「ITC が理解すべきコロナ環境下でのゼロトラストセキュリティ」
～DX を推進する為に必要なこと～

２０２１年3月３１日

企業内 ITC・IT ガバナンス研究会

序

新型コロナウィルス感染症の拡大に伴う外出自粛などの影響でテレワークの導入が進む中、サイバーセキュリティ上の対策として「ゼロトラストセキュリティ」に注目が集まっている。

概念としては決して新しいものではなく、「何も信頼できない」という前提のもとに、外部・内部を問わずネットワーク上のすべてのアクセスを制御するというコンセプトのセキュリティ対策として、Forrester Research 社が 2010 年に提唱した考え方である。

近年ではサイバー攻撃の手口も高度化・多様化しており、目的の企業を直接攻撃するのではなく、セキュリティの甘い関連企業を踏み台にしてネットワークに侵入し、間接的に目的の企業を攻撃する手法もある。　このため、従来の考え方である「境界型セキュリティ」だと間違いなく打つ手が足りなくなっている。

私共「企業内ITC・ITガバナンス研究会」としては、ITコーディネータ諸兄が理解しておくべき、次代のサイバーセキュリティ上の対策を、このゼロトラストの考え方「すべての通信を信頼しない(なにも信頼できない)」こととして、今後ゼロトラストへの適応が必要となってくることを前提として、各企業(主に中堅・中小)のセキュリティポリシーの見直し、それに伴うネットワーク構成や接続機器等々を再検討することや、NGAV（Next Generation Anti-Virus）製品やEDR（Endpoint Detection and Response）製品の導入・運用を考えることで、ゼロトラストについて展開、提言もして行きたい。

クラウドサービスの活用や、テレワーク導入によりゼロトラストでのセキュリティ対策が広まっている時代に在って、クラウドサービスも安心して利用できる(メリット)が、ランニングコストがかかり過ぎる(デメリット)と言われるこの概念を、整理致したい。

２０２１年3月
執筆者　一同

執筆メンバー　ITガバナンス研究会
久住　昭之(元 IT ｺｰﾃﾞｨﾈｰﾀ)
坂本　徳明(0064952006C)
瀬戸　昭彦(0065252006C)
滝沢　　康 (0012552001C)
千枝　和行(0029302004C)
古川　正紀(0005462001C)
牧田　一雄(元 IT ｺｰﾃﾞｨﾈｰﾀ)
山﨑　直和(0035252003C)

0. はじめに

働き方改革や新型コロナウィルス感染症拡大防止のため、テレワークで働く人が増えてきている。

テレワークでは、オフィスから離れた場所から働くということもあって、テレワーク導入に伴いクラウドサービスの利用も従来以上に増えてきた。

しかし、新しい働き方や新しいサービスを導入するに当たっては、課題となるのがセキュリティであり、従来のセキュリティ対策では、もはや社内システムや機密情報を守ることが困難になってきているため、新しいセキュリティ対策としての「ゼロトラスト」に注目が集まっている。

序章でも述べさせて頂いたが、この「ゼロトラスト」の概念は決して新しいものではなく、時節柄この概念が今にフィットしたのであろう。

ゼロトラストは、「全て信頼しない」という考え方から、セキュリティ対策を行う。

外部はもちろん、内部からのアクセスであっても、全てを疑い制御することになる。テレワークは、会社の端末を外部(自宅等)に持ち出して社内システムにアクセスするので、社内ネットワークと社外の境界線が曖昧になるため、従来のセキュリティ対策では運用できなくなるのである。

近年、外部からのサイバー攻撃による情報漏えいだけではなく内部の不正により、情報漏えいしてしまう事件が多発しており、そのため境界線内にある社内ネットワークの管理や監視の重要性が増している。

ゼロトラストネットワークでは、社内ネットワークは安全であるという考えを捨て、社外ネットワークに対するアクセスと、社内ネットワークで起こるトラフィックをすべて検査することになる。サーバーや情報資産など全てのアクセスに対して、セキュリティレベルをチェックし、それらが安全かどうか、適切な通信がされているかなどで、従来の考え方にとらわれないセキュリティを実現させなければならない。

ゼロトラストを採用する最も大きなメリットが、「クラウドサービスも安心して利用できる」ということにある。境界線を設けないため、クラウドサービスだけではなく、社内環境も、ゼロトラストでは有効に機能する。ここがゼロトラストのメリットといえる。

但し、「全てを信頼しない」ということは、社内から外部へのアクセス制限や添付ファイルの禁止などのセキュリティ対策を行うことも起こりうる。つまりひとつひとつのアクセスを認証しなければならないため、業務上は利便性が悪くなってしまう場合も覚悟しなければならない。

クラウドサービスの活用や、テレワーク導入によりゼロトラストでのセキュリティ対策

が広まるのは時代の趨勢であろう。働く場所がオフィスだけにとどまらず、アクセス元やアクセス先が社外になるのであるから、社内と社外の境界線だけをセキュリティ対策しても意味をなさない。

全てを信用せずにアクセス制限を設けるゼロトラストは、今後セキュリティ対策として適応することが必須と心得るべきである。

しかしながら、ITコーディネータがご支援する中堅・中小企業に置かれては、セキュリティ対策に掛けられる経費には大きな制約があるのも事実であろう。

そこで本論文では、中堅・中小企業のゼロトラスト対応について展開、妥当であろう提言をして行きたいと考えている。

１．ＩＴコーディネータが理解しておくべきafterコロナと企業・個人の働き方の変化

2019年末に中国湖北省・武漢で流行が確認された新型コロナウィルスは、当初、中国政府が秘匿していたこともあり、その対応が後手に回り、年明けの感染拡大を防ぐことが出来ず、スペイン風邪以来の未曾有のパンデミック（世界的大流行）となった。

この新型ウィルスの感染防止の為には、人と人とが接触することが感染源となる為、ソーシャルディスタンスが必要となり、極力外出を控えて感染拡大を防止することが国民の義務となった。

その影響は企業にも及び、特に人との接点が重要な流通・小売業、エンタテーメントなどは業務停止が長期間続き、倒産する企業も出るなど、影響は深刻化している。それに合わせて、企業は好むと好まざるとにかかわらず、新たな業務スタイルの導入を実行せざるを得ない状況に置かれることとなった、

多くの大手企業は出社をすることが出来ない為、仕事（作業）をテレワークで行うこととなり、会議もリモートで行われることがスタンダードとして広まっていった。

この様な遠隔で業務を行ったり、遠方と会議を行ったりするような業務形態は以前から存在していて、以下の様な発展をたどることになる。

・1980年代後期　：　電子メールや担当者間でのチャットを行うアプリの利用
・1990年代前期　：　インターネットの学術研究利用
・1990年代中期　：　営業担当者のリモートでの営業報告
・1990年代中期　：　専用線によるテレビ会議システム利用
・2000年代全期　：　クラウドサービス利用

先進企業にとっては、最近話題になっているような取り組みをいち早く進めていたので、特に目新しくは感じていない。

ところが、冒頭に述べたようなソーシャルディスタンスが必要になると、出社して業務を行う業務スタイルが困難になり、先進企業と言えど、従来の対象者を拡大して全社的にリモートシステムで業務を行う必要に迫られて、システム的な対応が取れる大手企業は順次対応していった。

しかし、中小企業の大半はその様なシステムを持っている企業は少なく、経済産業省・中小企業庁が推奨してきたDX化にも取り組んでこなかった企業は、従来通りの出社による業務形態を続けざるを得ない状況である。この問題を解決したいとは考えているが、どの様に構築したらよいかが分からず、当惑しているというケースが多いのではないだろうか。特にシステム担当者も置いていない企業は手が付けられていない状況の様である。

その一方で、中小企業でも気の利いた個人レベルの従業員間では、スマホを使ったSkypeやLine等の利用が普通に行われている。これらのToolは、所属している組織体の対応とは独立に進んでいく事もあり得ので、一種の「ねじれ現象」が密かに進んでいく事に経営者が気付かない可能性も起こり得る。

一方、働き方については、すでに安倍政権で働き方改革が提唱され、その検討結果が報告されている。その中で、次世代の働き方の基本形が論じられており、今回のコロナ過で

嫌が上でも注目せざるを得ない状況になっている。

この様な状況下において、リモート業務推進や、それに伴う組織の在り方、働き方の在り方、人事評価方法、情報セキュリティ等の在り方について、論じてみたい。

1-1. 企業は変革を迫られている

コロナ過により働き方の変革を迫られているように見えるが、日本では既に製造業の伸び悩みなどから、企業形態や働き方の変革が迫られていたが、コロナ過がそれを加速しているだけである。しかも問答無用で進んできている。

経済産業省は2020年1月に、「持続的な企業価値の向上と人的資本に関する研究会」を立ち上げ６回に及ぶ討議の末、2020年9月に報告書を取りまとめた。(座長：一橋大学大学院経営管理研究科 特任教授　伊藤 邦雄氏)

座長の伊藤氏はその中で、「コロナ禍は、「常識」を疑い、「慣性」に抗い、大きな変化のムーブメントを起こす好機でもある。これからは、人的資本の価値を最大限に引き出す方向に創造的かつ柔軟に変われる企業と、そうでない企業との間には、埋めがたいほどの企業力の差が生ずるだろう。」と述べている。この報告書の主な骨子は次のとおりである。

第１章：持続的な企業価値の向上と人的資本

新型コロナウィルス感染症への対応等の足下の状況も踏まえつつ、第四次産業革命などによる産業構造の変化、個人のキャリア観の変化など、企業・個人を取り巻く環境が大きな変化を迎えていることを踏まえ、今後のアクションの羅針盤となる変革の方向性を示している。

第２章：経営陣、取締役会、投資家が果たすべき役割

第1章での変革をリードする経営陣、経営陣を監督・モニタリングする取締役会、経営陣と対話を行う投資家について、それぞれが果たすことが期待される役割やアクションについて整理している。

第３章：人材戦略に求められる３つの視点と５つの共通要素

経営陣が主導して策定・実行する人材戦略について、経営戦略と連動した人材戦略について、上記の3つの視点（Perspectives)、5つの共通要素（Common Factors）を、3P・5Fモデルとして、整理して示したものである。

経済産業省は続いて2020年3月に、「変革の時代における人材競争力強化のための９つの提言」を取りまとめて公表した。その中で、３つのポイントを上げ解説している。

✓日本企業を取り巻く課題

グローバル競争の激化、デジタル化の進展によって、日本企業は急速かつ激しい変化にさらされている。さらに、日本では少子高齢化が急速にすすみ、人手不足が一層深刻化していく。既に「ゲームのルール」は変わっており、これま

での「勝ち筋」は通用しない。変革への対応力が求められる。

✓日本型人材マネジメントのアップデート

日本企業は、長期安定雇用による高い集団的能力を発揮し、経営競争力を強化してきたが、経営を取り巻く環境が不断に変化していく社会においては、その優位性が相対的に低下している。多様な個人が活躍し、変革に対応する経営を実現するために、経営トップ自らが率先して、人材マネジメントのアップデートや組織文化の改革に、スピード感を持って取り組まなければならない。

✓経営トップからステークホルダーへの積極的な発信と建設的な対話

競争力の源泉は「人材」であり、人材戦略は経営戦略の中心に位置づけられることを、経営トップは再確認し、具体的なアクションに繋げていくことが求められる。特に、経営トップは、従業員、資本市場、労働市場等のステークホルダーに対し、人材戦略を積極的に「見える化」し、建設的な対話を図っていく必要がある。

コアとなるビジネス業態の変化、人口動態やそこで働く人々の構成の変化があり、企業の、特に経営者はそれに合わせて人材戦略の根本的な変化が必要であることを説いている。従来のビジネスモデルや組織・人材対策が時代にそぐわなくなってきているのである。しかも、これらは、世界同時的に進行していることで、何も手を打たないと、取り残されてしまうと警鐘を鳴らしている。

