

2017.12.01

CSR・ERM トピックス <2017 年度第 9 号>

本誌は、CSR（企業の社会的責任）および ERM（統合リスクマネジメント）に関連する諸テーマについて、国内・海外の最近の動向や企業の抱える疑問などについて紹介・コメントした情報誌です。「コーポレート・ガバナンス」「リスクマネジメント」「コンプライアンス」「人権」「労働慣行」「環境」「品質」「CS（顧客満足）」「社会貢献」「CSR 調達」「情報セキュリティ」等、関連する様々なテーマを取り上げます。

国内トピックス：2017 年 10 月に公開された国内の CSR・ERM 等に関する主な動向をご紹介します。

<情報セキュリティ>

○独立行政法人情報処理推進機構が「制御システムのセキュリティリスク分析ガイド」を公表

（参考情報：2017 年 10 月 2 日付 同法人 HP）

独立行政法人情報処理推進機構（以下、IPA）は 10 月 2 日、「制御システムのセキュリティリスク分析ガイド」および「制御システムに対するリスク分析の実施例」を公表した。

近年の制御系システムは、開発のコスト削減のため Windows や UNIX などの汎用プラットフォームが使われ、制御の利便性から無線 LAN や外部ネットワークにつながれることが多く、セキュリティリスクにさらされる頻度が増大している。

また、制御系システムは 24 時間常時稼働が前提となっているため、システム停止は企業に与える影響が大きい。

本ガイドは、企業・組織の制御システム分野のセキュリティレベルの抜本的な向上と継続的な維持見直しを推進することを目的に、リスク分析の具体的な手順や、実際にリスク分析する際に役立つツール（リスク分析シートや各種チェックシート等）を取りまとめたもの。

本ガイドに掲載されているリスク分析手順の概要は以下の通り。

【第一ステップ】

- システム構成の把握
 - ◇ ネットワーク構成図を作成し、使われている主要機器類を把握する
 - ◇ 物理的なセキュリティゾーンを把握し、システムへの物理的アクセス状況を把握する
- 資産の把握
 - ◇ 制御システムに存在する資産（機器類、通信経路）を洗い出す
 - ◇ 資産の機能、稼働状況、接続されているネットワークなどを把握する
- データフローの把握
 - ◇ 情報や入力コマンドの流れを把握し、データフローを把握する
 - ◇ 情報の流れを把握し、どこからアクセスしコントロールできるのかを把握する

【第二ステップ】

- 資産の重要性の決定
 - ◇ 把握した資産の重要性判定基準を定義し、それに当てはめ重要度を決定する
- 事業被害とそのレベルの定義
 - ◇ 事業被害が発生した際にどの事業に与える影響があるのかという観点から定義する

- 脅威レベルの定義
 - ◇ 想定する脅威が発生する可能性を定義し評価する
 - ◇ 想定する攻撃手法から、危機ごとの脅威を把握評価する
- セキュリティ対策項目の確認
 - ◇ 想定する脅威に対するセキュリティ対策を把握する
 - ◇ 脅威と対策を比較し脆弱性を判断、必要なセキュリティ対策項目を洗い出す
 - ◇ 防御/検知/被害把握などセキュリティ対策を分類し、必要な対策を把握する

【第三ステップ】

- 具体的なリスク分析方法
 - ✓ 資産ベースのリスク分析
 - ◇ 資産ごとの重要度を決定し、脅威と対策を把握する
 - ◇ 脅威に対するセキュリティ対策を把握する
 - ◇ セキュリティ対策レベル、脆弱性を評価する
 - ◇ リスク値を評価する
 - ✓ 事業被害ベースのリスク分析
 - ◇ 攻撃手法を洗い出す
 - ◇ 攻撃を想定した対応を洗い出す
 - ◇ 脅威に対する対策を一覧にする
 - ◇ 脅威レベルに照らし合せて評価する

【第四ステップ】

- リスク分析結果からリスクの高い資産や攻撃シナリオを抽出し、脆弱性や脅威の低減策を検討し、実施の優先順位をつける

<CSR>

○ヤマハなど 167 の企業・団体が「SoundUD 推進コンソーシアム」を設立

(参考情報：2017 年 10 月 26 日付 同社 HP)

ヤマハは 10 月 25 日、言語や聴力への不安がない社会（音のユニバーサルデザイン化社会）の促進を目的として、同社を主催社とし、167 の日本企業・団体が参加する「SoundUD 推進コンソーシアム」*を設立した。

