情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

「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

2023年2月25日
修士論文・特定課題研究発表会

5515501　髙濱　聡一郎
情報セキュリティ大学院大学　後藤研究室

アジェンダ

1. 発表の概要
2. 業務委託に関するサプライチェーン攻撃の実態
3. 業務委託に関するセキュリティ対策の実態
4. 業務委託契約時のセキュリティ対策の合意形成
5. セキュリティを確保するための要件
6. 既存の取り組みによる解決可能性
7. 業務委託におけるセキュリティシミュレーション
8. 評価
9. まとめ

1. 発表の概要

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

問題意識

研究対象とする業務委託
⇒ コールセンターの受付業務などの一般的な業務委託

企業のセキュリティに関する取り組み

業務委託に関するサイバー攻撃
＝研究対象とするサプライチェーン攻撃

社会に対する多大な悪影響

目的 ： 業務委託におけるセキュリティの向上

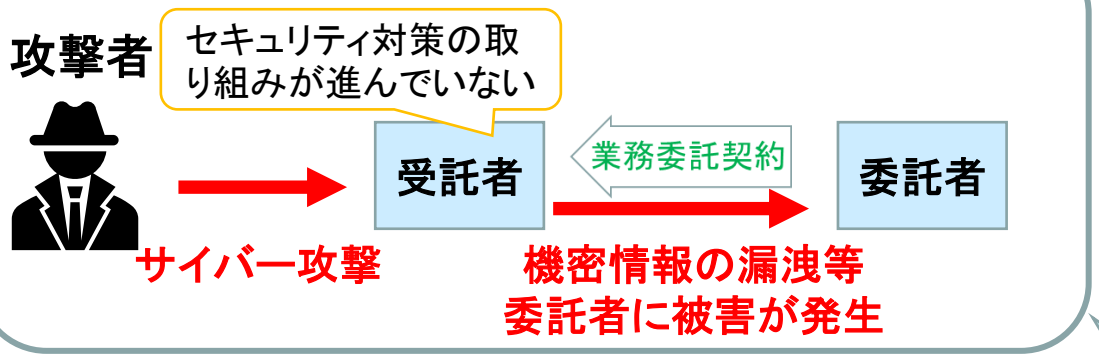
仮説 ： 実効性のあるセキュリティ対策が実施できていないから

貢献 ： 1.「業務委託のセキュリティを確保するための要件」 の提示
2.「業務委託におけるセキュリティシミュレーション」 の提案
3. 提案手法の利用者向けのドキュメントの作成
4. 2022年のインシデント等を基に、対策の実態や提案手法を分析し評価

2. 業務委託に関するサプライチェーン攻撃の実態

様々な組織でセキュリティ対策が行われているものの、業務委託に関するサプライチェーン攻撃によって、多大な被害が発生している

図表1 業務委託の取引先を介したサプライチェーン攻撃



企業の取り組み例

- ガイドラインの利用
  - 例：サイバーセキュリティ経営ガイドライン
- セキュリティ認証の取得
  - 例：ISMS、プライバシーマーク
- 外部監査の実施
  - 例：SOC2・SOC3

・情報セキュリティ10大脅威 2022　組織の脅威　第三位
「サプライチェーンの弱点を悪用した攻撃」がランクイン

・様々な被害が発生

図表2　業務委託に関するサプライチェーン攻撃の被害

EMOTET	ランサムウェア	システムへの不正アクセス	DDoS攻撃	ファイル転送サービスの侵害	不正サイトへの誘導	不正送金
受託者が感染し、不正メールを受信	受託者が感染し、データ暗号化、情報漏洩、業務影響が発生	攻撃を受けた受託者から自社情報が漏洩	受託者が攻撃を受け、業務影響が発生	受託者のサービス侵害により、情報漏洩	受託者HPの改竄による不正サイトへの誘導	受託者の決済サービスの悪用による不正送金

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」を元に筆者作成

3. 業務委託に関するセキュリティ対策の実態

業務委託の契約時点で業務委託のセキュリティが確保されていないことを確認

＜大企業・中堅企業が委託者となる業務委託＞

⇒ **受託者にセキュリティ対策を要請しているものの、その内容は結果責任を求める傾向にある**

＜中小企業が委託者となる業務委託＞

⇒ **受託者にセキュリティ対策を要請している割合が低く、セキュリティ対策の実施率も低い**

図表3　セキュリティ対策の要請割合

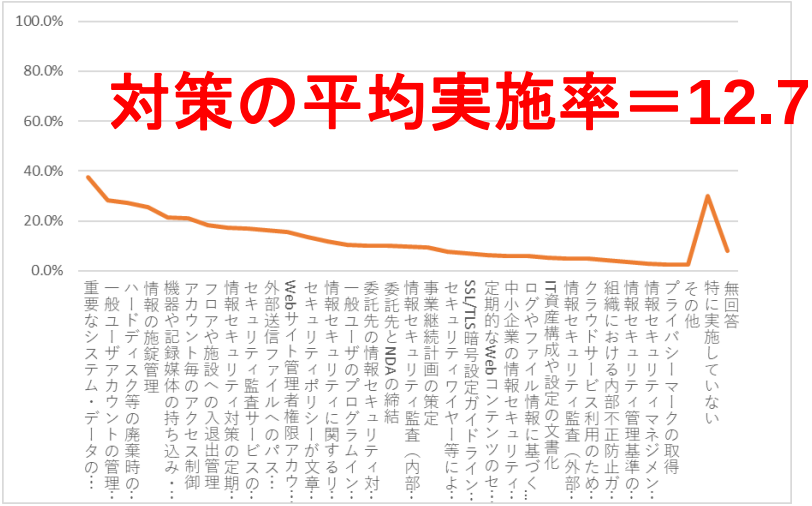
委託者	セキュリティ対策を要請している割合
大・中堅企業	86.2%
中小・小規模企業	10.1%