1-2. 全日空・みずほ銀行が教えるもの

日本を代表する大手企業から衝撃の発表があった。全日空は従業員に対し「減給」を行うと発表し、みずほ銀行は「週３日の出勤」にすると発表した。

全日空の場合、パンデミックにより、航空機が全く運行できない状況が続いており、前年比で5,100億円のマイナスになると発表した。当然このままでは会社は成り立たなくなるので、従業員の「減給」に話が及んだのであるが、その意味するものは、取りあえず解雇はしないので、不足する収入は他の業務を行って補填してくれ、というものである。そして、2020年10月の時点で、KDDIに２８名、家電量販店のNojimaに５名、Pasonaに４名、スーパーの成城石井に数名出向させると発表した。また、三重県・鳥取県も数名を職員として採用する意向を示している。

企業としては副業若しくは複数企業への勤務を認める、仕事はJOB型業務形態に変えていくと説明している。人材政策を変更することで、企業として改革するとともに、業態も変えていくという事である。

みずほ銀行も同様であり、商社の丸紅も人材戦略を大幅に改革すると発表している。

これら企業の対応は、元々火種としてあったものが現実化したもので、ICTやAIの活用とは別にafterコロナの時代の趨勢として広まっていくものと考えられる。

（この項は、2020年10月時点で執筆した）。

1-3.　企業も個人もポートフォリオを作成し適切なリスク分散が必要

最近のキーワードとして、SDGsやESG投資に代表されるような「持続的な企業価値の向上」が重要視されるようになってきている。

人材面から持続的な企業価値の向上を考えた時に必要なことは、ビジネスモデル、経営戦略と人材戦略が連動していることが不可欠であることである。それも自社内だけに閉じたものではなく、その取り組みが内外のステークホルダーに理解されるものでなければならない。現状の問題の一つは、人事部門が戦略上の重要な部門とみなされていない企業が多いことである。

一時ベストセラーとなった「内側から見た富士通」では、「人事評価として適材適所や能力開発、能力主義などと看板を掲げていても、それを真っ当に受け入れる企業文化が出来てはいない。現実には学歴・学閥に依存した５段階評価で人事評価を行っていて、人事改革などは現実的ではない。」と主張している（筆者の意訳）。たぶん、怖くてできないものと思われる。能力主義は外国企業の様には企業文化として根付いておらず、従業員の間にも文化として受け入れられていない。ここが、最大の問題点である。

現在は、事業スピード、製品サイクルの短命化、グローバル化が一昔前よりいっそう進んできており、自社の経営方針と関係なく、世の中は動いている。それに順応するには経営者の自覚が重要である、という認識が浸透されている必要がある。

「第４次産業革命」に代表されるように、業務形態としてはハードウェアを作って売るよりは、ソフトウェアで儲けのもとを開発するような柔軟に対応していく事が重要な企業戦略になりつつある。当然、コアとなる従業員のスキルが変化せざるを得ず、社内で調達できなければ、労働市場でこれらの人材を確保する必要に迫られる。企業変革を行うには、必要スキルと現状スキルのギャップを埋める戦略を推進していかなければならないのである。

一方、従業員側から傾向を見てみた場合、「変革の時代における人材競争力強化のための９つの提言」では以下の様な調査結果を記載している。

・４０歳以下の労働者では、将来自分のやりたかった仕事に就きたい

・そのためには、今の会社というよりは多くの選択肢を持ちたい

つまり、若い老労働者の傾向としては、自分がやりた仕事とをしていくというのが傾向で、一昔前と比べ大きく意識が変化してきている。現在では心理学が発達し、カウンセリング技術も上がっていて、自分の楽しいと感じる仕事でないと、業績を上げることが出来ないという事が分かっていて、心理にかなった行動を選ぶようになっていくと考えられる。

企業としては、必要とされる人材のAsIsとToBeのスキルギャップを埋めていくプラン作成が出来るか、多様な個人が活躍する人材ポートフォリオを描いて継続できるかが重要で、従業員エンゲージメントだけではなく、労働市場とのエンゲージメント能力も必要となってくる。

現状の企業では、都合の良い従業員だけで構成されているわけではなく、必要な能力を確保するためには従業員に対する再教育（リスキル形成）が必要になってくる。そして、継続的キャリア形成が出来るようなキャリアパス形成の援助を行う必要がある。個人の多様性を活かせる業務設計、すなわちJOB型による明確な業務定義に基づいた業務設計が出来るかどうかも重要になってくる。

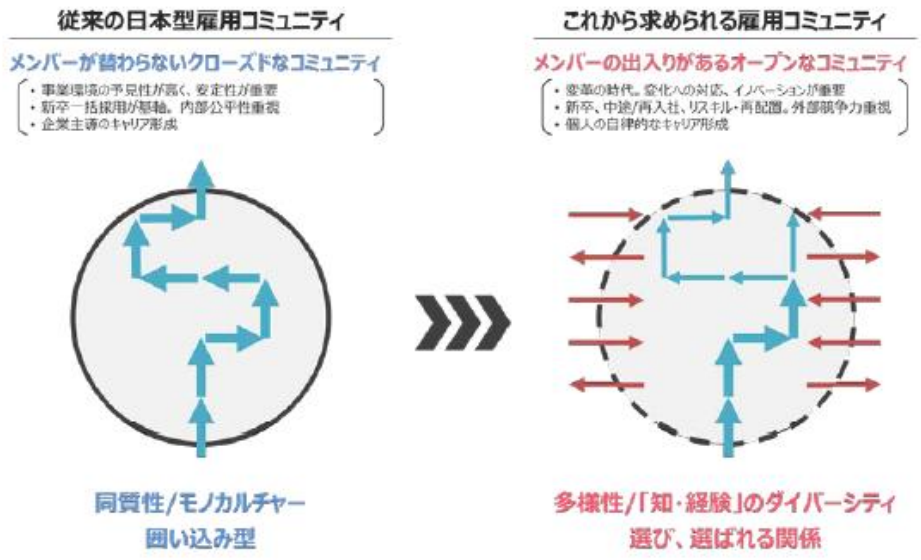
以上のように、最近の従業員は時間や場所にとらわれない働き方を望むような人が増加してきており、採用したら１人の従業員にいろいろな担当をさせるのではなく、特定の業務に対して欧米型のJOB型業務の推進を受け入れる環境と文化形成が必要になっていく。その事により、企業も個人も、必要とされる業務を進めていく事が可能となっていく。

1-4. 人材ポートフォリオはセキュリティ的には大問題

人材ポートフォリオを作成し、それに基づいてそこで働いている従業員や市場とのエンゲージメントを進めていくと、個人は得意分野を伸ばせるが、組織的には多様な従業員の集団とならざるを得ない。しかも、自社以外の異なる会社に勤務している、若しくは異なる会社からの異動・異なる会社への異動が起きてくる。

従って、従来の日本型コミュニティの様に閉じたものではなく、外部に開かれた複合型のコミュニティに変化していく事を意味している。

図表６：求められる雇用コミュニティの変化（イメージ）



（「持続的な企業価値の向上と人的資本に関する研究会」の16ページより引用）

これは、セキュリティ管理上は大問題である。自社に閉じている場合は、所属と職務・職位により、セキュリティを個別に付与して社内情報システムにアクセスして運用することが出来る。所属や職位が変わる場合、夜間バッチでセキュリティ変更を行い、変更後は旧組織の情報に一切アクセスできない出来なくすることで、セキュリテ

ィは守られる。しかし、企業をまたいで業務をするとなるとセキュリティが守られない危険にさらされる。

これを回避するためには、セキュリティ教育を行うとともに、欧米企業の様に従業員との間で「情報セキュリティに関する契約」を結んで、一定の歯止めをかける必要がある。それだけで安全という事ではないが、歯止めをかけると同時に、アクセス範囲を明確にし、情報漏洩の事故が発生したとしても必要最低限になるよう、ダメージコントロールを仕組みとして組み込んでおく必要がある。

これらの対応は、従来も行われてきているが、より明確にデザイン設計と運用を進める必要があることを示している。

1-5. オンライン化が進んでいない中小企業のＩＴ化や働き方はどうなる

前節までで述べた通り、事業のイノベーション創出の主流がハードウェアからソフトウェアへのパラダイムシフト、労働人口構成の変化、企業の人材ポートフォリオの構築（囲い込みから選択人事へ）、働き方改革と個人の能力発揮の機会の到来（協調から個人の創造性発揮）などが進行していて、大手企業はその対応を避けて通れない状況である。

一方、中小企業、特にオンライン化が進んでいない企業は、急激な社会変化とは無縁の業務スタイルで、コロナ過でも大手企業のテレワーク率は９０％以上なのに対して、中小企業では３０％あまりで、この数字が如実に物語っている。

一般に、中小企業がIT化を進めようと考えた時、IT化の比率が低いもしくは無いと、どこから手を付けたらいいか分からない。IT化を検討する前に、自社の業務フローや情報の流れを整理し、何を問題にしなければならないかを洗い出して把握しておく必要がある。これをやらないで、業務アプリの導入だけ進めると、思うような効果を上げることはできない。

基本的命題、何のためにIT化を進めるのか。それは、ITによって業務の機械化が出来る部分はITに任せ、考える時間を生み出して、本来やらなければならない業務の改革や改善にエネルギーを注ぐためである。

驚くことに、中小企業ではいまだに企業間連絡にFAXを使っている会社がある。個人がスマホのアプリを使う時代では、とても考えられない。それは、セキュリティ対策などと同様に心理学でいうヒューリスティックな対応で、他社の動向次第で決めたがるためと考えられる。今後人手不足になっていくわけで、電子メールや他の情報伝達手段に置き換えて合理化と情報の使い勝手向上を図る必要がある。

漁業関連など、６次産業化や企業連携が進んでいる事業体は、１社だけの取り組みでは効果が薄く、集団的な取り組みが必要となる。

下請け会社は、当然のことながら、親会社の意向に振り回されてしまう。

企業規模があまり大きくない場合、コスト的に１社では無理な場合は、組合化等の連携主体の取り組みが必要となる。場合によっては、ITC協会が、支援コンソーシア

ムを作り、ITCが支援するような取り組みを行ってもいいと考える。

一方、働き方に関しては、中小企業の従業員は一つの仕事に集中などは出来なくて、複数の業務を同時進行的に担うのが普通である。大企業の様に、自分のやりたい仕事に集中するなどは、資源的・環境的に困難な場合が多い。また、企業の事情での人員配置が多く、本人の意思が通りにくい風土が形成されている。中小企業の経営側から見ると、従業員に教育研修を施して高い技術を身に付けると条件の良い会社に転職してしまって定着してくれないので、どこまで育成していくのかは答えの無い難しい問題である。

1-6. 働き方とそれに関連する事象はどうなる

テレワークによる働き方への変化は、

・東日本大震災で働く場所が物理的に無くなったために実施した
・東日本大震災に基づく省エネ化を要求されたために実施した
・BCPとして、本来の場所以外での労働のために実施した

などの原因があり、少しずつ実施されてきていた。これがこの度のコロナ過により、必然として大企業を中心にリアル業務のオンライン化が急激に広まってしまった。この結果、出社する従業員が激減したので、都会のオフィスビルを削減、若しくは廃止をする企業が、大手だけではなく中規模企業にも出始めている。これらの減少は一過性ではなく、長期に継続される可能性がある。

テレワークが定着すると、今まで行われてきたリアル業務とテレワーク化すべき業務の切り分け、そのための人事評価制度はそれに合わせて変更させる必要が出てくる。テレワークは万能ではないので、よく考えて業務の切り分けを行う必要がある。リアル業務が絶対に必要となる業務を例示してみる。

・人間関係の面で必要	営業、カウンセリングなど
・能力が低いので介添えが必要	医療、介護、保育、低学年の教育など
・実際に人手が必要	建築土木、流通、機器搬入設置、修繕など
・機械化できない	大型船の造船、宮大工など

