分析 · 2026年5月16日

← 前へ·次へ →

真ん中に誰もいないとき

サーバーを通過するデータを暗号化することは内容を保護します。真ん中にサーバーを置かないことは、その問題を排除します。これらは同じではありません。

2人の人間、1つの会話

2人が部屋で向かい合って話すとき、誰も何も聞いていないと約束する必要はありません。そこにいなかったから聞いていないのです。2人が手から手へ紙を渡すとき、真ん中にいる誰かがそれを読んでいないと誓う必要はありません。真ん中には誰もいないからです。

日常生活のほとんどの事柄はこのように機能しています。私たちは、声を伝える空気や、手に持っている紙と秘密保持契約を結ぶことはありません。会話のプライバシーは仲介者の約束の上に成り立っているわけではありません。仲介者が存在しないからです。これはプライバシーを守る上で最も強力な形の1つです。何かや誰かが行儀良く振る舞うからではなく、何かや誰かが存在しないからです。

会話がデジタルチャネルに移行すると、これはデフォルトで変わります。通常のモデルは次の通りです。2人がサーバーに接続し、サーバーがメッセージを受け取り、暗号化するか暗号化して保存し、受信者に届けます。サーバーが真ん中にいます。サーバーは誠実かもしれません。監査されているかもしれません。有利な管轄区域で、厳格なプライバシーポリシーの下で運営されているかもしれません。これらすべてが真実かもしれません。しかし、サーバーは真ん中にいるのです。

暗号化と収集しないことの違い（第2部）

同シリーズの以前の記事で、コンテンツを暗号化することとメタデータを収集しないことは同じではないと主張しました。さらにもう一歩踏み込んで明確にするべきことがあります。サーバーを通過するデータを暗号化することと、サーバーを持たないことも同じではないということです。

最初のモデル（真ん中にサーバーがあり、コンテンツが暗号化されている）は、サーバーの運営者、保守担当者、システムを侵害する外部の攻撃者からコンテンツを保護します。そしてそれは重要です。しかし、サーバーを排除するものではありません。サーバーは依然としてそこにあります。メタデータを処理し続けています。依然として、裁判所命令、法的な介入、政治的圧力、またはセキュリティ侵害を受ける可能性のある場所です。誰かに信頼を置くことを必要とする場所であることに変わりはありません。

2番目のモデル（2つの末端の間にサーバーがない）は、暗号化されたコンテンツをより良く保護するわけではありません。暗号化が堅牢であれば、コンテンツはどちらの場合でも保護されます。変わるのはコンテンツではありません。変わるのは、*「サーバーはどうなるのか？」*という疑問の対象がなくなることです。疑問を呈する対象となるサーバーが存在しないからです。

信頼、不在、そして両者の違い

信頼は正しく置かれるかもしれません。誠実な企業は存在します。厳格な監査人も存在します。ユーザーに有利な法律も存在します。上記すべてを厳格に遵守する真面目なサービスも存在します。それに値する事業者に与えられる信頼は、悪い取り決めではありません。

しかし、信頼はどれほど堅固であっても信頼のままです。それは社会的な解決策であり、技術的な解決策ではありません。企業は所有者が変わるかもしれません。管轄区域は政府が変わるかもしれません。明日、裁判所命令が届くかもしれません。来月、新たな脆弱性が発見されるかもしれません。これらのどれも悪意から起こるわけではありません。事業者が存在し、存在するすべてのものは世界に起こりうる不測の事態にさらされているからです。

事業者が存在しないことは、同じ不測の事態にさらされません。裁判所命令は、存在しないサーバーにデータを要求することはできません。攻撃者は存在しないサーバーを侵害することはできません。企業のポリシー変更は、企業が一度も持ったことのないデータに影響を与えることはできません。重要なフレーズは単純です。存在しないデータは失われることはありません。

サーバー側の正当な主張について

真ん中にサーバーがあるプロフェッショナルなメッセージングサービスを提供する事業者は、通常、完全に有効な3つの主張を展開します。第1に、受信者がオフラインのときに配信を保証するためにサーバーが必要であること。第2に、コンテンツの暗号化は強力であり、したがって事業者はそれを読むことができないこと。第3に、サービスはヨーロッパの法律に準拠しており、データは法律によって保護されていること。

