

| | | | |
|--|---|-----|-----------------------------------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 1/19 |
| Application: ECU of In-Vehicle network | | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a |

関係各部署 御中
To departments concerned

| | | | |
|-----------------------------------|--------------------|-----------------------------|-------|
| Confidentiality classification | PROTECTED 関係者外秘 | 原紙保管 Storage of original | M/Y / |
| | | コピー保管 Storage of copy | M/Y / |

| | | | | |
|---|---|------------|------------|-----|
| <div>(別紙 2)</div> <div>設計/実装の脆弱性分析ガイド</div> <div>(Annex 2)</div> <div>Guide for Design Vulnerability Analysis</div> | 制御電子プラットフォーム開発部 | | | |
| | 制御ネットワーク・アーキ開発室 4G | | | |
| | E/E Architecture Development Div | | | |
| | System network & architecture development dept 4G | | | |
| | No. SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | | | |
| | 承認 Approved | 調査 Checked | 作成 Created | / / |
| | | | | |
| | | | | |

| | | | |
|--|---|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 2/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

目次

| | |
|--|-----------|
| 1. はじめに | 3 |
| 1.1. 本書の目的 | 3 |
| 1.2. 関連文書 | 3 |
| 2. CWE の概要 | 4 |
| 2.1. CWE の構造 | 4 |
| 2.2. CWE のビュー | 4 |
| 2.3. CWE のカテゴリ | 6 |
| 2.4. CWE の脆弱性 | 7 |
| 3. 脆弱性分析方法 | 9 |
| 3.1. 分析対象の把握 | 9 |
| 3.1.1. 分析対象の収集 | 10 |
| 3.2. 分析観点の選定 | 10 |
| 3.2.1. CWE のカテゴリ選定 | 11 |
| 3.2.2. CWE の脆弱性選定 | 14 |
| 3.2.3. 分析不要な CWE の脆弱性の除外 | 14 |
| 3.3. 脆弱性分析 | 15 |
| 3.3.1. CWE の脆弱性を把握 | 15 |
| 3.3.2. 脆弱性有無を確認 | 16 |
| APPENDIX1. セキュリティ仕様と CWE カテゴリの対応表 | 17 |

| | | | |
|--|---|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 3/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

1. はじめに

1.1. 本書の目的

本脆弱性分析ガイドは、システムや ECU の設計や実装時に混入する可能性がある脆弱性を検出する方法を示したガイドである。本書では、脆弱性分析の分析観点として、網羅的で具体的な脆弱性の分類指標である CWE を用いる。2 章に CWE の概要を示し、3 章に CWE を用いた脆弱性分析手法を示す。

1.2. 関連文書

本書の関連文書を以下に示す。

表 1.1 関連文書一覧

| 仕様書番号 | 名称 |
|--------------------------|--------------|
| SEC-ePF-VUL-CMN-REQ-SPEC | 共通脆弱性対策要求仕様書 |

表 1.2 公的関連文書一覧

| 文書名 | 名称/外部リンク |
|-----|--|
| CC | Common Criteria for Information Technology Security Evaluation (Version 3.1 Revision 5) |
| CEM | Common Methodology for Information Technology Security Evaluation (Version 3.1 Revision 5) |
| CWE | Common Weakness Enumeration (Version 4.5) https://cwe.mitre.org/index.html |

| | | | |
|--|---|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 4/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

2. CWE の概要

本章で CWE の概要を示す。

また、CWE List の最新バージョン(Version 4.5)を元に、本書を記載しているため、今後のバージョン変更によっては本書の説明が適切でなくなる可能性があることに注意すること。

2.1. CWE の構造




CWE は、ソフトウェアやハードウェアにおける多種多様な脆弱性の分類指標として体系化されている。CWE には、脆弱性の種類を表現するために、表 2.1 に示す識別タイプが存在する。

表 2.1 CWE の識別タイプ

| 識別タイプ名 | 概要 | 具体例 |
|--------|------------------------------------|--|
| ビュー | ある観点から、いくつかのカテゴリ、または脆弱性を選択して集めたもの。 | <ul style="list-style-type: none"> • Software Development (CWE-699) • Hardware Design (CWE-1194) • Research Concepts (CWE-1000) |
| カテゴリ | 共通の特性をもつ脆弱性をグループ化したもの。 | <ul style="list-style-type: none"> • Authentication Errors (CWE-1211) • Data Processing Errors (CWE-19) • Cryptographic Issues (CWE-310) |
| 脆弱性 | 個々の脆弱性を表したもの。 | <ul style="list-style-type: none"> • Improper Removal of Sensitive Information Before Storage or Transfer (CWE-212) • Authentication Bypass Using an Alternate Path or Channel (CWE-288) |

CWE の脆弱性には、抽象度の違いにより、表 2.2 に示す属性が付与される。

表 2.2 CWE の脆弱性の属性表

| 属性名 | アイコン | 概要 |
|---------|---|---------------------------|
| クラス |  | 最も抽象的な脆弱性の属性 |
| ベース |  | 特定のリソースや技術に依存しない脆弱性の属性 |
| バリエーション |  | 個々のリソースや技術が特定できるような脆弱性の属性 |

2.2. CWE のビュー

本書では、CWE で定義されたビューのうち、Software Development ビュー(以降、SW ビュー)、

| | | | |
|--|---|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 5/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

Hardware Design ビュー(以降、HW ビュー)を用いて脆弱性分析する。これらのビューは、ソフトウェア開発、および、ハードウェア設計において混入しやすい脆弱性が選定されているためである。

CWE の脆弱性は、CWE の公式ページから確認できる。図 2.1 に示した CWE の公式ページから、SW ビュー、HW ビュー、および、Research Concepts ビューを選択して、各ビューの脆弱性を確認することができる。

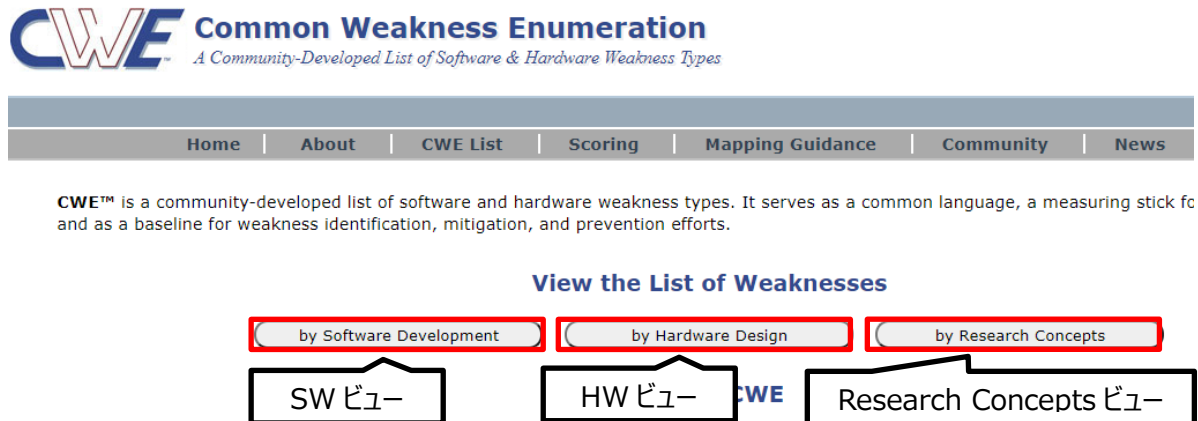


図 2.1 CWE のトップページ

SW ビュー・HW ビューは、ソフトウェア開発とハードウェア設計で混入しやすい脆弱性を、カテゴリ毎にグループ化したものである。一方で、Research Concepts ビューは、脆弱性の関係性を階層構造で表現している。各ビューの構造例を図 2.2～図 2.4 に示す。

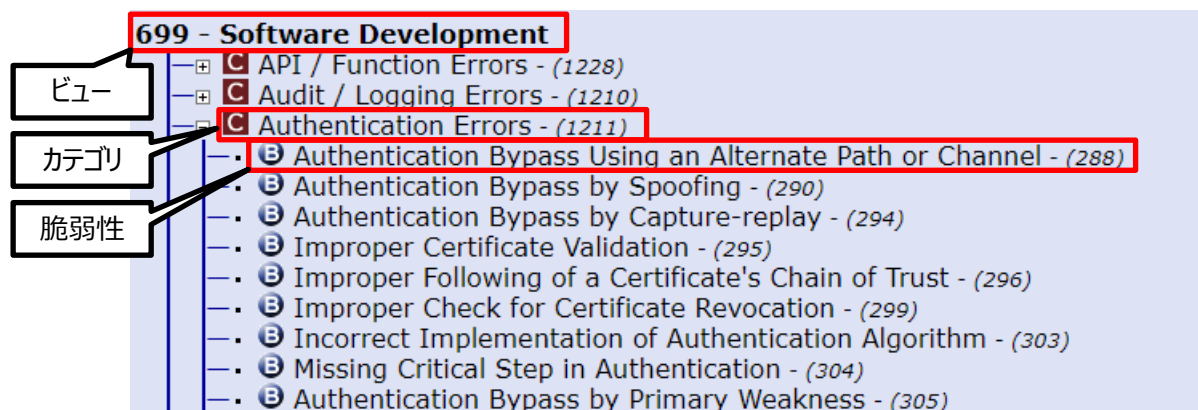


図 2.2 SW ビューの構造例

| | | | |
|--|---|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 6/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

