ActiveDirectoryを利用した攻撃手法

ActiveDirectoryは、ユーザ認証とアクセス制御を行うことができるWindowsサーバの機能で、攻撃者はシステム侵入後に侵害範囲を拡大するツールとして悪用します。

このActiveDirectoryを悪用したサイバー攻撃の手法について紹介します。

ActiveDirectoryを利用した攻撃の例

①パスワードをリセットする権限がすべてのユーザに付与されていた

➡ **攻撃者はフィッシングなどで非特権アカウントを乗っ取った後、さらに特権アカウントのパスワードをリセットして乗っ取る**

②ユーザをグループに追加する権限を持つユーザのアカウントが乗っ取られた

➡ **攻撃者は乗っ取ったアカウントをヘルプデスクグループ（ユーザのパスワードをリセットする権限を持つ）に追加し、同グループの権限で管理者のパスワードをリセットして乗っ取る**

紹介したのは、ActiveDirectoryを利用した攻撃のほんの一例です。
ユーザに付与する権限を必要最小限にするなどして被害を未然に防止しましょう。

TPCCAT
Tochigi Police Counter Cyber Attack Team