経済産業省
商務情報政策局　情報産業課

令和2年度
「重要技術管理体制強化事業」
（情報サービス産業の管理体制強化に向けた
セキュリティ技術動向等に関する調査）
報告書

2021年3月15日
ソフトバンク株式会社
〒105-7529
東京都港区海岸一丁目7番1号

目次

1. 事業概要

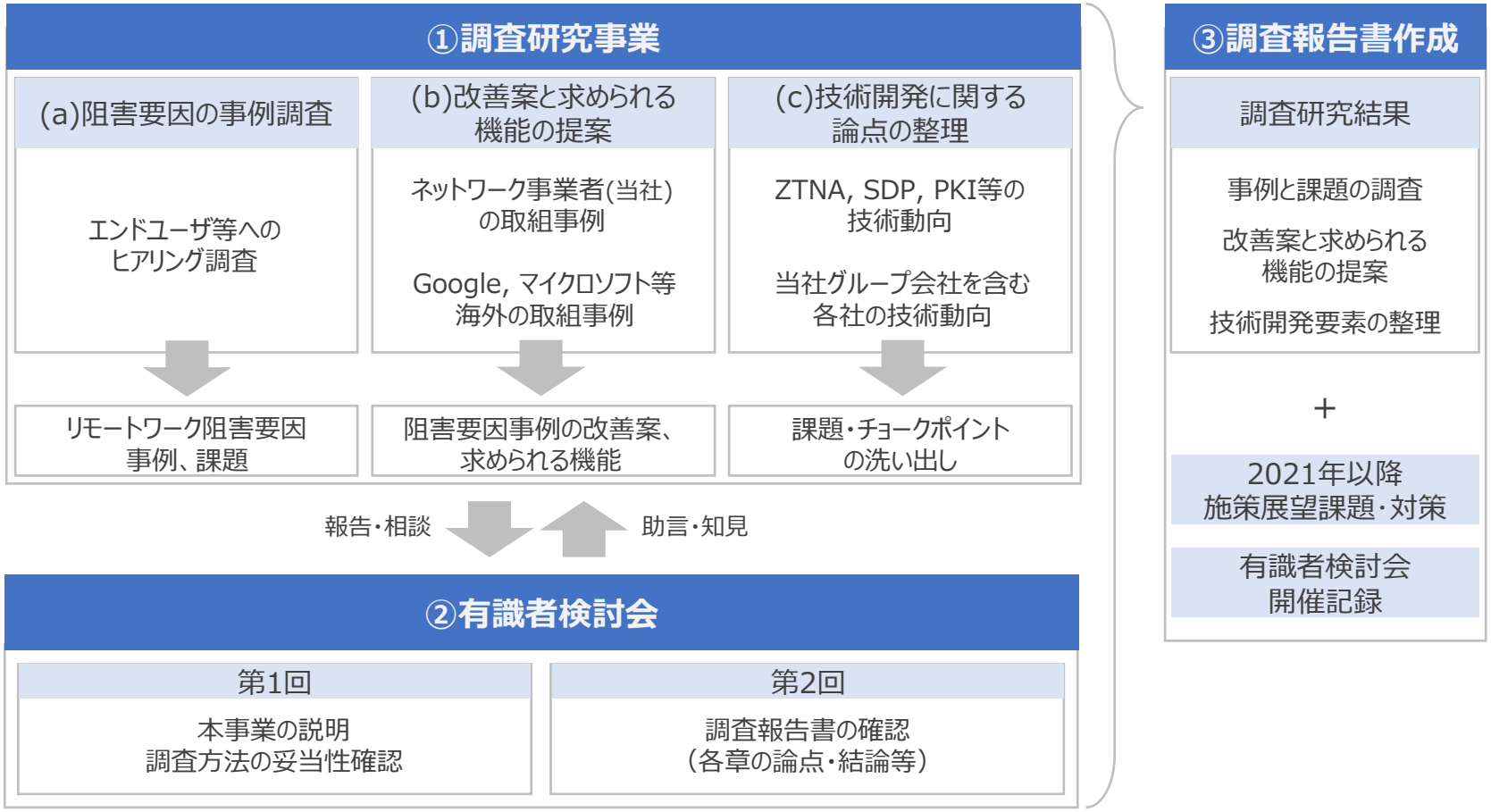
1.1 背景・目的

- 令和2年度 重要技術管理体制強化事業（情報サービス産業の管理体制強化に向けたセキュリティ技術動向等に関する調査）（以下、「本事業」）の背景・目的は以下の通り。

- 近年、技術革新を主導する民生技術と防衛技術の境界が曖昧となる中、懸念組織等への流出を防ぐ観点から技術管理の徹底が急務となっている。さらにコロナ禍におけるリモートワーク需要の急増により、経済活動・社会活動のクラウドへのシフトが加速している。しかし、依然として機密性の高い（漏えいした場合、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を社外に持ち出すことができず、リモートワークの阻害要因となっている。生産性の低下を招くことなく安全なリモートワークを実現するには、クラウド自体のみならず、フィジカルデバイスを含めたEnd to Endにおけるセキュリティ確保が重要な課題である。
- 本事業では、こうした状況を踏まえ、安全・安心で利便性の高いデジタル社会基盤の構築を目的に、そこで求められるセキュリティ技術（認証・認可技術等）に関する調査を行い、今後必要となる技術開発の具体化を行う。

1.2 事業内容

- 本事業は、リモートワーク阻害要因のヒアリング調査・課題対策調査・技術動向調査を行う①「調査研究事業」、外部からの客観的な助言・協力を得る②「有識者検討会」、これらの調査結果を、2021年の施策展望と併せて報告書とする③「調査結果報告書作成」の3パートにより構成されている。



2. ①調査研究事業
(a)阻害要因の事例調査

2.1 調査概要

(a) 阻害要因の事例調査

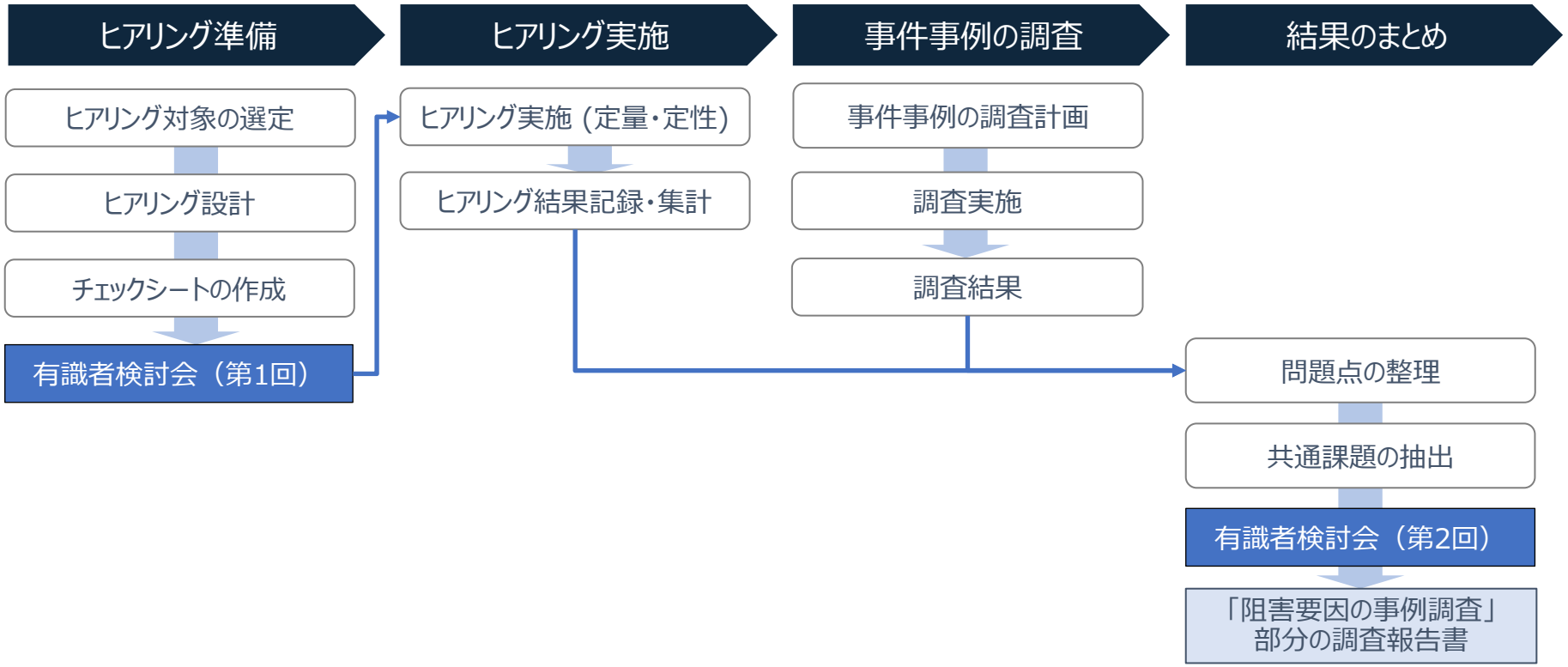
- **目的**
  リモートワーク実施の阻害となり得る、またはリモートワーク実施時に妥協している事例を調査し、調査結果から浮かび上がるセキュリティ観点での課題について把握する。

- **調査内容**
  ヒアリングによるリモートワーク阻害要因の調査および公表されているセキュリティ事件事例の調査の実施

- **ヒアリング**
  - ヒアリング対象： エンドユーザー等9件
  - ヒアリング時期： 2020年12月

- **ヒアリング調査の留意点**
  - 情報秘匿性の高い分野から幅広い業種で対象ユーザーを選定
  - 定性/定量の組み合わせで網羅的に調査
  - 事前チェックシートでポイントを明確にし、回答の精度を向上

- **事件事例の調査**
  - クラウド利用に関して2020年度の事件を調査
  - 産業スパイに関して直近5年間の事件を調査



2.2.1 ヒアリング準備 - ヒアリング対象

- 事業の目的・背景を踏まえ、ヒアリング対象は、**「業務上取り扱う情報の秘匿性が高く、漏えいした場合に、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、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企業」**と定めた。
- ヒアリング調査にご協力頂いた企業は下表の通り。なお、個別の回答内容は非公開とする。

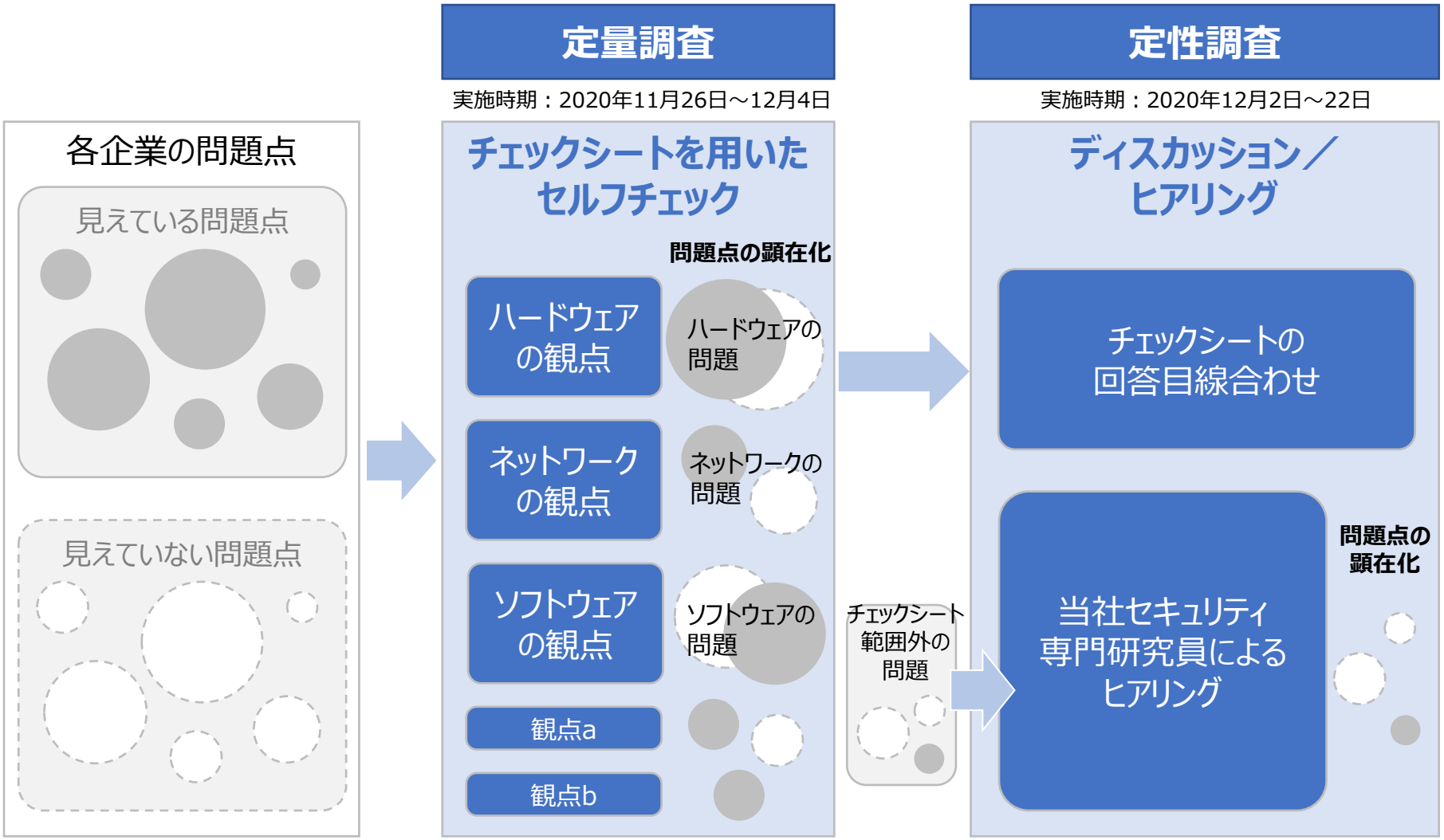
表：本調査のヒアリング調査にご協力頂いた企業一覧（一部、要望により非公開。掲載情報は2020年12月時点）

#	会社名 <五十音順>	業種	資本金 (百万円)	従業員数 (人)	分散拠点
1	イオンアイビス(株)*1	小売 / 情報	490	360	有
2	SHIFT(株)	情報・通信	67	3,829	有
3	シャープ(株)	製造	5,000	51,402	有
4	ソフトバンク(株)	情報・通信	204,309	17,300	有
5	パロアルトネットワークス(株)*2	セキュリティ	248,512	8,014	有
6	(株)バローホールディングス	小売	13,609	8,168	有
7	（会社名非公開A社）	-	-	-	有
8	（会社名非公開B社）	-	-	-	有
9	（会社名非公開C社）	-	-	-	有

※1: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: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。

2.2.2 ヒアリング準備 - ヒアリング設計

- ヒアリング調査の網羅性を向上するために、チェックシートを用いた定量調査と、ディスカッションによる定性調査を組み合わせて実施する。実行イメージは下記の通り。



図：ヒアリング調査の実行イメージ

2.2.3 ヒアリング準備 – 定量調査のチェックシート

- 定量調査のチェックシートは、グローバルで普及しているCIS Controls*1から特に重要であると考えられる16項目を抽出して作成した。
  - CIS Controls*1の項目数は全部で171項目、当社および当社グループ各社の多数の過去実績から、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項目を厳選した。
  - 各企業でセルフチェックを行ったのち、セキュリティ専門研究員との目線合わせを行い、回答精度を向上させた。

表：CIS Controls*1から厳選抽出した16項目（CIS Controlsを基に当社作成）

CIS#	CIS Title	Sub#	Sub-Title
1	ハードウェア資産のインベントリとコントロール	1.4	詳細な資産インベントリを維持する
2	ソフトウェア資産のインベントリとコントロール	2.1	許可されたソフトウェアのインベントリを維持する
3	継続的な脆弱性管理	3.4	オペレーティングシステムの自動化されたパッチ管理ツールを適用する
3	継続的な脆弱性管理	3.5	ソフトウェアの自動化されたパッチ管理ツールを適用する
5	モバイルデバイス、ラップトップ、ワークステーションおよび サーバに関するハードウェアおよびソフトウェアのセキュアな設定	5.1	セキュアな設定を確立する
6	監査ログの保守、監視および分析	6.2	監査ロギングを起動する
7	電子メールと Web ブラウザの保護	7.7	DNSフィルタリングサービスの使用
8	マルウェア対策	8.5	デバイスがコンテンツを自動実行しないように設定する
9	ネットワークポート、プロトコル、およびサービスの制限および コントロール	9.4	ホストベースのファイアウォールまたはポートフィルタを適用する
12	境界防御	12.1	ネットワーク境界のインベントリを維持する
12	境界防御	12.4	許可されていないポートを介した通信を拒否する
15	無線アクセスコントロール	15.7	Advanced Encryption Standard (AES)を活用して無線データを暗号化する
15	無線アクセスコントロール	15.10	個人所有のデバイスや信頼できないデバイス用に個別の無線ネットワークを構築する
16	アカウントの監視およびコントロール	16.8	関連付けされていないアカウントをすべて無効にする
16	アカウントの監視およびコントロール	16.9	休止アカウントを無効にする
16	アカウントの監視およびコントロール	16.11	未使用期間の経過後にワークステーションセッションをロックする

*1 CIS Controls：米国の団体 Center for Internet Security が発行し、グローバルで普及が進んでいるフレームワーク。[(参考) CIS Controlsについて]

（参考）定量調査のチェックシート

- 定量調査に使用したチェックシートは以下の通り。

表：定量調査のチェックシート（CIS Controlsを基に弊社作成）

#	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、ハードウェアのインベントリ(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ンベントリ(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既知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。	

（参考）CIS Controlsについて

- CIS Controlsとは米国の団体 CIS（Center for Internet Security）が発行し、グローバルで普及が進んでいるフレームワークである。詳細は以下の通り。

CISについて

- CISは、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もと、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の特徴

- 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である。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の取り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。

2.2.4 ヒアリング準備 - 定性調査のヒアリング方法

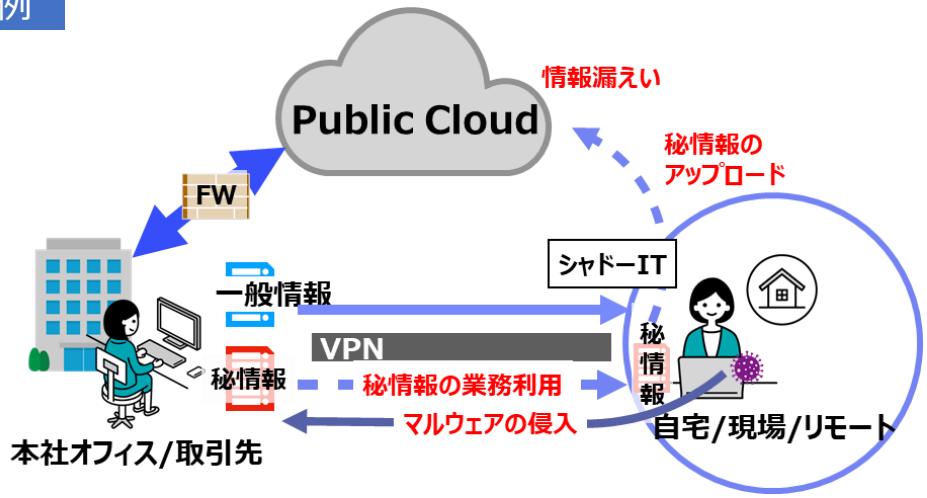
- 定性調査は、定量調査として行ったチェックシートのセルフチェックの目線合わせ、および当社セキュリティ専門研究員とのディスカッション／ヒアリングを通じて、リモートワークが阻害されている、または妥協している事例とその課題を網羅的に抽出できるように設計した。
- ディスカッション／ヒアリングにおいては、リモートワークの阻害事例や課題を構成図および表で示しながら進行するといった回答を引き出す工夫を検討した。

