Whitepaper

ゼロトラスト時代のデジタル認証基盤

上原　敏幸

目次

1. コンセプト

高度にデジタル化された現在では、企業が扱う情報はその企業のビジネスそのものの価値であると言えます。ビジネスの規模が大きくなればなるほどに扱う情報の重要度も高まり、その高まりに呼応するように情報の取扱いに対する市場の目は厳しくなるばかりです。
デジタル化の恩恵を主張し効率アップを求める声がある一方、デジタル化のリスクを主張し警鐘を鳴らす声もあります。両者の主張は平行線を辿り交わることがありません。突き詰めれば、システムを構築しサービスを提供する側を信用できるか否かが問われている様に思えます。

現状、「サービスを提供する側は過ちを犯さない」という前提の下、社会が成立しています。その前提が崩れた時、サービスを提供する側のみならず、サービスを受ける側も深刻なダメージを負うこととなります。サービスを受ける側は被害者であるとしても、サービスを提供する側の賠償能力を超える補償は受けられません。
生産効率を追求し、世界規模でサプライチェーンを構築している工業製品は、部品一つ欠けるだけで生産停止に追い込まれることは周知の事実でしょう。欠品を起こし、生産停止の原因となった一企業に全責任を負わせ全損失を補償させるのは無理があります。サプライチェーンに組み込まれた一企業に求められる責任は、一企業で補償できる範囲を逸脱しつつあります。

ネットワークの世界も同じです。利便性や効率を優先し、情報の統合、連携が求められています。ですが、情報が漏洩していないこと、改ざんがないことを誰が保証し、どうやって連携したシステム全体の健全性を確保するのでしょうか。ネットワークの世界も最終的に誰も責任を負えず、実質、野放しになる世界へと向かっている様に思えてなりません。

お気づきでしょうか。
たとえ、自社の管理体制を整えたとしても、市場からの信頼を得られなければ意味がありません。自社のシステムが他社のシステムに依存するのであれば、他者のシステムの管理体制までも含めて整えなければ意味がありません。サービスを提供する側は、サービスが確かな証拠を保持する事で、不正がない事を示せなければなりません。サービスを受ける側が、受け入れたサービスが信頼に値するものであるか、いつでも確認できる状態でなければなりません。

利便性や効率を追求しデジタル化が進む現在、サービス提供側を過信せず、サービス受給側からも検証できるシステムが市場から求められているのではないでしょうか。

情報には「情報を作る人」と「情報を読む人」が存在します。
サービスを提供する側、受ける側という役割で区分するシステムではなく、情報を作る側、読む側とで区分するシステムとして構築することにより、役割の垣根を超えた情報管理が可能となります。AKI[1]は情報を中心に置き、役割の垣根を超え、参加者全員で自らを統制できる「情報システムのセルフガバナンス」を実現します。まだ見ぬ脅威におびえ神経質に対策せざるを得なかった従来の情報管理の在り方に一石を投じるものと確信しております。

2. セルフガバナンスの推進

AKI は、セルフガバナンス推進のために、3つのコンセプトを提案します。

- 役割中心から情報中心へのパラダイムシフト
  - 作り手/読み手モデルの提案

- 唯一性の創出
  - 作り手/読み手/持ち手モデルの提案

- セルフガバナンス基盤の構築
  - 分散ログ情報

[1] Asymmetric key Infrastructure / 非対称鍵暗号基盤

2.1. 役割中心から情報中心へのパラダイムシフト

現在、広く採用されているソフトウェアモデルとしてクライアント/サーバーモデルがあります。このソフトウェアモデルは役割を中心にデザインされたモデルです。
「作り手/読み手モデル」は「情報」を中心に捉え、作成と検証、そして所有に着目して新たにデザインしたソフトウェアモデルです。

- 作り手とは
  - 情報を作る事が出来ます
  - 相対する読み手がいます

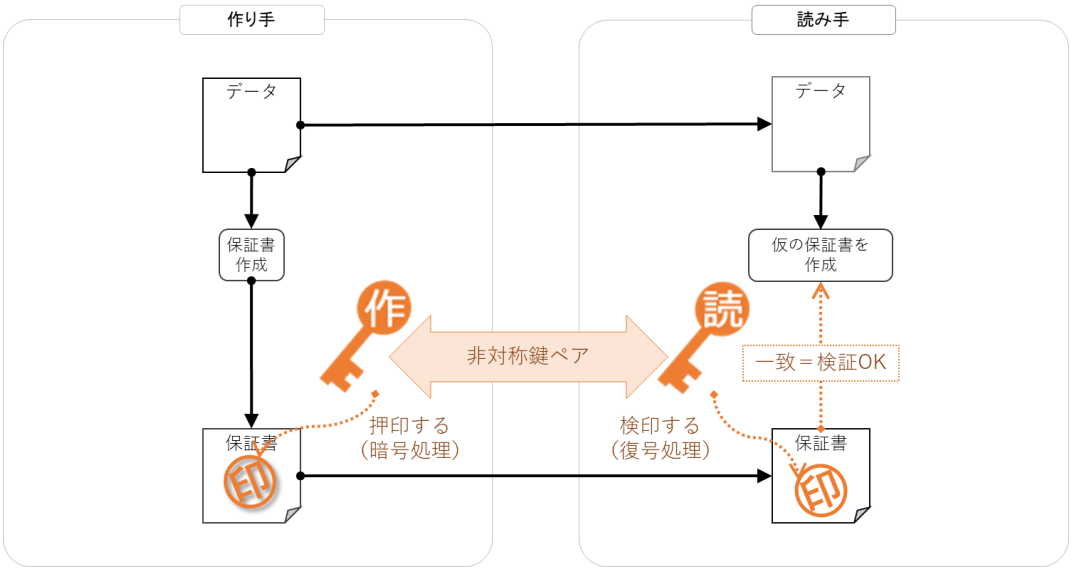
- 読み手とは
  - 情報を読む事ができます
  - 作り手が作った情報を原本として預かる事ができます
  - 相対する作り手がいます

作り手/読み手モデルの実現には非対称鍵暗号技術が最適です。
しかしながら、非対称鍵暗号基盤として最もメジャーである PKI[2]は、役割分担を中心におきデザインされている為、情報を中心としたモデルとの相性が良くありません。

そこで、作り手/読み手モデルに最適化したデザインを施し完成した暗号基盤が AKI です。本書は、コンセプト説明なので、暗号技術の詳細は極力排除いたしました。
暗号技術によりもたらされる効果を現実のオフィスワークに結び付けてイメージできるように作り手による暗号化処理を「押印」、読み手による復号化処理を「検印」と表現します。

