IBM i 2025

IBM i コンテンツ (2025年9月版)

IBM i 統合 MFA (Multi-Factor Authentication/多要素認証) によるセキュリティ強化

日本アイ・ビー・エム株式会社
テクノロジー事業本部
IBM Powerテクニカルセールス

© IBM 2025

IBM i 統合 MFA (Multi-Factor Authentication/多要素認証)によるセキュリティ強化

IBM i 7.6で新しいセキュリティ機能として IBM i 統合MFA が登場しました。
この資料では、IBM i 7.6で無償で利用可能なIBM i 統合MFAの概要・設定方法などをご紹介します。

目次

© IBM 2025

1. 多要素認証機能とは (1/2)

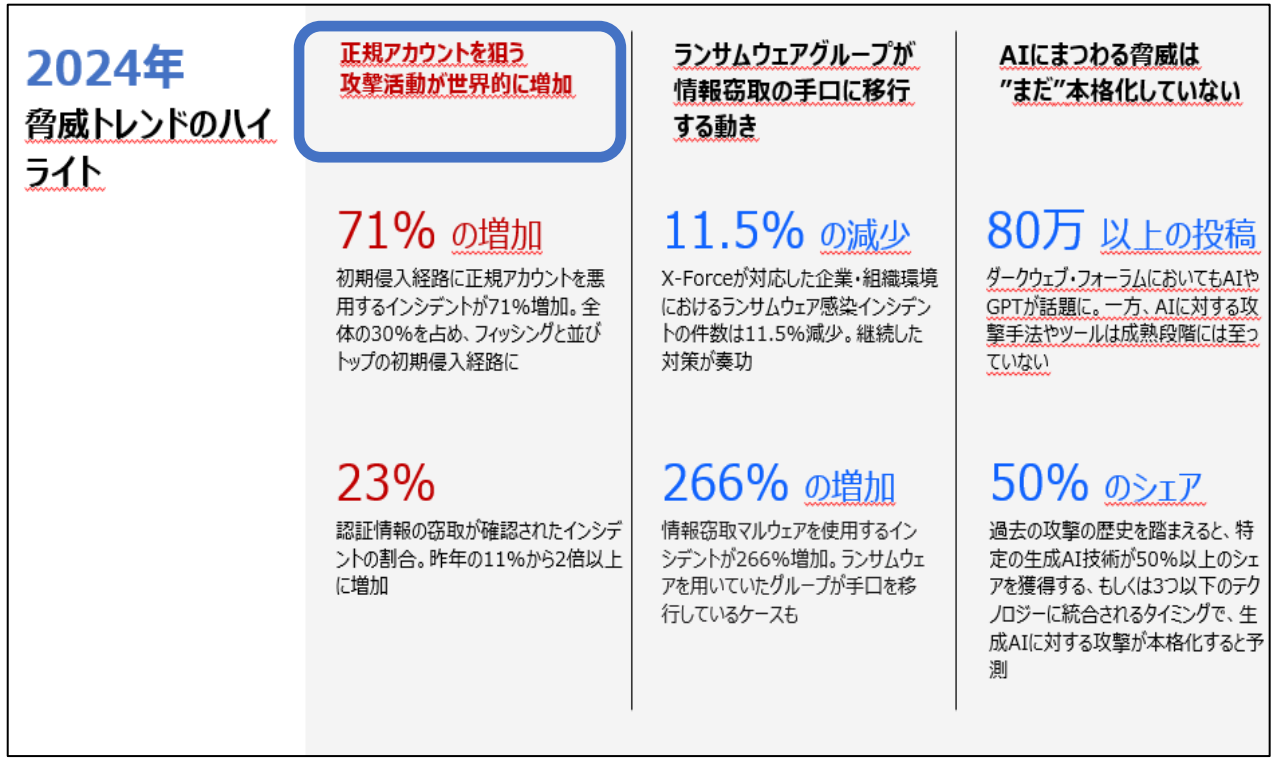
多要素認証機能が注目されている理由

- ランサムウェアなどの外部攻撃や内部不正等による情報漏洩リスクが増加傾向にあります。

- 上記の対策として今、**多要素認証(Multi-Factor Authentication：MFA)**が注目されています。

身近なところでの「多要素認証」の例：

✓証券・銀行アプリでの「ワンタイム・パスワード」
✓オンラインクレジットカード決済での「ワンタイム・パスワード」



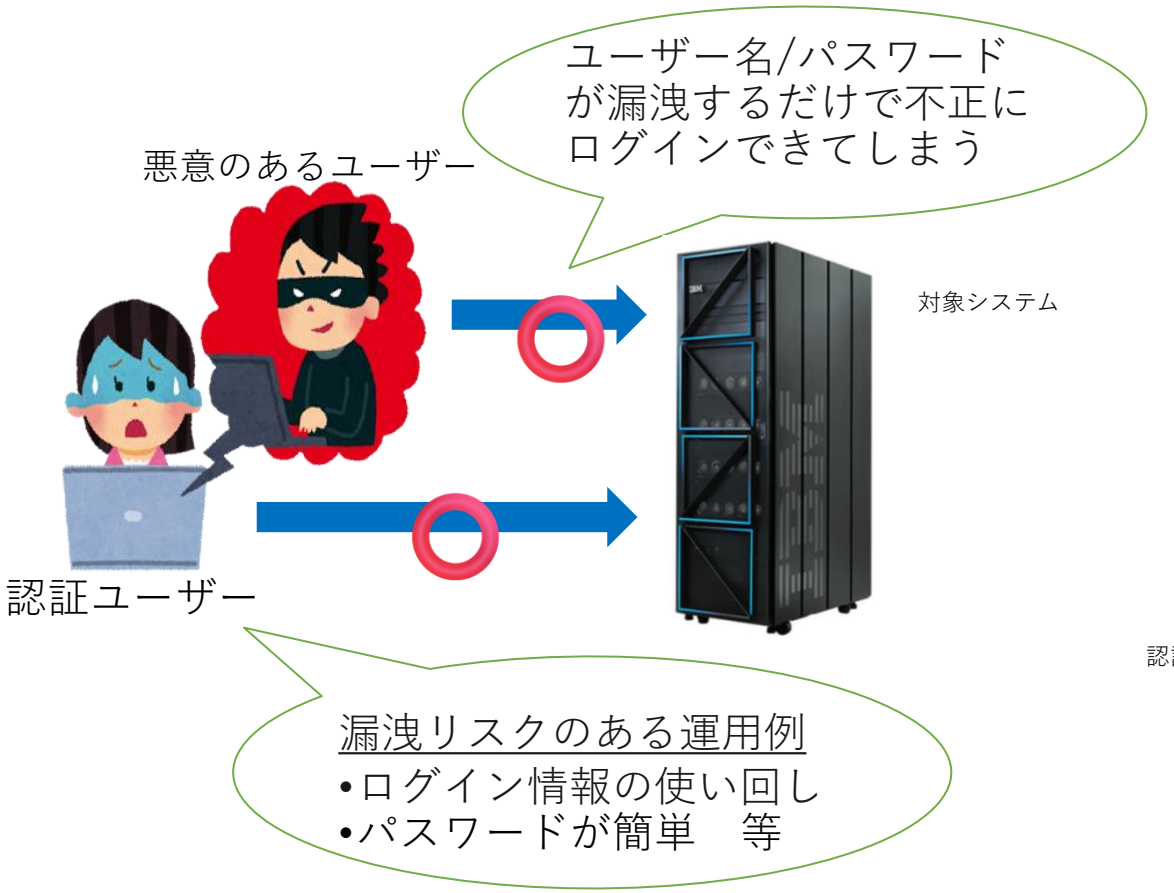
IBM：https://www.ibm.com/jp-ja/reports/data-breach

