経営相談 Q&A

「サイバーセキュリティ経営ガイドライン」の概要

Q 昨年6月、日本年金機構がウイルスメールの攻撃を受け情報が大量流出した事件がありました。2020年東京五輪を控え、日本を狙ったサイバー攻撃が増加する恐れがあるとも耳にします。そうした中、国が「サイバーセキュリティ経営ガイドライン」を公表したと聞きましたので、同ガイドラインの概要について教えてください。

A

1．ガイドラインの概要

様々なビジネスの現場でITの利活用は企業の収益性向上に欠かせないものとなっている一方で、取り扱う情報が大量かつ複雑化しており、サイバーセキュリティ対策は重要度を増しています。またサイバー攻撃は年々増加傾向で手口も巧妙化しており、企業は本格的な対応策をとることが求められている状況です。

経済産業省と情報処理推進機構（IPA）は昨年12月、民間企業向けのサイバーセキュリティ分野の経営指針となる「サイバーセキュリティ経営ガイドライン」を公表しました。同ガイドラインでは、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3原則」、および情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO※など）に対して経営者が指示すべき「重要10項目」をまとめています。

※CISO（Chief Information Security Officer）＝経営陣の一員、もしくは経営トップからその役を任命された、情報セキュリティ対策を実施する上での責任者のこと。

ダウンロードURL…
http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html

本ガイドラインには、セキュリティ担当者向けの資料として自社の現状を確認するための「サイバーセキュリティ経営チェックシート」なども添付されています。また本ガイドラインに沿ったセキュリティ対策を講じる企業に対しては、大手保険会社がサイバーリスク保険の保険料を割り引く

経営者が認識する必要のある「サイバーセキュリティ経営の3原則」

	項　　目	解　　説
1	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	・セキュリティ投資に対するリターンの算出はほぼ不可能であり、セキュリティ投資をしようという話は積極的に上がりにくい。また、サイバー攻撃などにより情報漏洩や事業継続性が損なわれるような事態が起こった後、企業として迅速かつ適切な対応ができるか否かが会社の命運を分ける。 ・このため、多様な経営リスクの中での一つのリスクとして、サイバーセキュリティリスクを経営リスクの中に適切に位置づけ、その対応について組織の内外に対応指針を明確に示しつつ、経営者自らがリーダーシップを発揮して経営資源を用いて対策を講じることが必要。その際、変化するサイバーセキュリティリスクへの対応や、被害を受けた場合の経験を活かした再発防止も必要。
2	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	・サプライチェーンのビジネスパートナーやITシステム管理の委託先がサイバー攻撃に対して無防備であった場合、自社から提供した重要な情報が流出してしまうなどの問題が生じうる。 ・自社のみならず、サプライチェーンのビジネスパートナーやITシステム管理の委託先を含めたセキュリティ対策を徹底することが必要。
3	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	・事業のサイバーセキュリティリスクへの対応等に係る情報開示により、関係者や取引先の信頼性を高める。 ・万一サイバー攻撃被害が発生した場合、関係者と、平時から適切なセキュリティリスクのコミュニケーションができていれば、関係者や取引先の不信感の高まりを抑え、説明を容易にすることができる。また、サイバー攻撃情報（インシデント情報）を共有することにより、同様の攻撃による他社への被害の拡大防止に役立つことを期待できる。 ・事業のリスク対応として平時から実施すべきサイバーセキュリティ対策を行っていることを明らかにするなどのコミュニケーションを積極的に行うことが必要。

（資料）経済産業省「サーバーセキュリティ経営ガイドライン」に一部加筆修正

制度も開始しています。

2．サイバーセキュリティ対策は重要な経営課題

IPA の調査によると、「サイバー攻撃への対応について取締役レベルで議論すべき」と考える企業が諸外国では約 9 割に達するのに対し、日本では 5 割に留まっています。日本年金機構の大量情報流出事件の社会的影響の大きさも記憶に新しいですが、世界的には、サイバーセキュリティは経営者がリーダーシップをとって積極的に関与すべき重要な経営課題だと考えられています。

本ガイドラインやチェックシートを参考にして、必要に応じて外部の専門家や専門企業の協力を仰ぎながら、自社に適したサイバーセキュリティ対策を早急に検討してみてください。

