Microsoft Entra ID証明書認証（CBA）に対応したNRAPKIで実現する認証セキュリティ強化とコスト削減の可能性

2024年8月
日本RA株式会社 営業本部

日本RA株式会社

ID+パスワード認証の危険性

- パスワードは本来自分しか知りえない記憶情報を鍵にするため、認証要素としては優れており、適切に管理し使用する限りは手軽で低コストな認証強度を保った運用ができます
- しかし、これを扱う人間は長く複雑なパスワードは覚えられないこと、セキュリティ意識・モラルの低さから管理が徹底されないこと、加えて、パスワードはネットワークを介して相手に渡す必要があるという点が問題となります
- 8桁以上で定期的に変更するといった、これまでの運用常識は非常識となり、IPAでは「できるだけ長く」「複雑で」「使い回さない」といった3点を安全なパスワードとして桁数の指定をしなくなりました

パスワードが解析されるまでの時間

パスワードの組合せ	桁数				
	6桁	8桁	10桁	12桁	14桁
アルファベット	400ミリ秒	22分	1ヶ月	300年	80万年
アルファベット＋数字	1秒	1時間	7か月	2000年	900万年
アルファベット＋数字＋記号	19秒	2日	52年	40万年	40億年

※上表はパスワード解読時間を調べられるHOW SECURE IS MY PASSWORDというサイト（https://howsecureismypassword.net/）で計測した情報を基に作成しています。
※アルファベットは大文字+小文字を混在させたもので測定しています

※日本の代表的な機関・団体では次のようなパスワードが推奨されています

- 内閣サイバーセキュリティセンター　10桁以上、英数字＋記号の混合
- JPCERT/CC　12桁以上、英数字＋記号

認証の3要素

知識

本人だけが知っていること

「パスワード」、「PIN」、「OTP」、
「暗証番号」、「秘密の質問」など

漏洩リスク

所有

本人だけが持っているもの

「IDカード」、「スマートフォン」、ワン
タイムパスワードの「トークン」など

紛失リスク

生体

本人の身体の一部やそれに
準ずる要素

「指紋」、「声」、「虹彩」など

怪我や身体的特徴の変化により
使えなくなる
プライバシーに関する課題

不正アクセスによる情報漏洩、損失を防止するために強固な認証が必要
2要素以上による多要素認証は基本として、各要素の長所と短所、導入コストとランニングコストなど総合判断がポイント

