資料９－１

サイバーセキュリティ対策情報開示の手引き

（案）

総務省　サイバーセキュリティ統括官

2019 年(平成 31 年）※月

目 次

はじめに

Society5.0 の実現に向けて、5G、IoT、AI をはじめとして ICT の利活用が社会・経済のあらゆる局面に浸透している今日において、企業が適切なサイバーセキュリティ対策をとることは経営層が認識すべき重要な経営課題となっています。その上で、各企業のサイバーセキュリティ対策の実施状況について適切に開示して説明責任を果たすことを通じ、利用者や取引先企業、さらには社会からの信頼感がより一層得られることが期待されます。

このため、総務省では、2017 年（平成 29 年）12 月より、総務省サイバーセキュリティ統括官の私的懇談会である「サイバーセキュリティタスクフォース（座長：東京電機大学　安田浩学長）」の下で「情報開示分科会（主査：弁護士法人英知法律事務所　岡村久道弁護士）」を開催し、民間企業におけるサイバーセキュリティ対策の情報開示を促進するため、議論を進めてきたところです。

本文書は上記の分科会において、企業が自らのサイバーセキュリティ対策の情報開示の在り方を検討する上で参考となる手引きとしてとりまとめたものであり、企業においてサイバーセキュリティ対策の検討・実施及び対策の開示を推進する上での一助となることを期待します。

2019 年（平成 31 年）○月
総務省　サイバーセキュリティ統括官

本編　サイバーセキュリティ対策情報開示の手引き

1．本手引きの趣旨・目的

（1）サイバーセキュリティリスクの増大と対策の必要性

今日の社会・経済において、ICT（Information and Communications Technology：情報通信技術）の利活用は必要不可欠となっている。例えば、

- ✓ 通信ネットワークに関しては、ブロードバンドサービスの普及率が 99%を超え、もはや社会・経済活動において必要不可欠な基幹インフラとなっている。【ブロードバンド化】
- ✓ クラウドサービスの普及が進み、各ユーザがネットワーク経由で様々なアプリケーション・情報サービスを安価で利用できる時代になっている。【クラウド化】
- ✓ また、ここ数年のスマートフォンの普及に伴ってモバイル化が進み、企業活動や生活の隅々にまで ICT の利活用が浸透し始めている。【モバイル化】
- ✓ IoT を活用した既存のビジネスモデルや業務プロセスの高付加価値化が進展し、企業の競争力の差別化要因になっていくことが想定される。【IoT 化】

このように、ICT 分野のブロードバンド化、クラウド化、モバイル化、IoT 化に伴い、これまで我が国のデジタル経済は急速に発展してきたほか、様々な産業でのデータの収集・分析・活用が進み、高付加価値化が進んでいるところである。

2019 年（平成 31 年）を目途に 5G 携帯電話サービスが開始されることにより、このような流れはより一層加速していくことが予測され、我が国が目指すべき社会像としての Society5.0 の到来を迎え、今後、サイバー空間とフィジカル空間の一体化が一層進展していくことが想定される。

他方、社会・経済のあらゆる局面で ICT の利活用が水や空気のように浸透するにつれ、サイバーセキュリティリスクも必然的に増大している。オンラインショッピングや行政サービスの利用などの一般の利用者の日常生活から、BtoB のサプライチェーンなどの企業活動に至るまで、今日の社会・経済は様々なサイバーセキュリティリスクにさらされている。

サイバーセキュリティリスクの大きさはインシデントの影響度の大きさと発生確率で表されるが、社会や経済の ICT への依存度が高まれば高まるほど、インシデントが起きた際の影響が大きくなり、またインシデントが起きる可能性も高くなる。

こうした中、サイバーセキュリティ対策に対する社会的要請は非常に大きくなっており、企業における重要な経営課題の一つとして位置づけられるべきものとなっている。

例えば、個人情報保護委員会によると、2016 年度（平成 28 年度）中に事業者が公表した個人情報漏えい事案（所管府省において把握したものに限る）のうち、漏えいした個人情報が 5 万件超の事案 22 件のうち 19 件が不正アクセス等によるサイバー攻撃事案となっている。

【図 1 ：公表された個人情報の漏えい状況】

漏えいした人数	平成 28 年度		平成 27 年度	
	件数	（割合）	件数	（割合）
500 人以下	145	（55.1%）	187	（64.0%）
501～ 5,000 人	53	（20.2%）	51	（17.5%）
5,001～ 50,000 人	39	（14.8%）	39	（13.4%）
50,001 人以上	22	（8.4%）	14	（4.8%）
不明	4	（1.5%）	1	（0.3%）
合計	263	（100.0%）	292	（100.0%）

電子媒体のみ	紙媒体のみ	電子媒体と紙媒体	不明
78	64	3	1
36	17	0	0
29	10	0	0
22	0	0	0
3	0	0	0
168	91	3	1

【図２：平成 28 年の個人情報漏えい事案】

	事業者	所管府省	公表日	漏えい人数（最大）	漏えい情報（主なもの）	漏えいの原因 *（斜体は報告書には無い追記事項）*
1	株式 会社A	総務省	平成28年6月21日	約62万件	会員ID、会員パスワード、氏名、生年月 日、性別、メールアドレス、住所、職業、 電話番号、ポイント 情報、決済手段区 分、PAIDメンバーID	不正アクセス *（ぜい弱性）*
2	株式会社B	総務省	平成28年6月14日	約33万件	氏名（漢字、カタカナ、ローマ字）、性別、 生年月日、メールアドレス、郵便番号、住 所、電話番号、パスポート番号、パスポート取得日	不正アクセス *（JTB関連）*
3	株式会社C	総務省	平成28年6月22日	約98万件	注文者氏名、注文者住所、注文者メール アドレス（PC/携帯）、注文者電話番号、 注文者コメント、管理者コメント、配送先 氏名、配送先住所、配送先電話番号、注 文金額、送状番号	不正アクセス *（設定ミスによるファイル蔵置）*
4	株式 会社D	総務省	平成28年4月21日	約43万件	・氏名、住所、メールアドレス、電話番号 等	不正アクセス（OSコマンド イン ジェクション）
5	株式会社E	総務省	平成28年4月22日	約64万件	・氏名、住所、メールアドレス、電話番、性別、年齢、職業	不正アクセス（OSコマンド イン ジェクション）
6	株式会社F	総務省	平成28年7月25日	約12万件	・パスワード、メールアドレス、電話番号、住所、生年月日、氏名	不正アクセス（SQLインジェクション）
7	株式会社G	国土交通省（観光庁）	平成28年6月14日	約678万件	氏名、性別、生年月日、メールアドレス、 住所、郵便番号、電話番号、パスポート 番号、パスポート取得日	外部からの不正アクセス *（添付ファイル）*
8	協会H	厚生労働省	平成29年2月17日	約19万人分	氏名、健康保険証の記号番号、医療機 関コード、再審査を求める理由、再審査 結果	紛失（誤廃棄の 可能性） *（FD、CD等）*
9	株式会社I	経済産業省	平成28年12月2日	約42万件	氏名、性別、生年月日、年齢、職業、電 話番号、メールアドレス、住所、購入履 歴、ログインパスワード、一部クレジットカード情報（カード会員名、カード番号、カード有効期限）	不正アクセス *（ぜい弱性）*
10	公益社団法人J	経済産業省	平成29年4月25日	約15万件	住所、氏名、電話番号、生年月日、ログインID、パスワード、メールアドレス 一部クレジットカード情報（カード会 員名、カード番号、有効期限、セキュリティコード）	不正アクセス *（Apache Struts2 ぜい弱性）*
11	株式会社K	経済産業省	平成29年3月23日	約118万件	氏名、生年月日電話番号、住所、性別、メールアドレス	不正アクセス *（Apache Struts2 ぜい弱性）*
12	株式会社L	経済産業省 総務省	平成29年3月10日	約40万件	メールアドレス、クレジットカード番号、クレジットカード有効期限、セキュリティコード、カード払い申込日、住所、氏名、電話 番号、生年月日、メールアドレス、加入月	不正アクセス *（Apache Struts2 ぜい弱性）*
13	株式 会社M	経済産業省	平成29年3月10日	36万件	クレジットカード番号、有効期限、メール アドレス	不正アクセス（Apache Struts2 ぜい弱性）
14	株式会社N	経済産業省	平成28年4月11日	約20万件	ユーザーID、パスワード、氏名、住所、電 話番号、メールアドレス、生年月日の内 顧客が登録した情報、加えて、537件はクレジットカード番号、有効期限、セキュリティコード	不正アクセス
15	株式 会社O	経済産業省	平成28年4月28日	約64万件	氏名、性別、住所、メールアドレス、家族に関する情報 ※漏えい項目は公表せず。	不正アクセス *（ケータイキットぜい弱性）*
16	株式会社P	経済産業省	平成28年4月27日	約13万件	氏名、住所、電話番号、メールアドレ ス、ログイン会員ID及びパスワード、クレジットカード情報（カード番号、有 効期限、カード名義、セキュリティコード）うち、カード情報は7386件	不正アクセス *（OpenSSLぜい弱性）*
17	株式会社Q	経済産業省	平成28年8月23日	約21 万件	氏名、住所、電話番号、法人担当者 名 ※漏えい項目は公表せず。	外付けハードディスクの紛失
18	株式会社R	経済産業省 総務省	平成28年8月26日	約11 万件	クレジットカード情報（カード番号、カード 名義、有効期限、セキュリティコード）、会 員情報（メールアドレス、パスワード、氏 名、住所、電話番号、その他の登録情 報）	不正アクセス *（ぜい弱性）*
19	株式会社S	経済産業省 総務省	平成28年5月11 日	約5万件	ニックネーム、メールアドレス、生年月 日、居住地域、性別 仮想通貨「コイン」の履歴情報	不正ログイン（リスト型攻撃）
20	株式会社T	経済産業省 総務省	平成28年11月29日	約58万件	ニックネーム、メールアドレス、生年月 日、居住地域、性別 仮想通貨「コイン」の履歴情報	不正アクセス *（リスト型攻撃）*
21	株式会社U	経済産業省	平成29年1 月1日	約5万9千件	メールアドレス、氏名、生年月日、性 別、住所、郵便番号、電話番号	不正アクセス *（SQLインジェクション）*
22	株式会社W	経済産業省	平成29年2 月27日	約120万件	氏名、住所、電話番号、生年月日、メールアドレス、性別 クレジットカード番号、カード有効期限	バックアップストレージの 盗難

このような事情を踏まえると、利用者の目線からすれば、自らの個人情報等を取り扱う企業が機密性の観点から適切なサイバーセキュリティ対策をとっているか否かが大きな関心事項となっている。平成 29 年版情報通信白書 [1]によれば、多くの人が、個人情報の企業への提供に対し、「不安」である一方で「仕方なく」個人情報を提供しているという認識の下でサービスを利用している実態があるため、企業側がより一層個人に対する説明責任を果たし、サービス向上に取り組んでいくことで、利用者の理解及び認識を高め、互いに Win-Win 関係を築いていくことの重要性が指摘されている。今後、特に PDS（パーソナルデータストア）や情報銀行など新たなビジネスモデルが出てくる中で、機密性の高い個人情報等を扱う機会が増える企業にとって、適切なサイバーセキュリティ対策の実施は重要な経営課題となっている。

サイバーセキュリティ対策の重要性の高まりは、個人情報に限られず、企業の業務システムについても該当する。従来、業務用システムについては、インターネットと直接接続しておらず、サイバー攻撃を受ける可能性は低いと考えられてきた。しかし、諸外国では、電力会社や原子力発電所等の業務用システムがサイバー攻撃を受ける事例も出てきており、今後 IoT 機器・システムの利用が進展していく中で、業務用システムにおいてインシデントが発生するリスクも高まっていくものと思われる。このような状況を踏まえ、企業活動を円滑かつ継続的に行う上で、システムの可用性や完全性の観点から適切なサイバーセキュリティ対策がとられているか否かについては、当該企業のみならず、一般消費者や取引先、株主など、当該企業に関係する様々なステークホルダーにとっても関心事項となり得るものである。また、サイバー攻撃によって自社にとって極めて高い価値を有する技術情報が外部に流出する可能性もあるなど、当該企業そのものにとっても重要な経営課題であることは論を待たない。

さらにいえば、サイバー攻撃の被害は、直接攻撃を受けた企業やその顧客にとどまらない。現代の生活やビジネスが各種の情報・取引のネットワークに依拠している中で、攻撃者は、さまざまな手法であらゆる企業や個人の利用ネットワークに不正アクセスし、一つの攻撃を契機に、当該企業が踏み台となって多数の企業に被害を発生させ、その連鎖被害がさらに別の多くの企業や多数の個人に及ぶ危険性も想定される。そして、その被害の種類は、企業情報・営業秘密、企業ブランド毀損、関連する個人情報・個人資産など広範囲に及ぶ可能性がある。ICT の利活用が進み、あらゆる組織・人・物が情報通信ネットワークでつながる社

[1] 平成 29 年度「情報通信白書」
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc122510.html

会になると、このような「被害のチェーン」が情報通信ネットワークを介して発生する可能性がある。

今日の社会の安心・安全を確保する上で、サイバーセキュリティは最も基本的な構成要素の１つである。様々なサイバーセキュリティリスクにさらされている中で、昨今、企業は経済・社会の構成要素として、社会的責任を適切に果たし、自らを取り巻く様々なステークホルダーからの信頼を得て、企業活動を円滑かつ継続的に展開していくためには、適切なサイバーセキュリティ対策をとる必要があり、今後その重要性はますます増していくことが想定される。

（２）サイバーセキュリティ対策の情報開示の意義

前述のように、企業においてサイバーセキュリティ対策は重要な経営課題となっているが、企業としての社会的責任を果たし、ステークホルダーからの信頼を得るためには、サイバーセキュリティ対策の実施のみならず、その内容について適切な情報開示が重要である。

