2026/4/27 版

FortiClient での IPsec-VPN 接続手順のメモ

これは、テスト中のあれこれをメモした程度のドキュメントです。
公開できるマニュアルの下書きの下書きレベルであることをご理解ください。

1. 事前に Windows をアップデートした方がいいかも

Win7 時代にブルースクリーンで起動しなくなったケースがありますが
回復(復元ポイント)でインストール前に戻す
Windows アップデートを行なう
FortiClient を再インストールする
で、OS が正常に戻り、FortiClient も使えるようになりました。
ただし、その後に Windows のアップデートを実施したら再度ブルースクリーンになり、Windows が起動しなくなりました。
また、このケースでは FortiClient インストール前に回復しますので再インストールが必要で、ブルースクリーンの繰り返しになりました。
※何かのドライバと FortiClient の相性が悪い可能性が考えられますので
PC の環境依存の可能性が高いと思われます。(b-mobile のドライバとの相性？)

2. FortiClient をダウンロードする

メーカーのダウンロードサイトからインストーラーを入手してください
https://www.fortinet.com/support/product-downloads
の FortiClient VPN only (DIY, no support) ←※これ以外は商用版なので使用 NG です。
で OS 毎の必要なインストーラーをダウンロードしてください。
最近は、ダウンロード時に氏名、国、所属、メールアドレスの入力を要求されるようになりました。現在は Ver7.4 系で、クライアントは 9 種類あります。

VPN for Windows	←通常はこれです
VPN for Mac	←通常はこれです
VPN for Linux .rpm	←CPU が Intel/AMD の RedHat 系(動作検証無し)
VPN for Windows 64-arm	←CPU が ARM の Windows(動作検証無し)
VPN for Linux 64-arm .rpm	←CPU が ARM の RedHat 系(動作検証無し)
VPN for Linux 64-arm .deb	←CPU が ARM の Debian 系(動作検証無し)

VPN for iOS　←iPhone、iPad 用(以前に SSL-VPN でテストした結果は後述)
VPN for Android　←Google の Play ストアで Forticlient VPN をダウンロードするのがいいかもしれません(2026/4 検証)
VPN for Linux .deb　←CPU が Intel/AMD の Debian 系(動作検証無し)

※注
Win11+FortiClient7.4 で動作不良を起こしたケースがありました。(2024 年 8 月確認)
Mac と FortiClient7.4 で正常に起動しない状況を確認しました。(2024 年 8 月確認)
※Win11 での動作不良は、2025 年初め辺りの OS アップデートで解消しているようです。

オンラインインストールした場合、メーカー側がバグ修正して、ダウンロード先のサーバ上のソフトがアップデート済になっている場合があります。そのため使用している PC 毎に微妙なバージョン違いが発生することがあり、全ての PC、Mac でこの不具合が発生するか？は正直判りません。また、Windows 側のアップデートで不具合が解消する場合もあります。

もし、オンラインインストールした FortiClient7.4 で動作に問題がある場合は、ネットワーク室の NAS で FortiClient7.2 を提供していますので、それをお使いください。
¥¥172.20.90.4¥Forticlient
でネットワーク室の NAS を検索し、「guest」で認証
7.2 のインストーラーを PC、Mac にコピーする。
なお、ネットワーク室の NAS は金研 F/W 内なので、ご自宅等からアクセスできません。
そのため、金研の Web サーバ経由で入手できるようにしました。
FortiClient7.4 よりも旧バージョンが必要な場合は、以下の URL から 7.2 のインストーラーをダウンロードしてください。
・Windows 版 7.2 オフラインインストーラー(約 150M)
https://www.network.imr.tohoku.ac.jp/Jpn/Forticliernt/FortiClientVPN_7.2.3.929.exe
・Mac 版 7.2 オフラインインストーラー(約 250M)
https://www.network.imr.tohoku.ac.jp/Jpn/Forticliernt/FortiClient7.2.dmg

