2016.12.1

CSR・ERMトピックス ＜2016 No.9＞

CSR・ERM トピックスは、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（「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）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。

国内トピックス：2016 年 10~11 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。

＜労働慣行＞

○厚生労働省が「過労死等防止対策白書」を公表

（参考情報：2016 年 10 月 7 日付　同省 HP）

厚生労働省は 10 月 7 日、過労死等の現状や防止施策の状況を取りまとめた「過労死等防止対策白書」を公表した。

本白書は、平成 26 年に成立・施行された過労死等防止対策推進法の第 6 条に基づいて国会に毎年報告を行う年次報告書であり、今回初の公表となる。

政府は、過労死等の防止に向けた対策を効果的に推進するため、昨年「過労死等の防止のための対策に関する大綱」を定めて下表の目標を掲げており、本白書では、それらに関連する過労死等の現状や推移をグラフ等のデータとともに掲載しているほか、政府の施策の実施状況、コラム形式の民間団体の取組紹介、関連法令・指針等の資料が一冊にまとめられている。

「過労死等の防止のための対策に関する大綱」の目標値に対する現状

項目	「過労死等の防止のための対策に関する大綱」の定める目標	本白書で示された現状	
		最新数値	データ推移の傾向
週労働時間 60 時間以上の雇用者の割合	5%以下（平成 32 年まで）	8.2%（平成 27 年）	平成 15、16 年（12.2%）をピークとして概ね緩やかに減少
年次有給休暇取得率	70%以上（平成 32 年まで）	47.6%（平成 26 年）	年次有給休暇の付与日数は長期的に微増
メンタルヘルス対策に取り組む事業場の割合	80%以上（平成 29 年まで）	60.7%（平成 25 年）	平成 14 年（23.5%）以降増加の傾向

出典：「平成 28 年版 過労死等防止対策白書（概要）」を基にインターリスク総研にて作成

本白書によると、労働者一人あたりの「年間総労働時間」は減少傾向となっているものの、パートタイム労働者比率の増加が要因だと考えられ、パートタイム労働者を除いた「一般労働者の年間総実労働時間」は、2,000 時間前後で高止まりしているとともに、「勤務問題を原因・動機の 1 つとする自殺者数」は平成 23 年をピークに減少傾向ではあるものの、9 年間連続（平成 19 年～27 年）年間 2,100 名を超す数で推移している。また、「精神障害に係る労災請求件数・支給決定件数」や「いじめ・嫌がらせの相談件数」については増加傾向にある。

＜CG＞

〇ISS が 2017 年版の議決権行使助言方針案を発表

（参考情報：2016 年 10 月 27 日付 同社 HP）

議決権行使助言会社の ISS（Institutional Shareholder Services Inc.）は 10 月 27 日、各国の投資家が議決権を行使するにあたっての助言に関する 2017 年度の方針案を公表した。

同方針案で ISS は、株主総会において相談役・顧問制度の新設議案に反対を推奨し、2017 年 2 月開催の株主総会より適用する、としている。

ISS は、日本では役員を退任した後も、同人が相談役・顧問として会社に残留し、影響力を行使する例が多い点を問題視している。このため、今後の株主総会において相談役・顧問制度を新たに定款に規定しようとする場合、その定款変更に反対を推奨する。一方、「取締役相談役」など、取締役・顧問を取締役の役職として規定する場合、株主はその取締役の選任議案に対して反対票を投じることができるため、定款変更議案には反対推奨しないとしている。

なお、ISS は社外取締役が監査役を兼ねる「監査等委員会設置会社」について、4 人以上の社外取締役を求める案も検討していたが、今回の助言案では見送られている。

海外トピックス：2016 年 9~11 月に公開された海外の CSR･ERM に関する主な動向をご紹介します。

＜生物多様性＞

〇世界自然保護会議において、象牙取引の全面禁止や海洋生物多様性保護などを決議

（参考情報：2016 年 9 月 13 日付　環境省 HP）

国際自然保護連合（International Union for Conservation of Nature and Natural Resources、以下「IUCN*」）主催の第 6 回世界自然保護会議**が 9 月 1～10 日までホノルルで開催され、象牙取引の全面禁止や海洋生物の多様性保護などが決議された。

