2016.5.2

CSR・ERMトピックス ＜2016 No.2＞

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 3 月～4 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「つながる世界の開発指針」を公開

（参考情報：2016 年 3 月 24 日　同機構 HP）

独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センターは 3 月 24 日､IoT*製品の開発者が開発時に考慮すべきリスクや対策を取りまとめた「つながる世界の開発指針」を公開した。

同指針は、あらゆる製品がインターネットに接続し、製品同士が相互に接続する「IoT 社会」が到来することにより、IoT 製品の利用者や製品自体の「安全性・セキュリティ」を脅かすリスクが懸念されることを受けて策定されたもの。懸念されるリスクとしては､「安全を脅かすリスク（自動車が不正に遠隔操作される等)」､「セキュリティを脅かすリスク（ATM 等から不正に送金される等)」､「機能を損なうリスク（テレビ等が混線により操作不能となる等)」が挙げられている。

同指針は、IoT 製品の開発に関わる企業の経営者、開発者及び保守者が活用することにより、つながる世界の安全安心を実現させることを狙いとしており、下表の通り 17 の開発指針を定めている。またそれぞれの指針ごとに、指針のポイント、指針とした背景の解説、具体的な対策例が示されている。

【表】開発指針一覧

大項目		指針
方針	つながる世界の安全安心に企業として取り組む	1 安全安心の基本方針を策定する
		2 安全安心のための体制・人材を見直す
		3 内部不正やミスに備える
分析	つながる世界のリスクを認識する	4 守るべきものを特定する
		5 つながることによるリスクを想定する
		6 つながりで波及するリスクを想定する
		7 物理的なリスクを認識する
設計	守るべきものを守る設計を考える	8 個々でも全体でも守れる設計をする
		9 つながる相手に迷惑をかけない設計をする
		10 安全安心を実現する設計の整合性をとる
		11 不特定の相手とつなげられても安全安心を確保できる設計をする
		12 安全安心を実現する設計の検証・評価を行う
保守	市場に出た後も守る設計を考える	13 自身がどのような状態かを把握し、記録する機能を設ける
		14 時間が経っても安全安心を維持する機能を設ける

運用	関係者と一緒に守る	15 出荷後も IoT リスクを把握し、情報発信する
		16 出荷後の関係事業者に守ってもらいたいことを伝える
		17 つながることによるリスクを一般利用者に知ってもらう

* IoT
Internet of Things の略であり、コンピュータが、センサー等を用いて「モノ(Things)」から迅速かつ正確に情報収集を行うことで、省力化とともに、自らが世界を観察、特定、理解するようになる概念をいう。

＜コーポレート・ガバナンス＞

〇日本生命保険が≪日本版スチュワードシップ・コード≫に係る取組みの強化を発表

（参考情報：2016 年 3 月 30 日付　同社 HP）

日本生命保険は 3 月 30 日、「責任ある機関投資家」の諸原則≪日本版スチュワードシップ・コード≫（以下、「本コード」という）に係る取組みを強化すると発表した。

本コードは、機関投資家が「スチュワードシップ責任*」を果たすにあたり有用と考えられる諸原則を定めており、本コードを受け入れる機関投資家に対して、本コードの各原則への対応状況をウェブサイトに公表するとともに、見直しを行うことを求めている。

同社は、2014 年 5 月 26 日に本コードの受入を表明しており、今般、投資先企業との対話および議決権行使について、以下の通り取組みを強化するとしている。

1. 企業との対話活動の強化

(1) スチュワードシップ責任を果たすための基本方針の開示

スチュワードシップ活動をより充実させるため、投資先企業との対話活動・議決権行使にあたっての基本スタンスを、以下 4 つの基本方針として明確化。

・投資先企業との建設的な対話
・PDCA の観点からの対話の実効性向上
・個別企業の状況を踏まえた議決権行使
・改善が期待できない場合の議決権行使における不賛同や株式の売却検討

(2) 対話活動の主なテーマと自社スタンスの開示

より建設的な対話活動を行うため、経営戦略、収益性、E(環境)S（社会）G（ガバナンス）などに関して、主な対話テーマと、当該テーマにおける投資先企業への期待や要望を明示。例えば ESG に関しては、コーポレートガバナンス・コードへの形式的な対応のみならず、以下のような実質的な対応を求めるとしている。

