経済産業省・ＩＰＡ 策定「サイバーセキュリティ 経営ガイドライン」

公益社団法人東京グラフィックサービス工業会
専務理事 斎藤 成

経済産業省では、IPA（独法・情報処理推進機構）とともに、「サイバーセキュリティ経営ガイドライン」を策定しました。このほど発表したガイドラインは、経営者のリーダーシップの下でサイバーセキュリティ対策を推進するためのもので、企業戦略として、IT に対する投資をどの程度行うのか、その中で、どの程度、事業継続性の確保やサイバー攻撃に対する防衛力の向上という企業価値のためにセキュリティ投資をすべきか注意喚起を促しています。同ガイドラインでは、IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象として、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がある「３原則」、及び経営者が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 最高情報セキュリティ責任者：企業内で情報セキュリティを統括する担当 役員等）に指示すべき「重要１０項目」をまとめたものであります。

経営の3原則

■サイバーセキュリティ経営の３原則

経営者は、以下の３原則を認識し、対策を進めることが重要である。

（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

【解説】

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えい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である。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である。

（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

【解説】

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

【解説】

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。 万一サイバー攻撃による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である。

サイバーセキュリティ 経営の重要 10 項目

経営者は、CISO 等に対して、以下の１０項目を指示し、 着実に実施させることが必要である。

1. 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

(2) サイバーセキュリティリスク管理体制の構築

2016.6

2. 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

（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

（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

3. 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

（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

（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

4. 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

（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

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 等に指示すべき「１０項目」

指示１：サイバーセキュリティリスクへの対応について、組織の内外に示すための方針（セキュリティポリシー）を策定すること。

指示２：方針に基づく対応策を実装できるよう、経営者とセキュリティ担当者、両者をつなぐ仲介者としての CISO 等からなる適切な管理体制を構築すること。その中で、責任を明確化すること。

指示３：経営戦略を踏まえて守るべき資産を特定し、セキュリティリスクを洗い出すとともに、そのリスクへの対処に向けた計画を策定すること。

指示４：計画が確実に実施され、改善が図られるよう、 PDCA を実施すること。また、対策状況については、CISO 等が定期的に経営者に対して報告をするとともに、ステークホルダーからの信頼性を高めるべく適切に開示すること。

指示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、自社同様に PDCA の運用を含むサイバーセキュリティ対策を行わせること。

指示６：PDCA の運用を含むサイバーセキュリティ対策の着実な実施に備え、必要な予算の確保や人材育成など資源の確保について検討すること。

指示７：IT システムの運用について、自社の技術力や効率 性などの観点から自組織で対応する部分と他組織に委託する部分の適切な切り分けをすること。また、他組織に 委託する場合においても、委託先への攻撃を想定したサイバーセキュリティの確保を確認すること。

指示８：攻撃側のレベルは常に向上することから、情報共有活動に参加し、最新の状況を自社の対策に反映すること。 また、可能な限り、自社への攻撃情報を公的な情報共有活動に提供するなどにより、同様の被害が社会全体に広がることの未然防止に貢献すること。

指示９：サイバー攻撃を受けた場合、迅速な初動対応により被害拡大を防ぐため、CSIRT（サイバー攻撃による情報漏えいや障害など、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）の整備や、初動対応マニュアルの策定など緊急時の対応体制を整備すること。 また、定期的かつ実践的な演習を実施すること。

指示１０：サイバー攻撃を受けた場合に備え、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。

2016.6

【事故事例】①

1台のパソコンがマルウエアに感染、原因はセキュリティソ フトの期限切れで……Ｐ社からの報告

プライバシーマークを付与されているＰ社から事故報 告が届いた。経緯は、契約しているインターネットプロバ イダーからＰ社にマルウエアに感染の疑いがあると連絡 がきた。早速、社内のパソコンを個々に点検したところ、 総務系の1台にトロイ型ウイルスがインストールされている可能性が確認された。 すぐに事故対策に乗り出し、感染したパソコンをネットから外し、関係者へ連絡すると共に、ベンダーへ対応を依頼した。ウイルス除去のためアンインストールができないため、クリーンインストールを実施、原状回復を行った。 今回の原因は、従業者が自身のパソコンのセキュリティソフトが期限切れであることに気付かず、システム管理者もその従事者の業務について「聖域」扱いで、日常の点検を 怠っていたとのこと。 安全確認が終わるまでの期間、パソコンが使用できず、 アナログ処理で対応し、再発防止策を講じた。 “アリの穴から堤も崩れる”の喩えのように、社内で例外を作ってはいけない教訓である。

【事故事例】②

ＤＭ発送の宛名データが別支店のものと入れ違いに…… ……Ｑ社からの報告

Ｑ社は、オンデマンド機でハガキの表の印刷とバリアブル 機能で宛名印字を両面印刷で行っている。大きな事故にはならなかったが、顧客から依頼された顧客への案内ハガキにおいて発送の宛名データと印刷データが2つの支店のものを処理した際に、案内状の内容が違っていたというもの。 経緯は、発注が代理店経由であったため、Ｑ社では指 示に従って印字、発送を行った。 Ｑ社の落ち度ではなかったものの、データが入れ違いになっていた。すぐに事故対策委員会を立ち上げ、緊急事態対応の体制を敷いた。幸い、エンドユーザからのクレー ムはなかった。顧客もプライバシーマークを付与されている業者だったため、責任は全て顧客側のデータ処理のミスとなった。ただ、エンドユーザへの補償の商品券の負担 は折半にしたとのこと。Ｑ社は「個人情報の事故」としての処理はせずに済んだが、ＩＳＯ9001の認証も受けているので、チェック体制に不適合があったと判断、品質面で の再発防止策を立て、今後は印刷データと宛名データの照合を品質と個人情報保護の両面から行うこととした。 顧客を信頼して業務を遂行することは当然だが、万が一を想定した2重チェックは必須である。

2016.6