2021年度　ITインフラ研究会
分科会B　活動報告会資料

検討テーマ

1.現在の無線利用状況と最新無線通信技術の動向
2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
3.クラウドシフト時代における企業の状況と今後の課題

2022年4月

ITインフラ研究会　分科会B

目次

はじめに

- 分科会Bでは、「レガシー資産からの脱却および最新技術導入を阻害する要因と導入アプローチの調査」を共通の研究テーマの基に3つのサブ検討テーマを選定しました。
- 検討テーマごとでチーム分けを行い、研究を進めました。本活動報告書は3つの検討テーマごとに章立てされ、構成されています。

No.	テーマ名	テーマリーダ	メンバ
1	既存踏襲が引き起こす経済的な損失と脱却アプローチの研究	日本製鉄株式会社 山本 大貴	伊地知、竹内(健)
2	現在の無線利用状況と最新無線通信技術の動向	株式会社カジマアイシーティ 竹内(伸)	櫻井 三石、山本(泰)
3	クラウドシフト時代における企業の状況と今後の課題	エクシオグループ株式会社 髙橋　清	冨松、二宮、深谷 鷗野、瀧下

テーマ選定

■メンバ13名全員から「検討したいテーマ」と「検討したいテーマの背景」を発表いただき、その中から検討テーマを3つに絞りこみました。

事前調査

分科会

全部で24テーマ案

氏名	No.	検討テーマ	現状の問題点 ビジネス面	現状の問題点 システム面	問題が発生している 原因・背景	問題の結果として 発生していること・影響
櫻井	10	ゼロトラストとは言うけれど	リモートワーク・クラウド利用の拡大に伴い、クラウドリソースをセキュアに利用する必要があるが、基準やセキュリティ対策が追い付かず自由度が低い。	ゼロトラストとは何ぞやを分かりやすく説明できるシステムがない。		
櫻井	11	IoT／DXとは言うけれど（工場・プラントを持つ方と特に語り合いたい）	工場ではFA系（OT系）とネットワークが閉じた世界。FA系はルールが厳しくてIoTどころか接続ができない。古い社内分析基盤にデータを送れない。			
櫻井	12	リモートワーク時代のWAN（SD-WAN・海外接続含）	システム配置がクラウドにシフトしており、クラウドするためインターネット接続できれば良い。情報システム部門が投資すべきなのはWANか、インターネット接続点か？		恐らく各企業ではMS系のアップデートトラフィックやビデオ会議の利用でWANが逼迫している。	本来拠点トラフィックを分散させるために、ローカルブレイクアウトなどが主流だったがリモートワークでトラフィックが減った。そもそもwanにどこまで投資すべきなのか。クラウド接続がメインに変わっていないか。	回線費用の最適化が出来ていないように思う。インターネット接続点の混雑でTEAMS・BOXが遅いといった事に繋がりが。
櫻井	13	無線通信徹底研究（工場・プラントでは特に）	WiFi、PrivateLTE、ローカル5G、920Mhz無線通信など無線通信をビジネスで利活用が求められている		現時点ではWiFiがいいところ。無線通信の使い分けや導入ルールなど調査・研究が足りていない。	WiFiはチャンネル混雑で品質が劣化しがち。空港の近くでは、DSFの影響を受けたりしている。好き勝手WiFiと競合することもある。	WiFi通信の不安定さ

3テーマに絞込み

（検討テーマ以外ついても、研究会全体での「お悩み相談室」やアンケート実施の枠を活用）

活動方針

3つのサブ検討テーマごとにサブチームを編成し、各サブチームリーダ（テーマリーダ）ごとに並行して活動を進める。

チーム編成

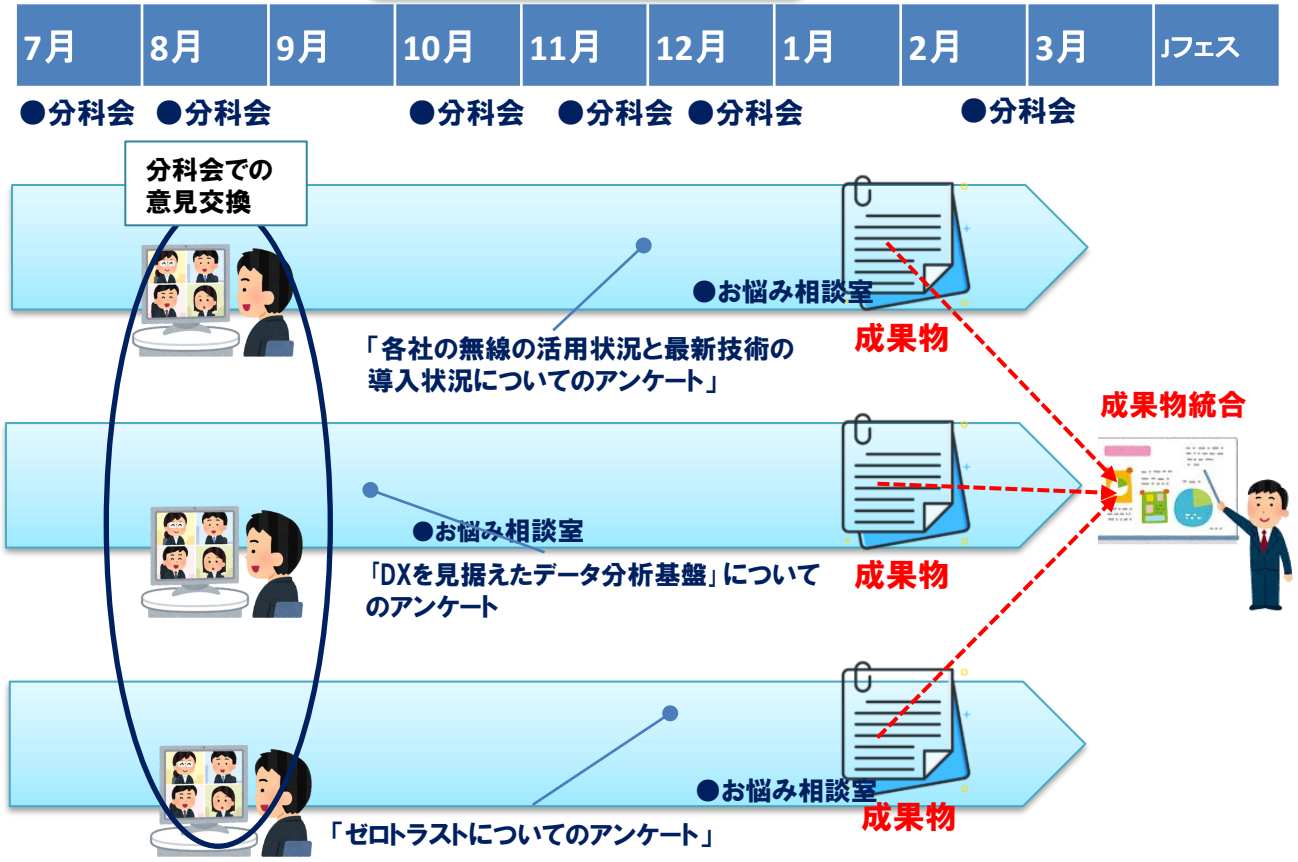
インフラ研究会チームB

リーダ メンバー 全4名
現在の無線利用状況と最新無線通信技術の動向

リーダ メンバー 全3名
既存踏襲が引き起こす経済的な損失と脱却アプローチの研究

リーダ メンバー 全6名
クラウドシフト時代における企業の状況と今後の課題

進め方



1：現在の無線利用状況と最新無線通信技術の動向

はじめに

無線LANは企業内のネットワークインフラを構成するにあたって基本となっており、有線LANに代わって広く普及している。新しい無線LAN規格(IEEE802.11＊)は数年おきにリリースされるが、オフィス内の利用など短距離の通信に用いられることが多く、広範囲に配置された機器の通信や屋外での利用などには不向きである。当たり前になってきた無線LANの利用である一方で、無線LANは目に見えない電波であるため、トラブルも複雑化してネットワーク管理者は現在も対応に苦慮している。

この研究テーマはインフラ管理者としての無線LANの障害事例と対策、無線LANの苦手としている広範囲の機器の通信、屋外利用などを各業界で無線技術の導入状況を交えて調査、研究したものです。

1.現在の無線利用状況と最新無線通信技術の動向
研究の要旨

- 各企業から聞いた現在の無線活用状況
  - 社内LANの環境は？
  - 無線の利用目的は？
  - 運用管理はどうしてる？
  - 社内規定はどうしてる？
  - 通信規格は？

- 近年の無線環境によくあるトラブル事例と対処方法はこれだ！
  - トラブル事例
  - トラブル解決策
  - ドーム型球場での高密度Wifi導入時の不具合

- 最新技術の動向
  - プライベートLTE
  - LPWA

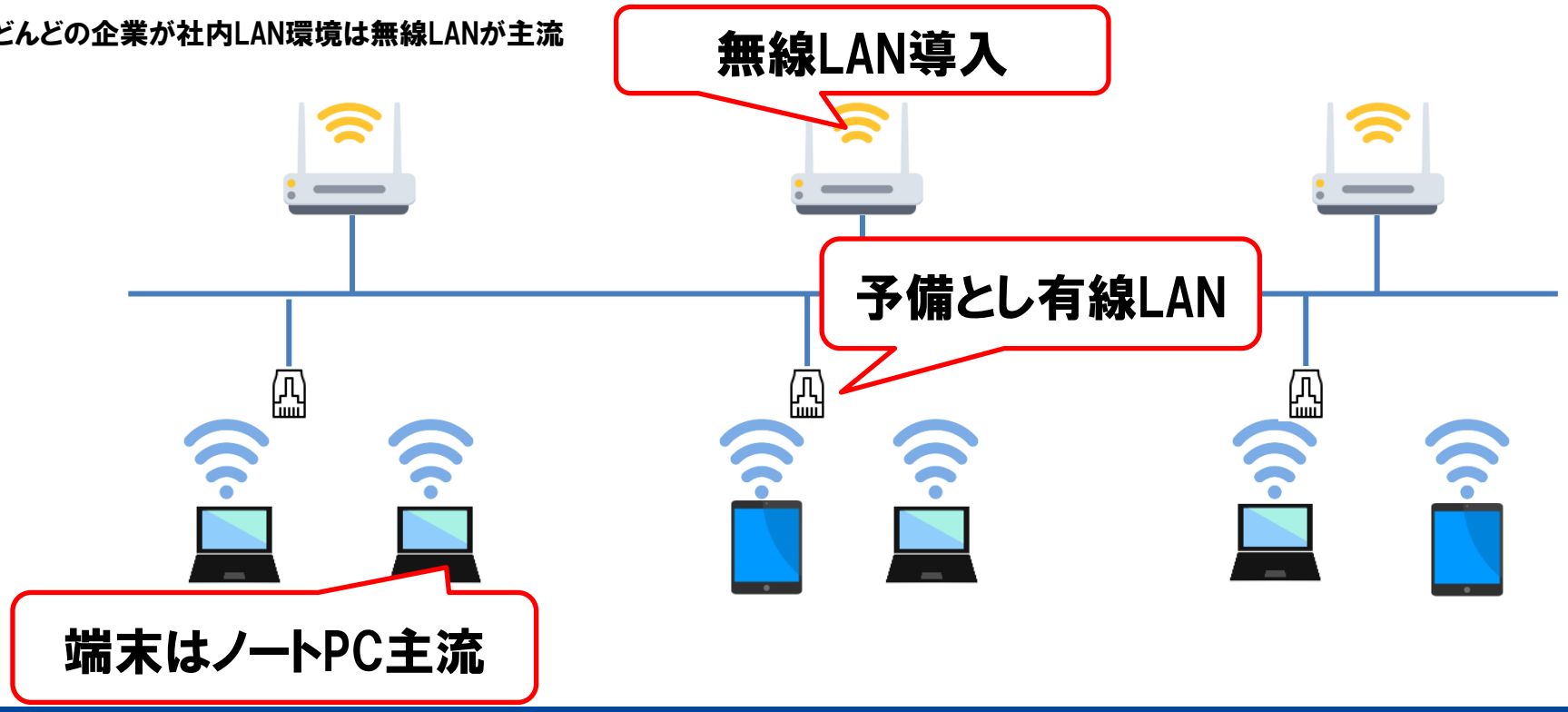
- 各社の無線の活用状況と最新技術の導入状況についてのアンケート調査
  - アンケート結果
  - アンケート結果考察

- ✓ 各企業から聞いた現在の無線活用状況
- ✓ 近年の無線環境によくあるトラブル事例と対処方法はこれだ！
- ✓ 最新技術の動向
- ✓ 無線の活用状況と最新技術の導入状況についてのアンケート調査

1.現在の無線利用状況と最新無線通信技術の動向
各企業から聞いた現在の無線活用状況

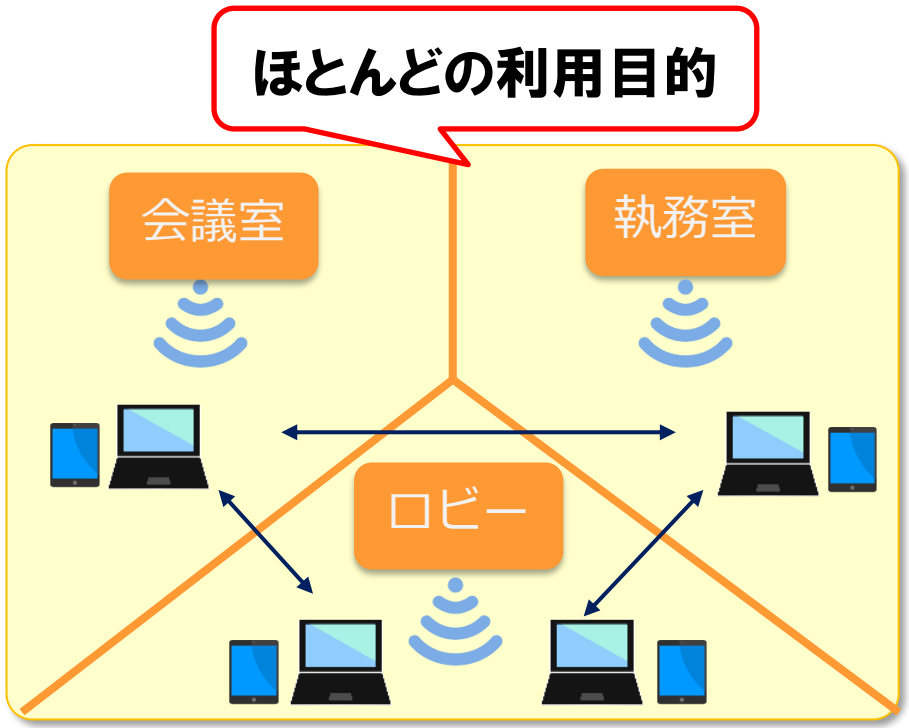
- 社内LANの環境は？
  - 9割以上の企業は無線LAN導入
  - 有線LANと併用、もしくは予備のために有線を一部配備
  - 社内の端末6～8割は無線LAN接続（ノートPC、タブレット）

