住友化学グループの情報セキュリティ確保に向けて

住友化学システムサービス株式会社
IT戦略室
中　井　加津代
兼　平　崇　之
清　水　寿　美

Ensuring Information Security in the Sumitomo Chemical Group

Sumitomo Chemical Systems Service Co., Ltd.
IT Strategy Office
Kazuyo NAKAI
Takayuki KANEHIRA
Sumi SHIMIZU

Many companies have conducted various activities to ensure information security since utilization of information technology became one of the ways to support business. However, changes in the threats surrounding the current IT environment and changes in the environment such as IT technology and globalization also have an effect on revisions of international standards, and so security measures in companies need to be reexamined. This report includes a discussion of information security in the Sumitomo Chemical Group.

はじめに

グローバルケミカルカンパニーとしてのさらなる飛躍を目指す住友化学グループでは、グローバル連結経営の支えとなるIT基盤の整備が急速に進められており、海外を含めたグループ会社が同一のネットワーク上で業務を遂行する環境が整備されてきた。これと並行して、情報セキュリティの基本的な方針を固め、住友化学㈱はじめ、グループ会社の対策推進を行ってきた。

しかしながら、外部環境からの情報システムの脅威は年々増大しており、グローバル連結経営を実現するためには、継続的に情報セキュリティを維持していく取り組みが求められる。

コンプライアンス経営やCSR経営を重視する住友化学グループでは、情報セキュリティ確保を経営課題の一つとして捉え、グループ全体を対象とした情報セキュリティマネジメントを進めてきた。

本稿では、グループ経営における情報セキュリティ確保の進め方や課題、課題解決に向けた対策について、主にマネジメントの観点から解説し、住友化学グループでの取り組みを紹介する。

脅威の変遷

近年、インターネットを主としたIT環境での犯罪行為は非常に巧妙化していると言われており、数々報道される情報セキュリティ事故がそれを裏付けている。これらの攻撃は手段の面だけではなく、目的の多様化傾向も報告されており、攻撃対象の範囲と種類は拡大する一方で、IT面における情報セキュリティリスクは非常に高まっている。

これらのIT環境における脅威の変遷を振り返り、企業の対応の動向を述べる[1)]。

1. サイバー攻撃の変遷

(1) インターネットの定着に伴う脅威の変化

2000年に入ってブロードバンドネットワークが普及して以来、インターネットは家庭や企業で本格的に利用されるようになった。2000年代後半には、オンラインショッピングサイトを代表とするインターネットを利用した直接的な商取引も社会に定着した。

IT環境の進化とともに、脅威も変化していく。

インターネット利用の拡大に伴い、インターネットを介したコンピュータウイルスやワーム*1といった不正プログラムによる攻撃が広まった。CodeRed*2、Nimda*3、SQLSlammer*4などのワームは、多数の企業に大きな被害をもたらしたとして知られている。しかし、これらの攻撃は自己顕示を目的とした愉快犯的な色合いが濃かったが、インターネット上の商取引の普及とともに、直接的な金銭の搾取を目的とする攻撃が活発化した。

一方で、2005年に個人情報保護法が施行され、イン

ターネット上、現実世界の両方の犯罪に有用な情報である個人情報の管理は厳しくなる。個人情報そのものの価値が闇市場で高まることになり、この搾取を目的とした攻撃も相次いだ。

攻撃者の目的が明確に金銭へと変遷していく中で、攻撃の方法は年々巧妙化していく。IT面の脆弱性をついて技術を駆使して侵入するような攻撃に加え、人の心理面の弱さをついて騙すような攻撃が猛威を振るい始めるのである。関係者を巧みに装ったメールに、不正プログラムの起動や不正なウェブサイトへの誘導を行うように仕掛ける標的型メール攻撃もその一例である。

(2) 新たなIT活用と市場化・軍事化する攻撃

近年、無線LANやスマートデバイス、クラウドサービスなどにより、市民生活、社会生活全般においてオンライン化がますます進んでいる。また、従来特殊な基盤を利用していた制御システムにも汎用技術の採択が進み、一般的なIT資産と同じように製造業のプラントや電力産業の発電施設など、重要インフラが犯罪者の脅威にさらされることになる。

