Vol.2019-EIP-84 No.1
2019/6/3

金融機関におけるサイバーセキュリティの アセスメントに関する考察

小梶顯義　原田要之助　後藤厚宏†

概要：金融機関のサイバーセキュリティに関するリスクは増大しているが，そのマネジメントに関する手法や標準は確立されていない．また，国際機関，国，公的機関，利用者等から金融機関に対するサイバーセキュリティ態勢を強化する要求も高まっている．これらの状況を踏まえ，本稿では，サイバーセキュリティのリスクアセスメントの手法や動向についての研究結果を示す．また，そのうえで今後の金融機関におけるサイバーセキュリティのリスクアセスメントについて考察する．

キーワード：金融機関，サイバーセキュリティ，リスクアセスメント，ISO/IEC31000，ISO/IEC31010，ISO/IEC27014

A consideration of assessment on cyber security in financial institutions

Akiyoshi KOKAJI　Yonosuke HARADA　Atsuhiro GOTO

Abstract: Risks related to cyber security in financial institutions are increasing, but management methods and standards have not been established. In addition, there is an increasing demand from international organizations, countries, public organizations, users, etc. to strengthen cyber security systems for financial institutions. Based on these circumstances, this paper presents the research results on cyber security risk assessment methods and trends. We also consider the risk assessment of cyber security in future financial institutions.

Keywords: Financial institution, cyber security, risk management, ISO/IEC31000, ISO/IEC31010, ISO/IEC27014

1．はじめに（サイバー攻撃の特性）

防衛省・自衛隊は，サイバー攻撃の特性について，「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」 [1]において，以下の特性をあげている．

表１：サイバー攻撃の特性

多様性	攻撃の主体・手法・目的・状況が様々である
匿名性	誰が実行したかについて，隠蔽・偽装することが容易である
隠密性	被害が露見するまで防御側が攻撃の存在を察知し難いものや，情報の窃取のようにそもそも被害発生の認識すら困難なものがある
攻撃側の優位性	攻撃の手法によっては攻撃手段を入手することが容易であること，ソフトウェアの脆弱性を完全に排除することが困難であること，攻撃側は相互連接するネットワークの最も脆弱なポイントをついて攻撃すればよいこと等から，攻撃側が防御側に対して圧倒的な優位にある
抑止困難性	「懲罰的抑止」によってであれ，「拒否的抑止」によってであれ，サイバー攻撃を抑止することは容易ではない

（参考文献［1］を基に筆者作成）

2．金融情報システムの特殊性

遠藤は，「金融情報システムにおける経営戦略としてのリスクマネジメントの体系化及びその実践」 [2]にて，金融機関のシステムの特殊性として以下の４点をあげている．

①決済システムとして広い範囲のネットワークに接続しており，可用性や大量即時処理への外部からの要求度合いが高い．

②顧客の財産情報を扱うことから，機密性・完全性に対する要求度合いが高い．

③レガシーシステムの存在である．保守や開発の難易度が高い．

④情報システムの健全性について当局の監視下に置かれていること．

よって，金融機関はサイバーセキュリティのリスクアセスメントについて金融情報システムの特殊性を考慮して実施することが求められる．

3．サイバーセキュリティリスクアセスメント

現在，国内外の政府機関，民間企業，調査機関等が以下のサイバーセキュリティのアセスメントを実施している．

3-1．アセスメント手法例

①　シナリオ法(一定の前提条件・仮定に基づく損失・影響

† 情報セキュリティ大学院大学　Institutions of Information Security

評価）

英ロイズ社と米サイエンス社は，2017 年 7 月，シナリオ法による評価レポートを公表している．シナリオ法とは，一定の前提条件・仮定に基づくサイバー攻撃を想定した時の損失･影響評価であり,一般的には予想最大損失額(PML, Probable Maximum Loss）を算出して評価に用いる．

