

不正アクセスに対する安全管理措置について (経営者向け)

2026年10月19日

プライバシーマーク推進センター
事故対応グループ



！これは、決して他人事ではありません。

不正アクセスの被害は、もはや大企業だけの話ではありません。
実際に被害にあうと、次のような事態が起こる可能性があります。

- 業務システムが止まり、事業が完全にストップする
- 顧客情報が流出による、謝罪対応・信用失墜
- 取引先から契約を打ち切られる
- 復旧等に数百万円～数千万円の費用がかかる など

被害の多くは、高度なハッキングではなく、**基本的な対策の漏れやミスの積み重ねが原因**です。

よくある原因

- ✓ ソフトウェアの更新をしていなかった
- ✓ アクセス権限の設定にミスがあった
- ✓ 簡単なパスワードを使用していた など

事故原因の**約3割！**

つまり、“**基本を徹底すること**”により、**多くの被害を防げる可能性が高くなる**のです。

そして、これは現場任せにできない“**経営の問題**”です。

セキュリティ対策は「コスト」ではなく、“**会社を守る投資**”と考えましょう。

「なぜ防げなかったのか？」をお客様・取引先・社会等に説明する責任は、経営者にあります。



まずは「今、自社がどうなっているか」を知ることから始めてください。

□ システム管理者に、現在のセキュリティ対策の状況を報告してもらう

- ・ 現場が独自の判断で、ルールの変更や省略をされていないか等を確認します。

□ 委託先(外部のシステム会社等)のセキュリティ対策も、自社と同レベルか確認する

- ・ 委託先に預けた自社の情報が事故に遭った場合、説明責任はあなたの会社にも発生します。

□ 確認した内容は、必ず記録に残す

- ・ 「経営者が確認した」という証拠が、いざという時に会社を守ります。



✓ 問題が見つかった場合には、放置せず、すぐに動きましょう。

□ 重大な問題は、最優先で今すぐ対応させる

- 重大な問題を放置すると、いつ攻撃や事故につながるかわかりません。できるだけ早く対応しましょう。

□ その他の問題も、いつまでに・誰が・何をするか計画を立てさせる

- 計画がないと対応が後回しになり、問題が長期間放置され、被害が広がる恐れがあります。

□ 計画通りに実行されているか、自分の目で確認する

- 「現場に任せたまま、忘れられていた！」が事故の典型パターンです。

□ 確認した内容は、必ず記録に残す

- 「経営者が確認した」という証拠が、いざという時に会社を守ります。



✓ 不正アクセス対策への投資を、惜しまないでください。

□ システム管理者を、1人だけに任せない

- いわゆる「ひとり情シス」は、止めましょう。担当者の退職や休職により、会社のシステム運用やトラブルへの対応が困難となります。

□ システム管理者に、必要な権限を与える

- 対応スピードが重要な場面でも「いちいち上司の許可待ち」では、対応が遅れて被害が広がります。

□ 全社員向けに、不正アクセス対策の教育の実施を徹底させる

- 攻撃の多くは「偽メールを開かせる」など、人の隙を狙っています。



経営者に求められる役割

- 1 知る：現状を確認する
- 2 動く：問題があれば即対応する
- 3 投資する：ヒト・モノ・カネを惜しまない

これらを怠ると、ある日突然、会社が止まります。

逆に言えば、この3つを押さえれば、多くの被害は防げます。

「うちは大丈夫」ではなく、
「今日から確認」を行いましょう！

それが、会社を守る経営者の仕事です。

上記3つを実行するにあたっては、平時からシステム管理者と密にコミュニケーションを取り、課題やリスクを早期に把握できる関係を築くことが重要です。

そのような現場を支える体制づくりこそが、“組織全体の強さ”につながります。



本資料は「概要編」となります。「本編」はプライバシーマーク付与事業者様限定公開です。付与事業者様は、Pマークポータルサイトから「本編」をご覧ください。

