2022/12/13 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

2022/12/9 加筆修正
2022/3/15 実施の SSL-VPN 装置のファームウェアアップデートで、Windows 版 Forticlient7.0.2 以降で通信異常が発生した問題は、2022/11/15 に実施した SSL-VPN 装置のファームウェア再アップデートで解消しましたので、説明を以前の内容に戻しました。

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
上記 URL にアクセスして、一番下の「FortiClient VPN」に移動します。
そこの「DOWLOAD」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 Ver7.0 系です。
※2022/212/9 時点で、Windwos 版は 7.0.7.345、Mac 版は 7.0.7.0245 がインストールされることを確認しました。これ以外は「How to Buy」と書かれているように購入するか、試用期限付きで期限後は使用できなくなるか、だと思いますので、ダウンロード、使用しないでください。

※Mac ユーザーへの注意
MacOS BigSur(Ver11.0)は「FortiClient 6.4.3」以降のバージョンが必要です。
それよりも古い FortiClient を使用している場合、Mac OS のアップデートをすると、
FortiClient が動作しなくなります(MacOS 側の仕様の変更のため)
その場合は、FortiClient 6.4.3 以降へのアップデートが必須となります。
現在、FortiClient VPN の「Download」から入手できるのは「FortiClient 7.0 系」なので
6.4 系が新規にインストールされことは、基本的にありません。

iPhone 版、Android スマホ版について
FortiClient iOS　　←iPhone、iPad 用(以前にテストした結果は後述)
FortiClient Android　　←Android スマホ版(以前にテストした結果は後述)
iOS 版は Apple から、Android 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　下記はサービス開始の際にテストした時の挙動です。
　　各々のソフトのバージョンアップによって挙動が変化している
　　可能性も考えられますので、必ずしも下記の説明通りとは限りません

iOS 版
・Wi-Fi 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
　金研の proxy を通過することも可能
　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

Android 版
・Wi-Fi 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
　Firefox+プラグインで proxy を通過できるようです。
・キャリア(電話)経由は proxy 通過以外が通信可能
　Android 版 Chrome には proxy の設定箇所が無いので proxy 通過はできない

Firefox+プラグインで proxy を通過できるようです。

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(メーカーサイトのダウンロード版)

FortiClient のインストーラーは proxy サーバを通過できない仕様ですが、金研の F/W 側を調整しましたので、金研内でインストール可能です。
インストール後のテストは「ソフトの設定の確認(接続の可否)」と「パスワードの確認」程度は可能ですが、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」で行ってください。

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(ダウンロード版 7.0 系を使う場合はこの設定です)

初回は
SSL-VPN を選択

接続名をつける	例：IMR
リモート GW にホストを設定	fg.imr.tohoku.ac.jp ※名前に対して SSL 証明書を取得しているので 「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

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、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」なの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。
※2022/12/13 修正
　Google の検索結果と Microsoft Store 側が変わっていたので、それを修正しました

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 - Microsoft Apps」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. 「Microsoft Store　アプリの取得」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. 画面が変わったら「インストール」ボタンをクリック
　　※金研内で問題無く「インストール」できることを確認しました
　　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
　　(2022/12/13 時点でバージョン 1.0.1041)
5. 閉じる