※2026/4/27 追記、修正

MacOS、iOS(iPhone、iPad)での VPN 接続について、加筆、修正しました。

・スマホ(Android)からの利用について

2026/4/15 に Android 版「Forticlient VPN」を使って VPN 接続できること確認しました。

動作検証した時点のバージョンは 7.4.6.0218 です。

※「Forticlient」というアプリもあるのですが、それはテストしていません

設定手順は

https://www.network.imr.tohoku.ac.jp/Jpn/pdf/ipsec-vpn/android.pdf

にマニュアル化しました。

スマホを使った VPN 接続で、できることは限られていますが、「PC を持っていない時に出先から所内の Web カメラを確認する」みたいな用途では使えそうです。

動作検証も、eduroam 経由、ドコモ回線経由の両方で VPN 接続を行い、ブラウザの Chrome で金研の大判プリンタ監視用ライブカメラの URL にアクセスして、ライブ動画が視聴できることで確認しました。

・iPhone/iPad(iOS) からの利用について

2026/4/17 の検証結果です。

現時点での結論：

Forticlient を使わずに、OS 標準の VPN(IPsec あるいは L2TP)を使用してください

・Forticlient　　接続 NG

・iPhone/iPad(iOS)の VPN 接続機能

(1)　IPsec を選択した場合(iPad で確認)

設定

→一般

→VPN とデバイス管理

→VPN をクリック

→VPN 構成を追加

タイプ　IPsec を選択、戻る

説明　　「IMR IPsec」等、他と重複しない名前を付ける

サーバ　　130.34.226.250

アカウント　　通知された金研 VPN サービスのユーザーID

パスワード　　ここで入力する場合は

　　通知された金研 VPN サービスのパスワード

証明書を使用　　OFF

グループ名　　IPsec-user
シークレット　　通知された事前共有キー(漏洩防止のため書きません)
を正しく入力して「完了」

VPN 接続が複数ある場合は、いずれかを選択(チェックマークが付く)
使用する時は「VPN」のスイッチを ON にする
正常に接続できると
　状況　スイッチが緑色に変化
　「接続済み」の表示
　右上に"VPN"の表示
となります。

(2)　L2TP を選択した場合(iPad で確認)
2026/4/17 の作業で、NAT 経由で複数の機器を同時に L2TP 接続した時に
1 台目以外が通信できない状況は親機の設定変更で解消しました。
https://www.tains.tohoku.ac.jp/contents/uploads/l2tp-ios.pdf
を金研向けの設定に読み替えることで VPN 接続できることは確認しています。
設定
→一般
→VPN とデバイス管理
→VPN をクリック
→VPN 構成を追加
タイプ　L2TP を選択、戻る

説明	「IMR L2TP」等、他と重複しない名前を付ける
サーバ	130.34.226.250
アカウント	通知された金研 VPN サービスのユーザーID
RSA SecureID	無効
パスワード	ここで入力する場合は 通知された金研 VPN サービスのパスワード
シークレット	通知された金研 VPN サービスの事前共有キー (漏洩防止のため、ここには書きません)
すべての信号を送信	ON

を正しく入力して「完了」

VPN 接続が複数ある場合は、いずれかを選択(チェックマークが付く)
使用する時は「VPN」のスイッチを ON にする

正常に接続できると
　状況　スイッチが緑色に変化
　「接続済み」の表示
　右上に"VPN"の表示
となります。

・MacOS からの利用について
基本としては、Forticlient の利用を推奨します。ただし、MacOS、Forticlient のいずれかのバージョンアップの際に、たびたび動作不良、接続不良が発生しています。
Forticlient が正常に起動しない、接続できない場合、MacOS の標準の VPN(「Cisco IPsec」あるいは　「L2TP」)を使用してください。

(1)　MacOS で「Cisco IPsec」を選択した場合
MacOS の「Cisco IPsec」の設定手順はこのようになります。
システム設定
→　ネットワーク
→　VPN をクリック
→　VPN 構成を追加
→　「Cisco IPsec」を選択

表示名	「IMR IPsec」等、他と重複しない名前を付ける
サーバアドレス	130.34.226.250
アカウント名	通知された金研 VPN サービスのユーザーID
パスワード	ここで入力する場合は 通知された金研 VPN サービスのパスワード

