2022 年 10 月 31 日

各　　位

会 社 名　株式会社ＮＩＴＴＡＮ
代表者名　代表取締役社長 李　　太 煥
（コード番号 6493 東証スタンダード市場）
問合せ先　執行役員 田中 靖彦
（TEL.　０４６３－８２－１３１１）

当社サーバーへの不正アクセスに関するお知らせ（第３報）

当社は、2022 年９月 13 日及び９月 30 日に公表した「当社サーバーへの不正アクセスに関するお知らせ」のとおり、当社内サーバーに対し第三者による不正アクセスを受けました。なお、現時点で、当社製品の生産やお客様への納品について、本件に起因する大きな影響は出ておりません。しかしながら、本件につきまして、お客様をはじめ関係者の皆さまに多大なるご心配ならびに一部業務遅延によるご迷惑をおかけする事態となりましたことを、深くお詫び申し上げます。

さて、当社は、不正アクセス攻撃の発覚以後、緊急対策本部を立ち上げるとともに、速やかに警察やシステム会社など関係諸機関への報告と助言のもと、被害範囲や不正アクセス原因及び復旧の見通しについて調査を進めてまいりました。
そして今般、システム会社及びサイバーセキュリティ専門会社の協力により、不正アクセスの原因及び影響範囲の調査と、攻撃の再発を防ぐ暫定対策が完了し、一部業務について停止していたシステムネットワークを近日中に復旧する見通しとなりました。
個人情報やお客様の情報につきましては、専門会社による上記調査及びインターネット上の情報調査により、漏洩等の被害は確認されておりません。また、インターネット上の情報調査につきましては継続し、漏洩等の新たな問題が判明した際には、適宜にお知らせいたします。
なお、今回の不正アクセス攻撃によるシステム障害の当社業績に及ぼす影響は、現在精査中です。2023 年３月期第２四半期決算発表につきましては、予定を大幅に変更することのないように進めております。
またこの度、サイバーセキュリティ専門会社の協力のもと進めてまいりました本インシデントに関する調査が完了し、報告書を受領いたしましたので、当該調査結果および再発防止に向けた取り組みにつきまして下記のとおりご報告申しあげます。

記

１．発覚と対応の経緯
・2022 年９月 13 日、当社内システムの停止及び対外公表
早朝、当社内において一部システムにアクセスできないことに気づき、保守を委託しているシステム会社に連絡、確認の結果、ランサムウェアにより複数のサーバーが暗号化され、機能を停止していることが判明いたしました。被害拡大を防ぐため、直ちにネットワークを遮断し、影響範囲の調査を開始いたしました。
更に、警察へ通報、会計監査人やお客様等の社外関係者へ連絡を行い、東京証券取引所及び当社のホームページにて対外公表を実施いたしました。

・2022 年９月 15 日、緊急対策本部の立ち上げ
影響範囲の調査により業務への影響が見込まれたため、緊急対策本部を立ち上げました。
情報漏洩等の被害は確認されておりませんでしたが、念のため、個人情報保護委員会へ報告いたしました。
また、会計監査人と決算対応の相談を開始いたしました。

・2022 年９月 19 日、情報漏洩についてインターネットの監視を開始
情報セキュリティ専門会社の協力により、当社より情報が漏洩していないか、ダークウェブ含めたインターネットの監視を開始いたしました。

・2022 年９月 21 日、フォレンジック等サイバーセキュリティ専門会社に相談開始
調査協力を得ているシステム会社の紹介により、フォレンジック等サイバーセキュリティ専門会社に相談し、不正アクセスの原因究明及び決算発表に影響する会計業務の早期復旧に向けて、支援を受けることといたしました。

・2022 年 10 月４日、フォレンジック調査結果の速報受領
フォレンジック調査結果の速報をもとに、サイバーセキュリティ専門会社、会計監査法人との三者にて、追加調査や会計業務復旧等の方針を検討いたしました。

・2022 年 10 月 11 日、フォレンジック調査結果の続報受領
フォレンジック調査結果の続報を確認の上、システムネットワーク及び業務の安全な復旧に向けて、サイバーセキュリティ専門会社による追加支援を受けることといたしました。

・2022 年 10 月 14 日、システムネットワーク及び業務の復旧作業開始
警察、各システム会社及びサイバーセキュリティ専門会社の協力により、システムネットワーク及び業務の安全対策を含む復旧計画を策定、作業を開始いたしました。

・2022 年 10 月 21 日、フォレンジック追加調査結果の受領、会計業務の復旧作業開始
フォレンジック追加調査結果をもとに、サイバーセキュリティ専門会社、会計監査法人との三者にて、不正アクセスによる影響のないデータの投入を含む、会計業務復旧の計画を検討し、作業を開始いたしました。

・2022 年 10 月 31 日、システムネットワーク及び業務の復旧、対外公表
各システム会社及びサイバーセキュリティ専門会社の支援により、システムネットワーク及び業務の安全対策を含む復旧作業の完了が近日中に見込まれることから、恒久的な再発防止策等を取りまとめ、東京証券取引所及び当社のホームページにて対外公表を実施することといたしました。

２．不正アクセスの原因

（１）VPN 装置におけるパスワード管理の不備
社内ネットワーク・システムを社外から利用するための VPN 装置において、昨年、顕在化した脆弱性に対応するためのアップデートを実施しました。しかし、アップデート前にパスワード情報が漏洩していたため、当時から存在していたアカウントについて、変更していなかったパスワードが不正アクセスに悪用されておりました。

（２）社内システムのセキュリティ管理不備

Webサイト等公開サーバーについてはセキュリティ管理がなされておりました。しかし、社内システムについては、対策ツールの導入や脆弱性管理が十分ではなく、不正アクセスによる、lockbit2.0 と呼ばれるランサムウェアの実行及び暗号化を防ぐことが出来ませんでした。

３．恒久的な再発防止策

（１）技術的対策

不正アクセスの直接的な原因となったVPN装置については、既にパスワード変更等暫定的な対策を実施済みでありますが、恒久的な再発防止策として、認証方式を強化いたします。

また、被害の再発を防止するために、社内システムについても次の対策を進めてまいります。

① 脆弱性管理の徹底
② 攻撃の監視や検知の強化
③ ネットワークアクセス制御の強化
④ 認証方式の強化

（２）組織的対策

外部の専門家による助言や評価等による知見を取り入れ、これまでも活動していた情報セキュリティ委員会及び監査の体制について、機能を継続的に改善してまいります。

また、上記体制の下、最新動向を踏まえた情報セキュリティ教育や訓練について、定期的に実施してまいります。

この度は、お客様はじめ関係各位に多大なるご心配、ご迷惑をおかけすることとなり、重ねて深くお詫び申し上げます。

以　上