Security White Paper 2023

改めて考える MFA の最適解

多要素認証がなぜ突破されているのか？

脆弱性や漏えいした認証情報を悪用してシステム侵入するランサムウェア対策として、多要素認証（MFA：Multi-Factor Authentication）の重要性が指摘されていますが、現在、その多要素認証を突破する攻撃手法が台頭しつつあります。攻撃防御の要となる多要素認証の最適解は何か？ 攻撃耐性やコスト、運用面を踏まえて改めて考察します。

2023 / 03

日本の企業・組織では DX が進み、機密情報や営業秘密がクラウドで共有されることも当たり前の時代となりました。その一方で、ランサムウェアを起因とするデータ漏えい・侵害の件数が著しく増加しており、脅威環境の変化を踏まえたセキュリティリスク対応も急務となっています。

脆弱性や漏えいした認証情報を悪用して侵入するランサムウェア対策として、重要性が指摘されている多要素認証（MFA：Multi-Factor Authentication）ですが、現在、その多要素認証を突破する攻撃手法が台頭しつつあります。

攻撃防御の要となる「多要素認証」の最適解は何か？ 攻撃耐性やコスト、運用面を踏まえて改めて考察します。

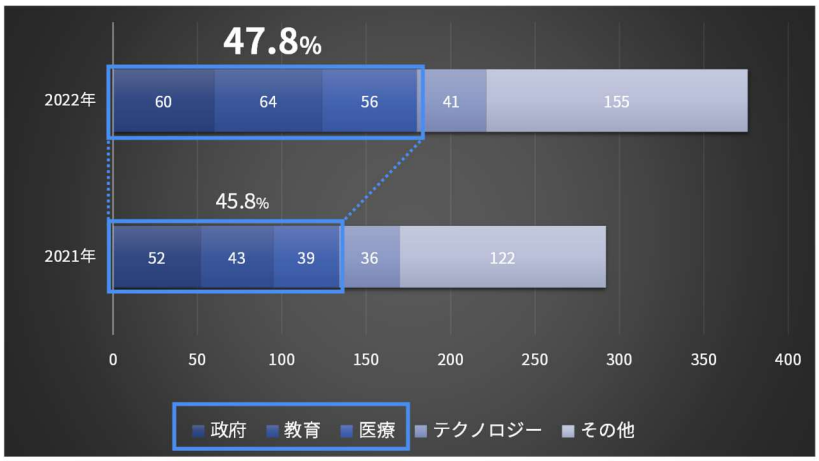
ランサムウェア被害が目立った 2022 年

ここに挙げたものは、あくまで一例であり、明日は我が身と考えるべきではありますが、2022 年は本当にランサムウェア被害が目立った 1 年でした。特に、脆弱な VPN 機器などからの侵入が多かったという状況です。

被害発生月・業種	被害内容
2 月 製造業	子会社が取引先との接続に利用していた**リモート接続機器経由**で、侵入されランサム感染。製造業の取引先である、大手企業も影響確認のため業務停止。
4 月 飲料メーカー	インターネット回線に接続した**ネットワーク機器の脆弱性経由**で侵入され、ランサム感染。個人情報を含む情報漏えいの可能性が否定できない状況に。
10 月 医療機関	取引先の**ソフトウェア未更新 VPN 機器から侵入**され、医療機関もランサム感染。電子カルテシステムが利用できず、数千人の患者に影響。

※ 各組織より公開された情報を元に Soliton にて整理

この数年で、ランサムウェア被害は増加傾向にあります。BlackFog 社のグローバルで公開されているランサムウェア事案の被害件数においても、2022 年は 2020 年と比べて 1.5 倍の 376 件に増えていると報告されています。これはあくまで氷山の一角であり、おそらくこの 10 倍程度は被害があるものと考えたほうが良さそうです。日本でも 2022 年後半から、被害組織の規模が大手グローバル企業だけではなくなってきたことは肌感覚としてあるのではないでしょうか。



