大塚商会の販売最前線からお届けするセールスノウハウマガジン

BP Navigator

usiness artner

2020 Vol.109

巻頭特集

安心・安全なネットワーク環境の提案を目指す!

ネットワークセキュリティ入門!

巻頭インタビュー

キャリアシフト株式会社 代表取締役

森本 登志男氏

テレワーク導入は重要な経営戦略
意識を変革するような提案を

Presented by Otsuka Corporation

大塚商会の販売最前線からお届けするセールスノウハウマガジン

BP Navigator

usiness artner

2020 Vol.109

CONTENTS

第54回

ニッポンの
BP TOP INTERVIEW
元気人

各界の最前線で活躍する
オピニオンリーダーに
IT業界復活のヒントを聞く

キャリアシフト株式会社
代表取締役
森本 登志男氏

テレワーク導入は重要な経営戦略
意識を変革するような提案を

総務省委嘱テレワーク マネージャーを務め、『あなたのいるところが仕事場になる「経営」「ワークスタイル」「地域社会」が一変するテレワーク社会の到来』（大和書房刊）の著者でもあるキャリアシフト代表取締役の森本登志男さん。マイクロソフトでの職務経験が長く、佐賀県庁をはじめとする官公庁や、数多くの民間企業のテレワーク導入を支援してきた森本さんに、企業にとってのテレワーク導入の意義や、導入支援をするうえでのヒントについて聞いた。

2020年はテレワーク導入が本格化するターニングポイント

BP：森本さんは、2011年に佐賀県庁のCIO（Chief Information Officer：最高情報統括監）に就任され、全国に先駆けて全庁にテレワークを導入するなど、公務員組織の枠組みに一石を投じたそうですね。今日のように「働き方改革」が本格化するかなり以前から、テレワーク推進にかかわってこられたわけですが、これまでを振り返って、日本の官公庁や民間企業におけるテレワーク導入への取り組みは、どこまで進んできたとお感じになりますか。

森本登志男氏（以下、森本氏）：佐賀県でテレワークの導入が成果を上げたことがきっかけになっていると思うのですが、2016年の佐賀県庁の任期を終えた後、多くの都道府県庁からご相談を受け訪問させていただきましたが、18年で一巡した感があり、今は市町村での動きが活発になってきています。

市町村でも、佐賀県庁のような成果を上げる事例が出てくれば、テレワークの導入は加速するでしょう。

一方、民間企業では、早いところは東日本大震災のタイミングで導入が広がりました。その後、働き方改革が叫ばれるようになって次の導入の波が来ました。現時点で導入の端緒に立てていない大企業がまだまだ多く存在している反面、中堅・中小企業の一部には急速に導入の機運が広がってきているように感じています。

わたし自身、昨年（2019年）から、従業員50名前後の中小企業からテレワーク導入のご相談を受けるケースが非常に多くなりました。

それも、デスクワークがメインではない、製造や工事の現場がメインとなるような会社が積極的になってきています。

オフィスではなく、製造や工事の現場がメインの会社には、テレワークにはそぐわないのではないかと思われるかもしれませんが、どの会社にも間接部門は存在し、現場や出先で業務に当たる社員から発生する事務処理や顧客との契約、書類のやりとりなどの業務がオフィスで行われています。

ご承知のように、日本人の労働力人口は年々減り続けていますが、製造業や建設業は特に人手不足が深刻なので、テレワークによる柔軟な働き方の実現が求められているようです。そのような状況にもかかわらず、積極的にテレワークに取り組み、導入している一群と、まだ検討にすら至っていない一群との格差が広がっています。

2020年は企業のテレワーク導入が本格化する年
テレワークは社員への福利厚生ではなく重要な経営戦略である

BP：テレワーク導入への動きは格差が広がっているようですが、2020年は導入が加速する年になるとご覧になっていたそうですね。

森本氏：いくつかの大きな外部要因が重なって、テレワーク導入を進めざるをえなくなると見ていました。

一つは、何と言っても深刻な採用難です。人手不足の中で優秀な人材を一人でも多く確保するためには、柔軟な働き方が実現できる「魅力的な」環境を整えなければなりません。

先ほど、格差が広がっていると話しましたが、先行する企業はすでに何年も前から人手不足の深刻化を予見し、先手を打っていたわけです。

また、テレワークの大きなメリットは、わざわざ出社しなくても、自宅でオフィスにいるのと同じように仕事ができることですが、それを生かして業務の継続性を担保する重要性が高まっていることも、テレワークの普及を後押ししています。

今年は7月に東京オリンピック・パラリンピックが開催されますが、開催期間中、都心部の公共交通が混乱することが予想されるため、この期間になるべく出勤しないように事前に取り組みを始めましょう、と総務省など1府4省が2017年から「テレワークデイズ」を毎年展開してきました。

2019年4月から施行された働き方改革関連法が、2020年には中堅中小規模の事業者にも適用が拡大されます。そうしたタイミングが、2020年に一度に押し寄せます。さらに、ここ数年は大きな地震や台風などの自然災害が相次ぎ、交通など社会インフラの混乱によって、社員が出勤したくてもできないような状況が何度も訪れました。

そして、今年2月以降の新型コロナウイルスの感染拡大により、多くの企業で在宅勤務が行われるという状況まで生まれてきました。

「テレワーク無しに業務の継続は無理である」という認識を持たざるをえない環境が突然生まれてしまいました。これまでにテレワークの導入を着実に進めてきた企業と、テレワークの準備ができていないまま在宅勤務に突入せざるを得なかった企業には、この期間、大きな差が生じていると予想します。テレワークの用意を何もしていなかった会社が、突然の在宅勤務でまずやらなければならないことは、自宅からインターネットにつながることのできる情報端末(PCやタブレット)と回線、それにWeb会議ツールの準備です。課のメンバー全員が自宅からWeb会議につないで、現在抱えている仕事の確認と、在宅の環境でそれらをどうこなすかを話し合うことから始めてみてください。

事前予測を大幅に超える形で、テレワークの普及の波が訪れた2020年ですが、間違いなくテレワーク本格化のターニングポイントとなるでしょう。

制度変更を伴うことが導入を妨げる大きなネック

BP:テレワーク導入の格差が生じているというお話をされましたが、いまだに導入に踏み切れていない企業では、何がネックとなっているのでしょうか。

森本氏:中堅・中小企業は、いざやろうと決めたらスピーディーに実現することも可能なのですが、社員数の多い大企業の中には、なかなか導入に踏み切れないところが多いようですね。

理由はいくつかあるのですが、テレワークを実践するための情報システムの導入に加え、就業規則をはじめとする制度の変更を行う必要が生じてくる点と、情報セキュリティへの不安が大きいですね。

大企業の場合、制度の対象となる人数が膨大なだけでなく、業務のバリエーションも広いです。同じ会社でも、それぞれの部門や職種に合った働き方は異なるので、どうやったら不公平にならないようなルールづくりができるのか、ということを考えるだけでも大変です。

