平成 19 年 10 月 1 日（制定）
平成 25 年 4 月 1 日（改訂）
平成 27 年 10 月 16 日(改定)

情報セキュリティ対策委員会

一般財団法人水源地環境センター
情報セキュリティ対策基準

この情報セキュリティ対策基準は、一般財団法人水源地環境センター（以下「当センター」という。）が定めた情報セキュリティポリシーに基づき、当センターの情報セキュリティ確保のために実施すべき対策基準を定めたものである。

第1編　基本的事項

1-1 就業規則・関係法令等の遵守

当センターは、情報セキュリティ対策を実施する際には、セキュリティポリシーのほか、就業規則(秘密保持に関する条項等)、不正アクセス行為の禁止等に関する法律、著作権に関する法律、個人情報の保護に関する法律、その他関係法令等を遵守するものとする。

1-2 対象範囲

情報セキュリティ対策基準の対象範囲は以下のとおりとする。

(1)当センターにおいて業務上取扱う情報（以下「情報」という。）

(2)当センターにおいて、ハードウェア、ソフトウェア、ネットワーク、電子記録媒体で構成され、これら全体で業務処理を行うもの（以下「情報システム」という。）

(3)情報及び情報システムを扱うすべての業務従事者（以下「業務従事者」という。）

1-3 情報セキュリティ体制

1-3-1　体制

当センターにおける情報セキュリティ対策を実施するため、情報セキュリティ最高責任者、情報セキュリティ対策委員会、情報セキュリティ統括責任者、情報セキュリティ副統括責任者、情報セキュリティ責任者、システム管理責任者を置く。

1-3-2　情報セキュリティ最高責任者

情報セキュリティ最高責任者は、当センターの理事長とする。情報セキュリ

ティ最高責任者は、情報の運用・管理を指導し、情報セキュリティ対策に係る事務を統括する。

また、情報セキュリティ対策委員会を設置し、当センターの情報セキュリティ体制の確立に努める。

1-3-3　情報セキュリティ対策委員会

(1)委員会の役割

情報セキュリティ対策委員会（以下「委員会」という。）は、情報セキュリティポリシーに基づき、情報セキュリティ対策基準等重要事項を定めるとともに、情報セキュリティ対策基準に関する評価・見直し等を行う。

(2)委員会構成メンバー

委員会の長は、担当役員とする。委員の構成は、情報セキュリティ副統括責任者、各部の情報セキュリティ責任者、及びシステム管理責任者等とする。

(3)委員会事務局

委員会事務局は、当センター企画部に置く。

1-3-4　情報セキュリティ統括責任者

情報セキュリティ統括責任者は、委員会の長である担当役員とする。情報セキュリティ統括責任者は、情報セキュリティ責任者及びシステム管理責任者を統括し、当センターの情報セキュリティ対策に係る事務を統括する。また、情報セキュリティ対策の企画・調整を行う。

1-3-5　情報セキュリティ副統括責任者

情報セキュリティ副統括責任者は、担当役員以外の役員とする。情報セキュリティ副統括責任者は、情報セキュリティ統括責任者を補佐し、情報セキュリティ統括責任者に事故があった場合その代理の任にあたる。

1-3-6　情報セキュリティ責任者

情報セキュリティ責任者は、各部の長とする。情報セキュリティ責任者は、各部が所管する業務に関する以下の事項を実施する。

(1)情報セキュリティ対策の統括・調整

(2)情報セキュリティ対策に関する業務従事者への教育

(3)情報セキュリティ事故が発生した場合の迅速な対応

(4)その他、情報セキュリティ統括責任者が指示する事項

1-3-7　システム管理責任者

システム管理責任者は、企画部長とする。システム管理責任者は、当センターが所管する以下の情報システムに関する管理を行う。

(1)当センター内の情報システムに関する設定、運用、変更
(2)その他、情報セキュリティ統括責任者が指示する事項

1-4 情報セキュリティ教育

1-4-1　教育の実施

情報セキュリティ統括責任者及び情報セキュリティ責任者は、業務従事者に対し、セキュリティポリシー及び情報セキュリティ対策基準に関する教育を実施しなければならない。

1-5 外部委託先に関する管理

1-5-1　契約事項の明示

業務従事者は、外部委託先への業務の仕様に、情報管理及び機密保持に関する契約事項を明示しなければならない。

1-5-2　契約事項の確認

情報セキュリティ責任者は、情報管理に関して委託先との契約が適正に行われているか確認しなければならない。

1-6 情報漏洩等への対応

1-6-1　報告

情報漏洩等のセキュリティに関する事案の可能性があることを認めた者は、速やかに、情報セキュリティ責任者に報告しなければならない。

1-6-2　応急措置

情報セキュリティ責任者は、情報セキュリティ対策委員会へ報告し、速やかに、応急措置を施さなければならない。

1-6-3　再発防止策

情報セキュリティ対策委員会は、事案による影響を最小限に留めるように対処するとともに、原因を究明し、再発防止策を施さなければならない。

第2編　情報漏洩対策に関する事項

2-1 情報の取扱い

2-1-1　業務以外での利用の禁止

業務従事者は、当センターの業務以外に、情報を利用してはならない。

2-1-2　情報の管理

(1)業務従事者は、当センター内において情報を利用することを原則とし、業務上利用する必要がある者（業務契約相手先等）への当該情報の移送（送付・運搬等）を除き、情報を記録媒体（紙、電子記録媒体等）、又は回線（インターネット等）を用いて当センター外（自宅等）に持ち出

