savic-net™ FX/G5におけるサイバーセキュリティ対応

Cybersecurity measures for the savic-net FX/G5 building management systems

畔柳　賢吾
Kengo Kuroyanagi

キーワード
savic-net FX，savic-net G5，ホワイトリスト型ウイルス対策ソフト，ファイアウォール，公開鍵暗号方式

アズビルではこれまで，ビル空調システム内の各構成機器に対して，公開鍵暗号方式によるプログラム改ざん防止やファイアウォールによるネットワーク経由の攻撃への対策を講じてきた。今回，さらなるセキュリティ強化を図るため，悪意をもった攻撃者がビル空調システム内の構成機器上で不正なプログラムを動作させようとした場合に，あらかじめ用意された，動作を許可する実行ファイルリスト（ホワイトリスト）に存在しないプログラムの動作を防ぎ，また不正アクセスを検出した際にオペレータに通知できる警報機能を備え，不正アクセス検出時の調査を迅速に行える機能を実現した。

To protect each component of its building air-conditioning systems, Azbil has been using measures such as public key cryptography to prevent tampering with programs, and firewalls to foil attacks through the network. In order to further tighten security, we have now implemented functionality that prevents malicious attackers from running unauthorized programs on the component equipment of the building air conditioning system (programs that are not on a white list of allowed executable files) and that warns operators with an alarm when an unauthorized access attempt is detected.

一般論文

1. はじめに

今日，サイバーセキュリティをめぐる状況はめまぐるしく変化してきている。無差別型のマルウェア[注1]が猛威をふるい，制御システムを狙った高度な標的型攻撃も報告されている。そのような状況の中，経済産業省による，ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン[(1)(2)]が策定され，ビル空調システムにおいても十分なセキュリティ対策が求められるようになってきた。

ビル空調システムのセキュリティ対策は「ウイルスを持ち込まない運用」の徹底が主であった。しかし，世の中のセキュリティ意識の高まりもあり，既に稼働中の建物も含めてより高いセキュリティ対策が求められている。

2. サイバー攻撃の対象と侵入経路

本稿では，アズビルのビル空調システムにおける不正アクセス対策について紹介する。ビル空調システムは，図1に示す通り，監視用PCと複数の統合コントローラなどで構成されている。統合コントローラで温度や湿度などの情報を収集・蓄積し，火災や機器故障などの異常がないことを，オペレータが監視用PC上で日々監視している。

サイバー攻撃は大きく分けて，過失操作を悪用した無差別型のサイバー攻撃と，悪意をもった攻撃者からの標的型のサイバー攻撃に分かれ，その侵入経路は，①監視用PC経由②外部ネットワーク経由③不正な端末機器経由が想定される。ネットワーク構成図と，想定される侵入経路を図1に示す。

また，ビル空調システムにおけるサイバー攻撃の中で，攻撃を受けたときの影響が特に大きいのが統合コントローラである。統合コントローラが攻撃を受けてシステムダウンすると，空調設備や防犯設備，電気設備などの制御が効かなくなったり，火災や機器故障などの監視ができなくなったり，データの収集ができなくなるなどの被害が出る。

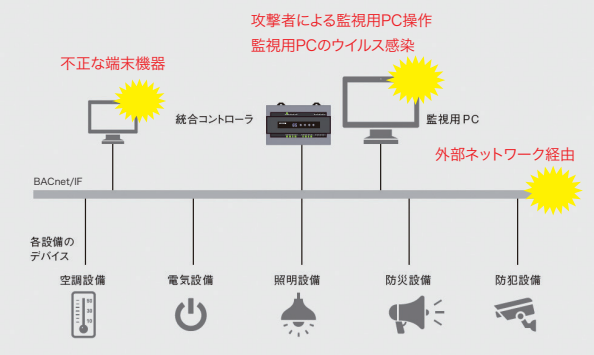


図1　ネットワーク構成図と侵入経路

注1　不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称

3. 従来のセキュリティ対策

アズビルのビル空調システムであるsavic-net FXおよび，savic-net G5では，統合コントローラに対する対策として，RSA(暗号を活用した)公開鍵暗号方式を利用したプログラム改ざん防止の仕組みを導入している。また，統合コントローラの不要なポートを閉じることで，ネットワーク経由で不正にアクセスされたり，DoS攻撃によりシステムダウンしたりするリスクを排除している。

しかし昨今，攻撃手法はより高度化しており，特に，明確な目的をもった悪意のある攻撃者による統合コントローラへの不正アクセスを防ぐ仕組みが従来技術では不十分であった[(3)(4)]。