●ほどんどの企業が社内LAN環境は無線LANが主流



1.現在の無線利用状況と最新無線通信技術の動向
各企業から聞いた現在の無線活用状況

- 利用目的は？
  - オフィスのモビリティ向上
  - IoTでの利用用途は事業に特化しているので少数（１割程度）

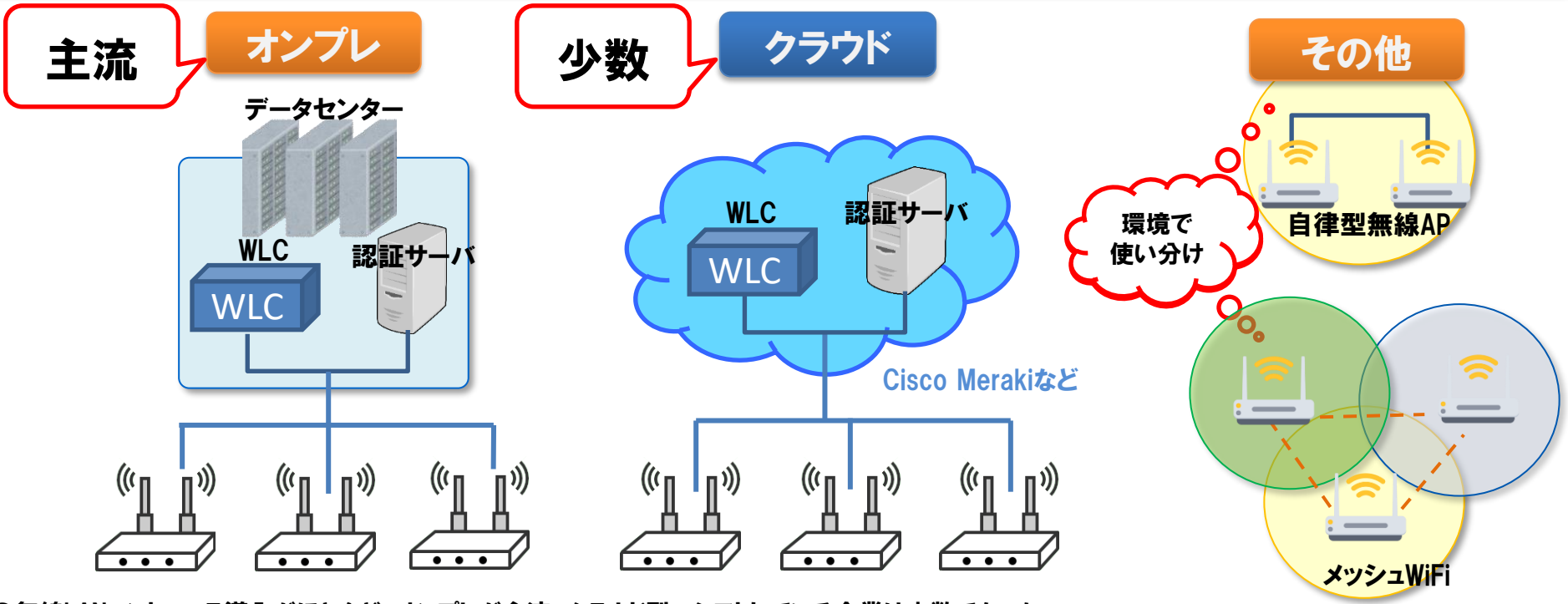


オフィス内のモビリティ向上

IoTでの活用

1.現在の無線利用状況と最新無線通信技術の動向
各企業から聞いた現在の無線活用状況

- 運用管理はどうしてる？
  - 無線LANコントローラ(オンプレ)が主流
  - 小規模拠点等では自律型で使い分け



●無線LANコントローラ導入がほとんど。オンプレが主流、クラウド型へシフトしている企業は少数であった。
クラウドのコントローラは各社セキュリティ上の都合で利用できなかったり、歴史も浅いことで柔軟な設定に対応できないこともある。今後もオンプレ型の主流は継続されるのではないかと考えられる。

1.現在の無線利用状況と最新無線通信技術の動向
各企業から聞いた現在の無線活用状況

- 社内規定（無線LAN利用規定）は？
  - 無線LANの利用に関する規定を設けている企業は少ない。
  - 少数だが無線AP設置やWiFiルータの持ち込み、利用を禁止の企業もある

●ポケットWiFiルータの持ち込み、テザリングの利用や利用部門独自での無線AP（野良AP）に関する社内規定を施行している企業は少ない。
規定がある企業は、利用部門独自での導入を禁止しているところが多いが、ポケットWiFiやテザリング利用の制限はない傾向にある。

1.現在の無線利用状況と最新無線通信技術の動向
各企業から聞いた現在の無線活用状況

- **利用している通信規格は？**
  - IEEE802.11acが主流。WiFi6の積極的な導入は見受けられない。
  - システム更改のタイミングでWiFi6導入に。

現在

- WiFi6導入への移行は検討
- 積極的な切り替えには至ってない

こないだ更改したばかり

端末が対応していないし。

IEEE802.11acで特に困ってない

これから

- テレワークの普及
- フリーアドレス化（無線）促進
- システム更改やオフィス移転等を機に高速化（WiFi6）

あくまで予感ですが。。。

- ✓ 各企業から聞いた現在の無線活用状況
- ✓ **近年の無線環境によくあるトラブル事例と対処方法はこれだ！**
- ✓ 最新技術の動向
- ✓ 無線の活用状況と最新技術の導入状況についてのアンケート調査

近年の無線環境によくあるトラブル事例と対処方法はこれだ！

■無線LAN導入（更改）時のトラブル事例

①現場からの「無線LANが遅い」という問い合わせ

- 単純に無線APの問題と断定できる例は少ない。複数の要因が考えられ、問題の切り分けが難しい。
- NWの運用を外部or子会社に委託している場合、サイトサーベイ等対応に時間がかかる

②リモートワーク増加に伴うリモートデスクトップ接続への対応

- VPN＋社内PCへリモートデスクトップの方式で運用。画面が途切れる等の問い合わせが多く寄せられた。
- 自宅NW、BYOD端末、VPNソフト、問題の切り分け確認箇所がただでさえ多い中、フロア内は全て無線LAN接続としていたため、自席PCまでの無線LANがボトルネックではないかと疑われた。

③無線LANの更改時における不具合対処

- 更改前と比べ、無線切断事象が多くなり、現場からの問い合わせが増えた。
- ログのエラーメッセージからだと、正常な切断とも区別がつきにくく、トラブルシューティングが難しい。

近年の無線環境によくあるトラブル事例と対処方法はこれだ！

■無線LAN導入（更改）時のトラブル対処方法

①現場からの「無線LANが遅い」という問い合わせ

・「そもそも無線は切れるもの」という認識を使用者に広める。
・電波干渉していないかという観点
ex.吹き抜けがあるフロアにて階をまたぐ移動をした結果、上の階のAPの電波を引きづっていた。（いわゆるスティッキー端末問題）
→端末自体の設定見直し、吹き抜けの柵に電波遮断シートを貼る等
ex.フロア内に多数のテザリングやモバイルルータ、野良APがあったため、無線APのチャネルと重複。
→フロア内でのテザリング、モバイルルータを使用禁止とした。
→切断等不具合が生じた際に逐一Excelシートに事象を記録していってもらい、情報収集した。

②リモートワーク増加に伴うリモートデスクトップ接続への対応

・オフィス内の有線LANを廃止し全面無線化をしたことがマイナスに働いてしまった。
→再度オフィス内に有線を引き直し、リモート接続は有線で行ってもらうことで、暫定解決。
→恒久対策としてクラウドの仮想デスクトップの導入を検討

・研究会内のアンケートでも半数以上が「各席あるいは各島に最低1本は有線LANを残している。」と回答。
→トラブル時の予備としてオフィス内の有線LANは一部残す運用とした。

③無線LANの更改時における不具合対処

・そもそもの原因のひとつが、デバイス起因の問題（証明書設定誤り）であった。
（無線LANシステムを更改したタイミングで発生していたため、機器に特化して調査継続。証明書有効期限等を見落としがち。）

近年の無線環境によくあるトラブル事例と対処方法はこれだ！

■ドーム型球場での高密度Wifi導入時の不具合
→複数の要因の切り分けに苦戦

＜原因（抜粋）＞

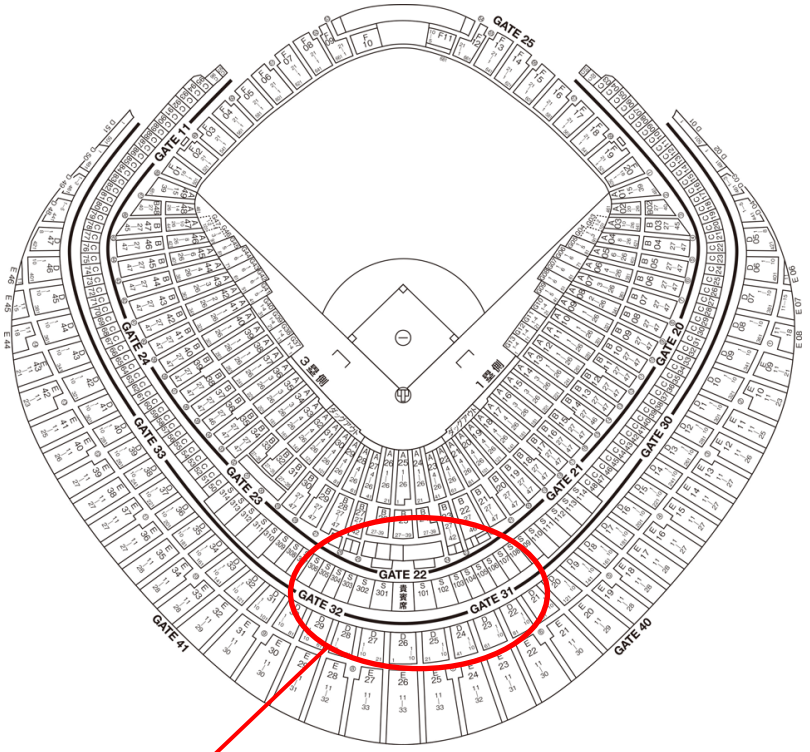
①特定の無線APに接続台数が集中
高密度Wifi導入に向けて無線APを数百台設置したが、人口が密集する22ゲート周辺で、至近ではない無線APに接続してしまう事象が多発

②特定のデバイスが接続することで検証が難航
デバイスが観客一人一人で異なることもあり、端末依存の問題も疑われる。（5GHz非対応端末もまだ多数存在しているのが現状）

③場内の他のWiFiによる干渉
テナントでPOS利用のためWiFiを利用している。
また、通信キャリアのフリーWiFiも各所設置されていることが判明

＜対応策＞

通信キャリアのフリーWiFiを停止し、さらに各APの個別チューニング（出力値や接続許可の閾値を高める等）により、サービスとして提供できるレベルまで改善。



https://www.tokyo-dome.co.jp/tourists/dome/seating-map.html

最も人が出入りし、客席も多いスポット
（バックネット裏でメインゲート、グッツなどの販売店も集中している箇所！）

- ✓ 各企業から聞いた現在の無線活用状況
- ✓ 近年の無線環境によくあるトラブル事例と対処方法はこれだ！
- ✓ **最新技術の動向**
- ✓ 無線の活用状況と最新技術の導入状況についてのアンケート調査

1.現在の無線利用状況と最新無線通信技術の動向
LPWA：Low Power Wide Area

■920MHz帯を利用したLPWA使い所とは？

１）長距離省電力

電源の無い場所でもボタン電池駆動型のセンサーなどから計測データを送信。
長距離伝送に適した無線技術。長距離伝送・省電力に割り切っており、送信データ量は極めて小さい。

２）920MHz帯は互換性が今一つ

WiFiの様な統一規格ではなく様々なサービスが乱立。用途に応じた無線システムの選択必要。
→2021年12月2日にWiFi Allianceより認証プログラムが発表された「IEEE802.11ah（WiFi HaLow）」も
注目したいが、日本国内ではまだ利用できないため様子見。（何年後？）

▼様々な種類のLPWAシステム

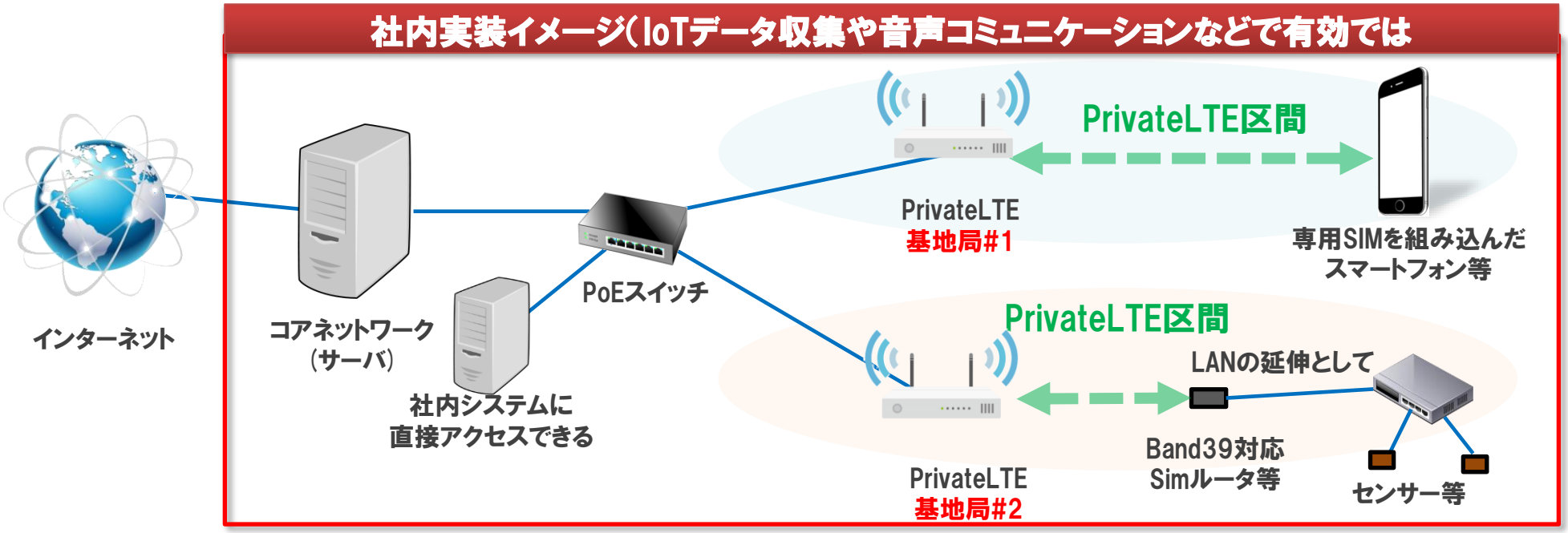
ライセンスバンド（非セルラー系）	アンライセンスバンド（非セルラー系）	アンライセンスバンド（非セルラー系マルチホップ型）
NB-IoT 基地局設置エリア内で150Kbps	LoRaWAN 最大15km で250～50kbps	UNISONet 500m～2kmで12～24kbps
LTE-CAT M1 基地局エリア内で1Mbps	Sigfox 最大50kmで100bps	Smart Hop 1kmで100kbps
	ELTRES 100km以上　上りのみ80bps	Wi-SUN FAN 1KMで50kbps～300kbps
	ZETA 2～10kmで100bps～50kbps	Smart Mesh 100mで250kbps

