# テレワーク等対応支援における
# 情報セキュリティ留意事項、
# その他接続不良などのトラブルシュート

合同会社IT相談製作所
上田幸哉

INSIGHT
I'm always here for you.

# はじめに

## ねらい

- 本研修では、テレワーク等における情報セキュリティの考え方や留意事項、および機材の接続不良などに代表されるトラブルシュートについて理解します。
- 基本的には、企業側の仕組み、ツール、ルールに合わせることになりますが、本質的な事柄を理解しておくことで、対応がしやすくなります。

# セキュリティ対策のポイント

# セキュリティ対策のポイント

## 考慮点

- パソコンに関すること
- インフラに関すること
- クラウドに関すること
- 個人情報や機密情報の扱いについて

# セキュリティ対策のポイント

## ● パソコンに関すること（設定編）

- アンチウィルスソフトを必ずインストール
  - ウィルスやハッキングからの防御
  - （企業側から指定されることもあるので、従うこと）
- スクリーンロック
  - パスワードを設定して、自分以外に操作できないようにする
- ローカルドライブのファイル
  - パソコンのドライブに保存されている業務用の情報
  - できるだけ保存しないほうが良い
    - 用が済んだら削除する
- WEBブラウザ
  - アップデートは常に最新
- 設定類
  - OSのセキュリティアップデートは常に最新（Windowsアップデート）

# セキュリティ対策のポイント

## ● パソコンに関すること（操作編）

- 情報のやりとり
  - メールの宛先や添付ファイルが正しいかどうかを確認すること
    - メールは一度送信してしまうと、取り返しがつきません
  - メールは誤送信のリスクがつきまとうため、できれば掲示板やクラウドサービスでの共有など、共有先がコントロールできるものを使用することでリスクを小さくできます
- まず、疑う
  - メールを使って巧妙な手口で、悪意あるリンクが送られてくる
  - むやみにクリックせず、ちょっと変だな？と思ったら相談する（クリックしない）
- 添付ファイルに注意
  - メールに添付されているzipファイルなども注意
  - 送信元を確認した上で、ダウンロードする

# セキュリティ対策のポイント

## ● インフラに関すること

- ネットワーク
  - インターネットとの接続口である、インターネットルータについて
    - ファームウェアの自動更新を行うように設定し、常にファームウェアを最新状態にしておく
    - Wi-Fi接続の場合、アクセスポイントに誰でも接続できないようにパスワードを設定しておく

# セキュリティ対策のポイント

## ● クラウドサービスに関すること

- クラウドサービスの利用
  - IDとパスワードの管理
    - 自分自身で用意したもの、企業側から貸与されたものであれ、クラウドサービスにアクセスするための、IDとパスワード情報は厳重に管理する
    - 複数のサービス間で、同じパスワードは使用しない
  - アクセス権の管理
    - 自分自身で用意したクラウドサービスにおいては、その管理も行わなければならない
    - クラウドサービスに保管されている情報へのアクセス権は、必要最低限とし、用が済んだら削除するなど管理を行うこと

# セキュリティ対策のポイント

## ● 個人情報や機密情報の扱いについて

- 個人情報とは
  - 『生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述などによって特定の個人を識別できるもの（他の情報と容易に照合することができ、それによって特定の個人を識別することができることとなるものを含む。）、または個人識別符号が含まれるもの。』（出典：個人情報保護法）
  - 重要なポイント
    - 個人に関する情報であること
    - 特定の個人を識別できること
  - 例）
    - 「本人の氏名」のみで特定の個人を識別できる場合
    - 名字（姓）だけでは特定できないが、会社名や住所などのプロフィールを組み合わせることで特定できる場合
- 個人情報の取り扱い
  - 個人情報は、その本人の合意のもとお預かりしている情報です
  - 許可なく、第三者に伝えたり、使用目的以外の活用は禁じられています
  - 認識を持って、その情報の扱いや行動に注意する必要があります

# セキュリティ対策のポイント

## ● 個人情報や機密情報の扱いについて

- 機密情報とは
  - 企業秘密とも呼ばれる、企業にとって重大な秘密情報のこと
    - 企業が保有している情報のうち、外部への開示が予定されていないもの
    - 情報秘密として分類管理されている情報
    - 開示されれば、企業に損害が生じ得る情報
  - 情報の例
    - 顧客情報
    - 従業員の情報、人事、住所、昇格
    - 取引先の情報
- 機密情報の取り扱い
  - 情報漏えいが最大のリスク
  - 聞き及んだ情報、ファイルなどに示された内容など、外部に知らせてはならない
  - 個人情報同様、慎重に取り扱う必要があります

# セキュリティ対策のポイント

## ● 情報の扱いに関する取り決め

- 情報セキュリティに対する誓約
  - 企業に雇用されるとき、情報セキュリティのルールについて誓約書なり交わされることがあります
  - 内容をよく確認し、業務に務める必要があります
- インシデント発生時
  - 故意、不注意を問わず、情報漏えいの可能性やミスを犯してしまうことは100%防ぎけれません
  - そのような事態が発生、または恐れに気がついたときは早急に報告する必要があります
  - セキュリティインシデントは、早く気づいて対処することでその被害を最小限に留めることができます

# セキュリティ対策のポイント

## まとめ

どれだけ気をつけていても、ミスやエラーを完全に防ぐことはできません。

もし、ウィルスやハッキングにあったとしても被害を最小限に抑えるために、パソコン上のファイルを最小限にしておくことをおすすめします。
極端な話、業務で使用されているパソコンが盗難にあったとして、影響がないようにしておくことが理想的ですが、できるだけ影響が少ないようにしておきましょう。

情報の取り扱いに関して、間違いや恐れを感じたときは、速やかに報告することで、その被害を最小限にできます。

# テレワークにおける
# よくあるトラブルとその対処方法

# よくあるトラブルとその対処方法

## ビデオ会議でのトラブル例

- ビデオ会議
  - ビデオ会議に参加できない
  - 相手の音が聞こえない
  - 自分の声が聞こえていない
  - 自分のカメラの画像が映らない
  - 音声が途切れる・相手の画像が固まる

# よくあるトラブルとその対処方法

## ビデオ会議のトラブル対策

- ネットワークの確認
  - インターネットに接続できているか
  - 適切な速度が確保されているか
    - アップロード速度、ダウンロード速度
- デバイスの接続を確認
  - カメラは認識されているか
  - スピーカー、マイクは認識されているか
  - 壊れていないか
  - デバイスの再接続
- パソコンの再起動

実際にZoomの画面を見ながら説明します

# よくあるトラブルとその対処方法

## ● その他、業務上こまったとき

- 連絡手段の確保
  - テレワークでは、気軽に声をかけたり、質問しに行くことが難しいです
  - メールのほかに、チャットや掲示板など気軽に連絡がとりやすい環境があるとよいです
  - ネットワークのトラブルを想定して、携帯電話などバックアップ手段を用意しておきましょう