制御システム　セーフティ・セキュリティ実践

～制御システム セーフティ・セキュリティ要件検討ガイド～

IPA 社会基盤センター連携委員
東芝情報システム株式会社
エンベデッドシステム事業部
企画グループ 参事
細目 紀子

本日の内容

- 海外のセキュリティ事件と企業の生の声
- セーフティ・セキュリティ要件の不適合事例
- 本ガイドの対象プロセス
- 本ガイドの目的
- 「既存の制御システム」におけるセキュリティ検討プロセス
- ガイドの効果的な活用方法
- セーフティとセキュリティをくらべてみる
- 参考情報

重要インフラとは？

金融
緊急サービス
医療
民間
情報
食品・農業
ダム
化学
水道
防衛
輸送

DHS:
米国国土安全保障省が定義する16の重要なインフラセクター

http://www.dhs.gov/critical-infrastructure-sectors

政府施設
エネルギー
通信・放送
重要製造施設
原子力

**みなさんが
システム開発している
セクターもあるのでは？**

※日本では、内閣サイバーセキュリティセンターが
重要インフラ１３分野１８セプターを指定

海外のセキュリティ事件

重要インフラ設備へのサイバー攻撃！！

■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。

輸送

日本の法律では
電子計算機損壊等業務妨害罪
(刑法二三四条の二第一項)

■サウジアラビア空港、政府機関への攻撃（2016年1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。

政府施設

■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。

エネルギー

■フランス国営放送局へのサイバー攻撃（2015年4月）
イスラム過激派からの大規模攻撃受け番組放送ができなくなった。

通信・放送

■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。

重要製造施設

■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。

原子力

重要インフラをささえる企業の生の声

2015年後半からセーフティシステム関連の製造業中心にヒアリング実施

	セーフティ	セキュリティ
動向・要件	プロセスは確立している。しかし、IoT時代に向けた新たなサービスや機能への対応が必要（自動運転、生産系と事務系システム連携など）	セキュリティ脅威は日々増加、変化している。将来にわたる脅威の全体像を特定することは不可能。
規格	認証取得のためのもの。認証取得のためのスキームと一体。ドメイン毎。	組込みシステムはドメインごとに作成中。セーフティとの関係は無し
プロセス	ドメイン毎に確立されたプロセスを定義	モデルとなるようなプロセスは未定義
課題（国内企業17社、2大学よりヒアリング）	セキュリティ要件の抽出において、**脅威分析の具体的な方法**が規格に明示されていない。個人差が大きく、脅威抽出の網羅性に確信が持てない。	
	セーフティ要件に影響するセキュリティ要件を、**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！	
	セキュリティにはセーフティのように確立したプロセスがなく、双方の要件を満たす設計含む**開発プロセスの進め方**がわからない。	
	セーフティ、セキュリティの双方に詳しい技術者は極めて少ない。セキュリティ要件がセーフティに及ぼす影響を同時に**評価・すりあわせ**ることが難しく、連携させる枠組みなし	

S＆Sプロセスの課題が見えてきた！

セーフティ・セキュリティ要件の不整合事例

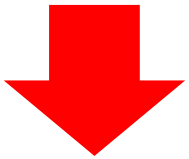
- ウィルスチェックソフトが安全保護システムの安全停止を妨害
  - 制御対象：ボイラー(石油)
  - 安全保護システム：SIL3　第3者認証を取得済
  - 事象：

