情報セキュリティ管理規程

第１章　総則

（目的）

第１条

本規程は、倫理規程第 8 条の規定における業務上知ることのできた秘密の取扱いに関し必要な事項を定めるとともに、日本下水道新技術機構（以下、「本機構」という。）のすべての情報資産を各種の脅威から保護するために体制及び対策を定め、高いレベルで情報セキュリティを確保することにより業務を円滑に推進することを目的とする。

（定義）

第２条

この規則における用語の定義は、次の各号に定めるところによる。

（１） 情報資産

本機構が所有する全ての情報（情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報を含む）及び関連する設備をいう。

（２） 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（３） 情報システム

コンピュータ、ネットワーク等で構成され、情報処理を行う仕組みをいう。

（４） ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（５） 管理区域

管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋や重要なストレージの保管庫をいう。

（６） 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（７） 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（８） 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（９） 個人情報

本機構が定める個人情報保護規程の第２条によって定義される個人情報をいう。

（１０）特定個人情報

本機構が定める特定個人情報取扱規程の第２条によって定義される個人情報をいう。

（１１）従業者

評議員、理事、監事及び本機構の指揮監督を受けて本機構の業務に従事している者をいう。

（情報セキュリティ対策基準）

第３条

本規程第 2 章の情報セキュリティ管理体制、第 3 章の情報セキュリティ対策の有効性、効率性の確保を目的として、遵守すべき行為及び判断等に関する事項を示す「情報セキュリティ対策基準」（以下「対策基準」という。）を別途理事長が定めるものとする。

（適用範囲）

第４条

本規程の適用範囲は、従業者及び共同研究に関与する者、委託事業者とし、情報セキュリティ対策について本規程を遵守するものとする。また、本規程に定めのない事項については、対策基準によるものとする。

２　共同研究に関与する者や委託事業者との間では、業務で取扱う情報の機密性に応じ情報セキュリティ要件について取り決めを定める契約を締結するものとする。

（委員会における情報の取扱い）

第５条

本機構で設置、運営する委員会で審議される項目には、共同研究者や技術審査を依頼する者の独自のノウハウや開発中の技術に関する情報が含まれているため、委員会で配布する資料や情報は委員会における審議の目的以外に使用してはならず、また委員会開催中だけでなく委員会終了後も何人に対しても開示してはならない。

なお、共同研究者や技術審査を依頼する者等から、情報開示に関して承認を得ている場合はこの限りではない。

２　第１項に記載の秘密保持義務を条件として、委員会の委員を委嘱するものとする。

（保護対象）

第６条

本規程で保護の対象とするものは、本機構が保有する全ての情報資産とする。

（情報資産の分類と定義）
第７条
本機構で取り扱う情報資産は、機密性、完全性及び可用性により分類し、対策基準に基づきセキュリティ対策を講じるものとする。また、それぞれに区分される情報の定義は次の各表に示す通りとする。

２　一つの情報資産に異なる区分の情報が複数存在する場合は、最高度の区分に従って情報を取り扱うものとする。

３　機密性に区分される情報の分類基準と対象とする情報資産は次の表の通りとする。なお、機密性１に区分される情報資産は公表可能な情報とする。

区分	分類基準	対象とする情報資産
機密性３	本機構が定める非公開情報のうち、特定の従業者又は組織など、業務上必要とする最小限の者のみが扱う情報資産	・ 本機構の定める特定個人情報取扱規程第 2 条に定める「特定個人情報」
機密性２	本機構が定める非公開情報のうち、機密性 3 以外の情報資産（機密性 2 に該当する全ての情報資産は、情報にアクセスすることが認められた者以外の従業者の利用を制限する。）	・ 本機構の定める個人情報保護規程第 2 条に定める「個人情報」 ・ 共同研究者及び審査証明依頼者の保有する機密情報 ・ 以下の内、情報が漏えいすることにより、本機構及び他の事業体の業務に支障を及ぼす恐れのある情報 ① 国、地方公共団体の入札情報 ② 国の政策支援に関する情報 ③ 地方公共団体の地域特性が判別できる情報 ・ 本機構が所管する以下の情報 ① 人事情報 ② 経理情報 ③ 財務情報 ④ 入札情報 ⑤ 予算管理情報 ・ その他、漏えいすることにより業務に支障を及ぼす恐れのある情報
機密性１	機密性 2 又は機密性 3 の情報資産以外の情報資産	

