物理的セキュリティと情報セキュリティの融合

株式会社フォーバルクリエーティブ
上席テクニカルスペシャリスト　馬場　重通

1. 言葉の意味を整理する

ファイアウォールやウィルスワクチンは､「情報セキュリティ」と呼ばれるものであり、TCP/IPパケット通信を利用したバーチャルな論理的世界において、情報資産を様々な攻撃から防衛することを目的にしています。

それでは「物理的セキュリティ」とは、一体どのようなものなのでしょうか？

実はコンピュータネットワークは、バーチャルな論理的世界の中で動作しているとはいうものの、何も無い空間に存在しているわけではなく、数多くのサーバやクライアントパソコン上にソフトウェアをインストールし、それらをネットワークで結び合わせることで、初めてインターネットなどの巨大なバーチャル空間が形成されるのです。

コンピュータは、人間の心と体の関係に似ています。人間の心は、バーチャル空間で様々に想像を巡らすことが可能ですが、実はその想像は、体という物質的なものが土台となって成り立っています。体という物理的な実体がこの世に存在しなければ、魂も存在できないという意味です。

以上のように、バーチャルなコンピュータネットワークは、サーバやパソコン、ハブやルータなどの物理的実体がこの世に存在して、始めて存在することが可能となります。

物理的セキュリティとは、実体であるサーバやパソコン、ハブやルータなどの機器そのものを不審者から守ることを目的にしています。

2. 灯台下暗しになっていないか？

夜間に不審者が会社の中に侵入し、営業用のパソコンを持ち逃げされたという事件は毎日のように発生しています。

ファイアウォールや暗号技術などを駆使して、外部からの不正アクセスを完璧なまでに防衛することに熱心なシステム管理者は数多くおりますが、サーバルームやビルの建物の中に不正侵入されないように扉に鍵を取り付けたり、ICカード認証装置などの出入管理システムの導入を考える管理者は、ほとんどいないのです。よって上記のような事件が多発することとなり、いとも簡単に個人情報や機密情報が盗難に遭い、また情報システムが破壊されてしまうのです。

3. 先ずはルーピングが基本中の基本

物理的セキュリティは、部屋の扉に鍵を掛け、不審者や部外者が勝手に立ち入ることができないようにすることが基本です。

しかし近年のオフィスは、オープンフラットが好まれる傾向にあり、壁も柱も敷居も無い、だだっ広く見通しの良い環境が発達してきました。

このようなオープンフラットオフィスは、社員同士のコミュニケーションを深め、企業活動発展のために大きく貢献してきたと言えます。

しかしその反面、営業部や経理部、人事部や開発部、情報システム部などが何の敷居も無いままに1つのフロアに同居していることから、顧客や宅配の業者、ビル清掃の人間が、容易にサーバやパソコンなどの情報システムに触れることができる環境となってしまいました。

このようなオープンフラットなオフィス環境は、部外者からの攻撃だけでなく、社内の人間によるパソコンの窃盗や個人情報の盗難も容易にしています。

2005年4月1日の個人情報保護法本格施行以降、日本では、オープンフラットオフィスが急速に見直され、各部署を単位としてパーティションで壁を立て部屋を作り、扉に鍵を掛けて、社内の人間でも勝手に他の部署に立ち入ることができないように、オフィス環境の改良が進められています。

以上のように、部署単位やセキュリティレベルの必要強度単位毎にパーティションで部屋を作ること

をルーピングと呼んでおり、ルーピングされた各オフィスエリアのことをセキュリティエリアと呼んでいます。

これはファイアウォールのパケット通過ルールの設定に、多少似ているところがあります。

4. セキュリティエリアにはセキュリティレベル（セキュリティ強度）の設定が不可欠

壁と扉を設置してセキュリティエリアが出来上がったら、次にそれぞれのセキュリティエリア（部屋）の重要度がどのくらいあるのかを、4段階のセキュリティレベルで色分けします。

例えば、受付や商談コーナー、喫茶室などは、お客様や業者など、社外の人間が主に利用する場所ですので、扉は常に開放しておくべきであり、特別に厳重なセキュリティを施す必要はありません。

この逆に、サーバルームやマシンルームなど大量の個人情報や機密情報が管理され、情報システムの中枢を担うデータベースサーバが管理されている部屋などは、例えシステム管理者であっても、限られた数人の人間しか立ち入ることができないよう、厳重なセキュリティシステムを設置する必要があるのです。

以下にセキュリティレベルを設定するための一例を示します。

要度レベル	内　　容	対　　策
レベル4	**サーバルーム、金庫室など：** アプリケーションサーバやデータベースサーバなど、情報システムの中核を守る。特にデータベースに記録されている大量の個人情報を一度に持ち出されるのを阻止する。	内部犯罪対策
レベル3	**研究開発部、経理部、人事部など：** 未発表新製品、特許申請前技術、財務諸表、人事評価情報など、会社を維持して行く上で極めて重要な情報を守る。	内部犯罪対策
レベル2	**一般社員が働く職場：** 社外の人が侵入し、各部署が個人情報や業務書類が勝手に持ち出されないようにする。	外部犯罪対策
レベル1	**受付や商談コーナー、オープンスペースなど：** 社外の人間が侵入しても問題のないリア。	NON セキュリティ

