Sure Archiver Use Case

ゼロトラスト時代のデジタル認証基盤

上原　敏幸

目次

1. SureArchiver とは 2
2. SureArchiver の活用提案 2
2.1. タイムスタンプ 3
2.2. さらば PPAP／レガシーメディアの復権 4
2.3. 終活／拡散する事で得られる確かな証拠 6
2.4. データの持ち出し／トレーサビリティ 7
3. 著作権について 8
4. 問い合わせ 9

1. SureArchiver とは

- 情報を安全にアーカイブ
  - アーカイブ対象ファイルの漏洩はありません
  - 改ざん不可能なアーカイブです
- アーカイブへの高度なアクセス制御
  - アクセス承認/アクセス否認が自由に行えます
  - パスワードレス暗号/パスワードレス復号を実現します

SureArchiver は AKI を利用した新時代のファイルアーカイバシステムです。
アーカイブファイルは、タイムスタンプ相当のデジタル署名が施されおり、1 ビットたりとも改ざんできません。
アーカイブファイルは、自由にコピーし配布する事ができ、どんなにファイルが拡散していても、ファイルオーナーは自由にアクセス制御を行う事が可能です。
そして、インストールレスで利用する事が出来ます。

※ SureArchiver は AKI の実践的 PoC 検証のために開発した Web アプリケーションです。
AKI が提案するコンセプトの全ては実装しておりませんので別途追加開発が必要です。
※ Google Chrome バージョン: 103.0.5060.66（Official Build）にて動作確認しています。

2. SureArchiver の活用提案

クライアント/サーバモデルで構成された現在の情報システムは、役割を主体に置いたセキュリティデザインです。
対して、SureArchiver は情報主体でセキュリティをデザインしています。
情報主体のセキュリティデザインが、従来の情報セキュリティに課せられた課題を解決します。

2.1. タイムスタンプ

SureArchiver が作成するアーカイブは、AKI 方式による署名は施されています。
AKI 署名に採用している暗号技術は、既存のタイムスタンプサービスで要求されている技術と同じです。
すなわち、SureArchiver にてアーカイブする事でタイムスタンプも同時に施した状態となり、非常に容易にタイムスタンプを導入する事が可能となります。

表 1　認定要件のポイント（抜粋）

要件（原文ママ）	SureArchiver 対応
デジタル署名方式を用いること	RSA 暗号を採用
時刻源は国立研究開発法人情報通信研究機構の UTC（NICT）とすること	対応可能
発行する(した)タイムスタンプと当該時刻源との時刻差が1秒以内となるよう、時刻の品質を管理及び証明する措置を講じること	構築可能
タイムスタンプは十分な安全性を有する暗号技術や装置等を用いて生成・管理すること。	構築可能

※ タイムスタンプの国による認定制度
https://www.soumu.go.jp/main_content/000742673.pdf

さらに、AKI署名は、秘密鍵をタイムスタンプ後に廃棄し公開鍵は非公開とする相互押印技術を採用してアーカイブファイルの唯一性を確保します。
従来のタイムスタンプと異なり、公開鍵の有効期限管理が不要なので、タイムスタンプの再押印も不要となります。

