

「ニュー・ノーマル」時代のテレワーク環境

～テレワーク開発環境によるイノベーション促進～

情報サービス産業協会 技術革新委員会

サイバーセキュリティ部会

技術革新委員会サイバーセキュリティ部会名簿

部会長	柴崎 正道	(株)網屋 取締役
委員	北口 仁	(株)エヌアイデイ マーケティング部システム課
	井上 克至	(株)NTTデータ セキュリティ技術部情報セキュリティ推進室 専任役
	木谷 浩	キヤノンマーケティングジャパン(株) サイバーセキュリティラボ
	橋本 賢	(株)JSOL 経営企画本部法務知財部
	渡辺 貴仁	(独)情報処理推進機構 セキュリティセンターセキュリティ対策推進部脆弱性対策グループ グループリーダー
	中村 宏	東芝デジタルソリューションズ(株) 情報セキュリティセンター 戦略企画室室長
	千葉 宣慶	東北インフォメーション・システムズ(株) 営業本部営業企画部セキュリティ推進課 シニアマネージャー
	坪井 正広	(株)野村総合研究所 品質監理本部情報セキュリティ部グループマネージャー
	太田 邦和	(株)リンクレア セキュリティ監理室
事務局	山本 英己	(一社)情報サービス産業協会 企画調査部・国際部

目次

1. 開発業務を推進するためのテレワーク環境構築事例	5
1. 1 急ごしらえのテレワーク環境	5
1. 2 A社テレワーク開発環境の事例	7
1. 3 テレワーク開発環境の構築ノウハウ	13
2. ニュー・ノーマル時代へ	16
2. 1 New Normal / 新しい生活様式	16
2. 2 テレワーク開発環境によるイノベーション促進	16
2. 3 会員のみなさまへ	18
用語集	19

はじめに

2019年12月中国武漢で確認され、湖北省を中心に感染の拡がりを見せた新型コロナウイルスは、2020年1月にとうとう日本へも波及した。その後、欧米など世界各国でも爆発的な感染拡大が現実となり、日本では3月末から東京都、大阪府等大都市圏を起点とした感染拡大が危ぶまれ、4月初旬には政府より緊急事態宣言が発令された。

それを受け、国民は不要不急の外出を自粛し人との接触機会を減らすことで感染確率を極小化するように求められた。感染防止策としてマスク着用、ソーシャルディスタンスの確保に加え、「STAY HOME」と銘打った外出自粛の社会的機運が醸成されるなか最も重要視された施策のひとつが「テレワーク」の活用であろう。

情報サービス産業に従事する我々JISA会員企業にとっては、2020年に予定されていた東京オリンピック・パラリンピックの開催に備え「テレワーク」の実施による勤務形態の多様化は既に企業運営課題のひとつであった。

しかしながら、オリンピック・パラリンピックの開催を目前に控え、その取り組みを本格化していこうという矢先にパンデミック対策として一気に「テレワーク」が浮上してきたわけである。

JISA会員企業においては、ほぼ全社員に近い比率でテレワーク環境の整備を済ませた企業もあれば、一部は検証を進めていたものの全社的なテレワークの実施体制は整っておらず、試行錯誤を繰り返しつつ急遽全社展開を進めるに至った企業もあったと聞く。

日本における爆発的な感染拡大の危機を何とか回避したと思われる今、GDPのマイナス成長が見込まれるほど落ち込みを見せた経済をどう回復させていくかが政治経済界の重要課題として注目を集めている。経済の刺激策が功を奏し、回復基調が予見できたとしても、ワクチン開発の目途が立たない限り、感染の第2波、第3波が到来することや新たな感染症の発生についても将来の脅威として考慮しておかなければならない。

そこで今「ニュー・ノーマル」と呼ばれる、ウイルスとの社会的共存を目指す新しい生活様式が提唱されるに至った。それは、ウイルスの感染拡大を避けつつ、経済の復興を段階的に実現していくための社会生活のあり方を象徴する概念である。我々企業人にとって、そのような生活様式の代表が「テレワーク」であり、多様性に満ちた新たな勤務形態によってこれまでにないイノベーションを産み出していくであろう未来像が今こそ志向されているのである。

「ニュー・ノーマル」を社会生活に溶け込ませるためには、「テレワーク」を事業継続上の手段として考えるのみならず、イノベーションを育む生産環境として位置づけることが重要であろう。

我々JISA サイバーセキュリティ部会においては、来るべき「ニュー・ノーマル」の時代を見据え、「テレワーク」を推進するためのベストプラクティスを会員諸氏に紹介することで少しでも業界の進展に寄与できればと考える次第である。

1. 開発業務を推進するためのテレワーク環境構築事例

1. 1 急ごしらえのテレワーク環境

2020 年東京オリンピック・パラリンピックが予定通りの開催であれば、半年後でよかった・・・

都内の企業、特に競技会場に近い場所の企業は、開催時の混雑回避に備えてテレワークの準備を進めてこられたことと思う。しかし、新型コロナウイルスにより東京大会は延期、さらに「緊急事態宣言」発出により急遽首都圏すべての企業で在宅勤務を余儀なくされた。ウイルス終息の先行きが見えないいま「緊急事態宣言」は解除となったが、当面の間は在宅勤務を継続される企業も多いのではないだろうか。

