制御システムのセキュリティリスクにどう備えるか？

～制御システムセーフティ・セキュリティ要件検討ガイド紹介～

独立行政法人 情報処理推進機構（IPA）
社会基盤センター 産業プラットフォーム部
調査役　久野 倫義

お話すること

- 重要インフラ設備へのサイバー攻撃例
- 重要インフラをささえる企業の生の声
- ガイドの特徴

重要インフラ設備へのサイバー攻撃例

重要インフラ設備へのサイバー攻撃例

■ 産業制御システムを狙うマルウェア
産業制御装置の安全システム操作を狙ったマルウェア（TRITON）が仕掛けられる事案が発生 (2017年12月)

■スウェーデンの交通系インフラシステムへのDDoS攻撃(2017年10月)
運輸管理局のITシステムがダウンし列車の発着管理に影響。
Webサイトやメールサービスも停止し列車予約ができなくなった。

■サウジアラビア空港、政府機関への攻撃（2016年11月）
PC数千台が破壊され、数日間業務が停止。新型のShamoonが使用された。

■イスラエル電力公社への大規模サイバー攻撃（2016年1月）
コンピュータ多数が使用不能状態になる。

■ドイツ製鉄所へのサイバー攻撃（2014年）
マルウェアにより情報入手、制御システム乗っ取りで生産設備が損傷。

■Stuxnet感染（2010年11月）
ウラン濃縮施設の遠心分離機がマルウェア感染。約8400台の遠心分離機が停止。

セーフティ・セキュリティ要件の不整合（想定例）

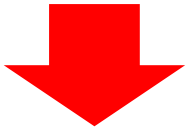
- ウィルスチェックソフトが安全保護システムの安全停止を妨害
  - 制御対象：ボイラー(石油)
  - 安全保護システム：SIL3　第3者認証を取得済
  - 事象：

    PCワークステーションを含む安全保護システムに、
    ウィルスチェックソフトを導入

    →ウイルスチェックソフトが、ワークステーションと
    安全保護システム間の固有通信を遮断

    （※セキュリティ機能にとっては正常側の動作）

    →安全停止処理の稼働要求時に、
    安全停止処理が実行されなかった



セーフティ・セキュリティ要件に整合を取る必要あり

重要インフラをささえる企業の生の声

セーフティシステムへのセキュリティ対応の課題と対策

（背景・課題）

- 重要インフラに対するサイバー攻撃の増加
- セーフティシステムにセキュリティ対策する場合、どのタイミングで、どのように関連付ければいいのか、わからない！
- セーフティ、セキュリティ双方に詳しい技術者は極めて少ない。
- セキュリティ対策がセーフティに及ぼす影響を設計・評価し、実現、連携させる枠組み（プロセス）がまだどこの業界も構築中！

（本ガイドの活用による対策案）

- 機能安全準拠のセーフティシステムに対し、サイバーセキュリティ対策のプロセスを汎用的に示し、まずはプロセスの概要をイメージしてもらう。
- セーフティシステムに、はじめてセキュリティ対応する読者に基本的な知識を習得してもらう。（手軽に読めるガイド、ケーススタディ編で理解を深める）

ガイドの特徴

ガイドの特徴と対象読者

制御システムセーフティ・セキュリティ要件検討ガイド

特徴

✓**セーフティ・ファースト**：既設セーフティシステムが有
✓**国際規格・標準**：IEC 61508、IEC 62443
✓**モデルシステム**：FA（Factory Automation）システム
他分野への適用に関するヒントも掲載

対象読者

✓**安全性が重視される制御システムに従事される方**
①システムを保有する事業者の方
②インテグレータ、メーカー、サプライヤの方
（安全関連システムの設計経験がある、
または、これからセキュリティ対策に取り組もうとしている方）

