

核融合科学研究所における VPN システムの運用

○中村 修^{A)}

^{A)}核融合科学研究所 技術部 制御情報技術課

1. はじめに

コロナウィルスが流行したことを機に、在宅勤務での対応が急激に増えることとなった。自宅から職場の機器へアクセスして業務を遂行するためには、VPN システムを利用することが不可欠となり、VPN システムの利用者が急激に増えることにもつながった。

本報告では、核融合科学研究所における VPN システムの運用について報告する。

2. VPN システムの構成機器

本研究所では、VPN アプライアンス製品として Ivanti 社製の ISA8000c を採用している。また、認証サーバとしては株式会社ソリトンシステムズ製の NetAttest EPS (EPS-ST05-A) を運用している。認証方式としては、パスワード認証に加えてクライアント証明書による二要素認証を行い、セキュリティ強度を高めている。

ISA8000c の本体写真を図 1 に、VPN システム全体の構成図を図 2 に示す。



図 1. ISA8000c の本体写真

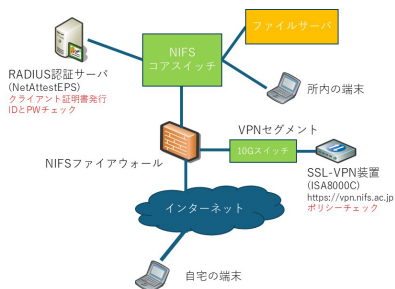


図 2. VPN システム全体の構成図

3. 運用

本研究所で発行するアカウントは 4 種類に分類され、それぞれアクセス可能なネットワーク範囲が区別されている。

本研究所の職員であれば、研究基盤 LAN のみにアクセスできる kiban から始まるアカウントか、研究基盤 LAN に加え LHD 実験 LAN にもアクセス出来る nifs から始まるアカウントが付与される。LHD 実験に参与する共同研究者においては、日本国内の共同研究者であれば、LHD 実験 LAN のみにアクセス出来る lhd から始まるアカウントが付与されるが、日本国外の共同研究者に対しては、LHD 実験 LAN 内の限られたサーバのみにアクセス出来る flhd から始まるアカウントが付与されることになっている。

SSL-VPN 接続時には、接続端末が定められたポリシーを満たしているかのチェックを行っている。

Windows 端末であれば、

- ・サポート対象の OS であること
- ・Windows パッチが適用されていること
- ・14 日以内の定義ファイルでアンチウィルスが動作していること

この 3 つに関してポリシーチェックを行っている。

mac 端末に関しては、

- ・サポート対象の OS であること
- ・14 日以内の定義ファイルでアンチウィルスが動作していること

この 2 つに関してポリシーチェックを行っている。

4. Ivanti (旧 Pulse Secure) の導入経緯

本研究所における Ivanti (旧 Pulse Secure) 製品の導入は 2020 年度に開始された。当初は Pulse Secure 製品としての導入を進めていたが、2020 年の 12 月に Ivanti による Pulse Secure の買収が発表された。導入途中での発表ではあったものの、仕様に沿った納品が可能であったため、そのまま 2020 年度内に PSA5000 の導入を完了した。

しかし、導入から約 1 年後の 2022 年 7 月に、PSA5000 の販売を 2023 年 1 月で終了すると Ivanti より通知があった。2023 年 1 月をもって重大なバグや脆弱性対応を除く機能アップデートの終了も通知さ

れた。さらに 2024 年 6 月で解析サポートも終了することになり、脆弱性対応も無くなるということで、後継機種への移行が提示された。

当時運用していた PSA5000 からは、後継機種へと移行するのが円滑であると判断し、現在運用している ISA8000c への移行を 2023 年 1 月に実施した。

5. ISA8000c における不具合等

5-1. ファームウェア更新に伴う不具合

macOS 14 対応のため、2023 年 12 月にファームウェアを 22.6R2.1 へ更新したところ、二要素認証に用いるクライアント証明書の検証が失敗するようになり、従来の運用が不可能となった。当日の解決を断念してロールバックによりサービスを再開し、config や失敗時のログを取得してサポートへ調査を依頼した。

