住友化学グループにおける情報セキュリティの確保に向けて

住友化学システムサービス(株)
ソリューション部
鈴　木　龍　大

Ensuring Information Security in Sumitomo Chemical Group

Sumitomo Chemical Systems Service Co., Ltd.
Solution Department
Tatsuhiro Suzuki

Sumitomo Chemical Group treats ensuring information security as one of its business issues, and has promoted information security management in the whole group. When managing information security in the group, points to ponder and approaches to take are different from when managing it in a single company. This article will discuss the approaches, issues, solutions for the issues and future efforts regarding ensuring security management in Sumitomo Chemical Group, by using some case examples in 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。

しかしながら、海外を含めたグループ会社の中には、まだ十分に情報セキュリティ対策が実施できていない会社も残っており、グローバル連結経営を実現するためには、情報セキュリティを、より一層強化していかなければならない。

また、コンプライアンス経営やCSR経営（Corporate Social Responsibility：企業の社会的責任）の重視、および、会社法や金融商品取引法等による内部統制の強化など、情報セキュリティに係わる社会的要請は、ますます高まってきている。

このような背景の下、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、住友化学グループでの事例に基づき、マネジメントの観点から、グループ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、および、更なるセキュリティ強化に向けた今後の取り組みについて述べる。

情報セキュリティ確保

1. 情報セキュリティとは

ヒト・モノ・カネに次ぐ経営資源である「情報」は、企業競争力を左右するほど重要なものであり、企業活動において効果的に活用することが求められる。しかしながら、情報の重要性の高まりに応じてリスクも高くなるため、情報は、危害や損傷を受けることなく安全な状態で管理する必要がある。このように、情報を安全な状態で管理することを、「情報セキュリティ」という。

情報セキュリティに関する国際規格である「ISO/IEC 27001:2005 情報セキュリティマネジメントシステム－要求事項」[1]（以下、ISO/IEC 27001:2005）では、情報セキュリティを「情報の機密性、完全性及び可用性を維持すること」と定義している。Table 1は、ISO/IEC 27001:2005[1]に基づく「機密性」、「完全性」、「可用性」の定義を示している。

機密性、完全性、可用性は、情報セキュリティの3要素と言われ、それぞれの要素をバランス良く維持することが重要である。

Table 1 Definition of 3 concepts of information security based on ISO/IEC 27001:2005
ISO/IEC 27001:2005に基づく情報セキュリティの3要素の定義

3 concepts of information security 情報セキュリティの3要素	Definition 説明
Confidentiality 機密性	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. 認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性。
Integrity 完全性	The property of safeguarding the accuracy and completeness of assets. 資産の正確さ及び完全さを保護する特性。
Availability 可用性	The property of being accessible and usable demand by an authorized entity. 認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。

2. 情報セキュリティ確保に向けた基本的な考え方

前述のとおり、情報は、企業競争力を左右する重要なものであるため、情報セキュリティ確保は、確実かつ優先的に実施しなければならない。しかしながら、企業の経営環境を無視して全ての対策を講じるのではなく、あくまでも経営的な観点からリスクを評価し、費用対効果に見合った対策を実施することが重要である。

また、ITの進歩や事業形態の変化に応じてセキュリティリスクは日々変化していくため、リスクの変化に応じて情報セキュリティ対策を適宜見直し、常に情報セキュリティを最適な状態で維持することも忘れてはならない。

情報セキュリティ対策の実施は、費用対効果を考慮したうえで、経営資源の投資を含め、最終的に経営者が判断する。従って、企業のシステム部門やIT責任者は、経営者がリスクを適切に評価し、正しい意思決定ができるよう、リスク分析の結果やリスク対策の効果などを、分かりやすく、かつタイムリーに経営者に提示することが求められる。

3. 情報セキュリティ確保のための管理手法（情報セキュリティマネジメント）

情報セキュリティを確保するための管理手法としては、情報セキュリティマネジメントシステム*1（ISMS：Information Security Management System）のフレームワークが、国際規格（ISO/IEC 27001:2005[1]）として定められている。

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、同シリーズの国際規格「ISO/IEC 27002:2006 情報セキュリティマネジメントの実践のための規範」[2]（以下、ISO/IEC 27002:2006）で定められた、情報セキュリティ確保のための管理策が広く利用されている。

ISO/IEC 27002:2006[2]では、Table 2で示すとおり、情報セキュリティ確保のための管理策を11のカテゴリに分けて定義している。

各企業は、自社の抱えるリスクの分析結果に基づき、それぞれの管理策を参考にして、自社にとって最適な管理策を考案し、導入することにより、情報セキュリティを確保していくのである。

Table 2 Category of controls to ensure information security (ISO/IEC 27002:2006)
情報セキュリティ確保のための管理策のカテゴリ（ISO/IEC 27002:2006）

