会誌「情報処理」Vol.64 No.11（Nov. 2023）「デジタルプラクティスコーナー」

中部産業連盟推薦論文

日々変化する情報セキュリティリスクに対応し続けるための，情報セキュリティ管理の構築と実践

青山　誠[1]

[1]（一社）中部産業連盟

現代において企業が永く事業継続するためには，情報セキュリティリスク管理，情報セキュリティ事故・事件の適切な管理，従業員に対する情報セキュリティ教育啓蒙活動等を継続的に実施し続けることが不可欠である．本稿では，進化し続けるサイバー攻撃等の情報セキュリティリスクに適切に対応するため，情報セキュリティ管理に必要な実施事項を状況別に整理，構築，連携し，改善し続ける手法およびその実施事例を紹介する．

1. 現代のIT社会情勢と情報セキュリティの意識

世界的な感染症の蔓延を引き金に，日本においてもビジネス現場におけるテレワークを含むITシステムの整備・推進のニーズが高まっている．加えて，近年は，自社敷地内に情報システムの本体サーバを設置せず，高速な広域ネットワーク技術を活用したクラウド型情報システムを主体とするシステム構成を組む組織が増加し続けている．

ITや通信分野に関する専門調査会社であるIDC Japanの調査によれば，日本のパブリッククラウドサービス市場規模（売上高）の推移および予測として，2021年の売上額1兆6千億円に対して，2026年には3兆7千億円に達するとしている[1]．これは市場規模が5年間で2.3倍になり，日本全体でクラウドサービスの活用が大きく進むことを意味する．このようにクラウドサービスの導入活用が進む主な要因は以下に示すとおりである．

- 組織が感染症対策として，従業員同士が物理的な距離をとれる施策を実施していること．
- IT人材不足により，自社内に情報システム管理の部門や担当者の確保が困難であること．
- 自社内に情報システム部門を持たず（縮小を含む），情報システム管理全体を外部委託することを目的とする管理体制が増加していること．

一方，クラウド型情報システムを主体としたネットワーク化や自社情報システムの外部委託化を進めることで，組織内の閉じた領域（自社の物理的な建物や自社敷地内に設置した社内サーバ）で管理していた重要情報が社外のデータセンタ等に保管され，外部委託の作業員や悪意のある第三者がその情報にアクセスしやすくなる．これは，ネットワークを利用したサイバー攻撃等の情報セキュリティリスクが高まることを意味する．

このような状況においても，多くの組織ではITシステムを導入する際には，収益性，利便性，効率性が優先され，情報の信頼性や安全性確保の優先度が下がる傾向にある．

次章では，近年増加，巧妙化しているサイバー攻撃の種類や対策を紹介する．

2. サイバー攻撃についての現状と被害

（1）近年の標的型攻撃の特徴）

標的型攻撃とは，特定の人物や組織が狙われて被害を受けるサイバー攻撃である．攻撃者の目的は以下のとおりである．

①機密情報の詐取（さしゅ）

特定企業が保有している機密情報（開発中の商品情報，特殊な業務ノウハウ，個人情報等）を詐取し，攻撃者本人がビジネスにおいて優位に立つために詐取した情報を活用する．

外国の第三者が，日本企業の機密情報を詐取するために攻撃を仕掛けてきた事例が多数ある．

②競合他社への妨害行為

競合他社を業務停止に追い込むような被害を与え，ビジネスにおいて自社が優位に立つ．後述するランサムウェア等は，対象組織の機密情報を不正に暗号化し，解除するための身代金を要求する．主に金銭目的ではあるが，身代金を支払っても機密情報の暗号化を解かないこともあり，競合他社に対する妨害行為が目的ともいえる．

（2）標的となる組織の傾向

攻撃者は，ビジネスにおいて優位に立つことや金銭的な利益や便益を得ることが主な目的である．そのため，標的となる組織は，他組織から見た場合の魅力的な機密情報を保有しており，かつ，情報セキュリティ上の脆弱性がある組織であると考えられる．

