ニューノーマル時代に必要なセキュリティ
～新たな課題と対策のポイント～

斎藤　建　　多川　剛

あらまし

新型コロナウイルスの流行により，ニューノーマル時代が到来した。働き方は，在宅でのテレワークなど，場所に依存しないスタイルへシフトしている。一方，サイバー攻撃は増加し，テレワークによる情報漏えいの危険性が懸念されるなど，様々な問題も浮き彫りになった。

本稿では，こうしたニューノーマル時代の変化に対応するために必要なセキュリティについて述べる。

1. まえがき

新型コロナが猛威を振るい始めて1年が経った。この1年，急速にテレワークに必要な環境や制度の整備が進められ，オフィスへ出社する必要がない新しい働き方がニューノーマルとして浸透してきている。これまでオフィス業務は都市部に集中していたが，業務によっては必ずしも必要がなくなり，リアルなイベントはオンラインで代替され，会議はオンライン化することとなった [1]。

しかし，テレワークにおけるセキュリティが後回しになっている企業も少なくない。そのため，テレワークに必要なセキュリティを実装し，安全な環境を構築することが急務になっている。

本稿では，こうしたニューノーマル時代において新たに出現した課題に対し，新たに必要となるセキュリティの考え方とその課題と解決策，更にはそれを実現する富士通のセキュリティソリューションを紹介する。

2. ニューノーマル時代に必要なセキュリティ

本章ではニューノーマル時代に適したセキュリティの考え方について述べる。

クラウド利用によって，社内のネットワークで守られていた情報（社内のサーバーに保管されていた情報）が，社外のストレージに格納されるケースが増えてきた。更に，コロナ禍によるテレワーク促進によって，社内ネットワークの中で，ファイアウォールなどによって守られていた従業員端末も社外に持ち出されることとなり，情報漏えいのリスクが高まっている。こうしたことを解決するためのセキュリティのポイントについて述べる。

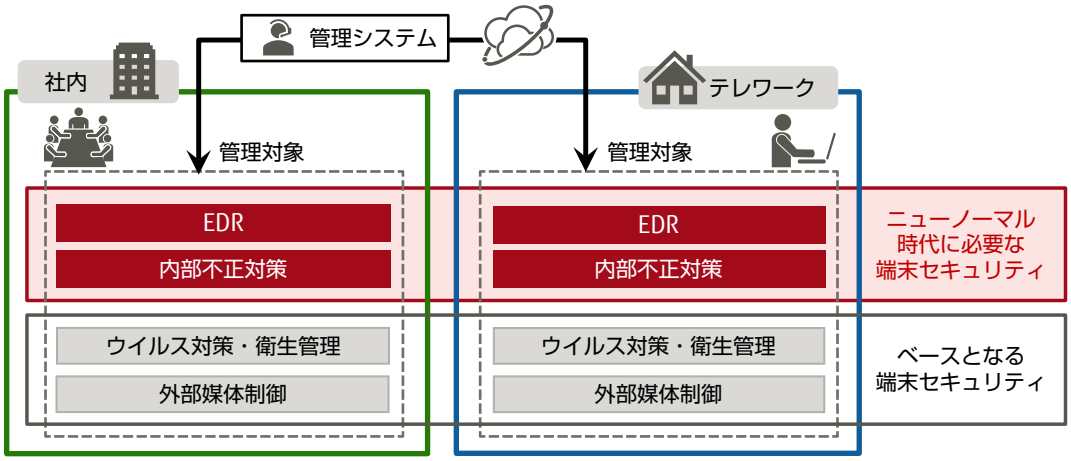
2.1 端末セキュリティ

本節では，ニューノーマル時代に必要な端末セキュリティについて述べる。ベースとなるセキュリティとニューノーマル時代において必要となる端末セキュリティのイメージを図-1に示す。

