The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System (2015)

サプライチェーン管理システムへのサイバー攻撃を軽減するための COBIT5 情報セキュリティフレームワークの有効性

Mark Wolden, Raul Valverde, Malleswara Talla

5J 05 f21012 岩﨑大輝

用語

- **ERP**(Enterprise Resources Planning): 企業内に散在している「ヒト」「モノ」「カネ」「情報」といった経営資源を一元管理し、迅速な意思決定のもとでそれらを最適配置・最適配分していく手法。ERPを実現する基幹系情報システムが企業の経営戦略や戦術の一翼を担っている。
- **SCMS**(Supply Chain Management System): サプライチェーン全体のプロセス（調達、生産、在庫、物流、販売など）を統合的に管理・最適化するシステムであり、サプライチェーンマネジメントの実行を支える中核的なツール。

つまり、
ERPで企業全体の情報を一元化し、
SCMSがそれをもとに効率的なサプライチェーン運用を実現させる

例: SAP ERPとSAP SCM、 Oracle ERPとOracle SCM Cloud など

用語

情報セキュリティフレームワーク: 組織が情報資産を保護し、セキュリティリスクを管理するための指針、標準、ベストプラクティスをまとめたもの。組織がセキュリティ対策を計画、実装、運用、監視、改善していく上での枠組みとなる。

- ISO/IEC 27000シリーズ: 情報セキュリティマネジメントシステム(ISMS)に関する国際規格群。特にISO/IEC 27001は、ISMSの要求事項を定めており、認証取得の対象となる。
- COBIT(Control Objectives for Information and related Technology): 事業体が業務で取り扱うITシステムの導入や運用、管理などを適切に行うIT統制の実践的な指針を定めたフレームワーク。
- PCI DSS(Payment Card Industry Data Security Standard): クレジットカード情報を扱うすべての組織(ECサイト、小売店、決済代行会社など)が守るべきセキュリティ要件をまとめている。

0. 概要

近年、サイバー攻撃やマルウェア攻撃は、多くの組織にとって大きな脅威となっている。ERPや管理向けのアプリケーションには、セキュリティの隙間が残ることがあり、サプライチェーン管理システム(SCMS)も同様に、情報セキュリティフレームワークが必要不可欠である。

本研究では、**SCMSに対するサイバー攻撃のリスク低減におけるCOBIT5 情報セキュリティフレームワークの実装効果**を調査した。

情報システムや組織の管理者に向けてアンケートを実施した結果、セキュリティをさらに強化したことが示された。加えて、ERPシステムに導入することが組織にとって有益であることも分かった。

1. はじめに

今日の競争が激化する市場において、サプライチェーンのパートナー間で情報を安全に共有することは重要である。また、情報共有はプライチェーンの有効な機能に不可欠である。(Valverde & Saade 2015)

しかし、システムとしてのサプライチェーン管理システム(SCMS)は悪意ある攻撃の標的になりやすく、運用に必要なセキュリティを保証するためには機密性の確保が求められる。

本論文では、サプライチェーンの脆弱性と柔軟性に注目し、セキュリティフレームワークCOBIT 5がサイバー攻撃の削減においてどれだけ効果的かを評価する。

2. サプライチェーンにおけるセキュリティの管理

2.1 フレームワーク

サプライチェーンのセキュリティにおける構成要素:

- 設計 (design)
- 構造 (structure)
- セキュリティ (security)

これらの要素は脆弱性が発生するリスクに影響するため、企業は設計と構造のバランスをとりつつ、セキュリティを強化する必要がある。セキュリティをビジネス戦略に組み込むことで、最適なバランスを決めやすくなる。

2.2 サプライチェーン設計と構造のリスク軽減

リスク管理における主要な2つのアプローチとして、以下が挙げられる。

レジリエンス(Resilience): 予期せぬ中断や障害が発生したときに、それに対応し、迅速に回復する組織の能力を指す。サプライチェーンにおけるレジリエンスは、事前に中断を想定し、復旧のための準備や柔軟な設計をしておくことが重要である。そのために、他のサプライヤーへの切り替えや代替手段の確保などを行う。