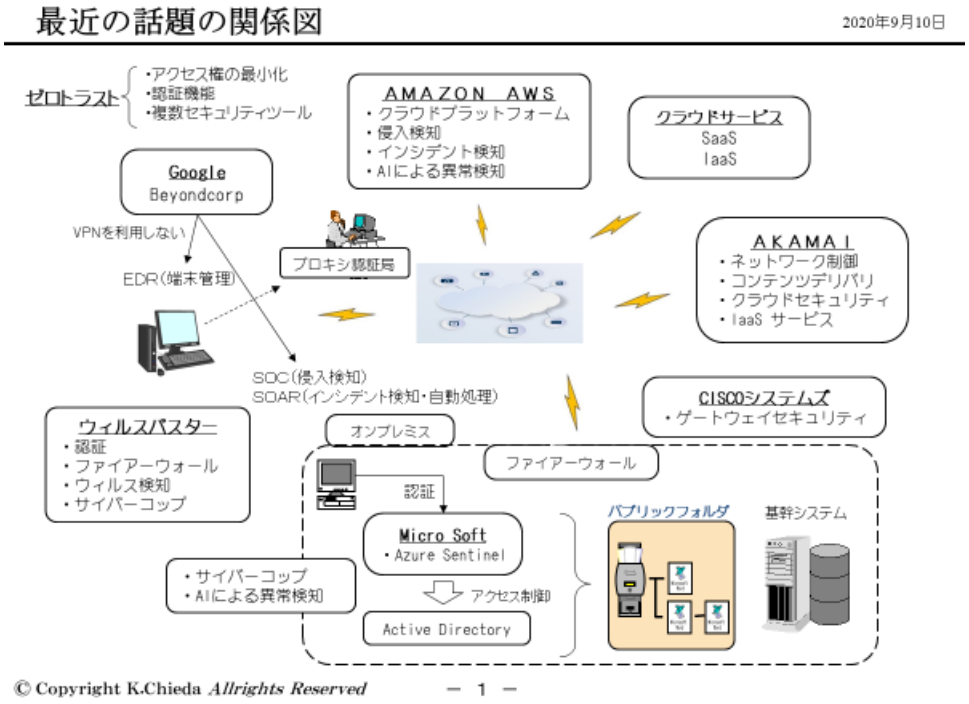
1-7. テレワーク化した場合の情報セキュリティ対応

テレワークは柔軟な働き方ができるので、それが望ましい労働者にとって大きなメリットがあるし、教育研修などはオンラインでできるので、利用しやすくなる。反面、結果や成果をどのように評価するのか、教育効果も適している人と適していない人がいるのでフォローをどうするのか、などの今まで体系的に制度として持っていない部分の体系化が必要になる。

オンライン化のもう一つの問題は、ネットワーク経由の侵入や、なりすましの問題をどのように対策するのか等の、防衛的機能を強化する必要が出てくることである。

・セキュリティポリシーの見直し

・オンラインに接続する機器の把握
・オンライン接続する機器への防御措置
・アクセス者の認証
・アクセス権と利用範囲の明確化
・企業システムへの侵入防止対策
・侵入検知と駆除アプリ
・クラウド利用の場合のプロキシ認証局の設置
・情報漏洩した場合のステークホルダーへの周知方法と内容
・侵入による破壊・情報漏洩に対する保険の準備



これらは、情報システム部門だけの問題ではなく、企業を上げて強化していかなければならない機能である。しかも企業規模や予算規模と関係なく必要となる機能で、中小企業と言えど出来る範囲から実行していかなければならない要素である。

参考資料：

持続的な企業価値の向上と人的資本に関する研究会報告書（経済産業省）

変革の時代における人材競争力強化のための９つの提言（経済産業省）

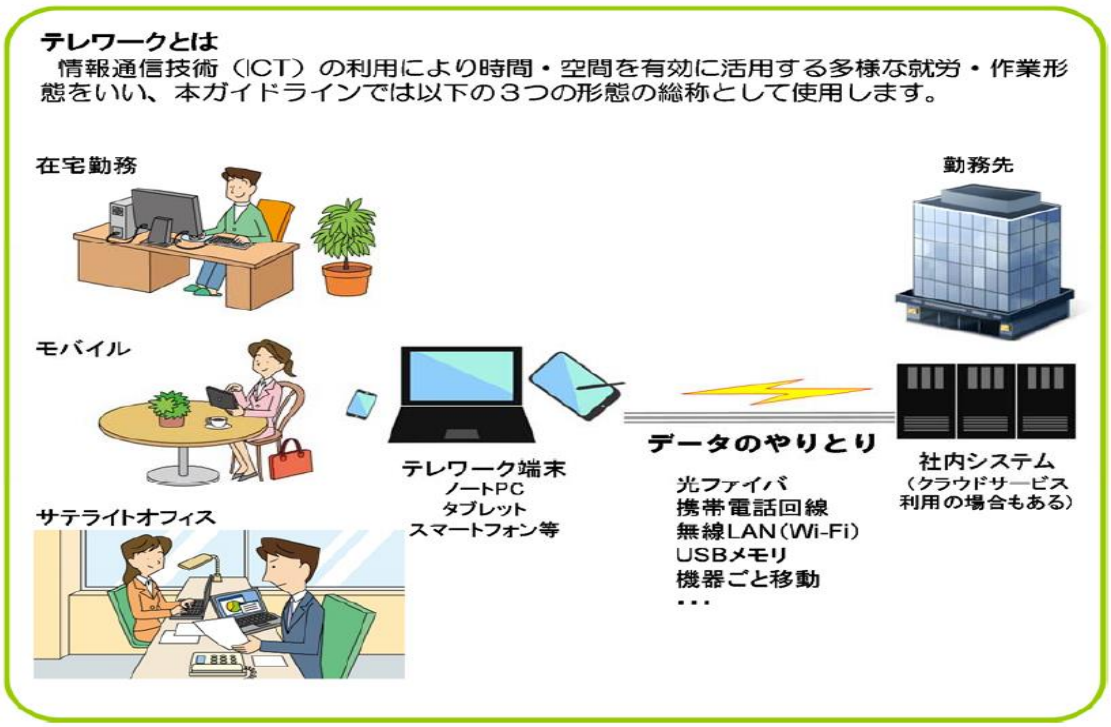
２．「withコロナ」「afterコロナ」時代のセキュリティとは

前章においては、2019年末に登場した新型コロナウィルスにより、企業や個人の働き方がどのように変化したかを概観したが、本章では前章の後半に少し触れた情報セキュリティという観点に着目して深掘り考察をしてみることとしたい。

２-１．　セキュリティ面の準備や対策は万全だったか？

2020年春、新型コロナウィルスの拡大を踏まえ、政府は緊急事態宣言を発令した。この結果、多くの企業が出社や不要な外出を制限せざるを得なくなり、結果的にテレワーク（下図参照）による在宅勤務の実施を余儀なくされた。では果たして多くの企業においてセキュリティ面の準備や対策を十分に講じることが出来ていたのだろうか。

世の中には様々な企業が存在する。「働き方改革」を前面に押し出し、数年前からテレワーク主体で活動を行っている企業もあれば、一方で諸々の理由からIT環境を全く整備することができなかった企業もあることだろう。ところが、そのような企業の対応状況には全くお構いなしで緊急事態宣言は全ての企業にテレワークの実践を要求した。結果として、相応の準備が進んでいて多少の追加対応だけで凌げた企業もあれば、有無を言わさずテレワーク環境の全面導入を余儀なくされた企業もあったであろう。特に後者のような企業においては、持ち出し専用のPC端末やWi-Fiルータを急遽大量購入して従業員に配布したとか、Web会議ツールを突貫で導入して整備した等、何とかテレワークができる環境だけは整えた、というのが現実だったと思われる。そうした様々な状況下において、セキュリティ面の対応は十分だったのであろうか。

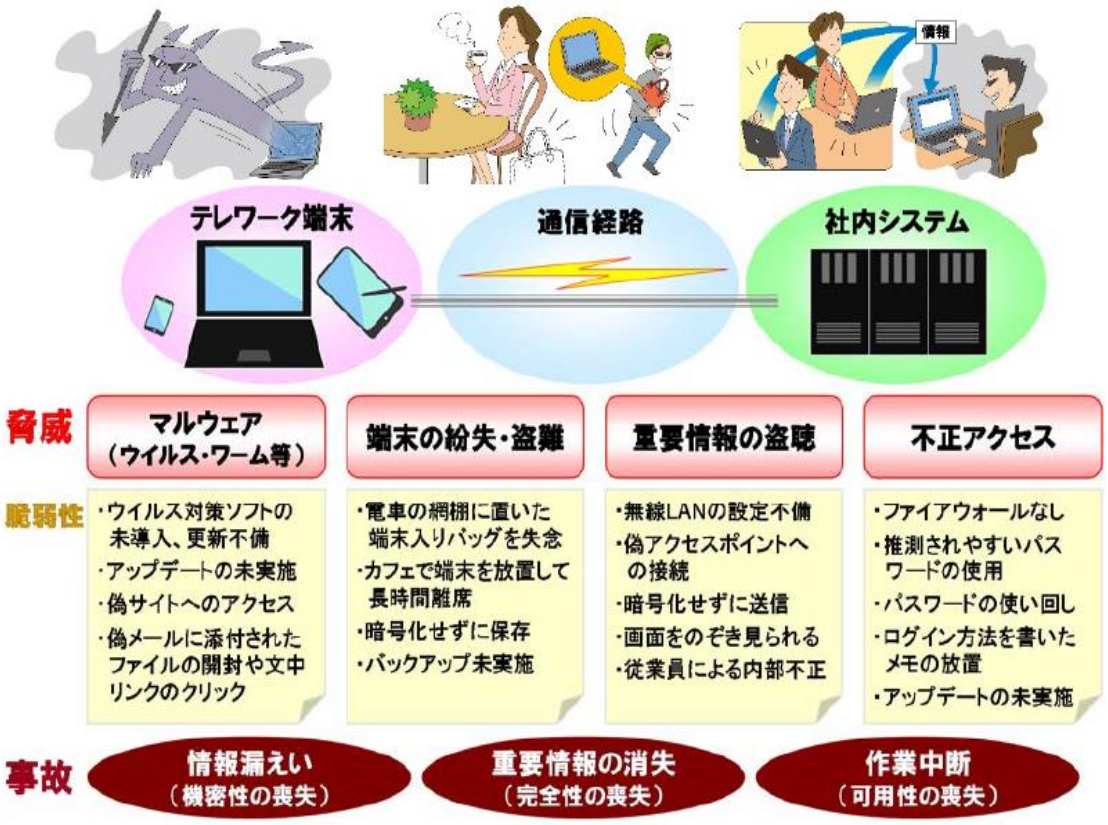


出典：テレワークセキュリティガイドライン第４版（総務省）

http://www.soumu.go.jp/main_content/000545372.pdf

2-2．テレワーク導入に伴って生じるセキュリティ上の課題

数年前からテレワークの導入は始まっているが、当時からセキュリティ面の課題は多く存在していた。インターネットの利用を大前提とするテレワーク環境においては、古くから多くの方法で検討されてきた従来型とも言える境界型セキュリティだけでは十分な対策が講じられている、とは言えないからである。境界型セキュリティは、ある程度の閉じた空間、つまりLAN環境をファイアウォール等で守るというのが基本的な考え方である。したがって、社内LAN環境での仕事を中心に行ってきた企業の従業員にとっては、テレワーク環境に移行しても同様のセキュリティ対策を講じれば大丈夫なはず！と誤解しがちで、テレワーク環境に潜む真のセキュリティリスク（下図参照）をきちんと認識していない可能性が高い。



出典：テレワークセキュリティガイドライン第４版（総務省）

http://www.soumu.go.jp/main_content/000545372.pdf

それでは、テレワーク環境と社内LAN環境で何がどう違うのか。テレワーク環境と言っても様々な形態が存在する。総務省がまとめた「テレワークセキュリティガイドライン第4版」によれば、主に次の6パターンに分類できるという。

