中小企業において目指すSecurity By Design

2020年11月5日

JNSA　日本ネットワークセキュリティ協会
西日本支部
中小企業のための Security by Design WG

目次

はじめに

本書は JNSA 西日本支部の「中小企業のための Security by Design WG」の活動をまとめたものです。

本 WG の目的を以下に示します。

【WG の目的】

これまでの西日本支部の活動の成果物を基に、経営者から IT システム投資の承認を得た後、中小企業の情報システム部門が考えるべき IT システムの導入、運用、廃止までのライフサイクルを考慮した情報セキュリティのあるべき姿を検討します。

なお、本書における「Security By Design」の目的を以下に示します。

IT システムの開発・導入においては、機能要件の定義が主になり、セキュリティ機能は非機能要件として、 重要視されず、後回しにされることが多々あります。しかし、一般的に IT システムの開発・導入においては、図1に示すように後工程での修正になるほどコストが増加する傾向にあり、IT システム導入後、十分なセキュリティ対策を行うことは、困難となります。従って、IT システムの企画・設計段階から、セキュリティを考慮した設計(Security by Design)の導入が重要となります。

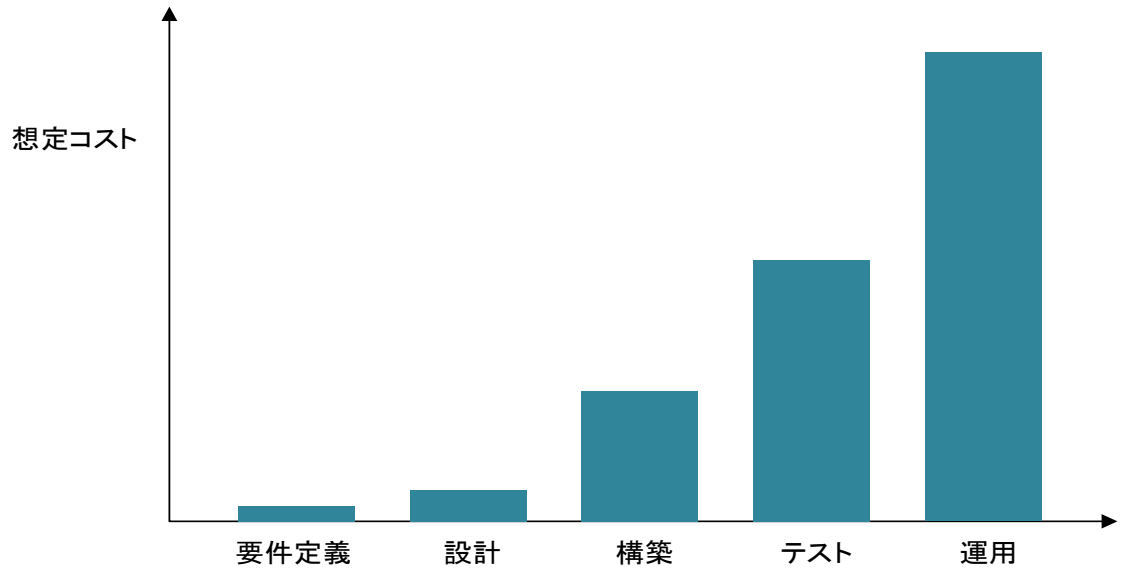


図1 IT システム開発工程とコストの関係

設計・導入段階で考慮すべき、コントロール、運用確認等セキュリティ要素の関係、体制及び運用を以下に示します。

- 「コントロール　技術的対策実装」と「運用確認・監視」 は対の関係となる。
- 「運用確認・監視」に必要な機能、体制は「コントロール　技術的対策実装」 段階にて整

備する。

- OODAループに対応可能な技術的対策、運用と体制も整備する。

V 字モデルにおける「Security By Design」の位置付けを図2に示します。

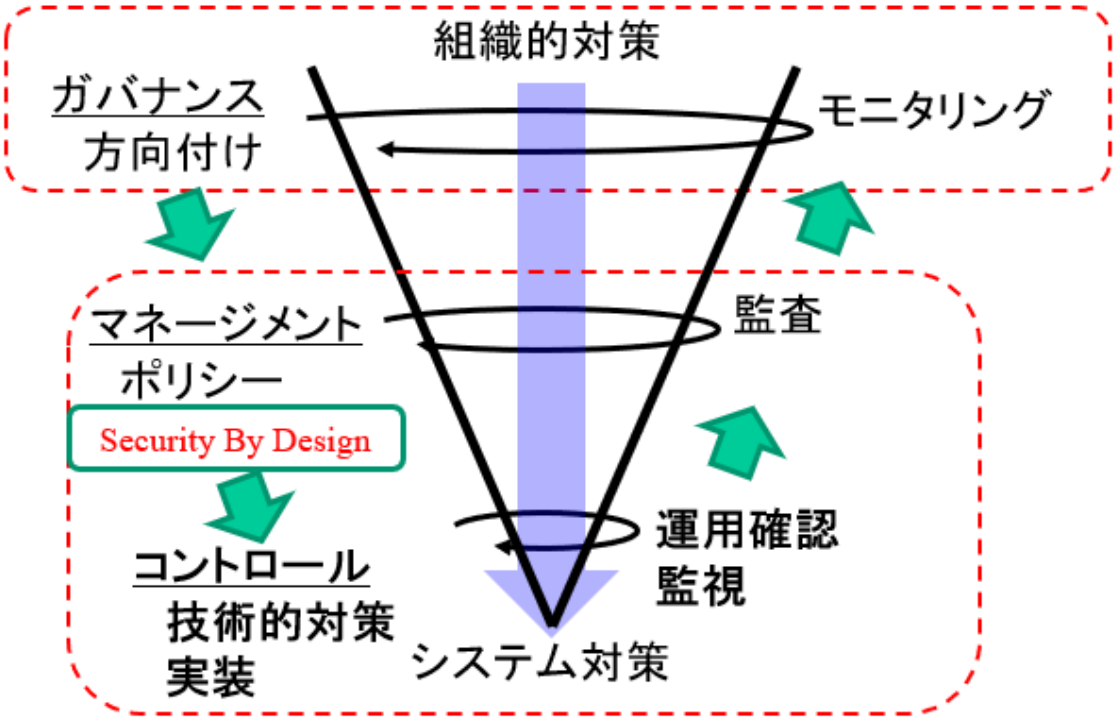


図2 V 字モデルにおける「Security By Design」の位置付け

1. これまでの西日本支部の活動と今回の活動

西日本支部での活動は、これまで「情報セキュリティ対策を行うことを前提とする組織」を支援する成果物を作成してきました。

一昨年度までの西日本支部の活動と成果物は、以下の3点であり、一連の情報セキュリティ対策プロセスを支援するものです。

- 日常業務に潜むリスクを認識する「気づき」
  「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」
  (略称 9to5 、参照先 https://www.jnsa.org/result/2013/chusho_sec/index.html)

- 認識したリスクを評価し受容レベルの決断、導入する対策の決定、その対策の日々の実施を文書化する「運用」
  「情報セキュリティポリシーサンプル改版(1.0 版)」
  (略称 ポリシーサンプル、参照先 https://www.jnsa.org/result/2016/policy/index.html)

・　その対策状況を確認する「チェック」
　「中小企業向け情報セキュリティチェックシート」
　（略称　チェックシート、参照先 https://www.jnsa.org/seminar/nsf/2014kansai/）

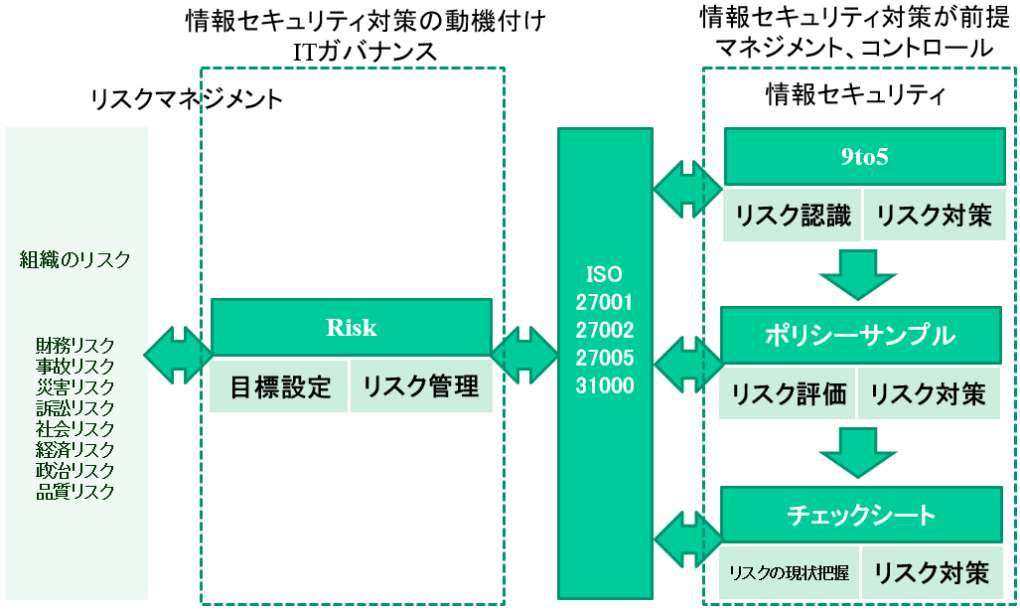
しかし、これらの活動は、組織の情報セキュリティ対策を行う動機付けが不確かな「情報セキュリティ対策を行うことが当たり前となっていない組織」にとっては、経営者が情報セキュリティ対策への投資を決断するには不十分ではないか、と西日本支部では考えました。また、以下のような仮説を立ててみました。

