第二部　JQAと始める情報セキュリティマネジメントの第一歩

当機構は、これから情報セキュリティマネジメントに取り組み始める企業が、まず自社の状況を把握するために利用することができるツールとして「情報セキュリティ簡易診断」サービスを開始しました。このサービスの特長や期待される効果について、企画センター ソリューションビジネス開発部 部長の宮下卓士に聞きました。

企画センター
ソリューションビジネス開発部 部長
宮下 卓士

新サービス「情報セキュリティ簡易診断」開始

今回新しく「情報セキュリティ簡易診断」を開発した背景をお聞かせください。

宮下　当機構は情報セキュリティマネジメントシステム（ISO/IEC 27001）の審査を長く行っていますが、認証取得に関するお問い合わせ・ご相談を受ける中で、情報セキュリティに関する取り組みの必要性を感じていても、実際に何から始めるのか、どのような対策を講じたら良いのか、という悩みを持っていらっしゃる企業が多いと感じています。特に製造業の場合、品質管理・製造技術などの知見や経験は多くお持ちですが、情報セキュリティ対策となると、知見や経験がやや少ないため、情報セキュリティ対策が進捗していないことが多いようです。

そのような情報セキュリティ対策を検討して実施することが、難しいと感じている企業に、基本的なことをJQAと一緒に確認することから始めませんか、というのがこのサービスを開発した意図です。

例えば「敷地内への人の出入管理」「パソコン利用者の登録」など、業種を問わず一般的に企業が実施する情報セキュリティ対策の基本があります。このような基本となる事項を、専門性を有するJQAの診断員と一緒に確認することで、「こういうところの対策をしていけばいいのか」ということがご理解いただけると思います。

情報セキュリティ簡易診断は、どのような流れで進めるのでしょうか。

宮下　情報セキュリティ簡易診断は、専用の「診断チェックシート」使って行います。お客さまにはまずこのチェックシートに沿って自社の状況を自己点検していただきます。その後JQAの診断員がお客さまを訪問し、チェックシート・自己点検結果を基にお客さまの情報セキュリティ対策の取り組みを評価します。チェックシート・自己点検でわからないところがあっても、診断員が一緒に診断しますので問題ありません。わからないところをどんどん診断員に聞いていただければと思います。

■ 図1　簡易診断の流れ

STEP 1 お申し込み	お申込み受付後、 診断実施日を調整
↓	
STEP 2 診断実施前	チェックシートに基づいてお客さまの状況を あらかじめ自己点検
↓	
STEP 3 診断当日	JQA認定診断員が訪問の上、 チェックシートおよび自己点検結果を基に 情報セキュリティ体制と運用・管理状況を診断

なお、このサービスに必要な日数と料金は、1日程度（約5時間）で、100,000円（税別）です。また、報告書は発行いたしません。

情報セキュリティマネジメントやISO/IEC 27001の知識がない状態でも受けてもいいのでしょうか。

宮下　全く問題ありません。ISO/IEC 27001の規格内容を見ても、具体的な情報セキュリティ対策のイメージがわかりにくいと感じる企業も多いでしょう。そのような企業にこのサービスを活用していただければ、情報セキュリティマネジメントの第一歩を踏み出していただくことができるサービスだと考えています。

