JAC WiFi Performance Investigation & Remediation Report

JAC WiFi パフォーマンス調査・改善レポート

Prepared for / 宛先

Mr. Yasushi Oyama, Japan Activation Capital

尾山 康 様, ジャパン・アクティベーション・キャピタル

April 2, 2026 / 2026 年 4 月 2 日

English Version

See page 12 →

日本語版

3 ページへ →

eSolia

JAC WiFi パフォーマンス調査・改善レポート

宛先

尾山 康 様, ジャパン・アクティベーション・キャピタル

2026 年 4 月 2 日

目次

概要

JAC 法人用 SSID「JAC」の WiFi スループットが、導入時の約 300Mbps から約 6〜7Mbps（クライアントのレポーティングマネージャーからの報告）に低下していた問題について、イソリアにて体系的な調査を実施し、複数の要因を特定の上、対処を行いました。すべての最適化適用後、Windows 端末で 5GHz 帯にて 170Mbps、iPhone で 6GHz 帯にて 499Mbps まで回復し、報告時のベースラインと比較して最大 24 倍の改善を達成しました。

問題の内容

JAC 法人 WiFi ネットワークの利用者から、インターネット接続が著しく遅いとの報告がありました。クライアントのレポーティングマネージャーからは WiFi 速度テスト結果が約 6〜7Mbps であるとの報告がありましたが、テスト時の端末、帯域、アクセスポイント等の詳細は記録されていませんでした。イソリアの診断テストでも、WiFi でのダウンロード速度が約 7Mbps であるのに対し、同一ネットワーク上の有線接続では約 700Mbps であることが確認されました。WiFi の速度は有線の約 1% に低下しており、すべての WiFi クライアントおよびすべてのアクセスポイントで同様の症状が発生していました。

導入時（稼働開始時点）には、WiFi スループットは約 300Mbps を記録しており、複数のテスト端末でストリーミングサービスも問題なく動作していました。

原因分析

調査の結果、主に 2 つの要因が特定されました。

1. セキュリティ検査による過剰な CPU 負荷

WiFi からインターネットへのトラフィックを制御する FortiGate ファイアウォールポリシーに、アンチウイルス、侵入防止（IPS）、VoIP 検査、ファイルフィルタリングを含む 8 つのセキュリティ検査プロファイルが同時に有効化されていました。これらのプロファイルはディープパケットインスペクション（DPI）が有効な場合に効果を発揮しますが、現在の SSL 検査モード（証明書検査）ではトラフィックの復号化を行わないため、4 つのプロファイルはセキュリティ上の実質的な効果がないまま CPU リソースを消費していました。この CPU 負荷は、FortiGate が WiFi セッションを有線セッションとは異なる方式で処理するため、WiFi トラフィックに対して不均衡に大きな影響を与えていました。

2. クライアントの帯域選択

アクセスポイントからの積極的な誘導がない状態では、多くのクライアント端末がより高速な 5GHz や 6GHz 帯ではなく、2.4GHz 帯に接続していました。2.4GHz 帯は利用可能な帯域幅が大幅に少なく、オフィス環境では干渉の影響を受けやすい特性があります。1 フロアに 6 台のアクセスポイントが設置されている環境では、2.4GHz 帯での同一チャネル干渉が問題をさらに深刻化させていました。

実施した変更

すべての変更は 2026 年 4 月 2 日に適用済みであり、即時有効です。

セキュリティポリシーの最適化

現在の検査モードでは実質的な保護効果がない 4 つのセキュリティプロファイルを、WiFi インターネットアクセスポリシーから削除しました。Web フィルタ、アプリケーション制御、DNS フィルタリングは引き続き有効であり、実質的なセキュリティレベルの低下はありません。

プロファイル	状態
Web フィルタ	有効（変更なし）
アプリケーション制御	有効（変更なし）
DNS フィルタ	有効（変更なし）
SSL 証明書検査	有効（変更なし）
アンチウイルス	削除（証明書検査モードでは無効）
侵入防止（IPS）	削除（証明書検査モードでは無効）
ファイルフィルタ	削除（証明書検査モードでは無効）
VoIP 検査	削除（証明書検査モードでは無効）

WiFi 帯域ステアリング

クライアント端末をより高速な 5GHz および 6GHz 帯へ誘導する機能を有効化しました。端末の信号が弱い場合、システムがより強い電波のラジオへの再接続を促すことで、個々の端末およびネットワーク全体のパフォーマンスが向上します。