・　経営者は、IT にも情報セキュリティにも興味はない
・　経営者の興味は、売り上げ、利益目標を達成するうえでの、経営課題の解決である

そこで、西日本支部では、自組織の社会における位置付け、社会や顧客からの期待といった「外部状況」と、自組織における現状の情報セキュリティへの取り組み状況を現す「内部状況」の両面から「組織の状況」の確定を行い、自組織が目指すべき情報セキュリティ対策と現状とのギャップを明示することで、IT 及び情報セキュリティ投資が、経営課題の解決に繋がるとの結論となり、経営者に情報セキュリティ対策への投資を決断してもらう動機になると考えました。
その考え方に基づいて、整理した結果を成果物としてまとめたものが次の資料です。

・　「経営者のための情報セキュリティ対策―ISO31000 から組織状況の確定の事例―」
　（略称　Risk、参照先 https://www.jnsa.org/result/2018/west_tebiki/）

なお、西日本支部のこれらの活動は、ISO　規格を考慮しています。各活動と成果物の関連性および成果物と ISO 規格との関係を図3に参考表示します。



ISO27001:情報セキュリティマネジメントシステム(要求事項)

ISO27002:情報セキュリティマネジメントの実践のための規範

ISO27005:情報セキュリティのリスクマネジメントに関するガイドライン規格

ISO31000:リスクマネジメント―指針

図3　JNSA 西日本支部のこれまでの活動の成果物と ISO 規格との関係図

１．１.「経営者のための情報セキュリティ対策」(Risk WG) の振り返り

「Risk　WG」では以下の考えに基づき、外部状況、内部状況の明確化を通じ、情報セキュリティ対策の改善点を洗い出すことで、経営者の情報セキュリティ対策への投資の動機付けとなると考えました。

- 外部状況が自組織のセキュリティ対策の動機付けとなり、目指すセキュリティの姿が定まる。
- 内部状況は、自組織における現状の情報セキュリティへの取り組み状況を現すものであり、内部要因による現状のセキュリティレベルとなっている。
- 目指すセキュリティ対策の姿と現状のセキュリティレベルの差異が改善すべき対策となる。

補足)外部状況と内部状況から目指すビジネスの姿、IT システムの姿も導き出すことができます。

この推論からセキュリティにおける外部状況、内部状況の関係を図4に、目指すセキュリティレベルの姿との差異が確認された場合において、外部状況を踏まえた組織体制や方針・戦略へのフィードバック、内部影響因子への説得、またリソース、人員、投資への再配備などの PDCA 活動を図5に示します。

なお、詳細については（https://www.jnsa.org/result/2018/west_tebiki/）を参照して下さい。

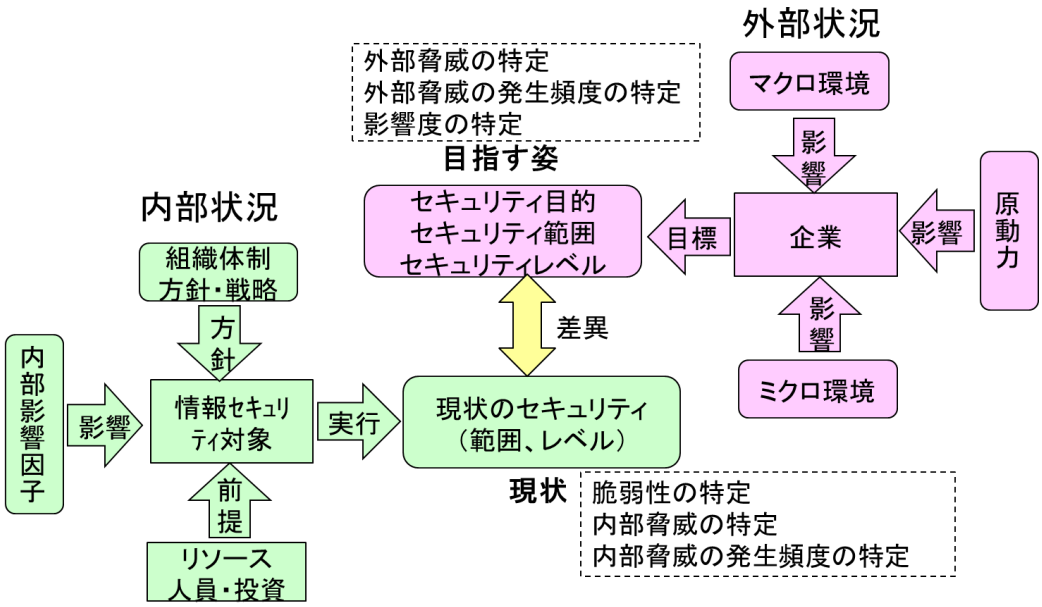


図4　セキュリティにおける外部状況と内部状況の関連

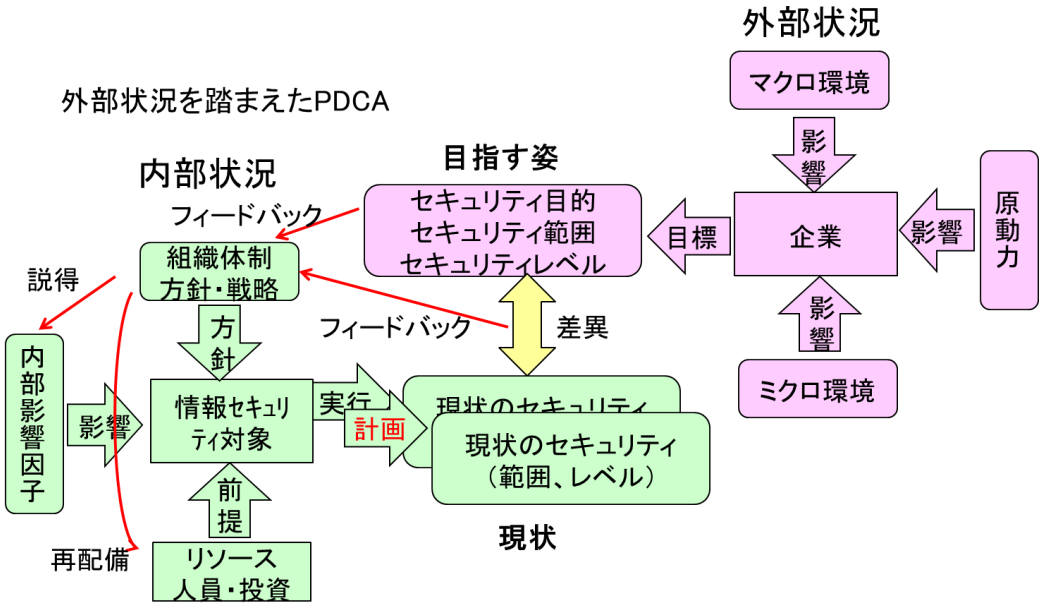


図5　目指す姿との差異が確認された場合

さらに「Risk WG」では様々な企業の情報セキュリティ対策が考えられるため、いくつかの仮想モデル企業を想定し、それらの企業毎に、経営者の視点による外部状況、内部状況を整理し、経営者に必要な対策を訴求するために、現状と目指す姿との差異を洗い出すためのプロセスの見える化を行いました。図6にプロセスの見える化の例を示します。