次の図は、サーバルーム内において、サーバの種類や情報の重要性に応じ、さらに3つのセキュリティレベルを設定し、エリアを区分けした図面です。

エリアの重要度に応じて、扉の鍵を解錠するための個人認証装置は、

レベル3：指紋認証装置

レベル2：ＩＣカード認証装置

レベル1：パスワード認証装置

と3種類が用意されています。

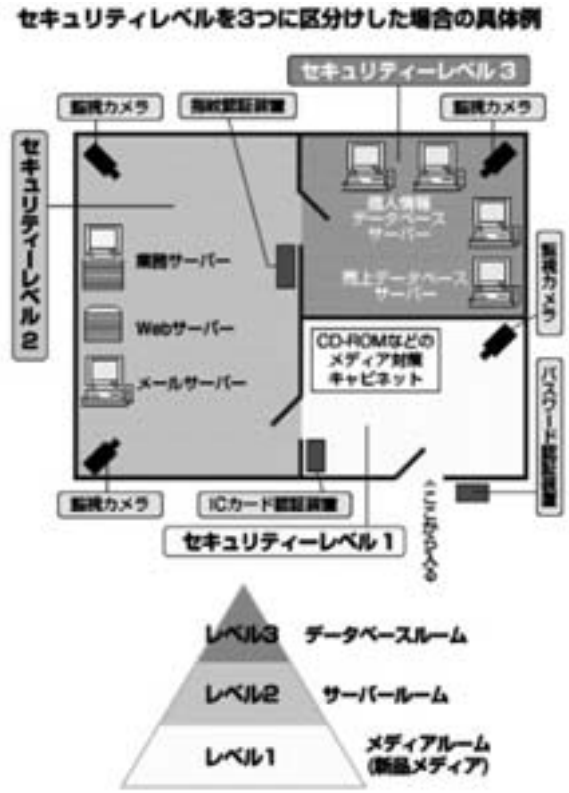
この図面で気をつけなければいけない点は、セキュリティレベルの重要度に応じて、エリアを入れ子状に設計するという点です。

例えばセキュリティレベル2エリアに進入する場合には、レベル1エリアからしか入ることができないように扉の位置を設計します。またレベル3エリアへ進入する場合には、レベル2エリアからしか入れないようにするのです。

このような入れ子状に建物を設計をすることにより、

レベル１の進入権限を持つもの：
パスワードを知っている。
レベル２の進入権限を持つもの：
パスワードを知っており、かつＩＣカードを所持している。
レベル３の侵入権限を持つもの：
パスワードを知っており、かつＩＣカードを所持している。なお且つ指紋を登録している。

となり、個人認証手段が積み上げられ、要求されるセキュリティレベルに応じたセキュリティ精度が確立されるのです。



5. 個人認証装置の選定方法

セキュリティエリアのレベルが上がれば上がるほど、成り済ましができない、本人を確実に確認できる最新な個人認証装置を導入する必要があります。個人認証装置の選定は、各セキュリティエリアの扉１つ１つに対して、入念に検討を進める必要があります。

各セキュリティエリアは入れ子状に設計し、セキュリティレベルが上がれば上がるほど、低位レベルエリア、中位レベルエリア、高位レベルエリア、最高位レベルエリアへと進入するように間取りの設計を行います。しかし、建物によっては、必ずしも前述のような理想的な間取りを設計できるとは限りません。低位レベルエリアからいきなり最高位レベルエリアへ進入する扉を設置しなければならないケースも多々あります。このような場合には、段々とレベルの高い個人認証装置を１台ずつ設置していく入れ子方式ではなくて、１枚の扉に対して複数の個人認証装置を設置する必要が出てきます。

それぞれのセキュリティレベルに応じて、どのような個人認証装置を設置したらよいか、以下に目安を示します。

セキュリティレベル	個人認証装置	扉の特徴	適用箇所
レベル 4	非接触 IC カード + 生体認証 （指紋認証など） + 二重扉	社内においては、最重要機密エリア。進入できる人間は極めて少人数に限られる。個人認証を確実に行う他に、扉を開けた隙に他の人間がなだれ込んでしまわないように、二重扉の導入を検討しましょう。	サーバルーム、 コンピュータールーム
レベル 3	非接触 IC カード + 生体認証 （指紋認証など）	全ての従業員が進入できるエリアではない。そのため、このエリアへの出入りは多くはないが、重要な個人情報などが格納されているので、少し時間が掛かっても個人認証は確実に行う必要がある。また入室の他、部屋から出るときにも個人認証を行い、退室履歴を取るようにしましょう。	ファイルや台帳、アンケート用紙や CD-ROM 等、個人情報が格納されている書籍庫など
レベル 2	非接触 IC カード	一般従業員の職場。ほとんどの従業員がこのアクセスクラスに属しており、出入りが頻繁に行われ、一度に多くの社員が出入りする扉である。そのため個人認証は非接触ＩＣカードでスムーズに行う必要がある。駅の改札のように。	一般従業員の職場など
レベル 1	NON または錠前と 鍵程度	昼間はフリースペースとして利用。夜間は施錠をするが、誰が開け閉めしたのかまでの履歴を取る必要はない。	受付や商談打合せコーナーなど

