クライアント構成のセキュリティ管理
—コロナ禍に端を発したセキュリティ管理の変化—

日本大学危機管理学部　教授　美濃輪　正行

Ⅰ　はじめに

1　コロナ禍による労働環境の変化

コロナ禍においてはPCを利用した業務は自宅やサテライトオフィスで行われ、テレワークの実施率が高くなった[1]。ユーザーはシステム環境保全の責任を負うことと引き換えに、働く場所の自由を得られた。テレワーク対応可能な業務範囲は限定されるが、労働環境が分散すること、通勤等の移動が減ること、人と人との接触機会を下げることにより、その効果は一定程度評価できるものである。

テレワークのシステム環境はインターネットを介して組織内のネットワークにアクセスして業務を可能とするものである。しかし、インターネット経由の業務操作はコロナ禍のテレワークに限定されるものではなく、働き方改革による労働の多様化、パブリッククラウドサービスの利用に伴い、いずれ遭遇する課題である。更にシステム環境が変化した際のセキュリティインシデントに遭遇する可能性も考慮して、その対策を練っておく必要がある[2]。

2　クライアントの定義

クライアントなる用語は、オープンシステムが普及し始めた1990年前後から頻繁に使われるようになった[3]。クライアントという用語には共通する定義は定められておらず、状況によって意味合いは変化する。様々なケースで共通する事実は、情報システムの処理の起点となることである。本論文では、ユーザーが操作の対象とする物理的な装置、及びそこに含まれる論理的な機能を指すものとする。

3　本論文の主旨

本論文は、コロナ禍の状況を踏まえてクライアント構成に関するセキュリティ対策の実装について検討するものである。本来あるべきクライアントの姿を模索するという観点から、様々なシステ

ム構成におけるクライアントを考察する意図で、メインフレームでクライアントに相当する構成要素からテレワーク環境下のクライアント構成まで考察の対象としている。最終的にはゼロトラストアーキテクチャ（Zero Trust Architecture、以降ZTAと表記）の原則に基づくクライアント構成の実装の検討へと展開する。尚、第Ⅱ章4節以降ではクライアントの用語は主にパーソナルコンピュータ（以降PCと表記）を指すものとする。

Ⅱ　クライアント構成形態と想定されるセキュリティインシデント

この章ではメインフレームで構成される情報システムの端末装置からインターネットに接続されたクライアントまで、その構成の概要と各構成におけるセキュリティインシデントについて論考する。

1　メインフレームに接続した専用端末装置

1960年代にあっては、メインフレームの操作インタフェースとして専用の端末装置が利用された。これらの入出力インタフェース部分は、飽くまでもメインフレームの一つの構成部位であり、論理的に独立した構成ではなく、クライアントという概念は存在しなかった。代表的な例として1970年代当時のIBM社のメインフレームの構成ではOSがMVS、ミドルウェアとなるIMS（Information Management System）はデータ処理、アプリケーション処理、トランザクション処理、更には処理結果を表示する端末の状態も管理する機能を提供した[4]。1970年以降はメインフレーム以外にもDEC社に代表されるような中小型機としてのオフィスコンピュータの形態も普及したが、入出力インタフェースの位置付けはメインフレームと変わるものではない[5]。これらのシステムは、ユーザーインタフェースとなる専用端末がシステム全体と論理的に一体化している。アプリケーション操作時は、ユーザーIDとパスワードによる認証が必要であったが、これは端末識別情報と同様にトランザクション制御に利用された。これらの情報システムでは、端末と端末制御装置の間は電話回線や専用回線で接続することも可能であった[6]。

現在のシステム構成と基本設計が大きく異なるが、メインフレーム環境でもサイバー犯罪が発生している。1971年に米国で発生した事例では犯人のJerry Neil Schneiderは、電話資材を取り扱う会社から資材をだまし取っていたが[7]、電話回線を介して発注用の専用端末から成りすまして注文していた。アクセスに必要な電話番号を会社の担当者に直接電話をかけて聞き出している。現在でいうところのソーシャルエンジニアリングに相当する手口である。国内でも内部犯行として勘定系システムの不正操作による事案が国内で発生している[8]。1981年に女性銀行員が架空の口座に1億3000万円の振替入金を偽装した事件[9]は社会的な反響が大きかった。これらはコンピュータ内部の処理に意図的に介入したものではなく、アプリケーション機能を利用した犯罪である。

2　スタンドアロン構成のPC

1970年代後半から徐々に個人向けのPCが普及していった[10]。初期のPCはハードウェアベンダの独自仕様であったため、文字コードや記憶媒体の互換性について十分配慮されていなかった。

PC単体の構成のセキュリティインシデントの形態としてはマルウェア感染が挙げられる。Apple Ⅱは1982年に、IBM PCには1986年に初のウイルスが登場した[11]。いずれもフロッピーディスクを介してPCのブートセクターに感染する動作をとった。1989年にはランサムウェアを含むフロッピーディスクが2万通郵送されたとの事件が発生している[12]。ネットワークが未発達な状況では、意図的な感染は物理的に記憶媒体を介した手口に止まる。また、ベンダごとの製品の仕様による互換性の不備も感染範囲を限定した。

