ニューノーマルの落とし穴、サイバー攻撃リスクに対抗!!
新しい働き方や非接触型ビジネスの必須項目!!
ウィズコロナ社会のサイバーセキュリティ読本

ニューノーマルに対応したビジネスや働き方を実践する企業が躍進する一方、サイバー攻撃のリスクが急拡大している。そこで今号ではウィズコロナ社会の必須項目であるサイバーセキュリティを大特集。まずはコロナ禍をめぐる世界と日本の窮状をレポートし、ついでわれわれが直面する産業構造のかつてない二極化についての分析をしてみたい。

急伸する非接触型ビジネスと落ち込む一方の接触型ビジネス

コロナ禍がいっこうに収まらないなか、アメリカをはじめとする世界主要国経済の2020年4月～6月期の実質国内総生産（GDP）は前年同期比9・1㌫減少となった（8月18日付、日経新聞）。「100年に一度の危機」といわれたリーマンショック当時の3・5倍の落ち込みといわれ、米国は年率32・9㌫減、ユーロ圏は40・3㌫減と惨憺たる状況だ。日本も年率27・8㌫減となり（8月17日、内閣府発表速報値）、7年半ぶりに500兆円を下回って485兆円。SMBC日興証券の集計によると東証一部上場企業の3割が最終赤字になり、上場地銀の6割も減益か赤字に。とくに深刻な赤字業種は運輸、旅行、外食など11種にもおよび、すでに余力のない中堅・中小企業がつぎつぎと「あきらめ倒産」に追い込まれている。経済アナリストたちはこの9月から年末、来年にかけて、資金繰りに困った中小企業の倒産が続出するので

カバー／P3イラスト©emojoez/shutterstock.com

いたるところに潜むサイバー攻撃リスク
中小企業も当事者としてセキュリティ対策整備を!!

はないかと予測する。しかも、GoTOトラベルキャンペーンなど早々に観光促進策が打ち出されたこともあって感染拡大傾向に逆戻りしてしまい、若干は持ち直すかにみえた景気はふたたび悪化の一途をたどっている。コロナ禍初期段階に一部で持ち上がっていた「災禍が収まりさえすれば抑制されていた需要が復活し、経済はV字型に回復する」という楽観的展開はもはやありえない。もしコロナ禍前の水準に戻るとしても、2023～24年頃にかけてゆっくりとU字型の回復に転じていくのではないか、というのが民間エコノミストたちの見方だ。あるいは一進一退を繰り返すW字回復をたどるといったほうが現実的ではないか。

だが、こうした世界的な恐慌状態にあって急伸している分野がある。いうまでもなく、ウィズコロナにおける新常態（ニューノーマル）に対応した非接触型ビジネスである。GAFAをトップとして、ネット通販やオンライン会議システム、レジレスサービス、ロボット店員、ドローン宅配サービス、IoT、自動運転、遠隔医療などに関するビジネスへの投資が活発化しているのだ。ウィズコロナ時代にあって、テレワークやオンラインミーティングなどの新しい働き方が一過性のものではないという認識はいまや常識。自民党税制調査会長の甘利明氏もそれを意識し、新国際秩序創造戦略本部の座長としてデジタルトランスフォーメーションの推進を明言している。

こうしてみると、これから先世界を待ち受けているのはV字型回復でもU字型回復でもない。非接触型ビジネスや新しい働き方を実践する強い企業が伸びつづけ、従来通りの飲食業や宿泊業などの接触型ビジネスがひたすら落ちていく極端な二極化、グラフにしてみれば上方に向かう線と下方に向かう線とがはなれていく「K字型」の構造なのではないか。当然、これからはあらゆる企業がこの「K」の上昇側に加わろうと積極的にICTを活用したり、非接触型ビジネスにカジを切ったりと生き残り戦略を模索していくことになる。

そんななか、非常に重要になってくるのがサイバーセキュリティ対策だ。どんなに成長の可能性を秘めたビジネスモデルでも、サイバー攻撃を機にすべてがご破算となりかねない。アメリカでは数万人のサイバーセキュリティ人材が育成されており、さまざまな組織・企業内にセキュリティ部門や専任ポストがあるのが当たり前だが、日本にはそういった体制は整っていない。今後、ニューノーマルに対応した新しいビジネスがつぎつぎと芽吹いていくというのに、このままサイバー攻撃というリスクを放置しておいていいはずがない。そこで、今号ではサイバーセキュリティを特集。ここ数年のサイバー攻撃のリスクや最新のセキュリティツール、業界や国としての対策などを概観し、ウィズコロナ社会におけるサイバーセキュリティのあるべき姿を探っていきたい。

