IoTデバイスセキュリティ

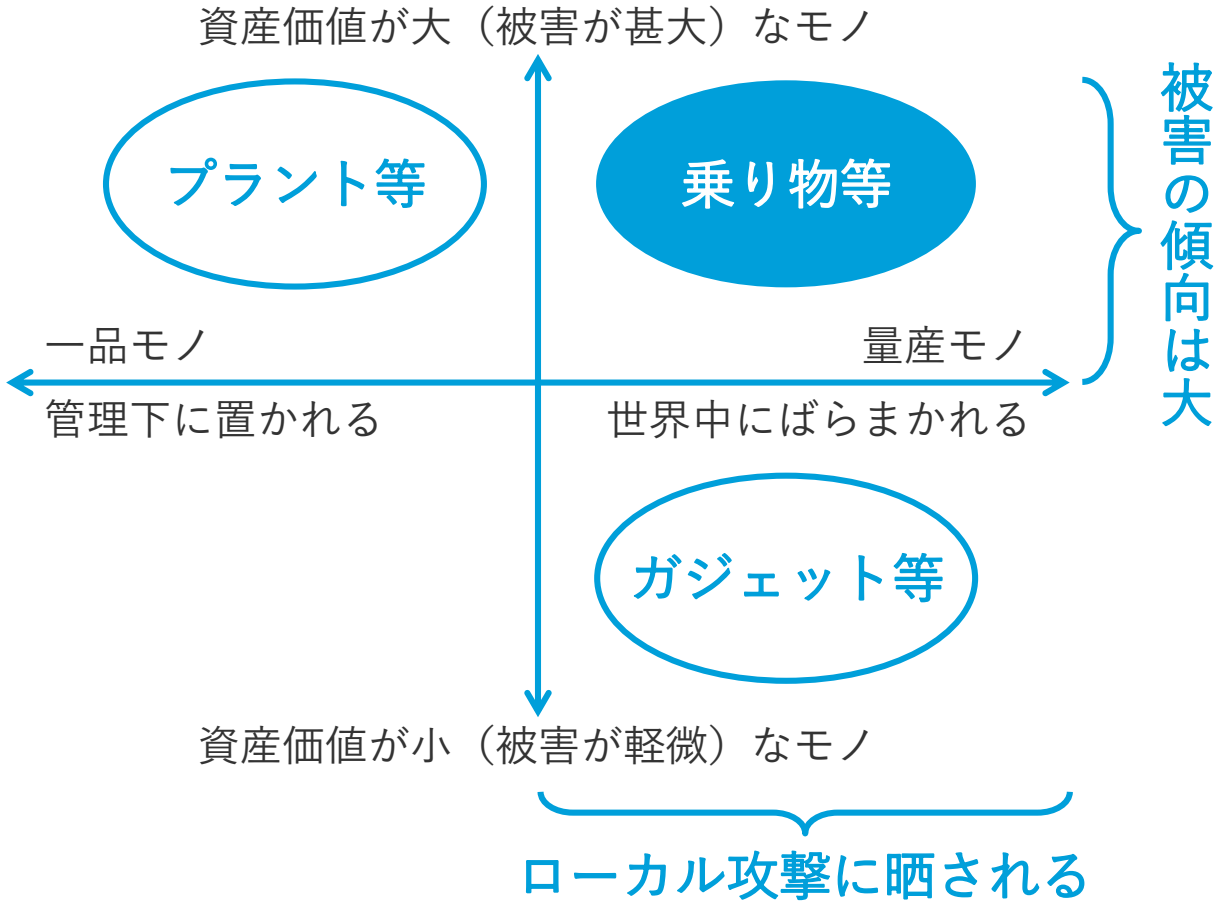
DNV GL ビジネス・アシュアランス・ジャパン株式会社 松並　勝

私の立ち位置：自動車セキュリティのトレーニング、アドバイザリ業務に従事

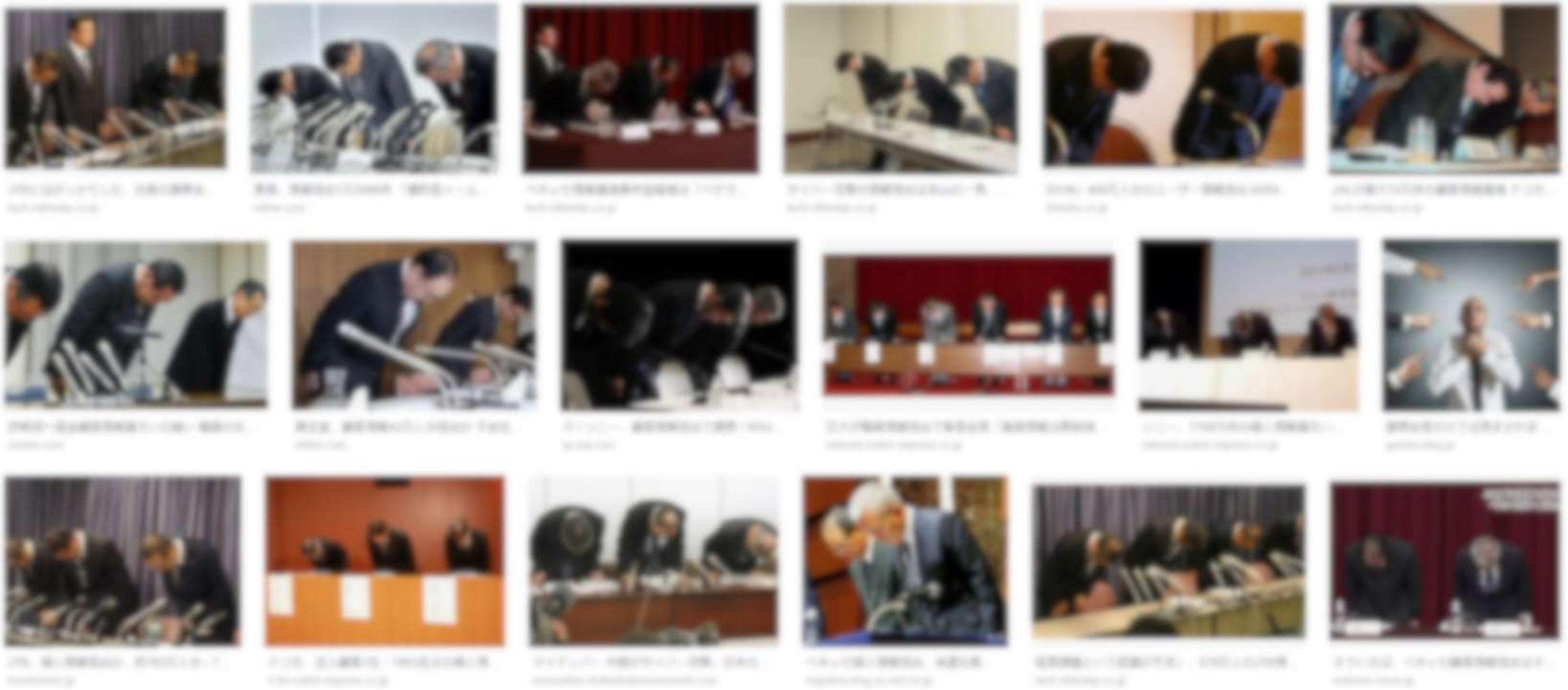
- 自動車というIoTジャンル
  - 人命を扱うので被害が大きくなりがち
  - ローカル攻撃（解析、改造）されがち
    - 例：ECUチューニング、イモビカッター、など検索するといろいろ

- 以降は、このような立場から見えるIoTデバイスセキュリティの話
  - 信頼の起点（root of trust）がとっても大切

- IoTいろいろ



完璧なセキュリティなどこの世にありません ➡ 謝罪会見・裁判 ➡ **説明責任** が求められる



DNV·GL

Cybersecurity法制化の流れ ➡ より 説明責任 が求められる

- カリフォルニア州 IoT分野のCybersecurity法案

Senate Bill No. 327

CHAPTER 886

An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.

[Approved by Governor September 28, 2018. Filed with Secretary of State September 28, 2018.]

その機器に**合理的**なセキュリティ機能 … を備えよ

TITLE 1.81.26. Security of Connected Devices

1798.91.04. (a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:

(1) Appropriate to the nature and function of the device.

(2) Appropriate to the information it may collect, contain, or transmit.

