4/2メール提出

情報セキュリティ対策の実施方法等について

令和　６年　４月　１日

環境省　大臣官房　環境影響評価課　御中

東京都千代田区麹町三丁目７番地６
株式会社プレック研究所
代表取締役社長　杉尾　大地

令和６年４月１日付けの契約の「令和６年度環境影響評価制度最適化調査業務」に係る情報セキュリティ対策とその実施方法及び管理体制について、下記のとおり届け出ます。

記

(1) 情報セキュリティ対策とその実施方法

環境省情報セキュリティポリシーを遵守し、情報セキュリティの確保のため別紙の対策を実施します。

(2) 情報セキュリティの管理体制

情報セキュリティ管理責任者			
氏　名	前澤　洋一		
所　属	総務部	役　職	専務取締役　部長
連絡先	TEL：03-5226-1101　　E-mail：csirt@prec.co.jp		

情報セキュリティ管理担当者			
氏　名	葭葉（辻阪）　吟子		
所　属	役員	役　職	取締役
連絡先	TEL：03-5226-1106　　E-mail：tsujisaka@prec.co.jp		

担当者等連絡先
部署名　　：企画開発部
責任者名　：宮元　亮祐
担当者名　：山本　浩一
ＴＥＬ　　：03-5226-1102
ＦＡＸ　　：03-5226-1113
E-mail　　：kikaku-k@prec.co.jp

情報セキュリティ規程

第1章　総則

第 1 条(目的)
　本規程は、第 4 条に定める情報セキュリティに関する基本方針に基づき、株式会社プレック研究所（以下、当社という。）が情報セキュリティを確保することにより、業務を継続的かつ効率的に遂行すること及び社会的信頼を獲得し、保持することを目的とする。

第 2 条(定義)
　本規程において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。
１.「役職員」とは、役員、職員、契約社員をいう。
２.「情報資産」とは、次にあげるものをいう。
(1)「情報」: 文書、図面及び電磁的記録をいう。
(2)「情報システム」:ハードウェア、ソフトウェア、ネットワーク及び記録媒体で構成されたものであって、その組み合わせにより、情報の記録、処理、通信等の業務処理を行うものをいう。

第 3 条(情報資産の対象範囲)
　本規程が対象とする情報資産は、次のとおりとする。
(1)当社における受託業務に関する情報。顧客より提供された情報及び業務において収集、作成した情報を含む
(2)当社の所有する知的財産及びそれに関する情報
(3)施設、設備機器及び情報システムに関する契約文書、取扱説明書、使用許諾証明書
(4)その他当社の運営に必要な文書などの情報

第2章　情報セキュリティに関する基本方針

第 4 条（情報セキュリティに関する基本方針）
１．当社は、個人情報保護法等の情報セキュリティに関する法令その他の規範を遵守する。
２．当社は、本規程に基づき、発注者、連携先、業務に関わる関係者などの信頼を損なうことのないよう、情報への不正アクセス、情報の紛失・改ざん・漏洩等の防止に向けた情報保護対策を講じる。
３．当社は保有する個人情報や、発注者、関係者から預かった機密情報等を適切に管理し、安全を確保する。
４．当社は情報セキュリティ対策を、技術の進歩や社会情勢等に適切に対応するよう継続的に見直し、最適化を図る。
５．当社の情報資産を利用する者は、情報セキュリティの重要性を認知し、この情報セキュリティ基本方針を遵守する責任を負うものとする。

第3章　組織体制

第 5 条(情報セキュリティ責任者)
１．代表取締役社長は、情報セキュリティ責任者を役員の中から 1 名指名する。
２．情報セキュリティ責任者は、当社における全ての情報資産の管理及び情報セキュリティ対策に関する決定権限及び責任を有する。

第 6 条(情報セキュリティ管理者)
１．各部署の情報セキュリティ管理者は、部署長をもってあてる。
２．プロジェクトの情報セキュリティ管理者は、管理技術者をもってあてる。
３．部署長は、受託業務に関する情報以外の所管する情報資産の適切な管理及び所管する職員の

