日本のサイバーセキュリティを「連携」「学び」「創造」

情報セキュリティマネジメント・セミナー2024

「委託先管理」どうやってますか？

2024年12月6日

日本ISMSユーザグループ インプリメンテーション研究会
尾崎 幸彦 (株式会社Speee)

自己紹介

株式会社 Speee セキュリティ推進室

尾崎 幸彦 (おざきゆきひこ)

- ISMS/ISMS-CLS主任審査員 (JRCA)
- 日本ISMSユーザグループ インプリメンテーション研究会 副主査

略歴	
～2018年12月	NECソフトウェア中部 → NECソリューションイノベータ株式会社 • 情報セキュリティ部門マネージャ
2019年4月 ～2021年10月	株式会社 日本環境認証機構 (JACO) • ISMS & BCMS 審査員
2021年11月～	株式会社 Speee • セキュリティ推進室 -情報セキュリティマネジメント専任

目次

1. 27001における委託先管理に関連する条文や管理策
2. 本テーマで取り扱う「委託先管理」
3. 他の規格やガイドライン、フレームワークでの「委託先管理」に該当する事項
4. 研究会メンバーからの情報
5. 委託先管理のDX

参考: 委託先管理に関連するインシデント例

27001における
委託先管理に関連する条文や管理策

委託先管理に関連する条文

JIS Q 27001:2023

4.1 組織及びその状況の理解

8.1 運用の計画策定及び管理

【管理策】

5.19 供給者関係における情報セキュリティ

5.20 供給者との合意における情報セキュリティの取扱い

5.21 情報通信技術(ICT)サプライチェーンにおける情報セキュリティの管理

5.22 供給者のサービス提供の監視、レビュー及び変更管理

5.23 クラウドサービスの利用における情報セキュリティ

8.30 外部委託による開発

委託先管理に関連する条文

JIS Q 27001:2023

4.1 組織及びその状況の理解

組織は，組織の目的に関連し，かつ，そのISMS の意図した成果を達成する組織の能力に影響を与える，**外部**及び内部の課題を決定しなければならない。

組織は，気候変動が関連する課題かどうかを決定しなければならない。

注記
これらの課題の決定とは，JIS Q 31000:2019の5.4.1 に記載されている組織の外部状況及び内部状況の確定のことをいう。

JIS Q 31000:2019 リスクマネジメント－指針

5.4.1 組織の外部状況及び内部状況の確定

リスクのマネジメントを行うための枠組みを設計するに当たって，組織は，外部及び内部の状況を検証し，理解することが望ましい。

組織の**外部状況の検証には，次の事項が含まれる場合がある**。ただし，これらに限らない。

- 国際，国内，地方又は近隣地域を問わず，社会，文化，政治，法律，規制，金融，技術，経済及び環境に関する要因
- 組織の目的に影響を与える，鍵となる原動力及び傾向
- 外部ステークホルダとの関係，並びに外部ステークホルダの認知，価値観，必要性及び期待
- 契約上の関係及びコミットメント
- ネットワークの複雑さ，及び依存関係

委託先管理に関連する条文

JIS Q 27001:2023

8.1 運用の計画策定及び管理

(前半省略)

組織は，ISMS に関連する，**外部から提供されるプロセス，製品又はサービス**が管理されていることを確実にしなければならない。

委託先管理に関連する管理策

JIS Q 27001:2023

5.19 供給者関係における情報セキュリティ

管理策

供給者の製品又はサービスの利用に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め，実施しなければならない。

目的

供給者関係において合意したレベルの情報セキュリティを維持するため。

委託先管理に関連する管理策

JIS Q 27001:2023

5.20 供給者との合意における情報セキュリティの取扱い

管理策

供給者関係の種類に応じて，関連する情報セキュリティ要求事項を確立し，各供給者と合意しなければならない。

目的

供給者関係において合意したレベルの情報セキュリティを維持するため。

委託先管理に関連する管理策

JIS Q 27001:2023

5.21 情報通信技術(ICT)サプライチェーンにおける情報セキュリティの管理

管理策

ICT 製品及びサービスの**サプライチェーン**に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め，実施しなければならない。

目的

供給者関係において合意したレベルの情報セキュリティを維持するため。

委託先管理に関連する管理策

JIS Q 27001:2023

5.22 供給者のサービス提供の監視、レビュー及び変更管理

管理策

組織は，**供給者**の情報セキュリティの活動及びサービス提供を定常的に監視し，レビューし，評価し，変更を管理しなければならない。

目的

供給者との合意に沿って，合意したレベルの情報セキュリティ及びサービス提供を維持するため。

委託先管理に関連する管理策

JIS Q 27001:2023

8.30 外部委託による開発

管理策

組織は，**外部委託したシステム開発に関する活動**を指揮し，監視し，レビューしなければならない。

目的

組織が要求する情報セキュリティ対策が，外部委託したシステム開発で実施されることを確実にするため。

委託先管理に関連する管理策

JIS Q 27001:2023

組織の能力に影響を与える**外部**の課題

外部から提供されるプロセス，製品又はサービス

供給者の製品又はサービス

供給者関係

サプライチェーン

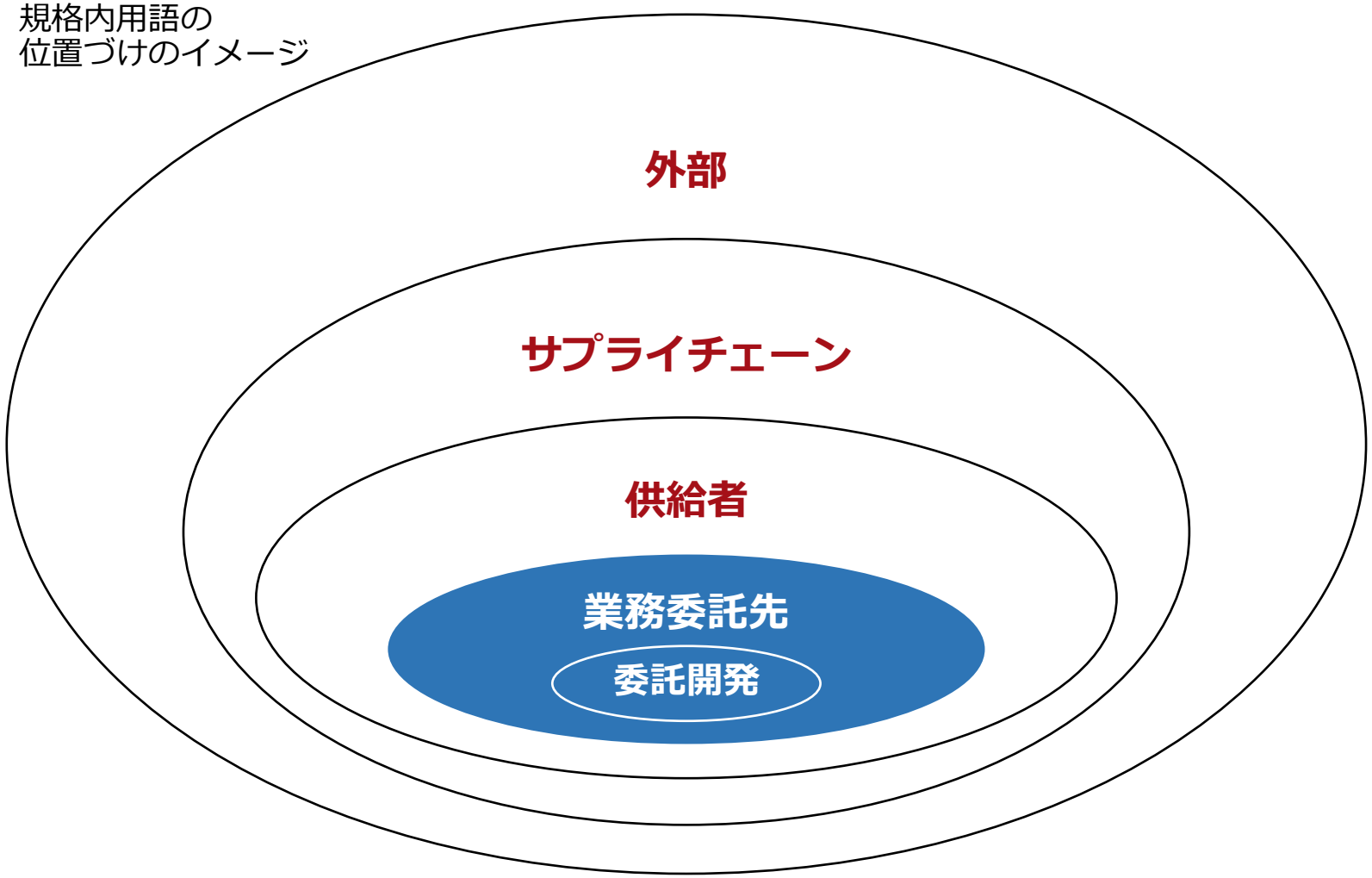
供給者

外部委託したシステム開発に関する活動

業務委託先とは規格における
これらの内枠を
指示している

委託先管理に関連する条文や管理策

規格内用語の
位置づけのイメージ



組織の能力に影響を与える**外部**の課題
外部から提供されるプロセス，製品又はサービス
供給者の製品又はサービス
供給者関係
サプライチェーン
供給者
外部委託したシステム開発に関する活動

本テーマで取り扱う「業務委託先管理」

3.51 外部委託する

ある組織の機能又はプロセスの一部を外部の組織が実施する取決めを行う。

注記

外部委託した機能又はプロセスは、マネジメントシステムの適用範囲内にあるか、外部の組織は、マネジメントシステムの適用範囲外にある。

「業務委託先」の定義

- 業務委託とは、雇用関係のない企業から仕事を委託され、特定の業務を行うことで報酬が支払われる働き方のことを指します。

- 働き方や契約形態を表すワードとしてよく使われる「業務委託」ですが、実は法律上「業務委託契約」という名称の契約は存在しません。民法上の「請負契約」と「委任／準委任契約」の3種の契約が、一般的な総称として「業務委託契約」と呼ばれています。

カオナビサイトより引用

本論における「業務委託先」の定義

- **請負契約**
  成果物の完成と引き換えに依頼主である企業から報酬が支払われる契約形態です。成果物を納品するにあたって、どんな業務を行ったか、何時間働いたかという過程は問われず、成果物が不備なく完成し納品されたかどうかのみが問われます。
  ＜請負契約を結ぶ業務委託の職種例＞
  デザイナー,ライター,プログラマー,コンサルタント(成果物の完成責任あり),営業,警備員,清掃員など
- **委任契約**
  成果物の有無は問わず、法律行為を扱う業務の遂行が求められる契約です。医師の診察や不動産の売買に関する手続きなどが該当します。
  ＜委任契約を結ぶ業務委託の業務例＞
  弁護士,医師,不動産業など
- **準委任契約**
  委任契約の中でも、法律行為に該当しない業務を扱うケースは、準委任契約となります。市場調査やイベント会場での受付業務、エステ施術など、幅広い業務が該当します。
  ＜準委任契約を結ぶ業務委託の職種例＞
  研究・調査業務,コンサルタント(成果物の完成責任なし),受付,美容師,エステティシャンなど