(3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

- 国連 WP.29 自動車分野のCybersecurity法案

Annex A Draft proposal to introduce a Regulation on Cyber Security

United Nations ECE/TRANS/WP.29/201x/xx

Economic and Social Council

Distr.: General
DD MM YYYY

Original: English

セキュリティが十分適切に考慮されたことを**説明(論証)**せよ

7.2.2.2. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered. This shall include:

a) The processes used within the manufacturer's organization to manage cyber security;
b) The processes used for the identification of risks to vehicle types;
c) The processes used for the assessment, categorization and treatment of the risks identified;
d) The processes in place to verify that the risks identified are appropriately managed;

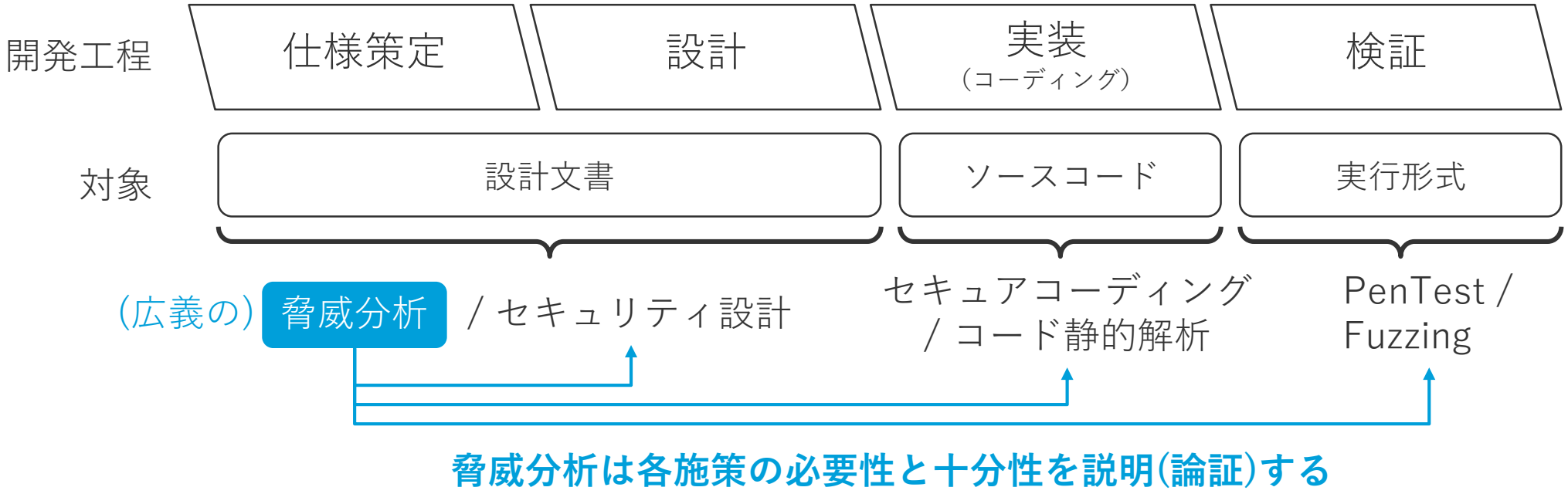
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
https://www.unece.org/trans/main/wp29/wp29wgs/wp29grva/grvainf2018.html

