個人情報保護・コンプライアンス向上対策

検討委員会報告書

令和５年９月

東京水道株式会社

目次

＜資料＞

はじめに

当社では会社設立以来、個人情報保護の取組やコンプライアンスの徹底について、様々な機会を捉えながら鋭意取組を実施してきたところですが、今年６月３０日、当社社員が、東京都水道局から貸与されているシステム端末（水道契約に関するお客さま情報を管理するシステムの専用端末。以下「システム端末」という。）からお客さまの個人情報を第三者に不正に提供していた疑いで書類送検されるという事案が発生しました。

本事案によりお客さま及び関係者の皆様に多大なご心配とご迷惑をお掛けしましたことを深くお詫び申し上げます。

現在、検察庁による捜査が続いている状況ではありますが、当社ではこのことを大変重く受け止め、事案の原因及び問題点を分析し、改善に向けた取組を早急に進めていかなければいけないと考えています。

このため、本事案公表後速やかに、個人情報保護の取組強化及びコンプライアンスの一層の徹底を図るため、社内に「個人情報保護・コンプライアンス向上対策検討委員会」（以下「検討委員会」という。）を設置しました。

検討委員会では、複数の外部専門家にも加わっていただき、これまで当社が実施してきた社員教育等の取組を検証するとともに、新たな対策について議論を重ねてきました。

この度、「社員に対する教育・研修」、「システム技術」、「情報漏えい対策」の３つの観点から、個人情報保護の取組強化及びコンプライアンスの一層の徹底に向けた対策を取りまとめました。

今後、速やかに本報告書でとりまとめた対策を実施するとともに、継続的に個人情報保護及びコンプライアンスの向上に向けた取組の見直し・改善を図ることで、当社の信頼回復に取り組んでまいります。

東京水道株式会社
代表取締役社長　野田　数

1　本事案の概要及び対応経過

（1）本事案の概要

当社社員（50代・主任、以下「事故者」という。）は、事業者に水道メータの払い出しなどを行う業務に従事しており、当該業務において、お客さまの住所や氏名等を照会する必要があるため、水道局から貸与されているシステム端末の操作権限を付与されていました。

事故者は、一度は断ったものの、令和３年８月頃から令和４年９月頃にかけて、知人（探偵業を営む方）からの求めに応じ、システム端末を操作して19名分のお客さま情報（住所、氏名及び電話番号）を不正に入手し、報酬を得て当該知人に提供していました。

なお、現時点で、提供された個人情報が、犯罪に使用されたとの情報はありません。

（2）本事案の対応経過

令和５年２月１日（水）
・警視庁からの情報提供により、当社社員が令和３年８月頃から令和４年９月頃にかけ、知人からの求めに応じて、水道局から貸与されているシステム端末を操作してお客さま情報（住所、氏名及び電話番号）を不正に入手し、報酬を得て当該知人に提供していた疑いがあることを把握 ・本事案を速やかに水道局へ報告 ・警視庁から厳重な情報管理を要請されたため、可能な限りでの調査・対応を開始
令和５年２月９日（木）
・事故者の人事異動を行い、お客さま情報を取り扱わない業務に変更
令和５年２月１１日（土）～１８日（土）
・事故者が使用していたシステム端末のログを調査するも、不正使用していた期間のログについては保存期間が過ぎていたため確認不能
令和５年３月３日（金）
・システム端末の利用者や利用目的をこれまで以上に把握できるように、システム端末操作カード（共用）の使用簿を改定
令和５年３月２１日（火）～３月２５日（土）
・不正利用に対する抑止力を高めるために、社内で利用しているシステム端末（共用）全１３８台のうち、上司の目が届きにくい場所に設置されている８台を、上司の席の隣若しくは上司の席から目視できる場所に移設
令和５年６月８日（木）～
・システム端末操作カードを共用としている部署については、共用から個人貸与に順次変更

令和５年６月３０日（金）
・警視庁から事故者を廃止前の東京都個人情報の保護に関する条例違反の疑いで書類送検したとの連絡を受け、当日開催を予定していた当社株主総会及び取締役会で報告 ・緊急の社内幹部会議を開催し、社長から社員の綱紀保持について指示 ・当社及び委託元である水道局との連名で本事案を報道発表（資料１） ・社内グループウエアのトップページにコンプライアンス強化の取組と綱紀保持に係る社長メッセージ(資料２)を掲載し、全社員へ周知徹底
令和５年６月３０日（金）～７月１０日（月）
・事故者が所属する部門（以下「当該部門」という。）の全事務所長を報道発表と同時に緊急招集し、本事案の説明を行うとともに、個人情報保護の取組強化及びコンプライアンスの一層の徹底について指示 ・当該部門の全事務所社員を対象に、個人情報の取扱い状況等について管理職が社員一人ひとりにヒアリングを実施し、第三者の個人情報を業務目的外で閲覧するなどの不適正利用がないことを確認
令和５年７月４日（火）～７月６日（木）
・当該部門においてコンプライアンス特別研修及び職場討議を実施
令和５年７月６日（木）
・個人情報保護委員会へ事故報告書（速報）を提出
令和５年７月１３日（木）
・個人情報保護・コンプライアンス向上対策検討委員会を設置（資料３）

（３）問合せへの対応

６月３０日の報道発表にあわせて社内に問合せ窓口を設置
８月末までの問合せ件数の合計は１７件、問合せ内容は下表のとおり
（内訳）
・お客さま　　２件（同一の方）
・メディア　　４件
・取引先　　１１件

【問合せ件数】

期間	件数
６月３０日（金）～　２日（日）	３
７月　３日（月）～　９日（日）	１０
７月１０日（月）～１６日（日）	１
７月１７日（月）～２３日（日）	２
７月２４日（月）～３１日（月）	１
８月　１日（火）～３１日（木）	０
合　計	１７

【問合せ内容】

内容	件数
問合せ（事件の概要等）	9
ご意見（会社への不信感）	2
その他（取引先への影響等）	6
合　計	１７

（４）被害者への対応

個人情報を不正提供されたお客さま全員に説明及び謝罪を実施

（５）事故者の処分及び損害賠償

事故者については、就業規則に基づき、懲戒処分審査委員会で処分案を決定し、臨時取締役会の決定を経て７月１９日付けで懲戒処分（懲戒解雇）

また、本事案により生じた損害がある場合には、事故者に請求予定

２ 本事案の原因分析及び課題の抽出

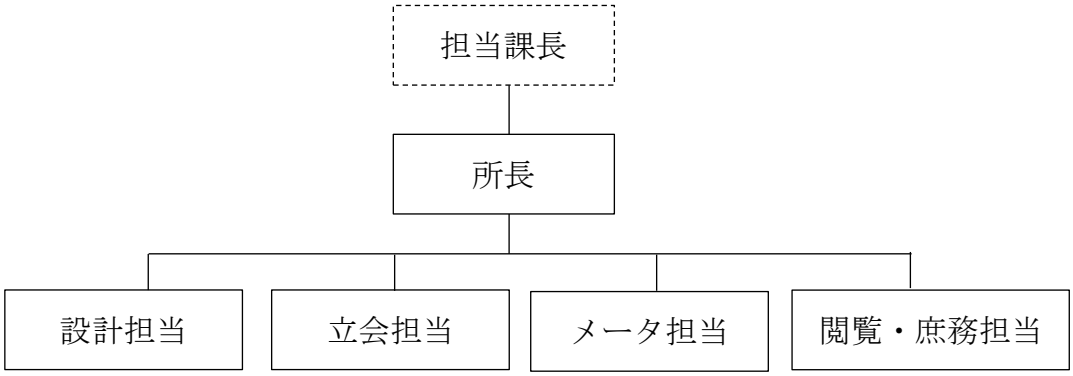
（１）当該職場の体制及び管理状況

本事案発生当時、事故者が勤務していた職場の体制は以下のとおりです。

事故者は、令和３年度は事業者に水道メータの払い出し等をするメータ担当、令和４年度は配置替により事業者が施行する給水装置の設置申請に係る審査をする設計担当として業務に従事していました。

各担当は、主任級以下の社員等から構成されており、主任である事故者の上司は所長（課長代理級）でした。所長の上司である担当課長については、複数の事務所を統括している関係もあり、特定の事務所に常駐することはなく、日常の業務管理等は所長が実施する役割を担っています。

所長は、事務所社員に対して、日常的な声掛け、注意喚起等を行っていましたが、当該社員の様子に不自然なところは無く、特に相談等を持ち掛けられたこともありませんでした。所長は、事務所内を随時巡回するなど、所内の状況把握に努めており、その際、システム端末の使用状況についても確認をしていましたが、事故者が業務を装いながら行った不正な端末操作までは気付くことができませんでした。



令和３年度	４名	３名	２名	２名
令和４年度	４名	３名	３名	３名

＊下線の箇所が、事故者が当時所属していた担当

（２）本事案の原因究明

不正行為が発覚した場合、事故者が不正を実施するに至った動機、機会、正当化の不正のトライアングルを解明し、その対応策を検討することが求められます。このため、本事案においては、組織的側面及び個人的側面から本事案を検証し、動機、機会、正当化について分析しました。

