企業を揺るがすサイバー脅威 経営にセキュリティーの視点を

政府が示したガイドラインを 読み解き、実践するポイントは?

企業をサイバー攻撃から守るのは情報システム部でしょうか?それとも経営者でしょうか。2015年末に経済産業省より公表された「サイバーセキュリティ経営ガイドライン」では、経営的な視点でサイバー攻撃から企業を守ることについて述べられています。政府の2016年度計画である「サイバーセキュリティ2016」へ盛り込まれ、本格的に対応が求められることとなります。

巧妙化するサイバー攻撃、企業の生き残りに求められる「経営力」

自社がサイバー攻撃を受けた場合、「具体的にどのような被害が発生するのか」「問題なく事業を継続できるのか」といったリスクについて、経営層が正確に把握している企業はどのくらいあるのでしょうか。サイバー攻撃が日々巧妙化し、その被害が拡大している中、企業の経営者にとってサイバー攻撃に対するリスクマネジメントが重要な経営課題の一つになっています。

一方で、サイバーセキュリティーに関連するリスクへの認識はさまざまで、その対策も企業ごとに異なっているのが実情です。情報システム部などの「現場レベル」でリスクを判断し、対応を進めている企業も少なくありません。

十分な対策を講じている組織がある一方で、対策の甘さを突かれ、サイバー攻撃によって経営を左右するような大きなダメージを負ってしまう企業もあります。

近年起こった大規模な個人情報流出を伴うセキュリティー事故

時期	事件	事件の概要
2016 年 6 月	旅行代理店において、標的型攻撃によるウイルス感染から、個人情報流出	旅行代理店のグループ会社において、取引先を装ったメールの添付ファイルを開いたことにより、端末がウイルスに感染。約 793 万人の顧客の個人情報の流出の可能性が発生した。
2015 年 6 月	日本年金機構において、標的型攻撃によるウイルス感染から、個人情報流出	職員が、メールに添付されていたファイルを開いたことでウイルスに感染。約 125 万人の基礎年金番号などの個人情報が流出した。
2014 年 7 月	通信教育会社の関連会社の元派遣社員が、顧客情報を持ちだし売却	グループ企業に派遣社員として勤務していたエンジニアが、スマートフォンを用いて、サーバーで保存されていた顧客 約 2260 万人の個人情報を持ちだして、名簿業者に売却した。

※報道を元に作成

企業として最低限取り組むべき課題は何か、政府が一つの指標を示しました。経済産業省が 2015 年 12 月に公表した「サイバーセキュリティ経営ガイドライン」です。

企業を揺るがすサイバー脅威　経営にセキュリティーの視点を

政府の年次計画に盛り込まれた「サイバーセキュリティ経営ガイドライン」

「サイバーセキュリティ経営ガイドライン」は、有識者で構成された情報処理推進機構（IPA）の検討会を経て策定されました。大企業、中規模企業において、サイバーセキュリティー対策が、明確に「経営課題である」と示されたのです。

「セキュリティーを経営課題として捉えること」そのものは、特に目新しい考え方ではありません。ISMS（Information Security Management System）やプライバシーマークといった情報セキュリティーに関するマネジメントシステムの導入も、徐々に進んでいます。しかしその一方で、セキュリティー対策への取り組みが、担当部門の現場レベルにとどまる企業もあり、「経営層が取り組むべき課題」と捉えていない企業も少なくなかったといえます。

そこに「サイバーセキュリティ経営ガイドライン」が一石を投じました。セキュリティーは経営者が取り組むべき「経営責任」の一つであり、リーダーシップを発揮するように求めたのです。

第三次安倍内閣では、2015 年に「サイバーセキュリティ戦略」を策定し、サイバーセキュリティーに対し国を挙げて取り組むことを重要な政策課題に位置付け、同戦略における 2016 年度の年次計画「サイバーセキュリティ 2016」※で、同ガイドラインの普及を掲げています。

※本記事執筆時点では、「サイバーセキュリティ 2016」は正式決定前の案の状態です。

ただし、あくまでガイドラインであり、法的拘束力はなく、経営者が取るべき方策の大枠を設定したに過ぎません。しかし、株式市場への情報開示について検討が進められるなど、今後企業に求められるセキュリティーガバナンスは、ますます高くなることが予想されます。経営者にセキュリティー対策を促すメッセージの一つといっても良いでしょう。

