資料５－１

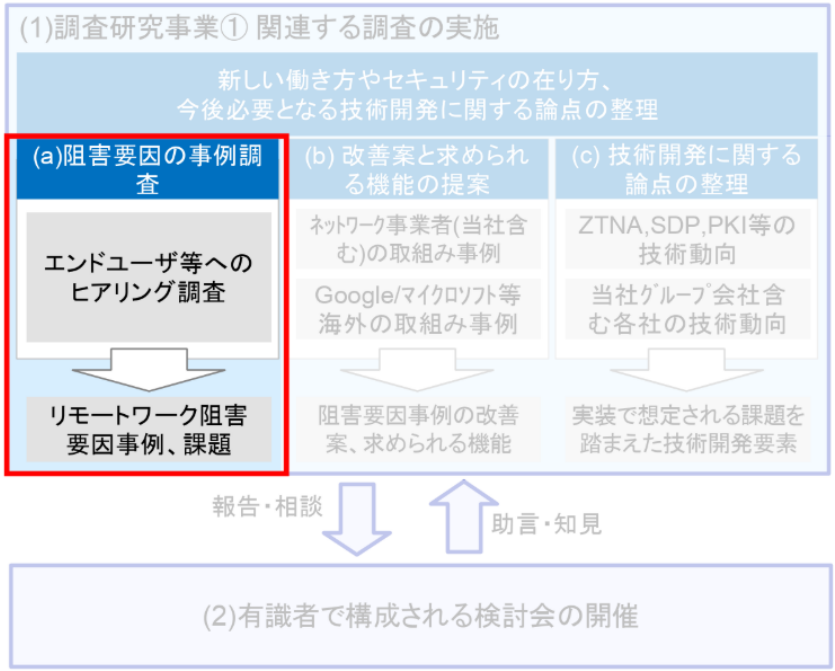
「(a) 阻害要因の事例調査」の実施方法

SoftBank

1）概要

セキュリティ要件整理のため、リモートワークという切り口から、リモートワークが阻害されている要因、又はリモートワークの実現に伴い妥協している点、リモートワークやクラウド環境における内部不正の懸念点などについて、チェックシートによる定量調査およびヒアリングによる定性調査の両面から調査を実施する。

またヒアリングに加えて、事件事例の調査からの課題抽出も行う。最終的にヒアリングの結果と調査結果、提起された課題を集計し、洗い出された阻害要因についてまとめる。



ヒアリング対象の要件確定

- 本調査では経済安全保障の観点から、懸念組織等への流出を防ぐ必要がある秘匿性の高い情報（漏洩した場合、産業上または安全保障上のリスクとなる設計図面や社内ネットワークの構成情報など）を保有し、リモートワークにおいてもその情報を扱う可能性のある組織に対してヒアリングによる調査協力を依頼し、ヒアリングを実施する。
- ヒアリング対象は、我が国全体への影響を鑑み、情報が漏洩した場合に秘匿性が高く、産業上または安全保障上のリスクとなる重要インフラ事業や金融業、重要システムを開発するシステム開発会社、主要産業、かつ リモートワークの機会も多いと思われる大企業から5社以上を選定予定。
- 併せて、建設現場のようなリモートが前提となる分散した拠点がある企業を選定予定。

選定基準

業界	社数（予定）	大企業		分散拠点
		資本金	従業員数	
金融、製造業、建設業、運輸業、その他の業種	2	3億円超過	300人超過	有
卸売業・小売業	1	1億円超過	100人超過	
サービス業	2	5000万円超過	100人超過	
小売業	1	5000万円超過	50人超過	

ヒアリング対象

ヒアリング先選定基準に沿って、弊社を含む以下9社をヒアリング対象として選出し、ヒアリングを実施。（一部ヒアリング先は、企業名非公開の要望あり）

ヒアリング候補	業種	資本金 [百万円]	従業員数	分散拠点
ソフトバンク株式会社	情報・通信	204,309	17,300	有
SHIFT株式会社	情報・通信	67	3829	有
イオンアイビス株式会社※1	小売 / 情報	490	360	有
パロアルトネットワークス株式会社 ※2	セキュリティ	248,512	8,014	有
シャープ株式会社	製造	5,000	51,402	有
株式会社バローホールディングス	小売	13,609	8,168	有
A社	（秘匿情報）	（秘匿情報）	（秘匿情報）	有
B社	（秘匿情報）	（秘匿情報）	（秘匿情報）	有
C社	（秘匿情報）	（秘匿情報）	（秘匿情報）	有