魅力的な標的が増え続けるに伴い、攻撃のための手法も進歩を遂げていく。攻撃者は脆弱性の検索や攻撃手法をツール化し、闇市場で売買し始める。これによって、特殊な技術や膨大な時間を要することなく、誰もが効率的な攻撃を成功させることが可能になった。

既知の脆弱性は簡単に侵入を許し、ゼロデイ攻撃*5の回数は年々増加している。特定の組織を狙った標的型攻撃は、メールの攻撃、不正プログラムの感染、より深く侵入するための情報の搾取、組織内のコンピュータの遠隔操作など、目的を遂げるまでに、複数の種類の攻撃を多段階で周到に仕掛けてくる事例も報告されている。2013年3月には、韓国で大規模な標的型攻撃が発生し、銀行3行と放送局3社が銀行取引や放送業務の停止に陥るなどの被害にあった。この事例では発生の9ヶ月前から攻撃が仕掛けられていたと言われており、その周到さ、執拗さが伺われる。重要インフラ制御システムへの攻撃事例もその件数が年々増加していることが報告されており、プラントを持つ製造業にとっても見過ごせない脅威である。また、「ハクティビズム」のように、主義主張のメッセージ発信のために公的機関や特定組織のWebサイトに侵入する事例や、国家を標的にした「サイバーテロ」なども相次いで報道されるようになった。このように、ついには、思想、政治的対立の攻防の手段としてもサイバー攻撃が使われるようになり、米国防総省は、サイバー空間を陸・海・空・宇宙に次ぐ第五の戦場と呼び、国家としての対策を強いられるまでになったのである。

2. 企業の対策

企業側の対策も、脅威の変化に合わせて、局所的な技術的対策から、従業員の意識向上や継続的な運用を重視する組織的な取り組みへと変わっていった。

インターネット普及当初は、外部からのネットワーク侵入を防御するファイアーフォールや、アンチウィルスなどのセキュリティ製品の導入が主流であった。その後、ISMSファミリ規格や日本版SOX法などの制度・法規の整備が進んだこともあり、2000年代後半からは組織としての包括的なマネジメントが求められるようになった。また、前述のような制御システムへの脅威の高まりを受け、制御システムの特性をふまえた固有のマネジメント規格CSMSが新たに国際標準として定義された。これらの規格については後の章で詳細を述べる。

顧客情報漏洩や制御系への攻撃は社外へも重大な影響を及ぼす。脆弱な海外拠点の一社への侵入からグループ全体に攻撃が広まり、顧客への影響も含め多額の被害が発生した事例もある。企業の情報セキュリティ対策の目的は、自社事業の保護に止まらず、社会的責任の完遂の意味合いを加え、重要な経営リスクの一つとなった。グローバルでグループ経営を展開する企業の場合、国境を越え、グループ全体を視野に入れた対策の必要に迫られているのである。

情報セキュリティマネジメント

脅威の変遷や各種法整備に伴い、企業は様々な情報セキュリティ対策を検討・実施してきた。その際、多

＊1 ワーム：独立して動作可能なプログラムで、自分自身を複製して感染する不正プログラム。
＊2 CodeRed：Microsoft製品の脆弱性を利用し、自己増殖を行うワームの一種。2001年に世界中に感染を拡げ、このワームが行う攻撃活動のため、一時的にインターネットが繋がりにくい状態に陥ったこともあった。
＊3 Nimda：Microsoft製品の脆弱性を利用し、感染を拡げるワームで、ブラウザ、Webサーバ、メールという、複数の経路で感染を拡げることでは初期のタイプ。2001年に流行し、Webサーバを経由しての感染はCodeRedと同じ方法が用いられた。
＊4 SQLSlammer：Microsoftのデータベースエンジンの脆弱性を利用し、自己増殖を行うワームの一種。2003年に発見された直後、10分程度で爆発的に感染を拡げ、このワームが行う攻撃活動のため、世界中でネットワーク障害が発生した。
＊5 ゼロデイ攻撃：あるソフトウェアのセキュリティ上の脆弱な箇所が、広く公表される前にそれを悪用した攻撃が行われること。攻撃者が独自にソフトウェアの脆弱箇所を発見して攻撃を始めることを意味し、ソフトウェアベンダや企業側の対策が無い状態で攻撃が行われるため、攻撃を受けた場合被害に合うリスクが高い。

