Sec10-01\_次世代の知的創造活動とセキュリティ対策

1. 更新履歴
   1. 2020年5月7日Rev0.1
2. 新型コロナウイルス対策
   1. 人との接触の制限
   2. テレワークの普及
   3. 利用者も提供者もテレワーク
      1. 利用者
         1. 任意の場所での作業
      2. 提供者
         1. 任意の場所での作業
   4. 対面からリモートに
      1. 固定電話から、チャット、音声、ビデオに
3. 新型コロナウイルスが終息した後の社会基盤
   1. いつでもどこでも
      1. それは電子図書館の理念
         1. モノから中身へ
   2. デジタルトランスフォーメーション（DX）

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX21.html>

* 1. Society5.0の加速

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-3-1.html>

1. 働き方改革での知的創造活動
   1. 紙での利便性を、デジタルでも実現
      1. 書籍との自然の出会い
      2. 書棚のブラウジングをPC上で再現
2. 情報を保有する機関等の利用
   1. 来館型、紙資料から、リモート、デジタルへの変化の加速
      1. 自然、必然
   2. 来館型サービスと遠隔サービスの仕切りに変化
   3. 紙とデジタルの優位性に変化
   4. 情報探索支援、レファレンスサービスは、利用者も提供者も職場以外の場所でも可能に
3. 必要なセキュリティ対策
   1. 組織の事業継続計画（BCP）の中で、セキュリティ対策を定義
   2. テレワーク環境でのセキュリティ対策
   3. 第６章　安全なテレワークのためのセキュリティ対策
      1. 【抜粋引用】テレワークではじめる働き方改革－テレワークの導入・運用ガイドブック－【厚生労働省】
      2. 図表Ⅱ-6-1　テレワークに必要なセキュリティの考え方
         1. 
      3. 1.ルールによるセキュリティ対策
         1. （1）セキュリティガイドラインの策定
            1. ●基本方針：セキュリティ全体の根幹
            2. ●対策基準：基本方針をもとに実施すべきことや守るべきことを規定したもの
            3. ●実施手順：対策基準の事項を具体的に実行するための手順を示したもの
         2. （2）セキュリティルール・情報管理ルールの策定
            1. ●自宅における作業環境、PC の保管及び管理方法
            2. ●自宅における休憩中の PC の取扱い 〔ロックだけでいいのか、保管して鍵をかけるのか〕
            3. ●モバイルワークにおけるPCの管理方法 〔体から離さない、ストラップをつける、のぞき見防止フィルターをつける〕
            4. ●オフィスから持ち出す PCの管理 〔暗号化、BIOSパスワードなどを義務付け〕
            5. ●オフィス以外での情報管理 〔紙情報の管理、共用スペースでの情報管理〕
            6. 図表Ⅱ-6-2　セキュリティルール・情報管理ルールの例

テレワーク作業中は、利用する情報資産の管理責任を自らが負うことを自覚し、セキュリティガイドラインが定める技術的・物理的及び人的対策基準に沿った業務を行い、定期的に実施状況を自己点検する。

アプリケーションをインストールする際は、システム管理者にその旨を申請し、許可を受けたアプリケーションのみをインストールする。

テレワークには必要な情報セキュリティ対策が講じられているものを使用し、スマートフォン、タブレット等に関しては不正な改造を施さない。また、インターネット経由で社内システムにアクセスする際、システム管理者が指定した通信手段のみを用いる。

機密性が求められる電子データを保存する際には必ず暗号化し、端末や電子データの入った記録媒体（USBメモリ等）の盗難に留意する。また、機密性が求められる電子データを送信する際には必ず暗号化する。

* + - 1. （3）ガイドラインとルールの遵守・浸透
    1. 2.技術的なセキュリティ対策
       1. （1） アクセスの管理・制限
          1. 本人認証
          2. 端末認証
       2. （２）暗号による管理
          1. ハードディスク（HDD）暗号化
          2. セキュアコンテナ

