

# AKI セキュリティ



AKI は当社の独自技術、非対称鍵基盤（Asymmetric Key Infrastructure）の略称です。システム運用者に全てを委ねるモデルではなく、運用者、利用者それぞれがセキュリティの一端を担い**相互に検証**することで、IT リテラシーに依存しない **Zero Knowledge Proof** を実現します。

エンドポイント型セキュリティ、**Zero Trust Architecture** と親和性の高い基盤技術となります。

AKI は、SaaS(Software as a Service)として、Amazon Marketplace から提供します。

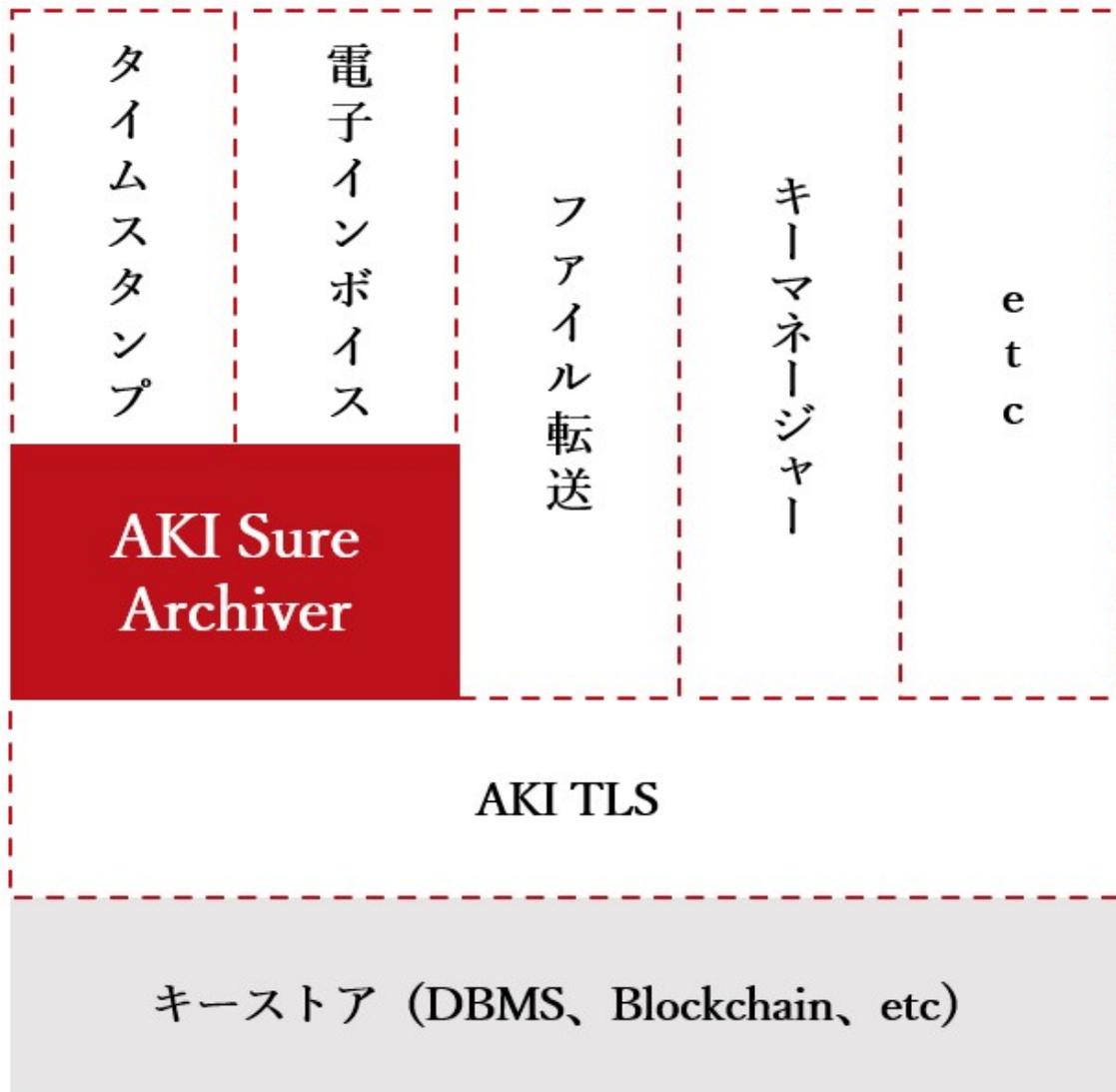
Zero Trust Architecture

：「決して信頼せず、常に検証する」アーキテクチャ

Zero Knowledge Proof

：「機密情報を明かさずに証明する」手法

# AKI Concepts



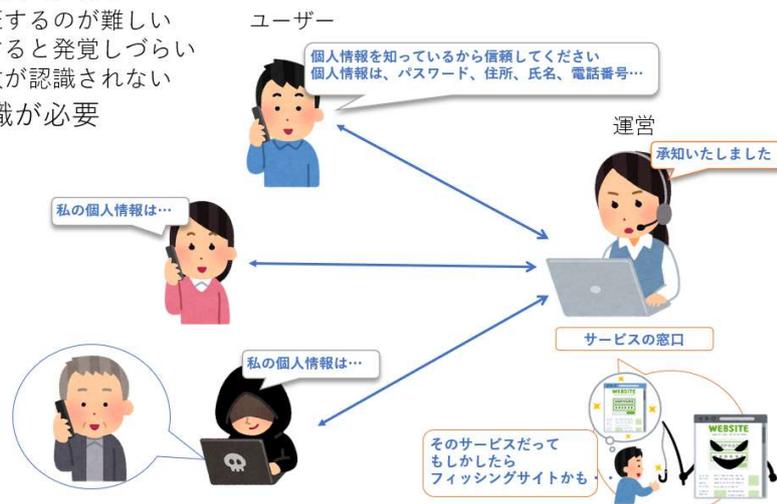
AKI を用いることで、特別な知識がなくても簡単に、電子署名・電子証明が可能となり、ファイルに対する高い改ざん耐性を得ることができます。

AKI Sure Archive を応用して、電子帳簿保存法に対応したタイムスタンプサービスや、電子インボイスサービス等の開発を進めています。

