株式会社キャンパスクリエイト

PFAS 対策技術コンソーシアム事務局
情報セキュリティ管理規程

2025 年 3 月 11 日制定

PFAS 対策技術コンソーシアム事務局

情報セキュリティ管理規程

第 1 章　総則

第 1 条　（目 的）

本規程は株式会社キャンパスクリエイト（以下「会社」という）が、PFAS 対策技術コンソーシアムの事務局としての業務（以下、「本業務」という）を運営する上で取り扱うコンソーシアム会員企業、個人、及び講演依頼先の研究者や取引先等（以下「顧客等」という）から提供される情報資産を各種の脅威から適切に保護し、事務局業務を正常かつ円滑に行うことを目的とする。

第 2 条　（定 義）

本規程における用語の定義は、次のとおりとする。

(1)「情報資産」とは、情報、情報システム、およびこれらを適切に運用・管理・利用するために必要なものをいい、ハードウェア、ソフトウェア、ネットワークや記録媒体のほか、業務上知り得た情報、知識、ノウハウ等をすべて含むものとする。

(2)「情報セキュリティ」とは、情報資産の「機密性」、「完全性」および「可用性」を確保し、維持することをいう。

(3)「機密性」とは、情報資産を、アクセス権限を持つ者のみに所定の方法にて開示し、アクセス権限を持たない者から保護することをいう。

(4)「完全性」とは、情報資産を、整合性を保ちながら改ざん等がなされることなく、正確に処理し、保持することをいう。

(5)「可用性」とは、情報資産を、アクセス権限を持つ者が必要なときに中断されることなく、利用できるように保持することをいう。

第 3 条　（適用範囲）

本規程は、本業務上取り扱う顧客等の情報資産すべてに適用する。なお、顧客等の情報資産の管理・取扱い等について、契約等により特段の運用ルール等を定めている場合には、当該運用ルール等に従うものとする。

第 2 章　情報セキュリティ管理規程の構成

第 4 条　（情報セキュリティ管理規程の構成）

本規程を含めた情報セキュリティ管理規程の構成は本規程及び、別紙の「情報セキュリティ管理基準」で構成するものとし、本規程に定めのない個別の基準・ルール等については、「情報セキュリティ管理基準」に定めるものとする。

第 3 章　組 織 体 制

第 5 条　（情報セキュリティ管理委員会）

会社は、PFAS 対策技術コンソーシアム事務局の情報セキュリティに関する統括組織として、情報セキュリティ管理委員会を設置する。

2 情報セキュリティ管理委員会は、情報セキュリティ管理基準に基づく情報セキュリティの徹底を推進するとともに、情報セキュリティに関し情報セキュリティ管理基準に定めのない事項についての判断基準を示す等、本業務に係る情報セキュリティ全般につき統括する。

3 情報セキュリティ管理委員会の委員長は株式会社キャンパスクリエイト 代表取締役とする。

4 情報セキュリティ管理委員会は、委員長及び、委員長が任命する委員とシステム管理者で構成するものとする。

第 6 条　（委員）

委員は、情報セキュリティ管理委員会の統括の下、情報セキュリティ管理基準に基づく情報セキュリティの徹底を推進するものとする。

第 7 条　（システム管理者）

システム管理者は、委員と連携し、本業務の情報セキュリティ取り扱いにおける指導・啓蒙や適切な環境の整備等、情報セキュリティ管理基準を徹底するために必要な措置を講じなければならないものとする。また、システム管理者は教育担当者を兼任することがある。

第 8 条　（教育担当者）

委員が任命した教育担当者は、本業務の担当者変更がある際などに、当該社員に対し情報セキュリティ管理基準を遵守させるために必要な教育を企画・運営するものとする。なお、教育の時期は本業務の一部または全部の引継ぎ時、情報セキュリティ管理委員会が必要と判断した時とし、内容は教育担当者が立案し、委員によって承認されるものとする。

第 5 章　リ ス ク 評　価　と 監　査

第 9 条　（リスク評価）

情報セキュリティ管理委員会は、技術の進歩や業務環境の変化等も考慮のうえ、情報資産のリスク評価を多方面から継続的に実施し、それを情報セキュリティ管理基準およびそれに基づく各種施策に反映させることにより、情報セキュリティの維持・向上を図るものとする。

