

# MIT（米国マサチューセッツ工科大学） テクノロジーレビュー社が挙げた 「パスワードの終わり」

## 指紋認証セキュリティカード 制御システム

参考URL : <https://www.asd-inc.net/>

2024年3月

**FB CO., LTD.**

株式会社 フィードバックコーポレーション  
Feed Back Corporation  
Since 1998

## 共同保有特許および専属販売権

---

【2022年11月15日】

エイエスディ株式会社より株式会社フィードバックコーポレーション並びに株式会社MDT ジャパンに対して「ブロックチェーンを利用したネットワークの認証システムとこれを使用した認証方法」の専属販売権を受託する。

【2023年11月28日】

株式会社フィードバックコーポレーションとエイエスディ株式会社が共同で保有する「ブロックチェーンを利用したネットワークの認証システムとこれを使用した認証方法」の特許査定の特許を受ける。

2019年

名古屋女子大学に指紋認証付き非接触 IC カード(AOC カード)の学生証を導入

【AOC カード】

サイズ : 85.6×54.0×0.76mm

照合時間 : 2 秒以下(平均 1 秒)

照合精度 : 本人拒否率 3%以下

他人受入率 0.001%以下

- ・指紋情報の照合によってのみ IC カードとして動作するので、紛失・盗難・なりすましによる被害の心配がなくなる
  - ・パスワード・暗証番号の管理・保守が無いので「人的ミスや内部不正」を防ぐ
  - ・利用者のアクセス制限の認証と同時に業務システムサイトの真正性の認証も兼ねるので「フィッシング攻撃」対策にも有効
  - ・内部データに対する外部からの改ざん、漏洩に対し堅牢で、安全性の最も高いオフライン端末
  - ・クレジットカードはもとより自治体(特に地方自治体)の住民データを保管する職員用パソコンの起動を AOC カード(パスワードレス)での制御が可能となる
  - ・病院のカルテに関するすべてのパソコン起動も制御可能となる。
- その他活用例は数多くある。



名古屋女子大学 学生証/職員証を 2022 年より実証中 5,000 枚数  
2024 年 2 月 基盤改良(薄さ 0.7mm)実用化完成  
これによりクレジットカード対応のパスワードレスカードの実用化可能となる。



(左) 指紋登録用リーダー (右) 読み取り用リーダー  
PC 用、店舗用、病院用



(活用方法)

この様な防犯対策が可能と成りました。

指紋認証カードシステムも MDT ジャパンは国内独占販売権を有することになり、医療機関ではパソコンパスワードレス化が完成したシステムを実施出来る様になりましたので、これまで病院が頭を悩まして来た患者カルテ(データ)の流出を阻止出来ます。

パスワードレス ID カードを職員が指紋認証を登録した場合パソコンはパスワード入力不可となり本人以外はパソコンを起動することが出来なくなります。パソコンごとに指紋認証カードリーダーの設置で簡単に防犯措置が取られます。侵入した職員はカード ID にすべて記録され入退と作業内容まで記録されます。

病院の職員の入退室(出勤記録含め)の記録も同様です。

この技術は病院同様にデータの盗用を止めることで国、地方自治体などで発揮します。

クレジットカードも成りすましの使用も防止できます。

**この指紋認証パスワードレス ID カードの最大の活用目標は国民が持つ政府(地方自治体)が発行した2種類の長たらしいパスワードを必要とする【マイナンバーカード】です。**

## 特許査定

特許出願の番号	特願 2021-193218
起案日	令和 5年11月27日
特許庁審査官	小林 秀和 3449 5S00
発明の名称	ブロックチェーンを利用したネットワークの認証システムとこれを使用した認証方法
請求項の数	3
特許出願人	エイエスディ株式会社 (ほか 1名)
代理人	田中 昭雄

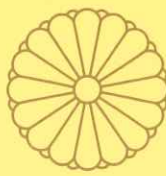
この出願については、拒絶の理由を発見しないから、特許査定をします。

---

上記はファイルに記録されている事項と相違ないことを認証する。

認証日 令和 5年11月28日 経済産業事務官 佐藤 隆

注意：この書面を受け取った日から30日以内に特許料の納付が必要です。



特許証  
(CERTIFICATE OF PATENT)

特許第7398183号  
(PATENT NUMBER)

発明の名称  
(TITLE OF THE INVENTION)

ブロックチェーンを利用したネットワークの認  
証システムとこれを使用した認証方法

特許権者  
(PATENTEE)

東京都品川区東五反田1丁目10番地7号

エイエスディ株式会社

広島県広島市中区上八丁堀5番25号

株式会社フィードバックコーポレイシ  
ョン

発明者  
(INVENTOR)

