テレワークでPC紛失、もう諦めるしかない?
盗難・紛失への情報漏えい対策

～情報漏えいのピンチを救うセキュリティ対策～

コロナ禍により急速にテレワークの導入が進んだものの、PCにおける情報漏えい対策の課題が顕在化

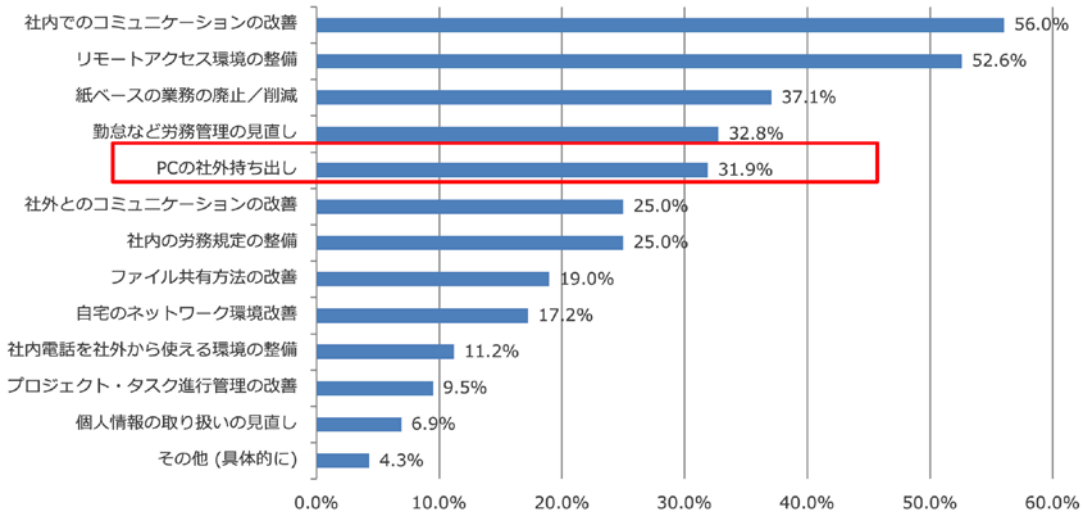
2020年4月の緊急事態宣言から約1年が経過し、新型コロナウイルス感染症拡大防止対策のためにテレワークを導入した企業も少なくない。しかし、急な導入を迫られたためさまざまな課題が顕在化してきているようだ。その中のひとつが「PCを社外に持ち出す際の情報漏えい対策」である。

ITmediaビジネスオンラインが行ったアンケート調査では、リモートワークを継続的に実施している企業が、そのために注力したこととして、「社内でのコミュニケーションの改善」「リモートアクセス環境の整備」「紙ベースの業務の廃止／削減」「勤怠などの労務管理の見直し」に続き「PCの社外持ち出し」（32%）を挙げたのに対し、未実施の企業では「PCを社外に持ち出せない」（11%）ことは大きな課題として認識されていない。つまり、リモートワークのためにPCを刷新し、継続的にテレワークをする段階になってはじめて、PCの持ち出しリスクに関する課題が顕在化していることが分かる。

