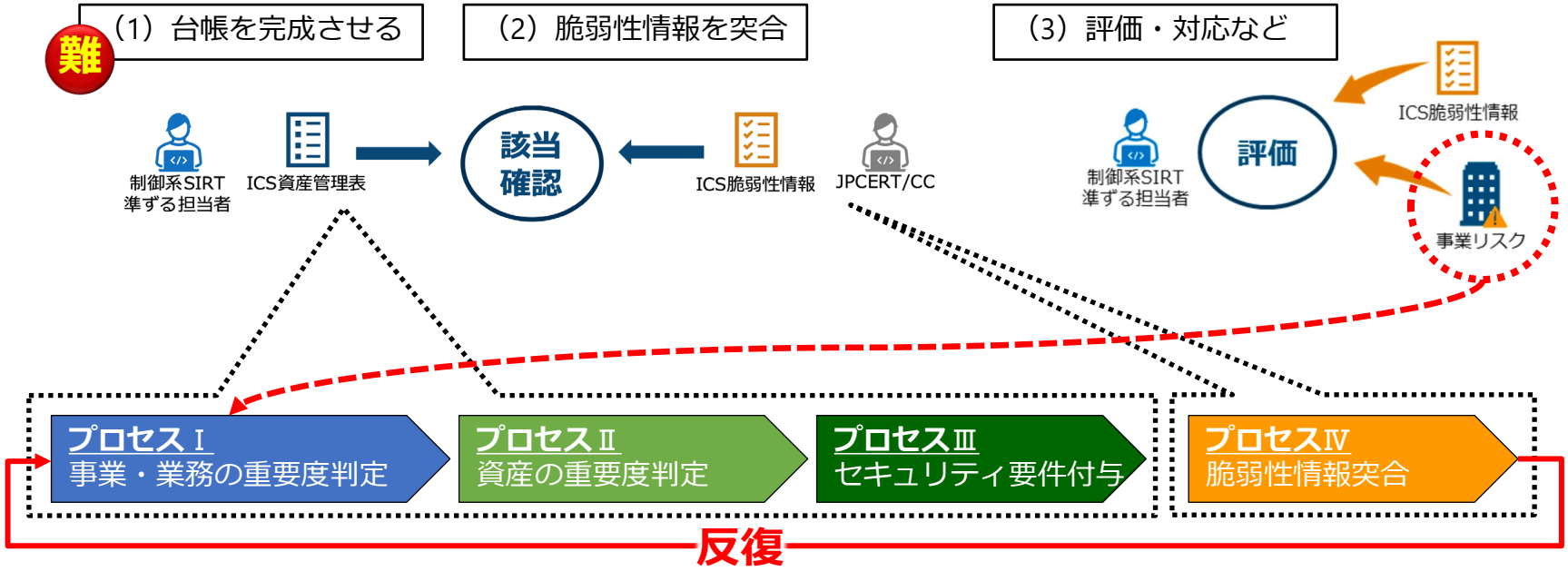
■ 脆弱性に関する3つの対応方針

- アップデートやパッチの適用等による当該脆弱性の**解消（根本的な対処）**
- ワークアラウンドの実施による当該脆弱性におけるリスクの**低減（低減対処）**
- いずれの対処も行わず当該脆弱性の**把握にとどめる（リスクの受容）**

出典： JPCERT/CC「制御系SIRTの機能を備えるための手引き - 制御システムを対象としたインシデント対応に備えて考慮すべきポイント -（CSIRTマテリアル補完資料）製造業分野 / Ver.1.0」
https://www.jpcert.or.jp/ics/sirt-for-ics_guide.html

重要度で絞り込み小さな範囲からスタートする

制御系SIRTの機能を備えるための手引き（p.11）の図5、6を参考



出典：JPCERT/CC「制御系SIRTの機能を備えるための手引き - 制御システムを対象としたインシデント対応に備えて考慮すべきポイント -（CSIRTマテリアル補完資料）製造業分野 / Ver.1.0」
https://www.jpcert.or.jp/ics/sirt-for-ics_guide.html

2. 「情報活用の課題」の解決へのチャレンジ

- c. 整理プロセスの全体像 -

脆弱性対応に至るまでの全体像

- 脆弱性対応に至るまでの4つのプロセスをそれぞれフェーズに分ける

進め方

プロセスⅠ 事業・業務の重要度判定	プロセスⅡ 資産の重要度判定	プロセスⅢ セキュリティ要件付与	プロセスⅣ 脆弱性情報突合
フェーズ①事業・業務一覧作成	フェーズ④資産一覧作成	フェーズ⑦要素分解	フェーズ⑨脆弱性情報取得
フェーズ②事業・業務重要性評価	フェーズ⑤資産重要性評価	フェーズ⑧付帯情報付与	フェーズ⑩脆弱性情報突合
フェーズ③重点事業・業務絞り込み	フェーズ⑥重点資産絞り込み		

作成物

【a. 事業・業務表】

事業・業務	評価 A	評価 B	重要性スコア	重点
ラインA	✓		5	
ラインB		✓	4	
ラインC	✓	✓	9	○
ラインD			0	③

① ②

【b. 資産管理表】

ラインC 資産	評価 C	評価 D	重要性スコア	重点	要件 E	要件 F
資産A		✓	5		−	−
資産 B	✓	✓	9	○	製品1	Ver3
資産C	✓	✓	9	○	製品2	Ver2
資産D	✓		4	⑥	−⑦	⑧−