© IBM 2025

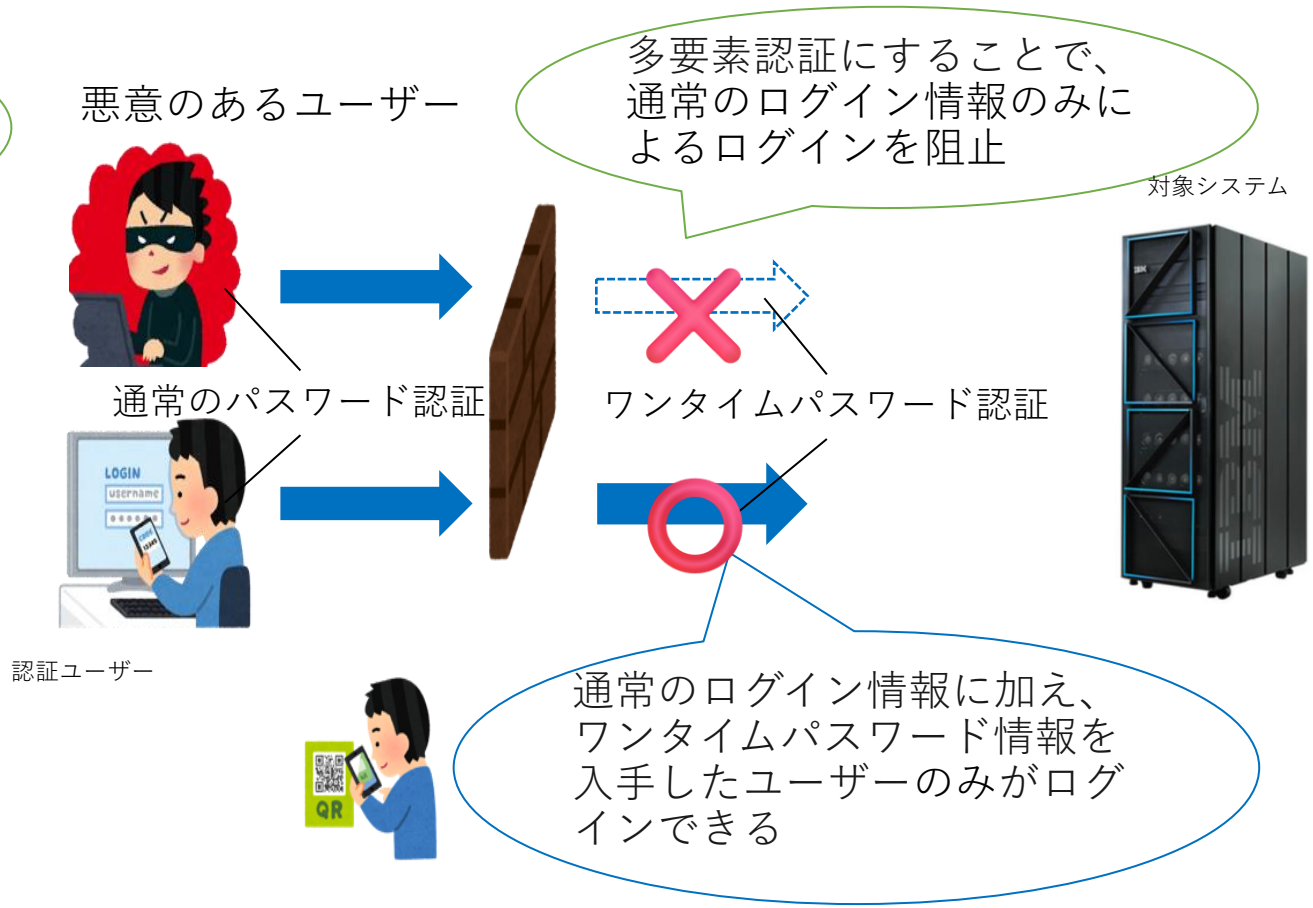
1. 多要素認証機能とは (2/2)

もしOSログインに多要素認証を実装しないと・・

多要素認証がない場合のログイン例



多要素認証を実装した場合のログイン例



© IBM 2025

2. IBM i 統合 MFA 概説 (1/3)

IBM i に統合されたMFA (多要素認証) ソリューション
- IBM i 7.6で無償で利用可能
- 1つのIBM i OSで完結して、パスワードと追加の要素認証が可能
- IBM i に追加の有償ソフトウェア等は不要
  - 業界のさまざまな TOTP クライアント認証システムとの互換性あり
  - ユーザー側でのTOTPトークン生成・認証S/W, H/W等は別途必要

多要素認証は最も効果的な
ランサムウェア対策の1つです

IBM i 統合MFAは
IBM i 7.6以降でサポート

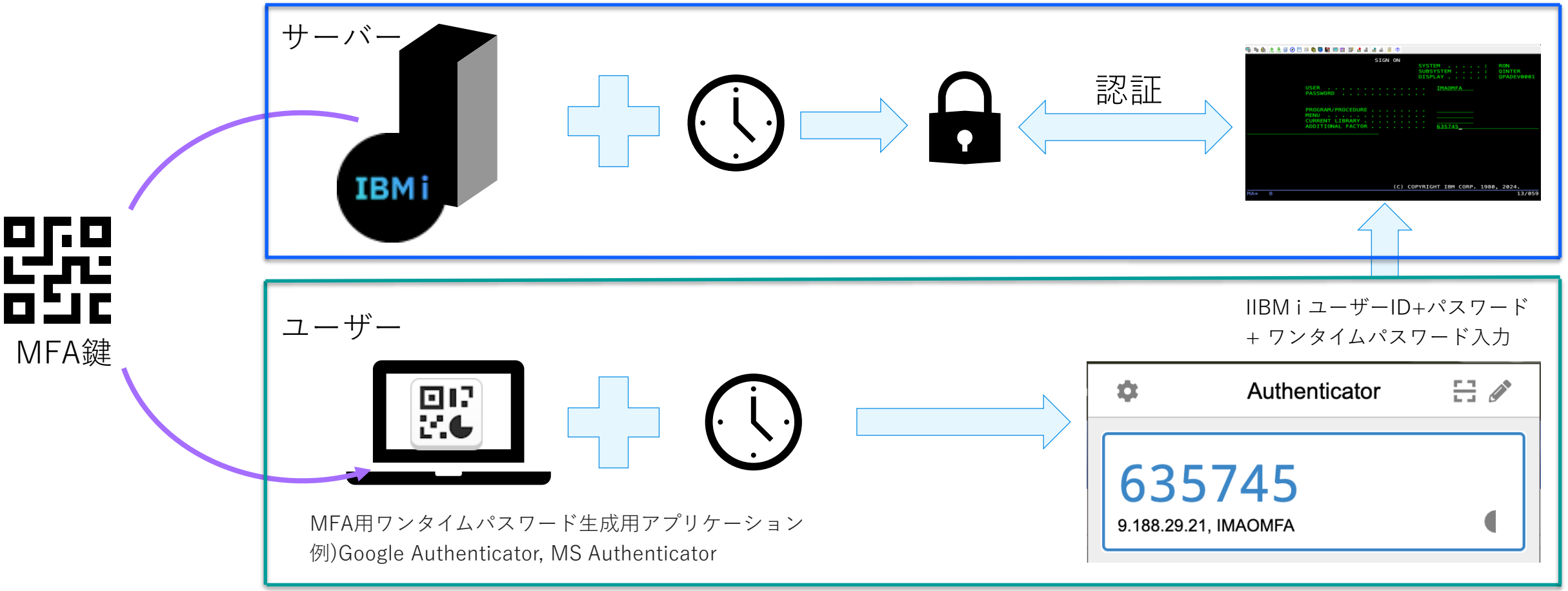
- ユーザープロファイルごとにMFA要否をパラメーターで指定
- 5250端末をはじめ、ユーザーからのあらゆるIBM i へのアクセスに対してMFAを設定可能
  - Access Client Solutions (ACS)
  - Navigator for i
  - FTPはじめ標準的なインターフェース、IBM i 独自のインターフェース

IBM i 統合 MFA (多要素認証)に関する情報
参照：多要素認証 (MFA)
https://www.ibm.com/docs/ja/i/7.6.0?topic=security-multi-factor-authentication-mfa

© IBM 2025

2. IBM i 統合 MFA 概説 (2/3)

MFA(多要素認証)はIDとパスワード以外に追加の認証要素が必要な強化された認証方式
TOTP(Time-based One-Time Password)は時刻ベースで生成したワンタイムパスワードを追加認証に使用
IBM i で生成したMFA鍵を多要素認証用のクライアント側のアプリケーションに登録してワンタイム・パスワードを生成してIBM i にログイン



