2020年度　ITインフラ研究会
分科会B　活動報告資料

コロナ禍の働き方・生活様式への適応に
貢献するITインフラ技術

2021年4月

ITインフラ研究会　分科会B

目次

1. 研究の背景

■研究テーマ

「ITインフラの技術トレンド、ビジネス活用」をメインテーマとして、特に**「コロナ禍の働き方・生活様式への適応に貢献するITインフラ技術」**を研究テーマとした。

■選定理由

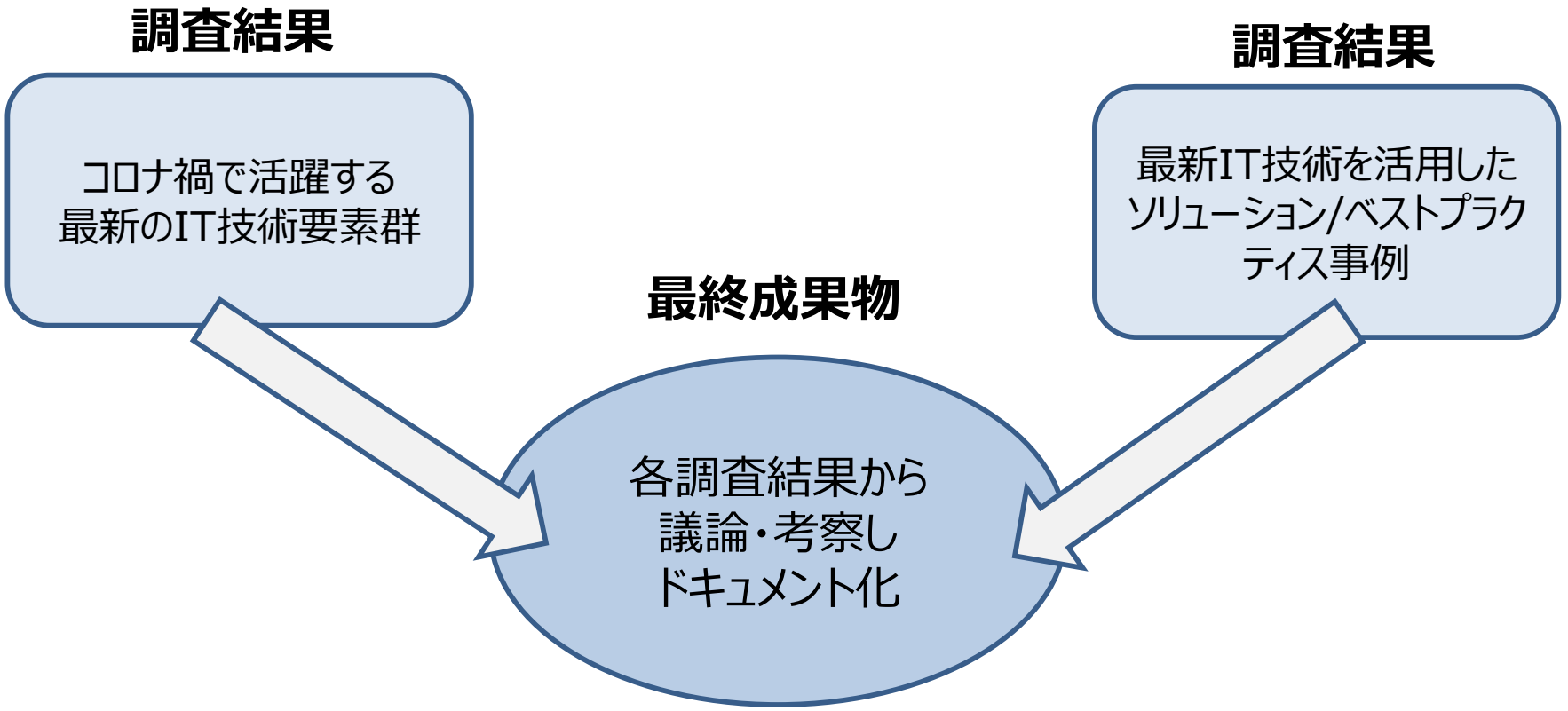
世界的なコロナウィルス感染拡大に伴い、働き方の変革が求められている、今だからこそ取り上げるべきテーマとして、「コロナ」「働き方・生活様式」を起点として研究活動を進め、この状況下で働き方改革に貢献するITインフラのあり方について技術分野から検討考察した。

■選定の背景

選定の背景として、以下があがった。
・世界規模での新型コロナウィルス感染拡大に伴い、日本をはじめ各国の生活様式は変容
・海外、国内のビジネスにも大きな影響
・あらゆる企業の事業活動が変化を求められる中、ITインフラが果たすべき役割は何か
・最新の技術動向・事例から、働き方・生活様式の変容に適合・貢献するITインフラ技術とそのあり方を明らかにする

2. 研究の目的・Goal

IT要素技術の最新動向を調査結果として纏めるとともに、コロナ禍においての働き方・生活様式・ビジネス要求などへ適応できる最新ITインフラ技術および活用されたソリューションやベストプラクティスはどういったものか各調査した結果を合流し最終的にドキュメント化することをゴールとした。



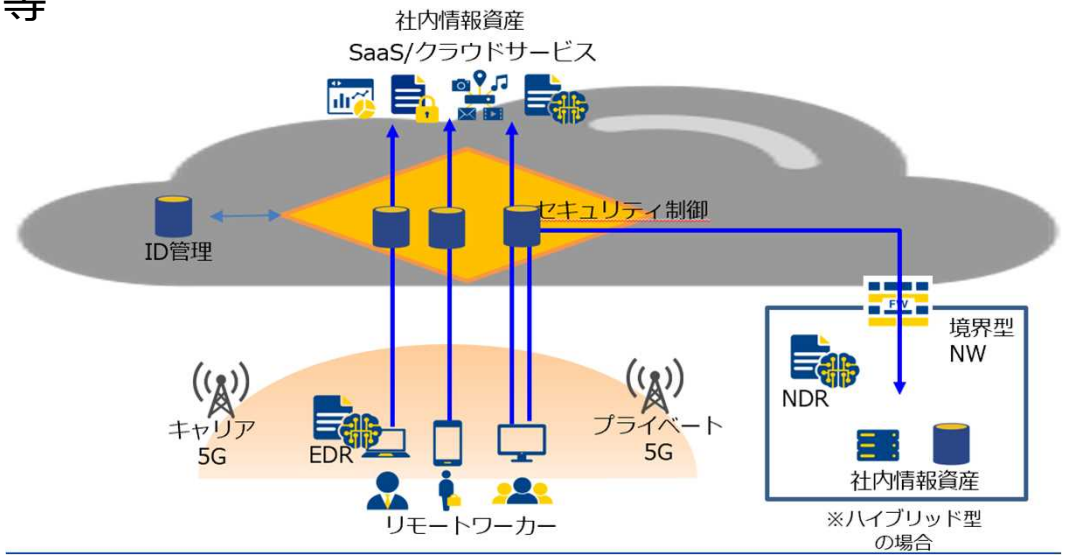
3. 研究活動における結論

■ニーズ
コロナ禍において、場所や時間、端末にとらわれないフレキシブルな働き方が求められている。
その実現に向け、ITインフラでは、生産性を下げず、安全、快適なリモートワークを行える環境の整備が必要である。

■多くの企業が持っている課題
・従来の境界防御型セキュリティ対策では守り切れない
・オフィスワーカー主体、社内システム利用前提としたネットワーク構成ではキャパシティ不足

■ITインフラでの解決策（技術要素/アーキテクチャ）
セキュリティ：EDR、MDM、多要素認証、Cloud SWG、リモートPCの活用 等
ネットワーク： ５Gの活用、アーキテクチャの変更 等

■理想的アーキテクチャに至るアプローチ
コロナ禍においては迅速性が求められており、
時間、コスト的にハードルの低いものから、
段階的に技術要素を取り入れ、アーキテクチャを
変えてくことを推奨する。
会社の状況に応じて、出来るところから段階的に
進めることが重要だと考える。



4. 研究の進め方(方針)

■基本方針

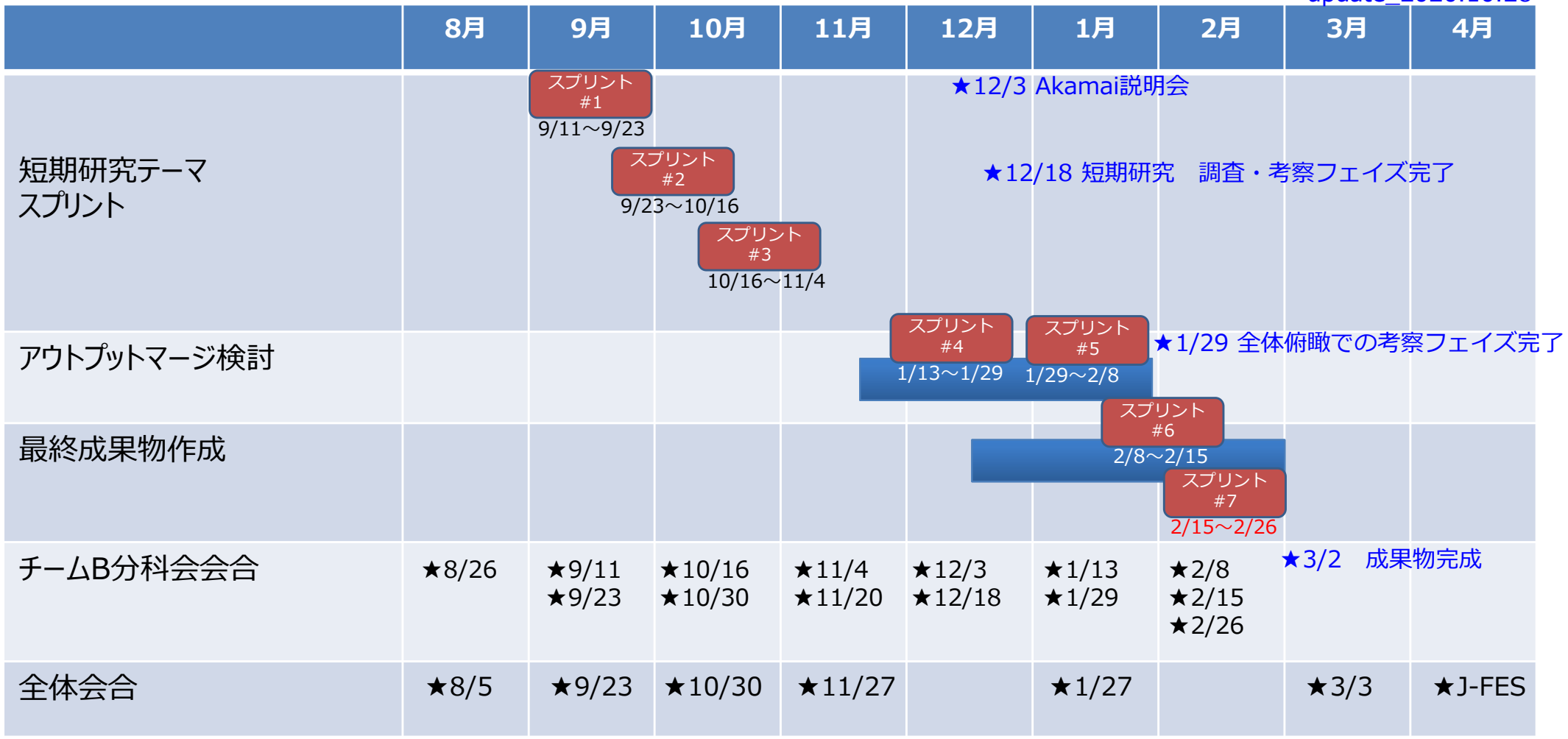
・アジャイル開発のコンセプトを適用
  - 短いスプリント期間(2~3週)で小さいアウトプットを繰り返す
  - 変化に対応・計画よりアウトプット重視
  - 各スプリントで短期研究テーマを設定、数名のセルに分かれて並列で調査、考察、報告