④ ⑤

【c. 脆弱性情報】

CVE	要件 E	要件 F
001	製品2	Ver1
002	製品4	Ver2
003	製品2	Ver2
004	製品9	Ver1

⑨

⑩

2. 「情報活用の課題」の解決へのチャレンジ

- d. 具体的な整理プロセス例：プロセスⅠ、Ⅱ、Ⅲ、Ⅳ

d．具体的な整理プロセス例：

プロセスⅠ：事業・業務の重要度判定

脆弱性対応に至るまでの全体像

■ まずはプロセスⅠで、事業・業務の重要度を判定する

進め方

プロセスⅠ 事業・業務の重要度判定	プロセスⅡ 資産の重要度判定	プロセスⅢ セキュリティ要件付与	プロセスⅣ 脆弱性情報突合
フェーズ①事業・業務一覧作成	フェーズ④資産一覧作成	フェーズ⑦要素分解	フェーズ⑨脆弱性情報取得
フェーズ②事業・業務重要性評価	フェーズ⑤資産重要性評価	フェーズ⑧付帯情報付与	フェーズ⑩脆弱性情報突合
フェーズ③重点事業・業務絞り込み	フェーズ⑥重点資産絞り込み		

作成物

【a. 事業・業務表】

事業・業務	評価 A	評価 B	重要性スコア	重点
ラインA	✓		5	
ラインB		✓	4	
ラインC	✓	✓	9	○
ラインD			0	③

① ②

【b. 資産管理表】

ラインC資産	評価 C	評価 D	重要性スコア	重点	要件 E	要件 F
資産A		✓	5		−	−
資産B	✓	✓	9	○	製品1	Ver3
資産C	✓	✓	9	○	製品2	Ver2
資産D	✓		4	⑥	−⑦	⑧−

④ ⑤

【c. 脆弱性情報】

CVE	要件 E	要件 F
001	製品2	Ver1
002	製品4	Ver2
003	製品2	Ver2
004	製品9	Ver1

⑩ ⑨

「プロセスⅠ：事業・業務の重要度判定」の手順

■ 目的：「重要性スコア」をもとに重要度（影響度）を判定し、
プロセスⅡの対象となる事業・業務を絞り込む（「重点」を特定）

プロセス	フェーズ	ステップ	作成物
プロセスⅠ 事業・業務の 重要度（影響度） 判定	フェーズ① 事業・業務一覧作成	ステップ1. 事業・業務を一覧化する	a. 事業・業務表
	フェーズ② 事業・業務重要性評価	ステップ2. 考えられる事業リスクを洗い出す	
		ステップ3. 事業リスクの重み付けの策定に使用する、影響の切り口を決める	
		ステップ4. ステップ3の影響の切り口に沿って、重み付けを策定する	
		ステップ5. 各業務（ライン）ごとに、該当するかどうかを確認する	
		ステップ6. 事業・業務の重要度（影響度）が求まる	
	フェーズ③ 重点事業・業務絞り込み	ステップ7. 最も重要な業務を絞り込む	

事業・業務	評価A	評価B	重要性スコア	重点
ラインA	✓		5	
ラインB		✓	4	
ラインC	✓	✓	9	○
ラインD			0	③

① ②

【具体例】フェーズ①事業・業務一覧作成

【a. 事業・業務表】

被害内容	(業務影響)	健康被害・人身事故(社外・顧客や周辺住人)	健康被害・人身事故(社内・従業員)	資産・環境の破損・汚染（社外）	法規法令違反	個人情報(社外・顧客)	個人情報(社内・従業員)	製品機密	出荷遅延	IP:知的財産(社内)	稼働停止	不良率向上	増退稼働	資産・環境の破損・汚染(社内)	電力・資源浪費	人命(最優先事項)に影響がある場合のフラグ	スコア（合計点）	ライン別の事業リスク（高い→ハイリスク）
社外	社会影響	✓		✓	✓	✓			✓		△	△	△					
	法規法令				✓													
	顧客影響				✓	✓		✓	✓		△	△	△					
財務(F)	損失		✓				✓		✓	✓	✓	✓	✓	✓	✓			
	社外賠償	✓		✓	✓	✓		✓	✓		△	△	△					
HSE		人命(HS)	人命(HS)	環境(E)										環境(E)	環境(E)			
SFOP		安全(S)	安全(S)			個人情報(P)	個人情報(P)		運用(O)		運用(O)	運用(O)	運用(O)					
重み付け一例		5	4	4	4	4	3	3	3	2	2	2	1	1	1			
重み付け根拠		外部×人命	人命	外部被害(重)	法規法令違反	外部×個人情報	個人情報	外部被害(低)	外部被害(低)	内部損害(高)	内部損害(高)	内部損害(高)	内部損害(低)	内部損害(低)	内部損害(低)			
ラインA	製品の組立							✓	✓	✓	✓	✓	✓	✓	✓		15	7
ラインB	樹脂成型→組立		✓	✓	✓				✓	✓	✓	✓	✓	✓	✓	✓	24	8
第2工場ラインC	化学薬品製造	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	32	10
第2工場ラインD	極端な例	✓														✓	5	9