5GHz チャネル幅の拡大

5GHz ラジオのチャネル幅を 40MHz から 80MHz に拡大しました。これにより、5GHz 帯におけるクライアント1 台あたりの利用可能帯域が実質的に倍増します。

自動チャネル管理

2.4GHz ラジオに自動無線リソース制御（DARRP）を有効化しました。これにより、アクセスポイントが自動的に最も混雑の少ないチャネルを選択し、6 台のアクセスポイント間の同一チャネル干渉を低減します。チャネル最適化は業務時間中の一時的な切断を避けるため、毎晩 1:00～1:30 に実行されます。

アクセスポイントの復旧

以前のトラブルシューティング時に物理的に切断されていた 2 台のアクセスポイント（JAC-431G-03 および JAC-431G-05）を再接続し、正常稼働を確認しました。現在 6 台すべてのアクセスポイントが稼働しており、クライアント負荷がより均等に分散され、カバレッジも改善されています。

テスト結果

改善前（ベースライン）

指標	値
WiFi ダウンロード（クライアント報告）	約 6～7 Mbps
WiFi ダウンロード（イソリア確認）	約 7 Mbps
有線ダウンロード（同一ポリシー）	約 700 Mbps
WiFi vs 有線パフォーマンス	約 1%
iPhone 接続状況	WiFi 経由で Web ページの読み込み不可

第 1 回テスト: セキュリティポリシー最適化後

テスト	端末	帯域	ダウンロード	アップロード
自然接続	Windows PC	5 GHz	160 Mbps	110 Mbps
5GHz 固定	Windows PC	5 GHz	160 Mbps	120 Mbps
2.4GHz 固定	Windows PC	2.4 GHz	21 Mbps	24 Mbps
自然接続	iPhone	不明	失敗（0.7～16 Mbps で不安定）	—

第 2 回テスト: 全最適化適用後（帯域ステアリング、80MHz チャネル、AP 復旧）

テスト	端末	帯域	ダウンロード	アップロード
自然接続	Windows PC	5 GHz	160 Mbps	190 Mbps
5GHz 固定	Windows PC	5 GHz	170 Mbps	210 Mbps
2.4GHz 固定	Windows PC	2.4 GHz	32 Mbps	21 Mbps
自然接続	iPhone	6 GHz（推定）	**499 Mbps**	113 Mbps

改善効果まとめ

指標	改善前	改善後	改善倍率
Windows 5GHz ダウンロード	約 7 Mbps	170 Mbps	**24 倍**
Windows 5GHz アップロード	—	210 Mbps	—
Windows 2.4GHz ダウンロード	—	32 Mbps	—
iPhone ダウンロード	接続失敗	499 Mbps	**完全復旧**
iPhone アップロード	接続失敗	113 Mbps	**完全復旧**

今後の推奨事項

iPhone の接続問題は解決済み。 初回テストでは、iPhone 端末が JAC SSID に安定して接続できない事象が確認されましたが、デュアルバンドネイバーレポートおよびクライアントステアリング機能の有効化後、iPhone は 499Mbps を達成し、全テスト中最速の結果となりました。現時点で iPhone の接続に関する追加対応は不要です。

2.4GHz 帯のさらなる改善見込み。 自動チャネル管理（DARRP）を有効化しましたが、初回の最適化サイクルはまだ実行されていません（毎晩 1:00 AM に実行予定）。現在の 2.4GHz 帯での 32Mbps は、アクセスポイントが重複しないチャネルに再配置された後にさらに改善が見込まれます。

ファームウェアのアップグレード計画。 現在の FortiGate ファームウェア（v7.4.5）には、WiFi トラフィックのハードウェアアクセラレーションに関する制限がある可能性があります。必要に応じてイソリアにて Fortinet 社と連携し、FortiOS 7.6.x へのアップグレードによる改善効果を評価いたします。

SSID リファレンス: JAC と JAC2

スタッフ向けに 2 つの法人 SSID が利用可能です。**JAC が主要ネットワークであり、可能な限り常に JAC を使用してください。** JAC2 は、JAC のセキュリティ要件に対応できない旧型デバイス向けの非表示フォールバックネットワークです。

