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2月15日

ソフトバンク株式会社

本事業の背景・目的

本調査研究では、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のに必要となる安全・安心で利便性の高いデジタル社会基盤の構築を目的として、セキュリティ技術を調査し、今後必要となる技術開発を具体化する。背景を踏まえ目的にと繋げるための事業実施の基本方針は次のように考える。

背景

経済安全保障への対応

- 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

コロナ禍の影響

- リモートワーク需要の急増
- 経済活動・社会活動のクラウドへのシフトが加速

リモートワーク阻害要因

- 従来型の境界型防御の問題
- 機密性の高いく漏洩した場合、産業上または安全保障上のリスクとなる情報の社外持ち出し禁止

目的

生産性低下を招かない
安全なリモートワークの実現

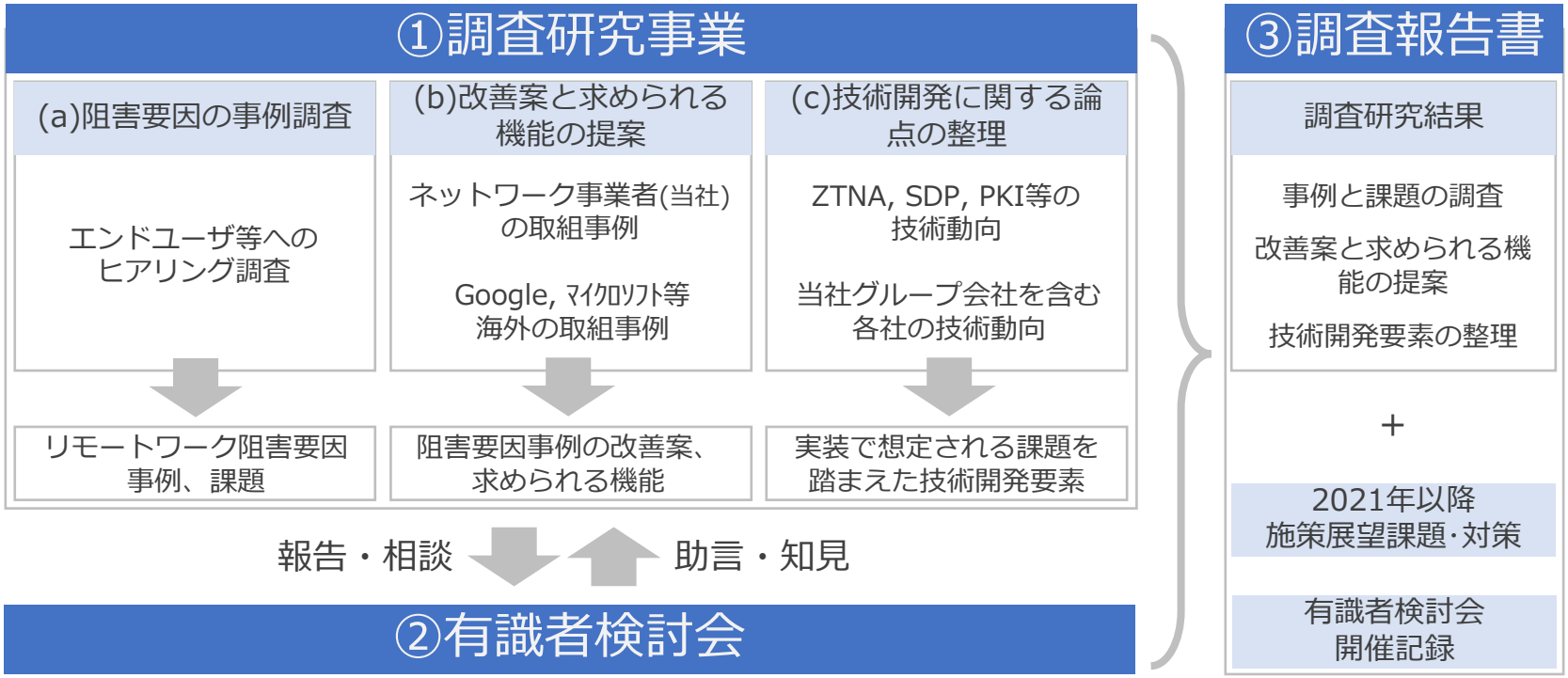
安全・安心で利便性の高い
デジタル社会基盤の構築

事業実施の基本方針

- 当社における関連事業やリモートワークやVPNサービスなどの提供で培った知見を活かし、具体的な課題抽出を行い技術開発要素をまとめる
- 当社の持つ人的ネットワーク等を活用して、ヒアリングや有識者検討会に対し入念な準備を行うとともに、広範な技術調査を行う

実施内容

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・技術動向調査を調査する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「調査結果報告書の作成」の3パートにより構成している。



事例と課題の調査

事例と課題の調査

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ヒアリングを実施した。

ヒアリング対象

会社名	業種	資本金	従業員数	分散拠点
ソフトバンク(株)	情報・通信	204,309	17,300	有
SHIFT(株)	情報・通信	67	3,829	有
イオンアイビス(株) 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	小売 / 情報	490	360	有
パロアルトネットワークス(株) 本資料では米国本社の情報を代替記載1ドル110円換算	セキュリティ	248,512	8,014	有
シャープ(株)	製造	5,000	51,402	有
(株)バローホールディングス	小売	13,609	8,168	有
（会社名非公開A社）	-	-	-	有
（会社名非公開B社）	-	-	-	有
（会社名非公開C社）	-	-	-	有

定量調査

#	チェックシート集計表	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。	33%
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。	33%
3	OSに最新のセキュリティパッチを適用できている。	33%
4	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	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	ローカルにログを取得できている。	67%
7	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。	67%
8	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	不要なアカウントを無効化できている。	56%
10	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	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	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	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	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	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	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%

定量調査
チェックシート補足

CIS Controlsを元にチェックシートを作成したが、**文章の通りに対策を推奨するものではない。**元は企業ネットワークを想定したチェックシートのためリモートワークへの読み替えが必要となる。ヒアリングの中で代替案などを聞きながらセキュリティ専門家による目線合わせを実施した。

#	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。	

定量調査結果

#	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。

定性調査結果

#	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。
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。
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。
8	**個人クラウド**	業務利用と個人契約のクラウドサービスアカウントの識別が難しい。
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。
10	**高機密データ**	個人情報やシステム管理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。

リモートワーク・クラウド利用に関する事件事例調査

#	カテゴリ	発生年月	企業名	概要	事象経緯
1	リモートワーク	2020年5月	NTT Communications	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洩した。	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。
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。
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。
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。
5	クラウド	2020年1月	福岡県	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。

産業スパイに関連する事件事例調査（1/2）

#	発生年月	企業名	概要	事象経緯	事実認定状況
1	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。	判決確定 （有罪）
2	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洩した。	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。	判決確定 （有罪）
3	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。	本人は持ち出しを認める （不正利用目的は否定） （2018年1月逮捕）
4	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。	本人は持ち出しを認める （持ち出したのが秘密情報であることを否定） （2019年6月逮捕）
5	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。	不明 （2019年2月起訴）

産業スパイに関連する事件事例調査 (2/2)

#	1生年月	企業名	概要	事象経緯	事実認定状況
6	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。	本人は持ち出しを認める （動機は不明） （2019年3月書類送検）
7	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。	本人は不正利用目的での持ち出しを認める （2019年3月逮捕）
8	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。	判決確定 （有罪）
9	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。	本人は持ち出しを認める （不正利用目的は否定） （2020年10月書類送検）
10	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。	本人は持ち出しを認める （不正利用目的は否定） （2020年9月逮捕）

事件事例調査結果

リモートワーク・クラウド利用に関する事件事例より

#	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	**個人クラウド**	業務利用と個人契約のクラウドサービスアカウントの識別が難しい。

産業スパイに関する事件事例より

#	項目	内容
1	**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。
2	**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。

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。

しかし、これらは技術による直接的な解決が難しいため、今回の課題として取り上げることを見送った。

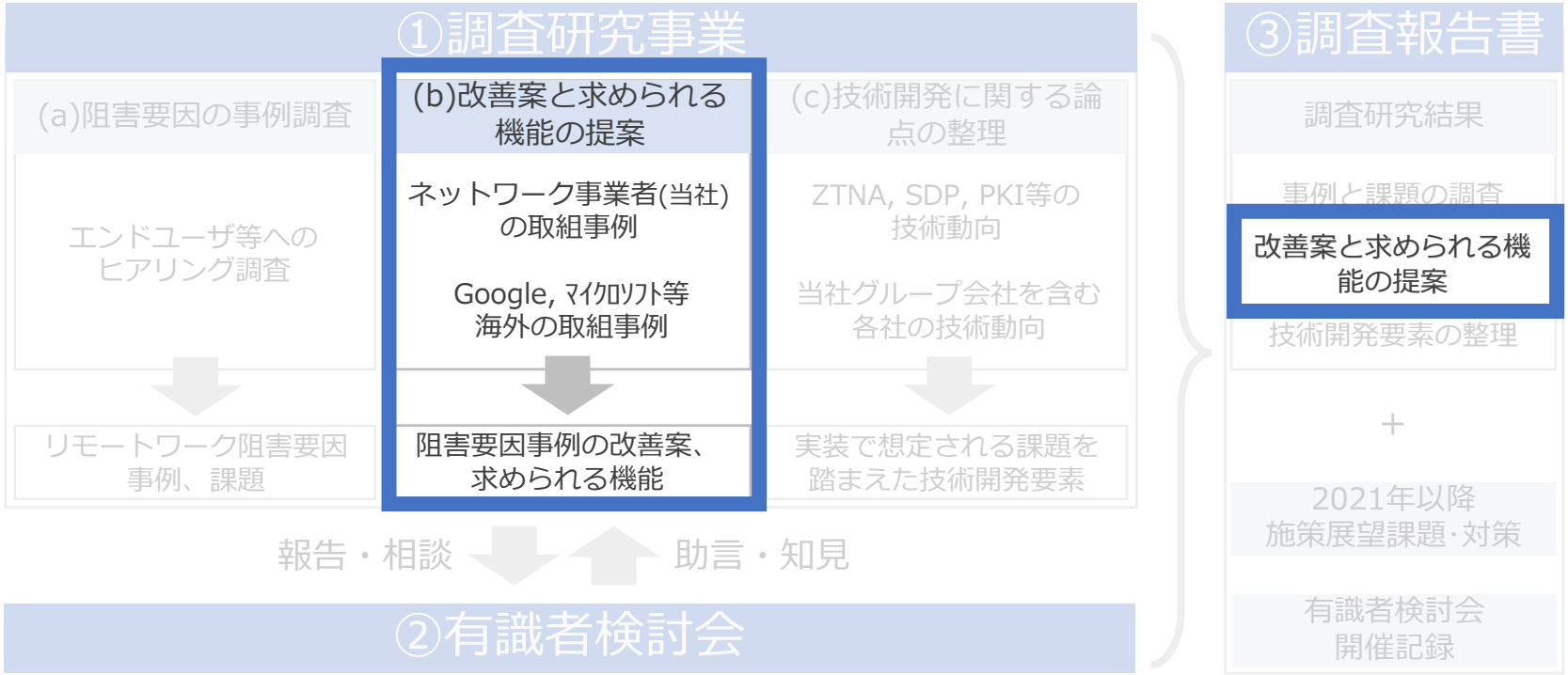
リモートワーク阻害要因まとめ

#	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	**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。
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。
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。
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。
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。
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。
8	**個人クラウド**	業務利用と個人契約のクラウドサービスアカウントの識別が難しい。
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。
10	**高機密データ**	個人情報やシステム管理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。

改善案と求められる機能の提案

改善案と求められる機能の提案

ネットワーク事業者の取り組みや海外事例からToBeとなる技術的な事項を情報収集した。収集したToBeとなる技術的な事項により、リモートワーク阻害事例の課題を解決できるか検証した。



