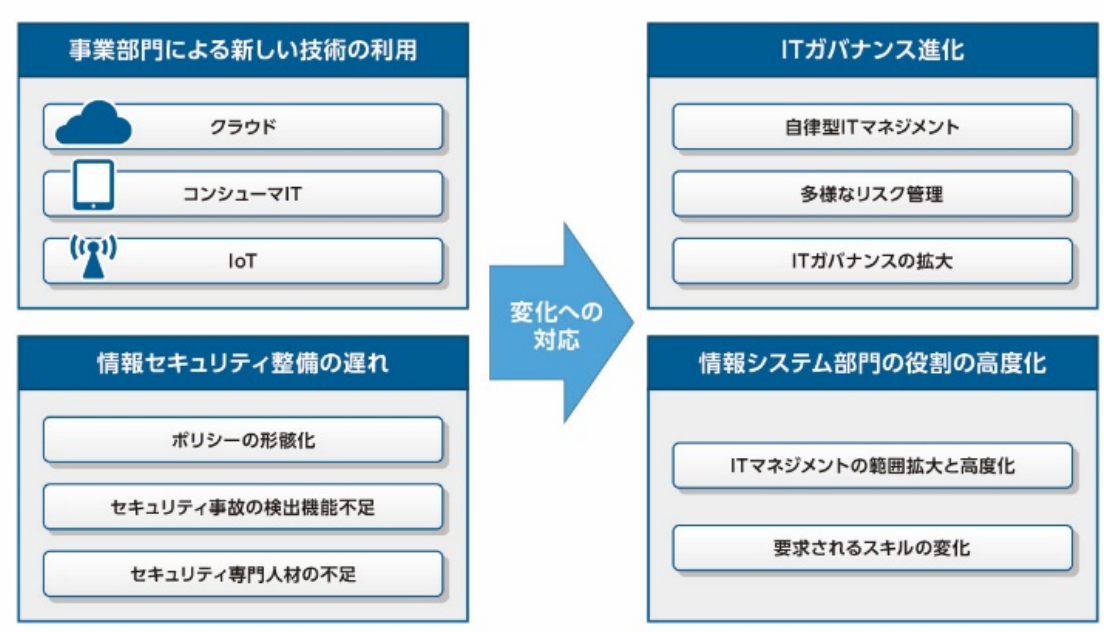
セキュリティリスクの拡大とITガバナンスの高度化

IT利用場面の拡大に対応した新たなITマネジメントの仕組みが作られていく。ITの新しい技術の浸透や巧妙化するセキュリティ攻撃に対して、ITガバナンスの重心はセキュリティガバナンスへ移っていく。高度なサイバー攻撃への対応はユーザ企業だけでは困難になり、ITベンダーやIT製品を選定する際の評価ポイントとして、セキュリティ技術の重要度が増していく。



1　背景と現在の状況

各種クラウド、コンシューマIT、オープンデータなどの新技術の活用が進んでいる。企業の事業部門による新たなサービスの提供や新事業のための仕組みとして、これらの新技術が浸透しつつある。

しかしIT活用場面の広がりや新技術の活用には新たなセキュリティ対応も必要になってきている。新技術の普及による接続デバイスの増加は著しく、モバイルデバイスや各種センサーなどの、数や種類が増えるにつれ、潜在的なサイバー脅威が増加している。また内部犯行によるセキュリティ事故の発生も後を絶たない。高度な監視や防止のしくみ作りが行われつつあるが、セキュリティへの投資効果の不透明さなどにも起因し、ポリシーの形骸化、事故の検出機能不足、専門人材の不足などの課題も抱えている。

このようなIT活用の進化と巧妙なセキュリティ攻撃は、企業の情報システム部門の役割の高度化をもたらしている。利用者に制約を課し、変化とリスクを最小化することを中心とするこれまでのITマネジメントは限界を迎えつつある。

2　3～5年後の姿

ITの利用場面は大きく拡大していく。事業部門、マーケティング部門、製造やサービスの現場、個人、多様なモノや製品自体でITが駆使されていく。この拡大に対応してITガバナンスは進化し、企業戦略との整合や新たな価値の提供に加え、セキュリティガバナンスの重要性が増していく。

これに伴いITマネジメントは新たな仕組みが作られ、情報システム部門の役割が変化していく。情報システム部門はITを活用した新サービス、新事業などに、より積極的な役割を遂行していく。またIT利用の拡大による利便性や革新性の代償として生じる多様なセキュリティの課題に対し、リスクの適切な管理を行い、巧妙化するサイバー攻撃への対策を進めていく。