1.現在の無線利用状況と最新無線通信技術の動向
sXGP (Shared eXtended Global Platform) =PrivateLTE

■phs周波数帯を利用した免許不要のPrivateLTE日本標準規格

１)2020年12月に周波数が拡張され実用性アップ

- sXGPは廃止に向かう公衆PHSサービスやコードレス電話などが利用していた1.9GHz帯を利用し下り12Mbps程度／上り4Mbps程度の通信ができる。(キャリアの4Gのような速度は出ません！)
- 企業内にコアネットワーク・基地局など設置することで、PrivateLTE環境を構築できる。
- 通信距離は見通しで数百m。周波数帯的に電波の回折性などにも優れ到達性が高い。



1.現在の無線利用状況と最新無線通信技術の動向
sXGPで使えるデバイスがまだ少ない

■利用する周波数は1.9GHz（Band39）

１）Band39は中国ではChina Mobile／China Unicomなどで利用されており、
中国市場向けのスマートフォンなどはBand39に対応している。・・・が少ない！

２）LANの延伸としてSIMルータで受信し、その先にLAN機器をぶら下げたいが、
sXGPで利用できるsimルータが数えるほどしか無い。

■iPhoneでも使いたい＞今は無理！

sXGP（PrivateLTE）を利用する端末はBand39に対応している必要があり、
かつ日本の技適を取得している必要がある。
→iPhoneは上記基準をクリアしているのに、実際には使えない（動かない）
原因は、iPhone自身がsXGP用SIMのPLMN-ID＝44190をサーチしないため。
（Simfreeとかそういう話ではない。さん何とかしてください）

※PLMN:Public Mobile Network Identifierの略。モバイル事業者識別用ID
上位3桁が国番号で日本は440or441。sXGPは44190で固定。iPhoneでもサーチして。

- ✓ 各企業から聞いた現在の無線活用状況
- ✓ 近年の無線環境によくあるトラブル事例と対処方法はこれだ！
- ✓ 最新技術の動向
- ✓ **無線の活用状況と最新技術の導入状況についてのアンケート調査**

アンケート結果と考察

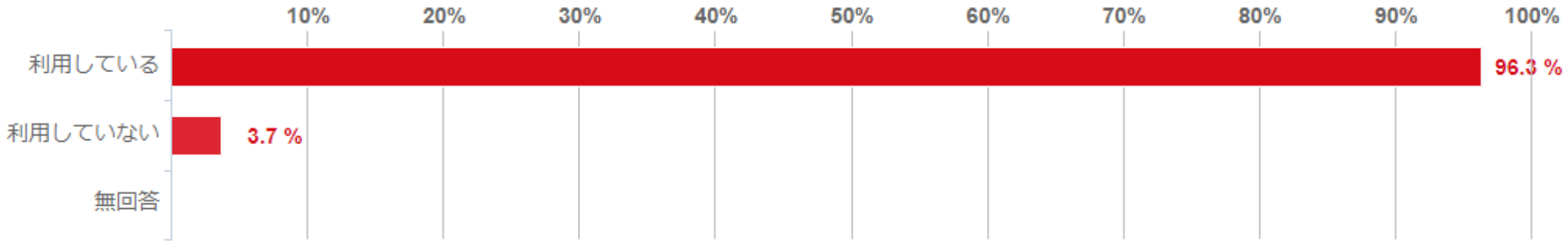
アンケート結果総評

- ほぼ全社で無線LANを利用しているがWiFi利用がほとんどであり、有線LANと比較した利便性を上げる意見が多かった。職場のフリーアドレス化やテレワークといった勤務場所の多様化にともない無線LANの利用が当たり前になっていると考える。
- 一方で、WiFi以外の無線LAN技術については、一部でIoT機器や屋外無線通信での利用を検討しているものの、それほど利用が進んでいない印象を受けた。しかしながら、今後コロナ禍や働き方の多様化にともない、IoTや屋外無線通信などの需要は高まると考えられる。回答では検討段階のものが多かったものの、今後は徐々に新無線技術を導入する会社は増えていくと思われる。
- そのほかアンケートでは各社の無線LAN運用状況についても質問した。有線LANと比べて障害切り分けが難しい、あるいは無線環境の運用ルールが曖昧であるといった回答が多かった。これには以下の二点が影響していると考えられる。
  - 働き方の多様化にともない個々人でモバイルルータを用意するなど無線LAN接続環境が多様化した
  - TeamsやSlackなど音声や動画によるリアルタイムのコミュニケーションが増えたことから、音声などの途切れなど無線通信に求められる通信品質が厳しくなってきた

アンケート結果と考察

■Q1　あなたの会社では無線LANを利用していますか。

（回答数: 27 ）



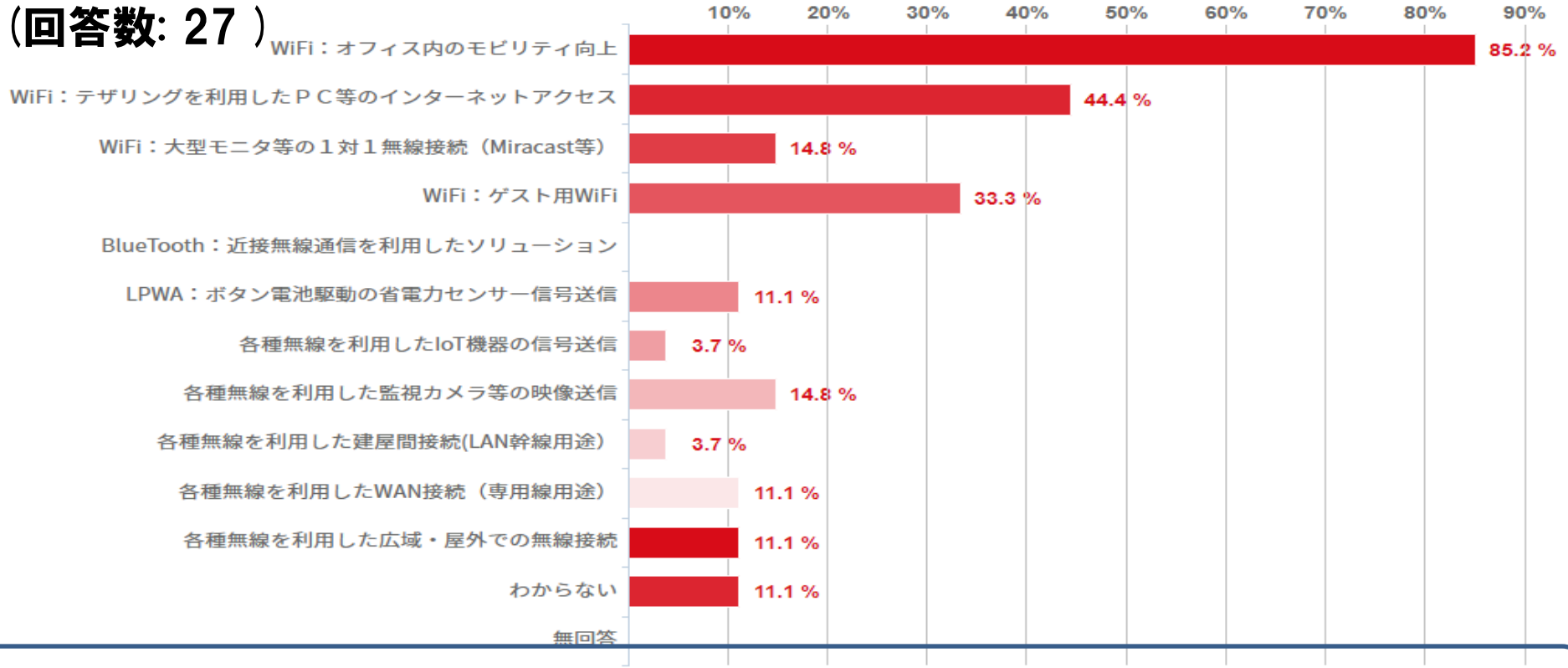
ほぼ全ての会社で無線LANを利用していると回答になった。

有線LANと同様に無線LANも社内ネットワークインフラの重要な要素となっている。

アンケート結果と考察

■Q2　無線通信全般を適用している業務領域は？（複数回答）

（回答数: 27 ）

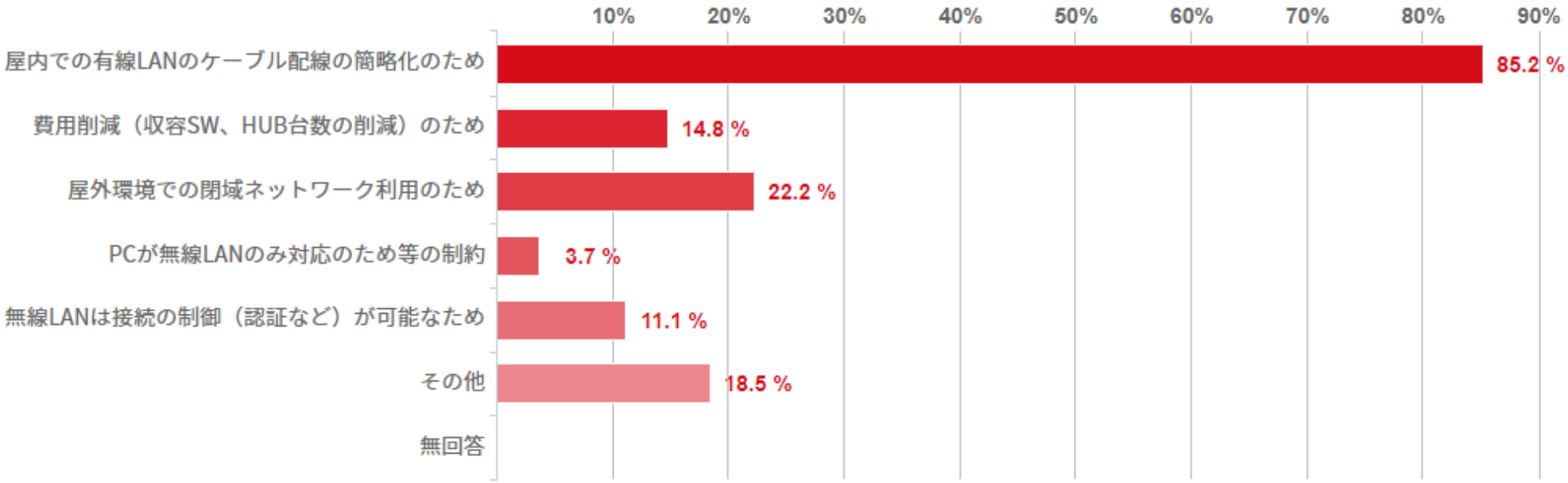


WiFi利用が最も多く、その用途もオフィス内のモビリティ向上といった業務環境の利便性に関する回答が多い。また、テザリングや、ゲスト用にWiFi利用しているケースも次いで多い。
その他にも、少数だがIoT機器や屋外利用など様々な用途での無線利用の回答があった。

アンケート結果と考察

■Q3　無線LAN導入の目的は何ですか？（複数回答）

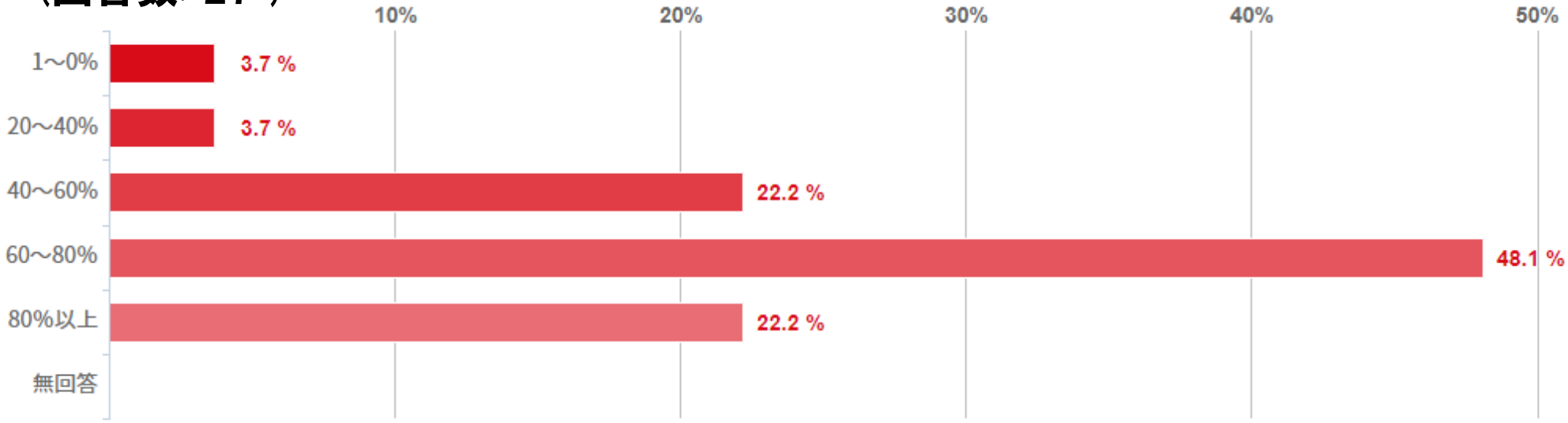
（回答数: 27 ）



無線LAN導入目的としては、屋内LAN配線の簡略化・屋外利用のためといった意見が多い。前問でWiFi利用によるモビリティ向上との回答でも多かったこととも関連する。有線LANと比較した無線LANのメリットを目的に利用している会社が多いと思われる。
その他では、PC利用上の制約やアクセス制御のため、無線LAN利用との回答もあった。