【組織的側面】

○事故者が勤務していた職場には、担当課長が配置されていましたが、担当課長は複数の事務所を統括的に管理する役割のため、日常的な業務管理等は所長が担うこととなっていました。

○所長は、社の情報セキュリティに関する規程に基づき、個人情報を持ち出す場合は情報セキュリティ管理者の承認を得る必要があるという指導を、職場の朝会や全体会議などで継続的に行っていました。
○一方、事故者は、日常的にシステム端末を業務で使用しており、今回の事案に際しても業務を装いながら勤務時間中に個人情報を検索し、その内容をメモ等に写して持ち帰っていたため、所長を含め周囲の社員は不正行為に気づくことができませんでした。
○当該業務で使用するシステム端末については、契約仕様書や委託者である水道局からの指導・引継、社内規定に従い利用されていましたが、所長の目が届きにくい場所に設置されていたこと、操作カードが共用であったことから、今回のような事案に対する抑止力を働かせることはできませんでした。

【個人的側面】
○事故者は、勤務態度や周囲との人間関係も良好で、金銭トラブルを抱えていたとの情報もなく、加えて、知人からの情報提供の依頼に対して、個人情報の不正提供は違法であるという認識を持っており、一度は依頼を断っていました。
○しかし、事故者は自身が依頼した人探しの案件に対する知人の対応に感謝の念を抱き、知人の役に立てればという思いに駆られ、また、他の企業の社員からも個人情報の提供を受けているとの知人からの言葉を安易に信用し、加えて金銭面での報酬も期待されたことから、悪いことと認識はしていたが不正に入手した個人情報を知人に提供し、報酬も受け取りました。
○事故者からは、自分の弱さが原因であったという言葉も聴取しており、本事案は、事故者の悪意ある行為が要因で、個人的な側面が大きいものでした。

不正のトライアングルにもとづく要因分析

要 因	内　容	対 応 策
動　機	・人探しのお礼 ・報酬で人探しの費用回収を期待	意識啓発 ⇒社員教育・研修
機　会	・システム端末を日常業務で利用 ・所長の目が届きにくい場所に端末が設置され不正利用に対する抑止効果が働きにくい状況 ・システム端末操作カードが共用のため、利用者の特定が困難	環境改善 ⇒システム技術
正当化	・「他企業の社員も情報提供してくれている」との知人の言葉に同調	リスクの明確化・周知 ⇒情報漏えい対策

（3）要因分析を踏まえた具体的取組の方向性

ア　社員に対する教育・研修

① 教育・研修

当社では、個人情報保護、コンプライアンス及び情報セキュリティに関する研修を定期的に実施（資料４）しており、研修内容も適宜見直しを図るなど、内容の充実に努めています。

② 事故者の研修受講状況

事故者が直近３年間に受講した個人情報保護等に関する研修は、以下のとおりです。事故者は、所定の研修を毎回受講し、研修受講後のアンケートには、常日頃からコンプライアンスを意識して行動することや、より良い環境作りが大切であると記述しており、個人情報保護、コンプライアンス、情報セキュリティに対する認識を持っていたことが確認できます。

事故者が受講していた研修一覧

区分	研修名	時期
個人情報保護	定例研修	令和３年１月
		令和４年２月
		令和５年１月
コンプライアンス	定例研修	令和３年１月
		令和４年２月
		令和５年１月
	汚職非行防止職場研修	令和３年２月
		令和４年１月
		令和５年１月
	ハラスメント防止職場研修	令和３年２月
		令和４年１月
		令和５年１月
	接遇研修	令和３年５月
	コンプライアンス推進月間における職場討議 題材：ハラスメント事例、ルールを守る職場づくり、交通事故防止への取組等	令和２年６月
		令和２年１２月
		令和３年６月
		令和４年６月
		令和４年１２月
	車両事故に係る職場討議	令和３年９月
		令和４年７月
	心理的安全性の職場研修	令和５年１月
情報セキュリティ	定例研修	令和３年１月
		令和４年２月
		令和５年１月
	文書誤送付に係る職場討議	令和３年８月
	コンプライアンス推進月間 における職場討議 題材：記録媒体の紛失	令和３年１２月

③ 具体的取組の検討（社員教育・研修）

○コンプライアンスに関するこれまでの社の取組として、当社は会社設立当初からコンプライアンス推進委員会を設置し、毎年度策定する年間行動計画（資料５）に基づき各種取組を実施することで、社員に東京水道グループの一員としての自覚と責任を持たせるなど、高い職業的倫理観の醸成に取り組んでいます。

○また、各職場で日頃から非行防止の意識付けを図ることに加え、年２回（６月及び１２月）、社で定める個人情報保護等に関する要綱等の理解促進及び社会規範の遵守を目的として、コンプライアンス推進月間を設定しています。

○コンプライアンス推進月間では、全社にコンプライアンスに関するポスターを掲示し啓蒙するほか、社員による自己点検（テスト）、管理職による職場点検、具体的テーマを設定しての職場討議を実施しています。

○一方で、社員の認識に目を向けると、令和３年度から毎年実施している社員への意識調査や直近の令和５年６月に実施した自己点検（テスト）において、個人情報保護に関する項目について、多くの社員が正しく認識していました。

○しかし、今回の事案では、知人からの教唆により、禁止事項と認識しながら不正行為を実行しています。

○研修により、知識が増し、理解が深まることは重要ですが、そのことだけでは不正行為を防止することはできなかったため、抑止効果がより高まるように研修内容を見直すなど、この点に関して改善の余地があると考えられます。

○「不正行為は発覚する」、「不正行為が発覚すれば、事故者は特定される」、「不正行為からは、得るものより失うものの方が大きい」といったことを社員に改めて浸透させることも重要です。

○さらに、デジタル社会の進展に伴い、個人情報保護への社会的要請が強くなっていることから、個人情報を取り扱う職場においては、専門的知識に裏付けられた社員の配置も個人情報の適切な管理及び社員の意識啓発に有効です。

イ システム技術

① システム端末の概要

○水道局から当社に貸与されているシステム端末は、お客さまとの契約内容や検針、料金等の情報をオンライン化し、お客さまからの届出や問合せに即時に対応できるシステムで、専用の通信回線網を用いるなど情報セキュリティ対策が施されています。

② システム端末の利用状況

○事故者の職場では、メータ情報（所在地、契約者、メータ位置等）を確認する際にシステム端末を使用しています。今回、事案が発生した職場では、所長の目が届きにくい場所にシステム端末が設置され不正に対する抑止効果が働きにくい状況でした。

○このため警視庁から本事案の情報提供が行われた後速やかに、社内におけるシステム端末の設置状況を改めて確認し、上司（所長）の目が届きにくい場所にシステム端末が設置されている場合には、所長の席の横に移設するなどの対応をしました（資料６）。
○また、システム端末の操作には専用カードとパスワードが必要で、権限を付与されている社員のみが操作できます。当社では、システム端末は主に受付や料金などを扱う事務部門で利用しており、事務部門ではシステム端末操作カードは、原則、個人貸与となっています。しかし、事故者の職場は技術部門で、システム端末を利用する社員数や頻度、利用できる情報が事務部門と比べて少なかったこともあり、システム端末操作カードが共用となっていました。
○システム端末操作カード（共用）の使用記録は専用の使用簿で管理していましたが、システム上のログも含め、使用した社員を確実に特定できる仕組みにはなっていませんでした。
○このため、システム端末の使用者や使用目的をより確実に特定できるように、本事案の判明後速やかに使用簿を見直すとともに、水道局へシステム端末操作カード（共用）の原則廃止を要望し、現在、システム端末操作カードを共用から個人貸与に順次変更しています。
○さらに、システム端末を取り扱う場合には、業務内容に応じてきめ細かく情報へのアクセス制限を設けるとともに、利用者や不正アクセスを特定できる仕組みが有効です。このため、改めてアクセス制限の内容を検証し、システム面での更なる改善を図ることで、個人情報の漏えい対策を万全なものにしていくことが重要です。

当社におけるシステム端末の設置状況（令和５年８月末時点）

拠　点	台　数	利用人数
給水管工事事務所(２１か所)	２１(　２１)	１２４
営業所等(１１か所)	３７８(　４８)	３０８
サービスステーション等 (１３か所)	３３７(　５５)	４１５
管路管理事務所(８か所)	８(　８)	２３２
管路整備部小管設計課	１(　１)	６２
多摩技術部設計課	１(　１)	５２
量水器事務所	１(　１)	２
南阿佐ヶ谷事務所	１(　１)	２
お客さまセンター	５２７(　２)	５４７
合　計	１，２７５(１３８)	１，７４４