「経営者のリーダーシップ」こそ、セキュリティー対策の原動力に

「サイバーセキュリティ経営ガイドライン」は、主に経営者向けのパートである「サイバーセキュリティ経営の 3 原則」と、セキュリティー担当役員や担当者を対象とした「サイバーセキュリティ経営の重要 10 項目」で構成されています。

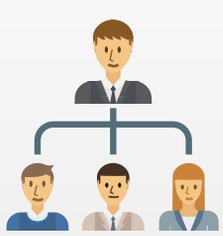
前半部の「サイバーセキュリティ経営の 3 原則」は、いわば企業の舵取り役である経営者が、サイバーセキュリティーと向かい合う際に認識しておくべき内容を三つにまとめたものです。

さらに後半では、経営者のもと、情報セキュリティー担当役員の「CISO（Chief Information Security Officer）」やセキュリティー担当者が実行すべき具体的な対策 10 項目をもとに、推進することを求めています。

では、実際に「サイバーセキュリティ経営ガイドライン」の具体的な中身を見てみましょう。

サイバーセキュリティ経営の3原則

1	2	3
経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要	自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策が必要	平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要



企業を揺るがすサイバー脅威　経営にセキュリティーの視点を

一つ目は、経営者によるリスクの認識、およびリーダーシップによるセキュリティー対策の推進です。ここではセキュリティーリスクが企業の命運を分ける課題とし、経営リスクの一つとして正しく捉え、リーダーシップにより経営資源を投じるよう求めています。

二つ目は、サイバーセキュリティーが「自社」に限定された問題ではないことに言及しました。現在のビジネスは、グループ会社はもちろん、委託先、サプライチェーン、取引先など多くのプレイヤーで、事業が成り立っています。そのうちどこか一つが攻撃を受ければ、連鎖して他のプレイヤーの事業まで停止してしまうかもしれません。それを防ぐには広い視野を持って対策を進めていく必要があります。

三つ目は、ステークホルダーとのリスクに関するコミュニケーションです。インシデント発生時はもちろん、平時より関係者と適切なコミュニケーションを取ることで信頼性の醸成を進めるほか、業界全体のリスク低減を見据えた情報共有の重要性も挙げています。

見逃してはならないポイントは、セキュリティーへの投資について「リターンの算出はほぼ不可能」と述べている点でしょう。これらが積極的な投資行動を回避させ、リスクを見過ごす原因になっていると指摘しています。

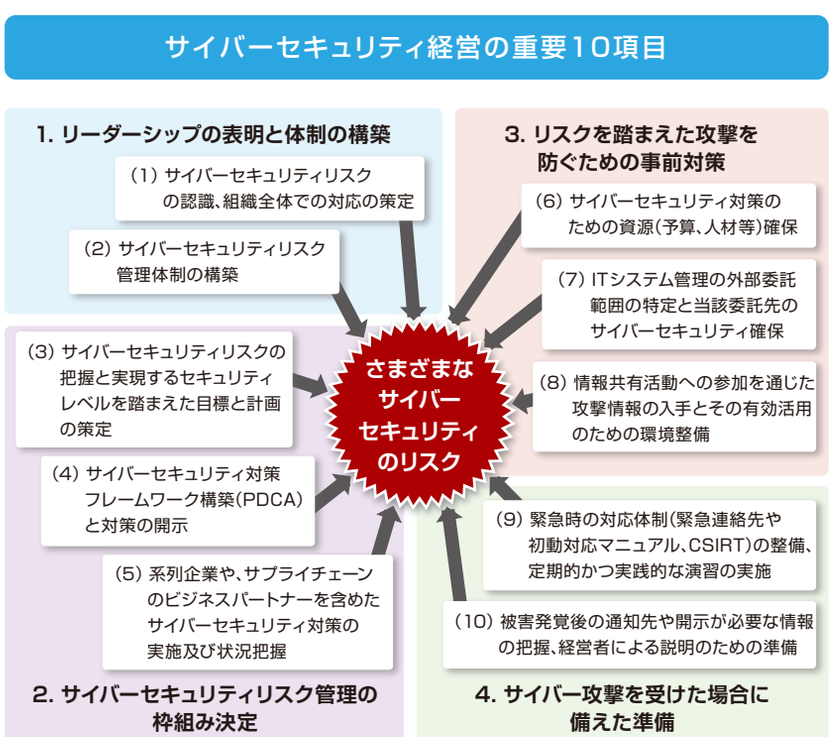
セキュリティー対策の「投資対効果」を示すことが困難であるということは、収益重視の企業経営のなかで、現場が重大な危機感を感じてもボトムアップで解決していくのが難しい課題であることを意味します。