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。

2. 「VPN 接続を追加する」の下に「IMR」が表示されますのでクリック

   詳細オプション

   →VPN プロキシ設定

   「セットアップスクリプトを使う」

   「http://proxy.imr.tohoku.ac.jp/proxy.pac」

   のように設定して「適用」

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。

7.　SSL-VPN の通信で可能なこと/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、Android 版は Windows 版と若干挙動が違うのは上記の通り

1)　Web ブラウザの利用

SSL-VPN 接続後、proxy サーバの設定を行い、所内限定

Web 名簿　　http://web.imr.tohoku.ac.jp/~office/inside/shokuinroku/

会議室予約システム　　http://web.imr.tohoku.ac.jp/~imr-yodo2/yoyaku/

をご自宅や出先から見ることができれば、SSL-VPN 接続と proxy サーバ設定は成功しています。

※2022/2/8 追記

新 Web サーバへの移行に伴い、金研の Web サーバは所外/学内サーバに変更されました。

そのため、従来の所内限定と同等のアクセス制限が必要なコンテンツは

「金研のグローバル IP アドレス発(+事務ネット発)」が「新しい所内限定」になります。

上記の URL でアクセス禁止(Forbidden)になった場合は

「金研の proxy サーバ経由では無くインターネット側から直接アクセス」

している状態ということになりますので

・proxy の設定が適切ではない

・OS 側で制約、仕様で SSL-VPN 接続時に proxy の設定を認識していない

のいずれかだと思われます。

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、研究室内(F/W 内のプライベート IP アドレス機器)を見ることができますので、proxy の設定無しで金研内の機器に 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

ご自宅からの実験装置の監視カメラの確認等に有効だと思います

proxy サーバの設定が必要な例

SSL-VPN 接続した状態で、proxy サーバの設定無しで、

東北大のホームページ→教職員向けにアクセスすると教職員向けとなり、

https://www.tohoku.ac.jp/japanese/target/teacher2.html

認証を通過すると
「東北大学外からのアクセスのため、内容が一部制限されております。」
と表示されます。
この表示の時は SSL-VPN 経由ではなく、プロバイダから直接、全学ポータルにアクセスしている状態です。

所内で使用している設定のまま持ち出した PC のように proxy.pac を使う設定で
SSL-VPN 接続を行い、東北大ホームページ→教職員向けにアクセスすると
「教職員向け（学内用）」となり、認証を通過すると
https://www.tohoku.ac.jp/japanese/target/teacher.html
のように「2」が無くなって
「東北大学外からのアクセスのため、内容が一部制限されております。」
の表示が出なくなります
これで、金研内から金研の proxy サーバ経由でアクセスしていると判断できます。

つまり
proxy を通す必要が無い通信は
インターネット側　　→SSL-VPN を使わずプロバイダの回線から直接通信
金研の F/W 内側　　→SSL-VPN 経由で通信、アクセス可能

proxy.pac を使う設定をすると、金研内の PC と同じ条件で通信できる(proxy.pac の記述に従う)ようになるので、東北大発、金研発が必要なサーバ(例えば学内限定、オンラインジャーナル等)について、所外から SSL-VPN 経由で通信可能になります。

※Windows ユーザーへの注意事項
Windows の場合、所内で Edge を使う通常の設定は「ローカルエリアネットワーク(LAN)の設定」ですが、その部分に**「ダイアルアップ接続には適用されません」**と説明があります。
Windows では SSL-VPN(仮想プライベートネットワーク)がダイアルアップ接続と見かけ上同じ扱いになるという、OS の仕様なので、**SSL-VPN 用の proxy サーバの設定箇所が金研内で proxy サーバを使用するための通常の設定箇所(=LAN の設定)と異なります。**
金研の SSL-VPN サービスの場合、
コントロールパネルのツール→インターネットオプション→接続にある「**fortissl**」(設定で IMR になっている場合もあります)を選択して「設定」から SSL-VPN 用 proxy サーバの設定をしてください。
設定箇所は違いますが、設定内容は金研内で使用する設定と同じです。

設定を自動検出する	チェックしない
自動構成スクリプトを使用する	チェックする
アドレス	http://proxy.imr.tohoku.ac.jp/proxy.pac

通常のブラウザの使用はこれで足りますが、proxy.pac を理解できないソフトも金研の proxy サーバ経由が必要な場合は、その下の設定も行う。

LAN にプロキシサーバを使用する	チェックする
アドレス	proxy.imr.tohoku.ac.jp
ポート	8080

おそらく SSL-VPN 接続時の IE/Edge は「fortissl」の設定を使用、SSL-VPN 接続を使わない時の IE/Edge は LAN の設定(プロバイダ等の指示)を使用する動作になると思います。Firefox については、「金研内で使用する proxy の設定」で通信できると思います。