カオナビサイトより引用

本テーマで取り扱う「業務委託先管理」

業務委託先	• **「請負契約」「準委任契約」での発注先となる、法人または個人(フリーランス)が対象**
	  • 業務内容はシステム開発/運用とは限らない
	  • **本論ではクラウドサービスは本テーマ対象から除外します**

管理	• **情報セキュリティ面における、評価や選択によるリスク管理**

クラウドサービスは業務委託か否か

クラウドサービスは業務委託か否か

クラウドサービス上で **個人情報を取り扱う場合**	クラウドサービスで **左記に該当しないもの**
• 約款等で個人情報の取り扱いを明示している場合は、法的に(個人情報の)委託に該当する	• 業務委託として取り扱う否かは、利用組織の基準・判断・解釈に拠る

クラウドサービスは業務委託か否か

個人情報保護委員会 FAQより

Q7-53
個人情報取扱事業者が、個人データを含む電子データを取り扱う情報システムに関して、クラウドサービス契約のように外部の事業者を活用している場合、個人データを第三者に提供したものとして、「本人の同意」(法第 27 条第1項柱書)を得る必要がありますか。または、「個人データの取扱いの全部又は一部を委託」(法第 27 条第5項第1号)しているものとして、法第 25条に基づきクラウドサービス事業者を監督する必要がありますか。

A7-53
クラウドサービスには多種多様な形態がありますが、クラウドサービスの利用が、本人の同意が必要な第三者提供(法第 27 条第1項)又は委託(法第 27 条第5項第1 号)に該当するかどうかは、**保存している電子データに個人データが含まれているかどうかではなく、クラウドサービスを提供する事業者において個人データを取り扱うこととなっているのかどうかが判断の基準**となります。

当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合には、当該個人情報取扱事業者は個人データを提供したことにはならないため、「本人の同意」を得る必要はありません。

また、上述の場合は、個人データを提供したことにならないため、「個人データの取扱いの全部又は一部を委託することに伴って・・・提供される場合」(法第 27 条第5項第1号)にも該当せず、法第 25 条に基づきクラウドサービス事業者を監督する義務はありません。

当該クラウドサービス提供事業者が当該個人データを取り扱わないこととなっている場合の個人情報取扱事業者の安全管理措置の考え方についてはQ7-54 参照。

当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合とは、契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等が考えられます。

クラウドサービスは業務委託か否か

個人情報保護委員会 FAQより

保存している電子データに個人データが含まれているかどうかではなく、**クラウドサービスを提供する事業者において個人データを取り扱うこととなっているのかどうか**が判断の基準となります。

クラウドサービスは業務委託か否か

個人情報の委託に該当するクラウドサービスの例①「kaonavi」

第11条　（保存データの取扱い）

1　お客様が本サービスに保存した全てのデータ及び情報（以下「保存データ」といいます。）は、お客様が保存することにより当社による管理及び取扱いを委託したものとします。

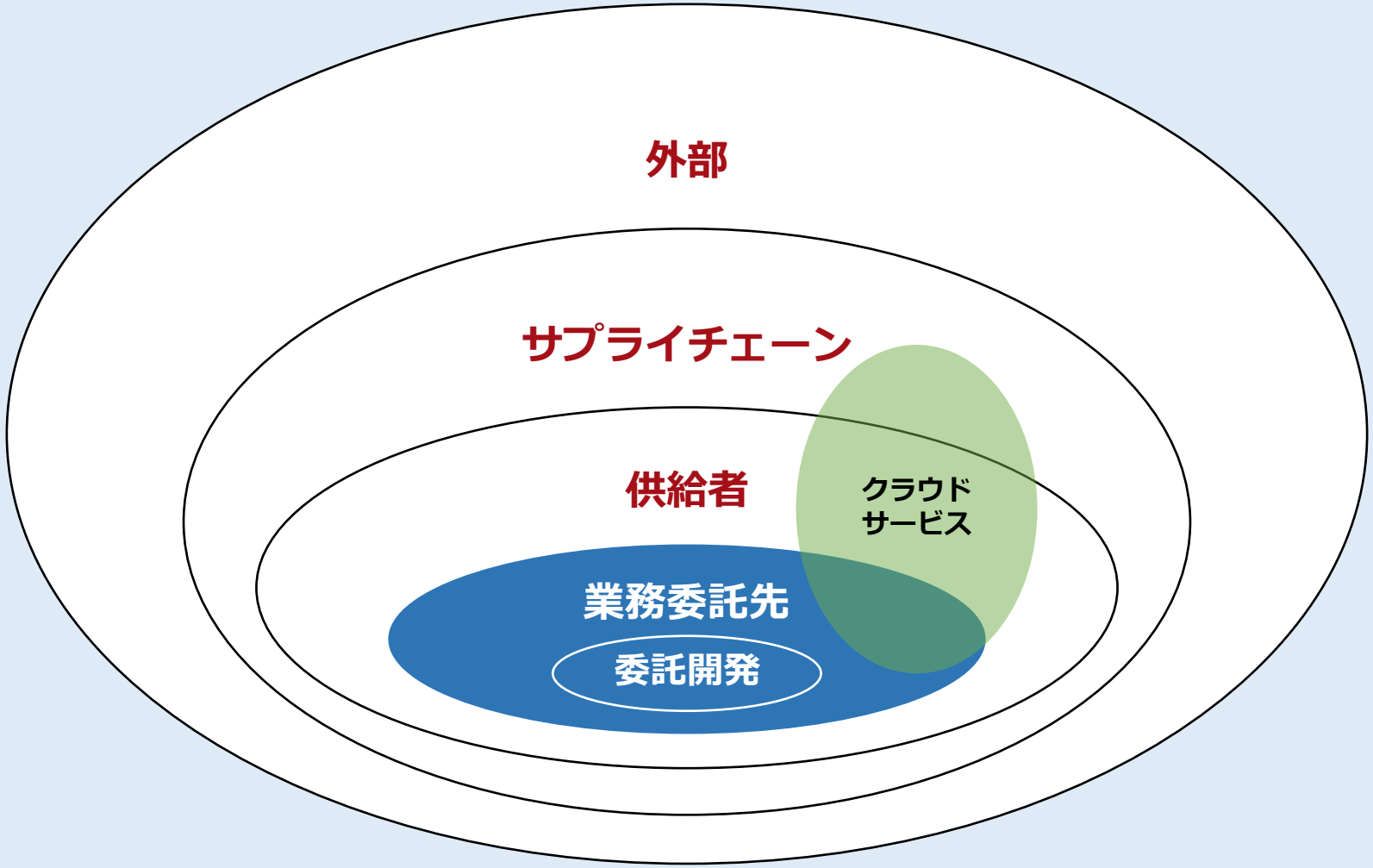
クラウドサービスは業務委託か否か

個人情報の委託に該当するクラウドサービスの例②
「smart HR」

第8条（お客様に関する情報の取扱い等）

1. 当社は、個人データについてはお客様の委託に基づき提供を受けるものとします。お客様が個人データを本サービスにアップロードする等により当社に開示したときは、お客様は、本サービスの利用のために当社に個人データの取扱いを委託したものとします。なお、当社は、お客様の登録データについて、本サービスの不具合対応等の必要性が認められる場合又はお客様の同意がある場合を除きアクセスしないものとします。

クラウドサービスは業務委託か否か



他の規格やガイドライン、フレームワークでの「委託先管理」に該当する事項

IPA 中小企業の情報セキュリティ対策ガイドライン

他の規格やガイドライン、フレームワークでの「委託先管理」に
該当する事項

IPA 中小企業の情報セキュリティ対策ガイドライン第3.1版

経営者は何をやらなければならないのか • 委託先の情報セキュリティ対策まで考慮する • 委託や外部サービス利用の際にはセキュリティに関する責任を明確にする	
規程サンプル 9 委託管理	1.委託先評価基準 2.委託先の選定 3.委託契約の締結 4.委託先の評価 5.再委託

IPA 中小企業の情報セキュリティ対策ガイドライン第3.1版

中小企業の情報セキュリティ対策ガイドライン 付録5 情報セキュリティ関連規程(サンプル)

9-1 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。

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	

在宅勤務やクラウドファースト時代に、対応していない確認項目もあるような・・・

個人情報の保護に関する法律についてのガイドライン

他の規格やガイドライン、フレームワークでの「委託先管理」に
該当する事項

3-4-4 委託先の監督

適切な委託先の選定	委託先の選定に当たっては、委託先の安全管理措置が、少なくとも法第23条及び本ガイドラインで委託元に求められるものと同等であることを確認するため、「10((別添)講ずべき安全管理措置の内容)」に定める各項目が、委託する業務内容に沿って、確実に実施されることについて、あらかじめ確認しなければならない。
委託契約の締結	委託契約には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を委託元が合理的に把握することを盛り込むことが望ましい。
委託先における 個人データ取扱状況の把握	委託先における委託された個人データの取扱状況を把握するためには、定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。