第 10 条　（監査の実施）

監査担当者は、情報セキュリティ管理基準の遵守状況を定期的に内部監査するものとする。

2 システム管理者より情報セキュリティ管理基準の遵守状況につき改善、勧告等を受けた被監査業務に関しては、適切な是正措置を講じなければならないものとする。

第 6 章　罰　則

第 12 条　（情報セキュリティ管理基準に違反した場合の措置）

会社は、社員が情報セキュリティ管理基準に違反した場合は、会社の就業規則に基づき懲戒に処す。ただし、受入出向社員については、出向元会社との出向契約に従うものとする。

2 臨時社員が情報セキュリティ管理基準に違反した場合は、「パートタイマーおよびアルバイト就業規則」に従うものとする。

3 派遣社員および協力会社社員が情報セキュリティ管理基準に違反した場合は、派遣元または業務委託先との契約に従うものとする。

付　則　本規程は令和7年4月 1 日より施行する。

別紙

情報セキュリティ管理基準

本基準は、会社が本業務において顧客等から提供される情報資産を各種の脅威から適切に保護し、事務局業務を正常かつ円滑に行うことを目的とし、会社が情報セキュリティ管理を行う上での情報セキュリティ対策の基準・ルールを定めるものとする。

重要情報の取扱い

(趣旨)

本基準は、本業務において顧客等から提供される機密情報及び個人情報の取り扱い（保存 ・ 移動 ・破棄）において注意するべき事項をまとめ、発生しうる問題を未然に防ぐことを目的とする。

(遵守事項)

1. 情報資産の分類

本業務で取り扱う情報資産は、以下のクラスに分類される。

クラス 1（一般情報）：顧客から第三者への頒布を含み、一般に公開することに合意した情報。
クラス 2（限定公開情報）：コンソーシアムの会員企業・個人に限り公開が許可された情報。
クラス 3（高度な機密情報）：個人情報を含むデータ、関係者外秘の情報。

各情報のクラス分けは、当該情報の提供者と文書による合意のもと確認を行う。

上記他、コンソーシアム会員外の一部の企業、または個人への提供を行う際には、情報提供者と文書による合意を確認の上、必要な関係者との契約を取り交わすものとする。

2.重要情報の管理

本基準では、クラス 2 およびクラス 3 の情報を「重要情報」とし、以下の管理を行う。

・表示

クラス2　当該情報中に、本情報資産が、限定公開である旨及び公開可能範囲について明示を行うこと。
クラス3　当該情報中に、本情報資産が、高度な機密情報であり、関係者以外の閲覧が禁じられる旨の明示を行うこと

・複製

クラス3　委員及び代表の許可を得ること。また、複製の記録を残すこと。

・配付

クラス3：情報資産の提供者、及び委員及び代表の許可を得ること。また、配付の記録を残すこと。
クラス2：公開の範囲を限定し、非公開のクラウドサービスのリンク先などの共有を行うことなどにより、配付を行う。

・暗号化

クラス2、クラス3共に保管場所のファイルサーバーやクラウドサービスのアカウント情報にパスワードを設定すること
パスワードは、適切かつ合理的な頻度で更新、及び管理を行い、セキュリティを担保すること

・印刷

クラス3：情報資産の提供者、及び委員及び代表の許可を得ること。また、配付の記録を残すこと。

・閲覧者の制限

クラス3：担当者に限る

2 重要情報の移動

(1) 電子メールで送信する際はパスワードを用いる。

(2) FAX の送信時には必ず宛先を確認し、誤送信を防止しなければならない。

(3) 原則外部記憶装置 USB メモリ、SD カード等を使用し、社外に持ち出してはならない。

(4) 機密情報及び個人情報を移動する際は、安全管理対策が講じられたサービスを利用する。

(5) クラウドサーバーやオンラインストレージ等の外部サービスを導入する場合は、システム管理者が協力会社社員と連携し、必要な機能やセキュリティ対策等をあらかじめ十分評価したうえで利用しなければならない。

