

皆さんの組織でも起こりうる?! 分かりやすい事例シリーズ④

各種システムの ログインID、パス ワード管理徹底を!

ID、パスワードはいわば「金庫の鍵」や「家の鍵」と同じです。これらを適切に管理しなければ、金庫や家の玄関を勝手に開けられてしまうように、システムへ不正ログインされてしまいます。

●パスワードは英大文字小文字+
数字+記号で10桁以上にする



パスワードが長すぎると
覚えられない・・・
何だったっけ??
(よくある話です)

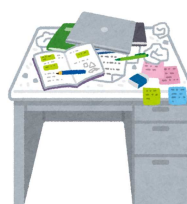
●パスワードの使い回しはしない

●他人にID、パスワード等を見られ
ないように配慮する

在職時に使っていたパスワード
でログインできる! ラッキー!



●システムへのアクセス権限がない
職員や退職者が勝手にログイン
できないように設定する



デスクマットに挟んだり、
付箋で貼り付けておくのは
やめましょう!

個人で行う対策だけではなく「組織全体での対策」も非常に重要です!

～実際に北海道で発生した事案～

企業Aに勤務していた社員が退職後、関係データ等を持ち出す目的でシステムに不正アクセス!



・退職者手続きの際、在職時にどんな権限を付与していたのか、確認しておく
・情報取扱ポリシーの作成、従業員に対する定期的な教育、執務室への入退室管理を行う
・離職者との秘密保持契約締結により情報漏えいを防止する
等の対策が有効です!

～ 万が一、被害に遭った場合は最寄りの警察署へ相談をしてください! ～

北海道警察サイバーセキュリティ対策本部