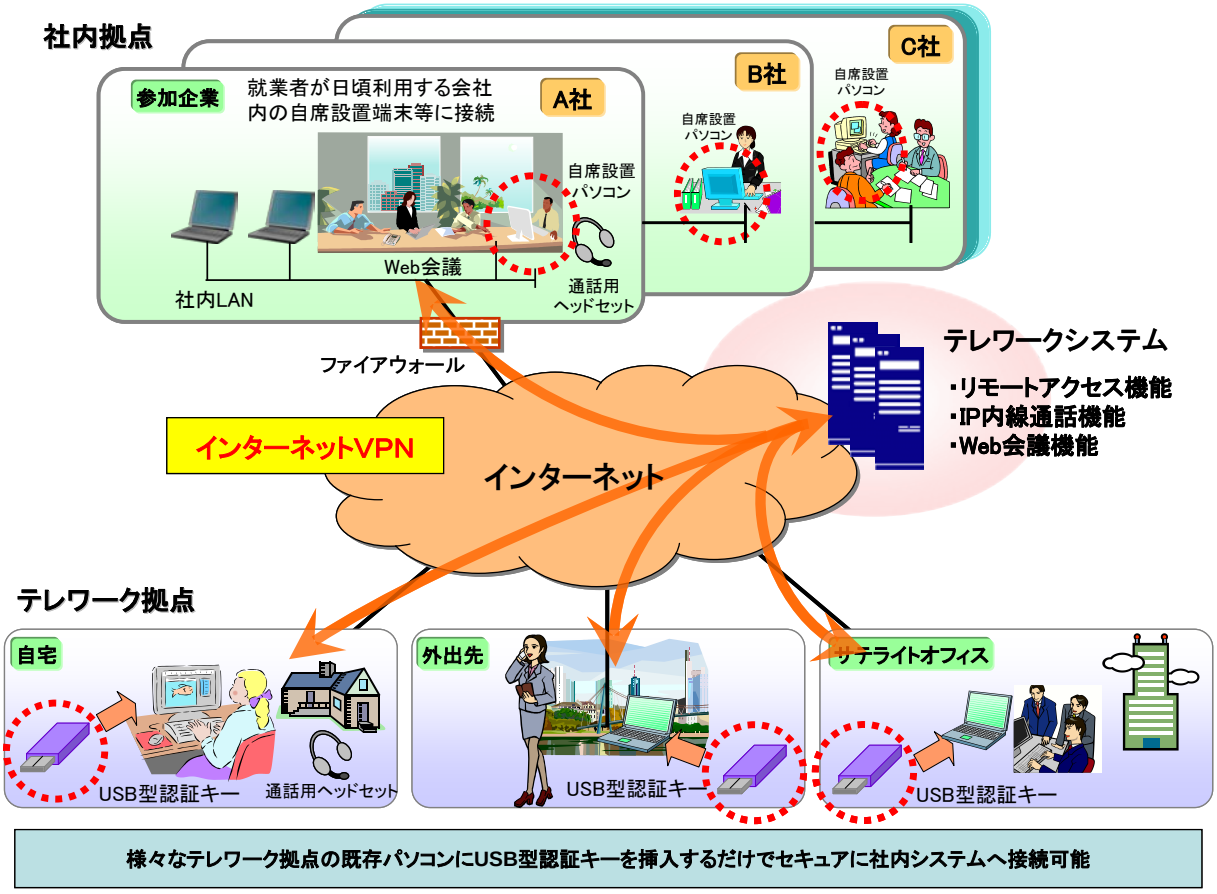
（ 別 紙１ ）

テレワーク試行・体験プロジェクトの概要

テレワーク試行・体験プロジェクトとは

テレワーク試行・体験プロジェクトとは、総務省及び厚生労働省が提供するテレワーク試行・体験システムを活用して、テレワークを行ったことのない多くの企業、地方公共団体等に勤務する社員・職員の方々にテレワーク（在宅勤務、モバイルワーク等）を試行・体験してもらい、テレワークの効果・効用を体感いただくことを通して、テレワークの普及促進を図るものです。

本プロジェクトでは、参加者が実際に業務に日頃使用しているパソコン、ネットワーク、アプリケーションなどの社内環境（社内拠点）と自宅などのテレワーク拠点を接続することで、安全・安心かつ容易に会社と同様の作業ができる環境を実現します。



試行・体験プロジェクトイメージ図

（１）テレワーク試行・体験プロジェクトで提供する機能概要

本プロジェクトでは、参加者に対し、パソコン画面データのみの転送を特徴としたリモートアクセスサービスを提供します。また、希望者には IP 内線電話サービス、Web 会議サービスも併せて提供します。

参加者は、テレワーク拠点であるサテライトオフィスや自宅等の手元端末から、本プロジェクトで配布する個人専用 USB 型認証キーを利用し、インターネットを経由して社内設置の業務用端末または社内システムにセキュアに接続し、パソコン画面データの転送により作業を行うことができます（リモートアクセスサービス）。

また、IP 内線電話サービス希望者は、手元端末から IP 内線電話サービスに接

続し、社内や他のテレワーク体験者との内線通話の発着信が可能となります（IP内線電話サービス）。

Web 会議サービス希望者は、手元端末から Web 会議サービスにセキュアに接続し､社内や他のテレワーク体験者との Web 会議に参加することが可能となります。（Web 会議サービス）

なお、参加者は、ブロードバンドにて Web 閲覧できるパソコン環境であれば本サービスを利用できますので、社内システムやネットワーク環境（既設のファイアウォール／ルータ等）の設定変更等煩雑な作業は不要です。

※　IP 内線電話サービスおよび Web 会議サービスは希望者のみ実施。いずれかのサービスのみ利用可能。

（２）安全性への対策

本プロジェクトでは、安心・安全にテレワークを体験していただくため、以下の安全対策を実施しております。

・ **なりすましによるアクセスの防止**

ユーザー名・パスワード等による認証に加え、個人専用の USB 型認証キー（ハードウェア認証）を採用し、USB 型認証キーなしでは、社内設置業務用端末へアクセスできない仕組みを実現することにより、なりすましによるアクセスを防止しております。

・ **ネットワークでの情報漏えいの防止**

通信を暗号化することにより､通信経路上での情報漏えいを防止しております。

・ **社内情報流出の防止**

テレワーク拠点端末で扱うデータは、社内の自席設置端末等の画面データのみとし、社内のファイルやメールの情報は、一切ダウンロードできない仕組みを実現することにより、テレワーク端末からの情報漏えいを防止しております。

・ **テレワーク端末のウィルス感染による社内ネットワークへの拡大防止**

社内の自席設置端末等の画面データ以外のファイル交換を禁止しているため、テレワーク拠点端末が感染するコンピュータウィルスなどが社内ネットワークへ拡大することを防止しております。