関連機関からの注意喚起等一覧

官公庁や各種団体から注意喚起や要請が各種発出されているが、攻撃手法は多様化しているのが実態であり、各機関が捕捉した事案や着目点により内容が異なってしまっている。企業が何をするべきなのか判断が困難な状況にある。

	機関名	注意喚起・指示内容	参考
1	国家サイバー統括室	相次ぐ情報漏えいを受け、脆弱性対応、多要素認証、委託先を含む対策の徹底を要請。経営層主導でシステム管理やデータ保護を見直し、サプライチェーン経由の侵害と漏えい情報の悪用を防ぐよう促している。	https://www.cyber.go.jp/pdf/press/taiou.pdf
2	警察庁	企業にはソフトウェア更新や強固なパスワードなど基本対策の再確認を要請。個人には流出元企業を装う偽メールへの警戒、パスワードの使い回し防止、多要素認証、詐欺電話対策を勧め、不審な場合は警察への相談を案内している。	https://www.npa.go.jp/bureau/cyber/index.html
3	個人情報保護委員会	大量・機微な個人情報を扱う事業者などに、リスクに応じた安全管理措置の見直しを要請。ログの保存・分析や侵入の早期検知などの対策例を示し、不要な個人データの消去と組織的・多層的な対策を求めている。	https://www.ppc.go.jp/news/press/2026/261007_houdou/?ref=tninf
4	金融庁	本人確認書類の画像を含む情報漏えいを踏まえ、金融機関に委託先管理や事故対応態勢の点検を要請。非対面での本人確認を厳格化し、画像送信方式からICチップ読み取り方式への早期移行を求めている。	https://www.fsa.go.jp/news/r8/sonota/20261009/20261009.html
5	総務省	所管事業者や関係団体に、迅速な脆弱性対応、認証強化、漏えい情報の悪用防止を要請。特に大量・機微な個人情報を扱う事業者に、経営層主導で委託先も含めたセキュリティ対策を徹底するよう求めている。	https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000678.html https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000680.html
6	経済産業省	サプライチェーン経由を含む不正アクセス被害を受け、①組織トップの手動、②脆弱性早期把握、③ゼロトラスト移行への取組みを要請。企業向け支援策を案内し、被害が生じた場合は、担当課室への迅速な情報提供を求めている。	https://www.meti.go.jp/policy/netsecurity/pdf/20261009_chuuikanki.pdf
7	IPA	経営者の責任で①公開サービスの精査、②利用サービスの洗い出し、③保有データの再点検を要請。異常がなくても認証・権限・公開範囲・暗号化などを見直し、不要な情報を削減するとともに、取引先を含む継続的な対策を推奨している。	https://www.ipa.go.jp/security/security-alert/2026/alert20261009.html
8	NICT	公開アプリを解析して接続先やAPIの情報を調べ、サーバの弱点を狙う「A2B攻撃」を特定。侵害確認、脆弱性点検、暫定的な緩和策を推奨し、他のサービスへの波及やAIによる攻撃の効率化にも注意を促している。	https://www.nict.go.jp/press/2026/10/13-1.html
9	JPCERT/CC	情報漏えい事案の攻撃手法や不信IPアドレス情報等を公開。APIの利用回数制限、アクセス制御、権限の最小化、脆弱性修正を推奨。従業員向けシステムも点検し、不要な公開機能の停止や保有データの削減を求めている。	https://www.jpcert.or.jp/at/2026/at260030.html

