福島県情報通信ネットワークシステム
情報セキュリティ実施手順

【相手方名を入力】編

（令和３年度資材等放射性物質検査事業に係る労働者派遣業務）

令和〇〇年〇〇月〇〇日制定

農林水産部 林業振興課

目　　次

取扱厳重注意

第１　目的

この福島県情報通信ネットワークシステム情報セキュリティ実施手順・管理運営要綱 【情報セキュリティ管理者・利用者編】（以下、「実施手順」という。）は、福島県情報セキュリティポリシー（以下、「セキュリティポリシー」という。）第１部　情報セキュリティ基本方針（以下、「基本方針」という。）２及び第２部　情報セキュリティ対策基準（以下、「対策基準」という。）第２の７の規定された事項のうち、福島県情報通信ネットワークシステムにおける情報セキュリティ対策を実施するにあたって利用者が守るべき事項、組織体制、管理方法、遵守すべき事項等について具体的に定めるとともに、福島県電子社会推進実施要綱第６条に基づき、福島県情報通信ネットワークシステムの管理運営について定めるものとする。

第２　用語の定義

この実施手順において次に掲げる用語の定義は、当該各項に定めるところによる。

１	福島県情報通信ネットワークシステム	(以下、「情報通信ネットワークシステム」とする。)第1層のネットワークシステム、第2層のサーバー基盤システム、第3層のグループウェア、県庁ホームページ、県庁Webメールで構成されるシステムの総称
２	ネットワークシステム	情報通信ネットワークシステムのアクセス回線及び構内回線で構成されるネットワーク
３	サーバー基盤システム	情報通信ネットワークシステムのサーバ及び他情報システムのサーバーを接続するためのシステム並びに認証基盤及びセキュリティ基盤で構成されるシステム
４	グループウェア	ファイル共有などを行うためのシステム
５	県庁ホームページ	福島県の公式ホームページ
６	県庁Webメール	電子メールを使用するためのシステム
７	利用者	委託事業会社の被雇用者で、情報通信ネットワークシステムを利用する者をいう
８	アカウント	パソコン、グループウェア及びインターネットを利用するために登録された利用者の権限データ
９	ユーザーＩＤ	パソコン、グループウェア及びインターネットを利用するために登録された利用者の識別コード
10	パスワード	パソコン、グループウェア及びインターネット利用において情報システムが利用者を確認するための暗証コード
11	端末	パーソナルコンピュータ、タブレット、スマートフォン
12	端末等機器	情報通信ネットワークシステムに直接接続する場合がある　パーソナルコンピュータ、タブレット、スマートフォン、サーバ、複合機などIPアドレスを割り当てられた機器

第３　組織体制と職務及び責務

福島県情報通信ネットワークシステムの管理については、対策基準で定められたもののほか以下の組織体制とする。

１　情報セキュリティ管理者

(1) 支援を要請した(事業を委託する)県の各部局の課長、県議会事務局の課長、教育庁の課長、各委員（会）事務局の課長、各地方振興局の部（室）長、各出先機関の長を、その所管組織の情報セキュリティに関する権限及び責任を有する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、所管組織内における情報機器の適正な管理に努め、情報機器

が正常に機能するために必要な措置をとらなければならない。

2　情報化テクニカルリーダー（ＩＴＬ）

情報セキュリティ管理者を補佐し、情報セキュリティ対策及び情報リテラシー向上を推進するために各所属長が指名した者を情報化テクニカルリーダー（ＩＴＬ）とする。

3　情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）

(1) 情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）は、福島県企画調整部情報政策課長とする。

(2) 情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）の職務は、次に掲げるとおりとする。

ア 福島県情報通信ネットワークシステムの利用内容及び利用方法に関すること。

イ 福島県情報通信ネットワークシステムの運用管理に関すること。

ウ 利用者のユーザーID、アカウント名等の付与に関すること。

エ ユーザーID、アカウント名の管理に関すること。

オ 福島県情報通信ネットワークシステムに係る障害対策に関すること。

カ 福島県情報通信ネットワークシステムのセキュリティに関すること。

キ その他必要な事項に関すること。

4　情報システム管理者（接続ｼｽﾃﾑ）

情報通信ネットワークシステムに接続する情報システムの管理者。各情報システムを所管する各部局の課（室）長、議会事務局の課長、教育長の課長、各委員（会）事務局の課長、各振興局の部（室）長、各出先機関の長