（3）標的型攻撃の種類と対策

ここでは，近年の標的型攻撃のうち，社会的に大きな影響を及ぼしているランサムウェアとエモテッドについて内容と対策を紹介する．

①ランサムウェア

感染したシステムに特定の制限（例.データの暗号化）をかけ，その制限の解除と引き換えに金銭を要求する．組織のネットワークに侵入し，データを暗号化するだけでなく窃取（せっしゅ）して，世に公開すると脅し，身代金を支払わざるを得ないような状況を作り出す．

社内ネットワークに接続されたパソコンにて，特定のWebサイトからファイルをダウンロードする際やEメールの添付ファイルやURL（Webのリンク）をクリックした際に感染する．

対策としては，ウイルス対策ソフトの最新化，OSおよびアプリの最新化，Eメールの添付ファイルや本文中のURLに注意することであるが，感染後の復旧準備として重要なファイルを定期的にバックアップすることが重要である．ただし，ランサムウェアは本体データとバックアップデータの両方とも制限を掛けることがあるため，データバックアップの際は，バックアップディスクを社内ネットワークから切り離すなど，踏み込んだ対策も重要である．

②エモテッド

被害を受ける側（攻撃メールの受信者）が過去にEメールのやりとりをしたことのある，実在の相手の氏名，Eメールアドレス，メールの本文等の一部が流用された，あたかもその相手からの返信メールであるかのように見える攻撃メールである．このようなメールは，エモテッドに感染してしまった組織から窃取された，正規のメール文面やEメールアドレス等の情報が使われている．

社内ネットワークに接続されたパソコンにて，Eメールの添付ファイルやURL（Webのリンク）をクリックした際に感染する．

対策としては，ウイルス対策ソフトの最新化，OSおよびアプリの最新化，Eメールの添付ファイルや本文中のURLに注意することであるが，信頼できないEメールに添付されたWord文書ファイルやExcelファイルを開いたときに，マクロやセキュリティに関する警告が表示された場合，「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしないことが重要である．

ここに挙げたサイバー攻撃のほかにも多種多様な攻撃手法および亜種（新しいタイプの攻撃）が出現する可能性がある．組織は，それらを含めたあらゆる脅威から組織の機密情報を守る必要がある．こうした脅威に対して適切に情報セキュリティ対策を実施し，組織の情報セキュリティを継続的に確保するためには，情報セキュリティマネジメントシステムの構築と運用が有効である．

3. 情報セキュリティマネジメントシステム（ISMS）とは

ISMS（Information Security Management System）とは，組織の情報セキュリティ管理の体系的な仕組みと具体的な運用のことである[2]．その目的は，組織がリスク管理の仕組みを実行することによって情報の機密性，完全性および可用性を確保し，情報セキュリティリスクを適切に認識し管理しているという信頼と安心を利害関係者に伝達することである．そのため，ISMSの運用を組織の日常業務の中に組み込むことがきわめて重要である．

ISMSでは，確保するべき情報セキュリティの3要素を以下のように定めている．

表1　情報セキュリティの3要素[2]

種別	意味	対策　例
機密性確保	対象とする情報やデータに対して、 正当な権限を持つ者だけがアクセスできること。	ログインID・パスワード アクセス権限設定
完全性確保	正当な権限を持たない者が情報やデータの変更や 削除が実施できないこと。	改ざん防止 改ざん検知
可用性確保	情報やデータを活用したいときに、使用できること	電源対策 システム二重化

ISMSの構築と運用を実施するには，ISO/IEC 27001というISMSの国際規格の活用が有効である．ISO/IEC 27001は，ISMSの要求事項を定めた規格文書であり，組織がISMSを確立し，継続的に運用し，組織の情報セキュリティを改善するための要求事項が記述されている．ISO/IEC 27001は，内部監査員や外部監査員の監査において，組織が情報セキュリティ要求事項を満たす能力を保有しているかを評価するための基準としても活用できる．

ISMS認証とは，組織の構築したISMSがISO/IEC 27001の要求事項を満たし，適切に運用されているかを，利害関係のない立ち位置から審査し証明することである．審査は，第三者であるISMS認証機関が実施する．ISMS認証によって，組織は，国際規格であるISO/IEC 27001が要求する情報セキュリティを確保するための仕組みを維持し継続的に改善していることを，利害関係者に示すことができる．