アンケート結果と考察

■Q4　全社の端末（個人配備端末、システム用端末）の中で、
無線LANで運用している端末の大まかな比率を教えてください。（選択）
（回答数: 27 ）

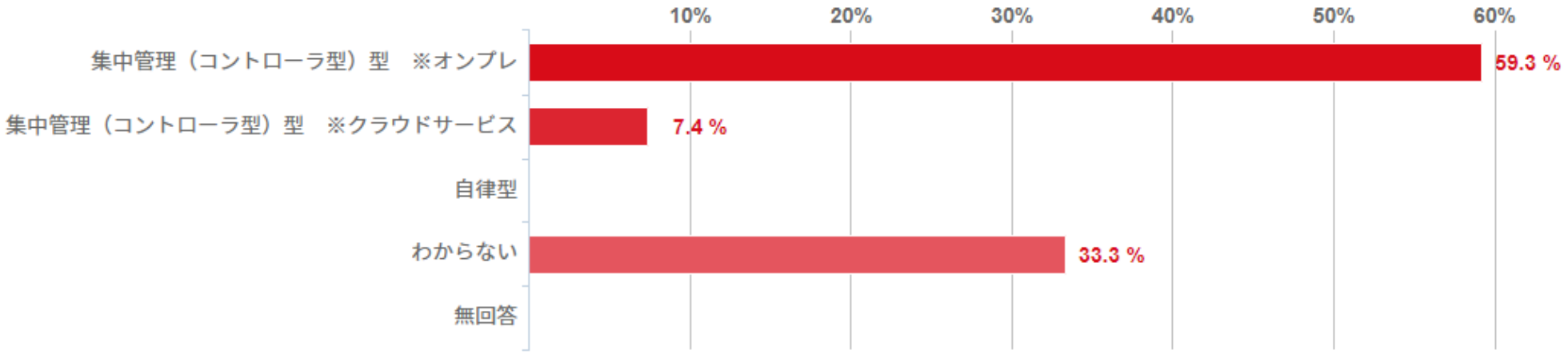


回答が半数近くが「60～80％で無線LAN利用」であり、またほぼ全ての会社で「40％以上の端末で無線LAN利用している」という状況になった。
前問までの回答を踏まえるとモビリティ向上のため、多くの社員PCで無線LANを使用しているものと思われる。また、80％以上が少ないことから、業務システムなど有線LANも併用しながらの運用だと思われる。

アンケート結果と考察

■Q5　導入している無線LANシステム(OA用)について教えてください。(選択)

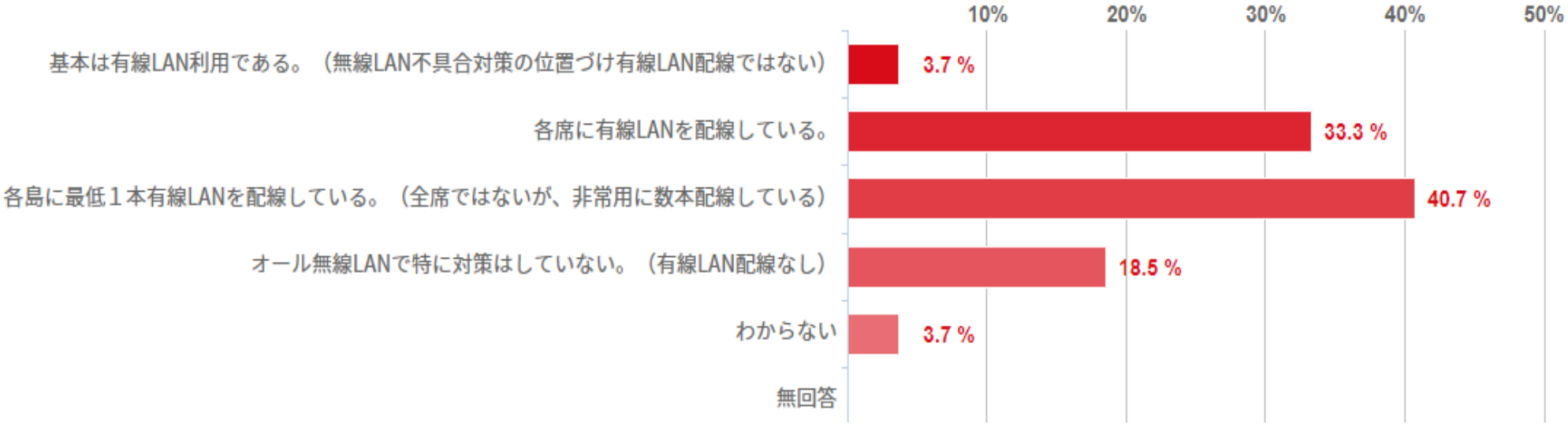
(回答数: 27)



WLC(無線LANコントローラ)による集中管理をしているかどうかの質問をしたところ、半数以上がオンプレ環境で集中管理と回答。クラウド型の集中管理もあるようだが利用数はまだ少ない模様。
また、自律型が0%だったが、「わからない」回答のうちいくらかは、社内無線LAN環境の規模によっては、自律型もあるのではと思われる。

アンケート結果と考察

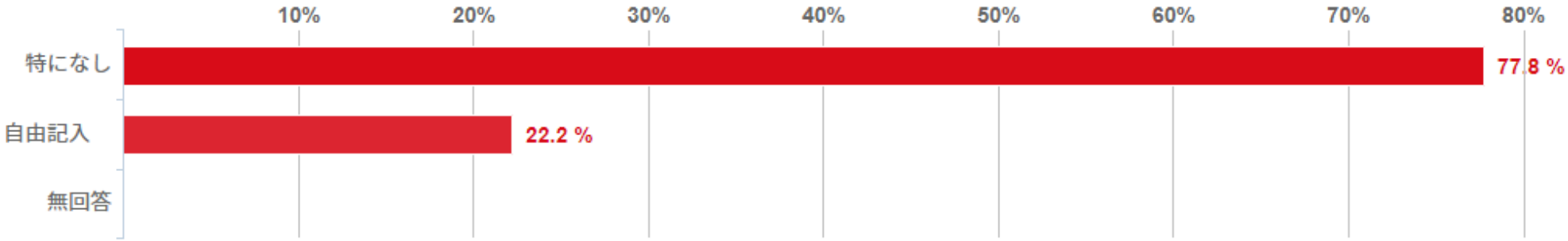
■Q6　無線LAN不具合時の対策として有線LANをどのように配線されておりますか。（選択）（回答数: 27 ）



最も多いのは各島に有線LANを用意、次に各席に有線LANを用意だった。両方を合わせると7割超えの回答となり、無線LAN利用を基本としているものの、不具合時を考慮して有線LANもある程度用意しているケースが多い。
一方で2割弱ではあるが、無線LANのみの利用で有線LANを用意しないという回答もあり、各社の運用方針の違いが出ていると言える。

アンケート結果と考察

■Q7　オフィス内へのモバイルルータ等の持ち込みによる電波干渉を防ぐために実施している対策(ポリシー、規則)はありますか。(選択)(回答数: 27)



自由記述回答

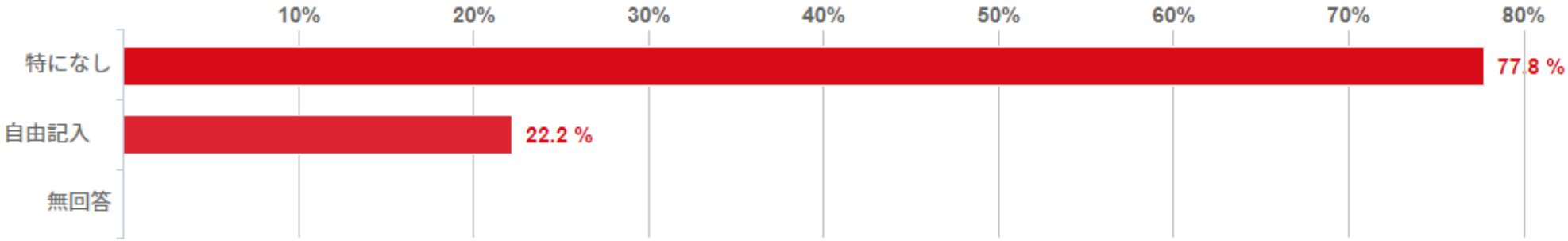
- オフィス内でのモバイルルーターの利用・部門で独自の無線LAN設置は禁止。テザリングは会社支給のiPhoneからのみ許可
- オフィス内の重要なフロアではモバイルルータ・テザリングの使用は原則禁止としている
- 社内ではIT部門から提供されている無線LANのみ利用可で、独自の無線AP設置は禁止されています。
- 各利用部門にて無線アクセスポイントを導入することは禁止している。(社内標準の無線システムを利用すること)
- 外部回線の利用は対象ルータ等の情報を申請・承認されたもののみ利用可能としている。
- オフィス内でのモバイルルータ・テザリングの使用は原則禁止としている

  各利用部門にて無線アクセスポイントを導入することは禁止している。(社内標準の無線システムを利用すること)

  Bluetoothのマウスなども禁止。(2.4GHzの無線と干渉するため)

アンケート結果と考察

■Q7　オフィス内へのモバイルルータ等の持ち込みによる電波干渉を防ぐために実施している対策(ポリシー、規則)はありますか。(選択)(回答数: 27)



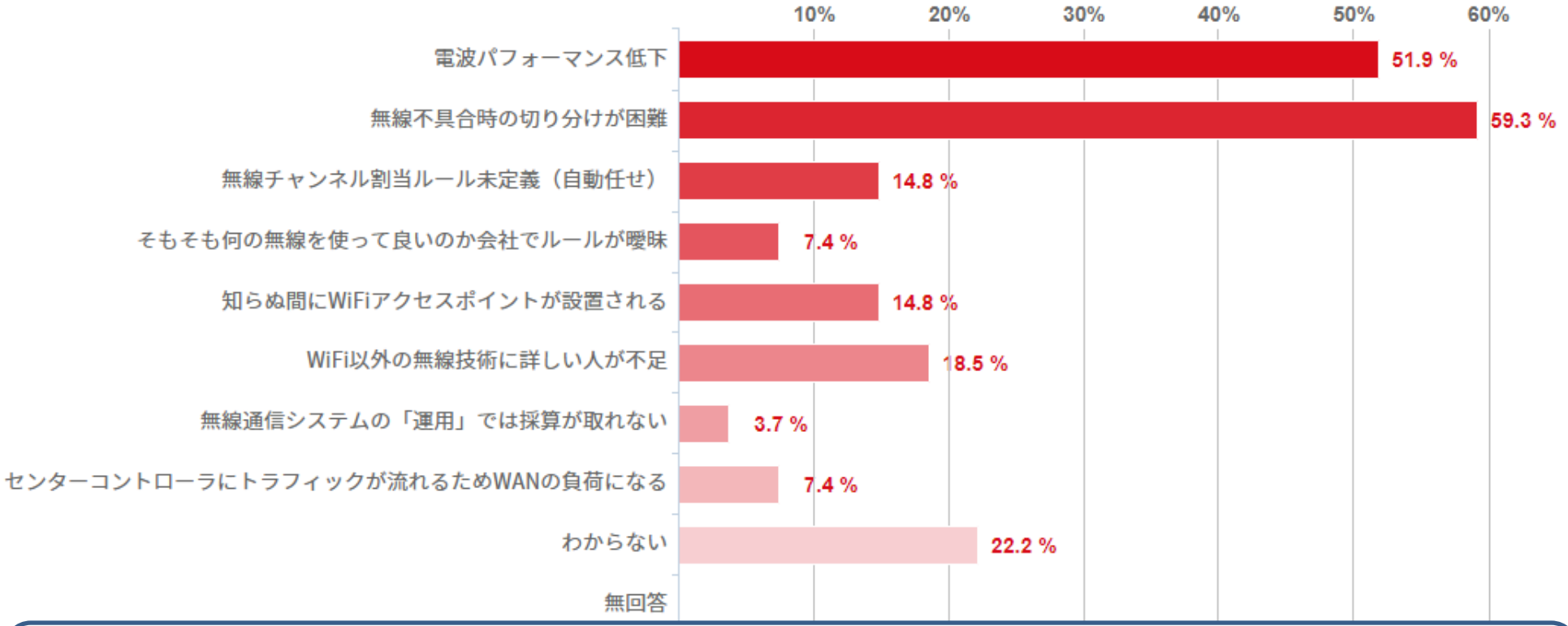
自由記述回答

- オフィス内でのモバイルルーターの利用・部門で独自の無線LAN設置は禁止。テザリングは会社支給のiPhoneからのみ許可
- オフィス内の重要なフロアではモバイルルータ・テザリングの使用は原則禁止としている
- 社内ではIT部門から提供されている無線LANのみ利用可で、独自の無線AP設置は禁止されています。

モバイルルータ持ち込みによる電波干渉は対策していない会社がほとんどだった。
また、対策としては、規則でモバイルルータや無線APの持ち込み禁止が多かった。
機器側での制限ではなく、モバイルルータや無線APを社内に持ち込み禁止にするなど規則で対策としている会社が多いと思われる。

アンケート結果と考察

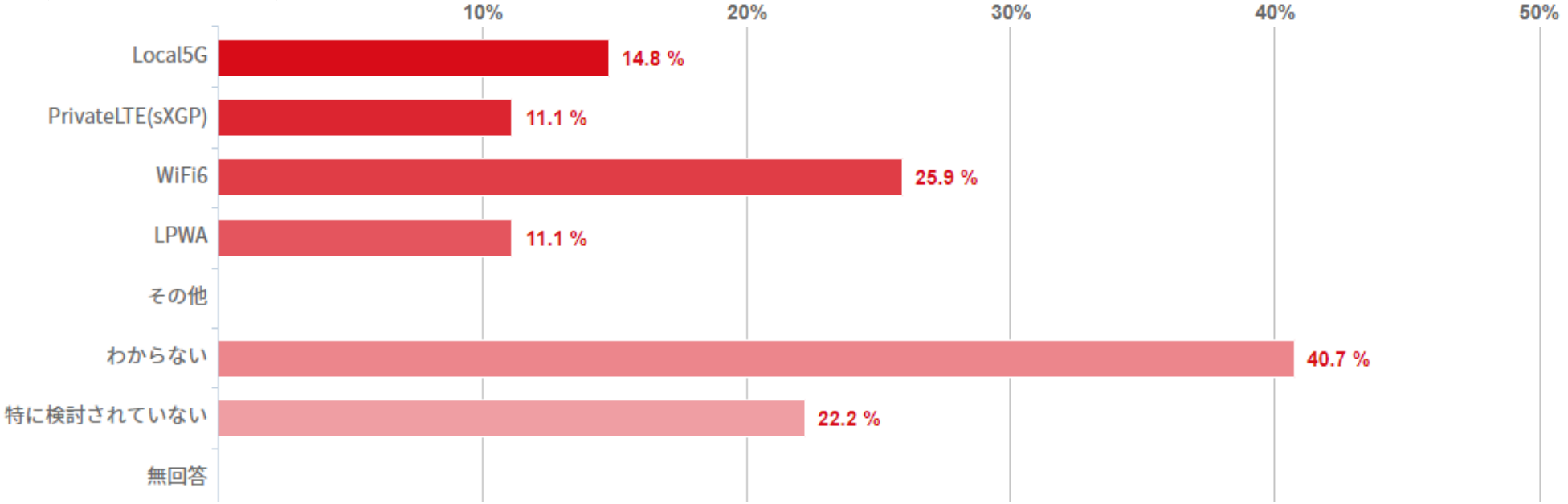
■Q8　無線通信を利用する上での課題は何ですか？（複数回答）（回答数: 27 ）