4. さらなるセキュリティ対策

そこで，ビル空調システムに対するさらなるセキュリティ対策を検討した。ビル空調システムの特徴として，日々の運用が比較的固定化される点，また外部ネットワークに接続せずローカルなネットワーク構成で構築される点が挙げられる。ローカルなネットワークであるためセキュアである一方，システム構成機器に対してウイルス対策ソフトを導入し，パターンファイルを常に最新に更新する運用が難しい。

こういったビル空調システムの特性を踏まえて，より強固なセキュリティを求めるお客さま向けに，あらかじめ用意された，動作を許可する実行ファイルリスト（ホワイトリスト)に存在しないプログラムの動作を防ぐ，ホワイトリスト型ウイルス対策ソフトを導入することにした。表1に，ビル空調システムに対して考えられる攻撃の種別とその影響，および対策について示す。

表1　攻撃種別ごとの対策

攻撃種別と影響 (手段･侵入経路･影響)	対策
インターネットサイト経由や持ち込みUSB経由で，監視用PCがウイルス感染し，警報の監視ができなくなる。	インターネット接続をしない，監視PCのUSBポートをふさぐ，などの物理的な対策により，過失によるウイルス感染を防ぐ。
監視用PC経由で悪意のあるオペレータや第三者により，統合コントローラが不正アクセスを受け，データ収集や警報の監視ができなくなる。	監視用PCに対するホワイトリスト型ウイルス対策ソフト導入により，監視用PC上での不正プログラムの起動を抑制し，統合コントローラへの攻撃を防止する。
ネットワークに不正に接続された端末機器や外部ネットワーク経由で，統合コントローラが不正アクセスを受け，データ収集や警報の監視ができなくなる。	統合コントローラに対するホワイトリスト型ウイルス対策ソフト導入により，統合コントローラ上での不正プログラムの起動を抑制し，統合コントローラへの攻撃を防止する。

4.1　ホワイトリスト型ウイルス対策ソフトとは

ホワイトリスト型ウイルス対策ソフトは，動作を許可する実行ファイルをリスト（ホワイトリスト)に登録し，そのリストを元に実行ファイルの起動，変更，削除を制御するタイプのウイルス対策ソフトである。表2にその特徴をまとめた。

表2　ホワイトリスト型ウイルス対策ソフトの特徴

機能	詳細
ウイルス実行の防止	ホワイトリストに登録されていない実行ファイル（拡張子:exe/dll/bat など)の起動は，保護機能によりブロックされる。
改ざんの防止	ホワイトリストに登録された実行ファイルは，保護機能により変更，削除がブロックされる。
変更管理	実行ファイルの変更，削除を行う場合は，対象ファイルを事前にホワイトリストから除外する必要がある。
ウイルスのネットワーク内侵入防止	保護機能有効時，外部ドライブ（CD/DVDドライブやUSB メモリなど)から，実行ファイルを直接起動することはできない。
運用中の保護	保護機能有効時，アプリケーションのインストールや更新はできない。

パターンマッチング型ウイルス対策ソフトでは，新しいウイルスが発生するたびにウイルス定義ファイルを更新しなければならないのに対し，ホワイトリスト型ウイルス対策ソフトでは新しいウイルスが発生してもウイルス定義ファイルを更新することなく運用できる。図2に両者の違いを示した。

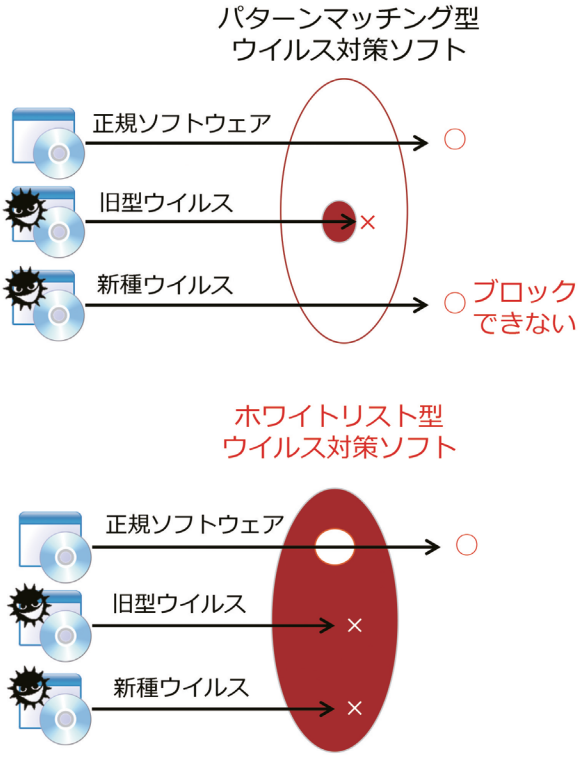


図2　パターンマッチング型ウイルス対策ソフトとホワイトリスト型ウイルス対策ソフトの違い

4.2　監視用PCへの対策

savic-net FXおよび，savic-net G5の監視用PCに対し，ホワイトリスト型ウイルス対策ソフトを導入し，監視用PCを経由した統合コントローラへの攻撃を防止した。

