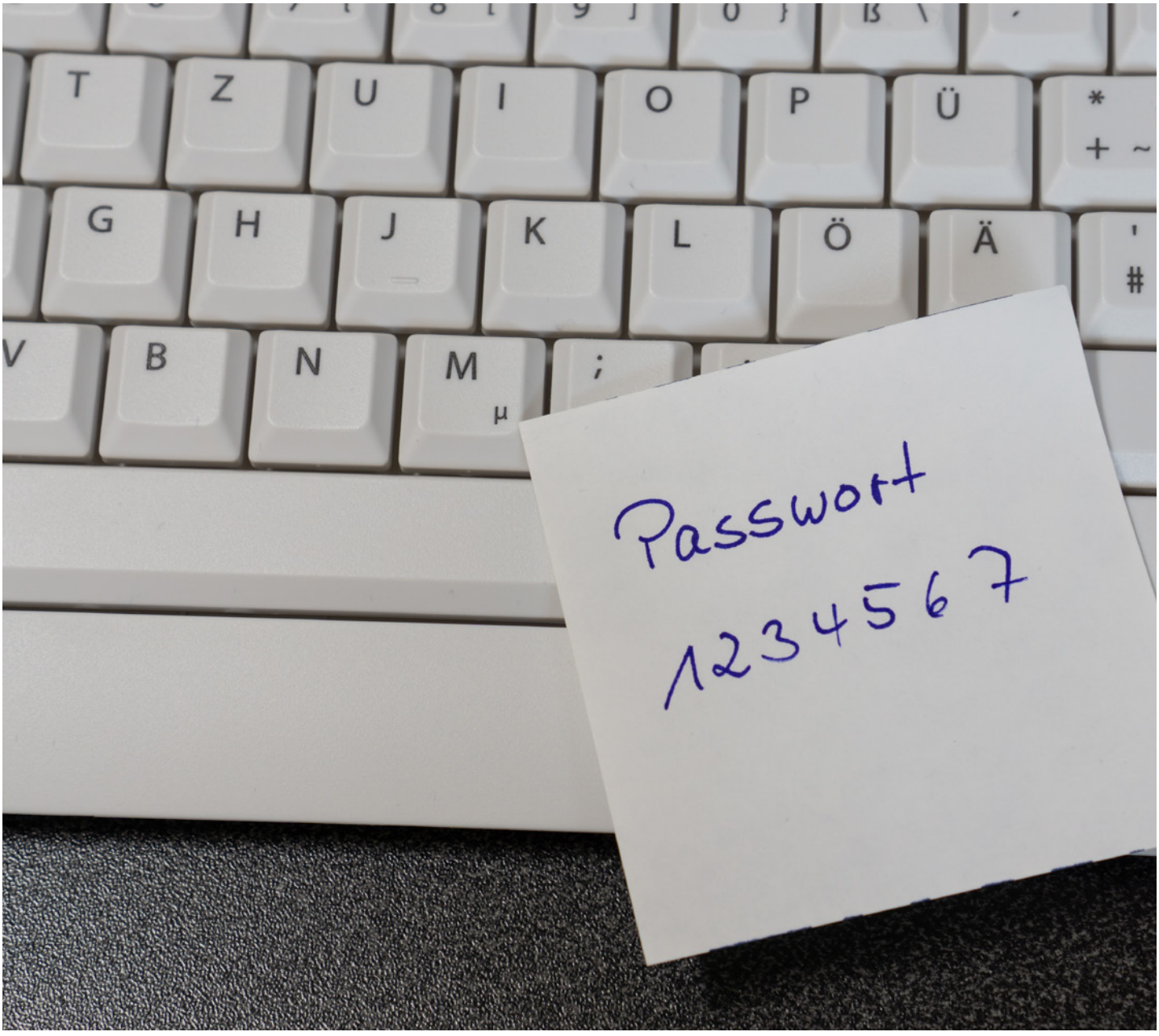
パスワードは本当に安全か?
情報漏えいのリスクから企業のPCを守る、2つのベストプラクティス

企業のPCが社外に持ち出される機会が増え、パスワードの漏えいやのぞき見、PCの盗難などによる情報漏えいのリスクが高まっている。これらを防ぐと同時にテレワークの業務効率を上げるためには、どのようなセキュリティ対策を講じるべきか。



働き方改革でテレワークが推進されていたが、新型コロナウイルス感染症（COVID-19）の拡大がその普及を加速し、これまでオフィスで使っていたPCを社外に持ち出して業務を行うケースも増えている。2021年3月に富士通が実施したテレワーク課題に関するアンケート調査によれば、社外への持ち出しPCが増えたことで「パスワードの漏えい」や「画面ののぞき見」「PCの盗難などによる情報漏えい」を懸念する企業が増加傾向にあるという。

