資料３－１

企業のセキュリティ対策に係る情報開示の実態等に関する調査

平成30年02月27日(火)

（１）国内における情報開示の事例調査

国内における情報開示の事例調査　概要

■ 対象企業

- 日経２２５に含まれる２０企業を調査対象とした。
- 業種分類大分野の6分野からそれぞれ3-4社を選択。

■ 国内における情報開示の事例調査

- 国内企業が公開している以下の資料に対し、情報セキュリティ対策に係る記載状況および記載内容を調査し、記載項目や粒度等の分析を実施した。
  - ①　有価証券報告書
  - ②　情報セキュリティ報告書
  - ③　CSR報告書
  - ④　サステナビリティレポート
  - ⑤　総合報告書（Annual Report)
  - ⑥　コーポレートガバナンス報告書

■ 調査手法

- ①～⑤については直近3期年分の資料、⑥については最新および調査請負事業者が所有する資料の直近2年分の資料を対象とした
- ②情報セキュリティ報告書は公開している企業が少ないため、日経225で報告書を公開している5企業を調査対象企業とした
- ③CSR報告書、④サステナビリティレポート及び⑤総合報告書については、情報セキュリティ対策に係る事項をいずれかに統合して記載されているため、まとめて分析
- 収集した調査対象資料に対し、情報セキュリティに関する記載内容について確認

1）有価証券報告書

1）有価証券報告書　概要

- 日経225に含まれる全企業を対象にした内閣サイバーセキュリティセンター（以下、NISCとする）の調査では情報セキュリティリスクを記載する企業の割合が図１のとおり年々増加しており、平成27年には67.1%の企業が記載している。業種別でみると、「金融」が100%、「運輸・公共」が90%、「消費」が87%の企業が開示している。
- 記載される内容は、システムの停止や機密データの漏えい等に関する概略であり、詳細な内容については記載されない傾向がある。
- 平成16年3月期から有価証券報告書への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、サイバー攻撃、不正アクセス、コンピュータウイルス等の内容がリスクとして記載されている。
- また、調査対象の企業の内、2社はリスクとなる内容に加え、「教育・人材育成」に関する取組について記載している。教育の対象者は、情報セキュリティに直接関係する職員だけではなく、役職員も対象としており、経営層の情報セキュリティへのかかわりが明確となっている。