・実効的なコーポレートガバナンス態勢の構築
・不祥事等を起こした場合の責任の明確化や再発防止策の策定・履行

(3) 「重点対話企業」との対話強化

低 ROE や低配当性向、コーポレートガバナンスに改善余地があるなどの課題の有無・程度と投資規模を考慮の上、「重点対話企業」を選定し、対話活動を強化。

今年度は「重点対話企業」を 200 社程度に拡大し、対話活動に取り組む予定。

2. スチュワードシップ活動にかかる体制の強化
（1）企業との建設的な対話を専門に担当する人材の追加配置

（2）対話・議決権行使の高度化に向けた新システムの導入

3. 「議決権行使精査要領」の改定
投資先企業の株主総会議案を精査する際の社内基準「議決権行使精査要領」を、6 月 1 日付で改正。
同要領に基づいて精査対象となった議案については、必要に応じて企業と対話を行い、自社の課題意識を表明の上、投資先企業における改善の取組み等を十分に検討した上で、賛否を判断。

（同社「『責任ある機関投資家』の諸原則≪日本版スチュワードシップ・コード≫に係る取組みの強化」を基にインターリスク総研作成）

詳細は、以下の URL を参照。
http://www.nissay.co.jp/news/2015/pdf/20160330a.pdf

* スチュワードシップ責任
本コードによると、「機関投資家が、投資先企業やその事業環境等に関する深い理解に基づく建設的な「目的を持った対話」（エンゲージメント）などを通じて、当該企業の企業価値の向上や持続的成長を促すことにより、「顧客・受益者」（最終受益者を含む。）の中長期的な投資リターンの拡大を図る責任」とされている。

＜レジリエンス＞

○内閣官房国土強靭化推進室が「レジリエンス認証」制度を創設

（参考情報：2016 年 4 月 18 日　一般社団法人レジリエンスジャパン推進協議会 HP）

内閣官房国土強靭化推進室は 4 月 18 日、国土強靭化*の趣旨に賛同し、事業継続に関する取組を積極的に行っている事業者を「国土強靭化貢献団体」として認証する「レジリエンス認証」制度を創設した。

本認証制度は、各種企業・団体の事業継続に関する積極的な取組を広めることにより、社会全体の強靭化を進めることを目的として創設されたもの。本認証を受けた企業・団体は、交付されたレジリエンス認証マークを広告等に活用できる、国土強靭化に関するセミナー・シンポジウムに関する情報が優先的に配信されるなどのメリットが期待できるという。認証は、一般社団法人レジリエンスジャパン推進協議会**によって、内閣官房国土強靭化推進室「国土強靭化貢献団体の認証に関するガイドライン」に基づいて行われる。認証基準は以下の通り。

（1）事業継続に係る方針が策定されている
（2）事業継続のための分析・検討がされている
（3）事業継続戦略・対策の検討と決定がされている
（4）一定レベルの事業継続計画（BCP）が策定されている
（5）事業継続に関して見直し・改善できる仕組を有し、適切に運営されている
（6）事前対策が実施されている
（7）教育・訓練を定期的に実施し、必要な改善が行われている
（8）事業継続に関する一定の経験と知識を有する者が担当している

(9) 法令に違反する重大な事実がない

(10) その他留意事項

①国土強靭化の取組を進め、国土強靭化の取組促進に積極的に協力すること。

②認証組織が行う国土強靭化の推進に関する調査等に協力すること。

（内閣官房国土強靭化推進室『国土強靭化貢献団体の認証に関するガイドライン』を基にインターリスク総研作成）

* 国土強靭化

災害や事故などにより致命的な被害を負わない強さと、速やかに回復するしなやかさを持つ国土・経済システムを目指す取組。

** 一般社団法人レジリエンスジャパン推進協議会

国土強靭化担当大臣私的諮問機関「ナショナル・レジリエンス懇談会」の結果を踏まえ、国土強靭化に向けた各種取組を実施していくことを目的として設立された組織。

海外トピックス：2016 年 3 月～4 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。

＜ジェンダー＞

〇国際労働機関（ILO）が女性の労働環境等に関する調査結果を公表

（参考情報：2016 年 3 月 8 日付　同機関 HP）

国際労働機関（International Labour Organization 以下、ILO）は、国際女性デー*である 3 月 8 日に女性の労働環境等に関する調査結果である『Women at Work Trends 2016』を公表した。

同レポートでは、女性の労働環境の現状と過去 20 年間の改善状況について解説している。具体的には、男女別の就業率、業種の傾向、有償労働・無償労働の割合、週の労働時間、賃金格差、社会保障の差などについて国別、地域別にデータを分析し、解説を加えている。ILO の事務局長である Guy Ryder 氏は、同レポートを受けて、「女性がやりがいのある仕事を見つけて働き続けるには、いまだに多くの障壁が残っている」と述べた。