[2] Public Key Infrastructure / 公開鍵暗号基盤

図 1 AKI の概要



- 作り手は、読み手にデータと押印済み保証書を送付する
  - データから保証書を作成する
  - 作成した保証書に作り手鍵で押印する

- 読み手は、作り手からデータと押印済み保証書を受け取り、検印する
  - データから仮の保証書を作成する
  - 受け取った押印済み保証書を読み手鍵で検印する
  - 検印した押印済み保証書と仮の保証書が一致するか確認する

※ 検印した押印済み保証書と仮の保証書が一致していれば、データは作り手が作成した情報である。

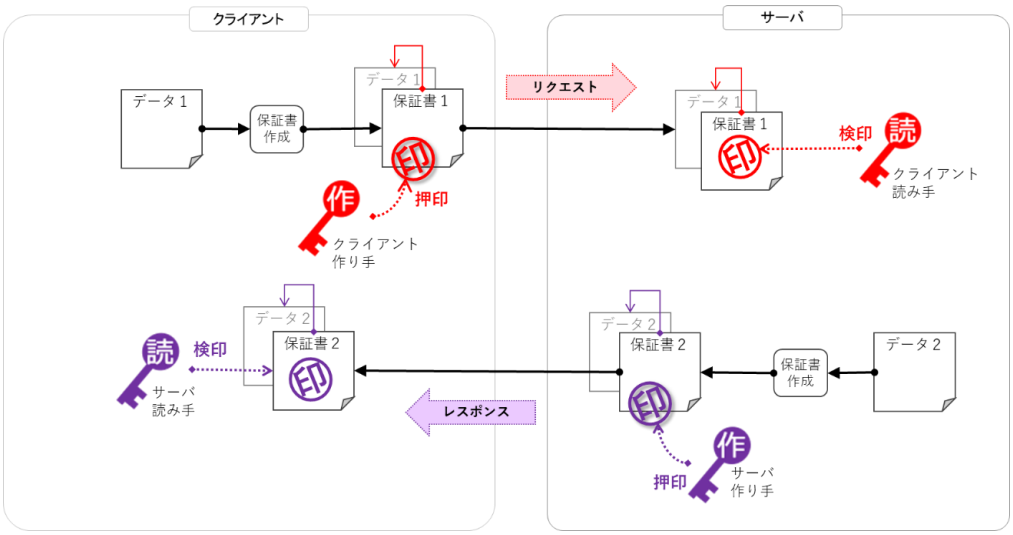
本書での解説は割愛しますが、保証書の押印/検印と同時に、データを暗号化/復号化することも可能です。パスワードレス[3]で情報の暗号化/復号化を行いますので、パスワード流出を懸念する必要はありません。

[3] ゼロ知識証明（Zero Knowledge Proof：機密情報を明かさずに証明する技術）を利用してパスワードレスを実現

2.1.1. 作り手/読み手モデルの概要

AKI による作り手/読み手モデルの具体例を説明します。
従来モデルでは役割が中心であり、クライアントもサーバもそれぞれが情報の作り手であり読み手でした。情報に着目すると、クライアントからサーバへのリクエストは、クライアントが作り手、サーバが読み手となります。そしてレスポンスでは逆の関係です。これらを踏まえ、「図 1　AKI の概要」を参考に従来モデルに適応した図を示します。

図 2　作り手/読み手モデルの適応



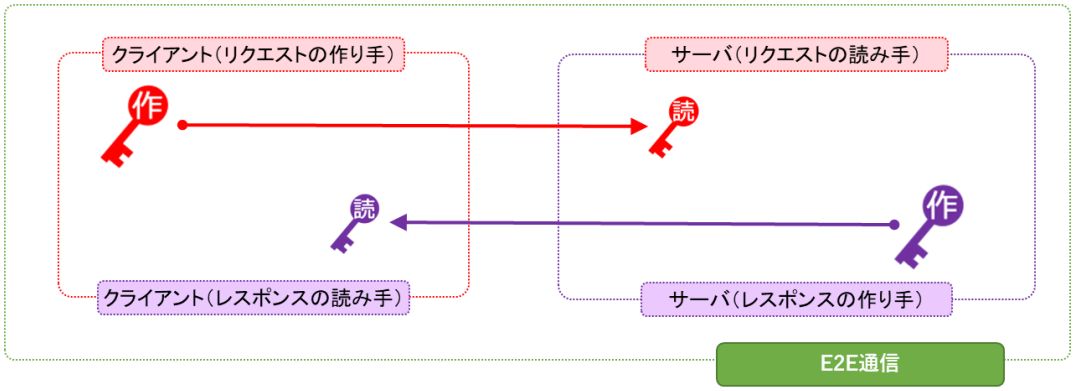
クライアントからサーバへのリクエストを赤色の鍵セット、サーバからクライアントへのレスポンスを紫色の鍵セットとして、表現しています。それぞれのデータには保証書が添付され押印が施されています。読み手は、保証書を検印し、受け取ったデータの真贋を判定します。

データ作成と参照を中心に据えることで非常にシンプルなデータフローとなりました。特筆すべきは、クライアントとサーバ間を AKI の暗号/復号オプションを使う事で E2E[4] セキュリティが構築できる事です。このシンプルで堅牢な E2E データ交換プロセスが、作り手/読み手モデルの基礎となります。

[4] End To End：通信を行う二者、あるいは二者間を結ぶ経路全体を指す

作り手/読み手モデルの特徴を絵図として以下にまとめました

図 3 作り手/読み手モデルのまとめ



2.2. 唯一性の創出

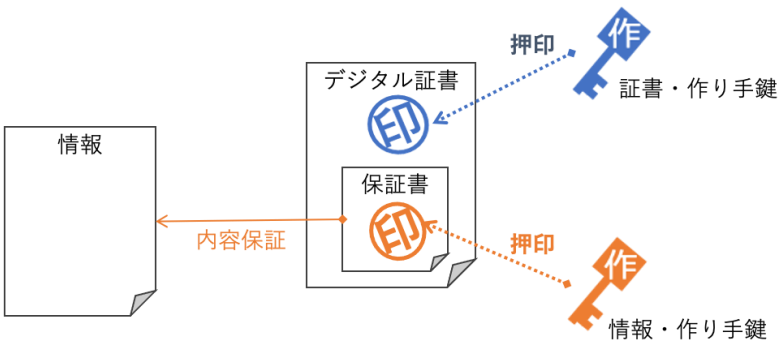
シンプルな E2E データ交換の仕組みが整いました。
続いて、データを「情報」として取りまとめ共有する仕組みを深掘りします。
情報とは取りまとめられたデジタルデータの集合体と定義します。
情報は、保存し、共有し、コピーし、配布する対象です。
デジタルデータはネットワーク、物理媒体を介して流通します。
情報の流通過程に潜在する脅威への対処が、現在のセキュリティ対策の柱の一つとなっています。

