Confidential

サイバーセキュリティに関する企業公開情報の調査レポート

日本IT団体連盟
サイバーセキュリティ委員会　企業評価分科会

2020年11月25日

IT連
日本IT団体連盟

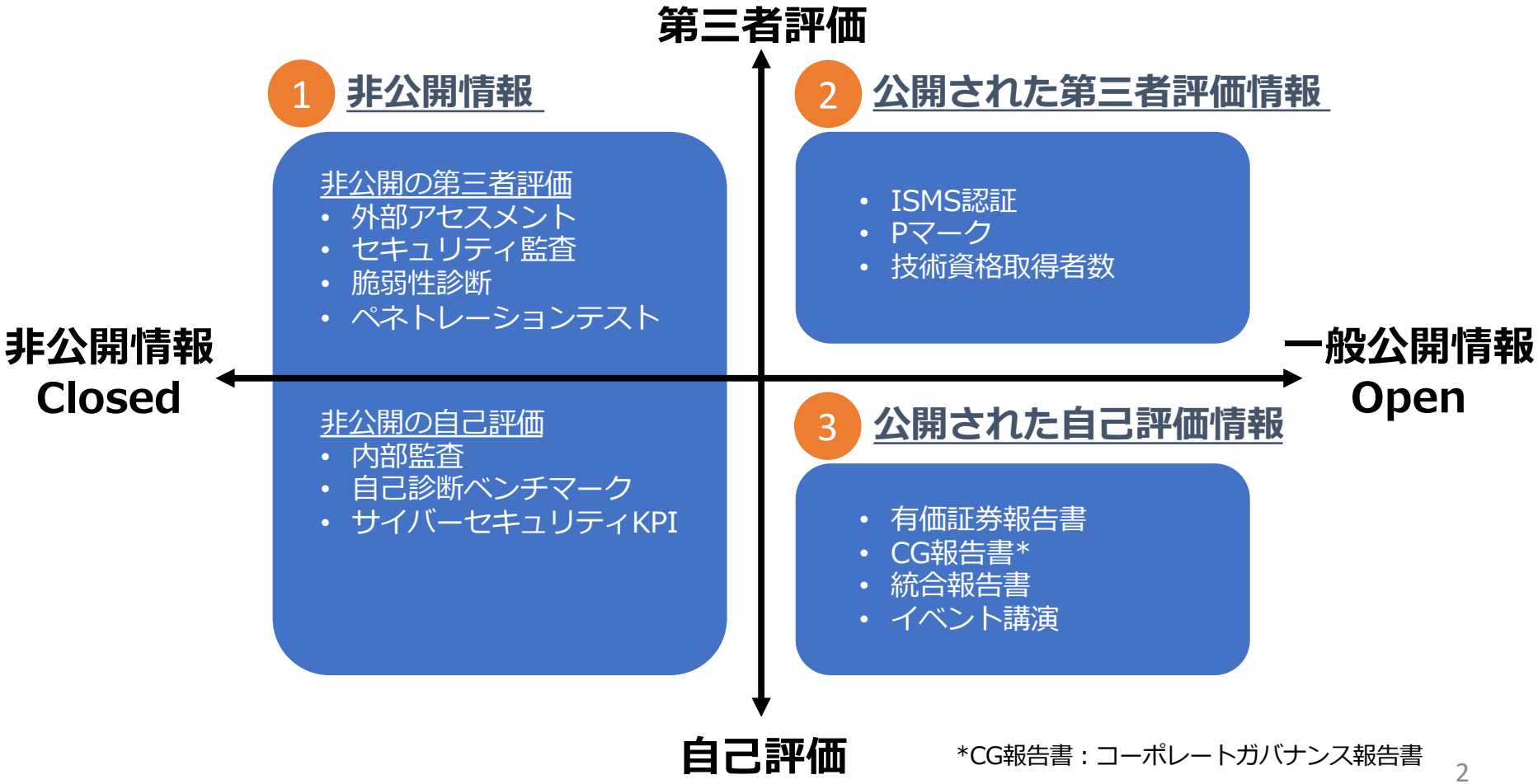
サイバーセキュリティ委員会 企業評価分科会の狙い

企業評価の意義	サプライチェーン全体において、企業の社会的責任であるセキュリティレベルの向上を実現すること
現在の課題	各企業のサイバーセキュリティ態勢の実情を比較/評価することが困難
今後の取組	咀嚼した内容の伝達・比較可能性の提供・情報開示の推進