東京都が5月11日に発表した新型コロナウイルス感染症対策本部報（第330報）¹によると、都内企業（従業員30人以上）のテレワーク導入率は3月から5月にかけて2.6倍と急増している。業種別にみると、事務・営業職が中心の業種（情報通信業、金融・保険業等）が76.2%、現場作業や対人サービスが中心となる業種（建設・製造、運輸・郵便、医療・福祉、飲食・宿泊、小売業等）が55%となっており、従来テレワークが難しいと思われていた業種においても感染防止のために急ぎ対応しなければならなかった状況がうかがえる。

ひとことにテレワークと言っても、作業内容によって技術的な難易度は異なる。たとえば文書作成やメールやり取りなどPC処理が比較的軽い作業や、オフライン中心の作業で必要に応じてネットワーク接続すればよい場合、手持ちのPCを暗号化してVPN接続するといった方法で十分対応できるであろう。個人所有PCや自宅Wi-Fiでの業務を許可するかは、会社規則などと折り合いが必要と思われる。接客や面接など対面性を重視する業務の場合も、ビデオチャットやWebミーティングを活用することである程度の運用が可能になる。しかし、テレワークだけで完結できない部分も多々あるため、例えば密を避けつつ一定期間ごとに少人数単位で物理的に顔を合わせるといった対応を組み合わせる必要もあるだろう。

直接業務がテレワーク可能であっても、勤怠管理や交通費などの経費管理、人事関連の申請といった間接業務を行う社内システムに直接アクセスするために出社を避けられないケースもある。従来の社内システムは会社に来ることが前提、すなわち社内ネットワークからの接続のみを考慮した構成であることが多い。そこでインターネットから安全にアクセスできるように構成変更するか、間接業務そのものをクラウドサービスに移行する方法が考えられるがいずれも短期間での実施は難易度が高い。勤怠管理のために月末は必ず出社しなければならない方も多いのではないだろうか。このように、ウイルスから避難するためのテレワーク化は、みんなで会社に集まって業務を行うメリットをそぎ落していくイメージが強く、利便性悪化や生産性低下もやむを得なかったかもしれない。

なかでも製品やサービスを生み出す開発作業は、テレワークが困難な業務のひとつであ

ろう。そもそも実機を持ち出せないなど、リモートワーク対応が不可能なケースも考えられる。また、従来の開発環境とテレワーク開発環境が完全同一にできなかった場合、画面レイアウトやタイミング、パフォーマンス調整などに差異が発生し、最終納品で何をどれだけ検証すればよいのかといった懸念も出てくるであろう。

開発規模やターゲット（クラウドで稼働するもの、Windows や Android アプリ、組み込み機器やドライバ等）によっても異なるが、開発環境は以下のような点で一般業務環境と異なる。

- ・ 処理能力の高い PC や Windows 以外の OS、複数台のサーバー構成等が必要
- ・ ソースコードや顧客預かりデータなど機密性の高い情報を取り扱う

そこで情報漏えい対策のためにも、通常時から業務用 PC と開発用 PC を分離している企業も多いと思われる。また、一般業務用 PC はコスト削減のために比較的低スペックで、開発作業に耐えられないのではないだろうか。つまり開発用テレワーク環境は、一般業務用テレワーク環境とは別に設けるとするのが当たり前と考えられる。

一方で、Web アプリケーションなどクラウド上で稼働するものは、開発もクラウド上で行うのが一般的である。クラウド開発環境は、仮想技術を用いて複数台構成や異なる OS 環境を組み合わせるなど、必要な処理に応じてサーバー資源を増減させることができるため自由度が高い。また、プロジェクト内で協調作業を行うためのコミュニケーション支援機能やバグトラッキングなどを備え、うまく活用すれば外部委託先と機能/フェーズ分担する場合などにも対応できると考えられる。また、24 時間 365 日いつでもどこからでも同じ環境にアクセスできるのもメリットである。では、緊急事態宣言以前よりクラウド開発環境を活用されていた企業は、開発作業の在宅勤務化をスムーズに行うことができたであろうか。

クラウド開発環境へ接続するにはアカウントや権限が必要であるが、IDaaS（クラウド上の ID 管理サービス、シングルサインオン等を提供）を利用していない場合は、個々の案件やプロジェクト毎に ID を管理することになる。そのような場合、自宅から直接クラウド開発環境へアクセスできるようになると、深夜など所定の時間帯外に業務を行うことも可能であり、上長が勤務実績を把握するためには個々のプロジェクト環境でアクセスログと勤務報告を突き合わせるなどの手間がかかることになる。テレワーク全般に言えることであるが、いわゆる 9 時から 5 時の時間労働を前提とすると、勤務実績の把握ができるようにシステム上の考慮も必要となる。

このように、テレワーク開発環境においては情報漏洩対策などの＜機密性＞はもちろんのこと、業務効率をできるだけ低下させないための＜可用性＞、さらには従来の開発環境と全く同じ成果物が生み出せる＜完全性＞の 3 つの観点が重要である。

1. 2 A社テレワーク開発環境の事例

[システムインテグレーターA社の事例]