3. 重要情報の保存期間、保存場所

(1)クラス2に該当する情報資産の保存期間は、受領日から半年間とする。

(2)クラス2に該当する情報資産のうち、本業務の範囲で、コンソーシアム会員限定で配布する資料、動画等の情報等の元データ等の保管期間は、当該の配信を開始した日から半年間とする。

(3)クラス3に該当する情報資産の保存期間は、受領日から半年とする。

(4)重要情報は、権限を有しない者の不必要なアクセスを防ぐため、適切なアクセス権が設定されている場所に保存し必要かつ合理的な安全管理対策を行なわなければならない。また、会社の承認を得ない社外への持ち出し或いは第三者に提示又は提供を禁止する。

4. 重要情報の保存期間完了後の措置

・重要情報の保存期間中の削除は禁止する。
・顧客及び取引先等との契約書により重要情報の破棄について定めている場合には、契約に従うものとする。
・紙媒体についてはシュレッダーを利用する等、破棄後に第三者が利用できない措置をとらなければならない。

委託管理基準

(趣旨)

本基準は、会社が外部の企業、機関または個人と委託契約もしくは再委託契約をする際の機密情報及び個人情報の取り扱いにおいて発生しうる問題を未然に防ぐことを目的とする。

(遵守事項)

1. 委託先または再委託先は機密情報及び個人情報の取り扱いにおいて十分な情報セキュリティ管理の水準を満たしていること、その他実績等も考慮した上で、信頼できる企業、機関、または個人を選定すること。

2. 委託契約及び再委託契約の際には、以下の項目を盛り込んだ契約書を作成する。

(1) 秘密保持に関する事項

(2) データ等の保管及び破棄についての取り決め

(3) セキュリティインシデントが発生した場合の報告及び連絡

(4) 違反した場合における契約解除等の措置及び損害賠償に関する事項

3. 機密情報及び個人情報を取り扱う業務を委託または再委託をする場合には、上記に加えて、次の事項を契約に盛り込むこと。

・機密情報及び個人情報の漏洩防止、盗用禁止に関する事項

・契約業務の範囲外の加工・複製の禁止

・第三者への提供の禁止

・契約期間終了後の返還・消去・破棄に関する事項

PC の取り扱い

(趣旨)

本基準は、会社の管理する全ての PC の安全性を確保し、発生しうる問題を未然に防ぐことを目的とする。

(遵守事項)

1. PC に導入するソフトウェア

(1) 原則業務に必要のないソフトウェアをインストールしてはならない。

(2) デバイスドライバ及び更新プログラム以外のソフトウェアは、システム管理者の許可を得たうえでインストールしなければならない。

2. システム維持

(1) OS 及びインストールしたソフトウェアは更新プログラム等を適用し、原則最新の状態で使用しなければならない。ただし、正式版ではないプログラムは原則インストールしてはならない。

(2) PC 利用において異常を感じた場合は速やかにシステム管理者に報告しなければならない。

3. PC 利用の制限

(1) PC の利用者は、与えられたアカウントでログインしなければならない。

(2) PC の利用者は、PC の利用者を無断で変更してはならない。

(3) ログイン時には PC 利用者が設定したパスワードを用いることとし、ロック解除方法が第三者に漏れないようにしなければならない。

(4) PC の利用者を変更する場合には、システム管理者に届け出なければならない。

4. ウイルス対策の徹底

(1) PC の利用者は、PC を利用する上でウイルス対策を徹底しなければならない。

(2)『ウイルス対策』に規定されている遵守事項を徹底しなければならない。

5. PC 及び外部記憶装置の廃棄等

(1) PC 及び外部記憶装置を廃棄またはリース返却等する場合にはデータを完全に抹消するか、物理的に破壊しなければならない。

6．PC の社外への持ち出し時の注意事項

(1) 社内 PC を業務目的以外の理由で社外に持ち出してはならない。

(2) 移動時の交通機関や人混みでは、盗難に遭わないよう、適切に PC を所持しなければならない。

(3) 社外で PC を使用する際には、盗み見に注意し安全な場所で利用しなければならない。

(4) 紛失防止のため、PC は常に手元に置き、放置しないようにすること。

(5) 紛失に気付いた場合は、『セキュリティインシデント報告・対応』に基づき速やかに対応しなければならない。

ネットワーク利用

(趣旨)

