統合リスク管理レポート vol.02

セキュリティと成熟度の関係考察

– セキュリティレベルと成熟度と投資の関係–

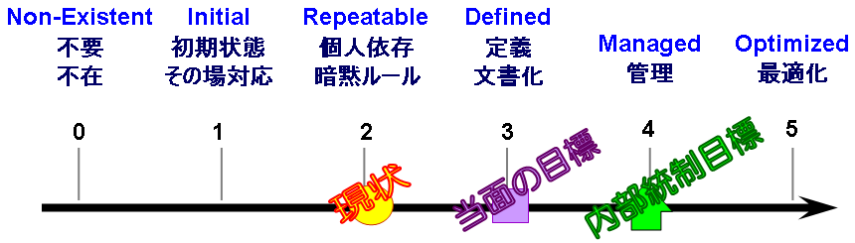
2012 年 7 月

LAC セキュリティコンサルティングチーム

セキュリティと成熟度の関係考察
＝ セキュリティレベルと成熟度と投資の関係 ＝

内田昌宏
Masahiro Uchida

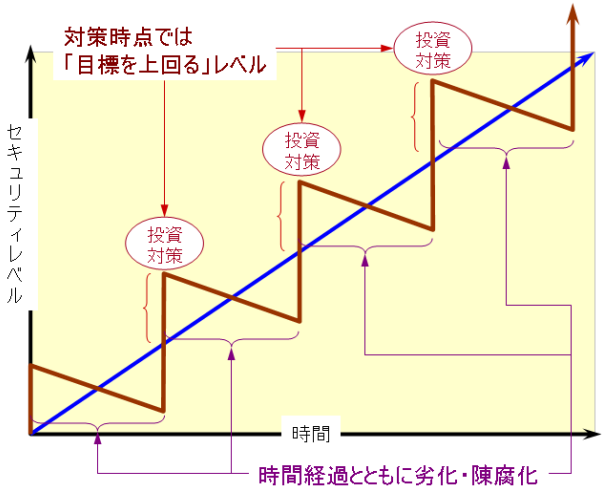
成熟度とは組織の能力を評価する指標のひとつである［図 1］。特にセキュリティを考える場合、マネジメントが形骸化していると、せっかく投資を行なっても継続的な成果を維持しにくいケースを多く目にしてきた。セキュリティレベルと成熟度にはどのような相関関係があるのだろうか、適切な投資とは…。これまでセキュリティアセスメントおよび成熟度評価を行ってきた結果から、統計的に傾向を分析し考察してみた。なお本稿で使用する「成熟度」は、おおむね「IT 成熟度[1]」を指している。



［図1　成熟度モデル指標］

1.　はじめに

インターネットを利用したビジネスやサービスが拡大している中、日々、OS やアプリケーションの脆弱性が発見され、脆弱性を悪用した新たな不正アクセスの手口が報告されている。このため、都度、対策を施さないと、情報セキュリティは時間経過とともに劣化・陳腐化していく［図 2］。



［図2　セキュリティレベルと時間経過］

多くの施策を導入すると、セキュリティが確保できたとの感覚を抱いてしまう。しかし一方で、投資効果について不安がつきまとうのはなぜだろう。また導入した施策だけで、推進態勢やマネジメントの課題は完全に解決できるのだろうか。

この命題に対し、直近セキュリティアセスメントを実施した 30 社を選定し［表 1］、いろいろな切り口から統計的な分析を試みた。選定した組織は、いずれも、従業員＝1 万人前後、資本金＝数百億以上の規模である。