3　限定的なネットワークに接続されたPC

ここではLAN（Local Area Network）及びVAN（Value Added Network）について取り上げる。

1980年代になるとPCの普及と並行して、構成間を接続するネットワークとしてLANが登場した。これは同一構内で専用端末とメインフレーム、オフィスコンピュータ等の接続を可能にした。PCが業務用に普及すると、メインフレームやオフィスコンピュータの専用端末としての機能をPC環境で疑似的に提供する端末エミュレーターが登場した。端末エミュレーターは接続するメインフレームやオフィスコンピュータ毎の仕様に準拠する必要があったため、多くの種類の端末エミュレーターが存在した。

端末エミュレーターが登場した1980年代中頃はクライアントという概念は未だ存在しない。またPCは高機能化して、複数のプログラムの同時実行やLANを活用したファイル共有サービスやグループウェアのネットワークアプリケーションの実行環境へと発展していく。

一方、VAN（Value Added Network）は、自組織内に限定されずに地点を跨いでネットワークで接続して付加価値サービスを提供するものである。VANにより提供されるネットワークは、通信事業者により提供される電話回線や専用回線であった。VANサービスは、通信事業者、電気メーカー、情報サービス会社等により提供され、PCの機能を活かしたものであった。代表的なサービスとして、企業向けにはEDI（Electric Data Interchange）やコンピュータ資源の貸し出し、個人向けには所謂パソコン通信、電子掲示板や電子メール、データベース検索があった。残念なことにVANサービスは、インターネットの様に相互に接続されたネットワークではなかった。

VANサービスにおいてもセキュリティ管理の必要性は認識されており、認証操作にはユーザーID及びパスワードの入力が求められた。この情報の漏洩は不正課金を招くものとして注意喚起されていた[13]。1988年にはNEC社が提供するPC-VANのサービスでは利用者が電子掲示板に添付されていたバイナリ情報をダウンロードして実行することによりトロイの木馬型のマルウェアの感染が確認されている[14]。この形態のインシデントは当時斬新であったが、インターネット普及後、Webサイトにマルウェアが添付されている状況を彷彿させる。

4　オープンシステムにおけるクライアント

Microsoft社よりWindows3.1が1991年に、Windows NTが1994年に出荷され、この時期より本格的にクライアントとサーバーという対をなす構成形態が急速に普及した[15]。サーバーとはサービスを提供する構成であり、クライアントとはサーバーが提供するサービスを要求する構成である。この関係はメインフレームと専用端末も同等と見做すことも可能であるが、ここでいうクライアントの特性として、独立した処理能力を持っている点が挙げられる。サーバーに対して一方的に従の関係になることは無い。サーバー構成はUNIX系OSによるシステムでも実装可能であるが、当時はWintelという言葉が流行し、Microsoft社のWindows OSとIntel社CPUを使ったPC及びサーバー機によって、クライアントサーバーモデルは最盛期を迎えた[16]。Intel CPUを搭載して、Micro Channel Architecture（以下MCAと表記）またはその拡張版の規格に則ったハードウェアはクライアントサーバー構成パタンのデファクトスタンダードの位置付けとなり、周辺機器もこのMCAに準拠した。クライアントサーバーモデルで前提となるネットワークは、物理層としてイーサーネットのIEEE802.3規格及び通信プロトコルとしてTCP/IPプロトコルに収束していった。

クライアント/サーバー型アプリケーションの普及と共に個人にPCを割り当てる組織が増えた。専用端末にはデータを保管できないが、PCクライアントにはデータを保管することが可能となるため、PC所有者には、マルウェアの感染、データ漏洩の防止、PC本体及び周辺機器の紛失の予防策等の管理責任が伴う。オープンシステム化が進むことにより、OSやミドルウェア、CPU等の設計仕様は標準的なものに収束していく。結果として、多くのユーザーが利用するこれらの製品で一つの脆弱性が発見されると、社会的な影響も大きくなる状況を生むことになる。

5　インターネットに接続するクライアント

インターネットが普及すると企業は社内ネットワークと外部ネットワークの間にファイアウォール経由で接続してクライアントは組織外の情報資源の活用や組織を跨いだ情報交換や発信が可能となった。これらのインターネット上のアプリケーションでは、クライアント側のブラウザとWebサーバー間のアプリケーションでHTTPプロトコルを使って通信する構成設計が多用された。これは社外向けから組織内のアプリケーションにも広まっていった[17]。Webアプリケーション側に表示以外の機能を配置してクライアントはブラウザを利用することにより、クライアント/サーバー型アプリケーションの複雑な構成の管理の手間を省けること、メインフレームの様に処理をサーバー側に集中できること、文字データ以外に画像データも処理の対象となること等が評価された。その他インターネットを活用したサービスとして電子メールが挙げられる。これはsendmail、POP3、IMAP、MIMEの仕様に則ったメールサーバー及びクライアント側のメーラーによって実現されるものであり、インターネット及びメールサーバーに接続されているクライアントであればメールのやり取りが可能となる。メール本文の領域にはHTML形式の記述、ファイルの添付、Webページのリンクの追加が可能となっており、表現の自由度が高い。