アジャイル(Agile): 急な変化や混乱に素早く、柔軟に対応できる能力を指す。これは予防的な戦略であり、将来の変化に備えて即応性・可視性・迅速性を高めておくことが重視される。その手段として、在庫のバッファ確保、信頼性の高いロジスティックシステムを持つこと、サプライヤーとの情報共有などが挙げられる。

2.3 セキュリティ強化対策

2.3.1 対策

1. 内部に対するセキュリティ対策
    - 監視カメラや周囲を囲うフェンスの設置
    - 企業拠点への立ち入りに際して、社員の付き添いを求める
2. 分析
   現在の状態や将来起こりうるリスクの要因に関する評価を行う
   → リスク源に対する脆弱性への対策が明確になる

最終的には、セキュリティ強化対策の柱に位置づけられる可視性によってより正確な情報が生成され、脆弱性の軽減に役立つ。

2.3 セキュリティ強化対策

2.3.2 予防的および反応的対策

ここで取り上げた多くの対策は、予防的性格を持っている。
例: 物理的セキュリティ、人的リソースの管理など

一方で、セキュリティプランは主に反応的性質を持っており、インシデントが発生した後の対応策として機能する。

2.3.3 監査

企業において、実施されているセキュリティ対策の適切性を評価する。

- 脆弱性を予防するために適切な対策が取られているかを確認。
- 監査を実施すること自体が予防策となり、何か問題が発生した後に活用できる。

2.4 サプライチェーンにおける脆弱性

ある研究によると、現在のサプライチェーンにおける効率重視の原則が、かえって非常に脆弱なチェーンを生み出していることが示されている。(Stephens and Valverde 2013)

企業は脆弱性を低減するために、様々な手法を採用している。

- サプライチェーンの構造と設計調整することで脆弱性を減らすリストラクチャリングやリエンジニアリングが行われている。

リストラクチャリング(Restructuring): サプライチェーン全体やその一部の構造・設計を根本的に見直し、再構築すること。

リエンジニアリング(Reengineering): 業務プロセスそのものを抜本的に見直すこと。

2.4 サプライチェーンにおける脆弱性

分析ツールの導入

将来発生するインシデントへの対処能力を高めることによって、サプライチェーンの大規模な中断に対応することができるようになる。

- 取引内容を分析するツール(Kraus, Valverde 2014)
  サプライチェーンの取引データを分析することで、不正の兆候を検出し、リスクを軽減することを目的としている。

つまり、サプライチェーンにおける脆弱性は、適切な分析ツールの導入によって緩和することができる。

2.5 COBIT フレームワーク

COBITは、次の4つのドメインから構成される。

- 計画と組織 (Plan and Organize: PO)
- 取得と導入 (Acquire and Implement: AI)
- 提供とサポート (Deliver and Support: DS)
- 監視と評価 (Monitor and Evaluate: ME)

それぞれのドメインには異なる管理項目(コントロール)が存在し、組織は、自社のニーズに応じて特定のコントロールだけを取り入れることもできる。COBITのコントロールは、ISO 27000シリーズのようなセキュリティ標準と組み合わせて活用されることが多い。

このようにして、セキュリティ管理の最大化が図られている。

3. 調査手法

量的アプローチと**質的アプローチ**を併用する方法が採用された。
(この組み合わせは、ネットワークの完全性、侵入検知と監視、物理的セキュリティに関する問題に対して、関係者の認識や意見を幅広く把握するために適していると考えられた。)

量的アプローチ: 数値化されたデータを統計的に分析し、一般化や予測を行うこと。
質的アプローチ: 人々の感情や経験、価値観など、数値化しにくい情報を収集・分析すること。

3. 調査手法

サードパーティERPツールセットの管理負荷や、ERPのロールベースアーキテクチャと組織のセキュリティフレームワーク管理システムとの関係と統合についても調査対象とされた。併せて、COBIT5の信頼性、データ監査証跡、プロセス文書化についても検討が行われた。

監査証跡: 情報システムが行なった処理内容や、処理対象や処理過程のデータ、利用者が行なった操作などを時系列にそのまま記録したデータのこと。システム監査の際に処理が適切に実施されたかどうかを確認するための基礎資料となる。

