

情報セキュリティ

基本的な考え方

TOPPANグループは、グローバルな社会課題を解決するリーディングカンパニーを目指し、事業に必要な情報やシステムを適切かつ安全に管理することが経営上の重要課題であることを認識し、グループを挙げて情報セキュリティ管理およびサイバーセキュリティ対策を進めることで、安心・安全な製品・サービスの提供に取り組んでいます。

IoTの高度化やデジタル化の急速な進展を背景に、サイバー攻撃の脅威が高まっており、機密情報や個人情報を含む情報資産の漏えいだけでなく、事業そのものの継続までが脅かされるようになっていきます。

こうした中で、DXの利活用を通じて企業価値を創造し、お客さまや社会の信頼に応えるため、TOPPANグループは「TOPPANグループ情報セキュリティ基本方針」や「TOPPANグループプライバシー方針」「個人情報保護方針」を掲げ、グループ一丸となり、技術面・運用面での対応を徹底しています。サイバー攻撃に対するツールや仕組みの導入、情報セキュリティ上の脅威に対する監視と対応体制の強化を積極的に進める一方で、全従業員がセキュリティを守る責任を自覚しグループの方針に従って業務を遂行できるよう、継続的に教育するなど、セキュリティシステムへの投資を継続的に行っています。

また昨今のサプライチェーンリスクの増加に対応するため、重要な情報を取り扱う委託先に対しては監査を実施しリスクの低減を図っています。

🌐 TOPPANグループ情報セキュリティ基本方針 >

<https://www.holdings.toppan.com/ja/about-us/our-corporate-approach/security-information.html>

🌐 TOPPANグループプライバシー方針 >

<https://www.holdings.toppan.com/ja/about-us/our-corporate-approach/group-privacy.html>

🌐 個人情報保護方針 >

<https://www.holdings.toppan.com/ja/privacy.html>

TOPPANグループ情報セキュリティ基本方針

私たちTOPPANグループは、情報コミュニケーション産業として、事業に必要な情報の管理が、お客さまの信頼に応え、TOPPANグループの永続的な発展を図るために、経営上の重要課題であることを認識し、TOPPANグループを挙げて情報セキュリティ管理に取り組めます。

1. 私たちは、法と社会秩序を遵守のうえ、社内の規程類に則り、当社の事業に必要な情報を適切に管理します。
2. 私たちは、情報を収集するにあたっては、正当な目的および方法をもってこれを行います。
3. 私たちは、お客さまより預託を受けた情報について、お客さまの信頼に応えるべく、安全に情報を管理します。
4. 私たちは、私たちの取り扱う情報資産について、不正なアクセスまたは滅失、毀損、改ざん、漏えい等の危険を深く認識し、必要かつ合理的な安全対策を講ずるとともに、問題が発生した場合は、適切かつ速やかに対処し是正します。
5. 私たちは、情報セキュリティマネジメントシステムを構築、運用、維持し、さらに継続的に改善を図ります。