オンラインミーティング

表を用いた
類似事例のヒアリング

構成図を用いた
問題箇所の具体化

構成図例



	ヒアリング項目（例）	回答例
1	リモートで取り扱うことが禁止されている情報や業務	設計図面、社内ネットワークの構成情報、秘情報
2	（1.の情報や業務について、）リモートで取り扱いが禁止されている理由	ネットワークの問題、認証・認可
3	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	設計図面、社内ネットワークの構成情報、秘情報
4	（3.の情報や業務について、）パブリッククラウドで取り扱いが禁止されている理由	認証・認可

2.3 ヒアリング実施

- ヒアリング調査は下記の通り実施した。

目的		リモートワーク実施の阻害となり得る、またはリモートワーク実施時に妥協している事例を調査し、調査結果から浮かび上がるセキュリティ観点での課題について把握する。
ヒアリング対象者		対象企業9社のセキュリティ業務担当者
定量調査	内容	1.　チェックシートのセルフチェック
	方法	チェックシート（回答項目：16項目、回答時間：30分程度）
	時期	2020年11月26日　～　2020年12月4日
定性調査	内容	1.　チェックシート回答の目線合わせ 2.　当社セキュリティ専門研究員によるヒアリング
	方法	オンラインミーティング（各社1時間程度）
	時期	2020年12月2日　～　2020年12月22日

2.4.1 調査結果 - 定量調査の集計結果

- 各企業への定量調査の結果は下表の通りである。
- **端末管理、Wi-Fi設定**に関する設問は、いずれも対策率が低かった。
- アカウント管理、マルウェアや外部脅威等へのセキュリティ対策に関しては過半数の企業が十分な対策を実施できていた。

表：定量調査の集計結果

#	カテゴリ	チェックシート集計表	対策率
1	**端末管理**	**ハードウェアのインベントリ(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。**	**33%**
2	**端末管理**	**利用しているソフトウェアのインベントリ(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。**	**33%**
3	**端末管理**	**OSに最新のセキュリティパッチを適用できている。**	**33%**
4	**端末管理**	**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。**	**33%**
5	セキュアな設定	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。	56%
6	監査ログの保守、監視	ローカルにログを取得できている。	67%
7	マルウェア対策	外部デバイス内の実行ファイルの自動実行を無効化できている。	67%
8	境界防御	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。	56%
9	アカウントの監視・コントロール	不要なアカウントを無効化できている。	56%
10	アカウントの監視・コントロール	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。	56%
11	アカウントの監視・コントロール	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。	56%
12	電子メールとWebブラウザの保護	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。	56%
13	境界防御	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。	44%
14	境界防御	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。	56%
15	**Wi-Fi設定**	**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。**	**11%**
16	**Wi-Fi設定**	**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。**	**11%**

2.4.2 調査結果 - 定量調査の共通課題

- 2.4.1項の結果から抽出した共通課題は以下の2項目である。

（定量調査結果のまとめ）
- 設問6,7　：ローカルログの保存と外部デバイスの実行については、高い割合で対策ができている。
- 設問15,16：アクセスポイントの管理についてはほとんどの会社が未対策であった。（→共通課題#1 Wi-Fi設定）
- 設問1～4　：過半数の企業において、インベントリの管理やOSソフトウェアのパッチ適用に関して最新状態の維持に課題がある。（→共通課題#2 端末管理）

表：定量調査から抽出した共通課題

#	項目	内容
1	**Wi-Fi設定**	在宅中のWi-Fiアクセスポイントの設定を従業員に任せているが、暗号化設定など確認手段がない。
2	**端末管理**	端末管理はVPNを張ると実施できるが、常にVPNが張られていないため、設定更新率が低い。

2.4.3 調査結果 - 定性調査の共通課題

- 定性調査において、チェックシートの項目と追加ヒアリング項目（p.13の項目例等）を軸にヒアリングを実施した。ヒアリングによる定性調査の結果から、抽出された共通課題を以下に示す。
- また、定性調査への回答内容は個社判別が可能となる恐れがあるため、非公開とする。

表：定性調査から抽出した共通課題

#	項目	内容
1	**回線逼迫**	リモートワークによる回線逼迫に対応するための回線増強には、数ヶ月単位の時間を要する。
2	**端末管理**	端末管理はVPNを張ると実施できるが、常にVPNが張られていないため、設定更新率が低い。
3	**プリンタ**	リモートワークでの社外のプリンタの利用が禁止されている。
4	**個人クラウド**	契約が容易でシャドーITと業務利用との区別が難しい。
5	**内部不正**	内部不正対策のため、教育や誓約書取得しているが、強制力が欠けている。
6	**高機密データ**	個人情報など高機密データを取り扱う業務はリモートワークが禁止されている。

2.5.1 事件事例調査の結果（1/3）

- 直近5か年に発生した情報セキュリティに関する事件事例をインターネット上の公開情報を用いて調査し、事件経緯から問題点を洗い出し、課題として抽出した。

表：直近5か年の事件事例調査結果

#	事件要因	発生年月	企業･団体名	概要	事象経緯	課題
1	リモートワーク	2020年5月	NTTコミュニケーションズ株式会社	企業向けクラウドサービスの管理サーバーなどが不正アクセスを受けたと発表。同サービスを利用する法人顧客の一部である621社のサービス申し込み情報や設定情報などが漏えいした。	2019年9月にシンガポールにあった同サービスの運用サーバーに侵入した後、複数の海外拠点を経由して日本国内にある同サービスの管理サーバーに侵入したとみられる。またリモートアクセスを利用したBYOD端末からの不正アクセスが判明した。	**BYOD**
2	リモートワーク	2020年5月	大阪府立大冠高等学校	大阪府は2020年5月7日、府内の公立高等学校に所属する教員が、生徒の個人情報360件を記録したUSBメモリを外部で紛失した可能性があると明らかにした。	教員はテレワークの必要性から、同校に所属する3年生の生徒情報を私物のUSBメモリに記録。その後、学外に出張したところ、USBメモリの所在が不明になっていることが判明。	**外部デバイス**
3	クラウド	2020年11月	公益財団法人ふくい産業支援センター	公益財団法人ふくい産業支援センターが運営するポータルサイト「ふくいナビ」の全データが、サーバ管理会社であるNECキャピタルソリューションの社内手続きミスにより完全消失した。	ふくいナビのクラウドサーバの賃貸借契約を結んでおり、その契約を更新していたが、NECキャピタルソリューションの社内手続きのミスで更新の手続きがされておらず、貸与期間が終了したとして全データが削除。	**クラウド利用**
4	クラウド	2020年12月	楽天株式会社	利用中の営業管理用SaaSが不正アクセスを受け、保管していた個人情報など最大148万6291件が流出した可能性があると発表した。営業管理用SaaSのセキュリティ設定にミスがあったことが原因。	社外のセキュリティ専門家の指摘で、営業管理用SaaSの情報が社外からアクセスできる状態になっていたことが分かった。	**クラウド利用**
5	クラウド	2021年1月	福岡県庁	県が管理していた新型コロナウイルス感染症の陽性者9500人分の氏名、住所などの個人情報がクラウドサービス上で外部から閲覧できる状態だったと発表。URLを知っていれば誰でも個別のファイルにアクセスできる状態が続いていた。	個人情報を含む複数のファイルなどへアクセス権限を付与するメールを外部に誤送信。同日、メールを受け取った男性から県へ連絡があり、フォルダやファイルを第三者が閲覧できる状態が発覚した。	**クラウド利用**

※2021年1月 当社調べ

2.5.1 事件事例調査の結果（2/3）

- 直近5か年に発生した情報セキュリティに関する事件事例をインターネット上の公開情報を用いて調査し、事件経緯から問題点を洗い出し、課題として抽出した。

表：直近5か年の事件事例調査結果

#	事件要因	発生年月	企業・団体名	概要	事象経緯	課題
1	産業スパイ	2017年 2月	オーエスジー 株式会社	会社から貸与されたパソコンで同社のサーバーにアクセスし、営業秘密に当たる工業用製品の設計データを複製し、持ち出した。データは、中国の競合会社に勤務する知人の中国人男性に提供されたとみられる。	私物の外付けハードディスクに複製し、不正に持ち出し提供した。	**外部デバイス**
2	産業スパイ	2017年 5月	フューチャー アーキテクト 株式会社	フューチャーアーキテクトの元役員が、在任中に同社に知らせないまま競合のベイカレント・コンサルティングとも雇用契約を結び、社員の情報をベイカレントに漏えいした。	個人端末から同社のサーバに接続し、機密情報を不正に取得。ベイカレント社の端末に複製したり社員宛にメールなどを実施した。	**外部メール**
3	産業スパイ	2017年 8月	DMG森精機 株式会社	取引先への機械納入時期といった顧客管理データにアクセスし、約300社分を印刷して不正に持ち出した。アクセスがあった月、その社員は退職予定で、同業他社へ転職の予定があった。	自社センター内にて製品情報を印刷し自宅へデータを不正持ち出しした。	**外部デバイス**
4	産業スパイ	2017年 11月	NISSHA 株式会社	超細密印刷技術やスマートフォンなどのタッチセンサー開発において、世界トップシェアを誇るNISSHA株式会社の元社員が、関連会社のコンピュータに不正アクセスし、技術情報をハードディスクにコピーしていた。その後その社員は退職し、中国の競合他社に転職した。	同社主力製品の技術情報を自分のハードディスクに不正に複製した疑い。	**外部デバイス**
5	産業スパイ	2017年 11月	株式会社 ゼネテック	システム開発やソフトウェアの販売などを手がけるゼネテックの元従業員が、営業機密情報を不正に持ち出した。その後、大阪に拠点を置く競合ソフトウェア会社に持ち出した情報を提供していた。	取引先顧客や取引情報を、ファイル転送サービスを悪用しゼネテックの営業秘密情報を私物の端末に転送。社外に無断で持ち出したことにより流出した。	**外部デバイス**

※2021年1月 当社調べ

2.5.1 事件事例調査の結果（3/3）

- 直近5か年に発生した情報セキュリティに関する事件事例をインターネット上の公開情報を用いて調査し、事件経緯から問題点を洗い出し、課題として抽出した。

表：直近5か年の事件事例調査結果

#	事件要因	発生年月	企業・団体名	概要	事象経緯	課題
6	産業スパイ	2018年 5月	アークレイ 株式会社	医療検査機器などの製造・販売しているアークレイ株式会社で、退職予定だった従業員が医療機関から提供を受けた患者情報などをUSBメモリーにコピーし不正に持ち出した。	使用していたパソコン端末を調べたところ、機密情報を書き出したログを確認し情報流出が発覚。 USBからの情報抜き取り。	**外部デバイス**
7	産業スパイ	2018年 5月	株式会社 アシックス	アシックスの元社員が、同社のシューズに関する営業秘密データを入手し、不正に私用メールに送信した。その後、その社員は退職し、プーマジャパンに転職した。	元従業員がサーバ不正アクセス履歴が発覚。 メールを使って元社員の個人アドレスに対して送付されていた。 また元社員の私物端末からメールへアクセスしていた。	**外部メール**
8	産業スパイ	2019年 1月	富士精工 株式会社	技術部門に所属する中国籍の元社員が、富士精工が営業秘密として管理していたドリルなどの同社製品の設計情報をUSBメモリーにコピーした。	富士精工のサーバーに不正アクセスを実行。 サーバー内から製品の設計情報やマニュアルなどを自身のUSBメモリーに転送していた疑い。	**外部デバイス**
9	産業スパイ	2019年 1月	積水化学工業 株式会社	技術部門に所属する元社員が、スマートフォンのタッチパネルに使われる「導電性微粒子」の製造工程に関する技術情報を、中国・広東省にある通信機器部品メーカー「潮州三環グループ」の社員にメールで送信した。	メールでの送信に加えて、 勤務時間中に自身のUSBメモリーにデータをコピーするなどして情報を持ち出していたことが調査で判明。	**外部デバイス**
10	産業スパイ	2019年 8月	株式会社 豊電子工業	営業部門に所属していた元社員が、機密情報と知りながら、不正な利益を得る目的で、同社の営業上の秘密にあたるロボットの設計図や生産ラインのレイアウト図などのデータ59件をハードディスクにコピーした。その後、その社員は競合他社に転職した。	ハードディスクにコピー後、競合他社へ一部開示、流出させた。	**外部デバイス**

※2021年1月 当社調べ

2.5.2 事件事例調査の共通課題

- 2.5.1項の結果から抽出した共通課題は以下の4項目である。

表：事件事例から抽出した共通課題

#	項目	内容
1	**BYOD**	個人所有デバイスに対するセキュリティ対策を強制することが難しい。
2	**個人利用のクラウド**	契約が容易でシャドーITと業務利用との区別が難しい。
3	**外部デバイス**	機密情報をUSBメモリなど外部デバイスで持ち出される。
4	**外部メール**	機密情報を個人メール宛て等で持ち出される。

2.6 まとめ

- 2.4 ヒアリング調査結果（定量／定性）と2.5 事件事例調査結果から、抽出されたリモートワークの阻害要因となりうる共通課題を以下に示す。(*1)

問題

ヒアリング調査（定量）により顕在化した問題

- リモートワーク環境の**Wi-Fi設定**
- **端末**の設定更新等の**管理**が不十分

ヒアリング調査（定性）により顕在化した問題

- リモートワークにより**回線**が**逼迫**している
- **端末**の設定更新等の**管理**が不十分
- **プリンタ**が利用できないことによる不都合
- 個人契約の**クラウド**サービスを業務で利用
- **内部不正**対策が教育や誓約書のみ
- **高機密データ**がリモートで取り扱えない

事件事例調査により顕在化した問題

- **BYOD**端末のセキュリティ対策が不十分
- 個人契約の**クラウドサービス**を業務で利用
- **外部デバイス**利用による不正
- **外部メール**利用による不正

技術的要因以外による問題*3
例）経営判断、心理的ハードル、企業文化・風土、コスト、従業員意識の問題による生産性低下等

*3 ：技術的要因以外による問題は、本事業の対象外とする。

リモートワークの阻害要因となりうる共通課題

#	項目	内容	カテゴリ
1	**回線逼迫**	リモートワークによる回線逼迫に対応するための回線増強には、数ヶ月単位の時間を要する。	ネットワーク
2	**Wi-Fi設定**	在宅中のWi-Fiアクセスポイントの設定を従業員に任せているが、暗号化設定など確認手段がない。	ネットワーク
3	**端末管理**	端末管理はVPNを張ると実施できるが、常にVPNが張られていないため、設定更新率が低い。	デバイス
4	**BYOD**	個人所有デバイスに対するセキュリティ対策を強制することが難しい。	デバイス
5	**外部デバイス**	機密情報をUSBメモリなど外部デバイスで持ち出される。	デバイス
6	**プリンタ**	リモートワークでの社外のプリンタの利用が禁止されている。	デバイス
7	**外部メール**	機密情報を個人メール宛て等で持ち出される。	データ
8	**個人クラウド**	契約が容易でシャドーITと業務利用との区別が難しい。	ネットワーク/認証
9	**内部不正**	内部不正対策のため、教育や誓約書取得しているが、強制力が欠けている。	データ
10	**高機密データ*2**	個人情報などの高機密データを取り扱う業務はリモートワークが禁止されている。	データ

*1： リモートワークを阻害する要因となりうる共通課題は、これらの課題に対して対策を講じなければリモートワークが推奨されないというものではない。

*2： 特定の従業員のみがセキュアルームなどの特定の場所や条件のみでアクセス可能とし物理・システム・規約により厳密な保護と取扱いが求められるデータを指す。

（参考）リモートワークの失敗や阻害要因の事例の共通課題の分析

- 第1回有識者検討会において、下記の様なリモートワークに対する企業側の心理的懸念を阻害要因とする意見があった。検討の結果、これらの阻害要因は技術による直接的な解決が難しいため、今回の課題としては取り上げることを見送る事とした。

心理的ハードルとコスト

- リモートワークの阻害要因として、経営判断や従業員の意識の問題による生産性低下等の心理的ハードルやコストの問題が考えられる。
- リモートワークに関連するガイドラインの整備やサイバーセキュリティ人材の育成も重要なテーマであり、心理的ハードルを下げる効果が期待できる。

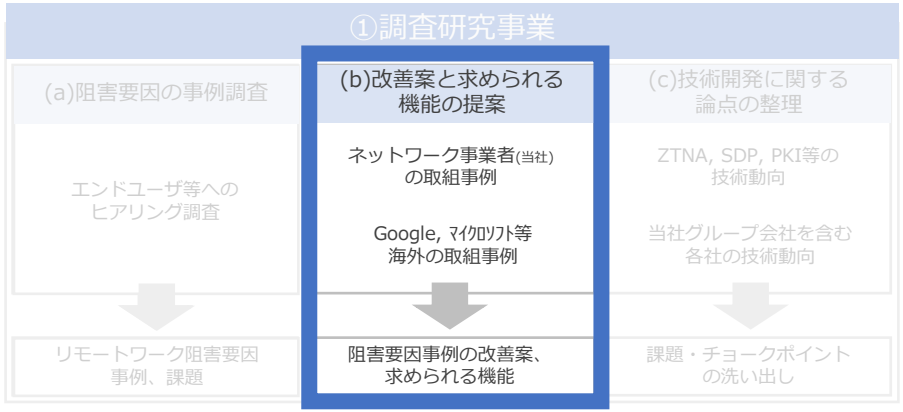
（参考）リモートワーク導入のメリット

- リモートワーク（テレワーク含む）には、企業、従業員共に多くのメリットがあると考えられる。
  当社が調査したリモートワークのメリットを以下に示す。

表：リモートワークの導入メリット（当社調べ）

企業／従業員	メリット
企業	災害や事故等で出社不可の状況でも業務継続できる状況が整ってきた（事業継続計画）
	育児・介護などの理由での離職率の低減に貢献
	執務エリアや交通費の最適化によるコスト削減
	従業員のタイムマネジメント意識が上がり無駄な残業が減る
	デジタル化により顧客へのコンタクト数が増えた
従業員	通勤時間・ストレス削減（時間の有効活用、通勤疲労軽減）
	生活リズムが改善しパフォーマンス向上（睡眠時間、食事時間など規則的）
	会議室の制約から開放（会議室確保や移動は不要に）
	集中力向上（割り込みが入らないので作業に集中することができる）
	会社の時間の有効活用として副業が解禁された
	自宅の方が業務環境が良い（モニターやNW環境など）
	働き方の多様化（家族との時間や子供の送り迎えなどの働きやすくなった）