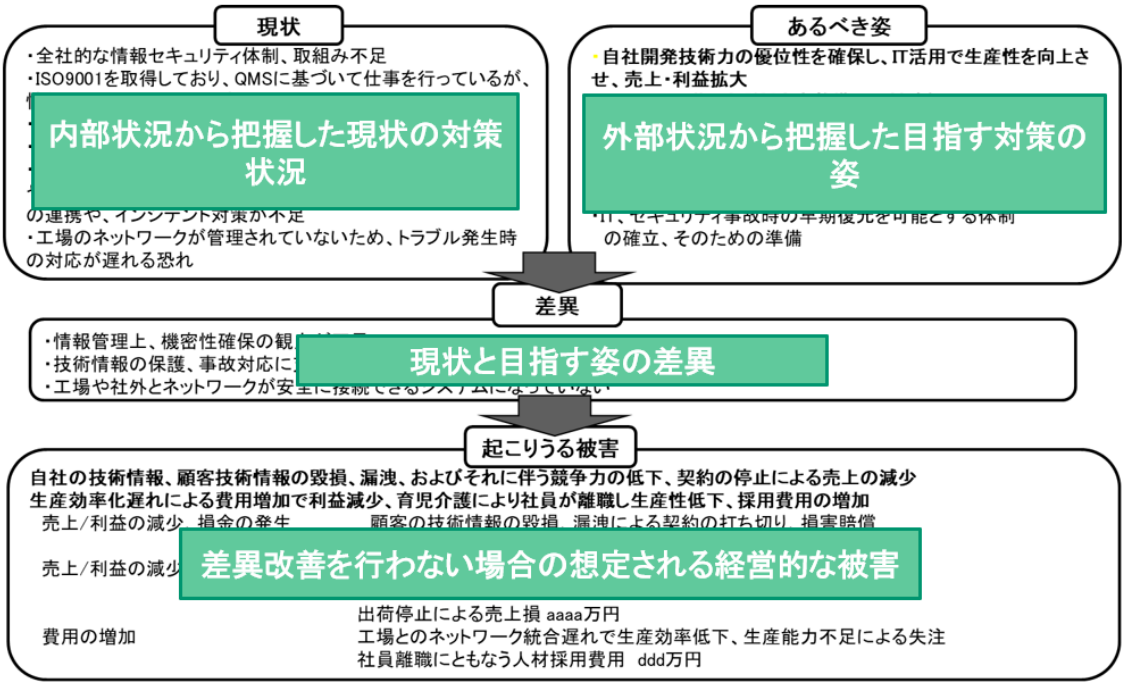


図6　現状と目指す姿の例

また改善施策については、図7に示す投資費用、回収計画という形で見える化を行いました。

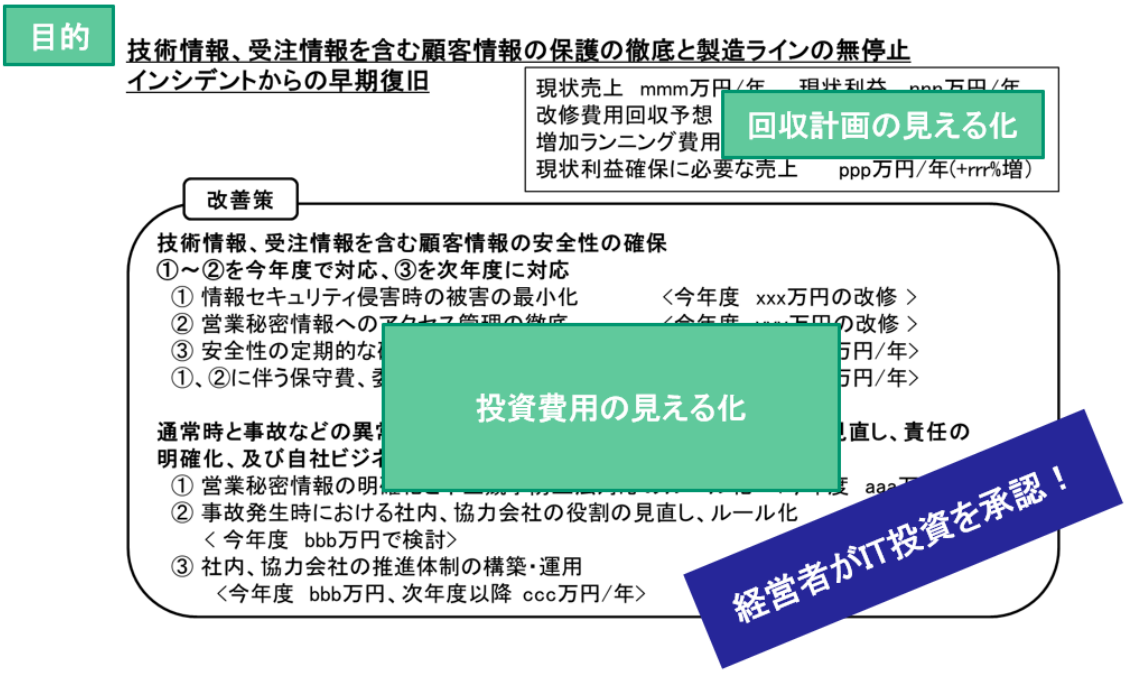


図7　投資計画と回収計画の例

１．２．本書の位置付け

本書は IT システムへの投資を承認した経営者と、経営者の承認に基づき具体的な情報セキュリティ対策の導入を行う情報システム部門を対象としています。

前項に示す「Risk　WG」から IT システムと情報セキュリティに取り組む方針が決定し、経営者の IT システム投資の承認を得た後、洗い出した改善策の具体化から始めることになります。

すなわち「Risk　WG」から続く IT システムと、情報セキュリティ対策の改善の具体化を、IT システムの企画段階で明らかにすることです。

図3に示す「9 to 5」、「ポリシーサンプル」、「チェックシート」は、情報セキュリティ対策を意欲的に進める組織に有用なツールではありましたが、経営者に情報セキュリティ対策の投資への理解が得られるものではありませんでした。

そこで「Risk　WG」では、経営者に情報セキュリティ対策の必要性を認識してもらい、投資を決意してもらうところまで進めました。

情報セキュリティ対策の具体化時に、様々な制約や立ちはだかる壁を乗り越え、効果のある運用とするために、明らかにすべき事項とそれに基づく要求仕様の作成を可能とする活動が、本書の「Security By Design」です。

改めて、本書の「Security By Design」活動と西日本支部のこれまでの活動との関係を、図8に示します。

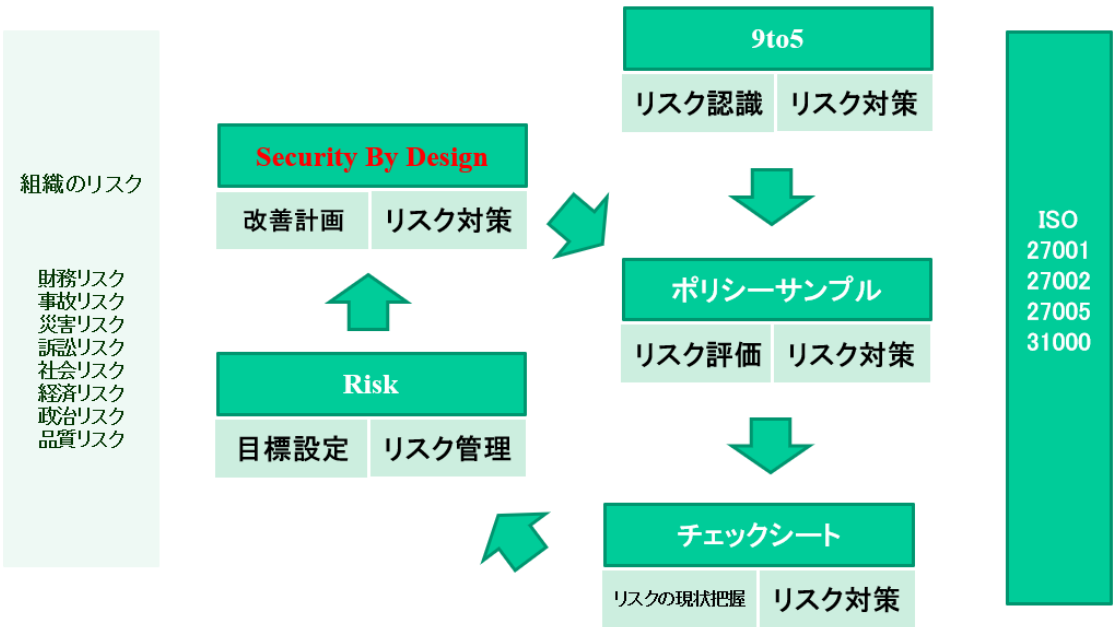


図8　本活動とこれまでの活動の成果物との関係

２．中小企業の Security By Design

前項で、西日本支部の活動の振り返りを行いました。とくに「Risk　WG」について重点的に振り返りを行いました。「Risk WG」は、経営者に IT システムへの投資を承認してもらうための活動でしたが、実際に経営者に IT システムへの投資を承認してもらった後はどう進めればよいのでしょうか？

多くの中小企業は、IT システムの導入や情報セキュリティ対策を外部のベンダーに依存しています。中小企業は、企業の根幹であるビジネスへの人的資産の投資が最優先であり、IT システムの導入や情報セキュリティ対策への人的投資は、外部のベンダーに依存する傾向が顕著です。また、それはやむを得ないことです。

ただし、IT システム導入や情報セキュリティ対策は、自社のビジネスの強化や効率化のために行うべきものです。主体は自分たちであり、外部ベンダーへの丸投げは、大きな誤りと言えます。

自社のビジネス、人的、財務的な体力に鑑み、外部ベンダーに対し、IT システムやセキュリティ機能、またその運用についての要求仕様を提示することが必要です。（図9）

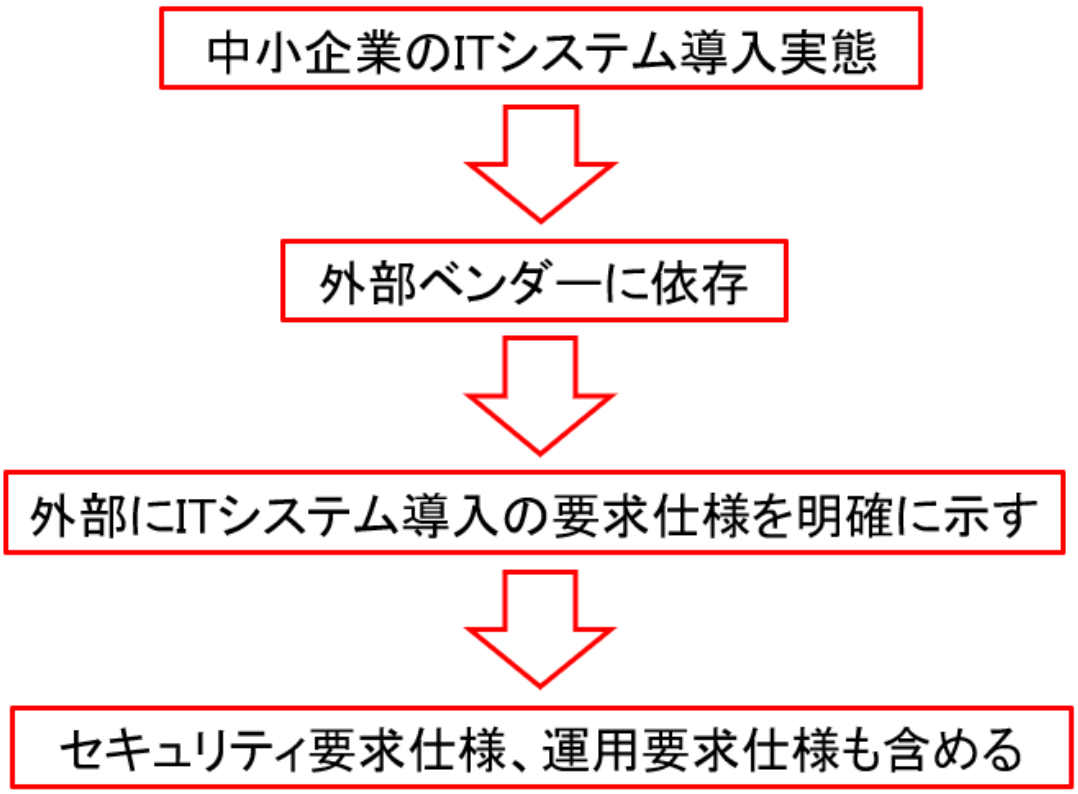


図9　中小企業の IT システム調達実態

IT システムの設計・導入前である企画段階で、セキュリティ機能及び運用の考慮漏れを防ぐために、現状のシステム機能、現状のシステムでは解決できない機能・課題・あるべき姿を RFP（Request for Proposal）に取りまとめ、RFP を基に外部ベンダーより IT システムの提案を受ける必

