特集I

製造業の情報セキュリティマネジメント

IoT（モノのインターネット）が進み、産業界全体が第4次産業革命ともいわれる大きな構造変化に向かおうとしている。ものづくりの革新も急速に進み、製造業における情報資産が急速に膨らみ始めており、リスクも拡大している。この結果、製造業でも情報セキュリティリスクを適切に管理する必要が高まり、情報セキュリティマネジメントの確立が新たな取引条件になろうとしている。本特集では、政府が第4次産業革命を踏まえて目指すべき未来社会として示すSociety 5.0とともに、製造業における情報セキュリティマネジメントシステム導入の意義とISO/IEC 27001活用事例を紹介する。

第一部
巻頭インタビュー

目指すべき未来社会、Society 5.0。

内閣府 政策統括官（科学技術・イノベーション担当）付
（総合科学技術・イノベーション会議事務局）
参事官（社会システム基盤担当）
布施田 英生 氏

経済的発展と社会課題の解決を両立させるSociety 5.0

ICTの先端技術の急速な進歩による第4次産業革命といわれる大変革が進行しています。政府は、科学技術イノベーションを成長戦略の重要な柱と位置付けており、この第4次産業革命を踏まえてわが国が目指すべき未来社会の姿としてSociety 5.0を示しています。

Society 5.0とは、「狩猟社会、農耕社会、工業社会、情報社会に続く新たな経済社会であり、サイバー空間とフィジカル空間を高度に融合させることにより、経済的発展と社会的課題の解決を両立し、人々が快適で活力に満ちた質の高い生活を送ることのできる、人間中心の社会」です。第4次産業革命によって経済を成長させていきながら、少子高齢化に伴う労働生産人口の減少やエネルギー資源確保の問題など社会課題も解決していくところがポイントです。

Society 5.0は、内閣府に設置された総合科学技術・イノベーション会議（CSTI）が、2016年度から2020年度の「第5期科学技術基本計画」の中で提言した概念です。安倍総理大臣を議長に、関係閣僚、学界、産業界の有識者によって構成されるCSTIが提言したSociety 5.0は、2016年1月の閣議決定を経て、産学官がともに実現を目指す国家ビジョンとなっています。

Society 5.0実現のための仕組みを策定

現在、CSTIが司令塔となり、関係官庁や機関が連携して、Society 5.0を強力に推進する取り組みが始まっており、2016年度には、Society 5.0を実現するためのプラットフォーム（基本的な仕組み）を策定しました。まず、Society 5.0で実現する代表的なシステムとして11のシステムをあげ、そのうち「高度道路交通システム」「エネルギーバリューチェーンの最適化」「新たなものづくりシステム」の3システムをコアシステムとして開発し、他のシステムとの連携協調を図りながら新たな価値を創造することとしました。

また、新たな価値やサービスのもとになるデータベースの構築を進めるとともに、プラットフォームを支える基盤技術として、AI（人工知能）技術、IoT（モノのインターネット）システム技術、ネットワーク技術、ビッグデータ解析技術、サイバーセキュリティ技術等を強化していきます。

さらにプラットフォーム構築のための環境整備として、知的財産戦略と国際標準化の推進、規制・制度改革の推進と社会的受容の醸成、能力開発・人材育成の推進を行います。

データの自由な流通のため、セキュリティの高度化を進める

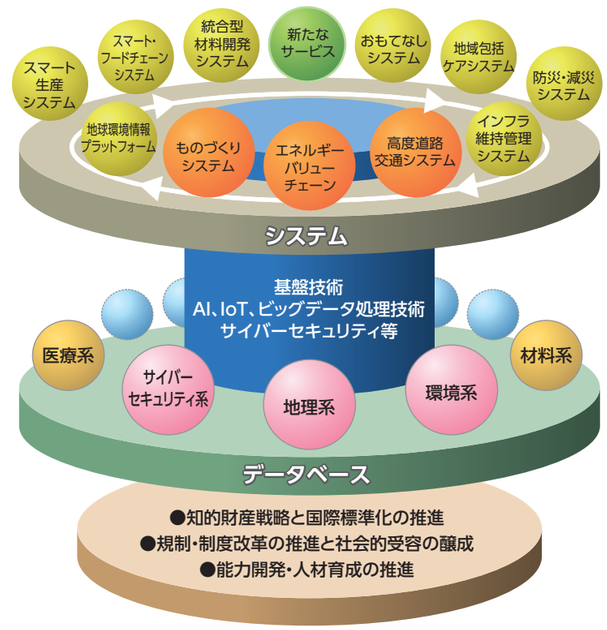
Society 5.0では、各分野のシステムが常に情報を吸い上げて、分析し、社会に還元して価値を生み出していくようになります。業界や分野をまたいで情報を活用していくデータ駆動型社会をさらに深化していく社会ともいえます。

それを実現する仕組みとして、現在、交通、エネルギー、インフラ管理などさまざまな分野が共通に利用できる三次元地図情報、映像情報、地球環境情報、ヒト・モノ・車情報、異業種間データ流通促進情報の5つのデータベースの整備を推進しています。

例えば、自動走行システムには走行中の自己位置推定や走行経路の特定のためにダイナミックマップといわれる高精度な三次元地図情報が必要です。このダイナミックマップを、AIを用いて自動的に生成できるようにするとともに、防災・減災やインフラ維持管理などでも共通に利用できるようにする仕組みを開発していきます。

このように、業種や分野を超えてデータが自由に行き交う環境では、高度なレベルでのセキュリティの確保が必要になります。単に機器のセキュリティを確保するだけでなく、サイバー空間全体のセキュリティ技術の高度化が必要であり、そのための研究開発を推進していきます。また、製品やサービスを提供する際には、企画・設計段階からセキュリティ確保を盛り込むセキュリティ・バイ・デザインの考え方をもち、セキュリティ品質を実現することが欠かせません。セキュリティ品質を確保するための費用はコストでなく価値を生み出すための投資であるという考えが一段と大切になるでしょう。

