ハイブリッドワーク環境における
デジタル・フォレンジック

2021 年 12 月
名和 利男

1. はじめに

新型コロナウイルス感染症の影響が長引く中で、アフターコロナに向けて経済社会が以前から大きく変わろうとしている。特に、在宅勤務等のテレワークの導入が進み、業務環境に大きな変化をもたらしている。

テレワークの推進はコロナ禍以前から総務省が推進してきた施策であるが、コロナ禍においては、閣議決定(全閣僚が合意して政府の方針を決定すること)で次のような「テレワークの推進」の方針が出されている。

少子化社会対策大綱 【令和 2 年 5 月 29 日閣議決定】[1]	「子育てと仕事の両立やワーク・ライフ・バランス、労働生産性向上、非常時における業務継続性の確保等の観点から、『世界最先端デジタル国家創造宣言・官民データ活用推進基本計画』等に基づき、情報通信技術を活用した、時間や場所を有効に活用できる柔軟な働き方であるテレワークについて普及促進を図る。」
成長戦略実行計画・成長戦略フォローアップ・令和 2 年度革新的事業活動に関する実行計画 【令和 2 年 7 月 17 日閣議決定】[2]	「企業におけるテレワークの取組が促される中で、テレワークの場合の労務管理の方法の明確化を図る。また、中小企業によるテレワークのための通信機器の導入について、支援の強化を図る。さらに、中小企業等のサイバーセキュリティ対策を支援する。」 「テレワークにおける適切な労務管理のためのガイドラインの周知啓発を行うとともに、新型コロナウイルス感染症の感染拡大の防止の観点からも、テレワーク相談センターの設置・運営やテレワーク導入に係る助成等による導入支援を強力に推進する。」 「新型コロナウイルス感染症の影響も踏まえ、テレワークに関して通信機器等の導入支援や相談体制の拡充等を行い、導入意向のある全ての中小企業がテレワークを実践できる環境を整備し生産性向上に繋げる。」
経済財政運営と改革の基本方針 2020 【令和 2 年 7 月 17 日閣議決定】[3]	「テレワークの定着・加速を図るため、新たなKPIを策定するとともに、中小企業への導入に向けて、専門家による無料相談対応や全国的な導入支援体制の構築など各種支援策を推進する。さらに、事業場外みなし労働時間制度の適用要件に関する通知内容の明確化や関係ガイドラインの見直しなど、実態を踏まえた就業ルールの整備に取り組む。」
世界最先端デジタル国家創造宣言・官民データ活用推進基本計画 【令和 2 年 7 月 17 日閣議決定】[4]	「略)これまでも、「新型コロナウイルス感染症に関する緊急対応策―第2弾―」(令和 2 年 3 月 10 日新型コロナウイルス感染症対策本部決定)等により、中小企業に対するテレワーク導入経費の補助や、テレワーク導入を図る企業や地方公共団体等に対する専門家(テレワークマネージャー)の無料相談対応等に取り組んできているが、こうした支援策を更に進める必要がある。(略)」 「このため、テレワークの普及に当たっては、関係府省庁が連携し、テレワークに必要な IT システム導入支援、専門家による相談体制やサテライトオフィス、必要なネットワーク環境の整備、ガイドラインの周知等に取り組むとともに、企業の取組を踏まえつつ、テレワーク・デイズやテレワーク月間の実施や表彰等の周知による啓発にも取り組む。KPI の目標値達成については、緊急事態宣言を受けた企業の取組の状況を踏まえた上で設定する。」
まち・ひと・しごと創生基本方針 2020 【令和 2 年 7 月 17 日閣議決定】[5]	「略)また、中小企業によるテレワーク通信機器の導入等の支援や、GIGA スクール構想の実現に向けた学校の ICT 環境整備やオンライン診療の適切な実施に向けた環境整備等、リモートサービス導入推進に向けた環境整備に取り組む。」

表 1　国によるテレワーク推進の方針(下線は筆者)

[1] 少子化社会対策大綱　https://www8.cao.go.jp/shoushi/shoushika/law/taikou_r02.html
[2] 成長戦略実行計画・成長戦略フォローアップ・令和 2 年度革新的事業活動に関する実行計画 https://www.kantei.go.jp/jp/singi/keizaisaisei/index.html
[3] 経済財政運営と改革の基本方針 2020　https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/2020/decision0717.html
[4] 世界最先端デジタル国家創造宣言・官民データ活用推進基本計画 令和 2 年 7 月 17 日 https://www.kantei.go.jp/jp/singi/it2/decision.html
[5] まち・ひと・しごと創生基本方針 2020　https://www.chisou.go.jp/sousei/info/index.html

