2024 年度冬期
グラデュエーションペーパー
予稿

題　　目
リスクファイナンス視点を取り入れた組込ソフトウェアの保守ビジネスの提案

技術経営論文	ビジネス企画提案

学籍番号	8823204	氏名	五十嵐 亮

教　　員	
主査	加藤 晃 教授
審査委員（担当）	青木 英彦 教授

東京理科大学大学院 経営学研究科 技術経営専攻

「リスクファイナンス視点を取り入れた組込ソフトウェアの保守ビジネスの提案」

目次

1. はじめに

筆者は組込ソフトウェアベンダーで業務をしている。近年、サイバー攻撃の対象は IT レイヤーから IoT 機器のファームウェアへと拡大しており、その脆弱性を悪用した攻撃が増加している。2018 年に報告された「Meltdown」や「Spectre」は、CPU レベルの脆弱性を突いたもので、従来のセキュリティ対策の枠組みを超えるものであった。これにより、ファームウェアによる迅速な対応が求められた。実際にはそのような脆弱性よりも優先的に対応すべきセキュリティリスクは存在しているものの、多くの企業で保守がコスト削減の対象とされ、十分な備えが行われていない現状がある。加えて、「ソフトウェア部品表（SBOM）」や欧州の「サイバーレジリエンス法（CRA）」の施行により、ソフトウェアの透明性や保守の重要性がさらに高まる可能性が高い。これらの背景から、組込ソフトウェアの保守体制を強化し、能動的なセキュリティ対策を取ることが、企業の競争力維持とリスク低減の鍵となると考えている。本研究では、組込ソフトウェアを特定のハードウェアを制御する専用ソフトウェア、リスクファイナンスを財務的影響に対応する戦略的手法と定義する。これらを基に、サイバーリスクへの効果的な対応と持続可能な保守モデルの構築を目指すものである。

2. 研究の問いと研究手法

組込ソフトウェアの保守に関する重要性は、Imanol Mugarza（2020）の研究において強調されている。この研究では、産業用 IoT システムの長寿命性に伴い、ソフトウェアの信頼性低下と、それを補う継続的な更新の必要性が示されている。本研究はこれに基づき、特に日本国内でのセキュリティパッチ適用率が著しく低い現状に焦点を当てる。この背景には、企業が投資する保守費用に対する効果が不明確であることが大きな要因であると考えた。

研究仮説

保守投資が進まない要因として、脆弱性が放置された場合の損失リスクの不明確さ、パッチ適用の具体的な効果の可視化不足、迅速な対応の経済的利点の理解不足が挙げられる。本研究では、これらを克服するために価値基準の明確化が必要であると仮説付け、以下のアプローチで検証を行う。

研究手法

① 損失リスクの定量化
保守不足によって生じるリスクや損失額を定量的に可視化に焦点を当て、具体的な事例を分析する。また、迅速なパッチ適用による損失低減額効果にも焦点を当てる。

② 修正ログ分析
オープンソースソフトウェア（OSS）の更新履歴を対象にテキストマイニングを実施

し、セキュリティパッチの割合や内容を把握する。この分析により、保守活動がセキュリティリスクの低減にどの程度寄与しているかを示す。

③　現状実態調査

脆弱性の検出数とサイバー攻撃の頻度との関係を市場環境の指標として用い、損失リスクの定量化事例の公表時期や OSS の修正傾向を時系列で照らし合わせることで、①と②の分析結果の影響度を評価する。

