

不正アクセスによる漏えい等の事案を踏まえ、速やかに実施すべき対策等について

公開日：2026年10月9日

注釈：追記すべき情報がある場合には、その都度このページを更新する予定です。

概要

直近において、国内の金融機関や通信事業者等の幅広い事業者から、不正アクセスの被害による情報漏えい事案の公表が相次いで行われています。特に、大量の個人情報を取り扱うオンラインサービス・アカウントサービス等に関するシステムが不正侵入され、個人情報を含むデータが窃取される事案が相次いでいるところです。
その様な大量の情報資産を保有する事業者や機微な情報を取り扱う事業者等の経営者におかれては、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要です。経営責任として情報漏えいを起こさないためのサイバーセキュリティ対策の点検や見直しを至急実施願います。

速やかに行うべき点検

現段階では、特定のプロダクトやサービスの脆弱性を狙った攻撃とは断定されておらず、公表事例の傾向から、外部公開しているアプリケーションやサービスの侵害、アカウントの侵害が起点となっていることがうかがえます。これらを踏まえた、速やかに行うべき点検は以下の通りです。

外部に公開しているアプリケーションの精査

・自組織が独自に構築・運用している外部公開アプリケーションやサービスがあるかどうかを確認してください。

・各アプリケーション、サービス単位で直近のログに異常が記録されていないか確認してください。

異常の見わけ方としては、たとえばエラーの出力量、平時との差異等が挙げられます。また、直近１ヵ月、その後３

・各アプリケーション、サービスの構成要素に現在未適用の脆弱性対応パッチがないか確認してください。

未適用のものがあった場合はできるだけ速やかに適用してください。

自組織が利用している外部サービスの洗い出し

・自組織が利用している外部サービスをすべて洗い出してください。

クラウドサービス、VPNサービス等様々な分類があること、また組織全体、部署単位での利用がありうることを踏まえ、できる限り網羅的に把握してください。

・サービス単位のログに異常が記録されていないか確認してください。

サービス単位でログの保有期間はそれぞれ異なることが想定されますので、その整理も必要です。また、サービス提供者と利用者で確認できるログにも違いがある可能性があります。誰がいつどのように確認できるかについて整理してください。異常な点については、ログイン失敗の量など比較的わかりやすいものから、ログイン元IPアドレス、ログイン時間等といった平時の情報との比較が必要なものがありますので、自組織の運用を考慮して異常または不審な点がないかを確認してください。

・サービス単位のアカウントに異常がないか確認してください。

作ったはずのないアカウントが存在しないか、削除・無効化されているはずのアカウントが有効化されていないか等の異常を確認してください。このような操作が記録されるログについての確認も並行しておこなうとより有効です。

外部に公開しているアプリケーション、自組織が利用している外部サービスのいずれにおいても、異常なログやアカウントの発見があった場合は、速やかにセキュリティインシデントと判定し、インシデント対応を進めてください。情報漏えいの可能性を考慮し、専門のセキュリティベンダーに詳細調査を依頼することを強く推奨します。

保有データの再点検

今回の多くの事案は情報漏えいにつながっています。情報を窃取されてしまうと、情報の悪用はもとより、「窃取した情報を公開する」と脅迫されたり、不正売買されるなど、情報を悪用した二次被害が拡大する傾向が強まっていますので、不要な情報は持たない、という基本原則のもと、自らが保有する情報資産を正確に把握し、必要最小限にする等、保有情報の再点検も必要です。これらの点検作業についても、速やかにおこなってください。

なお、今後各公的機関やセキュリティベンダー等から不審なIPアドレスやログの痕跡等、調査に活用できる情報が公表される可能性がありますので、当面情報収集を強化してください。

速やかに取り組むべき対策

前述の点検で異常がなかったとしても、外部公開アプリケーション、外部から利用可能なサービス、保有するデータについては、以下に示すような、より強固な対策を取ることを検討してください。

外部に公開しているアプリケーションについてその後取り組むべき対策

・外部公開範囲の見直し

・API連携等アプリケーション構成要素単位での管理状況の見直し
・アプリケーション構成要素単位での権限付与等見直し
・ログ取得内容、保持期間の見直し
・追加実装可能なセキュリティ対策の検討

自組織が利用している外部サービスについてその後取り組むべき対策

・認証機能（多要素認証・パスワード）の強化
・アカウント付与の範囲見直し
・アカウント棚卸の運用見直し
・API連携等アプリケーション構成要素単位での管理状況の見直し
・ログ取得内容、保持期間の見直し
・適用可能なセキュリティ対策の検討

