P2M マガジン No.9, pp.56-62 (2020)

IMHO：P2M のためのリスクマネジメント手法

越島　一郎　　Ichiro KOSHIJIMA†

1. はじめに

65 歳の定年を機に昨年 8 月中旬から 42 日を掛けて、ウラジオストックからユーラシア大陸最西端のロカ岬までバイクで単独横断した。4 月から大学内の研究センター勤務となった際に、名工大勤務 10 年半で 1 日も年休を取っていなかったため 40 日休めるとの通知を頂いた。しかし、企業勤務では 19 年で年休を 220 日以上残し、大学では年休制度など気にしないお勤めをしてきた身にとって、40 日を有意義に使用する方法が思い浮かばない。ふと目に入ったのが、Ewan McGregor の「Long Way Down」[1]であった。ただ、McGregor と同じにイギリス - アフリカ大陸縦断(84 日間、24,000km 弱)は荷が重いので、よしバイクでユーラシア大陸横断をしよう！

McGregor らは用意周到で、武装強盗（民兵？）対策のトレーニングを受け、各国とのビザ取得交渉等のアドミ業務のためにスタッフまで雇っていた。当方も、プロジェクトマネジメントを専門とし、企業での業務でも大学での教育・研究でも詳細に計画を立案し、それを実行することを「善」としてきた。しかしながら、大まかなコースは決めて詳細を検討すればするほど、自分と荷物を含めると重量 350Kg 以上になるバイクに跨り 16,000km を 65 歳が走るのは無謀に見えてくる。つまり、計画を立てることが、計画から外れる状況（＝リスク）を生み出し、辞める理由を積み上げる状況となった。

そこで、当方のユーラシア大陸横断プロジェクトでは、「計画しないことを計画」した。ルートも宿も決めない。精々計画は、次の日の目的地を決めるに止めることとして、以下の OODA ループを毎日実践した。実施した結果で翌日の意思決定にフィードバックされるのは、確実に把握できるバイク・身体コンディションである。

Observe : 前方 5-600km、1 日分の情報収集（道路、天気、宿等）

Orient : 収集した情報、バイク・身体コンディションから数カ所の目的地・ルートを策定

Decide : 目的地・ルートから実行案の意思決定

Act : 行動

この結果、2 度のアクシデント（シベリアでの「野良」牛との衝突でバイク破損、ポーランドでのスリップダウンで身体負傷）はあったものの、「最適性の原理」[1]の適用により有給休暇 40 日以内で乗り切ったことになる。リスクマネジメントとしては、合格であろう。

---

[1] 最適な方策は、初期状態と初期決定がどんなものであれ、その結果得られる次の状態に関して、以降の決定が必ず最適方策になっているという性質をもつ。（wikipedia 「ベルマン方程式」より）