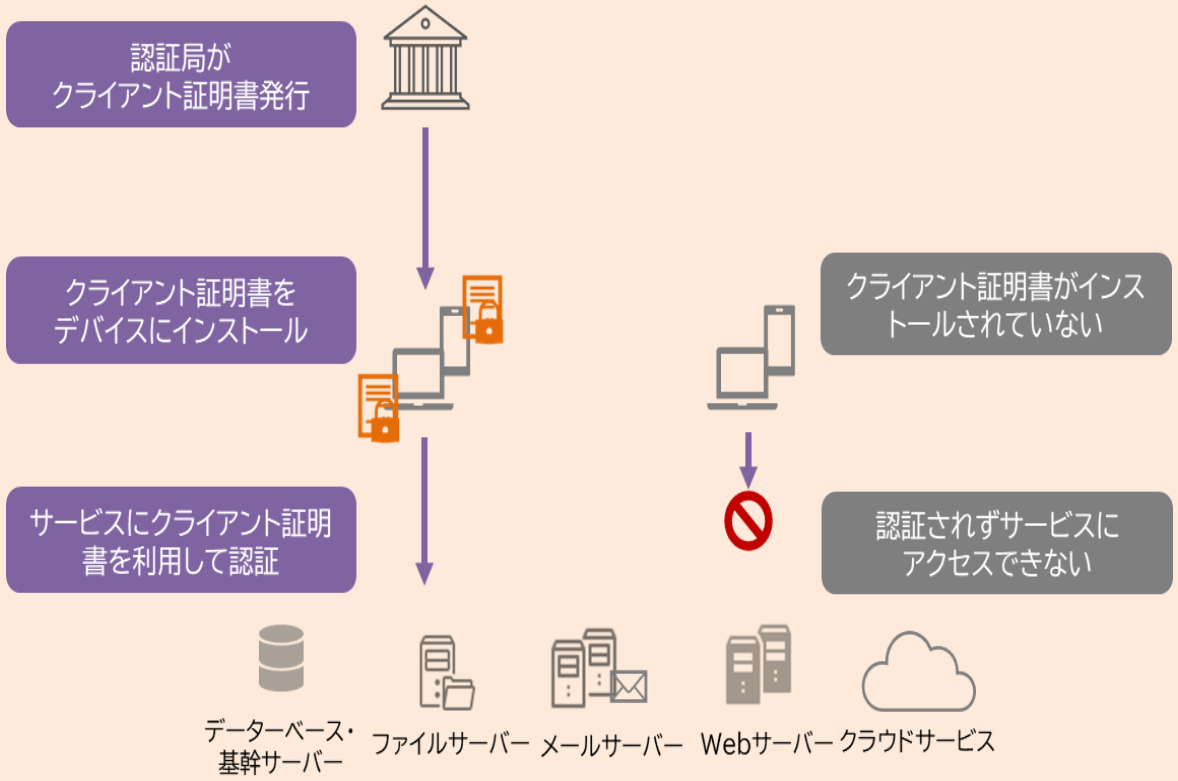
認証方式の選択

参考

方式	ID/PW	PINコード	OTP	ニーモック認証	秘密の質問	CAPTCHA認証	生体認証	リスクベース認証	MACアドレス認証	PKI証明書認証
概略	基本的な認証方式	数桁の数字の組み合わせによる暗証番号	1回ずつしか使用できないように設計された認証方式 ハードウェアトークン（セキュリティトークン）の使用、タイムスタンプ方式、チャレンジ・レスポンス方式、マトリックス認証などがある	文字列の代わりに写真の組み合わせを使った認証方式	あらかじめ決めておいた質問と、その回答による認証で、補助的なもの	画面に「判別しにくい歪んだ文字列の画像」を表示するなどして、コンピューターと人間を識別するためのテスト	指紋、顔、静脈、虹彩、声紋など、本人の身体から得られる生体情報の一部を登録し、認証する方式	普段とは異なる端末やブラウザからアクセスした際に、通常の端末やブラウザにアラートを発信する認証方式	各ネットワークカードが持つ固有のMACアドレスをアクセス制御に利用する認証方式	暗号化と復号で別々の暗号鍵を用いる公開鍵暗号方式を用いた技術や製品のこと
補足	記憶（知識）によるもののため、利用者のリテラシーの影響を受け漏洩リスクが付きまとう	単純で突破されやすい	パスワードにより流出しても再利用できない	ユーザーが写真を登録するため、突破されにくい	ショルダーハッキングなどリスクなしとは言えない	AIによる文字レス解析などにより使われなくなってきた	けがや事故により認証できなくなる可能性	追加のユーザー操作を必要とするアクティブ認証、利用場所を特定できる社内内システムなどではパッシブ認証・SSOでなりすましを抑制できるが、サポート運用側コスト増	MACアドレスの書き換えが容易なことや、MACアドレスの送受信にパケットのヘッダの非暗号化部分が使われるなどの点で、セキュリティ上の難点がある	鍵管理に必要なHSMや運用体制など高額なシステム、運用コストへの投資が必要のため、自営認証局構築は避けたい
認証強度	脆弱	脆弱	やや脆弱	強靭	脆弱	脆弱	強靭	やや脆弱	脆弱	強靭
認証要素	知識	知識	知識・所有	所有	知識	-	生体	所有	所有	所有
耐複製	×	×	×	△	×	-	△	-	×	○
利用汎用性	◎	◎	○	△	△	△	○	△	△	◎

