



Attack tree+を用いた セキュリティ評価の サンプル&評価キット のご案内

ISO/SAE 21434 Anex Gを例題として

AttackTree+の主な機能一覧

Threat Analysis

対応するマトリックス

- HEAVENS
- EVITA
- ISO26262
- ユーザカスタム

Attack Tree

考え方はFaulttreeに似ている

- カットセット分析を行う
- 重要度を計算する

入力例

f: Frequency 例: 10-12[1/h]

P: Probability 例: 0.02 (=1回/50回)

Mitigation Tree

- 対策を講じた後の内訳を評価する
- リスクが大きい時は見直しが必要

21434の評価項目とAttack tree+の対応

脅威 → インパクト評価 → アタックパス → 可能性評価 → リスク評価 → 対策

リスク評価

ID	Desc	Damage scenario No	Saf rela	Consequence IDs	Impact Description	Threat Scenario No. and Description	Assign likelihood using indicator	Indicator values	Attack Path/ of Attack	Frequ source objec	Frequ source objec type	Fre	Lik	C	Seris lev	Firis lev	Op ris lev	Pr an Le
9	Body Con...	侵害されたナビゲーションECUによる悪意制御信号送信	D.01: 夜間の運転中に、CAN信号の完全性が失われた結果、意図しないヘッドランプ消灯発生	Y	S-Major, F-Severe, O-Moderate, P-Negligible	S:街路樹への衝突は致命傷をもたらす。	T.01: 信号のなりすましは、電源スイッチアクチュエータECUの「ランプリクエスト」信号のCANメッセージの整合性の損失につながり、CAN信号の整合性の損失が原因で、夜間の運転中に意図しないヘッドランプがオフになる可能性があります。	EXPERTISE=3 KNOWLEDGE EQUIPMENT=C OPPORTUNIT ELAPSED=1	APx.2 侵害されたナビゲーションECUが悪意のある制御信号を送信	APx.1	Gate	0		R	M	H	L	Q
10	Body Con...	ゲートウェイECUが悪意信号を送信	D.01: 夜間の運転中に、CAN信号の完全性が失われた結果、意図しないヘッドランプ消灯発生	Y	S-Major, F-Severe, O-Moderate, P-Negligible	S:街路樹への衝突は致命傷をもたらす。	T.01: 信号のなりすましは、電源スイッチアクチュエータECUの「ランプリクエスト」信号のCANメッセージの整合性の損失につながり、CAN信号の整合性の損失が原因で、夜間の運転中に意図しないヘッドランプがオフになる可能性があります。	EXPERTISE=3 KNOWLEDGE EQUIPMENT=C OPPORTUNIT ELAPSED=1	APx.3 ゲートウェイECUが悪意のある信号を電源スイッチアクチュエータへ転送	APx.1	Gate	0		R	M	H	L	Q
11	Body Con...	悪意信号によるランプスイッチ偽装	D.01: 夜間の運転中に、CAN信号の完全性が失われた結果、意図しないヘッドランプ消灯発生	Y	S-Major, F-Severe, O-Moderate, P-Negligible	S:街路樹への衝突は致命傷をもたらす。	T.01: 信号のなりすましは、電源スイッチアクチュエータECUの「ランプリクエスト」信号のCANメッセージの整合性の損失につながり、CAN信号の整合性の損失が原因で、夜間の運転中に意図しないヘッドランプがオフになる可能性があります。	EXPERTISE=3 KNOWLEDGE EQUIPMENT=C OPPORTUNIT ELAPSED=1	APx.4 悪意のある信号は、要求に応じてランプスイッチを偽装	APx.1	Gate	0		R	M	H	L	Q

