4X-01

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

佐藤　誠之†　　藤本　正代†
情報セキュリティ大学院大学†

1. はじめに

重要インフラは、国民の生活や社会経済活動に必要不可欠であり、一旦そのサービスが停止に陥ると多方面に甚大な影響を与えることが想定される。この重要インフラ分野がサイバー攻撃のターゲットになっている昨今[1]、重要インフラ事業者だけセキュリティ意識が高く、対策を施しても重要インフラは守れない。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ついても、「事業等のリスク」としてサイバーセキュリティを認識し、適切な対策をとる必要があると考える。本研究では公開情報を用い、重要インフラ事業者とその設備関連事業者の経営層のセキュリティ意識について調査を行い、その関連性や分野別の違い等について分析を行った。

2. 重要インフラと設備関連事業者

内閣サイバーセキュリティセンター（以下、「NISC」という）が作成した重要インフラの情報セキュリティ対策に係る第4次行動計画[2]の中では、「重要インフラ分野」として、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット及び石油の14分野を特定している。

本研究では、この14分野の中から特に重要で設備との関わりが深い、情報通信、鉄道、電力、ガスの4分野に絞って調査を行った。

また本研究において、設備関連事業者とは重要インフラ事業者の設備に関する構築、保守を行っている事業者と定義した。

3. 研究手法

本研究では重要インフラ事業者とその設備関連事業者の経営層のサイバーセキュリティ意識を調査するにあたり、そのデータとして公開情報を使用する。

NISCの平成28年度企業のサイバーセキュリティ対策に関する調査報告書[3]によると、経営層が日頃から特に重要な問題としてサイバーセキュリティに取り組んでいる企業では有価証券報告書等の公開資料を用いた情報発信も積極的に行っているとしており、その手法を用いた。

公開情報としては、有価証券報告書の他、コーポレートガバナンス報告書、CSR・サステナビリティ報告書等あるが、本研究で使用する公開情報として、上場企業で作成が必須な有価証券報告書を選定した。　最新の有価証券報告書より、「事業等のリスク」の項目で、サイバーセキュリティに関する記載の有無で下記の通り評価を実施した。

表1 サイバーセキュリティの意識に関する評価

評価	有価証券報告書 「事業等のリスク」の記載状況
○	サイバーセキュリティに関する記載がある。 キーワード：サイバー/サイバー攻撃（アタック）、セキュリティ/情報セキュリティ、漏洩（漏えい）/情報漏洩（漏えい）/情報の漏洩（漏えい）、ウイルス（ウィルス）/コンピュータウイルス（ウィルス）、不正アクセス（侵入）/不正なアクセス（侵入）、ハッキング、流出/情報流出/情報の流出 ※物理的なセキュリティ、コロナ関連ウイルス、インサイダー関連の漏洩は除く
△	「事業等のリスク」の箇所にセキュリティに関する記載はないが、その他の箇所でセキュリティに関する記載がある。
×	セキュリティに関する記載なし。

また有価証券報告書の調査に加え ISMS 認証の取得状況についても調査を実施した。

4. サイバーセキュリティ情報の開示

NISCの平成28年度企業のサイバーセキュリティ対策に関する調査報告書[3]の有価証券報告書に関する調査の中で、記載が義務付けられている「事業等のリスク」項目において、サイバーセキュリティリスクを開示、記載する企業の割合は下記の通り年々増加しており、平成27年時点では6割以上の上場企業に開示、記載がみられる。

図1 サイバーセキュリティに関する記載状況の変化[3]

また同調査の中の分野別のサイバーセキュリティに関する記載状況は下記の通りとなる。

A Research on Cyber Security Awareness of Critical Infrastructure Operators and their Facility-Related Operators
†Masayuki SATO, Masayo FUJIMOTO
†Institute of Information Security

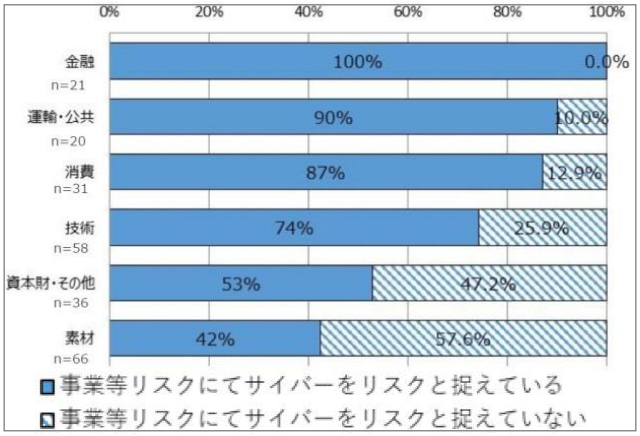

図 2 分野別サイバーセキュリティに関する記載状況[3]