説明責任

論証

セキュリティが十分適切に考慮されたことを説明(論証)する → 脅威分析が必要

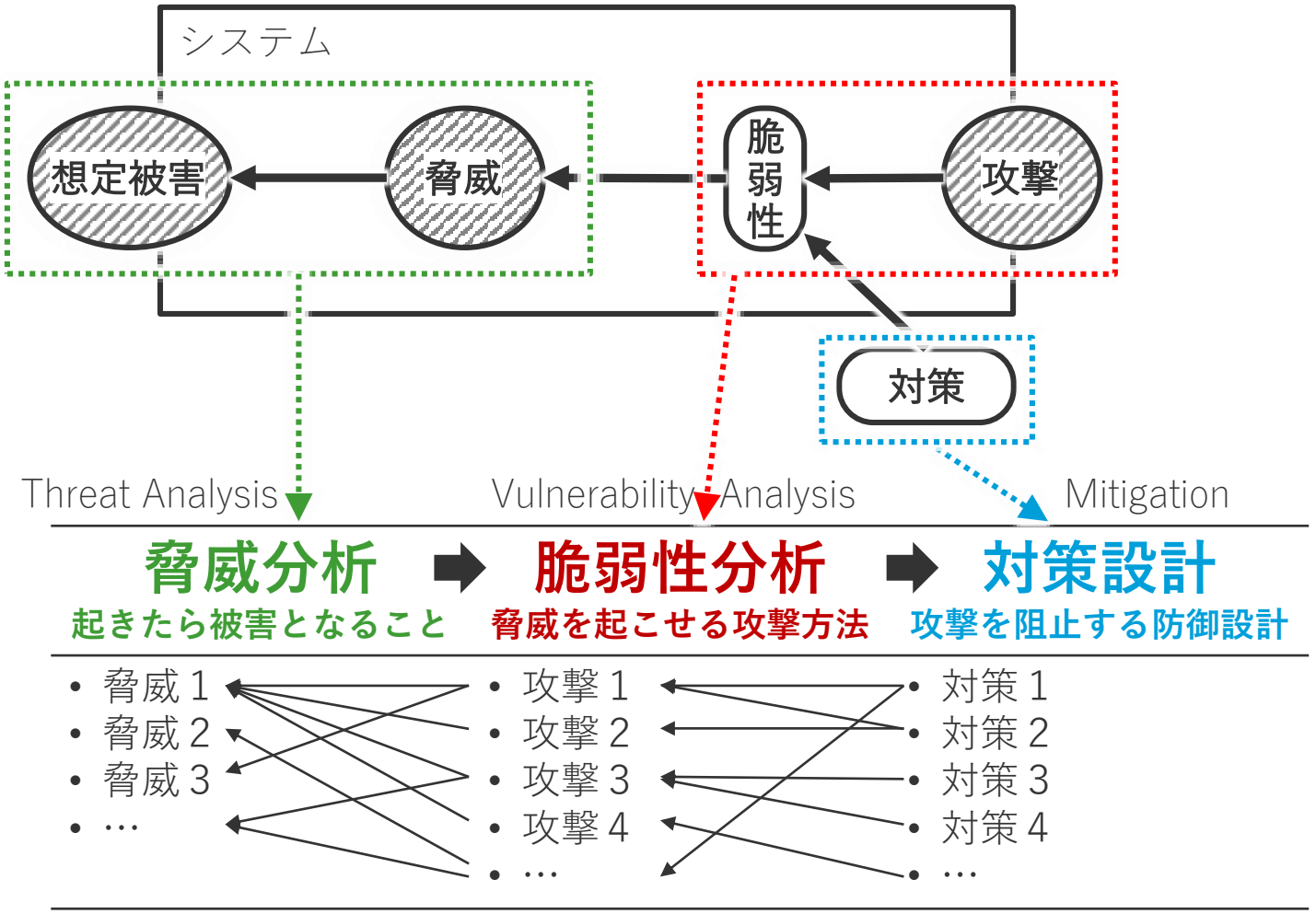
- PenTest、セキュアコーディング等のベストプラクティスは確かにセキュリティを高める
- だが、セキュリティが十分であるという説明はできない