© IBM 2025

2. IBM i 統合 MFA 概説 (3/3)

ユーザーのMFAによるサインオンの例

- ユーザーIDとパスワードを入力
- MFA（TOTP）パスコードを確認して ADDITIONAL FACTORに入力

- 認証され、メインメニューを表示

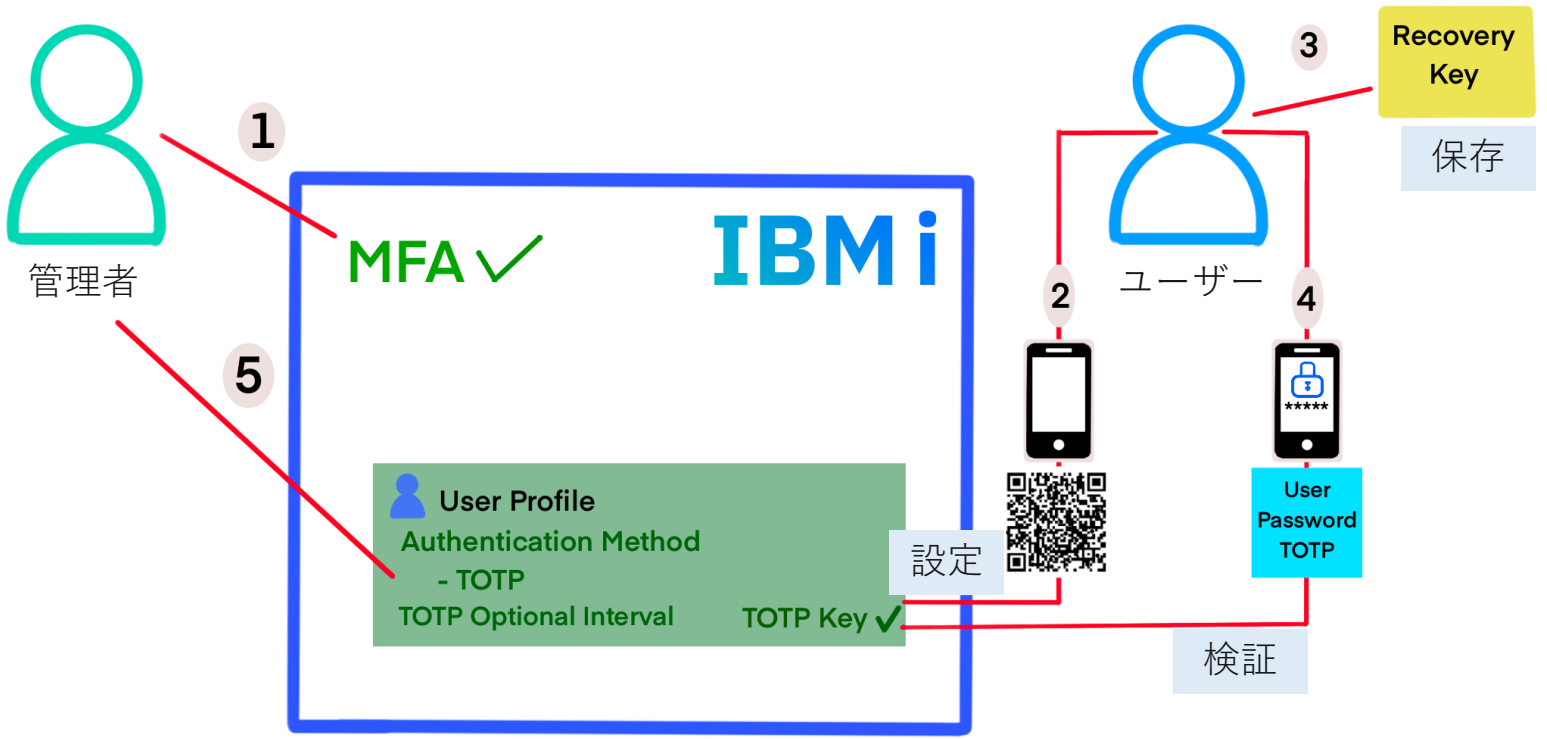
```
                              サインオン
                                                  システム . . . . . :
                                                  サブシステム . . . :
                                                  表示装置 . . . . . :

ユーザー . . . . . . . . . . . . . . ___________
パスワード . . . . . .

プログラム／プロシージャー . . . . . __________
メニュー . . . . . .
現行ライブラリー . . . . . __________
追加係数 . . . . . 996192_

MAIN                          IBM I メインメニュー
                                                  システム :   C70ADE21
次の 1 つを選択してください。

     1. ユーザー・タスク
     2. オフィス・タスク

     4. ファイル，ライブラリー，およびフォルダー

     6. 通信

     8. 問題処理
     9. メニューの表示
    10. 情報援助オプション
    11. IBM I ACCESS のタスク

    90. サインオフ

選択項目またはコマンド
===> _

F3= 終了    F4=ﾌﾟﾛﾝﾌﾟﾄ    F9=ｺﾏﾝﾄﾞ の複写    F12= 取り消し    F13= 情報援助
F23= 初期 ﾒﾆｭｰ の設定
(C) COPYRIGHT IBM CORP. 1980, 2024.
MA*   A                                          20/007
```

© IBM 2025

3. IBM i 統合 MFA を使ってみよう

1. 設定フロー概要

IBM i 統合 MFA を設定するには、追加のサインオン要素セキュリティ属性を有効にする必要があります
有効にすると、特定のユーザープロファイルを変更し、認証時に追加要素の入力を求めることができます
この資料では、TOTPを使用する設定方法をご紹介します。



参照：IBM Documentation システムにMFAを設定する

© IBM 2025

解説

管理者：
ステップ1
- TOTP認証方式を有効にするには、追加のサインオン要素セキュリティ属性を有効にする
  1. 前提要件のシステム要件が満たされていることを確認する
  2. 追加のサインオン要素セキュリティ属性を有効に設定にする
  3. (Option) サインオン画面をカスタマイズしている場合は、変更を行う
  4. IPLを行い、追加のサインオン要素セキュリティ属性を有効にする
  5. (Option) デバイスの時刻を同期するためのネットワークタイムプロトコル（NTP）クライアントを設定する
  6. ユーザーに、TOTP キーを設定する必要があることを通知する

ユーザー：
ステップ 2
- TOTPキーを設定する

ステップ 3
- リカバリーキーを安全な場所に保存する。 リカバリ・キーは、TOTPキーを設定したときに生成される

ステップ 4
- TOTPキーを多要素認証用のクライアント側のアプリケーションに入力し、検証する
- TOTPキーが設定されたことを管理者に通知する

管理者：
ステップ 5
TOTP認証方式を有効にする
- ユーザーがTOTPキーを設定しているかどうかを確認する
- ユーザーのTOTPキーが設定されている場合、ユーザープロファイルを変更して、認証方法に*TOTPを含めるように設定し、希望するTOTPオプション間隔を設定する

© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

管理者：

ステップ1

- TOTP認証方式を有効にするには、追加のサインオン要素セキュリティ属性を有効にする
  1. **前提要件のシステム要件が満たされていることを確認する**

     前提要件：

     セキュリティ・レベル(機密保護レベル) 40 または 50

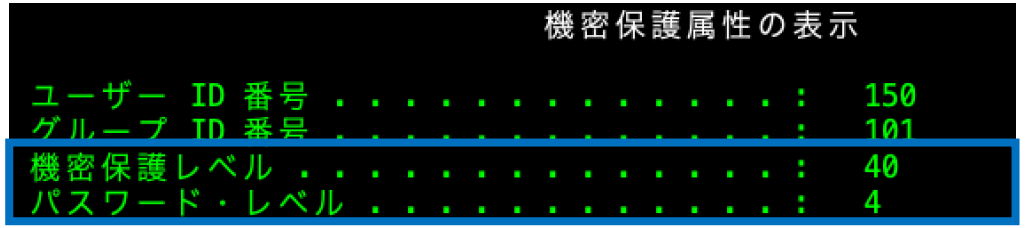
     パスワード・レベル　4

現在のセキュリティ・レベルと現在のパスワード・レベルを確認する方法

5250エミュレーターを使う場合

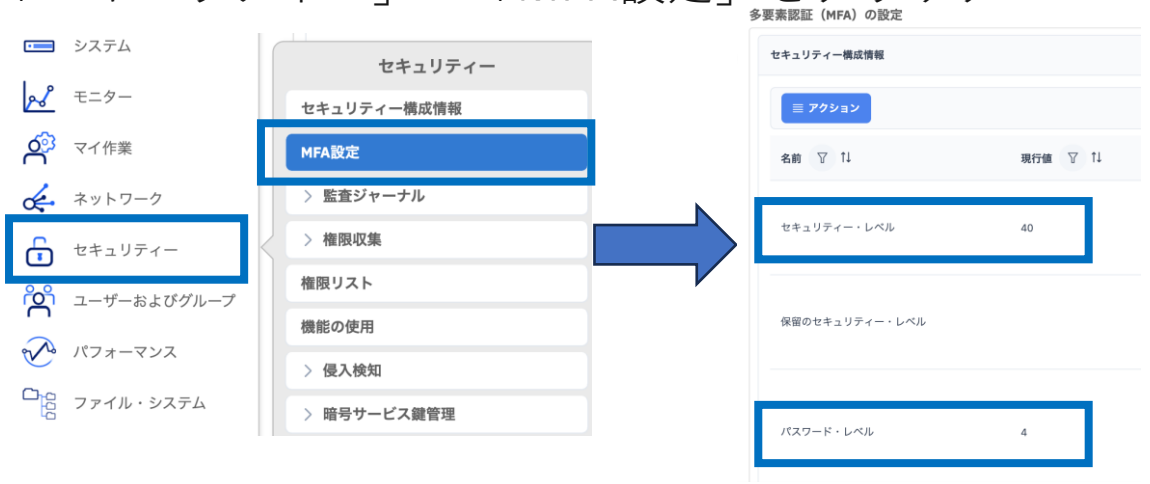
DSPSECAコマンド を実行

(機密保護属性の表示)



Navigator for i を使う場合

「セキュリティー」→「MFA設定」をクリック



© IBM 2025

解説

1. 前提要件のシステム要件が満たされていることを確認する
   - 前提要件：セキュリティ・レベル(機密保護レベル)は40以上、パスワード・レベルは4でなければならない。
   - 現在のセキュリティ・レベル(機密保護レベル)と現在のパスワード・レベルを表示する方法：
   - 5250エミュレーターでコマンドで表示する方法とIBM Navigator for i のメニューから表示する方法の2つがある。
     - 5250エミュレータで、セキュリティ属性を表示する（DSPSECA）コマンドを実行
     - IBM Navigator for i で、 「セキュリティ」→「MFA設定」を展開

- セキュリティ・レベル(機密保護レベル)を変更する必要がある場合は、「 システム・セキュリティ（QSECURITY）のシステム値の使用 」を参照して、変更した場合の影響を確認してください。

- パスワード・レベルを変更する必要がある場合は、「 パスワード・レベルの変更の計画 」を参照して、変更した場合の影響を確認してください。

© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

管理者：

ステップ1

- TOTP認証方式を有効にするには、追加のサインオン要素セキュリティ属性を有効にする

2. 追加のサインオン要素セキュリティ属性を有効に設定する

追加のサインオン要素セキュリティ属性を有効に変更する方法

5250エミュレーターを使う場合

CHGSECA コマンド で 追加のサインオン要素(ADLSGNFAC)パラメータを *ENABLEDに変更

コマンド：

CHGSECA ADLSGNFAC(*ENABLED)