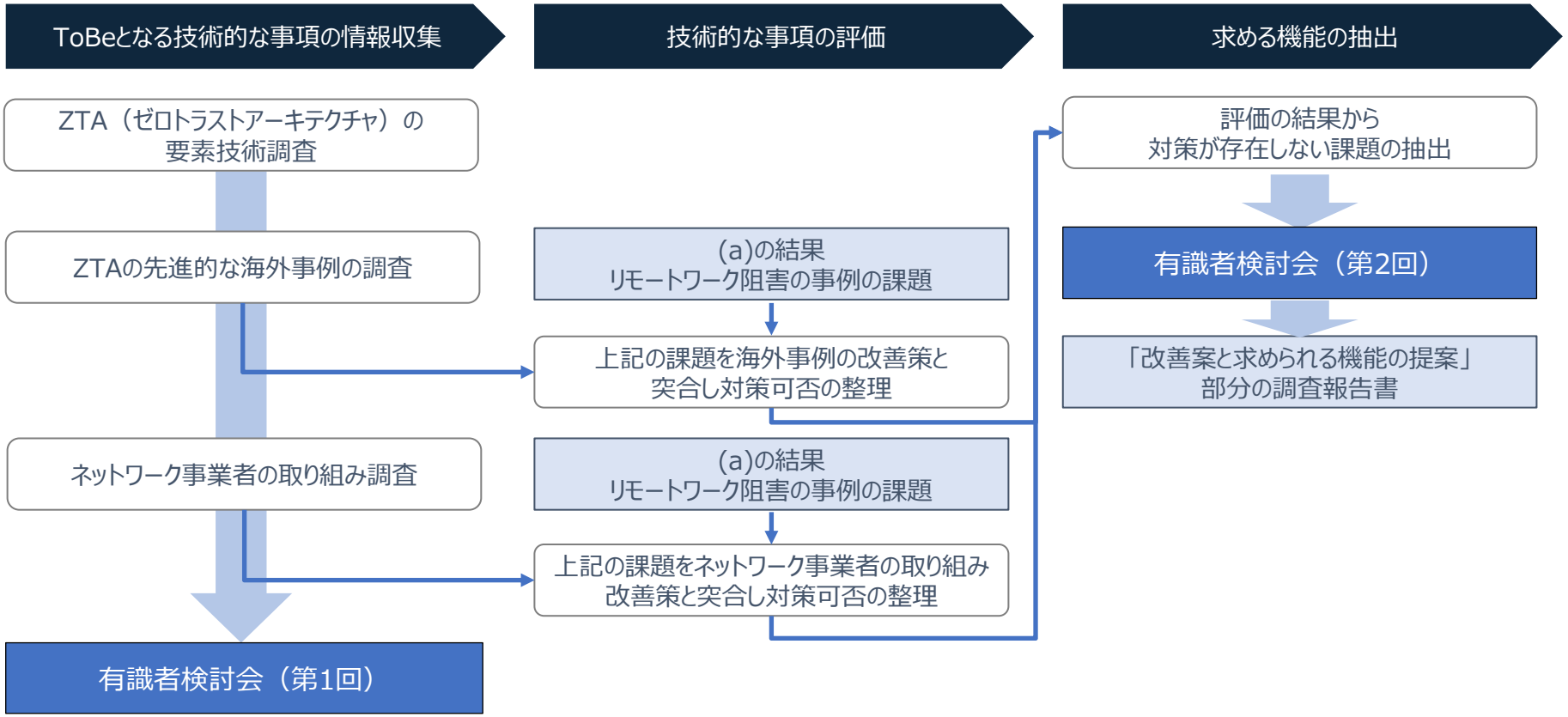
3. ①調査研究事業
(b)改善案と求められる機能の提案



3.1 調査概要

(b) 改善案と求められる機能の提案

- **目的**
  リモートワーク阻害要因事例の改善案を提案することで、これに求められるネットワーク制御、認証・認可等の機能を明らかにする
- **調査内容**
  - ZTA（ゼロトラストアーキテクチャ）の先進的な海外事例を文献調査やヒアリングにより情報収集
  - 国内ネットワーク事業者のセキュリティ対策をヒアリングにより情報収集
  - 阻害要因事例の改善案の評価・確認
- **対策が存在しない課題の抽出**
  - 阻害要因事例の対策可否を確認し対策が存在しない課題を抽出する
    - 海外事例
    - ネットワーク事業者事例



3.2 調査実施

- リモートワーク阻害要因事例の改善案を提案することで、これに求められるネットワーク制御、認証・認可等の機能を明らかにするという目的に沿って、下記の調査を行った。

	ZTA（ゼロトラストアーキテクチャ）要素技術調査	海外事例調査*1	ネットワーク事業者の取り組み事例調査*1
内容	情報セキュリティのアーキテクチャとして、ゼロトラストの適用可能性を検討するため、ゼロトラストアーキテクチャが実現する機能について整理する。	海外の先進的な事例を調査し、その概要と特徴を整理する。	当社におけるセキュリティ対策の取り組み事例をまとめ、その特徴を整理する。
対象	NIST SP 800-207 Zero Trust Architecture	・Google社「BeyondCorp」 ・マイクロソフト社 「マイクロソフトゼロトラストセキュリティ」	ソフトバンク株式会社 ・常時VPNによるリモートアクセス ・AIを活用した内部不正対策
方法	インターネット上の公開情報を用いた文献調査	・パートナー企業からの情報収集 ・インターネット上の公開情報を用いた文献調査	・実務担当者等からの情報収集
期間	2020年12月	2020年12月～2021年1月	2020年12月～2021年1月

*1　製品情報等は2021年1月時点のものである。

3.3.1 ZTA要素技術調査結果 - 定義

- 3.3節では、「NIST SP 800-207 Zero Trust Architecture」(*1)を参照し、ZTA（ゼロトラストアーキテクチャ）の概念や展開モデルを説明する。
- 本報告書における、ゼロトラスト関連用語は、下表に定義した内容を意味する。

図：ZTAのモデル定義（NIST SP 800-207 Zero Trust Architectureを参照し、当社作成）

表：本報告書におけるゼロトラスト関連用語の定義（NIST SP 800-207 Zero Trust Architectureを参照し、定義）

用語	定義
ZT (Zero Trust)	要求ごとの最小特権を持つアクセスを決定する際の不確実性を最小化するために設計された概念とアイデアの集合体のこと。
ZTA (Zero Trust Architecture)	ゼロトラストの概念を利用した組織のサイバーセキュリティ計画のこと。
ZTNA (Zero Trust Network Access)	ゼロトラストの概念を取り入れたユーザがリモートから社内リソースやクラウドリソースにアクセスするときのセキュリティソリューションのこと。VPNの代替として期待されている。

*1 米国国立標準技術研究所(NIST)が作成および公開している、ゼロトラスト・アーキテクチャの概念を取りまとめた文章。

3.3.2 ZTA要素技術調査結果 - 基本思想

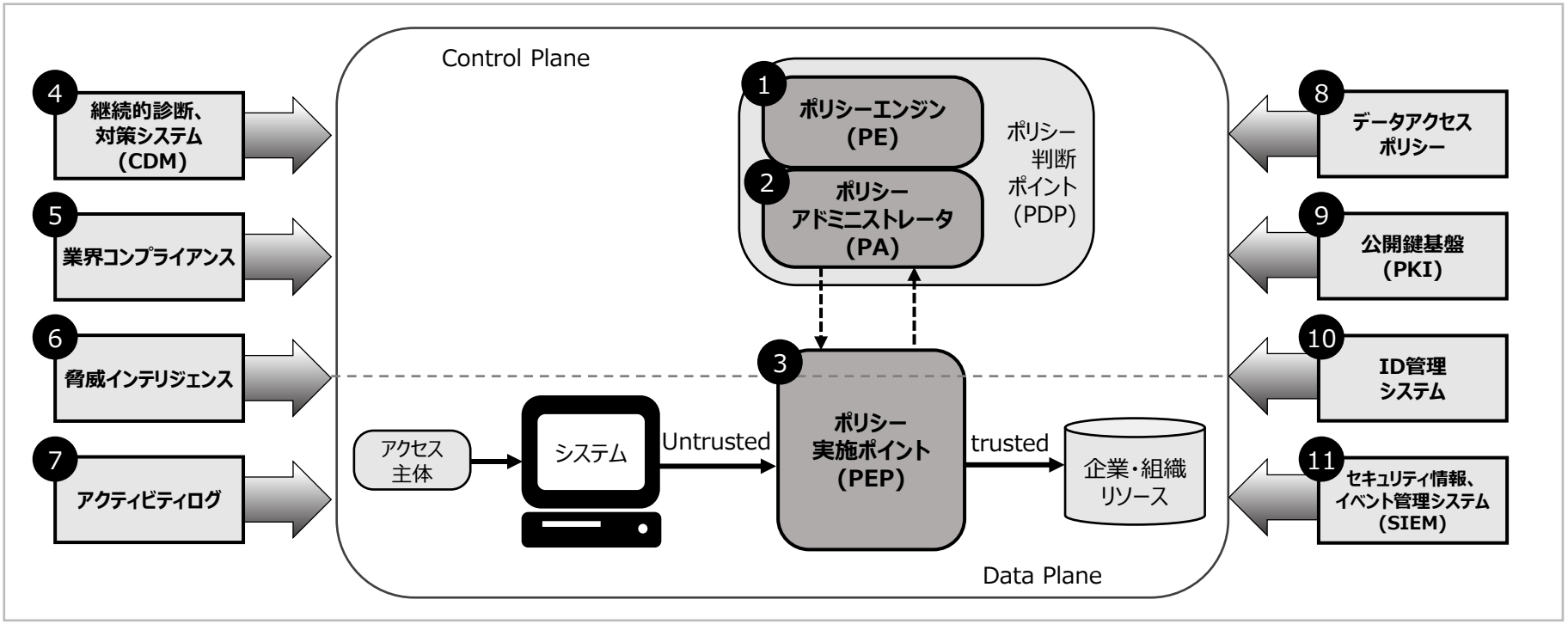
- ZTAは、以下の7つの基本思想に準拠して、設計・展開されている。

表：ZTAの基本思想（原文：NIST SP 800-207 Zero Trust Architectureより引用、和訳：当社作成）

	原文	和訳
1	All data sources and computing services are considered resources.	すべてのデータソースとコンピューティングサービスを**リソース**とみなす。
2	All communication is secured regardless of network location.	**ネットワークの場所に関係なく**、すべての通信を保護する。
3	Access to individual enterprise resources is granted on a per-session basis.	企業リソースへのアクセスは、**セッション単位**で付与する。
4	Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.	リソースへのアクセスは、クライアントアイデンティティ、アプリケーション/サービス、リクエストする資産の状態、その他の行動属性や環境属性を含めた**動的ポリシー**により決定する。
5	The enterprise monitors and measures the integrity and security posture of all owned and associated assets.	すべての資産の整合性と**セキュリティ動作を監視**し、測定する。
6	All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	すべてのリソースの認証と認可を動的に行い、**アクセスが許可される前**に厳格に実施する。
7	The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.	資産、ネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、**セキュリティ体制の改善**に利用する。

3.3.3 ZTA要素技術調査結果 - コンポーネント

- ZTAの11つからなる論理的構成要素（コンポーネント）は以下の通り。



図：ZTAのコアコンポーネント（NIST SP 800-207 Zero Trust Architectureを基に当社作成）

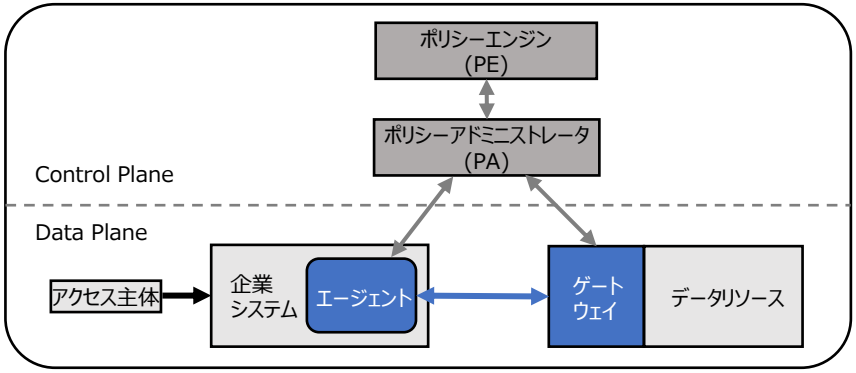
1. ポリシーエンジン（PE）
2. ポリシーアドミニストレータ（PA）
3. ポリシー実施ポイント（PEP）
4. 継続的診断および対策（CDM）
5. 業界のコンプライアンスシステム
6. 脅威インテリジェンスフィード
7. ネットワークおよびシステムのアクティビティログ
8. データアクセスポリシー
9. 企業の公開鍵基盤（PKI）
10. ID管理システム
11. セキュリティ情報およびイベント管理（SIEM）

3.3.4 ZTA要素技術調査結果 – 実装パターン

- ZTAでは4つの実装パターン（ZTA展開モデル）が提示されている。

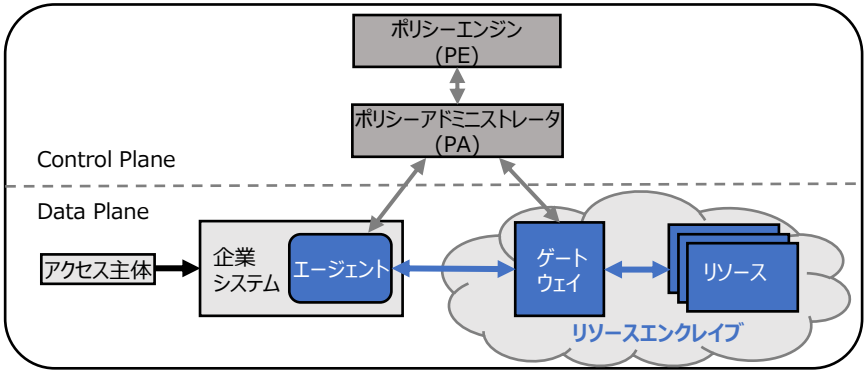
デバイスエージェント／ゲートウェイモデル

PEPがエージェント側とゲートウェイ側に分かれるモデルであり、主にオンプレミスまたは、IaaS構成に対して有用である。



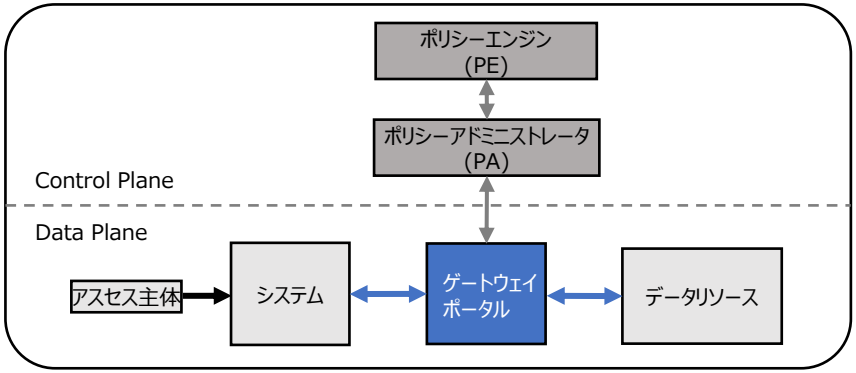
エンクレイブゲートウェイモデル

左記モデルのバリエーションである。リソースに個別のゲートウェイを設置できないSaaS、または自社管理外資産に対し有用である



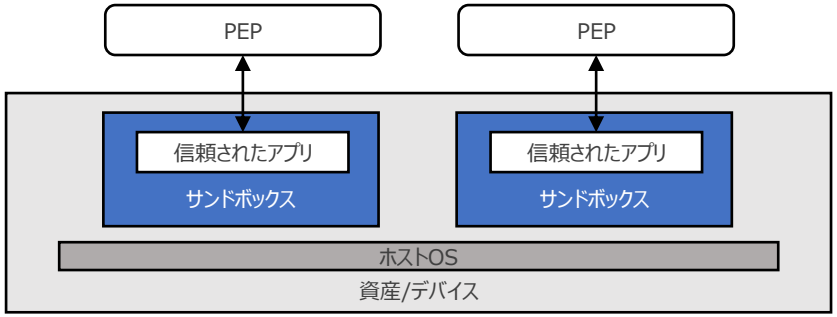
リソースポータルモデル

BYOD等エージェントをインストールできない端末からのアクセスに対して有用である。



アプリケーションのサンドボックス

個々のアプリケーションが他のアプリケーションから分離・保護されるモデルであり、MAM(Mobile Application Management)導入が一つの実装になる。



3.4.1 海外事例調査結果（Google社「BeyondCorp」）- 特徴と概要（1/2）

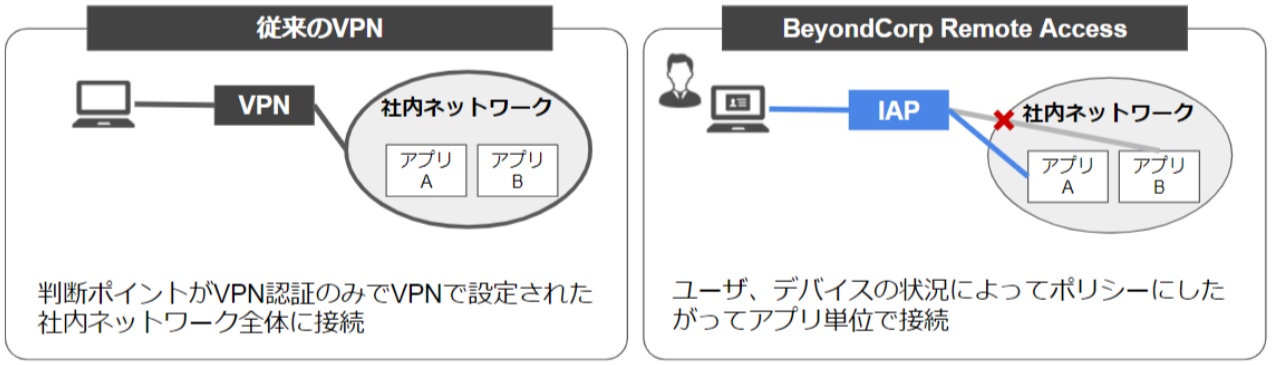
- Google社のゼロトラストアプローチに基づき構築したセキュリティネットワーク「BeyondCorp」について調査した。Google社自身の利用状況だけでなく、製品化されたクラウドソリューション「BeyondCorp Remote Access」の情報も補足的に参照している。
- 製品情報は2021年1月調査時点のものである。

特徴

Google社の従業員は、VPNを利用しなくても、サービス側でアクセス制御されているため、一般公開されていないイントラサイトに接続することが可能

VPNでは下記のような問題点があるが、それを解決するための技術として現在ではGoogle社の従業員が活用しているとのこと。

＜VPNの問題点＞
- 全社員が利用するVPNを短期間で構築するのは難しい
- 利用者によっては、VPNの設定は複雑である
- 判断ポイントがVPNの認証のみとなり、必要ないアプリにも接続可能となる
- 攻撃者に一度侵入を許すと被害が拡大する可能性が高い



図：従来のVPNとBeyondCorp Remote Accessとの違い

IAP(Identity-Aware Proxy)：
従業員が VPN を使用せずに信頼できないNWから会社のアプリやリソースにアクセスできるようにするための仕組み

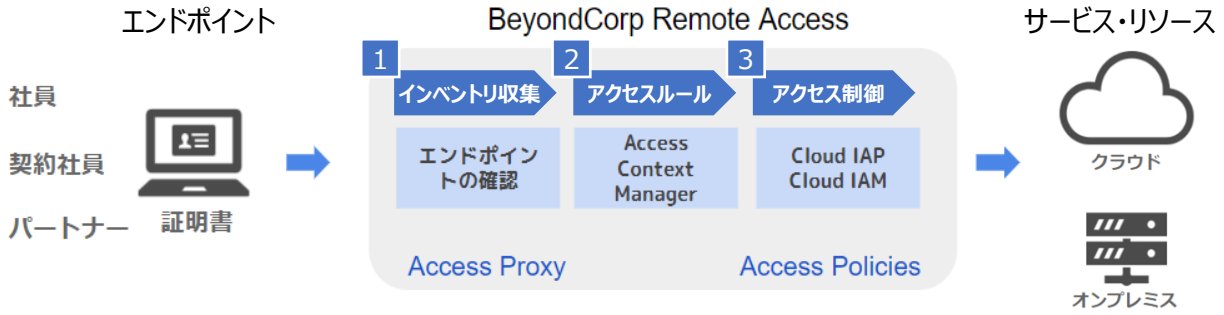
3.4.1 海外事例調査結果（Google社「BeyondCorp」）- 特徴と概要（2/2）

概要

BeyondCorpでは、
1. エンドポイントに関する属性情報（インベントリ）の収集
2. アクセスルールの定義
3. アクセス制御

の3つの仕組みで、アクセス制御を実現している。従来の境界型のアクセス制御と異なり、サービス毎にアクセスルールを定義し、そのルールに応じたアクセス制御を行う。それにより、各サービスへのアクセスは動的に制御され、かつ信頼レベルに応じた段階的な認証・認可が行われる。

