分析・2026年5月26日

← 前へ·次へ →

実際のプライバシー対見かけのプライバシー：立てておくべき問い

第2サイクルの実務的総括。アーキテクチャ的プライバシーを備えたサービスと、宣言的プライバシーにとどまるサービスとを見分けるための問いである。機微データに何らかのデジタルツールを採用する前に、欧州の専門職のための問診票。

要するに： 同じ法的告知を掲げる二つのサービスが、まったく異なる振る舞いをすることがある。一方は技術的な設計によって守る。他方は契約上の約束によって守る。その違いは告知を読んでも分からない——具体的な問いを立てることで明らかになる。答えの質は、その内容そのものと同じくらい、製品について物語る。

アーキテクチャ的プライバシーと宣言的プライバシーの違い

このサイクルのこれまでの七本の記事を通じて、我々は同じ問題の異なる層をたどってきた。Schrems II をめぐる国際移転の法。各 Cuaderno を封印する暗号学的ハッシュという数学的な発想。kill switch というアーキテクチャ上の選択と、それにほぼ常に伴う制度的な捕捉。エンドツーエンド暗号化の仕組みと、鍵がどこにあるかという実務的な問い。ビジネスモデルに応じたインセンティブの整合。自己主権的な暗号学的アイデンティティ。比例的な戦略としてのセルフホスティング。各記事はひとつの角度を扱った。サイクル最後となる本稿は、それらをひとつの問診票にまとめる。

覚えておくとよい区別は単純である。プライバシーが*アーキテクチャ的*であるサービスがあり、プライバシーが*宣言的*であるサービスがある。前者は技術的な設計に組み込まれている。プライバシーの約束に対する一定の違反は、アーキテクチャがそれを許さないために、技術的に困難または不可能である。後者は法的告知の文面に託されている。一定の違反は、起これば契約上は制裁の対象となりうるが、技術的には何もそれを妨げない。二つのモデルはともに GDPR を満たしうる。だが一方は構築によって守り、他方は約束によって守るのであって、その違いは実務上きわめて大きい。

続く問いは、一方の場合をもう一方から見分けるために設計されている。これらは高度な技術的問いではない。誠実な提供者なら誰でも自社の公開文書で答えられる問いである。答えの質と精度は、答えそのものと同じくらい、その製品について物語る。問いは6つの層に分類されている。機微データのためにサービスを採用する前に、最初の直感が見いだす問いだけでなく、すべての問いを立てておくのがよい。

第1層：アーキテクチャ

先に一つ用語を定めておきたい。ここでいう *operador* とは、サービスを提供する企業のことだ――サーバーとソフトウェアを管理する主体であって、特定の個人ではない。それを踏まえると、根本的なアーキテクチャ上の問いはこうなる。operador は、送信者と受信者のあいだのコンテンツに対して何をするのか? 可能な答えは三つあり、それらを見分けられることが大切だ。三つとも、似た語彙で宣伝されることがあるからである。

- 第一に：コンテンツは operador のサーバーを平文で通過し、そこで operador は、しないと約束していても、それを読むことができる。
- 第二に：コンテンツは operador のサーバーを暗号化されて通過し、鍵がユーザーの端末にのみ存するなら、operador はそれを読むことができない。
- 第三に：コンテンツは operador のいかなるサーバーも通過しない。その具体的な流れには operador のサーバーが存在しないからである。

この三つのあいだの違いは程度の違いではない。種類の違いである。

補完的な問いは――暗号化についての Cuaderno ですでに立てたものだが――こうだ。コンテンツを読むことを可能にする暗号鍵を持っているのは誰か。ユーザーが、そしてユーザーだけが持っているなら、暗号化は本物である。それに加えて operador が――「アカウント復旧」や「端末間の同期」という名のもとであっても――いかなる形であれ持っているなら、暗号化は名目だけのものである。この問いは、中間的で誠実な答えを許さない。

第2層：ビジネスモデル

ビジネスモデルについての問いは、アーキテクチャの問いと同じくらい重要であり、しかも同じ実質的な理由による。インセンティブは、宣言された目的がまったく同じであっても、時を経るにつれて体系的に異なる製品を生み出す。operador は今日どのように稼いでいるか。単一の源か、二つか、混合か。資金源に広告またはデータの収益化が含まれる場合、どのデータが収益化され、GDPR のどの法的根拠のうえでそれが行われるか。法的告知で宣言された目的は、専門職がサービスに委ねようとする第三者のデータをも対象に含めているか。

そして、常に立てられるとはかぎらない二次的な問い。operador の三〜五年先の財務状況はどうか。ベンチャーキャピタル段階にある会社は、安定した収益にある会社とは異なる圧力のもとで動いている。資金調達モデルの変更は、繰り返し、ユーザーとの暗黙の契約が交渉なしに書き換えられる瞬間である。

第3層：法域

欧州の専門職にとって、法域の問いは修辞ではない。operador はどの法域で設立されているか。データを処理するサーバーは物理的にどの国にあるか。先の二つの問いへの答えは同じか異なるか、異な