ステークホルダーの視点からすれば、例えば以下のような観点でサイバーセキュリティ対策に係る情報開示がなされると企業への信頼感が増すと考えられる。

- ✓ 取引先の視点では、自らの継続的な経済活動に必要なサービス・商材を調達している企業が適切なサイバーセキュリティ対策をとっていること等の開示がなされること。

- ✓ 一般の利用者の視点では、自らの個人情報や秘匿すべき情報を取り扱う企業が、当該情報の適切な取扱いや管理策を含め、適切なサイバーセキュリティ対策をとっている旨の開示がなされること。さらに、一般の利用者はメディアを通じて情報を入手することから、メディアの視点からも、このような情報開示がなされること。

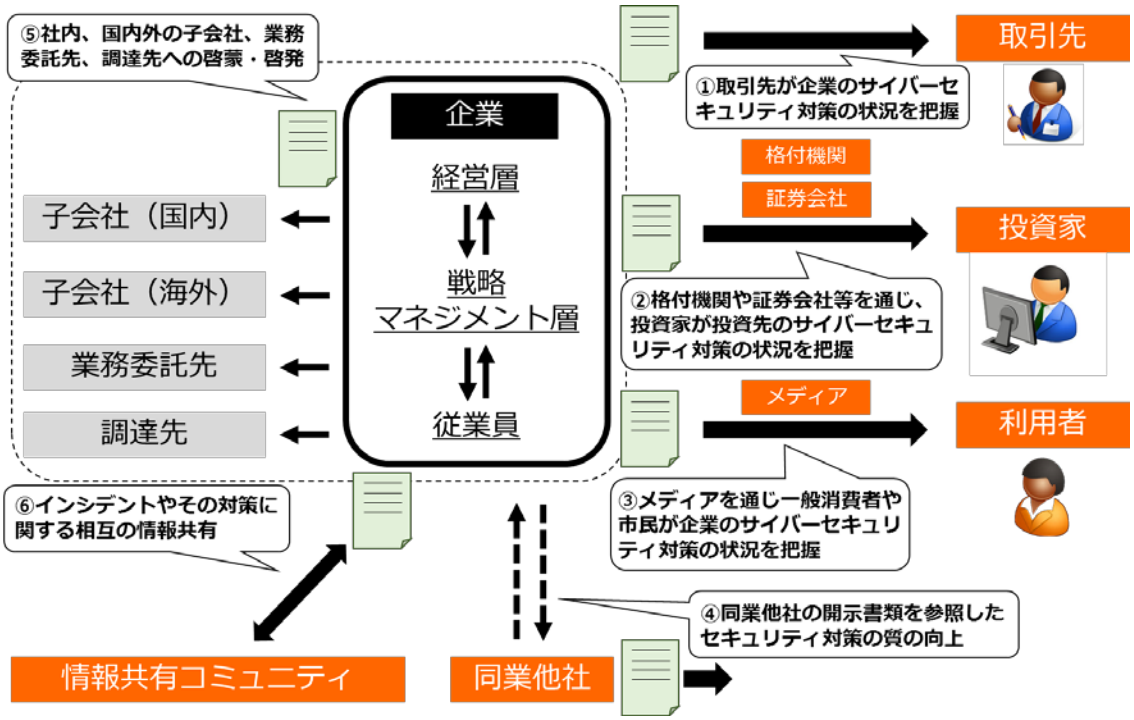
- ✓ 投資家の視点では、自らが投資している、または投資すべきと考えている企業が、企業活動に支障をきたさないよう、システムの機密性・完全性・可用性の観点から適切なサイバーセキュリティ対策をとっている旨の開示がなされること。また、投資家と企業を媒介する立場の証券会社等の視点からも、同様の情報開示がなされること。

上記のような観点から様々なステークホルダーに対して適切な情報開示がなされることで、ステークホルダーが企業のセキュリティ対策の状況を適切に把握・評価し、その上で企業がステークホルダーからの評価に基づき、サイバーセキュリティ対策の質の向上への取組をさらに進めていく、という社会構造になることが重要である。

なお、付言すれば、サイバーセキュリティ対策の情報開示は企業の立場からすれば、以下のような効果も期待できる。

- ✓ サイバーセキュリティ対策の情報開示を目指すことによって、開示内容に対応するよう、自社、子会社、業務委託先、調達先等のサイバーセキュリティ対策の質の向上の取組が進展すること。
- ✓ ステークホルダーからの信頼と高い評価を得て、自社の社会的評価や自社の商品・サービスのブランド価値の向上につながることが期待される。
- ✓ 対外的な情報開示が社内や子会社・グループ会社、外部委託先のサイバーセキュリティ対策の意識向上の観点に寄与するなど、関係者に対する啓蒙・啓発の観点からの効果が期待される。
- ✓ ISAC などの情報共有コミュニティでの情報共有や、同業他社の開示情報の参照を通じ、自社のサイバーセキュリティ対策の質の向上の契機になることが想定される。

【図３：企業をとりまくステークホルダーとサイバーセキュリティ対策の情報開示】



以下は、本手引きの策定に当たって開催したサイバーセキュリティタスクフォース情報開示分科会や実施した企業ヒアリングによる、実際の有識者や企業等からの声である。

- サイバーセキュリティに関する情報を報告書等において開示することにより、報告書が自社製品・サービスの営業・販促ツールとして利用されるようになっている。【取引先との関係】

- 情報を開示することにより生じるリスクもあるが、一方で信頼の輪を構築することにもつながる。それにより、信頼に基づく情報共有の推進が可能になる。またそのような信頼ベースのコミュニティにおいて、自社の取組に対するフィードバックを受けることができ、セキュリティ対策の向上につなげることができる。【コミュニティとの関係】

- IoT など新技術の利活用を積極的に推進することで投資家にアピールし、攻めの IT 経営銘柄に選定されることを目的としており、利活用に付随する取組としてサイバーセキュリティ対策についても開示している。【投資家との関係】

- 近年、個人情報の取扱いに対する顧客の見る目が厳しくなっていることや、問合せが増加していることなどを踏まえ、サイバーセキュリティ対策について情報開示を行い、広く一般に対して個人情報の適切な取扱いについて示す必要があると考えている。【一般の利用者との関係】

- 開示書類という形でサイバーセキュリティに関する社の姿勢をわかりやすく対外的に打ち出すことによって、社内の意識を醸成したり、現場の統制をかけたりする効果がある。【従業員との関係】

- 社内で勉強会を開催して、同業他社の開示事例をケーススタディとして勉強し、参考にしている。【社内との関係】

- 業務委託先がインシデントを起こすケースが後を絶たない中で、自らの対策内容を開示することで、業務委託先にもチェックがかかるようにしていき、当社と同等まで対策レベルを引き上げていきたい。【業務委託先との関係】

このように、サイバーセキュリティ対策の情報開示は、一義的には企業の社会への説明責任を果たし、ステークホルダーからの信頼を得る営みに位置づけられるものではあるが、自社のサイバーセキュリティ対策の強化にもつながることを意識する必要がある。

（3）本手引きについて

①　本手引きの目的

前述のとおり、今日において、企業におけるサイバーセキュリティ対策の実施やその対策の開示はステークホルダーからの信頼を得るのに重要な取組の１つとなっている。

一方で、サイバーセキュリティ対策については、各企業の経営状況なども踏まえた最適な解がそれぞれ存在し得る。また、一般論として全てのサイバーセキュリティ対策を詳細に開示した場合には逆にサイバー攻撃等を誘発するリスクもあることから、サイバーセキュリティ対策の開示の内容や方法は、各企業で経営層の責任の下で検討が必要である。

本手引きでは、このような事情を踏まえ、開示書類におけるサイバーセキュリティ対策の開示項目の例を示すとともに、既に公開されている開示書類の事例集を掲載することで、各企業が情報開示の在り方を検討する際の参考資料となることを目的とする。

なお、サイバーセキュリティ対策の情報開示は現時点であくまで任意の取組であるため、本手引きも強制力を持つものでは決してなく、あくまで開示の項目などの例を示したもので、最終的には開示の在り方や内容は各企業の経営判断として決定されるべきものということを明記しておく。

②　想定する本手引きの参照主体

本手引きの内容については、最終的には企業の意思決定に責任を負う経営層も把握していただきたいものであるが、社内のサイバーセキュリティ対策の実務担当者を中心に、企業における広報や情報開示の実務担当者、社内・業務用システムの実務担当者等の実務において参照していただきたい。

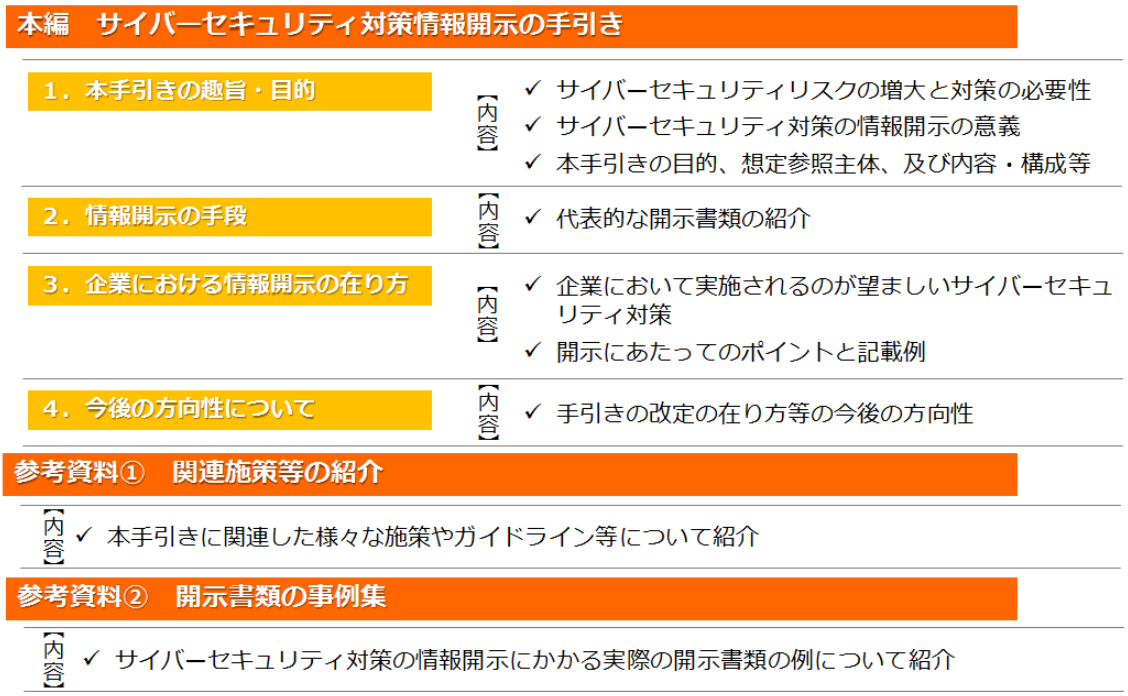
③　本手引きで扱う情報開示について

サイバーセキュリティ対策の情報開示はその開示の相手先と企業との関係性によって様々な粒度・形態の開示が想定されるが、一般に NDA（Non-Disclosure Agreement：秘密保持契約）を締結している場合や資本関係がある場合など特殊な紐帯関係のある相手先への情報の開示については、当事者間の合意ベースでなされるべきものであることから、本手引きにおいては、開示書類を通じた不特定多数のステークホルダー向けの情報開示を取り扱うこととする。

④　本手引きの内容・構成について

「本編　サイバーセキュリティ対策情報開示の手引き」で、情報開示の項目などについて紹介し、「参考資料①　関連施策等の紹介」で本手引きに関連した施策等について、「参考資料②　サイバーセキュリティ対策の情報開示に係る事例集」において、実際の開示書類について紹介することとする。

【図４：本手引きの内容・構成について】



なお、本手引きにおいて「サイバーセキュリティ」とは、サイバーセキュリティ基本法（平成 26 年法律第 104 号）第２条に規定する「サイバーセキュリティ」をいい、具体的には、いわゆる「情報のＣＩＡ」、つまり、情報の機密性（confidentiality）・完全性（integrity）・可用性（availability）の確保のために必要な措置及び情報システムや情報通信ネットワークの安全性・信頼性の確保のために必要な措置等を講じ、その状態を維持管理することが求められる。

２．情報開示の手段

実際に情報開示を行うに当たっては、様々な開示書類を活用することとなる。現在、サイバーセキュリティ対策の情報開示に活用されている主な開示書類は以下のとおりである。

①　有価証券報告書【制度開示】

金融商品取引法（昭和 23 年法律第 25 号）第 24 条に基づき、有価証券の発行者である会社は、事業年度ごとに、当該会社の商号、当該会社の属する企業集団及び当該会社の経理の状況その他事業の内容に関する重要な事項その他の公益又は投資者保護のために必要かつ適当な事項について記載した報告書（有価証券報告書）を内閣総理大臣に提出することが義務づけられている。

②　コーポレート・ガバナンス報告書【制度開示】

有価証券上場規程（平成 19 年 11 月 1 日東京証券取引所）第 204 条第 12 項第 1 号等に基づき、新規上場申請者は、コーポレート・ガバナンスに関する事項について記載した報告書（コーポレート・ガバナンス報告書）を提出することとされている。また、上場後、その内容に変更があった場合は、遅滞なく変更後の報告書を提出することとされている。コーポレート・ガバナンス報告書については、コーポレート・ガバナンスに関する基本的な考え方及び資本構成、企業属性その他の基本情報等を記載することとされている。

③　CSR 報告書／サステナビリティ報告書【任意開示】

CSR（企業の社会的責任）報告書は、環境や社会問題などに対して企業は倫理的な責任を果たすべきであるとする CSR の考え方に基づいて行う企業の社会的な取組をまとめた報告書であり、サステナビリティ（持続可能性）報告書とも呼ばれている。環境、労働、社会貢献などに関する情報や、事業活動に伴う環境負荷などが幅広く公表されている。

④　統合報告書【任意開示】

2013 年に国際統合報告評議会（IIRC）から「国際統合報告フレームワーク」が公表されたが、同フレームワークでは、「統合報告」を「財務資本の提供者に対し、組織がどのように長期にわたり価値を創造するかを説明すること」と位置づけている。我が国においては、

