資　料　２

公 表 資 料

株式会社イセトーに対する個人情報の保護に関する法律に基づく行政上の対応について

令和７年●月●日
個人情報保護委員会

個人情報保護委員会（以下「当委員会」という。）は、令和７年●月●日、株式会社イセトー（以下「イセトー」という。）における個人情報等の取扱いについて、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）第 147 条の規定による指導を行った。

第１　事案の概要

イセトーは、金融機関や地方公共団体等の取引先（以下「本件委託元」という。）から委託を受けて、様々な通知書（以下「通知書」という。）の印刷・発送業務（以下「本件委託業務」という。）を実施している。イセトーは、本件委託業務に伴い、本件委託元から、個人データ及び保有個人情報の取扱いの委託を受けているところ、令和６年５月 26 日、イセトーのサーバが第三者から不正アクセスを受け、通知書の内容及び発送先に関する個人データの漏えい及び毀損（以下「本件漏えい等事態」という。）が発生した[1]（以下、漏えい及び毀損が発生した個人データのうち、本件委託元から委託を受けて取り扱っていた個人データを「本件個人データ」という。）。

第２　事実関係

１　本件漏えい等事態の概要

(1)　本件は、イセトーのサーバが第三者から不正アクセスを受け、個人データを含む電子ファイルがランサムウェアにより暗号化され、さらに、窃取された同ファイルがダークウェブ上に公開されたことにより、本件個人データについて漏えい及び毀損が生じた事案である。

(2)　本件個人データの項目は、主に通知書に記載される氏名及び住所である。ただし、送付物の種類により、その他固有の情報が含まれる。

例えば、金融機関の通知書には確定拠出年金やローン残高等の金額、地方公共団体の納税通知書には税額情報等が含まれる。また、健康保険組合のジェネリック差額通知書には、要配慮個人情報が含まれる。

(3)　本件個人データに係る本人数は、合計 3,076,477 人[2]（うち、民間事業者委託分 2,509,886 人、行政機関等委託分 566,561 人）である。このうち、要配慮個人情報

[1] イセトーの従業者に関する個人データも漏えい及び毀損が生じたが、漏えい等が生じた個人データの多くは、委託により取り扱っていた個人データである。
[2] このほか、イセトーの従業者に関する個人データ 441 人分について漏えい及び毀損が発生した。

が含まれる個人データに係る本人数は、13,150 人である。

本件漏えい等事態で影響を受けた本件委託元は 41 団体（民間事業者 32 団体、行政機関等９団体）であり、本件委託元に委託していた再委託元（２以上の段階にわたる委託を含む。）を含めると、影響を受けた団体数は約 100 団体である。

２　イセトーにおける個人データの保管状況

イセトーは通知書の印刷・発送業務を受託するに当たり、委託元から、専用線、ファイル転送サービス等を通じて個人データを受領している。

イセトーは、社内ネットワークを業務系ネットワークと基幹系ネットワークに分けて業務を行っているところ、イセトーによれば、同個人データは、業務系ネットワークでのみ保管し取り扱うルール（以下「保管ルール」という。）としていた。

ただし、保管ルールは、あくまでイセトー内でのルールであり、委託元とイセトーとの間で締結された契約書等には同ルールに関する記載はなかった。また、イセトーによれば、保管ルールは、社内で公知のルールであったとのことであるが、規程等に明文化されたものではなく、従業者は日々の業務の中でルールを理解していたとのことである。

３　不正アクセスの侵入経路及び本件漏えい等事態の発生原因

(1)　侵入経路

外部調査機関によるフォレンジック調査により、攻撃者は、VPN 機器を経由し、基幹系ネットワークへ不正に侵入したことが判明した（しかしながら、イセトーによれば、イセトーにおけるログ取得が十分ではなかった[3]ことから、同 VPN 機器の認証回避方法及び基幹系ネットワークへの侵入方法の詳細の確認には至っていないとのことである。）。

同調査によれば、攻撃者は、基幹系ネットワークへの侵入後、同ネットワークのファイルサーバ及び PC から本件個人データを暗号化し、窃取した。なお、業務系ネットワークへの侵入には成功していないことが確認されている。

(2)　本件漏えい等事態の発生原因

ア　侵入に関する問題点

前記(1)のとおり、イセトーは、VPN 機器のログを適切に取得していなかったため、フォレンジック調査によっても真因は分かっていない。しかしながら、VPN 機器のアップデートに問題があり、侵入当時、最新のパッチが適用されていなかった。具体的には、イセトーは、令和３年４月以降、アップデートを行っておらず、侵入当時、脆弱性について対応が未了であった。