Category of controls to ensure information security 情報セキュリティ確保のための管理策のカテゴリ
1. Security Policy セキュリティ基本方針
2. Organization of information security 情報セキュリティのための組織
3. Asset Management 資産の管理
4. Human Resource Security 人的資源のセキュリティ
5. Physical and environmental security 物理的及び環境的セキュリティ
6. Communications and operations management 通信及び運用管理
7. Access Control アクセス制御
8. Information systems acquisition, development and maintenance 情報システムの取得、開発及び保守
9. Information security incident management 情報セキュリティインシデントの管理
10. Business continuity management 事業継続管理
11. Compliance 順守

これらの国際規格と、企業における情報セキュリティマネジメントシステムとの関係を整理すると、Fig. 1のようになる。Fig. 1で示すとおり、情報セキュリティの確保は、情報セキュリティに係わる国際規格を参考にして、経営戦略と整合のとれたマネジメントシステムを確立、運営することにより、実現できるのである。

また、ISO/IEC 27001:2005[1]では、「Plan－Do－Check－Act（計画－実施－点検－処置）」（PDCA）モデルを採用しており、組織における情報セキュリティマネジメントを、継続的に発展させていくことが求められている。

＊1 マネジメントシステムとは、組織の方針、手段およびプロセスを管理し、継続的に改善するためのフレームワークのことである。

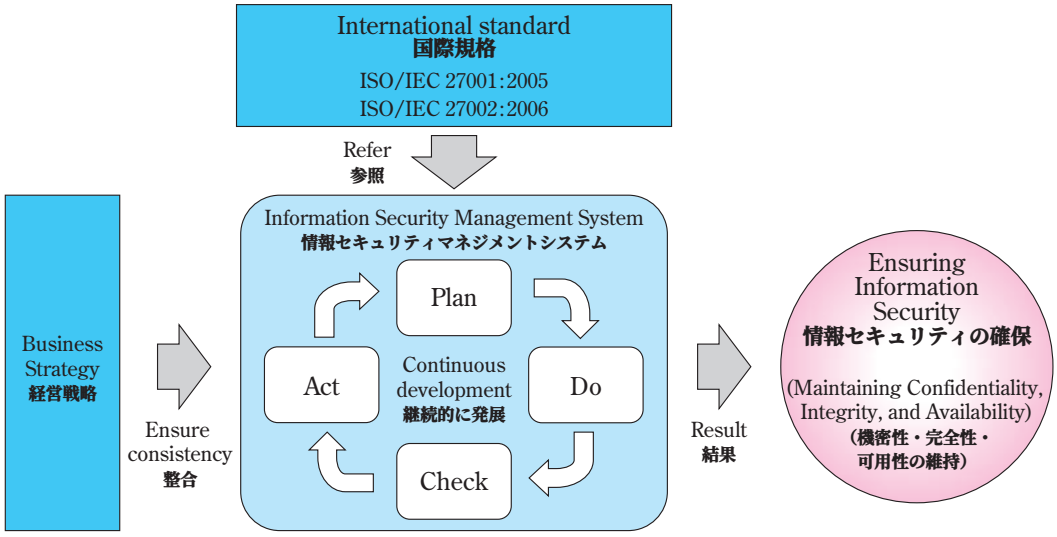


Fig. 1 Image of actions in companies for ensuring information security
企業における情報セキュリティ確保の取り組みイメージ

4. グループにおける情報セキュリティマネジメント

ISO/IEC 27001:2005[1]で定められた情報セキュリティマネジメントのためのフレームワークは、特に組織の規模や事業形態を特定していないため、単一の企業だけでなく、グループ全体に適用することも可能である。しかしながら、同一グループ内の企業であっても、事業形態や規模、IT専任要員の有無、ITの利用状況など、グループ各社により、それぞれ置かれている状況が異なるため、一律に同じ対策を適用することは現実的ではなく、グループ特有のアプローチが必要となる。

経済産業省が平成21年6月に公表した「情報セキュリティガバナンス導入ガイダンス」[3]では、グループにおける情報セキュリティマネジメントを実施するにあたってのアプローチが紹介されている。以下、それぞれのアプローチの要約を示す。

(1) ベースラインアプローチ

「ベースラインアプローチ」とは、情報セキュリティマネジメントのための共通的なベースライン（目的・目標・管理策）を設定し、グループ内の全ての会社において、一律にベースラインをクリアすることを求めるアプローチのことである。

ベースラインアプローチでは、グループの基本方針を満たした、妥当性かつ実効性のあるベースラインを設定することが重要となる。

(2) グループ企業マッピング

「グループ企業マッピング」とは、業種や規模および予算などにより、グループ内の会社を分類し、それぞれのタイプ別に、求められる情報セキュリティ要件を定め、適用していくアプローチのことである。