※1:イオングループのITインフラ・システム開発/保守・運用などを手がける企業様
※2:パロアルトネットワークス（株）は日本法人だが、本資料では米国本社の情報を代替記載
1ドル110円換算

２）実施方法

以下の３つの方法で、調査を実施する。

1	定量的な課題抽出のアプローチ
2	定性的な課題抽出のアプローチ
3	事件事例の調査

２－１）定量的な課題抽出のアプローチ

　ヒアリングによる課題抽出を実施するに当たって、民主主義的に課題の所在を明らかにしながら、抽出した課題の集計を可能とする必要があるため、定量的な課題抽出のアプローチを用いる。

　具体的には、独自にセキュリティセルフチェックシートを用意し、ヒアリング前にヒアリング対象企業に回答いただき、セルフチェックを実施していただく。事前にセルフチェックを実施していただくことにより、対象企業には社内体制を振り返り整理する機会となり、ヒアリング本番においてより詳細な課題抽出を可能とする。

　また、事前のセルフチェックのみでは各項目のチェック目線がずれる可能性があるため、オンライン会議で実施するヒアリングにおいても、当社のセキュリティ専門研究員が目線合わせを行いながら各項目について改めてヒアリングを行う。

[参考] セキュリティセルフチェックシートの作成方法

国際標準のセキュリティチェックシートであるCIS Controls*における大項目20項目、小項目171項目にわたるチェック項目の中から16項目を厳選し、セルフチェックシートを作成。

16項目の厳選方法について、当社の令和2年4月時点のリモートワーク環境のリスクアセスメント結果で課題として大きかった項目から、当社で問題になった事項については他社でも問題になっている可能性が高いとの仮説のもと、企業規模に関わらずリスクが顕在化されがちな最重要項目から16項目を厳選している。

そしてチェックシートの作成方法について、円滑なヒアリングのため、各厳選項目の論点はそのままに、独自に文言を変更しアンケート形式でリモートワーク環境における課題を洗い出すためのチェックシートを作成している。

[参考] CIS Controlsとは

CIS :
　米国国家安全保障局（NSA : National Security Agency)、米国国防情報システム局（DISA : Defense Information Systems Agency)、米国立標準技術研究所（NIST : National Institute of Standards and Technology)などの米国政府機関や、企業、学術機関などの協力の元、インターネット・セキュリティ標準化に取り組む団体。
CISはボランティアによる非営利団体であるため、特定の企業や製品を推奨することはなく、あらゆる組織にとって公平な立場で情報発信を行っている。

CIS Controls :
　CIS Controlsは、情報セキュリティ対策とコントロールの優先付けされたベースラインを示したコンセンサスドキュメント。APTなどの高度な攻撃を含めて現在までに認識されている攻撃と、近い将来に発生が懸念される攻撃を阻む上で、有効であると考えられる技術的なセキュリティコントロールに焦点をあてている。
各コントロールで定義されたアクションは、米国立標準技術研究所（NIST）のSP800-53で総合的に定義されている事項のサブセットで、大統領令（Executive Order）13636に対応した「サイバーセキュリティフレームワーク」を含むNISTの取組みに代わるものではない。あくまで「最初に最低限行わなければならない」ことに注力し、シンプルにすることを理念として作成されている。上位のコントロールを実践することによって、情報セキュリティにかけるコストを大幅に削減でき、効果が目に見えて改善されることが期待できる。