くの企業が拠所としてきたのが、ISO27000をはじめとするISMSファミリ規格である。

ここでは、ISMSファミリ規格で述べられている情報セキュリティマネジメントに関する考え方、及び代表的な管理策について述べる。

1. 情報セキュリティとは

「セキュリティ」とは、守るという考え方や行動である。

前述した多様化、かつ巧妙化している様々な脅威から、経営資源として欠かすことのできない「情報」や「資産」に加え、長い歴史を重ね築き上げてきた「企業ブランド」をも守らなければならない。

なぜなら、今やIT無しの企業活動は考えにくく、ITを安全にかつ積極的に活用することで、ビジネスチャンスが今まで以上に拡大できる半面、ITの誤用や悪用によりひとたび社会からの信用を失うと、事業継続そのものが困難な状況に陥る危険性もはらんでいるからである。さらに、悪意のある攻撃により加害者に仕立てられてしまう可能性も否めない。

それらを回避するためには、リスクに見合った対策を誰があるいはどの組織が講じていくかを決定し、確実に実行していくことが必要である。その一連の活動こそが、情報セキュリティマネジメントである。

「情報セキュリティ」とは、情報を守りながらも安全に活用できるように管理されていることであり、また、情報セキュリティが確保されている状態とは、情報の機密性、完全性、及び可用性が、適切に維持・管理されている状態である。

具体的には、**Table 1**の通りに定義されている。

情報システムマネジメントのフレームワークとして、情報セキュリティに関する国際規格である「ISO/IEC 27001：2013　情報セキュリティマネジメントシステム－要求事項」がある。また、情報セキュリティ確保のための具体的な管理策については、「ISO/IEC 27002：2013　情報セキュリティ管理策の実践のための規範」において、**Table 2**の通り14のカテゴリに分けて示されている。

Table 1　3 elements of information security
情報セキュリティの3要素

3 elements of information security 情報セキュリティの3要素	Definition 説明
Confidentiality 機密性	Only authorized people can appropriately use information asset. 許可された人だけが適切な情報資産を利用できること。
Integrity 完全性	Information asset is not falsified by unauthorized persons. 許可されていない人によって情報資産が不適切に変更されないこと。
Availability 可用性	Authorized individuals can use information asset when necessary. 許可された人が必要な時に情報資産を適切に利用できること。

Table 2　Control category based on ISO/IEC 27002：2013 [2)]
ISO/IEC 27002：2013に基づく管理策のカテゴリ

Control category	管理策のカテゴリ
Information security policies	情報セキュリティのための方針群
Organization of information security	情報セキュリティのための組織
Human resource security	人的資源のセキュリティ
Asset management	資産管理
Access control	アクセス制御
Cryptography	暗号
Physical and environmental security	物理的及び環境的セキュリティ
Operations security	運用のセキュリティ
Communications security	通信のセキュリティ
System acquisition, development and maintenance	システムの取得、開発及び保守
Supplier relationships	供給者関係
Information security incident management	情報セキュリティインシデント管理
Information security aspects of business continuity management	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
Compliance	順守

但し、あらゆる情報を守るために全ての管理策を同等に講じることが求められているわけではない。情報そのものの価値や脅威を受けた場合の影響度に鑑みて、費用対効果に見合った対策を優先順位をつけて講じることが重要であり、場合によっては経営判断が必要となる。

2. ISO/IEC 27002：2013において述べられた代表的な管理策

情報セキュリティ対策は、**Table 2**に示す通りであるが、一般的には**Table 3**の通り、組織的対策、人的対策、物理的対策、技術的対策の大きく4つに分けられる。

多くの技術的対策が示されてはいるが、それだけでは十分と言えず、ましてや脅威の変遷を踏まえると、むしろ包括的なマネジメントを実現するための組織的対策や人的対策がより重要となってきている。

なお、**Table 3**に記載されている管理策の具体例は、以下の通りである。

組織的対策

情報セキュリティに関する規定類を定め、経営者の承認を受け、全社及び関係者に周知することなどが必要である。

情報セキュリティは経営者が責任をもち、トップダウンで推進する必要があり、その推進においては各部門の責任者が調整することなどが必要である。

Table 3 Typical measures of ISO/IEC 27002：2013[3)]
「ISO/IEC 27002：2013　情報セキュリティ管理策の実践のための規範」の代表的な管理策

