社内管理はこちら

## 会社の個人情報の漏えいの原因は“内部原因”

「社内の情報漏洩の約8割は内部犯によるもの」と言われています。
事実、多発する情報漏洩事件における原因の多くは、ハッキングなどの外部要因ではなく、内部の人間による盗難、流出など内部要因が多くを占めています。

【よく聞く対応策例】

- ■会社関連情報入りのPCやUSBなど持ち出しの禁止
- ■社内に外部PCやソフト（個人利用ソフト）を持ち込まない
- ■媒体・端末の放置禁止・盗難対策（ノートPCにチェーンを付けるなど）
- ■定期的なログインパスワードの変更

**本当にこの対策だけで個人情報漏えいは防げると思っていますか？**

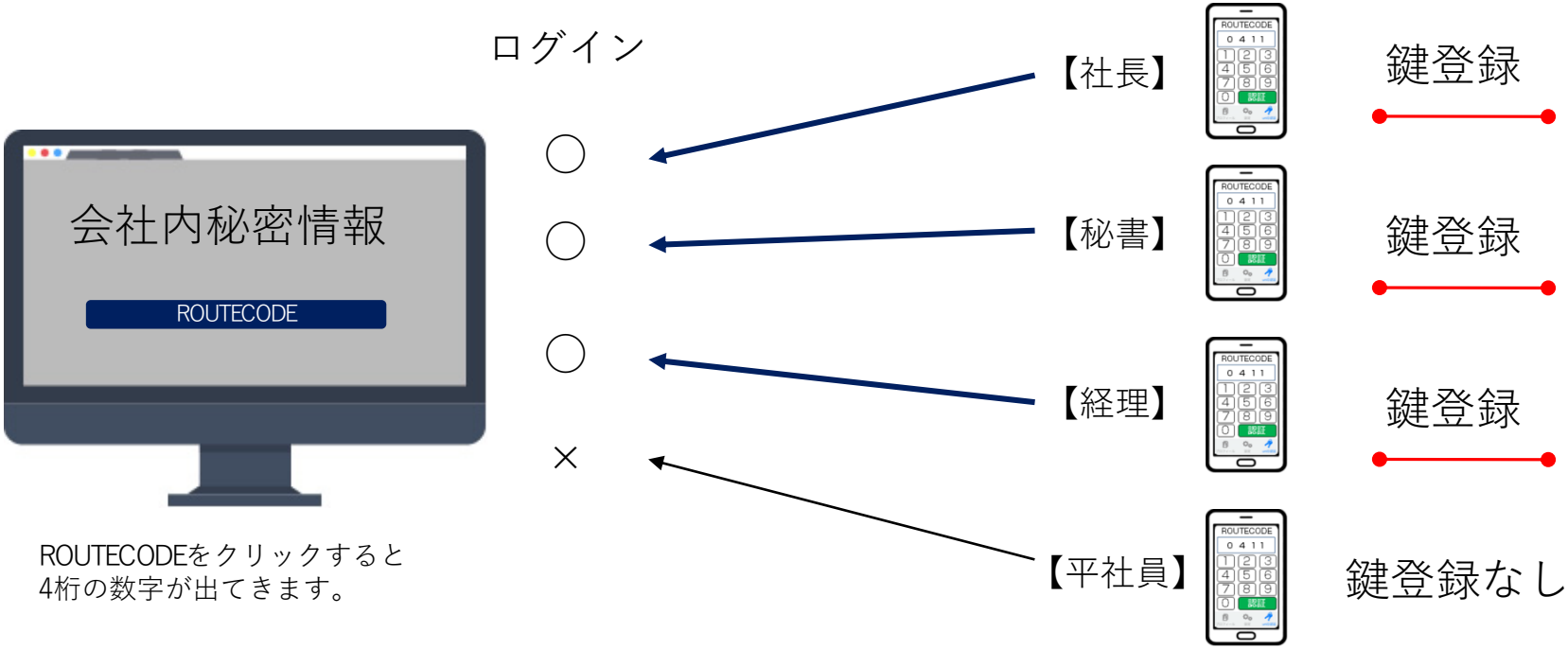
社員教育を含め社員ひとりひとりの意識が変わらなければ何をしても同じです。
退社しようとする人間やなにも考えていない社員は簡単には変わりません。
社内ルールを社員全員に意識のみで守らせることは不可能に近い内容です。

# ROUTECODE導入例（社内管理①）

特定の人間のみにしか見られたくない情報をROUTECODEを利用して管理

様々あるページの中で特定の人間以外に見られたくないページにのみROUTECODEを導入！

**《鍵は権限を与えた人間のスマホにのみ作成》**




**鍵登録をしていない平社員が4桁を入力してもログインすることは出来ません。**

# ROUTECODE導入例（社内管理②）

## 社員の個人情報の持ち出しをROUTECODEを利用して防御

さらに、退社する人間が出る毎にパスワードを変更する必要もございません。

### 【会社内】

鍵登録した端末を1台用意し社外持ち出しを
行えないようにする



ROUTECODEをクリックすると
4桁の数字が出てきます。

ログイン成立

### 【会社外】

鍵登録した端末がないため会社外でログインする
ことが出来ません。



ログイン不成立

※ただし、ログインしたい端末に出ている4桁を伝え
社内にある鍵登録をしている端末に入力すればログイン可能です。