    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）

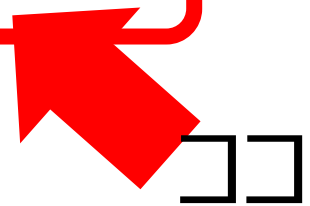
    →安全停止処理の稼働要求時に、
    安全停止処理が実行されなかった



セーフティ・セキュリティ要件に整合を取る必要あり

本ガイドの対象プロセス

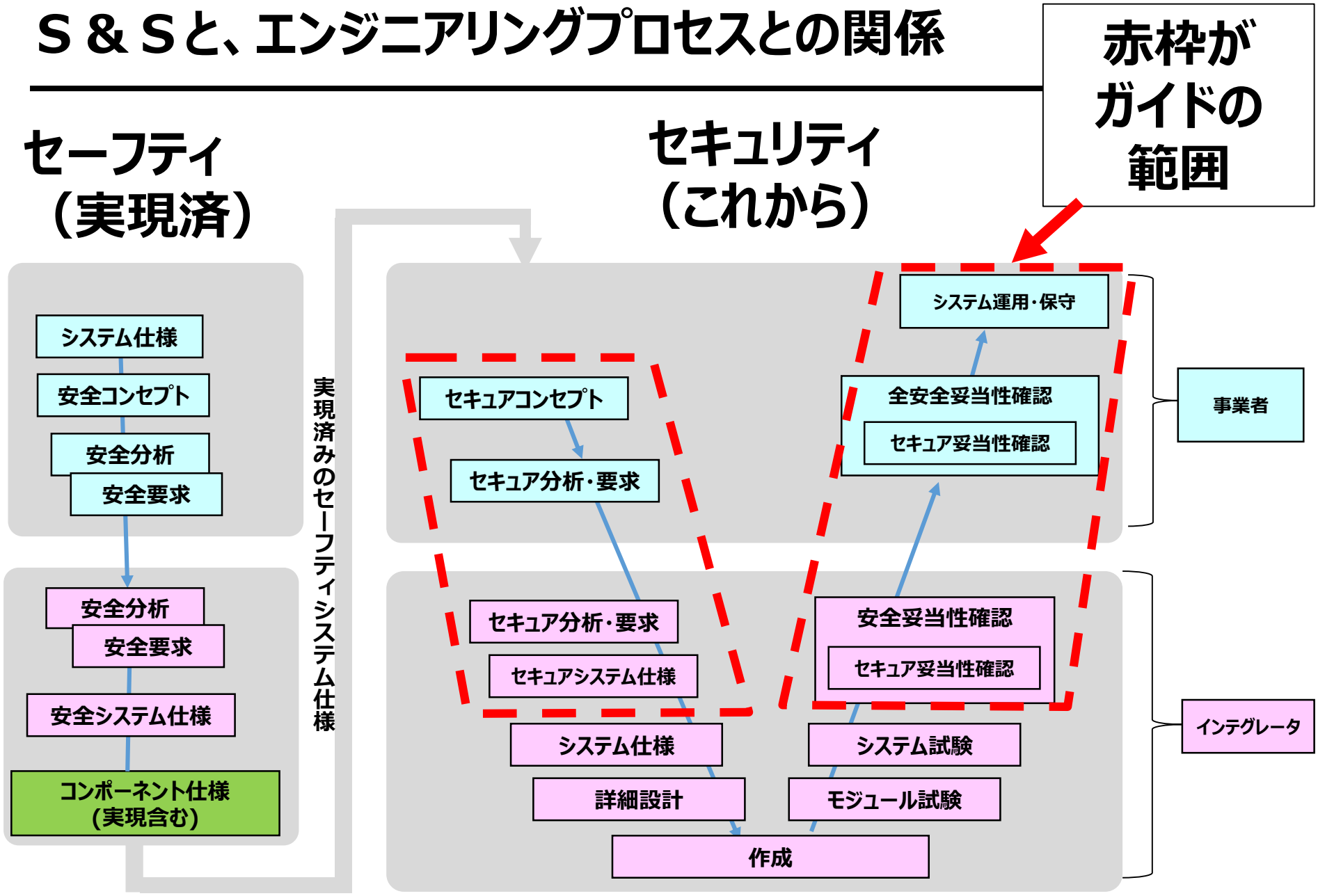
- **セーフティシステムに、セキュリティ要件を追加**



- セキュリティシステムに、セーフティ要件を追加

- 新規システムについて、
  セーフティとセキュリティ両要件の同時確立

S＆Sと、エンジニアリングプロセスとの関係



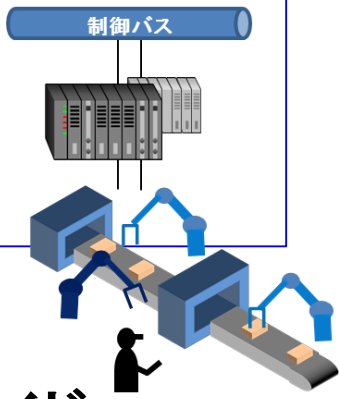
制御システム セーフティ・セキュリティ要件検討ガイドの目的

■ 機能安全等に準拠したセーフティシステムに対して、サイバーセキュリティ分析をどのように行えばよいのか？できるだけ**汎用的**に示したい。

■ セキュリティ要件をセーフティ要求・機能にどのようにすりあわせたらよいか？**基本的な考え方**を示す。

活動方針

✓**セーフティ・ファースト**：既設セーフティシステムが有。セーフティゴールありき
✓**想定読者**：セキュリティ対応が必要なセーフティ経験のあるインテグレータ
✓**国際規格・標準**：IEC 61508、IEC 62443
✓**モデルシステム**：FA（Factory Automation）システム
✓**アクター**：事業者、システムインテグレータ（＋機器メーカ）