2.1　ITガバナンスの進化

新たなITの採用やIT利用場面の拡大により、従来型のどちらかと言えば画一的で厳格なITマネジメントでは、経営視点でのITの高度活用を阻害したり、シャドーITを助長したりする可能性が高くなっていく。このためITガバナンスにも進化が必要となっていく。ITの高度活用や新技術の採用を迅速に行うためには、従来のどちらかと言えば情報システム部門にすべて集中するマネジメントでは困難になってくる。情報システム部門は主にIT利用の方針を作成して、事業部門などで新たにSaaSやコンシューマITの採用、導入、運用などを主体的に行っていくことでIT活用を迅速に行う、自律型ITマネジメントの仕組みに変化していく。

またスマートフォンなどのコンシューマ機器の活用やセンサーなどの接続デバイスの多種化と数の急激な増大は、運用やセキュリティの課題を飛躍的に増加していく。このような環境への対応は、リスクの最小化を目指すだけのITマネジメントでは限界が出てくる。セキュリティリスクのレベルに応じて、ネットワーク、ハードウェア、ソフトウェアなどのIT環境、ITの設置場所や利用場所、および利用する人や運用する人などを統制することで、享受する利便性や革新性に見合ったリスクを受け入れる、多様なリスク管理を行うITマネジメントが行われていく。

このようなITの新しい技術の浸透やセキュリティ攻撃の高度化に対応するためITガバナンスの範囲は拡大していく。よりセキュリティガバナンスに重心が移っていくとともに、オープンデータやビッグデータなどの活用が進むとデータガバナンスの領域へ広がっていく。また、グローバル事業でIT活用を進める企業では、セキュリティ面での一貫性、現地とのIT機能分担などの重要性がさらに増し、グローバルガバナンスの領域にも広がっていく。

2.2　情報システム部門の役割の高度化

ITの利活用を大きく拡大し始めている企業では、情報システム部門の役割が急速に高度化していく。基幹業務システムの運用を行うことが主業務であった時代は徐々に終わりを告げる。従来の情報システム部門が管理してきたシステムの範囲を超え、ITマネジメントのやり方を転換する必要に迫られていく。このような拡大された管理範囲では新たにITを活用した新サービス、新事業などを迅速に立ち上げ成功に導くため、高い先見性のあるシステム基盤の開発や先進技術などをマネジメントする、より高度な役割が中心となっていく。またこれに伴う巧妙なセキュリティ攻撃や情報漏洩の危険に対応する中心的役割を担っていく。

このようなITマネジメントの高度化は、情報システム部門に要求されるスキルにも変化をもたらす。これまでの情報システム部門のスキルに加え、事業視点からIT活用を企画し開発ができるスキルが重要視されていく。さらに強力なセキュリティ対応スキルやグローバル戦略が重要な企業では、異なる文化、商習慣などに対応するスキルが要求される。企業にとって、このような高度なスキルを備えた情報システム部門の役割は飛躍的に重要度を増していく。

2.3　セキュリティ対策の高度化

IT利用の拡大は、セキュリティ対策にも変革を必要としていく。巧妙化するとともに執拗なサイバー攻撃への対応はユーザ企業にとって技術的、コスト的に大きな負担になっていく。このためシステム構築や運用保守を行う段階でITベンダーやIT製品を選定する際、セキュリティが重要評価ポイントの一つとなっていく。

またインターネットを活用する多くのユーザ企業では、自社でインターネットと直接インタフェースを持ってセキュリティ対策をすることはリスクが高いと感じてきている。このためインターネットとのセキュアな接続を請け負うサービスの利用が増えていく。このようなサービスでは社内ネットワークとベンダーのデータセンターを直接接続し、入口／出口での防御、監視だけでなく、社内ネットワークの監視も併せて提供され、効果的な対策として利用が増加していく。

またセキュリティ対策の高度化の観点では、オンプレミスよりクラウド上の方が、よりセキュアなシステムの構築・運用が可能である、という意見を唱えるユーザ企業が増えていく。このようなトレンドからセキュリティ対策の進んだクラウド上で、セキュリティに経験豊富なITベンダーが構築・運用するシステムの利用が増加していく。ただし全てのセキュリティ対策をアウトソーシングすることは現実には難しく、より高度なセキュリティ対策を一元的に統合管理していくための仕組みの構築とそれを運用するセキュリティ高度専門人材の確保、およびセキュリティ対策の高度な自動化が併せて浸透していく。