世界自然保護会議では、2017-2020 年の IUCN 活動計画として、2013-2016 年の計画を引き継ぎ、

①自然の尊重・保全
②効果的で公平な自然資源の管理の促進と支援
③気候、食糧、開発の問題に対する自然に由来する解決策の普及

の 3 つのプログラム分野を掲げ、持続可能な開発目標（SDGs）との関連性やその達成に向けた取組の実施に貢献することなどが承認された。

また、今次会合で以下のような動議が承認され、IUCN の事務局、国家、政府機関、NGO 会員などに対し、各動議に対する支援や対応が求められた。

・象牙の国内取引について合法的なものも含めて禁止するための制度整備や支援を求める
・私有地や共有地の自主的かつ長期にわたる保全、その生物多様性保全への貢献を求める
・海域の最低 30%を海洋保護区等の区域型保全措置として設計することを求める
・海洋・沿岸生態系は炭素吸収源として気候変動に大きな役割を果たすことを認識する
・企業が生物多様性に関する報告に取り組むこと、政府は、その促進のための仕組みを構築することを求める
・湿地における狩猟のための鉛弾使用の段階的廃止や代替弾使用を求める

* IUCN

International Union for Conservation of Nature の略で、1948 年に世界的な協力関係のもと設立された、国家、政府機関、非政府機関で構成される国際的な自然保護ネットワーク。

**世界自然保護会議

IUCN の 4 年に 1 度の会員総会と、世界自然保護フォーラムの 2 つで構成される。今次の会員総会には、IUCN を構成する会員や科学者など、192 か国から 1 万人以上が参加し、IUCN の活動計画の決定、役員選挙、動議の採択などが行われた。世界自然保護フォーラムでは、900 以上のワークショップ、イベントなどが開催された。

＜コンプライアンス＞

〇国際標準化機構が贈収賄防止のためのマネジメントシステムに関する初の国際規格「ISO37001」をリリース

（参考情報：2016 年 10 月 14 日付 国際標準化機構 HP）

国際標準化機構（International Organization for Standard　以下、「ISO」）は 10 月 14 日、贈収賄防止のためのマネジメントシステムに関する初の国際規格「ISO37001」をリリースした。

同規格が策定された背景として、近年、贈収賄が国、組織、個人にもたらすダメージの大きさが広く認識されてきたこと、多くの企業や機関が贈収賄防止のための仕組みづくりに多くの投資をしていることがある。同規格は、企業等の組織が、自社業務やバリューチェーン上において想定される贈収賄リスクの低減に活用することを目的として、贈収賄の行為主体が自社従業員かビジネスパートナーによるものかにかかわらず、贈収賄リスクを予防、発見、対処するためのマネジメントフレームワークを示している。

同規格が規定している要求事項は以下の通り。

- 反贈収賄のポリシーと手順の策定
- 経営トップのリーダーシップ、コミットメント、責任
- コンプライアンスマネージャー等による監視
- 贈収賄防止に関する社内教育
- プロジェクトやビジネスパートナーのリスク評価、デューデリジェンス
- ファイナンス、調達、販売、及び契約内容の管理
- 報告、監督、調査、評価のスキーム
- 継続的な改善活動

同規格は、第三者審査によって認証を受ける認証規格となる。なお、贈収賄リスクは組織によって異なるという事情を踏まえ、同規格は国や規模、事業内容によらずあらゆる組織の事情に応じて柔軟に利用できるよう設計されている。

＜環境＞

〇ウォルマートが社会における企業の役割についての新たなビジョンを発表

（参考情報：2016 年 11 月 4 日付 同社 HP）

ウォルマートは 11 月 4 日、社会における企業の役割に関する新たなビジョンを公表した。

同ビジョンは、2005 年に同社が策定した環境持続可能性目標である①企業運営におけるゼロエミッションの実現、②100%再生エネルギーの運用、③天然資源と環境を維持する製品の販売という 3 つの目標について、現在までの進捗を踏まえて再構築されたものである。

同ビジョンでは、2025 年までに以下 3 つの項目を達成することを宣言している。

①米国、英国、日本、カナダなどの主要市場で自社事業から排出される廃棄物について埋め立て処分ゼロを達成する
②自社事業の運営に必要なエネルギー源の半分を再生可能エネルギーから調達する
③プライベートブランドパッケージを 100%リサイクル可能なものに代替するとともに、米国で生産される農作物を 2 倍に増やし、主要商品 20 製品について持続可能な調達を推し進める

なお、このビジョンは、2015 年 12 月に COP21 で採択されたパリ協定を踏まえて策定されており、同協定に整合する排出削減計画を策定するのは小売業者として初、としている。

また、ウォルマートでは、上記環境取組みのみならず、小売業に従事する労働者の尊厳を守るため、職業訓練プログラムを通じてキャリアアップの支援、賃上げに向けた支援を行うとともに、同一労働同一賃金の保証、予測可能性の高い勤務スケジュールの提供等を通じて、労働環境の整備にも取り組むとしている。