清本 尚一

出願番号  
(APPLICATION NUMBER)

特願2021-193218

出願日  
(FILING DATE)

令和 3年11月29日(November 29, 2021)

登録日  
(REGISTRATION DATE)

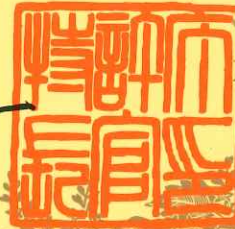
令和 5年12月 6日(December 6, 2023)

この発明は、特許するものと確定し、特許原簿に登録されたことを証する。  
(THIS IS TO CERTIFY THAT THE PATENT IS REGISTERED ON THE REGISTER OF THE JAPAN PATENT OFFICE.)

令和 5年12月 6日(December 6, 2023)

特許庁長官  
(COMMISSIONER, JAPAN PATENT OFFICE)

濱野 幸一

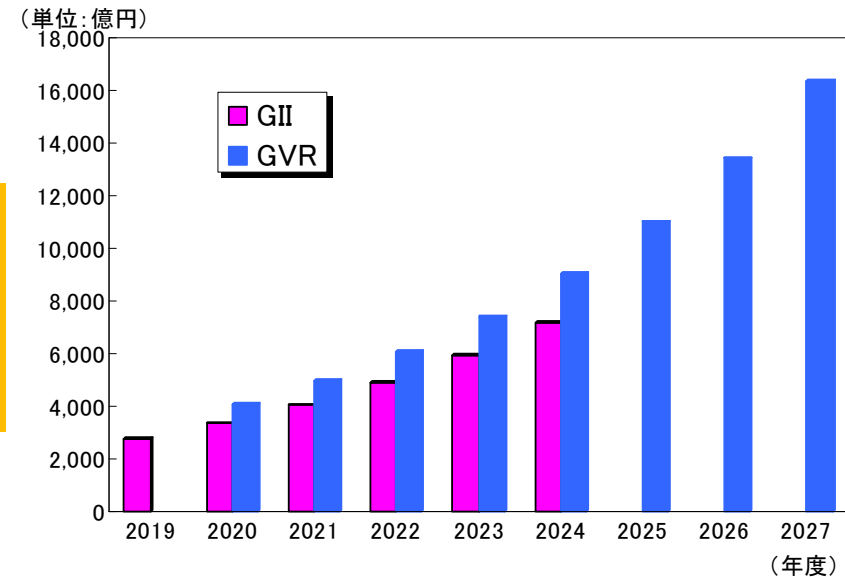


# 1. FIDaaS認証基盤サービスの背景と目的

● 当社のFIDaaS認証基盤サービスは、サイバー攻撃を水際でブロックします

◆ 米国の市場調査レポート（2社）のサイバーテロ対策の市場規模予想

（出典：2019年9月、Global Information, Inc. 2020年5月、Grand View Research のレポート）



**流出した暗証番号が、闇のインターネット・サイトで展示販売**

2020年8月時点で900社超（国内38社）の分が、闇のサイトに掲載を公表。（内閣サイバーセキュリティセンター-NISC）