運用開始後はホワイトリストの更新は不要とし，お客さまの都合でプリンタドライバやExcelなどのソフトウェアをインストールしたい場合に限り，許可された作業担当者が，一時的にホワイトリスト型ウイルスソフトを無効化してホワイトリストの更新ができるようにした。

4.3　統合コントローラへの対策

ネットワークに不正に接続された端末機器や，外部ネットワーク経由の攻撃への直接的な対策として，savic-net G5の統合コントローラに対してホワイトリスト型ウイルス対策ソフトを導入した。その特徴を本章で紹介する。

4.3.1　オペレータ操作画面

ホワイトリスト機能の操作は，統合コントローラごとにデバイス詳細画面より行うことができる。画面イメージを図3に示す。

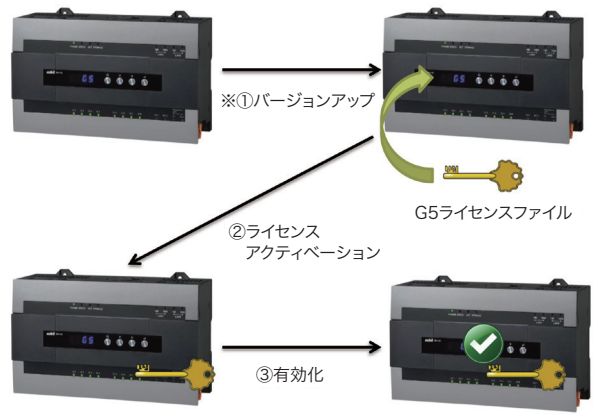
図3　画面イメージ

ホワイトリスト機能の有効・無効操作，ライセンス認証（以下，アクティベーション），操作時の事象ログ，警報など，監視システムの既存の仕組みにホワイトリスト機能を取り込むことにより，特定の権限をもったオペレータが監視業務の中で操作できるようになっている。

4.3.2　ライセンス管理

ホワイトリスト型ウイルス対策ソフトを導入するためには，お客さまにライセンスの費用負担が発生する。そのため，お客さまの求めるセキュリティレベルによって，ホワイトリストの導入要否を選択できる仕組みを導入した。ホワイトリスト型ウイルスソフトを使用したい統合コントローラのみライセンスを購入し，有効化できる設計とした。

新規の建物向けには，工場でアクティベーションしてリリースする。また。運用中にホワイトリスト型ウイルス対策ソフトが必要になった場合でも，ライセンスを購入すると即座にアクティベーションおよび，機能の有効化が可能な設計とした。運用中の建物向けのライセンスアクティベーションの流れを図4に示す。



※ホワイトリスト機能導入前のバージョンからのバージョンアップ時のみ

図4　運用中の建物向けのライセンスアクティベーションの流れ

4.3.3　既存機能への影響について

savic-net G5には，運用中にオペレータが自由に拡張アプリ[注2]を作成できる機能がある。運用中に自由にアプリを開発できる便利な機能であるが，その特性がゆえにホワイトリスト型ウイルス対策ソフトとの相性が悪い。

ホワイトリスト型ウイルス対策ソフトを導入した場合，統合コントローラ内のプログラムを変更する際に，ホワイトリストの更新が必要となる。つまり，拡張アプリを作成するたびにホワイトリストの更新による待ち時間が発生するため，お客さまの利便性を損ねてしまうという問題があった。

そこで，待ち時間の改善のため，運用中に更新されないプログラム（基本ベースライン）と，運用中に更新される拡張アプリで管理を分け，最終的にマージを行う仕組みを作成した。このように効率的にホワイトリストを更新する仕組みを導入することで，更新にかかる時間を90秒から10秒程度まで大幅に短縮化した。図5にその仕組みを記載する。

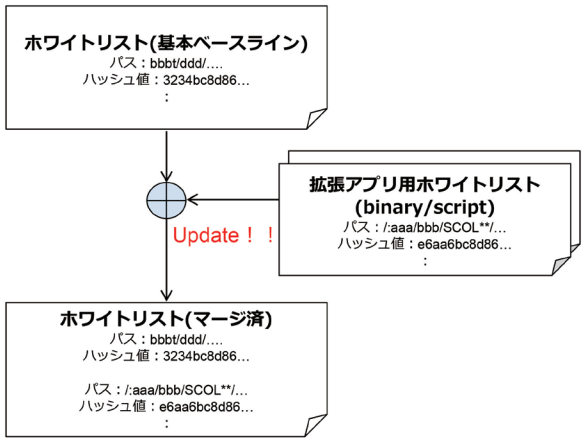


図5　ホワイトリスト更新の効率化

また，拡張アプリによる意図的な書き換えと，悪意をもった書き換えを区別して管理する必要がある。

拡張アプリ機能を実現するため，統合コントローラではDockerコンテナと呼ばれる仮想化技術を使用している。コンテナアプリを起動する際，アプリケーションが動作するコンテナレイヤが動的に生成されるため，ホワイトリストに登録されたファイルパスとの整合性が取れなくなる問題があった。そこで，動的に生成されたファイルに対してもホワイトリストの制御下となるよう，ホワイトリストの定義を行った。