社員数が数十名程度の中小企業なら、部門間や社員同士の合意形成がしやすく、社長のトップダウンによって一気に導入まで進むケースもありますが、規模が大きいと、導入の方法や範囲を決定するための検討項目が多い上に、導入決定に向けての根回しや合意形成をするだけでも数カ月や数年かかってしまうことが珍しくありません。

その結果、小回りの利く企業はどんどんテレワークを推進しているのに、スピード感に劣る会社だけが取り残されてしまうといった状況に陥るのです。

BP:非常によくわかります。

森本氏:大企業の場合、テレワークでの業務を前提としたセキュリティ対策についても、結論に至るまでの時間とコストを要してしまう傾向にあるようです。

さらには、テレワークを始めると社員が出社しなくなるので、「ただでさえ足りていない人手がますます不足して、仕事が回らなくなってしまうのではないか」という誤解を抱いている企業も少なくありません。

人手が増えたわけではないのに、テレワークを導入することで、以前よりも効率よく仕事を回せるようになったという事例も多く存在しています。創意工夫や検討でより良い運用法を作り出すのか、検討の前段階で決めつけによる思考停止をしてしまうのか。これが先ほどお話しした格差のどちらに位置するかを分けているポイントです。

BP:そうした企業は、本誌の読者である大塚商会のパートナー企業さまにとって、テレワーク導入を提案する有効なターゲットになると思います。どうやって働き掛けたらよいでしょうか。

森本氏:テレワークはシステムを導入しただけでは、効果的な実践はできません。制度の変革も必要となりますし、「組織風土の醸成」という要素が必要です。

通常、大塚商会のパートナー企業さまが向き合っている得意先は情報システム部門でしょうが、テレワークの導入に関しては、総務・人事部門が意思決定に強く関わります。システムの提案だけでは、顧客の検討は進みにくく、人事制度も含めた包括的な提案を行う必要があります。最終的には経営層も視野に入れた提案活動が必要となります。

Present! 『あなたのいるところが仕事場になる』(大和書房刊)プレゼントのお知らせ!!

パートナー様の日頃のご愛顧に感謝を込めて、森本 登志男氏の著書『あなたのいるところが仕事場になる」(大和書房刊)を50名のパートナー様にプレゼントいたします。プレゼントをご希望されるパートナー様は、大塚商会の担当営業までお申し出ください。締め切りは2020年4月30日です。応募が多数の場合、抽選となりますので、ご了承ください。

テレワークは社員への福利厚生ではなく、重要な経営戦略の一環であるという理解を促さねばなりません。

なぜ、経営戦略としてテレワークに取り組むべきなのかと言えば、取り組まないことによって人材確保はますます困難となり、事業の存続が危ぶまれることになってしまうからです。

この先、テレワークを推進する企業がさらに増えていけば、それらの企業は自社の働きやすさを強烈にアピールして、人材獲得を優位に進めていくことでしょう。

そうなると、労働人口の減少がますます進む中で、テレワークを実践していない企業は人材獲得競争で不利な立場に追い込まれてしまいます。

2020年は、いよいよ企業のテレワーク導入が本格化するターニングポイントの年になると申し上げましたが、ここで出遅れると、人材獲得競争で大きく水を空けられてしまう恐れがあります。こうしたポイントは、顧客側の担当分野で言えば、情報システム部門ではなく、人事部門や経営層へのアプローチとなってきます。トップ同士での提案や、セミナーなどへの誘導といった方策も併せて検討すべきでしょう。

働き方改革関連法の適用で中小企業のニーズが高まる

BP:制度の変革を伴うことが、企業のテレワーク導入を妨げる大きなネックになっているというお話でしたが、読者が得意先に提案できるいい解決策があれば教えてください。

森本氏:あくまでもひとつのアイデアですが、育児や親の介護といった自己都合で退職した元社員の方にテレワークの仕組みを使って仕事復帰してもらうという方法もあると思います。

元社員の方の中から、限られた時間、在宅でなら働けるという方の復帰を促すのです。すでに経験のある仕事を頼むので、安心して任せられるというメリットもあります。

この方法のいいところは、業務委託契約に基づいて働いてもらい、全社的に就業規則などの制度を変更しなくても済む点です。試験的に導入してテレワークの効果や、セキュリティ面での課題などを検証し、制度やシステムを整備して本格的に全社導入するといったステップを踏むことができます。

「ひとまず、スモールスタートから始めてみませんか?」と提案してみてはどうでしょうか。

BP:最後に本誌読者にメッセージをお願いします。

森本氏:制度変更やセキュリティの問題など、課題が山積しているのでテレワークの導入に踏み切れないとあきらめている会社があまりにも多いようです。しかし、いま導入に踏み切らなければ、会社や事業の存続そのものが脅かされてしまいかねない状況なのですから、得意先にテレワーク導入を提案する際には、そのことをしっかり伝えたほうがいいですね。

また今年4月には、働き方改革関連法の施行スケジュールに沿って、中小企業にも残業時間の罰則付き上限規定や5日間の有給休暇取得の義務化が適用されます。中小企業のテレワークへの対応がますます必要になってきますので、積極的に提案を行ってみてはいかがでしょうか。BP

キャリアシフト株式会社
代表取締役
森本 登志男氏
MORIMOTO TOSHIO

◎Profile

岡山県出身。京都大学工学部卒業。マイクロソフトでの16年間の勤務(米国含む)を経て、2011年～5年間、佐賀県最高情報統括監(CIO)を務める。全国に先駆けて佐賀県庁職員約4000人を対象にした全庁テレワークを導入。ICTを活用した地域の課題解決を行い、「鹿島酒蔵ツーリズム®」(令和元年度ふるさとづくり大賞・最優秀賞(内閣総理大臣賞・総務大臣表彰))を起ち上げ、観光要素の発掘と磨き上げ、PRにおいても功績を収めた。現在は総務省委嘱地域情報化アドバイザー・同テレワークマネージャーとして、官民にわたり広範囲に全国各地で活躍。2019年ニセコで開催されたG20観光大臣サミットではモデレーターを務めた。

巻頭特集!!

安心・安全なネットワーク環境の提案を目指す!

ネットワークセキュリティ入門!