2.1.1 現状の課題

従業員が端末を自宅など社外で利用する機会が増えたため，その端末を適切に管理することが難しくなっており，以下の課題が出てきている。

- 従来の企業管理システム配下にいない状況になり，常時企業のポリシーに応じて制御を行う仕組みが必要であること。
- 企業が統制できない使い方をされる可能性があるため，高まるマルウェア感染リスクを減らすこと。
- 在宅であると人の目がなく様々なことを行ってしまう可能性があるため，個人のモラルに依存しない仕組みが必要であること。



EDR：Endpoint Detection and Response

図-1　ニューノーマル時代に必要な端末セキュリティ

2.1.2 ニューノーマル時代に必要な端末セキュリティ

社内外で一貫した端末セキュリティを確保するためには，まずセキュリティのベースを社内外ともに統一して行い，その上で，テレワークにおいて必要なセキュリティを追加で対応していく必要がある（図-1）。

(1) ベースとなるセキュリティの実施

社内外の環境に限らず，まずはベースとなるセキュリティをしっかりと実施することが必要である。

ベースとなるセキュリティとは，ウイルス対策ソフトの導入，USBなど外部媒体の制御および，適切なパッチ適用などの衛生管理である。テレワークにおいては管理ネットワークが行き届かないこともあり，セキュリティが疎かになってしまうことがある。社内と同じ環境を，テレワーク環境でもしっかりと実装することが，まずは大事である。

(2) 新たに必要なサイバー攻撃対策

テレワーク環境下では，企業のポリシーに応じた防御が難しくなることや企業が統制できない端末の使い方によるマルウェア感染のリスクがある。

これを解決するために，端末においてサイバー攻撃を追跡するための対策が必要となる。攻撃者が残すログなどからサイバー攻撃を追跡・対応する対策がEDR（Endpoint Detection and Response）と呼ばれ，近年注目が集まっている。

(3) 内部関係者による情報漏えい対策

テレワークにおいては，従業員の行動に目が行き届きにくくなる。そのため，内部脅威からの被害を最小限に抑えるためのセキュリティが必要である。

従来のセキュリティの考え方としてのアクセスを制限し制御するだけでなく，内部不正が行われる前にその予兆を検知し，従業員への教育や施策の見直しにつなげることが必要となっている。

2.2 ネットワークセキュリティ

本節では，ニューノーマル時代に必要なネットワークセキュリティについて述べる。

2.2.1 現状の課題

テレワーク化が進む中では，データセンターに設置されているセキュリティのゲートウェイ（ファイアウォールやVPN装置）を経由し外部ネットワークへアクセスすると，性能の限界があり帯域がひっ迫する。これを回避するためには，企業が用意しているセキュリティのゲートウェイを経由することなくクラウドへ直接アクセスすれば良い。反面，危険なクラウドに直接アクセスすることによるマルウェア感染などの対策が課題となる。

2.2.2 ニューノーマル時代に必要なネットワークセキュリティ

本項では，ニューノーマル時代に必要なセキュアかつ帯域をひっ迫しないセキュリティについて述べる。必要と考えられるネットワークセキュリティについて図-2に示す。

(1) インターネットブレイクアウト

テレワーカーが直接，外部のクラウドへアクセスすることによって，マルウェア感染などのリスクが高まる。これを回避するために，企業が認めた安全なクラウドへのアクセスについてのみセキュリティのゲートウェイを通らないなど，クラウドへの振り分けを行う必要がある。これがインターネットブレイクアウトと呼ばれる。セキュリティのゲートウェイの負荷を軽減できるため，ニューノーマル時代におけるセキュリティとして必要な考え方といえる。