・最終成果物に各スプリント成果物を合流
・定期的に個々の成果物を全体俯瞰し、考察と知見を見い出す

4. 研究の進め方（スケジュール）

・研究スケジュール内での具体的な活動は、短期研究テーマスプリントのアウトプットを元に決定
・後半はスプリントのアウトプットを元に変更

update_2020.10.28



4. 研究の進め方(スプリント研究テーマ決め)

メインテーマを掘り下げ、チーム内でソリューション要求、要素技術を抽出し、それらを短期研究のテーマにした。

■Level_1テーマ
【メインテーマ/命題】

コロナ禍の働き方・生活様式への適応に貢献するITインフラ技術

breakdown

■Level_2テーマ
【ビジネス要求】

コロナ | **働き方** | **生活様式** | **多様化** | **リモート**

在宅 | **生産性** | **セキュリティ** | **スピード** | **新ビジネス**

breakdown

■Level_3テーマ
【ソリューション要求】
【要素技術】

短期研究テーマ 選定領域

ゼロトラスト	SASE	コンテナ	5G	認証認可
ローカルブレイクアウト		Docker	パブリッククラウド	
CASB	SWG	Kubernetes	EDR	
SDP	VDI	BYOD	SD-WAN	・・・

この領域の「キーワード」から短期研究テーマスプリントのテーマを選択しました

5. コロナ禍における働き方

新型コロナウイルス感染症の流行を受け、私たちの勤務形態は変化を余儀なくされた。

- **出社**
  - 工場勤務、病院看護、介護職など
  - **人と接する**ものの、マスク着用、ソーシャルディスタンス確保、パーテーション設置、こまめな換気など、**３つの密を避ける働き方**に変化
    ITでの対応：画像や位置情報による解析、警報、etc.

- **リモートワーク**
  - デスクワーク業務、サポート業務など
  - **人と直接接しない働き方**に変化
  - 環境整備のために**ITインフラの大幅な対応**が必要となった
    ITでの対応：デバイス、ネットワーク、セキュリティ、社内システムの整備、etc.

- **健康管理**
  - 出社/リモートワークを問わず、日常的な**体温計測**、**体調管理**が必須となる
    ITでの対応：非接触での計測、入館制御、データ管理、etc.

研究会参加者への関連が深く、アフターコロナ時代の働き方への影響も大きいと考えられることから、本研究会活動では、コロナ禍における働き方の変化として**リモートワーク**に着目した。

6. コロナ禍における働き方に関する課題

研究チームメンバの各所属企業、および関係者へのヒアリング/情報収集により、以下の課題が明らかになった。

- 部分的にリモートワークを行っていた企業で全社へ切り替えたことにで**キャパシティ不足**が発生
  - リモートアクセス用**VPN**の逼迫、リモート用ツールのライセンス/アカウントの不足

- リモート会議が主体となり他の**リモートアクセス環境との相性の悪さ**が露見
  - **VPN接続**時に企業のインターネット回線にトラフィックが集中しボトルネックとなる、**VDI環境**でリモート会議を行うとパフォーマンス不足により満足に接続できない

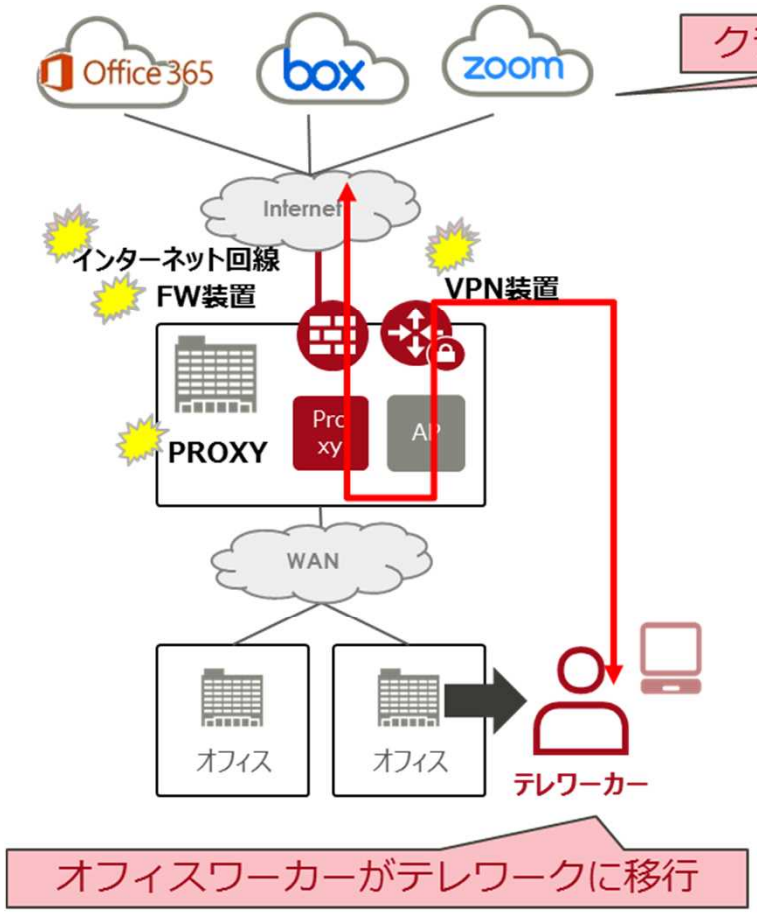
- そもそも**リモートワークの環境整備ができていない**
  - **セキュリティ**観点で社給PCの持ち出しが禁止されている、急な要請によりリモートアクセス環境が整備できない

- **出社しなければ行えない業務**が残りリモートワークへの切り替えが行えない
  - 紙媒体が必要となる業務、押印が必要な業務、運用オペレータ業務、etc…

これまでのITインフラがコロナ禍における働き方、特にリモートワークでは**足枷**となってしまうことがある。これらの課題を解決するために最新のIT技術群の調査を行う。