本基準は、機密保持及び情報資産の保護、有効活用を目的にネットワークの利用管理を行う。

(遵守事項)

1．接続機器

会社が許可していない機器を社内ネットワークに接続してはならない。

2．社内ネットワークへの接続時の注意事項

会社所有の PC を業務上やむを得ず社外ネットワークに接続する場合は、安全性が確保されたネットワークに接続しなければならない。やむを得ず、無料 Wi-Fi 等のネットワークを利用する場合は、VPN 経由等会社が認めた方法でアクセスしなければならない。

電子メール利用

(趣旨)

本基準は、電子メールで受け渡される情報の安全性を確保し、電子メール利用にあたって発生しうる問題を未然に防ぐことを目的とする。

(遵守事項)

1．電子メールアカウントの管理について

(1) 電子メールアカウントを業務目的以外で使用してはならない。

(2) 電子メールアカウントを不正に利用されたと思われる場合は、システム管理者に報告しなければならない。

2．電子メールの送受信について

(1) 当社の事業に関わる情報や、顧客、従業員のプライバシーに関わる情報などの機密情報は、原則として電子メールを用いて送信してはならない。

（2） 業務上やむを得ず機密情報を送受信する場合は、情報セキュリティ委員会の指示に従い、内容に応じて暗号化、電子署名などの処置を施さなければならない。

（3） 電子メールの送信にあたっては、送信先のメールアドレスに間違いがないか、確認の上送信しなければならない。

（4） 当社のセミナーやイベントの案内などのように社外の複数のドメインが混在するメールアドレスに対し、1 通の電子メールで同報送信する場合は、送信先メールアドレスが受信者間で閲覧できないよう、設定しなければならない。また、広告メール等の送信にあたっては法を遵守しなければならない。

（5） パスワードの使用にあたっては、漏えいによる不正使用を防止するため、他者が容易に推測できるものを使用してはならない。また、適切な期間ごとにパスワードを変更しなければならない。

（6） 送信元不明のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審な添付ファイルに対してはこれに操作を加えてはならない。

ウイルス対策

（趣旨）

本基準は、ウイルスによって引き起こされる情報漏洩やシステム破壊の被害を未然に防ぐことを目的とする。

（遵守事項）

1. ウイルス対策ソフトの導入

（1）原則全てのサーバ、PC にウイルス対策ソフトを導入する。

（2）ウイルス対策ソフトは、会社が選定したソフトを導入し、定期的に見直しを実施する。

2. ウイルス対策ソフトの利用

PC の利用者は、システム管理者が設定したウイルス対策ソフトの設定を変更してはならない。

3. PC における電子メールやインターネット閲覧を介してのウイルス被害の防止

（1）PC の利用者は、送信元不明（特にフリーメール）のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審だと疑われるメールの添付ファイルは安易に開いてはならない。また、安易にURLリンクをクリックしてはならない。

（2）電子メールサービスを利用中に、 不審だと疑われるメールの受信、ウイルスの発見、ウイルスと思われる症状を発見した場合は、システム管理者に報告しなければならない。

（3）インターネット閲覧によるウイルス感染を防ぐ為に、PC の利用者は安全ではないと思われるサイトを閲覧してはならない。また、 安易にファイルのダウンロードや URL リンクをクリックしてはならない。

4. ウイルスに感染した場合、または感染したと疑われる場合

（1）PC の利用者は、ウイルスに感染した場合、または感染したと疑われる場合は、システム管理者に報告しなければならない。

（2）PC の利用者は、有線LAN接続のPCはネットワークケーブルを外し、無線LAN接続のPCは無線LAN機能をOFFにしなければならない。

(3)システム管理者は情報セキュリティ部門の指示に従い、適切に対処しなければならない。

スマートフォンの取り扱い

(趣旨)

本基準は、会社の管理する全てのスマートフォンの安全性を確保し、発生しうる問題を未然に防ぐことを目的とする。

(遵守事項)

