石川県主催　働き方改革セミナー

「テレワークを適切に導入し」効果を出すための５つのポイント

令和３年1月29日

ITコーディネータ　横屋 俊一

ミニセミナーの内容

- テレワークとは
- テレワークを実施する目的
- テレワークを実施して得られる効果とは？
- テレワークを導入するプロセス
- 適切なテレワークを実施する5つのポイント
  1. 経営層と従業員の意識
  2. 仕事環境の整備（業務の見直し、必要なICT環境）
  3. コミュニケーション
  4. ルールとマネージメント（テレワーク規定、運用ルール）
  5. 情報セキュリティ
- テレワークに関する参考資料

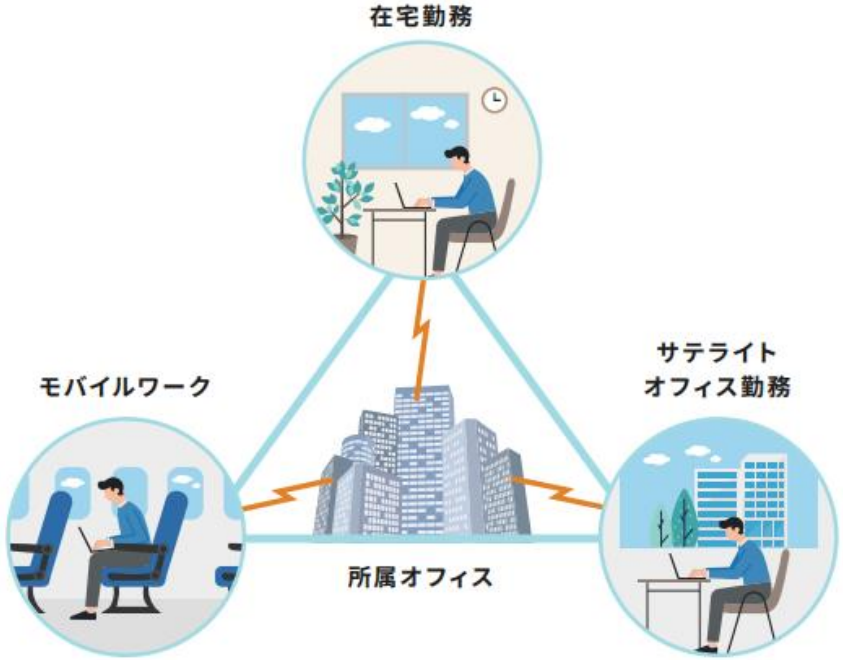
テレワークとは

テレワーク（TellWork）とは、

テレ	ワーク
Tele	Work
＝	＝
離れたところで	働く

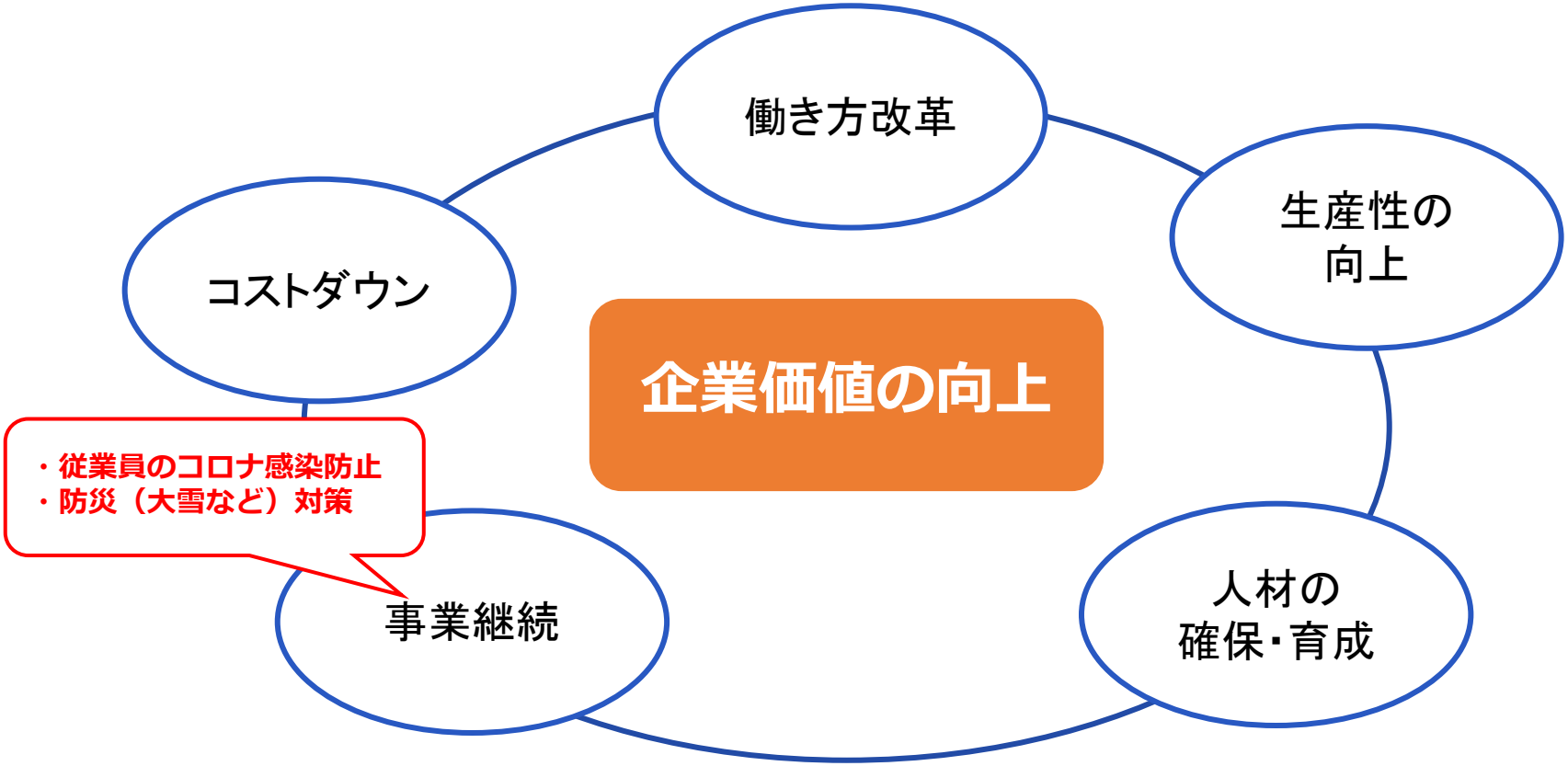
会社から離れて仕事をすることを言います。

その形態には図のような３つの形があります。



テレワークを実施する目的

テレワークとは、たんなる離れて仕事する
リモートワークの意味にとどまらず、**企業価値の向上**を目的とするものです。



テレワークを実施して得られる効果とは？

1. 企業の経営力向上

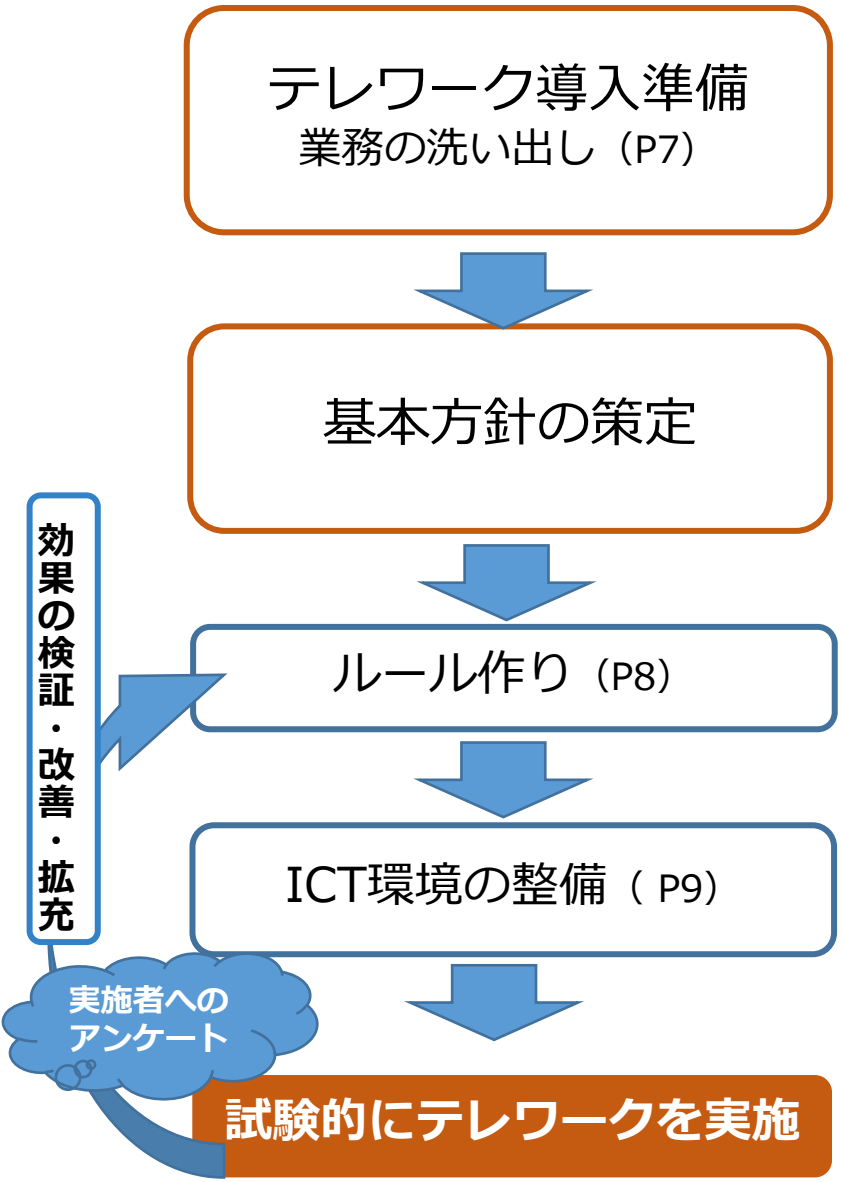
- 自宅で業務に集中できることによる業務の効率化
- 　⇒残業時間の削減
- 交通費やオフィスの家賃、電気代などのコスト削減
- 多様で柔軟な働き方に対応している企業であることによる優秀な人材の確保
- 　⇒採用力の向上
- 災害時（現在はコロナ禍）における事業継続体制の構築

生産性の向上

2. 従業員の満足度向上

- 仕事と育児・介護との両立が可能
- 　⇒離職者の防止
- 満員電車など通勤によるストレスや新型コロナウイルス感染リスクの軽減
- 通勤時間の削減による自由な時間の確保

テレワークを導入するプロセス①