設定項目	JAC（メイン）	JAC2（レガシー用）
SSID 名	JAC	JAC2
WiFi 一覧に表示	はい	いいえ（非表示 — 手動入力が必要）
セキュリティプロトコル	WPA3-SAE	WPA2-PSK
保護された管理フレーム（PMF）	必須	不要
H2E（Hash-to-Element）	必須	該当なし
利用可能帯域	2.4 GHz、5 GHz、6 GHz	2.4 GHz、5 GHz、6 GHz
対象デバイス	最新のノート PC・スマートフォン・タブレット（2020 年以降のモデル）	旧型デバイス、プリンター、IoT 機器、または JAC に接続できないデバイス
パスワード	別途提供	別途提供

JAC を強く推奨する理由

JAC は **WPA3-SAE**（Simultaneous Authentication of Equals）を採用しており、現行の企業向け WiFi セキュリティ標準です。JAC2 は **WPA2-PSK**（Pre-Shared Key）を採用しており、これは家庭用ルーターに搭載されている旧世代のコンシューマー向け標準です。セキュリティ上の差は大きく、主な違いは以下の通りです。

WPA3-SAE では、すべてのユーザーが同じパスワードを共有していても、各デバイスの接続が個別に保護されます。攻撃者が他のユーザーの WiFi トラフィックを傍受しても、その内容を復号化することはできません。また、オフライン辞書攻撃も防止されます。攻撃者が認証時のハンドシェイクを記録し、別のコンピューターで後からパスワードの解析を試みることもできません。

WPA2-PSK では、すべてのユーザーに同一の共有鍵が使用されます。パスワードを知っているユーザーは、同一ネットワーク上の他のユーザーのトラフィックを傍受・復号化できる可能性があります。認証時のハンドシェイクも、オフラインでのブルートフォース攻撃に対して脆弱です。

これらの理由から、**デバイスが技術的に接続できない場合を除き、すべてのスタッフは JAC に接続してください。** JAC2 は恒久的な代替手段ではなく、一時的な回避策として位置付けられています。

旧型ノート PC への推奨対応

ノート PC の内蔵 WiFi チップが古いために JAC ネットワークに接続できない場合、**USB WiFi 6E アダプター**が実用的かつ費用対効果の高い解決策です。一般的に JPY 6,000〜JPY 8,000 程度で、WPA3 の完全サポートに加え、5GHz および 6GHz 帯での高速通信が可能になります。これにより、旧型デバイスでもより安全な JAC ネットワークに接続しつつ、スループットの改善も享受でき、JAC2 を長期的に使用するよりも望ましい対応です。調達についてはイソリアまでお問い合わせください。

JAC2 の使用が推奨されるケース: デバイスが JAC ネットワークに接続できない場合、または接続後に接続断や認証失敗が繰り返し発生する場合は、一時的な対処として JAC2 への接続をお試しください。JAC2 は非表示 SSID のため、デバイスの WiFi 設定で SSID 名を手動入力する必要があります。どちらのネットワークを使用すべきか不明な場合は、イソリアまでお問い合わせください。

環境概要

構成要素	詳細
ファイアウォール	FortiGate 121G（HA アクティブ・パッシブ構成）、FortiOS v7.4.5
スイッチ	FortiSwitch 448E-FPOE、v7.4.3
アクセスポイント	FortiAP 431G × 6 台、ファームウェア v7.4.4
インターネット回線	1 Gbps 光回線
フロア	POLA 11F、単一フロア構成

お問い合わせ

株式会社イソリア 〒105-7105 東京都港区東新橋 1-5-2 汐留シティセンター 5 階 (Workstyling)

電話	03-4577-3380
メール	rick.cogley@esolia.co.jp
Web	https://esolia.co.jp
営業時間	月～金、9:00～18:00

eSolia

JAC WiFi Performance Investigation & Remediation Report

Prepared for

Mr. Yasushi Oyama, Japan Activation Capital

April 2, 2026

Contents

Summary

WiFi throughput on the JAC corporate SSID had degraded from approximately 300 Mbps at initial deployment to 6–7 Mbps as reported by the client's reporting manager. eSolia conducted a systematic investigation, identified multiple contributing factors, and applied targeted fixes. After all optimizations, throughput has been restored to 170 Mbps on 5 GHz for Windows devices and 499 Mbps for iPhone on 6 GHz — representing a 24× improvement over the reported baseline.