してはならない。ただし、業務上、当センター外で情報を利用せざるを得ないときは、当該業務の情報セキュリティ責任者の許可を得た上で、持ち出すことができるものとする。

(2)業務従事者は、情報を持ち出す許可を得て記録媒体を携行する場合は、身の回りから離さないようにし（電車の網棚には置かない等)、手荷物として持ち運ぶ。また、必要に応じて（携行する荷物が複数にわたる場合等)、施錠できる鞄等で携行するものとする。

2-1-3　情報の移送

業務従事者は、情報を移送（送付・運搬等）する場合は、2-1-2 情報の管理の規定に従うとともに、移送先の情報セキュリティ対策等の安全対策を確認した上で移送しなければならない。

2-1-4　情報の入手

業務従事者は、当センター外の者が作成した情報を入手する場合は、入手先の情報セキュリティ対策等の安全対策を確認した上で入手しなければならない。

2-1-5　不要となった情報の記録媒体の取り扱い

業務従事者は、不要となった情報の記録媒体（残余書類等）について、情報が漏洩しないように適切な措置を講じるものとする（シュレッダーによる廃棄等)。

2-2 情報システムの取扱い

2-2-1　業務以外での利用の禁止

業務従事者は、当センターの業務以外に、情報システムを利用してはならない。

2-2-2　ＰＣ等（パーソナルコンピュータ及び電子記録媒体）の利用

(1)業務従事者は、業務履行に際しては、当センターから貸与されたＰＣ等を利用することとし、個人所有のＰＣ等を利用してはならない。

(2)業務従事者は、当センター外（自宅等）に当センターから貸与されたＰＣ等を持ち出してはならない。

ただし、以下の場合の用途に限り、当該業務の情報セキュリティ責任者の許可を得た上で、持ち出すことができる。

①委員会、検討会等に用いるとき。

②業務打合せにおいてデモンストレーションを行うとき。

③学会、講演会等に用いるとき。

④業務上、当センター外でＰＣ等を利用せざるを得ないとき。

なお、貸与されたＰＣ等以外の当センター管理のＰＣ等を当センター外に持ち出す場合には、上記の規定に従うとともに、システム管理責任者の許可を得なければならない。

(3)業務従事者は、ＰＣ等を持ち出す許可を得た場合、以下の措置により、ＰＣ等を厳格に管理しなければならない。

①運搬時においては、身の回りから離さないようにし（電車の網棚には置かない等)、手荷物として持ち運ぶ。また、必要に応じて（携行する荷物が複数にわたる場合等)、施錠できる鞄等で携行するものとする。

②ＰＣ等については、パスワードの設定により保護するものとする。

2-2-3　ソフトウェアの利用

業務従事者は、当センターのＰＣに導入されているソフトウェア以外の新たなソフトウェアを無断で導入してはならない。

新たなソフトウェアを導入する場合には、当該ソフトウェアの必要性を明示した上で、システム管理責任者の許可を得なければならない。なお、システム管理者はこの許可に当たっては、当該ソフトウェアの安全性を確認しなければならない。

2-2-4　パスワードの管理

業務従事者は、当センターの情報システムにおいて、自己の保有するパスワードに関し、次の事項を遵守しなければならない。

(1)仮パスワードは、最初のログイン時点で変更すること。

(2)自己の保有するパスワードを秘密にしておくこと。

(3)パスワードは、定期的に変更すること。

(4)自己の保有するパスワード以外で情報システムを利用しないこと。

2-2-5　ウィルス対策

(1)業務従事者は、ＰＣのウィルスの自動チェック機能を解除してはならない。

(2)業務従事者は、当センター外から情報を取り入れる場合には、ウィルスチェック等による安全確認を行わなければならない。

(3)システム管理責任者は、ウィルスに対する情報収集を行い、ウィルスチェック用のパターンファイルを常に最新のものに保つよう、システム整備を行わなければならない。

2-3 インターネット

(1)業務従事者は、業務目的以外で外部の Web サイトへのアクセスを行ってはならない。

(2)システム管理責任者は、業務目的以外の Web サイトへのアクセスを制限する措置を講じなければならない。

2-4 電子メール

(1)業務従事者は、業務目的以外で電子メールを利用してはならない。

(2)業務従事者は、業務履行に当たり、個人所有の電子メールを利用してはならない。

(3)業務従事者は、Web メールを利用してはならない。

(4)業務従事者は、不審なメールが届いた場合は、開かずに削除しなければならない。

(5)システム管理責任者は、不審メールの受信に対する制限を施さなければならない。

2-5 その他例外措置

(1)業務従事者は、2-1～4 に定めるもの以外の例外措置の適用を希望する場合には、情報セキュリティ責任者に対し、以下を明確にして許可を求めなければならない。

①例外措置の適用を申請する情報セキュリティ基準の適用箇所（条項等）

②例外措置の適用を申請する期間

③例外措置の適用を申請する措置内容

④例外措置の適用を終了したときの報告方法

⑤例外措置の適用を申請する理由

(2)情報セキュリティ責任者は、許可の際には、以下の要件を充足していることを確認し、当該許可内容について、システム管理責任者、情報セキュリティ統括責任者に報告しなければならない。

①当該例外措置が業務遂行上必要不可欠であること。

②当該行為が情報セキュリティ上特段の支障を生じさせない。

なお、全体の情報セキュリティ対策の許可に当たっては、必要に応じて、情報セキュリティ対策委員会で許可方針を定めるものとする。

(3)業務従事者は、上記の許可を受け、例外措置を実施した場合には、それを終了したときに、情報セキュリティ責任者にその旨を報告しなければならない。ただし、情報セキュリティ責任者が報告を要しないと判断した場合には、この限りではない。

以 上

一般財団法人水源地環境センター

情報セキュリティ体制