図表4　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%

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

図表5　中小企業の被害防止のための組織面・運用面の対策の実施状況



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

契約時にセキュリティを確保する手法が必要！

4. 業務委託契約時のセキュリティ対策の合意形成

現状の業務委託の契約時のセキュリティ対策の合意形成について示す

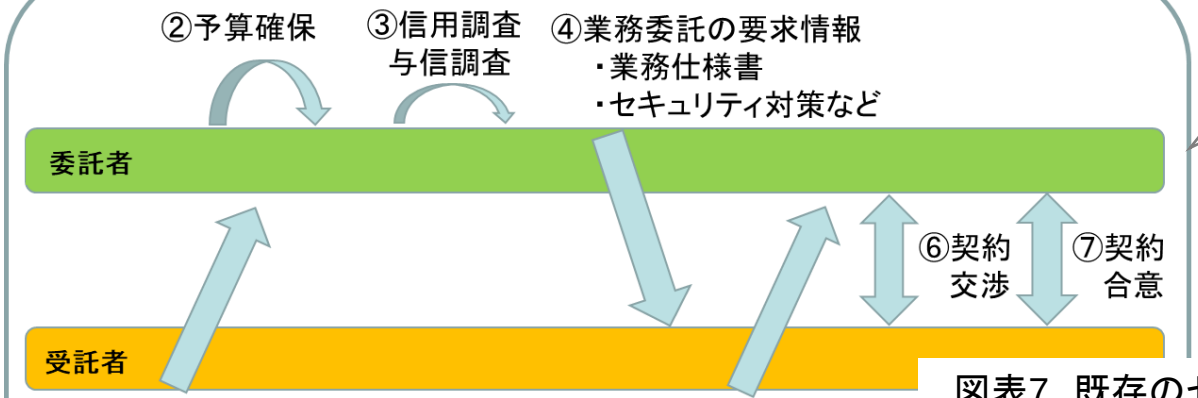
各社のセキュリティの取り組み

委託者・受託者ともに、予め1と2を実施
1. 組織全体のセキュリティ方針の策定
2. 管理体制の構築
3. 自組織で定めたセキュリティ対策を実施

参考

<ガイドライン・セキュリティ認証等>
例1：サイバーセキュリティ経営ガイドライン
例2：ISMS認証
例3：NIST sp800シリーズ・・・
例4：個人情報保護法ガイドライン等

図表6　大体の業務委託契約の合意プロセス



IPAの「ITサプライチェーンにおける情報セキュリティの責任範囲に関する調査」を参考に筆者作成

IPA、NTTデータ等の先行研究を参考に筆者作成

図表7　既存のセキュリティ対策の合意手法

方法	概要
チェックリスト	委託者が定めたセキュリティチェックリスト
事前外部認証	ISMS認証、SOC2/SOC3、Pマーク
公開資料	受託者の公開資料
専用の第三者監査	第三者による情報セキュリティ監査
実地検査（視察）	対策通りに行動しているかを確認する
技術診断	専用ソフト等で対策をチェックする
レビュー	証跡を確認する

セキュリティ対策

以前の意味：　予防対策
近年の意味：　予防対策＋事後対応

本研究での扱いはこちら

参考：チェックリストの例

チェックリストは、委託者から受託者に対して、受託者のセキュリティ対策の確認や、委託者が要求するセキュリティ対策をまとめたものとなっていることが多い

図表8　IPAの中小企業の情報セキュリティ対策ガイドラインの付録5より抜粋

9-2　委託先情報セキュリティ対策状況確認リスト

注：このサンプルは、委託先の情報セキュリティ対策の実施状況を確認するためのものです。
必要な項目を加筆修正してご利用ください。

会社名：　　確認者：　　確認日：

区分	No	確認項目	実施状況(○、×)
社内体制	1	情報セキュリティ管理責任者を定めている	
	2	情報セキュリティ対策を定めた規程を整備している	
	3	情報セキュリティへの取り組み方針を従業員や取引先に周知している	
	4	情報セキュリティ事故に対する対応手順を整備している	
	5	定期的に情報セキュリティに関する内部点検を実施している	
人的管理	6	情報セキュリティに関する教育を定期的に実施し、受講記録を作成している	
	7	従業員と守秘義務契約を交わしている	
物理的管理	8	関係者以外の事務所への立ち入りを制限している	
	9	機密情報の保管について施錠管理をしている	

5. セキュリティを確保するための要件

情報セキュリティ大学院大学

インシデント事例の独自調査*1や先行調査*2を基に、阻害要因＋制約・条件を分析し、業務委託のセキュリティを確保するための11個の要件を導出

図表9　セキュリティを確保するための要件

No	要件	説明
1	効率的な合意形成	最小限の時間やコストで契約時の合意形成を行う必要がある
2	情報提供と情報流出リスクの両立	委託者から受託者への情報提供による実効性向上と、情報提供により発生するリスクの回避を両立する必要がある
3	恣意的な回答への対応	受託者の恣意的な回答に対処する必要がある
4	委託者受託者双方の主体的な合意形成	当事者である委託者受託者主体の対策検討を実現する必要がある
5	セキュリティ対策の持続性の考慮	持続的なセキュリティ対策とする必要がある
6	セキュリティ対策の具体的な確認	セキュリティ機能の正常性を事前に確認する必要がある
7	取引先管理の負荷低減	取引先管理を効率的に実施できる必要がある
8	取引者間の関係性への対応	取引者間の関係に左右されず合意可能とする必要がある
9	委託者受託者の違いの考慮	取引者間の違いがあっても合意できる必要がある （業種・規模・環境・意識レベル・知識・費用）
10	不公正な取引防止策の考慮	不公正な取引とならないようにする必要がある
11	加害リスクの考慮	加害意識の観点が含まれるようにする必要がある