(2) セキュリティ機能のクラウド化

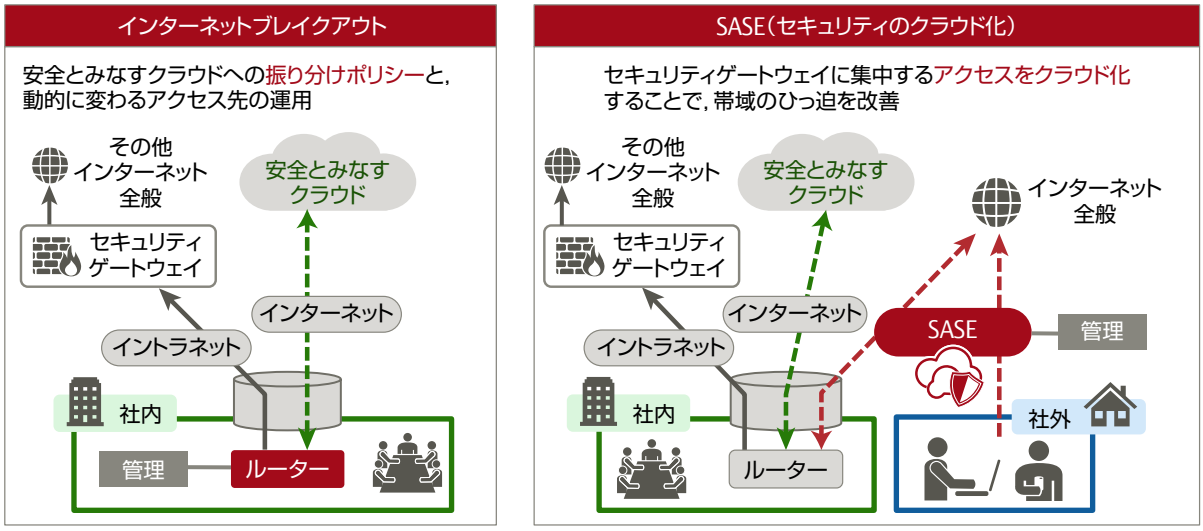
テレワーカーの増加によるセキュリティゲートウェイのひっ迫は，セキュリティゲートウェイへのアクセス一極集中に一因がある。これを解消する考え方として，クラウド化による動的なセキュアアクセスがある。この方法がSASE（Secure Access Service Edge）と呼ばれるものである。これまでデータセンター一極集中だったセキュリティ機能をクラウド化し，場所を問わず一括してセキュアにインターネットへアクセスできる環境を提供することが，ニューノーマル時代には必要である。

2.3 クラウドセキュリティ

本節では，クラウド利用におけるセキュリティについて述べる。

2.3.1 クラウドセキュリティの課題

ニューノーマル時代ではクラウドを利用した情報共有が必須となり，クラウド利用が急加速したた



SASE：Secure Access Service Edge

図-2　ニューノーマル時代に必要なネットワークセキュリティ

め，その管理が課題となっている。

特に従業員が自宅などで仕事をするテレワーク環境下においては，従業員に対し目が行き届かなくなり，管理が困難になることがある。そうした場合に考えられる一つの従業員の行動として，様々なウェブサイトへアクセスし，勝手に様々なクラウドを利用してしまうことがリスクの一つとして考えられる。

2. 3. 2　ニューノーマル時代に必要なクラウドセキュリティ

(1) クラウド利用状況の可視化

世に多数あるクラウド（特に個人向けサービス）を従業員が勝手に利用してしまうと，危険なクラウドにデータを格納することによって，情報漏えいのリスクが高まることがある。特にテレワーク環境下においては，様々なクラウドを利用してしまう従業員も出てくる。そのため，適切なクラウドの利用統制が必要になっている。

(2) クラウドのセキュアな設定管理

企業が従業員に提供している法人向けクラウドサービスにおいて，クラウドの管理が困難となっているケースがある。例えば設定ミスによって個人情報が社外の人間も閲覧できるようになってしまった事故事例も後を絶たない。そのため，ポリシーに応じた設定がなされているかどうかを監視/適用していく必要がある。

3.　ニューノーマル時代に必要なセキュリティソリューション

本章では，ニューノーマル時代に必要な新しいセキュリティ対策として，富士通が提供しているソリューションについて述べる。

3. 1　端末セキュリティのソリューション

本節では，富士通が提供しているテレワークに向けた端末セキュリティのソリューションについて述べる。

(1) サイバー攻撃対策ソリューション

テレワーク環境下においては，遠隔でもサイバー攻撃を追跡できる，EDRと呼ばれる対策が必要であると述べた。そこで富士通は「FUJITSU Security Solution Cybereason EDRサービス」を提供している。Cybereason EDRサービスの概要を図-3に示す。このサービスを利用することで，端末におけるデータをAI分析，攻撃の兆候をリアルタイムに監視し，必要に応じて端末を遠隔遮断するなど即時対応可能なソリューションを提供する。