テレワークで使うPCの情報漏えい対策の一つとして、企業の情報システム部門の管理者は「より厳重で安全性の高いパスワード管理が必要である」と考えるだろう。しかし、パスワードのポリシーを厳しく定めて従業員にパスワードの定期的な更新を求めても、パスワードの管理そのものが不十分であればそうした対策は無意味だ。厳し過ぎるパスワード管理は業務効率を低下させることもある。

本稿では、働き方が多様化する中で発生し得るセキュリティリスクと、今すぐできるセキュリティ対策を解説する。

厳密にすればするほど陥りがちな
セキュリティリスクと従業員の「負荷」が課題

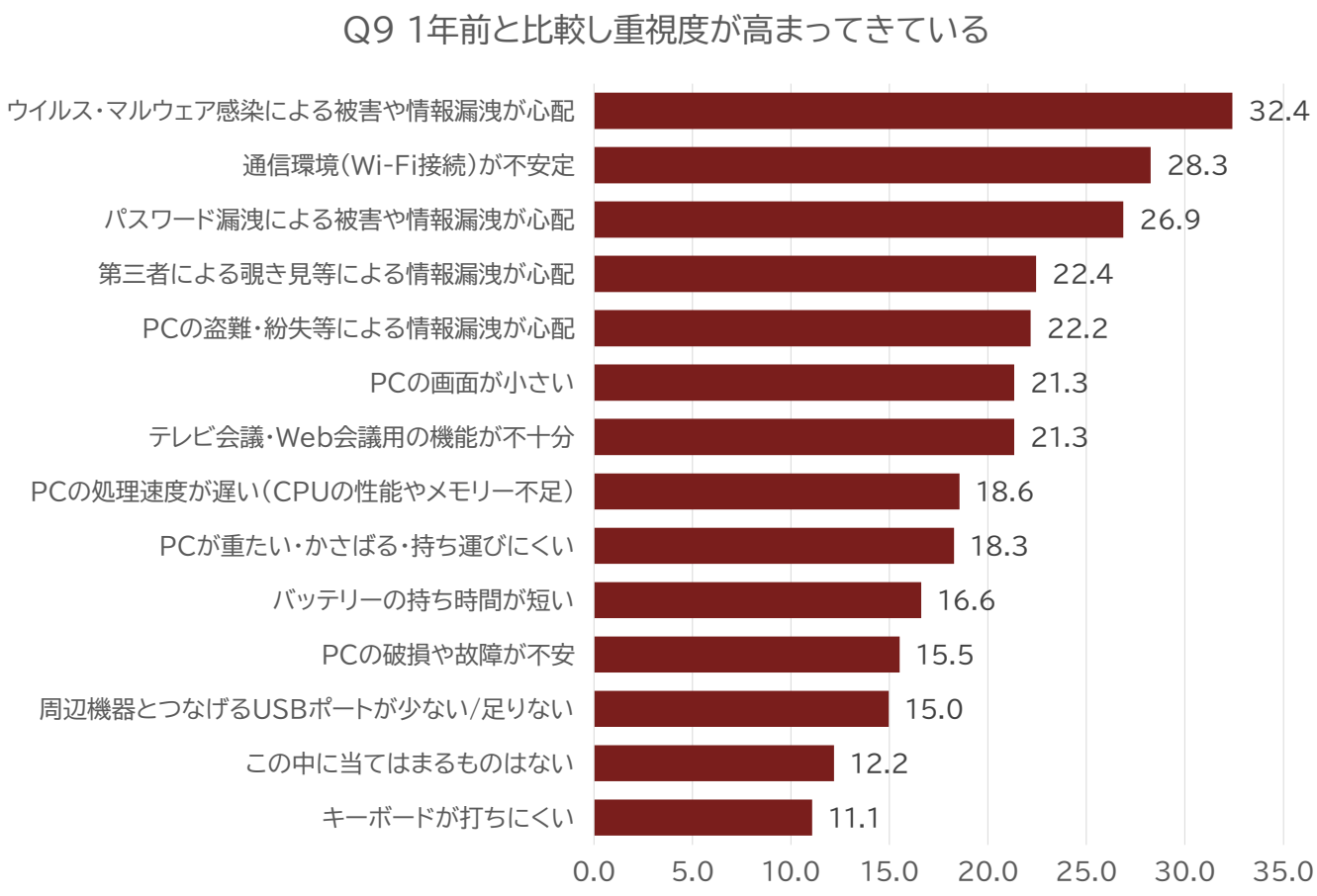
富士通が実施したアンケートによれば、「1年前と比較して重要度が高まっている」項目に、約2割の企業が「情報漏えい」を挙げた。第三者によるのぞき見やPCの盗難をきっかけとする情報漏えいは、コロナ禍においてテレワークが普及したことが背景にあるだろう。