これを受け、「統合報告書」という名前の書類を活用して、財務情報と非財務情報を連動して開示するケースが増えつつある。

⑤　アニュアルレポート【任意開示】

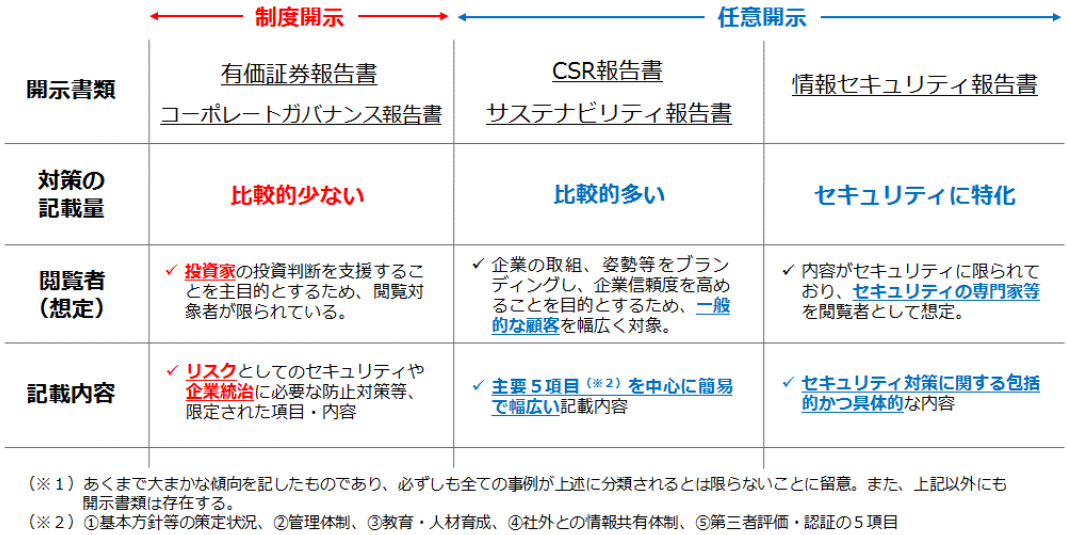
「年次報告書」とも呼ばれ、企業が年度末に株主や投資家、金融機関、取引先などの関係先に配布する、経営内容についての総合的な情報を掲載した冊子。

⑥　情報セキュリティ報告書【任意開示】

2007 年（平成 19 年）９月に経済産業省が「情報セキュリティ報告書モデル」を公表しており、企業の情報セキュリティの取組の中でも社会的関心の高いものについて情報開示することにより、当該企業の取組が顧客や投資家などのステークホルダーから適正に評価されることを目指している。同モデルにおいては、①報告書の発行目的といった基礎情報、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・認証等を基本構成としている。

なお、現状、サイバーセキュリティ対策に係る記載の量は、任意開示の書類（CSR 報告書、サステナビリティ報告書）が比較的多い傾向にあり、制度開示（有価証券報告書、コーポレート・ガバナンス報告書）の書類では比較的少ない傾向にある。

【図５：各開示書類の記載内容の現状と傾向】



（※１）あくまで大まかな傾向を記したものであり、必ずしも全ての事例が上述に分類されるとは限らないことに留意。また、上記以外にも開示書類は存在する。
（※２）①基本方針等の策定状況、②管理体制、③教育・人材育成、④社外との情報共有体制、⑤第三者評価・認証の５項目

（出典）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報告書（平成 30 年３月）をベースに総務省作成

3．企業における情報開示の在り方

（1）企業において実施されるのが望ましいサイバーセキュリティ対策

企業においては事業内容や経営戦略に即して最適なサイバーセキュリティ対策[2]を講じていくことが期待されるが、一般的な対策の内容としては概ね以下のとおりである。

① サイバーセキュリティ対応方針策定

サイバーセキュリティリスクを経営リスクの一つとして認識し、組織全体での対応の基本方針（セキュリティポリシー）を策定する。

② 経営層によるリスク管理体制の構築

サイバーセキュリティ対策を行うため、サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築する。その際、組織内のその他のリスク管理体制とも整合を図る。

③ 資源（予算、人員等）の確保

サイバーセキュリティリスクへの対策を実施するための資金確保とサイバーセキュリティ人材の確保を実施する。

④ リスクの把握と対応計画策定

経営戦略の観点から守るべき情報を特定した上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を策定する。その際、サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、残留リスクを識別する。

⑤ 保護対策（防御・検知・分析）の実施

サイバーセキュリティリスクに対応するための保護対策（防御・検知・分析に関する対策）を実施する体制を構築する（対応計画は④で策定）。

[2] 上述の①～⑩の対策については、経済産業省及び独立行政法人情報処理推進機構が策定している「サイバーセキュリティ経営ガイドライン Ver2.0」及び「サイバーセキュリティ経営ガイドライン Ver2.0 実践のためのプラクティス集」を参照。

⑥　ＰＤＣＡの実施

計画を確実に実施し、改善していくため、サイバーセキュリティ対策を PDCA サイクルとして実施する。その中で、定期的に経営者に対策状況を報告し、問題が生じている場合は改善する。またステークホルダーからの信頼性を高めるため、対策状況を開示する。（①の方針に基づいて②の体制で④の計画に基づいて対策を実施し、その結果について評価し、更に①や②や④に反映する。）

⑦　緊急対応体制の整備

影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を速やかに実施するための組織内の対応体制（CSIRT 等）を整備する。被害発覚後の通知先や開示が必要な情報を把握するとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備する。また、インシデント発生時の対応について、適宜実践的な演習を実施する。

⑧　復旧体制の整備

インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備を行う。BCP との連携等、組織全体として整合のとれた復旧目標計画を定める。また、業務停止後からの復旧対応について、適宜実践的な演習を実施する。

⑨　取引先・委託先やグループ単位のサイバーセキュリティ対策

監査の実施や対策状況の把握を含むサイバーセキュリティ対策の PDCA について、系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用をする。システム管理等の委託について、自組織で対応する部分と外部に委託する部分で適切な切り分けをする。

⑩　情報共有活動への参加

社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、サイバー攻撃に関する情報共通活動へ参加し、積極的な情報提供及び情報入手を行う。また、入手した情報を有効活用するための環境整備を行う。

企業におけるサイバーセキュリティ対策としては、いずれも重要であり、利用者等からすれば、これらの実施状況が開示されることにより、商品・サービスの選択などの際の参考になると考えられる。

なお、情報開示の在り方はステークホルダーによって異なる。例えば、企業と直接の紐帯関係のない一般消費者や投資家等の不特定多数のステークホルダーに対する情報開示と、NDA を結んでいる取引先や情報共有コミュニティ[3]に対する情報開示では提供可能な情報の範囲や粒度が異なる。

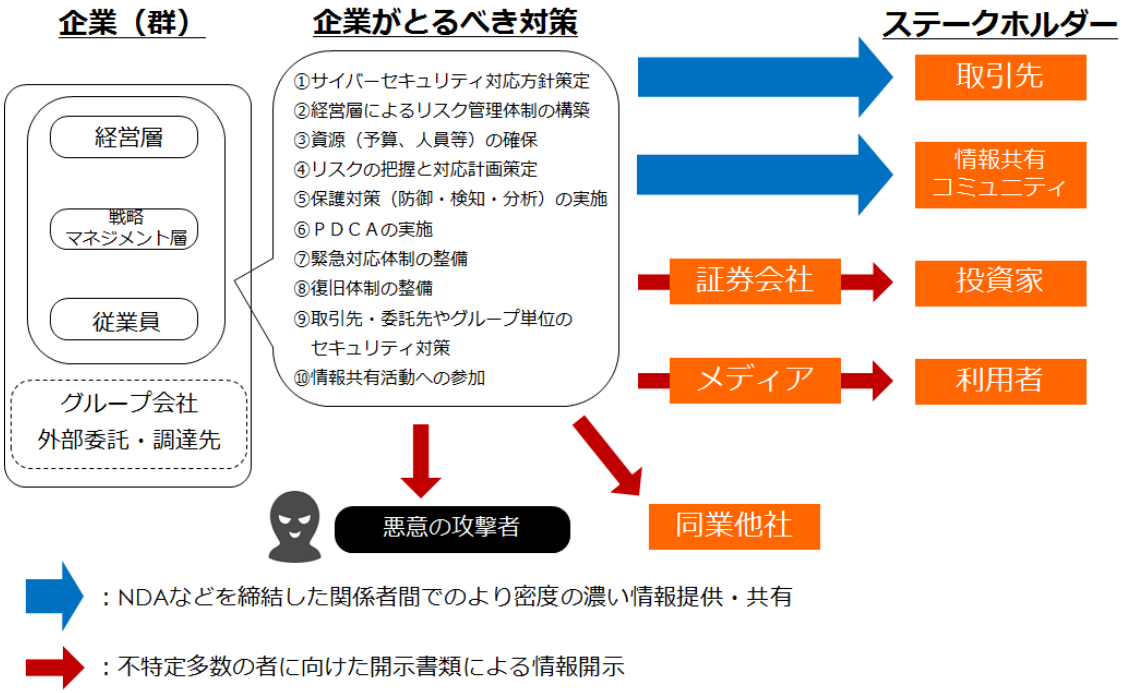
また、一般論として、サイバー攻撃への対応計画（④）や保護対策（⑤）を具体的に開示した場合は、かえってサイバー攻撃等を誘発するリスクもある。そこで、特に④、⑤、⑦、⑧、⑨などについては開示する内容について留意が必要な場合があり、全体として経営層の責任の上で開示のメリットとデメリットを判断の上で開示の内容を考えていく必要がある。

---

[3] 例えば、以下のような情報共有体制が存在。

- サイバーセキュリティ協議会：2019 年（平成 31 年）４月より、官民の多様な主体が連携し、サイバーセキュリティ分野における従来の枠を超えた情報共有・連携体制として、新たに創設された。同協議会では、サイバーセキュリティ対策のみならず、類似被害防止のためのインシデント情報の共有なども行われる予定である（https://www.nisc.go.jp/conference/cs/kyogikai/index.html）。
- 重要インフラの第四次行動計画：2017 年４月 18 日サイバーセキュリティ戦略本部決定。昨今のサイバー攻撃による急速な脅威の高まりや、2020 東京オリンピック・パラリンピック競技大会も見据え、安全かつ持続的なサービスの提供に努めるという機能保証の考え方に基づき、第３次行動計画を見直したもの。「重要インフラ行動計画」、「第４次行動計画」と略称を使うことがある。同行動計画の「情報共有体制の強化」の項目において、重要インフラ 14 分野における官民・分野横断的な情報共有体制が運用されている。
- CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response の略（セプター）。重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。2005 年以降順次構築が進められ、2017 年３月末現在、13 分野で 18 セプターが活動。
- C4TAP：Ceptoar Councils Capability for Cyber Targeted Attack Protection の略。重要インフラ事業者において、標的型攻撃が疑われるメールについての一定情報を共有することで、より多くの標的型攻撃に関する情報を収集・共有し、重要インフラサービスへの標的型攻撃の未然防止、もしくは被害軽減、サービスの維持、早期復旧を容易にすることを目指す取組。
- J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan の略。サイバー情報共有イニシアティブ。IPA を情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取組。
- ISAC：Information Sharing and Analysis Center の略。サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報は ISAC に参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。

【図６：ステークホルダーと情報開示の関係性】



また、開示書類の客観性・信頼性・説明力を高める観点から、開示書類に対する第三者意見、サイバーセキュリティ対策の認証取得等、補足的手段を記載することが望ましい。

（2）開示にあたってのポイント

企業は情報開示を通じて一般の利用者や取引先、投資家など様々なステークホルダーに説明責任を果たす必要があるが、その際、例えば以下のような点について留意が必要である。

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

→ 例えばサイバーセキュリティ対策の対応の基本方針を定めて公表するのみならず、自社のトップマネジメントの取組姿勢や取組の本気度をトップマネジメントのメッセージとして伝える、サイバーセキュリティ対策の取組内容を企業価値向上のプロセスと関連づけて記載するなどの工夫が考えられる。

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

→ 例えば KPI 設定による取組の成果の可視化や定量化への努力を通じてステークホルダーの客観的な評価を可能にする、サイバーセキュリティに係る重大事件・事故の存在や件数といった一見非開示にしがちな項目について記載するなどの工夫が考えられる。

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。

→ 例えば他社との差別化を意識したサイバーセキュリティ対策の取組内容を開示する、自社の重点領域を意識した取組を開示する、前期からの変更点について開示する、PDCA サイクルを意識して対策の取組内容を開示する、取得した第三者評価・認証を記載する、SOC（Security Operation Center）や CSIRT（Computer Security Incident Response Team）について記載するなどの工夫が考えられる。

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

→　開示内容の編集方針や構成の流れが曖昧でまとまりが悪く、そのうえ読み手を助ける工夫も施されていなければ、ステークホルダーは漠としたイメージしか持てないことから、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するなどの工夫が考えられる。

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

→　直近の重要トピックスをタイミングよく扱うことができれば、ステークホルダーとのより良い対話の起点となる可能性があるため、ステークホルダーが把握しておくべき直近の重要トピックスについて、対応の意義や対応の方針・考え、取組状況を記載するなどの工夫が考えられる。

（３）記載例

（１）及び（２）で述べた内容について、本項目において記載例を紹介する。記載例は（１）で紹介したサイバーセキュリティ経営ガイドラインの 10 の対策項目に沿って整理している。なお、記載例は、2016 年（平成 28 年）から 2018 年（平成 30 年）の間の日経 225 の対象企業 [4]の有価証券報告書、コーポレート・ガバナンス報告書、CSR 報告書、サステナビリティ報告書、統合報告書、アニュアルレポート、情報セキュリティ報告書等の実際の企業の開示書類の中から抽出した。

あくまで下記の事例は参考として示したものであり、各企業においては、それぞれの企業の経営方針や事業の実態に応じた適切なサイバーセキュリティ対策の開示の在り方を検討することが重要である。

① サイバーセキュリティ対応方針策定に関する情報開示

【記載のイメージ】

- ✓ 社長や CISO などの経営層のメッセージとしてサイバーセキュリティ対策の取組方針を記載する。
- ✓ サイバーセキュリティ対応の基本方針について、具体的な施策とともに記載する。
- ✓ 業界や社としての重要分野におけるサイバーセキュリティ対策の取組方針を記載する。