当レポートの想定シナリオ例は，以下のとおりである．

(1)クラウドインフラの制御プログラムが改竄され，無数のクラウドサーバーが停止するもの

(2)あるアナリストが電車に鞄を置き忘れ，鞄に入っていた脆弱性レポート（ある OS の全バージョンに影響を与えるもの）がダークウェブ上で売買され，サイバー攻撃が引き起こされるもの

それぞれの全世界でのリスク算定値である最大損失額は(1)で530億ドル,(2)で287億ドルと見積もられている．

シナリオ法の利点は，容易に「最悪ケース」を想定することができる点である．欠点は，前提条件・仮定の違いによる評価結果のブレが大きい点である．

② 累積超過収益率分析法（CAR 分析）

米国の経済諮問委員会は，2018 年 2 月，米国大統領経済報告 [3]において，累積超過収益率分析（以下，CAR 分析）による分析結果を公表している．CAR 分析とは，一定の前提条件・仮定に基づくサイバー攻撃による損失・影響評価であり，企業価値の損失額を評価する．

具体的には，サイバー攻撃が行われた際の企業価値の変動幅（実値）と攻撃が何もなかった場合の企業価値の変動幅（仮定値）の累積差分を算定する．

利点は，サイバー攻撃被害の定量化が難しい分野（営業秘密や戦略情報の漏洩等）での定量評価が可能という点である．

欠点は，実際に起きたサイバー攻撃を事後的に評価するものであり，また「何もなかった場合の価値の変動幅」を計量することは難しい点が挙げられる．

③ モンテカルロ法（確率論的損失評価）

国際通貨基金（IMF）は，2018 年 6 月，報告書「サイバー攻撃が金融業界に与える損失」 [4]を公表している．モンテカルロ法による Var（Value at Risk）計測は，金融業界では市場リスクの測定で用いられることが多い計測手法であり，過去のサイバー攻撃被害のデータや損失モデルに基づき，数万～数百万回のシミュレーションを繰り返すことによる確率論的損失評価である．具体的には，事象の頻度と損失金額の想定されるすべての場合を疑似的に計算機の上で再現して,その結果を統計的にまとめるものである．

評価結果は，一般に限定的なデータセットに依存するとされ，当報告書においても評価結果は「例示的な評価」であると述べている．また，特に，変化の激しい攻撃トレンドは過去のデータセットからの計測だけでは不十分と想定される．

一定の信頼区間（50%，90%，95%等）に基づき最大損失額を算出するため精緻であるが，評価結果の妥当性はデータセットとモデルに依存する点が特徴である．

従って，データセットとモデルが妥当な場合は，評価結果の妥当性も高くなる．また，妥当でない場合は，結果の妥当性も低くなる．

④ 非経済的要素による評価

これまで述べたリスクアセスメントにおける評価軸は主に経済的損失額だが，非経済的損失評価を評価軸であることが重要な場合もある．

内閣サイバーセキュリティセンター(以下，NISC）は，2018 年 7 月,「重要インフラの深刻度評価」 [5]を公表しており，そのなかで，評価対象を重要インフラサービスに限定しているものの，サービスの「持続性」「安全性」でサイバー攻撃の深刻度を評価している．

利点は，他手法には無い持続性・安全性といった観点を評価軸としている点が挙げられ，特に公共性の高い領域では有効と考えられる．

欠点は，定性評価であり定量評価をしていない点が挙げられ，他の手法との組合せが必要となる場合がある．

⑤ 簡易金額算出モデル

一般社団法人日本サイバーセキュリティイノベーション委員会(以下，JCIC)は，2018 年 9 月,「取締役会で議論するためのサイバーリスクの数値化モデル　～サイバーリスクの金額換算に関する調査」 [6]を公表している．

当調査では,「サイバーリスク指標モデル」として，サイバーリスクの損失金額換算を以下の体系で示しており，最大損害額（PML）やベンチマーク値を用いることが，日本企業の経営層がサイバーリスクを理解することに有効であるとしている．

