2026年ワイヤレス実態調査

相乗効果を引き出す：戦略的なワイヤレス投資により AI 時代における企業の成長を推進

日本

エグゼクティブサマリー

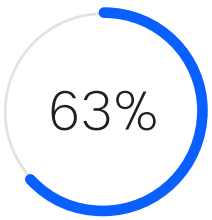
2026 年、Wi-Fi は単なる利便性向上のツールから、戦略的な成長を推進する不可欠なインフラへと大きく進化しました。世界中で、ワイヤレスに総合的に投資する組織は、業務の効率化から収益拡大まで、事業のあらゆる面で強力な ROI と測定可能なメリットを達成できる可能性が 4 倍高まっています。この相乗効果は、ワイヤレスが他の IT 投資とは異なり、企業全体に複合的なリターンをもたらすことを示しています。

一方、ほとんどの組織（98%）は、IT環境の複雑化が進み、セキュリティの脅威が増大し、このような課題に対処するために必要な人材の確保が難しくなっていると回答しています。組織は、さまざまな接続のニーズに対応し、従業員やや請負業者から自律型ロボット、スマートセンサー、AI アプリケーションまで、多様化するユーザーやデバイスを管理・保護することが求められています。

AI、自動化、最新のセキュリティ、そして認定された専門知識に包括的に投資しているグローバル組織は、そうでない企業に対して優位性を持っています。

+4x

ワイヤレス投資による強力なリターンを得られる可能性が 4 倍高い



ワイヤレス投資による平均 ROI が 63% 高い

今回初めてとなる本レポートでは、ワイヤレス AI のパラドックスが指摘されています。AI はワイヤレス ROI の主要な推進力であると同時に、リスク上昇の最大要因でもあるという点です。AI を活用した運用により、IT 担当者 1 人当たり、年間数百時間の節約につながる可能性がある一方で、インフラストラクチャの要件、セキュリティ脅威、人材不足の問題も増大します。 本レポートは、企業の主要な接続レイヤーとして Wi-Fi を軸に据えつつ、AI を活用したアプリケーション、IoT および OT 環境、企業における新たなユースケースなど、Wi-Fi が実現する広範なワイヤレスエコシステムについて考察しています。

調査では、老朽化したインフラストラクチャと、「複雑な運用」、「セキュリティ脅威の高まり」、「人材不足」という相関する 3 つの障壁が、ワイヤレス ROI の十分な実現を阻んでいることが明らかになりました。これらの課題が重なり合い、リスクが複合的に高まります。

運用面、セキュリティ面、人材面のこのような障壁に対処する組織は、そうでない組織より総合的に 63% 高い ROI を実現しており、戦略的なワイヤレス投資が、さまざまな側面で複合的で測定可能なリターンをもたらしていることが示されています。このことが、特に AI 活用が広がり、イノベーションが進む中で、ワイヤレス投資の機運が高まり続けている理由です。

総じて本調査では、ワイヤレスを戦略的に優先して取り組む日本の組織は、さまざまな側面で測定可能なリターンを得ていることが示されています。69% 以上の組織が社員の生産性の向上を挙げたほか、業務効率（68%）、顧客エンゲージメント（62%）に続いて、57% が収益に対するプラスの影響を挙げています。これは、最新のワイヤレス インフラストラクチャを整備することが事業の成長に直結することを示しています。

今こそ競争上の優位性を獲得するチャンスと言えます。2026 年、業務の簡素化やワイヤレスセキュリティのモダナイゼーション、専門認定の取得などに決意をもって取り組む日本の組織は、Wi-Fi を次の 10 年の戦略的な成長の推進力と位置づけるでしょう。

ワイヤレス戦略の正念場
AIのパラドックスとROI実現の障壁を乗り越える

ワイヤレス AI のパラドックスを明確にし、その重大さを理解する

2026 年、ワイヤレス AI のパラドックスは日本の企業リーダーにとって中心的な戦略課題となるものの、いち早く対処することでチャンスを掴むこともできます。AI はワイヤレス ROI の主要な推進力であると同時に、最大の課題を生み出す要因でもあります。世界において、AI を導入している組織はワイヤレスを戦略的に重視している割合が高く、ワイヤレス最適化を AI 展開戦略に組み込むことではるかに高いリターンを実現できる可能性が高くなっています。一方で、その AI によりかつてない運用上の複雑化が進み、新たなセキュリティ脅威が生じ、人材獲得競争に拍車がかかっています。