また、イセトーのパスワード管理においては、業務系ネットワークについて

[3] イセトーによれば、ログの取得の設定が適切ではなく、必要なログを取得できていなかったとのことである。

は、①英文字、記号、数字の３種混合、②８桁以上、③30 日で更新するパスワードポリシーを規定していた。他方、今回不正アクセスを受けた基幹系ネットワークについては、３種混合や８桁以上というような制限はなく、45 日でパスワード更新を行うということのみが規定されていた。

くわえて、本件で不正利用された管理者アカウントについては、基幹系ネットワークのものであるところ、平成 29 年２月から同じパスワードを使用していた。また、利用していたパスワードは推測がある程度容易な英小文字のみの 11 桁であり、十分な強度ではなかった。

以上から、本件における攻撃者の侵入については、不十分な脆弱性管理及びパスワード管理が原因となった可能性が高い。

イ　個人データの保管場所に関する問題点

前記２のとおり、イセトーでは保管ルールが存在した。そのため、本件個人データについては、業務系ネットワークでのみ保管し、基幹系ネットワークでは本件個人データを取り扱わないこととなっていた。

しかしながら、イセトーの全 56 部署のうち３部署においては、部署内において、本来アクセス権限がない従業者と業務データを共有する目的や、通知書発送の有無等の業務管理を行う目的で、保管ルールを遵守せず、本件個人データを基幹系ネットワーク上のサーバへコピーの上、業務を行っていた。

かかる状況の下、攻撃者が基幹系ネットワークへ不正アクセスを成功させたため、本来は基幹系ネットワークに存在しないはずの本件個人データが、ランサムウェアにより暗号化され、かつ窃取され、ダークウェブ上に公開されて漏えいする事態に至った[4]。

４　二次被害の発生状況

イセトーによれば、令和６年６月 18 日 11 時から 22 時 30 分の間、本件個人データがダークウェブ上へ公開されていた[5]。

イセトーでは本件委託元へ本件漏えい等事態に関する説明を行うとともに、本件個人データの悪用等による二次被害に関する情報提供を呼びかけているところ、現時点において、そのような情報提供は受けていない。

第３　個人情報保護法上の問題点

個人情報保護法第 23 条において、「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適

[4] なお、イセトーによれば、業務系ネットワークで保管ルールどおりに保管されていた個人データ（すなわち、本件漏えい等事態の対象ではない個人データ）については、全て本件委託元との契約におけるデータ廃棄規定等に従い、適切に削除が行われていたとのことである。

[5] 同期間以降は、ダークウェブ上の公開サイトへのアクセスはできず、ファイルのダウンロードは不可となっている。

切な措置を講じなければならない。」とされている。しかし、イセトーにおける個人データの取扱いに関し、以下の問題点が認められた。

(1) 外部からの不正アクセス等の防止（技術的安全管理措置）

個人情報の保護に関する法律についてのガイドライン（通則編）（以下「ガイドライン」という。）10-6(3)において、「個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。」と規定している。

しかしながら、前記第２の３(2)アのとおり、イセトーは、令和３年４月以降、VPN 機器のアップデートを実施しておらず、VPN 機器の認証に関連する脆弱性について対応が未了であった。その上、イセトーにおいては、基幹系ネットワークに関する管理者アカウントについて平成 29 年２月から同じパスワードを使用していた。そして、実際のパスワードは推測がある程度容易な英小文字のみの 11 桁であった。なお、イセトーは多要素認証を導入していなかった。

以上から、イセトーにおいては、VPN 機器を最新の状態にしなかったことによってブルートフォース攻撃に関する脆弱性等が残存し、かつ、管理者アカウントのパスワードの強度が十分ではなかったといえ、個人データを取り扱う情報システムを外部からの不正アクセスから保護する仕組みを導入し、適切に運用するという点で不備が認められる。

(2) 組織体制の整備（組織的安全管理措置）

ガイドライン 10-3(1)において、個人情報取扱事業者は、「安全管理措置を講ずるための組織体制を整備しなければならない。」と規定している。

この点、イセトーにおいては、保管ルールという重要な業務ルールについて明文化がされておらず、実際に一部の部署において保管ルールが守られていなかった。また、VPN 機器については、約３年もの間アップデートがなされておらず、パスワードポリシーについても、基幹系ネットワークについては桁数や文字についての制限がなく、更新日数についての規定は存在したものの遵守されておらず、約７年もの間、管理者アカウントのパスワード更新が行われていない状態であった。