ステップ1

業務（事業）の一覧化

【具体例】フェーズ②事業・業務重要性評価

- 業態などによって事業リスクや重み付けは異なる可能性がある
- BCPなど既存のものがあれば、そちらを活用しても問題ない

ステップ2
考えられる事業リスクを洗い出す

【a. 事業・業務表】

被害内容	(業務影響)	健康被害・人身事故(社外・顧客や周辺住人)	健康被害・人身事故(社内・従業員)	資産・環境の破損・汚染（社外）	法規法令違反	個人情報(社外・顧客)	個人情報(社内・従業員)	製品機密	出荷遅延	IP:知的財産(社内)	稼働停止	不良率向上	縮退稼働	資産・環境の破損・汚染(社内)	電力・資源浪費	人命(最優先事項)に影響がある場合のフラグ	スコア（合計点）	ライン別の事業リスク（高い→ハイリスク）
社外	社会影響	✓		✓	✓	✓			✓		△	△	△					
	法規法令				✓													
	顧客影響				✓	✓		✓	✓		△	△	△					
財務(F)	損失		✓				✓		✓	✓	✓	✓	✓	✓	✓			
	社外賠償	✓		✓	✓	✓		✓	✓		△	△	△					
HSE		人命(HS)	人命(HS)	環境(E)										環境(E)	環境(E)			
SFOP		安全(S)	安全(S)			個人情報(P)	個人情報(P)		運用(O)		運用(O)	運用(O)	運用(O)					
重み付け一例		5	4	4	4	4	3	3	3	2	2	2	1	1	1			
重み付け根拠		外部×人命	人命	外部被害（重）	法規法令違反	外部×個人情報	個人情報	外部被害（低）	外部被害（低）	内部損害（高）	内部損害（高）	内部損害（高）	内部損害（低）	内部損害（低）	内部損害（低）			
ラインA	製品の組立							✓	✓	✓	✓	✓	✓	✓	✓		15	7
ラインB	樹脂成型→組		✓	✓	✓				✓	✓	✓	✓	✓	✓	✓	✓	24	8
第2工場ラインC	化学薬品製造	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	32	10
第2工場ラインD	極端な例	✓														✓	5	9

ステップ3
重み付け策定に使用する影響の切り口を決める

ステップ4
ステップ3の切り口に沿って重み付けを策定する

ステップ5
各業務（ライン）ごとに確認する

ステップ6
求めたい重要度を算出

【具体例】フェーズ③重点事業・業務絞り込み

【a. 事業・業務表】

被害内容	(業務影響)	健康被害・人身事故(社外・顧客や周辺住人)	健康被害・人身事故(社内・従業員)	資産・環境の破損・汚染（社外）	法規法令違反	個人情報(社外・顧客)	個人情報(社内・従業員)	製品機密	出荷遅延	IP:知的財産(社内)	稼働停止	不良率向上	縮退稼働	資産・環境の破損・汚染(社内)	電力・資源浪費	人命(最優先事項)に影響がある場合のフラグ	スコア（合計点）	ライン別の事業リスク（高い→ハイリスク）
社外	社会影響	✓		✓	✓	✓			✓		△	△	△					
	法規法令				✓													
	顧客影響				✓	✓		✓	✓		△	△	△					
財務(F)	損失		✓				✓		✓	✓	✓	✓	✓	✓	✓			
	社外賠償	✓		✓	✓	✓		✓	✓		△	△	△					
HSE		人命(HS)	人命(HS)	環境(E)										環境(E)	環境(E)			
SFOP		安全(S)	安全(S)			個人情報(P)	個人情報(P)		運用(O)		運用(O)	運用(O)	運用(O)					
重み付け一例		5	4	4	4	4	3	3	3	2	2	2	1	1	1			
重み付け根拠		外部×人命	人命	外部被害(重)	法規法令違反	外部×個人情報	個人情報	外部被害(低)	外部被害(低)	内部損害(高)	内部損害(高)	内部損害(高)	内部損害(低)	内部損害(低)	内部損害(低)			
ラインA	製品の組立							✓	✓	✓	✓	✓	✓	✓	✓		15	7
第2工場ラインC	化学薬品製造	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	32	10

ステップ7

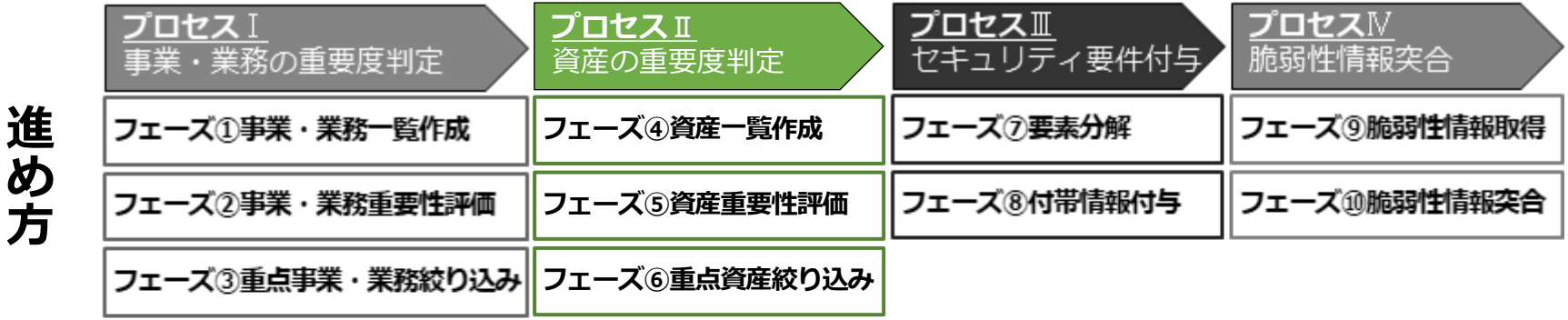
プロセスⅠでの絞り込み結果
（最も重要な業務として、第2工場ラインCを特定）

d．具体的な整理プロセス例：

プロセスⅡ：資産の重要度判定

脆弱性対応に至るまでの全体像

■ 次にプロセスⅡで資産の重要度を判定する



作成物

【a. 事業・業務表】

事業・業務	評価A	評価B	重要性スコア	重点
ラインA	✓		5	
ラインB		✓	4	
ラインC	✓	✓	9	○
ラインD			0	③

①　②

【b. 資産管理表】

ラインC資産	評価C	評価D	重要性スコア	重点	要件E	要件F
資産A		✓	5		−	−
資産B	✓	✓	9	○	製品1	Ver3
資産C	✓	✓	9	○	製品2	Ver2
資産D	✓		4	⑥	−⑦	⑧−

