東京海上ディーアール株式会社
海外リスクセンサー
配信時刻：2025 年 1 月 10 日 9:00
※情報は 2024 年 12 月 13 日 20:00 時点のもの

海外現地法人をとりまくサイバーリスクとその対策

対象地域

東南アジア・大洋州	✔	米州（含む中・南米）	✔	中東・アフリカ	✔
東アジア・南アジア	✔	欧州	✔	その他の地域および世界	✔

レポート要旨

- 近年、海外現地法人を介して本社等の他拠点に被害が拡大するサイバー攻撃被害が多発している。
- セキュリティ対策においては、同一の情報資産にアクセスできる場合は、全ての拠点において同一水準のセキュリティ対策の実施が求められる。
- 海外現地法人のセキュリティ対策を推進していくためには、各拠点のセキュリティ対策状況の把握と、本社が求める水準とのギャップ分析を行うことが必要となる。
- 現状把握やギャップ分析を行うための手法には様々なものがあるが、本稿では三種類の管理手法（調査票、セキュリティ監査、リスク評価サービス）を紹介し、特にセキュリティリスクレイティングサービスについて詳細を解説した。
- 結論として、セキュリティリスクレイティングサービスを含め、各管理手法にはメリットとデメリットがあるため、各管理手法の特徴を理解したうえで、それらを組み合わせて実施することが推奨される。海外現地法人を持つ本社においては、セキュリティ対策を現地任せにするのではなく、本社による海外現地法人のセキュリティリスクの可視化と、求められるセキュリティ水準に到達できるような積極的な支援が求められる。

レポート構成

1．海外現地法人で発生したサイバー攻撃被害

2020 年 1 月、大手製造業の A 社は不正アクセスによる情報漏えい被害について公表した。同社のプレスリリースによると、当初、漏えい対象のデータは採用応募者の個人情報および A 社の技術資料、営業資料であり、重要な社会インフラに関わる情報の漏えいは発生していないとされていた。しかし、そのおよそ 3 週間後に同社が公表した続報および防衛省の発表によると、漏えいした恐れのある情報に防衛装備品に関する「注意情報」が含まれていたことが判明した。本事案はサイバー攻撃によって日本の安全保障に影響を及ぼしかねない非常に重大なインシデントであるが、本事案の初期侵入は A 社本体に対してではなく、中国に所在する同社の海外現地法人のネットワークに対して行われていたことが後に明らかになっている。

上記のインシデント以降も、日系企業の海外現地法人におけるサイバー攻撃被害は多数発生している。【図表 1】は、2024 年に日系企業の海外現地法人で発生したサイバー攻撃被害を各社のプレスリリースに基づき一覧化したものである。

【図表 1：2024 年に日系企業の海外現地法人で発生したサイバー攻撃被害】

事案公表月	業種	海外現法所在地	事象	他拠点への影響拡大の有無
2024年12月	製造業	インドネシア	ランサムウェア	不明
2024年10月	卸売業	非公表	不正アクセス	不明
2024年9月	卸売業	タイ	ランサムウェア	有
2024年9月	運輸通信業	シンガポール	情報漏えい	無
2024年8月	製造業	ベトナム	情報漏えい	無
2024年8月	製造業	アメリカ	ランサムウェア 情報漏えい	無
2024年7月	製造業	中国	ランサムウェア	無
2024年6月	運輸通信業	ベトナム	情報漏えい	不明
2024年6月	運輸通信業	香港	不正アクセス	無
2024年2月	製造業	アメリカ	ドメイン窃取	無

出典：各社のプレスリリースを基に当社作成

注 1：他拠点への影響拡大の有無については、リリース内で言及の無いものを「不明」としている。

注 2：他拠点への影響拡大の有無の基準は、本稿執筆時点での公表情報に基づく。

サイバー攻撃の被害が海外現地法人に留まる局地的な被害の事例も多い一方、A 社のインシデントと同様に、その被害が本社をはじめ他の拠点にまで及んでしまっている事例も確認されている。2023 年以前でも、海外現地法人のネットワークを経由する形で、日本国内に保管されている個人情報や顧客情報、機密情報の漏えいが発生した事例は枚挙にいとまがない。海外現地法人におけるセキュリティ対策の不備が、本社を始め自組織のグローバルな全ての拠点に影響を及ぼす重大なリスクとなり得る。対岸の火事では決して済まされない。