ここで、5年以上前からテレワークを推進してきたA社のモデル事例をご紹介します。

システムインテグレーター A社

従業員： 社員 1, 000 名以上 （パートナ社員除く）

事業所： 首都圏、関西、中部

コンサルティング、システム構築、運用まで一貫サポート

ご承知の通り、2020 東京オリパラ会場周辺は普段から通勤混雑が激しく、さらに大会期間中は競技者及び運営、観戦者などであふれかえることが予想されている。そこで東京都からの要請で期間中の交通対策ⁱⁱが行われ、会場への立ち入りや付近の通過交通を制限する「進入禁止エリア」などが設置される。A社通勤経路はこれらのエリアに含まれており、いわば大会期間中の出社を政府から制限されている状態であり、テレワークが必須の企業の一つである。A社では、大会期間中にテレワーク実施や夏季休暇取得を推奨し、出社率 50%以下とする目標を掲げている。

A社では 2015 年頃から本格的に在宅勤務ができるような環境づくりを進めており、2019 年以降は営業担当者が社外から社内 OA システムをリモート操作できるようになっている。

このときの構成は、社内物理サーバー上に各人用の仮想環境（VDI）を割り振って、シンクライアント+携帯電話テザリングから接続。現在は VPN により自宅 Wi-Fi からの接続も可能となり、シンクライアントが 1 台あれば、社内、自宅、モバイル環境全てで何処にいても遜色なく OA システムにアクセスできるようになった。

A社ではテレワーク推進の前段階として、基幹ネットワークの拠点集約、一斉アクセスによる VPN / ネットワーク負荷テストなどを重ねて準備を進めてきた。最終的には VPN アクセスポイントを複数箇所とし、VPN ライセンスは社員と契約社員全員を賄える数の構成となり、オリパラ大会終了後もテレワーク継続を見据えた規模となっている。

図) テレワーク環境構築の過程

第 1 段階 ~2015 年	目的	営業が社外・お客様先から社内システムを利用して効率アップ
	達成	自分の PC からリモートデスクトップ接続 一部の営業担当者は直行直帰が可能に
第 2 段階 2015 年	目的	業務用 PC Windows 7 移行にあわせてシンクライアント化 VDI で統一することでクライアント保守性アップ
	達成	● 営業担当者が社外から社内システムをリモート操作 ● 社内物理サーバー上に各人用の仮想環境（VDI）を割り振っ

		て、シンククライアント+携帯電話テザリングから接続
第3段階 2017年	目的	オリパラに向けて全社員がどこからでも業務可能に 業務用 PC Windows 10 シンククライアント移行
	達成	● シンククライアントが1台あれば、社内、自宅、モバイル環境全てで何処にいても遜色なく OA システムにアクセスできる ● ビデオ会議やチャットなどのコミュニケーションツールも VDI 環境から利用可能 ● VPN により自宅 Wi-Fi からの接続も可能、VPN アクセスポイント複数箇所、全社員分の VPN ライセンス数
第4段階 ～現在	目的	開発環境を VDI で構築
	達成	● 開発業務のテレワーク化

〔働き方改革がテレワークを後押し〕

テレワークを推進するもう一つの理由に「働き方改革」がある。2019 年から「働き方改革を推進するための関係法律の整備に関する法律」が順次施行され、ワークライフバランスを重視し、通勤時間をなくして自宅で勤務するなど、仕事をこなしつつ育児や家庭コミュニケーションを充実させるための施策である。

政府においては、働き方改革を重要政策の一つと位置づけている。JISA においては 2017 年 4 月、働き方改革宣言ⁱⁱⁱを発表し、翌 2018 年 3 月、会員企業 88 社の賛同をえて企業名を公表した。宣言は、「宣言文」「JISA 会員企業の実践プロセス」「JISA の実践プロセス」から構成され、会員企業の実践プロセスとしては、以下から成り立っている。

第1フェーズ	健康経営の実現（労働日数の削減、労働時間短縮、休暇取得の促進等）
第2フェーズ	スマートワークの実現（脱時間労働への変革、ICT を活用した働き方の実現（2020 年までにテレワーク率 20%を目標）、ダイバーシティの実現
第3フェーズ	創発的ビジネスの追求、知的フロンティアの追求、活気あるチーム・組織の追求

JISA は以上の会員企業の取組を支援するための活動を行っている。

ここで、働き方改革の取り組み状況を客観的に判断・評価する方法をいくつかご紹介する。労働時間や年次有給休暇の取得率のみに注目するのではなく、人事制度や具体的な課題を見つけるための改善指標による「見える化」や、第三者による取り組み状況の認定、公に自己宣言するといったものがある。

表) 働き方改革の	働き方・休み方改善ポータルサイト 自己診断 ^{iv}
-----------	-------------------------------------

指標厚生労働省	企業向け/社員向けの自己診断による改善指標の可視化
厚生労働省	くるみんマーク・プラチナくるみんマークについて ^v 計画に定めた目標を達成し、一定の基準を満たした企業に対し、 「子育てサポート企業」として厚生労働大臣が認定
ファザーリング・ ジャパン	イクボスドットコム 「イクボス宣言」 ^{vi} ワークライフバランスの取り組みを、経営者や管理職が公に宣言する