教育訓練に関する権限及び責任を有する。
４．管理技術者は、当該管理技術者が管理する受託業務に関する情報の適切な管理に関する権限及び責任を有する。
５．情報セキュリティ管理者は、その所管する情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

第 7 条(情報システム管理者)
１．情報セキュリティ責任者は、情報システム管理者を指名する。
２．情報システム管理者は、情報システムにおける情報セキュリティに関する権限及び責任を有する。
４．情報システム管理者は、情報システムに対する侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

第 4 章 情報資産の分類と管理方法

第 8 条(情報資産の機密性による分類)
情報セキュリティ管理者は、その所管する情報資産について、以下の機密性に関する基準に従い機密性を有するものを特定し分類する。

○機密性を有する情報資産の分類
分類：機密性 3（取り扱い厳重注意）
分類基準：業務で取り扱う情報資産のうち、極秘文書に相当する機密性を有する情報資産
例）顧客から貸与された情報資産のうち取扱注意、禁複製等の指示あるもの
例）個人情報（生存する個人に関する情報であって、当該情報に含まれる記述により特定の個人を識別することができるもの）
例）その他、漏洩すると経営や業務に著しい支障が生じる情報資産

分類：機密性 2（取り扱い注意）
分類基準：極秘文書に相当する機密性は要しないが、これに準じた機密性を有する情報資産
例）顧客から貸与された情報資産（ただし取り扱い注意のものは除く）
例）顧客が特定される危険がある情報資産
例）公表前の見積り、入札等に関する情報資産
例）受託業務に関して作成した途中の文書のうち取り扱い注意のもの、
例）その他、漏洩すると経営や業務に支障が生じる情報資産

分類：機密性 1（社外秘）
分類基準：上記 2 分類に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産
例）受託業務に関して作成した途中の文書
例）公表前の広報資料
例）その他社内で作成する一般文書のうち社外に流出することが適切ではないもの

第 9 条(機密性分類に応じた情報資産の管理)
１．情報セキュリティ管理者は、その所管する情報資産のうち機密性を有するものについて、以下に示す分類ごとの取り扱い方針に沿って具体的な取り扱い方法を定め、必要に応じ取り扱いの制限を行う。また、情報資産が複製又は伝送された場合には、複製等された情報資産も第 8 条の分類に基づき管理しなければならない。
(1)機密性 3 に分類される情報資産の取り扱い
・原則として複製を行なってはならない。
・原則として持ち出しを禁止する。
・業務上必要最小限の者以外の者の閲覧やアクセスを厳重に制限する措置を講じなければな

らない。
例）紙及び記憶媒体の場合、施錠できるロッカーへの保管、電子化データの場合、アクセスの制限のかかったフォルダへの格納または記憶媒体に保存して施錠できるロッカーへの保管、パソコンのローカルディスクへの保存の禁止等）
・業務に必要な期間を過ぎた時点で速やかに他者に利用されない形で適切に廃棄もしくは消去、又は返却等の処置を講じなければならない。
例）紙の場合シュレッダー処理又は業者による溶融処理等、パソコン及び記憶媒体上のデータは消去ソフトの使用等電子データが読めなくなる処理の実施等）

(2)機密性 2 に分類される情報資産の取り扱い
・業務上やむをえず必要な場合を除いて、原則として複製を行なってはならない。
・極力持ち出さないこと。持ち出す場合には、情報セキュリティ管理者の許可を得た上で、管理に十分注意すること。
・業務上必要最小限の者以外の者の閲覧やアクセスを制限する措置を講じなければならない。
・業務に必要な期間を過ぎた時点で速やかに他者に利用されない形で適切に廃棄もしくは消去、又は返却等の処置を講じなければならない。

(3)機密性 1 に分類される情報資産の取り扱い
・複写・複製は、業務上必要最小限にとどめる。
・極力持ち出さないこと。持ち出す場合には、管理に十分注意すること。
・業務上認められた者以外の閲覧、変更を制限する措置を講なければならない。
・廃棄にあたっては、他者に利用されない形で適切に廃棄もしくは消去を行わなければならない。

