テレワーク時代の情報漏えい対策
PCの紛失や盗難はゼロにできない
今こそ求められる効果的な情報漏えい対策

コロナ禍を背景にテレワークが普及し、PCの紛失や盗難のリスクが増えている。厳格な社内ルールによって業務効率を下げることなく情報漏えいを防ぐ対策が必須だ。どの企業でも実践しやすい3つの具体策とは。

テレワークの普及を背景にPCを社外に持ち出すケースが増え、PCの紛失や盗難によるデータ漏えいのリスクが高まっている。

企業によっては、従業員に申請書の提出を義務付けたり、社外でのPCの管理を徹底させたりといった対策を打っている。ルールを厳格化すればユーザーの利便性を損なう一方、盗難や紛失のリスクをゼロにはできない。テレワークによってPCの持ち出しが常態化した今、あらゆる場所で盗難や紛失が発生することを前提とした情報漏えい対策を講じる必要がある。

有効策といわれているシンクライアントも、コストや構築工数、利便性の低下などが導入のネックになることもあるだろう。一方、従業員の業務効率を下げずに、低コストで持ち出しPCのデータを保護する方法がある。あらゆる企業にマッチする3つの具体策を紹介しよう。

シンクライアントではユーザーのニーズに応えきれない

PCの盗難や紛失による情報漏えいは企業に大きなダメージを与える。テレワークが常態化した今、多くの企業がこのリスクを身近に感じているのではないか。富士通が実施したアンケートによれば、ビジネスパーソンの約2割が「PCの盗難、紛失などによる情報漏えいが心配」だと答えている（図1）。

富士通は、2009年からこの課題に取り組んできた。同社は当時、約16万台のPCが稼働しており、そのうち約7万台は社外に持ち出すことを前提にしたモバイルPCだった。持ち出しの際は、申請書の提出などを義務付け、機密情報を扱う部署ではPCの持ち出しを禁止するなど、厳格なルールを設けていた。

だがルールを厳格化するあまり、出張先で業務を行えない、顧客先でプレゼンテーションができないなどの問題が生じた。富士通の本並裕輔氏（CCD事業統括部 プロダクトマネジメント部）は「報告書を作成するだけのために出張先から会社に戻らなければならないなど、業務効率の低下が問題視されていました」と当時を振り返る。

業務効率を下げてまで厳しいルールを設けても、社外にPCを持ち出す以上は盗難や紛失のリスクをゼロにはできない。そこで同社のIT管理部門とPC開発部門が協力して盗難・紛失による情報漏えい対策を目的としたソリューションの開発に踏み出した。