海外事例調査

リモートワークの活用推進に期待されているZTAの先進的な取り組み事例としてGoogle社とマイクロソフト社の事例を調査した。

- **海外事例：Google BeyondCorp**
- **海外事例：マイクロソフト ゼロトラストセキュリティ**

ゼロトラストとは

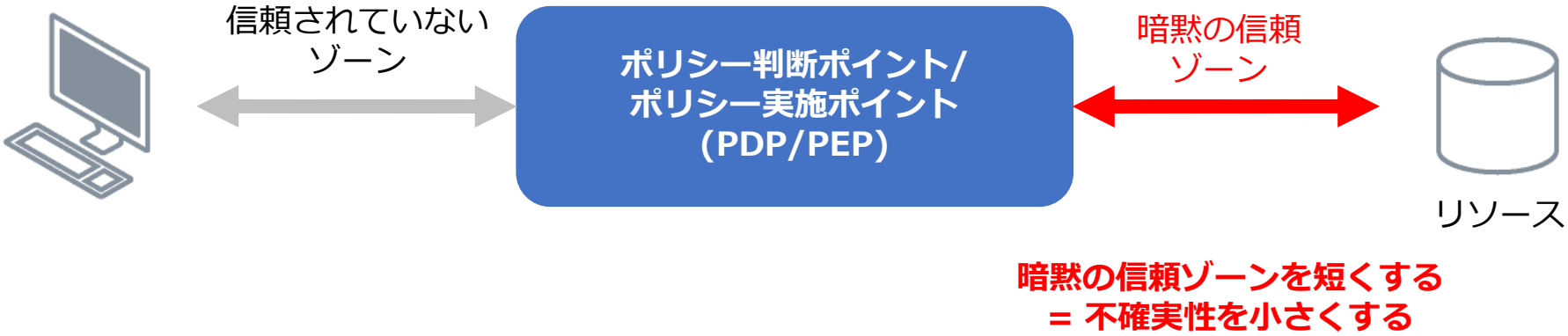
信頼は決して暗黙のうちに与えられるものではなく、継続的に評価する前提に基づいたサイバーセキュリティモデルである。

今回の調査ではゼロトラストはZTAを指している。ZTNAの場合はZTNAであることを明記して使い分ける。

- **ZT (Zero Trust)** は、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 Architechture)** は、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)** は、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。

NIST SP 800-207
Zero Trust Architecture

今回の調査ではNIST SP 800-207 Zero Trust Architectureから概念や展開モデルを参照した。



その他参考情報

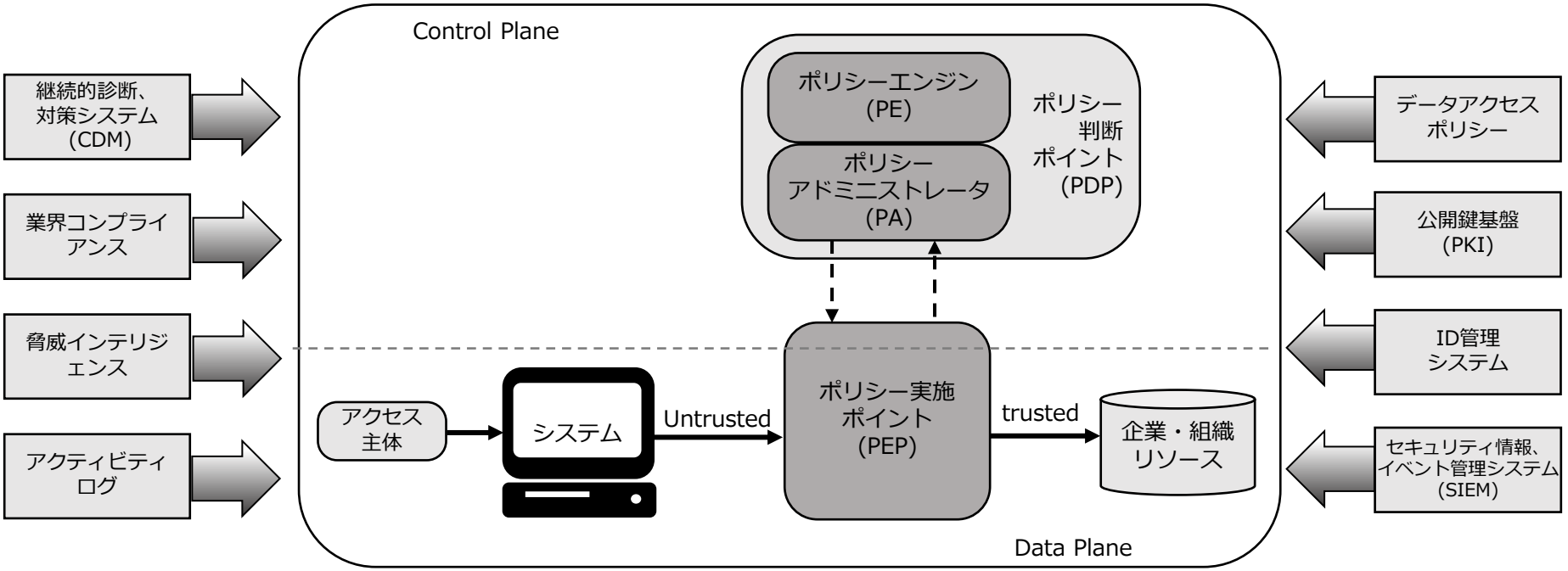
- 政府CIOポータル: 政府情報システムにおけるゼロトラスト適用に向けた考え方
  https://cio.go.jp/sites/default/files/uploads/documents/dp2020_03.pdf
- Cloud Security Alliance: SDPによる真のゼロトラスト実装
  https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2020/07/Software-Defined-Perimeter-and-Zero-Trust_J.pdf

ZTAの7原則

1. 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. **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. 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. 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. 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. 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. 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

ZTAの構成要素

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）



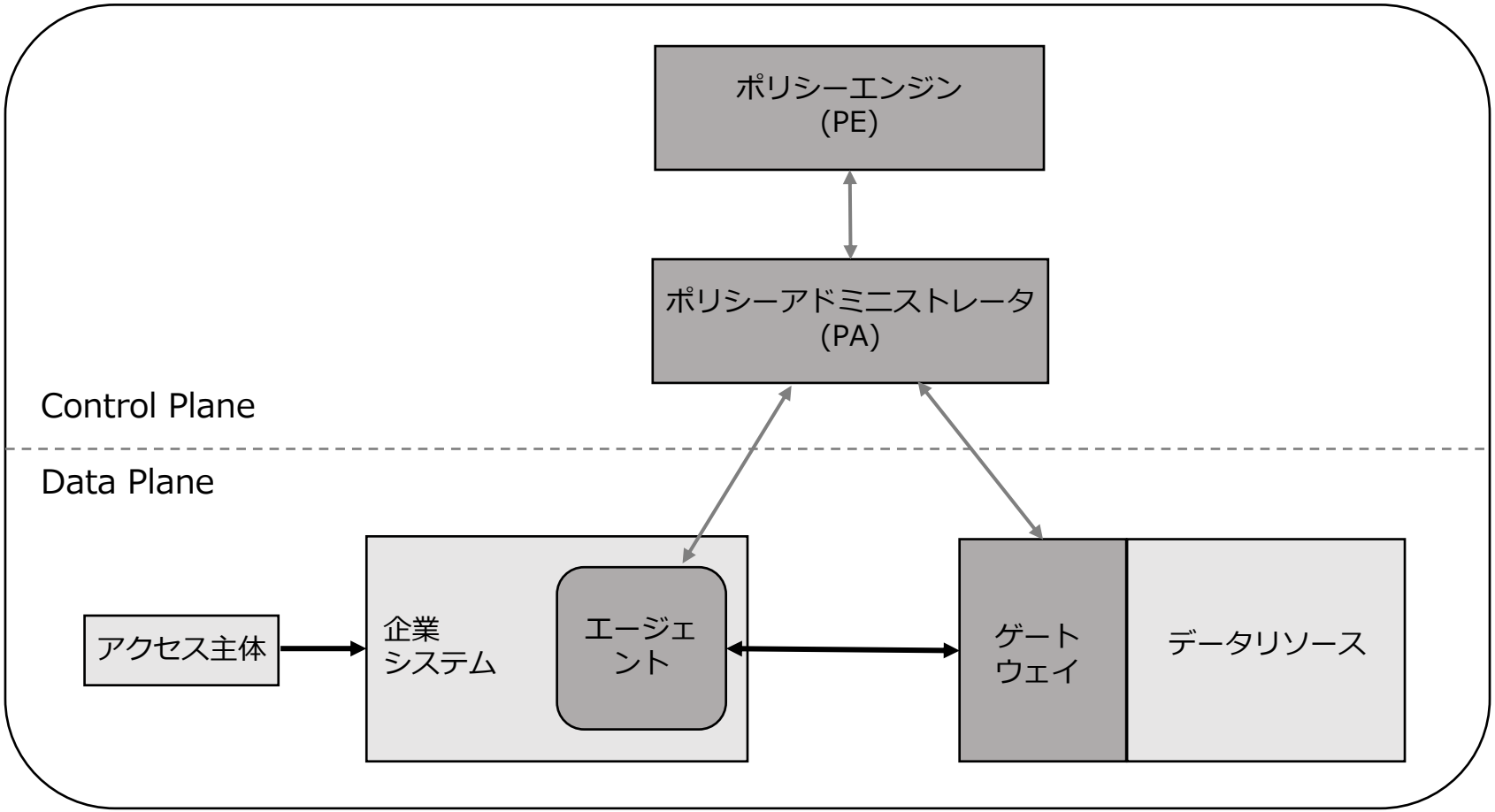
ZTAの展開モデル

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**
- **エンクレイブゲートウェイモデル**
- **リソースポータルモデル**
- **アプリケーションのサンドボックス**

