ひと、くらし、みらいのために
厚生労働省
Ministry of Health, Labour and Welfare

テレワーク導入時のICT活用における留意点

2023年度 テレワーク会場セミナー
（大阪会場）

2023/12/22

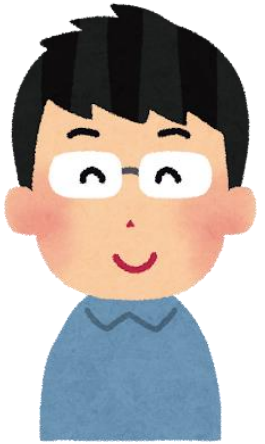
A-Intelligence
株式会社エー・インテリジェンス

© 2023 A-INTELLIGENCE INC.

◇ 自己紹介

- ◆ 大阪市内を拠点に中小企業様や小規模事業者様のIT回りをお手伝いしています。
- ◆『お客様のパートナーとして、お客様にとっての最善を、お客様と一緒に考える。』ことをモットーに活動しています。
- ◆ 何でもかんでも最新のトレンドを追いかけるのではなく、DIYでできることはDIYで、コストは必要最小限に、無駄のないIT投資をご提案しています。
- ◆ 公的機関の専門家相談員として、さまざまな事業者様からの IT活用全般についてのご相談対応や、セミナー講演などの活動もさせていただいています。

- 法人：株式会社 エー・インテリジェンス
  https://www.a-intelligence.co.jp
- 名前：中井 亮（なかい りょう）
- 資格：登録情報セキュリティスペシャリスト
  ITコーディネータ　etc.



© 2023 A-INTELLIGENCE INC.

◇ 本日のアジェンダ

① ICT活用を成功に導くための考え方

② テレワークを実現するためのツール

③ テレワークにおける情報セキュリティ

© 2023 A-INTELLIGENCE INC.

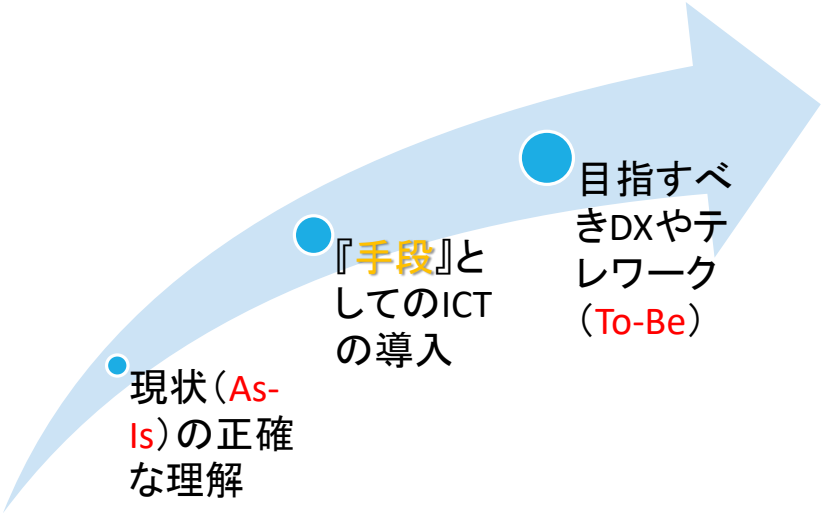
① ICT活用を成功に導くための考え方

© 2023 A-INTELLIGENCE INC.

◇ 手段と目標の逆転に要注意

世の中には様々なICT商材が溢れ、熾烈な営業活動が行われています。
その中で『使えないIT・使われないIT問題』に陥らないよう注意しましょう。

- ICTツール導入を検討する際は、常に現状（As-Is）と目標（To-Be）を意識するようにしましょう。
- 専門性が高い分野でもあるため、営業マンの説明を聞いて商談を進めているうちに、いつの間に『導入が目標』になってしまい、過剰性能や必要以上の商材を選択しがちです。
- 『自社には何が必要なのか？』『何が足りていないのか？』を常に念頭に置いて、予算面はもちろん、自社のリテラシーや運用能力に見合ったものを導入することが大切です。



© 2023 A-INTELLIGENCE INC.