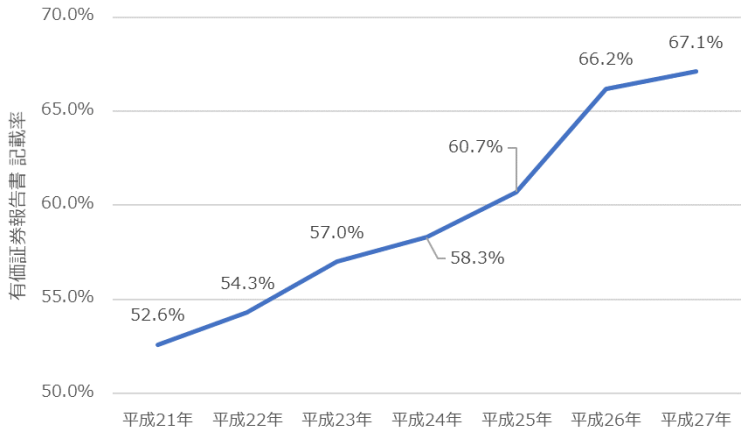


図１ サイバーセキュリティに関する記載状況の変化

出典：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（NISC）

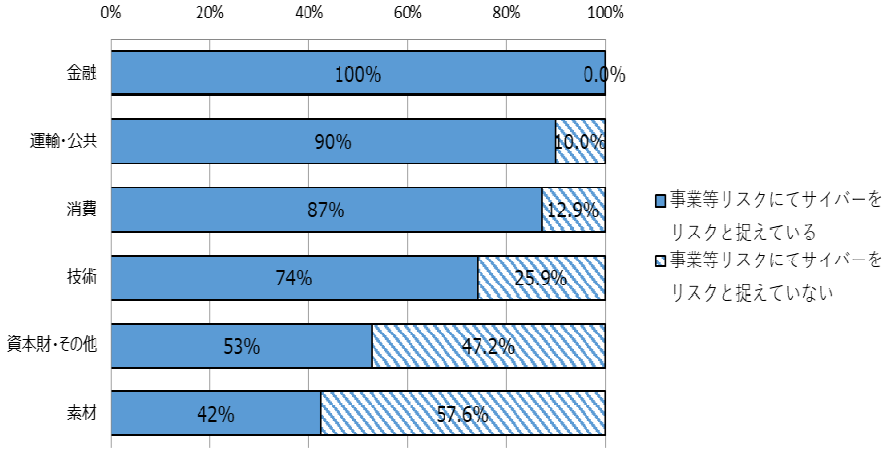


図２ 分野別サイバーセキュリティに関する記載状況

出典：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（NISC）

1）有価証券報告書　開示状況

大分野	中分野	記載の有無		
		平成26年度	平成27年度	平成28年度
技術	医薬品	×	○	○
	電気機器	○	○	○
	自動車	○	○	○
	通信	○	○	○
金融	銀行	○	○	○
	証券	○	○	○
	保険	○	○	○
消費	食品	×	×	×
	小売業	○	○	○
	サービス	○	○	○
素材	化学	○	○	○
	窯業	×	×	○
	非鉄・金属	○	○	○
	商社	×	×	×
資本財・その他	建設	○	○	○
	機械	○	○	○
	不動産	×	×	×
運輸・公共	鉄道・バス	○	○	○
	海運	○	○	○
	電力	○	○	○

凡例　○：セキュリティに関する記述有り　　×：セキュリティに関する記述無し　　ー：資料の開示無し

1）有価証券報告書　記載例　概要

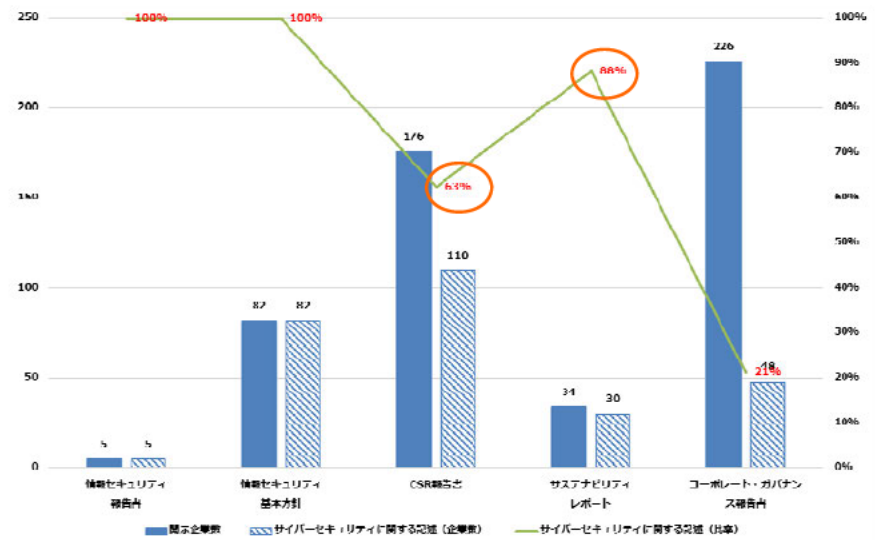
サイバー攻撃をリスクとして記載している企業	「教育・人材育成」を記載している企業
17社 (医薬品、電気機器、自動車、通信、銀行、証券、保険、小売業、サービス、化学、非鉄・金属、建設、機械、鉄道・バス、海運、電力)	2社 (通信、建設)

	記載例
リスク	● 技術（医薬品）：悪意をもった第三者による攻撃（サイバーアタック）により、システムの停止やセキュリティ上の問題が発生する可能性があります ● 金融（保険）：サイバー攻撃による不正アクセス又は情報システムの不備等により、情報システムの停止、誤作動もしくは不正使用又は情報漏洩等が発生する ● 消費（サービス）：システム障害やネットワークの寸断、システムへの不法な侵入および無差別攻撃に晒される可能性があります ● 素材（窯業）：ハッカーやコンピュータウィルスによる攻撃、不正アクセスその他不測の事態により、重要な業務の中断や機密データの漏洩などが発生
人材育成	● 技術（通信）：より高度なスキルを持つセキュリティ人材の育成に向けた取り組みなどを強化 ● 資本財・その他（建設）：情報管理に関するポリシーや事務手続等を策定し役職員等に対する教育・研修等により情報管理の重要性の周知徹底、セキュリティ対策等を行っています。

２）CSR報告書、サステナビリティレポートまたは総合報告書

2）CSR報告書、サステナビリティレポートまたは総合報告書　概要

- 日経225に含まれる全企業を対象にしたNISCの調査においても、CSR報告書及びサステナビリティレポートにおける情報セキュリティを記載する企業の割合はそれぞれ63%と88%と高い。
- 多くの企業が情報セキュリティにかかる内容を報告書に記載している。また、情報セキュリティに係るリスクだけではなく、「基本方針等の策定状況」や、「管理体制」、「教育・人材育成」、「社外との情報共有体制」、「第三者評価・認証」について記載されている。



