Sec01-08-99\_サイバーセキュリティ対策用新端末の改善について

1. 更新履歴
   1. 2020年1月29日0.6版
   2. 2020年1月17日0.5版
   3. 2020年1月16日0.4版
   4. 2020年1月9日0.3版
   5. 2020年1月8日0.2版
   6. 2020年1月6日0.0版
2. 目的
   1. 物理端末（インターネット系）の利便性が悪いため、業務効率が大幅に低下している。効率的・効果的な業務の遂行のために、改善を求める。
3. 改善案の検討理由
   1. サイバーセキュリティ対策業務は、関係機関の最新情報へのアクセス環境、情報交換環境、相談者と同レベルのIT環境、アクセス環境等が必須である
      1. 非正規職員だからインターネット環境はなくてもいいという対応では、サイバーセキュリティ専門員としての所掌業務を遂行することができない。
   2. 現状は、サイバーセキュリティ対策業務に支障をきたすレベルのインターネット環境
      1. 現状環境の選択は、専門員所掌事務である情報収集・蓄積・発信業務の遂行のために、インターネット系のアクセスを優先した
      2. しかしながら、物理端末（インターネット系）は、イントラがアクセスできない端末であるにも関わらず、アクセスサイト、環境、データ保存等に制限が多い。
      3. このような環境では、サイバーセキュリティ対策専門員の情報収集、蓄積、発信業務が円滑に行えない。
   3. そもそも
      1. Society5.0、DX、ITの活用をビジョンに掲げる職場の職員のOA環境として、利便性を犠牲にした過剰なセキュリティ対策になっていないか？
         1. ファイル無害化のようなシステムまで導入して分離したインターネット環境を従来以上に制限する理由は？
            1. 20年以上前の繋がらなければ、使わせなければ、安全という対応に見える
            2. インターネット環境の情報資源のリスク分析結果は？

リスクが過大に評価されていないか？

リスクの低い事項を適正に制限緩和してもいいのではないか？

* + 1. 正規職員と非正規職員でPC環境を分ける理由は？
       1. 産業労働局の非正規職員は、インターネットが使えなくてもいいという判断根拠は？
       2. 非正規職員は、インターネット系か内部事務系かの二者択一にした判断根拠は？
       3. もし、正規職員と非正規職員でPC環境を一括で差別する内規があるとすれば、非常勤・臨時職員制度の改正が施行される状況において、その規程の妥当性は？
    2. 関係者間の認識の共有不足により、対応が後手に回って、手遅れというような結論になっていないか？
       1. 専門員は、セカンドライフとして、「能力の発揮や自己実現の場」として、過去の経験・知見を生かして、何らかの貢献をしたいという職業倫理に基づいて行動していることを、認識していただきたい。

1. 環境改善案
   1.  改善概要
      1. 現状のアクセス制限の多い物理端末（インターネット系）の仕様であれば、別途TAIMSから切り離された端末を活用せざるを得ない
         1. 現状の物理端末（インターネット系）は、リカバリし直して、物理端末（内部事務系）とし、インターネットアクセスは、別途、環境を用意する
   2.  案（来年度調達以降）
      1. TAIMSとは独立した業務時間内常時接続のインターネットアクセス環境
         1. モバイル回線、モバイルルータ、 Windows10PC
         2. 専門員一人1台ずつ
      2. 物理端末（インターネット系）を物理端末（内部業務系）に変更
         1. 専門員3名に1台でも良い
   3.  暫定案
      1. 物理端末（インターネット系）を物理端末（内部業務系）に変更
      2. 案の環境が整うまで、インターネットアクセスは私物PC(Windows10, ChromePC)の利用を申請
   4.  希望しない案
      1. 物理端末（インターネット系）、物理端末（内部業務系）の2台
   5.  現状（1月10日現在）
      1. 物理端末（インターネット系）
      2. TAIMSイントラは、組織端末（内部業務系）を利用
2. 検討の根拠とする情報
   1. サイバーセキュリティ対策専門員の所掌業務
      1. 会計年度任用職員とは
         1. 学識・知識・経験に基づき、補助的な業務に従事し、行政運営を補完する
            1. 正規職員だけでは量もしくは質的に不足する業務を遂行する
      2. 専門員所掌事務
         1. (1)サイバーセキュリティに関する中小企業からの相談対応（窓口・電話・メールなど）及び相談記録作成⇒【受付業務】
            1. 電話での相談対応
            2. Webフォームでの相談受付、メールでの回答
            3. 窓口対応
         2. (2)サイバーセキュリティに関する中小企業支援施策の実施に関する業務（※普及啓発セミナーの運営、事例集作成等）⇒【情報発信】
            1. 「中小企業向けサイバーセキュリティ対策の極意」の追補情報の発信
            2. 中小企業向けサイバーセキュリティ対策情報の発信【体系的な情報アーカイブ】

