システム監査従事者のためのスキルアップ講座　講演

制御系システムとシステム監査 ～ビルシステムを事例として～

Industrial control system from the viewpoint of system audit : A case of Building automation system

渡部　宗一
Soichi Watanabe
イーヒルズ株式会社
eHills Corporation

1．制御系システムとは

「制御系システム」は、「情報系システム」と仕掛けはそれほど変わらないが、処理の対象が設備や機械の制御であり、多くは 24 時間 365 日稼働する。典型的な制御システムでは HMI（Human Machine Interface）という監視や操作をする機器と圧力計やバルブなどのフィールド機器の間にこれを制御するコントローラが設置される場合が多い。情報系システムでは「人」と「人」がデータのやり取りをするが、制御系システムでは「人」と「物」がデータをやり取りする。このため単なるデータではなく、物理の世界と関わるので、情報系の機密性・完全性・可用性に加え、「安全性」が重要である。このため、制御系システムには「安全計装システム（SIS:Safety Instrumented System）」が本体制御システムとは独立して設置され、システムを監視し、万一危険な兆候を検知した場合には、そのプロセスを安全にシャットダウンする。化学工場などには単に電源が切れてしまうと何分か後には爆発するようなプラントがたくさんある。ボイラーなども停止した後、一定時間冷却せずに再稼働すると爆発する。発電所や化学プラントでは現場に出る人へのあいさつは「ご安全に」である。

2．制御系システムのインシデント事例

(1) 水道分野：2001 年にオーストラリアで、解雇された元従業員が、在職時に使用していたリモートアクセスの経路とアカウントを利用し、外部から下水処理施設を不正操作し、下水を海洋に大量流出させた。

(2) 自動車分野：2005 年に米国内のダイムラーの 13 の工場が、外部から持ち込まれて接続されたノート PC からの不正プログラムによって操業停止。5 万人の労働者が 50 分作業ができずに 1,400 万ドル（約 17 億円）の損害。2008 年には西日本の自動車会社の工場で入れ替えた操作パソコンからウイルスが混入し、3 日間製造ラインがスローダウン。原因究明に 1 カ月。

(3) 石油化学分野：2008 年にトルコでパイプラインに設置されている監視カメラの通信ソフトの脆弱性から内部ネットワークに侵入され、動作制御系を不正アクセスされ、管内の圧力を異常に高められ、カメラやセンサの動作も止められ、通信も遮断されて爆発。

(4) 半導体分野：2011 年に日本の半導体メーカの品質検査装置が USB メモリからのマルウェアに感染し、不良品を出荷。感染元がわからず生産ライン停止。

(5) 製鉄分野：2014 年、ドイツで製鉄所の溶鉱炉のコントロールを許可する ID とパスワードが電子メールからのマルウェアで窃取され、溶鉱炉が正常停止できず損傷。

(6) 電力システム：2015 年ウクライナでサイバー攻撃による大規模停電。2016 年 12 月に米国の電力会社の社内 PC からロシアのハッカーが使うとされているマルウェアを発見。カナダの送電・配電会社でも侵入の痕跡を発見。2017 年 7 月に米国の原発の情報系システムに侵入。アイルランドで送電システムにロシアの関与するハッカーが侵入。英国で複数の制御系システ

ムが攻撃された。日本では報道されていないが、電力系システムへ攻撃が集中しており、英語圏では関心が高い。
(7) TV局：2015年4月にフランスのTV局が、お天気カメラのシステムを含む7つのルートからのサイバー攻撃を受け、全12チャンネルの放送が翌朝まで停止。

3．ランサムウェアの事例

(1) アルミ工場：2019年5月にノルウェーの工場がランサムウェアに感染し、世界40カ国の同社の工場すべてに広がった。
(2) 化学工場：2019年5月に米国の化学工場が感染し、全システムが停止して復旧に1週間。
(3) コンサルティング会社：2019年1月にフランスのコンサルティング会社がフィッシングメールから感染。ネットワークをシャットダウン。
(4) フォレンジック会社：2019年6月に英国のフォレンジック会社が感染し、一週間業務停止。
(5) 病院：2019年9月にオーストラリアの7つの病院が、2019年10月に米国の3つの病院が感染。米国の地方自治体、警察、病院は、2019年に140件（2018年は85件）のランサムウェアの攻撃を受けた。

制御システムへの攻撃で一番多いのは、従業員がID・パスワードを窃取された事例である。次に多いのがランサムウェアの攻撃である。これらには主としてフィッシングメールで行われる。日本ではメールの不自然さから気づける場合が多いが、今後注意を要する。