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

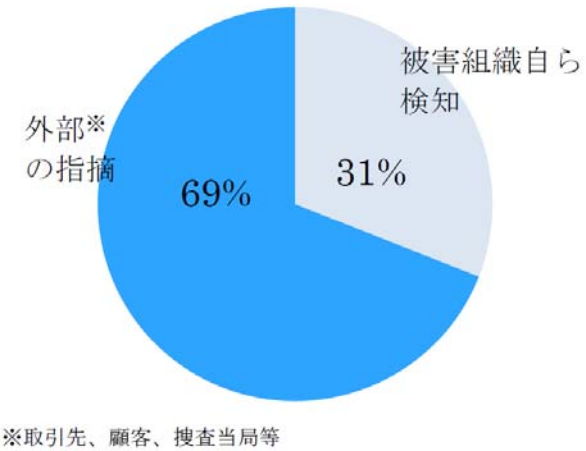
深刻化する情報セキュリティリスクへの対応組織として CSIRT への注目が高まっています。当社では CSIRT の構築を検討したいのですが、構築の効果とポイントについて教えてください。

Answer

1. はじめに

近年、企業が有する個人情報や重要な技術情報などを狙うサイバー攻撃は増加傾向にあります。また、特定の組織を狙う標的型攻撃を中心としてその手口が巧妙化しており、インシデントの発覚経緯の約 7 割は外部からの指摘によるものといったように、サイバー攻撃を受けたこと自体に気づかないことが多くなっています。

上記の背景に基づき、2015 年 12 月、経済産業省はサイバーセキュリティ経営ガイドラインを公開しました。同ガイドラインでは、緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備と定期的かつ実践的な演習の実施を求めており、巧妙化するサイバー攻撃に対し、専門性を持つ要員による組織的なインシデント対応が必要とされています。



【図 1】セキュリティ侵害の発覚経緯（出典：サイバーセキュリティ経営ガイドライン（経済産業省））

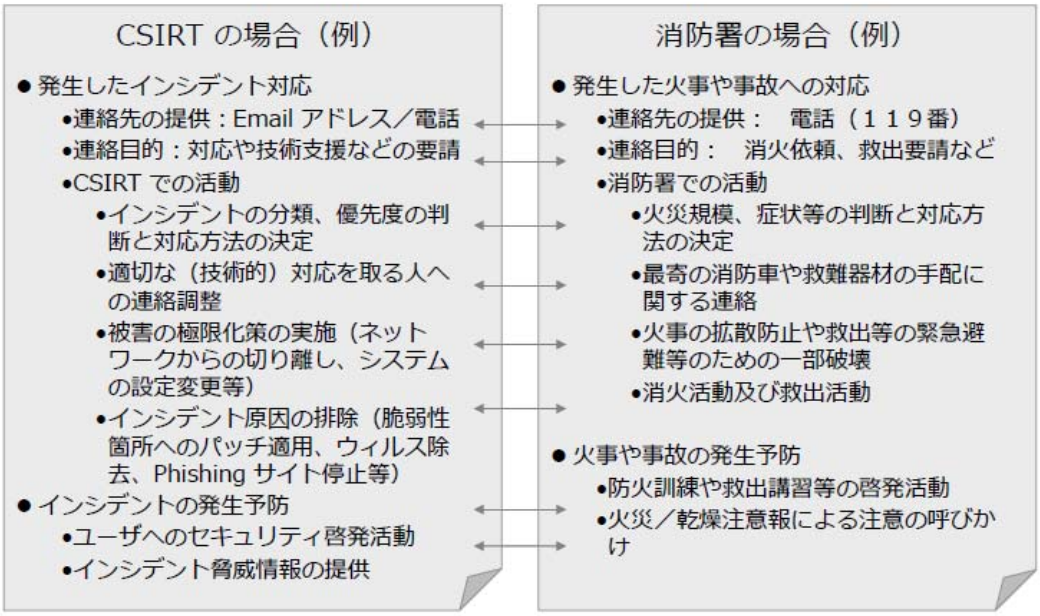
2. CSIRT とは

CSIRT（シーサート）とは、”Computer Security Incident Response Team”の略であり、その名が示すとおり、コンピューターセキュリティに関する初動対応などを担うチームとして組織されるものです。

