社会インフラを支える制御システムセキュリティの標準化動向

Trends on Control System Security Standardization for Social Infrastructure System

山田　勉†
Tsutomu YAMADA†

†株式会社 日立製作所 日立研究所

概要

制御システムにおいてオープンな通信方式や無線技術の採用により，設備機器の運用データなどが外部から盗み見あるいは改ざんされる恐れが高まっている。セキュリティを考慮した製品の導入や，継続的なセキュリティ維持の活動は今後一層重要となる。このような背景の下，標準規格の策定が様々な応用分野において進められており，特に国際標準規格 IEC 62443 が注目されている。

スマートグリッドやスマートシティのような，IT と M2M 制御システムとを融合する応用が求められている今日，無線通信の利用は不可欠である。一方，無線通信を制御システムに利用する際のリスクとして，干渉や妨害による通信途絶（可用性喪失）や，故意に不正なデータが送られる成り済まし（完全性喪失）が想定される。

しかしながら，30 年を超える例もある社会インフラの利用期間において，無線通信を臆することなく使うためには，制御システムのセキュリティを維持する考え方を取り入れ，システム全体でセキュリティを守るアプローチが不可欠と考える。通信の観点からは，有線通信も無線通信も考慮すべき対策は同様である。導入時のみならず，セキュリティ上重要な事象が発生した際には見直しが不可欠である。

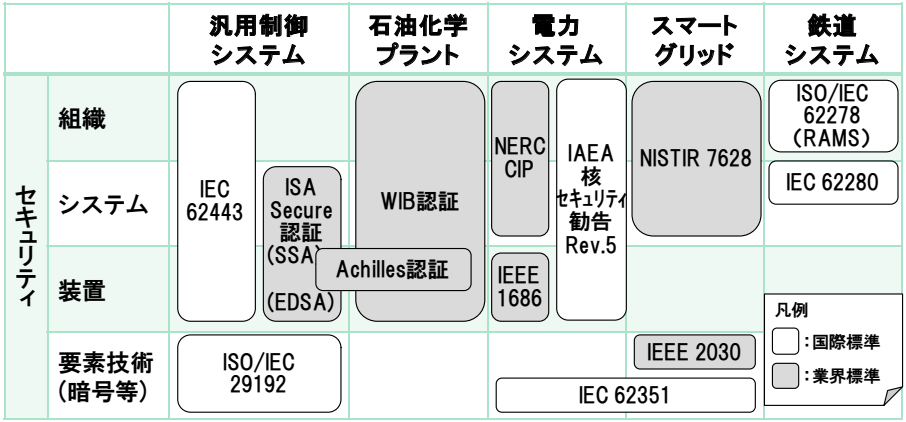

図　制御システムセキュリティ関連規格の概要

Abstract

Due to applying open communication technologies and wireless communication technologies, the anxiety of illegal disclosure of operating data about control system equipments has been arising. To protect control systems from an illegal operation, some security technologies and standards have been introduced. Especially, the international standard of IEC 62443 is the most promising.

To utilize wireless technologies on social infrastructure systems, which may be used over 30 years in some cases, author proposed that wireless technologies should be used in the manner of control system security.