各種報告書の公表状況とサイバーセキュリティに関する記述が含まれる割合

（出典：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（NISC））

- 「基本方針等の策定状況」については、ポリシーや基本方針の策定だけではなく、全役職員を対象に研修・訓練を実施して方針の浸透を図っていることがうかがわれる。
- 「管理体制」については、CSIRTによる平時からの対応及び事故発生時の対応を目的としたインシデント対応チーム等の設置について記載されていると共に、CISOを最高責任者とした管理が記載されている。
- 「教育・人材育成」については、全社員を対象にした教育を行い、企業全体の意識の向上を図っている記載がある一方、セキュリティに特化した「セキュリティ人材」の育成について記載されている。
- 「社外との情報共有体制」については、業種に応じたISACや日本シーサート協議会との連携や、内閣サイバーセキュリティセンター（NISC）における分野横断的演習への参加について記載されている。
- 「第三者評価・認証」については、情報セキュリティマネジメントシステム（ISMS）の国際規格「ISO／IEC27001:2005」および「JISQ27001:2006」の認証の取得等について記載されている。

2）CSR報告書、サステナビリティレポートまたは総合報告書　開示状況

大分野	中分野	記載の有無		
		平成26年度	平成27年度	平成28年度
技術	医薬品	×	×	×
	電気機器	○	○	○
	自動車	○	○	○
	通信	○	○	○
金融	銀行	×	○	○
	証券	○	○	○
	保険	○	○	○
消費	食品	×	○	○
	小売業	×	×	○
	サービス	○	×	×
素材	化学	×	×	×
	窯業	×	×	○
	非鉄・金属	○	○	○
	商社	×	×	○
資本財・その他	建設	×	○	○
	機械	○	○	○
	不動産	×	×	○
運輸・公共	鉄道・バス	○	○	○
	海運	○	○	○
	電力	—	—	×

凡例　○：セキュリティに関する記述有り　　×：セキュリティに関する記述無し　　—：資料の開示無し

2）CSR報告書、サステナビリティレポートまたは総合報告書　記載例　概要①

「基本方針等の策定状況」を記載している企業	「管理体制」を記載している企業
11社 (電気機器、自動車、通信、証券、保険、食品、サービス、化学、窯業、建設、鉄道・バス)	11社 (電気機器、自動車、通信、証券、保険、食品、サービス、化学、窯業、建設、鉄道・バス)

	記載例
基本方針等	● 素材（化学）：企業価値の維持・向上を図っていくために、「情報セキュリティポリシー」を制定 ● 金融（証券）：役職員の意識向上のため「野村グループ情報セキュリティ基本方針」を制定し、全役職員に対して研修・訓練を定常的に実施
管理体制	● 消費（食品）：セキュリティ事故発生時の即応を目的として、コンピューターセキュリティインシデント対応チームを設置しています ● 技術（通信）：情報セキュリティマネジメント体制として、代表取締役副社長がCISO（Chief Information Security Officer）として情報管理の最高責任者を担い、情報セキュリティの管理を徹底しています ● 金融（証券）：CSIRTを中心に、親会社およびグループ各社のサイバーセキュリティ対応組織が連携

2）CSR報告書、サステナビリティレポートまたは総合報告書　記載例　概要②

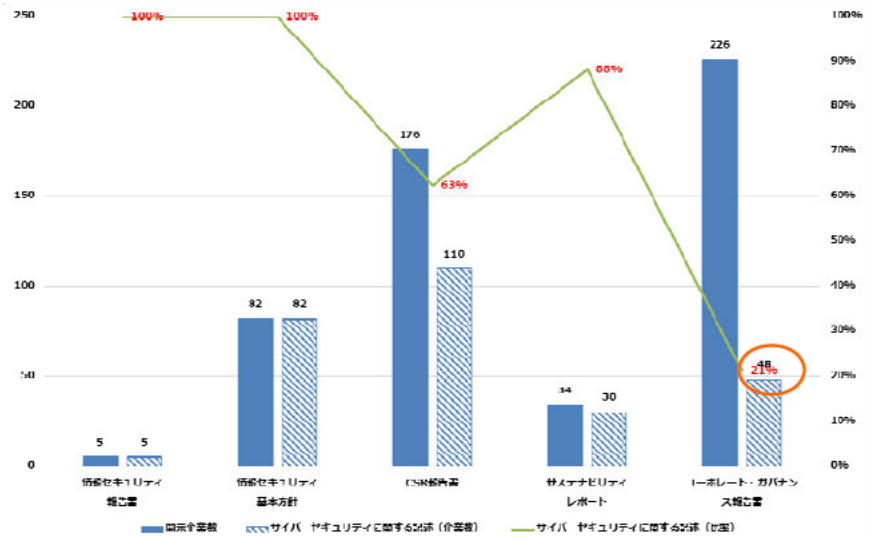
「教育・人材育成」を記載している企業	「社外との情報共有体制」を記載している企業	「第三者評価・認証」を記載している企業
10社 (電気機器、通信、証券、保険、食品、サービス、化学、窯業、非鉄・金属、鉄道・バス)	5社 (通信、証券、食品、化学、機械)	2社 (電気機器、サービス)