社内ネットワークのアクセスに限定されていたクライアントはインターネットと接続することによりリスクも拡大した。メールに添付されたマルウェア、ワンクリックで不要な料金を請求するサイト等、インターネット上のサービスには様々な罠が仕掛けられた。ネットワークを介してクライアントに感染する2000年代初頭のマルウェアで特徴的な機能を持つ例としては、OutLookのアドレス帳を介して感染するワーム型のLoveletter[18]、PCでWebページを閲覧することにより感染するNimda [19]、ウイルスファイル自体をメールに添付して送信するSobig [20]等が挙げられる。クライアントPCは様々な技量のユーザーが操作するため、インシデントの対応には限界がある。攻撃者にとってクライアントへの攻撃はコストが低く、効果が大きい。これらの状況を踏まえると、クライアントを標的とした金銭目的のランサムウェア攻撃は、攻撃者にとって理に適った手口であり、今後も継続することが予想される[21]。

6　仮想化クライアント

クライアントの機能について考えると、ユーザーの操作インタフェースとなる物理的なクライアント装置にプログラム及びデータ含む論理的な要素が配置されていることは必要条件ではない。

ここではその代表的な仮想化方式として、サーバー上で仮想化されたクライアント環境を利用する仮想デスクトップ基盤（Virtual Desktop Infrastructure　以下VDIと表記）を取り上げる。VDIでは専用のサーバーおよび制御用のユーティリティが前提となる。クライアントは画面表示以外の機能は原則として持たず、サーバー上の仮想クライアントでユーザーは業務操作を実行する。メインフレームまたはオフィスコンピュータの専用端末が入出力装置の機能に限定される状況と同等であるため、クライアント/サーバー型システムのエミュレーター版と捉えることもできる。物理クライアントにデータが保存されないことは、結果として物理的なクライアント内部のデータの漏洩予防策に繋がる。但し、仮想化クライアント環境へのアクセス時の認証についてはクライアント/サーバー型システムの機能と変わることはない。

7　インターネット経由で社内ネットワークに接続するクライアント

コロナ禍により、社内ネットワークが接続されていない場所でも業務システムの利用がより多くのユーザーに対して求められた。この要件は、インターネット経由で社内ネットワークにアクセスするVPNやリモートデスクトップまたはインターネットを介したクラウドサービス等で実装可能である。コロナ禍においてはテレワーク推進の目的で、これらの解決策がとられた。業務システムの早急なクラウドサービス化の実現は困難であること、システム環境の変更がほぼ不要であることも手伝って、VPN方式が多く採用された[22]。しかしながら、大量の従業員によるVPN構成の一斉アクセスによるネットワーク遅延、VPN機器の脆弱性等の問題が発生したこともあり、将来的に労働環境の柔軟性を持たせるという視点からは最適の解法となる訳ではない。一方でコロナ禍によるテレワークの必要性が高まる以前から、ZTAなる概念が存在した。既にGoogle社ではこの考え

に基づいて自社のセキュリティ管理に関わる機能が実装されている[23]。

Ⅲ　クライアント構成のセキュリティ対策

この章ではⅡ章で取りあげたクライアント構成のセキュリティインシデントについてZTAの概念の実装方式について考察する。

1　ZTAの解釈

ゼロトラストという概念は2010年にForester Research社のジョン・キンダーバーグ（John Kindervag）氏が提唱したものであるが[24]、2020年8月にNISTから「SP 800-207 Zero Trust Architecture」としてその定義が公開された。その中で次の7つの原則が記載されている[25]。

第1原則　データソースとコンピュータサービスは、全てリソースと見なす
第2原則　「ネットワークの場所」に関係なく、通信は全て保護される
第3原則　組織のリソースへのアクセスは、全て個別のセッションごとに許可される
第4原則　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
第5原則　組織が保有するデバイスは、全て正しくセキュリティが保たれているように継続的に監視する
第6原則　リソースの認証と認可は、全てアクセスが許可される前に動的かつ厳密に実施される
第7原則　資産・ネットワーク・通信の状態について可能な限り多くの情報を収集し、セキュリティを高めるために利用する

VPNを適用したシステム環境は境界防御に特化しており、境界を突破された際のリスクや内部犯行によるリスクへの対策として不十分である。実際に、VPNの脆弱性は複数報告されている[26]。VPNを通過して組織内ネットワークに侵入されることは、公開サーバーに限定されていたポートスキャンの初期段階の攻撃が組織内ネットワーク上の各構成にまで及ぶことと同等である。その後は組織内のネットワークへのアクセス、盗聴、資格情報の窃取、なりすまし、個人情報の窃取等の被害の拡散が予想される[27]。

VPNの問題以外にPPAPの問題をZTAの観点から考えると、別の課題も見えてくる。PPAP問題とはメールを介して暗号化されたファイルとパスワードを別々に送信する操作を指し、インターネット経路の途中でのデータ漏洩及び暗号化されたことによりマルウェアの検知が不可となる問題等が挙げられている。本論文執筆時点では具体的な解決案について策定段階の組織が多い[28]。

ゼロトラストの第1原則について考えると、メールに添付されるファイルは送信者と受信者の共有すべきデータであるが、その保管場所はメールの機能特性も手伝って動的である。経由箇所も含めれば、データは送受信に関わったメールサーバー及びクライアントに保管される。メールによる添付ファイルの送受信は、メールサーバー自体のアクセスは社外も含めて様々な地点から組織内