2．同一の資産には同一水準のセキュリティ対策が必要

セキュリティ対策においては、「桶の理論」または「the strength of a chain is in the weakest link（鎖の強度は最も弱い環で決まる）」 という言葉がよく用いられる[1]。桶に水を張った際に、桶の縁の高さがバラバラだとしたら、最も低い縁から水がこぼれるというイメージである。桶の縁の高さをセキュリティレベル、桶の中の水を守りたい情報資産と仮定すると、セキュリティレベルの低い箇所が一か所でもあった場合、その情報資産に対する保護のレベルは最も低い水準のものになってしまう。この言葉が示す重要なポイントは、同一の情報資産に対しては、全ての拠点において同一水準のセキュリティ方針（ポリシー）とそれに基づく対策が求められるという点である。「本社のみ対策ができている…」「一部の拠点のみ対策ができている…」という声をよく耳にするが、全ての拠点において同一水準の対策が施されていないと、その効果は大幅に減退することとなる。このことは、海外現地法人においても同様である。海外現地法人のネットワークを経由して、他の拠点の情報資産へアクセスが可能な場合、海外現地法人を含めて同一水準のセキュリティ対策が必要となる。

同一の情報資産に対して、同一のセキュリティ水準を提供するためには、セキュリティ対策を統括する本社もしくは地域統括会社など[2]が以下二点を行うことが重要となる。その二点とは、①各拠点のセキュリティ対策の現状を正確に把握すること、②各拠点に対して求められるセキュリティ対策の水準を明確に示すこと、である。しかしながら、殊に海外現地法人に関しては、これらの対応が適切に行えていない組織が散見される。KPMG コンサルティング株式会社（以降 KPMG コンサルティング）が 2024 年 2 月に公表したアンケート結果によると、回答企業の 39.1%が海外子会社のセキュリティ対策の取り組みを把握していないと回答している[3]。また、同調査によると、回答企業の半数以上において、本社が海外現地法人における情報セキュリティ対策に対して積極的な関与を行っていないことが明らかになっている[4]。このような状況においては、本社による自組織のセキュリティリスクの把握も困難になるだけでなく、海外現地法人の立場から見てもどのようなセキュリティ対策をどの水準まで行うべきなのか判断に苦慮することになる。結果として、拠点間でセキュリティ対策に不整合が生じてしまい、前述の様なインシデントの誘因となり得る。

上記の様な①本社による各拠点のセキュリティ対策の現状把握と、②本社から各拠点に対して求められるセキュリティ対策水準の明示化を行うためには、本社と各拠点間が密なコミュニケーションを行うことが求められる。海外現地法人の場合、地理的、言語的な制約もあり、円滑なコミュニケーションを行うことの難易度が高いため、そのための工夫が必要となる。

---

[1] 株式会社日経 BP「情報セキュリティ・マネジメントと ISMS」2007 年 5 月 30 日
[2] 海外現地法人に対して、これらの拠点のセキュリティ対策を統括する組織を、以降本稿では一括して「本社」と呼称する。
[3] KPMG コンサルティング株式会社「サイバーセキュリティサーベイ 2023」2024 年 2 月 26 日
[4] KPMG コンサルティング株式会社「サイバーセキュリティサーベイ 2023」2024 年 2 月 26 日

3．海外現地法人に対する管理手法の比較

海外現地法人のセキュリティ対策の向上に向けたコミュニケーションを行うため、各企業は様々な手法を用いている。先述の KPMG コンサルティングの調査によると、海外子会社のセキュリティ対策状況の把握のために用いられる代表的な手法として、①調査票（43.4%）、②海外子会社の監査（19.9%）、③外部のリスク評価サービス（8.0%）が挙げられている[5]。本章では、それぞれの調査手法のメリット、デメリットを比較していきたい。

