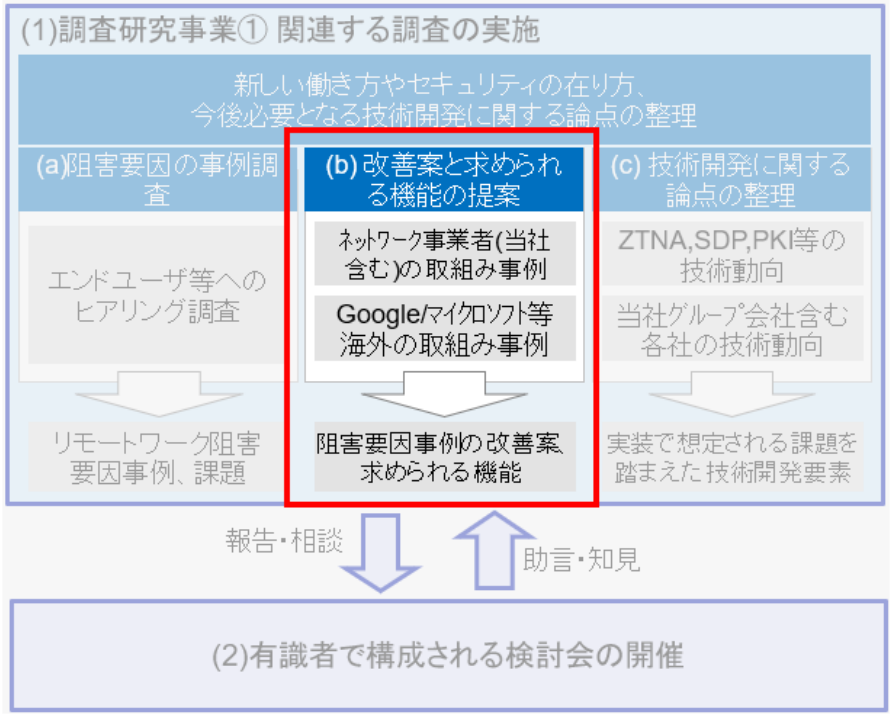
資料５－２

「(b) 改善案と求められる機能の提案」の調査方法

SoftBank

1）概要

　リモートワークに関わる技術についての海外事例やネットワーク事業者事例を調査した上で、技術や解決策を洗い出し（＝事例調査）、その技術や解決策と(a)チームのアウトプットである「リモートワーク課題」や「近年のセキュリティ事件事例の調査内容」 とを突き合わせ効果を検証し（＝効果検証）、改善案と求められる機能（今後必要となる技術開発も含め）についてまとめる。



２）実施方法

前述「事例調査」と「効果検証」についての概要は以下の通りである。

A）事例調査　・・・　リモートワークに関わる技術と解決策の調査

A1)　海外事例　　：Google BeyondCorp
A2)　海外事例　　：Microsoft ゼロトラスト成熟度モデル
A3)　通信事業者事例　：Softbank CIS Controls，常時VPN、内部不正対策

B）効果検証　・・・　課題を技術で解決できるのかどうかの検証

次頁以降、具体的な内容を記述する。

2-A）事例調査

A1：海外事例（Google BeyondCorp）

【調査概要】

- Google社が製品化したゼロトラストアプローチに基づくクラウドソリューション「BeyondCorp Remote Access」について調査する。

- Google社とのパートナーシップ関係からヒアリングを実施し、技術情報と具体的にその技術で何を解決することが出来るのか／出来ないのかを、Google社内での重要／極秘情報の取り扱い業務等の具体的業務ユースケース情報も入手しながら整理する。