携帯電話等にセキュアコンテナ（暗号化された企業用の業務データエリア）を作成するソフト及びサービス

* + - * 1. 情報漏えい対策付きの USB メモリ
      1. （３）運用のセキュリティ
         1. 電子データの原本保存

情報が改ざんされていない状態を保つためにも、情報の原本を常に意識して保存することはセキュリティ対策にもつながります。

例えばデータを自動バックアップするようにして、デー

タが誤って削除されてしまった場合でもデータの呼び出しや復元ができるようにしたり、データの閲覧記録や作業記録を取ったり、システム内で行われたことを監視や記録するソフトウェアを利用します。

このセキュリティでは、ネットワークやシステムの利用のハードルを上げるものではありません。

より厳密に「改ざんされていないデータ」を得るには、保存した時刻の認証や電子署名、印刷データ電子化・管理による方法も利用できます。

* + - * 1. ウイルス対策ソフト

インターネットに接続したり、外付けの記録媒体に接続する可能性がある限り、端末はウイルスに感染するおそれがあります。

ウイルスに感染すると端末が不具合を起こすほか、情報漏えいの危険性が高まります。そこで、事前に端末内にウイルス対策ソフトを導入し、ウイルスの早期検知、検知した場合の駆除を行うことができるようにしておく必要があります。

その機能を果たすソフトが、セキュリティ対策ソフトです。近年は不正アクセス検知や不正プログラム検出など、様々な悪意あるソフトウェアに対して有効な製品が増えています。

ウイルス対策ソフトは端末だけではなく、サーバに対して機能するものもあります。シンクライアント型端末を利用する場合はサーバのセキュリティを確保するために、端末自体よりもサーバに対してウイルス対策ソフトを導入すると効果的、かつコスト面から見ても有用です。

* + - * 1. 【コラム】導入した対策ソフトを含むソフトウェアを最新の状態にするアップデートの必要性

悪意あるソフトウェア等の手口は日々進化しており、対策ソフトのメーカーもそれに対抗すべく、日々最新の対策を講じています。そのため、導入した対策ソフトを含むソフトウェアを最新の状態にするアップデートを定期的に行うことが重要です。

特に情報システム関連の部署は、最新のソフトウェアがテレワーク実施者の利用しているPCに反映されているか、常に注意が必要です。

例えばリモートデスクトップを採用している職場の場合、オフィス内の PC が常時起動されたまま、再起動によって更新されるソフトウェアがなかなか更新されないことも有ります。

情報システム関連の部署やテレワーク推進部署が適宜メールや掲示板などを用いて事業所内に更新の周知を行い、システム上からも最新バージョンのシステムに切り替わっていないPCがないか、注意しましょう。

また、定期的なウイルスチェック（ウイルススキャン）の徹底も大切です。

* + - 1. （４）ネットワークのセキュリティ
         1. 概要

ネットワークを通じてやり取りされる情報、及びネットワークを支える機器・設備を安全に使い続けるため、ウイルス感染や不正アクセスがされにくいネットワークを用意しましょう。

十分にセキュリティ対策を施していないネットワークを使い続けた結果、情報資産全体に悪影響となり、最悪の場合、事業を一時的に停止しなければならない事態にもなるおそれがあります。

ネットワークのセキュリティは特に、個々のテレワーク実施者よりも組織の情報システムを担当する部署の意識が問われています。

テレワーク実施者が安全なネットワークを利用してアクセスできる環境を提供し、ネットワークからの不正侵入に対して対策をするとともに、日頃から問題が起きていないかをチェックする体制を作りましょう。

* + - * 1. より安全な回線の選択

テレワークでは、外部のネットワークを介して、社内ネットワークに通信をすることになります。

そのため、外部のネットワークを利用する場合に、テレワーク実施者が定められたVPN回線に接続してアクセス（暗号化通信）するルールやシステムを導入する、あるいは不正な通過パケットを自動的に発見、もしくは遮断する措置のできるシステムが求められます。

