FUJITSU

テレワークで変わった「守るべきポイント」、今求められるセキュリティ対策まとめ

ウイルスやマルウェアによる攻撃、不正アクセスやのぞき見による情報漏えい、モバイル端末の紛失・盗難……。テレワークが当たり前になる中で、さまざまなセキュリティリスクが可視化され、守るべきポイントも「境界」から「端末」へと大きく変化している。「安全な業務環境など存在しない」ということを念頭に、エンドポイントであるノートPCのセキュリティ対策について再考したい。

テレワークの拡大とともに広がる新たな脅威

新型コロナウイルス感染症蔓延への対策をきっかけに、日本国内で急速に進んだテレワーク。オフィスだけでなく、自宅やカフェ、シェアオフィスなど、場所を選ばずに働けるワークスタイルが広がったことは、コロナ禍以前から叫ばれてきた働き方改革も踏襲している。

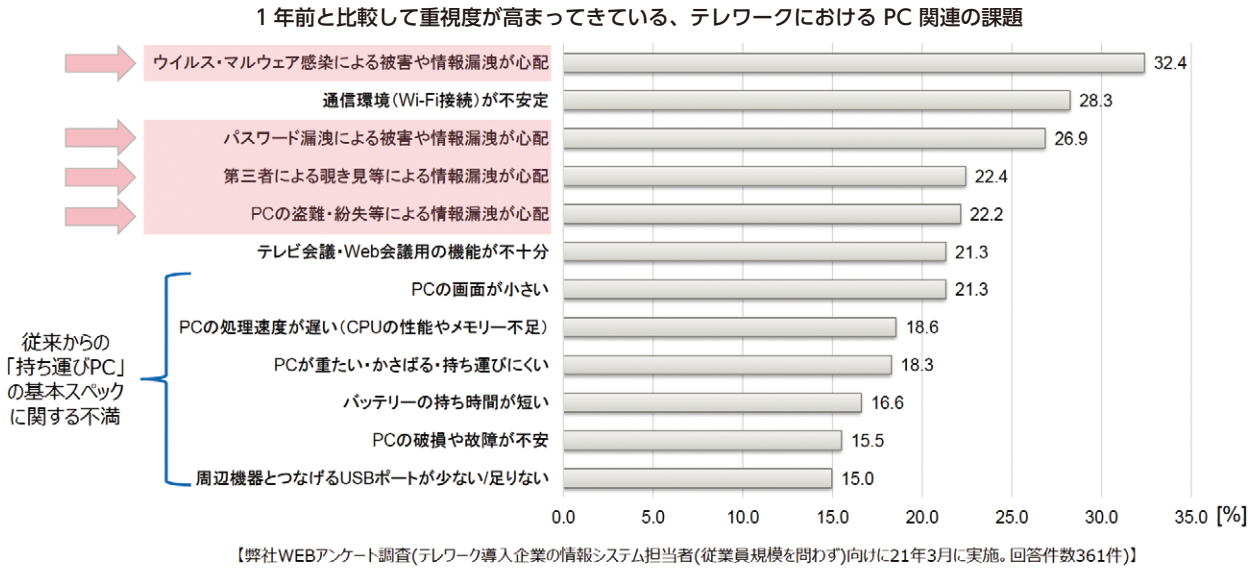
こうしたテレワーク普及を受け、大きく変わったのがセキュリティの考え方だ。以前はオフィス内とオフィス外のネットワークを分けて、その境界を守れば安心だったが、いまや社外で社員が利用するノートPCやタブレットなどに関してもオフィスにいるのと同等以上のセキュリティ対策をしなければならない。

実際、富士通がテレワークを実施している企業の情報システム担当者（国内351社）を対象に行ったアンケートにおいても「マルウェア感染」「パスワード漏えい」「第三者によるのぞき見」「モバイル端末の紛失・盗難」という4項目のリスクが上位になっており、多くの企業において共通の課題になっていることが分かる。

それら脅威に対して、社員が1人1台持つノートPC／タブレットごとに強固なセキュリティを確保しようと考えた場合、複数のセキュリティ対策製品を導入することが必要になるだろう。モバイル端末の購入に合わせて、「管理負荷」や「コスト」が積み上がることは、担当者にとっては大きな悩みではないだろうか。