次章では，組織が高いレベルの情報セキュリティ管理を実現するため，ISMSの要求事項を応用し具体的な管理体制を整理する．

4. 情報セキュリティ管理体制の構築

これまで情報セキュリティ管理について特に対策を行っていない組織の場合，短期間でISMSの構築やISMS認証を取得することは難しい．そのため，まずは以下の表に示す3つの実施事項を念頭に置いて整理し，構築および運用する．

表2　情報セキュリティ管理の3つの柱

<table>
<tr><th colspan="2">計画段階</th><th colspan="2">運用段階</th></tr>
<tr><td>1．
リスク
アセスメント</td><td>情報の洗い出し
リスク分析
セキュリティ対策の決定
セキュリティ対策の実施</td><td>2．
インシデント
管理</td><td>事件・事故・ヒヤリハットの収集
収集情報の一元管理
情報セキュリティ委員会で対策決定
セキュリティ対策の実施
セキュリティ管理策の見直し</td></tr>
<tr><td colspan="4">3．継続的な教育・啓蒙活動</td></tr>
<tr><td colspan="4">管理面・・情報セキュリティの組織的な管理教育
技術面・・技術的なセキュリティ管理のスキル教育
意識面・・組織人としての情報セキュリティ意識啓蒙活動</td></tr>
</table>

（1）リスクアセスメント[3]

情報セキュリティ管理の活動のうち，計画段階で実施する．組織は，組織に内在する情報セキュリティリスクを明らかにする必要がある．情報セキュリティの状況を確認する際，最初に企業で取り扱っている“情報”を洗い出す．次に，“情報”ごとに“情報の価値”を決定し，リスク分析を実施する．リスク分析の結果，リスクが高いと判断されたものから優先的に回避，除去するために必要な情報セキュリティ対策を検討し，実行する．

①“情報”の洗い出しと情報の価値の決定

組織が取り扱う“情報”にはさまざまなものがある．たとえば，事業運営上のノウハウ（知的財産），顧客や従業員の個人情報，物的資産等である．まず，業務上取り扱っている“情報”を特定し，機密性・完全性・可用性の3つの喪失時の影響度から“情報の価値”を決定する．組織の状況にもよるが，機密性確保がもっとも重要であると考えた場合，次の式で“情報の価値”を算出する．

“情報の価値”＝機密性喪失時の影響×（完全性喪失時の影響＋可用性喪失時の影響）

“情報の価値”は，値が大きいほど価値が高いと考える．

②リスク分析の実施

リスク値が大きいほどリスクが高いことを意味する．“情報”に対するリスクを導き出し，それぞれのリスクに対しリスクの値を導き出す．リスク値を算出する計算式は，組織が個別に検討することが必要である．

下表に示す例では，業務上取り扱っている“情報”に対してリスク分析を実施した内容を示している．結果，リスク値が高いリスクに対して，優先的に対策を実施することになる．

