2010 年 9 月 17 日

株式会社ヒューマネージ
コンプライアンス統括室

「不正アクセス」に関する弊社セキュリティ対策について

一部報道において、現在、中国にて日本へのサイバー攻撃が呼びかけられているとの報道がございました。

弊社では、情報セキュリティ基本指針に則り、弊社の管理する情報資産を、その周囲を取り巻く脅威から確実に保護するために、適切な情報セキュリティ管理策を確立し、実施しております。

「不正アクセス」に関する弊社のセキュリティ管理策は、以下の通りです。

記

1. サイバー攻撃とは

インターネット経由で他のコンピューターに不正アクセスを行い、各団体・企業にダメージを与えようとする行動のこと。主にウェブサイトのアクセス超過や、クラッキングによる情報の改竄・漏洩・棄損等を引き起こすものがある。

2. 「不正アクセス」に関連するセキュリティ管理策と対応状況

【想定されうる攻撃】

（1） DoS/DDoS 攻撃(*)

（2） 既知の脆弱性を狙った攻撃（SQL インジェクションやバッファオーバーフローなど）

（3） 未知の脆弱性を狙った攻撃（0-day 攻撃）

(*) DoS/DDoS 攻撃とは ：複数のネットワークに分散する大量のコンピューターから一斉に特定のサーバーへ大量のアクセスを行ったり、パケットを送信したりし、通信トラフィックやサーバー負荷を増大させサイトの稼働を阻害したり、停止させてしまう攻撃

【実施している対策】

（1）の対策 ：

DoS/DDoS 攻撃が行われた場合、システムが過負荷になることが想定されますので、システムの負荷状況を常時モニタリングしております。

万が一、大規模な DoS/DDoS 攻撃が行われた場合は、弊社ファイアウォールによる当該通信の遮断および iDC（データセンター）へのエスカレーションを実施します。

(2)の対策　　：

弊社では、弊社情報セキュリティポリシーおよび規程に基づき、サービスリリース時および修正時において、脆弱性検査を漏れなく適切に実施しております。

加えて、パッチ(修正プログラム)の適用、バージョンアップも漏れなく実施しております。

- 稼働中のサイトにおいて、残存する脆弱性はございません。
- OS ならびに稼働しているアプリケーションやサービスは、全て最新のパッチが適用されております。

(3)の対策　　：

サービスリリース時には、あらかじめ想定される脆弱性パターン(シグネチャ)での検査だけでなく、専門診断者による、手動のペネトレーション検査も実施しております。

しかしながら、未知の脆弱性に対する攻撃を防ぐことは難しいため、不正アクセス等に対しては、24 時間 365 日の監視を行い、被害の早期発見・早期対処が可能な体制を整備しております。

- 不正アクセスをしようとした試みも含め、すべてログに記録され、その内容を確認しております。
- 万が一、懸念される内容が発見された際の連絡・対応につきましても、適切かつ迅速に対応できる体制を敷いております。

以上