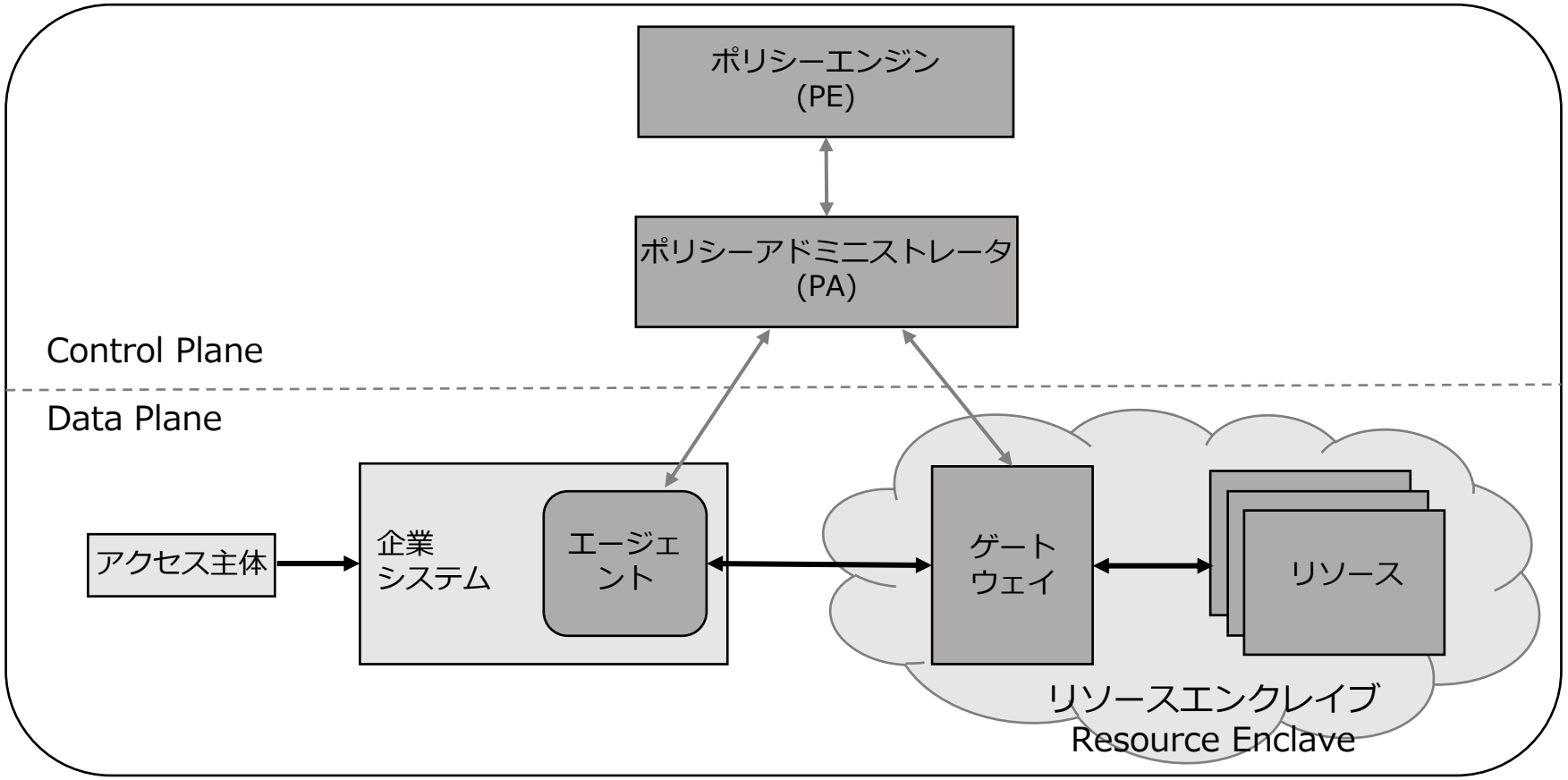
デバイスエージェント/ゲートウェイモデル

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**へ用いられる。



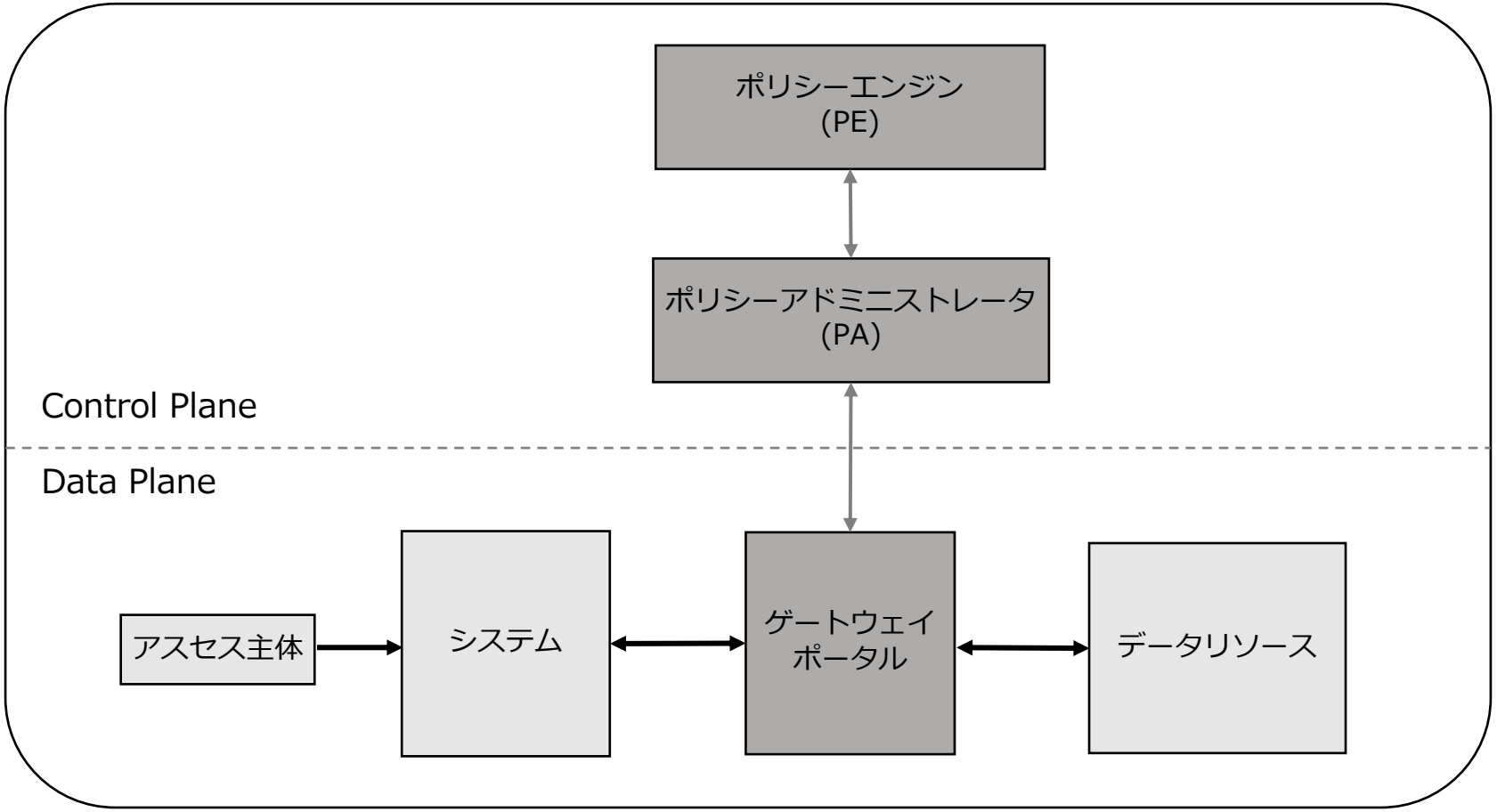
エンクレイブゲートウェイモデル

この展開モデルは、前述のデバイスエージェント/ゲートウェイ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。



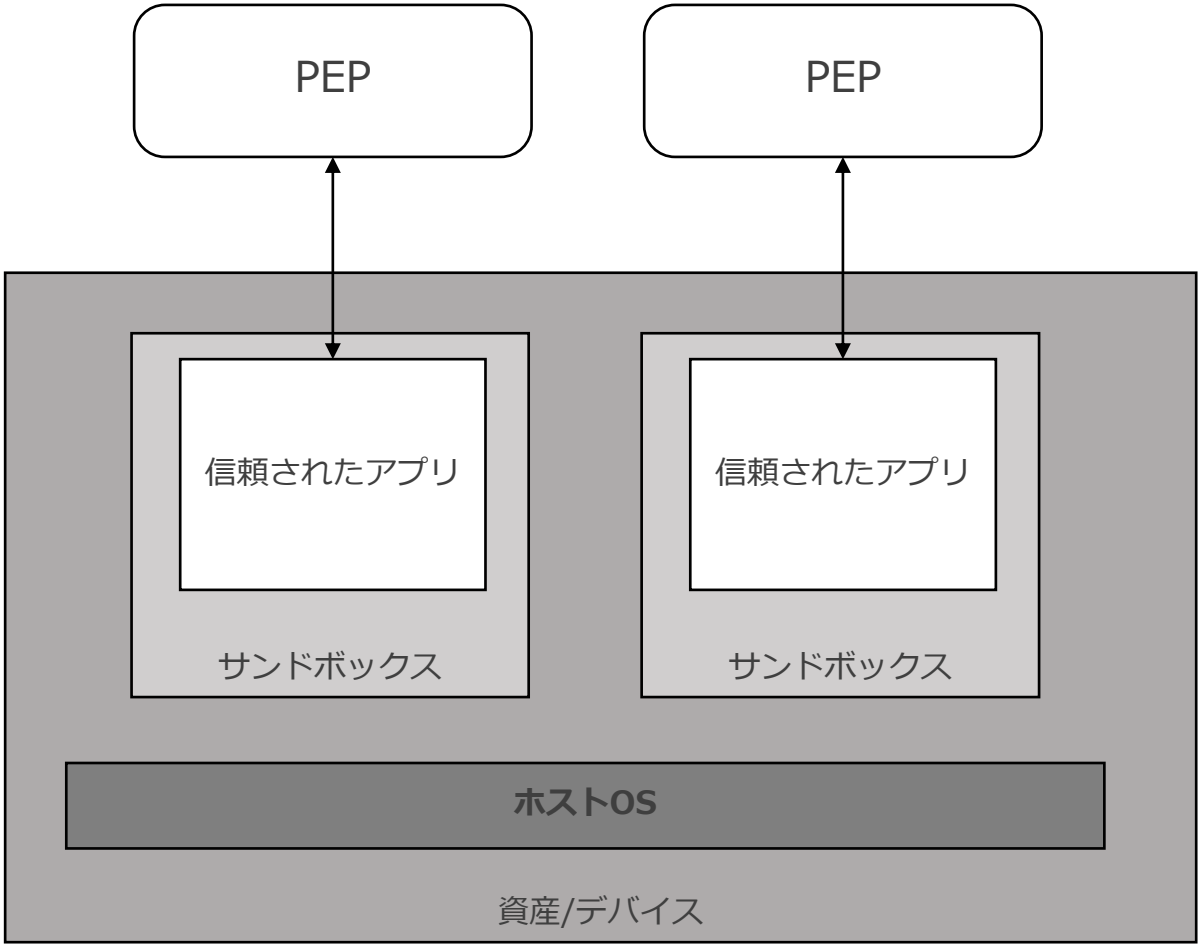
リソースポータルモデル

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で用いられる。



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。



海外事例
Google BeyondCorp

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。

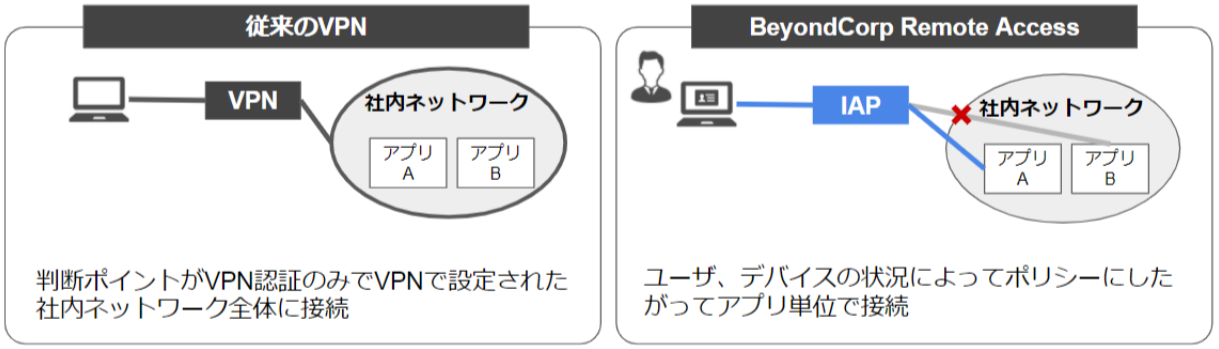
製品情報は2021年1月時点のものである。

Google BeyondCorp
概要と特徴（1/2）

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

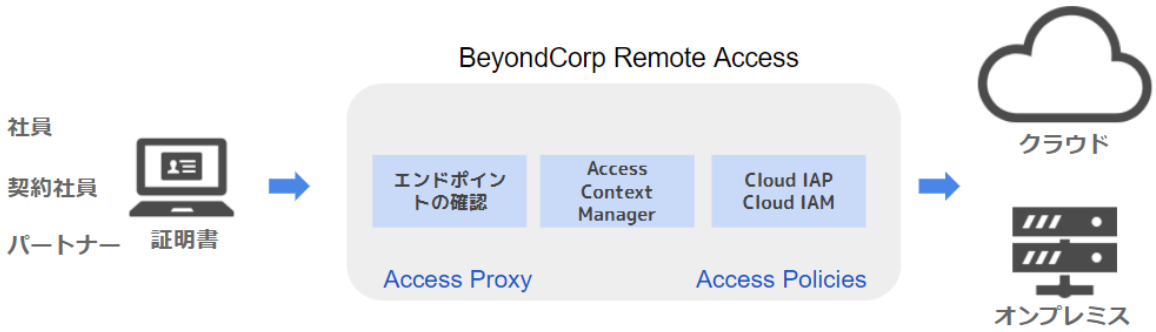


IAP＝Identity-Aware Proxy
従業員が VPN を使用せずに信頼できないネットワークから会社のアプリやリソースにアクセスできるようにするための仕組み

Google BeyondCorp
概要と特徴（2/2）

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。



Google BeyondCorp
事例検証結果

#	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制度があるとお聞きした。 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

海外事例
マイクロソフトゼロトラストセキュリティ

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「マイクロソフト 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。