「不具合時の切り分けが困難」「電波パフォーマンスの低下」がともに5割超えで多く、性能面や障害対応での課題を挙げる会社が多かった。その他には「会社でルールが曖昧」「知らぬ間にWiFiアクセスポイントが設置」などルール面での課題のほか、「WiFi以外の無線技術に詳しい人が不足」といったナレッジが溜まっていないといった課題が上がっている。

1.現在の無線利用状況と最新無線通信技術の動向
アンケート結果と考察

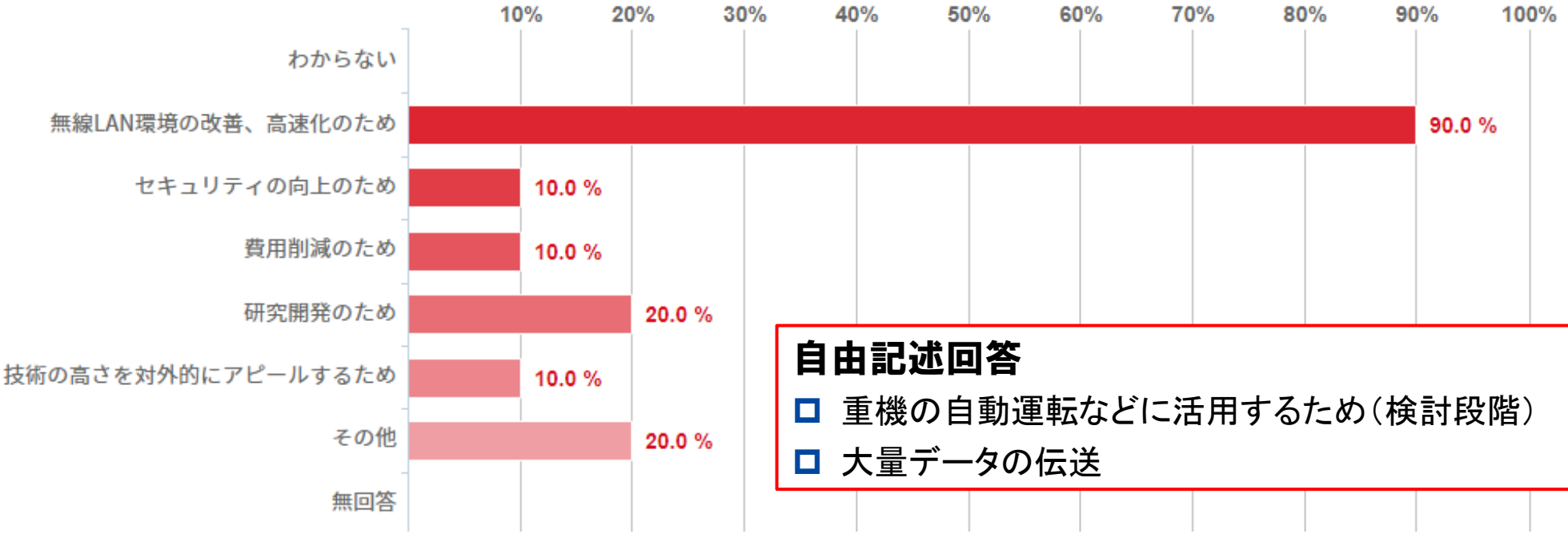
■Q9　今後導入または移行を検討している無線ソリューションはありますか（複数回答）
（回答数: 27 ）



各無線ソリューションで回答がばらけているが、WiFi6が若干多い結果となった。社内利用でWiFiを利用していることから、その延長でWiFi6を導入検討していると思われる。
一方で、「わからない」「特に検討されていない」といった回答も多く、まだ次世代無線LANに関して明確な方針が決まっていない会社が多いと思われる。

1.現在の無線利用状況と最新無線通信技術の動向
アンケート結果と考察

■Q10「Q9」で導入・以降を検討されている理由を教えてください（複数回答）
（回答数: 10 ）



自由記述回答

- 重機の自動運転などに活用するため（検討段階）
- 大量データの伝送

新技術の導入理由としては「無線LAN環境の改善、高速化」が多かった。WiFi利用のユーザが性能向上を目的としてWiFi6導入を検討していると思われる。そのほかセキュリティ向上や費用削減なども挙げられている他、研究開発や重機の自動運転など他業務との関連での検討も見られる。

1.現在の無線利用状況と最新無線通信技術の動向
アンケート結果と考察

■Q11　自社利用若しくはお客様に提供した実績のある無線通信ソリューションを選択してください（複数回答）（回答数: 27 ）

WiFi利用が最多で、今までの回答から自社内利用を含めたものかと思われる。
少数ではあるものの、PrivateLTEやLocal5Gなどもあり、新技術導入を進めている会社もある。

1.現在の無線利用状況と最新無線通信技術の動向
アンケート結果と考察

■Q12　自社利用若しくはお客様に提供した無線通信ソリューションにて苦労したこと、失敗したことがあれば記入ください。（任意回答）

自由記述回答（1/2）

- 無線LANを客先へ導入する際、お客様の利用端末の種類あるいはOSが多岐にわたることによる接続性の不具合、相性、等への対応について、構築時にすべてのパターンを想定することは難しく、またメーカーのノウハウとしても乏しく対応に苦労した。
- 弊社以外が導入したWiFiシステムとの電波干渉。
  工場内で勝手にシステム別WiFiが増殖（勝手にと言いながら、導入基準も示されていないので必然）
  「無線が遅い」と言われても切り分けに時間がかかる。そもそも速度保証していない。
- 現在、無線LAN更改案件を担当しており、4つの拠点で更改が完了しました（WiFi-6対応）。更改前と比べ、無線切断事象が多くなり、問い合わせが増えました。
  ログのエラーメッセージからだと、正常な切断とも区別がつきにくく、トラブルシューティングが難しいです（場所移動やPC閉じるとか）。そこで、100名以上が参加するTeamsで切断事象を記録していってもらい、情報収集したりしました。その結果、切断事象の原因のひとつが、デバイス起因の問題（証明書設定誤り）であることが分かりましたが、すべて解決はしていません。現在進行形で、とても苦労しています。
- 無線LANの性能劣化の疑いがかけられても、なかなかシロであることを証明しづらい。
  スマホの社内LAN接続を進めた結果、スマホの性能劣化が原因で通信不具合が発生（ちなみにiPhone5c）

1.現在の無線利用状況と最新無線通信技術の動向
アンケート結果と考察

■Q12　自社利用若しくはお客様に提供した無線通信ソリューションにて苦労したこと、失敗したことがあれば記入ください。（任意回答）

自由記述回答（2/2）

- スマートデバイス（iPhone等）の導入により、1アクセスポイント当たりの接続端末数が急増し、アンテナ側での処理に遅延が生じている。
- 事務所内での無線利用ではあまりトライブルは発生していない。屋外や広いエリアで利用する際に、長距離カバーできなかったり、途中で環境が変わったり（建物が間に建てられる）することで電波が届きづらくなることがある。
- フロアに3台設置していた無線APにささっていたLANケーブルが、LANケーブルを利用したい誰かによって引き抜かれ、戻されず、無線LANパフォーマンスが落ちている状態になっていることがあった。管理側では気付かず、無線LAN利用ユーザー側からの指摘により発覚。
- Ciscoのオンプレコントローラー型を導入したが、公式のマニュアルがあまり充実しておらず、構築に苦労した。
- 当社では社外持ち出しPCもしくはBYOD端末から、社内の自席PCにVDN接続し、リモートデスクトップにて画面転送を行っている。社内の自席PCは無線LAN接続であることから、不具合時の切り分けが難航する事例が多々ある。

先の無線LAN利用の課題に関連した回答が多かった。「不具合時の切り分けが困難」、「会社でルールが曖昧」と言った部分に対して具体的な事例を回答となっている。
現行無線LAN環境での課題が多いことから、新規無線LAN技術の導入に慎重になっているようにも見える

2：既存踏襲が引き起こす経済的な損失と脱却アプローチの検討

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
はじめに

2018年に発行された経済産業省「D X レポート～ITシステム「2025年の崖」の克服とDXの本格的な展開～」によると約8割の企業がレガシーシステムを抱えており企業のDXの足かせとなることを警鐘している。

しかしながら発行から4年が経過した今も「課題認識は共有されたが脱却に至っていない」企業が多く存在しているように見受けられる。

当研究テーマでは レガシーシステムの 既存踏襲が引き起こし得る
リスクの分析を行い そこから脱却するアプローチを研究・提案するもの。

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～なぜ既存踏襲が行われるのか～

■チーム内ヒアリング結果

分科会内13社に関して レガシーシステムの脱却ができない要因をヒアリング

コスト的要因	心理的要因	技術的要因
・脱却のための投資額が巨大	・使い勝手が変わるのを現場が嫌がる	・ブラックボックスのためどこから手を付けていいかわからない
・投資対効果が出せない	・現状困っていない(問題視されていない)	・代替技術がない
	・必要性が理解されない	
	・きっかけがない	

経営層

システム利用者

アプリケーションエンジニア etc

レガシーシステムの脱却の必要性をステークホルダーに
理解してもらえないケースが多い ≒ 実行効果の評価が難しい

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究 ～なぜ既存踏襲が行われるのか～

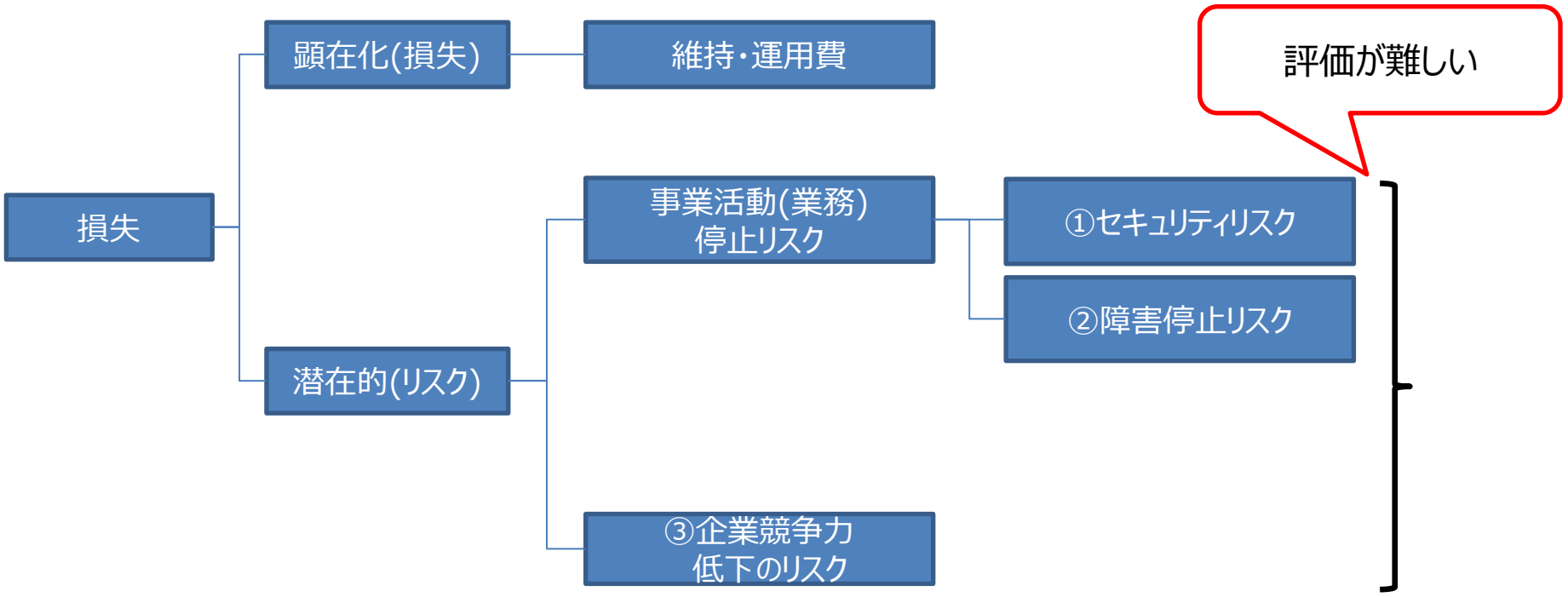
JUAS

■想定されるレガシーシステム脱却ストーリー

STEP	想定する実施内容	課題
洗出し	HW、SWにおいて保守切れしているもの、保守切れが発表されているもの、保守内であっても技術的に進歩性が今後見込めず枯れていくことが予想されるものを全て洗出し、リストアップ	各システムの一元的な構成管理
評価	リストアップされたレガシーシステムを定量的に評価し、脱却の優先順評価に利用	評価基準の整備
脱却方針・計画策定	リスク値に基づき全レガシーシステムにおける脱却方針と計画を策定	脱レガシーに関する技術、ノウハウ確立
ステークホルダー合意	リスクの説明と脱却計画を説明し合意形成(＋協力要請)	脱却実施に必要な費用と必要性整理
脱却の推進	計画に沿って個々のレガシー脱却	着実な推進・実行

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究 ～なぜ既存踏襲が行われるのか～

■レガシーシステム脱却における評価の視点



潜在的な損失(リスク)を影響度×発生頻度から定量的に評価

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

■潜在的な損失(リスク)評価の考え方

レガシー化している対象システムごとに以下を計算

①.セキュリティインシデント時のリスク＝Max(セキュリティインシデント発生時の影響度)×
(セキュリティインシデント発生頻度)

②.障害発生時のリスク＝Max(障害発生時の影響度)×Max (HW障害発生頻度,SW障害発生頻度)

③.企業競争力低下のリスク＝企業競争力への影響度 ×競争力低下の発生頻度

▼

レガシーシステムのリスクアセス値 ＝ MAX (①,②,③)

として評価を実施

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

①セキュリティリスクの評価

ｉ．セキュリティインシデント発生時に考えられる影響

3項目の影響度の内、最大値をセキュリティインシデント影響度として定義

影響の程度	業務影響	社会的 評価低下	情報漏洩
Ⅴ：極めて重大	・複数拠点の業務停止 ・他社業務の停止	・マスコミ、 SNS報道	・機密情報漏洩 ・個人情報漏洩 ・取引先情報漏洩
Ⅳ：重大	・単一拠点の業務停止 ・Gr企業の業務停止	―	・社外秘情報漏洩
Ⅲ：中程度	・複数業務の停止	―	―
Ⅱ：軽微	・単一業務の停止	―	―
Ⅰ：無視できる	・複数利用者(PC) の停止	―	―

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

①セキュリティリスクの評価

ⅱ．セキュリティインシデント発生頻度の定義

IPA 情報処理推進機構 共通脆弱性評価システムで用いられてるCVSS V3 で定義されている「基本評価基準」を参考に定義

【セキュリティインシデント発生確率における利用項目】

1.AV−攻撃元区分（ローカル、隣接、ネットワーク、物理）
2.AC−攻撃条件の複雑さ(高、低)
3.PR−攻撃前に必要な特権レベル（高、低、不要）
4.UI −ユーザ関与レベル(不要、要)

出典：IPA 情報処理推進機構 「共通脆弱性評価システムCVSS v3概説」
https://www.ipa.go.jp/security/vuln/CVSSv3.html

