AMT/NEWSLETTER
Cyber & AI Security

2026年11月13日

内閣官房国家サイバー統括室、「個人情報の漏えい等につながる不正アクセスへの対策について～ウェブサイトやモバイルアプリに関する基本的な対策の徹底～」を公表

弁護士 清水 亘 / 弁護士 髙橋 麟太朗

Contents

Ⅰ. はじめに

Ⅱ. 背景

Ⅲ. 概要

Ⅳ. 主なポイント
1. 運用・管理段階
2. 設計・開発段階
3. サプライチェーン

Ⅴ. まとめ

Ⅰ. はじめに

内閣官房国家サイバー統括室は、2026年11月5日、「個人情報の漏えい等につながる不正アクセスへの対策について～ウェブサイトやモバイルアプリに関する基本的な対策の徹底～」（以下「本対策」という。）を公表した[1]。

本対策の対象は、特にウェブサイトやモバイルアプリを使用した事業を運用し、個人情報を取り扱っている事業者等であり、それらの事業者に対し、改めて基本的な対策の徹底を求めている。

本対策には、二つの内容が盛り込まれており、①経営層をはじめ組織内の幅広い層に向けた基本的な考え方と、②ITシステム・サイバーセキュリティ担当者に向けた具体的な対策例である。

1 https://www.cyber.go.jp/pdf/press/261105_taiou.pdf

II. 背景

政府は、昨今相次いで発生している不正アクセスによる情報漏えい事案について、原因とみられる問題を確認している。具体的には、モバイルアプリ開発時のセキュリティ対策不足、ウェブサイト等の設定不備、サポートが終了しているソフトウエアや既知の脆弱性が未対策のソフトウエアの継続使用などである。つまり、本対策によれば、自組織又は委託先における基本的な対策が十分でなかったことが原因とみられる事例を複数確認しているという。

本対策によれば、こうした事例において、攻撃者は、インターネット上に公開されている我が国のウェブサイト等を標的として大規模な調査を行い、侵入方法が発見されたウェブサイト等に侵入して個人情報を窃取したとみられる。攻撃者が標的の調査や侵害に AI を使用している可能性も高い。また、これまでの脆弱性診断では比較的低いと評価されたリスクであっても、それが組み合わされることで侵入の原因となった可能性のある事例もみられる。さらに、攻撃の大規模化が容易になることで、事業規模の大小を問わず、幅広い事業者が攻撃対象となっていると考えられる。

III. 概要

本対策は、大きく三つの柱で構成されている。

運用・管理段階	● デジタル資産の適切な把握及び脆弱性の解消 ● アタックサーフェスの継続的な棚卸し及び最小化 ● AI の活用等による継続的な脆弱性診断及び不審な挙動の監視
設計・開発段階	● セキュリティ・バイ・デザインの適用 ● 利用する API のセキュリティ対策の強化 ● 公開前の脆弱性診断の実施
サプライチェーン	● 委託先のセキュリティ統制及び委託先からの接続経路の厳格化 ● オープンソースソフトウエア（OSS）や外部ライブラリ等の適切な管理

筆者まとめ

各項目には担当者向けの対策例が示され、末尾には参考資料が付されている。

IV. 主なポイント

本対策の主なポイントは、次のとおりである。

1. 運用・管理段階

ソフトウエアは、運用開始後に新たな脆弱性が発見・公表されることがある。そのため、利用するソフトウエアの構成要素やバージョン、利用箇所等を継続的に把握することが重要とされる。あわせて、自組織への影響を速やかに特定・対処できる体制の確保も求められる。本対策では、対策例として、SBOM（Software Bill of Materials：ソフトウエア部品表）やSCA（Software Composition Analysis：ソフトウエア構成解析）の活用、米国 CISA（米国サイバーセキュリティ・インフラストラクチャセキュリティ庁）の KEV（Known Exploited Vulnerabilities：既知の悪用された脆弱性）カタログに掲載されている脆弱性の優先確認などが挙げられている。

また、近時、本来は外部への公開を想定していないデバッグ用機能やシステム管理用エンドポイント等に対する不正アクセスも確認されている。このため、アタックサーフェスを最小化することが重要とされる。

さらに、AI を活用した攻撃に対応するため、防御側においても AI 技術の活用を積極的に検討することが重要とされている。ただし、AI による評価結果については、最終的な対応判断を人が確認するとしている。

2. 設計・開発段階

「後から守るのではなく、最初から安全に作る」という考え方に基づき、セキュリティ・バイ・デザインによる設計・開発を推進することが重要である。

近時は、API 経由の情報漏えいも報告されている。代表例が、NICT が注意喚起している A2B（App-to-Backend）攻撃である。対策例としては、認可不備の排除や、API キー等の認証情報をソースコードへ直接書き込まないこと（ハードコーディングしないこと）、レート制限の実装も挙げられている。

公開前には、リリース前に脆弱性診断やペネトレーションテスト（侵入テスト）を実施することが重要である。また、一定以上のリスクを有する脆弱性が残存する状態で本番公開を行わない方針を定めることも例示されている。

3. サプライチェーン

委託先が利用するリモート接続環境は、攻撃者にとって、正規の認証情報を用いた侵入口となり得る。それでも、サービス停止や情報漏えいに伴う影響は発注元である事業者自身が負うことになる。また、個人情報保護法第 25 条は委託先に対する必要かつ適切な監督を求めているが、取引上の地位を利用した一方的な負担の押し付けとならないよう留意することが必要である。

具体策としては、多要素認証（MFA）の適用、契約・調達におけるセキュリティ要件の明確化、ゼロトラストの考え方に基づくアクセス制御が挙げられている。OSS については、外部のソフトウエア部品を中身の分からないまま利用し続けることを避ける必要がある。そのための対策例として、委託開発における SBOM の提出と確認などが示されている。

Ⅴ. まとめ

本対策は、直近の一連の攻撃手口に焦点を当てたものである。そのうえで、ほかの手口も想定した対策を講じる必要があるとしている。具体的には、VPN 等のネットワーク機器の脆弱性を狙った攻撃、標的型メール攻撃、DDoS 攻撃などの手口に加え、AI の悪用が高度化・巧妙化する可能性である。

また、本対策は、サイバー攻撃による影響が経営リスクへと発展する可能性も考慮に入れるよう求めている。そのうえで、経営トップの判断の下でリスク評価を行い、必要なサイバーセキュリティ対策を強化するよう要請している。

企業においては、本対策の公表を契機として、事業規模を問わず、自社と委託先を含むサプライチェーンにおける基本的な対策を改めて点検したい。

以上

- 本ニュースレターの内容は、一般的な情報提供であり、具体的な法的アドバイスではありません。お問い合わせ等ございましたら、下記弁護士までご遠慮なくご連絡下さいますよう、お願いいたします。

- 本ニュースレターの執筆者は、以下のとおりです。

弁護士 清水 亘　　wataru.shimizu[at]amt-law.com
弁護士 髙橋 麟太朗　　rintaro.takahashi[at]amt-law.com
※メールを送信する際には、[at]を@に変更してお送りください。

- ニュースレターの配信停止をご希望の場合には、お手数ですが、お問い合わせにてお手続き下さいますようお願いいたします。

- ニュースレターのバックナンバーは、こちらにてご覧いただけます。