AKI は、情報が「作り手の意図した唯一のものであること」を保証することが、根源的なセキュリティ対策に繋がると考えました。そこで「相互押印[5]」という独自技術で、この「唯一性」を確保しました。「相互押印」とは「相互に一度だけ押印した特別な保証書を作ること」です。本書では「相互押印された保証書」を「デジタル証書」と表します。

2.2.1. 相互押印

相互押印の手続きは、作り手と読み手との印鑑リレーに例えることができます。

図 4 デジタル証書と情報、押印関係の概要図



[5] 特許出願中

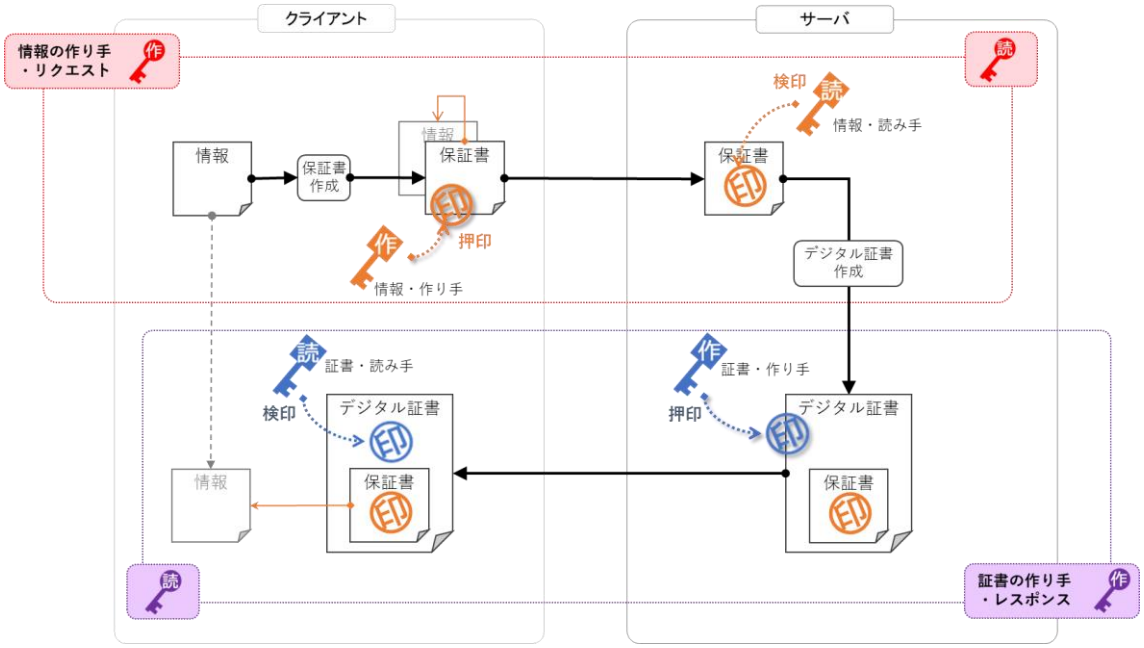
- 情報の作り手が保証書を作成し、情報・作り手鍵で押印した後、読み手に渡す
- 情報の読み手が保証書の正当性を確認した後、証書・作り手鍵で押印したデジタル証書を作り手に渡す

※ 作り手の手元には、情報と読み手が押印したデジタル証書が残ります。
※ デジタル証書には作り手が押印した保証書が同梱されています。

この押印リレーをデジタルデータに適応させたものが相互押印です。
相互押印自体は、伝統的に紙媒体で行われている手法を元にした、非常にシンプルな仕組みです。

しかしながら、デジタルデータに適応すると少々難解です。そこで、本書では、最初に単純なモデルで説明します。そして、そこにある問題点を示した後に改善策を示すことで、相互押印の基本構造の説明につなげていきます。ご承知おきください。

図 5 相互押印のイメージ図



※ クライアントとサーバとのデータ交換については「作り手/読み手モデルの概要」で説明した内容が当てはまります。
リクエストが赤枠、レスポンスが紫枠で抽象化しています。

※ 情報が橙色の情報・鍵セット、証書が青色の証書・鍵セットで表現しています。
※ 取り扱いの対象が、データからデータの集合である情報となっています。

- 保証書の作成と押印依頼
  - 情報から保証書を作成する
  - 保証書に情報・作り手鍵で押印する
  - 作成した保証書をサーバへ送付する
    - ✧ 本ケースは、デジタル証書の作成が目的なので、情報は送付しない

- サーバの押印処理
  - 情報・読み手鍵を使って、保証書を検印する
    - ✧ 保証書が正しい事を確認する
  - デジタル証書を作成する
    - ✧ 情報・作り手鍵で押印された保証書を内包する
  - 証書・作り手鍵で、デジタル証書を押印する
  - 作成したデジタル証書をクライアントへ送付する

- クライアントの検印処理
  - 証書・読み手鍵を使って、デジタル証書を検印する
  - 検印できたら、デジタル証書は正しく作成されている

「図 5 相互押印のイメージ図」において、赤色のリクエスト・鍵セットと紫色のレスポンス・鍵セットを使って押印者を特定することはできますが、E2E の為の鍵であり、相互押印には適切ではありません。そこで、新たに橙色の情報・鍵セットと青色の証書・鍵セットを用意し、相互押印の仕組みを表現しました。