5　情報システム担当者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）

情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）の指示に従い、情報通信ネットワークシステムの開発、設定の変更、運用、更新等の作業を行う者を情報システム担当者とする。

5　業務管理監督者

(1) 業務を受託した委託事業者の利用者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者を業務管理監督者とする。

(2) 業務管理監督者は、その契約期間において、所管する利用者に対して、実施手順に定められている事項を遵守させなければならない。

(3) 業務管理監督者は、次の内容について適切な対応を行い、若しくは利用者に行わせるようにしなければならない。

ア　福島県情報通信ネットワークシステムの利用において、情報セキュリティ対策について不明な点や、遵守することが困難な点があった場合、情報セキュリティ管理者又は情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）に相談すること。

イ　不正アクセスやコンピュータウィルス等、情報セキュリティに関する事案を認めた場合は、情報セキュリティ管理者に連絡すること。

ウ　福島県情報通信ネットワークシステムの異常及び故障を認めた場合は、情報セキュリティ管理者に連絡すること。

エ　業務管理監督者は、情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）又は情報セキュリティ管理者からウィルスチェックの案内が出された場合、速やかにウィルスチェックを実施すること。

オ　情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）又は情報セキュリティ管理者から修正プログラム適用の案内があった場合は速やかにこれを実施すること。

カ　情報資産の執務室外への持出しについて管理すること。なお、持ち出した情報資産をパソコン等で処理する場合には、そのパソコン等にファイル交換（共有）ソフト （Winny等）がインストールされていないことを確認すること。

キ　福島県情報通信ネットワークシステム及びこれに接続されている機器への私物等のパソコン、ＵＳＢメモリー、ハードディスク、テザリング機器の接続について管理すること。

ク　組織内の不正アクセス及びコンピュータウィルス等、情報セキュリティに関する事案を

把握すること。また、事案が認められた場合には、情報セキュリティ管理者と共同して詳細な調査を行うこと。

ケ　ソフトウェアのライセンス管理を適切に行うこと。

コ　情報セキュリティに関する情報を周知するための研修を組織内において行うこと。

6　利用者の責務

利用者は、次に掲げる責務を負う。

(1) 利用者は、実施手順に定められている事項を遵守するとともに、情報セキュリティ対策について不明な点や、遵守することが困難な点等が発生した場合には、速やかに業務管理監督者の指示を仰ぐこと。

(2) 不正アクセスやコンピュータウィルス等、情報セキュリティに関する事案を認めた場合は、業務管理監督者に報告すること。

(3) 福島県情報通信ネットワークシステムの異常及び故障を認めた場合は、業務管理監督者に報告すること。

(4) 業務管理監督者の許可を得ず、情報資産を執務室外に持ち出さないこと。

(5) 異動、退職等により業務を離れる場合には、知り得た情報を秘匿すること。

(6) ユーザーID及びパスワードは適切に管理すること。

(7) 個人情報の保護に十分配慮するとともに、福島県情報通信ネットワークシステムに登録された情報は善良に管理すること。

(8) 情報の改ざん、毀損、滅失及び虚偽の情報の提供並びに福島県情報通信ネットワークシステムの改造を行わないこと。

(9) コンピュータウィルス感染防止のため、ウィルス検出ソフトウェアを端末機に導入するとともに、システムを破壊する恐れのあるプログラムの登録や、出所不明のソフトウェア等を利用しないこと。

