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のための情報セキュリティ１１＋１か条（雛形）

福島県企画調整部情報政策課　（令和３年度版）

コンピュータやネットワークは、私たちの業務の効率化に役立っていますが、誤った使い方により、瞬時に大量の個人情報や機密情報が流出してしまう危険性も持ち合わせています。

福島県では情報セキュリティを確保するための基本方針である「福島県情報セキュリティポリシー」や関連する諸規程を整備しておりますが、〇〇〇〇も県職員と同様、これらの諸規程を守らなければなりません。

情報セキュリティ１１＋１か条では、県から貸与されたパソコンまたは県のネットワークを使用するにあたって、情報セキュリティ対策として、最低限守らなければいけない事項をわかりやすくまとめましたので、セキュリティ対策についてチェックしてください。

（※番号は「資料」を参照してください）

①　情報資産を持ち出さない。

パソコン、USB メモリー、フロッピーディスク、ＣＤ-Ｒ等情報資産を、無断で執務室外に持ち出してはいけません。

また、業務に関する情報（写真や感想を含む）を、個人のブログ、Twitter、フェイスブックなどに投稿することや、Dropbox、グーグルドライブなどのクラウドサービス上に保存すること、また、私物のスマートフォンや自宅パソコンにメールを送ることも情報資産の持ち出しとなります。

②　私物のパソコン、通信機器、記録媒体等を使用しない。

情報漏えいの９割が職員や委託業者等の内部の者による過失又は故意によるものと言われています。

私物のパソコンを許可なく県のネットワークに接続してはいけません。

私物の各種記録媒体等（USB メモリー、外付けハードディスク、デジタルカメラ、スマートフォン、携帯電話、携帯音楽プレイヤー等）を許可なく業務用パソコンに接続してはいけません。

私物のソフトウェアを業務用パソコンにインストールしてはいけません。私物スマートフォン等の通信機器を使用し、業務用パソコンをインターネットに接続する「テザリング（※）」も行ってはいけません。

※テザリング：スマートフォンなどの単体で通信可能な端末を経由してパソコン等をインターネットへ接続すること。福島県では、管理外のネットワークに職場内のパソコンを接続することは情報セキュリティ上大きな脅威であることから、テザリング利用を禁止している。

業務目的以外でパソコンを利用しない。

パソコンやインターネットを業務目的以外で使用してはいけません。業務目的外の使用は、コンピュータウイルスに感染する危険性が増大する等、セキュリティ上様々な問題を引き起こす可能性があります。昼休みや勤務時間外でも同様です。

最近の傾向としてインターネットを閲覧しているうちに、不正なウイルス等をダウンロードさせる「水飲み場攻撃」が増えています。

④　USB メモリーは適切に使用する。

USB メモリーは、紛失や盗難、コンピュータウイルスの感染などセキュリティ事故の危険性の高い記録媒体ですので、注意が必要です。

委託業務で使用する場合は、業務管理監督者から委託元の県機関へ申請し、許可を得た上で、危険性を十分に認識し、むやみに持ち歩かない、不使用時にはパソコンに接続したまま放置しない、使用時には暗号化やパスワードによる保護を行う（※１）、ウイルスチェックを実行する等のセキュリティ対策を行ってください。（※２）

⑤　席を離れる場合は、ノートパソコンの蓋を閉じる。

のぞき見や不正利用による情報漏えいを防止するため、離席時にはパソコンの蓋を閉じたりロック機能（ウィンドウズキー＋Ｌキー）を利用しましょう。また、スクリーンセーバーの待ち時間を３分以下に設定してください。（デスクトップ上で右クリックし、個人設定から設定できます。）

⑥　ウイルス対策ソフトウェアを有効に機能させる。

県のネットワークに接続するパソコン又は県から貸与されたパソコンを使用するためには、指定されたウイルス対策ソフトウェア（ウイルスバスターコーポレートエディション）をインストールし、パターンファイルを常に最新にする必要があります。

また、木曜日の 11 時からウイルスの予約検索が起動するので、この時刻にはパソコンは起動した状態にしておいてください。

⑦　パスワードを適正に管理する。

各種システムのパスワードは適切に管理してください。

- 初期設定のままでは使用しない
- 十分な長さ（８文字以上）とする
- アルファベット大小文字、数字、記号等の３種以上を組み合せた文字列が有効
- 他人から推測されにくいものにする（ユーザーID や誕生日等と同じものにしない）
- パスワードを書いたメモを目につくところに放置しない