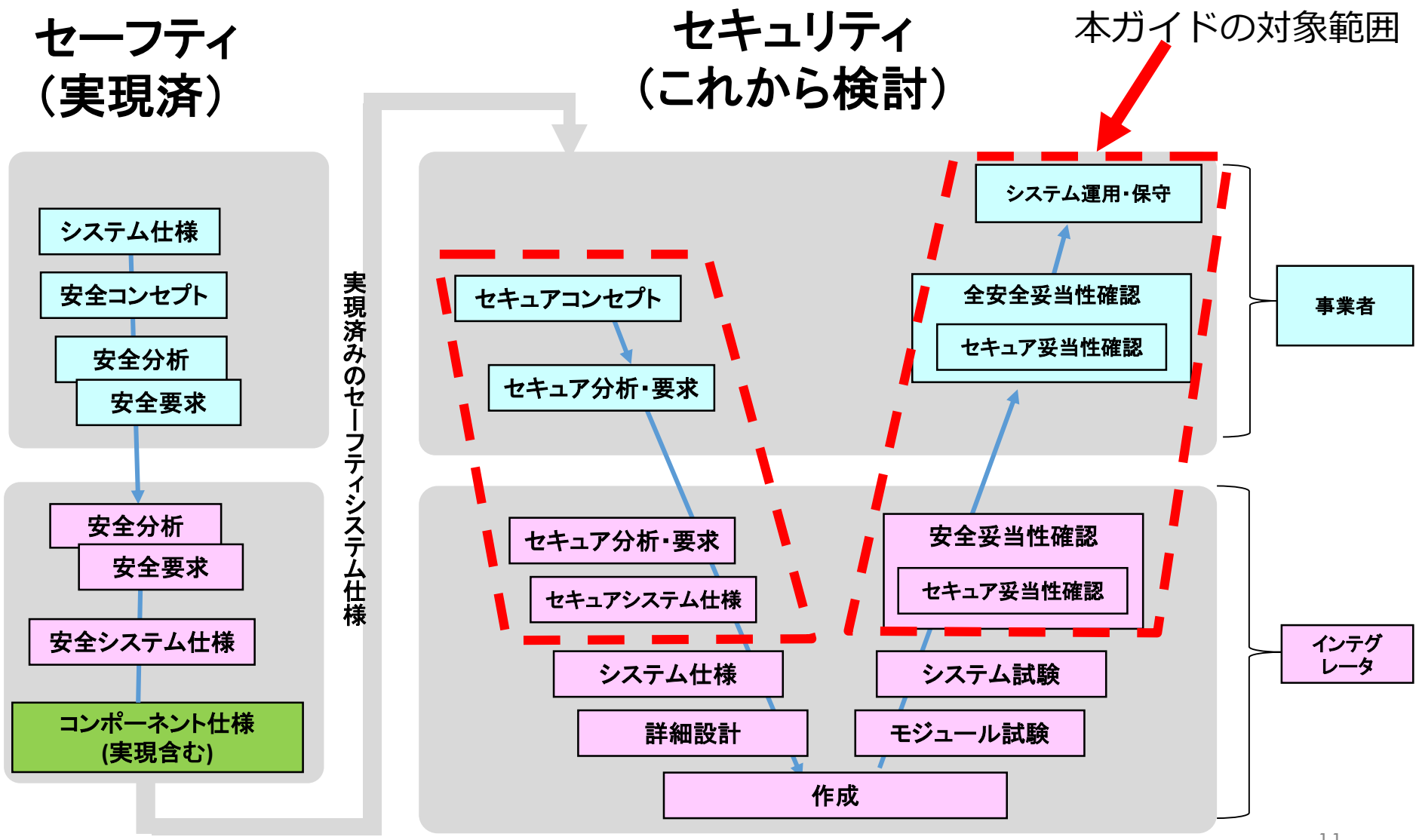
ガイドの構成

◆本ガイドは　2冊　構成です。

