



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-003 | バージョン 1.0 | 発行日 2026-08-24 研究ライン：融合領域（Cyber × Physical） DOI：[10.5281/zenodo.22081706](https://doi.org/10.5281/zenodo.22081706) ライセンス：[CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) — 出典を明示すれば自由に配布・改変できます。

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	3
要旨	3
1. 問題の所在	4
2. 脅威モデル	5
3. 実験方法	5
4. 測定結果	8
5. 考察	10
6. 利用者向けチェックリスト	11
7. 実装者への提言	12
8. 研究の限界と今後の課題	12
付録 A：再現の手順	13
付録 B：全データ	13
付録 C：用語対照	14
付録 D：出典	14

本報告の性質について

本報告は、当チームが自ら測定したデータを掲載する最初の報告です。すべての数値は完全に公開された制御環境から得られたものであり、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ます。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、六つの失効シナリオをそれぞれ 30 回、計 360 回測定し、三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. **失効は三類型に分かれ、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**。
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。）

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。

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-002『ポケットの中の密告者』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、その間に何が送られるのか
- 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せされたか。

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・WP-002 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。



判別基準：PROBE が観測する送信元アドレス



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ー——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

六シナリオ、各二変種、各セル 30 回、計 360 回。

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

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。

- 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。
- 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

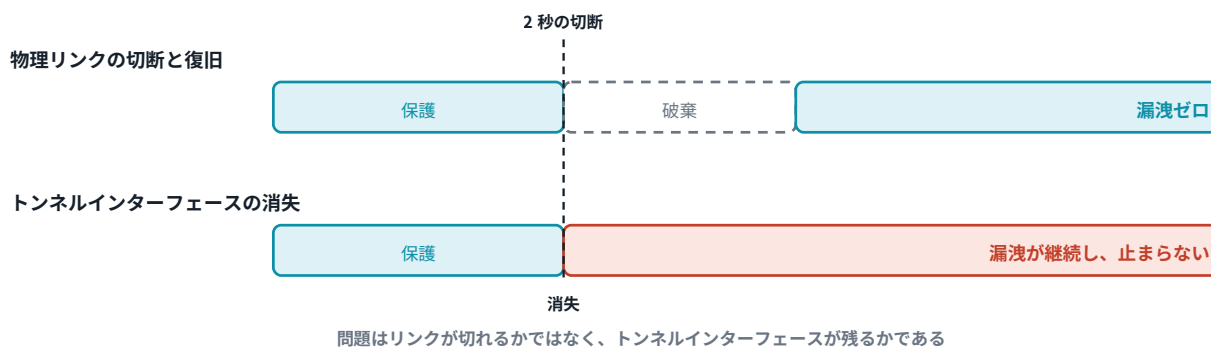


図 2：二つの失効を同一時間軸で比較

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。

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。六つ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 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）

5. 考察

5.1 三類型、三つの対策

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

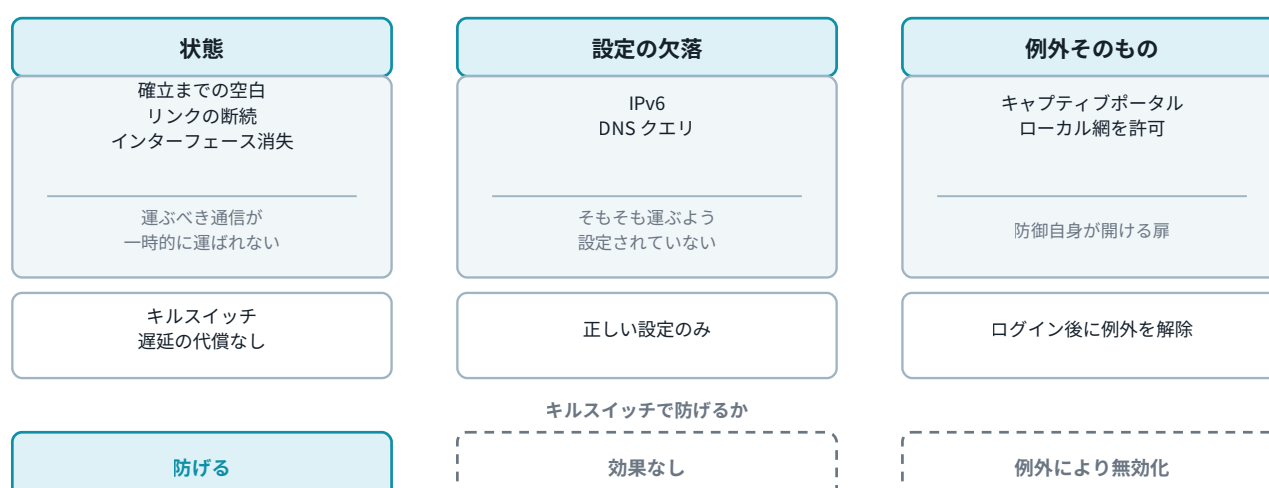


図 3：三類型の失効とそれぞれの対策

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、答えの異なる三つの具体的な問いに分解します。そのうち二つを正しく行っても、残る一つを補償しません。

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

以下の三点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。

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對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。

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
- スタブリゾルバを備えた構成（本実験では観測可能性のため停止）
- 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 `labs/v1k-274/` に公開されます。

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 `labs/v1k-274/data/` に、計 360 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

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 『音のない追跡』、WP-002 『ポケットの中の密告者』と同じ研究ラインに属し、三者は脅威モデルを共有します。

ライセンス：本報告はクリエイティブ・コモンズ表示 4.0（CC BY 4.0）で公開します。出典を明示のうえ、転載・翻訳を歓迎します。

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-003、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。