※弊社調べによる一般公開情報の要約になりますので、正確性を保証するものではありませんのでご参考までにご確認ください

クライアント証明書認証



利用者を制限

サービスへのログインをクライアント証明書がインストールされたユーザー・デバイスのみに制限

不正アクセス禁止

企業の管理外デバイスによるサービスの不正利用・アクセスの禁止が可能

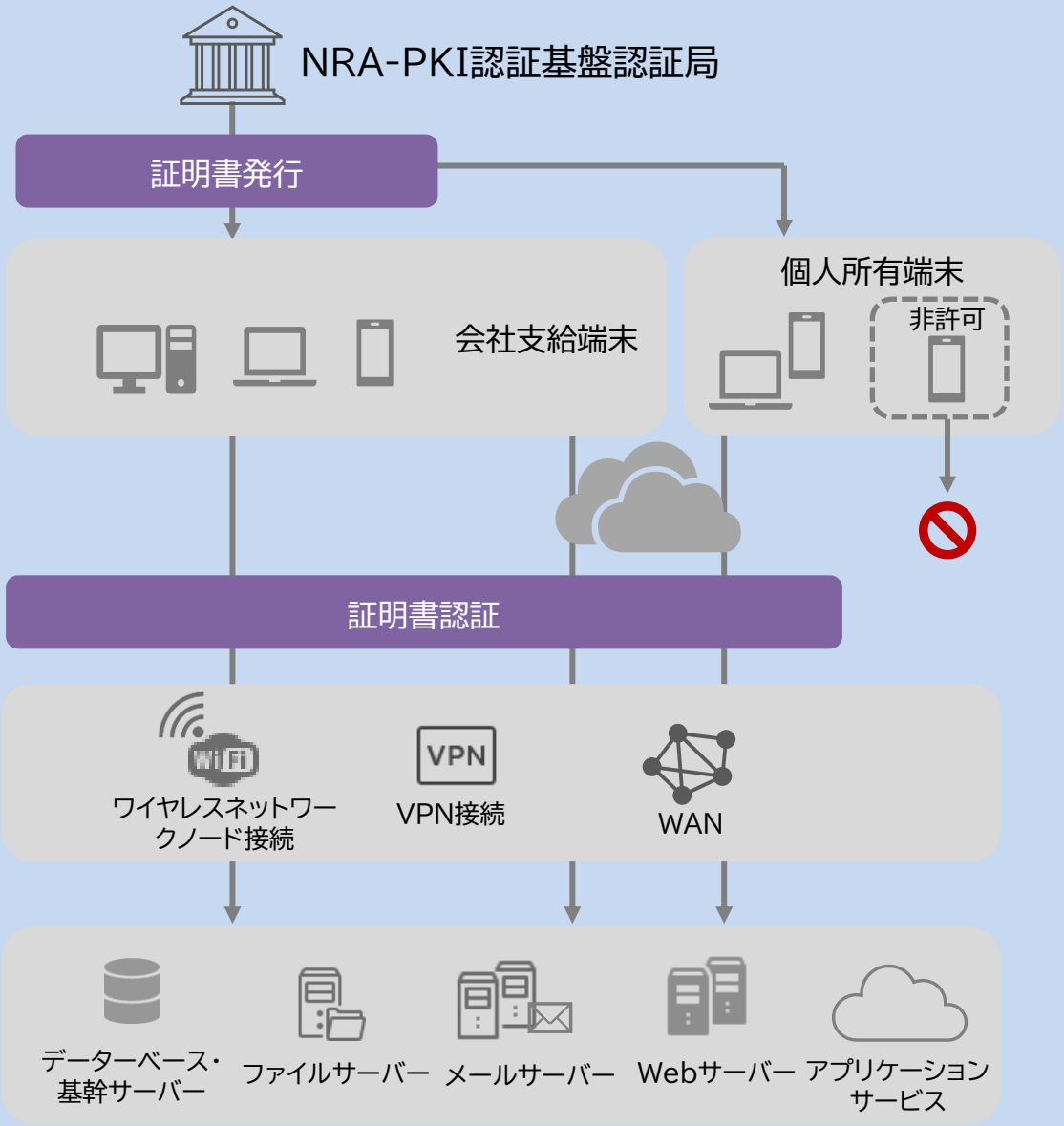
利用者負担が少ない

認証時にはクライアント証明書を選択するだけで認証できるため、他の認証要素と比較して認証時のユーザー操作負荷が低い

厳格な運用に最適

厳密な端末管理が求められるシステム、サービスに有効な認証方法

NRA-PKI統合認証基盤・クライアント証明書



NRA-PKIの特長

証明書の発行・管理を行う必要な機能をSaaSで提供

インハウス型（社内認証局）を構築するには初期投資から、人材育成、規定やシステムの維持管理に膨大なコストがかかります。
長期的見地から会社や事業の成長に合わせて認証局に対する維持と投資が増加し、財務的な負担になる可能性が高くなります。
クラウド型（ホスト型認証局）のように構築済みインフラを活用することで時間とリソースを大幅に節約します。

安全に管理された認証局

耐震措置、電源設備、消火設備、空調、ネットワーク監視、脆弱性チェックなど、安全で高度に管理された環境で運用される認証局により信頼性を維持しています。

コスパの高いライセンスモデル

働き方や利用シーンにより、ひとり n 台の複数端末が使用されることが多くなっています。一般的に電子証明書は利用 1 枚あたりの料金となりますが、NRA-PKIでは利用者あたりユーザーライセンスとしています。1 利用者 1 ライセンスのみの料金※で保有する複数の端末へ証明書をインストールして利用することができ、SaaS型のため初期費用もかかりません。

Web APIを無償公開

NRA-PKIはWebサービスAPIを用意しています。自社サービスのプログラムからAPI経由で電子証明書の発行、失効などの管理を自動化することができます。

※通常の基本販売モデルです。自社サービスの認証にWeb API連携などで組込みをご検討される場合は別途ご相談の上、サービス事業者様向けご提案をさせていただきます。