認証

種類	「共有シークレット」を選択
共有シークレット	通知された事前共有キー(漏洩防止のため書きません)
グループ名	IPsec-user

を正しく入力して「作成」で設定、接続できることを確認しています。

(2)　MacOS で「L2TP」を選択した場合

MacOS の「L2TP」の設定手順はこのようになります。

全学の VPN サービスの設定

https://www2.tains.tohoku.ac.jp/remote/remote-access

(学内限定)

の Mac の L2TP/IPsec と同様の設定で

サーバアドレス	130.34.226.250
アカウント	金研のもの
パスワード	金研のもの
共有シークレット	通知された事前共有キー(漏洩防止のため書きません)

と、金研の内容に読み替えて入力、

「全てのトラフィックを VPN 接続経由で送信」

を有効にすることで設定、接続できることを確認しています。

3.　FortiClient をインストールする

FortiClient は金研内でインストール可能ですが、VPN 接続本来の目的が「外部からの接続」なので、金研内の PC から VPN 接続を行うことに意味はありません。

そのため、設定確認、認証テストまでの場合は所内の有線 LAN、設定確認以降の実際の通信テストは金研内の場合は無線 LAN の「eduroam」あるいは所外(ご自宅、モバイルルータ等、利用する場所)で行ってください。

所内で「eduroam」が使用可能な場所は以下の通り(所内からのアクセス限定)

https://www.network.imr.tohoku.ac.jp/Jpn/inside/wireless_in.html

インストール作業はインストーラーが必要なソフトウェア等をネットワーク経由でダウンロードしながら進みますので、PC をネットワークに繋いだ状態で操作します。

Windows 版での経験からですが、結構時間がかかります(進んでないかと心配になる位)。

また、インストール後に再起動が必要になる場合があります。

PC の再起動を要求されるケースとされないケースがありますが(この違いの理由は不明)、再起動後もインストール作業が継続するので、実際にソフトが起動して利用 OK になるまで結構時間がかかります。インストールについては終了まで気長に待ってください。

4.　FortiClient を設定する

初回は

IPsec VPN を選択

接続名をつける	例：IMR、金研、金研 IPsec 等任意 ※SSL-VPN と同じ名前を使う場合は、SSL-VPN のサービス終了後に SSL-VPN の設定を削除して IPsecVPN の名前を修正してください
リモート GW	130.34.226.250 ※サーバ証明書の事情からホスト名は使用しません 130.34.x.x の IP アドレスは東北大学、 130.34.226.x の IP アドレスは金研と 割り当てを受けていますので、IP アドレスで 正規な機器と判断することができます。
認証方式	「事前供給鍵」を選択(デフォルトで選択済) ここで入力する事前共有鍵の内容は、利用許可のメールでユーザーに直接連絡します。 マニュアル、ドキュメントには記載しません。 ※これは、2025 年 12 月に発生したインシデントで

他部局で
「Web で公開していたドキュメントに記載した
供給鍵を不正侵入者に読まれた可能性がある」
という話があり、ドキュメント類へ記載して
公開するのは危険と判断したためです。

「ユーザー名入力」の場合　　毎回入力が必要
「ユーザー名を保存」の場合　　ソフトが設定を覚えて毎回表示します
パスワードについては毎回入力が必要です。
これは「不正利用防止のため」だと思いますが、FortiClient は覚えてくれません。

+詳細設定をクリックして開いた先の
-VPN 設定
-フェーズ 1
-フェーズ 2
については、以下のような設定変更が必要な場合があります。
ユーザーの環境や使い方に依存しますので、全員同じではありません。
※注 2026/4./6 修正
VPN 接続中に自宅ネットワーク内に機器(NAS、プリンタ)を使用したい場合は
「ローカル LAN の有効化」にチェックを入れる必要があるようです。
なお、バージョンによってはこの設定が無い場合があります。