日常生活や経済活動におけるさまざまなリスク

まず左上の表をご覧いただきたい。東京工業大学情報理工学院サイバーセキュリティ研究センター長を務める田中圭介教授の監修の下、弊誌独自にさまざまな業種・業界で高まるサイバー攻撃のリスクを列挙したものである。日常生活や経済活動のあらゆる場面に、実に幅広いリスクが潜んでいることが実感できると思う。なかでも、三菱重工業（名古屋地区）のネットワークへの不正アクセスは記憶に新しい。従業員がテレワーク時に、業務用パソコンでSNSに接続したことがキッカケでウイルスに感染し、それが社内ネットワークに広がってしまったこの事件は、ニューノーマルにおけるサイバーセキュリティ対策の重要性をあらためて浮き彫りにした。同社の発表によれば「取引先や技術に関する重要な情報は含まれていない」とのことだが、ニューノーマルに対応した新しい働き方やビジネスにはつねに重要情報漏洩のリスクがつきまとうのは事実だ。

進化するサイバー攻撃の最新トレンド

では今、とくにどのようなサイバー攻撃が増えているのか。独自のサイバーセキュリティシステムを組み込んだセキュアPCで世界的に高評価を受けている米HP社の子会社、㈱日本HPのパーソナルシステムズ事業本部プログラムマネージャーを務める大津山隆氏に、ここ数年のサイバー攻撃のトレンドを聞いてみた。曰く、その傾向は大きく分けて「①ファームウエア攻撃の増加」「②破壊的攻撃のトレンド」「③急速なマルウェアの進化」の3点だという。

まず①について、ファームウエアとはパソコンのハードウェアを制御するためのプログラムのこと。「ビジネス用パソコンのOSがウィンドウズ10になってかなりセキュリティレベルが上がったため、攻撃側があらたな抜け道としてOSの下層にあるBIOS（起動時のOSの読み込みなどを行うプログラム）などのファームウエアに攻撃を仕掛け、プログラムをのっとったり破壊したりする事例が増えている」そうだ。

また「日本では2015年に日本年金機構の年金情報管理システムサーバから125万件もの個人情報が流出した問題が起きたこともあって、サイバー攻撃といえば情報漏洩をイメージする人が多いが、実は10年頃か

さまざまな業種・業界で高まるサイバー攻撃のリスク

テレワーク	三菱重工業は8月7日、名古屋地区のネットワークに外部から不正アクセスがあり、従業員の個人情報などが漏えいしたことを発表。テレワーク中、外部ネットワークに接続した従業員の社用パソコンがウイルスに感染し、出社時に社内ネットワークに感染が広がった。テレワークにおけるサイバー攻撃の危険性があらためて指摘された。
IoT	Society 5.0（AIやIoT、ロボット、ビッグデータなどの革新技術をあらゆる産業や社会に取り入れることで実現するあらたな未来社会の姿）のキーテクノロジーともいえるIoT（Internet of Things）。インターネットを介してさまざまなモノ同士が相互につながり合い、あらゆる活動とその軌跡がデータ化され、蓄積されたビッグデータを分析・活用してあらたな価値を創出する――。この技術が普及することで人の生活は便利になり、あらたなビジネスも生まれやすくなるが、同時にIoT機器を狙ったサイバー攻撃が急増中。事実、アメリカでは数年前、セキュリティが脆弱な約10万台ものIoT機器が乗っ取られ、ネット企業へのサイバー攻撃に利用されるという事件が起きた。 「あらゆるモノがつながり合う」ということは、裏を返せば、その広範なネットワークに侵入した不正プログラムなどの排除や追跡が困難ということでもある。コネクテッドカーがハッキングを受けて遠隔操作されたり、監視カメラの映像がインターネット上で公開・拡散されたり、自動化工場の生産がマルウェアに狂わされたりと、被害の可能性は無限にある。
ICT教育	学校教育のICT化を一気に推進するため、政府主導ですすめられている「GIGAスクール構想」。2019年12月、政府は全国の学校に高速・大容量通信環境を整備し、全生徒に1人1台学習用パソコンかタブレット型端末を無償で配備する方針を打ち出した。24年度までに実現を目指すという。ICT教育は児童・生徒の学習効果を高める一方で、不正アクセスによる個人情報漏洩などさまざまなリスクも指摘されている。行政主導のセキュリティ整備と、教員・生徒双方のセキュリティリテラシー向上が必須だ。
サイバー兵器	2010年9月、特定の標的を狙う巧妙なワーム「スタクスネット」がイランの核燃料施設のウラン濃縮用遠心分離機を標的として用いられ、イランの核開発を妨害。世界初の制御システムを標的とするサイバー兵器といわれ、この攻撃がきっかけで国家間サイバー戦争が幕を開けたといわれている。
ファーウェイ排除	アメリカ政府はこの2月、中国ファーウェイが違法なバックドア（不正アクセスするための裏口）を製品に仕込んでいることの証明が可能だと発表。8月には禁輸措置の強化によって、アメリカの技術が関わる半導体やソフトがファーウェイにわたるのを完全に遮断することも決定した。これにより、ファーウェイは今後、5G対応などの高度なスマホが計画通りにつくれなくなる可能性が出てきている。 中国政府が通信インフラを介して全世界のネットワークを監視するのではないか、という疑念は以前からアメリカなどで高まっていたが、現在、ファーウェイ排除の動きは世界的に拡大しており、インド・イギリス・フランス・EU・オーストラリア・日本などで検討されている。