要があります。図10に示すように、RFP には現状のセキュリティ機能・運用及び、あるべきセキュリティ機能・運用も含める必要があります。特に、IT システム導入後、外部に運用を依頼する場合は、責任範囲を明確にする必要があります。

図10 「中小企業の Security By Design」は RFP を作成するプロセス

西日本支部では、「中小企業の Security By Design」とは、**「IT システムの企画段階において、自社の経営を踏まえた IT システムの要求仕様、求めるセキュリティ機能とその運用要求仕様を取りまとめ、RFP を作成するためのプロセス」**と定義しました。

なお、「自社の経営を踏まえた」IT システムの要求仕様、求めるセキュリティ機能とその運用要求仕様を考える上で、経営者と外部ベンダーとの橋渡しとなるコミュンケーションが必要となります。

西日本支部が考える「中小企業の Security By Design」は、図11に示す経営者と外部ベンダーとの橋渡しとなるコミュニケーションツールになります。

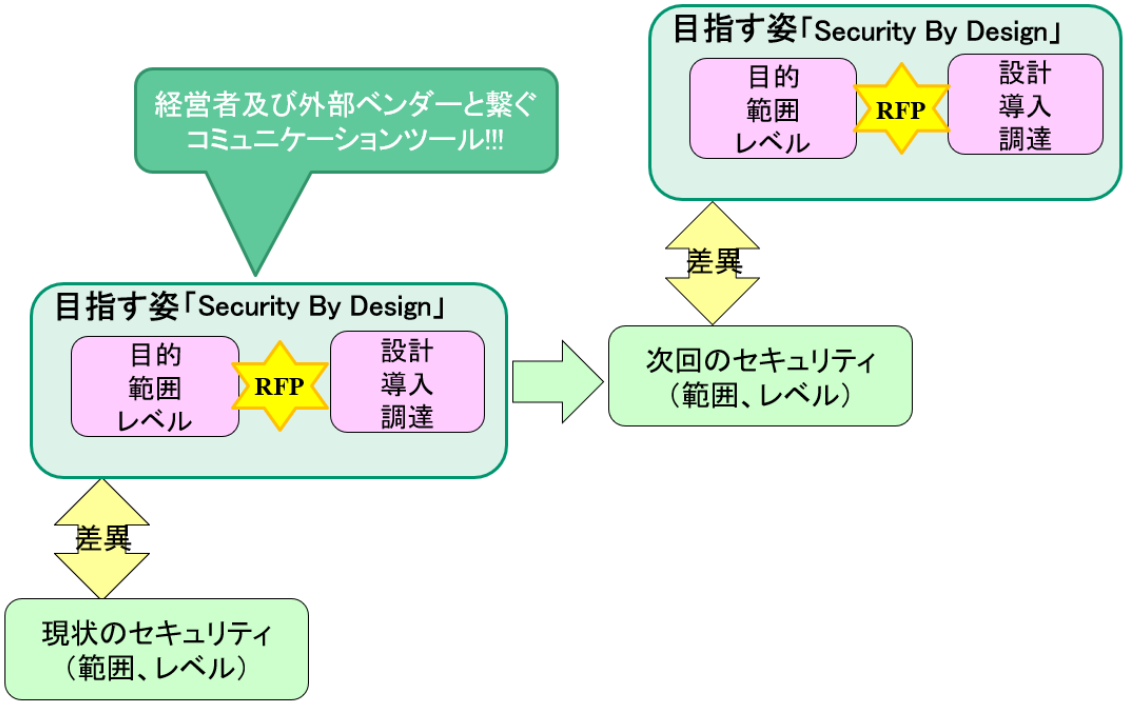


図11 経営者と外部ベンダーとの橋渡しとなる中小企業の Security By Design

３．RFP 作成で立ちはだかる壁

IT システムの設計・導入のために、企画段階で RFP を作成するにあたり、以下のようなことを実施します。

【企画段階で RFP 作成に向けて実施すること】

- ビジネス要件の把握
- 現状システムにおける脆弱性の把握
- 脅威を踏まえた改善に必要な技術の洗い出し
- 対策（管理策）の選択
- 対策の維持、運用内容の明確化（管理策の効果測定を含む）

しかし、現状の経営管理、システム管理（運用）、セキュリティ管理とは独立して RFP を作成すると、以下のような様々な壁が立ちはだかることになります。

【RFP 作成で立ちはだかる壁】

① 時間の壁

RFP 作成時に脅威、脆弱性の網羅性を求め、リスク分析、対策の検討に多くの時間を費やす可能性があります。

② 予算の壁

網羅的にセキュリティ対策を行っていくと、経営者に承認してもらった IT システム投資の予算を超過することがあります。

③ 運用の壁

情報セキュリティ対策を強化することにより、その運用も増加するため、その運用の稼働時間、費用の確保や運用のための技術の習得などの負荷が増大します。

構築後、スムーズに運用を移行するには、運用が可能な体制、技術の構築が必要であり、そのため、RFP 作成時に運用項目、運用に必要な体制、技術を明確化する必要があります。

④ 効果測定の壁

承認されて導入した情報セキュリティ対策が、期待通りの効果を発揮していることを、経営者に報告することが必要です。

しかし、効果を報告するには、導入する情報セキュリティ対策の効果を測定する指標が必要となります。そのため、情報セキュリティ対策の機能と併せて、効果測定機能も RFP で要求する必要があります。

RFP に効果測定機能を明確化しなければ、運用後にその機能がないことから、効果測定に大きな支障をきたし、経営者に導入した情報セキュリティ対策の効果を報告することができません。

⑤　経営者と情報システム部門のコミュニケーションの壁

経営者は、基本的に IT にも情報セキュリティにも興味がありません。あるのは、IT を利活用して売り上げ、利益目標を達成するための、経営課題の解決です。

そのため、RFP 作成時に経営者と情報システム部門間で何を、情報セキュリティ対策の効果とするかの取り決めがないと、経営者と情報システム部門間で、認識に差異が生じ、上述した予算の壁、運用の壁、効果測定の壁に影響を及ぼすことになります。

そこで、西日本支部としては、「①時間の壁、③運用の壁、④効果測定の壁」、「②予算の壁」に対して、RFP の作成を RFP 単独で考えるのでは無く、図12に示すように、PDCA プロセスの一部として考慮した RFP の作成が有効と考えました。

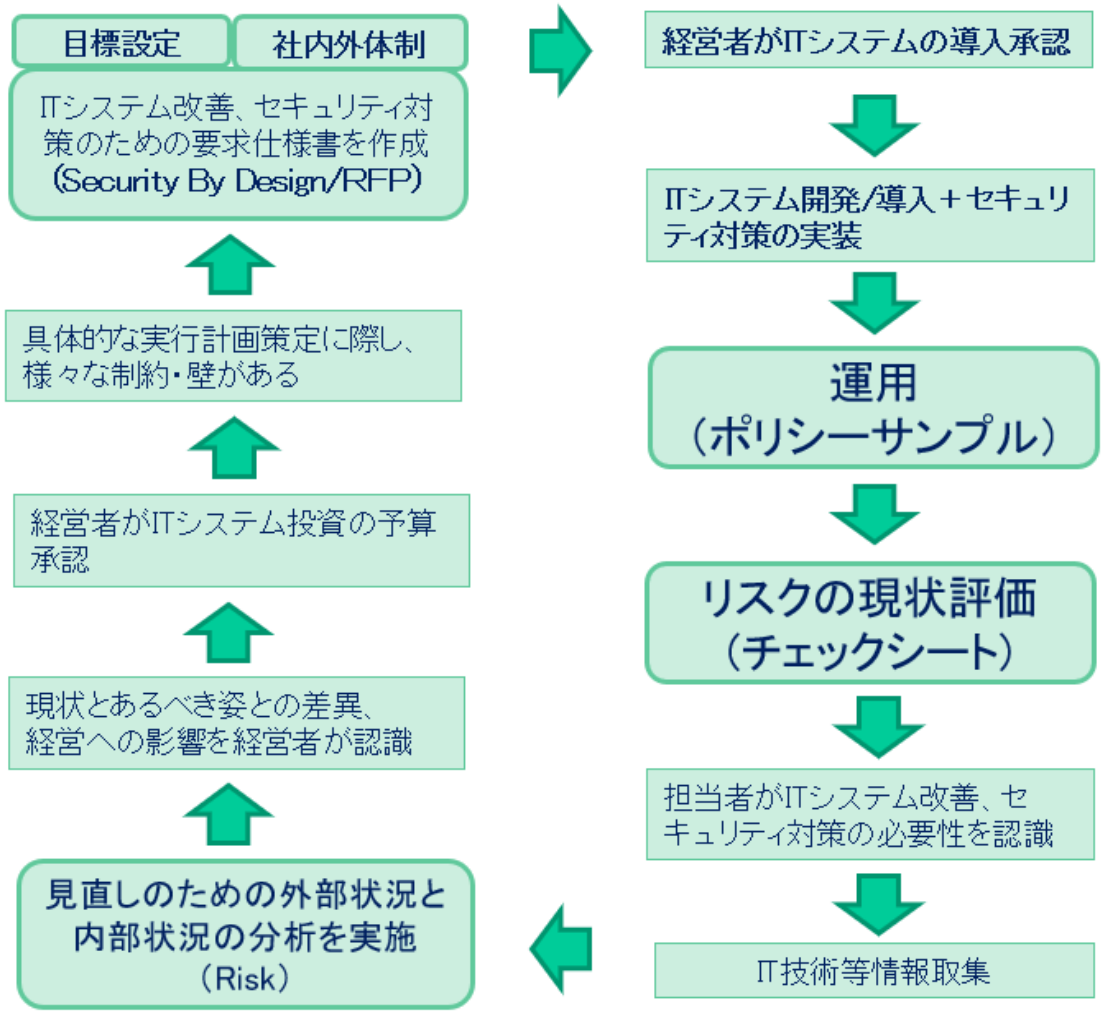


図12　PDCA プロセスの中の「Security By Design」の位置付け

それでは、RFP 作成を PDCA のプロセスの一部として考えた場合、RFP を作成するための「Security By Design」はどのようなプロセスになるのでしょうか？