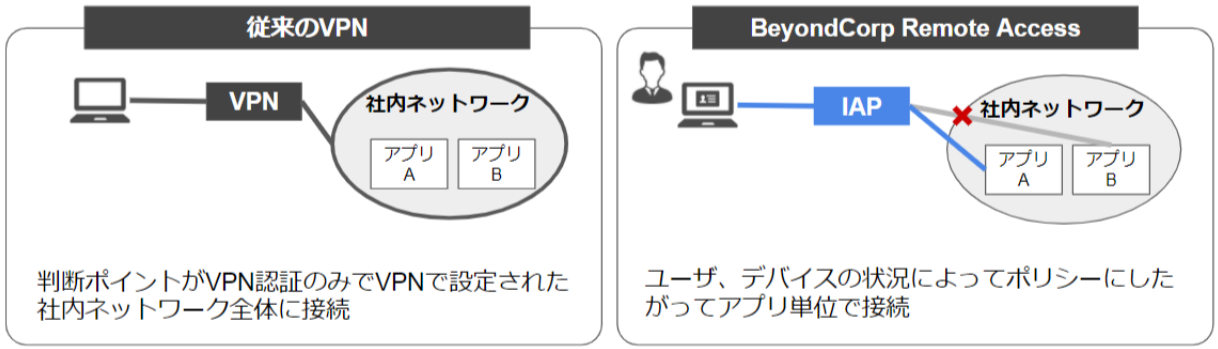
2-A）事例調査

A1：海外事例（Google BeyondCorp）

【技術の概要／特徴】

- BeyondCorpの特徴は「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である」という点である。

- 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。
  - ・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



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

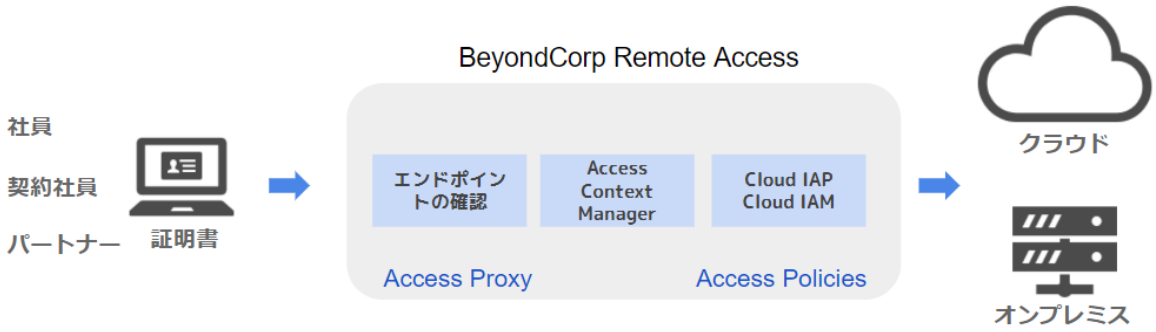
2-A）事例調査

A1：海外事例（Google BeyondCorp）

【技術の概要／特徴】

- BeyondCorpでは、従来ネットワーク境界にあったアクセス制御をユーザーやデバイス、そしてサービスに移し、デバイスの状態（OS、セキュリティ対策ソフト導入など）およびそれに関連するユーザー情報（アクセスポイント）と、それについてサービス側が知っている情報をもとにアクセスが制御される。

- サービスへのアクセス権限はサービスが付与する。また、この権限付与はサービス毎に動的に制御され、かつ信頼レベルに応じた段階的な認証・認可が行われる。



2-A）事例調査

A1：海外事例（Google BeyondCorp）

【調査まとめ事項】

項目	説明
事例の要旨 技術の概要／特徴	業務課題やセキュリティ課題に対し、どのような技術的対策が必要でどのように解決するのかをまとめる
具体的ユースケースと解決	実業務の具体例を挙げ、その解決前と解決後（Before/After）をまとめる
導入効果／コスト／期間	導入の効果と、導入にかかるコストや期間をまとめる