*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

*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」

6. 既存の取り組みによる解決可能性

各要件に関連する先行研究や事例を確認し、課題を整理

図表10　要件と先行研究の対応

No	要件	関連する先行研究やセキュリティの取り組み
1	効率的な合意形成	契約書の雛形[6] ⇒課題：雛形では個別事情に対応が困難
2	情報提供と情報流出リスクの両立	-
3	恣意的な回答への対応	直接的な管理や監査の徹底（セキュリティ先進企業の再発防止策） ⇒課題：受託者が複数の企業から業務を受託している場合などは、端末を業務ごとに用意する等の対応が必要。委託者にとっても、コスト面で現実的でない場合もありえる。また、力関係による押し付けになってしまうと、違法性の懸念や、不正の動機となりかねない。
4	委託者受託者双方の主体的な合意形成	中小企業の情報セキュリティ対策ガイドライン付属の詳細リスク分析シートの提供等（2.1.1節） ⇒課題：業務委託に特化していないため、業務委託のセキュリティ対策の検討を行う場合は使用しやすいとはいえない
5	セキュリティ対策の持続性の考慮	事前合意のとれたガイドラインの利用[21] ⇒課題：取引者間の違いや具体的な対策では事前合意が困難
6	セキュリティ対策の具体的な確認	No3と同様
7	取引先管理の負荷低減	セキュリティチェックシートの共通化[29] ⇒課題：現時点では試みで、未完成。 中小企業の情報セキュリティ対策ガイドライン付属の委託先情報セキュリティ対策状況確認リスト（2.1.1節） ⇒課題：利用時は状況に合わせて具体性を補う必要がある
8	取引者間の関係性への対応	-
9	委託者受託者の違いの考慮	業種の違い：- 規模の違い：取引先に提供する業務システムを通じた情報提供等[18] ⇒課題：業務システムを提供しない場合も考えられる 環境の違い：情報連携アーキテクチャの導入[31] ⇒課題：コスト負担の少ない方法も必要 意識レベルの違い：業界団体による啓蒙活動[21] 知識の違い：協力会の設立[30] 費用の違い：セキュリティ費用の一部負担[18] ⇒課題：どのように費用負担を考えるべきか不明
10	不公正な取引防止策の考慮	経産省等が主導作成した公正な取引に関する指針の発信[32]
11	加害リスクの考慮	サイバーセキュリティ経営ガイドラインVer2.0（2.11節） ⇒課題：指示９で加害リスクに触れてはいるが、文書全体として強調されていない

