FUJITSU

ホワイトペーパー

総務省の中小企業等担当者向け
ガイドラインを簡単解説！

テレワーク時代こそ必ず押さえておきたい

4つの
セキュリティ脅威と対策

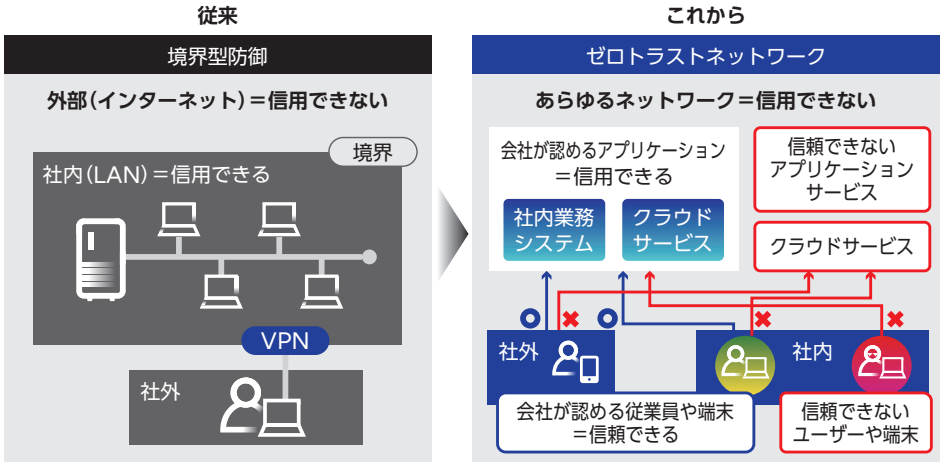
テレワークの普及によって社内ネットワークの外で業務を行うようになったことから、テレワークPCがサイバー攻撃に狙われるリスクが増加してきた。その対策は急務であるが、限られた時間・コスト・人材の中で具体的に何から着手していけばよいのかに悩むIT担当者も多いだろう。本ホワイトペーパーでは、特にテレワーク環境下で気をつけるべき4つのセキュリティの脅威と代表的な11の発生要因を示した上で、それを防ぐ方策を解説する。

テレワークの普及でセキュリティの方針は「ゼロトラスト」に

従来の境界型防御のアプローチでは不十分

テレワークが普及したことで、新しいセキュリティのアプローチが必要とされている。従来は、社外に持ち出される端末の数は限定的であり大半は社内ネットワーク内にあったため、社内と社外をファイアウォールなどで境界線を設け、「社内ネットワークの中は安全」「その外は危険」と捉えた上で対策を施す考え方が主流であった。いわゆる「境界型防御」の考え方である。

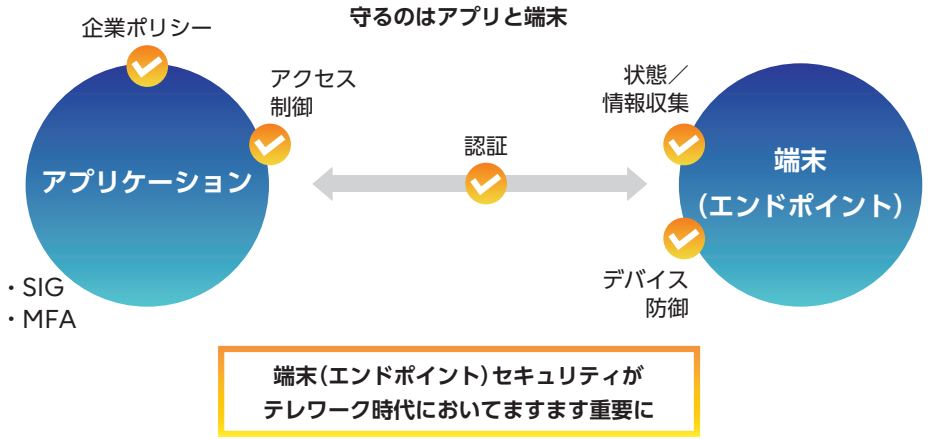
しかし、現在ではあらゆる端末が社外に点在し、さらに社内システムや外部のクラウドサービスを利用するようになったことで、もはや社内ネットワーク内の安全性を確保するだけでは不十分だ。代わりに、端末やユーザーが社内システム、クラウドアプリケーションなどあらゆるITリソースにアクセスする際に、それを「すべて信頼できないものである」とみなしたうえで都度認証・認可を行い、アクセスの正当性を検証するという考え方が広まってきた。これが「ゼロトラスト」セキュリティの考え方である。