記載例① ＡＮＡホールディングス（株） 統合報告書 2017

トップメッセージ 代表取締役社長片野坂 真哉

■「安全」と「人財」への投資

私たちのグループにおいて、長期的な視点で最も重要なのは「安全」と「人財」であり、経営の基盤、競争力の源泉として現行戦略に組み込んでいます。

まず、「安全」に関して、2016 年度中にボーイング 787 型機のエンジン部品に関する不具合や、空港の保安検査場などにおける業務手順の不徹底など、ご搭乗のお客様や関係先の皆さまにご心配をおかけした事象が生じました。これを受け、私はグループ各社に対して「安全」を経営の基盤として事業に取り組むよう改めて指示を出しました。また、2017 年度のグループ入社式において、2,799 名の新入社員に向け、「安全がすべて」という言葉を何度も投げかけました。「安全」の堅持が求められるのは、航空機のオペレーションだけに留まりません。食品の安全や情報セキュリティへの対応など、グループ全社で「安全」に対する取り組みを強化しなければなりません。

安全は経営の基盤であり、社会への責務です。今後も手間やコストを惜しまず、何よりも優先して「安全」を追求していく考えを、経営トップとして表明したのです。

[4]日経 225 の対象企業の業種は、【インフラ】電力３社、ガス２社、通信６社、【運輸・交通】鉄道・バス８社、陸運２社、海運３社、空運１社、倉庫１社、【メーカ等】機械１６社、窯業８社、非鉄・金属１１社、ゴム２社、パルプ・紙２社、医薬品９社、化学１７社、建設９社、鉱業１社、自動車１０社、食品１１社、水産２社、精密機器５社、石油２社、繊維４社、造船２社、鉄鋼５社、電気機器２７社、不動産５社、その他製造３社、【金融】銀行１１社、証券３社、保険６社、その他金融１社、【流通・サービス】 商社７社、小売業８社、サービス１２社、である。

サイバーセキュリティへの取組の強化に関する方向性について開示した事例である。「安全」の文脈において、情報セキュリティの対応が航空機のオペレーションや食品安全と並ぶ重要な事項として位置づけられていることが、社長メッセージという企業の経営方針として示されており、経営層の強いコミットメントがわかる内容となっている。

記載例②　味の素株式会社　サステナビリティレポート　2018

サイバーセキュリティの確保と個人情報管理

■ サイバーセキュリティの基本方針

味の素グループは、サイバーセキュリティを重大リスクと定義し、（略）

（参照）情報セキュリティに関するグループポリシー

（https://www.ajinomoto.com/jp/activity/policy/information_security_policy.html）

■ 情報セキュリティの管理体制

グループ全体のセキュリティ管理体制強化に向け、CSIRT 体制構築の検討を開始しています。

■ 情報セキュリティ教育

セキュリティ教育として新入社員、管理者向けに集合研修を実施しています。また、「情報取扱ガイドブック（改訂：電子版）」を公開し、味の素（株）全従業員に対するセキュリティ教育の一環として周知徹底するとともに、その内容の理解度テストを全従業員に対して実施しています。

また、情報セキュリティリスクに対する取り組みの一環として、味の素（株）では、役員、従業員を対象とした標的型メール攻撃対応訓練を 2016 年度より実施していますが、2017 年度より国内の味の素グループメール利用会社へ対象を拡大し、訓練を実施しています。

■機密情報の流出防止に向けた継続的な取り組み

味の素（株）および国内グループ会社に展開している標準パソコンへ人工知能を活用した振る舞い検知システムを導入し、不正の検知を徹底しています。味の素（株）から開始し、国内 4 社に導入、順次拡大中です。

また、国内外グループ会社の Web サイトを対象に、年 1 回、外部サービスを活用したセキュリティ診断を実施し、継続的な脆弱性対策を講じています。さらに、営業秘密漏洩防止に向けて、海外グループ会社へのアセスメントを開始しました。

■ セキュリティ点検

味の素（株）では毎年定期的に全職場セキュリティ点検を実施しています。主な点検項目は IT 機器や機密情報、個人情報の管理状況など、情報取り扱いの基本的事項です。外部クラウド・サービスの利用および管理状況についても、毎年チェックしています。

サイバーセキュリティ対策に関するポリシーに関する情報開示である。サイバーセキュリティを重大リスクと位置づけた上で、グループ全体での管理体制や教育や点検の在り方について記載し、その上で社としてのポリシーへのリンクを付すことで、ポリシーが具体的にどのような対策に結実しているのかがわかりやすくなるよう配慮されている。

記載例③　株式会社セブン&アイ・ホールディングス　CSR データブック　2018

セブン&アイ HLDGS.の重点課題

重点課題 2　商品や店舗を通じた安全・安心の提供

情報セキュリティおよび個人情報保護

情報セキュリティ管理体制の構築

セブン&アイ　HLDGS.　では、オムニチャネル戦略によりお客様との接点が拡大することが見込まれています。このような状況において、食の安全と同様、情報資産の安全・安心を確保していく取り組みが、オムニチャネル戦略を支える基盤と考えています。セブン&アイ　HLDGS.　は、オムニチャネルの取り組みで取得する顧客情報（個人情報）の適正な保護と利用を促進し、事業の安全・安心な運用を推進するため、「情報セキュリティ基本方針」と「個人情報保護基本方針」を定めるとともに、情報セキュリティマネジメントシステム ISMS 認証（ISO27001）を取得しました。ISMS に関わる PDCA サイクルの実施により、高いレベルでの情報セキュリティ体制の構築をしています。あわせて、オムニチャネルシステムにおける、特にクレジットカード情報および取引先情報を安全に取り扱うことを目的に、グローバルセキュリティ基準である PCIDSS 認定を取得しております。

また、情報セキュリティを重要なリスクの 1 つと捉え、情報管理委員会を設置してリスクの分析・評価・対策を検討しており、これをもとにした管理体制の構築を行っています。具体的には、グループの達成すべき情報セキュリティの水準を定め、グループ各社へ ISMS 認証における PDCA サイクルによる手法に準拠した展開を実施することで、情報管理・セキュリティの強化に取り組んでいます。

－「情報セキュリティ基本方針」はこちら

－「個人情報保護方針」はこちら

－ISMS 認証取得拠点の一覧および PCIDSS 認定取得についてはこちら

小売・流通業界における重要トピックスであるオムニチャネル戦略について、一般消費者や取引先などのステークホルダーが把握しておくべき情報セキュリティ対策の意義を始めとして、情報セキュリティに関する基本方針の策定状況や、情報セキュリティに関する管理体制、第三者評価・認証の取得状況、情報セキュリティのグループ展開状況などといったステークホルダーが知りたい情報が一通り記載されている。

② 経営層によるリスク管理体制の構築に関する情報開示

【記載のイメージ】

- ✓ 責任者の設置や、企業全体の情報セキュリティの推進体制の構造、各組織の権限と責任、主な活動内容について記載する。
- ✓ 企業全体のリスクマネジメントにおける位置づけや他のリスク管理体制との関係性を記載する。

記載例① 株式会社日立製作所 サステナビリティレポート 2017

多面的なリスクマネジメントの推進

情報セキュリティの推進

情報セキュリティの徹底

日立では、執行役社長が ISMS の実施および運用に関する責任および権限をもつ情報セキュリティ統括責任者として CIO を任命しており、2016 年度は執行役専務が務めています。情報セキュリティ統括責任者を委員長とする「情報セキュリティ委員会」が、情報セキュリティと個人情報保護に関する取り組み方針、各種施策を決定しています。決定事項は「情報セキュリティ推進会議」などを通じて各事業所およびグループ会社に伝達し、情報セキュリティ責任者が職場に徹底しています。

日立では、情報セキュリティと個人情報保護の取り組みにおいて、特に次の 2 点を重視しています。

1. 予防体制の整備と事故発生時の迅速な対応

守るべき情報資産を明確にし、脆弱性評価とリスク分析に基づいて情報漏えい防止施策を実施しています。事故は「起きるかもしれない」という考え方を一歩進めて、「必ず起きるものだ」という前提に立って、緊急時のマニュアルを作成し、対応しています。

2. 従業員の倫理観とセキュリティ意識の向上

担当者向け、管理者向けなど階層別にカリキュラムを用意し、e ラーニングによる全員教育などを通じて倫理観とセキュリティ意識の向上を図っています。また、監査を通じて問題点の早期発見と改善にも取り組んでいます。

情報セキュリティの徹底に関する情報開示である。機動的かつ実効性のあるリスクマネジメント体制に求められる、情報セキュリティ統括責任者の設置や、企業全体の情報セキュリティの推進体制の構造、各組織の権限と責任、主な活動内容といった項目について説明している。

また、重視している取組について、事故は「起きるかもしれない」という考え方を一歩進めて、「必ず起きるものだ」という前提に立つなど、セキュリティ意識の高さを打ち出すことにより、社としての取組の本気度に関心のあるステークホルダーの関心に一定程度適う内容となっている。

記載例②　ANA ホールディングス株式会社　有価証券報告書　2017 年度（2018 年３月期）

コーポレート・ガバナンスに関する施策実施状況
内部統制システムの充実に向けた当期における取り組み
リスクマネジメント

「ＡＮＡグループ・トータルリスクマネジメント規程」を定め、ＡＮＡグループの経営の安定性・効率性を高めることを目的としたリスクマネジメント体制を推進するとともに、グループ全体にまたがる重要テーマについては個別にリスク対策を強化しております。ＡＮＡグループを取り巻く様々な事業リスクに対しては、予防的な観点から、事前の準備や統制を図ることを目的とした「リスク管理」と、実際にリスクが顕在化した場合の「危機管理」の２つの側面からの体制を構築し、運用しております。

予防的観点からの「リスク管理」については、リスクの極小化を目的としたリスクマネジメントサイクル（リスクの洗い出し→分析→評価→管理・対策の検討実施→モニタリング）を構築し、グループ全体を対象に取り組みを行っております。また、リスクが顕在化した場合の「危機管理」においては、「ＣＭＭ（Crisis Management Manual）」を規定してグループ全体の対応体制を定めております。特に、航空機の運航に直接影響する危機への対応はＣＭＭの下部規程として「ＥＲＭ（Emergency Response Manual）」を定め、当規程に基づき事故やハイジャックを想定した実践的な演習を2002年より毎年実施しております。当期においても事故模擬演習、ハイジャック演習を１回ずつ実施しております。また、首都直下地震をはじめとする大規模災害等への備えとして、「事業継続計画（ＢＣＰ、Business Continuity Plan）」をＣＭＭの下部規定に定め、年に一度、バックアップ施設に設置された各種機器・設備の操作訓練を実施しております。

「情報セキュリティ」の分野においては、情報セキュリティの推進に係るポリシーをＩＳＯ27001（ＩＳＭＳ）に準拠して定めた「ＡＮＡグループ情報セキュリティ管理規程」や具体的な運用ルールを定めた管理細則を設定し、グループ全体に適用しております。ハンドブックやｅラーニングを活用してグループ全体への浸透を図りながら、遵守状況を点検する制度を設け、情報セキュリティ分野における対策をより堅固なものとしております。当期においては、グループ全社員を対象としたｅラーニングを１回、各グループ会社の全部署を対象とした自己点検を実施していることに加え、16 の事業所に対する情報セキュリティ専門部署によるアセスメントを実施しております。また、本年５月 25 日に施行されたＥＵデータ一般保護規則（ＧＤＰＲ）に準拠するため、各種規程類の改訂や業務手順の見直しを行いました。一方、サイバーセキュリティ対策においては、経済産業省の「サイバーセキュリティ経営ガイドライン」に準拠し、多層防御を行いつつ、毎年、第三者機関によるリスクアセスメントを実施し必要な対策を行っております。今後は米国の国立標準技術研究所（ＮＩＳＴ）のサイバーセキュリティ・フレームワークを活用し、クラウドセキュリティ対策、サプライチェーンに対するセキュリティ管理の見直し等を行う予定です。なお、これらの活動の実施状況については、都度「グループＣＳＲ・リスク・コンプライアンス会議」において報告しております。

リスク管理上の重要トピックスに対応した情報開示である。EU の一般データ保護規則（GDPR）へ

の準拠や、経済産業省のサイバーセキュリティ経営ガイドラインへの準拠、クラウドセキュリティ対策、サプライチェーンセキュリティ対策といったステークホルダーのみならず社会全般において話題となっているサイバーセキュリティ関係の重要トピックスを採り上げ、対応状況や今後の対応方針について一通り記載している。

また、「リスクマネジメント」のカテゴリの中で、「情報セキュリティ」や「サイバーセキュリティ」が社としてのトータルリスクマネジメント体制の下に位置づけられており、かつ、機動的かつ実効性のあるリスクマネジメント体制が既に運用されているなど、ステークホルダーにリスクマネジメントへの意識の高さが伝わる内容となっている。

③　資源（予算、人員等）の確保に関する情報開示

【記載のイメージ】

✓ 従業員等の教育や研修の内容について、定量的な情報と合わせて記載する。 ✓ サイバーセキュリティ対策にかかる予算について記載する。

記載例①　三菱電機株式会社　CSR レポート　2016

情報セキュリティーへの対応

各種施策

●情報セキュリティーの教育

三菱電機では、企業機密・個人情報の適切な取扱いを徹底する企業風土を醸成するために下記の教育プログラムを実施しております。

全従業員への教育

約 4 万人の全従業員を対象に情報セキュリティーの教育を年 1 回、e ラーニングで実施し、当社方針、情報漏洩事故概況、前年度の反省、個人情報保護法、不正競争防止法、一人ひとりが認識すべき安全管理措置（組織的・人的・物理的・技術的）を周知徹底します。

キャリアパスに沿った教育

新入社員教育、20 代対象の研修、30 代対象の研修、新任課長研修の中で、各階層で求められる役割を果たすために必要な企業機密管理・個人情報保護の教育を実施しています。

その他の個別教育

海外赴任者に対しては赴任前研修の中で、企業機密管理・個人情報保護に関する当社の取組状況、経済産業省の営業秘密管理指針、海外での情報漏洩事故の事例について教育しております。

