

2023年5月7日

お客様各位

株式会社ネットワーク
代表取締役社長 森田 晶一

当社への不正アクセスに関する経過報告

株式会社ネットワークは、当社の設備が攻撃者からの不正アクセスを受けたことを4月8日に検知し、前日の4月7日からランサムウェアに感染したことを、4月13日に第一報としてご報告致しました。インシデント発生から1か月が経過しました本日5月7日、これまでの経緯もまとめた追加のご報告を申し上げます。

社内調査の結果、当社の基幹システム（販売管理システム等）以外へ、外部からの不正アクセスがあり、業務系サーバー及び、業務系ファイルサーバーへ侵入された痕跡を確認致しました。また不正アクセスにより、一部の情報が外部に漏洩した可能性があることも判明しました。4月8日時点において、不正アクセスの疑いがある機器の停止（サーバー等）などの初動措置を終えております。また現在に至るまで、影響を受けた可能性があるお客様には、順次ご連絡を差し上げており、あわせて、再発防止に向けた対応を実施しております。

皆様には、多大なるご心配とご迷惑をおかけしておりますこと、心よりお詫び申し上げます。当社では、今回の事態を重く受け止め、再びこのようなことがないよう、より一層の管理体制の強化に努めてまいります。

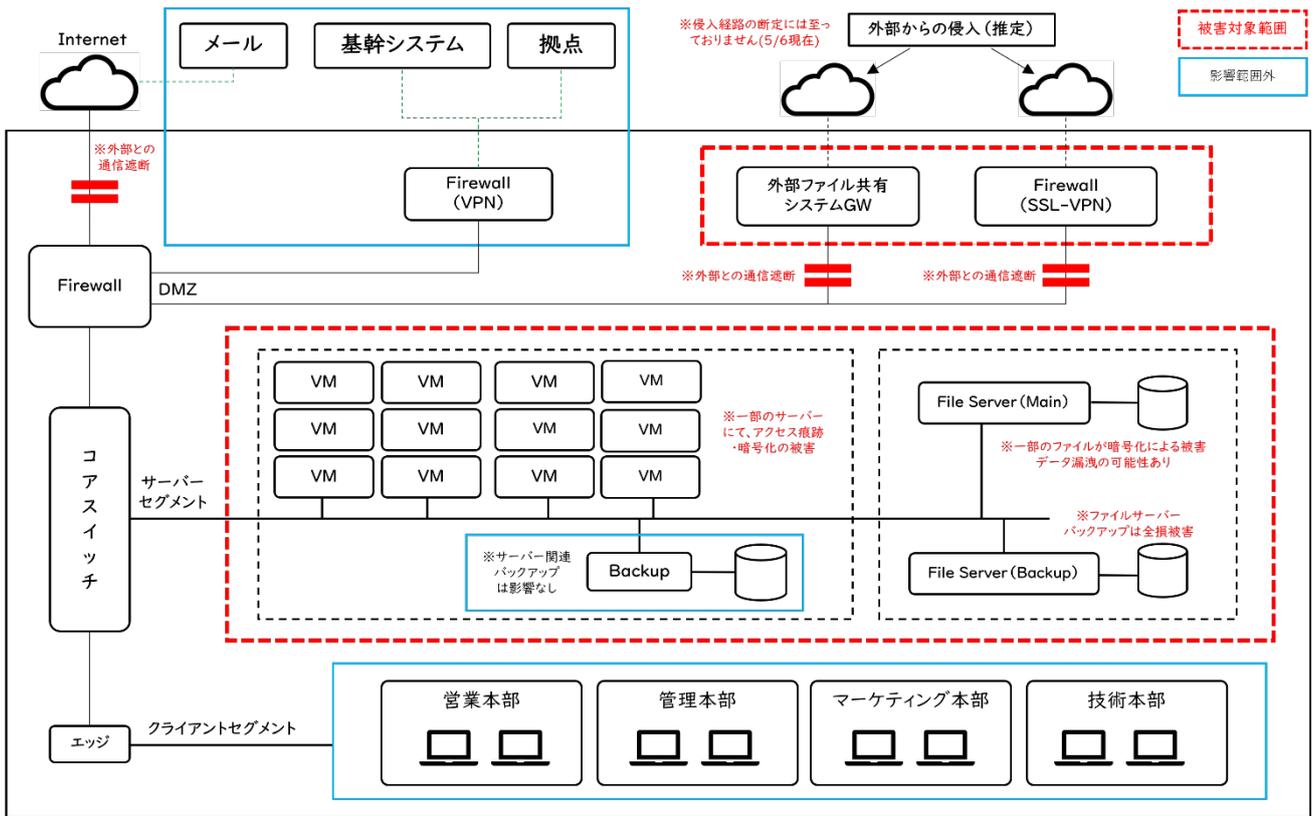
1. 不正アクセス検知後の当社対応経緯

4月8日早朝に当社社員が、業務系ファイルサーバーへアクセスしたところ、不審なファイルを発見しました。同日午前には外部アクセスの遮断、不正に利用されたアカウントの特定及び停止、本社内の業務系サーバー含む業務システム全体の緊急停止措置を実施致しました。同日午後には、基幹システム、各種SaaS関連サービス（メール等）、クライアントPC端末の調査を行い、不正アクセスは概要図に記載した範囲であることを確認致しました。

その後、アクセスログ調査から、一部の情報が漏洩した可能性があることが判明、当該データがお客様情報を含む内容であったことから、お客様毎にご報告を開始いたしました。

また、セキュリティ専門会社からの支援も得て、不正アクセスの痕跡があるサーバーのフォレンジック調査とログ分析により、侵入経路及び漏洩の可能性があるファイルの特定について調査を進めております。

【4月8日時点の発生事象概要図】



2. お客様への影響

現時点で、漏洩の可能性が判明している情報は、業務系ファイルサーバー及び、業務系サーバー内にあったお客様データの一部となります。本掲載においては、機密保持の観点から、個別のお客様に関する情報の開示は差し控えさせていただきます。本事象の影響を受けた可能性があるお客様には、順次ご連絡を差し上げております。

3. 今後の対応

事態発覚後に実施してきたセキュリティ対策により、現在の当社システムは安全に運用されているものと考えています。引き続き現在調査中の侵入経路及び、漏洩の可能性や未確認のファイルの特定について調査を行うとともに、再発防止のためのセキュリティ対策、監視体制の強化を進め、最新の攻撃手法に対応可能な対策を講じてまいります。

新たにお知らせすべき内容が判明した場合、速やかに情報を開示してまいります。ご理解賜りますよう、よろしくお願い申し上げます。