© TOSHIO NAWA

国による強い方針に基づき、各省庁がさまざまな施策を多角的に推進してきたことで、企業におけるテレワークの導入が一気に進んだ。内閣府が、2021 年 11 月 1 日公表した「新型コロナウイルス感染症の影響下における生活意識・行動の変化に関する調査[6]」によると、図 1 のとおり、地域および企業規模に関係なくテレワーク実施率は着実に増加している。

このテレワーク実施の形態に着目すると、「テレワーク中心（50%以上）」と「定期的にテレワーク（出勤中心：50%以上）」という「ハイブリッドワーク」が非常に多いことがわかる。

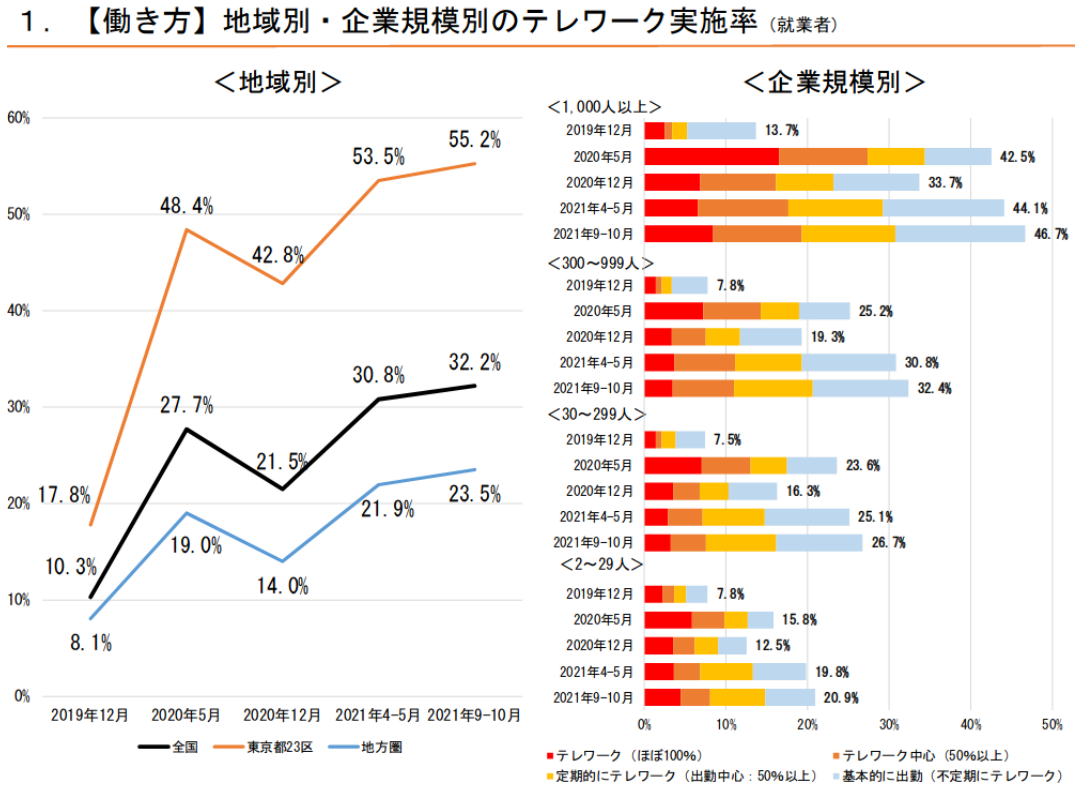

図 1:【働き方】地域別・企業規模別のテレワーク実施率（就業者）

一方、テレワークに起因したセキュリティインシデント発生も増加している。2020 年 9 月、個人情報保護委員会が、「テレワークに伴う個人情報漏えい事案に関する注意事項[7]」を公表し、実際に確認した個人情報漏えい事案の個別事例の内容と具体的な対策例を説明した。

この他にも、さまざまな種類のセキュリティインシデントが発生している。しかし、個人情報の漏洩や第三者に対する深刻な影響が発生しない限り、それぞれの企業や団体に閉じた形で対処が行われるケースが多くみられ、情報共有が活性化しづらい状況となっている。そのため、他所において発生抑止や被害防止につながる仕組みが整備されているとは言い難い。