**サイバーセキュリティに関する認証や評価を
まとめた企業の総合評価を実施**

評価情報の整理

1. **非公開情報**：非公開ではあるが、第三者や自社で評価した情報
2. **公開された第三者評価情報**：第三者による認証制度や資格制度
3. **公開された自己評価情報**：自社の取組み状況や姿勢の公開情報

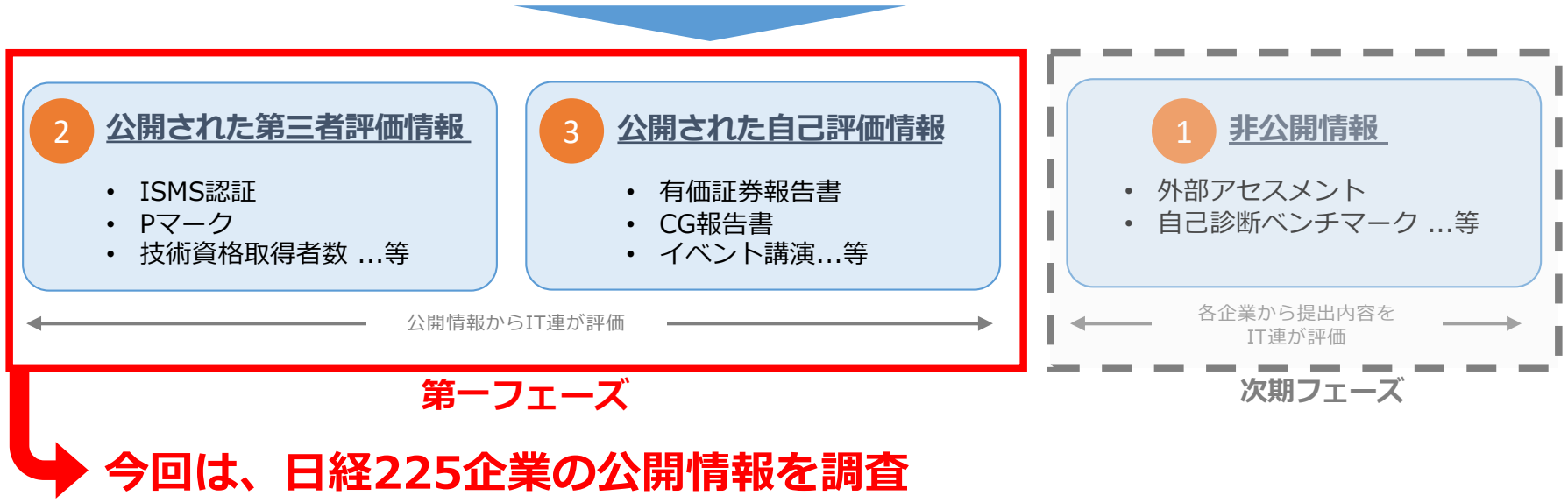


*CG報告書：コーポレートガバナンス報告書

今回の調査対象

2020年は、企業のサイバーセキュリティに関する取り組みについて、
日経225企業の公開情報を調査しました（第一フェーズ）。

	第一フェーズ	次期フェーズ
時期	2020年	2021年以降
対象企業	日経225のみ	全企業
非公開情報の評価	対象外	対象 （各企業から提出内容をIT連が評価）
公開情報の評価	対象	対象

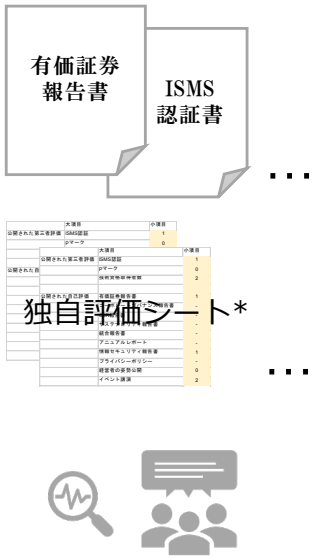


今回は、日経225企業の公開情報を調査

日経225　企業公開情報の調査

調査手法

1. 日経225を対象にした公開情報のデスクトップリサーチを実施（調査期間：2020年9月～11月）
2. 企業評価分科会で作成したIT連盟独自の調査項目をベースに、企業が対外的に発信しているセキュリティの取組み度合いを加点
3. 情報開示の業種傾向や積極的な企業事例について分科会にて分析を実施