例えば、178 ヶ国を対象にした同レポートの調査では、2015 年の男性の就業率が 72%であるのに対し、女性は 46%であり、その差は 26%も開いている。また、1995 年の調査から比較しても男女の就業率の差は、約 0.6%しか改善していない。さらに、女性の賃金は男性の賃金の 77%に留まっている。この他にも、就業機会、待遇、評価といった面で女性と男性の間の不平等を示すデータは多く、過去 20 年間で大きく改善しているとは言い難い結果であった。

同レポートでは、このような不平等を生む重要な要因として、家庭における無償の労働時間（家事や育児・介護に貢献している時間）の不平等を挙げている。

その他、同レポートで示されている主なデータは以下の通り。

データの種類	調査結果	
（15 歳以上の）就業率	【日本】 女性：47.6%、男性：67.7%	【世界平均】 女性：46%、男性：72%
	【東アジア】 女性：51.7%、男性：69.4%	【北アメリカ】 女性：55.1%、男性：64.9%
短時間（週 35 時間以下の）勤務者の割合	【日本】 女性：56.5%、男性：18.4%	【世界平均】 女性：34.2%、男性：23.4%
	【東アジア】 女性：13.9%、男性：10.3%	【北アメリカ】 女性：34.7%、男性：20.2%
無償労働（家事や育児・介護などに費やす）時間の長さ	【先進国】 女性：4 時間 20 分／日 男性：2 時間 16 分／日	【発展途上国】 女性：4 時間 30 分／日 男性：1 時間 20 分／日

（『Women at Work Trends 2016』を基にインターリスク総研作成）

* 国際女性デー

国連が 1975 年に定め、世界中の女性たちが女性の社会参加や労働差別の撤廃などを求める行動を起こす日として制定された国際的記念日。日本ではまだ認知度が高くないが、例えばロシアでは 3 月 8 日は祝日となっている。

＜人権＞

〇Shift が国連「ビジネスと人権に関する指導原則」に則した人権取組みに関する企業の報告をまとめたデータベースを公表

（参考情報：2016 年 3 月 22 日付　同機関 HP 他）

国連の「ビジネスと人権に関する指導原則（The United Nations Guiding Principles on Business and Human Rights; 以下、UNGPs）」*の研究機関 Shift は 3 月 22 日、UNGPs への対応状況に関する企業の報告をまとめたデータベース「The UN Guiding Principles Reporting Database」を公表した。

同機関は 2015 年 2 月に、国際会計事務所 Mazars と共同で、UNGPs に則した人権取組みに関する包括的な報告フレームワーク「The UN Guiding Principles Reporting Framework」を開発、公表した。同データベースは、企業がホームページに掲載している情報や報告書をもとに、同フレームワークの各質問項目に対する企業の取組状況をまとめたもの。同フレームワークの構成は以下のとおり。

【表】「The UN Guiding Principles Reporting Framework」の構成

PART A	人権尊重に関するガバナンス
A1	人権尊重方針の策定・公表
A2	人権尊重の組織・事業活動への組み込み
PART B	報告の中心となる人権問題の設定
B1	組織にとって顕著な人権問題の設定
B2	顕著な人権問題の選定プロセス
B3	（対象地域を限定する場合）地域の選定プロセス
B4	顕著な人権問題以外の問題による人権に対する重大な影響への対応
PART C	顕著な人権問題
C1	個別方針の策定
C2	ステークホルダー・エンゲージメント
C3	影響の評価
C4	顕著な人権問題に対する予防・損害低減策の実行
C5	顕著な人権問題への対策効果の追跡
C6	苦情・被害者への対応

（『The UN Guiding Principles Reporting Framework』を基にインターリスク総研作成）

公表日現在で、同データベースにはアパレル業、小売業、資源採掘産業、飲食産業など 30 社の情報が登録されており、登録企業数や業種は今後拡大するとしている。

* ビジネスと人権に関する指導原則（UNGPs）

2011 年 6 月に、国連人権理事会において承認された人権の保護、尊重、救済に関する指導原則で、すべての国家と企業に適用される。

本原則では、国・政府、企業、ステークホルダーの各主体について、人権の保護・尊重・救済の各側面からそれぞれの果たすべき役割を明示している。特に、企業については、人権尊重に関するあるべき取組等を提示するほか、企業活動が人権侵害の原因となる、または悪化させるリスクを提示している。一方、ステークホルダー向けには、企業の人権尊重取組を評価するためのベンチマークを提供している。

