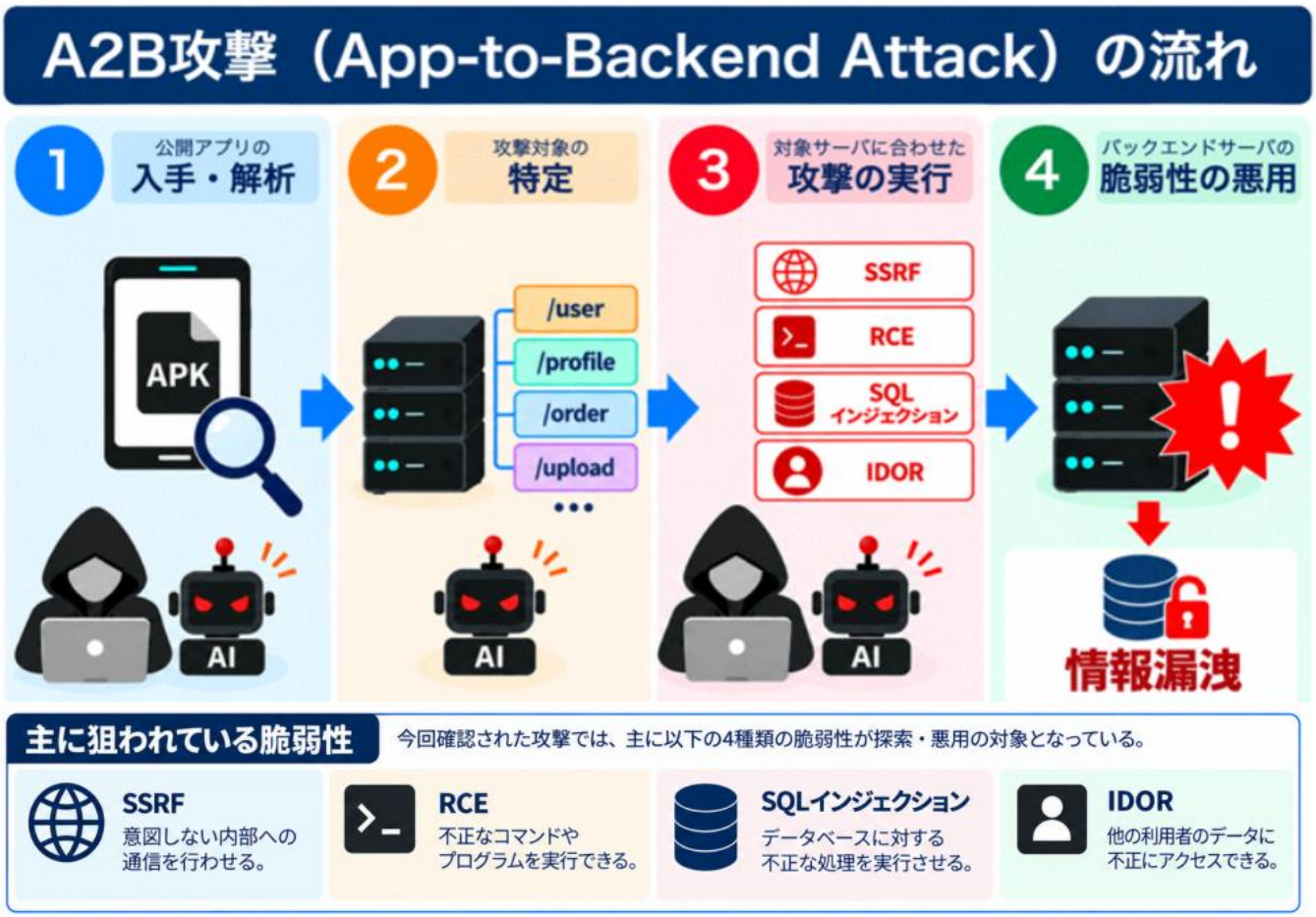
KBCS だより
令和８年　Ｎｏ．２５

A2B攻撃にご注意ください！

～アプリをきっかけに、サーバが狙われる新たなサイバー攻撃～

A2B攻撃とは？

攻撃者が、公開されているアプリを解析し、アプリの接続先であるサーバを狙う攻撃手法です。
アプリ自体に脆弱性がなくても、その裏側のサーバやＡＰＩの脆弱性を利用したサイバー攻撃によって、情報漏えいや不正操作が行われるおそれがあります。



引用：https//cynex.nict.go.jp/library/261013-01.html
ＮＩＣＴ（国立研究開発法人情報通信研究機構）脅威情勢分析チームLETTICE
【注意喚起】相次ぐ情報漏洩、その原因の一つは「アプリ解析からのサーバ攻撃」

企業が実施すべき対策

① 侵害の確認
ＡＰＩおよびインターネット上に公開しているホストについて、不審なアクセスや侵害の有無を優先的に確認してください。

② 脆弱性の点検
ＡＰＩおよび公開ホストについて、脆弱性や設定不備が存在しないか優先的に点検してください。

③ 暫定的な緩和策
攻撃による被害の発生や拡大を防止するため、業務への影響を考慮しながら、必要に応じて暫定的な緩和策を実施してください。

京都事業者サイバーセキュリティ支援ネットワーク
【公式ホームページ】 https://www.ksisnet.kyoto
【発行元】事務局：京都府警察サイバー対策本部

京都府警察サイバー対策本部公式Ｘアカウントです。
ぜひ、フォロー・いいね！をお願いします♪

@KPP_cyber