3. 分析結果

ソフトウェア保守の価値基準の明確化

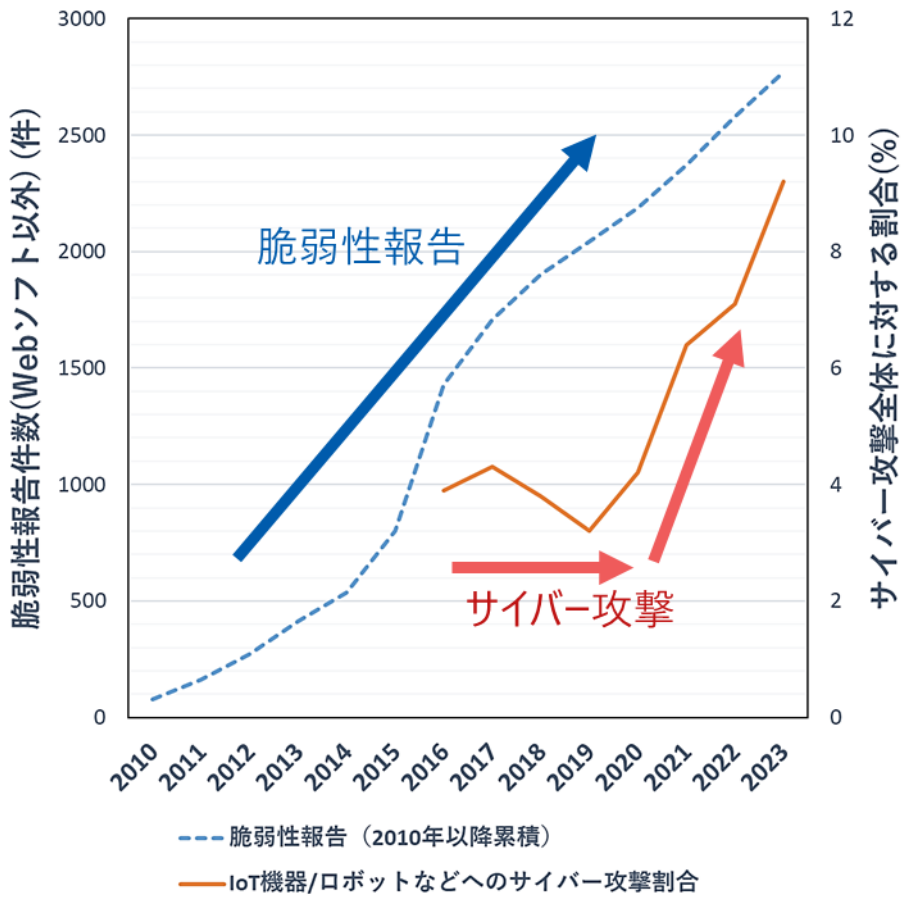
サイバー攻撃の損失額を定量化するための分析では、日本国内外で先行する複数のリスク評価モデルを参考にした。国内では「サイバーリスク指標モデル」（JCIC, 2018）として、14 項目の要素に基づき損失額を定量化する方法を提供している。これにより、企業は個人情報漏洩や業務停止の影響を金額で把握できるようになり、経営層がリスクを議論するための基盤を提供している。さらに、先行研究では「サイバーインシデントの損害発生モデルシミュレータによるサイバーリスク評価手法の提案」（磯部ら, 2018）において、シミュレーション手法が提案されており、具体例としてセキュリティパッチ適用間隔を 30 日と 60 日で比較した結果、損失額が 15%～17%削減されることが示された。

組込ソフトウェア製品の更新傾向

GitHub 上で公開されている OSS の修正履歴を分析した結果、プロジェクト開始後約 10 年を経過すると、セキュリティ強化や機能改善を示す特徴語の出現頻度が一様に増加する傾向が確認された。特に、セキュリティパッチの適用頻度は、新たな脆弱性に対応するための重要な活動として位置づけられ、プロジェクトの成熟度と密接に関連していることが明らかになった。こうした分析から、組込ソフトウェア製品においても、長期的な保守計画が必要であり、継続的な更新を通じて競争力を維持することが可能であると結論づけている。

現状分析

サイバー攻撃による損失額の推定シミュレーションや脆弱性への迅速な対応が損失額の低減効果が定量的に示した先行研究の公表は 2018 年に行われていることから、2018 年以降、保守投資効果が定量的に評価することが可能になっていることが示されている。そこで、2018 年以降の現状分析を行ったところ、国内の脆弱性報告件数は過去数年間で純増している一方で、IoT 機器を狙ったサイバー攻撃は急増している。IoT 機器の多くは、長期間の運用を想定して設計されているが、更新が容易でないため、放置された脆弱性を標的とした攻撃の増加が主な要因として考えられる。



出所：JPCERT、JIPDEC のデータを基に筆者作成

図 1　脆弱性報告とサイバー攻撃割合統計

4. 考察と新たなアプローチ

分析結果を通じて、組込ソフトウェア保守の課題に対して、単なる費用対効果の視点を超え、多角的な評価と新たなアプローチの必要性を明らかにした。すなわち、保守サービスの価値基準を明確化するだけでは、企業が保守サービスを活用しサイバー攻撃のリスクを低減する活動が推進されないことが示唆された。特に企業が保守サービスを活用したファームウェアの更新をためらう背景には、費用対効果だけでなく、技術的制約や心理的な阻害要因が強いことが見えてきた。

