栃木県警察サイバー対策センター
TOCHIGI POLICE
CYBERCRIME CONTROL CENTER

公開アプリを悪用した「A2B攻撃」について
～AIを駆使した攻撃者による「アプリ解析からのサーバ攻撃」～

令和８年10月13日、国立研究開発法人情報通信研究機構（NICT）は、8月下旬頃から、国内で相次いでいる企業での不正アクセスによる情報漏えい事案の原因の一部（攻撃手法）を特定したことを発表しました。

その攻撃手法とは、

一般に公開されているAndroidアプリを解析し、その情報を悪用してアプリの接続先であるサーバを攻撃する

といった手法で、

A2B攻撃（App-to-Backend Attack）

と名付けられています。

A2B攻撃の特徴は、

不特定多数のサーバに同一の攻撃を試みるのではなく、公開アプリから得られる情報を手がかりとして、対象となる個々のサーバごとに内容を変化させた攻撃が行われている

といった点です。

【A2B攻撃の流れと主に狙われている脆弱性】



出典　NICT　【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」



AIの活用によって、攻撃者によるアプリ解析や脆弱性探索が効率化されています。

アプリを公開している事業者につきましては、「公開アプリが解析されること自体を完全に防ぐことは困難」ということを前提に、サーバ側のぜい弱性に対する対策を徹底することが重要です。