調査項目の例

公開された第三者評価

- ISMS認証
- Pマーク
- 技術資格取得者数

公開された自己評価（株主向け）

- 有価証券報告書
- コーポレートガバナンス報告書
- 統合報告書

一般向けに公開された情報

- 自社ウェブサイト
- イベント講演

＊ 独自評価シートの内容は非公開

調査結果①（業種別）

情報開示に積極的な業種は、以下の通りでした。

順位	業種　　( ) は社数
1	**情報・通信業 (11)**
2	**建設業 (9)**
3	**保険業 (5)**
4	**銀行業 (11)**
5	**電気機器 (27)**
6	サービス業 (8)
7	卸売業 (7)
8	電気・ガス業 (5)
9	繊維製品 (4)
10	その他製品 (4)
11	小売業 (8)
11	精密機器 (4)
13	陸運業 (10)
14	不動産業 (5)
15	輸送用機器 (13)
16	機械 (15)
17	鉄鋼 (4)
18	食料品 (11)
19	医薬品 (9)
20	非鉄金属 (9)
21	ガラス・土石製品 (8)
22	化学 (17)

調査結果からの考察

- 情報・通信業は情報開示に概ね積極的であった
- 建設業は9社とも平均的に情報開示を行っていた
- 保険業、銀行業は情報開示度合いにばらつきが大きい
- また、電気機器、サービス業、卸売業においても、情報開示度合いにばらつきが大きい
- 電気・ガス業、陸運業、化学等の重要インフラ事業者では積極的な情報開示を行う企業は少ない

業種別順位の算出方式

- 業種は日経225の区分を採用
- 1業種3社以下の業種は対象外
- 順位はIT連盟が独自に作成した情報開示評価に基づき算出

調査結果②（企業別）

積極的にサイバーセキュリティ対策に関係する情報開示をすることにより説明責任を果たす事に取り組んでいる企業

社名の五十音順。公開情報をもとにIT連盟が調査分析を実施。辞退1社は上記に含まず。

情報開示事例のご紹介

㈱エヌ・ティ・ティ・データ

事業等のリスク

情報セキュリティに関するリスク

［リスクの内容と顕在化した際の影響］…社会的に重要なインフラ等を支える顧客を抱える当社にとってサイバー攻撃は特に重要なリスクであると認識しており、顕在化の可能性は日常的にあると認識しています。…

［リスクへの対応策］当該リスクを低減するため、当社は、情報セキュリティポリシーや個人情報保護方針を制定し、情報技術の進歩や社会情勢の変化に応じて、見直しや改善を実施しています。 …このほか、「情報セキュリティ委員会」のもと、外部の脅威動向と全社の活動状況、課題点を把握し、必要な施策を決定しています。更に、サイバー攻撃防止・検知のためのソリューションの導入、お客様と当社とのネットワーク環境の分離、24時間体制の監視運用を行うとともに、インシデント発生時の緊急対応のためのCSIRT組織として「NTTDATA-CERT」を設置しています。

[2020年3月期 有価証券報告書]

経営者のリスク認識と社会的影響が明記されており、その対応策として、PDCAサイクルを意識した取組み、CSIRT等の体制がわかる内容になっている。

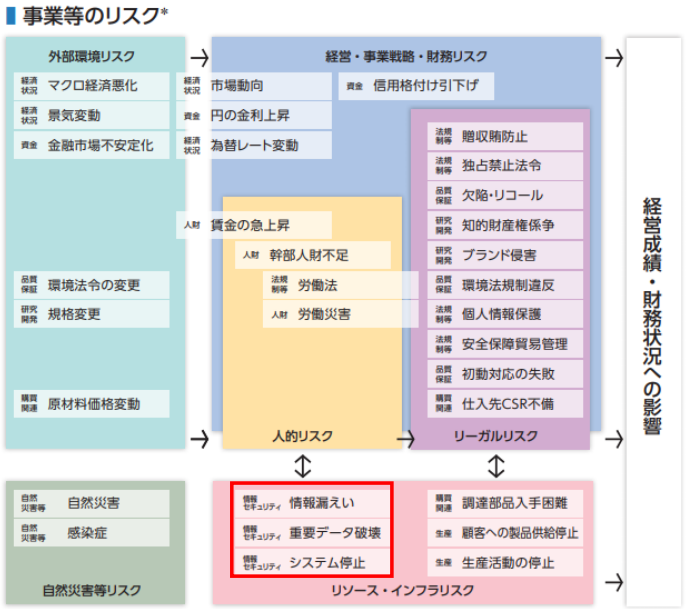
総務省「サイバーセキュリティ対策情報開示の手引き」の「(2) 開示にあたってのポイントにおける「比較容易性」を満たしている。