近年、訪日外国人が増加したり、障害者差別解消法が施行されている一方、日本語が分からない外国人や聴力に不安を持つ人を支援する取り組みは十分とはいえない。ヤマハは、このような取り組みを促進するため、音声アナウンスの内容を多言語に翻訳し、文字情報としてアプリやデジタルサイネージに表示できる自社技術を基に、他社・団体と協業する。

本コンソーシアムには、ヤマハのほか、IT 企業、航空会社・鉄道会社、商業施設の運営企業、地方自治体など、幅広い企業・団体が参加している。

同社は、2018 年 4 月より、本コンソーシアムの会員向けに、交通、商業、防災に関するテンプレートアナウンスを日英中韓の 4 言語の音声と 13 言語の文字で配信できる自社のタブレットアプリや、会員企業各社の製品やアプリに組み込むことができるような開発モジュール・開発キットの提供などを行う予定。**

本コンソーシアムでは、音に関するユニバーサルデザイン化に対応できる施設や対応アプリ・システムを拡充するための取り組み等を進めていく予定。

* SoundUD 推進コンソーシアム

SoundUD は「Sound Universal Design : 音のユニバーサルデザイン」の略。同コンソーシアムの公式サイトは、<https://soundud.org/>

** 2018 年 4 月より提供を予定している支援ツールは、同社 HP 参照

<CSR>

OEESG と無形資産投資に関する初めての体系的な手引きと政策提言、「伊藤レポート 2.0」を経済産業省が公表

(参考情報：2017 年 10 月 26 日付 経済産業省 HP)

経済産業省「持続的成長に向けた長期投資（ESG・無形資産投資）研究会」は 26 日、企業の無形資産などへの投資を促す報告書「伊藤レポート 2.0」を公表した。報告書では「競争力の源泉として無形資産に対する戦略投資の重要性が高まっている」と強調。一方、日本企業は人材や研究開発など無形資産への投資が欧米に比べて見劣りしていると指摘した。その上で企業が持続的な価値創造に向けた経営のあり方を見直し、投資家と対話するための「ガイダンス（価値協創ガイダンス）」を提案した。その背景・概要は以下のとおり。

1. 背景

企業が「稼ぐ力」を高めて持続的に企業価値を向上させ、そのような企業への投資が中長期的に収益を生み出す循環構造を生むことが重要であり、2014 年に発表した「伊藤レポート」は、資本生産性を高めるための日本型 ROE 経営や企業と投資家の対話促進に向けた政策提言を行った。

今後の課題は、長期投資が収益をもたらす循環を定着させること。同研究会では、伊藤レポート後に生じた動きを総括しつつ、無形資産投資や ESG 等を巡る論点を深掘りして議論し、今後の政策対応等を検討した成果を「伊藤レポート 2.0」としてまとめた。

2. 「伊藤レポート 2.0」の内容（ポイント）

- 第四次産業革命が企業の競争のあり方を大きく変化させ、無形資産に対する戦略投資の重要性が高まっている。他方、グローバル企業の投資額の増大に対し、日本企業の研究開発投資の伸びが鈍化しており、人材投資の水準も低い。
- ESG については投資家の間で長期リスク要因として見るコンセンサスが存在するが、投資収益への影響には見解に違いがある。
- 日本企業の ROE が改善する一方、欧米と比べて事業の収益性や資本政策に違いがある。日本企業の PBR（株価純資産倍率）が長年にわたり 1 倍前後で推移しており、業種・資産構成等ごとに欧米と比較しても極めて低い水準にある。
- このような課題認識を踏まえ、企業が持続的な価値創造に向けた経営のあり方を見直し、そのビジネスモデルや戦略、ガバナンス等を投資家等と対話するための「ガイダンス（価値協創ガイダンス）」を提案。ガイダンスの各要素についての考え方や議論を整理し、その活用も含め以下の 8 項目の提言を行った。

- (1) 企業と投資家の共通言語としての「価値協創ガイダンス」策定
- (2) 企業の統合的な情報開示と投資家との対話を促進するプラットフォームの設立
- (3) 機関投資家の投資判断、スチュワードシップ活動におけるガイダンス活用の推進
- (4) 開示・対話環境の整備