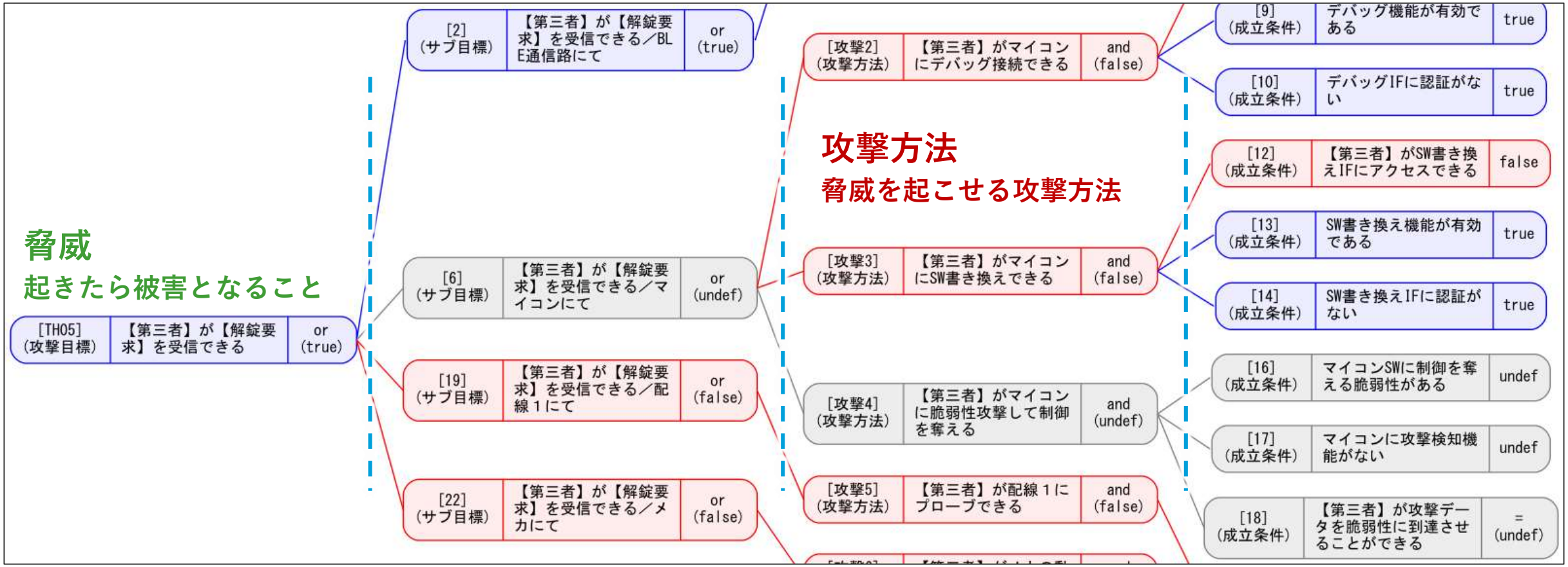
脅威分析は各施策の必要性と十分性を説明(論証)する

セキュリティ確保の構造：脅威分析 ➡ 脆弱性分析 ➡ 対策設計

これら全体を
（広義の）脅威分析
と呼んだりする



Attack Tree、脅威分析、脆弱性分析



脅威分析 ルートノードの洗い出し

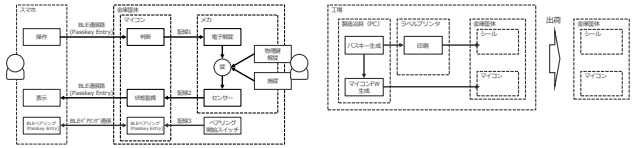
脆弱性分析 ツリー本体の洗い出し

DNV·GL

(広義の)脅威分析活動の成果物の構造

起きたら被害となること　　脅威を起こせる攻撃方法

設計 rev.N



対策ID	対策内容	割当
TCR1	マイコンを金庫筐体内部に設置する	HW
TCR2	マイコンの制御奪取系脆弱性を削減する	SW
TCR3	マイコンに制御奪取系脆弱性への攻撃検知機能を設置する	SW
TCR4	BLE通信路のペアリング方式は Passkey Entry とする	SW
TCR5	パスキーの生成にはセキュリティ用乱数を用いる	製造
TCR6	ペアリング開始操作後の120秒間だけペアリング応答する	SW
TCR7	ペアリング開始スイッチを金庫筐体内部に設置する	HW
TCR8	シールに注意書きして、パスキーを第三者に知られないように注意喚起する	製造

脅威分析

脅威一覧

脅威ID	脅威
TH7	【第三者】が【解錠】を【起動】する
TH9	【第三者】が【解錠要求】を【読取・推測】する
TH10	【第三者】が【解錠要求】を【作成・変更】する
TH11	【第三者】が【施錠状態】を【読取・推測】する
TH12	【第三者】が【施錠状態】を【作成・変更】する

脆弱性分析

攻撃一覧

攻撃ID	攻撃方法の内容
攻撃3	第三者がマイコンにデバッグ接続する
攻撃4	第三者がマイコンをFW書き換えする
攻撃5	第三者がマイコンの制御奪取系脆弱性を悪用する
攻撃6	第三者がBLE通信路で解錠要求を送信する
攻撃7	第三者がBLE通信路で解錠要求を受信する
攻撃13	第三者がBLE通信路で施錠状態を受信する
攻撃16	第三者がBLE通信路で施錠状態を送信する