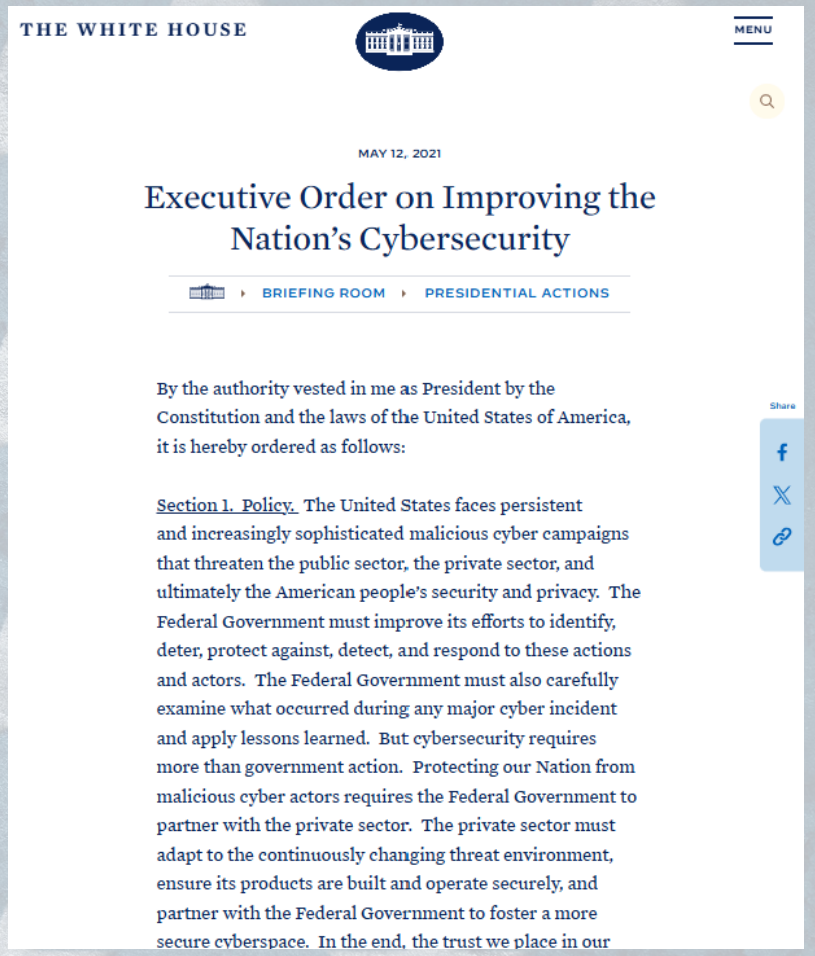
NRAPKIご提供プラン

プラン	スタンダード	ASP
販売形態	販売パートナー、ダイレクト	ダイレクト
単位	ユーザー※1	証明書
必要ライセンス	CA基本利用料(システム/年) クライアント証明書(ユーザー/年)※2	月次ご利用実績に基づく※4
最小購入単位	初回5ライセンス以上※3	設定なし
納品	ご注文受付後3営業日以内	随時※5

※1:利用ユーザー数でご契約いただきます。購入ライセンス上限まで利用ユーザー登録が可能、証明書の発行枚数に制限はありません。
※2:年間ライセンス(使用権)となりますので、実際の電子証明書の有効期間とは異なります。
※3:初回購入は5ライセンス以上とさせていただいておりますが、追加購入は1ライセンスから可能です。また、ライセンス期間中に追加するライセンスは主となるライセンスの終了日に合わせて月額按分でのご購入が可能です(1ヶ月～11ヶ月設定)。
※4:基本は月次利用実績に基づき月額請求となります。ビジネスモデルにあわあせて検討させていただき、個別契約が必要となります。
※5:基本的にWebAPI連携による証明書の発行・失効をシステム的に行っていただくため、事務的な納品作業は発生しません。

サイバーセキュリティに関する大統領令 EO 14028

- 米国サイバーセキュリティに関する大統領令 14028が発令（2022年9月14日）
- 連邦機関および請負業者に対し、ソフトウェア サプライ チェーンのセキュリティを大幅に強化する措置を講じるよう指示されました
- 米国政府機関に限らず、民間部門に取り入れられた事例にはNIST800-161や、SBOMにおける日本政府の取組など影響を与えています


THE WHITE HOUSE

MENU

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our

Share

Microsoftのコミットの一環としてフィッシング耐性の高い認証の機能強化

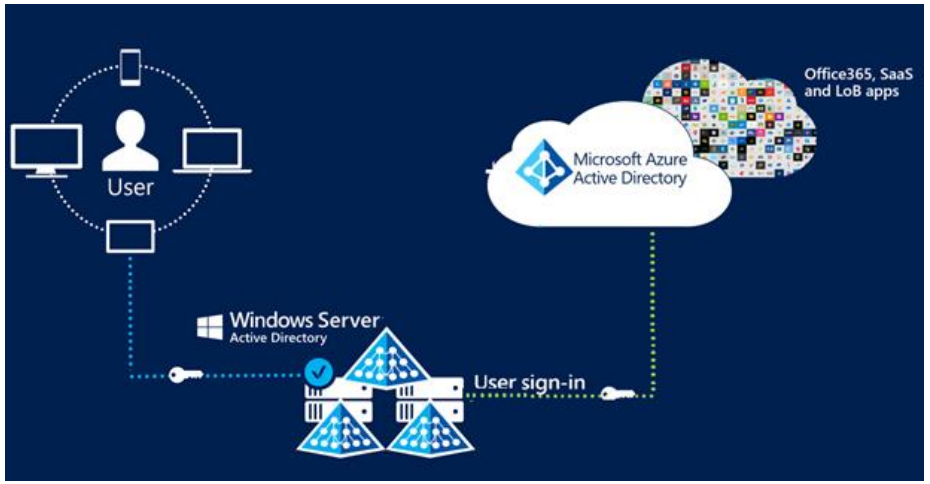
- Microsoft Entra ID 証明書ベース認証 (CBA) の一般提供開始
- 大統領令 14028 要件準拠したい、ADFSのような連携サーバーから Entra ID証明書ベース認証（CBA） に移行したいユーザーニーズへの対応