- (5) 資本市場における非財務情報データベースの充実とアクセス向上取り組み
- (6) 政策や企業戦略、投資判断の基礎となる無形資産等に関する調査・統計、研究の充実
- (7) 企業価値を高める無形資産（人的資本、研究開発、IT・ソフトウェア等）への投資促進のためのインセンティブ設計
- (8) 持続的な企業価値向上に向けた課題の継続的な検討

3. 今後の展開

今後、経済産業省は同ガイダンスをベースとして、企業のベストプラクティス研究やモデル事業の実施、投資家における開示等の評価を調査・検討する場を立ち上げる予定。

これに合わせ、本年から東京証券取引所の「企業価値向上表彰」や国際機関の統合報告優良企業表彰の審査に「価値協創ガイダンス」が組み込まれる。また、証券リサーチセンターのプロジェクトとして、特に証券アナリストがカバーしていない有望な新興企業等について、価値協創ガイダンスをベースとしたアナリスト・レポートが順次執筆・公表される。

* <http://www.meti.go.jp/press/2017/10/20171026001/20171026001.html>

海外トピックス：2017 年 10 月に公開された海外の CSR・ERM 等に関する主な動向をご紹介します。

<人権>

○英国内務省が英国現代奴隷法の実践ガイドの改訂版を公表

(参考情報：2017 年 10 月 4 日付 同省 HP)

英国内務省は、10 月 4 日、英国現代奴隷法（2015 年制定）に基づき発行されている、企業およびサプライチェーンにおける奴隷労働や人身取引の防止に向けたガイダンスの改訂版を公表した。

これは、2015 年の制定以来、「奴隷と人身取引に関する声明（ステートメント）」の報告対象となっている企業*で取り組んできた内容に鑑み、より一層の取り組みの深耕を期したものの。

具体的な改訂の主なポイントは、以下の通り。

- ・同法のもとで報告が義務化されていない売上高 3,600 万ポンド未満の企業に対しても、自発的に「奴隷と人身取引に関する声明（ステートメント）」を発行することを推奨。
- ・児童労働の定義について、国際労働機関（ILO）の定義をもとに「12 歳未満の児童によるあらゆる経済活動および 12 歳から 14 歳の児童による軽作業を超える仕事、その他最悪の形態の児童労働**」と明確化。
- ・サプライチェーンにおける人権取り組みの透明性の確保や人権に関するデューデリジェンスの実施などの項目につき、これまでよりも強調した表現を使用し、企業への要望を強化。

* 対象となる企業は、会計年度ごとに「奴隷と人身取引に関する声明（ステートメント）」を発行すること。なお、本ステートメントには取締役会の承認および担当役員の署名があること、当該企業のウェブサイトトップページに目立つようにリンクを貼ること、などが求められている。

** 最悪の形態の児童労働とは

ILO の 182 号条約（1999 年）によって定められている以下の事項。なお、SDGs では 18 歳未満の児童によるこれら最悪の形態の児童労働を 2025 年までに撲滅することを目指している。

- ① 人身売買、徴兵を含む強制労働、債務労働などの奴隷労働
- ② 売春、ポルノ製造、わいせつな演技に使用、斡旋、提供
- ③ 薬物の生産・取引など不正な活動に使用、斡旋、提供
- ④ 児童の健康、安全、道徳を害するおそれのある労働