情報セキュリティの教育に関する情報開示である。情報セキュリティの教育においては、社員一人一人のセキュリティ意識の向上、意識改革を通じて、セキュリティ対策を組織内に浸透させることが求められるが、全従業員への教育、キャリアパスに沿った教育、個別教育など、きめ細かな取組を行っている記載があり、ステークホルダー目線からも継続的なセキュリティ改善・向上の取組をしていることがわかる。

記載例②　富士通株式会社　CSR 報告書　2016

人材育成・キャリア開発
取り組みと実績
プロフェッショナル化の推進
2. セキュリティマイスター認定制度
　サイバー攻撃に関する脅威が多様化・高度化する現在、富士通ではお客様の情報資産を守るための取り組みの 1 つとして、富士通グループ内から高い技術を持つ技術者を発掘、認定し、フィールドへ配置する仕組みを整えました。認定制度では、現場ニーズに適合した 3 領域 15 種類の人材モデルを定義し、人材モデルごとに専門教育コースを開設しています。サイバーレンジ（仮想演習場）を採用した技術者育成教育も、新規に開発しました。また、コミュニティの有識者同士のナレッジ共有により、認定後のスキル向上にもつながっています。

　サイバーセキュリティ分野のプロフェッショナル人材の認定制度に関する情報開示である。セキュリティマイスター認定制度を通じてプロフェッショナル人材を育成し、顧客の情報資産を守ることが求められるフィールドに配置するというサイバー攻撃対応の考えや取組を説明している。独自の認定制度という他社との差別化を意識した取組内容が、企業価値向上のプロセスと関連付けられて記載されており、ステークホルダー目線からは、同社が人材育成に力を入れていることがわかる内容となっている。

記載例③　株式会社資生堂　有価証券報告書　2017 年度（2017 年 12 月期）

連結損益計算書及び連結包括利益計算書 連結損益計算書 情報セキュリティ対策費：574 百万円 前連結会計年度(自 2016 年 1 月 1 日至 2016 年 12 月 31 日) 当社の連結子会社の公式オンラインショップが外部からの不正アクセスを受けたことに伴う調査、お客さまへのお詫び及びセキュリティ対策に係る費用です。

情報セキュリティ対策費に関する情報開示である。情報セキュリティ対策費とセキュリティ事故の発生状況を重ね合わせることで、ステークホルダーが客観的な評価を下すことができるようになっている。

④　リスクの把握と対応計画策定に関する情報開示

【記載のイメージ】

- ✓ 経営戦略の観点から守るべき情報と当該情報に対するリスクについて、リスクマッピングなどに基づいて記載する。
- ✓ リスクアセスメントの実施や、サイバー保険の活用・専門セキュリティベンダーへの委託といったリスクに対する対策の在り方、対応計画等について記載する。

記載例①　ヤフー株式会社　有価証券報告書　2017 年度（2018 年３月期）

2.情報セキュリティに関わるリスク

（1）情報セキュリティ全般に関わるリスク

①情報セキュリティが侵害された場合、当社グループの業績に影響を与える可能性があります

当社グループでは、安全に安心して利用できるサービスをユーザーに提供するため、中長期的な視点で全社を挙げて情報セキュリティに取り組んでいます。

しかしながら、これらの取り組みが及ばず、業務上の人為的ミスや故意による不法行為、災害などによるシステム障害、マルウェア感染や標的型攻撃などのサイバー攻撃、システムや製品等の脆弱性などにより、情報漏洩、データの破壊や改ざん、サービスの停止などの被害等が発生した場合、当社グループの業績に影響を与えるだけでなく、当社グループの信用失墜につながる可能性があります。

②当社の子会社・関連会社の情報セキュリティが侵害された場合、当社グループの業績に影響を与える可能性があります

当社は、子会社・関連会社の情報セキュリティを支援しています。具体的には、情報セキュリティ対策の仕組みの共有や導入支援、脆弱性情報など情報セキュリティに関する情報の共有、各社の求めに応じて情報セキュリティ対策の相談対応などを行っています。さらに、子会社に対しては当社と同等の情報セキュリティ対策を行うための規程の提供や第三者認証取得支援などの支援を行っています。しかしながら、想定以上にサイバー攻撃などの脅威が発生した場合には追加費用が発生し、当社グループの業績に影響を与える可能性があります。

③サイバー攻撃などの脅威が想定以上に増口・高度化した場合、当社グループの業績に影響を与える可能性があります

当社グループでは、日々高度化するサイバー攻撃などの脅威に備え、必要かつ前衛的な対策を取るべく必要十分な費用の確保に努めています。

しかしながら、想定以上にサイバー攻撃などの脅威が発生した場合には追加費用が発生し、当社グループの業績に影響を与える可能性があります。

（2）パーソナルデータに関わるリスク

①パーソナルデータの情報セキュリティが侵害された場合、当社グループの業績に影響を与える可能性

があります。
当社グループではプライバシーポリシーをユーザーに公開し、サービスを通じお預かりしたパーソナルデータをプライバシーポリシーに準拠して利用しています。パーソナルデータは、アクセスする権限を持つ担当者を必要最小限に絞る、隔離された居室でのみ取り扱うなど複数の対策を組み合わせて保護しています。しかしながら、これらの対策が及ばず、情報セキュリティが侵害された場合、サービスの停止または繰退により、当社グループの業績に影響を与えるだけでなく、当社グループの信用失墜につながる可能性があります。さらに、パーソナルデータのうち「個人情報」の情報セキュリティが侵害された場合、上記リスクに加え、法的紛争に発展する可能性があります。ユーザー自身の個人情報の照会・変更・削除等は、ユーザー自身がシステムから行うようにしています。問い合わせに回答するためにやむを得ない場合等を除き、役員、従業員等が個人情報を参照できない対策を導入しています。また、個人情報を社外に業務委託する場合は、個人情報委託先選定基準を定め、一定水準以上の情報セキュリティ対策を実施できる業務委託先に限定して委託し、委託中は個人情報委託先の監督・監査を定期的に行っています。しかしながら、これらの対策が及ばず、情報漏洩、情報破壊や改ざんなどの被害等が発生した場合、信用の低下や損害賠償請求等の法的紛争が発生する可能性があります。
②銀行口座番号、クレジットカード番号等が漏洩した場合、ブランドイメージが低下したり、法的紛争に発展したりする可能性があります。
クレジットカード情報についてはそれらを取り扱う決済金融系サービス「Yahoo！ウォレット」と当社におけるほぼ全てのクレジットカード決済の加盟店管理業務において、クレジットカード決済に関する会員情報や取引情報および決済プロセス等におけるグローバルスタンダードのセキュリティ基準である「PCI DSS」の中でも最も難しい「レベル 1」の認定を取得しています。しかしながら、これらの施策によっても情報セキュリティが完全に保たれる保証はなく、万が一情報漏洩などの諸問題が発生した場合、当社グループの業績に影響を与えるだけでなく、当社グループの信用失墜につながる可能性があります。
③個人情報が「Yahoo!ショッピング」や「ヤフオク！」などの出店ストアから情報漏洩した場合、業績に影響を及ぼす可能性があります。

（3）通信の秘密に関するリスク
①通信の秘密が侵害された場合、当社グループの業績に影響を与える可能性があります
当社グループは、「Yahoo！メール」等のサービスにおいて、通信内容などの通信の秘密に該当する情報を取り扱っています。これらの取扱いの際には電気通信事業法に則り、情報セキュリティに対する取り組みのもと、適切な取り扱いを行っています。しかしながら、これらの情報が「Yahoo！メール」等のサービスを提供するシステムの不具合や、マルウェア等の影響、通信設備等への物理的な侵入、当社グループの関係者や業務提携・委託先などの故意または過失等によって侵害された場合、当社グループのブランドイメージの低下や法的紛争に発展し、ユーザーの減少やサービスの停止や縮退に伴う損害賠償や売上減少などによる業績に影響を及ぼす可能性があります。

（5）社内経営情報に関わるリスク

①会社の経営・財務など投資判断に影響を及ぼすような未公表の重要事実（インサイダー情報）や非公開の社内経営情報の情報セキュリティが侵害された場合、業績に影響を及ぼす可能性があります。

（6）遺伝子解析事業について

当事業では、ユーザーから提供された試料を検査し、解析した結果得られる個人の遺伝子に関する情報を機微な個人情報として取り扱います。当該遺伝子情報の取扱いにあたりセキュリティ確保には万全を期していますが、万一情報漏洩等が生じた場合には、信用の低下や損害賠償請求等の法的紛争が発生する可能性があります。

情報セキュリティやパーソナルデータに関するリスクについての開示である。事業を実施する上での様々なサイバーセキュリティリスクを想定し、またそれぞれについて対策を講じている旨が記載されており、ステークホルダーの目線からは、サイバーセキュリティリスクに対する感度の高さが伝わる内容となっている。

⑤　保護対策（防御・検知・分析）の実施に関する情報開示

【記載のイメージ】

✓ サイバーセキュリティ対策のうち、境界防御や内部防御を含む防御策やセキュリティオペレーションセンター（SOC）の設置、ログによる監視・検知などについて記載する。

記載例①　日本電気株式会社　サステナビリティレポート　2018

2017 年度の主な活動実績

サイバー攻撃対策強化

特定の企業・組織を狙い撃ちする標的型攻撃、ランサムウェア（ファイルが暗号化され、復号と引き換えに身代金を要求）、BEC（Business Email Compromise：ビジネスメール詐欺）、および不特定多数を狙ったばらまき型メール攻撃など、日々発生するサイバー攻撃は巧妙化・高度化しています。これに対抗する手段の 1 つとして、PC・サーバの脆弱性対策およびインシデントレスポンスの効率化を目的に、当社および国内関係会社全社に対してサイバー攻撃対策強化システム（GCAPS）の導入を推進しています。

GCAPS では、リスク認識に基づき対処を行う「事前防御」と、インシデント検知発生時の「事後対処」の 2 つの側面から PC・サーバ対策の強化を図っています。2018 年度以降、海外現地法人にも GCAPS を順次導入する予定です。

また、たとえ未知のマルウェアに感染した場合でも、SDN との連携により、感染端末からの不正通信を 24 時間 365 日体制で自動遮断しています。これにより、二次感染の拡大防止、セキュリティリスクの極小化を実現しています。

NEC では AI を組み合わせたサイバーセキュリティの先端技術領域において、実際の IT 環境における価値実証を行いながら、NEC の注力領域の成長に向けた先進的な社内レファレンスの構築を進めています。例えば、AI を活用した NEC の自己学習型システム異常検知技術である ASI を NEC Asia Pacific（シンガポール）で運用している実際の IT 環境に導入し、CSIRT による監視業務を実施しています。こうした実運用の中で得られた要求事項や改善点を製品開発部門へフィードバックすることで ASI の品質向上も図っています。

サイバー攻撃対策強化に関する情報開示である。標的型攻撃、ランサムウェア、ビジネスメール詐欺等という警戒・対処すべきインシデントの重点トピックスに対して、対策手段選定の意義や今後の対策強化に向けた戦略を説明している。

また、SDN や AI 等の新しい ICT の活用の位置づけを明確にすることで、ステークホルダーがサイバー攻撃への対策の強化を図っていることがわかる内容となっている。

記載例②　富士通株式会社　CSR 報告書　2017

情報セキュリティ

監視・分析・評価機能

セキュリティ監視

全世界に配備したセキュリティ監視機器から 1 日約 10 億件のログが集められます。情報セキュリティマネジメントを行ううえでこのログを効率的・効果的に管理することが重要です。

富士通グループでは、24 時間 365 日体制のセキュリティオペレーションセンター（SOC）を設置し、迅速・的確なインシデント対応、セキュリティアラート対応を可能にする仕組みを構築しています。社内ネットワークの各所に組み込まれた「セキュリティ監視機器」で生成されたログは、「ログ統合管理システム」に集約・一元管理され、そこからログ自動化・管理ツール「Systemwalker Security Control」に送られ、脅威が確認された場合アラート通知メールが SOC に送られる仕組みになっています。

SOC は「ローカルオペレーター」「インシデントマネージャー」「セキュリティアナリスト」というスタッフで構成され、受信したアラート通知メールの内容を分析し、脅威の質・範囲・重度を見極め、対応優先順序を付けて、迅速・的確に対処します。

ホワイトハッカーによるインターネット動向調査

変容するサイバー攻撃の脅威に対応するため、ホワイトハッカーによる世の中のインシデントや脆弱性を調査、またサイバーインテリジェンスを駆使し不正アクセスやマルウェアを解析した結果のリスク情報を基にログを調査し、新しい脅威からのリスクを最小限に抑えてインシデントの発生を防ぎます。

監視・分析・評価機能に関する情報開示である。サイバー攻撃対処のオペレーションについて、ステークホルダーが把握しておくべき SOC の設置・運用の意義を始めとして、ログの統合管理によるセキュリティ監視や、高度なプロフェッショナル人材の配備、ホワイトハッカーによるサイバーインテリジェンスの収集と活用などといった具体的な対策が記載されている。

また、サイバー攻撃がもたらすインシデントや脆弱性について、常に最新の状況を理解するとともに意識的に情報収集に取り組んでいることがメッセージとして伝わっている。

⑥　ＰＤＣＡの実施に関する情報開示

【記載のイメージ】

✓ サイバーセキュリティ対策のＰＤＣＡについて、リスク管理に関する KPI と合わせて公表する。 ✓ 発生したインシデントや事故情報を踏まえ、改善に向けた取組を記載する。 ✓ ISMS などの国際標準となっている認証の取得について記載する。

記載例①　西日本旅客鉄道株式会社　CSR　REPORT 2018（企業考動報告書）

CSR 重点分野の 2017 年度活動実績および 2018 年度重点取り組み計画
リスクマネジメント
情報セキュリティ
●Plan（2017 年度重点取り組み事項）
　JR 西日本グループ全体のセキュリティレベルの向上
●Do（2017 年度の主な取り組み）
　情報セキュリティ意識の醸成・インシデント対応訓練の実施
●Check（評価：○成果、※これから取り組むべき課題）
　○BCP 対策：新データセンター稼働によるシステムダウンリスク低減
　○サイバーセキュリティ対策：教育・訓練による危機対応能力の向上
　※高度化するサイバー攻撃へ更なる対策
●Action　（2018 年度重点取り組み計画）
　・JRW-CSIRT による危機対応能力の更なる向上
　・シェアードサービスのグループ会社展開による、情報セキュリティレベル向上
（2022 年までの到達目標）
　・情報セキュリティに関する重大な事故・被害が発生していない状態