グループ企業マッピングの場合、「どの要素を分類軸にしてグループ内の各社を分類するか」という点が重要なポイントとなる。

(3) IT基盤や体制の共通化・統合化

「IT基盤や体制の共通化・統合化」とは、リスク管理やコスト削減の観点から、グループ企業間でIT基盤や体制を、共通化・統合化するアプローチのことである。

また、IT基盤や体制の共通化・統合化以外にも、ユーザ教育のためのコンテンツなどを共有することも有効である。

住友化学グループにおける情報セキュリティマネジメントの取り組み

住友化学㈱（以下、住友化学）では、2000年に自社のセキュリティ規程を整備し、情報セキュリティ確保に取り組んできた。また、2006年より、住友化学グループ全体の情報セキュリティを確保するという方針のもと、グループにおける情報セキュリティマネジメントの確立・運営を進めてきた。

住友化学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するにあたっては、ISO/IEC 27001:2005[1]で定められた情報セキュリティマネジメントのフレームワークに加え、ベースラインアプローチ／グループ企業マッピングといった、グループ全体に対するセキュリティマネジメントのアプローチを参考にして、住友化学グループにとって最適な進め方を採用してきた。

以下、住友化学グループにおける情報セキュリティマネジメントについての基本的な考え方を述べたうえで、PDCAモデルの流れに沿って、その取り組みを紹介する。

1. 情報セキュリティマネジメントの考え方

住友化学グループにおける情報セキュリティマネジメントは、Fig. 2に示すとおり、グループ全体のマネジメントシステムが、グループ各社におけるマネジメントシステムを包含する、階層構造で進めている。

グループ全体、およびグループ各社のマネジメントシステムは、いずれもPDCAモデルを採用しており、各社のマネジメントシステムが、グループ全体のマネジメントシステムのDo（実施）の部分に位置付けられる。

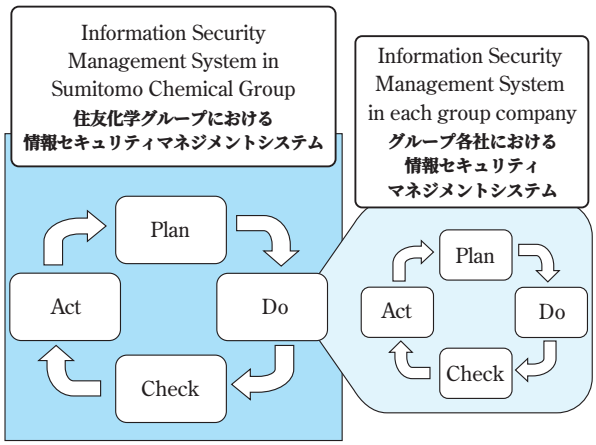


Fig. 2 Information security management structure in Sumitomo Chemical Group
住友化学グループにおける情報セキュリティマネジメントシステムの構造

2. （Plan）情報セキュリティマネジメントの確立

Plan（計画）フェーズでは、基本方針の定義や推進体制の整備を行う。具体的には、次の3つの点を考慮して活動を進めていく。

- グループ全体の基本方針の定義
- グループ各社の分類、およびタイプ別のベースラインの設定
- コミュニケーションルートや推進体制の整備

以下、上記3つのポイントに沿って、住友化学グループの事例を紹介する。

(1) グループ全体の基本方針の定義

グループ全体の情報セキュリティマネジメントを確立するにあたり、まず、「グループとして、どのような姿勢で情報セキュリティ確保に取り組むのか」といった、情報セキュリティマネジメントにおける、グループとしての基本方針を定義する。

住友化学グループでは、グループ全体で情報セキュリティ確保に取り組むという方針を示している。また、グループ各社における情報セキュリティ確保は、各社が自らの責任で実施し、各社の抱えるリスクに応じたセキュリティ対策を講じるようにしている*2。

住友化学では、情報セキュリティに係わる文書体系をFig. 3のとおり定義しており、グループ各社に対しても、セキュリティ規程を社則として制定し、情報セキュリティマネジメントを確立することを要求している。

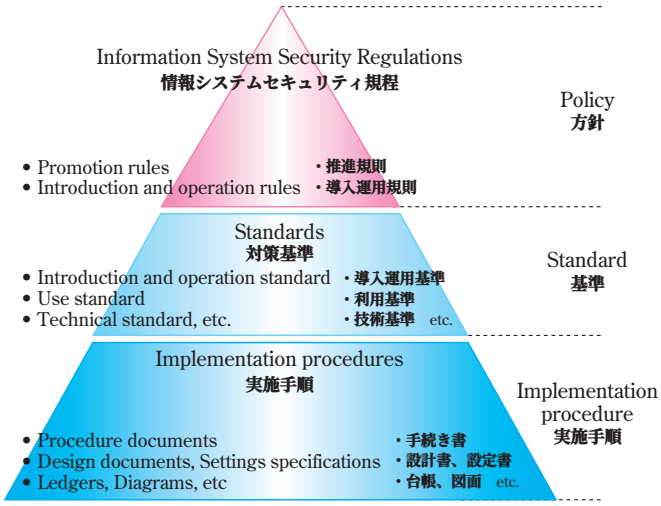


Fig. 3 Documents structure concerning information security in Sumitomo Chemical
住友化学における情報セキュリティに係わる文書体系