※ 後述、海外事例調査（Microsoft ゼロトラスト成熟度）と社内事例調査（Softbank）も調査まとめ事項は同様のため記述は割愛する

2-A）事例調査

A2：海外事例（Microsoft ゼロトラスト成熟度モデル）

【調査概要】

- E2Eセキュリティとしてゼロトラスト基盤技術に先進的に取り組んでいるMicrosoft社の「Microsoft ゼロトラスト成熟度モデル」について調査する。

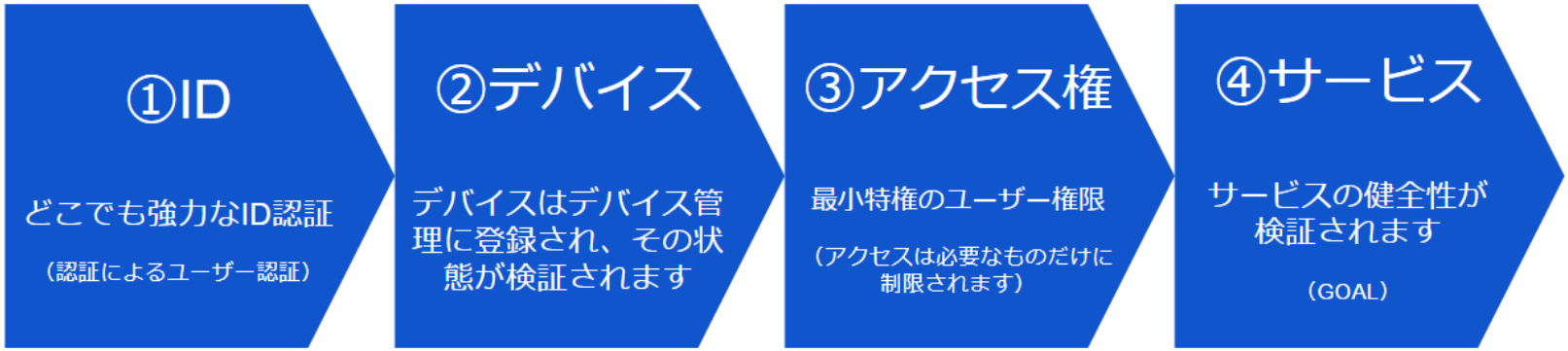
- Google調査同様に、Microsoft社とのパートナーシップ関係からヒアリングを実施し、技術情報と具体的にその技術で何を解決することが出来るのか／出来ないのかを、Microsoft内での重要／極秘情報の取り扱い業務等の具体的業務ユースケース情報も入手しながら整理する。

2-A）事例調査

A2：海外事例（Microsoft ゼロトラスト成熟度モデル）

【技術の概要／特徴】

- 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。



2-A）事例調査

A2：海外事例（Microsoft ゼロトラスト成熟度モデル）

【技術の概要／特徴】

- Microsoftサービスを使用したゼロトラストアーキテクチャは以下の通り

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

2-A）事例調査

A3：通信事業者事例（Softbank CIS Controls、常時VPN、内部不正対策）

【調査概要】

- 本調査の担当者自体が、弊社内の下記項目①～③について取り組んでおり、セキュリティ担当・情報システム部門とで過去対策・現状課題・今後の対策計画などをまとめているため、それら取り組み情報を本調査プロジェクトで活用する。

① CIS Controls
② 常時VPNの使用やリモートワークセキュリティ
③ 内部不正への対策

2-A）事例調査

A3：通信事業者事例（Softbank CIS Controls、常時VPN、内部不正対策）

【① CIS Controlsの概要】

- 会社支給の端末内にセキュリティ関連のソリューションを複数導入しているが、様々な経緯から端末の種類によって異なるソリューションが導入されていたり、対策として期待する機能に不足や重複が発生している現状がある。

  このため、一般的なセキュリティフレームワークである「CIS Contorols」を用いて、どういった機能を満たすことを期待して導入したソリューションなのかを可視化することで、現状の対策力バー範囲、不足範囲の明確化や、導入検討するソリューションの効果測定に役立てている。

※CIS（Center For Internet Security）
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

※CSI Controls
CISが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。現在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。