■ Society 5.0　プラットフォーム構築のイメージ



Society 5.0を新たなビジネスチャンスに

Society 5.0実現に向けて、産業界でも政府や学界と一体となった取り組みが始まっています。

一般社団法人 日本経済団体連合会（経団連）は、2017年2月14日に「Society 5.0実現による日本再興　～未来社会創造に向けた行動計画～」を発表し、Society 5.0を実現するための基盤となる領域を「Society 5.0実現官民プロジェクト」として実行するとしています。

一般社団法人 産業競争力懇談会（COCN）では、2017年2月23日に発表した「Society 5.0とCOCNの推進テーマ　～国と産業界の投資を集中すべき分野と政策～」の中で、Society 5.0重点貢献テーマ20件を抽出して、産業化、事業化を推進しています。

さらに、内閣府が主体で推進しているプログラムである「戦略的イノベーション創造プログラム（SIP）」でも、Society 5.0に向けた取り組みが進んでいます。

このような、産学官が連携した強力な推進体制により、「自動走行システム」など先行して開発が進むシステムは、2020年ごろにはその具体的な姿が見られるようになる見通しです。

今後は、一般企業の方々にとっても、Society 5.0の実現に向けた取り組みに参画される機会が急速に広がっていくと考えられます。Society 5.0は、未来に向けて企業の国際競争力を高め、新たな価値を創造し、ビジネスチャンスを広げる機会を提供するものになります。ぜひ、Society 5.0に関心をもっていただき、参画をご検討いただければ幸いです。 ■

第二部

これからの製造業を支える情報セキュリティマネジメントシステム

製造業の情報通信技術の活用範囲は、設計や製造工程から付加価値を生み出す工程全体へと着実に拡大・浸透し、情報セキュリティの必要性が高まっています。JQA審査事業センター 情報審査部 部長の秋山宏幸が、第4次産業革命ともいわれる産業構造や社会システムの変革が見込まれるなかで、製造業が情報セキュリティマネジメントシステムに取り組む意義を語ります。

審査事業センター
情報審査部 部長
秋山 宏幸

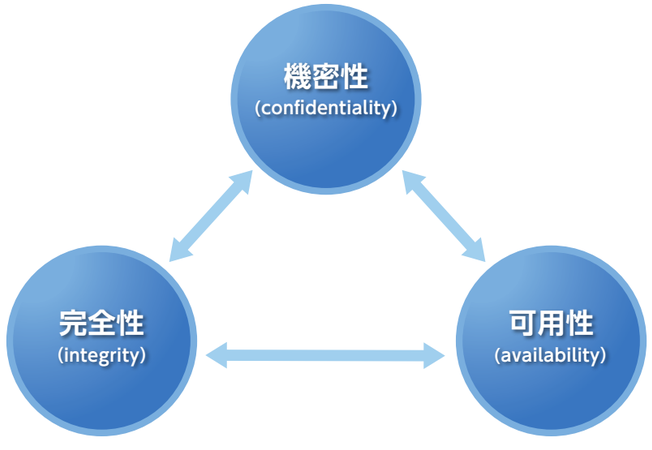
情報技術の進化で大きく変わる製造業の姿

情報セキュリティマネジメントシステムISO/IEC 27001は、組織にとって経営上の重要な課題となった情報セキュリティの対策を行う際の行動規範や基準となる考え方を示した規格として制定されました。この規格の中で、「情報セキュリティ」とは、「情報の機密性(*1)、完全性(*2)及び可用性(*3)を維持すること」と定義されています。つまり、機密情報を洩らさないだけでなく、情報が改ざんされることなく、必要なときに利用できる、言い換えれば安全性と利便性のバランスを適切に確保するための規格といえます。

かつて、情報を紙の書類や図面だけで管理していた時代には、保管場所を厳重に施錠すれば情報の安全性を確保することができました。しかし、パソコンやサーバー、LAN、インターネットが一般的に用いられるようになると、組織の情報に接触する経路や接続点が増大し、そこから第三者が情報システムに侵入したり情報が漏えいしたりするリスクを適切に管理することが求められるようになってきました。

いま、情報通信技術の発達により、革新的な技術やサービスが続々と登場しています。IoT(モノのインターネット)やビッグデータ、AI(人工知能)の活用が急速に進んでおり、身近なところでもスマートフォンやクラウドコンピューティングなどがめざましい勢いで普及しています。それに伴い、重要な情報を管理するリスクは一段と高まっているといえます。サイバー攻撃やウイルスなどの攻撃によるものに加えて、ヒューマンエラーや内部不正など人的管理の隙を突いた脅威なども、情報セキュリティ事故につながっています。このような情報セキュリティ事故は、組織の信用、評判を落とすばかりでなく、事業活動の停滞や財務的損失など、さまざまな不利益がもたらされることになります。

■ 情報セキュリティの3つの構成要素



ISO/IEC 27001は、これらの情報セキュリティのリスクを適切に管理するための規格であり、情報システム会社やデータセンター、ソフトウェア開発、インターネット関連企業などの情報通信分野の企業や、広告・印刷業界、産業廃棄物処理業など、事業活動で機密情報を扱う業種を中心に認証の取得が進んできました。

しかし、現在は、ものづくりを本業とする製造業でも、情報セキュリティへの関心が高まりつつあります。製造業でもIoT、ビッグデータ、AIなどの先進情報技術を活用していくことが、経営の重要なテーマになってきたことが影響していると考えられます。

