Vol.2010-CSEC-50 No.43
2010/7/2

セキュリティ投資モデルと Trust-but-verify アプローチによるモジュール選択

松浦幹太[†1]　楊鵬[†1]

情報セキュリティ経済学では，理論研究の進展は著しいが，問題分析以外の応用があまりなされていない．本研究では，最適投資理論を応用して，製品認証を受けた情報セキュリティモジュールのユーザ（モジュールを用いてシステムを開発するベンダ）向けガイドラインを試作した．経験的選択を信頼してモジュール選択を重ねてから投資理論で検証することにより PDCA サイクルを構成し，理論と実践を融合した点に，特徴がある．

Choosing Security Modules Based on an Investment Model and Trust-But-Verify Approach

Kanta Matsuura[†1] and Peng Yang[†1]

Security economics has many achievements in analysis-oriented theories. However, it lacks synthesis-oriented approaches. In an attempt at synthesis, we developed a users' guideline for product-validation systems regarding security modules. The guideline firstly trusts heuristic choices but eventually verifies a set of choices based on an investment theory so that users can construct a PDCA cycle paying attention to both theory and practice.

1. はじめに

情報セキュリティシステムを構築する際に，要件に基づき最適なシステム設計をしたいという要求は強い．しかし残念ながら，技術面だけにとどまらずリスクを科学的に扱う理論基盤に基づいた設計手法や評価手法は存在しない．ただし，IT システム設計案全体を見通しよく比較評価するためにベストプラクティスを文書化した VMM（Value Measuring Methodology）[1] が米国連邦政府で利用実績を積み重ねるなど，一定の文書化さえできれば新たな設計評価手法も利用され得るだけの土壌は整いつつある．

一方，システムの構成要素となるモジュール単位では，要件の客観的な表現を容易にする製品認証制度（モジュール製品を試験し認証する制度）が注目を集めている．例えば，日本の暗号モジュール試験及び認証制度 (JCMVP: Japan Cryptographic Module Validation Program)[2] は，2006 年 6 月から試行運用，2007 年 4 月から正式運用が始まり，現在に至っている．JCMVP では，暗号モジュールを 4 つのレベルに分けて試験及び認証している．生体認証モジュールに関しても，研究段階だが，適当な複数レベルに分けた試験及び認証制度を可能とするための評価基準作りが試みられている[3]．

モジュール選択を何度も行いながらシステムを構成する場合，ベストプラクティスに基づいて設計チームを稼働させることが多いだろう．東京大学生産技術研究所松浦研究室では，それら多くのモジュール選択結果の間に理論的整合性（ミクロ経済学に基づく解析的な理論モデルとの整合性）があるかどうかを簡易に検証し，代替案比較によるシステム設計を支援するためのドキュメントを作成し公開した[4]．システム構築には様々な立場の利害関係者が関わるが，想定する読者は「モジュールを用いてシステムを構築するベンダ」である．また，JCMVP が既に運用されていることに配慮し，4 つのレベルに分けて試験及び認証する制度を対象としている[⋆1]．本稿では，同ドキュメント（ガイドライン）の背景と内容を概説する．

2. 理　論

ミクロ経済学に基づく情報セキュリティへの最適投資理論が盛んに研究されるようになってから 10 年弱が経過している．ガイドライン 4) では，

- 定式化を最適投資以外の問題にも適用でき，一般性が高い．
- 公的データによる実証研究が存在する．
- 豊富な含意が導出されており，それらがベストプラクティスによく整合している．

を全て満たす貴重なモデルである Gordon-Loeb モデル[5] とその拡張[6] を理論基盤とする．そこでは，次の基本パラメータを定義して定式化が行われる．

†1 東京大学
The University of Tokyo

⋆1 ただし，レベルの個数が異なっても，基本的に同じ手法で PDCA サイクルを構築できる．

Vol.2010-CSEC-50 No.43
2010/7/2

λ: 攻撃等の脅威が成功した時の経済的損失.

t: 攻撃等の脅威が生起する確率（$0 \leq t \leq 1$）.

v: 攻撃等の脅威が生起した際に，生起したという条件の下で，脅威が成功する条件付き確率（$0 \leq v \leq 1$）．**脆弱性**と呼ばれる.

