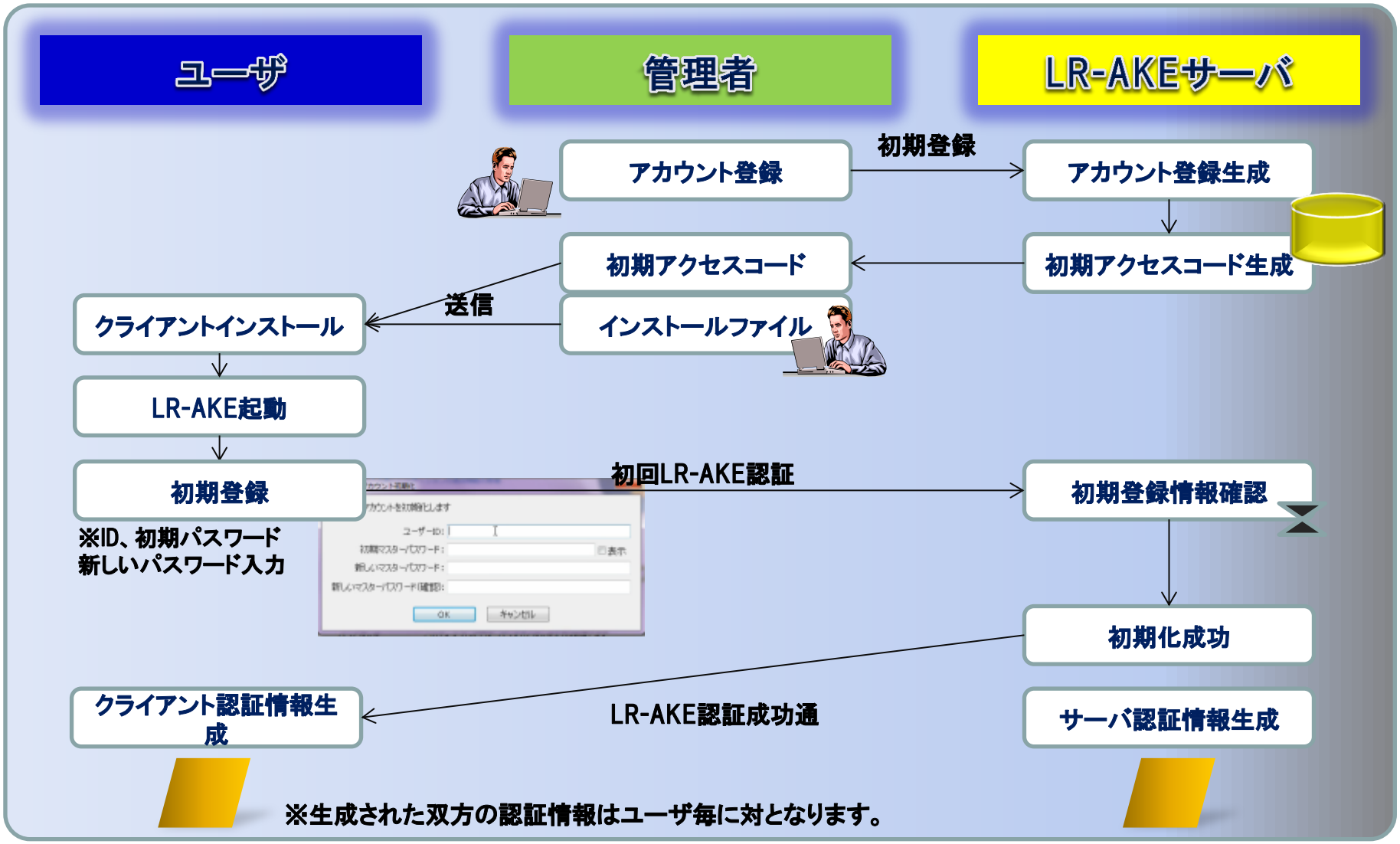