政府はこれらの先進技術によるブレークスルーがもたらす、「第4次産業革命」といわれる産業構造の大変革を日本企業がグローバルな市場と付加価値を獲得する方向で推進し、日本経済の成長の柱にしようとしています。製造業もこうした大変革の時代を前に、情報技術を使いこなすことが成長の基本条件となり、それに伴って増大する情報セキュリティリスクに取り組むことがますます重要になってきています。

製造業における情報セキュリティとは

製造業の情報セキュリティの課題は、将来に向けて急速に高まっていくことが予想されますが、実は現在でもさまざまな課題があるといえます。実際の製造現場で、情報セキュリティが確保できていない場合に想定されるトラブルを考えていきます。

まず、製造業には外部に洩れてはならないさまざまな情報があります。競争力の源泉となる自社の固有技術やノウハウ、知的財産権、製品の設計情報などはもちろんのこと、開発段階の情報も機密性が求められます。誰でも入手できるような製品でも、試作品や開発途上の製品が流出すれば大きな問題になります。また、さまざまな契約内容や取引条件、原価計算、見積もりや価格などの営業情報も外に洩れてはならない情報です。これらの情報が、コンピュータで作成され、サーバーに保管され、ネットワークを介してやり取りされるようになるなか、組織はこうした情報の機密性を厳重に確保しなければなりません。

受発注システムのセキュリティも重要な課題です。受発注ミスや受発注システムの不具合で、製造に必要な原材料や部品が正しい数量で納期に届かなければ、製品が作れなくなることも考えられます。

製造工程の管理もコンピュータ化が進んでいます。工場の生産システム、制御システムにおいて、使う部品や、工程の運転情報(例:加熱温度と時間、加工内容など)が正しく伝わらない、検査システムが正しく機能しないなどの事象が発生すれば、不良品の発生や重大な製品事故の原因になりかねません。

製造にかかわる情報セキュリティは、サプライチェーンの中でも厳重に確保される必要があります。製造業のセットメーカーのもとには、原材料、機械、電気・電子、情報通信、その他サービスなどさまざまな業種にサプライチェーンのすそ野が広がっています。サプライチェーンを束ねるセットメーカーは、サプライヤーである素材や部品メーカー、サービス供給者に自社と同じレベルの情報セキュリティを求めることになります。サプライヤーは、製品の設計情報はもとより、仕様や発注内容など、顧客から預かったさまざまな機密情報を守る義務を負っています。複数の顧客から受注する場合、ある顧客のための製造工程が他の顧客に洩れないようにするため、製造現場を分けたという例もあります。

同様にサプライヤー自身も、部品やサービスなどの調達先の情報セキュリティを厳しくチェックしなければなりません。サプライチェーンの中で受発注システムを共有する場合、セキュリティの弱いサプライヤーのコンピュータが標的型攻撃で乗っ取られて、何年もかけて取引先のセットメーカーのコンピュータをこじ開け、機密情報が漏えいした事件も起きているからです。

このため、自動運転が視野に入ってきている自動車産業や、急速な成長が見込まれる航空宇宙産業をはじめ、すでに多くの産業の取引でISO/IEC 27001同等の情報セキュリティが推奨または要求されているようです。

また、これまで通信機能を持っていなかった製品にもソフトウェアやマイクロコンピュータが組み込まれ、インターネットにつながるようになっています。家庭でも、DVDレコーダーなどの映像情報機器、エアコンや洗濯機、炊飯器、ホームセキュリティ機器が、外部からスマートフォンで簡単に操作できるようになっています。これらの製品のメーカーは、製品が使用される局面まで広げて情報セキュリティを考慮しなければなりません。さらに、IoTの時代になると、製品自体がインターネットを介して情報をやり取りしたり、使用状況がビッグデータとしてサーバーに蓄積され、分析処理されたりするようになります。製造業にとっての情報セキュリティの範囲がさらに拡大し、重要性が飛躍的に

高まっていきます。

今後、製品の情報化が進展していくなかで、製造業にとって情報セキュリティは品質と同様に重要になっていくと考えられます。

ISO/IEC 27001を利用して情報セキュリティを継続的に改善する

それでは、ISO/IEC 27001を導入、運用すると、どのように情報セキュリティを強化できるのでしょうか?

ISO/IEC 27001の特長は、組織の情報資産にかかわるリスクを明確にすることができることです。それまで漠然と感じていた情報セキュリティのリスクを明確に認識でき、正しい現状判断のもと、組織をあげた的確な対策が可能になります。

ISO/IEC 27001に取り組む組織は、組織にどのような情報資産があるかの目録を作り、それぞれの情報資産の機密性、完全性、可用性の喪失に伴うリスクを評価し、その評価結果から何らかの対策を行わなければならないリスク項目を明確にしていきます。

ISO/IEC 27001の2つ目の特長は、明確になった、対策が必要なリスクに対してどのように対応すべきかの管理策が示されていることです。

規格の附属書Aには、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、暗号など14の箇条に分けて、合計114の管理策が掲載されています。組織は、これらすべての管理策を実施しなければならないわけではなく、また、附属書Aに掲載されていない管理策を採用することもできます。組織が取り組む管理策を決定したら、附属書Aの管理策を参照して、対策に漏れがないか確認ができます。

管理策を決定したら、組織は必要な管理策とそれらの管理策を含めた理由を記載した「適用宣言書」を作成します。

ISO/IEC 27001に取り組むことで、組織は明確な基準を持って情報セキュリティリスクを認識でき、対策に優先順位が付けられるので、経営者の判断が適切に行えるようになります。

例えば、中堅・中小企業では、社内システムの構築をシステムインテグレーター（SI会社）やITベンダーに外注していたり、一部の社内担当者に一任していたりするケースが多く見受けられます。この場合、組織が守らなければならない情報資産がSI会社などに正しく伝わっているか、目指すべき情報システムがきちんと構築されているかを経営者が確認できないという懸念があり得ます。ISO/IEC 27001では、対策が必要な情報セキュリティリスクと管理策が明確になるので、経営者の判断のもと、適切な情報投資が実現できます。

