

2024年7月25日

ニデック株式会社

当社グループ会社におけるセキュリティインシデントの発生について（第三報）

6月10日及び同月27日にお知らせいたしました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。）におけるランサムウェア被害の発生についての第三報をお知らせいたします。関係者の皆様にご迷惑とご心配をおかけすることとなり深くお詫び申し上げます。

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おりますが、インスツルメンツが当社より委託を受け管理していた、株主優待としての贈答品（オルゴール）当選者の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。）したおそれが否定できないことが判明いたしました。

この度、その当選者である株主様に関しては調査が完了しましたので、当社は、インスツルメンツと連名で、個人データが漏えい等したおそれのある株主様宛に、本件に関する調査結果を7月19日に郵送しております。通知内容はこちらとなります。

インスツルメンツによる発表については下記をご参照ください。

弊社の不正アクセスによる個人情報漏えいの可能性に関するお詫びとお知らせ（第三報）

ニデックインスツルメンツ株式会社

ニデックマテリアル株式会社

東京丸善工業株式会社

ニデックインスツルメンツ秋田株式会社

株式会社サンセイキ

ニデックインスツルメンツサービスエンジニアリング株式会社

一般社団法人ニデックオルゴール記念館すわのね

日頃よりニデックインスツルメンツ株式会社をご愛顧いただき、誠にありがとうございます。

このたび、当社及び当社のグループ会社（以下「当社グループ」といいます。）は、2024年6月10日及び同月27日付けで当社及びニデック株式会社のウェブサイトにて公表させていただきましたとおり、外部の悪質な攻撃者（以下「本件攻撃者」といいます。）からサイバー攻撃を受け、複数のサーバー内のファイルが暗号化されるランサムウェア被害を受けました（以下「本件」といいます。）。

本通知では、本件に関する当社グループの現時点での調査結果を再度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。）。

なお、本件に関するランサムウェア被害は当社グループ以外のニデック株式会社及びそのグループ会社へは波及していないことを重ねてご報告させていただきます。

改めまして、皆さまにご迷惑とご心配をおかけしておりますことを心より深くお詫び申し上げます。

1. 本件の概要

2024年5月26日、ランサムウェアによる当社保有の業務システム等への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。

調査の結果、当社ホームページにて6月27日付けで公表した「弊社への不正アクセスによる個人情報漏えいの可能性に関するお詫びとお知らせ」のとおり、当社のみならず、国内当社グループのニデックマテリアル株式会社・東京丸善工業株式会社・ニデックインスツルメンツ秋田株式会社・株式会社サンセイキ・ニデックインスツルメンツサービスエンジニアリング株式会社・一般社団法人ニデックオルゴール記念館すわのね及び一部の当社海外現地法人(注)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ける一部データについて暗号化されたこと、及び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、当社グループが保有する情報の一部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が判明しました。なお、その後の調査により、現在当該ファイルは当該ダウンロードサイトからダウンロードできなくなっていることが確認されています。

これまでの対応経緯の詳細につきましては後述いたします。

注：当社グループとは別のネットワーク構成であるため、下記9社は、本件の影響を受けておりません。

- ① SCD Co.,Ltd
- ② SCD (Guangzhou) Co.,LTD
- ③ SCD (Hong Kong) Co.,LTD
- ④ ニデックインスツルメンツ（米国）株式会社
- ⑤ ニデックインスツルメンツ（メキシコ）株式会社
- ⑥ ニデックインスツルメンツ（欧州）株式会社
- ⑦ ニデックジェンマークオートメーション株式会社
- ⑧ ニデックジェンマークオートメーション（蘇州）株式会社
- ⑨ ニデックジェンマークオートメーション（欧州）株式会社

2. 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

▶ お取引先様他関係者の皆様に関する情報

- ・ 個人データの項目

氏名、性別、住所、生年月日、電話番号、メールアドレス

- ・ 個人データの件数

318,151件

（個人データの延べ件数であり、ご本人様の人数は318,151よりも少なくなります）

▶ 当社のオルゴールをご購入いただいたお客様及び当社主催のイベント等にご参加いただいた皆

様に関する情報

- ・ 個人データの項目
氏名、性別、住所、電話番号、メールアドレス
- ・ 個人データの件数
71,089 件
(個人データの延べ件数であり、ご本人様の人数は 71,089 よりも少なくなります)

▶ 従業員、元従業員、契約社員、元契約社員及びそのご家族に関する情報

- ・ 個人データの項目
氏名、性別、住所、生年月日、電話番号、メールアドレス、マイナンバー、口座情報、給与情報、賞与情報、退職金情報、雇用保険被保険者番号、健康保険証番号、基礎年金番号、旅券番号
- ・ 個人データの件数
13,290 件
(個人データの延べ件数であり、ご本人様の人数は 13,290 よりも少なくなります)

3. 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、当社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

初期的には、暫定対処として、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を行いました。

また、当社は、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。

4. 二次被害またはそのおそれの有無及びその内容

「1. 本件の概要」に記載したとおり、本件攻撃者によるリークサイトからはデータのダウンロードができなくなっていることを確認しております。また、「2. 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」に記載のとおり、漏えい等の可能性のある情報の項目の中に、クレジットカード情報等の経済的な二次被害を直接生じさせ得る情報は含まれておりません。以上のほか、当社においては、現時点で、本件に起因する個人データを用いた不正利用等の二次被害については、確認さ

れておりません。

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。

5. 再発防止策

当社は、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。

また、当社グループは、本件を受け、更なる情報管理体制の強化に努め、本件の再発防止に取り組んで参ります。

※「Virtual Private Network」の略称で、インターネット上に設定された仮想の専用線であり、特定の人のみが利用できる専用ネットワークを指します。

6. 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。

0570-004066【ナビダイヤル】

7. これまでの対応経緯の詳細

本件に関する当社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、当社グループ及びニデック株式会社は、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、当社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、当社グループの全社員に指示の上、当社グループの全 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、当社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、当社への攻撃と並行して当社の親会社であるニデック株式会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、当社及びニデック株式会社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、当社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、当社以外の国内グループ会社も、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、当社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、ダウンロードが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、当社の調査により、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トルメンツサーバー内に、ニデック株式会社の一部の株主様の個人データが保存されており、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たため、当社は、ニデック株式会社に対し、当該漏えい等のおそれについて報告しました。
- ・ 7月12日、漏えい等の可能性のある情報の項目・件数等の調査及び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3(2)「対応状況」をご参照ください。
- ・ 7月24日、個人情報保護委員会への確報を行いました。
- ・ 7月25日以降順次、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、本日、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」を公表いたしました。

お客様をはじめ、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