テレワークの全体像をつかむための現状把握

- テレワークが可能な業務はどの程度あるか
- どのくらいの従業員が対象となり得るのか
- コストはどのくらいかけられるか

テレワークの基本方針に盛り込むべき内容

- テレワークを導入する目的
- テレワークの対象者と部署、業務
- テレワークを行う頻度
- テレワークの予算

出典：厚生労働省「テレワークで始める働き方改革」

テレワークを導入するプロセス②

テレワーク導入準備
業務の洗い出し（P7）

業務洗い出しの☑ポイント

- ☑ **業務に必要な書類（紙書類、電子データ）**
- ☑ 業務にかかる時間
- ☑ コミュニケーション量
- ☑ セキュリティリスク
- ☑ すぐにできる業務、今はできない業務、当面できない業務に仕分け

現在の業務

直ぐ実施できる業務

自己完結性が高い業務

- 業務システムへの入力作業
- データの修正、加工
- 資料の作成
- 企画業務
- デザイン、プログラミングなど

今は実施できない業務

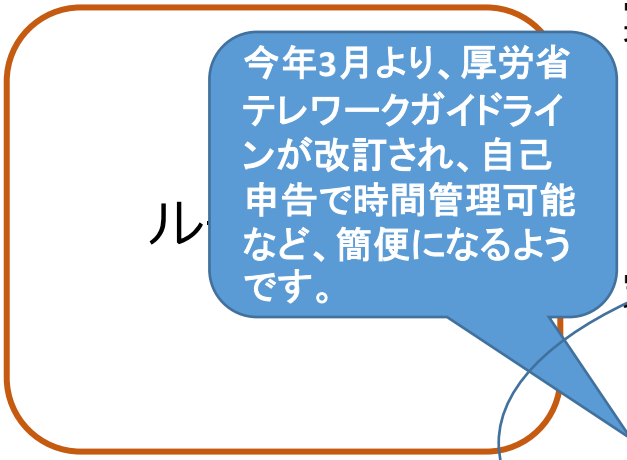
ツールやルールの整備により実施できる業務

- 帳票や資料をデジタル化することで出来る業務
- コミュニケーションの環境整備で出来るようになる業務
（商品開発や社内外の打合せ等）

当面実施できない業務

現場で人が機械などの操作を必要とする業務や接客業務

テレワークを導入するプロセス③



実施範囲の決定

- テレワーク対象者

⇒基準の明確化（介護・育児が必要な従業員）

- 実施頻度と対象業務

労務管理の方法（勤怠管理のルール）

- 始業、終業時間の変更や中抜け時の申請、承認などのルール
- 報告手段（メール、勤怠管理ツールなど）

テレワークの労働時間制度

- フレックスタイム制、みなし労働制

業務管理の方法

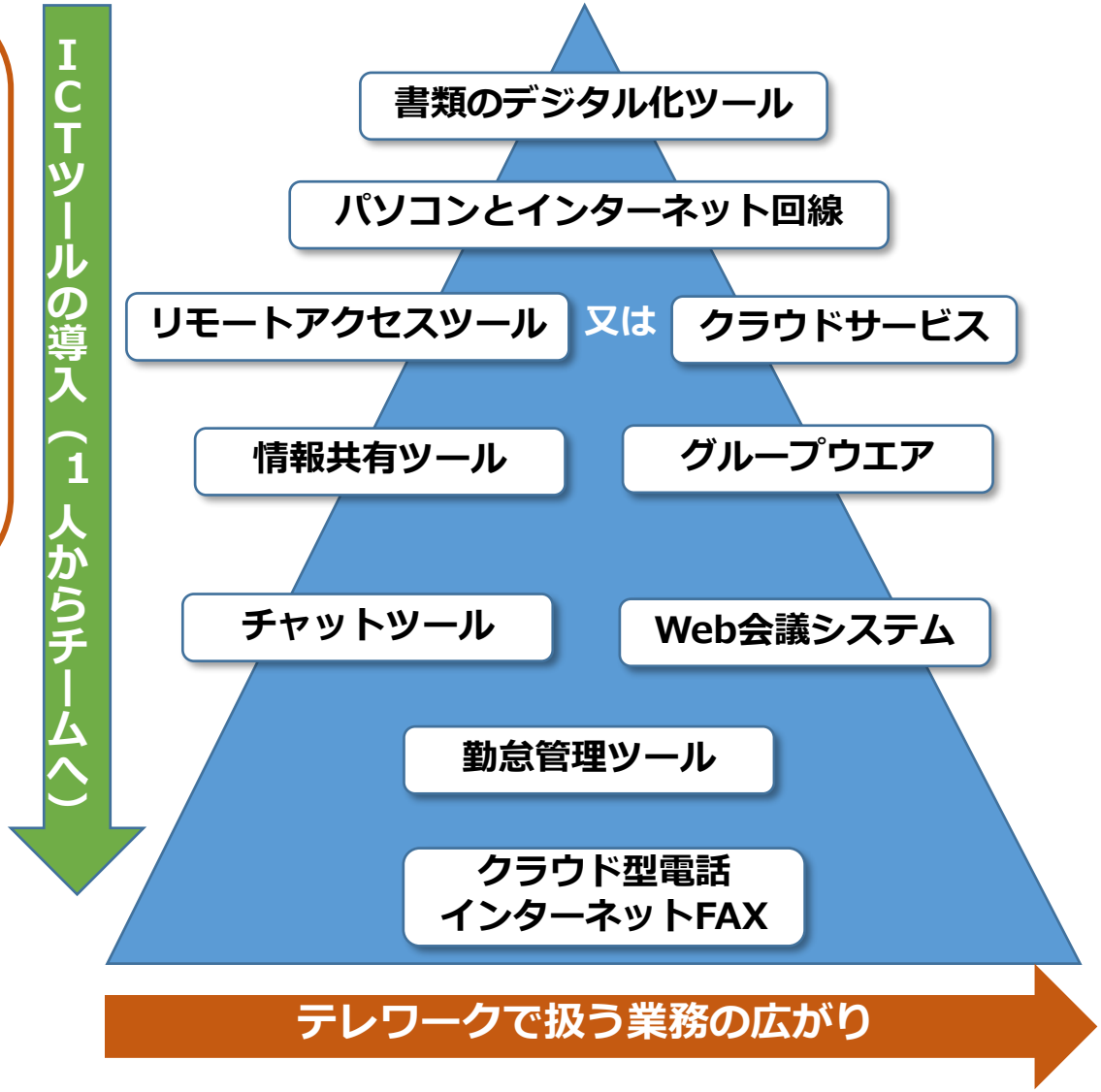
- 情報共有の方法（ツールなど）
- 進捗状況の把握を管理する方法（ツールなど）
- コミュニケーション方法

