

情報漏えい防止と活用に関する 情報システム部門の役割について

- 二兎を追う者は二兎を得る！
利活用と漏えい防止の両立術 -

アブストラクト

1. 研究の背景

今日、企業における経営資源は「人、物、金、情報」とされている。企業は保有している情報を利活用し、新たな商品・サービス・価値を創出することで業績を向上できる可能性を持っている。一方で、企業が情報を利活用するには情報漏えいのリスクが常につきまとう。情報漏えいが事業経営に与える影響は大きく、情報システム部門はリスクを恐れるあまり過度なセキュリティ対策を講じ、ユーザ部門の情報利活用を妨げている事象が発生している。経営資源の1要素とされる情報を利活用できないことは企業において情報漏えいと同等の損失であり、情報利活用とセキュリティ対策が両輪となった取り組みが求められる。本分科会では「情報利活用」と「セキュリティ対策」を両立できる技術・手法を探索し、安全で有益な情報利活用を促進するために情報システム部門がなすべきことを検討した。

2. 問題提起と課題設定

本分科会メンバー各社で、過度なセキュリティ対策によって情報の利活用が妨げられている事例を持ち寄り調査したところ、以下の問題点が挙げられた。

問題点1：情報システム部門が情報を守るだけのセキュリティ対策しかできていないこと。匿名化などの新技術による情報加工や運用次第で情報利活用とセキュリティ対策を両立できるパターンがあるにも関わらず、一律にセキュリティ対策を強化していること

問題点2：情報システム部門が日々変化する情報利活用ニーズとセキュリティリスクを把握しきれていないこと。ユーザ部門は業務のため情報利活用を優先し、ルールを無視した抜け道を作り情報システム部門が把握しないセキュリティリスクを発生させていること

上記問題点の原因を分析し、次の3点を解決すべき課題とした。

課題1：「セキュリティを担保した上で不自由ない有益な情報利活用を実現すること」が必要である。

課題2：「定期的に継続的にユーザ部門の情報利活用ニーズと利活用における不満点を吸い上げること」が必要である。

課題3：情報システム部門がユーザ部門から情報利活用ニーズとセキュリティ対策の実態を限られた時間で有効にヒアリングすることは難易度が高い。「情報利活用とセキュリティ対策に関する有効なヒアリング設問が明確になっていること」が必要である。

3. 研究内容および成果

課題を踏まえ、システム開発・運用のPDCAサイクルの「Plan(計画)」と「Check(評価)」の段階で利用できるツールを成果物として作成した。このツールは情報利活用とセキュリティ対策の両立において効果的な「Do(実行)」と「Act(改善)」を実現できる内容としている。ツールを用いてPDCAサイクルを回すことで問題を解決できると仮説を立てた。

・『情報利活用促進ツール：情報利活用パターンを考慮したセキュリティ対策リスト』

情報利活用パターン毎に利活用を考慮した適切なセキュリティ対策を選択できるツールである。情報システム部門は自社の要件に合うセキュリティ対策を選択することができ、有効なDo(実行)を実現できる。ツールの特徴として、(1) 情報利活用観点でのセキュリティ対策評価、(2) 分科会メンバー各社の有効な情報利活用ノウハウを追加、(3) IPA 公開情報と照合しリスク別にセキュリティ対策を網羅、

(4) セキュリティ対策の導入・運用コストを明示、(5) 継続的に取り組むべき運用内容を明示の5つが挙げられる。

・『情報利活用促進ツール : ユーザニーズ・不満収集シート』

ユーザ部門の情報利活用ニーズや利活用における不満を漏れなく収集するためのツールである。このツールを利用してシステム開発・運用 PDCA サイクルの Check(評価)を行うことで、(1) ユーザの声として挙がる情報利活用ニーズ、(2) ユーザ自身が認識に至っていない情報利活用ニーズ、(3) 情報利活用を優先して発生するセキュリティリスクの3つを収集・発見できる。収集結果を踏まえて、情報利活用促進ツール を用いることで、より有効な Act (改善) を実現できる。これらのツールを用いてシステム開発・運用の PDCA サイクルを回すことにより、システムを利用してから当初予定と異なることで発生する、あるいは更なるレベルアップへの要望で挙がってくるユーザ部門の声を「定期的かつ継続的」に吸い上げる仕組みが構築され、担当者のレベルに依存しないニーズ収集とセキュリティを担保した情報利活用促進ができると考えた。