Microsoft Entra ID証明書ベース認証 (CBA)

- Microsoft Entra ID（旧：Azure AD） の証明書ベース認証 (CBA) を使用すると、アプリケーションやブラウザーのサインイン時に、証明書による認証を直接、許可または要求することが可能
- Microsoft Entra ID で CBA がクラウドでサポートされる前は、顧客はフェデレーションの証明書ベースの認証を実装するために Active Directory Federation Service（ADFS）をデプロイする必要がありましたが、Microsoft Entra ID証明書ベース認証（CBA）を使用すると、Microsoft Entra IDに対して直接認証することができ、ADFS 環境の管理と保守の運用コストが削減され、IT 効率が向上するとしています

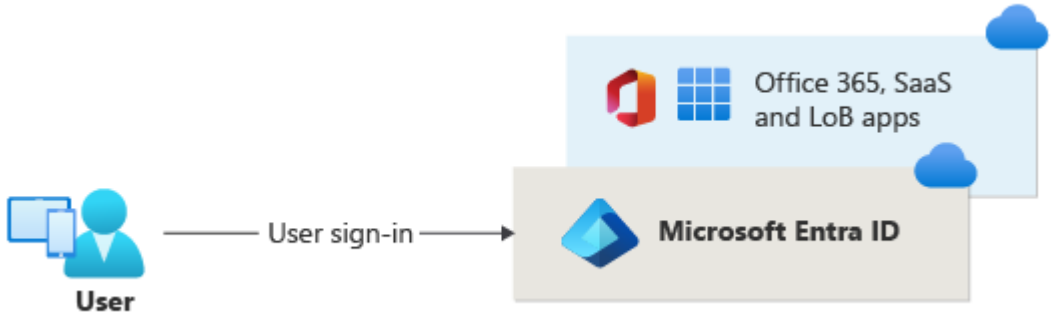
これまでは

ADFSによる証明書ベースの認証



これからは

Microsoft Entra ID 証明書ベースの認証



National Cyber Security Centre

英国の国家サイバーセキュリティセンター（National Cyber Security Centre）は「Office 365を使う場合には、ADFSを使うよりもAzure ADなどのIDaaSを使うほうがセキュリティリスクを低減できる」とのレポートを公表

ADFS利用を廃止しMicrosoft Entra IDへ移行する企業が急増

- 現在のハイブリッド環境 (Active Directory と Azure AD を使用する環境) では、ADFS ではなく Azure AD に対するネイティブ認証を優先することを勧めています
- Azure ADを主要な認証ソースとして使用している組織は、ADFSと比較して実際にリスクを下げるとしており、オンプレミスの ADFS または Active Directory インフラストラクチャで発生する停止やダウンタイムの影響を受けなくなります

AzuerADとADFSのシェア

出典：UK National Cyber Security Centre
https://www.ncsc.gov.uk/blog-post/securing-office-365-with-better-configuration