今，金額 $z \geq 0$ の情報セキュリティ投資を考える．Gordon-Loeb モデルでは，投資によって脆弱性を低減できると見なす．そして，低減後の脆弱性は投資金額と投資前の脆弱性のみに依存すると仮定し，低減後の脆弱性を $S(z, v)$ と表記する．この $S(z, v)$ を，セキュリティ侵害確率（SBP: security breach probability）関数と呼ぶ．最適投資問題は，この脆弱性低減による損失低減の期待値から投資額を差し引いた値 ENBIS（Expected Net Benefits from an investment in Information Security）を最大化する問題として定式化される．SBP 関数としては，いくつかの関数系が検討されている．とくに，$S(z, v) = v^{\alpha z+1}$ で定義される関数系は,「極めて低い脆弱性や高い脆弱性ではなく，中程度の脆弱性に対して重点投資すべきである」という投資指針を表現した解析解をもたらし，唯一の実証サポートを有する関数系として注目されている[7]．正の定数 α は，情報セキュリティの生産性を表現している.

ただし，情報セキュリティ投資の効果には本来，攻撃等の脅威の抑止力も含まれるはずである．そこで，拡張モデルでは,「投資に応じて脅威生起確率 t も低減される」と捉えて抑止力を理論に取り込む．投資後の脅威生起確率を $T(z, t) = t^{\beta z+1}$ でモデル化し，非負の定数 β を「脅威低減に関する（情報セキュリティの）生産性」と呼ぶ．これに伴い，先の正の定数 α は,「脆弱性低減に関する（情報セキュリティの）生産性」と呼ぶこととなる．この時，ENBIS 最大化問題の解析解は

$$z^* = \frac{\ln\left\{-1/\left(vt\lambda \ln(v^\alpha t^\beta)\right)\right\}}{\ln(v^\alpha t^\beta)} \tag{1}$$

で与えられる．ただし，$v \ln v + \beta(\ln t)\alpha^{-1} v + 1/(\alpha t \lambda) \geq 0$ の場合には，投資額をゼロに限りなく近づけた時の限界効用が限界費用を上回らないので，投資はなされない.

上記の結果は，横軸に α，縦軸に β をとった平面に表現すると体系的に理解できる．すなわち，**図 1** のようにまとめられる．この平面（二次元空間）を，**情報セキュリティの生産性空間**と呼ぶ．最適投資戦略は，脆弱性を横軸，最適投資額を縦軸にとったグラフ（最適投資曲線）で考察される．生産性次第で，最適投資曲線の型が変化する．生産性空間の原点付近では投資しないことが推奨され，その右側に広がる領域では中程度の脆弱性を重視した投資が推奨される．上方の領域では，高い脆弱性が重視される.

過剰投資に警鐘を鳴らす含意も導出されている．例えば，(1) 式を被害額の期待値 $vt\lambda$ で除して $x = -vt\lambda(\alpha \ln v + \beta \ln t)$ とおけば，

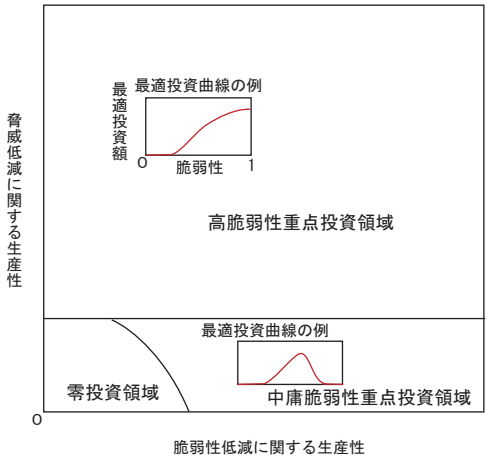

図 1 情報セキュリティの生産性空間と最適投資曲線
Fig. 1 Productivity space of information security and optimum investment curves.