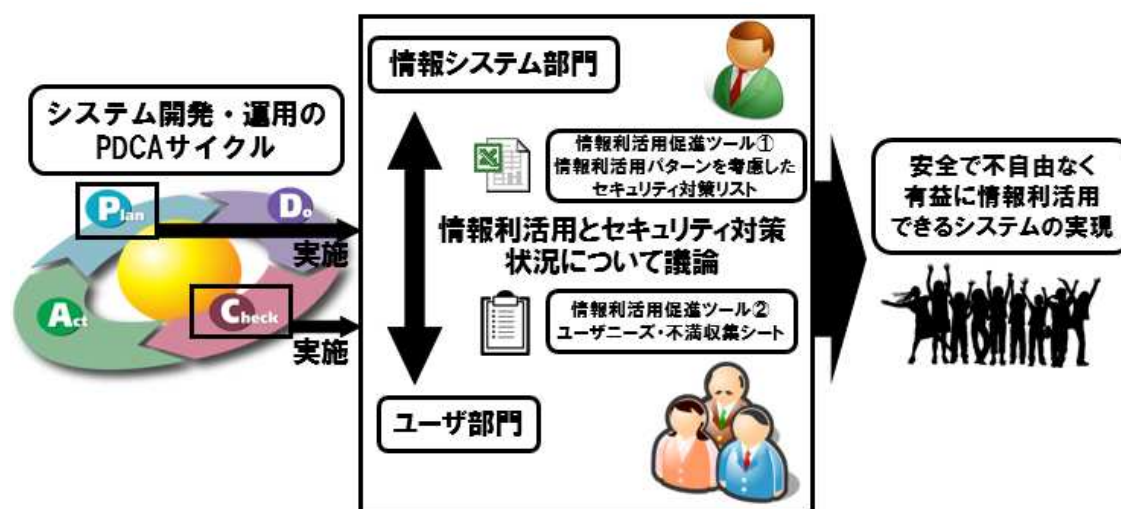


図1 成果物を用いた解決策のイメージ

4. 検証

ツールの「信頼性の検証」では、設問事項に組織で必要となるセキュリティ対策が網羅されていること、対策内容がリスクに対し適切に作用することを確認した。「組織における内部不正防止ガイドライン(IPA)」をはじめとした各種ガイドラインのセキュリティ対策と突合せを行い、情報システム部門が担うべき対策が十分に織り込まれており、且つリスク対策として適切であることを確認した。

ツールの「有効性の検証」では、40名(本分科会各社の情報システム部門とユーザ部門)へのアンケートを実施し、実際に企業で活用できるツールとなっていることを確認した。情報利活用促進ツールでは90%、ツールでは70%の「活用できる」という回答を得られ、有用であると判断した。特に情報利活用の観点から作成された対策リストは、「新鮮であり対策検討の参考になる」という意見が目立つ結果となった。一方、ユーザ部門からは「上から目線の設問が多く率直な意見を吸い上げられないと感じる」という否定的な意見もあり、改善後に再確認を依頼し有効性が向上したことを確認した。

成果物検証の後、2015年に発生したN機構の情報漏えい事故にツールを適用してPlan(計画)、Check(評価)を行い、情報漏えい事故未然防止と情報利活用の両立実現を確認することで解決策の仮説検証を行った。

5. 評価・提言

情報利活用とセキュリティ対策は相反するものとして本分科会メンバー各社では利活用を諦めている事案もあった。しかし、本研究を通して、ユーザの利活用ニーズを深く分析した上で情報利活用を促進すると、セキュリティ対策も両立可能な事案もあることを発見できた。また、情報利活用の促進が情報漏えい未然防止に繋がることは新たな知見である。セキュリティを担保し不自由ない情報利活用を提案できる本研究の成果は、経営資源の1つである情報を可能な限り最大限に活かすことで企業にとって有益な結果をもたらすことを確信する。