参考資料２－２

事　務　連　絡
令和８年11月５日

総務省所管事業者　各位
総務省所管・関係団体　各位

総務省サイバーセキュリティ統括官室

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

不正アクセスによる情報漏えい事案において、モバイルアプリの開発時におけるセキュリティ対策不足やウェブサイト等の設定不備、既知の脆弱性への未対応等、**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が複数確認**されています。

また、攻撃者は標的の調査や侵害にAIを使用している可能性も高く、従来は比較的低リスクと評価されていた脆弱性等を組み合わせて侵入した可能性も指摘されています。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ています。

このような状況を踏まえ、内閣官房国家サイバー統括室から、別添のとおり、**ウェブサイトやモバイルアプリにおける基本的な対策の徹底**として、脆弱性や設定不備への適切な対処及び継続的なセキュリティ診断・監視の強化、設計・開発段階からのセキュリティ対策の徹底、委託先を含めたサプライチェーン全体の対策強化等について、改めて基本的な対策を徹底していただくよう、通知が発出されましたので、注意喚起としてお知らせいたします。

経営層におかれましては、サイバーセキュリティの重要性を十分に御認識いただき、リーダーシップを発揮して対策の一層の強化に取り組んでいただくとともに、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、個人情報を取り扱う事業者等におかれましては、御注意ください。

総務省所管・関係団体におかれましては、貴団体加盟各社への周知をお願いいたします。

事業者向け

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～

２０２６年１１月５日
内閣官房国家サイバー統括室

政府では、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おいて、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ェアや既知の脆弱性が未対策のソフトウェアの継続使用など、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おります。

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、調査で侵入方法が発見されたウェブサイト等に侵入し、個人情報を窃取したとみられます。標的の調査や侵害にAIを使用している可能性も高く、AIが悪用されたことで、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ます。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ます。

こうした状況を踏まえ、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におかれましては、こうした攻撃手口による不正アクセスを防ぐため、以下の対策事項をご確認いただき、改めて基本的な対策の徹底をお願いいたします。

経営層をはじめ、組織内の幅広い皆様に向け、本対策の基本的な考え方やその背景にある状況について柱書に整理しておりますので、ご一読ください。また、ITシステム・サイバーセキュリティ担当者の皆様に向け、具体的な対策例を記載しております。各組織における対策の検討・実施にあたっての参考としてご活用いただければ幸いです。

１．運用・管理段階におけるセキュリティ対策の徹底

（１）デジタル資産の適切な把握及び脆弱性の解消

不正アクセスによる情報漏えい等の事案においては、ウェブアプリの中で使われているライブラリやフレームワーク等に存在する脆弱性を悪用し、組織内のシステムへの不正アクセスや情報窃取等を試みる攻撃が確認されております。特に、リモートの攻撃者が悪用可能な脆弱性については、組織内部への侵入の足掛かりとして悪用されるおそれがあります。

ソフトウェアは、導入時点で脆弱性が発覚していなかった場合においても、運用開始後に新たな脆弱性が発見・公表されることがあります。また、直接利用する製品だけでなく、当該製品に組み込まれたオープンソースソフトウェア（OSS）やライブラリ等の構成要素にも脆弱性が存在する可能性があります。

このため、組織において利用するソフトウェ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とともに、新たに公表される脆弱性情報及び悪用動向を収集し、自組織への影響を速やかに特定・対処できる体制を確保することが重要となります。特に、インターネットからアクセス可能なサーバーやネットワーク機器等については、攻撃者による悪用のリスクを踏まえ、優先的に対応する必要があります。

（サイバーセキュリティ担当者等向け）

・対策例 1. ソフトウェア構成情報の把握・管理：

新たな脆弱性が公表された際に、自組織への影響の有無及び影響範囲を迅速に特定できるよう、OS、ミドルウェア、フレームワーク、ライブラリ等について、製品名、バージョン、利用箇所等の構成情報を把握・管理する。また、必要に応じてソフトウェア部品表（SBOM）やソフトウェア構成解析（SCA）等を活用し、構成情報を継続的に更新する（参考資料 1-1）。なお、SBOM の活用に際しては、脆弱性情報との継続的な照合、影響範囲の特定、修正又は緩和策の実施までを一連の運用として確保する必要があることに留意する。