(2) 内部関係者による情報漏えい対策

内部関係者による情報漏えい対策として，内部不正の予兆を検知し防止する仕組みが必要であると述べた。

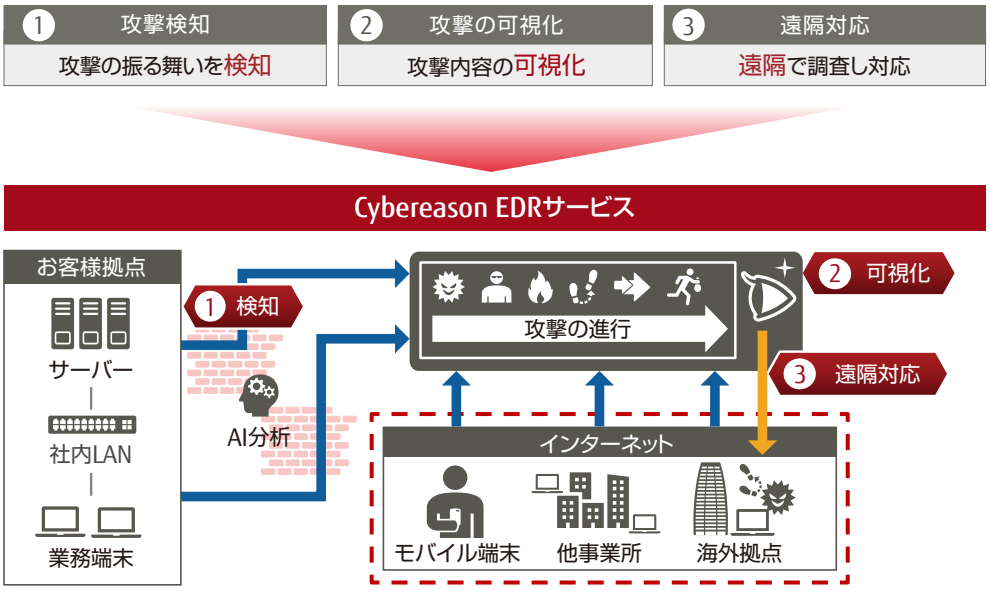


図-3　Cybereason EDRサービス概要

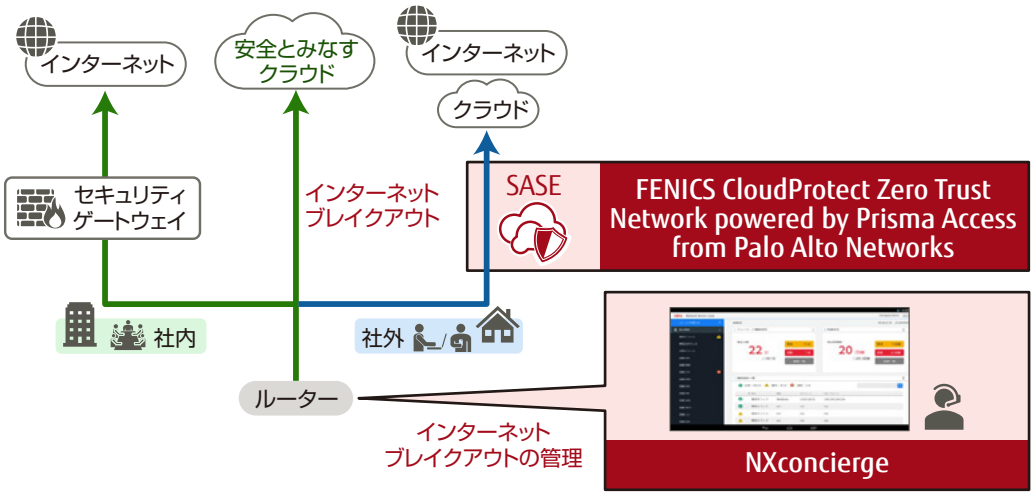


図-4　ネットワークセキュリティソリューションの概要

これを実現するために「FUJITSU Security Solution Dtex内部リスク可視化（UEBA）運用支援サービス」を提供している。このサービスによってユーザーの日常の行動を機械学習し，異常な行動を検出/分析することで，情報漏えいの発生を防ぐソリューションを提供する。