東京五輪の開催は、日本におけるセキュリティ対策への意識を高めています。また、外的な要因で必要に迫られているモバイルワークや在宅ワークでも、セキュリティ対策は必須の課題です。そこで今回の特集では、小規模オフィスから中堅中小企業で必要なセキュリティ対策への理解を深める知識を紹介します。次世代ファイアウォール、スイッチ、ルーターなどのネットワークに関するセキュリティ対策について、できるだけ簡単にお伝えします。

Check.1

ネットワークの入り口で不正アクセスから情報資産を守るゲートウェイセキュリティ

複雑化するサイバー攻撃から重要な情報資産を守るうえでは、インターネットとの接続点でネットワークを防御するゲートウェイセキュリティと、ネットワークに接続された情報端末を防御するエンドポイントセキュリティという二方向からの取り組みが大切だ。まずはゲートウェイセキュリティから具体的な対策を見ていきたい。

セキュリティの基本は防火壁による切り分け

現在、企業のネットワークセキュリティは大きく二つの方向から考えることができる。インターネットとローカルなネットワークの接点で通信情報の出入りを監視するゲートウェイセキュリティと社内の情報端末の保護を目的とするエンドポイントセキュリティである。マルウェア検知など双方の機能には重なる部分も多いが、それは決して無駄なことではない。一般的なアンチウイルスの併用は干渉などの弊害につながるが、入り口と端末における二重の検疫・防御態勢はセキュリティレベルの向上に確実に貢献するからだ。また、モバイルワーク・テレワーク普及に伴う、職種を越えたPC持ち出しの一般化も見落とせないポイントだ。エンドポイントセキュリティが注目される背後には、ネットワーク管理者の目が行き届かない持ち出し端末のセキュリティ担保という課題もある。

まずはゲートウェイセキュリティから見ていこう。その基本となるのが、インターネットとローカルなネットワーク領域の接続点に配置されるファイアウォールによる防御だ。その直訳は「防火壁」で、ネットワークセキュリティの分野ではあらかじめ設定したルールに従い、通信を制御する役割を担うことになる。

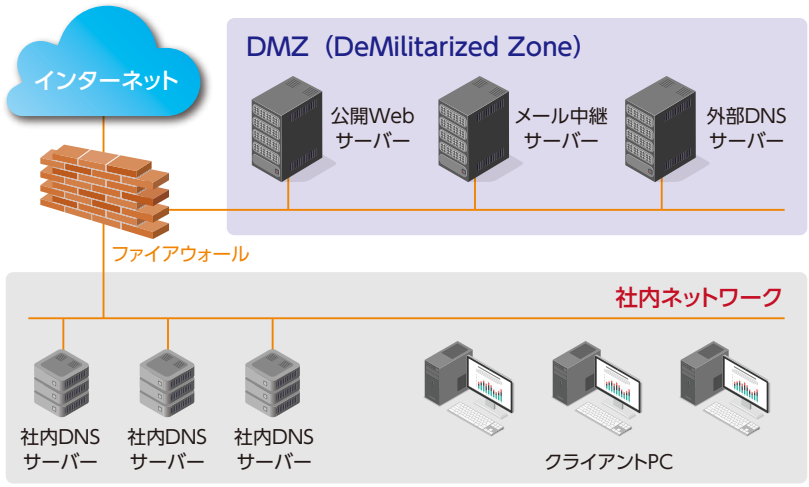
ファイアウォールの提供形態は、専用アプライアンスやルーターといったハードウェアのほかソフトウェアもあり多様だ。またインターネットとローカルネットワーク領域の中間に緩やかなルールが適用されるDMZ（Demilitarized Zone:非武装地帯）と呼ばれるセグメント（区域）を挟むことが一般的で、そこにWebサーバーなどの機器が配置される。

ファイアウォールによる通信制御でまず挙げられるのは、ポートの開閉による方法だ。ポートとはネットワークでデータをやり取りする際の扉のようなもので、メールを受け取る扉、Webページを見る扉などそれぞれ役割が割り振られている。そのため、特定のポートを閉じることで、例えば外部のWebブラウザーからネットワーク内の情報資産をのぞき見られる心配がなくなる。同様の機能はPCに実装されたファイアウォールにも備わっているが、ネットワークのファイアウォールの場合、さらに特定のIPアドレスからの接続可否もルールに加えることができる。

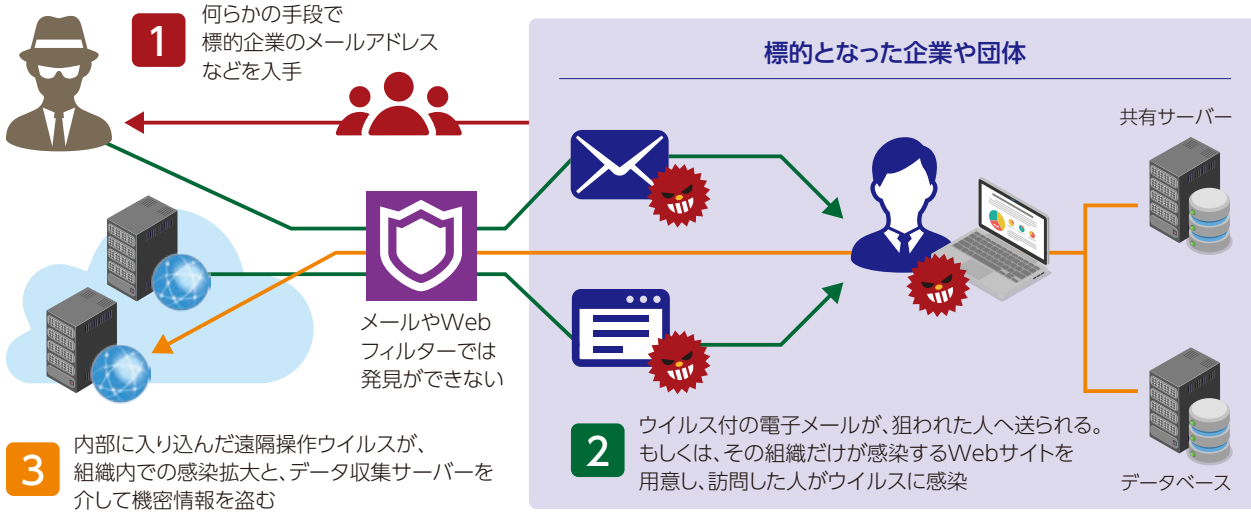
またファイアウォールは、グローバルIPアドレスとプライベートIPアドレスを変換する役割も担う。例えば外部のWebサイトにアクセスした端末のIPアドレスが外部に筒抜けになることを防止できる。

最小限の構成の場合、ファイアウォールにはこれらの機能が実装されていることが一般的だ。これによりネッ

ファイアウォールの基本的な考え方



標的型攻撃の一般的なシナリオ



トワークに一定の安全性は担保されるが、これだけでは、Webサイトに組み込まれたウイルスへの感染や、メール添付ファイルを装ったマルウェアによる攻撃を防御することはできない。そのため現在、ゲートウェイセキュリティにはさまざまな機能が登場している。