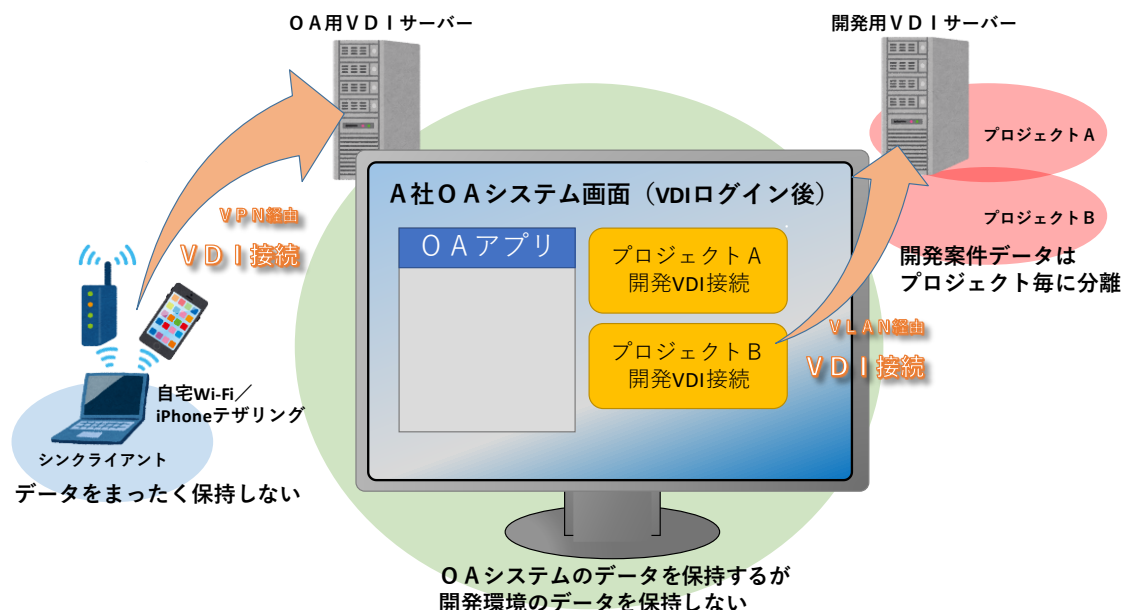
A社では、これらの指標の取得認定にも積極的に取り組んでいる。

〔テレワーク開発環境はシンクライアント+VDI x 2 段構成〕

前置きが長くなってしまったが、A社のテレワーク開発環境をご紹介します。前述の通り、在宅勤務・テレワーク化推進の後、第4段階にてそれらをうまく活用する形でテレワーク開発環境の構築を進めていった。A社のテレワーク開発環境は、OAテレワーク環境で利用しているシンクライアントを使って一旦OA用VDI環境にログインし、その後それぞれの開発プロジェクトで用意したVDI環境へ再びログインする仕組みになっている。

実際の開発環境には物理サーバーのほかにも、Azure (Microsoft)、AWS (Amazon)、GCP (Google) といったクラウド開発環境が含まれている。これらすべてが開発用VDIを介して接続することにより、一元的なアクセスコントロールと稼働状況の把握が可能となっている。

図) A社テレワーク開発環境へのアクセス方法



このようなシンククライアント+VDI x 2 段構成のメリットは、以下の通りである。

【機密性】 情報漏えい対策
● シンククライアントは画面表示と操作のみ データをまったく保持しないため、たとえ端末が盗まれても情報漏えいしない ● OA システムと各開発プロジェクト環境は完全分離 OA は一般アカウント権限、開発プロジェクトへはそれぞれの権限が必要 OA と開発間、あるいは開発間同士でのファイルやり取りは不可能
【可用性】 開発作業のしやすさ、リソース配分
● シンククライアント PC 及び OA 用 VDI までのネットワークは、画面表示と GUI 操作ができれば十分、OA と兼用可能 ● 開発用サーバー側でプロジェクト毎に必要な処理能力を割り当てる 仮想化サーバーを使うことで、案件や局面でのリソース最適化ができる ● 各人の作業状態をサーバー側で保持、どこにいても作業を再開できる
【完全性】 環境差異がないため余分な検証作業は不要
● 開発環境で動作している画面をそのままシンククライアントで操作、完全同一

[セキュリティ面での考察]

ここで、この構成におけるセキュリティ面での脅威と対策を見ていく。

- シンククライアントからの情報漏えい
一切のデータを保持しないため、端末を盗まれても情報は漏洩しない。
操作中に画面をのぞき見されない事だけ注意。
- シンククライアント自体のマルウェア感染
仮想デスクトップは VDI サーバー上で動作している。シンククライアント自体もシステム変更の禁止、アプリケーションの使用制限、U S B デバイスのアクセス制御、リムーバブルメディアの読み書き制限などで保護されている。
- 通信経路での盗聴
VPN によるトンネリングと暗号化により保護されている。
画面表示の情報をやり取りするのみで、盗まれて困るようなファイル転送など行わない。
- VDI サーバー上の仮想デスクトップ環境のマルウェア感染
各自用の仮想デスクトップ環境は、サーバー上でまとめて管理できる。
マルウェアスキャン、OS パッチ管理、インターネット接続先の制限などを集中管理。さらにサーバー側でまとめてバックアップを取ることで、ランサムウェア対策も可能。
- 担当している開発プロジェクト以外のデータアクセス
プロジェクト毎に開発環境自体が分離されており、さらにアクセスするには OA 環境へのログインとプロジェクトへのログインの 2 段階により保護されている。