これに対して、政府機関や情報セキュリティ関連団体が、ガイドラインや手引きなどを提供している。内閣サイバーセキュリティセンター（NISC）が 2021 年 9 月から運営しているポータルサイトにおける「情報セキュリティ関連の施策一覧[8]」の中で、テレワークのセキュリティガイドラインをいくつか見つけることができる。

[6] 新型コロナウイルス感染症の影響下における生活意識・行動の変化に関する調査　2021 年 11 月 1 日
https://www5.cao.go.jp/keizai2/wellbeing/covid/index.html
[7] テレワークに伴う個人情報漏えい事案に関する注意事項
https://www.ppc.go.jp/news/careful_information/telework/
[8] 情報セキュリティ関連の施策一覧　https://security-portal.nisc.go.jp/curriculum/

しかしながら、いずれのガイドラインも、セキュリティインシデントの発生抑止や被害防止を追求したものとなっているが、「セキュリティインシデントに備えた準備と発生時の対応」については、「インシデント対応計画を策定し、セキュリティインシデント発生時に速やかに対応・復旧ができるようにする」という要求事項が記載されているだけで、具体的な指南や参考となる事例が示されていない。

筆者の対処支援の中で観察している限りであるが、インシデント対応計画の策定と見直しの指示を受けた担当者は、自らの経験や知識の範囲で計画を作成することになるため、どうしても曖昧で漏れがある内容になってしまうことが多い。

そして、その「インシデント対応計画」において、最も重要なプロセスは、「発生箇所の特定」、「影響の評価」、「根本原因の追求」などであるが、いずれも後述する「デジタル・フォレンジック」の技術や手法を利用した調査を行うことになる。一般に、オフィス環境においては、インシデントに対する「備え」の一つとしてログ等の積極的な記録と保存および管理を行っていることが多いため、インシデント発生時の対応の難易度はそれほど高くない。しかし、一般的な在宅環境においては、ログの記録や保存は限定的であるため、PC やスマホ等のデバイスに残存している証跡を取得するなど、高度なデジタル・フォレンジック技術を利用した調査を行わなければならないことがある。

つまり、在宅環境においては、セキュリティインシデントに対する「備え」の不足や制約により、「発生時の対応」の難易度は高いといえる。特に、テレワーク（在宅勤務）と出勤（オフィス勤務）が混在したハイブリッドワークの環境では、これらの難易度は格段に上がる。

そこで、本コラムでは、このようなハイブリッド環境におけるデジタル・フォレンジックのあり方について考察する。

2. ハイブリッドワーク環境について

「ハイブリッドワーク」の一般的な定義は、「自宅で少なくとも週に 1 日は仕事をして、他の日はオフィスで仕事をすること」であるが、そのアプローチは、「働く場がどこであっても、働く人のために、働く体験をデザインすること」である。これにより、社員は、オンサイトでもオフサイトでも、また移動中であっても自由に働けるようになっていく。

ハイブリッドワークへの移行は、コロナ禍により加速化したことは事実であるが、それ以前から、一部の企業において推進されていた。スマートフォンからクラウドコンピューティングに至るまでのテクノロジーの進歩により、どこからでも作業やコラボレーションが可能となってきたためである。

多くの企業が、コロナ禍により大きく変化したビジネスモデルや業務プロセスに対応しようと、新たなテクノロジーへの投資を行ったが、テレワークの推進により、出勤機会の低減やオフィスに関連したコストを大幅に減少させている。これにより、経済的合理性の観点から、企業が以前の業務環境に戻る可能性を低くしているといえる。今後、競争上の優位性の獲得を狙う企業は、テレワーク環境を進展させていくと考えられる。一方、在宅勤務においては、仕事とプライベートの曖昧さやインターネットの通信速度の限界などにより、ストレスが積み重なったり、コミュニケーション不足による孤独感や業務評価への不安が発生したりするなどの課題がみられる。また、インターネットの利用が困難な業務プロセスや、そのシステムにアクセスするために出勤する必要性も一部残っている。そのため、ハイブリッドワークの環境を選択した企業は、その環境に適応した業務プロセスや労務管理などの仕組みを改善していくことになる。