3. 調査手法

研究者は、演繹的アプローチと帰納的アプローチの双方を用いて、研究の目標と目的を構造化し、実施した。また、複数の調査手法や設計哲学を使用することで、調査の理解が深まるため、本研究でも三角測量手法が採用された。そのため、調査技法としてアンケート調査が利用された。

この研究は、イギリスに本社を置く単一の企業を対象とするケーススタディアプローチで実施された。

ケーススタディ: 現実に起こった具体的事例を分析、検討し、その積み重ねによって帰納的に一般的な原理、法則を引き出す研究法。事例研究。

3. 調査手法

対象を一社に絞る理由:

- 調査回答率を高める
- COBIT 5を活用している企業であった

単一ケーススタディには一般化に限界があるがものの、情報システム研究においては単一事例でも有用な結果が得られることが過去の文献でも示されている。(Valverde, Toleman, and Cater-Steel 2011, Valverde 2008)

対象者の選定は、COBIT 5技術を使ってサプライチェーンセキュリティを担保している組織の社員および管理職から行われた。調査サンプルは、ケーススタディ企業のさまざまな拠点から無作為に選ばれた115名の回答者で構成された。回答者は、サプライチェーン管理に関わるシステムを実際に使用していることを条件に選ばれた。これら115名の回答により、COBIT 5の効果が評価された。

3. 調査手法

アンケートは6つのグループに分類され、全21問で構成。

1. 規則、責任、ポリシーの管理
2. ロールベースシステムのセキュリティへの影響
3. サードパーティERPツールセットの管理負荷
4. ERPロールベースアーキテクチャとセキュリティフレームワーク管理システム(COBIT 5)の統合関係
5. データ監査証跡
6. プロセス文書化

各設問には、「True」「False」「Mostly True」「Don't know」のいずれかで回答する形式が採用された。

4. 結果と考察

4.1 結果

4.1.1 規則、責任、ポリシーの管理

設問	回答
Q.1 適切なセキュリティポリシー、ガイドライン、または手順が確立されているか。	大多数が True
Q.2 既存のセキュリティポリシーやガイドライン、手順は、何が許可され、何が禁止されているかを明確に示しているか。	60%が Mostly True
Q.3 アクセス権限が付与される前に、関連する法律、セキュリティポリシーおよび手順に関するユーザーの義務が通知されているか。	ほとんどが True
Q.4 組織内に情報技術の「適正使用ポリシー」が存在するかを知っているか。	93.3%が Mostly True

4.1 結果

4.1.1 規則、責任、ポリシーの管理

設問	回答
Q.5 役職カテゴリーに基づいてロールを関連付けることができるか。	60%が Mostly True, 33.33%が True
Q.6 デフォルトロールを設定できるか。	66.7%が True
Q.7 あるロールに特定フィールドやテーブル、フォームへのアクセス権を付与した場合の影響を示すレポートが提供されているか。	ほとんどが Mostly True

4.1 結果

4.1.2 ロールベースシステムのセキュリティへの影響

設問	回答
Q.8 特定のデータへのアクセス権が、本当に必要な物のみに制限されているか。	50%が Mostly True, 42.8%が True
Q.9 ユーザのアクセス権を比較的簡単に無効化できるか。	過半数がTrue
Q.10 不正なアクセスや活動を検出する侵入監視システムが設置されているか。 Q.11 サーバールームなどの重要な施設への物理的アクセスは制限されているか。 Q.12 すべての情報システムへのアクセス、ユーザごとに個別に認証されているか。	大部分が True

4.1 結果

4.1.3 サードパーティERPツールセットの管理負荷

設問	回答
Q.13 ベンダー推奨のサードパーティ製品やレポートツールが、ERPに統合されたロールベースアーキテクチャを持っているか。	主に Mostly True, Don’t know
Q.14 管理者がユーザのアクセス権をウェブベースツールで確認できるか。	多数が True
Q.15 ERPシステムへのアクセス権付与と無効化を一元管理できるツールがあるか。	多数が Don’t know
Q.16 ERPシステムおよび関連サードパーティ製品のパスワード変更ポリシーを組織のセキュリティ管理システムから管理できるか。	21.43%が False または Don’t know

