リスクポートフォリオに基づいた サイバーセキュリティ対策選定プロセスの提案

島 成佳† 芦野 佑樹† 佐々木 良一§

† 日本電気株式会社 / 東京電機大学
211-8666 川崎市中原区下沼部 1753 /
120-8551 東京都足立区千住旭町 5
{shima@ap, y-ashino@cw}.jp.nec.com

§ 東京電機大学
120-8551 東京都足立区千住旭町 5
sasaki@im.dendai.ac.jp

あらまし 組織は，年々高度化・巧妙化するサイバー攻撃の脅威に対して，既存対策の強化や新規対策の導入を図り，適切なセキュリティレベルを維持しなければならない．しかし，組織では対策予算が限られていることから，脅威に対して効率的で効果的なセキュリティ対策を選定する必要がある．本論文では，脅威のリスクに基づきセキュリティ対策を選定する際に，リスクアセスメントを支援するためのリスクポートフォリオを用いたプロセスや手法に関して提案する．

Cyber Security Countermeasure Selection Process based on Risk Portfolio

Shigeyoshi Shima† Yuki Ashino† Ryoichi Sasaki§

†NEC Corporation / Tokyo Denki University
1753, Shimonumabe, Nakahara-ku, Kawasaki, Kanagawa, 211-8666 JAPAN /
Senjuasahichou 5, Adachi-ku, Tokyo 120-8551, JAPAN
{shima@ap, y-ashino@cw.jp.nec.com}

§ Tokyo Denki University
Senjuasahichou 5, Adachi-ku, Tokyo 120-8551, JAPAN
sasaki@im.dendai.ac.jp

Abstract Cyber-attack threats of organizations increase year by year. In such situation, organizations must maintain an appropriate security level. However, organizations must take measure for cyber security within the limits of the budget. Thus, organizations are hard to select appropriate countermeasures from cyber security countermeasures. This paper proposes processes and methods of countermeasure selection for information security supervisors. We describe analysis of risk processes and analysis method based on risk portfolio.

1 背景

サイバー攻撃は，年々手口が高度化・巧妙化し，目的が多様化している．また，ビジネスの場では，スマートフォン等の新たな機器の導入やクラウドサービス等の新たなサービスの利用が拡大している．組織はこれらの変化によって発生する新たな脅威に対応して，既存対策の強化や新規対策の導入を図り，組織の事業継続のために適切なセキュリティレベルを維持しなければならない．このため，現状の情報セキュリティ対策が適切なものであるかどうかの把握が

必要となる．

高まるサイバー攻撃の脅威に対応すべく，組織の情報セキュリティに係る予算は増加傾向にある．[1] しかし，増加傾向にあるとは言え限られた予算の中で，すべての脅威に対して十分なコストをかけて対策を講じることは困難な状況にある．このため，組織は現状のサイバー攻撃の動向や組織の情報システムの構成等を把握し，事業継続の観点から適切なセキュリティレベルを考慮しながら，予算の範囲内で効果的・効率的な脅威対策を実施しなければならない．組織の事業や情報システム等によって脅威の捉え方が異なるため，同じ脅威でも組織によってリスクの大きさが異なる．このため，他組織の真似や人任せにすることなく，組織自身でリスクを把握して主体的にマネジメントしていくことが重要となる．土井らも組織がリスクアセスメントを行う必要性を述べている [2]．

現状リスクマネジメントは，コンサルタント等の専門家の助けなしに実施することが困難である．例えば，NIST SP800-30 Revision 1[3] や ISO/IEC 27005[4]，ISO/IEC 31000[5] 等のドキュメントを参照してリスクマネジメントの実施を試みたとしても，情報セキュリティマネジメントや情報セキュリティガバナンス [6] 等の知識がなければこれらの内容を理解することすら容易でない．事実，NIST SP800-30 の想定読者はリスクマネジメントの専門家である．もし内容をある程度理解できても，実施策への落とし込みは容易でない．また，専門家の助けを得る場合でも，専門家とのコミュニケーションを通してリスクへの適切な対処を行うために，ある程度の知識や経験が必要となる．

リスクマネジメントは，他の ISMS(Information Security Management System) 等のマネジメントシステムと同様，プロセスを回して経験を積み知識を得ることで，より効果的・効率的な対処が可能となる．このため，組織はスモールスタートからでもリスクマネジメントのプロセスを回すことが必要である．

