情報セキュリティポリシーの転換
－テレワークを可能にするために－

倪　　永茂

はじめに

2020年初に中国武漢市で感染爆発が確認された新型コロナウイルス（Covid-19）がその後の世界を大きく変えた。ヒト、モノ、資本のグローバル化はウイルスの拡散にとっても好都合であった。

新型コロナウイルスの影響が約1年半経ったいまの2021年8月でも軽減する傾向が見られないどころか、変異ウイルスによる感染拡大の状況がより深刻になり、筆者が関係する栃木県では3度目の緊急事態宣言が発出された。

常識的にも科学的にもひとの移動を止めるのはウイルス対策として最も有効ではあるが、さまざまな理由でほとんどの国ではそれができない。その代わりに、日本では緊急事態宣言発令地域では出勤者7割減を目指すという国の方針にしたがい、テレワーク（在宅勤務）が導入されるようになった。

テレワークとは情報通信技術を活用した、場所や時間にとらわれない柔軟な働き方のことを指す。もともと、日本政府はテレワークを働き方改革の重要な位置づけとしており、2013年に閣議決定され、2014年に改訂された「世界最先端IT国家創造宣言」では「雇用形態の多様化とワーク・ライフ・バランスの実現」[1]という項目でつぎのこと、すなわち、「若者や女性、高齢者、介護者、障がい者を始めとする個々人の事情や仕事の内容に応じて、クラウドなどのITサービスを活用し、外出先や自宅、さらには山間地域等を含む遠隔地など、場所にとらわれない就業を可能とし、多様で柔軟な働き方が選択できる社会を実現できるとともに、テレワークを社会全体へと波及させる取組を進め、労働者のワーク・ライフ・バランスを実現する。」とうたっていた。さらに、政府の目標として、2020年にはテレワーク導入企業を2012年度比で3倍、週1以上終日在宅で就業するテレワーカー数を全労働者数の10％以上とすることとした。

新型コロナウイルスの感染拡大はテレワークの普及や定着にまたとない好機であるにも関わらず、筆者の勤務先である国立大学法人でさえも、テレワークの定着に程遠い状況にある。緊急事態宣言やまん延防止等重点措置の対象地域に関係する教職員以外は原則毎日出勤という従来の勤務体制が継続されているからである。その理由もまたさまざまであろう。法整備の問題以外に、経営側のリスクを取るリーダシップの欠如や、セキュリティ対策に関する知識不足、テレワークをサポートするための環境整備にかかるコストの高さとセキュリティ対策の難しさ、テレワークによる企業秘密や個人情報の漏洩に伴うリスクの高さ等が障害となっていることと考えられる。

そこで本文では、筆者の勤務先を事例として、従来の情報ネットワークがテレワークに対応できていないこと、クラウド情報システムの導入によってテレワークが実施可能になったこと、しかしセキュリティリスクが以前よりも増したこと、その対策として、情報ネットワークポリシーの転換が必要不可欠であることを説明する。

情報ネットワークポリシーとは何か、総務省の公式サイトではつぎのように説明している。すなわち、「情報セキュリティポリシーとは、企業や組織において実施する情報セキュリティ対策の方針や行動指針のことです。情報セキュリティポリシーには、社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するのが一般的です。」[2]重要なのは、方針や行動指針だけ

でなく、管理体制、運用規定、対策基準といった具体的な記述が必要だということである。

去る 2020 年 4 月の緊急事態宣言発令によって、多くの組織は準備期間もなく、テレワークという新しい勤務体制に切り替えたのが実情であろう。情報ネットワークポリシーの下でテレワークによる業務継続を行うべきであるが、現実はそうあまくなかった。しかし、Covid-19 の感染拡大から 1 年半も経ったいま、テレワークの課題を整理し、組織の情報セキュリティ対策の根幹となす情報セキュリティポリシーを再検討すべき時期に来ているのではないか。

Ⅰ 現状と課題

ここでは、筆者の勤務先における現状と課題について分析する。自分自身の置かれた業務の内容や、情報機器や情報ネットワークに対するスキルの違いによって、必ずしも多くの勤務者の考えている実情と一致するわけではないことを断っておく。また、セキュリティ対策のために、情報システム等の詳細な記述があまりできないことも付け加える。

1 コロナ禍以前の情報ネットワーク

組織全体として、インターネットとの相互接続は日本でも早い段階で実現した。1991 年に着任して間もなく、B クラスのドメイン登録申請が許可されたのに続き、個人用 E メールアドレスを取得し、今日までの 30 年間近く変えずに使ってきている。