ワイヤレス AI のパラドックス
AIは解決策であり、課題である

解決策

・AI を活用することで、複雑なワイヤレス運用を簡素化できる

・自動化により IT 部門は戦略に注力できるようになる

・スムーズなチケット処理とワークフローの迅速化を実現

課題

・AI 生成型サイバー攻撃が最大のセキュリティ脅威に

・高度なワイヤレス／AI スキルを持つ人材が不足

・IT 人材がワイヤレス分野から AI 分野にシフト

AI はワイヤレス分野において ROI を実現する最も有力な道筋であるものの、最大のリスク要因でもあります。

AI がワイヤレス分野に多面的な課題をもたらす

セキュリティ脅威の主な要因	ワイヤレス分野の IT 人材の主な流出先	ワイヤレス人材獲得の主な障壁
#1 セキュリティ強化を阻む予算やリソースの制約	**#1** AI／機械学習	**#1** 高度なワイヤレスや AI 統合のスキルを持つ求職者の不足
#2 ユーザーの不適切な行動、人的ミス、インサイダーリスク	**#2** サイバーセキュリティ	**#2** 時間のかかる採用プロセスや社内のボトルネック
#3 AI 生成型または自動化されたサイバー攻撃／自動化された侵入ツールおよび複数のセキュリティレイヤーやセグメンテーションを管理する難しさ	**#3** ソフトウェア エンジニアリング／アプリ開発 & クラウド インフラストラクチャ／DevOps	**#3** 社内の予算上の制約や採用凍結 & キャリア分野としてのワイヤレスに対する関心の低さ

AI ワークロードを導入している日本の組織は、そうでない組織とはワイヤレスに対する認識が大きく異なります。世界で見ると、ワイヤレスを戦略的に非常に重要であると考えているワイヤレスリーダーは、AI ワークロードを導入している組織では 56%、導入していない組織では 46% となっています。

戦略的な重要性が高まっている理由は単純です。AI ワークロードにより、これまで以上に高性能で強靭なワイヤレスネットワークが求められるためです。ワイヤレス最適化を AI 展開戦略に組み込んでいる組織は、はるかに高いリターンを実現しています。日本では 10 社中 7 社近くが、業務効率、顧客エンゲージメント、社員の生産性、収益拡大の領域で、ワイヤレス投資によりプラスの効果が生まれていると回答しています。

AI の進化に関わるこのようなチャンスと課題、そしてリスクはどのように関係し合っているのでしょうか？

AI はワイヤレス運用を簡素化し、複雑さの問題に対処する手段と見なされている一方で、AI 生成型または自動化されたサイバー攻撃／自動化された侵入ツールはワイヤレスセキュリティ脅威の高まりの 3 大要因の1つであり、日本においてはワイヤレス分野の人材の最大の流出先となる可能性があります。

障壁 1：現在の能力では複雑な運用に対応しきれない

AI パラドックスの解消を阻む第 1 の障壁は、運用上の複雑化が進んでいることです。日本のほぼすべてのワイヤレスリーダー（97%）が、ワイヤレス運用が複雑化し、受け身の姿勢になることで、リソースが圧迫され、戦略的な業務が妨げられ、複雑さの軽減につながる AIOps や自動化の取り組みが直接的に損なわれていると回答しています。これにより、「複雑化により業務が受け身になる」、「受け身になることでモダナイゼーションが制約される」、「モダナイゼーションされないことで、複雑さが持続する」という悪循環が生まれています。

日本の組織は、この複雑化の 3 つの主な要因として、「新たなセキュリティリスクを軽減する必要性（48%）」、「予測できないクライアント（36%）」、「新たなユースケースの出現に伴う帯域幅の要件の高まり（35%）」を挙げています。

