

# サイバーセキュリティの脅威と対策について パスワードレス認証 (FIDaaS 認証)の有効性



～ FIDaaS 認証は、パスワードに依存せず、  
サイバーテロを遮断する世界で始めてのセキュリティ基盤 ～

エイエスディ株式会社 (ASD Inc.) 代表取締役 **清本 尚一**

## 1. サイバーセキュリティの強化は喫緊の重要課題である。

- 1) サイバーテロの増加
- 2) テロ集団の攻撃目標
  - ・ 中堅病院
  - ・ 行政機関
  - ・ 社会インフラ

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、2025年には2137億ドル(約23兆円)に達する見込みとの報道も見られる。

また2022年のランサムウェア被害件数は、警察庁に報告があったものだけで37都道府県で230件あり、前年比57.5%増と急増中で、企業・団体の規模を問わず被害が発生している。

2021年10月に徳島県半田病院の電子カルテを暗号化し、約2か月間、病院機能を停止に陥らせたサイバーテロ集団のロックビットは、攻撃対象として、医療機関や警察、教育機関などを挙げている。

病院では、医療機器のネットワーク化が進むものの、セキュリティ対策が不十分で、それがサイバー攻撃の脅威に晒される一因となっている。

更に、この度のパンデミックにより各関係機関とのリモート・アクセス、データ交換の機会が激増する中、パスワード認証のみに基づいたVPNシステム環境と、それに対する人的ミスが相まって、セキュリティの穴を広げているものと考えられる。

実際、昨年10月の大阪急性期・総合医療センターにおけるランサムウェアの侵入口は、患者の食事の納入事業者のシステムである可能性が高い

とされている。病院側はサーバーに、患者の情報を集約、パスワード認証のみに基づいた脆弱なVPN装置により接続していたことが原因とされている。

二つの病院に対するサイバー攻撃からも共通してパスワード認証の弊害が想起される。

こうした事態を受け、厚生労働省は医療機関向けのセキュリティ対策のガイドライン<sup>2)</sup>を改定し、通知している。

3) 日本国内での警鐘(【表1】参照)

4) 米国調査機関による報告

MIT T.R.社<sup>3)</sup>およびガートナー社<sup>4)</sup>は、最も早期の実現が期待される先進技術(2022年版)として「パスワードレス認証」を挙げている。

【表1】IPAによる「情報セキュリティ10大脅威2022」

順位	事 案
1位	ランサムウェアによる被害
2位	標的型攻撃による機密情報窃取
3位	サプライチェーンの弱点を悪用した攻撃
4位	テレワーク等のニューノーマルな働き方を狙った攻撃
5位	内部不正による情報漏洩

※上記表中の事案は、FIDaaS認証により抑止可能

## 2. 現状の問題点

1) パスワードに依るセキュリティの崩壊

- ・ 人的ミスの増加

パスワードの抱える課題に連動【表2】

- ・ 携帯電話等オンライン端末の脆弱性

- ワンタイムパスワードの脆弱性が発覚
- ・フィッシング詐欺等で窃取されたパスワードや暗証番号が、「闇サイト」で売買
- 2) サイバーセキュリティ要員の不足

【表2】パスワードが抱える課題<sup>5)</sup>

◆利用者の記憶に頼る	
・単純な文字列にしてしまう	・紙に書いてしまう
・使い回してしまう	・忘れてしまう
◆サービス側で認証情報を保持する	
・成りすましの危険	・パスワードの管理コスト増
・認証情報が漏洩する懸念	・盗聴の危険

【表2】に挙げたとおり、パスワードの強化はユーザーに過剰な負担を強いることとなり、結果としてずさんな管理を招きがちである。ハッキングによる情報漏洩の81%はパスワードに起因するとの調査報告もある。

2020年8月時点で900社超(国内38社)の流出した暗証番号が、闇のサイトに掲載・販売されている事実を内閣府(NISC)が公表し注意を喚起した。

不正なアクセスを防ぐとする多要素認証も、巧妙に回避するサイバー攻撃が出現している。

例えば、Webアプリやブラウザのセッションに侵入する「セッションハイジャック」や、プログラムの脆弱性について不正アクセスを実施する「インジェクション攻撃」などが多要素認証を回避する手段として悪用されている。

リモートワークなどのワークスタイルの変化やDXの進展により、企業が扱うIDは膨大な数に上り、そのID管理と統制は簡単ではない。また、莫大な費用負担が生じる。

### 3. パスワードレス認証 (FIDaaS 認証)

- 1) 世界で初めての新技术(特許出願中)
- 2) パスワード無しで、人的ミスを排除
- 3) 利便性の向上

<ワンアクションで多要素・多段階認証>

- ・身分証(ICカード)の所持による証明
  - ・指紋による本人確認
  - ・電子署名(公開鍵暗号)の秘匿保持
  - ・アクセス履歴の照合
  - ・アクセスサイトの真正性の確認
- 4) セキュリティ手段のオフライン化
  - 5) ローコストで導入可能  
(容易な導入、維持コスト、導入コスト)

利用者は、AOCカード(指紋認証付きICカード)に指を乗せ、カードリーダーにかざすだけで全ての認証が完了する。複雑なパスワードの入力も無く、人的ミスの生じる余地は無い。

AOCカードは、ネットから切り離されたオフライン装置であり、ハッキング不可能である。

また、ブロックチェーンネットワークで管理されたアクセス履歴を照合することにより、アクセスサイトの真正性も担保することができる。【図1】参照のこと。

- 1) IPA「情報セキュリティ10大脅威2022」<https://www.ipa.go.jp/security/vuln/10threats2022.html> (本文中に脚注<sup>1)</sup>なし、リンク先404)
- 2) 厚労省「医療情報システムの安全管理に関するガイドライン」<https://www.mhlw.go.jp/content/10808000/000936160.pdf>
- 3) MITテクノロジーレビュー社 <https://www.technologyreview.jp/s/269568/mit-technology-review-has-released-breakthrough-technologies-of-2022/>
- 4) 米国ガートナー社 <https://www.gartner.co.jp/ja/articles/5-impactful-technologies-from-the-gartner-emerging-technologies-and-trends-impact-radar-for-2022>
- 5) 日経クロステック <https://xtech.nikkei.com/atcl/nxt/column/18/01677/060400001/>

【図1】FIDaaS認証の運用イメージ～ワンアクションで多要素・多段階認証