(1) 調査票

調査票は、チェックシートを用いてセキュリティ対策の実施状況を各拠点の担当者に回答させるものである。現状把握に役立つだけでなく、チェックシート記載の各チェック項目が求められるセキュリティ対策であるため、本社が求めるセキュリティ対策の水準を明示する役割も兼ねていることが多い。調査票を用いた現状把握のメリットは、その手軽さにあるだろう。Microsoft Excel などでチェックシートを作成し、各拠点の担当者へメールで配布すれば、追加のコストなどを生じさせずに複数拠点に対する現状把握が可能となり、定期的な実施にも適している。ゆえに、先述の KPMG コンサルティングの調査においても、最も多くの割合で利用されていた手法となっている。

一方、調査票を用いた現状把握のデメリットとしては、回答の客観的な裏付けを得ることが難しい点が挙げられる。チェックシートによる回答は担当者のセルフチェックで行われることが多く、本社が期待する様な対策が実際に行われているのかをモニタリングすることができない。また、チェック項目の内容が曖昧な場合は、回答結果に担当者によってバラつきが生じる可能性もある。調査票を用いた現状把握は、手軽に実施できるメリットはあるものの、その回答内容に信憑性が乏しいところがあり、結果として現状把握プロセスが形骸化する可能性がある。

(2) セキュリティ監査

二つ目に紹介する実態把握の手法として、本社によるセキュリティ監査が挙げられる[6]。調査票による現状把握がセルフチェック方式であったのに対して、セキュリティ監査の場合は本社メンバーが現地を訪問するなどして、対策の実施状況をモニタリングし、改善点が見つかった場合には是正措置を提言する。セルフチェック方式では回答内容の信憑性に課題が残る一方、監査の場合はより正確に現状を把握することができることがメリットとして考えられる。また、調査票による現状把握と比較して、実際に本社メンバーが訪問し監査を行うことによって、本社メンバーと海外現地法人の現場メンバーが直接コミュニケーションをとることができることも、セキュリティ監査のメリットとして挙げられる。本社側のメリットとしては、対策が必要な理由やその基礎となる考え方などを現場メンバーに伝達することができ、現地法人のガバナンス強化につなげることができる。また、海外現地法人側のメリットとしては、セキュリティ対策を行ううえで現場が感じた課題や問題点などを本社メンバーに共有することが可能となる。

---

[5] KPMG コンサルティング株式会社「サイバーセキュリティサーベイ 2023」2024 年 2 月 26 日
[6] 本来、監査には是正型監査や外部機関による保証型監査など様々な手法があるが、本稿では本社（自組織）による是正型の監査を想定している。

一方、セキュリティ監査のデメリットとしてリソースとコストの問題がある。本社メンバーが各拠点を訪問し現状把握を行う場合、全ての拠点に対してセキュリティ監査を行うことは現実的ではなく、監査対象を限定する必要がある。また、海外現地法人としても、監査対応によって通常業務に支障をきたす可能性もある。そのため、高い頻度で同一拠点に対する監査を行うことは困難となる。したがって、過去に実施した監査結果と現状との間に乖離が生じている可能性があり、リアルタイムで各拠点の現状を把握することには適していない。

(3) リスク評価サービス

三つ目に紹介する現状把握の手法は、セキュリティベンダーが提供している脆弱性診断やセキュリティリスクレイティングサービス（以降レイティングサービス）を利用し、技術的に海外現地法人のセキュリティ対策状況を把握する方法である。脆弱性診断では、診断対象のサーバやネットワーク機器に対して脆弱性や設定不備がないかを網羅的に診断することができる。その反面、診断を行うためにサーバやネットワークの内部に侵入し詳細な調査を行うため、診断対象は自組織で保有する情報資産に限定されることに加え、診断時に診断環境に影響を及ぼす可能性がある。したがって、事前に診断対象やスコープを適切に設定し、影響を最小限に抑制するための事前調整が求められる。一方のレイティングサービスとは、インターネット上に公開されているオープンソースの情報などを自動で収集し、外部からセキュリティリスクを評価するサービスのことである。レイティングサービスは、あくまで外部から公開情報に基づいて評価を行うため、対象のネットワーク内部までを診断する脆弱性診断に比べ評価可能な項目が表層的なものに留まるものの、対象システムに影響を与えることなく外部から評価を行うことが可能となる。