$$\frac{z^*}{vt\lambda} = -\frac{1}{x} \ln\left(\frac{1}{x}\right) \tag{2}$$

となる．(2) 式の右辺は，$x = e$ において最大値 $1/e$ をとる．ゆえに，最適投資額は，被害額の期待値の高々$1/e$ 倍すなわち 37%である．コストが被害額の期待値の 37%を越える場合には，そのままでは過剰投資の恐れがある．この含意は，元の Gordon-Loeb モデルにおいても導出できる.

3. 選択の枠組みと手順

3.1 概　　要

複数のモジュール候補から一つのモジュールを採用する際，候補の中には，認証を受けていないモジュール（以下では，非認証候補という）や，特定のセキュリティレベルで認証を取得したモジュール（レベル i を取得した場合，以下では，Lvi 認証候補という）が存在する．進めるべき手順は，4 段階から成る.

- 手順一: 採択枠組みの開発
  (1)　コスト・ストラクチャの構築

(2) リスク・ストラクチャの構築
- 手順二: 候補の分析
  (1) 総コストの算出
  (2) リスクスコアの算出
  (3) リスク許容境界の設定
  (4) 文書化の始動
- 手順三: 統合
  (1) 候補の選択
  (2) 選択結果の統合
  (3) 理論に照らした検証
  (4) 文書の更新
- 手順四: 文書化の完了
  (1) セキュリティ仕様の作成
  (2) 予算案の準備
  (3) 要件変更への対応
  (4) 改良改革

3.2 手順一: 採択枠組みの開発

採択の枠組みは，コストストラクチャとリスクストラクチャから構成される．

コストストラクチャの構築: コスト要素の構造を明らかにする．総コストを算出できるようにするのが主な目的であるが，開発チームが作業に体系的に取り組む体制（心構えも含む）となるのを促すことも，目的に含まれる．

リスクストラクチャの構築: リスク要因の相対的優先度を表現したリスクファクタを設定する．モジュールの採用による合計リスクの指標である「リスクスコア」を算出できるようにするのが主な目的であるが，開発チームが作業に体系的に取り組む体制（心構えも含む）となるのを促すことも，目的に含まれる．

コストストラクチャの構築では，存在し得る主要なコスト要素をリストアップし，各候補の合計コストを計算できるようにする．コストがどの程度複雑な構造を持つかは，ケースバイケースである．ここでは，例として，次のコストストラクチャが構築されたとする．

- 1.0 開発費用
  - 1.1 ハードウェアの導入による費用
  - 1.2 ソフトウェアの導入による費用
  - 1.3 サポートサービスの利用による費用
- 2.0 実装費用
  - 2.1 調達に際して発生する費用
  - 2.2 人件費
- 3.0 運用保守
  - 3.1 新人教育による費用
  - 3.2 メインテナンスによる費用

リスクストラクチャの構築では，優先度で重み付けをしてリスク要因を統合できるようにすることが肝要である．開発過程では，実装ミスや，あるレベルの要件に未対応などの可能性を，想定しなければならない．それらの不具合の発生確率を，ここでは不具合率と呼ぶ．リスクストラクチャの 5 つのリスク要因（Risk Factor）は,「実装対象の技術自体[⋆1]の不具合率と，4 つのセキュリティレベルそれぞれに対応する不具合率を，相対的にどの程度重視するか」というバランスを表現する．この重み付けは，製品の利用環境などに合わせなければならない．

