トンネルの外側
VPN の保護境界を測定する

VPN BOUNDARY – MEASUREMENT AND RESULTS

トンネルの外側

VPN の保護境界を測定する

Odysec 研究報告 WP-002 ｜ **バージョン** 1.0 ｜ **発行日** 2026-08-31 **領域**：サイバー × フィジカル（Cyber × Physical）

繁体字中国語版が正式版です。本書はその翻訳です。

目次

本報告の性質について

本報告の数値はすべて、完全に公開された制御環境から得られたものです。その トポロジファイルと全スクリプトは本報告とともに公開されており、誰でも再構築し、 再実行できます。

被検対象は手動で設定した WireGuard（`wg-quick`）であり、市販の VPN アプリケーションではありません。 市販製品は独自のキルスイッチ、DNS 処理、 再接続ロジックを実装しており、本報告はそれらについて何も知りません。本報告の 数値が当てはまる範囲は、第 3 章に記した環境に限られます。この境界は第 8 章で 改めて述べます。引用の際にこの線を越えないでください。

本報告が測定するのは**トンネルと経路制御の失効モード**であり、方法論の検証で あって製品評価ではありません。

要旨

「VPN は漏れる」という話は新しくありません。`AllowedIPs` に `::/0` がなければ IPv6 は運ばれず、リゾルバを指定しなければローカルのものが使われ続ける── どちらも文書に記載された既定の挙動です。欠けているのは「漏れるかどうか」では なく、**保護境界の形**です。どの時点で、どの通信が、どれだけ、どれほどの間。

四ノードの制御環境を用い、八つのシナリオ、計 17 通りの構成をそれぞれ 30 回、 合計 510 回測定し、四つの主要な知見を得ました。

1. **漏洩するかどうかを決めるのは「接続が切れるか」ではなく、「トンネル インターフェースが残るか」である**：物理リンクを 2 秒間切断して復旧させた 場合、30 回すべてで**漏洩ゼロ**でした。トンネルインターフェースとその経路は 切断中も存在し続けるため、パケットはトンネル内で破棄され、物理インターフェース へ迂回しません。一方、インターフェース自体が消失した場合（VPN プロセスの 異常終了、OS による回収、スリープ復帰後の未再構築）、**すべてのパケットが 実アドレスで送出され、しかも自然には止まりません。** 危険なのは電波が不安定に なることではなく、VPN が静かに動作を止めることです──そのとき通信は完全に 正常で、画面上に兆候は何もありません。
2. **失効は四類型に分かれ、対策はそれぞれ異なる**：状態型（確立までの空白、 リンクの断続、インターフェース消失）はキルスイッチで解決でき、しかも **遅延の代償を伴いません。**キルスイッチの有無でトンネル確立時間に統計的な 差はなく、露出が破棄に置き換わるだけです。設定欠落型（IPv6、DNS）には キルスイッチはまったく役に立ちません。第三の類型が最も気づきにくく、 キャプティブポータルの例外がローカル網を許可している場合、 **キルスイッチは終始正常に動作しているのに通信は外へ出ていきます。** 第四の類型はそもそも「漏洩」ではありません。次の項を参照してください。
3. **漏洩の有無は設定が決める確定的な結果であり、確率的な事象ではない**： IPv6、DNS、ポータル例外の三シナリオでは、漏洩割合のばらつきは**ゼロ**── 30 回の結果が完全に一致しました。v4 のみのトンネルで IPv6 は 100% 漏洩し、 リゾルバを引き継がない場合 DNS は 100% 漏洩します。例外は一度もありません でした。（時間系の測定にはばらつきがあります。第 4 章の四分位範囲を参照。）

4. **すべてを正しく設定しても、ローカルネットワークはこの端末が誰かを知る**： フルトンネル、リゾルバの引き継ぎ、厳格なキルスイッチがいずれも終始有効な 構成であっても、信頼できないローカル網は**毎回変わらず**この端末の MAC アドレス、OUI（NIC ベンダー）、ホスト名、ローカルアドレスを取得しました （30 回の実行で完全に一致）。これらの通信は「トンネルから漏れた」のでは なく、**そもそもトンネルに入ったことがありません**——ARP と DHCP は通常の IP 出力経路すら通らないため、キルスイッチは原理上それらに触れられません。 トンネルが守るのは運ぶよう設定されたものであって、「あなたがこの網に 存在すること」ではありません。

推奨される行動：VPN で所在地を隠すことに依存している場合、三点を確認して ください—— `AllowedIPs` が IPv6 を含むか（あるいは IPv6 を無効化しているか）、 リゾルバが実際にトンネルへ引き継がれているか、そして公衆網へのログイン後に ローカル網の例外を解除したか。三点は互いに独立しており、二つを正しく行っても 残る一つを補償しません。**さらに、この網にこの端末を認識させたくないのであれば、 必要なのは端末層の対策であって、いかなる VPN 設定でもありません。**