本研究は，これまでリスクマネジメントを実施していない，または，実施不十分な組織が，リスクマネジメントのプロセスを回すことが可能になることを目標とし，実現に向けたリスクマネジメントのプロセスや手法を創出する．本論文では，セキュリティの責任者や担当者を対象に，リスクマネジメントのプロセスをスモールスタートで回し始めるための簡易的なリスクアセスメントのプロセスや手法を提案する．

2 用語定義と想定するリスクマネジメント

本論文では，網羅性と実行性，入手容易性の観点から NIST SP800-30[3] を参照する．NIST SP800-30 は，NIST の Web サイトから入手可能である．また，邦訳されたもの [7] は IPA のサイトから入手可能である．

2.1 用語定義

「脅威」と「リスク」および関連用語は，NIST SP800-30 を参照し，以下のように定義する．

- 脅威
  組織の業務（ミッション，イメージ等を含む），組織の資産，個人，他の組織，または国家に負の影響をもたらしうるあらゆる状況または事象．要因としては，情報の正規の権限によらないアクセス，破壊，開示，または変更，および/またはサービス妨害（DoS）などがある．脅威は脅威源と脅威事象に分解することができる．
- リスク
  発生しうる状況または事象によってエンティティが脅かされる度合である．その状況または事象が発生した場合にもたらされる負の影響ならびに発生する可能性をもとに算出される．
- 脅威源
  脆弱性の意図的な利用を目的とした意図および方法，または脆弱性を誤って利用する可能性のある状況や方法．

- 脅威事象
  望ましくない結果または影響をもたらしうる事象または状況.

- 脆弱性
  情報システム，システムセキュリティ手順，内部統制，または実装に存在する弱点で，脅威源によって利用される可能性がある.

- 素因的条件
  組織，ミッション/業務プロセス，エンタープライズアーキテクチャ，または情報システム（その運用環境を含む）に存在する条件の一種であり，単一の，あるいは複数の脅威事象が組織の業務と資産，個人，他の組織，または国家に望ましくない結果または負の影響をもたらす可能性に影響を及ぼす.

2.2 リスクマネジメント

本論文では，NIST SP800-30 のリスクマネジメントを参照するため，そのプロセスを概説する.

NIST SP800-30 のリスクマネジメントプロセスには図 1 のように「フレーム化」「アセスメント」「対応」「モニタリング」の 4 ステップがあり，これらステップは相互に関係する.

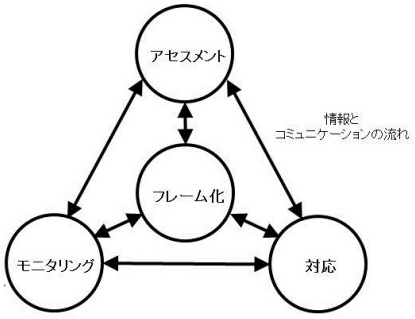

図 1: NIST SP800-30 のリスクマネジメントプロセス

- フレーム化
  組織がどのようにリスクをアセスメントし，リスクに対応し，リスクをモニタリングしようとしているかを取り扱うリスクマネジメント戦略を立てて，組織が投資と運用に関する意思決定を行う通常使用するリスク認識を明確に，かつ透明にすることにある.

- アセスメント
  リスクのアセスメントは，組織に対する脅威またはある組織を介して他の組織または国家に向けられた脅威と，組織の内部と外部に存在する脆弱性を特定して，脅威が脆弱性を利用する場合に発生する可能性のある被害と，被害が発生する高さからリスクを判断する.

- モニタリング
  組織のリスクフレームに準拠した，一貫性のある組織全体にわたるリスク対応を示すことである.

- 対応
  リスク対応の現在の有効性を判断し，組織の情報システム，およびそれらのシステムが稼働する環境に対する変更の内，リスクに影響を及ぼす変更を特定する．そして，計画されたリスク対応が実施されていて，かつ，組織のミッション/業務機能，法律，指令，規制，ポリシー，および標準/ガイドラインから導出され跡をたどることができる情報セキュリティ要求事項が満たされているか否かを確認する.

「アセスメント」にて，対象脅威を明確にしてリスクを分析すると，その脅威が事業に与えるリスクの大きさを把握できる．そして,「アセスメント」結果に基づき「モニタリング」や「対応」を行い，リスクマネジメントのプロセスを回していく.

