2026年11月25日

各　位

会社名 大崎電気工業株式会社
代表者名　取締役会長 CEO　渡辺 佳英
（コード番号 6644 東証プライム）
問合せ先　取締役専務執行役員
グループ経営本部長 上野 隆一
（TEL　03-6694-7140）

ランサムウェアによるサイバー攻撃に伴う生産停止に関するお知らせ（第三報）

業務再開の見通しに関するお知らせ

当社は、2026年11月18日付「ランサムウェアによるサイバー攻撃に伴う生産停止に関するお知らせ（第一報）」および同年11月20日付の第二報にてお知らせしましたとおり、2026年11月17日にランサムウェアによるサイバー攻撃を確認しました。お客様をはじめ関係する皆様に多大なご迷惑とご心配をおかけしておりますことを、あらためて深くお詫び申し上げます。

その後、外部の専門機関とともに、侵入経路の遮断状況および各システム・端末の安全性を確認してまいりましたが、**安全が確認できた範囲から業務を再開する見通しが立ちました**ので、2026年11月25日（水）時点の状況として下記のとおりお知らせいたします。

なお、調査は継続中であり、今後の調査結果により内容が変わる可能性があります。変更があった場合は、当社ホームページ等で速やかにお知らせいたします。

記

1. 本報の概要

（1）業務再開：侵入経路を遮断し、安全が確認できた範囲から、**2026年11月27日（金）以降、段階的に生産を再開する予定**です。受注済み製品の出荷および新規受注の再開時期は、生産とは別にご案内いたします。詳細は「3. 業務再開の見通し」をご参照ください。

（2）情報漏えい ：**社内システムから外部にデータが送信された事実を確認**しております。送信された情報の内容および範囲は調査中です。

（3）製品・生産設備：今回の攻撃による**生産設備への影響はなかったことを確認**しております。**ご利用中の製品・サービスの動作への影響は、現時点で確認されておりません。**

（4）グループ会社 ：**大崎電気システムズ株式会社に対する不正アクセスを確認**しました。同一のネットワーク上にあるグループ会社への影響は調査中です。詳細は「6. グループ会社への影響」をご参照ください。

2. 再発防止と安全確認の状況

再侵入や再暗号化を防ぐため、次の措置を講じ、安全性の確認を進めております。

対象	実施・確認状況
侵入経路（VPN 機器）	侵入を受けた機器および不正アクセスの中継に使われた可能性のあるサーバー等は停止しており、再稼働しておりません。外部からの接続は、接続方式および認証対策の安全性を確認したうえで再開します。
認証・アカウント	パスワードの再設定および多要素認証の適用状況を確認中です。
サーバー（仮想・物理）	確認した範囲では、**サーバーの改ざんの痕跡や暗号化ファイルの残存は確認されておりません。**監視・防御を継続しております。
ファイルサーバー等のデータ	確認した範囲では、**暗号化ファイルの残存は確認されておりません。**改ざんの有無を含めてデータの安全性を確認し、確認を終えたものから利用を再開します。
社内 PC	端末の安全性の確認を進めています。不正アクセスが確認された端末は隔離して、**安全性の確認が完了した端末から順次利用を再開**します。
Web サービス・業務システム 持ち出し用 PC	端末や認証情報を介した不正アクセスを防ぐため、認証情報の再設定とアクセス制御の確認を進めております。**確認できたものから再開**します。
生産設備	生産設備のネットワークは業務系ネットワークと基本的に分離しており、**今回の攻撃による生産設備への影響がなかったことは確認済です。**

上記の措置により、**同じ経路からの再侵入や社内システムの再暗号化のリスクは低減した**と判断しております。業務再開は、安全を確認した範囲に限ります。確認が完了していない範囲は引き続き利用を制限し、復旧後も監視を強化します。

情報漏えいの調査は、業務再開の判断とは別に継続します。

3. 業務再開の見通し

（1）方針 ： 安全が確認できた範囲から、手作業による対応を、システムを利用した通常業務へ段階的に切り替えます。**生産再開後、出荷に必要な条件を確認できた受注済み製品から順次出荷**いたします。新規受注の通常運用への切り替えは、お客様側システムとの連携を確認したうえで、出荷とは別に進めます。