※ 電子情報保護法におけるタイムスタンプの要件は十分に満たします。
正式に認可頂ける様活動を続けてまいります。

2.2. さらば PPAP／レガシーメディアの復権

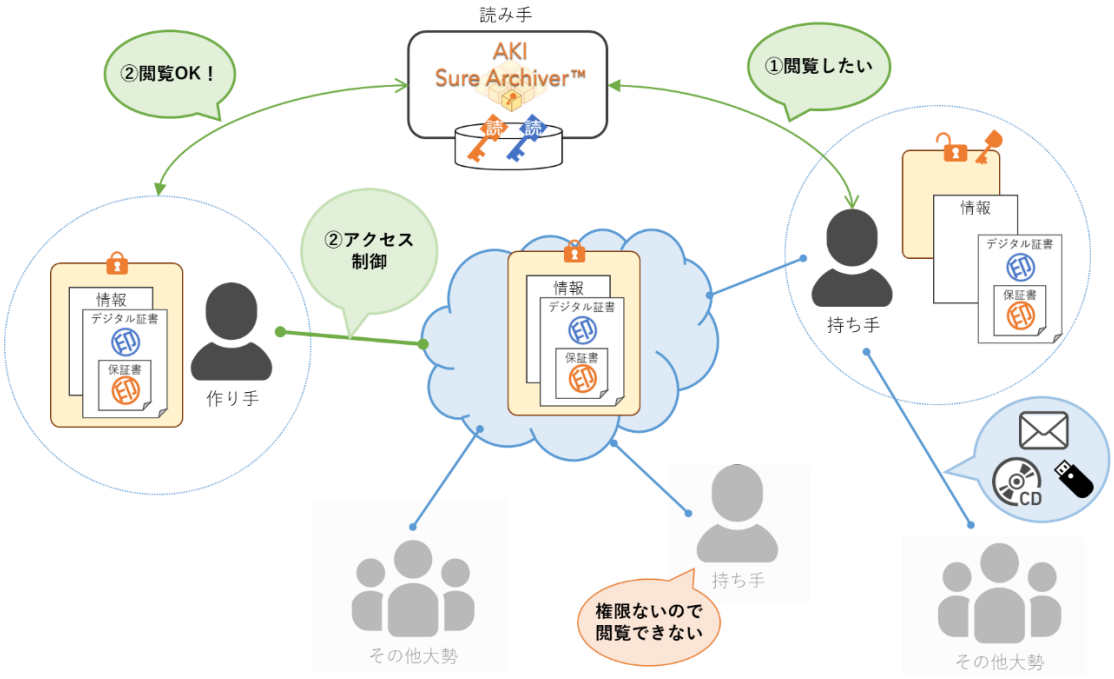
PPAP とは、日本固有のセキュリティ的風習です。

- Password 付 zip 暗号化ファイルを送ります
- Password を送ります
- （A）暗号化
- Protocol

形式的で論理的では無いので脱 PPAP の機運が高まっています。
代替え手段としては、クラウドストレージを活用する提案が多く見受けられます。
これは、メールという役割がクラウド共有という役割に置き換わったに過ぎず、
情報そのものの漏洩対策ではありません。
役割に縛られる事無く、E2E[1]で安全に情報交換する事こそが脱 PPAP の必要要件と考えています。
SureArchiver は、情報そのものに適切なアクセス制御を施し、E2E で安全に情報を交換する事が出来ます。

[1] エンドツーエンド：通信を行う二者、あるいは二者間を結ぶ経路全体を指す

図 1 さらば PPAP/作り手のアクセス制御



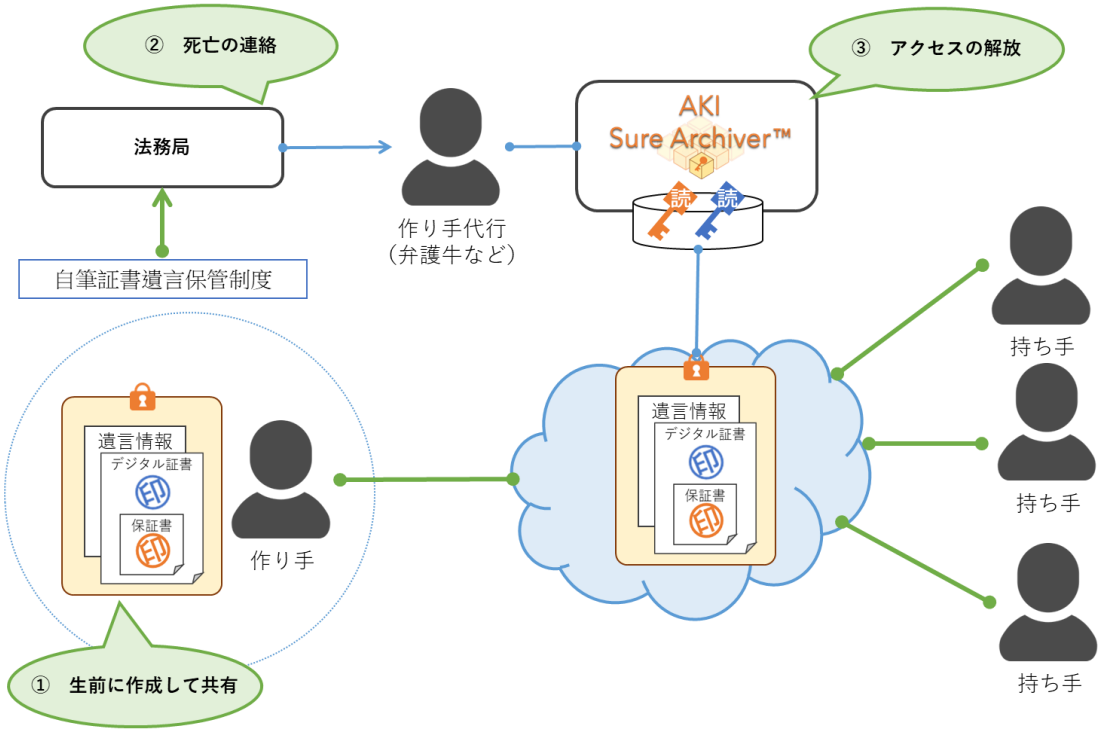
情報の作り手は、所有状況を追跡する様にアクセス制御を設定出来ます。
そして、いつでも情報の読み手へのアクセス制御を変更する事が出来ます。
作り手が自由にアクセス制御を出来るので、PPAPの運用課題を根源から改善し、
安全な情報共有を推進する事が出来ます。