表3　リスク分析・対策表　例

NO	組織	情報	①情報の価値	リスク内容	脅威の内容	②評価1～3	脆弱性内容	③評価1～3	リスク値①×(②＋③)	対策
1	IT業務運用部	顧客企業のシステムを管理するノウハウ	18	悪意のある人物に顧客システムに不正アクセスされ、顧客システムの稼働が妨害される	従業員が社内PCから、顧客システムに不正アクセスし、顧客システムの稼働を妨害する	3	顧客システムへのログインが、社内の全パソコンから可能。 顧客システムへのログイン時にアクセスログが残らない。 システム管理者のセキュリティ意識の低下	3	108	“顧客システムアクセスルーム”を新設し、顧客システムへは、この部屋に設置したパソコンでのみログイン可能になる設定を実施。 入室と、顧客システムへのログインを実施する際、使用者、利用目的、作業時間帯を申請し、管理者に承認を得る手続きを義務化。 アクセス時にログを残すように設定し、システム管理者が日次でログを確認し、不正アクセスの有無を確認する。
2	IT業務運用部	自社のシステムを管理するノウハウ	12	社外からの不正アクセスにより情報を盗まれる	社内サーバにインターネット側からサイバー攻撃を受ける	3	社内サーバのアクセス権が未設定 管理者のセキュリティ意識の低下	3	72	アクセス権を設定する。部署ごとに参照できるフォルダを分ける。アクセス時にログを残し、管理者が日次でログを確認し、不正アクセスの有無を確認する。
3	開発部	自社開発ソフトのプログラム本体	12	社外からの不正アクセスにより情報を盗まれる	社内サーバにインターネット側からサイバー攻撃を受ける	3	社内サーバのアクセス権が未設定 管理者のセキュリティ意識の低下	3	72	
4	開発部	自社開発ソフトの設定ファイル	9	社外からの不正アクセスにより情報を盗まれる	社内サーバにインターネット側からサイバー攻撃を受ける	3	社内サーバのアクセス権が未設定 管理者のセキュリティ意識の低下	3	54	※ 今後のリスク分析において対応を再検討する。
5	総務部	従業員の個人情報	8	紙データを盗難や不正使用される	従業員が紙データを盗難や不正使用する	2	個人情報の書類は鍵のかかる書庫で保管	1	24	※ 今後のリスク分析において対応を再検討する。

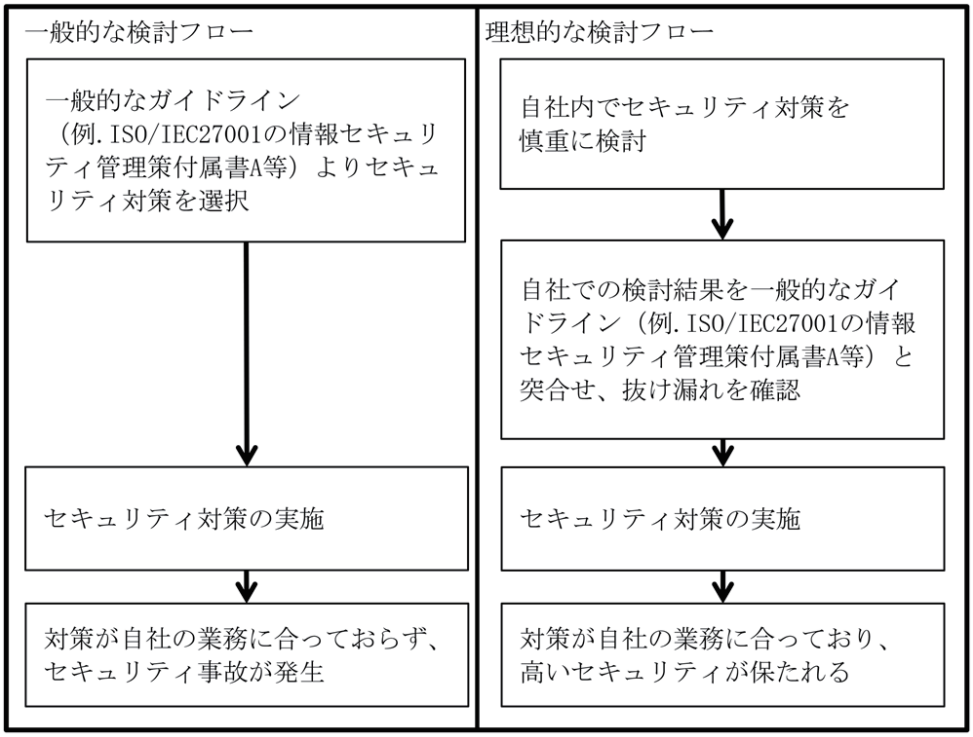
③情報セキュリティ対策の決定と実施

情報セキュリティ対策を決定する際の留意点は2つある.

1つ目は，リスク源の排除を最初に検討することである．たとえば，「取扱い個人情報の漏えいリスク」に対しては，まず，その個人情報を保有しない対策を検討する．2つ目は，自社内の関係者で情報セキュリティ対策案を検討し，それを一般的な情報セキュリティのガイドラインに照らし合わせて抜け漏れがないことを確認することである.

