NISC National center of Incident readiness and Strategy for Cybersecurity

参考資料

民間企業の
サイバーセキュリティリスク開示に係る
動向等について

平成26年度内閣サイバーセキュリティセンター委託調査

（　実施期間：　平成27年1月～3月　）

1. 有価証券報告書の調査

・上場企業225社（日経225）の平成21年度～25年度の5年間を対象

・「事業等のリスク」への<u>サイバーセキュリティリスクの記載状況</u>の調査・分析

- 開示企業数の増減
- 業種別の開示状況
- 記載内容
- 時系列的変化の状況
- インシデント発生事実の記載等

2. ヒアリング調査

・左記企業の中から13業種21社の協力を得て実施

・サイバーセキュリティリスクの<u>開示により期待される効果</u>等の調査

- サイバーセキュリティリスクを開示する理由・背景
- 開示していない理由・背景
- リスク開示による効果
- リスク開示に関する要望等

3. 海外文献調査

・米国や諸外国、国際機関等の英文文献を対象

・サイバーセキュリティリスクの<u>開示に係る取組状況</u>のとりまとめ

- 関連する法規制等の状況
- 法規制、監督省庁等の状況
- 企業における具体的な記載内容等

「有価証券報告書の調査」の主な結果

- 開示企業数は、平成21年度の52%（116社）から平成25年度の60%（136社）へと増加。
- 業種別では、通信、銀行、証券、保険、小売業、石油、造船、電力、ガス等の14業種が100%（合計51社）。
- 繊維、パルプ・紙、鉄鋼等の4業種は0%（合計14社）。
- 素材産業全体（64社）では開示割合が32.8%と低く、原材料費や為替の影響等のリスクと比べ、サイバーセキュリティリスクの認識が相対的に低いと考えられる。
- サイバーセキュリティリスクの記載文書が5年間同一の企業（65社）には、その記載の仕方が包括的で意味が広く捉えられる（想定インシデント・被害が具体的でない）ものが多かった。
- 自社で発生したサイバーセキュリティインシデントを記載している企業は調査対象企業中4社と少なかった。

平成25年度 日経225社-業種別サイバーセキュリティ情報開示状況

日経業種分類				開示企業数	開示企業%	
大分野	（社数）	中分野	（社数）		中分類	大分類
A 技術	57	01 医薬品	8	2	25.0%	61.4%
		02 電気機器	29	20	69.0%	
		03 自動車	9	4	44.4%	
		04 精密機器	5	3	60.0%	
		05 通信	6	6	100.0%	
B 金融	21	06 銀行	11	11	100.0%	100.0%
		07 その他金融	1	1	100.0%	
		08 証券	3	3	100.0%	
		09 保険	6	6	100.0%	
C 消費	28	10 水産	2	1	50.0%	85.7%
		11 食品	11	10	90.9%	
		12 小売業	8	8	100.0%	
		13 サービス	7	5	71.4%	
D 素材	64	14 鉱業	1	0	0.0%	32.8%
		15 繊維	5	0	0.0%	
		16 パルプ・紙	3	0	0.0%	
		17 化学	18	5	27.8%	
		18 石油	2	2	100.0%	
		19 ゴム	2	1	50.0%	
		20 窯業	9	3	33.3%	
		21 鉄鋼	5	0	0.0%	
		22 非鉄・金属	12	5	41.7%	
		23 商社	7	5	71.4%	
E 資本財・その他	35	24 建設	8	4	50.0%	51.4%
		25 機械	16	8	50.0%	
		26 造船	2	2	100.0%	
		27 その他製造	3	3	100.0%	
		28 不動産	6	1	16.7%	
F 運輸・公共	20	29 鉄道・バス	8	7	87.5%	85.0%
		30 陸運	2	2	100.0%	
		31 海運	3	1	33.3%	
		32 空運	1	1	100.0%	
		33 倉庫	1	1	100.0%	
		34 電力	3	3	100.0%	
		35 ガス	2	2	100.0%	
合計	225		225	136		