これらは一定期間ごとに記録を管理して不正な動きの有無を確認したり、システムがきちんと稼動しているのかの定期チェックが必要です。

また、モバイルワーク等を実施する際には、ウイルス感染や盗聴の危険性のある公衆Wi-Fiは利用せず、通信キャリアが提供するモバイルルータを利用するといったルールづくりが望まれます。

公衆Wi-Fiを利用する際には、通信路が暗号化されたサービスを利用することが必要です。

やむを得ず、それ以外の公衆 Wi-Fi を利用する際には、全て暗号化された通信のみを利用することで安全性を高めることができますが、意識しないところで通信するソフトなどもあるため注意が必要です。

こうした対策ができない場合には、機密情報は扱わず、公開情報のみを利用する業務に限定するなどの対応が求められます

* + - * 1. サーバ証明書

第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施しましょう。

正規のサーバ証明書の取得に加え、紛らわしくないドメイン名を使うこと等により、テレワーク実施者によるサーバ正当性の確認を容易にするとよいでしょう。

* + - * 1. 【コラム】モバイルワークにおけるセキュリティ対策の注意点等（例）

モバイルワーク時のルール（例）

①オフィス外を移動するときは、必ずPCを鞄に入れて常時携帯する

②PCのローカルエリアにファイルを保存しない

③ハードディスクを暗号化する

④社外環境で印刷出力しない

⑤インターネット接続は会社支給のモバイルルータからのみ可とする

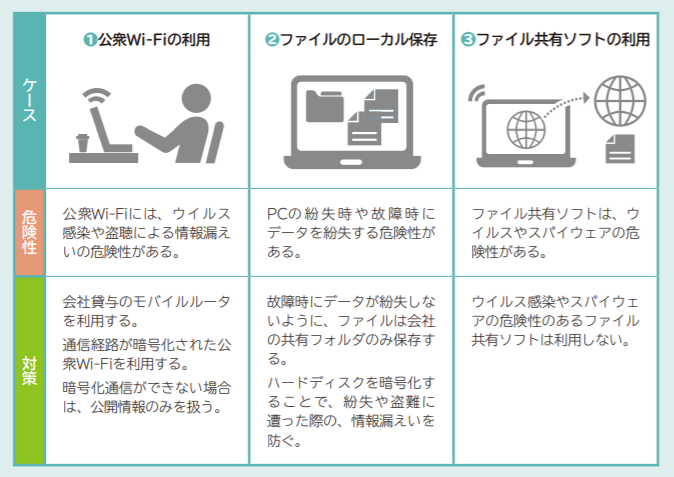
⑥社内環境へは暗号化通信を利用して接続する

⑦のぞき見防止フィルターを必ず装着する

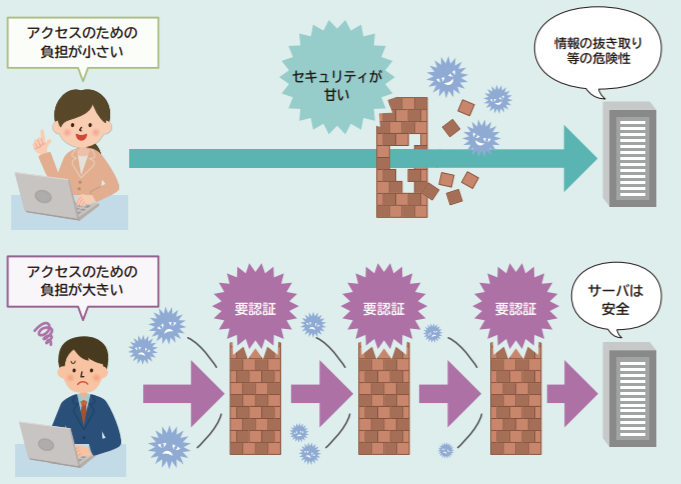
⑧PCを持ち帰る時は、上長にメールで報告する

⑨Web会議等の音声が発せられるときは、周囲に聞かれないよう注意する

危険性と対策について



* + - * 1. 【コラム】セキュリティ保護と業務効率向上とのジレンマ



