資料７－２

セキュリティ対策の情報開示の事例調査について

総務省　サイバーセキュリティ統括官室

（※）調査は現在も実施中であり、結果については内容が変更になる可能性があります。

調査結果のポイント

セキュリティ対策の情報開示の事例調査

■ セキュリティ対策の情報開示について、日経225の対象企業の過去３年分の開示書類について、「セキュリティ」に関する記載内容を比較・分析。

調査の概要

【調査対象の企業】　日経225（※）の対象企業

（※）【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

【調査対象の開示書類】　過去３年分の有価証券報告書、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

【調査方法】　上述の対象企業及び対象の開示書類について、「セキュリティ」に関する記載がある部分を抜粋し、その内容等について比較・分析を実施。

調査結果のポイント【暫定版】①

（１）制度開示と任意開示について

✓ 全体的な傾向として、制度開示に該当する有価証券報告書やコーポレートガバナンス報告書は、一部の例外を除いてセキュリティ対策に係る一般的な記載に止まる一方、CSR報告書、サステナビリティ報告書、アニュアルレポート、統合報告書等の**任意開示の書類の方が、記載が具体的で量も多く、**また、各社の**取組の独自性が見えやすい状況**であった。

➡ 手引きでは、**任意開示の事例を抽出**することが適当と考えられる。

➡ セキュリティ対策の情報開示の読み手としては、**現時点では**少なくとも投資家だけでなく、取引先や従業員等**様々な主体を含む広範なもの**が想定されていると考えられる。

（２）企業・業界ごとの開示の度合いについて

✓ 特に進んでいる業界は**「電機機器」**、**「通信」**、**「建設」**等であり、特に**「電機機器」**や**「通信」**では、自社のセキュリティのみならず、自社のセキュリティ関連商材・サービスに関する記載が存在するケースも存在する。

✓ また、日経225企業で情報セキュリティ報告書を作成している５社はいずれも「電機機器」や「通信」の業界である。

➡ 上記の業界では、セキュリティ対策の情報開示が**ブランド価値の向上や販促の観点**からも重視されている可能性がある。

調査結果のポイント【暫定版】②

（３）主要５項目の開示動向について

- ✓ 主要５項目のうち、「①セキュリティに関する基本方針等の策定状況」、「②セキュリティに関する管理体制」、「③社員に対する教育・人材育成」については、**記載の粒度や具体性、量は企業によって差異**があるものの、**半数以上の企業**が何らかの記載をしている。

- ✓ 他方、「④社外との情報共有体制」、「⑤第三者評価・認証の取得状況」については、全体の**20%を下回る企業のみ**が記載している状況であり、前者については**CSIRT又はSOCの構築**についての記載が、後者については**ISMS認証やPマークの取得**についての記載が大半である。

➡ **「④社外との情報共有体制」**、**「⑤第三者評価・認証の取得状況」**については、要素の有無で記載可能かどうかがはっきり分かれ、かつ、記載している企業も相対的に少数に止まることから、**外形的にもclear-cutな差別化要因の１つ**と考えられる。

調査結果のポイント【暫定版】③

（４）セキュリティ対策の情報開示の目的・動機について

✓ セキュリティ対策の情報開示を積極的に行っている企業とそうでない企業が存在するため、企業の開示へのモチベーションに働きかける要素が存在するのではないか。

→　業界単位で違いを生む要素はどのようなものが想定されるか。

【想定例】

①　業界全体に働く競争圧力や横並び意識の有無、大小

②　大量の個人情報を抱える等、業界の特性

③　発注先や取引先とのパワーバランス

④　CSRの概念の浸透度合い

⑤　狙われやすい業界かどうか　　等

→　企業単位で違いを生む要素はどのようなものが想定されるか。

【想定例】

⑥　過去にインシデントや不祥事が発生し、ガバナンスのPRの必要性がある　　等

➡ 今後の企業への継続的なヒアリングで上記の仮説を検証（インセンティブの議題で議論）。

調査結果のポイント【暫定版】④

（５）サプライチェーンに係るセキュリティ対策の情報開示について

- ✓ サプライチェーンでのセキュリティ対策については、メーカ（電機機器、機械等）等を中心に取組を開示している企業が一定程度存在。
- ✓ 典型的な例として、**CSR調達ガイドラインの策定・運用**や**取引先へのアンケート**の発出を行うケースが多く、場合によって国内外の**取引先への監査や点検等**を実施するケースも存在

→ **グローバルな取引**のある企業では**CSR調達に関する取組の実施やその開示**が進んでおり、当該文脈で取引先（調達先、受注先）へのセキュリティ対策の開示も進む傾向にある可能性がある。

（６）グループ単位のセキュリティ対策の情報開示について

- ✓ 日経225の企業においては、グループ単位でのセキュリティの基本方針を定め、国内外のグループ会社一括でセキュリティ対策や人材育成等の対策を講じている旨を開示するケースが比較的多い。

調査結果の詳細

調査結果①

（１）制度開示について

✓ 有価証券報告書は、「事業等のリスク」についてセキュリティリスクが、「コーポレート・ガバナンスの状況等」で対策や体制について簡潔に記載されるケースが多いが、例外的に、リスクやセキュリティ対策等について詳述しているケースが存在。

【ヤフー（株） 有価証券報告書（2018年３月期】

（15） 顧客情報等漏洩リスク
2004年8月　情報セキュリティマネジメントシステム（ISMS）の認証を取得

経営方針、経営環境及び対処すべき課題等
4.対処すべき課題
加えて当社グループでは、**個人情報の保護を筆頭にセキュリティの強化を最優先に取り組んで**います。今後も当社グループが提供するサービスを利用者が安全にかつ安心してご利用いただけるよう対策を講じていきます。