※台数のカッコ内は共用端末の数を内数で表記
※利用人数には、人材派遣会社等の社員を含む

③　具体的取組の検討（システム技術）

○システム端末の使用者が特定できるよう、システム端末操作カード（共用）を原則廃止とし、共用から個人貸与に順次変更を進めていますが、早期に対応が完了できるよう取組を進めることが必要です。

○また、従来の操作ログの保存期間では、今回の不正行為を確認できなかったことからログの保存期間の見直しをすることが必要です。

○事件が起きてからログを調査するだけでなく、不正行為の早期発見のために定期的なログの点検が必要です。操作ログの点検については、継続的に実施するとともに、常時監視していることを社員に意識させることが、不正行為の抑止策として必要です。

○さらに、業務内容に応じて設定しているシステム端末の閲覧可能情報の参照地域をこれまで以上に限定することで、不正なアクセスを抑止できるため、併せて検討が必要です。

○加えて、システム端末を上司の目が届く場所に移動させ、不正閲覧等の防止を図るほか、職場内に監視カメラを設置することで抑止効果を更に高める取組も有効です。

ウ 情報漏えい対策

①　ISMS等の取組

○当社は令和２年４月に旧東京水道サービス株式会社と旧株式会社PUCが統合して発足しました。ISMS（情報セキュリティマネジメントシステムに対する第三者適合性評価制度）は、統合前から適用していた旧株式会社PUCの業務には引き続き適用していますが全社共通の取扱いとはなっていません。

○現在、旧東京水道サービス株式会社を前身とする技術系部門では、水道局の情報セキュリティ基準に準拠した規定に基づき各種取組を行っていますが、ISMS適用職場に実施している審査機関による審査など、外部の第三者的視点からのチェック機能はありません。

○また、当社は、リスク対策としてリスク管理行動計画を導入しています。そこでは業務執行部署が、業務におけるリスクを洗い出し、対策を講じます。洗い出したリスクの中で、経営に大きな影響を及ぼすリスクについては、リスク管理委員会で取り上げて確認します。

○今回、当該部門は個人情報の不正利用をリスク管理の対象としていませんでした。過去に不正利用が発生していなくても、業務上システム端末操作の機会があるため、不正利用による情報漏洩をリスクと認識してリスク管理行動計画書でのリスクの評価が必要でした。

②　情報セキュリティに関する規程等

○当社では、個人情報保護や情報セキュリティに関する規程等を整備し、社員に対して遵守することを定めています。

○また、就業規則では、遵守事項として業務上知りえた企業情報、顧客情報、個人情報等を他に漏らさず、また、職場から持出し、又は職務以外に使用しないことを定めています。

○上記規定に違反した場合、懲戒処分に処すること及び被処分者に損害を賠償させることができると規定しています。

③　具体的取組の検討（情報漏えい対策）

○旧東京水道サービス株式会社を前身とする技術系部門についても、ISMS適用職場とし、会社として統一的な対策を取ることが必要です。

○各部署は、リスク管理委員会がリスク管理行動計画の中で「経営上の主要なリスク」として挙げている個人情報の不正利用のリスク評価を早急に実施し、本社管理部門（リスク管理委員会や取締役会）に諮ることが必要です。

○また、今回の事案と直接の関係はありませんが、不正行為を起こす背景に、私生活のトラブルが原因となるケースがあります。私生活のトラブルは不正行為に至らなくとも業務遂行に影響を及ぼす恐れもあります。上司には相談しづらい、社員個人のトラブルに対応する相談窓口等があることで、社員個人のトラブルに起因する事件・事故のリスク軽減を図ることが期待できます。

3 個人情報保護及びコンプライアンスの強化に向けた更なる対策

本事案の原因分析等を踏まえ、既に実施済の対策以外で速やかに実施すべき対策を「社員に対する教育・研修」、「システム技術」、「情報漏えい対策」の３つの観点で整理して以下のように取り組んでいきます。（資料７）

なお、当社は水道局からシステム端末の貸与を受けて業務を履行しているため、システム改善については既に局へ改善要望を行い、現在、局と協力して取組を進めております。

（１）社員に対する教育・研修の充実・強化

ア　コンプライアンス遵守の再徹底

○今回の事案を受けて、全社員に対してコンプライアンス遵守の徹底を図るため、本事案を題材とした臨時の研修を速やかに実施することで、受講者の印象に強く残り、定例の研修以上に抑止効果が向上します。

○また、既存の研修やコンプライアンス推進の取組に、今回の報告書の内容を反映するとともに、新たなリスクが顕在化した場合には見直しを図っていきます。

○さらに、こうした研修等だけでなく、毎日の朝会などの場も活用しながら、今回の報告書の内容を社員一人ひとりに浸透させていきます。

イ　教唆対策研修

○闇バイト等の個人を対象とした悪意ある接触が増加するなか、社員個人を守り、不正行為を予防するため、甘言等に惑わされないように教唆対策を目的とした研修を実施します。事例等を研究することで、教唆を見抜き被害を未然に防ぎます。

ウ　専門人材の育成

○個人情報を取り扱う部署には、個人情報を適切に管理・活用できるよう、個人情報保護士の資格取得を奨励し、個人情報を取り扱う社員全体へのさらなる意識啓発につなげます。

（２）システム技術による対策の強化

ア　システム端末操作カード（共用）の原則廃止

○水道局から貸与を受けているシステム端末操作カードについて、システム端末操作カード（共用）の原則廃止を要望し、水道局が個人カードへの切り替えを順次実施しています。

イ　システム端末操作ログの保存期間の延長

○システムを介しての不正行為の調査では、操作等のログが重要な情報となりますが、今回、事件が発生してから一定の期間が経過しており、事件当時のログが存在していませんでした。同様の事案に備え、遡っての調査が可能なように保存期間の延長を水道局へ提案しました。

ウ　システム端末操作ログのチェック

○事件が起きてからログを調査するのではなく、不正行為等の早期発見のために定期的に不正利用に対するチェックを行う機能を設けることが望まれます。完全に不正を検出することは困難ですが、常時、監視していること

を社員に周知することで不正行為の抑止機能として効果があるため、操作ログのチェック機能についても水道局へ提案しました。

エ　システム端末参照画面の制限

○情報セキュリティにおいて、アクセス可能な情報を最小範囲に留めることが望まれます。業務遂行等との兼ね合いでバランスの取れたユーザー毎のアクセス権の付与または、情報のマスキング等の実施を水道局へ提案しました。

上記対策のほか、職場内に監視カメラを設置することで不正閲覧等の抑止効果を更に高める取組も検討しましたが、現在、当社と同様に水道局からシステム端末の貸与を受けている他の団体にも影響が生じるため、今回、速やかに実施すべき対策の対象とはせず、中長期的な課題として取り組んでまいります。

（３）情報漏えい対策の充実・強化

ア　ISMSの全社適用

○国際規格に基づくISMSの全社適用のためには、仕組みの構築や継続的な改善に加え、毎年の外部審査や内部監査等の取組が必要になりますが、取り扱う情報を安全に管理する仕組みに対して客観的な評価が得られます。

○行政から委託されている情報を取り扱う企業として、より高い情報セキュリティを確保するため、現在、対象外としている業務を含めて早期のISMS全社適用を促進します。

イ　リスク管理行動計画の見直し

○今回の事案を受け、各部署は自部門のリスク管理行動計画書の中で、個人情報の不正利用に関するリスクを、経営上大きな影響を及ぼすリスクとして評価し、業務の特性に応じた対策を講じます。

ウ　外部相談機関の導入

○個人的なトラブルに限らず、育児・介護等仕事を続けるうえで現代社会において社員が抱える悩みは多種多様です。その全てを上司に相談し解決することは困難です。

○このため、社員個別の悩みについて外部専門家に相談できる仕組みを構築し、社員が安心して仕事に専念できる環境を整備します。

専　門　家　意　見

情報漏えい対策・社員教育専門家

影島 広泰　氏（弁護士　牛島総合法律事務所）
中井 杏　氏　（弁護士　牛島総合法律事務所）

1. 個人情報保護法に基づく安全管理措置及びその水準について

個人情報保護法第23条は、「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切な措置を講じなければならない。」と定めており、本事案に対する対応は、これを満たしている必要があります。

安全管理措置は、「個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならない」とされております（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、「通則ガイドライン」といいます。）3-4-2）。

ここでいう「事業の規模及び性質」に関しては、電力会社グループにおける個人情報の取扱いが問題となった事案において、個人情報保護委員会が「国民の生活の基盤として不可欠な社会インフラ」の「公共的性質に鑑みると、各事業者においては、その取り扱う個人データに関し、高い水準での従業者の監督を含めた安全管理措置の整備が必須」であるとしていることに注目する必要があります（個人情報保護委員会「一般送配電事業者及び関係小売電気事業者による新電力顧客情報の不適切な取扱い事案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」（2023年6月29日））。東京水道株式会社（以下「東京水道」といいます。）は、都民の生活に不可欠な水道事業という社会インフラを提供しており、また、取り扱う個人データは、東京都と給水契約を締結した世帯に関する情報であり、非常に多量の個人データを取り扱っています。