④　⑤

【c. 脆弱性情報】

CVE	要件E	要件F
001	製品2	Ver1
002	製品4	Ver2
003	製品2	Ver2
004	製品9	Ver1

⑨

「プロセスⅡ：資産の重要度判定」の手順

- 目的：プロセスⅠで絞り込んだ事業・業務に属する資産をリストアップし、重要度（影響度）を判定、最重要資産はどこにあるかを見定める

プロセス	フェーズ	ステップ	作成物
プロセスⅡ 資産の重要度判定	フェーズ④ 資産一覧作成	ステップ1. 重点事業・業務の資産を、既存の装置リスト（資産台帳）等を参考に洗い出す	b. 資産管理表
	フェーズ⑤ 資産重要性評価	ステップ2. 事業リスクの重み付け策定に使用した影響の切り口と重みを用い、対象資産が該当するかどうか確認する	
		ステップ3. 各資産の中で、重要度・優先度が求まる	
	フェーズ⑥ 重点資産絞り込み	ステップ4. 最も重要な資産を絞り込む	

ラインC資産	評価C	評価D	重要性スコア	重点
資産A		✓	5	
資産B	✓	✓	9	○
資産C	✓	✓	9	○
資産D	✓		4	

④ ⑤ ⑥

【具体例】フェーズ④資産一覧作成

- 既存の台帳（例えば、装置台帳、固定資産台帳など）を、流用しても問題ない
- 自社のリソースや時間を考慮し、さらに他の業務についても資産の洗い出しが可能と思われる場合は、複数の重要な業務に対する資産を洗い出しても良い

業務	資産	役割	個別資産(装置)における、異常時に想定する重要影響														想定しておくべき各資産の影響度の合計
			健康被害・人身事故（社外・顧客や周辺住人）	健康被害・人身事故（社内・従業員）	資産・環境の破損・汚染（社外）	法規法令違反	個人情報（社外・顧客）	個人情報（社内・従業員）	製品機密の漏洩・改ざん	出荷遅延	IP:知的財産(社内)の漏洩・改ざん	稼働停止	不良率向上	縮退稼働	資産・環境の破損・汚染（社内）	電力・資源浪費	
			5	4	4	4	4	3	3	3	2	2	2	1	1	1	スコア
ラインC(化学	FA-123456	プログラマブルロジックコントローラ（PLC）			✓					✓		✓	✓	✓			12
	FA-123447	モーター制御装置		✓	✓					✓		✓	✓	✓		✓	17
	FA-115458	温度センサー									✓	✓	✓				6
	FA-113459	インバータ								✓		✓	✓	✓	✓	✓	10
	FA-123458	射出成形機	✓	✓	✓	✓				✓	✓	✓	✓	✓	✓	✓	29

プロセスⅠで求めた最も重要な業務

ステップ1
最も重要な業務に属する資産を洗い出す

【具体例】フェーズ⑤資産重要性評価

プロセスＩで用いた
影響の切り口と重み

業務	資産	役割	個別資産(装置)における、異常時に想定すべき悪影響														想定しておくべき各資産の悪影響度の合計
			健康被害・人身事故(社外・顧客や周辺住人)	健康被害・人身事故(社内・従業員)	資産・環境の破損・汚染（社外）	法規法令違反	個人情報(社外・顧客)	個人情報(社内・従業員)	製品機密の漏洩・改ざん	出荷遅延	IP:知的財産(社内)の漏洩・改ざん	稼働停止	不良率向上	縮退稼働	資産・環境の破損・汚染（社内）	電力・資源浪費	
			5	4	4	4	4	3	3	3	2	2	2	1	1	1	スコア
ラインC(化学)	FA-123456	プログラマブルロジックコントローラ (PLC)			✓					✓		✓	✓	✓			12
	FA-123447	モーター制御装置		✓	✓					✓		✓	✓	✓		✓	17
	FA-115458	温度センサー									✓	✓	✓				6
	FA-113459	インバータ								✓		✓	✓	✓	✓	✓	10
	FA-123458	射出成形機	✓	✓	✓	✓				✓	✓	✓	✓	✓	✓	✓	29

ステップ2
対象資産が該当する
影響項目を確認する

ステップ3
対象業務内での
重要度を算出

【具体例】フェーズ⑥重点資産絞り込み

- 複数の業務で資産を洗い出した場合、プロセスⅠの結果とプロセスⅡの結果を用いることで、洗い出した資産の中での重要資産を特定する事もできる
- 例えばプロセスⅠの値×プロセスⅡの値でスコアを算出

業務	資産	役割	個別資産(装置)における、異常時に想定すべき悪影響														想定しておくべき各資産の悪影響度の合計
			健康被害・人身事故(社外・顧客や周辺住人)	健康被害・人身事故(社内・従業員)	資産・環境の破損・汚染（社外）	法規法令違反	個人情報(社外・顧客)	個人情報(社内・従業員)	製品機密の漏洩・改ざん	出荷遅延	IP:知的財産(社内)の漏洩・改ざん	稼働停止	不良率向上	縮退稼働	資産・環境の破損・汚染（社内）	電力・資源浪費	
			5	4	4	4	4	3	3	3	2	2	2	1	1	1	スコア
ラインC(化学)	FA-123456	プログラマブルロジックコントローラ (PLC)			✓					✓		✓	✓	✓			12
	FA-123447	モーター制御装置		✓	✓					✓		✓	✓	✓		✓	17
	FA-115458	温度センサー									✓	✓	✓				6
	FA-113459	インバータ								✓		✓	✓	✓	✓	✓	10
	FA-123458	射出成形機	✓	✓	✓	✓				✓	✓	✓	✓	✓	✓	✓	29