4.3.4　不正アクセス検出時のオペレータへの通知

不正アクセスを防止する仕組みがあっても，それをオペレータに通知する仕組みがないと，攻撃を受けているにもかかわらずその状況を放置してしまうことになりかねない。そこで，統合コントローラへのホワイトリスト型ウイルス対策ソフトでは，不正アクセスを検出した際に警報が発報される仕組みを開発した。不正アクセス検出時のフローを図6に示す。

注2　統合コントローラで動作する制御系アプリケーション

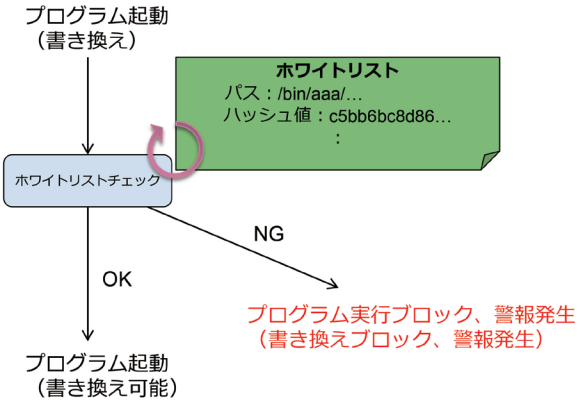


図6　不正アクセス検出時のフロー

オペレータが，統合コントローラに対する不正アクセスがあったことを即座に認識できるため，迅速な初動対応が可能である。画面イメージを図7に示す。

図7　不正アクセス検出時の警報表示

4.3.5　不正アクセス検出時の調査

実行ログとセキュリティイベントログを記録しているため，不正操作検出後の調査が容易となる。いつ，どこのファイルが起動されたのか，アクセス権限，ファイルハッシュ値（改ざんされたかの検証用）がログで追跡できるため，不正操作検出後の調査が可能となる。調査フローを図8に示す。

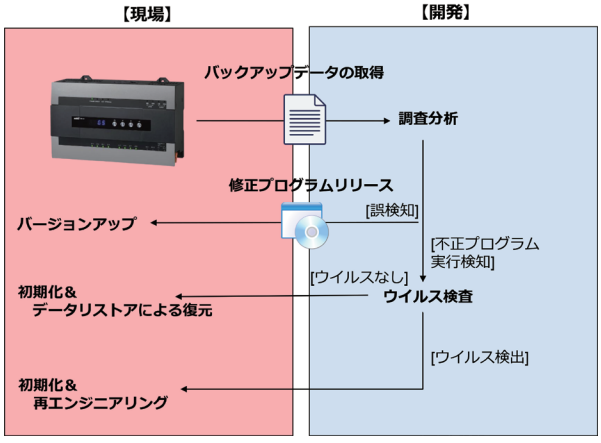


図8　不正アクセス検出後の調査･処理フロー

5. おわりに

セキュリティの提供が当たり前品質として求められるようになってきている状況において，すべての建物に対しての最低限のセキュリティレベルの提供と，より高度なセキュリティレベルを求めるお客さまに向けたソリューションの提供を可能とした。

アズビルでは，世の中で日々報告される膨大な脆弱性情報を一元管理し，迅速に製品に適用していくための組織体制を構築している。世の中の動向を注視しつつ，建物ごとの運用に合わせたセキュリティ対策を実施している。脆弱性対策の製品適用までのリードタイムの短縮化により，建物のセキュリティインシデントを防止し，より一層の顧客満足度の向上を図っていくことが今後の課題である。

＜参考文献＞
(1) 経済産業省
ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第1版(2019.6)
https://www.meti.go.jp/press/2019/06/20190617005/20190617005_01.pdf
(2) 経済産業省
ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（個別編：空調システム）第1版
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/pdf/20221024_1.pdf
(3)「産業用制御システム向け侵入検知製品の実装技術の調査」調査報告書
https://www.ipa.go.jp/files/000101403.pdf
(4) 制御システムのセキュリティリスク分析ガイド 第2版
https://www.ipa.go.jp/files/000080712.pdf

＜著者所属＞
畔柳　賢吾　アズビル株式会社
ビルシステムカンパニー開発本部開発1部