ISO/SAE 21434リユース分析(6.4.4)と プロセステーラリング(6.4.3)ガイドライン

アイテムまたはコンポーネントのサイバーセキュリティリスク管理の要求は、コンセプトから廃棄までのライフサイクル全体で規定されています。これらの要求を実現するためのアクティビティは、リユース分析の結果に基づいたプロセステーラリングが可能です。ただし以下に基づいて論理的根拠を示す必要があります。

リユース分析が必要なケース

- リユースする開発済みアイテムまたはコンポーネントへの変更が予定されている（変更には設計の変更、実装の変更を含む。またキャリブレーションデータ、コンフィグレーションデータもサイバーセキュリティ機能に影響を与えるものは考慮する。）
- 別の使用環境でリユースされる
- 既知の攻撃や脆弱性の変更、アセットの変更、アイテムやコンポーネントに関する情報の変更

リユース分析の実施

リユースするアイテムとコンポーネントに対して、以下を実施します。

- 変更の特定：
  アイテム、コンポーネントの変更、環境の変更など
- 変更の影響を分析:
  サイバーセキュリティに関わるか、サイバーセキュリティクレームおよび先に適用した想定への影響
- 影響する、または、不足している作業成果物の特定（既存の脅威分析とリスク評価）
- サイバーセキュリティ活動（プロセステーラリング）の定義：
  サイバーセキュリティプラン

  リユース分析で変更の影響を受けるものの例：
  - » サイバーセキュリティ要求
  - » 設計と実装
  - » 運用環境と運用モード
  - » メンテナンス
  - » サイバーセキュリティ管理
  - » 既知の攻撃に対する感受性と既知の脆弱性の暴露
  - » アセット（電子ID、データ/コード、ファームウェア、アプリケーション、暗号化キーなど）

既存コンポーネントの場合は、以下の追加対応が必要です。

- 割り当てられたサイバーセキュリティ要求に準拠できるかの評価
- アイテム統合するために既存の文書が十分かどうかの評価

注）本テンプレートは、現時点で有効と思われる内容をまとめたものです。将来に渡って有効性が保証されるものではありません。

TÜVRheinland®
Precisely Right.

対象
アセット：サイバーセキュリティ侵害がアイテムの利害関係者に損害を与える可能性のあるもの

変更（MODIFICATION）の種類
- 設計の変更：仕様の変更、データの変更
- 実装の変更
- 使用環境の変更

1 変更の要約

2 変更内容
以下を明確にする
- 変更の種類
- サイバーセキュリティ特性（CIA）とその影響度
- アタックパスとその実現可能性

3 変更による影響
インパクト評価とアタック実現性評価よりリスク値を使用

安全性（ASILレベル）のリスク値の例

機能安全脅威	アタック実行可能性			
	極低	低	中	高
QM	1	1	1	2
ASIL A	1	1	2	3
ASIL B	1	2	3	4
ASIL C	2	3	4	5
ASIL D	3	4	5	5

財務、運用、プライバシーのリスク値の例

影響度合	アタック実行可能性			
	極低	低	中	高
無視できる	1	1	1	1
中程度	1	1	2	3
かなりある	1	2	3	4
非常にある	2	3	4	5

インパクト評価

安全	非常に重大	ASIL Dに相当。生命にかわる傷害（安否不明）や致命的な傷害をもたらす。
	重大	ASIL Cに相当。重傷および生命を脅かす障害（生存もしくは生存の可能性は高い）。
	中程度	ASIL Bに相当。軽傷および中程度の障害をもたらす。
	無視できる	ASIL Aに相当。傷害をもたらさない。
財務	非常に重大	利害関係者が克服できないほどの最悪の事態をもたらす。
	重大	利害関係者が克服できる程度の重大な事態をもたらす。
	中程度	利害関係者が限られたリソースで克服できる程度の不便を強いられる事態をもたらす。
	無視できる	利害関係者は、無視できる程度の影響か無関係である。
運用	非常に重大	車両の意図しない操作から車両が操作不能になるまでの、車両が動作しなくる事態をもたらす。
	重大	車両に搭載された機能の損失をもたらす。
	中程度	車両の機能や性能の部分的な低下をもたらす。
	無視できる	車両の機能や性能の気づかない程度の低下をもたらす。
プライバシー	非常に重大	道路使用者に重大または不可逆的な影響をもたらす。
	重大	道路使用者に深刻な影響をもたらす。
	中程度	道路使用者に多大な不便をもたらす。
	無視できる	道路使用者に影響をもたらさないか、多少の不便をもたらす。