**2020年にランサムウェア攻撃に支払われた被害額は、世界で400億円に達した**

サイバーテロによる被害額は、2025年には2137億ドル（約23兆円）に達する見込み。（日本経済新聞2021年5月12日）

**2021年10月、徳島県の町立半田病院で、電子カルテが暗号化、身代金を要求された**

「愛知県がんセンター」、「九州歯科大学」等、昨年だけで11の医療機関でもサイバー攻撃。（日本経済新聞2021年11月12日）

**政府は、「経済安全保障推進法案」の骨子を発表、3月に閣議決定**

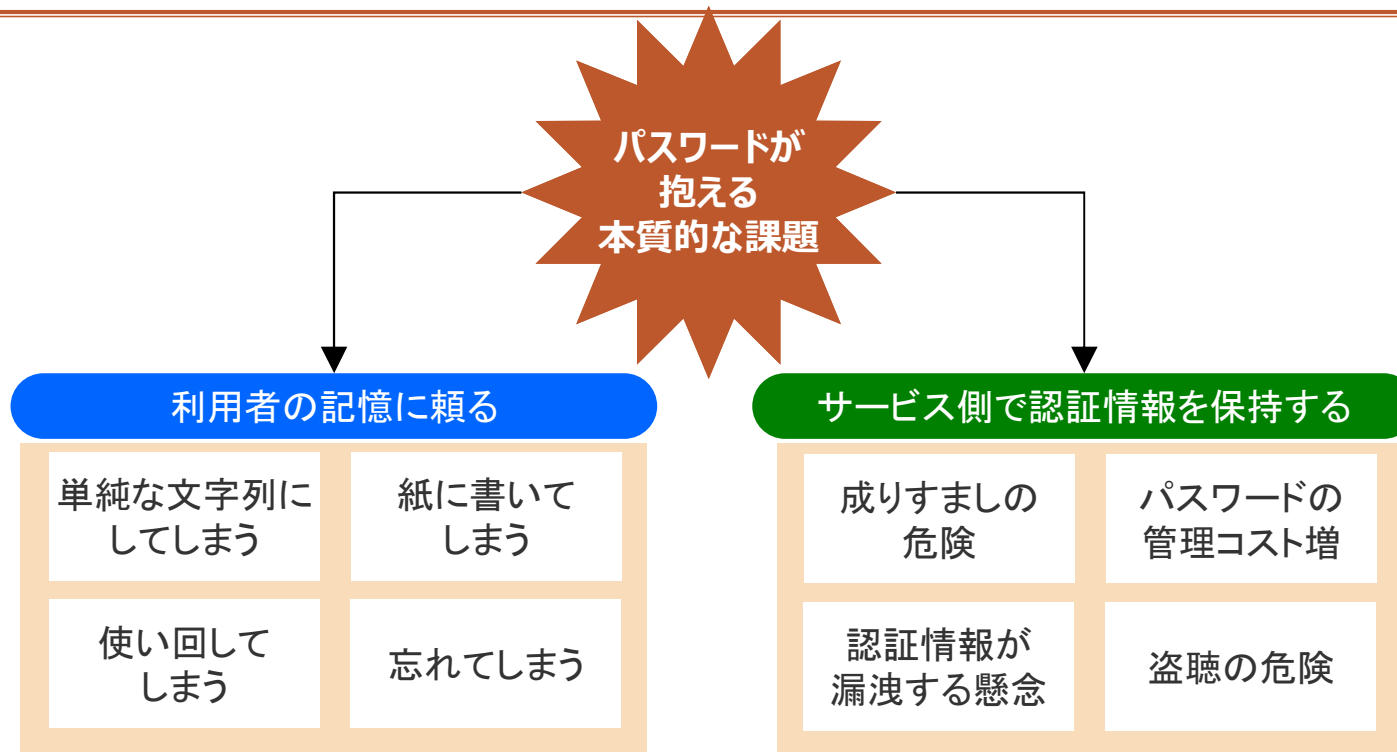
官民にサイバー攻撃への備えを義務付ける。情報の保護義務かと情報漏洩に対する罰則検討。（日本経済新聞2021年12月20日）

**政府は、「サイバー・フィジカル・セキュリティ対策フレームワーク」で「新たな社会（Society5）」を提唱**

出典：内閣府ホームページ（[https://www8.cao.go.jp/cstp/society5\\_0/index.html](https://www8.cao.go.jp/cstp/society5_0/index.html)）

出典：内閣府ホームページ（[https://www8.cao.go.jp/cstp/society5\\_0/index.html](https://www8.cao.go.jp/cstp/society5_0/index.html)）