（2）技術開発改良に関わるリスク
③設備投資の計画策定や実行が適切に行われなかった場合、サービスの品質が低下したら、逆に過剰投資で費用が増加する可能性があります
大量の通信トラフィックをスムーズにコントロールするためのシステムやネットワークの構築、**決済機能や顧客情報の管理のためのセキュリティ面の強化**、ユーザーからの問い合わせの増加・多様化に適切に対応するためのシステムの強化充実、ビッグデータの活用等、今後は従来にも増して大規模な設備投資をタイミングよく実施していく必要性がより高まるものと予想されます。

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。

調査結果②

【ヤフー（株） 有価証券報告書（2018年３月期】

（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す、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。

調査結果③

【ヤフー（株） 有価証券報告書（2018年３月期】

b.当社の取締役（監査等委員である取締役を除く。）および使用人並びに子会社の取締役、監査役等および使用人、又はこれらの者から報告を受けた者が当社の監査等委員会に報告するための体制その他の監査など委員会への報告に関する体制
（h）内部監査部門は、監査結果の他、当社および子会社の事故等の発生状況、子会社を含めた内部監査の計画、子会社の監査結果等に関して、随時又は監査等委員会において報告をすることとしています。また、**当社および子会社の事故等の詳細な内容については、リスクマネジメント部門・情報セキュリティ部門が監査等委員会へ報告を行う**こととしています。

g.当社の損失の危機の管理に関する規程その他の体制
（d）**情報セキュリティリスクマネジメントを実効性あるものとするため、最高情報セキュリティ責任者(CISO)を任命し、併せて情報セキュリティ統括組織を設置**しています。また、「情報セキュリティ規程群」を定め、情報資産の取扱基準を定めるとともにその周知、教育を行っています。さらに、情報セキュリティインシデントに総合的に対応する組織を設置し、情報セキュリティインシデント情報を一元的に管理・運用し、各部門や社外組織間の調整、および直接的に対応を行う各部門の活動を支援する体制をとっています。**一定水準を超えるリスクについては、CISO又は経営陣がリスク受容やリスク対応を最整決定する体制**になっています。

②業務の適正を確保するための体制の運用状況の概要
（c）常勤の監査等委員は、以下のとおり会社の事項について、報告を受ける等しています。
ii.セキュリティ関連部門長より、セキュリティ関連の報告及びERM（エンタープライズリスクマネジメント）活動の進捗等について報告を受けています。

b.リスクマネジメント体制に関する運用状況
（d）情報セキュリティ統括組織が中心となり、当該改定内容の全使用人への周知・教育、改定内容に沿った体制の構築、およびそれらの状況の点検を行い、結果を社長と最高情報セキュリティ責任者に報告しています。
（e）**情報セキュリティマネジメントシステム（ISMS）の第三者による審査を受け、当該マネジメントシステムの認証を更新**しています。
（f）会社として情報セキュリティに関する適切なリスクの判断ができるよう、当該リスクに係る社内外への課題の変化、残存するリスクの状況、およびリスクの軽減策の実施状況について社長が把握するためのマネジメントレビューを行っています。

c.業務執行の効率性の向上に関する取組みの状況
（d）内部監査部門において、職務の執行の効率性、有効性に関する全社的評価や改善のため、年間を通じて部門別の監査を行ったほか、全社セキュリティ管理等テーマ毎の全社横断的な監査も行っています。

e.企業集団の業務の適正性確保に関する取組みの状況
（e）子会社および関連会社の情報セキュリティに関する情報交換の場としてグループCISO会議を開催しています。
また、**複数の子会社に対し、当社と同様のマルウェア対策のシステムを導入し、当社の情報セキュリティ統括組織の担当者を出向させる等して、グループ全体における情報セキュリティ水準の向上**を図っています。

調査結果④

【ANAホールディングス（株） 有価証券報告書（2018年３月期】

（15） 顧客情報等漏洩リスク

当社グループは、ＡＮＡマイレージクラブの会員数約3,268万人（平成30年３月末日現在）に関わる会員情報をはじめ、膨大な顧客等に関する**情報を保持しており、個人情報保護法やその他諸外国の類似法令により、これらの個人情報を適切に管理することが求められています。当社グループでは、プライバシーポリシーを定め、個人情報の取扱いに関する当社グループの姿勢・考え方を広くお客様に告知するとともに、システム対策を含め情報セキュリティについては想定しうる対策**を講じています。また、セキュリティホールをなくすべく、業務手順の改定やシステム改修を継続的に実施していますが、**不正アクセス**や業務上の過失等、何らかの原因により大規模な個人情報漏洩事故が発生した場合、多額の損害賠償費用が発生し、また、信用失墜により、当社グループの経営に影響を及ぼす可能性があります。

（18）ＩＴ（システム）リスク

当社グループは、お客様へのサービス及び運航に必要な業務等、システム依存度が高い業種といえます。自然災害、事故、**コンピュータ・ウィルス**、不正アクセス、電力供給の制約や大規模停電、故障や不具合等によりかかるシステムあるいは通信ネットワークに重大な障害が発生した場合、お客様へのサービス及び運航の維持が困難になるとともに、信用失墜により当社グループの経営に影響を及ぼす可能性があります。また、当社グループのシステムは他提携航空会社においても使用されており、その影響範囲は自社グループ内にとどまらなくなる可能性があります。

（ⅱ）リスクマネジメント

「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。

- ✓ コーポレートガバナンス報告書は、セキュリティに関する社内体制について簡潔な記載がなされている。また、有価証券報告書の「コーポレート・ガバナンスの状況等」の体制に関する記載内容と同じ記載内容であるケースも多い。