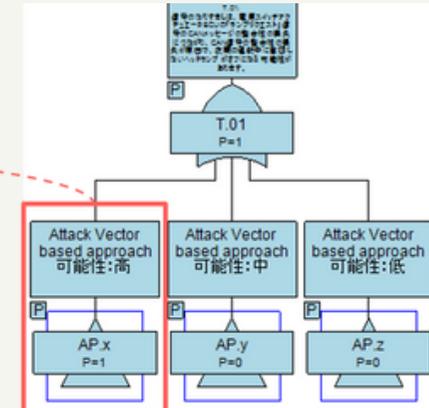
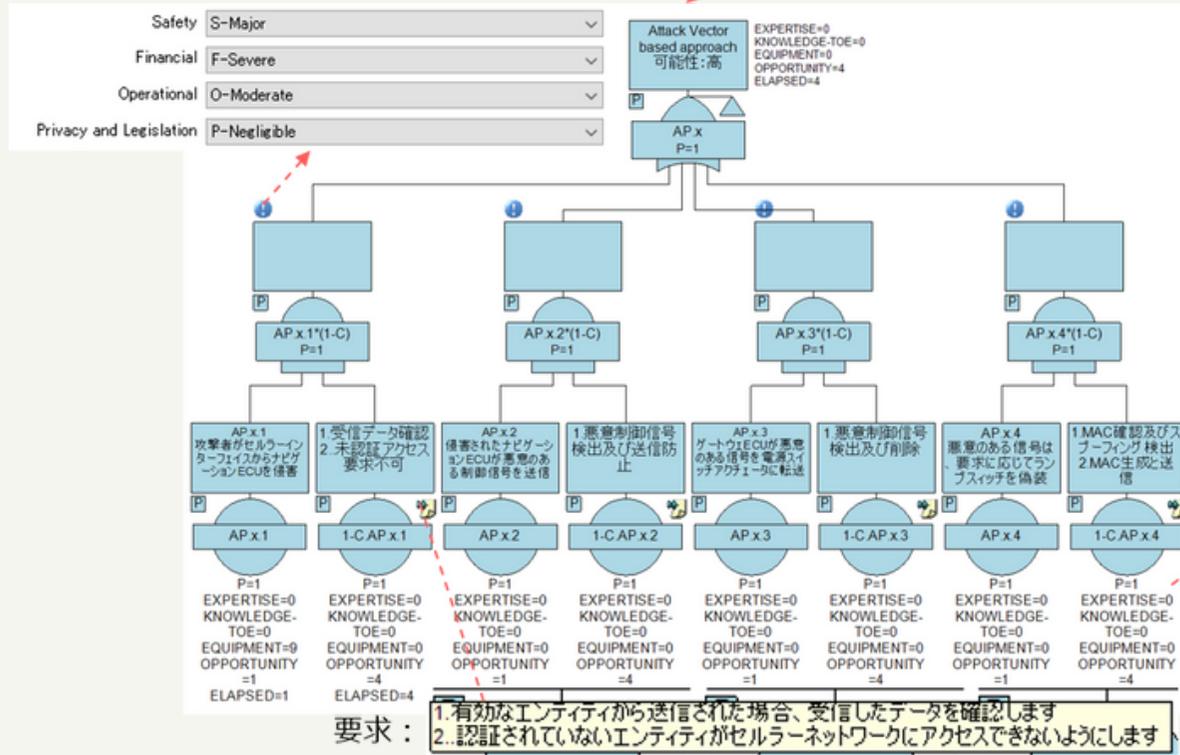
脅威を定義