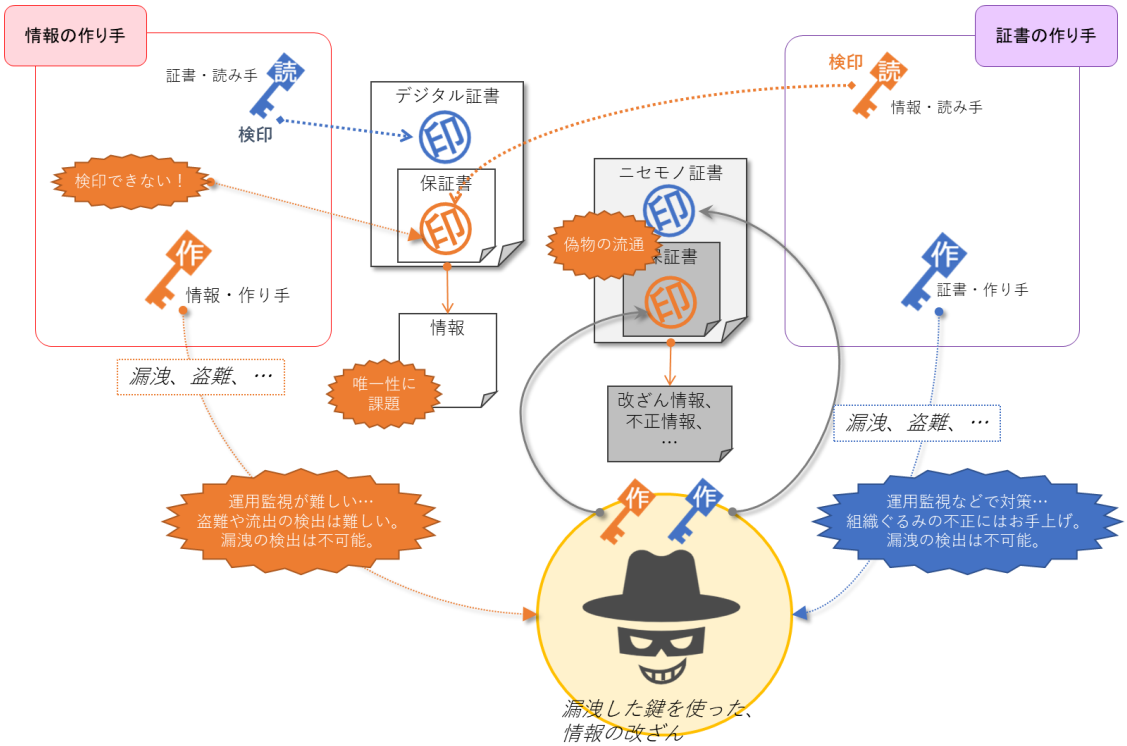
相互押印に使用する情報・作り手鍵と証書・作り手鍵に着目すると、三つの課題があることが分かります。
一つ目は、クライアントは証書・読み手鍵でしかデジタル証書の検印ができないことです。クライアントが情報・読み手鍵も所有すると非対称鍵の関係性が壊れてしまいます。また、第三者が情報をデジタル証書で検印する際には、情報/デジタル証書/証書・読み手鍵/情報・読み手鍵をセットで渡す必要があります。

二つ目は、検印結果の共有ができない事です。
作り手と読み手、さらに第三者の読み手との間で検印結果の共有ができなければ、情報が意図しない形で流通していることを検知し対策する事ができません。

三つ目は、唯一性[6]の欠如です。
相互押印に直接使用する橙鍵と青鍵は、デジタル証書の作成に使い続ける形で描かれています。この仕様だと、一つの情報から得られるデジタル証書は必ず一意[7]となってしまう為、複数枚のデジタル証書を作ると、もっとも重要な唯一性が失われてしまいます。

鍵を使い続けるリスクはこれだけではありません。作り手鍵が漏洩した場合、作り手鍵を入手した者が不正なデジタル証書を作成できることになり、漏洩した作り手鍵で作成した過去全てのデジタル証書の信頼を失います。

図 6 相互押印の課題



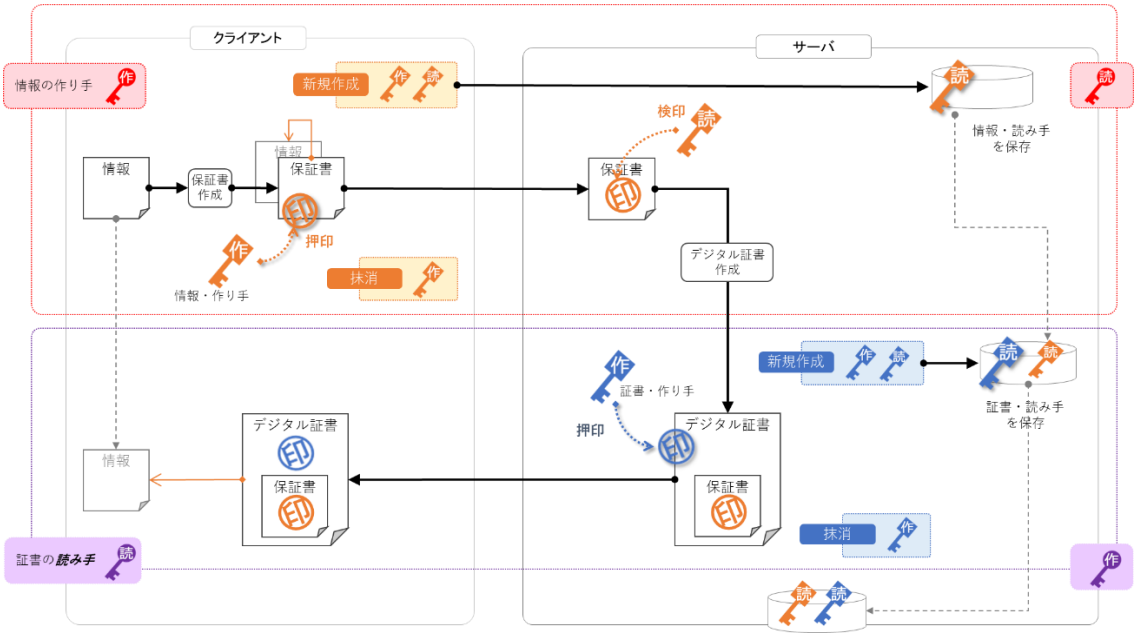
[6] ただ一つである事

[7] ただ一つだけ存在している事

2.2.2. 作り手/読み手/持ち手モデル

これらの課題を解決するため、相互押印毎に常に新規に鍵を作成し、鍵の生成破棄、鍵の所有関係を見直しました。以下のフローをご確認ください。

図 7 相互押印の改良イメージ/デジタル証書の作成



デジタル証書の作成ステップは以下の通りです。
変更された事項は赤字下線で強調しています。

- 保証書の作成と押印依頼
  - 情報・鍵セットを新規作成する
  - 情報から保証書を作成する
  - 保証書に情報・作り手鍵で押印する
  - 作成した保証書と情報・読み手鍵をサーバへ送付する
    - ✧ 本ケースは、デジタル証書の作成が目的なので、情報は送付しない
  - 情報・作り手鍵は廃棄が望ましい

- サーバの押印処理
  - 証書・鍵セットを新規作成する

- 情報・読み手鍵を使って、保証書を検印する
  - ✧ 保証書が正しい事を確認する
- デジタル証書を作成する
  - ✧ 情報・作り手鍵で押印された保証書を内包する
- 証書・作り手鍵で、デジタル証書を押印する
- 作成したデジタル証書をクライアントへ送付する
- 証書・作り手鍵は廃棄する
- 情報・読み手鍵と証書・読み手鍵が保存されている

- デジタル証書を受領する
  - 証書・読み手鍵を持っていないので検印はしない

「図 7　相互押印の改良イメージ/デジタル証書の作成」では保証書/デジタル証書の作成に新規作成した鍵セットを用い、検印に使用する情報・読み手鍵、証書・読み手鍵をサーバが保持しています。