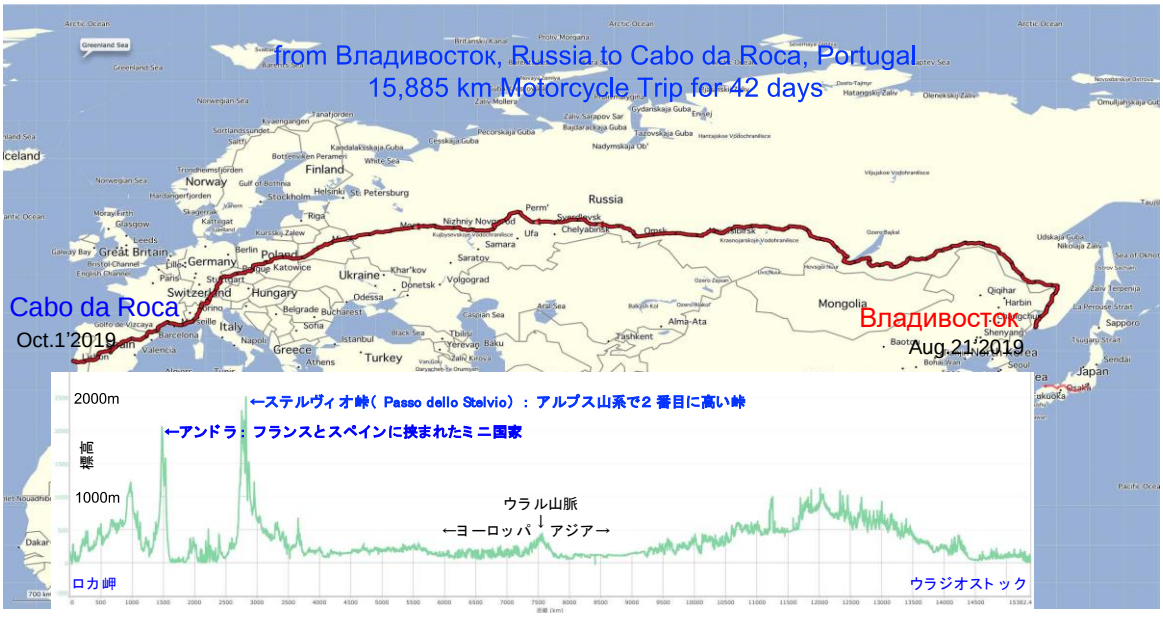

図 1-1 ウラジオストックからロカ岬走行ルート

2. リスクマネジメントに関する研究動向

濱田ら[2]は、2013 年に日本におけるリスクマネジメントに関する学術論文並びに書籍を、リスク特定手法論、リスク分析手法論、調査、フレームワーク論、導入事例に分けて総括している。（表 2-1 参照）この後に、集中的なレビューは行っていないが、CiNii にてキーワードを“プロジェクト＋リスク”、“プログラム＋リスク”として文献検索を行うと、学術誌では下記 4 件がヒットする。

1. プロジェクトとプログラムのリスクマネジメントにおける機械学習と知識創造の統合アプローチ:Machine-in-the-loop（機械参加型）知識創造プロセスの提案, 森 俊樹 , 内平 直志, 国際 P2M 学会誌 14(1), 415-435, 2019
2. プロジェクトリスクのポートフォリオ管理のための分析モデルの考察, 岩崎 祐子, 楓 森博, 渡辺 研司, 国際 P2M 学会誌 13(2), 300-308, 2019
3. プロジェクトファイナンスにおけるリスクマネジメントに関する考察, 岩崎 祐子, 渡辺 研司, 国際 P2M 学会誌 12(2), 103-118, 2018
4. 実践的リスク管理手法の検討 : 大規模 IT サービス・プログラムの実践から得た知見(<特集>プロジェクトと組織のリスク), 金子 暁信, プロジェクトマネジメント学会誌 15(4), 21-26, 2013

このため、濱田の文献レビューは網羅性があり、以下のように結論付けた課題は、未だに十分な研究がなされていないと言える。

リスク特定：モデルプロセスとプロジェクト実行中のプロセスが同様のものであれば高い効果でリスクを特定することができる。

しかし、実行中にモデルプロセスが条件変化していた場合にはチェックすべき項目や議論すべき内容は異なるため、特定したリスクに確証を持つことは難しい。

リスク分析：分析に用いたデータが主観的推定である場合もあり、これも確率シミュレーションの結果と方法に確証を持つことはできない。確率シミュレーションではモデルプロセスを明らかにしてアクティビティへの指示や使用する投入資源、投入する人材などの条件も構造化することも必要である。

フレームワーク：スキームでのリスクマネジメントの重要性が議論されており、スキームで設定した条件がシステムやサービスで変化したときのリスクマネジメントの議論が不足している。これでは 3S（スキーム、システム、サービス）で条件変化するリスクに対応していくことは難しい。

したがって、リスクマネジメントの検討課題は、1）モデルプロセスが変化した場合、2）モデルプロセスの構造化が不備な場合、3）モデルプロセスの設定条件が変化した場合への対応である。

3. これからのリスクマネジメント研究

プロジェクトやプログラムにおけるリスクマネジメント研究の前提は「目的達成は共通価値」である。如何に扱いが厄介なオーナーであっても、自身が関わるプロジェクトやプログラムの失敗を祈念することはない。（と信じたい。ただし、下町ロケットの XX 重工は別か）これは、プロジェクトやプログラム遂行に関わる企業の社会的責任とコーポレートガバナンスから当然と考えられている。