・対策例 2. 脆弱性情報の継続的な収集及び影響確認：

米国 CISA の KEV（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等、実際に悪用が確認されている脆弱性について、自組織で利用するソフトウェアへの影響を優先的に確認する。また、製品ベンダー、NVD（米 NIST が運営する脆弱性データベース）、JVN（一般社団法人 JPCERT コーディネーションセンター及び独立行政法人情報処理推進機構(IPA)が共同運営する脆弱性データベース）等が公表する脆弱性情報及び悪用動向を継続的に収集し、管理するソフトウェア構成情報と照合することで、影響の有無及び影響範囲を速やかに特定する。必要に応じて、脆弱性検知を自動化するための脆弱性管理ツールを活用する。

（サイバーセキュリティ担当者等向け）

・対策例 3. 脆弱性対処の優先順位及び対応期限の決定：
脆弱性への対応を適切に優先順位付けするため、脆弱性の深刻度、実際の悪用状況、インターネット経由での悪用可能性、システムの重要度及び事業への影響等を踏まえた評価基準をあらかじめ策定する。当該基準に基づき対応の優先順位及び期限を決定し、修正プログラムの適用やバージョンアップ等の対処を実施する（参考資料 1-2、1-3）。

・対策例 4. 緩和策の実施及び是正状況の管理：
修正プログラムの適用が直ちに困難な場合は、製品ベンダーが公表するセキュリティアドバイザリ等を確認し、影響を受ける機能の停止、アクセス制限等の暫定的な緩和策を講じる。また、修正プログラムの適用や緩和策の実施後は、その有効性を確認するとともに、未対応の脆弱性や残存リスクを管理し、恒久的な対処が完了するまで継続的に確認する。特に、既に悪用が確認されている脆弱性については、関連するログ等を確認し、侵害の兆候の有無についても調査する。

（２）アタックサーフェスの継続的な棚卸し及び最小化

不正アクセスによる情報漏えい等の事案においては、業務上不要な機能やサービスが外部に晒されていたことに起因するインシデントが発生しています。具体的には、インターネットに公開されたシステム管理画面に対し、推測されやすい認証情報の悪用、総当たり攻撃、認証機能の脆弱性を悪用した認証回避等により不正アクセスが行われたことが確認されています。他にも、本来は外部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がインターネットからアクセス可能な状態となっていたことにより、不正アクセスが行われたことが確認されています。

このように、業務上不要な機能やサービスの外部公開は、攻撃者に新たな侵入経路や情報窃取の機会を与える要因となります。そのため、インターネットに公開されているウェブアプリやウェブサービスについて、公開範囲やアクセス制御、設定状況等を継続的に点検し、意図しない公開や不要な機能等を速やかに解消することで、インターネット上に露出している攻撃対象領域（アタックサーフェス）を最小化することが重要となります。

（サイバーセキュリティ担当者等向け）

・対策例 1. アタックサーフェスの把握：

ネットワーク構成情報、クラウドサービスの設定情報、既存の資産台帳等から、インターネットに公開している IP アドレス、FQDN（Fully Qualified Domain Name）、サービス、通信ポート、ウェブアプリ、API 等を洗い出す。また、ASM（Attack Surface Management）等を活用して外部から観測可能な資産を探索し、内部の管理情報と突合することで、管理対象から漏れている資産や意図しない公開状態を把握する。把握した資産については、管理責任者、用途、公開の必要性等を確認し、継続的に管理する（参考資料 1-4）。

・対策例 2. 不要な公開機能の停止・制限：

✓ アプリケーション：インターネットに公開されている管理画面、デバッグ用エンドポイント、開発・検証環境、データベース管理機能等について、外部からのアクセス可否及び公開の必要性を点検する。特に、リバースプロキシ、ロードバランサー、API ゲートウェイ等における URL パスやホスト名に基づく振り分けルール、ルールの優先順位、想定外の URL パスに対するデフォルトの転送・応答動作等を確認し、本来公開すべきでない機能に外部から到達できないことを検証する。不要な機能は停止・無効化し、管理上必要な機能についても、アクセス元制限、多要素認証等を組み合わせて保護する。