成果

制御システムセーフティ・セキュリティ要件検討ガイド

ガイドの効果的な活用方法

まず、ガイドの基本編で、S&Sプロセスの概観をつかむ！

・目的
・基本的な考え方
をイメージする

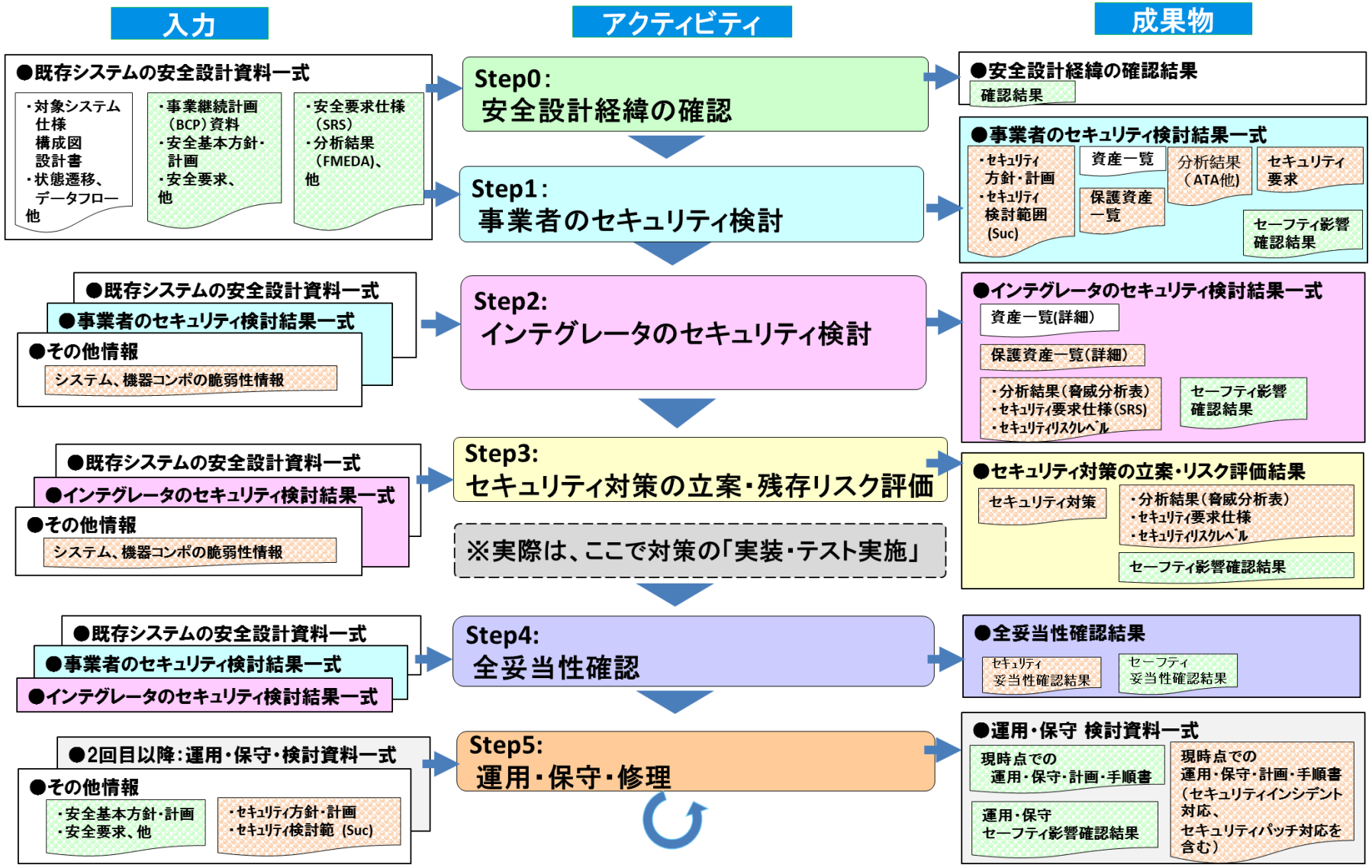
・プロセスの流れを
つかむ

・産業分野適用時
のポイントを参考に！

・疲れたら・・
コラムを読む！

セーフティ・セキュリティ検討の全体像

プロセスの流れをつかもう！



「既存の制御システム」におけるセキュリティ検討プロセス

Step0　安全設計経緯の確認

対象システムの
おさらい！

Step1　事業者のセキュリティ検討

事業者の
セキュリティ決意表明！

Step2　インテグレータのセキュリティ検討

脅威と脆弱性
はどこに？

Step3　セキュリティ対策の立案・残存リスク評価

※実際には、ここで対策の実装・テストが実施されます

現実的＆効果的
(確実、速い、できれば安い)
な対策を考えよう！

Step4　全妥当性確認

Step5　運用・保守・修理

セキュリティはナマモノ。時間とともに
脅威も脆弱性も変化します。

ガイドの効果的な活用方法

次に、ガイドのケーススタディ編で、演習してみる！

