

弊社お客さま情報の漏えいについて

この度は、お客さまに多大なご迷惑、ご心配をおかけしておりますこと、心より深くお詫び申し上げます。

以下に、よくあるご質問と回答を掲載いたしますので、ご確認くださいませようお願いいたします。

1. 情報漏えいの詳細に関するご質問		
①	漏えいの経緯を教えてください	(株)イセトーにおいて、外部からの不正アクセスによるサイバー攻撃を受け、一部サーバーや PC のファイルが暗号化されるランサムウェア被害が発生しました。 その後の調査の結果、弊社のお客さまに関する情報が漏えいしたことが確認されました。
②	どういった情報が漏えいしたのか	お客さま管理番号(店番、お客様番号等)、口座番号、氏名、住所が漏えいしましたが、お客さまによって漏えいした情報は異なります。 お手数をおかけいたしますが、詳細は弊社からご郵送しておりますお知らせをご覧ください。
③	電話番号や e-mail アドレスは漏えいしていないのか	電話番号や e-mail アドレスは漏えいしていません。
④	キャッシュカードの暗証番号や、インターネットバンキングのパスワード等は漏えいしていないか	キャッシュカードの暗証番号や、インターネットバンキングのパスワード等は漏えいしていません。
⑤	(株)イセトーとはどのような会社か	弊社からお客さまへお送りする各種発送物や、社内で使用する帳票類の印刷や発送を委託している会社です。
2. お客さまへのご連絡に関するご質問		
①	案内までに時間がかかったのはなぜか	データがサイバー攻撃によって暗号化されていたことから、専門家を交えて確認・分析を行ったため、詳細な状況や対象となるお客さまの特定に時間を要しました。 ご案内が遅くなり申し訳ございません。
②	すでに取引が終了しているのに案内が届いたのはなぜか	本件は重要なお知らせのため、すでにお取引を終了されたお客さまにもお送りしております。 何卒ご理解賜りますようお願いいたします。
③	同様のお知らせが複数届いたのはなぜか	複数の口座をお持ちのお客さまについては、お届けの氏名、住所、電話番号をもとに同一のお客さまであることを確認できた場合は、お知らせを1通におまとめしております。 一方、同一のお客さまであることが確認できなかった場合には、それぞれの口座についてのお知らせをご郵送しております。 何卒ご理解賜りますようお願いいたします。

④	家族のお知らせが、自分とは別の日に到着したのはなぜか	ご家族のみなさまにはなるべく近い日付で到着するようご郵送しておりますが、口座ごとのご案内となるため、ご家族のみなさまで到着日が異なる場合がございます。 何卒ご理解賜りますようお願いいたします。
3. お客さまへの影響に関するご質問		
①	不正払出のおそれはあるか	漏えいの対象となった、お客さま管理番号(店番、お客様番号等)、口座番号、氏名、住所だけでは、お取引内容の照会や、出金・振込みといったお手続きを行うことはできません。 また、本件に関してお客さま宛に口座番号やキャッシュカードの暗証番号をお聞きしたり、カードをお預かりしたりするようなことは一切ございません。 まことに恐れ入りますが、お客さまにおかれましては不審な問い合わせにご注意をいただき、万が一、そのような事態がございましたら、弊社お客さま相談窓口(0120-701-675 平日 9:00-17:00)か、お取引店までご連絡をお願いいたします。
②	個人情報が悪用された事実はあるか	現時点でお客さまの個人情報が悪用されたという事実は確認されておりません。 まことに恐れ入りますが、お客さまにおかれましては不審な問い合わせにご注意をいただき、万が一、そのような事態がございましたら、弊社お客さま相談窓口(0120-701-675 平日 9:00-17:00)か、お取引店までご連絡をお願いいたします。
③	私は、今後、どのようなことに注意すればよいのか	本件に関して、弊社が口座番号やキャッシュカードの暗証番号をお聞きしたり、カードをお預かりしたりするようなことは一切ございません。 まことに恐れ入りますが、お客さまにおかれましては不審な問い合わせにご注意をいただき、万が一、そのような事態がございましたら、弊社お客さま相談窓口(0120-701-675 平日 9:00-17:00)か、お取引店までご連絡をお願いいたします。
④	万が一、本件が原因と考えられる被害にあった場合はどうすれば良いか	まことに恐れ入りますが、お客さまにおかれましては不審な問い合わせにご注意をいただき、万が一、そのような事態がございましたら、弊社お客さま相談窓口(0120-701-675 平日 9:00-17:00)か、お取引店までご連絡をお願いいたします。
4. 再発防止に関するご質問		
①	(株)イセトーにおける再発防止策を教えてください	本件は、VPN(インターネット上に構築する仮想の専用回線)から、(株)イセトー社内のネットワークに侵入されました。 今後は、(株)イセトーにおいて本件の原因となったVPNを使用しない体制とすると共に、認証強化を図り不正アクセスが起らない環境

		<p>を構築いたします。なお、環境構築までの間は外部ネットワークとの接続を制限し業務対応を行います。</p> <p>また、本件は、(株)イセトーとしての業務効率化の観点から、一部の情報を、本来とは異なる取扱いをしていたことが、情報漏洩につながりました。</p> <p>具体的には、お客さま情報は、本来、インターネットに接続した環境では取扱わない運営としていたにもかかわらず、その運営が守られていなかったものです。</p> <p>今後、委託業務に関するデータについては、(株)イセトーにおいて、本来利用可能な環境以外へデータの移送ができない環境を構築し、業務上必要なデータについては、保管期限など取り扱いルールを明確に定め業務終了後にデータを確実に削除する運営とします。そして、これらのルールが遵守されるよう、同社において監査を徹底します。</p> <p>また、(株)イセトーにおいて、個人情報を含む情報セキュリティに関する教育とルール遵守に関する社員研修を行い、再発防止の徹底を行います。</p>
②	銀行(委託元)としての再発防止策を教えて欲しい	<p>弊社は(株)イセトーと抜本的な再発防止策につき協議し、お客さま情報の確実な安全確保をはじめとした施策を確認いたしました。</p> <p>(株)イセトーが再発防止策として策定した各施策については、弊社において委託元部署ならびに外部委託管理・サイバーセキュリティ専門部署により、終了ならびに定着状況をモニタリングいたします。</p> <p>また、弊社では従前より、外部委託先に対し半年毎にモニタリングを行い、あらかじめ取り決めた方法に従って委託業務を的確に遂行しているかを検証し、必要に応じて監督・指導を行う態勢を構築しておりますが、今回の事態を弊社が未然に発見、防止することが出来なかったことを踏まえ、モニタリングの実効性強化のため確認事項の拡充を行います。</p>