表 2　JCIC「サイバーリスクの数値化モデル」における想定損失額

	想定損失額	内容
直接被害	1)個人情報漏えいによる金銭被害	セキュリティ事故によって個人情報が漏えいした場合の想定損害額（基礎情報価値×機微情報度×本人特定容易度×社会的責任度×事項対応評価×顧客数で算出）
	2)ビジネス停止による機会損失	サイバー攻撃に起因して社内システムや EC サイトの停止によって,業務が停止し,本来得られるはずだった売上機会の損失額.
	3)法令違反による制裁金	法規制に違反したことによる制裁金や罰金(「EU の一般データ保護規則（GDPR)」による制裁金等)

	4) 事故対応費用	影響範囲や原因を調査するための費用（フォレンジック費用），データの復旧 費用，応急処置や再発防止のためのセキュリティ強化費用等
間接被害	5) 純利益への影響	特別損失等による純利益減少額
	6) 時価総額への影響	株価下落による時価総額減少額

（JCIC「サイバーリスクの数値化モデル」に基づき筆者作成）

3-2．各アセスメント手法の有効性

ISO/IEC31010 [7]では，リスクアセスメントプロセス及びリスクアセスメント手法の有効性を以下の通り整理している．

3-2-1．リスクアセスメントのプロセス

リスクアセスメントの主なプロセスは，以下のリスク特定，リスク分析，リスク評価から構成されると定義されている．

表 3　リスクアセスメントの主なプロセス

リスク特定	リスクを発見するプロセス
リスク分析	既存の管理策の有無及び有効性を考慮して，特定したリスク事象の「影響」，「発生確率」及び「リスクレベル」を決定するプロセス
リスク評価	リスク分析で得たリスクの知見を用いて対策に関する決定を下すプロセス

（ISO/IEC31010 に基づき筆者作成）

3-2-2．リスクアセスメント手法の各プロセスにおける有効性

前述のサイバーセキュリティのリスクアセスメント手法について，各プロセス単位で有効性（各手法がそのプロセスにおいて有効がどうか）を独自に整理した．その結果は，表 4 の通りである．

表 4　サイバーセキュリティの
リスクアセスメント手法の有効性

リスクアセスメント手法	リスクアセスメントプロセス					アウトプットの性質
	リスク特定	リスク分析			リスク評価	
		影響	発生確率	リスクレベル		
シナリオ法（英ロイズ、米サイエンス）	△	◎	△	○	×	定量
累積超過収益率分析法（CAR分析）（米経済顧問委員会）	△	◎	△	○	×	定量
モンテカルロ法（IMF）	△	◎	△	○	×	定量
重要インフラの深刻度評価(NISC)	×	◎	×	○	×	定性
簡易金額算出モデル(JCIC)	×	◎	×	○	×	定量

凡例：◎：推奨，○：適用可能，×：適用不可

（筆者作成）

(注)シナリオ法，CAR 分析，モンテカルロ法のリスク特定及び発生確率は，リスクのシナリオ，モデル及び発生確率を特定されたものとして分析するため，△としている．

これらのサイバーセキュリティのリスクアセスメント手法では，リスク事象の影響の確認に重点を置いているため，リスク特定やリスク評価等では適用不可であることが分かる．

従って，金融機関は，サイバーセキュリティの後述の一般的なリスクアセスメント手法と組み合わせることが必要と考えられる．

4．一般的なリスクアセスメント

4-1. ISO/IEC31010

ISO/IEC31010 は，リスクマネジメントに関して，より技術的な視点から，ISO/IEC31000 を補完する具体的なリスクアセスメント手法をまとめたものであり，このプロセスを実施するために実際に採用できる手法を解説するものである．

このうち，IT リスクに適用可能な代表的なアセスメント技法について述べる．

①　ブレーンストーミング（非形式アプローチ）

ブレーンストーミング法は，必要な知識を有する担当者が，自由な議論をおこなうことにより，脅威，脆弱性，リスク，意思決定のための基準等を明らかにする技法である．

利点は，従来想定されていなかったリスクに対して考慮できる可能性があること，準備も含めて素早く実施できる点が挙げられる．

欠点としては，参加者の知識や経験が不十分な場合には有効な結果が得られない可能性が高いこと，参加者の知識や発想の偏りに左右されやすく，すべての潜在的なリスクが網羅されて特定されているかなど，プロセスの包括性を確認することが難しい点が挙げられる．