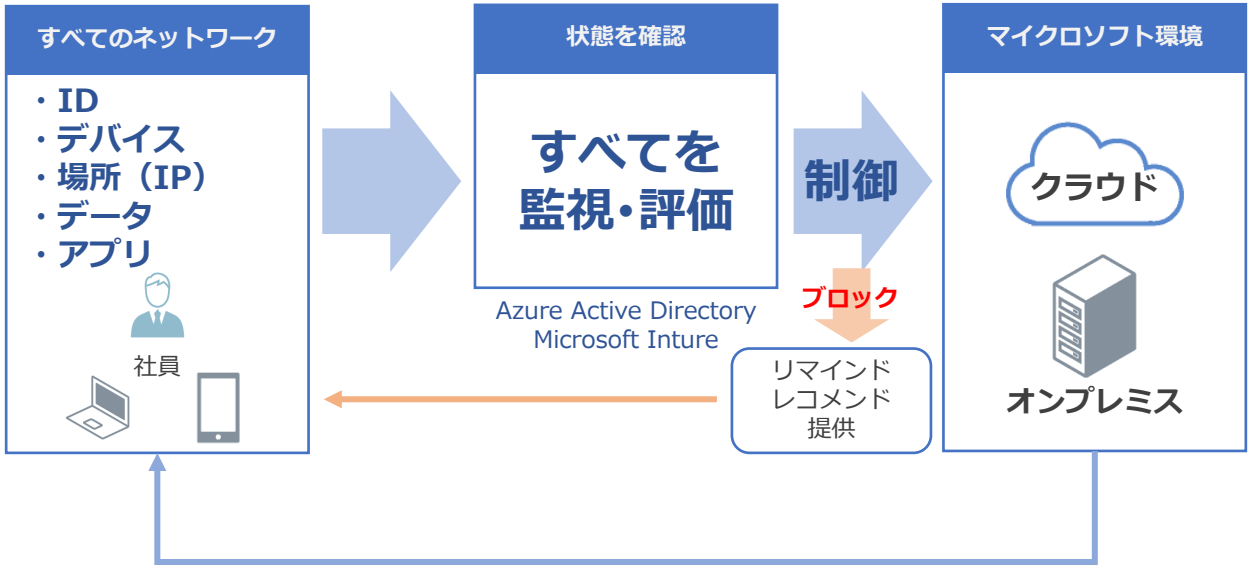
製品情報は2021年1月時点のものである。

マイクロソフトゼロトラストセキュリティ
概要と特徴（1/2）

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。

マイクロソフトゼロトラストセキュリティ
概要と特徴（2/2）

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。



マイクロソフトゼロトラストセキュリティ
事例検証結果

#	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	○	GPOにて設定。
3	端末管理	○	SCCM、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	○	SCCM、Intune等にて実施。
6	プリンタ	○	データそのものの制御（RMS、AIP）
7	外部メール	-	-
8	個人クラウド	○	AzureADテナント制限。
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

海外事例検証結果

ZTAはリモートワーク阻害要因のリスク低減として有用な手段であることが確認できた。
しかし、ZTAだけで全てのリモートワーク阻害要因を解決できないこともわかった。

#	リモートワーク阻害要因	海外事例（ZTA）	
		Google BeyondCorp	マイクロソフト ゼロトラスト セキュリティ
1	回線逼迫	○	○
2	Wi-Fi設定	○	○
3	端末管理	○	○
4	BYOD	○	○
5	外部デバイス	○	○
6	プリンタ	○	○
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

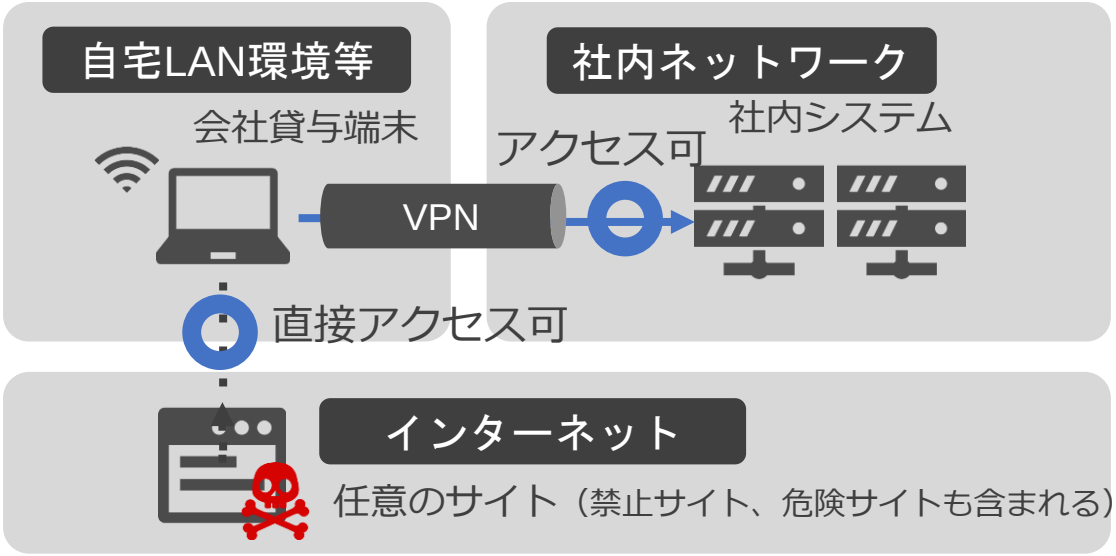
国内ネットワーク事業者事例調査

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。

- **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**

ソフトバンクの常時VPN
概要と特徴（1/3）

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。



ソフトバンクの常時VPN
概要と特徴（2/3）

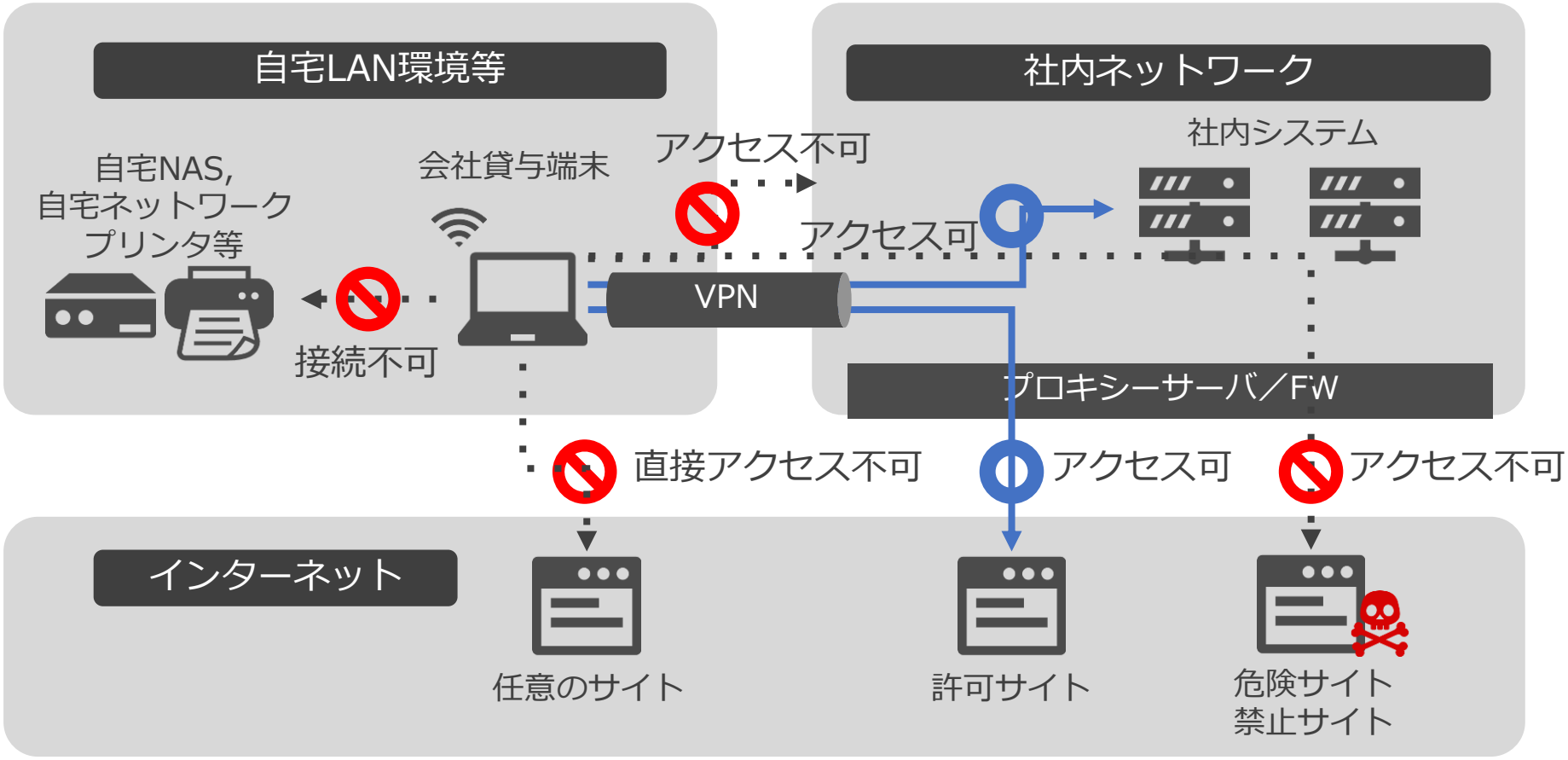
これを解決するため、社外環境において会社貸与端末からインターネットやSaaS等、社外のサイトへアクセスする際の経路を制御することとした。

具体的には、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、自宅やネットカフェ等、場所に関わらず、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。