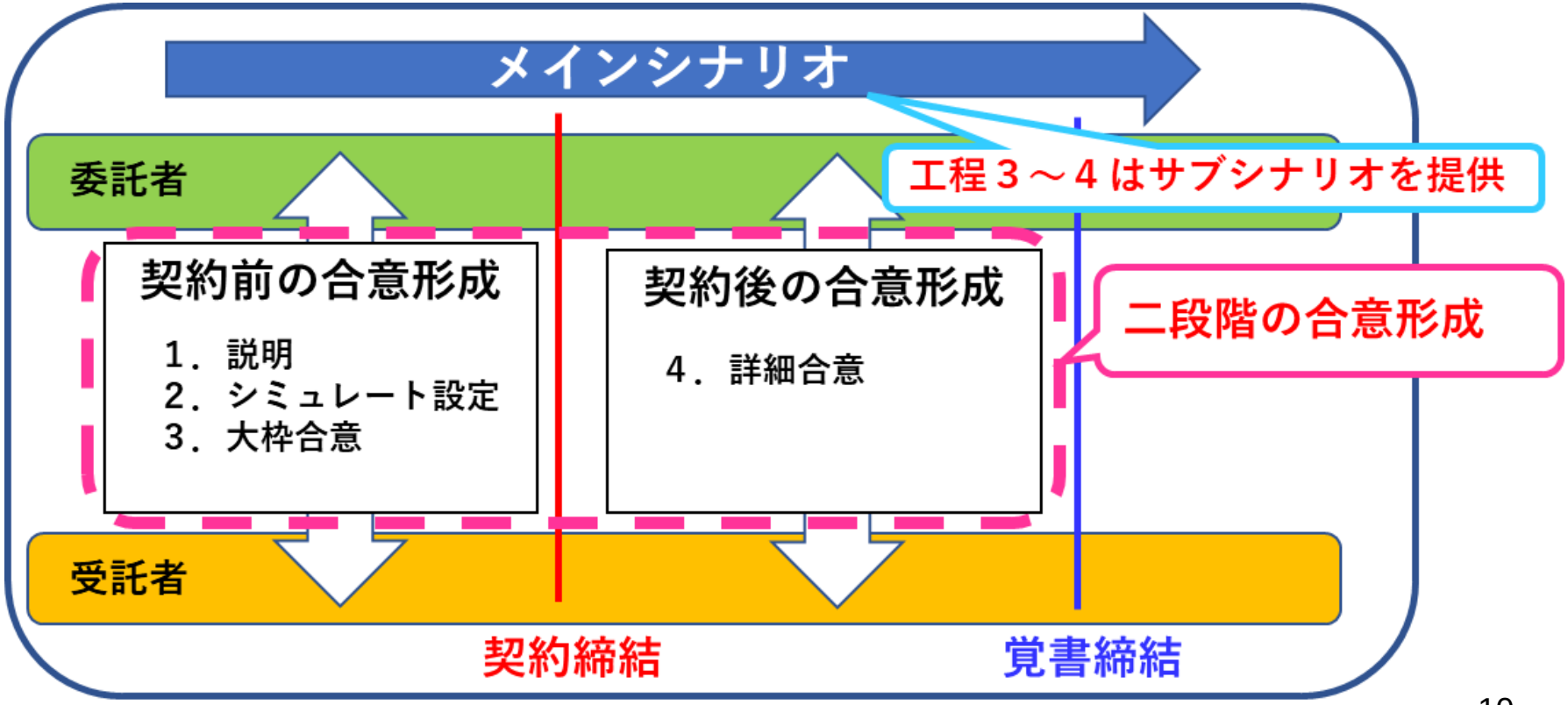
7.業務委託におけるセキュリティシミュレーション

業務委託の契約時に対象となる業務委託をシミュレートし、適切なタイミングで、助言や判断材料を提供することで、実効性のあるセキュリティ対策を導出する手法

特徴1： 二段階の合意形成

特徴2： シナリオ（指示や質問）

図表11　業務委託におけるセキュリティシミュレーションの全体像



7－1. メインシナリオ

メインシナリオをユーザーに示すことで、各工程を円滑に進めることが期待できる

図表12　メインシナリオの内容

	No	工程	メインシナリオ
契約前の合意形成	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
契約後の合意形成	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。

7-2. 工程1

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

契約後の合意形成で実効性のあるセキュリティ対策が合意できるように、本手法の説明および実施に当たっての心構えを利用者に伝える

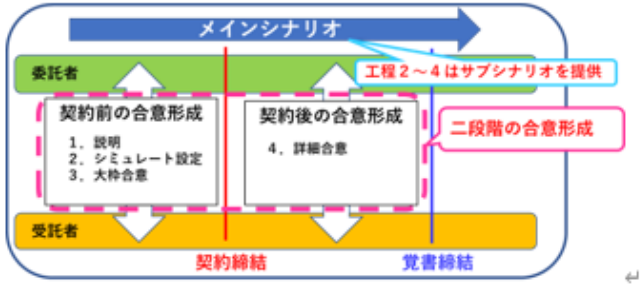
図表13　工程1の説明資料

説明資料

■業務委託におけるセキュリティシミュレーションとは

・業務委託のセキュリティを確保するため、契約時に取引者間で実効性のあるセキュリティ対策を決めるための手法です。

・本手法は契約前の合意形成と契約後の合意形成の 2 段階で合意を行います。契約前の合意形成で、工程 1～3を実施し、契約後の合意形成で工程 4を実施します。



■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

■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

7-3. 工程2

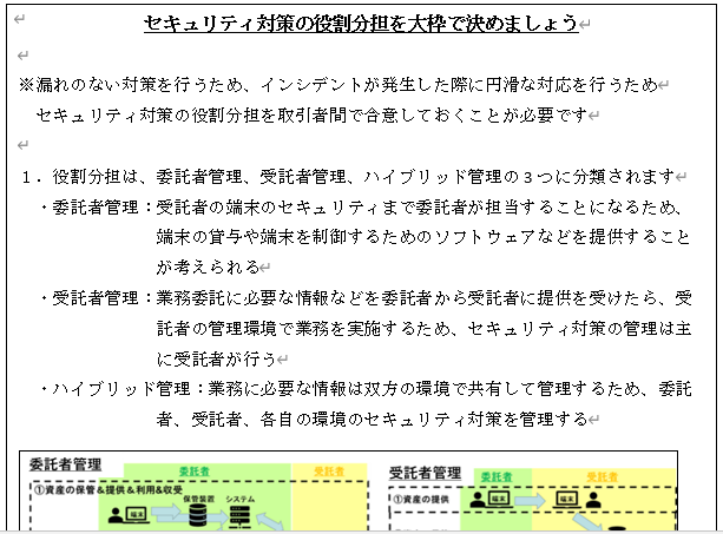
対象とする業務委託をシミュレートするための情報を収集する

図表14　工程2のシミュレート設定の確認項目

No	シミュレート設定の確認項目
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

※本確認項目は、下記のドキュメントを参考に、前述の業務委託のセキュリティ確保の要件が満たされるように作成した
・中小企業の情報セキュリティ対策ガイドライン第3版

図表15　No1の補足資料の一部



セキュリティ対策の役割分担を大枠で決めましょう

※漏れのない対策を行うため、インシデントが発生した際に円滑な対応を行うため
セキュリティ対策の役割分担を取引者間で合意しておくことが必要です

1．役割分担は、委託者管理、受託者管理、ハイブリッド管理の３つに分類されます
・委託者管理：受託者の端末のセキュリティまで委託者が担当することになるため、端末の貸与や端末を制御するためのソフトウェアなどを提供することが考えられる
・受託者管理：業務委託に必要な情報などを委託者から受託者に提供を受けたら、受託者の管理環境で業務を実施するため、セキュリティ対策の管理は主に受託者が行う
・ハイブリッド管理：業務に必要な情報は双方の環境で共有して管理するため、委託者、受託者、各自の環境のセキュリティ対策を管理する