具体的には、「Endpoint Verification*1」を利用し、インベントリ（暗号化ステータス、OSやユーザーの詳細など）情報を収集する。また、「Access Context Manager*2」を使用して、アクセスルールを定義する。そのルールに基づいて、「IAM Conditions*3」によって、各サービス・リソースに対するアクセス制御を行う。また、「IAP」を使用することでネットワークレベルのファイアウォールに頼らずに、リソースレベルのアクセス制御モデルを確立できる。



図：BeyondCorp Remote Accessの仕組み

*1 Chrome 拡張機能がインストールされているデバイスに関する属性を収集する拡張機能。
*2 Google Cloudのプロジェクトとリソースに対するアクセス制御を行う機能。ユーザー属性（デバイスの種類とOS、IPアドレス、ユーザーID等）に応じた制御が可能。
*3 Google Cloudリソースに対する条件付き、属性ベースのアクセス制御を定義して適用できる機能。IAMはIdentity and Access Managementの略語。

3.4.2 海外事例調査結果（Google社「BeyondCorp」）- 評価結果

- リモートワーク阻害要因に対し、当社調査での範囲でGoogle社「BeyondCorp」にて対策可能な機能を確認し一覧で示した。

表：「BeyondCorp」にて対策可能な機能一覧（当社調べ）

#	リモートワーク阻害要因	Google BeyondCorp	該当機能の概要
1	回線逼迫	○	IAPによりVPNを使わずにアクセス可能。
2	Wi-Fi設定	○	署名付きのIAPヘッダーを使用しアプリを保護。
3	端末管理	○	Googleエンドポイント管理を利用して端末を管理。
4	BYOD	○	インタビューにてBYOD制度があることを確認。 ただ、実際には必要性を感じていなかったり、手続等煩雑なため利用者はほとんどいないとのこと。
5	外部デバイス	○	Googleエンドポイント管理の「Windows向けの高度なデスクトップセキュリティ」で制御。
6	プリンタ	○	Google Driveのファイル共有オプションにて制御。
7	外部メール	-	-
8	個人クラウド	○	Google Cloud Identity / Resource Manager による組織のポリシーにて制御。
9	内部不正	-	-
10	高機密データ	-	-

○：対策可能
-：対策可能なソリューションを確認できなかった

3.5.1 海外事例調査結果（マイクロソフト社「ゼロトラストセキュリティ」）
- 特徴と概要（1/2）

- ゼロトラスト基盤技術に先進的に取り組んでいるマイクロソフト社の「ゼロトラストセキュリティ」について調査した。マイクロソフト社のゼロトラスト成熟度モデルの論文だけでなく、製品化されたソリューションの情報も補足的に参照している。
- 製品情報は2021年1月調査時点のものである。

概要

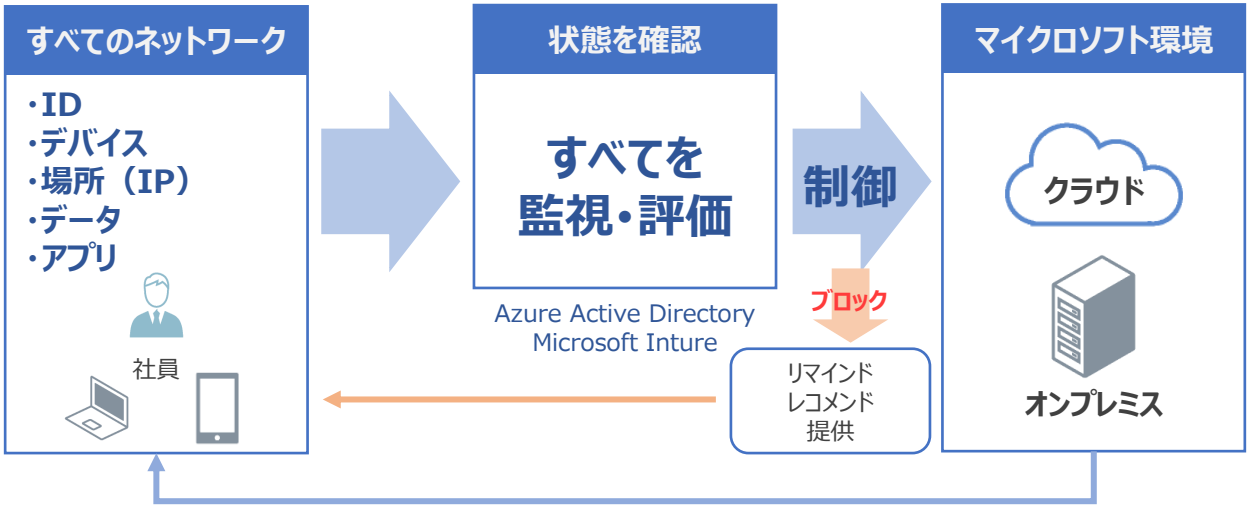
理想的なゼロトラスト環境では4つの要素（**①ID、②デバイス、③アクセス権、④サービス**）が必要という考え方から、その４要素を構造化したアプローチを採用している。

3.5.1 海外事例調査結果（マイクロソフト社「ゼロトラストセキュリティ」）
- 特徴と概要（2/2）

特徴

主要なコンポーネントは、デバイス管理とデバイスセキュリティポリシー構成用の「Intune」、デバイスヘルス検証用の**AzureAD条件付きアクセス**およびユーザーとデバイスインベントリ用の「AzureAD」の2つである。

主要コンポーネント以外にもOSからOffice365など、デバイス自身やファイルなど含めて全体をカバーしている。



3.5.2 海外事例調査結果（マイクロソフト社「ゼロトラストセキュリティ」）
- 評価結果

- リモートワーク阻害要因に対し、当社調査の範囲でマイクロソフト社「ゼロトラストセキュリティ」にて対策可能な機能を確認し、一覧で示した。

表：マイクロソフト社「ゼロトラストセキュリティ」にて対策可能な機能一覧（当社調べ）

#	リモートワーク阻害要因	マイクロソフト ゼロトラスト セキュリティ	該当機能の概要
1	回線逼迫	○	AzureAD Application Proxyにて実現。
2	Wi-Fi設定	○	グループ ポリシー オブジェクト、Microsoft Intuneにて設定。
3	端末管理	○	System Center Configuration Manager、Microsoft Intune等にて実施。
4	BYOD	○	個人端末を社内のレギュレーションに合わせるキッティングを実施する。
5	外部デバイス	○	System Center Configuration Manager、Microsoft Intune等にて実施。
6	プリンタ	○	データそのものの制御（Azure Information Protection）。
7	外部メール	○	Microsoft Cloud App Security、インサイダーリスク管理にて制御。
8	個人クラウド	○	AzureADテナント制限。
9	内部不正	○	インサイダーリスク管理。
10	高機密データ	-	-

○：対策可能
-：対策可能なソリューションを確認できなかった

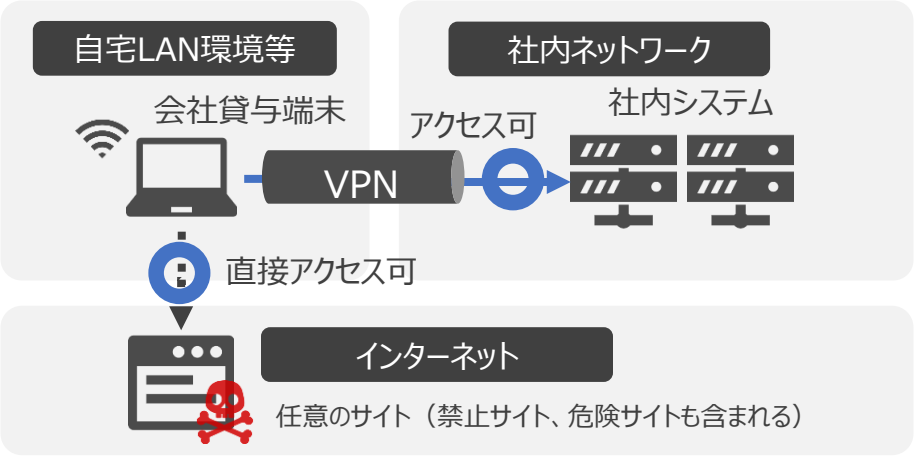
3.6.1 ネットワーク事業者事例調査結果（ソフトバンク株式会社）- 常時VPN（1/3）

- 国内ネットワーク事業者の取り組み事例として、通信キャリアであるソフトバンクのサイバーセキュリティ対策を調査した。同社の対策はZTA導入前であるものの、リモートワーク阻害要因に対しリスク低減効果が見込まれる施策であるため今回の調査対象とした。
- 本項では常時VPN化前の課題について説明する。

課題

これまでソフトバンクではリモートワークなどの社外環境において、会社貸与端末から社内システムへアクセスする際、VPNを必須としていたが、社外のサイトへアクセスする場合には、VPNを張らずに直接アクセスすることが可能であった。

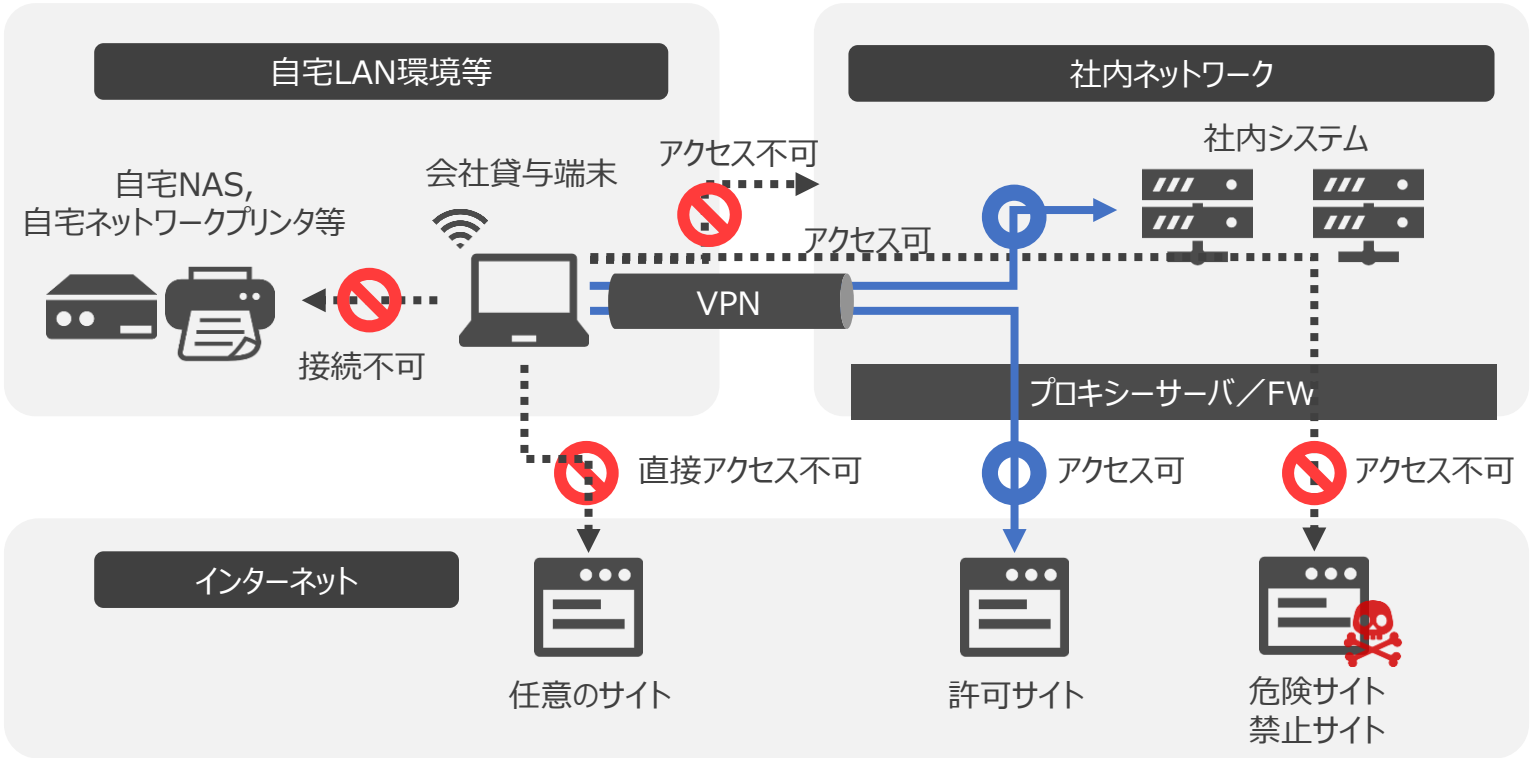
このため、アクセスを禁止しているサイトや危険なサイトへのアクセスを企業側が監視・制御できない状態にあった。



3.6.1 ネットワーク事業者事例調査結果（ソフトバンク株式会社）- 常時VPN（2/3）

- 常時VPN化の実施内容とアクセスルート、制御状況を以下の図に示す。

前頁に示した課題を解決するため、管理者側で端末側からの全ての通信を強制的にVPN経路でアクセスさせるようパラメタを設定（社員による設定変更は不可）。
これにより、常にVPN経由でなければ社内外のサイトへアクセスできない仕様とし、企業側によるアクセス制御や通信監視が可能になった。またWEBサイトへのアクセスだけでなく、自宅のNASやネットワークプリンタへのアクセスも不可となり、社内情報の持ち出し防止としての効果にもつながった。

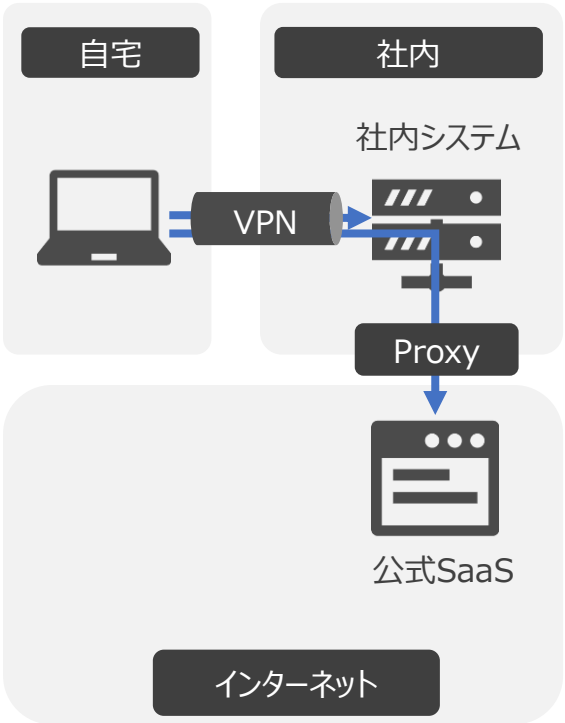


3.6.1 ネットワーク事業者事例調査結果（ソフトバンク株式会社）- 常時VPN（3/3）

- ZTA化を検討している企業への参考事例として、ソフトバンクの常時VPNからZTA化までの構成の遷移計画を３ステップにまとめた。

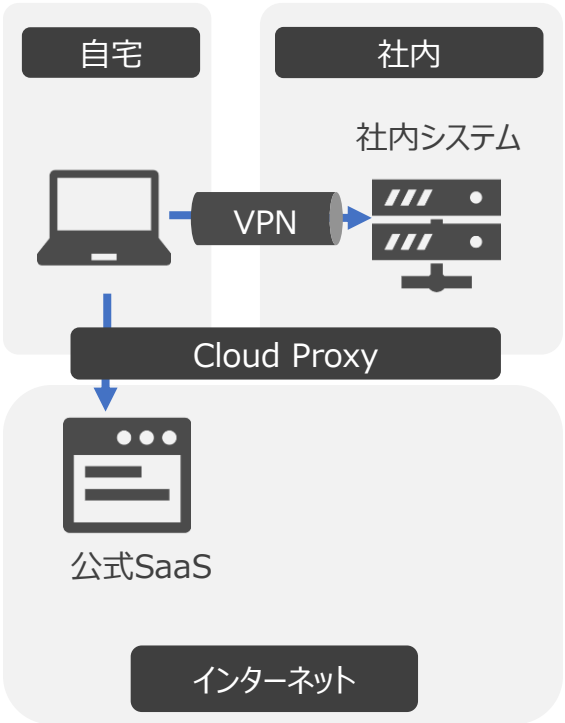
Step1

社外のアクセスを常時VPN化



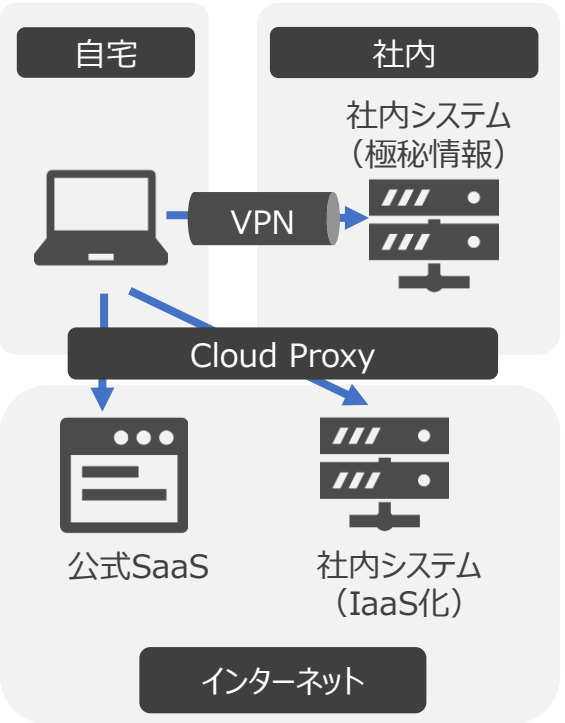
Step2

インターネットアクセスを クラウドプロキシ化



Step3

社内システムをIaaS化
（通信の秘密等の極秘情報は境界型防御を継続）



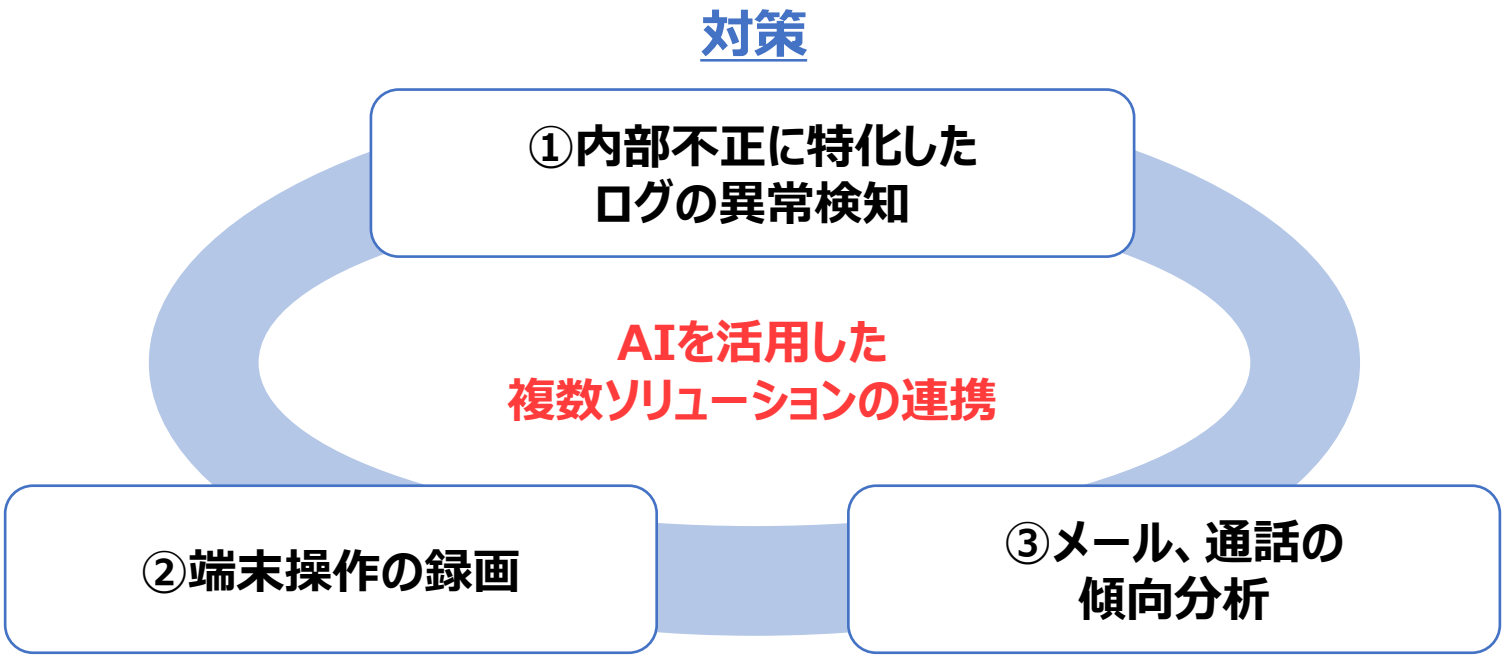
※一般的な企業がZTA化を計画する場合の構成パターンを「(参考) ZTA導入のパターン」に記載する。

