PCを起動「できなくする」サイバー攻撃
ビジネスの停止を防ぐ
テレワーク時代のセキュリティ対策

企業を狙ったサイバー攻撃は激化、高度化を続けている。「狙われるのは大企業だけ、自社は関係ない」という認識は大きな誤解だ。PCを攻撃して事業を止めてしまうような攻撃に、中小企業はどう対抗すべきか。

2020年以降、新型コロナウイルスの感染拡大によって、テレワークを中心に働き方が大きく変わった。

富士通が実施した企業アンケートによれば、多くの企業が「1年前と比べてコンピュータウイルスやマルウェアによる被害や情報漏えいが心配になった」と考えていた。

しかし、特に中小企業においては「ウイルス対策ソフトを使えば十分だ」と感じる傾向がある。「顧客情報の漏えいで大きな損害を被るのは大企業だけ」という認識も根強く、それがセキュリティ対策を遅らせる要因になっている。

これらは大きな誤解だ。業務を継続できなくなってしまうタイプのサイバー攻撃もあり、企業規模を問わず対策が必要だ。一方で中小企業は予算や人員が限られており、セキュリティの専門人材がいない場合もある。大規模なセキュリティシステムの導入が難しい中で高度化するサイバー攻撃に対抗するために、何をすべきか。

中小企業のセキュリティ対策を遅らせる「2つの誤解」

「『ウイルス対策への過信』と『被害への過小評価』という2つの誤解が、中小企業のセキュリティ対策を遅らせています」と、富士通の山嶋雅樹氏（CCD事業統括部プロダクトマネジメント部シニアマネージャー）は警鐘を鳴らす。前述した同社の調査では、情報漏えいを心配する声が目立った。その一方で、特に中小企業の対応が遅れがちであるという。

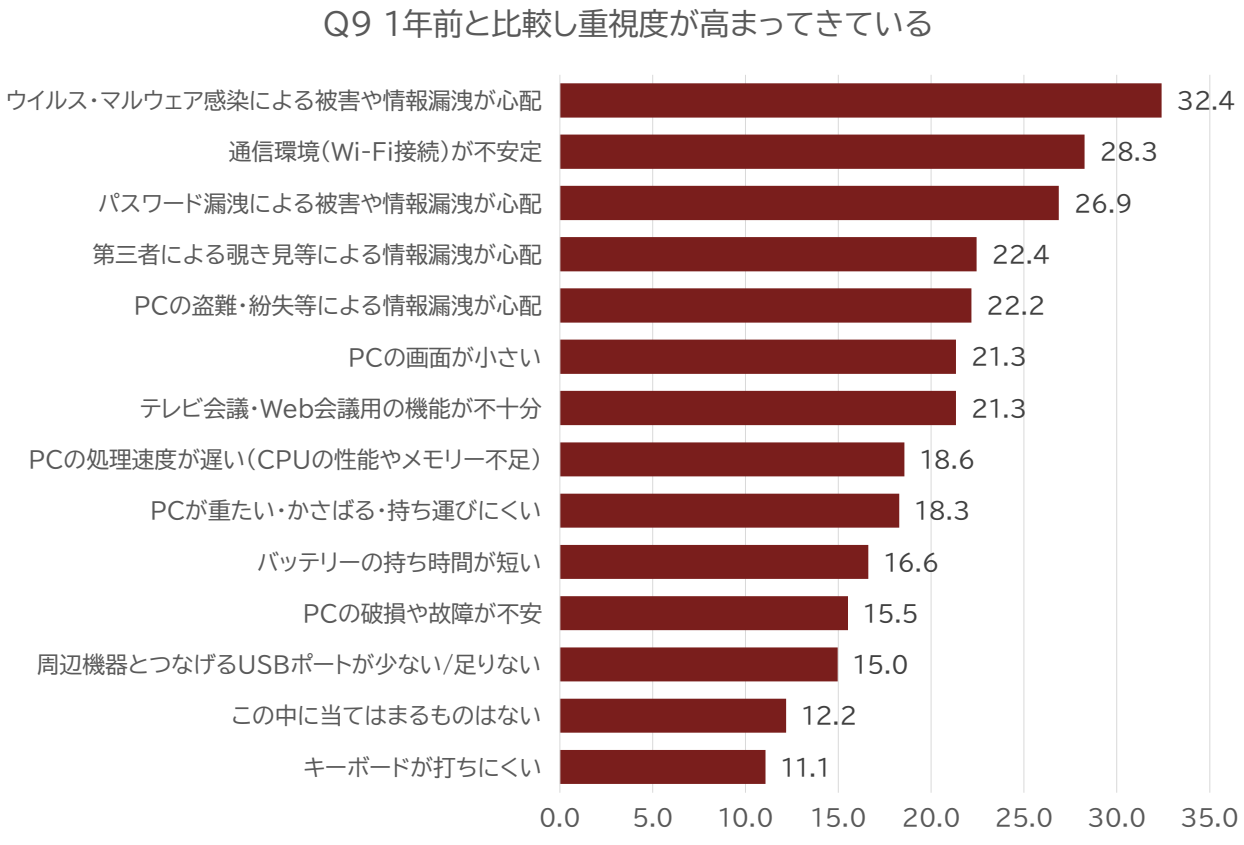
「中小企業には、いまだに『セキュリティ=ウイルス対策』という認識が残っています。ウイルス対策をしていれば十分で、セキュリティ専用のソフトウェアやアプライアンスを購入したり、セキュアなクラウドサービスに毎月利用料を支払ったりといった『過剰対応』は不要という考え方です」（山嶋氏）