約 3 か月後、当該事象はファームウェアの不具合であるとの回答を得た。それから約 2 か月後に公開されたファームウェア 22.7R2 へ更新したが、同様の不具合が再発した。さらに約 3 か月後、接続アプリ ISAC (Ivanti Secure Access Client) の更新案内があったものの、改善は見られずサポートへの調査依頼を継続することとなった。

最終的に 2025 年 1 月、「Allow legacy certificates for end to end communications」の設定を有効化することで回避可能との回答を得たため、当時の最新ファームウェア 22.7R2.4 への更新を行い、設定変更を行うことで不具合は解消された。しかし、設定変更で解消する事象に 1 年以上を要し、その間に macOS 15 がリリースされるなど、サポート対応の遅延が目立った。

5-2. 脆弱性対応

2024 年 1 月に、非常に深刻度の高い脆弱性 CVE-2024-21887 (CVSS スコア 9.1) が発表された。サポートからは「即時の XML ファイル適用、または適用不能な場合は機器停止」という強い勧告があった。機器を停止させるわけにはいかないため、XML ファイルを適用して運用を継続することにした。

その後も追加の XML ファイルの適用指示があり、対応して運用を継続した。改ざんを受けたかチェックするツールを試してみたが、幸いにして改ざんはみられなかった。多くの機関が攻撃を受けて改ざんを受けたものの、本研究所では改ざんされるまでには至らなかったが、ファイアウォールのログからは、XML ファイルを適用した後に攻撃を受けている痕

跡が確認された。

恒久対策としては、脆弱性に対応されたファームウェア 22.3R1.1 への更新が必要とされたが、サポートからは改ざんの有無にかかわらず工場出荷時へ戻してからアップグレードパスに従って更新するよう指示があったため、更新作業に丸一日を要した。

その後 2025 年 1 月には CVE-2025-0282 (CVSS スコア 9.0)、一か月後の 2 月には CVE-2025-22467 (CVSS スコア 9.9) の重大な脆弱性が立て続けに発見され、ファームウェアの更新を行うこととなった。その際もサポートからの指示は、工場出荷時に戻してから行う手順であった。

5-3. Windows Update Agent の更新による接続障害

Windows Update の適用後、VPN 接続が失敗する事象が繰り返し発生した。原因は Windows Update により、Windows Update Agent のバージョンが更新され、Windows パッチのポリシーチェックが失敗するためであった。

2024 年度では、4 月、5 月、7 月、11 月。2025 年度には 4 月、9 月、12 月と Windows Update Agent が更新され、対応するまで Windows Update を行わないようにアナウンスを行っている。

対応するには OPSWAT 社の提供する ESAP (Endpoint Security Assessment Plug-In) の更新が必要なのだが、サポート会社からの提供に 2 週間程度を要する。サポートに対して、例えばバージョンを無視するなどしてバージョンが上がっても Windows パッチのチェックが行えるようにならないか相談したが、バージョン管理は重要と考えているので対応予定はないとの回答であった。

5-4. サポート終了の通知

2023 年 1 月に導入を決定した ISA8000c であったが、2025 年の 8 月に販売終了が発表され、2027 年 1 月でサポートを終了するとの通知を受けた。ISA8000c での運用を開始してから 2 年程度での通知であり、サポート終了までの実運用期間は 4 年に満たない結果となってしまった。

6. まとめ

Pulse Secure の Ivanti による買収は、本研究所の VPN システム運用に大きな影響を及ぼしたと考えられる。買収に伴う方針の変化は、しばしばユーザーに不利益をもたらすことがあるが、本研究所における事例でも同様の傾向がみられた。

現在、本研究所では Ivanti 製品の後継機ではなく、代替となる別製品の検討を進めている。特に脆弱性対応の負荷が高いことを踏まえ、クラウド型サービスへの移行も選択肢として検討している。また利用者の要望に基づき、アクセス制御パターンの増加に対応可能な設計もあわせて行う必要がある。

参考文献

[1] JPCERT/CC

<https://www.jpcert.or.jp/at/2024/at240002.html>