「エンドポイントセキュリティ」がより重要に

ゼロトラストセキュリティにて特に重要なのが、PCを代表とするエンドポイントやアプリケーションへの対策である。これまでエンドポイントの対策といえば、長らくウイルス対策ソフトが活用されてきた。それは現在でも重要な対策の1つであるが、最近では、ウイルス対策ソフトで防御できずに端末に侵入してきた脅威をいち早く検知して迅速に対応するソリューションであるEDR（Endpoint Detection and Response）も重要視されている。

エンドポイントからWebサイトやクラウドサービスにアクセスする際は、不審なインターネット通信を遮断したり、セキュリティインシデント時には情報収集を行ったりなども重要だ。クラウドへ正しい端末がアクセスできるかといった「アクセス制御」や、本当に正しいユーザーかどうかといった「認証」はより重要になる。これまでファイアウォールなどを含めて複数の製品にて担っていたセキュリティ対策を端末側だけで考えなければならなくなっているともいえるだろう。



テレワークで必ず対処すべき「4つの脅威」と「11の発生要因」

即効性のある対策のポイントを紹介

テレワークのセキュリティ対策指針として参考になるのが、総務省が2021年5月に発表した「テレワークセキュリティガイドライン」だ。最新のテレワークを取り巻く環境やセキュリティ動向の変化に基づき、多面的な対策の解説が網羅されている。しかし、セキュリティの専門担当がいないような人的リソースに不安を抱える企業が、ここで紹介される対策をすべて進めていくのは困難である。そこで、同じく総務省が中小企業向けに公開している「中小企業等担当者向けテレワークの手引き」を参考にしたい。そこには、テレワークを実施する際に最低限のセキュリティを確実に確保するための対策が具体的に示されている。

本資料では、「テレワーク環境で想定される代表的な脅威」の例として「マルウェア感染」「不正アクセス」「端末の紛失・盗難」「情報の盗聴」の４つの脅威に言及し、それらが発生する主な要因と即効性のある対策のポイントを11の発生要因に分けて紹介する。各ポイントについて対策ができているか次ページからチェックし、できていない場合は早急に実施したい。

テレワークで必ず対処すべき脅威・発生要因と想定される被害

脅威	発生要因	被害	富士通が提案する解決策
1. マルウェア感染	①添付ファイル付きメールの受信・開封 ②悪意あるサイトの閲覧・ダウンロード ③ USB メモリ接続	・個人情報漏えい→賠償義務発生 ・感染発覚→信頼失墜・取引停止 ・情報復旧不可→業務停止	**ウイルス・マルウェア対策の強化**
2. 不正アクセス	④脆弱性に未対応 ⑤簡単な文字列のログインパスワード ⑥ログインパスワードの転用	・個人情報漏えい→賠償義務発生 ・感染発覚→信頼失墜・取引停止	**本人認証の強化**
3. 端末の紛失・盗難	⑦サテライトオフィスに端末を忘れて紛失 ⑧カフェなどで離席した際に端末が盗難	・重要情報紛失→業務停滞 ・紛失 / 盗難発覚→信頼失墜・取引停止 ・顧客情報漏えい→賠償責任発生	**データ保護の強化**
4. 情報の盗聴	⑨オンライン会議 URL を不正に取得 ⑩のぞき見防止なしでカフェでテレワーク ⑪カフェの無線アクセスポイントを利用	・未公開情報が公開→事業に影響 ・盗聴発覚→信頼失墜・取引停止 ・ID/ パスワード悪用で顧客情報漏えい →賠償責任が発生	**データ保護の強化** **本人認証の強化**

