2013年12月25日

独立行政法人情報処理推進機構（IPA）

狙われる脆弱性・・・SCADA システムの真の問題とは？

～SCADA システムのパッチ管理に関するグッドプラクティス～

本概要は、欧州ネット・情報セキュリティ機関（ENISA：European Network Information Security Agency）が発行する、“Windows of exposure...a real problem from SCADA systems? – Recommendations for Europe SCADA systems?” の概訳となります。内容の詳細につきましては、原文をご参照ください。

URL：

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/window-of-exposure-a-real-problem-for-scada-systems

この10年間で制御監視（SCADA）システムは、独自仕様の隔離されたシステムから、オープンアーキテクチャや標準技術を使った、社内ネットワークやインターネットに接続されたシステムへと大きな変革を遂げた。この変革は、外部からの攻撃への脆弱さを増大させることにもなった。SCADA システムのセキュリティを強化する方法の1つは、パッチを適切に適用することである。

SCADA システムにパッチを適用するにあたっては、鍵となる2つの大きな問題がある。「パッチの不良率の高さ」と「パッチの提供率の低さ」である。ICS-CERT の Kevin Hemsley 氏によれば、2011年当時 ICS-CERT に届け出があった脆弱性の対策パッチの不良率は60%であったという。また、2012年当時公開されていた364件の脆弱性のうち、パッチが提供されていたのは50%以下であったという。

セキュリティの観点から言えば、パッチは脆弱性を修正し、正常な動作を維持する極めて重要なものだが、安全性の観点から言えば、システムの安定性を脅かしかねないものである。

とは言え、欧州として「パッチを当てていない SCADA システムに依存することが許されるのか？」という懸念もある。2011年の報告書に記したように、サービスを中断することなくパッチを適用することを可能にする技術の研究が求められている。

SCADA システムにおけるパッチ適用の現状

SCADA システムへのパッチ適用に関しては、できるだけ迅速に適用しようという企業や、あまり乗り気でない企業、確たるポリシーが無く、パッチを適当するかしないかは現場のエンジニア任せの企業など、様々なケースが考えられる。

パッチ管理ポリシーの検討にあたっては、北米電力信頼度協議会（NIRC）の「Critical Infrastructure Protection（CIP）」、米標準技術研究所（NIST）の「NIST SP800-82 産業制御システムガイド」、International Society of Automation（ISA）の「TR62443-2-3 産業オートメーション・制御システムセキュリティ」、独連邦エネルギー・水道連合会（BDEW）の「Anforderungen an sichere Steuerungs- und

Telekommunikationssysteme, Ausführungshinweise zur Anwendung des BDEW Whitepaper」等を参考にすることができる。なお、最後の BDEW による白書の2.1.1.3節では、重要インフラにおけるパッチの適用に関して以下のように定めている（抜粋）。

1. 通常のシステム運用内で、全てのコンポーネントにパッチが適用できること
2. 通常のシステム運用を中断させることなく、また、可用性に影響を与えることなくパッチが適用できること
3. できれば、先ずは冗長環境でパッチを適用し、検証すること
4. ベンダは、システム全体のパッチ管理を支援すること
5. パッチの適用／解除は必ずシステム所有者の許可を得てから行うものとし、自動化しないこと

パッチ適用に関する考慮事項： 運用面

パッチの適用にあたっては、運用面において以下を考慮するべきである。

● パッチ管理ポリシー

パッチ管理の目的は決められた手順と方法で、システムのセキュリティと機能を最新に保つことである。IT システムと SCADA システムではダウンタイムの許容度や優先すべきことなどに相違があるため、ポリシーは IT システム用と SCADA システム用に分けて策定する必要がある。ポリシーには、構成管理（ハード、ソフト）、パッチ管理（スケジュール、手順等）、バックアップ計画、パッチ検証計画、インシデント対応計画、運用部門との調整、パッチが適用できないシステムへの対応等を含める。

パッチ管理は、法規により要求されている場合も多い。パッチ管理を検討し、実施証跡等を残す場合、法規へのコンプライアンス要件を満たしていることを確認する必要がある。

● 脆弱性・パッチに関するベンダとのサービス契約

ベンダと交わすサービス契約には、パッチ管理におけるベンダの責任範囲が規定される。最も一般的なのは、ベンダが OS と SCADA アプリケーションの脆弱性の是正に責任を負う、というものである。他にも「どのレベルで誰が検証するのか」「どのレベルで誰が適用するのか」、「パッチのシステムへの配布方法」「問題発生時の責任は誰が負うのか」「サービス契約の有効期限はいつまでか」などについてもベンダと相談する必要がある。