→ セキュリティ対策に係る記載の具体性や記載量については、その他の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の方が充実している。

↓以降はその他の開示書類（※）について記述

（※）情報セキュリティ報告書については、サンプル数が少ないことから省略。

調査結果⑤

（２）グループ単位でのセキュリティ対策

→　日経225においては、グループ単位でのセキュリティの基本方針を定め、国内外のグループ会社一括でセキュリティ対策や人材育成等の対策を講じている旨を開示するケースが比較的多い。

【日清紡ホールディングス（株） 統合報告書（2018年】

グループ各社が守るべきルールを「情報セキュリティガイドライン」に定めており、その遵守状況を確認するために、IT内部監査を国内外の子会社に対し定期的に実施し、継続的改善を図っています。情報システム利用者が守るべきルールを教育資料として定め、定期教育を通じグループ全体の利用者へ情報セキュリティ対策への意識向上を図っています。

【ミネベアミツミ（株） CSRレポート（2018年】

ミネベアミツミグループでは、従業員の情報セキュリティへの意識向上を目的に、情報セキュリティ教育を実施しています。年1回の情報セキュリティに関する説明会の実施、新入社員や中途採用社員に対する入社時の教育のほか、個別指導を実施しています。2017年度は1年を通じて、情報セキュリティに関する説明会を実施し、派遣社員、協力会社従業員を含む13,565名の従業員が参加しました。

【日立製作所（株） サステナビリティレポート（2017年】

日本国外のグループ会社については、国際規格である**ISO／IEC 27001に則った「グローバル情報セキュリティ管理規程」**を定め、情報セキュリティ管理の強化に努めています。日本の親会社から日本国外のグループ会社に対してビジネスチャネルによる展開を行うとともに、米州、欧州、東南アジア、中国、インドなどの地域統括会社によるサポートとセキュリティシェアドサービスの利用を積極的に推進することで、セキュリティ対策の徹底を図っています。

日立の情報セキュリティは、日立製作所が定めた情報セキュリティマネジメントシステムのPDCAサイクルにより推進しています。**日立では、すべてのグループ会社および部門で1年に1回情報セキュリティおよび個人情報保護の監査を実施**しています。
日立製作所における監査は、執行役社長から任命された監査責任者が独立した立場で実施。監査員は自らが所属する部署を監査してはならないと定め、監査の公平性・独立性を確保するようにしています。
日本国内のグループ会社（222社）については、日立製作所と同等の監査を実施し、その結果を日立製作所が確認しています。**日本国外のグループ会社についてはグローバル共通のセルフチェックを実施し、日立全体として監査・点検**に取り組んでいます。また、**職場での自主点検として、全部門が「個人情報保護・情報セキュリティ運用の確認」を1年に1回実施**しています。**併せて重要な個人情報を取り扱う業務（654業務＊1）については「個人情報保護運用の確認」を1カ月に1回実施し、安全管理措置や運用の状況を定期的に確認**しています。
＊1 2017年3月時点の登録業務数

調査結果⑥

【日本電気（株） CSRレポート（2017年）】

NEC グループでは、情報セキュリティ点検により、セキュリティ対策の実施状況を確認し、改善計画を立案・実行する活動を継続して実施しています。

2016 年度は、**当社および国内関係会社60社において情報セキュリティ点検を実施**しました。一般従業員と各施策の管理者を対象に、対策の実施状況を確認する個人単位の役割別点検（個人点検）を実施し、実態を正しく把握することで有効性を高める改善を行いました。**海外現地法人についても34社で個人点検を実施し、対策状況をきめ細かく把握するとともに意識や認知度の向上**をはかりました。

こうした継続的な活動により、情報セキュリティ対策の実施状況は当社および国内関係会社において、着実に改善されています。しかし、**一部の対策については、依然として改善の余地があるものも散見されるので、これらの対策の実施徹底を当社および国内関係会社に注意喚起**しました。一方、海外現地法人については、国内関係会社の実施レベルには到達していないため、**点検結果をもとに各社へ対策を指示するとともに、定期的に対策状況をフォロー**しました。

【京セラ（株） CSR報告書（2017年）】

京セラグループでは、経営戦略、商品開発、各種ノウハウ、技術、組織、人事情報等を会社の重要資産と認識し、京セラグループ統一の「情報セキュリティ管理方針」を制定しています。さらに情報セキュリティ管理方針をベースに、秘密情報管理、知的財産管理、物理的セキュリティ管理、来場者管理、人的管理等に関して「電子情報セキュリティ管理規程」、「個人情報保護管理規程」、「技術ノウハウ流出防止ガイドライン」を定め、管理の徹底をはかっています。また、京セラグループでは、社長を委員長とした「電子情報セキュリティ委員会」を設置し、職制や業務に応じた定期的な従業員教育の実施、情報機器の持ち出し対策、情報資産の漏えい対策、IT資産管理の徹底、内部監査、サイバー攻撃へのセキュリティ対策などを実施しています。さらに、海外の京セラグループ会社においても、情報セキュリティ管理方針、関連規程類に準じ、各国の法制度、商慣習、文化、ビジネス形態に応じて対策の強化に取り組んでいます。

