2023 年 10 月 6 日
富士ソフト株式会社

当社の社内システムに対する不正アクセスについて（10/6 追記）

10 月 6 日の報告

今回発生した不正アクセスについて、本日までの調査で確認できました点についてご報告させていただきます。

10 月 2 日にご報告した通り、今回の不正アクセスは、当社を狙った標的型攻撃であることが確認できています。当社内の端末に社外から侵入されたことで、20 ファイルが持ち出されました。その直後に、当社 SOC※1 にて検知し、CSIRT※2 がアクセスを遮断して被害を局所化、以降のサイバー攻撃は発生しておりません。持ち出された 20 ファイルにつきましては、全てが当社の作業上の資料であり、お客様から受領した資料やお客様に納品する資料は含まれておりません。

その後、標的型攻撃が停止されていることを確認しており、追加的に対応した当社の多重防御対応により抑止効果が発揮できていると考えております。被害を受けたシステムを除き、当社社内システムに被害がないこと、また、当社が使用する標準開発管理環境にも不正アクセスの影響がないことを確認いたしました。
第三者機関にも協力を頂き、サーバなどのログ調査を継続しておりますが、現在のところ、不審なログ等はないことを確認しています。引き続き対応を進め、調査が完了次第、あらためて最終的な報告を実施させていただく予定です。

本件に関して、関係する皆様にご迷惑とご心配をおかけいたしますことを心よりお詫び申し上げます。
今後、同様の事態を起こさないよう、再発防止に努めるとともに、不正アクセスなどの犯罪行為には厳正に対処してまいります。

※1 SOC とは「Security Operation Center」の略称で、サイバー攻撃の検出・分析を行い、対応策のアドバイスなどを行う専門組織です。

※2 CSIRT とは「Computer Security Incident Response Team」の略称で、インシデント（サイバー攻撃によるセキュリティ事故）の予防及び発生後の迅速な対処を行うことを目的とした組織（機能）です。

10 月 2 日の報告

今回発生した不正アクセスは、当社を狙った標的型攻撃であることが調査により判明しました。攻撃により一部の環境の侵害を受けましたが、すぐに封じ込めができており、また他の環境にもマルウェア感染等の被害が出ていないことを確認できています。攻撃者の侵入経路は既に特定し封鎖済みであり、9 月 22 日以降は攻撃も確認されていません。

本日時点において当社内で影響範囲の特定と対策はできておりますが、引き続き第三者機関にも協力を頂き、さらに厳密な範囲の確認、発生事象の詳細確認等を行い、最終的な対応を行う予定です。

本件に関して、関係する皆様にご迷惑とご心配をおかけいたしますことを心よりお詫び申し上げます。

今後、同様の事態を起こさないよう、再発防止に努めるとともに、不正アクセスなどの犯罪行為には厳正に対処してまいります。

9 月 27 日の報告

富士ソフト株式会社は、社内システムに対して第三者から複数の不正アクセスがあり、2023 年 9 月 22 日に社内情報の一部に情報漏えいの可能性があることを確認いたしました。現在、関係機関への報告は完了しており、その後の対策で被害も最小限にとどめられていると判断しています。

また、第三者機関の協力も得ながら、引き続き、発生事象の詳細および原因の調査、防衛対策に取り組んでおりますが、今後の調査により、関係者の皆様に影響の可能性がある事象が明らかになった場合には、速やかにご報告させていただきます。

本件に関して、関係する皆様にご迷惑とご心配をおかけいたしますことを心よりお詫び申し上げます。

今後、同様の事態を起こさないよう、再発防止に努めるとともに、不正アクセスなどの犯罪行為には厳正に対処してまいります。

以上

<お問い合わせ>
●ニュースリリースについて
コーポレートコミュニケーション部　広報窓口
URL：https://www.fsi.co.jp/
TEL：050-3000-2735
E-MAIL：mkoho@fsi.co.jp