また、PDCAの中で常に活動の見直しを図ることができるため、情報通信技術の発展に伴う新たなリスクにも的確に対応できるようになるのもマネジメントシステムの特長です。モバイルネットワークやクラウドコンピューティングなどの先進的な技術に対しても、適切なセキュリティ対策を行いながら、安全に活用できるようになります。

さらに、多くの組織があげているISO/IEC 27001を導入するメリットは、情報セキュリティを通じた社会や顧客からの信頼獲得と社員の情報セキュリティ意識・モラルの向上です。ISO/IEC 27001の認証取得は、継続的改善による情報リスクの低減を実現している明確なエビデンスとなります。一般に製造業企業の社員の皆さんは、品質やコスト、納期などに高い意識を持っていると思われますが、ISO/IEC 27001に取り組むことで、社員の情報セキュリティへの意識やモラルが高まり、新たな気づきや改善にもつながります。

JQAのISO/IEC 27001認証サービス

JQAでは、お客さまの“組織のチカラ”を高めるサービスを提供することを目指し、審査、教育、サポートの幅広い側面から、ISO/IEC 27001の有効活用をお手伝いしています。

JQAの審査では、ISO 9001やISO 14001の審査と同

■ 附属書Aの箇条と目的

箇　条	目　的
A.5　情報セキュリティのための方針群	
A.5.1　情報セキュリティのために経営陣の方向性	情報セキュリティのための経営陣の方向性及び支持を,事業上の要求事項並びに関連する法令及び規制に従って提示するため.
A.6　情報セキュリティのための組織	
A.6.1　内部組織	組織内で情報セキュリティの実施及び運用に着手し,これを統制するための管理上の枠組みを確立するため.
A.6.2　モバイル機器及びテレワーキング	モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため.
A.7　人的資源のセキュリティ	
A.7.1　雇用前	従業員及び契約相手がその責任を理解し,求められている役割にふさわしいことを確実にするため.
A.7.2　雇用期間中	従業員及び契約相手が,情報セキュリティの責任を認識し,かつ,その責任を遂行することを確実にするため.
A.7.3　雇用の終了及び変更	雇用の終了又は変更のプロセスの一部として,組織の利益を保護するため.
A.8　資産の管理	
A.8.1　資産に対する責任	組織の資産を特定し,適切な保護の責任を定めるため.
A.8.2　情報分類	組織に対する情報の重要性に応じて,情報の適切なレベルでの保護を確実にするため.
A.8.3　媒体の取扱い	媒体に保存された情報の許可されていない開示,変更,除去又は破壊を防止するため.
A.9　アクセス制御	
A.9.1　アクセス制御に対する業務上の要求事項	情報及び情報処理施設へのアクセスを制限するため.
A.9.2　利用者アクセスの管理	システム及びサービスへの,許可された利用者のアクセスを確実にし,許可されていないアクセスを防止するため.
A.9.3　利用者の責任	利用者に対して,自らの秘密認証情報を保護する責任をもたせるため.
A.9.4　システム及びアプリケーションのアクセス制御	システム及びアプリケーションへの,許可されていないアクセスを防止するため.
A.10　暗号	
A.10.1　暗号による管理策	情報の機密性,真正性及び／又は完全性を保護するために,暗号の適切かつ有効な利用を確実にするため.
A.11　物理的及び環境的セキュリティ	
A.11.1　セキュリティを保つべき領域	組織の情報及び情報処理施設に対する許可されていない物理的アクセス,損傷及び妨害を防止するため.
A.11.2　装置	資産の損失,損傷,盗難又は劣化,及び組織の業務に対する妨害を防止するため.
A.12　運用のセキュリティ	
A.12.1　運用の手順及び責任	情報処理設備の正確かつセキュリティを保った運用を確実にするため.
A.12.2　マルウェアからの保護	情報及び情報処理施設がマルウェアから保護されることを確実にするため.
A.12.3　バックアップ	データの消失から保護するため.
A.12.4　ログ取得及び監視	イベントを記録し,証拠を作成するため.
A.12.5　運用ソフトウェアの管理	運用システムの完全性を確実にするため.
A.12.6　技術的ぜい弱性管理	技術的ぜい弱性の悪用を防止するため.
A.12.7　情報システムの監査に対する考慮事項	運用システムに対する監査活動の影響を最小限にするため.
A.13　通信のセキュリティ	
A.13.1　ネットワークセキュリティ管理	ネットワークにおける情報の保護,及びネットワークを支える情報処理施設の保護を確実にするため.
A.13.2　情報の転送	組織の内部及び外部に転送した情報のセキュリティを維持するため.
A.14　システムの取得,開発及び保守	
A.14.1　情報システムのセキュリティ要求事項	ライフサイクル全体にわたって,情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため.これには,公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む.
A.14.2　開発及びサポートプロセスにおけるセキュリティ	情報システムの開発サイクルの中で情報セキュリティを設計し,実施することを確実にするため.
A.14.3　試験データ	試験に用いるデータの保護を確実にするため.
A.15　供給者関係	
A.15.1　供給者関係における情報セキュリティ	供給者がアクセスできる組織の資産の保護を確実にするため.
A.15.2　供給者のサービス提供の管理	供給者との合意に沿って,情報セキュリティ及びサービス提供について合意したレベルを維持するため.
A.16　情報セキュリティインシデント管理	
A.16.1　情報セキュリティインシデントの管理及びその改善	セキュリティ事象及びセキュリティ弱点に関する伝達を含む,情報セキュリティインシデントの管理のための,一貫性のある効果的な取組みを確実にするため.
A.17　事業継続マネジメントにおける情報セキュリティの側面	
A.17.1　情報セキュリティ継続	情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込まなければならない.
A.17.2　冗長性	情報処理施設の可用性を確実にするため.
A.18　順守	
A.18.1　法的及び契約上の要求事項の順守	情報セキュリティに関連する法的,規制又は契約上の義務に対する違反,及びセキュリティ上のあらゆる要求事項に対する違反を避けるため.
A.18.2　情報セキュリティのレビュー	組織の方針及び手順に従って情報セキュリティが実施され,運用されることを確実にするため.