Win 版 FortiClient の 7.4.3 よりも古いバージョンを使っている場合(7.2 系で確認済)
・フェーズ 1 の DH グループを 5→20 にチェックを変更
・フェーズ 2 の DH グループを 5→20 にプルダウンを変更
をしないとリンクダウンが発生して、IPsec-VPN の接続ができません。
DH グループは暗号化強度を決定するパラメータで、
・親機(VPN の接続先)とクライアントで設定を揃える必要がある
・「5」の設定には脆弱性があり、使用が推奨されなくなった
・7.4.3 から初期設定で「20」となった
・「20」は楕円曲線暗号を使用していて低負荷・高速、パフォーマンスがいい
という事情から、
初期設定で「5」になっている Win 版 FortiClient は「20」への設定変更が必須
です。7.4.3 よりも古いバージョンの Win 版 FortiClient を使っているユーザーが接続できない場合は、詳細設定の DH グループの数値を確認してください。

Mac 版 FortiClient ですが、DH グループの「19」「20」は設定項目にありますが、
サポートされていません。そのため Win 版 FortiClient は「20」の設定が OK なのに
Mac 版 FortiClient で「20」を設定しても、接続エラーが発生します。
親機側で「18」が使えるように設定を追加しましたので
・フェーズ 1 の DH グループは「18」にチェックを変更
・フェーズ 2 の DH グループは「18」にプルダウンを変更
をしないとリンクダウンが発生して、IPsec-VPN の接続ができません。
Mac 版 FortiClient では「18」の設定必須です。

2 回目以降は PC 起動で常駐しているので、Windows11 の場合、
タスクトレイの「＾」→青色のアイコンを右クリック
→「ユーザーが設定した接続名(IMR 等)に接続」で、ソフトが起動し認証画面が出ます。
また、おそらく初回のみだと思いますが、OS にネットワークの種類の指定を聞かれた場合は、「プライベート」にします。もし「パブリック」になってしまうと NAS と通信できない等になると思うので、その場合は「プライベート」に切り替える必要があります。

設定が終わって IPsec-VPN で接続できてしまうと、あまり確認する必要はないのですが、IPsec-VPN 用の仮想 I/F はこのような感じです。
ipconfig /all で確認

接続固有の DNS サフィックス	:
説明	: Fortinet Virtual Ethernet Adapter (NDIS 6.30)
物理アドレス	: 00-09-0F-FE-00-01
DHCP 有効	: はい
自動構成有効	: はい
リンクローカル IPv6 アドレス	: fe80::8518:c4d8:1d8d:d4bd%26(優先)
IPv4 アドレス	: 172.31.41.2(優先)
サブネット マスク	: 255.255.255.255
リース取得	: 2026 年 3 月 11 日 13:50:32
リースの有効期限	: 2162 年 4 月 17 日 20:48:01 ←機器の仕様で 100 年以上先の日付になるとのこと (気にしなくて OK)
デフォルト ゲートウェイ	: 172.31.41.3
DHCP サーバー	: 172.31.41.3
DHCPv6 IAID	: 436209935
DHCPv6 クライアント DUID	: 00-01-00-01-2B-48-34-BB-B8-20-8E-27-A5-72
DNS サーバー	: 172.16.20.2 172.20.90.31
プライマリ WINS サーバー	: 172.20.90.31
セカンダリ WINS サーバー	: 172.20.45.8
NetBIOS over TCP/IP	: 有効

通常の有線 LAN の時との違い

デフォルトゲートウェイがおかしく見えますが、これで通信 OK

サブネットマスクも 255.255.255.255 で問題無し

※注

なぜか、7.4 系は WINS サーバと通信しないようで、NAS へのアクセス、

リモートデスクトップの際に名前(共有名)が使えません

7.2 系は名前(共有名)が使えてるので、おそらく、7.4 系のバグ？ではないかと思います。

5. IPsec-VPN でできること/テスト結果

所内の PC とほぼ同じことが所外の PC から可能になります。

また、PC の場合、FortiClient クライアントを起動する以外は、金研内で使う設定から変更が必要な箇所は「ほぼ」ありません。

※「設定変更不要」が、SSH の port forwarding を利用した時と大きく違います。

なお、iOS 版、Android 版は Windows 版と若干挙動が違うのは上記の通り

※注

IPsec-VPN 接続中は全ての通信が金研発の通信経路になります。

そのため、金研の F/W 運用ポリシーに従ったアクセス制限がかかります。

その結果、ご自宅発インターネット宛てでアクセス OK だったのに、IPsec-VPN 接続中は金研発インターネット宛てになるので、アクセス NG になる場合があります

