2025/4/23 版

SSL-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.　SSL-VPN 接続用ソフト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。
現在は Ver7.4 系です。
クライアントは 6 種類あります。
VPN for Windows
VPN for Mac
VPN for iOS　　←iPhone、iPad 用(以前にテストした結果は後述)
VPN for Android　　←Android スマホ版(以前にテストした結果は後述)
VPN for Linux .rpm　　←動作検証無し
VPN for Linux .deb　　←動作検証無し

※2025/1/8　説明を追記、2024/4/23 若干修正
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)
なお、オンラインインストーラーでインストールした場合、メーカーがバグを確認してソフトウェアをアップデートしている場合があり、全ての PC、Mac でこの不具合が該当するか？は判りません。
※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。

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。
なので、こちらのインストーラーを入手してください。

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ので、金研の Web サーバ経由で入手できるようにしました。
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

iOS 版は Apple から、Andoroi 版は Google からのダウンロードになります。
※2022/2/8 に確認した状況を追記
iOS 版は 7.0.2(以下は不明)、Android 版は 7.0.2.0031 です。
iOS 版と Android 版のテスト結果
※注意　下記は金研で SSL-VPN サービスを開始の際にテストした時の挙動です。
　　バージョンアップによって挙動が変化していることがあります。
　　必ずしも下記の説明通りとは限りません。その旨、ご了承ください。
iOS 版
・Wifi 接続で DNS サーバを金研 F/W 内で使う「172.16.20.2」に手で修正すれば、
　金研内のプライベートネットワークとのホスト名で通信可能になる
　修正しないと金研 F/W 内のサーバとは IP アドレスを使わないと通信できない
　※PC のクライアントの場合、DNS サーバは SSL-VPN 側を使うが iOS 版は

そのような動作では無いようです
・キャリア(電話)経由は契約している端末が無いので状況不明
※求むテスター

Andoroid 版
・Wifi 接続は DNS サーバを金研 F/W 内で使う「172.16.20.2」に手で修正すれば、
金研内のプライベートネットワークとのホスト名で通信可能になる
・キャリア(電話)経由は proxy 通過以外が通信可能
のような動作になることが分かりました。

メーカーから提供されるクライアントの動作に依存しますので、その仕様の範囲でしか動作しませんので、「こういう動作がしない」と言われても対応はできません。
また、問題がある挙動はメーカーの修正、アップデートを待つことになります。

3. FortiClient をインストールする
FortiClient のインストーラー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、設定確認以降の実際の通信テストは所外(ご自宅、モバイルルータ等、利用する場所)か、金研内なら無線 LAN の「imr-guest」「eduroam」で行ってください。
無線 LAN システムが使用可能な場所(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です)、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

SSL-VPN を選択

接続名をつける	例：IMR
リモート GW	fg.imr.tohoku.ac.jp ※名前に対しての証明書なので 「130.34.226.190」だとアラートがでます)
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くれる

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。

2 回目以降は PC 起動で常駐しているので、Windows10 の場合、

タスクトレイの「 ^ 」→青色のアイコンを右クリック

→「”IMR(ユーザーが設定した接続名)”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、Win10 の場合はネットワークの種類の指定を聞かれると思いますので「プライベート」にします。もし「パブリック」になってしまうと通信できないと思うので、その場合は「プライベート」に切り替える必要があると思います。

設定が終わって SSL-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、SSL-VPN 用の仮想 I/F はこうなります。

ipconfig /all で確認

PPP アダプター fortissl:

接続固有の DNS サフィックス . . . :
説明. . . . . : fortissl
物理アドレス. . . . . :
DHCP 有効 . . . . . : いいえ
自動構成有効. . . . . : はい
IPv4 アドレス . . . . . : 172.31.40.128(優先)　←IP アドレスは PC 毎に違います
サブネット マスク . . . . . : 255.255.255.255
デフォルト ゲートウェイ . . . . . :
DNS サーバー. . . . . : 172.16.20.2
プライマリ WINS サーバー. . . . . : 172.20.90.31
セカンダリ WINS サーバー. . . . . : 172.20.45.9
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は設定されなくて正解

サブネットマスクも 255.255.255.255 で正解

DNS サーバは金研の F/W 内のサーバが 1 つだけ通知されます。

WINS サーバは 2 つ通知されるのですが、これは機器側の仕様のようです。

5　ストア版 Forticlient について

※2025/4/23 追記

Win11 では正常に動作しないようです。Win11 ではストア版を使用しないでください。

メーカーもストア版 Forticlient をサポートしていないようです。

以下、「どうしても Win10 でストア版を使用したい」ユーザーへの説明です。

メーカーサイトからのダウンロード版以外に、マイクロソフトから入手できるストア版 Forticlient も利用可能です。ただし、既にサポートされていない可能性がありバグ、セキュリティホールがあるかもしれません。また、後述するように、共有 PC や NAS へのアクセスとリモートデスクトップへの接続の際に「共有名が使えません」。

これは、ストア版 Forticlient の「仕様」でトラブルではありません。

ストア版 Forticlient は共有名が使えないデメリットがありますが、一度設定して接続できるとパスワードを覚えますので、毎回パスワードを入力する必要が無くなるというメリットもあります。両方インストールして共有名の要不要で使い分けすることが可能です。