したがって、東京水道は、まさに高い水準での安全管理措置の整備が求められる事業者であるといえます。

また、行政機関等から個人情報の取扱いの委託を受けた者は、当該委託を受けた業務について、行政機関等と同様の安全管理措置義務を負うこととされており（個人情報保護法第66条第1項及び第2項第1号、個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）（以下「事務対応ガイド」といいます。）80頁）、行政機関等が「4-8（別添）行政機関等の保有する個人情報の適切な管理のための措置に関する指針」に基づいて負うべき安全管理措置を実施するよう要求されている地位にあります（事務対応ガイド75頁）。

2. 本報告書における「個人情報保護及びコンプライアンスの強化に向けた更なる対策」

東京水道は、プライバシーマーク付与事業者であることも踏まえると、個人情報保護法及びJIS Q 15001:2017において、安全管理措置として求められている“項目”は、全て実施されていたものと認識しています。

したがって、本事案における問題は、上記のとおり安全管理措置として求められている項目が実施されていたにもかかわらず、漏えいが発生したという点にあることになります。東京水道としては、本事案が発生した原因に関し、「高い水準での安全管理措置の整備」が行われているといえるよう、安全管理措置の“手法”について更なる対応の強化が必要となるということを意味します。

そこで、本項では、本報告書において今後実施することとされている対応が、通則ガイドラインで示されている安全管理措置の“手法”の例示や、事務対応ガイドの「（別添）行政機関等の保有する個人情報の適切な管理のための措置に関する指針」に照らし、合理的なものであるかを検討します。

他方で、通則ガイドラインに記載された安全管理措置の手法は、あくまでも例示に過ぎないため、そのいずれを採用するか、あるいは例示されていない他の手法を採用すべきかなど、採るべき手法を検討する必要があります。

この点、東京地判平成26年1月23日判時2221号71頁（SQLインジェクション事件）は、個人情報を取り扱うシステムの発注を受けた事業者について、「その当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示的に合意されていたと認められる」、「個人情報の漏洩を防ぐために必要なセキュリティ対策を施したプログラムを提供すべき債務を負っていたと解すべき」であると判示しています。上記裁判例は、システム開発委託契約における債務について述べるものではありますが、講ずべきセキュリティ対策が契約書に具体的に記載されていないケースにおいて、委託を受けた者が講ずべきセキュリティの水準とは何かを考えるにあたり参考になると思料されます。

また、東京地判平成31年1月25日判時2436号68頁（暗号資産流出事件）でも、当時の業界における一般的なセキュリティ対策として何が採用されていたかを認定し、それを基準として債務不履行に当たるかが判断されています。

したがって、東京水道においても、東京都から受託した業務の遂行に当たっては、「その当時の技術水準に沿ったセキュリティ対策」を講ずることが求められているということができます。

そこで、本報告書で示された対応が、現時点で公表されているセキュリティ等に関するガイドラインを踏まえ、現時点の技術水準に沿ったセキュリティ対策といえるかについて検討します。

(1) 社員に対する教育・研修の充実・強化

本報告書では、「本事案を題材とした臨時の研修を速やかに実施すること」、「既存の研修やコンプライアンス推進活動の内容に、今回の報告書の内容を反映するとともに、新たなリスクが顕在化した場合には見直しを図る」とされております（14頁）。

通則ガイドライン10-4「人的安全管理措置」の手法の例示として「個人データの取扱いに関する留意事項について、従業者に定期的な研修等を行う。」ことが挙げられており、上記対応は合理的な対応策であると考えられます。

また、経済産業省「秘密情報の保護ハンドブック」（2022年5月）（以下「秘密情報保護ハンドブック」といいます。）では、「『秘密情報に対する認識向上（不正行為者の言い逃れの排除）』に資する対策」として、「秘密情報の取扱い方法等に関するルールの周知」が挙げられており、社内の規程等について、継続的に研修等を実施することが重要であることや、社内で起こった秘密情報の漏えいとその結果に関する事例といった具体的事例を取り上げながら説明することも効果的と指摘されています（61頁）。

さらに、「秘密情報の管理に関する従業員等の意識向上」のための方法としても、「情報漏えいの事例の周知」や、「情報漏えい事案に対する社内処分の周知」が挙げられています（68頁）。

独立行政法人情報処理推進機構（IPA）「組織における内部不正防止ガイドライン 第5版（2022年4月改訂）」（以下「内部不正防止ガイドライン」といいま

す。）においても、「教育による内部不正対策の周知徹底」が指摘されており、「①全ての役職員に教育を実施し、組織の内部不正対策に関する方針及び重要情報の取り扱い等の手順を周知徹底させなければならない。②教育は繰り返して実施することが望ましい。また、教育内容を定期的に見直して更新し、更新内容を内部者に周知徹底させなければならない。」とされています（72頁）。

そこで、定期的な研修とその内容の見直し、情報漏えい事案やその社内処分の周知は、内部不正を防止するために重要な対策だと考えられます。

したがって、本報告書の対応は、現時点の技術水準に沿ったセキュリティ対策といえ「高い水準での安全管理措置の整備」に資するものであると考えられます。

(2) システム技術による対策の強化

ア．システム端末操作カード（共用）の原則廃止

本報告書では、システム端末操作カードを共用から個人カードに切り替えることを水道局に要望しているとされております（14頁）。

通則ガイドライン10-6「技術的安全管理措置」では、「アクセス者の識別と認証」のための手法の例示として、ユーザーID、パスワードを利用した従業者の識別・認証手法が挙げられており、上記対応は合理的な対応策であると考えられます。

また、秘密情報保護ハンドブックでは、秘密情報への「『接近の制御』に資する対策」として、「情報システムにおけるアクセス権者のID登録」が挙げられており、「ID・パスワードは複数の従業員間で同じものを使い回さないことが重要」（39頁）、「個別ＩＤ付与を行わないままに共通パスワードのみで管理する場合、万一情報漏えいが発生した場合に追跡が困難になるケースがあることに注意」（42頁）と指摘されております。

内部不正防止ガイドラインでは、「情報システムでは、利用者…及びシステム管理者…の識別において、共有ID及び共有のパスワード・ICカード等を使用せず、個々の利用者ID又はシステム管理者IDを個別のパスワード・ICカード等で認証しなければならない。」と指摘されております（44頁）。

そこで、個別のID、パスワードを利用することは、内部不正を防止するために重要な対策だと考えられます。

したがって、本報告書のとおり、システム端末操作カードを個人カードに切り替えることができれば、現時点の技術水準に沿ったセキュリティ対策を行っているといえ「高い水準での安全管理措置の整備」に資するものであると考えられます。

イ．システム端末操作ログの保存期間の延長及びシステム端末操作ログのチェック

本報告書では、システム端末操作ログの保存期間の延長と、システム端末操作ログのチェック機能について水道局に提案しており、常時、監視していることを社員に周知するとされております（14～15頁）。

通則ガイドライン10-3は、「組織的安全管理措置」の手法の例示として、担当者の情報システムのログを通じて個人データの取扱いの検証を可能とすることが挙げられております。また、通則ガイドライン10-6は、技術的安全管理措置として、外部からの不正アクセス等の防止の手法ではあるものの、ログ等の定期的な分析により、不正アクセスを検知することを挙げております。

上記によればログの取得は、ログを検証することで、個人データの取扱い状況の把握や、不正の検知にあるところ、その目的を達することができるような保存

期間になるよう延長することは合理的な対応策であると考えられます。ログの定期的な分析は、外部からの不正アクセスに対しても、内部不正に対しても同様に有効であると考えられ、合理的な対応策であると考えられます。

また、秘密情報保護ハンドブックでは「事後的に検知されやすい状況を作り出す対策」として、「PCやネットワーク等において、誰が（利用者IDの記録）、どの端末から、いつ、どの秘密情報にアクセスされたか（アクセス履歴）、どのような操作をしたか…といったログを取得し、保存します。加えて、ログを記録・保存していることについては事前に社内に周知」することが指摘されております（59頁）。

内部不正防止ガイドラインでは、「内部不正の早期発見」及び「内部不正の影響範囲を特定するために、事象の具体的状況を把握するとともに、被害の最小化策や影響の拡大防止策を実施」するために、「重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を記録し、定めた期間に安全に保存することが望ましい」（68、89頁）と指摘されております。また、「ログ・証跡の保存を行っている事実を従業員に通知することは、内部不正の発生を抑止する上で効果的な方法と考えられるため、一般的には、通知することが望まれます」とされております（69頁）。

そこで、ログを取得し、事後的な検証のために適切な期間保存することや、ログの保存を行っていることを従業員に通知することは、内部不正を防止するために重要な対策であると考えられます。

したがって、本報告書のとおり、ログの保存期間を延長し、ログを取得していることを社員に周知することにより、現時点の技術水準に沿ったセキュリティ対策を行っているといえ「高い水準での安全管理措置の整備」に資するものであると考えられます。