一般的に VDI といえば、物理または仮想で各人用のデスクトップ環境を稼働させることを指すが、そのときの端末側は一般的な PC（非シンククライアント、FAT PC）の利用も含まれる。そこで、端末側を画面転送に特化したシンククライアント専用端末とすることで、セキュリティ強度を高める方法、それが今回のシンククライアント+VDI 構成なのである。

〔開発環境への VLAN は 2 種類で運用しやすく〕

開発用 VDI サーバー ⇔ クラウド開発環境間は、案件/プロジェクト毎に個別の VPN で接続する方法もあるが、A 社の場合はネットワークコア業者を経由させることで Azure や AWS と自社間に専用線を引くイメージで接続されている。そこで案件単位のセキュリティを確保するために、専用線内を VLAN で分離している。開発用 VDI サーバーから各開発環境への接続方法は大きく 2 種類、「共用 VLAN」、「専用 VLAN」がある。

「共用 VLAN」は複数プロジェクトで共用する形で、OA 環境と同レベルのセキュリティポリシーがあらかじめ施されており、クラウド開発環境からインターネットへは出られないようになっている。B2C や基幹システムの開発などに用いられている。

「専用 VLAN」は共用でカバーできない場合に用いられ、プロジェクト個別のポリシー設定やインターネット接続も可能となるが、各プロジェクトの責任範疇となる。

このように、開発案件のセキュリティポリシーに合わせて VLAN 設定のプリセットを用意することで、基本的なセキュリティを容易に維持しつつ個々のニーズに対応でき、さらに運用管理の負荷も軽減できるメリットが得られた。

共用 VLAN	● OA 環境と同じセキュリティポリシー ● 開発環境からインターネット接続はできない
専用 VLAN	● プロジェクトの管理責任においてインターネット接続も可能

【勤怠管理の一元化】

一般的に、クラウド開発環境はいつでもどこからでもアクセスできるメリットがある反面、案件が差し迫った状況になるとつい自宅 PC で接続して作業してしまう、といったことが起こらないとも限らない。これは情報漏えいリスクとなる事は言うまでもないが、深夜休日に業務を行った場合の勤務管理が困難になる点も大きな課題である。

A 社の開発環境にアクセスするには、必ずいったん OA 環境に入らないといけない。そこで OA 環境へのログイン/ログアウト時刻を勤務開始/終了時刻とみなすことで、開発要員の勤務が把握できる。A 社勤務管理システムでは、OA 用 VDI サーバー上でログイン/ログアウト時刻を収集し、勤務データとして自動的に取り込む仕組みを作り、勤怠管理も一元的に行えるようになっている。

【コミュニケーションツールも重要】

テレワークに欠かせないのが、ビデオ会議やチャットなどのコミュニケーションツールである。A 社では i - Phone FaceTime のほか、Microsoft Teams も採用、VDI 環境からも利用できるようにしている。シンクライアントには意図的に Web カメラを搭載しない時期があったという。当時はカメラから画像の形で情報漏えいすることを警戒し、セキュリティ要件として Web カメラ非搭載にしていた。しかしビデオチャットがより身近になり、コミュニケーション方法として有効に使うべきとの判断で、現在は Web カメラを搭載する機種を採用している。合わせて、セキュリティレベルの高い部屋では、個人所有のスマホなどカメラが付いている機器すべての持ち込みを制限するルールを追加している。

【快適なレスポンスのために】

テレワーク作業効率を高めるために、インフラ側で注目すべき点が2つある。1つめはVPN接続でのネットワークの速さ、2つめはVDIサーバーの負荷状態である。

まずネットワークの速さであるが、どんなテレワーク環境も社内のレスポンス（快適さ）を超えることはできない。A社シンクライアントからOA用VDI環境までの通信は、iPhoneテザリングや通信カードのモバイル回線で接続する方法と、各社員が個人契約しているプロバイダを経由する自宅Wi-Fiのいずれかとなる。自宅Wi-Fiはプロバイダや接続形態（フレッツの場合、戸建て向け/集合住宅向け）にも依存するが、モバイル回線よりも高速で快適な作業ができる。また、テレワーク増加に伴いモバイル回線の通信量が増加、従量課金の負担を回避するためにも積極的に自宅Wi-Fiを活用している。

次にサーバー負荷であるが、VDIの仕組み上、1台の物理サーバーを複数人で共有する形になっている。そのため、誰かがCPU負荷の高い処理を実行、または頻繁にディスクアクセスすると他のユーザでレスポンスが悪化する。特に業務開始時刻9時～10時にはアクセスが集中しやすいため、在宅でも時差勤務をすることで負荷分散を図れる場合がある。

A社ユーザによると、シンクライアント端末を好きなところへ持ち運んでもって作業に集中できるメリットがあり、さらに自宅ではセカンドディスプレイを接続することでさらに快適になるとのこと。

このように、快適な開発環境は快適なテレワーク環境の上に成り立つということで5年以上前からテレワーク化を推進し、OA業務と開発業務を明確に分離しつつもインフラ環境は共用するA社のスタイルは大変有用な事例であり、これからテレワーク開発環境を構築しようと考えておられる方々にはご参考にして頂けるのではないだろうか。