	パターン①	パターン②	パターン③	パターン④	パターン⑤	パターン⑥
	リモートデスクトップ方式	仮想デスクトップ方式	クラウド型アプリ方式	セキュアブラウザ方式	アプリケーションラッピング方式	会社PCの持ち帰り方式
概要	オフィスにある端末を遠隔操作	テレワーク用の仮想端末を遠隔操作	クラウド上のアプリーションを社内外から利用	特別なブラウザを用いて端末へのデータの保存を制限	テレワーク端末内への保存を不可とする機能を提供	オフィスの端末を持ち帰りテレワーク端末として利用
テレワーク端末に電子データを保存するか？	保存しない	保存しない	どちらも可	保存しない	保存しない	保存する
オフィスの端末と同じ環境を利用するか？	同じ	テレワーク専用の環境	クラウド型アプリに関しては同じ	ブラウザ経由で利用するアプリに関しては同じ	テレワーク専用の環境	同じ
クラウドサービスを利用するか？	しない	しない	する	する	する／しない どちらも可	する／しない どちらも可
私用端末の利用(BYOD)との親和性	一定の条件のもとで可	一定の条件のもとで可	一定の条件のもとで可	一定の条件のもとで可	一定の条件のもとで可	―
高速インターネット回線の必要性	必須	必須	望ましい	望ましい	望ましい	不要
備考	―	―	―	―	―	紙媒体で持ち出す場合も本パターンに相当

出典：テレワークセキュリティガイドライン第4版（総務省）

http://www.soumu.go.jp/main_content/000545372.pdf

各パターンの詳細説明については「テレワークセキュリティガイドライン第4版」を参照していただくとしてここでは割愛するが、すべてのパターンにおいて、従業員は自宅等から何らかの形でインターネットを介して社内IT環境に接続する。そして遠隔で業務を行うことになる。つまり大半のケースで家庭用ルータ等を使用しなければならない。果たしてそのような家庭用ルータは、十分なセキュリティ対策が講じられているのであろうか。

2-3．家庭用ルータに潜むセキュリティ問題

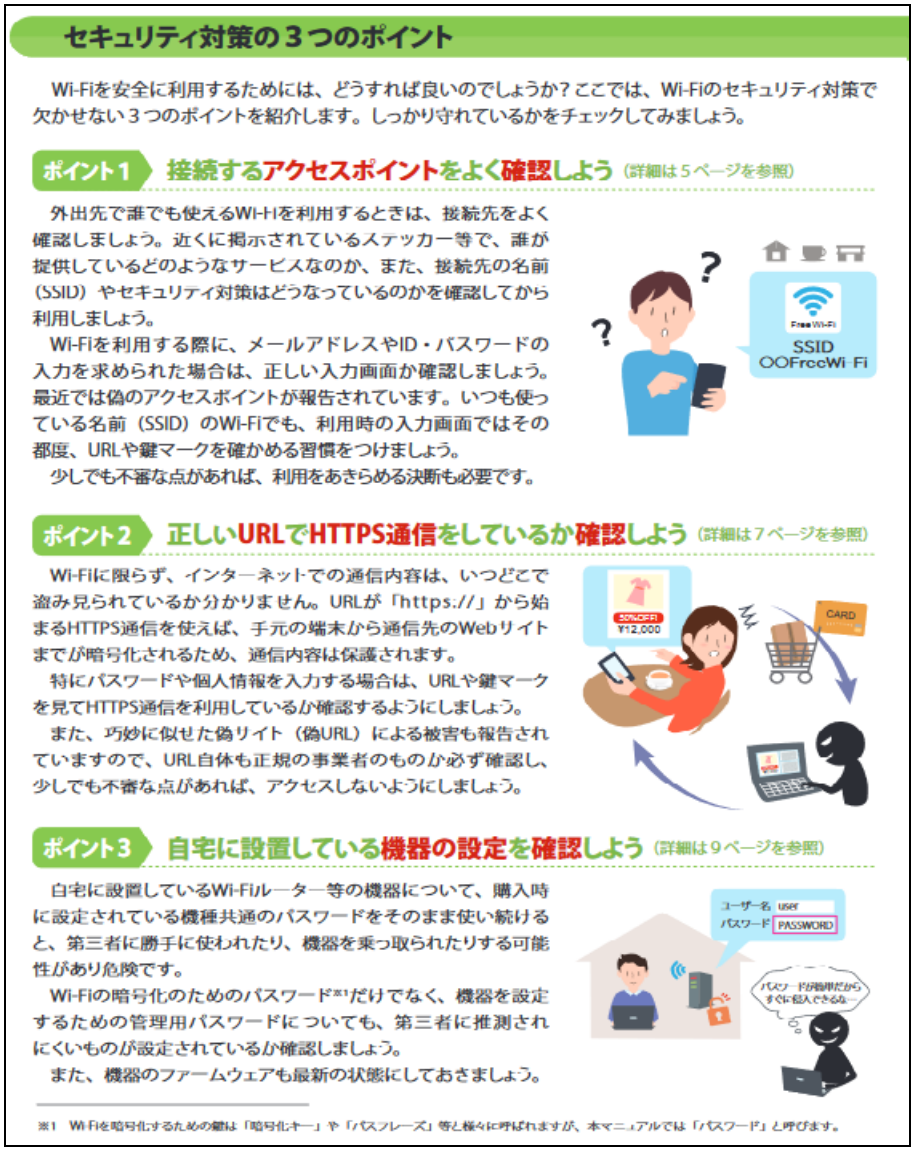
現在、家庭用ルータは、多くの家庭で利用されており、販売されている機器の種類だけでも数百以上あるだろう。ドイツのフラウンホーファー研究機構が報告書として取りまとめた「Home Router Security Report 2020（ホームルーターセキュリティレポート2020年版）」という調査レポートによると、調査対象とした127種類のすべての家庭用ルータで既知の重大な脆弱性が見つかった、と報告されている。しかも、各ルータに対する最新版のアップデートを適用した場合においても大半の脆弱性は修正されないままになっているという。また、「一部のルータは簡単にハッキングが可能であり、利用者が変更できない形で誰でも思いつくような簡単なパスワードが使用されている場合もある。具体的には、50台のルータで管理者の認証情報がハードコーディングされており、そのうちの16台では一般的、つまり推測しやすいログイン認証情報が使用されていた。」とも同調査レポートは述べている。つまり、多くの家庭用ルータが深刻なセキュリティ欠陥の影響を受ける可能性を有しているということを示しており、接続する機器や利用者をサイバー攻撃のリスクにさらしているのである。

出典：Home Router Security Report 2020（ホームルーターセキュリティレポート2020年版）
https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf

2-4．Wi-Fi接続に関する国からの注意喚起

前節で記載のような背景もあり、総務省はWi-Fiの利用者や提供者向けに用意している既存のセキュリティ対策ガイドラインに対して最新の技術動向やセキュリティ動向を踏まえて随時見直しを行い注意喚起している。具体的には、利用者向けのマニュアルである「Wi-Fi利用者向け簡易マニュアル」、公衆無線LAN提供者向けに必要なセキュリティ対策をまとめた「Wi-Fi提供者向けセキュリティ対策の手引き」がそれに該当する。

特に、利用者向けの「Wi-Fi利用者向け簡易マニュアル」では、Wi-Fi接続を行う際の注意事項や正規サイトのURLに対してHTTPSを用いた通信を行っているか等をしっかり確認するように求めている。



セキュリティ対策の３つのポイント

Wi-Fiを安全に利用するためには、どうすれば良いのでしょうか？ここでは、Wi-Fiのセキュリティ対策で欠かせない３つのポイントを紹介します。しっかり守れているかをチェックしてみましょう。

ポイント１ 接続するアクセスポイントをよく確認しよう （詳細は５ページを参照）

外出先で誰でも使えるWi-Fiを利用するときは、接続先をよく確認しましょう。近くに掲示されているステッカー等で、誰が提供しているどのようなサービスなのか、また、接続先の名前（SSID）やセキュリティ対策はどうなっているのかを確認してから利用しましょう。
Wi-Fiを利用する際に、メールアドレスやID・パスワードの入力を求められた場合は、正しい入力画面か確認しましょう。最近では偽のアクセスポイントが報告されています。いつも使っている名前（SSID）のWi-Fiでも、利用時の入力画面ではその都度、URLや鍵マークを確かめる習慣をつけましょう。
少しでも不審な点があれば、利用をあきらめる決断も必要です。

ポイント２ 正しいURLでHTTPS通信をしているか確認しよう （詳細は７ページを参照）

Wi-Fiに限らず、インターネットでの通信内容は、いつどこで盗み見られているか分かりません。URLが「https://」から始まるHTTPS通信を使えば、手元の端末から通信先のWebサイトまでが暗号化されるため、通信内容は保護されます。
特にパスワードや個人情報を入力する場合は、URLや鍵マークを見てHTTPS通信を利用しているか確認するようにしましょう。
また、巧妙に似せた偽サイト（偽URL）による被害も報告されていますので、URL自体も正規の事業者のものか必ず確認し、少しでも不審な点があれば、アクセスしないようにしましょう。

ポイント３ 自宅に設置している機器の設定を確認しよう （詳細は９ページを参照）

自宅に設置しているWi-Fiルーター等の機器について、購入時に設定されている機種共通のパスワードをそのまま使い続けると、第三者に勝手に使われたり、機器を乗っ取られたりする可能性があり危険です。
Wi-Fiの暗号化のためのパスワード※1だけでなく、機器を設定するための管理用パスワードについても、第三者に推測されにくいものが設定されているか確認しましょう。
また、機器のファームウェアも最新の状態にしておきましょう。

※1 Wi-Fiを暗号化するための鍵は「暗号化キー」や「パスフレーズ」等と様々に呼ばれますが、本マニュアルでは「パスワード」と呼びます。

出典：Wi-Fi利用者向け簡易マニュアル（総務省）

https://www.soumu.go.jp/main_content/000690266.pdf

2-5．ゼロトラストセキュリティの必要性

それでは改めて新型コロナウィルスの登場によって急遽テレワーク環境の全面導入を余儀なくされた企業が行うべきセキュリティ対策とは何か、に話を戻して考察していくこととしたい。前節までに述べたとおり、テレワーク環境においては脆弱性のある家庭用ルータ等を利用しなければならず従来の境界型セキュリティの考えに基づく対策では対処にも限界がある。考えられる基本的な対策としては、せいぜい次に挙げられることくらいであろう。

・信頼できないWi-Fi接続は行わない。
・ルータ等の関連NW機器に接続する際に使うパスワードについては初期設定のままとはせず簡単には類推できないものに変更する。
・端末側でもロック機能や暗号化等の対策を講じる。
・VPN接続を必須とする。
・多要素認証を取り入れる。

しかし、これでは弱い。ましてや新型コロナウィルスの登場に便乗して日々進化しつつあるサイバー攻撃を防ぐことはほぼ不可能だろう。そこで改めて見直されてきたのが、エンドポイントを守るために効果的とされる「ゼロトラストモデル」と言われる考え方に基づくセキュリティ対策である。

境界型セキュリティでは、ある程度の閉じた空間、つまりLAN環境を「信頼できる環境」と位置づけ、外部からの脅威に対してファイアウォール等による多層の防御によりエンドポイントを守ってきた。それに対してゼロトラストモデルでは、いつ何時でも、どのような環境でも信頼できる環境は存在しない！という前提に立ち、徹底したエンドポイントの保護を志向する、という考え方で対策を講じるものである。具体的なセキュリティソリューションとしては、NGAV/NGEPPやEDR等が有名である。

ソリューション	概要
NGAV/NGEPP（Next Generation Antivirus/ Next Generation Endpoint Protection Platform）	マルウェア特有の動作を手がかりにマルウェアを検知するソフトウェアの総称。従来の「アンチウイルスソフトウェア」や「ウイルス対策ソフトウェア」で使われたパターンマッチング技術とは異なり、振る舞い検知やAI・機械学習といった技術を用いてマルウェアと疑わしいものを検知・ブロックし、対象デバイスをマルウェア感染から守る。
EDR（Endpoint Detection and Response）	パソコン等の対象デバイスにおけるエンドポイントでの操作や動作について記録・監視し、サイバー攻撃を受けたと思われる挙動を検知次第、すぐに対処することを目的としたソフトウェアの総称。万が一、上記のNGAVやNGEPPをすり抜けるようなサイバー攻撃を受けてしまったとしても被害を最小限にすることを目的の一つとしている。