【Do】 情報セキュリティ意識の醸成・インシデント対応訓練の実施
　インシデント対応・情報連携組織「JR 西日本グループ CSIRT（JRW-CSIRT）」を通して、情報セキュリティ意識の醸成、危機対応能力の向上に取り組んでいます。当社では、標的型攻撃メール訓練や、行政機関と連携した重要インフラ向け訓練への参画、社内端末の監視基盤強化など、マネジメント面・技術面で対策を進めています。また、グループ会社に対してはセキュリティ担当者向けに集合研修を実施し、インシデント対応時の能力向上を図っています。
【Check】
　グループ各社ともリスクマネジメント体制が確立され、リスク低減の取り組みが進みつつあります。今後は、リスク事象発生時における初動対応を含め、一層のレベルアップに努めていきます。
　●情報セキュリティ

前中期経営計画の期間では、BCP 対策として新データセンターを稼働させ、自然災害によるシステムダウンのリスク低減を行いました。また、サイバーセキュリティ対策では、JRW-CSIRTや社員教育により、危機対応能力の向上を推進しましたが、高度化するサイバー攻撃へ更なる対策の充実が必要です。

【Action】 今後も継続的に取り組みを進めます

各部門、各グループ会社の経営マネジメントにリスクマネジメントの概念が組み込まれていることや、組織風土上の課題を認識、改善し、新たなコンプライアンスリスクに対して適切に対応しながら必要な対策を講じることができるよう、着実に以下の取り組みを進めてまいります。

●情報セキュリティ

・JRW-CSIRT による危機対応能力の更なる向上

・IT 部門が運営するシェアードサービスのグループ会社展開による、グループ全体の情報セキュリティレベル向上

サイバーセキュリティ対策のアクションプランに係る達成状況に関する情報開示である。PDCA のサイクルに則して、持続的なセキュリティレベル向上への取組姿勢をプロアクティブかつ丁寧に説明している。これにより、ステークホルダーの目線からは、実効性のある情報セキュリティマネジメントシステムが既に運用されており、リスクマネジメントに力を入れていることがわかる内容となっている。

記載例② 株式会社電通 統合報告書 2018

情報セキュリティ

情報管理体制の整備および強化

電通では、電通グループ内で保有もしくは取引先からお預かりした個人情報などを含む重要情報を守るため、「電通グループ情報セキュリティ基本方針」を制定し、厳格な情報セキュリティ管理体制を整備しています。この基本方針に基づき、「情報管理規則」とその他関連細則を制定し、遵守すべき規則として明確化するとともに、研修や説明会、パンフレット等を通じて役職員へのきめ細かい周知活動を行っています。また、2018 年 5 月 1 日時点で、電通ならびに電通国内グループ会社計 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。これらの施策により、日々変化し高度化する ICT（情報通信技術）環境に電通グループ全体で機動的に対応し、より一層の情報セキュリティ管理の徹底を図っています。

PDCA の実施を含む ISMS 認証の取得に関する情報開示である。親会社のみならずグループ会社も含めた ISMS の認証取得数を開示することで、ステークホルダーが PDCA の実施について客観的な評価が得られるようになっている。

記載例③ 株式会社ジーエス・ユアサ コーポレーション GS ユアサレポート 2018

マテリアリティと KPI
マテリアリティ：機密情報管理の徹底
活動概要：セキュリティ対策の推進と不正アクセス監視の強化
■適用範囲：グローバル
KPI：高セキュリティレベル検知時のサイバー攻撃対応率
2018 年度目標：100%
■適用範囲：国内
KPI：大量データ出力時の情報流出確認対応率
2018 年度目標：100%
■適用範囲：海外
KPI：不正アクセス監視システムの海外グループ展開計画の達成
2018 年度目標：100%
活動概要：情報セキュリティ教育の推進
■適用範囲：国内
KPI：情報セキュリティ習熟度テストの合格率
2018 年度目標：100%

機密情報管理の徹底という目標を管理するために設定される KPI に関する情報開示である。KPI にしやすい項目だけを KPI に設定するのではなく、サイバー攻撃への対応やセキュリティ監視といった一見定性的な項目についても定量化への努力を行って数値化することで、ステークホルダーの客観的な評価を可能にする内容になっている。

記載例④ 日本電気株式会社 CSR レポート 2017

目標と成果

2016 年度の目標、成果・進捗、達成度

（達成度：◎目標達成、〇目標ほぼ達成、△目標一部達成、X 進捗なし）

目標：

２．ISMS（Information SecurityManagement System：情報セキュリティマネジメントシステム）の成熟度モデルを BCMS に適用した“見える化”の実施。

・プロトタイプを各部門に実施し、現状把握と監査の推進をはかる。

成果・進捗：

・事業継続計画を作成していた約 400 の部門で実施し、客観的な指標で自部門の防災、事業継続の成熟度を“見える化”することができました。

・各部門・グループ各社ごとに点検・検証を行っていた内部監査を、体系化・システム化することで、20～25%の工数削減を実現しました。

・これまで事業の継続をあまり意識してこなかった一部の事務部門や研究部門では「勤務者の命を守る」意識が向上したものの、さらなる意識向上、体制整備が課題として残りました。

・プロトタイプシステムにいくつかの改善点があることがわかりました。

達成度：◎

サイバーセキュリティ対策のアクションプランに係る達成状況に関する情報開示である。目標設定をして、それに対して成果や進捗がどうだったか、また目標に対する達成度合いがどれぐらいであったかという自己評価結果を具体的に開示することで、同社の PDCA サイクルにおいてどのような分析や検証がなされているのかがステークホルダーにわかるようになっている。また、事業継続の観点からどのような取組をしているのか、ステークホルダーが同社と前向きな対話をしていく起点になり得る記載の内容となっている。

記載例⑤　株式会社リコー　サステナビリティレポート　2017－統合報告書－

社会的責任に関する主な指標と実績 ガバナンス 指標：情報セキュリティ重大事件・事故件数 対象範囲：リコーグループ 実績： 2015 年 3 月期（2014 年度）　0 2016 年 3 月期（2015 年度）　2 2017 年 3 月期（2016 年度）　0 備考：外部への発表を要する重大な法令違反、事件・事故等の発生件数。 2016 年 3 月期：ノート PC の盗難、システム障害によるサービス不具合

情報セキュリティ重大事件・事故に関する情報開示である。情報セキュリティ重大事件・事故の存在や件数について記載しており、情報セキュリティ対策の取組の実績に対するステークホルダーの客観的な評価を得ることを可能にしている。

記載例⑥　帝人株式会社　統合報告書　2016

社会関連課題への取り組み

情報セキュリティ

管理体制の強化と従業員への教育

帝人グループでは、営業機密、技術情報、個人情報などの漏えい防止策を講じるとともに、情報システムの管理を徹底することで、情報セキュリティの維持・向上に努めています。各部署で IT 責任者、個人情報保護責任者、および営業秘密責任者を定め、毎年、情報システム、ネットワーク、施設、個人情報、営業機密などの情報資産の管理状況を確認するとともに、経営監査部が、全てのグループ会社に対して情報セキュリティ監査と個人情報保護監査を実施しています。従業員に対しては、情報セキュリティに関する研修を実施しており、情報セキュリティ e-ラーニングの定期受講を義務付けています。

しかしながら、2015 年 7 月に社外からのサイバー攻撃により、業務用パソコン 1 台から従業員の社内ネットワーク ID やメールアドレスなどの情報が流出したことが判明しました。二次的被害は確認されていませんが、従業員に対して情報の取り扱いや不審メールへの対処法について改めて周知徹底するとともに、システムの強化を行うなどの再発防止策を講じています。

情報セキュリティ重大事件・事故に関する情報開示である。情報セキュリティ重大事件・事故の存在を、その後に実施した再発防止策と併せて開示することで、社会からの信頼回復や、ステークホルダーとの前向きな対話の起点になり得る記載の内容となっている。

記載例⑦　株式会社日立製作所　サステナビリティレポート　2017

情報セキュリティの推進

情報漏えいの防止

日立製作所では情報漏えいを防止するために「機密情報漏えい防止 3 原則」を定め、機密情報の取り扱いに細心の注意を払い、事故防止に努めています。また万が一、事故が発生した場合は、迅速にお客様に連絡し、監督官庁に届け出るとともに、事故の原因究明と再発防止対策に取り組み、被害を最小限にとどめるよう努めています。

情報漏えい防止の具体的施策として、暗号化ソフト、セキュアなパソコン、電子ドキュメントのアクセス制御／失効処理ソフト、認証基盤の構築による ID 管理とアクセス制御、メールや Web サイトのフィルタリングシステムなどを IT 共通施策として実施しています。昨今多発している標的型メールなどのサイバー攻撃に対しては、官民連携による情報共有の取り組みに加え、IT 施策においても防御策を多層化（入口・出口対策）して対策を強化しています。

また、サプライヤーと連携して情報セキュリティを確保するため、機密情報を取り扱う業務を委託する際には、あらかじめ日立が定めた情報セキュリティ要求基準に基づき、調達取引先の情報セキュリティ対策状況を確認・審査しています。さらに、サプライヤーからの情報漏えいを防止するために、サプライヤーに対して、情報機器内の業務情報点検ツールとセキュリティ教材を提供し、個人所有の情報機器に対して業務情報の点検・削除を要請しています。なお、2017 年 5 月、ワーム型ランサムウェアにより一部の社内システムに不具合が生じ、メール送受信などに一時影響が出ましたが、情報漏えいは確認されず、お客様や社外への被害拡大はありませんでした。

情報セキュリティ重大事件・事故に関する情報開示である。情報漏えいの防止策のさまざまな取組を実施していることについて記載したうえで、セキュリティインシデントの発生が情報漏えいに繋がらなかったことをプラスに解釈し、前向きな取組姿勢を伝える内容になっている。

記載例⑧　コムシスホールディングス株式会社　CSR レポート　2016

2015 年度の取り組みについて (総括)
項目：安心安全な業務体制
ベンチマーク：セキュリティ事故 0 件
評価：B
2015 年度の取り組みについての総括：
情報漏えいには至っていないが、3 社でインシデントが発生した。発生件数は減少しており、情報セキュリティの重要性に対する理解・浸透を図ることで、セキュリティ事故撲滅に努める。
＊評価について
「S」・・・A以上の成果が得られた
「A」・・・目論見どおりの成果が得られた
「B」・・・ほぼ目論見どおりの成果が得られたが、一部に課題が残った
「C」・・・ある程度の成果が得られたが、課題も多く残った
「D」・・・あまり成果が上げられず、多くの課題が残った

情報セキュリティ重大事件・事故に関する情報開示である。時間軸を設定したうえで、長期的な将来にわたって具体的な取組の成果を独自の指標で見える化することにより、ステークホルダーが客観的に評価することが可能になるという記載上の工夫が施されている。

⑦　緊急対応体制の整備に関する情報開示

【記載のイメージ】

✓ CSIRT の設置など、有事の影響範囲や損害の特定、初動対応、再発防止策の検討などを行う体制を構築している旨を記載する。 ✓ インシデント発生時の対応について演習を実施している旨の記載をする。

記載例①　株式会社静岡銀行　ディスクロージャー誌　2018　静岡銀行グループの現況 2018

コンプライアンス・リスク管理体制
システムリスク管理
サイバーセキュリティ管理強化への取り組み
　近年のサイバー攻撃による脅威の高まり等を踏まえ、組織横断的機関である静岡銀行 CSIRT※1 を設置し、各種セキュリティ対策や対応訓練を実施しています。また、静岡県警察本部との共同対処協定書締結に加え、外部団体である金融 ISAC※2 および日本シーサート協議会※3 に加盟し情報収集活動や共同演習を実施するとともに、セキュリティ会社と専属契約を締結してサイバー攻撃に迅速に対応できる体制を整備するなど、実効性の向上に取り組んでいます。
※1 Computer Security Incident Response Team の略でコンピュータセキュリティにかかる事案に対処するための組織の総称
※2 金融機関間でサイバーセキュリティに関する情報を共有し、連携して対策にあたる枠組みとして設立された法人
※3 企業の組織内 CSIRT が多数加盟している専門的な知見を有する団体

　サイバーセキュリティ管理強化への取組に関する情報開示である。CSIRT の設置インシデント発生時におけるセキュリティ関係機関との連携や、外部の情報共有活動への参加、訓練・演習の実施といった緊急対応体制に関するトピックスを採り上げ、対応状況を記載している。また、専門用語には注釈が付されるなど読み手に配慮した記載になっている。

⑧　復旧体制の整備に関する情報開示

【記載のイメージ】

✓ 有事の際の、復旧に向けた手順・対応方法や計画（いわゆる BCP）を定めている、又は体制を構築している旨を記載する。

記載例①　株式会社セブン&アイ・ホールディングス　CSR データブック　2018

セブン&アイ HLDGS.の重点課題
重点課題 2　商品や店舗を通じた安全・安心の提供
情報セキュリティおよび個人情報保護
サイバー攻撃への対応
　セブン&アイ は、外部からのサイバー攻撃への対応として、情報セキュリティ事故に対する迅速かつ適正な対応・収束を組織的に行うことにより、特に技術的な面で影響・被害を最小限にする役割を担う 7&i SIRT(7&iComputer Security Incident　Response Team)を設置しています。
　また、発生した情報セキュリティ事故が、7&i CSIRT において重大インシデント（被害の程度が大きい状況など）と判断された場合には、7&i SIRT(7&i Security Incident Response Team)を招集し、緊急対応方法や復旧に向けた標準的な対応方法、公表方法などの対外的な対応を判断し実行する体制を構築しています。

　商品や店舗を通じた安全・安心の提供を脅かすサイバー攻撃への対応に関する情報開示である。インシデントの発生に備えて、復旧に向けた標準的な対応方法、公表方法などの対外的な対応を判断し実行する体制を構築していることについて記載するなど、ステークホルダーの目線からは、有事においても事業継続性の確保に力を入れていることがわかる内容になっている。

