自動車サイバーセキュリティ講座

サイバーセキュリティとは何か？
～安全性（セーフティ）との関係～

2020年9月4日

高田 広章

名古屋大学 未来社会創造機構 モビリティ社会研究所 教授
名古屋大学 大学院情報学研究科 教授
附属組込みシステム研究センター長
APTJ株式会社 代表取締役会長兼社長
Email: hiro@ertl.jp　URL: http://www.ertl.jp/~hiro/

AGENDA

サイバーセキュリティとは何か？

- 用語の定義：安全性（セーフティ）と機能安全
- 用語の定義：情報セキュリティ，サイバーセキュリティ
- 安全性とセキュリティの違い
- 車載システムで守るべき資産とリスク
- セキュリティ対策と機能安全の類似性
- セキュリティ対策と安全対策の関係
- 例）CRCとMAC
- 安全性とセキュリティの両立の困難性
- 取り組むべき技術課題
- 組込みシステムに向いたセキュリティ強化技術の例
- その他に取り組むべきこと

用語の定義：安全性（セーフティ）と機能安全

安全性（セーフティ，safety）

- システムが規定された条件のもとで，人の生命，健康，財産またはその環境を危険にさらす状態に移行しない期待度合い（JIS X 0134）
- 信頼性（機能単位が，要求された機能を与えられた条件のもとで，与えられた期間実行する能力（JIS X 0014））とは明確に異なる概念

機能安全（functional safety）

- 機能的な工夫（安全を確保する機能）により極力安全を確保する（NECA 技術委員会報告 第3の波「機能安全」の概要）
  - 本質安全と対比される考え方
- 電気・電子システムの誤動作を原因とするハザードによる不合理なリスクがないこと（ISO 26262独自訳）

用語の定義：情報セキュリティ

情報セキュリティ（information security）

- 情報の機密性，完全性および可用性の維持（JIS X 5080）
- さらに，真正性，責任追跡性，否認防止，信頼性などの特性の維持を含める場合も（ISO/IEC 27001）

機密性（confidentiality）

- アクセスを認可された者だけが情報にアクセスできることを確実にすること

完全性（integrity）

- 情報及び処理方法が，正確であること及び完全であることを保護すること

可用性（availability）

- 認可された利用者が，必要なときに，情報及び関連する資産にアクセスできることを確実にすること

用語の定義：サイバーセキュリティ

セキュリティとは？（まずは）

- 単なる「セキュリティ」は意味が広い
  - 辞書で最初に書かれているのは「安全」で，セーフティと区別がつかない
  - 「安全確保」「防護」という意味もある
- 「セキュリティ」という用語は，主に，故意による攻撃からの防衛を意味している場合が多い
  - national security ＝ 安全保障
  - home security ＝ 防犯
  - 「○○セキュリティ」とは，攻撃から○○を守ることを意味していることが多い
- それに対して安全技術は，主に，自然に発生する故障や，（故意でない）人為的なミスに対処することを主眼としている

サイバーセキュリティとは？（様々な定義）

- サイバー攻撃に対する防御行為（デジタル大辞泉）
  - サイバー攻撃とは，「コンピューターネットワーク上で，特定の国家，企業，団体，個人に対して行われるクラッキング行為」（デジタル大辞泉）
    - ECUに対する直接的な攻撃も考えると，「コンピュータネットワーク上で」の部分が狭いように思われる
  - この定義では，「サイバー」は守るべきものではなく，攻撃の手段を表している（他の「〇〇セキュリティ」とは用語ででき方が異なる）
- 認可されないアクセスや攻撃に対してサイバーフィジカルシステム（CPS）を守るために取られる手段（SAE J3061独自訳）
  - 「サイバー」をCPSと置き換えて，攻撃から「サイバー」を守るという定義にしているが，無理があるように思われる

サイバーセキュリティとは？（様々な定義）– 続き

- サイバーセキュリティ基本法による定義（一部省略）

> 電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること

  - 攻撃に限定されていない広い定義で，焦点がぼけている
  - 「人の知覚によっては認識することができない方式」の部分は1つの本質であろう
- 現時点で良さそうに思える定義（2案）
  - サイバー攻撃（電子的方式，磁気的方式その他人の知覚によっては認識することができない方式による攻撃）からの防御行為
  - 電気・電子システムに対する攻撃を原因とするハザードによる許容できないリスクがないこと（ISO 26262流）

サイバーセキュリティとは？（様々な定義）– 続き

- 自動車の電気・電子部品やその機能に対する脅威シナリオに対して，資産が充分に保護されている状態（ISO/SAE DIS 21434による「自動車のサイバーセキュリティ」の定義，独自訳）
  - 脅威シナリオ：損傷シナリオにつながる可能性のあるネガティブアクション（≒ 攻撃？）の記述（statement）
  - 損傷シナリオ：資産（1つまたは複数）のサイバーセキュリティプロパティ（1つまたは複数）の侵害による悪影響または望ましくない結果
  - （直接的な）攻撃対象を「自動車の電気・電子部品やその機能」としつつ，（最終的に）守るべきものは「資産」として，両者を区別している
    - ✓そう言われてみれば，home security（防犯）においても，“home”は（直接的な）攻撃対象であり，（最終的に）守るべきものではないように思われる