⑧ メールの誤送信、メールからの情報漏洩、不審メールに注意する。

複数の相手方に送信する場合には、To、Cc、Bccの使い分け（※３）が誤っていないか、メール送信前にもう一度確認してください。

重要な情報を送信する場合には、メール本文には記載せず、パスワードを設定した添付ファイルに記載して送信してください。（※２）

不審メール（差出人に心当たりがない。タイトルや本文の内容がおかしい等）が届いたら、添付ファイルは開かない、本文中のURLはクリックしない、等を徹底してください。

最近では、業務に関係する内容を装い添付ファイルやリンクを開かせる「標的型攻撃」や、やりとりを何度か行い相手を信用させた後に不正プログラムを送る「やりとり型攻撃」等、不審メールを送る手法は巧妙化し高度化しています。

⑨　セキュリティ事故が起こった場合の対応手順を理解し、実践できるようにする。

意図しないパソコンの動作やセキュリティ事故が起こった場合は、速やかに業務管理監督者へ報告してください。併せて、業務管理監督者は〇〇（報告すべき県機関）へ連絡してください。

コンピュータウイルスに感染した場合（※４）は、まず該当パソコンの LAN ケーブルを抜いていいか直ぐに指示を受けてください。LAN ケーブルが抜かれたことを検知して巧妙に感染の痕跡を消してしまうケースがあります。

⑩　修正プログラムを適用する。

〇〇（委託元の県機関）から修正プログラムの適用について情報提供があった場合は、速やかに、業務管理監督者と相談してください。業務管理監督者は修正プログラムの適用について速やかに検討してください。

⑪　パソコンの設定、構成等の変更、アプリケーションのインストール、クラウドサービスの利用が必要になった場合は、業務管理監督者に相談する。

パソコンの設定、構成等の変更、アプリケーションのインストール、メールやインタ

ーネットストレージ等のクラウドサービスの利用が必要になった場合は、業務管理監督者に相談してください。業務管理監督者は、IP アドレスの変更等の軽微な場合を除いて〇〇（委託元の県機関）へ申請し、許可を得てください。

★　情報セキュリティ対策の協議について。

情報セキュリティ対策は、計画、実行、チェック、見直しを繰り返し行っていくことが必要となります。新たな対策が必要になるごとに業務管理監督者と県で密接に協議を行い、情報セキュリティの強化を行っていきますので、ご協力をお願いします。