被害組織の 47.8% が政府・教育・医療機関

残りの半数は業種多岐にわたる
どの業種もターゲットになることは
継続して注意が必要

業種別ランサムウェア被害件数推移（グローバル）
BlackFog社のデータを基にSolitonでグラフ作成

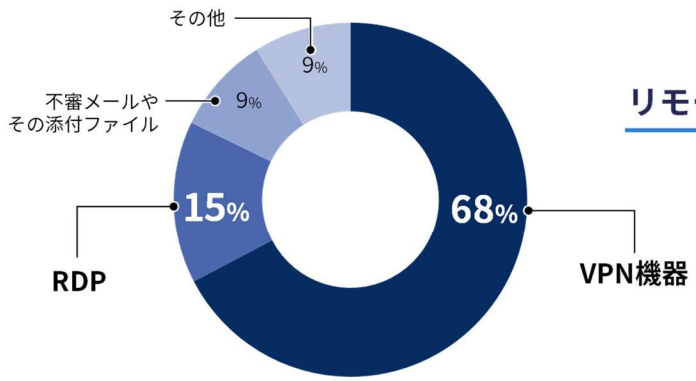
The State of Ransomware in 2023(BlackFog, February 3rd, 2023)
https://www.blackfog.com/the-state-of-ransomware-in-2023/

被害公表した組織の業種を見てみると、2022 年では全体の 47.8%が政府・教育・医療機関での被害でした。日本でも、医療機関への攻撃が報道されることが増えていることから、これはグローバルの攻撃傾向と見て良さそうです。ただし、業種が多岐にわたっているだけで、残り半数は民間企業で被害が発生しているわけですので、どの業種も狙われる可能性があるということを忘れずに、引き続き対策する必要があります。

日本における“侵入型”ランサムウェアの被害

現在主流となっているランサムウェアは、日本では、「侵入型ランサムウェア」と言われています。別名、二重恐喝型、暴露型、標的型などとも呼ばれるもので、**従来のランサムウェアとは異なり、企業や組織を狙い**、侵入後に情報を盗み出したうえでデータを暗号化し、復号化のために金銭を要求するとともに、それに応じなければ盗み出したデータをリークサイトで暴露する二重の恐喝をする攻撃手法です。

警察庁から発表されたレポートにおいても、この侵入型ランサムウェアの被害が急増していることが報告されており、日本でもこのタイプの攻撃が増えています。



ランサムウェアの感染経路（令和4年9月15日 警察庁）

リモートアクセス経由の侵入 83%

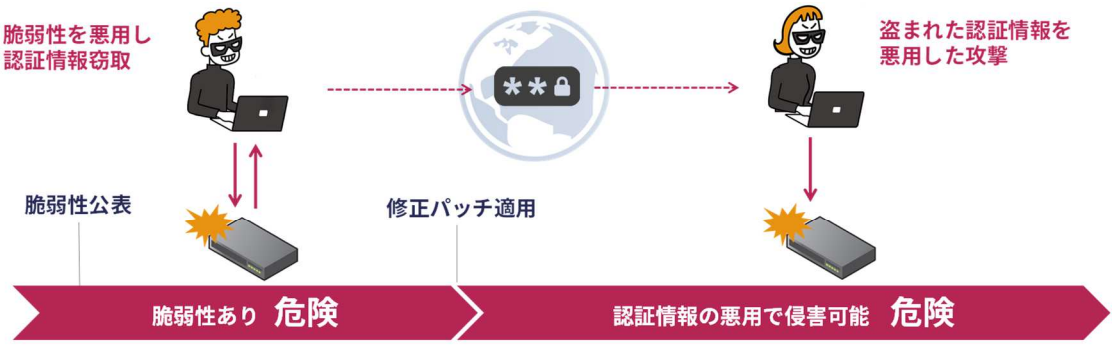
令和４年上半期におけるサイバー空間をめぐる脅威の情勢等（令和4年9月15日 警察庁）
図表7：感染経路（注 図中の割合は小数第１位以下四捨五入しており、総計が必ずしも100にならない）