6. コロナ禍における働き方に関する課題

COVID-19禍により表面化した課題：①通信ネットワークのキャパシティ不足



クラウドサービスの利用が多くなる

- インターネット回線の輻輳／帯域不足
- VPN装置の性能不足
- FW装置の性能不足
- PROXY装置の性能不足

テレワーカーの急激な増加で、従来と異なる利用状況に
想定外の負荷となり性能限界となったポイントが複数発生し、レスポンス低下による機器の増設や強化が必須となった。

出典：富士通エフサス

6. コロナ禍における働き方に関する課題

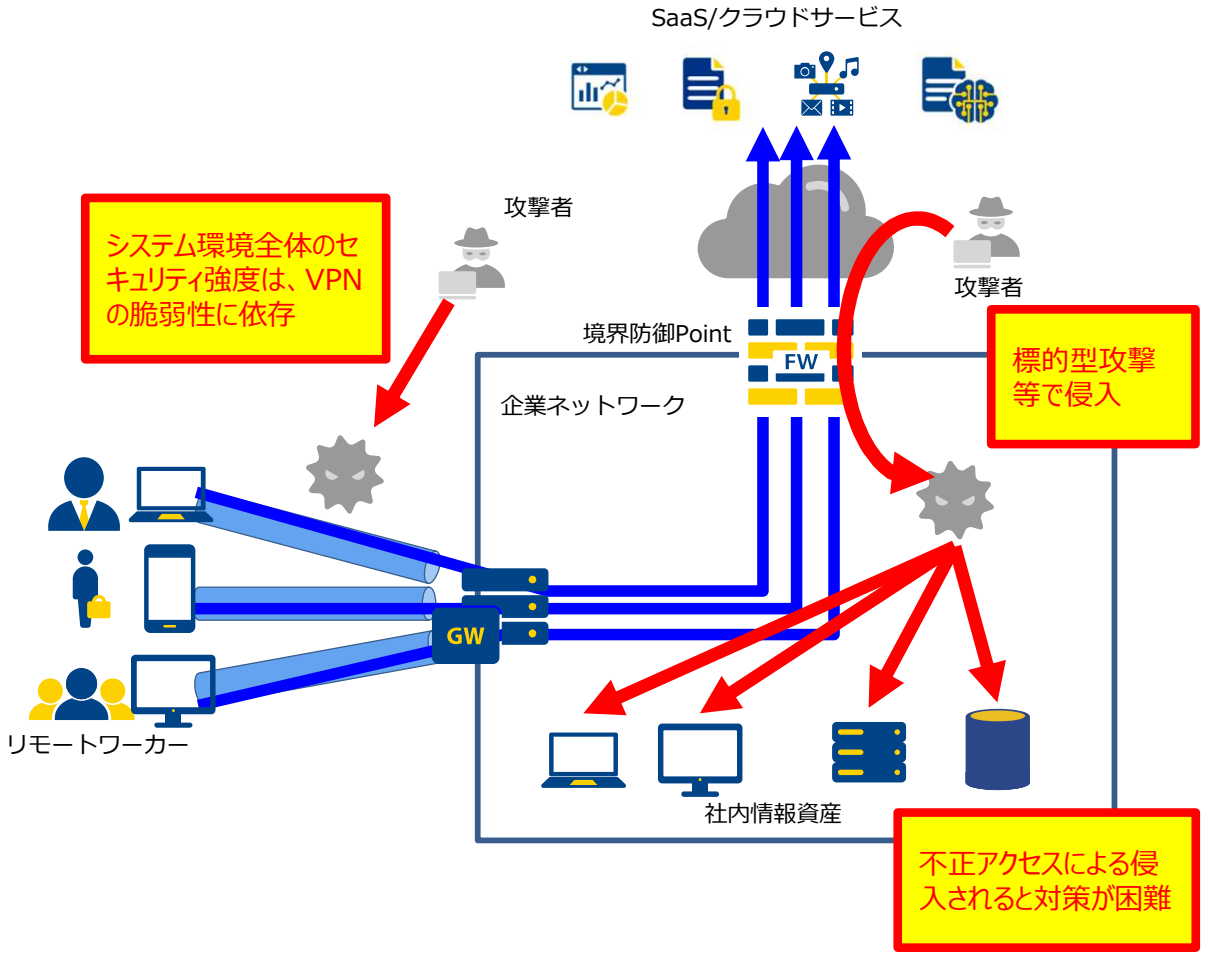
COVID-19禍により表面化した課題：②セキュリティ

■境界防御型セキュリティの限界

- クラウド活用、リモートワーク拡大で通信は企業ネットワークの外へ展開
- 境界防御が機能しない境界防御の内側に侵入後は対処困難

■DC集約型VPNの限界

- これまでは、VPNの閉域性によるアクセス制御でセキュリティレベルを担保。セキュリティ強度は、VPNの脆弱性に依存



7. コロナ禍における課題とニーズの分析

■コロナ禍における課題

1 セキュリティ

・社内LANへ安全に接続する環境を構築する必要がある。
・社用PC持ち運びにより、企業機密情報の漏洩リスクが高まる。

2 通信ネットワークのキャパシティ不足

・在宅勤務・リモートワークを推進することで、インターネットを経由して、社内LANへ接続するが、ネットワークのキャパシティ不足が発生している。
・リモート会議が主流となったが、音声の途切れなど利用者ネットワーク環境の影響を受けやすくなった。

■コロナ禍におけるニーズ

1 フレキシブルな就業環境

・在宅勤務やリモートワークが浸透し、各企業で、出社しなくても生産性を下げることなく、且つ、場所にとらわれない就業場所での勤務を推進している。

8. 要素技術調査の全体像

コロナ禍における課題とニーズの分析結果から「セキュリティ」及び「通信ネットワークのキャパシティ不足」が課題であることが分かりました。これらの課題に対応し、フレキシブルな就業環境を準備するため必要と思われるIT要素技術の調査を実施した。

■Level_1テーマ
【メインテーマ/命題】

コロナ禍の働き方・生活様式への適応に貢献するITインフラ技術

breakdown

■Level_2テーマ
【ビジネス要求】

コロナ | **働き方** | **生活様式** | **多様化** | **リモート**

在宅 | **生産性** | **セキュリティ** | **スピード** | **新ビジネス**

breakdown

■Level_3テーマ
【ソリューション要求】
【要素技術】

短期研究テーマ 選定領域

ゼロトラスト	**SASE**	**5G**	**認証認可(多要素認証)**
ローカルブレイクアウト	Docker	パブリッククラウド	コンテナ
CASB	**SWG**	Kubernetes	**EDR・NDR**
SDP	**リモートPC・VDI**	**BYOD**	**SD-WAN**	**MDM** ・・・

・・・ 短期研究テーマスプリントで調査した要素技術

・・・ 課題解決のために、特に必要と考える要素技術

8. 要素技術調査の全体像

■リモートPC(リモートデスクトップ)

普段、出勤時に使用しているオフィスに設置している会社PCのデスクトップ環境を、自宅等のリモートワーク環境の端末からインターネット経由で接続し、会社PCのデスクトップ画面を遠隔操作する仕組み。

画面転送のみを行うため、接続元のリモートワーク環境の端末は、低スペックでも構わない。

社員へ支給しているPCやBYODでの利用も可能であり、仮想デスクトップ方式(VDI)のように専用の基盤や環境を準備する必要もないため、比較的、容易に導入が可能。

また、普段、オフィスで使用している会社PCと同じ環境(画面)で操作・利用できるので、生産性を下げることなく、リモートPCを利用するための研修も不要。

リモートワーク環境で作成したデータや資料等は、オフィス側の会社PCの環境で保存されるため、リモートワーク環境の端末にデータを残さない。

ただし、会社PCとの接続は、インターネット回線で行うため、十分な回線速度の確保が必要。

8. 要素技術調査の全体像

■MDM(モバイルデバイス管理)

リモートワーク環境の端末として、BYODを使用する場合、情報漏洩に備えて、媒体をリモート操作できるMDMを採用するのが一般的である。

ただし、BYODの場合、私用領域まで管理してしまうため、プライバシー問題に考慮したMAM(モバイルアプリケーション管理)やMCM(モバイルコンテンツ管理)といった効率的なツールも出てきている。

＜MDMの主な機能は、次のとおり＞

主な機能	内容
リモートロック・リモートワイプ	端末の紛失・盗難が発生した場合、リモートで端末所在の確認、端末のロックを行う。遠隔操作でデータ消去も可能。※ただし、通信圏外では機能しない
アクセスコントロール	ウィルス対策やソフトウェアの脆弱性対応、許可されていないデバイス、ネットワークやアプリへの接続禁止など、企業のポリシーに合わせたデバイス管理を実現
ログ監視	外部接続とのログを取得。ネットワークを経由しないデータの持ち出し監視も可能。

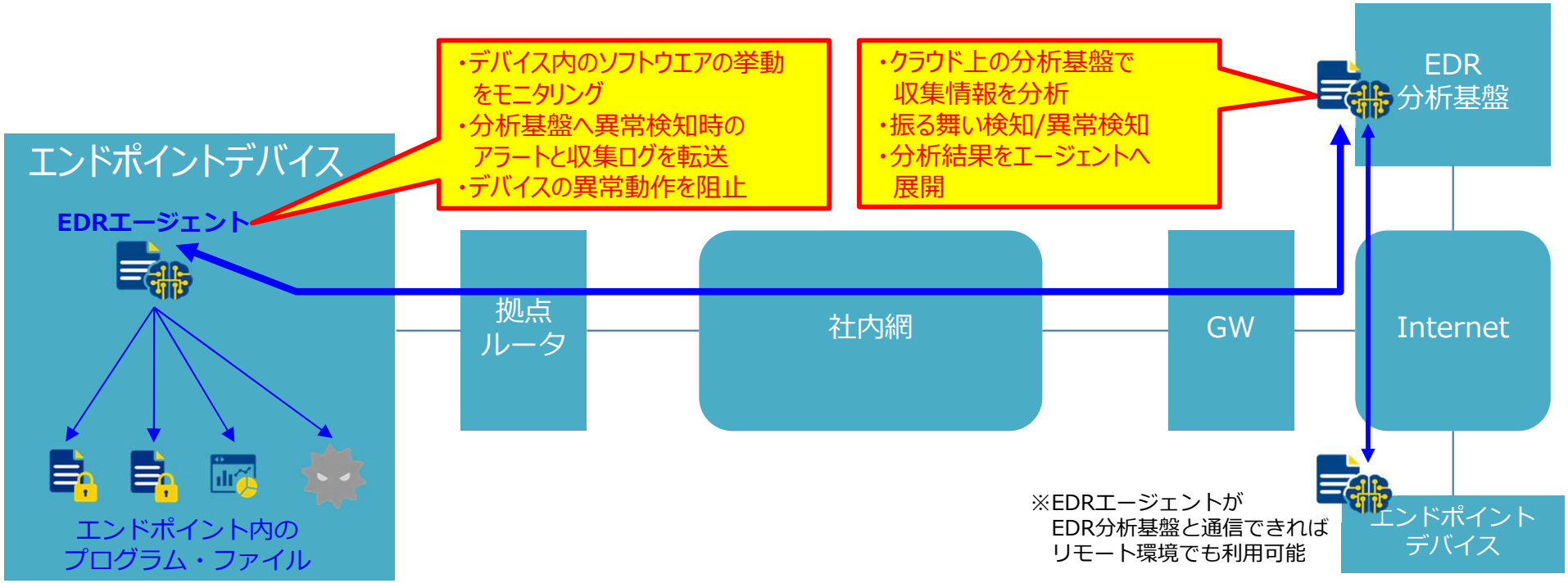
8. 要素技術調査の全体像

■EDR(Endpoint Detection and Response エンドポイントでの検出と対応)

最近のサイバー攻撃は、高度化・巧妙化しており、マルウェアの攻撃を境界防御の形で防ぐのは困難になっている。
万が一、マルウェアの侵入を許したとしても、即時に検知し、その脅威を除去する仕組みが必要。

EDRは、エンドポイント(リモートワークPCや会社PC等)上でマルウェア等の不審な動きがないか、常にエンドポイントの操作や動作を監視し、疑わしい挙動や痕跡があった場合、すぐに対処する。

つまり、EDRは、マルウェアの攻撃を防ぐことを目的としているのではなく、サイバー攻撃を受けることを前提に、初動対処のスムーズ化(マルウェアの検知や除去など)、被害の最小化を目的としたツール。