1) 企業の社会的責任：経済的健全性と倫理的健全性
   - 企業が永続的に存続するためには、企業価値を向上し、ステークホルダーを満足させる必要がある。（事業展開の必要性）
   - 企業価値を左右する要因は経済的健全性と倫理的健全性である。(健全な事業展開による価値創造：財務的・非財務的価値）
2) コーポレートガバナンス：説明責任と内部統制
   - 企業行動の原則として、関係するすべての行動について、それらのプロセスと結果の透明性を高める必要がある。（アカウンタビリテイ:説明責任）
   - 内部統制の仕組みとプロセスを通して、株主の利益を確保する。（コーポレートガバナンス:企業統治

しかし、これからの研究でこの前提は引き継がれるだろうか？

3.1 不可抗力への対応

昨今頻発する自然災害や感染症パンデミック、非合理的で強権的な政策、ストライキ、戦争・テロ等は、図 3-1 のロス・コントロール方策は効力を発揮で

きない不可抗力「予測や制御のできない外的事由」（Force Majeure）である。このような Force Majeure への対応は、２章で濱田が示したリスクマネジメントの検討課題に合致しており、十分な研究が成されていない。

このため現状では、粛々と事態を受け止めて、ロス・ファイナンシングとして Force Majeure 契約条項によって契約責任の免除を願うこととなる。しかしながら、現実には「契約責任の免除」交渉となった途端に、「目的達成は共通価値」の前提が崩れ、オーナー側とプロジェクト側で Force Majeure を認めるか否かを巡って深刻な論争が引き起こされる可能性が高い。

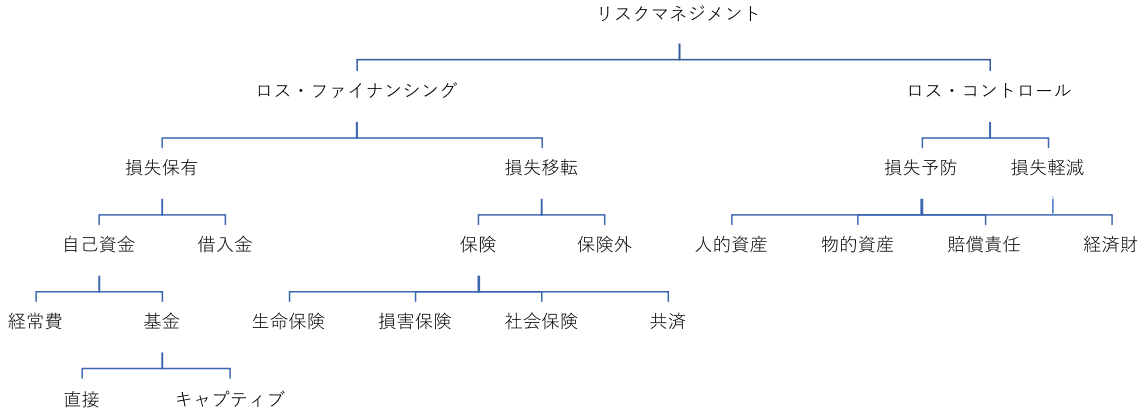

図 3-1 狭義[2]のリスクマネジメント構造[3]

このような状況に対する研究アプローチとして、以下の２つが挙げられる。

1) Risk Appetite：能動的なリスクテイクによるリスクマネジメントの在り方の検討[4]
2) OODA ループ：不確実性に対応する仕組みのプロジェクト・プログラムへの組み込み方の検討[5]

3.2 意図的不安全行為への対応

筆者が現在関わっているサイバーセキュリティにおいて、サイバー攻撃は意図的な行為であって、図 3-2 にあるように違法性の認識がある意図的な行為までも含めて検討せざるを得ない。

更に、システムが複雑系で様々な脆弱性を内包し、刻一刻と新たな攻撃方法が開発されている。したがって、新たなサイバー攻撃に予め備えることはほとんど困難である。このため、サイバーセキュリティマネジメントでは近年２つのアプローチが注目されている。