（吉村謙一）

経営者が担当幹部（CISO 等）に指示すべき「サイバーセキュリティ経営の重要 10 項目」

項目			対策例
リーダーシップの表明と体制の構築	1	サイバーセキュリティリスクの認識、組織全体での対応の策定	・経営者が組織全体の対応方針を組織の内外に宣言できるよう、企業の経営方針と整合を取り、サイバーセキュリティリスクマネジメントの方針（セキュリティポリシー）を策定する。
	2	サイバーセキュリティリスク管理体制の構築	・組織内に経営リスクに関する委員会を設置し、サイバーセキュリティリスクに責任を持った者が参加する体制とする。 ・組織の対応方針（セキュリティポリシー）に基づき、CISO 等の任命及び、組織内サイバーセキュリティリスク管理体制を構築する。CISO 等には、組織の事業戦略を把握するため取締役会への参加及び緊急時のシステム停止等の経営者レベルの権限を付与することを検討する。
サイバーセキュリティリスク管理の枠組み決定	3	サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定	・経営戦略に基づくさまざまな事業リスクの一つとして、サイバー攻撃に伴うリスク（例えば、戦略上重要な営業秘密の流出による損害）を識別する。 ・識別したリスクに対し、実現するセキュリティレベルを踏まえた対策の検討を指示。例えば、ソフトウェア更新の徹底、マルウェア対策ソフトの導入などによるマルウェア感染リスクの低減策を実施する。また、重要業務を行う端末、ネットワーク、情報システム又は情報サービス（クラウドサービスを含む）には、多層防御の導入や情報資産別のネットワークの分離等を検討する。
	4	サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示	・サイバーセキュリティリスクに継続して対応可能な体制（プロセス）を整備する（PDCA の実施体制の整備）。必要に応じて監査を受け、現状のサイバーセキュリティ対策の問題点を検出し、改善を行う。
	5	系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握	・系列企業やサプライチェーンのビジネスパートナーのサイバーセキュリティ対策の内容を契約書等で合意する。またサイバーセキュリティ対策状況（監査を含む）の報告を受け、把握する。
リスクを踏まえた攻撃を防ぐための事前対策	6	サイバーセキュリティ対策のための資源（予算、人材等）確保	・必要なサイバーセキュリティの事前対策を明確にし、それに要する費用を明らかにするよう、指示を行う。セキュリティ担当者以外も含めた従業員向け研修等のための予算を確保し、継続的にセキュリティ教育を実施する。 ・組織内人事部門に対して、組織内の IT 人材育成の戦略の中で、セキュリティ人材育成、キャリアパス構築を指示し、内容を確認する。
	7	IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保	・自組織の技術力を踏まえ、各対策項目を自組織で対応できるかどうか整理する。 ・委託先のサイバーセキュリティリスク対応を徹底するため、委託先のセキュリティレベルを契約書等で合意し、それに基づいて委託先の監査を実施する。
	8	情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備	・情報の入手と提供という双方向の情報共有を通じて、社会全体でサイバー攻撃の防御につなげることが重要。情報共有を通じたサイバー攻撃の防御につなげていくため、情報を入手するのみならず、積極的な情報提供が望ましい。
サイバー攻撃を受けた場合に備えた準備	9	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、定期的かつ実践的な演習の実施	・サイバー攻撃による被害を受けた場合、被害原因の特定および解析を速やかに実施するため、関係機関との連携や、ログの調査を速やかにできるようにしておくよう指示する。また、対応担当者にはサイバー攻撃に対応する演習を実施する。なお、インシデント収束後の再発防止策の策定も含めて訓練を行うことが望ましい。 ・初動対応時にはどのような業務影響が出るか検討し、緊急時に組織内各部署（総務、企画、営業…）が速やかに協力できるよう予め取り決めをしておく。訓練においては技術的な対応のみならず、プレスリリースの発出や、所管官庁等への報告手順も含めて想定する。
	10	被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備	・サイバー攻撃の被害が発覚後、速やかに通知や注意喚起が行えるよう、通知先の一覧や通知用のフォーマットを作成し、対応に従事するメンバーで共有。また、情報開示の手段について確認をしておく。 ・経営者が組織の内外への発表を求められた場合に備えて、サイバーセキュリティインシデントに関する被害状況、他社への影響などについて経営者に報告を行う。 ・インシデントに対するステークホルダーへの影響を考慮し、速やかにこれを公表する。社外への公表は、インシデントや被害の状況に応じて、初期発生時、被害状況把握時、インシデント収束時など、それぞれ適切なタイミングで行う。

（資料）経済産業省「サーバーセキュリティ経営ガイドライン」に一部加筆修正