この複雑性は、運用面での目に見える負担として表れており、自分の所属する部門に寄せられるワイヤレス関連の対応依頼が週当たり 50 件以上という回答が 31% であったことからも、IT 部門が月に何百時間もワイヤレス関連の対応に費やす場合もあることが示されています。

懸念されるのは、このような複雑性が主な原因となって、場当たり的な対応になっていることです。回答者の 56% が、ほとんどの時間を受け身のトラブル対応やインシデント管理に費やしています。これは、戦略的なプロジェクト、研修、認定の取得、ネットワークの最適化といった先を見据えた取り組みが後回しになってしまうことを意味します。

この受け身の運用姿勢は、モダナイゼーションの取り組みを直接的に損ないます。場当たり的なトラブル対応に追われるチームは、戦略的なワイヤレス計画、研修、認定の取得、自動化の導入といった他の取り組みにリソースや注意を振り向けられない可能性があります。

この運用上の課題をさらに深刻化させる重要な要因が、可視性の欠如です。87% の組織が可視性の欠如により、Wi-Fi の問題に効果的に対応できていないと回答しています。課題として挙げられたものの上位には、クライアントの可視性、アプリケーションおよびクラウドの可視性、そしてパケットの可視性の不足があります。

エンドツーエンドの可視化ができていなければ、問題を迅速に切り分けることができません。これは、本来の原因が別にある問題のスケープゴート（責任転嫁先）としてワイヤレスネットワークが使われるという、特に危険な状況を招く要因となります。実際、53% の組織が、インシデントの 10% 以上が誤ってワイヤレスに原因があるものとされていると回答しています。

AI を活用した組織変革が進む中、ワイヤレスリーダーの大多数は、複雑化する課題を克服する最も有望な解決策は AI だと考えており、大幅な時間の短縮、ネットワーク運用の簡素化、問題対応の迅速化など、顕著で測定可能なメリットがあるとしています。

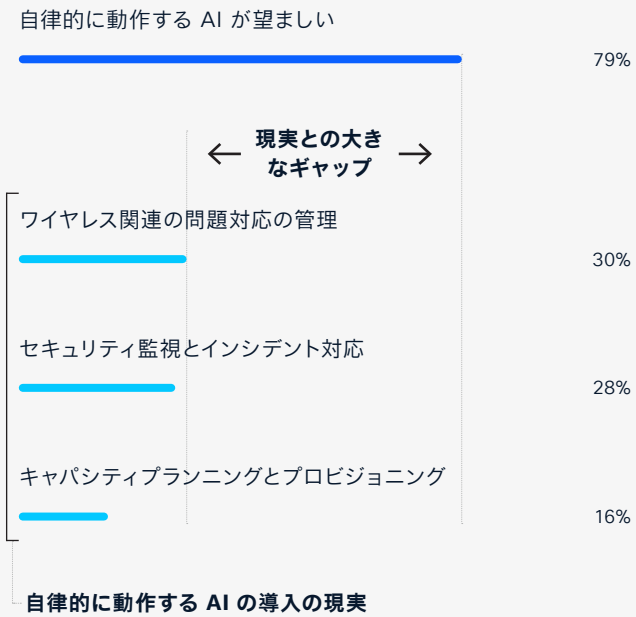
一方、日本では AI 機能をワイヤレスに展開していくにあたり、希望と現実の間に大きなギャップが存在します。

運用上の複雑さだけを見ても、ワイヤレス AI のパラドックスの解決、ひいてはワイヤレスによる ROI の強化に対する大きな課題となっています。これに、セキュリティ脅威の高まりという第 2 の障壁が重なると、組織の強靭性や業績に対する影響がさらに深刻化します。

可視性の課題に直面する組織は 87% にのぼります。

クライアントの可視化ができていない	46%
アプリケーション／クラウドの可視化ができていない	45%
パケットの可視化ができていない	33%

AI のギャップ：希望と現実



障壁 2：ワイヤレスセキュリティは包囲網の中 – IoT の普及に伴い、AI を活用した脅威に直面

ワイヤレスセキュリティは、日本の組織が AI パラドックスを解消し、ワイヤレスによる高い ROI を実現することを阻む第 2 の重大な障壁です。組織は事業に不可欠な業務のためのプラットフォームとして Wi-Fi を安心して展開することができない一方で、高まるセキュリティ脅威や経済損失の拡大に直面しています。

