制御系システムの現状と課題～ビルシステムを事例として～

イーヒルズ株式会社　取締役　　渡部　宗一氏

多発する大規模サイバー攻撃

2019 年から海外では数多くの大規模サイバー攻撃が発生している。米国では、身代金を要求するランサムウェアにより、約 950 の自治体が被害にあい、システムの復旧総額が 1 億数千万ドルにも及ぶ、との報告もあり、ニューヨーク州では 2020 年 1 月に「ランサムウェアへの身代金支払いを禁止する法案」が提出されたが、本法が成立するかは不明である。感染後のさらなる攻撃による個人情報漏えいや、長期間に及ぶ業務停止被害や影響の大きさに比べれば、身代金を支払った方が被害を少なく抑えられるため、今後も身代金支払いで解決する企業が増えることが推測される。また、情報システムを攻撃するよりも、制御系システムを攻撃した方が被害が広範囲に及び巨額な身代金を払うだろう、との推測から、制御系や工場へのシステムへの攻撃が増えてきていると想定される。

日本でもランサムウェア「WannaCry」などの観測件数は増加傾向にあり、海外同様の大規模な事件が発生することが推定される。

制御システムとセキュリティインシデント

制御システムはおもに工場などを動かし、24 時間 365 日停止することができないシステムを指す。電力、ガス、水道、鉄道などの重要インフラはすべて制御システムで動いている。

情報系システムが人と人の間でのデータのやり取りであるのに対し、制御システムは人と物の間のやり取りであり、機器そのものを動かしている。

制御システムは、機密性・完全性・可用性に加え、**特に安全性が重視**される。制御システムの中には、プラント爆発など危険な状態が発生した際に他に被害が及ばないよう、本体制御システムとは独立し、プロセスを安全に止めるために稼働する「安全計装システム」が装備されているが、制御系システムよりもシステムを停止させることが簡単なことから、安全系システムをターゲットにした攻撃が行われるケースもある。

ここ数年に起きた制御システムの大規模インシデントの要因として、外部から持ち込まれた保守用 PC や USB 経由で感染するケースが最も多く、その他、退職した元従業員が変更されていないアカウント・パスワードを使いリモートアクセスで侵入したり、フィッシングメール経由で ID／パスワードを奪って攻撃する、等が挙げられる。制御システムの最新のネットワーク図面がなく、感染経路が判明できないために復旧できず、全システムの変更を余儀なくされたケースも報告されている。

昨今、世界各国で電力系システムが狙われる傾向があるが、日本はサイバーセキュリティに対する意識が高く、防御ができているために大事には至っていないが、何もしていなければ実際は大きな被害が起きているはずである。

制御系システムへの攻撃手法としては、①従業員にソーシャルメディア等でフィッシングメールを発信して ID／パスワードを奪う、②一般的なランサムウェア感染、③特定企業の制御系システムを狙ったランサムウェアが特に多い。日本でもランサムウェア被害がないわけではない。現状は変な日本語のメールなど、言葉の壁に守られて事前に怪しいと判断できることから被害が少ないが、今後、自動翻訳技術の高度化に伴い、流ちょうな日本語によるフィッシングメール感染被害が大きくなると推察している。

ビルシステムの現状～ビルのセキュリティ対策の問題点

通常、ビルでは空調、照明、制御などのために数百台のサーバーを設置・稼働している。その中でも、サーバールームの空調設備は重要である。通常サーバーは、サーバールームの温度上昇により自動的にシステムをシャットダウンする機能を持っていることから、サーバー冷却のための空調設備に対し、温度上昇を表示させないような攻撃が仕掛けられた場合、サーバー停止により、大規模な損害が発生する可能性がある。その他、照明システムや火報システムへの攻撃などもビル運営にとっては大きなリスクとなり、さらに、サーバーが踏み台となる可能性も高い。

その他、ビル内の各種諸室では鍵管理は行っているが、誰が入室したかどうかの細かな入退室管理ができないために、不正行為を監視できないケースが多い。また、テナントビルの場合、テナント室内にはビル管理会社は基本的に立ち入ることができないので、テナント室内のスイッチ盤や天井裏などからの侵入や不正操作を防ぐことは難しいことなどもリスクとなっている。