警察庁のデータでは、**侵入経路は VPN 機器からの侵入が最も多い 68%を占めており、リモートデスクトップはその次となっています**。つまり、侵入型ランサムウェアに効果的なリスク対策をしたければ、まず、侵入経路であるリモートアクセスからの侵入対策を強化しなければならないということになります。

漏洩した認証情報を悪用した攻撃

リモートアクセス経由での侵入対策としては、まず脆弱性対策が基本です。各ベンダーの提供する情報をよく確認したうえで、修正バージョンをいち早く適用するということが推奨されます。VPN ばかりが注目されますが、VPN 以外にもリモートアクセスできる仮想化製品なども視野に入れ、脆弱性対策を実施していく必要があります。

しかし、一つ注意しなくてはならないのは、脆弱性対策だけでは不十分であるという点です。パッチ適用前に脆弱性を突いて **認証情報、つまり、ID・パスワードが盗まれていた場合**、パッチを適用して脆弱性が無くなっても、パスワードを変更していなければ、盗み出された正規のアカウントと認証情報を使って侵入されてしまいます。日本国内においても、既に盗まれてしまった認証情報を使って攻撃されるケースがかなり発生しています。



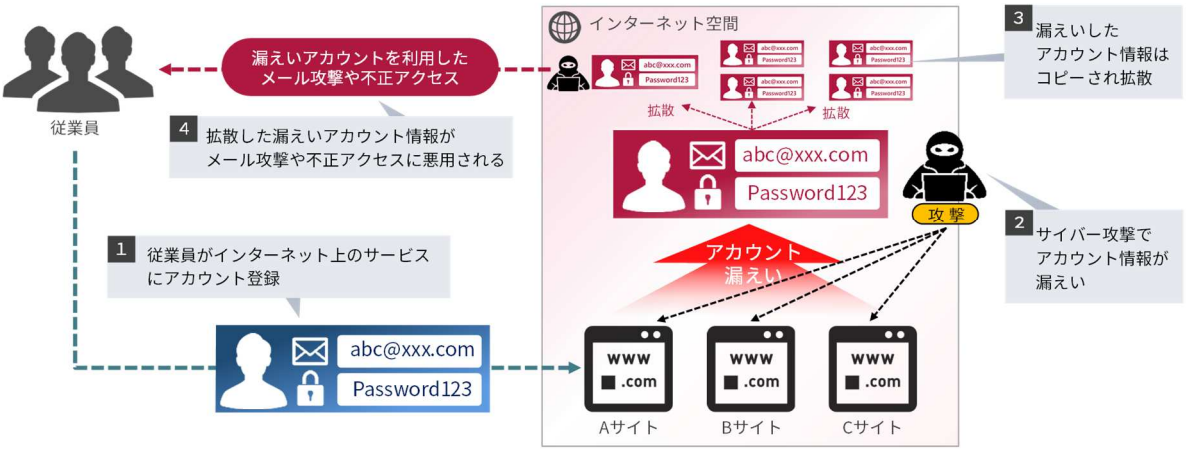
“VPN機器での脆弱性公表～認証情報を悪用した攻撃”のタイムライン例

最近のサイバー攻撃とインシデント対応のポイント（JPCERT/CC, 2021年2月） https://www.isaca.gr.jp/cism/img/2021_kouen1.pdf

考察事項①「日常的なアカウント漏洩」

認証情報を窃取する手段は VPN 機器への脆弱性攻撃だけではありません。インターネット上には企業で認められたクラウドサービスだけでなく、会員向けニュースサイトなど、アカウントを登録して利用するさまざまな便利サービスがあり、**それらに登録したユーザーアカウントが、サイバー攻撃により流出する事件が多発しています**。従業員が業務利用目的で登録したユーザーID やパスワードが漏洩した場合、不正アクセスや標的型攻撃のターゲットとなるリスクが高まります。

ソリトンシステムズがこれまでご依頼いただいて実施した「漏洩アカウント被害調査」（調査数 2000 ドメイン以上）でも、**99.9%の企業・団体で、現職職員のパスワードを含むアカウント漏洩が確認されおり、これはもう日常と思って対策するしかない**、というのが現実といえそうです。