## 2. (1) パスワードにまつわる課題



出典: 日経クロステック/<https://xtech.nikkei.com/atcl/nxt/column/18/01677/060400001/>



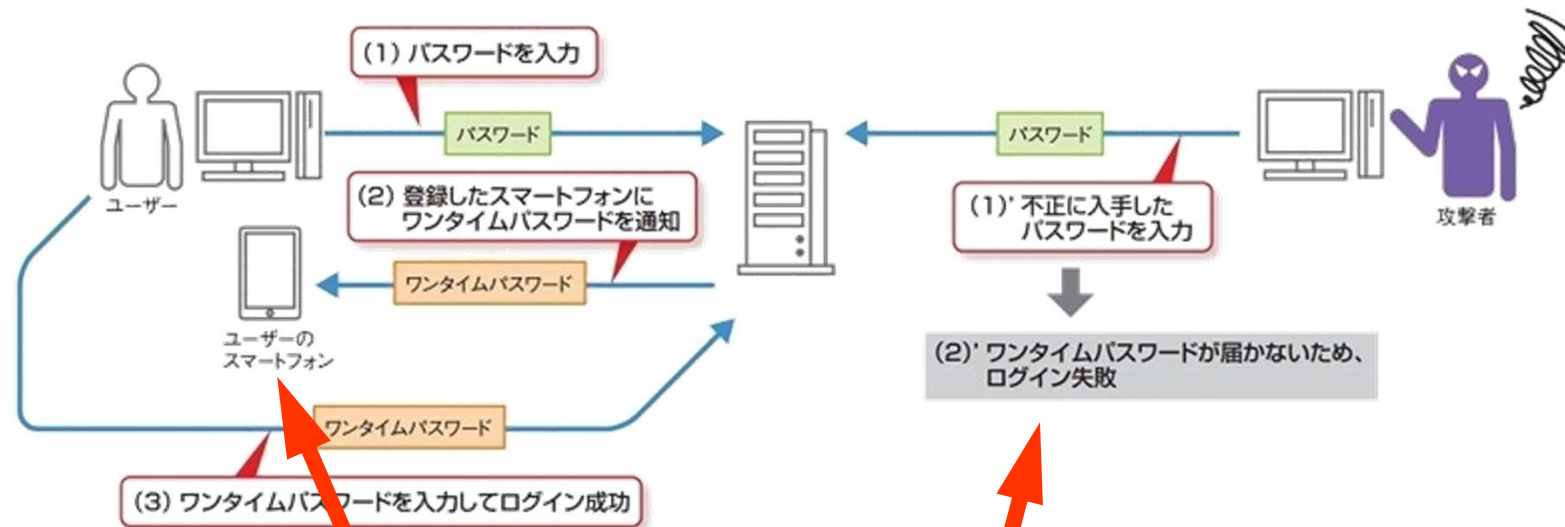
課題は未解決のまま!



## 2. (2) パスワードの弊害 ～パスワードレスの必要性

- 米Microsoft(マイクロソフト)は2022年7月中旬、大規模なフィッシング攻撃(フィッシング詐欺)が展開されているとして注意を呼びかけた。
- Microsoft 365(旧称Office365)を利用する企業や組織。2021年9月以降、1万を超える企業や組織に対して攻撃が行われているという。

この攻撃の特徴は、大規模なことに加えて**多要素認証(MFA: Multi-Factor Authentication)**を破ること。攻撃者は多要素認証を破り、正規ユーザーのメールアカウントなどを乗っ取る。




パスワードとワンタイムパスワードを組み合わせた多要素認証の流れ (出所:日経NETWORK)

ワンタイムパスワードは、何故安全なのか？  
そのスマホは、だれのモノ！  
スマホもオンライン端末です…

### 3. (1) FIDaaS認証基盤の位置付け (1)

米国の著名な調査機関が、2022年度の重要核心技術として「パスワードレスの実現」を提示

- \* マサチューセッツ工科大学 (MIT) のメディア企業MITテクノロジーレビュー社が、「世界を変えるブレークスルー・テクノロジー10、2022年版」の第3位に「パスワードの終わり」を挙げました。



\*2022年のブレークスルー・テクノロジーは以下のとおり

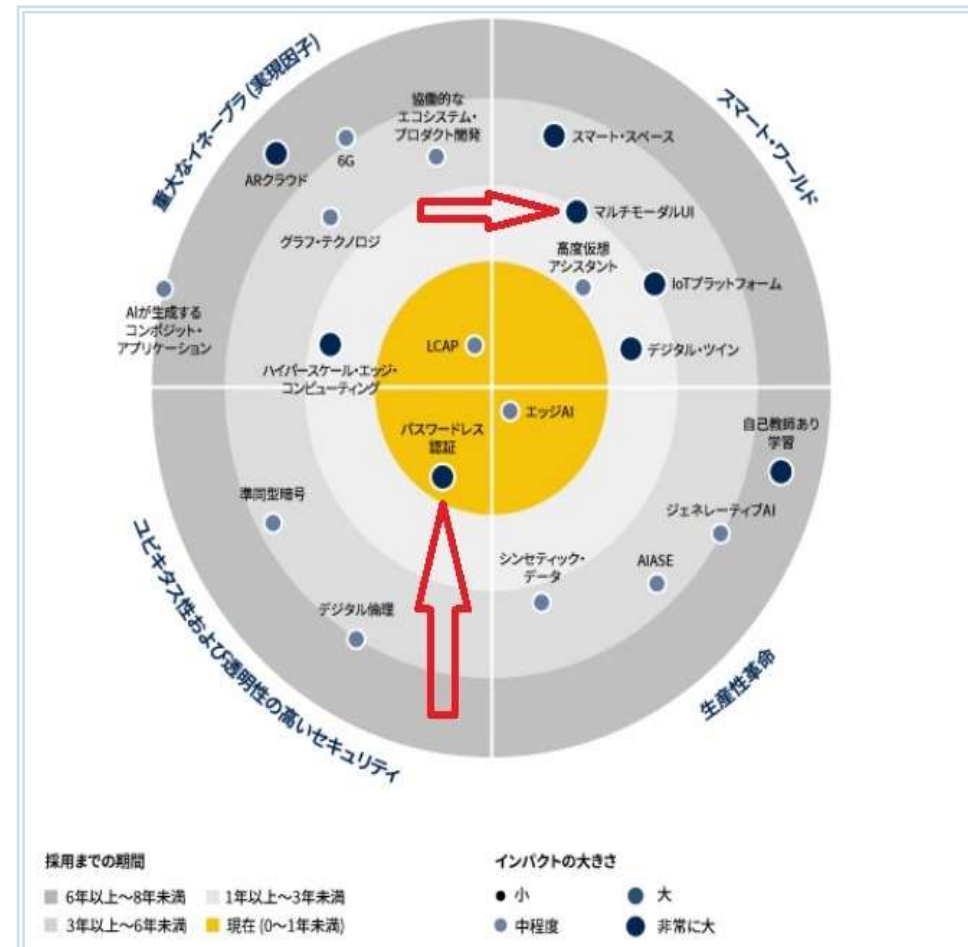
1. 新型コロナ飲み薬
2. 実用的な核融合炉
3. パスワードの終わり
4. タンパク質構造のAI予測
5. プルーフ・オブ・ステーキ (Proof of Steak)
6. 送電網向け「長持ち」蓄電池
7. AIのための合成データ
8. マラリアワクチン
9. 炭素除去工場
10. 新型コロナ変異株追跡