Navigator for i を使う場合

「セキュリティー」→「MFA設定」をクリック

「追加サインオン・ファクタ」を右クリックし、「変更」を選択。「使用可能」を選択し、「保管」をクリック

© IBM 2025

解説

2. 追加のサインオン要素セキュリティ属性を有効に設定する
   - 現行の設定を確認したい場合は、セキュリティ・レベル(機密保護レベル)とパスワード・レベルの確認と同じ下記方法で確認する
   - 現在の追加のサインオン要素セキュリティ属性を表示する方法：
   - 5250エミュレーターでコマンドで表示する方法とIBM Navigator for i のメニューから表示する方法の2つがある
     - 5250エミュレーターで、セキュリティ属性を表示する（DSPSECA）コマンドを実行
     - IBM Navigator for i で、「セキュリティ」→「MFA設定」を展開
   - 追加のサインオン要素セキュリティ属性が有効(*ENABLED)になっていない場合は、追加のサインオン要素セキュリティ属性を変更する
   - 追加のサインオン要素セキュリティ属性を有効に設定する方法：
   - 5250エミュレーターでコマンドで表示する方法とIBM Navigator for i のメニューから表示する方法の2つがある
     - 5250エミュレーターで、機密保護属性の変更 (CHGSECA)コマンドを実行
       - CHGSECA ADLSGNFAC(*ENABLED)
     - IBM Navigator for i で、「セキュリティ」→「MFA設定」を展開。「追加サインオン・ファクタ」を右クリックし、「変更」を選択。「使用可能」を選択し、「保管」をクリック。

© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

管理者：

ステップ1

（補足）追加のサインオン要素セキュリティ属性の変更が許可されていない場合の対応

SSTセキュリティ属性の変更（CHGSSTSECA）コマンドを使用して、追加サインオン要素の変更（CHGADLSGN）パラメータを*YESに設定し、変更を許可する

- 変更には、SSTユーザーID(保守ツールID)とパスワードの入力が必要。変更の機能特権を持ったSSTユーザーIDを確認の上、下記の例のようにCHGSSTSECAコマンドで変更する

コマンド例：

- **CHGSSTSECA REQUSRID(SSTUSR) REQPWD(dfkjaie*_578222) CHGADLSGN(*YES)**

再度、CHGSECA ADLSGNFAC(*ENABLED) コマンドを実行し、追加のサインオン要素セキュリティ属性を有効にする。

追加サインオン要素セキュリティ属性を有効に設定した後に、その変更を禁止するには、 SSTセキュリティ属性の変更（CHGSSTSECA）コマンドを使用して、追加サインオン要素の変更（CHGADLSGN）パラメータを*NOに設定する。

コマンド例：

- **CHGSSTSECA REQUSRID(SSTUSR) REQPWD(dfkjaie*_578222) CHGADLSGN(*NO)**

© IBM 2025

解説

- （補足）追加のサインオン要素セキュリティ属性の変更が許可されていない場合の対応
SSTセキュリティ属性の変更（CHGSSTSECA）コマンドを使用して、追加サインオン要素の変更（CHGADLSGN）パラメータを*YESに設定し、変更を許可する。

- 変更には、SSTユーザーID(保守ツール・ユーザーID)とパスワードの入力が必要
- ご参考リンク：
  - 保守ツール・ユーザー ID
  - https://www.ibm.com/docs/ja/i/7.6.0?topic=concepts-service-tools-user-ids
  - 保守ツールの概念
  - https://www.ibm.com/docs/ja/i/7.6.0?topic=tools-service-concepts
- 変更の機能特権を持ったSSTユーザーIDを確認の上、下記の例のようにCHGSSTSECAコマンドで変更する

コマンド例：
- CHGSSTSECA REQUSRID(SSTUSR) REQPWD(dfkjaie*_578222) CHGADLSGN(*YES)

再度、CHGSECA ADLSGNFAC(*ENABLED) コマンドを実行し、追加のサインオン要素セキュリティ属性を有効にする

追加サインオン要素セキュリティ属性を有効に設定した後に、その変更を禁止するには、 SSTセキュリティ属性の変更（CHGSSTSECA）コマンドを使用して、追加サインオン要素の変更（CHGADLSGN）パラメータを*NOに設定する

コマンド例：
- CHGSSTSECA REQUSRID(SSTUSR) REQPWD(dfkjaie*_578222) CHGADLSGN(*NO)

© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

管理者：

ステップ1

- TOTP認証方式を有効にするには、追加のサインオン要素セキュリティ属性を有効にする

3.（Option）サインオン画面をカスタマイズしている場合は、変更を行う

- カスタマイズされたサインオン画面がある場合は、IPLの前にサインオン表示画面ファイルのソース・コードを変更して、画面表示を変更する
- 詳細については、下記を参照
  - サインオン画面表示の変更
  - https://www.ibm.com/docs/ja/i/7.6.0?topic=file-changing-signon-screen-display
  - サインオン・ディスプレイ・ファイルの作成
  - https://www.ibm.com/docs/ja/i/7.6.0?topic=description-creating-sign-display-file

© IBM 2025

3.IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

管理者：

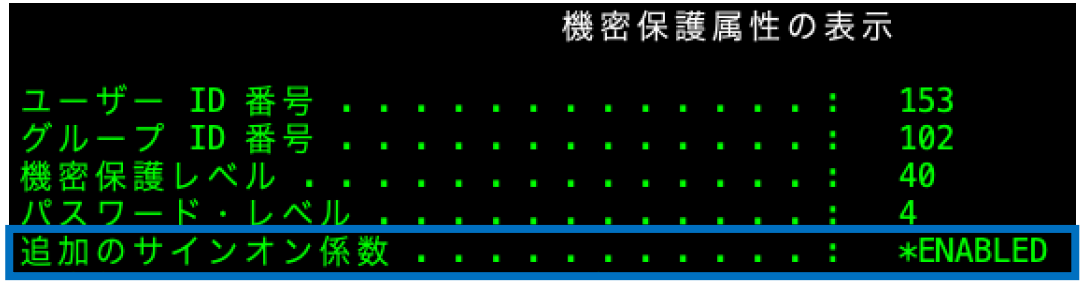
ステップ1

4. **IPLを行い、追加のサインオン要素セキュリティ属性を有効にする**
   - 追加のサインオン要素セキュリティ属性を*DISABLEDから*ENABLEDに変更した場合、有効になるようにシステムをIPLする
5. **(Option) デバイスの時刻を同期するためのネットワークタイムプロトコル（NTP）クライアントを設定する**
   - TOTP認証方式では、サーバーの時間がクライアントの認証デバイスと同期している必要がある
   - TOTPアルゴリズムでは、わずかな時間のずれは許容される
   - サーバーとデバイスのクロックを同期させるには、NTP（Network Time Protocol）クライアントの使用が推奨されている
   - システム値 QTIMADJ が QIBM_OS400_NTP に設定されている場合は、 NTP クライアントは実行中である
   - *NONE に設定されている場合は、NTP クライアントは実行されていない
   - コマンド **STRTCPSVR SERVER(*NTP)** を使用して NTP サービスを始動
     詳細はネットワークタイムプロトコル（NTP）による時刻同期を参照

© IBM 2025

解説(1/3)

4. IPLを行い、追加のサインオン要素セキュリティ属性を有効にする
   - 追加のサインオン要素セキュリティ属性を*DISABLEDから*ENABLEDに変更した場合、有効にするためにシステムをIPLする
   - IPLはシステムの停止と開始が必要である
     - システムを停止する時にはすべてのバッチ・ジョブが完了し、すべてのユーザーがシステムからサインオフしていることなどを確認し、データを損傷したり、システムが予期しない動作をしないように注意する必要がある
     - 詳細はシステムの開始と停止を参照ください
   - IPL後、追加のサインオン要素セキュリティ属性が有効になっているか確認する場合は、セキュリティ・レベル(機密保護レベル)とパスワード・レベルの確認と同じ下記方法で確認する
     - 5250エミュレーターでコマンドで表示する方法とIBM Navigator for i のメニューから表示する方法の2つがある。
       - 5250エミュレータで、セキュリティ属性を表示する（DSPSECA）コマンドを実行
       - IBM Navigator for i で、 「セキュリティ」→「MFA設定」を展開



© IBM 2025

解説(2/3)

4. IPLを行い、追加のサインオン要素セキュリティ属性を有効にする
    - 追加のサインオン要素セキュリティ属性を有効にするとサインオン画面が英語表示となる
    - 2025年9月に下記PTFが提供され、PTFの適用によりサインオン画面の日本語表示が可能
        - 2930用 PTF SJ07037
        - 2962用 PTF SJ07051
        - その他言語用のPTF番号は下記を参照
            - Known Issue: DT447953
            - https://www.ibm.com/mysupport/s/defect/aCIgJ00000049EPWAY/dt447953?language=ja

© IBM 2025

解説(3/3)