インパクト

21434の評価項目とAttack tree+の対応

脅威 → インパクト評価 → アタックパス → 可能性評価 → リスク評価 → 対策

インパクト(SFOP)の評価



実現可能性(feasibility)評価

EXPERTISE: 0 LAYMAN

KNOWLEDGE-TOE: 0 PUBLIC

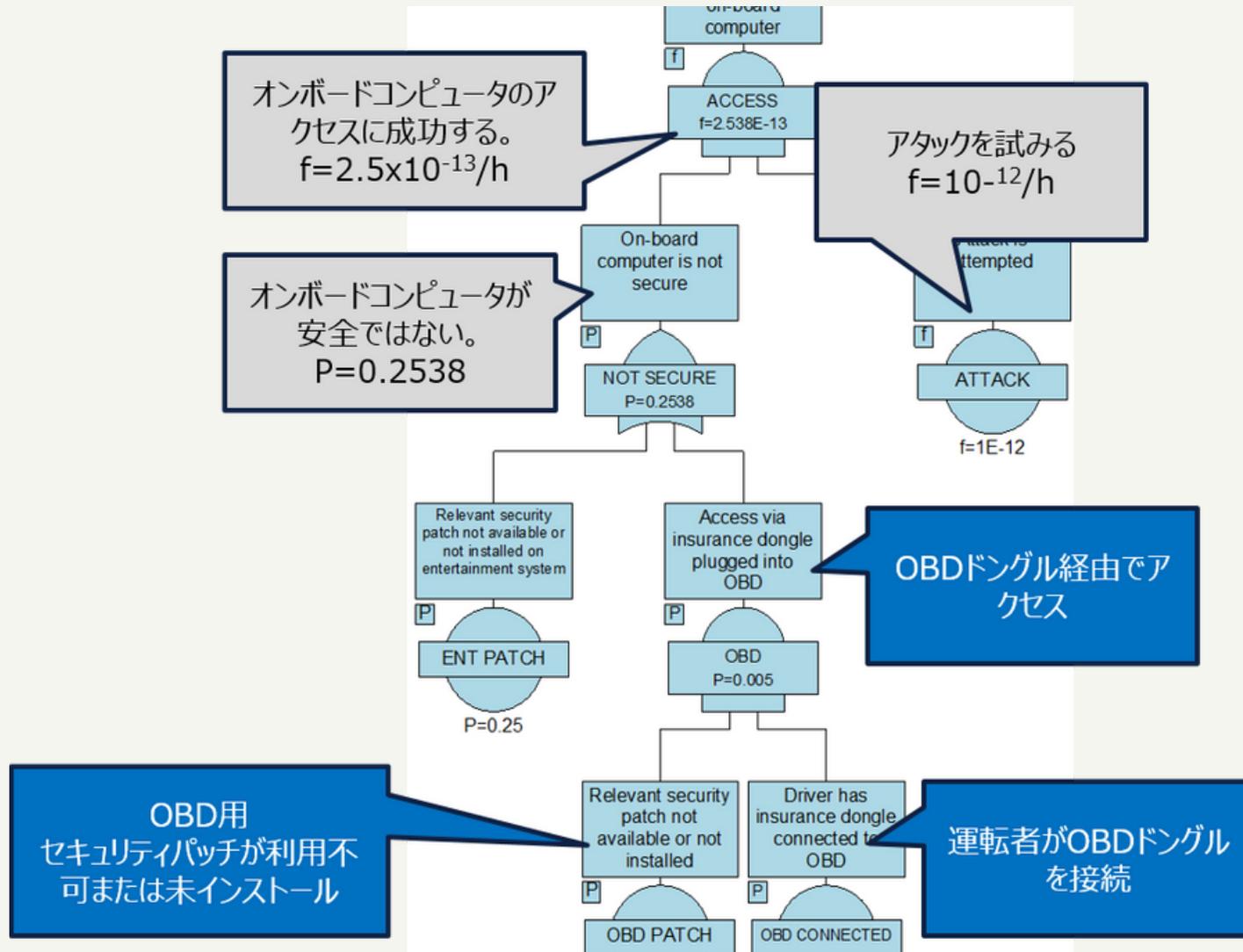
EQUIPMENT: 0 STANDARD

OPPORTUNITY: 1 EASY

ELAPSED: 1 1M

21434の評価項目とAttack tree+の対応

脅威 → インパクト評価 → **アタックパス** → 可能性評価 → リスク評価 → 対策



21434の評価項目とAttack tree+の対応

脅威 → インパクト評価 → アタックパス → 可能性評価 → リスク評価 → 対策

対応マトリクス

- HEAVENS
- EVITA
- ISO26262
- カスタム

		Consequence - Safety			
Likelihood		S-NONIMPACT	S-LOW	S-MEDIUM	S-HIGH
NONE	QM	QM	QM	QM	QM
LOW	QM	LOW	LOW	MEDIUM	MEDIUM
MEDIUM	QM	LOW	MEDIUM	HIGH	HIGH
HIGH	QM	MEDIUM	HIGH	HIGH	HIGH
CRITICAL	QM	HIGH	HIGH	CRITICAL	CRITICAL

Typical Risk Matrix Setup

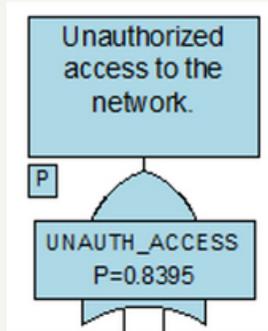
Asset description	Description	Likelihood	Controllability	Safety consequence	Safety risk level
Internal vehicle network	Bogus information sent to VNET	MEDIUM	TIMING	S-MEDIUM	MEDIUM
Automated functions i.e auto pilot / ...	Bogus information sent to VNET	MEDIUM	TIMING	S-MEDIUM	MEDIUM
Automated City / Low speed breaki...	Collision detection system disabled / malfunctioned	LOW	FIREWALL	S-HIGH	MEDIUM
Internal vehicle network	DDOS Attack on Vehicle Network	CRITICAL	PACKET	S-LOW	HIGH
Vehicle cameras	Cameras disabled by internal malicious user	LOW		S-LOW	LOW
Automated functions i.e auto pilot / ...	Malware sent to network to disable automated fu...	HIGH	FIREWALL	S-MEDIUM	HIGH
Lane Detection	Malware sent to network to disable automated fu...	HIGH	FIREWALL	S-HIGH	HIGH
Internal vehicle network	Man in the middle attack on network	HIGH	FIREWALL	S-LOW	MEDIUM
Automated City / Low speed breaki...	Control override system	NONE	FIREWALL	S-MEDIUM	QM
Lane Detection	Lane parameters modified or non-existent, vehicle...	LOW		S-HIGH	MEDIUM
Lane Detection	Lane detection system tampered with	LOW		S-HIGH	MEDIUM
Vehicle cameras	Cameras disabled by wireless attack	LOW	FIREWALL	S-MEDIUM	LOW

アイテム

確率 (Attack treeと連携可)

21434の評価項目とAttack tree+の対応

脅威 → インパクト評価 → アタックパス → 可能性評価 → リスク評価 → 対策



Unauthorized access to the network 不正アクセス	Account Privileges ユーザ権限	Data Encryption データ暗号化	Encryption Strength 暗号化強度	PR Mitigation 案内・通知	Consequence 影響	Probability 可能性