ステップ4
プロセスⅡでの絞り込み結果
（最優先で実施すべき資産特定）

d．具体的な整理プロセス例：

プロセスⅢ：セキュリティ要件付与

脆弱性対応に至るまでの全体像

- プロセスⅢでは、プロセスⅡで作成した資産管理表に、セキュリティ要件を付与する

進め方

プロセスⅠ 事業・業務の重要度判定	プロセスⅡ 資産の重要度判定	プロセスⅢ セキュリティ要件付与	プロセスⅣ 脆弱性情報突合
フェーズ①事業・業務一覧作成	フェーズ④資産一覧作成	フェーズ⑦要素分解	フェーズ⑨脆弱性情報取得
フェーズ②事業・業務重要性評価	フェーズ⑤資産重要性評価	フェーズ⑧付帯情報付与	フェーズ⑩脆弱性情報突合
フェーズ③重点事業・業務絞り込み	フェーズ⑥重点資産絞り込み		

作成物

【a. 事業・業務表】

事業・業務	評価A	評価B	重要性スコア	重点
ラインA	✓		5	
ラインB		✓	4	
ラインC	✓	✓	9	○
ラインD			0	③

【b. 資産管理表】

ラインC資産	評価C	評価D	重要性スコア	重点	要件E	要件F
資産A		✓	5		−	−
資産B	✓	✓	9	○	製品1	Ver3
資産C	✓	✓	9	○	製品2	Ver2
資産D	✓		4	⑥	−⑦	⑧−

⑩

【c. 脆弱性情報】

CVE	要件E	要件F
001	製品2	Ver1
002	製品4	Ver2
003	製品2	Ver2
004	製品9	Ver1

「プロセスⅢ：セキュリティ要件付与」の手順

- 目的：プロセスⅡで絞り込んだ最重要資産をシステム単位に要素分解し、付帯情報を付与する

プロセス	フェーズ	ステップ	作成物
プロセスⅢ セキュリティ要件付与	フェーズ⑦ 要素分解	ステップ1．最重要資産の中で、システムを洗い出す	b.資産管理表
	フェーズ⑧ 付帯情報付与	ステップ2．システムごとに付帯情報を付与する	

ラインC 資産	評価 C	評価 D	重要性 スコア	重点	要件 E	要件 F
資産A		✓	5		–	–
資産B	✓	✓	9	○	製品1	Ver3
資産C	✓	✓	9	○	製品2	Ver2
資産D	✓		4		–⑦	⑧–

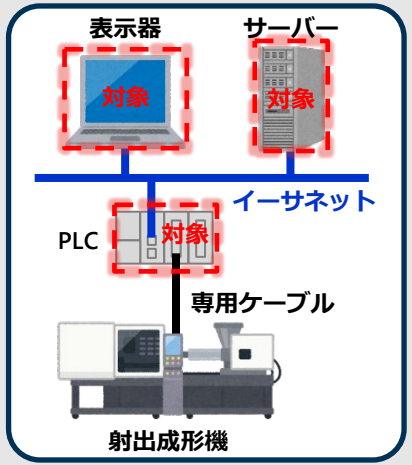
【具体例】フェーズ⑦要素分解

- 今回は、下記理由より「物理的LANポート」を持つシステムを優先的に洗い出した
  - アタックサーフェースの中でも重要度の高いネットワークからの侵入経路を抑えられる
  - 現場に依頼する場合でも、作業者が分かりやすい（洗い出しやすい）
- ただし、これだけでは洗い出しが不十分であり、課題は残る

業務	資産	役割	個別資産(装置)における、異常時に想定すべき悪影響												想定しておくべき各資産の悪影響度の合計	ベンダ名	システム名
			健康被害・人身事故(社外・顧客や周辺住人)							良率向上	縮退稼働	資産・環境の破損・汚染（社内）	電力・資源浪費			
			5							2	1	1	1	スコア		
ラインC(化学)	FA-123456	プログラマブルロジックコントローラ(PLC)								✓	✓			12		
	FA-123447	モーター制御装置								✓	✓		✓	17		
	FA-115458	温度センサー								✓				6		
	FA-113459	インバータ								✓	✓	✓	✓	10		
	FA-123458	射出成形機								✓	✓	✓	✓	29	XXX社	Windows 10
															YYY社	Windows Server 2022
															ZZZ社	PLC−Z

ステップ1

最重要資産の中で、システムを洗い出す



射出成形機のシステム構成イメージ

プロセスⅡで求めた最重要資産

【具体例】フェーズ⑧付帯情報付与

- 今回は、脆弱性情報と突合するための最低限の情報として、「ベンダー名」と「システム名」とした
- 脆弱性対応に必要な情報（例えば、IPアドレス等）や管理・運用情報等を追加しても良い

