
AMT/NEWSLETTER

Cyber & AI Security

2026 年 10 月 15 日

国家サイバー統括室、「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」を公表

弁護士 清水 亘 / 弁護士 石川 雅人 / 弁護士 田中 滉大

Contents

- I. はじめに
- II. ウェブシステム等の適切な管理
 - 1. 脆弱性の適切な管理
 - 2. アカウント管理・認証
 - 3. レジリエンスの向上
- III. サプライチェーンを通じた侵害への対策
 - 1. 委託先企業等のセキュリティ対策状況の把握
 - 2. 委託契約におけるセキュリティ要件の明確化
 - 3. 情報共有範囲の明確化
 - 4. サプライチェーン全体のリスクマネジメント
- IV. データの適切な管理
 - 1. 保有する情報資産の適切な管理
 - 2. 保有情報の最小化
 - 3. 適切なアカウント管理・アクセス制御
 - 4. データ保護の徹底
 - 5. ログ取得・監視・分析の強化
- V. その他の注意喚起
- VI. まとめ

I. はじめに

近時、サイバー攻撃の脅威が現実のものとなり、日本国内の極めて多数の企業、大学、公的機関等からの情報漏えいが相次ぎ、被害はますます深刻化している。

このような背景を踏まえ、内閣官房国家サイバー統括室は、2026 年 10 月 9 日、「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」(以下「本文書」という。)と題する文書を公表した¹。本文書は、国内の企業等への注意喚起として、(1)ウェブシステム等の適切な管理、(2)サプライチェーンを通じた侵害への対策、(3)データの適切な管理等の対策の徹底を促すものである。

以下では、本文書の概要を説明する。

II. ウェブシステム等の適切な管理

本文書は、インターネットに公開されているシステムは特にサイバー攻撃の対象となりやすいので、「いつ攻撃を受けてもおかしくない」という前提で、次のような対策を講じることが重要である、としている。

1. 脆弱性の適切な管理

システムの脆弱性情報が公表されると、攻撃者は短期間のうちに悪用を開始する場合がある。そのため、修正プログラムの適用を後回しにせず、インターネットに公開されていない内部のサーバ等も含め、リスクを適切に判断し、計画的かつ迅速に次のような対応を実施することが必要である。

- OS、ミドルウェア、CMS（コンテンツ・マネジメント・システム）、アプリケーション等のセキュリティパッチやアップデートを速やかに適用する。
- サポートが終了している製品・バージョンを利用しない。
- 利用していないシステムや機能は停止・削除する。
- 定期的に脆弱性診断等を実施する。
- 不要なポート、プロトコル、サービス等を無効化する。

2. アカウント管理・認証

アカウントについては、適切な認証対策を実施することによって、不正アクセスのリスクを大幅に低減させることが可能である。

- 多要素認証(MFA)を導入する。
- 推測されやすいパスワードの使用を禁止する。
- 管理者アカウントの利用者、アクセス権を必要最小限にする。
- 退職者や異動者、利用されていないもの等の不要なアカウントを速やかに無効化する。

3. レジリエンスの向上

サイバー脅威の増大に鑑みれば、侵入を完全に防ぐことは困難である。不審な挙動の早期発見と迅速な対応こそが、被害発生および拡大の防止につながる。

¹ 内閣官房国家サイバー統括室「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」

<https://www.cyber.go.jp/pdf/press/taiou.pdf>

- ログを適切に取得・保管する。
- 不審な通信や大量のアクセスを監視する。
- 侵入検知・防御システムを活用し、パターンファイル等を定期的に更新する。
- 外部からの異常な認証試行を把握する。
- 事業継続計画等にサイバーセキュリティを組み入れる。
- インシデントが起きた場合の対応態勢を整備する。

Ⅲ. サプライチェーンを通じた侵害への対策

本文書は、サイバー攻撃への対策は、自社システムのみを対象として考えるのではなく、個人情報や業務情報を預ける委託先企業等を含むサプライチェーン全体で安全性を確保する観点で取り組むことが重要だと述べている。なぜなら、攻撃者は、比較的防御が弱い委託先企業等を足掛かりとして侵入し、その後、標的となる企業へアクセスを拡大する手口を用いることがあるからである。本文書は、サイバーセキュリティ対策の実施にあたっては、「委託先企業と共に管理する」という認識の下で、次のような適切な安全管理措置を講じることが求められる、としている。

1. 委託先企業等のセキュリティ対策状況の把握

- 委託先等の情報セキュリティ方針、管理体制や委託先等との役割分担・責任分界を確認する。
- 個人情報や業務情報の取扱状況を定期的に点検する。
- セキュリティ認証の取得状況や監査結果を確認する。
- 再委託先を含む管理状況を把握する。
- 契約締結時だけでなく、継続的に確認を行う。

2. 委託契約におけるセキュリティ要件の明確化

- 情報の取扱方法を明確に定める。
- アクセス権管理やログ管理の実施を求める。
- 不正アクセスや漏えいが発生した場合の報告義務を規定する。
- インシデント発生時の委託先との連携体制を整備する。