	Contents 目次	Control 管理策
Organized Measures 組織的対策	5.1.1 Policies for information security 5.1.1 情報セキュリティのための方針群	A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties. 情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知することが望ましい。
	6.1.1 Information security roles and responsibilities 6.1.1 情報セキュリティの役割及び責任	All information security responsibilities should be defined and allocated. 全ての情報セキュリティの責任を定め、割り当てることが望ましい。
Human measures 人的対策	7.2.2 Information security awareness, education and training 7.2.2 情報セキュリティの意識向上、教育及び訓練	All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. 組織の全ての従業員、及び関係する場合には、契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受け取ることが望ましい。
Physical measures 物理的対策	11.1.1 Physical security perimeter 11.1.1 物理的セキュリティ境界	Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities. 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、用いることが望ましい。
Technical measures 技術的対策	12.2.1 Controls against malware 12.2.1 マルウェアに対する管理策	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness. マルウェアから保護するために、利用者に適切に認識させることに併せて、検出、予防及び回復のための管理策を実施することが望ましい。

人的対策

情報セキュリティの意識向上のための教育を定期的に行うことなどが必要である。

物理的対策

情報処理施設におけるセキュリティを保つため、隔壁や認証ドアなど、情報セキュリティ区画内に物理的境界を設けることなどが必要である。

技術的対策

マルウェア対策のためのソフトウェアを導入し、その重要性やパターンファイルの最新化を利用者に意識づけ、異常時の対応に関する運用手順を定めることなどが必要である。

3. ISO/IEC 27001：2013、ISO/IEC 27002：2013 改訂のポイント

2013年10月1日に、ISO/IEC 27001：2013、及びISO/IEC 27002：2013が発行された。いずれも、既存の規格で示された根本的な取り組みを変更するものではなく、多くを2005年度版の継承としている。

しかし、他のISOマネジメントシステムの規格構成の共通化に伴い、全体的に強化・明確化されており、また、環境や技術の変化に対応した改訂となっている。

主な改訂のポイントは、以下の通りである。

ISO/IEC 27001：2013

- マネジメントシステム規格の共有化の適用

多くの企業が、組織のガバナンスを強化させるために、様々なマネジメント規格、例えば、品質：ISO 9001：2008、環境：ISO 14001：2004　などを採用している。

よって、マネジメントシステム間の整合性向上を図り、組織の負担を軽減するために、共通の目次である「上位構造」や「共通テキスト」、「共通用語定義」の使用を義務付けている。

- 新しいビジネス環境及びシステム環境へ対応

現代は、リスクマネジメントの社会といっても過言ではない。リスクをゼロにすることが不可能だからこそ、いかにリスクをコントロールするかが企業活動に必要不可欠である。

よって、原則的にすべてのマネジメントシステムにリスクの概念が導入され、それは「ISO 31000：2009リスクマネジメント－原則及び指針」が基本となる。

また、組織の方針を明確にする「情報セキュリティ目的」の導入により、経営層以下組織全体が企業活動に貢献するために目指すべき目的と、そこに至る道標としての目標を示し、確実に達成することが望まれている。

ISO/IEC 27002：2013

- 組織における情報の管理・取扱いに関する技術及び環境の変化に対応

外部委託により、組織の情報を活用するのは自らの組織だけであると限定できない環境となってきた。よって、供給者に対する管理策が一つにまとめられている。

また、クラウドサービスなどについても、供給者関係の部分に記載されている。

- 幅広い利用者に向けて、この規格を一層使いやすいものへ

情報セキュリティ管理策の指針を提供するが、技術的な詳細については、一般的な管理策の解釈や他の規格に譲り、削除されている。

4. PDCAからCAPDへ

マネジメントシステムの活動の基本としてPDCAサイクル（Plan→Do→Check→Act）がある。

しかし、最近では、現状の把握が十分にされないまま対策を計画、実行しても効果が薄いとの考えから、情報セキュリティの分野だけでなく、教育、防災、マーケティングなどの分野においても、CAPDサイクルの活用が提唱されている。

CAPDサイクルでは、まず組織の現状を正確に把握してリスクを可視化し、その結果を受けて有効な対策案を検討する。勿論、緊急性が高い場合は、直ぐに対策を実行する。そして、各組織に合った対策を計画し、着実に実行していく。