そのため判断を現場任せにせず、リーダーシップによるトップダウンで対応していくことが求められているのです。無論、対策を推進するというのは、闇雲に投資額を増やすという意味ではありません。直面するリスクに関する情報をしっかりと現場から収集し、事業継続性への影響を踏まえた上で、ときに大胆さを持ちつつも、バランスをもって合理的に判断していくことが必要です。

CISOやCSIRTなど「橋渡し人材」を設置することが実践のポイント

「サイバーセキュリティ経営の重要10項目」のパートでは、前述の3原則のもと、実際に経営者のリーダーシップによって、CISO（Chief Information Security Officer）やセキュリティー担当者が実践すべき「10」のセキュリティー対策を述べています。

この10項目では、サイバーセキュリティーリスクへの対応について、組織の内外に示すための「セキュリティポリシー」を策定することをはじめ、サイバー攻撃を受けた場合に備えて経営者が実践すべき内容を示しています。具体的には、「被害発覚後の通知先や開示が必要な情報項目の整理をするとともに、組織の内外に対し、経営者がスムーズに必要な説明ができるよう準備しておくこと」といった対策です。



このようにリスクへ対応するための体制構築をはじめ、リスク管理の枠組みや、リスクへの事前・事後対策など解説しています。想定される危機をイメージできるよう、対策を怠った場合のシナリオや対策の例もあわせて記載されています。

各項目の推進は当然重要ですが、注目すべきは、それらを推進する上で「CISO」や、組織においてインシデント対応などを行う「CSIRT（Computer Security Incident Response Team）」など、ビジネスとセキュリティーの間をつなぐ、いわゆる「橋渡し人材」の存在を前提として語られていることです。これはサイバーセキュリティー経営を実践する上での大きなポイントです。

企業の置かれているリスク環境を把握し、経営へ与える影響を他の役員へ説明したり、上層部で決定したセキュリティー戦略を組織へフィードバックする際の司令塔となるCISOは、非常に重要な役割です。経営層がセキュリティーに関してもリーダーシップを発揮するには、こうしたバックボーンが不可欠であることを、ガイドラインは示しています。

一方で、情報処理推進機構（IPA）が2015年に実施した「企業におけるサイバーリスク管理の実態調査」によれば、セキュリティーを専門に扱う役員「CISO」を任命している企業は、年間売上高10億円以上の大企業で38.3%、1～10億円の中堅企業で17.7%に過ぎません。

セキュリティー人材の不足が叫ばれており、今後、安定した企業運営において、マネジメント面、技術面からセキュリティーを理解し、効果的なセキュリティー対策を実践できる優秀な人材の確保こそ、「大きな鍵」となるでしょう。

2020年の東京オリンピック・パラリンピックに向けて、高まるセキュリティーリスク

2020年には、東京オリンピック・パラリンピック競技大会といった大きなイベントを控えています。世界から日本が注目され、かつ経済効果への期待が高まる一方、サイバー攻撃への懸念は拭い切れません。攻撃者にとっては、話題性のあるイベントはサイバー攻撃の格好の標的なのです。実際、2012年に開催されたロンドンオリンピック・パラリンピック競技大会では、ウェブサイトに対する攻撃だけでも約2億回に及びました。

さらにIoTの拡大やビッグデータ、人工知能など、サイバー空間とビジネスの関わり方も、大きな変化を迎えています。「国境」という壁がないサイバーの世界で、企業がいかに悪質なサイバー攻撃から自らの身を守り、事業継続性を確保していくか。「サイバーセキュリティ経営ガイドライン」は、経営者の大きな役割を示したと同時に、いかにセキュリティーガバナンスを推進するか課題を投げ掛けています。