---

1. 問題の所在

1.1 誰にとっての問題か

多くの人にとって VPN の漏洩はプライバシーの問題です。当チームの前二報が想定 する読者——つきまとう相手から逃れようとしている人——にとっては、身体の安全の 問題です。

WP-001『すぐそばの目』の方法論は「第零原則：クリーンな端末に移る」から 始まります。ではその端末がネットワークに接続した後は。その端末の実アドレスや DNS クエリがトンネルの外へ漏れ、加害者の手の届く網に落ちれば、それ以前の慎重さは すべてその瞬間に無効になります。**一度の漏洩で居場所は判明します。**

これはまさに「デジタルのリスクが現実の身体的リスクへ転化する」典型的な経路で あり、本報告が前二報を継ぐ理由です。

1.2 欠けているのは境界の形

VPN の漏洩は技術者のあいだで長く議論されてきましたが、公開されている論述の 多くは「漏れる可能性があるので注意」の水準にとどまります。中国語圏の情報は 製品レビューが中心で、体系的な失効試験はほとんど見当たりません。

その水準では読者の助けになりません。「可能性がある」は次のいずれにも答えません。

- 接続ボタンを押してから保護が実際に効くまで、どれほどの空白があり、その間に 何が送出されるのか
- エレベーターで電波が切れて復旧するあいだ、漏洩は起きるのか
- VPN プロセスが OS に回収された場合、それに気づけるのか。通信は止まるのか、 平文で流れ続けるのか
- キルスイッチの代償は何か。何を防ぎ、何を防がないのか

いずれも測定可能です。それを測るのが本報告の仕事です。

1.3 本報告が答える問い

1. 各失効シナリオにおいて、クライアントの実アドレス、DNS クエリ、通信は トンネルの外へ出るか
2. 出るとすれば、どの範囲で、どれだけの間か
3. キルスイッチはどのシナリオで有効・無効か。その代償は何か
4. これらの失効を利用者は察知できるか

---

2. 脅威モデル

2.1 攻撃者

本報告が想定する攻撃者は、**被害者のいるローカルネットワークを支配して**います。 自宅のルーター、ホテルや空港の Wi-Fi、あるいは加害者が提供するテザリングです。 つきまとい事案では極めてありふれた位置――同居者、元パートナー、住居の通信機器を 管理する者は、自然にこの位置を得ます。

攻撃者は端末に侵入する必要も、暗号を破る必要もありません。必要なのは **見ること**だけです。どのパケットが実アドレスで出ていくか、どのドメインが 問い合わされたか。

2.2 能力の仮定

攻撃者にできること：

- ローカル網上の全通信とその送信元アドレスを観測する
- ローカル DNS リゾルバの指定を含む DHCP 設定を配布する
- そのリゾルバを経由する全クエリを観測・記録する
- ローカル網上でサービスを稼働させる

攻撃者にできないこと：

- WireGuard トンネル内部の復号
- 被検端末上でのコード実行
- トンネル終端の掌握

つまり本報告が扱うのは完全に**迂回**の問題です。暗号は破られておらず、 一部のものがそもそも暗号化経路に入っていないだけです。

2.3 被害者の状況

WP-001 の仮定を引き継ぎます。被害者はすでに監視の可能性を察知して対策を とっており、**技術知識は限られて**います――一般的な助言に従って VPN を導入し、 画面に「接続済み」と表示されるのを見て、所在地は保護されたと考えています。

その認識と実際の状態との隔たりが、本報告の検証対象です。

---

3. 実験方法

3.1 環境とトポロジ

実験は EVE-NG ネットワークエミュレーション環境で行いました。四ノードはいずれも Debian 13 で、シリアルコンソール経由のスクリプトによって全自動で操作され、 人手の介入はありません。