サイバー攻撃の脅威の変化（HP社による分析）

①ファームウェア攻撃の増加	②破壊的攻撃のトレンド	③急速なマルウェアの進化
・マルウェア感染のなかでEメールの添付ファイルに起因する割合は94パーセント（※1） ・アンチウイルスが見逃したエンドポイント攻撃の割合は57パーセント（※2） ・70パーセント以上のセキュリティ被害がエンドポイントの侵害から ・エンドポイント攻撃の99パーセント以上はEメール、ウェブサイト、チャット、USBを経由		

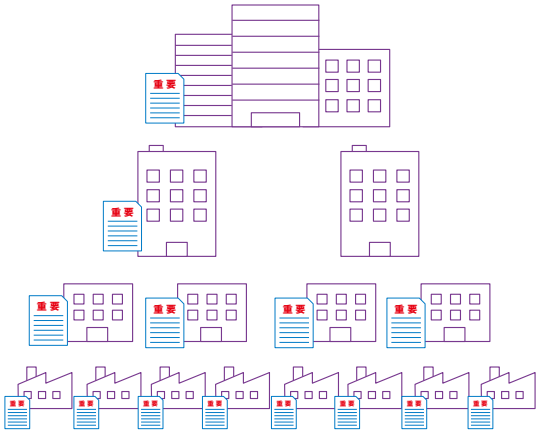
（※1）2018 Data Breach Investigations report 11th Edition, Verizon, 2018
（※2）Ponemon Institute 2018 State of Endpoint Security Risk sponsored by Barkly, October 2018

ら②の破壊的攻撃がドンドン増加している」という。システムや情報を改ざんしたり、情報やシステムにアクセスできないようにしたり、社会的に重要なシステムの停止によって混乱をもたらす可能性のあるケースが多くなっているのである。

このようなリスクが高まるなか、恐ろしいのが③マルウェアの進化や多様化に従来のアンチウイルスソフトだけでは十分に対応できないという事実だ。大津山氏によれば「従来のアンチウイルスソフトの基本スタンスは、世に出回っているウイルスのパターンを把握したうえで、それに合致するものを検知して止める」というもの。かつてはこの方法が有効だったが、「最近では1日に35万ものマルウェアが誕生しており、ウイルスの種類も増えていてパターンファイルによる検知ではとても追いきれない」という。

これら3点に加えて、攻撃・侵入の方法としては三菱重工業のケースがそうだったように7割以上のセキュリティ被害がエンドポイント（パソコンなどの端末のこと）からはじまっており、エンドポイント攻撃の99パーセント以上がEメールやウェブサイト、チャット、USBを経由。そして「標的型攻撃メールに緊急性の高そうなメッセージを添えるなど、エンドポイントの先にいる人間の心理の隙をついて添付ファイルを開かせ、攻撃に成功する例が多い」そうだ。

■大企業から中小企業まで、サプライチェーンの弱点を狙ったサイバー攻撃が顕在化・高度化



大企業

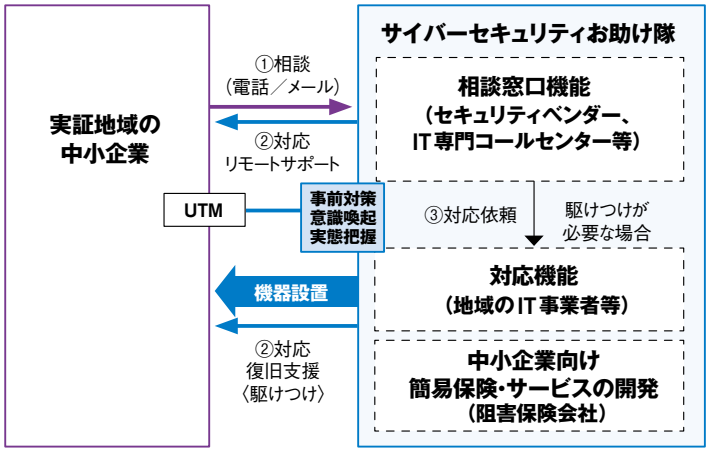
2020年1月以降、三菱電機、NECなど、防衛省と取引関係にある企業が過去に高度なサイバー攻撃被害に遭っていたことが明らかに。防衛機微情報が狙われた可能性。