＜CSR 調達＞

〇Initiative for Responsible Mining Assurance が責任ある鉱業のための保証基準のドラフトを発表

（参考情報：2016 年 4 月 5 日付　同団体 HP、ティファニー社 HP）

Initiative for Responsible Mining Assurance（以下、「IRMA」）は、4 月 5 日、責任ある鉱業のための保証基準「IRMA Standard for Responsible Mining」のドラフトを発表した。

IRMA は、2006 年 6 月に、カナダ・バンクーバーにおいて立ち上げられた、責任のある鉱業のための保証基準を策定するための部門横断的なイニシアチブである。アングロアメリカン社をはじめとする鉱業企業、ティファニーやウォルマートといった小売企業、NGO や業界団体等が加盟しており、鉱業分野において環境、人権、社会的基準への遵守を独立的に検証する自発的システムを開発・確立することを目的としている。

本ドラフトは、関連業界や NGO、影響を受ける地域社会、労働団体等と対話や議論を実施し、規格案を試験的に実施した上で、改訂された草案として発表されたものであり、今後、60 日間のレビューおよびパブリックコメント期間を経て、2016 年後半の発行を予定している。

同ドラフトでは、4 章（①企業の健全性、②社会的責任、③環境責任、④計画的管理）にわたり以下のような内容について基準を策定している。

【主な内容】

Principle	Chapter
①企業の健全性 Business Integrity	– 法令遵守 – 収入及び支出の透明化
②社会的責任 Social Responsibility	– 児童労働および人権に関するデューディリジェンス – 緊急時対応計画 – 地域住民の健康と安全 – 効果的なステークホルダー・エンゲージメント（コミュニケーションやその他の取り組みなども含めた協力関係の構築）のための対話　など
③環境責任 Environmental Responsibility	– 水質管理、水量管理 – 廃滓管理 – 大気汚染への対応 – 騒音 – 水銀の管理　など
④計画的管理 Planning and Managing for Positive Legacies	– 社会的、環境的影響調査の実施 – 開墾・開山および閉山　など

（『IRMA Standard for Responsible Mining』IRMA-STD-001 Draft v2.0 を基にインターリスク総研作成）

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、サイバー攻撃の脅威に注目が集まっていますが、サイバー攻撃の現状はどのようなものでしょうか。また、企業においてはどのような対策を講じるべきでしょうか。

Answer

1. サイバー攻撃とは

(1) サイバー攻撃とは

サイバー攻撃とは、「コンピュータシステムやネットワークに悪意を持った攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行を行うこと」（経済産業省 サイバーセキュリティ経営ガイドライン）を指します。

近年、IT の発達に伴い、攻撃手段は多様化・高度化の一途を辿っていますが、主な攻撃手段としては、以下のものが挙げられます。

攻撃手段	攻撃の概要
不正アクセス	本来アクセス権限を持たない者が、サーバや情報システムの内部へ侵入する攻撃。
フィッシング攻撃	金融機関などの正規の Web サイトを装い、そこに電子メールなどで誘導することで、暗証番号やクレジットカード番号などを詐取する攻撃。
標的型メール攻撃	対象の組織から重要な情報を盗むことなどを目的として、担当者が業務に関係するメールだと信じて開封してしまうよう巧妙に作り込まれたウイルスを電子メールで送りつける攻撃。
DoS（サービス妨害）攻撃	サーバの処理能力を超える極めて多大なリクエストを一斉に送信することで、システムのサービスを妨害する攻撃。
水飲み場攻撃	対象の組織や個人がよく利用すると思われる Web サイトをあらかじめ改ざんしておき、アクセスした利用者にマルウェアを導入させる攻撃。

