



Part A. 考慮すべき脅威、脆弱性、および、攻撃方法の全体像

バックエンドサーバーへの攻撃



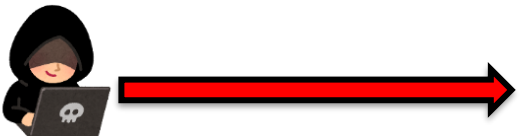
- (1) データの改ざん
- (2) サービスの中断
- (3) データの紛失・漏えい

外部通信経由での攻撃



- (16) 遠距離／近距離無線通信経由
(テレマティクス／リモートキーなど)
- (17) エンターテインメントアプリ／
3rd パーティ製ソフト経由
- (18) USBデバイスなどのコネクタ経由

通信チャネル経由による攻撃



- (4) メッセージ／データのなりすまし
- (5) データの不正操作（改ざん／消去）
- (6) セッションハイジャック／
リプレイ攻撃
- (7) データの盗聴／漏えい
- (8) DoS攻撃
- (9) 特権昇格
- (10) ウイルス感染
- (11) 通信チャネルの不正利用

車両データ／コードへの攻撃



- (19) データ／プログラムの抽出／解析
- (20) データ／プログラムの不正操作
- (21) データ／プログラムの消去
- (22) マルウェア感染
- (23) ソフトウェアの追加／改ざん
- (24) システム／サービスの中断
- (25) 各種パラメータの操作

正規利用者による攻撃



- (15) 誤使用／誤設定など
無意識による攻撃

プログラム更新に関わる攻撃



- (12) 不正なアップデート
- (13) アップデートの拒否

悪用の恐れがある潜在的な脆弱性

攻撃とは直接紐付かないため、
別途解説



■ 車両に対する脅威分析で考慮が必要な脅威

- 最低限考慮が必要な脅威／脆弱性
- 脅威を実現するための攻撃方法と脆弱性の一覧

✓ **バックエンドサーバに対する攻撃**

✓ 通信チャネルに関わる攻撃

✓ プログラム更新に関わる攻撃

✓ 正規利用者の誤操作による攻撃

✓ 外部通信経由での攻撃

✓ 車両のデータ／コードへの攻撃

✓ 悪用の恐れがある潜在的な脆弱性

■ 脅威を防ぐためのセキュリティ対策

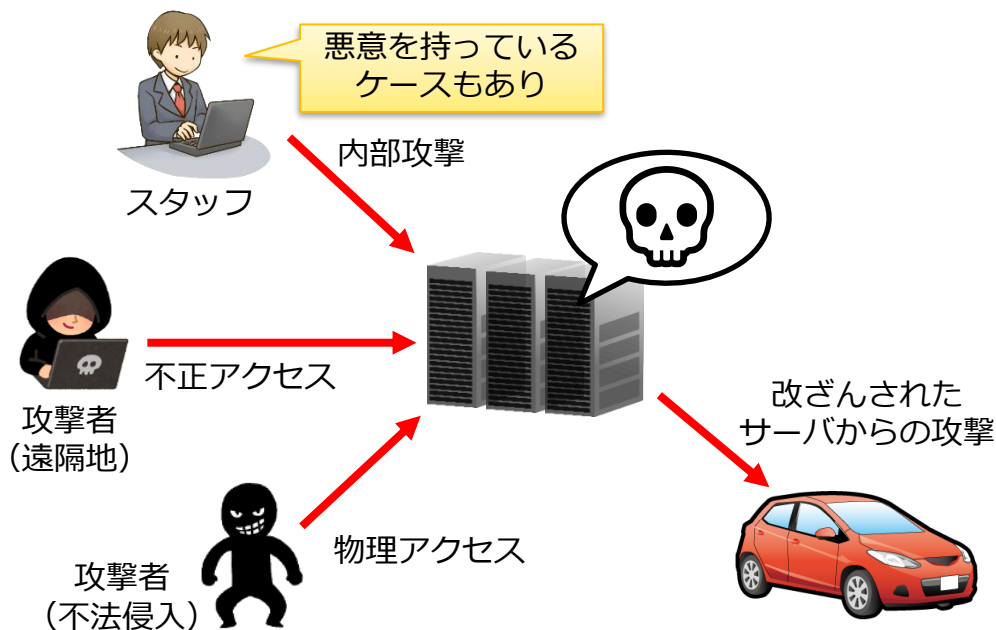
- 攻撃方法／脆弱性に応じたセキュリティ対策の一覧

→ 上記の脅威を防ぐセキュリティ対策



想定脅威 (1) : バックエンドサーバのデータ改ざん

No.	利用される脆弱性／攻撃手法の例
1.1	スタッフのアクセス権限を利用したデータ改ざん
1.2	サーバへの信頼できないインターネットアクセス (バックドア、SQL攻撃、パッチ未適用のソフトウェアの脆弱性を悪用するなど)
1.3	サーバーへの不正な物理アクセス (USBメモリや、他のメディア経由による不正な接続)



想定脅威 (1) による影響

- 以下、全ての影響に繋がる恐れあり

影響分類 (UN-R155 Annex5 より)

- (a) 自動車の安全な走行への影響
- (b) 車両機能の動作が停止
- (c) ソフトウェアの変更による性能低下
- (d) ソフトウェアを一部変更 (影響なし)
- (e) データの完全性の侵害
- (f) データの機密性の侵害
- (g) データの可用性の損失
- (h) その他 (犯罪性を含む)