テレワーク実施者のコスト負担

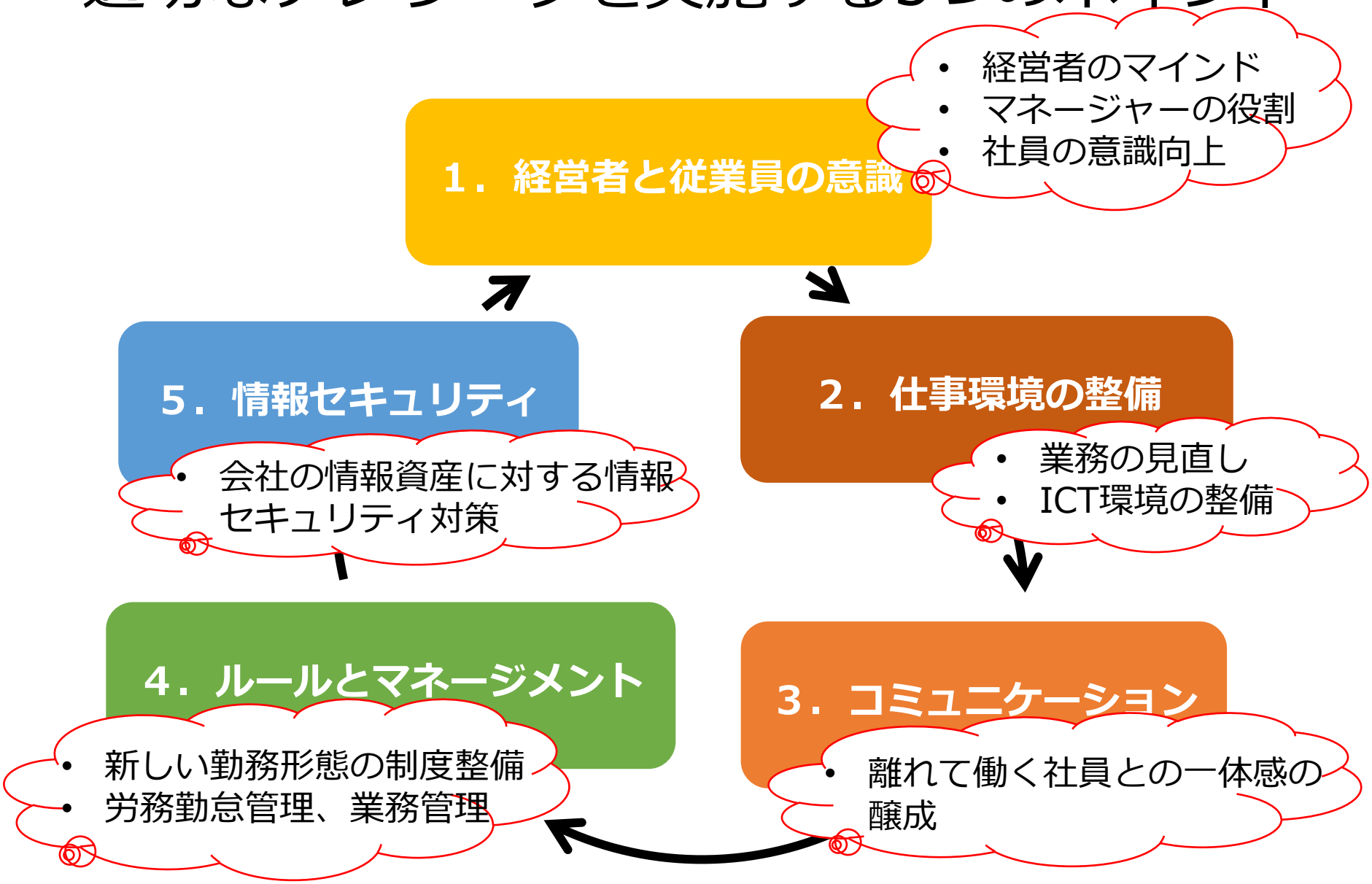
- テレワーク手当の有無
- 通信料、水道光熱費などの会社負担のルール

テレワークを導入するプロセス④

ICT環境の整備



適切なテレワークを実施する5つのポイント



テレワークはトップダウンで

経営トップがテレワークを
実施する目的を明確にし、
強い意志を表明する。

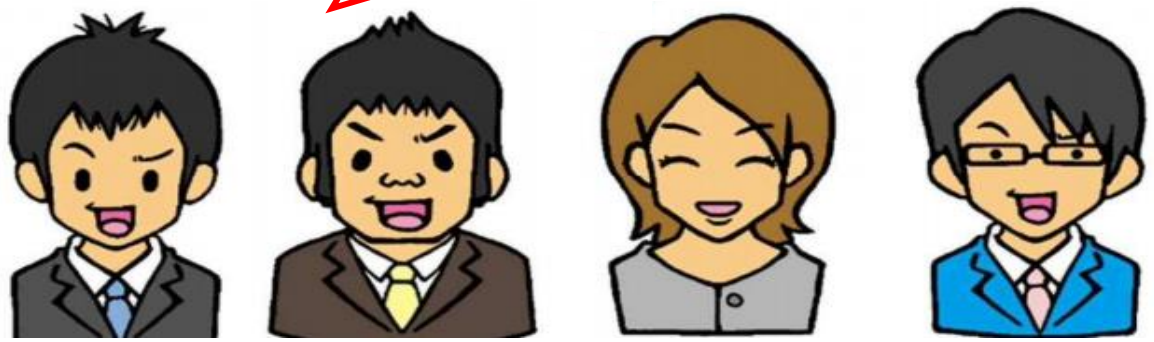
テレワークはマネージャーが率先して実践

テレワークはマネージャーに負担がかかるため、ブレーキになりやすい。
率先して使って、メリットを部下に伝える努力が必要

従業員の前向きな意識の醸成

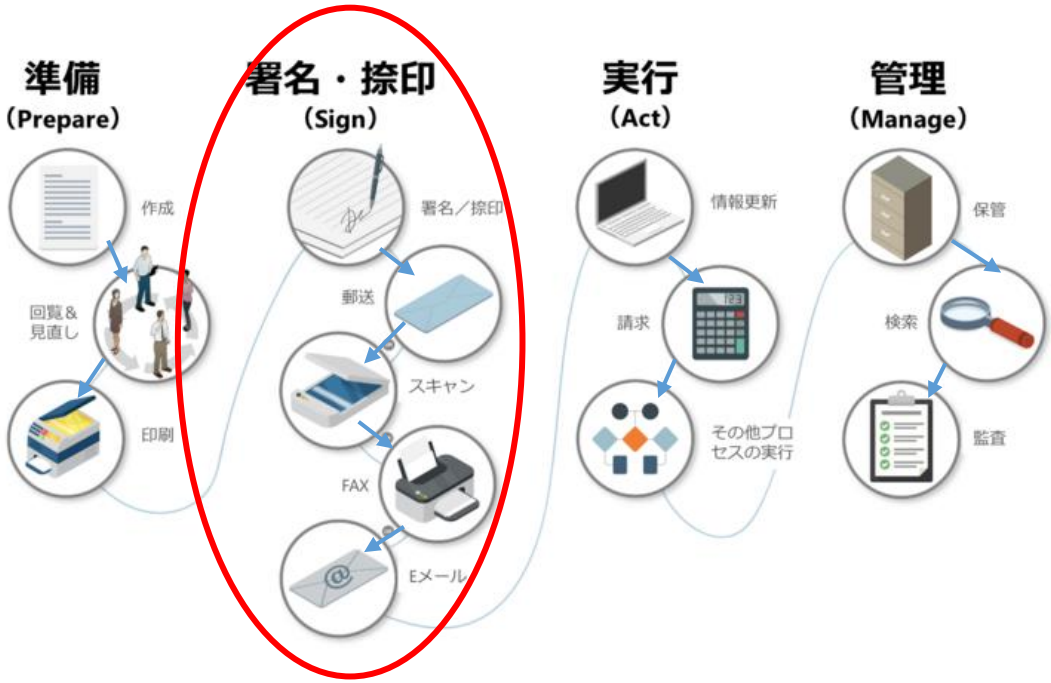
テレワークで得られるメリットは多いことを理解し、前向きな意識を持ってもらう。
（マネージャー、上司の役割は大きい）

- 育児や介護と仕事の両立がしやすくなる。
- 通勤時間の削減による、プライベートな時間を作り出せる。
- 時間外労働が少なくなる。
- 自分の裁量で業務に取り組める。



いつもの仕事（業務フロー）の見直し

1. 業務フローを見直し、紙書類のデジタル化を検討する。
   - どのような業務フローなのか
   - 業務に必要な書類は紙種類かデジタル化されているか
   - その文書に署名、押印が必要なのか
   - その業務は必要なのか、無駄がないか



紙書類をデジタル化してテレワークへ

2. 現存する紙の書類をデジタル化する。
   - デジタル化できる紙の種類と紙保存が必要なものに分ける。
   - **スキャナ**を使って紙の書類をデジタル化する。
   - Faxは複合機の機能やクラウド型Faxサービスを使ってデジタル化する。
3. デジタル化した書類へのアクセスを整備する。
   - データの保管場所を整備
   - アクセス権の設定
4. デジタル化された書類を使う業務フローへ改善！