② テレワークを実現するための仕組み

© 2023 A-INTELLIGENCE INC.

◇ VPN

テレワークする場所と会社との間の通信を暗号化することで、
仮想的（Virtual）な専用通信回線（Private Network）を作り出します。

- 本来インターネットは地球規模の公開ネットワークですので、通常の通信を行うと第三者に傍受されて情報を盗まれるリスクがあります。
- VPNを使えばそうしたリスクを回避しつつ、自席にいる時と同じように社内システムやデータにアクセスすることができるようになります。
- VPNを使うためには会社側に接続の受け口となる機器やソフトウェアが必要となりますが、導入自体はそれほど難しいことはありません。
- もちろんVPNを使う人数にもよりますが、以前と比べるとコストもリーズナブルになっています。

[自宅など]　　[社内システムやデータ]

© 2023 A-INTELLIGENCE INC.

◇ リモートデスクトップ

手元にあるPCから会社のPCを遠隔操作する方法です。

- テレワーク導入時に直面することが多い、「会社のPCに入っているソフトを使う業務をどうするか」という問題は『リモートデスクトップ』という方法で解決できます。
- リモートデスクトップを導入するにはクラウドサービスを使用する方法や、Windowsが備えている標準機能を使用する方法などがあります。
- Windowsの標準機能を使えばランニングコストは掛かりませんが、事前にVPNの導入が必要なことや、運用管理をしっかり行うにはある程度の専門知識が必要となります。
- クラウドサービスならVPNは不要ですが、有料と無料のサービスで以下の点が異なります。
- 有料のものは継続的に課金が発生しますが、専門知識がなくても使える運用管理機能が提供されていたり、困ったときにはサポートも受けられます。
- 無料のものは課金は発生しませんが、運用管理機能が提供されていないためセキュリティリスクが生じやすくなることや、サポートも受けられない点に注意が必要です。

© 2023 A-INTELLIGENCE INC.

◇ シン・テレワークシステム

誰でも無償*で利用できるクラウド型のリモートデスクトップツールです。

- 前頁の通り、リモートデスクトップにはVPNを使用する方法とクラウドサービス型があります。
- どちらの方式も、通常ならVPN環境の構築やクラウドサービスの利用に一定の初期費用やランニングコストが必要となりますが、『シン・テレワークシステム』は新型コロナ対策としてIPA*とNTT東日本が無償提供しているクラウドサービス型のリモートデスクトップツールです。
- 公式サイトからソフトをダウンロードして簡単な設定をするだけですぐに使用開始できるため、これからテレワークを始められる場合にもオススメのツールです。
- **将来的には他のツールに移行する必要が生じるかもしれないことや、こちらもサポートは提供されていませんので注意が必要ですが、** テレワーク導入の第一歩として活用しましょう。

NTT東日本

IPA 独立行政法人 情報処理推進機構

新型コロナウイルス対策 緊急構築 実証実験

公式サイトURL：https://telework.cyber.ipa.go.jp/

*今後無償提供が終了する場合、終了期限の6ヵ月前に公式アナウンスされる予定となっています。
* 経済産業省管轄の独立行政法人で、日本のIT化や人材育成を推進している組織です。

© 2023 A-INTELLIGENCE INC.