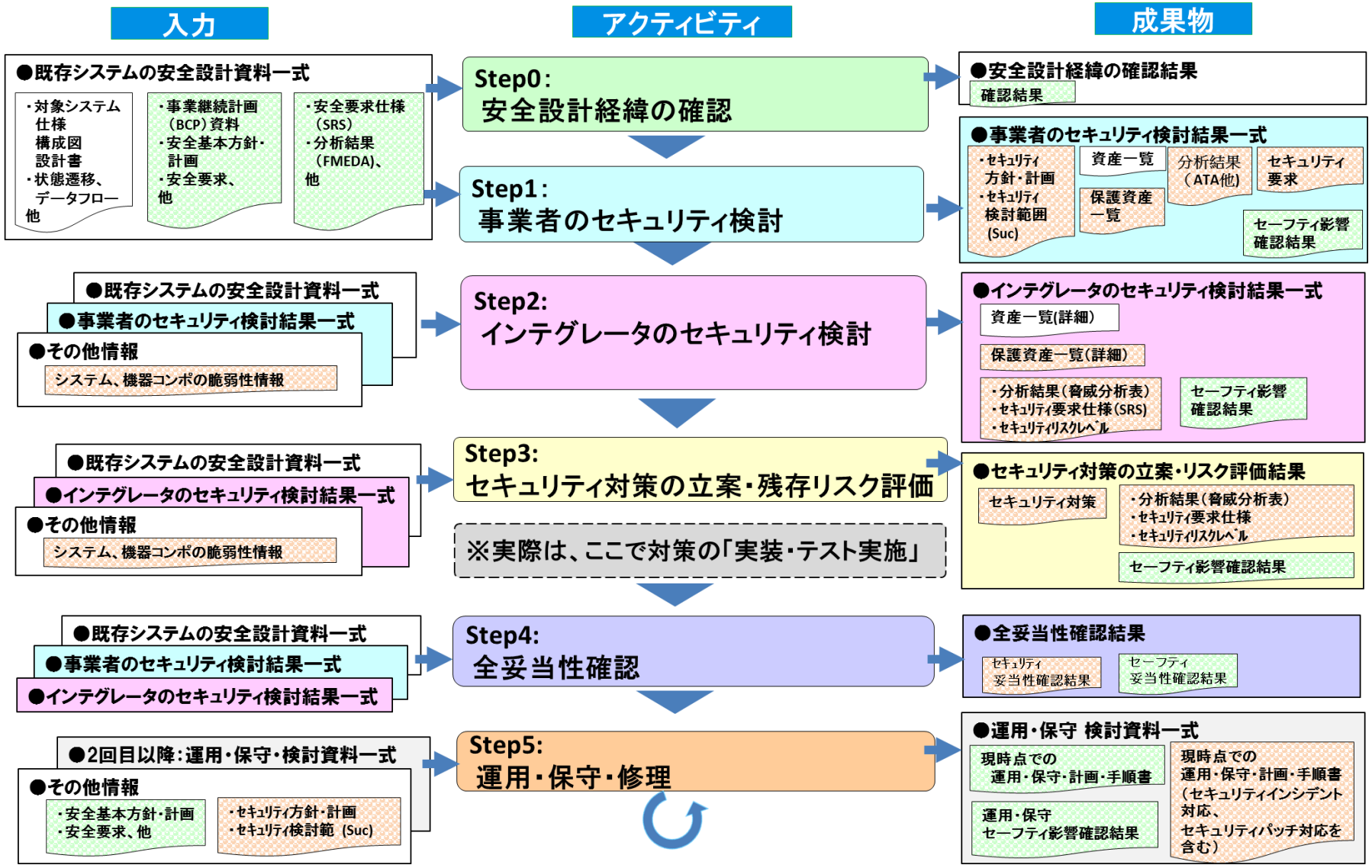
＜基本編＞
セーフティシステムに
セキュリティ対応するときの
・プロセスの外観
・各業界の事例コラムを掲載！