日本の組織の 86% が、過去 12 か月に 1 件以上のワイヤレス セキュリティ インシデントを経験しています。39% は、過去 2 年間にワイヤレス脅威が、頻度、被害、検出や復旧の難しさの点で高まったとしています。

ワイヤレスリーダーは、 AI 生成型または自動化されたサイバー攻撃をワイヤレス サイバーセキュリティの脅威の増大を招く要因トップ 3 の 1 つとして挙げています。これらの脅威は、ネットワークの脆弱性を突き、防御策に応じた攻撃戦略を練り、人間の攻撃者の能力をはるかに超える規模とスピードで攻撃を仕掛けることができます。また、AI により、Wi-Fi ネットワークに対する攻撃のハードルが低くなり、AI 生成型または自動化された脅威アクターは、巧妙で迅速な攻撃をこれまでより大幅に少ないリソースで仕掛けることが可能となっています。

日本の組織において、攻撃対象領域は拡大し続けています。インシデントに見舞われた組織の 39% が、侵害を受けた IoT や OT デバイスにより業務が中断したと回答しています。Wi-Fi は IoT で最も一般的に活用されている接続テクノロジーであるため、非常に脅威にさらされやすいことが示されています。IoT デバイスが普及し、特にデバイスが管理されていない場合、1 つの弱みがネットワーク全体を危険にさらすことになり、複合的な脆弱性につながります。

これらのセキュリティインシデントの経済的な影響は甚大です。日本の組織の 46% が、ワイヤレスセキュリティのインシデントにより経済的損失を経験しています。過去 1 年間の被害額が 100 万米ドル超であった組織は 34% に上り、これだけでも、Wi-Fi セキュリティ投資を正当化できるほど大きな経済的影響が明らかとなっています。

日本の組織におけるワイヤレス セキュリティ インシデントによる損失は、金銭面にとどまりません。26% が顧客の信頼を失い、28% が規制上の罰則やコンプライアンス上の影響に直面しているなど、評判の毀損や規制上のリスクにより、その影響はインシデントの直接的なコストをはるかに超えて広がっています。

ワイヤレスネットワークの脅威が高まる主な要因

セキュリティ強化を阻む予算やリソースの制約	31%
ユーザーの不適切な行動、人的ミス、インサイダーリスク	30%
AI 生成型または自動化されたサイバー攻撃／自動化された侵入ツール	29%
複数のセキュリティレイヤーやセグメンテーションを管理する難しさ	29%
IoT やコネクテッドデバイスの普及（デバイスの急速な拡大）	28%

一方で、多くの組織は依然として自社のワイヤレスセキュリティに信頼を寄せています。71%が今後2年間でワイヤレスセキュリティ障害が増加すると予測しているにもかかわらず、67%が「自組織はワイヤレスネットワークを十分に保護できている」と回答しています。

ワイヤレスセキュリティの向上を阻む主な 3 つの障壁として、「導入の複雑さ」、「老朽化したインフラストラクチャ」、「性能上の不安」が挙げられています。これらの障壁は単独で存在しているのではなく、人材不足、可視性の欠如、増大する運用負荷といった組織全体が抱える課題と密接に絡み合っており、セキュリティ刷新の足かせとなっています。

この結果、脆弱性のギャップはさらに拡大します。リスクが高まる中でも、組織は旧式のシステム、複雑さ、性能上の不安による制約を受け、変革を思うように進められず、レジリエンス（回復力）が低下します。

一方、証明書やプロファイルによる最新の認証を導入している組織は、より優れたセキュリティの成果を上げており、業績もこれらを導入していない組織より高いことが調査で示されています。また経済的な損失も最新の認証プロトコルを活用していない組織より平均的に低くなっています。

しかしながら、最新のセキュリティプロトコルを導入するには専門知識が必要となりますが、このような専門性を獲得するのはますます困難になりつつあります。これが第 3 の障壁、ワイヤレス人材の獲得競争です。