多要素認証を回避するAiTM攻撃

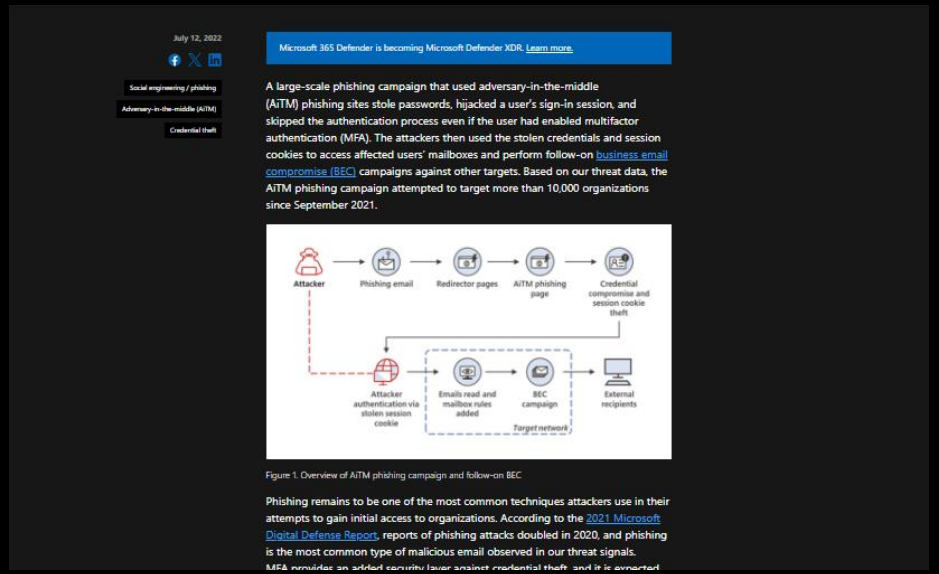
AiTM（Adversary-in-the-Middle）攻撃とは

- 多要素認証を通過した状態のデータ（セッションCookie）を盗み出すフィッシング攻撃
  - 攻撃者が、ユーザーが多要素認証に成功した認証済みのセッションCookieを取得し、Webサイトの多要素認証を回避して正規ユーザーになりすましログインする
- 2021年9月以降、1 万以上の組織が標的に

Microsoftは、**FIDO**（Fast IDentity Online）**v2.0**および**証明書ベースの認証**をサポートするソリューションを使用することが多要素認証のフィッシング耐性をより強固にできるとしています

従来のフィッシング攻撃との違い

従来のフィッシング攻撃は、偽装サイトに入力されたID・パスワードなどの認証情報のみ窃取する手口のため、多要素認証が設定されているサイトであれば、多くの場合は認証を通過できません。一方のAiTM攻撃は、多要素認証に成功した後のログイン状態を保つセッションCookieを取得しますので、多要素認証を設定していても、そもそも認証画面を回避されてしまうこととなり、従来のフィッシング詐欺に比べ、多要素認証を突破される可能性が高いものと言えます

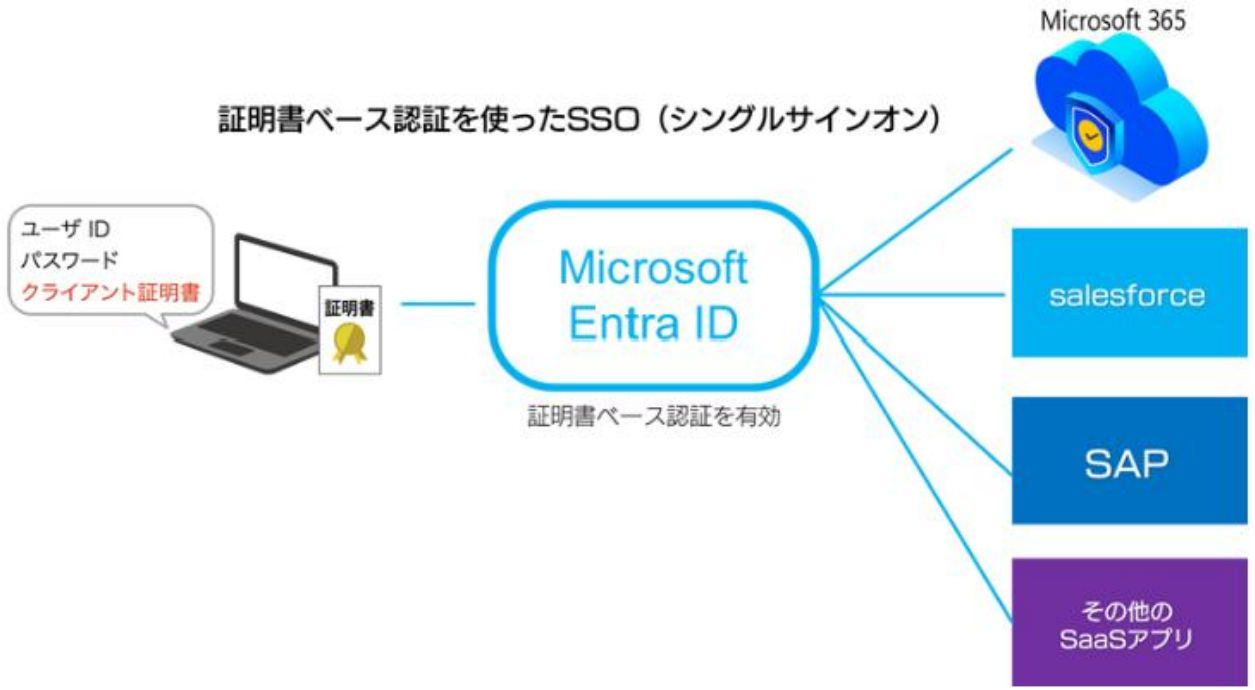


https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

Microsoft Entra ID証明書ベース認証 (CBA)に対応した NRA-PKIクライアント証明書

- NRA-PKIクライアント証明書はEntra ID CBAベータリリース時から実装評価を行い、正式版がリリースされた直後から数多くご採用いただいています
- Entra ID CBAとの連携によって、Microsoft365、クラウドサービスに証明書認証を容易に実装が可能です