脆弱性診断やレイティングサービスによって海外現地法人の現状把握を行うメリットとして、技術的な裏付けを得ることが可能であるという点が挙げられる。調査票やセキュリティ監査においては、主に海外現地法人の現場メンバーからの回答が現状把握のエビデンスとなることが多いが、脆弱性診断やレイティングサービスはサーバやネットワーク機器の設定情報を参照するため、客観的にセキュリティリスクを評価することが可能である。また、レイティングサービスの場合、評価対象のリスクを常時監視可能なサービスが多いため、リアルタイム性に優れた手法でもある。

これらのサービスを利用する際のデメリットとしては、コストの問題が挙げられる。これらのサービスを利用する場合は、セキュリティベンダー等からサービスやツールのライセンスを購入する必要がある。いずれも診断対象数に応じて従量課金する料金設計であることが多いため、予算などに応じて診断対象を限定する必要が生じる場合がある。また、コストの問題に加えて、診断結果に対するフィードバックの難しさという課題もある。本社で海外現地法人のセキュリティ対策の不備を発見し指摘したとして、海外現地法人のリソースや能力不足などの問題により、対応の優先順位付けや具体的な対策の実施に苦慮することが想定される。

これまで、海外現地法人の現状把握の手法として、代表的な三つの手法を紹介してきた。【図表2】にて概要を整理した通り、いずれの手法にもメリットとデメリットがあり、一概にどの手法が優れていると述べることはできない。したがって、各拠点に求められるセキュリティ対策の水準と、自組織のリソース、予算などを考慮しつつ、これらの手法を組み合わせて実施することが望

ましい。次章では、取り組みの一例として、レイティングサービスをベースとしながら、セキュリティ監査や調査票での現状把握を併用する際に推奨される対応について紹介する。

【図表 2：セキュリティ対策の管理手法の概要】

手法	概要	メリット	デメリット
調査票	本社側が用意したチェックシートを配布し、各拠点の担当者に回答させる。	・コストを抑制し、手軽に実施することができる。 ・複数拠点に対して、同時に現状把握を行うことができる。	・セルフチェック方式となり、回答の裏付けがない。 ・設問項目によっては、回答者の主観によって回答内容にバラつきが生じる。
セキュリティ監査	本社メンバーが実際に海外現地法人へ来訪し、セキュリティ対策状況を評価する。	・本社メンバーが実際にセキュリティ対策状況を現地で確認することができる。 ・本社メンバーと海外現地法人メンバーとが直接コミュニケーションをとることができる。	・リソースとコストの関係上、監査の頻度に制約が生じる。 ・同一拠点に対する監査の頻度が広くなってしまうため、リアルタイムな現状把握には適していない。
リスク評価サービス	脆弱性診断やセキュリティリスクレイティングサービスなどを活用し、診断対象の脆弱性や設定不備の有無を技術的に評価する。	・サーバやネットワーク機器の設定情報などを確認できるため、客観的にリスクの把握ができる。 ・セキュリティリスクレイティングサービスの場合は、常時診断対象をモニタリング可能なサービスもあるため、リアルタイム性にも優れている。	・各種サービスやライセンス購入のコストが生じるため、予算によって診断対象を限定する必要がある。 ・海外現地法人側に人材やリソースが不足している場合、診断結果に対する対応に苦慮する可能性がある。