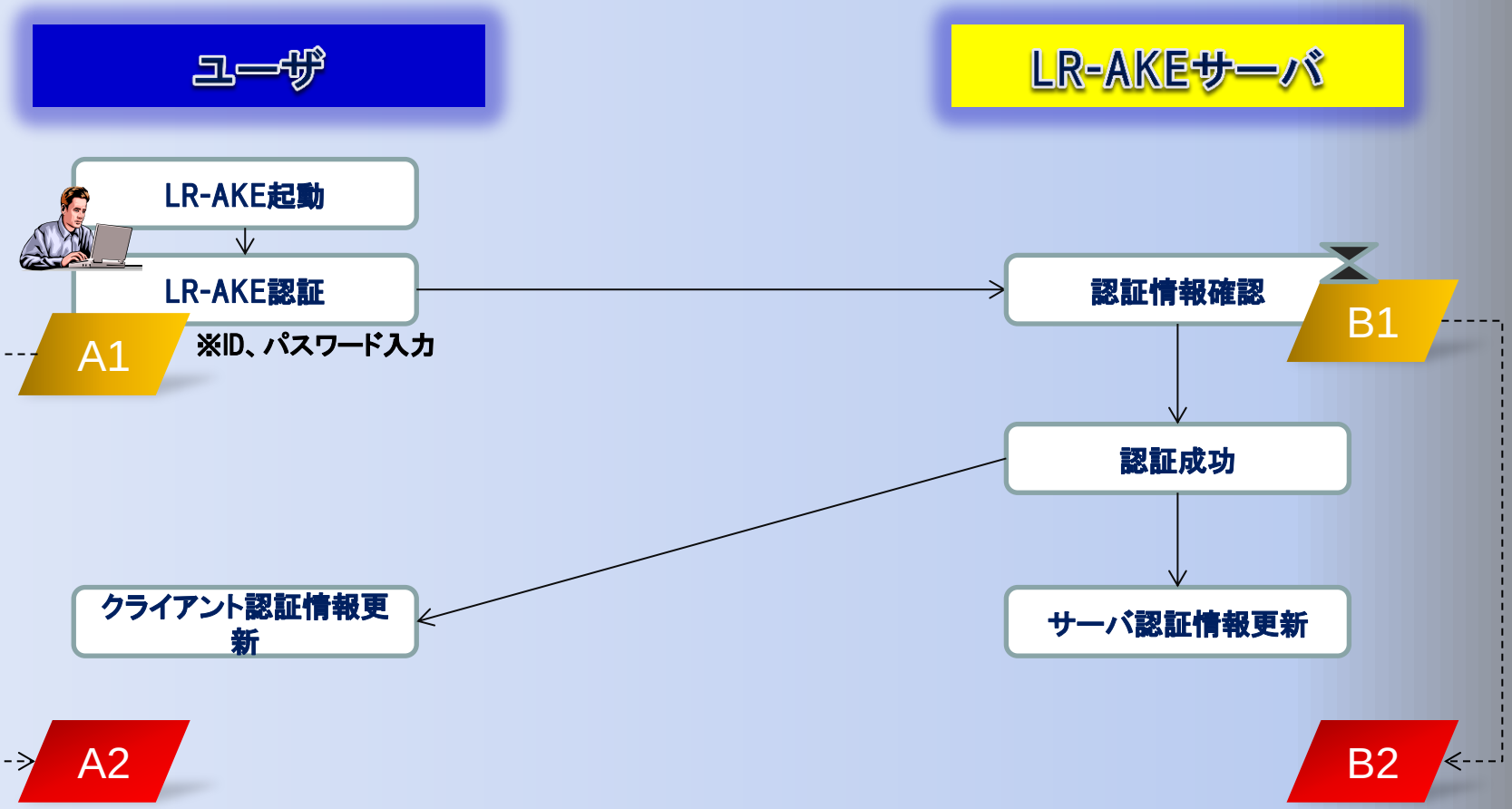
インストールから初期化