一つの情報に対し保証書/デジタル証書の作成は一度切りですから、情報・作り手鍵、証書・作り手鍵を保持する必要はありません。では、作り手鍵を保持し続けた場合、悪用は可能でしょうか。保証書/デジタル証書の作り手は、作成後、相手に渡してしまうため、相手に渡した保証書/デジタル証書を差し替える術はなく、悪用はできません。利用価値の無い鍵は安全性の観点から破棄すべきでしょう。不要な鍵を破棄する事で、より確かな唯一性を得る事ができます。

説明簡素化のため暗号化は割愛しましたが、デジタル証書に内包する保証書を暗号化し、証書・読み手鍵を持たない者が保証書を読めない状態にすることも可能です。

デジタル証書を受け取ったクライアントは情報の作り手としての役割を終えます。
この、情報とデジタル証書を所有している状態を「持ち手」と定義します。「持ち手」はクライアントのみならず、別の第三者でもかまいません。

- 作り手とは
  - 情報を作る事が出来ます
  - 相対する読み手がいます

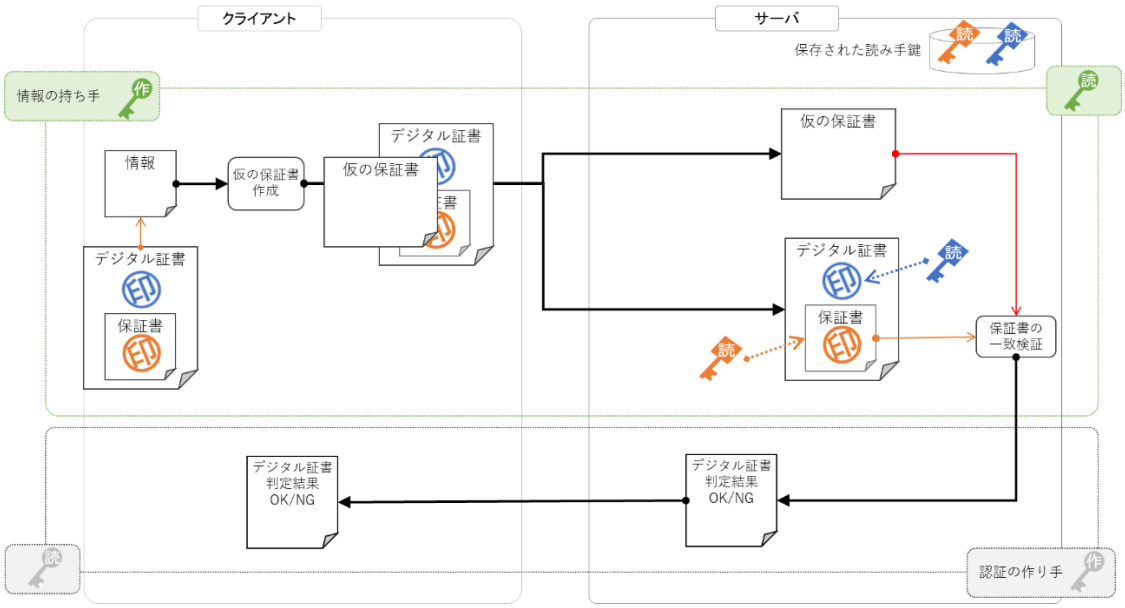
- 読み手とは

- 情報を読む事ができます
- 作り手が作った情報を原本として預かる事ができます
- 相対する作り手がいます

- 持ち手とは ←New
  - 情報を所有しています

続いて、持ち手の検証フローを示します。
情報とデジタル証書しか所有していない状況で検印ができれば、作り手/読み手/持ち手モデルの完成としたことになります。

図 8 持ち手がデジタル証書を検印



※ 持ち手のリクエストが緑枠、レスポンスが灰枠で抽象化しています。

デジタル証書の検証ステップは以下の通りです。

- デジタル証書の検印依頼
  - 情報から仮の保証書を作成する
  - 仮の保証書とデジタル証書をサーバへ送付する

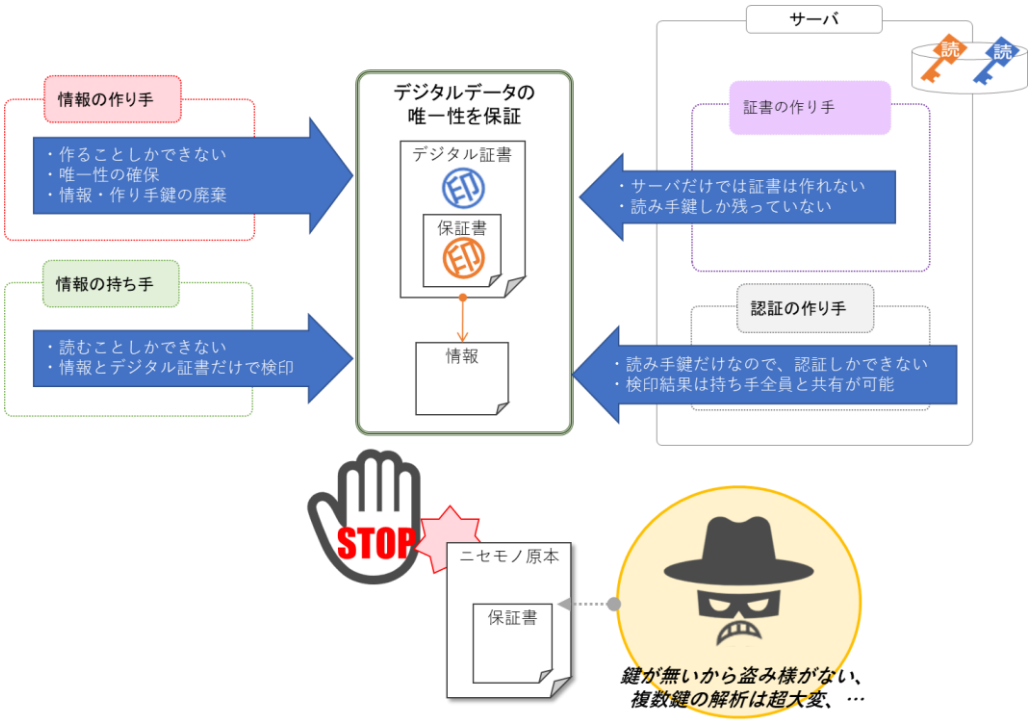
- デジタル証書の検印
  - 証書・読み手鍵を使って、デジタル証書を検印する
  - 情報・読み手鍵を使って、デジタル証書内の保証書を検印する
  - デジタル証書内の保証書と仮の保証書を比較する
  - 一致すれば検印 OK、不一致で検印 NG

