脅威分析に基づいた制御システムのセキュリティ向上策の提案

Proposal of security improvement measures for Control System based on threat analysis

竹本和弘・ネットワーク分科会・情報セキュリティ大学院大学

Abstract: There are various information security threats in the control system. In this study, I focus on low information security awareness of control system users and propose a method to improve them. The proposed method aims to deepen the understanding of threats and evoke the necessity of information security measures by structurally identifying the threats occurring in the control system by the control system user using the threat analysis method.

1．研究の背景と目的

【背景】

・近年,プラントで機器制御に用いられる制御システムへのサイバー攻撃が行われており,その脅威と影響の大きさが注目されている

・制御システムにおけるセキュリティ上の最も根本的な課題として,制御システムユーザーの情報セキュリティ意識の低さが挙げられる

【目的】

制御システムユーザーの情報セキュリティ意識を向上させ,制御システムの情報セキュリティレベルの向上を図る

2．研究のアプローチ

制御システムユーザーの情報セキュリティ意識の向上を図る

↓

実際に運用している制御システムが抱えるセキュリティ脅威の認識を深める

↓

脅威分析手法を用いて制御システムのセキュリティ脅威を具体的に識別する

↓

制御システムユーザー向けの脅威分析手法を提案

【脅威分析手法とは】

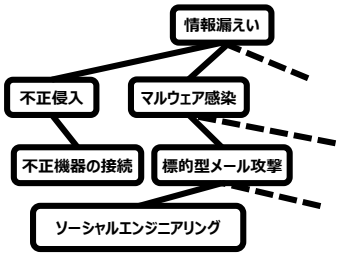
システムの守るべき資産を明らかにし,それら資産に対する脅威を識別して,リスク評価や対策を策定する手法

代表的な脅威分析手法

STRIDE：脅威を６分類で識別

Spoofing(なりすまし)
Tampering(改ざん)
Repudiation(否認)
Information Disclosure(情報漏えい)
Denial of Service(Dos攻撃)
Elevation of Privilege(特権の昇格)

Attack Tree：脅威をツリー状に分解



3．制御システムユーザー向け脅威識別手法の提案

制御システムユーザー向けに簡易化した新たな脅威識別手法(STRIDE-Tree)を提案

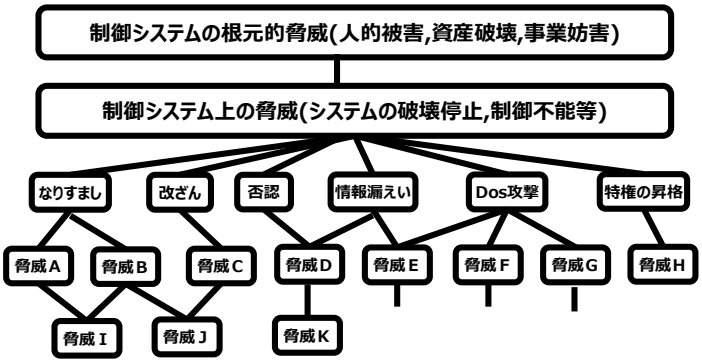


図１　STRIDE-Treeのイメージ

4．提案手法の検証

実際に運用されている制御システムに対してSTRIDE-Treeによる脅威分析を実施

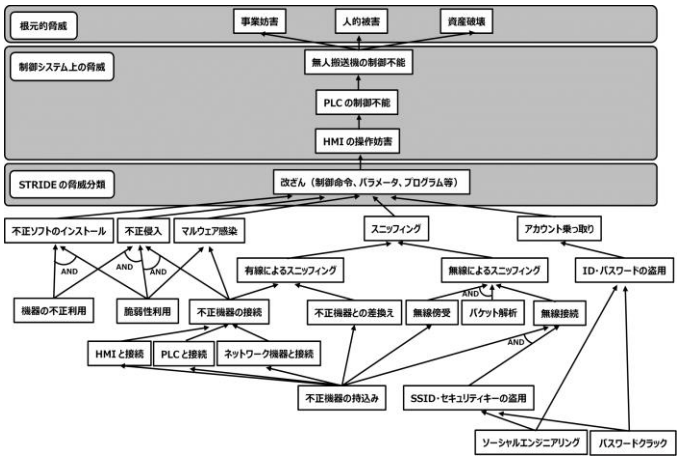


図２　STRIDE-Treeの一例

5．まとめ

本研究では,漠然としか捉えられなかった制御システムの脅威を体系的に識別して明示したことで,制御システムユーザーが直感的に脅威を認識する手法を示した．制御システムユーザーが本提案手法を活用することで,制御システムに対する脅威と情報セキュリティ対策の必要性を能動的に考察するための一助となることを期待する．