2-A）事例調査

A3：通信事業者事例（Softbank CIS Controls、常時VPN、内部不正対策）

CIS Controls活用の事例

端末種別毎の対策状況の可視化

		PC種別			
		種別A	種別B	種別C	
CIS Contorols	ｾｷｭﾘﾃｨ対策項目1	ｿﾘｭｰｼｮﾝA	ｿﾘｭｰｼｮﾝA	ｿﾘｭｰｼｮﾝA	
	ｾｷｭﾘﾃｨ対策項目2	ｿﾘｭｰｼｮﾝA	ｿﾘｭｰｼｮﾝA	ｿﾘｭｰｼｮﾝA	
	ｾｷｭﾘﾃｨ対策項目3	ｿﾘｭｰｼｮﾝA	ｿﾘｭｰｼｮﾝB	ｿﾘｭｰｼｮﾝB	種別毎に違うｿﾘｭｰｼｮﾝを導入している
	ｾｷｭﾘﾃｨ対策項目4	ｿﾘｭｰｼｮﾝC	ｿﾘｭｰｼｮﾝC	無し	種別によって対策ができていない
	ｾｷｭﾘﾃｨ対策項目5	ｿﾘｭｰｼｮﾝC ｿﾘｭｰｼｮﾝD	ｿﾘｭｰｼｮﾝC	ｿﾘｭｰｼｮﾝC	同じ機能でｿﾘｭｰｼｮﾝが重複している
	ｾｷｭﾘﾃｨ対策項目6	無し	無し	無し	対策が取れていない
	:				

ソリューション毎の効果測定

		ｿﾘｭｰｼｮﾝA	ｿﾘｭｰｼｮﾝB	ｿﾘｭｰｼｮﾝC	
CIS Contorols	ｾｷｭﾘﾃｨ対策項目1	✔	✔	✔	
	ｾｷｭﾘﾃｨ対策項目2	✔	✔		
	ｾｷｭﾘﾃｨ対策項目3	✔		✔	
	ｾｷｭﾘﾃｨ対策項目4	✔		✔	
	ｾｷｭﾘﾃｨ対策項目5		✔	✔	
	ｾｷｭﾘﾃｨ対策項目6				
	:				

2-A）事例調査

A3：通信事業者事例（Softbank CIS Controls、常時VPN、内部不正対策）

【②常時VPNの概要／仕様】

- 現状、リモートワークにおいて社内システムへアクセスする際はVPN経由でアクセスする必要があるが、VPNを張るのは各自が操作する形式になっているため、SaaSなど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をすることも可能な状態にある。