✓ ネットワーク/クラウド：クラウドサービス、ネットワーク機器、ウェブサーバー等について、インターネットへの公開範囲やアクセス制御に関する設定を点検する。特に、クラウドストレージのアクセスや外部共有設定、ファイアウォール等における不要な通信の許可、ウェブサーバーにおける意図しないファイル公開等を確認する。設定不備が認められた場合には、不要な公開設定の削除、アクセス権限の見直し、公開範囲の制限等により速やかに是正する。また、是正後は外部からのアクセス確認等を通じて、意図しない公開が解消されたことを検証する。

・対策例 3. 継続的な外部露出の監視：

システムの新設・変更や設定変更等に伴い、新たな外部公開資産や意図しない公開状態が生じる可能性があることを踏まえ、インターネットから観測可能な資産やサービスの公開状況を継続的に点検する。既存の資産台帳や過去の点検結果と突合し、未把握の資産や公開状態の変化を検出する。意図しない公開が認められた場合には速やかに是正する。

（3）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

従来から、構築時のセキュリティ対策だけでなく、運用開始後も継続的にセキュリティ診断や点検を実施し、脆弱性や設定不備等の発見や、ログ監視やシステム上の不審な挙動の検知を通じて、侵害の兆候を早期に把握・対処することが重要とされてきました。

一方、AI を活用した脆弱性の探索や攻撃手順の自動化等、サイバー攻撃への AI 技術の活

用が進展しており、攻撃の高度化・効率化が懸念されています。これにより、従来の対策を継続・強化することに加え、新たな脅威や攻撃手法の変化に迅速に対応できる体制の確保が一層重要となっています。

このため、従来から実施されてきたセキュリティ診断や監視・検知、インシデント対応等の取組を着実に継続・強化するとともに、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なります。有効性や適用範囲、運用上のリスクを十分に検証しながら導入・活用を進め、セキュリティ運用の迅速化・高度化を図ることが求められます。

具体的には、ウェブサイトやモバイルアプリの公開前だけではなく、認証・認可、API、個人情報の取扱い等に係る重要な変更時及び運用開始後も、リスクに応じて継続的に診断、点検及び監査を実施し、検出された脆弱性を是正した上で、その結果を確認することが必要です（参考資料 1-5、1-6）。

（サイバーセキュリティ担当者等向け）

・対策例 1. 継続的なセキュリティ診断及び点検：
ウェブアプリ、API、ネットワーク機器、クラウド環境等について、定期的な脆弱性診断やペネトレーションテストを実施するとともに、システムの重要な変更時にも必要な診断・点検を行う。さらに、AI を活用したセキュリティ診断ツール等の導入・活用を積極的に検討し、診断対象の攻撃経路の探索、テストケースの生成、脆弱性の検証、検出された問題の影響分析や対応優先度の評価支援等を通じて、効率化を図る。AI による評価結果については、根拠や妥当性を確認し、最終的な対応判断については人による確認を行う。

・対策例 2. ログ及びワークロードの継続的な監視・検知：
ウェブサーバー、API ゲートウェイ、認証基盤、クラウドサービス等のログを取得し、SOC（Security Operation Center）による監視体制や SIEM（Security Information and Event Management）によるログの集約・相関分析等を通じて、不審な認証、権限の不正使用、大量のデータ取得等を継続的に監視する。また、EDR（Endpoint Detection and Response）等を活用し、端末、サーバーにおける不審なプロセスの実行や通信等の挙動を継続的に監視・検知する。さらに、AI を活用したセキュリティ監視・運用等の導入・活用を積極的に検討し、AI による大量のログやアラートの横断的な分析、異常な挙動や攻撃の兆候の検出、複数の事象の関連付け、調査対象の優先順位付け等を通じて、従来の監視では把握が困難な不審な活動の早期発見や、セキュリティ担当者の負荷軽減、検知・分析の迅速化及び高度化を図る。