※Mac ユーザーへの重要な注意事項

※2021/5/27 追記

以下の説明は 6 系で確認していますが、7.0 系での挙動は未確認です

Mac の Safari の場合、proxy の設定が正しい状態でも「proxy の設定を理解できない挙動」になるようです。テストの結果、proxy.pac の設定でも、port 番号の 8080 を使う設定でも通信 NG でした。これは

- Safari ではなく Firefox を使った場合に proxy サーバ経由の通信が可能なことから MacOS と FortiClient の問題で proxy サーバの port8080 との通信ができないということはない(MacOS と FortiClient の制約では無い)
- proxy の設定ではなく、Safari に http://proxy.imr.tohoku.ac.jp/proxy.pac を入力したところ、proxy.pac の内容(Javascript で記述されたテキストファイル)が Safari 上に表示されたことで、SSL-VPN 経由で Safari と proxy サーバ間の http の通信(port80)に制限は無いことを確認(proxy.pac の取得の問題では無い)

という辺りの検証で、「SSL-VPN 経由で Mac は proxy サーバと通信(port80 と port8080)できるにも関わらず、Safari だけが proxy の設定が正しくても設定を理解できない(仕様)」と判断しました。

以上から、「Mac で SSL-VPN 接続し、proxy サーバを経由した通信が必要な場合は、その時だけ Firefox を使う必要がある」と判断します。

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)　←7.0.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。

Windows7 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、IP アドレスを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~~

~~金研内で使っている設定のまま、SMTP/IMAP で送受信できることを自宅から確認しています。~~

~~※メールソフトの設定の関係で、POP3 の受信を確認していませんが~~

~~IMAP と同じサーバなのでおそらく問題ないだろうと判断~~

※2022/6/13 追記

金研のメール環境移行に伴い、この説明が不適切になりましたので記載を削除しました。

2021 年 10 月末に金研のメール環境は東北大メールに移行しました。

また、2022 年 4 月末で金研のメールボックスサーバの提供を終了しています。

そのため、SSL-VPN 経由でのメールの利用は既に意味がありません。

5) 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)

6) SSH 接続

SSL-VPN 接続後の SSH 接続の挙動はこうなります。

金研外への SSH 接続	→SSL-VPN 経由する必要が無いためダイレクトに通信する
金研内への SSH 接続	→SSL-VPN 経由で通信可能
金研の SSH 認証サーバ	→SSL-VPN 経由で通信可能
	※この通信はネットワーク室職員以外使わないかも

※2022/2/8 追記

新 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。

また、新 Web サーバのアクセス制限(業者さん等のために要申請でアクセス可能)があるため、WinSCP の通常の設定では学内からのアクセスにならないため、自宅等から SSL-VPN を使用しても Web コンテンツ更新は NG となります

(インターネットからダイレクトに通信するため)

ただし、SSL-VPN では無く、「金研の SSH 認証サーバ利用申請と WinSCP のトンネル設定」で、金研以外の場所から新 Web サーバのコンテンツを更新することは可能なので、ネットワーク室にご相談をお願いします。

7)　時刻同期(NTP)

自宅の PC 等の場合は、プロバイダ指定、公開タイムサーバを使えば問題ありませんが、金研から所外に持ち出した PC の場合、金研のタイムサーバを設定していると時刻の同期ができませんが、SSL-VPN 経由で金研のタイムサーバと時刻同期できることを確認しています。

~~8)　金研のサーバと FTP~~

~~所外にいる時に、Web コンテンツの更新等のために SSL-VPN 経由で「ms.imr.tohoku.ac.jp」に FFFTP を使ってアクセスできることを、自宅から確認しています。~~

※2022/2/8 追記

新 Web サーバ移行に伴い、この説明が不適切になりましたので記載を削除しました。

なお、研究室内に自前の FTP サーバがある場合は SSL-VPN 経由で接続可能です。