テレワークを実施することにより、業務フローの改善とIT化の促進につながります！

テレワークに必要なICT環境とは

ITツール

- 業務処理系 ITツール
- コミュニケーション・情報共有系 ITツール
- 勤怠管理系 ITツール

ハードウエア

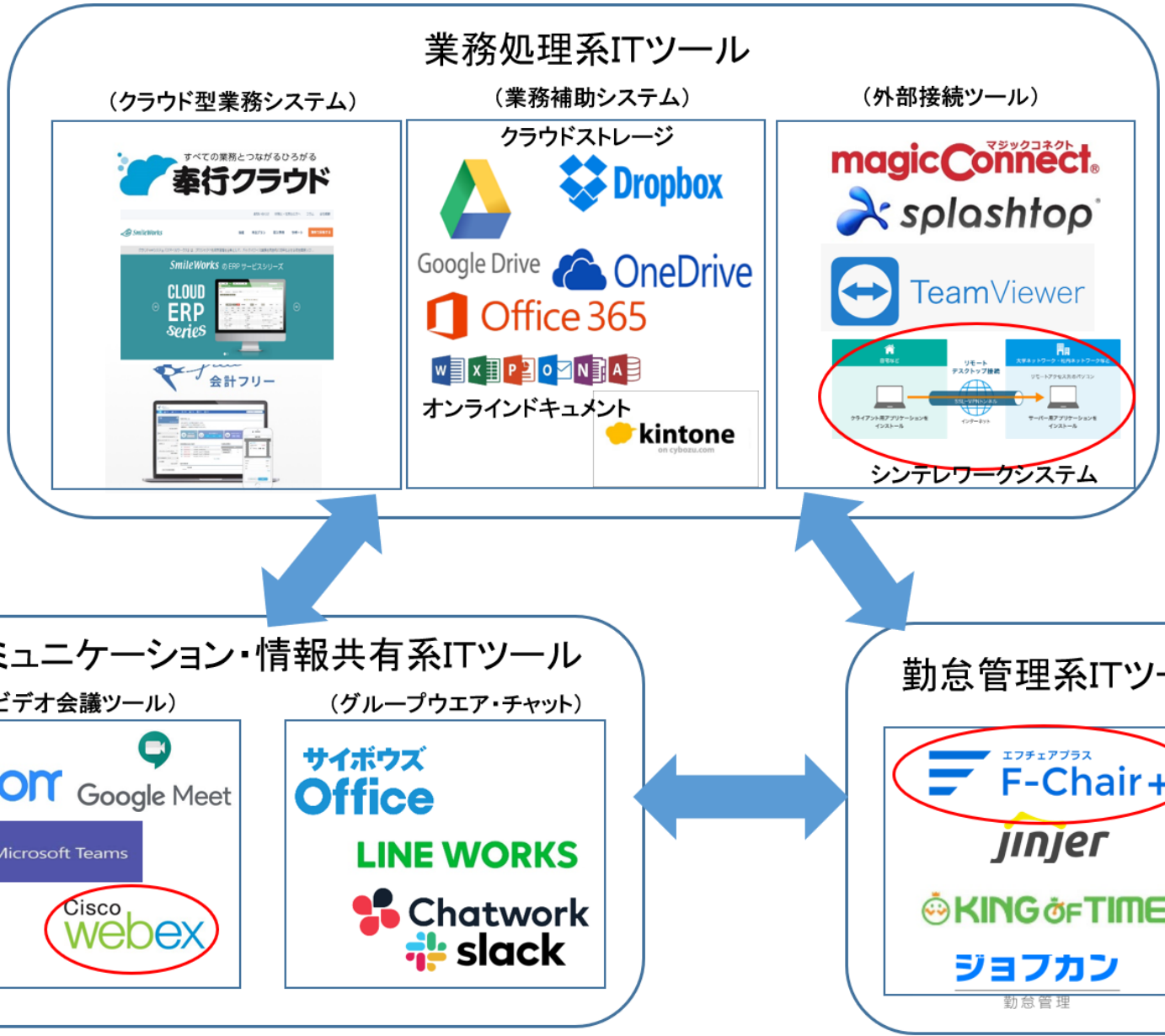
- BYOD＊
- 会社の自席PCを持ち出し
- テレワーク専用機

ネットワーク

- 自宅のネット環境
- 貸与Wifiルーター
- スマホのテザリング

＊BYOD（Bring Your Own Device）：自分の機器を業務に活用する仕組み

テレワークに必要となるITツール

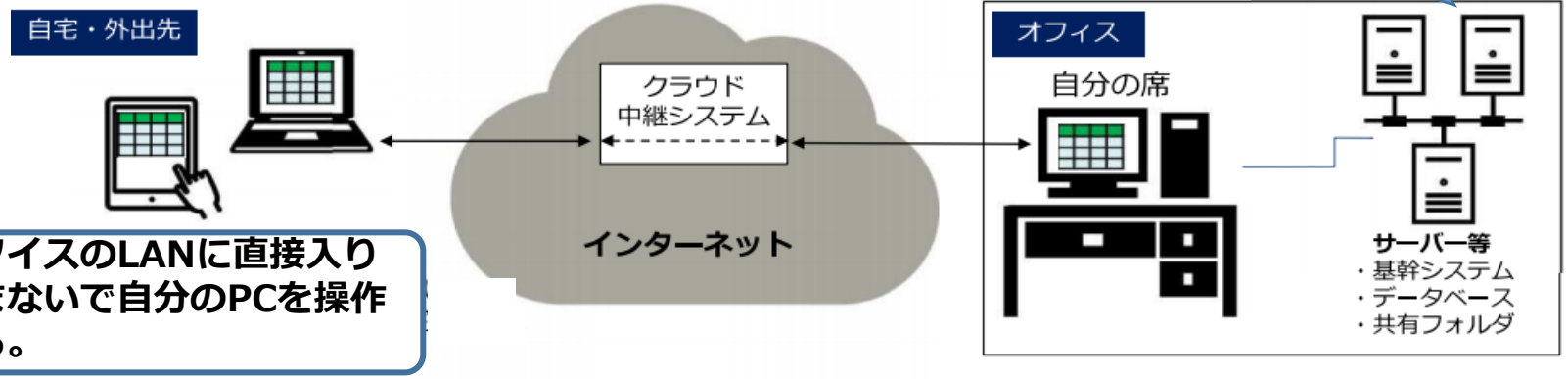


テレワークで社内に接続する方法

② 仮想ディスクトップ方式

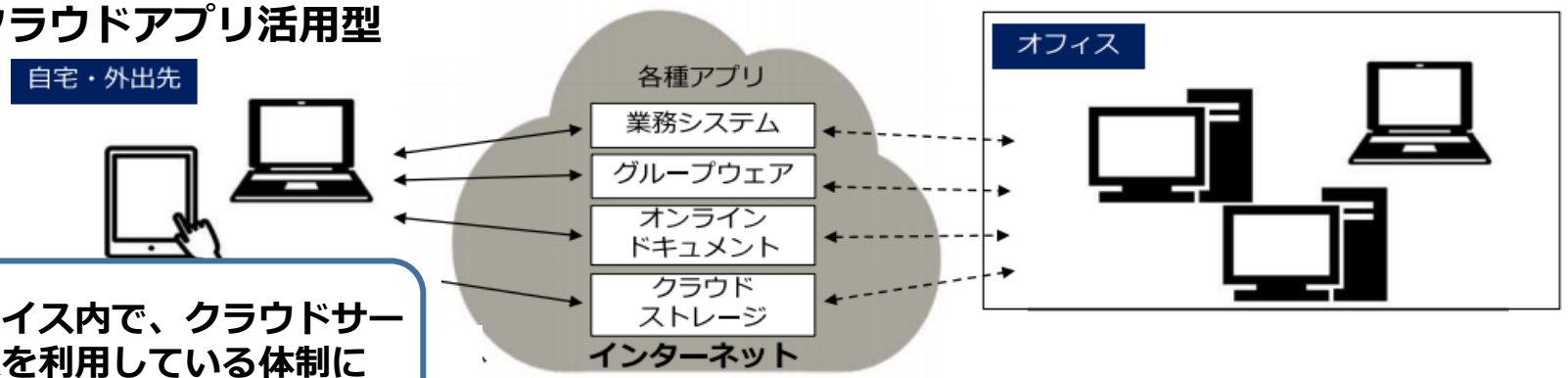
サーバー上の従業員に割り当てられた仮想ディスクトップに接続する方式

① リモートディスクトップ型



オフィスのLANに直接入り込まないで自分のPCを操作する。