[2] 企業に悪影響を及ぼすビジネスリスクの結果としての資産損失を、リスク処理手段としてのロスコントロールとロスファイナンスによって最小の経費で資産損失を最小化することである。文献 3 より

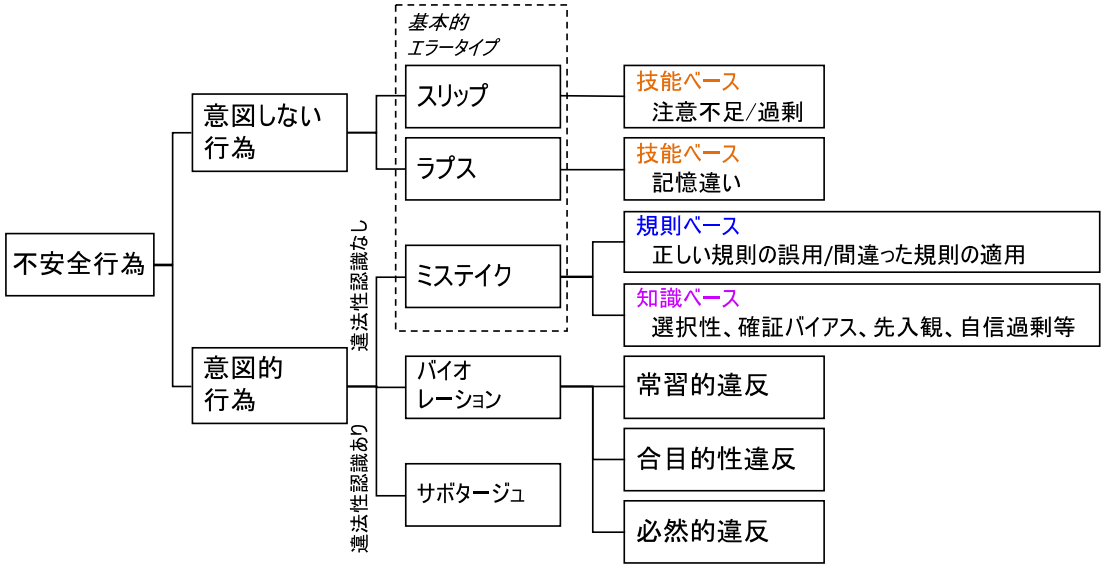

図 3-2 システムを望ましくない状態に陥れる可能性のある行為[6]

1) NIST Cybersecurity Framework (NIST-CSF) [7]：
サイバーセキュリティに対して、経営層が正しい「現状認識」を行うためのフレームワークとして提供されている。
・現場と経営層の間のコミュニケーションを改善する
・組織的なサイバーセキュリティの問題を共通の言語を使用して検討する
・組織のセキュリティの現状を評価する
・組織のセキュリティプロファイルの目標設定
・サイバーセキュリティの状況を改善するロードマップを作成できるようにする
・組織内のサイバーセキュリティリスク管理に関する意思決定を強化する

リスク管理すべきセキュリティ機能を図 3-3 に示す５つに分類（IPDRR: Identify, Protect, Detect, Respond, Recover）し、セキュリティ対策を向上させるためのカテゴリーを明確化することで、「経営リスク」を「現場での実装」へと展開している。

2) Consequence-driven Cyber informed Engineering (CCE)[9]：
従来の IT リスク評価（リスク値）＝（情報資産の価値）X（脅威ランク）X（脆弱性ランク）は、HILF[3]な事象にはそぐわない。このため、「発生してほしくない事象」からセキュリティ対策を導く手法として開発されている。