防火壁ではサイバー攻撃をブロックするのは困難

ここで簡単にサイバー攻撃について振り返っておこう。企業の情報資産を狙った攻撃としてまず挙げられるスパイウェアは、多くの場合、メール添付ファイルやインターネット上のダウンロードファイルを装ってエンドポイントに侵入する。そのあと、エンドポイントを拠点にネットワーク上の情報資産を収集し、攻撃サーバーに送信する。またボットウェアと呼ばれるウイルスに感染した端末は、DoS攻撃をはじめとする標的型攻撃の踏み台として悪用されることになる。

これらの脅威からローカルネットワークを守るゲートウェイセキュリティには以下のようなタイプがある。

●プロキシサーバー型ファイアウォール

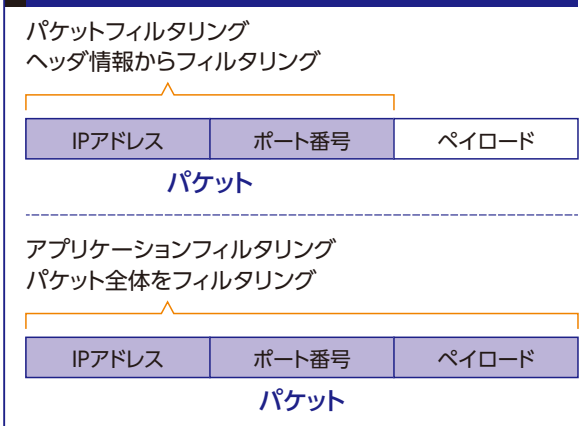
一般的なファイアウォールは、IPアドレスというパケット通信の送り状の部分を参照して通信情報の出入りをチェックする。それに対し、通信の中身まで検査して不正を発見、防止するのがプロキシサーバー型ファイアウォールだ。

この方法はアプリケーション型とも呼ばれ、例えば特定キーワードを設定しておくことで、内から外への情報漏えいやギャンブルサイトなど勤務中の閲覧が適切ではないWebサイトへのアクセスを制御することも可能になる。一方で検査対象のデータ読み込み量が増えるため、通信速度に影響が出やすいというデメリットもある。プロキシサーバー型の提案では、ネットワークのトラフィック量に見合った機器の選定が大切になるだろう。

進化したゲートウェイのセキュリティ対策とは

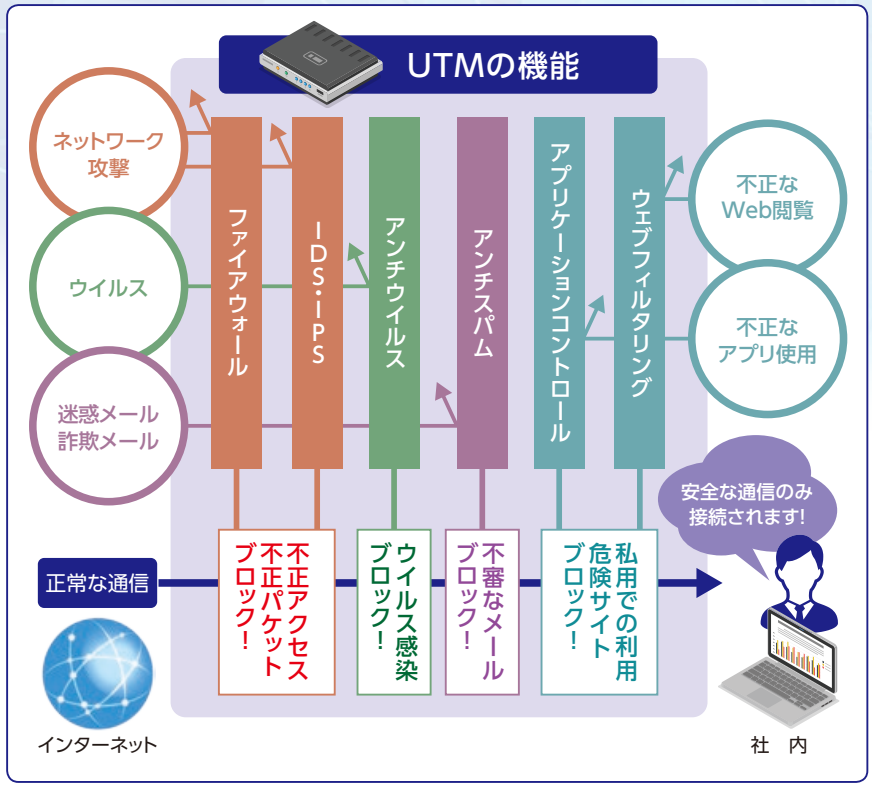
ファイアウォールだけではより高度化するサイバー攻撃からローカルネットワークを守るのは難しい。しかし高度な攻撃に対応する機能を個別にそろえようとすると、コストも管理の手間も大

2つのフィルタリング方法



※パケット通信においてパケットに含まれるヘッダなどの付加情報を除いた本体データをペイロード(payload)と呼ぶ。

きなものになる。こうした中注目されているのが、ゲートウェイセキュリティに関連する高度な機能を一台のきょう体に統合したUTM(Unified Threat Management:統合脅威管理)だ。その主な機能を見ていこう。



●IPS/IDS

IDS(Intrusion Detection System:不正侵入検知システム)は、外から内に入る情報通信をリアルタイムで監視し、不正なアクセスを検知した際は管理者に通知する。検知には大きく二つの方法がある。一つは事前登録した不正なアクセスパターンに基づく「シグネチャ型」、もう一つは正常なパターンに合致しないアクセスをピックアップする「アノマリ型」だ。前者は未知の脅威への対応は困難だが、後者は未知の脅威にも対応するというメリットの一方、誤検知も多くなるというデメリットを持つ。

IDSが不正侵入を検知・通知するだけなのに対し、遮断というアクションまで伴うのがIPS(Intrusion Prevention System:不正侵入防止システム)だ。検知後のタイムラグが発生しないというメリットの一方、誤検知のリスクはより大きなものになる。

またIPS/IDSは、内から外の情報通信の監視も行う。そのため、侵入したスパイウェアによる情報資産の持ち出しを水際で検知してブロックすることも可能になる。

●未知のウイルス対策(サンドボックス)

ゲートウェイであれ、エンドポイントであれ、ウイルス検知はデータベースを参照して行うのが一般的だ。シグネチャ型と呼ばれるこの方法は、新種ウイルスを検知することは不可能だ。この問題を解決するのが、隔離された仮想環境でプログラムを実行し、振る舞いを検査する「サンドボックス」と呼ばれる方法だ。

ただしこの方法も万全ではない。サンドボックスでの分析は時間が掛かるため、検査はファイルのコピーで行うのが一般的だ。その第一の理由は分析完了前に、エンドポイントに到達したマルウェアが活動を開始する可能性があることだ。また、一定時間を経て活動を開始するマルウェアの検知は難しいという課題もある。