業務	資産	役割	個別資産(装置)における、異常時に想定すべき悪影響														想定しておくべき各資産の悪影響度の合計	ベンダ名	システム名
			健康被害・人身事故(社外・顧客や周辺住人)	健康被害・人身事故(社内・従業員)	資産・環境の破損・汚染（社外）	法規法令違反	個人情報(社外・顧客)	個人情報(社内・従業員)	製品機密の漏洩・改ざん	出荷遅延	IP:知的財産(社内)の漏洩・改ざん	稼働停止	不良率向上	縮退稼働	資産・環境の破損・汚染（社内）	電力・資源浪費			
			5	4	4	4	4	3	3	3	2	2	2	1	1	1	スコア		
ラインC(化学)	FA-123456	プログラマブルロジックコントローラ (PLC)			✓					✓		✓	✓	✓			12		
	FA-123447	モーター制御装置		✓	✓					✓		✓	✓	✓		✓	17		
	FA-115458	温度センサー									✓	✓	✓				6		
	FA-113459	インバータ								✓		✓	✓	✓	✓	✓	10		
	FA-123458	射出成形機	✓	✓	✓	✓				✓	✓	✓	✓	✓	✓	✓	29	XXX社	Windows 10
																		YYY社	Windows Server 2022
																		ZZZ社	PLC−Z

プロセスⅡで求めた最重要資産

ステップ2
付帯情報を付与し、最重要資産のシステム情報を取得

d．具体的な整理プロセス例：

プロセスⅣ：脆弱性情報突合

脆弱性対応に至るまでの全体像

- プロセスⅣにて、資産管理表と脆弱性情報を突合する

進め方

プロセスⅠ 事業・業務の重要度判定	プロセスⅡ 資産の重要度判定	プロセスⅢ セキュリティ要件付与	プロセスⅣ 脆弱性情報突合
フェーズ①事業・業務一覧作成	フェーズ④資産一覧作成	フェーズ⑦要素分解	フェーズ⑨脆弱性情報取得
フェーズ②事業・業務重要性評価	フェーズ⑤資産重要性評価	フェーズ⑧付帯情報付与	フェーズ⑩脆弱性情報突合
フェーズ③重点事業・業務絞り込み	フェーズ⑥重点資産絞り込み		

作成物

【b. 資産管理表】

事業・業務	評価 A	評価 B	重要性スコア	重点
ラインA	✓		5	
ラインB		✓	4	
ラインC	✓	✓	9	○
ラインD			0	③

①　②

ラインC 資産	評価 C	評価 D	重要性スコア	重点	要件 E	要件 F
資産A		✓	5		−	−
資産B	✓	✓	9	○	製品1	Ver3
資産C	✓	✓	9	○	製品2	Ver2
資産D	✓		4	⑥	−⑦	⑧−

④　⑤

【c. 脆弱性情報】

CVE	要件 E	要件 F
001	製品2	Ver1
002	製品4	Ver2
003	製品2	Ver2
004	製品9	Ver1

⑩　⑨

「プロセスⅣ：脆弱性情報突合」の手順

- 目的：取得した脆弱性情報と資産管理表を突合し、脆弱性対応が必要な資産を見定める

<table>
<tr><th>プロセス</th><th>フェーズ</th><th>ステップ</th><th>作成物</th></tr>
<tr><td rowspan="3">プロセスⅣ
脆弱性情報突合</td><td>フェーズ⑨
脆弱性情報取得</td><td>ステップ1．JVN等から脆弱性情報を取得する</td><td>c．脆弱性情報
<table><tr><th>CVE</th><th>要件E</th><th>要件F</th></tr><tr><td>001</td><td>製品2</td><td>Ver1</td></tr><tr><td>002</td><td>製品4</td><td>Ver2</td></tr><tr><td>003</td><td>製品2</td><td>Ver2</td></tr><tr><td>004</td><td>製品9</td><td>Ver1</td></tr></table></td></tr>
<tr><td rowspan="2">フェーズ⑩
脆弱性情報突合</td><td>ステップ2．脆弱性情報のベンダー名、影響を受けるシステムを利用して、資産管理表と脆弱性情報を突合し、脆弱性の可能性のある資産を抽出する</td><td rowspan="2">b．資産管理表
<table><tr><th>ラインC資産</th><th>評価C</th><th>評価D</th><th>重要性スコア</th><th>重点</th><th>要件E</th><th>要件F</th></tr><tr><td>資産A</td><td></td><td>✓</td><td>5</td><td></td><td>－</td><td>－</td></tr><tr><td>資産B</td><td>✓</td><td>✓</td><td>9</td><td>○</td><td>製品1</td><td>Ver3</td></tr><tr><td>資産C</td><td>✓</td><td>✓</td><td>9</td><td>○</td><td>製品2</td><td>Ver2</td></tr><tr><td>資産D</td><td>✓</td><td></td><td>4</td><td></td><td>－⑦</td><td>⑧－</td></tr></table></td></tr>
<tr><td>ステップ3．システムのバージョン情報を確認し、脆弱性のある資産かどうかを確定する</td></tr>
</table>

【具体例】フェーズ⑨脆弱性情報取得

ステップ1

JVN等から脆弱性情報を取得する

ID	タイトル	最終更新日
JVNVU#00003	EEE社製無線LANルーターにおける複数の脆弱性	2024/12/16
JVNVU#00002	ZZZ社製PLC製品における複数の脆弱性	2024/12/16
JVNVU#00001	TTT社製品に対するアップデート（2024年11月）	2024/12/16

JVN等の脆弱性情報イメージ

JVNVU#00002

ZZZ社製PLC製品における複数の脆弱性

概要

ZZZ社が提供する PLC製品には、複数の脆弱性が存在します。

影響を受けるシステム

- PLC-A
  - Ver 1.100およびそれ以降
- PLC-C
  - Ver 2.100およびそれ以降
- PLC-Z
  - Ver 3.100およびそれ以降