上記２つのアプローチを直接 P２M に適用することは難しいが、リスク対応機能を NIST-CSF の IPDRR に合わせて展開することや、CCE を「プロジェ

[3] HILF: High Impact Low Frequency

機能	識別子	カテゴリー
特定	ID.AM	資産管理
	ID.BE	ビジネス環境
	ID.GV	ガバナンス
	ID.RA	リスクアセスメント
	ID.RM	リスクアセスメント管理戦略
	ID.SC	サプライチェーンリスクマネジメント
防御	PR.AC	アクセス制御
	PR.AT	意識向上およびトレーニング
	PR.DS	データセキュリティ
	PR.IP	情報を保護するためのプロセスおよび手順
	PR.MA	保守
	PR.PT	保護技術
検知	DE.AE	異常とイベント
	DE.CM	セキュリティの継続的なモニタリング
	DE.DP	検知プロセス
対応	RS.RP	対応計画の作成
	RS.CO	コミュニケーション
	RS.AN	分析
	RS.MI	低減
	RS.IM	改善
復旧	RC.RP	復旧計画の作成
	RC.IM	改善
	RC.CO	コミュニケーション

図 3-3 CSF の構成（5 つの機能・23 のカテゴリー）[8]

クトとして発生してほしくない事象」からリスク対策を導出するアプローチ　として採用することは研究の価値があると考える。

表 3-1 CCE の手順

ステップ	実施事項	内容
1	経営の視点で結果事象の優先順位づけ	組織のミッション達成に必要な基幹機能・サービスを特定
2	安全の視点でシステムの分解	基幹機能・サービスの実施に影響を及ぼす重要システム・デバイス・コンポーネントの特定
3	攻撃者の視点で結果事象を元に対象の絞り込み	想定する脅威エージェントのアセスメントを元に、標的システムに特定の影響を与える方法“How”を攻撃視点で分析(サイバーキルチェーンによる分析)
4	セキュリティの視点で対策の実施	ステップ 3 で特定されたキルチェーンプロセスを止める対策を実施

4. おわりに

COVID-19 のパンデミックによって、「不可知」「不可抗力」「不作為」な事項・事象も、リスクマネジメント対象とせざるを得ない状況となっている。そのため、学会のマガジン向けとして、学術的ではなくリスクマネジメント研究に対する私見を述べた。ご参考になれば、幸いである。

参考文献

[1] Ewan McGregor et.al, Long Way Down: An Epic Journey by Motorcycle from Scotland to South Africa, Atria Books; Reprint edition, 2009

[2] 濱田佑希等, 国際 P2M 学会誌, Vol. 7, No. 2, pp.53-74, 2013

[3] 石名坂邦昭, リスク・マネジメントの理論, 白桃書房, 1994

[4] 岩崎 祐子, 渡辺 研司, プロジェクトリスクのポートフォリオ管理のための分析モデルの考察, 国際 P2M 学会誌, Vol.13, No.2, pp.300-308, 2019

[5] 加藤勇夫等, プログラムにおけるプロジェクト価値継承のための価値変換に関する基礎的考察, 国際 P2M 学会誌, Vol.13 No.1, pp.229-248, 2018

[6] 古田一雄, 長崎晋也, 安全学入門, 日科技連, 2007

[7] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[8] https://www.secure-sketch.com/blog/nist-cybersecurity-framework

[9] https://inl.gov/cce/

2020 年 8 月 3 日　受理

ハバロフスクから 690km　シベリアの何処か
森林地帯を道路が貫いている。この道を自家用車（中古日本車が殆ど）は時速 140-150km で飛ばしてゆく。大型トラックの往来が大変多く、バイクで追い越し前に進んでゆくが、ちょっと休んでいると追い越されて、追いつ追われつの鬼ごっこが 1 日続く。その内に顔見知りとなり、道を譲ってくれる様になった。
なお、幹線道路は整備されているが、外れると未舗装となり、バイクは泥だらけである。道路整備にアスファルトを使用するには、原油を余すことなく利用する産業構造が必要である。
これからは、「モノ」より ICS で「コト」の時代、シベリアの未舗装道路は無くなることは無さそうである。

ツアーの終点ポルトガルのロカ岬
左上の十字架が見える石碑には、「ここに地終わり海始まる」の詩が刻まれている。
大型の観光バスが来るたびに、中国人観光客が殺到し、石碑の前で撮影会が繰り広げられ、他の観光客は近づけない。この状況から、スペインで COVID-19 が大流行した理由は、直ぐに思い至る。

この地に至るまで 11 か国を通過したが、日本人を見たのはベラルーシのミール城だけであった。一時期、世界を席巻した日本人団体客は何処へ行ったのだろうか？