（サイバーセキュリティ担当者等向け）

・対策例 3. インシデントの調査・対処の迅速化：
不審な挙動や侵害の兆候を検知した場合に、関連するログやシステムの状態を速やかに調査し、不正アクセスの有無及び影響範囲を確認できる体制を整備する。また、SOAR（Security Orchestration, Automation and Response）等を活用した調査・対応手順の自動化に加え、AI によるアラートの要約、関連情報の収集・分析、対応手順の提案等の活用を検討し、初動対応の迅速化を図る。なお、AI による分析や自動対処については、誤検知・誤判断や業務への影響を考慮し、適切な検証及び人による監督の下で実施する。

２．設計・開発段階におけるセキュリティ対策の徹底

（１）セキュリティ・バイ・デザインの適用

昨今のサイバー攻撃の傾向を踏まえると、モバイルアプリやウェブクライアント及びそれらのバックエンドサーバーは、必ずしもセキュリティ・バイ・デザインの考え方に基づいて設計されていないことも多く見受けられることから、セキュリティを考慮した設計・開発を徹底することが重要です。万が一、脆弱性や設定不備がリリース後に発覚した場合、後から修正するコストは設計時に防止する場合と比較して大幅に増加するほか、サービス停止や情報漏えい等の重大なインシデントにつながるおそれがあります。そのため、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、要件定義から運用までのライフサイクル全体にセキュリティを組み込むセキュリティ・バイ・デザイン（参考資料 2-1、2-2、2-3）による設計・開発を推進することが重要となります。

（サイバーセキュリティ担当者等向け）

・対策例 1. 要件定義・設計フェーズにおけるセキュアなアーキテクチャの検討：
要件定義・設計フェーズにおいては、脅威モデリングを実施し、想定される攻撃経路やアタックサーフェスを把握した上で、認証・認可、暗号化、ログ取得、アクセス制御等のセキュリティ要件を明確化する。また、管理機能や運用機能をインターネットへ不用意に公開しないネットワーク構成や、ゼロトラストの考え方を踏まえたアクセス制御等についても設計段階から検討する。加えて、取り扱う情報の内容に応じて、アプリケーション、データベース、運用管理機能等を単にネットワーク上で分離するだけでなく、システムの重要度及びリスクに応じて、クラウドのアカウント、サブスクリプション等の管理境界を分離することを検討する。なお、システムを設計する際には、非機能要件を含む設計基準の策定において、認証・認可、可用性、ログ取得、監視、障害対応、バックアップ、データ保護等の非機能要件を体系的に検討し、要件定義、設計、調達、開発、検収及び運用の各段階で確認すべき項目を明確化する。

（サイバーセキュリティ担当者等向け）

・対策例 2. 実装フェーズにおけるセキュリティツール（SAST、SCA）の活用：
実装フェーズにおいては、静的アプリケーションセキュリティテスト（SAST）やソフトウェア構成解析（SCA）を活用し、開発段階からセキュリティ上の問題を早期に検知する。これにより、危険な関数の利用やセキュアコーディング違反、利用している OSS やライブラリに含まれる既知の脆弱性等を継続的に把握する。また、必要に応じて、SBOM を活用することで、利用しているソフトウェア構成要素の可視化及び脆弱性管理を効率的に実施する。

・対策例 3. テストフェーズにおけるセキュリティツール（DAST、IAST）の活用：
テストフェーズにおいては、動的アプリケーションセキュリティテスト（DAST）や対話型アプリケーションセキュリティテスト（IAST）を活用し、実際に稼働するアプリケーションに対するセキュリティ検証を実施する。特に、認可不備、入力値検証不備、セッション管理の不備等、自動解析によって検出可能な問題について継続的に確認し、必要に応じて手動による検証も行い、リリース前に是正する。また、必要に応じて、これらのセキュリティテストを継続的インテグレーション/継続的デリバリー（CI/CD）パイプラインへ統合し、開発ライフサイクル全体を通じた継続的なセキュリティ確保につなげる。

（２）利用する API のセキュリティ対策の強化

不正アクセスによる情報漏えい等の事案においては、ウェブアプリやモバイルアプリが利用する API 経由での不正な操作によって情報漏えいが発生していることが確認されています。国立研究開発法人情報通信研究機構（NICT）が注意喚起している「A2B（App-to-Backend）攻撃」に代表されるように、公開アプリケーションの解析を通じて API エンドポイントの脆弱性や認可不備を特定し、バックエンドから機密情報を不正に窃取するインシデントが報告されています（参考資料 2-4）。

