ぜひユーザーにご案内ください

今すぐ対策！
多要素認証！
（MFA）

******

# パスワードだけでは守れない

# 乗っ取りは起きる前提です！

**MFA（多要素認証）未設定** ＝ 危険な状態のまま業務を続けている、ということ

## 不正アクセスでこんな被害が

被害1

### メール乗っ取り

取引先・顧客になりすました連絡が行われ、**誤送金や情報漏えいなどの二次被害**につながる恐れがあります。
**社内外の信用低下**に加え、事実確認・謝罪・再発防止などの**対応工数が増加**します。

被害2

### クラウドデータへの不正アクセス

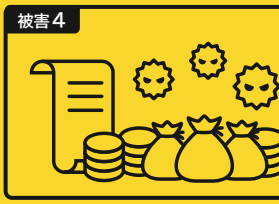
データの持ち出しだけでなく、**改ざん・削除が発生する可能性**があります。
復旧やログ調査が長期化し、**業務影響と追加コスト**につながります。

被害3

### 管理者アカウント侵害

権限・設定を握られ、**ユーザー追加や権限変更、設定改変が行われる恐れ**があります。
**影響が部門を越えて全社に波及**し、正常化までの負荷が大きくなります。

被害4



### Azure の踏み台利用（クラウド計算資源の悪用）

侵害IDを足がかりに**VM/コンテナ等を大量作成**され、スパムメール送信や暗号資産採掘などに**悪用される恐れ**があります。
その結果、**高額請求が短期間で発生**し、最悪、会社の業績へのインパクトになりえます。

## 「パスワードは突破される」前提で、必ずMFAの設定を！

**多要素認証の設定確認** 以下の手順で多要素認証が設定されているかご確認ください。 ※費用はかかりません。

### Microsoft

**1 STEP** 多要素認証の設定方法を確認してください。

Microsoft Authenticator で microsoft Authenticator を使用する365

**2 STEP** 設定できない場合は、多要素認証のリセットをお試しください。

多要素認証(MFA)のリセット手順 - 2025 年

### AWS


**MFA設定手順資料**をご用意いたしました！
ぜひご活用下さい。

テナント乗っ取り防止対策について

### Google Cloud

下記公式ブログの「**今すぐ2段階認証プロセスを有効にする**」セクションを参考に設定してください。

Google Cloud での MFA の必須化について知っておくべきこと

Google Workspace管理者ヘルプ 2段階認証プロセスでビジネスを保護する

本件に関するご質問は、担当営業までお問い合わせください。

DIS ダイワボウ情報システム株式会社

ぜひユーザーにご案内ください ぜひユーザーにご案内ください 今すぐ対策！