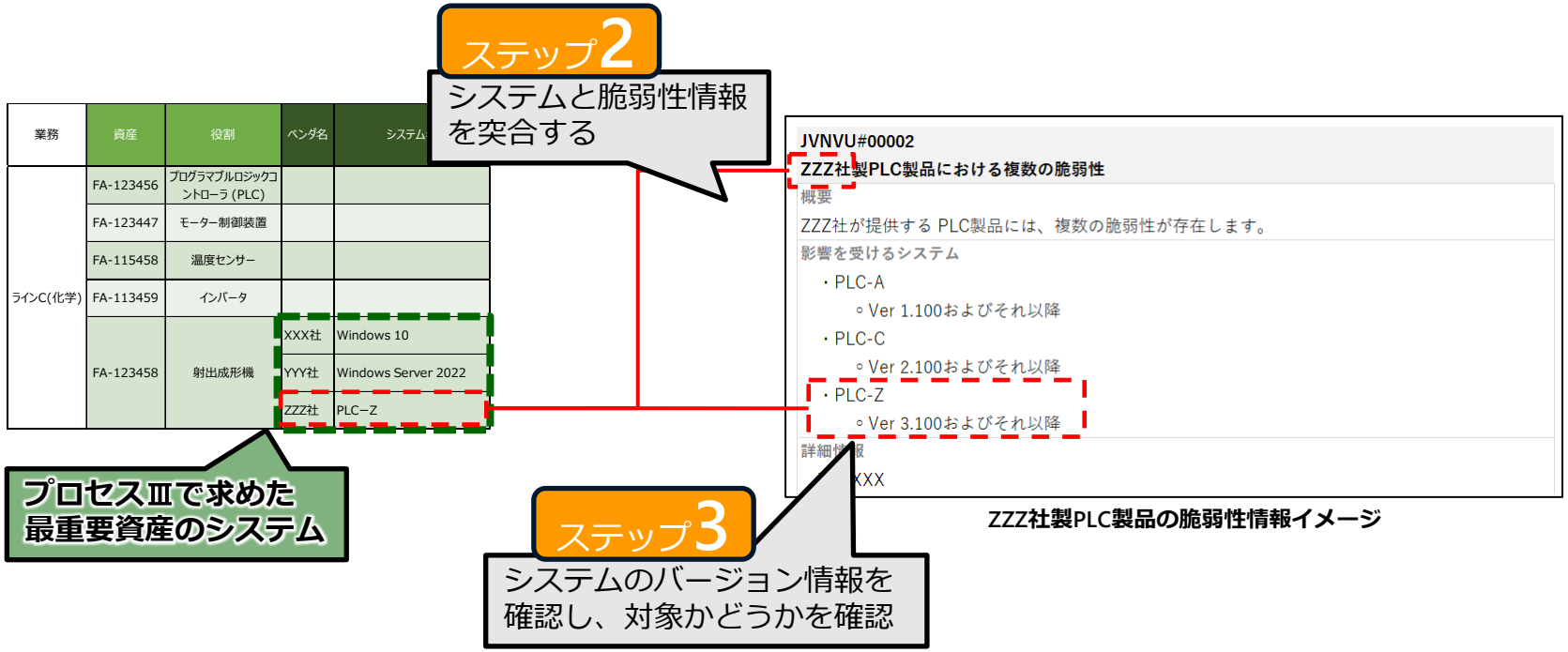
詳細情報

XXXXXX

ZZZ社製PLC製品の脆弱性情報イメージ

【具体例】フェーズ⑩脆弱性情報突合

- 突合しやすいよう、システムのバージョン情報も付帯情報に含めることが理想だが、常に最新情報を管理することが難しいため、今回は突合後にステップ3として確認した



ZZZ社製PLC製品の脆弱性情報イメージ

2. 「情報活用の課題」の解決へのチャレンジ

- e. まとめ -

今回の活動で明らかにしたかった点

脆弱性対応推進に向けた資産管理の一助へ、具体的な実施の流れを

- 制御システムの脆弱性対応を進めたいが、なかなか進まない
- 調べてみると、「実施すべき」と考えていても「対象の有無」=資産管理からして難しい
- それ以前に、対象の資産が多過ぎ、調査範囲が広過ぎ、「どこから手を付けるか」

⇒ **重要なものから**少しずつ進め、ループしながら広げる考え方に向けて、**絞り込み**：プロセスⅠ、Ⅱ

- 「事業／装置」と「ネットワーク上の機器」をリンクさせる（セキュリティ要件）必要がある
- 「装置」の単位と「ネットワーク上の機器」の単位や要件が必ずしも一致せず、重要度を定めにくい