委託者管理　受託者管理

7-4. 工程3と工程4(その1)

第3の大枠合意の工程では、実施する対策と担当組織を合わせ、第4の詳細合意の工程では、具体的なセキュリティ対策について合わせる

図表16　工程3と工程4で用いるサブシナリオの一覧

No	分類	サブシナリオ名	シミュレート設定項目
1	予防対策	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	事後対策	インシデント対応	-
11	全体的な対策	実効性維持対策	-
12		再委託時の対策	10

本サブシナリオは、
下記のドキュメントを参考に、前述の業務委託のセキュリティ確保の要件が満たされるように作成した
・中小企業の情報セキュリティ対策ガイドライン第3版
・個人情報の保護に関する法律についてのガイドライン（通則編）

7-5. 工程3と工程4(その2)

利用者にシナリオ、対策例、判断材料、参考情報を提供することで、実効性のあるセキュリティ対策の導出を促進する

図表17　工程3と4のサブシナリオの例

判断材料

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あり、管理システムによっては管理できないことがあるため、管理対象端末の種類を把握することが重要

8. 評価

提案手法の有用性について、4つの方法で分析し評価した

1. 既存手法（チェックリスト）との比較

2. 2022年のインシデントを基にした分析

3. 代表的なインシデント事例を基にした分析

4. 先進企業のインシデント事例を基にした分析

8-1. 既存手法との比較

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

「業務委託におけるセキュリティシミュレーション」は、チェックリストよりも、業務委託のセキュリティを確保するための手法として適している

図表18　既存手法との比較

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
概要	1．委託者が受託者のセキュリティ対策を確認し、受託者に対し要求するセキュリティ対策を提示するための手法 2．委託者が要求するセキュリティ対策の項目一覧である	1．委託者と受託者の双方が主体となってセキュリティ対策を確認および導出する手法 2．当該業務委託特有の事情をシミュレートしたシナリオを用いる
セキュリティ対策に対する納得度	△	○
業務委託の特有性への対応	△	○

委託者受託者間の違いや関係性に考慮する等の業務委託の要件への対応

8-2. 2022年のインシデントを基にした分析

各事例で「業務委託におけるセキュリティシミュレーション」を実施した場合の効果を分析

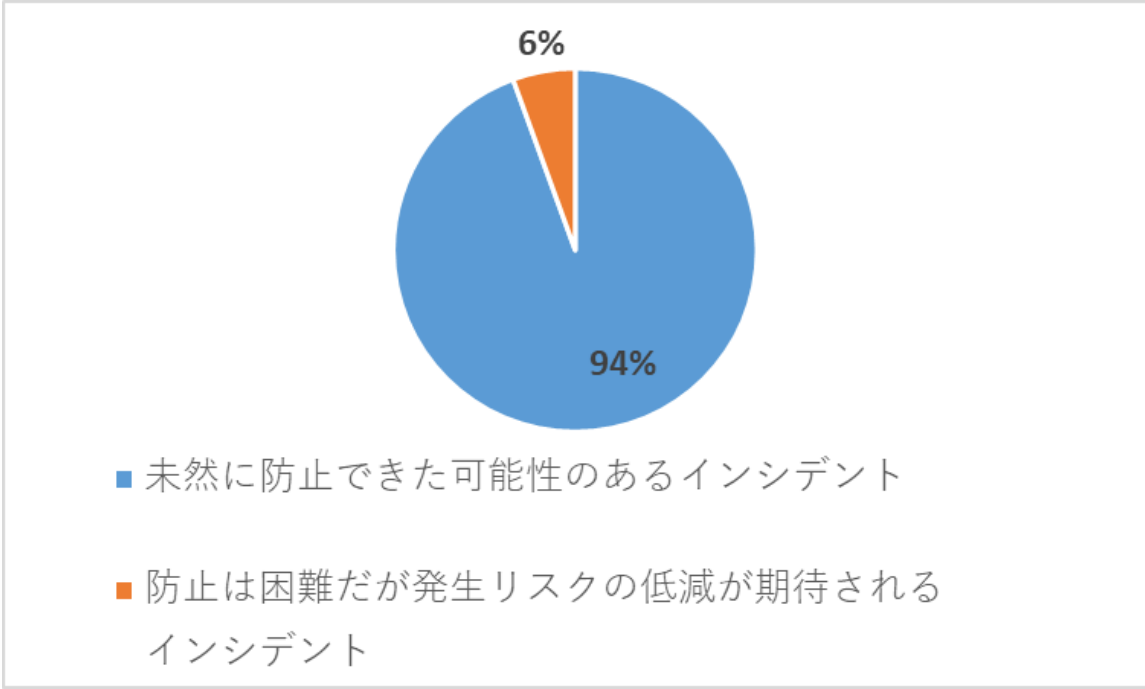
1. **分析対象のインシデントの94%は、提案手法を実施していた場合は未然に防止できていた可能性があることを確認**
2. **メール関連のインシデントである分析対象のインシデントの6%は、未然に防止できたと言い切れないものの、発生リスクを低減できたと考えられる**