３．情報資産を取得した者あるいは作成した者は、取得した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。
４．役職員は、業務上必要のない情報を取り扱ってはならない。

第 10 条(例外措置の許可)
１．情報セキュリティ管理者及び情報システム管理者は、情報セキュリティに関する規程を遵守することが困難な状況で、業務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないこと(以下「例外措置」)について合理的な理由がある場合には、情報セキュリティ責任者に許可を求めることができる。
２．情報セキュリティ責任者は、情報セキュリティ管理者あるいは情報システム管理者から例外措置の許可の求めがあった場合、例外措置を許可することができる。

第4章　ネットワーク及び電子化情報のセキュリティの確保

第 11 条(ネットワークへのアクセス管理)
１．情報システム管理者は、ネットワーク接続に係るユーザーアカウントの付与、ネットワーク上でのアクセス制限、機密性を有する情報資産へのアクセス状況のモニター等、ネットワークを介した情報資産へのアクセスを適切に管理できるための措置を講じなければならない。
２．各部署の情報セキュリティ管理者は、所管する部署の役職員及びアルバイト等のネットワークへのアクセスを適正に管理しなければならない。
３．役職員は、自己の管理するユーザアカウントに関し、次の各号の事項を遵守しなければならない。
(1)自己が利用しているユーザアカウントは、他人に利用させてはならない。
(2)自己の管理するパスワードに関し、適切に管理しなければならない。

第 12 条(ネットワークセキュリティの確保)
１．役職員は、業務に使用するパソコン等について、ネットワークセキュリティ確保のため、以下の事項を遵守しなければならない。なお、技術的な対策方法等については、情報システム管理者が別途手順書において具体的な方法を定める。
(1)パソコン、記憶媒体における情報漏洩を防止するための措置を講じる（暗号化、パスワードの設定等)。

(2)パソコン、記憶媒体を社外に持ち出す場合には、盗難、紛失等に十分注意する。
(3)ウィルス対策を適正に実行する。
(4)社内ネットワークへの個人パソコンの接続は原則禁止とし、特段の理由がある場合には情報システム管理者の許可を得る。
(5)ファイル交換ソフト、ファイル共有ソフト等、ファイルが流出する危険性のあるソフトウエアやサービスは原則使用してはならない。
(6)メールは発信する前に送信先アドレスを確認するなど、誤送信を防止する。
(7)グループメールを使用する際には、情報セキュリティ管理者に相談の上使用する。
(8)メールやアップロードサーバを介したデータの送信においては、パスワードの取り扱い等情報保護の措置を講じる。

第６章　人的セキュリティ対策

第 13 条(情報セキュリティ規程等の掲示)
　情報セキュリティ管理者は、役職員が常に情報セキュリティ規程等を閲覧できるように掲示しなければならない。

第 14 条(情報セキュリティに関する研修・訓練)
　情報セキュリティ責任者は、定期的に情報セキュリティ規程等の周知及び情報セキュリティに関する研修・訓練を実施しなければならない。

第 15 条(役職員の遵守事項)
１．役職員は、情報セキュリティ規程及び関連する手順書(以下「情報セキュリティ規程等」という)を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに所属の情報セキュリティ管理者に相談し、指示を仰がなければならない。
２．役職員は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

第 16 条(臨時職員への対応)
１．情報セキュリティ管理者は、臨時職員に対し、採用時に情報セキュリティに関する基本方針等について、必要な内容を理解させ、実施及び遵守させなければならない。
２．情報セキュリティ管理者は、臨時職員の採用の際、必要に応じ、情報セキュリティに関する基本方針等を遵守する旨の同意書への署名を求める。
３．情報セキュリティ管理者は、臨時職員に情報資産を取り扱う作業を行わせる場合において、情報資産の使用は必要最低限の範囲としなければならない。

第 17 条(外部委託事業者への対応)
　情報セキュリティ管理者は、情報資産を取り扱う業務を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティ規程等について、必要な内容を理解させ、実施及び遵守させなければならない。

