株主優待当選者各位

2024年7月19日
ニデック株式会社
ニデックインスツルメンツ株式会社

ランサムウェア感染に関するお詫びとご報告

日頃よりニデック株式会社（以下「当社」といいます。）をご愛顧いただき、誠にありがとうございます。

2024年5月26日、ニデックインスツルメンツ株式会社（以下「インスツルメンツ」といいます。）保有の業務システム等へのランサムウェアによる不正アクセスが発生し、システム内の情報が暗号化されました。

当社は、インスツルメンツに対し、株主優待の贈呈品としてのオルゴールの送付先である株主様の個人データの取扱いを委託していたため、インスツルメンツの社内システムのサーバー及びファイルサーバー等において、当該株主様の個人データも保管されており、これに伴い当該個人データが漏えい、滅失又は毀損（以下「漏えい等」と総称します。）した可能性を否定できないことが判明しました（以下「本件」といいます。）。

インスツルメンツは、ランサムウェア被害の発生後、適時に必要な調査を進めてまいりましたが、このたび調査を完了いたしましたので、本通知では、インスツルメンツ及び同社グループ会社（以下「インスツルメンツグループ」といいます。）から個人データが漏えい等したおそれのある当社の株主様宛に、本件に関するインスツルメンツグループの調査結果をご報告申し上げます（一部の内容は、これまでに公表した内容と重複します。）。

株主様に不正確な情報をお伝えしてさらにご迷惑をおかけしないよう慎重に調査してまいりましたが、その結果、株主様へのご連絡にお時間を頂戴しましたことを深くお詫び申し上げます。

1. 漏えい等が発生し、または発生したおそれがある個人データの項目と件数
    - 個人データの項目　氏名、住所、郵便番号
    - 株主様の人数　482名
    - 個人データの件数　482件

上記個人データが漏えいした可能性のある株主様は、当社が2020年から2023年までの間に株主優待としてオルゴールを贈呈した株主様のみであり、それ以外の株主様はこれに含まれません。

なお、本件攻撃者によるリークサイトにおいて、本件に関連すると思われるダウンロードサイトへのリンクが掲載されましたが、当該リンクからダウンロード可能であったファイルの中には、当該株主様の個人データは含まれていないことを確認しております。

2. 原因と対応状況

(1) 原因

本件の原因は、本件攻撃者が、システムの管理者アカウントの ID 及びパスワードを何らかの形で不正に取得し、インスツルメンツの業務システム内にアクセスしたことにあると考えられます。

(2) 対応状況

インスツルメンツは、当社と協議の上、すべての ID に対するパスワードの変更及びサイバー攻撃を受けた端末のネットワークからの隔離等の、被害の拡大を防止し、外部の方々が保有・保管するシステムに影響を及ぼすことが無いようにするための対策を行いました。

また、インスツルメンツは、現在までに、インターネットに接続する場合は、原則としてクリーン PC（社内ネットワークに接続しない端末）を使用するとともに、クリーン PC 以外の端末は、メールやウェブ会議を利用する場合等の業務上必要な最小限のものを除き、インターネットとの通信を遮断することで、外部からの不審な通信を受け付けないようにしております。メールについても、接続元 IP アドレス制限を行い、意図しない第三者の利用を防止しております。これらの措置を含む総合的なセキュリティ対策により、外部の方々が保有・管理するシステムに影響が及ぼすことのないよう努めております。

3. 二次被害またはそのおそれの有無及びその内容

ランサムウェアによる不正アクセスが発生したのは、インスツルメンツ保有の業務システムであり、当該業務システムとは完全に別個の当社の業務システムにはランサムウェアの被害は及んでおらず、当社との関係においては、当社がインスツルメンツに委託した情報に限定して本件の被害が生じております。そのため、当社に関しては、本件において二次被害のおそれはありません。

万が一、当社グループを騙り、又は本件攻撃者を自称する等の不審なメール等を受信された場合は開かず、また、当該メッセージに記載された URL 等へのアクセスはしないようお願い申し上げます。