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

①セキュリティリスクの評価

ⅱ． セキュリティインシデント発生頻度の定義

AV：AttackVector-攻撃元区分

脆弱性のあるコンポーネントをどこから攻撃可能であるかを評価

レベル(V3)	内容	値
ネットワーク(N)	対象コンポーネントをネットワーク経由でリモートから攻撃可能である。例えば、インターネットからの攻撃など	0.85
隣接(A)	対象コンポーネントを隣接ネットワークから攻撃する必要がある。例えば、ローカルIPサブネット、ブルートゥース、IEEE 802.11など	0.62
ローカル(L)	対象コンポーネントをローカル環境から攻撃する必要がある。例えば、ローカルアクセス権限での攻撃が必要、ワープロのアプリケーションに不正なファイルを読み込ませる攻撃が必要など	0.55
物理(P)	対象コンポーネントを物理アクセス環境から攻撃する必要がある。例えば、IEEE 1394、USB経由で攻撃が必要など	0.2

出典：IPA 情報処理推進機構 「共通脆弱性評価システムCVSS v3概説」
https://www.ipa.go.jp/security/vuln/CVSSv3.html

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

①セキュリティリスクの評価

ii． セキュリティインシデント発生頻度の定義

AC：Attack Complexity-攻撃条件の複雑さ

脆弱性のあるコンポーネントを攻撃する際に必要な条件の複雑さを評価

レベル(V3)	内容	値
低(L)	特別な攻撃条件を必要とせず、 対象コンポーネントを常に攻撃可能である。	0.77
高(H)	攻撃者以外に依存する攻撃条件が存在する。例えば、次のいずれかの条件に合致する場合などが該当する。攻撃者は、設定情報、シーケンス番号、共有鍵など、攻撃対象の情報収集が事前に必要となる。攻撃者は、競合が発生する条件、ヒープスプレイを成功させるための条件など、攻撃を成功させるための環境条件を明らかにする必要がある。攻撃者は、中間者攻撃のため環境が必要となる。	0.44

※ 出典
IPA 情報処理推進機構 「共通脆弱性評価システムCVSS v3概説」
https://www.ipa.go.jp/security/vuln/CVSSv3.html

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

①セキュリティリスクの評価

ii． セキュリティインシデント発生頻度の定義

PR：Privileges Required-攻撃前に必要な特権レベル

脆弱性のあるコンポーネントを攻撃する際に必要な特権のレベルを評価

レベル(V3)	内容	値
不要(N)	特別な権限を有する必要はない。	0.85
低(L)	コンポーネントに対する基本的な権限を有していれば良い。例えば、秘密情報以外にアクセスできるなど	0.62
高(H)	コンポーネントに対する管理者権限相当を有する必要がある。 例えば、秘密情報にアクセスできるなど	0.27

※ 出典
IPA 情報処理推進機構 「共通脆弱性評価システムCVSS v3概説」
https://www.ipa.go.jp/security/vuln/CVSSv3.html

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

①セキュリティリスクの評価

ii． セキュリティインシデント発生頻度の定義

UI：User Interaction-ユーザ関与レベル

脆弱性のあるコンポーネントを攻撃する際に必要なユーザ関与レベルを評価

レベル(V3)	内容	値
不要(N)	ユーザが何もしなくても脆弱性が攻撃される可能性がある。	0.85
要(R)	リンクのクリック、ファイル閲覧、設定の変更など、 ユーザ動作が必要である。	0.62

※ 出典
IPA 情報処理推進機構 「共通脆弱性評価システムCVSS v3概説」
https://www.ipa.go.jp/security/vuln/CVSSv3.html

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

①セキュリティリスクの評価

ⅱ． セキュリティインシデント発生頻度の定義

セキュリティインシデント発生頻度＝攻撃容易性値 X＝AV×AC×PR×UI

発生頻度	値別分類
5.非常に高い	0.4≤X
4.高い	0.3≤X<0.4
3.発生し得る	0.2≤X<0.3
2.考えにくい	0.1≤X<0.2
1.考えられない	X<0.1

※ 出典
IPA 情報処理推進機構 「共通脆弱性評価システムCVSS v3概説」
https://www.ipa.go.jp/security/vuln/CVSSv3.html

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

②障害停止のリスク評価

ｉ．障害発生時に考えられる影響

2項目の影響度の内、最大値をセキュリティインシデント影響度として定義

基本的に、セキュリティインシデント発生時の影響度 評価項目と同じ

但し障害停止時に情報漏洩が発生することは考えられないため除外

影響の程度	業務影響	社会的 評価低下
Ⅴ：極めて重大	・複数拠点の業務停止 ・他社業務の停止	・マスコミ、 SNS報道
Ⅳ：重大	・単一拠点の業務停止 ・Gr企業の業務停止	―
Ⅲ：中程度	・複数業務の停止	―
Ⅱ：軽微	・単一業務の停止	―
Ⅰ：無視できる	・複数利用者(PC) の停止	―

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

②障害停止のリスク評価

ⅱ．障害発生の発生頻度の定義

2項目の内、最大値を障害発生の発生頻度として定義

発生頻度	HW障害	SW障害
5.非常に高い	HWが保守切中または保守切れが発表されており自営保守も不可能	対象システムにおける本体プログラムの変更がある
4.高い	―	対象システムにおけるIFの改造が有り かつ動作環境（OSパッチ、ウイルス対策ソフトなど）の変更がある
3.発生し得る	HWが保守切中または保守切れが発表されているが自営で修理可能	対象システムにおけるIFの改造または動作環境（OSパッチ、ウイルス対策ソフトなど）変化の何れかが定期的に発生
2.考えにくい	―	対象システムにおいて IF含め 改造はなく、変更は発生しない
1.考えられない	HWが保守終了が発表されていない	―

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

③企業競争力低下のリスク評価

ｉ.対象システムに投資せず、他社が積極的なIT投資を図った場合に想定される影響

2項目の内、最大値を企業競争力低下の影響度として定義

影響の程度	フロントオフィス システム	バックオフィス システム
Ⅴ：極めて重大	・コア事業 商品/サービス QCDレベルの相対的低下	・複数拠点、事業部の 生産性の相対的な低下
Ⅳ：重大	・コア事業 商品/サービス QCDレベルの相対的低下	・単一拠点、事業 部の生産性の相対的な低下
Ⅲ：中程度	―	・複数業務の 生産性の相対的な低下
Ⅱ：軽微	―	・単一業務の 生産性の相対的な低下
Ⅰ：無視できる	―	―

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

③企業競争力低下のリスク評価

ⅱ.企業競争力低下の発生頻度の定義

チェックが付けられない場合は、一律「3」の評価とする

発生頻度	内容
5.非常に高い	・対象システムの新技術が世間一般的に浸透している ・競合他社が対象システムへの投資を公開している
4.高い	・対象システムの新技術が世間一般的に認知され始めている ・競合他社が対象システムに関する技術提携などを表明している
3.発生し得る	・その他
2.考えにくい	―
1.考えられない	―

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

実施例.

	①セキュリティリスク アセスメント値	②障害停止リスク アセスメント値	③企業競争力低下 リスクアセスメント値	総合値
品質管理システム (VB6)	16 (影響度 4 発生頻度 4)	20 (影響度 4 発生頻度 5)	15 (影響度 5 発生頻度 3)	20
決済システム (COBOL)	15 (影響度 5 発生頻度 3)	25 (影響度 5 発生頻度 5)	25 (影響度 5 発生頻度 5)	25
特定箇所の L2NW スイッチ (保守切れ)	6 (影響度 3 発生頻度 2)	10 (影響度 2 発生頻度 5)	9 (影響度 3 発生頻度 3)	10

2.既存踏襲が引き起こす経済的な損失と脱却アプローチの研究
～既存踏襲が引き起こすリスク分析～

■レガシーシステムのリスクアセスメント値毎の優先度評価と対応方針

発生頻度						
5	非常に高い	C (5)	B3 (10)	A1 (15)	A2 (20)	A3 (25)
4	高い	C (4)	B1 (8)	B3 (12)	A1 (16)	A2 (20)
3	発生し得る	C (3)	C (6)	B1 (9)	B3 (12)	A1 (15)
2	考えにくい	C (2)	C (4)	C (6)	B1 (8)	B3 (10)
1	考えられない	C (1)	C (2)	C (3)	C (4)	C (5)
		無視できる	軽微	中程度	重大	極めて重大
		I	II	III	IV	V

影響度

【判定結果】

A.最優先で脱方針を検討・実行

十分な経営資源を投じて早期脱却を
最優先で実施すべき。並行して 脱却完了までの
リスク低減策も並行して検討

B.やむを得ない事情を除き脱方針を検討・実行

グループCまでリスク値を低減可能な場合は脱却の優先度は低い
しかしならグループCへリスク値低減するためのリソースが大きい場合や
低減自体が難しい場合は、脱却方針の検討・実行を実施すべき

C.可能であれば 脱方針を検討・実行

余裕があれば 脱却方針の検討・実行を実施すべきであるが
リソースが十分でない場合は、A・Bグループを優先し実施。
時間経過と共にリスク値は上がる可能性があるため注視と定期的な
評価は継続

3.クラウドシフト時代における企業の状況と今後の課題
～クラウド化・SASE・ゼロトラスト・エッジコンピューティング～

- サブテーマ①：　導入企業に聞いた！導入後に解ってきた傾向と対策
- サブテーマ②：　SASE・ゼロトラストなどの新技術に移行されない根本原因

活動テーマ

メインテーマ：**クラウドシフト時代における企業の状況と今後の課題**

～クラウド化・SASE・ゼロトラスト～

サブテーマ①：　導入企業に聞いた！導入後に解ってきた傾向と対策

サブテーマ②：　SASE・ゼロトラストなどの新技術に移行されない根本原因

導入企業に聞いた！導入後に解ってきた傾向と対策

■はじめに

社内システムのクラウド利用も進み、またご存知の通り、昨今のコロナウィルスの影響で、
日本にも急速にテレワークでの就業が加速度的に浸透し始めている。

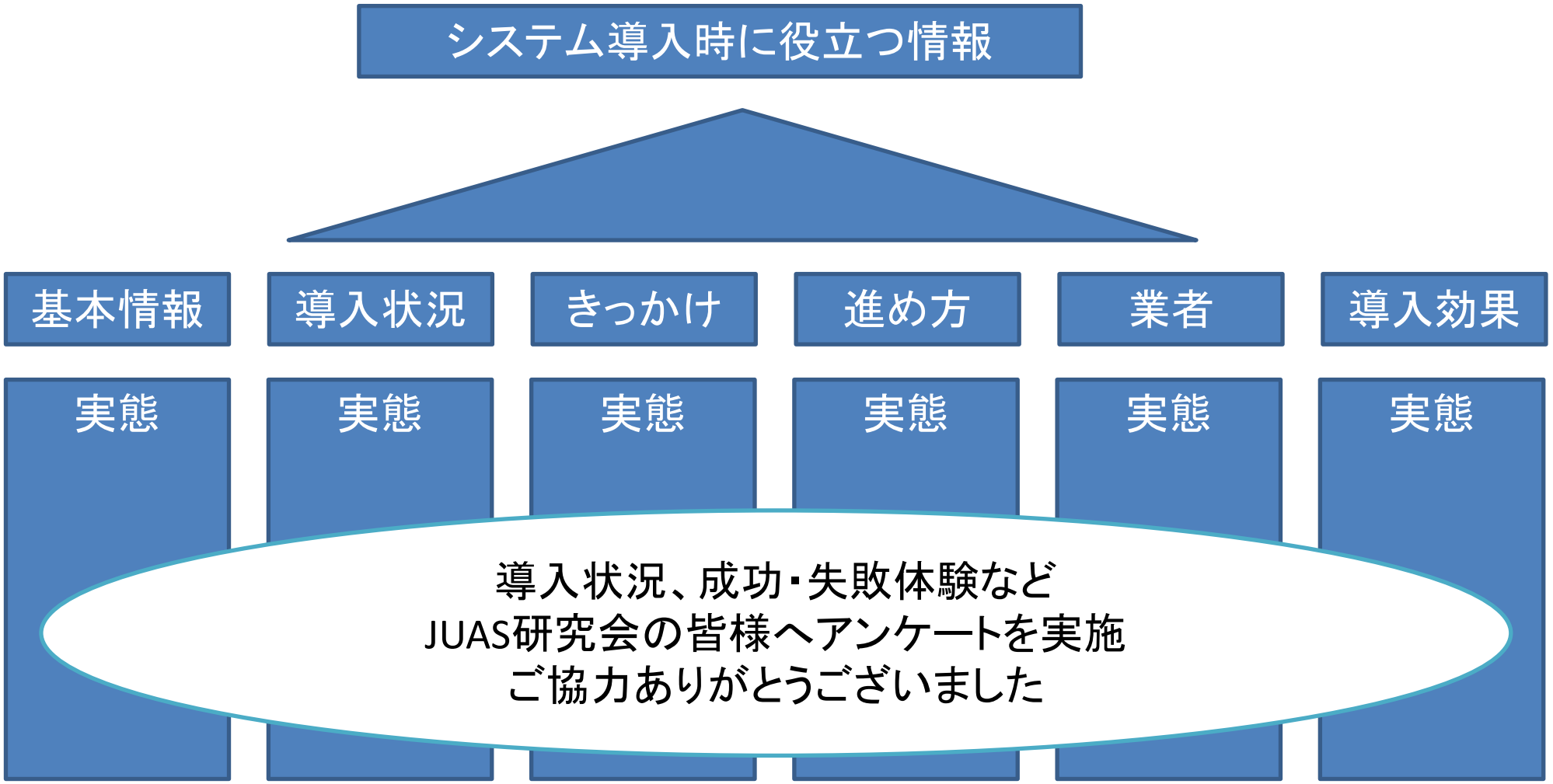
この変化に伴い、今までのセキュリティの考え方がミスマッチとなっており、【ゼロトラスト】と言う
考え方・セキュリティ手法を検討・導入する企業が増えている。「ネットワーク」を信頼するのではなく、
動作するアプリやデバイスを「守る」と言う発想だ。

「どこで利用してもセキュリティ的に安全な環境」を構築するためには、
この【ゼロトラスト】の考え方に沿った環境・製品を導入していく必要がある。

ただ、【ゼロトラスト】と言う言葉も、一時期の「クラウド」と同じ様に一人歩きし始め、
経営層などから「ウチにはゼロトラストと言うソフトは導入済みなのか？」と言った、
若干的外れな話が舞い込んで来る状況ではないだろうか？。