1. 3 テレワーク開発環境の構築ノウハウ

〔A社のセキュリティ要件〕

A社ではテレワーク開発環境を構築するにあたり、絶対に譲れないセキュリティ要件が2つあった。

表) A社セキュリティ要件

1. 機密情報の漏えい防止
2. OA環境、開発環境、お客様ネットワークの3つを完全分離

機密情報の漏えい防止のポイントは、やはりシンクライアントの採用が最重要である。シンクライアント端末は内部に一切のデータを残さないため、端末を持ち出した際に万一紛失・盗難にあっても情報は漏洩しない。A社によると、シンクライアント機種選定にはいく

つかの試行錯誤がなされた。

ネットワーク分離については前述の通り、シンククライアント + VDI x 2 段構成及び 2 種類の VLAN を活用することで実現している。

[シンククライアント環境の選定、試行錯誤で 2 世代目]

シンククライアント環境を構築する場合、従来 PC にシンククライアント・ソフトウェアを導入する方法と、シンククライアント専用機を導入する方法がある。社内すべての PC を一度に置き換えるのはコスト的にも作業負荷的にも大変難しいため、部門ごとに入れ替え時期を決めて順次移行する方法が一般的である。

A 社の場合は、Windows XP から Windows 7 への移行タイミングで従来 PC から VDI への一斉切り替えを行なっている。つまり、従来 PC 資産を暫定利用するステップ（シンククライアント・ソフトウェア利用）を踏まず、一気にシンククライアント端末完全移行の方法を採用した。実際の導入作業は部門単位で順次移行を行っている。対して VDI 側であるが、当初から VMware Horizon を採用している。A 社によると多機能かつ安定性が高評価につながり現在に至っている。

シンククライアント機種は当初市販品 F を採用していた。一般的な用途においては十分な製品であったが、情報管理が特に厳しい業種の顧客を抱える A 社にとっては、クライアント内部に「データを保存する機能」は不必要であった。しかしながら F 製品はデータ保存を禁止させることができず、更なるセキュリティ向上のためデバイスの記憶装置に書き込みが全くできない仕様にカスタマイズできる製品 V に変えた。

[テレワーク開発環境構築において、考慮が必要であったポイント]

実際に運用しながら試行錯誤した点や、検討された課題などを QA 形式で紹介する。

- シンククライアント + VDI（画面転送方式）を採用した理由
情報漏えい防止のため。RDP（リモートデスクトップ）は音声・映像のリレー機能に問題があり、Web 会議を行うためには VDI である必要があった。
- シンククライアント ⇔ OA 用 VDI 環境間のネットワーク帯域の確保
家庭のネットワークは光が必須、i-Phone テザリングの回線確保。
基本的に画面を投げるだけなので、どんなに開発環境が重くても OA 用の帯域で賄えるが、新型コロナ対応前後で 1.4 倍に増速。i-Phone の FaceTime で動画チャットを多用すると通信費の請求が高額となったため、OA 環境の Teams で画面共有と音声のみ利用にルール変更。

- 通信回線が止まってしまったらどうなる
シンククライアントはオフラインでは利用できない。
アクセスポイントを複数冗長化することで対策している。
- シンククライアント側の認証方法
機密保持のためにあえてシングルサインオンを不採用に。
シンククライアントへの認証、Wi-Fi や i-Phone テザリング等のネットワーク認証、VPN 認証、VDI 認証などを個々に行わなければならないため、手間がかかるが盗難時にも安心できる。
- シンククライアントには一切データを保持しない弊害
シンククライアントは電源を切るとすべての設定が消えるため、外部モニタの解像度などの設定も毎回設定しなおさなければならない。
- いわゆるショルダーハックの対策
作業場所によっては第三者にシンククライアント画面をのぞき見されるリスク。
視野角を狭く、隣の人からも画面が見れない「のぞき見防止シート」を標準装備。
- コストメリットはあったか
設備費用を削減するという狙いはなく、セキュリティ向上と利便性を追求した。
開発作業をいつでもどこでも自由にできる、アイデアが浮かんだ時にすぐ形にできる、クリエイティブなメリットが得られた。
- 各開発用 VDI のアカウントやアクセス権の管理
開発工程が進むにつれて、プロジェクトへの参加メンバー数が増減する。画面や機能単位でチーム分担するなど、プロジェクトのライフサイクルにあわせて必要なアカウント数やアクセス権が変動する。また、プロジェクトが完了した後は保守環境を除いてすみやかに廃棄しなければならない。
A 社では情報システム部門が VDI アカウントを一元管理。各開発プロジェクト内のアクセス権はプロジェクトの責任範疇とし、定期的に棚卸し管理を行なっている。(クラウド環境の廃棄忘れ等には CASB 導入も検討)
- Windows アップデートやセキュリティパッチの展開
VDI サーバーで稼働している Windows(ユーザが操作する対象)のアップデート。
セキュリティ緊急パッチは必要な対象を洗い出して個別に配布、Windows アップデートについては VMware との相性問題が発生しやすく、一定期間の検証が必要。
- シンククライアント自体のアップデート
A 社シンククライアントは Windows 10 IoT Enterprise を採用。この OS 自体も機能アップや不具合改善が必要であり、過去に数回アップデートを実施。ユーザ側でのアップデートは不可。情報システム部門に機器を預け、部門ごとにスケジュールを建てて実施。
- 将来の展望