(2) グループ各社の分類、およびタイプ別のベースラインの設定

情報セキュリティの確保は、各社の抱えるリスクに応じて、費用対効果に見合った対策を実施すべきである。そのため、グループ全体における情報セキュリティマネジメントを進めるにあたっては、グループ内のすべての会社に一律に同じ対策を実施するのではなく、事業形態や会社の規模等に応じてグルー

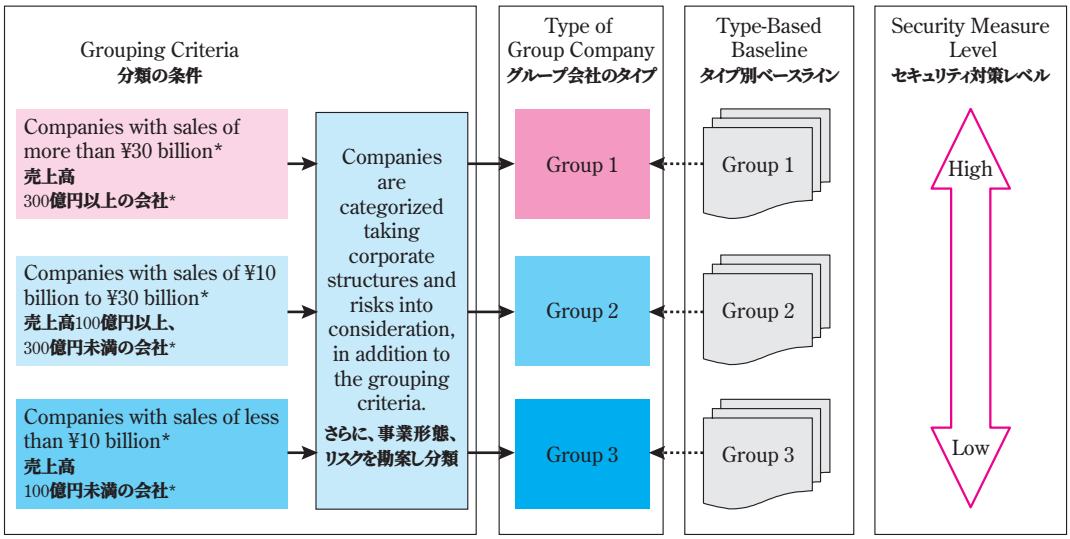
*2 住友化学グループでは、情報セキュリティの中でも、特に電子化された情報や情報システムを対象にセキュリティ確保を進めてきたため、「情報セキュリティ」でなく、「情報システムセキュリティ」という表現を用いている。しかし、本稿では、「情報セキュリティ」で統一している。

プ各社を分類し、タイプ別にベースラインを設定することが有効である。タイプ別のベースラインの設定は、経済産業省の「情報セキュリティガバナンス導入ガイダンス」[3]で紹介されている、ベースラインアプローチとグループ企業マッピングを組み合わせた方法と言える。

住友化学グループでは、売上規模や事業形態、および各種リスクを考慮して、グループ各社を3つのタイプに分類している。また、住友化学のセキュリティ規程・基準をベースに、これら3つのタイプ別のベースラインを定め、テンプレートとして各社に開示することにより、グループ各社の情報セキュリティマネジメントが円滑に進むようにしている。Fig. 4は、グループ各社の分類とタイプ別のベースラインの設定を示している。

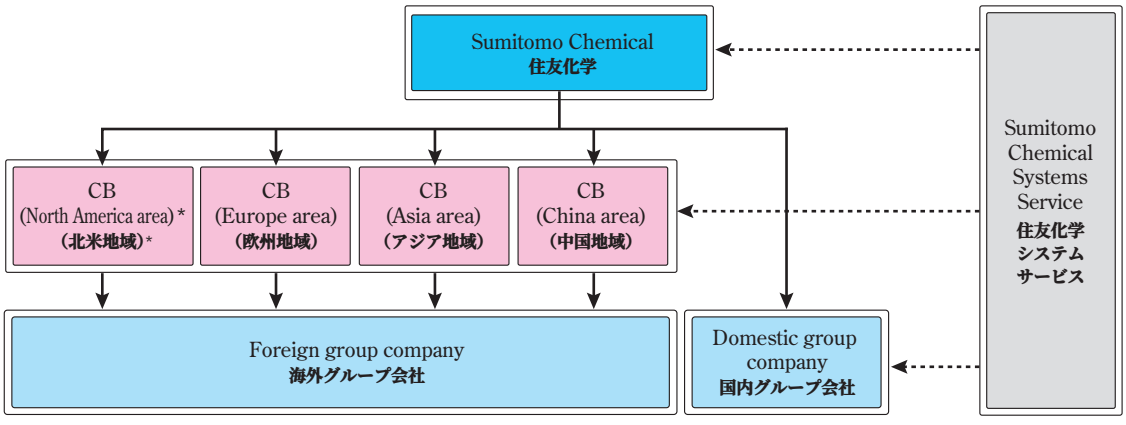
(3) コミュニケーションルートや推進体制の整備

グループ全体の情報セキュリティマネジメントを確立するにあたっては、グループ各社とのコミュニケーションを十分にとり、グループの基本方針やベースラインなどを徹底する必要がある。そのため、定期的に情報共有や意見交換のためのミーティングを開催し、グループ全体で情報セキュリティに対する意識を高めていくことが有効である。また、グループ全体、およびグループ各社の情報セキュリティマネジメントを推進していく体制を整備することも重要である。