# AKI TLS

## 既存のTLSは……

- そんなに安全安心ではないかも？
  - 信頼：信頼の根拠を検証するのが難しい
  - 検知：一度偽証に成功すると発覚しづらい
  - 事故：事件発生まで事故が認識されない
- 使う人は常に最新の知識が必要



## AKI TLSなら……

- 「決して信頼せず、常に検証する」アーキテクチャ
  - 信頼：デジタル鍵を提供します
    - お互いが自分の“信頼できる鍵”を持つ
  - 検知：不正なやり取りを即時検知できます
    - お互いの鍵で常に相互に検証
  - 事故：鍵の有効性をリアルタイムで制御
    - 万が一事故が起きても該当の鍵を無効化することで被害を最小化できる
- 使う人の知識に依存しない、安心して利用できるサービスです

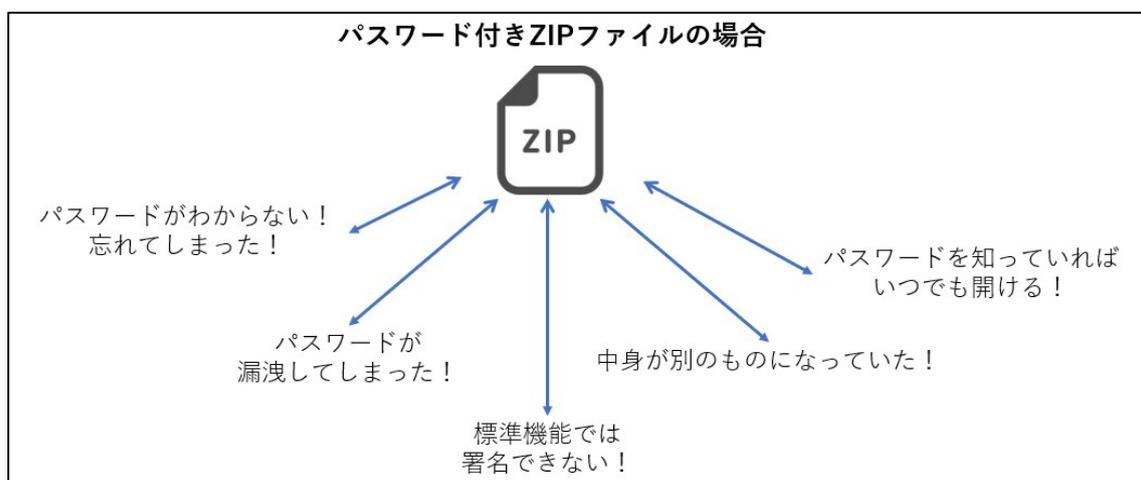


特許出願中

AKI TLS は、お互いが対となる鍵を持ち、双方で暗号・複合する通信方式です。通信が成立した時点で相互検証が完了します。

中間攻撃や、サーバー・クライアントのなりすまし等に高い耐性を持ちます。

# AKI Sure Archiver



パスワード付き ZIP ファイルが持つ様々な課題解決に役立つ、今までにないデジタルファイルを提供するサービスです。

AKI Sure Archiver のアーカイブファイルを利用者が保持し、開く為の鍵をサービス運営者が保持します。双方で分担保持することで、セキュリティコスト低減、リスク分散、リスク限定化が図れます。