1. スマートフォンの使用

会社の業務に利用するスマートフォンは、会社が支給・貸与するものでなければならない。

2. スマートフォンの利用の制限

(1) スマートフォンの利用者は、スマートフォン利用者を無断で変更してはならない。

(2) ログイン時にはスマートフォン利用者が設定したパスワードを用いることとし、ロック解除方法が第三者に漏れないようにしなければならない。

(3) スマートフォンの利用者を変更する場合には、システム管理者に届け出なければならない。

3. スマートフォンの社外への持ち出し時の注意事項

(1) スマートフォンを業務目的以外の理由で社外に持ち出してはならない。

(2) 移動時の交通機関や人混みでは、盗難に遭わないよう、適切にスマートフォンを所持しなければならない。

(3) 社外でスマートフォンを使用する際には、盗み見に注意し安全な場所で利用しなければならない。

(4) 紛失防止のため、スマートフォンは常に手元に置き、放置しないようにすること。

(5) 紛失に気付いた場合は、『セキュリティインシデント報告・対応』に基づき速やかに対応しなければならない。

セキュリティインシデント報告・対応

(趣旨)

本基準は、セキュリティインシデントが発生した場合及びセキュリティインシデントの発生と疑われる場合に、適切な報告、対応、情報システム環境の復旧がそれぞれ速やかになされることと、継続的な再発防止が行われることを目的とする。

セキュリティインシデントとは次のような事態を指す。

(1) セキュリティに対する侵害

例　情報漏洩、ウイルス感染、DoS 攻撃、記録媒体等の紛失　等

（2） システム・ネットワークの故障・損壊

例　電源異常、自然災害　による機器損壊　等

（3） 情報資産への脅威

例　建物への侵入　等

（遵守事項）

1．平時の準備

セキュリティインシデントが発生した場合、あるいは発生が疑われる場合は、情報セキュリティ管理委員会及びシステム管理者に遅滞なく報告がなされ、速やかにセキュリティインシデントの分析、封じ込め、原因の根絶、復旧が可能となるよう、2項以降に示す対応について以下の準備作業を行い、関係者への周知を徹底する。

(1)情報セキュリティ管理委員会は、セキュリティインシデントが発生した場合、あるいは発生が疑われる場合においての対応を準備し、会社での周知を徹底する。

(2)システム管理者は、想定するセキュリティインシデントの具体的な対応手順を策定する。

(3)システム管理者は、策定した対応手順でセキュリティインシデントに対応可能となるよう、定期的に訓練を行い、併せて対応手順に問題がないか確認を行い、対応手順に問題があれば是正する。

（4） システム管理者は、セキュリティインシデントの検知に必要な情報セキュリティ対策を導入し、情報セキュリティ管理基準に適応する環境を整備しなければならない。

2．セキュリティインシデントあるいは発生が疑われる事業が発生した際の対応

(1)セキュリティインシデントあるいは発生が疑われる事象を検知したものは、情報セキュリティ管理委員会及びシステム管理者に遅滞なく報告しなければならない。

(2)システム管理者は、協力会社社員と連携し、報告されたセキュリティインシデントに応じ、策定した対応手順に従い、被害の特定、原因の分析を行う。なお、策定した対応手順に該当しないセキュリティインシデントの場合、情報セキュリティ管理委員会は、そのための実行責任者を任命し、対応組織を始動し、被害の特定、原因の分析を行う。

(3)特定したセキュリティインシデントの原因に基づく対応手順に則り、被害の拡散を防止し、被害箇所の原因の根絶、修復を行い、復旧をする。

(4)顧客及び取引先等利害関係者に影響の生じるセキュリティインシデントが発生した場合、情報セキュリティ管理委員会は、事実関係及び再発防止策等について、顧客及び取引先等利害関係者に速やかに報告することとする。

(5)セキュリティインシデントに関する情報は、実行責任者のもと、以下の情報について一元的に収集、管理、記録する。

・セキュリティインシデントの発生状況及び対応状況に関する情報

・顧客及び取引先等利害関係者の影響等に関する情報

・セキュリティインシデントの再発防止

(6)セキュリティインシデントの対応後、情報セキュリティ管理委員会は関係部門と連携の上、同様のセキュリティインシデントの再発防止、および対応手順の不備等について改善を行う。