⇒ **セキュリティ要件**と**物理的リスク**を**つなぐポイント**として今回は**物理LANポート**を使用：プロセスⅢ、Ⅳ

すべてを最初から実施するのではなく、あるものはしっかり活用する

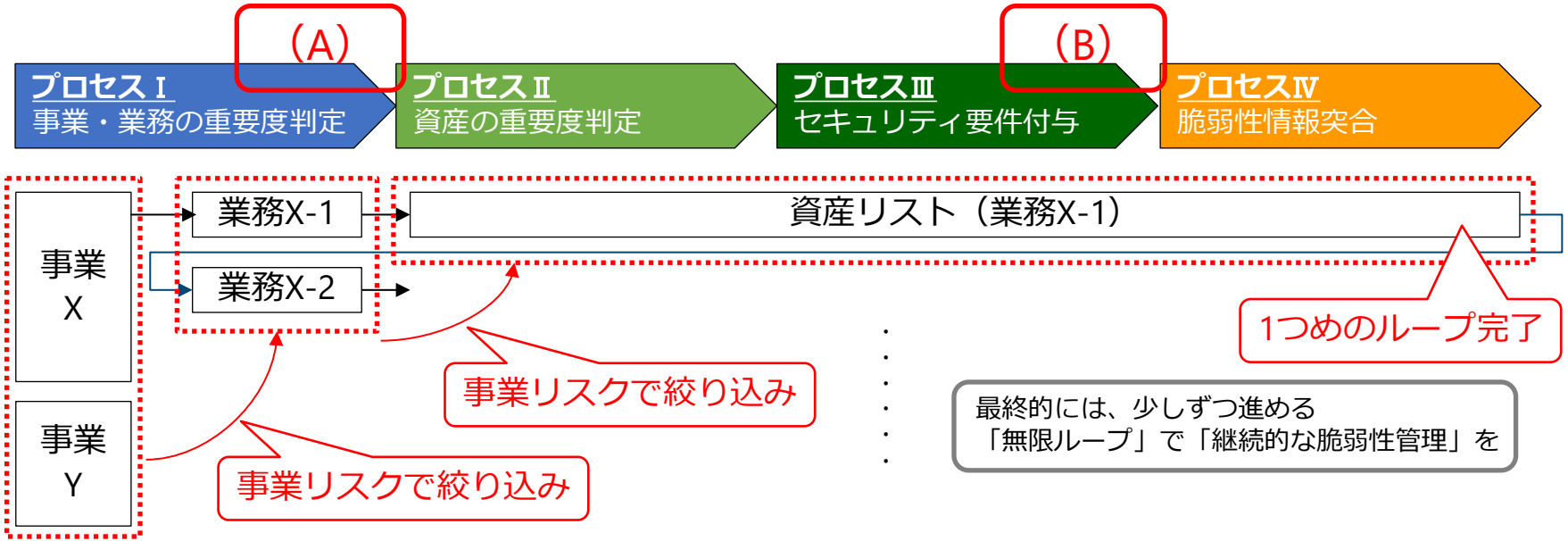
有用なツールも販売されており、それらを使いこなす際等の判断に必要な材料を提示したい

まとめ

具体的に対象を絞り込み、突合していく1つの流れ（ループ）、**推進イメージを紹介**

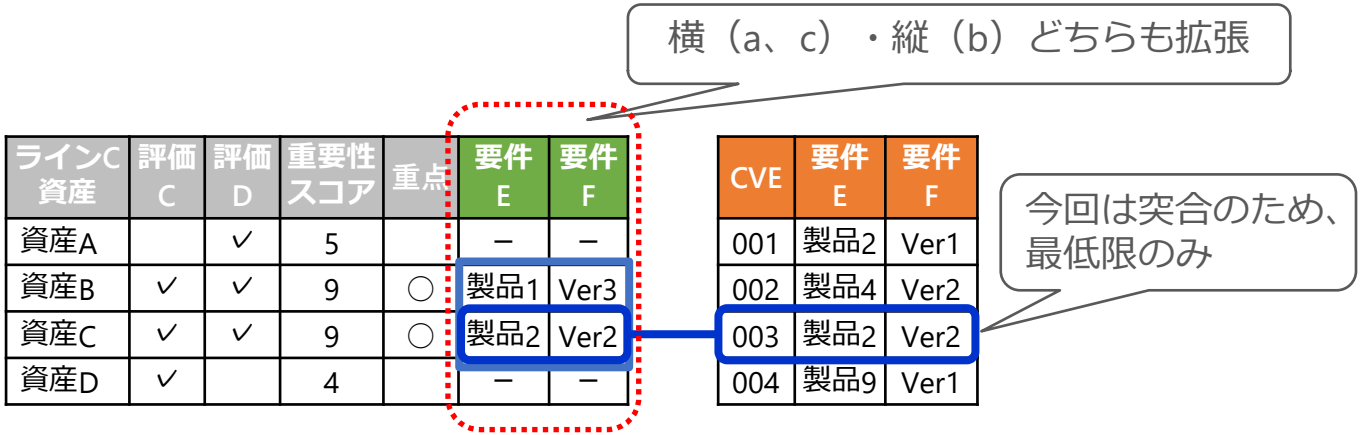
A) **事業・業務および資産の重要度判定（絞り込み）例**の提示

B) 脆弱性情報との突合に必要な、**最低限のセキュリティ要件（項目）例**の提示



脆弱性対応をさらに促進するための次のステップ

- **プロセスⅢの拡張**と、**プロセスⅣまでの実例・経験を増やすこと**で、さらに有用な形に
  a. 脆弱性対応に関して（脆弱性情報の突合だけでなく）突合後に必要なセキュリティ要件の抽出
  b. 物理装置（資産）単位と、セキュリティ（脆弱性）管理単位を結合する他の要素の洗い出しと、その確認方法の検討（今回は要素を「物理LANポート」とした）
  c. 脆弱性対応の後に控えるサイバー攻撃対策（リスクアセスメントなど）の要件抽出と整理



3. パネルディスカッション

- さらに深掘り -

各種お問い合せ、ご相談は

情報収集やセキュリティ評価など、IT／OTセキュリティで困ったら、
下記へお気軽にお問い合わせください。

■ **情報系・制御系セキュリティに関する各種ご相談・調査依頼等**
国内コーディネーショングループ

— Email：dc-info@jpcert.or.jp

— https://www.jpcert.or.jp/ics/

■ **制御システムのインシデントに関する報告やご相談**
インシデントレスポンスグループ

— Email：info@jpcert.or.jp

— https://www.jpcert.or.jp/ics/ics-form.html

※資料に記載の社名、製品名は各社の商標または登録商標です。

Thank you!