Unauthorized access to the network. P=0.8395	User accounts do not have administrative privileges. P=0.6451	Sensitive Data encrypted P=0.9985	Data encryption is not of a high standard and is broken P=0.475	Strong press release. Reassures customers P=0.6251	Minor damage to reputation Some data loss gathered from compromised user account	0.1605
				Press release fails to reassure customers P=0.3749	Reputation drastically damaged Some data loss gathered from compromised user account	0.09629
		Sensitive data stored as plain text P=0.0015	Data is encrypted using a high standard of complexity and is not broken P=0.525	Strong press release. Reassures customers P=0.6251	Minor damage to reputation	0.1774
				Press release fails to reassure customers P=0.3749	Reputation drastically damaged	0.1064
		Sensitive Data encrypted P=0.9985	Data encryption is not of a high standard and is broken P=1	Strong press release. Reassures customers P=0.6251	Minor damage to reputation Some data loss gathered from compromised user account	0.0005420
				Press release fails to reassure customers P=0.3749	Reputation drastically damaged Some data loss gathered from compromised user account	0.0003255
	Regular user accounts have Administration privileges. P=0.3549	Sensitive Data encrypted P=0.9985	Data encryption is not of a high standard and is broken P=0.475	Strong press release. Reassures customers P=0.6251	Minor damage to reputation	0.08832
				Press release fails to reassure customers P=0.3749	Reputation drastically damaged Full unrestricted access	0.05297
		Sensitive data stored as plain text P=0.0015	Data is encrypted using a high standard of complexity and is not broken P=0.525	Strong press release. Reassures customers P=0.6251	Minor damage to reputation	0.09762
				Press release fails to reassure customers P=0.3749	Reputation drastically damaged	0.05855
		Sensitive Data encrypted P=0.9985	Data encryption is not of a high standard and is broken P=1	Strong press release. Reassures customers P=0.6251	Minor damage to reputation Full unrestricted access	0.0002986
				Press release fails to reassure customers P=0.3749	Reputation drastically damaged Full unrestricted access	0.0001791