このような方法で情報セキュリティ対策内容を決定することで，自社の業務上の情報セキュリティリスクを解決できる具体的な対策を導き出すことができる．一般的なガイドラインのみで対策内容を導き出してしまうと，「電子メールを送る際は添付ファイルにパスワードを付ける」や「重要データはバックアップを取得する」等，表面的な対策内容で終始してしまう可能性が高まるからである.

表4　情報セキュリティ対策検討フロー



（2）インシデント管理[3]

情報セキュリティ管理の活動のうち，運用段階で実施する．組織は，組織で発生した情報セキュリティの事件・事故に対して，組織内で一元的に管理し，対処および再発防止等の適切な処置を実施する必要がある．組織の人員全員から，事件・事故・ヒヤリハットの事象があった際に事態を情報セキュリティ委員会に報告し一元管理する．その後，セキュリティ対策を立案し，対応内容を人員全員に共有する.

①事件・事故・ヒヤリハットの収集

組織の人員全員が，組織内で発生したインシデント（事件，事故，ヒヤリハット）の事象を報告できるようにする．その際，Eメールや社内グループウェアの掲示板等，適用可能なツールを選択する．

②収集情報の一元管理

収集した情報を情報セキュリティ委員会で一元管理するため，下表のようなシートを使用して事象ごとに状況を管理する．

表5　情報セキュリティインシデント記録簿　例

発生日	発生事象	業務への影響	対象組織	原因	インシデントレベル（0～3）	対策内容	実施予定日	実施完了日
3月25日	配送業者が別の担当で誤ってセキュリティエリアまで入ってきてしまっていた。	特になし	全組織	いつもと来た人が違うが大丈夫だろうという先入観があった	LV1：ヒヤリハット	普段来ていない担当者や担当変更にはセキュリティエリアの説明を徹底	4月15日	4月15日
3月30日	データ移行作業用PCが持ち出しの記録を記載や報告せず使用されていた。	データ移行作業用PCがなく作業遅延がおこった。所在が不明だった。	全組織	貸出をリストのみにしており各々のタイミングで貸し出しできる状態だった。	LV2：軽微な事故	担当者を置き、担当者を通してリスト管理と貸出し時にラックから出す管理を徹底	4月15日	4月15日
5月30日	個人データを添付したメールを宛先を間違えて全く違う人に届けてしまった。	添付ファイルにパスワードを付けていたため、情報漏洩は防げたと考える。	全組織	メーラーにて送信時に誤送信防止機能を付けていなかった。	LV2：軽微な事故	メーラーに送信ボタンを押した後に、再度宛先を確認する機能を追加する。	4月15日	4月15日

③対策の決定，セキュリティ対策の実施，管理策の見直し

インシデントごとに，情報セキュリティ委員会にて情報セキュリティ対策を決定し，実施または実施を指示する．その際，組織に情報セキュリティの管理策（社内規程）があれば，改訂して内容を組織の人員に周知・徹底する．

（3）継続的な教育・啓蒙活動

情報セキュリティ管理において，組織の人員に対しての継続的な教育や啓蒙活動は重要である．その理由は，ITシステムを用いた技術的対策や建物や仕事場等への物理的対策が優れていても，組織の人員が不正を働いた場合は，情報セキュリティ事件・事故に発展する可能性が高いからである．教育・啓蒙活動で取り扱う内容としては，組織の具体的な仕事内容に沿った教育内容を用いることが望ましい．一般的な情報セキュリティに関する書物などの内容を活用すると，実施事項のイメージが付きづらいからである．

（4）課題：情報セキュリティ管理活動の非連携と連携

リスクアセスメント，インシデント管理，継続的な教育・啓蒙活動は，すべて情報セキュリティ管理を行う上で重要な実施事項であるが，それぞれを独立した活動にしてしまうと効果的ではない．たとえば，リスクアセスメントの結果，導き出された対策内容や，インシデント管理の結果，導き出された対策内容を従業員が理解していない場合が該当する．