NIST SP800-53
組織と情報システムのためのセキュリティおよびプライバシー管理策

他の規格やガイドライン、フレームワークでの「委託先管理」に該当する事項

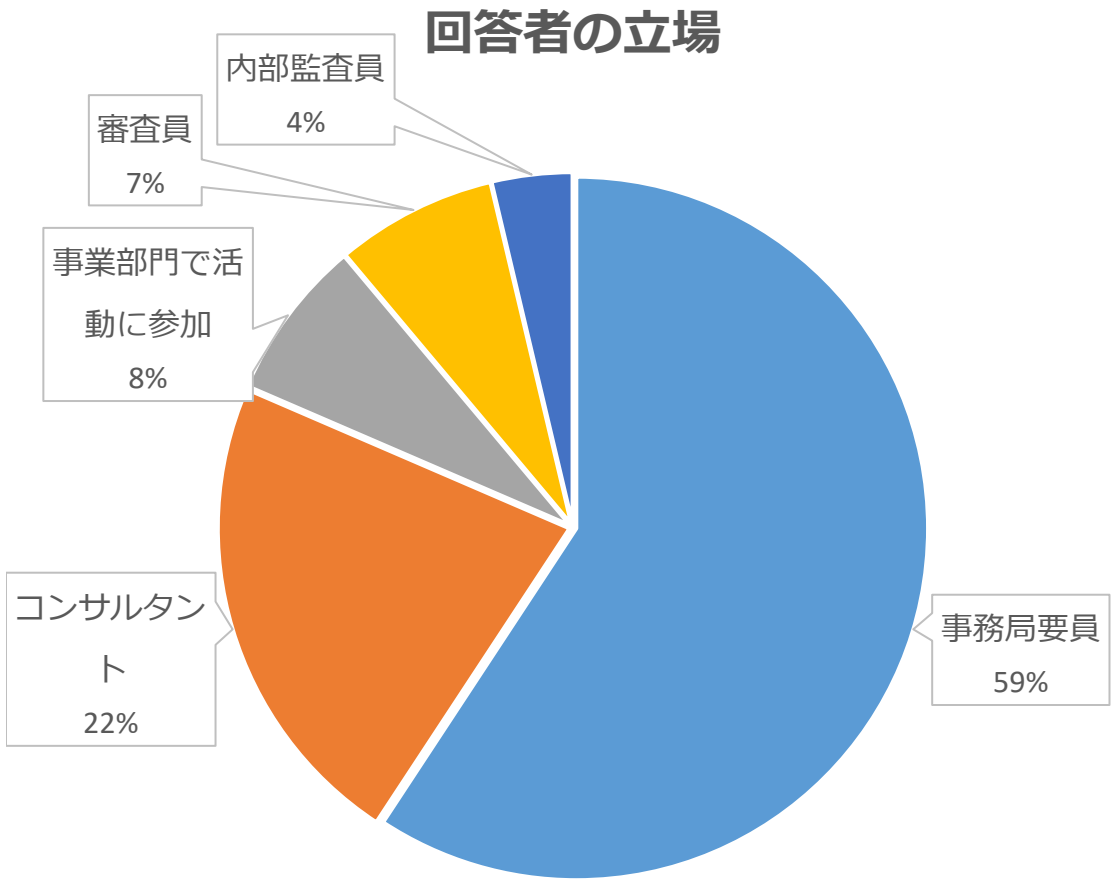
3.20 サプライチェーンのリスクマネジメント	
a	策定、文書化し、対象者に配布する
b	サプライチェーンのリスクマネジメントのポリシーと手順の策定、文書化、および配布することを管理するために、担当者を指定する
c	現行のサプライチェーンのリスクマネジメントをレビューし、更新する

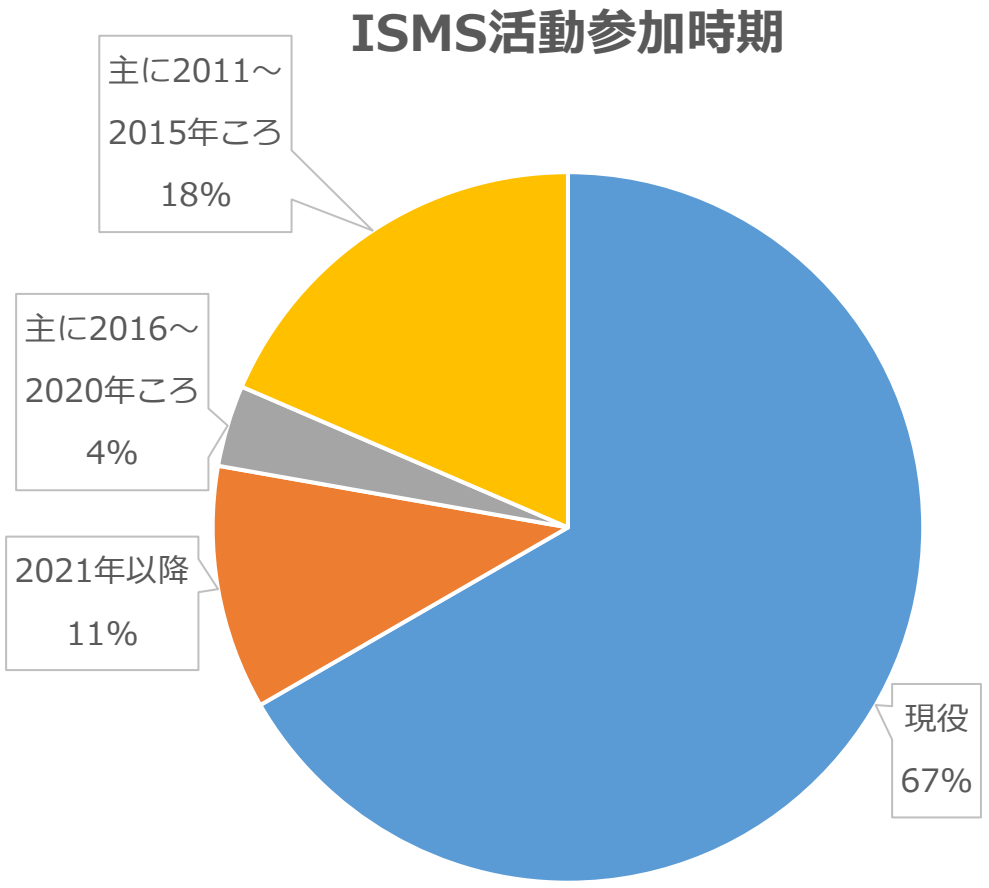
NIST SP800-53A
セキュリティコントロールを評価するアセスメントのガイドライン

SR-06 サプライヤーの評価とレビュー		
判断基準	SR-06_ODP	供給業者や契約者、および彼らが提供するシステム、システムコンポーネント、またはシステムサービスに関連するサプライチェーンリスクを評価およびレビューする頻度が定義されているかどうかを判断する。
	DS-SR-06	供給業者や契約者、および彼らが提供するシステム、システムコンポーネント、またはシステムサービスに関連するサプライチェーンリスクが、前項の頻度で評価およびレビューされているかどうかを判断する
評価方法	SR-06 調査	以下から選択: サプライチェーンリスク管理ポリシーと手順; サプライチェーンリスク管理戦略; サプライチェーンリスク管理計画; システムおよびサービス取得ポリシー; サプライチェーン保護に関する手順; 取得プロセスへの情報セキュリティ要件の統合に関する手順; 供給業者のデューデリジェンスレビューの記録; システムセキュリティ計画; その他関連する文書または記録
	SR-06 インタビュー	以下から選択: システムおよびサービス取得の責任を持つ組織の担当者; 情報セキュリティの責任を持つ組織の担当者; サプライチェーン保護の責任を持つ組織の担当者
	SR-06 テスト	以下から選択: 供給業者レビューを実施するための組織のプロセス; 供給業者レビューをサポートおよび/または実施するためのメカニズム