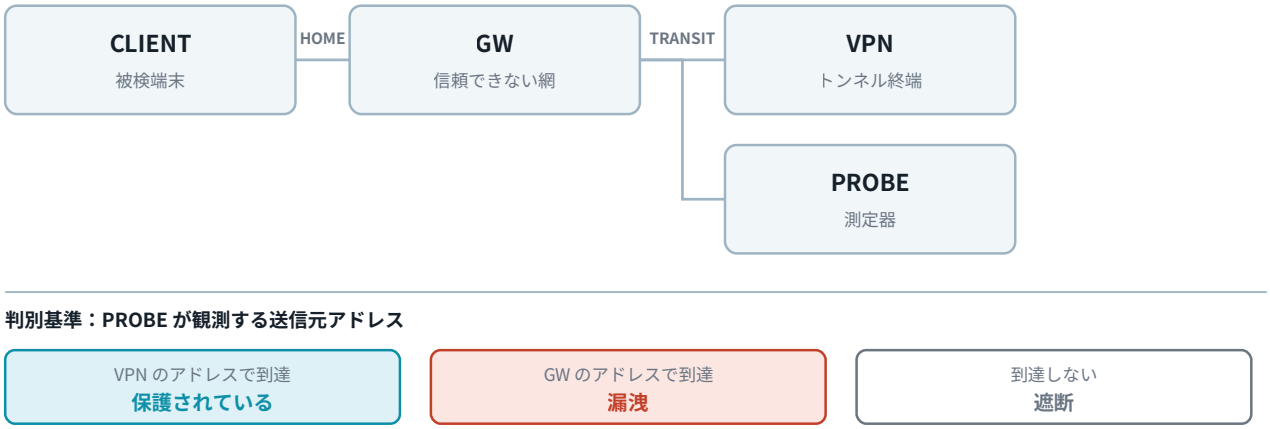

図 1：実験トポロジと判別基準

ノード	役割
CLIENT	被検端末。DHCP で信頼できない網の設定を取得し、WireGuard トンネルを確立
GW	家庭用ルーター／信頼できないローカル網。DHCP、ローカル DNS リゾルバ、対外 NAT
VPN	トンネル終端。トンネル通信はここから自身のアドレスで送出される
PROBE	測定器。権威 DNS と HTTP／UDP 受信端。各要求の送信元アドレスを記録

アドレスはすべて RFC 5737 と RFC 3849 の文書用範囲を用いており、読者が再構築 しても実在の網と衝突しません。

3.2 判別の原理

測定全体がただ一点に依拠します。**PROBE が観測する送信元アドレス**です。

観測された送信元	判定
VPN のアドレス	トンネル経由で送出、保護されている
GW のアドレス	漏洩——トンネルを迂回して直接送出
到達しない	遮断（キルスイッチ作動）または消失

この判別が成立する前提は、**二つのセグメント間に迂回路がないこと**です。測定前に 検証済みで、GW に NAT を設定していない状態では CLIENT はいかなる方法でも TRANSIT セグメントへ到達できません。この検証がなければ送信元アドレスは経路と 一対一に対応せず、測定全体が意味を失います。

3.3 ビーコンの設計

時間窓の測定には 20 ミリ秒間隔の UDP ビーコンを用います。HTTP ではなく UDP を 選んだのは意図的です。UDP は接続状態も再送もハンドシェイクも持たないため、 送出できたか否かがその瞬間の経路と filtering の状態を忠実に反映します。 **TCP の再送は時間軸を均してしまい、窓の境界が測れなくなります。**

ビーコンと擾乱（たとえば「接続コマンドの発行」）は**同一プロセスの同一時計**の 上で動きます。二つのプロセスに分ければプロセス起動のジッタ——実測で数十ミリ秒、 測定対象と同じ桁——を扱わねばなりません。時間の計算はすべてクライアント自身の 単調時計上で完結し、PROBE は送信元の帰属のみを担うため、ノード間の時刻同期は 一切不要です。

各ビーコン番号の結末は三通りしかありません。VPN のアドレスで到達、GW の アドレスで到達、到達しない。この三つで対象となる全事象を覆えます。

3.4 シナリオと対照

八シナリオ、各セル 30 回、計 510 回。s1 から s6 は各二変種、s7 は帰属を 切り分けるため補足の変種を一つ加えています（4.4 節を参照）。

シナリオ	擾乱	基準群	対照群
s1 確立の空白	接続コマンド発行	キルスイッチなし	あり
s2 リンクの断続	2 秒切断後に復旧	キルスイッチなし	あり
s3 インターフェース消失	トンネル IF を削除	キルスイッチなし	あり
s4 IPv6	定常状態	`AllowedIPs` が v4 のみ	`::/0` を含む
s5 DNS	定常状態	リゾルバを引き継がない	引き継ぐ
s6 ポータル例外	トンネル未確立	ローカル網の例外あり	厳格なキルスイッチ
s7 範囲外	定常状態	VPN 未使用	フルトンネル＋引き継ぎ＋厳格なキルスイッチ （補足群：同一構成でキルスイッチなし）
s8 スタブリゾルバ	定常状態	リゾルバ指定なし	リゾルバ指定あり

