制御システムセキュリティ対策最前線～どう守るか

【現場適応セキュリティ対策ガイド】

IoT機器をサイバー攻撃に備え，そして守る

アドソル日進　吉村　隆男

1.　はじめに

ここ最近の予想をはるかに超えたIoT（Internet of Things：モノのインターネット）の急速な普及や拡大に伴い，巧妙に制御系システムを標的としたサイバー攻撃が増えており，深刻化している。直接人命や社会システムに大きな影響を及ぼす可能性があることから対策することが急務となっている。特に，IoT関連機器の開発・製造を進めている製造業やその利用者にとっては喫緊の課題になっている。

サイバーセキュリティ対策向けのプラットフォームとして米国で誕生したのが，仮想システムの技術を使ってサイバー攻撃に対して"隔離"と"遮断"を実現した「LynxSECURE」である。LynxSECUREは当社アドソル日進が国内独占販売権を持っており，国内でも既に技術検証サービスが始まっている。

IoTが広がるにつれて，これまでは対処の必要がないと考えられていた制御系システムについてもサイバー攻撃への対策が求められており，現状のままで放置しておくと重大事故を発生させてしまうだろう。サイバー攻撃の内容が高度化・複雑化している現在では，ハッカーに侵入されることを前提とした，端末や制御機器自体に防御策を講じることが必要となっている。これらIoT機器のセキュリティリスクを極小化するには，サイバーセキュリティ対策プラットフォームLynxSECUREをIoT機器に搭載することをお勧めする。米国ではすでに軍事・防衛・車両・電力などで利用が始まっている。

ご存知の通り，すでにIoT機器にワイヤレスネットワーク経由で侵入できることが実証されている。2015年7月に米国のセキュリティ研究者が行った実験では，自動車の電子制御ユニット（ECU）を攻略し，エンジン，ステアリング，ワイパなどを外部から自由に操作できることを証明した。このため，「米国の自動車メーカがハッキング対策のために140万台の自社製品をリコールする」と報道があったことは記憶に新しいことである。同様のことが日本の国内でも発生することは，時間の問題だろう。

制御系のシステムに向けたサイバー攻撃の手法が，一般のエンタープライズシステムに対する攻撃と異なっているわけではない。エンタープライズ系システムと同様に，制御系システムにインターネットに接続されている部分があると，その接続点のすべてがマルウェアの侵入口となりうる。IoTがさらに拡大すると予想されるこれからの社会では，制御系のシステムについても，システム内部の制御機器をサイバー攻撃から守るための対策が重要になるわけである。

ここで当社について簡単に触れておく。創立40周年を迎えた当社は，IoTシステム開発を事業の3本柱の1つに据えるインテグレータである。IoTの基礎となる組み込みソフトウェアと無線通信機器についての長い経験と深い知見を持つ。国内の事業所は，東京・大阪・福岡・仙台の4ヵ所。2016年3月には米カリフォルニア州サンノゼ市にセキュリティR&Dセンタを開設した。

2，　制御機器そのものに防御機能が必要

サイバー攻撃への対策というと，インターネット回線との出入り口に防御の目が向きがちだ。しかし，サイバー攻撃の手口は日々進化しており，この防御法だけではいつ破られてもおかしくない。サイバー攻撃の内容が高度化・複雑化している現在では，ハッカーやマルウェアに侵入されることを前提として，端末や制御機器自体に防御策を講じることが必要となっている。（**図1**）

3. 制御系システムをサイバー攻撃から守るポイントは〝隔離〟と〝遮断〟

今までインターネットとの接続を想定していなかった制御機器をどのようにすればサイバー攻撃の脅威から守ることができるのか。

ポイントは2つある。"隔離"することと"遮断"することである。"隔離"とはソフトウェアとハードウェアを重要度に基づいてグループ分けし,そのグループごとに別々の領域で稼働させることである。重要な機能をマルウェアから隔離してしまえば,攻撃を受けることもなくなるわけである。また,"遮断"は攻撃を防げなかった場合に被害拡大を防ぐことである。重要度ベースの"隔離"を細かいレベル設定しておけば,被害が他のグループに拡大することを防げる。