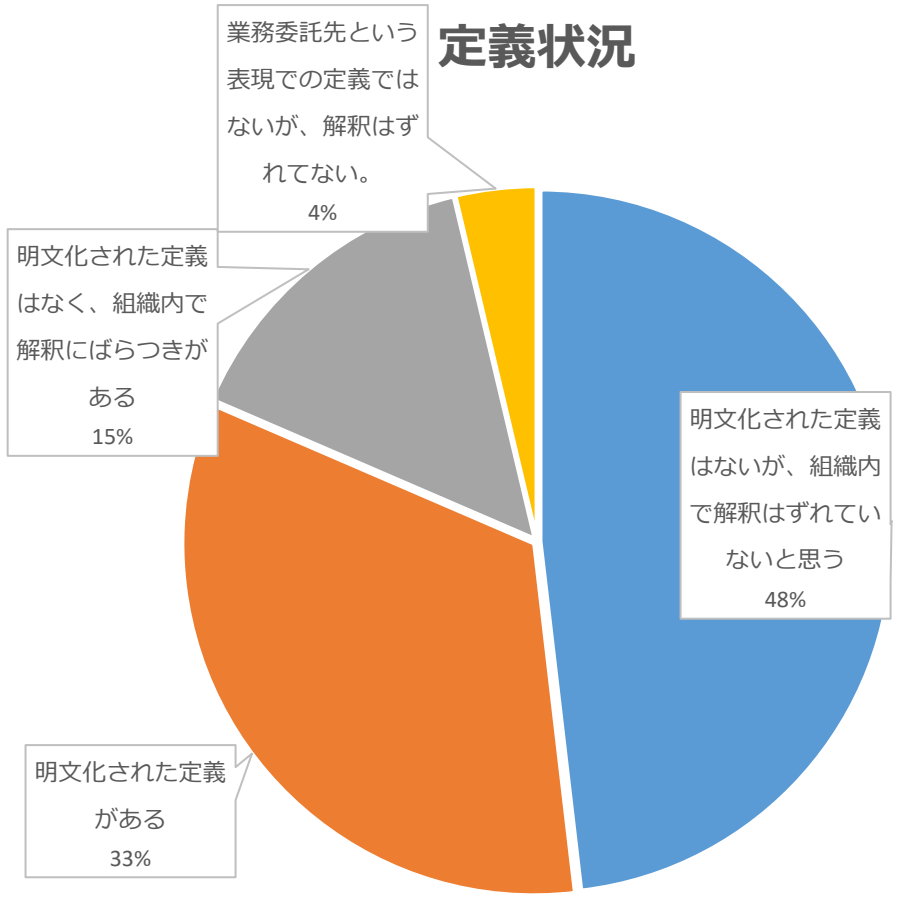
研究会メンバーからの情報

回答者プロフィール





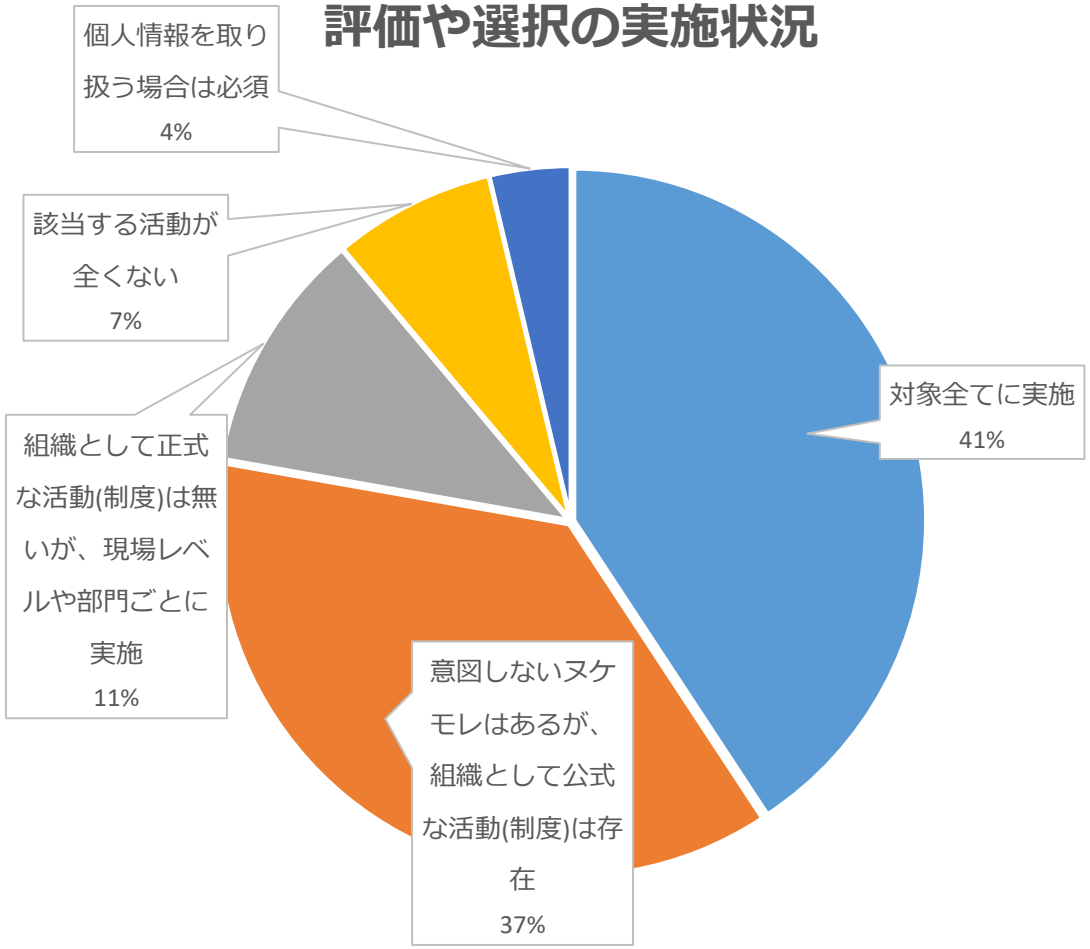
「業務委託先」の定義



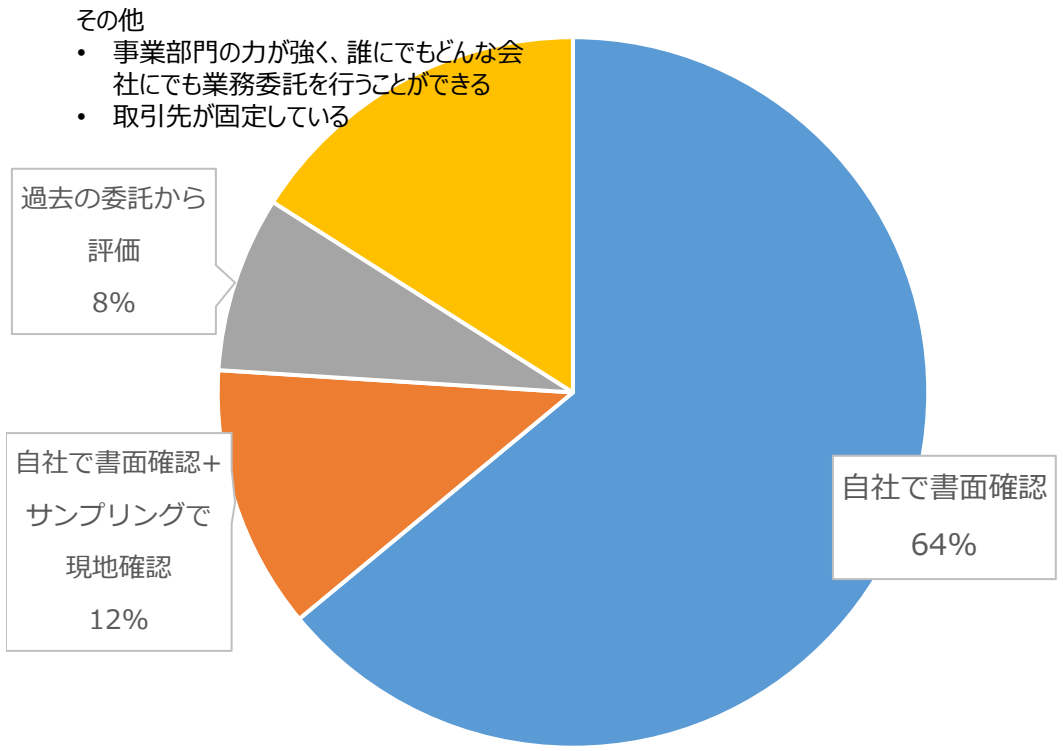
明文化された「業務委託先」定義の例	
1	• 会社が管理責任を持つ情報資産を預託する外部組織 • 会社が管理責任を持つ情報資産にアクセスする権限を持つ第三者 • 会社が管理責任を持つ情報資産の保管場所、保存場所にアクセスする権限を持つ第三者 • 情報セキュリティに関する業務の一部または全部を委託する外部組織 • 情報システムの開発、変更、運用、保守を委託する外部組織 • 会社の情報資産が移送、保存されるインフラストラクチャ、プラットフォームを提供、管理する外部組織
2	企業秘密管理規程に定める企業秘密を取り扱う業務のうち、当社が当該業務の実施を子会社以外の第三者に委託するものをいう
3	当社または子会社が業務を委託する、当社および子会社以外の会社および会社以外の団体等をいう
4	社外に業務を委託し、契約に基づき成果物を納品するまたは、業務（稼働）を提供いただく

評価や選択の実施状況/方法

評価や選択の実施状況

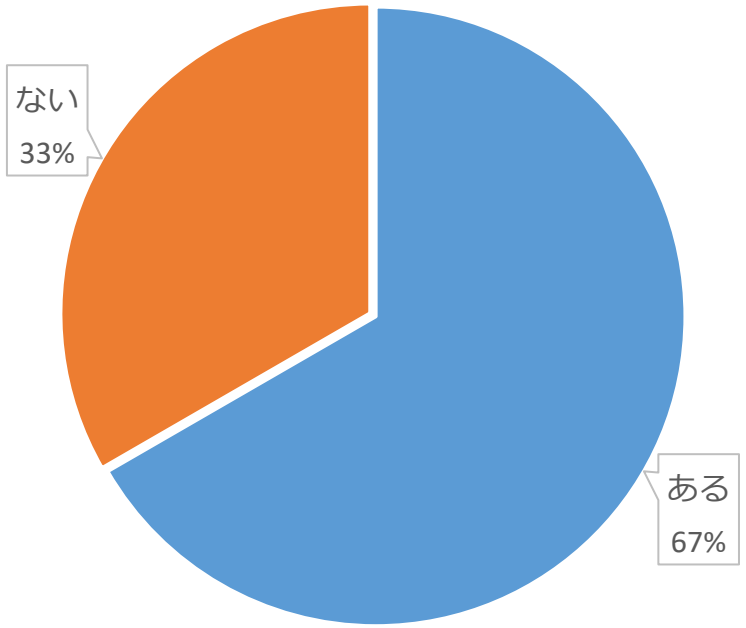


評価や選択の方法



評価や選択の差異

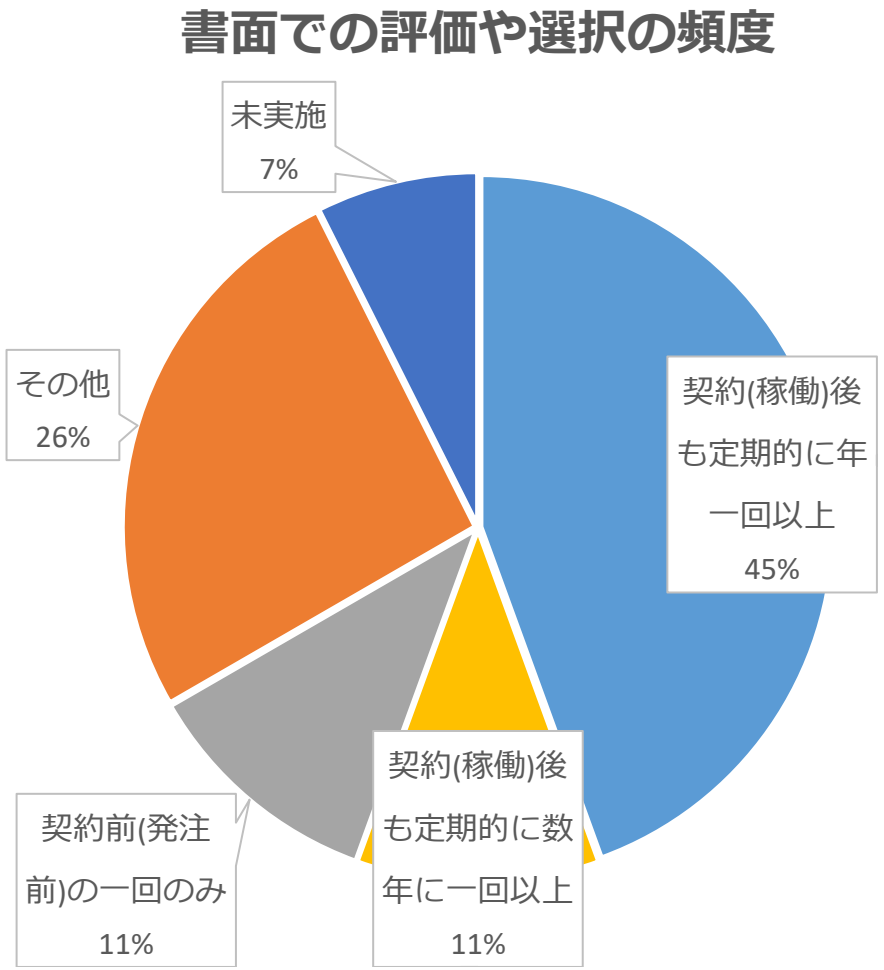
取り扱う情報レベルで、チェック内容や方法に差異はありますか？



「ある」場合の事例

- 個人情報や秘密情報の預託が発生しない場合は、チェックから除外
- 刑法134条(秘密漏示)が適用される委託先の場合は、チェックから除外
  - 医師、薬剤師、医薬品販売業者、助産師、弁護士、弁護人、公証人
- ISMS認証取得の場合は、チェック項目を一部除外