表１:チェックシートの項目一覧

#	リモートワークにおけるセキュリティ対策状況を教えてください。当てはまるものに「○」を選択してください。	○/×
1	クライアント端末は、会社のオンプレミスのプライベートネットワークに接続しなくても、ハードウェアのイベントリ(構成情報)を定期的に自動取得し最新状態に更新できている。	
2	クライアント端末は、会社のオンプレミスのプライベートネットワークに接続しなくても、利用しているソフトウェアのイベントリ(構成情報)を定期的に自動取得し最新状態に更新できている。	
3	クライアント端末は、会社のオンプレミスのプライベートネットワークに接続しなくても、OSに最新のセキュリティパッチを適用できている。	
4	クライアント端末は、会社のオンプレミスのプライベートネットワークに接続しなくても、ミドルウェアやアプリケーションプログラムに最新のセキュリティパッチを適用できている。	
5	クライアント端末は、会社のオンプレミスのプライベートネットワークに接続しなくても、ハードウェアおよびソフトウェアは、予め定められたセキュリティ標準設定を維持できている。	
6	クライアント端末は、会社のオンプレミスのプライベートネットワークに接続しなくても、ローカルにログを取得できている。	
7	クライアント端末は、会社のオンプレミスのプライベートネットワークに接続しなくても、外部デバイスないの実行ファイルの自動実行を無効化できている。	
8	クライアント端末は、会社のオンプレミスのプライベートネットワークに接続しなくても、Windowsファイアウォール等のホスト型ファイアウォールのポリシーを更新できている。	
9	クライアント端末は、会社のオンプレミスのプライベートネットワークに接続しなくても、不要なアカウントを無効化できている。	
10	クライアント端末は、会社のオンプレミスのプライベートネットワークに接続しなくても、一定期間利用されていないアカウントを無効化できている。	
11	クライアント端末は、会社のオンプレミスのプライベートネットワークに接続しなくても、ログイン状態で一定時間操作が行われていないアカウントに対し、自動的にセッションのロックができている。	
12	会社は、リモートワークのネットワーク(自宅やシェアオフィスなど)においても、DNSフィルタリングにより基地の悪意あるドメインへのアクセスを制御できている。	
13	クライアント端末は、リモートワークのネットワーク(自宅やシェアオフィスなど)においても、ネットワーク機器(モデムやルータ、アクセスポイントなど)を把握できている。	
14	クライアント端末は、リモートワークのネットワーク(自宅やシェアオフィスなど)においても、ネットワーク型ファイアウォールを介して通信を制限できている。	
15	リモートワークの無線LAN(自宅やシェアオフィスのアクセスポイント)は、AES暗号化方式のみに制限できている。	
16	リモートワークの無線LAN(自宅やシェアオフィスのアクセスポイント)は、業務用と個人用で分離できている。	

２－２）定性的な課題抽出のアプローチ

　定量的なアプローチのみでは当社が想定していない未知の課題を導き出すことができないため、オープンクエスチョンとディスカッションの方式で定性的な課題抽出のアプローチを用いる。

　このアプローチでは、オンライン会議にて下記＜流れ＞の通りヒアリングの実施を行う。定性的ヒアリングでは、図１、２を用いてリモートワークの環境およびパブリッククラウドの利用状況について視覚的に認識合わせを行い、議論の焦点を合わせる。ヒアリング時間に余裕があった場合、表２の４項目について追加でヒアリングを行う。

　また、セキュリティ観点のヒアリングは非常にセンシティブなものとなるため、本音ベースでの回答をいただくことが困難と予想される。その対策として、ディスカッション時には当社の事例を紹介しながらヒアリングを実施することで、本音を引き出す工夫とする。