●感染端末遮断ソリューション

UTMの中には、IT資産管理やネットワークスイッチと連携し、ウイルスに感染したエンドポイントを隔離する機能を備える製品もある。ローカルネットワーク上のエンドポイントからサーバーなどへの不審なアクセスや外部への不信な通信を検知し、端末をネットワークから遮断することが基本的な考え方になる。

●Webコンテンツフィルタリング

インターネット上には、ギャンブルサイトやポルノサイトのように業務中のアクセスが不適切なサイトのほか、個人情報の収集やマルウェアのダウンロードを目的とするサイトが存在する。Webコンテンツフィルタリングは、一定のポリシーに基づき、不適切なサイトへのアクセスを制限することで、組織の生産性を高め、より高度なセキュリティを実現する。SNS投稿による情報漏えい防止という観点から、この機能に注目する企業も多い。

●アンチボットネット

標的型攻撃の踏み台としての悪用を目的としたボットウェアに感染したPCは、動作の不安定化や処理速度の低下といった影響が現れるが、見かけからその判断を下すのは難しい。アンチボットネットは、通信ログ分析を通し、ボットウェアへの感染を発見し、C&Cサーバーと呼ばれる外部サーバーとの通信やDoS攻撃をシャットアウトする。

そのほかUTMはアンチスパム、IPsec-VPN、SSL-VPNなどの機能を備えることが一般的だ。

Check.2

アンチウイルスだけではない。情報端末を多角的に保護するエンドポイントセキュリティ

ネットワークと情報資産を確実に保護するうえで、ゲートウェイと共に注目したいのがエンドポイントのセキュリティ対策だ。エンドポイントセキュリティは、従来のアンチウイルスを中軸にした新たなセキュリティ対策で、多様な機能を統合し、エンドポイントの情報機器をサイバー攻撃などのリスクからガードする。

新種ウイルスにも対応 次世代アンチウイルスとは

エンドポイントセキュリティにおいて中心的な役割を担うのは、アンチウイルス機能であることは昔も今も変わりない。アンチウイルスを中軸に、総合的な観点から、情報端末と情報資産を守ることがその基本的な考え方になる。

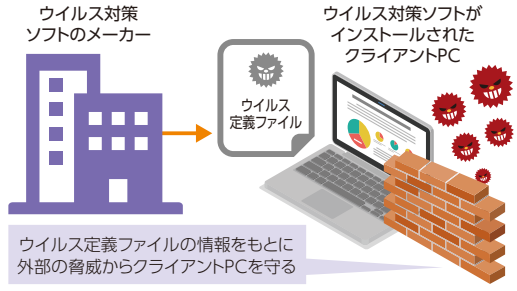
アンチウイルス製品ベンダー各社が総合的なエンドポイント防御に取り組む背景の一つに、Windows 10に標準搭載されるWindows Defenderの存在があることは間違いない。これまでウイルス検知は、ベンダー各社が独自に構築したウイルス定義データベースに基づくシグネチャ方式が一般的だっただけに、膨大なWindowsデバイスのリアルタイム情報が反映されたウイルス定義データベースを持つWindows Defenderの登場が、従来のアンチウイルス製品に大きなインパクトを与えたことは否定できない。

その一方で、自動生成される新種マルウェアや、ぜい弱性が発見されて修正プログラムが提供されるまでの短い期間にぜい弱性を攻略するゼロデイ攻撃など、シグネチャ型では防御が困難な攻撃も増えている。こうした中、AIを活用した次世代アンチウイルスや、情報端末の振る舞いを監視してマルウェア感染を検知するEDRなどの最新技術の組み合わせを通しエンドポイントを防御するというのがエンドポイントセキュリティ製品の基本的な考え方になる。

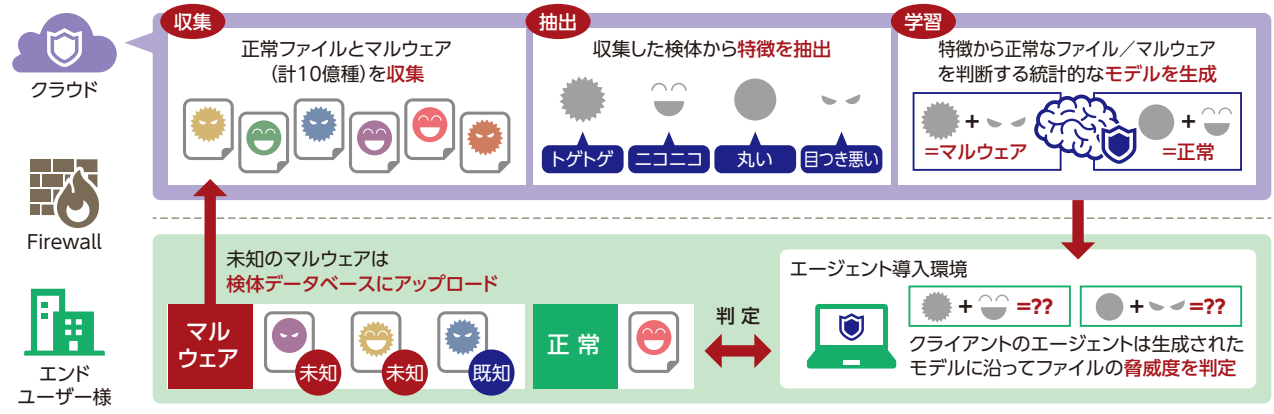
また従来はWindows Defenderとサードパーティ製アンチウイルスの併用は困難だったが、現在は『MVISION Protect Standard』(マカフィー)のようにWindows Defenderと連携し、その機能を補完するアンチウイルスも登場している。

従来のアンチウイルスに加え、エンドポイントセキュリティ製品が提供する機

シグネチャ検知の考え方



EDR の対応範囲 イメージ



能には以下のようなものがある。

●次世代アンチウイルス

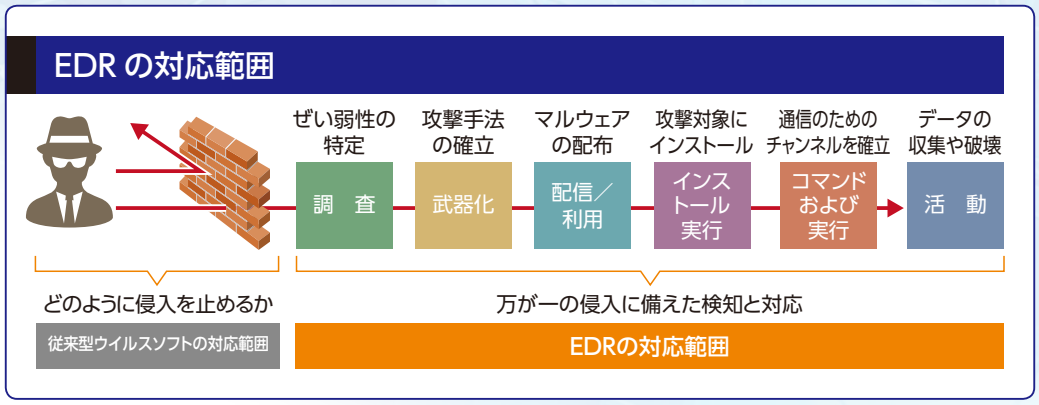
シグネチャに基づくウイルス検知は、誤検知が少ないというメリットを持つ一方、脅威の種類が増えるとそれに応じて参照するシグネチャファイルも大きくなり動作に時間が掛かるようになる、これまで発見されていない新たな脅威には対応できないというデメリットも持つ。

