5E-08

情報セキュリティマネジメントの継続的改善に資するリスクアセスメント

中山幸雄† 津田和彦†
筑波大学†

１．はじめに

情報セキュリティ対策を行う場合、守るべき資産を洗い出し、その機密性、完全性、可用性から資産価値を計算し、資産に対する脆弱性と脅威を想定しリスクを算定する方式をとっていることが多い。それらを定期的に見直す場合に、資産そのものは変化しないので、結果的に、リスクがないとされることがある。情報セキュリティインシデントの発生は、リスクを十分に認識していないため、対策が脆弱になるから発生するのであり、リスクアセスメントの方法を実態に即したものにする必要があると考える。

２．リスク算定方法

情報セキュリティリスクの算定方法の流れは、一般的方法として（JIPDEC,2008 年）による方法がある。それは、資産の洗い出し、洗い出した資産の価値の算出、リスク値の算出により算定される方法である。資産の価値算出は、機密性、完全性、可用性の値、リスク値の算定は、資産価値に脅威及び脆弱性を乗じた値が用いられる（リスク値＝資産の価値×脅威×脆弱性）。組織があらかじめ定めたリスク受容値より、リスク値が高い場合、リスク受容値より値が低くなるようにリスク対策を講じる。

このリスク算定方法は、ISO/IEC27001：2005(JISQ27001：2006)にも適合する方法でもあることから、情報セキュリティマネジメントシステム（ISMS）を適用している企業はこの方法によることが多い。

３．課題

この方法は資産の洗い出しやリスク算定を初めて行う場合にはメリットが大きい。なぜなら、守るべき資産を整理できることや、リスク対策をとるかどうかの判断が明確になるからである。

一方でリスクの見直しの際には課題が残る。それは、リスク値をどのように見直すか分かりにくいことがある。なぜなら、最初のリスクの算定によりリスク対策を講じるので、すでに資産が守られている状況であり、リスクを想起しにくいということがある。

リスク値を見直す際に、リスク値に影響を与える因数として脅威、脆弱性があるが、守られた状態からリスク値を見直すとなると、情報キュリティインシデントが発生する等して新たな脅威、脆弱性が確認されないと、認識がしにくい。また、リスク値に影響を与える因数として、資産価値があるが、機密性、完全性、可用性も最初の設定段階で適用を誤る等でもないと資産そのものをいくら眺めても変化はない。

筆者は、これらの要因が情報セキュリティリスクアセスメントの継続的改善を妨げる要因と考える。リスクはまだ顕在化していない性質のため、どういうことが起こり得るかを想起することが必要になるが、リスク対策が取られていればどういう場合にリスクが生じるか想起がしにくい。実際に筆者の経験において、リスク値の見直しが形骸化している例をいくつも見ており、問題意識を形成している。形骸化を防ぎ、情報セキュリティマネジメントの継続的改善に資するリスクアセスメントはいかにあるべきかを考察した。

４．セキュリティ境界とリスク

既にリスク対策がとられた資産は保護されているという前提にたつ。しかし、その対策の境界が脆弱になると脅威が侵入する可能性が出てくる。筆者は、リスク対策がとられた境界を４つ定義したので図１に示す。それは、事業・サービスによる境界、組織・人による境界、場所による境界、技術（ネットワーク）である。

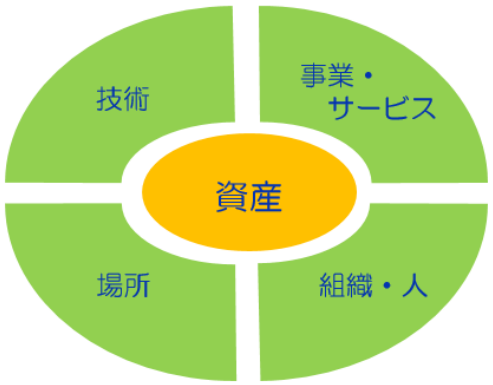

図１　境界に守られる資産

この境界を資産の保有者及び管理者が認識す

「Risk assesment for Continuous improvement in a Information Security Management」
† Yukio Nakayama, Kazuhiko Tsuda Tsukuba University

Copyright ©2015 Information Processing Society of Japan.
All Rights Reserved.