6. 監視カメラシステムとの連動

受付や商談コーナーなど、一般のお客様や宅配便業者が出入するスペースは、一般的に何の出入管理を行う必要もなく、営業時間内は、扉は開けっ放しにしておくケースが多いでしょう。

このようなエリアはＮＯＮセキュリティエリアと呼ばれており、オープンな企業イメージを損なわないためにも、夜間以外には鍵の施錠をしないのが一般的です。

とは言うものの、不正侵入者はこのようなＮＯＮセキュリティエリアから建物に侵入を試みますので、何のセキュリティも必要ないというわけではありません。

このような場合には、監視カメラを天井に設置して、画像を記録しておくことをお勧めいたします。

監視カメラはただ単に画像を録画し続けるだけですので、例え不審者が侵入したとしても、それを阻止することはできません。しかし実際に犯罪が発生した場合には、監視カメラで録画した映像を詳しく分析することで、犯人逮捕に役立てることができる唯一の方法となります。

また監視カメラを設置されていると、犯人は警戒をしますので、犯罪の抑止･予防にも繋がります。

監視カメラは、上記のような部外者への抑止効果以外にも、社内の人間の犯罪抑止にも繋がります。例えば個人認証をせずに共連れによって扉の中に進入するような内部の人間に対しては、扉の出入り部分に監視カメラを設置することで、共連れを抑止することが可能となります。

上記の場合、出入管理装置と監視カメラシステムを連動させ、扉が開いたタイミングで１０秒程度動画を録画します。それ以外のときは録画を中止すると

よいでしょう。不要な場面を撮影しないことにより、録画テープまたは録画記憶容量の節約に繋がる他、不正が起こった場合には、該当映像の検索をスムーズに行えるからです。

出入管理システムと監視カメラシステムを連動させることによりメリットが生じることとして、室内にいる人間が朝の最初の一人、または夜の最後の一人になった場合、室内の録画を行うという点です。

機密情報漏洩などの内部犯罪のほとんどは、他の社員がいない、一人の状態であるケースが多いという統計結果が出ています。

ですから、出入管理システムで部屋内の人数を常にカウントし、一人の状態を検知した場合には、監視カメラシステムに接点などで信号を出力し、室内の録画を開始するように指示を出すと良いでしょう。その後室内の人間がゼロになった際には、または２～１０名程度に増えた際には、録画を終了するように設定しましょう。

7. 生体認証装置を利用する場合は、個人情報保護法の遵守が必須

扉の鍵を解錠するための個人認証装置に生体認証装置を設置する場合には、従業員から指紋や静脈、虹彩(アイリス)パターンを採取し、認証装置内に登録しなければなりません。よって生体情報の利用目的を明示して、社員に承諾を得ることや、安全管理対策を実施して、生体情報が外部に漏れないように努めなければなりません。

認証装置内に登録される生体情報は、社員ＩＤや氏名と関連付けられて保管されますので、生体情報は完全なる個人情報に該当します。

ＩＣカード認証の場合には、個人情報保護法の遵守は必要ありません。なぜならば、ＩＣカードは企業サイドが従業員に対して発行するものですから、従業員個人から個人情報を取得する必要が無いからです。

8. 物理的セキュリティの未来像

論理的な情報資産であるデータベースサーバや、データベースサーバにアクセスするためのクライアントパソコンは、結局は１つの物理的なハードウェアから成り立っており、サーバルームや各職場の机の上に設置されています。ですから、情報資産は情報セキュリティで守るとともに、物理的セキュリティである出入管理システムでも守って行かなければなりません。

各クライアントパソコンからサーバへアクセスする際には、パスワードやICカード、指紋認証などの生体認証装置にてログオンを実施すると思います。

さてここで、出入管理システムは、各職場の部屋の中に存在する人間をリアルタイムに把握することが可能です。ですから、出入管理システムと情報セキュリティを融合させることにより、部屋の中に存在しない社員がクライアントパソコンからログオンしようとした場合には、明らかに成り済まし犯罪であることを検知することが可能となります。情報セキュリティ業界と物理的セキュリティ業界は、今まで会い交えることなく、それぞれに独立して製品開発を行い成長してきましたが、ここに来て両者のセキュリティシステムを融合させることにより、予想もしなかった大きな相乗効果が期待できることが分かって参りました。

例えばクライアントパソコンにログインをしたまま部屋の外に出た場合には、クライアントパソコンを自動でシャットアウトさせることも可能となるのです。

いままで物理的セキュリティは、目に見える物だけを守ればよいとされてきましたが、情報セキュリティシステムと融合させ統合することにより、より知的なトータルセキュリティプログラムを実現することが可能と見られていることから、今後は、物理的セキュリティと情報セキュリティの高度な融合をより一層推し進めて行くことにより、人間の犯罪心理や犯罪行動パターンに即したセキュリティプログラムが開発されることが期待されています。