業務委託におけるセキュリティシミュレーション
Security Simulation in Outsourcing

髙濱聡一郎・法制倫理分科会・情報セキュリティ大学院大学

In recent years, supply chain attacks through group companies and business partners with relatively inadequate security measures have had a significant impact on society. This study focuses on supply chain attacks related to outsourcing in Japan and proposes "Security Simulation in Outsourcing," a method to ensure security at the time of contract. Comparison with existing methods and analysis of case studies showed that the proposed method is useful for ensuring security in outsourcing due to its ability to address issues specific to outsourcing, among other reasons.

1. 背景・貢献

★業務委託に関するサイバー攻撃により多大な被害が発生
　自動車業界の事例：自動車会社の全工場が停止(2022年3月)
　医療業界の事例　：診療業務が3週間以上停止(2022年11月)

★セキュリティ対策を要請していない or 要請していても要請内容が不十分
　⇒ **契約時に実効性のあるセキュリティ対策を合意することが重要**

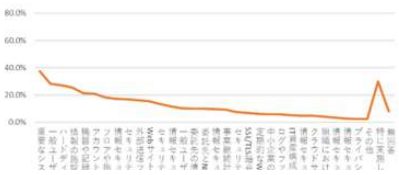
セキュリティ対策の要請割合

委託者	セキュリティ対策を要請している割合
大・中堅企業	86.2%
中小・小規模企業	10.1%

大・中堅企業のセキュリティ対策の要請内容

秘密保持契約を求めるといった対策の要請割合	推奨設定等の具体的な対策の要請割合
86.2%	平均23.1%

中小企業・小規模企業者自身のセキュリティ対策の実施状況



対策の平均実施率
⇒ 12.7%

株式会社NTTデータ経営研究所「令和3年度サイバー・フィジカル・セキュリティ対策促進事業(企業におけるサプライチェーンのサイバーセキュリティ対策に関する調査)調査報告書」とIPAの「2021年度中小企業における情報セキュリティ対策に関する実態調査-調査報告書-」を基に筆者作成

本研究の貢献

1. 業務委託のセキュリティを確保するための要件を提示
2. 業務委託のセキュリティを向上させる手法を提案
3. 提案手法の利用者向けのドキュメントを作成
4. 2022年のインシデント事例等を基に分析し評価

2. 契約時の業務委託のセキュリティ確保の要件

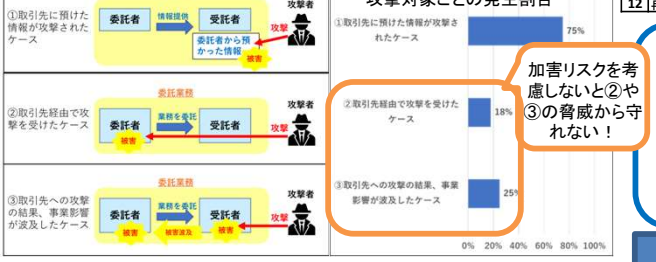
インシデントの独自調査*1や先行調査*2を基に、要件を分析した

No	要件	提案手法の特徴　※後述
1	効率的な合意形成	シナリオ（シミュレート設定）
2	情報提供と情報流出リスクの両立	二段階の合意形成
3	恣意的な回答への対応	シナリオ（説明工程の心構え４）
4	委託者受託者双方の主体的な合意形成	シナリオ（説明工程の心構え４）
5	セキュリティ対策の持続性の考慮	シナリオ（説明工程の心構え 前書）
6	セキュリティ対策の具体的な確認	シナリオ（説明工程の心構え２等）
7	取引先管理の軽減	–
8	取引者間の関係性への対応	シナリオ（説明工程の心構え３等）
9	委託者受託者の違いの考慮	シナリオ（説明工程の心構え３等）
10	不公正な取引防止策の考慮	シナリオ（説明工程の心構え４）
11	加害リスクの考慮	シナリオ（説明工程の心構え１等）

*2 先行調査
・株式会社NTTデータ経営研究所「令和3年度サイバー・フィジカル・セキュリティ対策促進事業(企業におけるサプライチェーンのサイバーセキュリティ対策に関する調査)調査報告書」
・IPAの「2021年度中小企業における情報セキュリティ対策に関する実態調査-調査報告書-」
・みずほリサーチ&テクノロジーズ株式会社の「令和3年度サイバー・フィジカル・セキュリティ対策促進事業(サイバーセキュリティ経営に関する調査)調査報告書」
・小川 らのDX(デジタル・トランスフォーメーション)時代のサプライチェーン・セキュリティ～サプライチェーンにおけるトラスト(信頼)の構築に向けて～：3. サプライチェーン・セキュリティの脅威と対策の動向」