制定日 2001年4月1日
最終改定日 2023年10月1日

TOPPANホールディングス株式会社
代表取締役社長 CEO 麿秀晴

ガバナンス

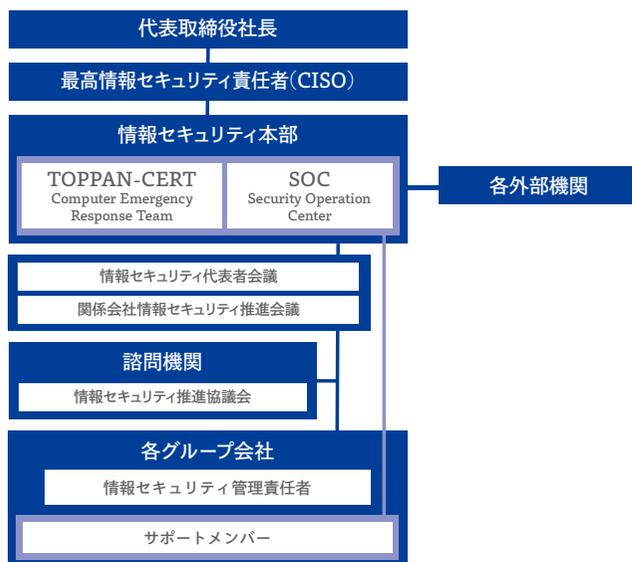
推進・管理体制

TOPPANグループでは、情報セキュリティ本部を設置し、監理・統制、技術、ならびに人財面で対応しています。社内外のセキュリティリスクや被害件数のモニタリングを行うとともに、サイバー攻撃や情報漏えいなどのインシデントや脆弱性が発見された際のプロセスを整備し、これらの分析・対応を行う組織横断的なサイバー対応の専門チームを設けて、グループ会社を統括し、外部機関とも連携を図りながら情報セキュリティ管理を推進しています。また、情報セキュリティにバックグラウンドをもつ情報セキュリティ本部担当役員を最高情報セキュリティ責任者(CISO)として任命しています。

グループ会社には情報セキュリティ管理責任者を置き、情報セキュリティ本部による統制のもとで定期的な情報共有の場などを通じて各組織のセキュリティ管理を推進しています。

セキュリティインシデントが発生した際の事業継続計画(BCP)を踏まえた演習においては毎回CISOや事業部門幹部も参加して対応力の強化を図っています。ガバナンス推進の一環として、情報セキュリティマネジメントシステムに基づいた内部監査の実施と第三者認証の取得も進めています。

情報セキュリティの組織管理体制



情報セキュリティマネジメント

CISOのもと、情報セキュリティ本部が情報セキュリティに関する全体計画の策定、規程の整備・見直しなどを行い、グループ会社との定期的な会議体を設けて、情報セキュリティに関する方針や施策の共有を図っています。

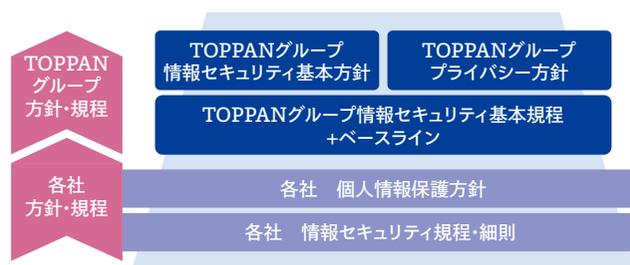
また、グループ会社に対しては、定期的な監査を実施し、マネジメントの状況確認と是正改善を行っています。

さらに、これらの活動については、CISOに定期的な報告を行うとともに、万一、インシデントが発生した場合にも、CISOに適宜報告を行い、迅速にインシデントに対応する体制となっています。

セキュリティガバナンスを支える規程体系

TOPPANグループでは、ISO/IEC 27000およびJIS Q 15000に準拠したTOPPANグループ情報セキュリティ基本方針とTOPPANグループ情報セキュリティ基本規程を定め、グループ各社ではこれらに基づいた個人情報保護方針ならびに規程・細則類を制定し、管理体制の構築およびルールの周知を組織的に推進することでセキュリティガバナンスを支えています。

情報セキュリティ規程体系



戦略・施策

課題と対応

TOPPANグループは事業拡大を進める中で、特に海外における企業や事業の買収などを行っており、新たにTOPPANグループに加入する企業の情報セキュリティの確保が重要な課題となっています。この課題に対応するため、グループ基本規程をもとに新たに加わる会社の情報セキュリティ規程との整合性を確認し、不足がある場合には迅速にその規程の整備・改善を行っています。これにより、国内外の全グループ会社で統一された情報セキュリティ基準を維持しています。

さらにサイバーセキュリティリスクに対応するためのフレームワークである米国のNIST CSF(サイバーセキュリティフレームワーク)を基準とした第三者評価を事業ごとに実施することで、現在のセキュリティ状況と目標水準とのギャップを分析し、その差を埋めるための具体的な対策を計画・実行しています。これにより、グループ全体の情報セキュリティ統制を包括的に強化し、持続的な安全性の向上を図っています。

目指す姿実現に向けた中長期的な戦略

TOPPANグループでは、情報セキュリティ基本方針に示した通り、事業に必要な情報の管理を経営上の重要課題として位置付けています。私たちが目指す姿として掲げるDX事業の加速やグローバル事業を拡大するため、自社や顧客の安心・安全を守るだけでなく、サプライチェーン全体でビジネスを加速するための情報セキュリティを目指し、「監理・統制の徹底」「技術的な対策」「人材育成」の3つの側面での取り組みを進めています。