さらに、働き方が柔軟になった影響で、キャリアアップや転職を意識する社員が増えていると言われている。一般に、優秀な社員は、仕事の手順や裁量が任されている環境で、十分なスキルと知識を持って、高い生産性を発揮できる。そのため、ハイブリッドワーク環境は、そのような優秀な社員を獲得するためにも、維持および進展させて行く必要があるといえる。

ちなみに、東京都産業労働局が 2021 年 3 月に公表した「多様な働き方に関する実態調査(テレワーク)結果報告書[9]」によると、図 2 のとおり、テレワークの継続意向について、 7 割以上が「継続したい」と回答している。

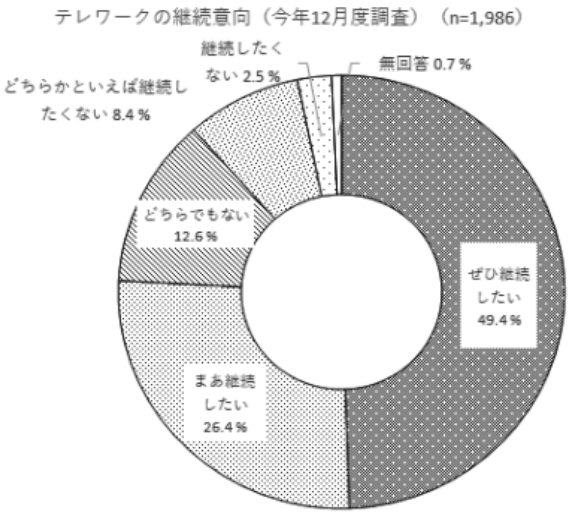

図 2: テレワークに関する今後の意向

3. ハイブリッドワーク環境を実現するシステム

このように、アフターコロナでも進展していくと考えられるリモートワーク環境を実現するシステムは、リモートワーク環境の捉え方により大きく異なる。その大まかな区分けは、「ハイブリッド・ワークプレイス(業務場所)」、「ハイブリッド・ワークスペース(業務空間)」という表現で示すことができる。

- ハイブリッド・ワークプレイス(業務場所)
  ワークプレイス(業務場所)の概念を、従来の「会社の物理的なオフィス」から大きく変更せずに、社員が在宅勤務であっても、VPN などを介したリモートアクセスにより、オフィスのオンプレミスのシステム上で業務を行うことが多い。
- ハイブリッド・ワークスペース(業務空間)
  社員は、会社のオンプレミスのシステムに依存あるいは制約を受けることなく、クラウドサービスをベースに「いつでも、どこでも」業務を行うことができる。

今後、クラウドサービスの進展とともに、ハイブリッドワークの環境は、業務が行われる場所(ワークプレイス)を中心した形態から、社員がより自由に業務を行うことが可能な空間(ワークスペース)と形態に移行すると考えられる。

[9] 多様な働き方に関する実態調査(テレワーク)結果報告書
https://www.hataraku.metro.tokyo.lg.jp/hatarakikata/telework/30_telework_tyousa.pdf

これを裏付けるものとして、2021 年 6 月、経産省が公表した「半導体・デジタル産業戦略[10]」の中で、データセンターなどのデジタルインフラを迅速かつ計画的に整備していくことが掲げられており、現在、データセンターの整備に関する有識者会合[11]が行われている。さらに、2021 年 11 月、政府が推進している「デジタル田園都市国家構想[12]」を実現するために、地方でのデータセンターや光ファイバー海底ケーブルの整備で 1000 億円超の予算措置をとるとした。

さらに、「クラウドファースト」と呼ばれる、システム開発時にクラウドサービスの利用を優先する考え方に基づいたクラウド利用が進展している。政府においても、2021 年 3 月、各府省情報化統括責任者（CIO）連絡会議が決定した「政府情報システムにおけるクラウドサービスの利用に係る基本方針[13]」において、政府情報システムの構築・整備に関しては、クラウドサービスの利用をデフォルト（第 1 候補）として考える「クラウド・バイ・デフォルト原則」が出された。

現在は、ハイブリッド・ワークプレイスとハイブリッド・ワークスペースが混在している状況であるが、今後、民間企業および政府機関でもクラウドファーストの浸透が加速すると見られるため、クラウドベースのハイブリッド・ワークスペースに偏っていくと考えられる。

4. ハイブリッドワーク環境におけるデジタル・フォレンジック

ハイブリッドワーク環境を構成するいずれかのシステムにおいてセキュリティインシデントが発生した場合、あるいはその環境で行われる業務活動において法的紛争や訴訟が起こった場合、電磁的記録の証拠保全および調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・ 情報収集等を行うことになる。このような一連の技術的調査手法や技術が「デジタル・フォレンジック」である。