3.2 ネットワークセキュリティのソリューション

本節では，ネットワークセキュリティのソリューションについて述べる。図-4はその概要である。

(1) インターネットブレイクアウトを実現するソリューション

セキュリティのゲートウェイを通らずに直接Webへセキュアなアクセスを実現するためのインターネットブレイクアウトの必要性については既に述べた。

これを実現するために「FUJITSU Network NXconcierge」を提供している（図-4）。顧客が必要となるSaaSへのアクセスを一元管理・制御する

ことによって，セキュリティのゲートウェイの負荷を軽減したセキュアなアクセスを実現する。

(2) SASEを実現するソリューション

データセンター一極集中のセキュリティ機能をクラウド化し，自由でセキュアなアクセスを可能にするSASEの考え方を実現するソリューション「FUJITSU Managed Infrastructure Service FENICS CloudProtect Zero Trust Network powered by Prisma Access from Palo Alto Networks」を提供している（図-4）。これによってSASEに必要な機能を提供し，顧客のSASE実現を可能にする。

3.3 クラウド利用におけるセキュリティソリューション

本節では，クラウド利用に対するセキュリティソリューションについて述べる。

(1) クラウド利用状況の可視化

世に多数あるクラウドの利用統制を実現するために，富士通ではMcAfee社と連携し，「McAfee MVISION Cloud（CASB）」を提供している。このソリューションによって，様々なクラウドのそれぞれの危険性と従業員の利用状況を可視化できるだけでなく，既存のファイアウォールなどと連携してアクセスの停止などの対応ができる。

(2) クラウドのセキュアな設定管理

企業が従業員に提供しているクラウドにおいても，設定ミスなどによる情報漏えいのリスクがあることは既に述べた。

これを解決するために，「Prisma Cloud」を提供している。このソリューションによって，誤った設定を自動的に見つけ出しアラームを上げ，適切な設定に変更を促す。

4. むすび

新型コロナウイルスの流行に伴い，急激にテレワークが普及してきた。このようなニューノーマル時代において，セキュリティの観点から改善すべき課題があることや，その考え方，およびその課題解決を実現する富士通のソリューションの一端を紹介した。

まだ課題もある。サイバー攻撃は更に進化することが予測され，内部関係者による情報漏えいの穴も完全に塞ぐには容易でない。今後はこうしたことを解決していかなければならないだろう。

本来，コンピューターの技術は，人類を豊かにするために生まれてきたものである。つまり，セキュリティはこれを正しく実現する技術であるといってよく，我々はこの歴史の扉を明るい未来へ押しあけていく責務があると考えている。

参考文献・注記

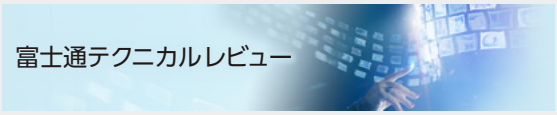
[1] International Labour Organization：A practical Guide: Teleworking during the COVID-19 pandemic and beyond (2020).
https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/instructionalmaterial/wcms_751232.pdf

著者紹介

斎藤　建（さいとう　けん）
富士通株式会社
戦略企画・プロモーション室
サイバー攻撃対策啓発活動およびセキュリティ商品のプロモーション/マーケティングに従事。

多川　剛（たがわ　たけし）
富士通株式会社
戦略企画・プロモーション室
サイバーセキュリティ商品の拡販に従事。

この記事は，富士通の技術情報メディア「富士通テクニカルレビュー」に掲載されたものです。
他の記事も是非ご覧ください。



https://www.fujitsu.com/jp/technicalreview/