の利用者がアクセスするためセキュリティ管理が考慮されているとはいえ、一旦誤送信やなりすましが発生した場合にはデータの安全性が担保されない。例として、添付ファイル付きのメールは受信者の判断で宛先を設定して転送できるようなケースを想定すると、データの公開範囲やアクセス制御の適正化の観点からは決して好ましいものではない。

2　クライアントデバイスの認証

ここからはZTAに則った構成設計で重要なポイントとなる認証機能について考察する。前提としてZTAの概念に従い、クライアントは多様なネットワークを介して接続されるものと考える。認証操作は、クライアント物理構成を対象としたデバイス認証とアプリケーションの操作者を対象とするユーザー認証に分類される。

デバイス認証には、クライアント単体で完結するローカル型とネットワーク経由で管理サーバーが認証するネットワーク型に分類できる。ローカル型は、クライアントデバイスにおけるPIN入力や生体認証が該当する。PCについてはBIOSのハードウェア・パスワード機能もこれに含む。ネットワーク型はクライアントに接続した管理サーバーで認証処理を行う。例としてWindowsシステムのドメインコントローラ―及びアクティブディレクトリによる制御が挙げられる。特定の管理ドメインの範囲でデバイスを管理できること[29]、紛失時に当該デバイスを操作不可とすることも可能である[30]。ネットワーク型のMicrosoft社のアクティブディレクトリは、MS ダイナミックアクセス制御としてユーザー認証の結果のデータに紐づけてリソースのアクセス制御も可能である[31]。ネットワーク制御のデバイス認証はUEM（Unified Endpoint Management）製品の機能で実装可能で、MobileIron社 のMobileIron UEM[32]、VMWare社 のVMware Workspace ONE[33]、IBM社 のMaaS360[34]、BlackBerry社のBlackBerry UEM[35]ある。MDM（Mobile Device Manager）はデバイス内のソフトウェアや環境設定に関する管理や監視の機能を提供するが、UEMはこの機能を内包し、デバイスのアクセス制御機能も提供する。

デバイス認証はデバイスを識別して管理する目的で行われるもので本質的にはユーザー認証と異なるが、各ユーザーがデバイスを占有する場合はデバイス認証とユーザー認証を統合させることも可能である。強力な認証機能が必要な場合は、公開鍵暗号基盤の技術を利用して、各ユーザーに割り当てられたクライアントデバイスに秘密鍵を埋め込み、サーバー側の公開鍵と連携した認証[36]を行う方式が推奨される。クライアントデバイスでは、秘密鍵が簡単に搬出できないよう対応を要する。その他にデバイスのIPアドレス及びMACアドレスを検証する方式も挙げられるが、いずれも変更可能かつサーバー上に比較データを保持するため、これらが盗まれたり改竄されたりするリスクもある。PCについては、過去インテル社よりCPUの個体識別情報をCPU idとして参照する機能が実装されていたが、現在は提供されていない[37]。紛失や盗難のリスクに配慮すると、デバイス認証は必須である。ユーザー認証とデバイス認証を独立させるメリットとしては、各々の認証資格に対して条件を設定して権限を付与することができる点である。

3　ユーザー認証

ZTAの概念を考慮して強固な認証基盤を構築しようとした場合、FIDO2（Fast Identity Online）の規約に準拠する認証操作及びPCのマザーボード上に装填されるセキュリティ関連の機能を提供するTrusted Platform Module（以降TPMと表記）[38]の活用が効果的である。

ZTAの第5原則と第6原則の条件に従うと、デバイスやユーザーからのアクセスの都度検証が求められる。前節で挙げた公開鍵暗号基盤の活用が考えられるが、FIDOによる認証はこれを実装する技術規約である。FIDOとはFIDOアライアンスが提唱する公開鍵基盤を利用した認証機能に関する規約で、W3Cの規約を補完して別途認証処理に関するCTAP（Client-to-Authenticator Protocols）を規定するものである[39]。複数の規格が存在するが、事前に公開鍵による鍵ペアが生成され、クライアント側に秘密鍵が保持される点は共通である。FIDO UAF（User Application Framework）は当規約に従うモバイルデバイスを対象に、指紋、顔、虹彩等の生体認証を組み合わせたものである。認証要求を受け取るとデバイス上でこれらデバイスの認証操作が求められる。FIDO U2F（Universal 2nd Factor）は、モバイルデバイスの条件はないが規約に則った外部デバイスに秘密鍵が保管されていることが前提となる。パスワード入力による認証操作後、専用デバイス内の秘密鍵のデータを使って認証処理を行う。FIDO2は、PCまたはモバイルデバイスが本体内または外部デバイスの認証装置と連携してブラウザを介して認証処理を行う。FIDO規格に従った認証システムでは、システム管理者はサーバー環境にパスワード等の情報を保有しない。サーバーからFIDO認証の要求受け取るとクライアントデバイスでパスコード入力等の認証操作が発生する。