情報ネットワーク管理部門が 2007 年に情報セキュリティマネジメントシステムに関する国際規格 ISO ／ IEC 27001 の認証、さらに、2014 年に 27001:2013、翌 2015 年に 27031 の認証を取得したことに象徴されるように、組織の情報ネットワーク・ポリシーや、セキュリティ対策への取組が国際的ルールに合致し、その毎年の現地検証をパスしている。

組織内情報ネットワークは大きく、2 つの系統に分けられている。

事務系は独自のドメインシステムを使っていて、個人情報保護のために、外部からのアクセスは徹底的に遮断することにしている。E メールですら、外部から読み書きできない。

研究教育系は事務系に比べて規制はだいぶ緩やかで、E メールの読み書きは Web ベースではあるが、外部からもできる。ただし、メールの外部への自動転送や、外部からの POP や IMAP によって受信したメールの取得は許可されていない。

また、外部への Web アクセスは原則としてプロキシサーバ経由になる。情報化社会では、インターネットへの Web アクセスを認めないことはやはり無理であろう。

組織内のネットワークは強力なファイアウォールによってインターネットと遮断されている。しかも、日常的に監視していて、組織内部から外部への不審なアクセスがあるとすぐに通報され、情報ネットワーク管理部門のスタッフが立ち入り調査を行い、疑われるパソコンをいったん押収し、記憶装置の初期化やアンチウィルスソフトの強制導入、セキュリティ改善措置の提出がその後求められる。

Wi-Fi 利用はパソコン教室（および他の極わずかな教室）や図書館内に限られる。ユーザ認証がやや複雑であることに加えて、プロキシサーバ経由のインターネットアクセスであるため、学生の必携品であるスマートフォンとの相性は必ずしもよくない。

組織構成員間の情報共有は公式 Web サイトやプライベート Web サイト（外部からはアクセスできない）を通じて行われているが、個々の構成員からは情報発信ができない。いわゆる、お知らせとしての役割しか果たしていない。

それを改善するために、部門（部局）の一部には情報共有のためのグループウェアが設置されている。ミーティングためのスケジュール調整や会場の予約、情報（ドキュメント）共有、部門構成員間の連絡機能（メールの送受信）等が備わっているが、部門を跨る使い方や、外部からのアクセスは許されていない。

このように、コロナ禍以前の情報ネットワークは出勤を前提にポリシーが制定されていて、外部からのアクセスはほぼ、公式 Web サイトや E メール（研究教育系構成員のみ）に限られている。テレワークという勤務形態をまったく想定していない。日本政府が推進しようとしているテレワーク

導入目標にも明らかに対応していない。

2 コロナ禍でのテレワーク

情報ネットワークの構成や特徴からもわかるように、事務系では、テレワークのできることが大幅に限られる。

実際にそう実行している構成員がいないかもしれないが、印刷資料を持ち帰って仕事し、情報の共有を電話で行う、といったテレワークが考えられる。しかし、資料は電子化されていることがほとんどであるため職場での事前印刷が必要であったり、仕事の成果をその日に詳細報告ができないことなどから、仕事の効率が大きく低下するだけでなく、数日以上をわたる日数のテレワークは事実上不可能であろう。

その改善策として、半日交代の勤務体制が有効かもしれないが、実行に移ったことはなかった。

研究教育系は比較的長期間のテレワークが工夫次第でなんとかなる。もともと、研究は個人ベースか研究室単位で行っているので、大型実験設備や危険を伴う実験用試材を必要としない研究であれば、自宅でも継続できる。オンライン授業や指導等の教育活動も似ていて、実験等を伴わないものであれば、工夫次第で対面教育並みの効果が得られる。オンラインミーティング等は Zoom や Microsoft Teams、Slack 等のツールを活用すれば成り立つ。

ただ、研究教育系は事務系のサポートを必要とする仕事がないわけではないし、組織内の情報共有等が E メールだけでは不十分なことが多い。また、研究教育のために蓄積されてきた膨大な資料（書籍や電子化データ等）をすべて自宅に持ち帰ることが不可能であろう。組織内 LAN や、研究室のパソコンや NAS（Network Attached Storage）に自宅からの遠隔アクセスできればいいが現状では許可されていない。

このように、テレワークの効率がよくないためか、2020 年 5 月 14 日、第 1 回緊急事態宣言が解除された日から、組織は原則として毎日出勤という従来の勤務形態に戻った。また、目下の第 3 回緊急事態宣言発令期間中でも、テレワークする事務系構成員はほとんど見かけなくなった。