(10) 利用者は、業務管理監督者からウィルスチェックの指示が出された場合、速やかにウィルスチェックを実施すること。

(11) 利用者は、ウィルスチェックの予約検索の実施日時（毎週木曜日11時から）に出勤している場合は、パソコンにログインすること。

(12) 利用者は、業務管理監督者から修正プログラム適用の指示が出された場合、速やかにこれを適応すること。

(13) 著作権法で保護されているシステム、プログラム及びデータ等の不正登録を行わないこと。

(14) 他の利用者又は第三者の名誉を傷つけ、不利益をもたらす利用を行わないこと。

(15) 端末機が不正に利用されることがないよう、これを防止すること。

(16) 情報資産については、外部の者に見られないよう細心の注意を払うこと。

(17) 住民の個人情報、特定の職員にしか扱えない情報については、フォルダを別にする、ファイルにパスワードを付与する等の情報漏えい等に関する措置を講じること。

(18) 情報システムに入力される電子データ及び出力結果は正確であることをその都度確認すること。

(19) 日常から、クリアデスク、クリアスクリーン等情報資産の物理的な盗難防止対策を行うこと。

(20) 福島県情報通信ネットワークシステムに接続されたパソコン等の機器は業務に必要な範囲で使用するものとし、業務目的以外で使用しないこと。

(21) 業務管理監督者の許可を得ず、福島県情報通信ネットワークシステム及びそれに接続されている機器に、私物等のパソコン、USBメモリー、ハードディスク等を接続しないこと。

(22) ぜい弱性のあるソフトウェア及びサポート期間が終了したソフトウェアは、速やかに更新又は削除すること。

(23) 業務管理監督者の許可を得た場合であっても、ファイル交換（共有）ソフト（Winny等）

がインストールされているパソコン等では業務に関する情報資産を扱わないこと。

(24) 福島県情報通信ネットワークシステムに接続されている機器をテザリングにより、県ネットワーク以外のネットワークに接続しないこと。

第４　情報システムの管理

１　情報システムの監視

(1) 情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）は、福島県情報通信ネットワークシステムの正常な稼働を確保し、かつ、情報セキュリティに関する事案を検知するため、福島県情報通信ネットワークシステムについて、機器の作動状況の監視及び通信記録の内容確認等の必要な管理行為を行うものとする。また、必要と認める場合には、福島県情報通信ネットワークシステムに接続された各端末等機器に蓄積されたデータ、履歴等を要求することができるものとする。

(2) 情報システム管理者(情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ)は、情報セキュリティに関する事案について、福島県情報通信ネットワークシステムに接続された機器の操作を行った利用者からの聞取り等の調査をすることができるものとする。

(3) 情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）は、必要と認める場合には、業務管理監督者に対し、問題点の改善等を求めることができるものとし、改善を求められた業務管理監督者は速やかに改善を行うものとする。

２　端末へのソフトウェアの導入並びに機器の増設及び交換

(1) 利用者が業務上の必要からソフトウェアを端末に導入する場合、又は機器の増設又は交換を行う場合、又は登録を必要としアカウントが発行されるクラウドサービス（以下、「クラウドサービス」という。）を利用する場合は、「端末機に関する変更申請書（第４号様式）」により業務管理監督者の許可を得なければならない。

ただし、次のソフトウェア（メーカーサポートが終了しているバージョンを除く）を導入する場合には、業務管理監督者の許可は不要とする。

（ア）Adobe Reader DC

（イ）FFFTP（最新版であること）

（ウ）一太郎ビューア(最新版であること)

(エ)パスワード付圧縮ファイルを作成するための7-zip(最新版であること。)

（オ）「パソコン管理（第2号様式）パソコン・ソフトウェア等導入協議書」または「（様式第5号）ソフトウェア・機器使用協議書」により情報システム管理者と協議済みのソフトウェア

（カ）ネットワーク管理者（CISO補佐）又は情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）から導入指示のあったソフトウェア

（キ）業務に使用する情報システムで、その情報システムを所管する情報システム管理者（接続ｼｽﾃﾑ）が、「福島県電子社会推進実施要綱第８条」で定める情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）調達協議を経ているソフトウェア

（ク）業務で国が設置したサービスを利用する場合に利用が必須のソフトウェア

（ケ）ISO/IEC 15408(Common Criteria)等の国際基準に基づくセキュリティ要件を満たしているか同等程度のセキュリテイ要件を満たしている複合機プリンタのドライバ

（コ）その他情報政策課の定める「協議不要ソフトウェア一覧」に掲載されているもの

(2) 導入禁止ソフトウェア

以下のソフトウェアは、利用を禁止する。また、すでにインストールされているものを発見した場合は、速やかに削除すること。

（ア）正規配布方法以外（作者又はメーカーの許可を得ない　配布）で取得したソフトウェ

ア（改ざんされウィルス等が含まれている場合があるため。）

（イ）(1)以外の圧縮展開ソフトウェア（代表的な圧縮展開ソフトウェアはMicrosoft社がWindows用に提供しており、これ以外を用いることは安全性について判断が難しいため。）