* calculated before consolidated accounting
連結前

Fig. 4 Category of group companies and type-based baseline setting
グループ各社の分類とタイプ別のベースラインの設定



* Will be established
設置予定

Fig. 5 Information security management promotion structure in Sumitomo Chemical Group
住友化学グループにおける情報セキュリティマネジメントの推進体制

住友化学グループでは、2006年に、住友化学と住友化学システムサービス㈱（以下、当社）が一体となって、国内外のグループ各社に対して、グループとしての基本方針やタイプ別のベースラインなどを説明して徹底を図った。以降、グループ各社との情報共有や意見交換のため、定期的にミーティングを開催している。

また、情報セキュリティマネジメントを推進する体制としては、欧州・アジア・中国にITサポート拠点（Corporate Branch：CB）を設け、近隣地域のグループ各社をサポートする体制を整備している。今後、北米にもITサポート拠点を拡大する予定である。

Fig. 5は、住友化学グループにおける情報セキュリティマネジメントの推進体制を表している。

2.（Do）情報セキュリティマネジメントの導入・運用

前述のとおり、Do（実施）フェーズは、グループ各社における活動が主体となる。従って、グループ全体としての情報セキュリティマネジメントの導入・運用は、次の2つの点を考慮して活動を進めることになる。

- グループ各社における情報セキュリティマネジメントの導入支援
- グループ全体の進捗状況の把握

以下、上記の2つのポイントに沿って、住友化学グループの事例を紹介する。

(1) グループ各社における情報セキュリティマネジメントの導入支援

グループ各社の中には、大小さまざまな規模の会社が存在するため、IT専任要員を持たない会社も多数存在する。情報セキュリティマネジメントを導入するにあたっては、ITに関する専門知識が必要となるため、IT専任要員を持たない会社に対しては、セキュリティ規程の整備やリスク分析など、各社における導入作業の支援が必要となる。

住友化学グループでは、グループ唯一の情報システム会社である当社が、グループ各社における情報セキュリティマネジメントの導入を、サービスとして提供することで、グループ各社の活動を円滑に進めるよう支援している。各社の活動を支援するサービスには、セキュリティ規程整備支援、リスク分析・対策検討支援、セキュリティ教育実施支援といったサービスが含まれる。

(2) グループ全体の進捗状況の把握

グループ全体としての情報セキュリティマネジメントを確実に導入するためには、グループ各社の情報セキュリティマネジメントの実施状況を把握し、何か問題が発生した場合は、適宜対応をとっていく必要がある。

住友化学グループでは、グループ各社における情報セキュリティマネジメントの導入を促進するための手段として、グループ各社におけるセキュリティ規程の整備状況を把握し、定期的に開催するミーティングでその進捗を管理している。

3.（Check）情報セキュリティマネジメントの監視・見直し

Check（点検）フェーズでは、グループ各社における情報セキュリティマネジメントが有効に機能し、情報セキュリティが確保されていることを確認する。また、計画段階で定めたベースラインの妥当性などについても合わせて確認する。

確認のための手段としては、グループの内部監査を利用して、情報セキュリティ監査を実施することが有効である。情報セキュリティ監査の方法論としては、経済産業省が平成15年4月に公表した「情報セキュリティ監査基準」[4]、および、情報セキュリティ監査基準に付随する各種ガイドラインが広く利用されている。

住友化学グループでは、2008年度より、住友化学によるグループ内部監査の一環として、情報セキュリティ監査を実施している。グループ内部監査では、3年を1サイクルとして、国内外のグループ各社に対する監査を実施している。内部監査を、点検のみでなく、助言・啓発の場として利用し、グループ全体の情報セキュリティマネジメントが有効に機能するようにしている。

また、情報セキュリティ監査の手法としては、経済産業省の「情報セキュリティ監査基準」[4]、および情報セキュリティ監査基準に付随する各種ガイドラインを参考にして、住友化学グループとしての監査手順を整備し、監査を行っている。

4.（Act）情報セキュリティマネジメントの維持・改善

Act（処置）フェーズでは、監査で発見した事実に基づき、必要に応じてベースラインや運営方法の改善を図ることで、グループ全体の情報セキュリティマネジメントを、継続的に発展させていく。

住友化学グループでは、監査で発見した課題を関係者間で共有し、必要に応じて、グループ全体としての情報セキュリティマネジメントの進め方や、タイプ別のベースラインの見直し等を実施している。