ポータルサイト内「サイバーセキュリティ対策情報の書棚」「ナレッジデータベース」「アーカイブ」

* + - * 1. 中小企業に伝えたいホットな情報発信

⇒Twitterで発信

ポータルサイトのトピックスで発信

* + - * 1. プレゼン用マスタースライド及び解説文を事前作成及び改訂
        2. 出張相談・個別助言

都支援事業等でのプレゼンテーションおよび個別相談対応

* + - 1. (3)課長級、課長代理級からの指示に基づく各種資料作成業務⇒【情報収集・整理・蓄積】
         1. 【情報収集・整理・蓄積】【予測調査】（専門員としてのスキル、知識の習得と蓄積）
         2. 「中小企業向けサイバーセキュリティ対策の極意」の改訂（追補資料の作成）
         3. 「中小企業向けサイバーセキュリティ対策の極意」の内容の詳細化（解説資料の作成）
         4. 中小企業向けサイバーセキュリティ対策のハンドブック【対策情報の書庫】【ナレッジデータベース】の維持・更新
      2. （４） その他付随する業務
         1. ガイドブック送付依頼受付及び発送
         2. 会議等設営準備
         3. 係内庶務
    1. 求められる能力（専門員公募要項より）
       1. 事務処理(Word,Excel等のパソコン操作を含む)について一定の知識・能力を有する
          1. ⇒最低限、社会人の常識とされる「ITパスポート試験」レベルのITリテラシー（知識・能力）を有すること
       2. サイバーセキュリティや情報システムに関する基本的な知識を有していることが望ましい
          1. ⇒IT関連の基礎技術とされる「基礎情報技術者試験」認定レベルの知識・能力を有すること
          2. ⇒可能であれば、「情報セキュリティマネジメント試験」認定レベルの知識・能力を有すること
       3. 職務を遂行する意欲を有している
          1. 想像性・創造性
          2. 公務員倫理、職業倫理に沿った行動の中で、自己の能力を発揮し自己実現する意欲を有すること
  1. 所掌業務毎の必要環境
     1.  情報の収集
        1.  インターネットアクセス環境
           1. セキュリティ及びIT関連の最新情報サイト
           2. 相談内容の検証のためのサイトへのアクセス環境
        2.  イントラアクセス環境
           1. 都庁アカウントメールのアクセス環境
     2.  情報の整理・蓄積
        1.  情報整理
           1. マインドマップツール, VISIO, VSC,,,
        2.  情報蓄積
           1. 次世代技術検証環境

次世代IT技術の実践によるノウハウ等の習得

* + - * 1. GitHub環境
      1.  小冊子編集用
         1. Indesignツール
         2. EPUBアクセスツール
      2.  インターネットアクセス環境
         1. 相談対応

相談者との同様の環境

ブラウザは、Edge, Chrome, Firefox

被害サイト

相談者に伝える情報サイト

相談・届け出クイックリスト登録サイト等

* + - * 1. TCYSSメンバー組織との情報交換・共有環境
        2. クラウドサーバ環境
      1.  イントラアクセス環境
         1. 部門共有サーバアクセス環境

担当間情報共有管理

個人毎情報管理

* + 1.  情報の発信
       1.  インターネットアクセス環境
          1. 極意ポータルサイトへのアクセス
          2. Twiiterへの投稿環境

1. 検討に当たっての参考情報
   1. 物理端末（インタネット系）
      1. ■インターネットアクセス環境
         1. ●相談者と同じブラウザが使えない
            1. IEでは、見えないサイトがある。IEを推奨しないサイトが多々ある。
            2. Chrome, Firefoxを利用できるように
         2. ●有用な情報保持サイトが使えない
            1. Pocket,
            2. SlideShare
         3. ●IEでは
            1. サイバーセキュリティ対策の極意ポータルサイトのTwiiterガジェットが表示できない
            2. ソース表示ができない
            3. Pocketサイトが見えない
            4. はてぶのブックマークレットが使えない
            5. ⇒edgeもしくはChromeを使えるようにすべき
            6. 青ヶ島村ホームページさえ見えない
      2. ■ファイル操作環境
         1. 再起動時に全てのユーザファイルが削除される
      3. ■相談対応
         1. 攻撃方法を検証できないと防御方法を把握できない、伝えられない
   2. 組織端末（内部業務系）
      1. 一時ユーザとしての利用であり、継続的に環境が保存されるか不明。