情報セキュリティの分野では、各フェーズによって、例えば、次の活動などがあげられる。

- C：監査、自己点検によるリスクの可視化
- A：リスク分析の結果を受け、必要な対策案を検討
- P：リスクに対応した対策の導入を計画
- D：対策の実行

PDCAサイクルあるいはCAPDサイクルのいずれにしても、各フェーズにおいて実施すべき活動が適切に行われることが重要である。

このように、技術や環境の変化に合わせ、ISMSファミリ規格といった国際規格やマネジメントの考え方も、対応し続けるのである。

制御システムセキュリティ

これまで、制御システムは固有かつ特殊な構成であり安全であると認識されてきた。しかし、システムのネットワーク化・オープン/汎用化が進んだ結果、イランの核燃料施設が被害を受けたStuxnet*6が示す通り、制御システムの安全神話は崩壊した。

こうした動向をしっかり踏まえ、制御システムの情報セキュリティ対策に取り組んでいくことが肝要である。

1. セキュリティインシデントの動向

Stuxnet以降、制御システムへの深刻なサイバー攻撃の被害報告はなされていない。しかし、イスラエルで犯行声明を伴った道路トンネル管理システムへの攻撃で8時間以上にわたり通行止めが起きる[4]など、脅威は高まっている。米国国土安全保障省からも、重要インフラ事業者への標的型サイバー攻撃の深刻化を懸念する発表がされている。

2. 制御システムセキュリティ対策の方向性

制御システムセキュリティ対策の方向性として、情報システムセキュリティ対策をベースとした、マネジメントシステムであるCSMS (Cyber Security Management System) が構築されている。

CSMSの国際標準は、IEC62443シリーズで定義されている。IEC62443-2-1は、**Table 4**及び**Table 5**の通り、制御システムセキュリティの固有要件を持つが、ISMSファミリ規格（ISO/IEC27001他）との共通要件も多い。

Table 4 Requirement analyses of IEC62443-2-1 and ISO/IEC27001[5]
IEC62443-2-1とISO/IEC27001の要件の分析

	IEC62443-2-1
Number of requirement 要件数	126
Unique requirement 固有要件	26
Common requirement 共通要件	100

Table 5 Unique requirement of IEC62443-2-1
IEC62443-2-1の固有要件

	Number of requirement 要件数
Risk identification, classification and assessment リスク識別、分類、及び評価	4
Security policy, organization, and awareness セキュリティ方針、組織、及び認識	3
Personnel security 要員セキュリティ	2
Physical and environmental security 物理的環境的セキュリティ	2
Access control アクセス制御	7
System development and maintenance システム開発とメンテナンス	3
Information and document management 情報・文書管理	1
Incident planning and response インシデント対応計画	2
Review, improve and maintain the CSMS CSMSの見直し・改善・維持	2

＊6 Stuxnet：2010年にイランを中心とする中東各地域で発見された、制御システムを標的としたコンピュータウイルスの一種。イランの原子力発電所に影響を及ぼした。

3. セキュリティ対策の取り組み

前項の通り、制御システムセキュリティは情報システムセキュリティをベースとし、制御系固有の差異をCSMSとして追加する二階建て構造と捉えると理解し易い。Table 6の様な相違点が情報システムと制御システムにあるため、情報システム部門と工務/製造部門が手を組む機会はこれまであまり無かった。しかし、北朝鮮からのサイバー攻撃を発表した韓国で原子力発電所をネットワークから完全に分離する[4]など、原子力をはじめとする制御システムの安全神話は崩れ、重要なインシデントに繋がる脅威がますます増している。これまでの範疇にこだわることなく互いに協力して、制御システムセキュリティに喫緊に取り組むことが大切である。

Table 6 Difference between information system and a control system
情報システムと制御システムの相違点