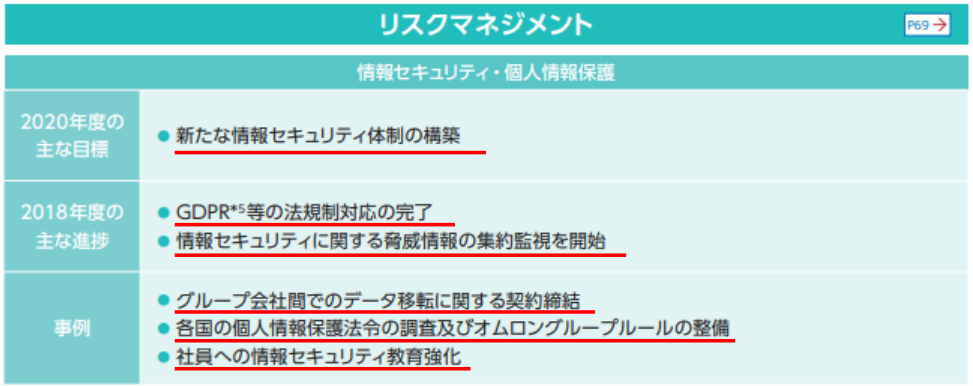
情報開示事例のご紹介

オムロン㈱

リスクマネジメント

VG2020開始と共に、現在の統合リスクマネジメントがスタートしました。…グローバルに事業を展開する中で、さまざまなリスクに対応していく必要があります。そのため、経営や財務状況に影響を及ぼしうるリスク全般を分類し、その相互関連を把握しています。…





[統合レポート2020]

リスクをどのように経営者が捉えており、どのように対応しているのかが、外形的に分かりやすい文章で、必要十分な情報をバランスよく記載している。

「理解容易性」を満たしている。

情報開示事例のご紹介

コムシスホールディングス㈱

情報セキュリティ・個人情報保護に関する教育

コムシスグループでは、個人情報を含む企業情報の漏えい事故防止のため…
情報セキュリティの基礎知識や要員としての責務を学び、社員がそれぞれの理解度を確認しながらスキルアップを図っています。

■ コムシスグループ各社のeラーニング受講修了率

(%)

会社名	2016年度	2017年度	2018年度
日本コムシス	100.0	100.0	100.0
サンコム	100.0	100.0	100.0
TOSYS	—	100.0	100.0
COMJO	100.0	100.0	100.0
CSS	100.0	100.0	100.0

4つのCSR重要課題	KPI	評価	2018年度の実績	2019年度に向けた課題および改善点
1 安心・安全の追求	重大人身※事故発生件数0件 COMJO・CSS：対象外 ※当社が定める重大人身事故の発生件数	○	0件	引き続き、重大人身事故の発生防止に努める。
	情報セキュリティ事故0件	○	0件	引き続き、情報セキュリティ事故の発生防止に努めるとともに軽微なインシデントの発生防止にも努める。

[CSR REPORT 2019*]