1.マルウェア感染のリスクとその対策

マルウェアに感染してしまうとコンピュータが使用できずに業務停止したり、情報漏えい、また第三者からの遠隔操作で攻撃に荷担してしまったりする可能性がある。
特に近年多発しているのがランサムウェアによる被害だ。データの暗号化解除と引き換えに身代金を要求するこのサイバー攻撃は、企業規模や業種に関係なく被害が相次いでいる。

Check 01 添付ファイル付きメールの受信／開封

発生要因は？

メールからダウンロードした実行ファイル(.exe)またはWord、Excelファイルなどに仕込まれた悪意のあるマクロを実行させるなどして感染させる。最近では、本物と見間違うように細工した巧妙な攻撃メールも増えている。

対策は？

- **見慣れないファイル形式であるなど、少しでも不審なファイルは安易に開かない**
- **OSやアプリのソフトウェアアップデートの徹底。サポート切れのOSやソフトは使わない**
- **ウイルス対策ソフトやEDR製品を導入する**

チェックして確認

Check 02 悪意のあるサイトの閲覧・ダウンロード

発生要因は？

偽のメール、不正な広告、改ざんされた正規サイトなどから攻撃者の不正なサイトへ誘導する。そこで不審なファイルをユーザーに気づかれないようにダウンロードさせてファイルの実行を誘い、マルウェアに感染させる。

対策は？

- **日々使うサイトのURLは意識しておき、見慣れないURLは安易にクリックしない**
- **OSやアプリのソフトウェアアップデートの徹底。サポート切れのOSやソフトは使わない**
- **ウイルス対策ソフトやEDR製品の導入**

チェックして確認

Check 03 USBメモリ接続

発生要因は？

悪意のあるファイルを保存したUSBメモリをわざと落とし、拾った人のPCから感染させる手口が知られている。ある実証実験によると、落ちているUSBを拾った多くの人は自分のPCに接続するという結果が報告されている。

対策は？

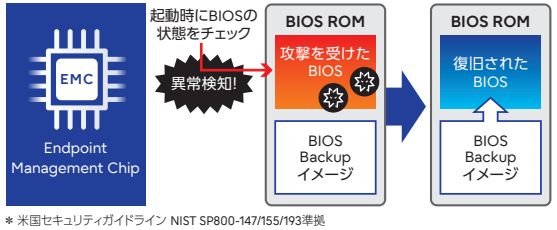
- **持ち主がわからないUSBメモリを拾った場合、絶対に自分のPCに差し込まない**
- **OSやアプリのソフトウェアアップデートの徹底。サポート切れのOSやソフトは使わない**
- **ウイルス対策ソフトやEDR製品の導入**

チェックして確認

セキュリティ強化におすすめ 対応機種を確認 >

富士通の法人向けPC独自のマルウェア感染対策機能

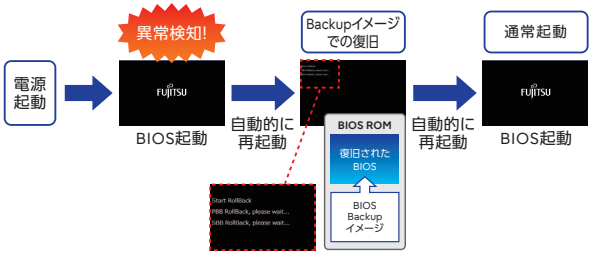
富士通独自の新開発ハードウェア「Endpoint Management Chip (EMC)」では、PC起動時にBIOSへの攻撃や異常を検知し自動で修復。PCが起動しないといったトラブルを回避することができる