サイバー保険を活用したリスク移転の可能性

サイバー保険は、企業が直面するセキュリティリスクを経済的に軽減する有効な手段として注目される。CCDS のサーティフィケーションプログラム（CCDS, 2019）の事例では、保険契約を通じてセキュリティ基準を満たす製品が市場で選ばれやすくなり、結果としてセキュリティ対策が促進されることを目指している。このようなリスクファイナンスの活用は、保守活動への投資の一環として企業のリスク軽減戦略を補完する考え方である。

保守活動の心理的抵抗要素の低減

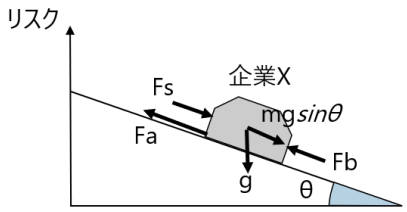
ゼミでの議論から、保守活動の実施が阻害される理由として「手間」や「更新後の不安定性への懸念」が挙げられた。このような心理的障壁は、正常性バイアスが働くことで更新の必要性を過小評価する傾向を助長する。この課題に対処するためには、「更新プロセスの簡略化」「更新後のリスクを最小化する仕組みの提供」および「重要性の啓発」が重要である。

外部環境の変化に応じた対応

欧州のサイバーレジリエンス法（CRA）や日本の JC-STAR 制度（IPA, 2024）など、セキュリティに関する規制の強化は、企業にとって外部圧力として機能する。しかし、それと同時に企業内部の抵抗要素も顕在化しており、これを克服する取り組みが必要である。

組込ソフトウェア保守の坂道モデル

本研究では、組込ソフトウェア保守の動態を説明するための「組込ソフトウェア保守の坂道モデル」を提案する。このモデルでは、5 フォースモデルにより競争環境に存在する「力」を特定し、PEST 分析により外部環境を「斜面の角度」、市場要求を「重力」、企業内部の要因を「摩擦力」として表現し、ニュートンの運動法則を適用した可視化方法を提案とする。例えば、規制強化は斜面の角度を大きくし、保守活動を促進する力として働くが、一方で摩擦力が強い場合は、活動が停滞する可能性があるというものである。



PEST分析による売り手への後押し要素が増えるほどθは90°に近づく

Fs + mg$sin\theta$ ＞ Fb + Fa　：右に動く →　保守サービスを活用する
Fs ＜ Fb + Fa – mg$sin\theta$ ：左に動く →　保守サービスを活用しない

要素	意味
X	企業の意思決定
m	企業Xの判断力
Fs	売り手からの利用促進 保守必要とする圧力
Fb	買い手のモチベーション 保守不要とする圧力
Fa	保守利用の抵抗力
θ	PEST分析の傾向 売り手後押しなら ＋ 買い手後押しなら －
g	市場要求

出所：筆者作成

図 2　組込ソフトウェア保守の坂道モデル

5. ビジネスモデルの提案

組込ソフトウェア保守の現状課題を解決するため、新たなビジネスモデルの提案を試みた。従来のビジネスモデルが「コストと対価」の 1 対 1 の構造に留まり、短期的な価値に偏る点や、更新作業への心理的・実務的な抵抗が保守活動を妨げる課題の存在が明らかでありこれらの課題を克服するため、以下の 2 つの主要要素を含むモデルを提案する。