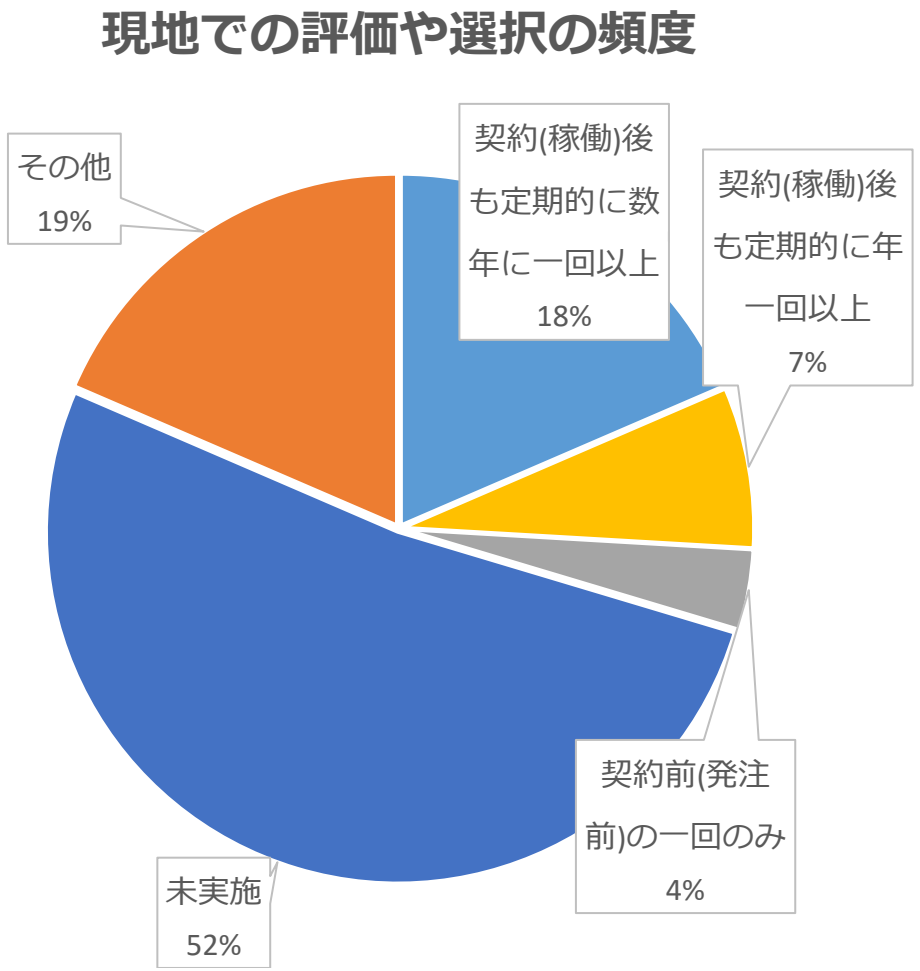
評価や選択の頻度 (書面)



その他の事例

- サンプリングで評価
- 委託先の納品手続きの中で評価する
- 個人情報や会社の機密を扱う場合、委託先の重要性変更の発生の都度
- 「秘密保持契約書」の締結をもって評価と見做す
- 組織の担当者がしっかりしているところは、毎年、実施するが、めんどくがっている担当者は言っても実施しない。

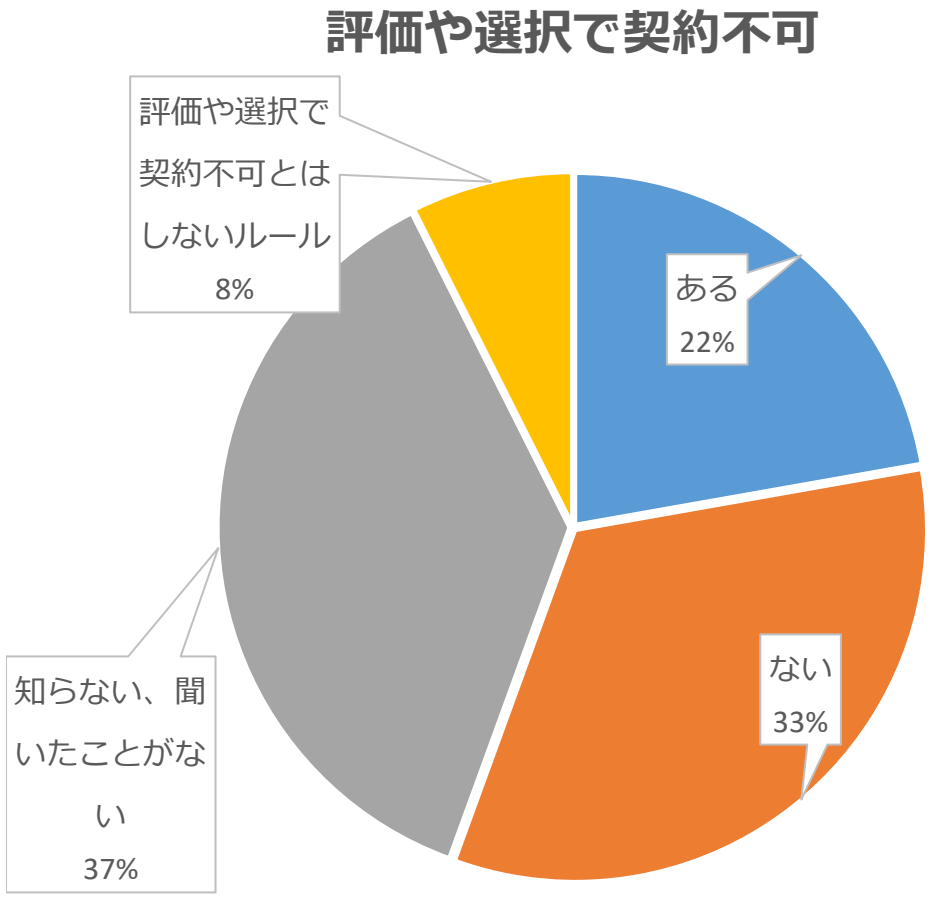
評価や選択の頻度 (現地)



その他の事例

- 契約内容には現地訪問について触れているが、現時点では実施無し
- 個人情報や会社の機密を扱う場合、委託先での事故発生の度合いにより
- 事故や同業界の事故事例など、自社にとって脅威が高いとされる状況が生じ、経営層が課題認識に至る場合に