FIDO2に対応したサービスやサイトにはMicrosoft Azure、Yahoo Japan、GitHub等がある[40]。FIDO2にはGoogle Chrome、Mozilla FireFox、Microsoft Edge、Safariのブラウザが、Windows、iOS、AndroidのOSが対応している[41]。外付けのデバイスとしてUSB接続型のFIDO2対応セキュリティーキーも利用できる。このデバイスには指紋認読取り機構を含む製品もある[42]。

Microsoft社は、生体認証データによって完結する「Windows hello」なるローカル認証の機能を提供していたが、この機能は2019年にFIDO2の認定を得ている[43]。2018年には、Microsoft社のAlex Simons氏はWindowsサインオン時のパスワード操作を不要とする処理の実現方式について、秘密鍵をTPMに格納することに言及している[44]。既にAzure Active DirectoryはFIDO2に対応しており、Windows11の導入前提条件には、TPM 2.0の機構を含むハードウェアということが含まれている[45]。Microsoft社の認証機能に関する一貫した戦略がうかがえる。

4　外部からの攻撃者による不正操作の防止

デバイス認証、ユーザー認証がより強固に管理されることにより、なりすまし行為や資格情報剥奪の防止に役立つ。但し、外部ネットワークからの攻撃者によって組織内ユーザーのメールやWebサイトの操作を介したマルウェア感染やフィッシング詐欺に対して効果は限定的である。FIDO認証を利用したとしても、マルウェア感染後に遠隔操作を許すと、権限悪用の可能性が懸念

される。クライアントデバイスの管理主体はユーザーであることを勘案して外部からの攻撃に対しては別途検討が必要である。

初期段階の攻撃検知は、時々刻々と変化する脆弱性と攻撃パタンを認識することが前提である。組織内で攻撃に関する情報を把握して適切な対応をとることは、特定の組織に標的を絞った攻撃が多いこと[46]、攻撃技術が高まったこと[47]により、技術的に困難になりつつある。技術面の補完を考えると、セキュリティサービスベンダが提供するSIEM（Security Incident and Event Management）の利用が推奨される[48]。

被害を完全に抑えることができないことを想定して、情報流失や不正出金が発生したインシデントを検出する出口対策も検討の余地がある[49]。また、インシデント発生後の調査ではクライアントデバイスを含めてOS及びアプリケーションのログの保管および改ざん防止が必須である。ログ取得の対象となる機能、ログの詳細レベル、ログの保存期間の判断に加えて、攻撃時にログを改竄または消去されないよう管理者権限の不正利用にも注意すべきである[50]。

5　内部犯行による不正操作の防止

組織内のメンバーによる不正行為もセキュリティ管理上大きな課題である[51]。内部犯行では予め資格情報を持ってアプリケーションを操作するため、システム処理に例外が発生する訳ではなく別途検知機能が必要となる。本要件には，攻撃者や内部犯行のアプリケーション操作と平常時の操作を人工知能を用いて判別するUEBA（User and Entity Behavior Analytics）なる技術が適用可能で[52]、製品としては、RSA NetWitness Platform[53]、FireEye Helix[54]がある。

内部犯行に対しては、セキュリティ管理の視点からワークフローシステムの採用も解決の一助となる。一連の業務処理で特定の業務範囲について自分のアカウントで操作するため犯意が削がれることが期待できる。万一インシデントが発生しても、認証制御が厳密に管理されていれば確定的な操作証跡は残る。ワークフローシステムの難点としては、業務の範囲が動的に変化する場合は適用が困難であることである。例として電子メールで重要情報をやり取りする様な業務が挙げられる。

6　デバイス構成及びネットワークを介したサービスの管理

クライアントデバイスはユーザーが主体的に管理するものであり、システム設計及び組織の運用規約に依存するが、システム管理者の対応は限定されることもある。ZTAの第5原則を勘案すると、クライアントデバイスや周辺機器の紛失、クラウドストレージの利用等の管理も検討を要する。

クライアントデバイスの紛失対策としてはデバイス認証機能が効果的である。更に物理的なディスク機構内データの読み取り防止を考慮するならば、ディスク機構に保存されるデータを暗号化する対策が挙げられる[55]。暗号化キーは安全性が高いTPM内に保存可能である[56]。

データ保存が可能でクライアントデバイスに装着するUSBメモリ、外付けSSDディスクは紛失のリスクが伴うものであり、その要件を本質的に再考すべきである。代替策としてのクラウド上の

ストレージサービスの利用に際してはZTA第5原則に従い、システム管理者が管理可能であることが条件である[57]。シャドーITとして利用されていたクラウドサービスでアカウントが乗っ取られ、修復が困難になった事例も発生している[58]。

製品としてのクライアントデバイスのハードウェア及び導入する製品ソフトウェアにも注意を要する。最近の例としてはSolarWinds社のシステム管理ツールがサプライチェーン攻撃によって不正アクセスをもたらした[59]。製品においても安全が確保されている訳ではない。国内でも防衛省が情報セキュリティ基準を米国の「NIST SP800-171」と同程度強化する改正を行うことを検討している[60]。