（ウ）(1)に該当するソフトウェアに付属する以外のかな漢字　変換ソフトウェア(Windows標準のかな漢字変換ソフトウェア(MSが提供しているIME等)は十分な機能を持っており、これ以外を用いることは、安全性について判断が難しいため。）

（エ）(1)以外で利用が必須のソフトウェア以外のJava実行環境(Java関連ソフトウェアは、脆弱性管理が難しく、また、攻撃対象としてよく使用されるため。JRE、JavaSE)

（オ）P2P技術を用いたファイル交換ソフト(winny等)

（カ）(1)以外でインターネットエクスプローラ用の拡張用アドイン(Yahooツールバー、google Toolbar、JWord等、業務システムの不具合の原因になるため。）

（キ）脆弱性のあるソフトウェア、脆弱性情報の確認方法が不明確なソフトウェア（配布ホームページ等に、脆弱性の修正情報がない。）及びサポート期間が終了したソフトウェア。

（ク）無償の音声再生ソフトウェア、変換ソフトウェア、動画作成・編集ソフトウェア（パソコンにプレインストールされている、またはDVD書き込みを内に添付されたソフトウェアを除く。）（理由：著作権法的場問題があること及び情報漏えいリスクがあるため）

（ケ）著作権法で保護されているソフトウェアで、その保護の範囲を超えて不正に利用される恐れのあるもの（フリーソフト等で正式に配布されているものであっても、その内部で使われている部品等に関し、著作権上の未解決の係争が生じているものを含む。

(3) 利用者は、クラウドサービスを利用する場合、２要素認証等のセキュリティ強化機能が提供されているときは、これを有効にしなければならない。

(4) 業務管理監督者は、クラウドサービスのアカウントを「クラウドサービス利用管理簿（参考様式）」により管理しなければならない。

３　使用するソフトウェアのバージョン

オペレーテングシステム(以下、「ＯＳ」という）及びブラウザソフトを使用する場合は、以下のバージョンとする。

(1) ＯＳ

ア　使用を認めるOSは次のとおりとする。

・Windows10 Professhional（64bit版）
・Windows10 Enterprise E3（64bit版）
・Windows10 Enterprise E5（64bit版）

イ　業務管理監督者は、ア以外のOSを使用する必要がある場合には、事前に情報セキュリティ管理者及び情報システム管理者に「（第５号様式）ソフトウェア・機器使用協議書」により協議し同意を得なければならない。

ウ　業務管理監督者は、ア以外のＯＳを使用する場合は、常にセキュリティ情報に注意し、修正プログラムが公表された場合は速やかに適用するものとする。

エ　情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）は、同意を得ずにア以外のOSを使用した者のネットワーク利用を停止することができる。

(2) ブラウザソフト

ア　Internet　Explorer Ver11、GoogleChromeまたはFirefoxを使用するものとする。

イ　業務管理監督者は、ア以外を使用する必要があるものは、情報セキュリティ管理者及び情報システム管理者情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）に「（第５号様式）ソフトウェア・機器使用協議書」により協議し､同意を得るものとする。

ウ　業務管理監督者は、イを使用する場合は、常にセキュリティ情報に注意し、修正プログラムが公表された場合は速やかに適用するものとする。

4　配線

(1) 業務管理監督者は、主要な箇所の配線の変更や追加が必要な場合は、情報セキュリティ管理者及び情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）と協議をするものとする。