3つの主張はすべて真実です。どれも事の本質を変えるものではありません。遅延配信のためにサーバーがメッセージを保存できることは事実です。また、遅延配信が数十年にわたって改良され今日運用されている、デバイス間の直接通信プロトコルによって別の方法で解決できることも事実です。真面目なサービスでは、通信中のコンテンツの暗号化が強力であることは事実です。そして、ヨーロッパの法律が他の多くの場所よりもユーザーを保護しているのも事実です。

問題は、真ん中にサーバーがあるサービスが合法かどうか、安全かどうか、コンテンツを保護するかどうかではありません。それらはそうであり得ますし、合法であり、通常は安全です。問題は、真ん中にサーバーを持つことはアーキテクチャ上の選択であり、技術的な制約ではないということです。そして、すべての選択には結果が伴います。真ん中にサーバーがあるアーキテクチャは、信頼しなければならない行為者を必然的に生み出します。真ん中にサーバーがないアーキテクチャでは、そうなりません。

法律が言うこと、アーキテクチャがすること

GDPRは特定のアーキテクチャモデルを要求していません。データ最小化、目的制限、データ保護・バイ・デザインおよびデフォルト、コンプライアンスを証明する能力といった結果を要求しています。真ん中にサーバーがあるサービスは、これらすべての要件を満たすことができます。真ん中にサーバーがないサービスは、宣言によってではなく、その構造そのものによってそれらのいくつかを満たします。絶対的な最小化、つまりメッセージを配信するために厳密に必要なもの以外は何も収集しないことは、何かを収集できるサーバーが存在しない場合には些細なことです。

日常の機密性の高くない用途では、サーバーアーキテクチャは完全に合理的であり、真面目な事業者を信頼することは有効な取り決めです。その他の用途、つまり法規制に基づく職業上の秘密を伴うもの、倫理的責任を伴うもの、特に機密性の高い情報を扱うものについては、信頼の拠点が欠如していることは贅沢ではなく、構造的な利点です。

プロフェッショナルな読者のために

プロフェッショナルな通信サービスに直面したときに問うべき質問（本シリーズの過去の記事ですでにおなじみですが）には、もう1つのアーキテクチャ上の質問が追加されます。

1. 転送中にコンテンツを暗号化していますか？（おそらく「はい」。）
2. 私がいつ誰と話しているかについてのメタデータを生成し、保存していますか？（おそらく「はい」。）
3. 私のデバイスと受信者のデバイスの間にサーバーは存在しますか？
4. 存在する場合：誰が、どの管轄区域で運営していますか？そして、私に関するデータを引き渡すには何が起こる必要がありますか？
5. 存在しない場合：前の質問は無意味です。

2つのカテゴリーの違いは程度の問題ではなく、種類の問題です。クライアント、患者、または同僚に説明する時が来たとき、最も正直な表現は最もシンプルでもあります。一方には真ん中に誰かがいて、もう一方には誰もいない、ということです。

この記事で Cuadernos Lacre の初期サイクルは終了します。暗号化、メタデータ、職業上の秘密について話した後、私たちはアーキテクチャの全体像を完成させました。コンテンツを暗号化することと、真ん中にサーバーを持たないことは別のことです。どちらも合法かもしれませんが、信頼の起点を排除するのは後者だけです。

参考文献および関連資料

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984。システムの保証は中間のチャネルではなく、末端で実装されなければならないという原則の基礎的文献。

- 規則 (EU) 2016/679 第25条 — データ保護・バイ・デザインおよびデフォルト。
- 規則 (EU) 2016/679 第5条1項(c) — データ最小化の原則。
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton。設計によってデータ収集を最小限に抑えるアーキテクチャに関する章。

← 前へGDPR とビジネスチャット：なぜ多くの組織が知らずに違反しているのか次へ
→CUADERNOS_LIST_SCHREMS_TITLE

最近の記事

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

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 1557dc50da88162248e4cd4cae05801cc8e4b7304db32edbf00120b15df22385

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