2-6．運用の重要性

それではNGAV/NGEPP やEDR等のゼロトラストモデルに準拠したセキュリティソリューションを導入したら安心と言えるのであろうか。それだけでは不十分で、それらソリューションを導入した後の運用が非常に重要である。勿論、検知や防御も重要であるが、サイバー攻撃を検知した際、まず最優先でどのような対処をすべきか、原因の調査や今後のセキュリティ対策に反映させるためにどのようなログ情報を収集すべきか等を予め考えて運用方法を決めておくことが重要である。まさにそのあたりのセキュリティ運用如何によって、様々なサイバー攻撃から本当に守れるか否かが左右されるといっても過言ではない。

例えば、テレワーク環境においては社内のセキュリティに強いIT管理者は常に別の場所にいるものである。したがって有事の際においても、傍にいて対象デバイスに関するサポートやメンテナンスを簡単に行うことは出来ない。また近くに対象デバイスがあればログの収集等も容易に出来るであろうが、遠隔操作ではなかなか思うような情報が収集できないだろう。このように、IT管理者が離れた場所にいても、対象デバイスの隔離や必要なログ情報の収集等を遠隔に行えるような運用面の考慮が必要である。

2-7．マネージドセキュリティサービス（MSS）

最近は、大手ITベンダーが競うように「マネージドセキュリティサービス（MSS）」というサービスを提供し始めている。これは大手ITベンダーに所属するセキュリティエンジニアがユーザ企業に代わってセキュリティ運用を行うというものである。具体的には、アラート監視、ログ解析、リスク判定等を適宜実施し、その結果を踏まえた分析結果の報告や改善策の提案等を実施するものである。本章の前半で述べたような緊急事態宣言の発令により急遽テレワーク環境の導入を余儀なくされた企業にとっては、容易に近年の様々なセキュリティ脅威に対する知見等をサポートしてもらえることから有益なサービスと言えるであろう。

2-8．本章のまとめ

「withコロナ」「afterコロナ」時代のセキュリティとは、NGAV/NGEPP やEDR等に代表されるゼロトラストモデルに基づくセキュリティであり、今回の緊急事態宣言に伴う突貫のテレワーク環境整備でその導入に拍車がかかった格好である。

新型コロナウィルスの流行は、やっとワクチンが出始めたものの新種も確認されつつあり、残念ながら現時点では未だに終息の目処が立っていない。また、仮に新型コロナウィルスの流行が終息したとしても今後新たな感染症がまた流行る可能性もある。つまり、感染症対策と上手に付き合うことが余儀なくされる「withコロナ」「afterコロナ」時代に突入したのである。この環境下では、感染症対策に伴うテレワークの活用による働き方改革が進み、一方で巧妙化・多様化するサイバー攻撃と常に向き合っていく必要がある。まさにゼロトラストモデルの考え方をしっかりと理解し、様々なサイバー攻撃に打ち勝っていく必要があるのである。

参考資料：

・テレワークセキュリティガイドライン第4版（総務省）
http://www.soumu.go.jp/main_content/000545372.pdf

・Home Router Security Report 2020（ドイツ：フラウンホーファー研究機構）
https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf

・Wi-Fi利用者向け簡易マニュアル（総務省）
https://www.soumu.go.jp/main_content/000690266.pdf

3.「Withコロナ時代」の汎用ビジネスツール活用

3-1.　DX化を進める事の利益

経済産業省などがDX化を進める事を推奨して久しい。

たまたま今回のコロナウィルス感染への対応で、日本全体が他国に比較してデジタル化が遅れていることを露呈することになった。諸外国の中でも、特に中国のIT化はものすごく進んでいて、デジタル特区的なものを設定して、生活上の活用は勿論、国民の行動までデジタルデータで把握できるような大規模な実験が行われている。ITのビジネスを日本でやるよりは中国で行った方が良いと考えているIT技術者は少なくない。

政府にとってIT化を進める事は、申請や給付の作業の把握とスピードアップ、不正の摘発など、コントロールと合理化に寄与するのでメリットは大きい。

一方、中小企業にとってIT化することにはどんなメリットがあるだろうか。社内処理、企業間処理、主務官庁への申請・給付業務に分けて考えてみたい。

①社内処理での利益

DX化を始める前に、企業のプロセスがどうなっているのかを可視化し、共通認識を形成しておく必要がある。

日本の企業風土では次のような現象を抱えてる企業が多い。

・紙資料を所有し、話を通さないと情報開示しない
・作業手順が個人に帰属し、徒弟関係を結ばないと開示しない
・経営者の方針と関係なく、場末の赤提灯に連れていき勝手に指示を出す

仕事の進め方が個人に帰属し、特定の人間が権力構造を勝手に構築し、企業の利益が損なわれている。この様なケースはよく見られるが、実は情報共有と人事評価制度の見直しを推進すると消滅してしまうのである。茨城県の某流通会社で、流通システムを導入するため業務プロセスの整理を行ったところ、たったそれだけでIT化以前にも係わらず従来に比べて４０％ものコストダウンが実現したケースがあった。業務プロセスの整理が放置されたままになっていて、共通認識が形成されていない事が問題なのである。また、少数ではあるがそれに付け込んで、個人的な権力構造を作る輩が問題なのである。

従って、IT化を進める事は業務プロセスを見直すことに他ならないのである。情報がどのように流れ、それが経営の意思決定にどの様に結びついているのかの共通認識の形成と同時に、合理的な処理によるコストカットに結びつくのである。余剰となった労力は他の業務に振り向ければ、さらに経営の効率化に寄与する。

②企業間処理での利益

企業間でのやり取りを電子化すれば、非常にスムーズな業務運営が可能となる。業界VANなどは３０年以上前から存在する。

情報交換だけではなく、発注・受注業務を電子的に行えば、早く正確に処理できるので、経営上は好ましい。現在では共通EDIの普及が進められている。この共通EDIの導入に合わせて社内システムを再編成すれば、合理的でスピーディーな業務処理が実現できるので経営に貢献できる。

③主務官庁への申請・給付業務・査察対応での利益

企業側のDX化による申請・給付・査察等の業務は、主務官庁にとっては正確で素早い処理の実現によるコスト削減に寄与するので、官庁側にとってのメリットは大きい。官庁側の問題点は、セキュリティ対策と、ハンコを突きたがる人の処遇かもしれない。

中小企業側にとっても労力削減とスピードアップにつながるのでメリットは大きい。社内システムと連動できれば一番良いが、それはコストが伴ってくるので、対費用効果の判断に委ねられる。社内作業の大部分が紙でも、申請業務自身が電子化されれば、納税の電子化を例にとっても分かる通り、それなりのメリットはある。

電子化をすでに実現して運用している企業から見れば、何故電子化を進めないのか疑問が湧いてくるのであるが、当該企業にはそれなりの悩みもある。DX化を進める上で問題として指摘されているのは以下の点である。

①経営者のDX化に対する認識

②業務改革を進める企業風土の形成の不足

③導入・運用を継続していけるだけのシステム要員の確保

①と②は意識改革が必要であり、③はそれだけのスキルを持った要員の確保・維持が出来るだけの財政力があるかどうかにかかっている。意識改革は事例を見せたり他の企業とのベンチマークをしたりである程度進められるが、コストや要員のスキルの制約がある場合、その解決策を示せないと相手にしてもらえないので推進は決して簡単ではない。

次節以降で簡単に導入できて、スケールアップが可能なツールが登場してきているので、それについて触れてみたい。

3-2. リモートで共同作業をする便利なツールが登場している

リモートワークが一般企業でもすでに広まっているが、もともとは東日本大震災でオフィスが使えなかったり、節電のため出社しないで業務を遂行するなどが必要とされる一部の企業で行われていた。一方、国内にある外資系の企業のうち、創造性を求められる職種の人達は、企業内のフリースペースであったり、本人が選択した任意の場所での業務広く浸透してきて、それを支援するツール（グループウェア等）のソフトウェアも沢山登場してきていた。米国の場合、５０年以上も前から衛星（インテルサット）を使ったリモートワークで、普段は会社から数百キロ離れた自宅で仕事をし、

月に１～２回出社するだけという業務形態が存在していたので、その流れが継続発展してきているだけである。

会議システムも多数存在し、MicroSoft・Google・Ciscoなどは専門会社を買収して自社のサービスにそれらを組み入れ、オフィス支援システムの品揃えを行ってきた。

マイクロソフトの場合、Office365とクラウドサービス（OneDrive等）を使えば、グループワーク的なことは可能となり、マイクロソフトが提供するデジタルの世界だけで業務を完結させることが可能である。それにTeamsで会議システムを加えると、リモートで完全に処理が完結できる。

GoogleもSuite＋Chromeを提供していて（更にGoogle Workspace）、そこで提供されているビジネスサービスや会議システムを使って、その閉じた世界で業務を完結させることが出来る。

更にクラウドサービスを利用すれば、もっと高度な美辞なる環境を利用することが出来る。

◇Google Cloud Platform（GCP）

・コンピューティング
Compute Engine ： ハイパフォーマンスな仮想マシンによるインフラ
App Engine ： 開発に集中できるメンテナンス不要のプラットフォーム
Container Engine： インフラストラクチャー上でDockerコンテナを運用
・ストレージ
Cloud SQL ： 可用性の高いフルマネージドMySQLデータベース
Cloud Storage ： 多機能なAPIを備えたオブジェクトストレージ
Cloud Datastore ： 自動拡張するフルマネージドNoSQLデータベース
・ビッグデータ
BigQuery ： ビッグデータを手頃な料金でリアルタイムに解析
Cloud Dataflow ： リアルタイムデータプロセッシングサービス
Cloud PubSub ： 高信頼、多対多の非同期メッセージングでサービス間連結
・サービス
Cloud DNS ： 高いパフォーマンスと信頼性に優れたDNSサービス
Cloud Endpoints ： 一つのソースコードで複数のクライアントに対応
Translate API ： 多言語間のコミュニケーションを簡単に
Prediction API ： ログデータから将来のトレンドを予測

Google以外でもクラウドプラットホームサービスが提供されている。

◇Amazon Web Services(AWS)
Amazon Web Servicesとは、Amazon.comにより提供されているクラウドコンピューティングサービスである。クラウドのタイプとしてはIaaSに分類される。これらのサービスは全世界で18の地域に提供されている。

◇Windows Azure
Microsoft Azureは、マイクロソフトのクラウド プラットフォーム である。
2008年のProfessional Developer Conferenceで発表され、2009年末までのサービス開始前の評価期間を経て、2010年1月に世界21ヶ国で正式にサービスを開始した。

◇Openshift
OpenShiftというのはRed Hatが主導で開発しているコンテナプラットフォームで、最近の一行説明は"Enterprise Kubernetes for Developers“ということになっています。

◇Red Hat
レッドハット とは、クラウド技術サービスを中心とした会社であり、またLinuxディストリビューションのRed Hat Enterprise Linuxを製品として販売・開発・サポートしている。

3-3.　中小企業は小規模に利用できる便利ツールから始めれば良い

専用のシステム構築や、ビジネスソフトの導入となると導入コストが気になるわけであるが、標準サービスとして提供されているOffice365やOneDriveは少額コストからはじめられる。もう少し文書管理を強化したいのであれば、ゼロックスのDocuWorksを廉価版から利用すればよいし、企業データを可視化して業務改善に繋げたければ、Power BIを無料ライセンスで試してみて、効果を確かめながら少しずつライセンスを増やしていけば、費用的負担は最小限に止められて効果的である。

特にPowerBIはデータを集計する上で必要な作業があり、集計を効果的に行うには、実はデータ作成時点でのレベル合わせが必要であることに気づく。既にある山の様なデータを持ってきてBIソフトで解析したり、AI（人工知能）にかけて新しいサービスを考える際に、データのレベル合わせとクリーニングが出来ていなければ利用できない。この事に気づいて行動を起こすことが業務改善の第一歩となるのである。

したがって、業務ツールの問題ではなく、従業員のデータに対する理解が業務改善に必須なのである事を理解してもらう必要がある。

データの大部分が紙で保存されている場合、どの様にしてデジタル化するかに迷ってしまうが、今は写真からOCR機能を使って文書を取り出すアプリが多数で回っているので、それらを利用すれば手軽に社内データをデジタル化して、分析対象とすることが出来る。マイクロソフトの場合、Office Lensが提供されているので、まず試行してみると良い（Office LensのWindows版は2020年で提供が終了）。