（資料）

※１　ファイルにパスワードを設定する方法

インターネットで個人情報などの重要な情報を送信する場合には、上記の送信先等を確認した上で、暗号化やパスワードによる保護をして送信してください。

（１）7-Zip を使って圧縮フォルダを暗号化する。

（２）Ｗｏｒｄ、Ｅｘｃｅｌ【バージョンが 2013、2016 の例】

①メニューバーの「ファイル(F)」をクリックする。

②「情報」→Word は「文書の保護」、Excel は「ブックの保護」をクリックする。

③「パスワードを使用して暗号化」をクリックして、設定画面からパスワードを入力し「OK」ボタンを押すとパスワードが有効になる。

（３）一太郎

①　文書等作成中に、メニューバーの「ファイル(F)」をクリックする。

②　メニューコマンド「セキュリティ(R)」をクリックする。

③　セキュリティウインドが表示されるので、文書閲覧の制限、文書編集の制限等を考慮してパスワードを設定する。

④　ファイルを保存するとパスワードが有効になる。

※２　USB メモリー等を使用する際のウイルス手動検索方法

（１）LAN ケーブルを抜く。

（２）スタート→すべてのプログラム→ウイルスバスターCorp.クライアント→ウイルスバスターCorp.クライアントを開く。

（３）「手動検索」タブを開き、ウイルスチェックしたいドライブにチェックを入れて「検索」ボタンを押す。

（４）「セキュリティリスクが検出されませんでした」と表示されれば OK。

「〇個の不正プログラムが検出されました」と表示されたら LAN ケーブルを挿す前に情報政策課へ連絡する。

※３　メール送信時のＴｏ、Ｃｃ、Ｂｃｃの使い分け

（１）Ｔｏ（送信先）

送信先を入力します。複数のメールアドレスを入力でき、送信相手全員に同じ内容を連絡する場合に使用します。（会議の開催通知等）

To 欄に入力された全てのメールアドレスが、受信側の全員のメールに表示されます。

（２）Ｃｃ（同報）

To で入力した送信先以外にも同じ内容のメールを送信する場合に使用します。

To との使い分けは、To は本人への連絡、Cc は報告や情報提供のための写しの送付となります。

Cc 欄に入力した全てのメールアドレスが、受信側の全員のメールに表示されます。

（３）Ｂｃｃ（隠し同報）

多数の送信先に一斉同報メールを送信する場合や、送信先のメールアドレスをメール上に表示したくない場合（メールマガジン等）に使用します。

Bcc 欄に入力したメールアドレスは、受信側のメールには表示されません。

（※なお、宛先の入力が Bcc 欄だけの状態では送信できないので、Ｃｃ欄に送信者のアドレスを入力し、Ｔｏ欄は空欄のまま送信して下さい。）

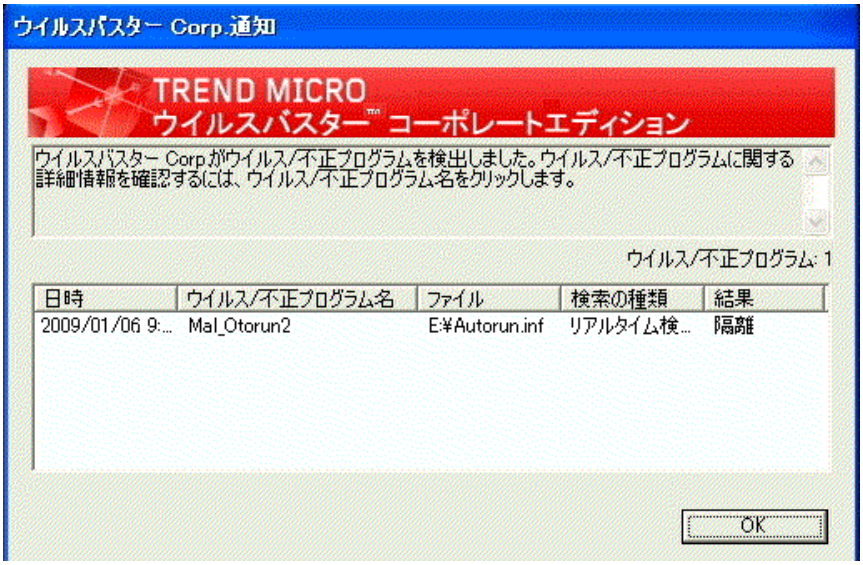
（注意）

メールアドレスは個人情報ですので、外部の複数の相手方へ送信する場合は、原則として Bcc を使用します。

送信先が５件を超える場合、注意喚起が表示されますので確認の上送信してください。

※４　ウイルスバスターにおけるウイルス検出画面

ウイルスバスターが、ウイルスを検出した場合、以下のような通知画面が表示されます。「OK」をクリックすると、通知画面は閉じてしまうので、以下のような画面が表示された場合、直ぐに業務管理監督者へ連絡してください。併せて、業務管理監督者は○○（報告すべき県機関）へ連絡してください。



セキュリティポリシー及び関連規程

○　**福島県情報セキュリティポリシー（第１部）情報セキュリティ基本方針**
　情報セキュリティを確保するために福島県が組織的、計画的に取り組むための統一的な基本方針。

○　**情報セキュリティポリシー（第２部）情報セキュリティ対策基準**
　セキュリティポリシーに基づき、情報セキュリティ対策を実施するにあたっての組織体制、管理方法、遵守すべき事項及び判断基準等を定めたもの。

○　**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**
　【情報システム以外の委託事業者編】
　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ついて定めたもの。

福島県情報通信ネットワークシステム

県の基幹ネットワークである県情報通信ネットワークシステムは、情報セキュリティを確保するため、①ＬGWAN（※）系ネットワーク、②インターネット利用仮想ネットワーク、③個人番号利用事務ネットワークの３つに分離されており、それぞれ次の場合に使用します。

① ＬGWAN系ネットワーク：所属の共有サーバやグループウェアの利用、国の機関や市町村等との情報のやりとりを行うネットワーク
② インターネット利用仮想ネットワーク：仮想化環境共通基盤を使用してインターネットを利用するネットワーク
③ 個人番号利用事務ネットワーク：「行政手続における特定の個人を識別するための番号の利用等に関する法律」に基づき、特定個人情報（マイナンバー＋個人情報）の提供・取得に用いられるネットワーク（一部の所属のみ利用可能）

①と②は１人１台のグループウェア端末から利用できますが、②のネットワークからグループウェア端末へデータを移行する場合には、無害化処理等を行う必要があります（テキストデータのコピー＆ペーストについては、無害化処理等は不要です）。
なお、特定個人情報等の機密性の高い情報は、②では取り扱うことはできません。

※　地方公共団体間のコミュニケーションの円滑化、情報の共有による情報の高度利用を図ることを目的とし、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク）