Kawasaki
Powering your potential

News Release

川崎重工業株式会社

NO.2021044

2021 年 7 月 30 日

# 当社グループへの不正アクセスについて（調査報告）

川崎重工は、第三者による不正アクセス（2020年12月28日公表）について、国内外の全事業拠点で、外部専門機関との特別プロジェクトチームによる高度な専門調査を進めてきました。

これまでの調査で、当社グループ外に情報が流出した可能性を確認し、不正アクセスの範囲・種類を特定するとともに対策を講じ、情報流出の可能性があるお客様へ調査結果を報告しました。

現在までお客様および取引先に関する具体的な被害は確認されていませんが、改めて関係する皆様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。

なお調査報告については下記のとおりですが、お客様に関する具体的な情報、不正アクセス対策の詳細は、情報セキュリティ確保の観点から開示できない点をご了承いただきますようお願い申し上げます。

記

１．調査結果

（１）マルウエア調査※1

当社グループの主要国内拠点および侵害を確認した海外拠点のPC、サーバ（約29,000台）のマルウエア調査を実施し、海外拠点においてはマルウエア除去による正常化を、国内拠点にはマルウエアが侵入していないことを確認しました。

（２）フォレンジック※2分析

通信量が多いPC、サーバ（約6,700台）を抽出し、侵害の痕跡を調査した結果、不正アクセスを受けた可能性のある国内外拠点のサーバ（合計36台）を特定しました。これらのサーバに詳細なフォレンジック分析を行い、うち15台のサーバに不審な暗号化ファイルがあったことが判明しました。さらに暗号化ファイルに含まれる可能性がある情報を絞り込み、その情報に関係するお客様に分析結果の報告を行いました。

（３）通信ログ調査

通信ログを調査した結果、タイ、インドネシア、米国の拠点からインターネット上の不審なサーバに向けたデータ送信を確認しました。

なお、上記のとおり、情報流出の可能性を確認しましたが、個人情報流出については、現時点で確認された事実はありません。

２．対策状況

海外拠点と国内拠点間の通信管理の厳格化、データ交換プロセスの変更、認証基盤の不正アクセス対策を実施し、現時点で新たな攻撃、被害は確認されていません。さらに常時通信監視の継続、特にリスクが高いと思われる国内外拠点については端末監視を強化し、不正アクセスの検知体制を拡充しました。

３．今後の対応

再発防止に向けては、国内外拠点間の通信ネットワーク監視とアクセス制御の厳格化を進め、不正アクセスをいち早く検知するとともに、迅速な被害範囲の特定と対応が可能となるプロセス強化、さらに人員増による体制強化と情報セキュリティの意識向上を目的とした社内教育の拡充を進めています。

そして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、サイバーセキュリティ総括部を中心として警察、関係省庁、セキュリティ専門会社等と連携しながら、当社グループ全体で強力に推進していきます。

※1　不正かつ有害な動作を行う意図で作成された悪意のあるソフトウエアや悪質なコードの総称

※2　記録媒体に残された詳細なデータから、事故原因や犯罪の証拠を探し出す作業

以 上