- 検印依頼の結果を受領
  - 検印結果を受領

持ち手は仮の保証書とデジタル証書をサーバに送ることで、検印結果を得ることができます。

説明簡素化のため暗号化は割愛しましたが、情報を暗号化し、サーバにデジタル証書の検印を依頼しなければ情報を復号化できない状態することも可能です。この場合、クライアントはサーバからデジタル証書の検印結果に加え、復号化に必要な鍵を受け取ることになります。情報の暗号化は、流通過程に潜在する脅威への対策として効果的です。

図 9 相互押印の完成



情報とデジタル証書をセットにして、自由にコピーして配布して共有する事が可能となります。唯一性確保と暗号化により、サーバ管理の下、全クライアントを識別した上で、情報とデジタル証書のセットで情報を安全に流通させる手法を示しました。
サーバは全てのクライアントを識別しますので、特定のクライアントにのみ、情報を閲覧可能(復号化可能)にすることも、情報を閲覧不能(復号化禁止)にすることも容易です。さらに、意図しないクライアントからの閲覧要求があれば、意図しないルートで情報が流通していることを把握できます。

本手法のシステム要件上の特徴は以下の通りです。

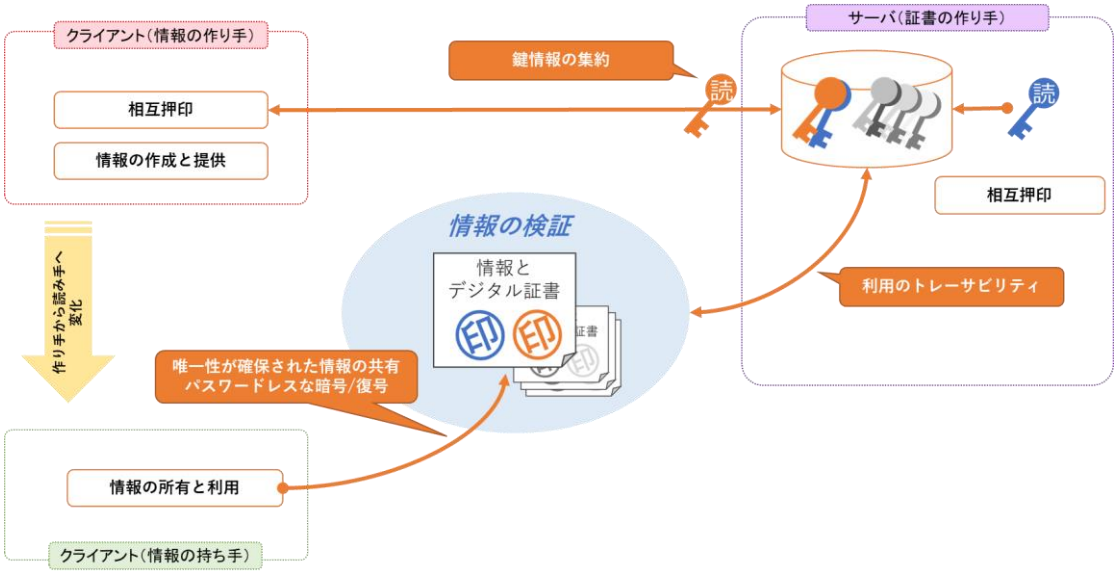
- サーバは「鍵の関係性管理」と「鍵へのアクセス管理」が主機能であり、コンパクトなシステムである
- クライアント/サーバ間の通信内容は主に保証書/デジタル証書と鍵となるため、通信量が少ない

作り手/読み手モデルに、持ち手という概念を組み込むことで、情報を、安心安全に、保存し、共有し、コピーし、配布できる仕組みが整いました。

作り手/読み手/持ち手モデルで扱われる情報は、そのライフサイクルにおいて適切に保証される情報となります。

作り手/読み手/持ち手モデルは役割ではなく情報が主体なので、組織という役割を超える事が出来、自社だけでなくサプライチェーン全体のセルフガバナンスに結び付きます。

図 10 唯一性のまとめ

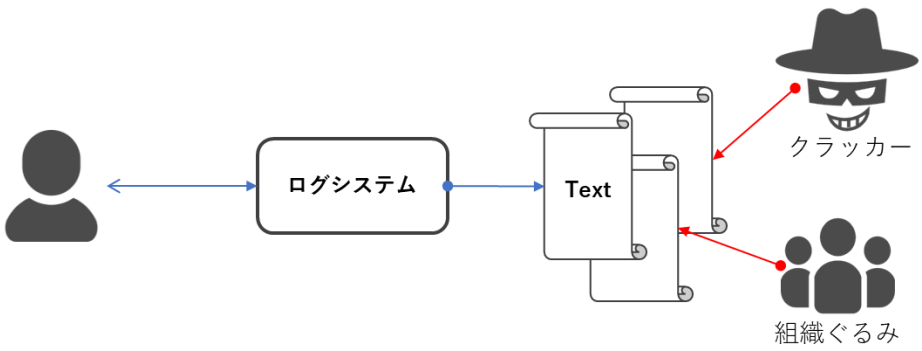


2.3. ログ情報基盤の構築

シンプルで堅牢なデータ交換プロセスが確立し、情報を安全に流通させる事ができました。最後のコンセプトは、セルフガバナンスが可能な情報基盤の実現です。
ガバナンスは、組織における不正行為を未然に防ぎ、体制管理をするために必要不可欠です。情報システムは、定期的に情報システムのログを収集し、適切な運営がなされているのかを監査します。監査結果を運営にフィードバックする事でガバナンスが保たれます。

しかしながら、「ログを収集し監査する」作業は、字面程簡単ではありません。
単なるテキストの積み上げで作られたログの改ざん有無を判断するのは容易ではなく、ログを分析し、矛盾が無いか調査するには膨大な作業時間と高い専門性を必要とします。
また、ログの多くは公開を前提にしておらず、ログ自体に機密が記録されている為に第三者を交えた監査が難しい状況に陥る事もありえます。この様なシステム監査の在り方を変えなければなりません。