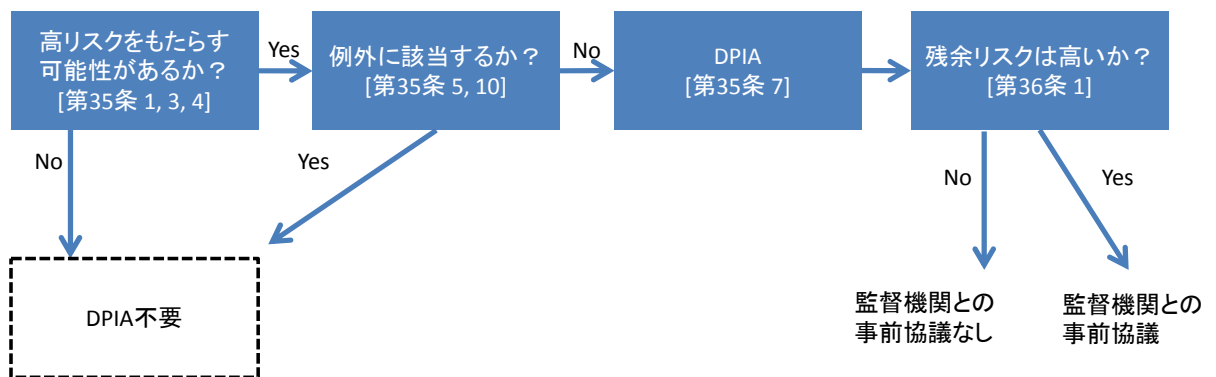
<情報セキュリティ>

○EU の第 29 条作業部会がデータ保護影響評価に関するガイドラインを採択

(参考情報：2017 年 10 月 4 日付 欧州委員会・第 29 条作業部会 HP)

EU の「第 29 条作業部会」*は 10 月 4 日、「データ保護影響評価（Data Protection Impact Assessment＝DPIA）およびデータ処理が“高リスクをもたらす可能性があるか”の判断に関するガイドライン」を採択した。

2018 年 5 月 25 日より適用開始となる一般データ保護規則（GDPR**）の第 35 条において、データ処理が自然人の権利・自由に高いリスクをもたらす可能性がある場合に、処理に先立ちデータ保護影響評価を実施しなければならないと定められている（下図参照）。データ保護影響評価では、当該データ処理がもたらすデータ主体の権利および自由に関するリスクを評価するのみならず、当該リスクを許容可能なレベルにまで低減するための対策を特定することもあわせて求められている。事前協議の要請を受けた監督機関は、データの取り扱いが GDPR に違反すると考える場合、データ取り扱いの禁止処分など、GDPR 第 58 条で定めるあらゆる権限を行使できる。



【出典】 DPIA ガイドラインを基にインターリスク総研にて作成

本ガイドラインは、データ処理に対しデータ保護影響評価を実施する必要があるかの判断基準およびデータ保護影響評価の実施方法等について整理したもの。本ガイドラインの構成は以下のとおり。

- I. はじめに
- II. ガイドラインの目的
- III. データ保護影響評価：規則の解説
 - A. データ保護影響評価の対象
 - B. データ保護影響評価の対象となる処理業務
 - a) 実施が義務的となる処理業務
 - b) 実施を要求されない処理業務
 - C. 既存の処理業務の取り扱い
 - D. データ保護影響評価の実施方法
 - a) 実施時期
 - b) 実施責任者
 - c) 実施手法・基準
 - d) データ保護影響評価の公表の必要性
 - E. 監督機関との事前協議が求められるケース
- IV. 結論および推奨事項

附属書類 1 - EU における既存のデータ保護影響評価に関するフレームワークの例

附属書類 2 - データ保護影響評価が GDPR の規定に適合しているかの判断基準

* 第 29 条作業部会

EU データ保護指令第 29 条によって設置された個人データの取り扱いにかかる個人の保護に関する助言機関。EU 加盟各国のデータ保護監督機関の代表、欧州データ保護監督官（EDPS）の代表等によって構成される。

** EU 一般データ保護規則（General Data Protection Regulation : GDPR）

EU を含む欧州経済領域（EEA）域内で取得した「氏名」や「クレジットカード番号」などの個人データを EEA 域外に移転することを原則禁止するもので、EEA 域内に現地法人・支店・駐在員事務所を置くすべての企業・団体・機関が適用対象となる。2016 年 5 月 24 日に発効し、2018 年 5 月 25 日に施行予定。

<気候変動>

OCDP が社内炭素価格に関するレポートを発表

(参考情報：2017 年 10 月 12 日付 CDP プレスリリース)

企業の気候変動情報開示を推進する国際 NGO の CDP は、10 月 12 日に社内炭素価格に関するレポート”Putting a price on carbon～Integrating climate risk into business planning～”を発表した。同レポートは、2017 年の CDP 気候変動プログラム、サプライチェーンプログラムにおいて世界の 6,086 社の企業から報告されたデータに基づき、世界の企業における社内炭素価格の現状について整理したものである。

社内炭素価格とは、企業が自社の事業における CO2 排出に対して、内部で仮想的な価格を設定する仕組みである。気候変動に伴い、炭素税*や排出権取引制度**の導入などの低炭素化に向けた政策の変動が想定される中で、企業におけるリスクマネジメントおよび機会の把握に役立つ手段として広まりつつある。