区分	再開・正常化の見通し	備考
生産 ・埼玉事業所、 ・岩手大崎電気株式会社 ・大崎プラテック株式会社	**11 月 27 日（金）以降**	安全を確認した端末・システム・データを利用し、**段階的に生産を再開**いたします。
受注済み製品の出荷	**12 月 1 日（火）以降**	生産再開後、出荷に必要な条件の確認が完了したものから再開します。納期は個別にご案内いたします。
新規受注（受発注・お客様側システムとの連携）	**12 月 7 日（月）以降**	システム連携先にお客様については、確認できたお客様から順次再開いたします。

（2）お客様への対応 ： 受注済み製品の納期や、新規受注の再開に向けたシステム連携については、担当の事業部または資材部門から個別にご案内いたします。

（3）留意事項 ：再開予定は現時点の見通しであり、安全確認の進捗により変更する場合があります。変更があった場合は、当社ホームページ等で速やかにお知らせいたします。

4. 情報漏えいについて

（1）確認した事実 ： 2026 年 11 月 19 日、インターネット上のサイトに、当社のシステムに保存されている情報と思われる技術情報が掲載されていることを認知しました。その後の調査では、不正アクセスにより、社内システムから外部のクラウド型ストレージサービスにデータが送信された事実を確認いたしました。

（2）調査状況 ： ログの確認に時間を要しており、外部に送信された情報の内容および範囲は引き続き調査中です。

（3）当社の対応 ： 当該サービスの提供事業者に対し、データの保全・隔離・削除等を求める手続きを進めております。警察等の関係当局には、引き続き事態の報告・相談を行っております。当社は、攻撃者の要求には応じない方針です。

（4）個人情報・お取引先様情報 ： 外部に送信された情報に個人情報が含まれるかは調査中です。関係法令に基づき、個人情報保護委員会への報告や対象となる方への通知など、必要な対応を行います。お取引先様との秘密保持契約に基づき管理している情報が含まれる場合はお取引先様に個別にご連絡いたします。

（5）お願い ： 「当社のシステムに保存されている情報と思われる技術情報」とされるものにアクセスしたり、拡散したりしないでください。当該サイトへのアクセスに起因して生じた被害について、当社は責任を負いかねますので、アクセスは絶対におやめください。

また、「当社のシステムに保存されている情報と思われる技術情報」とされるものをインターネット上で見かけた場合でも、転載や SNS での再投稿、当該情報へ誘導するリンクの共有なども絶対におやめください。

5. 製品・サービスの安全性について

本件は当社の社内システムに対する攻撃であり、**スマートメーター等の製品・サービスそのものが攻撃対象ではありません。**

生産設備への影響はなかったことを確認しており、**お客様がご利用中の製品・サービスの動作への影響は確認されておりません。**

6. グループ会社への影響

（1）確認した事実 ： 大崎電気システムズ株式会社が、当社がサイバー攻撃を受けた同日（11 月 15 日）に今回の侵入に使われたものと同一の VPN 機器を経由した不正アクセスを受けていたことを確認いたしました。

（2）調査状況 ：同一のネットワーク上にあるグループ会社への影響は、外部の専門機関とともに調査中です。

（3）その他のグループ会社 ： 同一のネットワーク上にないグループ会社（株式会社エネゲート、EDMI LIMITED など）では、現時点で被害は確認されておりません。状況に変更があった場合は、速やか当社ホームページ等でお知らせいたします。

7. 業績への影響

影響額（見込み額を含む）は、業務再開の状況や調査の結果にもよるため、現時点では未定です。開示すべき事項が生じた場合は、適時開示等によりお知らせいたします。

8. 今後の予定

業務再開の状況、情報漏えいの調査結果等、公表すべき事項が判明した場合には、当社ホームページ等で速やかにお知らせいたします。

9. 関係者の皆様へのお願い

① 受注済み製品の納期や今後のご発注についてご不明な点がございましたら、担当の事業部または資材部門にお問い合わせください。

② 当社を装った不審なメールを受け取った場合は、添付ファイルやリンクを開かないでください。不審な電話を受けた場合は、個人情報等を伝えずに電話をお切りください。いずれの場合も、下記のお問い合わせ先にご連絡ください。

お客様をはじめ関係する皆様に多大なご心配、ご迷惑をおかけしておりますことを、重ねてお詫び申し上げます。

【本件に関するお問い合わせ先】

○ お客様・お取引先様： 当社事業部または資材部門へお問い合わせください。

○ 報道機関の皆様　： コーポレートコミュニケーション部　pr_all@osaki.co.jp

以　上