

ITシステムの幽霊退治、してありますか？

ITシステムに潜む幽霊とは？

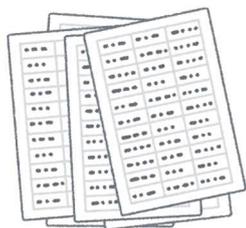
今も昔も心霊現象というのは好きな人にはたまらない話題ですが、実はITシステムにも幽霊が潜むのをご存じでしょうか？

それは、「**アカウント幽霊**」です。

どちらかといえば、幽霊アカウントとかゴーストIDと呼ばれるほうが多いですが、その正体は、利用者がいないにもかかわらず、適切に処理されずにシステムに**放置されたままのアカウント**です。



このようなアカウントが生じる原因としては、不定期に発生した退職者のアカウントを都度整理していなかったり、テスト用など開発時に使われたアカウントが、その後本番運用になったにもかかわらず削除されず、そのまま忘れられてしまった、などがあります。



これらのアカウントは当然ながらパスワードの更新もされず、場合によってはシステム管理者も知らないまま何かしらの特権が付与されていたりすることもあり、セキュリティの観点からは重大な脆弱性として適切な管理が求められます。

特にテレワーク用などリモートログイン環境がある場合は、幽霊アカウントはサイバー攻撃者の格好の標的となってしまうため、早期の対処が必要です。

アカウントは適時適切な棚卸しを

利用者不明の幽霊アカウントを排除するのはもちろんのことですが、実は現在利用中のアカウントについても適切なタイミングで見直しをする必要があります。

例えば、人事異動で担当業務が変わったにもかかわらず、以前の部署の顧客リストや発注情報など、現業務に不必要なデータへのアクセス権が残っていると、データ持ち出しなど、今後の不正の温床となってしまう可能性があります。



ですから、人事異動や業務再編などが発生したタイミングで随時アクセス権を見直すほか、年に一回程度は全アカウントの『棚卸し』を行うなど、適切なアカウント管理を定期業務の一つとして手順に組み入れ、IT事故を未然に防ぎましょう。