1) 監理・統制の徹底

● セキュリティベースライン評価を用いたグローバル統制

グループ全体として統制のとれた情報セキュリティ強化のため、全グループ会社を対象にTOPPANグループ情報セキュリティ基本規程を基にしたベースライン評価を実施しています。評価では、組織的・人的・物理的・技術的対策、インシデント対応、個人情報保護の成熟度を採点し、改善計画を策定、その進捗をモニタリングし、グループ全体のセキュリティ水準向上を目指しています。評価結果は、事業会社・部門、グループ全体の施策へ反映させています。

また、特に海外企業買収などの際は、当社規程との整合を確認し、

必要に応じ整備・改善を行い、グループ全体での情報セキュリティの統制を図っています。

● 改正個人情報保護法への対応

個人情報保護法改正に対しては、情報セキュリティ規程などの個人情報関係ルールの改定を適時行っています。また、個人情報保護委員会から開示されたガイドラインに従って、仮名加工情報および個人関連情報への対応、越境移転がある場合の本人への通知、インシデント発生時における報告対応を行っています。

● 個人情報とプライバシー保護に関する各国法規制への対応

個人情報保護やプライバシーへの意識の高まりを受けて、世界各国でプライバシー保護に関する法規制が制定されています。TOPPANグループはプライバシーを保護・尊重する姿勢を示すため、2025年4月に「TOPPANグループ プライバシー方針」を策定しました。TOPPANグループが展開する各国や地域における当該法規制に関する、情報収集や調査を通じて、法規制への適切な対応を実施しています。

🌐 TOPPANグループ プライバシー方針 >

<https://www.holdings.toppan.com/ja/about-us/our-corporate-approach/group-privacy.html>

● プライバシーマークおよびISMSへの対応

情報セキュリティにかかわる認証として、プライバシーマークおよびISMS(情報セキュリティマネジメントシステム)を取得しています。個人情報などお客さまの重要な情報を安全に取り扱うため、ルールの制定、環境の構築、要員の教育に取り組んでいます。

● マイナンバー制度への対応

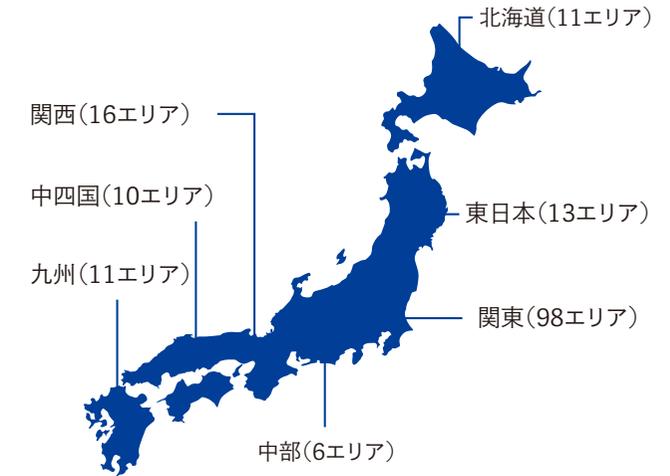
従業員のマイナンバー取り扱い業務、およびお客さまによる顧客のマイナンバー収集を代行する業務などに対応するため、セキュリティエリアの基準に、個人情報保護委員会「特定個人情報の適正な取り扱いに関するガイドライン」に基づく安全管理措置を追加しました。他の情報取り扱いと分離するため、独立したマイナンバー取り扱いルームを設け、専門チームによる認定監査を実施しています。

● セキュリティエリアの設置

TOPPANグループでは、個人情報(マイナンバー含む)の取り扱い、金銭的価値を有する証券印刷物の生産や取り扱い、その他機密指定案件の取り扱い業務は、入退室制限、独立したネットワーク環境など、内部不正や外部からの不正アクセス防止などの対策が施されたセキュリティエリアで行っています。

その結果、2024年度の情報の不正な持ち出しなどの事故は0件であり、今後も事故0件を継続することを目標としています。

セキュリティエリアのある拠点とその数
(2025年3月31日現在)



※ 個人情報を取り扱うセキュリティエリアの数

● セキュリティエリアの安全管理策

個人情報取り扱い業務および機密情報取り扱い業務については、セキュリティエリアの運用管理ルールを定期的に更新し新たなリスクに対応しています。併せて、現場での日常的なチェックと、定期的な内部監査によって、セキュリティレベルの維持向上を図っています。