★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

図表19　提案手法による解決可能性の確認結果

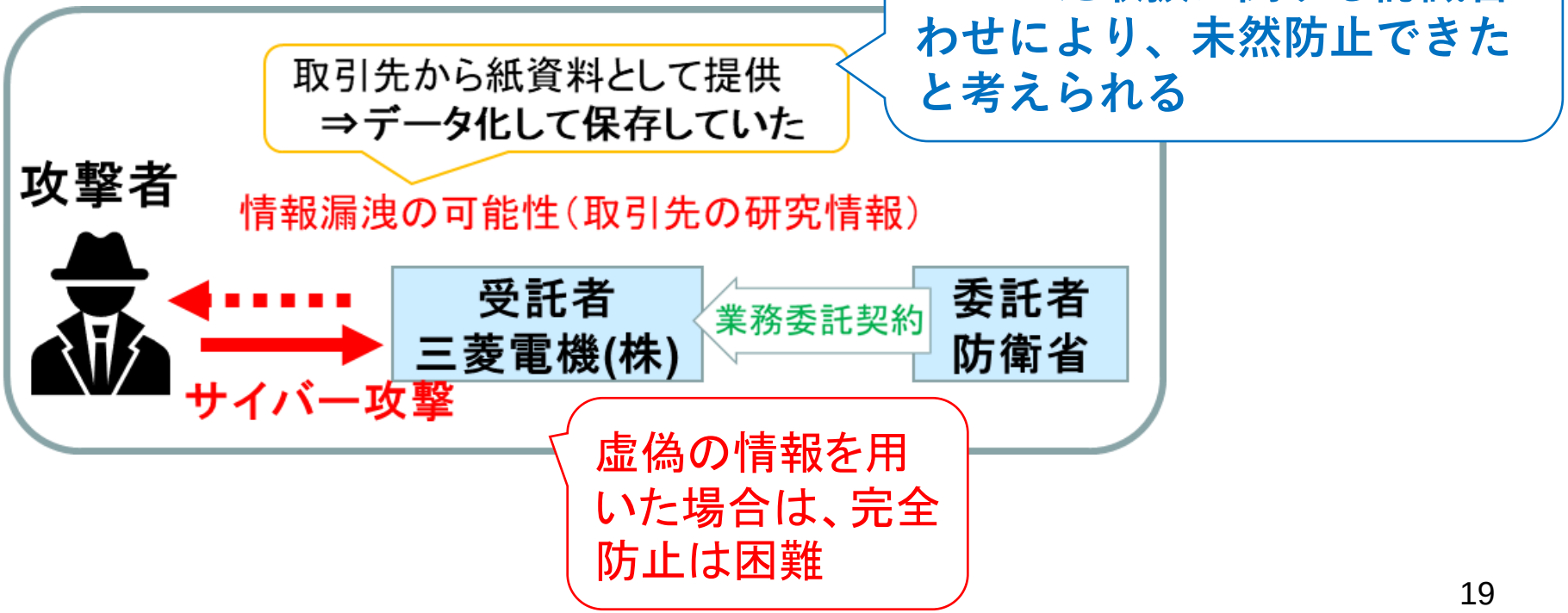


8-3. 代表的なインシデント事例を基にした分析

本事例の委託者と受託者のやり取りの中で、受託者が委託者の要求どおりに従わなかったことが確認されている

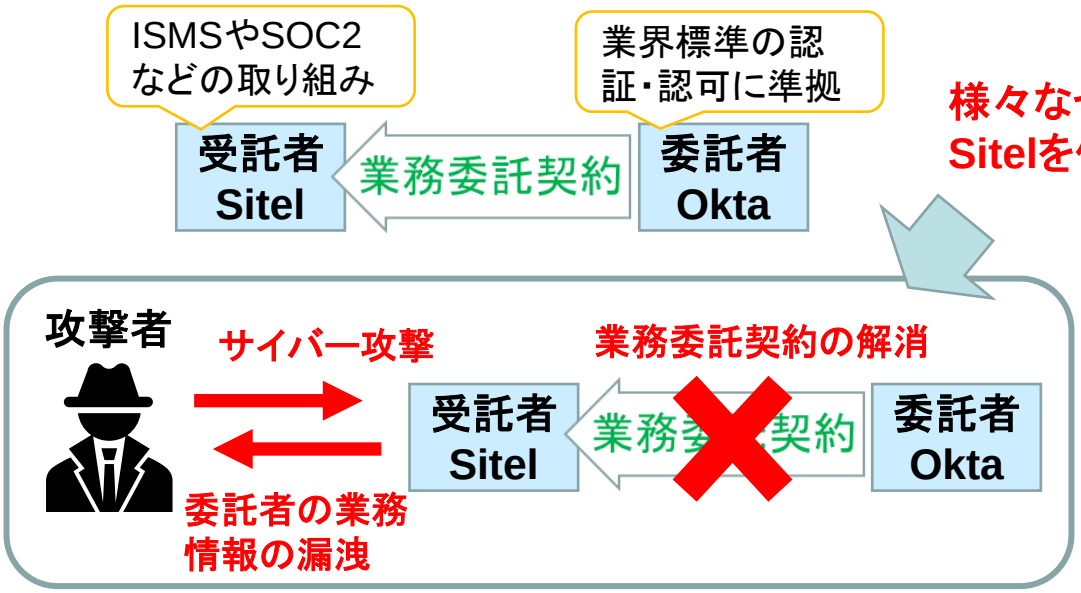
＜本手法を利用していた場合＞
- 研究情報が被害対象に含まれることを未然に防げたと考えられる
- 意識合わせに虚偽の情報を用いる等の行為については、完全に防止することは困難

