

不正アクセスによるサイバー攻撃の被害について（第3報）

日頃より格別のご高配を賜り、誠にありがとうございます。

2026年2月13日および3月5日に公表いたしました、弊社サーバーへの不正アクセスおよび情報流出の件に関しまして、お取引先様、ならびに関係先の皆様に多大なるご心配とご迷惑をおかけしましたことを、改めて深くお詫び申し上げます。

外部調査会社によるフォレンジック調査が完了し、システムの復旧および再発防止策の策定を終えましたので、下記の通りご報告申し上げます。

記

1. 調査結果と復旧状況

外部調査会社による調査の結果、今回の不正アクセスはVPN機器の脆弱性および一部アカウントの認証情報の特定を起点としたものであることが判明いたしました。

これを受け、弊社ではサーバー、端末、ネットワークの全初期化、および安全性の確認を完了し、本日までにすべての業務システムが正常に稼働・復旧したこと（一部暗号化されたデータを除く）をご報告いたします。

2. 情報流出への対応

攻撃者のリークサイトにて公開された情報については、引き続き外部専門家とともに監視を継続しております。対象となる可能性があるお取引先様には個別にご連絡を差し上げ、誠実に対応を進めております。現時点において、二次被害の報告は受けておりませんが、引き続き警戒を緩めることなく対応してまいります。

3. 再発防止策の実施

今回の事態を重く受け止め、二度と同様の事象を発生させないよう、以下のセキュリティ体制を抜本的に強化いたします。

項目	具体的な実施内容
再侵入防止策	今回侵入経路となったリモートアクセスVPNの廃止
認証の強化	全システムにおいてパスワードの変更と認証強度を強化
監視・検知の高度化	意図しないツールやプロセスの実行を防止する仕組みを導入
復旧性・耐障害性強化	システム復旧の迅速化を図るバックアップ方法の変更
教育の徹底	全役職員を対象とした情報セキュリティ教育の実施

4. 今後について

弊社は今回の事案を真摯に受け止め、サイバーセキュリティを経営の最優先事項の一つとして位置づけ、信頼回復に全力を尽くしてまいります。

改めて、関係者の皆様に多大なるご迷惑をおかけしましたことを、心より深くお詫び申し上げます。

以上

○本件に関するお問い合わせ

管理部

電話：0465-38-2424

受付時間：月曜日～金曜日（年末年始・祝日を除く）9時～17時