◇ その他のクラウド型リモートデスクトップツール

サポートが受けられる有償のクラウド型リモートデスクトップツールには、
例えば下記のようなサービスがあります。

[国内系サービス]

- mAgic Connect（提供元：NTTクロノス）
  https://www.magicconnect.net
- Remote View（提供元：RSUPPORT）
  https://content.rview.com/ja/
- RemoteOn（提供元：ジャパンメディアシステム）
  https://www.remoteon.ne.jp/

[海外系サービス]

- TeamViewer（提供元：TeamViewer）
  https://www.teamviewer.com/ja/
- Splashtop（提供元：スプラッシュトップ）
  https://www.splashtop.co.jp
- AnyDesk（提供元：AnyDesk Software）
  https://anydesk.com/ja

- 各サービスとも、色々なプランや機能をラインナップしていますので、詳細は各公式URLをご参照ください。
- これらのサービス以外にもクラウド型リモートデスクトップツールは色々なメーカーから提供されています。

今回ご紹介したリモートデスクトップツール以外にも、
テレワークに有用な様々なICTツールが各社から提供されています。
それらも活用しながらテレワークの導入を更に働き方改革やDXへ繋げましょう。

© 2023 A-INTELLIGENCE INC.

◇ テレワークに役立つガイドブック類

下記のページではICTツール類をはじめ、
テレワークの導入に役立つ様々なガイドブックが提供されています。
ぜひご参照ください。

一般社団法人 日本テレワーク協会

テレワーク導入ガイドライン

https://japan-telework.or.jp/suguwakaru/guide/

© 2023 A-INTELLIGENCE INC.

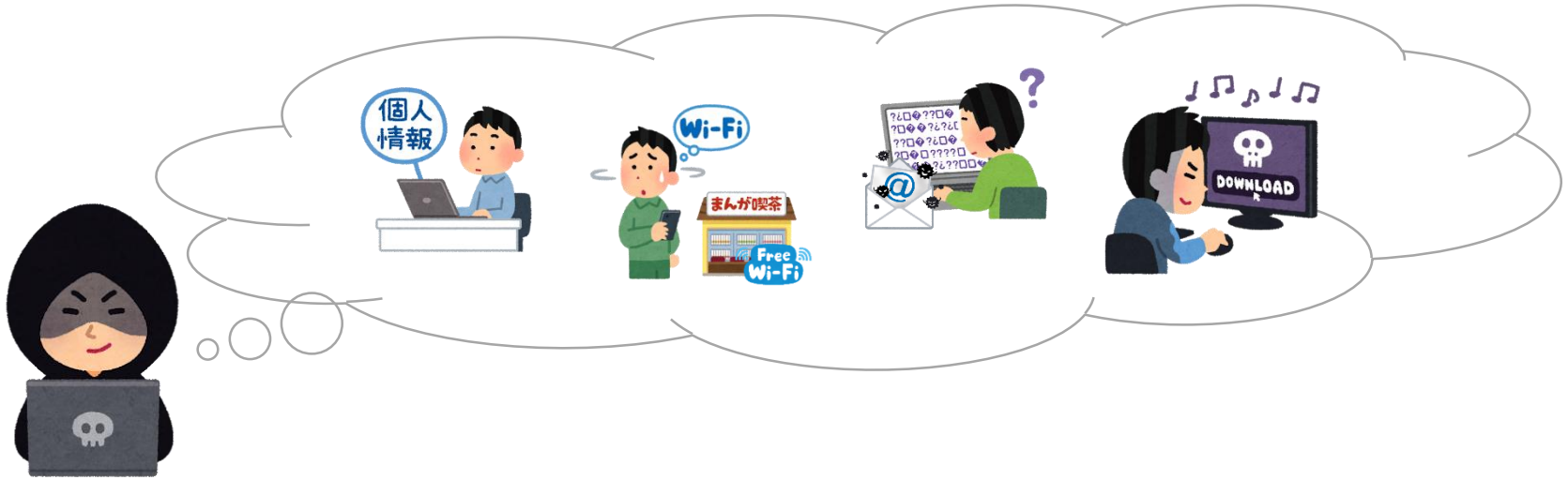
③ テレワークにおける情報セキュリティ

© 2023 A-INTELLIGENCE INC.