<内部監査での運用管理のチェック>

専門の監査員により、セキュリティエリアの設置・管理・運用の状況を定期的に監査し、結果を評価認定することで、運用管理レベルの維持と強化を図っています。

<入退室管理>

セキュリティエリアには、許可された人間のみが入退室可能な技術的対応(本人認証、共連れ防止策等)を施しています。

また、画像、映像、音声などを記録・通信する装置(カメラ、携帯電話、スマートフォン等)の持ち込みは禁止し、エリアの外に私物入れロッカー等を設置しています。

<エリア内管理>

セキュリティエリア内では、監視カメラを死角ができないように設置し、不正なデータ持ち出しに対するモニタリングが可能な対応をしています。

<端末管理>

セキュリティエリアで使用される端末には、原則として外部記憶媒体の接続を禁止し、不要な接続先へのアクセスを制限するとともに、IDとパスワードに加えてその他要素も加えた二要素認証を適用したログインを行っています。

また、ログ管理システムに操作ログを収集・保管し解析することによって、不正が疑われる場合には監視センターより責任者へ連絡して確認を取る運用を行っています。



監視カメラ



入退管理

● サプライチェーンに対するセキュリティ管理

TOPPANグループでは、個人情報や機密情報の取り扱いを含む一部の業務をグループ会社や協力会社に委託したり、他社のクラウドサービスを活用したりして業務を行うことがあります。

その場合、これらの委託先が当社のセキュリティ基準を満たしていることを確実にするため、委託する業務内容や情報の種類に応じて、適切なセキュリティ対応を実施している外部委託先を認定する制度の導入やクラウドサービスの安全性確認を行い、サプライチェーンリスクの低減を図っています。

● 社内業務における情報資産の取り扱い対応

TOPPANグループでは、社内業務で取り扱う情報資産の機密性に応じて区分をつけ、情報資産の区分に応じた、保管、持ち出し、開示等に関するルールを規定し安全な情報資産の取り扱い対応を実施しています。

● 情報セキュリティにおける重大インシデント対応ガイドラインの制定

サイバー攻撃の脅威は世界的規模に拡大し、その悪質さ、巧妙さが想定外なだけでなく、瞬時にして甚大な被害に拡大することから、従来の事故対応の手法では対応し得ないものとなっています。

TOPPANグループでは、サイバー攻撃等による重大インシデントに対応するためのベースとなる「考え方」「態勢」「対応フロー」をガイドラインとしてまとめ、想定外の事象が発生し得るとの前提に立った対応力強化を図っています。

● サイバーセキュリティインシデント対応体制

TOPPANグループでは、サイバーセキュリティインシデント対応専門チーム「TOPPAN-CERT」を中心とした、インシデントに迅速に対応するグローバル体制を整えています。TOPPAN-CERTは、内閣サイバーセキュリティセンター(2025年7月に国家サイバー統括室に改組)と日本シーサート協議会(NCA)が主催する連携分野横断的演習に毎年参加し、実際にサイバー攻撃を受けた場面を想定した演習を行っています。CERTメンバーが中心となって対応を行い、演習後には振り返りを実施することで、対応手順や課題を検証し、サイバー攻撃を受けた際の対応手順の改善に役立てています。

● サイバーセキュリティ状況の共有

社内外のサイバーセキュリティ環境の状況の理解を深めるため、情報セキュリティ関係者向けに四半期ごとのサイバーセキュリティ情報共有会を実施しています。

● 委託先認定監査

個人情報や機密情報の取り扱いを含む一部業務の外部委託や、他社クラウドサービスの活用の際に、委託先がTOPPANグループのセキュリティ基準に適合するため、委託する業務内容や情報の種類に応じた外部委託先を認定する制度の導入やクラウドサービスの安全性確認を行い、サプライチェーンリスクの低減を図っています。

2) 技術的な対策

● PC 内での不審な挙動を検知するためのツール (EDR:Endpoint Detection and Response) によるPC・サーバへの対策

2019年度より導入を開始したEDRの展開を進め、社内の事務端末をはじめ、製造現場の端末やMac、サーバへのEDR導入を完了しました。また、ネットワークログなどを組み合わせ、高度なウイルスを早期に検出・対処する体制を継続的に強化しています。

