ITサプライチェーンにおける業務委託リスクに関する考察

A study on outsourcing risk in IT supply chain

渡邊浩平・マネジメント分科会・情報セキュリティ大学院大学

We are aware of issues regarding effective reduction methods for chained outsourcing risks in the IT supply chain and have resolved them by proposing the promotion of advanced outsourcing relationships in IT projects that use control measures to reduce security risks. The result is the presentation of a "help flow chart" for building advanced consignment relationships in IT projects, which can contribute to discussions when considering the reduction of chained outsourcing risks.

①背景/目的

ガイドラインが示す通りITサプライチェーン管理の重要性は更に高まっていくと指摘されている。

- **サイバーセキュリティ経営ガイドライン**：サプライチェーン全体のセキュリティ対策を強く推奨
- **NIST CSF**：サプライチェーンリスクマネジメントの項目が大幅に強化
- **IPA情報セキュリティ**：サプライチェーン攻撃が3年連続上位に

ビジネスモデルや技術開発に前のめりになりリスクマネジメントの変化への対応は十分か

連鎖する業務委託リスクへの有効な低減方法を提案することで、ITプロジェクトにおける前進した委託関係の構築を助けることが目的。

②研究手法

ITサプライチェーンのリスク種別毎の特徴を提示 → リスク把握を阻害する要因の検討と仮説検証 → リスク把握を高める為の新たな課題を発見 → 課題を解決する為の管理策の提案 → 有効性をインシデント事例を用いて有効性評価

対象	【内部リスク】
部品ベンダー	委託事業者は、グローバル拠点での生産が多く部品の品質にばらつきが生じ、セキュリティリスクが高くなる。
製品ベンダー	再委託により納期遅延や委託事業者の管理も煩雑になりがちである為セキュリティリスクが生じやすい。
ソフトウェアベンダー	不正コード埋め込みのリスクが高まる。
委託事業者	セキュリティ対策・連携不足、情報搾取、不正機能の組み込みリスクが高まる。
運用保守委託事業者	事業者のガバナンスの低さによる、不正な操作や連携・確認不足が多くなる。
廃業委託事業者	事業者の不正行為による機密情報搾取が発生しやすい。

	研究仮説	結果と課題
仮説Ⅰ	委託元の管理者がセキュリティ基準も用いて選定を行えば業務委託リスクを把握出来る	課題：業務委託リスクの把握に作用する要因とは言い切れない 課題：多数のITサプライチェーンインシデント事例や判例から妥当る検証が必要 NG
仮説Ⅱ	委託元と委託先の管理者が、両者が納得する業務範囲を定められれば迅速な対応が期待される	課題：業務委託リスクの把握に作用する要因と言える 課題：改正民法等をきっかけに情報セキュリティ対策の見直し・強化に繋げる必要 OK
仮説Ⅲ	参加企業が一丸となった新たな枠組みがプロジェクトを円滑に進める	課題：業務委託リスクの把握に作用する要因と言える 課題：PMやSEが受け入れ可能な法的縛り等を効かせた新たな仕組み作りが必要 OK