＜流れ＞
1. 10分 ヒアリング背景・目的の説明
2. 20分 定量的チェックシートの目線合わせ
3. 20分 定性的ヒアリングの実施

図１:リモートワーク環境およびクラウド活用環境の認識合わせに用いる図

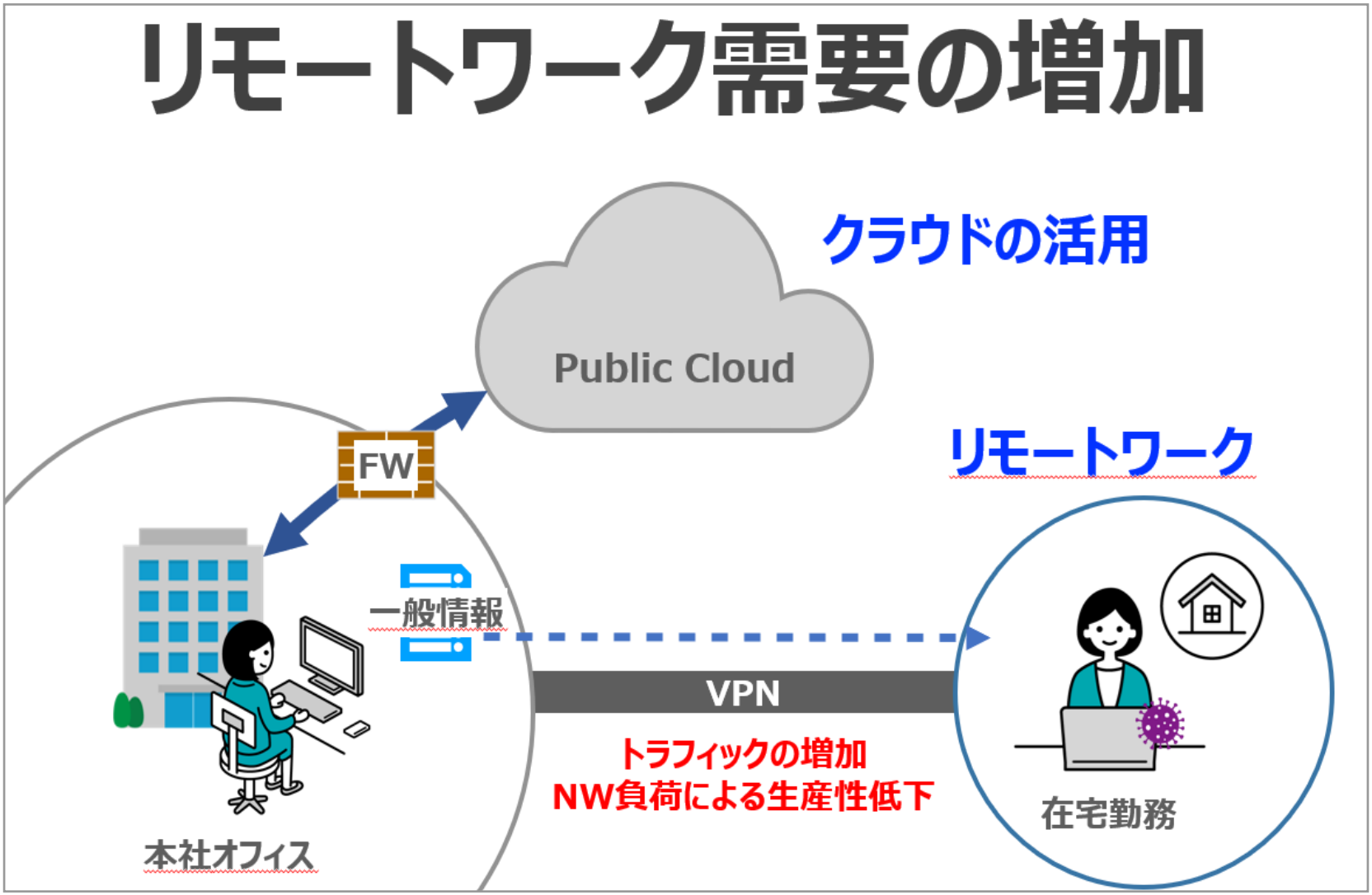


図２:リモートワーク環境およびクラウド活用におけるセキュリティ懸念点のヒアリングに用いる図

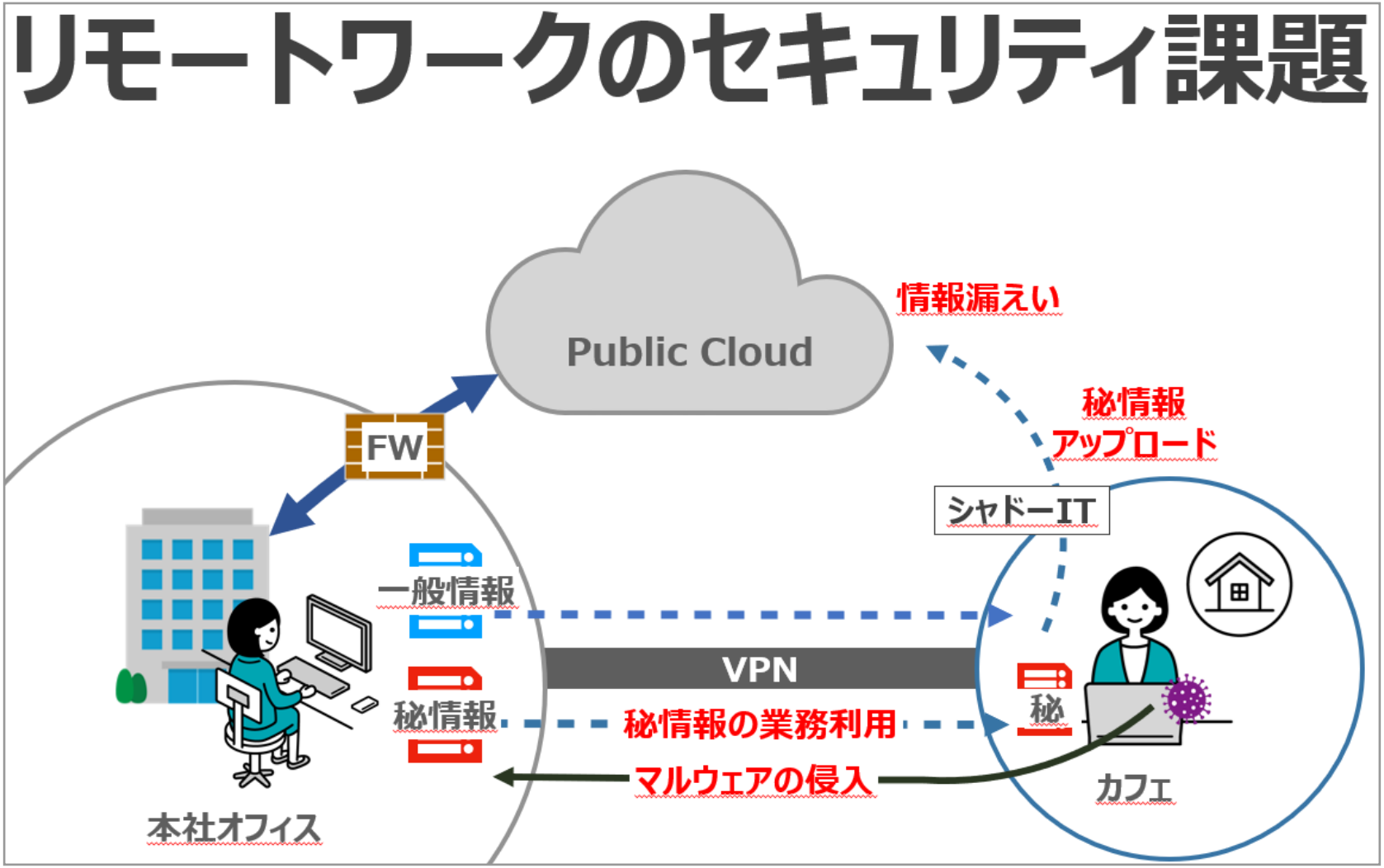


表２:定性調査のための追加ヒアリング項目

1	御社では、リモートワークで取り扱うことが禁止されている情報や業務はありますか？
2	どんな条件やソリューションがあれば、リモートワークできるようになると考えていますか？
3	御社では、パブリッククラウドで取り扱うことが禁止されている情報や業務はありますか？
4	どんな条件やソリューションがあれば、パブリッククラウドを活用できるようになると考えていますか？

２－３）事件事例の調査

近年のセキュリティ事件の事例について調査し、セキュリティ課題の抽出を行う。日本固有の重要技術を流出させないことが重要なため、産業スパイや内部不正による情報漏えい事件（2017年以降）に関するインターネット文献を有料／無料問わず調査する（有料文献：朝日新聞DIGITAL、日経クロステックなど）