● パブリッククラウドのセキュリティ設定ミスを検出するサービス(CSPM: Cloud Security Posture Management)の活用

メガクラウド特有の不適切な公開権限の設定などによるセキュリティリスクを可視化し、問題のある設定を早期検出・是正につなげるためにCSPMの展開を進めております。開発・テスト環境を含め、パブリッククラウド利用時のリスクを低減する活動を強化していきます。

● 外部からのモニタリングによるサイバーセキュリティの強化

TOPPANグループに対するサイバー攻撃の兆候や外部から見つけられる可能性のある脆弱性を早期に発見するため、セキュリティレーティングサービスや脅威インテリジェンスを活用した攻撃者視点での外部からのモニタリングと、OSINT(Open Source INTelligence)の活動を継続しています。TOPPANグループだけでなく、個人情報・機密情報を取り扱う委託先にも対象を広げ、サプライチェーン全体でのセキュリティ強化にも努めています。

● Webサイトの脆弱性診断対応強化

Webサイトの脆弱性を狙ったサイバー攻撃の対策として、これまで脆弱性診断の運用を行ってききましたが、日々発生する新たな脆弱性に対応するために、定期的かつ自動的にネットワーク診断を行う脆弱性監視の運用や外部サービスによる脆弱性の検出を行っています。これにより、自社サービスの安全性向上に加え、より安全なサービスのお客さまへの提供につなげています。

また、コーディングに関するセキュリティガイドラインを刷新し、APIなどクラウドネイティブアプリケーションに脆弱性を含みにくい設計を心掛けています。

● IT資産管理情報を活用した不正な端末の接続排除

データベース上で管理しているIT資産情報と実際の社内ネットワーク通信の整合性チェックを行うシステム、および社内LAN上にネットワークセンサーを導入し、不正な端末の持ち込みによるウイルス感染や情報漏えいのリスクを低減する活動を展開しています。

● 電子メール攻撃への対策

ランサムウェアの感染経路の入口としても頻繁に使われるメール添付ファイルやビジネスメール詐欺などの電子メールを悪用した脅威に対し、AI分析や機械学習を活用して電子メールを検疫するサービスを2022年度に導入し、主要な国内グループ会社への展開を完了しました。

今後も海外を含めたグループ各社への展開を図り、標的型攻撃やウイルス感染などのリスクを低減し、メール攻撃耐性強化を図ります。

● 工場のセキュリティ強化

スマートファクトリー化に伴い様々なモノがネットワークとつながることになり、これまで以上にサイバー攻撃の可能性が上がります。そのためTOPPANグループでは、2023年6月に工場セキュリティガイドラインを発行し、工場内のネットワークやサーバの設定、ログやバックアップの取得のような工場で実施すべき具体的なセキュリティ対策を示すとともに、この内容を従業員に周知・教育することでセキュリティ強化を図っています。

3) 人財育成

TOPPANグループでは、情報セキュリティ戦略の達成に求められる人財像を設定し、育成・確保に努めています。

・専門セキュリティ人財

TOPPANグループのセキュリティを支える人財としてセキュリティを専門とする業務従事者および情報処理安全確保支援士やCISSPなどの有資格者

・プラスセキュリティ人財

各職域・業務のセキュリティを支える人財として情報セキュリティにかかる業務従事者および情報セキュリティマネジメント試験合格者やベンダーによる研修修了者・有資格者

● 全従業員向け教育の実施

TOPPANグループでは、年1回、全従業員のセキュリティレベル向上のために定期教育を実施しています。

2024年度は、「～社会の変化に先手を打ち、情報セキュリティの脅威に新生TOPPANグループ一丸となって挑もう～」をテーマに、サイバー攻撃への備え、日常業務におけるセキュリティ上の留意点、

第三者認証の取得

ISMS認証取得「ISO/IEC 27001」とプライバシーマーク付与認定(JIS Q 15001:2017)などをTOPPANグループ各社で取得しています。(2025年4月1日現在)

ISMS認証取得(ISO/IEC 27001)

(情報セキュリティマネジメントシステム)