(2) 近年におけるサイバー攻撃の目的の傾向変化

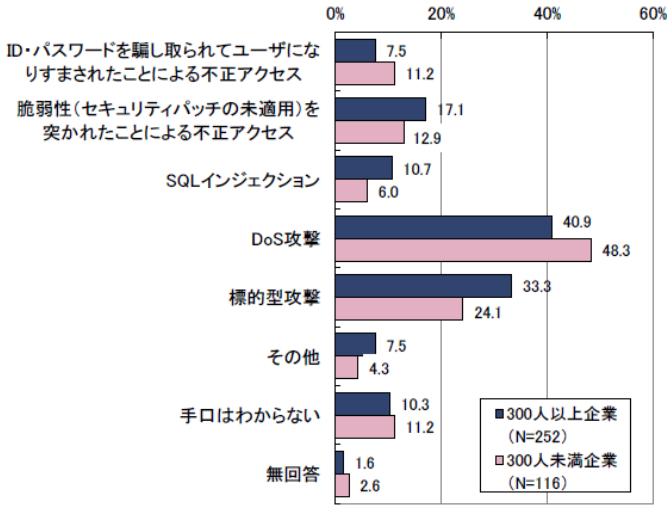
まず、サイバー攻撃の目的に着目すると、以前は「いたずら」や「能力の誇示」といったものが中心でしたが、最近では、「金銭目的」や「組織活動の妨害」に変化しているといわれています。近年では、企業が保有する情報を暗号化し、復号と引き換えに金銭を要求する「ランサムウェア」というサイバー攻撃が登場しています（「ランサム」は英語で身代金の意）。

これに伴い、攻撃対象も多様化しています。政府機関や大企業といった有名な組織だけでなく、例えば中小企業や個人の金融機関のインターネットバンキングの口座から、攻撃者の口座に金銭を振り込ませる不正送金被害も年々増加しています。

2. サイバー攻撃の現状

独立行政法人 情報処理推進機構（以下、「IPA」）の「2014 年度情報セキュリティ事象被害状況調査」によれば、2014 年度の 1 年間にサイバー攻撃に遭遇した企業の割合は 15.1%であり、2012 年度の同調査と比較して 5.5 ポイント増加しています。

右図に示す通り、攻撃方法としては標的攻撃によるマルウェア（悪意のあるソフトウェア）感染の被害が多いですが、DoS 攻撃（サービス妨害攻撃）による業務サーバの機能停止、サーバの脆弱性を突かれた不正アクセスや情報の改ざんなどの被害も報告されており、様々な手口のサイバー攻撃が試行されています。また、組織の規模とサイバー攻撃の手口に大きな関係がないことも分かります。



サイバー攻撃の手口（従業員規模別）

（出典:2014 年度情報セキュリティ事象被害状況調査（IPA））

3. 企業に求められるサイバー攻撃対策

(1) 方針・組織体制の整備

まず、サイバー攻撃のリスクが企業経営上の重要なリスクであることを、経営層が明確に明示することが必要です。特に中小企業においては、未だ「自社はサイバー攻撃の対象にはなり得ない」との認識が少なくありません。また、対策にはシステム投資を含む多額の費用がかかるケースもあります。そこで、「サイバーセキュリティポリシー」を策定するなどして、サイバー攻撃リスクの重要性と自社としての対応方針を社内外に明示することが必要です。

また、各種の対策を円滑に進めていく上で、専任組織または専任者を設けるといった組織体制の整備も必要となります。中小企業においては、専任組織等の設置は難しいと思われますが、少なくとも同リスク対策を立案・推進する責任者を明確にしておくことは必要です。

(2) 予防

サイバー攻撃の予防のポイントとなるのは「マルウェアを組織内に入れない」こと、「組織内に入れてもマルウェアを活動させない」ことの二点です。

まず、前者（組織内に入れない）の具体的な対策としては、「マルウェア対策ソフトをインストールし、定義ファイルを最新にしておく」ことが挙げられます。但し、標的型攻撃メールなどは必ずしもマルウェア対策ソフトで検知できるものではなく、万全の対策とはいえません。そこで、「役職員にサイバー攻撃に関する教育・訓練を実施し、サイバー攻撃の兆候に気づかせる」ことも重要となります。例えば標的型攻撃メールやフィッシング攻撃で表示された Web ページをサイバー攻撃と見破ることができれば、被害発生を未然に防ぐことにつながります。

後者（活動させない）の具体的対策としては、「パソコン、サーバのセキュリティパッチを確実に運用する」ことです。マルウェアはパソコンやサーバのソフトウェアの不具合を突

いて行動することがあるため、不具合を修正するためのセキュリティパッチを適切に適用し、マルウェアが行動できない環境を作ることも重要です。

これらの対策は、いずれも大きなコストを伴わずにできることばかりですから、できるだけ早期に実施すべき内容といえます。

なお、コストはかかるものの、不正侵入の早期発見のため、「侵入検知システム」も有効です。

(3) 被害低減

前述の通り、IT の進歩に伴い、サイバー攻撃の手段はますます発達しており、あらゆる攻撃手段に対して先回りして予防することは困難です。特に標的型攻撃は、「成功するまでしつこく攻撃する」という特徴があり、メールの文面も巧妙化しているため、予防のみでは十分とはいえません。いかにして、攻撃を受けた際に迅速に対応し、被害を最小限に抑えるかが重要になります。