Ⅳ　今後の課題と展望

コロナ禍に端を発したテレワーク活用の状況からZTAに基づくセキュリティ管理についてクライアント構成を軸に考察してきた。ZTAはセキュリティ管理の視点で提示された概念の提示であり、セキュリティ要件は組織ごとに異なる。米国のセキュリティサービスベンダの調査によれば、ZTAの実装段階について、ロードマップ構築中38%、準備未了26%、未着手11%であり、既に実施しているとの回答は20%に止まるとの結果が出ている[61]。一方でインターネット空間では常に標的を探し出そうとする試みがなされている[62]。昨今のサイバー攻撃は金銭目当てのものが多く、規模に拘わらず利益を生むと判断された組織が標的となることが予想される[63]。

インターネットを基盤とした情報システムは、文字情報中心のレガシーシステムを凌駕して様々な可能性を現実のものにしてきた。ビジネスモデルを進化させ、労働形態に多様性をもたらした。テレワークやクラウドサービスの活用により、組織内のネットワークとインターネットとの境界は曖昧になった。更にコロナ禍は技術活用の歩を速めたことになる。クライアントは組織内ネットワークに存在する構成からインターネット上の独立した構成へと変化を遂げつつある。攻撃者はそのような状況を好機と捉える。ZTAの登場は技術的な進化の必然と解釈することもできるが、現在の状況を打開するに十分な材料となるであろう。

---

[1] 緊急事態宣言（7都府県）後のテレワークの実態について、全国2.5万人規模の調査結果を発表　パーソル総合研究所　2020/04/17（2021.12.14閲覧）
https://rc.persol-group.co.jp/news/202004170001.html

[2] リモート接続ねらうサイバー攻撃が急増 テレワーク増加で NHK 2020年11月12日（2021.12.14閲覧）
https://www3.nhk.or.jp/news/html/20201112/k10012708711000.html

[3] システム構成（集中と分散）の歴史 木暮　仁（2021.12.14閲覧）
http://www.kogures.com/hitoshi/history/shuchu-bunsan/index.html

[4] 進化する銀行システム　技術評論社　2017年2月17日　星野武史　第9章　IMSというミドルウェア　P.88

[5] VAX & VMS ものがたり Hewlett Packerd Enterprise（2021.12.14閲覧）
https://h50146.www5.hpe.com/products/software/oe/openvms/history/vaxvms20/pdf/vmsbookj.pdf
[6] ネットワークの発達と企業情報システム 海老澤信一　経営論集 第 17 巻第 1 号 2007 年 183 ～ 197 頁
https://www.u-bunkyo.ac.jp/center/library/image/ba2007_183-197.PDF
[7] コンピュータ犯罪　秀潤社　ドン・B・パーカー 1977年2月15日　P.81 8 元コンピュータ犯　ジェリーシュナイダー
[8] わが国における情報ネットワーク関連判例の動向　岡村久道（2021.12.14閲覧）
https://www.soumu.go.jp/joho_tsusin/policyreports/chousa/yubikitasu_j/pdf/r-wg_040301_2_3.pdf
[9] 大阪地方裁判所 昭和５６年（わ）４７５３号 判決
https://daihanrei.com/l/大阪地方裁判所 昭和５６年（わ）４７５３号 判決
[10] 【プロローグ】あなたが初めて買ったのはいつ？パソコンは「マニア向け」から「生活の必需品」に　日経XTECH 2014.03.24（2021.12.14閲覧）
https://xtech.nikkei.com/it/pc/article/basic/20131028/1110104/
[11] ウイルスの歴史 G DATA（2021.12.14閲覧）
https://www.gdata.co.jp/labs/history
[12] 世界初のランサムウェアは1989年にフロッピーディスクで広められた 2017年04月14日（2021.12.14閲覧）
https://gigazine.net/news/20170414-world-first-ransomware/
[13] VANがわかった!!　すがやみつる　講談社　1986年5月28日　P.154 IDナンバーとパスワード
[14] ウイルスの歴史 G DATA（2021.12.14閲覧）
https://www.gdata.co.jp/labs/history
[15] 日本のコンピュータ PCサーバ　誕生と発展の歴史 IPSJ Computer Museum
http://museum.ipsj.or.jp/computer/pc/history.html
[16] 令和元年版　情報通信白書 メインフレーム及びサーバーの国内出荷台数　総務省（2021.12.14閲覧）
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd111140.html
[17] イントラネットとは? インターネットやエクストラネットとの違い NTT Communications（2021.12.14閲覧）
https://www.ntt.com/business/services/network/internet-connect/ocn-business/bocn/knowledge/archive_108.html
[18] VBS/LOVELETTERに関する対策について IPA　2000年 5月 7日（2021.12.14閲覧）
https://www.ipa.go.jp/security/topics/vbs-loveletter.html
[19] 新種ウイルス「W32/Nimda」に関する情報　IPA　2001年 9月 19日（2021.12.14閲覧）
https://www.ipa.go.jp/security/topics/newvirus/nimda.html
[20] 新種ウイルス「W32/Sobig」に関する情報　IPA　2003年 1月 16日（2021.12.14閲覧）
https://www.ipa.go.jp/security/topics/newvirus/sobig.html
[21] メール詐欺を中核とするサイバー攻撃――Office 365ユーザーをどうやって守っていくか @IT 2017年10月16日（2021.12.14閲覧）
https://atmarkit.itmedia.co.jp/ait/articles/1710/16/news004.html
[22] テレワーク導入組織に対するセキュリティ対策意識調査 P.13 テレワーク環境＜社内ネットワーク/社内ファイルサーバー＞ 2021年06月21日 デジタルアーツ株式会社（2021.12.14閲覧）
https://www.daj.jp/company/release/common/data/2021/062101_reference.pdf
[23] BeyondCorp Enterprise: より安全なコンピューティング時代の到来 2021年1月27日　Google（2021.12.14閲覧）
https://cloud.google.com/blog/ja/products/identity-security/introducing-beyondcorp-enterprise
[24] John Kindervag of Forrester Research Discusses “Zero-Trust Architecture” YouTube 2011年4月8日（2021.12.14閲覧）
https://www.youtube.com/watch?v=0GbqUxBYvyo