そのため、ウェブアプリやモバイルアプリにおける外部連携を支えるバックエンド API に対しては、堅牢な認証・認可の実装、厳格な入力値検証の徹底、認証情報の安全な管理及び異常アクセスの検知・制御を実施することが重要となります。

（サイバーセキュリティ担当者等向け）

・対策例 1. 認可不備の排除：
API における認可不備は、認証された利用者が本来アクセス権限を持たない情報や機能へアクセスできる状態を生み出し、情報漏えいや不正操作につながるおそれがある。そのため、API リクエストが要求した機能及びデータに対する正当な権限を利用者が有することをサーバー側で検証するとともに、最小権限の原則に基づくアクセス制御を実装する。認可不備は、大きく「オブジェクトレベルの認可不備（BOLA)」と「機能レベルの認可不備（BFLA)」に分類される（参考資料 2-5、2-6)。

・対策例 2. 認証情報の安全な管理：
ソースコードやアプリケーションパッケージ内に、API キー、アクセストークン、秘密鍵、データベース接続情報等の認証情報が埋め込まれている場合、ソースコードの漏えいや、アプリケーション解析によって、認証情報が窃取される可能性がある。そのため、API キーやアクセストークン等の認証情報は、ソースコードへハードコーディングせず、サーバー側ではシークレットマネージャー等を利用して認証情報を管理する。また、認証情報には必要最小限の権限のみを付与するとともに、漏えい時の影響を低減するため、有効期間の設定や定期的なローテーションを実施する。開発プロセスにおいては、ソースコード管理リポジトリへのコミット時や CI/CD パイプラインにおいてシークレットスキャンを実施し、認証情報の混入を早期に検知できる仕組みを整備する（参考資料 2-7)。

・対策例 3. API レート制限による不正利用対策の実装：
API は自動化されたツールによる総当たり攻撃や認証試行、情報収集等の対象となることがあるため、不正利用を抑止するための対策を実装する。特に、認証機能やパスワードリセット機能等については、短時間に大量のリクエストが送信された場合にアクセスを制限するレート制限を実装するとともに、同一 IP アドレスや同一アカウントからのアクセスに限らず、複数の IP アドレス等からのアクセスも含め、認証の成功・失敗の状況やアクセス頻度等を踏まえて、異常なアクセスを検知できる仕組みを設ける（参考資料 2-8)。

（３）公開前の脆弱性診断の実施

不正アクセスによる情報漏えい等の事案においては、SQL インジェクション、OS コマンドインジェクション、リモートコード実行（RCE)、サーバーサイドリクエストフォージェリ（SSRF)、ディレクトリトラバーサル等の脆弱性を悪用した攻撃による情報漏えい事案が発生しています。

そのため、個人情報を取り扱うウェブアプリやウェブシステムにおいては、リリース前に脆弱性診断やペネトレーションテストを実施し、潜在的な脆弱性を事前に発見・修正することが重要です。また、その際には、診断の目的や対象範囲を明確にするとともに、検出され

た脆弱性に対して適切な是正措置を実施し、その結果を確認した上で本番環境へ公開することが重要となります。

なお、脆弱性診断の実施にあたっては、製品やプラットフォームに存在する既知の脆弱性への対応だけでなく、自社又は委託先が開発したウェブアプリやモバイルアプリのバックエンド機能に固有の設計・実装上の脆弱性も、診断及び是正の対象とする必要があります。

また、ウェブアプリの技術的な検証項目については、対象システムの特性及びリスクに応じて診断範囲を定めることが重要となります（参考資料 2-9）。

（サイバーセキュリティ担当者等向け）

・対策例 1. セキュリティ基準の設定：
脆弱性診断を実施する際は、あらかじめ受容可能なリスク水準を定め、その基準に基づいてリリース可否を判断する運用を整備する。例えば、脆弱性の深刻度評価や悪用可能性、システムの重要度等を踏まえたセキュリティゲートを設定し、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。また、診断結果に対する修正責任者や対応期限の明確化や、修正漏れを防止する仕組みを整備する。