中小企業

経済産業省は「サイバーセキュリティお助け隊」事業を実施。同事業を通じて地域・企業規模にかかわらず中小企業もサイバー攻撃の対象となっていることが判明。

同事業の実証地域:
①岩手、宮城、福島 ②新潟 ③長野、群馬、栃木、茨城、埼玉 ④神奈川 ⑤石川、福井、富山 ⑥愛知 ⑦大阪、京都、兵庫 ⑧広島、山口

■経済産業省「お助け隊実証事業」(令和元年度)



実証結果

中小企業　側	保険会社、セキュリティベンダー　側
・自社の攻撃実態などへの気づき ・セキュリティ事前対策の促進 ・事後対応への意識向上　等	・中小企業のセキュリティ対策状況の把握 ・中小企業の被害実態の把握 ・中小企業の求めるサービスの把握　等

■駆け付け支援の対象となった特徴的な対応事例

古いOSの使用	私物端末の利用
○Windows XPでしか動作しないソフトウェア利用のために、マルウェア対策ソフト未導入のWindows XP端末を使用。 ○社内プリンタ使用のために、社内LANに接続したことで、意図せずにインターネット接続状態になり、マルウェアに感染。 ○検知・駆除できていなかった場合の想定被害額は5500万円。	○社員の私物iPhoneが会社のWi-Fiに無断で接続されていたことが判明。 ○私物iPhoneは、過去にマルウェアやランサムウェアの配布に利用されている攻撃者のサーバーと通信していた。 ○検知・駆除できていなかった場合の想定被害額は4925万円。

ホテルWi-Fiの利用	サプライチェーン攻撃
○社員が出張先ホテルのWi-Fi環境でなりすましメールを受信し、添付されたマルウェアを実行。感染によりアドレス情報が抜き取られた後、当該企業になりすまして、取引先等に悪性メールが送信された。	○実証参加企業でマルウェア添付メールを集中検知。 ○取引先のメールサーバーがハックされてメールアドレスが漏えいし、それらのアドレスからマルウェア添付メールが送付されていた。 ○メールは賞与支払い、請求書支払い等を装うなりすましメールであり、サプライチェーンを通じた標的型攻撃であった。

もはや外部から押し寄せるウイルスやマルウェアを事前にすべてはじくことは不可能。つねに何らかの攻撃を受ける可能性があるという前提に立って考えねばならない時代なのだ。そこでHP社は昨今、攻撃を受けた後にすみやかにウイルスを検出したり、自己復旧したりといった多層的な防御システムを組み込んだセキュアPCの開発と普及に取り組んでいる。なかでもPC本体のハードウェアから完全に隔離された仮想マシン内でウェブサイトの閲覧やドキュメントファイルの開封などを行い、本体への攻撃・侵入を防ぐ「HP Sure Click(HPシュアクリック)」は、検知に依存しない画期的な仕組みとして注目されている。そのあたりについては本誌20頁の対談記事に詳しく掲載されているので、ぜひご一読いただきたい。

サプライチェーン全体のセキュリティ対策が急務

こうしたさまざまなサイバー攻撃のリスクについて、国はどのような問題意識を持ち、いかに対策を打ち出そうとしているのだろうか。「ここ数年の傾向として、サプライチェーンの弱点を狙ったサイバー攻撃が顕在化・高度化している」と話すの

は、経済産業省商務情報政策局サイバーセキュリティ課の尾崎洸課長補佐。たとえば「大企業が海外の企業を買収して子会社をつくった場合、システム構成が違っているために本社のセキュリティ対策をすぐには子会社に導入できず、その隙をつかれて侵入されたり、大手メーカーが製品の設計図を下請けの中小企業に渡したところ、セキュリティが十分でないとこから外部に流出してしまったり」といったケースがみられるという。事実、2020年1月以降、三菱電機やNECなど、防衛省と取引関係にある企業が過去に高度なサイバー攻撃被害にあっていたことが明らかになったが、三菱電機の件では海外拠点のサーバーから不正アクセスを許したという経緯があった。「サイバー攻撃はもはや会社ごとに対策を整えるだけでは防ぎきれず、サプライチェーン全体を守らねばならない事態となっている」のだ。