４　完全性に区分される情報の分類基準と対象とする情報資産は次の表の通りとする。

区分	分類基準	対象とする情報資産
完全性２	機構業務で取り扱う情報資産のうち、改ざん、誤謬又は破損により、関係者の権利が侵害される、又は機構業務の適確な遂行に支障（軽微なものを除く）を及ぼすおそれがある情報資産	・ 機密性３及び機密性２に該当する情報 ・ 本機構の定款・規程 ・ Web で公開している情報 ・ その他、完全性が確保されないことにより業務に支障を及ぼす恐れのある情報
完全性１	完全性２の情報資産以外の情報資産	

５　可用性に区分される情報の分類基準と対象とする情報資産は次の表の通りとする。

区分	分類基準	対象とする情報資産
可用性２	機構の業務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、関係者の権利が侵害される、又は機構業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・ 機密性３及び機密性２に該当する情報 ・ 本機構の定款・規程 ・ Web で公開している情報 ・ 情報システム・ネットワーク ・ その他、可用性が確保されないことにより業務に支障を及ぼす恐れのある情報
可用性１	可用性２の情報資産以外の情報資産	

（守秘義務）

第８条

本機構の従業者は、本機構で保有する機密性３及び機密性２の情報資産について、本機構の業務に従事している間だけでなく、本機構の職を退いた後も他の従業者又は本機構外の者、その他第三者に開示・漏えいしてはならない。

（目的外利用の禁止）

第９条

本機構で保有する情報資産は、本機構の業務以外で利用してはならない。

（個人情報及び特定個人情報の取り扱い）

第１０条

個人情報及び特定個人情報の取り扱いについては、「個人情報保護規程」及び「特定個人情報取扱規程」によるものとする。

第２章　情報セキュリティ管理体制

（情報セキュリティ管理責任者）
第１１条
　企画部長を情報セキュリティ管理責任者とする。

２ 情報セキュリティ管理責任者は、本機構の従業員に対し、情報セキュリティを確保するために遵守する事項について研修を行うものとする。

３ 情報セキュリティ管理責任者は、本機構の情報セキュリティについて監査を行い、第 14 条に定める情報取扱責任者に対し、適宜見直しを指示するものとする。

４ 情報セキュリティ管理責任者は、本機構の情報システム、ネットワークについての管理責任を有し、それらのセキュリティの状況について確認し、適宜見直しを行うものとする。

５ 情報セキュリティ管理責任者は、本機構の情報システム、ネットワークについての企画、開発、設定の変更、運用、更新等を行うものとする。

６ 情報セキュリティ管理責任者は、本機構の情報資産に対する侵害が発生した場合又は侵害の恐れがある場合に、必要かつ十分な措置を行うものとする。

７ 情報セキュリティ管理責任者は、本機構の情報システム及びネットワークに対する情報セキュリティ対策についての作業等を行う、情報セキュリティ担当者を指名するものとする。

８ 情報セキュリティ管理責任者は、自身の権限に属する事務を第 12 条に定める情報セキュリティ管理者および情報セキュリティ担当者に処理させることができるものとする。

（情報セキュリティ管理者）
第１２条
　企画部企画課長を情報セキュリティ管理者とする。

２ 情報セキュリティ管理者は、情報セキュリティ管理責任者を補佐するとともに、その指示に従い情報システム及びネットワークに対する情報セキュリティ対策を実施するものとする。

３ 情報セキュリティ管理者は、情報セキュリティ管理責任者の指示に従い情報システム及びネットワークの企画、開発、設定の変更、運用、更新等を行うものとする。

（情報セキュリティ担当者）
第１３条

情報セキュリティ担当者は、情報セキュリティ管理責任者の指示に従い、情報システム及びネットワークに対する情報セキュリティ対策の作業を行うものとする。

２ 情報セキュリティ担当者は、情報セキュリティ管理責任者の指示に従い、情報システム及びネットワークの企画、開発、設定の変更、運用、更新等の作業を行うものとする。

（情報取扱責任者）
第１４条
各部の長を情報取扱責任者とする。

２ 情報取扱責任者は、各部の所管する情報資産の管理責任を有し、各部の情報セキュリティを確保するために遵守すべき事項等について所属する部の従業者に対し指導及び助言を行うものとする。

３ 情報取扱責任者は、当該部署の情報取扱担当者を指名し、所管する情報資産のセキュリティ対策を実施させるものとする。

４ 情報取扱責任者は、所管の情報資産に対する侵害が発生した場合又は侵害の恐れがある場合は、速やかに情報セキュリティ管理責任者に報告するとともに、一次的な対応を指示するものとする。