セキュリティの強化は、「情報資産」の保護のために重要かつ、盗難・紛失以外にもオンラインから情報の抜き取り等の危険性がある現代において不可欠なものです。

しかし、セキュリティを強化すればするほどICT環境が複雑になるため、従業員に求める認証作業やICT環境構築を担う情報システム担当者の作業が増えてしまいます。

その結果、作業の煩雑さから業務効率が低下する問題が発生し、従業員のテレワーク利用が普及しにくくなるおそれもあります。

企業ごとの業務や風土によって適度なバランスを模索することが必要です。

* + 1. 3.物理的なセキュリティ対策
       1. ルールによるセキュリティ対策と技術的なセキュリティ対策では不十分な場合があります。例えば、盗難やスパイ活動、破壊等の損害など、PCやサーバという実体あるもの（ハードウェア）が危機にさらされる場合です。
       2. そこで「物理的なセキュリティ対策」が必要となってきます。具体的には監視カメラや入退出管理といった盗難防止策や、施錠棚やシュレッダーによる情報漏えいの防止策などが挙げられます。
       3. 物理的なセキュリティはテレワークの導入と同時に厳密に見直す、ということはほとんどありません。しかし、基本的に情報や情報に関する設備のある場所について、例えば「サーバや書類ラックは常に施錠されているか」「入退室の記録が適切な期間保管されているのか」といった確認が重要です。
       4. テレワークでは所属オフィス以外の場所が「オフィス」になります。そのため、新しく執務環境とみなす場所については、オフィス同様の物理的セキュリティ対策をする必要があります。例えば、在宅勤務時には「自宅に会社貸与のPCを施錠管理できる棚があるか」「執務中の家の立ち入りは不特定多数ではないか」などの確認は必要です。これらの確認には、テレワーク利用申請等の申請書類に執務環境を明記させたり、誓約書等を交わすことで十分な注意を約束するように指導するなどの対応が有効です。
       5. また、ペーパーレス化を進めることは、セキュリティ対策にもつながります。資料を全て電子化しておくことで、紙資料をオフィス外に持ち出す必要がなくなるので紛失や盗難が防げるほか、社内での情報整理が簡単になるので、情報の管理がしやすくなります。

