[連載] ISMS適合性の監査から有効性の監査へ

2. 見えないものには対応できない —情報セキュリティリスクの可視化—

2.1. 情報セキュリティリスクの把握

目に見えているリスクにはそれに合った適切な対応策をとることができます。しかし、目に見えていないリスクに対しては、その特性を考慮できず、一般的な対応策のみで適切ではないかもしれません。
リスクアセスメントの結果、多くの情報資産のリスクが分析されます。これらの重要度、脅威、脆弱性、リスク、およびリスク対応策が適切かどうかなど、内部監査でどのように判断するのでしょうか。

例えば、「新製品図面」という情報資産があります。

■ **重要度**
企業の将来を左右するような新製品であれば、重要度は非常に高いものです。

■ **脅威と脆弱性**
電子データであれば漏えい、改ざん、紙データであれば、盗難、紛失、滅失などが起きては困るインシデントです。

■ **リスクとリスク対応**
電子データへのアクセス権管理や定期的なバックアップ、紙データの耐火書庫などへの保管と施錠などのリスク対応策が考えられます。

もしかすると、これは見えているリスクへの一般的対応策であって、見えていないリスクがあるかも知れません。

見えていないリスクの例を挙げてみます。

■ **図面の完全性**
図面に変更が生じたとき、変更の情報は関連する部署や協力会社へ正確にもれなく伝えられているでしょうか。

■ **図面の機密性**
部品製作のために協力会社に図面を提供しているとき、その図面の機密性が確保された環境で保管され、適切に取り扱われているでしょうか。また、協力会社が更に他の協力会社に業務委託している場合、再委託先の機密性は確保されているでしょうか。
これらの状況は契約書や覚書などに明記され定期的にチェックしているでしょうか。

■ **ライフサイクル**
新製品図面の発生から廃棄までのライフサイクルは決められ、かつその記録はあるでしょうか。特に、協力会社に提供し開発を業務委託した図面類は、契約完了時に適切に返却または廃棄されているでしょうか。

■ **図面の移送**
その図面を移送するとき、例えばメールでの暗号化や輸送時の手渡しなど、誤送信や紛失などのリスク対応策を検討し、実施しているでしょうか。

などなど

これらのリスクを発見するには、情報資産それ自体の機密性·完全性·可用性のリスク分析だけでは不足なようです。リスク分析の対象は、情報資産と情報資産のセキュリティに影響を与える物理的な保護（ファシリティ）、情報資産の運用（ライフサイクル）、法令、規制、契約書の順守事項などもあります。

2.2. 見えないリスクの可視化

組織のあらゆる事項を可視化することは、正確な現状把握によってリスクを見つけ出し、適切な対策を導き出すためにも有効です。

組織の特徴を知っているつもりでも、可視化すると実は知らないことや勘違いしていることが多く見つかります。

では、どのようなものを可視化できればよいのでしょうか。

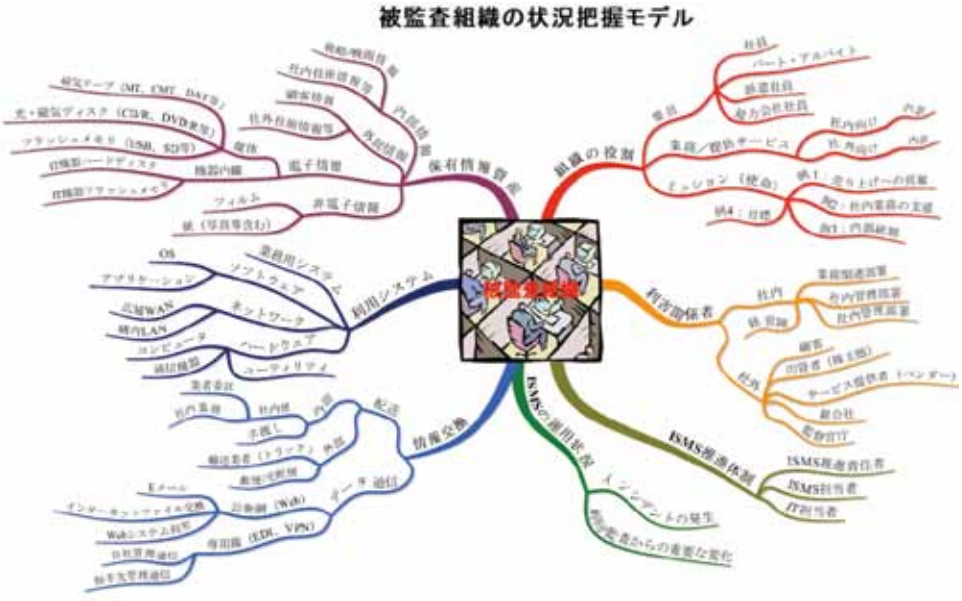
- 組織の実態と特徴
- 組織を取り巻く環境
- 潜在的リスク（脅威）
- 脆弱性
- リスク対応策