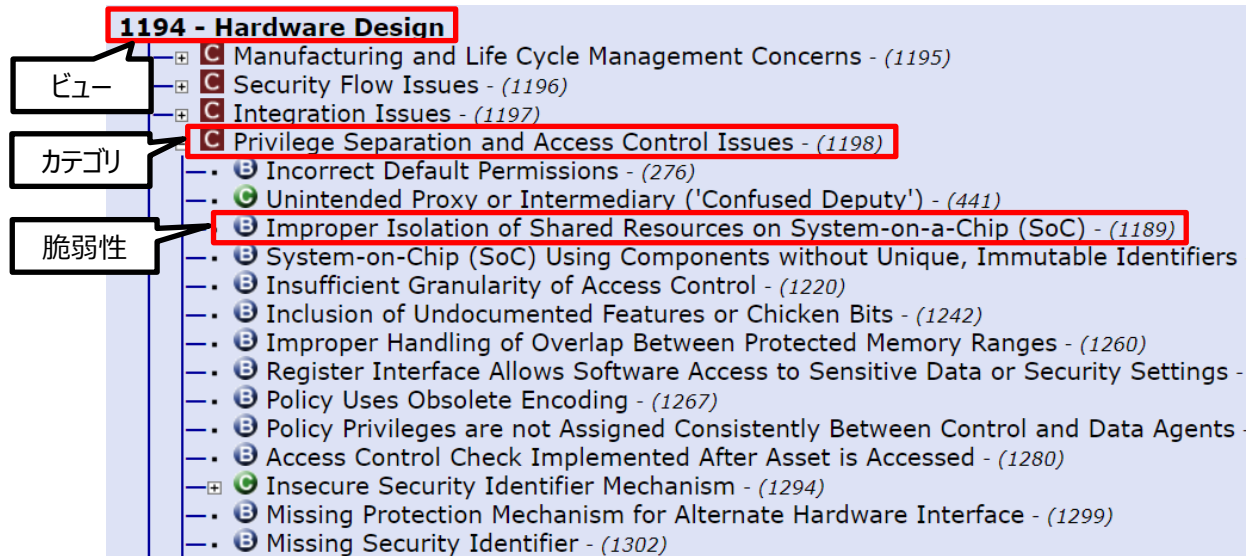


図 2.3 HW ビューの構造例

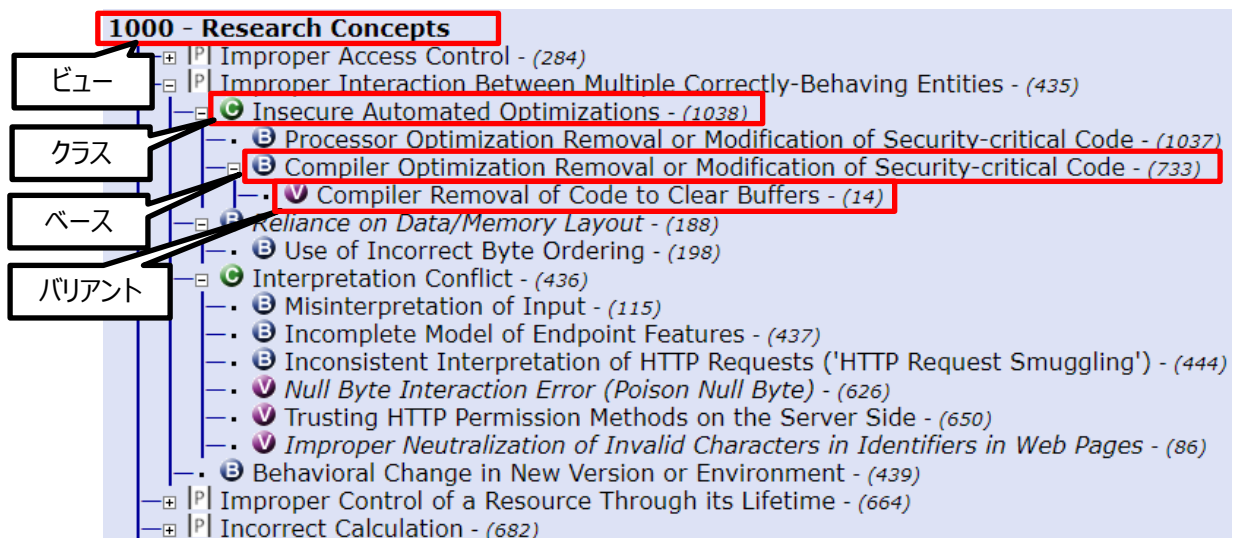


図 2.4 Research Concepts ビューの構造例

2.3. CWE のカテゴリ

SW ビューや HW ビューでは、共通の特性を持つ脆弱性をグループ化した CWE のカテゴリが複数存在する。そのため、特定の特性に着目したい場合に CWE のカテゴリを活用することができ、例えば、SW ビューの“Authentication Errors”の CWE のカテゴリでは、認証に関連する脆弱性がグループ化されている。

| | | | |
|--|--|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 7/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

2.4. CWE の脆弱性

CWE のビューに含まれる CWE の脆弱性を選択すると、説明ページが表示される。説明ページの項目のうち、本書で参照する項目を表 2.3 に示す。また、説明ページの例を図 2.5 に示す。

表 2.3 説明ページに記載されている情報

| 項目 | 記載内容 | 本書での参照箇所 |
|------------------------|----------------------|---------------|
| Description | 脆弱性の概要 | 3.3 節 |
| Extended Description | 脆弱性の詳細情報 | 3.3 節 |
| Relationships | 参照可能なビューと関連する脆弱性の情報 | 3.2.2 項、3.3 節 |
| Demonstrative Examples | 脆弱性が発生する具体的な例（コードなど） | 3.3 節 |
| Weakness Ordinalities | 脆弱性の独立性や、他の脆弱性との順序関係 | 3.2.3.1 項 |

CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer

Weakness ID: 212
Status: Incomplete

Abstraction: Base
 Structure: Simple

Presentation Filter: Complete

Description
 The product stores, transfers, or shares a resource that contains sensitive information, but it does not properly remove that information before the product makes the resource available to unauthorized actors.

Extended Description
 Resources that may contain sensitive data include documents, packets, messages, databases, etc. While this data may be useful to an individual user or small set of users who share the resource, it may need to be removed before the resource can be shared outside of the trusted group. The process of removal is sometimes called cleansing or scrubbing.
 For example, software that is used for editing documents might not remove sensitive data such as reviewer comments or the local pathname where the document is stored. Or, a proxy might not remove an internal IP address from headers before making an outgoing request to an Internet site.

Relationships

Relevant to the view "Research Concepts" (CWE-1000)

| Nature | Type | ID | Name |
|------------|------|------|---|
| ChildOf | C | 669 | Incorrect Resource Transfer Between Spheres |
| ParentOf | B | 226 | Sensitive Information in Resource Not Removed Before Reuse |
| ParentOf | B | 1258 | Exposure of Sensitive System Information Due to Uncleared Debug Information |
| CanPrecede | B | 201 | Insertion of Sensitive Information Into Sent Data |

Relevant to the view "Software Development" (CWE-699)

| Nature | Type | ID | Name |
|----------|------|-----|---|
| MemberOf | C | 199 | Information Management Errors |

(一部省略)

| | | | |
|--|---|-----|-----------------------------------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 8/19 |
| Application: ECU of In-Vehicle network | | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a |

▼ Demonstrative Examples

Example 1

This code either generates a public HTML user information page or a JSON response containing the same user information.

Example Language: **PHP** (bad code)

```
// API flag, output JSON if set
$json = $_GET['json']
$username = $_GET['user']
if(!$json)
{
    $record = getUserRecord($username);
    foreach($record as $fieldName => $fieldValue)
    {
        if($fieldName == "email_address") {

            // skip displaying user emails
            continue;
        }
        else{
            writeToHtmlPage($fieldName,$fieldValue);
        }
    }
}
else
{
    $record = getUserRecord($username);
    echo json_encode($record);
}
```

The programmer is careful to not display the user's e-mail address when displaying the public HTML page. However, the e-mail address is not removed from the JSON response, exposing the user's e-mail address.

► Observed Examples

► Potential Mitigations

▼ Weakness Ordinalities

| Ordinality | Description |
|------------|---|
| Primary | <i>(where the weakness exists independent of other weaknesses)</i> |
| Resultant | <i>(where the weakness is typically related to the presence of some other weaknesses)</i> |

図 2.5 CWE の脆弱性説明ページの例 (CWE-212 を一部抜粋)

| | | | |
|--|---|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 9/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

3. 脆弱性分析方法

脆弱性分析は、設計資料・実装に対して脆弱性がないかを確認することである。脆弱性分析の手順は、下記(1)～(3)のとおり、まず分析対象の範囲を決めて設計資料・実装を収集し、次に分析対象に関連する分析観点(CWE)を選定し、最後に分析対象と分析観点を突き合わせて確認する。

- (1) 分析対象の把握 (3.1 節参照)
- (2) 分析観点の選定 (3.2 節参照)
- (3) 脆弱性分析 (3.3 節参照)

脆弱性分析の全体イメージを図 3.1 に示す。

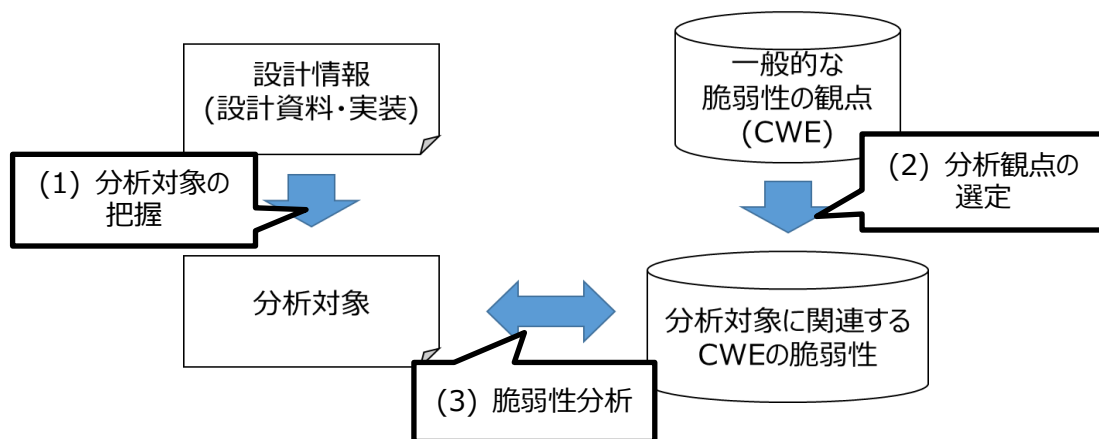


図 3.1 脆弱性分析の全体イメージ

また、(1)(2)(3)の作業の結果、分析対象毎に脆弱性分析結果として記載すべき内容を表 3.1 に示す。

表 3.1 脆弱性分析結果として記載すべき内容

| No. | 記載項目 | 記載内容 | 関連する章 |
|-----|----------|--|-------|
| (1) | 分析対象 | ・ 分析対象の設計資料・実装を識別する情報 | 3.1 節 |
| (2) | CWE の脆弱性 | ・ 「分析対象」に関連する CWE のカテゴリ/脆弱性 | 3.2 節 |
| (3) | 脆弱性分析結果 | ・ 「CWE の脆弱性」毎の脆弱性分析結果（脆弱性有無、対策要否、判断根拠） | 3.3 節 |

3.1. 分析対象の把握

脆弱性分析の対象は、セキュリティ機能とインタフェースとする。セキュリティ機能とインタフェースを対象とする理由は、システムや ECU に悪用されうる脆弱性を残さないために、資産を保護するセキュリティ機能に脆弱性がないこと、および、攻撃の入口となるインタフェースに脆弱性がないことが重要なためである。なお、セキュリティ機能とインタフェースに対して脆弱性分析することは、CC/CEM

| | | | |
|--|---|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 10/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

