セキュリティ・安全分析の GSN 活用による改善

櫻庭　孝弘† 和田　学†

Improvement of safety analysis and security analysis using GSN

Sakuraba Takahiro, Wada Manabu

ねらい　システムのセキュリティ脅威からの保護や、システムに関する危害の防止のための対策を適切に講じるためには、セキュリティ脅威・ハザード分析やリスク評価を抜け洩れなく実施し、合意形成することが重要である。GSN[1]を用い従来分析手法を改良することで、網羅性および合意形成に至るまでの作業工数を削減することができたので、本稿ではその効果を報告する。

キーワード　安全分析、セキュリティ分析、GSN

Target: This abstract is to provide our experience for improving Security Analysis and Safety Analysis using GSN

Keywords: Safety Analysis, Security Analysis, GSN

1．想定する読者・聴衆

本書および本発表が想定する読者・聴衆は、セキュリティまたは安全性が要求されるシステムやソフトウェアの企画者・設計者・開発者など、脅威分析やリスクアセスメントの実施・レビューに携わる者を想定する。

2. 背景

制御システム分野では、機能安全対応とセキュリティ対応は必須になりつつある。セキュリティや安全性の保証を如何に効率的に実施できるかが競争力を左右する重要課題の一つである。

現在セキュリティ脅威分析に用いられる手法は Microsoft 社の脅威モデリング(Threat Modeling)手法[2]やアタックツリー(Attack Tree)[2]分析など、安全分析の手法は HAZOP[3]、フォールトツリー分析(FTA)[3]、FMEA[3]などが主流である。

しかし、これらの手法を用いても、網羅性と生産性の両立は難しく、適切な脅威・ハザードを網羅的に抽出するためには、経験豊かな有識者が時間を掛けてレビューをする必要があった。

3. 課題

図 1、図 2 は無線通信をサポートする組込み機器の脅威分析を実施した例である。

図 1 では、アタックツリーを用い、トップダウンでセキュリティ脅威毎に可能性のある攻撃手法を網羅的に洗い出すことを試みたものである。作業者によって挙げる項目やその順序が全く異なるツリーができ、網羅性も不十分、妥当性の判断もしづらいという問題が出た。

図 2 はその対策として、データとセキュリティ特性、攻撃機会や手段などの組合せを表形式で列挙する方式に変更したものである。組み合わせ項目数は膨大になり、一見網羅性が改善されたように見える。しかし、実際に各項目を逐一レビューすると項目毎の攻撃可能性の列挙不足が指摘されるなど網羅性の解消には至らず、一方で非常に多くの時間を要した。

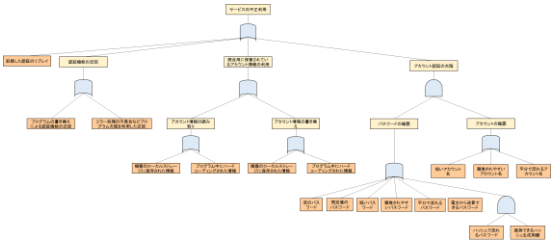

図 1 アタックツリーによる攻撃可能性分析結果の例

Fig1. Attack tree example

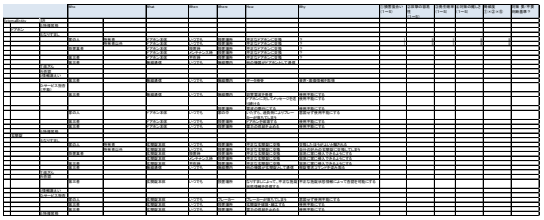

図 2 表形式での条件組み合わせによる脅威抽出例

Fig2. Threat analysis with tabular form

また安全分析においても同様である。図 3 は農業機械向けのハザード抽出例である。FTA で条件漏れがでないよう、機能と場所・状態・危害の対象等の組み合わせを表形式で列挙し、さらに各項目に HAZOP のガイドワードを組み合わせて機能不全を洗い出すよう工夫したが、9 千件近い条件とガイドワードの組合せがあり、

非常に多くの工数を要した。

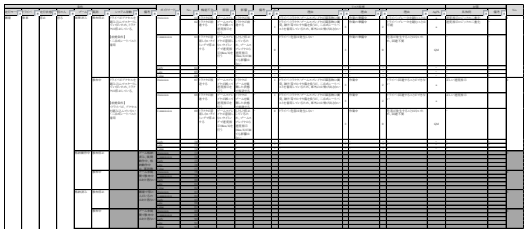

図 3 表形式でのハザード抽出例

Fig3. Hazard analysis with tabular form

Attack Tree や FTA は、列挙項目の妥当性や網羅性が判断しづらいことが問題である。一方、網羅性をあげようとして単純に条件の組合せを表形式で列挙すると、組合せの数が膨大になってしまう。これにより、単純に検討項目数が増え多大な工数が必要になること、観点毎の列挙項目の妥当性を確認するための一覧性が損なわれることが課題である。

4. 提案・実験

上記課題を解決するために、GSN を用いて項目列挙の観点や前提条件などを明らかにしつつトップダウンで条件の組合せを検討する手法を提案する。

GSN はトップに提示されたゴールについて、それを達成する条件や思考を可視化するための記法である。

前提条件を明記しつつサブゴールを展開する観点の順序を分析対象に合わせて適切に設定することで、検討すべき条件組合せを必要最低限に絞り込むことができ、レビュー性も向上する。