ウ．システム端末参照画面の制限

本報告書では、業務遂行等との兼ね合いでバランスの取れたユーザー毎のアクセス権の付与または、情報のマスキング等の実施を水道局へ提案するとされております（15頁）。

通則ガイドライン10-6は、「技術的安全管理措置」の「アクセス制御」の手法の例示として、「ユーザーIDに付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる従業者を限定する」ことを挙げております。

また、事務対応ガイド4-8-5では、「アクセス制限」として「保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する職員の範囲と権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限る」こととされております。

したがって、システム端末から閲覧することができる情報を制限することは、合理的な対応策であると考えられます。

また、秘密情報保護ハンドブックでは、「『接近の制御』に資する対策」として、「ルールに基づく適切なアクセス権の付与・管理」が推奨され、「アクセス権の範囲については、その秘密情報を知る必要がない者にまでアクセス権を付与してしまうと、情報漏えいリスクを不必要に高めてしまうこととなるため、当該秘密情報の内容・性質等を踏まえて、『知るべきものだけが知っている（need to know）』の原則に基づいて、その秘密情報へのアクセス権限を付与する者を必要最小限にすることが重要」と指摘されております（38頁）。

内部不正防止ガイドラインにおいては、重要情報を区分し、区分に応じて取り扱い可能な役職員の範囲を定め、それにより「限定された利用者のみが重要情報にアクセスできるように、利用者ID及びアクセス権の登録・変更・削除等の設定について手順を定めて運用しなければならない」と指摘されております（40頁）。

そこで、個人情報へのアクセス権限を付与する者を必要最小限にすることは、内部不正を防止するために重要な対策であると考えらえます。

したがって、本報告書のとおり、システム端末から閲覧することができる情報を制限することにより、現時点の技術水準に沿ったセキュリティ対策を行っているといえ「高い水準での安全管理措置の整備」に資するものであると考えられます。

(3) 情報漏えい対策の充実・強化

ア. ISMSの全社適用

本報告書では、現在対象外としている業務も含めて、ISMSの全社適用を促進するとされております（15頁）。

通則ガイドライン10-2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等の防止その他の個人データの安全管理のために、個人データの具体的な取扱いに係る規律を整備しなければならない」とされており、10-3では「組織的安全管理措置」として、個人データの取扱いに係る規律に従った運用等を行わなければならないとされております。

個人データの取扱いに係る規律としてJIS Q 27001を採用しこれを全社的に統一することは、当該規律に従った運用を行うために有益なことであるため、合理的な対応策であると考えられます。

また、秘密情報保護ハンドブックでは、「決定された対策を実効的に講じていくためには、その内容を社内でルール化することが必要」とされており、「従業員等が、…秘密として保持すべき情報、その取扱い方法について理解できる内容としておくことが重要」と示されております（25頁）。

また、取引先の管理能力の事前確認にあたり、ISMSなどの基準・認証・資格などを参考とすると指摘されております（82頁）。

そこで、個人データの取扱いに係る規律を統一することは、社内でルールを作成し、それを従業員等が理解できる内容とすることができることから、内部不正を防止するために重要な対策であると考えられます。またその基準をISMSとすることは、現時点の技術水準に沿ったセキュリティ対策であるといえます。

したがって、「高い水準での安全管理措置の整備」に資するものであると考えられます。

なお、特に、東京水道は、2020年4月に東京水道サービス株式会社と株式会社PUCが統合して発足した会社であるところ、個人データの取扱いに関する規律を統一化し、一律の体制、運用を整備することは重要であると考えられます。

イ. リスク管理行動計画の見直し

本報告書では、リスク管理行動計画書の中で、個人情報の不正利用に関するリスクを、経営上大きな影響を及ぼすリスクとして評価し、業務の特性に応じた対策を講じることとされております（15頁）。

この点は、個人情報保護法に基づく安全管理措置を行うための前提となるものであり、安全管理措置自体として求められる手法の例示には含まれておりません。

しかし、経済産業省、独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドラインVer3.0」（2023年3月）12頁において、「経営者が認識すべき3

原則」の一つとして、「経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要」であると挙げられ、「サイバーセキュリティリスクを多様な経営リスク…の中での一つとして位置づけ、…経営者自らがリーダーシップを発揮して自社の組織や事業におけるリスクを把握した上で、それに応じた対策の推進を主導することが必要」であると指摘されております。

また、独立行政法人情報処理推進機構「『企業の内部不正防止体制に関する実態調査』報告書」（2023年4月）によれば、回答企業のうち39.6%が内部不正リスクは「事業リスクが高く優先度の高い経営課題として認識」しているとされております。

したがって、個人情報保護法に基づく「高い水準での安全管理措置の整備」を行う前提として、個人情報の不正利用に関するリスクを、経営上大きな影響を及ぼすリスクとして評価することは、重要であると考えられます。

ウ. 外部相談機関の導入

本報告書では、社員個別の悩みについて外部専門家に相談できる仕組みを構築するとされております（15頁）。

この点は、個人情報保護法に基づく安全管理措置として求められる例示には含まれておりませんが、内部不正防止ガイドラインにおいては、「適正な労働環境及びコミュニケーションの推進」として、「職場外の相談窓口から適切な上位の上司にフィードバックし、状況を改善するような環境を整備することが望まれます」と指摘されております（87頁）。

したがって、外部相談機関を導入することは、現時点での水準に沿ったセキュリティ対策の一つとして合理的なものであると考えられます。

3. 今後の対応について

以上のとおり、本報告書における「個人情報保護及びコンプライアンスの強化に向けた更なる対策」は、現時点の技術水準に沿ったセキュリティ対策として適切なものが挙げられており、「高い水準での安全管理措置の整備」に向けた適切な対応であると考えられます。

しかし、通則ガイドラインは、組織的安全管理措置における「取扱状況の把握及び安全管理措置の見直し」において、「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。」と義務づけており、安全管理措置は継続的な評価、見直し及び改善に取り組む必要があります。個人情報保護法における安全管理措置は「リスクに応じて、必要かつ適切な内容としなければならない」とされているところ、リスクは時の経過とともに変わっていくものである以上、見直しをしなければならないのは当然のことといえます。また、東京地判平成26年1月23日判時2221号71頁（SQLインジェクション事件）も、「その当時の技術水準に沿ったセキュリティ対策」が必要であると指摘しているところであり、今後も社会情勢や技術の進歩に応じて、セキュリティ対策の見直しを継続することが重要であると思料いたします。

以上

システム技術専門家

丸山 満彦氏（公認会計士・公認情報システム監査人 PwCコンサルティング合同会社）

１　本事案に対する会社の対応について

個人データが漏えいした場合の対応については、「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）」（令和4年9月一部改正）（以下、「通則ガイドライン」といいます。）の「3-5 個人データの漏えい等の報告等（法第26条関係）」に記載があります。今回の事案においては、この記載内容に準拠して対応がなされていたという認識をしています。

また、本事案の原因分析等を踏まえ、すでに実施済みの対策（資料７）以外で速やかに実施すべき対策として、「社員に対する教育・研修」、「システム技術」、「情報漏えい対策」の３つの観点で整理し、東京都水道局と協力して取り組んでいますが、その内容についても本事案を受けて適切な進め方だと思料いたします。具体的な対策の良し悪しについては、組織の内外の状況、情報システムの状況、物的な施設の状況、職員等の状況に依存するため、最適解が何かを決めることは難しいものの、組織が経営者を責任者に、外部専門家を含めて「個人情報保護・コンプライアンス向上対策検討委員会」（以下、「本委員会」といいます。）を立ち上げ、議論を重ねたということもあり、組織にとって適切な対策となっていると思料いたします。

さらに本事案を受けて、利害関係者に対して本事案の概要及び対応経過、本事案の原因分析及び課題の抽出、個人情報保護及びコンプライアンスの強化に向けた更なる対策を公表することについては、利害関係者へのリスクコミュニケーションの一環として適切であると判断します。

２　今後に対する会社への期待について

(1)　情報セキュリティ対策は総合的な視点で対策を実施することが重要

個人情報保護法における安全管理措置については、通則ガイドラインの「（別添）講ずべき安全管理措置の内容」において「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」、「技術的安全管理措置」という章立てで規定されています。その全てを考慮して、対策をすることが重要であるが、本質的に重要なことは具体的な脅威シナリオ（例えば、外部の攻撃者がインターネットを通じて内部のネットワークに侵入し、サーバ等の管理者権限を奪取し、個人データを外部に転送する。内部者が他人のID・パスワードを盗み見等により入手し、他人になりすまして個人データにアクセスし、他に漏えいする。）を踏まえてリスク管理の一環として対策をすることです。