表6　情報セキュリティ管理活動が連携していない場合

項目	リスクアセスメントと非連携	インシデント管理と非連携	継続的な教育・啓蒙活動と非連携
リスク アセスメント		リスク分析の際、日々の運用で発生した事件・事故の対策内容を考慮できない。	リスクアセスメント及びインシデント管理により決定したセキュリティ対策が、組織の人員にどの程度浸透しているか分からない。
インシデント管理	事件・事故等の発生原因分析と対策を導き出す際、それが元々の想定リスクの顕在化有無を判断できない。		
継続的な教育・啓蒙活動	リスクアセスメント及びインシデント管理により決定したセキュリティ対策を組織の人員が理解できない。		

次の表に示すとおり，互いの活動の結果を取り入れ連携することで，組織として情報セキュリティ管理の効果を高めることができる．

表7　情報セキュリティ管理活動が連携している場合

項目	リスクアセスメントと連携	インシデント管理と連携	継続的な教育・啓蒙活動と連携
リスク アセスメント		リスク分析の際、日々の運用で発生した事件・事故の対策内容を考慮し、現実的に効果のあるセキュリティ対策を立案できる。	リスクアセスメント及びインシデント管理により決定したセキュリティ対策を、組織の人員に浸透させることができ、今後の事件・事故の発生を抑止することができる。
インシデント管理	事件・事故等の発生原因分析と対策を導き出す際、リスク分析により想定していたリスクなのか、想定外のリスクの顕在化なのかを判断できる。		
継続的な教育・啓蒙活動	リスクアセスメント及びインシデント管理により決定したセキュリティ対策を、組織の人員が理解できるようになり、今後の事件・事故の発生を抑止することができる。		

5. 事例．情報セキュリティ管理活動の相互連携

リスクアセスメント，インシデント管理，継続的な教育・啓蒙活動を相互に連携して運用した事例を紹介する．

（1）事例企業概要および課題

A社は，従業員数約300名の自動車部品の製造業である．近年の製造業を標的としたサイバー攻撃により他社の製造工場が停止する被害が発生していることなどから，A社としても情報セキュリティ管理の活動を継続的に実施してきた．しかし，活動内容が表面的で一般的な内容に終始し，形だけの情報セキュリティ管理になっており，もっと具体的で効果のある活動に変えていく必要があった．

私としては，情報セキュリティ管理は，特にリスクアセスメント，インシデント管理，継続的な教育・啓蒙活動の3つを，それぞれの独立した活動ではなく，相互に連携し同時進行で実施し続けることによって有効な活動になっていくと考えているため，次の活動を計画し実行した．

（2）実施事項

まず，情報セキュリティ管理活動の実施事項の年間計画を作成し実施時期を定めた．

それぞれの活動を相互に連携させることを意識して，その後の活動に入った．

表8　月別実施計画

月別実施計画	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
継続的な教育・啓蒙活動						○						○
リスクアセスメント	○											
インシデント管理	○	○	○	○	○	○	○	○	○	○	○	○
情報セキュリティ委員会	月末	月末	月末	月末	月末	月末	月末	月末	月末	月末	月末	月末

①継続的な教育・啓蒙活動

実施月を年2回に定め，情報セキュリティ教育の内容は，一般的な情報セキュリティの対策に加え，リスクアセスメントやインシデント管理の中で決定したセキュリティ対策の具体的な内容を含めた．また，期間の途中に職に就く要員については，同様の内容を着任したときに教育する計画にした．

②リスクアセスメント

年1回4月に実施すると定めたが，必要に応じて期の途中でも臨時で実施する計画とし，実施した．リスクアセスメントの中で行うリスク分析と情報セキュリティ対策を立案する際，継続実施しているインシデント管理で決定した対策を確認し，新たなリスクの可能性を慎重に導き出した．

③インシデント管理

日々収集しているインシデントの内容を情報セキュリティ委員会で細かく確認した．その際，リスクアセスメントおよび情報セキュリティ対策の内容を振り返り，発生したインシデントが当初想定していたリスクかどうかを確認した．当初から想定していたリスクが顕在化した場合は対策の再検討を行い，想定していなかった場合は，リスクアセスメントの実施手順の見直しを行い，次年度の活動に反映した．

④情報セキュリティ委員会

インシデントの内容を確認し，情報セキュリティ対策を検討する活動を基本とした．その中で，リスクアセスメントの内容の振り返り，次年度のリスクアセスメントの実施手順の見直し，委員会での決定事項を継続的な教育・啓蒙活動に含めて周知徹底する方策を検討した．

（3）効果

情報セキュリティ管理活動を以下の点で改善できたと考える.