	記載例
人材育成	● 技術（通信）：情報セキュリティに関する講座の開講など、さまざまな取り組みを実施し、日本のセキュリティ人材育成に貢献 ● 素材（窯業）：情報セキュリティレベルの向上のため、eラーニングなどによる教育 ● 運輸・公共（鉄道・バス）：全社員を対象に情報セキュリティ教育を実施し、各職場内で情報セキュリティに対して取り組む意識の向上を図っています
情報共有	● 技術（通信）：US-CERTやJPCERTコーディネーションセンターと連携するとともに、FIRSTや日本シーサート協議会への加盟などにより国内外のCSIRT組織と連携し、動向や対策法などの情報共有を行っています。また、内閣サイバーセキュリティセンター（NISC）が主催する分野横断的演習にも参加し、ノウハウ共有・情報収集に努めています ● 金融（証券）：金融ISAC、日本CSIRT協議会等の外部情報共有機関を通じた攻撃者や攻撃方法に関する情報の収集・共有体制を構築しています
第三者認証	● 技術（電気機器）：情報セキュリティの担当役員からのメッセージ、第三者評価・認証などの、より詳細な内容は「情報セキュリティ報告書2016」に記載しています ● 消費（サービス）：情報セキュリティの向上のため、親会社ならびにグループ会社計49社が情報セキュリティマネジメントシステム（ISMS）の国際規格「ISO／IEC27001:2005」および「JISQ27001:2006」の認証を取得しています

3）コーポレートガバナンス報告書

3）コーポレートガバナンス報告書　概要

■ 日経225に含まれる全企業を対象にしたNISCの調査では、<u>コーポレートガバナンス報告書における情報セキュリティを記載する企業の割合は21%となっている</u>。



各種報告書の公表状況とサイバーセキュリティに関する記述が含まれる割合

（出典：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（NISC））

■ 「内部統制システム等に関する事項」項目において、グローバルな推進体制や情報セキュリティ及び個人情報保護に関する体制を整備する等、<u>情報セキュリティへの対応に関する管理体制の整備について記載される傾向がある</u>。また、ITセキュリティの回避措置やサイバーセキュリティの強化等の内容が防止対策として記載されている。

3）コーポレートガバナンス報告書　開示状況

大分野	中分野	記載の有無	
		平成27年度	平成28年度
技術	医薬品	○	○
	電気機器	×	×
	自動車	○	○
	通信	○	○
金融	銀行	×	×
	証券	×	×
	保険	×	×
消費	食品	×	×
	小売業	×	×
	サービス	○	○
素材	化学	×	×
	窯業	○	○
	非鉄・金属	○	○
	商社	×	×
資本財・その他	建設	×	×
	機械	×	×
	不動産	×	×
運輸・公共	鉄道・バス	×	×
	海運	×	×
	電力	○	○

凡例　○：セキュリティに関する記述有り　　×：セキュリティに関する記述無し　　ー：資料の開示無し

3）コーポレートガバナンス報告書　記載例　概要

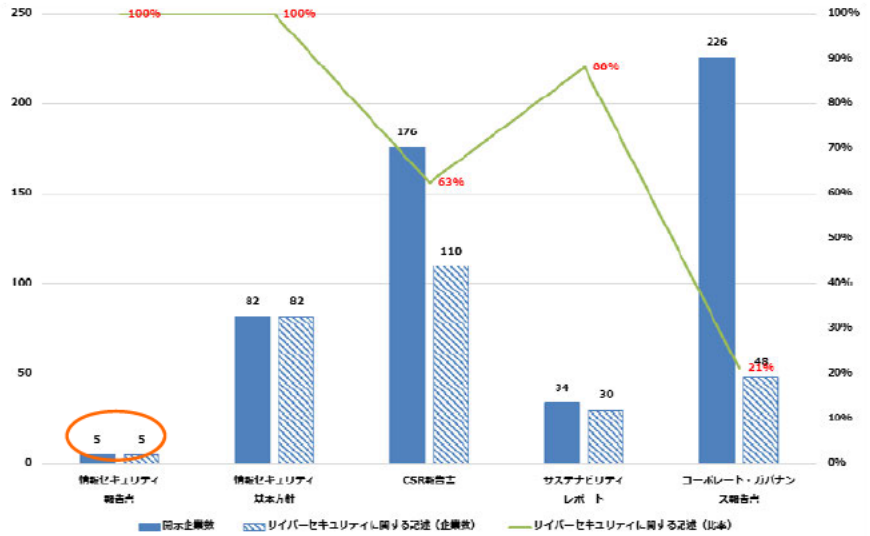
「管理体制」を記載している企業	「防止対策」を記載している企業
2社 (自動車、通信)	4社 (医薬品、自動車、その他製造、電力)

	記載例
管理体制	● 技術（自動車）：機密管理を含めた情報セキュリティ全般に対して、グローバルな推進体制や仕組みを整備 ● 技術（通信）：情報セキュリティ及び個人情報保護に関する体制を整備
防止対策	● 技術（医薬品）：リスクの程度・内容に応じた対応策・コンティンジェンシープランに基づき回避措置、最小化措置を行う ● （その他製造）：サイバー攻撃の増加・巧妙化に対してサイバーセキュリティの強化を進める