※附属書Aの箇条A5～箇条A18は、ISO/IEC 27002 (情報セキュリティ管理策の実践のための規範)の箇条5～箇条18に規定したものをそのまま取り入れており、両者の整合が保たれている。なお、ISO/IEC 27002の箇条1～箇条4は次の通り。0 序文、1 適用規格、2 引用規格、3 用語及び定義、4 規格の構成

様に、プロセスアプローチを重視しています。業務、プロセス、システムの各レベルでPDCAが回せているか、マネジメントシステムが有効に機能しているかについて、実際の業務の流れに沿って確認します。

また、審査先組織の業種に詳しい審査員が担当することも、JQAの審査の特長です。業務上の重要な情報セキュリティリスクを見逃さないように、対象業務に精通し、専門性を持った審査員が審査を担当します。これにより、組織の事業目的と情報セキュリティのバランスを意識した審査を行います。

ISO/IEC 27001は、すでにISO 9001やISO 14001を導入している企業にとって取り組みやすいマネジメントシステムです。ISO/IEC 27001は、2013年に改定され、いち早くマネジメントシステムの共通要素が採用されています。ISO 9001やISO 14001も2015年に改定され、規格の構造が共通化されました。

例えば、ISO 9001の認証を取得している組織は、品質面で、「4 組織の状況」として「4.1 組織及びその状況の理解」「4.2 利害関係者のニーズ及びその期待の理解」を行ったうえで、「6.1 リスク及び機会に対する活動」に取り組み、「6.2 品質目標及びそれを達成するための計画策定」を行っています。ISO/IEC 27001においても、同様に、情報セキュリティ面から、組織の状況を理解し、リスクと機会を特定したうえで計画を策定するため、取り組みやすいと考えられます。

また、「組織の状況の理解」「リスク及び機会の特定」「取組み計画の策定」を、企業活動として品質面や環境面と一体的に進めることができれば、マネジメントシステムの統合運用もしやすいといえます。JQAでは、さらに、「統合マネジメントプログラム」によって、組織のマネジメントシステムの統合度向上をサポートしています。

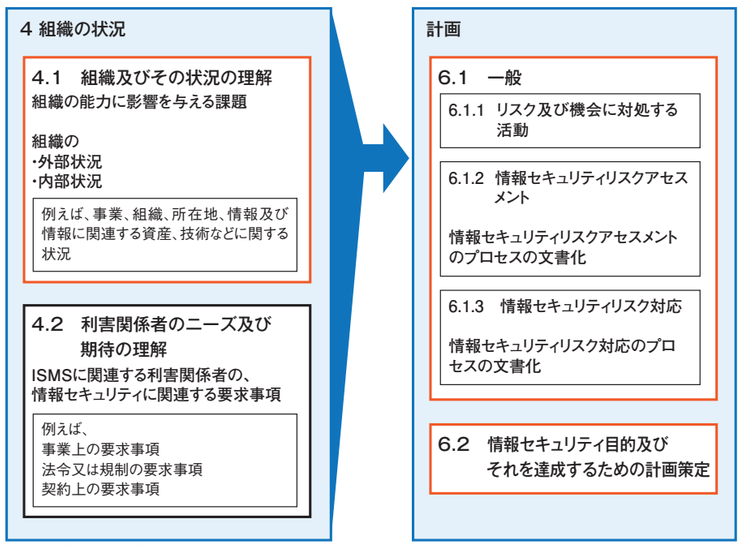
なお、JQAでは、新たにISO/IEC 27001の認証取得を検討されている組織の方々に、業務相談や予備評価を通じてサポートする体制を整えています。

業務相談は、規格の解釈やマネジメントシステムに関するお悩みやお困りごとに、審査員がお応えするサービスです。

予備評価は、登録審査の前に、予行演習としてマネジメントシステムの構築・運用状況を審査と同様の形式で確認し、確認結果を報告書にまとめてご提供するものです。

JQAでISO 9001やISO 14001などの認証を取得されているお客さまには、専任の担当がご相談を承りますので、詳細についてはお気軽にお問い合わせください。 ■

■ リスク及び機会に対処する活動



（数字は規格の箇条番号）

(*1)機密性(confidentiality)
許可されていない個人、エンティティまたはプロセスに対して、情報を使用せず、また開示しない特性

(*2)完全性（integrity）
資産の正確さおよび完全さの特性

(*3)可用性(availability)
許可されたエンティティが要求したときに、アクセスおよび使用が可能である特性

第4次産業革命とSociety 5.0が製造業を根本から変革する

4～5ページのインタビューにあるように、IoT、ビッグデータ、AIを核とした技術革新によって、いま「第4次産業革命」と呼ばれる産業界全般にわたる構造変化が進行し、政府は第4次産業革命を踏まえてわが国が目指すべき社会をSociety 5.0として示しています。

IoTの浸透で実社会のあらゆる情報がデータ化され、ネットワークで自由にやり取りされます。ビッグデータは、集まった大量のデータを分析し、新たな価値を生む形で利用可能にします。AIによって、機械自身が自ら学習し、人間を超える高度な判断が可能になります。