3. 情報共有範囲の明確化

- 委託先へ提供する個人情報や業務情報を必要最小限とする。
- 業務終了後の委託先でのデータ削除を徹底する。
- 委託先に付与するアクセス権を適切に管理する。

4. サプライチェーン全体のリスクマネジメント

- 重要な取引先や委託先を洗い出す。
- サプライチェーンを含めた情報資産の流れを可視化する。
- サプライチェーン上の重要な依存関係を把握する。
- 定期的なリスク評価を実施する。

IV. データの適切な管理

企業が保有する個人情報や業務情報は、重要な経営資産であるが、不必要な情報の保有や、アクセス権限の管理や保管方法が不十分である場合には、不正アクセスを受けた際に被害が大規模化するおそれがある。また、近年の攻撃者は、窃取した情報を公開すると脅迫したり、不正に売買したりする等、情報そのものを標的とする傾向を強めている。そこで、本文書は、「保有する情報資産を守る」という視点に立った、次のような安全管理措置が求められる、としている。

1. 保有する情報資産の適切な管理

適切な保護措置を講じるためには、自社が保有する情報資産の全体像を把握することが重要である。

- 個人情報や業務情報の所在や管理者を把握する。
- 重要な情報資産を分類し、管理対象を明確にする。
- 利用目的や保存期間を明確にする。
- 定期的に情報資産の棚卸しを実施する。

2. 保有情報の最小化

万が一情報漏えいが発生した場合でも、保有する情報が少なければ被害の拡大を抑えることが可能である。

- 利用目的を終えた情報は速やかに削除する。
- 法令上の保存期間を経過した情報は適切に廃棄する。

3. 適切なアカウント管理・アクセス制御

必要以上の権限が付与されている場合、不正アクセス時に大量の情報が一度に取得されるおそれがある。

- 業務上必要な者のみにアクセスを許可する。
- 閲覧権限と更新権限を適切に分離する。
- 管理者権限の付与を必要最小限とする。
- 定期的にアカウントや権限設定を確認する。

4. データ保護の徹底

万一、情報が窃取されたとしても、適切な保護措置が講じられていれば悪用のリスクを低減することができる。

- 保存データを暗号化する。
- 通信経路を暗号化する。
- パスワードや認証情報を平文で保存しない。
- 外部電磁的記録媒体の利用やデータ保存等に関するルールを整備する。
- バックアップデータについても適切に保護する。
- クラウドサービスを利用する場合は、サービス仕様を理解し、保存領域やデータベース等の公開設定およびアクセス権限設定をよく確認する。

5. ログ取得・監視・分析の強化

不正アクセスを早期に発見し、被害範囲を迅速に特定するためには、適切な監視・分析体制が不可欠である。また、不正侵入される事案が複数確認されている状況に鑑み、不審な通信や大量のアクセスの痕跡がないか、アクセスログ等の点検・分析を実施することが推奨される。

- 個人情報や業務情報へのアクセス記録を取得する。
- 不審なアクセスや大量データの取得を監視する。
- ログを一定期間保管する。
- 異常を検知した場合の対応態勢を整備する。

V. その他の注意喚起

サイバー攻撃の脅威が現実化した状況を踏まえ、本文書の公表と同日(2026 年 10 月 9 日)に複数の注意喚起が公表されている。

まず、一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)は、「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」として、現時点で確認されている攻撃手法等に基づき、API 経由のアクセスへの対策等の実施を推奨する注意喚起を行った²。

また、個人情報保護委員会は、「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)」として、個人情報等の適切な取扱いおよび不正アクセスによる個人データ漏えい防止のための対策を促す注意喚起を行った³。

さらに、経済産業省商務情報政策局サイバーセキュリティ課は、「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」として、本文書を含む注意喚起を参照のうえ、自社のみならず、サプライチェーン全体でセキュリティを管理するという認識の下、①組織のトップによる主導、②脆弱性情報の早期把握と対応、③「ゼロトラスト」への移行等、対策の徹底を呼びかけた⁴。

独立行政法人情報処理推進機構(IPA)も、「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」と題する注意喚起を行っている⁵。

VI. まとめ

本文書が述べるように、サイバー攻撃に起因する不正アクセスによって、個人情報や業務情報が流出すれば、事業停止、顧客対応等、多方面にわたる経営リスクへと発展する可能性がある。サイバー攻撃の手法は、急速に進化する AI の悪用を含めてますます高度化・巧妙化している。世界情勢の複雑化をも背景として、サイバー攻撃は、増えることはあっても、減ることは決していないであろう。上記のとおり、同日に複数の注意喚起が公表された背景には、同様の認識があるものと思われる。

企業等の経営者は、「いつ誰が攻撃されてもおかしくない」「自社を 100%守り切るのは不可能」という前提を再認識し、

² 一般社団法人 JPCERT コーディネーションセンター「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」[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](#)

³ 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)」[大規模な漏えい等事案を踏まえた対応について\(注意喚起\)\(令和8年10月7日\)](#) | 個人情報保護委員会

⁴ 経済産業省 商務情報政策局 サイバーセキュリティ課「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」[20261009_chuuikanki.pdf](#)

⁵ 独立行政法人情報処理推進機構(IPA)「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」[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](#) | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

サイバーセキュリティリスク対応を経営課題と位置づけ、必要な投資や人的体制整備を含むサイバーセキュリティ対策を強化することが急務である。

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 石川 雅人 masato.ishikawa[at]amt-law.com
弁護士 田中 滉大 koudai.tanaka[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。