Attack tree+のデモ版と一緒に 評価キットも提供いたします

本資料は株式会社ウェーブフロントが Attack Tree+をご賛助のお客様向けに作成したものです。当社の許可なく、掲載内容を複製、転載、第三者の利用に供することを禁止します。

サイバーセキュリティ評価分析支援ツール

Attack Tree+

ISO/SAE 21434 Annex G

を題材としたサンプルプロジェクトファイル参照のための
初期設定および操作説明

2020.07.29

株式会社 ウェーブフロント

目次

1	はじめに	1
1.1	初期設定や起動に関する説明	1
1.1.1	詳細用 Attack Tree+実行プログラムの置き換え(Eveの置き換え)	1
1.1.2	プロジェクトファイルやグリッド調整のための設定ファイルの配置	2
1.1.3	「Attack Tree+」の起動	3
1.1.4	グリッドの調整	4
1.1.5	「Attack Tree+」の終了	7
2	サンプルプロジェクトの説明	8
2.1	プロジェクトファイルの読み込み	8
2.2	表示内容の確認	9
2.3	ヘルプの利用方法	12
2.4	Threat analysis モジュール	14
2.4.1	変更構成継ぎ	15
2.4.2	プロジェクトツリー	15
2.4.3	リスクマトリクス	16
2.4.4	アセット一覧	18
2.4.5	脅威分析(Threat 一覧)	21
2.5	Attack tree モジュール	24
2.5.1	概要説明	24
2.5.2	Attack tree モジュールの表示	25
2.5.3	変更構成継ぎ	26
2.5.4	Attack tree 機能の調整	27
2.5.4.1	Attack tree の全体表示	27
2.5.4.2	拡大縮小	28
2.5.4.3	ページ移動	28
2.5.4.4	全ページ表示	30
2.5.4.5	Impact 設定	31
2.5.4.6	Feasibility(アタックの可能性)または Frequency の設定	32
2.5.5	カットセット分析	33
2.5.5.1	カットセット分析の実行	34
2.5.5.2	シミュレーションのカットセットの参照	34
3	最後に	38

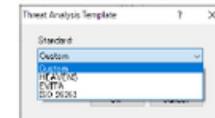
1

プロジェクトツリーは、アーキテクチャーやアセット以外に Impact に関するコードや Feasibility に関するコードを管理しています。各コードは、マスタデータでありテーブルで用意されますが、プロジェクトツリーにも表示されます。下記にプロジェクトツリーを示します。



2.4.3 リスクマトリクス

「Attack Tree+」の「Threat analysis」モジュールでは、リスクマトリクスを設定することができます。事前に準備されたものとして以下が存在します。



16

配布内容、及びご連絡先

配布物一覧

- Attack tree+デモ版
- 21434の評価サンプル
- Attack tree+の評価キット

ご連絡先

株式会社ウェーブフロント
メール：sales@wavefront.co.jp
電話：045-682-7070