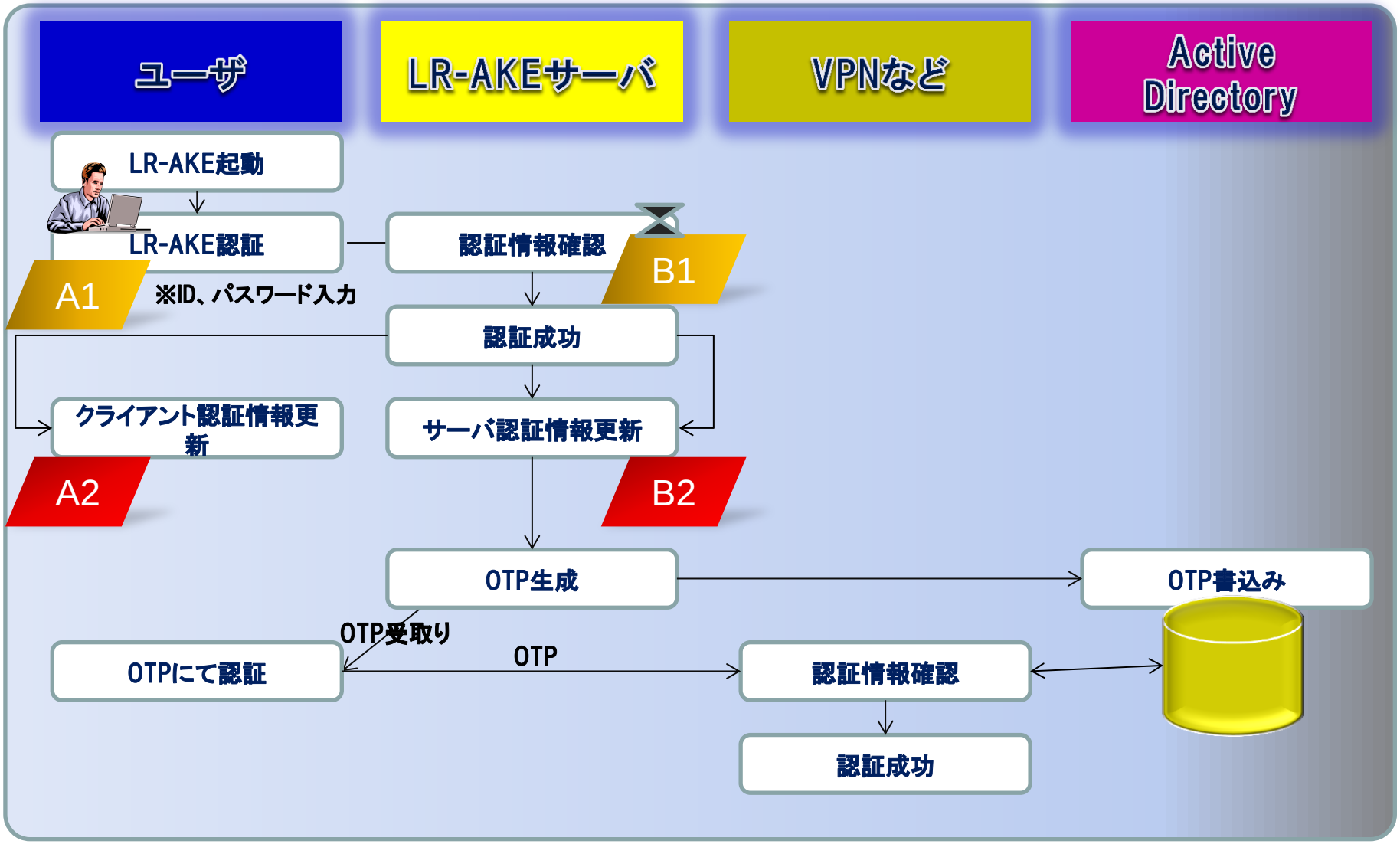


通常認証



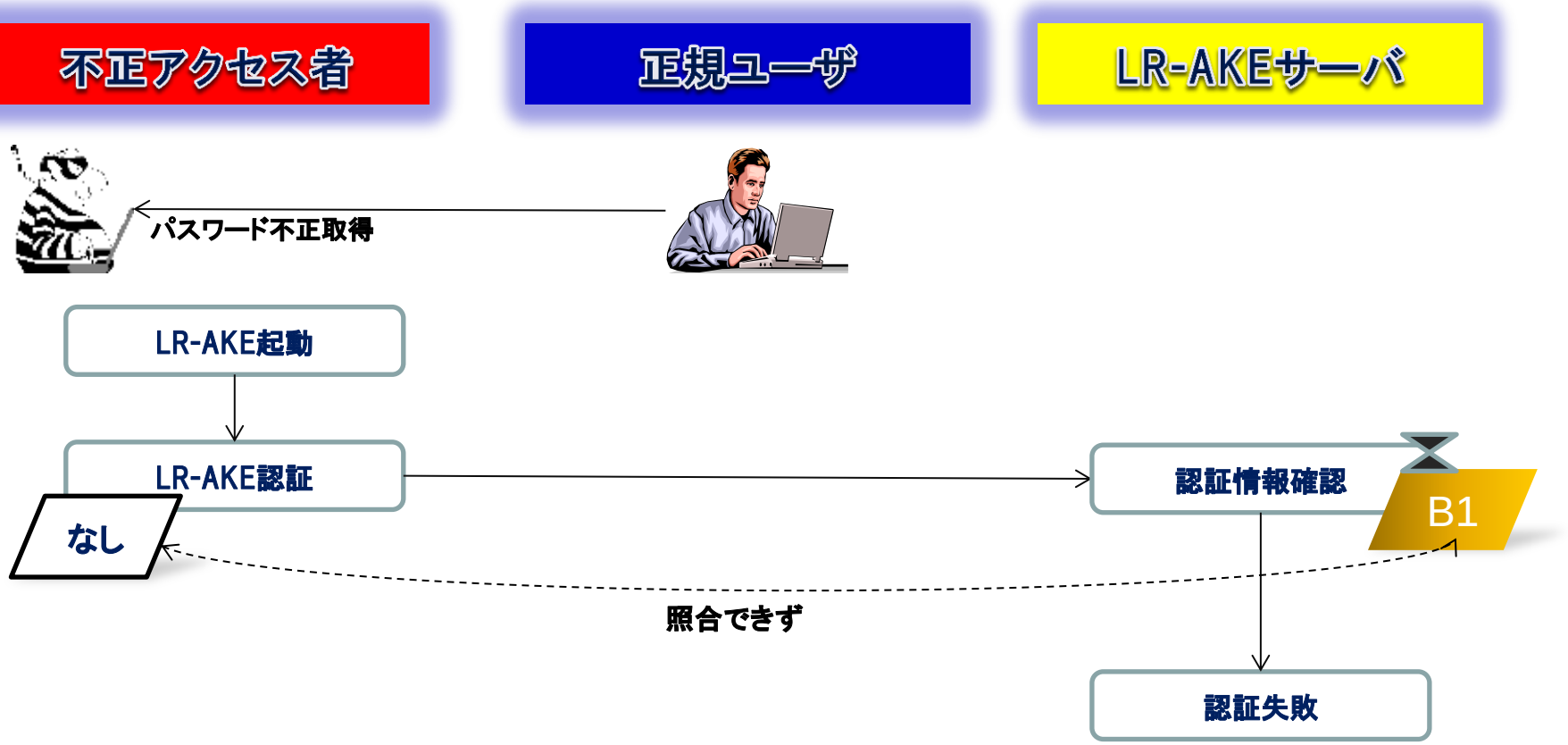
※LR-AKE認証の成功の度に対となる双方の認証情報は書き代わります。

Acrive Directory等連携認証



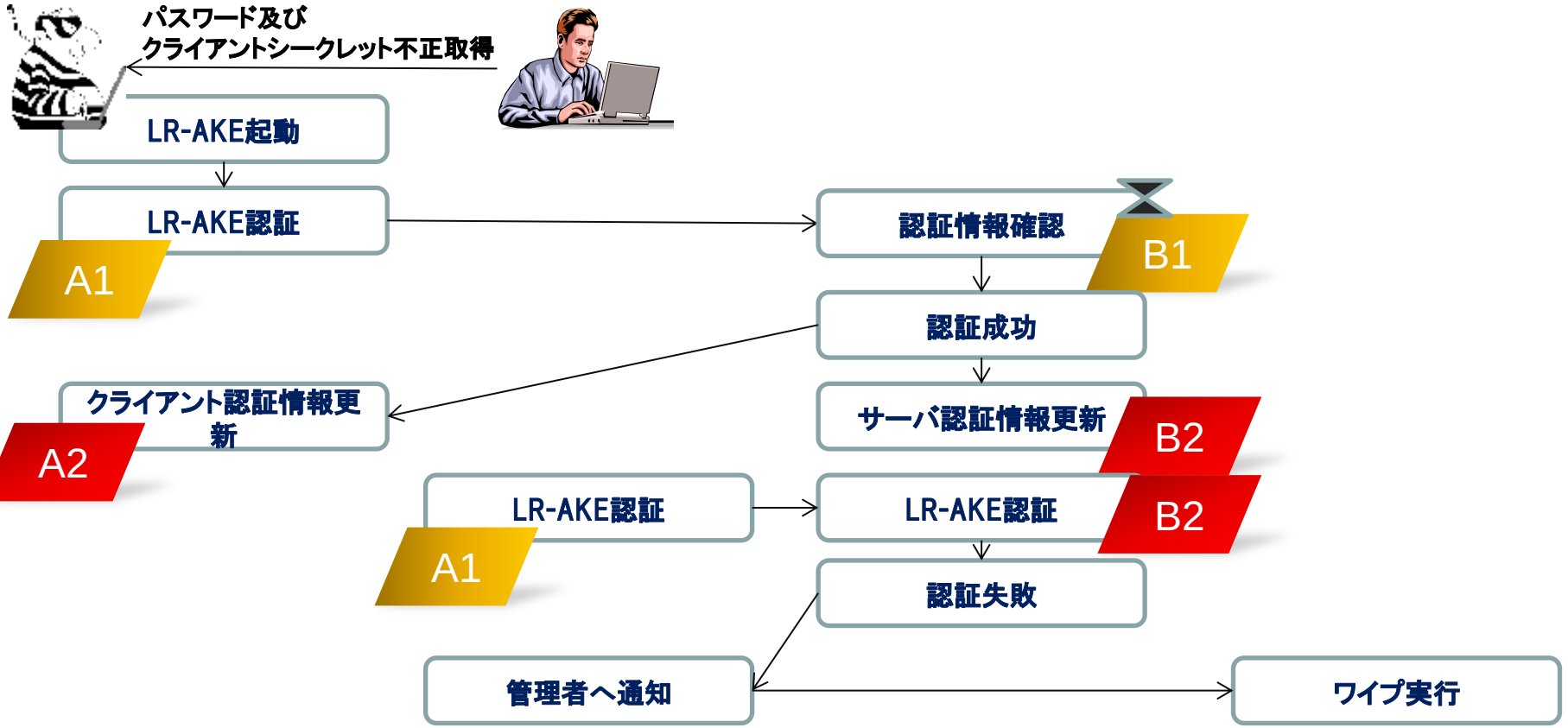
不正アクセスパターン