の脆弱性評価においても言及されている。

セキュリティ機能とインタフェースの種類と具体例を、表 3.2 に示す。セキュリティ機能は、仕様書で規定されている場合と、脆弱性対策としてセキュリティ機能を適用する場合が考えられる。インタフェースは、攻撃の入口として悪用されうる ECU 非開封の外部通信と ECU 開封後の HW レベルの全てのインタフェースを分析対象に含める。但し、セキュリティ機能に影響しないと判断できるインタフェースは対象外としてよい。

表 3.2 セキュリティ機能とインタフェースの分析対象

| 分析対象 | 分析対象の種類 | 具体例 |
|----------|-------------------------------|--|
| セキュリティ機能 | A) セキュリティ主管部署が発行する仕様の設計・実装 | ・標準リプログラミングセキュリティ |
| | B) セキュリティ主管部署以外が発行する仕様の設計・実装 | ・標準以外の ECU 独自リプロセキュリティ |
| | C) 脆弱性対策として適用するセキュリティ機能の設計・実装 | ・共通脆弱性対策要求仕様書で脆弱性対策として規定されたセキュリティ機能 (JTAG 認証など) ・識別した脆弱性の対策として新たに追加したセキュリティ機能 |
| インタフェース | ECU が有する全てのインタフェースの設計・実装 | ・ECU 非開封の外部通信インタフェース (CAN、Ethernet) ・ECU 開封後の HW レベルのインタフェース (JTAG、UART 等) |

3.1.1. 分析対象の収集

表 3.2 を参考に、「セキュリティ機能」や「インタフェース」の設計資料や実装を収集する。脆弱性分析の設計資料・実装が特定できるように、設計資料・実装の識別情報を脆弱性分析結果に記載しておく。

3.2. 分析観点の選定

CWE の脆弱性すべてが、セキュリティ機能やインタフェースに関連するとは限らないため、3.1 節で特定した「セキュリティ機能」や「インタフェース」の設計や実装に対して、関連する CWE のカテゴリと脆弱性を選定する。3.2 節の作業イメージを図 3.2 に示す。

| | | | |
|--|---|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 11/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

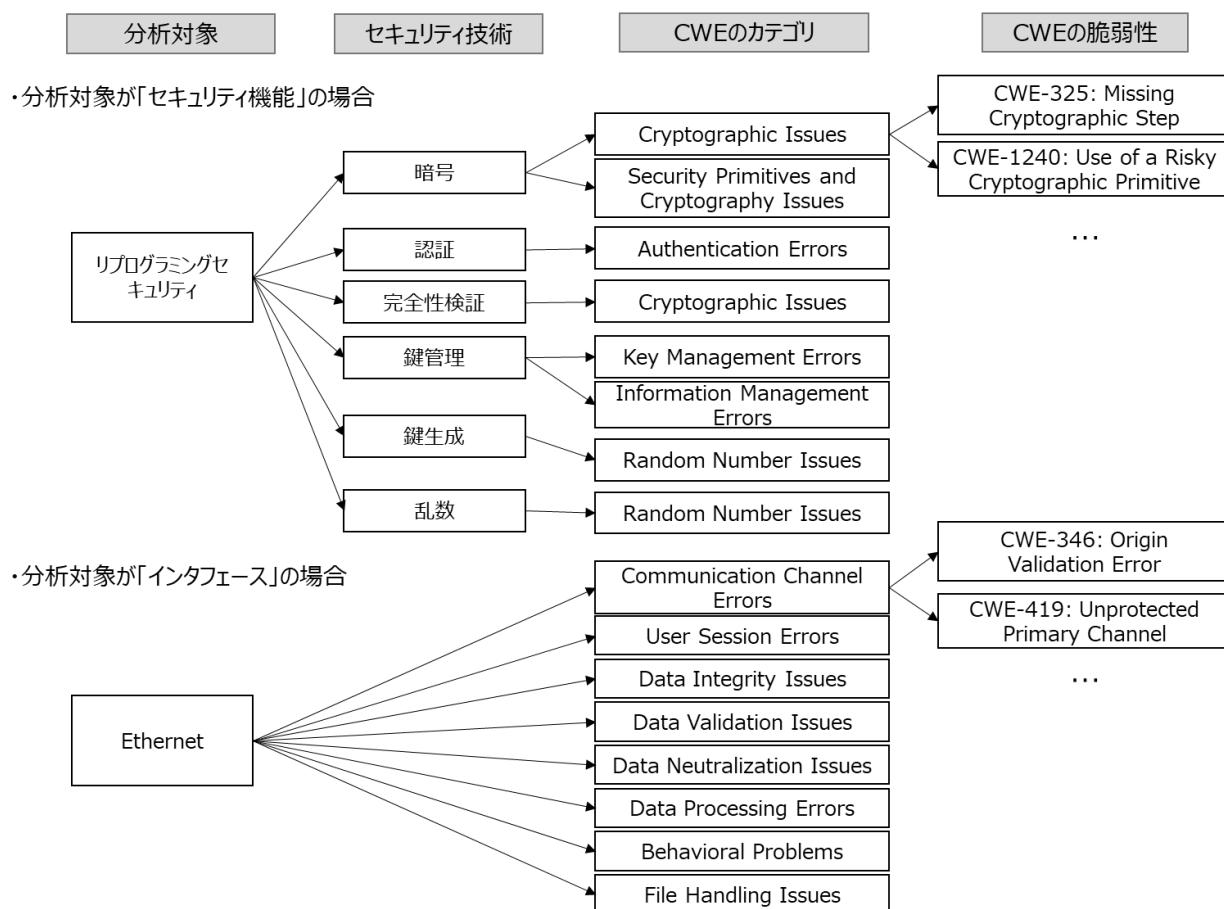


図 3.2 分析観点の選定の作業イメージ

3.2.1. CWE のカテゴリ選定

セキュリティ機能とインタフェースに関連する CWE のカテゴリを選定する。

3.2.1.1. セキュリティ機能の CWE のカテゴリ選定

セキュリティ機能に対する CWE のカテゴリの選定方法を示す。

CWE のカテゴリと紐づけできるようにするため、セキュリティ機能をセキュリティ技術に分解後、セキュリティ技術に対応する CWE カテゴリを選定する。

(1) セキュリティ機能をセキュリティ技術に分解

表 3.3 の該当基準を参考に、セキュリティ機能をセキュリティ技術に分解する。なお、表 3.3 のセキュリティ技術は、CWE の全カテゴリからセキュリティ技術に関連する CWE のカテゴリをグループ化したものである。

| | | | |
|--|---|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 12/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

表 3.3 セキュリティ技術一覧

| セキュリティ技術 | 該当基準 |
|----------|--|
| 暗号 | 暗号アルゴリズムを実装している場合、または暗号化・ハッシュ化の暗号アルゴリズムを使用している場合 |
| 認証 | 認証を使用する場合 |
| 完全性検証 | 暗号署名の完全性検証を行う場合 |
| 鍵管理 | 鍵を授受・保管する場合 |
| 鍵生成 | 鍵を生成する場合 |
| パスワード | パスワードを授受・保管する場合 |
| 乱数 | 乱数を生成する場合 |
| 権限管理 | アクセス権限の割り当てやユーザグループの定義など、権限に関する設定・処理をする場合 |

表 3.4 に示した「分析対象の種類」毎の対応を下記に示す。

A) セキュリティ主管部署が発行する仕様の設計・実装

CWE のカテゴリ選定結果を以下に示す。(※)

・ Appendix1. セキュリティ仕様と CWE カテゴリの対応表

(※) 仕様ではセキュリティ機能の具体的な実現方法を指定しておらず、設計・実装工程で実現方法を決定する場合がある。設計・実装工程で新たに決定した実現方法において、表 3.3 に該当するセキュリティ技術がないか確認すること。例えば、仕様では「認証」を指定しており、設計・実装の過程で認証方式として C&R 認証を適用した場合、チャレンジ生成で「乱数」、レスポンス生成で「暗号」のセキュリティ技術を特定する必要がある。

B) セキュリティ主管部署以外が発行する仕様の設計・実装

表 3.3 を参考にセキュリティ技術に分解すること。

C) 脆弱性対策として適用するセキュリティ機能の設計・実装

表 3.3 を参考にセキュリティ技術に分解すること。

(2) セキュリティ機能に関連する CWE カテゴリの選定

(1)で選定したセキュリティ技術に関連する CWE ビューと CWE のカテゴリを選定する。セキュリティ技術と CWE のカテゴリの対応関係は、表 3.5 を参考にすること。

| | | | |
|--|---|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 13/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

表 3.5 セキュリティ技術と CWE カテゴリの対応関係

| セキュリティ技術 | CWE ビュー | CWE カテゴリ名 |
|----------|---------|--|
| 暗号 | SW | Cryptographic Issues |
| | HW | Security Primitives and Cryptography Issues |
| 認証 | SW | Authentication Errors |
| 完全性検証 | SW | Cryptographic Issues |
| 鍵管理 | SW | Key Management Errors |
| | SW | Information Management Errors |
| 鍵生成 | SW | Random Number Issues |
| パスワード | SW | Credentials Management Errors |
| | SW | Information Management Errors |
| 乱数 | SW | Random Number Issues |
| 権限管理 | SW | Permission Issues |
| | SW | Privilege Issues |
| | SW | Authorization Errors |
| | SW | Business Logic Errors |
| | HW | Privilege Separation and Access Control Issues |

3.2.1.2. インタフェースのユースケースに応じた CWE のカテゴリ選定

インタフェースに対する CWE のカテゴリの選定方法を示す。

インタフェースは、図 3.3 のように通信機能とデータ処理に分けられる。各インタフェースの通信機能とデータ処理に対して、関連する CWE のカテゴリを表 3.6 を参考に選定する。

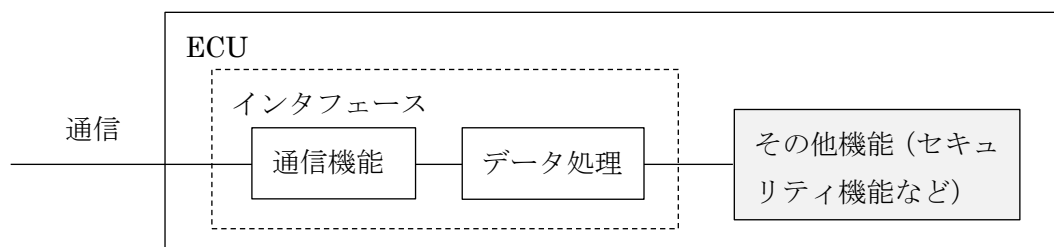


図 3.3 インタフェースの構成

表 3.6 インタフェースとカテゴリの対応関係

| 対象 | 説明 | CWE ビュー | CWE カテゴリ名 |
|------|--|---------|------------------------------|
| 通信機能 | ECU 外部または HW レベルの通信機能（例：Ethernet、JTAG） | SW | Communication Channel Errors |
| | | SW | User Session Errors |

| | | | |
|--|---|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 14/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

| 対象 | 説明 | CWE ビュー | CWE カテゴリ名 |
|-------|--------------------------------|---------|----------------------------|
| データ処理 | 受信データやコードの処理 (例：コードのダウンロード) | SW | Data Integrity Issues |
| | | SW | Data Validation Issues |
| | | SW | Data Neutralization Issues |
| | | SW | Data Processing Errors |
| | | SW | Behavioral Problems |
| | ファイルやパスの操作 (例：ファイルパスの参照処理) | SW | File Handling Issues |