では、管理負荷やコストを可能な限り抑えつつ、エンドポイント端末のセキュリティをしっかりと確保するためにはどうすべきなのだろうか。

テレワーク実施中のお客様の調査結果……テレワーク実施中のお客様の PC 関連の課題は、セキュリティ関連が上位に



テレワーク実施中の企業は、PCのセキュリティに課題を感じている

ウイルスやマルウェアから端末を強固に守るEDR

まずは日々、巧妙化するウイルスやマルウェアへの対策だ。一般的な「ウイルス対策ソフト」で事足りると考えているかもしれないが、いまや攻撃を100％防ぐことは不可能に近い。だからこそ、端末がマルウェアに感染してしまった際に、できるだけ早くそれを検知して被害を最小限に抑えるセキュリティ対策（EDR：Endpoint Detection and Response）が重要になる。

富士通
システムプラットフォームビジネス部門
CCD 事業統括部プロモーション推進部・部長
丸子 正道 氏

2021年現在、EMC／セキュアBIOSを搭載したノートPCである「LIFEBOOK U9,U7シリーズ」は世界最高レベルの安全性を誇る

EDRに関しては多種多様なサービスがセキュリティ対策企業から提供されているが、「BIOSのマルウェア対策が重要なのではないか」という考えから、最新の富士通のノートPC「LIFEBOOK Uシリーズ」に搭載されたのがEndpoint Management Chip（以下、EMC）とセキュアBIOSだ。

富士通 CCD事業統括部 プロモーション推進部 部長の丸子正道氏は、端末自体のウイルス／マルウェア対策についてこのように説明する。

「ノートPCやタブレットを使ってテレワークをする場合、オフィスのICT環境と比較して、ウイルス／マルウェア感染のリスクを強く感じているという声を多くのお客さまからいただいています。そこでEMCとセキュアBIOSを標準搭載すること

生体認証技術の比較

	指紋		顔		手のひら静脈	
認識精度	他人受入率 0.0001%以下	○	他人受入率0.001% （当社製品の場合）	○	**他人受入率 0.00001%以下**	◎
登録対応率	3～10%の人が使えない （ユーザーへのヒアリング）	△	社員証などの写真を流用できる⇒100%	◎	**実績ベースで100%の人が利用できている**	◎
認証速度	皮膚の状態によって、何回も認証失敗するケースあり	△	認証時間が早いが、マスク着脱などに時間がかかる	○	**体感で1秒切る程度**	○
対偽造	体表の情報なので、偽造リスクが高い	△	顔の動きを検知する等の設定が必要	○	**静脈パターンの再現は非常に困難**	◎
外的要因への耐性	乾燥や荒れ、汗、傷、摩耗に影響を受けやすい	△	マスク等の有無、髪型、周囲の照度の影響を受ける可能性がある	○	**体内情報のため外的要因を受けにくい**	◎
コロナ対策の影響	センサーに接触	△	マスク着用時に認証精度悪化	△	**非接触 マスクの影響なし**	○

で、端末を購入するだけでセキュリティ対策ができているという状況を目指しました」（丸子氏）

BIOSがウイルスやマルウェアの攻撃を受けたときにEMCが検知し、BIOSを改ざんされた場合は速やかに自己回復する機能は画期的だ。情報漏えいなどのリスクを防ぐとともに、マルウェアに感染して動かなくなった端末をICT担当者が復旧させる作業が不要となる。

他人受入率0.00001%以下の手のひら静脈認証

ノートPCやタブレットへの不正アクセスによる情報漏えいや、情報漏えいによる賠償責任のリスクは大半の企業が気にかけている部分だろう。従来のIDとパスワードによる認証では、一般的に名前や生年月日をベースとしたパスワード設定をするケースが多いため、それらの情報から類推され、パスワード漏洩につながることも多い。一方、セキュリティポリシーを厳格化し、パスワードを複雑化することで社員から覚えられないなど不満が出るというケースもある。

