

テロ対策ネットワーク静岡

～テロを許さない社会づくり～

令和8年NO.5



令和8年8月10日発行

発行: 静岡県警察本部
警備部公安課

TEL
代表 054-271-0110



【企業向け】デバイスコード認証を悪用したサイバー攻撃の手口にご注意ください



デバイスコード認証

別の端末を使って簡単にログインすることができる仕組みのことです。

例: テレビで動画視聴サービスにログインする場合

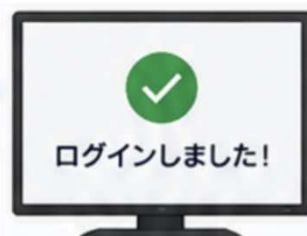
テレビにコードが表示される



テレビに表示されたコードを
スマホに入力、本人確認実施



テレビでログイン完了



デバイスコード認証を悪用した手口の一例

① 企業に取引先等をかたるメールを送り、URLにアクセスさせる

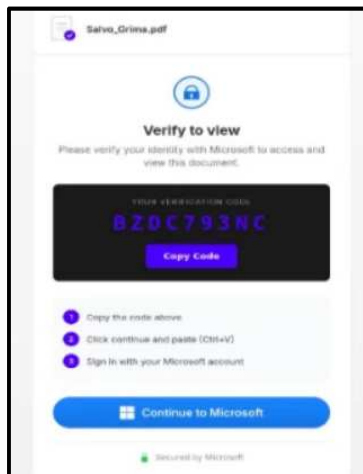
見積書を送付します。
添付ファイルをご覧ください。



ファイルの共有先は以下です。
以下から認証してください。

<https://▲▲▲▲▲.com>

② ファイルの閲覧には認証が必要とし、認証コードを表示する



③ 本物のMicrosoftデバイス認証ページに誘導し、認証コードを入力させる

アクセス許可コードの入力

アプリまたはデバイスに表示されるコードを入力すると、アカウントにアクセスできるようになります。

信頼できないソースからのコードは入力しないでください。

コード

次へ

④ 指示に従い認証を進めると、**攻撃者のデバイスから被害企業のMicrosoft365アカウントへのアクセスが承認されてしまう**。攻撃者はパスワードや追加の多要素認証なしで、**企業のOutlook、Teams、OneDriveなどのMicrosoft365サービスにアクセスできるようになってしまう**。

対策

・ 唐突にデバイスコードの入力・認証を求められた場合は、サイバー攻撃を疑う。

・ Microsoft Entraを利用している環境であれば、組織におけるデバイスコード認証でのアクセスブロックを検討する。詳細は下記Microsoftのサイト等をご覧ください。

<https://learn.microsoft.com/ja-jp/entra/identity/conditional-access/policy-block-authentication-flows>