[25] NIST SP800-207「ゼロトラスト・アーキテクチャ」の解説と日本語訳 pwc 2020年12月20日（2021.12.14閲覧）
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/zero-trust-architecture-jp.html

[26] コンピュータウイルス・不正アクセスの届出事例［2021 年上半期（1 月～6 月）］独立行政法人情報処理推進機構 セキュリティセンター
2021年 8月23日　2-4. 脆弱性や設定不備を悪用された不正アクセス（2021.12.14閲覧）
https://www.ipa.go.jp/files/000093083.pdf

[27] 小規模サイト管理者向け セキュリティ対策マニュアル IPA ISEC P.12 1.2 ポートスキャン（2021.12.14閲覧）
https://www.ipa.go.jp/security/fy12/contents/crack/soho/soho.pdf

[28] できることから考える PPAP の現状と代替案について HENNGE（2021.12.14閲覧）
https://hennge.com/jp/service/one/white-paper/ppap.html

[29] 認証制御システムにより管理対象デバイスは追加定義される。次の製品の例が挙げられる。
TeamViewerアカウントの「信頼できるデバイス」「デバイス認証」について　TeamViewer 2020年12月24日（2021.12.14閲覧）
https://community.teamviewer.com/Japanese/kb/articles/13954-teamviewerアカウントの-信頼できるデバイス-デバイス認証-について
信頼できるパソコンを追加または削除する　Google（2021.12.14閲覧）
https://support.google.com/accounts/answer/2544838?hl=ja&co=GENIE.Platform%3DDesktop
Device Activation salesforce（2021.12.14閲覧）
https://help.salesforce.com/s/articleView?id=sf.security_overview_identity_verification.htm&type=5
信頼済みデバイスを Microsoft アカウントに追加する Microsoft（2021.12.14閲覧）
https://support.microsoft.com/ja-jp/account-billing/信頼済みデバイスを-microsoft-アカウントに追加する-fe3860c8-bc04-9770-e218-b4fd6b767f4b

[30] デバイスを無効化する操作には次の例がある。
Azure portal を使用してデバイス ID を管理する Microsoft（2021.12.14閲覧）
https://docs.microsoft.com/ja-jp/azure/active-directory/devices/device-management-azure-portal
MFA デバイスの無効化 Amazon（2021.12.14閲覧）
https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa_disable.html
IBM MaaS360 Mobile Device Management（SaaS）デバイスのオペレーティング・システムによるデバイス・アクション（2021.12.14閲覧）
https://www.ibm.com/docs/ja/maas360?topic=inventory-device-actions-by-device-operating-system

[31] ダイナミック アクセス制御の概要 Microsoft 2021年11月8日（2021.12.14閲覧）
https://docs.microsoft.com/ja-jp/windows-server/identity/solution-guides/dynamic-access-control-overview

[32] MobileIron 統合エンドポイント管理 MobileIron（2021.12.14閲覧）
https://www.mobileiron.com/sites/default/files/2019-01/MobileIron-UEM_Datasheet_JA_A4_v2.2.pdf

[33] Workspace ONE 統合エンドポイント管理（UEM）（2021.12.14閲覧）
https://www.vmware.com/jp/products/workspace-one/unified-endpoint-management.html

[34] MaaS360 IBM（2021.12.14閲覧）
https://www.ibm.com/docs/ja/security-verify?topic=integrations-maas360

[35] BlackBerry UEM（2021.12.14閲覧）
https://www.blackberry.com/ja/jp/products/blackberry-uem

[36] Internet Engineering Task Force（IETF） Request for Comments: 7616　R. Shekh-Yusef, Ed.（2021.12.14閲覧）
HTTP Digest Access Authentication Internet Engineering Task Force（IETF）
https://datatracker.ietf.org/doc/html/rfc7616