共有後の情報へのアクセス制御が可能になる事で、搬送メディアに課せられていた
課題もクリアされます。
SureArchiver はメールの PPAP 問題に限らず、セキュリティ面から敬遠されていたメ
ディアを再び情報共有のツールとして安心して活用する事が可能となります。

2.3. 終活／拡散する事で得られる確かな証拠

SureArchiver が作成したアーカイブファイルは、元のファイルがどのように拡散しようとも、唯一性の元でアクセス制御できます。
この特性を生かし、拡散する事でその情報が確かである証拠とする事が可能です。
活用の一例として、終活ビジネスへの応用例を示します。

表 2 遺言の共有



遺言情報が、生前に共有されている事で、改ざんされていないという確かな証拠となります。
SureArchiver が作成したファイルは、どんなに拡散しようとも、デジタル的には唯一なので、誰が必要としたか等のトレーサビリティを得る事も可能です。
個人主導の新しい DRM[2]としても活用可能です。

[2] Digital Rights Management：デジタルコンテンツの著作権を管理する技術

2.4. データの持ち出し／トレーサビリティ

46 万人余りの個人情報が入った USB メモリーの紛失騒動が記憶に新しいかと存じます。
この事件では、改めて人に依存する漏洩対策の在り方が浮き彫りになりました。

主な対策は以下の通りです。

- 許可の不徹底
- 運搬手段
- 作業後の行動
- サイバー責任の素養

残念ながら、これらの対策は今と何ら変わりません。
もしも悪意をもって的確な対策が取られたら対策は難しいです。

SureArchiver は情報の E2E セキュリティモデルです。
そして、暗号/復号のプロセスに人は参加する事が出来ない仕組みとなっており、全ての鍵は SureArchiver サービスに集中管理されます。
つまり、情報の搬送に際し明確なトレーサビリティが取得する事が出来ます。
持ち出された情報には詳細なデジタル証書を付与する事が可能なので、漏洩された場合にも、誰が何時のレベルで調査するヒントにもなります。
これらは、今はアイデアベースであり検証が必要な事案ではありますが、例えばセキュアな境界から情報を持ち出す Gateway に SureArchiver を適応する事で、情報の持ち出し方を改革する事が可能となります。

これは SureArchiver が提供する革新的な特徴です。

3. 著作権について

本ドキュメントの著作権は、Tosiyuki Uehara 及び株式会社 GFS に帰属します。引用に際しては、出典を明記してください。無断転載を禁止します。 転載および商用利用に際しては、事前に株式会社 GFS にご相談ください。

本ドキュメントは、予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

4. 問い合わせ

本件に関するお問い合わせは、下記の連絡先までお願い致します。

株式会社GFS（GFS Corporation）
https://e-gfs.co.jp
aki_customer@e-gfs.co.jp

AKI テクニカルアドバイザー
上原　敏幸
sure.archiver@gmail.com

変更履歴

日付	バージョン	変更内容
2022/7/7	1.00	初版