評価や選択で契約不可とした例

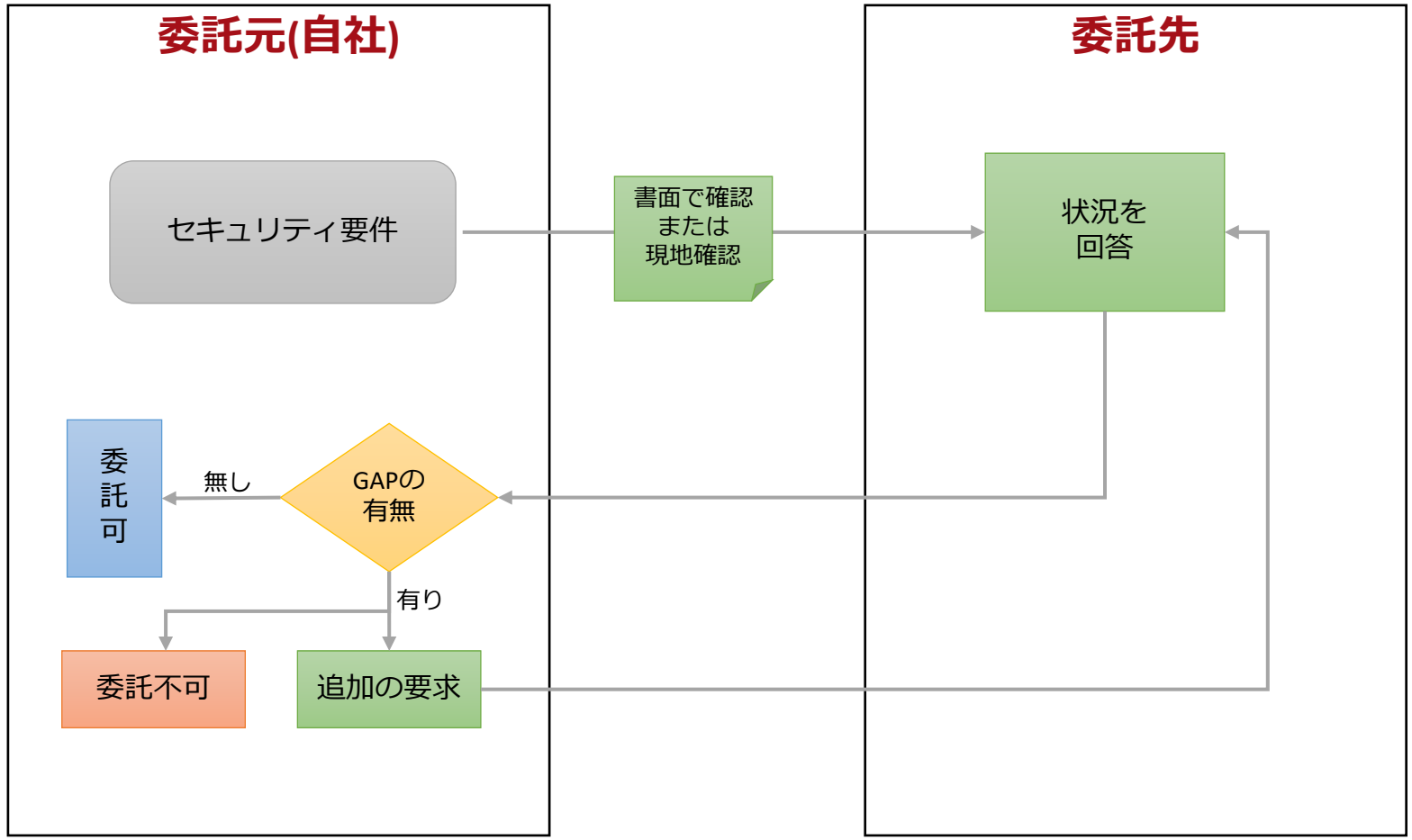


「ある」の事例

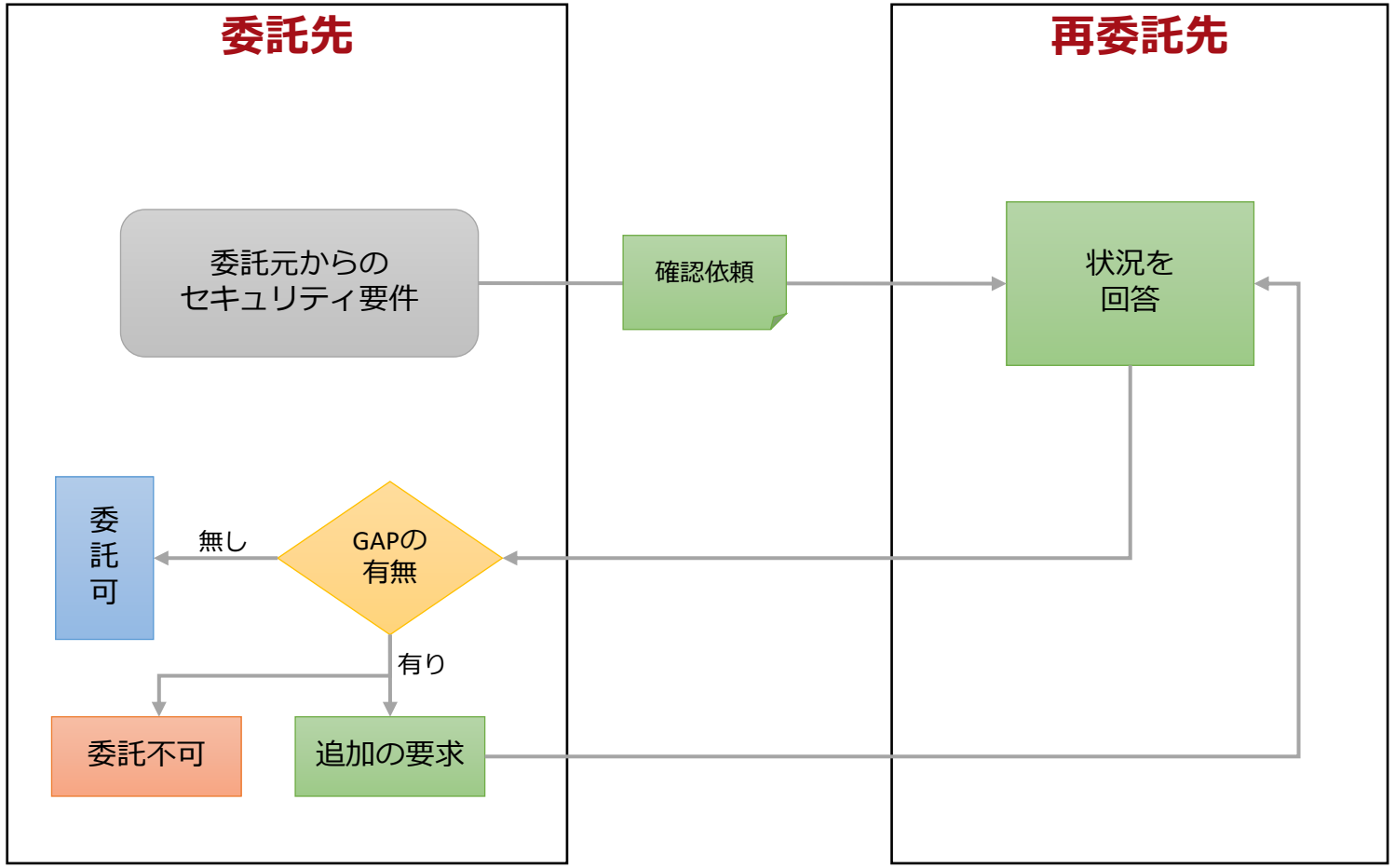
- 不合格となった取引先へは、その旨を通知し、期限を設けて不足部分を対応していただき調達部門がそれを確認（書面可）できた場合に、合格としている。
- ルールや秘密保持契約を守れない場合、最初は契約できていた場合でも、発注できないランクとなり、実質契約不可と同等となる。

- 現地監査に行った結果、セキュリティが保てる環境ではなかったため。開発委託先が木造アパートの一室で侵入を防ぐことも、温度管理もできていなかったということを聞いたことがあります。

評価や選択

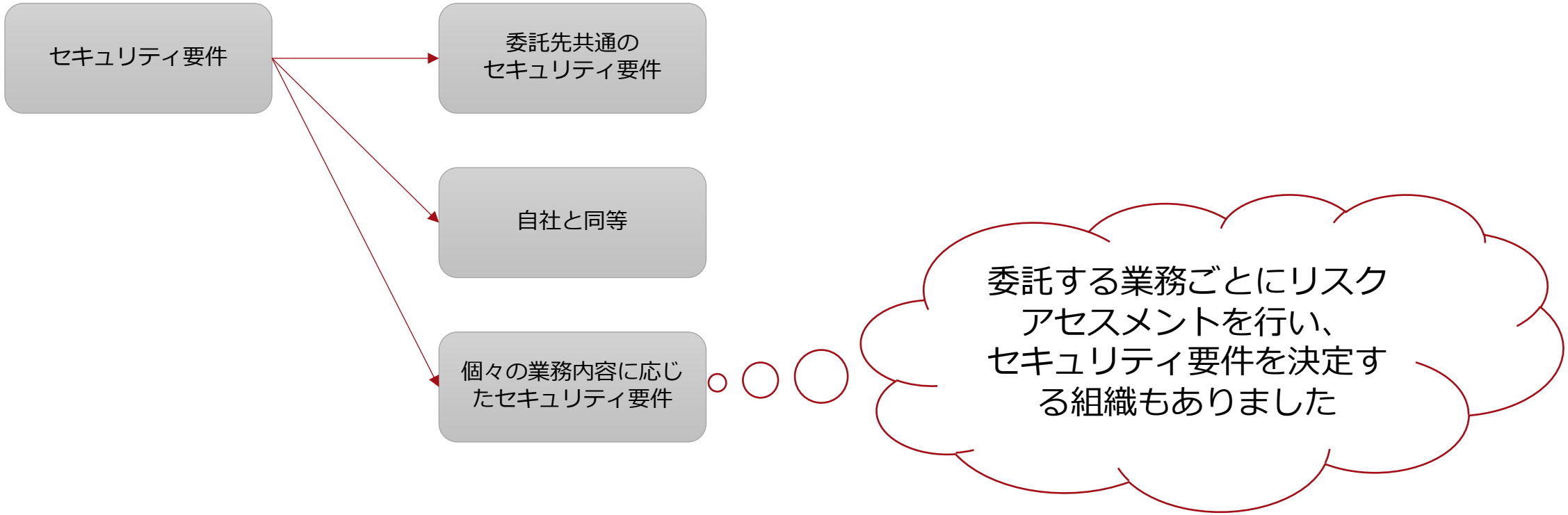


評価や選択



評価や選択

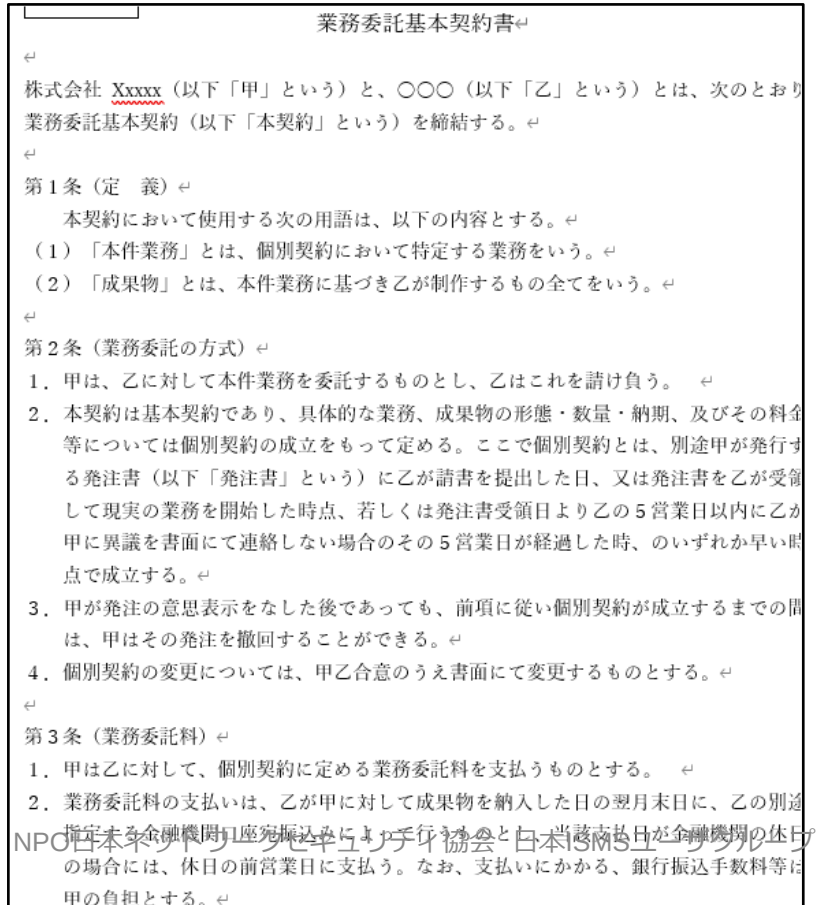
委託先に求めるセキュリティ要件の例



業務委託契約書の記載項目例

情報セキュリティの観点で、委託先と取り交わす
「業務委託基本契約書」にあると望ましい項目

- 秘密保持
- PC等のセキュリティ対策
- 監査権
- 再委託



業務委託基本契約書

株式会社 Xxxxx（以下「甲」という）と、○○○（以下「乙」という）とは、次のとおり業務委託基本契約（以下「本契約」という）を締結する。

第１条（定　義）
本契約において使用する次の用語は、以下の内容とする。
（１）「本件業務」とは、個別契約において特定する業務をいう。
（２）「成果物」とは、本件業務に基づき乙が制作するもの全てをいう。

第２条（業務委託の方式）
１．甲は、乙に対して本件業務を委託するものとし、乙はこれを請け負う。
２．本契約は基本契約であり、具体的な業務、成果物の形態・数量・納期、及びその料金等については個別契約の成立をもって定める。ここで個別契約とは、別途甲が発行する発注書（以下「発注書」という）に乙が請書を提出した日、又は発注書を乙が受領して現実の業務を開始した時点、若しくは発注書受領日より乙の５営業日以内に乙が甲に異議を書面にて連絡しない場合のその５営業日が経過した時、のいずれか早い時点で成立する。
３．甲が発注の意思表示をなした後であっても、前項に従い個別契約が成立するまでの間は、甲はその発注を撤回することができる。
４．個別契約の変更については、甲乙合意のうえ書面にて変更するものとする。

第３条（業務委託料）
１．甲は乙に対して、個別契約に定める業務委託料を支払うものとする。
２．業務委託料の支払いは、乙が甲に対して成果物を納入した日の翌月末日に、乙の別途指定する金融機関口座宛振込みにより行うものとし、当該支払日が金融機関の休日の場合には、休日の前営業日に支払う。なお、支払いにかかる、銀行振込手数料等は甲の負担とする。

業務委託契約書の記載項目例

秘密保持に関する条項で記載が望ましい項目

1	秘密情報の定義
2	法令に基づく開示要求への対応
3	秘密情報の契約(開示目的)内のみでの利用
4	秘密情報の無許可の開示や漏洩の禁止、秘密情報を利用した製品サービスの提供禁止
5	秘密情報の承諾なき複製改変や解析の禁止
6	無断開示・第三者提供した場合の被害賠償
7	契約終了完了時の返却・廃棄と、その証明の提出
8	秘密保持義務の契約終了後の有効期間
9	監査権(報告又は立ち入り)
10	所轄裁判所