4．制御システムの特長～ビル分野を事例として～

ビルがコンピュータ制御されているというイメージはあまりないかもしれないが、空調、照明、エレベータ等を制御するために、高層ビルになると100台から200台程度のPC・サーバと、1万台を超えるコントローラが設置され、ちょっとした工場よりはるかに大きいシステムが動いている。

オフィスビルのリスクを洗い上げてみると、(1) 空調システムを乗っ取られて（お客様の）サーバルームの温度が上昇し、サーバが停止すること、(2) 防災システムによる監視が不能になること、(3) 照明システムが制御不能で全館停電になること、(4) ビル内のサーバが乗っ取られて外部攻撃の踏み台にされること、である。そして、攻撃されやすい場所は、各階の空調機械室である。鍵は厳格に管理しているが、いろいろな人が入る可能性があり、誰がどのくらい入っていたかは管理していないこともある。また、テナント室内の天井裏には、たくさんのコントローラがあり、ここも守るのが難しい。

ビル制御システムそのものには資格を持った専門家が付いていて、情報系のITも専門家が見ているが、その間のつなぎの部分について、社内人材が不足している等の運用上の問題点がある。

ビルシステムでは、システムのライフサイクルも問題になる。設計から建築工事が終わるまでに3～5年かかる。仕様で決めたOSは稼働開始時にはほぼサポート切れ間近の状態になるのである。そしてビルの耐用年数は60年以上もある。制御系システムにはこのような事例が多く、実は往年の名機PC98は、過去につくったソフトウェアの延命のために高値で取引きされている。

ビルシステムで見られるセキュリティ上の弱点には、以下のようなものがある
(1) ネットワークが単一：一旦侵入されるとすべての機器に到達する可能性。
(2) 工場出荷時のままのコントローラ：ID・パスワードが容易に推測可能で、侵入されると自由に操作できる。
(3) 最新の機器のネットワーク図が未整備：影響範囲が特定できない。
(4) バックアップがない：システム復旧に時間がかかる可能性がある。
(5) 情報系システムとの安易な（未知の）接続：情報系システムからのウイルス感染や攻撃。(省エネ管理用のものが多い)
(6) 不適切なプリンタ共有：想定外のネットワークと繋がって、ウイルス感染やサイバー攻撃。
(7) 分電盤の鍵が共通：分電盤の鍵は感電防止が目的で、セキュリティ目的ではない。

5．制御系システムのサイバーセキュリティ対策

制御系システムでは、以下の点で情報系のセキュリティ対策がそのまま使えない。
(1) セキュリティパッチ：検証システムがなくテストができない。システムが止められず、パッチを当てるタイミングがない。
(2) ウイルス対策ソフト：パターンファイルの配信システムがなく、検証システムがないので、

更新後の動作保証ができない。
(3) IPS/IDS の導入：高価すぎるので工場や建物ごとにおけない。シグネチャの更新やシステム管理にインターネット接続が必要になる。
(4) 監視端末の ID ／パスワード：異常発生時に即座に対応する必要があり、権限がなくて使えないという状況が許されない。
(5) コントローラの ID ／パスワードの設定・定期変更：万単位の機器のパスワードを全部異なるものにすると保守できない。
(6) ログの取得：大量のログがネットワークを圧迫し、精密な制御が不能。
(7) ウイルス感染時の対応：運用中のシステムをシャットダウンしたり、ネットワークから切り離すことができない。
(8) 複数のベンダーによる構築：原因切分けが複雑で、全体を詳細に把握している人がいない。

制御系システムのセキュリティの基本的な考え方は、まず、既存システムは無菌室を作って外部から隔離、新規システムには外部からの侵入対策として監視・予防を組み込むということである。そして、インシデントが発生したときには、迅速に復旧できるようにバックアップ・運用を強化することが重要である。予防の中心は運用と物理セキュリティが中心になる。そしてネットワーク構成をセグメント分けして影響を限定するようにしていく。そして、お金に余裕があればインシデントの検知をすることにしている。

6. 最後に

運用には人が大事である。WannaCry ではたくさんの被害が出たが、英国の中でもウェールズでは感染を防いだ。同じシステムでもパッチが適用され、ポートが管理されていた。サイバーセキュリティには、システムがきちんと作られていることも大事だが、運用する人も大事なのできちんと見ていく必要がある。

（成田　和弘　記）
（2019 年 12 月 11 日開催）