山本レポート：システム安全性向上―世界の最前線（3）

セキュリティを考慮した安全性

国立大学法人 名古屋大学
大学院 情報学研究科
教授　山本 修一郎
博士（工学）

IEEE COMPUTER 誌の 8 月号に、Bloomfield 氏 がセキュリティを考慮した安全性 (SIS, Security Informed Safety) について寄稿していたので紹介したい[1]。彼は Adelard 社の創設者で、City, University of London の教授でもある。

SISのねらい

SIS のねらいは、安全性技術者（safety engineer）がセキュリティについての認識を深めることと、そのためにプロセスと知識を提供することである。Bloomfield らは、政府の支援を受けて、鉄道分野と自動車分野における codes of practice (CoPs) を開発した。セキュリティエンジニアと安全性エンジニアの協働作業プロセスを作成した。このプロセスは、安全性技術者のためにセキュリティ知識を提供するとともに、セキュリティ技術者に安全性知識を提供している。製品とサービス、活動のセキュリティ関連リスクが、安全性について受け入れ不能なリスクを引き起こさないことを CoP で確認する必要がある。

また、相互依存性が考慮され、単一または少数の要素の障害が広範囲に影響する可能性がある場合についても、システム論的リスクを管理するための推奨事項を提示している。CoP のもう一つの重要な側面は、トランスポーテーション・エコシステムを構成するすべての組織がトランスポーテーションシステムのユーザーと社会全体に対して安全性リスクを最小化することについてより良い活動をすべきだという認識である。換言すれば、特定の組織に閉じて安全性リスクを最小化するだけでは不十分だという認識が重要である。

CoPの作成

Bloomfield らによる CoP の作成では、次の方針を設定している。

[方針1] 既存の関連原則と、SISについての考察およびアセスメント経験の分析に基づく一般原則を収集

[方針2] 注釈とコメントを提供することにより、一般原則を鉄道と自動車分野に適応

[方針3] CoPの適用について、詳細説明とガイダンスからなる支援情報を付録として提供

CoP の開発では、以下に示すようにトップダウン手法とボトムアップ手法を組み合わせている。

◆トップダウン手法

CoP の一般原則を確認するために、CAE(Claims-Argument-Evidence) ケースを作成している。CAE ケースでは、原則が産業界の高水準ビジョンをどのように支援するかを示すことができる。CAE ケースでは、ゴールを下位ゴールに段階的に分解する。また最下位ゴールを証拠によって保証することにより、最上位のゴールが成立することを論理的に確認できる。

トップダウン手法では、まずトランスポーテーション分野の包括的なビジョンから始める。たとえば、鉄道システムが安全でセキュアであると誰もが確信しているように世界をみている。このことから、最上位の主張を導くことができる。

「鉄道移動に対して、サイバーセキュリテイの課題が、受け入れ不可能なリスクを発生することはないという正当化された確信 (confidence) がある」

次いで、アシュアランスについての CAE 手法を用いて、原則の集合によって支持される下位の主張のネットワークを作成できる。このようにして作成された CAE では、以下のような主張から構成されている。

- 現在と将来の組織的側面
- 資源と競争優位性
- 開発サイクル
- 保証ケース
- 製品の将来の振る舞い
- 他のステークホルダの確信

◆ボトムアップ手法

ボトムアップ手法の場合、重要安全分野についての既存のセキュリティおよび安全性に焦点をあてた原則

表 1　CoP で参考にした資料

組織	文書	URL
英国政府	The Key Principles of Cyber Security for Connected and Automated Vehicles	https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles.
EU Agency for Network and Information Security	Cyber Security and Resilience of Smart Cars: Good Practices and Recommendations	https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
US National Highway Traffic Safety Administration	Cybersecurity for Modern Vehicles4	https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf.
UK National Cyber Security Centre	EU Network and Information Security (NIS) Directive guidance	https://www.ncsc.gov.uk/guidance/nis-guidance-collection.
UK Office for Nuclear Regulation	Security Assessment Principles for the Civil Nuclear Industry	http://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf.