業種	社数
金融（銀行、保険など）	4
エネルギー	2
医療、医薬品	2
情報通信	5
製造	4
運輸、物流	3
サービス	5
商社、商業、小売	5
計	30

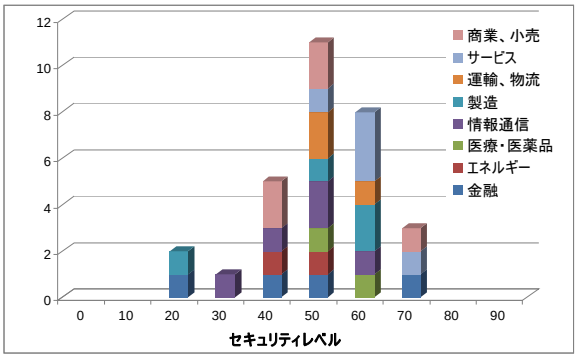
［表1　選定組織］

[1] COBIT 成熟度モデルの考え方を、情報セキュリティに独自にアレンジして適用した。

2. 統計結果の分析

2.1. セキュリティレベル

［表 1］の組織をアセスメント評価（リスク分析）した結果から、独自にセキュリティレベルを数値化し、ヒストグラムで表現すると、［図 3］のようにほぼ正規分布になった。特に業種や規模による特徴は見られなかった。

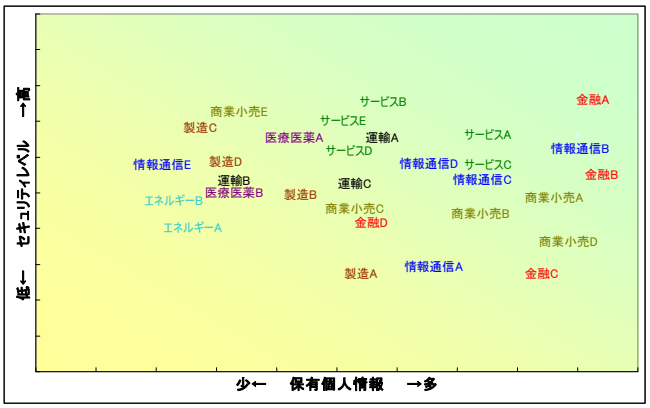


［図3　セキュリティレベル］

このセキュリティレベルの差が生じる要因はどこにあるのだろうか。掘り下げてみよう。

2.2. 保有個人情報とセキュリティレベルの相関

［表 1］の組織を、保有個人情報の多さを横軸に、セキュリティレベルを縦軸に二次元散布図にプロットしてみた［図 4］。



［図4　保有個人情報とセキュリティレベルの関係］

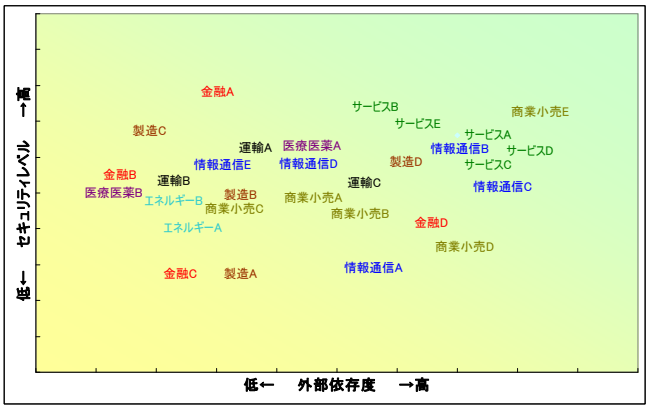
保有個人情報の多さとセキュリティレベルには、特に関係性は見出せなかった。それどころか、個人情報保護法の下においてもなお、セキュリティレベルが低い組織が存在しており、

- スピード重視のビジネスモデル、あるいは事業拡大・利益追求が優先され、リスクと投資の適切なバランスが見出せていない
- IT 担当者や委託先の意識・スキルに依存した対策が施されている