4. 仮想化システムの考えでIoT機器をサイバー攻撃から守る

LynxSECUREでは,この2つのポイントを仮想システムの仕組みで達成している。

LynxSECUREは,アンチウィルスソフトウェアなどの一般的なセキュリティツールとは防御の仕組みが大きく異なる。一般のセキュリティツールがOS上にインストールされるのに対して,LynxSECUREはOSよりも下の階層で動作する。OSやその上で動作するアプリケーションソフトからは通常のハードウェアに見える「仮想マシン」という環境を複数用意する仕組みである。ウィンドウズやリナックスなどのOSは,「ゲストOS」としてLynxSECUREの上で動作する構成になる。LynxSECUREの本体はハードウェアのすぐ上で動作するベアメタルハイパーバイザとなっており,CPUコア・メモリ・入出力装置などの振る舞いをハードウェアに近いレベルでコントロールする。これらのハードウェア要素を重要度別のグループに割り当てることによって,ハードウェアの隔離を実現している。

また,OS・ミドルウェア・アプリケーションなどのソフトウェアについては,重要度別のグループごとに設けたドメイン(区画)内で稼働させる方式を採用。あるグループで動作するソフトが他の区画にアクセスできないようにすることで,ソフトウェアの"隔離"と"遮断"を実現している。(**図2**)

5. LynxSECUREの4つの特長

第1に,Intel VTのVT-x(IA-32仮想化支援機構)とVT-d(I/0仮想化支援機構)を利用した「セキュア・セパレート・カーネル」が実装されている。ハードウェア・OS・ミドルウェア・アプリケーションの全レイヤにわたり壁があるので,マルウェアによる不正操作はシャットアウトされる。