受講率や事故件数等、取組みの成果の可視化や定量化への努力により、ステークホルダーが客観的な評価をしやすくなっている。

「表現真正性」、「適時公表性」を満たしている。

＊ 2020年より統合報告書を発行

情報開示事例のご紹介

㈱コンコルディア・フィナンシャルグループ

CONCORDIA Financial Group

事業等のリスク

システムに係るリスク

当社グループは、保有する情報とコンピュータシステムを適切に保護するため、…システムリスクに対する体制整備をおこなうとともに、オンラインシステムに関しては、万が一、システムに障害が発生した場合に備えて、コンピュータ機器・回線の二重化や危機管理に対する訓練を実施し、早期回復をおこなえるよう努めています。またサイバー攻撃などに対応するためグループ各社が設置したCSIRTとの連携をはかるため当社にCFG-CSIRTを設置し、大規模地震などの災害に備え、オンラインシステムのバックアップセンターを設置しています。しかしながら、過失、事故、ハッキング、コンピュータウィルスの発生、システムの新規開発・更新等により重大な障害が発生し、こうした対策が有効に機能しない等の場合、当社グループの業務運営や業績、財務状態に大きな影響を与える可能性があります。

[2020年3月期 有価証券報告書]

守るべき情報資産を明記した上で、リスクに対する体制が記載されている。グループCSIRTが中心となりグループ各社のCSIRTと連携していることが分かる。

「目的適合性」を満たしている。

情報開示事例のご紹介

J.フロントリテイリング㈱

J. FRONT RETAILING

情報セキュリティへの取り組み

JFRグループでは、テクノロジーの進化およびその進化がもたらすビジネスの変革のスピードは加速度的に増し、すでに顕在化している「テクノロジーの進化に係るリスク」は、業界の垣根を破壊するデジタル・ディスラプターの攻勢や、消費者と商品・サービスを直接つなげるスマートフォンを活用したサービスの飛躍的な進歩により、リアル店舗の小売事業を中核とする当社グループに中期的に非常に大きな影響を与えると認識しています。

企業に対する情報セキュリティの確保に関する社会的な要請がますます高まる中、JFRグループでは2018年7月にセキュリティリスクを最小化するため、事業活動において徹底した情報セキュリティ管理を行い、JFRグループが保有する情報資産をリスクから適切に保護するための指針として情報セキュリティポリシーを策定しました。JFRグループの全従業員が情報セキュリティポリシーを遵守できるよう、定期的に教育や訓練を実施しています。

[サステナビリティ報告書2019]

経営者のリスク認識がメッセージとして伝わる内容であり、対策の取組み内容が関連付けて記載されている。

「目的適合性」を満たしている。

情報開示事例のご紹介

㈱スカパーＪＳＡＴホールディングス

事業等のリスク - 個人情報及び重要情報の流出や取扱い及びサイバーセキュリティに関するリスク

当社は、ISMS（情報セキュリティマネジメントシステム）の認証及びプライバシーマークを取得し、…当社グループを対象とした個人情報管理委員会・情報セキュリティ管理委員会を設置し、情報セキュリティ管理の状況をモニタリングしております。

また、セキュリティインシデント発生時の対応を行う組織としてCSIRT（シーサート、Computer Security Incident Response Team）を設置し、訓練も実施しております。一方、システム対応として、個人情報及び事業上の重要情報保管時の暗号化サーバの利用、不正侵入防止システムやウィルス対策ソフトによる感染防止、各システムによるログの取得、セキュリティ診断による脆弱性の発見等を実施しております。

[有価証券報告書－第13期]

CSIRT体制や技術対策等のセキュリティ対策が具体的に明記されており、真実を忠実に表現している。

「表現真正性」を満たしている。

情報開示事例のご紹介

ソフトバンク㈱

情報セキュリティの4つの対策

1.組織的対策

「ソフトバンクグループ情報セキュリティ対策ガイドライン」に沿って、従業員が順守すべき「情報セキュリティポリシー」を制定するとともに、情報セキュリティ管理責任者（CISO）を選任しています。…

2.人的対策

各種通信サービスなどを提供する企業として、お客さまの個人情報保護を最優先に据えて、…

3.物理的対策

4.技術的対策

[アニュアルレポート2019]