各変種が変えるのは一点のみです。 一つの変種が二箇所を同時に変えれば、差が 出てもどちらに帰属するか判断できません。s4 ではサーバー側を両群ともデュアル スタックで用意し、被検変数はクライアントの `AllowedIPs` だけです。

s3 の擾乱の選び方には説明を要します。第一版では「トンネル対向の削除」で失効を 模擬しましたが、それでは何も測れません。インターフェースは残り経路もそこを 指したままなので、パケットは黙って破棄されるだけで**漏洩しません**。真に危険 なのはインターフェースが経路ごと消えることで、通信はただちに元の既定経路へ 戻ります。**擾乱の選択を誤ると偽の陰性を測ることになります。**

3.5 測定器の検証

本研究の過程で三度の**静かな失効**に遭遇しました。測定器はすでに壊れているのに、 真の陰性結果とまったく同じ見え方をするものです。気づかなければ、そこで得られた 「漏洩なし」が結論として書かれていたはずです。

1. **クライアントが IPv6 を取得できない**：ノードイメージがルーター役のために IPv6 転送を既定で有効にしており、Linux は転送が有効なときルーター広告を 受け付けません。クライアントには IPv6 アドレスがまったく存在せず——IPv6 漏洩 試験は「漏洩なし」と出ますが、それは漏れる v6 がそもそも無いからです。
2. **ルーターがルーター広告を送出できない**：`ip addr flush` は `fe80::` link-local アドレスも一緒に消去し、しかも自動では復活しません。一方、広告は link-local を送信元としなければなりません。**失敗は完全に静かです**。DNS サービスは毎回の広告を送信済みとしてログに記録するため、ログ上は正常に見え、 実際にはパケットキャプチャにクライアントの要請だけが映り応答は皆無でした。
3. **設定は適用されたのに効いていない**：トンネル設定内のリゾルバ指定は システムのリゾルバ管理機構を経て有効になりますが、本実験は「クライアントが どこに問い合わせたか」を直接観測するためその機構を停止していました。結果として 設定は適用されたように見えてリゾルバは変わらず、対照群は基準群と完全に同一に なりました。

ここから一つの原則が導かれます。同種の測定を行う方にも推奨します。

> **各シナリオを開始する前に、測定器自体が測定可能な状態にあることを検証する。 結果を直接見に行かない。**

三項目はいずれも否定的検査としてプロビジョニングスクリプトに組み込みました。 たとえば link-local が復活しなければ、壊れた測定器の上で実験を走らせずに中断 します。

---

4. 測定結果

以下の数値は 30 回実行の中央値、括弧内は四分位範囲です。平均値ではなく中央値を 用いるのは、この種の遅延分布が右に歪んでおり、平均は少数の外れ値に引かれるため です。

4.1 状態型の失効

シナリオ	キルスイッチなし	あり
s1 接続コマンド→保護発効	53.3 ms（52.8–71.9）、その後も **2 パケット**漏洩（最悪 4）	53.4 ms（53.2–53.5）、漏洩 **0**
s2 2 秒切断後に復旧	復旧後 47.8 ms で再保護、漏洩 **0**	43.2 ms、漏洩 **0**
s3 トンネル IF 消失	**すべてのパケットが漏洩**し、止まらない	事象の 8.6 ms 前が最後の到達、以後完全に沈黙、漏洩 **0**

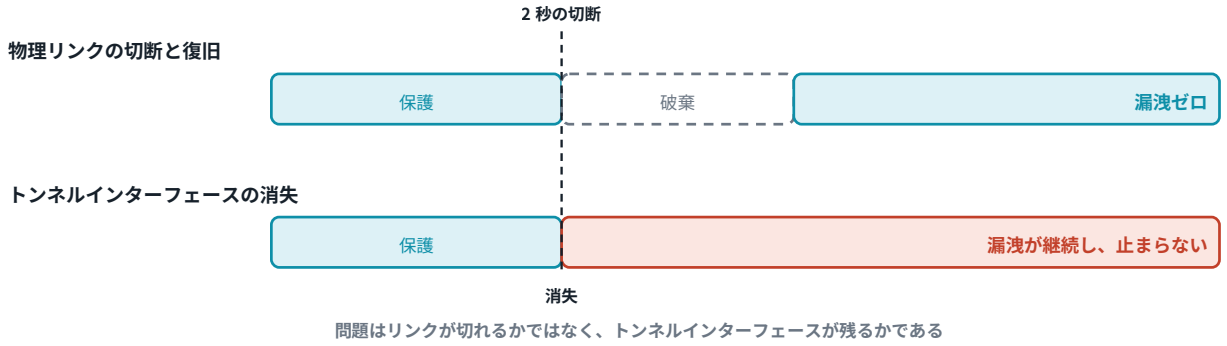

図 2：二つの失効を同一時間軸で比較

三項それぞれに注目点があります。

s1：利用者が接続を押した後、保護は即座には効きません。本環境では約 53 ミリ秒 の確立期間に、なお 2 ないし 4 個のパケットが実アドレスで送出されます。主観的には 「もう接続した」状態ですが、実際にはまだです。