◇ テレワークとセキュリティリスク

- 従来の情報セキュリティの考え方は、内部と外部、業務用とプライベートなど、明確な境界を設け、内部や業務用とされた部分をしっかり守るという考え方が主流でした。
- しかしテレワークではその境界が曖昧になりやすく、仕事の進め方も個人の裁量が大きくなるため、無意識や気軽にハイリスクな行動を行ったり、それによる事故が起きやすくなります。
- また、コロナ禍で突貫準備のテレワークを導入し、それをそのまま続けているというケースも多く、その弱点を突いた攻撃による被害も増加しています。

テレワークやクラウドが普及するほど柔軟な働き方が可能になりますが、
それは攻撃の機会や弱点の増加とトレードオフであることを認識しておきましょう。



© 2023 A-INTELLIGENCE INC.

◇ 対策の進め方と考え方

どんなセキュリティリスクに対して、どこまで備えるべきなのか？

マッチポンプな一面があることは否定できない

- ✓ 営業活動やセミナー等でニーズを喚起し、利益に繋げている業界の実態は否めない。
- ✓ 「情報セキュリティ」という強いワードに踊らされ、闇雲な対策や投資に陥らないよう要注意。

リスクを正しく理解して優先順位を考える（リスク分析）

- ✓ 大企業と中小企業では、晒されるリスクの種類や内容も異なれば、優先順位も異なるはず。
- ✓ 自社が抱えるリスクを正しく理解し、重要度の高いものから優先的に対策することが大切。

技術的・物理的・ルールによる総合的な対策の実施（リスク対策）

- ✓ 技術的対策は効果的だが実施までに高コストや長時間を要し、生産性低下などが生じる場合も。
- ✓ 物理的対策やルールによる対策は必要最低限のコストで実施でき、即効性も高く効果的。
- ✓ ただしこれらの対策は形骸化し易いため、継続的な見直しと教育・啓蒙を続けることが重要。

© 2023 A-INTELLIGENCE INC.

◇ 運用体制の整備

［ルールの整備］

- テレワーク時の業務ルールを定めましょう。
- PCやスマホの持ち帰りルールや禁止事項、利用しても良いソフトやクラウドサービスなども予め決めておきましょう。
- SNSの利用ルールなど、一部は就業規則にも折り込めますので、社労士などとも相談して必要に応じて改定しましょう。
- これらは形骸化し易いので、定期的な見直しやチェック体制も同時に考えておきましょう。

［情報セキュリティ担当の配置］

- アカウントの作成や削除、それに伴う管理簿の更新など、イメージよりもICT運用は事務的な仕事が多々あります。
- 特に退職者アカウントの放置やルールの形骸化はハイリスク要因となります。
- ICTの専門知識の有無よりも、まずはそうした事務的な面をきちんと管理できる体制を作りましょう。
- また、トラブル発生時に迅速に報告を受けられる連絡体制を定めましょう。

［機材の準備］

- 社員の私物を利用しても良いですが、管理面やセキュリティ対策が甘くなる可能性があるため、できれば適切な対策を行った機材を会社側で用意しましょう。
- 私物の利用を許可する場合でも、セキュリティソフトの利用を必須化するなど、一定の基準をルールとして定めましょう。
- 特に私物のUSBメモリなどの使用はハイリスク要因となりますので注意が必要です。

［専門家への相談］

- 社内だけではルールの検討や整備、技術的な対策が難しい場合は専門家に相談しましょう。
- ただし専門性の高さや社会的関心の高まりを逆手に取って、相場を超える価格や必要以上の過剰提案をする業者も増加しています。
- 必要に応じて相見積りや公的窓口に相談するなどして、信頼できる業者に依頼しましょう。

© 2023 A-INTELLIGENCE INC.