アクセスコードを不正取得した流れ



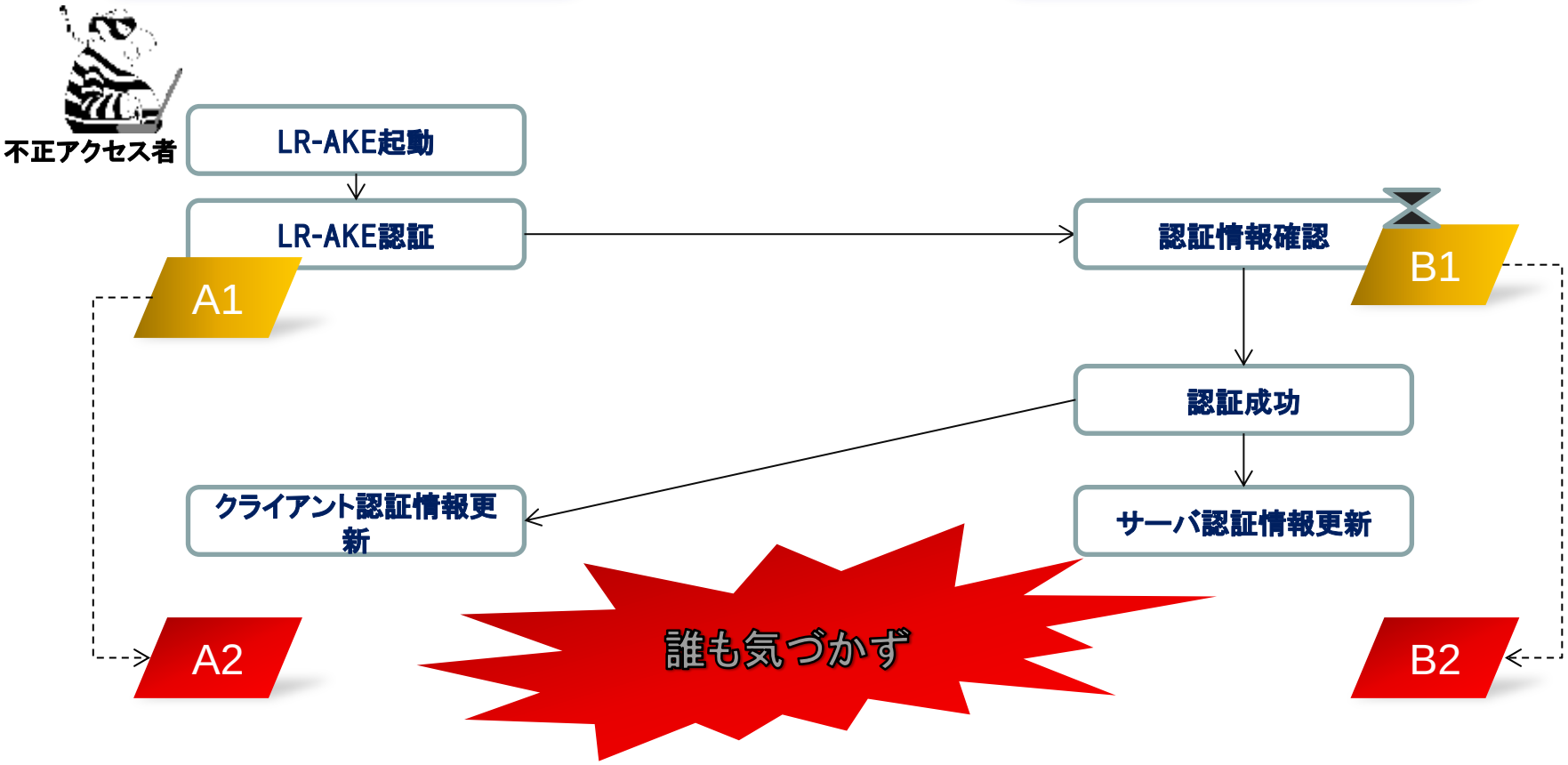
※不正アクセス者にLR-AKEクライアントソフトがインストールされていることが前提

アクセスコード及びクライアント認証情報を不正取得した流れ



※不正アクセス者にLR-AKEクライアントソフトがインストールされていることが前提

正規ユーザのPCにてなりすましたケース



※不正アクセス者はアクセスコードを知っていることが前提

脅威・脆弱性について

脅威
ユーザ端末からクライアント認証情報が盗まれる
脆弱性
不用意な管理によるパスワード漏洩

対策
クライアント認証情報とパスワードの両方が盗まれ、かつ即時にログインしない限り安全です。またパスワードは短くて良いためメモ等に書留める運用をさければ安全です。

脅威
中間者攻撃にて盗聴されパスワードを解析される
脆弱性
非暗号化やパスワードが平文で通信路を流れる仕組み

対策
LR-AKEは通信プロトコルであるため、サーバとのやりとりは暗号化されております。また、パスワードそのものは通信経路を流れ為、通信経路で盗聴はされません。

脅威
サーバからハッシュ化されたパスワードが盗まれパスワードを解析される
脆弱性
サーバへの侵入に対する防御の甘さ

対策
LR-AKEはサーバ認証情報にはパスワードが保存されておらず(ハッシュ化もしていない)、万が一サーバ認証情報が漏えいしてもパスワード解析は不可能です