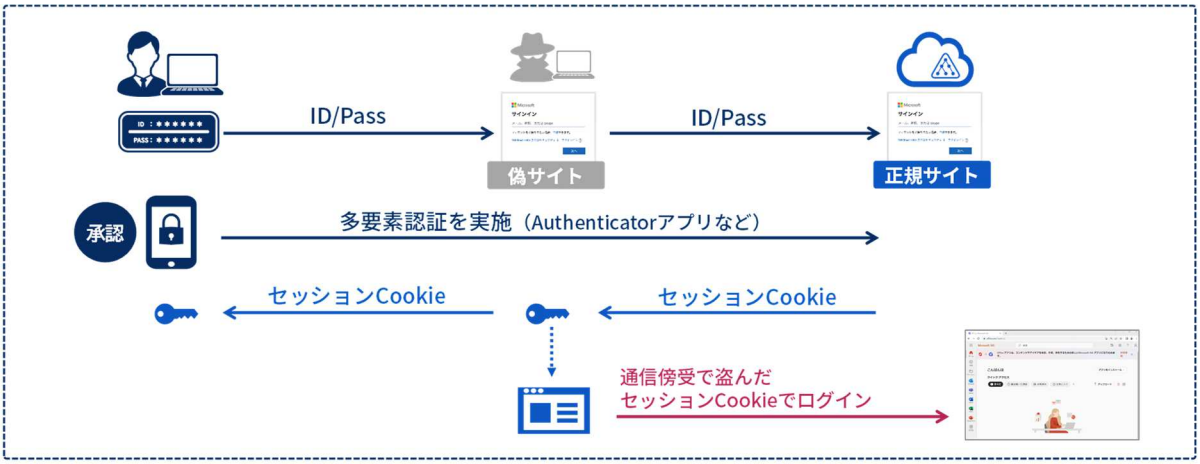
考察事項②「多要素認証を突破する攻撃の急増」

アカウントとパスワードだけでは不正にログインされるという前提に立ち、もう一つ鍵をつけるのが多要素認証（MFA）です。アカウントとパスワードともう一つ何かがないとログインできないため、認証情報を悪用した攻撃を防ぐことができます。しかし、これで安心という訳ではありません。昨年の夏頃ニュースになりましたが、**最近はこの多要素認証を突破する攻撃が出現しています。**

- 日経クロステック／日経 NETWORK、2022 年 7 月 27 日
  「多要素認証」を破る大規模フィッシング、1 万社以上の Microsoft 365 利用企業を襲う
  https://xtech.nikkei.com/atcl/nxt/column/18/00676/072100111/
- 日本経済新聞、2022 年 8 月 3 日
  「多要素認証」破る攻撃　Microsoft 365 利用企業襲う
  https://www.nikkei.com/article/DGXZQOUC285SD0Y2A720C2000000

米 Microsoft からの情報として、2021 年の 9 月以降、1 万を超える企業や組織に対してフィッシング攻撃で MFA（Multi-Factor Authentication）を突破する攻撃が行われている、という注意喚起が出されました。

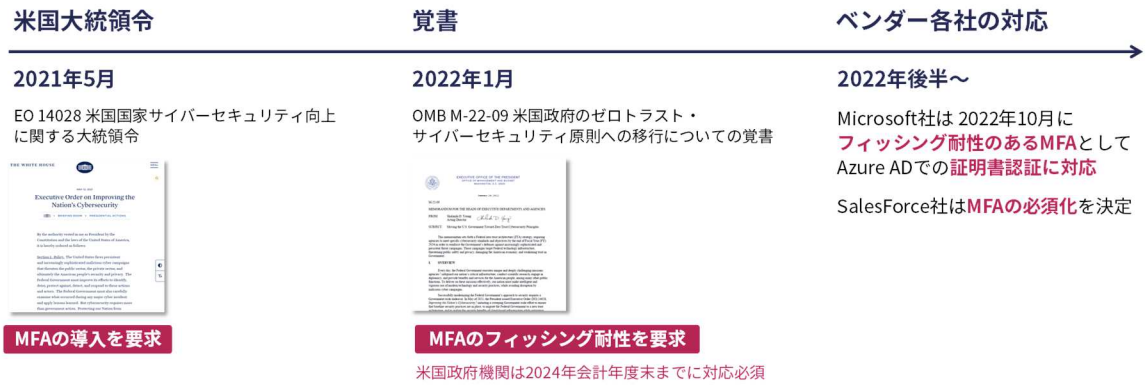
攻撃者は、偽サイトに入力させた ID とパスワードを正規サイトにそのまま送り、利用者がスマホアプリなどで承認操作（＝多要素認証）を実施すると、中間にいる攻撃者はログインで利用するセッション Cookie を通信傍受で盗むことができ、これをもって多要素認証が突破されています。



