2020年4月１３日

セキュリティチェックリストの作成について

　今年度のデータマネジメントプランで設定済みのデータ単位、セキュリティレベル単位ごとに、レベルに対応するチェックリストを作成してください。セキュリティレベルやデータ単位の変更を必要とする場合は、データマネジメントプランの修正も行い、併せて提出してください。

提出されたチェックリストについて、改善が必要な場合は、情報セキュリティ専門委員会から、個別に連絡のうえアドバイスを行いますので、技術的相談等がありましたら、あわせてシートに記入してください。

セキュリティレベルの設定

セキュリティレベル３（高）：

要配慮個人情報や、住所・氏名等直ちに個人が識別できる情報を含むデータ、個人とIDの対応表等

セキュリティレベル２（標準）：

仮名化情報等、直ちに個人が特定できないデータ等

セキュリティレベル１（低）：

複数人をまとめた統計データ、個人に紐づけられていないデータ等

セキュリティレベル３（高）のデータに対する対策

セキュリティレベル３（高）のデータ（以下、レベル３データと呼ぶ）は、特定の個人が直ちに識別できるなど、漏洩時に個人に直接被害がおよぶ恐れがあるデータです。レベル３データはあらかじめ定めたセキュリティ管理エリア内で取り扱うものとします。

研究でデータ分析等の処理を行う場合は、原則としてセキュリティ管理エリア内で仮名化処理等によりレベル２データを作成し、そのレベル２データを用いるものとします。

レベル2データはセキュリティ管理エリア外で取り扱っても構いません。

　レベル３データを取り扱う場合、データ収集段階からデータ分析の段階まで、データの漏洩や不正アクセス対策を綿密に行ってください。

【組織的安全対策】

1. 情報管理責任者は、レベル３データを取り扱うセキュリティ管理エリア（以下、管理エリアと呼ぶ）を定めてください。また、レベル３データを管理エリア外に持ち出してはならないことをプロジェクト参加者に周知してください。
2. 情報管理責任者は、脆弱性対策等の安全対策の確認のため、データの収集、分析、保存等に使用する機器（以下、データを取り扱う機器と呼ぶ）の一覧を台帳等で管理してください。データを取り扱う機器には、サーバ、端末、センサ、ネットワーク機器等を含みます。
3. 情報管理責任者は、レベル３データを取り扱う者を定め、台帳等で管理してください。その際、レベル３データを取り扱う者は必要最小限としてください。
4. 情報管理責任者は、レベル３データを取り扱う端末を定め、台帳等で管理してください。また、定められた端末以外ではデータを取り扱ってはならないことをプロジェクト参加者に周知してください。
5. 情報管理責任者は、レベル３データを取り扱う者に対して、データの取り扱い等に関する教育プログラムを受講させ、修了したことを確認し、台帳等で受講状況を管理してください。
6. データ収集時には、管理エリア外から管理エリア内にレベル３データを移動させる必要がありますが、その手順や安全対策を定めてください。
	* USBメモリや外付けハードディスク等の記憶媒体で移動させる場合は、データの暗号化等の対策が必要です。
	* 管理エリア内のサーバへのデータのアップロード等、ネットワーク通信でデータを移動させる場合は、セキュリティが確保された専用回線を用いる場合を除き、通信路の暗号化等の対策が必要です。
7. 情報管理責任者は、レベル３データを取り扱う者に対して、原則としてレベル３データの複製は許可しないことを周知してください。また、レベル３データの複製を作成することが必要な場合は、情報管理責任者に許可を得なければならないことを周知してください。
8. 情報管理責任者は、レベル３データを取り扱う者に対して、レベル３データを取り扱う端末にデータを残してはいけないことを周知してください。
9. データに対して、仮名化処理や分析処理を行い新しいデータを作成する場合は、作成されたデータのセキュリティレベルを設定する必要があります。情報管理責任者は、データを取り扱う者に対して、データを処理して新しいデータを作成する場合はあらかじめ情報管理責任者と相談し、作成するデータのセキュリティレベルを定めなければならないことを周知してください。
10. 情報管理責任者は、レベル３データを取り扱う者に対して、レベル３データに対して仮名化処理や分析処理を行った結果、新しいデータのセキュリティレベルが２または１になったものとして管理エリア外に持ち出す場合は、情報管理責任者の許可を得る必要があることを周知してください。
11. 情報管理責任者は、レベル３データおよびレベル３データを処理して作成されたデータがどこに保存され管理されているかを把握し、台帳等で管理してください。

【物理的安全対策】

* 1. 管理エリアは常時施錠し、指定された者以外は立ち入れないよう入室制限を行ってください。可能な限り、ICカードや生体認証など、入室した者を特定できるようにしてください。
	2. やむを得ず管理エリアとしてサーバルーム等の専用の室が確保できない場合は、指定された者以外がデータを取り扱う機器への直接的な操作ができないよう、対策を講じてください。
	3. 管理エリア外に管理エリア内の機器へのアクセス端末を設置する場合は、鍵のかかる部屋に設置するなど、アクセス端末の設置場所について十分な安全対策を講じてください。
	4. データを取り扱うすべての機器について、紛失や盗難防止対策を講じてください。