- RiskFactor$=(p_0, p_1, p_2, p_3, p_4)$ と定義する．ここに，p_0 は対象技術の優先度を表し，p_i はレベル i（$1 \leq i \leq 4$）の優先度を表し，$p_0+p_1+p_2+p_3+p_4 = 100\%$ とする．例えば，$(0, 0, 100\%, 0, 0)$ は，レベル 2 のみ重視することを表す．$(30\%, 60\%, 10\%, 0, 0)$ は,「レベル 1 を最も重視し，レベル 2 もある程度望ましいが，執着しない．かつ，対象技術（自体に不具合がないこと）もある程度重視している.」ということを表す．
- もし，ある高い安全性レベルが必要ならば，より低い安全性レベルの優先度を 0 にする．例えば，レベル 2 の安全性が絶対条件ならば，$p_1 = 0$ に設定する．
- 脅威低減効果があまり高くないと思われる場合には，高いレベルへの過剰投資になっていないか注意する．
- 脅威低減効果が充分高いと思われる場合には，高いレベルへの投資不足になっていないか注意する．

3.3 手順二: 候補の分析

まず，コストストラクチャに基づいてコスト要素の試算を行い，統合する．ここでは，特段の理論は用いず，単純に総和をとる．

次に，各リスク要因の優先度と想定される不具合率を掛け算し，その結果をそのリスク要

⋆1 以降では単に「対象技術」と記す．暗号モジュールの場合は，暗号アルゴリズム自体．

因のリスクスコアとし，そして 5 項目のリスクスコアの総和を当該候補のリスクスコアとして算出する．モジュールのセキュリティレベルが 5 種類（レベル 4，レベル 3，レベル 2，レベル 1，非認証）しかないため，各候補のとり得るリスクスコアは，せいぜい 5 つの値にしか分かれない．ここに，リスクスコアとは，モジュールの採用による合計リスクの指標であって，0 から 100 までの値を取り得る．不具合率の重み付け総和をとったということを踏まえて% を添えて表記するが，何か具体的な確率を意味するわけではない．

Lvi 認証候補に関しては，レベル i までのリスク要因の不具合率を 0%，レベル $i+1$ 以上のリスク要因の不具合率を 100% と見なす．

非認証候補の不具合率の値には，認証制度の運営機関により公開されたレベル別の実装不具合率を用いる．ただし，公開データが粗く，全てのレベル分けに対応していない場合には，簡易に（しかしやや慎重に）考えて「等分した値以上である」と推定する[⋆1]．手順三の統合作業で必要となるので，候補に非認証モジュールが含まれていない場合でも，かりに非認証候補があればリスクスコアがいくつになるかを算出しておく[⋆2]．

- 例として，2009 年のデータ[8] を参照してみる．レベル 1 とレベル 2 の合計不具合率が 50%であり，レベル 3 とレベル 4 の合計不具合率が 75%であった．等分して下限を決め，非認証候補に関しては，レベル 1 およびレベル 2 のリスク要因の不具合率をいずれも 25%+ と設定し，レベル 3 およびレベル 4 のリスク要因の不具合率をいずれも 37.5%+ と設定する．同じ実データによれば，認証を受けようとする暗号モジュールですら，アルゴリズムの実装不具合率は 8%にも及んだ．よって，非認証候補に関しては，暗号アルゴリズムの不具合率を 8%+ と設定する．ここで，“x%+”という表記は，不具合率が x% 以上であることを意味する．

もう一点の注意事項として，候補のリスクスコアが 0% となることは，決して「当該候補を採用すれば構成されるシステムから脆弱性が排除される」ことを意味しているわけではない．リスクスコアの定義から明らかなように，リスクスコアが 0% となることは，当該候補の採用がユーザの IT セキュリティシステム構築方針を最大限に満たすことだけを意味する．言い方を変えると，リスクスコアが 0% となる候補を採用しても脆弱性は依然として存在するかもしれないが，ユーザに重要視されていない，と考えてよい．

例 1: ユーザが設定したリスクファクタを，$(30\%, 60\%, 10\%, 0\%, 0\%)$ とする．この時，Lv2〜Lv4 のモジュールであればいかなる認証候補でもリスクスコアは 0% になり，Lv1 のモジュールであればいかなる認証候補でもリスクスコアは 10% になり，認証を取得していないモジュールであればいかなる非認証候補でもリスクスコアは 19.9%+ となる．