・対策例 2. 適切な第三者ベンダーの選定：
脆弱性診断やペネトレーションテストを第三者へ委託する場合は、対象システムの特性や利用技術を踏まえ、十分な技術力や実績を有する事業者を選定する。特に、ウェブアプリ診断、API 診断、モバイルアプリ診断等の実施実績や診断手法、診断体制等を確認するとともに、情報セキュリティサービス基準に適合したサービスを提供している事業者を選定する（参考資料 2-10）。また、自動診断のみならず、手動による検証や業務ロジックを考慮した診断が実施されるかどうかについても確認する。

３．サプライチェーンを通じた侵害への対策

（１）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

業務委託先や保守事業者の環境を足掛かりとして、発注元のシステムへ侵入される事案が確認されています。特に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」となり得ます。こうした場合でも、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ります。

また、個人情報の取扱いを委託する場合には、個人情報の保護に関する法律第 25 条により、委託先に対する必要かつ適切な監督が求められています（参考資料 3-1）。そのため、委託先を含めたサプライチェーン全体を管理・統制の対象として捉え、ガバナンスの行使と接続経路の多層防御を両輪として、次の対策例を参考に対策を検討してください。なお、委託先に対策を求める際は、費用負担や実施方法について十分に協議し、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してください（参考資料 3-2）。

（サイバーセキュリティ担当者等向け）

・対策例 1. 委託先からの接続経路の保護及びアカウントの保護：
委託先が利用する VPN、リモートデスクトップ、保守用回線等の接続経路を洗い出し、多要素認証（MFA）を適用する。
- ✓ 重要度の高い経路から計画的に多要素認証へ切り替える
- ✓ 多要素認証の適用が困難な経路には、接続元 IP アドレスの制限、作業時のみの接続開放、作業記録の取得等の代替策を講じる
- ✓ 接続経路の管理とあわせ、作業が完了した委託先のアカウントや、常時付与されたままの管理者権限を棚卸しし、無効化・最小化する

・対策例 2. 契約・調達におけるセキュリティ要件の明確化：
発注仕様書や業務委託契約書に、秘密保持義務に加え、再委託の手続き、インシデント発生時の通知義務・連絡先、契約終了時のデータ消去等の要件を盛り込む（参考資料 3-3)。
- ✓ 委託先の選定時には、第三者認証や「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度)」(2027 年 3 月申請受付開始予定）等の客観的な評価を活用する（参考資料 3-4)

・対策例 3. ゼロトラストの考え方に基づくアクセス制御：
一度接続すると社内ネットワークに幅広くアクセスできる境界型 VPN のみへの依存から脱却する。委託先の作業員ごとに、認可された端末から必要なサーバー・機能のみへ通信を限定するなど、ゼロトラストの考え方に基づくアクセス制御の強化を図る（参考資料 3-5)。

（２）オープンソースソフトウェア（OSS）や外部ライブラリ等の適切な管理

システム開発において OSS や外部ライブラリの活用は不可欠です。一方で、これらに深刻な脆弱性が公表されると、攻撃者による探索・悪用が短期間のうちに行われる場合があります。そのため、外部のソフトウェ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ります。次の対策例を参考に、構成部品の可視化と迅速な対処体制を整備してください。

（サイバーセキュリティ担当者等向け）

・対策例 1. 深刻な脆弱性の公表時における初動対応手順の明確化：
修正や対策が未提供の脆弱性（ゼロデイ脆弱性）への注意喚起や深刻な脆弱性の公表に伴い、緊急の対処が求められた際に、保守事業者任せにせず、迅速に判断できる手順をあらかじめ定める。

- ✓ 開発・保守を委託している自組織の主要システムにおいて、組み込まれている OSS のバージョンやサポート終了（EOL）状況を平時から把握する
- ✓ NVD、JVN 等の公開情報をもとに、委託先と連携して自社システム（組み込み部品）への影響有無を速やかに照合する（参考資料 3-6）
- ✓ 影響調査の責任者、委託先との役割分担、経営層への報告基準を定める
- ✓ 修正プログラムの適用、又は WAF（Web Application Firewall）等による防御、該当機能の停止等、暫定対策の判断手順を定める