【技術的安全対策】

1. レベル３データをサーバ等に保存する場合は、サーバの使用（直接ログインやWebインタフェースを介したアクセス等）について、可能な限り多要素認証によるユーザ認証を行ってください。
2. 可能な限り、レベル３データを取り扱う機器に対して、ユーザ認証等のアクセス制限を設定してください。
3. レベル３データを取り扱う機器にデータを取り扱う者のアカウントを設定している場合は、定められた者以外が機器を使用できないよう、アカウント管理を適切に実施してください。
4. 管理エリア内への不正侵入や盗難対策のため、監視カメラの設置を検討してください。また、いつ、誰がデータにアクセスしたかを追跡できるよう、可能な限り管理エリア内の機器やデータへのアクセスログを記録し、適切に保管してください。
5. 管理エリア外に管理エリア内の機器へのアクセス端末を設置する場合、アクセス端末は専用端末とし、外部ネットワークには接続しないでください。また、ユーザ認証等のアクセス制限や、通信路の暗号化等、十分な技術的安全対策を講じてください。
6. データを取り扱うすべての機器について、セキュリティ対策ソフトウェアの導入、適切なアクセス制限の設定、ソフトウェアの最新バージョンへのアップデートなどの脆弱性対策を実施してください。また、その実施手順を定めてください。
7. データを取り扱う機器間のネットワーク通信を行う場合、機器への不正アクセスを防止するため、ファイアウォール等により必要最小限の通信のみ許可するようアクセス制限を施してください。
8. データを取り扱う端末がネットワークに接続されている場合、外部からの不正アクセスや端末から外部への意図しないデータ漏洩を防止するため、ファイアウォール等により必要最小限の通信のみ許可するようアクセス制限を施してください。
9. データを取り扱う機器間のネットワーク通信を公衆回線（キャンパスネットワーク等を含む）を介して行う場合、通信路の暗号化等を行い、データの盗聴や改ざんを防止する対策を実施してください。

【データの破棄】

1. 研究や事業の期間終了後には、データ漏洩を防ぐため、データにアクセスできないよう適切にデータを破棄してください。
2. データを破棄したときは、破棄した事実を台帳等で管理してください。

【非常時の対策】

1. データの漏洩やパスワードの流出、管理エリア入室のための鍵やICカード紛失等の可能性が発生した場合、各機関で定められた対応方法に従って報告等を行うとともに、情報管理責任者に報告しなければならないことを周知してください。また、情報管理責任者は、iLDi統括情報管理責任者にすみやかに報告してください。

セキュリティレベル２（標準）のデータに対する対策

　セキュリティレベル２（標準）のデータ（以下、レベル２データと呼ぶ）は、直ちに特定個人の識別ができないデータであり、レベル３データに対して仮名化処理等を行ったデータ等が該当します。データ漏洩時のリスクはレベル３データよりは低いものの、研究データとして不正アクセスやデータ漏洩を防止する対策を行ってください。

【組織的安全対策】

1. 情報管理責任者は、脆弱性対策等の安全対策の確認のため、データの収集、分析、保存等に使用する機器（以下、データを取り扱う機器と呼ぶ）の一覧を台帳等で管理してください。データを取り扱う機器には、サーバ、端末、センサ、ネットワーク機器等を含みます。
2. 情報管理責任者は、レベル２データを取り扱う者を定め、台帳等で管理してください。
3. 情報管理責任者は、レベル２データを取り扱う端末を定め、台帳等で管理してください。また、定められた端末以外ではデータを取り扱ってはならないことをプロジェクト参加者に周知してください。
4. 情報管理責任者は、レベル２データを取り扱う者に対して、データの取り扱い等に関する教育プログラムを受講させ、修了したことを確認し、台帳等で受講状況を管理してください。

【物理的安全対策】

1. データを取り扱うすべての機器について、紛失や盗難防止対策を講じてください。

【技術的安全対策】

1. 可能な限り、レベル２データを取り扱う機器に対して、ユーザ認証等のアクセス制限を設定してください。
2. レベル２データを取り扱う機器にデータを取り扱う者のアカウントを設定している場合は、定められた者以外が機器を使用できないよう、アカウント管理を適切に実施してください。
3. データを取り扱うすべての機器について、セキュリティ対策ソフトウェアの導入、適切なアクセス制限の設定、ソフトウェアの最新バージョンへのアップデートなどの脆弱性対策を実施してください。また、その実施手順を定めてください。
4. データを取り扱う機器間のネットワーク通信を行う場合、機器への不正アクセスを防止するため、ファイアウォール等により必要最小限の通信のみ許可するようアクセス制限を施してください。
5. データを取り扱う端末がネットワークに接続されている場合、外部からの不正アクセスや端末から外部への意図しないデータ漏洩を防止するため、ファイアウォール等により必要最小限の通信のみ許可するようアクセス制限を施してください。
6. データを取り扱う機器間のネットワーク通信を公衆回線（キャンパスネットワーク等を含む）を介して行う場合、通信路の暗号化等を行い、データの盗聴や改ざんを防止する対策を実施してください。

【データの破棄】

1. 研究や事業の期間終了後には、データ漏洩を防ぐため、データにアクセスできないよう適切にデータを破棄してください。
2. データを破棄したときは、破棄した事実を台帳等で管理してください。

【非常時の対策】

1. データの漏洩やパスワードの流出等の可能性が発生した場合、各機関で定められた対応方法に従って報告等を行うとともに、情報管理責任者に報告しなければならないことを周知してください。また、情報管理責任者は、iLDi統括情報管理責任者にすみやかに報告してください。