3.6.2 ネットワーク事業者事例調査結果（ソフトバンク株式会社）- 内部不正対策

- 高機密な情報を扱う企業において、内部不正対策は非常に重要な取り組みである。扱う情報の重要性や機密レベルにより対応のレベルは異なるが、ネットワーク事業者としてソフトバンクの内部不正対策の概要と、リモートワークにおける効果について確認する。
- また技術的な要素だけではなく、従業員に対するセキュリティ意識向上訓練を実施することも重要である。

概要

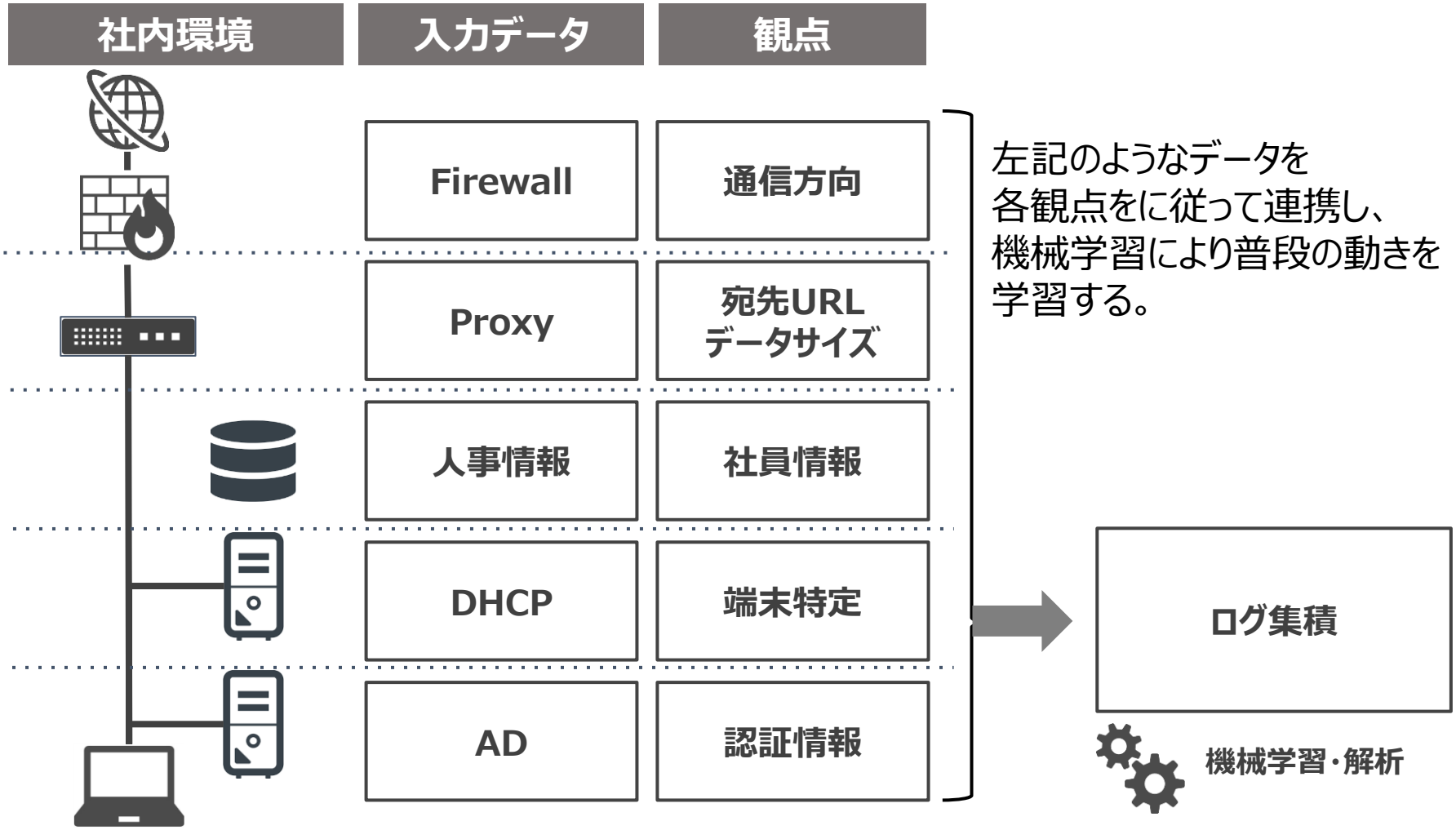
ソフトバンクの内部不正対策は、大きく３つの領域に取り組んでいる。各領域の情報は連携され、組み合わせることで高い網羅性を実現している。



3.6.2 ネットワーク事業者事例調査結果（ソフトバンク株式会社）
- 内部不正対策　①ログの異常検知（1/2）

- 複数種類のログデータを用いた機械学習、統計分析をすることにより、不正と思われる異常なふるまいを検知する。

（入力するデータとその観点の例）



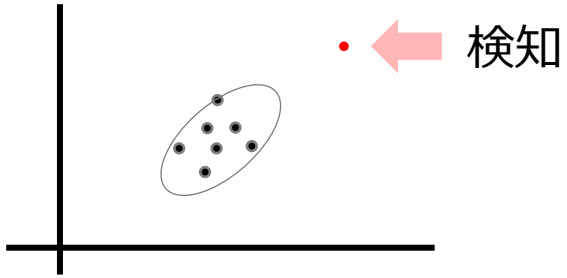
3.6.2 ネットワーク事業者事例調査結果（ソフトバンク株式会社）
- 内部不正対策　①ログの異常検知（2/2）

（ログ解析と異常値検知）

- 通信や端末動作のログの解析により異常なふるまいを検知する仕組みを導入し、大量データ送信等を検知できるようにする。
- 機械学習により通常のログ傾向を学習し、統計分析により異常値を検知する。

表：「ログの異常検知」により検知が可能な項目

項目	検知内容
データ送受信	• 普段と異なるデータのやり取り • 外部へ大量データ送信
不審アクセス	• 普段アクセスしない場所へのアクセス • 疑わしいドメインへの接続
認証・その他	• 普段と異なる時間のアクセス



3.6.2 ネットワーク事業者事例調査結果（ソフトバンク株式会社）
- 内部不正対策　②端末操作の録画

- 端末やサーバにエージェントを導入することで、以下のような機能を実現する。

機能

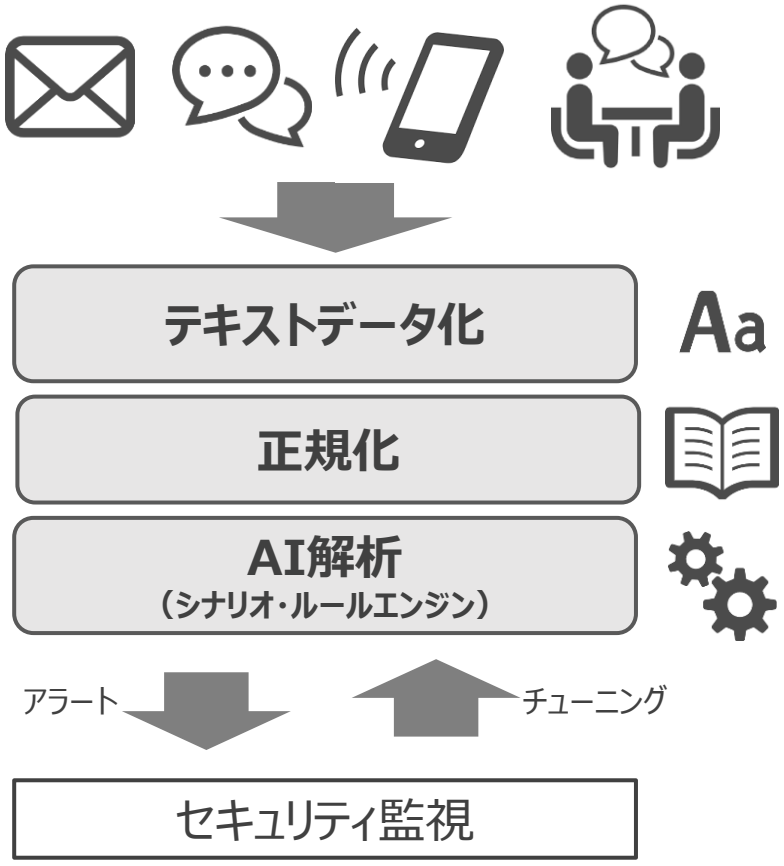
検知	調査	抑止
• 悪意のあるふるまいの検知 • 過失の検知 • テキスト分析	• 端末画面、サーバ画面の連続録画 • 録画内容のメタデータ化により長期保管	• プロセスブロック • ポップアップ警告

（期待される効果）

- 画面の動きや画面内で入力されたテキストの内容を含めた分析により、怪しいふるまいの検知ができる。
- 端末、サーバ上の操作がすべて画面の録画として記録できるため、端末上のプロセスの動きや通信系のログの他、通常のOS等のログでは残らないサイト上での操作、サイトの表示内容、マウスの動き、開いたファイルの内容の特定などができ、実際の操作を示す証跡に使うことができる。
- 端末の操作内容に応じて、端末内のプロセスブロックや、ポップアップで警告を出したりすることにより、不正を未然に防止することができる。また、セキュリティルールの教育効果もある。

3.6.2 ネットワーク事業者事例調査結果（ソフトバンク株式会社）
- 内部不正対策　③メール、通話の傾向分析

- 言語情報をテキストデータ化・正規化しAI解析を行うことで不正の予兆検知等を実現する。



（機能の概要）
- メール、チャット等テキストデータ
- 通話、会議中の会話等の音声データ

といった言語情報をもとに、入力データの言語解析を行い、不審な動きを検知することにより、不正の予兆検知や外部共犯者の検知などにつなげる。

（期待される効果）
- **人の相関関係可視化**
  疑義者とのコンタクトを可視化→時間・頻度・関係性
- **非構造データの分析**
  シナリオ・ルールに基づいた不正・違反の検知
- **不正の予兆・発見**
  情報漏えい以外にコンプライアンス違反なども応用可能

3.6.3 ネットワーク事業者事例調査結果（ソフトバンク株式会社）- 評価結果

- リモートワーク阻害要因に対して、常時VPNと内部不正対策が補完関係でリスクを軽減する効果があるかを評価し、以下表にまとめた。
- 常時VPNと内部不正対策の補完関係によるリスク軽減効果を確認できた。

表：ネットワーク事業者（ソフトバンク）の事例にて対策可能な機能一覧

#	リモートワーク阻害要因	ソフトバンク事例		該当機能の概要
		常時VPN	内部不正対策	
1	回線逼迫	-	-	※ネットワーク事業者は問題になりにくい
2	Wi-Fi設定	○	-	Wi-Fi設定によらずVPNで暗号化した経路が確保される。
3	端末管理	○	-	常にVPNが張られるため設定更できる。
4	BYOD	-	-	※別の対策（VDI）により対策済み
5	外部デバイス	-	○	基本制限されており、不正に利用された場合もふるまいにより検知される。
6	プリンタ	-	-	※ペーパーレス化のため問題になりにくい
7	外部メール	-	○	メールの内容からも不正の検知がされる。
8	個人クラウド	-	○	不審なアップロードが検知される。また、クラウド上での操作も端末画面録画で後から追える。
9	内部不正	-	○	3つの内部不正対策の組み合わせにより守っている。
10	高機密データ	-	-	-

○：対策可能
-：対策可能なソリューションを確認できなかった

3.7 まとめ

- 現時点では、既存のZTAの海外事例に内部不正対策を追加しても、高機密データを取り扱う業務をリモートワーク推進することは難しいと考える。

表：各事例の結果のまとめ

#	リモートワーク阻害要因	海外事例（ZTA）		ソフトバンク事例	
		Google BeyondCorp	マイクロソフト ゼロトラスト セキュリティ	常時VPN	内部不正対策
1	回線逼迫	○	○	※ネットワーク事業者は問題になりにくい	
2	Wi-Fi設定	○	○	○	-
3	端末管理	○	○	○	-
4	BYOD	○	○	※別の対策（VDI）により対策済み	
5	外部デバイス	○	○	-	○
6	プリンタ	○	○	※ペーパーレス化のため問題になりにくい	
7	外部メール	-	○	-	○
8	個人クラウド	○	○	-	○
9	内部不正	-	○	-	○
10	高機密データ	-	-	-	-

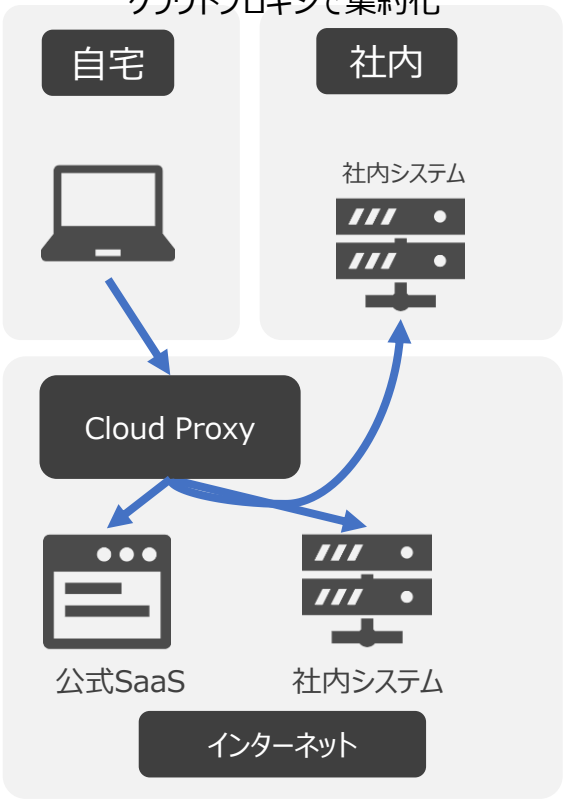
○：対策可能
-：対策可能なソリューションを確認できなかった

（参考）ZTA導入のパターン

- 一般的な企業がZTA化を計画する場合の参考となるように構成パターンを下記に記載した。各企業の現在の構成や優先するテーマにより選択すべきパターンは異なる。最終的に全ての対応が必須ではない。

パターンA

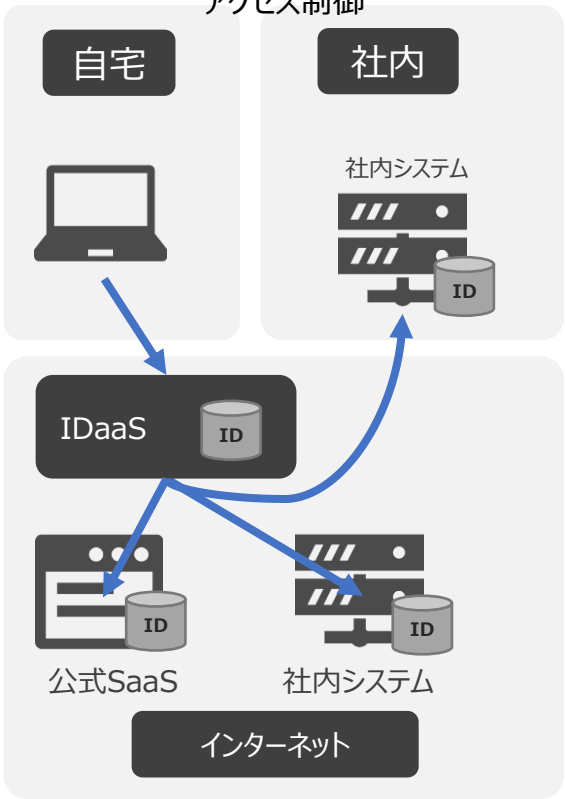
社内外でのアクセスを
クラウドプロキシで集約化



VPNやProxyを未導入な企業が
導入し易い

パターンB

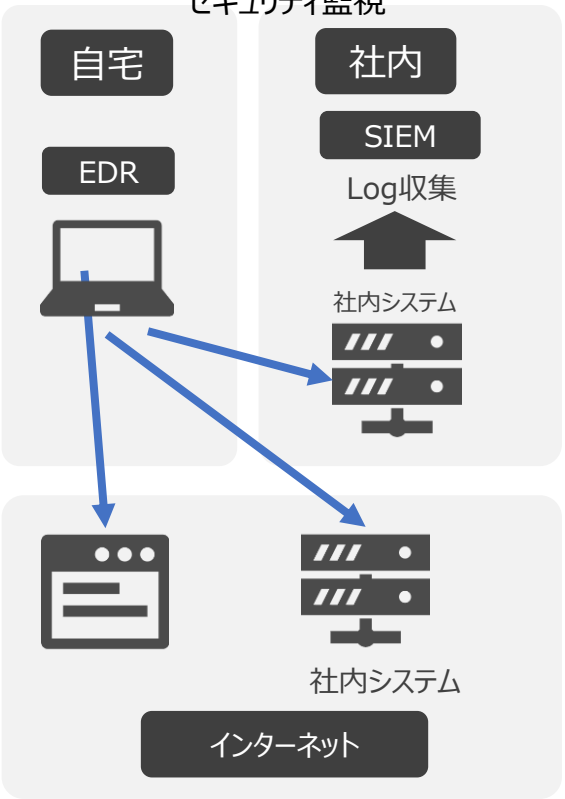
IDaaS導入により
アクセス制御



統合認証SSOを未導入な企業が
導入し易い

パターンC

SIEM、EDR等による
セキュリティ監視



すでにSOCを保有するか、
委託している企業が導入し易い

（参考）ZTAへの取り組み

- 一般的な企業がZTAへ取り組む場合、以下のようなソリューションの導入から検討するのが進めやすいと考えられる。あくまでも具体的にイメージするための例示であり、当該ソリューションを推奨するものではない。

A. ゼロトラストネットワークの構築（ZTNA）

アクセス元およびアクセス先を集約し、監視・制御ができるようにする。

- Zscaler Private Access (Zscaler)
- PulseWorkspace (Pulse Secure)
- Secure Access Cloud (Broadcom)

B. アイデンティティ管理の統合

アクセスしようとする人が用いるデバイス、ネットワーク、アプリケーション、場所などから判断し、認証強度の制御などをする。

- Okta Identity Cloud (Okta)
- Azure AD Application Proxy (マイクロソフト)
- Onelogin (Onelogin)