業務委託契約書の記載項目例

PC等のセキュリティ対策に関する条項で記載が望ましい項目

1	PCのセキュリティ対策 ・委託元から貸与するPCに行うセキュリティ対策 ・委託先PCを使う場合のセキュリティ対策 ・委託先PCを使う場合、委託元の事前の承諾 ・委託元環境へのアクセス権設定責任	5	委託先PC起因での委託元IT環境の障害に対する賠償責任
2	アクセス履歴取得への承諾	6	委託元IT環境下での委託先PC障害時に責任を負わない
3	禁止行為 ・セキュリティ対策の無効化 ・意図的なコンピュータウィルスの混入 ・業務に無関係なサイトへのアクセス ・故意に委託元へのアクセスと拡散行為	7	作業場所の指定、制限
4	委託元のセキュリティ対策に不備がある事に気づいた場合の通知	8	委託元が貸与したPCの第三者への貸出禁止

業務委託契約書の記載項目例

監査権に関する条項で記載が望ましい項目

1	(セキュリティ面を含む)本契約上の遂行状況や遵守状況を確認するため、監査が出来る
2	報告書や資料の提出を求めることが出来る
3	改善を求めることができ、受託者は直ちに応じるものとする
4	再委託先についても同様

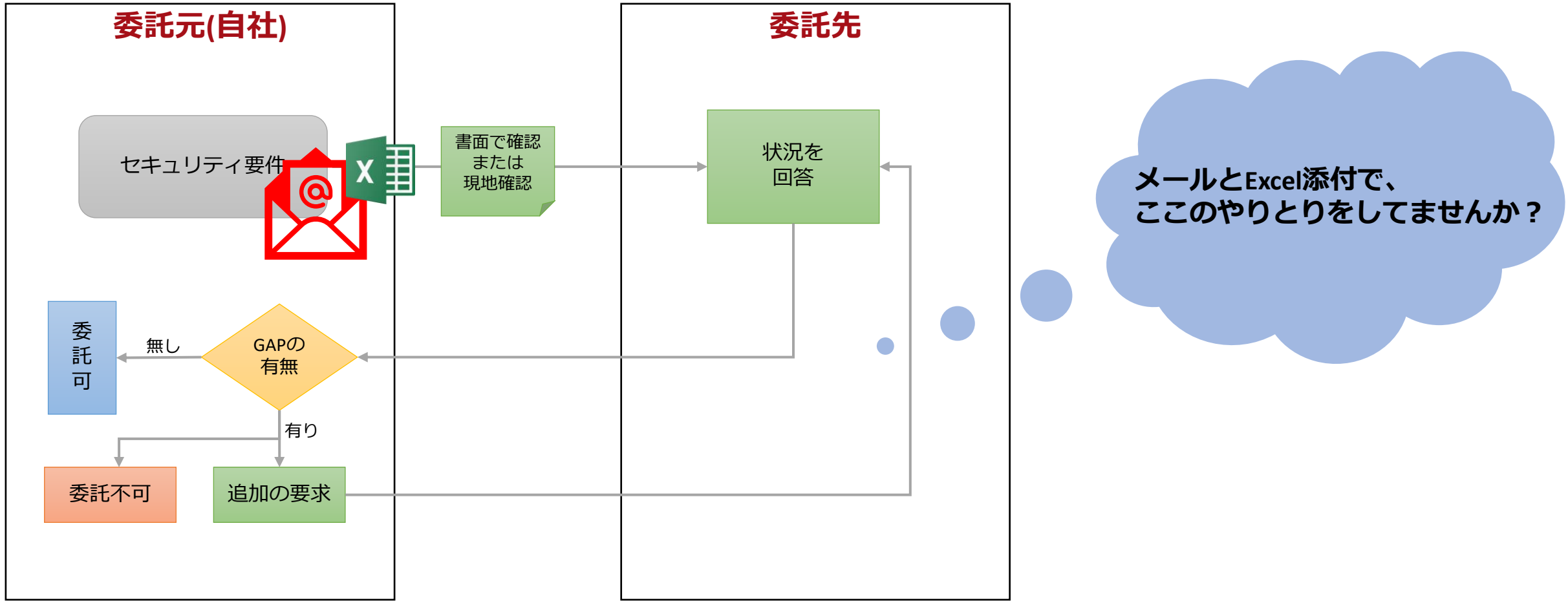
業務委託契約書の記載項目例

再委託に関する条項で記載が望ましい項目

1	再委託の事前承認、または禁止
2	再々委託の制限、または禁止
3	(委託先の)再委託先の監督義務 ・義務にはセキュリティ要求事項が含まれる ・本契約と同等のセキュリティ対策の実施 ・監査権(報告又は立ち入り)

委託先管理のDX

委託先管理のDX



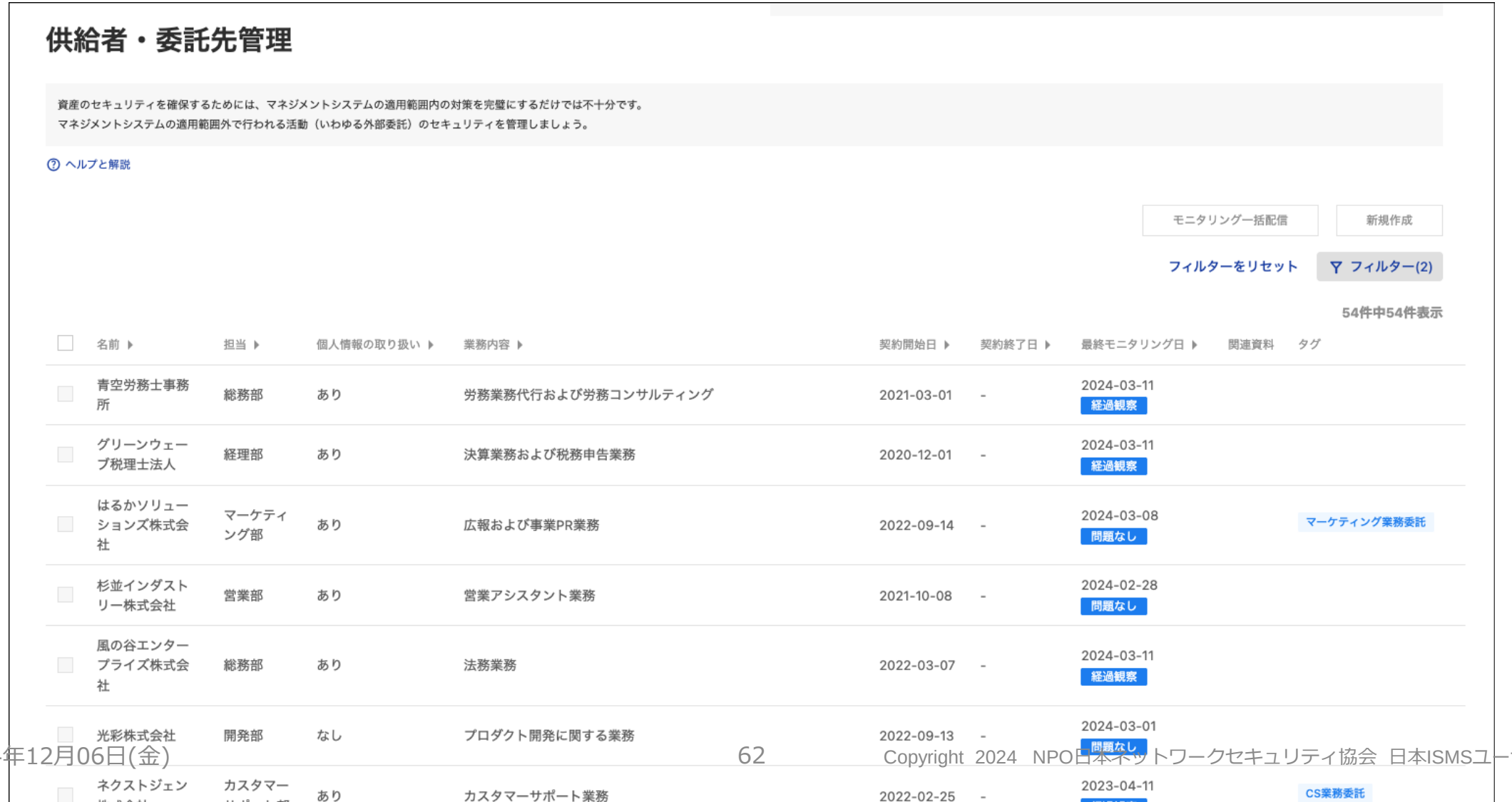
委託先管理SaaSの例

	SecureNavi	セキュリオ	Conoris BP
特徴	ISMS・Pマーク運用自動化ツールの 一機能として委託先管理機能	情報セキュリティ教育サービスが主で 委託先管理機能もあり	委託先管理に特化 再委託も管理可能 大企業向け

委託先管理SaaSの例

		SecureNavi	セキュリオ	Conoris BP
概要		ISMS・Pマーク運用自動化ツール	情報セキュリティ教育サービス	委託先管理に特化
特徴		委託先管理を含むISMS・Pマークの要求事項に効率的に対応	オプションとして委託先管理機能	再委託先管理機能・チェックシート回答での承認機能
機能	委託先管理(マスター)	自社独自のマスターを作成可能	自社独自のマスターを作成可能	国内法人データベースと連携し、法人マイナンバーベースの委託先マスタ管理が可能。
	Webでのチェックシート	○	○	○
	チェックシートのテンプレート	・3種類の標準テンプレートが利用可能 ・新規オリジナルシートも作成可能	・23種類のテンプレートが利用可能（Pマーク対応済） ・柔軟なチェックシート作成や評価が可能 ・7業界＋個人事業主（契約社員）に特化したテンプレート有 ・新規オリジナルシート作成やCSVインポートも可能	・複数のテンプレートがデフォルトで利用可能（ISMS基準含む） ・金融や自動車など業界に特化したテンプレート有 ・カスタマイズも可能
	依頼メールの発信	・作成したチェックシートを任意のタイミングで先方の担当者に依頼メール発信 ・複数の委託先に、一括で依頼メールの発信が可能	・作成したチェックシートを任意のタイミングで先方の担当者に依頼メール発信 ・複数人の担当者へ送信可能	・システム上で申請書提出時に自動で次の担当者に依頼メール発信 ・担当者にリマインドメールを自動送信
	再委託先管理	機能なし	・第三者委託している委託先を絞り込める	委託先への再委託先管理の委任または委託元から再委託先、再々委託先へのwebでのチェックシート送付・回収と管理
料金		月額数万円～　※個別見積もり （委託先管理だけではなく、リスクアセスメントや内部監査など、ISMS・Pマーク運用に必要なすべての機能が利用可能）	・EPスタンダードプラン（利用ユーザー50名以上） 360円/月/ユーザー ＋オプション機能：15,000円 初期費用：無し	ライトプラン（管理対象社数50社以内）60,000円 / 月 ～＋初期費用 ※ユーザーアカウント数による課金なし
想定ターゲット		ISMS/Pマーク取得企業向け	ISMS/Pマーク取得企業向け	大企業向け
		https://secure-navi.jp/	https://www.lrm.jp/seculio/	https://www.conoris.jp/conoris-bp

