KPMG
cutting through complexity

2015年6月

新たなITリスクに立ち向かう 連載シリーズ 第14回

高まりつつある制御システムにおける情報セキュリティの脅威とその対策

情報セキュリティに関する事件というと、企業からの顧客情報の漏えいや金融機関における不正送金が有名である。これらITシステムのものに加え、近年では、工場やプラントなどで使用されている制御システムにおける情報セキュリティについての事件も、徐々に知られるようになってきた。制御システムはエネルギー産業や交通機関といった、我々の生活にとって重要なインフラを支えており、それに対する攻撃は多数の人命が危険にさらされることもあり、社会的影響が大きい。

本稿では、ITシステムとの比較を通して、制御システムにおける情報セキュリティ対策のポイントを述べる。

1. 制御システムの情報セキュリティ事件

制御システムは、ICS（Industrial Control Systems：産業用制御システム）やSCADA（Supervisory Control And Data Acquisition：監視制御およびデータ取得システム）等と呼ばれ、発電所、水処理施設、石油・ガスプラント、交通機関、製造工場といった我々の生活における重要なインフラや産業において、装置や機器の監視・制御を行っている。

これらは、情報システムというよりも専用の装置や機器とみなされてきたため、これまで制御システムに対する情報セキュリティへの関心も高くなかった。しかしインフォメーションテクノロジーの発展により、制御システムにおいてもオフィスなどで利用されるITシステムと同じ技術が用いられるようになり、ITシステムと同様のサイバー攻撃が通用するようになってきた。

実際に、Windowsの脆弱性を利用したマルウエアStuxnetにより、イランの核燃料施設にあるウラン濃縮用遠心分離器を異常作動させ破壊した事件（2010年）や、Windowsの脆弱性を突いたコンピューターワームConfickerによる南米の発電所の停止（2011年）等が起こっている[1]。

1 「制御システムセキュリティの脅威と対策の動向およびCSSCの研究概要について」（技術研究組合制御システムセキュリティセンター、2014年9月16日）
http://www.css-center.or.jp/pdf/about_CSSC_20140916.pdf

©2015 KPMG Consulting Co., Ltd., a company established under the Japan Company Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

2. 制御システムとITシステムの特徴

制御システムの情報セキュリティ対策では、まずオフィスなどで利用されるITシステムとの次のような特徴の違いを理解する必要がある。制御システムの要諦は安全性で、かつ障害や停止が発生しにくいように設計されていることがわかる。

【図表1】制御システムとITシステムの特徴

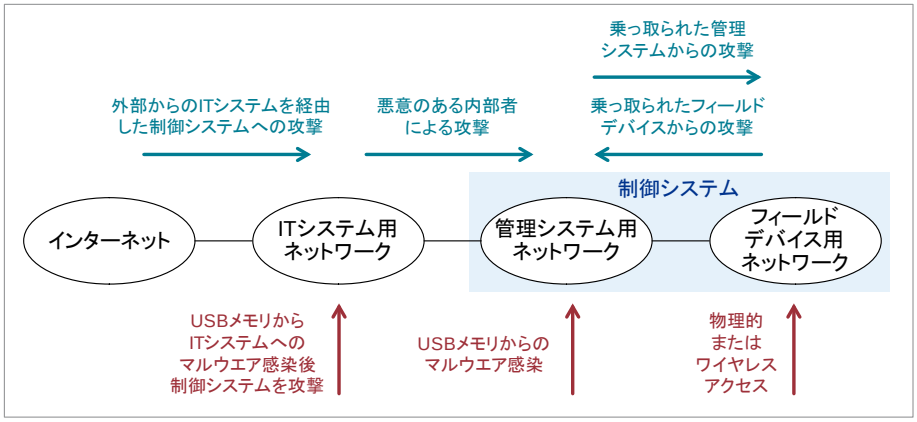
項目	制御システム	ITシステム
リスク管理	人の安全性を最も重要とし、機器の保全やプロセスの可用性も重要である	データの機密性と完全性が最も重要である
機器	伝統的に特殊な機器が用いられる	PC技術が用いられる
ライフサイクル	長期（10-18年間）	短期（3-5年）
処理速度	リアルタイム処理で遅延は許容不可である	高速処理ではあるがリアルタイム処理ではない
使用環境	システムは高温、ほこり、振動といった過酷な環境に耐えなければならない	システムはデータセンター等の環境で運用される
通信プロトコル	特殊プロトコルと汎用プロトコルが混在して利用されている	汎用プロトコルが利用されている
セキュリティツール	セキュリティツールは制御システム用に開発する必要がある	汎用のセキュリティツールが存在する
システム変更	システム変更の際は、制御システムを停止、または冗長化する	システム変更は手順に従って実行、または自動実行される

3. 制御システムへのセキュリティ攻撃パターン

制御システムは、直接インターネットに繋がっていることは少ないが、オフィスなどで利用されるITシステムのネットワークを経由して、インターネットに繋がっている場合があり、ITシステムを経由した外部から攻撃される可能性がある。

さらに、制御システムは、一般的に制御用のコンピュータや監視用の画面といった管理システム、およびフィールドデバイスと呼ばれる制御システムから実際に制御されるセンサーやアクチュエータ（作動器）等の装置や機器から構成され、それぞれが以下のようなセキュリティ攻撃の対象となる。

【図表2】制御システムへのセキュリティ攻撃パターン



©2015 KPMG Consulting Co., Ltd., a company established under the Japan Company Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

4. 制御システムにおける情報セキュリティ対策

特定の対策や技術だけで情報セキュリティを担保できないのは、制御システム・ITシステムともに同じである。制御システムもITシステムのセキュリティ対策と同様に、次のような組織・プロセス・技術の対策がまず重要である。

- 組織的対策：規程・マニュアルの整備、従業員教育、インシデント対応チーム組成
- プロセスに関する対策：リスクアセスメント、ログ監視
- 技術的対策：侵入テスト、セキュリティログ分析　等

この対策に加え、前述した制御システムの特徴および攻撃パターンを考慮し、例えば、次のような制御システム固有の対策を検討していく必要がある。

- ITシステム用ネットワークと制御システム用ネットワークを非接続とすること
- 制御システムのソフトウエアベンダーおよびOSベンダーからのパッチやアップデートといったセキュリティ対策を、インターネットに接続せず実施すること
- 制御システム固有のプロトコルに特化したファイアウォールを導入すること　等

5. まとめ

海外では犯罪組織等が関わる制御システムに対する攻撃の報道もあるが、国内では制御システムへの大きな攻撃はまだ報告されていない。しかし、報告がないために対策の優先度が下げられ、潜在的な攻撃対象となる制御システムが多数存在していることが懸念される。

制御システムの情報セキュリティ対策といっても、基本的にはITシステムにおける対策の考え方が準用できる。その上で、制御システムの特性に合わせた個別対策を施すことが求められる。

KPMGコンサルティング株式会社
シニアマネジャー　万仲　隆之

Windowsは米国Microsoft Corporationの米国およびその他の国における登録商標です。

KPMGコンサルティング株式会社

東京本社
〒100-0004
東京都千代田区大手町1丁目9番5号
大手町フィナンシャルシティ　ノースタワー
TEL ： 03-3548-5305
FAX ： 03-3548-5306

名古屋事務所
〒451-6031
名古屋市西区牛島町6番1号　名古屋ルーセントタワー
TEL ： 052-571-5485

kpmg.com/jp/kc

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

©2015 KPMG Consulting Co., Ltd., a company established under the Japan Company Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International.