③ クラウドアプリ活用型



オフィス内で、クラウドサービスを利用している体制になっている場合は、社内でも社外でも同様な業務が可能

リモートデスクトップ型接続に必要なITツール

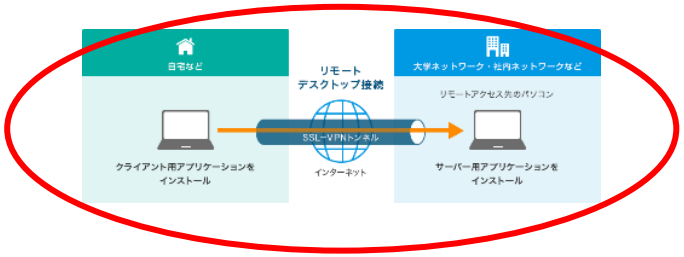
リモートデスクトップ型ITツール

会社のPCやサーバーに社外から安全（VPN接続）にアクセスできる
リモートアクセスサービス

magicConnect マジックコネクト

splashtop

TeamViewer



シン・テレワークシステム

リモートデスクトップ型接続事例
（シン・テレワークシステム）

NTT東日本について　NTT東日本の取り組み　公開情報

ホーム > … > 2020 > 4月

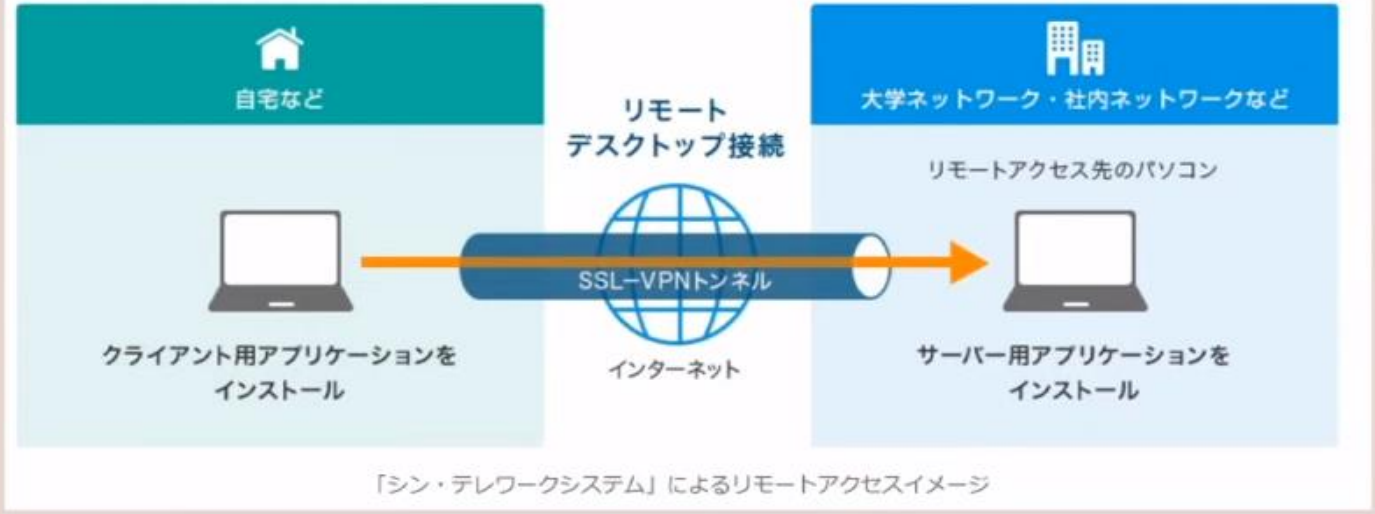
(報道発表資料)

2020年4月21日
東日本電信電話株式会社

NTT東日本とIPAによる「シン・テレワークシステム」の緊急構築と無償開放について
～職場や大学のパソコンに自宅から安全にアクセスし在宅勤務や研究等の継続が可能～