こうしたなか、経済産業省はとくに中小企業におけるサイバーセキュリティ強化のための施策に注力、昨年1年間の実証事業として全国8地域1064社を対象に「サイバーセキュリティお助け隊」を展開した。これは各実証地域内において、損害保険会社やITベンダー、その他地元団体などの連携の下、中小企業にセキュリティ監視機器を設置し、サイバー攻撃が起こった際の駆け付け支援や簡易保険での対応を行う体制を構築するというもの。「まずは中小企業がどの程度、どういったサイバー攻撃を受けているか、また受ける可能性があるか、そのデータ収集もかねてこの事業に取り組んだところ、実証地域のほぼすべてでリスクにつながる事案が発生した」そうだ。具体的には、1年間で計910件のアラート（中小企業におけるサイバー攻撃リスクにつながる事案）が発生、そのうち「重大な事案の可能性あり」と判断し対処を行った件数は128件。特徴的な対応事例としては「マルウェア対策ソフト未導入の古いOSを使いつづけていたり、社員が出張先ホテルのWi—Fi環境で標的型攻撃メールでマルウェアに感染したり、取引先のメールサーバがハックされてメールアドレスが漏洩したりといったサイバー攻撃が確認された」とのこと。なかには「対処を怠った場合の被害想定額が5000万円近くになる」という試算も。

このように中小企業もサイバー攻撃の対象となっている実態があらためて浮き彫りになったこともあり、同省は今後も「サイバーセキュリティお助け隊」を継続しつつ、産業界をあげて中小企業におけるサイバーセキュリティ強化を促していくという。また、中小企業も使いやすいなど一定の水準を満たしたセキュリティサービスを「お助け隊サービス」として認定し、中小企業がそのサービスを利用している旨をマークを使って取引先などにアピールできる仕組みづくりなど、中小企業のサイバーセキュリティ対策の見える化にも取り組むという。「これまで、中小企業にとってセキュリティ対策といえば売り上げには直接結びつかないものであり、コスト意識から後回しにされがちだったが、今後は自社の付加価値・魅力として積極的に体制を整え、取引先や顧客にも積極的にアピールしていくべき」と尾崎課長補佐。1通のメールからはじまったサイバー攻撃が取引先にも被害をおよぼし、サプライチェーン全体を揺るがす可能性がある今、サイバーセキュリティ対策の不備は企業価値を大きく損なう要素となっている。これからは中小企業もサイバー攻撃リスクの当事者として、セキュリティ意識を高めていかなければならない。

経済産業省
中小企業サイバーセキュリティ対策促進事業
（2020年度補正予算額7.7億円）

経済産業省では2020年度の中小企業サイバーセキュリティ対策促進事業として、本文でも触れたサイバーセキュリティお助け隊事業（事後支援）のほか、登録セキスペ派遣事業（事前支援）にも取り組む。これは中小企業に情報処理安全確保支援士（登録セキスペ:全国約2万人）を派遣し、セキュリティ基本方針や関連規定の策定支援を行う事業だ。

また、日本各地域における「セキュリティコミュニティ」構築の動きも支援していく。地域単位で、地場企業のセキュリティ対策支援やセキュリティ情報共有を担うコミュニティが求められており、すでに関西地域では、経済産業局・総合通信局や民間団体が中心となったセキュリティコミュニティによる情報共有が進展しているという。

事例01

三菱重工ネットワーク不正アクセス事件に学ぶ ニューノーマルにおける セキュリティ対策のポイント

今年に入ってから発覚したサイバー攻撃事案のなかでも、コロナ禍におけるテレワークがキッカケとなったことで注目された三菱重工グループのネットワークへの不正アクセス事件。ニューノーマル型の新しい働き方や非接触ビジネスにおいては、この手のリスク対策が欠かせない。セキュリティ関連のプロフェッショナル集団である㈱ブロードに、そのポイントを聞いた。

三菱重工業の発表によれば、事の経緯としては4月29日、三菱重工グループ名古屋地区の従業員がテレワーク中に業務用モバイルパソコンから社内ネットワークを経由せずSNSを利用した際、ダウンロードしたファイルからマルウェアに感染。そして5月7日の出社時、そのパソコンを社内ネットワークに接続したことで、5月18日よりマルウェアの感染が内部ネットワークに拡大した。この不正アクセスを受けて、同グループの従業員の氏名やメールアドレスなどの個人情報のほか、通信パケット、サーバーのログ、設定情報などが流出したという。

㈱ブロードはこの件について「現在の企業向けのサイバーセキュリティ分野で頻繁に観測され、注意喚起されている代表的なサイバー攻撃パターンの組み合わせからなる事例だ」と指摘する。まずSNSでダウンロードしたファイルからマルウェアに入り込まれたのは「ソーシャルエンジニアリング」と呼ばれる手法で、高度な技術を使うのではなく「人間の心理的な隙や行動のミスに漬け込んで悪意あるファイルを開封させたり、URLをクリックさせたりするもの」だという。当然、従来のアンチウイルスソフトによる「検知」ではこうした攻撃は防ぎきれない。人の判断はつねに100%正しいとはかぎらないため、企業とテレワーカー自身のサイバーセキュリティリテラシーが問われるのだ。