「どんなに細心の注意を払っていたとしてもPCの盗難や紛失事故は起こり得るという前提に立って、どうすればPC内部のデータを

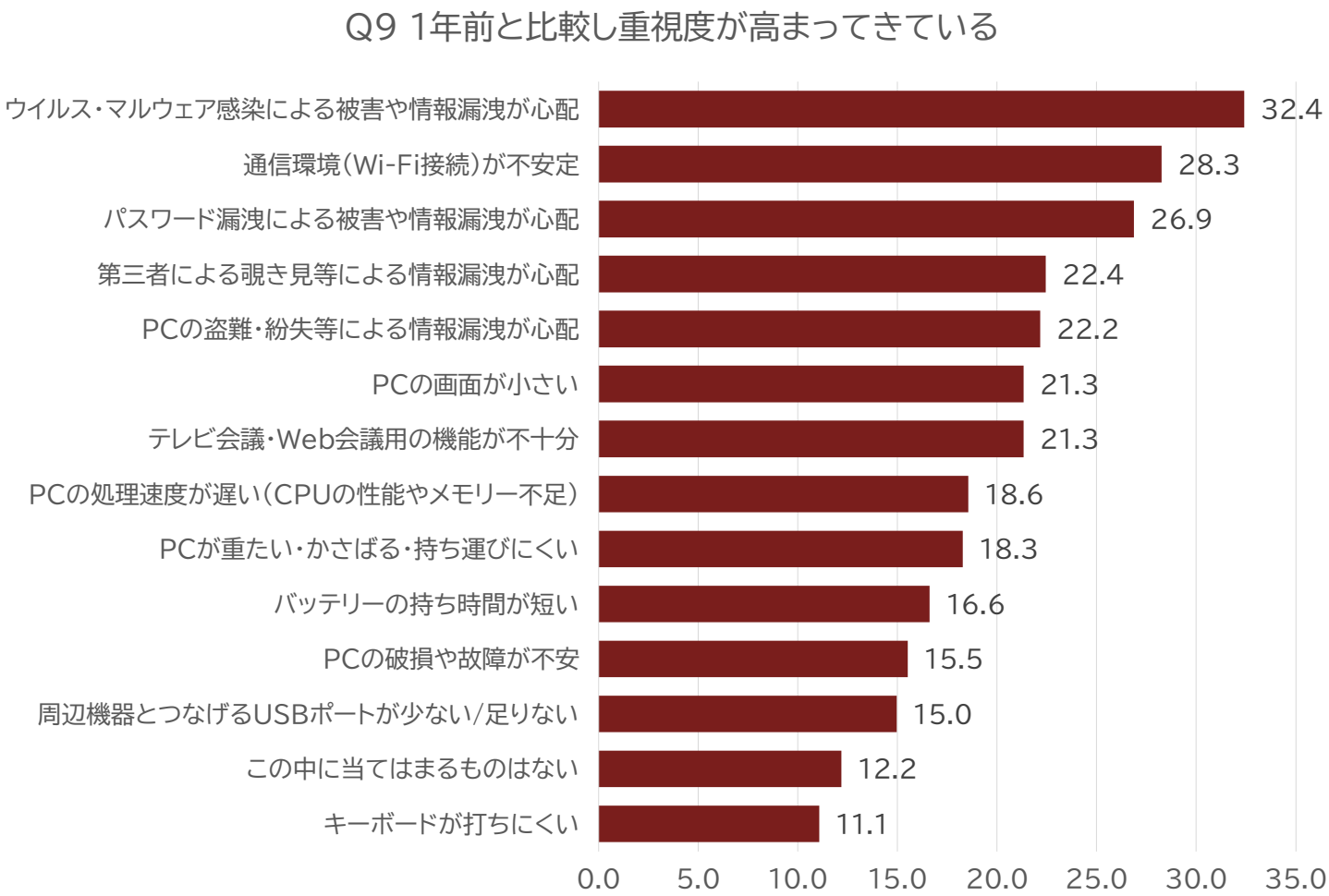

図1　1年前と比較して「重視」しているPC利用環境における課題（出典：富士通の2021年3月調査結果）

盗まれないようにできるかを徹底的に議論しました」（本並氏）

こうして誕生したのが、PCを遠隔からロック、消去できる「CLEARSURE（クリアシュア）」だ。

情報漏えいの防止策としてシンクライアントを使う手もある。だが本並氏によれば、シンクライアントの導入にはそれなりのコストや工数が掛かり、予算や人的リソースが潤沢ではない企業にとってはハードルが高い。シンクライアントは仮想環境に接続するための専用端末であり、端末の機能を最小限に抑えている分、ユーザーの利便性にも影響があるという。こういった面からシンクライアントを導入できないケースも多いだろう。

そこで富士通はPCの有用性を生かしつつ、情報漏えいを防ぐソリューションとして、前出のCLEARSUREに加え、PCのデータを秘密分散の技術で保護する「Portshutter Premium Attachecase（ポートシャッタープレミアム アタッシュケース）」、外部デバイスやネットワークの接続を制御する「Portshutter Premium（ポートシャッタープレミアム）」も取り揃えている。いずれも低コストで導入が可能だ。それぞれのソリューションにどのような特徴があるのか見ていこう。

PCの電源がオフでもデータを遠隔からロック、消去できる

PCのデータを遠隔から管理できるソリューションは珍しくないが、CLEARSUREは「PCの電源がオフの状態でも作動する」という点で他とは一線を画す。

CLEARSUREに内蔵されているLTE通信モジュールが、遠隔からのコマンドを受信して、PCのロック、消去を指示する仕組みだ。これによってPCの盗難・紛失の連絡を受けたシステム管理者が遠隔から素早くPCをロックしたり、PC内のデータを消去したりできる。データ消去はシステム管理者だけが実行できる機能だが、土日や深夜などシステム管理者とすぐに連絡が取れないときは、従業員自身がスマートフォンからPCをロックすることもできる。PCの盗難や紛失に気付いた時点でスピーディに対処できるので安心だ。

システム管理者はCLEARSUREの管理画面から、最後にPCを起動させた日時やデータ消去およびロックの実行結果、リモート指示を実施した時点でのPCの位置情報などを確認できる。取引先や経営層から情報漏えいの発生有無を問われた際にこうした情報を役立てられると本並氏は話す。

リモートデータ消去を提供する一般的なサービスの多くは、PCが電源オフの状態では機能しないが、CLEARSUREはハードウェアのカスタマイズを含む富士通の独自技術により電源オフ時のリモートデータ消去、PCロックを実現したという。ハードウェアとしてのPCと、セキュリティソリューションの両方を自社で提供する富士通の強みといえるだろう。

「リスクを排除するためにPCの持ち出しを禁止するというルールを決めるのは簡単ですが、業務効率は下がるでしょう。万一の盗難や紛失時にも有効な策を用意しておくことが重要です」（本並氏）

PCに保存したデータを秘密分散技術で守る

CLEARSUREを使えばリモートでデータを消去できるが、その作動条件としてPCがネットワーク圏内に置かれている必要がある。富士通の菰田吉康氏（CCD事業統括部　プロダクトマネジメント部）は、PCがインターネットにつながらない環境にあることを想定したデータ漏えい対策も必要だと話す。

「地下街やビルの内部など、都市部でもインターネットにつながりにくい場所があります。そこでPCをなくしてしまえば、遠隔からデータを操作することは難しい。このリスクにも対策が必要だと考えました」（菰田氏）