多要素認証を突破する AiTM 攻撃例（Adversary in the Middle）
上記は簡略化して記載。Pass-the-Cookieと呼ばれる手法であるが、この他にもMFAを突破する攻撃手法が複数報告されている。

もともと米国では、2021 年 5 月に大統領令で MFA 導入が要求されていましたが、多要素認証を突破する攻撃にも対応しなければならなくなり、2022 年 1 月に出された覚書では、フィッシング耐性のある MFA の導入が要求され、米国政府機関は 2024 年会計年度末までに対応することが求められています。

これを受け、Microsoft 社では**フィッシング体制のある MFA の一つとして Azure AD へのデジタル証明書認証に対応しました。**また Salesforce 社では利用者へ MFA 利用を必須化するなど、ベンダー各社の対応も進んでいます。



Executive Order on Improving the Nation's Cybersecurity：https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles：https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
認証強度 - シナリオに適した認証方式を選択可能に：https://jpazureid.github.io/blog/azure-active-directory/authentication-strength-choose-the-right-auth-method-for-your/
多要素認証（MFA）への対応のお願い：https://help.salesforce.com/s/articleView?id=000392813&type=1

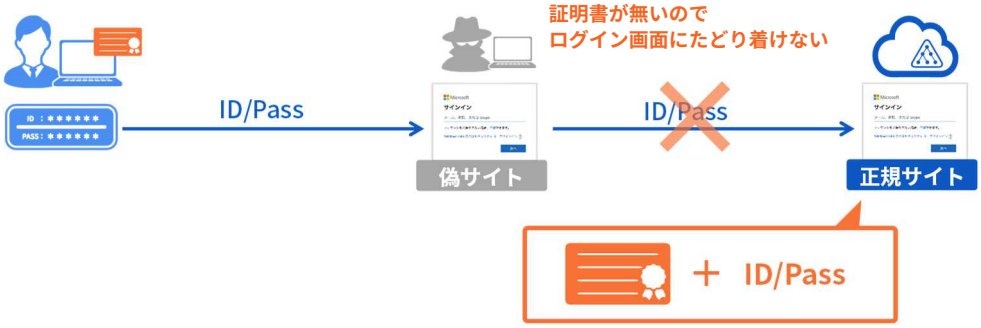
フィッシング耐性のある多要素認証を考察

日本の企業・組織において、どのような多要素認証が最適なのでしょうか。多要素認証は一つの認証要素ではなく異なる複数の認証要素を組み合わせるもので、認証要素には「知識」「所有」「生体」の 3 種類があります。

- **知識** … 導入運用は容易だが漏洩しやすい（パスワード、イメージマトリクスなど）
- **所有** … 導入運用性・コストのバランスから広く利用される（USB キー、IC カード、**デジタル証明書**など）
- **生体** … 導入・運用コストとも比較的高め、漏洩時の対応に限界がある（指紋、顔、静脈など）

パスワードとパスワードなど、同じ認証要素の組み合わせでは多要素認証にはならず、IC カードとパスワード、顔認証とパスワードなど、２つを組み合わせるものが多要素認証となります。