3-4.　運用上のリスクを考える上でのチェックリスト

前項までで述べた便利ツールに限らず、リモートワークをする上でセキュリティ上どの様な事柄に注意をすべきであるかについては、前章で詳細な解説がなされた。IPA

等が指摘しているリモートアクセス上の注意点を要約した内容を、以下に例示してみる。セキュリティ上の詳細な議論は次章以下で行うが、これらの点も点検する上で参考になると思う。

・自宅やレンタルスペースでの物理的セキュリティ（覗き見、データ窃盗など）等への警戒は守られているか？
・自宅やレンタルスペースのネットワークセキュリティ（ルータ監視など）はなされているか？
・テレワークソフト自身のインストールがセキュリティホールになっていないか？
・テレワークソフトは常に最新版になっているか？
・レンタルスペース等での、共有Wi-Fi利用時のファイル共有禁止措置はとられているか？
・オンライン上のなりすまし（アバターなど）は監視されているか？
・オンラインで利用している個々のPCのOSのアップデート（機能更新）はどの様に実行するのか？
・オンラインで利用している業務アプリのアップデート（機能更新）はどの様にするのか？
・自宅PC毎のセキュリティソフトのアップデートはどの様にするのか？
・自宅PC毎のセキュリティソフトはクラウド対応になっているか？
・会社に戻って出社した際の、自宅PC接続時のセキュリティレベルやセキュリティチェックはどうするか？
・自宅で使っていたUSBメモリをそのまま会社のシステムに繋げていいのか？
・使用目的が終わった企業情報を、自宅ＰＣから漏れなく削除する方法はあるのか？
・なりすましメールやフィッシングに対する教育は徹底されているか？
・油断している個人PCから侵入したランサムウェアに対する対策は考えてあるか？
・各人が取り扱う情報のバックアップや情報受け渡しの手段はクラウド経由になっているか。USBを使用している場合、紛失対策は考えてあるか？

参考資料：

Web会議サービスを使用する際のセキュリティ上の注意事項（IPA）

４．ゼロトラストと情報セキュリティポリシーとの関係

情報セキュリティポリシーという概念が企業の中で一般的になり、制定される様になってから約20年が経過している。

一方で、企業を取り巻く環境（特に情報セキュリティ）についてはこの10年で劇的な変化を遂げてきている。

ところが、情報セキュリティポリシーの利活用も含め見直しがきちんとされていない企業も多数存在している様に思われる（出典：情報セキュリティ大学院大学アンケートより）。とはいえ、情報セキュリティポリシーを策定していないか、策定してから見直しを行っていない様な中小・中堅企業にとって、ゼロトラストという”黒船”は、情報セキュリティに対する考え方・方針を見直す良い機会と思われる。

ITCはそれを加速する手伝い（方向付け）に機会があれば積極的に関与すべきと思われる。

経済産業省が2015年に“サイバーセキュリティ経営ガイドライン”を策定（2017年にVer2.0 に改定）して、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進しようとしている。

これは、企業戦略として、ITに対する投資やセキュリティに対する投資等をどの程度行うかなど、経営者による判断が必要となることを周知徹底し、実行させる狙いだが、現状では不十分と思われる。特に経営層への情報セキュリティ教育は重要と思われるので、本章では、それらも踏まえて論じてみたい。

4-1. 企業における情報セキュリティポリシーの歴史

2001年頃から情報セキュリティポリシー第一次ブーム始まる

→ NIMDA等のウィルスによるインシデントやホームページの改ざん等により一部の民間企業で情報セキュリティポリシー策定開始

2002年頃から住基ネットワークの導入に伴いすべての国・都道府県・市町村で情報セキュリティポリシーが策定された。

→ 官公庁の入札・取引条件に情報セキュリティポリシー策定が要件に入った為、民間企業での情報セキュリティポリシー策定が加速された。

20XX年　ISMSの認証の為情報セキュリティポリシーを策定する会社が増えた？

2007年頃から情報セキュリティポリシー第二次ブーム到来

→ J-SOX法の施行に伴い、情報セキュリティポリシーの見直しやグループ内への展開？が行われた。

2010年　Forrester Research社により内部ネットワークといえども信頼しないことを基本とするゼロトラストネットワークモデル提唱

2015年　経済産業省が経営者向け“サイバーセキュリティ経営ガイドライン”を発表。

2017年　経済産業省が経営者向け“サイバーセキュリティ経営ガイドライン”を改定。（Ver2.0）

2019年　働き方改革法による在宅勤務やクラウドサービスの利用増加にともないゼロトラストがバズりだす。

2020年頃から在宅勤務の増加に伴い、ゼロトラストに注目が集まり国も対応。

4-2. 企業における情報セキュリティポリシーの現状

企業における情報セキュリティポリシーの現状を以下の様に分類してみる。

A.情報セキュリティポリシーを策定している

A-A.問題なくPCDAのサイクルが回っている。

A-A-A.全社の組織で回しており何ら問題無い。

A-A-B.IS部門か有志(個人)の頑張りでなんとか回している。

A-B.作成しっぱなしで見直しすらできていない。

B.情報セキュリティポリシーを策定していない

B-A.インシデントの対応が会社としてできている。

B-B.インシデントの対応が場当たり的に終わっている。

B-C.今まで大きなインシデントが(たまたま)発生していない。

（インシデントが発生しても気がついていない。）ロナ過により働き方が変化していることで、何も手を打たないと、取り残されてしまうと警鐘を鳴らしている。

4-3. 企業における情報セキュリティポリシーの課題

情報セキュリティポリシーの形骸化

・組織・体制の問題点

① 経営層の無関心（代替わりすると特に　コストセンター）

② IS部門、や特定の個人による情報セキュリティ組織
③ 担当者がメンバーの情報セキュリティ委員会
（どこかの会社もそうでした）
→ 情報セキュリティ委員会の形骸化
④ セキュリティの人材不足
⑤ 不十分なセキュリティ教育

・情報資産の問題点
① 情報資産の分類が適切に行われず、見直しも形骸化
（情報資産のライフサイクルの考え方に沿った
運用が出来ていない）
② 情報資産の見直しに合わせた対策の見直しも行われていない。
→ 定期的なリスク評価が出来ていない。
→ 適切な見直しが行われていれば、ゼロトラストの環境でも何ら問題なかったはず。

・文書の不整合
セキュリティポリシーとガイドラインやマニュアルの見直しが適切に行われていない。
→ 整合性を意識した規程類の見直しが行われていない。

・教育が不十分
情報セキュリティポリシー上の役割を意識した教育や、インシデント発生時の模擬訓練が出来ていない。

4-4. 人材ポートフォリオはセキュリティ的には大問題

ITCとしては、
（AAB）IS部門か有志（個人）の頑張りでなんとか回している。
（AB）作成しっぱなしで見直しすらできていない。
（BB）インシデントの対応が場当たり的に終わっている。
といった様な会社をターゲットにするべき。

参考資料：

サイバーセキュリティ経営ガイドライン（経済産業省）
https://www.meti.go.jp/policy/netsecurity/mng_guide.html
2018 年情報セキュリティアンケート調査結果（情報セキュリティ大学院大学）
http://lab.iisec.ac.jp/~harada_lab/survey/2018/2018_questionnaire_result.pdf
中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

5. セキュリティ・トレンドからみるゼロトラストとITコーディネータ

そもそも、インターネットというものは、開放的ですべてを共有し中央に集中した権力を持たないという思想のもとに「オープンでフリー」が前提になっている。それゆえ、インターネット上には善と悪、可能性と危険性といった矛盾が存在する。これまでのセキュリティの考え方は、その悪の面をみて閉鎖的であり、隠すことが前提で、共有することが例外と考えてきたといっても過言ではないだろう。「クラウドはガバナンスがきかない。セキュリティが心配だから使えない。」という人たちが今でもいる。確かに、クラウドが登場した当初は技術的に未熟であり制約も多く、その捉え方が間違いだったわけではない。それゆえ、自らのビジネスを脅かす存在としてクラウドを捉え、いろいろと理屈を重ねて積極的に否定してきた。その結果、ITの活用は進んではいたものの、セキュリティ環境はそれほど変わらなかったのである。

しかし、そのような制約がある中においても、可能性を見出し、その制約を克服してビジネスの可能性を広げてきた先進的なITコンサルタントたちがいたことも事実である。表に見える現象にとらわれて本質的な変化を見誤るべきではない。テクノロジーの変化の必然、すなわち、なぜこのような変化が起きるのか、その理由を探り、変化を先取りする姿勢がITコーディネータに求められるのではないだろうか。

コロナ禍におけるリモートワークの急速な拡大や企業におけるDX推進などで、セキュリティに対する考え方の転換が一層強く求められている。セキュリティについて古い価値観に過剰適応することなく、次の10年を見据え、ITコーディネータ自らの立ち位置を見直す時期に来ていることを認識すべきであろう。本章ではそのような思いをもってゼロトラストを論じてみたい。

5-１．セキュリティ・トレンドの捉え方

まずは、当ITガバナンス研究会の過去の研究成果報告からセキュリティのトレンドを振り返ってみる。

2014年の研究成果として「BYODを利用するための提言～利用とリスクのバランス～」と題する報告書をまとめた。そこでは、個人所有デバイスを業務に使う背景として、①コンシューマITの台頭、②デジタル・ネイティブの増加、③ワークスタイルの変化をあげ、企業はセキュリティ対策を実践するうえで、従来とは明らかに異なる発想や枠組みが求められることを認識すべきであり、IT利用の主導権が「管理者（IT部門）」から「エンドユーザー（社員）」に移ることが想定されることを指摘した。

また、2017年には「サイバーセキュリティ経営を支援するITコーディネータにとって必要となる知見とは」と題する報告書をまとめた。そこでは、従来、外部からの攻撃を入口で防ぐことを目的としたセキュリティ対策を施していれば企業の内部まで入り込まれることはないと考えられていたが、サイバー攻撃のアプローチが年々、しかも急激に変化を遂げており、情報技術を駆使して防御策を講じても、攻撃者は次々にその手口を変化させて防御策を突破し、対策をすり抜けて企業の内部まで入り込んでおり、従来の入口対策の知見だけでサイバー攻撃への対策を講じるのは、もはや危

険と言わざるを得ない状況であることから、「そのセキュリティ知見はもう危険かもしれませんよ」とITコーディネータに警鐘を鳴らした。

さらに、2018年には「中小企業におけるIoT～ITCが考えておくべきこと～」と題する報告書をまとめ、そこでは、企業がIoT システムを通じて新たなサービスを提供するに当たって、「セキュリティ品質」が保証されていることが前提であるとし、IoTシステムが提供するサービスの効用と比較してセキュリティ・リスクを許容し得る程度まで低減していくことが、今後の社会全体としての課題（チャレンジ）となることを指摘した。

これらの報告書の背景には、ITの管理統制において一定の範囲で自由を認め、その可視化を進めつつセキュリティ・リスクを低減させるという、セキュリティに対する考え方の方向転換があり、その論点は境界防衛型情報セキュリティからの脱却である。本論文のテーマであるゼロトラストもこれらと同じ背景を有し、これまでのセキュリティ・トレンドに沿って進化したものであり、決してこれまでと異質なものではない。

5-2. ゼロトラストの本質

2020年8月に、米国国立標準技術研究所（NIST）が公表した「Special Publication（SP）800-207 ゼロトラスト・アーキテクチャ)」によると、ゼロトラストとは、スタティックなネットワークベースの境界線防御から、リソースに焦点を当てた防御へと移行する、進化するサイバーセキュリティの一連のパラダイムを指す用語であり、組織が所有する環境は暗黙の信頼がないことを前提としている。そのため、ネットワークの場所がリソースのセキュリティ態勢の主要な要素とみなされなくなり、ネットワークセグメントではなく、リソース (資産、サービス、ワークフロー、ネットワークアカウント等) を保護することに焦点を当て、資産やビジネス機能に対するリスクを継続的に分析・評価し、これらのリスクを緩和するための保護策を講じることであるとしている。