s2 は本報告で最も直感に反する結果です。物理リンクを切断して復旧させても、 30 回すべてで**漏洩ゼロ**でした。トンネルインターフェースとその経路は切断中も 存在し続け、パケットはトンネルへ入って対向不達により破棄されます（約 102 個の 番号欠落として観測できます）。**物理インターフェースへは迂回しません。** 網の 切り替え、エレベーター、電波断はすべてこの類型です。

s3 はその逆です。インターフェース自体が消えると経路は物理インターフェースへ 戻り、以後すべてのパケットが実アドレスで送出されます。しかも**自然には止まらず**、 測定窓が閉じる時点でも漏洩し続けていました。対応する現実の事象は、VPN プロセスの 異常終了、OS による回収、スリープ復帰後の未再構築です。

4.2 設定の欠落

シナリオ	基準群（よくある既定）	対照群（正しい設定）
s4 IPv6 通信	v4 のみのトンネル → **100% 漏洩**（30 回すべて）	`::/0` を含む → 0.7%
s5 DNS クエリ	リゾルバを引き継がない → **100% 漏洩**（30 回すべて）	引き継ぐ → **0%**

両基準群ともばらつきはゼロです。**確率の問題ではなく、設定が決める必然です。**

s4 対照群に残る 0.7% は、トンネル確立前に送出された 2 パケット——s1 で測った 尾と同じものであり、IPv6 に固有の問題ではありません。

s8：スタブリゾルバの下での同じ問題。 s5 では「クライアントがどこへ問い合わ せたか」を直接観測できるようにするため、システムのスタブリゾルバを意図的に停止 していました。しかし現実のデスクトップでは既定で有効です。s8 はそれを有効にした 条件で測り直しました。各セル 30 回、毎回 10 個の重複しない名前（各セル 300 クエリ）です。

測定項目	リゾルバ指定なし	リゾルバ指定あり
トンネルのみを通った名前	0	**10 / 10**
ローカルリゾルバのみを通った名前	**10 / 10**	0
両方へ送られた名前	0	0

部分的な漏洩も、二重送信もありません。 この組み合わせでは、トンネルによる リゾルバの引き継ぎは完全に有効でした。その機構は、トンネルインターフェース上に 全ドメインを覆うルーティングドメインを設定するもので、スタブリゾルバはこれに より他のインターフェースへクエリを振り分けなくなります。この点は説明に値します。 スタブリゾルバの split DNS 機構こそ「一部のクエリがローカルへ流れる」原因に なりうるものですが、本実験ではその現象を観測しませんでした。

4.3 例外そのもの

キャプティブポータルの例外は、ホテルや空港のポータルにログインできるように するためのものです。その時点でトンネルは未確立なので、ほぼすべてのキルスイッチ 実装がローカル網を許可します。

変種	信頼できない網に到達したパケット	完全遮断
厳格なキルスイッチ	**0**	30/30 回
ポータル例外あり	**226**（30 回とも同一）	0/30 回

観測点は GW に置きました。攻撃者が支配しているのはまさにローカル網であり、 そこへ届いたパケットはすでに相手の手中にあります。現実世界での誘導手段は DNS です。例外下でもローカルリゾルバには到達できるため、攻撃者はローカル網の アドレスを返すだけで足ります。

キルスイッチは終始正常に動作しているのに、通信は外へ出ていきます。八つの シナリオのなかで最も気づきにくいものです。利用者にはキルスイッチが有効だと見えており、 実際に有効だからです。

4.4 範囲外

前三類型の失効に共通する形は「トンネルに入るべき通信が入らなかった」ことです。 第四の類型は異なります。**そもそもトンネルに一度も入ったことのない通信が、 まとまって存在する**のです。トンネルはそれらを運ぶよう設定されたことがなく、 一部は IP の通常の出力経路すら通りません。

観測点は GW、すなわち信頼できないローカル網の側に置きました。三つの構成を それぞれ 30 回測定しています。

観測項目	VPN 未使用	すべて正しい構成	補足：同一構成でキルスイッチなし
クライアントが送出したフレーム（中央値）	23	6	22
識別可能な情報の項目数	10	**4**	9