TOPPAN(株) 情報コミュニケーション事業本部 TOPPANコミュニケーションプロダクツ(株) TOPPANグラフィックコミュニケーションズ(株) (株)TBネクストコミュニケーションズ	IC23J0567
TOPPANエッジ(株) TOPPAN(株) 情報コミュニケーション事業本部 TOPPANコミュニケーションプロダクツ(株) ティージーエス(株)	JQA- IM2142
TOPPANデジタル(株) サービスマネジメントセンター インフラサービス部、サービスオペレーション部 ICT開発センター DXソリューション開発部	IC23J0568
TOPPANエッジ(株) トッパングループ関西ビジネスセンター	JQA- IM0137
TOPPANインフォメディア(株) 本社(知財担当を除く)、第一営業本部第一部(小石川営業所)、第三営業本部第一部一課(関西営業所)、福島工場、相模原工場(開発部門を除く)、相模原北工場、相模原西工場、西倉庫、滝野工場	JUSE- IR-404
TOPPANテクニカル・デザインセンター(株)	JP22899-I-2
(株)ONE COMPATH	IS 533218
TOPPAN(株) 西日本事業本部 九州事業部・中四国事業部セキュリティエリアおよびISMS推進委員会	I308
TOPPANグラフィックコミュニケーションズ(株) 関西制作本部 TOPPAN(株) 西日本事業本部 関西クロステックビジネスイノベーション事業部	IC13J0361
TOPPAN(株) 東日本事業本部	IS 606897
TOPPANコミュニケーションプロダクツ(株)滝野工場 TOPPAN(株) 西日本事業本部 関西情報系技術部 情報系滝野生産技術T	IC14J0376

TOPPAN(株) 中部事業部 TOPPANコミュニケーションプロダクツ(株) 名古屋工場	IC17J0444
TOPPANエッジITソリューション(株) ITサポートセンター、NEXTプロジェクト、営業部、システム開発部 業務サービスグループ(帳票変換担当)インフラサービスグループ(導入支援・保守担当)、システム管理部、ISO/RM推進部	JUSE- IR-403
(株)トスコ	IC07J0211
(株)アイオイ・システム	J0265
東京書籍(株) 教育DX事業関連部門 (株)学習調査エデュフロント	IC23J0562
おかびファーマシーシステム(株)	IS 794168
その他非公開:1事業者	

ISMS認証取得(ISO/IEC 27017)

(クラウドセキュリティマネジメント)

TOPPANデジタル(株) ICT開発センター DXソリューション開発部 3チーム	SC22J0025
TOPPANエッジITソリューション(株) ITサポートセンター、NEXTプロジェクト、営業部、システム開発部、システム管理部、ISO/RM推進部	JUSE-IR-403-CS01(基となるISMS登録番号:JUSE-IR-403)
東京書籍(株) 教育DX局 DX開発本部 教育システム開発部、教育システム事業推進室、DX事業創出本部 DX企画部 インクルーシブ教育チーム	SC24J0029(基となるISMS登録番号:IC23J0562)

プライバシーマーク付与認定(JIS Q 15001)

TOPPAN(株)	10190891
TOPPANコミュニケーションプロダクツ(株)	24000216
TOPPANグラフィックコミュニケーションズ(株)	10190298
TOPPANエディトリアルコミュニケーションズ(株)	24000308
TOPPANロジスティクス(株)	10450006
TOPPANトラベルサービス(株)	10450093
TOPPANエッジ(株)	10190934

TOPPANエッジITソリューション(株)	10820089
TOPPANデジタル(株)	24000478
(株)トスコ	11820447
(株)ジェイエスキューブ	10860018
TOPPANクロレ(株)	24000032
東京書籍(株)	10190966
(株)フレーベル館	24000369
(株)BookLive	28000007
東京都チャレンジドプラスTOPPAN(株)	24000419
(株)ONE COMPATH	24000445
TOPPANコスモ(株)	24000449
(株)TBネクストコミュニケーションズ	24000464
TOPPANインフォメディア(株)	24000473
livepass(株)	25000225
(株)理研ジェネシス	14300052
(株)ブックリスタ	10824078

リスク管理

情報セキュリティにかかるリスクは、TOPPANグループに関連する主要なリスク項目を示した「事業等のリスク」に特定しており、総合的なリスク管理に組み込まれています。

(サステナビリティ関連リスクにかかわるリスク管理の詳細は、有価証券報告書「第2 事業の状況 2 サステナビリティに関する考え方及び取組 (1)サステナビリティ共通 ③リスク管理」を参照ください)