独自管理策の提案
お助けフローチャート

※セキュリティリスク低減策

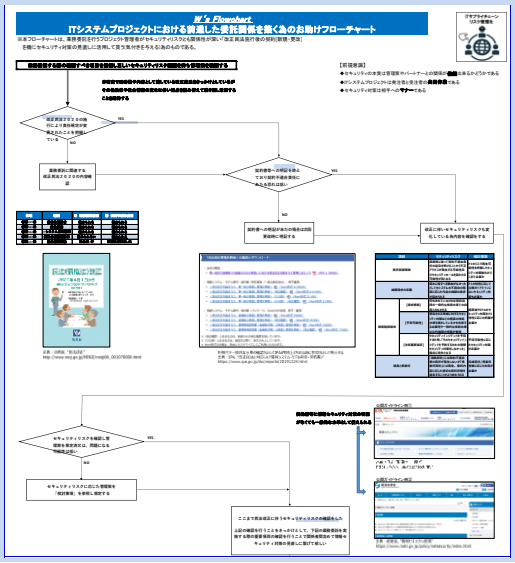
実際にITサプライチェーン上で発生した事例を収集

再発防止策情報を公開してる事例2010年以降

③提案/有効性

前進した委託関係をきづく為のお助けフローチャートを提案（一部抜粋版）

40ケースのインシデント事例を用い管理策を使用した場合の低減率を評価



項番	年度	委託元業種	発生場所	直接原因	確認項目									
					フローチャート項目						不足項目			低減率
					把握/合意	監査	技術	教育/指導	予備	ガイドライン	構築間	仕様変更	脆弱判断	
1	2012	卸売・小売	再委託先	SWバグ	1	1		1			1	1		60.0%
2	2013	電気	委託先	ウィルス	1	1		1			1			75.0%
3	2013	卸売・小売	委託先	SWバグ						1				100.0%
4	2013	官公庁	委託先	人的ミス	1		1	1						100.0%
5	2013	卸売・小売	委託先	不正アクセス			1					1		50.0%
6	2013	サービス	委託先	人的ミス		1		1			1			66.7%
7	2013	サービス	再委託先	不正アクセス			1				1			50.0%
8	2014	医療	委託先	不正アクセス					1					100.0%
9	2014	製造	委託先	人的ミス	1	1					1			66.7%
10	2014	運輸	委託先	人的ミス				1						100.0%
11	2014	教育	委託先	内部不正	1		1	1						100.0%
12	2014	情報通信	委託先	監視脱失		1						1		50.0%
13	2014	情報通信	委託先	内部不正		1	1							100.0%
14	2014	教育	再委託先	内部不正				1	1			1	1	50.0%
15	2014	官公庁	再委託先	監視脱失	1			1						100.0%
16	2014	情報通信	委託先	不正アクセス								1		0.0%
17	2015	官公庁	委託先	人的ミス			1							100.0%
18	2015	教育	委託先	人的ミス	1		1	1	1					100.0%
19	2015	教育	委託先	人的ミス			1			1				100.0%
20	2015	サービス	委託先	不正アクセス	1		1		1					100.0%
21	2015	サービス	委託先	不正アクセス	1		1							100.0%
22	2015	卸売・小売	再々委託	不正アクセス							1			0.0%
23	2016	NPO	委託先	SWバグ		1	1		1	1				100.0%
24	2016	サービス	委託先	不正アクセス			1							100.0%
25	2016	官公庁	委託先	不正アクセス			1							100.0%
26	2016	サービス	委託先	不正アクセス			1						1	50.0%
27	2016	サービス	委託先	ウィルス				1	1		1		1	50.0%
28	2016	卸売・小売	委託先	不正アクセス						1				100.0%
29	2017	官公庁	委託先	不正アクセス			1							100.0%
30	2017	官公庁	委託先	不正アクセス					1					100.0%
31	2017	卸売・小売	委託先	不正アクセス									1	50.0%
32	2017	卸売・小売	委託先	不正アクセス		1	1		1					100.0%
33	2017	サービス	再委託先	不正アクセス		1	1			1				100.0%
34	2017	サービス	委託先	不正アクセス		1	1			1				100.0%
35	2018	官公庁	委託先	不正アクセス	1	1	1			1	1	1		66.7%
36	2018	サービス	再委託先	人的ミス		1			1					100.0%
37	2019	サービス	再委託先	人的ミス				1						100.0%
38	2019	官公庁	再委託先	内部不正			1		1	1		1	1	60.0%
39	2020	サービス	委託先	人的ミス	1		1	1						100.0%
40	2020	サービス	再委託先	内部不正			1							100.0%
合計	-	-	-	-	11	12	23	12	10	8	8	7	5	81.1%

低減率Av 81.1%

お助けフローチャートを管理されたプロセスまで対応出来ていれば8割以上のインシデントへ効果がある

各組織で判断および気付きを与え連鎖する業務委託リスクの低減を検討する際の議論に貢献することができる