Kawasaki
Powering your potential

News Release

川崎重工業株式会社

NO.2020093

2020 年 12 月 28 日

当社グループへの不正アクセスについて

川崎重工は、下記のとおり、社外から不正アクセスを受け、詳細な調査の結果、一部の情報が海外拠点から外部に流出した可能性があることを確認しましたのでご報告します。

現時点では、社内からの情報流出に関して特定できた事実はありませんが、不正アクセスの範囲が複数の国内・海外拠点であるため公表までに時間を要したこと、ならびにお客様をはじめ関係先にご迷惑とご心配をお掛けしますことを深くお詫び申し上げます。

記

１．概要

2020年6月11日、社内で実施しているシステム監査において、本来発生しないはずの海外拠点（タイ）から日本国内のサーバへの接続を発見し、同日中に不正アクセスとして同拠点と国内拠点との通信を遮断しました。しかし、続いて断続的に他の海外拠点（インドネシア、フィリピン、米国）を経由した国内のサーバへの不正アクセスが確認されたため、海外拠点からのアクセス監視強化とアクセス制限の厳格化を進め、不正アクセスを遮断しました。その後も全社的なセキュリティ対策強化を継続的に実施しています。

２．経緯

6月11日	国内拠点のシステム監査で、海外拠点（タイ）からの不正アクセスを確認 海外拠点（タイ）と国内の接続を遮断 不正アクセスの範囲を特定する調査を開始
6月15日	海外拠点（タイ）から社外にデータが送信されていた可能性を確認
6月16日	海外拠点（タイ）から国内データセンターの複数サーバへの不正アクセスが発生していたことを確認
6月24日	海外拠点（インドネシア、フィリピン）から国内拠点への不正アクセスを確認 両拠点と国内拠点の接続を遮断
7月8日	海外拠点（米国）から国内拠点への不正アクセスの疑いを確認 海外拠点（米国）と国内拠点の通信を制限
8月3日~	すべての海外拠点と国内拠点の通信を厳格に制限 国内とタイの端末約2万6千台の詳細検査を実施 （10月末までに正常化を確認）
10月5日~	侵害があった海外拠点（タイを除く）の端末約3千台の詳細検査を実施 （11月末までに正常化を確認）
10月30日	通信監視により8月以降、国内へ不正侵入されていないことを確認
11月30日	遮断した海外拠点の接続を再開
12月21日	遮断した海外拠点の接続を再開した後の通信監視により、上記海外拠点を起点とする通信に異常がないことを確認

３．影響

当社グループはこれまでにも、個人情報、社会インフラ関連情報をはじめ重要な機密情報を取り扱うため、情報セキュリティ対策は最重要課題として取り組んできましたが、今回の不正アクセスは痕跡を残さない高度な手口によるものです。

ついては不正アクセス確認後、外部専門機関との特別プロジェクトチームによる調査・対策を進めています。その調査で内容不明の情報が外部に流出した可能性を確認しましたが、現時点では個人情報を含め、社内からの情報流出に関して特定できた事実はありません。

なお今回の不正アクセスの影響を受けた可能性があるお客様には、個別に連絡をしています。

４．今後の対応

引き続き、海外拠点と国内拠点間の通信ネットワークでの監視とアクセス制御の厳格化を進めるとともに、社長直轄組織のサイバーセキュリティ総括部（2020年11月1日付設立）が、再発防止に向け、最新の不正アクセス手法に対応したセキュリティ対策の強化を推進していきます。

以 上