同レポートによれば、2014 年の世界における社内炭素価格の導入企業が 150 社だったのに対し、2017 年には導入企業が 607 社、今後 2 年以内に導入を検討している企業が 782 社の計 1,389 社と、この 4 年間で導入企業が大幅に増加している。日本国内における導入企業数も、2016 年の 104 社から 2017 年に 129 社へと増加した。また、CDP は同レポートの中で、投資家はその投資判断において、企業の意思決定に炭素価格が組み込まれているかをますます重視するようになっていることを指摘し、次回の CDP 質問票において炭素価格に関する質問を拡充することを明らかにしている。

* 炭素税

経済活動に伴い排出する温室効果ガスの量に応じて税金を課す仕組み。

** 排出権取引制度

あらかじめ各企業・国などに対して温室効果ガスの排出権を排出枠という形で定めておき、排出枠を超過して排出する主体と排出枠を下回る主体との間で権利の売買を可能とすることで、全体の排出量をコントロールする制度。

Q&A：CSR・ERM等に関するさまざまなご質問についての解説を行うコーナーです。



Question

近年、「森林破壊ゼロ方針」を公表する企業が増えていると聞いています。森林破壊ゼロ方針が拡大している背景を教えてください。

Answer

1. 森林破壊ゼロの考え方

コモディティ（パーム油、大豆、牛肉、木材・紙など）生産のためのプランテーション開発に起因して、東南アジア、南米、アフリカなどの地域で森林破壊が問題になっています。森林破壊により生物多様性が失われるとともに、炭素蓄積量の高い泥炭地や密度の高い森林が開発されることで、大量の温室効果ガス（GHG）が排出されることから、重要な環境問題となっています。コモディティ生産を直接行っていない企業も、原材料調達を通じて間接的に森林破壊に関わっており、NGO などから追及される事例が増えています。

そのため近年では、企業が自主的に「森林破壊ゼロ方針」を策定し、原材料調達における取り組みを強化する例が増えてきました。一般的に「森林破壊ゼロ方針」には、以下の項目を含みます。

- ① 泥炭の深さに関わらず泥炭地における伐採をしないこと
- ② 森林伐採のための火の使用を禁止すること
- ③ 高保護価値（HCV）地域における伐採をしないこと
- ④ 高炭素蓄積（HCS）地域における伐採をしないこと
- ⑤ 先住民族の有する土地の権利を尊重すること
- ⑥ 地域コミュニティから「自由意思による、事前の、十分な情報に基づく合意（FPIC）」を得ること
- ⑦ 法的に認められた土地のみで生産すること
- ⑧ 強制労働、奴隷労働を禁止すること

2. 森林破壊ゼロをめぐる経緯

（1）草創期

2008年の生物多様性条約第9回締約国会議（CBD-COP9）において、国際環境NGOの世界自然保護基金（WWF）がZero Net Deforestation by 2020（2020年までに森林破壊をネットゼロ）宣言への署名を呼びかけ、67か国の賛同を得ました。

それを受けて、2010年には世界の消費財メーカーや小売業約400社が加盟するコンシューマー・グッズ・フォーラム（TCGF）の理事会が、2020年までに森林破壊をネットでゼロにすることを決議しました。決議では熱帯林の破壊につながるパーム油、大豆、牛肉、紙などのコモディティの調達を責任ある形で行うことを目標とし、TCGFはそれぞれの資源について調達ガイドラインを整備するなどの取り組みを積極的に進めています。

2011年にはシンガポールの大手パーム油企業であるGolden Agri-Resources（GAR）が国際環境NGOとともに、新しい森林保護方針を発表しました。この森林保護方針は、HCV・HCS地域および泥炭地の開発禁止、FPICの順守などを掲げており、その後、各社が森林破壊ゼロ方針を策定する際にこれらの項目が踏襲されるようになりました。

(2) 普及期

2013年から14年にかけて、Greenpeaceによる”Tiger Challenge”キャンペーンなどにより、NGOは企業が森林破壊ゼロのコミットメントを行うことを強く求めるようになります。一部のNGOは企業の森林破壊ゼロへの対応状況をレーティングし、特定企業のサプライチェーンを調査して、森林破壊に関与していると告発しました。