ステークホルダーが特別な専門知識がなくても理解できるよう、4つの対策に整理し、写真等を活用して外形的に分かりやすい文章で表現されている。

「理解容易性」を満たしている。

情報開示事例のご紹介

ソフトバンクグループ㈱

SoftBank Group

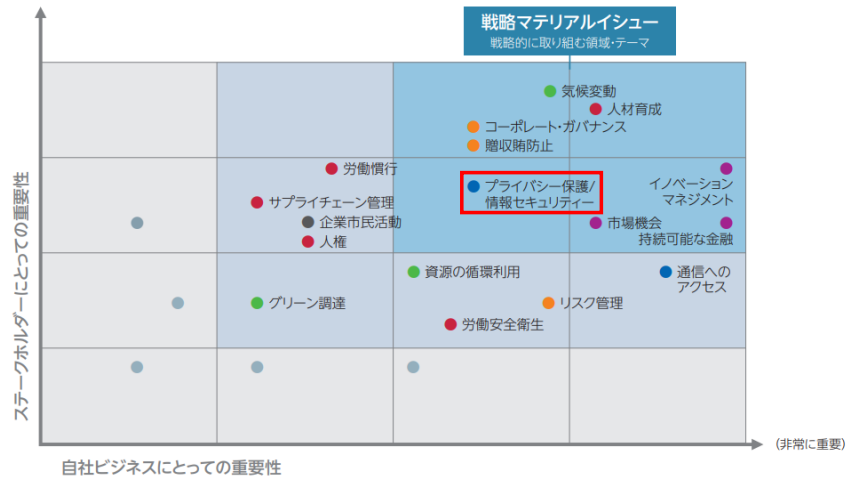
サスティナビリティ - 戦略マテリアルイシュー

当社が取り組むべきサスティナビリティに関する課題を検討し、ステークホルダーの皆様からの期待と当社グループのビジネスにおける重要性を踏まえ、戦略的に取り組むべき領域・テーマを「戦略的マテリアルイシュー」として特定しました。

活動テーマとマテリアルイシュー

活動テーマ	マテリアルイシュー
1. 知恵と知識をつなぎ、社会の成長とイノベーションを推進する	• イノベーションマネジメント • 持続可能な金融 • 市場機会
2. テクノロジーの進歩に伴う新たな課題に対応し、未来への責任を果たす	• 通信へのアクセス • プライバシー保護/情報セキュリティー
3. すべての人が自分らしく挑戦できる環境をつくり、次世代と事業の成長を図る	• 人材育成 • 労働安全衛生 • 労働慣行 • 人権 • サプライチェーン管理
4. 最先端テクノロジーを活用し、エネルギー問題をはじめとした環境課題の解決に挑む	• 気候変動 • 資源の循環利用 • グリーン調達
5. 社会をリードする企業にふさわしい透明性の高いガバナンスとコンプライアンスを実践する	• リスク管理 • コーポレート・ガバナンス • 贈収賄防止
6. グループの強みを活かし、世界中の人々とともに、社会のさらなる幸せに貢献する	• 企業市民活動

戦略マテリアルイシュー



[アニュアルレポート 2020]

他の戦略的テーマとプライバシー保護・情報セキュリティがの重要性の位置づけが明記されており、経営者の認識が伝わる内容になっている。

「目的合理性」を満たしている。

情報開示事例のご紹介

㈱ディー・エヌ・エー

ステークホルダーの立場の尊重に係る取組み状況

（個人情報・情報セキュリティ）

当社グループは、「グループ情報セキュリティポリシー」において情報セキュリティ管理に関する基本方針を定め、社長を委員長とする情報セキュリティ管理委員会及び個人情報管理委員会を設置し、セキュリティ監査、セキュリティ人材の育成、教育・啓発等を含む情報セキュリティ管理に関するさまざまな取り組みを行っています。特に、当社の子会社であり、ヘルスケア事業を営む株式会社DeNAライフサイエンスでは、情報セキュリティマネジメントシステムの適合性評価制度であるISO/IEC 27001:2013（JIS Q 27001:2014）（通称:ISMS）の認証を取得しています。また、当社の子会社であり、ヘルスケア事業を営むDeSCヘルスケア株式会社もプライバシーマーク(JIS Q15001:2017)の認証を取得しています。

[コーポレート・ガバナンスに関する報告書（2020年6月）]

機微情報を取扱う子会社において、取得した第三者認証が記載されている。

「比較容易性」を満たしている。

情報開示事例のご紹介

日本電信電話㈱

セキュリティ推進体制・マネジメント体制

　グループCISO委員会を中心に、NTTグループ各社と連携したガバナンス体制を構築しています。2018年度はグループCISO委員会を4回、セキュリティマネジメント連絡会を6回開催しました。…

[アニュアルレポート 2019]