3 テレワークのための施策

しかし、コロナ禍において、テレワークによる業務遂行のための改善策を施す努力を組織として怠ったわけではない。

目立つ対策として 4 つ取り上げると、ひとつは情報共有システムを新規に立ち上げ、外部からのアクセスを可能にしたことである。それに伴い、従来のプライベート Web サイトが廃止された。それによって、事務系構成員が業務の一部を自宅からできるようになった。

2 つ目はクラウド型オンラインミーティングシステムの導入である。会議だけでなく、授業もそのシステムを使ってオンライン形式で実施できる。資料の配布等もシステム上で可能である。

3 つ目は学習支援システムの導入である。すべての授業をオンラインで行うために、クラウド型学習システムを 2020 年 4 月に急遽導入するようになり、授業の出席管理、教材配布、学生によるレポート提出、学生への連絡、授業中のアンケートや意見交換が可能になった。

4 つ目は Wi-Fi の整備、組織内の教室すべてに Wi-Fi が使えるようにしたことである。対面授業とオンライン授業がそれによって両立する体制がやっとネット環境の面で整った。

以上の 4 つの対策はともに情報ネットワーク管理部門の助言を受けたものの、情報ネットワーク管理部門が主導的に実施したものではない。また、Wi-Fi 整備以外の 3 つは組織の外部にあるクラウド型システムであるため、大学のファイアウォールを経由していない。ファイアウォールによって外部からアクセスできないといった制限は受けない。Wi-Fi についても理由をここでは明らかにしないが、それもファイアウォールを経由していない。

4 新たな課題の整理と分析

ここでは上記 3. で説明したような、テレワークのために導入した新しいシステムによって生じる課題について整理し、その要因を分析してみることにする。

1）セキュリティリスク

潜在的な課題であるが、最も重視すべき課題でもある。よくいわれるように、利便性はセキュリ

ティリスクとトレードオフの関係にある。利便性を追求すると、セキュリティの低下は避けられない。反面、強固なセキュリティ対策を施すと、コロナ禍以前のように、テレワークでできる業務は大幅に限られる。

利便性とセキュリティを両立するためには、情報ネットワーク部門による徹底したシミュレーションと検証を行い、セキュリティガイダンスのようなものを組織の全構成員に周知し、各クラウド型システムに対する個々の管理チームの設置、すべてのクラウドシステムを統括する最高責任チームの設置等が必要であろう。

セキュリティリスクの予見と防止、リスクの検知と通報、リスク発生後の危機管理等、各チームでやれることが多く考えられる。しかし、現状では外部のクラウドシステム運営管理会社に任せることがほとんどで、主体的な取組がすくない。

この課題を完全に解決するのは難しいが、日々努力して少しずつ改善していくことが可能であろう。セキュリティインシデントが起きたら、組織への大打撃になりかねないからである。

2）情報が一元管理になっていない

クラウドシステムは従来の業務システムとの連携を考えたうえで検討を重ねて慎重に導入したわけではない。Covid-19 が一気に国レベルの問題になったのは 2020 年 3 月であり、その後の 1 か月間でテレワークのためのクラウドシステムを導入するのに、どうしてもトップダウン方式、すなわち経営側の短い日数での決断に頼らざるを得ない。また、導入コストもメーカーの選定を大きく左右したのであろう。

そのため、たとえば、教務システムという従来の業務システムへの登録作業は、学習支援システムとのデータベース共用はできず、学習支援システムへの登録がもう一度必要になる。

また、個々のクラウドシステムを統括する利用ガイドラインが不備のため、業務連絡は従来の E メールを利用するひと、オンラインミーティングシステムを使用するひと、情報共有システムを利用するひと等でバラバラになってしまい、効率の低下を招いている。改善するには、構成員それぞれのスキル向上のための研修会の開催や、利用ガイドラインの整備充実が望まれる。

3）研修会が少ない

各システム導入時に説明会が一度開かれていたものの、各構成員のスキルにあったオンライン研修会の開催はその後少ない。その結果、システム利用の個人差が大きく、毎日活用するひとと、従来通りの E メールにだけ頼って業務するひとといった両極端の現象が多く確認されている。利用履歴等の情報は個人情報に関わるので、それを活用して利用を促すことや、スキルを把握することができていない。

