Digital ESSAY

「裸な太陽」

坂口　裕靖

SARS-CoV-2 によって引き起こされる COVID-19 が流行っております。この原稿を書いている時点では、どこまで広がるか予想がつかない状態ではありますが、社会全体に薄く広く広がっているような印象があります。現時点では明確な治療手順もわかっていなければ、手洗い・うがい以外に有効な予防策も判明しておらず、でも電車通勤もやめるわけにもいかない状況で、もはや「安全地帯」は存在せず、蔓延待ったなしではないでしょうか。

何しろ飛沫感染や接触感染が疑われるわけですから、なるべく他人との接触を少なくすることが、予防の上では有効でしょう。その意味でリモートワークは大変有効かと思います。とはいえ、すべての職種においてリモートワークが可能というわけでもないのがややこしいところです。目の前のブツを加工しなければならないとか、実行するために必要な環境がそこらのご家庭では用意できない、あるいはそもそもその場所にいること自体に意味があるなど、ノンリロケータブルな職種は多いと思います。一方でパソコンと資料があればできる仕事なら、リモートワークも可能でしょう。

仮に個々の仕事がリモートで実行可能だとして、単独でできる仕事には限りがあり、どうしても他の人々との協調動作が必要となってくるかと思います。このコミュニケーションがいかに円滑に行えるかで作業効率は大きく違ってきます。このあたりはチケットシステムやチャット、メールなどを適宜使い分けて行くしかないでしょう。どうしてもリアルタイムで複数人が相談しなければならない場合は、ビデオチャットが有効です。文字ベースのコミュニケーションしか取れないチャットシステムの場合、文字で表すことが苦手なメンバーは意思疎通が難しくなります。ビデオチャットであれば、文字ではなく音声や身振り・手振りを使うことができるため、同じ時間であってもやりとりできる内容は深くなり、コミュニケーション負荷が下がります。一方で通信の帯域幅もそれなりに消費するため、多人数が参加する場合はそれなりの設備を用意する必要があるでしょう。まずは音声会議でなんとかならないか、あたりが落としどころではないでしょうか。交換機によってはパーティライン的に使える場合もあるため、活用したいところです。

さて、リモートワークにおける最大の問題は「ファイル」の扱いでしょう。どんなシステムであっても、「ファイル」の形式にデータを落とした途端、一気に漏洩の可能

One Point BUZZ WORD

Site-to-Site VPN

お仕事でお客さんのネットワークとの間に VPN を張ることがちょくちょく出てきましたが、通常お客さん側のマシンにこちらからアクセスすれば要件を満たす場合が多く、実は網同士を接続しなければならない（お客さん側から弊社マシンにアクセスしたい）という要件はそんなに多くありません。であれば、お客さん側で受けのアクセスサーバを立ててもらって、そちらに弊社クライアント単位で接続しに行けば十分だったりするわけですが、この受けサーバの運用負担をどうするかが議論になったりして、結局何らかの接続用機構をこちら側で用意する話になったりします。

そんな場合に AWS の Site-to-Site VPN を使うと、コネクションの維持自体を AWS に丸投げできるので大変便利です。ただし設定できる PSK に制限があり、「長さは 8 ～ 64 文字、使用可能文字種は英数字、ピリオド（.）、および下線（_）で、先頭はゼロ（0）以外」と多少癖があります。また、AWS 側端点の IP アドレスも問題で、これは VPN を張った後じゃないと判明しないのに、接続先の IP は事前に必要なので、このあたりの手順的な問題も事前に合意が必要です。基本的に VPN を設定したら、対抗側ルータ用の設定ファイルをダウンロードし、対抗側を設定する、という流れを想定しているようで、AWS 側が従となることは一切想定していないようです。接続が切れないように多重化されており、AWS 側の端点は 2 つあるので、対抗側も対応しなければなりません。受け側のルータがサポート外だと、設定に苦労するかも。時間・流量課金は発生しますが、EC2 を立ててアクセスサーバにしても同様に発生するわけですし、時間課金は東京リージョンで 0.048USD/h と、t3a.medium と同程度、流量課金は EC2 と同額。手間を考えると Site-to-Site VPN の方が楽でしょう。VPC 自体が VPN でつながるので、後は好きなようにマシンを起動すれば良いのです。