４）情報セキュリティ報告書

4）情報セキュリティ報告書

- 情報セキュリティ報告書を公開している企業は少なく、<u>日経225の内で公開している企業は電気機器、通信企業の5社のみ</u>となっている。
- 公開している資料では、技術面の取組、体制の構築、マネジメントシステムについて記載されている。また、全ての報告書において情報セキュリティの最高責任者として経営層の考え方が記載されており、責任と方針が明確にされている。



各種報告書の公表状況とサイバーセキュリティに関する記述が含まれる割合

（出典：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（NISC））

- 経済産業省は「情報セキュリティ報告書モデル」を公開しており、その中で基本構成として記載項目を7つ設定しているが、公開されている報告書も本モデルを参考に作成していることが想定される。

①基礎情報

②経営者の情報セキュリティに関する考え方

③情報セキュリティガバナンス

④情報セキュリティ対策の計画、目標

⑤情報セキュリティ対策の実績、評価

⑥情報セキュリティに係る主要注力テーマ

⑦（取得している場合の）第三者評価・認証等

4）情報セキュリティ報告書　開示状況

大分野	中分野		記載の有無		
			平成26年度	平成27年度	平成28年度
技術	電気機器	A社	○	○	○
		B社	○	○	○
		C社	○	○	○
		D社	○	○	○
	通信		○	○	○

凡例　○：セキュリティに関する記述有り　　×：セキュリティに関する記述無し　　ー：資料の開示無し

4）情報セキュリティ報告書　記載例　概要

記載例
● 技術（電子機器） A社：情報セキュリティガバナンスの基本的な考え方
● 技術（電子機器） C社：CISOメッセージ、基本方針 ● 技術（電子機器） D社：トップメッセージ ● 技術（通信） ：Message from the CISO、情報セキュリティ方針
● 技術（電子機器） A社：情報セキュリティマネジメントシステム ● 技術（電子機器） B社：情報セキュリティガバナンス ● 技術（電子機器） C社：情報セキュリティマネジメント体制 ● 技術（電子機器） D社：CSR委員会による情報セキュリティガバナンスの強化、効率的なマネジメント体制、ウェブ環境の安全管理体制の確立 ● 技術（通信） ：情報セキュリティマネジメント体制、情報セキュリティガバナンス情報セキュリティ戦略
● 技術（通信） ：情報セキュリティ活動年表
● 技術（電子機器） A社：製品・サービスの情報セキュリティ確保に向けた取組 ● 技術（通信） ：情報セキュリティの取り組み、情報セキュリティソリューションの提供、情報セキュリティ施策実施状況
● 技術（電子機器） B社：維持・向上を目指すセキュリティ分野 ● 技術（電子機器） C社：重点施策
● 技術（電子機器） A社：第三者評価・認証、プライバシーマーク取得状況、ISMS認証取得状況、ITセキュリティ評価認証の取得状況、暗号モジュール試験・認証の取得状況、制御機器向けセキュリティ認証の取得状況 ● 技術（電子機器） B社：第三者認証・評価、ISMS認証の取得状況、プライバシーマーク付与認定の取得状況、ITセキュリティ評価認証の取得状況 ● 技術（電子機器） D社：第三者認証の効果的な活用、第三者認証の活用目的、ISMSの推進による「顧客満足度の向上を支える業務改善活動」の具現化、プライバシーマークを活用した個人情報保護の強化、個人情報保護の高いレベルでの「均質化」と最適化に向けた取り組み、マネジメントシステムの効率的な運用、グループに会社における認証取得状況、ISO/IEC15408認証取得製品

日本企業が公開している各資料の比較

- 記載率に関して
  - 情報セキュリティに特化した情報セキュリティ報告書を除く、有価証券報告書、コーポレートガバナンス報告書並びにCSR報告書、サステナビリティレポート及び総合報告書及びにおける情報セキュリティに係る事項の記載率を比較すると、CSR報告書、サステナビリティレポート及び総合報告書の記載率が高い。
- 想定される主たる閲覧対象者に関して
  - 有価証券報告書及びコーポレートガバナンス報告書の目的は、投資家の投資判断を支援する等を主目的としているため、閲覧対象者が限られていると考えられる。
  - CSR報告書、サステナビリティレポート及び総合報告書の目的は企業の取組、姿勢等をブランディングし、企業信頼度を高めることを目的としているため、一般的な顧客を幅広く対象としていると考えられる。
  - 情報セキュリティ報告書は、内容が情報セキュリティに限られているため、閲覧対象者は情報セキュリティの専門家等を中心としていると考えられる。
- 記載内容に関して
  - 有価証券報告書はリスクとしての情報セキュリティ、コーポレートガバナンス報告書は企業統治に必要な防止対策や体制の整備について記載されている。
  - CSR報告書、サステナビリティレポート及び総合報告書は想定される閲覧対象者が幅広いため、記載される内容も簡易で幅広く記載される傾向がある。
  - 情報セキュリティ報告書は文章及び用いられる語句も専門的な内容が記載されている。
- 開示の傾向に関して
  - 企業は、情報セキュリティへの対策について、投資判断支援を目的に資料を閲覧する投資家ではなく、企業が提供するサービスを直接的あるいは間接的に利用する一般的な顧客を、アピールすべき対象者として意識していると考えられる。その結果として、情報セキュリティ対策を記載する媒体としてCSR報告書、サステナビリティレポート及び総合報告書が選択され、内容についても簡易で幅広いテーマを取り扱っていることが想定される。