1. ガイドブック等の作成に当たって
   1. セレンディピティの意識
2. 【参考】情報探索行動の考察
   1. 人は図書館と本棚をどう見ているのか？【佐藤翔】
      1. ブラウジング用配架法の構築
      2. 曖昧さを持つ情報要求を満たすため、 利用できる感覚全てを用いて広範で多量な情報源から、 必要なものを選びとる行為
         1. 松田千春「ブラウジングとは何か」
      3. セレンディビティ
      4. まとめ
         1. 書か・図書館を対象とする視線追尾研究
   2. 図書館における資料探索行動に着目したセレンディピティ. のある情報推薦システムの提案
      1. 既存の情報推薦システムでは精度を重要視したアイテムが推薦されてきた
      2. 推薦されたアイテムに対する「セレンディピティ」が新たに要求されるようになってきている
      3. 資料を間覧し経路を触りながら図書館資料を探索する手法にヒントを得て、実世界空間での資料探索行動を情報 推薦システムの組みとして取り入れることによって、セレンディピティのあるアイテムを推する手法の実現を目指 す。
      4. 資料を探索する過程でジャンルの移り変わりを見せることでセレンディビティのあるアイテムとの出会いを促す
   3. Wikipediaでの分類
      1. 学問体系
      2. 研究方法
      3. 専門分野
      4. 関連分野・境界領域
      5. Subtopic
   4. 1.（2004年）国立国会図書館「電子図書館中期計画2004」の実施に向けて
      1. 3.7.1.情報探索の行動パターンと提供すべきサービス
         1. デジタルアーカイブ・ポータルとしてどんな機能が必要かを考えるに当たって、 一般的な利用者がどのような手順で情報探索を行うのかのモデルに対応して ポータルのモデルを想定することが必要である。
         2. まず第一に、 利用者の情報探索の行動パターンは、 おおよそ、 6つの段階に分けて考えることができる。何かについて調べたいと思うことを課題として設定し「問題の定義、 情報ニーズの識別」を行う。 ポータルとしてはE-レファレンスやオンラインチュートリアルのサービスが必要となる。
         3. 次に、 「情報探索戦略の策定」として、 どんな情報源から調べるかを選び出す。「情報源の範囲及び利用順位の決定」を行うため、 サブジェクトゲートウェイ的な機能により、 情報を提供しているWebサイトやデータベースへのナビゲーションや 情報源への拾い読み（ブラウジング）を支援するサービスが必要となる。
         4. 3番目に、 「情報源の所在確認、 情報源へのアクセス」として、 選ばれた情報源に個別に実際に当たってみる行為で、 として、 メタデータ検索、 シソーラス検索などのセマンティック検索を支援するサービスが必要となる。
         5. 4番目に、 「情報の獲得（情報源の咀嚼、 情報の抽出）」として、 色々あたってみた情報を咀嚼して、 有用そうな情報を選別することで、 様々なデータベースを渡り歩くことなく統合検索し、 あるデータベースの検索結果から他のデータベースの二次情報、 一次情報への直接アクセスが一連の作業として行えるようにするサービスが求められる。
         6. そして、 選別された情報をあわせて自分が調べたかった内容として纏めることで、 「情報の統合（情報の組織化、 提示）」を行うために、 検索結果を利用者の目的に応じて利用しやすい形でアウトプットする機能が必要となる。
         7. 最後に、 今回調べた内容は正しそうだったか、 調べ方は合理的だったかを改めて見直すことで、 「評価（成果の評価、 プロセスの評価）」を行うことで一連の情報探索行動を終えることとなる。
         8. これらの段階を総合的に解決するポータルのイメージとしては、 「あるテーマで何かを知りたいとき、 色々なところから提供されている情報を、 １つの窓口から入って、 そこで解決できるようにしたもの」と想定する。
      2. 3.7.2.情報探索行動における図書館の方向性
         1. 図書館は、 紙の資料の時代から「情報探索することを助けること」を仕事としてきた。 しかし、現在のように多くの情報が氾濫し、 かつ様々なジャンルでの情報探索のニーズに応えるためには、 図書館自身の業務のやり方も変わっていかなければならない。 今後図書館は、どんな方向に向かっていくべきかを考えてみる。
         2. 一つ目は、 「個別の図書館から、 壁のない図書館へ」ということ。「個別の図書館が、 自館の所蔵資料に関する情報提供だけでは、 利用者の情報収集行動を支援できない。」ということで 「個別図書館サービスの横断的利用が可能になるようなサービスの提供を目指す」必要がある。
         3. 二つ目は、 「図書館サービスの枠を越えて」ということで、 「図書館だけでは、 利用者の情報収集行動を支援できない。」ということ。「同じ分野、 同じ利用者層をターゲットにした複数の専門情報サイトが連携して、 利用者がワンストップで利用できるようにする」ことが大切と考える。
      3. 3.8.デジタルアーカイブ・ポータルの利用イメージ
         1. 大きな流れとしては、 まず、 メタ情報がついたデジタルコンテンツをデジタルアーカイブに構築しておき、 利用者の任意の条件からメタ情報を検索し、 そのメタ情報の一覧から、 必要なものを選択すると必要なデジタルコンテンツが直接見えるようになるというイメージを想定している。 そしてそれは、 一つの機関の情報についてではなく、 他機関の情報を含めて統合的に利用できるようにすることにより、 利用者は情報の所在に関係なく、 利用できるようになるものである。（図１）