②　チェックリスト法

チェックリスト法は，過去のガイドラインなどの知見等によって作成された確認項目の一覧を用いて，リスクアセスメントを行う方法である．

利点は，チェックリストがうまく作成されているときには，項目を理解できれば専門知識を持たない人でも利用することができること，チェック項目を共通化することによりリスクアセスメントの結果の比較や第 3 者によるレビューが可能な点である．

欠点としては，リスクアセスメントの結果がチェックリストの網羅性に依存している点，想定外のリスクに対する考慮が難しい点が挙げられる．

③　故障木解析(FTA)

故障木解析（Fault Tree Analysis.以下,FTA）は，分析対象となる脅威を頂上対象とし，脅威の発生過程における因果結果を表現したFT（Fault Tree：故障木）と呼ばれる樹形図を用いて分析する手法である．FTAは，潜在的な原因および頂上事象までの経路を特定するとともに，各原因事象の発生確率が判明しているときに，頂上事象の発生確率を計算する定量的手法として利用される．

利点は，大規模かつ複雑な対象領域に対して，高度でかつ体系的な分析が可能である点である．

欠点としては，専門知識が必要であることおよび作業コストが大きいこと，モデルが大規模になった場合に人手で検証することが難しい点が挙げられる．

④　事業影響度分析(BIA)

事業影響度分析（Business Impact Analysis．以下,BIA）は，特定の業務プロセスの中断リスクが組織の運営にどのように影響するかを分析し，運用管理するために必要な能力を特定および定量化する手法である．BIAは，事業継続計画の策定の際に実施され，予期せぬインシデントによって主要な業務プロセスの中断を防ぐために必要な対策の検討に活用されている．

利点は，事業の中断という通常業務では想定しにくい観点から分析することにより，業務の依存関係を発見しやすい点である．

欠点としては，分析者の業務に対する理解度に依存すること，組織の動的な振舞いを分析できない可能性があること等があげられる．

⑤　詳細リスク分析アプローチ

リスクアセスメントの対象となる資産の価値（影響度），脅威の発生頻度，対策の程度（脆弱性）からリスクレベルを決定する手法である．

利点は，リスクレベルの評価尺度が定義されれば取り組み易い点，半定量的な分析結果によりリスクの順位付けもしくは比較が可能である点がある．

欠点としては，資産を全て特定することが必要となる点である．一般的な中堅企業の場合でも数千になり，機密性・完全性・可用性の３つで分析するのでかなりの手間がかかることとなる．また，分析においては高中低などの３段階で実施されることが多い．

したがって，金融機関においては，資産の数と資産の段階の設定などの制約から用いられていないことが多い．

4-2. 代表的リスクアセスメント手法の有効性

ISO/IEC31010 [7]では，リスクアセスメント手法の有効性について，表５の通り，リスクアセスメントプログラムのプロセスごとに整理している．

表５の通り，手法ごとに有効性には優劣があることが分かる．アセスメント手法を選定する場合には，各手法の有効性を踏まえて，手法を選定することが重要である．

表５　一般的なリスクアセスメント手法の有効性

リスクアセスメント手法	リスクアセスメントプログラム					アウトプットの性質
	リスク特定	リスク分析			リスク評価	
		影響	発生確率	リスクレベル		
ブレーンストーミング法	◎	×	△	×	×	定性
チェックリスト利用法	◎	×	×	×	×	定性
故障木解析（FTA）	○	×	◎	○	○	定量
事業影響度分析（BIA）	○	◎	×	○	○	定性
詳細リスク分析アプローチ	◎	◎	◎	◎	○	半定量