【参考】関連機関からの注意喚起の内容分析結果

各注意喚起を統合すると**80項目以上の要求事項**が存在

分野・対象	統合した対策	国家サイバー統括室	警察庁	個人情報保護委員会	金融庁	総務省（10月9日）	総務省（10月13日）	経済産業省	IPA	NICT	JPCERT/CC
経営・体制	経営層主導でセキュリティ対策を進める	★	—	★	★	★	—	★	★	—	—
経営・体制	必要な投資・人員・社内体制を確保する	★	—	★	—	—	—	—	★	—	—
経営・体制	リスクに応じて対策を点検・見直し、不備を是正する	★	★	★	★	★	★	★	★	—	★
経営・体制	ゼロトラストへ移行する	—	—	—	—	—	—	★	—	—	—
資産把握	管理対象のシステム・機器・サービスを洗い出す	★	—	★	—	—	—	—	★	★	—
資産把握	APIを洗い出し、管理対象として棚卸しする	—	—	★	—	—	—	—	★	★	—
脆弱性管理	脆弱性情報を早期に収集・把握する	★	—	★	—	—	—	★	★	—	—
脆弱性管理	修正プログラム・更新を速やかに適用する	★	★	★	—	★	—	★	★	—	★
脆弱性管理	サポート終了製品・バージョンの利用をやめる	★	—	★	—	—	—	—	—	—	—
脆弱性管理	脆弱性診断・設定不備の点検を行う	★	—	★	—	—	★	—	—	★	—
脆弱性管理	APIの認可不備、SSRF、遠隔コード実行、SQLインジェクション等を点検する	—	—	—	—	—	—	—	—	★	—
公開範囲	不要なシステム・機能・API・公開サービスを停止・削除する	★	—	—	—	—	—	—	★	★	★
公開範囲	不要なポート・プロトコルを無効化する	★	—	—	—	—	—	—	—	—	—
認証	強固なパスワードを使用し、推測されやすいものを避ける	★	★	★	—	—	—	—	★	—	—
認証	同一・類似パスワードの使い回しを防ぐ	—	★	★	—	—	—	—	—	—	—
認証	多要素認証を導入・利用する	★	★	★	—	★	—	—	★	—	★
認証	ログイン失敗時のアカウント停止・ロックを行う	—	—	★	—	—	—	—	—	—	—
認証	漏えいが疑われる認証情報を無効化・初期化・再発行する	—	—	★	—	—	—	—	—	★	★
アカウント管理	不要なアカウントを無効化する	★	—	★	—	—	—	—	—	—	—
アカウント管理	不正作成・不正な再有効化などの異常を確認する	—	—	—	—	—	—	—	★	—	—
アカウント管理	アカウント・権限を定期的に棚卸しする	★	—	★	—	—	—	—	★	—	—
アクセス制御	利用者・管理者・API利用者の権限を必要最小限にする	★	—	★	—	—	—	—	★	—	★
アクセス制御	閲覧権限と更新権限を分離する	★	—	—	—	—	—	—	—	—	—
アクセス制御	接続元・端末等に応じてアクセスを制限する	—	—	★	—	—	—	—	—	★	★
アクセス制御	許可・基準適合した端末だけにアクセスを認める	—	—	★	—	—	—	—	—	—	—
アクセス制御	アクセスごとに状況を評価し、許可の可否を判断する	—	—	★	—	—	—	—	—	—	—
API対策	データ取得の都度、利用者のアクセス権限を確認する	—	—	★	—	—	—	—	—	—	★
API対策	APIへの要求件数・利用回数を制限する	—	—	★	—	—	—	—	—	—	★
API対策	ログイン・検索・SMS送信等に個別の回数制限を設ける	—	—	—	—	—	—	—	—	—	★
API対策	許可したHTTPメソッドだけを受け付ける	—	—	—	—	—	—	—	—	—	★
API対策	APIトークンに適切な有効期限を設定する	—	—	—	—	—	—	—	—	—	★
API対策	応答に不要な情報を含めず、識別番号を推測困難にする	—	—	★	—	—	—	—	—	—	—
防御・侵害拡大防止	ファイアウォール等で不正アクセスを遮断する	—	—	★	—	—	—	—	—	—	—
防御・侵害拡大防止	ウイルス対策ソフト等を導入・更新する	—	—	★	—	—	—	—	—	—	—