5. (Option) デバイスの時刻を同期するためのネットワークタイムプロトコル（NTP）クライアントを設定する
   - TOTP認証方式では、サーバーの時間がクライアントの認証デバイスと同期している必要がある
   - TOTPアルゴリズムでは、わずかな時間のずれは許容される
   - サーバーとデバイスのクロックを同期させるには、NTP（Network Time Protocol）クライアントの使用が推奨されている
   - 時刻が大きくずれている場合、NTP クライアントの設定により大きく時刻が変更され、ジョブの実行順序やログに影響が出る可能性があるため、注意が必要である。また、時刻が大きくずれている場合には、NTPサービスによる自動的な時刻同期の修正ができない場合がある。その場合には、システム値 QTIME や QDATETIME で時刻設定をした上で、NTPサービスの起動を実施してください。
   - 現在設定されている時刻は下記コマンドで確認できる
     - **DSPSYSVAL SYSVAL(QDATETIME)**
   - システム値 QTIMADJ が QIBM_OS400_NTP に設定されている場合は、 NTP クライアントは実行中である
   - *NONE に設定されている場合は、NTP クライアントは実行されていない
   - NTP サービスが起動していたら、コマンド **ENDTCPSVR SERVER(*NTP)** を使用して停止する
   - NTP 設定のため、コマンド CHGNTPA を使用し、下記の例のようにNTPサーバーを設定する
     - **CHGNTPA RMTSYS('**(NTPサーバーのアドレス)**') ACTLOG(*POLL)**
       - * ACTLOG(*POLL) はログファイルを出力するための設定
   - コマンド **STRTCPSVR SERVER(*NTP)** を使用して NTP サービスを始動する

詳細はネットワークタイムプロトコル（NTP）による時刻同期を参照ください

© IBM 2025

3. IBM i 統合 MFA を使ってみよう

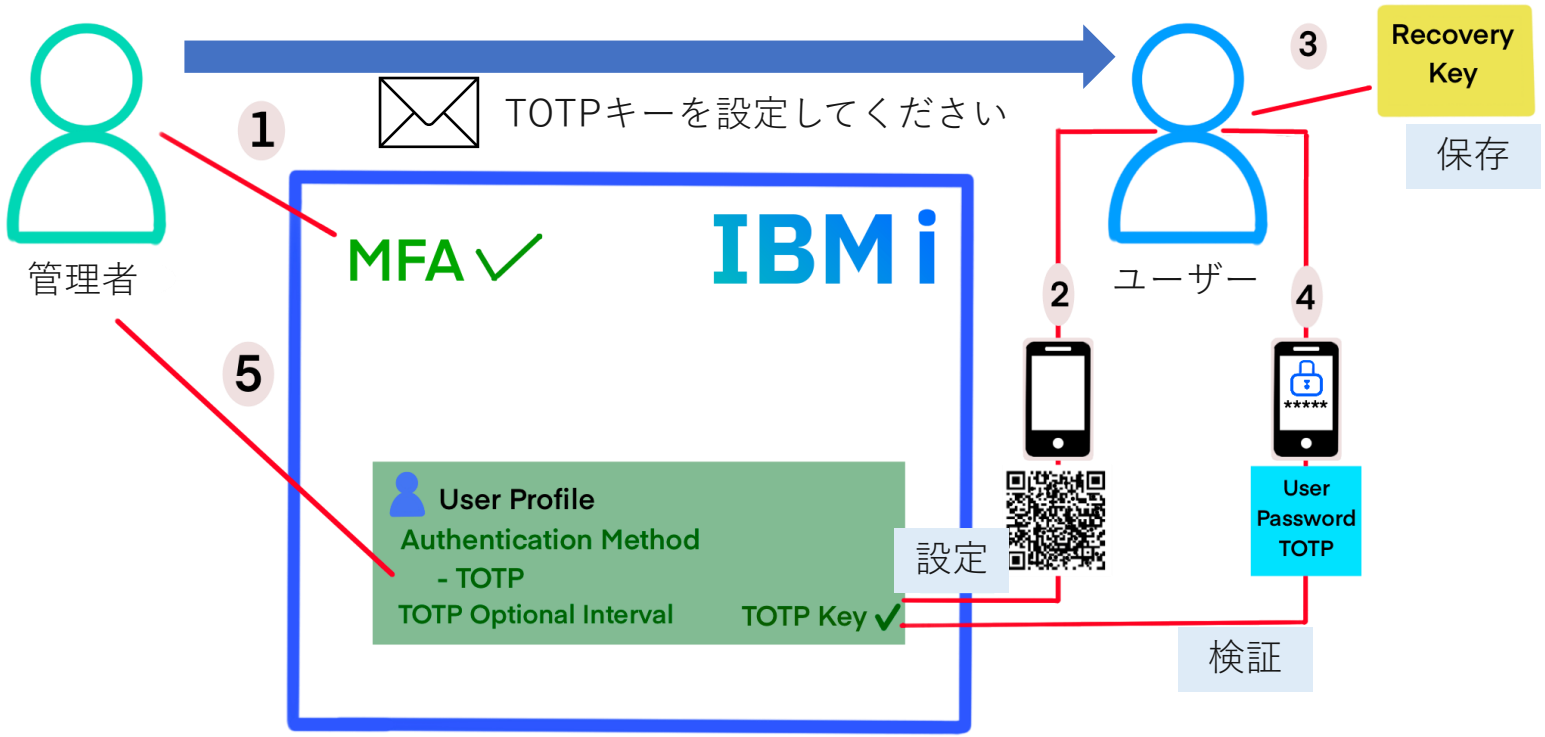
2. 設定方法のご紹介

管理者：

ステップ1

6. ユーザーに、TOTP キーを設定する必要があることを通知する

- 管理者はユーザープロファイルのTOTPキーを設定することはできない
- ユーザーの認証方法を *TOTP に設定するには、ユーザーと管理者の両方による操作が必要である



© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

ユーザー：

ステップ 2

- ユーザーがTOTPキーを設定する

ステップ 3

- リカバリーキーを安全な場所に保存する。 リカバリ・キーは、TOTPキーを設定したときに生成される

ステップ 4

- TOTPキーを多要素認証用のクライアント側のアプリケーションに入力し、検証する
- TOTPキーが設定されたことを管理者に通知する

ユーザーは上記のステップ2から4を下記2つのどちらかを使用する方法でTOTPキーを設定する

a. 5250エミュレーターでのコマンド
b. Navigator for i

この資料ではユーザーのユーザープロファイル名は「USER01」とする

© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

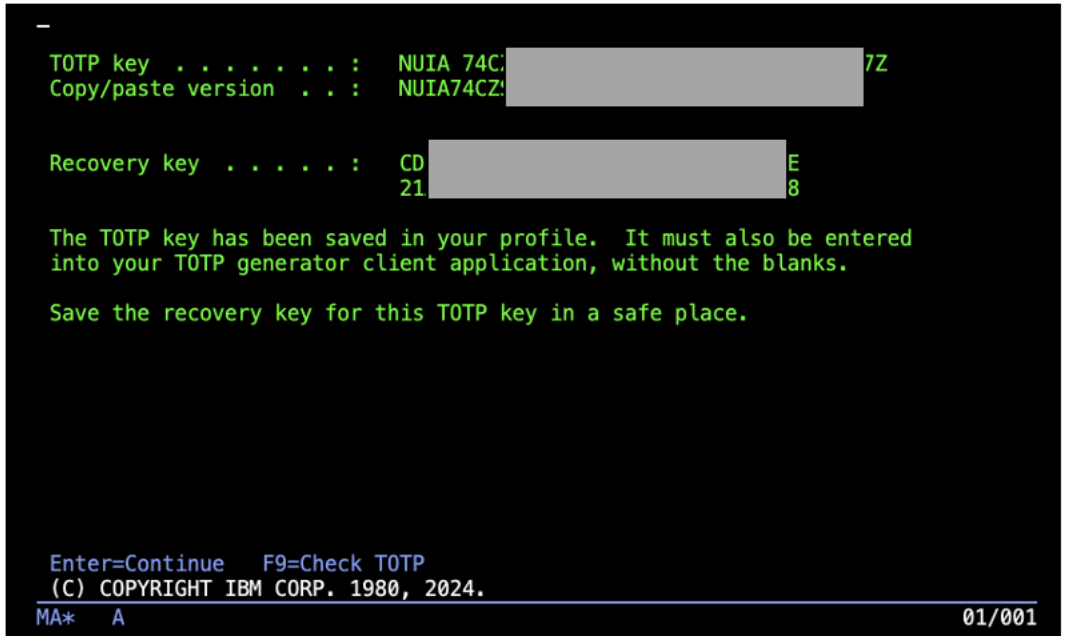
a. 5250エミュレーターでコマンドを使う場合

5250エミュレーターでユーザー「USER01」でサインオンする

ステップ 2

- **ユーザーがTOTPキーを設定する**
- 下記コマンド を実行すると、現在サインオン中のユーザー「USER01」のTOTPキーが生成され、そのユーザープロファイルに保存される

  CHGTOTPKEY TOTPKEY(*GEN)
- コマンド実行後の画面



© IBM 2025

解説

- **ユーザーがTOTPキーを設定する**
- TOTP キーの変更 (CHGTOTPKEY) コマンドを使用する。
- CHGTOTPKEY TOTPKEY(*GEN) の実行により、TOTPキーがユーザープロファイルに保存される。
  CHGTOTPKEYコマンドでは、キーを生成、指定、または削除もできる。
- TOTPキーはユーザープロファイルに保存され、コマンド実行後、画面に表示される。
- TOTPキーを指定する場合、値は32文字で、32進数文字（A～Z、2～7）のみで構成されている必要がある。
  - TOTPキーを指定するコマンド例：
    - CHGTOTPKEY TOTPKEY(DJFEFD67453D5W3E34RR2GJKEPX445D3)
- ユーザープロファイルの認証方法に*TOTPが含まれている場合、TOTPキーの削除はできない。

© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

a. 5250エミュレーターでコマンドを使う場合

ステップ 3

- **リカバリーキーを安全な場所に保存する。 リカバリ・キーは、TOTPキーを設定したときに生成される**
  - ステップ2でCHGTOTPKEY TOTPKEY(*GEN)コマンド実行後に表示される「Recovery Key」を安全な場所に保存しておく

ステップ 4

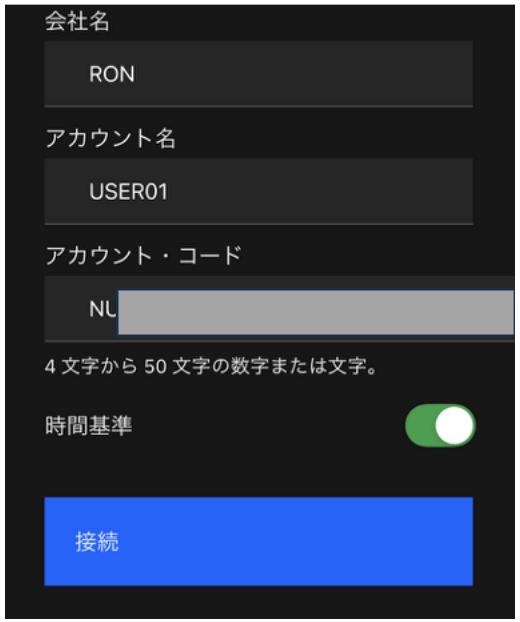
- **TOTPキーを多要素認証用のクライアント側のアプリケーションに入力し、検証する**
  - クライアント側のアプリケーション(例： Microsoft Authenticator、 Google Authenticator、 IBM Security Verify)に接続情報、TOTPキーを入力する
  - TOTPの検査（CHKTOTP）コマンドを使用し、クライアント側のアプリケーションによって生成された TOTP キーが正常に検証されることを確認する
- **TOTPキーが設定されたことを管理者に通知する**

© IBM 2025

解説

- **リカバリーキーを安全な場所に保存する。 リカバリ・キーは、TOTPキーを設定したときに生成される**
  - 「Recovery Key」を安全な場所に保存します。リカバリー・キーは、TOTPキーが機能しない場合、ワンタイム・リカバリーとして、ユーザー・パスワードの代わりに使用できる
- **TOTPキーを多要素認証用のクライアント側のアプリケーションに入力し、検証する**
  - クライアント側のアプリケーション(例： Microsoft Authenticator、 Google Authenticator、 IBM Security Verify)に接続情報、TOTPキーを入力する
  - TOTPの検査（CHKTOTP）コマンドを使用し、クライアント側のアプリケーションによって生成されたTOTP キーが正常に検証されることを確認する
  - 成功すると「 CHKTOTP WAS SUCCESSFUL。 」のメッセージが表示される
  - CHGTOTPKEYコマンド実行後の画面で F9=Check TOTP を押すと、CHKTOTP コマンドのプロンプトが表示される。
- **TOTPキーが設定されたことを管理者に通知する**
  - 正常にTOTPキーが設定されたことを管理者に通知する

クライアント側のアプリケーションとして
IBM Security Verifyを使用した場合の
TOTPキーの入力する画面



© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

b. Navigator for i を使う場合

Navigator for iにユーザー「USER01」でサインオンする
ステップ 2

- **ユーザーがTOTPキーを設定する**
  - QIBM_NAV_ALL_FUNCTION ファンクション ID の許可がない場合、
    サインオン後に 「My MFA 鍵の管理」 画面が表示される

  - QIBM_NAV_ALL_FUNCTION ファンクション ID の許可がある場合、
    [マイ作業] > [My 追加認証要素] > [My MFA 鍵の管理] を展開する

© IBM 2025

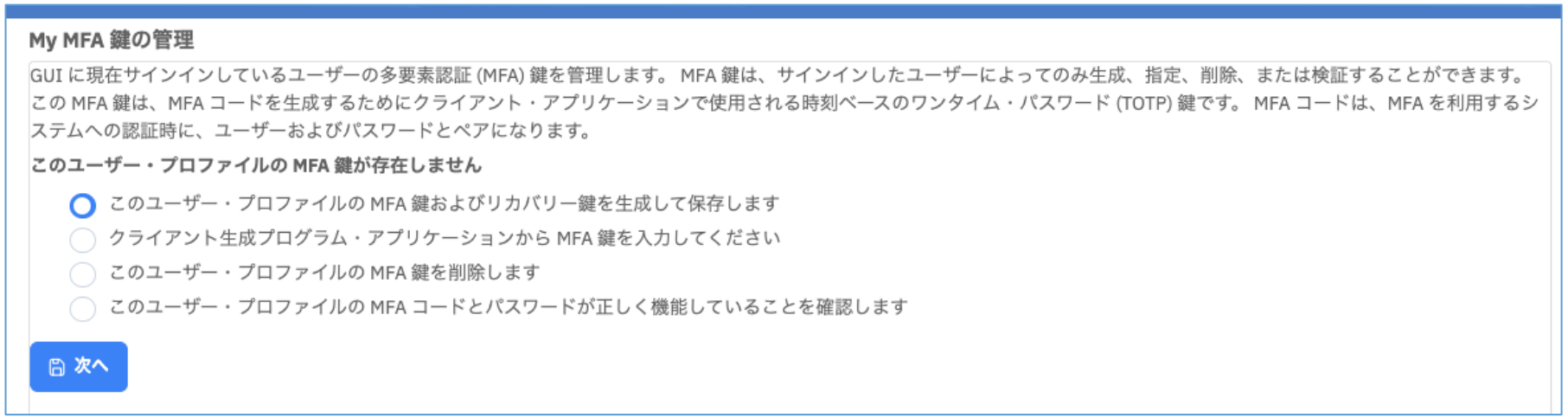
3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

b. Navigator for i を使う場合

ステップ 2

- **ユーザーがTOTPキーを設定する**
  - 「このユーザー・プロファイルのMFA鍵およびリカバリー鍵を生成して保存します」を選択し、「次へ」をクリックする
  - MFA鍵およびリカバリー鍵が生成され、ユーザー・プロファイルに保存される



© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

b. Navigator for i を使う場合

ステップ 3

- **リカバリーキーを安全な場所に保存する。 リカバリ・キーは、TOTPキーを設定したときに生成される**
  - 画面下に表示された「リカバリー鍵」をコピーして、安全な環境に保存する

© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

b. Navigator for i を使う場合

ステップ 4

- **TOTPキーを多要素認証用のクライアント側のアプリケーションに入力し、検証する**
  - クライアント側のアプリケーション(例： Microsoft Authenticator、 Google Authenticator、IBM Security Verify)を使用し、「1.保存されたMFA鍵」に表示されたTOTPキー（MFA鍵）を手動で入力するか、二次元バーコードをスキャンし、入力する
  - 「2.MFA鍵の検証」メニューを使用し、クライアント側のアプリケーションによって生成された6桁のTOTP キー(MFAコード)が正常に検証されることを確認する
- **TOTPキーが設定されたことを管理者に通知する**

© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

管理者：

ステップ 5

TOTP認証方式を有効にする

1. ユーザーがTOTPキーを設定しているかどうかを確認する

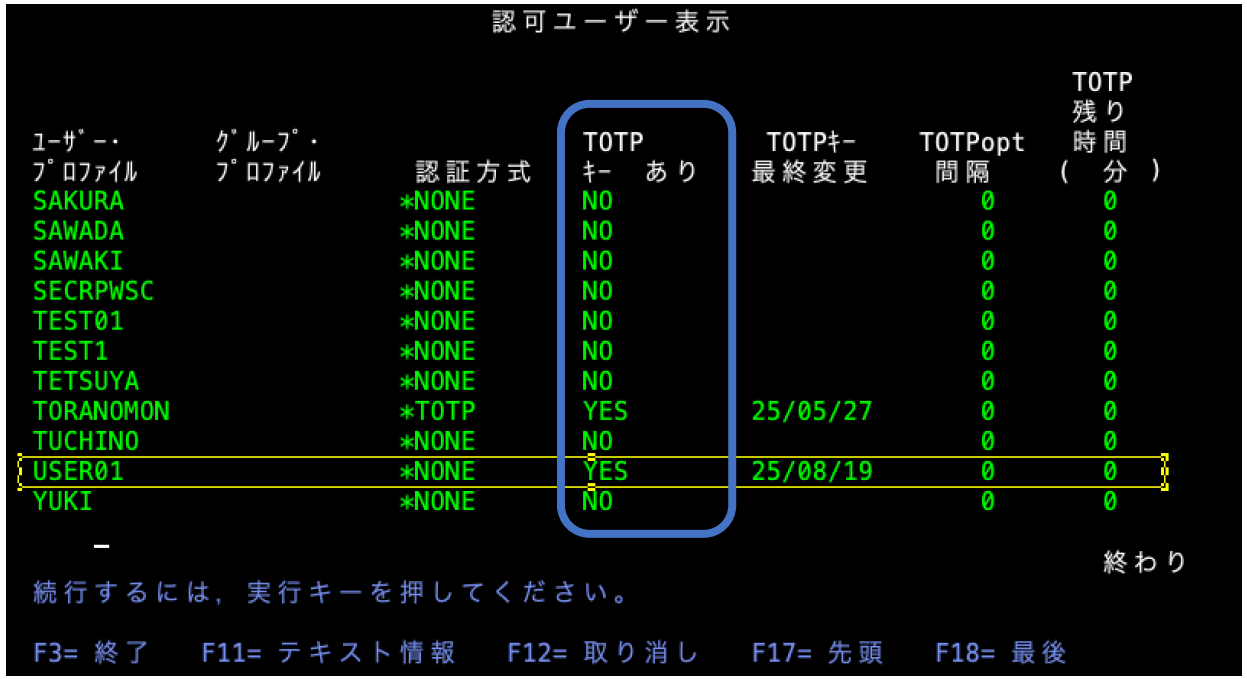
5250エミュレーターを使う場合

DSPAUTUSR コマンド の追加認証情報ビューを使用し、対象のユーザー・プロファイルの項目「TOTPキーあり」が「YES」になっているかを確認する

コマンド：

DSPAUTUSR

画面表示後、F11キーを2回押す



© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

管理者：

ステップ 5

TOTP認証方式を有効にする

1. ユーザーがTOTPキーを設定しているかどうかを確認する

Navigator for i を使う場合

「セキュリティー」→「MFA設定」をクリック
画面の下の方の「ユーザー」をクリック
フィルターの「MFA鍵が存在します」(YES)がデフォルトで適用されたリストが表示される
対象のユーザー・プロファイルが表示さえているか確認する

© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

管理者：

ステップ 5

TOTP認証方式を有効にする

2. ユーザーのTOTPキーが設定されている場合、ユーザープロファイルを変更して、認証方法に*TOTPを含めるように設定し、希望するTOTPオプション間隔を設定する

5250エミュレーターを使う場合

CHGUSRPRF コマンド の AUTHMTHパラメータで「*TOTP」を指定し、認証方法を設定し、TOTPOPTITVパラメータで希望するTOTPオプション間隔(分単位)を設定する

- TOTPオプション間隔とは
  - ユーザーがTOTPキーを使用して一度ログインした後、それ以降の認証でTOTPキーを入力せずにログインが許可される時間
  - *NONEを設定すると認証の度にTOTPキーが必要となる

コマンド例：

CHGUSRPRF USRPRF(USER01) AUTHMTH(*TOTP) TOTPOPTITV(1)

設定は以上である

© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

管理者：

ステップ 5

TOTP認証方式を有効にする

2. ユーザーのTOTPキーが設定されている場合、ユーザープロファイルを変更して、認証方法に*TOTPを含めるように設定し、希望するTOTPオプション間隔を設定する

Navigator for i を使う場合

「ユーザーおよびグループ」→「ユーザー」をクリック
フィルターでユーザーの名前「USER01」など対象のユーザー名を入力し、「OK」をクリック
表示されたユーザープロファイルをダブルクリック

© IBM 2025

3. IBM i 統合 MFA を使ってみよう

2. 設定方法のご紹介

Navigator for i を使う場合(つづき)

ユーザーのプロパティー画面が表示される
「TOTP鍵を仕様したMFA認証」にチェックを入れ、認証方法を設定し、
「オプションの間隔(分)」で希望するTOTPオプション間隔(分単位)を設定する
「OK」をクリック

- オプションの間隔(分)とは
  - ユーザーがTOTPキーを使用して一度ログインした後、それ以降の認証でTOTPキーを入力せずにログインが許可される時間
  - *NONEを設定すると認証の度にTOTPキーが必要となる

設定は以上である

© IBM 2025

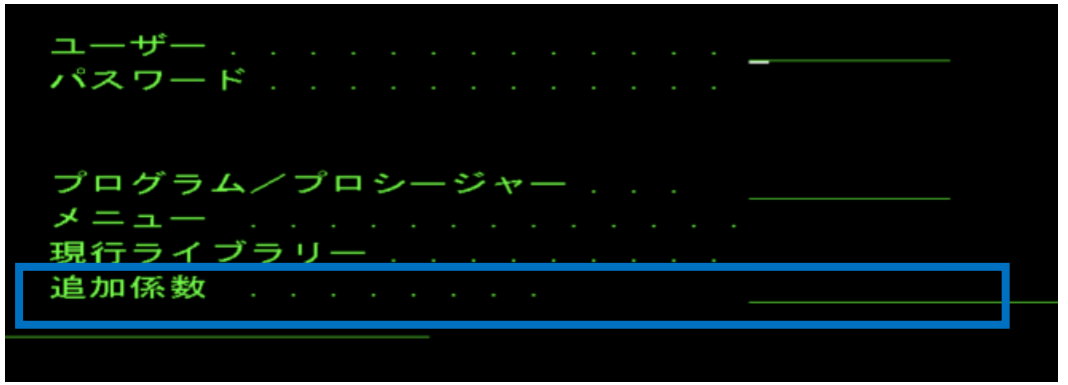
3. IBM i 統合 MFA を使ってみよう

3. ログイン方法のご紹介

さまざまなインターフェースでMFAのTOTPキーの入力が可能となっている

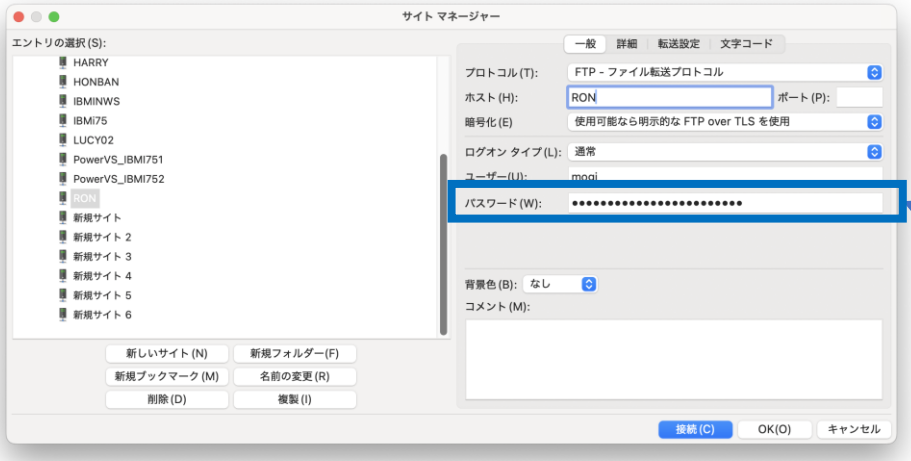
IBM i Access Client Solutions

5250エミュレーター



Navigator for i

FTPソフトウェア



追加係数のフィールドがない場合は、
「パスワード:TOTPキー」と入力する
例：myAmazingPa$$w0rd:358538
参照：追加要素を付加したパスワード
https://www.ibm.com/docs/ja/i/7.6.0?topic=method-password-appended-additional-factor

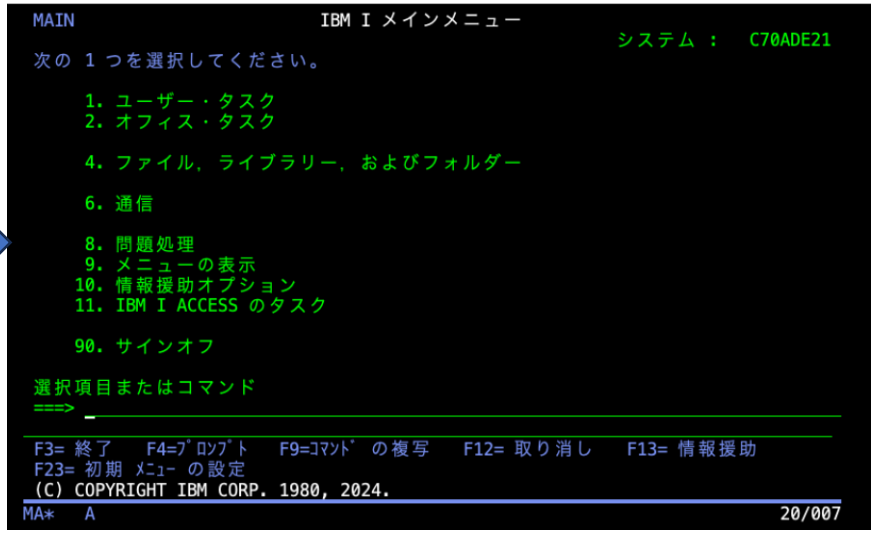
© IBM 2025

3. IBM i 統合 MFA を使ってみよう

3. ログイン方法のご紹介

5250エミュレーターでのログイン例
(他のインターフェースも同様)

1. ユーザープロファイルとパスワードを入力
2. クライアント側のアプリケーション(例： Microsoft Authenticator、 Google Authenticator、 IBM Security Verify) によって生成された TOTP キーを確認し、Additional Factorに入力
3. 認証され、メインメニューが表示される