まずは、現状運用されている IT システムを評価することから始まります。チェックシート等で現状の IT システムを評価して、その結果、運用変更だけでは、十分なセキュリティ対応が難しいと担当者が考えた場合は、根本的に IT システムを見直すことになります。

見直しを契機にして、組織を取り巻く外部状況と内部状況の両面から組織の状況の確定を行い、自組織が目指すべきビジネスとセキュリティ対策と現状とのギャップを明示します。

そして、目指すべきビジネスの方向性において、IT システムを見直すことが、経営課題の解決になると経営者に承認された場合、次のプロセス「Security By Design」に進むことになります。

「Security By Design」プロセスでは、リスクの現状評価結果及び、目指すべきビジネスとセキュリティ対策と現状とのギャップを「Security By Design」への入力とします。ビジネス要件は機能要件として、またセキュリティ要件は非機能要件として、改善すべき IT システムの要件として「RFP」に取りまとめることになります。この「RFP」を反映して導入された IT システムには、改善されたビジネス機能とセキュリティ機能が実装され、それぞれの運用結果が出力されます。「Security By Design」への入力と出力の関係を図13にまとめておきます。

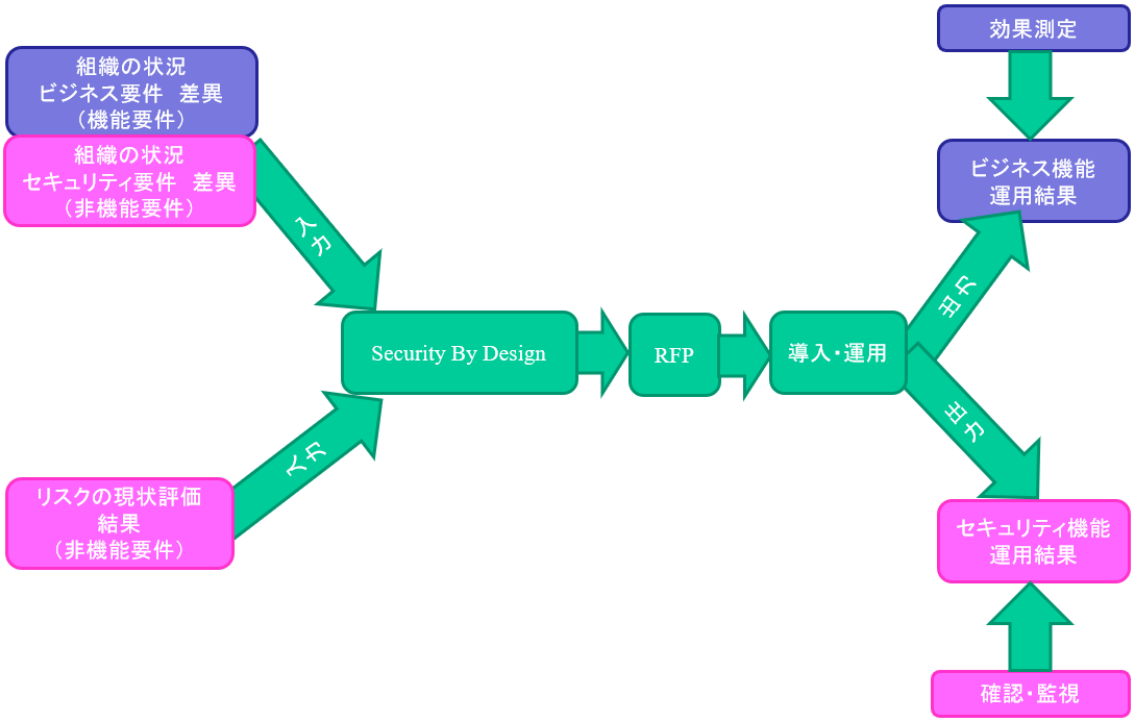


図13 「Security By Design」への入力と出力

【① 時間の壁、③運用の壁、④効果測定の壁への対処】

- 現状運用をベースにしたチェックシート等の評価結果及び、組織の状況の確定から明示されたあるべきビジネスとセキュリティと現状運用とのギャップを「Security By Design」の入力とすることにより、ビジネス上の脅威と脆弱性の把握を効率的に行います。

- 但し、脅威や攻撃を完全に把握することは不可能であり、全てを防御できないため、事故発生を前提に考えることが必要です。特に、現状想定していない脅威や攻撃に対応することはできません。
- 事故発生を前提とすることから、組織の状況の確定時に、情報セキュリティ事故の早期発見を可能とする機能と運用、体制の確立を目指し、あるべき運用と体制を明確化します。
- 「Security By Design」に入力する機能要件と非機能要件から、それぞれの機能の評価項目を定め、評価指標の測定機能と運用、体制を RFP 作成時に明確化します。

【②予算の壁への対処】

- チェックシート等の評価結果及び組織の状況の確定で把握したリスクのなかで、受容可能なものがないか選別を行います。また西日本支部の成果物「情報セキュリティチェックシート」では、現状のセキュリティレベルを 4 段階で評価していますが、このように現状のリスク評価をレベルで評価し、レベルの低い項目から優先順位付けして対応します。

なお「③運用の壁、④効果測定の壁」については、運用という共通的な要素があります。次項において、この情報セキュリティの運用の重要性について整理します。

３．１．RFP 作成時に運用機能を考える重要性

RFP作成時に情報セキュリティ対策の機能のみならず、情報セキュリティ対策の運用を支える機能を検討する重要性は、以下の理由によるものです。

- 脅威や攻撃の全てを防止できないため、事故発生を前提とすると、情報セキュリティ事故の早期発見が必要となり、早期発見のための機能の実装とそれを監視、分析する運用が必要となります。
- 中小企業で、技術力のある専任メンバーを割り当て、運用を実施するのは現実的ではなく非効率となるため、現実的かつ効率的な監視、分析を行うシステム機能の実装や、サービスの利用が必要となります。
- IT システムの開発、運用や情報セキュリティ対策の構築、運用のクラウド活用も含め、外部委託している中小企業においては、日常の運用を円滑に進めるために、自組織、委託先のそれぞれの責任と役割を明確化し、委託先とのコミュニケーションを確保する必要があります。

３．２．Ｖ字モデルと OODA との関係を再確認

前項で、RFP 作成時に情報セキュリティ対策の運用を考える重要性について整理しました。

これは「図2 Ｖ字モデルにおける「Security By Design」の位置付け」からも、明らかです。

マネージメント、コントロールに対する運用に、それぞれ監査、運用確認・監視が対応して存在

します。この部分は PDCA サイクルの実行、チェック、見直しが該当します。さらに「D」は「OODA」というループを内包します。

この「OODA ループ」は、V字モデルにおける運用確認・監視の一部であり、この運用確認・監視を円滑に行うためには、コントロールの実装において、その OODA を可能とする運用機能を実装していることが前提となります。

RFP にその運用と必要な機能の要求がなければ、必要な運用機能を具備しない情報セキュリティ対策のシステムを導入することになり、運用に支障をきたし、効果測定が行えないことになります。

図14に V 字モデル、OODA から運用の早期検討が必要となる関係を示します。

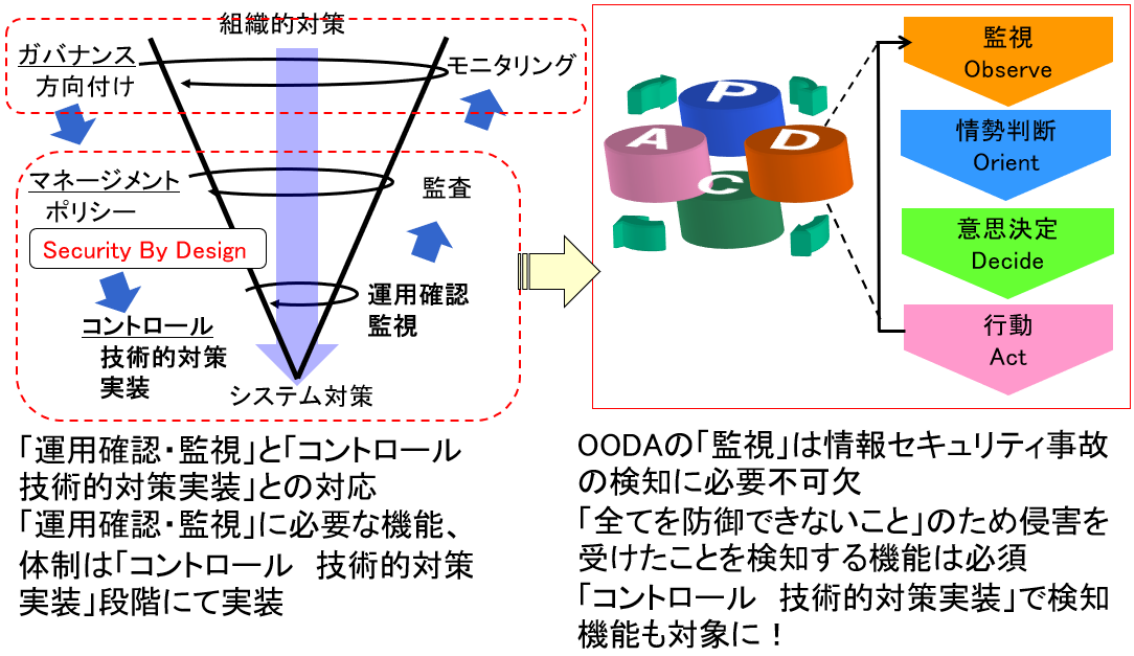


図14 V 字モデル、PDCA と OODA の関係

４．経営者の役割を考える

４．１．経営者と情報システム部門のコミュニケーションの壁

本項では、3項に記載した5つの「RFP 作成で立ちはだかる壁」のうち、「経営者と情報システム部門のコミュニケーションの壁」について、改めて整理します。

「図2の V 字モデルにおける「Security By Design」の位置付け」における経営者の役割は、IT ガバナンスとモニタリングの部分が該当します。図 15に対応部を示します。