出典：当社作成

4．海外現地法人に対するセキュリティ対策

(1) レイティングサービスの特徴

以下では、レイティングサービスをベースとした海外現地法人のセキュリティ対策の現状把握について、その取り組みの推奨例について述べるが、その前段としてレイティングサービスの概要を紹介したい。レイティングサービスは各種ベンダーから様々なサービスが提供されているが、各サービスで共通している特徴として以下のものが挙げられる。①企業や組織が持つサイバーリスクのレベルを評価する、②評価した結果を数値やランクによって可視化する、③評価は対象ドメインに紐づく公開情報に基づき外部から対象システムに影響を与えることなく実施される、というものである[7]。③にて記載の通り、公開情報を基に外部から企業のセキュリティリスクを評価することが可能であるため、自組織だけでなく、他社も含めたリスク評価が可能であり、国内外の子会社・関連会社や、サプライチェーン上の企業、買収予定企業のリスク評価などに多く用いられている。

レイティングサービスの代表的なサービスである Security Scorecard 社が提供する Security Scorecard Ratings（以降 SSC）では、診断対象のドメインを入力するだけで、当該ドメインに対するセキュリティリスクの数値化と、検出されたリスクの確認が可能となる。【図表 3】は、SSC のレイティング手法である。最初のステップのデータ収集は SSC が多数の手段を用いて常時モニタリングを行い、既に 1,100 万ドメイン以上のデータを蓄積している。診断対象のドメインがこの SSC が事前に収集したデータに含まれている場合は、数秒～数十秒で即座に当該ドメインのセ

[7] サイバーセキュリティ.com「サイバーリスク・レーティング」を参照。

キュリティリスクのスコアリングが可能となる[8]。【図表 3】の通り、集計されたデータは、ステップ 3 に記載の 10 個のリスクカテゴリに分類され、カテゴリごとのスコアリングと、それらを統合した総合評価としてのスコアリングが行われる。スコアリングは 100 点満点の数値化に加え、A～F の 5 段階で定性的な評価も併せて行われる。

【図表 3：SSC のレイティング手法】

出典：東京海上ディーアール株式会社、「Security Scorecard」

(2) レイティングサービスを活用した海外現地法人のリスク管理

海外現地法人のセキュリティ対策を推進するのに際して、レイティングサービスを推奨する一番の理由として、セキュリティリスクの多寡をスコアで可視化できるという点が挙げられる。2．で述べた様に、海外現地法人のセキュリティ対策を組織として向上させていくためには、①各拠点のセキュリティ対策の現状を正確に把握すること、②各拠点に対してセキュリティ対策の求められる水準を明確に示すこと、の二点が重要となる。レイティングサービスのスコアリングを用いることで、①と②のいずれも部分的に実現することができる。まず①海外現地法人の現状把握についてだが、スコアという明示的な指標があることによって、セキュリティリスクの増減を可

[8] 診断対象のドメインが SSC のデータベースに登録がない場合は、最大 1 週間程度でスコアリングが可能となる。。

視化することができる。レイティングサービスの例として紹介した SSC の場合、評価対象のドメインを SSC のダッシュボード[9]に登録することによって、常時評価されたスコアの把握が可能となり、追加の設定を行うことでスコアに変動が生じた際にアラートを送付する機能も有している。スコアという明示的な指標があり、かつ最新のスコアを常時把握することができるため、本社が海外現地法人の現状把握を行うことが可能となる。

続いて②各拠点に対して求められるセキュリティ対策水準の明示化についてだが、こちらについてもスコアを用いることで、本社が期待する水準を明示することが可能となる。「今回のスコアは D ランクなので、〇月までに C を目指しましょう」という様に、スコアという指標を示すことで、本社と海外現地拠点との間で目指すべきセキュリティレベルの共通認識の形成が容易となる。また、スコアがあることによって、海外現地法人の現状を踏まえたうえで、ステップバイステップでの目標を設定することが可能となるだけでなく、対策した結果がスコアに反映されるため、海外現地法人のモチベーション向上にも寄与する。このように、レイティングサービスをコミュニケーションツールとして活用することによって、言語や地理的な隔たりがある本社と海外現地法人との密な連携が可能となる。なお、本社と海外現地法人とでコミュニケーションを行う際には、本社が一方的に対策の不備やスコアの低さを指摘するのではなく、本社側もスコア改善に向けた連携や伴走を行うことを示すことが重要となる。