また、ゼロトラストは単一のアーキテクチャではなく、ワークフロー、システム設計、および運用のための一連の基本原則であり、ネットワークが侵害されている場合であっても、正確かつ最小の権限となるよう、不確実性を最小化するための概念とアイデアの集合体のことである。具体的にはつぎのことを基本としている。

1. すべてのデータソースとコンピューティングサービスをリソースとみなす
2. ネットワークの場所に関係なく、すべての通信を保護する
3. 企業リソースへのアクセスは、セッション単位で付与する
4. リソースへのアクセスは、クライアントアイデンティティ、アプリケーション/サービス、リクエストする資産の状態、その他の行動属性や環境属性を含めた動的ポリシーにより決定する
5. すべての資産の整合性とセキュリティ動作を監視し、測定する
6. すべてのリソースの認証と認可を動的に行い、アクセスが許可される前に厳格

に実施する

7. 資産、ネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に利用する

また、ネットワーク接続に関しては次のことが基本的な条件になっている。

1. 企業のプライベートネットワークは、暗黙のトラストゾーンとみなさない
2. ネットワーク上のデバイスは、企業が所有していないか、構成可能なものではない場合がある
3. どんなリソースも本質的に信頼されるものではない
4. すべての企業リソースが企業のインフラストラクチャ上にあるわけではない
5. リモートの企業主体と資産は、ローカルネットワークの接続を完全に信頼できない
6. 企業のインフラストラクチャと非企業のインフラストラクチャとの間で移動する資産とワークフローには、一貫したセキュリティポリシーが必要。

5-3. ゼロトラストを導入するとはどういうことか

ゼロトラストは、前述の通り、リソースの保護に焦点を当てたサイバーセキュリティのパラダイムであり、信頼は決して暗黙のうちに与えられるものではなく、継続的に評価されなければならないという前提に基づいている。そのため、ゼロトラストを導入するということは、企業がビジネスに対するリスクをどのように評価するのか、その考え方を明確にするということであり、単なるセキュリティ技術の導入とは異なる。

また、ゼロトラストは概念であるため、特定の機能を持つソリューションや製品を指すものではない。自社のIT環境に大きく影響を及ぼすため、ITインフラの抜本的な変革が求められることから多額の予算を要する可能性がある。また、IT部門だけでなく、多くの関係者を巻き込みながら推進することにもなりうる。既存の構成に何かを組み込んで終わりというものではなく、技術の置き換えで単純に達成することはできないことを認識すべきである。

ゼロトラストは企業におけるセキュリティ上の諸課題を解決し、利便性とセキュリティを向上する打ち手に見えるが、安易に「我が社もゼロトラスト化を」と進めると思わぬ落とし穴にはまってしまう可能性がある。そのため、まずはなぜゼロトラストが必要なのかという導入の目的を明確にし、どのようなゼロトラストを実現するかという自社なりの解釈が必要になる。

よって、ゼロトラストの導入は、自社のデータ資産を保護するために、ビジネスプロセスを改善しながら、ゼロトラストと既存の境界ベースの防御策を平行して運用する、ゼロトラストの原則、プロセスの変更、およびテクノロジーソリューションの段階的な導入を目指すべきであろう。また、前述のように、ゼロトラストへの変革はアーキテクチャの変更を伴うため、できる限り小さく始めることを心がけるべきであろ

う。

5-4. ITコーディネータに求められること

新たなテクノロジーにはダークサイドがあり、そのテクノロジーがビジネスにとって役に立つものであればあるほどリスクを伴う。謙虚さを持たず良い面だけを見るのは良くない。しかし、リスクをとる覚悟も必要であろう。良い面と悪い面のバランスである。「どこに軸足を置いて、どの範囲までやるのか」の判断を求められる難しい時代が来ている。

ITコーディネータは、ITを前提とした事業や経営の変革について、課題を指摘し、自分の考えを示すことができなければならない。つまり、テクノロジーを使えることではなく、そのトレンドを踏まえて、事業や経営の戦略や施策を語れるかどうかがITコーディネータの価値なのではないだろうか。

「中小企業は違う」「まだそこまでの需要はない」などの考え方は、クラウドの黎明期のメンタリティと何も変わらない。これではまた過去の二の舞になるだけである。そのためにもテクノロジーの進化の道筋を理解し、それをビジネスに結びつけて考える習慣を持つように心がけるべきだと考える。

デジタル化が加速する中、企業によって明暗が分かれる要因は、「変化に対応ができたかどうか」であろう。3～5年の未来を見据えて変化に対応していくためには、それぞれの組織に合わせた未来志向型セキュリティが求められている。クライアントのセキュリティコンサルタントとしてのITコーディネータに求められる役割も変化しつつある。

参考資料：

ゼロトラスト・アーキテクチャ(NIST Special Publication 800-207)
BYODを利用するための提言～利用とリスクのバランス～ -（ITガバナンス研究会）
サイバーセキュリティ経営を支援するITCにとって必要となる知見とは -（ITガバナンス研究会）
中小企業におけるIoT～ITCが考えておくべきこと～ -（ITガバナンス研究会）

6. おわりに

このところ(2021年3月)、マルウェア「Emotet（エモテット）」の被害が急増している模様である。「脅威の侵入経路の多様化」と言われる、「ヒト・モノ(デバイス)・データ」がさまざまな場所に分散したIT環境へと大きく変容している結果、セキュリティ確保に大きな脅威が訪れているということである。

これまでの章で述べてきたように、新しい時代・環境に合わせた変革が出来ない組織は落ちこぼれてしまう。新しい働き方が普及されたことにより、社内外のネットワークの境界線が曖昧になっており、サイバー攻撃が多様化しているため、社内ネットワークが狙われる可能性も十分にある。そのため、境界線の内側が安全とは言い切れなくなっている、この対応を間違いなく行うことが喫緊の課題となるわけである。

この脅威は企業規模には関係なく、ゆえに中堅・中小企業にとって。課題解決に繋がる支援体制が、前章で述べた通り私たちITコーディネータに求められるところである。

つまりは、適用する領域や機能、特性に合わせたリスクを抽出・評価し、リスク対応を行うことになる。

この視点において、ITコーディネータとしてユーザ支援を行う上で、セキュリティ対策を怠ると個人情報や機密情報が漏えいする恐れがあり、情報が漏えいしてしまった場合、大きな経済的、社会的損失を生む。損害賠償を求められることがあり、ランニングコストよりも情報漏えいした場合の損失の方が大きくなるということを、徹底して支援対象者（経営者など）に理解いただき、適正なコストを掛けて仕組みを導入するところまで実行頂きたいものと考える。

最後に、本論文が読者諸兄の役に立てれば幸いである。

以上

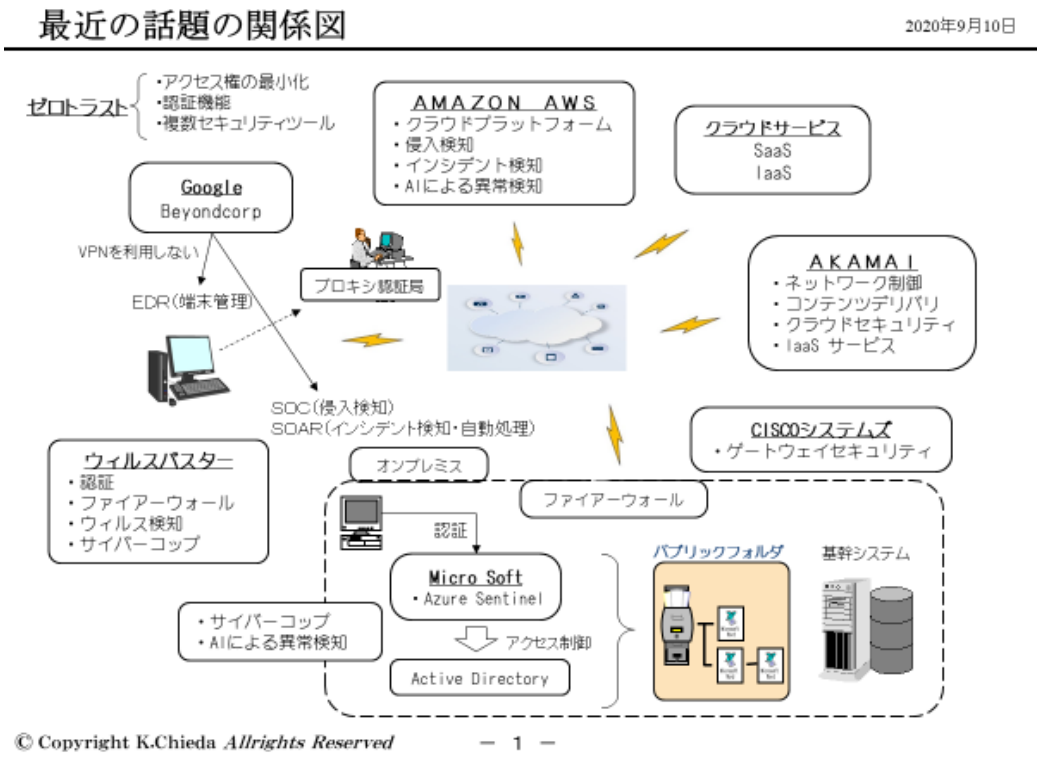
添付資料

ゼロトラストセキュリティ　Q&A（1）	
領　域	ゼロトラストセキュリティ
テーマ	ゼロトラストセキュリティとは何か
質問	２０００年代半ばより、ゼロトラストセキュリティというものが言われ始めましたが、いったいどのようなものでしょうか。
回答	ゼロトラストとは「すべてを信頼しない」という意味で、米調査会社フォレスター・リサーチのアナリストだったジョン・キンダーバーグ氏（現・米パロアルト・ネットワークス CTO）が提唱したものであり、「何も信頼できない」という前提のもと外部・内部のネットワークを問わず、すべてのアクセスを制御するというコンセプトのセキュリティ対策です。 今から十数年前であり、この時代は、クラウドサービスが登場してきた時代です。 それまでは、「オンプレミス」と言って、組織内の閉ざされた中でのみ情報処理が行われていたため、外部からの侵入はに対しては、侵入口さえ押さえておけば、内部的には問題ないと考えられており、セキュリティ防御もそのように考えられて対策が取られていた。 また、通信も業界ＶＡＮやＶＰＮで行われており、インターネットは専門家が管理するファイアウォールに守られていて、侵入手口は限定的であった。 ところが、クラウドシステムの登場により、情報システムのコストを設備費用から経費に置き換え、要員を配置換えする事で、経営の効率化を図ることで経営の機動性を強化させることが出来るようになり、コスト的にも有利に進めることが出来るようになった。 当然のこととして、企業情報の大部分が社外に起これるようになり、従来と異なる情報セキュリティ上の防御が必要となってきたため、ゼロトラストセキュリティの様な考え方と対策が必要となってきたのであり、今後ともその重要性は増してくる。
備　考	出典：　東京エレクトロンデバイス株式会社(加筆修正)

別紙

ゼロトラストセキュリティ　　Q&A（2）	
領　域	ゼロトラストセキュリティ
テーマ	ゼロトラストセキュリティに取り組むには（1）
質問	ゼロトラストセキュリティに取り組むには、どの様にしたら宜しいのでしょうか。
回答	ゼロトラストセキュリティを実装するには、ユーザー、デバイス、アプリケーションなどネットワークを構成するすべてのコンポーネントを検証し、信頼できることを証明するための仕組みが必要になります。その仕組みがリソースへのアクセスを許可する前にIDとデバイスの正常性を検証し、アクセスが許可されている場合であっても明示的に許可された必要最小限のリソースのみにアクセスを制限します。これによって、セキュリティを担保するのです。
備　考	出典：　東京エレクトロンデバイス株式会社(加筆修正)