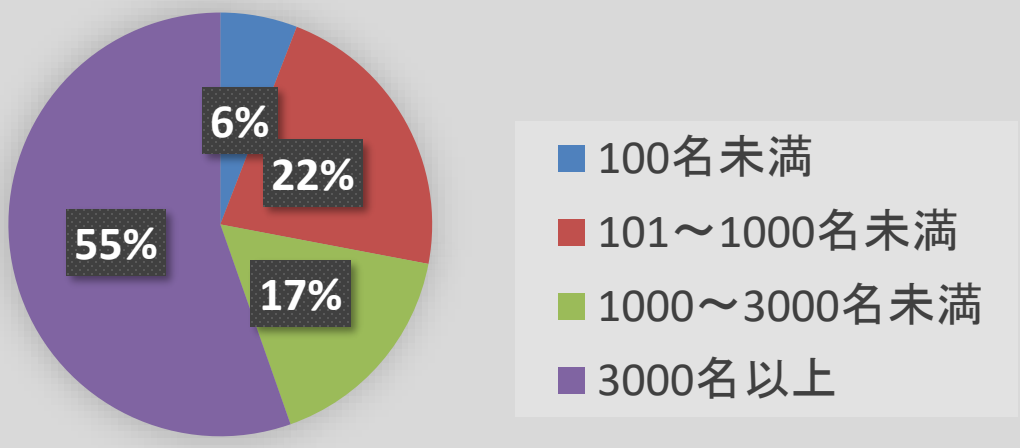
私たちのチームでは、この様な世の中で、ゼロトラストの考え方に沿った製品を導入するにあたり、
実際の導入状況や、導入時にどの様なハードルがあったか。導入出来ない根本原因は何なのか。
また、そのハードルをどの様に乗り越えて導入したのか、「生の声」も交えて調査し、皆さんの会社へ
導入する際の「あんちょこ」として活用頂ければと思い、今回の研究テーマを定めた。

導入企業に聞いた！導入後に解ってきた傾向と対策



導入企業に聞いた！導入後に解ってきた傾向と対策
アンケート結果1. 基本情報【回答者の属性】

■従業員数



■事業所配置　**全国50カ所以上に拠点がある企業が61.1%**　10～50カ所未満27.8%

■会社での役割　**自社システム選定担当44.4%**　システム運用16.7%　他社提案33.3%　他5.6%

導入企業に聞いた！導入後に解ってきた傾向と対策
アンケート結果 2.導入状況【企業へのSASE導入状況】

Q. EDRの導入状況　　製品例：CrowdStrike、Intune、Symantec、McAfee

導入済み	**77.8%**
導入中or展開中	5.6%
検討中(半年以内に導入予定)	5.6%
検討中(1、2年以内に導入予定)	11.1%
検討していないor不要	0%
不明	0%

Q. CASBの導入状況　　製品例：Zscaler、McAfee、Akamai、PaloAlto

導入済み	11.1%
導入中or展開中	11.1%
検討中(半年以内に導入予定)	5.6%
検討中(1、2年以内に導入予定)	**38.9%**
不明	33.3%

導入企業に聞いた！導入後に解ってきた傾向と対策
アンケート結果 2.導入状況【企業へのSASE導入状況】

Q. IAPの導入状況　製品例：Akamai、Zscaler(ZPA)、NetScope(NPA)

導入済み	**38.9%**
導入中or展開中	5.6%
検討中(半年以内に導入予定)	11.1%
検討中(1、2年以内に導入予定)	11.1%
検討していないor不要	5.6%
不明	27.8%

Q. SIEMの導入状況　製品例：Splunk、QRadar、Exabeam

導入済み	16.7%
導入中or展開中	16.7%
検討中(半年以内に導入予定)	5.6%
検討中(1、2年以内に導入予定)	16.7%
検討していないor不要	5.6%
不明	38.9%

導入企業に聞いた！導入後に解ってきた傾向と対策
アンケート結果 2.導入状況【企業へのSASE導入状況】

Q. IAMの導入状況　製品例Okta、HENNGE One、Onelogin、AzureAD

導入済み	**44.4%**
導入中or展開中	33.3%
検討中(半年以内に導入予定)	5.6%
検討中(1、2年以内に導入予定)	11.1%
検討していないor不要	0%
不明	16.7%

Q. SD-WANの導入状況　製品例VeloCloud、Cisco、HPE Aruba、Fortinet、

導入済み	22.2%
導入中or展開中	11.1%
検討中(半年以内に導入予定)	0%
検討中(1、2年以内に導入予定)	**27.8%**
検討していないor不要	11.1%
不明	27.8%

導入企業に聞いた！導入後に解ってきた傾向と対策
アンケート結果 3.導入時の課題

Q. 導入時の課題及びその解決方法について教えてください。

–**「セキュリティ物」は投資効果を説明するのが困難。**対策を取らないとリスクがあることを決裁者にわかるように
説明することで導入の必要性が伝わり、予算も付きやすくなる。

–経営層への説明の際、作成済みのセキュリティロードマップを用いて、**どの範囲をカバーする製品なのかを明確化**した上で、製品の特長を噛み砕いて説明し、納得いただいた。

–昨年度予算承認が下りずSD-WAN等の導入は進んでいない。全体的にコスト削減のようで**既存の使えている**
ネットワークを今更改する必要性が伝わらなかったのかと思った。

–某SD-WAN製品を導入中だが、**一部手配済みの回線種別が未サポートであることが判明**し、回線手配し直している。(フレッツなどのIPoE回線)

–**インシデントをトリガに検討**を進めたところスムーズに検討が進んだ。

導入企業に聞いた！導入後に解ってきた傾向と対策
アンケート結果 4.進め方【RFP作成のポイント・進め方】

Q. RFP作成時(もしくは提案時)に気を付けている(気にしている)ことがあるか？

ある　5.6%

ない　50.0%

わからない　44.4%

Q. RFP作成時に気を付けているポイントは？

1. システム導入後のビジョンをしっかり示す　7ポイント

2. 特定のベンダーや製品に決まらないようにすること　4ポイント
3. 選定前に自社環境でPoCを実施した上で方針を示す　3ポイント
4. コンサル会社など自社以外の意見を反映している　3ポイント
5. 3か年計画、中期経営計画など経営方針マッチする内容を盛り込む　1ポイント
6. 公平性を保つようにする　1ポイント
7. 自社の社員のみで検討作成する　0ポイント

導入企業に聞いた！導入後に解ってきた傾向と対策
アンケート結果 5.業者【ベンダー・メーカーとの関係】

Q. 導入検討の際、ベンダーもしくはメーカーは、自社の要望を理解していたか？

十分理解していた　11.1%
そこそこ理解してくれていた　27.8%
あまり理解してくれていなかった　5.6%
不明　55.5%

Q. ベンダー、メーカーへの意見

●ポジティブ(上記Qの回答が1or2の方)

－日頃から出入りしているメーカーの営業マンなので自社環境を一定程度理解頂いている。これに加えて、ソリューション(製品)に求めている背景・展望などを理解いただけるように説明している。
－当社のセキュリティロードマップ等を提示し、また部内の事情も説明した上で、製品の提案を実施させたため
－元々自社内のネットワーク構築を以前から担当しているベンダで自社内のネットワーク要件や経験を理解しているベンダだったため
－要望に合致した提案を頂いたから。
－具体的な将来像が明確化されておらず、明確に要件を伝えられていないため「そこそこ」になってしまっている。

▲ネガティブ(上記Qの回答が3or4の方)

－RFxの情報には本質的な要望が何であるか、要件の優先順位をどのように考えているのかが反映されていなかったため。

導入企業に聞いた！導入後に解ってきた傾向と対策
アンケート結果 6.導入効果

Q. 導入してみて当初想定と実際の効果は想定どおりでしたか？(達成率)

想定通り　5.6%

実環境では実現できないことが多少発生した　11.1%

想定以上に課題が浮き彫りになった　0%

わからない　83.3%

Q. 効果がでた要因は？

–SDWANのケースでは、Teams・**特定クラウドサービスのトラフィックをブレイクアウトさせることで**WANやデータセンタ側のインターネット接続点の**負荷軽減につながった**。
一方で、SDWAN装置におけるホワイトリストアクセス許可の**設定数上限が運用上問題**になったことや**IoTデータの伝送は当初想定に無い**と相乗りが許可されないなど自由度が低くて活かし切れていない

–**必要な要件・サービスが明確**になっており、それにマッチする製品の中で選定を行ったため

導入企業に聞いた！導入後に解ってきた傾向と対策
アンケート結果 7.導入していない理由

Q.SASE、ゼロトラスト、SD-WANを導入していない方はその理由/課題を教えてください。

－検討中のため、導入にいたっていない。

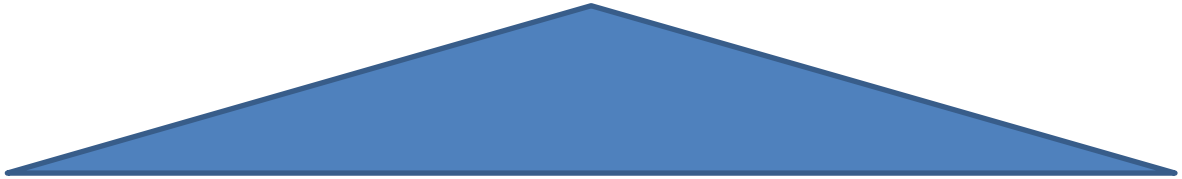
－導入している。在宅勤務の拡大で、自宅からクラウド直の通信要件が増え、DCにあるセキュリティの仕組みを通らなくなることが問題視され、今後もロードマップに基づき、SWG等の導入を予定している。

－導入実績がないため、中々踏み切れない。

－世間的なセキュリティインシデントが発生し、経営層が不安に感じないと予算化が難しい。

導入企業に聞いた！導入後に解ってきた傾向と対策

システム導入時に役立つ情報



基本情報	導入状況	きっかけ	進め方	業者	導入効果
実態	実態	実態	実態	実態	実態

・導入製品については、製品種別で濃淡があった（すべてを導入している企業は少ない）
⇒ゴールイメージを作成した上で、まずは必要な製品から導入しセキュリティを高める

・導入にあたっての課題は、やはりコスト
⇒どの様に経営層に説明できるかがカギとなる！

・導入するベンダーとの付き合い方、大きなポイント
⇒ RFP等を用いて、システム導入後のビジョンも共有する

導入企業に聞いた！導入後に解ってきた傾向と対策
考察・まとめ

■アンケート及び実態から考える良い進め方

・全体のゴールイメージ（全体像）を明確にした上で、それぞれの製品選定を進める。
（当たり前のことだけど、意外と出来ていない！）

・全てを一度に導入するのではなく、必要に応じて順番に製品を導入する手法も有り。（↑のイメージが重要！）

・経営層に説明する際は、ゴールイメージを共有し、導入する製品が「何」を対策する事ができるのか明確にした上で、導入にかかるコストだけではなく、導入しなかった場合の損害リスクも試算し提示する

・ベンダーに対しては、ゴールイメージを共有し理解して貰った上で、単体製品の導入のみではなく、全体を考慮した導入となるよう、依頼する。（買って終わり・売って終わりにならないように！）

・関係者（ベンダー含む）に、導入後のフィードバックを必ず行う（次回の製品導入に反映させる！）

■今後の課題

・ほぼ同一のサービス内容・コストの製品が候補に挙がってきた際の選定方法
・他社の動向をどの様にキャッチアップするか？（JUASに参加？！）

ベンダーとも経験を
共有しよう！

導入企業に聞いた！導入後に解ってきた傾向と対策
活用ツール「導入にあたってのチェックリスト」

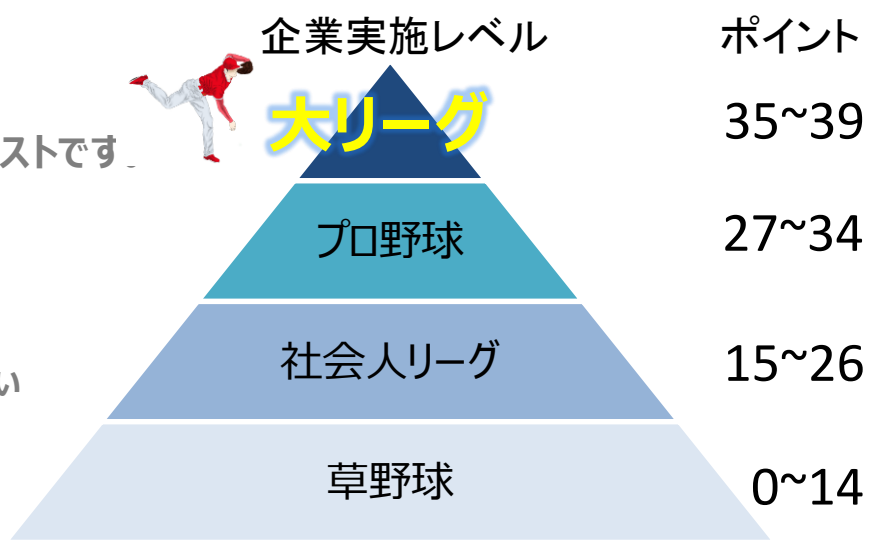
■ チェックリストの使い方

位置づけ

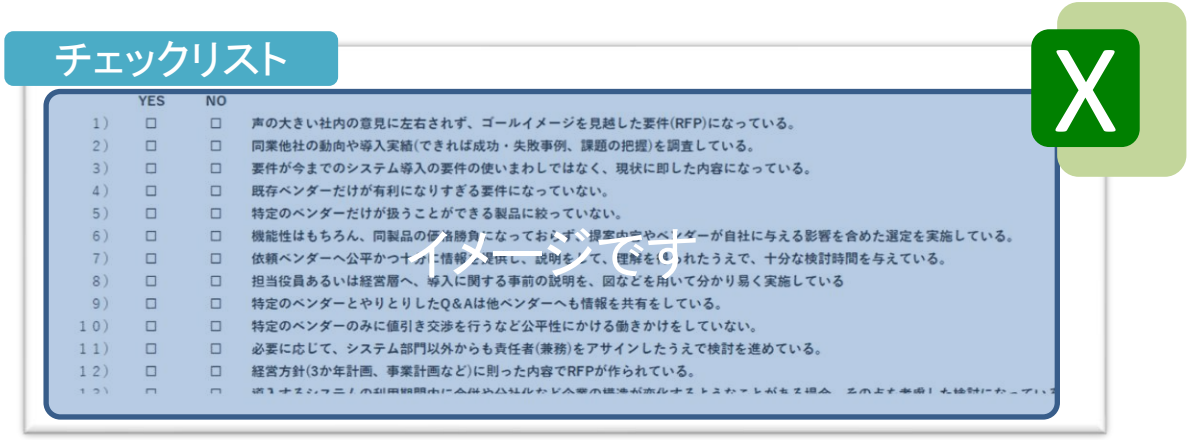
新たにシステムの導入を検討する際、重要になる項目をまとめたチェックリストです。
どの程度達成できているかお試しください。
※皆様からのアンケート結果でいただいた成功体験をもとに作成しております

手順

1．各項目をチェックします。※できる、まぁまぁできる、たまにできる、できていない
2．項目につき“0～3ポイント”で計算
3．合計ポイントを数えます。
4．あたなの会社が現在どのレベルか確認