2014年9月には国連気候サミットにおいて「森林に関するニューヨーク宣言（NYDF）」が採択され、当時、日本を含む56の国と地域、53の企業、16の先住民族団体、54のNGOが署名しました。この段階で、ウィルマー、GAR、カーギルなどのトレーダー（全世界のパーム油貿易量の約60%を占める）が森林破壊ゼロ方針を掲げるに至りました。また花王、ケロッグ、ジェネラルミルズ、ジョンソン&ジョンソン、ダノン、ハーシーズ、ペプシコ、マース、ユニリーバ、ロレアルなどの製造業も森林破壊ゼロのコミットメントを行いました。

3. 現状

このような流れを受けて、近年、森林破壊ゼロのコミットメントを行う企業は急増しています。Supply Change*の2017年の報告**によれば、調査対象とした718社のうちコミットメントを行った企業は447社に上ります。また最近ではミシュランタイヤやGMがタイヤに使用する天然ゴムについて森林破壊ゼロを目指すと表明するなど、4大コモディティ（パーム油、大豆、牛肉、木材・紙）を越えて取り組みが広がりつつあります。

ESG投資の拡大と合わせて、機関投資家の森林破壊に対する関心も高まっています。CDPフォレストプログラムは、365の機関投資家（運用資産総額22兆ドル）を代表して、企業に対して森林減少や劣化に関する質問書を送付し、評価する枠組みです。質問内容には森林破壊ゼロ方針に関する項目もあります。他にも森林破壊リスクが高いコモディティを調達する企業を選定し、格付けする”Forest 500”プログラムが2015年に開始されました。欧米ではForest 500の企業に対して、森林破壊に関する株主提案が行われる事例もあり、その数は2011年から2017年半ばまでの間に50件にも上っています***。

4. おわりに

まだ原材料調達に関して取り組みを開始していない企業は、まず環境や人権の観点からリスクが大きい原材料を使用していないか調査することが推奨されます。リスクが大きい原材料を使用している場合、トレーサビリティの確立、原材料の合法性確認、持続可能性認証を受けた原材料の使用などの取り組みを進めることが求められます。そして、一定段階まで取り組みが進んだ先進企業は、森林破壊ゼロのコミットメントやそれを実現するための取り組みまで踏み込むことが期待されています。

* 米国の環境NGOであるForest Trendが主導するイニシアチブで、コモディティ由来の森林破壊に関する企業のコミットメントなどの情報を追跡、開示している。CDPや世界自然保護基金（WWF）とも連携している。

** “Tracking Corporate Commitments to Deforestation-Free Supply Chains” (Supply Change / 2017)

*** “Investor concern for forests” (Global Canopy Programme, Forest 500 / 2017)

以上

株式会社インターリスク総研は、MS&AD インシュアランスグループに属するリスクマネジメント専門のコンサルティング会社です。CSR（企業の社会的責任）・ERM（全社リスク管理）等に関するコンサルティング・セミナー等のサービスを提供しています。

弊社サービスに関するお問い合わせ・お申込み等は、下記のお問い合わせ先、または、お近くの三井住友海上、あいおいニッセイ同和損保の各社営業担当までお気軽にお寄せ下さい。

お問い合わせ先

㈱インターリスク総研 リスクマネジメント第三部

TEL.03-5296-8912（危機管理・コンプライアンスグループ）

TEL.03-5296-8913（環境・CSRグループ）

TEL.03-5296-8914（統合リスクマネジメントグループ）

<http://www.irric.co.jp/>

主な担当領域は以下の通りです。

＜危機管理・コンプライアンスグループ＞

- ◆ 危機管理・海外危機管理
- ◆ コンプライアンス（法令遵守）
- ◆ 役員賠償責任（D&O）
- ◆ CS・苦情対応
- ◆ 製品安全・食品安全

＜環境・CSRグループ＞

- ◆ 環境経営（環境リスク・ブランディング）
- ◆ 環境マネジメントシステム（ISO14001等）
- ◆ 生物多様性
- ◆ エネルギー（再エネ・省エネ）
- ◆ 社会リスク（環境デューデリジェンス・人権リスク等）

＜統合リスクマネジメントグループ＞

- ◆ ERM（全社リスク管理）
 - ・リスクマネジメント体制構築
 - ・企業リスク分析・評価（リスクアセスメント）
- ◆ 情報漏洩リスク

本誌は、マスコミ報道など公開されている情報に基づいて作成しております。

また、本誌は、読者の方々に対して企業のCSR・リスクマネジメント活動等に役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。

不許複製／Copyright 株式会社インターリスク総研 2017