・**付録の分析シート**を使い、ガイドに沿って自ら記入してみましょう！

・ＦＡシステムの構成をイメージする

・分析してみる

・対策を考える

・セーフティを侵害していないか？再度確認

ガイドの紹介：セーフティへの影響を考える際の観点（例）

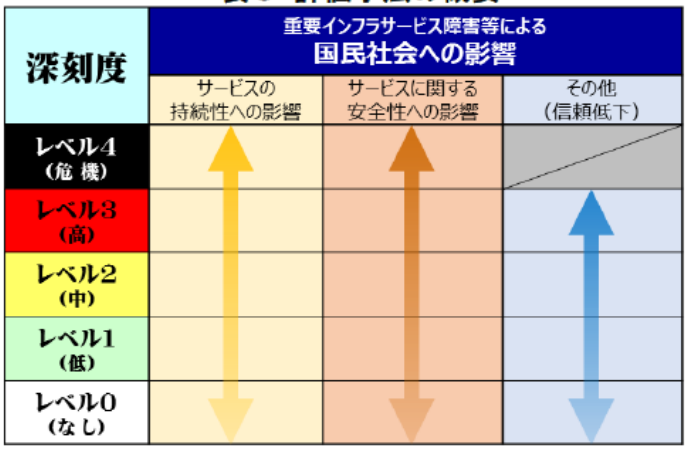
- ✓セキュリティリスクがシステムハザードを発生させることはないか
- ✓セキュリティ対策によって安全機能の性能に影響を与えることはないか
- ✓セキュリティ対策の実装が安全機能を無効化させることはないか
- ✓安全機能がセキュリティ対策をバイパスしていないか

参考：サイバー攻撃による重要インフラサービス障害等の深刻度評価基準（試案）について

表２　評価の観点及び評価指標

重要インフラサービス障害等による国民社会への影響	
評価の観点	**評価指標**
サービスの持続性への影響	提供支障（範囲・時間・代替性等）
	同時多発性
サービスに関する安全性への影響（施設・設備の安全性を含む）	人的・物的被害（人数・被害額等）
	住民避難等（範囲等）
	環境影響（原状回復費用・範囲等）
	同時多発性
その他	サービスに対する信頼低下