⑨　取引先・委託先やグループ単位のセキュリティ対策に関する情報開示

【記載のイメージ】

- ✓ アンケートや調達ガイドラインの策定、取引先や委託先等のサイバーセキュリティ対策についてどのように把握しているかを記載する。
- ✓ 国内外の子会社のサイバーセキュリティ対策の強化のための取組について記載する。

記載例①　日本電気株式会社　サステナビリティレポート　2018

サプライチェーン・マネジメント

CSR 調達に関する基本的考え方

サプライチェーンのグローバル化の中で、企業にはサプライチェーン全体においてサステナビリティを強く意識した責任ある調達活動を行うことが求められています。NEC は、自社のみならずサプライチェーンを構成するサプライヤーとも協力して、環境や社会全体に与える影響に十分配慮しながら事業を行うことで社会から信頼され、サステナブルな社会価値創造に貢献できるものと考えています。

NEC は、サプライヤーと協力して社会における重要な課題と事業が社会に及ぼしうる影響について共に学びながら、よりよいサプライチェーン構築に向けた取り組みを続けていきます。

基本方針と取り組み

NEC では、NEC のサステナブル経営方針および社会的責任の国際ガイダンス規格 ISO26000、ISO20400 を基に「NEC グループ調達基本方針」を策定し、CSR 調達に関する社内統制とサプライヤーへの展開を図っています。購買倫理などの社内統制の観点からは、「資材取引に関する基本規程」を制定して、すべての従業員に対して規程遵守を徹底しています。さらに、これを強化するために、調達プロセスにおける具体的な業務規程を制定し、定期的な教育を行うことで調達関係者に周知徹底しています。お取引先への展開の観点では、「CSR 調達ガイドライン」を策定し、お取引先との相互理解を深めています。この規程に基づいてサプライヤーと密に連携しながら活動を推進し、長期的な視点でパートナーシップを深める努力を続けています。

●NEC グループ調達基本方針

●CSR 調達ガイドライン

また、上記の方針やガイドラインをベースに、「人権」「労働・安全衛生」「公正取引」「環境」「情報セキュリティ」「品質・安全性」を CSR 調達における６重点リスクと認識し、サプライチェーン全般にわたってこれらの項目に十分配慮した調達（CSR 調達）が行われるよう、契約、周知徹底、書面確認、現地監査の各段階で取り組みを推進しています。

□契約

日本国内のサプライヤーには、基本契約書の締結や、環境と安全衛生管理に関する宣言書の取得を通じて、これらの履行・遵守を担保しています。北米、欧州、アジアでは、サプライヤーから環境と安全衛生管理に関する宣言書を取得しています。さらにアジアでは、個別注文書

に CSR 条項を盛り込んでいます。

□周知徹底

NEC グループ調達基本方針や CSR 調達ガイドラインをはじめとする各種説明書面をサプライヤーに提示し、内容を確認いただいています。また、日本国内では「CSR・情報セキュリティ施策説明会」を開催し、委託先と取り組む最新の施策について情報の共有を図っています。

□書面確認

情報セキュリティ分野では、サプライヤーにおける要求事項遵守状況や取り組み状況を確認するための書類点検を実施しています。

□現地監査

情報セキュリティ分野では、サプライヤーを訪問しての現地監査を継続的に実施しています。改善を要する事項をサプライヤーと共有し、改善施策が講じられるところまでフォローしています。

なお、2016 年度まで実施していた現地監査（CSR-PMR）については、実効性や今後の取り組みについて検討の結果、2017 年度は実施を見送りました。

委託先・調達先等について十分な接点や情報がステークホルダーにはないことから、適切かつ優良な取引先と取引していることを、企業の基本方針として記載することで、ステークホルダーが委託先・調達先等の状況まで一定程度把握できるような記載となっている。

記載例②　日本電気株式会社　サステナビリティレポート　2018

法令遵守の周知徹底

書類点検：情報セキュリティの強化

社会の重要な基盤である情報システムの構築を担う NEC にとって、委託先を含めた情報セキュリティ管理の強化と徹底も、最重点課題の一つです。とりわけ調達部門では、委託先の管理と啓発に力を入れています。毎年、委託先を対象にした説明会の実施や、教育資料・ツールの作成、書類点検などを行っています。

2017 年度の実績は、以下のとおりです。

- 委託先の経営層および CSR 担当役員向けの CSR・情報セキュリティ施策説明会：全国 13 会場で計 14 回開催。約 1,500 社、約 2,000 名が出席
- 委託先の NEC グループ業務従事者向けの遵守事項教育：約 900 社が教育資料をダウンロード
- 委託先各社の取り組み状況を確認するための書類点検：約 1,500 社で実施
- 委託先訪問点検：約 100 社で実施今後も、委託先の情報セキュリティレベル向上施策を継続的に行っていきます。

訪問点検：情報セキュリティ訪問点検

サプライチェーンで一貫した情報セキュリティの確保をするためには、指示事項や要請事項をサプライヤーの従業員まで浸透させることが重要です。現場が、これらの決められた事項を守らなければ事故に直結する恐れがあるからです。

NEC では、委託先における情報セキュリティ管理の仕組みについて、「NEC グループお取引先様向け情報セキュリティ基準」を毎年発行しています。

訪問点検では、サプライヤーの作業現場を訪問して、インタビューや確証の確認、視察を実施することでこの基準書に記載された要求水準への適合性を点検します。対象とする委託先は、取引規模だけでなく、取り扱う情報の重要性や秘密の程度および書類点検結果などを総合的に勘案して決定します。

2017 年度は約 100 社のサプライヤーを訪問し、9 社に情報セキュリティの管理制度の改善を申し入れました。

委託先の管理と啓発のための取組について定量化への努力を行って実績を数値化し、ステークホルダーの客観的な評価を可能にする内容になっている。

記載例③　東洋紡株式会社　CSR 報告書　2017

調達お取引先

CSR 調達ガイドライン

CSR 調達ガイドラインの周知（CSR 調達アンケート結果）

お取引先へは、適宜アンケートなどを通じて、CSR 調達ガイドラインの周知をお願いしています。前回 2014 年度に引き続き、2016 年度にも、お取引先に対し、CSR ガイドラインに基づいたアンケートを実施し、下記の通り CSR 活動への取り組み状況について回答をいただいています。

- CSR 活動への取組み状況

  「ＣＳＲ調達ガイドライン」として定めた項目に関して、会社方針の制定、従業員への周知、実行するための仕組みづくりや実施状況の把握・管理について調査を行いました。各項目とも約８割の企業で「定着・運用中である」との回答が得られました。また、前回 2014 年のアンケートに比べ、各項目１～５ポイントの改善が見られています。

  取引先の CSR 活動への取組み状況（2016 年度）

  情報セキュリティ対策

  定着・運用中 84%　計画中である 9%　計画していない 6%　無記入 1%

記載例②と同様、取引先の管理と啓発のための取組について定量化への努力を行って実績を数値化し、継続的な改善に繋げるとともに、ステークホルダーの客観的な評価を可能にする内容になっている。

記載例④　キヤノンマーケティングジャパン株式会社　CSR 報告書　2018

情報セキュリティー

情報セキュリティーガバナンスとマネジメント

効率的なマネジメント体制

マネジメント体制は、グループ情報セキュリティー統括体制と各社マネジメント体制の 2 つに分けています。

グループ情報セキュリティー統括体制はキヤノン MJ の情報セキュリティー主管部門がグループ統括事務局の役割を果たし、グループ全体の情報セキュリティーマネジメントを統括しています。

そして、グループ本社機能を持つ組織が、IT・物理・人的セキュリティー施策など、グループ共通のルールや対策の企画立案・推進を行っています。

また、サイバー攻撃に対しては、CSIRT を配置して予防対策を行っています。

一方、各社マネジメント体制では、それぞれの会社の事業特性に応じて、情報セキュリティー主管部門や部門管理体制を設置し、運用しています。

体系的にルールを整備

キヤノン MJ グループでは、キヤノンのグローバル基準である「グループ情報セキュリティールール」を基軸としながら、グループ全体の情報セキュリティーを推進するための幹となる「グループ情報セキュリティー基本方針」と「グループ情報セキュリティーマネジメント規程」を制定しています。

これらの方針や規程を踏まえ、キヤノン MJ グループ全体の情報セキュリティー基盤を支える規程類と、重要な情報資産である個人情報保護や機密管理に関する規程類は、それぞれの規程の中で定める要素が重複することがないようにしています。

たとえば、個人情報保護や機密管理に共通する安全管理措置に関する規程については、個別の規程に定めるのではなく、全社情報セキュリティー基盤を支える関連規程などを外部引用しています。これにより、規程類の二重管理の負荷や、各規程間の不整合を防ぐことができます。

また、個人情報保護や機密管理に関する規程は、グループ各社の業種・業態に応じた管理手法を反映させる必要もあるため、キヤノン MJ グループ統一の規程をベースにした上で、必要に応じて、個別にカスタマイズされた規程を整備しています。

このように、共通する要素の規程間での重複を避け、かつ、各グループ会社の事情に合わせた規程類を整備するような工夫を通じて、体系的なルールの整備に結び付けています。

グループ全体の IT セキュリティー最適化の実現

グループ共通対策としての IT 統制

キヤノン MJ グループでは、グループ会社を含めた統一された IT セキュリティーポリシーに基づき、世の中で日々多発しているサイバー攻撃や不正アクセス、情報漏えいなどの防止に対し、ネットワーク統制、システム・アプリケーション統制、パソコン・メディア統制などの IT 統制を行っています。

これにより、グループ内の対策レベルの均一化と運用コストの削減を実現し、安心安全な IT 環境を実現しています。

また、IT セキュリティーの実装にあたっては、積極的にグループ取り扱い製品を導入することで、運用

ノウハウの蓄積や製品改良に活かしています。
IT 統制の主な内容
＜システム・アプリケーション統制＞
スパムメール対策
電子メール添付ファイル自動暗号化
電子メールモニタリング
ファイル転送サービス
グループ基幹システムの集中管理
＜ネットワーク統制＞
ネットワーク集中管理
ウェブフィルタリング
外部向けサイトの脆弱性対策
ログ管理
IP アドレス管理
＜パソコン・メディア統制＞
ウイルス対策ソフトの自動更新
OS セキュリティーパッチ適用自動化
PC セキュリティーチェッカー
パソコンのハードディスク暗号化
セキュリティー機能付き USB メモリー

グループ全体での IT ガバナンス・情報セキュリティガバナンスの取組に関する情報開示である。グループ会社等について十分な接点や情報がステークホルダーにはないことから、国内外のグループ会社に対して、組織面、ルール面、技術面の 3 つの観点から IT ガバナンス・情報セキュリティガバナンス上適切な対応を行っていることを記載するとともに、情報セキュリティガバナンスへの網羅的な取組が企業価値の源泉に繋がることを経営者が認識していることがメッセージとして伝わり、ステークホルダー目線でグループ単位のガバナンスに力を入れていることがわかる内容となっている。

記載例⑤　JFE ホールディングス株式会社　CSR 報告書　2017

リスクマネジメント

個別リスクへの対応状況

情報セキュリティ

JFE グループは、「情報セキュリティ管理規程」を制定し、不正利用の防止、情報漏洩の防止などの対策を実施しています。規程は外部機関から得られた情報や事故事例などを参考にして定期的に見直し、対応の強化を図っています。また従業員に対する指導・周知と、自主チェックリストに基づく監査により、対策実施の徹底を図っています。

また、情報セキュリティを中心に IT に関する重要課題を「グループ情報セキュリティ委員会」において審議し、グループとしての方針を決定しています。同委員会で決定された方針に基づき、「JFE-SIRT」が情報セキュリティ施策の立案と実施推進、情報セキュリティ監査、インシデント発生時の対応指導を行い、グループ全体の情報セキュリティ管理レベル向上を推進する役割を担っています。

なお、「JFE-SIRT」は他企業とセキュリティ関連情報を共有化し、インシデント発生時には相互に連携することを目的に、「日本シーサート協議会」「電力 ISAC」等の社外団体に加盟しています。

JFE グループの主な情報セキュリティ対策

不正利用の防止

①JFE 統合セキュリティシステムによる認証基盤

②パスワード＋α（IC カードなど）によるパソコン起動認証

情報漏洩の防止

盗難・紛失対策

①生体認証などによるデータセンターへの入退室管理

②執務室への入室制限

③セキュリティワイヤーによる機器管理

④モバイルパソコン内ハードディスクの暗号化

⑤リムーバブルメディアの暗号化

情報漏洩対策

①リムーバブルメディアへの書き出し制限とログ管理

②グループ外への発信メールチェック

③グループ内外への発信メールの全量保管

④社外サービス（Web メール・掲示板、ファイル共有等）の利用制限

⑤認定パソコン以外のグループネットワークへの接続防止

外部脅威への対策

①ファイアウォールによる外部からのアクセス制限

②不審な通信の検知・防御

③マルウェアに対する多重の侵入防止対策

グループ全体の情報セキュリティ管理に関する情報開示である。グループ全体の情報セキュリティ管理のレベル向上の推進役であるCSIRTの役割が丁寧に記載されており、機動性かつ実効性のある情報セキュリティガバナンス体制が適切に構築・運用されていることがメッセージとして伝わり、ステークホルダー目線ではグループにおける対策が一定程度なされていることがわかる内容となっている。

記載例⑥　コニカミノルタ株式会社　統合報告書　2018

IT セキュリティマネジメントシステムおよび情報漏洩防止策

コニカミノルタでは、グループ全体の IT セキュリティ管理体制を確立し、各社の IT セキュリティレベルを継続的に高めています。マネジメントの仕組みとして、日本国内のグループ会社すべてで、国際規格である ISO/IEC 27001 認証を 2009 年から継続して取得しています。海外グループ会社も個別に社内のマネジメントの仕組みを構築しており、2017 年度末時点で 16 社が同認証を取得しています。2016 年 1 月から、KM-CSIRT（KONICA MINOLTA Computer Security Incident Response Team）を発足させ、重大な IT セキュリティ事故が発生した時に迅速に対応できる体制を整備しました。

2017 年度は、相対的にリスクが高いと考えている APAC／中国地域の子会社各社と、マルウェアの一種であるランサムウェアが発生したことを想定した訓練を実施、各地域との連携を強化しました。