また副産物として、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にもつながる。

ソフトバンクの常時VPN
概要と特徴（3/3）

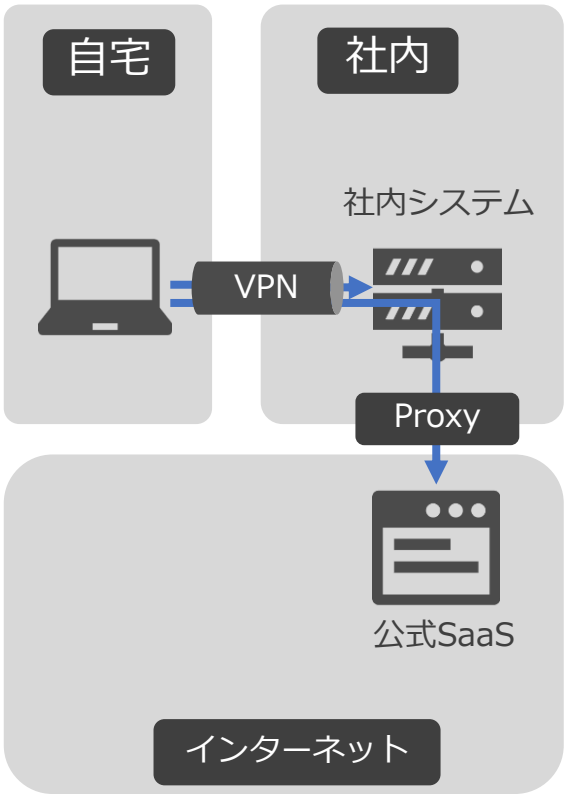
常時VPN化した場合のアクセスルート、制御状況を以下の図に示す。



ソフトバンク

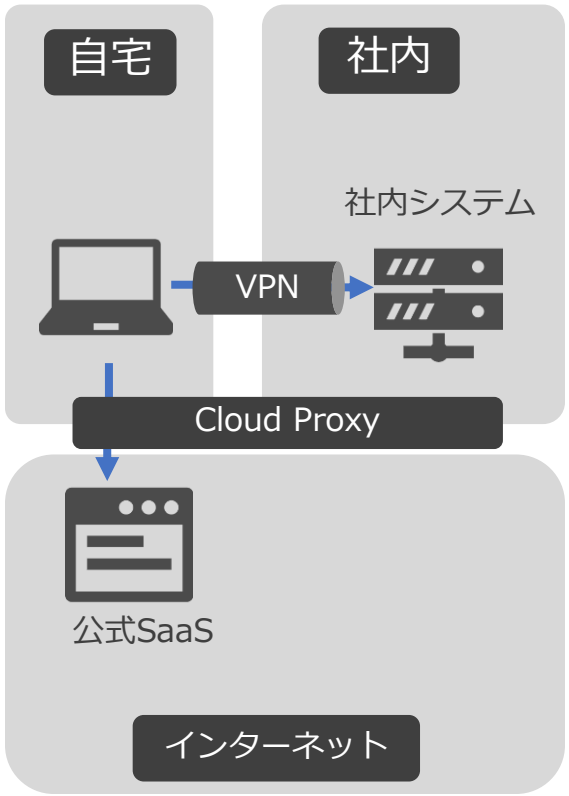
ZTA化に向けた3ステップ

Step1



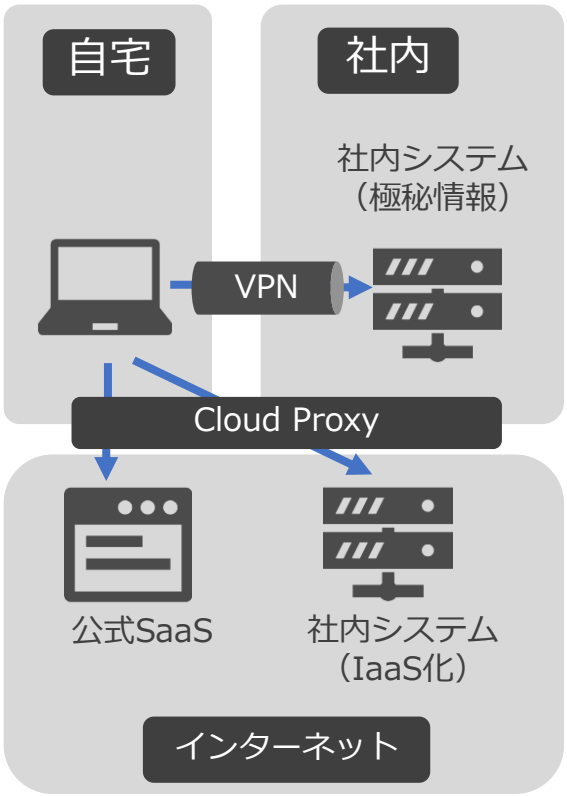
社外のアクセスを
常時VPN化

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）

ソフトバンクの内部不正対策
概要と特徴（1/2）

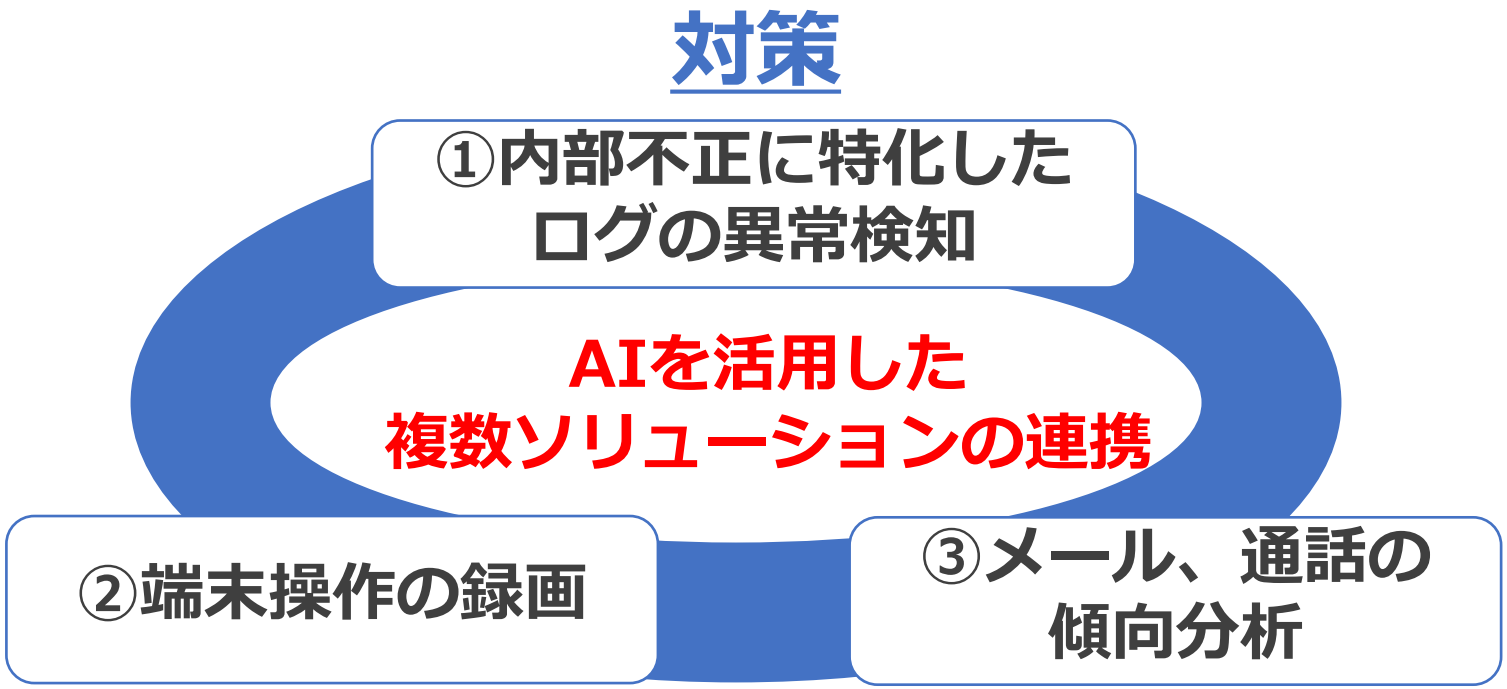
これまで、ソフトバンク内のセキュリティ監視は外部脅威からのサイバー攻撃に関する監視・検知が主体であったが、昨今の内部不正事案の増加に伴い、抜本的な対策見直しがなされた。

（これまでの対策の課題）

- 既存のログ解析の相関ルールにおいて、その大半は社外からのサイバー攻撃に関するものであり、**内部不正を検知するルールは限られていた**。
- 正当権限者が不正を犯すケースの場合、特定のエラーの発生や不審なコマンドなど打たれるわけではなく、**ログ上には一見して不審な点が残りにくかった**。
- 内部不正をつきとめるためのログ解析の観点やノウハウは、**既存のセキュリティ監視とは異なる専門性、スキルを要していた**。

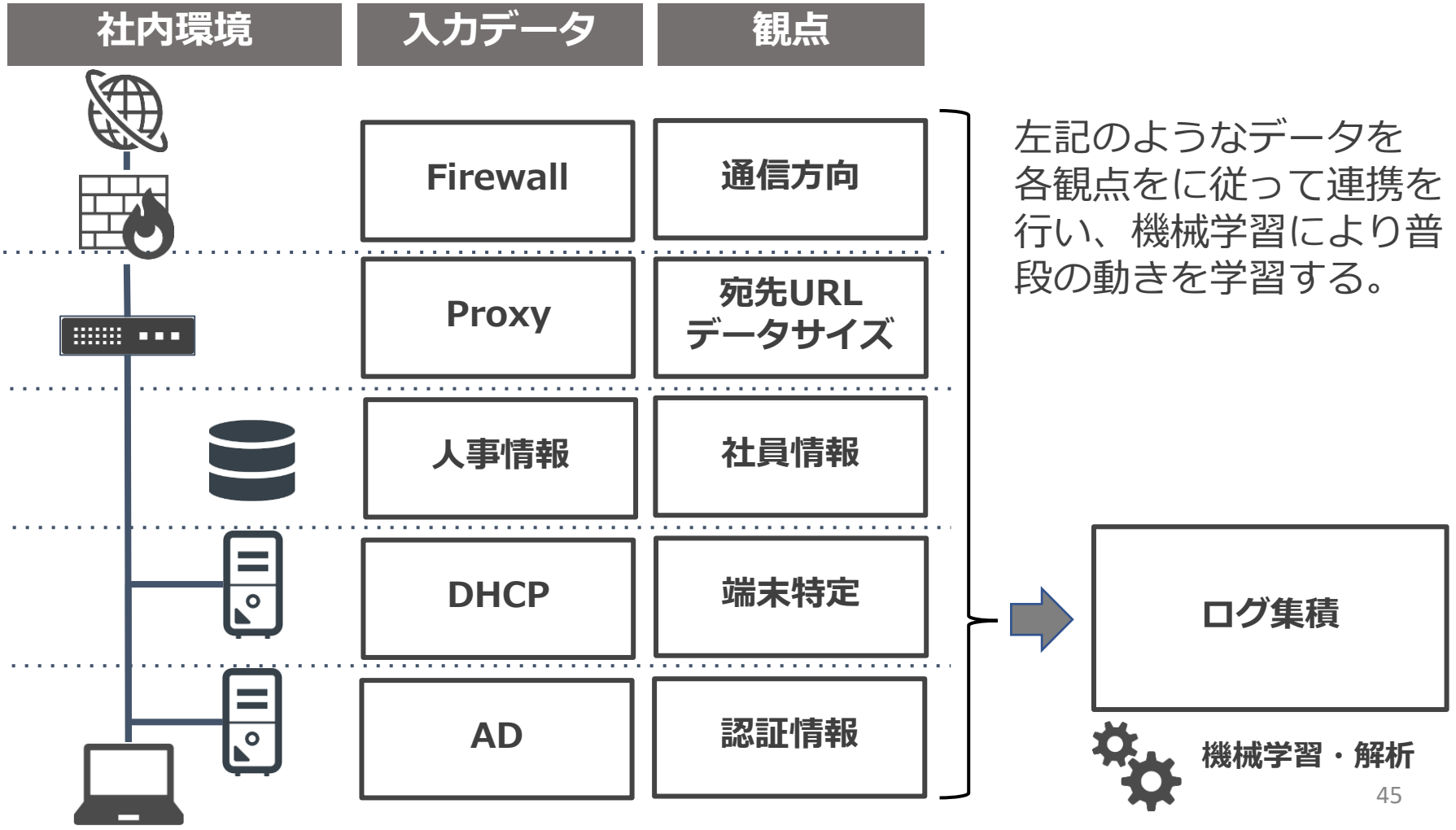
ソフトバンクの内部不正対策

概要と特徴（2/2）



ソフトバンクの内部不正対策
①ログの異常検知（1/2）

（入力するデータとその観点の例）

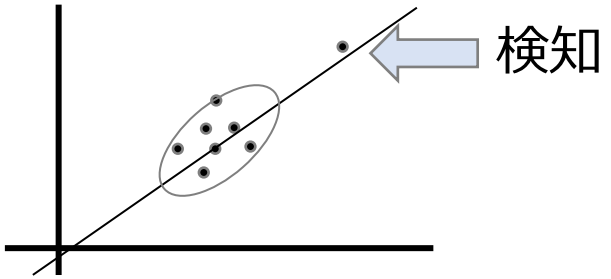


左記のようなデータを各観点をに従って連携を行い、機械学習により普段の動きを学習する。

ソフトバンクの内部不正対策
①ログの異常検知（2/2）

（入力するデータとその観点の例）

- 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。



（検知される事象の例）

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

ソフトバンクの内部不正対策
②端末操作の録画（1/2）

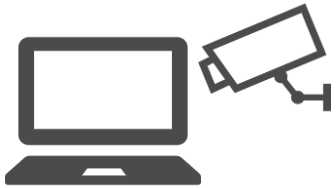
端末やサーバにエージェントを導入することで、以下のような機能を実現する。

検知

- 悪意のある振る舞いの検知
- 過失の検知
- テキスト分析

調査

- 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



抑止

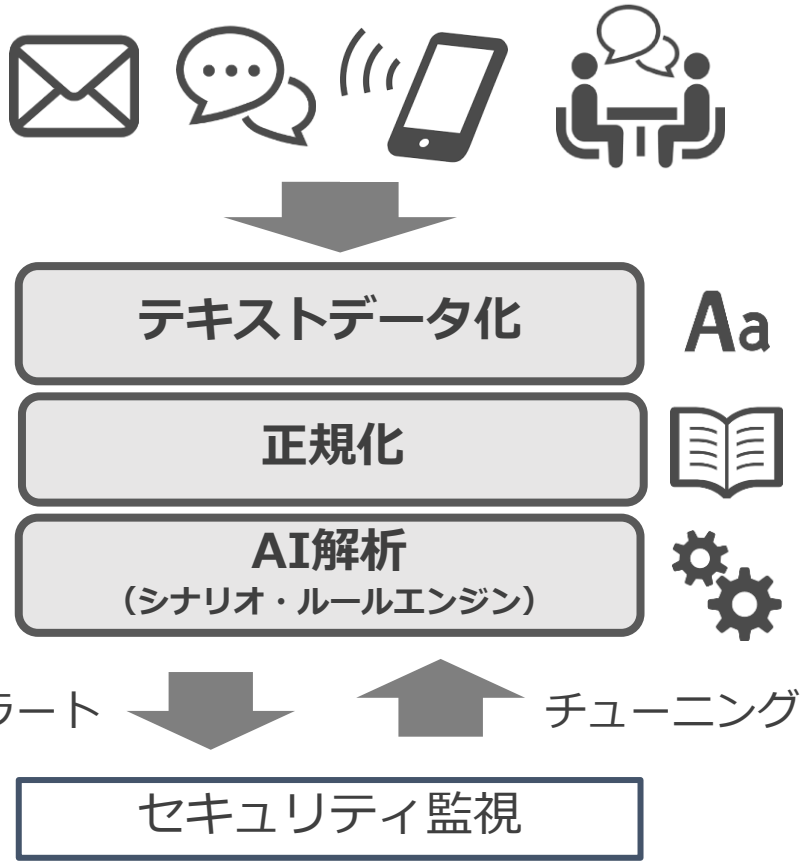
- プロセスブロック
- ポップアップ警告

ソフトバンクの内部不正対策
②端末操作の録画（2/2）

（期待される効果）

- 画面の動きや画面内で打たれたテキストの内容を含めた分析により、**怪しい振る舞いの検知**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、**不正を未然に防止したりセキュリティルールの教育効果**もある。