CSIRT の具体的な役割としては、実際に攻撃を受けた際の対応ばかりを想定しがちですが、その他にも、

- コンピューターセキュリティインシデントの予防活動
- コンピューターセキュリティインシデントに関する報告の受付
- 原因の調査
- 対応の検討・実施

などがあり、CSIRT のイメージは、たとえば火事に対する「消防署」と位置付けられます。

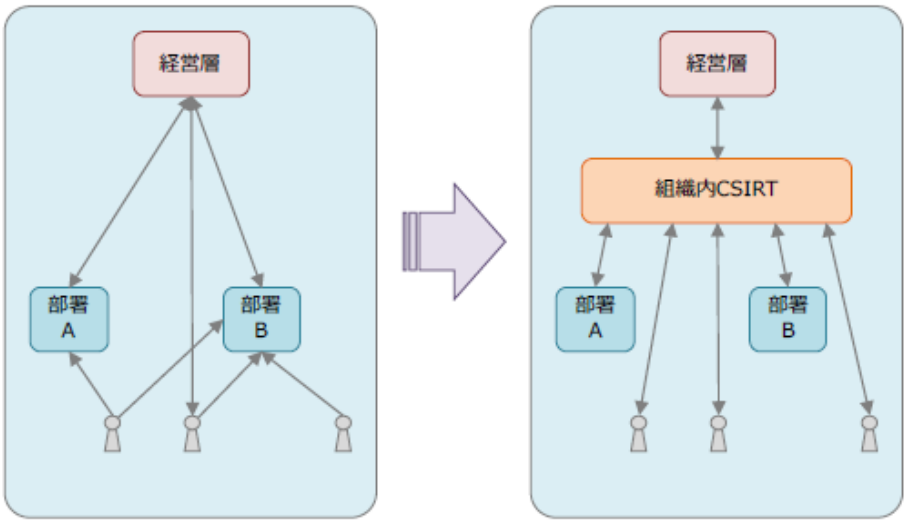


【図 2】CSIRT と消防署の役割比較例（出典：組織内 CSIRT の役割とその範囲（JPCERT/CC））

CSIRT は、経営層の意思決定に基づいた全社的な対応を行う組織として、情報システムで行われている業務や、情報システムで扱っているデータの重要性を把握することはもちろん、組織としてどのような順序で情報システムやデータを復旧させることが望ましいのか、リスクを総合的に判断しながら対応方針を立案することが求められます。

CSIRT 構築の効果としては、社内の情報管理の一元化とセキュリティ対応の指示の迅速化が挙げられます。

過去に発生した情報セキュリティインシデントでは、各部門で起こった問題が全社で共有されず、影響範囲や被害が把握できないまま被害が拡大するというケースがしばしば見られます。不正アクセスやウイルスによる情報漏洩が発生し、漏洩した情報に顧客や取引先の情報が含まれていた場合、当該情報を管理していた部門だけでなく、組織全体への影響を見据えた対応が求められます。CSIRT の組成により、インシデント関連の情報が CSIRT に集約かつ一元管理され、組織全体としての対応を迅速かつ適切に行うことが可能になります。



【図 3】CSIRT の効果のイメージ（出典：CSIRT ガイド（JPCERT/CC））

3. CSIRT 構築のポイント

日本シーサート協議会が 2015 年 11 月に公開した「CSIRT 人材の定義と確保 Ver.1.0」では、各企業の CSIRT において必要な機能、体制、人材を明確に示しています。

【表 1】CSIRT の役割と業務内容

グループ	役割名称	業務内容
情報共有	PoC 1)（社外）	日本シーサート協議会、FIRST2）、CSIRT、警察、監督官庁、等々との情報連携
	PoC(社内)	法務、渉外、IT部門、広報、各事業部、等々との情報連携
	IT部門との連携	適格で要領を得た文書の作成
	リーガルアドバイザー	コンプライアンス、法的内容とシステム間の翻訳
	ノーティフィケーション	各関連部署との連絡ハブ、情報発信
情報収集・分析	リサーチャー、 キュレーター	定例業務。インシデントの情報収集、 各種情報に対する分析、国際情勢の把握
	脆弱性検査、診断	ネットワーク、OS、セキュアプログラミングの検査、診断
	脆弱性分析、評価	ネットワーク、OS、セキュアプログラミング診断結果の評価
	セルフアセスメント	平時のリスクアセスメント。 有事の際の脆弱性の分析、影響の調査
	ソリューションアナリスト	ソリューションマップ作成、FiT&Gap 分析 3)、 リスク評価、有事の際の有効性評価
インシデント対応	コマンダー	全体統括。意思決定。社内PoC。役員、CISO 4）、 または経営層との情報連携
	インシデント管理	インシデントの対応状況の把握。コマンダーへの報告。 対応履歴把握。
	インシデントハンドラー	インシデント現場監督。セキュリティベンダーとの連携
	インベスティゲーター	社内捜査に必要な論理的思考、分析力、 社内システム理解力を使った内偵
	トリアージ	事象に対する優先順位の決定。
	フォレンジックス	証拠保全、システム的な鑑識、足跡追跡。マルウェア解析。
社内教育	教育、啓発	社内のリテラシー向上、底上げ。