3.2.2. CWE の脆弱性選定

3.2.1 項で選定した CWE のカテゴリに属する CWE の脆弱性を把握する。ビューを表示し、CWE のカテゴリを選択することで、CWE の脆弱性を確認することができる。図 3.4 に例を示す。

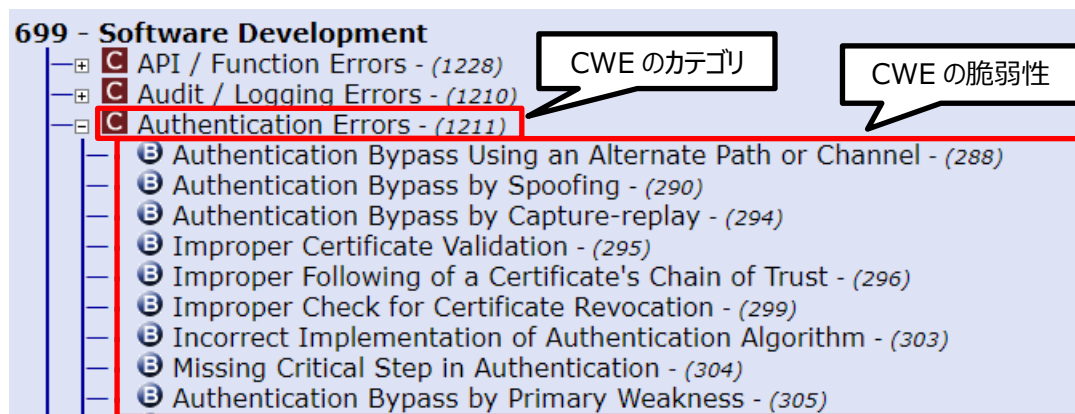


図 3.4 CWE のカテゴリに紐づく CWE の脆弱性の確認例 (CWE-1211)

3.2.3. 分析不要な CWE の脆弱性の除外

3.2.2 項で選定した CWE の脆弱性のうち、表 3.7 の脆弱性を分析観点から除外してもよい。

表 3.7 分析観点から除外できる脆弱性の種類

| 脆弱性の種類 | 除外可能な理由 |
|---------------------------|--|
| セキュリティに直接関係ない脆弱性 | その CWE の脆弱性の悪用だけではセキュリティに影響なく、セキュリティに直接関係する脆弱性を検出し、対策することで十分であるため。 |
| 共通脆弱性対策要求仕様書で対策を要求している脆弱性 | 脆弱性対策が既にされているため。 |

| | | | |
|--|--|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 15/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

3.2.3.1. セキュリティに直接関係ない脆弱性の除外

CWE の脆弱性で、「Weakness Ordinalities」項目の「Ordinality」が“Indirect”となっている脆弱性は、セキュリティに直接関係ない脆弱性と判断することができる。例を図 3.5 に示す。

| ▼ Weakness Ordinalities | |
|-------------------------|--|
| Ordinality | Description |
| Indirect | (where the weakness is a quality issue that might indirectly make it easier to introduce security-relevant weaknesses or make them more difficult to detect) |

図 3.5 セキュリティに直接関係ない CWE の脆弱性の例

3.2.3.2. 共通脆弱性対策要求仕様書で対策を要求している脆弱性の除外

CWE の脆弱性の説明と、共通脆弱性対策要求仕様書に記載された対策要件を比較し、同じ内容の CWE の脆弱性は除外できる。除外可能な CWE の脆弱性は、以下を参考にしてもよい。


- ・ Appendix2. CWE 脆弱性と共通脆弱性対策要求仕様書の対応表

3.3. 脆弱性分析

脆弱性分析では、3.1 節で特定した分析対象の設計や実装に、3.2 節で選定した CWE の脆弱性が存在しないかを確認する。脆弱性分析方法を以下に示す。

3.3.1. CWE の脆弱性を把握

脆弱性分析する前に CWE の脆弱性を理解する必要があるが、CWE の脆弱性の内容は、表 2.3 の「Description」「Extended Description」「Demonstrative Example」の項目から把握することができる。また、SW ビューや HW ビューの脆弱性は、特定のリソースや技術に依存しないベース属性の脆弱性を中心に構成されているため、具体的な脆弱性を理解しにくい場合がある。技術やリソースに依存した具体的な脆弱性を把握したい場合には、Research Concepts ビューのツリー構造を表示し、確認対象の CWE の下位に属する CWE の脆弱性を確認する。(図 3.6 参照)。

1000 - Research Concepts
 Improper Access Control - (284)

確認対象の
CWE の脆弱性

| | | | |
|--|---|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 16/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

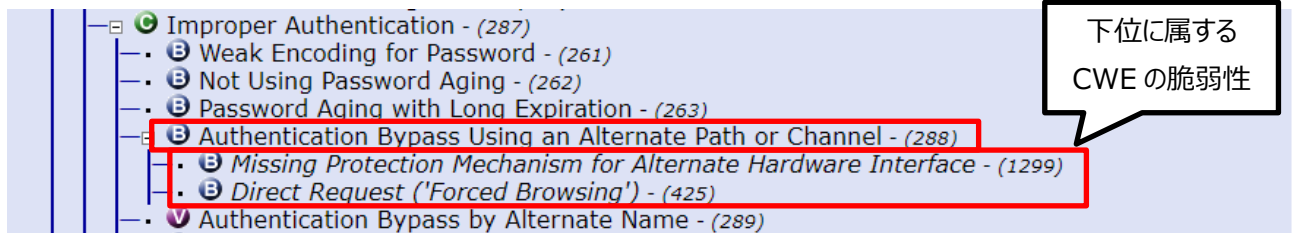


図 3.6 Research Concepts を用いた調査の例 (CWE-288)

3.3.2. 脆弱性有無を確認

分析対象の設計や実装に、CWE の脆弱性が存在しないかを確認する。脆弱性分析の結果として、脆弱性有無(非該当/該当)と対策要否と判断理由を記載する。

脆弱性が存在しない場合は、脆弱性有無は“非該当”とする。脆弱性が存在した場合は、脆弱性有無は“該当”とし、対策要否を検討する必要がある。設計や実装に対策した場合は、新たに脆弱性が混入する可能性があるため、対策の設計や実装に対して、再度脆弱性分析する必要があることに注意すること。また、脆弱性は存在するがシステムや ECU 環境においては悪用できないと判断できる場合は、対策しないことが考えられる。(例：脆弱性を悪用するためのインタフェースが存在しない、または脆弱性の悪用に一定以上の高度な攻撃能力が必要など)

| | | | |
|--|---|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 17/19 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

Appendix1. セキュリティ仕様と CWE カテゴリの対応表

| 仕様書 | セキュリティ技術 | CWE カテゴリ名 |
|-----------------------|----------|--|
| 多層分離要求仕様書 | 権限管理 | Permission Issues |
| | | Privilege Issues |
| | | Authorization Errors |
| | | Business Logic Errors |
| | | Privilege Separation and Access Control Issues |
| 2 層目メッセージフィルタリング要求仕様書 | 完全性検証 | Cryptographic Issues |
| | 権限管理 | Permission Issues |
| | | Privilege Issues |
| | | Authorization Errors |
| | | Business Logic Errors |
| メッセージフィルタリング要求仕様書 | 暗号 | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | 認証 | Authentication Errors |
| | 鍵管理 | Key Management Errors |
| | | Information Management Errors |
| | 権限管理 | Permission Issues |
| | | Privilege Issues |
| | | Authorization Errors |
| | | Business Logic Errors |
| | | Privilege Separation and Access Control Issues |
| センタ-接続機器認証要求仕様書 | 暗号 | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | 認証 | Authentication Errors |
| | パスワード | Credentials Management Errors |
| | | Information Management Errors |
| | 乱数 | Random Number Issues |
| | 権限管理 | Permission Issues |
| | | Privilege Issues |
| | | Authorization Errors |
| | | Business Logic Errors |

| | | | |
|--|---|-----|-----------------------------------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 18/19 |
| Application: ECU of In-Vehicle network | | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a |

| 仕様書 | セキュリティ技術 | CWE カテゴリ名 |
|------------------------------|----------|--|
| | | Privilege Separation and Access Control Issues |
| 標準プログラミング セキュリティ要求仕様 書 | 暗号 | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | 認証 | Authentication Errors |
| | 完全性検証 | Cryptographic Issues |
| | 鍵管理 | Key Management Errors |
| | | Information Management Errors |
| | 鍵生成 | Random Number Issues |
| | 乱数 | Random Number Issues |
| センター通信セキュリ ティ要求仕様書 | 暗号 | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | 認証 | Authentication Errors |
| | 完全性検証 | Cryptographic Issues |
| | 鍵管理 | Key Management Errors |
| | | Information Management Errors |
| | 鍵生成 | Random Number Issues |
| 無線通信セキュリティ 要求仕様書 | 暗号 | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | 認証 | Authentication Errors |
| | 完全性検証 | Cryptographic Issues |
| | 鍵管理 | Key Management Errors |
| | | Information Management Errors |
| | 鍵生成 | Random Number Issues |
| | パスワード | Credentials Management Errors |
| | | Information Management Errors |
| | 権限管理 | Permission Issues |
| | | Privilege Issues |
| | | Authorization Errors |
| | | Business Logic Errors |
| | | Privilege Separation and Access Control Issues |
| メッセージ認証(フル FV 版) 要求仕様書 | 暗号 | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | 完全性検証 | Cryptographic Issues |

| | | | |
|--|---|-----|-----------------------------------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 19/19 |
| Application: ECU of In-Vehicle network | | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a |

| 仕様書 | セキュリティ技術 | CWE カテゴリ名 |
|----------------------------|----------|---|
| 車載鍵管理 CAN-Ethernet 中継要求仕様書 | (該当なし) | - |
| 車載鍵管理マスタ 要求仕様書 | 暗号 | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | 鍵管理 | Key Management Errors |
| | | Information Management Errors |
| | 鍵生成 | Random Number Issues |
| 車載鍵管理スレーブ 要求仕様書 | 乱数 | Random Number Issues |
| | 暗号 | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | 完全性検証 | Cryptographic Issues |
| | 鍵管理 | Key Management Errors |
| | | Information Management Errors |

| | | | |
|--|---|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 1/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