具体的な課題や対策の事例は、次章で説明する。

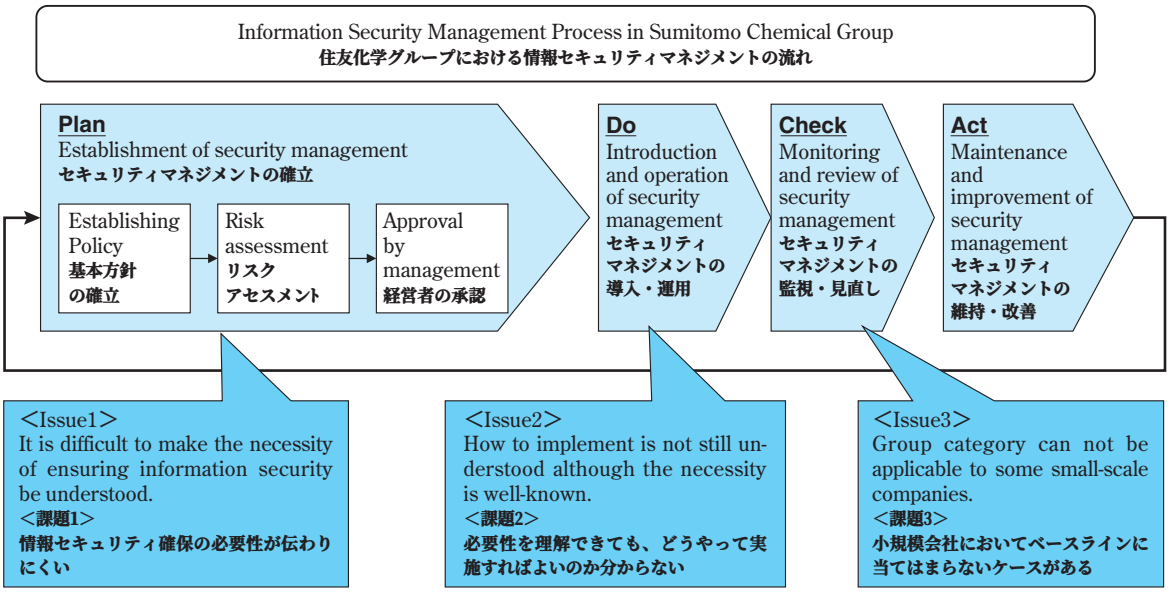


Fig. 6 Issues of information security management in Sumitomo Chemical Group
住友化学グループの情報セキュリティマネジメントにおける課題

住友化学グループの情報セキュリティマネジメントにおける課題と対策

住友化学グループの情報セキュリティマネジメントでは、大小さまざまな課題に対応し、適宜改善を進めている。Fig. 6は、住友化学グループの情報セキュリティマネジメントを確立、運用していくにあたって発生した課題を表している。

以下、Fig. 6で挙げた3つの代表的な課題について解説するとともに、課題解決に向けて実施した対策についても説明する。

1.〈課題1〉情報セキュリティ確保の必要性が伝わりにくい

住友化学グループでは、グループ各社における情報セキュリティ確保は、各社が自らの責任で実施し、各社の抱えるリスクに応じたセキュリティ対策を講じるようにしている。しかしながら、2006年にグループの基本方針を示した当初は、グループ各社のセキュリティ規程の整備は順調には進まなかった。

原因として、グループ各社に対して、情報セキュリティ確保の必要性が十分に伝わっていないことが考えられたため、定期ミーティングの場を利用して、セキュリティ被害の動向などを共有することとした。その結果、各社のセキュリティに対する意識が高まり、各社におけるセキュリティ規程の整備状況は、前進し始めた。

情報セキュリティ確保の必要性を伝えるためには、できるだけ身近なテーマでの事例を繰り返し紹介し、どの会社も似たようなリスクを抱えているという事実について、認識を持ってもらうことが重要である。

2.〈課題2〉必要性を理解できても、どうやって実施すればよいのか分からない

グループ各社の中には、規模が小さく、IT専任要員を持たない会社も多数存在する。IT専任要員がいない場合、情報セキュリティ確保の必要性（why）は理解できても、何を（what）、どうやって（how）実施すればよいのか分からないため、各社における情報セキュリティマネジメントの導入が進まなかった。

この課題を解決するため、住友化学グループでは、当社がグループ各社における情報セキュリティマネジメントの導入支援として提供しているサービスの内容を見直し、グループ各社のIT責任者に、セキュリティ対策の意義を理解してもらうようにした。具体的には、Fig. 7で示すとおり、セキュリティ対策の内容に加えて、セキュリティ対策の意義や対策実施時のポイントを説明し、IT責任者のセキュリティ意識を向上していった。セキュリティ対策の意義を理解することで、外部に業務委託している作業についても、その妥当性をチェックできるようになる。