ログインパスワードはPCを守る一般的な方法だが、業務で利用するPCが社外に持ち出される機会が増えれば、より厳重で安全性の高いパスワード管理が必要になる。

「パスワードのポリシーを厳格にすればするほど、従業員はその制約の中で効率的な運用を模索します。それによって、かえって漏えいのリスクにつながる場合もあります」

そう語るのは、富士通の花山兼一氏（CCD事業統括部 プロダクトマネジメント部）だ。

例えばパスワードのポリシーを「10文字以上で、大文字と小文字、英数字、記号を含むランダムな文字列」と規定し、しかもそれを「定期的に変更すること」を強制すれば、従業員はいちいち覚えてはいられない。素早く仕事を始めるために同じパスワードを使いまわしたり、パスワードを付箋（ふせん）に書いてPCやデスクに貼り付けたりしてしまいがちだ。また、会社の業務とプライベートで同じパスワードを使いまわしてしまうと、プライベートで設定したパスワードが盗まれた場合に、そのパスワードで業務システムに不正ログインされてしまう可能性もある。



1年前と比較して「重視」している課題（出典：富士通の2021年3月調査結果）

さらに花山氏は、今だからこそ発生し得る新たな「のぞき見」のリスクについても警鐘を鳴らす。

「今の監視カメラの解像度は高く、パスワードを打つ動作で『どの指で何のキーを押したか』が分かってしまいます。同一のパスワードを何度か入力している様子を映せれば、パスワードを当てられる可能性は十分にあり、そうなると複雑なパスワードにしていても全く意味がありません」（花山氏）

「Windows 10の生体認証」でも安心できない理由

パスワードに代わる認証手段に生体認証がある。「Windows 10」にはPCのカメラや指紋センサーを利用した生体認証機能「Windows Hello」が標準搭載されており、これを使えばよりセキュアなサインインができるはずだ。しかし花山氏は、同機能の「落とし穴」を指摘する。

「Windows Helloでは、生体認証が使えないときのために『PIN』（4桁以上の暗証番号）によるサインインを可能にしています。設定したPINが4桁の数字であれば、『総当たり攻撃』によって数十時間程度で突破されるリスクがあります」（花山氏）

Windows 10は、さまざまなハードウェアと組み合わせて使う汎用（はんよう）OSだ。そのため代替手段としてPINの運用はやむを得ない。しかし、PINが使える限りパスワードと同等のリスクがあるため、ビジネスで利用するPCのセキュリティとして万全とは言えない。

パスワードの厳重な管理を従業員に徹底させ、PC利用環境の制限を厳しくすれば、現場の従業員に負荷が掛かって業務効率が低下する可能性もある。かと言ってWindows Helloを使った生体認証でも万全ではないとなると、どのように対策をすればよいのか。花山氏はこの課題に対して「ログイン方法を抜本的に見直すべきです」と強調する。

BIOS段階からの生体認証でセキュアに起動

パスワード運用における問題を解決するため、富士通は10年以上も前から指紋認証や手のひら静脈認証といった独自の生体認証技術とソフトウェアを開発。同社の法人向けノートPC「LIFEBOOK」シリーズ、法人向けタブレット「ARROWS Tab」シリーズに搭載している。

LIFEBOOKとARROWS TabはPCを立ち上げる際、生体認証によってBIOSを起動する。OSの起動前にパスワードを使わない認証を通すため、OSの不正サインインを防ぐだけでなく、PC盗難でOSを初期化されるといったPCそのものの不正利用もブロックできる。

生体認証を利用すれば、ユーザーはパスワードを設定する必要も入力する必要もなくなる。のぞき見によるパスワードの漏えいやパスワードの定期的な変更に伴う管理負荷がなくなるので、セキュリティの強化と業務効率の向上を両立させることができる。

PCの生体認証と言えば、指紋センサーによる指紋認証やカメラによる顔認証が一般的だ。富士通の法人向けPCに添付されている本人認証ソフトウェア「AuthConductor Client Basic」は、指紋認証や顔認証（オプション）に加えて手のひら静脈認証にも対応している。花山氏によれば、手のひら静脈認証は指紋や顔認証よりもセキュリティの優位性があるという。