◇ 結局一番のセキュリティホールは？

いくら技術的な対策を施しても、結局は人間が一番のセキュリティホール。

- 会社のPCで業務に関係のないサイトを閲覧したり、無断でフリーソフトをインストールする。
- 無断で私物のUSBメモリを差し込んで、家にデータを持ち帰ったり、逆にデータを持ってくる。
- 無断でフリーメールやクラウドサービスの無料アカウントを作って、業務のデータをUPする。
- 怪しいメールの添付ファイルを開いてしまったけど、変わった様子はないのでスルーした。
- ギガを節約したくて、社内のWi-Fiにコッソリと私物のPCやスマホを接続して使用している。
- 支給されているスマホを私物化し、ゲームなど業務に関係のないアプリをインストールする。

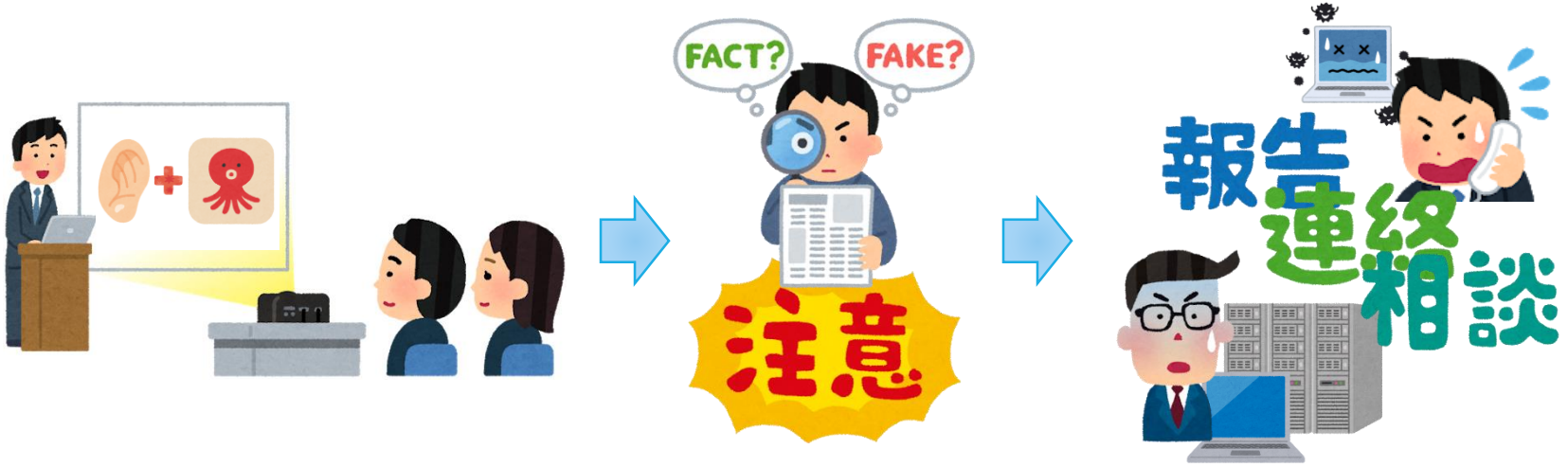
『このぐらいイイじゃん。』『このぐらい大丈夫でしょ。』『みんなやってるし。』
こうした意識や行動がやがて事故へと繋がります。

© 2023 A-INTELLIGENCE INC.

◇ 教育・啓蒙こそ最後の砦

- 技術的な対策と比べて、教育・啓蒙の取り組みは低コスト・短期間で実施できます。
- 場当たり的に一度限り実施するのではなく、定期的でも不定期でも、同じ内容でも違う内容でも、最新の報道事例も取り上げつつ、継続的に実施することが重要です。
- それが無意識の注意力を養い、リスクを未然に防ぐ回避行動に繋がると共に、万が一アクシデントが起きたとしても迅速なホウレンソウを可能とします。

教育・啓蒙はいくらしても、し過ぎることはない。
『耳にタコ』ができるほどの啓蒙を。



© 2023 A-INTELLIGENCE INC.

今回はこれからテレワークを実施されようとしている事業者様に、
特に意識していただきたい点についてご説明させていただきました。

皆様がテレワークや働き方改革に取り組まれていく中で、
今回お話した内容がお役に立てば幸いです。

© 2023 A-INTELLIGENCE INC.