また、被害にあったパソコンが社内ネットワークに接続されたのを機に、社内のほかのサーバーやパソコンにマルウェアが伝播したという点も見逃せない。「昨今のサイバー攻撃ではメールやウェブサイトの閲覧に使用するパソコンを足掛かりに、『より貴重な情報』を狙ってネットワークでつながるほかのIT資産へのアクセスを試みる例が多い」と。その伝播の仕方としては「主にサーバー管理者が使用する『特権アカウント』のIDやパスワードを悪用して機器から機器へと広がっていったと推察できる」という。なお発表によれば、三菱重工業では今後の予防策として特権アカウントのパスワードをすべて異なるものに変更したほか、業務用モバイル端末から外部ネットワークに接続する場合、強制的にVPN(※)経由で社内ネットワークを経由するよう変更したそうだ。

テレワークの浸透で、社外で個人が使用するパソコンがサイバー攻撃を受ける例は増加しており、その被害が会社全体、あるいはサプライチェーン全体にまで広がるリスクも高まっている。これまで以上に企業活動におけるセキュリティ体制を整えることが肝心だが、「こうしたサイバー攻撃の事案が持ち上がると、働き方に制約を設けたりしがちだが、それで業務効率や生産性を落としては元の子もない」とブロード。「だからこそ、企業はユーザーの利便性や自由を阻害しない、自由かつ安全なセキュリティ対策を模索しなければならない」と話している。

その点、本誌でも以前より取り上げ、ブロードが営業展開に注力している「Bromium(現・HP Sure Click Enterprise)」は、メールやSNSなどをパソコン本体とは隔離された仮想パソコンにおいて開くことで、本体の安全を確保するので安心だ(20頁にも関連記事を掲載)。また、同社では特権アクセス管理分野で世界的に高い評価を得ている米国BeyondTrust社の製品をベースに、安全と利便性を兼ね備えた特権アカウント(権限やパスワード)管理や安全なリモートアクセスについても提案できるという。

ニューノーマル型の新しい働き方や非接触ビジネスにおいては、こうした新しい発想のセキュリティツールが心強い味方となるはずだ。

※ VPN……ネット接続している利用者間に仮想のトンネルを構築し、プライベートなネットワークを拡張する技術

事例02

中小企業のテレワークにピッタリ 手軽かつ低コストなセキュリティアプリ

セキュリティの専門部署や人材がいない中小企業にとって、盤石なサイバーセキュリティ対策を整えるのは難しい。が、最近では手軽かつ低コストに導入できる現場目線のセキュリティソフトやアプリも多数開発されている。その一例として、トビラシステムズ㈱の「トビラフォン Cloud」を紹介したい。

「トビラフォン」は2011年、トビラシステムズ㈱がリリースした日本初の迷惑電話防止機器だ。その仕組みは、同社が独自にデータ収集・分析した迷惑電話番号リストをユーザー全体に共有することで、まだかかってきていない迷惑電話まで強力にブロックするというもの。明田篤社長によれば、この約10年、全国の警察の協力と利用者からの情報提供などで集まったデータ総数は延べ9億件以上。「常時、約3万件の悪質な迷惑電話番号のブラックリストを最新情報に更新しつづけている」そうだ。

「テクノロジーで社会課題を解決すること」を目指す明田社長

15年からはモバイルフォン向けに開発した同様の仕組みのモバイルアプリが大好評。「3大通信キャリアと提携し、各社のモバイルフォンのオプションパックとして採用されている」という。

そんな同社が今年3月末、あらたにクラウド型ビジネスフォンアプリ「トビラフォン Cloud」をリリース、企業によるテレワーク導入が急速にすすむなかで大いに注目を集めている。これは自前のスマホにインストールするだけで「050」からはじまるIP電話番号が付与され、すぐさまビジネスフォンの機能（内線・保留・転送など）を付与できるというアプリ。たんに番号を使い分けられるだけでなく、通話料は私用とは別途契約企業に請求がいくので経費区分を明確化できる。ほかにも通話が手軽に録音できたり、業務時間外に社用番号のほうにかかってきた電話のみ自動音声に切り替えられたりとさまざまな機能があり、「働き方や業態にあわせて快適かつ効率よくカスタマイズできる」のが特徴だ。

