

connect8 使用上の厳守事項

 安全に『connect8』を利用して頂くにあたり、下記の事項をご確認下さい 

なお、下記の事項は『connect8』利用時のみだけではなく、安全にIT 端末を利用する上でも必要な項目です

(その1) ウィルス等の感染による被害にあわないようセキュリティ対策

※ウィルスに感染してしまうと、自分のコンピュータが被害を受けるだけでなく、インターネットの別のコンピュータに対する感染活動を行い、加害者となってしまうことがあります。安全にコンピュータを利用するためには、ウィルス対策ソフトの導入や、インターネットサービスプロバイダによるウィルス対策サービスの利用が必須です

- 端末により異なりますが、セキュリティソフト（McAfee/Norton/ウイルスバスター等）の導入して下さい。
- OS やブラウザ等は常に最新の状態に更新して下さい。
- 身に覚えのない送信者からのメールの開封および不審なサイトの閲覧、ダウンロードはお控え

下さい。

(その2) 盗難・紛失時の、第三者の不正利用対策

※ID/パスワードの適正な設定・管理は、端末の置き忘れや紛失等の方が一の際に、第三者の不正利用を防止したり、なりすまし等の被害を防ぐ事が出来ます

- 端末に「画面ロック」の設定を行って下さい。
- connect8へログインする際は、ID/パスワードを保存せず、ログイン毎に入力するようにして下さい。
- 一時的に端末を使用しない際でも、ログアウトをするようにして下さい。

(その3) アプリケーションソフトを介した情報漏洩対策

※アプリケーションソフトの中には、連絡先情報等へのアクセス許可を求められ、個人情報等の情報漏洩の原因となる場合があります

- connect8で使用する端末には、通信以外に不要なアプリケーションソフトのインストールはしないようにして下さい。

《 個人端末でのご利用について 》

原則個人端末での利用は禁止とします。やむを得ず利用する場合は、上記注意事項及び利用規約を遵守の上、施設責任者及びユーザーの責任でご利用下さい。

厳守項目チェックシート

下記の内容をよくご確認の上、チェック欄にし印をつけ、事務局まで返送下さい。

- connect8利用規約／施設責任者向け運用ルール／connect8使用上の厳守項目を確認した。
- セキュリティソフト（McAfee/Norton/ウイルスバスター等）の導入は済んでいる。
- OS やブラウザ等は最新状態に更新されている。
- connect8を利用する端末においては、身に覚えのない送信者からのメールの開封、不審なサイトの閲覧及びダウンロードは行わない。
- 端末に「画面ロック」の設定を行っている。
- セキュリティ ID は施設責任者以外の第三者に知られることのないよう管理し、入力には施設責任者が必ず行う。
- connect8へログインする際は、ID／パスワードを保存せず、ログイン毎に入力する。
- 一時的に端末を使用しない際でも、ログアウトをする。
- connect8で使用する端末には、通信以外に不要なアプリケーションソフトのインストールはしない。

※個人端末での利用は原則禁止とします。

やむを得ず利用する場合は、施設責任者の管理のもと、細心の注意をもって利用して下さい。

※施設責任者及びユーザーの規約違反により生じた損害については、施設責任者が負うものとします。

私は上記事項に関して、その内容を十分に理解し、上記の内容に関して、全て確認のうえ connect8を利用します。

令和 年 月 日

事業所名

施設責任者名（自署）