また、サイバー攻撃で損害を被るのは大企業だけだという考えも根強いという。

「サイバー攻撃の被害に対して、経営層に『ひとごと感』があるのかもしれません。『自分たちの事業規模ならサイバー攻撃を受けても大きな被害は出ないだろう』という認識も、対策を遅らせる要因になっていると思います」（山嶋氏）

しかし同氏によれば、それらはいずれも誤解だ。防御を突破して侵入したマルウェアはPCのOSやアプリケーションを不正に操作し、企業の情報を外部に送信して「データ漏えい」を起こす。ランサムウェアは端末内のデータを暗号化して使用不可能にし、データを“人質”に取って金銭の支払いを要求する。

ソフトウェアベンダーが気付く前の脆弱（ぜいじゃく）性を狙って攻撃したり、発見されても対応ができていない（ゼロデイ）脆弱性を狙って攻撃したりする手法もある。これらは従来のウイルス対策ソフトでは検知や対応が難しい。



1年前と比較して「重視」している課題（出典：富士通の調査結果）

PCを起動不能に、BIOSを狙う攻撃者

「従来のウイルス対策ソフトでは対応できない脅威として、PCのBIOSやファームウェアの脆弱性を狙う手法が問題視されています」（山嶋氏）

BIOSはPCの起動を制御するプログラムだ。ハードウェアの動作を規定するもので、電源を入れた直後、OSよりも前に起動する。そのため書き換えられるとOSを起動できず、PCが全く使えなくなってしまう。

BIOSを書き換えられたPCは、専門の知識を持った技術者が正しいBIOSに書き直して再セットアップをする必要がある。その間ユーザーはPCを使用できず、中のデータも取り出せない。業務は完全にストップしてしまう。

「PCのBIOSやファームウェアが改ざんされた場合、復旧には『コマンド』の入力が必要になります。それは知識を持った人でないと対応できず、操作ミスによって復旧が不可能になってしまう場合もあります」（山嶋氏）

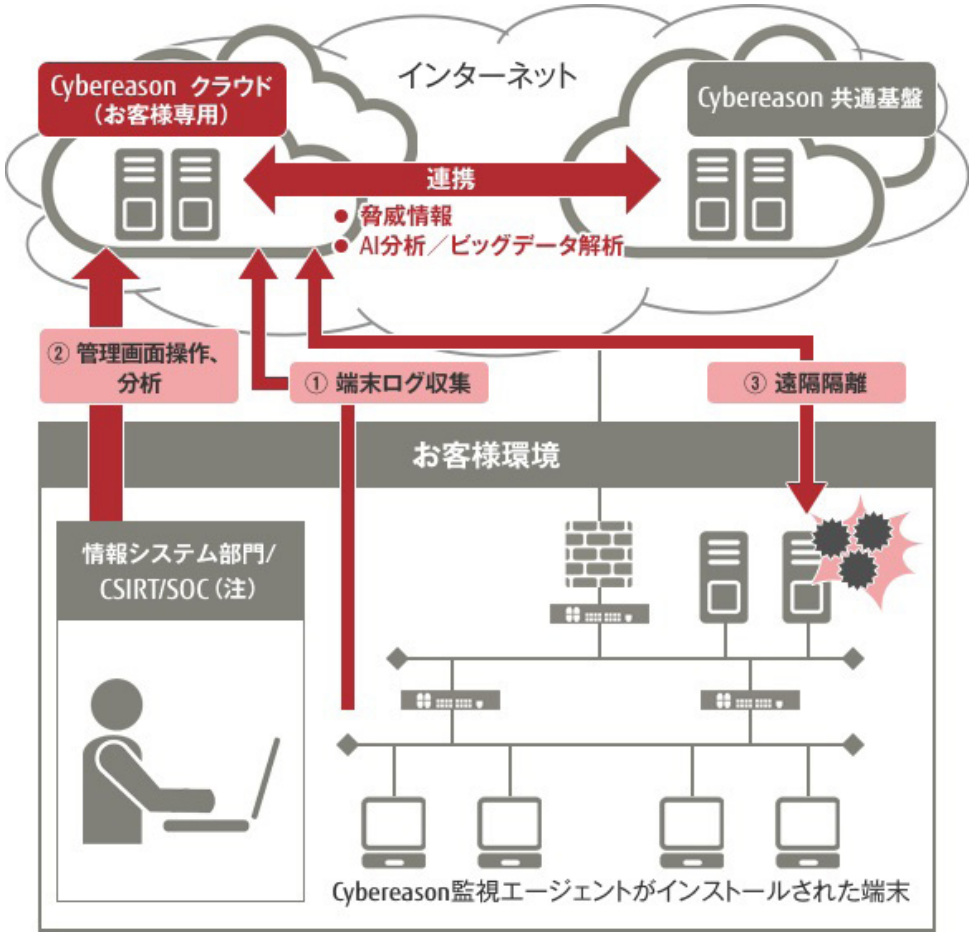
BIOSを狙う攻撃も高度化を続けている。山嶋氏によれば、昨今は「書き換えたBIOSの再書き換えを不能にする攻撃」もあるという。そうなると、メーカーでマザーボードを交換しなければならない。いずれも専門の知識を持った人材かメーカーに頼る必要がある。復旧にコストがかかる上に、復旧まではビジネスが完全に止まってしまう。