これまで、レイティングサービスを活用した海外現地法人に対する取り組みを紹介したが、前章で述べた様に、レイティングサービスにも課題が存在する。以下では、レイティングサービスの課題の整理を行う。第一の課題として、評価可能な領域が限定的であるという点が挙げられる。前述の通り、レイティングサービスはドメインに紐づく公開情報を基に外部から診断を行うサービスであるため、非公開のものやドメインに紐づかない情報資産に対して評価を行うことができない。また、ツールを用いて自動的にドメイン情報と情報資産の紐づけを行うため、自組織のドメインに関係のない情報資産の情報が含まれる形でスコアリングが行われる可能性もある[10]。したがって、レイティングサービスを導入するだけで評価対象のリスクを全て可視化できるわけではない。第二の課題として、コスト面の課題が挙げられる。SSC の場合、常時スコアをモニタリングするドメイン数に応じた従量課金制となっている。国内外の全グループ企業に対するスコアリングを行うことが理想的ではあるものの、予算の関係上全ての拠点の評価が難しい場合は、評価対象を限定する必要がある。

(3) 各管理手法を組み合わせてセキュリティ対策を実現することが重要

レイティングサービスを用いることで海外現地法人のセキュリティリスクの可視化や、スコアを介したコミュニケーションの活性化が期待される一方、評価範囲やコスト面などの課題も存在する。３．では、海外現地法人のセキュリティリスクの管理手法として調査票、セキュリティ監査、レイティングサービスを含めたリスク評価サービスの三種類の手法を紹介した。レイティン

9 SSC はブラウザ経由で利用する SaaS サービスであり、ダッシュボードとは SSC で評価しているドメインとそのスコアを一覧化した画面のことである。
10 SSC では誤った情報がドメインに紐づいていたスコアリングが実施された場合、ドメインの所有者であれば紐づけの解除を SSC へ申請することができる。

グサービスを導入したからといって、調査票やセキュリティ監査が不要となるわけではない。むしろ、海外現地法人のセキュリティ対策の実効性を高めていくためには、これら全ての管理手法を組み合わせて実施することが推奨される。

先述の通り、レイティングサービスを全ての拠点に対して実施することが予算的に難しい場合は、その評価対象を限定する必要がある。そこで、調査票を用いる管理手法を併用することで、調査票を全拠点に対する現状把握の手法として運用し、アクセス可能な情報資産の水準や事業影響などを鑑み、重点拠点のみレイティングサービスによるスコアリングを行うことが、コストと実効性を考慮した際に推奨される。また、レイティングサービスの場合は評価項目が限定的であることが課題点として挙げられるが、レイティングサービスで評価できない項目を調査票で補うことも可能である。セキュリティ監査においても、レイティングサービスや調査票を用いる管理手法の課題点を補完することが可能である。調査票の回答の信憑性の確認や、レイティングサービスにて評価ができない項目については、実際に本社メンバーが現地に訪問し監査を行うことで、より正確な現状把握が可能となる。また、レイティングサービスによる遠隔でのスコアリングだけでなく、本社メンバーが現地を訪問し、海外現地法人の現場メンバーと直接対話できることもセキュリティ監査の実施のメリットと言える。ただし、２．で述べた様に、リソースやコストの関係から監査対象を限定する必要がある。したがって、調査票で全拠点に対する現状把握を行い、その内の重点拠点に対してはレイティングサービスを用いて常時スコアリングとスコアを介したギャップ分析やコミュニケーションを行い、特にスコアの低かった拠点や新規で設置した拠点などに対しては、セキュリティ監査として本社メンバーが直接訪問し、現状把握や現場とのコミュニケーションを行うことが最適解ではないかと考える。