最低限必要とされている「通則ガイドライン」以外の事項についても、様々な脅威シナリオを踏まえて対策をすることがリスク管理上は重要となります。

また、組織は個人データ保護のためだけに情報セキュリティ対策をするわけではありません。組織がとるべき情報セキュリティ対策についてのガイダンスは、国際機関、各国のセキュリティ機関、民間団体等から数多く公表されています※。これらのガイドラインも参考にしつつ、脅威シナリオを踏まえてどのような脅威、リスクに対して優先的に対応するべきかを組織的に検討し、場合によっては、主要な取引先である東京都水道局とも連携をとりつつ、コスト、実現可能性も踏まえた総合的な視点で対策をすることが重要となります。

(2) 不断の見直しと改善を継続することが重要

昨今、サイバー犯罪（金銭取得が目的）や国家を背景としたサイバー攻撃（情報収取、知財情報摂取、重要インフラの機能停止等を目的としていると想定されます。）が増加をしていると言われています。

脅威シナリオが現実に起こる可能性は、情報技術の変化、国際情勢の変化等により、変わってきます。例えば、米国の国土安全保障省の配下にあるサイバーセキュリティ・インフラセキュリティ庁（以下、「CISA」と言います。）では、事業者等に対して、脅威情報（攻撃者、攻撃手法等）、脆弱性情報（ソフトウェアの問題等）、サイバー対策についての情報を公開（https://www.cisa.gov/news-events/cybersecurity-advisories）しています。脅威情報については、ほぼ毎週１件のペースで公表されています。また、脆弱性情報は全世界で情報を集約していますが、今年は全世界で約4万件に達する推定（CVEデータベース：https://www.cve.org/Downloadsを2023.08.22に閲覧）されます。

このように状況において、現在とられている情報セキュリティ対策が適切なものか、将来にわたっても適切であり続けられそうかということは、非常に重要なこととなってきます。

そのため、組織内外の状況、及びその変化、今後の予想等を踏まえ、情報セキュリティ対策を、定期的に、事案が発生した場合に、新たな状況変化が発生したという情報を入手した場合に、見直し、改善していくことは、非常に重要となります。このような対応ができるように組織を整えていくことが、重要といえるでしょう。

※例えば、次のようなものがよく使われています。

- 経済産業省 - サイバーセキュリティ経営ガイドラインと支援ツール (https://www.meti.go.jp/policy/netsecurity/mng_guide.html)
- 国際標準 - ISO/IEC 27002:2022：Information security, cybersecurity and privacy protection - Information security controls (https://www.iso.org/standard/75652.html)
- 米国政府 - 米国国立標準技術研究所（NIST）- Cybersecurity Framework (https://www.nist.gov/cyberframework)

おわりに

都民の生活基盤として不可欠な社会インフラである水道事業に携わっている当社は、その公共的性質に鑑みると、個人情報の取扱いに関しては、一般の企業より高い水準での安全管理措置が求められます。

このため、業務の履行にあたっては、個人情報保護及びコンプライアンス向上に係る施策や教育を繰り返し実施し、事故の未然防止に努めてきたところではありますが、この度、社員が個人情報を第三者に不正提供するという事案が発生したことは誠に遺憾であり、大変重く受け止めております。

今回、本報告書で取りまとめた対策を確実に実行することで、個人情報保護及びコンプライアンスの一層の徹底を図るとともに、職場環境や社員に対する処遇の更なる向上、人材育成をはじめとした人事制度の強化等に向けた取組を一層推進し、今後加速化される受託業務の拡大にしっかり対応できる盤石な組織体制を構築してまいります。

東京水道株式会社
代表取締役社長　野田　数

資　　料

資料１

令和５年６月３０日
水　　道　　局
東京水道株式会社

東京水道株式会社社員による個人情報の不正提供の疑いについて

水道局の業務委託先である東京水道株式会社（東京都政策連携団体）（以下「東京水道（株）」という。）の社員が、個人情報を第三者に不正に提供していた疑いで書類送検されたとの情報が、本日、警視庁からありました。

この間、警視庁からの要請により情報管理を行ってまいりましたが、上記の状況を踏まえ、本日発表することといたしました。お客さま及び関係者の皆様に多大なご心配をお掛けし、深くお詫び申し上げます。

今後、個人情報保護の取組強化及びコンプライアンスの一層の徹底に取り組んでまいります。

１　概要

東京水道（株）の社員が、令和３年８月頃から令和４年９月頃にかけ、知人からの求めに応じて、水道局から貸与されているシステム端末を操作してお客さま情報（十数名程度の住所、氏名及び電話番号）を不正に入手し、報酬を得て当該知人に提供していた疑いがあります。

なお、現時点で、提供された個人情報が犯罪に使われたとの情報はありません。

２　経緯

令和５年２月、警視庁からの情報により、東京水道（株）社員による不正提供の疑いがあることが判明。以降、警視庁の捜査に最大限協力するとともに当該社員からの聴取や緊急の取組などを実施。

本日、廃止前の東京都個人情報の保護に関する条例違反の疑いで、警視庁が在宅のまま本件を送検

３　対応

今後、詳細が明らかになり次第、事実関係に基づき、不正提供の対象となったお客さまに対して説明及び謝罪を行うとともに、当該社員に対して、厳正に対処してまいります。なお、当該社員は、事案の判明後速やかに、お客さま情報を取り扱わない部署に異動しています。

また、東京水道（株）において、この間、緊急の対応策を行ってまいりましたが、今後、個人情報の適正な取扱いについて社員へ改めて周知徹底を図るとともに、更なる個人情報保護の取組強化策を講じてまいります。さらに、水道局においても同社に対して改めて指導等を行い、東京水道グループとしてコンプライアンスの一層の徹底に取り組んでまいります。

【問い合わせ先】
（本件に関すること）
東京水道株式会社お客さまサービス本部
窓口サービス部
電話　03-3343-1985
（政策連携団体に関すること）
水道局総務部主計課
電話　03-5320-6324

資料２

令和５年６月 30 日
代表取締役社長
野田　数

所属長各位

綱紀の厳正な保持について（通知）

当社では、会社発足以来、綱紀粛正等に関する啓発について、機会を捉えて実施してきたところですが、今般、当社社員がお客さまの個人情報を第三者に不正に提供していた疑いが発生しました。

事実であれば、このような事態は当社のみならず、東京水道グループ全体に対するお客さまからの信頼を著しく損なうものとなります。

コンプライアンス意識の向上は、「令和５年度東京水道株式会社目標」にも掲げられた、重要な課題の一つであり、今後も、全社的な研修等、コンプライアンス強化の取組を推進していきますが、所属長各位におかれましては、社員のみなさんに対して、お客さまからの疑惑や不信を招くような行為は厳に慎むよう、改めて周知徹底するほか、適切な指導、監督に努めるなど、社員の綱紀保持に全力を尽くしてください。

以上

資料３

個人情報保護・コンプライアンス向上
対策検討委員会設置要綱

（設　置）

第１条　この要綱は「当社社員による個人情報不正提供の疑い」を受け、東京水道株式会社における個人情報保護の取組強化及びコンプライアンスの更なる徹底を図ることを目的に、個人情報保護・コンプライアンス向上対策検討委員会（以下「委員会」という。）を設置する。

（構　成）

第２条　委員会の委員（以下「委員」という。）及び各種専門家は、別表１に揚げる者で構成する。

２　委員会の委員長（以下「委員長」という。）は、代表取締役社長の職にある者をもって充てる。

３　副委員長は、個人情報保護管理者の職にある者をもって充てる。

４　各種専門家は、情報漏えい対策・システム技術・社員教育等の専門知識を有する者をもって充てる。

５　委員長は、必要があると認めるときは、委員及び各種専門家以外の者を委員会に出席させることができる。

６　委員会に特定の分野を所掌する部会を設置し、部会は検討、及び調整した案を委員会に報告する。

７　部会は、別表２に揚げる者で構成する。

８　部会の長は、お客さまサービス本部窓口サービス部給水装置課長の職にある者を、副会長は同部業務管理課長の職にあるもの者をもって充てる。

９　委員長が必要と認めるときは、委員会に委員及び各種専門家以外の者を出席させ、又は他の方法により意見を聞くことができる。

（所掌事項）

第３条　委員会は、次に揚げる事項について所掌する。

(1) 部会に対して、必要な指示をすること。

(2) 部会の進行を管理すること。

(3) 部会が報告した社内の現状分析及び改善に向けた具体案を協議・審議し、成案として取りまとめること。

(4) その他必要と認める事項に関すること。

２　部会は、次に揚げる事項について所掌する。

部会は、委員長から指示がある事項を検討し、原案を作成して委員会へ報告する。

（委員長の職務）

第４条　委員長は、委員会を招集し、会議を主催して議事を総理する。

２　委員長に事故があるとき又は委員長が欠けたときは、副委員長がその職務を代理する。

（部会長の職務）

第５条　部会長は、部会を招集し、会議を主催する。

資料３

２　部会長に事故があるとき又は部会長が欠けたときは、副会長がその職務を代理する。

（委員会及び部会の庶務）

第６条　委員会及び部会の庶務は、特命担当本部長及びお客さまサービス本部にて処理する。

（補　則）

第７条　この要綱に定めるもののほか、委員会の運営に必要な事項は、委員長が別に定める。

（附　則）

この要綱は、令和５年７月１３日から施行する。

資料３

別表1

委員長	代表取締役社長
副委員長	取締役副社長（個人情報保護管理者）
委　員	常勤取締役
	社外取締役*1
	監査室長
	管理本部長
	お客さまサービス本部長
	多摩お客さまサービス本部長
	水道技術本部長
	多摩水道技術本部長
	ソリューション推進本部長
	事業戦略部長
	総務部長
	人事部長
	窓口サービス部長（区部・多摩）
	東京都水道局経営改革推進担当部長
	東京都水道局経営改革推進担当課長
各種専門家*2	情報漏えい対策
	社員教育
	システム技術