ることが重要である。リスクは変化によって生じうるので、境界が変化しうる事象を捉える。筆者はその変化要因として境界に影響を与える利害関係者を加えることとし、その例を図２に示す。

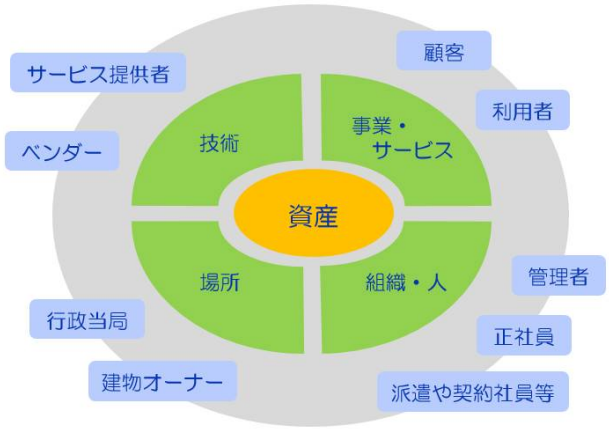

図２　境界と利害関係者例

５．利害関係者とリスク

利害関係者の変化は、よく発生することであり、その変化が境界に影響を与えるという視点を持てばリスクも見出しやすい。最初のリスク算定においてセキュリティ対策がとられているので、リスクは主に運用面において発生する。

(1)事業・サービスの境界（a とする）

顧客や利用者の変化が影響し、事業・サービスの境界が脆弱になる。ここでは、顧客や利用者の変化により守るべき資産に変更が生じていないかという視点が重要になる。事業・サービスの境界では守るべき資産の変動が大きいという視点から対策に漏れがないか、脆弱になっていないかを確認しなければならない。

(2)組織・人の境界（b とする）

社内の管理者、正社員、派遣や契約社員等の組織構成員の変化が影響し、人・組織の境界が脆弱になる。ここでは、例えば管理者の異動等による変更が、アクセス権の削除漏れ等につながる場合や、鍵の返却漏れ等、運用面において脆弱になっていないかを確認しなければならない。

(3)場所の境界（c とする）

オフィスの移転は直接、場所の境界に影響を与える。またビルへの入居者の場合、ビルオーナからの規制や場所によって行政からの規制が異なってくる。状況によって騒音等、利害関係者に影響を与えるリスクが生じることもある。

(4)技術（ネットワーク）の境界（d とする）

ネットワークの境界は技術的にも重要である。ネットワークの境界はルータやファイヤウォールにて明確になっていても、管理が明確になっているかという視点が重要になる。自社のネットワーク設備であっても管理が別の場合もありうる。また別会社がルータまで用意し、そこから内側が自社の管理ということもあり得る。自社の管理下でなければ統制が及ばないため、管理面での対策がもれていないか等リスクを想起し確認しなければならない。また、外部サービスを受けている場合は、境界は外部になるため、セキュリティのサービスレベルにおいてリスクを想起する必要がある。M&A 等でサービス提供者が異なった場合等の変化も技術の境界に影響を与える。

６．継続的改善に資するリスクアセスメント

リスクアセスメントが形骸化しないためには、境界の変化を敏感に捉えて、リスクを想起していくことが重要である。リスク値の算定においては、脆弱性の変化に着目することとなる。したがって、最初に算定されたリスク値を見直す際には、リスク値＝資産の価値×脅威×脆弱性を、リスク値＝資産の価値×脅威×（脆弱性×境界の変化）と捉えることとする。境界の変化＝a の変化の度合＋b の変化の度合＋c の変化の度合である。変化の度合いは組織で段階を定義する。これにより、境界の変化が生じる場合は、脆弱性が上がるという捉え方となる。

この方法によるメリットは、既に実施しているリスクアセスメント方法を大幅に変更するのではないので、仕組み化しやすいことがある。方法を大幅に変更すると、組織の抵抗感が生じ、それが継続的改善の阻害になる。それから、境界の変化は資産の保有者または管理者にとって分かりやすい。リスクは想起することが重要で、それは実際に資産の保有者や管理者が想起できなければならない。想起しやすくなることにより、情報セキュリティマネジメントの浸透にもつながり継続的改善に資する。デメリットとしては、最初のリスクアセスメントが非常に貧弱なものである場合や境界が明確に設定されていない場合には、変化を認識しにくい。これも継続的改善の阻害要因となる。

筆者は情報セキュリティマネジメントを実施している組織と議論し継続的改善が重要であると考えている。今後の視点では本稿の方法を適用した事例研究を増やす予定である。

[参考資料]

(1)日本情報経済社会推進協会「ISMS ユーザーズガイド JISQ27001：2006 対応リスクマネジメント編」2008 年 1 月

Copyright ©2015 Information Processing Society of Japan.
All Rights Reserved.