特集Ⅱ

いまから取り組む製造業の情報セキュリティマネジメント

第一部　まずは身の丈にあったシステムから

モノのインターネット(IoT)化や人工知能(AI)技術が製造業を含む産業全体に普及し、情報セキュリティマネジメントに取り組む重要性が高まっています。しかしながら、製造業においては、情報セキュリティマネジメントの取り組みが十分に浸透しているとはいえないのが現状です。第4次産業革命と呼ばれる技術革新による変化の中で、製造業はどのようなリスクにさらされているのか、対応するにはまず何から手をつけるべきなのか、ISO/IEC 27001主任審査員の川合浩司が解説します。

ISO/IEC 27001主任審査員
CSMS主任審査員
川合 浩司

製造業における情報セキュリティのいま

急速に高まる情報セキュリティ対策の必要性

あらゆる産業において品質管理やコストダウンのためのIT化が着実に進められてきましたが、近年急速に普及しているIoT化や人工知能は産業や社会を根底から変えると言われています。これに伴って情報セキュリティリスクも増大しており、対策を行うべき範囲は急速に拡大しています。

また、一つの企業が抱えるリスクのサプライチェーン全体への影響も考慮する必要があります。例えば近年では、情報セキュリティが堅牢なターゲットを攻撃するために、まずサプライチェーン内で比較的防御の甘い取引先を狙い、そこを踏み台にターゲットである企業を攻撃する手法が頻発しています。この場合、踏み台に利用された企業は結果的に加害者になってしまい、その後の取引に重大な影響を及ぼすことが懸念されます。

このように、情報セキュリティに関するリスクは一企業にとどまらずサプライチェーン全体に影響を及ぼすようになっているため、取引先に対して情報セキュリティの取り組みの強化を促す企業が増えています。実際に、取引先から情報管理の取り組みについて問われたことがあるという企業は多いのではないでしょうか。

情報セキュリティについての誤解

しかし、製造業においては、情報セキュリティマネジメントの取り組みが十分に浸透しているとはいえないのが現状です。

これには、情報セキュリティというと、「個人情報保護」に注目し「当社はモノ作りだから、それほど重要な個人情報は持っていない」と考えがちなことも一因としてあるかと思います。しかし多くの製造業では、取引先の情報、設計情報、品質情報、製造ノウハウなど、いったん漏洩すると事業に大きな影響を与える可能性がある情報を保有しています。それらの情報をしっかり守る

ことが求められているのです。

さらに、情報セキュリティというのは、情報漏洩対策に限ったものではありません。情報を必要なときに使用できるように管理することも需要です。例えば、生産ラインを動かす制御系システムのデータが壊れてしまうと生産ラインが止まってしまうというリスクが考えられます。「必要なときに使えるように情報を管理する」ということもまた、情報セキュリティにおいて重要な要素の一つです。

製造業の情報セキュリティとは何か

製造業が取り組むべき情報セキュリティとしては、①お客さまから預かった設計図などの情報や自社が保有している情報の機密性を保持すること、②自社の生産ラインを稼働させるための情報（受発注データなども含む）を必要なときに利用できるようにすることが考えられます。

①は自社の信頼と競争力に関わる問題です。製造業には外部に漏れてはならない情報が数多くあります。取引先から預かった情報が漏れれば、企業の信用は失墜します。そのほかにも、企業は競争力の源泉となる固有技術や知的財産、新製品の開発情報を保有しています。合併や買収、事業提携に関する情報もあるでしょう。これらの情報を共有する範囲を決め、許可された者以外アクセスできないようにしっかりと管理する必要があります。

②は生産の継続性に関わる問題です。生産設備を動かしている情報（例:加熱温度と時間・加工内容など）が壊れてしまえば、品質の低下や製品事故の原因になったり、生産ラインが止まってしまったりします。生産システムの多くがコンピュータによってコントロールされている現在、データが破壊されてしまうことのほかにも、サポートされていない古いソフトウェアで動いているパソコンのデータが使えなくなるなど、リスクにはさまざまなものが考えられます。増大するリスクへの対応の甘さは、製品の品質や生産活動そのものに多大な影響を与える可能性があります。