AIや機械学習などの最新テクノロジーを活用してファイルを精査し、シグネチャに頼ることなく既知および未知の脅威からエンドポイントを保護するのが次世代アンチウイルス(NGAV:Next Generation Anti-Virus)だ。未知の脅威に対応できる一方、実運用では誤防御への対応や一定のチューニングが必要になる点に注意が必要だ。

●EDR(検知と対処)

これまでエンドポイントセキュリティは、情報端末へのマルウェアの侵入を食い止めることに力を注いできた。それに対し、情報端末の振る舞いの監視を通してマルウェアの侵入を検知し、侵入後の対応を迅速に行うことを目的とするのがEDR(Endpoint Detection and Response:検知と対処)と呼ばれる機能だ。

EDR製品には管理者が感染端末にコンソール経由でアクセスし、調査のための情報収集やマルウェアの隔離・削除や復旧をリモートで行う機能が備わっているものがある。マルウェアの侵入を許した際の情報漏えいの有無、影響範囲などの可視化は、特に大企業の情報システム部門で大きな役割を果たすと考えられている。



●HDD暗号化

PC持ち出しの一般化に伴い、新たに生じたのがPC盗難・紛失時のデータ保護の観点だ。その対策としてまず挙げられるのが、ハードディスク内のデータを暗号化することで、第三者による不正な読み出しを困難にするHDD暗号化だ。Windows 10に標準搭載されるドライブ暗号化機能「BitLocker」のほか、多様なサードパーティ製品が提供されている。

●デバイスコントロール

マルウェアの侵入経路として考えられるのはインターネットだけではない。USBメモリーをはじめとする、ユーザーがエンドポイントに接続する外部デバイスも重要な侵入経路の一つだ。所定のルールに従い、エンドポイントのデバイス接続を制御するのがデバイスコントロールと呼ばれる機能になる。

外部要因だけではない情報資産漏えいリスク

さらに言うと、ローカルネットワークの情報資産を確実に守るうえでは、外部からの侵入者やマルウェア対策だけでは不十分だ。機密情報の漏えいの多くは、従業員による持ち出しが原因であることがその理由だ。また不用意なSNS投稿により機密情報や個人情報が流出するケースもある。

その対策として挙げられるのがActive Directoryによるアクセス制限だが、それ以外に機密情報の動きを監視することで漏えいを防止するという方法論もある。DLP(Data Loss Prevention)は、ネットワーク接続端末内の機密情報の所在を常時監視し、あらかじめ設定したポリシーに基づき、重要データの外部送信やUSBメモリーへの書き込みの際にアラートを出すほか、操作をブロックするソリューション。それにより外部からのサイバー攻撃だけでなく、内部要因による情報漏えいに対しても確実に対応することが可能になる。内部要因による不正の抑制という観点では、エンドポイントのログ監視ツールも有効だ。

また働き方改革に伴うテレワークの普及は、ローカルネットワークだけにとどまらないセキュリティ対策が強く求められることにもつながっている。拠点間や社外のエンドポイントとローカルネットワークを結ぶVPNはその一例である。スマートフォンやタブレットなどのモバイルデバイスの場合、MDM(Mobile Device Management:モバイルデバイス管理)もエンドポイントセキュリティの重要な要素の一つになる。ドライブを暗号化し、盗難・紛失時にはそのデータをリモートで消去できるMDMは、モバイルデバイスのセキュアな運用を実現するうえで不可欠な存在になっている。

Check.3

エンドポイントセキュリティの選び方

セキュリティへの考え方に見合ったソリューションを提案したい

これまでマルウェア検知は、ウイルス定義データベースに基づいて行われることが一般的だった。しかしサイバー攻撃の進化に伴い、その限界も明らかになりつつある。こうした状況を受け、新たに登場したのが「次世代アンチウイルス(NGAV)」と呼ばれる新技術だ。その方法論は各社それぞれ異なるが、AIによる機械学習を通し、未知の脅威に対抗するというのがその基本的な考え方になる。

一方、エンドポイントへの侵入を許した脅威をいち早く検知し、対応策を図る役割を担うのがEDRだ。現時点ではNGAVは極めて高い防御力を誇っ

初歩から上級者向け鉄壁の防御まで ネットワークセキュリティメニュー一覧

⬅ introduce

Plan.1

モバイルデバイス管理(MDM)
1ライセンス500円(月額)～

Plan.2

アンチウイルス製品
1ライセンス980円(月額)～

データバックアップ
月額1000円(1ユーザー)～

Plan.3

エンドポイントセキュリティ
1ライセンス2000円(月額)～

メールアーカイブソフト
月額2000円(1ライセンス)～

Webフィルタリングソフト
1ライセンス1万円(年額)～

情報セキュリティ教育(eラーニング)
1名5000円～

ネットワークと情報資産を確実に保護するうえで、ゲートウェイと共に注目したいのがエンドポイントのセキュリティ対策だ。エンドポイントセキュリティは、従来のアンチウイルスを中軸にした新たなセキュリティ対策で、多様な機能を統合し、エンドポイントの情報機器をサイバー攻撃などのリスクからガードする。

ているが、攻撃者が何らかの抜け道を見つける可能性は否定できない。そのため、アンチウイルスとEDRの組み合わせは、情報端末と情報資産を確実に守るうえで大きな意味を持つ。

ゲートウェイのIPS/IDSがネットワークに流れる通信を監視するのに対し、エンドポイントのIPS/IDSは端末に入ってくる通信の監視が主な役割になるため、併用により二重の監視体制が整うことになる。

またデバイスコントロールは、USBメモリーをはじめとする外部デバイス接続を管理する機能。エンドポイントを起点にしたサイバー攻撃を防ぐうえで重要な役割を担う。セキュリティに対するエンドユーザー様の考え方に応じ、最適な提案を心掛けたい。BP

月額500円のモバイルデバイス管理からUTMアプライアンス製品やプロキシサーバー立ち上げまで、ネットワークセキュリティに関する商材は数多い。また今回の記事では触れなかったが、データを人質に身代金を要求するランサムウェア攻撃に対しては、LTOなどによるネットワークから隔離された形のデータバックアップが効果的だ。また内部要因による情報漏えいという観点ではデータリークプロテクションやIT資産管理による操作ログ取得も重要なポイントになる。エンドユーザー様のセキュリティに対する考え方や予算感に応じて商材を組み合わせ、最適な提案を行いたい。

highend ➡

Plan.4

- サーバーセキュリティソフト
  1台2万円(年額)～
- セキュリティスイッチ
  1台2万円～
- データバックアップ(クラウド)
  1TB 5万円(月額)～