第 3 の障壁 : ワイヤレス分野は AI 人材の獲得競争で劣勢

第 3 の障壁は人材です。運用上の複雑さ、高まるセキュリティ脅威と並び、ワイヤレス投資の ROI最大化を阻む要因となっています。

人材不足はモダナイゼーションの進展を鈍らせるだけでなく、運用負荷の増大ややセキュリティリスクの拡大に直結し、AIOps の導入も困難にします。これにより、「人材が不足している組織はモダナイゼーションが遅れる」、「複雑さやセキュリティリスクが高まる」、「コストが上昇する」、「トップ人材がより先進的な組織に流出する」という負の連鎖が生まれます。

日本の組織の 95% が採用の課題があると回答しており、IT 人材が AI やサイバーセキュリティといったより注目度の高いテクノロジー分野を重視していると考えています。これによりスキルギャップが生じ、運用コストの上昇（45%）、士気の低下（37%）、イノベーションの停滞（35%）を招いています。

日本において人材とマイナスの結果に相関関係があることは明らかです。ワイヤレス人材の獲得が極端に困難な組織は、場当たり的な業務に費やす時間が格段に長くなります。また、影響は業務面にとどまらず、セキュリティインシデントによる年間コストも、問題なく人材を獲得できている組織より高くなります。

人材を獲得できず、認定資格を持つ人材も不足している組織は、運用コストの増加、セキュリティリスクの増大、不十分な自動化、モダナイゼーション力の低下といった複合的に不利な状況に直面しています。複雑さが増し、業務上の成功には専門スキルが欠かせないものとなり、特に人材獲得競争が激しさを増す中で、人材や認定取得にいち早く投資する組織は、高い競争力を得ることができます。

人材の危機は、ワイヤレス AI のパラドックスが、さまざまな要因が絡み合って生まれていることを示しています。AI をワイヤレス運用の中核に導入しなければ、人材を失い続けることになります。人材が不足すると、セキュリティのモダナイゼーションなどの戦略プロジェクトの実現が困難になります。最新のセキュリティが整備されていなければ、インシデントのコストが上昇し、人材とテクノロジーの双方への投資が難しくなります。