ISO/IEC 27001は変化する脅威に対応する仕組み

ISO/IEC 27001は、情報セキュリティマネジメントシステムを確立・実施・維持し、継続的に改善するための国際規格です。

情報セキュリティに取り組むうえでポイントとなるのは、リスクマネジメントの考え方です。情報技術の進歩は非常に速く、また企業の事業内容や製造体制も変化していきます。情報セキュリティ対策はある時点では最新、完璧の対策であったとしても、すぐに陳腐化したり実情にそぐわなくなったりする可能性があります。変化する環境に対応するために、ISO/IEC 27001には、想定される潜在的なリスクへの対策を選択し、継続的に改善していくPDCAの考え方が取り入れられています。

認証機関によるISO/IEC 27001の審査を受けることで、企業自身が気づいていないリスクに気づくということもあります。情報を取り巻く状況が激しく変化する中で、一つの企業だけで全ての変化に適切に対応す

るのは簡単なことではありません。審査を受けることで定期的に第三者の視点でチェックする仕組みが整いますから、情報セキュリティに取り組むうえで非常に有効だといえるでしょう。

また、ISO/IEC 27001の特長として、対策が必要な情報セキュリティリスクに対してどのように対応すべきかを示す管理策が、必要な対策の見落としを防ぐためにあらかじめ示されているということがあげられます。情報セキュリティのための方針群、組織、人的資源、資産、アクセス制御など14の箇条にわたって管理策が記載されており、ISO/IEC 27001に取り組む企業は、自社の状況や、情報セキュリティリスクに合わせて必要な管理策を参照することができるのです。

情報セキュリティマネジメントシステム構築のポイント「リスクアセスメント」

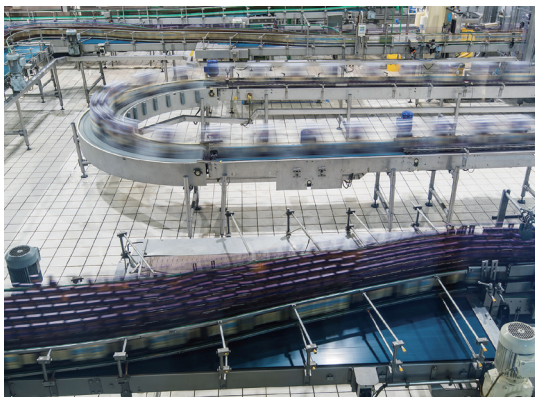
ここからは、情報セキュリティマネジメントシステム構築の重要なポイントである「リスクアセスメント」の進め方を解説します。

リスクアセスメントとは、情報セキュリティに関するリスクを洗い出し、その特性やレベルを分析・評価することです。まず自社が持つ情報および情報処理施設に関連するその他の資産（以下、情報資産）に関するリスクを明確にすることから始めるのが良いでしょう。

情報資産の一覧を作成し、分類する

情報資産に関するリスクを明確にするためには、そもそも企業がどんな情報資産を保有しているのかを洗い出す必要があるため、まず目録を作成します。企業は、設計図や注文書、顧客データのような情報そのもののほかに、そのような情報を取り扱うためのコンピュータシステム、ネットワークなどの情報資産を保有しています。これらの情報資産を棚卸しして一覧を作成します。個々のデータを十把ひとからげに並べるのではなく、それぞれの情報資産の特性（例:紙／電子データ、保管場所など）に応じて分類していくと、この次のリスク分析を行う上で良いでしょう。

最近は情報システム自体を外部の情報通信システム会社に委託したり、データのやり取りや保存場所としてクラウドのような外部のサービスを利用している



■ 図1　情報資産の例

分類	資産の例
ハードウエア	サーバ、クライアントパソコン、周辺機器、ネットワーク機器
ソフトウエア	OS、アプリケーション、ユーティリティ
データ	顧客情報、受注情報、経理情報
記録媒体	磁気記録、光記録、その他バックアップ
施設・設備	社屋、サーバルーム、空調設備、防火設備、電源装置
紙媒体・書類	契約書、手順書、規程集
人間	正社員、契約社員、顧客