Table of Contents

| | |
|---|-----------|
| 1. INTRODUCTION..... | 2 |
| 1.1. PURPOSE OF THIS DOCUMENT..... | 2 |
| 1.2. RELATED DOCUMENTS | 2 |
| 2. OUTLINE OF CWE..... | 3 |
| 2.1. STRUCTURE OF CWE | 3 |
| 2.2. VIEW OF CWE..... | 4 |
| 2.3. CATEGORY OF CWE..... | 6 |
| 2.4. CWE VULNERABILITY | 6 |
| 3. VULNERABILITY ANALYSIS METHOD..... | 9 |
| 3.1. UNDERSTANDING THE ANALYSIS TARGET..... | 10 |
| 3.1.1. COLLECTION OF ANALYSIS TARGET | 11 |
| 3.2. SELECTION OF ANALYSIS PERSPECTIVE | 11 |
| 3.2.1. SELECTION OF CWE CATEGORY | 12 |
| 3.2.2. SELECTION OF CWE VULNERABILITY | 15 |
| 3.2.3. EXCLUDING CWE VULNERABILITY THAT DOES NOT REQUIRE ANALYSIS | 16 |
| 3.3. VULNERABILITY ANALYSIS | 17 |
| 3.3.1. UNDERSTANDING CWE VULNERABILITY..... | 17 |
| 3.3.2. CONFIRM FOR VULNERABILITY | 17 |
| APPENDIX1. CORRESPONDENCE TABLE BETWEEN SECURITY SPECIFICATIONS AND CWE CATEGORIES | 19 |

| | | | |
|--|--|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 2/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

1. Introduction

1.1. Purpose of this document

This Vulnerability Analysis Guide provides a method for detecting vulnerabilities that may be introduced during the design and implementation of systems and ECUs. This guide uses CWE, an exhaustive and specific vulnerability classification index, as the analysis perspective for vulnerability analysis. Chapter 2 provides an overview of CWE, and Chapter 3 provides the vulnerability analysis methodology using CWE.

1.2. Related documents

The documents related to this document are as follows.

Table1.1 List of Related Documents

| Specification Number | Title |
|--------------------------|---|
| SEC-ePF-VUL-CMN-REQ-SPEC | Requirements Specification of Common Vulnerability Countermeasure |

Table1.2 List of Public Related Documents

| Abbreviation in this document | Title and External links |
|-------------------------------|--|
| CC | Common Criteria for Information Technology Security Evaluation (Version 3.1 Revision 5) |
| CEM | Common Methodology for Information Technology Security Evaluation (Version 3.1 Revision 5) |
| CWE | Common Weakness Enumeration (Version 4.5) https://cwe.mitre.org/index.html |

| | | | |
|--|--|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 3/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

2. Outline of CWE

An outline of CWE is presented in this chapter.

Note that this document is based on the latest version of the CWE List (Version 4.5), so the explanations in this document may not be appropriate due to future version changes.

2.1. Structure of CWE



CWE is systematized as a classification metrics for a wide variety of vulnerabilities in software and hardware. CWE has the identification types shown in Table 2.1 to express the types of vulnerabilities.

Table 2.1 Identification type of CWE


| Identification type name | Outline | Concrete example |
|--------------------------|--|--|
| View | A collection of selected categories, or vulnerabilities, from a certain point of view. | <ul style="list-style-type: none"> • Software Development (CWE-699) • Hardware Design (CWE-1194) • Research Concepts (CWE-1000) |
| Category | A grouping of vulnerabilities that have common characteristics. | <ul style="list-style-type: none"> • Authentication Errors (CWE-1211) • Data Processing Errors (CWE-19) • Cryptographic Issues (CWE-310) |
| Vulnerability | A representation of an individual vulnerability. | <ul style="list-style-type: none"> • Improper Removal of Sensitive Information Before Storage or Transfer (CWE-212) • Authentication Bypass Using an Alternate Path or Channel (CWE-288) |

CWE **Vulnerabilities** are assigned the attributes shown in Table 2.2, depending on the level of abstraction.

Table 2.2 CWE Vulnerability Attribute Table

| Attribute name | Icon | Outline |
|----------------|---|--|
| Class |  | Most Abstract Vulnerability Attributes |
| Base |  | Vulnerability attributes independent of specific resources or technologies |

| | | | |
|--|--|-----|-----------------------------------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 4/22 |
| Application: ECU of In-Vehicle network | | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a |

| | | |
|---------|---|--|
| Variant |  | Vulnerability attributes that allow individual resources and technologies to be identified |
|---------|---|--|

2.2. View of CWE

In this document, among the **View** defined in CWE, the Software Development View (hereafter referred to as **SW View**) and Hardware Design View (hereafter referred to as **HW View**) are used for vulnerability analysis. These **Views** are selected for vulnerabilities that are likely to be introduced in software development and hardware design.

CWE **Vulnerabilities** can be found on the official CWE page. From the official CWE page shown in Figure 2.1 CWE Top Page, you can select the **SW View**, **HW View**, and Research Concepts **View** to check **Vulnerabilities** in each view.

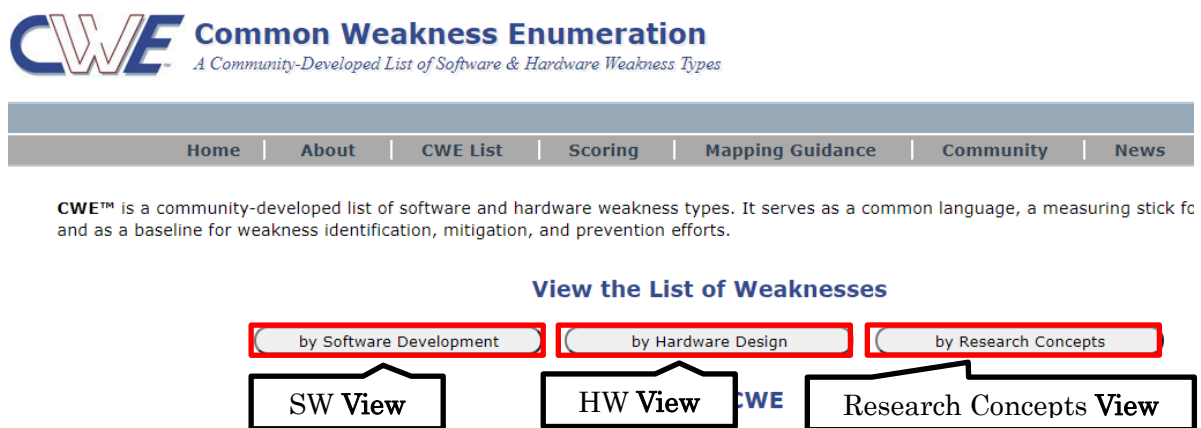


Figure 2.1 CWE Top Page

The **SW View** and **HW View** are groups of **Vulnerabilities** that are likely to be introduced in during software development and hardware design. On the other hand, the Research Concepts **View** expresses vulnerability relationships in a hierarchical structure. Examples of the structure of each **View** are shown in Figure 2.2 to Figure 2.4.

| | | | |
|--|--|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 5/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

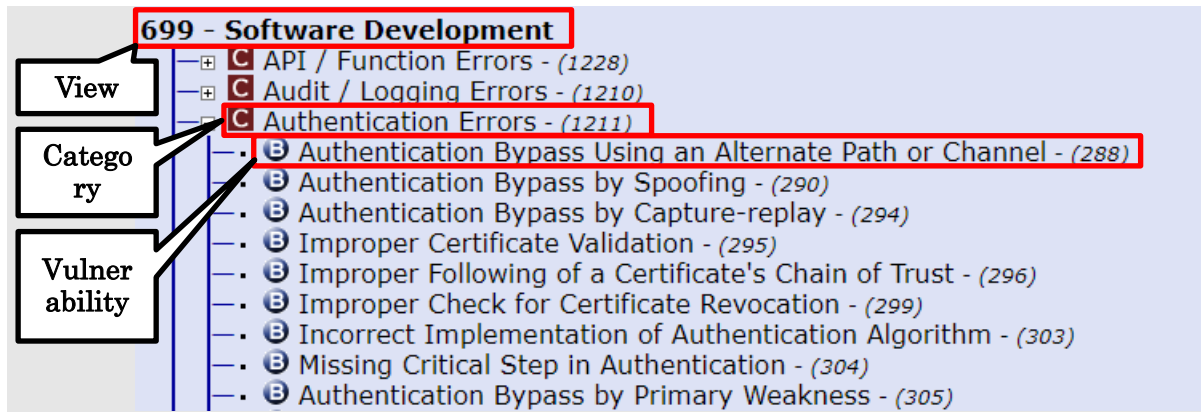


Figure 2.2 Structure example of SW View

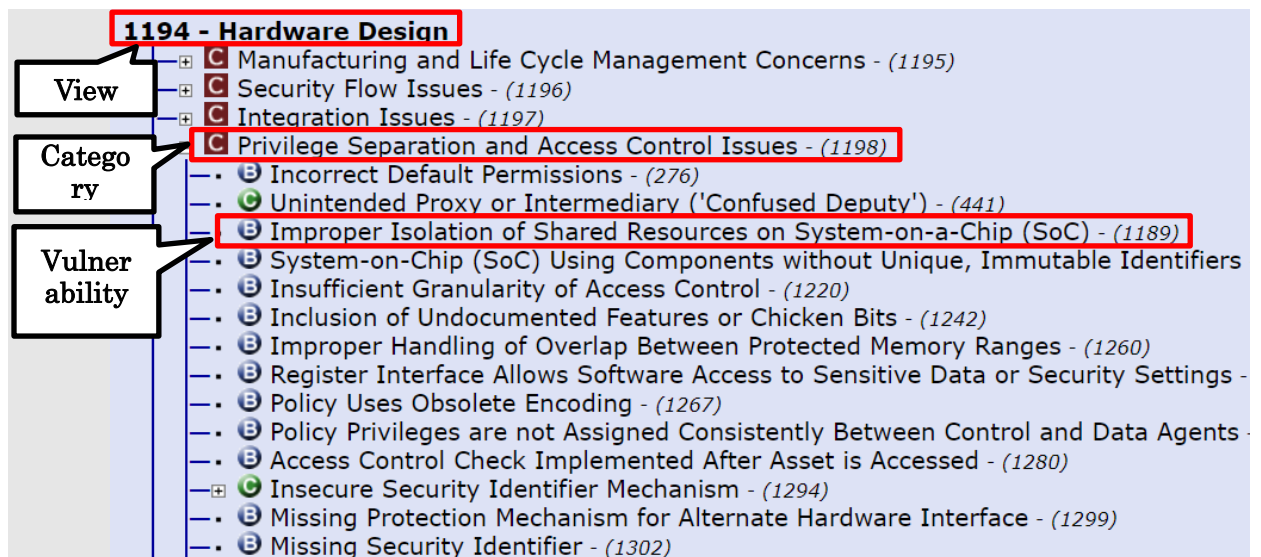


Figure 2.3 Structure example of HW View

| | | | |
|--|---|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 6/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