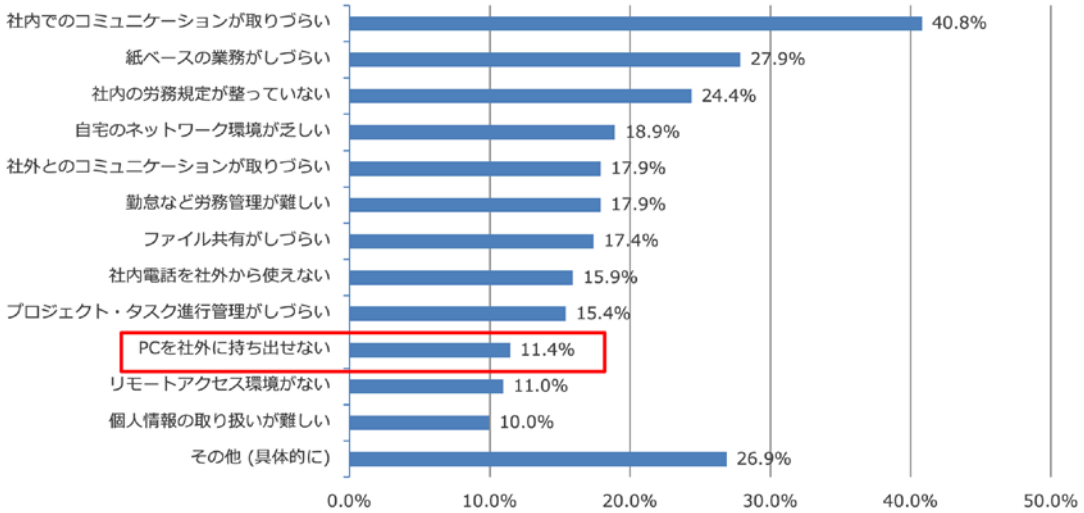
昨今の情勢から「ノートPC／モバイル／タブレット端末」の刷新を検討する企業は多いが、テレワークを継続する上で重要なポイントになっているPCの社外持ち出しに伴うセキュリティ課題をどう解決すればよいのか。

テレワーク導入において押さえるべき3つのセキュリティポイント

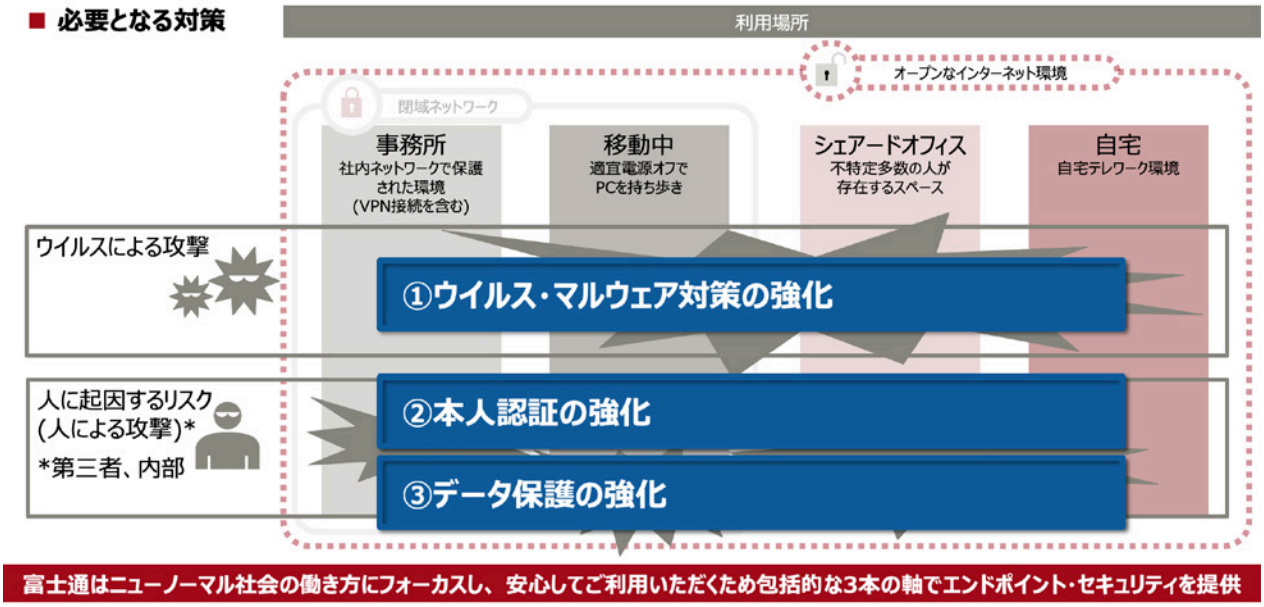
2020年7月、ニューノーマル時代における新たな働き方として「Work Life Shift」というコンセプトを掲げ、固定的な場所や時間にとらわれず、約8万人の従業員が“原則テレワーク”に移行した富士通は、PCにおけるセキュリティ対策を整理・分析し、3つの対策を取るべきだと定めた。脅威の種類は大きく分けて「ウイルスによる攻