そのためにも、サイバー攻撃を受けたときの緊急対応の手順を定め、研修・訓練によって役職員に浸透させることが必要です（緊急対応の標準的な手順は下表の通り）。

特にポイントとなるのは、攻撃が疑われた段階で社内報告・初動対応を開始することです。例えば、標的型攻撃メールと気づかずに添付ファイルを開いてしまい、半年後に外部からの指摘でサイバー攻撃を受けていた事実に気づくケースも発生しています。

また、緊急対応を行う組織である CSIRT（Computer Security Incident Response Team）*を整備する企業も増えています。平時より CSIRT を設置し、アクセスログの監視等を実施している企業もありますが、多くの企業では、システム部門を中心に、有事の際に CSIRT を立ち上げることとしているようです。

もっとも、いかに手順や組織を整備しても、従業員がこれに従って、行動できなければ意味がありません。そこで、CSIRT または周辺の要員を対象とした訓練を定期的に実施することが望まれます。なお、組織規模が大きくない企業において CSIRT の組成が難しい場合、緊急時には速やかに役割分担を行い対応に当たることができることが望まれます。

また、従業員の過失に起因して攻撃を受けた場合、自身への責任追及等の恐れから、迅速な報告がなされないことも想定されます。迅速に報告・共有を行うことの重要性を、継続的に周知徹底させることも求められます。

【緊急対応の標準的な手順】

大項目	小項目	実施内容
(1) 検知	責任者・上長への連絡	サイバー攻撃の疑いを持った場合、その事実を所定の連絡ルートに沿って迅速に責任者まで報告する。その際、「疑いを持った状況」「疑いを認知した日時」を併せて報告する。
(2) 初動対応	ネットワークからの遮断・システムの停止	被害の拡大を防ぐため、該当のパソコンのネットワークからの遮断、感染の恐れがある情報システムの停止などの処置を行う。 業務委託先のシステムにも影響が及ぶ場合は、自社同様に、ネットワークからの隔離等の処置を行わせる。
	ログ、状況の保全 (いわゆる「現場保存」)	被害を受けたパソコンなどは、電源を切り、そのままの状態で保管する。ログを取得している場合は、併せて保管する。 後日の調査や分析のために必要となるため、被害を受けたパソコン等は隔離保管する。
(3) 調査・分析	影響範囲の特定	サイバー攻撃により被害を受けた範囲を通信ログやヒアリング等で特定する。 外部への情報漏洩が確認できた場合、漏洩したデータの特定も行う。
	原因究明	ログの分析、被害を受けたパソコンやデータの分析、不正アクセスの痕跡の確認等の原因究明を行う。
(4) 被害者への通知・情報開示		情報漏洩が発生した場合、被害者に漏洩の事実を通知する。漏洩による影響が広範囲に及ぶと考えられる場合は、ホームページでの情報開示や記者会見による公表を行う。 犯罪性がある場合は警察へ届け出る。必要に応じて、所管省庁等へ報告する。 報告先や公表基準（要否、時期、対象など）等については、予めマニュアル化しておく。
(5) 復旧・再発防止	復旧	感染したパソコンとは別のパソコンを用意し、OS、アプリケーションのインストール及び、バックアップデータを復元する。復元するデータは事前にマルウェアのチェックを行う。 なお、ネットワークへの接続は、組織内にマルウェアが残っていないことが確認できてから行う。
	再発防止	同様の被害を抑制するため、被害情報を社内周知する。 社内教育マニュアルを改訂し再教育を行う。

4. おわりに

従来、サイバー攻撃は大企業や政府機関などが多く狙われてきました。しかしながら、近年は大企業の取引先である中小企業を攻撃し、そこを踏み台にして大企業の情報を不正に入手する方法も広がっています。今回は必要最低限の対策を中心に、概要をお示しするに留めましたが、企業の IT 活用度、規模、業種などによっては、追加対策の検討も必要となります。システム改修等、より高度な取組が必要と思われる場合には、専門業者に相談することが望まれます。

* CSIRT（Computer Security Incident Response Team）
コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う。（日本シーサート協議会 HP より）

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