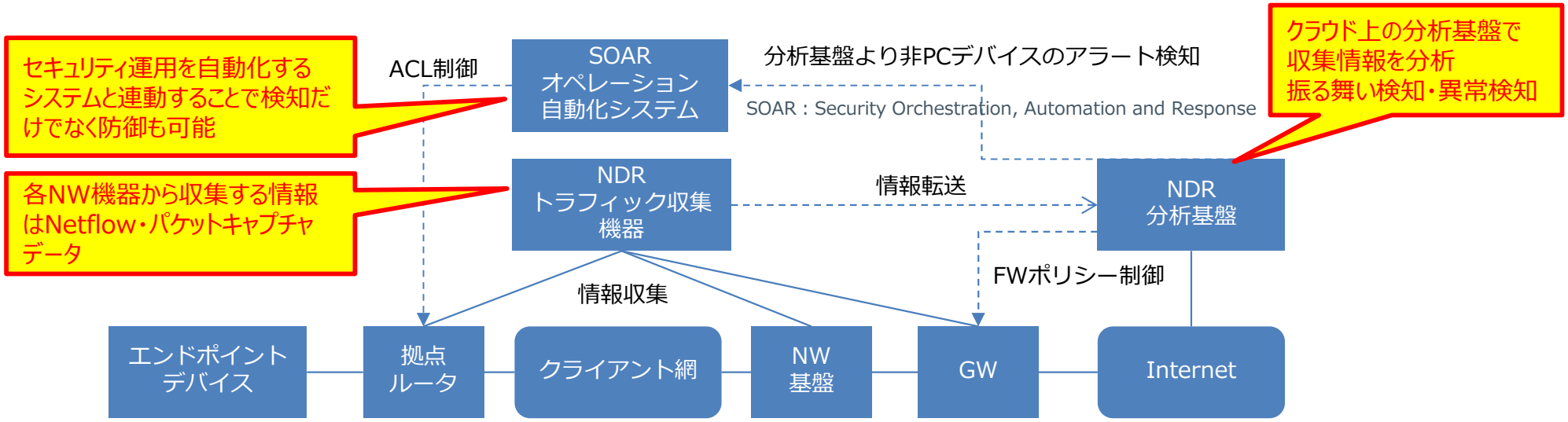
8. 要素技術調査の全体像

■NDR(Network Detection and Response ネットワークでの検出と対応)

近年、標的型攻撃等でマルウェアを侵入させた後のラテラルムーブメント攻撃で境界防御の内部で被害が発生する事例が一定数確認されている。

従来のDC集約型・境界防御型の企業ネットワークは、ネットワークの内部と外部の境界にセキュリティ機能を集約配置するモデルが主流である。このモデルは、セキュリティ脅威の侵入を前提として考えておらず、境界から内部に侵入された後のセキュリティ対策が困難という課題がある。

これに対し、NDRは企業ネットワークのトラフィックの流れに注目し、脅威の侵入が発生することを前提としたセキュリティ対策技術である。NDRは企業ネットワークのトラフィックを振る舞い検知の手法で収集・分析することで、脅威の侵入初期段階での発見、早期対処の実行を可能とする仕組み。EDRがエンドポイント【点】の対策であるのに対して、NDRは、EDRが動作する前段階、つまり侵入初期段階での検知・対策開始を目的としている。



8. 要素技術調査の全体像

■Cloud SWG(Cloud Secure Web Gateway)

外部へのアクセスをセキュアに行うためのプロキシ。従来は、社内PCからインターネット経由でWebアクセスを行う場合、プロキシサーバがHTTPS通信を中継したり、SSLの複合化、サイトのキャッシュ保存を行うなど、内・外を分ける働きをしていましたが、攻撃手法が多様化する中で、プロキシサーバでURLフィルタリングをするだけでは防御できなくなってきました。

そこで、プロキシに、セキュアな機能を追加したのが、SWGです。特に、Cloud SWGの場合、自社設備を保有する必要がないため短期間で導入でき、費用も低コストです。また、どこからでもアクセスできるため、リモートワークにも対応できます。

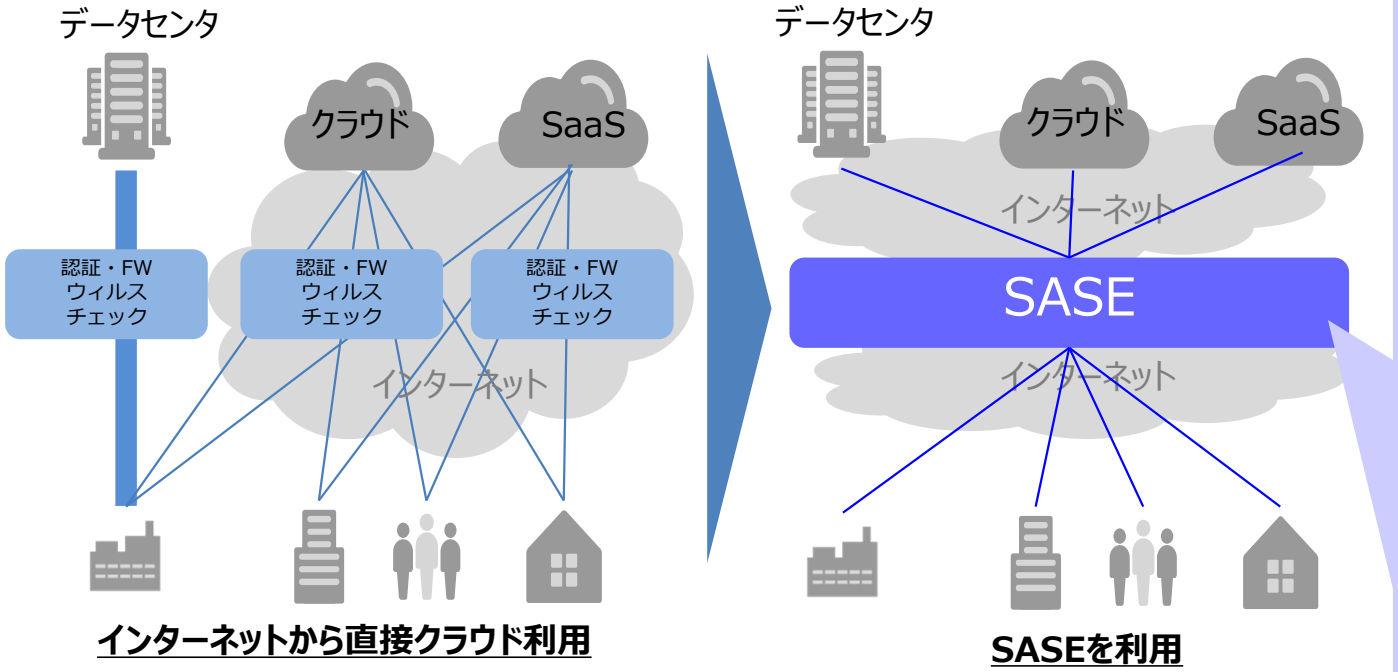
主な機能	内容
Web(URL)フィルタリング	企業ポリシーに則り、Webサイトの制限・禁止、カテゴリーでブロック
AP制御	企業ポリシーに則り、アプリケーションの制限・禁止、許可してないアプリのブロック
アンチウィルス	PC内に侵入するウィルスの検知・駆除
サンドボックス	コンピュータ上に仮想環境を構築し、マルウェアや不正プログラムを分析
SSL通信の監視	SSL通信を複合化して、リアルタイムで通信内容をチェック
DLP連携	DLP(Data Loss Prevention)連携。データそのものを監視、情報漏洩を防ぐ

8. 要素技術調査の全体像

■SASE(Secure Access Service Edge)

SWGは、SASEフレームワークのソリューションの一つ。SASEとは、クラウドサービスでネットワークとセキュリティ強化の機能を一括で提供するアーキテクチャ。全てのエンティティ(※)は、どこからでも必ずSASEのEdgeを経由して通信する仕組み。SASEフレームワークには、SWGの他に、SD-WAN、WAN Optimazation、CDN、CASB、ZTNA等がある。

※エンティティ：通信の主体…ユーザ、支社、本社、デバイス、アプリケーション…etc



ネットワークセキュリティをまとめて提供
(提供機能ラインナップはベンダにより様々)

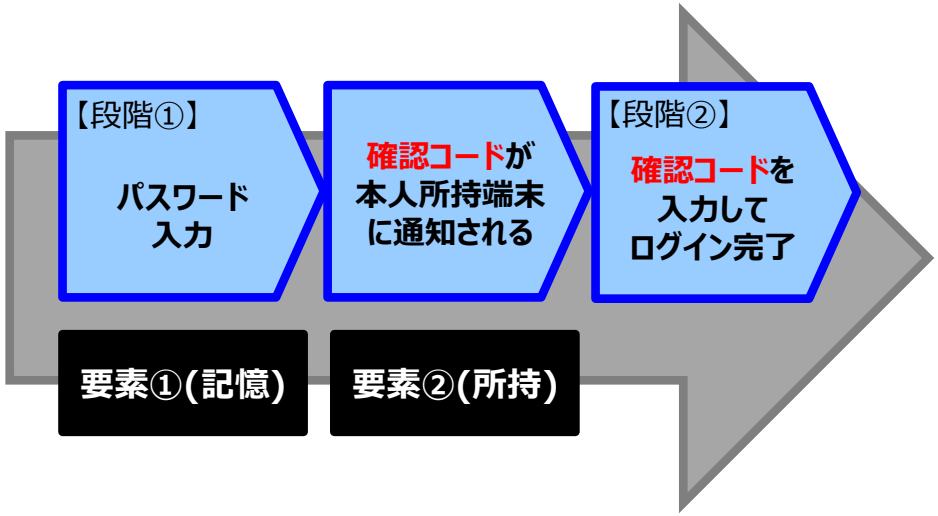
主な要素技術	概要
SD-WAN	ソフトウエア制御でInternet上に MPLS同等のVPN的通信経路を構築・提供
WAN Optimazation	WANトラヒック最適化 有線制御、遅延低減etc
CDN	コンテンツ配信ネットワーク
Cloud SWG	Cloud Secure Web Gateway Web通信の可視化、アクセス制御
CASB	Cloud Access Security Broker クラウドの利用状況の可視化、操作制御 セキュリティ機能を提供
ZTNA	Zero Trust Network Access ユーザアクセスポリシーを一元管理 ユーザ通信を毎回検証・認証するネットワーク
Threat Detection	脅威検知(IPS等) マルウェア検知 振る舞い検知(通常と違う異常行動etc)
FaaS	Firewall as a service クラウド上に実装されるFireWall機能

8. 要素技術調査の全体像

■多要素認証

Webサービスへのログイン時に、複数の要素(記憶・所持・生体情報)を用いて認証することを「多要素認証」と呼ぶ。
仮に、ID及び１つ目のパスワードを不正利用されても、次の認証で拒絶されるため、ログインできないことから、不正ログイン防止に効果がある。
同じ要素の認証を多段で実施する方法として、「多段階認証」もある。

【多要素認証の必要性】
スマートフォンの普及やインターネットサービスの拡大により、不正ログイン被害が多く発生している。
各種インターネットサービス(SNS、ショッピングサイト等)の多くは、
ID及びパスワードによる本人認証方式を採用している。
しかし、ID及びパスワードによる本人認証方式では、悪意のある
第三者にID及びパスワードを知られた場合、不正にログインされ、
個人情報漏洩や金銭被害に遭う恐れがある。



8. 要素技術調査の全体像

■５Ｇ(第5世代移動通信システム)