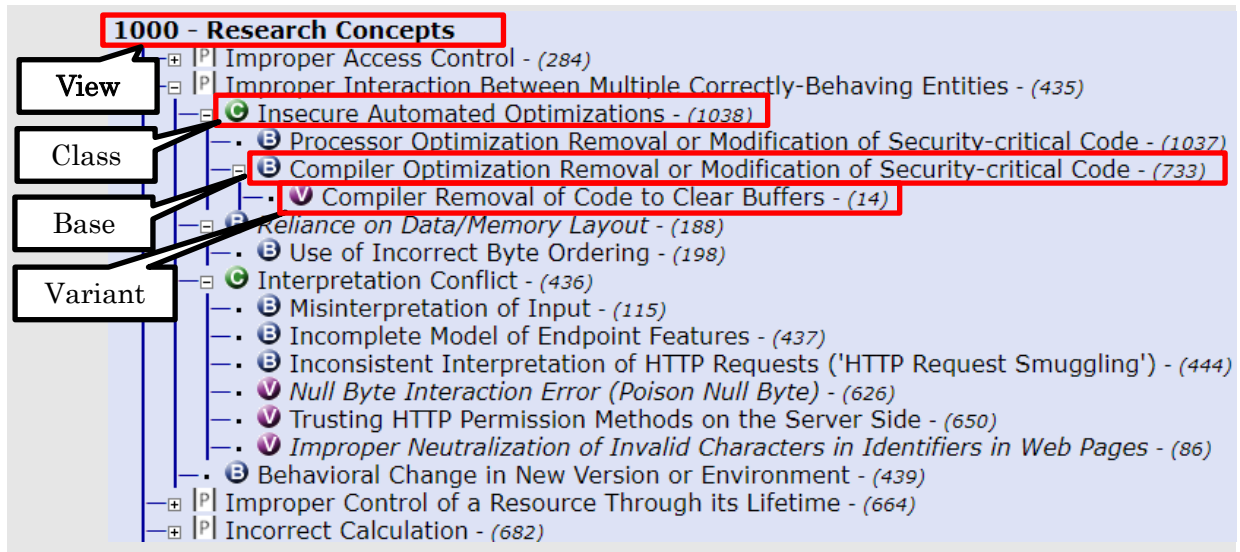


Figure 2.4 Structure example of Research Concepts View

2.3. Category of CWE

In the SW **View** and the HW **View**, there are multiple CWE **Categories** that group **Vulnerabilities** with common characteristics. Therefore, CWE **Categories** can be used to focus on specific characteristics. For example, the CWE **Category** of “Authentication Errors” in the SW **View** groups authentication-related vulnerabilities.

2.4. CWE Vulnerability

Selecting a CWE **Vulnerability** in the CWE **View**, bring up an explanation page. Table 2.3 shows the items on the explanation page that are referenced in this document. An example of an explanation page is shown in Figure 2.5.

Table 2.3 Information provided on the explanation page

| Item | Description | References in this document |
|------------------------|--|-----------------------------------|
| Description | Vulnerability outline | Section 3.3 |
| Extended Description | Detailed information about the Vulnerability | Section 3.3 |
| Relationships | Visible views and related Vulnerability information | Sub Section 3.2.2、 Section 3.3 |
| Demonstrative Examples | Concrete examples of Vulnerabilities (code, etc.) | Section 3.3 |

| | | | |
|--|--|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 7/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

| | | |
|-----------------------|--|---------------------|
| Weakness Ordinalities | Vulnerability independence and ordering relationship with other vulnerabilities | Sub Section 3.2.3.1 |
|-----------------------|--|---------------------|

CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer

Weakness ID: 212

Abstraction: Base

Structure: Simple

Status: Incomplete

Presentation Filter: Complete ▾

▼ Description

The product stores, transfers, or shares a resource that contains sensitive information, but it does not properly remove that information before the product makes the resource available to unauthorized actors.

▼ Extended Description

Resources that may contain sensitive data include documents, packets, messages, databases, etc. While this data may be useful to an individual user or small set of users who share the resource, it may need to be removed before the resource can be shared outside of the trusted group. The process of removal is sometimes called cleansing or scrubbing.

For example, software that is used for editing documents might not remove sensitive data such as reviewer comments or the local pathname where the document is stored. Or, a proxy might not remove an internal IP address from headers before making an outgoing request to an Internet site.

▼ Relationships

▼ Relevant to the view "Research Concepts" (CWE-1000)

| Nature | Type | ID | Name |
|------------|------|------|---|
| ChildOf | ✓ | 669 | Incorrect Resource Transfer Between Spheres |
| ParentOf | Ⓑ | 226 | Sensitive Information in Resource Not Removed Before Reuse |
| ParentOf | Ⓑ | 1258 | Exposure of Sensitive System Information Due to Uncleared Debug Information |
| CanPrecede | Ⓑ | 201 | Insertion of Sensitive Information Into Sent Data |

▼ Relevant to the view "Software Development" (CWE-699)

| Nature | Type | ID | Name |
|----------|------|-----|---|
| MemberOf | Ⓒ | 199 | Information Management Errors |

(Partially omitted)

| | | | |
|--|---|-----|-----------------------------------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 8/22 |
| Application: ECU of In-Vehicle network | | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a |

▼ Demonstrative Examples

Example 1

This code either generates a public HTML user information page or a JSON response containing the same user information.

Example Language: **PHP** (bad code)

```
// API flag, output JSON if set
$json = $_GET['json']
$username = $_GET['user']
if(!$json)
{
    $record = getUserRecord($username);
    foreach($record as $fieldName => $fieldValue)
    {
        if($fieldName == "email_address") {

            // skip displaying user emails
            continue;
        }
        else{
            writeToHtmlPage($fieldName,$fieldValue);
        }
    }
}
else
{
    $record = getUserRecord($username);
    echo json_encode($record);
}
```

The programmer is careful to not display the user's e-mail address when displaying the public HTML page. However, the e-mail address is not removed from the JSON response, exposing the user's e-mail address.

► Observed Examples

► Potential Mitigations

▼ Weakness Ordinalities

| Ordinality | Description |
|------------|---|
| Primary | <i>(where the weakness exists independent of other weaknesses)</i> |
| Resultant | <i>(where the weakness is typically related to the presence of some other weaknesses)</i> |

Figure 2.5 Example of CWE Vulnerability explanation page (Excerpt from CWE-212)

| | | | |
|--|--|-----------------------------------|------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 9/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

3. Vulnerability analysis method

Vulnerability analysis is to confirm that there are no vulnerabilities in design documents and implementations. The procedure of vulnerability analysis is as follows (1) to (3). First, determine the scope of the analysis target and collect design documents and implementation, then select the analysis perspective (CWE) related to the analysis target, and finally compare and confirm the analysis target and the analysis perspective.

- (1) Understanding the analysis target (see Section 3.1)
- (2) Selection of analysis perspective (see Section 3.2)
- (3) Vulnerability analysis (see section 3.3)

An overall image of vulnerability analysis is shown in Figure 3.1.

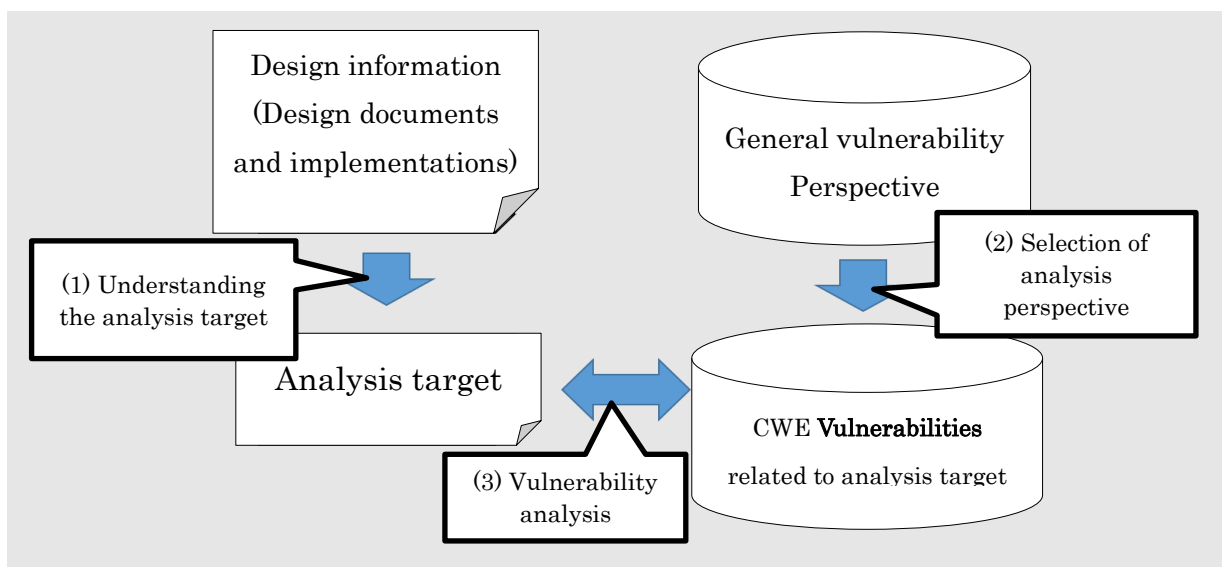


Figure 3.1 Overall image of vulnerability analysis

Table 3.1 shows the contents to be described as vulnerability analysis results for each analysis target through the work in (1), (2), and (3)..

Table 3.1 Contents to be described as vulnerability analysis results

| No. | Described items | Description | Related chapters |
|-----|-----------------|---|------------------|
| (1) | Analysis target | <ul style="list-style-type: none"> Information that identifies design documents and implementations to be analyzed | Section 3.1 |

| | | | |
|--|--|-----|-----------------------------------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 10/22 |
| Application: ECU of In-Vehicle network | | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a |

| No. | Described items | Description | Related chapters |
|-----|--------------------------------|---|------------------|
| (2) | CWE Vulnerabilities | • CWE Categories/Vulnerabilities related to “Analysis target” | Section 3.2 |
| (3) | Vulnerability analysis results | • Vulnerability analysis results for each " CWE Vulnerabilities " (presence or absence of vulnerabilities, necessity of countermeasures, grounds for judgment) | Section 3.3 |

3.1. Understanding the analysis target

The targets of vulnerability analysis are security functions and interfaces. The reason for targeting security functions and interfaces is to ensure that there are no vulnerabilities in the security functions that protect assets and that there are no vulnerabilities in the interfaces that serve as entry points for attacks, in order to leave no vulnerabilities that can be exploited in the system or ECU. Vulnerability analysis for security functions and interfaces is also mentioned in CC/CEM vulnerability assessment.