パッチ適用に関する考慮事項： 技術面

また、技術面にはおいては、以下を検討するべきである。

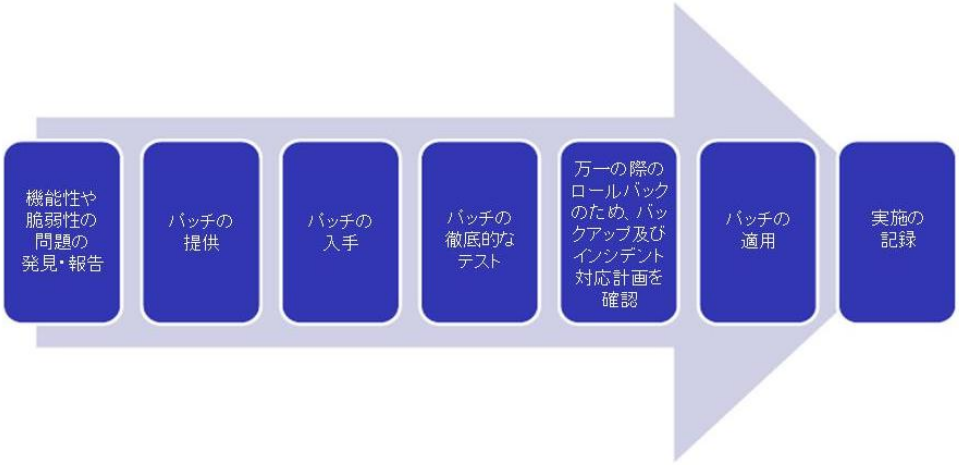
● パッチを適用しないという選択

状況によってはパッチ適用しない、という選択も考えられる。事情は様々あると思われるが、どうしても適用のためのダウンタイムが許容できなかったり、適用に伴うリスクが恩恵（当該パッチにより解決される脆弱性がもたらすリスク）を遥かに上回る、影響を受ける機器の CPU やメモリなどのパッチ処理のためのリソースの不足、サポート切れやベンダの撤退・廃業によりパッチが提供されない、リスク低減に

ファイアウォールなど代替対策を取っている、等が挙げられる。何にしても、製品の設計段階など、早期からパッチ管理について検討することが望ましい。

- **SCADA システムへのパッチ適用フロー**

パッチの適用は以下のフローで行われることが望ましいが、パッチがすぐに提供されるとは限らないほか、徹底的なテストが必要になるためすぐには適用できず、システムが脆弱な状態がある程度続くことも想定される。



パッチは、先ずは開発環境などでテストし、問題や影響がないことを確認してから本番環境での適用を検討する。テストの実施以外にパッチがシステムに悪影響を与えるリスクを低減する方法として、パッチ適用の優先度付けがある。例えば、システムを重要度よってグループ化し、パッチが出たらそのまま開発環境や訓練環境といった重要度の低いシステム(「Early Adaptors」)に当て、問題が一定期間出なければ、重要度の高い本番環境(「Business Critical Systems」)にも適用する。また、所在が地理的に広範囲にわたっているシステムの場合、システムの所在地と重要度でグループ化し、先と同様に重要度の低いシステムからパッチを適用する。これにより、何かあった場合でも技術者が迅速に駆けつけ対処することが可能となる。

SCADA システムにおけるパッチ適用の課題

IT システムにおけるパッチ管理はかなり確立されているが、SCADA システムは IT システムとは異なるため、そのまま流用するのは難しい。以下に、幾つかの観点から見た課題の例を挙げる。

- 運用上の課題
  - SCADA システムの脆弱性の深刻度の評価に、IT システムの脆弱性の深刻度の評価手法(Common Vulnerability Scoring System:CVSS)を使うのは適切ではない(制御環境に合わせ、カスタマイズが必要)
  - SCADA システムの脆弱性の根本原因への取組が必要(多くはバグでなく仕様(意図的な設計))
  - パッチ適用までに時間が掛かることを考慮すると、脆弱性情報に攻撃コード情報を含めることで、攻撃者に更なるアドバンテージを提供してしまう、など

- 技術面での課題
  - パッチ管理システムが必要（但し、同システムを攻撃に悪用された場合のリスクも大きな懸念）
  - パッチを適用するために、システムを止められない
  - 未だ古いシステムを多く利用しており、パッチが存在しない（サポートが終了、またはベンダが撤退・廃業している）、など

- 法的な課題
  - 多くの SCADA ベンダは国際企業であり、様々な国の法規に縛られることになる。これらの法規が、パッチの提供に影響を及ぼす可能性がある
  - オープンソースの使用に伴う法的問題の有無の確認が、パッチの開発・提供に影響を及ぼす可能性がある、など

グッドプラクティスと推奨策

以下に、SCADA システムにおけるパッチ適用にあたってのグッドプラクティスの例を挙げる。

- パッチ適用以外の対策（補償対策）
  - 不要な機能やサービスの停止など、SCADA システムのセキュリティを堅固にする
  - ファイアウォールの活用、ネットワークのセグメント化による多層防御を導入する、など

- パッチ管理プログラムの立ち上げ＆サービス契約
  - パッチ管理プログラムを立ち上げる（パッチ管理ポリシーを策定する）
  - パッチ管理に関するサービス契約をベンダと取り決める、など

- パッチのテスト
  - ユーザ側でも必ずテストを行う（テスト環境はできるだけ本番環境に似せる）
  - 認定を取得しているシステムは（例：FIPS140-2等）、パッチ適用後、原則認定を取り直す、など

- パッチの配布
  - 可能かつ現実的な限り、デジタル署名またはハッシュによる検証を活用してパッチの正当性を確認する、など

- パッチ適用のスケジュール
  - 本番環境への適用は、テストが完全に終わってからとする
  - システムへのパッチの配布方法によっては、運用部門の責任者の許可を得る、など

パッチ管理は、セキュリティ上の問題を全て解決してくれる特効薬ではないが、重要なセキュリティ対策の1つであり、各々の組織に即したポリシーに基づき、適切に行っていくことが重要となる。

以上