(出典 : <https://www.technologyreview.jp/s/269568/mit-technology-review-has-released-breakthrough-technologies-of-2022/>)

### 3. (2) FIDaaS認証基盤の位置付け (2)

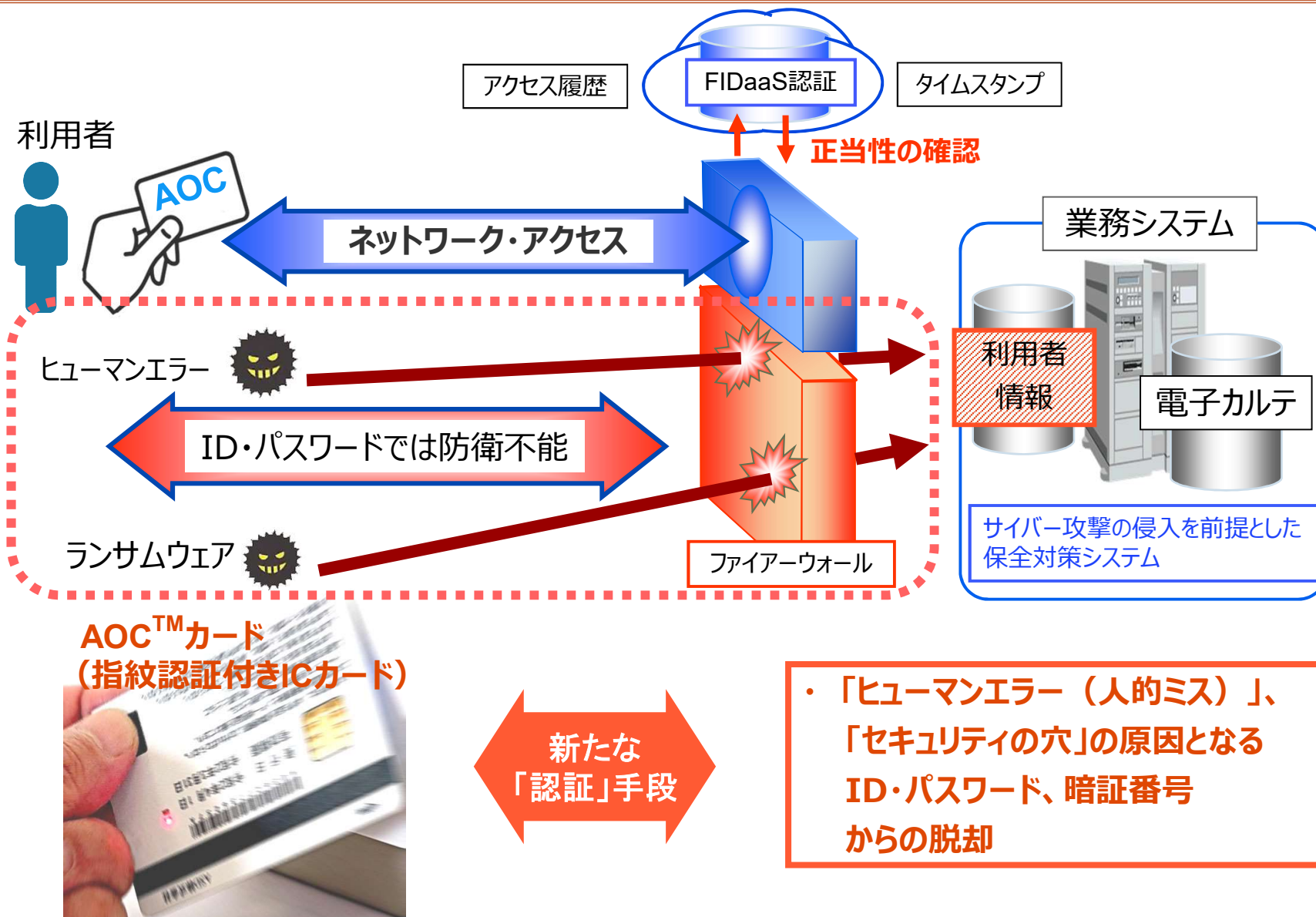
- \* 米国のガートナー社は、「市場に変革をもたらす可能性が最も高い先進テクノロジー・トレンド20」の2022年版において「パスワードレス認証」を挙げ、20テーマの中で最も早期の実現が期待されるとしています。

