2012 年 8 月 9 日
独立行政法人情報処理推進機構（IPA）

# ICS-CERT マンスリー・モニター（2012 年 5 月号）概要

本概要は、米国土安全保障省の運営する ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）発行の“ICS-CERT Monthly Monitor May 2012”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。（※本文中のリンク先は、全て英文となります）

URL：http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_May_2012.pdf

## 1. 4 月のインシデントレスポンス活動 - 外部記録媒体によるウィルス感染未遂事件

電力会社にて、外部記録媒体を通じた制御システムのウィルス感染未遂事件が発生。作業員が、制御システムに接続されている管理 PC の USB ポートに外部記録媒体が挿されているのを発見し、不審に思い外部記録媒体、管理 PC および制御システムのウィルスチェックを行ったところ、外部記録媒体がウィルスに感染していることが判明。管理 PC および制御システムはオートラン機能が無効になっていた為、感染していなかった。なお、外部記録媒体は、別の作業員がルーティン業務の中でデータをダウンロードする為に使用し、抜き忘れたものと判明しており、悪意のある行為ではなかった。

＜外部記録媒体の利用に関する対策例＞

- 出所不詳な媒体や、私物の媒体は決して接続しない
- 媒体は組織所有のものを明確にラベル付けして管理、使用する
- 不具合のあるものや、感染の疑いのある媒体は、使用可能なものと分けて保管する
- 可能な限りシステムのオートラン機能を無効化する

## 2. 今月のトピックス

（1）国際環境における脆弱性情報ハンドリングの複雑さ

2011 年の、Billy Rios 氏と Terry McCorkle 氏による 100 の SCADA 脆弱性発見を例に見てみると、先ず、複数国、複数ベンダ、異なる言語やコミュニケーション手段に跨ってのパッチ開発、情報公開の調整に時間と労力が非常に掛かる。また、研究者がどのように公表することを考えているかによって、脆弱性のもつ影響力や、研究者と CERT の関係も大きく変化する。

（2）XP サポート終了予定

Windows XP SP3 の延長サポートの終了期限が、2014 年 4 月 8 日に終了。リプレイス・アップデートにあたって、以下の懸念が考えられる。

- 制御システム・機器ベンダは、Window のライフサイクルを考慮していない、新しい IT 環境への移行をどうするか
- 制御系のアプリケーションの動作要件に、XP SP3 でしか使えない又はサポートしていないブラウザ等がないか。あった場合どうするか
- 制御系機器で、組み込みシステム向けの XP や Windows CE を必要するものがないか。あった場合どうするか

## 3. Control System Security Program（CSSP）ニュース

＜Industrial Control Systems（ICS）Joint Working Group（JWG） 2012 Spring＞

ICSJWG 2012 Spring が、ジョージア州サバンナで開催され、インシデントレスポンス、標準の策定、解析手法やツール、脆弱性管理に情報共有など幅広いテーマでパネルやプレゼンテーション、トレーニングが提供された。中でも、インシデントレスポンスは共通のテーマとしてカンファレンスを通じて取り上げられ、ICS-CERT によるリモート支援や、実際に現地に人員を派遣して行ったオンサイト支援の内容を学ぶセッションもあった。このほか、8 時間の制御システムセキュリティトレーニングコースや、他国からの参加者との情報共有を目的とした International Partners' Day などが開催された。

次回、ICSJWG 2012 Fall は、今秋 10 月 15 日～18 日にコロラド州デンバーで開催される。

## 4. 最近公表された制御システム関連の脆弱性

原文の RECENT PRODUCT RELEASES をご参照ください。

## 5. 今月のオープンソースニュース（ハイライト）

- ブレットタイム（bullet time）の考え方をサイバーセキュリティに応用。攻撃を検知した場合にネットワークの速度を遅くし、防御側に攻撃をかわす時間的猶予を与える（2012-04-20）
- セキュリティ基盤のなさこそが問題 ― 重要インフラを守るため、米国はリスク評価に基づいた効果的な対策を可能にする、システムライフサイクルに沿った総合的なアプローチを取ることが重要（2012-04-27）
- 電力や交通管制システムなどのミッションクリティカルなシステムにバックドア（2012-04-25）
- サイバー攻撃に対する備えが足りないのはわかるが何をすればよいかはわからず（2012-04-25）
- 米国に対して大規模なサイバー攻撃が行われるのは時間の問題。議会にサイバーセキュリティ対策の規制化を迫る（2012-04-24）
- イランの石油業界にサイバー攻撃。制御システムがウィルスに感染（2012-04-23）
- 日本で制御システム向けのセキュリティセンタが開設。60 名以上の重要インフラ関係者および経済産業省（METI）が参加（2012-04-20）
- 着用可能なファイアウォールを用いて、心臓ペースメーカのハッキングを防止（2012-04-19）
- スマートグリッドのセキュリティ対策、整備に追い付かず（2012-04-18）
- APT 攻撃 ― 検知は困難だが、ログや通信を注意深く分析することで日頃とは違う動きを見つける糸口に（2012-04-18）
- 米エネルギー省パシフィックノースウェスト研究所、コンピュータをマルウェアに感染させたのがどのアプリケーションで、どの外部ネットワークと接続しているのかを自動的に探すオープンソフトウェアツール“Hone”をリリース（2012-04-17）
- ABB WebWare にバッファオーバーフローの脆弱性。システムライフサイクル的に末期にある製品のため ABB は修正パッチ提供せず（2012-04-04）
- 米国の水道や電力業界あてのサイバー攻撃、日々増加（2012-04-04）
- 大手電力会社のシステム機器の脆弱なパスワードが、システムをハッキングの危険に晒す（2012-04-04）

## 6. 今後のイベント

原文の UPCOMING EVENTS をご参照ください。

以上