（2）情報開示に関する海外の取組の調査

情報開示に関する海外の取組の調査　概要

■ 対象国

- 米国、EUを調査対象とする。
- EUについては個別の加盟国（イギリス、フランス、ドイツ及びオランダ）も調査対象として選択する。

■ 調査

- 各国において、企業リスクについて公開を義務付けている法令等の調査を実施する。

米国のサイバーセキュリティリスク開示についての法規等

- 米国では、証券取引委員会（SEC）登録会社（上場企業）は、連邦法である1933年証券法 に基づき投資家に対して十分な情報に基づく投資判断を行うことを保証すべきとの基本的な考え方がある。投資判断に影響を及ぼしうるようなサイバーセキュリティリスク情報についても、可能な範囲で投資家と情報を共有すべきであるとするCF Disclosure Guidance: Topic No. 2 Cybersecurity（以下「CFDG:Topic No.2」と称する）の考え方の根拠となっていると考えられる。
- CFDG:Topic No.2
  - 米国SECは年次報告書として、米国企業にはForm 10-K、外国企業にはForm 20-Fというフォーマットでの提出を求めている。Form 10-Kに記載すべきRisk Factors（リスク要因）については連邦規則であるRegulation S-K に規定Item503(c)があり、どの企業にもあてはまるような一般的な記述ではなく、リスクが当該企業あるいは投資家が手にする有価証券にどのような影響を及ぼすかについて、具体的に分かり易く説明するよう明記されている。
  - その上で、サイバーセキュリティリスクやサイバーインシデントについての開示義務に関する、SEC 企業財務局（Division of Corporate Finance）の見解を示したものがCFDG:Topic No.2であり、SEC登録会社がForm 10-Kにおいて、サイバーインシデントに関するリスクやこれに伴う事業への影響について、1933年証券法の開示義務の枠内でどのように説明すべきかという点についてのガイダンスを提供している。登録会社が自社特有の事実と状況を考慮しつつ、サイバーセキュリティについて何をどのような場合に開示すべきかを判断する助けとなる内容となっており、Risk Factorsの項についてRegulation S-KのItem 503（c）に従うべきことが明記されている。

EUのサイバーセキュリティリスク開示についての関連法規等

- EUにおける動き
  - EU議会及びEU理事会は「財務諸表及び関連報告に関する指令(2006/43/EC(2006年), 78/660/EEC(1978年) and 83/349/EEC(1983年))」を2013年6月26日に修正し、新たな指令として「EU会計指令(2013/34/EU)」を決定した。また2014年に「EU非財務報告指令(2014/95/EU)」が決定され、一部修正が行われている。

- 「EU会計指令(2013/34/EU)」
  - 第17条「大企業、中企業及び公共の利益に係る企業の追加開示」第1項「大企業、中企業及び公益に係る企業は第16条で求められた事項(財務状況)に加え以下の項目を開示すべきである」の(p)において、「財務諸表及び金融上の影響に含まれない契約の性質及び目的に基づいて、事業の財政情報を評価するためにリスク若しくは利益の開示が必要である。」としている。19条「マネジメントレポートの項目」の第1項には「マネジメントレポートには主なリスク及び直面している不確実性に関する説明を伴った、事業の開発及び業績が含まれていなければならない。」と記載。

- 「EU非財務報告指令(2014/95/EU)」
  - 第8条において「この指令の対象となる事業体は、具体化する可能性が最も高いと思われる重大な影響を及ぼすリスクに係る事項に及び、すでに具体化しているリスクに係る事項と関連する適切な情報を提供すべきである。」と記載されている。その上で「EU会計指令(2013/34/EU)」の19条を一部改正し、非財務諸表に関する開示項目として業務に関連する重要なリスクに関して当該事業体がこれらのリスクをどのように管理しているかについて開示することが追記された。

EU諸国のサイバーセキュリティリスク開示についての関連法規等

- イギリス
  - イギリスでは、2006年の改正会社法(The Companies Act 2006) において事業者に対してリスクの開示と報告を求めている。また、同法に関連したリスクマネジメント及び企業内統治に関するベストプラクティス及び取組のガイダンス「Guidance on Risk Management, Internal Control and Related Financial and Business Reporting」 を発行することで、企業のリスク開示を促している。なお、英国の制度は指令「EU会計指令(2013/34/EU)」を十分に満たしていると評価されている 。