- \* 2022年の先進テクノロジー・トレンドの検知レーダー(20テーマ)

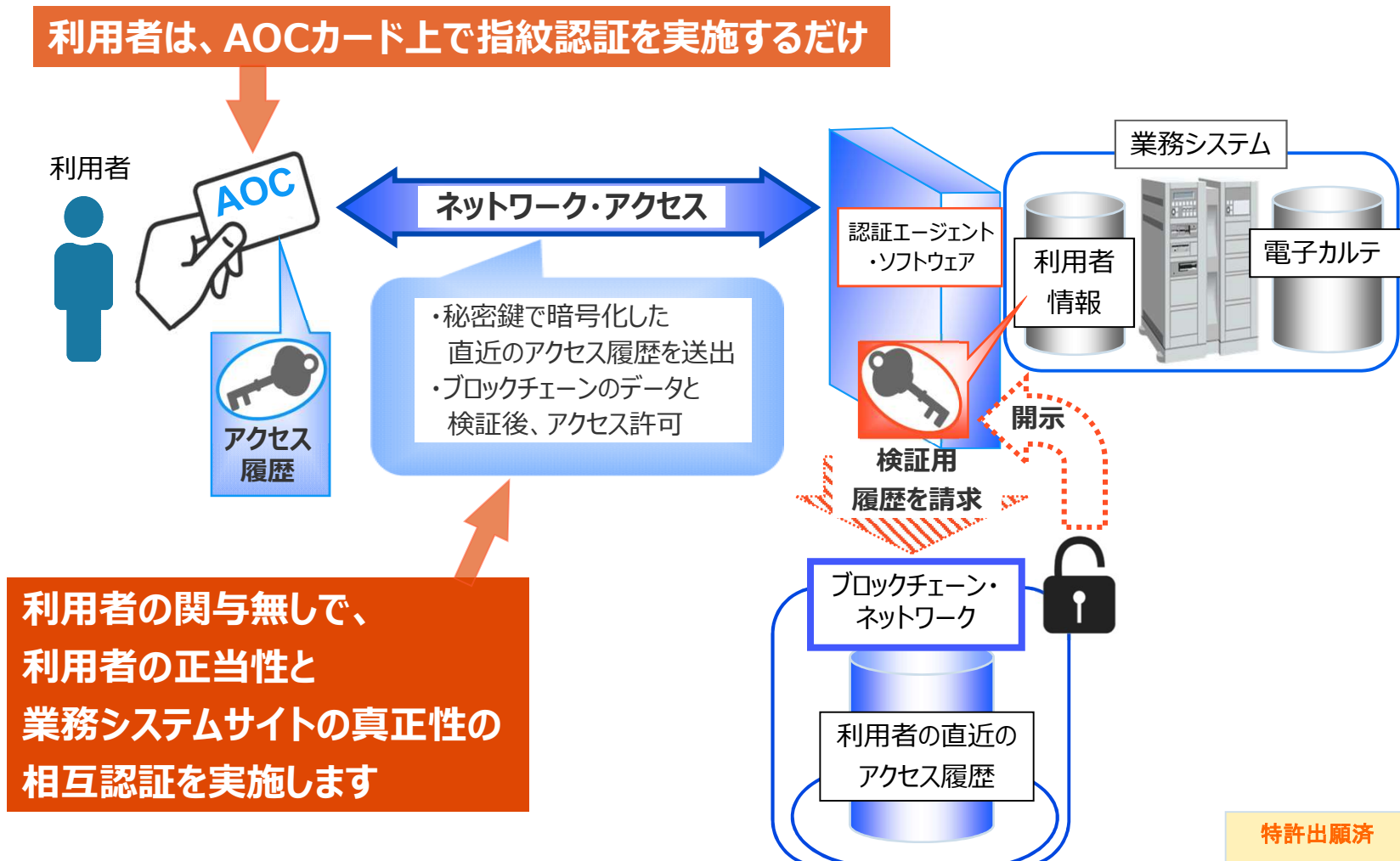


(出典 : <https://www.gartner.co.jp/ja/articles/5-impactful-technologies-from-the-gartner-emerging-technologies-and-trends-impact-radar-for-2022> )

## 4. (1) FIDaaS認証とは (システム概要)

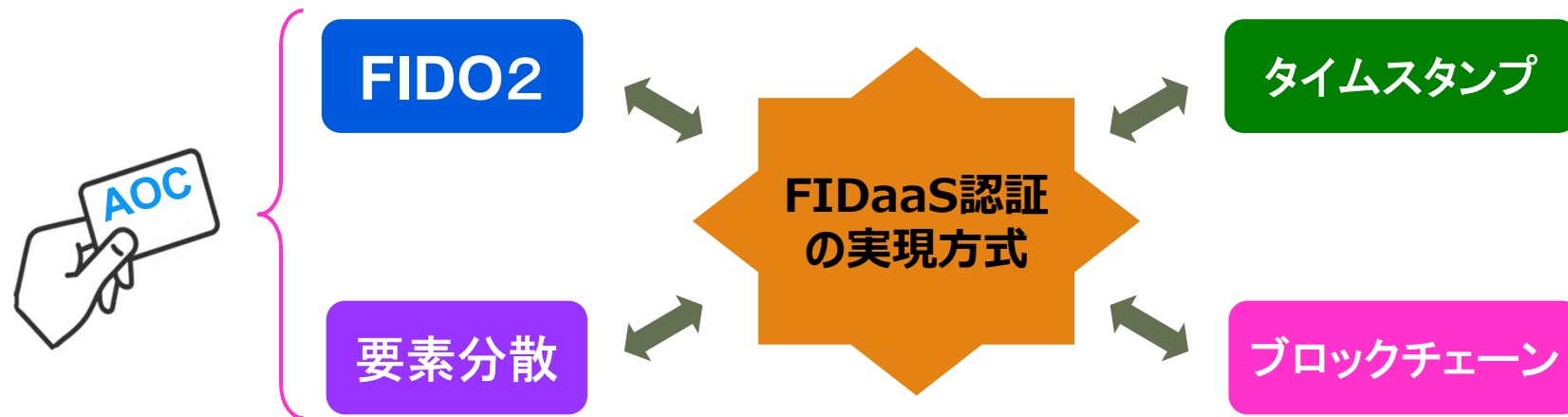
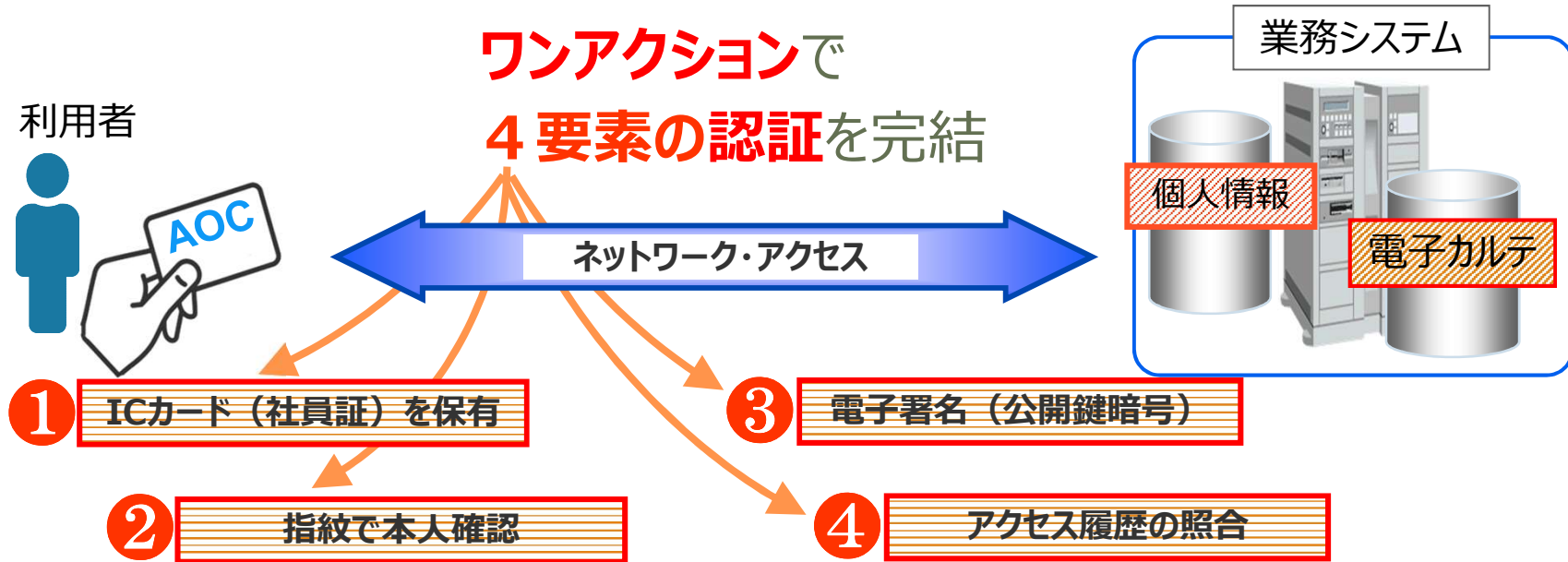