	Information system 情報システム	Control system 制御システム
Priority 優先度	C: Confidentiality 機密性 I: Integrity 完全性 A: Availability 可用性	A: Availability 可用性 I: Integrity 完全性 C: Confidentiality 機密性
Renewal Term 更新タイミング	3 – 5 years 3年～5年	10 – 20 years 10年～20年
Department 担当部署	Information System Department 情報システム部門	Engineering Works/Producing Department 工務/製造部門
Required Performance 要求性能	Non-real-time 非リアルタイム Delay and a stop are permitted. 遅延や停止は許容	Real Time リアルタイム Delay and a stop are fatal. 遅延や停止は致命的
Threats and Risks 脅威･リスク	Loss of data and business opportunities データ、ビジネス機会の喪失	Loss of human life, equipment, and products 人命、設備、製品の喪失

グローバル経営の製造業にとっての情報セキュリティの課題

グループ企業にとっては、自社だけではなく、グループ会社のいずれかが攻撃者に侵入されると、グループ全体に影響が及ぶことが懸念される。制御システムも危機にさらされている以上、BtoBが中心の製造業にとっても例外とは言えない。

以下にグローバル経営企業がグループ全体を統制して情報セキュリティを維持するための課題と、住友化学グループでの、情報システムを対象にした取り組み事例を紹介する。

1. グローバル統制

(1) 統制のための枠組み[6]

情報セキュリティリスクをマネジメントするためには、対策製品を導入するだけではなく、前述の各種規格に定めるようにマネジメントの枠組みを整備し、継続的に運営することが必要になる。すなわち、規程を定め、体制の役割・責任を明確にし、それに基づいてリスク管理策を定着化・推進する活動のPDCAを回すことである。

しかし、企業の抱えるリスクは情報セキュリティ以外にも様々に存在する。これらの対策は、経営方針に基づいて適正な投資配分を行う必要がある。また、様々なリスクを横断的に捉えた上で、対策が計画・推進され、経営層がその状況・結果を把握・評価できなければならない。そして、それらの取り組みや情報セキュリティに対する意識の向上を組織内に徹底させるには、経営層が主導する形が望ましい。

(2) 住友化学グループにおける枠組み

住友化学グループでは、近年、本社情報システム部門主導によるグループ共通の取り組み推進を強化している。経営層をメンバーとする内部統制委員会の下で、それぞれのリスクの主管部署を定めてリスク対策を管理することで、グループ全体のリスクマネジメントを行っている。この枠組みの中で情報システムセキュリティを重要リスクの一つと位置づけて、経営層が主導する形で取り組みを進めている。

2005年、まずは本社において情報システムセキュリティポリシーを制定し、情報システムセキュリティマネジメント体制を構築、情報システムの導入・運用、及び情報システムセキュリティの推進における基本的な基準を定め、実装してきた。そして、徐々に同様の規程・体制の構築・運用をグループ各社にも要求し、本社組織からその整備・運用状況の監査を行っている。

また、冒頭に述べたようなリスクの高まりを受け、これらの枠組みをさらに確かなものにし、変化にスピーディに対応していくため、本社規程類をグループ共通としようとしている。これによってグループ各社への要求をより明確にし、共通の物差しでグループ全体が評価できるようにする。また、これらの規程類を本社情報システム部門で維持管理を行うことで、グループ全体が素早く外部の脅威の変化に備えることができるようにする。

さらに、グループ各社が自主的に行うモニタリング・評価活動として共通の「自己点検」のスキームを定め、グループ各社で年に1度実施することを計画中である。規程類の提示と遵守状況の監査を本社情報システム部門が行うだけではなく、グループ各社が自立して

「自己点検」、問題点の把握、改善計画、改善の実行のCAPDサイクルを回すことが狙いである。

(3) 海外グループ会社に対する取り組み

グローバル経営を行う企業にとって、海外拠点は、一般的に本社から目が届きにくく、統制が難しいことが多い。しかし、前述のようにその弱点をつかれた被害事例も発生しており、このような海外拠点をマネジメントすることはグループ全体の情報セキュリティにとって重要な課題となる。

住友化学グループでは、海外主要地域にリージョナルヘッドクオータを設置し、IT専任要員を配置している。そして、エリア内のグループ会社のITマネジメントを統括し、その中で情報セキュリティ推進指導を行っている。