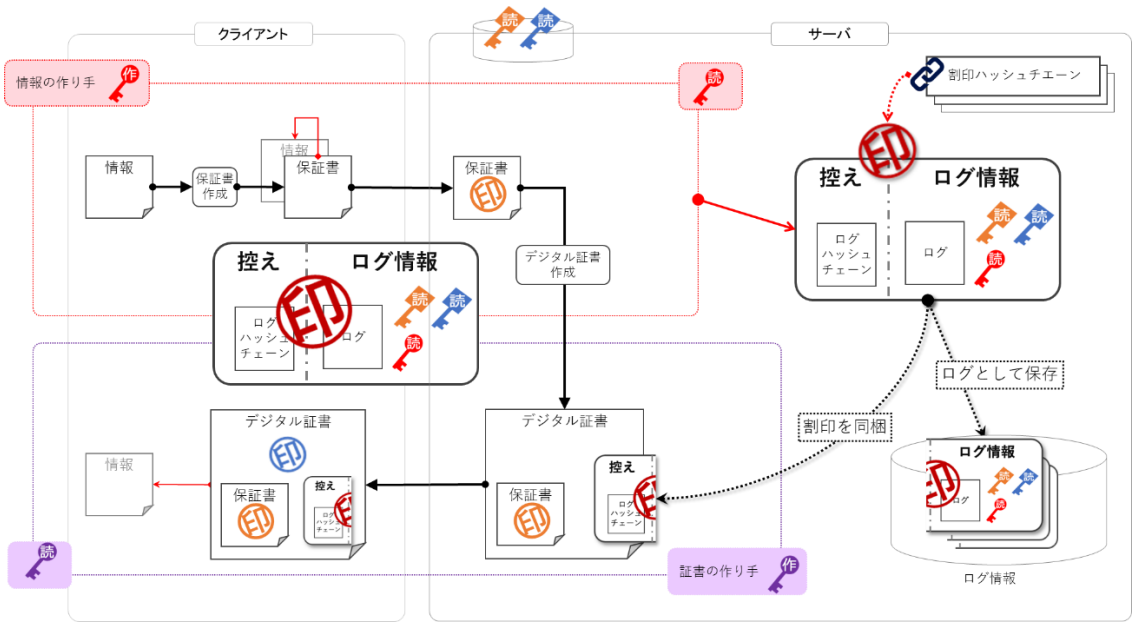
図 11 従来型ログシステム



本項では作り手/読み手/持ち手モデルをログにも適用し、ログ開示を意識したログ作りへのパラダイムシフトを提案します。
ログの読み手を想定し、見せられない箇所を暗号化する等、用途に応じた記録方法を用い、クライアントのログ開示要求に答えられるログを作成した上で、それらをハッシュチェーンで繋ぎ連続性を確保します。
さらに、ログ毎に算出されるハッシュチェーンの値をデジタル証書に含めることで、サーバのログ情報をも監査できるデジタル証書が完成します。

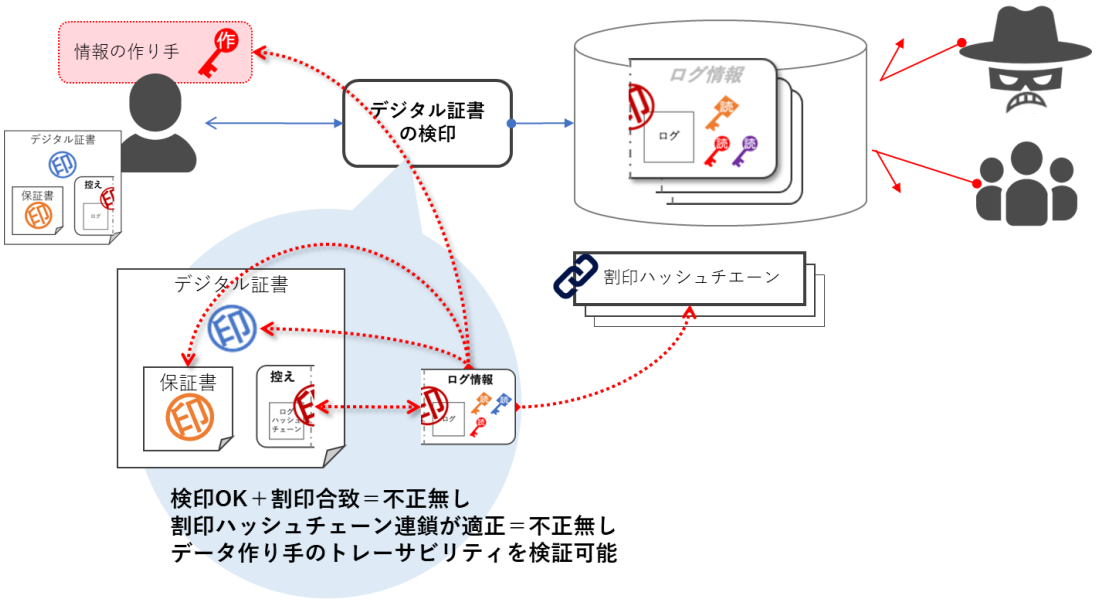
ハッシュチェーンの値を含むデジタル証書は、サーバ側はクライアントからの検印要求時に自身のログ情報監査に活用でき、クライアント側はサーバからログ情報を入手し、自身の持つデジタル証書と照合することでサーバが適切に運用されているかを監査できます。

図 12 全員参加型ログシステムの概要



- 作り手と読み手のデータフローをログ情報として記録する
- その際、ログ情報には、ログの読み手を意識した形で記録する
- 読み手はログ情報に連続性を持った情報を割り印として押印する
- 割印情報を持った控えのログ情報をデジタル証書に埋め込む