## 4. (2) FIDaaS認証の仕組み



- ① バックグラウンドで、利用者のカード内に秘匿された「直近のアクセス履歴」を秘密鍵で暗号化し、「認証エージェント」に送ります。
  - ② 「認証エージェント」では、利用者の直近のアクセス履歴をブロックチェーンネットワークより取り寄せ、両者を照合し、利用者のアクセスの権限を検証します。
- ※ AOCは、「指紋認証付きICカード」の意味で当社の登録商標。

## 5. パスワードレス、実現へのアプローチ



## 6. FIDaaS認証導入メリット ～ セキュリティ

---

- ICカードは、内部データに対する外部からの改竄、漏洩に対し堅牢で、安全性の最も高いオフライン端末です
- AOCカードは、指紋情報の照合によってのみICカードとして動作するので、紛失、盗難時にも、「なりすまし」による被害の心配は不要です
- パスワード・暗証番号の管理・保守が無いので「人的ミスや内部不正」も起きません
- 利用者のアクセス権限の認証と同時に業務システムサイトの真正性の認証も兼ねるので「フィッシング攻撃」に対する対策にも有効です。

## 7. FIDaaS認証事業のターゲット市場

### ■ 昨年10月にランサムウェア攻撃を受けた徳島県つるぎ町立半田病院における事例分析

- ・**ベッド数120床の地方中核病院。**
- ・**患者約8万5千人分の電子カルテが暗号化**され閲覧できなくなった。
- ・ハッカー集団からの身代金要求額は、800万円だったと言われているが、身代金を支払わずに、**総費用2億円と2ヶ月間の期間を費やして病院内システムをリニューアル**させた。
- ・旧ソ連圏に關係する**ハッカー集団「ロックビット」**が、病院への攻撃を宣言。  
国家が捜査に乗り出すような大病院でなく、中堅病院をターゲットとすることを公言。
- ・医師たちのセキュリティに対する意識は低く、このケースも**一医師のID・パスワード管理のミス**から始まったとされている。
- ・以上の条件から、全病院の中、**100床～300床規模**の3877の中堅病院での電子カルテの保護対策が喫緊の課題と考え、**当面の5年間でその3割に当る1163病院への導入を目標とする。**

### ■ 多発する自治体からの個人情報流出

- ・東京商エリサーチの調べによると、**2021年だけで約575万人の個人情報**が漏洩されていて、自治体等の行政サービス機関からの情報流出も多発している。最近では、**宮城労働局の書類の盗難等の内部不正**や**尼崎市でのUSBメモリによる個人情報の持ち出し騒動**等枚挙に暇が無い。
- ・ID・パスワード管理に代表される**ヒューマンエラー**が、**内部不正のみならず、サイバー攻撃の元凶**になっている。
- ・**地方自治体に導入されているPCのログイン制御ソフトウェア**は、職員の身分証明書であるICカードとの連携が進み、**PC用のカードリーダーも250万セットが配備**されている。勿論、ICカードの採用は、カードの盗難、紛失問題に始まり、**他人使用(なりすまし)の問題がクローズアップ**され、指紋付きカードを含めてFIDaaS認証のターゲット市場と目される。