三セルとも識別可能な情報の項目数の**ばらつきはゼロ**です——30 回の実行結果が 完全に一致しました。

「すべてを正しく設定した」構成でも**なお外に出る四項目**と、キルスイッチが それを防げない理由は次のとおりです。

なお取得できる情報	防げない理由
MAC アドレス	イーサネットフレームは必ず実 MAC を載せます。厳格なキルスイッチの下で出ていける唯一のフレームはトンネル自身のものですが、それも同じく実 MAC を載せています
OUI（NIC ベンダー）	MAC の先頭 3 バイトから直接得られる
ホスト名	DHCP はホスト名を平文で載せ、その要求は生ソケットを通るため IP 出力チェーンを経由しない
ローカルアドレス	ARP は異なるフィルタ系統に属し、同じく IP 出力チェーンを経由しない

補足の変種により、原因を項目ごとに帰属させられます。

- **トンネル自体が取り除いたのは一項目だけ**でした（NTP）。これは通常の ルーティングされる IP 通信であり、フルトンネル設定に一括して運ばれます。 残る九項目に、トンネルは触れてもいません。
- **別の五項目を取り除いたのはキルスイッチであって、トンネルではありません**： mDNS、LLMNR、そして IPv6 のルーター要請、近隣要請、MLD はいずれも IP 出力 経路を通るため、遮断規則に当たります。
- **四項目はどちらでも防げません**。理由は上表のとおりです。

この類型の意味：キルスイッチは終始有効、トンネルは終始存在し、リゾルバも 確かに引き継がれている——それでも信頼できないローカル網は、この端末が誰かを 知っています。それは「漏洩」ではなく、運ぶ範囲の境界です。まさにそのために、 前三類型の対策はここではすべて無効です。

> **本節が支持できない推論**：本実験が試験したキルスイッチの実装は一種類だけ です（IP 出力チェーンに作用する規則集）。**これをもって「いかなるキルスイッチも ARP と DHCP を防げない」と推論してはなりません**——ネットワークデバイス層の 送出フックに作用する規則集は未試験です。また、識別可能な情報の一覧は本 クライアントに導入されたソフトウェアに左右されます。本実験の DHCP クライアントは ベンダークラスとクライアント識別子を既定で送出しないため、ここで測ったのは 「送出されなかった」であって「その経路が存在しない」ではありません。他の OS は 送出します。

4.5 総合

通信／事象	既定設定での結果
IPv4 定常	保護される
IPv4 物理リンクの断続	保護される
IPv4 トンネル IF 消失	**100% 漏洩、しかも止まらない**
IPv4 接続直後の数十ミリ秒	2–4 パケット漏洩
IPv6 すべて	**100% 漏洩**
DNS クエリすべて	**100% 漏洩**
ポータル例外下	**100% 流出**（キルスイッチが正常動作していても）
ローカル網上の身元情報	**すべて正しくても四項目が外に出る**（MAC、OUI、ホスト名、ローカルアドレス）

---

5. 考察

5.1 四類型、四つの対策

類型	シナリオ	対策	キルスイッチ
状態	確立の空白、断続、IF 消失	キルスイッチ	✔ 有効、代償なし
設定の欠落	IPv6、DNS	正しい設定	✘ 効果なし
例外そのもの	ポータルがローカル網を許可	ログイン後に解除	✘ 例外により無効化
範囲外	ARP、DHCP のホスト名、イーサネット層の MAC	端末層の対策へ：MAC の無作為化、ホスト名を送らない	✘ 触れられない

図 3：四類型の失効とそれぞれの対策。キルスイッチが覆うのは第一類型のみです。

この区分が本報告の主要な実用的産物です。「VPN は安全か」という曖昧な問いを、 答えの異なる四つの具体的な問いに分解します。**そのうち三つを正しく行っても、 残る一つを補償しません。**

前三類型の違いは「トンネルが運ぶべきものをきちんと運べたか」にあります。 第四の類型の違いは、**それらの情報がはじめからトンネルの責務の範囲にない** ことにあります。VPN を「姿を消すもの」と捉える人が最も誤解しやすいのが、 まさにこの類型です。買ったのは見破られないことだと思っていても、実際に 買ったのは通信の中身と宛先を見られないことです。

5.2 キルスイッチの代償は思われているより小さい

よくある懸念は、キルスイッチが接続を遅くするというものです。測定はそれを否定 します。キルスイッチの有無でトンネル確立時間に**統計的な差はありません** （s1：53.3 対 53.4 ミリ秒、s2：47.8 対 43.2 ミリ秒）。

接続が遅くなるのではなく、露出がパケットの破棄に置き換わるだけです。s1 では 漏洩するはずだったパケットが手元で止められ、s3 では漏洩を防げる唯一の機構と なります。