Problem Description

Users on the JAC corporate WiFi network reported significantly slow internet performance. The client's reporting manager confirmed WiFi speed test results of approximately 6–7 Mbps, though details of which device, band, or access point were not recorded at that time. eSolia's own diagnostic testing confirmed download throughput of approximately 7 Mbps over WiFi, compared to approximately 700 Mbps for wired connections on the same network — a 99% reduction. The issue affected all WiFi clients and all access points.

At the time of initial deployment (go-live), WiFi throughput was measured at approximately 300 Mbps, and streaming services functioned without issue across multiple test devices.

Root Cause Analysis

The investigation identified two primary contributing factors.

1. Excessive security inspection overhead

The FortiGate firewall policy governing WiFi-to-internet traffic had eight security inspection profiles enabled simultaneously, including antivirus scanning, intrusion prevention (IPS), VoIP inspection, and file filtering. While these profiles provide value when deep packet inspection is active, the current SSL inspection mode (certificate inspection) does not decrypt traffic. As a result, four of these profiles were consuming CPU resources without providing meaningful security benefit. This CPU overhead disproportionately affected WiFi traffic due to the way the FortiGate processes wireless sessions compared to wired sessions.

2. Client band selection

Without active guidance from the access points, many client devices were connecting on the 2.4 GHz band instead of the faster 5 GHz or 6 GHz bands. The 2.4 GHz band has significantly less available bandwidth and is more susceptible to interference in an office environment. With six access points on a single floor, co-channel interference on 2.4 GHz further compounded the problem.

Changes Applied

All changes were applied on April 2, 2026 and are immediately effective.

Security Policy Optimization

Four security profiles that provided no effective protection under the current inspection mode were removed from the WiFi internet access policy. The remaining profiles — web filtering, application control, and DNS filtering — continue to provide active protection. There is no reduction in meaningful security coverage.

Profile	Status
Web Filter	Active (unchanged)
Application Control	Active (unchanged)
DNS Filter	Active (unchanged)
SSL Certificate Inspection	Active (unchanged)
Antivirus	Removed (ineffective under certificate inspection)
Intrusion Prevention	Removed (ineffective under certificate inspection)
File Filter	Removed (ineffective under certificate inspection)
VoIP Inspection	Removed (ineffective under certificate inspection)

WiFi Band Steering

Client steering features were enabled to guide devices toward the faster 5 GHz and 6 GHz bands. When a device maintains a weak signal, the system will encourage it to reconnect to a stronger radio, improving both individual and overall network performance.

5 GHz Channel Widening

The 5 GHz radio channel width was increased from 40 MHz to 80 MHz, effectively doubling the available bandwidth per client on the 5 GHz band.

Automatic Channel Management

Automatic radio resource provisioning (DARRP) was enabled on the 2.4 GHz radios. This allows the access points to automatically select the least congested channel, reducing co-channel interference between the six access points. Channel optimization runs nightly between 1:00 and 1:30 AM to avoid any momentary disruption during business hours.

Access Point Restoration

Two access points (JAC-431G-03 and JAC-431G-05) that had been physically disconnected during previous troubleshooting were reconnected and confirmed operational. All six access points are now active, distributing the client load more evenly and providing better coverage.

Test Results

Before remediation (baseline)

Metric	Value
WiFi download (client report)	~6–7 Mbps
WiFi download (eSolia confirmed)	~7 Mbps
Wired download (same policy)	~700 Mbps
WiFi performance vs. wired	~1%
iPhone connectivity	Unable to load web pages on WiFi

Round 1: After security policy optimization

Test	Device	Band	Download	Upload
Natural connection	Windows PC	5 GHz	160 Mbps	110 Mbps
Forced 5 GHz	Windows PC	5 GHz	160 Mbps	120 Mbps
Forced 2.4 GHz	Windows PC	2.4 GHz	21 Mbps	24 Mbps
Natural connection	iPhone	Unknown	Failed (0.7–16 Mbps fluctuation)	—

Round 2: After all optimizations (band steering, 80 MHz channels, AP restoration)

Test	Device	Band	Download	Upload
Natural connection	Windows PC	5 GHz	160 Mbps	190 Mbps
Forced 5 GHz	Windows PC	5 GHz	170 Mbps	210 Mbps
Forced 2.4 GHz	Windows PC	2.4 GHz	32 Mbps	21 Mbps
Natural connection	iPhone	6 GHz (est.)	**499 Mbps**	113 Mbps

Improvement summary

Metric	Before	After	Improvement
Windows 5 GHz download	~7 Mbps	170 Mbps	**24×**
Windows 5 GHz upload	—	210 Mbps	—
Windows 2.4 GHz download	—	32 Mbps	—
iPhone download	Failed	499 Mbps	**Fully restored**
iPhone upload	Failed	113 Mbps	**Fully restored**

Ongoing Recommendations

iPhone connectivity resolved. During initial testing, an iPhone device was unable to reliably connect to the JAC SSID. After enabling dual-band neighbor reports and client steering, the iPhone achieved 499 Mbps — the fastest result of all tests. No further action is required for iPhone connectivity at this time.