「手のひら静脈認証の最大の特徴は『体内の情報を使うこと』です。顔や指紋による認証は『表に出ている特徴』を使いますが、手のひら静脈認証は、手のひら内の静脈パターンの特徴点を抽出して数値化、暗号化して使います。体内の情報ですので、普段の生活では見たり使ったりする機会がなく、盗難や偽造によるなりすましが非常に困難です」

指の静脈パターンを使う静脈認証もある。しかし手のひらの方が血管が太くて本数も多く、パターンが複雑だ。そのため安定して認証できる点も手のひら静脈認証の優位点だと花山氏は説明する。

これらの理由から、富士通は手のひら静脈認証を推奨している。モバイル用途のためにATMで使用されている認証装置と同じ原理の手のひら静脈センサーを小型化／超薄型化してLIFEBOOKに搭載した。

ユーザーは認証の際、PCに内蔵されたセンサーの上部に手のひらをかざす。高速で連続撮影しているため、手のひらをかざしたままにしておく必要はない。花山氏は「慣れれば認証は一瞬で完了します」と言う。

「AuthConductor Client Basic」はWindowsのサインインだけでなく、個別の業務アプリケーションやWebブラウザでサービスにログインする際に、事前に登録したIDやパスワードを代行入力する機能がある。これにより、手のひらをかざすだけでWindowsや業務アプリケーションへのサインインが可能となり、IDやパスワードを打ち込む必要がなくなる。手のひら静脈認証は確実な本人確認と利

手のひら静脈センサー内蔵PCでの手のひら静脈認証のイメージ

便性の向上を両立させることができる仕組みであると言える。

「個人情報の漏えいは、たった1件でも大問題になります。従業員のパスワード管理が不十分なことに起因する情報漏えいは、それとは比べものにならないほど深刻な被害をもたらします。セキュリティ対策は事故が起こってからでは遅いのです。手のひら静脈認証に対応した富士通の法人向けPCは、軽快かつ安定した本人認証によってお客さまの重要なデータの漏えいを防ぎます。テレワークにおける情報漏えいリスクを懸念するのであれば、この機会に手のひら静脈認証の導入をご検討いただければと思います」（花山氏）

背後からの「のぞき見」をシステムが検知

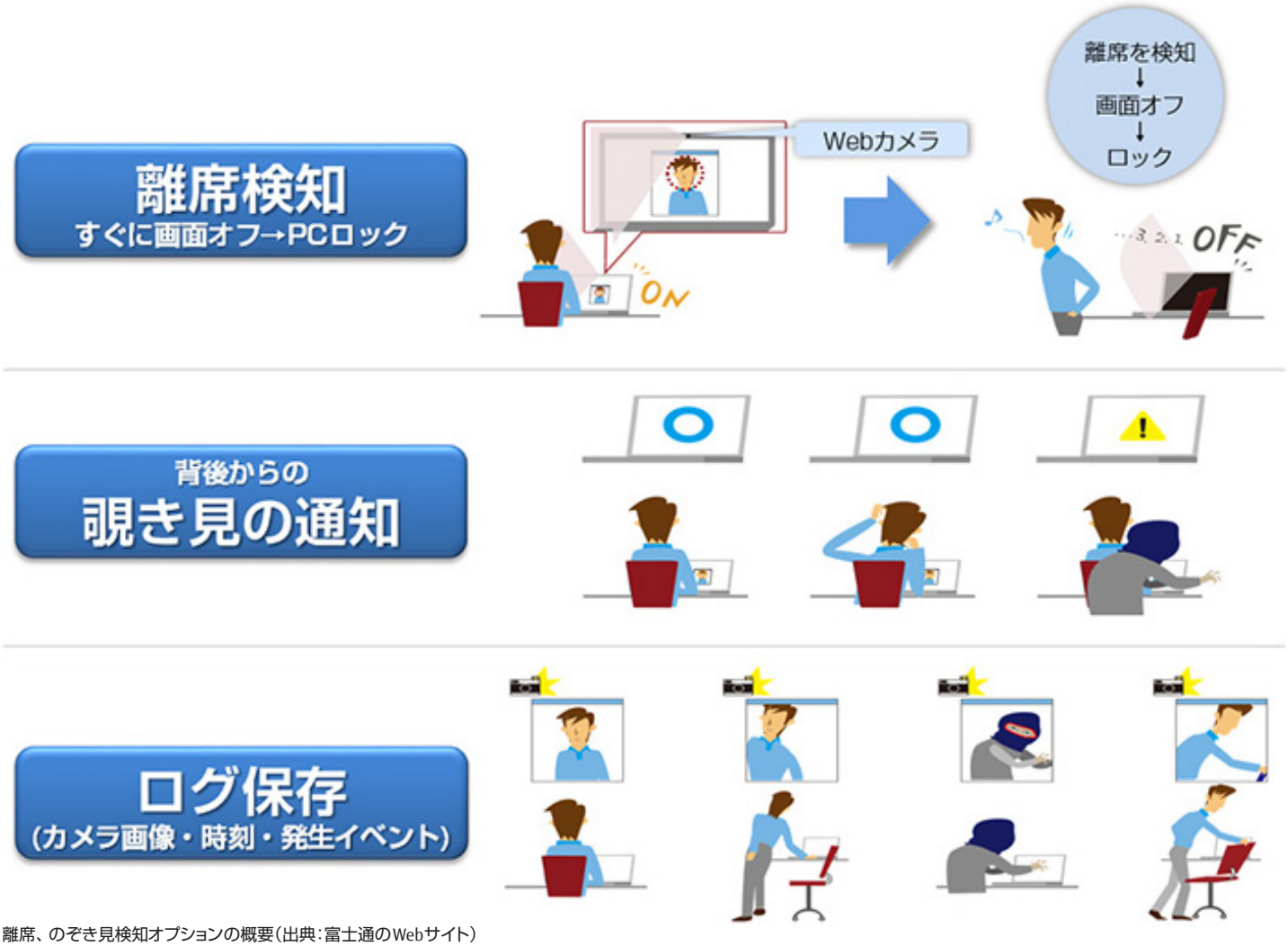
PCのビジネスでの利用シーンは多岐にわたる。テレワークの普及によって今後もさまざまな場所で使う機会が増え、カフェやシェアードオフィスなど社外の人の目に触れるケースも日常的になるだろう。そこで懸念されるのが、背後から誰かにPCをのぞき見されることだ。