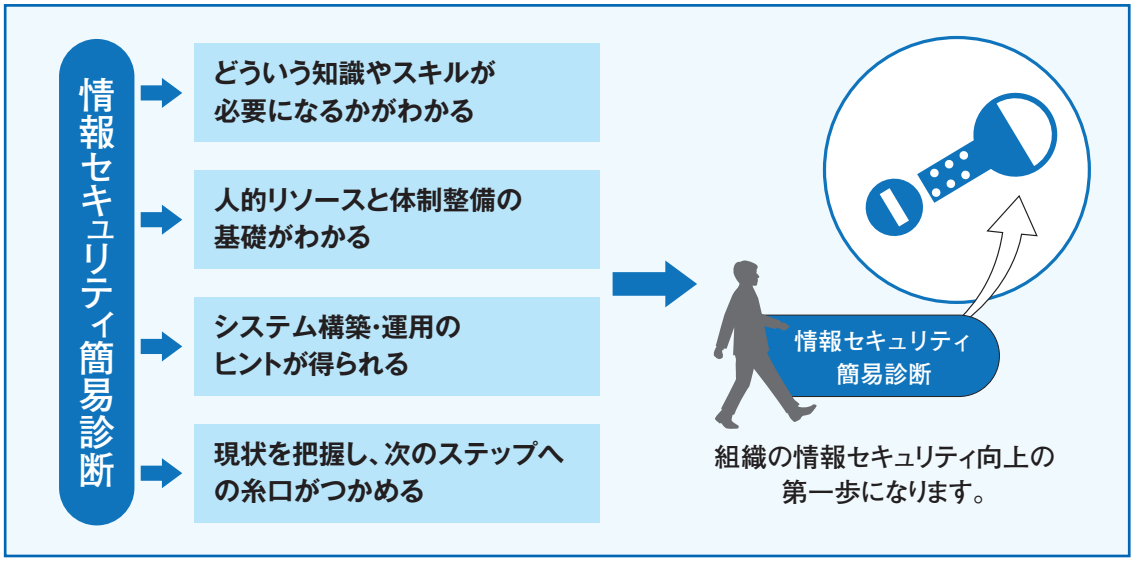
このサービスを受けることで、どのような効果が期待できるでしょうか。

宮下　情報セキュリティ対策に取り組むために、何をすればいいのかが明確になる、ということがいえるでしょう。企業の情報管理の現状を把握し、情報セキュリティ対策のために必要になる知識やスキル、人的リソースと社内体制などについて、取り組むべきポイントとのギャップを明らかにします。現状何ができているのか、また逆に何が不足しているのかがわかれば、しっかりした情報セキュリティマネジメントシステムを構築する道筋が描けるようになります。このサービスを利用することで、結果的に大きく回り道することなくISO/IEC 27001の認証取得を見通すこともできるのではないかと思います。

■ 図2 こんな組織におすすめです

- **取引先から情報セキュリティの取り組みを求められている組織**
- **情報セキュリティ対策として、何から手をつけていいのかわからない組織**
- **情報セキュリティ対策の必要性を感じながらも、始めるきっかけがなかった組織**
- **ISO/IEC 27001の認証取得を検討している組織**

■ 図3　期待される効果



情報セキュリティ管理基準による診断チェックシート

情報セキュリティ簡易診断で用いるチェックシートは、経済産業省策定の「情報セキュリティ管理基準」のうちの「管理策基準」に基づいて、企業が情報セキュリティに取り組むための具体的なチェックポイントがわかりやすく解説されています。