「ヒアリング調査」の主な結果

- 開示している企業からは、サイバーセキュリティリスクの社内検討が経営者及び企業内の開示関係者・各事業責任者等のリスク認識を高め、具体的なリスク及び対策を共有するうえで大きな効果があったとの意見が多かった。

- また、サイバーセキュリティリスクの開示に関する課題・要望として、以下のような意見があった。
  - サイバーセキュリティリスクを具体的に開示するとその脆弱性が攻撃されるリスクが増し、どのように記載すべきか判断が難しいために、国等でサイバーセキュリティリスク開示に係るガイドラインを作成して欲しい。
  - サイバーセキュリティリスクの開示が不十分な企業が多いので、国等が音頭をとって開示を促進する指導をして欲しい。
  - サイバーセキュリティリスクに関する情報の入手に苦労しているので、国等は積極的にサイバー攻撃に関する情報やサイバー攻撃対策ガイド等を提供して欲しい。

- サイバーセキュリティリスクを開示していない企業について、その理由として以下のような意見があった。
  - 情報漏えいやITシステム停止等のリスクは開示する程大きくないと考えている。
  - 情報漏えいやITシステム停止等のリスクを「事業等のリスク」として記載しているが、大きな脅威は事故・災害、操作ミス、メール誤送信等の社内要因にあると考えている。

「海外文献調査」の主な結果（米国）

- 米国企業のForm 10-Kに記載するリスク要因については連邦規則（Regulation S-K　Item503（c））にて規定されており、どの企業にもあてはまるような一般的な記述ではなく、当該企業特有の内容について、具体的に分かり易く説明するよう要求されている。

- また、サイバーセキュリティリスク開示に関するガイダンスとしては、米国証券取引委員会（SEC）企業財務局から2011年10月に発行された「CF Disclosure Guidance: Topic No. 2 Cybersecurity」（CFDG: Topic No.2）がある。同文書は、上場企業がサイバーセキュリティについて、自社特有の事実と状況を考慮しつつ、どのような場合に何を開示すべきかを判断する助けとなるガイダンスである。

- 上記に基づき、米国企業においては、サイバーセキュリティに関する自社特有の事実・状況に照らしたリスクや想定被害について詳しく開示している傾向があり、被害事例を開示する企業も見られる。

- なお、証券法は、詳細な開示によって当該企業がサイバーセキュリティ上の危険に晒されるような場合にまで開示を求めるものではないとしている。

「海外文献調査」の主な結果（EU）

○ EUでは、現在、欧州議会において、データ保護指令の更新及び指令（Directive）から規則（Regulation）への昇格を目指した審議が行われている。
その中で審議継続中の「EUデータ保護規則案」の修正案に、上場企業のサイバーセキュリティリスク開示を求める内容も含まれている。

（修正案） 指令の詳述4に対する案

（4）ネットワーク及び情報セキュリティ（NIS）に関する情報交換や協同によるリスク回避、検知及び対応を実現するためには、協力のメカニズムは連合レベルで確立されるべきである。またメカニズムを効果的かつ包括的なものとするためには、全てのメンバー国が自国内において高いレベルのNISを実現できるような最低限の機能と戦略を有する必要があり、それはリスクマネジメント文化を推進し、最も重大なインシデントが確実に報告されるためにも、少なくとも情報インフラのしかるべき事業者にも適用されるべきである。株式市場上場企業において自主的にインシデントを財務報告書に公表するよう促進されるべきである。法的枠組みは、市民のプライバシーと完全性を保護する必要性に基づくべきである。CIWINは本指令により事業者に拡大すべきである。

（修正案） 指令の14条第4節第1号に対する案

事業者は監督当局に報告することに加え、インシデントについて企業が自主的に財務報告書に公表することを奨励しなければならない。

理由：サイバーインシデントは、多大なる財務上の損失と多額の費用を必然的に伴う。株主や投資家は、これらの事件の結果について通知されるべきである。企業に対して、自発的にサイバーインシデントの公開を促すことにより、将来のインシデントの可能性やそのようなリスクの特質はもちろん、サイバーセキュリティ侵害を低減するためのリスク回避行動の妥当性等についての分野横断的な議論を促すこととなりうる。

EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive", 2013/2/7, EU委員会
http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security をもとに和訳