2.4 GHz performance expected to improve further. Automatic channel management (DARRP) was enabled but has not yet completed its first optimization cycle (scheduled nightly at 1:00 AM). The current 32 Mbps on 2.4 GHz should improve once the access points redistribute across non-overlapping channels.

Future firmware planning. The current FortiGate firmware (v7.4.5) may have limitations in hardware acceleration for WiFi traffic. eSolia can track this with Fortinet as needed and evaluate whether an upgrade to FortiOS 7.6.x addresses the issue, which could yield additional throughput improvements.

SSID Reference: JAC vs JAC2

Two corporate SSIDs are available for staff use. **JAC is the primary network and should always be used when possible.** JAC2 is a hidden fallback network for older devices that cannot connect to JAC due to its stricter security requirements.

Setting	JAC (Primary)	JAC2 (Legacy Fallback)
SSID name	JAC	JAC2
Visible in WiFi list	Yes	No (hidden — must be entered manually)
Security protocol	WPA3-SAE	WPA2-PSK
Protected Management Frames	Required	Not required
H2E (Hash-to-Element)	Required	Not applicable
Available bands	2.4 GHz, 5 GHz, 6 GHz	2.4 GHz, 5 GHz, 6 GHz
Target devices	Modern laptops, phones, tablets (2020 and newer)	Older devices, printers, IoT, or any device unable to connect to JAC
Password	Provided separately	Provided separately

Why JAC is strongly preferred

JAC uses **WPA3-SAE** (Simultaneous Authentication of Equals), the current enterprise-grade WiFi security standard. JAC2 uses **WPA2-PSK** (Pre-Shared Key), which is the older consumer-grade standard found on home routers. The security difference is significant:

WPA3-SAE protects each device's connection individually, even when all users share the same password. An attacker who captures another user's WiFi traffic cannot decrypt it. WPA3 also prevents offline dictionary attacks — an attacker cannot record authentication handshakes and attempt to crack the password later on a separate computer.

WPA2-PSK uses a shared key that is identical for all users. Any user who knows the password can potentially capture and decrypt other users' traffic on the same network. The authentication handshake is also vulnerable to offline brute-force cracking.

For these reasons, **all staff should connect to JAC unless their device is technically unable to do so.** JAC2 should be treated as a temporary workaround, not a permanent alternative.

Recommendation for older laptops

If a laptop cannot connect to the JAC network due to an older built-in WiFi chip, a **USB WiFi 6E adapter** is a practical and cost-effective solution. These adapters typically cost JPY 6,000–JPY 8,000 and provide full WPA3 support along with the faster speeds available on 5 GHz and 6 GHz bands. This allows the device to connect to the more secure JAC network while also benefiting from improved throughput, and is preferable to using JAC2 long-term. Contact eSolia to arrange procurement.

When to use JAC2: If a device cannot connect to the JAC network, or connects but experiences persistent issues (such as repeated disconnections or failure to authenticate), try connecting to JAC2 as a temporary measure. Since JAC2 is hidden, the SSID name must be entered manually in the device's WiFi settings. Contact eSolia if you are unsure which network a device should use.

Environment Summary

Component	Details
Firewall	FortiGate 121G (HA active-passive pair), FortiOS v7.4.5
Switch	FortiSwitch 448E-FPOE, v7.4.3
Access Points	6× FortiAP 431G, firmware v7.4.4
Internet	1 Gbps fiber
Floor	POLA 11F, single floor deployment

Contact Us

eSolia Inc. Shiodome City Center 5F (Workstyling) 1-5-2 Higashi-Shimbashi, Minato-ku Tokyo 105-7105, Japan

Phone	03-4577-3380
Email	rick.cogley@esolia.co.jp
Web	https://esolia.co.jp/en
Hours	Monday-Friday, 9:00-18:00 JST