例えば、セキュリティ分析の例では組み込み機器が対象であれば、製品ライフサイクル毎にユースケースや攻撃サーフェース、攻撃機会などが異なる。これを考慮し最初に製品ライフサイクルを列挙し、ライフサイクル毎に攻撃条件を検討することで考慮すべき条件の組合せを絞り込むことができる。

また、安全分析の例では、分析対象のシステムが利用される場所によって、考慮すべき危害を受ける対象を限定することができる。

図 4 の左が従来手法を用いた分析、右が提案手法を用いた分析の例であるが、従来手法では分析の観点や根拠が不明確であったものが、提案手法では GSN の、Strategy や Context として明示されている。

図 5 は組み込み機器のセキュリティ脅威分析で用いたツリーノード展開の観点の適用順の例である。

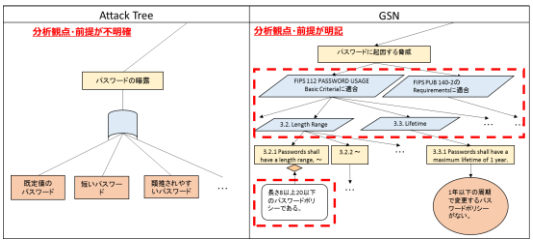

図 4 Attack Tree と GSN の比較

Fig4. Comparison of Attack Tree and GSN

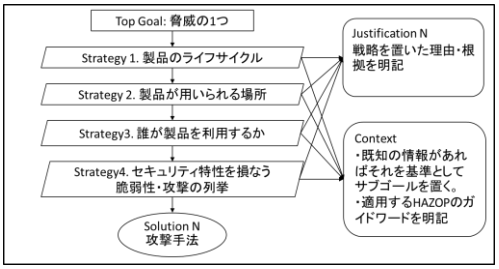

図 5 組み込み機器の GSN を使った分析例

Fig5. Example of analysis of embedded system using GSN

5. 効果

GSN を用いることで、ツリーの展開の段階毎にその観点や前提・証拠を明示することができ、レビューや結果の合意の形成が効率的に行えるようになった。

また、列挙観点とその順序および前提の置き方は分析ノウハウそのものであると考えるが、GSN はこのノウハウを可視化でき、それによりノウハウ自体の検討・改善に役立った。

表 1 に農業機械の 1 つであるブームスプレーヤに対しての安全分析に従来手法を用いた場合と GSN を用いた場合の実施結果の比較を示す。”従来手法”として載せているのは機能安全経験 4 年の 1 名、初学者 3 名のチームで、図 3 に示す FTA 的な表形式での分析を行った結果である。一方、”GSN を用いた分析”は、機能安全経験 1 年 1 名が本書の分析手順によって分析をした結果である。

従来手法では抽出できなかったハザードが 5 つ抽出でき、網羅性が約 1.7 倍向上した。また、所要時間は 1/3 以下に削減できた。

表 1 安全分析結果の比較表

Table 1. Comparison of safety analysis results

	従来手法	GSN を用いた分析
抽出ハザード数	7	12
所要時間	360 hr	100 hr

†株式会社ヴィッツ
WITZ Corporation, NAGOYA PARK PLACE BLDG.
13-1, SAKAE2-CHOME, NAKA-KU, NAGOYA, 460-0008, JAPAN
E-mail: sakuraba@witz-inc.co.jp, wada@witz-inc.co.jp

6. まとめ(今後の課題・謝辞等)

セキュリティ分析および安全分析において、下記のような分析手法の改善を行うことで、網羅性・生産性を共に改善することができた。

① 分析対象に合わせた分析観点の検討の実施

分析対象において検討するべき観点、検討不要な観点を整理する。これにより、不要な分析作業を省略できる。

② 分析観点の適用順番の工夫

例えば、図 5 に示した組み込み機器の場合、製品のライフサイクルを最初の分析観点としてあげている。

組み込み機器においては、その機器の攻撃タイミングや関わる人物等が製品のライフサイクルによって変わってくる。そのため、先にライフサイクルで分けることで、分析の重複を避けることができる。

このように、どのような順番で観点を適用すればよいか工夫することで、不要な分析作業を省略できる。

③ 分析ガイドラインの利用

①、②が整理された分析ガイドラインに従って分析を進める。これにより、作業の効率化、抜け漏れを防止できる。

④ GSN の表記の利用

GSN の表記法を用いることで、分析における前提や根拠などの議論が明確化できる。これにより、レビュー者が妥当性を確認しやすくなり、工数の削減につながる。

今後は、セキュリティ分析・安全分析対策の網羅性・生産性をより上げるために、分析ガイドラインの改善、他プロダクトのガイドラインの整備に取り組んでいきたい。

7. 用語・文献

文　　献

[1] GSN COMMUNITY STANDARD VERSION 1, http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf

[2] Microsoft Developer Network, Threats and Countermeasures, Chapter 3 Threat Modeling https://msdn.microsoft.com/en-us/library/ff648644.aspx

[3] ISO 26262 におけるソフトウェア安全解析の検討, 株式会社 OTSL http://www.ipa.go.jp/files/000004108.pdf

略 号 一 覧

GSN : Goal Structuring Notation

HAZOP : Hazard and Operability Study

FTA : Fault Tree Analysis

FMEA : Failure Mode and Effects Analysis