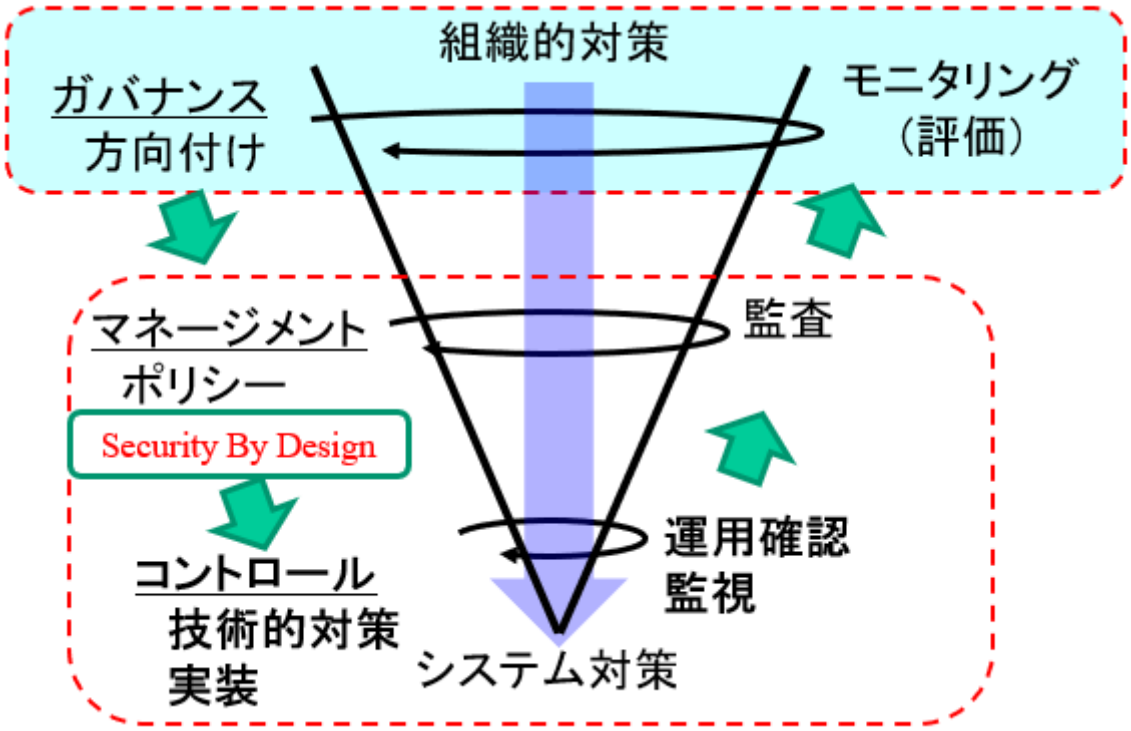


図15 V 字モデルにおける経営者の役割

営業担当は営業のことだけを考え、製造部門は製造のことだけを考える傾向があり、それでは部分最適となってしまいます。部分最適を推し進めると、組織全体では矛盾が生じ、立ち行かなくなります。

そのため、組織全体での最適化を目指す必要があり、それを可能とするのが経営者であり、経営者の責任です。経営者は「次々刻々と変化する経営環境への対応、企業競争力の維持・強化」を全体最適で推進する役割が求められます。

Security By Design においても同様に、全体最適が必要であり、それは経営者の責任です。以下に Security By Design における経営者の役割を示します。

【Security By Design における経営者の役割】

- 組織全体の最適化のために、組織のトップとしての意思表示や、取りまとめを行い、リーダーシップを発揮する必要があります。
- 経営課題や経営ビジョンの視点から、IT システムが抱える様々な課題解決に向けた意思決定を行うことが必要です。
- IT システムが、課題解決を達成するために求める情報セキュリティ対策への意思決定を行うことが必要です。
- 体制の構築、経営資源（ヒト、モノ、カネ、情報）の配分は、経営者にしかできません。最適な配分の決定を行うことが必要です。

これらの役割を経営者が担うにあたり、経営者が理解すべきことは、情報セキュリティ対策に終わりはなく、またどれだけ情報セキュリティ対策に取り組んでも、全てを防御できるわけではない、ということです。

3項に事故発生を前提とした Security By Design が必要であることを記載しましたが、事故前提の Security By Design において、経営者が行うべきことを以下に示します。

【事故前提における Security By Design において経営者が行うべきこと】

- 経営の視点から、受容可能なリスクか否かの判断基準は、経営者が示します。
- PDCA サイクル以外に、監視、その対応を行う OODA ループを確立するためのセキュリティ体制を構築します。
- セキュリティ体制に必要な人員は、委託先を含めて確保します。
- 経営者にしかできない意思決定を行います。そのため、セキュリティ推進活動に、経営者は積極的に関与します。
- これらを行うには、経営者自身が、情報セキュリティ推進メンバーとのコミュニケーションを積極的に行なわなければなりません。

４．２．情報セキュリティ対策の評価

図15にガバナンスの方向付けとモニタリングを、組織的対策として表示しました。

ガバナンスでは、経営者が経営課題、経営ビジョンに基づき、IT システムの導入、情報セキュリティ対策の方向付けを行います。モニタリングは方向付けとの対の関係となるため、方向付けに基づき、マネージメント、コントロールを行った結果を集め、その評価を行い、フィードバックすることが求められます。

西日本支部が考えた 1.1 項の「Risk　WG」における経営視点での「あるべき姿」が方向付けとなり、モニタリングは、経営者が承認した情報システムと、情報セキュリティ対策に投資した結果の確認と、その評価が対応することになります。

この評価には情報システム投資の評価が重要となります。情報システム投資の評価ができないと、情報セキュリティ対策のビジネスへの効果の把握ができません。そのため、情報セキュリティ対策の評価と同様に、情報システム投資の評価は重要です。

その評価方法について、本項で整理します。評価を行うには評価指標が必要なことから、表1に一般的な評価指標を示します。

	名称	説明
KGI	「重要目標達成指標」 Key Goal Indicator	目標達成の達成度合いを評価するための指標。 例）経営利益○○％達成
KPI	「重要業績評価指標」 Key Performance Indicator	最終目標を達成するために、必要なプロセスを評価する定量的な指標。 例）製品歩留まり○％向上、販売管理費○％削減

表1　一般的な評価指標

具体的な例がある方が判りやすいため、図16に示す「Risk　WG」で作成した「経営者向け情報セキュリティ対策実践手引き」の製造業における情報セキュリティ対策を例に考えます。