図表20　三菱電機のインシデント事例



8-4. 先進企業のインシデント事例を基にした分析

＜本手法を利用していた場合＞
・インシデントが発生したとしても、契約解消を回避できた可能性が高い



様々なセキュリティの取り組みを行っている
Sitelを信頼し、Oktaは業務を委託

＜契約解消の要因＞
1. 報告書の提出が遅さ
2. 報告書の内容が不十分
3. ログ収集の遅さ

契約後の合意形成のインシデント対応のサブシナリオを活用することで、契約解消の要因となった3点について、契約の時点で具体的に認識合わせができたと考えられる

9. まとめ

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

＜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」 の提示
2. 「業務委託におけるセキュリティシミュレーション」 の提案
3. 提案手法の利用者向けのドキュメントの作成
4. 2022年のインシデント等を基に、対策の実態や提案手法を分析し評価

＜今後の課題＞
1. 取引先管理の負荷低減への対応
2. 提案手法の工程3，4で使用するサブシナリオの十分性
3. 提案手法を使用した場合に発生する利用者への負担の評価
4. 中小企業と小規模企業者の扱い

＜提案手法の更なる実効性向上のためには＞
1. 委託者受託者の各組織内部の合意形成が重要
2. セキュリティ意識の向上のため、経営者の意識改革、組織文化、法制度等の研究が重要

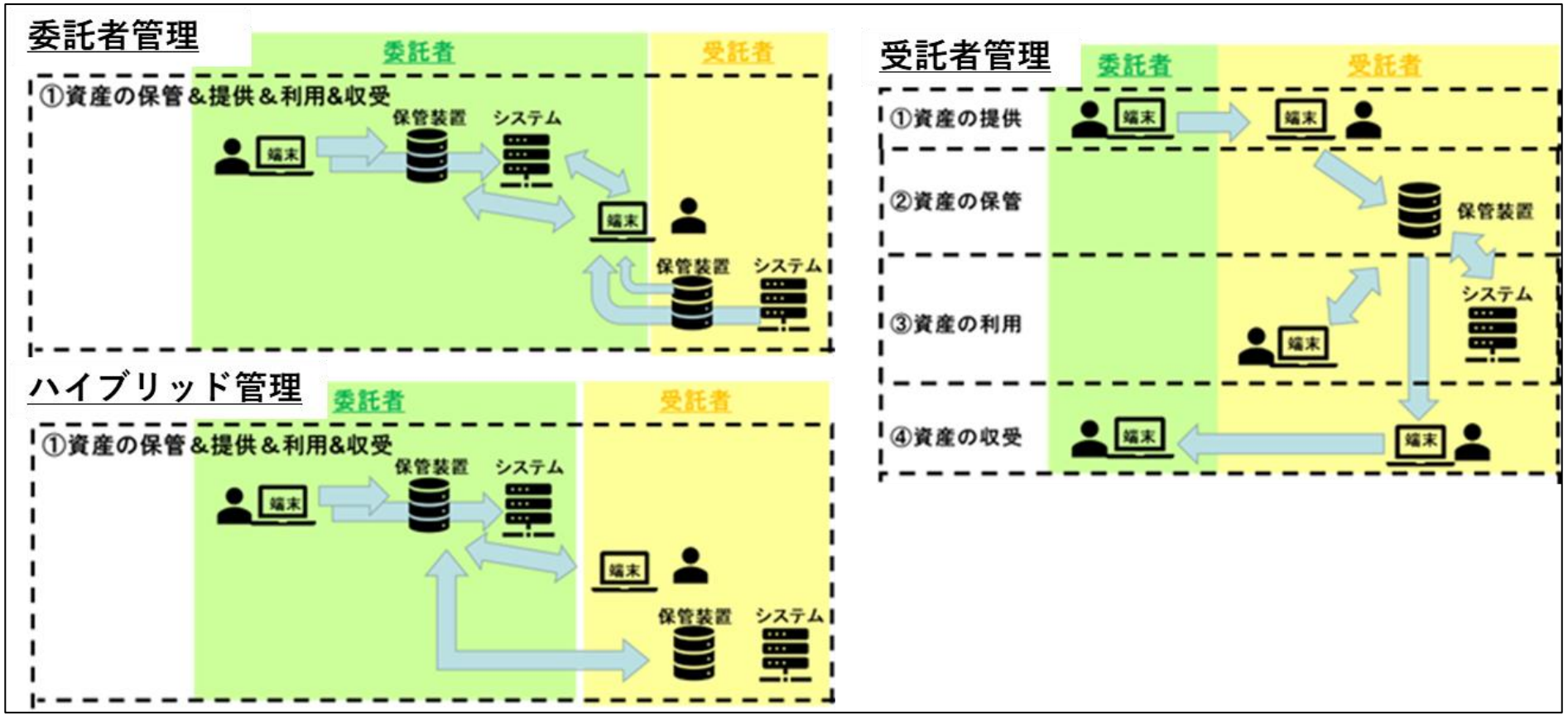
参考1：要件と特徴の対応

No	要件	提案手法の特徴
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	2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）
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）
5	セキュリティ対策の持続性の考慮	シナリオ（説明工程・対策例・判断材料・参考情報の提示）
6	セキュリティ対策の具体的な確認	シナリオ（説明工程・対策例・判断材料・参考情報の提示）
7	取引先管理の負荷低減	-
8	取引者間の関係性への対応	シナリオ（説明工程、シミュレート設定・対策例・判断材料・参考情報の提示）
9	委託者受託者の違いの考慮	シナリオ（説明工程、シミュレート設定・対策例・判断材料・参考情報の提示）
10	不公正な取引防止策の考慮	シナリオ（説明工程）
11	加害リスクの考慮	シナリオ（加害リスクの強調）