- フランス
  - フランスではEU指令「EU会計指令(2013/34/EU)」及び「EU非財務報告指令(2014/95/EU)」に従い、同指令の国内履行として2017年8月9日政令(Décret n° 2017-1265 du 9 août 2017)を制定し、CSR関連の非財務報告を義務づけた。なお同政令は社会・環境分野に係わる内容であり、情報セキュリティ等に紐づけられるリスクに関して言及はされていない。同政令に先立つ2017年7月12日に決定された法令(Ordonnance n° 2017-1162 du 12 juillet 2017)第8条により、商法第225-100-1条が改正され、第3項に「会社が直面している主なリスクと不確実性の記述」を報告書として開示することが求められた。

- ドイツ
  - ドイツでは「EU会計指令(2013/34/EU)」に対応させるため、2015年に「EU会計指令実施法(BilRUG)」に基づいて、商法(HGB)を改正している。同法289条では各企業に義務付けられる状況報告書記載事項として289条(2)1. a)「全ての重要な取引種類の防護の方法であって保全措置の貸借対照表計上の構造において把握されたものを含めた，会社のリスク管理の目標と方法」、b)「会社がさらされている価格変動リスク，減損リスク，流動性リスク及びキャッシュフロー変動から生じるリスク」(6)「会計過程における内部統制システム及びリスク管理システムの重要な特徴について記述しなければならない。」と記載されている。

- オランダ
  - オランダは2016年9月28日に「 EU会計指令(2013/34/EU) 」及び「 EU会計指令実施法(BilRUG) 」に基づいて、オランダの民法典上商法・会社法にあたる民法典第2編「Burgerlijk Wetboek Boek 2」の改正を行った 。民法典第2編§7「年次報告書」第391条の1項において「年次報告書は法人が直面している主なリスクと不確実性についても説明しなければならない。」と記載されている。

（3）米国及びEUにおける情報開示の事例調査

米国及びEUにおける情報開示の事例調査　概要

- 対象企業
  - 米国20企業、EU18企業を対象
  - 企業の選択に当たっては、各国の上場企業のうち、業種の偏りが出ないように選択

- 調査対象資料
  - 米国についてはForm 10-K、EUについては各企業が公開しているAnnual Report等を対象として設定

- 調査手法
  - インターネット上に公開されている最新の資料を対象
  - 収集した調査対象資料に対し、情報セキュリティに関する記載内容について確認

米国企業の開示情報事例

■　重要情報資産への影響に関する言及

明確に顧客情報等の個人情報流出を想定リスクとして挙げている企業	開発機密及び知的財産等に関する情報の流出
12社 (通信、製造、ダム、福祉、金融、小売、情報技術(2)、交通、化学、製薬)	11社 (化学(2)、通信、製造、防衛、金融、製薬、情報技術(2)、交通(2))

＊上記は重複含む

記載例
● (製薬)：情報システムの著しい中断、情報セキュリティの侵害、重要機密情報や知的財産の損失 ● (情報技術)：自社及び顧客、その他第三者のデータやシステム情報の漏洩・悪用・紛失・破壊・それらデータへの不正アクセス、個人情報や知的財産情報の窃取、重要データやシステムへのアクセス権の喪失 ● (ダム)：顧客及び財務データの物理的もしくは電子上の喪失やセキュリティ侵害・不正流用、顧客に関する情報もしくは機密情報の窃盗、機密情報・個人情報流出 ● (交通)：機密情報及び保護された情報の漏洩、重要データの損失又は危険にさらされる

■　法的リスクへの言及

法的罰則リスクのみを記載	訴訟リスクのみを記載
5社(農業・食料、製薬(2)、情報技術、化学)	1社(原子力)

法的罰則及び訴訟リスクの両項目を記載
7社 (通信、製造、エネルギー、金融、小売、製薬、情報技術(2)、水道)

記載例
● (通信)：財務データや機密または個人情報などの貴重な情報の盗難やその他の価値ある情報の漏洩は、訴訟や政府の追求、捜査対象になりうる ● (金融)：訴訟費用の上昇、行政介入、著しい規制の影響、訴訟提起されることによる規制に定める罰金・刑罰、プライバシー又はその他の適用可能な法律の違反、大規模な訴訟を提起される、規制に関する審査の増加 ● (小売)：訴訟または賠償責任による損失、規制の強化、刑罰、サービスの停止

■　平時からの情報セキュリティに関する取り組み言及

平時の情報セキュリティに関する事項を記載している企業
16社 (化学(2)、不動産、通信、製造(2)、福祉、電力(2)、金融、小売り、製薬、情報技術、水道、交通、製薬)
記載例： ・(製造)：セキュリティ侵害に対する適切な措置や操作をしており、こうした脅威を適切に識別し監視する重要なリソースに投資している。 ・(情報技術)：システム・データを保護するためのセキュリティ・暗号化などのセキュリティ手段への投資、アカウントやシステムに対する監視、不審な状況下におけるアカウントの凍結、サイバーリスクの特定の側面を対象とした保険。