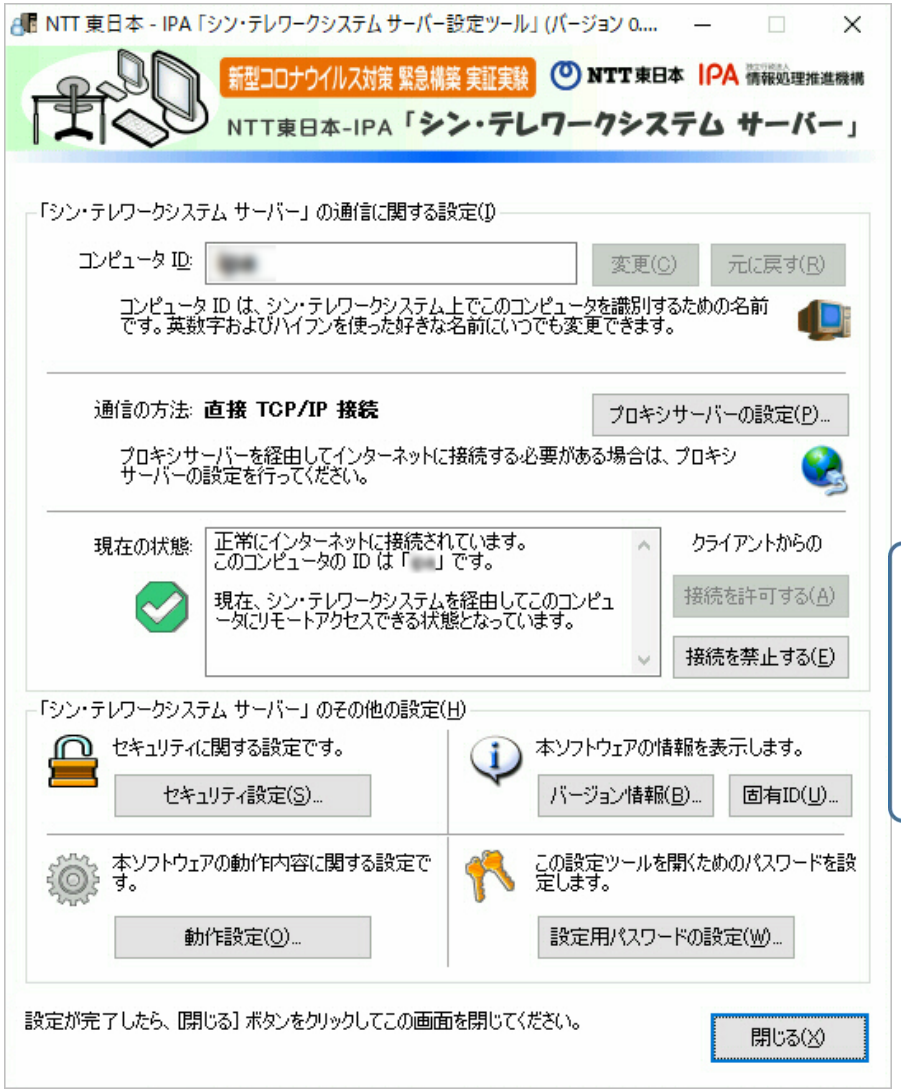
2020年10月31日まで、
実証実験として開放

⇒2021年10月31日まで
無償継続延長されました！



「シン・テレワークシステム」によるリモートアクセスイメージ

リモートデスクトップ型接続事例
（シン・テレワークシステム）



グローバルIPやルーター／ファイアウォールの設定は一切不要で、各種インターネット回線でも利用可能となっています。
このように、いろいろな制約を取っ払ってあるので、設定や接続がすごく簡単です。

会社のPCのデスクトップ環境を自宅等のテレワーク端末から遠隔で操作

クラウドアプリ型接続に必要なITツール

クラウドアプリ型ITツール
インターネット環境があればどこからでも使える **クラウド型の業務システムや会計ソフト**など  すべての業務とつながるひろがる 奉行クラウド 
Excelの代わりに使える **クラウドデータベース**や**オンラインドキュメント**など kintone on cybozu.com Office 365 Outlook OneDrive Word Excel PowerPoint OneNote SharePoint Microsoft Teams

クラウドアプリ活用型の接続イメージ

接続するネットワーク環境

インターネット接続
接続が安定している **自宅のインターネット回線**
料金分担を明確にしやすい **モバイルWi-Fiルータ**
手っ取り早い **スマートフォンのテザリング** ⇒電話併用での長時間利用はバッテリーを消耗します。
無料で使える **公衆Wi-Fi** ⇒盗み見や不正アクセスされる可能性があり、お薦めでみません。

情報共有のためのITツール

データファイル共有
OneDriveやDropbox、Googleドライブなどの**クラウドストレージやグループウエア** ⇒オフィス内で、ファイルサーバーやNASが構築できている場合は、外部で利用する人向けに同期（バックアップ）させることもできます。

コミュニケーションをとるためのITツール

電子メール・チャット
スマホや事務所外のPCで、送受信できる**WEBメール**     ⇒特定のPC以外からも、メールの送受信が可能
LINEやGhatworksなどの**チャットツール**や**グループウエア**        ⇒リアルタイムにコミュニケーションをとりたいときには、 チャットツールが有効です。

コミュニケーションをとるためのITツール

会議システム・商談システム
自宅や出先にいても会議ができる**WEB会議システム** Cisco webex　zoom　Google Meet　Microsoft Teams
電話に代わる、顧客との**WEB商談システム**

コミュニケーションをとるためのITツール

電話・FAX
スマートフォンに会社の電話を転送したり、会社番号で発信したり、内線利用として使える**クラウド型ビジネス電話** 
会社に送られたFAXを外部や自宅で受信したり、外部や自宅からFAX送信したりできる**インターネットFAX** 

勤怠や業務を管理するためのITツール

勤怠管理と業務管理
どこからでも勤怠記録ができる**クラウド型勤怠管理システム** エフチェアプラス F-Chair+ KING OF TIME jinjer ジョブカン 勤怠管理 ⇒管理し過ぎないマネージメントを心がけましょう。 • テレワーク実施者は過度に管理されているとストレスになります。 • マネージャーにとっても管理に時間を取られることは、負担になります。

勤怠管理ツールの実例


F-Chair+
LLC
横屋俊一
退席する
着席中
着席する
退席中
6:12
退席する
着席中
8:35
細切れの業務時間も集計
着 退 129分
08:54 11:03
着 退 114分
12:58 14:52
着 退 130分
16:02 18:12
勤務時間 6時間13分
横屋俊一
日次 月次
2020/04/29 水
翌日
在席データ一覧
08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00
着 退 15分
12:59 13:14
着 退 97分
13:30 在席中
合計
画面
外出先からも確認できる！
09:00
退席中 山田 (5時間23分)
退席中 鈴木 (7時間13分)
退席中 田中 (9時間31分)
作業画面の自動撮影
17:37
17:45
キャプチャされた
画面で仕事内容を
共有

新しい勤務形態のルールを整える

就業規則の整備（届出要）	運用ルールの整備（届出不要）
就業規則（本則） 就業規則（本則）にテレワークに関する基本事項をテレワーク勤務規定を追加する。 **テレワーク勤務規定** • テレワークを実施する場所 • 日数、時間 • 対象者や業務 ・申請方法、連絡方法など	**テレワークの手引き** テレワーク実施の運用ルール説明資料 • 始業、終業報告 • 勤怠管理 • コミュニケーションの取り方 • トラブル時の対応円滑に関するポイント • Q&A集 • テレワーク実施時のセキュリティ・ルール

- テレワーク導入のための労務管理等Q&A集（厚生労働省）
https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/RomuQA.pdf

- テレワークモデル就業規則～作成の手引き～（厚生労働省）
https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/TWmodel.pdf