図2　Portshutter Premium Attachecaseは秘密分散でデータを守る

そもそも端末にデータを保存できないシンクライアントを使えばよいのではないかという考え方もあるだろう。しかし、シンクライアントを使用するにはネットワークに接続する必要があるため、圏外ではデータ閲覧や編集作業ができない点がネックとなる。シンクライアントではなくPCでの運用において、ローカルディスクに保存したデータを安全に利用できるようにするにはどうするべきか。

これを解決するのが「秘密分散」という技術を使って開発された「Portshutter Premium Attachecase」だ。ファイルを自動的に意味のないデータに変換し、オフィス内ではファイルサーバーとPCに分散保存する。出張やモバイルワークなどでユーザーがPCをオフィスの外に持ち出す際には専用のツールを使ってファイルサーバーに格納されている分散片をスマートフォンまたはUSBメモリに格納する（図2）。2つの分散片を結合できなければファイルを復元できないため、万一PCを盗まれたとしてもスマートフォンまたはUSBメモリさえ手元にあれば、第三者はファイルを開くことができないという仕組みだ。

「Portshutter Premium Attachecaseを使えば、ローカルディスクに保存したデータを安全に保護できます。ファイルは自動的に分散保存されますので、これまでと同じ操作性を実現。利便性と秘密分散による高いセキュリティを両立させています」（菰田氏）

PCのポートを制限し、フリーWi-Fi利用もカット

第三者によるデータ搾取を防止するPortshutter Premiumも持ち出しPCのデータ保護対策として有効だ。USBメモリなどの記憶媒体を接続するポートを遮断し、データの持ち出しを防止できる。

「もともとは企業の内部不正を防止するために開発したソリューションです。社内データの持ち出しを禁止するルールを設けてもそれを徹底するには限界がありました。システムによって内部不正を確実にブロックする手段が必要だと考えたのです」（菰田氏）

Portshutter Premiumでは登録された記憶媒体だけを利用できるように設定できる。登録されていない機器がPCに接続された場合はポートを遮断できるため、私物のUSBメモリやスマートフォンにデータをコピーできない。

その他、Portshutter Premiumはネットワークの接続を制御する機能もある（図3）。

「外出先で気付かないうちに許可されていないネットワークに接続し、データを盗まれてしまうケースがあります。Portshutter Premiumの最新バージョンはネットワークごとに接続の可否を設定して、危険性があるネットワークのパケット送受信を自動的に遮断します」（菰田氏）

Portshutter Premiumは、富士通の法人向けPC「LIFEBOOK U9311」「LIFEBOOK U7411」「LIFEBOOK U7511」などに標準装備されており、設定をすればすぐに利用できる。多数のPCに対して外部デバイスやネットワークの接続制御を一括で設定できる「Portshtter Premium V2 集中管理オプション」（別売り）も用意しており、主に大企業から引き合いがあるという。

働く場所を自由に選べる時代こそ、PCの紛失・盗難対策は必須だ。富士通の法人向けPCに標準搭載されているPortshutter Premium、無線WANモデルを選択することで利用可能なCLEARSURE、カスタムメイドのPortshutter Premium Attachecaseなどのソリューションを目的に合わせて活用することで、あらゆる規模の企業で従業員の利便性を損なわずに情報漏えいを防げる。

「個々のソリューションにはそれぞれの強みがあります。お客さまのニーズに合ったものを選び、二重三重の防御態勢を取っていただくことが重要だと考えています」（菰田氏）

■ 機能イメージ

図3　Portshutter Premiumの仕組み

強固なクライアントセキュリティに対応したテレワークモデル、LIFEBOOK U7シリーズ。

作業生産性を高める大画面（15.6型・14型）でありながら、持ち運びに便利な軽量タイプのLIFEBOOK U7シリーズ。オフィスワークから在宅ワークまでシームレスな働き方が実現できます。また、ウイルス・マルウェア攻撃の被害を最小限に抑えるEndpoint Management Chip（EMC）をはじめ、遠隔消去、生体認証、のぞき見防止など、さまざまなセキュリティ対策が可能です。富士通の法人向けPCに搭載したエンドポイントセキュリティについては、こちらをご覧ください。

14 型スリムモバイル
LIFEBOOK U7411

15.6 型スリムモバイル
LIFEBOOK U7511

FUJITSU Notebook LIFEBOOK U7シリーズは、インテル® Core™ i5 vPro® プロセッサー搭載（詳しくはこちら）

テレワークでストレスなく快適かつセキュアに作業をするには、第11世代インテル® Core™ i5 vPro® プロセッサー搭載機種をお薦めします。購入のご相談は、富士通または販売パートナーまでお問い合わせください。

※この冊子は、TechTargetジャパン（https://techtarget.itmedia.co.jp/）に2020年7月に掲載されたコンテンツを再構成したものです。
https://techtarget.itmedia.co.jp/tt/news/2107/01/news06.html

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）
富士通株式会社　〒105-7123 東京都港区東新橋1-5-2 汐留シティセンター
※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。