IT責任者は、各社における情報セキュリティマネジメントの推進役であり、セキュリティ対策の可否について、経営者が適切な判断ができるよう、正確に情報を伝える責任を担っている。グループにおける情報セキュリティマネジメントの成否は、各社のIT責任者の理解度により大きく左右されるため、IT責任者の意識向上が重要な課題となる。

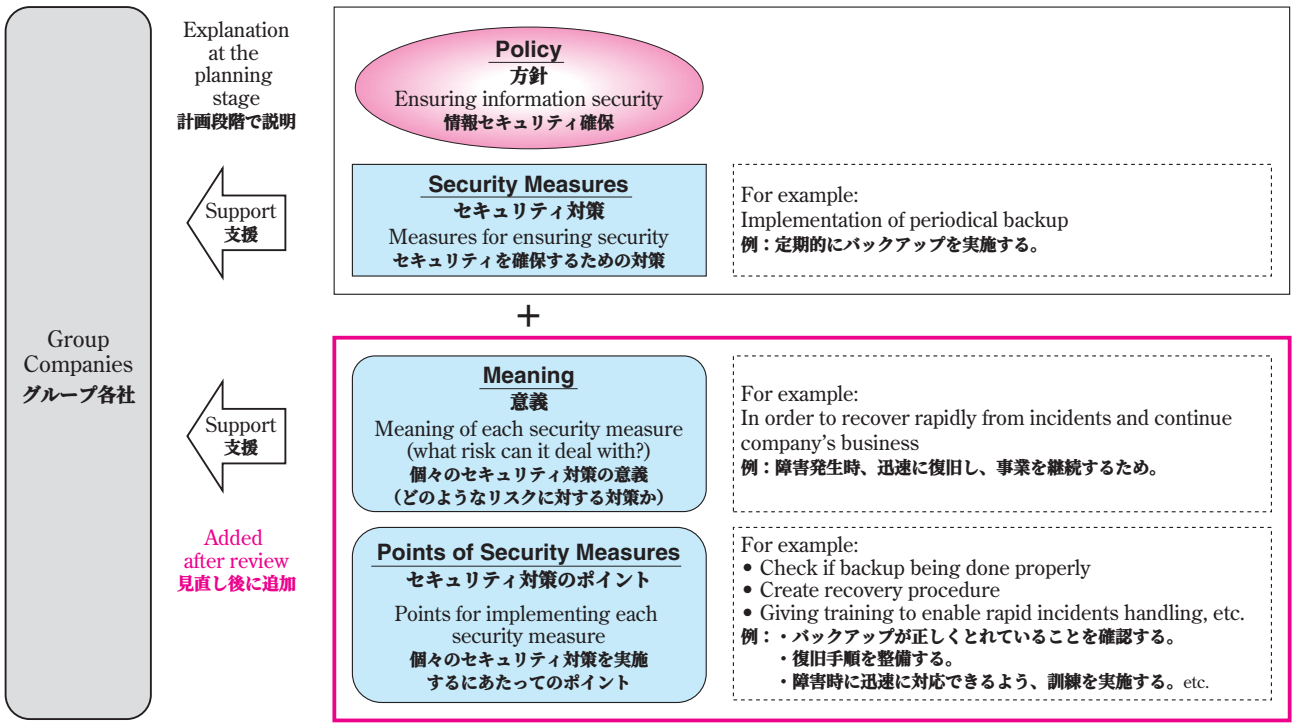


Fig. 7 Review of support for group companies to implement security measures
グループ各社に対するセキュリティ対策支援の見直し

3.〈課題3〉小規模会社においてベースラインに当てはまらないケースがある

住友化学グループでは、売上規模や事業形態などを考慮してグループ各社を3つのタイプに分類し、タイプ別にベースラインを定め、テンプレートとしてグループ各社に配布した。しかし、実際に海外を含めたグループ各社に展開してみると、ITへの依存度が低い会社や、IT資産を自社では殆ど持たない小規模な会社など、ITリスクが想定したよりも低い会社が存在した。

そのため、計画段階で定めたタイプ別のベースラインを見直し、ITリスクが低い会社にも適用できるベースラインを設定した。ベースラインの見直しにあたっては、ISO/IEC 27002:2006[2)]で定められた管理策のカテゴリを意識し、必要な要素は漏らさないようにした。

セキュリティ対策は、企業の抱えるリスクに応じて、費用対効果に見合った対策を講じることが重要である。従って、グループ各社に適用するベースラインについても、各社の状況を把握した上で、現実的かつ実効的なものにしていくことが重要である。

本章では、3つの事例から課題と対策を説明した。共通的に言えることは、「事実を正確に把握し、適宜改善を実施することが重要」という点である。特に、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る場合、事実を正確に把握することが困難になるため、日頃からグループ各社とのコミュニケーションを十分にとっておく事が必要となる。

住友化学グループのセキュリティ強化に向けた今後の取り組み

住友化学グループでは、グループ全体のマネジメントシステムの確立・運用、および、技術的対策の実施等により、大きな被害は防止できる対策を講じている。しかしながら、今後、グループ連結経営を更に進めていくにあたり、より一層、グループ各社の情報セキュリティを強化していく必要がある。