例 2: ユーザが設定したリスクファクタを，$(10\%, 0\%, 80\%, 10\%, 0\%)$ とする．この時，例 1 と同様にして計算すると，Lv4 認証候補，Lv3 認証候補，Lv2 認証候補，Lv1 認証候補，非認証候補のリスクスコアは各々0%，0%，10%，90%，24.55%+ となる．

最後に，リスク許容境界（算出されたそれぞれのリスクスコアに対して投資できる最大予算）を見積もる．ただし，具体的なモジュールを想定してそれに対して投資できる最大予算を考えるのではなく，現在のモジュール選択問題の置かれた状況のもとで，それぞれのリスクスコアに対していくら投資できるかを考える．ここでは，Lv1 認証候補のリスクスコアに対して許容できる最大コストが例 1 で 28 万円，例 2 で 10 万円となったとする．また，Lv2 認証候補のリスクスコアに対して許容できる最大コストが例 1 で 40 万円，例 2 で 50 万円となったとする．

手順三へ移る前に，文書化を始動させる．すなわち，コストストラクチャの構築方法，リスク要因の設定根拠，リスク許容境界を決定する流れに関わる全ての情報と仮定を，明確かつ正確に文書化する．

3.4 手順三: 統合

分析した候補から何を選択するかを，最適投資理論で直接は支援しない．しかし，必要な利害関係者を集め，経験的ではあっても費用対効果を強く意識した協議によって選択する．総コストがリスク許容境界におさまらない候補は選択しない．また，このモジュールが破られることに起因する被害額の期待値を見積もることができる場合，総コストが被害額の期待値の 37%を越える候補も選択しない．

システム開発においてモジュール選択（採択）が一回あるいは少数回しか行われない場合，選択結果の統合は行わず終了する．

モジュール選択（採択）が多数回行われる場合には，選択結果の統合を行う．あるモジュール選択を行った結果選択された候補の総コストを Z，許容できる最大コストを Z_{max}，その選択に至る分析で算出した非認証候補のリスクスコアを R とする．横軸にリスクスコア，縦軸にコストをとり，点 (R, Z) と点 (R, Z_{max}) をマーキングして，両者を結ぶ線分を記す．この作業を，全てのモジュール選択に関して（同じ平面で）実施する．ただし，選択に際し

⋆1 例えば，レベル 1 とレベル 2 の不具合率の合計が公開されていてその値が 60% である時には，レベル 1 とレベル 2 の不具合率をそれぞれ「30% 以上」と推定する．
⋆2 統合時に必要になってから算出するのではなく，この段階で算出しておく．

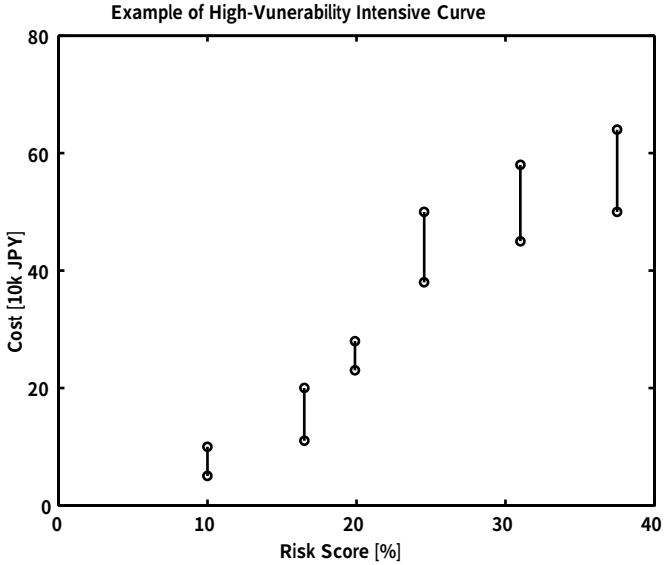

図 2 モジュール選択の統合例 1
Fig. 2 Example of a set of module choices (1).