リモートワーク実施企業が「リモートワークを継続／実施するにあたって注力したこと」
2020年12月～21年1月実施　ITmediaビジネスオンライン「働き方（リモートワーク）に関する調査レポート」より抜粋



リモートワーク未実施企業が「リモートワークを継続／実施しにくい要因」
2020年12月～21年1月実施　ITmediaビジネスオンライン「働き方（リモートワーク）に関する調査レポート」より抜粋



撃」と「人に起因するリスク（内部／第三者による攻撃）」の2つある。この2つの脅威に対し、オフィス、移動中、シェアードオフィス、自宅という利用シーンを想定すると、セキュリティ対策は「ウイルス、マルウェア対策の強化」「本人認証の強化」「データ保護の強化」の3つが必要だと考えたのだ。

富士通は、これらの3つのセキュリティ対策のために、さまざまな技術を開発・提供している。

1つめの「ウイルス、マルウェア対策の強化」としては、BIOSを狙う新型マルウェアからBIOSを保護し自動復旧できる、富士通が独自に開発した新しいハードウェア「Endpoint Management Chip」（EMC）を、2つめの「本人認証の強化」では確実な本人認証を実現するソフトウェア「AuthConductor Client Basic」を提供している。

とりわけ多くの経営者や情報システム部門が重要視するセキュリティ対策が3つめの「データ保護の強化」であろう。テレワークに後ろ向きになる理由の多くが、情報漏えいのリスクがあることからも「データ保護の強化」はテレワークにとって避けることのできない課題と言える。そこで富士通では「データ保護の強化」として、遠隔から即座にPC内のデータ消去を実施したり、スマホでPCをロックしたりすることが可能な「CLEARSURE（クリアシュア）」というソリューションを提供している。

現在、各社から数多くの盗難・紛失による情報漏えい対策ソリューションが提供されているが、どれも同じというわけではない。次項では、盗難・紛失による情報漏えい対策ソリューションに求められる機能を解説する。

盗難・紛失による情報漏えい対策ソリューションに求められる機能は「PCの電源がオフでも機能する」こと

PCを社外に持ち出すと、移動中の電車でかばんごと網棚に置き忘れたり、シェアードオフィスで席を外した隙に盗難にあったりするなど、情報漏えいにつながるリスクにさらされる。そのため、盗難や紛失に気づいた時に即座にPCロックやデータ消去ができることがデータ保護の強化対策として最も重要なポイントになる。

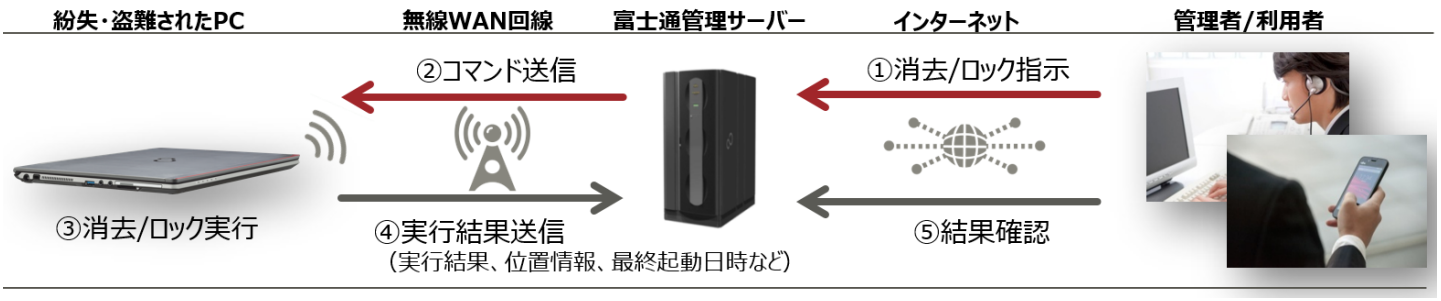
しかし、一般的なデータ消去のソリューションでは、動作条件としてPCの電源がオンでインターネットに接続されている必要がある場合がほとんどだ。これでは電源がオフのときにはデータを消去できず、情報漏えいのリスクが残ったままになってしまう。