5.3 「切断こそ危険」という直感が誤りである理由

多くの人は VPN の漏洩を「接続が切れた瞬間に丸裸になる」と想像します。s2 の 結果はそうではないことを示します。トンネルインターフェースが存在するかぎり、 切断中のパケットは迂回ではなく破棄されます。

真に危険なのはインターフェースの消失であり、それは利用者から**見えません**。 通信は完全に正常で、ページも普通に開き、兆候は何もありません。手がかりになり うるのは、利用者が注意を向けない場所だけです——VPN アプリのアイコンの状態や、 通知領域から静かに消えたトンネルの表示です。

この隔たり自体が risk です。**利用者は「まだネットに繋がるか」で保護の有無を 判断しますが、その判定基準は最も危険な状況でこそ誤った答えを返します。**

6. 利用者向けチェックリスト

以下の各項目は互いに独立しています。順に確認してください。

一、IPv6 はトンネルの内側にあるか トンネル設定の許可範囲が IPv4 と IPv6 の双方を含むことを確認してください。 利用中の VPN が IPv6 に対応していない場合は、トンネルの外を流れるに任せるより、 OS の層で IPv6 を無効化するほうが安全です。

二、リゾルバはトンネルに引き継がれたか 接続後、システムが実際に使用している DNS サーバーが、ローカル網から配布された ものではなくトンネル提供のものへ変わっていることを確認してください。 **設定ファイルに書いてあることと、効いていることは別です**——本研究でもまさに、 設定は適用されたように見えてリゾルバは変わらず、エラーも出ない事例に遭遇しま した。システムの実際の状態で判断してください。

三、キルスイッチの例外は解除したか 公衆 Wi-Fi のポータルにログインするためにローカル網を許可した場合、 **ログイン完了後にその例外を解除してください**。例外が存在するあいだ、 キルスイッチはローカル網に対して無効です。

四、ローカルネットワークは依然としてこの端末を見分けられる 以上の三点をすべて正しく行っても、信頼できないローカル網はあなたの MAC アドレス、OUI（NIC ベンダー）、ホスト名、ローカルアドレスを取得します。 「この網にこの端末を認識させたくない」ことが脅威モデルに含まれるのであれば、 必要なのは端末層の対策です——MAC アドレスの無作為化、ホスト名を識別性のない 文字列に変更すること——**いかなる VPN 設定でもありません**。

もう一つ、理解しておくべき限界があります。**「ネットが繋がるかどうか」から保護の 有無は判断できません。** 最も危険な状況で通信は完全に正常です。身体の安全に 関わる状況であれば、アプリの状態表示に頼らず、重要な操作のたびに対外アドレスを 自ら確認してください。

7. 実装者への提言

1. **インターフェースの消失は失効事象として扱い、能動的に通知すべきである**： 現在の挙動は静かなフォールバックであり、利用者は気づきようがありません。 本研究で最も害が大きく、かつ最も修正が容易な項目です。
2. **ポータル例外は自動失効すべきである**：時間制限を設けるか、トンネル確立後に 自動的に撤回する。例外が無期限に存在することは、最も必要な場面でキルスイッチを 無効化することを意味します。
3. **リゾルバの引き継ぎは検証可能であり、失敗時には報告すべきである**：設定の 適用に失敗しても何も表示されなければ、利用者は誤った安心のもとで操作します。
4. **確立期間中のパケットは既定で遮断すべきである**：測定はそれが確立遅延を 増やさないことを示しています。
5. **キルスイッチの作用範囲は正直に開示すべきである**：IP 出力チェーンに作用 する規則集は ARP と DHCP には届きません。製品の画面がキルスイッチを 「すべての通信を遮断する」と表示しているなら、それは実装と一致しない説明 です。この二つも対象に含めるには、規則をネットワークデバイス層の送出フック まで下ろす必要があります。

6. **利用者のホスト名を信頼できない網へ渡すべきではない**：DHCP のホスト名 オプションは平文で送出されますが、自分の端末が識別可能な名前を広めている ことを多くの利用者は知りません。プライバシーを訴求する製品は「接続時に MAC アドレスとホスト名を無作為化する」選択肢を用意し、その限界も併せて 説明すべきです。

---

8. 研究の限界と今後の課題

8.1 外的妥当性の境界（最も重要）

本報告の被検対象は手動設定の `wg-quick` であり、いかなる市販 VPN アプリケー ションとも同一ではありません。

市販製品は独自のキルスイッチ、リゾルバ引き継ぎ、再接続ロジックを実装しており、 その挙動は本実験とまったく異なりうります——より良いかもしれず、より悪いかも しれません。本報告はいかなる市販製品も試験しておらず、製品評価として引用されて **はなりません**。