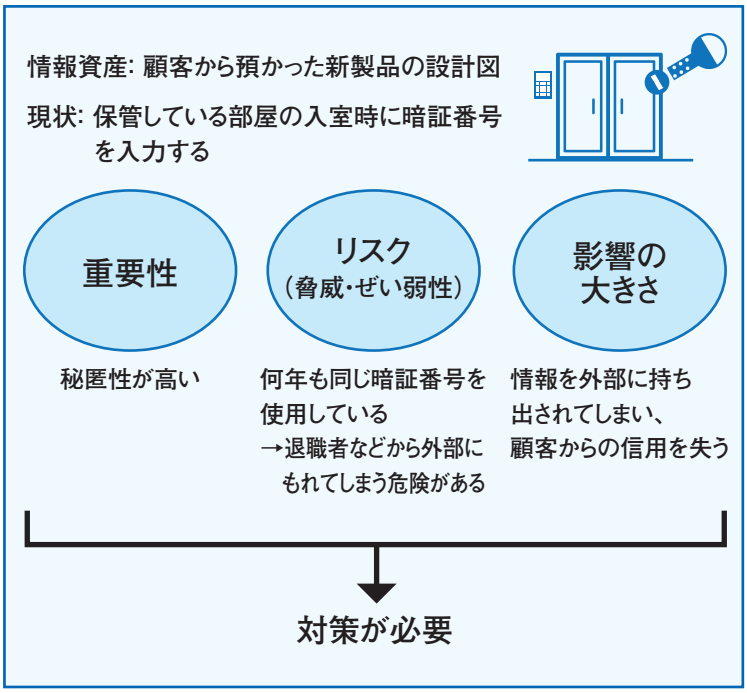
ケースも増えています。このように一見すると社内にはない情報も、企業の情報資産としてリストアップするのを忘れないように注意してください。

現状を把握し、リスク分析を行う

目録によって企業にどのような情報資産があるか明らかになったら、重要性、考えられる脅威、脅威に対するぜい弱性（つけこまれやすさ）、事故が発生した場合の影響の大きさなどの観点からそれぞれの情報資産を分析し、評価していきます。そして、優先順位の高い情報セキュリティリスクを特定します。

リスク分析によって、それまで気づかなかった現状に潜むリスクが明らかになることもあります。例えば、「データの受け渡しにUSBメモリやディスクなどの媒体を使っている」という運用がされており「ネットワークにつながっていないから問題になることはない」と考えていたとしても、媒体そのものが壊れたり紛失してしまったりする、あるいは媒体経由で生産システムがウイルスに感染するという脅威が発見されることもあります。全てのリスクに自力で気づくのは難しい面もあるため、まずはこのリスク分析の部分を外部の専門家に手伝ってもらうという方法も考えられるでしょう。

■ 図2　リスク分析の例



リスク分析の結果に基づいて対応方法を決める

分析の結果、それぞれのリスクに対して、どのような対応をとるのかを決めます。ここで参照するのが管理策です。企業は、リスク分析の結果明らかになった自社の状況に応じて「この管理策を実施する」「この管理策は状況に合わないので採用しない」という決定を行います。例えば、開発を全く行っていない企業であれば、開発に関する管理策を採用する必要はないでしょう。もちろん、企業の状況に合った管理策が規格に載っていなければ、他の方法を採用して対応します。

■ 図3　特定されたリスクへの対応の例

（図2の場合）

入室に使用する暗証番号に対する変更のルールを定めて実行する
（管理策 A.9.3.1）

企業によって抱えるリスクは異なりますから、リスク分析の結果、企業が具体的にどのような管理策を講じるのかはさまざまです。例えば「書類を鍵のかかるキャビネットに入れる」としている会社（A）もあれば、そうではない会社（B）もありますが、そのために会社（B）が直ちに要求事項に対して不適合となるわけではありません。会社（B）はキャビネットのある部屋自体の入退室を厳重に管理し、関係者以外の入室を厳しく制限しているためキャビネットに鍵をかける必要はない、という判断がされているのであれば、リスク分析の結果に基づいた対応がとられていると言えるでしょう。書類のセ

キュリティを確保するために「部屋の出入りの管理を厳重にする」、さらに「キャビネットに鍵をかける」など、どこまでの対策を行うことにしても、それがリスク分析の結果とひもづいていれば良いのです。

リスク分析の結果、「対策を講じない」つまり「リスクを受容する」、と判断することもまた対応方法の一つです。その場合も、そのリスクの持つ影響の大きさや発生可能性の高さ、対策にかかるコストといった要素を総合的に分析し、企業としての判断が対応方法に反映されていることが重要です。

ISO/IEC 27001の審査で認証機関は、このようなリスク分析の妥当性を重視しています。どのようにリスク分析を行い、その結果を反映した対応がとられているかがポイントとなります。

実施する管理策が決まったら、企業は管理策の適用状況（適用する管理策／適用しない管理策、その管理策を適用しない理由など）を記載した「適用宣言書」を作成します。適用宣言書を作成することで、その企業が情報セキュリティに関してどのような管理策を講じているのかが一目でわかるようになります。