(2) 情報政策課が管理するＨＵＢからパソコン等の情報機器までのＬＡＮケーブルの配線の変更や追加は、所管の情報セキュリティ管理者が行うものとする。

5　ユーザーＩＤ及びパスワードの管理

(1) ユーザーＩＤ及びパスワードの入力後、福島県情報通信ネットワークシステムやクラウドサービスが利用可能な状態で端末を放置してはならない。

(2) 利用者間でユーザーＩＤ、パスワードを共有してはならない。

(3) 指定されたアカウント名を使用するとともにパスワードの設定を行い、それらを適切に管理しなければならない。

(4) パスワードの漏洩、不正利用の防止に努めなければならない。

(5) パスワードは自分の名前を用いたり、ユーザーＩＤや、誕生日等と同じにするなど容易に推測できるものは避けなければならない。

(6) パスワードは秘密にし、パスワードの照会には一切応じてはならない。

(7) パスワードを記録したメモ等は厳重に管理し、本人以外は参照できないようにしなければならない。

(8) パスワードは８文字以上とし、文字列は想像しにくいものとしなければならない。

(11) パスワードが漏洩したおそれがある場合には、パスワードを速やかに変更しなければならない。

(12) 複数のアカウント及びユーザーＩＤを持つ利用者は、パスワードをアカウント、ユーザーＩＤ間で共有してはならない。

(13) 端末にパスワードを記憶させてはならない。

6　情報資産の移転

利用者は、パーソナルコンピュータ等の情報資産を移転する場合は、不要なデータは削除しなければならない。

7　情報資産の廃棄

(1) 利用者は、業務で使用した情報機器、記憶装置等の重要な情報資産の廃棄するときは、業務管理監督者の許可を得ることとし、行った処理について、「（第３号様式）パソコン・記録媒体処分申請確認書」により日時、利用者及び処理内容を記録しなければならない。

(2) 利用者は、情報資産が不要となった場合は、磁気破壊または物理的破壊を行い記録媒体から情報を復元できないようにしたうえで廃棄しなければならない。

(3) 情報機器、記憶装置等の廃棄については、関連法に従い適正に廃棄処理を行わなければならない。

第５　コンピュータウィルス対策

１　情報システム管理者は、ウィルスチェックプログラムの予約検索機能により、毎週１回端末のウィルスチェックを行う（利用者はウィルスチェックを行っている間、端末の電源を切断しないこと）。

２　情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）は、ウィルスチェックプログラムの入っていない端末及びウィルスチェックプログラムを最新のものに保っていない端末の利用を停止することができる。

３　情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）は、インターネットとの接続点にウィルスチェックサーバを設置し、インターネットとの間で送信・受信されるデータのウィルスチェックを行い、コンピュータウィルスの侵入及び拡散を防止する。

取扱厳重注意

第６　障害発生時の措置

１　利用者は、福島県情報通信ネットワークシステムの障害を発見した場合には、業務管理監督者に報告するものとする。

２　報告を受けた業務管理監督者は、速やかに情報セキュリティ管理者及び情報システム管理者（情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑ）に連絡するものとする。

３　ソフトウェアの誤作動時に、福島県情報通信ネットワークに関係するソフトウェアを除去する場合には、第１項及び第２項に準じて取扱うものとする

第７　運用における情報セキュリティ対策

業務管理監督者は、実施手順が遵守されているかどうかについて、また、問題が発生していないかについて常に確認を行い、問題が発生していた場合には速やかに情報セキュリティ管理者に連絡しなければならない。

第８　ネットワークシステムへの情報機器の接続

１　業務管理監督者は、ネットワークシステムにパーソナルコンピュータ等の機器を新たに接続する場合には、「（第５号様式）ソフトウェア・機器使用協議書」により、情報セキュリティ管理者に届け出るものとする。

第９　ネットワーク利用の注意

１　ネットワークシステムで利用できるプロトコルはＴＣＰ／ＩＰに代表されるインターネット主要プロトコルのみである。

２　無線ネットワーク装置は、盗聴等の情報セキュリティ上の問題があるため、情報システム管理者が許可したもの以外は接続してはならない。

３　情報機器におけるＩＰアドレス等は指定されているものを使用し、情報システム管理者が許可した場合以外はＩＰアドレスの自動取得（ＤＨＣＰ）等に設定してはならない。

第10　コンテンツ・フィルタリング機能等

１　情報システム管理者は、コンテンツ・フィルタリング機能により暴力・非合法等の不適切サイトは表示しないものとする。

２　業務管理監督者は、業務上、不適切なサイトを閲覧する必要がある場合は、「（第２０号様式）コンテンツ・フィルタリング適用除外申請書」により情報セキュリティ管理者及び情報システム管理者に申請するものとする。

３　適切なサイトと思われるにも関わらず、コンテンツ・フィルタリング機能により表示されない場合は、情報セキュリティ管理者及び情報システム管理者にＵＲＬを連絡するものとする。情報システム管理者は、連絡を受けたURLを審査し適切と認めた場合は、コンテンツ・フィルタリングから適用除外の設定を行うものとする。

第11　その他

この実施手順に定めるもののほか、情報セキュリティ対策に関して必要な事項は、委託事業者と県が協議して定めるものとする。

附　則

この実施手順は、令和○○年○○月○○日から施行する。