この中でも、**フィッシング耐性が高いのがデジタル証明書です**。デジタル証明書を用いた公開鍵暗号方式は、利用端末が特定できる上、フィッシングによる認証情報詐取を防止できるメリットがあります。また**正規の証明書を持たない攻撃者はログイン画面にたどり着けないため、パスワードリスト攻撃対策になるだけでなく、脆弱性攻撃の成立も困難なものとします。**



フィッシング耐性のほか、認証デバイス紛失時の対応や利用用途、対応 OS、またコストにおいても優位点があり、**デジタル証明書は、企業・組織にとって採用しやすい多要素認証といえます。**

	デジタル証明書	他の多要素認証（所有、生体）
攻撃耐性	攻撃者はログイン画面まで到達できない	攻撃者はログイン画面まで到達できる場合が多い ※
紛失時の対応	当該証明書をセンター側で失効し、新しい端末へ証明書の再発行する	緊急時の代替認証の手順を整備しておく。 物理デバイスの場合は代替機へ交換する。
利用用途	VPN、無線 Wi-Fi、クラウドサービスなど、様々な認証に利用できる	無線 Wi-Fi 認証に利用できないなど、用途が限られる
対応 OS	PKI 技術は実績豊富で信頼性が高く、マルチ OS で動作。	OS 毎に利用可能な認証要素が異なる場合がある

※FIDO2 や PIV スマートカードはフィッシング耐性有

多要素認証の運用は大変？

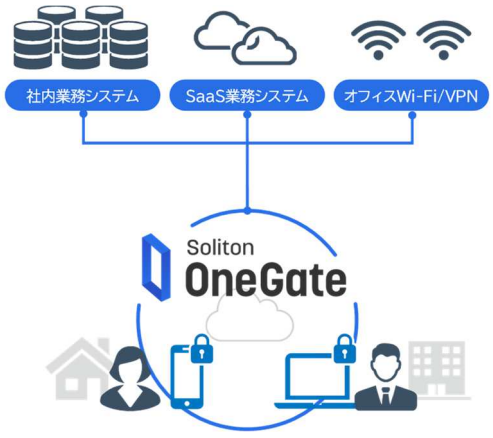
優位性の高いデジタル証明書ですが、CA の導入構築や長期運用を考えるとしり込みされる方もいるかもしれません。プライベート CA を標準搭載したクラウド型の多要素認証サービスなら、導入負荷をかけず、強固な認証環境を簡単に自社に適用することができます。

ソリトンワンゲートなら、デジタル証明書の自動発行と発行済み端末情報の自動記録に対応しています。1 人が複数端末を利用している場合も、利用中の端末を素早く特定し、証明書の失効運用も簡単です。

日本企業のニーズに対応する多要素認証サービス

企業の大切な情報を管理する業務システムを、ID とパスワードだけで利用していたら、第三者にとって、乗っ取りは簡単です。また、会社が許可していない端末が繋がってしまう環境では、情報漏えいリスクは大きく高まります。

OneGate は、**パスワードの脆弱性を解決するデジタル証明書で、利用者と利用端末を特定**し、企業の情報を不正アクセスから守ります。



さいごに

今も引き続き、ランサムウェア攻撃は増加傾向にあり、侵入経路であるリモートアクセスの認証強化は急務といえます。企業・組織への多要素認証（MFA）の導入においては、MFA を突破する攻撃があることも考慮し、フィッシング耐性の強い MFA を採用することが重要です。

高い攻撃耐性に加えて、利用端末の特定ができ、リモートアクセスはもちろんクラウドサービスや無線 Wi-Fi など、さまざまな用途に適用できるデジタル証明書認証はおススメです。

デジタル証明書認証に標準対応する**「ソリトンワンゲート」**サイトでは、導入事例やデモ動画、ご利用用途に応じた各種設定ガイドを公開しています。ぜひ、アクセスしてみて下さい。

Security White Paper 2023

改めて考える、MFA の最適解　- 多要素認証がなぜ突破されているのか？ -

SOGWP2303-A
発行　　2023 年 3 月
発行所　　株式会社ソリトンシステムズ
お問合せ先　　netsales@soliton.co.jp