【調査対象の具体例（参考として、調査している中から3つを抜粋して例示）】

発生	業種	概要
2018年5月	電気機器	患者情報等をUSBメモリーにコピーし不正に持出し
2019年1月	化学	スマホのタッチパネル技術情報を中国企業に流出
2019年8月	電気工業	ロボットの設計図等を不正コピーし競合他社に流出

【調査まとめ事項】

「漏えいの経緯」を明確にし、解決すべき課題として情報をまとめていく。（その課題内容を、後述「③効果検証」フェーズにて「情報漏えい自体を技術的に防ぐことができたのか」を検証する）

項目	説明
漏えいの経緯	どのような役割／立場の人物が、どのような手段で情報に不正にアクセスし、情報を持ち出したのか／漏えいさせたのかをまとめる
発生防止の要素	どのような対策が実施されていれば事件発生を防ぐことができたのかを、技術的な要素を挙げ課題としてまとめる

２－４）想定されるアウトプット

各調査の結果として、下記4点についてまとめる。

1	定量的な共通課題
2	定性的な共通課題
3	事件事例の一覧
4	阻害要因のまとめ

定量的な共通課題 アウトプットイメージ

セルフチェックシートの集計と各課題における対策率を算出する。

セルフチェックシートの集計表の例

#	チェックシートの設問	A社	B社	C社	…	平均対策率
1	ハードウェアのイベントリ(構成情報)を定期的に自動取得し最新状態に更新できている。	○	×	○	…	78%
2	利用しているソフトウェアのイベントリ(構成情報)を定期的に自動取得し最新状態に更新できている。	○	×	×	…	26%
:	:	:	:	:	:	:
15	リモートワークの無線LANは、AES暗号化方式のみに制限できている。	×	○	×	…	42%
16	リモートワークの無線LANは、業務用と個人用で分離できている。	×	×	×	…	0%

定性的な共通課題 アウトプットイメージ

ヒアリングで得られた定性課題の一覧表を作成する。

定性課題一覧表の例

#	ヒアリングで出てきた定性課題一覧
1	(例) リモートワーク環境でのネットワーク接続によりクライアント端末にマルウェアが持ち込まれる。
2	(例) 個人のオンラインストレージに業務データを保存されることによる、情報漏えい。
:	:
:	～～～
:	～～～

事件事例の一覧 アウトプットイメージ

調査した事件事例について、その発生時期、企業名、事件概要、漏洩の経緯、対策状況、事件の事実認定状況についてまとめ、具体的な対策の考察を行い、考察結果についてもまとめる。

事件事例一覧表の例

発生時期	企業名	事件概要	（漏えいなどの）経緯	対策状況	事実認定状況
2018/5	XXX	～～～	患者情報等をUSBメモリーにコピーし不正に持出し	・外付けデバイス等の利用制限 ・ファイルの機密度～～～	本人は持ち出しを認める（動機不明） (2019/3書類送検)
2019/1	XXX	～～～	スマホのタッチパネル技術情報を中国企業に流出	～～～	本人は持ち出しを認める（不正利用目的は否定） (2020/10書類送検)
2019/8	XXX	～～～	ロボットの設計図等を不正コピーし競合他社に流出	～～～	本人は持ち出しを認める（不正利用目的は否定） (2020/9逮捕)
:	:	:	:	:	:

阻害要因のまとめ アウトプットイメージ

定量調査、定性調査、および事件事例調査から浮かび上がった課題を一覧にまとめる。

リモートワークおよびパブリッククラウド阻害要因一覧表の例

#	リモートワークおよびパブリッククラウド活用の阻害要因一覧	リモートワーク	パブリッククラウド
1	～～～	✓	✓
2	～～～	✓	✓
:	:	:	:
:	～～～	✓	―
:	～～～	―	✓

阻害要因の方向性
内部不正リスクが高い可能性

他人の目	リモートワークは**他人の目がない**ため、内部不正行為の機会が増えてしまう
テナント識別	パブリッククラウドは組織が契約したテナントと個人など組織以外が契約した**テナントを識別**し制限することが難しい
誓約書	内部不正対策はアクセス制限などの仕組みではなく、**誓約書**で牽制している