ソフトバンクの内部不正対策
③メール、通話の傾向分析（1/2）



・情報漏えい検知
・コンプライアンス違反

- 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元に、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

ソフトバンクの内部不正対策
③メール、通話の傾向分析 (2/2)

（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**
  情報漏洩以外にコンプライアンス違反なども応用可能

ソフトバンク
事例検証結果

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軽減効果をもたらしていることがわかった。

#	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振る舞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

事例検証結果

既存のZTAと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。

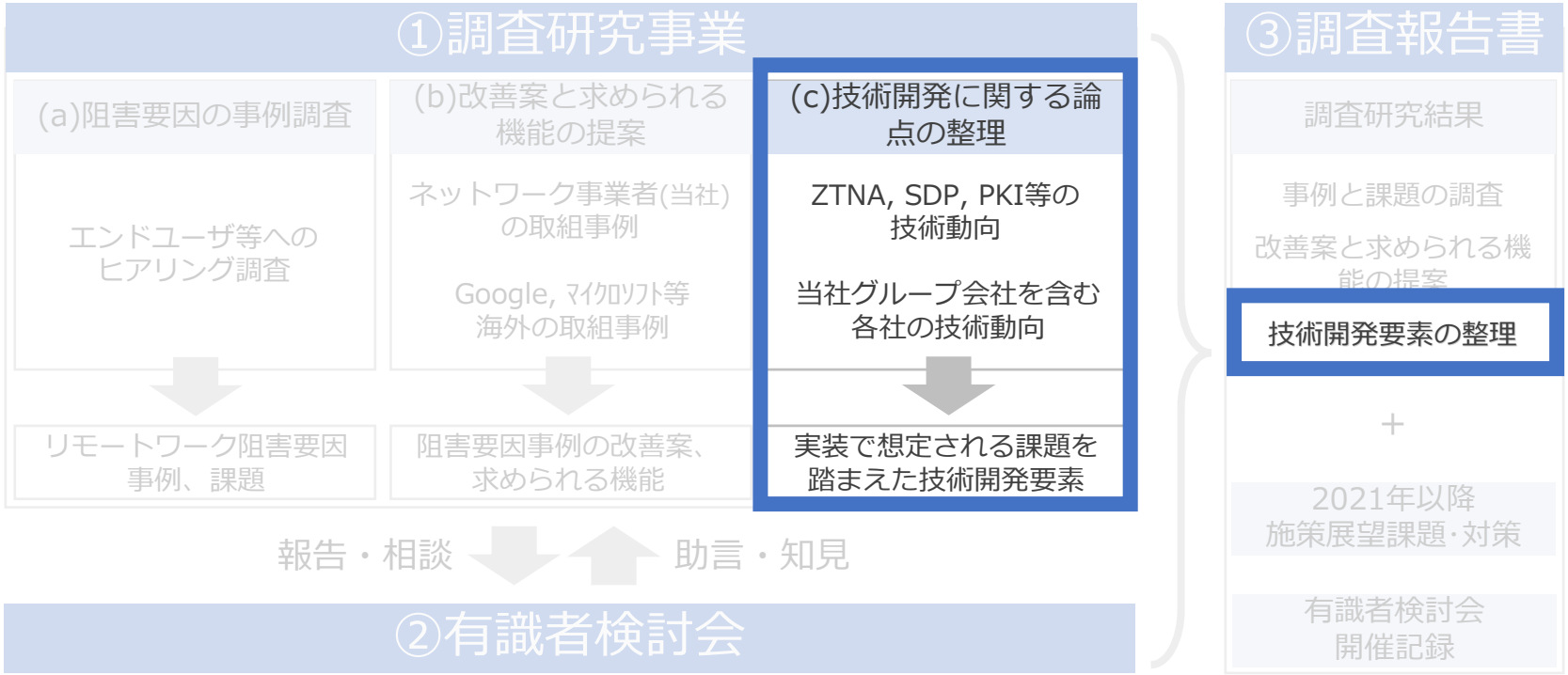
#	リモートワーク阻害要因	海外事例（ZTA）		ソフトバンク事例	
		Google BeyondCorp	マイクロソフト ゼロトラスト セキュリティ	常時VPN	内部不正対策
1	回線逼迫	○	○	※ネットワーク事業者は問題になりにくい	
2	Wi-Fi設定	○	○	○	-
3	端末管理	○	○	○	-
4	BYOD	○	○	※別の対策（VDI）により対策済み	
5	外部デバイス	○	○	-	○
6	プリンタ	○	○	※ペーパーレス化のため問題になりにくい	
7	外部メール	-	-	-	○
8	個人クラウド	○	○	-	○
9	内部不正	-	-	-	○
10	高機密データ	-	-	-	-

○：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

技術開発要素の整理

技術開発要素の整理

メインプレイヤーの最新の取り組みや周辺技術研究動向を収集し、適用可能性を考慮した上で必要な技術開発要素を整理した。



ZTA展開モデルから調査対象を選定

調査対象技術はリモートワークと相性がいいとされる、アメリカ国立標準技術研究所(NIST)から発行されたゼロトラストアーキテクチャ(ZTA SP800-207)より、モデル毎のソリューション例(下記図1)から**ZTNA**や**SDP**(**Software Defined Perimeter**)および**VDI**(**Virtual Desktop Infrastructure**)や**UEM**(**Unified Endpoint Management**)、 **PKI**(**Public Key Infrastructure**)とした。

調査方法はガートナー社のレポートを基本とし、インターネットなどの情報から補足して結果をまとめた。

シンクライアントは、ゼロクライアント等関連情報を探したが、現時点で有益なレポートが存在しなかった。

NIST SP 800-207 ZTA展開モデル			
ゲートウェイモデル	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	
ZTNA/SDP	**VDI**	**UEM** MAM, MTDから変更	＋ **PKI**
		シンクライアント 情報不足	

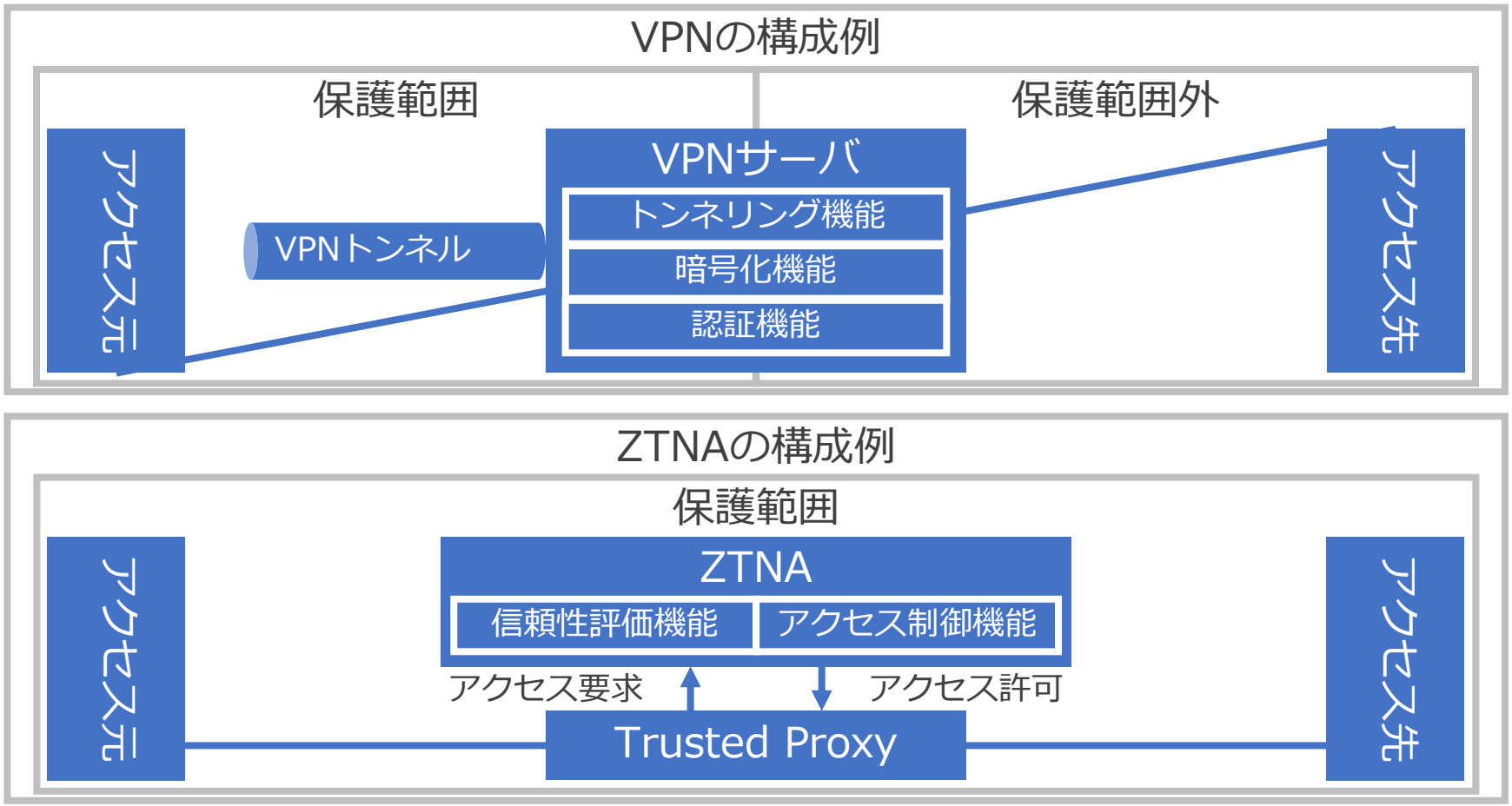
ZTNA/SDP概要

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った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為、本調査目的から同一のものとして扱うこととする。

VPNとの構成の違い


VPNの構成例
保護範囲
保護範囲外
アクセス元
VPNトンネル
VPNサーバ
トンネリング機能
暗号化機能
認証機能
アクセス先
ZTNAの構成例
保護範囲
アクセス元
ZTNA
信頼性評価機能
アクセス制御機能
アクセス要求
アクセス許可
Trusted Proxy
アクセス先

ZTNA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。

ZTNAメインプレイヤー（1/3）

■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)
Microsoft	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

ZTNAメインプレイヤー (2/3)

■クラウド型サービス（1/2）

提供会社	本社	サービス名
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

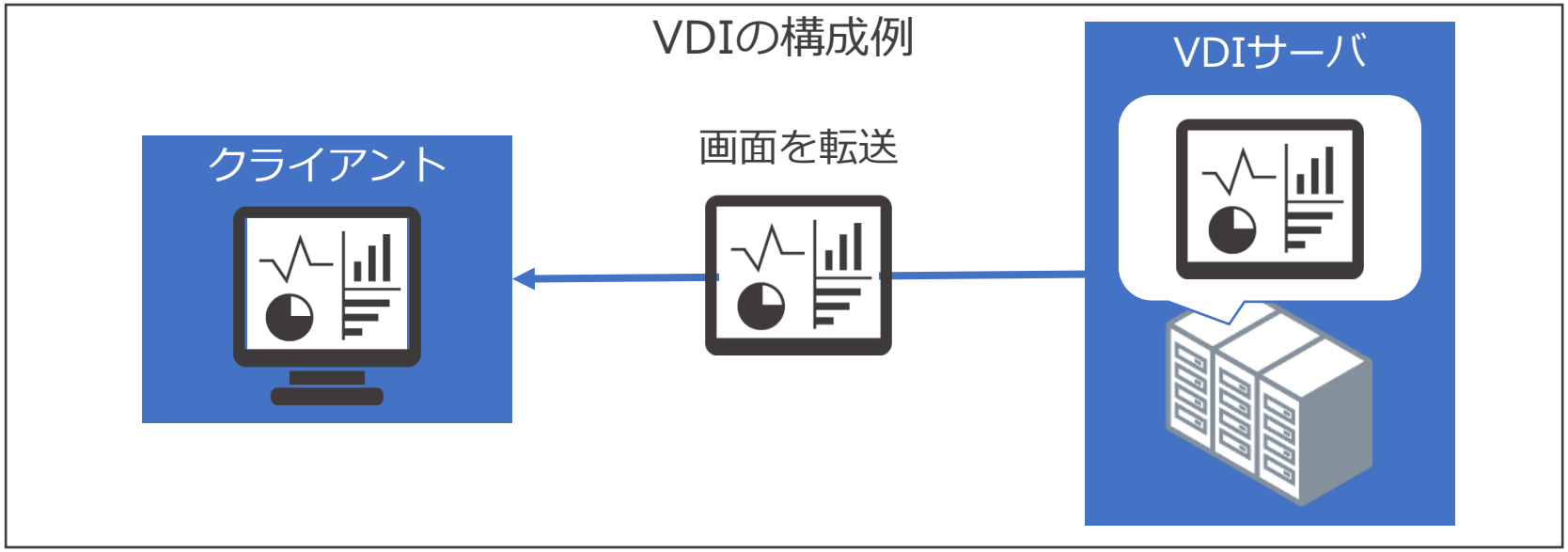
ZTNAメインプレイヤー (3/3)