1) Web ブラウザの利用

IPsec-VPN 接続中に Google へのアクセスを確認しています。

ネットワーク室の例ですが

http://172.20.90.4/ で NAS の Web 画面

http://172.20.90.2/ でプリンタの Web 画面

等を見ることができたので、金研内の機器に Web ブラウザでアクセス可能なことを確認しています。

※http を使う Web カメラに IPsec-VPN 経由で自宅などからアクセスすることが可能

実験装置の監視カメラの確認等に有効だと思います。

2)　NAS へのアクセス

¥¥172.20.90.4　　で NAS 検索(WINS 不要)

¥¥no-tera　　で NAS 検索(WINS 必要)　←FortiClient 7.4 は名前指定が NG

でネットワーク室の NAS にアクセスできることを自宅から確認しています。

3)　PC のファイルへのアクセス

NAS とは違い、PC の場合は標準の状態で別サブネットからの共有が禁止になっています。

そのため金研側の PC にあらかじめスコープ設定の調整が必要です。

※ノートンインターネットセキュリティ等のセキュリティソフトを使っている場合は
「セキュリティソフト側で設定変更が必要」になる場合があります。

Windows11 の F/W 機能を使っている場合

まず、コントロールパネルからネットワークとインターネット

→ネットワークと共有センター

→左下の関連項目より、Windows Defender ファイアウォール

→左側詳細設定

→受信の規制

→ファイルとプリンタの共有（SMB 受信）　プライベート

クリックして設定タブを開く

→「スコープ」タブのリモート IP アドレスの追加をクリック

IPsec-VPN 経由、無線 LAN(個人認証)のから、自分の PC に共有をかけたい場合は
「172.31.0.0/16」を入力(追加)して OK(IPsec-VPN と金研の無線 LAN の両方への許可)
「適用」して設定保存

※通常はローカルサブネット(自研究室の中)のみになっているので
IPsec-VPN や無線 LAN を使わなくても、別研究室の PC 間、VPN 接続している
遠隔地の PC-仙台の PC のような共有は、Windows の初期設定で NG です
金研の PC は F/W 内なので「持ち出さない PC」は「任意」でもあまり影響が
ありませんが、この場合は誰でもアクセスできないように認証は必要です

※eduroam 経由のノート PC から金研の PC が検索、共有可能なことを確認しています。

4)　リモートデスクトップ

金研側の自分の PC の名前はあらかじめ控えておきます。

(自分の PC の名前が分かっていれば、WINS サーバを使って調べます)

※注

7.4 系では PC の名前が使えないようです

また、Win11 はアップデートの状況に依存して、設定箇所が移動する場合があります。

そのため、別の PC の場合、手順が必ずしも同じとは限りません

リモートデスクトップの許可設定(Win11 バージョン 25H2)

→「設定」

→システム

→リモートデスクトップ

→リモートデスクトップを有効にするを「オン」

→「リモートデスクトップユーザー」でユーザーを選択、アクセス可のユーザーを決定

　※アクセス先になる PC 側ユーザーがアドミングループならば追加不要

スコープは任意なので問題無し

リモートデスクトップの指定で

IP アドレス

PC の名前　　←Forticlient7.4 系では名前指定が NG

のいずれかで接続します

この手順で、eduroam 経由のノート PC から IPsec-VPN で、金研のデスクトップ PC にリモートデスクトップ機能でアクセス、操作可能なことを確認しました。

