



あなたの会社のサーバが 狙われている!!



業務で使用している各種サーバに脆弱性や運用管理に不備があると、Webサイトの改ざんや情報漏えい、不正メールの送信に悪用されるなどし、サービスの停止や顧客への補償のほか、企業としての信用を損なうなど、事業に大きな影響が出る可能性があります。

下記の一例を含め、サーバのセキュリティ対策が取られていない場合には、早急に適切な対策を実施してください。

適切なサーバのセキュリティ対策の実施を!!

＜サーバのセキュリティ対策の一例＞

- OSやサーバソフトウェア、ミドルウェアをバージョンアップし、**脆弱性を解消**してください。ただし、ソフトウェアをバージョンアップした場合、今まで動作していたアプリケーションが正常に動作しなくなる場合がありますので、事前に検証を実施してください。
- 不要なアカウントが登録されていると不正利用される可能性がありますので、**必ず削除**してください。
- パスワードが推測されやすい場合、悪用される可能性が高くなるので、**他人から推測困難なパスワード**を使用してください。また、初期パスワードは必ず変更してください。
- アクセスログは事故や故障、不審な動きがあった場合に、原因特定のために必要となりますので、**ログを保管**するとともに、不正にアクセスされていないかなどを**定期的に確認**してください。



この他にも、Webサーバやメールサーバなど、それぞれのサーバごとに実施すべきセキュリティ対策もありますので、適切な対策を実施して、安全なサーバの運用に努めてください。

サイバー犯罪（インターネットに関する犯罪）の通報やご相談は・・・

石川県警察本部生活環境課サイバー犯罪対策室



076-225-0110



cyber@police.pref.ishikawa.lg.jp