全社員規模でテレワークを導入するための課題「情報漏えい対策」

～「安心、安全なテレワーク環境」の要となる、PCに必要なセキュリティとは?～

テレワークという働き方への移行は急加速。一方でセキュリティ課題は残ったままというケースも

新型コロナウイルス感染症の対策によって、テレワークへの対応は事業継続（BCP）の観点から急速に重要性が高まった。テレワークを基本として、必要に応じて出社するという勤務スタイルを採用する企業も現れている。

このように全社員規模でのテレワークが進む一方で、テレワーク導入におけるサイバーセキュリティの課題も浮き彫りになってきた。その中でも大きな課題となっているのが、ネットワークやセキュリティの在り方、デバイスの使い方などポリシーやルールの早急な見直しへの対応だ。テレワークの制度や社外へ持ち出すPCを保護する仕組みは以前からあったものの、限られた場所、限られた時間で利用することを前提としたコロナ禍以前の対策であり、ニューノーマルでのテレワークでは異なる考え方が求められているためだ。

サイバー攻撃がより巧妙化し続けており、テレワークにおいてセキュリティ対策は急務となっている。従業員がなりすましメールに気付かないままマルウェアに感染し、PCを乗っ取られた状態で社内の重要なデータにアクセスしてしまうといった事故も起こっている。ユーザーが知らないうちに重要データを外部に送信させられたり、悪意を持った人間が外部からPCを操作して重要データを盗み取ったりするケースも少なくない。テレワークの場合、社内ネットワークに施したセキュリティの範疇を越えるシーンがおのずと増えるため、対策を強化する必要がある。

テレワーク時代、もはや境界防御では巧妙化するサイバー脅威を防げない

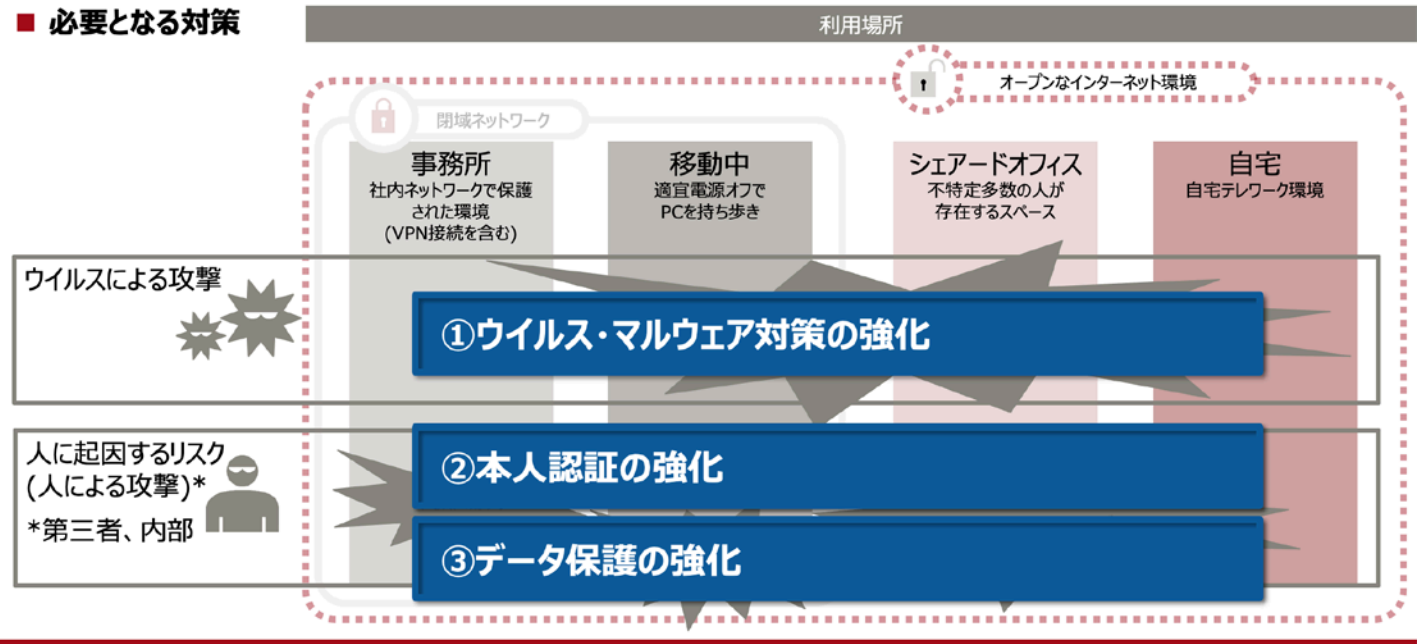
巧妙化するサイバー攻撃対策として現在は、社内と社外という『境界を前提にしたセキュリティ対策』ではなく、リソースへのアクセスを基本的に信頼しないことを前提にした「ゼロトラストネットワーク」という考え方に注目が集まっている。だが、こうしたゼロトラストのリソースへのアクセスポリシー（認証／制御）だけでは十分なセキュリティを確保できない場合もある。システム全体のセキュリティという観点からは、組織のネットワークを介したリソースへのアクセスだけでなく、各アプリケーションやワークロードにも認証や制御が必要になる。設定の不備やユーザーの操作ミスなど、オペレーション上の課題にも対応することが求められる。