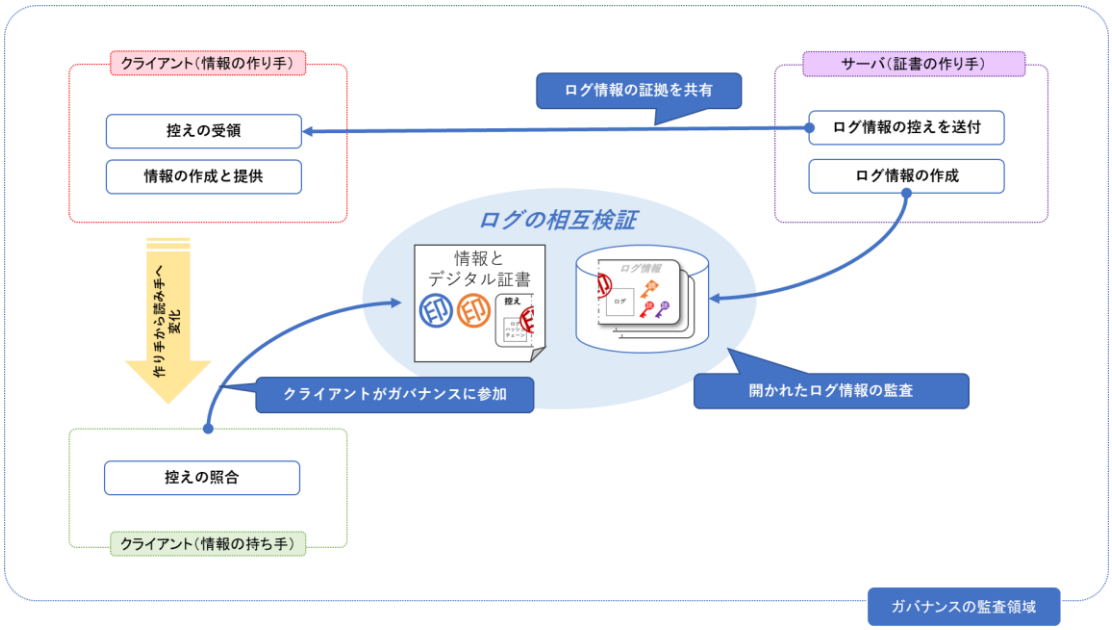
図 13 効果イメージ



- サーバ側によるログ情報検査
  情報の検印時に送付されるデジタル証書内のログ控えを使って、ログ情報の割印検査と、割印ハッシュチェーンによる連続性検査が出来る。
  ログ情報検査に不適合を検出したら、即、不正検出と判断できます。
  E2E が確保されているので、誰が、いつ、どの様な操作を行ったのか、など、ログに記録されていれば細かなトレーサビリティを検証するも可能です。
- クライアント（読み手/持ち手）側によるログ情報検査
  サーバ側からログ情報と割印ハッシュチェーンの提供を受けることにより、デジタル証書内のログ控えを使って、ログ情報の割印検査と割印ハッシュチェーンによる連続性検査が出来る。
  ログ情報検査に不適合を検出したら、即、不正検出と判断できます。
  クライアント単独での検査も可能ですが、他のクライアントの保持するデジタル証書を集めることで、より信頼度の高い検査が出来ます。

AKI が提案するデジタル証書は、唯一性による証拠能力と、サーバ、クライアント双方で検証に活用できるという特徴を持ちます。そして、「決して信頼せず、常に検証する仕組み」であるゼロトラストを指向したシステムとなります。デジタル証書を蓄積し、サーバ、クライアント双方で検証することにより、無理なく持続可能なセルフガバナンスが実現されます。

図 14 ログ情報基盤のまとめ



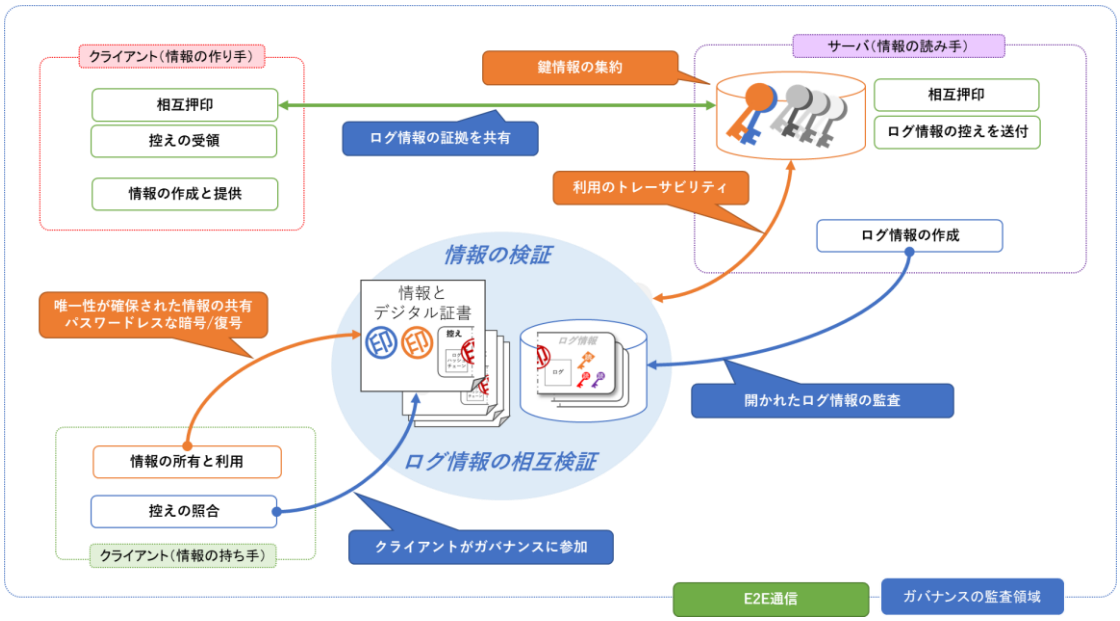
3. 総括

AKI は「デジタル証書を用いた情報の自由な取り扱い」と、「割符ログを用いた相互検証できる情報システム」を提供します。それは、サービス提供者を全面的に信頼する従来型のシステムではなく、サービス提供者と利用者の双方で信頼性を担保し、検証できる新しいセルフガバナンス・システムです。

サービス提供者を全面的に信頼する従来型のシステムは、信頼を寄せたシステムの信頼性を問われた時、さらに別のシステムに信頼を求める必要があります。サービスの提供者と利用者により支えられるセルフガバナンス・システムには、全面的に信頼を寄せる相手は存在しません。また、一つの鍵に依存するシステム、もしくは、一所に全てを集約するシステムは、一つの綻びで全てが崩壊します。一方、情報毎に鍵を生成し、鍵と情報とを分けて保持するシステムは、一つの綻びだけでは全崩壊には至らず、被害は限定的です。不正を試みる者にとって、費用対効果が悪いものとなるでしょう。

個別に鍵を割り当てられた機器間で E2E 通信を行い、誰が作った情報であるか、誰が読む情報であるかを区別する強力なトレーサビリティを実現します。情報の作り手から、情報を得るべき相手に、情報を E2E で受け渡すことが可能です。鍵の集中管理、情報とログの分散保持を組み合わせた、当事者同士で信頼を担保するセルフガバナンス・システムは、今後、新たなシステム形態として発展していくものと確信しております。

図 15 AKI 総括



- 「図 3　作り手/読み手モデルのまとめ」
- 「図 10　唯一性のまとめ」
- 「図 14 ログ情報基盤のまとめ」

今後とも、情報セキュリティの代名詞となる様に鋭意鍛錬を続けてまいります。
是非とも AKI ご評価の機会を頂ければ幸いに存じます。

4. 参考文献

デバイスプロビジョニングシステム [特許情報] : 6340120 : ソフトウェア / 考案者 上原敏幸 , 田島健. - 日本, 2018 年 5 月 18 日.
電子証明システム [特許情報] : 6480528 : ソフトウェア / 考案者 上原敏幸 , 田島健. - 日本, 2019 年 2 月 15 日.
電子証明システム [特許情報] : 6340107 : ソフトウェア / 考案者 上原敏幸 , 田島鍵. - 日本, 2018 年 5 月 18 日.

5. セーフハーバーステートメント

本書は、AKI のコンセプトを説明するものです。
これは情報提供のみを目的としており、いかなる契約にも組み込むことはできません。素材、コード、または機能を提供することを確約するものではありません。
購買決定を行う際の判断材料になさらないで下さい。
AKI について説明されているすべての機能の開発、リリース、時期、および価格は変更されることがあり、著者の裁量に任されています。

6. 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。

7. 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