リモートワークにより、会社PCのリモートデスクトップ利用やオンライン会議などが多くなりましたが、現状、通信遅延によるストレスがあるのも事実です。5G環境が一般化することで、通信容量が大きくなり高速化するとともに、同時接続数も拡大しますので、リモートワークを行う上では、必要なインフラだと言えます。

1G	1980年代、アナログ携帯電話
2G	1990年代、アナログ→デジタルに移行 インターネット開始
3G	2000年代、モバイル機器でのインターネットが一般化
4G	2010年代、LTEとスマートフォンの台頭で利便性向上

5G (5th Generation)

- ■ 高速で大容量の通信
- ■ 高信頼性で低遅延な通信
- ■ 多数のデバイスと同時接続可

＜4Gと5Gの違い＞

項目	4G	5G	向上度合い
通信速度	1Gbps(最大)	20Gbps(最大)	20倍
同時接続機器数	10万デバイス/㎢	100万デバイス/㎢	10倍
遅延速度	10ms	1ms	1/10

8. 要素技術調査の全体像

＜5Gの2つの周波数＞

5Gは、**Sub6(3.6GHz～6GHz)**と**ミリ波(28GHz～300GHz)**の2種類の周波数値帯を利用します。

周波数は、高ければ高いほど「帯域幅」が広くなり、データ通信がスムーズになります。「Sub6」は4Gと周波数値が近いため、通信速度においては「ミリ波」に大きく劣ります。

※4Gは、3.6GHz未満の周波数帯です。

そのため、4Gの時より早くなるけれども、それほど速度向上は見込めません。では、どうして5Gには2つの周波数帯があるかというと、「Sub6」「ミリ波」どちらもメリットとデメリットがあり、それを補いあうために2つの周波数を用意しています。

項目	Sub6	ミリ波
通信速度	大きくミリ波に劣る	**超高速通信**
同時接続機器数	大きくミリ波に劣る	**多数同時接続可能**
遅延速度	大きくミリ波に劣る	**超低遅延**
電波の届く範囲	**電波の届く範囲が広い** **障害物の影響を受けにくい**	電波の届く範囲が狭い 障害物の影響を受けやすい
設備の普及	4G技術の転用ができるので、**設備の普及が早い**	設備の普及には、時間がかかる

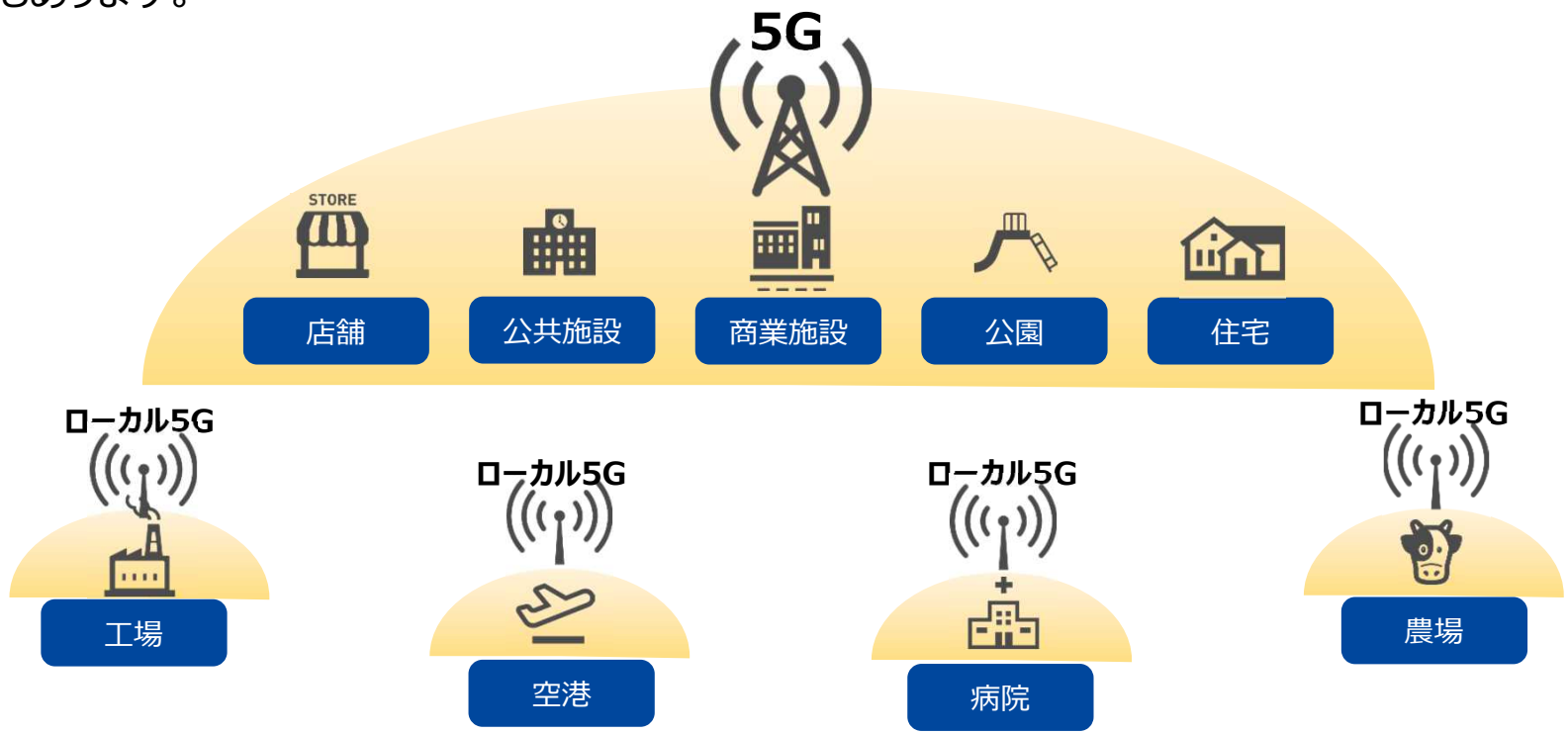
8. 要素技術調査の全体像

＜ローカル5Gとは？＞

5Gは、2020年3月に大手キャリアによるサービスが開始されました。しかし、キャリアによる5Gの環境が全国的に整備されるのは、1年半から2年後と言われており、現状、整備が十分に進んでおらず、利用できるエリアも限定的です。

そこで、5Gを局地的にプライベート利用する**「ローカル5G」**という仕組みがあります。

限られたエリアで利用する条件で、免許制による5Gを利用します。自己の建物や土地の敷地内で利用できますので、例えば、工場、空港、病院などでの利用が考えられます。Wi-Fiよりも広範囲をカバーできるので、Wi-Fiの代わりに導入する動きもあります。