C. EDRによるセキュリティ監視

EDR(Endpoint Detection and Response) によりPCの操作や振る舞いの監視を行い、サイバー攻撃等を受けたことを検知・対処する。

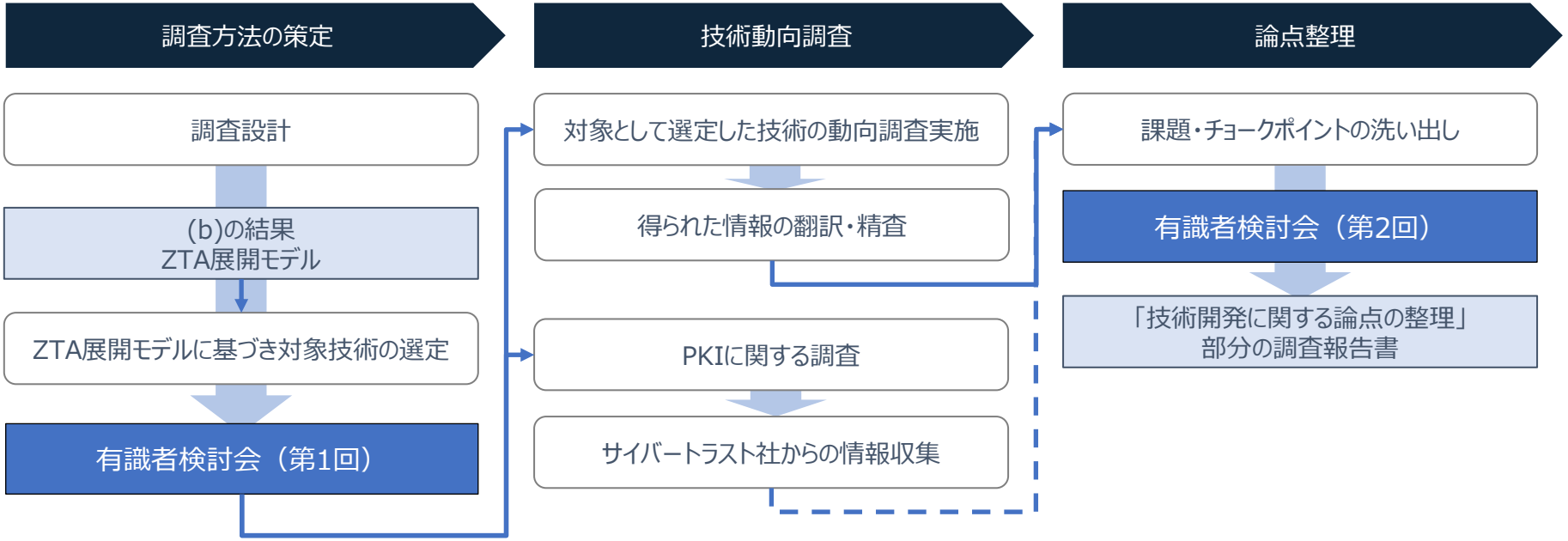
- Cybereason (Cybereason)
- CrowdStrike (CrowdStrike)
- Carbon Black (Carbon Black)

4. ①調査研究事業
(c)技術開発に関する論点の整理

4.1 調査概要

(c)技術開発に関する論点の整理

- **目的**
  ZTNAやSDPのメインプレイヤーの最新の取り組みや周辺技術動向の情報を収集し、適用可能性を考慮した上で、懸念点や課題を抽出する。
- **調査内容**
  - 方法：
    ガートナー社のレポート調査、インターネット上の公開情報調査、当社グループ企業「サイバートラスト」からの情報収集
  - 対象：
    ZTNA/SDP,VDI,UEM,MAM,PKI
  - 時期：　2020年12月～2021年2月
- **論点整理の留意点**
  - チョークポイントの洗い出し
    - 日本のソリューションが存在するか
  - PKIの課題の洗い出し



4.2 調査実施

- ZTNAやSDPのメインプレイヤーの最新の取り組みや周辺技術動向の情報を収集し、適用可能性を考慮した上で、懸念点や課題を抽出するという目的に沿って、下記の調査を行った。

	技術動向調査	（追加調査）PKIに関する調査
内容	リモートワーク要件との親和性が高いZTA展開モデルを参照し、選出した技術に関する動向調査 （各技術の概要、動向、メインプレイヤー）	・PKIに関する課題を洗い出すための情報調査、および当社グループ企業「サイバートラスト」からの情報収集 ・PKIに関連する懸念点の整理
対象	・ZTNA／SDP (Software Defined Perimeter) ・VDI (Virtual Desktop Infrastructure) ・UEM (Unified Endpoint Management) ・MAM (Mobile Application Management)	・PKI (Public Key Infrastructure)
方法	・ガートナー社のレポート調査 ・インターネット上の公開情報を用いた文献調査	・インターネット上の公開情報を用いた文献調査 ・当社グループ企業「サイバートラスト」からの情報収集
期間	2020年12月～2021年2月	2020年12月～2021年2月

4.2.1 調査実施 - 調査対象

- 調査対象として、3.3節に記載したZTA展開モデルを参考に、4つの要素技術を選定した。

ZTA展開モデルを参考に、モデル毎のソリューション例から
① ZTNA／SDP (Software Defined Perimeter)
② VDI (Virtual Desktop Infrastructure)
③ UEM (Unified Endpoint Management)
④ MAM (Mobile Application Management)
とした。

調査方法はガートナー社の提供する調査レポートの活用を主とした。一部、インターネット上の公開情報を補足的に参照して結果をまとめた。

調査対象技術		
ZTA展開モデル（NIST SP 800-207）		
ゲートウェイモデル*1	リソースポータルモデル	アプリケーションサンドボックスモデル
① ZTNA／SDP	② VDI	③ UEM ④ MAM

*1 3.3.4項に示したモデルのうち、「デバイスエージェント／ゲートウェイモデル」と「エンクレイブゲートウェイモデル」を「ゲートウェイモデル」と表現した。

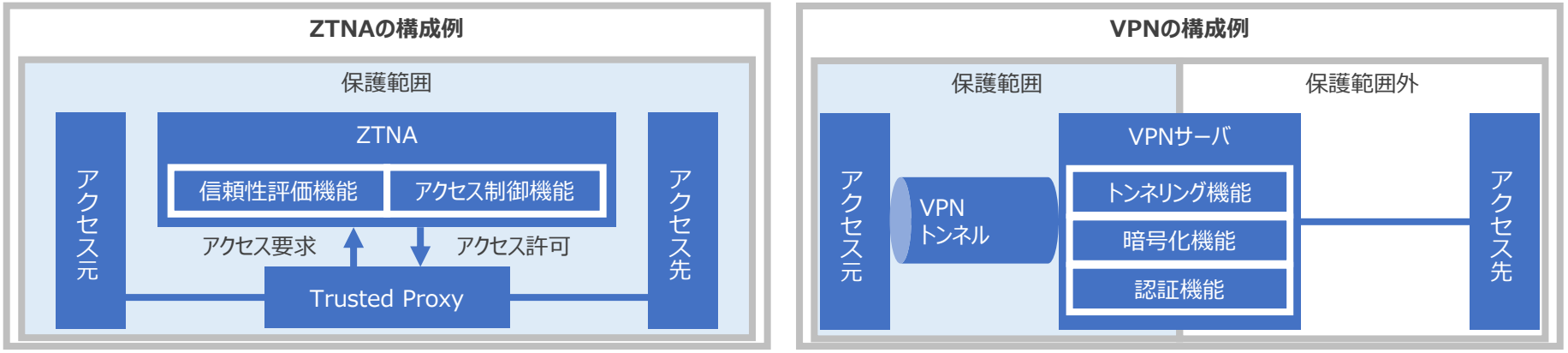
4.3.1 調査結果 ①ZTNA／SDP - 概要および技術動向

概要

ZTNAとは、アクセス元に対してアクセス許可を継続的に評価して与えるというZTAの考え方を取り入れた製品およびサービスである。従来のインターネットとイントラネットの間をVPNで認証し、アクセスさせるなどの境界型セキュリティとは異なり、アクセス先（アプリケーションや情報資産等）への接続要求が発生するたびにアクセス元の状態（ユーザー情報や端末のセキュリティ状態等）を評価し、動的にアクセス許可を与える仕組みとなっている。

SDPも集中的なアクセス制御を行うという考え方は同じであるため、本調査では同一のものとして扱うこととする。

下図のとおりZTNAはVPNと比較して保護範囲が広いという特徴がある



技術動向

昨今のリモートワーク需要増加にともない注目されており、特にVPNと比較されることが多い。

クラウド型サービスを例にとると、アクセス元とアクセス先の通信を仲介する形でアクセス制御やアクセス許可を一元的に行う仕組みとなっている。大手ベンダーでは仲介する拠点を複数もっており、近い拠点を自動的に選択する仕組みをもつことで低遅延を実現させている。インターネット上で実現させる為、デジタル・トランスフォーメーションの取組みの結果、ほとんどの企業でアプリケーション、サービス、データを社内よりも社外に置くことが主流になると考えられる。

4.3.2 調査結果 ①ZTNA／SDP - メインプレイヤー（1/2）

- ZTNA／SDPのメインプレイヤーと提供製品を以下に示す。

■オンプレミス型製品

提供会社	本社	製品名
AppGate (split from Cyxtera)	アメリカ	AppGate SDP
BlackRidge	アメリカ	Transport Access Control
Google Cloud Platform (GCP)	アメリカ	Cloud Identity-Aware Proxy (Cloud IAP)
マイクロソフト	アメリカ	Azure AD Application Proxy
		Web Application Proxy (Windows server only)
Odo	イスラエル	Zero trust access platform
Pulse Secure	アメリカ	Pulse SDP
Safe-T	イスラエル	Secure Application Access
Systancia	フランス	Systancia Gate
Unisys	アメリカ	Stealth
Verizon	アメリカ	Vidder PrecisionAccess
Waverley Labs	アメリカ	Open Source Software Defined Perimeter
Zentera Systems	アメリカ	CoIP Platform

4.3.2 調査結果　①ZTNA／SDP - メインプレイヤー（2/2）

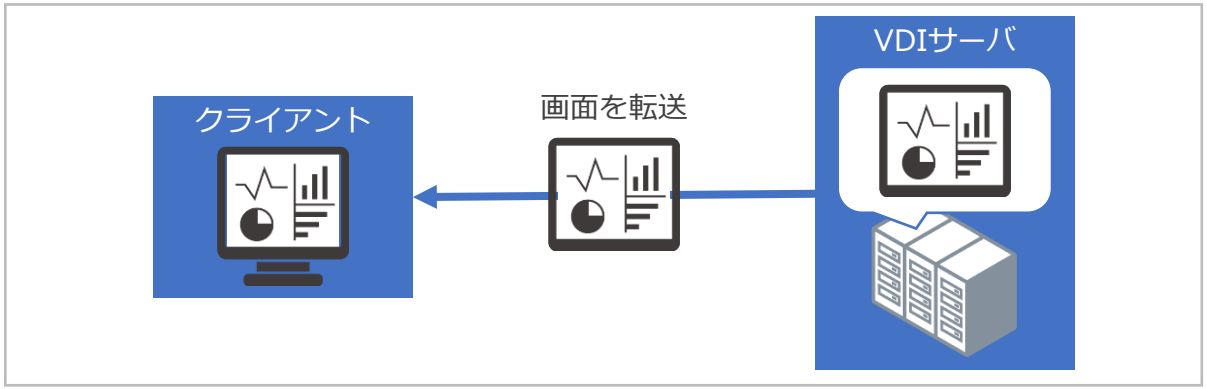
■クラウド型サービス

提供会社	本社	製品名
Akamai	アメリカ	Enterprise Application Access
Axis Security	イスラエル	App Access Cloud
Banyan	アメリカ	Zero Trust Remote Access Platform
Broadcom	アメリカ	Secure Access Cloud
Cato Networks	イスラエル	Cato Cloud
Cisco	アメリカ	Duo
Citrix	アメリカ	Workspace Essentials
CloudDeep Technology (China only)	中国	DeepCloud SDP
Cloudflare	アメリカ	Cloudflare Access
Cognitas Technologies	アメリカ	Crosslink
Google	アメリカ	BeyondCorp Remote Access
Hangzhou Cloudaemon Technology	中国	Taiji Perimeter
InstaSafe	インド	Secure Access
NetFoundry	アメリカ	Zero Trust Networking Platform
Netskope	アメリカ	Netskope Private Access
Okta	アメリカ	Okta Identity Cloud
OPAQ	アメリカ	Secure Access Service Edge
Palo Alto Networks	アメリカ	Prisma Access
Perimeter 81	イスラエル	Software-Defined Perimeter
Proofpoint	アメリカ	Proofpoint Meta
SAIFE	アメリカ	Continuum
TransientX	アメリカ	TransientAccess
Wandera	アメリカ	Wandera Private Access
Zero Networks	イスラエル	Access Orchestrator
Zscaler	アメリカ	Private Access

4.4.1 調査結果　②VDI - 概要および技術動向

概要

VDIとは、クライアントのデスクトップ環境をサーバ上に用意し、作業をサーバ上の環境下で完結させることを目的とした仕組みである。クライアントにはサーバ上のデスクトップ画面が表示され、そこで作業を行うため、クライアントからの情報漏えいのリスク軽減効果が期待できる。



図：構成例

技術動向

クラウド上にVDIを構築しサービス提供するDaaSは、利用者増加に伴うスケールアップが容易に行えることや、拠点も国や地域に幅広く展開されてきていることから、VDIの利用用途にマッチしている。これまでは利用企業やソリューションベンダがDaaSを構築・提供してきたが、クラウドベンダ自体がDaaSを提供する動きも進んでいる。

アクセス先が利用企業の内部システムにもある場合は、利用企業の環境に構築するオンプレミス型のVDIソリューションとDaaSを組み合わせたハイブリッド型のVDIソリューションも提供されている。

4.4.2 調査結果 ②VDI - メインプレイヤー

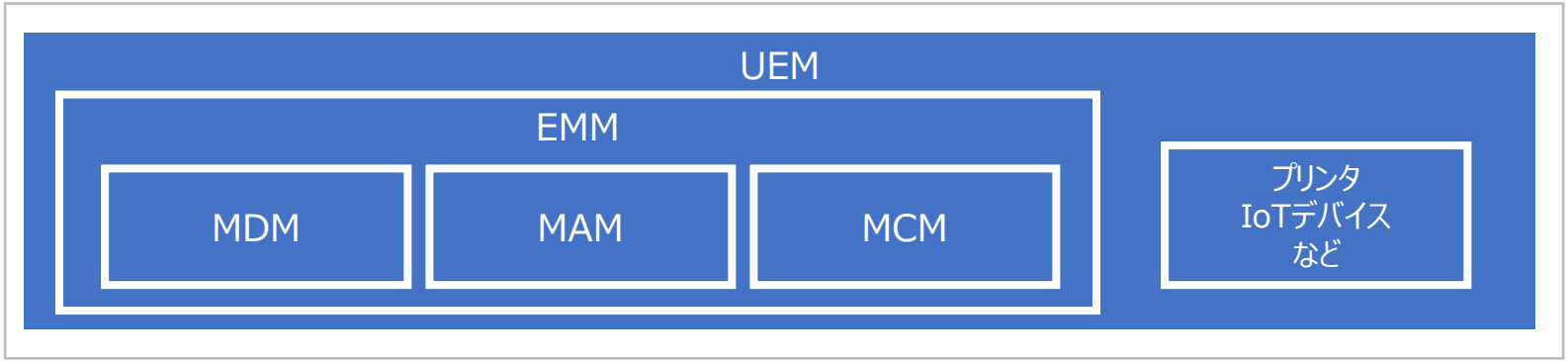
- VDIのメインプレイヤーと提供製品を以下に示す。

提供会社	本社	製品名
Anunta	インド	Managed DaaS on Azure Cloud Fully Managed Horizon Desktops
Amazon Web Service	アメリカ	Amazon WorkSpaces
Citrix	アメリカ	Citrix Managed Desktops
Cloudalize	ベルギー	Desktop-as-a-Service
CloudJumper	アメリカ	Cloud Workspace
dinCloud	アメリカ	dinWorkspace
Diso	スイス	Secure Workplace
Dizzion	アメリカ	Cloud Desktops
Effortless Office	アメリカ	Effortless Desktop
Evolve IP	アメリカ	Desktop as a Service
Kivito	ドイツ	deskMate
マイクロソフト	アメリカ	Windows Virtual Desktop
Nutanix	アメリカ	Xi Frame
Paperspace	アメリカ	Paperspace Core
Cox Business-RapidScale	アメリカ	Desktop as a Service
Tehama	カナダ	Tehama
Tilon	韓国	Dstation
VMware	アメリカ	Horizon Cloud
Workspot	アメリカ	Workspot Desktop Cloud

4.5.1 調査結果 ③UEM - 概要および技術動向

概要

UEMとはエンドポイントのデバイスを一元的に管理することを目的とした製品である。モバイルデバイスの管理製品であるMDM（モバイルデバイス管理）やMAM（モバイルアプリケーション管理）およびMCM（モバイルコンテンツ管理）を統合しており、プリンタやIoTデバイスも管理対象としている。



図：UEMの位置づけ

技術動向

エンドポイントのデバイス管理技術としては、端末からスマートフォンのデバイスを管理する為のMDM、スマートデバイス上の業務アプリケーションを個人利用のアプリケーションと分離して管理する為のMAM、メールデータや業務ファイルなどコンテンツを管理する為のMCMが存在する。また、それらを統合した製品としてEMM（Enterprise Mobility Management）が登場し、さらにEMMから管理対象を拡張したUEMが登場してきた。

UEMは今までデバイス管理を別々の製品で行ってきた場合や、より管理対象を増やしたい場合（プリンタやIoTデバイスなど）に向いているが、多機能であるため、目的に応じて製品選定を行う必要がある。

4.5.2 調査結果 ③UEM - メインプレイヤー

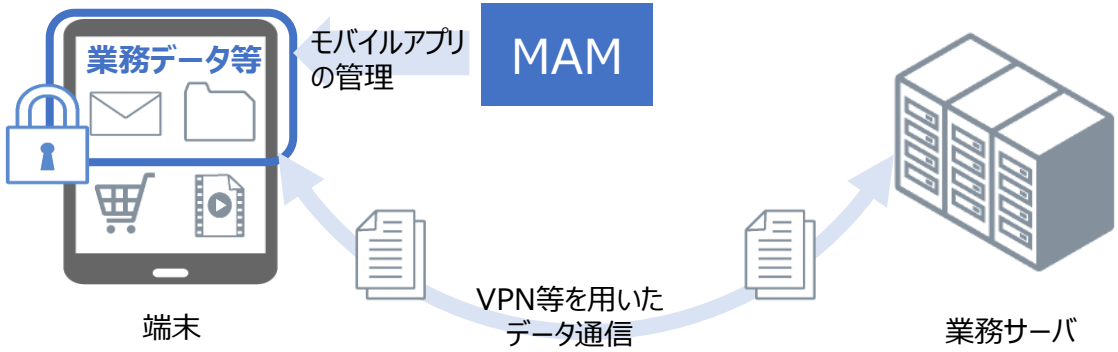
- UEMのメインプレイヤーと提供製品を以下に示す。

提供会社	本社	製品名
42Gears	インド	SureMDM
Cisco	アメリカ	Meraki Systems Manager
Google	アメリカ	endpoint management
Hexnode	アメリカ	Hexnode MDM
IBM	アメリカ	MaaS360 UEM
Ivanti	アメリカ	Ivanti UEM
Zoho	アメリカ	ManageEngine
Matrix42	ドイツ	Secure Unified Endpoint Management
マイクロソフト	アメリカ	Microsoft Endpoint Manager
ProMobi Technologies	インド	Scalefusion
Sophos	イギリス	Sophos Mobile
VMware	アメリカ	Workspace ONE

4.6.1 調査結果 ④MAM - 概要および技術動向

概要

MAMとはスマートフォンやタブレットなどのモバイル端末にインストールされたアプリケーションを管理する仕組みである。
モバイル端末を業務利用するアプリケーションやデータのみを分離して管理できることから、個人所有の端末を業務に利用するBYODの用途で使われることが多い。