Plan.5

- 法人向けVPNソフト
  10万円(年額)～
- VPNアプライアンス
  10万円～
- サーバーバックアップソフト
  10万円(1年)～
- ファイアウォール(アプライアンス)
  10万円～
- バックアップ用NAS
  10万円
- データリークプロテクション
  10万円(年額)～

Plan.6

- LTO装置
  60万円～
- Active Directoryサーバー
  100万円～
- IT資産管理アプライアンス
  50万円～
- サンドボックス専用製品
  100万円(年額)～

IT Keyword
最新ITキーワード

2025年の崖
【2025 cliff】

経済産業省が2018年に発表した『DXレポート ～ITシステム「2025年の崖」克服とDXの本格的な展開～』が今改めて注目されている。日本企業のデジタルトランスフォーメーション(DX)への取り組みの遅れに警鐘を鳴らす同レポートにおいて、「2025年の崖」という言葉で表現される弊害は、実は我々が常日頃、目にしている基幹システムの課題にほかならない。

エンジニアが自嘲交じりに口にする言葉の一つに、“秘伝のタレ”がある。東京の老舗うなぎ屋の中には、江戸時代からつぎ足しつぎ足し使ってきたというタレが自慢の名店がある。しかしこの場合、継ぎ足されるのは必要に応じて書き足されてきたソースコードだけに始末が悪い。その結果、旨いのか不味いのかもよく分からないが、変更を加えると何が起こるのか分からないため放置するほかないシステムが生まれることになる。

実際のところ、長く企業で稼働する業務システムの中には、「なぜこんな機能があるのかだれも分からない」「どんなプログラムが動いているのかよく分からない」といった、“秘伝のタレ”化したレガシーシステムは少なくない。その第一の課題は、運用コストの増大だ。ある調査では、システムの老朽化、複雑化によるシステム障害で生じる経済損失を年間4兆円におよんでいるという。

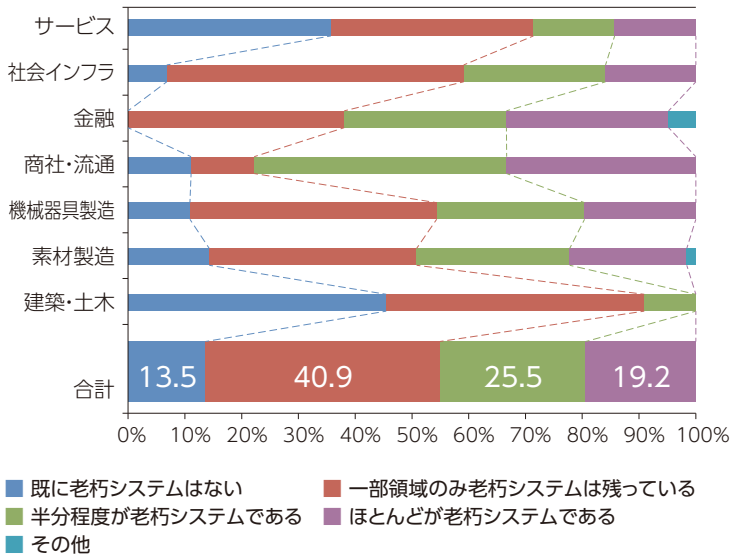
ITの力で製品やサービス、ビジネスモデルを改革するDXが大きな注目を集める中、日本企業の取り組みの遅れを指摘する声は多い。その最大の要因は、“秘伝のタレ”化したレガシーシステムにある。それこそが「2025年の崖」の本質だ。

DXの基盤となるシステムの全面的な見直し、刷新には巨額のコストが必要になる。だがある調査によると、日本企業のIT

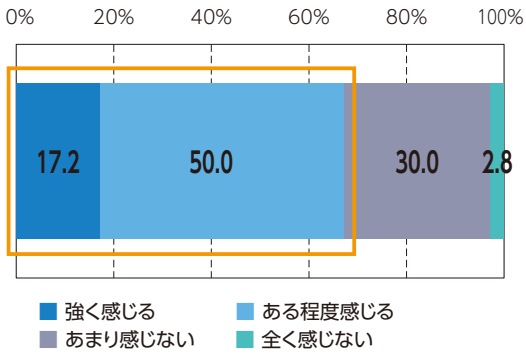
『DXレポート ～ITシステム「2025年の崖」克服とDXの本格的な展開～』より

●既存システムの現状と課題

約8割の企業が老朽システムを抱えている



約7割の企業が、老朽システムが、DXの足かせになっていると感じている



出典：一般社団法人日本情報システム・ユーザー協会「デジタル化の進展に対する意識調査」(平成29年)を基に作成

関連予算の80%は現行システムの維持に費やされているという。そこから浮かび上がるのが、レガシーシステムの維持に四苦八苦し、新たな一手を打ち出せない日本企業の姿だ。

2015年時点で基幹系システムが20年以上稼働する企業の割合は20%。仮に現状のまま運用を続けたとするとその割合は2025年には60%に及ぶ。それによる経済損失は年間12兆円に及ぶとDXレポートは推定する。

日本企業の多くは、1980～1990年代に世界に先駆けてコンピュータを経営に導入し、大きな成果を挙げた。それがなぜ、このような事態に陥ったのだろうか。レポートでは大きく二つの理由を指摘する。

一つは、エンジニアの所属先がユーザー企業ではなく、ベンダー企業に偏っているという日本特有の事情である。ベンダーによる受託開発を前提とした人材の割り振りは、ユーザーにITシステムのノウハウが蓄積されにくい構造につながるからだ。またこの構造は、ベンダー企業によるエンジニア確保の困難さにもつながる。確かに、最新テクノロジーを学んだエンジニアにとり、秘伝のタレと揶揄されるレガシーシステムのお守りは苦痛でしかないはずだ。

もう一つが、1980年代以降、大規模なシステム開発を手掛けてきた人材の引退である。継ぎ足しにより属人化したシステムを知るエンジニアの退職は、システムのブラックボックス化に直結する。1982年に22歳でキャリアをスタートしたエンジニアは今年60歳。今の状態が続く限り、ブラックボックス化するシステムは今後急速に増え続けることは間違いない。

「2025年の崖」という言葉が広がった背後には、ERPシステムのデファクトスタンダードであるSAP ERPが2025年に保守期限切れを迎えるという事情もある。だがここまで見てきた通り、その言葉が示す課題は2025年に限られたものではない。