この課題は上記の課題 1）と 2）とも深く関係するし、また、従来の対面式コミュニケーションはテレワークでは難しいので、構成員個々人が業務に対する質問や悩みを相談する機会が少ない。パソコンや E メール等は数十年わたって利用してきた結果、ほぼすべての構成員が業務に活用できるようになったが、短期間で導入してきたクラウドシステムに適応するためには、対面指導や、学習機会を多く設けるべきであろう。

同様なことはオンライン授業等の業務にも当てはまる。インターネット向けにライブ中継しながら、教室で対面授業を行うには、高いスキルやアシスタントが必要となるケースは少なくない。コロナ禍以前と異なるスキルが求められる以上、相応しいスキルアップのプログラムを組織として用意し提供することが望ましい。

Ⅱ 情報セキュリティ・ポリシーの転換

筆者の勤務先だけでなく、日本では多くの企業が似たような悩みを抱えている。テレワークという新しい時代では、生産性とセキュリティ対策との両立、あるいは、トレードオフをどう考えるべきなのか。

1 テレワークは時代の流れ

Covid-19 によって鮮明になったのはテレワークの必要性である。従来でも、政府によるテレワークの推進が行われていて、本文のはじめにも書いた通り、雇用形態の多様化とワーク・ライフ・バランスを実現するためである。

筆者がこの 1 年間で実感したテレワークによるメリットのひとつとして、海外とのオンラインカンファレンスやオンライン授業ができるように

なったことである。まさにインターネットの良さである、時間的空間的隔たりを解消してくれている。

重要なのは、テレワークを強制するのではなく、職場勤務とテレワークを個々人の意思と状況に応じて選べる仕事形態の多様化は新しい時代に相応しいものではないか。

このように、職場は従来の勤務先から、自宅になったり、出張先になったりして、これからも多様化することは間違いない。

教育の対象者である学生もオンライン授業によって、多様な学びの可能性を知り、必ずしも決められた教室にいないと勉強できないことはないことを身をもって実践してきた。学生のこれからの様々な要望に応えるためにもオンライン授業を継続すべきであろう。

2 守るべき対象の変化

従来の考え方では、インターネットと組織内ネットワークとは物理的に分けることができるので、その間に強固なファイアウォールを設けることによって、外部からの侵入や内部からの不正アクセスを遮断することができている。それはいわゆる水際作戦、あるいは、境界防御という発想である。

しかし、テレワークの一般化によって、境界という発想自体が業務に合わなくなる。なぜなら、外部と内部とを分けることは業務に支障をきたすからである。理想論として、勤務先と在宅勤務の自宅を論理的に結び、いわゆる論理的ネットワーク、あるいは、仮想的ネットワークとして捉えるべきであろう。

外部からの侵入、あるいは、内部からの不正アクセスなのか、それとも業務の一環なのか、それを見分ける技術が必要になるし、在宅勤務の組織構成員は必ずしも情報ネットワークの専門家ではないので、利用する情報機器（パソコンやスマートフォン等）が完全に信用できるわけでもない。ハッカー（クラッカー）やウィルスに乗っ取られる可能性がないわけではないからである。

あるいは、信頼できないことを前提としてセキュリティ対策を講じる、いわゆるゼロトラストセキュリティを実現する方向にかじ取りを切る時期になったのかもしれない。

幸い、導入されたクラウドシステムはすべて外部にあるので、テレワークの業務を組織内部の情報ネットワークから切り離しても成立すると考えるならば、従来の考え方でも数年間は生き延びられるかもしれない。

しかし、クラウドシステムによって重大なセキュリティインシデントが起きた場合、組織にとっての損失は内部も外部もそれほどの差はなく、結局、組織としての責任が問われる。したがって、情報セキュリティ対策はクラウドシステム事業者に大きく依存することが仕方ないとしても、情報ネットワーク部門と事業者との連携がより重要になってくる。

つまり、いままでのような組織内部だけを守ればいいという発想は時代遅れになっている。

3 正当なひとと正当な情報機器の確認

従来のネットワークでは、組織内部の不正アクセスの有無を日常的に監視しているが、ユーザ認証はログイン ID とパスワードのみに頼っているし、ログイン時に利用している情報機器の正当性についても特別のチェックはしていない。基本的には、いわゆる「性善説」に立った発想である。

しかし、テレワークでは、信頼できないことを前提にシステムを運用するため、ユーザのなりすましや、ウィルスに汚染された情報機器からのアクセスをつねに意識することがセキュリティ対策上好ましい。パスワードレス認証や、ソフトトークンによる認証が実用段階になったので、その活用を視野にいれよう。