委託先台帳 –Secure Naviの場合-



供給者・委託先管理

資産のセキュリティを確保するためには、マネジメントシステムの適用範囲内の対策を完璧にするだけでは不十分です。
マネジメントシステムの適用範囲外で行われる活動（いわゆる外部委託）のセキュリティを管理しましょう。

ヘルプと解説

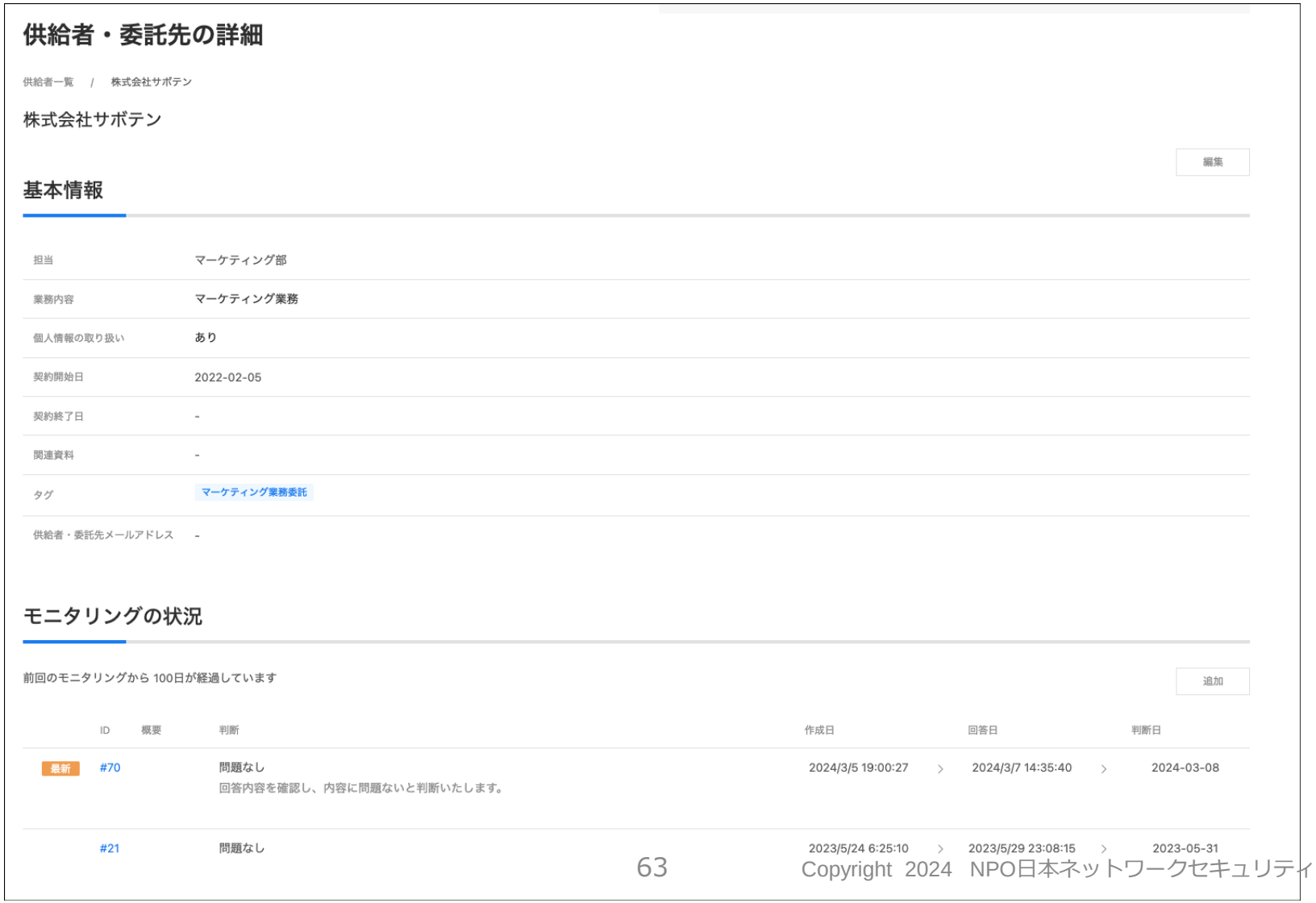
モニタリング一括配信　新規作成

フィルターをリセット　フィルター(2)

54件中54件表示

名前	担当	個人情報の取り扱い	業務内容	契約開始日	契約終了日	最終モニタリング日	関連資料	タグ
青空労務士事務所	総務部	あり	労務業務代行および労務コンサルティング	2021-03-01	-	2024-03-11 経過観察		
グリーンウェーブ税理士法人	経理部	あり	決算業務および税務申告業務	2020-12-01	-	2024-03-11 経過観察		
はるかソリューションズ株式会社	マーケティング部	あり	広報および事業PR業務	2022-09-14	-	2024-03-08 問題なし		マーケティング業務委託
杉並インダストリー株式会社	営業部	あり	営業アシスタント業務	2021-10-08	-	2024-02-28 問題なし		
風の谷エンタープライズ株式会社	総務部	あり	法務業務	2022-03-07	-	2024-03-11 経過観察		
光彩株式会社	開発部	なし	プロダクト開発に関する業務	2022-09-13	-	2024-03-01 問題なし		
ネクストジェン	カスタマー	あり	カスタマーサポート業務	2022-02-25	-	2023-04-11		CS業務委託

委託先台帳 -SecureNaviの場合-



供給者・委託先の詳細

供給者一覧 / 株式会社サポテン

株式会社サポテン

編集

基本情報

担当	マーケティング部
業務内容	マーケティング業務
個人情報の取り扱い	あり
契約開始日	2022-02-05
契約終了日	-
関連資料	-
タグ	マーケティング業務委託
供給者・委託先メールアドレス	-

モニタリングの状況

前回のモニタリングから 100日が経過しています

追加

	ID	概要	判断	作成日	回答日	判断日
最新	#70		問題なし 回答内容を確認し、内容に問題ないと判断いたします。	2024/3/5 19:00:27	2024/3/7 14:35:40	2024-03-08
	#21		問題なし	2023/5/24 6:25:10	2023/5/29 23:08:15	2023-05-31

委託先アンケート –Secure Naviの場合-

供給者モニタリング

供給者一覧 / 株式会社サボテン / モニタリング

このモニタリングを削除

概要

編集

ステップ1：回答を依頼する（もしくは自社で回答する）

外部公開URLを発行し、SecureNaviのアカウントを持たない供給者に対して、質問への回答を依頼することができます。
一度発行したURLは、いつでも無効化することができます。

外部共有を有効化

外部公開URLを共有する
以下のURLを、回答を依頼する人に共有してください。

https://

回答を依頼するメールを送る
SecureNaviから、回答を依頼するメールを送ることもできます。

メール送信画面を開く

ステップ2：回答をもとに判断する

山田一郎　によって、 2024/3/7 14:35:40 に回答されました。

#	質問	回答	コメント
1	パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	はい	
2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル（コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれる） は最新の状態にしていますか？	はい	
3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	はい	
4	重要情報（営業秘密など事業に必要で組織にとって価値のある情報や顧客や従業員の個人情報など管理責任を伴う情報のこと）に対する適切な取り扱い	はい	

委託先アンケート –Secure Naviの場合-

情報セキュリティアンケートへのご協力のお願い

SecureNavi株式会社から、株式会社サボテン様に対して、以下の情報セキュリティアンケートへの回答依頼が届いています。

このアンケートはすでに回答されています。ご協力ありがとうございました。

山田一郎　によって、 2024/3/7 14:35:40 に回答されました。

#	質問	回答	コメント
1	パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	はい	
2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル（コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれる） は最新の状態にしていますか？	はい	
3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	はい	
4	重要情報（営業秘密など事業に必要で組織にとって価値のある情報や顧客や従業員の個人情報など管理責任を伴う情報のこと）に対する適切なアクセス制限を行っていますか？	はい	
5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	部分的にはい	
6	電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつけていますか？	はい	
7	電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施していますか？	はい	

【参考】委託先管理に関連するインシデント事例など

解決策は特に示していないので、
「他山の石」として、リスクアセスメントのネタにご利用ください。

事件事故の類

お客様が再委託要員に 直接指示した内容が不適切	SIerでの事例。 お客様が再委託先要員に誤ったシステム設定作業を直接指示(具体的にはポートの開放)し、それが原因で外部から侵入された。
委託先のセキュリティ責任者が PCを飲酒紛失	紛失当事者は委託業務での業務従事者では無かったが、従事者の上司だったためPJのMLに入っており、委託業務関係情報が受信メールに蓄積されていた。 さらに、紛失当事者は委託先会社のセキュリティ責任者で特権があり、PCの暗号化を独断で解除していた。
委託先社員が ICカード入館証を紛失	数か月に一度しか出社しない要員だったため、発覚するまでに時間を要した。
委託先PCから社内への感染拡大	委託先PCがランサムウェアに感染。 社内ネットワークに接続して作業していたため、全社に感染拡大。 再発防止策として、委託先(再委託先含む)の使用するPCは全て貸与に変更。

評価や選択での不備

書面点検での回答不備	書面回答に「ISMS認証取得済み」とあったが、ISMS-ACサイトで確認したところ、委託先の部門は認証登録範囲外であった。 委託先担当者に「認証登録範囲」の概念を理解してもらえず、回答修正が叶わなかった。
書面点検が回答困難	委託元から送付されてきたセキュリティ状況チェックの各設問がオープンクエスチョン形式で、どんな回答が適切なのか想定が困難であった。 他には、社内用語や業界特有の用語多用で、質問意図が理解できない例など。
書面点検内容の陳腐化	質問(点検)項目が数年間見直されておらず、リモートワークやクラウドサービス利用等が全く考慮されていないため、実情に見合った回答が困難。

最後に

最後に

今回お届けした情報が、皆さんの組織での業務委託先管理の、継続的改善の一助になれば本望です。