考察 · 2026年5月16日

← 前へ·次へ →

デジタル時代における守秘義務

専門家と顧客の通信が技術的に不適切なチャネルで行われる場合、秘密は情報漏洩の日に破られるのではない。ツールを選択した瞬間に、すでに破られているのだ。

ほぼ誰も見ていない問題

弁護士が顧客から機密書類をスマートフォンで受け取る。医師が同僚と繊細な診断について相談する。心理士が精神科医と患者の治療方針を調整する。税理士が監査待ちの申告データを送信する。これらは全てインスタントメッセージで行われていますが、それらのメッセージが実際にどこに辿り着くのかを立ち止まって考える人はほとんどいません。

答えはほとんどの場合同じです：専門家が管理していないサーバー、必ずしも熟知していない法律が適用される国、そして直接的な経済的意味で「データを蓄積すること」をビジネスモデルとする企業の管理下にあります。メッセージは転送中に暗号化されているかもしれませんが、サーバーに到達した時点で、それは第三者のインフラに保存されたコピーとなり、その第三者の運用、法律、商業的決定に委ねられます。専門家の決定ではありません。

法規制が求めるもの

欧州一般データ保護規則（GDPR）の第32条は明確です：個人データを処理する者は、リスクに見合ったセキュリティレベルを保証するために「適切な」技術的および組織的措置を講じなければなりません。措置の適切さは、「アプリが何をしていると自称しているか」ではなく、実際のリスクに照らして測定されます。もし顧客データが、欧州経済領域と同等の保護レベルを保証しない法域のサーバーに辿り着いた場合、データ管理者（すなわち専門家）は、おそらく自分でも十分には認識していないリスクを負うことになります。

そして、これは GDPR だけの問題ではありません。弁護士、医師、心理士、監査人、ジャーナリストなどのために特別に規定されている守秘義務は、顧客との通信が機密であることを求めています。「可能な限り機密であること」ではなく、無条件に機密であることです。使用される技術的チャネルがこれを保証できない場合、専門家は職務倫理が許容しないリスクを冒していることになります。

パラドックスは、そのリスクが不可視であることです。オフィスのメッセージングを監査する人はいません。チャットプロバイダーにデータ処理契約を求める人もいません。リスクが表面化するのは、

常に手遅れになってからです。漏洩、公開された脆弱性、あるいはユーザーに通知されることなく他大陸で執行された裁判所の命令。これらが起きて初めて、リスクは現実のものとなります。

専門家が技術的に必要とするもの

守秘義務を負う人物が必要とするものは、要件の観点から見れば、実は驚くほどシンプルです：

- メッセージが、コピーを保存する中間サーバーを経由せず、送信者のデバイスから受信者のデバイスへ直接届くチャネル。
- 法域とポリシーが、宣伝文句ではなく設計（by design）によって GDPR と整合しているインフラストラクチャ。
- 業務上の連絡先（顧客名、電話番号、連絡先リスト）を第三者に引き渡すことなく、通信相手と本人確認を行う方法。
- プロバイダーの言葉に依存せず、メッセージが正しい相手に届いたことを確認できる検証可能なシステム。

これらは過度な要求ではありません。実のところ、デジタル化以前の専門的な通信においては当然のことと考えられていたものです。書留郵便はこれら全ての基準を満たしていました。オフィスの電話交換機から顧客の交換機への通話も同様です。奇妙なのは、今日これらの保証が求められていることではなく、デジタルチャネルへの移行過程で、誰も気づかないうちにこれらが失われてしまったことです。

「暗号化すること」と「保存しないこと」の違い

有用な比喩があります。メッセージを暗号化してサーバーに保存することは、書類を金庫に入れ、その金庫を見知らぬ人の家に置いてくることと同じです。金庫は頑丈です。書類は原則として読めません。しかし、書類は*依然として他人の家の中にあります*。そして、その他人は裁判所の命令を受けたり、サイバー攻撃を受けたり、サービス規約を変更したり、別の倫理観を持つ別の会社に買収されたり、あるいは明日消滅したりする可能性があるのです。

手続き的でも信頼ベースでもない、構造的な代替案は、書類をオフィスから一歩も出さないことです。専門家の机から顧客の机へと、いかなる仲介者も介さずに直接移動させることです。デバイス間のポイント・ツー・ポイント通信が技術的に行っているのはこれ、つまり仲介者の排除です。仲介者が悪だというわけではありません。ただ、守秘義務という文脈において、仲介者は*不要*なのです。そして、安全であることを目指すすべてのシステムにおいて、不要なものは原則として排除されなければなりません。

責任の問題

結局のところ、守秘義務を負うすべての専門家が、断固とした「イエス」で答えられるべき問いは以下の通りです：

> もし明日、顧客との会話が漏洩し、裁判所や職能団体から機密保持をどのように管理しているか問われたとき、自分が使用したチャネルが第三者のインフラにコピーを保存していないことを技術的に証明できるか？ 会話に関わった二人のデバイスからデータが一歩も外に出ていないことを証明できるか？ 他の大陸にある企業の言葉に頼ることなく、機密性が「約束」ではなく「アーキテクチャ」によって保証されていたことを証明できるか？

もし答えがノーであれば、問題は具体的なツールそのものではありません。問題は、ツールがサポートするように設計されていなかった責任を、ツールに委ねてしまったことです。それは機密ファイルを透明な封筒に入れ、郵便配達員が中を見ないことを信じるようなものです。

専門家が顧客との通信に選ぶツールは、その人物が顧客の信頼をいかに大切にしているかを物語ります。その信頼が約束ではなくアーキテクチャに依存するように設計されたツールが存在します。そして、そうでないツールも存在します。その違いを知ることは、仕事の一部です。

引用された法的枠組み

- GDPR（EU 規則 2016/679）、特に第5条、第25条（設計によるデータ保護）、第32条（処理の安全性）。
- 守秘義務に関する国内法（弁護士法、医師法、公認会計士法、個人情報保護法など）。
- 刑法等における業務上過失致死傷罪や秘密漏洩罪に関する規定。
- 守秘義務および職務上の秘密に関する専門職団体の倫理規程。

← 前へ「暗号化」＝「プライバシー」ではない：メタデータが物語る真実次へ →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

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 ab68a9914eb14002794ba0d198fc7d45d6d58e96d7f56d74bd1821b388869334

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

JavaScript のみで動作します。トラッカー、プロファイリング、データ共有は一切ありません。更新情報を受け取るには：RSS。