対策設計

攻撃を阻止する防御設計

防御が十分であることの確認

テスト項目

SCR2-2	ソースコードのあるソフトウェアモジュールについては、ソースコード静的解析ツールにより表SCR2-2の脆弱性を検出して対応する
SCR2-3	BLE通信のPasskey Entryによる保護を破るPenTestを実施する
SCR2-4	BLE通信のプロトコルスタックのFuzzingテストを実施する
SCR2-5	BLE通信のメッセージ受信部分をコードレビューする

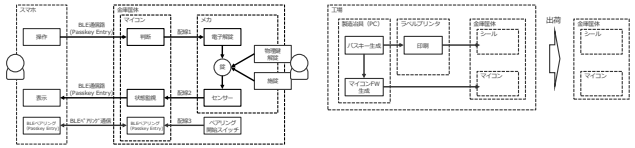
根拠 に基づいて、セキュリティが十分適切に考慮されたことを 説明(論証)

よってこのシステムは
セキュアである

すべての脅威が発生しない
ので被害は起きない

すべての攻撃が失敗する
のでどの脅威も発生しない

設計 rev.N



対策ID	対策内容	割当
TCR1	マイコンを金庫筐体内部に設置する	HW
TCR2	マイコンの制御奪取系脆弱性を削減する	SW
TCR3	マイコンに制御奪取系脆弱性への攻撃検知機能を設置する	SW
TCR4	BLE通信路のペアリング方式は Passkey Entry とする	SW
TCR5	パスキーの生成にはセキュリティ用乱数を用いる	製造
TCR6	ペアリング開始操作後の120秒間だけペアリング応答する	SW
TCR7	ペアリング開始スイッチを金庫筐体内部に設置する	HW
TCR8	シールに注意書きして、パスキーを第三者に知られないように注意喚起する	製造

脅威一覧

脅威ID	脅威
TH7	【第三者】が【解錠】を【起動】する
TH9	【第三者】が【解錠要求】を【読取・推測】する
TH10	【第三者】が【解錠要求】を【作成・変更】する
TH11	【第三者】が【施錠状態】を【読取・推測】する
TH12	【第三者】が【施錠状態】を【作成・変更】する

攻撃一覧

攻撃ID	攻撃方法の内容
攻撃3	第三者がマイコンにデバッグ接続する
攻撃4	第三者がマイコンをFW書き換えする
攻撃5	第三者がマイコンの制御奪取系脆弱性を悪用する
攻撃6	第三者がBLE通信路で解錠要求を送信する
攻撃7	第三者がBLE通信路で解錠要求を受信する
攻撃13	第三者がBLE通信路で施錠状態を受信する
攻撃16	第三者がBLE通信路で施錠状態を送信する

すべての攻撃はこれら対策により成功しない

テスト結果

SCR2-2	ソースコードのあるソフトウェアモジュールについては、ソースコード静的解析ツールにより表SCR2-2の脆弱性を検出して対応する
SCR2-3	BLE通信のPasskey Entryによる保護を破るPenTestを実施する
SCR2-4	BLE通信のプロトコルスタックのFuzzingテストを実施する
SCR2-5	BLE通信のメッセージ受信部分をコードレビューする

実際に攻撃が成功しないことを確認している

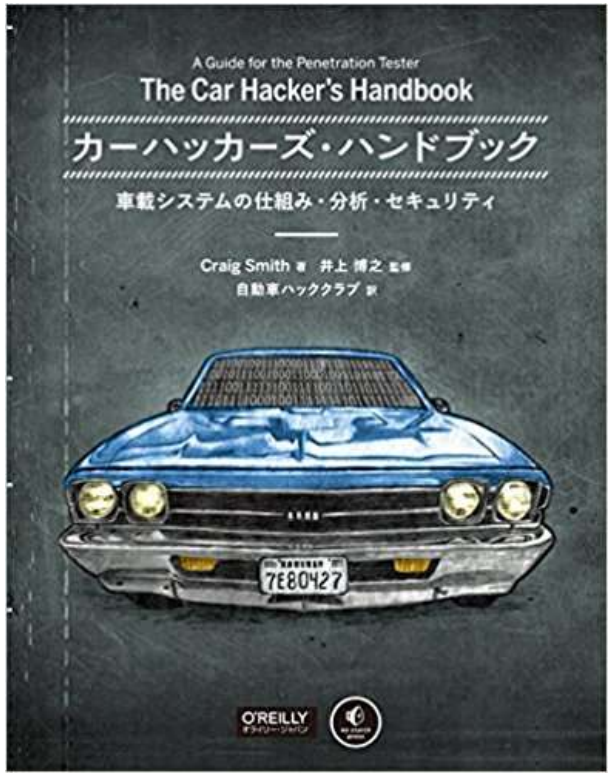
WP.29 法規案

7.2.2.2. The vehicle manufacturer shall demonstrate that the processes used within their CSMS ensure security is adequately considered.