4. 再発防止策

インスツルメンツは、当社と協議の上、再発防止策を講じております。具体的には、インスツルメンツは、本件を受け、社内アカウントの不正使用を防止するため、全ての社内アカウントのパスワードを変更し、不要なアカウントについては削除しました。また、業務システムへの不正アクセスを防止するため、社外から VPN を通じて社内ネットワークに接続することが可能なユーザを限定する設定に変更しました。

5. お問い合わせ先

本件に関するお問合せは下記の連絡先までお願いいたします。

ニデックインスツルメンツシステム障害コールセンター　電話；0120－234430

（土日祝日を除く日本時間月曜日から金曜日 9:00～18:00 まで）

6. これまでの対応経緯詳細

本件に関する当社及びインスツルメンツグループのこれまでの対応経緯は以下のとおりです。なお、

当社及びインスツルメンツグループは本件攻撃者からの身代金要求には一切応じておらず、また、外部セキュリティ専門機関と連携し、リークサイトの継続的な監視を続けております。

- 5 月 26 日、インスツルメンツの情報システム部の社員が、本件に関する攻撃を検知しました。同日中に、初動対応として、EDR ソフトやマルウェアの駆除ソフトを利用し、本件の原因となったマルウェアの駆除を行いました。また、弊社内で対策チームを組織しました。
- 5 月 27 日、インスツルメンツグループの全社員に指示の上、インスツルメンツグループの全 PC について、本件の原因となったマルウェアが起動されていないことを確認しました。

  同日、バックアップデータからのデータ復旧によって、最低限の対外的業務継続体制を構築しました。
- 5 月 28 日、インスツルメンツグループの情報が外部の第三者に漏えいした可能性が否定できないことから、本件について長野県警に通報・相談を開始しました。加えて同日以降、社内基幹システムおよび周辺システムの復旧を行うとともに、セキュリティ製品を取り扱うベンダーと連携の上、復旧対応等を試みてまいりました。
- 6 月 3 日、外部セキュリティ専門機関に依頼の上、事実関係の専門調査を開始しました。なお、本件攻撃者からは、当社に対し身代金の支払要求がありましたが、反社会的勢力に対する利益供与には応じられないこと等の理由から現時点に至るまで、身代金の支払いは一切実施しておりません。
- 6 月 10 日、当社及びインスツルメンツのホームページにおいて、「弊社にて発生したセキュリティインシデントについて」を公表いたしました。また、同日、インスツルメンツにおいて個人情報保護委員会に対する速報を行うとともに、従業員に対して同旨の正式な社内通知を行いました。また、インスツルメンツ以外のインスツルメンツグループ会社も、翌 11 日、個人情報保護委員会に対する速報を行いました。
- 6 月 12 日、外部弁護士への相談を開始しました。
- また、同日、外部セキュリティ専門機関から、初期的な調査の報告を受けました。
- 6 月 18 日、本件攻撃者によるリークサイトにおいて、インスツルメンツグループに関連すると思われるダウンロードリンクが掲載され、インスツルメンツグループの情報がダウンロード可能な状態になっていることを確認しました。ただし、その後の調査により、6 月 19 日以降、そのリンクからダウンロードができない状態になっていることを確認しております。
- 6 月 26 日、インスツルメンツからの調査報告により、本件攻撃者によって不正アクセスが可能であったインスツルメンツサーバー内に、前記 1 記載の株主様の個人データが保存されていたため、当該株主様の個人データが漏えい等したおそれが否定できないことが判明しました。
- 7 月 12 日、漏えい等の可能性のある情報の項目・件数等の調査が完了いたしました。

同日、個人データが漏えい等した可能性のあるご本人様の特定が完了いたしました。

- 7 月 15 日、お取引先様及びお客様により安心・信頼いただける環境の構築が完了いたしました。その具体的な内容は、前記 2(2)「対応状況」をご参照ください。
- 本日、個人データが漏えい等した可能性のあるご本人様に対し、その旨をご報告する通知書を送付するとともに、個別に通知することができないご本人様等に向けて、当社ホームページにおいて「ランサムウェア感染に関するお詫びとご報告」を公表の予定です。
- 7 月 24 日、個人情報保護委員会への確報を行う予定です。

株主様をはじめ、関係者の皆様にご迷惑及びご心配をおかけする事態となりましたこと、改めて深くお詫び申し上げます。

以上