＊米国セキュリティガイドライン NIST SP800-147/155/193準拠

EMCの概要

自動的にBackupイメージでの復旧作業を実行。仮に攻撃を受けた場合でも、正常時の環境に戻すことが可能



セキュアBIOS＋EMCの異常検知時の動作

2.不正アクセスとその対策

不正アクセスとは、権限を持たない第三者が勝手に他者のPCやサービスに侵入する行為であり、主に侵入して情報を盗み取ることを目的とする。情報漏えいの発生やそれに伴う賠償責任の発生、また、取引先や顧客からの信頼失墜や取引停止となる可能性がある。

Check 04 脆弱性に未対応

発生要因は？

テレワークの普及に伴い、社外から社内へアクセスするVPN機器の脆弱性が利用されて不正アクセスされる事件が多数発生している。社内システムへ侵入され情報漏えいする可能性がある。

対策は？

- **VPNの最新の更新プログラムは迅速に適用する**
- **古いVPN機器を使用する際はソフトウェアアップデートを行う**
- **二要素認証などを導入する**

チェックして確認

Check 05 簡単な文字列のログインパスワード

発生要因は？

従業員個人がパスワードを管理しており、かつ文字列を簡単なものに設定しているとブルートフォースアタック（総当たり攻撃）によって突破され、不正アクセスされる可能性が高まる。

対策は？

- **英字、数字、小文字、大文字などを組み合わせた複雑かつ長いパスワードを設定する**
- **ID管理製品でパスワード管理やポリシー設定を管理者が行う**
- **二要素認証などを導入する**

チェックして確認

Check 06 ログインパスワードの転用

発生要因は？

複数のサービスを利用するとパスワードを覚える面倒から、多くのユーザーはパスワードの使いまわしをしてしまいがちだ。しかし、使いまわしはパスワードリスト攻撃などによって突破される可能性が高くなる。

対策は？

- **サービスごとに必ず異なるパスワードを設定する**
- **二要素認証を導入する**
- **パスワードをユーザーに管理させないよう、シングルサインオンを設定する**

チェックして確認

不正アクセス対策におすすめ 対応機種を確認 >

富士通の法人向けPCで利用可能な本人認証強化機能

本人認証の強化対策として「AuthConductor Client Basic」を用いて二要素認証やシングルサインオンを設定。手のひら静脈認証や指紋認証、顔認証など、利用者本人の生体情報を使って、Windowsや業務システムに一度の認証でスピーディーにサインイン可能
また、生体情報を登録してからでないとPCの利用ができないといった機能や、本人認証をサーバーを立てずにPC上で実施できる機能を活用することで、セキュリティーポリシーに合わせた運用が可能

3.端末の紛失・盗難とその対策

PCを持ち出す機会が増加するテレワークでは端末の紛失・盗難のリスクも増加する。PCが盗難に遭うと内蔵のストレージを取り出して他のデバイスに接続され、情報漏えいの発生やそれに伴う賠償責任の発生、また、取引先や顧客からの信頼失墜や取引停止につながる可能性も高くなる。

Check 07 サテライトオフィスに端末を忘れて紛失

発生要因は？

サテライトオフィス、シェアオフィス、コワーキングスペースなど働く場所が多様化している。PCを持ち歩く機会も増え、紛失する可能性が非常に高まっている。

対策は？

- **PCに接続する記憶媒体を制限する**
- **LANポートやBluetooth搭載機器とのペアリングを制限する**

チェックして確認

Check 08 カフェなどで離席した際に端末が盗難

発生要因は？

オフィス、サテライトオフィス、自宅だけではなく、外出中、出張中にて飲食店やカフェなどでスキマ時間を利用して作業を行う人も増えている。少しの間なら大丈夫という油断で放置した端末が盗難に遭う可能性も。

