事業者の皆さまへ

会社の情報、狙われています。

1 サイバー攻撃情勢の概要
2 確認すべき３つの事項
3 実施すべき５つの対策
4 もしも、被害が疑われたら
5 最寄りの警察署等への早期通報
6 メッセージ
7 通報・相談窓口

警視庁

1　サイバー攻撃情勢の概要

事業者をとりまく状況

約９秒に１回

令和7年、全国の警察施設の
インターネット接続点に設置された
センサーで検知した不審通信

警察庁集計／海外からの通信が全体の99%

123件

令和８年上半期
ランサムウェア被害報告

警察庁集計／半期として過去最多

令和８年下半期
情報漏えいを伴う『不正アクセス』
『ランサムウェアへの感染』
多発!!

企業が警戒したい主な脅威

1. ランサムウェア攻撃
   データの暗号化・窃取、業務停止や恐喝
2. サプライチェーンや委託先を狙った攻撃
   自社だけでなく、業務委託先・取引先等から侵入
3. システムの脆弱性を悪用した攻撃
   VPN・公開サーバ・APIやIDを狙う
   ※APIとは、異なるシステムやアプリ間をつないでデータや機能を共有する仕組み。
4. 機密情報を狙った標的型メール攻撃
   メール文面等の巧妙化

被害を防ぐための第一歩

外部公開機器・アカウントの権限等を点検するとともに、ログ管理、
OSやソフトウェア等の更新、個人情報等の情報資産の適切な管理を行う。

出典：警察庁 「令和8年上半期におけるサイバー空間をめぐる脅威の情勢」 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf
IPA 「情報セキュリティ10大脅威2026」https://www.ipa.go.jp/security/10threats/10threats2026.html
をもとに、警視庁が作成

2　確認すべき３つの事項

担当者と期限を決め、点検を開始

1　公開アプリケーションに係るサーバ

アクセス・エラーログの急増やアプリケーションが

アクセスするサーバに関する不審な通信がないか確認。

2　外部サービス(クラウド、VPN等)

普段と違うログイン・時刻、エラーログの急増、

覚えのない新規アカウント等や権限変更がないか確認。

3　資産管理（保有データ、資機材）

不要な個人情報は削除するなどし、

各情報等の保管場所とアクセス権を確認。

問題に気付いたら

侵害経路を即遮断。
証拠を保全。責任者・専門家へ速やかに連絡し、改善。

出典：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」
https://www.ipa.go.jp/security/security-alert/2026/alert20261009.html
をもとに、警視庁が作成

3　攻撃を防ぐ実施すべき５つの対策

点検だけで終わらせず、仕組みを改善

1　多要素認証等の導入

認証機能を強化。
アカウントへの権限付与を必要最小限にするなど見直す。

2　脆弱性への迅速な対処

OS、アプリケーション等に対する最新のパッチを適用。
不要なポート、サービス等を無効化。

3　API経由のアクセスへの対策

アクセス回数を制限。悪意ある試みを防ぐために、アクセスの急増に注意。
本人確認に加え、アクセス権限の有無をその都度確認。

4　被害に備える

ログ保存、緊急時連絡先の確認、保守管理業者との対応手順を整備。

ランサムウェアによって生じるシステム障害発生時の事業継続計画の策定。

5　業務委託先のセキュリティ対策も確認

出典：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」
https://www.cyber.go.jp/pdf/press/taiou.pdf
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」
https://www.ipa.go.jp/security/security-alert/2026/alert20261009.html
個人情報保護委員会「個人情報保護委員会WARNING不正アクセスによる個人データ漏えい防止のための注意喚起」
https://www.ppc.go.jp/files/pdf/261007_warning.pdf
をもとに、警視庁が作成

4　もしも、被害が疑われたら

放置せず、初動対応へ切替え

1　記録を残す

まず、ネットワークから遮断する。
ログ・端末を保全する。
時系列を記録する。

2　拡大を止める

専門家と相談し、侵害経路を遮断する。

3　適切に報告・連絡する

保守管理業者・経営層・関係機関への報告・連絡を判断。
従業員は、システム担当等に報告・連絡すること。

一次情報を確認

関係機関の注意喚起・更新情報等はこちら

国家サイバー統括室
関係機関の注意喚起一覧

警察庁サイバー警察局
注意喚起、サイバー警察局だより

情報処理推進機構
不正アクセスを踏まえた緊急点検

警視庁サイバー(公式X)
注意喚起、セキュリティ情報等

5　最寄りの警察署等への早期通報

証拠が消える前に、まず相談

通報は「すべて判明してから」では遅い

不明点があっても、判明した事実を先に伝える。

警察に伝える情報（わかる範囲で）

いつ・何が

発見日時、経緯、被害・影響範囲

何を狙われたか

端末・サーバ、アカウント、情報の種類

攻撃の手掛かり

通信・認証ログ、攻撃元IP、URL、IoC

保存した証拠

画面画像、メール、マルウェアのハッシュ値等

※　証拠を消去・改変せず、復旧と保全は専門家と調整。

通報・脅威分析への協力で期待できること

- 注意喚起や防御情報の共有につながる。
- 被害拡大防止や捜査の手掛かりになる。
- 攻撃の手口・関連事案の分析が進む。

6　メッセージ

組織を守るのは、日々の備えと迅速な連携

最近のサイバー空間では、多くの事業者において、様々な手口によるサイバー攻撃の被害を受けた情報流出事案が続発しており、事業の継続や顧客の信頼を脅かす経営上のリスクとなっています。

特に、機微な情報や大量の個人情報を取り扱う事業者の皆様におかれましては、継続的にセキュリティ対策等について確認・見直しを行うとともに、社員に対して適切なセキュリティ教育を行うなどの対策を進めていただけますようにお願いします。

また、不審な通信や情報流出の兆候を把握された場合は、侵害経路を速やかに遮断した上で、証拠を保全し、早期に警察へご相談ください。

被害情報の共有は、ほかの事業者の皆様方への被害防止や攻撃手口の解明にもつながります。

7　通報・相談窓口

全国統一のオンライン窓口も利用可

警察庁

通報・相談・情報提供

全国統一のオンライン窓口

警視庁

通報・相談・情報提供
被害届の提出

最寄りの警察署へ

緊急時は、１１０番通報



警視庁
〒100-8929
東京都千代田区霞が関２丁目１番１号
電話：03-3581-4321
公式HP　https://www.keishicho.metro.tokyo.lg.jp/



出典一覧
NCO　「不正アクセスによる偽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
IPA　「情報セキュリティ10大脅威2026」https://www.ipa.go.jp/security/10threats/10threats2026.html
「不正アクセスによる偽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」https://www.ipa.go.jp/security/security-alert/2026/alert20261009.html
個人情報保護委員会「個人情報保護委員会WARNING不正アクセスによる個人データ偽えい防止のための注意喚起」https://www.ppc.go.jp/files/pdf/261007_wamin.pdf
警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢」　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf
をもとに、警視庁が作成