DXレポートはDX実現シナリオとして、2020年までにシステム刷新の経営判断を行うと共に、2021～2025年をシステム刷新集中期間（DXファースト期間）とし、計画的なシステム刷新を進めるというロードマップを提案する。必ずしもそのスケジュールに従う必要はないが、多くの企業にとり、“秘伝のタレ”化したレガシーシステムの刷新が急務の課題であることは間違いないだろう。BP

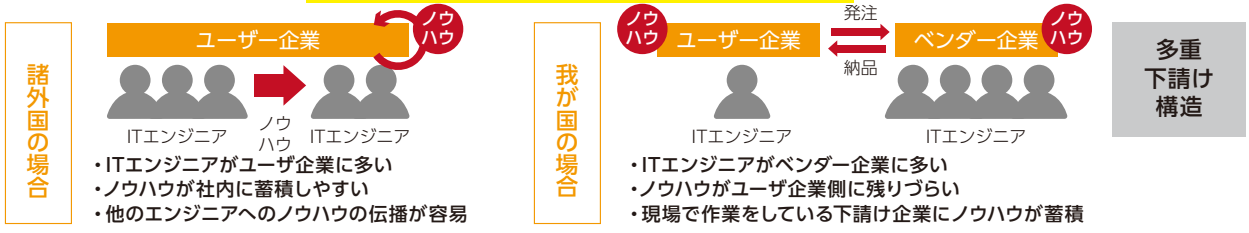
●既存システムの問題点の背景

▸ 事業部ごとの最適化を優先し、全社最適に向けたデータ利活用が困難に

各事業の個別最適化を優先し**システムが複雑となり、企業全体での情報管理・データ管理が困難に。**

▸ ユーザ企業とベンダー企業の関係がレガシー化の一因

我が国では、ユーザ企業よりも**ベンダー企業の方にITエンジニアの多くが所属している。**



▸ 有識者の退職等によるノウハウの喪失

国内企業では、大規模なシステム開発を行ってきた**人材の定年退職の時期（2007年）が過ぎ、人材に属していたノウハウが失われ、**システムのブラックボックス化が進展している。

▸ 業務に合わせたスクラッチ開発多用によるブラックボックス化

国内には**スクラッチ開発**や汎用パッケージでも**カスタマイズを好む**ユーザ企業が多い。このため、**個々のシステムに独自ノウハウが存在**するようになってしまう。何らかの理由でこれが**消失したときにブラックボックス**化してしまう。

出典：DXに向けた研究会一般社団法人日本情報システム・ユーザー協会説明資料を基に作成

Possibility of IT basic technology

進化するIT基礎技術の可能性

text by 石井英男
1970年生まれ。ハードウェアや携帯電話などのモバイル系の記事を得意とし、IT系雑誌やWebのコラムなどで活躍するフリーライター。

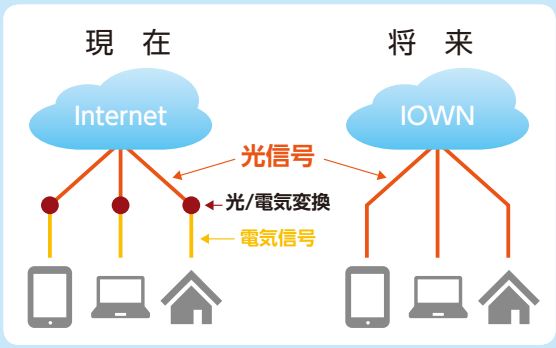
NTTが実現を目指すオールフォトニクス・ネットワーク「IOWN」とは?

今回のコラムは、ここ2、3年で実用化されるものではないが、夢のある次世代技術を取り上げたい。2019年10月31日、NTTがインテル、ソニーと共同で業界団体「IOWN Global Forum」の設立を発表した。IOWN(アイオン)とは、Innovative Optical and Wireless Networkの略で、NTTが2030年頃の実用化を目指して推進しているオールフォトニクス・ネットワークに基づく次世代ネットワーク基盤の構想である。オールフォトニクス・ネットワークとは、その名の通り、ネットワークから端末までエンドツーエンドで全てを光化したネットワークである。光ファイバーでは、同時に波長が異なる光を伝送することができるが、IOWNでは、機能ごとに別の波長を割り当て、端末やサーバー内は光のまま演算をおこなう光プロセッサを使うという構想だ。IOWNのキモは、全て光で処理をおこなうということである。現在でも、インターネットの基幹ネットワークとしては光ファイバーによる光通信が利用されており、フレッツ光のように、自宅やオフィスまで光ファイバーを引くFTTHサービスも普及している。しかし、現在のインターネットでは、端末の直前までは光通信でも、端末側では直接光通信をおこなえないので、電気信号に変換する必要があり、端末で演算や処理をおこなった結果は、再び電気信号から光信号に変換する必要がある。IOWNでは、光信号のまま処理をおこなうことにより、光信号と電気信号の変換処理が不要になるため、消費電力やレイテンシを大きく削減できる。

NTTは、このオールフォトニクス・ネットワークでは、従来のネットワークに比べて、電力効率100倍、伝送容量125倍、エンドツーエンドでの遅延を1/200にするという目標を掲げている。現在のIT社会は、電子技術であるエレクトロニクスを基盤としているが、IOWNでは、光技術であるフォトニクスの世界へとシフトすることになる。もちろん、その実現は容易なことではない。インテルも以前から、シリコンフォトニクス(シリコンを用いたフォトニクス技術)に関する研究開発をおこなっており、2016年6月には、100Gbpsの通信に対応したシリコンフォトニクス光トランシーバーの出荷を開始している。しかし、光で演算をおこなう光プロセッサに関しては、まだ研究レベルにとどまっており、量産はされていない。まずは、完全に光だけで演算をおこなう光プロセッサではなく、メニーコアCMOSチップ内のコア間を光で結び、チップ内で光信号処理をおこなう光電融合型チップが開発されることになるだろう。

IOWN Global Forumの設立の狙いは、IOWNの実現に向けた研究開発の加速と、IOWNが実現する世界観の普及の促進である。オープンなフォーラムであり、海外、国内を問わず、多くの企業にメンバーになってもらいたいと、NTTの担当者はコメントしている。また、NTTの隅田社長は11月13日におこなわれた講演で、65社がIOWN Global Forumへの参加を検討していることを明らかにした。その中には、マイクロソフトやベライゾン、オレンジ、中華電信など、大手IT企業や各国を代表する通信事業者が名を連ねており、IOWNへの期待が大きいことがうかがわれる。

IOWNの実用化には、まだいくつも超えなくてはならない技術的ハードルがあるため、あと10年での実用化はかなり難しいと筆者は考えているが、限界が見えつつある現在のインターネットの閉塞感を打破するための有望な構想といえるだろう。BP



NTTが開発した超小型O-E-O変換素子。光信号を電気信号に変え、再び光信号に変えることで、光信号の波長変換が可能。IOWNの実現には、こうした技術のさらなる進化が必要になる