安全性とセキュリティの違い

何を守るか（守るべき資産）の違い

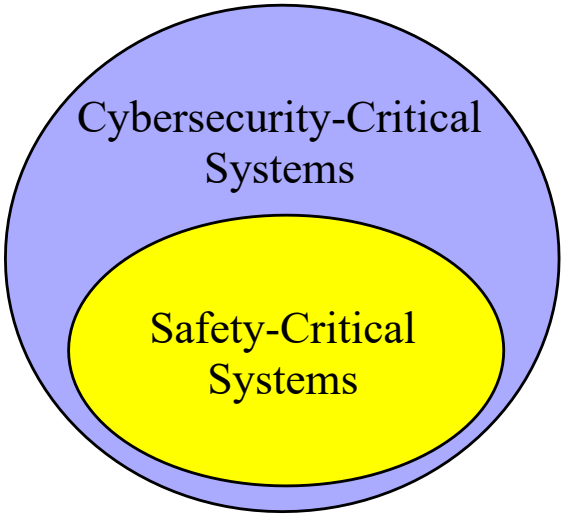
- 安全性：人の生命，健康，財産またはその環境
- ○○セキュリティ：○○（例：情報）
- サイバーセキュリティ：限定しない
- ! サイバーセキュリティの方が範囲が広い（例えば，個人情報を守ることは安全性の範囲外）．ただし，「財産」を広く捉えると，違いはなくなる

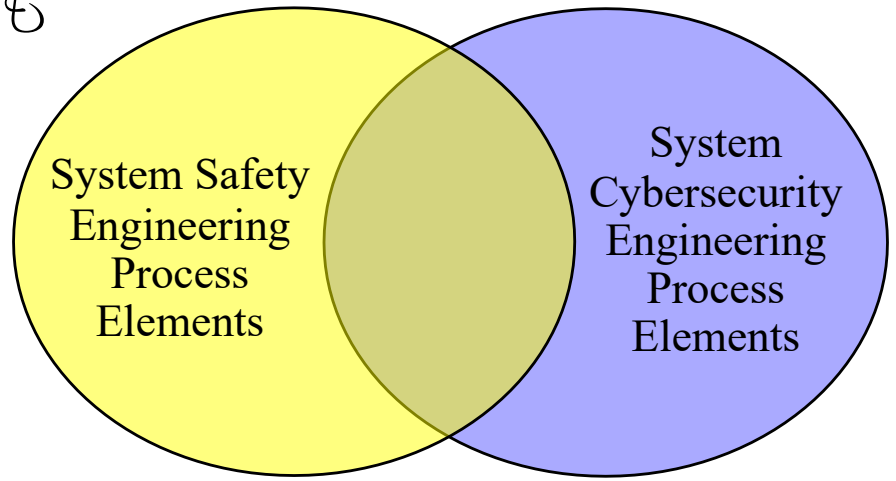
何から守るかの違い

- 安全性：故障，（故意でない）人為的なミス，性能限界
- セキュリティ：故意による攻撃
- サイバーセキュリティ：サイバー攻撃，電気・電子部品やその機能に対する攻撃

SAE J3061における安全性とサイバーセキュリティ

- セーフティクリティカルシステムは，すべてサイバーセキュリティクリティカルシステムである
  - 逆は成り立たない
  - 守るべき資産の違い
- セーフティエンジニアリングプロセスとサイバーセキュリティエンジニアリングプロセスには，共通部分もあるが，相違もある
  - 何から守るかの違い





車載システムで守るべき資産とリスク

安全性にかかわる資産

- （主に）人の生命や健康に対するリスク

安全性には含まれない資産（境界は曖昧）

- 金銭，物品（自動車そのもの，車内に置いた物品），エネルギー（電気自動車の電気），環境の盗難・破壊
  - 機械的な攻撃（例：鍵をこじ開けて自動車を盗難する）は，サイバーセキュリティの範囲外
  - これらを守る機能が電気・電子部品で実現されていれば（例：電子キーやイモビライザ），そこから先は範囲内
- 個人情報やその他の情報の流出・改ざん
  - 「情報セキュリティ」の範囲内

さらに「他に迷惑をかけないこと」も

- 車載システムがサイバー攻撃の踏み台に利用される

セキュリティ対策と機能安全の類似性

- 許容できないリスクに対して，セキュリティ対策を行う

セキュリティ対策は機能によって行うのが基本

- 「セキュリティ機能」によってセキュリティを確保する
- 「本質セキュリティ」もないわけではないが…

「セキュリティ機能」の決定が重要

- 機能安全においては，安全性を確保するために必要な安全機能が定義できれば，後は信頼性を確保すればよい
  - 安全性を確保するために取るべき手段（安全機能を含む）を抽出するための分析作業が，安全要求分析
- セキュリティにおいても同様
  - セキュリティ要求分析の技術が重要に
- 信頼性確保の部分は，安全性とセキュリティで大きい違いはなく，共通化が可能