【沖電気工業（株） アニュアルレポート（2018年）】

情報セキュリティ
OKIグループは情報セキュリティ基本方針のもと、情報セキュリティ体制を整備し、お客様および自社の情報の適正管理・保護に努めています。

情報セキュリティの３つの仕組み
OKIグループは下図に示す3つの仕組みを基盤として、PC、ネットワーク、情報システムなどにおける情報セキュリティ対策を幅広く推進しています。また、セキュリティ事故対応専門組織としてOKI-CSIRT※（オキ・シーサート）を設置し、社外組織とも連携して、予防施策および事故発生時の対応力強化に取り組んでいます。2017年度は、インシデント発生時における対応の実効性を高めるために、サイバー攻撃および情報流出の発生を想定した訓練を実施し、全社の緊急連絡体制との連携などを確認しました。

海外における施策の強化
OKIグループは、海外における情報セキュリティ施策を推進しており、各国・地域で情報セキュリティガイドラインの制定や各拠点のセキュリティ管理者の任命、管理ツールの導入などを進めています。2017年度は、これまで国内で実施してきた標的型メール攻撃への対応訓練を、欧米、中国、アジア拠点の電子メール利用者全員を対象に実施しました。

個人情報保護の徹底
OKIグループは、「個人情報保護ポリシー」に基づき、個人情報保護管理責任者のもと、**各部門およびグループ各社に個人情報保護管理者をおいて、個人情報保護を徹底**しています。2017年度は改正個人情報保護法に対応するため関連規程を改訂するとともに、EU一般データ保護規則（GDPR）への対応を検討し、2018年5月に方針書としてまとめました。2018年6月現在、**OKIおよびグループの7社がプライバシーマーク付与認定**を受けています。

調査結果⑦

【キヤノン（株） CSR報告書（2018年）】

■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。

調査結果⑧

【富士通（株） CSR報告書（2017年）】

富士通グループ情報セキュリティ基本方針
ICT を基幹事業とする富士通グループでは、「快適で安心できるネットワーク社会づくり」への貢献を企業理念に掲げ、グループ全体の情報セキュリティを確保しながら、ICT 製品およびサービスの提供を通じたお客様の情報セキュリティの確保とそのレベルアップに努めています。
2015 年 12 月に**経済産業省および独立行政法人情報処理推進機構（IPA）が「サイバーセキュリティ経営ガイドライン」を公表**したことを受け、取締役会に直属するリスク・コンプライアンス委員会において、**グループ全体をカバーするグローバルなセキュリティポリシーの検討を行い、2016年4月に「富士通グループ情報セキュリティ基本方針」を策定**しました。
・富士通グループ情報セキュリティ基本方針（全文）
http://www.fujitsu.com/jp/documents/about/csr/management/security/security-2016-04.pdf

情報セキュリティマネジメント体制
富士通グループでは、昨今のサイバー攻撃の増加を受けて、2015年8月にリスク・コンプライアンス委員会の下に**最高情報セキュリティ責任者（CISO: Chief Information Security Officer）を設置**しました。また、グローバルな情報セキュリティマネジメント体制の強化を目指して、**CISO の傘下に世界各リージョン最高情報セキュリティ責任者（リージョナル CISO）を設置**しました。米州・EMEIA・オセアニア・アジア・日本の 5 つのリージョンにおいてグローバルな ICT ビジネスを支えるグローバルな情報セキュリティガバナンスの強化を図っています。

セキュリティ統制機能
全社セキュリティポリシー策定
富士通グループ各社は、「富士通グループ情報セキュリティ基本方針」に基づき、国内外のグループ会社において情報管理やICT セキュリティに関する社内規定を整備し、情報セキュリティ対策を実施しています。**グローバル共通の富士通グループ情報セキュリティ基本方針の下、グループ会社向けの情報管理関連規定と情報セキュリティ規定を用意**しています。また海外では、その**国の制約に合わせて、会社ごとに規定、ポリシーを独自に作成・整備**しています。

セキュリティ審査・監査
富士通グループでは、**国内外の事業部門を対象に情報セキュリティ監査を実施**しています。この監査は、**事業部門から独立した監査部門**が行います。監査は、事業部門の特性や事業戦略、推進中の情報セキュリティ施策などを踏まえた方法で行われます。例えば、**国内においてはイントラネット敷設時に規定通りに設置されているかの現地調査を実施し審査しているほか、インターネット公開しているサーバは開設時の監査と定期的な脆弱性監査を実施**しています。また海外では **ISO27001 準拠のセキュリティ要件に従い、管理状況についてアセスメントツールを使用して監査**しています。監査を受けた事業部門は、この監査結果を踏まえて、情報セキュリティ対策の改善に努めます。

情報セキュリティ教育
情報漏えいを防ぐためには、規程類を従業員に周知するだけでなく、従業員一人ひとりのセキュリティに対する意識とスキルを向上させることが重要と考えています。そこで、**富士通および国内グループ会社の従業員16万人を対象として、新入社員研修や昇格・昇級時研修の際に、併せて情報セキュリティ教育を実施**するとともに、役員を含む全従業員を対象とした e-Learningを日本語と英語で毎年実施しています。**海外グループ会社の従業員に対しても、年1回のセキュリティ教育を約10カ国語で実施**しています。また、海外の情報セキュリティ管理者には、管理者として必要なセキュリティ教育も実施しています。

情報セキュリティに対する意識啓発
国内富士通グループでは、2007年に「情報管理 徹底宣言！～情報管理は富士通グループの生命線」という国内グループ共通のスローガンを策定して掲げています。富士通および国内グループ会社の各事業所に啓発ポスターを掲示するほか、全従業員の業務用パソコンにシールを貼付するなどの施策を行い従業員一人ひとりの情報セキュリティに対する意識の向上を図っています。これ以外にも、イントラネットを利用し、世の中で多発している情報漏えい事件を紹介することによる注意喚起や、毎月 1 回のセキュリティチェックデーを設け、幹部社員が自部門のセキュリティ対策状況を確認する活動を行っています。