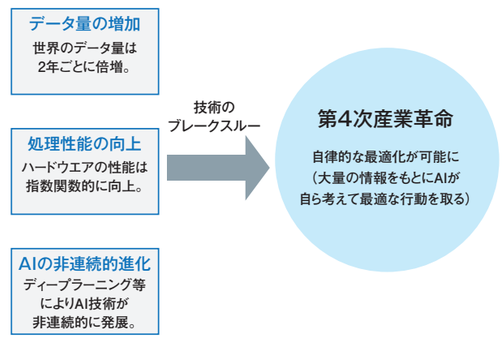
これらの技術進歩は、産業界さらには社会システム全般の構造を変える潜在力があるとみられています。いわば、水力や蒸気機関により動力を獲得し機械化が実現した第1次産業革命、電力の活用が進み重化学工業が誕生した第2次産業革命、コンピュータによる自動制御が進んだ第3次産業革命に匹敵する技術革新であることから、第4次産業革命と位置づけられているのです。

第4次産業革命では、製造業は、高度情報技術によってサービス化し、自律的に最適化することが可能になります。経済産業省の新産業構造部会の資料によれば、大量生産工場で即時対応・オーダーメイド生産が可能になり、製造・物流・販売をデータで連携させることで、ムダゼロ・リードタイムゼロが実現します。プラントの状態を常時監視し、異常や予兆の早期検知、適切なアラームが可能になるといわれます。

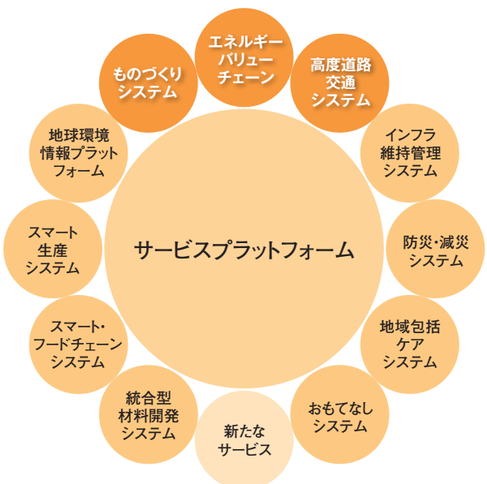
政府は、この第4次産業革命を日本経済発展の柱とし、未来に向けた経済社会システムの再設計を行う「新産業構造ビジョン」を掲げています。さらに、第4次産業革命によって、狩猟社会、農耕社会、工業社会、情報社会に続く新たな経済社会 ＝ Society 5.0の実現を目指しています。Society 5.0は、産学官が連携して実現を目指す、産業界、学界、官界共通の国家ビジョンです。

内閣府は、Society 5.0実現のための総合戦略2015で定めた11システムのうち「高度道路交通システム」「エネルギーバリューチェーンの最適化」「新たなものづくりシステム」をコアシステムとして開発し、新たな価値の創出を目指しています。

■ 第4次産業革命



■ Society 5.0のイメージ



第三部　製造業のISO/IEC 27001活用事例

川西航空機器工業株式会社

品質同様に情報セキュリティは信頼の基盤
―成長する航空宇宙分野で発展し続ける

航空機用標準部品をはじめ、航空宇宙分野向けにさまざまな機器や部品の設計・製造を行っている川西航空機器工業は、2005年に情報セキュリティマネジメントシステム（ISMS）の認証を取得している。管理責任者を務めるマネジメントシステム課 課長の吉原健氏に、ISMS導入の経緯と今後の戦略についてうかがった。

業界内でいちはやくISMSを導入

航空宇宙産業は、市場の成長性が高く、日本の高度なモノづくり力が生かせる産業であることから、将来に向けた有望産業として位置づけられ、国もその振興に力を入れている。

川西航空機器工業は、創業間もない1952年に航空機部品の製造を開始。以来、航空宇宙分野一筋に事業を発展させてきた。現在では、航空機用標準部品をはじめ、陸・海・空の自衛隊各種機器や国際宇宙ステーション部品まで、さまざまなパーツの設計・製造に携わっている。

高度な精度と安全性が求められる製品を扱うことから、顧客である防衛省・自衛隊、機体メーカー、装備品メーカー、エンジンメーカーなどと取引するためには、顧客からのさまざまな要求を満たし認定を得る必要がある。同社では、認定企業に求められる高度な要求に応えるため、品質、環境、機密情報保全のための厳しい管理体制を保ってきた。

マネジメントシステムについては、1998年にISO 9001の認証を取得し、2004年5月には航空宇宙産業の品質規格JIS Q 9100の認証を取得した。2005年5月には、ISO 14001の認証を取得している。

情報セキュリティに関しては、2005年2月にまず3D-CADを使用する設計部門で、のちにISO/IEC 27001に引き継がれるISMS適合性評価制度の認証を取得した。


マネジメントシステム課 課長
吉原 健 氏

「2005年当時、すでにISO 9001は製造業として当たり前の規格になっていましたが、ISMSは業界内でも早い導入でした。その背景には、この頃から航空宇宙部品の製造工程で電子化や情報通信機器の利用が進み、それに対応した情報セキュリティ体制が顧客から求められるようになったことがあります。もう一つの導入の理由は、1998年以来ISO 9001を活用するなかでマネジメントシステムによる継続的改善に手応えを感じ、経営者が新しいマネジメントシステムの導入に積極的だったことがあると思います」（吉原課長）。

2007年にISO/IEC 27001に移行し、翌年ISO/IEC 27001の認証範囲を本社工場に拡大。さらに、2017年には那須工場を認証範囲に加えた。

13年間の活用で定着した情報セキュリティ

すでに、13年にわたり活用してきたISMSだが、同社にとっていまや「なくてはならないもの」になっているという。その理由は3つある。

第1は、情報通信技術の急速な発展のなかで高まりつつある情報セキュリティリスクへの対応と、社員の情報セキュリティ意識の定着である。

「航空宇宙業界は、安全性重視の観点から情報通信技術の活用については比較的慎重だとされてきました。それでも、より高精度の製品を生産し、事業を円滑に進めるためには、情報通信システムの利用拡大は避けて通れません」（吉原課長）。