このような複合的な構図から、組織が 3 つすべての障壁に同時に対処し、パラドックスから脱却しなければならないことが示されています。

ワイヤレス人材の流出やスキル人材不足に AI が関与

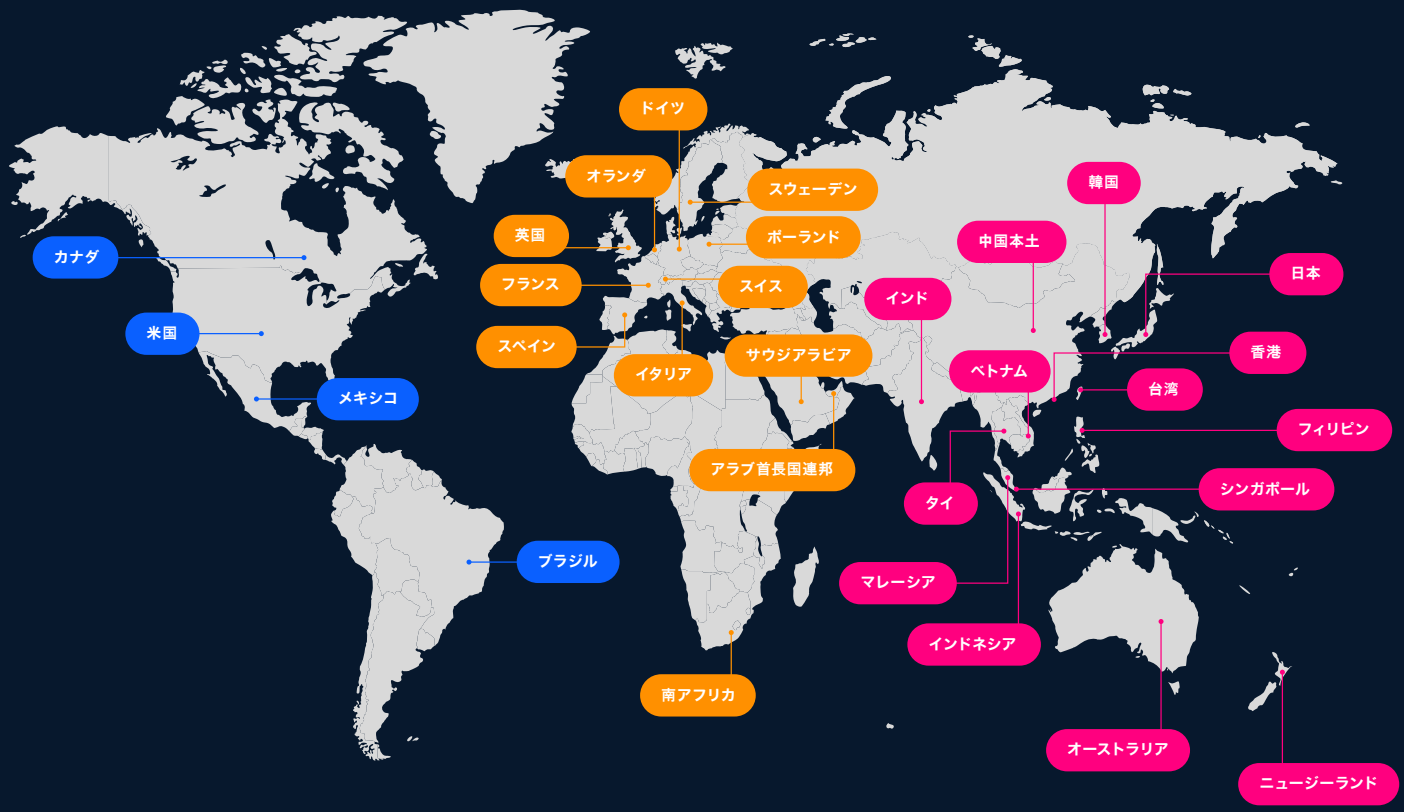
ワイヤレス人材の流出先のトップ 3

AI／機械学習	50%
サイバーセキュリティ	49%
ソフトウェア エンジニアリング／アプリ開発	36%
クラウド インフラストラクチャ／DevOps	36%

ワイヤレス人材の獲得が困難である最大の理由

高度なワイヤレスまたは AI 統合スキルを持つ求職者の不足	61%
時間のかかる採用プロセスや社内のボトルネック	35%
社内の予算上の制約や採用凍結	34%
キャリア分野としてのワイヤレスに対する関心の低さ	34%

調査方法



本調査は 30 の市場の 6,098 の組織（日本の 209 の組織を含む）におけるインタビュー調査に基づいています。調査は、2025 年 11 月に Sandpiper Research and Insights により実施されました。

調査範囲

回答者属性：社員数 250 名以上の組織に所属するワイヤレスに関する意思決定者や技術の専門家 6,098 名を対象にインタビュー調査を実施しました。10 名中 6 名（61%）の回答者が年間売上高 1 億米ドル以上の組織に所属しています。

南北アメリカ — 22%

欧州、中東、アフリカ — 28%

アジア太平洋 — 50%

調査対象地域：本調査は、オーストラリア、ブラジル、カナダ、中国本土、フランス、ドイツ、香港、インド、インドネシア、イタリア、日本、マレーシア、メキシコ、オランダ、ニュージーランド、フィリピン、ポーランド、サウジアラビア、シンガポール、南アフリカ、韓国、スペイン、スウェーデン、スイス、台湾、タイ、アラブ首長国連邦、英国、米国、ベトナムの 30 市場で実施されました。

調査対象業界：事業サービス、建設、教育、エンジニアリング、設計・建築、金融サービス、政府・公共サービス、医療、製造、メディア・通信、天然資源、不動産、飲食サービス、小売、テクノロジーサービス、運輸、旅行サービス、卸売業など、幅広い業界から回答を得ました。

調査時期：本調査は 2025 年 11 月に実施されました。

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**