

2025年 2月 4日

お客様 各位

マルティスープ株式会社

## 「iField」環境の一部への不正アクセスに関するお知らせ

拝啓 平素より当社が提供するサービス「iField」をご利用いただき誠にありがとうございます。

「iField」を運用しているクラウドサービス環境の一部において、外部からの不正アクセスが確認された件について、2024年11月5日以降、随時お客様に対しご報告を行ってまいりました。この度、第三者機関の協力の下、当社環境のセキュリティに関する調査・対策を実施し、その結果を踏まえた上で本不正アクセスの経緯、原因、再発防止策を下記の通りまとめましたので、ご報告いたします。なお、本内容を以て本件の最終報告いたします。

敬具

### 記

#### 1. 経緯

本不正アクセスに関する一連の経緯は、下記の通りとなります。

2024年10月16日に当社の利用するメール送信サービスを介してスパムメールの大量発信が行われたことが発覚し、当該サービスの停止に始まる緊急対策と原因調査を実施しました。調査の結果、AWSアクセスキーの不正利用によるものと判断されたため、既存のアクセスキーの削除等の対策を行いました。ログの調査にてストレージサービスの一部への不正アクセスの痕跡も確認され、早急に対策を施すとともに調査を全関連環境に拡大いたしました。当該調査において、前述の範囲以外では重大なセキュリティ侵犯は確認されませんでした。

被害の全容が確認され次第、個人情報保護委員会やIPAへの報告、お客様への説明を行いました。また第三者機関にも相談した結果、アクセス元の特定は困難と結論づけて断念し、外部機関によるセキュリティ調査を実施の上でセキュリティ強化施策を適用しました。今後も引き続き対策を実施してまいります。

#### 2. 影響の範囲

本不正アクセスにより影響を受けた範囲は以下となります。

開発・運用のための情報管理環境の一部

- (1) メール送信サービス
- (2) ストレージサービス

個人情報が流出した可能性のある対象数 432名分

個人情報が流出した痕跡は発見されておりません。外部への情報流出の可能性については完全に否定できるものではありませんが、現時点で流出の事実、あるいはそれら情報が不正利用された事実はいずれも確認されておりません。

#### 3. 原因

第三者によるAWSアクセスキーの不正利用とみられておりますが、その窃取経路、方法については特定することができませんでした。

#### 4. 再発防止策

- (1) サービス提供環境を含む当社ITインフラに対するアクセス状況常時監視体制の強化
- (2) 定期不定期でのITセキュリティの見直しおよび対策の実施
- (3) セキュリティ調査を含むセキュリティ確保のための各種情報の継続的入手およびセキュリティ強化
- (4) 全社員及びパートナー企業に対するセキュリティや情報漏洩に関する教育の強化
- (5) CSIRT設立、第三者機関との協力による組織、体制面でのセキュリティ強化

今後において情報の流出や不正利用等が確認された場合には個別にご連絡させていただきます。

また、今回のセキュリティ調査の結果を受けて、インシデントにつながる可能性のある脆弱性については即時見直しおよび対策を実施しております。インシデントの発生の可能性は極めて低い状態となっており、この状態を維持、向上させていくべく、体制の強化、対策の推進に努めてまいります。

この度は、多大なるご迷惑ご心配をおかけしましたことを心よりお詫び申し上げます。

今後同様の事象が発生しないようセキュリティ品質の向上と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。

引き続き「iField」をご愛顧いただきますよう、何卒よろしくお願い申し上げます。

以上