期間を定めてPDCAを回すことで、変化するリスクを見直しながら対応し、改善の成果を上げていくマネジメントシステムが有効だ。

同社では、納入先からの調査項目に新しい管理項目が入った場合は、導入の必要性を検討したうえ、管理策に採り入れている。また、セキュリティの運用で問題が発見された時は、小さな問題であってもすぐに情報セキュリティ委員会を開催し、対応策を検討している。社員の注意喚起が必要な場合には、毎朝実施している朝礼で全社員に伝達している。同じようなことでも、繰り返し伝えていくことが社員の意識づけにつながっている。

また、毎年1回実施されるJQAの審査のなかで、情報セキュリティの専門知識を有する審査員と対話することも役に立っている。最新の技術的課題についての指摘を参考にするほか、ISMSに取り組んでいくためのヒントを得ることも多い。

第2は、顧客の信頼獲得だ。顧客が要求する情報セキュリティ体制を有することのエビデンスとして、現在では、ISO/IEC 27001の認証取得が実質的な必須条件となっている。

第3は、外部調達先との連携だ。同社のビジネスフローは、顧客が求める製品を、自社の設備と技術とともに外部調達先の協力を得ながら完成品として納品するものだ。現在、材料調達や加工作業の外注など約200社の外部調達先を有しているが、顧客につながるサプライチェーン全体で同等の情報セキュリティ管理体制を維持している。外部調達先がISO/IEC 27001の認証を取得していれば二者監査も簡略化でき、国際標準で運用しているため互いのコミュニケーションも取りやすい。

情報セキュリティを会社の強みに

今後の課題について、吉原課長は、情報通信技術の急激な発展に伴う情報資産の増加とセキュリティリスクに対応していくこと、社員の意識のさらなる向上をあげている。

「技術の発展はすさまじく、スマートフォンのようにひと昔前のコンピュータと同等の機能と情報量を有する機器がポケットの中に入る時代になっています。だからこそ、変化するリスクを常に見直し、必要に応じて対応を行うとともに、社員の意識も高めていかなければならないと思います」。

同社は、最近問題が拡大しているサイバー犯罪に対応するため、専門知識を有する講師を招いて、メールを使ったフィッシング詐欺やウイルス感染など具体的な事例について学習し、社員の意識づけを図っている。

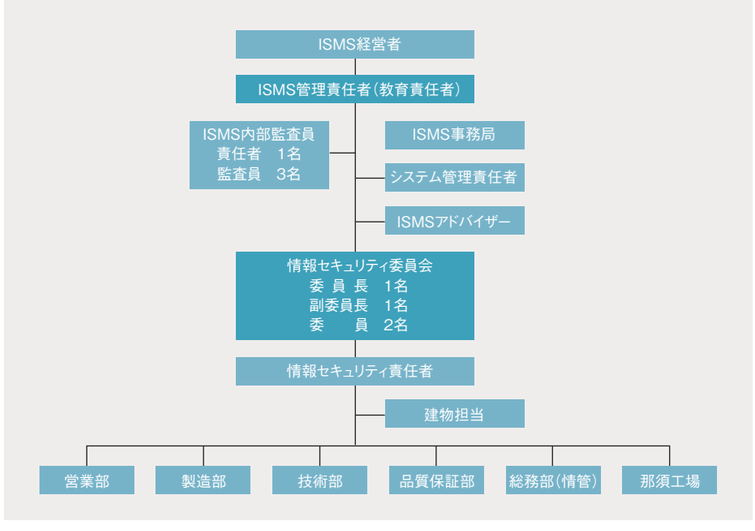
成長分野とされる航空宇宙産業だが、情報セキュリティをはじめ、品質、環境、安全などの分野で厳しい管理体制を求められることが、従来は参入のハードルとなってきた面もある。しかし、今後は、異業種からの参入も増え、競争が激化するものと予想している。

「これからは、競争のなかで切磋琢磨しながらよりよい製品を送り出していくようになっていくと思います。当社の社員は、航空宇宙分野のエキスパートとして優れた技術を提供することにプライドを持っています。情報セキュリティに関しても、同等のプライドを持てるようさらに意識を高め、当社の武器となるようにしていきたい。それによって、海外企業との競争でも勝ち残っていけるような企業になりたいと思います」（吉原課長）。 ■

川西航空機器工業株式会社のプロフィール

所在地	兵庫県川西市
創業	1950年12月
会社設立	1967年6月
事業内容	航空機・宇宙関連機材の設計・開発・製造及びサービス提供（引取り修理）

■ ISMS組織図



第三部　製造業のISO/IEC 27001活用事例

日興電気通信株式会社

取引先からの要望によるISO/IEC 27001認証取得から3年、「定着」から「進化」へのステップアップを図る

映像情報機器を用いたVisual Networkシステムなどの開発設計から製造・販売までを幅広く手がける日興電気通信は、2014年に情報セキュリティマネジメントシステム ISO/IEC 27001の認証を取得した。取締役 品質統括 兼 品質管理部部長の宮内利治氏と総務部 部長代理の山中一生氏に、ISO/IEC 27001導入の経緯と活用の状況についてうかがった。

顧客からの信頼を得るために ISO/IEC 27001導入を決断

近年の画像処理技術などの発展により、映像情報は多岐にわたる情報からユーザーが必要とする情報を自動抽出、加工することが可能となっている。日興電気通信は、映像通信技術にネットワークを融合させた「Visual Network」を提唱し、映像情報を「視る」「送る」「活かす」「見せる」といった幅広いニーズに対応する機器・システム・ソリューションを提供している。その用途は、空港や道路などの交通インフラの監視、河川や消防などの防災監視や防犯監視、工場等でのFA用途まで広がりを見せている。