情報システム部門がいくら「PCの利用環境には注意するように」と指示しても、公共のスペースでPCを使えば機密情報を表示した画面をのぞかれる可能性はゼロではない。急な電話対応などで使用中のPCをそのままにしてうっかり離席してしまうケースも起こり得る。

富士通はそうした場合に対し、内蔵カメラを応用してPCの画面を自動的にオフにしたりPCをロックしたりする「AuthConductor Client 離席・のぞき見検知オプション」を提供している。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、その特徴を次のように語る。

「第三者による画面ののぞき見を防ぐ一般的な対策には、ノートPCの画面に貼るプライバシーフィルターがあります。しかしこれは『横からののぞき込み』を防ぐもので、真後ろや肩越しからのぞき込まれたり、ユーザーが離席した瞬間に正面から見られたりすれば、情報は丸見えになります」

「離席・のぞき見検知オプション」は、富士通の法人向けノートPC「LIFEBOOK U9311」「LIFEBOOK U7311」「LIFEBOOK U7411」「LIFEBOOK U7511」などで利用できる。登録済みのユーザーが在席



離席、のぞき見検知オプションの概要（出典：富士通のWebサイト）

しているかどうかをPC内蔵のカメラで常に監視し、ユーザーが離席したことを検知すると、数秒でPCの画面を消してPCをロックする。離席中の不正利用を防げるため、ユーザーは人目がある環境でもストレスなくPCを使えるようになる。

また、ユーザーの背後で画面をのぞき込んでいる人を検知すると「のぞき見されていませんか?」というメッセージを表示してユーザーに注意を促す。

「富士通ではカメラを使ってユーザーの在席・離席の状態を監視する機能を『継続検知』と呼び、10年近くにわたって開発に取り組み、ノウハウを蓄積しています。前出の生体認証は『PCを使い始めるとき』のセキュリティ対策で、『離席、のぞき見検知オプション』は『PCを使っている最中』のセキュリティ対策です。PCの不正利用による情報漏えいを防ぐにはそれぞれのシーンで適切なセキュリティ対策を講じることが重要です」(菰田氏)

どこで働いていても、情報漏えいの防止は徹底したい。しかし、それによってユーザーに不便を強いては生産性が低下してしまう。LIFEBOOKには、セキュリティと利便性を高レベルで実現するためのセキュリティ機能が搭載されている。これは富士通が持つ豊富な技術力と長きにわたりセキュリティに取り組んできた経験と実績によるものだ。LIFEBOOKは情報漏えいのリスクに「起動時の生体認証」と「利用中ののぞき見対策」という2つのベストプラクティスで対抗する。ビジネスで利用するPCを選定する際の最有力候補と言えるだろう。

※この冊子は、TechTargetジャパン(https://techtarget.itmedia.co.jp/)に2019年6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/2106/24/news02.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。