© IBM 2025

解説

- MFAを有効化していないユーザープロフィールは、サインオン画面にTOTPキー入力フィールドが表示されていても、ユーザープロフィールとパスワードの入力のみでログインが可能
- IBM i でのMFAは、一部のアプリケーションやソフトウェア・インタフェースに対応しておらず、うまく機能しなかったり、クライアント・アプリケーションの変更が必要になったりすることがある。
  - 例：後でサーバーに認証するために、ユーザーのパスワードをキャッシュしたり保存したりするクライアント・アプリケーションは、MFAはうまく機能しないことがある。
  - 詳細については下記のリンク先を参照
    - IBM i ソフトウェアとクライアント・アプリケーションに関する考慮事項
    - https://www.ibm.com/docs/ja/i/7.6.0?topic=mfa-i-software-client-application-considerations
- IBM i 統合 MFAの代替ソリューションとして、IBM PowerSCの多要素認証機能がある
  - IBM PowerSC は、IBM i 統合 MFAとは異なり、IBM i に統合されておらず、有償のソフトウェアであるが、他にもセキュリティ機能を持っている
  - 詳細についは下記のリンク先を参照
    - iWorld 「IBM PowerSCを用いてIBM i のセキュリティーを強化しましょう」
    - https://iworldweb.info/column/product/enhance-ibm-i-security-with-ibm-powersc

© IBM 2025

4. 補足情報

1. IBM i 7.6 Documentation 多要素認証 (MFA)
   https://www.ibm.com/docs/ja/i/7.6.0?topic=security-multi-factor-authentication-mfa

2. iWorld(イグアス様サイト）2025年、対策を施すべきIBM iのセキュリティー保護の重要ポイント
   https://iworldweb.info/column/product/top-ibmi-security-projects-2025

© IBM 2025

今後のIBM i 関連イベントの予定 (IBM主催 – 通年開催分)

時期	セミナー名	内容	URL等
通年開催	IBM Power Salon	IBM Powerユーザー向けWebサロン。 8月を除く毎月第二水曜日9-10AM開催	https://ibm.biz/power-salon
通年開催	IBM i Club	IBM i ユーザーコミュニティー	https://ibm.biz/ibmiclub
通年開催	IBM i リスキリングカレッジ	IBM i の最新スキル習得	過去ビデオ↓ https://ibm.biz/reskill
通年開催 (本年度募集終了)	IBM i RiSING 若手コミュニティー	IBM i 若手コミュニティー。 年末-年初に来年度募集を予定。	https://ibm.biz/IBMiRiSING

予定は変更となる可能性があります。

© 2025 IBM Corporation

今後のIBM i 関連イベントの予定 (IBM主催 – 個別開催分)

時期	セミナー名	内容	URL等
9/7 (日) - 12 (金) (本年度募集終了)	米国ロチェスター研究所ツアー	IBM i 開発本部の見学と最新情報の紹介。同時通訳有。毎年開催予定。	お問い合わせ IBMiContact@wwpdl.vnet.ibm.com
10/2 (木) 10AM - 正午	IBM i Essentials 2025 Autumn	IBM i 事例ビデオと最新情報。Q&Aセッションもあります。	以下のURLよりアクセスしてご視聴ください。 事前申し込みは不要です。 https://ibm.biz/Essentials_Web
11/27 (木) 10AM - 6PM	IBM i Advantage 2025	IBM i ユーザー向けセミナー。今年は外部会場 (新宿) を予定。i-Evoも同日開催。	セミナーポータルで案内予定 (未掲載)↓ https://ibm.biz/powerevents-j
12/3 (水) 終日	IBM TechXchange Japan	日本IBMの製品・サービスの総合セミナー	2024年セミナー (終了分) 案内↓ https://ibm.biz/txjapan

予定は変更となる可能性があります。

© 2025 IBM Corporation

IBM i 関連情報 (2025/05/09 更新)

IBM i ポータル・サイト
https://ibm.biz/ibmijapan

i Magazine (IBM i 専門誌。春夏秋冬の年4回発刊)
https://www.imagazine.co.jp/IBMi/

IBM i World 2024 オンデマンド・セミナー
https://video.ibm.com/recorded/133917616
IBM i World 2023 オンデマンド・セミナー
https://ibm.biz/ibmiworld2023
IBM i World 2022 オンデマンド・セミナー
https://video.ibm.com/recorded/132423205

月イチIBM Power情報セミナー「IBM Power Salon」
https://ibm.biz/power-salon

IBM i 関連セミナー・イベント
https://ibm.biz/powerevents-j

IBM i Club (日本のIBM i ユーザー様のコミュニティー)
https://ibm.biz/ibmiclubjapan

IBM i 研修サービス (i-ラーニング社提供)
https://www.i-learning.jp/service/it/iseries.html

IBM TechXchange Powerユーザーコミュニティー (日本)
https://ibm.biz/ibm-power-user-community

IBM i RiSING - IBM i 若手技術者コミュニティー
https://ibm.biz/ibmirising2025

新・IBM i入門ガイド［操作・運用編］
https://www.imagazine.co.jp/01-ibm-i-jikkoukankyou-of-ibm-i-nyumon-guide-sousa-unyou/
新・IBM i入門ガイド［開発編］
https://www.imagazine.co.jp/01-development-tools-of-ibm-i-nyumon-guide-kaihatsu/
これから使う人のためのIBM i入門ガイド (旧バージョン)
https://www.imagazine.co.jp/imagazine-7071/

IBM i 情報サイト iWorld
https://ibm.biz/iworldweb
IBM i 製品とサポートのロードマップ
https://ibm.biz/ibmiroadmap2024
IBM i 7.6 技術資料
https://www.ibm.com/docs/ja/i/7.6.0?topic=documentation-overview-whats-new

IBM Power ソフトウェアのダウンロードサイト (ESS)
https://ibm.biz/powerdownload
Fix Central (HW・SWのFix情報提供)
https://www.ibm.com/support/fixcentral/
IBM My Notifications (IBM IDの登録 [無償] が必要)
「IBM i」「9105-41B」などPTF情報の必要な製品を選択して登録できます。
https://www.ibm.com/support/mynotifications
IBM i 各バージョンのライフサイクル
https://www.ibm.com/support/pages/release-life-cycle
IBM i 以外のSWのライフサイクル (個別検索)
https://www.ibm.com/support/pages/lifecycle/

IBM Power Systems Virtual Server 情報
https://ibm.biz/pvsjapan

© IBM 2025

© IBM 2025

ワークショップ、セッション、および資料は、IBMによって準備され、IBM独自の見解を反映したものです。それらは情報提供の目的のみで提供されており、いかなる読者に対しても法律的またはその他の指導や助言を意図したものではなく、またそのような結果を生むものでもありません。本資料に含まれている情報については、完全性と正確性を期するよう努力しましたが、「現状のまま」提供され、明示または暗示にかかわらずいかなる保証も伴わないものとします。本資料またはその他の資料の使用によって、あるいはその他の関連によって、いかなる損害が生じた場合も、IBMは責任を負わないものとします。 本資料に含まれている内容は、IBMまたはそのサプライヤーやライセンス交付者からいかなる保証または表明を引きだすことを意図したものでも、IBMソフトウェアの使用を規定する適用ライセンス契約の条項を変更することを意図したものでもなく、またそのような結果を生むものでもありません。
本資料でIBM製品、プログラム、またはサービスに言及していても、IBMが営業活動を行っているすべての国でそれらが使用可能であることを暗示するものではありません。本資料で言及している製品リリース日付や製品機能は、市場機会またはその他の要因に基づいてIBM独自の決定権をもっていつでも変更できるものとし、いかなる方法においても将来の製品または機能が使用可能になると確約することを意図したものではありません。本資料に含まれている内容は、読者が開始する活動によって特定の販売、売上高の向上、またはその他の結果が生じると述べる、または暗示することを意図したものでも、またそのような結果を生むものでもありません。 パフォーマンスは、管理された環境において標準的なIBMベンチマークを使用した測定と予測に基づいています。ユーザーが経験する実際のスループットやパフォーマンスは、ユーザーのジョブ・ストリームにおけるマルチプログラミングの量、入出力構成、ストレージ構成、および処理されるワークロードなどの考慮事項を含む、数多くの要因に応じて変化します。したがって、個々のユーザーがここで述べられているものと同様の結果を得られると確約するものではありません。
記述されているすべてのお客様事例は、それらのお客様がどのようにIBM製品を使用したか、またそれらのお客様が達成した結果の実例として示されたものです。実際の環境コストおよびパフォーマンス特性は、お客様ごとに異なる場合があります。
IBM、IBM ロゴ、ibm.com、Db2、Rational、Power、POWER8、 POWER9、POWER10、AIXは、世界の多くの国で登録されたInternational Business Machines Corporationの商標です。
他の製品名およびサービス名等は、それぞれIBMまたは各社の商標である場合があります。
現時点での IBM の商標リストについては、www.ibm.com/legal/copytrade.shtml をご覧ください。

インテル, Intel, Intelロゴ, Intel Inside, Intel Insideロゴ, Centrino, Intel Centrinoロゴ, Celeron, Xeon, Intel SpeedStep, Itanium, およびPentium は Intel Corporationまたは子会社の米国およびその他の国における商標または登録商標です。
Linuxは、Linus Torvaldsの米国およびその他の国における登録商標です。
Microsoft, Windows, Microsoft Excel, Windows NT および Windowsロゴは Microsoft Corporationの米国およびその他の国における商標です。
UNIXはThe Open Groupの米国およびその他の国における登録商標です。
JavaおよびすべてのJava関連の商標およびロゴは Oracleやその関連会社の米国およびその他の国における商標または登録商標です。