図：構成例

技術動向

MAMツールはBYODの用途やアプリやアプリのライセンス管理を行いたい企業、独自のアプリストアを運営している場合の利用に向いている。
モバイル管理の関連技術としては他に、モバイル端末自体の設定などを管理するMDMや業務に必要なコンテンツを管理するMCMがあり、またMDMやMAMおよびMCMを統合したEMMが存在する。それぞれ利用用途によりメリット・デメリットがあるため、目的に照らし合わせて最適な技術を選択する必要がある。

4.6.2 調査結果 ④MAM - メインプレイヤー

- MAMのメインプレイヤーと提供製品を以下に示す。

提供会社	本社	製品名
Appaloosa	フランス	Appaloosa MAM
App47	アメリカ	MAM
Apperian	アメリカ	Apperian MAM
Oracle	アメリカ	Oracle Mobile Security Suite
Pulse Secure	アメリカ	PulseWorkspace

4.7 まとめ

- リモートワークを行う上で必要と考えられる調査対象技術を使用したサービスやシステムに対して、日本に本社を置くメインプレイヤーが存在していない現状が確認できた。地政学的リスクを考慮する場合は国別でのマルチベンダ対応が求められる。
- また、サービスやシステムを構築・利用する上で、NIST SP800-171*1やGDPR（General Data Protection Regulation）*2など海外のルール・標準・法律によって規制を受ける可能性についても考慮する必要がある。

■調査対象技術毎の国別内訳　（社数）

	アメリカ	イスラエル	フランス	中国	インド	ベルギー	スイス	ドイツ	イギリス	韓国	日本
ZTNA SDP	27	6	1	2	1						**0**
VDI	13				1	1	1	1		1	**0**
UEM	8				2			1	1		**0**
MAM	4		1								**0**

*1 非連邦政府のシステムおよび組織に存在する「機密指定はされていないが管理対象となる情報」を保護するための推奨セキュリティ要件を示したもの。
*2 欧州連合 (EU) 内の全ての個人のために、データ保護を強化し統合することを意図する規則のこと。

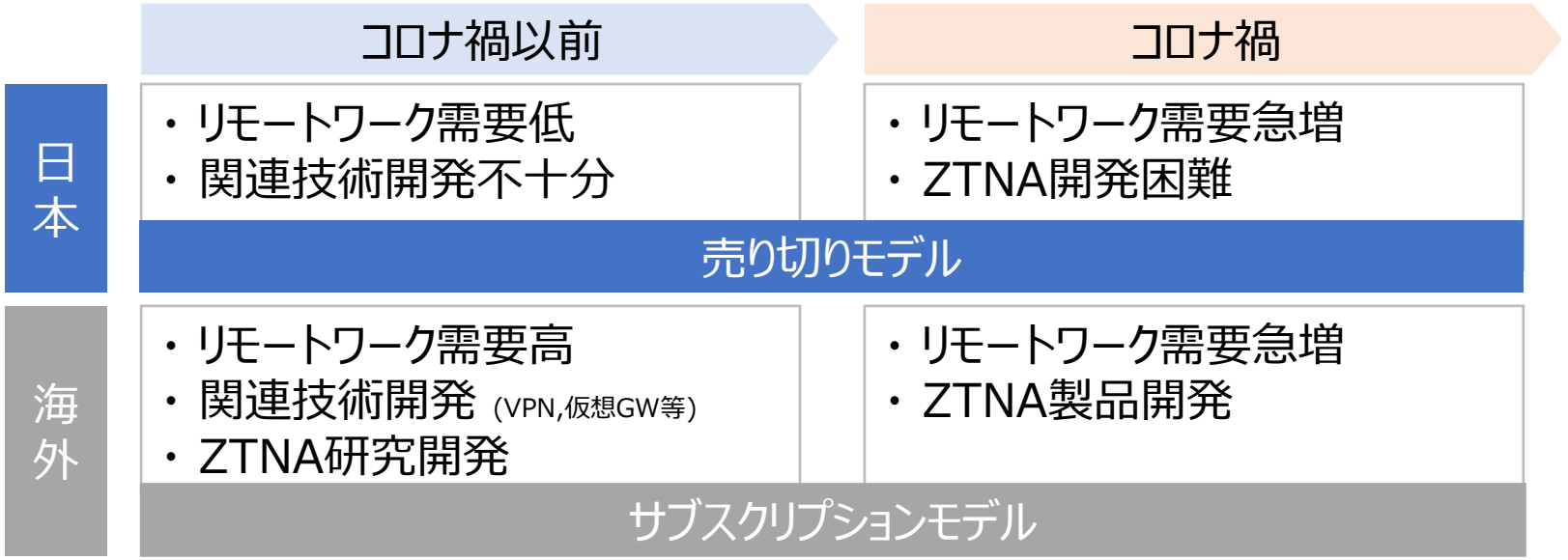
（補足）ZTNAのコア技術のプレイヤーが日本にいない原因の仮説

- 4.7節に示した通り、ZTNA関連技術に関しては、日本に本社を置くメインプレイヤーが存在していないという現状がある。その原因の仮説を以下に示す。

技術トレンドの感度に起因する問題

コロナ禍以前において、海外とは異なり国内ではリモートワーク需要が少なく、純国産のVPNや仮想GW、リモートアクセスソリューション開発、市場育成につながらなかった可能性がある。感染症対策や災害対策の需要から海外のソリューションベンダ（例：Citrix, Pulse Secure, PaloAltoなど）は既存のVPN、仮想GW、リモートアクセスソリューション技術をもとにZTNAソリューションの開発を急速に進める事ができ、国内のソリューションベンダはもはや追いつけない状態であると思われる。

さらに、ZTNAでは運用で継続的にセキュリティレベルを維持することが前提となるが、日本ではサービスの売り切りモデルを好む傾向がありサブスクリプションモデルの浸透の遅れがZTNAの国内需要が急速に増加しない要因の一つではではないかと考える。



（補足）PKIに関する追加調査結果 - 懸念点

- インターネット上で安全に通信を行う上でPKI（公開鍵暗号基盤）は根底技術であり、またZTAの主要コンポーネントとしても定義されている重要技術であるため、個別に取り上げて懸念点を洗い出した。
- PKIの利用において懸念点があるかサイバートラスト社の意見も含め当社で下記調査を行った結果を下記に示す。PKIに関する懸念は小さいということが明らかになった。

#	懸念点	結果	
1	自国のルート認証局は利用できるか	日本では2社選択可能。	懸念小
2	自国のルート認証局が海外に買収される可能性はあるか	日本では認証局の買収、経営統合に関する特別な保護や制限はない。	懸念有
3	サービスやシステムで自国の証明書が利用できるか	標準で利用可能なサービスを選択する、または手動で登録が可能なサービスを選択することが求められるが、利用可能である。	懸念小
4	クライアント証明書を大量に発行する仕組みはあるか	認証局にもよるが、API経由で大量発行する仕組みがある。IoT専用サービスもある。	懸念小
5	IoTデバイスにクライアント証明書を導入する仕組みがあるか	デバイス側の問題であるため、ユーザにインターネット経由で登録・更新できる製品を選定することが求められる。	懸念小
6	安全な鍵管理方法があるか	デバイス側の問題であるため、ユーザにIPA「IoT開発におけるセキュリティ設計の手引き」(*1)に準拠した製品を選定することが求められる。	懸念小

*1 今後のIoTの普及に備え、IoT機器およびその使用環境で想定されるセキュリティ脅威と対策をまとめた文章。
（最終更新2019年4月16日、独立行政法人情報処理推進機構 技術本部　セキュリティセンター [https://www.ipa.go.jp/security/iot/iotguide.html]）

（補足）PKIに関する追加調査結果 - 日本のルート認証局

- 地政学的リスクがPKIに存在するかを確認するため、日本のルート認証局を調査した結果を下記に示す

会社名	概要
セコムトラストシステムズ株式会社 主要株主: セコム（株） 100% C=JP, O=SECOM Trust Systems CO.,LTD., OU=Security Communication EV RootCA1 C=JP, O=SECOM Trust Systems CO.,LTD., OU=Security Communication RootCA1 C=JP, O=SECOM Trust Systems CO.,LTD., OU=Security Communication RootCA2	2004年にWebTrust認定を取得し、日本のパブリックルート認証機関としてマイクロソフト社や主要なブラウザーメーカーの製品内に認証局証明書が格納されている。
サイバートラスト株式会社 主要株主: SBテクノロジー（株） 64.83% C=JP, O=Japan Cetification Services, Inc. CN=SecureSign Root CA12 C=JP, O=Cybertrust Japan Co., Ltd.. CN=SecureSign Root CA12 C=JP, O=Cybertrust Japan Co., Ltd.. CN=SecureSign Root CA14 C=JP, O=Cybertrust Japan Co., Ltd.. CN=SecureSign Root CA15 C=JP, O=Cybertrust Japan Co., Ltd.. CN=Cybertrust iTrust Root Certification Authority	1997年に国内初の商用電子認証センターを開局。2006年WebTrust監査に合格。日本のパブリックルート認証機関として主要なOSやブラウザにルート認証局証明書を組み込む活動を実施中。

5. 総括

5.1 施策展望課題・対策の検討

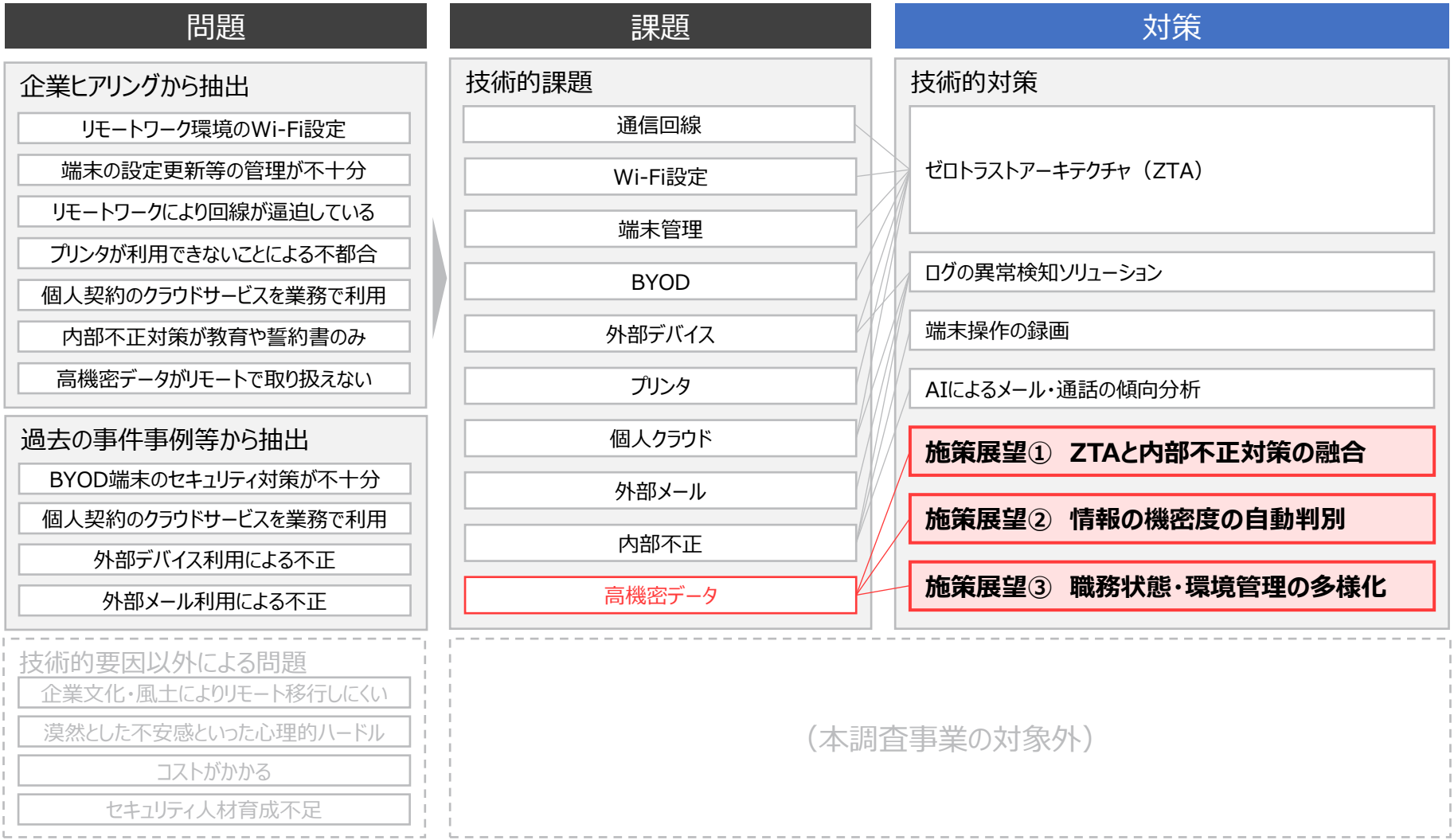
- 2章から4章で示した3つの調査研究の結果から、我が国としての課題を整理し、施策展望の検討を行った。

- 企業へのヒアリングなどからリモートワークやパブリッククラウドの活用阻害要因となり得る技術的課題を10個洗い出した。
- リモートワークの活用推進で期待されているZTAに注目し、ZTAの海外事例とネットワーク事業者事例を調査した。これによりZTAをはじめとする対策技術により課題10個中9個はリスク低減が可能だった。残る1個の課題、高機密データを取り扱う業務のリモートワーク推進にはさらなる対策が必要と考える。
- また、ZTAを構成する要素を日本企業が提供している事例が乏しく、海外ベンダーへ依存していることが懸念される。

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
秘匿性の高い情報を取り扱う業務のリモートワークを推進するには、
現在市場にあるセキュリティ対策では不十分と考える。

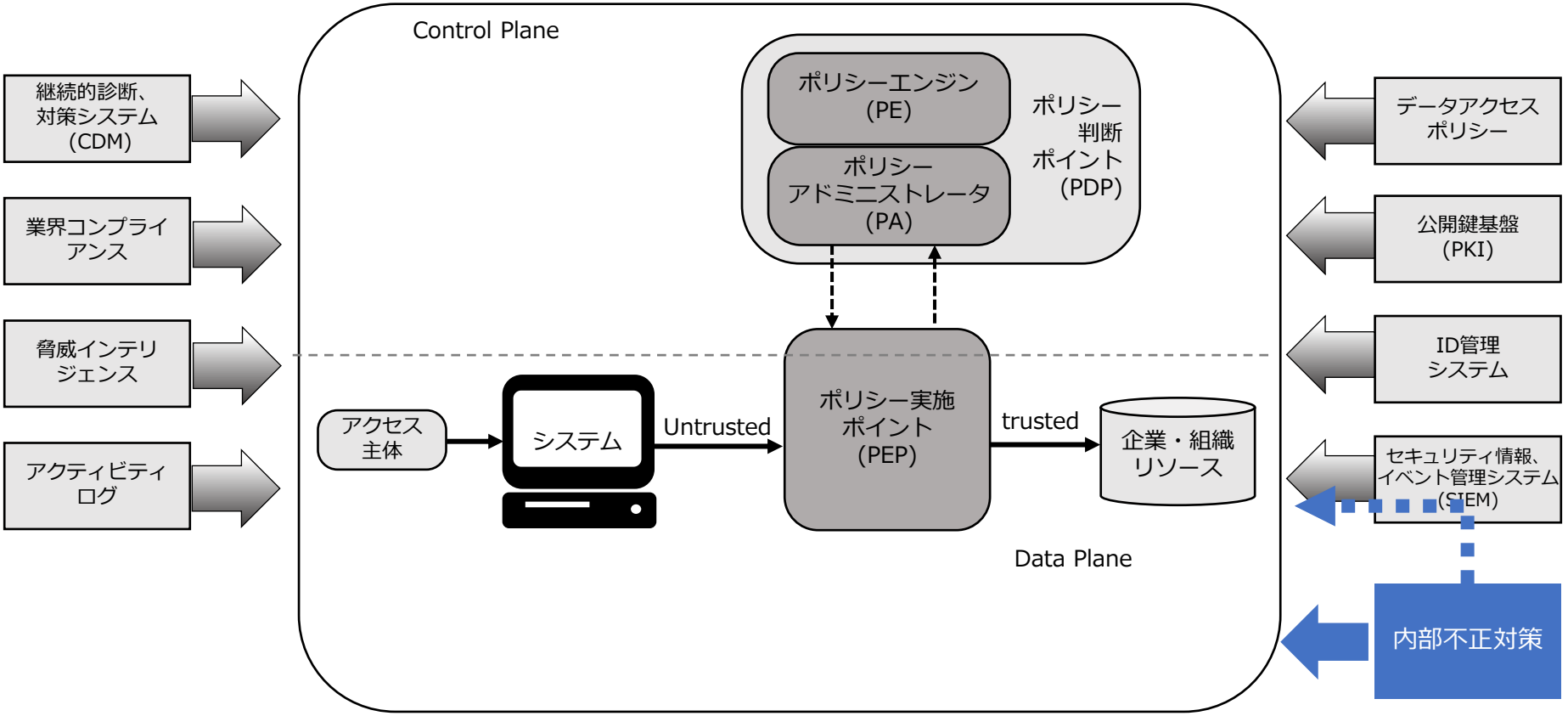
5.2 今後必要となる技術開発要素

- 秘匿性の高い情報を取り扱う業務のリモートワークへのセキュリティ対策として、施策展望①～③の技術開発が今後必要となると考えられる。



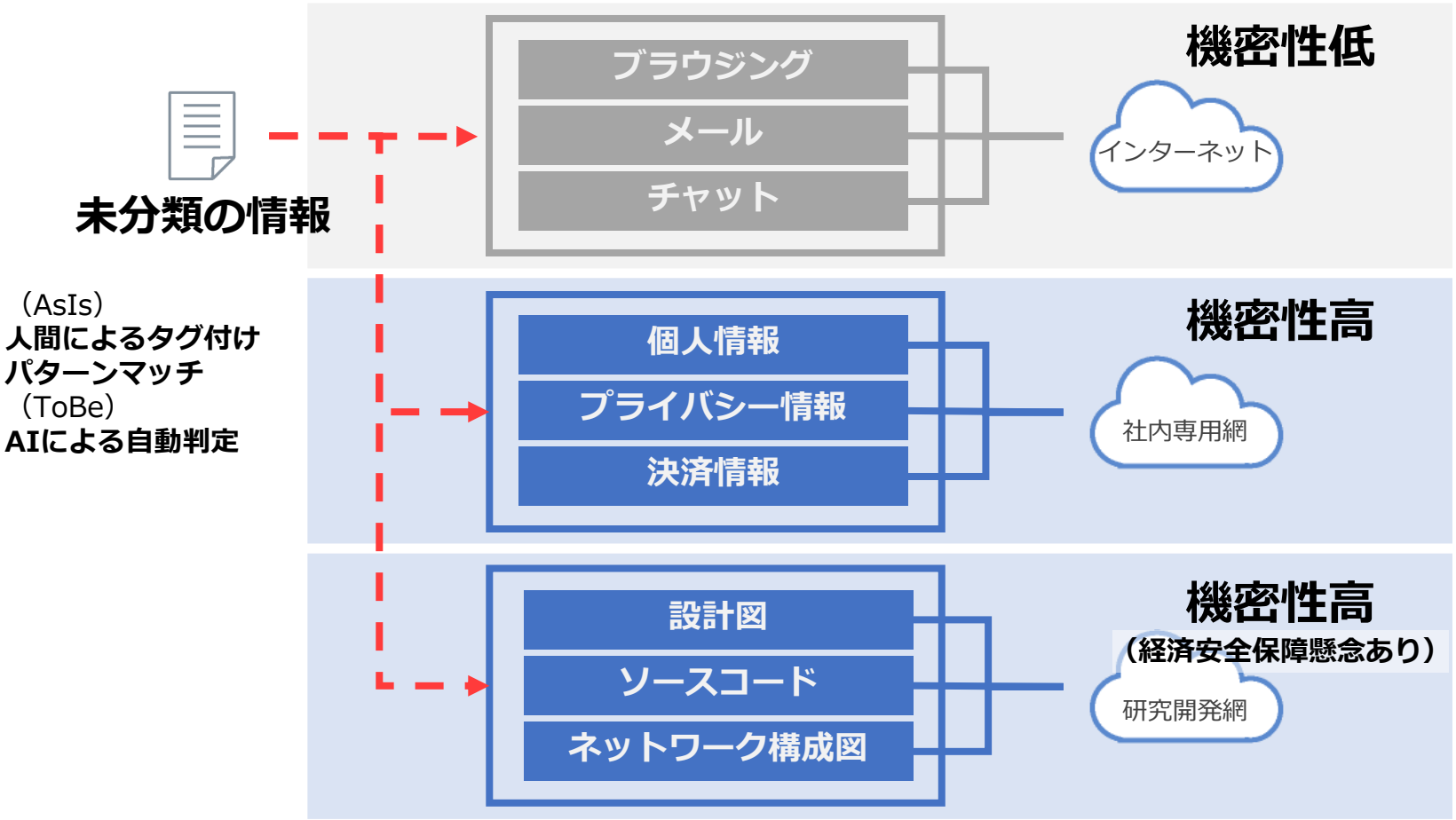
5.2.1 施策展望① ZTAと内部不正対策の融合

- 内部不正対策をZTAと組み合わせることで高機密データをリモートワークで取り扱うハードルを下げることが期待できる。
- 内部不正対策の情報をZTAの検証の一要素として扱う。SIEM経由ではSIEM交換が難しくなるため標準サポートを期待する。