（出典：CSIRT 人材の定義と確保 Ver.1.0 （日本シーサート協議会））

1）Point of Contactの略称。社外窓口として、JPCERT、NISC、警察、監督官庁、日本シーサート協議会、他CSIRT等との連絡窓口となり、情報連携を行う一方、社内窓口として、IT部門調整担当社内の法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、情報連携を行う。
2）Forum of Incident Response and Security Teamsの略称。世界中の CSIRT が相互の情報交換やインシデント対応に関する協力関係を構築する目的で 1990年に米国 CERT/CC などが中心となって設立されたフォーラムです。
3）情報システムを導入する際に、導入企業のビジネスプランやシステム化要求などのニーズと、情報システムの機能性がどれだけ適合（フィット）し、どれだけ乖離（ギャップ）が生じるかを分析すること。
4）Chief Information Security Officerの略称。企業内で情報セキュリティを統括する担当役員のこと。

また、同資料は企業の特性によって CSIRT をパターン分けし、CSIRT の役割の自社保有部分、及びアウトソーシング部分を想定した人材の定義と確保に関する情報を例示しています。例えば CSIRT（例 A）の役割は、「社内で情報共有はするが、システム維持についてはベンダーに任せる。インシデント発生時のミッションとしては、自社として守るべき優先順位の判断を行う。最低限の自警団の機能として活動する。手に負えなくなった場合には、外部機関（セキュリティ専門ベンダー等）に支援を要請する。」と定義しています。

【表 2】CSIRT のパターン

パターン	定義
例A	ユーザ企業で総務部門等を主体として構築・運用されているCSIRT
例B	ユーザ企業でIT系子会社、または情報セキュリティに関する専門部門を主体として構築・運用されているCSIRT
例C	IT系、セキュリティベンダー系企業において構築・運用されているCSIRT
例D	その他（学術機関、政府機関、法執行機関など）

（出典：CSIRT 人材の定義と確保 Ver.1.0 （日本シーサート協議会））

一見、CSIRT のメンバーには IT に関する専門知識が不可欠に見えますが、CSIRT（例 A）のようなケースも考えれば、以下のようなマネジメントスキルを備えていればよいといえます。

- ベンダーと会話できるスキル
- 社内情報共有としてベンダーの言葉を伝えられるスキル
- 優先順位を決定できるスキル

また、CSIRT が平時の予防を含めた対応を担うケースもあれば、インシデントが起こった際に特別に結成される場合もあります。平時の監視は専任が、緊急時の対応は兼任も含めたフルメンバーで行う、といった形も現実的でしょう。

4. おわりに

今や、規模・業種等に関わらず、あらゆる企業がサイバー攻撃のリスクに曝されていますが、一方で、サイバーリスクを自社にとってのリスクと認識し、十分な対策を講じている企業は決して多いとはいえません。

サイバー攻撃を完全に予防することが難しくなりつつある中、企業規模の大小等を問わず、CSIRT を構築・運用する必要性は高まっています。

自社の実態に応じた CSIRT のあり方を検討したうえで、そのあり方に応じた人材の育成・確保を図ることが急務といえます。

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（全社的リスク管理）に関しても、以下のテーマについてコンサルティング・セミナー等を実施しております。
これらのコンサルティング等に関するお問い合わせ・お申込み等は、下記の弊社お問い合わせ先、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。

お問い合せ先
㈱インターリスク総研　事業リスクマネジメント部
TEL.03-5296-8912（CSR・法務グループ）
TEL.03-5296-8914（統合リスクマネジメントグループ）
http://www.irric.co.jp/

◇CSR（企業の社会的責任）
◇企業リスク分析・評価
◇危機管理
◇法務リスク全般
◇食品リスクマネジメント
◇D&O（役員賠償責任）
◇ERM（全社的リスク管理）
◇コンプライアンス（法令遵守）
◇海外危機管理
◇製造物責任（PL）・製品安全（PS）
◇情報セキュリティ
◇CS・苦情対応　他