■クラウド型サービス（2/2）

提供会社	本社	サービス名
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

VDI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為、クライアントからの情報漏えいのリスクを軽減できる効果が期待できる。



VDI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。

VDIメインプレイヤー (1/2)

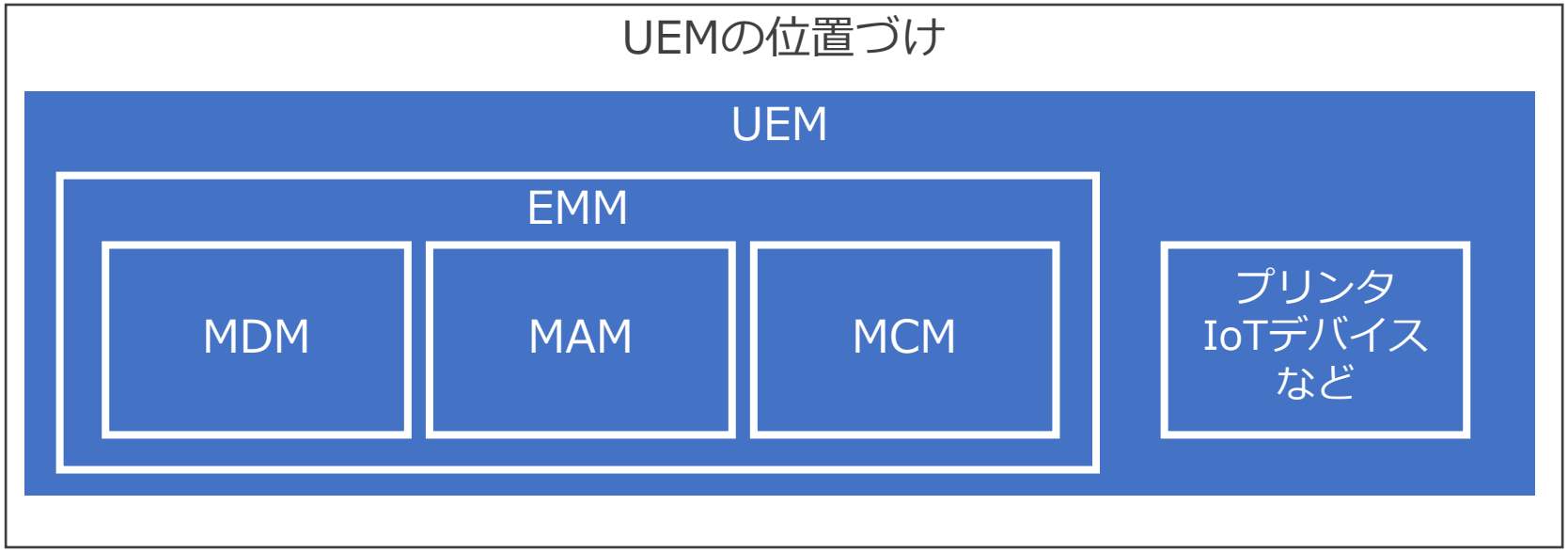
提供会社	本社	サービス名
Anunta	インド	Managed DaaS on Azure Cloud Fully Managed Horizon Desktops
Amazon Web Service	アメリカ	Amazon WorkSpaces
Citrix	アメリカ	Citrix Managed Desktops
Cloudalize	ベルギー	Desktop-as-a-Service
CloudJumper	アメリカ	Cloud Workspace
dinCloud	アメリカ	dinWorkspace
Diso	スイス	Secure Workplace
Dizzion	アメリカ	Cloud Desktops
Effortless Office	アメリカ	Effortless Desktop
Evolve IP	アメリカ	Desktop as a Service
Kivito	ドイツ	deskMate
Microsoft	アメリカ	Windows Virtual Desktop
Nutanix	アメリカ	Xi Frame

VDIメインプレイヤー (2/2)

提供会社	本社	サービス名
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

UEM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。



UEM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。

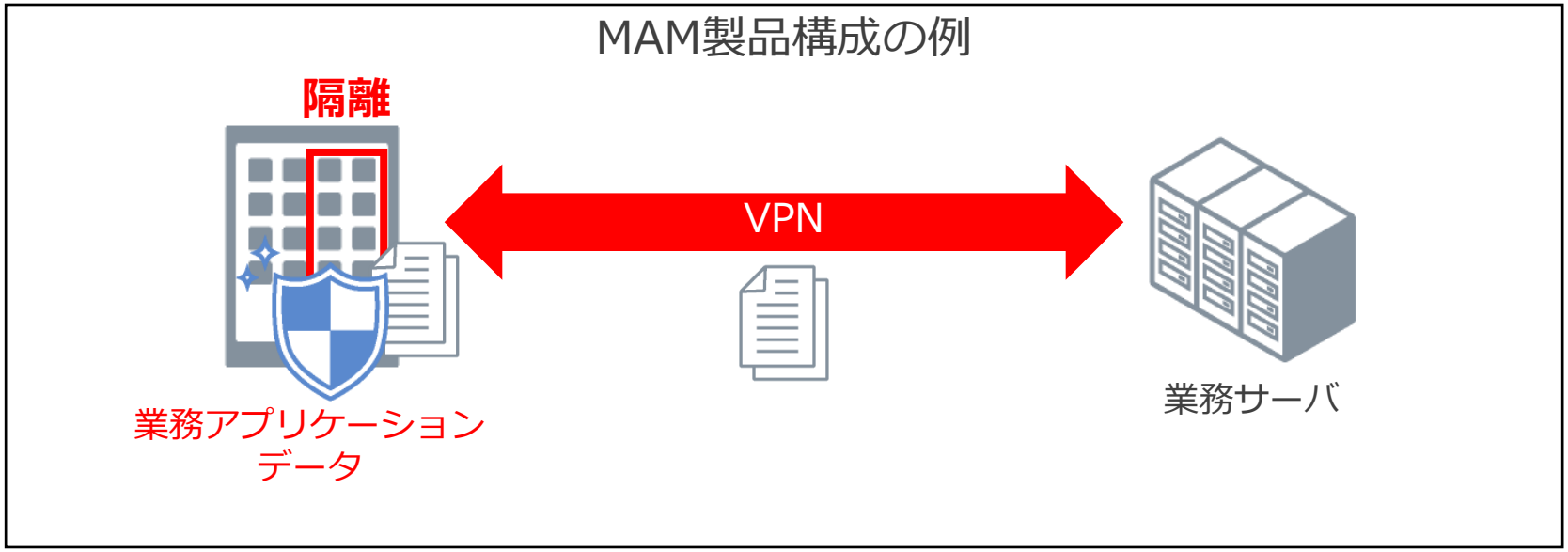
UEMは今までデバイス管理を別々の製品で行ってきた場合や、**より管理対象を増やしたい場合（プリンタやIoTデバイスなど）**に向いているが、多機能である為目的に応じて製品選定を行う必要がある。

UEMメインプレイヤー

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
Microsoft	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

MAM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。



MAM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為、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。

MAMメインプレイヤー

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

PKIへの懸念調査

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。

懸念点は長年認証局を運用されてきた実績のあるサイバートラスト社にもご意見をいただいた。

PKI懸念点一覧

PKIの懸念は小さい

#	懸念点	結果	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に準拠した製品を選定することが求められる。	懸念小

日本のルート認証局

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。

技術開発要素の整理まとめ

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。**地政学的リスクにより、高機密データを取り扱う際に使用するサービスやシステムに対する安全性が脅かされることが懸念される状況となっている。

■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

総括

施策展望課題・対策

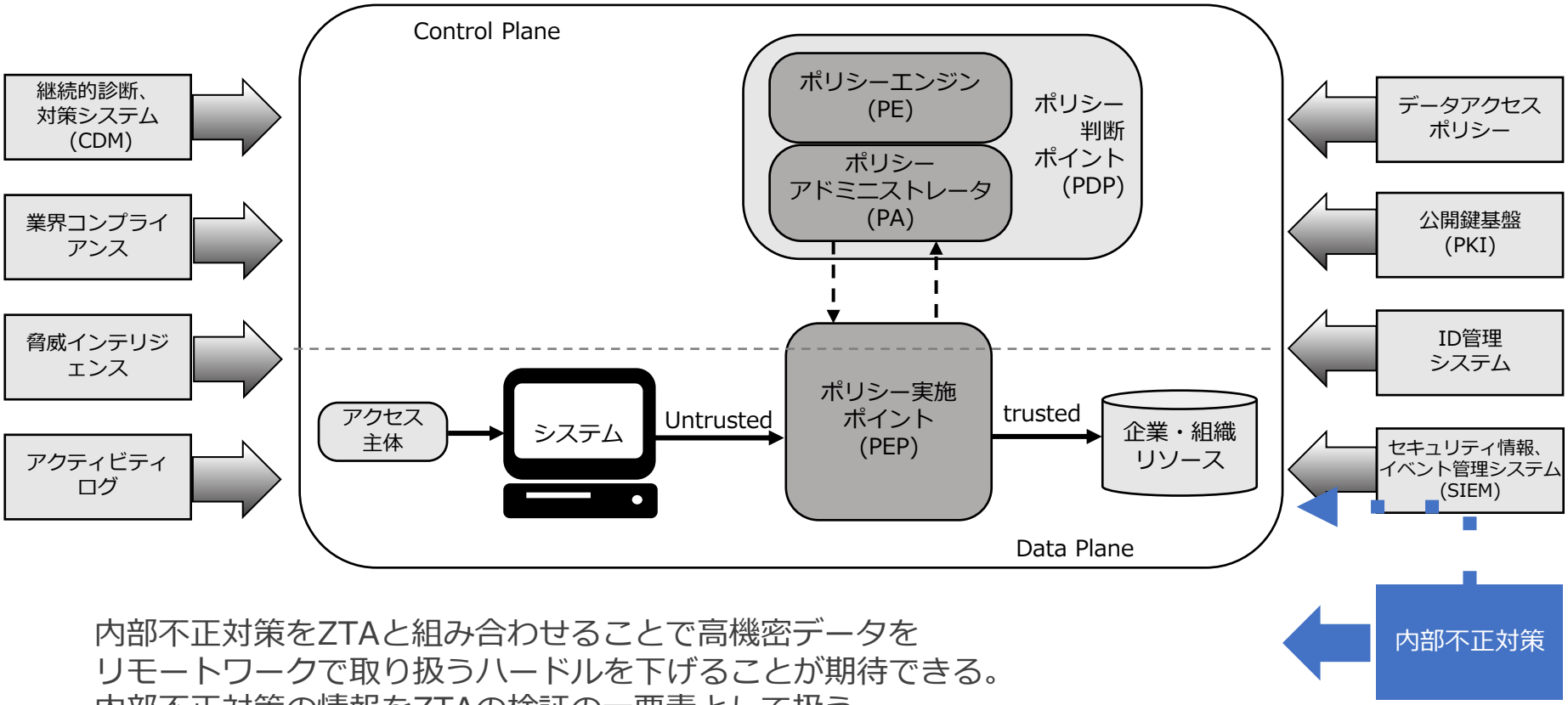
安全・安心で利便性の高いデジタル社会基盤の構築を目的に、本事業の調査成果をもとに求められるセキュリティ技術について施策展望・課題・対策について整理する。

総括

- 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を始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をリモートワーク推進にはZTAだけではなく、内部不正対策との融合と強化が必要と考える。
- 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。