などと推察される。

2.3. 外部依存度とセキュリティレベルの相関

［表 1］の組織を、IT（開発、運用管理等）の外部依存度[2] を横軸に、セキュリティレベルを縦軸に二次元散布図にプロットしてみた［図 5］。



［図5　外部依存度とセキュリティレベルの関係］

外部依存度とセキュリティレベルにも、特に関係性は見出せなかった。むしろ相対的には、外部依存度が高くてもセキュリティレベルが維持できているケースが多く、

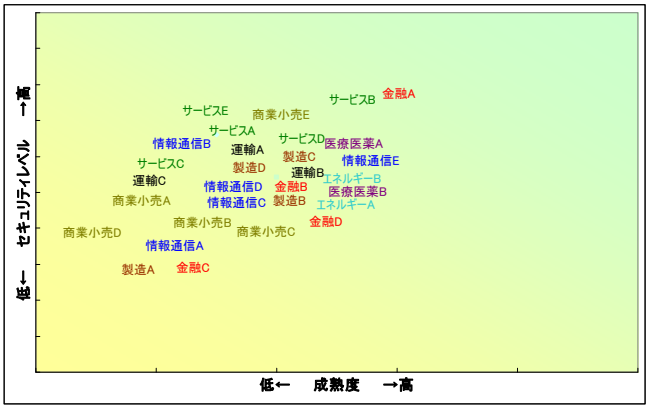
- 委託先に対して、明確にセキュリティ要件が提示されている（ただしこの推測は、外部依存度が低くてもセキュリティレベルが高いはずなので、必ずしもあてはまらない）
- クラウドサービスが拡大する中、サービス提供事業者が安全性の担保を差別化要素としている（委託元から明確なセキュリティ要件が提示されなくても、選定したベンダが、たまたまセキュリティレベルが高かった…というケースもあるかもしれない）

などと推察する。

[2] 外部依存度の高さ＝〝外部丸投げ〟ではないことを申し添えておく。

2.4. 成熟度とセキュリティレベルの相関

［表 1］の組織について、成熟度を横軸に、セキュリティレベルを縦軸に二次元散布図にプロットしてみた［図 6］。

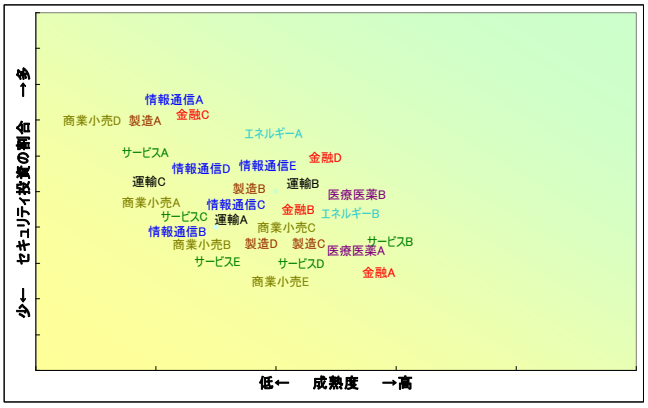


［図6　成熟度とセキュリティレベルの関係］

成熟度とセキュリティレベルには比例関係があるようにみえ、セキュリティレベルの差を生む要素として、成熟度が関係していることを見出した。

さて先に［図 2］では、投資をすればその瞬間、セキュリティも一定レベル高くなることを示した。では投資が成熟度向上に直結するのだろうか。

そこで［表 1］の組織について、成熟度を横軸に、投資割合（売上に対するセキュリティ投資額の割合）を縦軸に二次元散布図にプロットしてみた［図 7］。なお、ここでの投資額は、セキュリティアセスメントでのインタビューを通して得た情報、および導入している施策等から推定した。



［図7　成熟度と投資割合の関係］

なんと成熟度と投資割合は反比例しているようにみえる（少なくとも比例関係には見えない）。

このことから［図 6］は、「成熟度が向上すれば、セキュリティレベルが向上する」と解釈するのが妥当だ。

しかし一方で釈然としない部分も残る。

［図 6］で見る限り、成熟度ポイントそのものは決して高いとはいえず（30 社平均=2.27）、このことは以下のような実態を想像させるからだ。

- リスク低減策の投資効果や有効性が評価されておらず、適切なリソース（人、コスト）の配分が行なわれていない。
- 運用管理コスト削減のしわ寄せが、セキュリティ投資の抑制に拍車をかけ、ますます非機能要件であるセキュリティ対策が後回しになる。