アタック実現性の評価

		アタックベクターベース	例
高	最小限の労力で高度に実現可能：攻撃パスを達成するのは簡単、または、ほぼ確実	ネットワークから	セルラー
中	中程度な努力がいるが実現可能：攻撃パスを達成することは実行可能で珍しいことではない	隣接から	Bluetooth
低	かなりの努力がいるが実現可能：攻撃パスの達成は実現可能	ローカルから	メモリーカード
極低	合理的努力では実行不可能：攻撃パスを達成することは困難かほとんど不可能	物理的なアクセス	

4 影響する作業成果物の特定

成果物リスト		
リスクアセスメント手法	▪ ダメージシナリオ ▪ 識別された資産とサイバーセキュリティ特性 ▪ 脅威シナリオ ▪ ダメージシナリオに関連する影響カテゴリ別の影響評価	▪ 識別された攻撃パス ▪ 攻撃の実現可能性評価 ▪ リスク値 ▪ 脅威シナリオごとのリスク処理の決定
コンセプトフェーズ	▪ アイテム定義 ▪ 脅威分析とリスク評価 (TARA) ▪ リスク対応の決定 ▪ サイバーセキュリティ目標	▪ サイバーセキュリティクレーム ▪ 検証レポート ▪ サイバーセキュリティコンセプト ▪ サイバーセキュリティコンセプト検証報告書
製品開発フェーズ	▪ サイバーセキュリティ仕様 ▪ 開発後のサイバーセキュリティ要件 ▪ サイバーセキュリティ仕様の検証レポート ▪ 脆弱性分析レポート ▪ 統合と検証の仕様 ▪ 統合と検証報告書	▪ モデリング、設計、またはプログラミング言語とコーディングガイドライン ▪ ソフトウェアユニット設計とソフトウェアユニット実装 ▪ 妥当性確認仕様 ▪ 妥当性確認報告書

5 リスク値によるプロセステーラリング

リスク値

5	新規開発に準ずる
4	いくつかのステップ (例：アイテム定義からダメージシナリオ) を省略可能
3	リスク対応策の検討と実装　および統合テストと妥当性確認
2	統合テストの実施
1	アクション不要

6 テーラリング　CS計画への反映

下記の該当箇所にチェック (省略または統合する開発ステップにチェック)

アイテム定義	アセット定義	ダメージシナリオ	脅威シナリオ	影響評価	アタックパス分析	アタック実現性評価	リスク値の決定

リスク対応策	サイバーセキュリティ目標	サイバーセキュリティクレーム	サイバーセキュリティ目標とクレームの検証	脆弱性評価	統合とテスト	妥当性確認

リユース分析とテーラリング

管理番号															
関連文書															
対象アセット															
1	変更の要約														
2	変更の内容														
	設計の変更 *CS:サイバーセキュリティ	☐ CS機能	☐ CS性能	☐ CSデータ	☐ コスト	☐ 新たな脅威	☐ 新たな脆弱性	☐ その他							
	実装の変更	☐ ソフト修正	☐ ハード変更	☐ 開発ツール変更	☐ ガイドライン変更	☐ 製造方法変更	☐サプライヤー変更	☐ その他							
	使用環境の変更														
3	変更の影響														
	リスク値	インパクト評価				アタック実現性評価									
4	影響する作業成果物														
5	影響範囲の分析														
	省略または統合するプロセスの選定およびその論拠 *CS:サイバーセキュリティ	アイテム定義	アセット定義	ダメージシナリオ	脅威シナリオ	影響評価	アタックパス分析	アタック実現性評価	リスク値の決定	リスク対応策	CS目標	CSクレーム	CS目標とクレームの検証	脆弱性評価	統合とテスト	妥当性確認
6	テーラリング可否（省略または統合するステップに記述） *CS:サイバーセキュリティ	アイテム定義	アセット定義	ダメージシナリオ	脅威シナリオ	影響評価	アタックパス分析	アタック実現性評価	リスク値の決定	リスク対応策	CS目標	CSクレーム	CS目標とクレームの検証	脆弱性評価	統合とテスト	妥当性確認

責任	署名	日付
作成		
確認		
承認		

テュフ ラインランド ジャパン株式会社
カスタマーサービス
info@jpn.tuv.com
東日本地域Tel: 045-470-1850
西日本地域Tel: 06-6355-5400

横浜市港北区新横浜 3-19-5
新横浜第二センタービル
Tel. 045-470-1860 Fax 045-473-5221

www.tuv.com

TÜVRheinland®
Precisely Right.