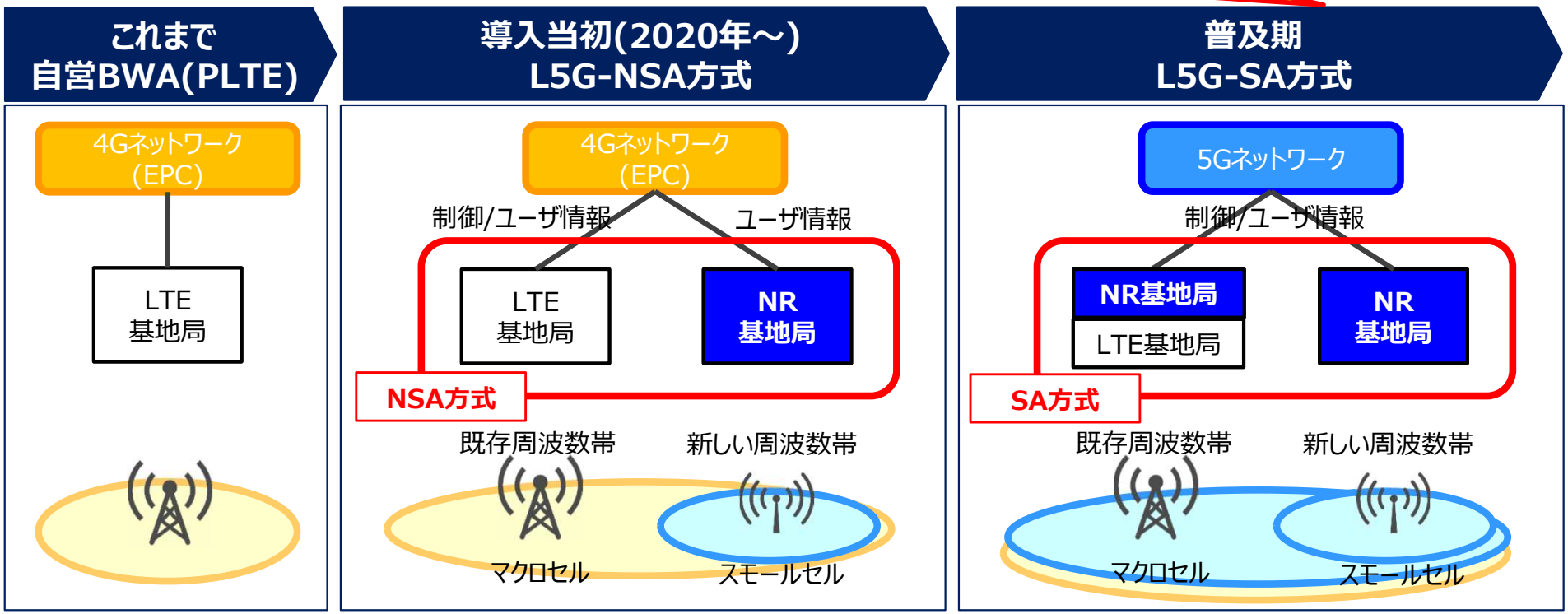
8. 要素技術調査の全体像

＜5Gの方式＞

5Gには、NSA(Non Standalone)方式とSA(Standalone)方式がある。

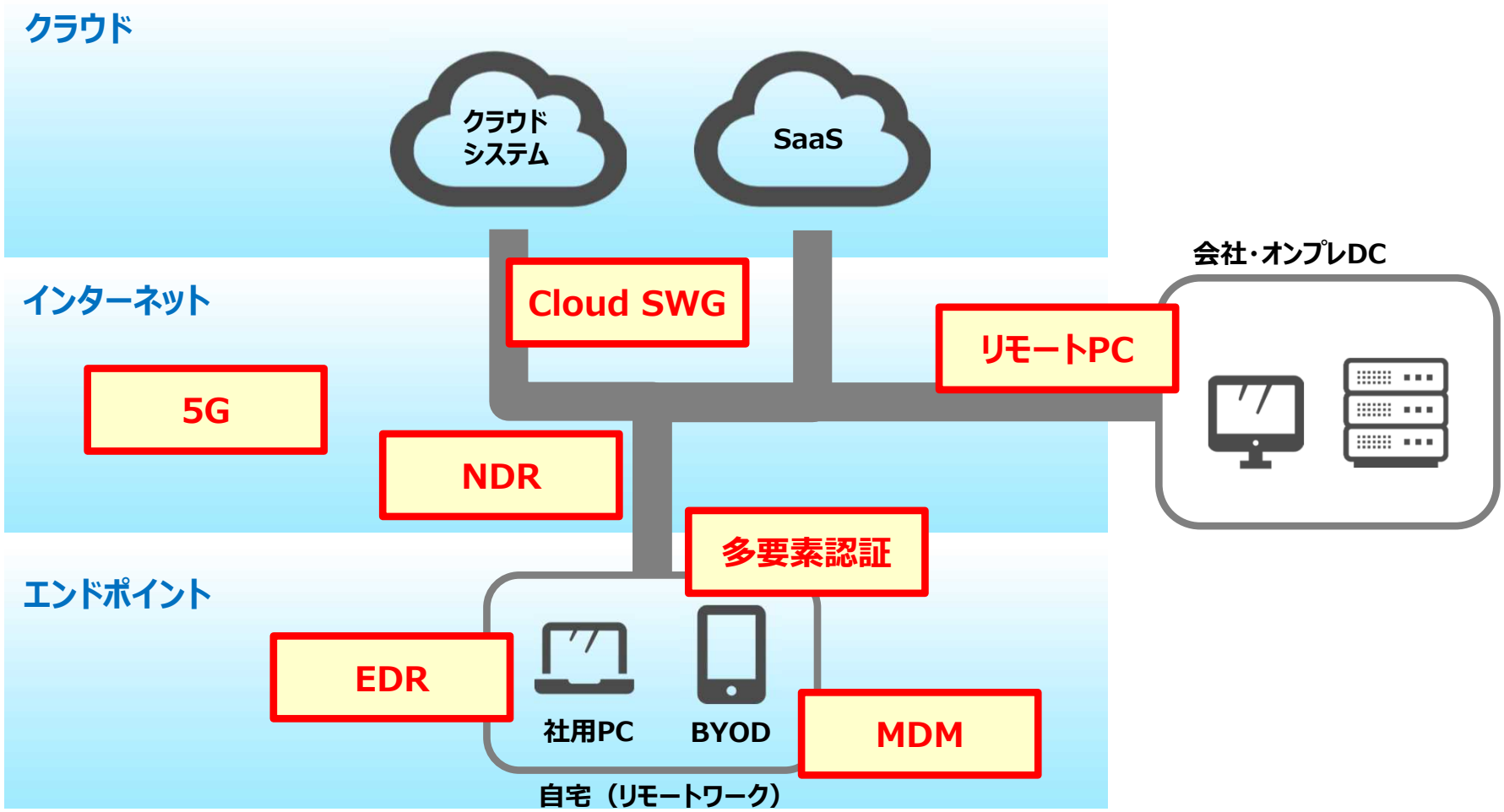
5Gの導入当初は、コストを抑えつつ、円滑に導入を進めるため需要の高いエリアを中心に、NR(New Radio)基地局とLTE基地局が連携したNSA方式のみ。4G(LTE)との差は「高速通信:20Gbps」程度。
低遅延や同時接続機器数(100万デバイス/㎢)といった性能向上が見込めるのは、SA方式からである。

ローカル5Gは、2021年度に、工場等、特定エリアで普及の兆しがあるが、一般企業での活用が期待されるキャリア5G(SA方式)は、2023年頃まで待つ必要がある



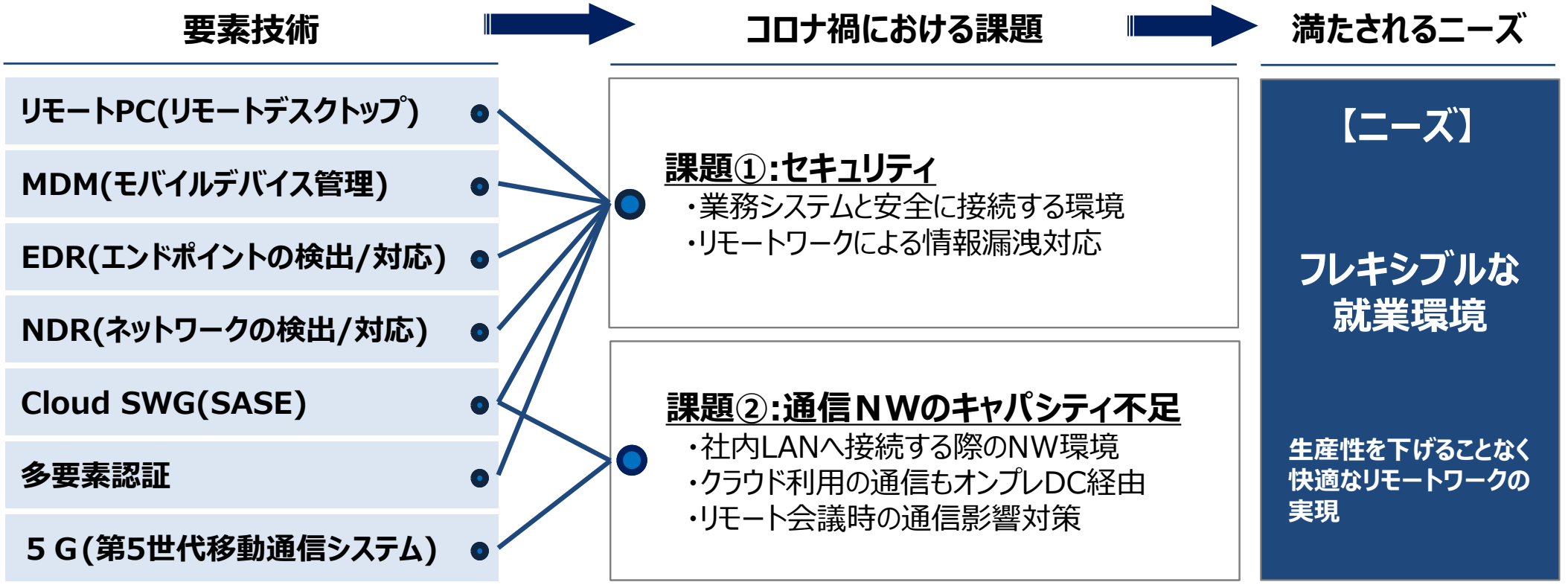
9. 要素技術調査の結果考察

生産性を下げることなく、フレキシブルな働き方を実現するための快適なリモートワーク環境を準備するためには、**エンドポイントと業務システムへのアクセス部分のセキュリティ強化**及び**快適なネットワーク環境**といった「ITインフラ技術」が必要と考える。



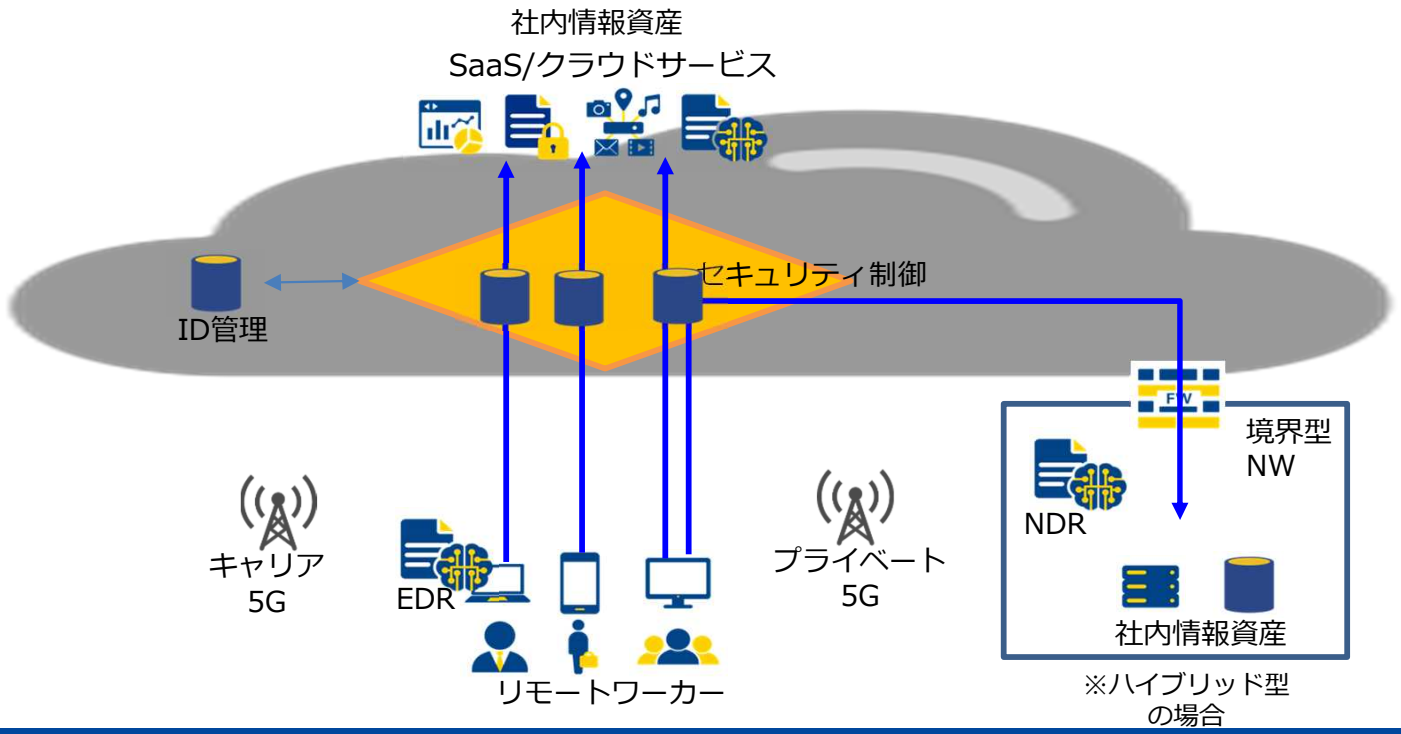
10. 課題・ニーズに応える要素技術とソリューションの考察

外部から社内システムに安全に接続するためには、リモートPCやSWGといった利便性とセキュリティ強化を考慮したツールの導入が必要。また、システムのクラウド化及び侵入経路の多様化に対応するためには、従来の境界型防御ではなく、ゼロトラストを含めたSASEフレームワークの適用を検討。NWの強化にあたっては、今後の5Gの普及に期待したい。