このような不備については、イセトーにおいて、経営層を含む管理者が適切に状況を把握できていなかったこと、また、個人データの取扱いに関する責任分担や役割の明確化が不十分であったことに起因するものと考えられ、安全管理措置を講ずるための組織体制の整備に問題があったものと認められる。

(3) 個人データの取扱いに係る規律に従った運用（組織的安全管理措置）

ガイドライン 10-3(2)において、個人情報取扱事業者は、「あらかじめ整備された個人データの取扱いに係る規律に従って個人データを取り扱わなければならない。」と規定している。

この点、イセトーにおいては、印刷・発送業務に係る個人データは業務系ネットワークでのみ取り扱う旨の保管ルールとなっていたものの、実態は３部署において同ルールが遵守されておらず、業務系ネットワークから本件個人データをコピーし、基幹系ネットワーク上のサーバに保存を行っていた。今回不正アクセスを受けた領域は、基幹系ネットワークにとどまっており、仮に保管ルールが守られていた場合、本件個人データについて漏えい等は発生していなかったであろうという点を考慮すると、本件個人データの保管場所について規律に沿った運用が実施されていなかった問題は大きいといえる。

また、ログ取得が不十分であった点については、定期的な設定確認、取得状況の把握等を行っておらず、個人データの取扱いの検証が可能な状態ではなかった。

(4)　取扱状況の把握及び安全管理措置の見直し（組織的安全管理措置）

ガイドライン 10-3(5)において、個人情報取扱事業者は、「個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない。」と規定している。

イセトーにおいては、個人データの取扱状況について、定期的な監査や点検が十分に実施できていなかった。そのため、長期間にわたり[6]３部署が保管ルールを遵守せず、基幹系ネットワーク上のサーバに本件個人データを保管するという不適切な取扱いを発見及び是正することができなかった。これは、イセトーにおいて、個人データの取扱状況を把握するための体制が整備されていなかったことに起因しており、その結果、本件漏えい等事態の影響が拡大したものといえる。

(5)　従業者の教育（人的安全管理措置）

ガイドライン 10-4 において、個人情報取扱事業者は「従業者に、個人データの適正な取扱いを周知徹底するとともに適切な教育を行わなければならない。」とされている。

イセトーは、従業者に対して、定期的に、一般的な情報セキュリティ等に関する研修を行っていたが、保管ルールを明文化することなく、日常業務における暗黙のルールとして、委託元からの個人データ等の取扱いを行っていた。そのため、保管ルールは従業者が常時確認できる状態ではなく、同ルールを周知しているといえる状態ではなかった。

このように、従業者に対する個人データの適正な取扱いの教育及び周知徹底が不十分であったことが、保管ルールを認知しながらも基幹系ネットワークへ本件個人データを移していた部署、また、目の前の業務遂行や効率化を重視し、リスク回避策が不明瞭なまま本件個人データを取り扱っていた部署が生じた一因となったものと考えられる。

---

[6] イセトーによれば、本件個人データについては、令和元年頃から保管ルールを逸脱した取扱いがなされていたものと認められるとのことである。

(6)　小括

以上のとおり、イセトーにおいては、技術的安全管理措置、組織的安全管理措置及び人的安全管理措置に不備が認められる。

第４　当委員会の対応について

１　イセトーに対しては、以下の点について、個人情報保護法第 147 条の規定による指導を行う。

(1)　前記第３の問題点を踏まえ、法第 23 条及びガイドラインに基づき、必要かつ適切な措置を講ずること。

(2)　既に進めている再発防止策を確実に実施するとともに、爾後、適切に運用し（必要に応じて見直すことを含む。）、継続的にその取り扱う個人データの漏えい等の防止その他の個人データの安全管理のために必要かつ適切な措置を講ずること。

２　本件は、攻撃者により実際に情報が窃取され、漏えいが生じた個人データに係る本人数が多く、再委託元等複数にわたる委託元を含めた場合、影響を受けた団体数も多い。また、委託元は地方公共団体も多く、税関係情報等について多くの住民の保有個人情報の取扱いの委託を行っていたケースも複数見受けられ、行政機関等における個人情報の取扱いについての国民に対する透明性や信頼性の確保の観点を考慮すべきである。さらに、漏えいが生じた個人データの項目には、氏名及び住所に加えて、例えば、確定拠出年金に関する金額、ローン残高、納税額等、個人の財産に関する情報等、漏えい等をした場合に、本人の権利利益の侵害が更に拡大する可能性がある個人データが含まれる。このような事情等を考慮し、本件については、本資料のとおり公表する。

以　上