封蝋の小史

4世紀もの間、一滴の赤い蝋は、手紙が誰にも読まれていないことを保証していました。私たちはデジタル時代への移行でそれを失いました。しかし、取り戻すことは可能です。

紙以前

遠く離れた誰かに秘密裏に何かを伝える必要性は、文字よりも古いものです。メソポタミアでは、行政的または私的なメッセージが書かれた粘土板は、同じく粘土製のカプセルに入れられ、焼かれる前に封印されて送られました。内容を読もうとすれば、必然的にカプセルを壊すことになり、受け取った人は一目でカプセルが無事に届いたかどうかを知ることができました。古代ローマでは、羊皮紙の巻物は紐で縛られ、蝋や鉛で封印されました。その目的は常に同じです。いかなる不正な閲覧も、消すことのできない物理的な痕跡を残すようにすることでした。

封蝋の時代

中世の終わりから20世紀に至る数世紀の間、ヨーロッパにおける秘密通信の標準的な手段は、折りたたまれた紙を封蝋で封印することでした。溶けた蝋を紙の継ぎ目に流し込み、個人や機関の印章を押し当てました。これは装飾ではありませんでした。公証人、外交官、商人、そして一般市民も、同じ論理で使用していました。封蝋が完全で印章が識別可能であれば、内容は読まれていません。もし割れていれば、その手紙は開けられる前でさえ侵害されていることを意味しました。

封蝋の強みは、その費用や厳粛さにあるのではありません。極めて特異な構造的特性にありました。すなわち、それを剥がして再びつけようとするいかなる試みも、目に見える痕跡を残すということです。封印された手紙を気づかれずに開ける方法はありませんでした。そしてこれは、機密性が、配達人、御者、郵便局員といった仲介者の約束に依存するのではなく、封筒自体の物理的な設計に依存することを意味しました。それは誰かの言葉ではなく、証拠に基づく信頼でした。

デジタルへの移行

電信、電話、電子メール、企業向けメッセージング。電子通信は、速度、世界的な到達範囲、そして1通あたりほぼゼロのコストをもたらしました。同時に、封蝋の保証も奪い去りました。デフォルトでは、すべてのメッセージは仲介者を経由します。私たちがその誠実さを確認できるのは、利用規約に

書かれた約束、技術認証、そして不透明な監査を通じてのみです。私たちに警告してくれる、割れた蝋のしずくに相当するものは何一つありません。

デジタル封蝋

封蝋に力を与えていたのは、封蝋そのものではなく、それが表すものでした。つまり、第三者を信頼する必要のない、設計によって検証可能な完全性です。この特性は、デジタル領域で再構築することができます。ただし、1つではなく2つの要素が必要です。1つ目は暗号化された封印です。この出版物の各記事の下部に表示されているSHA-256ハッシュは、文字通りデジタル封蝋です。割れた蝋が不正な閲覧を暴露したように、コンテンツがいかなる変更を受けても、ハッシュは目に見えて変化します。2つ目は通信チャネルのアーキテクチャです。通信する2人の間にサーバーが存在しなければ、信頼を与えるべき仲介者も存在しません。検証可能な完全性と仲介者の不在という2つの要素の組み合わせは、折りたたまれた紙の上の赤い蝋が4世紀にわたって日常的に行ってきたことを、デジタルの世界で再現するものです。

その名前

この出版物がCuadernos Lacreと名付けられているのは、封蝋が歴史的な装飾ではなく、具体的な技術的特性だからです。つまり、いかなる事業者の約束もなく、構造によって検証可能な完全性です。シリーズの各記事は、現代のデジタル版におけるその同じアイデアの各部分を分析しています。暗号化、メタデータ、職業上の秘密、通信アーキテクチャ、ヨーロッパの法的枠組みなどです。この名前はまた、機密性とは契約するサービスではなく、情報が流通するチャネル自体の特性であることを思い起こさせるためのものでもあります。

参考文献および関連資料

- Maxwell, M. — *The Wax Tablets of the Mind: Cognitive Studies of Memory and Literacy in Classical Antiquity*, Routledge, 1992（メソポタミアの粘土板とブッラの封印に関する章）。
- Daybell, J. — *The Material Letter in Early Modern England: Manuscript Letters and the Culture and Practices of Letter-Writing, 1512-1635*, Palgrave, 2012。完全性と著作者の証明手段としての封蝋に関する章。
- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984。封蝋の原則の現代的な定式化。保証は中間のチャネルではなく、末端にあるべきである。

次へ →「暗号化」＝「プライバシー」ではない：メタデータが物語る真実

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 36d08a6bc8e5db2d0ceed6f4d95dc6ca4f13b444bf4ab4dcfe3b5334e268ce68
ES

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

当サイトはクッキーを使用せず、第三者のリソースも読み込みません。自社運用の匿名訪問者カウンター（欧州サーバー上の Umami）を使用し、ライト/ダークテーマの切り替えに必要な最小限の 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。