- 年間計画とすることで，活動を形骸化させることなく継続できるようになった.
- 情報セキュリティ委員会で活動全般を統括可能になった.
- リスクアセスメントにより当初想定したリスクと，インシデント管理により顕在化し対応したリスクを比較することができるようになり，自組織に関係する具体的な対策内容を導き出すことが可能になった.
- 従業員の継続的な教育・啓蒙活動の内容に，自社の業務に沿った具体的な情報セキュリティの対策内容を含めることが可能になり，教育効果を高めることができた.

6. まとめ

本稿では，サイバーセキュリティの現状および，ISO/IEC27001（ISMS）に準拠した情報セキュリティ管理活動としてリスクアセスメント，インシデント管理，継続的な教育・啓蒙活動を連携して行うことにより，効果を発揮する点を中心に事例を交えて紹介した.

組織はこれらの情報セキュリティ管理活動を，一般的な内容に終始するのではなく，意味のある活動を具体的に実施し，状況を継続的に改善することが大切である．そして，その後は，活動を情報セキュリティの内部監査や外部のセキュリティ監査により指摘を受け，是正対応し，一連の情報セキュリティ管理の活動を経営者に報告し助言を受ける仕組みにするとよい．この活動を繰り返すことで，自然にISMS認証を取得可能な組織になっていくことが望ましい.

また，サイバー攻撃は日々進化しており，組織の脅威であるが，攻撃手法は情報技術の観点では数十年間大きな変化はないと考える．サイバー攻撃による新たな被害が発生するのは，IT技術を活用している企業や個人が働き方やシステムの利用方法を大きく変化させた場合である．たとえば近年のリモートワーク化，パブリッククラウド化，工場や病院のIoT化等が該当する．よって，IT技術を活用する組織は，特に，自組織の日常業務や取り扱う情報の種類が大きく変化した場合等に，新たなサイバー攻撃等の被害に合う可能性を認識し，繰返し情報セキュリティ対策を実施し続けることが重要であると考える.

本稿が各社，各組織の今後の継続的な事業活動の一助になれば幸いである.

参考文献

1）IDC Japan（株）：2022年3月31日 国内パブリッククラウドサービス市場予測を発表，IDC Media Center，https://www.idc.com/getdoc.jsp?containerId=prJPJ48986422（2023年4月10日アクセス）
2）ISO/IEC：ISO/IEC 27001：2022　情報セキュリティ，サイバーセキュリティおよびプライバシー保護―情報セキュリティマネジメントシステム―要求事項，第3版2022年10月英和対訳版
3）経済産業省：（独） 情報処理推進機構，サイバーセキュリティ経営ガイドライン Ver 2.0，サイバーセキュリティ経営ガイドライン（2017），https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf（2023年4月10日アクセス）

青山　誠（非会員）
aoyama@chusanren.or.jp
2003年よりNECソフトウェア中部（現・NECソリューションイノベータ（株））において，公共インフラ系ITシステムのプロジェクトに所属し，システム企画，設計開発，構築，保守運用管理に従事．主にデータベースやネットワークに関する設計構築を担当する中で，情報セキュリティを考慮した設計や管理手法を適用．2017年より現職にて，顧客企業に対し情報セキュリティ管理の適用やITシステム企画・導入コンサルティング等に従事．経済産業大臣認定ITストラテジスト，データベーススペシャリスト，情報セキュリティアドミニストレータ，中小企業診断士．

採録決定：2023年4月12日
編集担当：斎藤彰宏（日本IBM）