本論文ではリスクマネジメントを回す最初のステップである「アセスメント」に注目し，スモールスタートが可能となるリスクアセスメントを実現すべく，そのプロセスや手法を提案する.

2.3 リスクアセスメント

本論文では，図 2 に示す NIST SP800-30 のリスクアセスメントを参照にするため，そのプロセスを概説する．

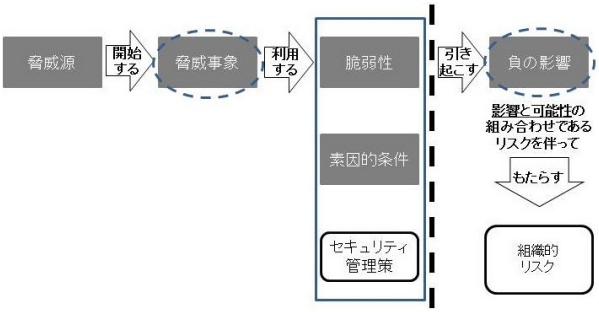

図 2: NIST SP800-30 のリスクアセスメントプロセス

リスクアセスメントでは，対象とする脅威（脅威源，脅威事象）と脆弱性，素因的条件等から，アセスメントが必要なリスク因子を定義する．リスク因子は，リスクアセスメントにおけるリスクのレベル判断を行うための入力データとなる．リスクのレベルは，リスク分析手法にリスク因子を入力して得られる負の影響の大きさである．リスク分析手法は，入力データと関係があるため，リスク因子の定義時に決定する．

3 本論文のリスクアセスメントプロセスと手法

本節では，2.3 節に基づく簡略化プロセスと，そのプロセスで用いるリスク分析の手法を提案する．このような初心者向けのリスクアセスメントに関する提案は筆者が知る限りない．

3.1 リスクアセスメントの簡略化

本簡略化プロセスでは，リスクマネジメントのプロセスを回す過程で，リスクアセスメントを強化していくことを前提とし，2.3 節に示す本来のプロセスに近づいていくように考慮する必要がある．

リスクアセスメントは，図 2 の「脆弱性」と「負の影響」の間にある縦の点線の箇所で，「リスク因子の定義」と「リスクの分析」の大きく 2 つのプロセスに分けることができる．本論文では，プロセスを簡略化し，「リスク因子の定義」と「リスクの分析」を以下のように定義する．

- リスク因子の定義
  リスク因子の定義では，まず事業に影響を及ぼす可能性のある脅威を洗い出す．図 2 を見ると，「脅威源」から脅威を洗い出すことになるが，「脅威源」は 2.1 節の用語の定義のように「脆弱性」と関係性がある．そして，「脅威源」や「脆弱性」に関する情報は，公開情報であったとしても専門家でないと類推できない情報や，公開されていない情報などがあり，情報セキュリティの知見がなければ十分に収集することが困難である．このため，本論文では「脅威事象」のみから対象とする脅威を洗い出すことにする．

  「脅威事象」に関する情報は，セキュリティ事故のニュースや，情報セキュリティ白書 [8]，業界のガイドライン等から得ることが可能である．情報収集は，各種メディアで報道された情報セキュリティの事件や事故をまとめたサイト（サイバーセキュリティ事件簿[1] 等）を閲覧し，詳細情報を得たい事件や事故を再検索すると効率的である．事件や事故の情報と，組織の事業や扱う情報資産等を照らし合わせることで，自組織でも発生しうる脅威事象を洗い出すことが可能である．

  ここで，対象脅威のリスク因子を定義するための情報も得られるが，「脅威事象」のみの情報を基にすると図 2 の本来のプロセスと比べ，対象脅威の網羅性およびリスクアセスメント結果の精度が低くなる可能性がある．このため，リスクマネジメントのプロセスを回して，リスクアセスメントを強化していくことを前提とし，リスク因子を定義する際に「脅威源」「脆弱性」「素因的条件」等の要素を順次加えながら，対象脅威の網羅性やリスクアセスメント結果の精

[1] http://www.mbsd.jp/casebook_index.html

度を高めていくことを勧める.「脅威源」や「脆弱性」を加える際には，適切な最新情報を用いることが対策脅威の網羅性やリスクアセスメント結果の精度を高くすることにつながるため，コンサルタント等の専門家の助けを得ることが望ましい.