*1 独自調査
・2022年に発生したインシデントの攻撃対象の分析
・先進企業のインシデント分析

分析例：加害リスクの考慮

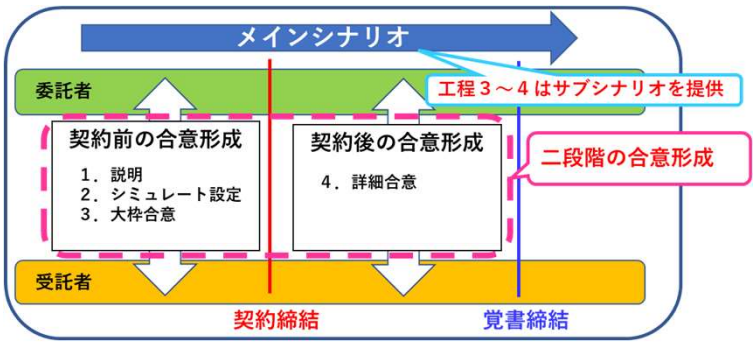


3. 既存手法との比較

	契約時に広く利用されているセキュリティ対策の合意形成の手法	提案手法
	チェックリスト	セキュリティシミュレーション
セキュリティ対策に対する納得度	△：委託者の要請 or 確認	○：双方で導出
業務委託のセキュリティ要件への対応	△：未考慮	○：考慮

4. 提案手法

業務委託におけるセキュリティシミュレーション
⇒ 契約時に実効性のあるセキュリティ対策を合意する手法



提案手法の特徴

1. 二段階の合意形成
　⇒具体的な情報提供と情報流出リスクを両立する
2. シナリオ　※指示や質問のこと
　⇒シナリオに沿って進めることで、円滑に実効性のあるセキュリティ対策を導出することが期待できる
　⇒シナリオには、1個のメインシナリオと12個のサブシナリオを提供

工程1：説明工程の利用者向けドキュメントの一部

■業務委託におけるセキュリティシミュレーションの利用に際しての心構え
実効性のあるセキュリティ対策を導出するには、委託者受託者共に持続可能な対策とする必要があります。なぜなら、無理があると対策に穴が開く恐れや、形骸化する恐れがあるためです。持続可能な対策とするため、下記５点を意識してください。
1．保有している IT 機器が攻撃者に操られ外部組織や取引先に攻撃を行う加害リスクがあります。そのため、重要情報を保持していない場合も対策が必要です。
2．セキュリティ対策に完璧はありません。また、リソースにも限りがあります。そのため、許容可能な範囲にリスクを制御するために必要なセキュリティ対策を実施しましょう。そのためにはセキュリティ対策の内容を具体的に合わせる必要があります。
3．組織ごとに様々な事情があり、また組織間の関係性も異なります。そのため、委託者受託者双方が互いの事情に理解を示すことが重要です。
4．公正取引の観点や各種法制度等、社会的な要請に応える必要があります。そのため、委託者と受託者双方が主体的かつ誠実に取り組むことが重要です。
5．建設的な合意形成とするため、既存のセキュリティ対策の穴を探すのでは無く業務委託で実施するセキュリティ対策をどうすべきかを考えましょう

メインシナリオ

No	工程	メインシナリオ
1	説明	説明資料を読み、手法の説明および実施に当たっての心構えを確認してください
2	シミュレート設定	シミュレート設定の質問に回答してください
3	大枠合意	サブシナリオに従って、業務委託で実施する対策と各対策の実施をどの組織が行うかを決めてください
4	詳細合意	サブシナリオに従って、誰がどのようにいつ実施するか等、具体的なセキュリティ対策を決めてください。

サブシナリオ（工程3，工程4）

No	サブシナリオ名	シミュレート設定項目
1	業務端末のマルウェア感染対策	-
2	ソフトウェアへの攻撃対策	-
3	認証機能を狙った不正アクセス対策	-
4	メールを利用したサイバー攻撃対策	2
5	インターネット介したサイバー攻撃対策	3
6	外部サービスを介したサイバー攻撃対策	4
7	無線LANを介したサイバー攻撃対策	5
8	個人所有の情報機器を介したサイバー攻撃	6
9	重要情報に対するサイバー攻撃の対策	7-9
10	インシデント対応	-
11	実効性維持対策	-
12	再委託時の対策	10

工程2：シミュレート設定

No	シミュレート設定
1	補足資料を参考に、役割分担の基本方針を決めてください
2	電子メールを利用しますか
3	インターネット閲覧やWebダウンロード等のインターネット利用を行いますか
4	クラウド等の外部サービスを利用しますか
5	無線LANを利用しますか
6	スマートホンや個人PC等の個人所有機器を利用しますか
7	個人情報や営業秘密等の重要情報を扱いますか
8	重要情報は書類やCD等の物体で扱いますか
9	重要情報はデータとして扱いますか
10	再委託を行いますか

サブシナリオの例

判断基準

No	シナリオ	対策例	コスト	運用手間	参考情報
1	端末を把握していますか	利用には申請を必要とする等の端末利用ルールを周知し、一覧表にまとめ、定期的に最新情報を確認する	低	多	ルールを順守しない可能性を考慮し、手間はかかるが、巡回や決済情報の確認を行うことを検討することも考えられる
2		端末管理システムを導入	高	少	・管理数が多いほど良い ・端末には様々な種類が

5. 評価

2022年に公表されたインシデントを基に提案手法の有効性を分析

結果1：インシデントの94%
⇒未然防止できた可能性が高い
結果2：インシデントの6%
⇒未然防止は困難だが、発生リスクを低減できた可能性が高い

★調査対象数：18件
★調査方法
1. 各組織のニュースリリースを確認し、2022年に公表されたインシデント数を確認(115件)
2. 業務委託に関連するインシデントを抽出(28件)
3. 原因情報が提供されているインシデントを抽出(18件)
4. 原因から提案手法実施した場合の発生防止やリスク低減の効果の可能性を分析