凡例：◎：推奨，○：適用可能，×：適用不可

（ISO/IEC31010 に基づき筆者作成）

(注)ブレーンストーミング法の発生確率は評価者の経験に依存していると考えられるため，△としている．

5. 今後の金融機関におけるサイバーセキュリティのリスクアセスメントに関する考察

5-1. 金融機関において必要となる事項

金融機関は，サイバー攻撃の特性や金融情報システムの特殊性を踏まえ，リスクアセスメントを行う必要がある．

- サイバー攻撃は１章に述べた特性から完全に防御するのは困難である．また，金融情報システムの外部性という特性，大量の顧客情報の保有から，サイバー攻撃により問題が生じた場合の影響の範囲が広範囲に及ぶため，直接的な被害額だけでなく，間接的な経営への影響も含めて想定することが重要と考えられる．
- また，レガシーシステムを保有していることから，具体的な対策を導き出せるアセスメント手法を採用することも必要と考えられる．
- 加えて，当局の監視下にあることから，社外に説明可能な客観性の高いアセスメントであることも必要と考えられる．

5-2. 金融機関におけるリスクアセスメント手法

5-2-1. サイバーセキュリティリスクアセスメント手法の活用

１章のサイバー攻撃の特性，２章の金融情報システムの特性を踏まえ，サイバーセキュリティリスクアセスメントについて，以下のとおり考える．

- シナリオ法は前提条件・仮定による評価結果のブレが大きい点，CAR分析は「何もなかった場合の価値の変動幅」を計量することは難しい点から，金融機関が活用するのは困難と考えられる．

・モンテカルロ法は，将来，事案が多くなれば，即ちデータセットが多くなれば，結果の妥当性が上がるため活用可能になると考えられるが，現状は事案が多くないため，活用は困難と考えられる．
・重要インフラの深刻度評価と簡易金額算出モデルは，リスク特定，発生確率，リスク評価はできないが，大きな制約事項は無く，金融機関にとって重要な影響特定が可能になると考えられる．

5-2-2．一般的なリスクアセスメント手法の活用

前述のとおり，サイバーセキュリティリスクアセスメント手法では，リスク特定，発生確率，リスク評価はできないので，それらが可能となる一般的なリスクアセスメント手法と組合せ実施することが有効と考えられる．

具体的には，FTA，BIA，詳細分析アプローチとの組合せが有効と考えられるが，これらの手法はアウトプットの性質が異なるため，アセスメントの目的に応じてこれらの手法を使い分けることが必要である．

また，サイバーセキュリティリスクアセスメントを完全に補完するものではないが，ブレーンストーミング法は基本レベルのリスク対策を短時間で策定したい場合，チェックリスト利用法は対策の網羅性等を一定の基準に基づき確認したい場合等に有効なツールとなると考えられる．

6. まとめと今後の研究

サイバーセキュリティリスクアセスメントのうち重要インフラの深刻度評価と簡易金額算出モデルは金融機関にとって有効なモデルと考えられる．また，一般的なリスクメント手法と組合せて活用することが必要であると考えられる．

当考察について，CISO へのヒアリング，障害事例や成功事例の研究，各種基準との比較等を通して，有効性を検証していたいと考えている．

謝辞

本研究の調査や分析にご協力いただいた，後藤研究室，藤本研究室，原田研究室の先輩同僚の皆様に謹んで感謝の意を表します．

参考文献

[1] 防衛省・自衛隊, *防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて,* 2012.

[2] 遠藤正之，*金融情報システムにおける経営戦略としてのリスクマネジメントの体系化及びその実践,* 2015.

[3] 米政府経済顧問委員会（CEA），“米国大統領経済報告,” 2018.

[4] 国際通貨基金（IMF），“サイバー攻撃 k が金融業界に与える損失,” 2018.

[5] NISC，*重要インフラの深刻度評価,* 2018.

[6] 日本サイバーセキュリティイノベーション委員会（JCIC），*取締役会で議論するためのサイバーリスクの数値化モデル,* 日本サイバーセキュリティイノベーション委員会（JCIC）, 2018.

[7] ISO/IEC, *ISO/IEC31010,* 2009.

[8] ISO/IEC, *ISO/IEC27014,* 2010.