- リスクの分析
  リスク分析では，大きく分けて，影響や発生確率を定量的または定性的に捉える 2 つの手法がある.
  - 定量的なリスク分析
    リスクの大きさは金額等の定量的な数値で表し，一般的に「影響×発生確率」によって算出する．金額換算困難な資産の評価は難しい．リスク因子は，影響を金額，発生確率をパーセント（百分率）によって特徴付ける．影響は事例が少ないと精度の高い数値を出すことが難しい．また，発生確率は変化の激しい環境だと過去の統計情報の有効性が問題となる．提案されているリスクの定量化手法 [9] でも，データの正確さが算出結果の信頼性に影響があるとしている．JNSA は個人情報漏えい事故に関する情報を収集し，想定損害賠償額算出式を示している [10].
  - 定性的なリスク分析
    リスクの大きさは，定義したリスク因子の尺度を基に表す．リスク因子は，影響や発生確率等の項目を 3〜5 段階の尺度で分類し，その分類によって特徴付ける．例えば，リスクの大きさは各項目の分類尺度の和や積で算出する．リスク因子に関しては，設定する項目数や，分類の尺度や基準などを定義する必要がある.

営業情報や技術情報等の営業秘密の消失や流出，サービス停止，風評被害等のサイバー攻撃の被害（負の影響）は金額的な評価が難しい．また，発生確率もセキュリティ事故が必ずしも公表されるわけではないことから，統計的に正確な値を把握することが困難である．加えて，日々新たな攻撃手法や脆弱性が発見されることから，過去の統計情報が必ずしも当てになるとは言えない.

このため，本論文では定性的なリスク分析を用いる．リスクの尺度は，NIST SP800-30[3] の Appendix を参照すると 5 段階に分類していることから，これに倣うものとした．また，リスク因子の項目数は，増やすと評価や算出が複雑になることから，影響と発生確率の 2 つにすることにした.

3.2 リスクポートフォリオを用いたリスクアセスメント手法

3.2.1 リスクポートフォリオ

リスクの分析では，脅威ごとの影響と発生確率から算出した結果を表に一覧として表すことが一般的である．しかし，表を用いた場合，脅威全体の状況や脅威の影響と発生確率の度合い等を把握することが容易ではない．このため，本論文では脅威のリスクを把握しやすく，リスクが変化した際にも対応しやすいように，金融分野でも使われているリスクポートフォリオを用いることにした.

リスクポートフォリオは，リスクをコントロールするために，被害の大きさと発生確率を軸として図 3 に示すように「回避」「低減」「保有」「移転」の 4 領域から構成される．以下に，4 領域に位置づけられた脅威のリスクの特徴について述べる.

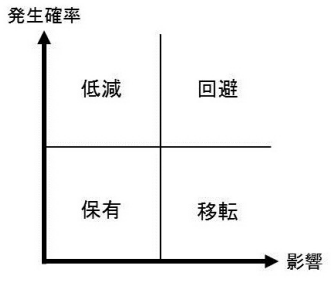

図 3: リスクポートフォリオ

- 保有
  脅威の影響が小さく，発生確率も低く，リ

スクが小さいことから新たな対策を講じる必要がない，許容可能なリスク.

- 低減
  脅威に対して対策を講じることによって，脅威の発生確率を下げた方がよいリスク．リスクを低減することで，リスクが保有可能となる.

- 移転
  脅威の影響は大きいが，発生確率が低いため，保険等の他の手段に移転した方がよいリスク．ただし，リスクをすべて移転できるとは限らない.

- 回避
  脅威の発生確率が高く，影響も大きいため，脅威発生の要因を取り除くことで，この脅威への対応を不要にする.

3.2.2 リスクポートフォリオを用いたアセスメント手順

3.2.1 節のリスクポートフォリオを用いて，以下に示す手順でリスクアセスメントを実施する.

1. 影響と発生確率の分類の定義
   リスクポートフォリオの影響と発生確率で，5 段階の分類基準を定義する．例えば，NIST SP800-30 を参照すると，「非常に高い」から「非常に低い」の 5 段階の尺度とし，各段階に対して半定量的な値や説明を付けて定義している.