1)　リスクファイナンスの導入

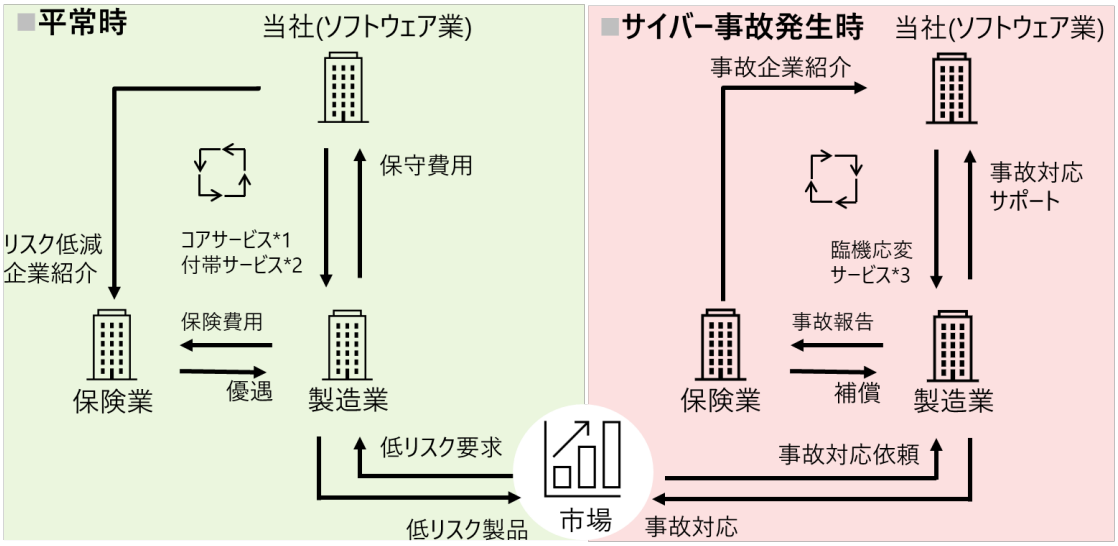
新たなモデルでは、保守サービスにリスクファイナンスの概念を取り入れ、サイバー保険を活用する。具体的には、ソフトウェア保守を積極的に実施する企業を「リスクの低い顧客」として保険料を優遇できる仕組みを設ける。このモデルにより、保険会社はリスクの低い顧客を獲得でき、製造業は保険料の軽減とセキュリティ向上の両方を実現できる。さらに、サイバー保険の優遇措置を通じて、保守サービスの利用を促進するインセンティブを提供する。

2)　抵抗を軽減するためのサービス設計

保守活動への抵抗を軽減するため、心理的・実務的障壁に対応する具体的なサービスを設計した。ノードグレン(Nordgren, 2023)が述べる「惰性対策」、「労力削減」、「感情的障壁」、「心理的反発の軽減」への対応したサービスを提供し、利用者の抵抗を取り除くことに重点を置いている。

B2B プログラムの提案

本プログラムを通じ、製造業は保守サービス利用により保険料を軽減でき、ソフトウェアベンダーは保守活動の収益基盤を拡大できる。一方、保険会社は低リスク顧客を増やすことで、収益性と持続可能性を向上させる。つまり、このプログラムにより、保険業界、製造業、ソフトウェア業界がそれぞれ利益を享受できる「Win-win-wins」の関係を構築する。

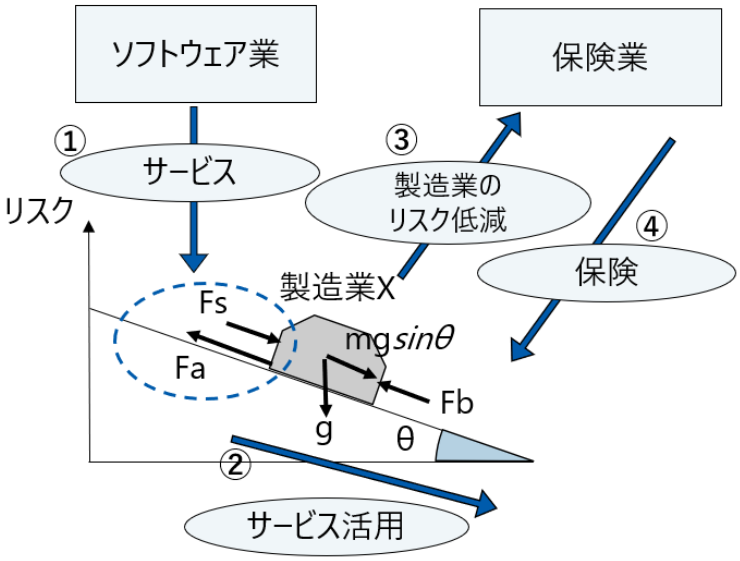


出所：筆者作成

図 3 B2B プログラム

本プログラムは、「組込ソフトウェア保守の坂道モデル」を活用しており、その関係性を図 4 に示すように視覚化する。このモデルに基づき、ソフトウェア企業が提供する保守サービスは、製造業が直面する保守活用上の障壁を効果的に低減する。このプロセスにより、製造業は市場の要求に迅速かつ円滑に対応できるようになり、「坂道を滑るように」保守サービスを活用したリスク低減活動を推進することが可能となる。