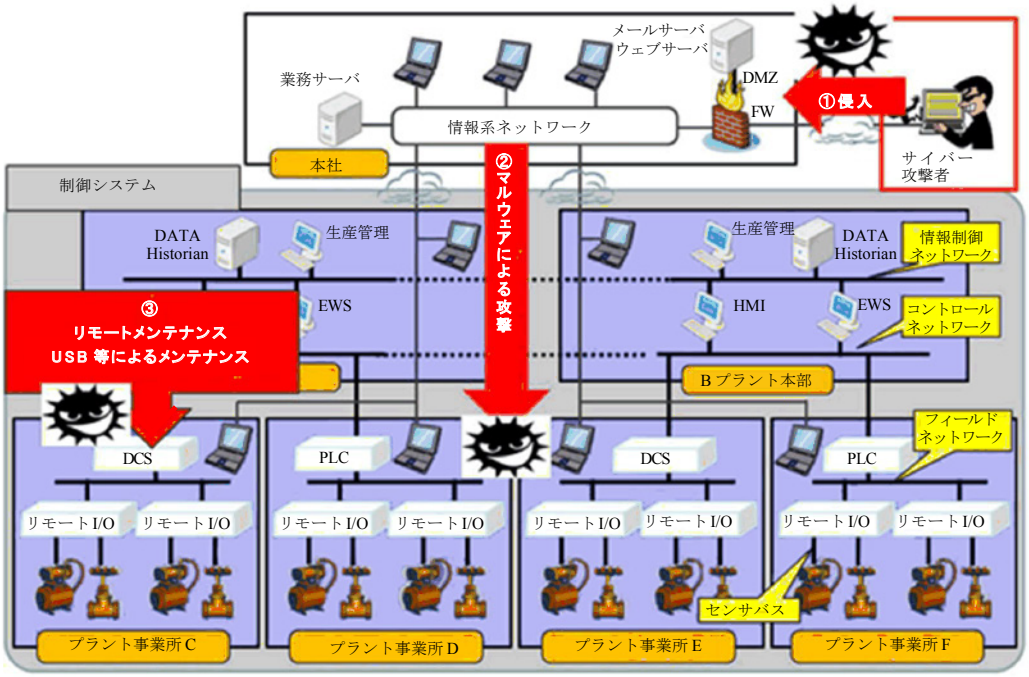

図1 産業制御システムにおける脅威

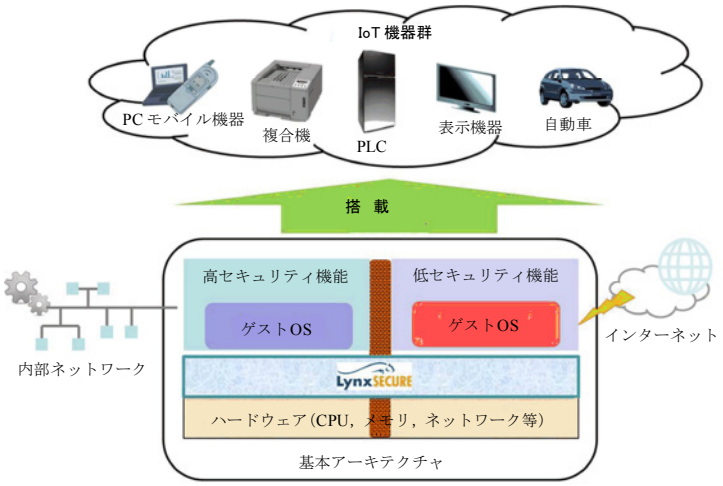

図2　LynxSECUREの仮想化システムによる動作の仕組み

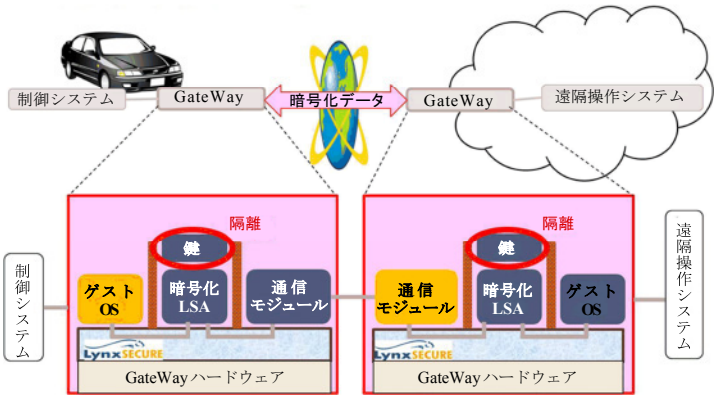

図3　遠隔操作／自動運転用ゲートウェイ(マルウェアから見えない隔離領域で鍵を管理)

第2に，LynxSECUREハイパーバイザ層は，必要最小限の機能で構成された「Small Trusted Code Base」になっている。フットプリントはきわめて小さいので，メモリ容量の制限が厳しい組み込み系システムへの適用が容易である。

第3の特徴は，ハイパーバイザ層のすぐ上位で，OSレスで動作可能な「LynxSecure Application（LSA)」がある。OSの脆弱性を突いた攻撃を受けるリスクがなくなるので，それだけ安全なシステムを構築できる。

第4に，暗号鍵を安全に管理するための「LSA.connect」がある。これはハイパーバイザ内に形成されたセキュアな通信経路となるもので，専用ドメインに格納された暗号鍵をアプリケーションやOSが参照するのに最適である。マルウェアが暗号鍵を盗み出すことを完全に防ぐ。

6. 社会・産業向け装置での実績

このような特徴を持つLynxSECUREはさまざまな制御系システムに適用できる。たとえば，自動車に搭載された制御システムが外部から不正操作されることを防ぐために，遠隔操作システムとの間でやり取りされる制御コマンドやデータを暗号化する仕組みが良く使われる。そこで，遠隔操作システムと制御システムがネットワークと接する場所にLynxSECUREを組み込んだゲートウェイ装置を配置して，暗号鍵を隔離する。マルウェアが暗号鍵を不正に利用できないようにして自動車の安全性を確保するのである。(図3)

また，IoT機器では，内部の制御システムをLynxSECUREベースで構築することによって重要機能をしっかりとガードできる。内部ネットワークを使う重要機能とインターネットを利用する一般機能を設計段階できちんと分け，それぞれを別々のドメインで動作させるように実装すれば，インターネットからのサイバー攻撃を受けても，その影響が重要機能に及ぶことを避けることができる。

7. 専任の技術者が日本で対応

当社は，単にソフトウェアを販売するだけではない。導入企業の要望に応えるために，LynxSECUREのカスタマイズや暗号化設計も行うことができる。また，ソフトウェアの設計図に相当するソースコードも保有しているので，技術者集団が日本でのいかなる要望にも対応できる体制を整え，対応を開始した。

LynxSECUREの開発・販売を通して，製造業をはじめとした皆さまに，この脅威に対する懸念を和らげ，安全・安心を提供できるようになった。

ヨシムラ・タカオ
アドソル日進㈱
セキュリティ・ソリューション推進部
〒108-0075・東京都港区港南4-1-8
電話(03) 5796-3131