また、情報漏洩防止策も継続的に取り組んでおり、次世代ファイアウォール導入によるネットワーク監視強化に加えて、2017 年度は新たにエンドポイント内部における不審な挙動の監視を開始しています。

グループ全体の情報セキュリティ管理に関する情報開示である。国内外のグループ会社における ISO/IEC 27001 の認証について定量的に記載するとともに、CSIRT の設置、海外の子会社向けの訓練や保護対策についても記載するなど、ステークホルダー目線でグループ単位のサイバーセキュリティ対策がなされていることがわかる内容となっている。

記載例⑦　株式会社ニコン　サステナビリティ報告書　2018

情報資産リスクマネジメント

■情報資産の管理方針

ニコングループでは、「ニコングループ情報セキュリティ基本方針」に基づき、国・地域の状況に応じた情報セキュリティ管理体制を整備しています。国内ニコングループでは、さらに「ニコングループ情報管理規程」で詳細を規定しています。海外グループ会社についても、各社が本基本方針に準拠したルールを定め、具体的な施策を展開しています。

ニコングループ情報セキュリティ基本方針
https://www.nikon.co.jp/sustainability/csrmanagement/governance/security_policy.pdf

■情報管理体制

ニコングループでは、社長を情報管理の最高責任者と定めています。そのもとに、情報セキュリティ推進本部を設置し、グループ全体の情報管理に関する施策の立案、および体制整備・維持に取り組んでいます。

具体的には、ニコンの事業部、本部、グループ会社ごとに各組織長を責任者と定め、情報セキュリティ推進本部の指導のもと、適切な情報管理の徹底に努めています。

2019年3月期も引き続き、お客様データを安全に管理するため、関係部門と検討を重ね情報管理体制の強化に努めていきます。

■取引先の情報管理

ニコングループでは、開示情報の管理を取引先（業務委託先）任せとすることが重大な情報セキュリティリスクにつながるととらえています。

これに基づき、2018 年 3 月期には、ニコングループの委託業務に従事する取引先担当者を対象に、情報セキュリティ確保に関する要請事項を記載した携帯カードを約100社分、合計約1,100枚配付しました。

また、2019 年 3 月期には、新たな取り組みとして、「情報セキュリティ通信」（業務委託先向け冊子）を発行します。携帯カードとともにこの冊子を配付し、取引先の情報管理の強化に努めていきます。

■情報セキュリティ教育

ニコングループでは、情報セキュリティに関する従業員への意識付けおよび実効性の向上を目的に、情報セキュリティ教育を実施しています。この教育プログラムには、情報管理に関するポリシー・ルールなどに加え、具体的事例も盛り込んでいます。

また、国内ニコングループおよびアジアグループ会社では、「情報セキュリティハンドブック」を配付してい

ます。
このハンドブックを通じて、従業員一人ひとりが情報管理の重要性を理解し、高い意識で規程を遵守できるよう、恒常的な教育に取り組んでいます。
2018 年 3 月期は、国内ニコングループの従業員を対象に、「私たちがインターネットで注意すべきこと」をテーマとした e ラーニングを実施しました。また、欧州、米州およびアジアの海外グループ会社においても、e ラーニングや季刊誌を利用した情報セキュリティ教育を実施しています。

■情報セキュリティ監査
ニコングループでは、情報セキュリティの徹底に向けて、内部監査を定期的に実施しています。
2018 年 3 月期は、全部門（約 130 部門）に対してチェックリストを配付し、企業機密の管理状況や取引先におけるセキュリティ管理施策の実施状況などについて監査を実施しました。さらに、要配慮個人情報を保有する可能性、マイナンバー業務の環境変化などを重要テーマと位置付け、8 部門（ニコン 6 部門、国内グループ会社 2 社）について実地監査を行いました。
2019 年 3 月期は、個人情報管理などをテーマとした監査を行う予定です。
また、一部の海外グループ会社に対してセルフリスクアセスメントを実施しました。

グループ全体の情報セキュリティ管理に関する情報開示である。グループ全体の基本方針の策定・公表と管理体制の構築、人材育成、情報セキュリティ監査、委託先の情報管理の取組など、幅広い項目について定量的な情報と合わせて簡潔に記載し、グループ・サプライチェーン単位での対策への意識の高さがわかる内容となっている。

⑩　情報共有活動への参加に関する情報開示

【記載のイメージ】

- ✓ ISAC やセプター、J-CSIP といった情報共有コミュニティに参加していることを記載する。
- ✓ IPA や JPCERT/CC 等による脆弱性情報等の注意喚起情報の活用法策について記載する。

記載例①　日本電信電話株式会社　アニュアルレポート　2018

マテリアルの具体例 2　情報セキュリティ・個人情報保護の強化
NTT グループの通信ネットワーク・情報システムを守る取り組み
NTT-CERT

コンピューターセキュリティに係るインシデントに対応する組織（CSIRT：Computer Security Incident ResponseTeam）として、2004 年に「NTT-CERT」を立ち上げ、グループに関連するセキュリティインシデント情報の受け付け、対応支援、再発防止策の検討、トレーニングプログラムの開発及びセキュリティ関連情報の提供などに取り組んでいます。さらに、NTT グループのセキュリティ分野における取り組みの中核として、相談窓口を提供し、NTT グループ内外の組織や専門家と協力して、セキュリティインシデントの検知、解決、被害極小化、及び発生の予防を支援することにより、NTT グループ及び情報ネットワーク社会のセキュリティ向上に貢献しています。

NTT-CERT は、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図っています。

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。加えて、NTT-CERT はグループ各社の CSIRT 構築を推進し、対応能力の向上にも努めています。

今後も、NTT-CERT は脆弱性や攻撃情報などの収集範囲を Dark Web などにまで広げ、情報分析プラットフォームの強化、サイバー脅威対応の更なる自動化・高度化など、変化する脅威に継続的に対応していきます。

情報セキュリティ・個人情報保護の強化の推進役であるCSIRTに関する情報開示である。グループの通信ネットワーク・情報システムを守るうえでのCSIRTの意義・役割や、専門家・セキュリティ関係機関との連携や情報共有活動への参加を通じた今後の対策機能強化に向けた戦略を説明している。これにより、ステークホルダーが、CSIRTを起点としたグループ及び情報ネットワーク社会のセキュリティ向上への貢献について把握することができるようになっている。

４．今後の方向性について

「１．本手引きの趣旨・目的」で述べたように、ICT の利活用が拡大している今日の社会においては、以前にも増してサイバーセキュリティリスクへの対応の重要性が増している。そのため、ステークホルダーに対してサイバーセキュリティリスク及びその対策の情報開示を行うことは、その信頼を得るために重要な取組となっている。

したがって、サイバーセキュリティ対策の情報開示に関し、本手引きが企業の経営層やサイバーセキュリティ対策の実務担当者、広報やＩＲの実務担当者における取組の参考になることを望むものである。

他方、サイバーセキュリティ対策に関する情報開示の取組は、前提となっているサイバーセキュリティリスクの在り方やその対策の在り方によって今後も大きく変わり得ることが想定される。また、現状においても、情報又は情報システムの機密性に関する対策の開示に比べて、可用性や完全性に関する対策の開示についてはまだ途上にある状況である。

本手引きについても、このような企業における開示状況やサイバーセキュリティの動向を踏まえ、関係者の意見も踏まえつつ、適宜見直しの検討を行うこととする。

また、本手引きでは取り上げなかったが、情報開示や情報共有については、不特定多数の第三者への情報開示だけではなく、社内への周知・啓発や取引先・グループ会社・情報共有コミュニティ等との間での情報共有など、様々なパターンが存在する。企業単位でのサイバーセキュリティ対策の質が向上するには、これらの情報開示・情報共有についても取り組むことが望ましい。

参考資料①

○関連施策等の紹介

（１）参考となるガイドライン等

・　サイバーセキュリティ戦略

サイバーセキュリティ基本法に基づき、サイバーセキュリティ戦略本部での検討を経て閣議決定される、我が国の政府の３年間のサイバーセキュリティに関する施策の基本的な方針。直近では 2019 年（平成 31 年）７月に策定されており、目指すサイバーセキュリティの基本的な在り方に関する３つの観点として、①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働、が挙げられている。

・　企業経営のためのサイバーセキュリティの考え方

内閣官房内閣サイバーセキュリティセンターによって策定された、企業経営のためのサイバーセキュリティの基本的な考え方を示したもの。企業が意識すべき３つの留意事項の１つとして、「情報発信による社会的評価の向上」が挙げられている。

・　サイバーセキュリティ経営ガイドライン Ver2.0

経済産業省と独立行政法人情報処理推進機構（IPA）において策定されたガイドラインで、大企業及び中小企業（小規模事業者を除く）の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「３原則」、及び経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要１０項目」をまとめたもの。2017 年（平成 29 年）11 月に改訂。

・　サイバーセキュリティ経営ガイドライン Ver2.0 プラクティス集

上記のガイドラインの「重要１０項目」を実践する際に参考となる考え方やヒント、実施手順、実践事例が記載されている。

・　サイバーセキュリティ経営ガイドライン解説書 Ver1.0

上記のガイドラインの３原則、重要１０項目を具体的に実施するための考え方について解説している。

・　小さな中小企業と NPO 向け情報セキュリティハンドブック Ver1.00

内閣官房内閣サイバーセキュリティセンターが 2019 年（平成 31 年）３月に公開した、特に小規模な事業者や、セキュリティ担当者を置くことが難しい企業及び NPO（特定非営利法人）に向けて、サイバーセキュリティをわかりやすく解説したハンドブック。

・　中小企業の情報セキュリティ対策ガイドライン第３版

独立行政法人情報処理推進機構（IPA）において策定されたガイドラインで、中小企業の経営者や IT 担当者が、セキュリティ対策の必要性を理解し、情報を管理するための具体的な手順等を示したガイドライン。2019 年（平成 31 年）３月に改訂。

・　Cybersecurity Framework Ver1.1

2014 年に米国国立標準研究所（NIST）が発行した、重要インフラのサイバーセキュリティ対策の強化を目的としたガイドラインで、組織のサイバーセキュリティのリスクに対して、現状と掲げた目標とのギャップを分析し、必要となる対策の検討および組織としての対策レベルの底上げを図ることを目的としている。2018 年にサイバーサプライチェーンリスクマネジメントにおけるフレームワークの利用に関する説明を大幅に増やすなどの改定を行い、Cybersecurity Framework Ver1.1 として公開。

・　ISO/IEC 27001、ISO/IEC 27002

ISO/IEC 27001 は組織の事業リスク全般を考慮して文書化した ISMS を確立、実施、維持及び継続的に改善するための要求事項を規定した規格。一方、ISO/IEC 27002 は組織の情報セキュリティリスクの環境を考慮に入れた管理策の選定、実施及び管理を含む、組織の情報セキュリティ標準及び情報セキュリティマネジメントを実施するためのベストプラクティスをまとめた規格。

・　情報セキュリティマネジメントシステム（ISMS）適合性評価制度

情報セキュリティの個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用するための制度。

・　サイバーセキュリティマネジメントシステム（CSMS）適合性評価制度

組織の産業用オートメーション及び制御システム(IACS：Industrial Automation and Control System)を対象として、その構築から運用・保守に渡ってサイバー攻撃から守るためのセキュリティ対策を実施し、システムを運用する制度。 本制度における「CSMS」とは、制御システムに関するセキュリティマジメントのことを意味する。

・　CSIRT 構築マテリアル

組織の事業内容や規模、部門構成、業務遂行形態、それぞれの組織や事業に対応する脅威やリスクの定義により、それぞれの組織内 CSIRT の活動内容や形態などが大きく異なる。CSIRT 構築マテリアルは、このような状況を踏まえ、これから組織内 CSIRT を構築しようとする組織に対して、その構築過程に必要な情報及びノウハウを提供することを目的として公開されている。

（２）関連施策集

・　IT 導入補助金（サービス等生産性向上 IT 導入支援事業）

中小企業・小規模事業者等が、自社の課題やニーズに合った IT ツール（ソフトウエア、サービス等）を導入する経費の一部を補助することで、業務効率化・売上増をサポートする事業。申請に当たって、以下の SECURITY ACTION が必須要件となっている。

・　実践的サイバー防御演習「CYDER」

NICT ナショナルサイバートレーニングセンターにおいて開発・実施されている実践的なサイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）。政府のサイバーセキュリティ戦略等に基づき、サイバーセキュリティ基本法に規定される国の行政機関、地方公共団体、独立行政法人、重要社会基盤事業者等を対象として行われている。

・　SECURITY ACTION

中小企業自らが情報セキュリティ対策に取り組むことを自己宣言するという制度。ただし、情報セキュリティ対策状況等を、IPA が認定するものではないことに留意。

・　コネクテッド・インダストリーズ税制

一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により、生産性を向上させる取組について、それに必要となるシステムや、センサー・ロボット等の導入を支援する税制措置。

参考資料②

○開示書類の事例集

例	名称	企業名	発行年	備考
1	情報セキュリティ報告書 2018	日本電気株式会社	2018	全般的に記載量が多い。
2	情報セキュリティ報告書 2018	富士通株式会社	2018	全般的に記載量が多い。
3	情報セキュリティ報告書 2018	株式会社日立製作所	2018	全般的に記載量が多い。
4	情報セキュリティ報告書 2016	株式会社エヌ・ティ・ティ・データ	2016	全般的に記載量が多い。
5	情報セキュリティ報告書 2018	キヤノンマーケティングジャパン株式会社	2018	全般的に記載量が多い。
6	NTT アニュアルレポート 2018	日本電信電話株式会社	2018	対策が幅広く記載
7	サステナビリティ報告書　2018	株式会社ニコン	2018	対策が幅広く記載。
8	CSR データブック 2018	株式会社セブン＆アイ・ホールディングス	2018	対策が幅広く記載。
9	有価証券報告書 2017 年度	ヤフー株式会社	2018	リスクの記載量が多い。
10	CSR　REPORT 2018（企業考動報告書）	西日本旅客鉄道株式会社	2018	PDCA の記載が存在。
11	統合報告書　2017	ANA ホールディングス株式会社	2017	トップメッセージに記載が存在。