対策は？

- **Windows PCの「BitLocker」などストレージの暗号化機能を必ず有効にする**
- **重要なデータを端末には保管しないようにする**
- **MDMなどで遠隔からデータ消去できる製品を導入する**

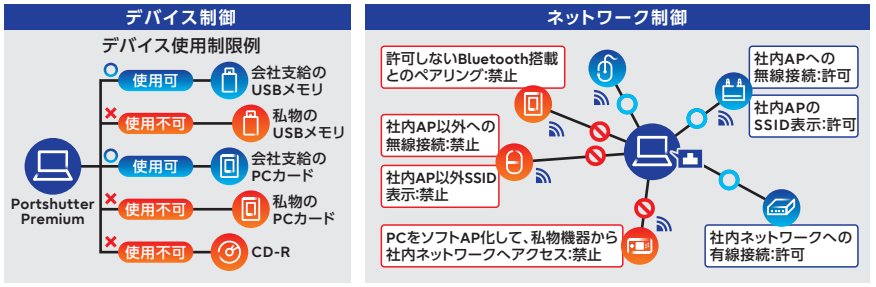
チェックして確認

紛失・盗難対策におすすめ　対応機種を確認 >

富士通の法人向けPCで利用可能なデータ漏えい防止機能

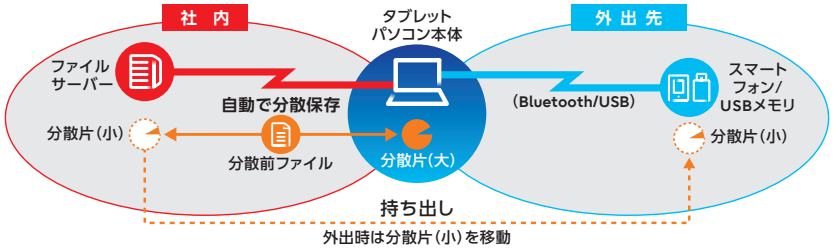
端末からの情報漏えい対策

「Portshutter Premium」によってPCに接続する記憶媒体、LANポートやBluetooth搭載機器とのペアリングを制限する設定がPC管理者権限で可能



盗難・紛失を想定した情報漏えい対策

「Portshutter Premium Attachecase」によってデータ無意味化して、複数のデバイスに自動分散することで第三者によるデータの読み取りを防止する。



4.情報の盗聴とその対策

テレワークでは、端末上のデータやネットワークでやり取りされているデータを知らないうちに盗み取られてしまうことがある。
情報の盗聴にあった場合、情報漏えいの発生や、それに伴う賠償責任の発生、また、取引先や顧客からの信頼失墜や取引停止につながる可能性がある。

Check 09 オンライン会議URLを不正に取得

発生要因は？

画面の盗み見、メールの盗聴、会議IDの総当たりなどで、何らかの形でオンライン会議のURLが不正に取得され、第三者が知らずに会議に参加することで内容が盗聴される可能性がある。

対策は？

- **オンライン会議のURLは必要な人に限定して招待のURLを送る**
- **許可されたアカウントしかオンライン会議に参加できない設定にする**
- **会議や録画へのアクセスにパスワードを設定する**

チェックして確認

Check 10 のぞき見防止なしでカフェでテレワーク

発生要因は？

電車の中やカフェなど人が密集しやすい場所にてPCを扱うと、横からまたは背後から簡単に画面をのぞき見されてしまい、情報漏えいにつながりやすい。

対策は？

- **のぞき見防止フィルターなどを利用する**
- **カフェなどでは重要なファイルを開かない**
- **どうしても重要なファイルを扱う場合は、のぞき見されにくい場所を選んで作業する**

チェックして確認

Check 11 カフェの無線アクセスポイントを利用

発生要因は？

カフェやホテルなどで無料で利用できる無線LANは、中には通信が暗号化されていないものも多く存在する。同環境での通信は容易に内容を傍受できることが知られており、情報漏えいのリスクがある。