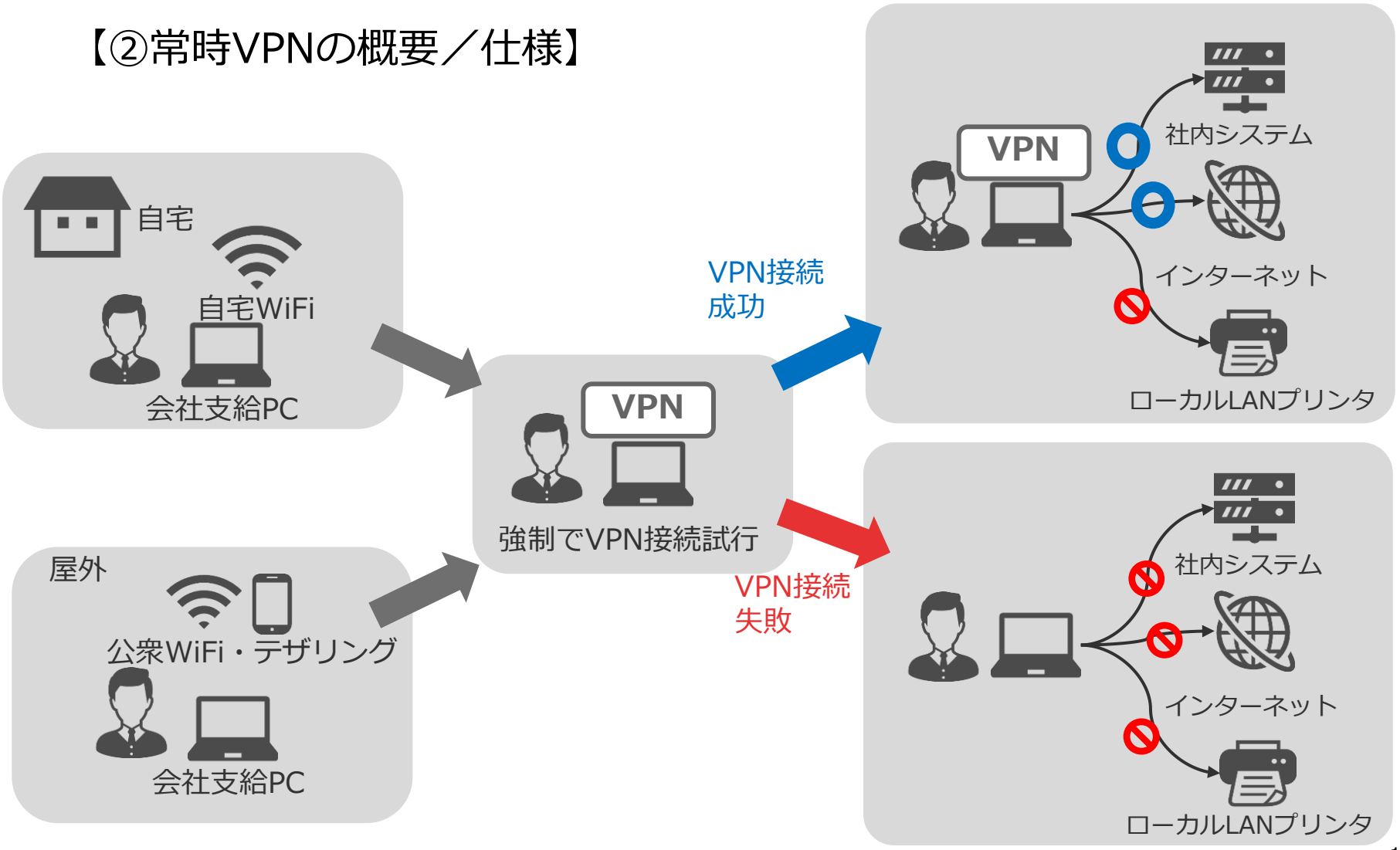
  このため、危険なサイトや禁止しているサイトへのアクセスを企業側が制御できない状態にある。

- これを解決するため、社外環境において会社貸与PCからインターネットへアクセスする際には、強制的にVPNが張られるような仕組みを導入し、常時VPN経由で社内外のサイトへアクセスする仕様とし、企業側によるアクセス制御を可能とする。

2-A）事例調査

A3：通信事業者事例（Softbank CIS Controls、常時VPN、内部不正対策）

【②常時VPNの概要／仕様】



2-A）事例調査

A3：通信事業者事例（Softbank CIS Controls、常時VPN、内部不正対策）

【③内部不正への対策】

- 今まで、社内のセキュリティ監視対策は外部脅威からのサイバー攻撃の検知が主体であったが、昨今の内部不正事案の増加を受けて以下の対策をしている。

  - セキュリティ監視チームの中に内部不正専用の監視チームを構築
  - 内部不正を検知するために以下の（１）～（３）のソリューションの導入を推進（詳細は次頁以降）

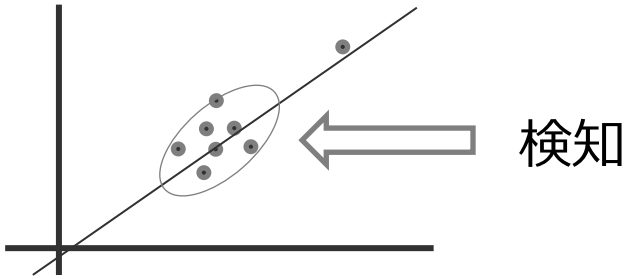
    （１）ログの異常値分析
    （２）端末操作の録画
    （３）メール、通話の傾向分析