The types and examples of security functions and interfaces are shown in Table 3.2. Security functions can be defined in specifications or applied as vulnerability countermeasures. Interfaces include unopened ECU external communication and all HW level interfaces after ECU opening that can be exploited as entry points for attacks. However, interfaces that can be judged not to affect security functions may be excluded.

Table 3.2 Analysis target of security functions and interfaces

| Analysis target | Type of analysis target | Concrete example |
|--------------------|--|--|
| Security functions | A) Design and implementation of specifications issued by the department responsible for security | • Standard Reprogramming Security |
| | B) Design and implementation of specifications issued by the departments other than responsible for security | • Non-Standard ECU-specific Reprogramming Security |

| | | | |
|--|--|-----|-----------------------------------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 11/22 |
| Application: ECU of In-Vehicle network | | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a |

| | | |
|------------|---|--|
| | C) Design and implementation of security functions applied as vulnerability countermeasures | <ul style="list-style-type: none"> • Security functions specified as vulnerability countermeasures in the Requirements Specification of Common Vulnerability Countermeasure (JTAG authentication, etc.) • Newly added security functions to address identified vulnerabilities |
| Interfaces | Design and implementation of all interfaces of ECU | <ul style="list-style-type: none"> • ECU unopened external communication interfaces (CAN, Ethernet) • HW level interface after opening ECU (JTAG, UART, etc.) |

3.1.1. Collection of analysis target

Collect the design document and implementation of "security functions" and "interfaces" by referring to Table 3.2. In order to identify the design document and implementation of the vulnerability analysis, the identification information of the design document and implementation should be described in the vulnerability analysis results.

3.2. Selection of analysis perspective

Not all CWE **Vulnerabilities** are related to security functions and interfaces, so select relevant CWE **Categories** and **Vulnerabilities** for the design and implementation of the "security functions" and "interfaces" identified in Section 3.1. Figure 3.2 shows the work image of Section 3.2.

| | | | |
|--|--|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 12/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

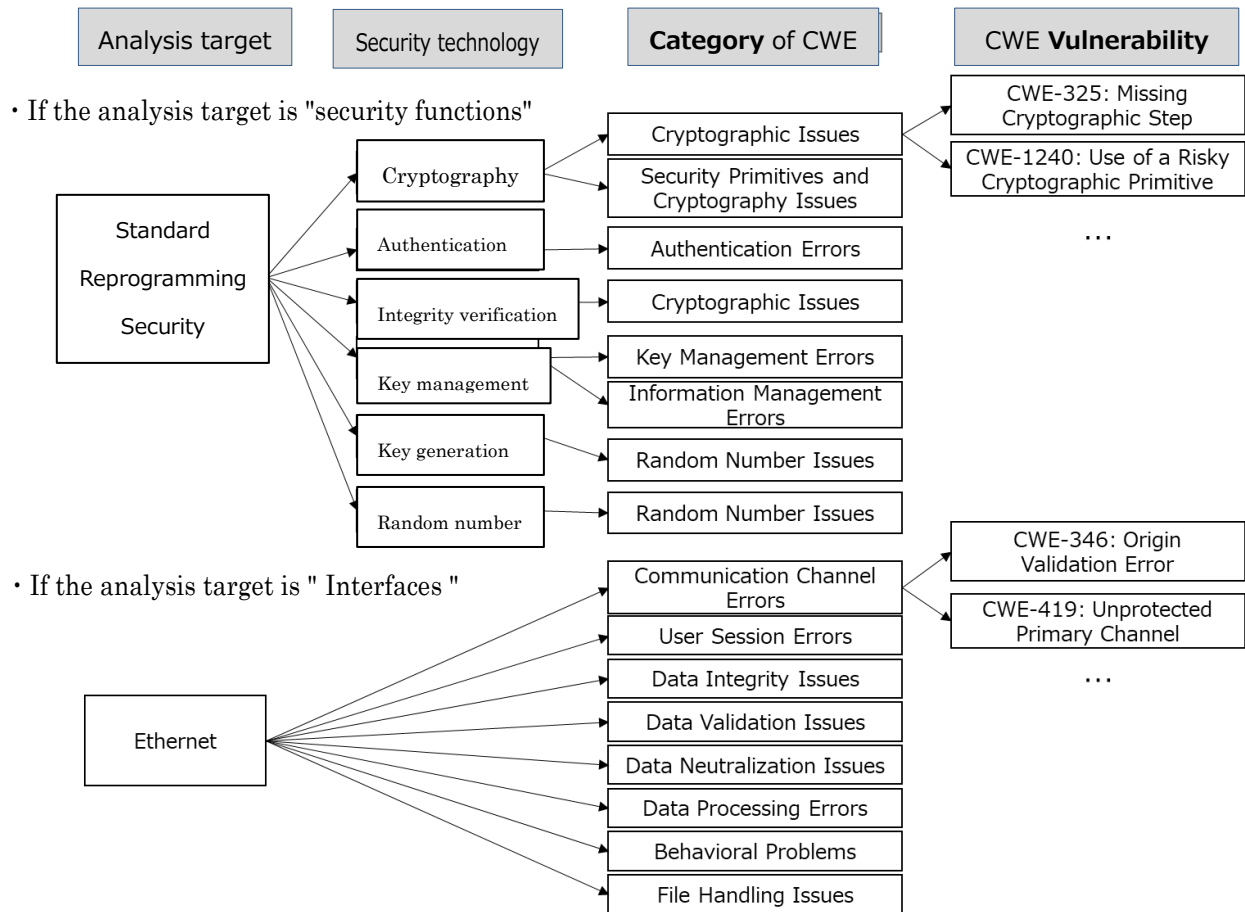


Figure 3.2 Work image of selection of analysis perspective

3.2.1. Selection of CWE Category

Select CWE **Categories** related to security functions and interfaces.

3.2.1.1. Selection of CWE Category for security functions

This section shows how to select of CWE **Categories** for security functions.

In order to be able to link with the CWE **Category**, after decomposing security functions into security technology, select the CWE **Category** corresponding to the security technology.

(1) Decomposing security functions into security technology

Decompose security functions into security technologies with reference to the applicable criteria in Table 3.3. The security technology in Table 3.3 is a grouping of CWE **Categories** related to security technology from all CWE **Categories**.

| | | | |
|--|--|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 13/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

Table 3.3 List of security technologies

| Security technology | Applicable criteria |
|------------------------|--|
| Cryptography | In the case of implementing a cryptographic algorithm, or In the case of using a cryptographic algorithm for encryption/hash |
| Authentication | In the case of using a authentication |
| Integrity verification | In the case of verifying the integrity of a cryptographic signature |
| Key management | In the case of giving/receiving/storing keys |
| Key generation | In the case of generating keys |
| Password | In the case of giving/receiving/storing passwords |
| Random number | In the case of generating random numbers |
| Privilege management | In the case of setting and processing permissions, such as assigning access permissions and defining user groups |

The procedure for each “Type of analysis target” shown in Table 3.2 is shown below.

- A) Design and implementation of specifications issued by the department responsible for security.

Selection results of CWE **Category** are shown below. (※)

- Appendix1.

(※) The specification does not specify a specific implementation method for security functions, and the implementation method may be determined during the design and implementation process. Confirm whether there is a security technology corresponding to Table 3.3 in the implementation method newly determined in the design and implementation process. For example, if the specification specifies "Authentication" and C&R authentication is applied as the authentication method during the design and implementation process, it is necessary to specify the security technology of "Random number" for challenge generation and " Cryptography " for response generation.

- B) Design and implementation of specifications issued by the departments other than responsible for security

Decompose into security technologies with reference to Table 3.3.

| | | | |
|--|--|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 14/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

C) Design and implementation of security functions applied as vulnerability countermeasures

Decompose into security technologies with reference to Table 3.3.

(2) Selection of CWE **Category** related to security functions

Select CWE **Views** and CWE **Categories** related to the security technology selected in (1). Refer to Table 3.4 for the correspondence between security technologies and CWE **Categories**.

Table 3.4 Correspondence between security technologies and CWE Categories

| Security technology | CWE View | CWE Category |
|------------------------|----------|--|
| Cryptography | SW | Cryptographic Issues |
| | HW | Security Primitives and Cryptography Issues |
| Authentication | SW | Authentication Errors |
| Integrity verification | SW | Cryptographic Issues |
| Key management | SW | Key Management Errors |
| | SW | Information Management Errors |
| Key generation | SW | Random Number Issues |
| Password | SW | Credentials Management Errors |
| | SW | Information Management Errors |
| Random number | SW | Random Number Issues |
| Privilege management | SW | Permission Issues |
| | SW | Privilege Issues |
| | SW | Authorization Errors |
| | SW | Business Logic Errors |
| | HW | Privilege Separation and Access Control Issues |

3.2.1.2. Selection of CWE Category for interfaces use case

This section shows how to select a CWE **Category** for an interface.

Interfaces are divided into communication functions and data processing as shown in Figure 3.3. Select the relevant CWE **Category** for the communication function and data processing of each interface by referring to Table 3.5.

| | | | |
|--|--|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 15/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