第 18 条(技術的セキュリティ措置)
　情報システム責任者は、すべての情報資産を適切に管理するため、情報システム担当者に、以下の技術的セキュリティ措置を講じさせるものとする。
(1)ハードウェアの導入・調達・保守・管理
(2)ネットワークの維持・管理
(3)情報システム及び情報サービスの導入・調達・開発・管理
(4)セキュリティ侵害対策・違反防護策等の導入・維持・管理

第７章 情報セキュリティ規程等の遵守状況の確認

第 19 条(遵守状況の確認及び対処)
1．情報セキュリティ管理者は、情報セキュリティに関する基本方針等の遵守状況について適宜確認を行い、問題を認めた場合には、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。
2．情報セキュリティ責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

第 20 条(情報資産の取扱状況調査)
1．情報セキュリティ責任者は、不正な取扱いの調査のために、役職員が使用している書棚等の什器類、パソコン等の端末、記録媒体のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。
2．前項の調査を行った場合には、情報セキュリティ責任者はその結果を情報資産管理委員会に報告しなければならない。また、調査を行ったことを調査の対象となった役職員に報告しなければならない。

第 21 条(役職員の報告義務)
1．役職員は、情報セキュリティに関する基本方針等に対する違反行為を発見した場合、直ちに所属の情報セキュリティ管理者に報告を行わなければならない。
2．報告を受けた情報セキュリティ管理者は、その内容を情報セキュリティ責任者に報告しなければならない。
3．違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

第 22 条(例外措置の許可)
1．情報セキュリティ管理者及び情報システム管理者は、情報セキュリティに関する規程を遵守することが困難な状況で、業務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないこと(以下「例外措置」)について合理的な理由がある場合には、情報セキュリティ責任者に許可を求めることができる。
2．情報セキュリティ責任者は、情報セキュリティ管理者あるいは情報システム管理者から例外措置の許可の求めがあった場合、例外措置を許可することができる。

第 23 条(緊急時の例外措置)
情報セキュリティ管理者及び情報システム管理者は、業務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後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。

第 24 条(例外措置の記録の管理)
情報セキュリティ責任者は、例外措置の記録を適切に保管しなければならない。

第 8 章 事故及び侵害時の対応

第 25 条(緊急時対応計画の策定)
情報セキュリティ責任者は、情報セキュリティに関する事故、情報セキュリティ規程等の違反等により情報資産への侵害が発生した場合又は発生するおそれがある場合において、連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておかなければならない。

第 26 条(緊急時対応計画に盛り込むべき内容)
緊急時対応計画には、以下の内容を定めなければならない。
(1)関係者の連絡先
(2)発生した事案に係る報告すべき事項
(3)発生した事案への対応措置

(4)再発防止措置の策定

第 27 条(緊急時対応計画の見直し)
情報資産管理委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

第 9 章 法令遵守

第 28 条(法令遵守)
役職員は、職務の遂行において使用する情報資産を保護するために、次の各号の法令のほか関係法令を遵守し、これに従わなければならない。
(1)著作権法(昭和 45 年 5 月 6 日法律 48 号)
(2)不正アクセス行為の禁止等に関する法律(平成 11 年 8 月 13 日法律 128 号)
(3)個人情報の保護に関する法律(平成 15 年 5 月 30 日法律 57 号)
(4)その他、顧客の所在地における条例(東京都個人情報保護条例など)

第 10 章 違反時の対応等

第 29 条(懲戒処分)
情報セキュリティ規程等に違反した役職員及びその監督責任者は、その重大性、発生した事案の状況等に応じて、就業規則等による懲戒処分の対象とする。

第 11 章 本規程の見直し

第 30 条（情報セキュリティ規程等の見直し）
１．情報セキュリティ責任者は、定期的に又は必要に応じて、情報セキュリティ管理者に情報セキュリティ規程の実施状況について点検・評価を行わせ、その結果を踏まえ、状況セキュリティ規程等の見直し案を検討する。
２．本規程の見直しは、取締役会における審議・承認を経て代表取締役社長が通達する。

付　　則
この規程は、平成 25 年 10 月 1 日より実施する。