2-A）事例調査

A3：通信事業者事例（Softbank CIS Controls、常時VPN、内部不正対策）

（１）ログの異常値分析

- 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。



（２）端末操作の録画

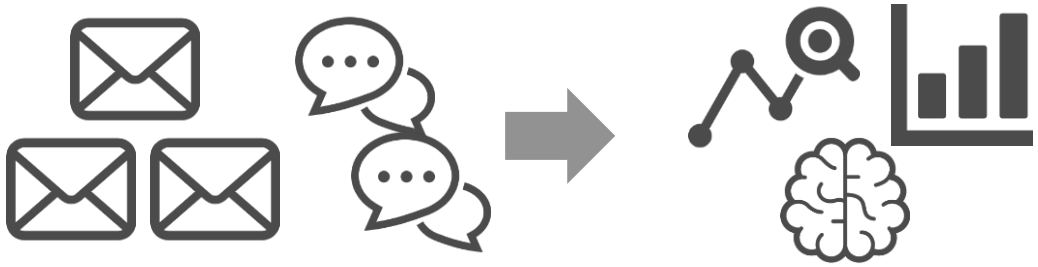
- 端末の操作がすべて記録できるよう画面の録画を実施し、実施したコマンド、サイト上の操作、送信ファイルの特定などができるようにする

2-A）事例調査

A3：通信事業者事例（Softbank CIS Controls、常時VPN、内部不正対策）

（３）メール、通話の傾向分析

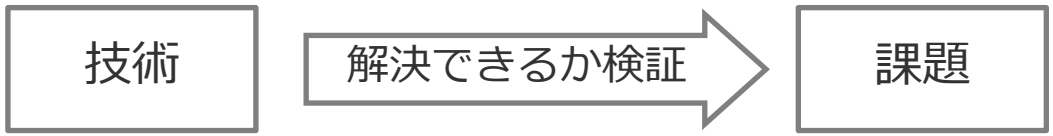
- メール、チャットの文章など内外と交わされる言語情報から不審な動きを検知することにより、不正の予兆検知や外部共犯者の検知などにつなげる



2-B）効果検証

【概要】

- Ａ)事例調査で得られた情報を「技術」、「(a) 阻害要因の事例調査」で得られた情報を「課題」とし、 「課題」を「技術」で解決することができるのかを検証する。



・Google BeyondCorp
・Microsoft セロトラスト成熟度モデル
・Softbank リモートワーク対策など

・ (a) 阻害要因の事例調査からの課題
・近年のセキュリティ事件事例

- 課題が、調査した技術では解決できない課題であった場合、「新たに開発しなければならない技術」を検討する。その検証結果をふまえ、最終的に「あるべき姿」とそこに「求められる機能」として最終報告をまとめていく想定である。

【検証結果まとめ】

- (b)としての最終まとめとイコールになるため、後述「3.想定されるアウトプット」に記載

3）想定されるアウトプット

「事例調査」や「効果検証」の結果として、下記内容をまとめる。

項目	説明
課題と対策	各課題に対し、解決策となる技術をマッピングした「課題と対策分類の一覧表」を作成した上で、どの技術がどの課題への対策となるのかを具体的にまとめる ①課題と対策分類の一覧表 ②具体的な内容 ・ZTNAで解決できる課題 ・SDPで解決できる課題 ： ・上記以外の、新しい機能が必要な課題
求められる新しい機能	課題の中で、既存技術では解決できない課題については、新しい機能開発／技術開発を検討しまとめる ・ネットワーク制御／認証・認可機能など

また、表中の「 ①課題と対策分類の一覧表」のイメージは下記である。

技術カテゴリー	課題A	課題B	課題C	・・・
認証・認可：ZTNA / SDP	該当(ZTNP)	該当(SDP)		
デバイス管理：MAM / MDM		該当（MAM）	該当（MAM）	
リモート接続、仮想端末：VPN / VDI / DaaS / シンクライアント			該当（VPN）	
その他	該当(XX技術)			