不正アクセスを防止するという観点で導入が進められているのが生体認証だ。指紋認証、顔認証は一般的だが、丸子氏は富士通独自の技術である「手のひら静脈認証」のメリットを以下のように語る。

「手のひら静脈認証は、体内情報である静脈パターンを使った生体認証です。指紋認証が他人受入率0.0001％以下であるのに対して、他人受入率0.00001％以下という高い認証精度を誇ります」（丸子氏）

偽造リスクのある指紋認証や顔認証と比較して、体内情報を用いる手のひら静脈認証は、偽造しにくい点も注目だ。また「指静脈での認証は冬場の寒い日などには認証されにくいことから、安定して認証できる手のひら静脈認証を選択した」という自治体もあると丸子氏は続ける。

端末のOSやアプリケーションのID/パスワード情報と連携できるため、新たに手のひら認証用のシステムを構築しなくても利用できる。たとえば、200桁のパスワードを連携させたとしても一瞬で確実にログインできるため、高度なセキュリティとユーザービリティを両立する認証方法と言えるだろう。

ノートPCに内蔵した赤外線カメラで手のひらを撮影することで、瞬時に本人の静脈かどうかを認証しログインできる手のひら静脈認証。非接触で利用できるため衛生的だ

モバイル端末が盗難に遭っても安心な秘密分散ソフトウェア

「シェアオフィスやカフェなどで離席した隙に端末を盗まれた」「電車に置き忘れた」といったケースの対策として紹介したいのが、秘密分散ソフトウェアだ。

リモートで端末内のデータを消去したり、強制ログオフしたりするサービスなども富士通では取り揃えているが、富士通の端末に搭載できる秘密分散ソフトウェアが画期的なのは、端末内のデータを見ることができない点にある。

「秘密分散ソフトウェアを利用することで、PCで作成したデータを自動で変換・分割して、『PC本体』と『ファイルサーバ』または『特定のスマートフォンやUSB』に常時分散保存します。万が一、PCを盗まれても、PCにあるデータだけでは元のデータに復元することができないため、機密データの漏えいを防ぐことが可能です」（丸子氏）

社外でPC作業をする場合には、持ち出したいデータのみを分散片として個人のスマートフォンなどに移して利用できる。社外で変更したデータは、社内に戻った際にファイルサーバと同期することで、最新データを保存可能だ。

「データ全部をサーバ側において、端末自体にデータを持たせないシンクライアントもありますが、テレワークの時代には運用が難しい面もあるかと思います。そのため、必要なデータだけを持ち出すことができ、かつ、端末を盗まれたとしても暗号化で機密情報を見られないシステムを採用しました」（丸子氏）

第三者からの、のぞき見を検知してログオフ

シェアオフィスやカフェなどでテレワークをしている際、電話対応やトイレで少し席を外した隙に機密情報をのぞき見されてしまったという事案も増えてきている。のぞき見を防ぐプライバシーフィルターなどは一般的だが、より強固なのぞき見対策として有用なのが富士通の「離席・のぞき見検知オプション」だ。

「端末内蔵のカメラで操作している人の顔と服の色を継続的に検知することで、本人以外の顔が映ると画面をロックする機能が離席・のぞき見検知オプションです。また離席時、カメラに本人の顔が映らなくなると自動的にログオフします」（丸子氏）

端末自体の盗難とは違い、情報を盗まれたことに気が付きにくいのぞき見を検知するとともに、席を離れた際にもオートロックしてくれる機能は、正にテレワーク向けのセキュリティだろう。

アフターコロナ時代も、働き方改革に取り組む企業を中心にテレワークはスタンダードになっていくと予想される。その分、モバイル端末を守るエンドポイントセキュリティは、機密情報やビジネスを守るためにはより不可欠なものになっていく。

「テレワークにおいても、社員1人ひとりが安心して使える端末環境を整えることが生産性の向上につながっていきます。今後もメーカーとして、場所を選ばず仕事ができるセキュアな環境を実現するお手伝いをしていきたいと考えています」（丸子氏）

- ゼロトラストネットワーク時代にPCに備えるべきセキュリティ
- マルウェア攻撃の被害を最小限に抑える超軽量モバイルPC FUJITSU Notebook LIFEBOOK U9シリーズ

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。