＊１社外取締役・監査等委員：中島 美砂子（弁護士・公認会計士　中島法律事務所）
：中島 文明　（株式会社ジャノメ社外取締役）
：芳賀 良　（株式会社海外交通・都市開発事業支援 機構社外取締役）

＊２情報漏えい対策・社員教育：影島 広泰（弁護士　牛島総合法律事務所）
情報漏えい対策・社員教育：中井 杏　（弁護士　牛島総合法律事務所）
システム技術：丸山 満彦（公認会計士・公認情報システム監査人　PwCコンサルティング合同会社）

別表２

部会長	お客さまサービス本部窓口サービス部給水装置課長
副会長	お客さまサービス本部窓口サービス部業務管理課長
委　員	管理本部事業戦略部経営企画課長
	管理本部事業戦略部技術調整課長
	管理本部総務部リスク管理課長
	管理本部人事部人事課長
	お客さまサービス本部水道ITサービス部水道IT第二課長
	多摩お客さまサービス本部窓口サービス部業務管理課長
	多摩お客さまサービス本部窓口サービス部給水装置課長

資料４

個人情報保護等研修一覧

研修名等	対象社員	主な研修内容
○個人情報保護		
新任研修 ＜e-ラーニング＞	新規採用者	業務遂行に必要な個人情報保護の基本的知識の習得
定例研修 ＜e-ラーニング＞	全社員（毎年）	業務遂行に必要な個人情報保護の基本的知識のアップデート
○コンプライアンス		
新任研修 ＜e-ラーニング＞	新規採用者	コンプライアンスや汚職等非行防止に関する基本的知識の習得
定例研修 ＜e-ラーニング＞	全社員（毎年）	コンプライアンスや汚職等非 行防止に関する知識（事例）のアップデート
不当要求防止対策	管理職及び課長代理級社員並びに職務上 必要のある社員	暴力行為、不当要求への対応及び予防策
人権問題Ⅰ	課長代理級以下の社員	同和問題、ハラスメントその他の人権問題への理解・意識啓発
人権問題Ⅱ	管理監督職	同和問題、男女平等推進、セクシュアル・ハラスメントの防止その他の人権問題への理解・意識啓発
心理的安全性の確保	管理監督職	心理的安全性のある職場づくりの重要性、人間力を磨く、ハラスメントが起きない職場づくり
管理職研修 ＜e-ラーニング＞	管理監督職	コンプライアンス、ハラスメント防止、心理的安全性のある職場、労務管理、人事制度（評価）
○情報セキュリティ		
新任研修 ＜e-ラーニング＞	新規採用者	業務遂行に必要な情報セキュリティの基本的知識の習得
定例研修 ＜e-ラーニング＞	全社員（毎年）	業務遂行に必要な情報セキュリティの基本的知識のアップデート

資料５

コンプライアンス年間行動計画

年間取組方針	心理的安全性の確保を中心にした『職場環境の改善』及び『コンプライアンス違反を許容しない風土の維持、発展』を目指す

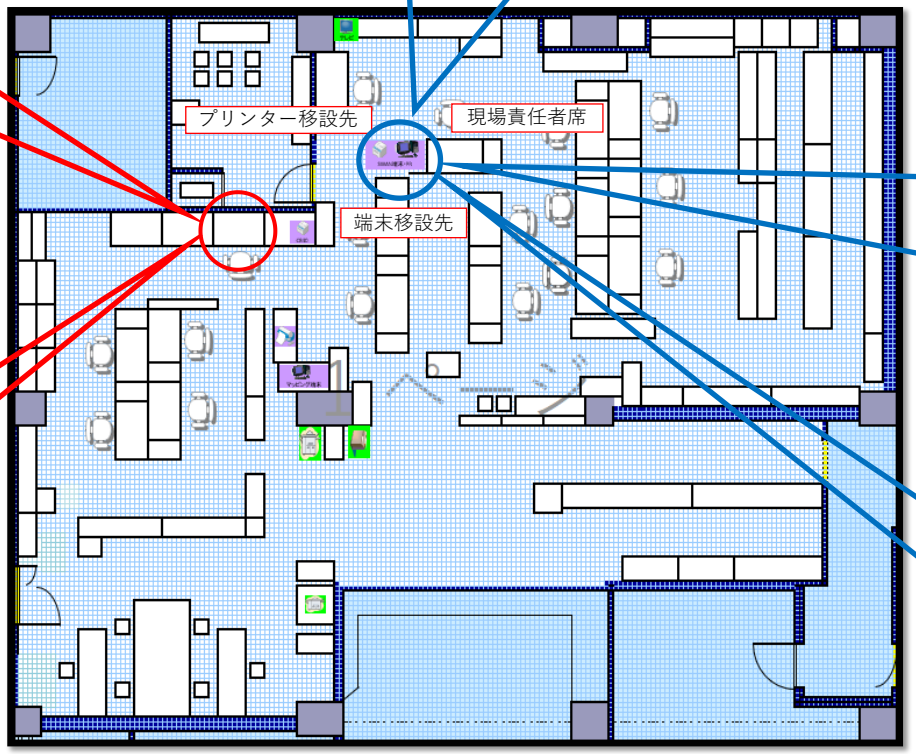
No	基準	取組の視点	行動の内容	令和5年度 Ⅰ	Ⅱ	Ⅲ	Ⅳ
1	高い規範意識、創造的かつ自律的な行動	お客さまからの信頼を得るため、一人ひとりが高い規範意識のもと行動する	●コンプライアンス推進期間を年2回設け、意識づけを図る	6/1～6/30 コンプラ推進期間 推進期間重点取組 ・非行等防止の意識付け ・情報の適正管理の徹底 ・心理的安全性のある職場　等		12/1～12/28 コンプラ推進期間 推進期間重点取組 ・非行等防止の意識付け ・情報の適正管理の徹底 ・心理的安全性のある職場　等	
			●コンプライアンス推進委員会を活用した非行事例等の情報共有・コンプライアンスの強化	○ コンプライアンス推進委員会	○ コンプライアンス推進委員会	○ コンプライアンス推進委員会	○ コンプライアンス推進委員会
			●コンプライアンス通信等によるコンプライアンス意識の啓発等で補完し、規範意識の徹底を図る ・ヘルプライン通報件数、対応完了件数等の社員へのフィードバック ・外部窓口を設置した内部通報窓口の普及 ・心理的安全性について	○ コンプライアンス通信発行	○ コンプライアンス通信発行	○ コンプライアンス通信発行	○ コンプライアンス通信発行
			●外部窓口を設置した内部通報窓口の運用	内部通報窓口の運用			
			●新規採用者（中途採用者含む）を対象として当社社員として遵守すべきコンプライアンス意識を醸成を図る	○ 新入社員研修 （コンプライアンス科目） （4月 上旬）		○ 管理職研修（職場研修講師育成） 定例研修（職場研修）	
			●全社員を対象としたコンプライアンス職場研修及び定例研修を通じて、一人ひとりが高い規範意識を身に付ける	コンプライアンス科目　eラーニング		コンプライアンス（事例編） 定例研修	
2		決められたことに従うだけではなく、お客さまサービス向上のために、率先して業務改善に取り組む	●職場におけるショートミーティングで法令順守の意識の徹底等を図る ・業務知識や業務情報の共有を図る	ショートミーティングの実施（毎日）			
			●社員のコンプライアンス意識・エンゲージメントを把握し、現状と課題を明らかにする			調査実施	
			●「心理的安全性」（他メンバーが自分の発言することに対して拒絶したり、罰を与えるようなことをしないという確信をもち、安全な場所であるとの信念がメンバー間に共有された状態）のある職場づくりの検討・実施（対象：管理職（外部講師）、全社員（定例研修（職場研修））による実施）			研修内容等の検討 全社員向け心理的安全性研修（定例研修） 管理職向け心理的安全性研修（外部講師）	
			●若手社員を中心とした業務報告会での発表や論文発表会を通じて、自発的な業務改善に取り組む環境づくり		若手発想PT ○ 若手発想PT説明会	論文募集 ○ 中間報告会	○ 論文発表会　○ 論文審査会 若手発想PT ○ 活動報告会
3	安全・安定的供給のための確実かつ効果的な事業運営	東京水道グループの経営方針のもと、着実な事業運営を行い、東京の水道事業を支えていく	●経営方針等の浸透（経営目標の策定・周知）	中期経営計画等の進捗状況管理 ○ 2023年度事業計画等を社内イントラネットにて公開 ○ 2023年度事業計画等を社内報に掲載（4月号） ○ 経営改革プラン改訂版を社内イントラネットにて公開 ○ 2022年度事業計画等を取締役会に報告 ○ 第一回全管理職会議にて事業計画の内容説明			
			●全管理職会議の開催 ・上司のマネジメント力を高めるための内容を強化 ・「危機意識を持った上司の模範的行動」の意義の浸透 ・上司自らが「コンプライアンスを実践する風土をつくる」意識の向上 ・心理的安全性のある職場環境づくりの意識付け		○ 全管理職会議	○ 全管理職会議	
			●社長等による事業所訪問 ・現場における危機意識への対応	社長を含む役員による事業所訪問の実施 ○ 訪問計画策定	○ 訪問開始 社長が社員と直接コミュニケーションを図ることで、相互の共通理解と、社員のモチベーションを向上させ、社の一体感を醸成する。		
			●社長による訓示の動画配信	第１回　社長による訓示の動画配信（4/3～）		第２回　社長による訓示の動画配信	
			●管理職・監督職の役割と経営・組織的視点を持った管理職・監督職の育成（研修実施等）	管理職・監督職のマネジメント研修の実施（R4未受講者・R5課長 適正な労務管理研修	マネジメント（管理職）	マネジメント（管理職）フォローアップ	
			●取締役会等による適切な経営判断	取締役会の毎月開催（１２回）			
			●東京水道グループとしての一体感の醸成	ともにプロジェクトの推進 ○「ともに、やってみよう」実施通知 ○水道週間イベント実施(6月) 第１回　グループ報の発行		○近代水道125周年記念・東京水道の日イベント実施 第２回　グループ報の発行	