表３　評価手法の概要



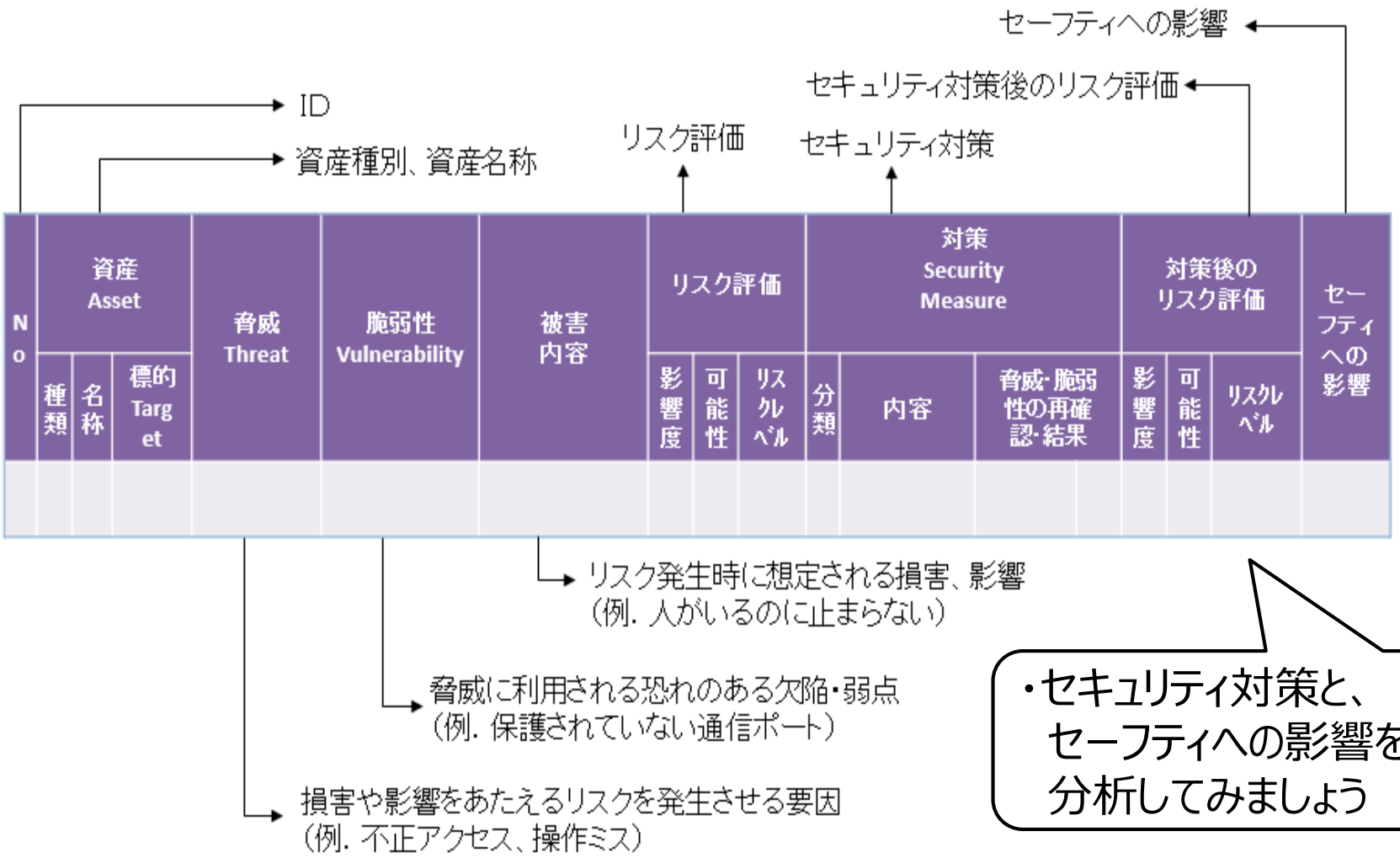
本ガイドのケーススタディ編では、セーフティへの影響度の視点で、リスク評価を行っています。