富士通が提供する盗難・紛失による情報漏えい対策ソリューション「CLEARSURE」の最大の特長は、PCの電源がオフの状態でも、無線WAN回線を利用してリモートからデータ消去やPCをロックできる点だ。できるだけ長時間使えるように電源をオフにした状態でPCを持ち歩くユーザーは多い。そのため電源がオフの状態でもデータを消去できる点は、安全・安心にテレワークを行うために非常に重要なポイントとなる。

システム管理者だけではなくユーザー自身でもPCロックなどの情報漏えい防止操作が可能

CLEARSUREではシステム管理者による遠隔操作でPCのロックや内蔵ドライブのデータ消去ができるほか、実行結果や最後にPCが起動された時刻、リモート指示を実施した時点でのPCの位置情報も把握できる。これらの情報を情報漏えいの発生有無の判断やPCを捜索する際の手掛かりとして活用することが可能だ。さらにユーザー自身がスマートフォンからPCをロックする運用も可能なので、休日や土日、深夜などでシステム管理者とすぐに連絡が取れない場合でもスピーディーな対策をとることができる。

CLEARSUREからのロック指示を受信したPCのロック処理が正常に完了すると、システム管理者からのロック解除指示がない限り



CLEARSUREの仕組み

PCは起動できなくなるため、第三者がPCを立ち上げて操作することは不可能だ。「データ消去」を実行した場合、PCに搭載されている暗号化機能付きのHDD／フラッシュメモリディスクの暗号鍵が上書き消去される。これにより全てのデータを無効化するため、本体を分解してドライブを抜き取ってもデータを復元することはできない。

シンプルな管理画面もCLEARSUREの特長である。システム管理者がログインすると、管理端末一覧が表示される。そこから対象の端末を選択して「端末ロック」「データ消去」などのメニューを選択、実行するだけでよい。

生命保険会社でも採用実績がある情報漏えい対策ソリューション「CLEARSURE」

ある生命保険会社では、全国1万2000人の営業職員が利用するタブレットPCでCLEARSUREを活用している。手のひら静脈認証と組み合わせることで、より強固なセキュリティを確保し運用されている。また、ある流通小売企業では、顧客向けサービスのデジタル化に伴い、店頭に顧客向けのタブレットPCを設置した。その際、閉域LTE網とCLEARSUREを併用することで、不特定多数のユーザーが操作する端末のデータを安全かつ確実に保護できる仕組みを実現している。CLEARSUREは、これらの事例以外でも重要なデータを扱う企業で数多く活用されている実績のあるソリューションだ。

テレワークにおけるセキュリティ対策に最適なCLEARSURE

CLEARSUREを導入することによって、高度なセキュリティを実現するだけでなく、オフィス以外で仕事をするユーザーに安心感を与え、利便性を向上させることができる。さらには情報システム部門の情報漏えいに対する不安を取り除き、運用負担の軽減も可能だ。

生産性を維持・向上しながら安全・安心なテレワークの実現を求めている企業にとって、CLEARSUREはまさに効果的なセキュリティ対策であると言えるだろう。

CLEARSUREの管理画面

お問い合わせ先

〔購入相談窓口〕通話料無料　0120-959-242

受付時間　9:00～18:00（土・日・祝日、当社指定の休業日を除く）

※富士通パートナー及び弊社担当営業から購入を希望されるお客様は、直接担当者へお問い合わせください。