セキュリティガバナンス体制が概念図で整理されており、それぞれの役割や関係性が簡潔にまとめられている。また、委員会や連絡会の実施回数が明記されている。

「理解容易性」を満たしている。

情報開示事例のご紹介

富士通㈱

サステナビリティマネジメント - 情報セキュリティ管理

GDPR対応

富士通は、グローバルでの個人情報保護体制を構築し、個人データ保護の強化を図っています。CISO組織と法務部門主導の下、海外リージョン等と連携し、GDPRに対応するための権利保護に関するガイドラインや社内規定、ルールの整備、設計・初期設定時のチェックシートの作成、運用プロセスへの反映や従業員教育を実施しています。個人データのEU域外移転規制への対応として、お客様から処理の委託を受けた個人データの取り扱いに関する、グループの共通ルールを定めた個人データ処理者のための拘束的企業準則（BCR-P）を2017年12月にオランダの欧州データ保護機関に申請しました。

また、2019年1月23日、欧州委員会によって日本とEU間の十分性認定が発効されたことを受け、当該十分性認定に基づき域外移転を行った個人情報の取り扱いに関する社内ルールを整備・周知しました。

[統合レポート2019]

新たな法制度への対応が整備されたことを、ステークホルダーの関心があるタイミングで具体的かつ簡潔に記載されている。

「適時公表性」を満たしている。

今後の予定

2021年以降、次期フェーズとして「対象企業の拡大」、及び「非公開情報の評価」も行う予定です。

	第一フェーズ	次期フェーズ
時期	2020年	2021年以降
対象企業	日経225のみ	全企業
非公開情報の評価	対象外	対象 （各企業から提出内容をIT連が評価）
公開情報の評価	対象	対象

2 **公開された第三者評価情報**
- ISMS認証
- Pマーク
- 技術資格取得者数 …等

3 **公開された自己評価情報**
- 有価証券報告書
- CG報告書
- イベント講演…等

1 **非公開情報**
- 外部アセスメント
- 自己診断ベンチマーク …等

公開情報からIT連が評価

各企業から提出内容を
IT連が評価

次期フェーズ

（参考）
東証一部上場企業（全社）の情報開示動向

東証一部上場企業（全社）の制度公開報告書を調査したところ、有価証券報告書でセキュリティに関するリスク事項を公開している企業は74%、コーポレートガバナンス報告書では42%でした。

	有価証券報告書		コーポレートガバナンス報告書	
	記載社数	記載率	記載社数	記載率
2019年11月調査（n=2,139）	1,231	58%	918	43%
2020年10月調査（n=2,176）	1,603	↗ 74%	873	→ 42%

有価証券報告書の
記載率が大幅アップ

検索条件：〔上場市場 ： 東証一部 〕、〔 キーワード ： 「システムリスク OR 情報セキュリティ OR サイバーセキュリティ OR 個人情報 OR プライバシー OR サイバー攻撃 OR 不正アクセス」を含む 〕

（参考）
総務省「サイバーセキュリティ対策情報開示の手引き」

（２）開示にあたってのポイント

①目的適合性

- 記載事項の決定にあたっては、ステークホルダーへの説明責任を果たすために開示を行うという目的を踏まえること
- 以下の②～⑤を踏まえつつ、ステークホルダーにとって有益と思われる情報を提供すること

② 表現真正性

- 自社のサイバーセキュリティ対策について、真実を忠実に表現すること
- 情報の完全性、中立性、合理性を可能な限り確保すること

③ 比較可能性

- 同業種・同規模間、同じ企業の異時点間等の一定の範囲で比較可能にするための基礎となる情報を提供すること
- 定量的な情報や、対策の有無が直接記載の有無につながるような情報など、客観的な評価が可能な情報を記載すること

④ 理解容易性

- 読み手に特別な専門知識がなくても理解できるよう、簡潔かつ明瞭な表現で十分な情報を記載すること
- 必要に応じて専門用語に注釈等を付すこと
- 概念図や写真等を活用し、読み手に受け入れやすいものとすること

⑤ 適時公表性

- 社会的に大きなインシデント等の発生後や新たな法規制の導入など、ステークホルダーの関心があるタイミングで適切な情報を速やかに公表すること

出所：総務省「サイバーセキュリティ対策情報開示の手引き」（2019年6月）
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00032.html

ありがとうございました。