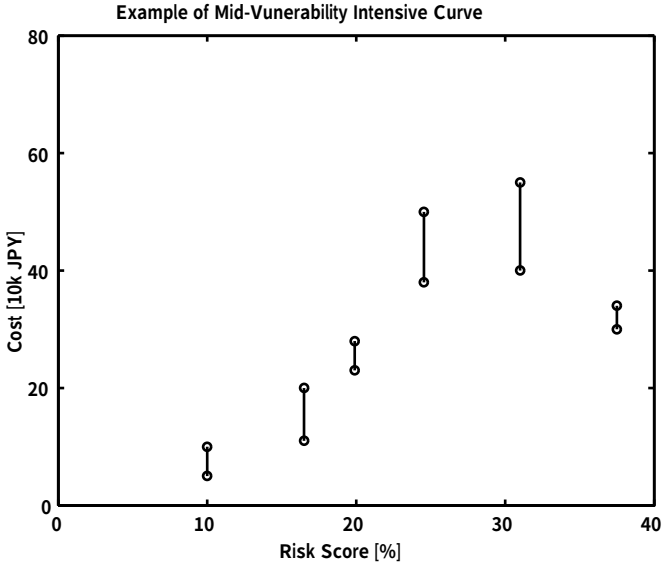

図 3 モジュール選択の統合例 2
Fig. 3 Example of a set of module choices (2).

て明らかにリスク回避的[⋆1]な意志決定をした場合には，マーキングをせずに省略する（すなわち，統合作業に含めない）．

いよいよ，理論に照らした検証を行う．例えば，例 1 では某 Lv1 認証候補，例 2 では某 Lv2 認証候補が選択されたとする．さらにいくつも選択を行い，全てを一つの図（平面）に統合した結果が**図 2** のようになった場合（統合例 1），**図 3** のようになった場合（統合例 2），そして**図 4** のようになった場合（統合例 3），を考える．

統合例 1 のように各線分を通る高脆弱性重視型の最適投資曲線を引くことが可能な場合や，統合例 2 のように各線分を通る中庸脆弱性重視型の最適投資曲線を引くことが可能な場合には，とりわけ問題視せず，統合結果を受け入れる．

統合例 3 のように，それらのいずれでもない場合には，意志決定の基礎となる考え方や基準が首尾一貫していなかった恐れがある．よって，統合結果を受け入れず，現在の文書を基に信頼性の低い作業を洗い出して分析を再度行うなど，PDCA サイクルを回して再度統合する．追加サイクルを経て統合結果が受け入れられたら，終了する．このように「まずは経験的選択を信頼し，要所で体系的に検証して進むべき方向性を定める」という方針は，情報セキュリティ投資の効果を計量する米国連邦政府の取り組み[9] でも試みられ,「trust but verify approach」と呼ばれることがある．

最後に，統合作業も含めた追記を行い，文書を更新する．

3.5 手順四: 文書化の完了

以下を遂行し，文書化を完了させる．

- システム全体に関して首尾一貫したセキュリティ仕様を明確にし，文書に反映させる．
- システム全体に関してほぼ揃った精度で予算案を準備し，文書に反映させる．
- 手順三と手順四の実行中に，急遽システムへの要件が大きく変わるなどの事態が生じる

⋆1 リスク回避的とは，投資家の投資リスクに対する選好特性の一つである．投資の期待収益に第一の基準を置かず，極力リスクの小さい投資機会を選択する特性を，リスク回避的という．一方，リスクに関わりなく，より期待収益が見込める投資機会を選択する特性のことをリスク中立的という．本研究の最適投資理論では，リスク中立性が仮定されている．