セキュリティ対策

1. ルールによるセキュリティ対策
   - 情報セキュリティ対策のうち、実施が最も難しいのは「人」の部分です。
   - 情報セキュリティガイドラインを定め、テレワーク実施者に遵守してもらう。
   - ルールを定着させるには、従業員への教育やルールの遵守が自分にとってメリットになることを自覚してもらうこ。
2. 技術的なセキュリティ対策
   - ネットワーク接続のセキュリティ対策
   - 会社のデータにアクセスする権限の対策
3. 物理的なセキュリティ対策
   - 紙書類、データ・ファイルの持ち出し、会社PC持ち出しに対する対策

ルールによるセキュリティ対策

セキュリティガイドライン　事例

※赤字は第4版改定で追加した項目

経営者が実施すべき対策

（情報セキュリティ保全対策の大枠）

1. 経営者は、テレワークの実施を考慮した情報セキュリティポリシーを定め定期的に監査し、その内容に応じて見直しを行う。
2. 社内で扱う情報について、その重要度に応じたレベル分けを行った上で、テレワークでの利用可否と利用可の場合の取扱方法を定める。
3. テレワーク勤務者が情報セキュリティ対策の重要性を理解した上で作業を行えるようにするため、定期的に教育・啓発活動を実施させる。
4. 情報セキュリティ事故の発生に備えて、迅速な対応がとれるように連絡体制を整えるとともに、事故時の対応についての訓練を実施させる。
5. テレワークにおける情報セキュリティ対策に適切な理解を示した上で、必要な人材・資源に必要な予算を割り当てる。

システム管理者が実施すべき対策

（情報セキュリティ保全対策の大枠）

1. システム全体を管理する重要な立場であることを自覚
シーに従ってテレワークのセキュリティ維持に関する技
期的に実施状
2. 情報のレベル分 アクセス制御、暗号化の要否や印刷可否などの
3. テレワーク勤務者の情報セキュリティに関する認識を確実なものにするために、定期的に教育・啓発活動を実施する。
4. 情報セキュリティ事故の発生に備えて、迅速な対応がとれるように連絡体制を確認するとともに、事故時の対応についての訓練を実施する。

（マルウェアに対する対策）

5. フィルタリング等を用いて、テレ クセスしないように設定する。
6. テレワーク勤務者がテレワーク ルする際は申請させ、情報セキュリティ上の問題が ことを確認した上で認める。
7. 貸与用のテレワーク端末にウイルス対策ソフトをインストールし、最新の定義ファイルが適用されているようにする。
8. 貸与用のテレワーク端末のO デートを行い最新の状態に保つ。
9. 私用端末をテレワークに利用 報セキュリティ対策が施されていることを確認させた 認める。
10. ランサムウェアの感染に備え、重要な電子データのバックアップを社内システムから切り離した状態で保存する。
11. 金融機関や物流業者からの事務連絡を装うなどの不審なメールが迷惑メールとして分類されるよう設定する。

（端末の紛失・盗難に対する対策）

12. 台帳等を整備し、貸与するテレワー 理する。

（重要情報の盗聴に対する対策）

13. テレワーク端末において無線LANの脆弱性対策が適切に講じられるようにする。

（不正アクセスに対する対策）

14. 社外から社内システムへアクセスするための利用者認証について、技術的基準を明確に定め、適正に管理・運用する。
15. レワーク勤務者がインターネット経由で社内システムにアクセスする際のアクセス方法を定める。また、社内システムとインターネットの境界線にはファイアウォールやルータ等を設置し、アクセス状況を監視するとともに、不必要なアクセスを遮断する。
16. 社内システムへのアクセス用のパスワード ことができないように設定する。

（外部サービスの利用に対する対策）

17. メッセージングアプリケーションを含むＳＮＳに関する従業員向けの利用ルールやガイドラインを整備し、その中でテレワーク時の利用上の留意事項を明示する。
18. ファイル共有サービス等のパブリッククラウドサービスの利用ルールを整備し、情報漏えいにつながる恐れのある利用方法を禁止する。

情報・データのアクセス管理

従業員に対する教育・啓発活動

WEPやWPA方式による無線LAN

テレワーク端末にはウイルス対策ソフトの導入

重要なデータのバックアップ

SNSやファイル共有サービスの使用ルール

出典：一般社団法人日本テレワーク協会　https://japan-telework.or.jp/tw_about-2/guide/

ルールによるセキュリティ対策

セキュリティガイドライン　事例

テレワーク勤務者が実施すべき対策

（情報セキュリティ保全対策の大枠）

1. 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、情報セキュリティポリシーが定める技術的・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。
2. テレワークで扱う情報について、定められた情報のレベル分けとレベルに応じたルールに従って取り扱う。
3. 定期的に実施される情報セキュリティに関する教育・啓発活動に積極的に取り組むことで、情報セキュリティに対する認識を高めることに務める。
4. 情報セキュリティ事故の発生に備えて、直ちに定められた担当者に連絡できるよう連絡体制を確認するとともに、事故時に備えた訓練に参加する。

（マルウェアに対する対策）

5. マルウェア感染を防ぐため、ＯＳやブラウザ（拡張機能を含む）のアップデートが未実施の状態で社外のウェブサイトにはアクセスしない。
6. 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。（私用端末利用の場合）テレワークで利用する端末にインストールするアプリケーションは、安全性に十分留意して選択する。
7. 作業開始前に、テレワーク端末にウイルス対策ソフトがインストールされ、最新の定義ファイルが適用されていることを確認する。
8. 作業開始前に、テレワーク端末のＯＳ及びソフトウェアについて、アップデートが適用され最新の状態であることを確認する。
9. テレワークにはルールに定められた情報セキュリティ対策が適用さ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（脱獄、root化等）を施さない。
10. テレワーク作業中にマルウェアに感染した場合、その報告漏れや遅れが被害拡大につながる恐れがあることを自覚し、電子メールの添付ファイルの開封やリンク先のクリックに一層の注意を払う。

（端末の紛失・盗難に対する対策）

11. オフィス外に情報資産を持ち出すとき、その原本を安全な場所に保存しておく。
12. 機密性が求められる電子データを極力管理する必要が無いように業務の方法を工夫する。やむを得ない場合は必ず暗号化して保存するとともに、端末や電子データの入った記録媒体（ＵＳＢメモリ等）等の盗難に留意する。

（重要情報の盗難に対する対策）

13. 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。
14. 無線LAN利用に伴うリスクを理解し、テレワークで利用する場合は確保すべきセキュリティレベルに応じた対策が可能な範囲で利用する。
15. 第三者と共有する環境で作業を行う場合、端末の画面にプライバシーフィルターを装着したり、作業場所を選ぶ等により、画面の覗き見防止に努める。

（不正アクセスに対する対策）

16. 社外から社内システムにアクセスするための利用者認証情報（パスワード、ＩＣカード等）を適正に管理する。
17. 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アクセス方法のみを用いる。
18. テレワークで使用するパスワードは、使い回しを避け、一定以上の長さで他人に推測されにくいものを用いるように心がける。

（外部サービスの利用に対する対策）

19. メッセージングアプリケーションを含むＳＮＳをテレワークで利用する場合、社内で定められたＳＮＳ利用ルールやガイドラインに従って利用するようにする。
20. テレワークでファイル共有サービス等のパブリッククラウドサービスを利用する場合、社内ルールで認められた範囲で利用する。