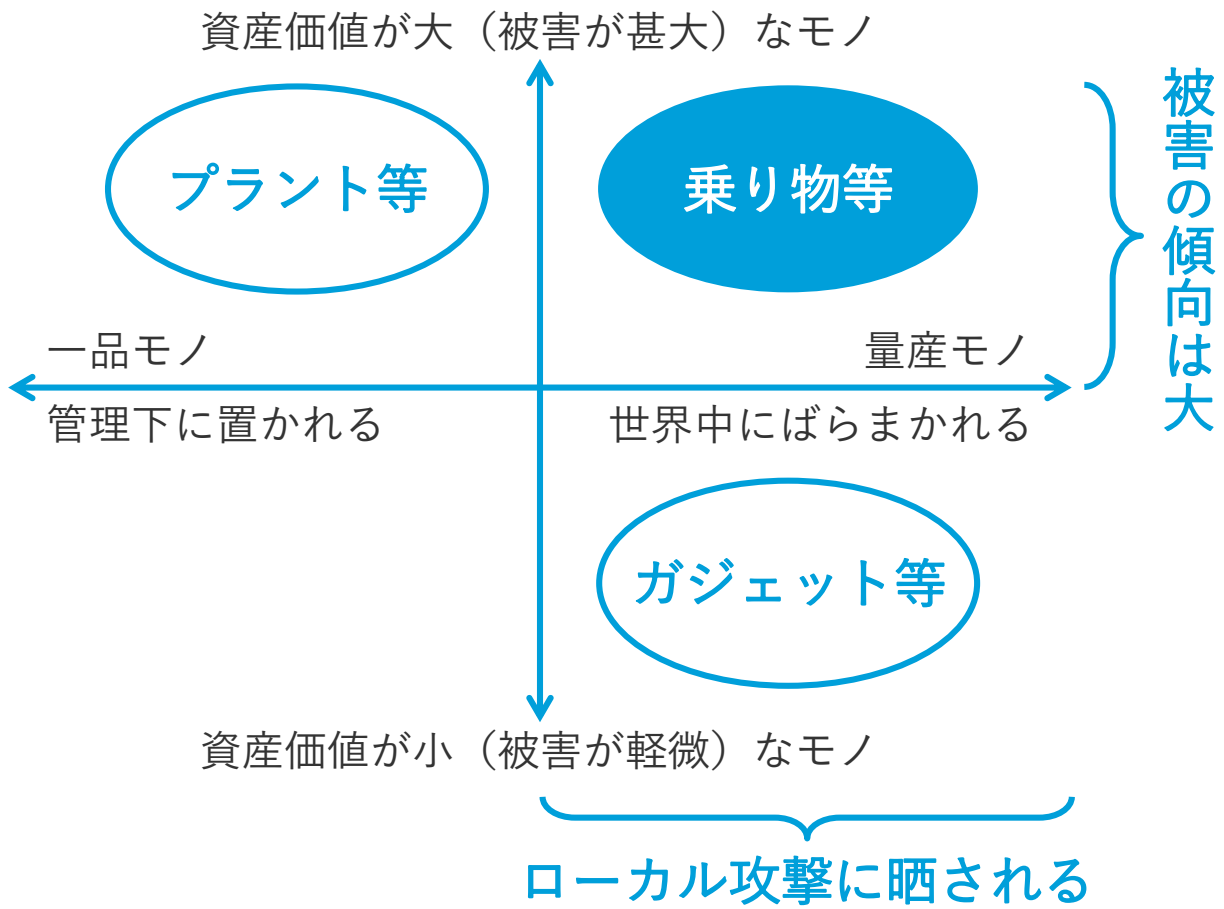
論証

根拠

量産モノのIoTはローカル攻撃（解析、改造）を想定しなければならない

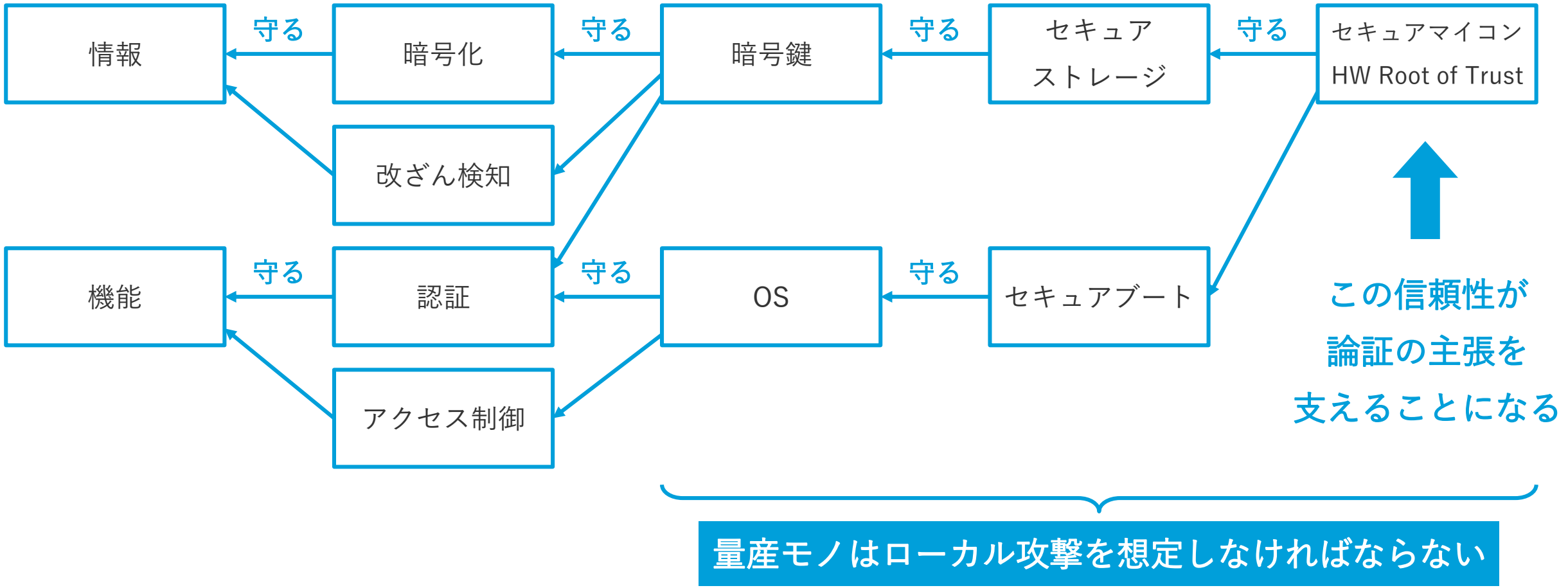


皆さん買いましょう！



https://www.amazon.co.jp/dp/4873118239
https://www.amazon.co.jp/dp/4781702368

後ろ盾チェーン … その終端には誰もが信頼する 根拠 が必要 … HW Root of Trustがそれを担う



まとめ

- セキュアマイコンやセキュアプロトコルなど「共通化された道具」が信頼の起点として提供される
- 「共通化された道具」をうまく組み合わせてシステムをセキュアに構築することになる
- ただし「うまい組み合わせ」は製品ごとに異なるので、「脅威分析」は製品単位で行うことになる
- 完璧なセキュリティというものはこの世に存在しないので、脅威分析により論証できることが必要になる
- だから、まだ脅威分析を始めていないみなさんは

宣伝：脅威分析研究会 SIGSTA

- 脅威分析に興味を持つ人たちが集まって脅威分析にまつわる議論をする勉強会
  - https://sites.google.com/view/sigsta
- どなたでも参加（ML登録＆会合参加）できます
  - 参加登録はWebから。**なにも責任は発生しません**
- 2018年は幹事↓が忙しくなってしまって会合は開催できていませんが、2019年は会合やります！

情セ大
大久保 隆夫

CAV-Tech
田口 研治

DNV GL
松並 勝