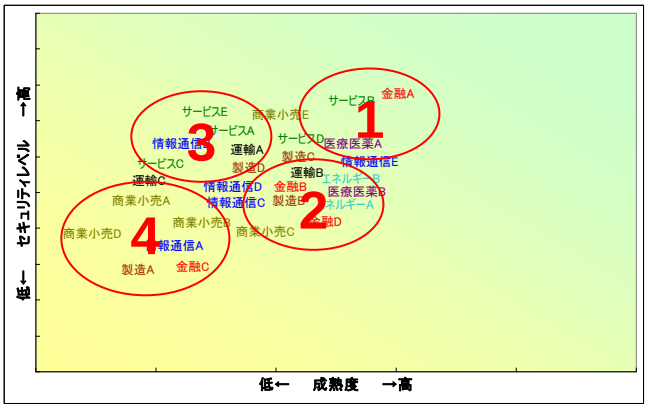
この推測が正しければ、以下のような成熟度向上を阻害する矛盾を抱えることになる。

- それでもビジネス戦略に応えるため、運用でカバーせざるを得ない。このため非効率稼動や手戻りが発生し、「人件費の含み損」を抱えることになる。人件費の含み損は、通常は数字として表には出ないため、ますますリソースの配分が厳しくなる。
- リソースの配分が遅れると、人材育成・人材確保が遅れ、ますます特定の人に依存した属人的な運用となる。

つまり過度な投資抑制は、成熟度向上をも妨げる結果になるといえる。

2.5. 成熟度とセキュリティレベルと投資の考察

［図 6］を 4 象限に分類し、特徴をみた［図 8］。



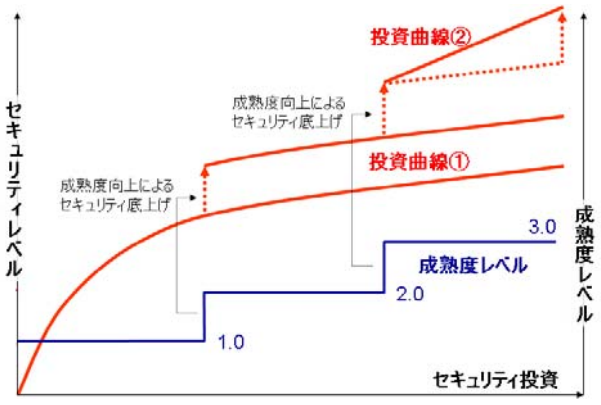
［図8　4 象限に分類］

» グループ①（成熟度・セキュリティレベルともに高い）は、相対的に投資割合は低い。
» グループ②とグループ③は、相対的にみて投資割合にばらつきがある。
» グループ④（成熟度・セキュリティレベルともに低い）は、相対的に投資割合は高い。

どういうことだろう。最も合理的な解釈は、

- 成熟度が低い分、投資によりセキュリティの維持向上を図っている。言い換えると、成熟度が低い場合は、投資によりセキュリティレベルを維持向上させる必要がある。
- 一方で成熟度が向上すれば、その分、セキュリティの底上げが可能になり、同じ投資でもより大きなセキュリティレベル向上が期待できる。あるいは最も有効性が高い施策に投資している。
- 一般的に組織における IT 投資額は、売上の 0.8%～2.0%[3] といわれており、かなり幅がある。PDCA のプロセスを組織にあわせて運用することができれば、属人的ではない組織運営が実現でき、かつ最適なコスト配賦（運用負荷、管理コスト）が評価できる。

ということになる［図 9］。



［図9　セキュリティレベルと成熟度と投資］

投資曲線は成熟度の向上とともに、傾きが緩やかになっていく（［図 9］投資曲線①）。一方成熟度が 3 以上に向上すれば投資対効果も向上すると推測される（［図 9］投資曲線②）。