調査結果⑨

（3）サプライチェーン単位でのセキュリティ対策

- ✓ メーカ（電機、機械等）等を中心に取組を開示している企業が存在。
- ✓ 典型的な例として、CSR調達ガイドラインの策定・運用や取引先へのアンケートの発出を行うケースが多い。場合によっては取引先への監査や点検を行うケースもある。

【パナソニック（株） サステナビリティレポート 2018】

調達方針

●CSR調達の実践
法令や社会規範、企業倫理を順守し、人権・労働、安全衛生、地球環境保全、情報セキュリティなど社会的責任を果たす調達活動を購入先様と共に推進してまいります。

●購入先選定と評価
当社では、**新規の購入先選定時に、CSRを実践していることを取引条件**とし、人権・労働、安全衛生、地球環境保全、**情報セキュリティ**などの観点から確認を行っています。**全ての購入先様にCSR自主アセスメントを要請、実施いただき、当社の基準を満たしていることが確認できた購入先とのみ、CSRの要求事項を盛り込んだ取引基本契約書を締結し、取引を開始**します。
また、**既存の購入先に対しても、CSR自主アセスメントを実施し、評価結果に応じて改善に向けた指導や啓発活動**を行っています。

●「パナソニック サプライチェーンCSR推進ガイドライン」の徹底
2016年3月、パナソニックグループでは国際基準や業界での標準的な考え方を参照し、パナソニックグループのCSR調達の考え方を伝えるとともに、購入先様に順守いただきたいCSRの要請項目を**「パナソニック サプライチェーンCSR推進ガイドライン」**（以下、調達ガイドライン）として発行しました。
調達ガイドラインでは法規制を満たしつつ、国際条約や基準を加味し、下記のような内容を定めています。

5）**情報セキュリティ**：情報漏洩の防止、コンピューター・ネットワークの脅威に対する防御

【東京エレクトロン（株） サステナビリティレポート 2018】

お取引先さまとの取り組み

製品の品質を向上させるためには、お取引先さまとの強いパートナーシップ構築が欠かせません。TEL では、品質の維持・向上に向けたお取引先さまへの期待を具体的なものにするため、2000 年より独自のアセスメントシステムである **Supplier Total Quality Assessment（STQA）を実施**しています。
新規取引を開始する際には、この STQA により、製品品質やコスト、**情報セキュリティ体制**ならびに人権・倫理・安全・環境など企業の社会的責任分野の取り組みについて、**セルフアセスメント形式でチェックをおこないます。リスクがあると判断した場合は、お取引先さまを訪問し、現場で不適合箇所や TEL が期待する品質水準をご理解いただいた上で、改善策の立案・実行をお願いしています。そして、すべての改善が完了するまでお取引先さまを継続的にサポートします。重要部品を扱うお取引先さまや品質問題が発生したお取引先さまでは 3 年ごとに現場での監査を実施しています。**また、装置を構成する部品、ユニットの設計、製造上の変更により発生する品質問題の削減、品質改善コストの低減のために、お取引先さまに対する変更管理教育に力を入れています。
お取引先さまに対して説明会を実施し、変更管理の重要性をご理解いただく他、2015 年度からウェブトレーニングを実施しています。

調査結果⑩

【（株）日立製作所 サステナビリティレポート 2017 】

情報漏えいの防止

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。

【カシオ計算機（株） サステナビリティレポート 2017】

カシオが取り組むCSR調達

カシオは公正で公平な取引のもと、法令遵守、人権・労働・安全・健康への配慮、生物多様性の保全や化学物質のリスク管理などによる環境保全、**情報セキュリティなどの社会的責任をサプライチェーンを通じて遂行するために「資材調達方針」を制定**しています。お取引先のご理解・ご賛同によるパートナーシップ体制の構築によりCSR調達水準のさらなる向上に取り組んでいます。

遂行管理の徹底

CSR調達の遂行状況について確認するため、2007年度より、**日本国内の主要なお取引先に対して企業の社会的責任（CSR)遂行に関するアンケート調査※1を開始し、2009年度からは対象を中国とタイのお取引先まで拡大して実施**、2011年度の調査結果や社会環境の変化を踏まえてアンケートの見直しを行い、重複する項目を整理し、新たなテーマとして「紛争鉱物不使用方針」について追加しました。
※ アンケートの項目は**（社）電子情報技術産業協会（JEITA）版「サプライチェーンCSR推進ガイドブック」に準拠**しています。
（1）人権・労働 （2）安全衛生 （3）環境 （4） 公正取引・倫理 （5）品質・安全性 **（6）情報セキュリティ** （7）社会貢献

【ANAホールディングス（株） 統合報告書 2017】

■ サプライチェーンにおけるCSR推進
ANAグループは、自らの事業活動のみならず、**サプライチェーン全体（購入先、製造元、委託先など）でCSR推進に取り組むことが重要であると認識**しています。社会的責任に関する国際ガイダンス（ISO26000）を参考に「ANAグループ購買方針」を定め、これに基づき、「サプライヤマネジメント方針」および「CSRガイドライン」を整備し、ビジネスパートナー各社と共有しています。2016年度は、**170社の取引先を対象にCSRガイドラインに基づいたモニタリングアンケートを実施**するなど、サプライチェーンにおけるCSR推進に取り組みました。