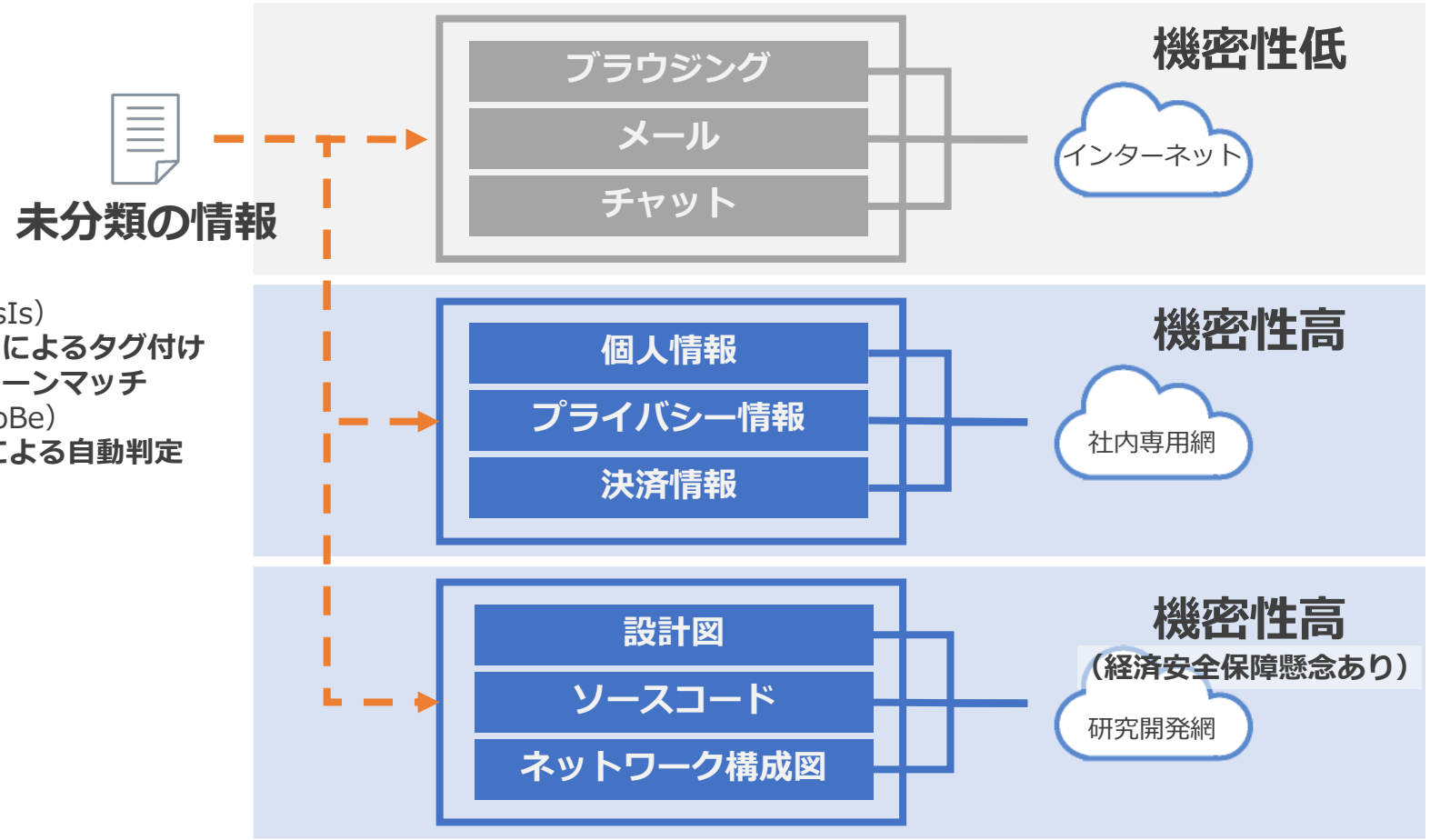
施策展望①
ZTAと内部不正対策の融合



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。

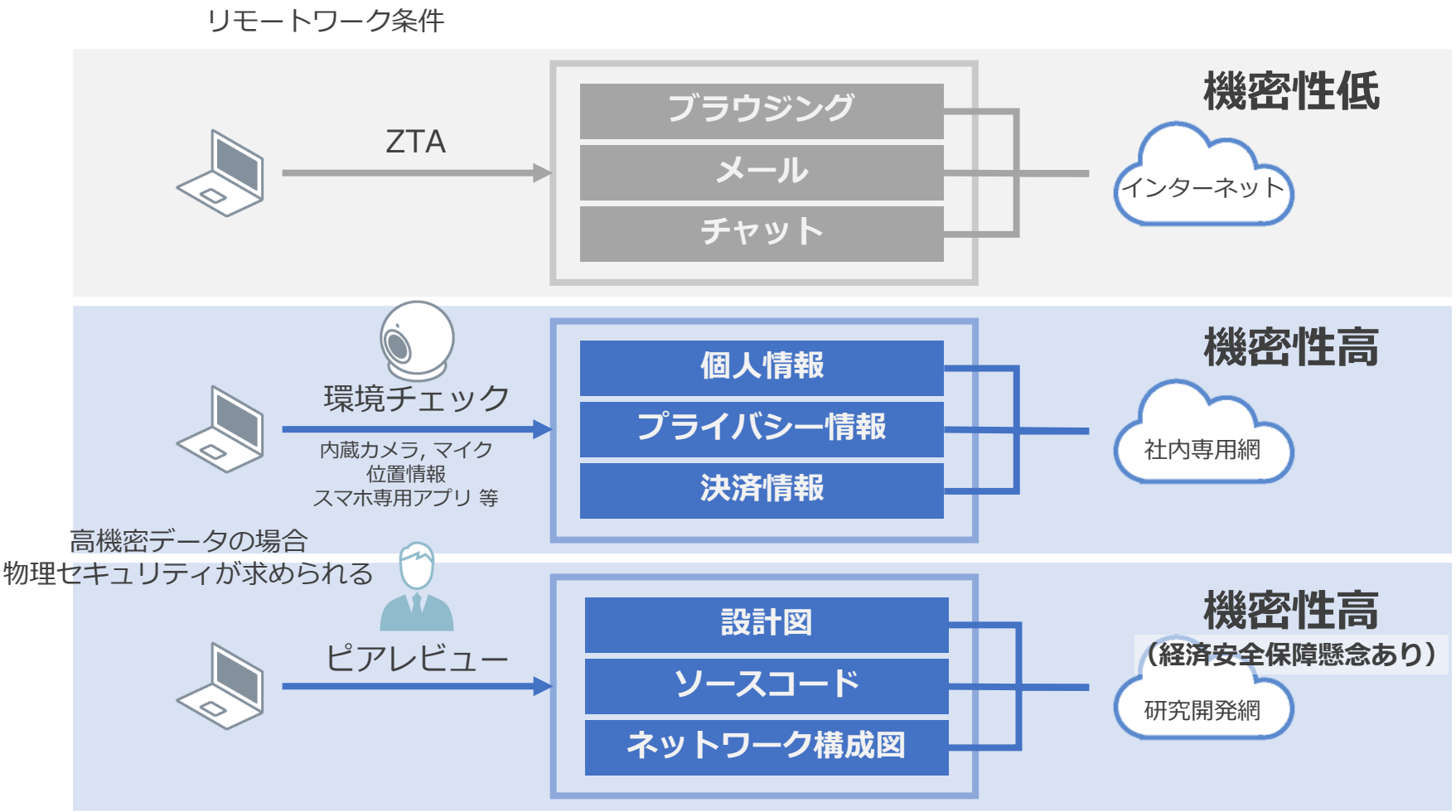
施策展望②

情報の機密度の自動判別



施策展望③

職務状態・環境管理の多様化

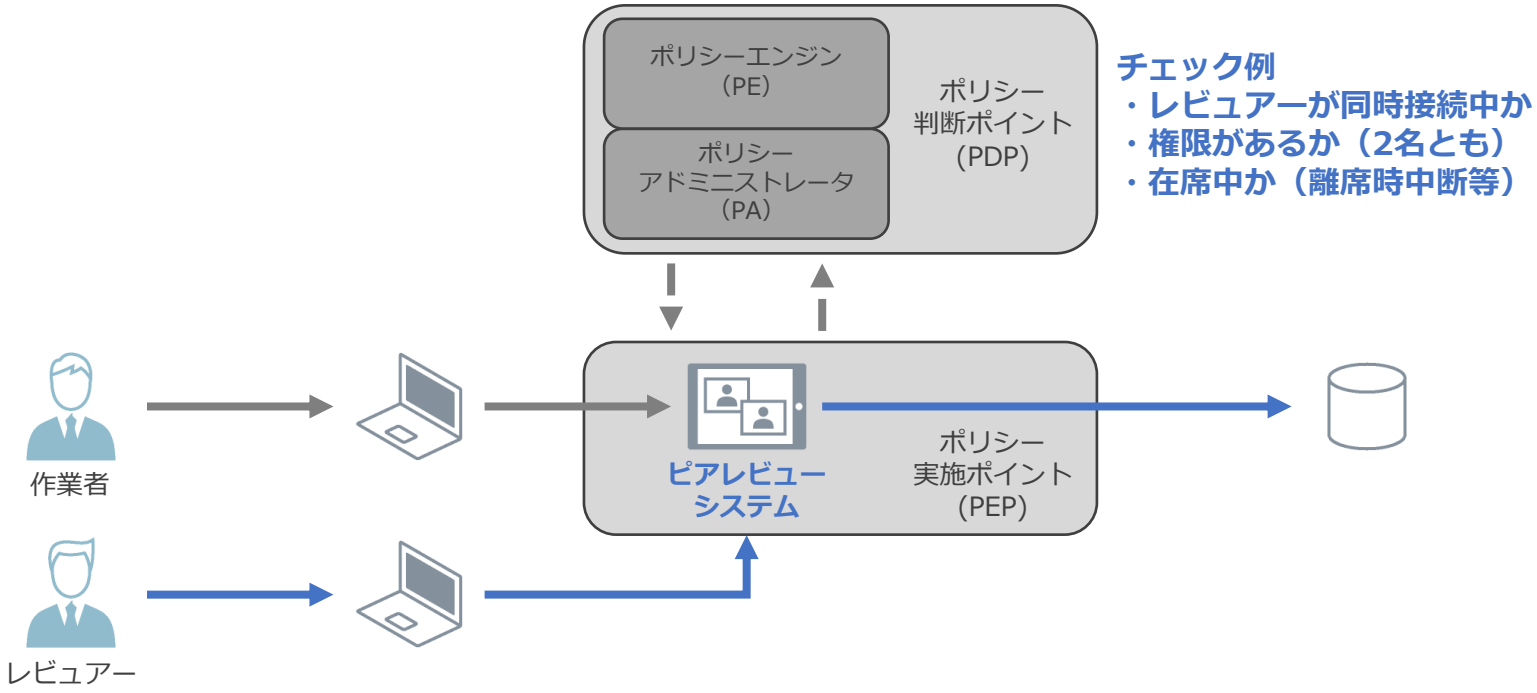


自治体業務のリモートワーク等にも応用の可能性

施策展望③補足1
環境チェック

- 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。

施策展望③補足2
ピアレビュー



- 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。

過度な監視は不要

- 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。

従業員のプライバシーに配慮

- 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。

（追加調査検討事項）

1. **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）を網羅した調査が今後求められる。
2. **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今後求められる。
3. **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今後求められる。

ZTAコンポーネント調査イメージ

#	コンポーネント	ソリューションカテゴリ	国産ソリューション例
1	ポリシーエンジン(PE)	ZTNA/SDP	• ActSecureセキュリティ ゲートウェイサービス
2	ポリシーアドミニストレータ(PA)	ZTNA/SDP	
3	ポリシー実施ポイント(PEP)	ZTNA/SDP, Firewal, Proxy, VDI, ThinClient, UEM	• i-FILTER • InterSafe WebFilter • RevoWorks • ThinBoot
4	継続的診断および対策(CDM)	Vulnerability Management, CMDB	• SKYSEA
5	業界のコンプライアンスシステム	FISMA, FISC, PCIDSS	
6	脅威インテリジェンスフィード	IoC, OSINT, Cyber Threat Intelligence, Dark Web	
7	ネットワークおよび システムのアクティビジティログ	EDR, EPP, NDR	• FFRI yarai
8	データアクセスポリシー	DLP, CASB	• InfoBarrier • ALog ConVerter • ESS REC • WEEDS Trace • 秘文
9	企業の公開鍵基盤	PKI	• CyberTrust • SECOM Trust Systems
10	ID管理システム	Active Directory, LDAP, IDaaS	• HENNGE • TrustLogin
11	セキュリティ情報およびイベント管理	SIEM, UBA	• Logstorage

※調査中。ZTA対応, ZTNA/SDP連携対応はいずれのソリューションも未確認。

施策展望まとめ

（課題）
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はリモートワークが禁止**されていることがあった。
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。

（対策）

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**