不当な情報機器を排除するには、アクセス・更新・削除したファイルの履歴や、情報機器の所在位置の把握等、個人情報保護との両立を考慮しなければならないが、AI 技術を活用した対策が必要であろう。

また、従来のクラウドシステムでは必ずしも満足できる管理になっていないのは、ドキュメントのバージョン管理、あるいは、世代管理という機能である。改ざん、あるいは削除されたファイルを回復させるには、ファイルのバックアップは勿論のこと、バージョン管理を活用すれば、不正アクセスから守ることができる。

ファイルの暗号化、ファイルの正当性を保証するためのデジタル署名付きファイル等、技術の進歩に見合ったシステムの採用を見据えたことも必要であろう。

4 システムに対するセキュリティリスクの評価と対策

テレワークのために導入された個々のクラウドシステムは本組織ではすべて、SaaS（Software as a Service）というサービスであり、カスタマイズできるものはあまりない。

クラウドシステムは大まかに分けると、ハードウェアに近い順では、ハードウェア・物理ネットワーク、OS、ミドルウェア、アプリケーション、コンテンツ（電子データ）[3]になり、それを包括してサービス運用される。SaaSという利用形態では、利用する組織は最上位のコンテンツ（電子データ）に対してしかセキュリティ対策ができないといわれる。

セキュリティ対策の向上を目指すなら、PaaS（Platform as a Service）やIaaS（Infrastructure as a Service）への切り替えを早急に検討しよう。

終わりに

潜在的リスクに対処するために、また、よりよい仕事環境や労働者のワーク・ライフ・バランスを実現するために、テレワークは一過性の勤務形態にするのではなく、企業や組織の経営者や指導者たちがリーダーシップを取り、政府の呼びかけに応じながら、将来を見据えて力強く移行すべきであろう。

しかし、企業や組織の情報ネットワークは従来のままでは、多くがテレワークに対処できないことが明白になってきている。情報セキュリティの守るべき対象が変わったからである。ファイアウォールによって物理的に企業や組織を内外に二分するという考え方がテレワーク時代では通用しなくなった以上、情報セキュリティ・ポリシーの転換が求められる。

本稿では筆者のいる勤務先を事例に、新型コロナウイルスが発生する以前の情報ネットワークの状況、コロナ禍1年目におけるテレワークの課題、コロナ禍2年目におけるテレワークのための改善策を振り返って整理した。テレワークが実現困難な状況から大幅に改善されたのは喜ばしいことではあるが、情報セキュリティ・ポリシーの下で、リスクを検討しながら施策を展開してきたわけではなかった。テレワーク時代に実行可能で実現可能な情報セキュリティ・ポリシーに転換することが必要である。

日本では、テレワークが多くの企業や組織にとって初めての試みであり、多くの新しい課題を模索しながら改善していくことになる。そのためにも情報セキュリティ・ポリシーを一気に変えるのではなく、新しい状況を踏まえて徐々に転換することになろう。

---

[1] 2013年に閣議決定され、2014年に改訂された「世界最先端IT国家創造宣言」、https://www.kantei.go.jp/ jp/singi/it2/kettei/pdf/ 20140624/siryou1.pdf（2021.8.25アクセス）

[2] 総務省「安心してインターネットを使うために 国民のための情報セキュリティサイト」、https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/ business/executive/04-2.html（2021.8.25アクセス）

[3] Symantec社、「5分でわかるクラウドセキュリティの5つのポイント ― クラウド導入を検討している企業担当者様向け」、https://www.digicert.co.jp/ welcome/pdf/wp_cloudsecurity.pdf（2021.8.25アクセス）

参考文献

会田和弘（2021）、「非営利組織などの小さな組織の情報セキュリティポリシーの策定の試み」総合政策研究（63）、161-166。

税所哲郎（2020）、『現代組織の情報セキュリティ・マネジメント改訂版：その戦略と導入・策定・運用』白桃書房。

南大輔（2020）、『エンタープライズシステム クラウド活用の教科書～スピードが活きる組織・開発チーム・エンジニア環境の作り方』技術評論社。

Transforming Information Security Policies:
To Enable Telework (Remote Work)

NI Yongmao

Abstract

To address the potential risks and to achieve a better work environment and work-life balance for workers, telework should not be a transient form of work, but rather a powerful transition with organizational leaders taking leadership and looking to the future.

It is becoming clear that many organizations' information networks will not be able to cope with telework in Covid-19. This is because the target of information security has changed. As the idea of physically dividing an organization into internal and external parts by firewalls is no longer valid in the telework era, the information security policy needs to be changed.

（2021 年 10 月 29 日受理）