性が高まります。「ファイル」は単独で解釈可能なデータ列ですから、システムの垣根を超えて伝達することができます。これは、せっかくシステムが用意した可視性や変更を制御する仕組みを容易に突破できることを意味します。通常アプリを開発する局面で一番手間がかかるのは、編集システムなわけですから、一般的なアプリで扱える「ファイル」で部分部分を連結したいというのはよく分かりますが、同時に「ファイル」の受け渡しを不可避なものにしてしまうという問題をはらんでいます。このため、「ファイル」の運用はファイルサーバなどの「ファイル」を安全に管理できるシステムを前提として組まれることになります。こうした環境でリモートアクセスしようとすると、どうしても「ファイル」の扱いがややこしいことになります。漏洩や喪失の可能性を最小限にするためには、「ファイル」の保存先として、管理可能な端末に囲い込みたいところです。となると、リモートワークする端末を予め用意して置かなければなりません。この端末は持ち歩くことになるわけですから、仮に紛失したとしても、内部のファイルを守れるようにしておかなければなりません。ファイルシステムの暗号化や、ハートビートが途切れたらデータ消去するなどといった対策を仕込む必要があり、今回のようにいきなり大量のユーザーがリモートワークしなければならないような状況に対応することは大変困難です。

逆に言えば、「ファイル」が社外に出なければ問題ないわけですから、編集するため、わざわざリモート側の端末に「ファイル」をダウンロードする必要をなくすことができれば、このあたりを一気に解決できることになります。一番本質的な解決は「ファイル」を排除して、全てを Web アプリ化することでしょう。アクセス制限はアカウントで行えるなら、外部流出を気にする必要はなくなりますし、適当なマシンからアクセスできるようにシステムアップすることも容易でしょう。ただ、残念ながら事前にそういうワークフローを構築して置かなければならず、今更無理かもしれません。

もう一つの解決策は、遠隔地から社内の自分のマシンにリモートログインし、そこで作業を行うというものです。「ファイル」のダウンロード先は社内ですから、防御は完璧なはず。一方でパスワードが割れるとリモートログインされ放題になるわけですが、このあたりの状況はアカウントの防御と変わりありません。ファイアウォールの内側であっても、最近のリモートアクセスサービスの大部分は問題なくログインできてしまうので、あまり気にする必要はありません。逆に言えば、社内の環境を本当に防御したいのであれば、これらのリモートアクセスサービスへの対策が必要でしょう。

具体的には Windows と Mac が混在しているなら SplashTop business が、Windows だけなら desktopVPN が使い勝手良いかと思います。いずれも月額固定の料金制ですし、通信内容は基本的にサービス提供側に筒抜けになる（ただし通信経路は暗号化されるので、そこは大丈夫であること、筒抜けになるからといってサービス提供側がしゃぶり尽くすかどうかは別問題だし、普通は読みもしないと思いますが）わけですから、そこいらへんのリスクを勘案する必要はあるでしょう。ユーザーが組織を離れた場合、アカウントをきめ細かく ban する手間が必要になるというのもありますが、端末を紛失するリスクと比べてどちらがお得かは考慮に値するでしょう。それでも、一度会社側マシンにサーバソフトをインストールしておけば、リモート側の端末は何でも使えるのが大きな利点です。例え出張先でも、そこらのネットカフェやホテルの端末からでも、通信経路を暗号化した上で問題なく使えるわけですから。これを延長すれば、そもそも会社で個人に配布するマシン自体を強固な物理防御内のマシンと、机上のシンクライアントとに分けておいて、シンクライアントを持ち出し自由にするとかもあるでしょう。きちんとパスワード等の管理がなされているのなら、シンクライアントを紛失しても、漏洩リスク等を気にする必要はありません。少なくとも「ファイル」ごと紛失することは論理的にも物理的にもできませんので。

しかし今回、いろんな会社がリモートワークを実施することで、地獄の釜が開いてしまうのかもしれません。リモートワークで仕事になるなら、リモートワーク可能な従業員分の床面積は最悪省略可能になるじゃないですか。その分オフィスを小さくできるわけで、机を確保するのが難しくなっていくかもしれません。逆に言えば、ネットワーク環境が整備されているのなら地方も首都圏もさほど違いはないので、働く場所の選択肢は増えることになります。さすがに仕事を覚えるまでの部分をリモートで行うのは難しいかもしれませんが、なんで面と向かって教えなければならないかというとマニュアル・職能がきちんと確立されてないことの裏返しだからであり、これらが整備されるのであれば、フルリモートで問題なくなるなるでしょう。そこまで突き詰めた時、本社機能として何が本社ビルに残るべきなのでしょうか。郵便物をスキャンする仕事だけだったりして。

Hiroyasu Sakaguchi
株式会社 IMAGICA Lab.