現在 A 社内のデータセンターに VDI サーバーを設置しているが、これらをクラウドに移行していく構想がある。クラウド移行により、物理サーバーに比べてサーバー資源のプロビジョニングが自由に行えるようになり、障害復旧も容易になることから更なる運用コスト削減が期待される。

2. ニュー・ノーマル時代へ

2. 1 New Normal / 新しい生活様式

New Normal という言葉自体は、2000 年代初頭、ネット社会が本格化し新たなビジネスモデルが登場しはじめた時期に語られるようになり、世界金融危機（リーマンショック）の際の経済・社会の価値観の転換にあわせ広く使われるようになった。そして今回、新型コロナウイルスの感染拡大が進むにつれて、アジア諸国を中心に頻繁に使われるようになっていく。いわゆる黒船の来航のごとく、それまでの概念の転換が迫られ、以後の経済社会や個人の生活様式に大きく影響を及ぼす状況を表すとされる。

本稿においては、新型コロナウイルスのパンデミックと緊急事態宣言が出されたことにより、ソーシャルディスタンス、在宅勤務（テレワーク）、オンライン教育、オンライン購入（調達）・デリバリー、オンラインコンテンツ利用、オンライン決裁などに代表されるテクノロジーの強制的な利活用の状況が起こり、人々の意識が転換された。これは「思ったより使える」という感覚とともに、パンデミック中の一過性のものにとどまらず、その後もあらたな生活様式として普及していくだろうことを念頭においている。なお、テクノロジー業界にとっては大きな機会ともいえるが、個人情報、働き方や会社の仕組みの再検討の必要性、セキュリティの重要性の再評価等、見直すべき課題も浮き彫りになりつつある。

2. 2 テレワーク開発環境によるイノベーション促進

いままでの開発環境のイメージは、各社ノウハウなど秘匿性が高い情報を扱ううえ、できる限り高性能のワークステーションを占有するなど、ハード的にもソフト的にも社外に持ち出せないというものであった。プロジェクトが佳境に入ると、窓のない殺風景な開発ルームで徹夜を繰り返した経験をお持ちの方もいらっしゃるかもしれない。

いわば企業の生命線ともいえる開発環境を社外からアクセスできるように変えることは、大きな決断力を必要とする。しかし実現すれば、開発作業者の働く環境を大きく改善し、その結果、生産性向上や新しい発想を生み出す可能性を高めるものになるであろう。

テレワーク開発環境の実現によって、働き方改革、ワークライフバランスを満たしつつ^{vii}、

1. いつでもどこでもアイデアが浮かんだらすぐに試することができる
通勤時間短縮など、空いた時間でアイデアを考える余裕が出てくる
2. 時間労働から裁量労働、成果物重視に変わっていくことで、
業務時間の使い方や各自の効率化を工夫・追求
より良い「ものづくり」に打ち込める
3. さらに自己研鑽、スキルアップに力を入れていくことができる
それまで作れなかったものが作れるようになっていく

といった効果が期待できる。

開発作業者を多く抱えるシステムインテグレーターでは、なかなか在宅勤務率を上げられないという問題を抱えておられたかと思う。悩みどころであった開発環境をうまくテレワーク化することにより、より完全なテレワークが達成できる。そのとき社会はどのように変化するであろうか。

- 通勤距離がゼロになる、通勤圏内に住む必要がなくなる
東京一極集中が原因の様々な課題の解消（都市機能の限界、教育、福祉、医療など）
地方創生、日本全体の活力を上げる
天災などの被害分散、BCP
- 在宅で十分働ける、事務所へ出勤しなくてもよい
障がい者や家庭の事情などで出勤が困難な人の雇用
高齢化社会、不足する若手を補う人材としてシニア層の雇用
- 事務所が必要なくなる、固定費の削減
オフィスの賃貸料、通勤定期代、首都圏住宅手当などの削減
シェアオフィス、コワーキングスペースなどのスタイル拡大・定着
- 時間で勤務量を計りにくい、裁量労働制への加速
同じ時間でも人によってパフォーマンス差が出る、時間＝給与でなくなる
働くことのみならず人生を豊かにすることに価値を見出す人もいる、働き方改革

このように環境が変化していくことにより、いままでの常識・制約が打破され、必要とされるものが変わっていく。

まずインフラ増強である。社会人の在宅勤務だけでなく、学生も遠隔授業をおこなう。回線キャリアのキャパシティ計画を上回る需要が発生していると思われ、逼迫した状態が続く恐れもある。さらに、多くの人々が大量の通信を必要とするようになったいま、使えば使うほど金額が跳ね上がる従量課金の仕組みも変革が必要なのかもしれない。

つぎに制度面である。社員の能力を最大限に引き出すために、看護休暇、半日休暇、時間

単位休暇などフレキシブルな働き方に対応した会社制度の見直しも必要であろう。また、印鑑が必要な業務を完全になくす、在宅勤務にかかる経費（光熱費、通信費など）を個人負担とするかなど、テレワーク化の足かせとなる既存制度をなくしていく努力も必要であろう。

このように、インフラ面、制度面の両輪をうまく回していくことが、イノベーション促進につながるものと確信する。世界中がコロナ禍のなか、外出できなくても生産性を維持することができる姿こそニュー・ノーマルであり、日本の競争力を高めるためにも”いま”取り組むべきではないだろうか。