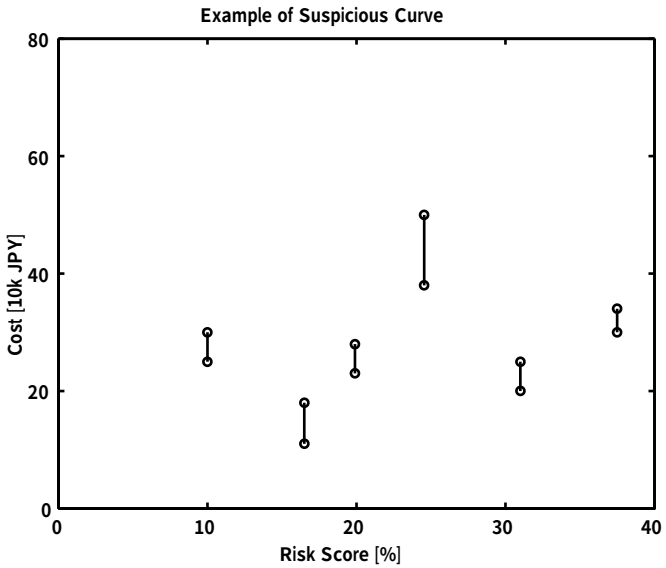

図 4 モジュール選択の統合例 3
Fig. 4 Example of a set of module choices (3).

恐れがある．その場合，現在の文書を基に，要件変更の要請に対応すべきか棄却すべきかを速やかに決定する．

- 要件変更の要請に対応する場合には，サイクル増加を有効利用すべく，要請に該当しない事項に関しても改良を試みる．

4. むすび

情報セキュリティと経済学にまたがる学際的研究が，重要性を増している．実際，概ね 2000 年頃から研究成果が盛んに発表されるようになり[10]，2002 年 5 月に始まった国際会議 WEIS（Workshop on Economics and Information Security）が発展して確かな研究コミュニティが形成された．そして，2009 年の WEIS におけるパネル討論で参加者らの意見の一致を見たように，これまで構築してきた理論で何を作って社会貢献できるかが問われる時代になっている．しかし，例えば「ただ乗り問題」のように「何故そのような問題が起きるのか」を分析する理論研究では一定の成果があがっているものの，実証研究では苦戦が続き，何かを開発・構築し社会実装する試みはそもそもほとんど見受けられない．本研究は，世界に先駆けてアナリシスの時代からシンセシスの時代へ移行する流れを生むべく，ミクロ経済学的な理論を実務文書に応用した枠組み開発である．先駆けゆえ問題も多いかもしれないが，ケーススタディにも取り組んで改良を重ねてゆきたい．

謝辞 本研究の一部は，新エネルギー・産業技術総合開発機構（NEDO）産業技術研究助成事業（若手研究グラント）による助成を受けた．

参考文献

1) CIO Council Best Practices Committee: Value Measuring Methodology How-To-Guide (2002).
2) 情報処理推進機構: 暗号モジュール試験及び認証制度.
http://www.ipa.go.jp/security/jcmvp/index.html
3) 井沼 学: バイオメトリクスセキュリティに関する研究, 産業技術総合研究所情報セキュリティ研究センター平成 21 年度研究成果報告会 (2010).
4) 東京大学生産技術研究所松浦研究室: 情報セキュリティモジュールの認証製品利用に関するガイドライン (2010).
http://kmlab.iis.u-tokyo.ac.jp/resources/guideline_1_0.pdf
5) Gordon, L.A. and Loeb, M.P.: The Economics of Information Security Investment, *ACM Trans. Info. & Sys. Sec.*, Vol.5, No.4, pp.438–457 (2002).
6) Matsuura, K.: Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model, in Johnson, M.E. (ed.) *Managing Information Risk and the Economics of Security*, pp.99–119, Springer (2009).
7) Liu, W., Tanaka, H. and Matsuura, K.: Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms, 情報処理学会論文誌, Vol.48, No.9, pp.3204–3218 (2007).
8) Communications Security Establishment, Canada: CMVP Annual Report (2009).
9) Paller, A. and Streufert, J.: Developing Metrics for Cybersecurity Programs, Federal Office Systems Exposition 2010 Conference (2010).
10) Matsuura, K.: Security Tokens and Their Derivatives, Technical Report29, Centre for Communications Systems Research, University of Cambridge (2001).