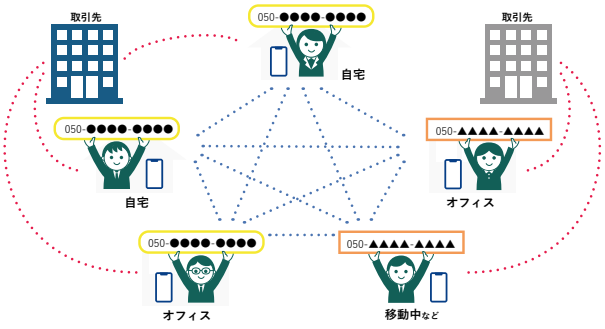
もちろん、セキュリティ面にもさまざまな工夫が凝らされている。自社開発のセキュリティシステムが組み込まれているほか、従来のモバイルサービス同様の迷惑電話フィルタ機能が付されているので、しつこい営業電話を防ぐことができる。また通常、自前のモバイルフォンを社用に使うと電話帳などにプライベートとビジネスの両方のデータが入るので、万が一端末を紛失したときに顧客データが流出してしまう恐れがあるが、「トビラフォン Cloud」なら心配ご無用。「すべてのビジネス関連のデータがクラウド上に保存されるので、紛失時はサーバアカウントを停止すれば流出を防げる」のだ。

これだけの機能がありながら、アプリ利用料は基本セット月額3000円＋通話料。「無料通話が2000円分ついているので、5台のモバイルフォンに内線番号を振り分けるとして、1台当たり200円」と低価格で導入できる。しかもウェブ上で申し込みが完結するため、最短で翌営業日から使えるのもうれしい。

リリース以降、利用者数は順調に伸びており、「テレワークを急いで導入しなければならず困っている」といった中小企業経営者のほか、税理士事務所や弁護士事務所、大企業からもチーム単位での利用などについての相談や問い合わせが相ついでいるそうだ。「セキュリティ専門人材のいない中小企業でも、気軽に低コストで導入できるのでぜひ検討してみてほしい」と明田社長。ニューノーマルにおけるサイバーセキュリティ対策、まず第一歩としてこうしたアプリの導入からはじめてみてはどうだろうか。

iPhone 版

Android 版



右上：2011年にリリースした日本初の迷惑電話防止機器、固定電話用の「トビラフォン」 左上：同社モバイルアプリの利用画面。迷惑電話番号の危険性をユーザーに知らせるだけでなく、約537万件のデータベースに登録された公共機関や店舗、企業、宅配事業者の携帯電話番号まで表示してくれる　下：トビラフォン Cloud利用例（利用者全員に外線番号を付与したケース）。振り分けられた番号をそれぞれが担当し、全スタッフ間は内線で連絡をとりあえる