ＥＵ企業の開示情報事例

■　重要情報資産への影響に関する言及

明確に顧客情報等の個人情報流出を想定リスクとして挙げている企業	開発機密及び知的財産等に関する情報の流出
6社 (製造(航空)、情報技術(2)、建設、金融(2))	3社 (製薬、運輸、製造(航空))

＊上記は重複含む

記載例
記載例: ● (建設)：情報セキュリティの欠陥は顧客、従業員及び社のデータ盗難及び流出につながる ● (製造(航空))：機密情報漏洩、個人情報流出、知的資産損失 ● (製造)：知的資産の盗難、社やビジネスパートナーにひもづく機密情報漏洩

■　法的リスクへの言及

法的罰則リスクのみを記載	訴訟リスクのみを記載
2社(エネルギー資源、情報技術)	0社

法的罰則及び訴訟リスクの両項目を記載
3社 (建設(2)、交通(航空))
記載例： ● (情報技術)：法令遵守違反（「上場企業会計改革および投資家保護法（Sarbanes-Oxley Act)、「PCIデータセキュリティスタンダード」、データプライバシー） ● (建設)：データ保護法違反による罰則や訴訟 ● (交通)：顧客、契約パートナー及び公的機関からの契約上・法上の請求に対する支払

■　平時からの情報セキュリティに関する取組への言及

平時の情報セキュリティに関する事項を記載している企業
全18社
記載例
● (資源)：・継続的にエクスターナル・デベロップメントを監視し、脅威やセキュリティインシデントに関する情報を共有。シェルの従業員や契約スタッフは月次コースや定期意識キャンペーンを受け、サーバー脅威から社を保護することを求められる。定期的に災害回復計画とセキュリティ対応プロセスを評価し適応させ、セキュリティ監視能力強化を図る。 ● (運輸)：IT委員会の副次的委員会である情報セキュリティ委員会が、ISO 27002（情報セキュリティマネジメントの国際基準）に基づくガイドライン、標準、手続きを設定している。リスクマネジメント、IT監査、データ保護及び企業機密保持(コーポレートセキュリティ）グループがITリスクと現在の状況を監視・評価している。外部のデータベースに加え、チェコ、マレーシア及びアメリカに中央データセンターを設置し、地理的にデータを分散し局地的に運用している。従業員のデータアクセスおよび利用をその業務の範囲内に限定している。全システムとデータは定期的にバックアップされ、重要データはデータセンター間で複製されている。バグや潜在的なギャップの発見と機能向上のため、全ソフトウェアを定期的にアップグレードする。Eポストプラットフォームは、2016年次監査完了後、ドイツ連邦情報技術安全局（情報セキュリティ庁）にIT基本保護(IT Grundschutz)の基準に基づいて再証明された。また、EポストプラットフォームはTÜV情報技術有限会社に、サイトプライバシー保護基準に従い再証明を受け、リーガルとデータ保護の要求を満たしている。

米国及びEU企業の情報セキュリティに関する比較

- 情報流出等の情報資産への影響に関して
  - 情報流出・漏洩に関して、BtoCビジネスを主たる業務としている企業とBtoBビジネスを主たる業務としている企業では、流出を想定する情報の性格に違いがみられる。業務に関連が強い情報ほど、株価やレピュテーションに直結し、企業価値の損失を想定しているためだと考えられる。また米国の企業が情報の種類や記載事項に関して詳細に記述しているのに対して、EU加盟国所在企業は記載企業数が少なく、情報漏洩の種別等に関しても詳しく記述していない。
- 法的リスクへの言及に関して
  - 米国では情報セキュリティに関して法的罰則及び訴訟リスクについて言及している企業が12社であるが、ＥＵの企業では５社にとどまっている。また、米国の企業では8社が訴訟リスクに言及しているのに比べ、ＥＵでは訴訟リスクについて言及している企業が3社である。こうした差異は米国とEU諸国の会社法・商法及び訴訟手続等の法令・規則等に違いがあると考えられる。
- 平時からの事前対策に関して
  - 米国企業は平時からの情報セキュリティに係る取組を開示している企業が16社であったのに比べ、ＥＵ企業は調査対象全18社が記載していた。また、ＥＵ企業はより具体的かつ詳細な取組内容を記載している。平時からの情報セキュリティに関する取組の開示状況の差は、米国とEUで各企業に対して法令等で義務付けられている非財務分野における開示情報に関する違いが要因であると考えられる。
- その他
  - 米国及びEUの企業はともに想定インシデントとしてサイバー攻撃を挙げているが、米国企業では6社が情報セキュリティに関するテロ攻撃について言及しており、EUの調査対象企業には見られない特徴である。