このように各管理手法にはそれぞれメリットとデメリットがある。それぞれの管理手法の特徴を理解したうえで、適宜管理手法を組み合わせながら、海外現地法人のセキュリティ対策向上に取り組むことが望ましい。

５．まとめ

本稿では、海外現地法人のセキュリティ対策の向上に必要な施策として、本社による①各拠点のセキュリティ対策の現状を正確に把握すること、②各拠点に対して求められるセキュリティ対策の水準を明確に示すこと、の二点が重要となると述べた。その理由として、セキュリティ業界で頻繁に用いられる「桶の理論」を引用し、同一の資産に対しては全ての拠点で同一のセキュリティ方針とそれに基づく同水準のセキュリティ対策が求められることを解説した。しかしながら、本社が海外現地法人のセキュリティ対策を管理し統制することは言語や地理的な制約などもあり難易度が高い。そこで上記の求められる二つの施策を実現するために、調査票、セキュリティ監査、リスク評価サービスの三つの手法についてそれぞれのメリットとデメリットを比較しつつ紹介した。三つの手法の内、特にリスク評価サービスの一例であるレイティングサービスは、評価結果がスコアという明示的な指標で確認ができるため、海外現地法人のリスク変動の把握やコミュニケーションにおいて有用であることを述べた。ただし、いずれの手法にもメリットとデメリットがあるため、結論として、各サービスの特徴を理解したうえで適宜管理手法を組み合わせることが、最も合理的な対策になると考えられる。

本稿の冒頭でも述べた様に、海外現地法人にて発生したインシデントが、本社をはじめとする

他の拠点にまで被害が拡大する事案は多数発生している。海外現地法人のセキュリティリスクは、局所的なものではなく、グローバルに影響を及ぼす甚大なものになりかねない。セキュリティ対策を現地任せにするのではなく、「桶の縁の高さ」を揃えるためにも、本社による海外現地法人のセキュリティリスクの可視化と、求められるセキュリティ水準に到達できるような積極的な支援が求められる。

以上

本レポートに関する注意事項

1. 本レポートは、主に新聞等における報道内容や関連する企業や団体等のホームページ等を情報源として活用し作成しております。
2. お客様社内での利用に限ります。本情報をお客様から再配信することは固くお断り致します。
3. 本レポートは、日本国内でご利用いただくことを前提に作成しております。海外でのご利用には、主に以下の点において適していない場合があります。
   （1） 日本国内で一般的に得られる公開情報をもとに作成しているため、現地の実情とは異なる場合があります。
   （2） 宗教・政治・領土問題等、日本国内では問題がなくても、海外で発信した場合には問題を惹起する可能性があります。
4. 本レポートは、あくまでも情報提供として供するものであり、レポート内の情報（事実関係および分析・評価結果）をもとにしたお客様社内での判断等に東京海上ディーアール株式会社・東京海上日動火災保険株式会社・その他関係会社が責任を負うものではありません。

コンサルティングのご紹介

東京海上ディーアール株式会社 ビジネスリスク本部では、グローバルリスクマネジメント推進体制構築に関わるコンサルティングサービスをご提供しております。以下はコンサルティングの例です（以下に明示したコンサルティングに限定されません）。ぜひ、お気軽にお問合せください。

- ☐ リスクマネジメント体制構築
- ☐ リスクマネジメント・危機管理文書の第三者評価
- ☐ 海外事業拠点・事業展開国のリスク評価
- ☐ BCP・緊急時対応計画の策定（感染症・戦争・政変・テロ等を含む）
- ☐ 危機発生時のシミュレーション訓練・演習
- ☐ 地政学リスク・政治リスクのマネジメント、分析・調査、総合的なアドバイザリー　等

東京海上ディーアール株式会社
サイバーセキュリティ事業部　主任研究員　三宅　諒介（専門分野：サイバーセキュリティ）
〒100-0004 東京都千代田区大手町 1-5-1
大手町ファーストスクエア ウエストタワー23 階
Tel. 03-5288-6674
https://www.tokio-dr.jp/