オフィスビルのあらゆる機器を制御・監視する BA（Building Automation）システムの IT 面でのセキュリティの問題点としては、ビルや工場のために独自に開発されたシステムであるために、事前検証するシステムがなく、OS のセキュリティパッチが発行されても、それを充てられない点が挙げられる。また、多くのビルは、計画・設計時点で最新 OS の採用を決定しているが、着工～完成に至るまでに数年を要することから、竣工後すぐに利用 OS がサポート切れとなるケースも多い。結果として古い OS を利用せざるを得ず、OS を安全に動かすために、システムの外部接続をしない、などの対応が必須となる。

セキュリティを高めていくために「人」は重要である。技術的にセキュリティを強化しても、「人」による運用ができていないとセキュリティ事故に繋がることもある。2015 年に中部国際空港でサーバー空調機故障とネットワーク障害が起きたが、空港のセキュリティに大きく関係する空港設備の設計図が記載された論文とネットワークスイッチの詳細な製品情報がネットに公開されていて、セキュリティ上大きな問題を抱えていたという事例もあった。

また、日本ではセキュリティ対策も性善説に基づいて行われており、悪意を持った「人」の行為を防ぐことは難しい。日本では工場や工事現場で働く人の教育レベルも高く、細部まで監視・指導をしなくても十分に現場は回るため、監視する手順が欠けていることが多い。今後日本において、オリンピック関連工事などで外国人労働者の増加が予想されるが、現状のままでは悪意を持った「人」がなんらかの犯罪行為を行っても、それを発見することは難しい。

ビルシステムのセキュリティ対策

（１）情報系システムのセキュリティ対策がそのまま使用できない理由

前述のとおり、制御システムと情報系システムでは条件が異なるため、以下の理由で情報系システムでの対策をそのまま制御系システムに適用できない。

・OS が古いためにセキュリティパッチが当てられない

・ウイルス対策ソフトは動作検証できない場合が多く利用できない

・IPS（不正侵入防止システム）や IDS（侵入検知システム）を導入しても、情報系の従業者を雇えないためにシステムから上がる情報を理解する事ができない

・緊急対応を可能にするために常時ログイン状態にあり、操作者を特定できない

・大型ビルなどでは万単位にあるコントローラーの ID やパスワードをすべて変更することは不可能である（バンクごとに変更するなどで対応）

・ウイルスに感染しても、制御システムを停止させられないために、そのまま稼働し続けなければならない

・複数のベンダーがシステムを構築しているために、障害が起きたときの原因の切分けが不可能である

（２）最近の BA システムのセキュリティ上の弱点

BA システムのセキュリティ上の弱点としては、以下が挙げられる。

・ネットワークが単一ですべてが一層であるため、いったんシステムに侵入されたら全システムが感染する

・コントローラーの ID やパスワードが出荷時のままのため、簡単に侵入され、自由に操作できてしまう

・最新機器ネットワーク図がなく、ウイルス感染の被害範囲が把握できない

・機器の適切なバックアップがなく、復旧に時間を要する

・各種設備システムが共通で利用するプリンタの設定が不適切で、すべてのシステムが繋がってしまうケースがあり、予想外の感染やサイバー攻撃を受ける可能性が高い

・制御盤のカギが全国共通であり、ネット等でも容易に入手できるため、セキュリティ機能を果たしていない

（３）制御システムのセキュリティ対策

セキュリティ対策のためには、既存システムの場合は外部から切り離すこと。新システムは外部とつなげなければならないケースが多いため、システムの監視を強化することが考えられる。

制御システムのセキュリティ対策の手順は以下のとおり。

１．予防：インシデントの発生を予防するするために運用・物理セキュリティを行う

２．限定：インシデント発生時に影響範囲を最小限に抑える

３．復旧：迅速な復旧　　※バックアップを一番重視している

４．検知：インシデント予兆の検知

セキュリティ対策には「人」が重要

世界各国でさまざまなセキュリティインシデントが起きている。たとえば 2019 年 5 月に発生したランサムウェア「WannaCry」は、世界 150 カ国、30 万台に及ぶ感染被害をもたらした。このなかで、イギリス全土で共通の病院システムが感染被害にあったが、その中でも適切なシステム管理を行っていたウェールズのみ感染しなかった、という事例がある。これは同じシステムを利用しても運用のセキュリティレベルが異なれば、感染の度合い被害が大きく異なる、という

良い事例である。

サイバー攻撃の他、重要データの紛失（データ管理の不備）や操作ミス、設計ミスなど、システム自体というよりも「人」が原因で重大なインシデントに繋がることもある。

サイバーセキュリティは、システムだけで対策を講じようとすると、かなりコストがかかるため、「人」によるシステムの運用体制を構築することが重要である。

以上