従来までのデジタル・フォレンジックは、「電磁的記録の証拠保全および調査・分析」を行う対象を、その実施を求める主体が「保有および管理するオンプレミスシステム」と想定していた。そのため、ハイブリッドワーク環境において、従来のデジタル・フォレンジックの知識体系を利用することが困難な状況が見られる。例えば、次のようなシーンである。

- 従業員の自宅において発生したセキュリティインシデント
- クラウドサービス提供事業者において発生したセキュリティインシデント

いずれも、「電磁的記録の証拠保全および調査・分析」を実施するには、従業員や他社（クラウドサービス提供事業者）から献身的な協力を期待することになる。

そのため、ハイブリッドワーク環境におけるデジタル・フォレンジックは、事前に「電磁的記録の証拠保全および調査・分析」を行う対象のシステムを保有および管理する主体（従業員やクラウドサービス提供事業者）に対して、セキュリティインシデント発生時に備えた取り決めとその実効性の確保をしておく必要がある。しかし、次のようなケースでは一定の限界が発生する。

- 従業員が、他社から指揮命令を受ける派遣社員である場合
- クラウドサービス提供事業者が、個別対応を受け付けないパブリッククラウドである場合

現時点では、このようなケースは非常に少ないと考えられるため、以下の知見は、従業員やクラウドサービス提供事業者との事前の取り決めができているという前提とする。

---

[10] 半導体・デジタル産業戦略 https://www.meti.go.jp/press/2021/06/20210604008/20210604008.html
[11] デジタルインフラ（DC等）整備に関する有識者会合
https://www.meti.go.jp/policy/mono_info_service/joho/conference/digital_infrastructure.html
[12] デジタル田園都市国家構想 https://www.cas.go.jp/jp/seisaku/digital_denen/index.html
[13] 政府情報システムにおけるクラウドサービスの利用に係る基本方針
https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210330.pdf

4-1. リモートフォレンジック

コロナ禍で緊急避難的に導入されたテレワーク環境において、さまざまなセキュリティインシデントや内部犯行が発生したが、「電磁的記録の証拠保全および調査・分析」を行うにあたり、幾つかの困難な状況が見られた。例えば、インシデントの発生場所が、数百キロ離れている従業員の自宅であったため、迅速な証拠保全ができず、なかなか調査に着手できないという事例が多数みられた。

このような状況においては、リモート機能を使ったデジタル・フォレンジック（以下、リモートフォレンジック）を行うことになる。コロナ禍以前は、調査に係るコストを抑制するためにリモートフォレンジックを選択することが多かったが、ハイブリッドワーク環境では、遠隔地での業務が一般的になったことで、リモートフォレンジックの抵抗感が薄らいできている。

リモートフォレンジックの知識体系は、最近のサイバー環境に対して十分とは言えないが、必要な知識体系が整備されており、有用なツールも提供されている。

従来のデジタル・フォレンジックと比べると、リモートフォレンジックには、幾つかの前提や制約がある。特に、インシデントが発生した遠隔地（以下、オンサイト）にあるデバイスの管理者の献身的な協力が必要となるところである。この作業は、フォレンジック専門家がインターネットを介して、オンサイトのデバイスにリモートアクセスして証拠を収集して取得することであるが、デバイス上のデータ量が非常に大きい場合あるいは証拠の取得の必要性が低い場合、リモートアクセスした状態で調査および分析を実施することもある。

このようなリモートフォレンジックにおいて必要なものは、VPN などの「暗号化通信」と、第三者に認証されかつ十分にテストが行われた「フォレンジック専用ツール（特に証拠収集ツール）」である。ワークフローは、プロセス全体を通して電磁的証拠の完全性を確保するように設計されたものでなければならない。特に留意すべき事項としては、「Forensically-Sound」と呼ばれる「法科学的に見て健全な」状態を確保することである。この概念は、電磁的証拠は改ざんや欠損が発生しやすい特性を持つため、取得した証拠が正しいことを保証し、第三者による検証が可能な手法や手続きを取ることを求めるものである。