同社が、ISO/IEC 27001の認証を取得することになった理由は、顧客からの情報セキュリティに関する要望であった。同社の事業は、主に大手情報通信システム会社から受注し映像監視システムを設計・製造するケースと、官公庁・公共機関向けに入札によってシステムを直接納入するケースがある。いずれも案件ごとにカスタムの映像監視システムを提供するもので、設計開発から運用に至るまで、同社が扱うほぼすべての情報について機密性を確保する必要がある。最大手の顧客である情報通信システム会社からは、日頃から情報セキュリティの強化を求められており、取引に当たってはISO/IEC 27001もしくは同等の情報セキュリティ体制を持つことを要望されていた。一方、官公庁入札においても、納入先や案件によって違いはあるもののISO/IEC 27001の認証が事実上の条件であるなど、情報セキュリティの状況が自社の評価に影響するケースが増えていった。

「設計開発業務のコンピュータ化が進むなかで、機密性の高い情報資産が急速に増えていきました。従来から独自のルールで機密情報を守っていましたが、お客さまの信頼を得るためにはISO/IEC 27001認証が不可欠と判断し、導入を決断しました」（宮内取締役）。

取締役 品質統括 兼 品質管理部 部長
宮内 利治 氏

総務部 部長代理
山中 一生 氏

運用とハードの両面で準備を行う

2012年にISO/IEC 27001による情報セキュリティマネジメントシステムの構築に着手し、まず情報収集と規格の理解を進めた。同社は、すでにISO 9001、ISO 14001の認証を取得しており、マネジメントシステムについて知識や経験を持っていたが、ISO/IEC 27001には附属書Aに詳細な管理策が定められており、規格の構成の違いからその理解や適用には戸惑いを覚えた。特に、管理策の専門用語の解釈に迷うことも多かった。

同社では、担当者が、書籍やJQAの規格入門セミナー、研修機関が開催する内部監査員養成講座への参加を通じて規格の知識を深めるとともに、最大手顧客の調達部門に相談しながら情報セキュリティのルールづくりを進めた。

これと並行して、入退室を厳しく制限したサーバー室の設置や、社員通用口のICカード式の電子錠による入退室管理の導入など、物理的、環境的なセキュリティ強化を進めた。さらに、セキュリティレベルを考慮して、納品メーカーとの商談専用スペースを工場と区分けして設置した。

運用面では、運用ルールを全社員にわかりやすく伝えるため、同社独自の「情報セキュリティ・ルールブック」を作成した。規格が求める管理策や顧客からの要求事項を、わかりやすい言葉に書き直してまとめ、全社員が閲覧可能としている。

情報セキュリティマネジメントシステム構築から1年間の運用期間を経て、2014年1月に認証を取得した。

社員の意識向上と顧客の信頼獲得で成果

ISO/IEC 27001の認証取得から約3年間を経て、社員の情報セキュリティに関する意識および知識の向上と、事故の未然防止、顧客の信頼獲得などで成果を上げている。

「情報通信システムは技術の発展がめざましく、利便性の向上と同時にセキュリティリスクも拡大する傾向があります。そのようなリスクに対応していくために、マネジメントシステムで継続的な改善を続けています」（宮内取締役）。

システムを運用するなかでセキュリティリスクについて新たな気づきがあり、改善を図った例もある。例えば、複合プリンターから出力する書類や図面の放置や紛失を避けるため、本人のICカードで認証しなければ出力できないようにした。また、使用が許可されていないアプリケーションソフトをインストールした場合は、情報セキュリティ棚卸しで発見できるので、担当部門に改善を求めている。情報システムの運用監視の記録から、軽微なセキュリティインシデントが発生する傾向を分析し、インシデントを起こしやすい時期には事前に注意喚起を行い、事故の予防と啓発に役立てている。さらに、新入社員向けのセキュリティ・ルールブック入門編も作成した。

顧客からの信頼向上については、ISO/IEC 27001認証取得によって二者監査が簡略化されたことに加え、顧客のサプライチェーンを担う企業としての責任を果たすという意味でも成果をあげている。同社は、サプライヤーに対して同等の情報セキュリティが確保されるよう指導し、サプライヤーとの資料のやり取りについてのルール化を行っている。

「定着の3年間」から、「進化の3年間」へ

今後の戦略について、山中部長代理は次のように語る。

「ISO/IEC 27001認証取得からこれまでの3年間は、いわば『定着の3年』でした。次の3年間は『進化の3年』にしたいと考えています」。

同社では、リスク管理の観点から新しい情報通信技術の導入には慎重な姿勢で臨んできた。例えば、現在同社はオフィスのネットワークに無線LANを採用しておらず、クラウドシステムも活用していない。社員の情報セキュリティへの意識が定着してきたなかで、技術的にも安全性が担保されるならば、今後はこうした新技術も積極的に採用することが可能になる。

「先進技術を適切に活用することで、効率化や生産性の向上とともに、社員のはたらき方も含めた改善、改革を進めていきたいと思います」（山中部長代理）

「情報セキュリティを守ることは、いまや製造業全般の課題になっていると思います。当社は過去3年間で培った情報セキュリティの経験や知識を、今後の技術開発やソリューションにも生かしていきたいと思います」（宮内取締役）。

同社は、今後、ISO/IEC 27001とISO 9001、ISO 14001の統合を行い、一体的な運用で効果的な活用を目指していく。■

日興電気通信株式会社のプロフィール

所在地	東京都品川区大崎（本社） 横浜市青葉区鴨志田町（工場）
創業	1959年3月
事業内容	・監視システムの設計・開発、製造、保守及び販売 ・映像機器及び通信機器の設計・開発、製造、保守及び販売 ・コンピュータ及び周辺機器の診断、修理

■ ISMS組織図