本報告が支持できるのは、これらの失効モードがプロトコルと経路制御の層で **起こりうる**こと、およびその測定手法が実行可能かつ再現可能であることです。 特定の製品の挙動を知るには、その製品を別途試験する必要があります。それは エミュレーション環境ではなく実機を要する、性質の異なる作業です。

8.2 測定分解能

ビーコン間隔は 20 ミリ秒であり、すべてのミリ秒値はこの量子化誤差を含みます。 s1 の 53.3 ミリ秒は実際にはおよそ 33〜53 ミリ秒の範囲にあります。間隔を短くすれば 分解能は上がりますが、測定自体がシステムに与える擾乱も大きくなります。

8.3 環境の差異

実験はエミュレーション網で行っており、リンク遅延は現実の網より大幅に小さい です。実環境での確立時間はより長くなるため、本報告の時間窓は典型値ではなく **下限**として読むべきです。

s1 の「実行全体で 53 パケット漏洩」という数値は結論に含めていません。それは 実験パラメータ（接続前 1 秒の基線）の産物だからです。現実にはその長さは利用者が 接続するまでの時間に依存し、数秒のこともあれば起動からずっとということもあります。

8.4 今後の課題

- 実機上の市販 VPN アプリケーションに対する同種の測定
- ネットワークデバイス層の送出フックに作用するキルスイッチが ARP と DHCP を 覆えるか（4.4 節では未試験）
- 他の OS の DHCP クライアントが送出する識別可能なフィールド（ベンダークラス、 クライアント識別子）
- モバイルプラットフォームのスリープ・復帰時の挙動
- 測定環境自体の梱包。非技術者が自分の設定を試せるように

8.5 求めるフィードバック

本報告の環境で他の構成や製品を試験し、異なる結果を得られた場合はお知らせ ください。本報告の手法に欠陥があるとお考えの場合も同様です。実験環境を完全に 公開しているのは、まさにそうした検証を可能にするためです。

付録 A：再現の手順

実験環境のトポロジファイルと全スクリプトは本報告とともに、以下のアドレスで 公開しています。

https://odysec.org/research/wp-002-lab-vlk-274.tar.gz

展開すると `vlk-274/` ディレクトリになります。

環境は自由に入手できる Debian 13 のみを使用し、**合法的に再配布できないイメージを 意図的に一切使用していません**。したがって読者は完全に再構築できます。四つの プロビジョニングスクリプトはいずれも冪等で反復実行可能であり、本研究の期間中に 環境をゼロから三度再構築しています。

再現手順、測定ツールの用法、記録形式は当該ディレクトリの説明文書にあります。

付録 B：全データ

各実行の生結果は JSON Lines 形式で、上記アーカイブ内の `vlk-274/data/` に計 510 件を 公開しています。集計スクリプト `aggregate.py` により本報告の全統計量を再現し、CSV を 出力できます。

付録 C：用語対照

中文	English	日本語
隧道	tunnel	トンネル
隧道介面	tunnel interface	トンネルインターフェース
洩漏	leak	リーク
中斷開關	kill switch	キルスイッチ
允許範圍	allowed IPs	許可 IP 範囲
解析器	resolver	リゾルバ
解析器接管	resolver takeover	リゾルバの引き継ぎ
路由器公告	router advertisement	ルーター広告
信標	beacon	ビーコン
建立空窗	establishment gap	確立までの空白
入口網頁	captive portal	キャプティブポータル
對照組	control group	対照群
離散度	dispersion	ばらつき
外部效度	external validity	外的妥当性
範圍之外	out of scope	範囲外
可識別資訊	identifying information	識別可能な情報
網卡位址	MAC address	MAC アドレス
網卡廠商代碼	OUI	OUI
主機名稱	hostname	ホスト名
送出鏈	output chain	出力チェーン
原始通訊端	raw socket	生ソケット

付録 D：出典

本報告のデータはすべて当チームが構築した制御環境から得たものであり、外部の データ出典はありません。プロトコルの挙動は WireGuard 公式文書および `wg-quick` マニュアルに、アドレス範囲は RFC 5737 と RFC 3849 に依拠します。

本報告は WP-001『すぐそばの目：近距離監視の検出と対応』と同じシリーズに属し、 脅威モデルを共有します。

引用の書式：Odysec（2026）『トンネルの外側：VPN の保護境界を測定する』 Odysec 研究報告 WP-002、バージョン 1.0。

免責事項：本報告は技術研究および教育目的であり、法的助言を構成しません。 個別事案の法的評価は弁護士にご相談ください。台湾で身体の安全に差し迫った危険が ある場合は 110 番へ、保護サービスおよび相談専用回線は 113 番です。