

【緊急注意喚起】サイバー攻撃・不正アクセス急増に伴う情報セキュリティ対策のお願い

SOIC 会員企業・事業者の皆様へ

2026 年 9 月以降、日本国内の多様な企業やサービスにおいて不正アクセス事案や情報漏洩被害が相次いで発生しており、その被害規模・件数ともに、非常に深刻な状況になっています。

大手企業や特定インフラに限らず、問い合わせ窓口や Web フォームを持つ地域の中小企業も標的となったり、攻撃の足がかりとして悪用されたりするケースが急増しています。

自社および顧客のデータ、取引先からの信頼を守るため、今一度セキュリティ体制の見直しと、全社的な注意喚起・周知をお願いいたします。

1. 経営者・管理者向け：企業として取り組むべき対策

Web サイトやフォーム経由での情報漏洩事故を防ぎ、組織を守るため、設定の確認とルールの徹底が必要です。以下、自社で適用可能な対策について実施をお願いします。

1) Web フォーム・問い合わせ窓口のセキュリティ再点検

- Web サイトの問い合わせフォーム、顧客登録システム、EC サイト等のシステムを利用している場合は、CMS、プラグイン、フレームワークなどが最新バージョンに更新されているか確認してください。
- 外部に上記の Web 管理・運用を委託している場合は、委託先に対してセキュリティの運用状況（脆弱性対策・アクセスログの監視）を直ちに問い合わせてください。

2) 認証の強化（多要素認証の導入）

- 業務利用しているクラウドサービス（メール、ストレージ等）、Web サイトの管理画面へのログインには、パスワードのみに頼らず多要素認証（MFA）やパスキーなどを必須化するようにしてください。

3) アクセス権限とアカウント管理の見直し

- 退職者や外部委託業者のアカウントが残っていないか定期的に確認し、不要なアカウントは削除してください。
- 「最小権限の原則」に基づき、業務上必要な範囲のみアクセス権限を付与してください。

4) バックアップと緊急連絡体制の整備

- 重要データは定期的にバックアップを取得し、ネットワークから分離した状態（オフラインや隔離された環境など）で保管してください。
- 万が一、不正アクセスや情報漏洩が疑われる場合の「初期対応手順」と「緊急連絡網」を整理してください。

2. 従業員の皆様へ：日々の業務で徹底していただきたい注意点

今回は Web サイトの問い合わせ窓口や、アプリ利用者登録などのサービスが攻撃の対象となっています。

従業員の方は以下のポイントについて確認し、適切に対処するよう周知をお願いします。

① 不審な問い合わせ・偽装メールへの注意（★重要）

1) 情報漏洩発生企業をかたるフィッシングメールにご注意ください

- 情報漏洩を公表した実在の企業やサービスを装い、「アカウント情報の確認」「パスワード再設定のご案内」「個人情報流出に関するお詫びと確認」などをあおる不審なメールが急増しています。
- メール内のリンクをクリックさせ、偽のログイン画面等で ID・パスワードや個人情報を盗み取ろうとする攻撃（フィッシング）です。
- 不審なメールが届いた場合は、本文中のリンクやボタンは絶対に押さず、公式サイトや正規の問い合わせ窓口から真偽を確認してください。

2) 不審な問い合わせ・添付ファイル・URL を開かない

- メールや問い合わせフォームなどを通じて届いた、不審な URL、ファイル（ZIP、PDF、マクロ付き Excel/Word など）は安易に開かないでください。
- 「至急」「請求書」「未払い」といった不安をあおる文言に惑わされず、差出人のメールアドレスをよく確認してください。

3) Web サイト・アプリへの個人情報入力は必要最小限に

- 個人情報（氏名、メールアドレス、電話番号など）の情報漏えいリスクを考慮し、Web サイトやアプリへの会員登録は必要なものに限定し、登録する場合も入力する個人情報は必要最小限にしましょう。
- 利用しない Web サイト、アプリからは退会して、情報漏洩リスクを低減させましょう。

② アカウントとパスワードの管理

1) パスワードの使い回し禁止

- パスワードを、複数のサービスに使い回さないようにしましょう。連鎖的に不正アクセスされる危険性があります。

2) 多要素認証・パスキーの設定

- 個人で利用する銀行、証券、EC サイト、Google、各種 SNS などでは多要素認証またはパスキーを設定しましょう。これにより万が一ログイン情報が流出しても不正アクセスを防止できる可能性が大幅に高まります。

以上、社内イントラネットでの展開、メールでの周知、文書の掲示など、用途に合わせて編集してご活用ください。