表 2　CoP の構成

章	内容	原則の分類
1. セキュリティポリシ、組織、文化	既存の安全性ポリシーと組織文化へのセキュリティの影響	組織
2. セキュリティを考慮した開発プロセス	システムライフサイクル工程におけるセキュリティ要求	開発プロセス
3. 効果的な防御の維持	運用時のセキュリティ保証	運用プロセス
4. インシデント管理	セキュリティインシデントの管理	運用プロセス
5. セキュア安全性設計	システム設計におけるセキュリティ開発	設計
6. 安全でセキュアな世界への貢献	トランスポーテーションエコシステムのセキュリティを向上するための外部組織との協調と連携	組織

とガイダンスから出発する。たとえば、表 1 のような文書がある。

これらの文書で記述されている原則の共通性分析に基づいて、共通する課題を抽出できる。これらの共通課題をトップダウン手法の推奨ガイドラインと比較することにより、重要項目が適切に網羅されていることを確認できる。この結果、①組織的セキュリティ原則、②製品あるいはプロジェクトライフサイクル原則、③設計原則という 3 種類の原則があることを明らかにしている。

CoP の内容

作成された CoP の構成を表 2 に示す。CoP の章は、1. セキュリティポリシ、組織、文化、2. セキュリティを考慮した開発プロセス、3. 効果的な防御の維持、4. インシデント管理、5. セキュア安全性設計、6. 安全でセキュアな世界への貢献からなる 6 章となっている。

まず、第 1 章では既存の安全性ポリシーと組織文化へのセキュリティの影響について述べている。2 章では、システムライフサイクル工程におけるセキュリティ要求について説明している。3 章では、効果的に防御を維持するために、運用時のセキュリティ保証について述べている。4 章では、セキュリティインシデントの管理プロセスについて述べている。5 章では、システム設計におけるセキュリティ開発について述べ、セキュア安全性設計を明らかにしている。6 章では、トランスポーテーション・エコシステムのセキュリティを向上するための外部組織との協調と連携について述べ、安全でセキュアな世界への貢献のあり方を明らかにしている。

なお、表 2 では 3 種類の原則との対応関係も示した。

CoP の各章では、具体的な推奨対策を説明している。推奨対策では、アウトカムベースですべきこととすべきでないことについて対策内容と関連資料へのノートが示されている（表 3）。

表 3　CoP 6 章の内容例

話題	内容	ノート
リスク管理	より広いトランスポーテーションシステムとより一般的な社会を分析して、製品やサービス障害が引き起こすリスクを管理すべきである	注1：製品やサービスの安全性関連特性と適用される法制度に依存する 注2：トランスポーテーション能力の低下などが社会的リスクに含まれる
相互運用性	組織が提供する製品・サービスは産業標準について適切な水準で準拠すべきである	―
情報共有	製品・サービスについて、適切な設計情報と保証情報を提供することにより、顧客がセキュリティを評価できるようにすべきである	知財権を保護するために、詳細設計情報などの機密情報を非公開についての合意の下で提供すべきである
連携	適切な組織と脅威を軽減するためのプラクティスを共有すべきである	関連組織には政府機関、産業団体などが含まれる
国際的な課題	サプライチェインを構成する他国との連携を考慮すべきである	サプライチェインリスク関連資料 Protection of National Infrastructure (https://www.cpni.gov.uk/supply-chain) National Cyber Security Centre (https://www.ncsc.gov.uk/guidance/supply-chain-security)

まとめ

本稿で紹介した、CoP について、まとめると以下の 3 点になる。

- CoP は、一般原則に基づくトップダウン手法と実在のガイドラインに基づくボトムアップ手法の両面から構成すべきである。
- セキュリティを考慮した安全設計のための CoP が対象とするトランスポーテーションシステムは、SoS である。
- 個別システムに閉じた安全設計だけでなく、相互接続性を考慮した広範囲の安全性リスクについても保証する必要がある。

【参考文献】
[1] Robin Bloomfield, Peter Bishop, Eoin Butler, Robert Stroud, Security-Informed Safety: Supporting Stakeholders with Codes of Practice, IEEE COMPUTER, August 2018, pp.60-65

＜システム安全性のことなら下記へ＞
yamamotosui@icts.nagoya-u.ac.jp