CSRガイドライン　情報セキュリティ 個人情報・機密情報の適切な管理・保護

調査結果⑪

【東京海上ホールディングス（株） サステナビリティレポート 2018】

外部委託管理に関する方針

東京海上グループは、業務の一部または全部を外部へ委託する場合のお客様の保護と利便性の向上ならびに業務の健全性および適切性を確保するため、**「東京海上グループ 外部委託管理に関する方針」**を定めています。また、東京海上日動では、外部委託にあたっては、同方針に基づき、**「外部委託先選定基準」「情報セキュリティ管理態勢基準」に沿って委託先を選定**するとともに、委託先に対する管理態勢を定めた**「外部委託管理に関する規程」に基づき、毎年、外部委託先の実態調査を行い、不備がみつかった場合には、その改善**に努めています。東京海上グループでは、これからも、取引先とともにバリューチェーンと一体となった取り組みを推進していきます。

【（株）NTTドコモ サステナビリティレポート 2016】

■CSR調達の推進
ドコモは、調達方針として、広く国内外のサプライヤのみなさまに対し、公正に競争機会を提供し、ビジネスニーズに即した競争力ある製品・サービスを、経済合理性に基づき調達することを掲げています。また、調達製品の生産過程において、人権の配慮や労働慣行の順守、安全衛生の確保などの社会的な責任を果たすことが重要であるとの考えから、2009年に「NTTドコモCSR調達ガイドライン」を制定しました。また、2013年12月にはNTTグループのCSR調達が導入されたのを機に、ドコモとしても取組みの充実を図るため、**「NTTドコモ サプライチェーンCSR推進ガイドライン」**と名称もあらためたうえで、社会の要請を踏まえた内容へと改定しました。
ガイドラインでは、CSRに関連する7つの領域（人権・労働、安全衛生、環境、公正取引・倫理、品質・安全性、**情報セキュリティ**、社会貢献）で項目を定め、**電気通信設備と携帯電話端末のサプライヤを適用範囲に運用**しています。

●ガイドラインの運用とチェック体制
ドコモは、調達全般の責任者として副社長をトップに、ガイドラインに基づきサプライヤとともにCSR調達に取組むことを基本スタンスとしており、双方でCSRを推進しています。また、こうした考えを理解していただくために**、ウェブサイトにガイドラインを公開し、サプライヤへの説明会を開催**しています。さらに、原則として年1回、**端末・設備関係の製造委託サプライヤを対象範囲としたお取引先に「CSR調達チェックシート」の提出を求め、CSRの実施状況を把握したうえで、必要に応じて改善を依頼**しています。2015年度は**100%となる66社から回答**を得ました。チェック項目はCSRに関連する7つの領域（人権・労働、安全衛生、環境、公正取引・倫理、品質・安全性、**情報セキュリティ**、社会貢献）で140項目におよび、例えば人権分野では、結社の自由および団体交渉の権利行使の順守をはじめ、児童労働、強制労働に関してもモニタリングしています。

調査結果⑫

【日本電気（株） CSRレポート 2017】

お取引先の点検
「NEC グループ お取引先様向け情報セキュリティ基準」や「お客様対応作業における遵守事項」などに基づき、**お取引先の情報セキュリティ対策の実施状況を点検・評価（訪問点検、書類点検）**し、結果をお取引先にフィードバックして改善の徹底をはかりました。**2016 年度は、書類点検を約1,450 社、訪問点検を 50 社に対して実施**しました。継続的な活動により、お取引先の情報セキュリティ対策の実施状況は着実に改善されています。しかし、一部の対策については、他の対策に比べ、実施率が低いものが依然として存在しますので、これらの対策の実施徹底をお取引先に依頼しました。お客さまへの提供製品・システム・サービスにおけるセキュリティ対策状況の点検NEC グループのお客さま対応案件のセキュリティ対策推進状況を“見える化”するシステムの利用促進により、セキュア開発あるいは運用・保守の対策が不十分な案件を特定し、問題案件の改善促進を継続して実施しました。

サプライチェーンマネジメント
基本方針と取り組み
NEC では、社会的責任の国際ガイダンス規格 ISO26000 に基づく CSR 経営のもとで「NEC グループ調達基本方針」を策定し、CSR に関する社内統制およびお取引先への展開をはかっています。特に購買倫理などの社内統制に関しては、「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おり、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資材調達関係者に周知徹底しています。また、お取引先と協働で CSR 推進活動を行うために**「サプライチェーン CSRガイドライン」**を策定し、相互理解を深めながら着実な成果が上がるよう、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。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」を重点リスクと認識し、**サプライチェーン全般にわたりこれら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の取り組みを推進**しています。

➢契約
お取引のあるすべてのお取引先に、「NEC グループ調達基本方針」および「サプライチェーン CSR ガイドライン」を提示。日本国内のお取引先には、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も、これらの履行・遵守を担保しています。また北米、欧州、アジアでは、お取引先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。

➢周知徹底
お取引先に、**NEC グループ調達基本方針、サプライチェーン CSR ガイドラインなど紛争鉱物や環境保護を含む各種ガイドラインを提示し、ご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、お取引先と取り組む最新の施策について情報共有**を行っています。

➢現地監査
情報セキュリティ分野、ならびに人権・安全衛生の分野で、**お取引先を訪問しての現地監査を実施しています。改善を要する事項をお取引先と共有し、改善施策が講じられるところまでフォロー**しています。

書面確認：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システム・インテグレータである 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、調達部門においては、委託先の管理と啓発に力を入れています。毎年、以下のような取り組みを行っています。
・委託先の経営層および CSR 担当役員向け、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50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。