2. 対象脅威の選定
   2.3 節で述べたように，「脅威事象」をもとに対象脅威を選定する．対象脅威に関する情報収集の際には，「1. 影響と発生確率の分類の定義」の判断に用いる情報も得るようにする.

3. 対象脅威のマッピング
   対象脅威の影響と発生確率を 5 段階で分類した結果を，図 4 のように 5× 5（25 マス）で表されるリスクポートフォリオの対応するマスにマッピングする.

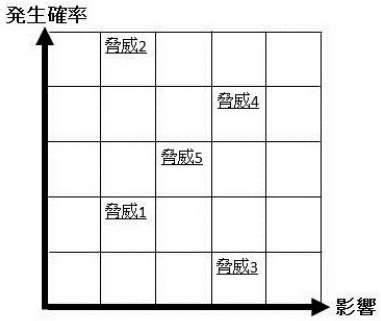

図 4: 対象脅威のマッピング

4. 対象脅威のリスクの分類
   対象脅威がマッピングされたリスクポートフォリオに対し，事業継続の観点から図 5 のように発生確率と影響に関して許容可能／許容不可能な境界に線を引いて，リスクへの対応を判断する．発生確率と影響は同じ尺度で表せないこともあり，このとき境界線は図 5 のように必ずしも直線で交わるわけではない.

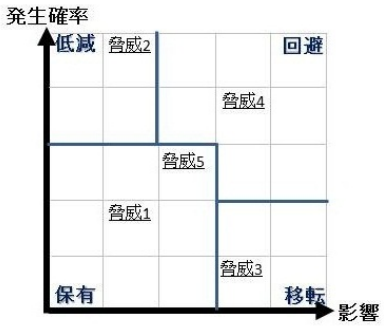

図 5: リスク判断

5. 対象脅威のリスク判断
   4 領域の対象脅威に関して，以下に基づいてリスクへの対応を判断する.

   - 「保有」の領域にある脅威は，事業に対するリスクが小さく，許容可能なリスクと判断できる．この脅威には新たな対策を講じる必要がないが，既存対策の確実な実施や，代替対策の検討が必要である.
   - 「低減」の領域にある脅威は，事業に対するリスクが比較的大きく，許容範

囲を超えるリスクと判断できる．このため，この脅威の発生確率を低くする対策を講じ，リスクを小さくする．例えば，スパムメールの添付ファイルが原因となるマルウェア感染が頻繁に発生するならば，スパムメールをフィルタリングするシステムを導入し，スパムメールを減らしてマルウェア感染確率を低減する．

ただし，脅威のリスクを把握しながらも予算等に基づく事業判断により，対策を講じないことも考えられる．

- 「移転」の領域にある脅威は，事業に対するリスクが比較的大きく，許容範囲を超えるリスクと判断できる．このため，この脅威の影響を小さくする対策を講じ，リスクを小さくする．影響を小さくする対策としては，保険の加入や他社サービスの利用等が挙げられる.「低減」と同様に，脅威のリスクを把握しながらも予算等に基づく事業判断により，対策を講じないことも考えられる．
- 「回避」の領域にある脅威は，事業に対するリスクが大きく，許容できないリスクと判断できる．このため，この脅威の発生要因を取り除くか，または，対策を講じて他の領域に移す．例えば，「回避」に自社の Web サーバからの個人情報漏えいという脅威があれば，Web サーバの運用を停止する．

4 考察

本節では，リスクポートフォリオを用いる効果について考察する．

4.1 サイバー攻撃以外の脅威とのリスク比較

サイバー攻撃の脅威に対するリスクが把握できても，脅威対策を講じるかどうかの投資判断は難しい．そこで，サイバー攻撃以外の脅威もリスクポートフォリオを用いたリスク分析を行い，サイバー攻撃とそれ以外の脅威のリスクポートフォリオを重ね合わせることを考える．複数のリスクポートフォリオを重ねることで，事業全体での脅威の関係性が把握可能となり，サイバー攻撃の脅威対策に対する投資判断しやすくなると考える．ただし，異なるポートフォリオを重ね合わせる手法が必要となる．