また、今後は、IT基盤や体制の共通化・統合化といった、品質向上やコスト低減の取り組みも進めていかなければならない。

以下、住友化学グループにおける情報セキュリティマネジメントの強化に向けた、今後の取り組みについて述べる。

1. セキュリティ意識をより一層高める

これほど世間で情報セキュリティに関する事故が報道されているにも係わらず、未だに情報漏洩やシステム不具合といったセキュリティ事故が後を絶たない。セキュリティ事故は、社会的信用の低下や巨額の損失につながるなど、一度発生すると、企業にとって取り返しのつかない大きな痛手となることが多い。

住友化学グループの情報セキュリティマネジメントにおいては、これまで実施してきた活動を継続するとともに、セキュリティ意識をより一層高める取り組みを強化することが重要であると考えている。

セキュリティ意識向上の手段としては、内部監査の一環で実施している情報セキュリティ監査に加えて、自己点検（セルフチェック）の有効性に着目している。

自己点検とは、グループ各社のIT責任者が、セキュリティ対策のために実施している自分達の活動状況を、評価シート*3 などに基づき、自ら点検する行為であり、継続的なセキュリティ意識の維持・向上に有効とされている。また、計画段階で定めた作業の漏れの確認や、作業の有効性確認のためにも、自己点検を活用できる。

2. IT基盤の共通化・統合化

住友化学グループでは、IT基盤の共通化や統合化を実現するため、グループ共通のIT標準を整備し、グループ各社への適用を進めている。基幹システムやネットワーク環境においては、既に複数会社で共通化・統合化を実現しているものもあり、グループ各社は、個々にIT基盤を持つのではなく、サービスとして購入し、利用している。

住友化学では、今後、PC管理やウイルス対策ソフトの運用など、国内外のグループ各社向けに、IT基盤の共通化・統合化の範囲を拡大していくことにより、全体最適を進め、更なるコスト低減や合理化を目指している。

3. データの有効活用による効果的かつ効率的なマネジメントの実現

住友化学グループでは、国内外のグループ各社に対する情報セキュリティ監査を実施しているため、グループ各社における情報セキュリティマネジメントの実施状況について、詳細な内容を把握できる。グループ各社に対する監査は、3年を1サイクルとして実施しているため、1サイクルが完了する時点（予定では2011年）では、グループ全体の状況を詳細に把握できることになる。

蓄積したデータを有効活用することで、事実に即した対策が講じられるようになるため、先に述べたIT基盤の共通化・統合化などの課題を、より効果的に実施できる。例えば、セキュリティリスクの高い地域を優先してIT基盤の共通化を実施することにより、情報セキュリティを確保し、被害を未然に防ぐといった対応がとれるようになる。

今後は、監査からのインプットだけでなく、定期ミーティングや自己点検の結果も随時反映し、データの更新周期を短くすることで、マネジメントの精度を向上することを目指している。

おわりに

本稿では、住友化学グループでの事例に基づき、マネジメントの観点から、グループ全体における情報セキュリティ確保の取り組みを説明してきた。グループにおける情報セキュリティマネジメントは、一朝一夕で実現できるものではない。しかし、一歩一歩確実に進めていくことで、情報セキュリティを確保するだけでなく、グループ各社間の連携強化によるスピード感のあるマネジメントの実現といった、ワンランク上の活動も実現できるようになる。

企業のITへの依存度が高まる中で、ますますセキュリティリスクは大きくなる。また、我が国の政策としても、説明責任の観点から、各社における情報セキュリティマネジメントの状況を社内外のステークホルダーに報告書として開示するといった、情報セキュリティガバナンスの強化が求められる傾向にある。

住友化学グループにおける情報セキュリティマネジメントは、事業環境や法規制の変化にフレキシブルかつスピーディに対応できるとともに、今後のグローバル連結経営を支えるIT基盤として実効性のあるものでなければならない。

そのためには、グループ各社とのコミュニケーションをより一層強化し、互いにセキュリティ意識を高める活動を続け、グループ全体で一体感を持って取り組んでいけるような、全体最適のマネジメントシステムに仕上げていくことが重要となる。

引用文献

1) ISO/IEC 27001:2005　情報セキュリティマネジメントシステム－要求事項.
2) ISO/IEC 27002:2006　情報セキュリティマネジメントの実践のための規範.
3) 経済産業省：平成21年6月，情報セキュリティガバナンス導入ガイダンス.
4) 経済産業省：平成15年4月，情報セキュリティ監査基準.

*3 評価シートには、「セキュリティ意識教育を、年1回実施しているか？」など、グループ方針に沿った評価項目が列記されており、各社のIT責任者が評価結果を記入する。これにより、各社のIT責任者自らが、自社のセキュリティ対応状況をチェックできるようになる。

PROFILE

鈴木　龍大
Tatsuhiro Suzuki
住友化学システムサービス株式会社
ソリューション部