（情報取扱担当者）
第１５条
情報取扱担当者は、情報取扱責任者の指示に従い、所管する情報資産のセキュリティ対策を行うものとする。

第３章　情報セキュリティ対策

第１節　情報資産の管理

（管理責任）
第１６条
各部の所管する情報資産についての管理責任は、情報取扱責任者が有するものとする。

（情報資産台帳）
第１７条
情報セキュリティ管理責任者及び情報取扱責任者は、本機構の情報資産について、本規程第７条に従い、機密性、完全性、可用性を分類した情報資産台帳を作成し、利用範囲や保存

媒体等を管理するものとする。

（情報の作成）
第１８条
　従業者は、業務上不要な情報を作成してはならない。

２ 情報を作成する者は、情報の作成時及び作成途上においても第 7 条の規定に従い分類するものとする。また、情報の作成途上で不要となった場合には、当該情報を消去するものとする。

３ 作成した情報及び作成途上の情報が機密性 2 に該当する場合は、表紙や余白等にその情報の取扱い方法を表示するものとする。

（情報資産の入手）
第１９条
　本機構外の者が作成した情報資産を入手した者は、第 7 条の規定に従い分類するものとする。なお、入手した情報資産の分類が不明な場合、情報取扱責任者に判断を仰ぐものとする。

２ 入手した情報が機密性 2 に該当する場合は、表紙や余白等にその情報の取扱い方法を表示するものとする。

（情報資産の保管）
第２０条
　機密性 2 に区分される情報資産の内、電磁的記録については関係者以外がアクセスすることができないフォルダに保管するもとする。

２ 機密性 2 に区分される情報資産の内､印刷物等についてはフラットファイル等に格納し、保管場所を特定するものとする。なお、格納するフラットファイル等には情報の取扱い方法を表示するものとする。

（情報資産の利用）
第２１条
　機密性 2 に区分される情報資産は、第 18 条又は第 19 条に従い取扱い方法が表示されたものを、必要最小限の数量のみ印刷又は複写するものとする。

２ 機密性 2 に区分される情報資産を外部に持ち出す際は、情報取扱責任者の許可を得るものとする。

（情報資産の送信・郵送）

第２２条

機密性 2 の情報資産を電子メール等により送信する際は、暗号化又はパスワード設定を行うものとする。

２　機密性 2 の情報資産を郵送等により送付する際は、封筒に格納するなど外部に情報が漏洩しない対策を行うとともに、郵送先に誤りがないか二重のチェックを行うものとする。

（情報資産の運搬）

第２３条

機密性 2 の情報資産を運搬する際は、文書等については封筒等に封入し、カバン等に入れて持ち運ぶものとし、電磁的記録等についてはパスワードの設定を行うなど、情報資産の不正利用を防止するための措置を講じるものとする。

（情報資産の提供・公表）

第２４条

機密性 2 の情報資産は原則として情報にアクセスすることが認められた者以外の従業者及び外部に提供・公表してはならない。ただし、法令等に定められている場合及び業務遂行上の必要性が認められる場合は、情報取扱責任者に許可を得て提供・公表するものとする。

（文書の廃棄）

第２５条

機密性 2 に区分される情報資産の内、文書については、再利用せず不要になり次第シュレッダー等で裁断し、判読不能な状態にして廃棄する。

（パソコン等の廃棄）

第２６条

パソコン等の機器や電磁的記録が可能なストレージ、その他の情報機器については情報セキュリティ管理責任者の指示がない限り廃棄してはならない。

２ パソコン等の機器や電磁的記録が可能なストレージを廃棄又はリース品を返却する際は、専用ソフト等による情報消去を行い、保存されている情報を消去し、復元不可能な状態にする措置を講じるものとする。

（その他）

第２７条

情報資産の管理に関し本規程に定めのない事項については、対策基準に従うものとする。

第２節　情報システム、ネットワークのセキュリティ対策

（サーバ等の管理）

第２８条

　情報セキュリティ管理責任者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じるものとする。

（機器の定期保守及び修理）

第２９条

　情報セキュリティ管理責任者は、所管するサーバ等の機器の定期保守を必要に応じて実施するものとする。

２　情報セキュリティ管理責任者は、コンピュータを外部の業者に修理させる場合、内容を消去した状態で行わせるものとする。内容を消去できない場合、情報セキュリティ管理責任者は、修理を委託する事業者との間で、機器の機密性に応じて守秘義務契約を締結するなど、秘密保持に必要な措置を講じるものとする。