具体的には、まず、ソフトウェア企業が提供する保守サービスにより、脆弱性対策のパッチに関する情報収集と適用判断が迅速かつ適切に行われる（図 4 中①）。次に、これが製造業における保守サービスの利用を促進し、持続的なセキュリティパッチの適用を可能にする（図 4 中②）。このプロセスにより、製造業のサイバーリスクが低減されるという成果が得られる（図 4 中③）。さらに、リスク低減が進んだとしても、潜在的なリスクに備えるためのリスク転嫁手段としてサイバー保険の重要性は依然として高いものの、リスクが低減された企業に対しては保険料の引き下げが可能となる（図 4 中④）。これにより、製造業は低コストでサイバー保険に加入でき、保険会社は低リスク顧客の獲得を通じて利益を拡大することができる。B2B プログラムを通じて、保守活動とサイバーリスク管理が相互に補完し合い、持続可能なセキュリティエコシステムの構築が可能であることを提案する。



出所：筆者作成

図 4　ビジネス企画提案と組込ソフトウェア保守の坂道モデルの関係

6. まとめと今後の課題

本研究では、ファームウェア更新が十分に行われない要因を分析し、その改善策を提案した。過去の事例や OSS 更新履歴の調査により、ソフトウェア保守の必要性が定量的に示されている一方で、更新の遅延がサイバー攻撃の標的となる現状を確認した。

さらに、5 フォースモデルや PEST 分析を行うことで、更新を阻害する「抵抗要素」をニュートンの運動法則を用いた可視化モデルで明確化した。本モデルは、製造業の保守活動を円滑化する方法を視覚的に示す一方、抵抗要素の具体的低減手法や実証事例の不足が今後の課題として残されている。

分析した課題を踏まえ、製造業、ソフトウェア業、保険業をつなぐ新たなビジネスモデルを提案した。本モデルはリスクファイナンスや多面的インセンティブを組み込み、ファームウェア更新を促進する仕組みを構築している。この提案は、SBOM や国際的なセキュリティ規制と密接に関連し、今後の進展にも柔軟に対応できる可能性を示唆している。

今後は、提案モデルの定量的検証や実証研究を進め、効果の裏付けと課題の特定を行う必要がある。また、業界全体を巻き込むアライアンス形成の推進や、その実効性を評価するプロセスも重要である。本研究の成果が、組込ソフトウェア保守の課題解決と持続可能なセキュリティ向上に寄与することを期待している。

参考文献

European Commission. (2024). EU cyber resilience act. *European Commission*. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Mugarza, I., Flores, J. L., & Montero, J. L. (2020). Security issues and software updates management in the industrial Internet of Things (IIoT) era.

JCIC. (2018). 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. https://www.j-cic.com/pdf/report/QuantifyingCyberRiskSurvey-20180919(JP).pdf

Cusumano, M. A. (2004). ソフトウェア企業の競争戦略.

磯部義明, 藤田淳也, 上脇正, 中畑昌也, 末岡正嗣, 藤井裕之, & 落合正人. (2018). サイバーインシデントの損害発生モデルシミュレータによるサイバーリスク評価手法の提案.

教学 大介. (2021). サイバー保険の開発と日本企業のセキュリティ実態.

Porter, M. E. (2018). [新版]競争戦略論 I.

Nordgren, L., & Schonthal, D. (2023). 変化を嫌う人を動かす: 魅力的な提案が受け入れられない 4 つの理由.

加藤 晃. (2018). CFO 視点で考えるリスクファイナンス: 顧客本位のコンサルティングセールス.

諏訪 良武. (2009). 顧客はサービスを買っている: 顧客満足向上の鍵を握る事前期待のマネジメント.

梶浦敏範/佐藤徳之/CRMJ 研究会. (2023), サイバーリスクマネジメントの強化書 経団連「サイバーリスクハンドブック」実践の手引き