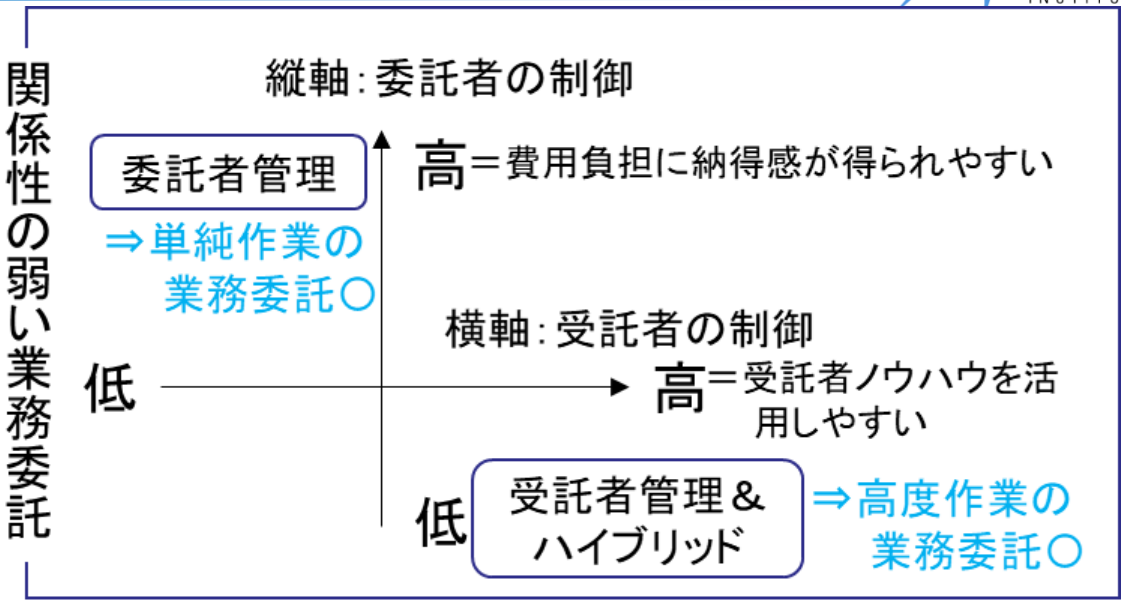
参考2：説明工程の心構えと要件・特徴との対応

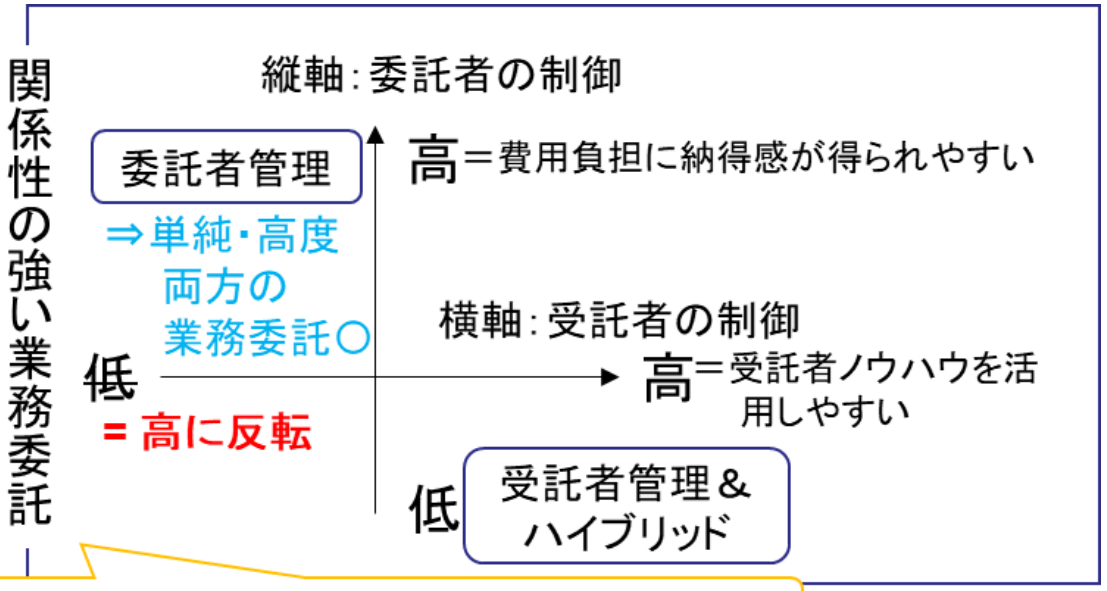
No	説明資料の心構え	対応する要件およびシナリオの考慮事項
前書	実効性のあるセキュリティ対策を導出するには、委託者受託者共に持続可能な対策とする必要があります。なぜなら、無理があると対策に穴が開く恐れや、形骸化する恐れがあるためです。持続可能な対策とするため、下記5点を意識してください。	セキュリティ対策の持続性の考慮
1	保有しているIT機器が攻撃者に操られ外部組織や取引先に攻撃を行う加害リスクがあります。そのため、重要情報を保持していない場合も対策が必要です。	加害リスクの考慮
2	セキュリティ対策に完璧はありません。また、リソースにも限りがあります。そのため、許容可能な範囲にリスクを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。	セキュリティ対策の具体的な確認
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。	取引者間の関係性への対応 委託者受託者の違いの考慮
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。	取引者双方の主体的な合意形成 不公正な取引防止策の考慮 恣意的な回答への対応
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	言葉の扱い方（脆弱性という言葉の扱い）

参考3：セキュリティ対策の役割分担



参考4：業務委託における難易度と役割分担の関係





資本関係のある会社間の業務委託など