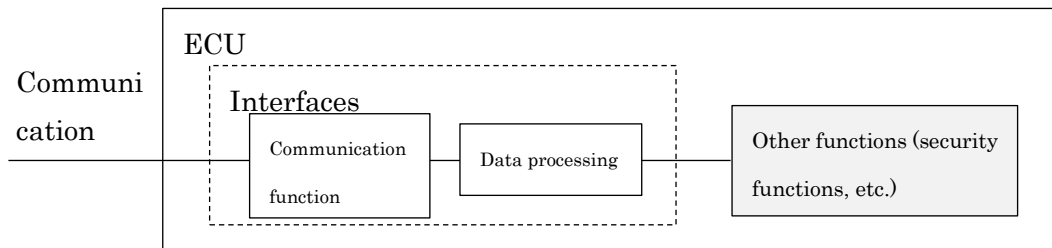


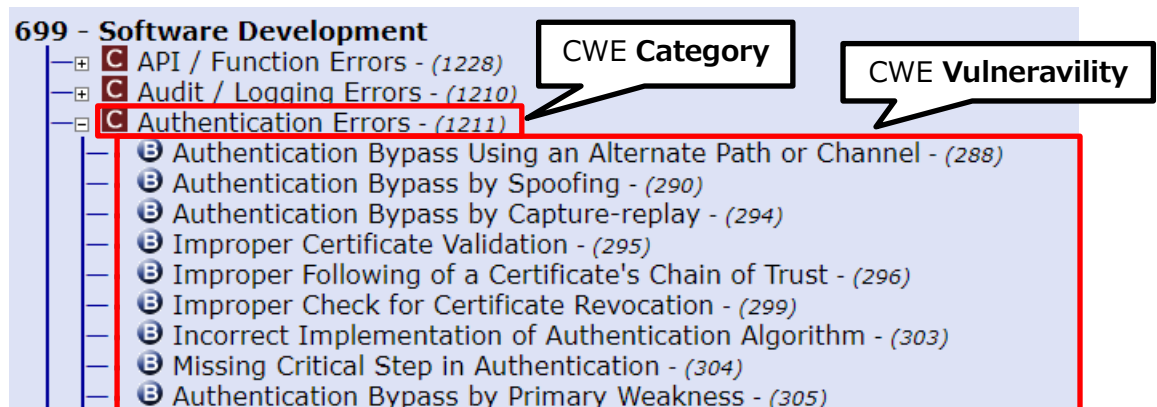
Figure 3.3 Interface composition

Table 3.5 Correspondence between interfaces and Categories

| Target | Explanation | CWE View | CWE Category |
|------------------------|--|----------|------------------------------|
| Communication function | ECU-external or HW-level communication functions (e.g. Ethernet, JTAG) | SW | Communication Channel Errors |
| | | SW | User Session Errors |
| Data processing | Processing received data and code (e.g. code download) | SW | Data Integrity Issues |
| | | SW | Data Validation Issues |
| | | SW | Data Neutralization Issues |
| | | SW | Data Processing Errors |
| | | SW | Behavioral Problems |
| | Working with files and paths (e.g. file path reference processing) | SW | File Handling Issues |

3.2.2. Selection of CWE Vulnerability

Understand CWE **Vulnerabilities** belonging to the selection of CWE **Category** in Section 3.2.1. Developer can confirm CWE **Vulnerabilities** by displaying the **View** and selecting the CWE **Category**. An example is shown in Figure 3.4.



| | | | |
|--|--|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 16/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

Figure 3.4 Confirmation example of CWE Vulnerability linked to CWE Category (CWE-1211)

3.2.3. Excluding CWE Vulnerability that does not require analysis

Among the CWE **Vulnerabilities** selected in Section 3.2.2, the vulnerabilities in Table 3.6 may be excluded from the analysis perspective of view.

Table 3.6 Types of vulnerabilities that can be excluded from an analytical perspective

| Vulnerability type | Excludable reason |
|---|--|
| Vulnerabilities not directly related to security | Exploitation of the CWE Vulnerability alone does not affect security, and it is sufficient to detect vulnerabilities directly related to security and take countermeasures. |
| Vulnerabilities for which countermeasures are required in the Requirements Specification of Common Vulnerability Countermeasure | Vulnerability countermeasures have already been taken. |

3.2.3.1. Excluding vulnerabilities not directly related to security

Among CWE **Vulnerabilities**, if the "Ordinality" of the "Weakness Ordinalities" item is "Indirect", it can be judged that the vulnerability is not directly related to security. An example is shown in Figure 3.5.

| ▼ Weakness Ordinalities | |
|-------------------------|--|
| Ordinality | Description |
| Indirect | (where the weakness is a quality issue that might indirectly make it easier to introduce security-relevant weaknesses or make them more difficult to detect) |

Figure 3.5 Examples of CWE Vulnerabilities not directly related to security

3.2.3.2. Excluding vulnerabilities for which countermeasures are required in the Requirements Specification of Common Vulnerability Countermeasure

By comparing the description of the CWE **Vulnerability** with the countermeasure requirements described in the Requirements Specification of Common Vulnerability Countermeasure, the same CWE **vulnerability** can be excluded. CWE **Vulnerabilities** that can be excluded may refer to the following.

| | | | |
|--|--|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 17/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

• Appendix2. Correspondence Table of CWE **Vulnerabilities** and Requirements Specification of Common Vulnerability Countermeasure

3.3. Vulnerability analysis

In the vulnerability analysis, confirm whether the design and implementation of the analysis target identified in Section 3.1 have the CWE **Vulnerability** selected in Section 3.2. The vulnerability analysis method is shown below.

3.3.1. Understanding CWE Vulnerability

Although it is necessary to understand the CWE **Vulnerability** before performing vulnerability analysis, the contents of the CWE **Vulnerability** can be understood from the items of "Description", "Extended Description", and "Demonstrative Example" in Table 2.3. But, SW **View** and HW **View** vulnerabilities are composed mainly of base attribute vulnerabilities that do not depend on specific resources or technologies, so it may be difficult to understand specific vulnerabilities. If you want to understand specific vulnerabilities that depend on technologies or resources, display the tree structure of the Research Concepts **View** and confirm the CWE **Vulnerabilities** that are subordinate to the CWE to be confirmed. (See Figure 3.6).

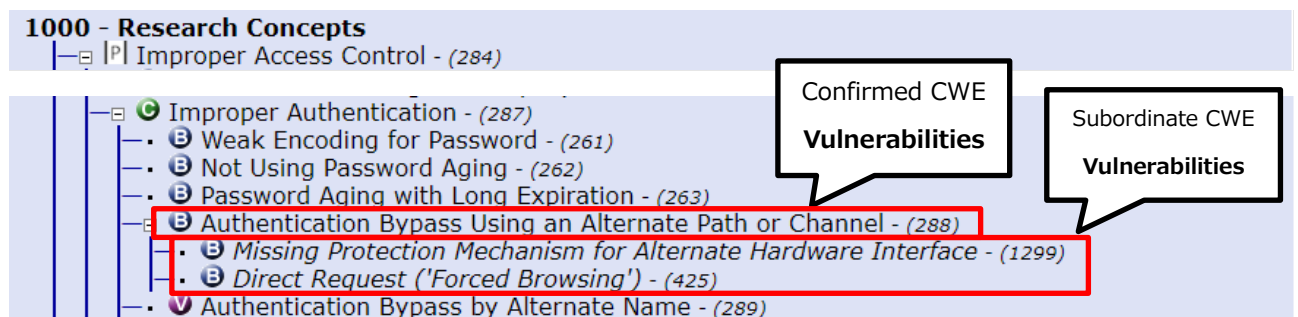


Figure 3.6 Example of a survey using Research Concepts (CWE-288)

3.3.2. Confirm for vulnerability

Confirm for CWE **Vulnerabilities** in the design and implementation to be analyzed. As a result of vulnerability analysis, describe the presence or absence of vulnerabilities (not applicable/applicable),

| | | | |
|--|---|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 18/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

the necessity of countermeasures, and the reason for the judgment.

If there are no vulnerabilities, the presence or absence of vulnerability is “not applicable”. If there are vulnerabilities, the presence or absence of vulnerability is “applicable”, it is necessary to consider whether countermeasures are necessary. Note that when countermeasures are taken in design and implementation, new vulnerabilities may be introduced, so it is necessary to re-analyze vulnerabilities in the design and implementation of countermeasures. Also, if a vulnerability exists but it can be determined that it cannot be exploited in the system or ECU environment, it is conceivable that no countermeasures will be taken. (Example: There is no interface to exploit the vulnerability, or exploitation of the vulnerability requires a certain level of advanced attack capability, etc.)

| | | | |
|--|--|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 19/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

Appendix1. Correspondence table between security specifications and CWE Categories

| Specification | Security technology | CWE Category |
|---|------------------------|--|
| Requirements Specification of Multi-Layered Separation | Privilege management | Permission Issues |
| | | Privilege Issues |
| | | Authorization Errors |
| | | Business Logic Errors |
| | | Privilege Separation and Access Control Issues |
| Requirements Specification of 2 nd Layer Message Filtering | Integrity verification | Cryptographic Issues |
| | Privilege management | Permission Issues |
| | | Privilege Issues |
| | | Authorization Errors |
| | | Business Logic Errors |
| Requirements Specification of Message Filtering | Cryptography | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | Authentication | Authentication Errors |
| | Key management | Key Management Errors |
| | | Information Management Errors |
| | Privilege management | Permission Issues |
| | | Privilege Issues |
| | | Authorization Errors |
| | | Business Logic Errors |
| | | Privilege Separation and Access Control Issues |
| Requirements Specification of Online Client Authentication | Cryptography | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | Authentication | Authentication Errors |
| | Password | Credentials Management Errors |
| | | Information Management Errors |
| | Random number | Random Number Issues |
| | | Permission Issues |

| | | | |
|--|---|-----|-----------------------------------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 20/22 |
| Application: ECU of In-Vehicle network | | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a |

| Specification | Security technology | CWE Category |
|---------------|-------------------------|--|
| | Privilege management | Privilege Issues |
| | | Authorization Errors |
| | | Business Logic Errors |
| | | Privilege Separation and Access Control Issues |

| | | | |
|--|---|-----|-----------------------------------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 21/22 |
| Application: ECU of In-Vehicle network | | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a |

| Specification | Security technology | CWE Category |
|---|------------------------|--|
| Requirements Specification of Standard Reprogramming Security | Cryptography | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | Authentication | Authentication Errors |
| | Integrity verification | Cryptographic Issues |
| | Key management | Key Management Errors |
| | | Information Management Errors |
| | Key generation | Random Number Issues |
| Requirements Specification of Center Communication Security | Cryptography | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | Authentication | Authentication Errors |
| | Integrity verification | Cryptographic Issues |
| | Key management | Key Management Errors |
| | | Information Management Errors |
| Requirements Specification of Wireless Communication Security | Cryptography | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | Authentication | Authentication Errors |
| | Integrity verification | Cryptographic Issues |
| | Key management | Key Management Errors |
| | | Information Management Errors |
| | Key generation | Random Number Issues |
| | Password | Credentials Management Errors |
| | | Information Management Errors |
| | | Privilege Separation and Access Control Issues |
| | Privilege management | Permission Issues |
| | | Privilege Issues |
| | | Authorization Errors |
| | | Business Logic Errors |

| | | | |
|--|---|-----------------------------------|-------|
| In-Vehicle Network | Requirements specification of vulnerability countermeasure for ECU | | 22/22 |
| Application: ECU of In-Vehicle network | No. | SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | |

| Specification | Security technology | CWE Category |
|--|------------------------|---|
| Requirements Specification of Message Authentication for FULL FV | Cryptography | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | Integrity verification | Cryptographic Issues |
| Requirements Specification of Key Information Gateway | (Not applicable) | - |
| Requirements Specification of Key Management Master | Cryptography | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | Key management | Key Management Errors |
| | | Information Management Errors |
| | Key generation | Random Number Issues |
| | Random number | Random Number Issues |
| Requirements Specification of In-vehicle Key Management Slave | Cryptography | Cryptographic Issues |
| | | Security Primitives and Cryptography Issues |
| | Integrity verification | Cryptographic Issues |
| | Key management | Key Management Errors |
| | | Information Management Errors |