4.1 結果

4.1.4 パスワードとPIN認証 & 4.1.5 ガバナンス文書化

設問	回答
Q.17 強力で複雑なパスワードポリシーが強制されているか。	64.29%が True
Q.18 RSAトークンなどの二要素認証が強制されているか。	42.86%が True
Q.19 セキュリティ管理プロセスは文書化されているか。 Q.20 セキュリティ違反やインシデントに関する正式な報告手順が定められているか。	Mostly True が最も多い
Q.21 情報セキュリティ関連の役割と責任は正式に文書化されているか。	Mostly True と True がほぼ同数であった

4.2 考察

ケーススタディの結果は、規則、責任、ポリシーの適切な管理によって、COBIT 5の実装が効果的に行われ、SCMSに対するサイバー攻撃を防止・軽減できることを示した。関連文献でも示されているように、サプライチェーン管理には多数のリスクが伴うため、セキュリティ管理ツールが不可欠である。

経営陣

この研究では、経営陣の姿勢がセキュリティシステムの効果に大きな影響を与えることが明らかになった。トップマネジメントは、COBIT 5の導入に必要なリソースを投入する責任を負っており、情報セキュリティに関する意思決定の承認も行う。

4.2 考察

中間管理層

管理者が情報セキュリティプログラムを積極的に支援し、ルールの施行と一貫性を保つ意思を持つ事が、情報セキュリティフレームワークの実装効果に直接的な影響を及ぼすことが示された。ある研究でも、中間管理層が情報セキュリティフレームワークの有効性に最も影響を与える存在であると指摘している。(Ramachandranら, 2008)

階層構造

組織内部の階層構造も、情報セキュリティシステムの有効性を左右する重要な要素であることが示された。組織内の階層は、責任の所在を明確にし、誰がどの程度セキュリティに関する決定に関与するかを定める。これにより、情報システムセキュリティフレームワークの実施が円滑に進められる。こうした階層と効果の関係については、システムの分散度や構造がその有効性に影響を与えることが示されている。(Siponen, 2000)

4.2 考察

ERPシステム

情報セキュリティの有効性は、組織メンバーの意識にも依存している。経営陣は、セキュリティ対策の限界、能力、対抗措置について、組織メンバーに対して明確に伝達する責任を負っている。

従業員は、自社の情報システムセキュリティフレームワークを理解し、その重要性を認識するとともに、情報システムを使用・運用する際の行動がもたらす影響についても自覚してもらう必要がある。情報セキュリティに対する意識が、システム手順、技術、ポリシーの理解と運用に不可欠であると指摘されている。(Siponen, 2000)

4.2 考察

情報セキュリティ意識

手順や規則の遵守度合いには、個人差が生じる。

今回のケーススタディでは、従業員の多くが情報システムプログラムについて認識していた一方で、プログラムの目的や理念に対する理解や信念にバラつきがあった。セキュリティプログラムの成功には、単に存在を知っているだけでなく、それが個々の価値観や理解と一致していることが重要。

組織は、このような内部要因を深く探る必要があり、そうすることで情報システムセキュリティフレームワークの実装効果をさらに高めることができる。

5. 結論

ケーススタディの調査結果

COBIT 5情報システムセキュリティフレームワークの導入が、企業アプリケーションのセキュリティを強化し、SCMSに対するサイバー攻撃のリスクを効果的に軽減できることを明確に示した。COBIT 5は、ポリシーやルールセットを厳格に定義し、企業全体で情報セキュリティの文化を根付かせることを支援する。

特に、以下の要素は、情報セキュリティフレームワークの効果を高めるために重要であることが判明した。

- 適切な役割と責任の明確化
- 教育と意識向上プログラムの実施
- 規則・手順の明文化
- ポリシーと技術的対策の適切な連携

5. 結論

さらに、トップマネジメントによる支援と関与も、情報セキュリティ体制の成功に不可欠であることも示された。また、以下のような実務的取り組みも、実装効果を高める上で重要な役割を果たしている。

- ERPのロールベースアーキテクチャとの整合性確保
- 監査証跡の記録と利用
- プロセス文書化の徹底

COBIT 5フレームワークの導入は、組織における情報システムセキュリティの堅牢化に大きく貢献し、SCMSやERPシステムにおけるサイバー攻撃のリスクを大幅に軽減できる。