・対策例 2. 委託開発における SBOM の提出と確認：
開発・改修を委託する際に、使用するソフトウェア部品の明示と SBOM の提出を契約・仕様に定める。検収時には、既知の脆弱性やライセンスの確認結果とあわせて内容を確認する（参考資料 3-7）。

- ✓ 検収時に、提出された SBOM と設計書との突合、及び既知の脆弱性やライセンス違反の有無を確認する
- ✓ ソフトウェア構成解析（SCA）ツール等を活用し、納品後も新たな脆弱性の公表を継続的に監視する体制を整える

上記対策については、昨今の一連の攻撃手口に焦点を当てたものであり、VPN 等のインターネット上に露出した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、さらには AI の悪用が高度化・巧妙化する可能性も想定した対策を講じる必要があります。

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、経営トップの判断の下、運用しているシステムの特徴や保有している情報の内容に基づくリスク評価を行った上で、必要なサイバーセキュリティ対策の強化をお願いいたします。

【参考資料】

1-1. 経済産業省「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver2.0」
https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html
1-2. CISA「Stakeholder-Specific Vulnerability Categorization (SSVC)」
https://www.cisa.gov/resources-tools/resources/stakeholder-specific-vulnerability-categorization-ssvc
1-3. IPA「脆弱性対応におけるリスク評価手法のまとめ」
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/risk-assessment-methods.html
1-4. 経済産業省「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～」
https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html
1-5. IPA「安全なウェブサイトの運用管理に向けての 20 ヶ条」
https://www.ipa.go.jp/security/vuln/websecurity/sitecheck.html
1-6. IPA「EC サイト構築・運用セキュリティガイドライン」
https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html

2-1. 経済産業省・内閣官房国家サイバー統括室「サイバーインフラ事業者に求められる役割等に関するガイドライン」
https://www.meti.go.jp/press/2025/03/20260331001/20260331001.html
2-2. IPA「セキュリティ・バイ・デザイン 導入指南書」
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/ngi93u0000002kef-att/000100451.pdf
2-3. デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf
2-4. 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」 」
https://cynex.nict.go.jp/pdf/library/lettice/261013-01.pdf
2-5. OWASP「OWASP API Security Top 10 - API1:2023 Broken Object Level Authorization」
https://api-security.owasp.org/editions/2023/en/0xa1-broken-object-level-authorization/
2-6. OWASP「OWASP API Security Top 10 - API5:2023 Broken Function Level Authorization」
https://api-security.owasp.org/editions/2023/en/0xa5-broken-function-level-authorization/
2-7. OWASP「OWASP Mobile Top 10 2024 - M1: Improper Credential Usage」
https://owasp.github.io/www-project-mobile-top-10/2023-risks/m1-improper-credential-

usage.html

2-8. OWASP「OWASP API Security Top 10 - API4:2023 Unrestricted Resource Consumption」
https://api-security.owasp.org/editions/2023/en/0xa4-unrestricted-resource-consumption/

2-9. OWASP「Application Security Verification Standard (ASVS)」
https://owasp.org/projects/asvs

2-10. 情報セキュリティサービス基準審査登録制度「情報セキュリティサービス台帳」
https://sss-erc.org/iss_book/vds/

3-1. 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」（委託先の監督）
https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/

3-2. 経済産業省・公正取引委員会「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」
https://www.meti.go.jp/policy/netsecurity/partnership2.html

3-3. IPA「中小企業の情報セキュリティ対策ガイドライン 第4.0版」付録5：情報セキュリティ関連規定（サンプル）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0_app_5.docx

3-4. 経済産業省「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）」
https://www.meti.go.jp/policy/netsecurity/scs.html

3-5. IPA「ゼロトラスト導入指南書～情報系・制御系システムへのゼロトラスト導入～」
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/zero-trust.html

3-6. JVN（Japan Vulnerability Notes）
https://jvn.jp/

3-7. 経済産業省「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引 ver2.0」（1-1再掲）
https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html

【基本的な対策についての基準】
サイバーセキュリティ戦略本部「政府機関等のサイバーセキュリティ対策のための統一基準」
https://www.cyber.go.jp/policy/group/general/kijun.html
サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティ対策のための統一基準」
https://www.cyber.go.jp/policy/group/infra/policy.html

以上