る場合どの法律が適用されるか。米国企業が運営する欧州リージョンは、Schrems II の観点では欧州の答えではない。サーバーがどこにあろうと、その企業は FISA 702 に服している。

実務的な補完の問いはこうだ。明日、operador の法域で有効な情報機関の命令が、私や私の顧客のデータの引き渡しを求めてきたら、何が起こるか。誠実な答えが「会社はそれを引き渡す義務を負うだろう」で始まるなら、宣伝がいかに反対のことを示唆しようと、そのサービスはその命令から守らない。誠実な答えが「会社はそれを平文で持っていないので引き渡せないだろう」で始まるなら、そのサービスは守る。そしてその違いは、プライバシーポリシーの質ではなく、ほぼ全面的に最初の二つの層に依存する。

第4層：operador と kill switch

operador は、サービスを遠隔で停止、遮断、削除、または機能低下させるための技術的能力をどれだけ保持しているか。この問いは妄想的なものではなく、実務的なものである。デジタルプラットフォームは近年その能力を繰り返し行使してきた。あるときは自らの発意で、あるときは政府の命令のもとで、あるときは所有や方針の変更を経て。能力が存在するのであれば、それが契約上どのような前提として宣言されたもとで行使されるかを知り、宣言されていない前提のための余地を残しておくのがよい。近年の実務は、そうした前提が同じくらい重要であることを示してきた。すなわち、予期せぬ司法命令、国際的な制裁、企業統治の変更、別の方針を持つ事業体による買収である。

対となる問いは継続計画である。operador が――正当であれそうでなかれ、いかなる理由であれ――専門職に対してその能力を行使した場合、どれだけの稼働時間が引き続き利用可能か、どのようなデータのエクスポート手続きが存在するか、そしてどの代替の提供者へ移行できるか。答えが「そんなことは起こらないはずだ」で始まるなら、それは実務的な答えではなく、約束である。

第5層：アイデンティティとアクセス

サービスへのアクセス認証情報を管理しているのは誰か。operador がユーザーの関与なしにユーザーのアクセスをリセットできる場合――一般に「アカウント復旧」と呼ばれる手続き――、operador は技術的にアカウントの管理者であり、適切な手続きを通じて要求してきた者にそれを引き渡すこともできる。アイデンティティが暗号学的にユーザーの端末に存するために operador がアクセスをリセットできない場合、operador はそれを引き渡すこともできず、命令のもとでさえできない。二つの様式は文脈に応じていずれも正当だが、ここでもまた異なっており、どちらを採用しているのかを知っておくのがよい。

専門職がアクセスを失った場合、専門職のデータはどうなるか。operador に依存する復旧の仕組み――アカウントの、ファイルの、セッションの――は存在するか。operador がそれらを使うよう強要された場合、それらの仕組みはその分野の職業倫理と両立するか。

第6層：未来

この最後の層は、見通しを要するためにおろそかにされがちである。サービスが別の会社に買収されたら何が起こるか。ほとんどすべての買収には、その後数か月以内の利用規約の見直しが伴う。規制上の要求が変わったら何が起こるか。欧州法は2022年以降、削除と遮断の義務を増やしてきたのであって、減らしてはいない。operador が消滅したら何が起こるか。クラウドサービスの少なからぬ部分は、operador の閉鎖というシナリオに備えた文書化された脱出計画を持っておらず、専門職はもはや準備する時間がなくなってからその問題に気づく。

この層について覚えておくとよい定式がある。operador への依存が少ないアーキテクチャほど、operador の変化に対してより強靭である。あらゆる様式のセルフホスティング、自己主権的な暗号学的アイデンティティ、間にサーバーを介さない通信――これらはいずれも、現在の依存の面を減らすという手順によって、将来のリスクの面を減らす。それはリスクを消すのではない。減らすのである。

構造と約束の違い

このサイクルをただ一文に蒸留するとすれば、それはこうなる。構造的な答えは、operador も、行政も、法律も変わったとしても保たれる。約束による答えは、約束する者がそれを保てるかぎり、また保とうとするかぎり保たれる。両者は採用の時点ではどちらも正しいことがありうる。だが、時の経過と状況の変化に左右されずに持ちこたえるのは、二つのうち一つだけである。

これは、各専門職が採用するすべてのサービスに構造的な答えを要求すべきだという意味ではない。比例性は依然として正当である。内部経理のための表計算が必要とする答えは、患者の診療記録が必要とする答えと同じではない。意味するのはこうだ。専門職たることとは、それぞれの場合にどの種類の答えを受け入れたのかを知っており、その種類の答えがその具体的なデータに比例していると意識的に決めていることにある。