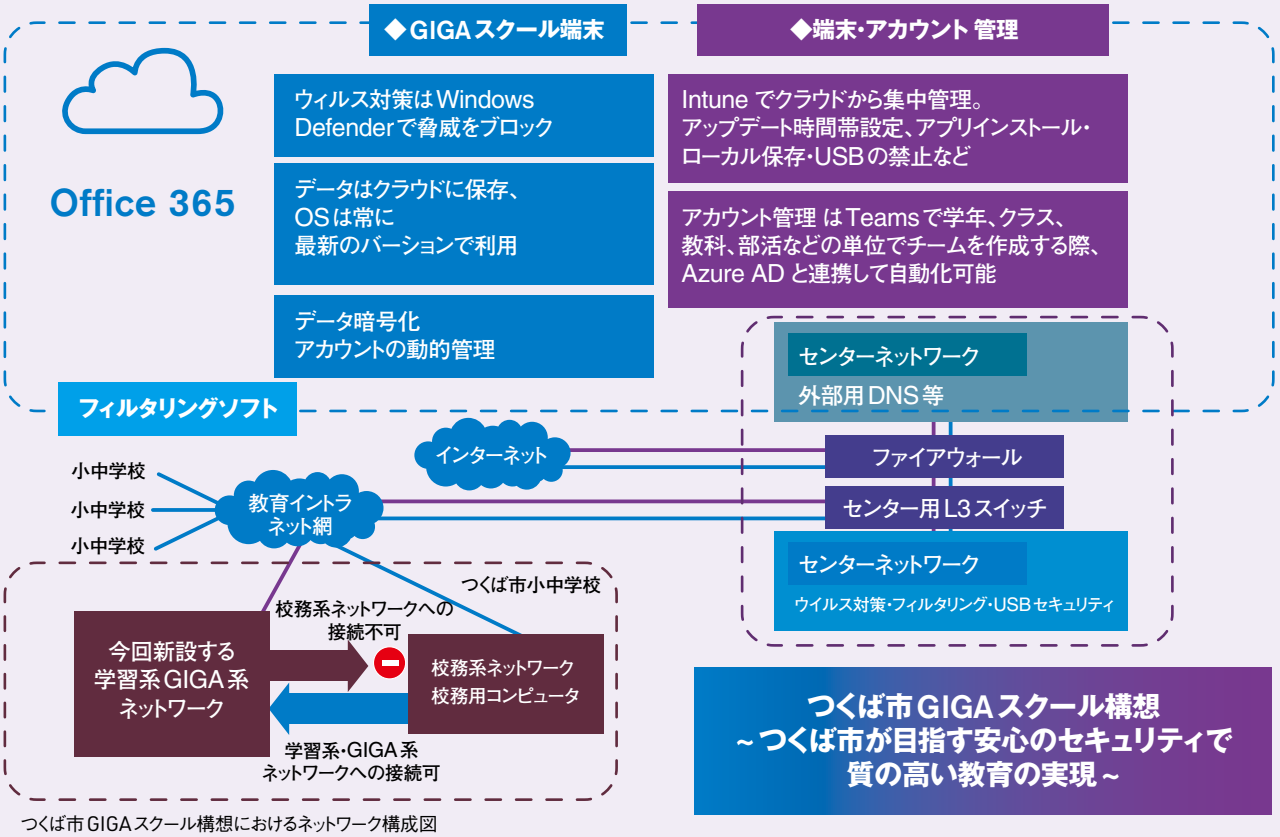
ICT教育の現場に欠かせない セキュリティモラルとリテラシー

全国の学校の高速・大容量通信環境整備と、全生徒への1人1台学習用端末配備を主軸に、政府主導ですすめられている「GIGAスクール構想」。ICT教育の普及による児童・生徒の学習効果に期待が高まる一方、不正アクセスなどのサイバー攻撃リスクを懸念する声も。はやい段階から地域の全小・中学校52校におけるICT教育を実践してきたつくば市に、これからのICT教育現場におけるセキュリティ対策やセキュリティリテラシー教育について聞いた。

つくば市総合教育研究所兼学び推進課情報担当指導主事の中村めぐみ氏によれば、同市では現在「通常登校時でも休校時でも教師・生徒双方向での問題解決学習と個別最適化学習を展開し、『誰一人取り残さない』教育を実現するため、学校内の学習支援ツールのクラウド型への仕様変更をすすめている」という。では、学習者用端末やすべてのデータを校内のサーバーで管理するオンプレミス方式（自家運用）からクラウド方式とすることで、サイバーセキュリティ対策上はどのような変化があるのだろうか。「当市では従来から、各校の学習者用端末に接続されたルータにフィルタリングや暗号化の仕組みを取り入れたり、校務用PCに複数のセキュリティソフトを導入したりと、不正アクセスなどの攻撃に備えてきた」と中村氏。今後も設計上、機械上のセキュリティを最大限にかけていくことに変わりはないが、「サイバー攻撃が多様化している今、すべてを防ぎきるのは不可能。だから、不正アクセスの可能性ありきで事前にリスクマネジメント体制を整えておくことが肝心だ」と話す。たとえば「学校関係者はあらかじめ、クラウドサービス（つくば市の場合は『Microsoft Azure（マイクロソフト アジュール）』）上で不正アクセスや情報漏洩の経路や方法、痕跡をたどる方法や知識をできるだけ備えておいたほうが望ましいし、情報漏洩時には、迅速に考えられる被害の大きさと広がりを見据え、第三者機関と連携して事態の収束をはかっていかねばならない」と。

そしてもう一点、中村氏はもっとも重要なポイントとして教師・生徒・保護者への「セキュリティリテラシー教育」をあげる。クラウド型のICT教育においては「教師と生徒たちがクラウドを介してインタラクティブ（双方向）に活動し、家庭学習の課題のアップロードや必要な資料のダウンロード、生徒同士で研究チームを立ち上げてのオンラインミーティングなどを柔軟に行う」ことで学習効果が上がる。だが、その自由度が高ければ高いほど、クラウドサービスを利用する側のリテラシーが問われることに。「生徒がデジタルポートフォリオ（個人の学習評価などのデータ）にむやみに顔写真や個人・家族情報をアップしてしまったり、オンラインミーティングでルールや作法を破ってトラブルに発展したり、他人のアカウントを面白半分で乗っ取ったり」と、モラルとリテラシーの欠如によるリスクは枚挙にいとまがない。「教師も生徒もその保護者も、こうしたリスクを回避するための考え方と情報管理能力をシッカリ身につけておくことが教育現場における一番のサイバーセキュリティ対策になる」と中村氏は力を込める。

つくば市では市独自の「情報教育単元」をつくっているほか、総合的学習の時間内にもセキュリティモラル・リテラシーを盛り込んでいるそうだが、これらは他地域においても必須だ。今後、全国的にGIGAスクール構想をすすめていくのであれば、政府はこうしたサイバー分野におけるリテラシー教育の推進にも注力すべきではないだろうか。



つくば市GIGAスクール構想におけるネットワーク構成図