- PCと同様にiPhone、Androidなどのスマートデバイスから Microsoft365の証明書ベース認証が利用できる
- Microsoft Entra IDでSSO（シングルサインオン）連携している他社のSaaSサービスでも証明書ベース認証を利用できるので、Microsoft 365以外のクラウドサービスの認証セキュリティも強化することができる
- ADFSを排除して、SaaS型のNRAPKIであれば、すぐにセキュリティと利便性が高い多要素認証へ移行可能
- 標準的なSSO機能があるEntra IDでは、Entra ID CBAは無償のため他のSSO、IDaaSサービス（例：Onelogin、Okta、サテライトオフィス、HENNGEなど）から置き換えることも可能

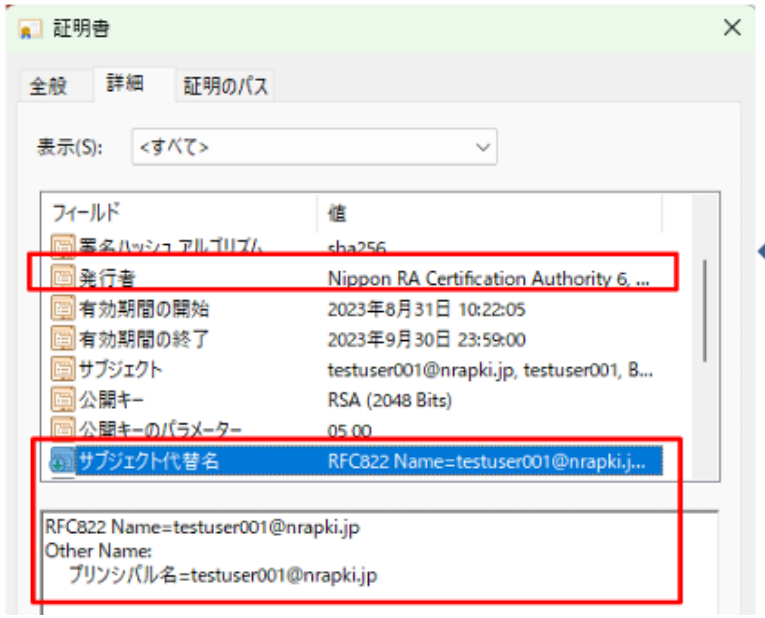


NRA-PKIを使ったMicrosoft Entra ID 証明書認証

参考

- Microsoft Entra ID CBAの仕様

認証時にチェックしているのは以下２つ。
・証明書の発行元（中間CA）
・証明書フィールドのUPN or RFC822Name（Entra IDユーザのユーザープリンシパル名と比較）



証明書のUPNと
RFC822 Nameの値

Entra IDユーザの
ユーザープリンシパル名

NRA

NRA-PKIを使ったMicrosoft Entra ID 証明書認証の設定

参考

NRA-PKI認証局証明書登録

Microsoft Entra ID 証明書ベース認証設定

1 Microsoft Entra 管理センターメニューより「認証方法」の設定へ

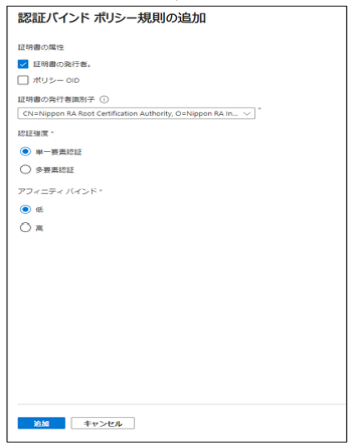
2 「認証方法 | ポリシー」から「証明書ベースの認証」を選択

3 「有効化およびターゲット」より「証明書ベースの認証」を有効にする

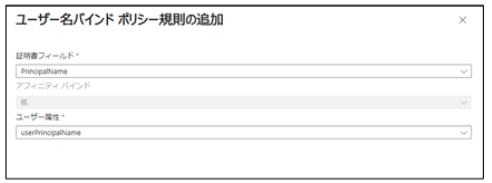
4 「証明書ベースの認証」の設定項目を設定する

本手順書は単一要素認証の設定例です。
多要素認証をご利用の際は、別の認証要素の追加設定が必要となるため、画面内の「詳細情報」から詳細をご確認ください。

「構成」より、「認証バインド」の構成情報を指定
（ここではNRA-PKI単一認証を選択）



「ユーザー名バインド」を設定



「規則の追加」から、「ユーザー名バインドポリシー規則の追加」画面より「証明書フィールド」に「PrincipalName」、「ユーザー属性」に「userPrincipalName」を選択し追加

再度「規則の追加」から、「ユーザー名バインドポリシー規則の追加」画面より「証明書フィールド」に「RFC822Name」、「ユーザー属性」に「userPrincipalName」を選択し追加