対策は？

- **公衆無線LANはなるべく利用せず自社で契約しているモバイルWi-Fiを使う**
- **やむを得ず公衆無線LANを利用する場合はVPN通信を行う**

チェックして確認

テレワークでおすすめしたい富士通のPC

使いやすさとセキュリティを備えたPCをラインアップ

富士通の法人向けPCには、安全性を高めるセキュリティ機能が豊富に用意されている。すでに紹介したように、「マルウェア感染」「不正アクセス」「紛失・盗難による情報漏えい」「盗聴」の4つの観点からセキュリティを強化する機能をPCの標準機能またはオプション機能として提供しているため、企業としては、PCの導入とセキュリティ対策製品を別途導入して管理が煩わしくなってしまうリスクを解消できる。

利便性の観点からは、テレワークに最適なモデルとして下記の左側の表が示すように、超軽量・薄型を徹底的に追求した「LIFEBOOK U9シリーズ」と13.3型ワイドから 15.6型ワイドまでの画面サイズで、高いモビリティとビジネスに求められる拡張性を両立させた「LIFEBOOK U7シリーズ」を用意している。

テレワークPCとして、どの程度の質量や画面サイズを選定するのか、セキュリティ機能は何が必要なのか、自社の中ではどの程度持ち運びの用途があるのか、重要な情報を抱えているのか、などを整理しながら検討していきたいところだ。

テレワークにおすすめの富士通のモバイルノート PC

	圧倒的な軽さのU9シリーズ		選べる画面サイズU7シリーズ		
	スリムコンバーチブル	ウルトラ・スリムモバイル	スリムモバイル	スリムモバイル	スリムモバイル
	LIFEBOOK U9311X/H	LIFEBOOK U9311/H	LIFEBOOK U7311/H	LIFEBOOK U7411/H	LIFEBOOK U7511/H
					
サイズ	13.3型ワイド	13.3型ワイド	13.3型ワイド	14.0型ワイド	15.6型ワイド
CPU	インテル®Core™i7-1185G7 インテル®Core™i5-1145G7	インテル®Core™i7-1185G7 インテル®Core™i5-1145G7 インテル®Core™i5-1135G7 インテル®Core™i3-1125G4	インテル®Core™i5-1145G7 インテル®Core™i5-1135G7 インテル®Core™i5-1125G4 インテル®Celeron® 6305	インテル®Core™i5-1145G7	インテル®Core™i5-1145G7
メインメモリ	4G～32GB	4G～32GB	4G～40GB	4G～64GB	4G～64GB
ストレージ	SSD・標準 128GB/256GB/512GB	SSD・標準 128GB/256GB/512GB	SSD・標準 128GB/256GB/512GB	SSD・標準 128GB/256GB/512GB	SSD・標準 128GB/256GB/512GB
タッチ入力	標準	タッチパネルモデルあり	タッチパネルモデルあり	—	タッチパネルモデルあり
バッテリー駆動時間※	約11.0時間 （標準バッテリー） 約22.5時間 （大容量バッテリー）	約11.0時間 （標準バッテリー） 約23.0時間 （大容量バッテリー/ タッチパネル非対応モデル） 約16.8時間 （大容量バッテリー/ タッチパネルモデル）	約12.9時間 （標準バッテリー） 約26.0時間 （大容量バッテリー）	約17.0時間 （標準バッテリー） 約23.0時間 （大容量バッテリー）	約15.0時間 （標準バッテリー） 約20.0時間 （大容量バッテリー）
質量	約877g	約738g	約0.99kg	約1.12kg	約1.32kg