そして何より重要なのは、PCなどデバイスのセキュリティだ。これらにトータルで対応すること必要なのだ。

ゼロトラストネットワーク時代にPCが備えるべきエンドポイントセキュリティ

2020年7月、ニューノーマル時代における新たな働き方として「Work Life Shift」というコンセプトを掲げ、固定的な場所や時間にとらわれず、国内約8万人の従業員が“原則テレワーク”に移行した富士通は、セキュリティ対策を整理分析し大別すると3つの対策を行うべきだと定めた。

脅威の種類は大きく分けると「ウイルスによる攻撃」と「人に起



テレワークを含む各利用シーンにおける必要な対策

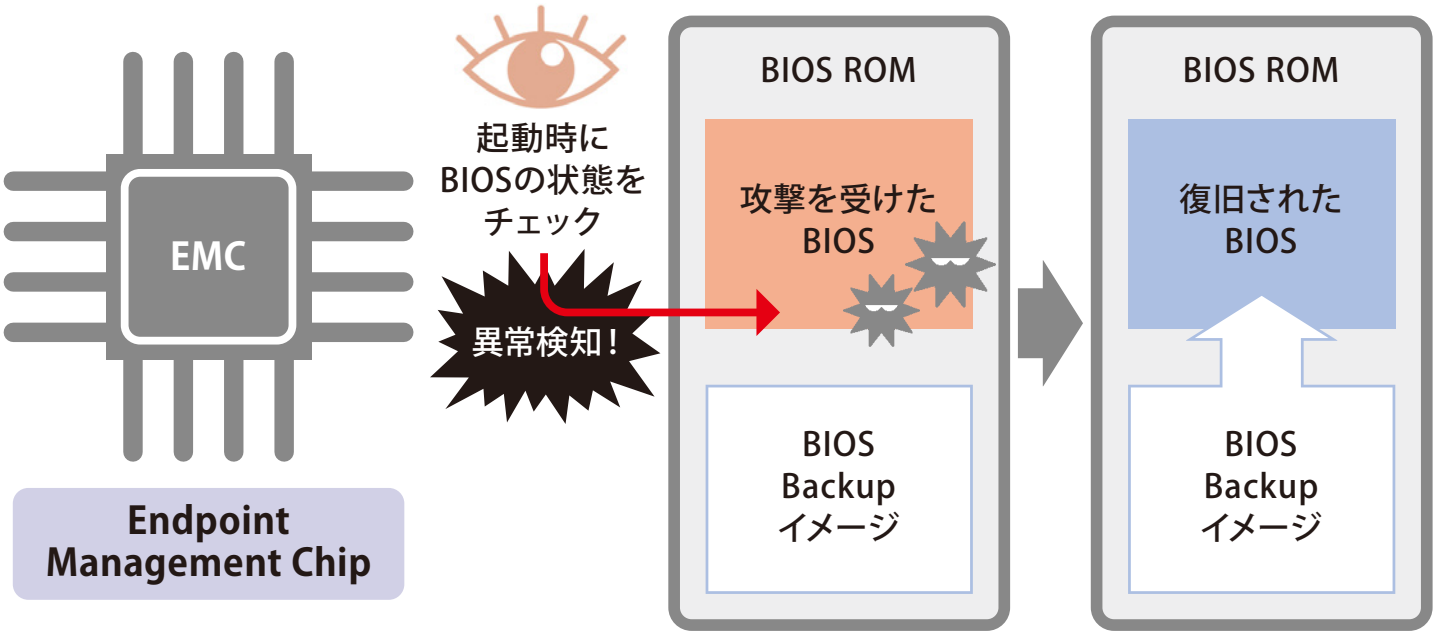
因するリスク（内部／第三者による攻撃）」の2つだ。この2種の脅威に対し、オフィス、移動中、シェアードオフィス、自宅という利用シーンを想定すると、セキュリティ対策は「ウイルス、マルウェア対策の強化」「本人認証の強化」「データ保護の強化」の3つが重要になると考えている。

次項では富士通が法人向けPCで提供する3つのエンドポイントソリューションを解説する。

【①ウイルス・マルウェア対策の強化】
アンチウイルスソフトでは守ることができない サイバー脅威への対策とは

最新のウイルス、マルウェア対策の強化対策の一つが、FUJITSU Notebook LIFEBOOKおよびFUJITSU Tablet ARROWS Tabシリーズ（一部機種を除く）に組み込まれた、富士通が独自に開発した新しいハードウェア「Endpoint Management Chip」（EMC）だ。