調査結果⑬

（４）取得している認証

✓ ISMS認証（ISO/IEC27001）又はＰマークの取得を開示していた事例が29社。

業種	企業名	媒体	内容
医薬品	大塚ホールディングス（株）	統合報告書	事業活動に応じて「個人情報保護マネジメントシステム（プライバシーマーク）」認証や「情報セキュリティマネジメントシステム（ISMS）」認証を取得
電気機器	三菱電機（株）	CSRレポート	2008年1月にプライバシーマークを全社で取得し、個人情報の適正な取扱いに努めている
電気機器	富士電機（株）	富士電機レポート	2018年4月1日現在、ISMS認証は富士電機（株）の3部門と2社の子会社が取得し、プライバシーマーク認定は、富士電機（株）と3社の子会社が取得
電気機器	富士通（株）	CSR報告書	ISMS（情報セキュリティ・マネジメントシステム）（注 1）認証の取得（2016 年 6 月現在 43 組織認証取得済）を推進するなど、お客様情報など機密情報の管理徹底を図っている
電気機器	沖電気工業（株）	アニュアルレポート	2018年6月現在、OKIおよびグループの7社がプライバシーマーク付与認定を受けている
電気機器	セイコーエプソン（株）	サスティナビリティレポート	ISO27001に準拠したISMS認証（情報セキュリティーマネジメントシステム認証）を取得し、組織的な情報セキュリティーマネジメントの継続的な向上に取り組んでいる
電気機器	（株）アドバンテスト	有価証券報告書	主要な基幹システムサーバーとネットワークのハブは、ISMS（情報セキュリティマネージメントシステム）の承認を受けたシステムセンタに設置
電気機器	カシオ計算機（株）	サスティナビリティレポート	2007年11月に情報セキュリティマネジメントシステム（ISO27001）※2の認定を受けている
電気機器	キヤノン（株）	ＣＳＲ報告書	キヤノンS&Sは、ISMSおよびプライバシーマークの認証に加えてISO9001を取得
電気機器	（株）リコー	ＣＳＲ報告書	2003年にリース業界ではじめてISMSの認証を取得し、2004年にはプライバシーマークを取得
精密機器	コニカミノルタ（株）	統合報告書	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
通信	（株）スカパーＪＳＡＴホールディングス	有価証券報告書	ISMS（情報セキュリティマネジメントシステム）認証及びプライバシーマークを取得
通信	ＫＤＤＩ（株）	統合レポート	2009年4月に、ISMS認証（注）（ISO/IEC27001）を全社に拡大
銀行	（株）静岡銀行	統合報告書	2008年3月、「ISO27001」の認証を取得

調査結果⑭

業種	企業名	媒体	内容抜粋
保険	ＳＯＭＰＯホールディングス（株）	統合報告書	鹿児島センター部が2017年3月22日付で情報セキュリティマネジメントシステムの国際標準規格であるISMS認証（ISO27001）を取得
保険	東京海上ホールディングス（株）	サスティナビリティレポート	情報セキュリティに関する外部認証として、「情報セキュリティマネジメントシステム適合性評価制度（ISMS）」などの認証を取得
小売業	（株）セブン＆アイ・ホールディングス	有価証券報告書、CSR報告書、統合レポート	(ISMS)認証(IS027001)を取得しており、情報セキュリティの強化および必要に応じた認証拠点の拡大に取り組み
サービス	（株）ディー・エヌ・エー	有価証券報告書	「ISO/IEC 27001:2005（JIS Q 27001:2006）（通称:ISMS）」を認証取得する等、国際基準を満たすセキュリティマネジメントに努めている
サービス	（株）電通	統合レポート	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
サービス	ヤフー（株）	有価証券報告書、統合報告書、コーポレートガバナンス報告書	年1回の情報セキュリティマネジメントシステム（ISMS）の第三者による審査を受け、当該マネジメントシステムの認証を更新
サービス	楽天（株）	有価証券報告書	楽天グループの主要な事業において情報セキュリティマネジメントシステム（ISMS）の認証を取得
建設	コムシスホールディングス（株）	有価証券報告書 CSR報告書	統括事業会社のＩＳＯ/ＩＥＣ27001（情報セキュリティマネジメントシステム）やプライバシーマークの認証取得の実績を生かす
建設	清水建設（株）	有価証券報告書	エンジニアリング事業本部においては，情報セキュリティマネジメントが適切に実施されていることを証する「ＩＳＯ/ＩＥＣ 27001:2013/ＪＩＳ Ｑ 27001:2014（情報セキュリティマネジメントシステム）」の認証を取得
建設	（株）長谷工コーポレーション	CSR報告書	国際規格 ISO/IEC27001 を活用しており、2005 年 8月に認証を取得
建設	日揮（株）	統合報告書、アニュアルレポート	2006年に ISO/IEC27001認証を取得し、1年ごとの継続、3年ごとの更新審査を受審
機械	千代田化工建設（株）	有価証券報告書	当社グループでは本社はもとより主なグループ会社でISMS認証を取得して、定期的な教育や監査等の情報セキュリティマネジメントを徹底し、これらのリスクの回避・影響の最小化に努めている
その他製造	凸版印刷（株）	CSR報告書	ISO／IEC 27001 認証取得状況
陸運	日本通運（株）	CSR報告書	ISMS（情報セキュリティマネジメントシステム）認証
倉庫	三菱倉庫（株）	CSR報告書	ISO27001の認証を取得し、定期的に認証機関の第三者評価を受けつつ情報セキュリティレベルの向上に努めている

（５）その他特徴のある情報開示

✓ 目標や実績を公開している企業：日本電気（株）、カシオ計算機（株）、京セラ（株）、西日本旅客鉄道（株）

【日本電気（株） CSRレポート 2017】

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 Security Management 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：◎