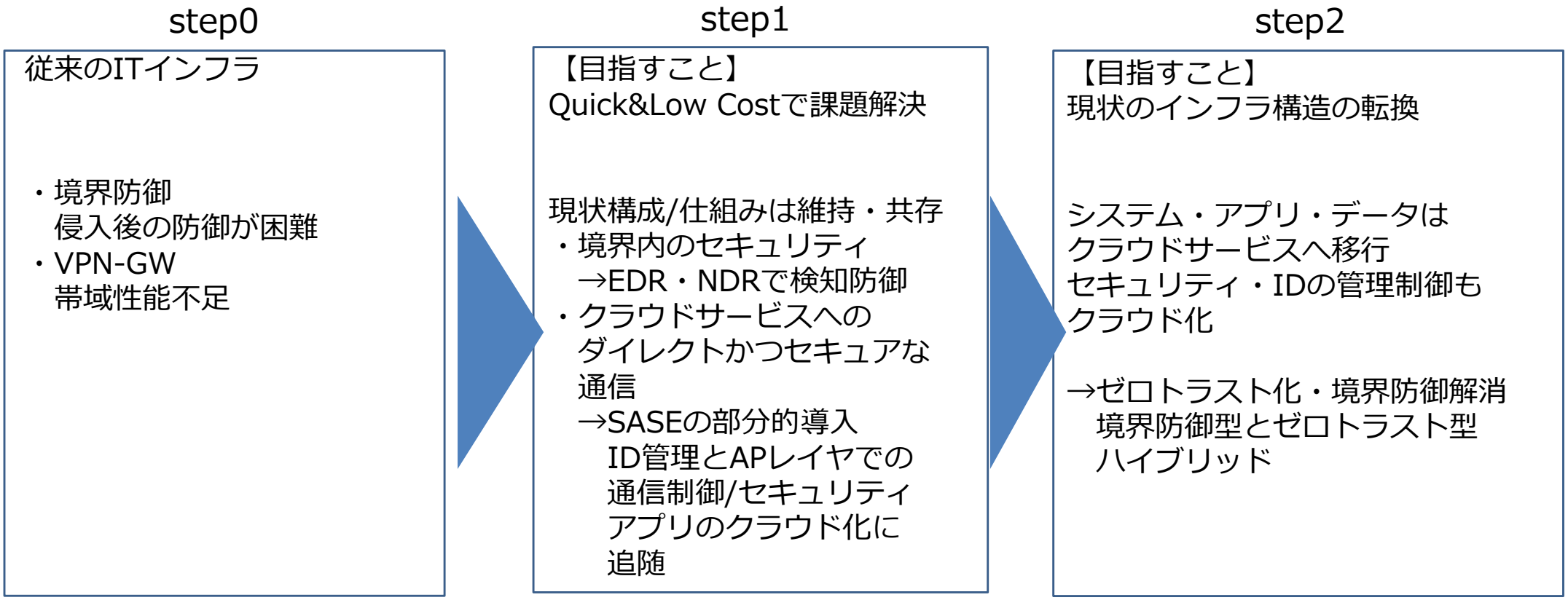
10. 課題・ニーズに応える要素技術とソリューションの考察
理想的アーキテクチャ

・ITインフラのゼロトラスト化
　アクセス環境：5Gによる快適かつ場所を選ばないネットワークアクセス(広帯域・低遅延・多重接続)
　アクセス制御：ID・ビジネスロール・APレイヤでの管理・制御をクラウド基盤上のサービスで適用
　セキュリティ：シグニチャパターンからユーザの行動分析・権限・振る舞い検知等の多重条件検証に移行
・システム・アプリ・データはクラウドサービスへ移行
　セキュリティ・IDの管理制御もクラウド化へ進む
　→ゼロトラスト化による境界防御解消、または境界防御型とゼロトラスト型のハイブリッド形態



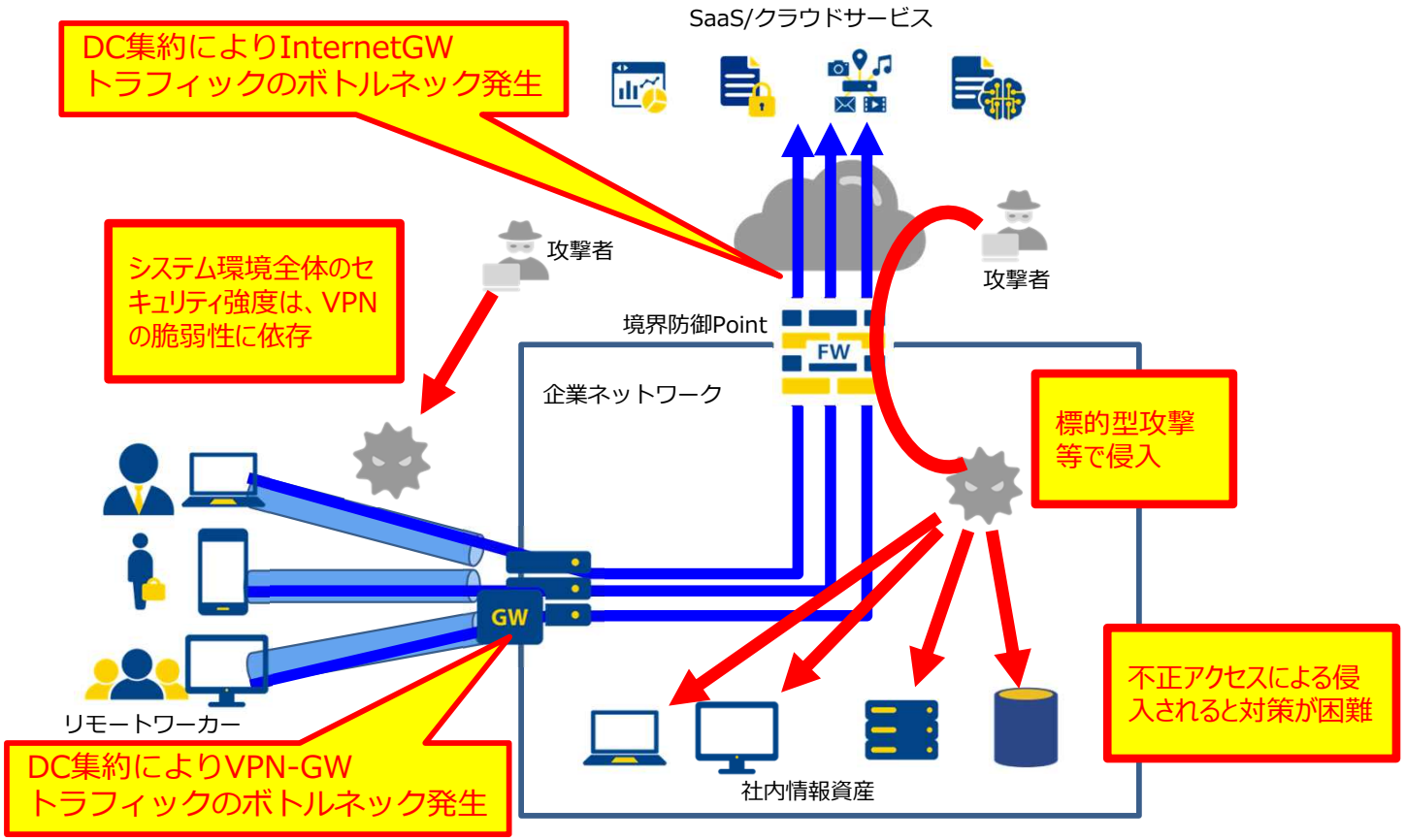
11. 理想的アーキテクチャに至るアプローチ

・コロナ禍での働き方改革を企業が推進するためには、タイムリーな状況適応とITインフラの構造転換が必要。この2点を両立させるには、段階的なstepを経て従来のあり方を変えていく必要がある



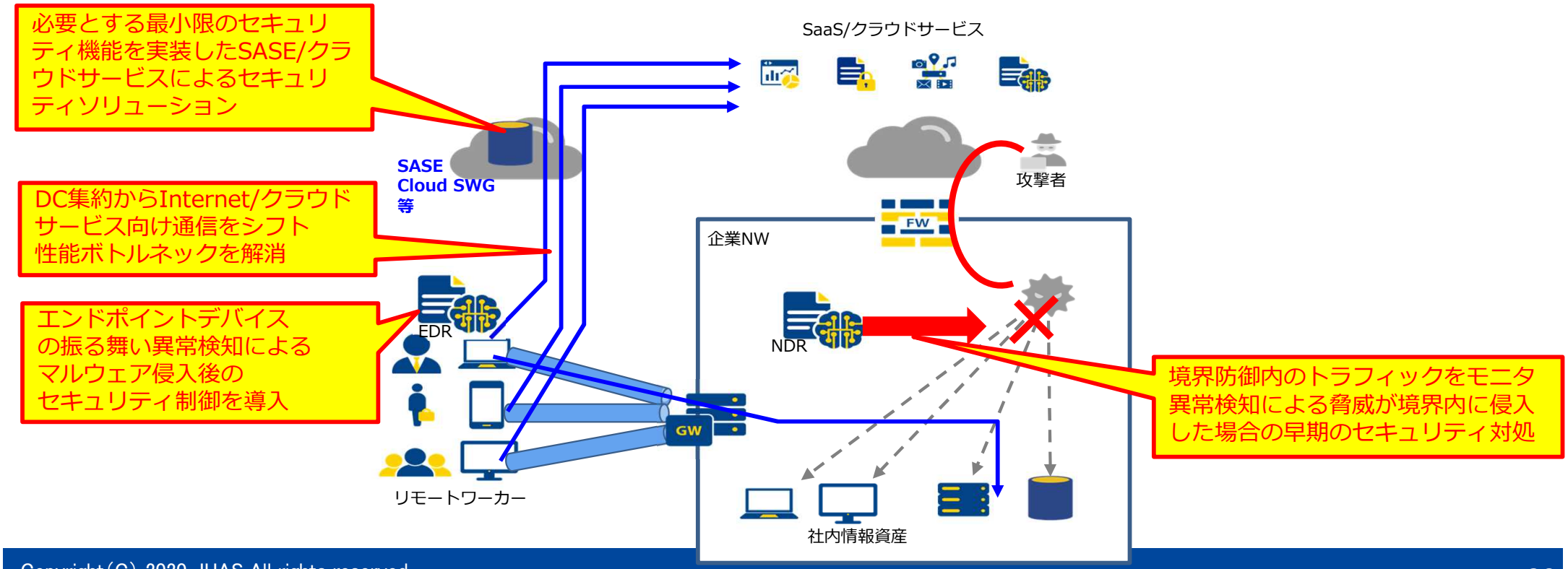
11. 理想的アーキテクチャに至るアプローチ
step0 従来のITインフラ

・境界防御型のセキュリティ課題
・DC集約型VPNの性能課題
→この2つの課題を解決することで快適なリモートワーク環境を整備する
　既存の環境を大きく変更するのは、コストも時間もかかり、即応性に欠ける