被監査部署の可視化は監査相手を知ることです。監査相手を知ることで、内部監査ポイントを重点化することができます。限られた時間で、効果的な監査を実施するには、重点ポイントをはずさないことです。

どのように可視化したらよいのでしょうか。

- ISMSの構築と維持のために作成した業務関連図
- I情報資産の抽出のために作成した業務フロー
- IISMS推進部署、被監査組織へのインタビュー情報
- 社内資料の調査

など、いろいろな手段がありますが、ここでは可視化のツールとしてマインドマップによるモデル化の例を示します。



リコージャパン株式会社 ソリューションマーケティング本部 コンサルティング推進室 情報セキュリティコンサルティンググループ 羽田 卓郎氏　提供

図 2-1　【参考】可視化手法「マインドマップ」の例　ー被監査組織の状況把握モデルー

トニー･ブザン（Tony Buzan）氏によって考案されたマインドマップは、「キーワード」の連鎖での記述が基本です。人間の頭脳には、大量の記憶が納められていますが、それを取り出すのが「キーワード」です。箇条書きや文書によらず、キーワードさえあれば自分の頭脳から膨大な記憶を引き出すことができます。分析者の思考過程が「キーワードの連鎖」の形で可視化されるため、参加者全員でその思考過程を共有し、レビューすることができます。

被監査組織を可視化できれば、見えているリスクと見えていないリスクの関連も分かってきます。そして、それまで見えなかったリスクに気づきます。

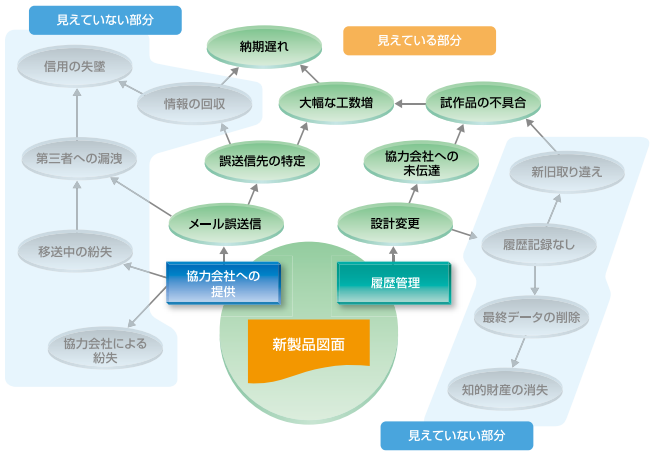


図 2-2 新製品図面に関連する可視化の例

監査側と被監査側は同じ情報を共有することが望まれます。どちらのレベルが低くても、組織のマネジメントシステムは劣化してしまいます。ISMSでは、組織の状況（プロフィール）やリスク認識を共有することで、より高いレベルのマネジメントシステムを目指すことができます。

2.3. リスク分析対象の構造

通常、情報資産を中心にリスクアセスメントが実施されています。

しかし、ISMSでは特定された事業上の要求事項、特定された法令および規制の要求事項に対するリスクアセスメントも要求されています。

情報資産に対する脅威は、情報資産の運用（情報のライフサイクル）や、情報資産の置かれている環境（ファシリティ）、および情報資産に関連する法令、規制、契約などへの順守などが関係するため、これらを含めたリスクアセスメントを実施しなければなりません。

情報資産を保護するには、以下のリスク分析対象の構造を理解しておきます。

- ■ 情報
- ■ 情報を格納している媒体
- ■ 媒体を保管している設備
- ■ 設備の置かれている環境（部屋、建物、敷地など）
- ■ 電子媒体の情報操作のためのIT機器とソフトウェア
- ■ IT機器への電源の供給や通信などのサービス
- ■ これらを運用する人

などです。

情報資産に関わるリスク分析対象を分類します。

(1) 情報
(2) 物理的資産
(3) サービス資産
(4) ソフトウェア資産
(5) 無形資産
(6) 人材

リスクアセスメントでは、これらの情報資産が組織、すなわちISMS適用範囲にあるかどうかを確認し、もれのない資産台帳を作成し、その脅威を識別し、脆弱性を認識し、そして対策を検討します。

内部監査では、リスク分析対象が組織の中で認識され、適切にリスクアセスメントされているかをチェックする必要があります。

次回は「3. ビジネスの維持･発展のための監査とはなにか　―有効性監査の実際―」です。