「完全なるウイルス・マルウェア防御」は存在しない

「攻撃者は高度な技術を持っています。ターゲットの弱点を次々と見つけて狙ってくるため、ベンダーもユーザー企業も対応が難しくなっています。これからは『攻撃は受けるものだ』という前提に基づいて対処する必要があります」（山嶋氏）

境界で防御することを前提にしたセキュリティシステムだけでは不十分な今、企業が実際の被害を最小限に抑えるために重要なのが「エンドポイント」の対策だ。

具体的にはEDR（Endpoint Detection and Response）の導入が効果的だ。EDRは米国のアナリストが提唱した概念で、PCなどエンドユーザーが使っている端末の状況をリアルタイムで監視する仕組みだ。不正な挙動を検知すると管理者に通知し、それと同時に感染した端末を隔離した後に復旧する。自然災害、火災などの有事において「業務停止時間をいかに少なくするか」を求める、BCP（事業継続計画）と似たような概念である。



FUJITSU Security Solution Cybereason EDRサービスの概要（出典：富士通の製品サイト）

「完全なるウイルス・マルウェア防御は存在しません。防御によるセキュリティ対策に加えて、攻撃を受けて万が一防御を突破されてからの事後対策を考えたシステムがEDRです」（山嶋氏）

ただし、EDRの導入には課題がある。全端末から常に情報を集めて状態を可視化するため効果は高いが、情報を集約して異常な動きがないかどうかを監視するスペシャリストが必要になる点だ。

富士通は、こうした現場の対応負荷を軽減するために「FUJITSU Security Solution Cybereason EDRサービス」を提供する。膨大なログを収集して独自のAIエンジンで分析し、未知の脅威であっても怪しい振る舞いを検出する。攻撃の流れをダッシュボードで可視化し、原因特定までの時間を短縮する。

「BIOS攻撃」にも対抗、自動復旧チップを搭載したノートPC

従来の手法で防ぎきれない脅威は、これからも増え続ける。企業は攻撃を受けた際、システムを復旧させてビジネスが止まる時間を最小限に抑える方法を考える必要がある。しかし山嶋氏によれば、現実は厳しい。

「大企業ではEDRの導入が進みつつあります。しかし中小企業のお客さまにはハードルが高く、当社はそこに危機感を持っています」（山嶋氏）

EDRの導入が難しく、現状のセキュリティ対策が不十分になっている企業に対して富士通は、独自開発した「Endpoint Management Chip」（EMC）を提供する。同社の法人向けPC「LIFEBOOK Uシリーズ」のうち「U9311」「U7411」「U7511」に標準搭載されている。

EMCは、もともと富士通がPCの管理機能を強化するために開発した多用途チップだった。それにBIOSとファームウェア攻撃に対応する機能を追加して、持ち運んでも苦にならない軽量さと薄さ、大画面を備えたPCに実装した。

EMCの特徴は「書き換え不能な保護領域」の存在にある。PCのBIOSが攻撃を受けて書き換えられた場合はハードウェアが検知し、保護領域にある正規のBIOSのマスターイメージを読み込んで復旧する。検知と復旧は全て自動で実行されるため、ユーザーは攻撃を意識せずに通常通りPCを使い続けられる。