＜ケーススタディ編＞
・プロセスの詳細を解説
・FAシステムの事例で
プロセスをシミュレーション
・セキュリティの脅威分析～
対策の検討まで

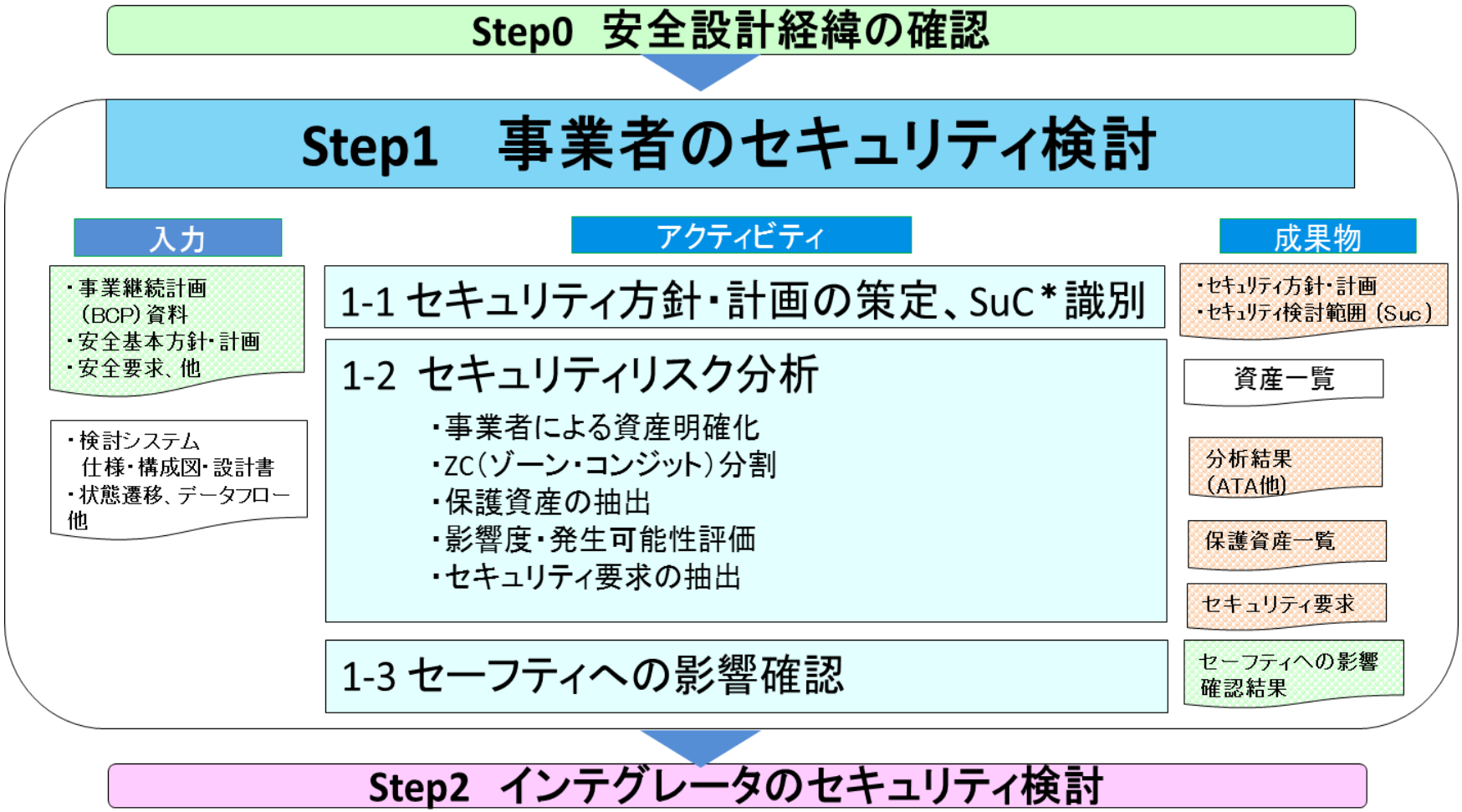
セーフティ・セキュリティ検討プロセスフロー（参考）



「既存の制御システム」に対する S&S 検討プロセス（全体像）

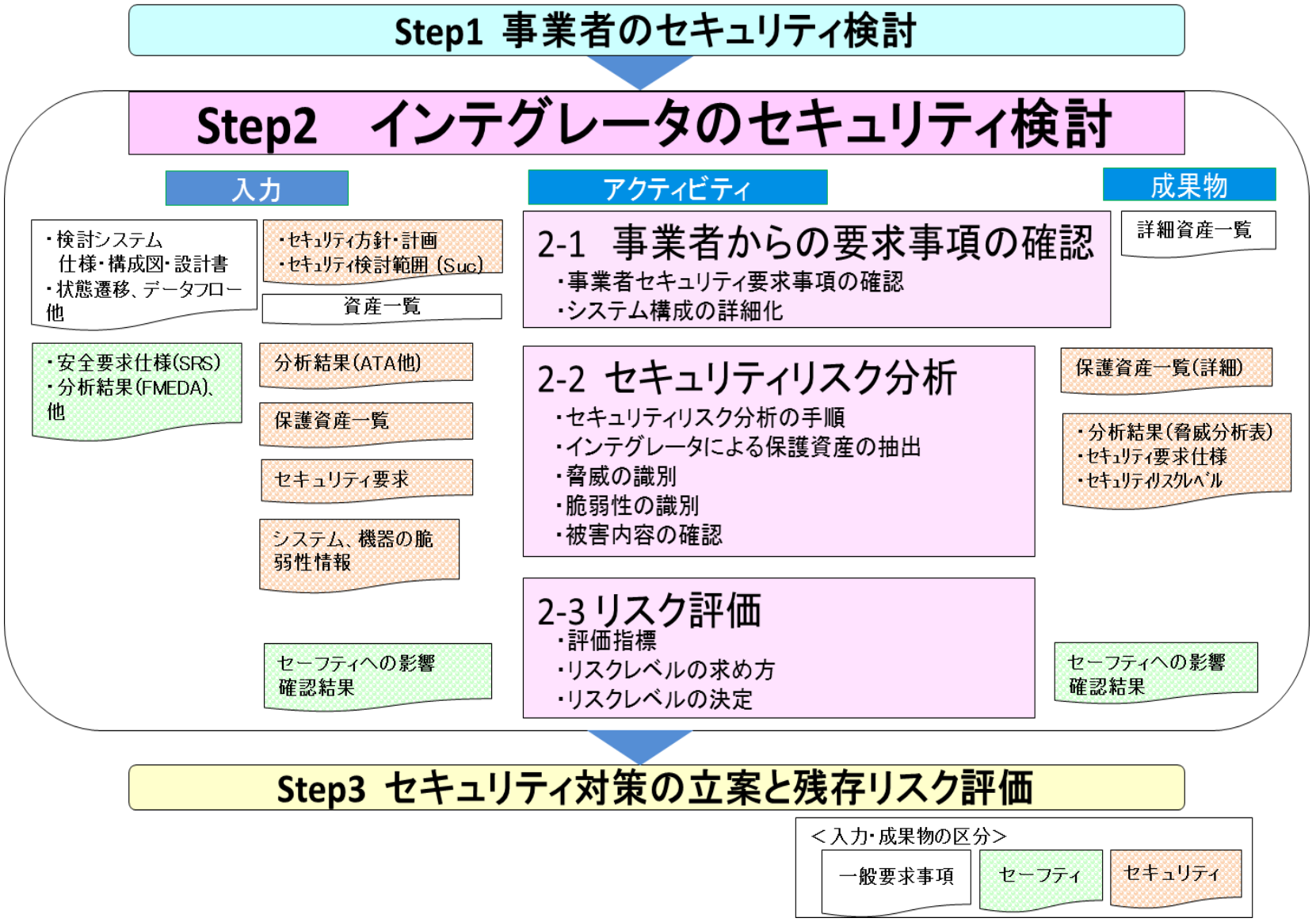


Step1　事業者のセキュリティ検討

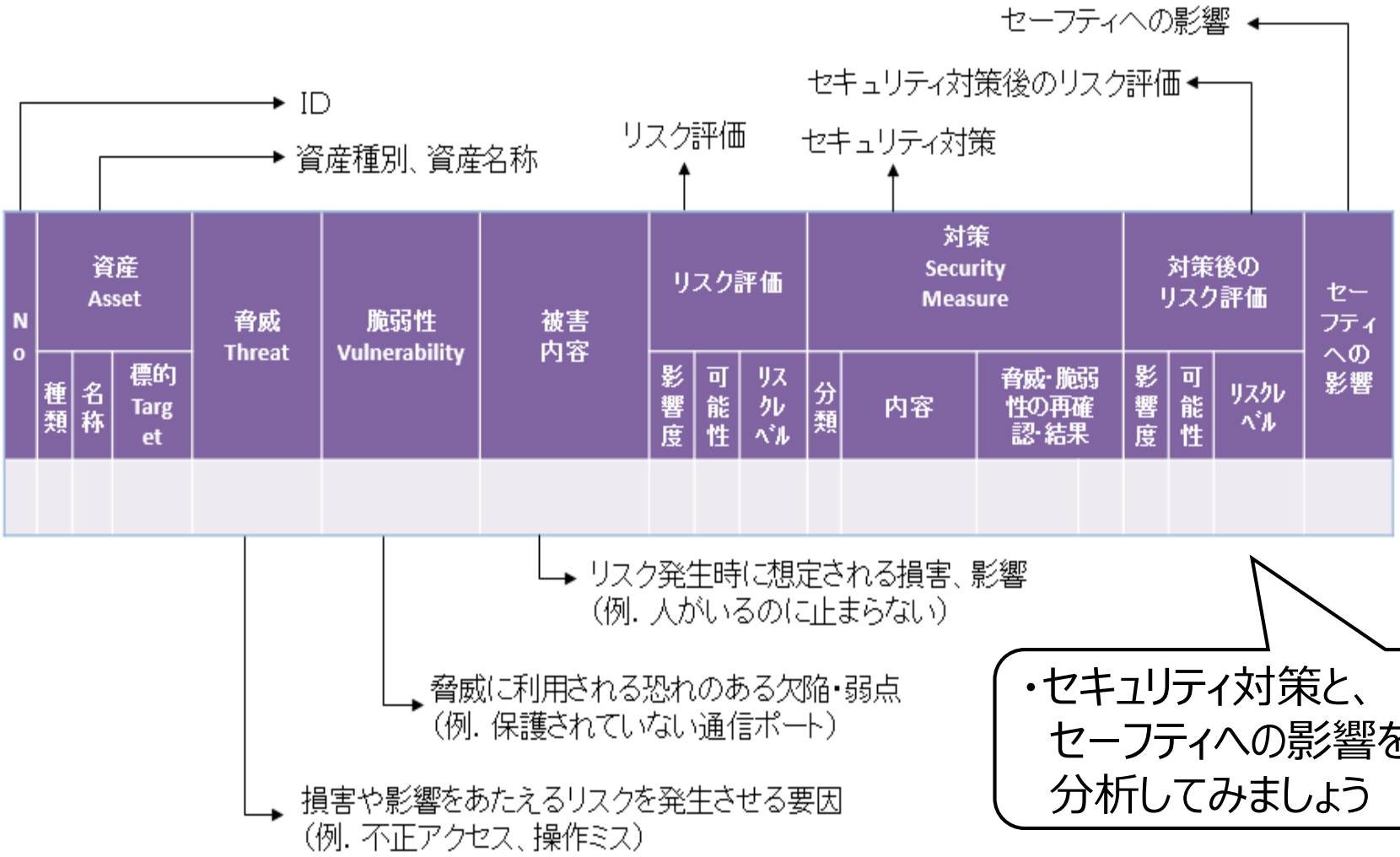


＊) SuC（System under Consideration）：セキュリティ検討対象システム

Step2　インテグレータのセキュリティ検討



