平成 28 年 11 月 4 日

各　位

株式会社新生銀行
新生インベストメント&ファイナンス株式会社

新生銀行グループの新生インベストメント&ファイナンスにおける パソコン端末のウイルス感染による情報漏えいの可能性に関するお知らせとお詫び

株式会社新生銀行（東京都中央区、代表取締役社長　工藤　英之、以下、「新生銀行」）のグループ会社である新生インベストメント&ファイナンス株式会社（東京都千代田区、代表取締役社長　谷屋　政尚、以下、「SIF」）において、社員のパソコン端末が不正なプログラム（マルウェア）に感染し、SIF の子会社である特別目的会社、有限会社ワイエムエス・ナイン（以下、「YMS9」）が保有する債権の債務者の方の法人・個人情報が外部に漏えいしている可能性があることが判明いたしました。

本件に関して、現時点で判明している概要および対応について、以下の通りお知らせいたします。

お客さまをはじめ関係者の皆さまに多大なるご心配、ご迷惑をおかけする事態に至り、ここに深くお詫び申し上げます。新生銀行および SIF としては、今般の事態を重く受け止め、新生銀行グループにおける情報セキュリティの更なる強化に取り組み、再発防止に努めてまいります。

1. 概要および経緯

(1) 新生銀行と SIF の関係

SIF は新生銀行の 100%子会社である新生プリンシパルインベストメンツ株式会社が 100%出資する子会社であり、投融資業務を行っています。

新生銀行は、SIF を含む一部のグループ会社に対しても新生銀行のネットワークインフラを提供し、サイバーセキュリティの監視、運用管理を行っています。

(2) 経緯

平成 28 年 10 月 25 日（火）に SIF 社員 1 名のパソコン端末が「なりすましメール」により外部サイトから疑わしいファイル（マルウェア）をダウンロードしたことを新生銀行のサイバーセキュリティシステムが検知したことから、同日、当該パソコン端末をネットワークから隔離し、セキュリティ対策ソフトによるスキャンを実施し、ネットワークに戻しました。

その後、同年 10 月 27 日（木）に当該パソコン端末がインターネットの特定の外部サイトにデータを送信していることを新生銀行のサイバーセキュリティシステムが検知したことから、同日、当該パソコン端末をネットワークから再度隔離し、確認したところ、10 月 25 日（火）から 10 月 27 日（木）までの間、当該パソコン端末のブラウザのスクリーンショットが定期的に外部の不正なサイトに自動送信されていたことが判明しました。

同年 10 月 27 日（木）から感染したパソコン端末を調査した結果、不正なサイトへの自動送信があった 10 月 25 日（火）から 10 月 27 日（木）の間、当該パソコン端末からアクセスした二つの社内システムで取り扱っていた、YMS9 が保有する債権の債務者の情報 35 件、債権譲渡契約の情報 1 件、郵便等配達証明書の情報 2 件が外部に漏えい

している可能性があることが判明しました。また、今般感染したマルウェアは未知のマルウェアであったことから、10 月 25 日（火）の段階では、セキュリティ対策ソフトでは検出できなかったことも判明しました。

新生銀行では、SIF からの報告を受けて、監督官庁に本事象の内容を報告いたしました。なお、これまでに漏えいした可能性のある情報の不正使用などの事実は確認されておりません。また、新生銀行が管理する同行およびグループ会社のネットワークにおいて、今回発覚した外部の不正なサイトへの、他のパソコン端末によるアクセスは検知されておりません。

2. 漏えいの可能性がある情報

(1) 債務者の情報 35 件

SIF は YMS9 から同社が保有する債権に関する事務を受託しています。YMS9 が保有する 35 件の債権について、債務者の商号または氏名、債権の状況、返済の実績、回収の予定となります。なお、35 件のうち、27 件は個人の方の情報となります。

(2) 債権譲渡契約の情報 1 件

YMS9 と法人のお客さまの債権譲渡契約 1 通について、契約した法人の商号、住所、代表者名、債権の連帯保証人 1 名（個人）の氏名となります。

(3) 郵便等配達証明書の情報 2 件

YMS9 が発送した郵便等の配達証明書に記載された法人の商号と代表者の氏名となります。

3. 対象となるお客さまへの対応

SIF では、情報が漏えいした可能性のある法人・個人のお客さまについて、平成 28 年 11 月 2 日より、状況のご説明とお詫びのご連絡を順次行っております。流出した情報を悪用され、被害を受けられた場合には、SIF までご連絡いただくようお願いしています。SIF では、今後もお客さまには誠意ある対応を行ってまいります。

4. 再発防止策

新生銀行と SIF では、今般の事態の重要性に鑑み、新生銀行および同行がネットワークを管理するグループ会社も含めた情報セキュリティの強化策として、ファットクライアント型端末のシンクライアント型端末への移行の促進、セキュリティ対策と運用方法の見直しと強化、社員教育の更なる充実などに取り組み、再発防止に努めてまいります。

以　上