トップのリードで身の丈にあったシステムを構築し、成果を上げる

情報セキュリティマネジメントシステムの担当者に必要なスキルとは

ISO/IEC 27001に基づいた情報セキュリティマネジメントシステムを構築し運用するには、マネジメントシステムに関する知見やスキルに加え、情報システムに関する知見やスキルも求められます。とはいえ、企業によっては両方の知見やスキルを兼ね備えた人材が確保できないこともあるでしょう。

その場合は、マネジメントシステムのスキルのある従業員とITの素養のある従業員とがペアを組んで進める方法が考えられます。もしISO 9001の認証を取得している企業であれば、その事務局担当者もしくは経験者とともに、情報システムの運用に携わってきた担当者が協力してシステムを構築すると効果的でしょう。

目的と範囲を明確にして外部のリソースも活用する

企業内部のリソースが足りない場合、コンサルタントやシステムインテグレーターなどのIT専門企業、近年経済産業省が養成を進めている中小企業向けの情報セキュリティ専門家などの外部リソースを活用する方法もあります。その場合、システム構築・運用のどの部分を外部リソースに依頼するのか、すなわち外部リソースに何を期待するのかを具体的に決めておくことが大切になります。認証取得までを段階的に考えると、「リスク分析の部分を手伝ってください」「具体的な手順書を作ってください」「手順書の作成と教育を行ってください」「内部監査のやり方のアドバイスをください」「登録審査をサポートしてください」というような依頼内容になっていくでしょう。ただし、外部リソースに任せっきりにしてしまい、企業の実情に合わない重たいシステムを構築してしまう危険性には十分注意してください。外部からのアドバイスを受けることの目的は、あく

までも最終的に内部リソースだけでマネジメントシステムを回せるようにすることにあります。

また、まず情報収集をするというのであれば、独立行政法人 情報処理推進機構（IPA）が提供するウェブサイトの情報セキュリティに関するコンテンツやセミナーなどのイベントは参考になるでしょう。もちろんJQAでも、新たにISO/IEC 27001の導入を検討している企業のためのセミナーや、業務相談や予備評価などのサポートサービスを用意しています。また、これから新たに情報セキュリティに取り組もうとする企業を対象とした「情報セキュリティ簡易診断」（→第二部 29ページ参照）のサービス提供も開始しました。企業の状況に応じて、適宜このような外部サービスを利用していくと良いでしょう。

トップマネジメントの判断のもと、メリハリをつけて取り組む

これは他のマネジメントシステムにも共通していえることですが、内部のリソースを活用するにしても、外部に委託するにしても、いずれにしてもうまくマネジメントシステムを構築・運用していくためにはトップマネジメントの理解と関与が不可欠です。トップの号令のもと、組織体制を作り、企業の状況に合った情報セキュリティの方針を定めて、全社をあげて取り組めるようにしなければなりません。

JQAの審査では最初に経営者へのヒアリングを行いますが、そこで、経営者がどれくらい本気なのか、セキュリティに対してどのような企業文化を持っているかなどを確かめています。「入札参加資格になっているからISO/IEC 27001の認証を取得する」「競合他社がやっているからうちもやる」というような判断で取り組み始めた企業もあるようですが、やはり、外部環境の変化に対応しながら継続的な改善を実践していくためには、経営者の本気の関与が重要だと思います。

最後に、ISO/IEC 27001の取り組みで成果を上げるために大切なことは、常に身の丈に合った情報セキュリティマネジメントシステムの維持に気をつけることです。

ISO/IEC 27001は現状を把握しリスクに優先順位をつけて取り組むものです。あまり難しく考えずに、トップマネジメントの判断のもとメリハリをつけて取り組み、身の丈にあったマネジメントシステムを構築しPDCAを回していくことで、少しずつレベルアップすることを目指すのが良いでしょう。

■

情報セキュリティマネジメントに取り組まれる製造業のお客さまのお問い合わせ先

一般財団法人 日本品質保証機構
マネジメントシステム部門 企画センター
カスタマーリレーション部
TEL: 03-4560-5710
E-mail: ms-suishin@jqa.jp

※当機構は製造業を熟知した情報セキュリティマネジメントシステム審査員を擁しています。情報セキュリティ簡易診断を含めお気軽にお問い合わせください。