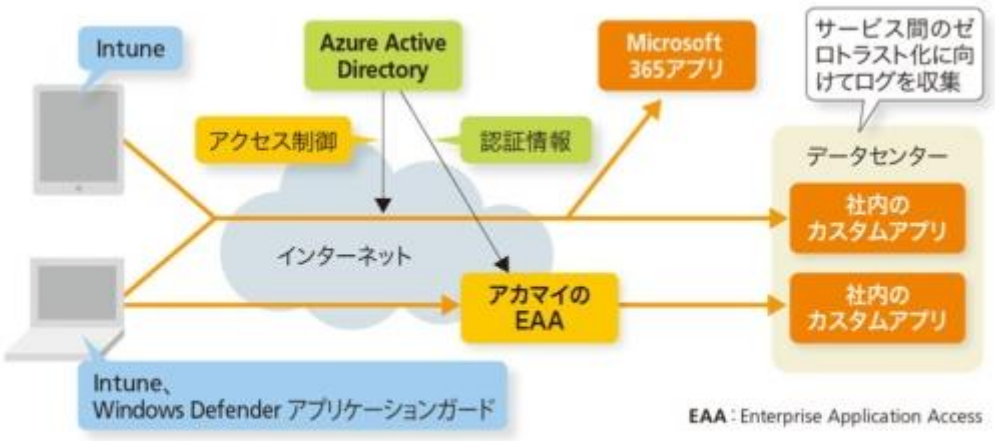
ゼロトラストセキュリティ　　Q&A（3）	
領　域	ゼロトラストセキュリティ
テーマ	ゼロトラストセキュリティに取り組むには（2）
質問	ゼロトラストセキュリティにはどのような取り組み方があるのでしょうか。
回答	このようなゼロトラストセキュリティのソリューションは、大きく２種類のアプローチに分けられます。 1つは主にネットワーク／セキュリティベンダーが採用しているもので、ネットワークのセグメンテーションを細分化（マイクロセグメンテーション）し、すべてのトラフィック／パケットを検証・検査するセキュリティプラットフォームを構築してゼロトラストを実現しようというアプローチです。このようなセキュリティプラットフォームを導入すると、個別に導入していた各種セキュリティ製品の運用を単一ソリューションに集約・統合し、運用管理負荷を軽減できるというメリットが得られます。ただしセキュリティプラットフォームの技術はそれぞれベンダー固有のものであり、標準化もされていないため、場合によっては特定ベンダーにロックインしてしまう可能性があります。 もう1つのアプローチは、ＩＤベースでリソース単位のアクセス制御を行うというものです。主に認証システムベンダーやIDaaS（IDentity as a Service）ベンダーが採用しています。ID認証プロキシ（IAP：Identity-Aware Proxy）を利用して認証し、アプリケーションやデータレベルのセキュリティ対策が可能になります。このアプローチは標準化された技術を利用しているため、マルチベンダー環境であっても信頼性が確保できるというメリットがあります。ただしゼロトラストセキュリティの環境を構築するには、複数のソリューションを組み合わせなければならず、運用管理が難しくなるケースもあります。
備　考	出典：東京エレクトロンデバイス株式会社（加筆修正）

ゼロトラストセキュリティ　　Q&A（4）	
領　域	ゼロトラストセキュリティ
テーマ	ゼロトラストセキュリティの全体像
質問	ゼロトラストセキュリティの説明を聞いてもよく分かりません。全体像はどうなっていますか。
回答	ゼロトラストセキュリティのソリューションは、それを提供しているベンダーが個々のイメージで語っているだけで、これといった全体像は存在していないと思います。 筆者が考えるソリューションを中心としたゼロトラストセキュリティの全体像を以下に示します。 
備　考	

ゼロトラストセキュリティ　　Q&A（5）	
領　域	ゼロトラストセキュリティ
テーマ	ゼロトラストセキュリティとセキュリティポリシー
質問	ゼロトラストセキュリティを検討するにあたって、既に制定してあるセキュリティポリシーとどのように結び付けたらよいのでしょうか。
回答	セキュリティポリシーは、ポリシー部分とルール部分と実施（プロセス）部分から成り立っています。実施部分は、仕組み（ソリューション）部分とヒューマンリテラシー部分に分けられて定義されます。 ゼロトラストセキュリティといえど、ヒューマンリテラシー部分は従来と変わるところが無く、変更点のみを再教育すれば強化されます。 ソリューション部分は、ポリシーやルールを実現する仕組みを、ソリューション内に組み込む必要があり、全面的に見直しが必要とされます。 セキュリティ上管理すべきものはアクセスする要員と接続するデバイスであり、従来の様なオンプレミスでは、要員には人事システムがあり、個人単位に組織とアクセス権レベルを付与して、その情報を Active Directory に夜間バッチで送信して、人事異動の際にも即座にアクセス対象が管理されるような仕組みを構築できます。接続機器に関しては、機器管理システムにデバイス登録を行い、登録外の機器の検出が出来るようにしています。 この様な仕組みを、社外で利用するクラウドシステムにも同様に適用する必要があります。この仕組みを外部アクセスする際のプロキシシステムを新たに構築し、それを社内システムのアクセス権管理、接続デバイス管理と一元的に管理する必要があります。 マイクロソフトはクラウド向けに Azure Active Directory を提供し、従来の Active Directory と同様に管理センターを実現できるようにしています。 アカマイは Enterprise Application Access を提供し、 ・既存の Okta ソリューションと統合する ・リモートワーカーを安全にサポートする ・多要素認証（MFA） に対応する などのサービス提供を行っています。 これらの機能をセキュリティポリシーに従って、認証、アクセス管理等が実現出来るようにすることが、要件となります。
備　考	出典：

ゼロトラストセキュリティ　　Q&A（6）	
領　域	ゼロトラストセキュリティ
テーマ	ゼロトラストセキュリティの基準など
質問	ゼロトラストセキュリティを検討する上で、必要となる基準の様なものはありますか。
回答	ゼロトラストの定義としてNIST（National Institute of Standards and Technology, NIST, アメリカ国立標準技術研究所）より「SP 800-207: Zero Trust Architecture（ZTA）」がリリースされています。2019/9/23に Draft1（Withdrawn Draft） がリリース、2020/2/13に Draft2 に更新されました。 このドキュメントに含まれる重要なメッセージは大きくは５つの項目に分かれております。 【Zero Trust の原則】 Zero Trust Architecture（ZTA）で実行されるべきコンセプト的ガイドラインがリストされています。 ・全データソース、コンピューティングサービスはリソースと見なされる ・ネットワークの場所に関係なく、すべての通信が保護される ・組織リソースへのアクセスは、セッションごとに許可される ・組織リソースへのアクセスは、動的なポリシーによって決定される ユーザ ID、アプリ、リクエストアセットの状態 その他の動作属性を含めることができる ・所有し関連するすべてのデバイスが可能な限り最も安全な状態であることを保証し資産の継続的な監視と安全状態の保持 ・すべてのリソース認証と許可は動的であり、アクセスが許可される前に厳密に強制される ・ネットワークインフラと通信の状況を可能な限り収集し体制に利用、改善を行う ネットワークに接続される全リソースは、リクエスト元であってもリクエスト先であっても Zero Trust Architecture（ZTA）の中では動的ポリシーを導き出すために利用されるリソースとして扱われ、リクエスト、セッションごとに決定された動的ポリシーによって必要最小限権限を付加し、そのリクエストは暗号化とともにリソースアクセスが保護され、継続的な状態確認のためネットワーク全体の可視化が必要となります。そして可視化におけるタイムリーな情報はネットワーク全体にフィードバックされる、というプロセスが必要になります。
備　考	出典：

ゼロトラストセキュリティ　　Q&A（7）	
領　域	ゼロトラストセキュリティ
テーマ	ゼロトラストセキュリティのソリューション
質問	各企業や組織がゼロトラストセキュリティを進めていく上でのソリューションはありますか。
回答	ゼロトラストセキュリティを導入する具体的な方法として、マイクロソフトが提案するソリューション例を簡単に紹介します。 マイクロソフトはIDベースによるゼロトラストセキュリティを推奨しています。その中心的な役割を果たすのが、ネットワークを構成するユーザー、デバイス、アプリケーションなどのセキュリティ分析状況を可視化する「Azure Sentinel」です。Azure SentinelはOffice 365をはじめとするSaaSアプリケーション、サーバーやクライアントデバイスのネットワークサービス、主要ベンダーの各種セキュリティ製品などの各種ログをデータベース上に蓄積、ビルトインの機械学習モデルAzure Machine Learningによる独自モデルを使って分析処理を行い、ユーザーの異常行動や相関関係ルールに合わない脅威を検知するという機能を提供します。 Azure Sentinelでは「Azure Active Directory (AAD)」による共通ID認証基盤の運用を想定していますが、オンプレミスのActive Directory環境、その他のクラウドサービスなどのクラウド認証もサポートしています。ネットワークへのすべてのアクセスは、AADで「登録されているユーザーか」「登録されているデバイスか」「外部に情報漏えいしたIDではないか」といった検証が行われることになります。またWindows OSのセキュリティ機能である「Windows Defender」と連携し、「デバイスにインストールされているセキュリティ対策が最新か」「デバイスにマルウェアが感染していないか」という確認も行われます。
備　考	出典：東京エレクトロンデバイス株式会社（加筆修正）

ゼロトラストセキュリティ　　Q&A（8）	
領　域	ゼロトラストセキュリティ
テーマ	ゼロトラストセキュリティの事例
質問	ゼロトラストセキュリティの導入事例はありますか。
回答	auカブコム証券は米Microsoft（マイクロソフト）の「Microsoft 365 E5」を中心に、ゼロトラストネットワークに取り組んだ。多くの社内システムをスマホで操作できるように改善しているという。  **auカブコム証券の構成** ［画像のクリックで拡大表示］ まずスマホには MDM／MAM（Mobile Device Management／Mobile Application Management）ツールである「Microsoft Intune」を導入した。クラウドで提供する IDaaS（ID as a Service）である「Azure Active Directory」を介して、Intune がアプリケーションの利用を制御する。「例えば業務アプリでテキストをコピーした場合、そのテキストを業務アプリにはペーストできるが非業務アプリにはできないようにするといった制御ができる」（au カブコム証券の石川陽一システム統括役員補佐兼システム開発部副部長兼 IT 戦略グループ長）。
備　考	出典：日経ＸＴＥＣＨ

ゼロトラストセキュリティ　　Q&A（9）	
領　域	ゼロトラストセキュリティ
テーマ	ゼロトラストセキュリティチェック
質問	リモートワークを行う際の注意点はどのようなものですか。
回答	リモートワークをする上で、セキュリティ上どの様な事柄に注意をすべきであるかについては、ＩＰＡ等が指摘しているリモートアクセス上の注意点を公表しています。それらを要約した内容を、以下に例示してみます。 ・自宅やレンタルスペースでの物理的セキュリティ（覗き見、データ窃盗など）等への警戒は守られているか？ ・自宅やレンタルスペースのネットワークセキュリティ（ルータ監視など）はなされているか？ ・テレワークソフト自身のインストールがセキュリティホールになっていないか？ ・テレワークソフトは常に最新版になっているか？ ・レンタルスペース等での、共有 Wi-Fi 利用時のファイル共有禁止措置はとられているか？ ・オンライン上のなりすまし（アバターなど）は監視されているか？ ・オンラインで利用している個々のＰＣのＯＳのアップデート（機能更新）はどの様に実行するのか？ ・オンラインで利用している業務アプリのアップデート（機能更新）はどの様にするのか？ ・自宅ＰＣ毎のセキュリティソフトのアップデートはどの様にするのか？ ・自宅ＰＣ毎のセキュリティソフトはクラウド対応になっているか？ ・会社に戻って出社した際の、自宅ＰＣ接続時のセキュリティレベルやセキュリティチェックはどうするか？ ・自宅で使っていたＵＳＢメモリをそのまま会社のシステムに繋げていいのか？ ・使用目的が終わった企業情報を、自宅ＰＣから漏れなく削除する方法はあるのか？ ・なりすましメールやフィッシングに対する教育は徹底されているか？ ・油断している個人ＰＣから侵入したランサムウェアに対する対策は考えてあるか？ ・各人が取り扱う情報のバックアップや情報受け渡しの手段はクラウド経由になっているか。ＵＳＢを使用している場合、紛失対策は考えてあるか？
備　考	出典：