[37] インテル、CPUへの識別ID埋め込み案を撤回　ASCII 1999年01月27日（2021.12.14閲覧）
https://ascii.jp/elem/000/000/314/314427/
[38] Trusted Platform Modules Strengthen User and Platform Authenticity 2005年1月（2021.12.14閲覧）
https://trustedcomputinggroup.org/resource/trusted-platform-modules-strengthen-user-and-platform-authenticity/
[39] FIDO Alliance Specifications Overview FIDO Alliance　FIDO Alliance（2021.12.14閲覧）
https://fidoalliance.org/specifications/
[40] FIDO2 に対応したサイトの例は次の通り。
Microsoft　Azure
FIDO2 パスワードレス認証のブラウザー サポート（2021.12.14閲覧）
https://docs.microsoft.com/ja-jp/azure/active-directory/authentication/fido2-compatibility
Yahoo Japan
Yahoo! JAPANでの生体認証の取り組み（FIDO2サーバーの仕組みについて）（2021.12.14閲覧）
https://techblog.yahoo.co.jp/advent-calendar-2018/webauthn/
GitHub
GitHub supports Web Authentication（WebAuthn）for security keys（2021.12.14閲覧）
https://github.blog/2019-08-21-github-supports-webauthn-for-security-keys/
[41] FIDO2: Web Authentication（WebAuthn）FIDO Alliance 2020/6/29（2021.12.14閲覧）
https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/
[42] 利便性と高セキュリティ性を備えたFIDO2対応デバイスとは？ @IT 2019年04月23日（2021.12.14閲覧）
https://atmarkit.itmedia.co.jp/ait/articles/1904/24/news008.html
[43] Microsoft Achieves FIDO2 Certification for Windows Hello FIDO Alliance　2019年3月6日（2021.12.14閲覧）
https://fidoalliance.org/microsoft-achieves-fido2-certification-for-windows-hello/
[44] Now you can sign into your Microsoft Account with your face or a security key—no password needed PC World 2018年11月20日（2021.12.14閲覧）
https://www.pcworld.com/article/402951/microsoft-account-no-password-sign-in.html
[45] Windows 11 の仕様、機能、コンピューターの要件を確認する Microsoft（2021.12.14閲覧）
https://www.microsoft.com/ja-jp/windows/windows-11-specifications
[46] 令和2年におけるサイバー空間をめぐる脅威の情勢等について　警察庁　2021年3月4日（2021.12.14閲覧）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_cyber_jousei.pdf
[47] 白書2021に見る情報セキュリティの動向　IPA セキュリティセンター セキュリティ対策推進部 セキュリティ分析グループ 2021年10月（2021.12.14閲覧）
https://www.ipa.go.jp/files/000093736.pdf
[48] SIEMセキュリティ入門：進化と次世代機能 macnica（2021.12.14閲覧）
https://www.macnica.co.jp/business/security/manufacturers/exabeam/feature_07.html
[49] ポイントは出口対策、入り口やデータ保護対策も大事　相馬 基邦　日経XTECH　2012.07.06（2021.12.14閲覧）
https://xtech.nikkei.com/it/article/COLUMN/20120617/403227/
[50] ［クライアント編］監視エージェントを使い，操作内容を詳細に記録する　榊原康　日経XTECH 2008.05.15（2021.12.14閲覧）
https://xtech.nikkei.com/it/article/COLUMN/20080403/297901/
[51] 情報セキュリティ10大脅威 2021（2021.12.14閲覧）
https://www.ipa.go.jp/security/vuln/10threats2021.html
[52] UEBAとは FIREEYE（2021.12.14閲覧）
https://www.fireeye.jp/products/helix/what-is-ueba.html
[53] NetWitness® Platform Documentation（Japanese）RSA（2021.12.14閲覧）

https://community.rsa.com/t5/netwitness-platform/nw-netwitness-platformの概要/ta-p/527497

[54] FireEye HelixとUEBA（2021.12.14閲覧）
https://www.fireeye.jp/content/dam/fireeye-www/regional/ja_JP/products/pdfs/ds-fe-helix-ueba.pdf

[55] ドライブ全体暗号化システム　IPA（2021.12.14閲覧）
https://www.ipa.go.jp/security/it-product/fd-enc

[56] ソフトウェア完全ディスク暗号化のプロテクションプロファイル ハードディスクの盗難・紛失リスクの低減 IPA 技術本部 セキュリティセンター
情報セキュリティ認証室 2013年11月12日（2021.12.14閲覧）

[57] ファイルはクラウドに置く XTECH 原 隆 2015年7月9日（2021.12.14閲覧）
https://xtech.nikkei.com/it/atcl/ncd/15/062600028/

[58] フィッシング詐欺による患者情報漏洩インシデントの発生について　岡山大学病院　2021年8月4日（2021.12.14閲覧）https://www.okayama-u.ac.jp/user/hospital/news/detail284.html

[59] SolarWinds was a cybersecurity wakeup call, says Microsoft's president Brad Smith cnet 2021年10月20日（2021.12.14閲覧）
https://www.cnet.com/tech/services-and-software/microsofts-brad-smith-says-solarwinds-was-a-cybersecurity-wakeup-call/

[60] 防衛装備庁 技術シンポジウム2019発表要旨　防衛装備庁における情報セキュリティ基準の改正に係る取組 前野明　2021年11月12日（2021.12.14閲覧）
https://www.mod.go.jp/atla/research/ats2019/index.html

[61] 2021 ゼロトラスト　プログレスレポート ivanti（2021.12.14閲覧）
https://www.ivanti.co.jp/lp/security/reports/zero-trust-progress-report

[62] インターネット定点観測レポート（2021年 7〜9月）JPCERT/CC 2021年10月19日（2021.12.14閲覧）
https://www.jpcert.or.jp/tsubame/report/report202107-09.html

[63] ランサムウェア被害のコスト、2031年には28兆円超に　ZDNet Japan 2021年6月11日（2021.12.14閲覧）
https://japan.zdnet.com/article/35172207/