脅威分析シート（様式を提供）



本ガイドを用いた演習付セミナー（10月23日実施）

時間		概要	資料	講師
13:30 ～ 13:45	15分	～はじめに～ 制御システム セーフティ・セキュリティ要件検討の課題		社会基盤センター 調査役　久野　倫義
13:45 ～ 14:15	30分	～ガイドの基本編から～ 要件検討ガイドの対象となる制御システムとプロセスの紹介	・テキスト（基本編）	産業サイバーセキュリティセンター 調査役　石田　茂
14:15 ～ 14:30	15分	休憩		
14:30 ～ 17:20	170分	～ケーススタディ編から～ 事例による要件検討プロセスの演習と解説	・テキスト（演習編） ・演習の流れ 全体図 ・システム構成図 ・プロセスフロー ・情報シート ・分析シート	社会基盤センター 調査役　久野　倫義 連携員　細目　紀子 産業サイバーセキュリティセンター 調査役　石田　茂
17:20 ～ 17:30	10分	質疑応答		

多数の方にご参加いただきました！
今後も、実施予定です。

ガイドブック紹介のまとめ

- 制御系システムの各分野で活用可能な汎用的なガイドブックです
- 実際の開発現場で、セーフティ・セキュリティ検討時に参考となる基本的な手順・考え方を紹介しています（国際規格準拠）
- ケーススタディ事例による解説！　（ 分析シートつき）
- はじめてのセーフティ・セキュリティ教育教材として、ご利用ください。

（PowerPointイメージですので、そのまま使えます！）

ご清聴、ありがとうございました！