「規則の追加」より認証を許可する認証局（NRA-PKI認証局）を設定
※NRA-PKI認証局証明書登録でアップロードした次の２つの認証局（ルート・中間）証明書を設定

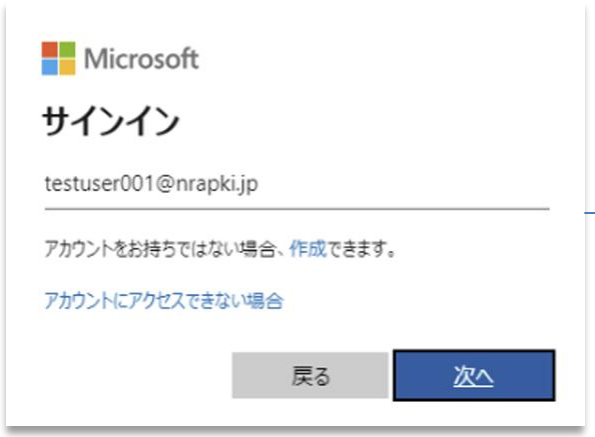
詳細は弊社サポート情報「Microsoft Entra CBA 用サービス向けマニュアル」をご覧ください
https://www.nrapki.jp/support/?p=1574

NRA

NRA-PKIを使ったMicrosoft Entra ID 証明書認証イメージ

参考

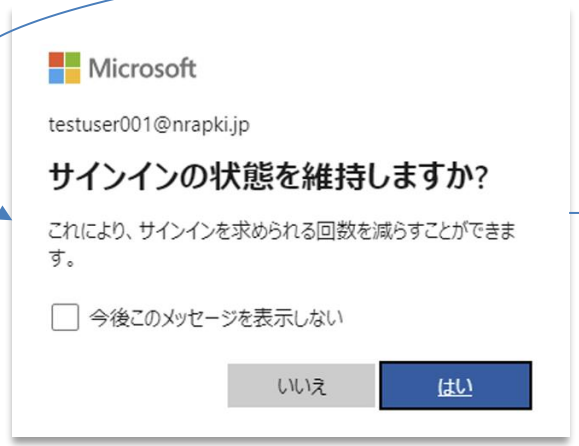
「サインイン」画面でアカウントを入力

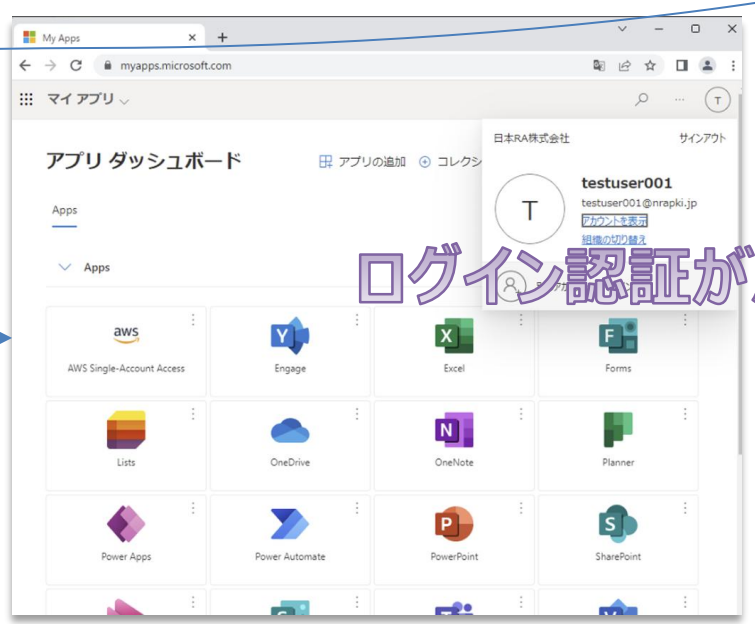


「パスワードの入力」画面で「証明書または
スマートカードを使用するを選択

デバイスにインストールされている
適切なクライアント証明書を選択

「サインインの状態を維持しますか？」画面が表示された場合は、
「はい」もしくは「いいえ」のどちらかを選択





ログイン認証が成功

NRA

NRA-PKIを使ったEntra ID 証明書認証

参考

【Microsoft Entra IDの仕様上の注意事項】

- ID/Password認証は常に有効になります
  - 単一要素認証で証明書認証を有効にしてもID/Password認証は常に有効になっています。
  - 証明書のみの認証を許可する場合は、管理者が利用者が知らないパスワードを付与してID/Password認証できなくする必要があります
- 失効リストの取得は失効リストの有効期間に依存します（１週間）
  - 失効リストの取得（更新）周期は、Microsoft Entra IDで設定できません。失効リストの有効期間が切れた時に再取得されます（NRA-PKIの失効リスト有効期間は１週間）
  - したがって、端末の紛失等でログインできなくする場合は、証明書を失効するのではなく、Microsoft Entra IDのアカウント自体を無効にする運用が必要になります

NRA