しかし、一部の地域では、グループ各社の情報セキュリティを推進するためのIT要員の確保が困難であったり、雇用の流動性が激しくようやく確保した要員もスキルが要求水準に上がった途端に辞めてしまうことがある。そのため、本社やリージョナルヘッドクオータからの指導だけでは、なかなか進まない場合も多い。外部のITベンダに委託しても、ベンダコントロールが十分に行えなければ、セキュリティ対策製品を導入しているにもかかわらず適切な運用が行われないなどの懸念もある。また、グループ各社が個々にリソース調達や対策ソリューションを維持していると、グループ全体でみれば運用コストが重複することになる。

こうした問題への対策として、住友化学グループでは、地域ごとの共有ITサービスを起ち上げようとしている。基本的なIT基盤を、マネジメントも併せてサービス提供することで、自社だけではITマネジメントが困難なグループ各社においても、一定の情報セキュリティの維持を最適なコストで行えるようになることが狙いである。

東南アジア地域のように、国や言語が多岐にわたるような地域では、サービス全体のコントロール、サービス利用するグループ各社ごとのマネジメント業務やサービスデスク業務、現地での実作業、それぞれで役割分担をする構造を取ろうとしている。全体のコントロールはリージョナルヘッドクオータが、利用各社ごとのマネジメント業務・サービスデスク業務は、地域全体をカバーできる大手ベンダが担う。現地作業は、高度なスキルを要するものは大手ベンダが各国のサイトに指示をし、比較的簡易な作業はグループ各社が利用するローカルベンダを継続して使用する構想である(**Fig. 1**)。これによって、ユーザ対応やマネジメント対応の品質を維持しつつ、多言語への対応やスピーディなオンサイト作業を可能にする。また、ローカルベンダを活用することで、運用費用を抑えることができる。

このような共有ITサービスの一部はすでに稼働中であるが、今後本格的に各地域内に展開していかなければならない。サービスの拡大にあたっては、世界中の様々な国の法規などにも細やかに対応していくことが今後の課題である。