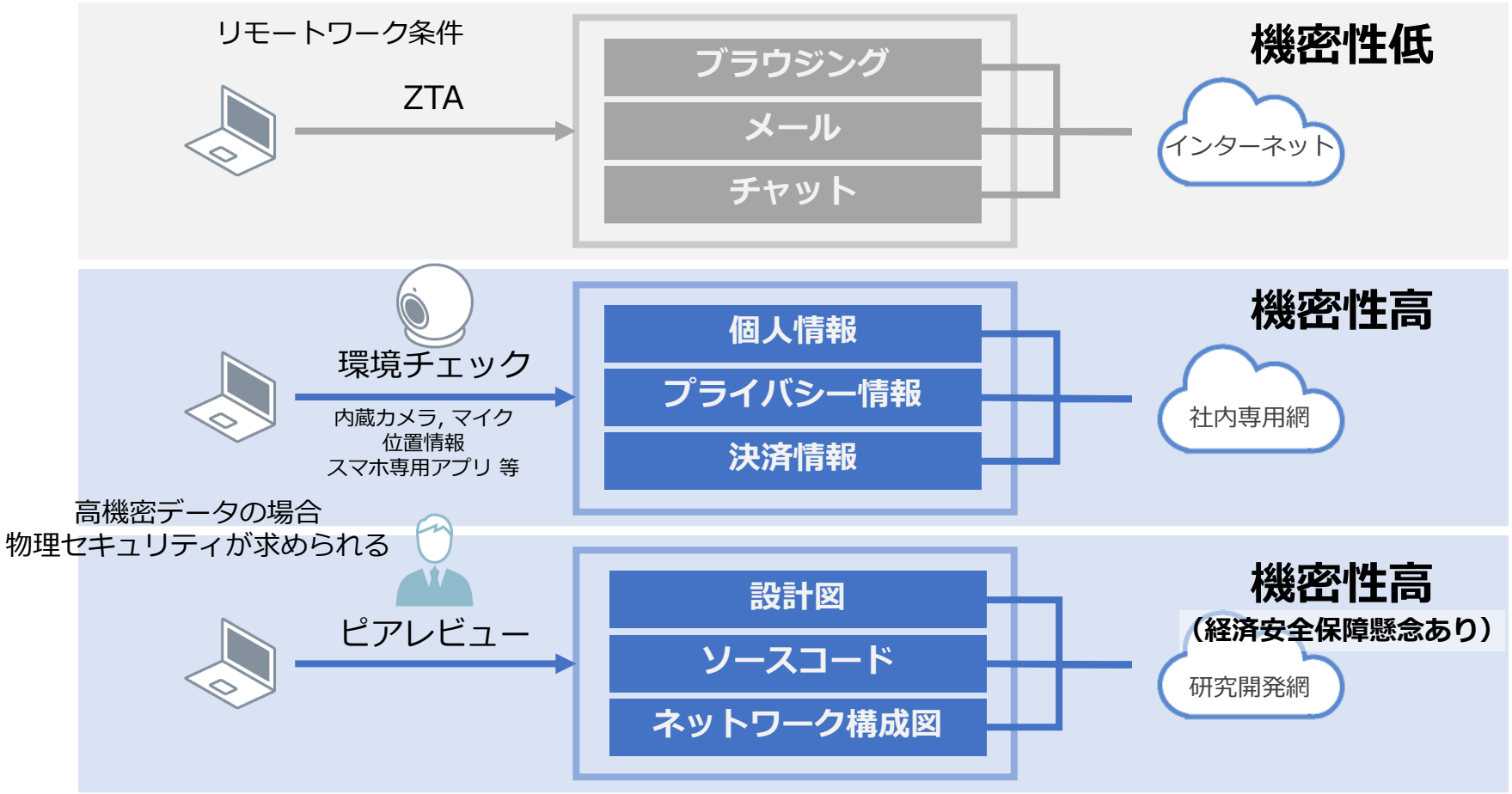
5.2.2 施策展望② 情報の機密度の自動判別

- AIによる自動判断機能で高機密情報を判断することにより、人間が故意に機密度低の情報としてタグ付けを行い、情報を持ち出す状況を阻止することが期待できる。現在は、市場にある製品の事例も人間によるタグ付けが前提、または、パターンマッチによって判別される程度である。



5.2.3 施策展望③ 職務状態・環境管理の多様化

- リモートワークに限らず、従来のオフィス環境でも同じセキュリティレベルを維持することができ、場所にとらわれることがない新たな働き方を選択することができる。オフィスに限らず自治体業務や大学キャンパス等にも応用の可能性がある。



5.2.3 施策展望③ 職務状態・環境管理の多様化（補足1 環境チェック）

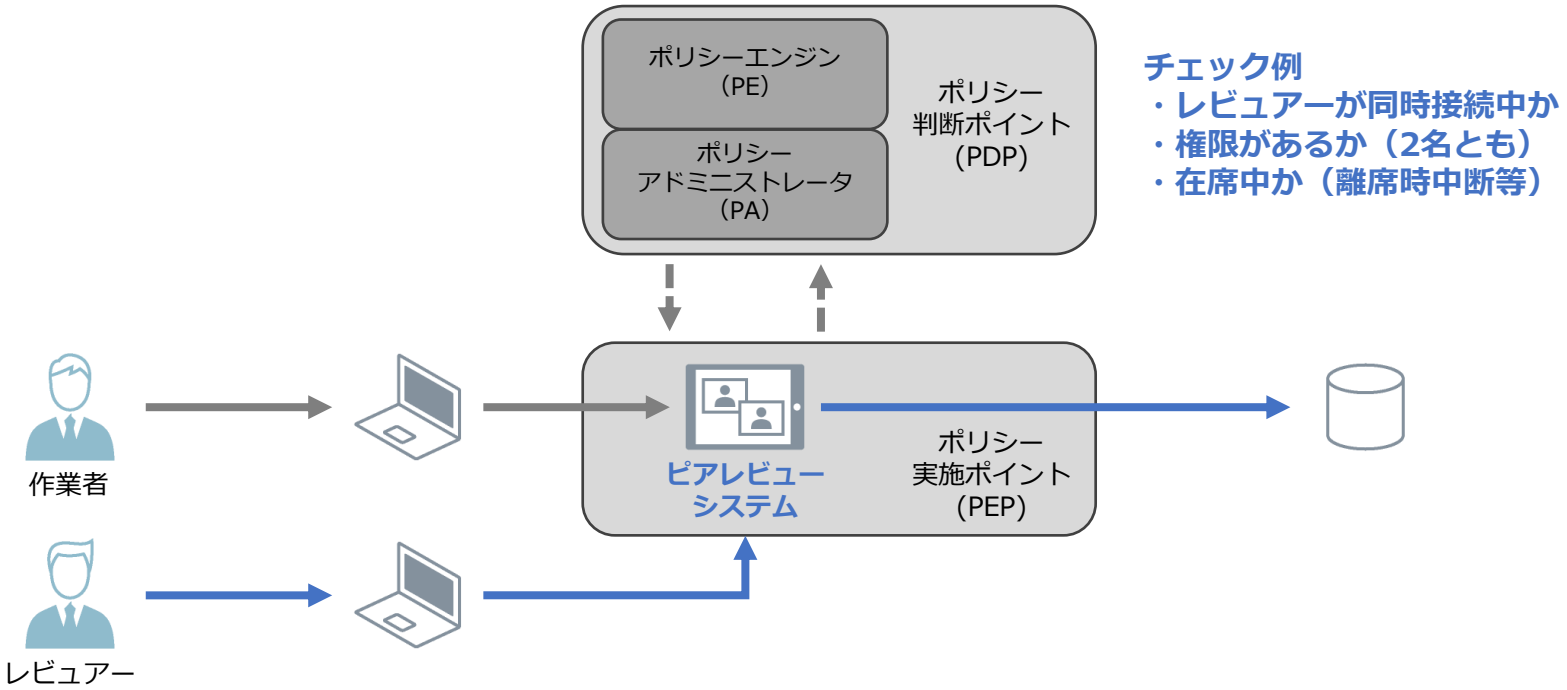
- 施策展望③の環境チェックについて補足する。
- 環境チェックとは、機密情報へのアクセスをコントロールのために、従業員の労務環境を確認する仕組みである。
- 従業員のプライバシー保護のため、端末から送信される情報は検知結果（True/False）のみ（端末内で判定処理）が望ましい。

環境チェック

5.2.3 施策展望③ 職務状態･環境管理の多様化（補足2 ピアレビュー）

- 施策展望③のピアレビューについて補足する。
- ピアレビューとは、作業者が経済安全保障を脅かす懸念のある機密度が非常に高い情報を取り扱う際に、作業者以外にレビュアーの監視を求める仕組みである。
- 立場や職種が同じ者同士で行うことで、警備員やAIで検出することが難しい不正や作業ミス等を発見することが期待できる。

ピアレビュー

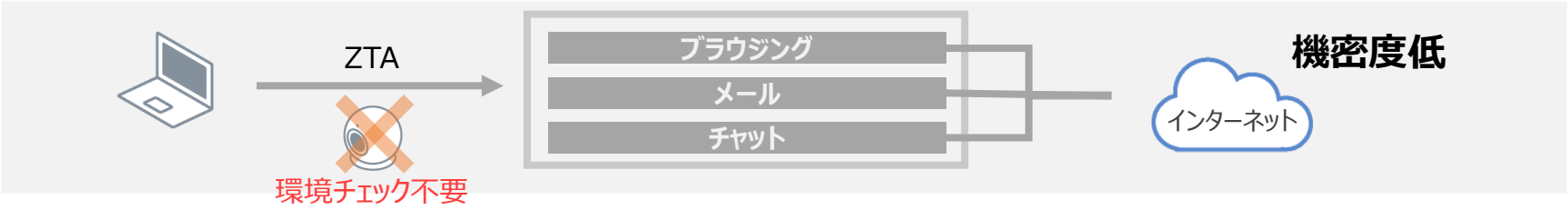


5.3 留意点

- 各々の施策を行う際には、以下の事項に留意する必要がある。

留意点① 監視の程度

- 機密度の低い情報を取り扱う業務に過度な監視は不要である。
- 過度な監視は働きにくさによる生産性低下やシャドウITにつながる可能性がある。
- 職務状態・環境管理はコストもかかるため、安易に監視する必要はない。



留意点② 従業員のプライバシー保護

- リモートワークを活用するため、カメラやマイク、位置情報などを用いて職務状態・環境管理する場合は、従業員のプライバシーへ配慮が必要である。
- リモートワークの条件（職務状態・環境管理）に同意できない従業員にはこれまで通りオフィスでの勤務を認めるオプトアウトも必要である。
- これまでリモートワークを認めてきた業務に監視を追加する場合は労働条件の不利益変更にも当たる可能性があるため、特に慎重に検討すべきである。
- 高機密データにアクセスしないときは無効にするなど配慮が必要である。

5.4 施策展望のまとめ

- 本事業では、安全・安心で利便性の高いデジタル社会基盤の構築を目的に、そこで求められるセキュリティ技術（認証・認可技術等）に関する調査を行い、今後必要となる技術開発の具体化として3つの施策展望を示した。

（課題）
- 秘匿性の高い情報を取り扱う業務についてはリモートワークが禁止されている。
- 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のある高機密データを取り扱う業務に関してはさらなるセキュリティ対策が必要である。
- 高機密データを取り扱う業務のリモートワークを推進するには、現在市場にあるセキュリティ対策では不十分と考える。

（施策展望）

1．ZTAと内部不正対策の融合
2．情報の機密度の自動判別
3．職務状態・環境管理の多様化

（効果）

新たなセキュリティ対策を開発することでリモートワークに限らず、従来のオフィス環境でも同じセキュリティレベルを維持することができ、場所にとらわれない新たな働き方を選択できる。

5.5 今後実施することが望ましい調査事項

- 本事業の調査結果を踏まえ、安全・安心で利便性の高いデジタル社会基盤の構築に向けて、2021年度以降の施策展望として、以下の詳細調査の実施を提案する。

1.「緊急対応による課題」・「恒久的な課題」の整理

今回はコロナ禍の緊急対応として課題ヒアリングを実施したが、コロナ後にも求められる恒久的な課題を明確に分けることができるようにヒアリング、整理することが求められる。例えば、回線逼迫は緊急対応時のみ発生し、恒久的な対応時には計画猶予があるため発生しない。

2. 重要インフラ分野の網羅

今回の調査では6業種以上（秘匿情報が有り）9社の企業からご協力を得たが、経済安全保障の観点から重要インフラ14分野（情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、科学、クレジット、石油）を網羅した調査が求められる。

3. ZTAの11コンポーネントでのメインプレイヤー調査

今回はZTAの展開モデルの4つを参考にしたが、より詳細なZTAの11コンポーネントを参考にした調査が求められる。

4. 内部不正対策とメインプレイヤー調査

今回は内部不正対策の市場を詳しく調査することができなかったが、内部不正対策をカテゴリに分類した調査が求められる。

5. 技術要素の調査範囲の拡大

今回はサイバーセキュリティやリモートワークに範囲を絞っていたが、暗号化や認証認可等の基礎技術基盤、OSやブラウザ、仮想化基盤等にも範囲を拡大して調査することが求められる。

6. ②有識者検討会の開催

6.1 有識者検討会の開催

- セキュリティ及び5G等の次世代ネットワークに関する学識者や実務経験者等の専門家4名で構成される検討会を下記の通り開催した。

会議名称		情報サービス産業の管理体制強化に向けたセキュリティ技術検討委員会
会議目的・役割		安全・安心で利便性の高いデジタル社会基盤の構築に求められるセキュリティ技術（認証・認可技術等）に関する調査、ならびに今後必要となる技術開発の具体化に関し、専門的見地からの指導・助言を行う。
議題	第1回 2021年1月19日	1. 本調査事業の概要について 2. 各調査研究の実施方法について
	第2回 2021年2月15日	1. 調査報告書について
開催方法		オンライン
委員 (五十音順)	鵜飼　裕司 岡部　寿男 林　　達也 平山　敏弘	株式会社 FFRI セキュリティ 代表取締役社長 京都大学学術情報メディアセンター　センター長 株式会社パロンゴ CTO 情報経営イノベーション専門職大学 教授

6.2 有識者検討会 議事要旨（第1回）

- 第1回の要点は下記の通り。
- 議事要旨全文は、別紙2「有識者検討会議 議事要旨（第1回）」参照。

■各調査研究の実施方法について

(a) 阻害要因の事例調査

① 技術的要因以外（企業文化、心理的ハードル等）によりリモートワークが阻害される場合がある。
② チェックシートが全て充足されなければリモートワークを実施するべきではないという論調は避けるべき。

(b) 改善案と求められる機能の提案

③ 海外事例は先進的ではあるが、コスト・時間の面で導入負荷が高いといった欠点もあるため、調査報告書として導入を推奨していると読み取れないように留意すべき。
④ ゼロトラストの定義を明確にするべき。

(c) 技術開発に関する論点の整理

⑤ 証明書の管理は重要な技術である。
⑥ バイタル認証はプライバシー上の問題がある。
⑦ 国内のソフトウェアに関するサプライチェーンとしてのチョークポイントを整理することが重要。

■会議総括

⑧ リモートワークの阻害要因は、経営的観点で考えると「事故が起きないか」「勤勉に励むことができるか」という2つの要因に集約される。
⑨ 今までとこれからの違いになれる必要がある。（オフィスワーク中心からリモートワーク中心へ）
⑩ 内部不正のみならず、勤怠管理の古い考え方がリモートワークの推進を阻害している。

6.3 有識者検討会 議事要旨（第2回）（1/2）

- 第2回の要点は下記の通り。
- 議事要旨全文は、別紙3「有識者検討会議 議事要旨（第2回）」参照。

■調査報告書について

(a) 阻害要因の事例調査

① 脅威には、内部脅威と外部脅威の2つがあり、内部脅威の方が対策が困難である。
② コロナ禍における喫緊の表層的対応と、本質的対応を分けて考えるべき。
③ 本報告書がリモートワーク導入しない理由にされないように、メリット等も示し前向きにまとめるべき。

(b) 改善案と求められる機能の提案

④ ゼロトラストへ段階的な移行を推進するようなメッセージを込められるとよい。
⑤ 内部不正に関して、対策のロードマップや方針を報告書内で示せるとよい。
⑥ 海外事例に関して、それぞれの企業が持つ技術的な強みで整理すると事例として反映しやすくなる。
⑦ リモートワーク阻害要因とその対策をレイヤ等に基づいて分類・マッピングするべき。

(c) 技術開発に関する論点の整理

⑧ 米国企業が主流の状況下で我が国として経済安全保障を実現するデジタル社会を構築するうえでPKIは重要である。
⑨ システムを構成するコンポーネントの評価には課題が残る。
⑩ 地政学的リスクについて、具体的に過去の経緯を交えながら、注釈や説明を加えられるとよい。
⑪ 昨今、オープンソースを用いた開発も主流のため、どこまでオープンな技術であるかということも重要。

6.3 有識者検討会 議事要旨（第2回）（2/2）

- 第2回の要点は下記の通り。
- 議事要旨全文は、別紙3「有識者検討会議 議事要旨（第2回）」参照。

■調査報告書について

総括

⑫ ZTAと内部不正対策の融合は今後重要になってくる。
⑬ ポリシーエンジンに内部不正対策も織り込まれているべき。
⑭ 過度な監視をしないという制約の下、具体的な方法を示すことで実行容易性が増す。
⑮ 機密度を考える上で、トラストという概念の理解が必要であるので、説明を追加するべき。
⑯ 高機密データを取り扱う業務についても、対策を行うことでリモートワークを実施できると読めるように、前向きな表現に修正すべき。
⑰ 多様化は重要である。状況に応じた実施可能な作業を決める必要がある。
⑱ 監視については従業員のプライバシーを侵害しないようにすべき。
⑲ オフィス勤務でもリモートワークでも、同じように働けるように仕事そのものの切り分けが肝要。

■会議総括

⑳ 2回に渡る委員会の中で活発に議論ができ、調査報告書が世の中のためになることを期待する。
㉑ 全体的に前向きな表現となるようにするべき。
㉒ リモートワークやゼロトラストアーキテクチャの導入のハードルを上げすぎないように、納得できるステップを示すことが現実的であり、重要である。

EOF