（敷地外への機器の設置）

第３０条

　情報セキュリティ管理責任者は、機構が管理する施設の外にサーバ等の機器を設置する場合、定期的に当該機器への情報セキュリティ対策状況について確認するものとする。

（管理区域）

第３１条

　管理区域は、固定された隔壁で区画された専用の事務室とし、外部からの侵入が容易にできない構造とする。

２　情報システム管理責任者は、管理区域への入退室について許可された者のみに制限する措置を講じるものとする。

（バックアップの実施）

第３２条

　情報セキュリティ管理責任者は、サーバ等に記録された情報について、必要に応じて定期的にバックアップを実施するものとする。

（アクセス制御）

第３３条

　情報セキュリティ管理責任者は、所管するネットワーク又は情報システムに、権限のない

者がアクセスできないように制限するものとする。

（利用者 ID の取扱い）
第３４条
　情報セキュリティ管理責任者は、利用者の登録、変更、抹消等の情報管理、従業者の異動、出向、退職に伴う利用者 ID の取扱い等の方法を定めるものとする。

（パスワードに関する情報管理）
第３５条
　情報セキュリティ管理責任者は、従業者のパスワードに関する情報を厳重に管理するものとする。

（不正プログラム対策）
第３６条
　情報セキュリティ管理責任者は、所管するパソコン等に不正プログラム対策ソフトウェア等を常駐させるなど、不正プログラム対策について適切な措置を実施するものとする。

（不正アクセス対策）
第３７条
　情報セキュリティ管理責任者は、ネットワークにファイアウォールを設定するなど、不正アクセス対策について適切な措置を実施するものとする。

（可搬媒体）
第３８条
　電磁的記録を持ち運ぶことができる可搬媒体は、原則として情報セキュリティ管理責任者が貸与する USB メモリを使用するものとし、その他の可搬媒体を本機構が管理するパソコン等に接続してはならない。ただし、容量不足等の理由により他の可搬媒体を使用せざる得ない場合は、別途情報セキュリティ管理責任者と協議するものとする。

２ 従業者は、貸与された USB メモリを厳密に管理するものとし、USB メモリ内のデータは不要になり次第速やかに削除しなければならない。

（従業者が本機構の外で使用する機器の登録）
第３９条
　本機構の従業者が、本機構の外で各自のスケジュール管理及びメールの受発信を行うために端末を使用する際は、その端末について事前に情報セキュリティ管理責任者に報告し登録するものとする。

（その他）
第４０条
　情報システム、ネットワークのセキュリティ対策に関し本規程に定めのない事項については、対策基準に従うものとする。

第３節　事故・欠陥等の対応
（事故等の報告）
第４１条
　従業者及び共同研究に関与する者、委託事業者は、情報セキュリティに関する事故、情報システムにおける欠陥及び誤動作を発見した場合、速やかに情報取扱責任者に報告しなければならない。

２ 報告を受けた情報取扱責任者は、一次的な対応を指示するとともに、速やかに情報セキュリティ管理責任者に報告しなければならない。

（ネットワークの遮断）
第４２条
　従業者及び共同研究に関与する者、委託事業者は、情報セキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（事故等の対応）
第４３条
　情報セキュリティ管理責任者は、情報セキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、情報取扱責任者に対し適切な措置を求めなければならない。

第４節　その他のセキュリティ対策
（研修）
第４４条
　情報セキュリティ管理責任者は、情報セキュリティに関する研修を実施し、従業者は、定められた研修に参加しなければならない。

（監査）
第４５条
　情報セキュリティ管理責任者は、情報セキュリティ対策を徹底するために、情報セキュリティの管理現場に対し監査を実施するものとする。

２ 公平性、公正性、中立性及び特に専門性を期するために、必要に応じて外部の監査組織による監査を実施するものとする。

（見直し）
第４６条
情報セキュリティ監査の結果及び情報セキュリティを取り巻く状況の変化に応じ、本規程及び対策基準の見直しを図るものとする。

第４章　その他

（罰則）
第４７条
本機構は、本規程に違反した従業者に対して就業規則に基づき処分を行い、その他の従業者及び共同研究に関与する者、委託事業者に対しては、契約又は法令に照らして決定する。

（改正）
第４８条
この規程の改正は、理事会の決議を経て行う。

附 則
この規則は、令和元年６月２０日から施行する。