5)　メールの送受信

金研内での東北大メール利用と同様となります。

6)　金研内のプリンタへの印刷

金研内で使っている設定のまま、ノート PC から eduroam 経由の IPsec-VPN で金研のプリンタに印刷できることを、確認しています。

7)　SSH 接続

IPsec-VPN 接続後の SSH 接続の挙動は全て金研発になります。

8)　金研 Web サーバとの SCP/SFTP 接続

Web サーバのコンテンツ更新で使用する SFTP は上記の SSH と同じ挙動です。

金研 Web サーバは所外、学内の仮想レンタルマシン上にあるため、東北大(TAINS)がアクセス制限をしていますので､TAINS へ許可申請をしないと金研 Web サーバへの SCP/SFTP を使ったファイル転送はできません。そのため、金研内からはアクセス OK(TAINS へ許可申請済)、自宅、出張先からは原則アクセス NG となっています。

ですが、IPsec-VPN 接続中は全ての通信が金研発になるので、IPsec-VPN 接続を使えば自宅、出張先でも金研 Web サーバのファイル更新が可能です。

9)　所外との FTP 接続

研究室に FTP サーバがある場合は、以前から FTP 接続可能です。

IPsec-VPN 接続中は全ての通信が金研発になるので、IPsec-VPN 接続中に所外 FTP サーバとの FTP 接続が可能なことを確認しています。

例：IPsec-VPN 接続中の PC の FFFTP -> ftp.freebsd.org　等への FTP 接続を確認済

10)　時刻同期(NTP)

金研の F/W で所外のタイムササーバとの通信を遮断しているため、IPsec-VPN 接続中はマイクロソフト、アップル、プロバイダ提供、公開タイムサーバ等と時刻同期は NG になります。(金研の所内向けタイムサーバ(172.26.20.2)と同期は可能)。

ですが、その場合でも、IPsec--VPN 未使用状態の時に PC 等は時刻同期を行うので、大幅に時間がずれるということは、おそらく起こらないと思います。

6. FortiClient と Win11 標準の VPN 機能との併用について

※重要：併用すると「Win11 標準の VPN の使用時にエラー」が発生する
トラブルが起こりますので注意
併用する場合は、それを理解して使いわけするようにお願いします。

テストをした結果
※FortiClient のアップデート、Win11 のアップデートで挙動が変わるかもしれません。

Win11 標準の VPN　　接続 OK
↓
FortiClient の VPN　　接続 OK
↓
Win11 標準の VPN　　接続 NG(エラー発生)
↓
「IKE and AuthIP IPsec Keying Modules」サービス再起動
↓
Win11 標準の VPN　　接続 OK(エラー解消)

という挙動になりました。
併用すると
・Win11 標準の VPN を使用した後に FortiClient を使用するのは問題無い
・FortiClient を使用したの後に Win11 標準の VPN を使用するとエラー発生、接続不能
・エラーを止めるには「IKE and AuthIP IPsec Keying Modules」サービス再起動
　サービス再起動の手順は
　Windows ツール→コンピュータの管理
　サービスとアプリケーション→サービスで
　「IKE and AuthIP IPsec Keying Modules」を探して停止、開始
　あるいは PC の完全な再起動を行う
という状態になり、エラー発生にはまります。
エラー対応を考えると Win11 標準の VPN と FortiClient を「適当に併用する」使い方は推奨しませんので
・どちらを使うか？はユーザーの判断
　全学の VPN サービスは L2TP/IPsec なので、そちらも使う場合は FortiClient を
　使わない方がエラーで悩まずに済みそう
　反対に、これまでの金研の SSL-VPN に慣れているなら、同じソフトを使った方が
　簡単かも

・併用したいユーザーは、エラー時は自分で対処

ということになりますが、片方にバグ(特に FortiClient のアップデート後にその可能性があります)が入って動作不良、接続不良を起こした場合、接続方法が複数あれば一時的な回避手段にはなりますので

・通常はどちらかを 1 つをメインに使用する(併用しない)

・何かしらの動作不良を起こした場合のバックアップとして切り替える

ただし、Win11 標準の VPN で起きるエラー回避はユーザー自身で行う

という使い方を推奨します。