2. 3 会員みなさまへ

最後に、内閣サイバーセキュリティセンターから発行されている、

「テレワークを実施する際にセキュリティ上留意すべき点について」^{viii}

をご紹介します。この文書は政府機関等、重要インフラ事業者を対象としたものであるが、広く一般にも活用できるよう公開されている。

この文書では、テレワーク開始にあたって事前に行うこととして、

- 導入目的の明確化
- 対象範囲の決定
- 導入計画の策定、社員への説明

そのあと、各種ルールの策定、インフラ整備を進めていくべきとしている。そして、それまで運用しているセキュリティポリシーやルールなど守りつつ、テレワーク実施によって不足する部分を補っていくことを推奨している。

技術的に特に注意が必要な事項として、VPN の脆弱性対応、フリーメール利用の注意やメール暗号化、意図しないリモートデスクトップ公開や脆弱性対応、遠隔会議システム（Zoom など）を利用するリスク、カメラやマイクなどから SNS へ機密情報が洩れるリスクなどについて、具体的な対策を紹介している。ぜひご一読いただきたい。

サイバーセキュリティ部会内でテレワーク状況をディスカッションしたところ、ある委員から次のようなコメントが得られた。「テレワーク実施後の社内アンケート。一般職・管理職とも 90%が肯定的、なかでも研究職は業務に集中できるという理由で満足度が高い。一方で、社内の別チームとのコミュニケーションが減ってしまった、上司側が部下へのコミュニケーションを取りづらいついていて/何をやっているか不安になる。部下側からの不満はないようだ。」

また、別の委員からは、「今の急ごしらえのテレワーク環境では、回線速度がボトルネックになって快適さが得られていない。でもテレワークをやめて以前の状態に戻すようなことはせず、インフラ増強していく方針。」

いずれもテレワークに肯定的な意見が多かった。もはやテレワークは一過性のものではなく、コロナウイルスが収束しても元にはもどらないと考える。そのとき、会社でも自宅でも同じセキュリティレベルを担保できるのが「あるべき姿」であり、そこにどうやってたどり着くかを考えていかなければいけない。

我々サイバーセキュリティ部会における今後の課題として以下2点があげられた。

1. テレワーク前提のセキュリティのあり方
インフラや制度が変わると、リスクの再評価が必要
今までとは異なる場面で思いもよらない問題が発生する可能性を留意する
2. インシデントレスポンスの見直し
何かあったときの連絡フローや招集条件等をテレワーク前提で見直す
今まで事務所内で関係者全員にすぐ連絡が付けられる状況とは異なる
テレワーク状態での対応や判断の遅れにつながる可能性を留意する

A社のテレワーク開発環境（シンククライアント+VDI x 2段構成）を紹介したが、新型コロナウイルスの緊急対策としてそのまま採用できるかというコストや時間的に難しい部分もあるであろう。しかし、最終形態イメージとして「シンククライアント+VDI x 2段構成」がご参考となれば、A社が試行錯誤に費やした時間を再び繰り返す必要がなく、結果的に最短期間で堅牢なテレワーク開発環境が構築できるものと思われる。

新型コロナウイルス対策としてだけでなく、ビジネス継続性 BCP、働き方改革など、通勤時間に縛られない労働環境は、皆様にとっても魅力的だと思われる。この機会を好機ととらえご検討されてみてはいかがでしょうか。本稿が JISA 会員みなさまの一助となれば幸いである。

以上

用語集

シンククライアント
最小限の GUI と通信機能を備え、サーバー上のデータやアプリケーションを操作するための端末装置。一般的な PC と比べてシンプルな構成のため、保守性に優れている。 一般的な PC にシンククライアント・ソフトウェアを導入することで、既存資産を順次移行させる方法もある。
VDI (Virtual Desktop Infrastructure)
ユーザ毎に独立した複数の仮想 OS 環境を物理サーバー上で共存させ、シンククライアント等から接続してデスクトップ PC として利用する仕組み。
VPN (Virtual Private Network)

インターネットを介した拠点間通信を、暗号やトラフィック制御により仮想的に専用線のようにする仕組み。

拠点に専用ルーターを設置するだけで VPN 網を構築できるクラウド型 VPN もある。

i 東京都防災ホームページ(第 330 報)テレワーク導入率緊急調査結果

<https://www.bousai.metro.tokyo.lg.jp/taisaku/saigai/1007261/1007864.html>

ii 東京都オリンピック・パラリンピック準備局 会場周辺交通対策 2020.2

https://2020tdm.tokyo/traffic/202002_Plan.html

iii JISA 働き方改革宣言

<https://www.jisa.or.jp/tabid/2492/Default.aspx>

iv 厚生労働省 働き方・休み方改善ポータルサイト

「働き方・休み方改善指標」を用いた自己診断

<https://work-holiday.mhlw.go.jp/diagnosis/>

v 厚生労働省 くるみんマーク・プラチナくるみんマークについて

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kodomo/shokuba_kosodate/kurumin/index.html

vi イクボスドットコム

<https://ikuboss.com/>

vii 厚生労働省 働き方・休み方改善ポータルサイト

テレワーク推進の効果

<https://work-holiday.mhlw.go.jp/telework/effect.html>

viii 内閣サイバーセキュリティセンター

テレワークを実施する際にセキュリティ上留意すべき点について

<https://www.nisc.go.jp/active/general/pdf/telework20200414.pdf>