最近のマルウェアではPCのBIOSをターゲットに攻撃する種類も現れている。BIOSが感染すると初期化しても駆除が難しいケースもあり、従来の対策であるアンチウイルスソフトウェアだけでは守ることができない。LIFEBOOKやARROWS Tabシリーズなどの EMCを組み込んだPCであれば、攻撃に対する防御を強化すると同時に、万が一に備えて、起動時にBIOSの状態をチェックしてサイバー攻撃などの異常を素早く検知できる。またBIOSのバックアップイメージを保存しているため、BIOSの異常を自動的に修復することも可能だ。これにより、サイバー攻撃を受けた場合に素早く復旧するレジリエンスを確保できる。



BIOS、ファームウェアリカバリー機能を提供。PC起動時にBIOSへの攻撃や異常を検知して迅速に修復する

【②本人認証の強化】
IDとパスワードだけの本人認証では「真の安心・安全」は困難

IDとパスワードによる本人認証を利用している企業は多いが、IDがメールアドレスである場合は、パスワードの総当たり攻撃や安易なパスワードの使い回しから漏えいしたパスワードが使われて社内システムに不正アクセスされる事故も起きかねない。

そこで本人認証の強化が重要となってくる。富士通では認証ソフトウェア「AuthConductor Client Basic」を提供している。AuthConductor Client Basicは、Windowsや業務システムへのログイン時に、手のひら静脈、指紋、顔認証、ICカードなどのセキュリティデバイスを使ってIDやパスワードの入力を代行するクライアントソフトウェアだ。複数のIDやパスワードの組み合わせを覚える必要がなく、シングルサインオン（SSO）を設定すれば認証は一度のみで済むため、セキュリティを強化しながらユーザーの利便性を高められる。こうしたユーザーのリテラシーを問わないアプローチは、セキュリティ対策の鉄則の一つと言える。

ソフトウェアと各種センサーデバイスを連携させたソリューション。ユーザーの利便性と安全性を両立する

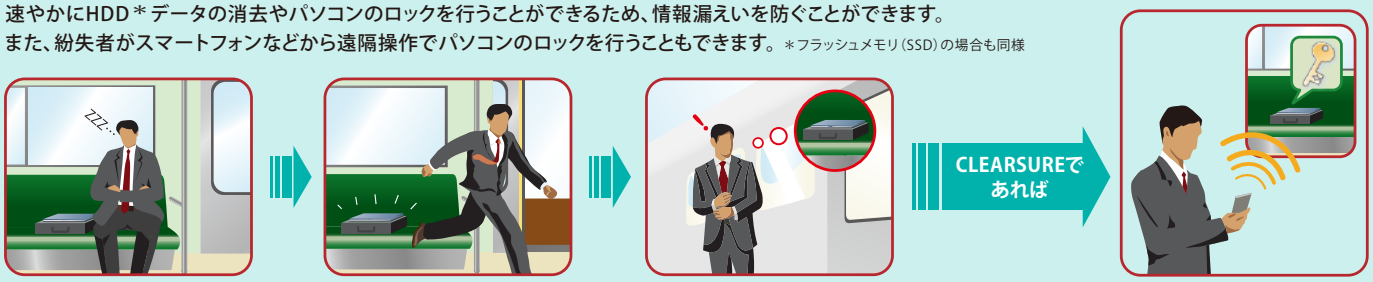
【③データ保護の強化】
PC持ち出しにつきまとう PCに紛失や盗難による情報漏えいのリスク

データ保護の強化はテレワークには最重要対策といっても過言ではない。遠隔操作でPCのロックやデータ消去をすることで、盗難、紛失したPCからの情報漏えいを防止する機能が求められる。

富士通が提供するCLEASUREを利用すると、スマートフォンで遠隔からPCのデータを保護できる。大きな特長は、PCの電源がオフでも3G／LTE回線を利用してPCをロックし、データを消去できることだ。これにより、万一の際には紛失者自身がスマートフォンからロックを指示でき、また管理者からは即座にPCのデータを消去できる。

紛失・盗難の危険性と対策

これまでパソコンの紛失・盗難は情報漏えいの危険性を高め、企業ではモバイルパソコンの持ち出しを制限する原因の一つにもなっていました。
例えば、電車内でパソコンを置き忘れてしまった場合、後からそのパソコンに対して情報漏えいを防ぐ対策をとることは困難でした。
CLEARSURE対応パソコンであれば、紛失者が管理者と連絡をとることで、管理者のパソコンから遠隔操作により
速やかにHDD＊データの消去やパソコンのロックを行うことができるため、情報漏えいを防ぐことができます。
また、紛失者がスマートフォンなどから遠隔操作でパソコンのロックを行うこともできます。＊フラッシュメモリ（SSD）の場合も同様



CLEARSURE対応PCでは、電源がオフでも3G／LTE回線を利用して、スマートフォンからの遠隔操作でPCをロック可能。万一の際も被害を最小限に抑えられる

セキュリティ対策は直接的な利益を生み出すものではない。しかしサイバー攻撃が巧妙化し続ける現在、何らかの対策を打たなければ甚大な被害を招きかねず、利益と信頼を失いかねない。テレワーク移行とともにPCのセキュリティ対策を見直してみてはいかがだろうか。

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。