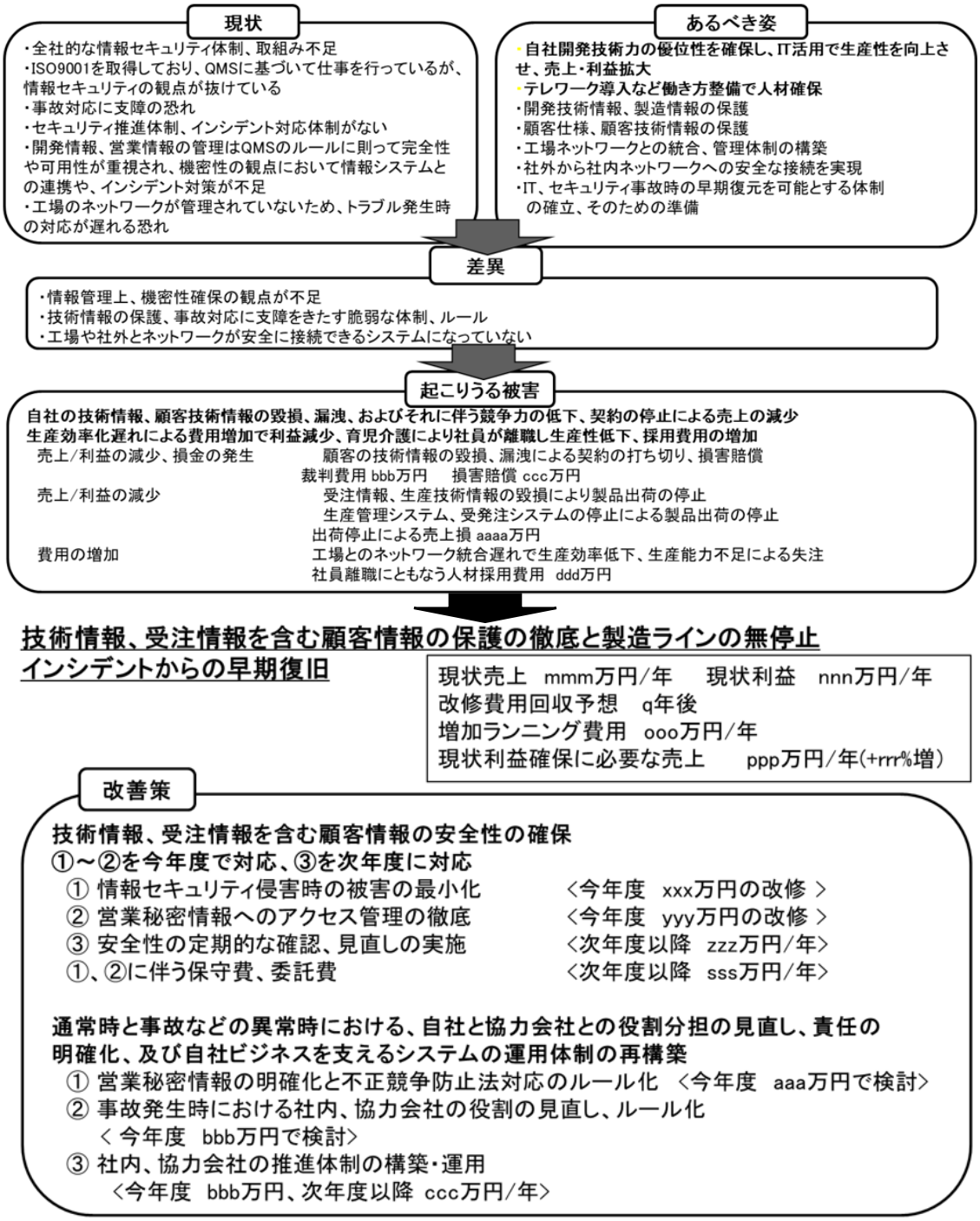


図 16「Risk WG」 製造業の情報セキュリティ対策の導入例

本例を、経営者向けの評価に引用するため、評価指標に KGI を採用した場合にどうなるか検討します。

経営者にとって、あるべき姿とKGIの関係は、以下の通りです。

【経営者にとってあるべき姿】

- 自社開発技術力の優位性を確保し、IT 活用で生産性を向上させ、売上、利益を拡大する。
- テレワーク導入などの働き方改革を進め、人材を確保する。

【KGI】

- 自社開発技術力の優位性の確保、売上げ 10% up
- IT 活用、生産性 20% up （効率化によるコスト20% down）
- 優位性確保、IT 活用により利益 20% up
- テレワーク活用による人材確保、離職率 10% down

KGI に紐づく KPI は、図13で示したビジネス機能の運用結果を評価する指標になります。

それでは、情報セキュリティを評価するための指標はどうなるでしょうか。「経営者視線での KGI、KPI、リスクとその実行する Task の関係」を図17に整理します。

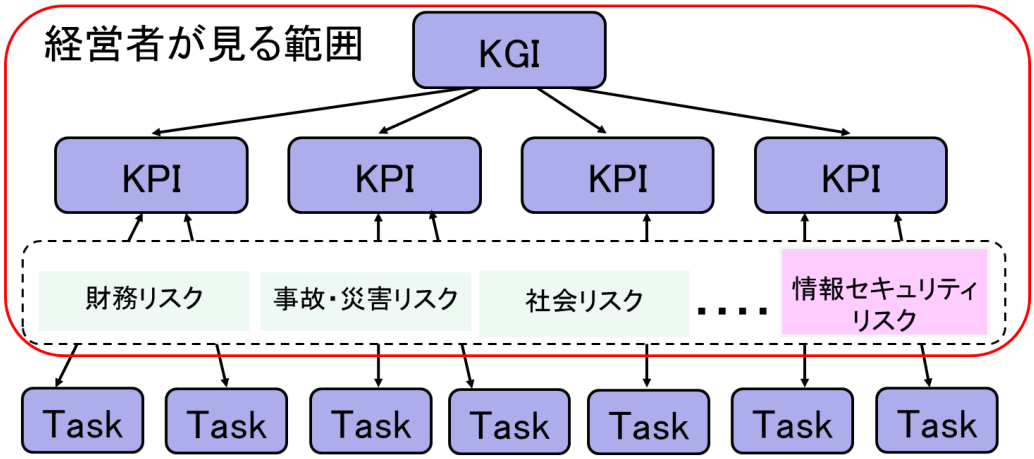


図17 経営者視線での KGI、KPI、リスクとその実行する Task の関係

経営者にとっての情報セキュリティの評価は、把握したリスクに対するコントロールの対応状況とその結果であり、経営者にしかできない阻害要因の改善のための契機が、V字モデルのモニタリングとなります。

経営者が、情報セキュリティリスクに積極的に対応する必要がある理由も、この図 17から理解して頂けるものと考えます。

なお、情報システム部門は、経営者へ情報セキュリティリスクに対応した結果を報告する際、その方法に注意する必要があります。

経営者にマルウェア感染をした、またはマルウェア感染から防御した、という技術的な報告を行っても、被害あるいは被害想定を具体的に報告しなければ、経営リスクとして、経営者の心に

届きません。

そのため、図 18に示す「業務影響ベースでの情報セキュリティリスク」を考慮し、図19に示すリスク対応として捉えた情報セキュリティの目的と、そのリスク対応への評価指標を示す必要があります。

経営者の情報セキュリティリスクの見方

ITへの影響ではなく、業務インパクト

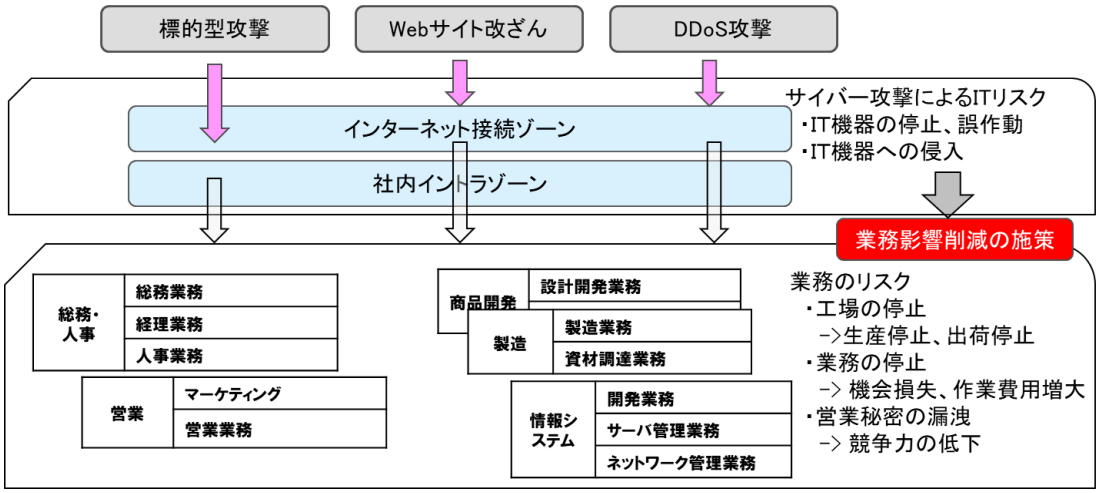


図 18　業務影響ベースでの情報セキュリティリスク

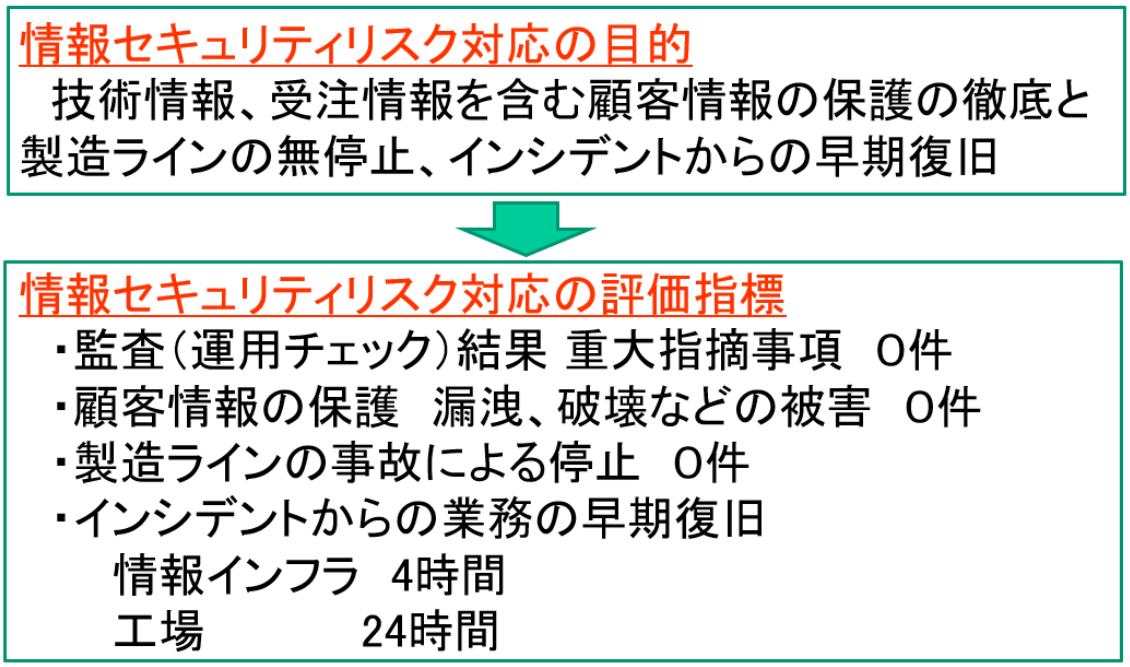


図19　情報セキュリティをリスク対応として評価

3項の図13と図17の関係を図20にまとめます。この図のセキュリティ機能運用結果を評価するための IT 戦略の KPI-1～KPI-N が、図19の情報セキュリティリスク対応の評価指標です。監査（運用チェック）は、組織の状況の確定から導かれる、情報セキュリティのあるべき姿を基に実施される必要があります。