【カシオ計算機（株） サステナビリティレポート 2017】

■マネジメント
評価　◎：すべての目標達成、〇：目標をおおむね達成、△：成果より課題が残る、×進捗なし

＜2016年度の行動目標・計画＞
カシオグループ全体における情報セキュリティガバナンスの強化と関連する安全対策の推進。

＜2016年度の実績＞
従業員向けのグループ共通規程を発効。併せて従業員への浸透を図るため、情報セキュリティハンドブックを発行し、啓発を推進。
＜評価＞〇

＜2017年度の行動目標・計画＞
カシオグループ全体における情報セキュリティガバナンスの強化と関連する安全対策の推進。

調査結果⑯

【西日本旅客鉄道（株） CSR報告書 2018】

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
●Plan（2017年度重点取り組み事項）
情報セキュリティ（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】JR西日本グループ全体のセキュリティレベルの向上
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

調査結果⑰

✓ 事故の存在や件数等を公表している企業：（株）日立製作所、（株）リコー、コムシスホールディングス（株）、大阪瓦斯（株）

【（株）日立製作所 サステナビリティレポート 2017 】

情報漏えいの防止

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。**

【（株）リコー 統合報告書 2018】

重点経営リスク
• 情報セキュリティ
情報セキュリティ重大事件・事故件数（リコーグループ
2016年3月期（2015年度） 2
2017年3月期（2016年度） 0
2018年3月期（2017年度） 0
※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：TRM案件。顧客情報の入ったノートPCの盗難、システム障害によるサービス不具合

【コムシスホールディングス（株） CSR報告書 2016】

■安心安全な業務体制
・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。

【大阪瓦斯（株） CSR報告書 2018】

顧客プライバシー
■評価
2016年度実績　個人情報の紛失に対応
2016年度は、大阪ガスグループ会社2社において、お客さま情報が記載された書類の紛失がありました。業務手順の見直しと厳密な管理の再徹底を実施し、再発防止に努めました。

調査結果⑱

✓ 第三者意見を記載している企業：日本精工（株）

【日本精工（株） CSR報告書 2018】

第三者からのご意見　上智大学 名誉教授　上妻 義直 氏
1. CSRマネジメントのグローバル化
地域別売上高・従業員数の３分の２を海外に依存するビジネス実態を考慮すれば、CSRマネジメントにもグローバル化が必要なことは明らかですが、それを着実に進行させている様子が今年度のCSRレポートからよく伝わってきます。たとえば、「NSKビジョン2026」の浸透活動として世界各国で開催されたファシリテーター育成のためのワークショップ、グローバル経営大学に象徴される多文化を受容するグループ風土の形成、管理基準・管理規定の大幅改定による情報セキュリティ体制のグローバル展開、次期中期経営計画への組み込みを模索するSDGs目標など、事業活動とCSRマネジメントをグローバル水準で一体化する施策が多数見られます。いずれも今後の進展が期待される取り組みばかりです。

✓ 積極的な情報開示を表明している企業：キヤノン（株）、富士通（株）

【キヤノン（株） CSR報告書 2018】

■積極的な情報開示と社会への貢献
キヤノンマーケティングジャパングループ（以下、キヤノンMJグループ）は、情報開示による社会貢献として「情報セキュリティ報告書」発行の他にも、「オフィスツアー」による活動事例紹介、各種団体への協力、安全なインターネット活用のためのセキュリティー情報サイトの運営などを行っています。

【富士通（株） CSR報告書 2017】

富士通グループは、「情報セキュリティ報告書」を 2009 年から毎年発行し、情報セキュリティへの取り組みをグローバルに公開し、株主、お客様などのステークホルダーの信頼確保に努めています。
・2017 年度版「富士通グループ 情報セキュリティ報告書」
http://www.fujitsu.com/jp/about/resources/reports/securityreport/2017-securityreports/

調査結果⑲

✓ サイバーセキュリティ経営ガイドラインに準拠している旨を開示している企業

分野	企業名	媒体	内容
電気機器	日本電気（株）	CSRレポート	ガイドラインに適合するための実装ガイド等を発行
電気機器	富士通（株）	CSR報告書	ガイドラインに基づき、情報セキュリティ事故の予防、再発防止のための教育・啓発・監査・情報共有などの施策を継続的に実施
証券	野村ホールディングス（株）	統合報告書	参考にしつつ、包括的なサイバーセキュリティ対策の強化に努めている
水産	マルハニチロ（株）	CSR報告書	ガイドラインに準拠して、情報セキュリティ体制および情報セキュリティ対策の継続的な改善をはかっている。
化学	（株）トクヤマ	CSR報告書	CSIRTがサイバーセキュリティ経営ガイドラインで設置を求められていると記載している。
化学	（株）三菱ケミカルホールディングス	統合報告書	ガイドラインに基づき、外部機関などと連携し、最新情報の収集や緊急対応体制を整備
化学	宇部興産（株）	CSR報告書	ガイドラインに基づき、制御システムのセキュリティ対策検討、セキュリティインシデント発生時に被害を最小化するための体制構築、海外グループ会社のセキュリティ体制の強化などを実施
非鉄・金属	古河電気工業（株）	サスティナビリティレポート	ガイドラインに沿った仕組みの整備（CISIRTなど）
商社	双日（株）	有価証券報告書 コーポレートガバナンス報告書	当該ガイドラインを踏まえた関連規程の改定、ガイドラインの整備等
建設	鹿島建設（株）	統合報告書 アニュアルレポート	準拠して対策を講じている（K-SIRTを設置し、情報収集）
空運	ANAホールディングス（株）	有価証券報告書	ガイドラインに準拠し、多層防御や第三者機関によるリスクアセスメントを実施