整理された問診票

このサイクルを総括する12の具体的な問い。それぞれの答えが次の問いに情報を与えるよう順序立てている：

1. コンテンツは operador のサーバーを通過するか。通過する場合：平文か、operador の鍵で暗号化されているか、それともユーザー専用の鍵で暗号化されているか。
2. エンドツーエンド暗号化がうたわれている場合、暗号鍵はどこにあるか。operador は、「復旧」を含むいかなる形であれ、その一部を知っている、または保持しているか。
3. サービスはどんなメタデータを生成し、保持するか。どれくらいの期間か。誰がそれを見られるか。
4. operador はどのように資金を得ているか。資金源に広告またはデータの収益化が含まれる場合、宣言された目的は、専門職が委ねた第三者のデータをも対象に含めているか。
5. operador の三〜五年先の財務状況はどうか。モデルの差し迫った変更を示唆する要因はあるか（上場の保留、枯渇しつつある資金調達ラウンド、起こりうる買収）。

6. operador はどの法域で設立されているか。サーバーは物理的にどの国にあるか。両者が異なる場合、処理にはどの国の法律が適用されるか。
7. operador の法域で有効な情報機関の命令が私のデータの引き渡しを求めたら、何が起こるか。会社は技術的にそれに従えるか。
8. operador は、サービスを停止、遮断、または削除するための技術的能力をどれだけ保持しているか。どのような契約上の前提のもとでか。歴史的に記録されてきた、どのような契約外の前提のもとでか。
9. operador がその能力を、正当にせよ不当にせよ、私に対して行使した場合の脱出計画はあるか。代替の提供者へデータを移行するための、文書化された手続きはあるか。
10. アクセス認証情報を管理しているのは誰か。operador は私の関与なしにそれをリセットできるか。それは私を守るのか、それとも私をさらすのか。
11. この具体的な機能について、欧州製の、セルフホスト型の、あるいは間にサーバーを介さない代替手段は存在するか。評価したリスクと比べて、その実際のコストはどれほどか。
12. 今日の決定が、五年後に検査官、監査人、あるいは漏えいの被害を受けた顧客によって精査されたとき、現在の選択は今日手元にある論拠で擁護できるものだろうか、それとも、もっともな問いを立てなかったことを詫びる必要が生じるだろうか。

これらの問いは完璧な答えを期待してはいない。誠実な答えを期待している。誠実な operador はそれを答えることができ、誠実さに欠ける operador は正確に述べることを避けるものだ。二種類の operador のあいだの実務的な違いは、大げさに言うつもりはないが、さらに詳しく尋ねる必要が生じる前にさえ、彼らが自発的に差し出す答えをゆっくり読むことで感じ取れることが多い。

本稿をもって Cuadernos Lacre の第2サイクルを締めくくる。Schrems II から受け継いだ編集上の負債から始め、実務的な問診票で終えた。その道のりで我々はいくつもの概念を――ハッシュ、暗号化、アイデンティティを――、そして応用的な分析を――kill switch、ビジネスモデル、セルフホスティングを――たどってきた。本誌が掲げた編集上の意図は、問題の網羅的なリストで読者を圧倒することではなく、いかなる新しいサービスを前にしても、自分がどの種類の答えを受け入れようとしているのかを見分けるための道具を手渡すことにあった。その見分け――アーキテクチャと約束のあいだの――こそが道具である。あとは、各専門職が自らの実務において問いに値すると見なすデータのために、それを役立てればよい。

参考文献および関連資料

- 本誌、第2サイクル（2026年5月）――*シュレムスII*、*5年後の現状*、*SHA-256 とは本当は何なのか*、*キルスイッチと制度的キャプチャ*、*エンドツーエンド暗号化を本当に説明する*、*信頼の指標としてのビジネスモデル*、*24の言葉：暗号学的アイデンティティとは何か*、*プロフェッショナルな実践としてのセルフホスティング*。この問診票が拠って立つ七本の記事。
- 規則（EU）2016/679――一般データ保護規則。問診票が立てるすべての問いの参照法的枠組みであり、とりわけ第5条、第6条、第25条、第28条、第32条、第33条、および第V章。
- 欧州データ保護会議――Schrems II、国際移転、影響評価、能動的責任に関する実務的なガイドラインおよび意見（2020-2024年の刊行物）。

- スペインデータ保護庁——2022-2024年に公表された、不適切な移転手段を用いた、または実質的内容を欠く形式的な影響評価を行った管理者に対する制裁。
- noyb.eu——Maximilian Schrems が率いる欧州デジタル権利センター。欧州のデータ保護規範の、見かけ上ではなく実際の遵守に関する申立て、不服申立て、分析の公開リポジトリ。

← 前へ専門的実践としてのセルフホスティング次へ →署名では解決できないこと

最近の記事

- 考察・2026年6月29日 あなたは匿名ではない
- 考察・2026年5月27日 署名では解決できないこと
- 分析・2026年5月25日 専門的実践としてのセルフホスティング

この記事をダウンロードして、必要な場所で活用してください。

↓ Markdown ↓ テキスト形式 ↓ PDF

ファイルはお使いのデバイスにダウンロードされます。そこから保存、Solo2 へのインポート、または任意の場所での共有が可能です。Cuadernos が送信先を決定することはありません。

封蝋・SHA-256 c0532b9176446d947b0e72f0d8d1fb1b1b2ad488c071566026c94e802a7f9976

Cuadernos Lacre・Menzuri Gestión S.L. による刊行物・
著者：R.Eugenio・編集：Solo2 チーム