本研究で選定した重要インフラ分野の情報通信は、この調査の分野では技術に含まれ、74%の記載率、鉄道、電力、ガスは運輸・公共に含まれ、90%の記載率となる。

5. 調査結果

情報通信、鉄道、電力、ガスの重要インフラ４分野で重要インフラ事業者とその設備関連事業者を３１社選定し、調査を実施した。　調査に伴い選定した設備関連事業者は、事業の経営方針等を支配される、重要インフラ事業者の子会社ではない事業者とした。

有価証券報告書の「事業等のリスク」項目にセキュリティ関連の記載の有無で評価した結果を下記に記す。

表 2 サイバーセキュリティの意識に関する評価結果

分野	重要インフラ事業者	評価	設備関連事業者	評価
情報通信	A 社	○		
	B 社	○	a 社	○
	C 社	○	b 社	○
	D 社	○	c 社	○
			d 社	○
鉄道	E 社	○		
	F 社	○	e 社	×
	G 社	○	f 社	○
	H 社	○	g 社	△
			h 社	×
電力	I 社	○		
	J 社	○	i 社	×
	K 社	○	j 社	×
	L 社	○	k 社	○
			l 社	△
ガス	M 社	○		
	N 社	○	m 社	○
	O 社	○	n 社	○
	P 社	○	o 社	○

有価証券報告書の評価と ISMS 認証の取得状況の評価に点数付けを行った結果は下記の通りである。

・有価証券報告書：○：2 点、△：1 点、×：0 点

・ISMS 認証取得状況：○：1 点、×：0 点

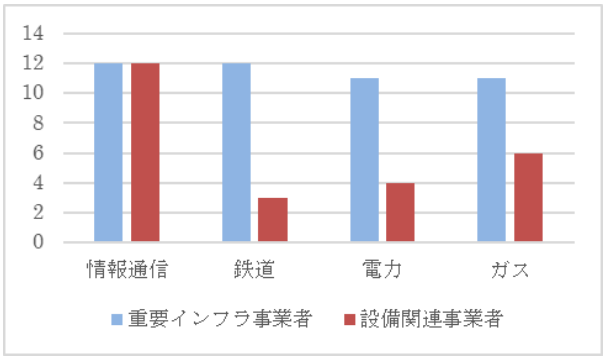

図 3 分野別の評価結果

また過去 10 年の有価証券報告書のデータを基に経年変化を確認したところ、近年、電力、ガス分野で「事業等のリスク」の項目でサイバーセキュリティに関する記載の強化や、新たな追記が確認できた。

6. まとめ

今回選定した分野の重要インフラ事業者については、重要インフラサービスを安全かつ持続的に提供するという社会的責任を負う立場で、また所管省庁からの指導等もあり全般的に経営層のセキュリティ意識が高いことが分かった。　一方、そのサプライチェーンの一部である設備関連事業者については分野や事業者によって、経営層のセキュリティ意識に差があることが分かった。

また電力分野での記載内容強化に関しては、2016 年に日本電気技術規格委員会（JESC）が電力分野のサイバーセキュリティに関するガイドラインを技術基準等に組み込み、2017 年に電力 ISAC(Japan Electricity Information Sharing and Analysis Center)が設立され、サイバーセキュリティに関する情報の収集、分析、共有が行われていることが分かった。[4]　こういった取り組みより、経営層がサイバーセキュリティをリスクとして再認識したのではと考えられる。

参考文献

[1] ICS-CERT, Year in Review 2012-2016
https://www.us-cert.gov/ics/Other-Reports
(参照 2021-01-07)
[2] NISC, 重要インフラの情報セキュリティ対策に係る第４次行動計画（第４次行動計画）, 2018
[3] NISC, 平成 28 年度 企業のサイバーセキュリティ対策に関する調査報告書, 2017
[4] 経済産業省, 電力分野におけるサイバーセキュリティ対策と「産業サイバーセキュリティ研究会 電力 SWG」での検討状況, 2019
https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/denryoku_anzen/pdf/019_04_00.pdf
(参照 2021-01-07)