3.　まとめと所見

組織の成熟度とは、問題発見～解決行動～改善にいたる組織の能力を表す指標である。

» 成熟度をレベル 2 から 3 に上げるためには、個人依存からの脱却を推進する必要がある。このため情報セキュリティ推進部門（IT 部門）では、ルールや基準値に基づくプロジェクト管理とレビューを徹底すべきである。
» 某社では、インフラ系部門と事業系部門のローテーションを断行したという。立ち上がりに時間は要したものの、結果として個人に依存していた部分が明らかになったとの事。マネジメントの決断に脱帽！
» IT を使いこなす能力とその効果は、それを使う人の意識の高さに依存する。組織の成熟度を向上させるには、並行してそこにいる個人（一般の従業員）のスキルも成熟させなければならないと考える。

4.　おわりに

成熟度が低い場合は、情報セキュリティ定着にも大きな労力を必要とする。実態が見えていないため、理想論／規則／罰則が啓発の手段となりがちである。しかしある一定レベルまで底上げ（成熟度の向上）ができた後は、リスクコミュニケーションを基軸にした相互啓発が、自律的で成熟した事業活動を実現すると確信する。

以上

2012 年 7 月
内田昌宏（うちだまさひろ）
技術士（情報工学部門）
株式会社ラック
理事　エグゼクティブコンサルタント

[3] 「平成 22 年度企業の IT 投資動向に関する調査報告書」（http://www.meti.go.jp/policy/mono_info_service/joho/itdoukou/2010/）より

【徒然素心ひとりごと】

「内部統制」がわからない。ますますわからない。

「内部統制」とは、業務を適正に効率よく運営するための仕組みを確立することで、組織を向上させる…という建設的で健全な組織運営を目的としている…と考えていた。
しかし一方、同じ「統制」を使う言葉に「情報統制」があり、これには公開情報を制限し、都合のよい情報のみを提供する…という作為的でネガティブなニュアンスがある。

さて、
内部統制…internal control、情報統制…control of information　というように、
両方とも「control」という単語が使われているのですね。
（英和辞典、英英辞典を調べても、control にはポジティブな印象は持てなかった。）

あらためて考えてみると、内部統制は、
　〝あたりまえのことを、あたりまえのようにやる〟。
　〝あたりまえ〟とは〝決められたルール通り〟ということ。
すなわち〝よけいなことはするな〟をコントロールすること（させること）なのかな。
とすれば、そこには意思はなく、機械のように決められたことを淡々とこなす姿が浮かび上がる。

そして、内部統制を評価するモノサシとして成熟度が使われています。
「成熟」には〝果物が成熟する〟というように文字通り成長を喜ぶポジティブなイメージが。

COBIT に惚れている私にとって、気持ち悪いのは、
コントロールできているか（全員が例外なく同じことを行っているか）を、成熟度（十分に成長しているか）というモノサシで評価することの矛盾。
「全員が例外なく同じことを行うこと」を担保すればするほど、永遠にその組織に成長は訪れないだろうな…と思ってしまう。

と、こんなことを同僚につぶやいたら、
「人に対して、間違えを起こさないようにルール通りやらせることも統制だが、
　人が間違わないように、環境を整備（入力ミスをしたら IT が受け付けない…とか）する
　ことこそ統制だ」
といわれました。

だったら「control」なんて言葉、使わないでほしいな…、いまさらですが…。

LAC のセキュリティコンサルタントは、お客様の課題にひとつひとつ丁寧に向き合い、お客様の立場で課題解決を支援いたします。
レポートの内容、情報セキュリティに関するご相談はこちらまで。

株式会社ラック http://www.lac.co.jp
〒102-0093
東京都千代田区平河町 2-16-1 平河町森タワー
TEL : 03-6757-0113　E-mail : sales@lac.co.jp