・PDFダウンロード無料！
https://www.ipa.go.jp/sec/reports/20180319.html

展示ブースでサンプル
を確認ください

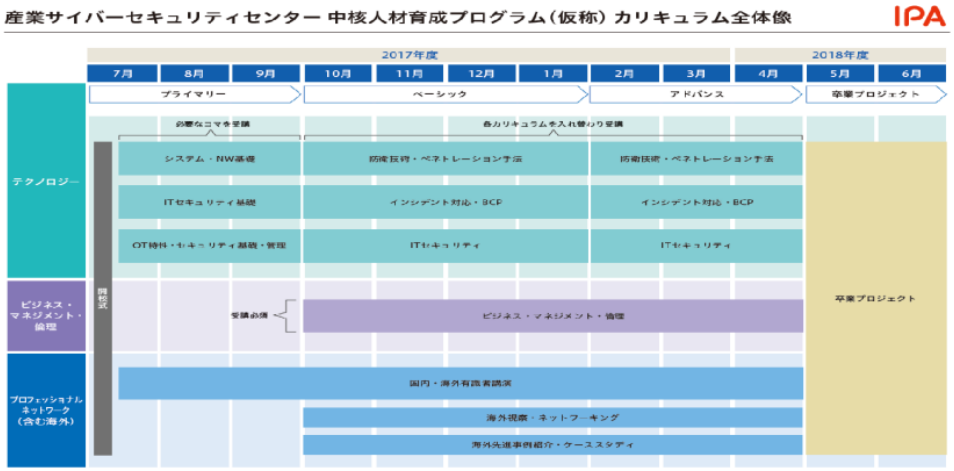
関連事業

セキュリティセンター（ISEC）

https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

産業サイバーセキュリティセンター（ICSCoE）

・人材育成事業
「中核人材育成プログラム」と「短期プログラム」を提供



「中核人材育成プログラム」
1年間のカリキュラム

https://www.ipa.go.jp/icscoe/activities/index.html