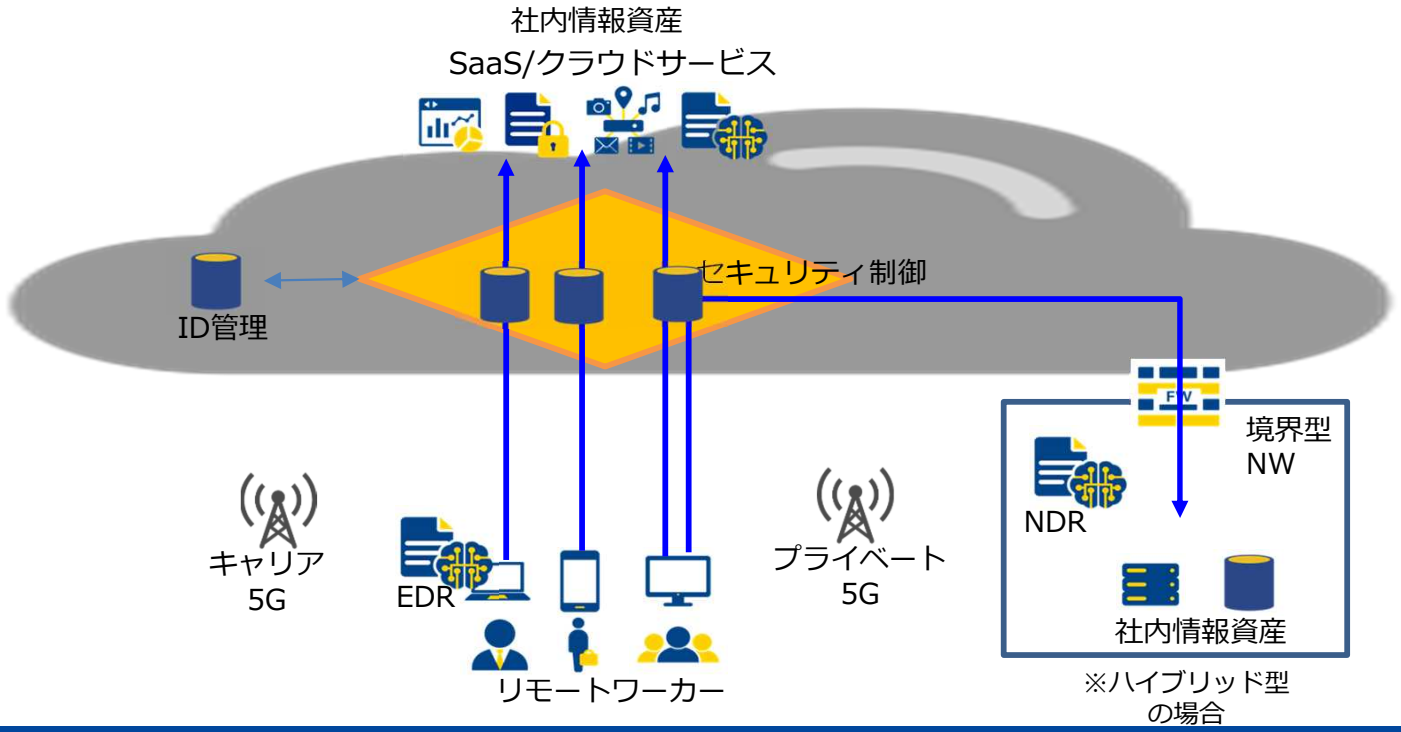
11. 理想的アーキテクチャに至るアプローチ
step1 Quick&Low Costでの課題解決

・コロナ禍という世界全体に一律で影響を与える状況にタイムリーに適応する
　→初期対応は時間とコストがかからない方法を採用する
　→現状のITインフラの構成、仕組みは継続維持できること、導入準備に時間がかからないこと
・クラウド上でサービス展開するSASEのソリューションを導入することでスピードを担保
・SASEの諸機能のうち、必要かつ最低限なものを選択することで最小限のコストで展開
　サービス利用型であれば、利用する規模・内容・期間に応じたサブスクリプション型課金
　サービスオプションでトラフィックログの監査・アラート検知等のセキュリティ運用自動化を組込み省力化
・パブリッククラウド上のサービスを利用するInternetトラフィックをDCから分離する事で性能問題を解消



11. 理想的アーキテクチャに至るアプローチ
step2 構造転換・ゼロトラスト化

・今後はシステム・アプリ・データはクラウドサービスへ移行　セキュリティ・IDの管理制御もクラウド化していく
・現状のインフラ構造の転換による根本的なITインフラの変更を、中長期計画で進める
- 境界防御型のインフラ形態から、徐々にシステム・アプリ・データをクラウド上へ移行
- システム・アプリ・データのクラウド移行とともに、アクセス環境の高度化を実装していく
-- クラウド型サービス適用
✓利用状況/利用量に合わせたコストで利用が可能　サービス切替/利用拡大時のリソース増減対応も容易
✓ID管理、IDに紐づくログ管理、システムとのAPI連携の仕組みを事前に構築　*SaaS等活用が最適
✓セキュリティ運用はクラウド型サービス適用により自動化・省人化が前提
→取扱う情報が動的かつ膨大なため人的オペレーションのみでは管理困難



12. コロナ禍における働き方への貢献
ITインフラが取り組むべきこと

・働き方の改革に寄与するITインフラを作るには、まずやるべきことは何か?
→各企業ごとに置かれている状況は異なっている。
これまでの研究活動を通して、**着手すべきPointを提言**する。

1.低コストで素早くリモートワークを実施できる環境の整備
- 現状のインフラ環境に変更を加えない
- クラウド型サービスを適用すれば、低コストでスモールスタートも可能

2.企業の状況・事業内容を分析し、導入すべきソリューションを絞る
- 多数あるSASEの機能の中から、必要な機能を選択して初期導入
- 業務アプリのユーザIFプロトコルはhttpに集約される傾向にあるため「Cloud SWG導入」が有力候補
  ただし事業内容や業界の慣習、法令等を考慮するとリモートワークやクラウド移行が最適解でないケースもある
  ex.工場、物流、建築、エッセンシャルワーク…etc ただしこれらの事業において、IT技術全般の適用自体にメリットが全くないというわけではない

3.クラウド型/ゼロトラスト型のセキュリティを同時に導入
- SASEソリューション+リモートアクセスに社員の利用をシフト、セキュリティ面でも安全・快適な環境を
- 導入の初期段階からID・役割に紐づく権限管理、ログ収集分析、それらと連動するアクセス制御の要件を整理
- 導入と並行して運用自動化による省力化を前提条件として組込む
  →APレイヤ、ID、振舞い分析等、取り扱う情報が動的かつ膨大なため人的オペレーションのみでは管理困難

補足：うまくいかないときは、スモールスタートで始めているので、すぐにやめて他のソリューションに切り替えられる

JUAS　ITインフラ研究会　チームB　メンバー

#	氏名	
1	近藤	リーダー
2	尾形	サブリーダー
3	荒木	
4	狩野	
5	菊地	
6	木島	
7	志田	
8	中島	（交代：竹内→中島）
9	野口	
10	沢井	幹事団・アドバイザー

敬称略

参加者の感想

自主的にITトレンドの調査を行え、参加メンバーと議論が行えたので、とてもためになる活動でした。参加してよかったと思っています。

各メンバ所属企業やコロナ下での対応も様々だったので、もっと時間を取っていろいろ議論したかったです。

メンバーの皆さまの考え方、システム環境などを知ることができたこと。また、熱心な対応を通じて大変良き環境で非常に有意義でありました。

リモートワークに関連した技術を多く学び、インフラに関する知見を広めることができた。

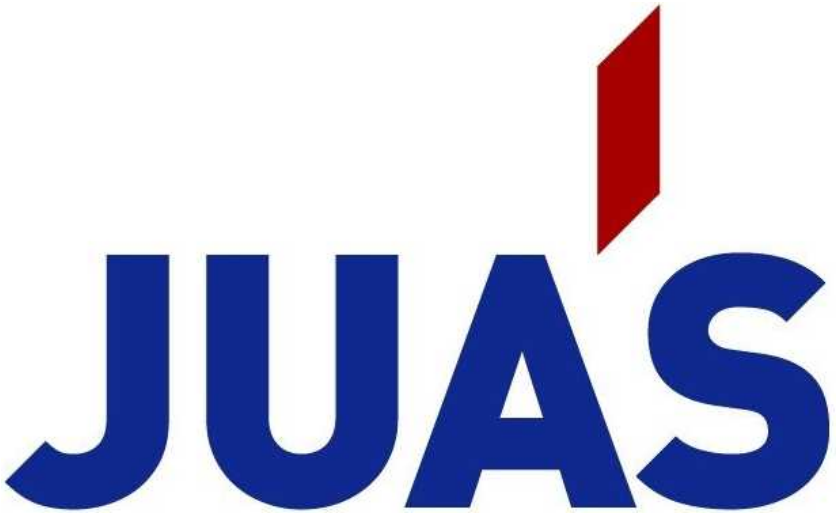
やはり対面で議論をしたかったのと、各社さんへの訪問の機会が無く残念でした。

他社のテレワーク状況が聞けて参考になりました。

短期研究スプリントをこなすことで、文字通り、短期間で多くの最新ITインフラ技術を調査・確認でき、非常に勉強になりました。

業務上ではこれほど技術に特化して調べることがなかったので、最新動向など知れて有意義でした。また皆さんから他社動向を聞けたことも意義のあることでした。

インフラという面での実務に今だ全然携われていない私には1つ1つの用語やツールですら勉強となりました。


JUAS