1. 「Forticlient ストア版」で検索します。
   ※マイクロソフトのサービスなので Edge あるいは Google Chrome を
   使ってください。Firefox だと問題があるかもしれません。
2. 「FortiClient - Windows に無料でダウンロードしてインストールする」
   が上位に出てくるのでアクセスします
   ※Microsoft Store の修正で検索結果は変わる場合があります
3. 「ダウンロード」をクリック
   ※メールアドレスの入力を求められる場合があります
4. ダウンロードしたファイルを実行する
   既にストア版をインストール済の場合は「開く」ボタンになります
   「詳細」あるいは「開く」でバージョン確認ができます
   (2025/1/8 時点でバージョン 1.0.1041)

インストールはこれで終了です。

インストールできたら接続のための設定をします。

1. 「設定」→「ネットワークとインターネット」→「VPN」→「VPN 接続を追加する」

VPN プロバイダー	FortiClient を選択
	※重要「Windows(ビルドイン)」を選択しないこと
接続名	IMR(ユーザー指定で任意に付けられます)
サーバ名またはアドレス	fg.imr.tohoku.ac.jp

を入力して保存します。

設定はこれで終わりです。

自宅等から接続手順

1. タスクトレイの「ネットワーク」で「IMR」を選択
2. Win10 では「VPN」が開くので、上記の設定済の「IMR」をクリック→接続
3. 認証で「ユーザー名」「パスワード」を入力

※ストア版 Foriclient は「ユーザー名」「パスワード」を覚えて保存するので、
次回の接続は楽になります

基本的には、これで従来型 Forticlient と同様に VPN 接続ができます。

・問題点

「ストア版 Foriclient は WINS サーバが使えません」

※ダウンロード版 Foriclient は WINS サーバの情報を受け取って共有の際に
使えるのですが、ストア版ではそれができません(＝共有名が使えない)

そのため、これはネットワーク室の NAS での例ですが

NAS へのアクセスで

¥¥no-tera	NG
¥¥172.20.90.4	OK

となることが判りました。

この問題のため、従来の Foriclient ではできていた「¥¥no-tera」のような「共有名での NAS へのアクセス」ができない仕様です。これは当方では対処、解決不可能です。

また、リモートデスクトップも同様で

共有名での指定	NG
IP アドレスでの指定	OK

となります。

・ストア版 Foriclient での NAS の利用とリモートデスクトップの問題点の回避方法

ストア版 Foriclient では

・自宅等からの利用の際は「事前に目的機器の IP アドレスを確認」すること

・NAS への接続は「¥¥IP アドレス」で使うこと
・リモートデスクトップの利用は「IP アドレス指定」にすること
でアクセス可能になりますので、利用する場合はそのようにお願いします。

6.　SSL-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、SSL-VPN 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、Andoroid 版は Windows 版と若干挙動が違うのは上記の通り

※2025/1/8　追記
2024/12/25 に金研では proxy サーバの運用を終了しました。
そのため、それ以前からのユーザーは PC/Mac の proxy サーバの設定は不要になりましたので、全て設定解除してください。
以前は自宅・出張先の PC から金研に SSL-VPN 接続中は
金研向け　　->　VPN の仮想インタフェースへ
インターネット　->　通常の通信
※オンラインジャーナル等は東北大発にならないと利用できない物が多め
proxy サーバ経由にして、HTTP/HTTPS を金研発にしていました。
のように、金研向きにする必要があるか？を Forticlient が判断していたのですが
(VPN 経由でインターネット向きが遅くなることを懸念しました)
2024/12/25 の proxy サーバの運用終了に合わせて、
全ての通信　　->　VPN の仮想インタフェースへ
と、SSL-VPN 接続中は全ての通信が金研発の通信経路になるよう変更されました。

1)　Web ブラウザの利用

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ますので、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 SSL-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 無し)　←ストア版クライアントはこの形式のみ OK

¥¥no-tera　　で NAS 検索(WINS 必要)　←7..x は名前指定でも OK
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になります。
　※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」になると思います。

Windows10 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 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
　SSL-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(SSL-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
　　SSL-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

金研の PC のノートンインターネットセキュリティを一時的に停止、F/W 機能を無効にした状態で、金研の PC が検索可能、共有可能なことを自宅から確認しています。

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るようです)

※2021/3/5 追記

Win10 はアップデートの状況に依存して、設定箇所が「コンパネ」から「設定」に移動している場合があります。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(Win10 Pro　バージョン 20H2)

→「設定」

→システム

→画面左側の[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」

→「ユーザーアカウント」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

この状態で「金研の自分の PC」にリモートデスクトップ機能を使って自宅 PC からアクセス、操作可能なことを確認しています。

リモートデスクトップの指定で

IP アドレス　　←ストア版クライアントはこの形式のみ OK

PC の名前　　←7.0.x は名前指定でも OK

のいずれかで接続します

5)　メールの送受信

2024/12/25 以降、SSL-VPN 接続中は全ての通信が金研発となるように通信経路が変更されたので、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、SSL-VPN 経由で金研のプリンタに印刷できることを、自宅から確認しています。(翌日、印刷された紙が出ているのを確認)

7)　SSH 接続

2024/12/25 以降、SSL-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、2024/12/25 以降、SSL-VPN 接続中は全ての通信が金研発となるように通信経路が変更されたので、SSL-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になりました。

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。

2024/12/25 以降、SSL-VPN 接続中は全ての通信が金研発となるように通信経路が変更されたので、SSL-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：SSL-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、2024/12/25 以降、SSL-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)。

その場合でも、PC 等は SSL-VPN 未使用状態で同期すると思いますので、大幅に時間がずれるようなことは起こらないと思います。