一般に、デジタル・フォレンジックでは、証拠に手を加えることなく保存することが常に基本となっている。従来の知識体系では、電源を切った状態のマシンをイメージングしたり、フォレンジック用の OS を起動したりして作成したデッドボックス・イメージ（ライブホストから取得され、オフラインで検査されたハードドライブのイメージのこと）のみを扱っていた。リモートフォレンジックが広く利用されるにつれ、この原則は変容しつつある。最近のリモートで行うことが可能なライブイメージングツールは、技術と信頼性が向上している。

4-2. オンサイトに取得用デバイスを設置

リモートフォレンジックの作業は、通常、オンサイトに「取得用デバイス」を設置して行う。このデバイスは、外付けの USB ハードディスクや、オンサイトに緊急的に発送したノート PC などになることが多い。もし、対象デバイスがネットワークストレージと接続されている場合、ネットワークストレージに証拠を転送させることで、「取得用デバイス」を利用することなく、証拠収集を遠隔で実施できることがある。

残念ながら、ほとんどのオンサイトのインフラでは、ストレージデバイスに「オーバー・ザ・ワイヤー（ケーブルを介した）のフォレンジックイメージング」をサポートしていない。そのため、リモートフォレンジックにおいては、オンサイトに「取得用デバイス」と「証拠収集ツール」が必要となる。ただし、既存のネットワークストレージそのものを対象とする場合は、必要としないことがある。

オンサイトで収集された証拠を保存した「取得用デバイス」は、フォレンジック専門家の手元に送り届けるが、保存したデータが大きくない場合は、SFTP などのセキュアなプロトコルでリモート転送し、調査および分析を迅速化することがある。

4-3. リモートフォレンジックにおいて留意すべき事項

デジタル・フォレンジックによる調査結果が、裁判等の係争で利用される場合、「電磁的証拠」の取得および保全に係るプロセスや作業をフォレンジック専門家が証明しなければならないことがある。具体的には、提出された「電磁的証拠」に証拠力があることを裁判官等に説明することが求められる。

さまざまな説明方法があるが、リモートアクセスのためのソリューションを利用して、専門家が実際にリモートアクセスを模擬環境で再現した上で、オンサイトを想定したデバイスを起動させ、ライブイメージを実行し、フォレンジックイメージを作成する過程を、裁判官等に観察させることがもっとも効果的である。この際、誰が「取得用デバイス」を対象デバイスに接続したのかを立証する必要がある。

4-4. リモートフォレンジックの現実は厳しい

実際には、「電磁的証拠」の収集、取得、保全のために、直接オンサイトに行かなければならない状況が多い。この大きな理由は、デジタル・フォレンジックを支援する技術的に優れた人材が非常に少ないことである。オープンソースや有償を問わず、有用なフォレンジックツールが広く普及しているが、デジタル・フォレンジックの前提となる厳格な手続きや配慮事項に精通している必要がある。その他、オンサイトへのリモートアクセスに必要となる IT 管理者やネットワーク管理者の支援が得られない場合や、オンサイトにおいて協力が必要となる管理者による作業に完全性が疑われる、つまり正確な証拠収集作業をすることが期待できない場合などがある。

5. おわりに

これまでの情報通信技術やインターネットをベースにした環境変化の過程を眺めると、変化のたびに、多くのユーザーがそれまで発生していなかった新たな問題に困惑し、いたずらに被害を拡大させてしまうことを繰り返してきた。そして、そのような被害事例が必然的に集約され、分析や共有が積極的に行われることで、対策と浸透がはじまり、発生抑止や被害軽減に繋がっていく。ところが、その実現の頃には、すでに次の変化が始まり、新たな問題が発生している。

今後、ハイブリッドワーク環境は、アフターコロナのニューノーマルの一つになると考えられる。この環境で発生する問題は、これまでとは比較にならない深刻な被害を発生させるものであるにも関わらず、発生抑止や被害軽減の仕組みを十分に作ることすら困難なものとなる。特に日本型企業は、すでに実効性の欠けたレガシーなセキュリティ戦略やプラクティスから抜け出せず、問題解決に最善な戦略と取り組みに懸念すら抱く傾向がみられる。そして、依然として周囲が採用したものに無自覚に同調する姿勢が強い。

今後のハイブリッドワーク環境は、オンプレミス環境では容易だった「発生したセキュリティインシデントに対する状況把握」の難易度が格段に高まることを理解し、それを受け入れる姿勢を持たなければならない。その上で、「電磁的証拠」の収集、取得、保全を迅速かつ確実に実施できる態勢の整備が急務である。

（了）