4.2 見える化によるリスクコミュニケーションの効果

4.2.1 専門家とのリスクコミュニケーション

リスクポートフォリオは，組織がコンサルタント等の専門家の助けを借りる際にも役立つと考える．リスクポートフォリオを用いると，組織側と専門家側で，双方の脅威に対するリスク認識の相違が一目瞭然であり（リスクポートフォリオ上で脅威が置かれたマスの位置が同じかどうか），互いのリスク認識を把握しやすい．もしリスクの認識が異なっていれば，双方で位置づけに関して話し合うことで意識を合わせることができ，両者で脅威の位置を修正できる．

4.2.2 経営層とのリスクコミュニケーション

本論文でリスクポートフォリオを用いた理由は，経験や知識が十分にないセキュリティの責任者や担当者でも，リスクを把握しやすいことにある．これは，NIST SP800-30 で示されている組織階層（図 6）の間のコミュニケーションにも役立つと考える．例えば，情報セキュリティに係るポリシや計画の承認，投資の判断等を行う第 1 層の経営層は，リスクマネジメントの経験や知識を十分に有しているとは考えづらい．リスクポートフォリオは経営戦略を立てる際に用いられることもあり，経営層に馴染みのあるリスクポートフォリオを用いて説明すると理解されやすいと考える．さらに，4.1 で述べたように，サイバー攻撃以外の脅威と比較した結果を示すことで，経営層に対しての説明力がより増すと考える．

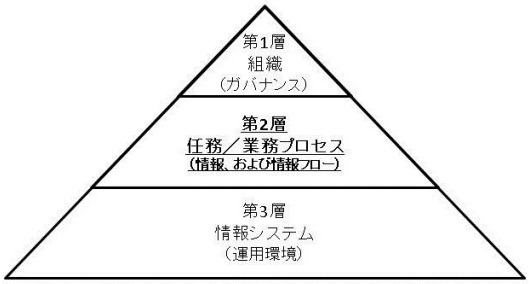

図 6: 組織図

5 まとめ

本論文では，サイバー攻撃の脅威に対するリスクをマネジメントするために，スモールスタートでプロセスを回し始めることができるリスクポートフォリオを用いたリスクアセスメントのプロセスおよび手法について提案した．提案したプロセスおよび手法は，まずはリスクマネジメントをスタートさせるものであり，初心者を対象としたものと位置付けられる．このため，リスクマネジメントを回しながらリスクアセスメントの結果をよりよくする過程において，より有効なプロセスや手法への移行が考えられる．

今後，事業内容や企業規模，情報システム等を想定し，本論文に示したプロセスを基にリスクアセスメントのロールプレイを行い，提案手法の改善や新たな課題抽出を行う．また，この際に定性的なリスク分析の具体的な分類の内容や基準についても検討する．本提案手法は，利便性向上と効率化の観点から，情報セキュリティ部門の責任者や担当者，コンサルタント等の専門家向けにツールとして提供することを想定している．このため，今後支援ツールの設計・試作を行う．

アセスメント以外のリスクマネジメントのステップ（モニタリング，対応）においても，リスクポートフォリオを用いることで，効率的で効果的なマネジメントを可能とする手法について検討していきたい．

謝辞

本論文の作成にあたり，本研究のアイディアに関してご熱心に議論に加わりコメントを頂きました，東京電機大学 勅使河原可海先生に感謝の意を表します．

参考文献

[1] NRI SecureTechnologies: 企業における情報セキュリティ実態調査 2013 第 2 版, 2014.

[2] 土井智朗，内田勝也: 情報セキュリティ意識向上に向けた効果的なリスクアセスメント手法の提案, 2008.

[3] National Institute of Standrads and Technology: NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, 2012, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf .

[4] ISO/IEC: ISO/IEC27005, Information technology - Security techniques - Information security risk management, 2011.

[5] ISO/IEC: ISO/IEC31000, Risk management, 2009.

[6] 経済産業省: 情報セキュリティガバナンス導入ガイドライン, 2009.

[7] 独立行政法人情報処理推進機構 (IPA): リスクアセスメントの実施の手引き, 2013, https://www.ipa.go.jp/files/000025325.pdf

[8] 独立行政法人情報処理推進機構 (IPA): 情報セキュリティ白書, 2014.

[9] 岡本卓馬: 情報セキュリティにおけるリスクの定量化手法, 2005.

[10] NPO 日本ネットワークセキュリティ協会 (JNSA): 2012 年情報セキュリティインシデントに関する調査報告書,2014.