

重要インフラ事業者とその設備関連事業者におけるサイバーセキュリティの意識に関する研究

A Research on Cyber Security Awareness of Critical Infrastructure Operators and their Facility-Related Operators

佐藤 誠之・法制・倫理分科会・情報セキュリティ大学院大学

Abstract: At a time when critical infrastructure field has become the target of cyberattacks, only critical infrastructure operators are highly aware of cyber security, and even if countermeasures are taken, critical infrastructure cannot be protected. It is necessary to recognize cyber security as "Risks associated with business activities" and take appropriate measures for critical infrastructure operators and facility-related operators that are part of their supply chain. In this research, we conducted a survey on the awareness of cyber security among the top management of critical infrastructure operators and facility-related operators by using public information. In addition, we conduct surveys of changes in the content of Cybersecurity over time and hold hearings with business operators, and propose that "Integrated efforts of critical infrastructure operators and facility-related operators" and "Specific information disclosure on cyber security of critical infrastructure operators" are effective for business operators and fields that do not consider Cybersecurity as "Risks associated with business activities".

1. 背景

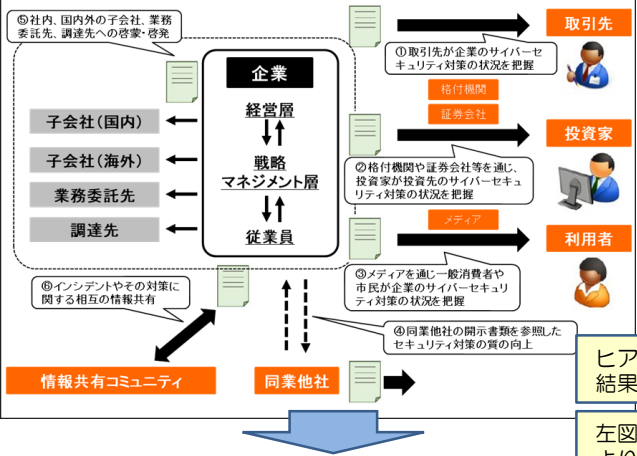
- 重要インフラへのサイバー攻撃の懸念
- サプライチェーンリスクの高まり

2. 研究手法

- 公開情報により経営層のサイバーセキュリティに関する意識を調査（経年変化も確認）
- 重要インフラ事業者とそのサプライチェーンの一部である設備関連事業者に着目
- 一部、事業者へのヒアリングを実施

有価証券報告書の「事業等のリスク」項目で、サイバーセキュリティに関する記載の有無を確認
「情報通信」、「鉄道」、「電力」、「ガス」の4分野に絞り、重要インフラ事業者と設備関連事業者を31社選定し調査を実施

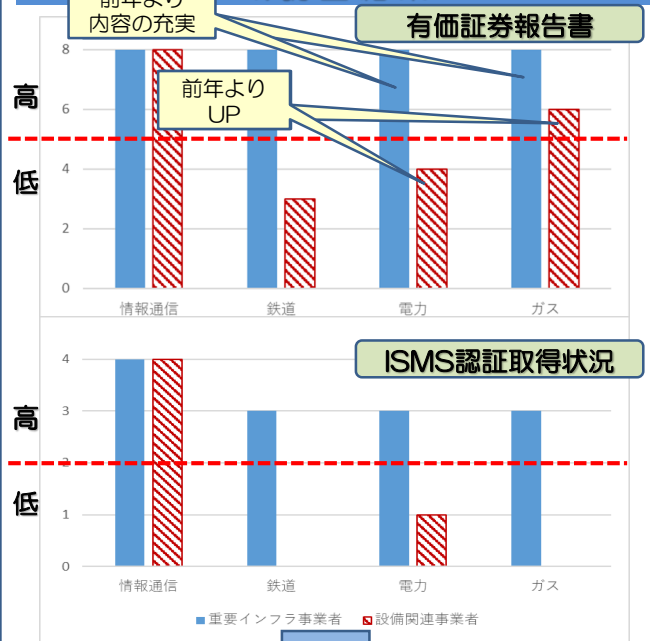
3. サイバーセキュリティに関する情報開示



情報開示によるメリット有

法改正、サイバーセキュリティ対策情報の開示の公表等もあり、情報開示の充実が求められている

4. 調査結果



事業者種別	サイバーセキュリティに関する意識
重要インフラ事業者	⇒ 高
設備関連事業者	分野や事業者によって差あり
情報通信・ガス	⇒ 高
電力・鉄道	⇒ 低

5. サイバーセキュリティ意識向上に向けた提言

- 重要インフラ事業者と設備関連事業者の一体となった取り組み（指導、情報共有等）
- サイバーセキュリティに関する具体的な情報開示の推進

今後の研究・課題

- サンプル企業を拡大しての調査
- 提言に関する効果の検証