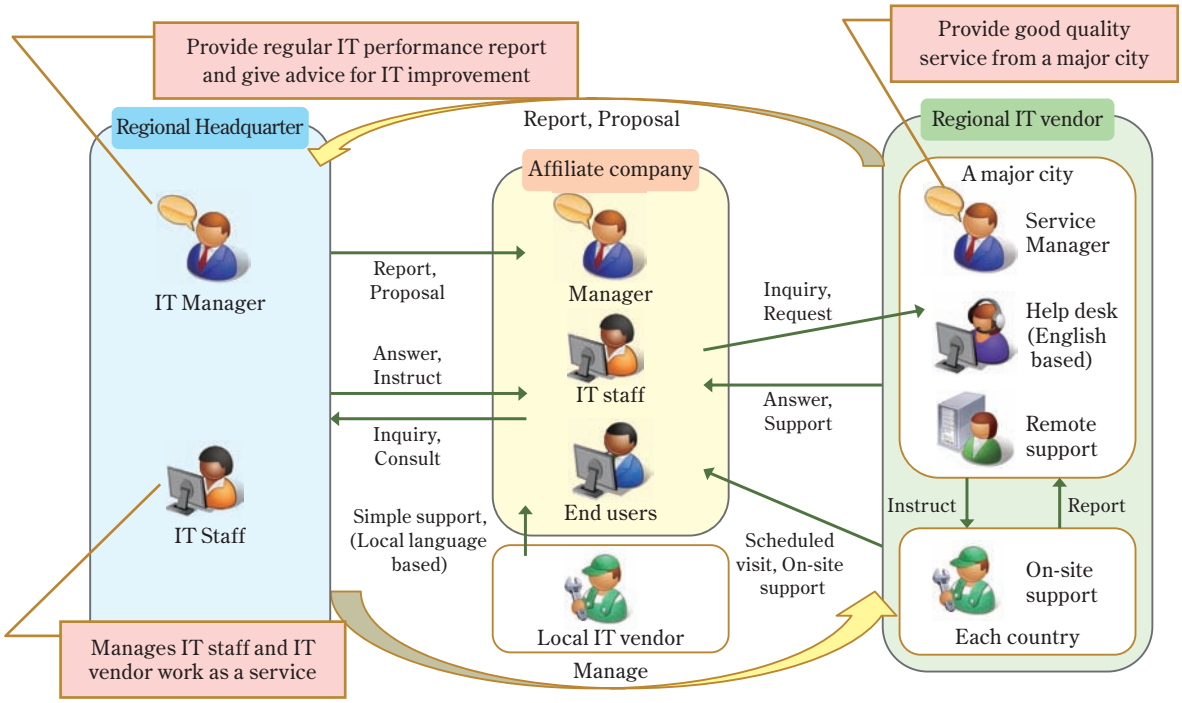

Fig. 1 Operational image of the Regional IT Service
地域ITサービスの 運用イメージ

2. グループ全体の文化とするために

これまで述べたマネジメントの枠組みや共有ITサービスが定着したとしても、新たなサービス加入を行うことや、モニタリング活動によって発見された問題点への対処を実施することは、グループ会社に負担を強いることになる。グループ各社は当然、情報セキュリティにかけるコストはできるだけ抑えたい思いがある。とりわけ、昨今の石油化学業界の厳しさを背景に、コスト削減要求は激しい。全社リスクマネジメント組織からのトップダウン推進を行っているとは言え、正しくリスクを理解していなければ、コストとそれによって得られるセキュリティとのバランスで適正な投資判断ができないことも想定される。

こうしたことが起こらないようにするために、グループ各社の投資判断をする上位層の社員に、脅威や情報セキュリティの重要性を正しく理解してもらうべく、教育・啓蒙活動を継続的に行わなければいけない。

また、そういった経営に近い立場になる以前から、基本的な情報システムの利用に関する注意事項や、立場に応じて求められる責任を、定期的に、あるいは立場が変わるイベントごとに、全ての社員にしっかりと理解してもらう。そうすることで組織としてのマネジメントがよりスムーズに行われ、対策費用も最低限に抑制できるだろう。

一方で、グループ各社に情報セキュリティ対策を受け入れてもらうために、情報セキュリティの必要性を説くだけではなく、より魅力的なサービス提供や費用削減の努力を弛まずに行う。そして、それを各社に丁寧に説明して、受け入れやすいシナリオを考えていくことが、グループ唯一の情報システム会社である我々の課題である。

おわりに

本稿では、IT環境と脅威の動向を解説し、企業が情報セキュリティリスクをマネジメントするための代表的な手法を説明した。そして住友化学グループでの事例に基づき、グローバルなグループ経営企業の課題を紹介した。

ITは日々目覚ましい進歩を遂げ、我々の社会生活の利便性を向上するだけでなく、ワークスタイル自体を変革しようとしている。

企業は、グローバル化で競争激化する経済環境にあって、経営をスピードアップし、企業価値を高めるために、これらのITを駆使することを躊躇することはできない。

攻撃者と脅威を正しく理解し、適切な情報セキュリティマネジメントをすることは、もはや事業を継続しようとする企業にとって、必須要件となりつつある。

住友化学グループの世界中のお客様に、資源、エネルギー、食糧、環境など国際社会が抱える課題解決に貢献する製品、技術を提供し続けるため、当社はグループにおける情報セキュリティマネジメントを確立していく。

引用文献

1) “2013年版10大脅威～身近に忍び寄る脅威～”, ㈱情報処理推進機構 (2013).
2) “ISO/IEC 27002：2013　情報セキュリティ管理策の実践のための規範” (2013), piii.
3) “ISO/IEC 27002：2013　情報セキュリティ管理策の実践のための規範” (2013), p2.
4) 宮地 利雄, “制御システム・セキュリティの現在と展望　この1年間を振り返って”, (一社) JPCERTコーディネーションセンター (2014), p.11, http://www.jpcert.or.jp/ics/2014/20140205ICSC-JPCERTCC_Miyachi.pdf (参照 2014/3/24).
5) “制御システムにおけるセキュリティマネジメントシステムの構築に向けて～ IEC62443-2-1の活用のアプローチ ～”, ㈱情報処理推進機構 (2013), p.16. http://www.ipa.go.jp/files/000014265.pdf (参照 2014/3/24).
6) “情報セキュリティガバナンス導入ガイダンス”, 経済産業省 (2009), http://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf (参照 2014/3/24).

PROFILE

中井　加津代
Kazuyo NAKAI
住友化学システムサービス株式会社
IT戦略室

清水　寿美
Sumi SHIMIZU
住友化学システムサービス株式会社
IT戦略室
シニアマネージャー

兼平　崇之
Takayuki KANEHIRA
住友化学システムサービス株式会社
IT戦略室