資料５

No	基準	取組の視点	行動の内容	令和5年度 Ⅰ	Ⅱ	Ⅲ	Ⅳ
3	安全・安定的供給のための確実かつ効果的な事業運営	東京水道グループの経営方針のもと、着実な事業運営を行い、東京の水道事業を支えていく	●時間外労働の適正管理	時間外労働の把握による労務管理（超過勤務情報提供（毎月１回）、平準化の取組）	○集計・報告	○新就業システムでの超勤実績把握方法周知 ○集計・報告	○管理職昇格者への昇格時研修 ○集計・報告
				ノー超勤ウィーク（年２回）・ノー超勤ＤＡＹ（毎月１日）の実施			
			●管理職と社員の面談 （目標制度面接において課題の把握、人事考課の説明）	○面談時の聞き取り内容、留意点に関する周知	目標設定面談	目標成果中間面談	目標成果期末面談
			●人材育成方針に則した、プロパー社員を中心とした人材育成	人材育成方針に則した人材育成施策の推進（ＯＪＴ計画書等の運用）			
			●社内インターンシップ制度の運用	社内インターンシップ検討・実施			
			●チューター制度の運用	チューター制度の運用	○　コーチング研修		
4		法令等を遵守し、政策連携団体として、また株式会社として適正な業務執行を行う	●監査等委員会によるガバナンスの強化	監査等委員会の開催（原則月１回）			
				監査室連絡会議（原則月１回）			
			●業務執行部門から独立した監査室による、適正かつ実効性のある内部監査の実施	○監査結果報告			○監査結果報告 ○社内周知 ○随時監査 ○月次監査
			●契約監視委員会による入札結果の調査、分析、監視		対象案件の選定	○第１回契約監視委員会 調査の実施	○第２回契約監視委員会 資料作成
5		水道事業が都民生活に与える影響の大きさを認識し、危機管理を徹底する	●リスク管理委員会による会社を取り巻く様々なリスクの認識とリスク管理 ・リスク管理委員会でリスク所管各委員会を統括し全社的なリスクマネジメントを推進 ・部門ごとにリスク管理行動計画を整備運用し、リスク管理・対応行動の推進を図る 　また、適正に運用されているかについて監査等委員会による監視を行う	リスク管理行動計画の定期点検	○ リスク管理委員会	リスク管理行動計画の定期点検	○ リスク管理委員会
			●工事事故防止対策委員会 ・現場パトロールの実施や工事事故防止対策委員会の開催を通じて、当社社員と工事受注者の安全対策及び事故防止に関する知識を充実 ・四半期ごとに事故防止通信を発行し、当社社員と工事受注者の安全意識向上を図り、安全教育を支援 ・リスクマネジメント対応事例集に、レベルⅠ等の事故事例を追加して当社社員や工事受注者に情報を周知し、類似事故を抑制	工事事故防止対策委員会 ○幹事会（4月）　○本部委員会	○幹事会・委員会（6月）	○委員会（12月） ○本部委員会	○委員会（3月）
				安全対策の実施（○安全管理に関する実施計画策定　○中間報告）			
				安全管理に関する情報提供（○四半期ごとに事故防止通信を発行　○リスクマネジメント対応事例集に、レベルⅠ等事故の事例を追加）			
			●水道施設等の管理及び整備に関わる受託業務改善委員会 ・水道施設等の管理及び整備に関わる受託業務改善委員会の開催により、受託業務の適正かつ的確な遂行	水道施設等の管理及び整備に関わる受託業務改善委員会 ○本部委員会	○委員会・幹事会（6月）	○委員会（12月） ○本部委員会	
				受託業務の適正実施（○業務の適正実施に関する実施計画策定　○中間報告）			
				過去の再発防止策の継続実施（○再発防止策の再周知　○再発防止策の実施状況確認　○頻発事例における業務フローの点検）			
6	お客さまへの誠実・公正な対応	一人ひとりが東京水道グループの一員であるという意識を持ち、謙虚で誠実なお客さま対応を行う	●新入社員研修 接遇（電話・窓口・現場）の実施 （4月～5月予定） ビジネスマナー研修の実施 （6月予定） ●接遇研修 新人の2回目と中途採用者	○ 新入社員研修 （接遇・ビジネスマナー等含む） ・接遇（電話・窓口・現場） ・ビジネスマナー	新入社員研修フォローアップ 実施内容検討	○ 新入社員フォローアップ研修 ・ビジネスマナー	○ 接遇研修（新人2回目、中途採用者）
			●受注者との相談窓口運用により受注者からの相談等について誠実に対応	受注者相談窓口の運用			
				契約相談の継続監視			
7		政策連携団体の経営について都民の理解が得られるように、情報公開など見える化、透明化を推進する	●経営情報等の公表による会社情報の透明化		○R4年度決算 事業内容の公表	○第１四半期 決算の公表 ○非競争型受託等事業運営状況 人件費等報告	○第２四半期 決算の公表 ○第３四半期 決算の公表
			●透明性を確保するための発注方法等の継続 （入札参加者増の取組）	透明性を確保するための発注方法等の継続（入札参加者増の取組・入札審査委員会の開催(随時)）			
						来年度に向けた局受託業務等に関する入札審査委員会の開催　○	
				業者登録対応			
				電子入札システム対応（業者に対する電子入札システムへの登録推進）			

資料６

システム端末の移設事例



資料７

個人情報保護等対策一覧（既存・新規）

項目		検討事項	対応内容
社員教育・研修	個人情報保護	意識啓発・抑止	採用時・定例研修
		専門人材の育成	個人情報保護士等の資格取得
	コンプライアンス	意識啓発・抑止	採用時・定例研修
		意識啓発・防御	不当要求防止研修
			教唆対策研修
		コンプライアンス遵守の徹底	臨時研修
		組織に浸透	コンプライアンス推進委員会
			年間行動計画
		意識醸成	コンプライアンス推進月間
		浸透度の評価	自己点検・職場点検
	情報セキュリティ	意識啓発・抑止	採用時・定例研修
システム技術	システム端末の情報セキュリティ（技術面）	不正アクセス防止	専用ネットワーク
			専用カードとパスワード
			参照画面の制限
		大量持出防止	ダウンロード不可
	システム端末の情報セキュリティ（運用面）	記録の保存	操作ログの取得
			操作ログの保存期間延長
		監視	システム上でのログチェック
		使用者の厳格管理	共用カードの原則廃止
		周囲から見えない	見え易い場所に移設
	システム端末の情報セキュリティ（制度面）	ルールの明確化	情報セキュリティに関する規程等の遵守
情報漏えい対策	ISMS等	保護対象の明確化	資産管理台帳の作成
		保護対象別の対策	リスク評価の実施
		対策の評価	内部監査・外部審査
		リスク管理行動計画	リスク管理行動計画書の見直し
	情報セキュリティに関する規程等	禁止規定	第21条（遵守事項）
		罰則規定	第50条（懲戒）
		損害賠償	第54条（損害賠償）
	その他	個人的な悩み	外部専門機関への相談

※　　：新規