「攻撃された際、いかに迅速に対応して正常な状態に戻すかという観点から、BIOSへの攻撃に対してPCメーカーができることを考えた答えがEMCです」と、山嶋氏は自信を見せる。

EMC搭載PCを社員に配布しておけば、BIOSへの攻撃によってPCが起動不能になるトラブルを未然に防げる。オプションではなく標準装備なので管理の負担も低減できる。人手不足が深刻な中小企業に寄り添った結果の仕様と言える。

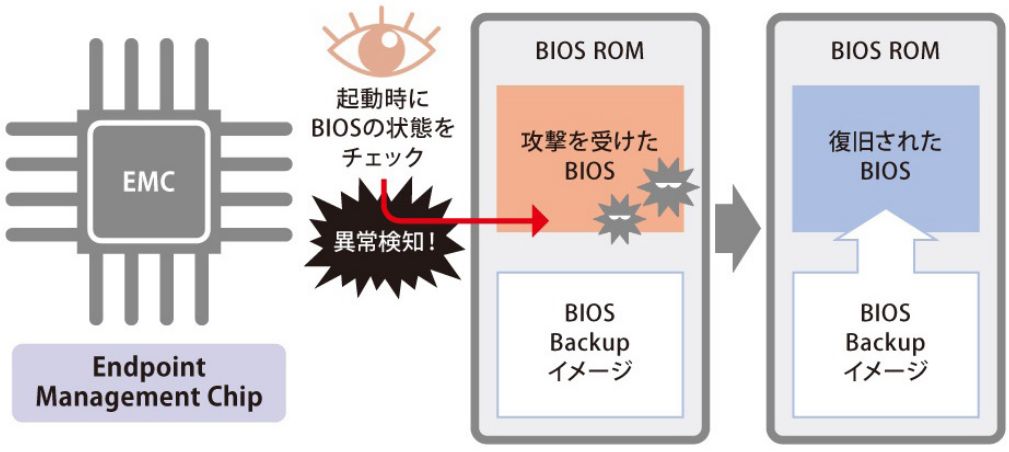
富士通のEMCは、米国のNIST（標準技術研究所）によるセキュリティガイドラインに準拠した技術として第三者機関から検査報告を受けている。

しかしEMCは、あくまで「PCのハードウェアが攻撃されたときの復旧を自動化する機能」だ。OSやアプリケーション、ネットワークなど、その他を狙う攻撃に対するセキュリティ対策も引き続き必要だ。「セキュリティ対策は『多層の備え』が重要です。1つの施策で全ての脅威を排除できるものではありません。攻撃の本質を正しく理解して、環境の変化に合わせて対策をアップデートする必要があります」（山嶋氏）

コロナ禍によってテレワークが急激に普及した。一般的な「自宅からインターネットに接続し、VPNなどを通して社内システムに入る」というネットワーク形態は、インターネット接続時に悪意のある攻撃を受けやすい。

当初は「不十分な装備でもビジネスを続けるため」に持ち出していたPCも、テレワークの長期化や定着化に伴ってセキュリティを見直す時期に来ていないだろうか。

PCを見直す際のキーワードは「自己修復能力」だ。離れていても社員の業務環境を守り事業を継続するため、これから社員に支給するPCはBIOS攻撃からの自己修復が可能な富士通LIFEBOOKが有力な選択肢の一つと言えるだろう。



Endpoint Management ChipによるBIOS書き換え対策の概要（出典：富士通の製品サイト）

ゼロトラストネットワークに求められる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、「FUJITSU Notebook 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FUJITSU Notebook 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。

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。

14型スリムモバイル
LIFEBOOK U7411

15.6型スリムモバイル
LIFEBOOK U7511

端末の動作ログを収集、分析し、悪意のある動作を検出、対策する「FUJITSU Security Solution Cybereason EDRサービス」

Cybereason EDRサービスは、端末の動作ログを収集、分析し、悪意のある動作を検出、対策するクラウドサービスです。攻撃者の心理を取り込んだ攻撃検知AIの活用により、未知の脅威であっても、怪しい振る舞いを検出することが可能です。

- AI／ビッグデータ解析によるリアルタイム検知
- 業務に影響を与えない軽いエージェント
- 攻撃の全体像を直感的に可視化した完全日本語ダッシュボード

「FUJITSU Security Solution Cybereason EDRサービス」については、こちらをご覧ください。

※この冊子は、TechTargetジャパン（https://techtarget.itmedia.co.jp/）に2021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/2106/04/news07.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。