しかし、対象システムによっては、左記のように、明確に、サービスの持続性等と組合わせて影響度をはかるケースもあります。

分析シートは適宜工夫して使って下さい。

引用：サイバー攻撃による重要インフラサービス障害等の深刻度評価基準（試案）について 2018年4月11日　NISC　HPから
http://www.nisc.go.jp/active/infra/pdf/pubcom_shinkokudo1.pdf

脅威分析シート



セーフティとセキュリティをくらべてみる

No.	項目	セーフティ （機能安全）	サイバー セキュリティ
0	ユーザの期待	許容できる安全性	いつでもセキュア
1	対象範囲は？	潜在的な危険 (ハザード)	潜在的な脅威 （スレート）
2	分析は？	安全分析 （ハザード&リスク分析）	脅威分析
3	技術課題は？	安全性	脆弱性
4	確認方法は？	故障注入テスト	ペネトレーションテスト（侵入テスト） 脆弱性テスト
5	システム・製品 ライフサイクル	計画・企画・開発・生産 運用・廃棄	計画・企画・開発・生産 運用・廃棄 ※出荷後の監視・対策 ※インシデントレスポンス 時間の経過とともに、リスクレベルは変化！ ・脆弱性が拡散、 ・攻撃者が変化（動機・スキル）

参考情報： 国際規格、ガイドライン等

	ドメイン	安全規格	セキュリティ規格	参考資料（ガイドライン等）
0	--	IEC 61508	IEC 62443 ISO/IEC 27001(ISMS) ISO/IEC 15408(CC)	経済産業省 セキュリティ関連コンテンツ一覧 http://www.meti.go.jp/policy/netsecurity/secdoc/secdoc_list.html 国土交通省 重要インフラにおける情報セキュリティ確保に係るガイドライン http://www.mlit.go.jp/sogoseisaku/jouhouka/sosei_jouhouka9999.html IPA 制御システムのセキュリティリスク分析ガイド https://www.ipa.go.jp/security/controlsystem/riskana 推奨 New！ つながる世界の開発指針（第2版） https://www.ipa.go.jp/sec/reports/20170630.html
1	自動車	ISO 26262	SAE J3061 ISO/SAE 21434＊ 策定中 ISO/TC22にて策定中！	CCDS製品分野別セキュリティガイドライン 車載器編 https://www.ccds.or.jp/public_document/index.html
2	電力	電気事業法		電力制御システムセキュリティガイドライン https://www.denki.or.jp/wp-content/uploads/2016/07/d20160707.pdf 監視制御用計算機システムにおけるセキュリティ対策のガイドライン（追補1） https://www.jema-net.or.jp/cgi-bin/user/summary.cgi?jem=1158
3	施設監視制御	ISO 16484 (BACS)		IoTセキュリティ総合対策 - 総務省 サイバーセキュリティタスクフォース http://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/index.html http://www.soumu.go.jp/main_content/000510701.pdf
4	鉄道	IEC 62278(RAMS)	IEC 62280	鉄道分野における情報セキュリティ確保に係る安全ガイドライン 第3版 http://www.mlit.go.jp/sogoseisaku/jouhouka/sosei_jouhouka9999.html
5	医療・ ヘルスケア	IEC 60601 IEC 62304 IEC 82304 ISO 14971	IEC 62304 AnnexC IEC 80001 IEC 27002 ISO/IEC 27799	医療機器における情報セキュリティに関する調査 https://www.ipa.go.jp/security/fy25/reports/medi_sec/ 医療情報システムの安全管理に関するガイドライン第5版 w 医療・ヘルスケア用にリバイス！ https://www.good-hs.jp/guidelines.html
6	産業機械	IEC 62061 ISO 12100 ISO 13849-1	IEC 62443 IEC TR 63069＊ 策定中 IEC TR 63074＊ 策定中	制御システムセキュリティ運用ガイドライン http://www.neca.or.jp/wpcontent/uploads/control_system_security_guideline.pdf

ガイドブック紹介のまとめ

詳しくは
展示ブースで！

- 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。

（PPTイメージですので、そのまま使えます！）

・PDFダウンロード無料！
・自社で印刷すれば
購入の必要なし！

ご清聴、ありがとうございました！