セキュリティ対策と安全対策の関係

安全対策はセキュリティ対策としても有効な場合がある

- システムの安全性を向上させるための対策は，セキュリティを強化する上でも有効な場合がある
  - 故意による攻撃で起こることは，故障によっても起こりうるため

安全対策だけではセキュリティ対策として不十分

- 故障によって起こる確率が極めて低い（現実的には起こらない）事象も，故意による攻撃では起こりうる
  - ISO 26262では，二重故障（独立なコンポーネントが同時に故障するケース）は，基本的には想定しなくても良い
- 特に，内部の者による故意による攻撃は想定されていないことが多い

例) CRCとMAC

CRC（巡回冗長検査）

- データから作り出す小さいデータ（CRCコード）を使って，データの誤りを検出する技術
  - データ転送や保存などに伴うランダムエラーの検出に広く使われる … 安全性対策
- CRCコードは，正しいCRCコード付きデータの間の最小ハミング距離が大きくなるという性質を持つ

【参考】CANの脆弱性

- CANでは，15ビットのCRCコードで，最小ハミング距離を6としている．よって，5ビットまでの誤りを検出できるはずだったが…
- CRCコードを付けた後にビットスタッフィングをしているため，最小のハミング距離が短くなっている
- CAN FD（ISO版）では，この問題が解決されている

MAC（メッセージ認証符号）

- データと共通鍵から作り出す小さいデータ（MAC値）を使って，データ（メッセージ）の完全性を確認し，認証する技術
- MAC値は，データとMAC値の組を多数入手しても，MAC値を入手していないデータに対するMAC値を（共通鍵を知ることなしに）計算することが難しいという性質を持つ
  - 共通鍵を知らない第三者によるデータの改ざんを検出できる … セキュリティ対策
  - CRCコードは，この性質を満たさない

理解度確認問題

- CRC付きデータにMAC値を付けてよいか？
- CRC付きデータを暗号化してよいか？
- 暗号化したデータにCRCを付けてよいか？

! これがわからないと，妥当なシステム設計ができない

安全性とセキュリティの両立の困難性

どこまでのリスク評価を行うか？

- 機能安全規格は，厳密なリスク評価を要求する
- セキュリティリスクを厳密に評価するのは難しい

Guarantee文化とBest Effort文化の衝突？

セキュリティ分析（リスク評価を含む）の困難点

- 攻撃の可能性（attack goal）の網羅方法
  - どのような攻撃がありうるかを，網羅的に数え上げるのは難しい（犯罪の手口は常に新しいものが出てくる）
- 脅威は変化するため，セキュリティリスクを厳密に評価するのは難しい

  例）高性能な計算機ができると，暗号が破りやすくなる

  例）セキュリティホールが公表されると，攻撃が容易になる

取り組むべき技術課題

セキュリティ要求分析手法の確立と支援技術

- 中長期的には，形式手法や人工知能による分析支援が求められる

システムのアーキテクチャからの考慮

- セキュリティ確保に重要な部分と，安全性確保に重要な部分を分離したアーキテクチャとする

組込みシステムに向いたセキュリティ強化技術の開発

- 情報セキュリティ対策のための要素技術は数多く開発されており，それらの多くは組込みシステムにも使える
- 組込みシステムでは，限られたリソース下でのセキュリティ強化技術が求められる

連携セキュリティ基盤（信用フレームワーク）の構築

- 他社で開発されたシステムをどれだけ信じてよいかを判断する仕組みを，業界を超えて構築する必要

組込みシステムに向いたセキュリティ強化技術の例

AUTOSARにおけるCANのメッセージ認証

- AUTOSARでは，セキュアオンボード通信（SecOC）モジュールが，メッセージ認証をサポート
- メッセージを認証するための方式としては，共通鍵を用いたメッセージ認証コード（MAC）と，非対称鍵を用いたデジタル署名の両方に対応
- フレッシュネス値を用いて，メッセージが古いものではないことを検証
- MACとフレッシュネス値は，一部分のみを転送すること（トランケーション）にも対応
  - CANメッセージの長さを考えると，全体を送るのは無理
  - MACのトランケートは，保護の強度を弱める（偶然の一致の可能性が高まる）が，これが許される理由（条件）は？

その他に取り組むべきこと

セキュリティ対策に対する相場観の醸成

- ソフトウェアの安全性の規格も相場観に過ぎず，それと同様に，セキュリティ対策に対する相場観を作ることが必要

変化する脅威に対応する仕組みの導入

- 変化する脅威に対応してシステムを更新する仕組み（制度面も含めて）を導入する（その必要性の認識を広める）

人材育成

- 情報セキュリティ技術と車載組込みシステム技術の両方に精通した技術者が必要

ユーザに対する啓蒙

- ユーザに対して，セキュリティが強い/弱いの意味を理解してもらう必要がある