保有するデータについてその後取り組むべき対策

・データ保有の是非の再検討
・データ保管場所の再検討
・データアクセスのログ取得内容、保持期間の見直し
・データの暗号化

総合的なサイバーセキュリティ対策の更なる推進

しっかりとしたサイバーセキュリティ対策のためには、このような緊急的な点検、対策ののちに、社内体制の整備だけでなく、国外拠点や取引先まで考慮した対応が必要です。
経産省の「サイバーセキュリティ経営ガイドライン」などを参考にしつつ、経営者のリーダーシップのもと取り組みを進めてください。

【サイバーセキュリティに関して経営者が認識すべき３原則】

1. サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要
2. サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
3. 平時及び緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

・サプライチェーンを通じた侵害への対策については、自社のシステムのみを対象として考えるのではなく、情報を共有する取引先や委託先等と連携した取り組みが必要です。サプライチェーン全体におけるリスクを把握し、対策推進を進めてください。なお、IPAでは、サプライチェーンを構成する企業のセキュリティ対策状況を共通の基準で評価・可視化することで、委託元企業・委託先企業双方の負担を軽減しつつ、サプライチェーン全体のセキュリティ水準の底上げを図る「サプライチェーン強化に向けたセキュリティ評価制度（SCS評価制度）」について、2027年3月の制度開始にむけ、準備を進めています。

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）

（ご参考）政府機関等からの注意喚起

・国家サイバー統括室（NCO）

不正アクセスによる漏えい等の事案を踏まえた対応について

・経済産業省

不正アクセスによる情報漏えい等の事案を踏まえた注意喚起及び情報提供に係る協力依頼

・金融庁

現下の情勢を踏まえたサイバーセキュリティ対策の強化と各種取引申込等における対応について

・警察庁

サイバー警察局便り「情報流出に注意」

・個人情報保護委員会

大規模な漏えい等事案を踏まえた対応について（注意喚起）

・一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）

直近で相次いでいる国内組織における不正アクセスに関する注意喚起

ご活用可能なIPAの各種施策

・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

中小企業向けに情報セキュリティ対策の考え方や、段階的に実現するための方策を紹介する「中小企業の情報セキュリティ対策ガイドライン」を公開しています。

・5分でできる！情報セキュリティ自社診断

中小企業者の方むけに25個の診断項目に答えることで、自社の情報セキュリティ対策状況を簡単に把握できるツールです。取り組みの手掛かりとなる「解説編」も活用ください。

5分でできる自社診断 解説編

・SECURITY ACTION セキュリティ対策自己宣言

「SECURITY ACTION（セキュリティアクション）」は、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度です。取り組み段階に応じて、ロゴマークを無料で使用でき、規模や業種を問わず共通する基本的な対策を実行することで、顧客や取引先との信頼関係の構築に大いに役立ちます。

・サイバーセキュリティお助け隊サービス

「サイバーセキュリティお助け隊サービス」は、中小企業のセキュリティ対策に不可欠な「見守り」「駆
「保険」などのサービスをワンパッケージで安価に提供可能な、民間の事業者から提供されるサービスで

としています。 2027年3月制度開始予定です。

・サイバーセキュリティ相談窓口（企業組織向け）

IPAでは企業組織向けに、セキュリティに関する総合的な相談窓口を設けています。各種インシデント発生時の初動対応に関する相談、その他の情報セキュリティに関する一般的な相談などでご活用ください。

参考資料

・経済産業省

サイバーセキュリティ経営ガイドラインと支援ツール

・IPA

サイバーセキュリティ経営ガイドライン Ver 3.0実践のためのプラクティス集

お問い合わせ先

■ 企業組織向けサイバーセキュリティ相談窓口

E-mail　**cs-support@ipa.go.jp**

企業組織向けサイバーセキュリティ相談窓口 >

注釈：個別のシステムおよび環境に関するご質問を頂いても回答ができない場合があります。詳しくは製品ベンダなどにお問合せください。

■ コンピュータウイルス・不正アクセスに関する届出窓口

コンピュータウイルス・不正アクセスに関する届出窓口 >

更新履歴

2026年10月9日　　掲載

書籍・刊行物

現在販売中のIPAの書籍・刊行物を掲載しています。 →

採用情報

IPAの採用に関する情報をご紹介します。 →

調達情報

IPAの調達・契約情報をご案内します。 →

Beyond Digital

独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan

〒113-6591
東京都文京区本駒込二丁目28番8号
文京グリーンコートセンターオフィス（総合受付13階）

organization

セキュリティセンター →

産業サイバーセキュリティセンター →

デジタル＆AIシステムズ・デザインセンター →

デジタル人材センター →

category

情報セキュリティ →

試験情報 →

デジタル人材の育成 →

社会・産業のデジタル変革 →

IPAについて →

ウェブサイトのご利用について → 個人情報保護方針 → ウェブアクセシビリティ方針 →

情報セキュリティ基本方針 → 情報公開 → 協同事業制度 → サイトマップ → アーカイブ →

ページトップへ

目的別

お問い合わせ

法人番号 5010005007126

ページトップへ

目的別

お問い合わせ