

## 1人1台タブレットの配付について

## ○ 配付物

- ・タブレット (iPad) 本体 ※SIMカードなし
- ・充電器、タブレットカバー
- ・1人1台タブレットの配付について (本紙)
- ・オンライン会議用マニュアル (Webex meetings、Zoom)
- ・職員のための情報セキュリティ5か条
- ・パスワード等について

## ○ 設定済のもの

- ・iPadを使用するための基本設定
- ・議事堂内のWi-Fi環境の設定
- ・AppleID (icloud.comメール) の設定
- ・Webex meetings 及び Zoom (オンライン会議) アプリのインストール

## ○ 注意事項

- ・タブレットは県貸与物品ですので、その管理については十分な注意を払ってください。また、別添の「職員のための情報セキュリティ5か条」を参考にしてください。
- ・タブレットを破損、紛失、盗難等された場合や、パスコード等をお忘れになった場合はすぐに議会事務局までご連絡ください。
- ・議事堂内ではインターネット等の利用が可能です。議事堂外でのインターネット等の使用については、別途Wi-Fi環境等の設定が必要となります。その際はお手数ですが各自で設定をお願いします。
- ・周辺機器 (Wi-Fi環境整備機器、キーボード等) については各自でご用意ください。
- ・Word、Excel、PowerPoint、PDFの各ファイルについては、閲覧のみ可能となります。
- ・新たなアプリのインストールについては当面されないようにお願いします。今後の取扱いについては、プロジェクト会議等で検討の予定です。
- ・apple IDやメールアドレス (xxx@icloud.com) は変更しないようにお願いします。
- ・タブレットのメールアドレスについては公表せず、議会事務局や執行部との連絡に使用するために設定していますので、ご了承ください。
- ・パスコード (電源を立ち上げる際の6ケタのコード) やパスワード等については事務局で設定していますが、セキュリティ確保のため、ご自身で変更をお願いします。また、変更後のパスワード等は必ず議会事務局までご連絡いただくとともに、各自で管理をお願いします。(指紋認証はされないようにお願いします。)
- ・今後、設置が予定される議会スマート化に関するプロジェクト会議において、タブレットの使用方法等が新たに示された場合は、それに従ってご使用ください。

県の行政情報にはプライバシー性が非常に高い情報が数多く存在します。これらの情報が漏えいした場合、損害賠償を請求されたり、行政事務の運営に影響したりする可能性があります。同時に、個人としても懲戒処分の対象となる可能性があります。情報セキュリティ事故は身近なリスクであることを認識の上、適切な対応を実施してください。

### ◇第1条 パスワードは適切に管理すること

パスワードが他人に知られると情報システムへ侵入されるリスクがあります。

- ・パスワードは他人に知られないように管理すること
- ・パスワードを設定する際は最低8文字以上、アルファベット・数字等を混ぜた組み合わせにすること
- ・パスワードは最低年に1度は変更すること、また、初期パスワードはすぐに変更すること

### ◇第2条 職場のパソコンは適切に管理すること

職場のパソコンを庁舎外へ持ち出すときは所属長の決裁が必要です。

ソフトウェアのインストールにもウイルス感染などの危険性があります。

- ・勝手に庁舎外へ持ち出さないこと、紛失したり、盗難の被害にあわないよう適切に管理すること
- ・パソコンに重要な業務データ（重要性分類特A）を保存しないこと
- ・職場のパソコンを行政WAN等の決められた業務ネットワーク以外に繋がらないこと
- ・ウイルス対策ソフトの定義ファイルの更新やセキュリティパッチの適用はすぐに対応すること
- ・ウイルスを検出したらすぐにLANケーブルを抜き、ウイルス対策ソフトによる処理状況を確認すること
- ・私物のパソコンを行政WAN等の業務ネットワークに繋がらないこと
- ・ソフトウェアの利用時は必ずライセンスを確認すること（不正コピー厳禁）
- ・勝手にソフトウェアをインストールしないこと

### ◇第3条 業務データは慎重に取り扱うこと

業務データの庁舎外への持ち出しには紛失したり盗難にあうリスクが伴います。

重要な業務データは私物パソコンでは原則扱ってはいけません。

- ・重要な業務データ（重要性分類B以上）を勝手に庁舎外に持ち出さないこと
- ・重要な業務データ（重要性分類A以上）を勝手に私物のパソコン等で扱わないこと
- ・紛失のおそれがあるので、USBメモリーやSDカード等の使用は必要最小限にすること
- ・USBメモリーなどでデータの受け渡しを行う場合は、必ず事前にウイルスチェックをすること
- ・ハードディスクおよびCDなどの媒体を処分する際は、物理的に破壊するなど適切に処理すること

### ◇第4条 インターネットメールは慎重に使用すること

誤送信による情報漏えいや、データを傍受されるリスクなどがあります。

メール受信の際も、迷惑メールからウイルス感染する危険性があります。

- ・インターネットメールで個人情報（重要性分類特A）を送付しないこと（原則禁止）
- ・重要な業務データ（重要性分類B以上）を送付するときはパスワード設定等の対策を行うこと
- ・送信前に宛先に間違いがないか必ず確認すること
- ・不審なメールの添付ファイルの開封や、URLのクリックは絶対しないこと

### ◇第5条 ホームページの閲覧には十分注意すること

ホームページの閲覧によりウイルスに感染する場合があります。

業務に無関係なホームページを閲覧してはいけません。

- ・業務に無関係なホームページを閲覧しないこと
- ・株の売買やショッピングなど業務に無関係な電子商取引を行わないこと

平時の対応が重要です。何かいつもと違う事があったら、すぐ所属長（情報セキュリティ管理者）に報告して指示を仰ぎましょう【早期対応が重要です】