テレワーク実施者が行うべき対策

テレワーク実施者のガイドライン（例）
• 新しくアプリケーションをインストールする場合には、システム管理者に申請する。 • 端末に最新のウイルス対策ソフトがインストールされていることを確認する。 • 端末のOS及びソフトウエアについて、最新の状態であることを確認する。 • マルウエアに感染した場合、報告の遅れが被害拡大につながる恐れがあることを自覚する。 • 電子メールの添付ファイルの開封やリンク先のクリックに注意を払う。 • 機密性が求められる電子データを送信するときは、必ず暗号化するかパスワードを設定する。 • 周りに第三者がいる場所で作業するとき（ZOOM等のビデオ会議システムなども含む）は、端末の画面の覗き見防止フイルターを装着する。 • 作業している時のSNS投稿は、端末画面の映り込みによる情報漏えいのリスクがあるため、避ける。 • 社内システムにアクセスするためのIDやパスワードは適正に管理する。 • パスワードは使い回しを避け、一定以上の長さで他人に推測されにくいものを使うように心がける。

システム管理者が行うべき対策

技術的セキュリティ対策①

ネットワークセキュリティ対策	対策のポイント
社外からのアクセスは暗号化されたデータ通信**VPN接続**によるリモートディスクトップ方式にする。	
外部サービスの利用やGoogleDriveなどのパブリッククラウドの利用には、暗号化されたクラウドサービスを使用してもらう。	• 暗号化されているGoogleDrive、Dropbox、OneDorive、BOXなどの利用可能なサービスを定めておく。
無線LAN利用	• 自宅等で利用するアクセスポイント、Wifiルータの設定は暗号化（WPA3、WEPなど）を行うよう指導する。 • 公衆Wifiの利用は禁止する。

システム管理者が行うべき対策

技術的セキュリティ対策②

アクセス権限の対策（本人認証）	対策のポイント
社外からの不正アクセスを防止するため、下記の二つの本人認証のための対策をとる。 **1．多要素認証**	• 認証の3要素である「知識情報」、「所持情報」、「生体情報」の中から2つ以上を組み合わせて認証を行うもの。 • IDやパスワード（知識情報）でログイン後に、自分自身のスマートフォンのSMSにコード（所持情報）が届く仕組みです。
2．端末認証	• あらかじめ登録されている端末からのみアクセスを可能にする。

システム管理者が行うべき対策

物理的セキュリティ対策③

紙資料、USB、PCなどからの情報漏洩対策	対策のポイント
紙資料 USB、PC、タブレット、スマホ	• 紛失や盗難を防ぐためには、出来るだけ紙資料を電子化して、紙書類を社外に持ち出さないようにする。 • 紛失や盗難にあったときの情報漏洩のリスクを考え、これらの機器によって持ち出すファイルを暗号化する。また端末そのものにはパスワード設定や暗号化（ハードディスク暗号化）する。 • スマホにはセキュリティロック機能を掛け、紛失時にはリモートロック機能を使い、利用不可にする。

BYODのセキュリティ対策

個人所有のパソコンやタブレット、スマートフォーンを業務で利用するときは、端末の状況に管理が行き届かず、マルウエアに感染するリスクが高まります。

BYODのセキュリティ対策	対策のポイント
システム管理者が行う対策	• 個人所有の端末の利用は許可制にし、許可を受けた端末のみ、社内への接続が出来るようにする。 • 管理者による端末の接続のとき、管理者は端末のセキュリティ対策の状況をチェックするようにする。 • BYODの利用規則を定める。
BYODの利用者が行う対策	• OSや使用するアプリはアップデートを行い、最新の状態にしておく。 • ウイルス対策ソフトを導入し、最新のパターンファイルを適用する設定を行っておく。

- テレワークセキュリティガイドライン（総務省）

https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/Security.pdf

テレワークに関する参考資料

- テレワーク実践活用 テキストブック（総務省）
http://teleworkkakudai.jp/expert/pdf/text-book_2019.pdf

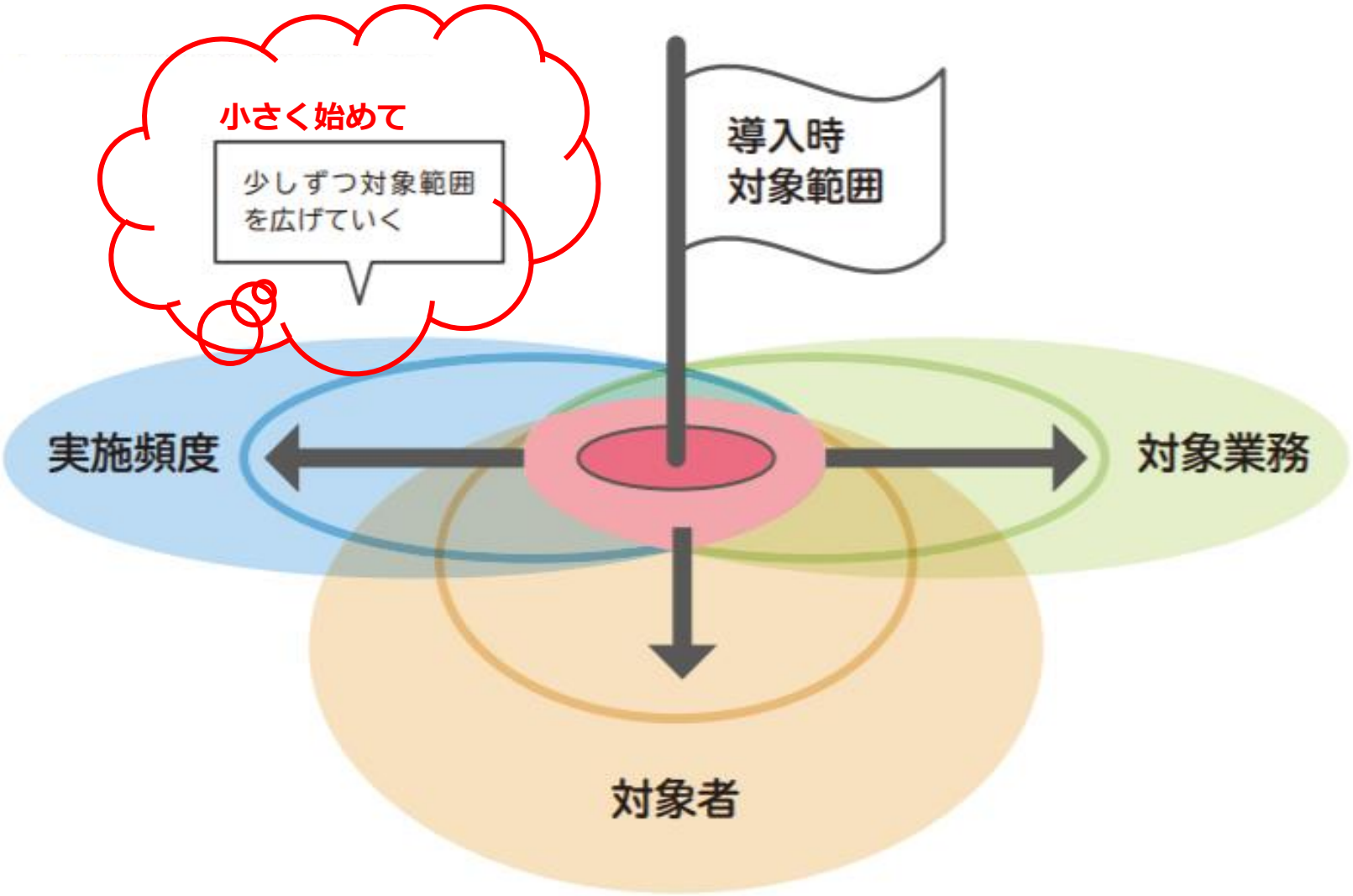
- テレワークの導入・運用ガイドブック（厚生労働省）
https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/H28hatarakikatakaikaku.pdf

- テレワーク導入のための労務管理等Q&A集（厚生労働省）
https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/RomuQA.pdf

- テレワークモデル就業規則～作成の手引き～（厚生労働省）
https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/TWmodel.pdf

- テレワークセキュリティガイドライン（総務省）
https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/Security.pdf

まとめ



ご清聴　ありがとうございました。