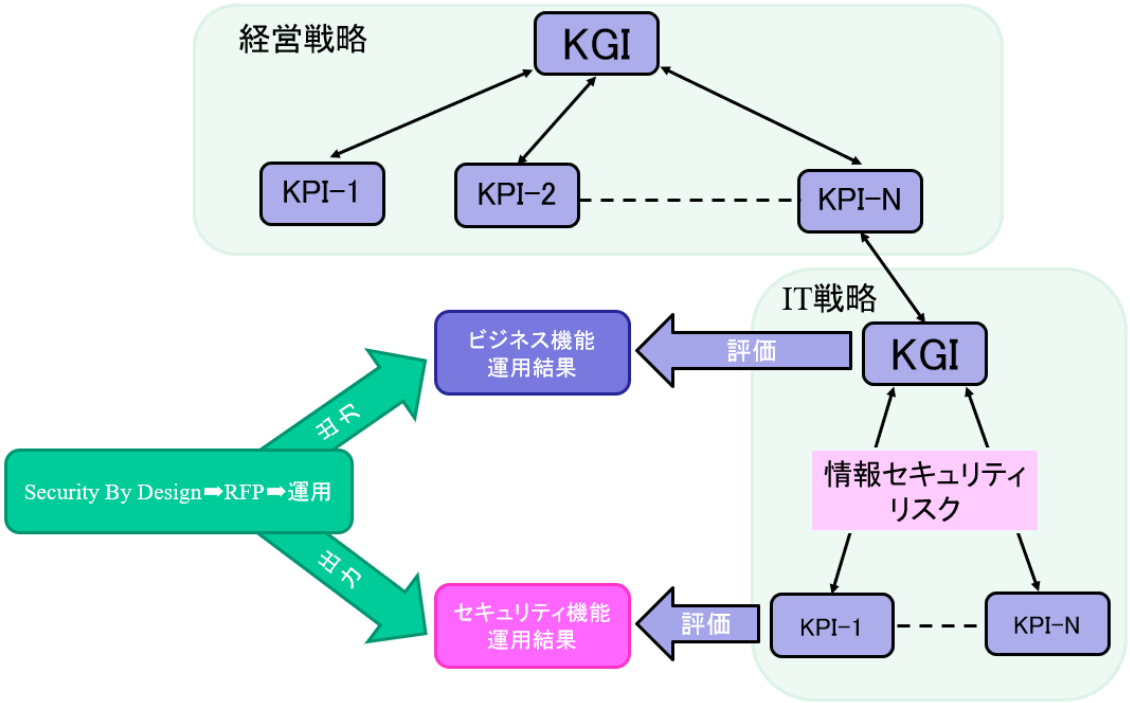


図20 KGI、KPI と情報セキュリティリスク対応の評価指標の関係

最後に情報セキュリティリスクが経営リスクの一部であることを、経営者は再認識する必要があります。

様々な経営リスクが存在しますが、そのリスクは、単独で存在するのではなく、あるリスクが発生すると他のリスクにも影響を及ぼします。情報セキュリティリスクも同様であり、図21に示すように、他のリスクにも影響を及ぼします。

情報セキュリティは IT 部門に任せる傾向が強いのですが、経営者が深く関与する必要があることが、この図からも明らかだと考えます。

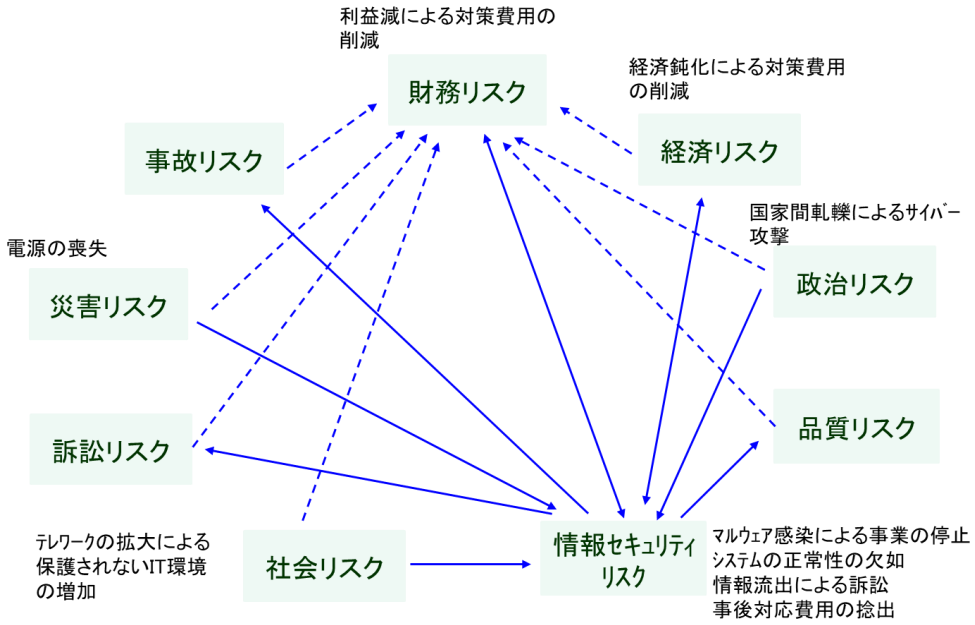


図21 リスクの共鳴

５．まとめ

本書の目的は、経営者からITシステム投資の承認を得た後、中小企業の情報システム部門が考えるべきITシステムの導入、運用、廃止までのライフサイクルを考慮した情報セキュリティの姿を検討することでした。

一般的に、ITシステムの開発・導入においては、後工程になるほど修正が困難な傾向にあります。従って、ITシステムの企画・設計段階から、情報セキュリティを考慮した設計(Security by Design)が重要となります。

これまで西日本支部では、情報セキュリティ対策における運用、評価、組織の状況の確定から、あるべき情報セキュリティの姿を導く、様々な活動をしてきました。

そこで、「Security By Design」においても、設計プロセス単独で考えるのではなく、ITシステムと情報セキュリティのライフサイクル（設計・導入・運用・更新・廃棄サイクルとPDCAを内包したV字モデル）を考慮し、組織の状況の確定より導かれるビジネスと情報セキュリティのあるべき姿を基に、システム設計を行うことが必要です。

また、ビジネスのあるべき姿から、ITシステムの評価指標を導き、この指標と情報セキュリティの評価指標を結びつけることにより、ITシステムの評価を通して、間接的にビジネス目標と情報セキュリティを結びつけることを提示しました。

経営を考えなければいけない経営者と、ITシステムの導入を検討するシステム管理者である技術者は、用いる用語が異なるため、意思疎通が簡単ではありません。しかし、ITシステムの企画段階から、運用時の情報セキュリティ評価を考慮することで、ビジネス目標と情報セキュリティ評価を結び付けることができ、ビジネスという共通の用語で、経営者と情報セキュリティの重要性

を認識しているシステム管理者の意思疎通が図れます。

情報セキュリティの評価ができなければ、図22に示すように、有効なモニタリングもできず、情報セキュリティ活動の繋がりが切れてしまいます。

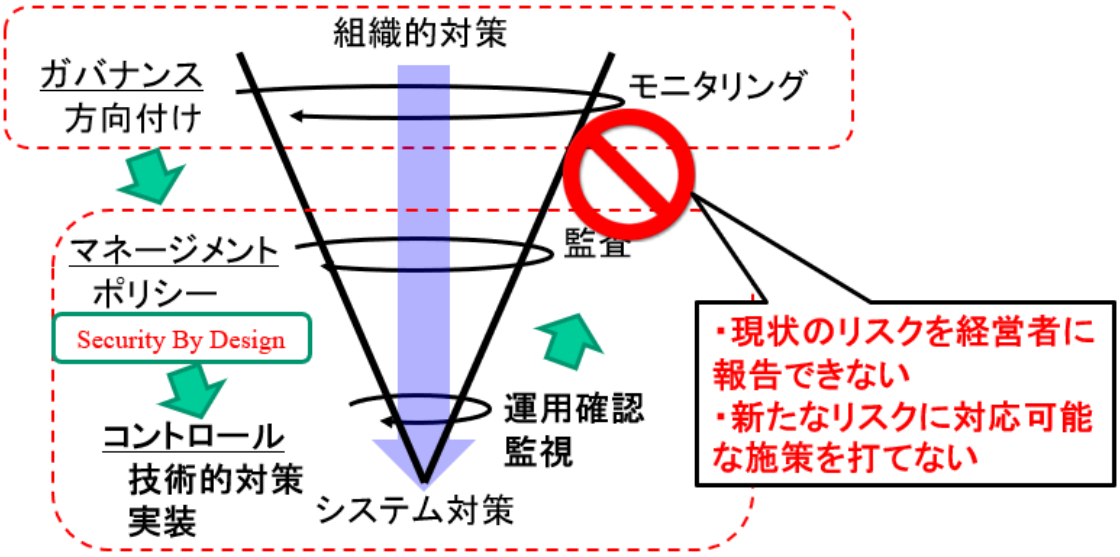


図22　経営者とのマネージメントの分断

IT システムの設計段階では、情報セキュリティへの考慮だけではなく、ビジネス目標に紐付く情報セキュリティの評価指標も併せて検討することにより、この切断を防止し、情報セキュリティ対策を継続して行う必要があります。

最後に、本書では、設計時に必要となる情報セキュリティの具体的なコントロールを提示することができませんでした。以下に、業界ごとに参考になるセキュリティ規格を紹介することで、本書の締めくくりにします。

① 全般
- ISO27001　付属書 A
- ISO27002
- NIST　SP800 シリーズ

② EC サイト他カード業界
- PCIDSS

③ 製造
- IEC62443 シリーズ

④ 医療
- 厚生労働省　医療情報システムの安全管理に関するガイドライン

以上

「中小企業のための Security by Design WG」メンバー

井上 陽一　（JNSA 顧問、日本エレクトロセンサリデバイス株式会社）
金子 啓子　（JNSA 顧問、大阪経済大学　経営学部准教授）
大室 光正　（株式会社インターネットイニシアティブ）
河野　愛　（株式会社インターネットイニシアティブ）
小柴 宏記　（ジーブレイン株式会社）
元持 哲郎　（アイネット・システムズ株式会社）
吉崎 大輔　（日本電気株式会社）
米澤 美奈　（株式会社ソリトンシステムズ）

嶋倉 文裕　（サブスクライバ）

WG にご協力を頂いた皆様

青木　茂
今井　実
大財　健治
塩田　廣美
西川　和予