富士通のモバイルノート PC と利用できるセキュリティ機能

●：標準装備または添付
○：カスタムメイド
－：設定無し

		スリムコンバーチブル LIFEBOOK U9311X/H	ウルトラ・スリムモバイル LIFEBOOK U9311/H	スリムモバイル LIFEBOOK U7311/H	スリムモバイル LIFEBOOK U7411/H	スリムモバイル LIFEBOOK U7511/H
ウイルス・マルウェア対策	BIOS のセキュリティ強化（EMC）	●	●	●	●	●
	Secured-core PC	○	○	○	○	○
本人認証	FUJITSU Security Solution AuthConductor Client Basic V2	●	●	●	●	●
	手のひら静脈センサー（PalmSecure-F シリーズ互換）	○	○	○	○	○
	手のひら静脈センサー（PalmSecure-SL シリーズ互換）	○	○	○	○	○
	指紋センサー	●	●	○	○	○
	Web カメラ（顔認証対応）	○ *1	○ *1	○ *1	○	○
	BIOS/ ストレージパスワード	●	●	●	●	●
	BIOS パスワードの生体認証での代行	●	●	●	●	●
	スマートカード	○ *2	○ *2	○ *2	○ *2	○ *2
データ保護	Portshutter Premium	●	●	●	●	●
	暗号化機能付フラッシュメモリ（SSD）	●	●	●	●	●
	セキュリティチップ	●	●	●	●	●
	Portshutter Premium Attachecase	○	○	○	○	○
	プライバシーフィルター	－	○ *3	○ *3	○ *3	○ *3
	プライバシーカメラシャッター	－	○ *4	○ *4	○ *4	○ *4
	ハードディスクデータ消去ツール	●	●	●	●	●

詳細は製品サイトでご確認ください

＊1：タッチパネルモデルのみ標準搭載。 ＊2：AuthConductor Client Basic はスマートカードに非対応です。 ＊3：タッチパネルモデル除く。＊4：タッチパネルモデルは標準搭載、タッチパネル非対応モデルは、カスタムメイドで Web カメラを選択した場合のみ対応。

富士通の法人向けダイレクト販売サイト「富士通WEB MART」

専門スタッフとの相談も可能

富士通の法人向けPCを購入する際にぜひ活用いただきたいのが、富士通の法人向けダイレクト販売サイト「富士通WEB MART」だ。同サイトでは法人向けとしてノートPC「LIFEBOOKシリーズ」、デスクトップPC「ESPRIMOシリーズ」、タブレット「ARROWS Tabシリーズ」、PCサーバー「PRIMERGYシリーズ」、ワークステーション「CELSIUSシリーズ」、周辺機器・ソフト ウェアなどを取り扱っている。Webサイト上でのオンライン注文と決済のほか、電話での注文も可能だ。もちろん、購入相談窓口で専門スタッフに相談しながら、PCを選定していくこともできる。

購入時の便利なサービスとしては、送料無料※、翌日お届け、クレジットカード/銀行振込/代引きなどへの対応も行っている。また、安心できるサービスとしては、保守サービス、訪問セットアップサービス、リカバリメディア作成代行サービスなどを提供している。

※会員登録（無料）が必要

セキュリティ強化のためのPC選定をサポート

富士通WEB MARTでは随時、キャンペーンも実施しているので、常にサイトをチェックしていただくとよいだろう。例えば、数量限定でのお得なわけあり品や翌日にお届け可能な短納期モデルの提供も行っている。

ダイレクト販売サイトというと、購入するモデルを事前に確定させ、できるだけ安くすぐに購入したい方向けのものと思う方もいるかもしれないが、富士通WEB MARTは、そうしたニーズだけでなく、PC選定段階から相談やアドバイスに対応していることも大きな特徴だ。

特に中堅中小規模の企業が抱えるさまざまな課題にも、ユーザーに寄り添って対応している。テレワークが本格化する中、新しい働き方に対応でき、セキュリティの高いPC選定をどのように行っていけばよいか迷っている方は、ぜひ一度ご利用・ご相談いただければ幸いである。

お問い合わせ先
〔購入相談窓口〕0120-959-242
受付時間9 時～18 時（土曜・日曜・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