チェックリスト



できれば大リーグ、少なくともプロ野球以上をめざしましょう！！

導入企業に聞いた！導入後に解ってきた傾向と対策
活用ツール「導入にあたってのチェックリスト」

■チェックリスト

項目	内容	できている(3)	まぁまぁ出来ている(2)	あまりできていない(1)	できていない(0)
1）	声の大きい社内の意見に左右されず、ゴールイメージを見越した要件(RFP)になっている。				
2）	同業他社の動向や導入実績(できれば成功・失敗事例、課題の把握)を調査している。				
3）	要件が今までのシステム導入の要件の使いまわしではなく、現状に即した内容になっている。				
4）	既存ベンダーだけが有利になりすぎる要件になっていない。				
5）	特定のベンダーだけが扱うことができる製品に絞っていない。				
6）	価格勝負になっておらず、サービス内容も含めた選定を実施している。				
7）	依頼ベンダーへ十分に情報を提供、または説明をして、理解を得られたうえで、十分な検討時間を与えている。				
8）	依頼ベンダーへ公平に情報を提供、または説明をしている。				
9）	特定のベンダーのみに値引き交渉を行うなど公平性にかける働きかけをしていない。				
10）	必要に応じて、システム部門以外からも責任者(兼務)をアサインしたうえで検討を進めている。				
11）	経営方針(3か年計画、事業計画など)に則った内容でRFPが作られている。				
12）	導入するシステムの利用期間内に企業の構造が変化するようなことがある場合、その点を考慮した検討になっている。				
13）	依頼ベンダーの提案に対して具体的な評価をフィードバックしているか。				
	小計				
	合計				
オマケ	他社の良いサービスがあれば一緒に持ってきてほしい・教えて欲しい(導入会社の本音)				

SASE・ゼロトラストなどの新技術に移行されない根本原因

■SASE・ゼロトラストの必要性

コロナ禍の影響により加速した在宅勤務や約7割の企業（※）が利用を開始したパブリッククラウドサービスの、またはより高度化するマルウェアの対して既存のセキュリティソフトやアクセス制御では情報漏洩の対策は不十分となってきた。

（※）令和3年度版情報通信白書より

社内外から情報資産を利用するようになったことで、エンドポイント・ネットワーク・クラウドそれぞれのセキュリティ強化を実施するためSASE・ゼロトラストの導入が必須となっている。

SASE・ゼロトラストなどの新技術に移行されない根本原因

■SASE・ゼロトラスト導入の実態

導入の必要性に対し、日本企業のSASE・ゼロトラストの認知度・導入状況は他国に比べ低いものになっている。

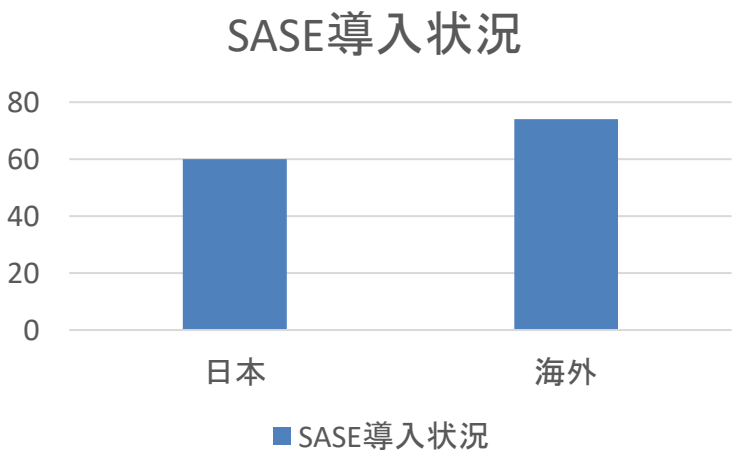
SASE導入状況（NetMotion Software 2021年4月調査より）

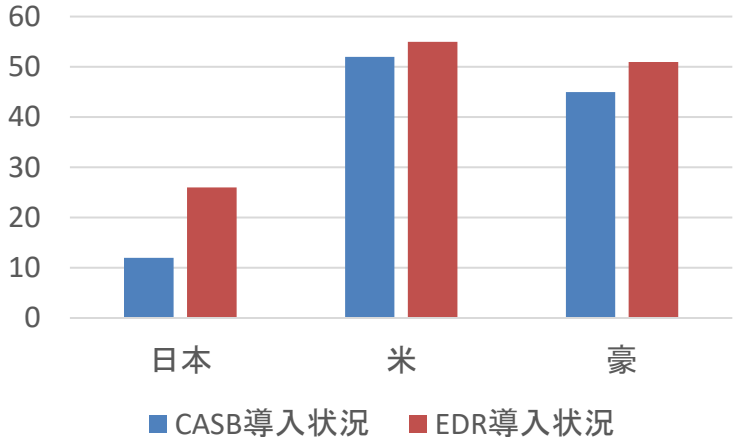
日本60% 海外（英豪独米）74%

ゼロトラスト導入状況（NRI セキュアテクノロジーズ 2022年2月調査より）

CASB　日本12% 海外（米）52% 海外（豪） 45%

EDR　　日本26% 海外（米）55% 海外（豪） 51%





SASE・ゼロトラストなどの新技術に移行されない根本原因

■研究テーマについて

SASE・ゼロトラストの導入の必要性に対して、低い導入状況の要因を調査しすでに導入を実施した企業の意見を踏まえ新技術移行で遭遇する課題、その解決策の参考となればと本研究テーマを定めた。

SASE・ゼロトラストなどの新技術に移行されない根本原因

■現行システムに起因する移行の問題点

■企業の実態調査

アンケート結果より、下記の要因で移行されないものと推定できた

- 現時点で十分なセキュリティを確保しているため、経営陣に必要性を理解されない（**予算確保不可**）
- 導入実績がないことより、対費用効果を考えると導入に踏み切れない（**現状維持**）

また、一般的に以下も問題に上がるものと推測できる

- 導入にあたり、オンプレミス環境の構成見直しが必要
  （**設計し直しする知見が必要、複数の担当部門と連携が必要**）
- オンプレミス環境を前提に策定されたセキュリティ基準の見直しが必要（**策定基準変更**）
- オンプレミス環境であったときよりも、セキュリティレベルを上げる必要がある（**セキュリティ向上**）
- クラウドサービスのため、サービス仕様が頻繁に変わることに対する運用時の負荷考慮する必要あり
  （**運用時の問題検討**）

SASE・ゼロトラストなどの新技術に移行されない根本原因

■現行システムに起因する移行の問題点

■調査結果分析結果

SASE・ゼロトラストに関するシステムの構成はネットワークやEDRなど社内システムすべてに関係する。
その特性上システム移行の影響が広範囲となり以下問題が浮上する。

導入できていない企業については大きく分けて以下の問題があると考えられる。

①予算確保
②導入する必要性を数値化して示すことができない
③導入する際の技術的な不安
④導入後の運用負荷が不明確

提案する立場にある担当は、上記の懸念事項を解消することが必須であると考えられる。

SASE・ゼロトラストなどの新技術に移行されない根本原因

◆企業の実態

ITインフラ研究会のメンバにアンケート調査を実施。

・回答者の基本情報【属性】
- 従業員数　100名未満　5.6%
　～1000名　22.2%
　～3000名　16.7%
　3000名以上　55.6%
- 会社での役割　**自社システム選定担当44.4%**　システム運用16.7%　他社提案33.3%　他5.6%

■アンケートでの声

・世間的なセキュリティインシデントが発生し、経営層が不安に感じないと予算化が難しい。

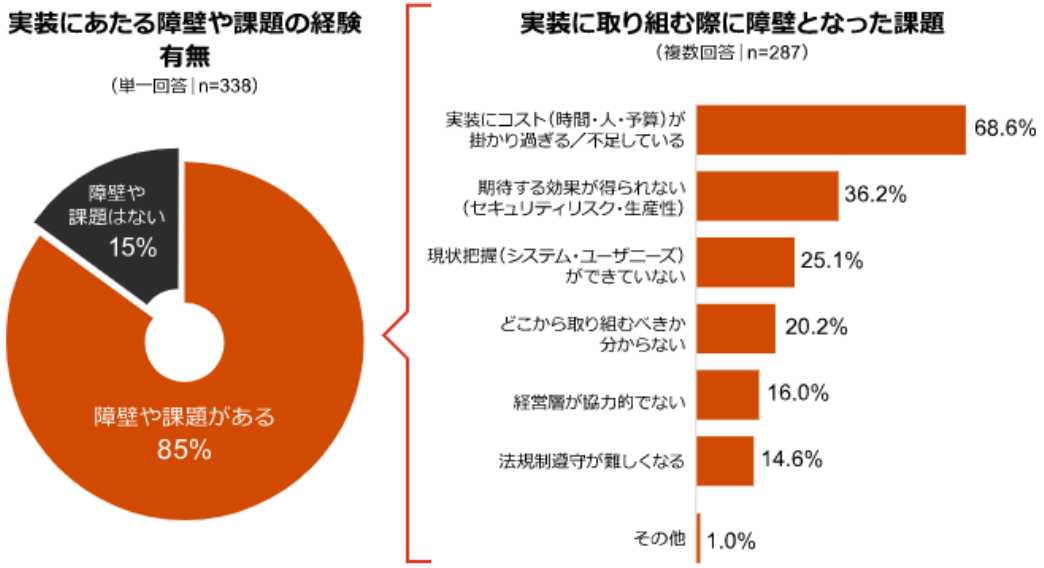
・導入実績がないため、中々踏み切れない

経営層による判断で導入されていない

SASE・ゼロトラストなどの新技術に移行されない根本原因

■国内企業の実態調査
（ゼロトラストに先進的に取り組む国内企業338社に対して行われたアンケート結果）

コストの不足や費用対効果の部分がかなり割合を占める結果が出ている



図．ゼロトラスト実装にあたっての障壁や課題
[引用]国内企業における「ゼロトラスト・アーキテクチャ」の実態調査2021

SASE・ゼロトラストなどの新技術に移行されない根本原因

◆調査結果分析

■コストがかかる（右図参考）

→導入におけるコストが予算内での優先度が低い

→導入後のコスト削減効果が薄い

■セキュリティ向上効果を実感しにくい（右図参考

→導入前後で実際にセキュリティインシデントが発生していない企業は実感しにくい

→導入にあたっての期待値が高すぎる

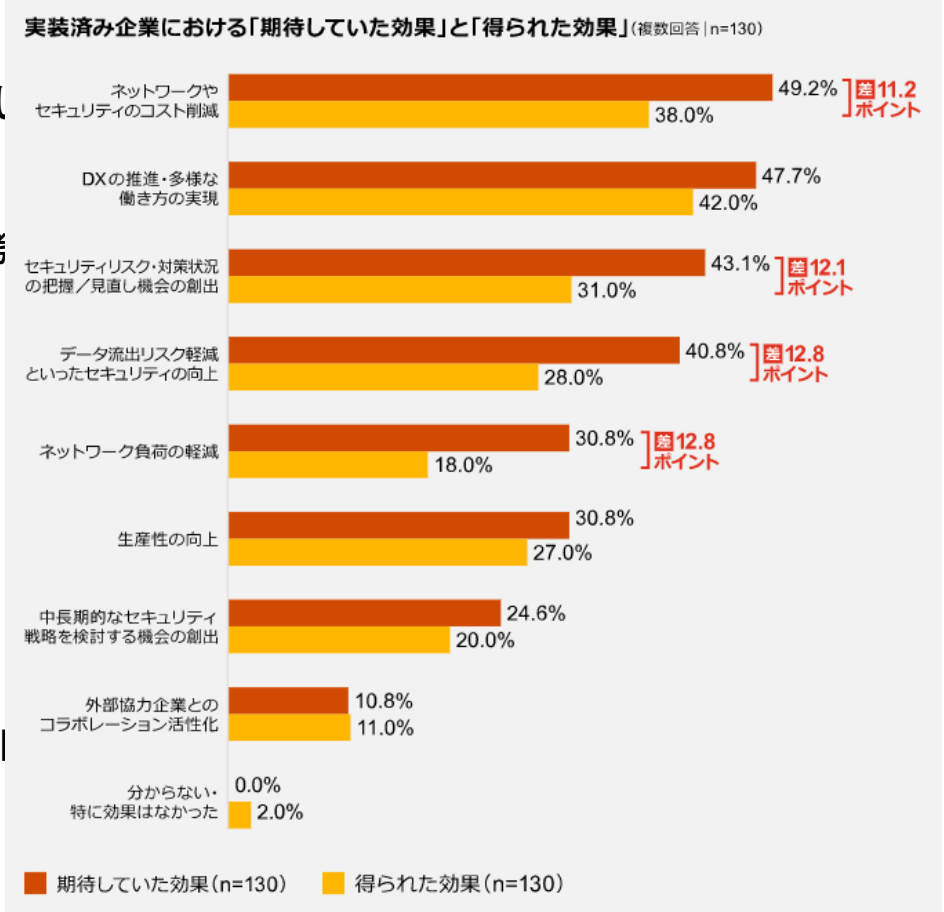
→効果を実感するためには一定期間が必要

■導入実績がない

→予算化が難しい、現行システムへの影響が不

■経営陣が協力的でない

→必要性を説明し、説得するのが難しい



図．ゼロトラストに期待していた効果と得られた効果のギャップ
[引用]国内企業における「ゼロトラスト・アーキテクチャ」の実態調査2021

SASE・ゼロトラストなどの新技術に移行されない根本原因

◆提言

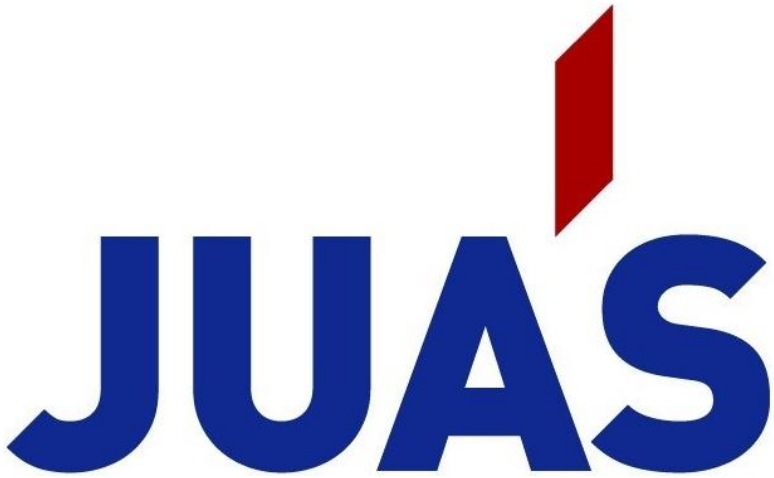
調査結果から、以下の二点が最も大きい原因と考えられた。

・経営層に必要と考えていない

・費用対効果が低いと考えられている

SASEやゼロトラストを導入することでの効果がセキュリティ向上以外にも
DXの推進・多様な働き方の実現があるということが、調査結果からも明らかになった。

DXの推進や多様な働き方の実現が今後のビジネス展開に大いに影響をもたらしと考えられるので、「経営層にはその旨を含めて説得する」「費用対効果の検討項目に含める」などの対処が導入障壁には効果的と考えられた。


JUAS