■ 図4　診断チェックシート（抜粋）

項　番	解　説	確認内容	判定	メモ
6.2 モバイル機器及びテレワーキング				
6.2.1 モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用する。	モバイル機器とは、スマートフォン、持ち出しするパソコン（無線を使ってインターネットに入ることを含む。）、ハンディターミナルなど、移動可能な機器を使う場合の会社としての方針（考え方）や使用方法などのルールを決めることです。 ここで言うモバイル機器を使用する上での方針は、5.1.1で記載した方針群の一つとなります。	モバイル機器を使用するための方針は作成しているか		
		モバイル機器を使用するための使用方法、禁止事項などルールを作成しているか		
7.3 雇用の終了及び変更				
7.3.1 雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、その従業員又は契約相手に伝達し、かつ、遂行させる。	従業員、派遣社員、パートタイマー、アルバイトなど全ての従業員が、退職する場合や人事異動で部署が変わる場合、退職者や異動者が行うべき責任や追っている義務の内容を明確にして、その人に内容を伝えて、遵守させることです。 例えば、退職者する方に、仕事で知った取引先や製造物などの情報を、同業者に話すことは禁止する、退職してもその責任を所有していることを伝える、退職時に退職後の機密保持合意書に署名してもらうなどです。 また、人事業務から営業業務などに異動する場合に人事情報へのアクセスの必要性はなくなります。（管理職で、部下の情報を見ることはあるえますが） 人事業務を行っていたときに知り得た従業員の情報などを他の従業員に話したりしてはいけないことを引き続き遵守することなどもあります。	退職時や異動時などに際して、情報セキュリティに対して引き続き所有する責任や義務を定めているか		
		上記で決定した責任や義務を従業員や（委託先などの）契約相手に伝達して、遂行させているか。		
8.1 資産に対する責任				
8.1.4 全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却する。	社員、契約社員、アルバイト、派遣社員といったあらゆる形態の従業員が、退職する場合は、全ての資産（パソコン、メールアドレス、職員手帳、社員証など）を返却することを要求しています。 直接雇用者のみならず、外部委託先なども対象です。 例えば、製品輸送を契約している運送会社に入門証を貸与しているが、その運送会社と運送委託契約が終了したときに入門証を回収する必要があります。 貸与品が、多いときなど貸与時に渡したものをリスト化して、受領サインをもらっておき、退職時にそのリストに基づいて返却物を確認することなどが、考えられます。	組織（会社）から離れる人々から、貸与した資産を全て返却させているか		
8.3 媒体の取扱い				
8.3.1 組織が採用した分類体系に従って、取外し可能な媒体の管理のための手順を実施する。	構築された分類体系に従って、媒体（HDD、USBメモリ、DVD、サーバのDISK装置など）に関する手順を構築することです。 8.2.1と8.2.3が、関連する対策です。 この項は、特に「取り外し可能な媒体」に対してですので、使用方法、使用者登録、暗号化、パスワード、持出、保管、データ復元を不可能にするなど、多岐にわたる管理方法を検討する必要があります。 これらの管理方法を検討して、管理方法を実施することとなります。	分類体系に従った取外し可能な媒体の管理手順が策定されているか		
		上記の管理手順に従って、取外し可能な媒体の管理が実施されているか		
11.1 セキュリティを保つべき領域				
11.1.1 取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。	サーバ、情報、製造技術（製造工程）、新規開発製品サンプル、顧客からの預かり品など情報や設備に対して、漏えい、盗難、火災や地震による破損などを起こさないために物理的な対策を講じることです。 設置の基準の例として、 ・ラックなどを設置している部屋は、上階の床下から、現在の床までの壁で囲う。 ・無窓とし、窓ガラスが有る場合は格子を設置し、飛散防止シートを貼る。 ・入室・退室の管理装置を設置する。 ・紙、サンプルなどの保管のため、中が見えない鉄製で、施錠できるロッカーを設置する。 ・敷地に不正侵入されないように外周に侵入センターを設置する。 ・死角や重要な部屋の出入口に監視カメラを設置する。 ・敷地への門や一般訪問者の建物出入口などに受付を設置し、社員や一般者の入門を管理する。 などが、考えられます。 新しいセキュリティ対策機器が、開発されるため、基準も見直していく必要があります。 設備投資がかかる事柄が多く、全てを設置しなければならないものではありません。投資計画に反映しながら、物理的対策を向上させていくことになります。	敷地、部屋、設備に関して物理的なセキュリティ対策を行う具体的な基準を定めているか		
		上記で定めた物理的なセキュリティ対策の基準に基づき、セキュリティ対策機器などを設置しているか		

「情報セキュリティ管理基準」は、業種や規模を問わず幅広い組織が適用できる実践的な情報セキュリティの規範として、国際規格ISO/IEC 27001およびISO/IEC 27002に準拠する形で策定された基準です。このため、簡易診断はISO/IEC 27001とも整合性を持っており、組織が情報セキュリティ体制を国際標準に発展させていくことにもつながります。