2012 年 9 月 5 日

独立行政法人情報処理推進機構(IPA)

ICS-ALERT-11-343-01A インターネットから接続可能な制御システム

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)が発行する、"ICS-ALERT-11-343-01A-Control System Internet Accessibility"の抄訳となります。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-ALERT-11-343-01A.pdf

1. インターネットからアクセス可能な制御システムが存在

ICS-CERT では、研究者や専門家による SHODAN(インターネットに接続されているコンピュータ機器を探せる検索エンジン)、ERIPP(Every Routable IP Project:インターネット上の全ての IP アドレス(ポート 80)への接続を試みるプロジェクト)、グーグルその他の検索エンジンを利用した、インターネットに接続されている制御システムを探す調査研究に関するレポート等をチェックし、対応を行っている。こうしたインターネット上で利用可能なサーチエンジンやツールは、調査研究だけでなく、ハッカーによるサイバー攻撃に利用されている。

インターネットに接続された制御システムが発見された場合、ICS-CERT では、所有者や運用者にサイバー攻撃により侵入される危険性があることを通知し、侵入の有無や影響の調査・対策の支援を行っている。

これ迄にも、重要インフラ業界の複数事業者でインターネットからアクセス可能な状態にある制御システムが見つかっている。多くは、制御システムの脆弱な状態を認識していなかったり、設定ミスであったり、リモートモニタリングやメンテナンスのためといった事情がある。また、ファイアウォールを設置せず直接インターネットに接続していたり、パスワードもデフォルトのままなケースが多々ある。デフォルトパスワードはしばしば公開文書に記載されており、セキュリティ強度はないに等しい。ICS-CERT では、所有者、運用者、ベンダと協力し、こうしたセキュリティ上の脆弱な点を是正すべく、セキュリティ対策の見直しを支援している。

2. ICS-CERT に報告があった最近の事例

- 2011 年 2 月、複数事業者の監視制御システム(SCADA)がインターネットに接続されている旨の報告を受ける。詳細調査により、多くがデフォルトの ID/パスワードを利用していることが判明
- 2011 年 4 月、水道業界を中心に 75 のインターネットに接続された制御システム機器について報告を受ける。詳細調査により、多くがデフォルトの ID/パスワードを利用しることが判明
- 2011 年 9 月、数千のインターネットに接続された制御システム機器について直接報告を受ける。現在までに、海外を含め、63 の他の CERT と協力し、問題の制御システムの所有者・運用者に通知・支援を行っている

また、システムへのアクセスに関する脆弱性は、システムや機器の認証機能自体が脆弱であったり、ID/パスワードを所有者・運用者によって変更できないなど、是正が困難なケースもある。以下に、そうし

た製品の脆弱性の例を挙げる。

- ClearSCADA：例外処理発生時に、認証無しにセーフモードで診断機能が利用可能になる脆弱性
- シーメンス：脆弱なトークン生成機能により認証が回避される脆弱性
- RuggedCom：デフォルトのバックドアアカウント（パスワードは画面表示されるMACアドレスを強度の弱い暗号方式で返還したもの）の脆弱性

3. 対策

ICS-CERT では、所有者・運用者に対し、自身の制御システムがインターネットに接続していると信じる、信じないに関係なく、制御システムの監査を行い、デフォルト ID/パスワードを是正するよう勧告している。なお、確認方法・是正方法については、必要に応じてベンダに相談すること。

DHS Control System Security Program（CSSP）では、制御システムのセキュリティ評価ツール（無料）Cyber Security Evaluation Tool（CSET）を提供している。本ツールでは、以下の評価を可能にしている。

1. 現状のセキュリティ対策方針の提示
2. セキュリティの改善が必要な個所の特定
3. 既存のシステム構成／ネットワーク構成の明確化
4. 基礎的なサイバーセキュリティ計画の提示

また、ICS-CERT では、制御システムの脆弱性を軽減するため、以下の施策の実施を勧告している。なお、実際に対策を行う前に、影響分析とリスク評価を行うこと。

- 制御システム機器のネットワークへの接続は最低限に抑える。制御システムは、インターネットに直接接続させない
- 制御システムネットワークとリモートデバイスは、ファイアウォールで守る。また、企業のビジネスネットワークとは隔離させる
- リモートからのアクセスが必要な場合、VPN（Virtual Private Network）などセキュアな手段を用いる。但し、VPN のセキュリティの強度は、接続機器のセキュリティの高さ（弱さ）に準じることを理解した上で検討する
- 可能な限り、デフォルトのシステムアカウントは削除、無効化、またはリネームする
- ブルートフォースアタックによるリスクを軽減するため、アカウントのロックアウトポリシーを設定する
- 強固なパスワードの使用を義務付けるポリシーを導入する
- 第三者ベンダによる管理者レベルの権限を持つアカウントの作成を監視する

補足リソース

CSSP：多層防御戦略による制御システムのサイバーセキュリティの改善

ICSA-10-228-01-ベンダによるデフォルト管理者アカウントに関する注意喚起

ICS-CERT：CSAR-SSH スキャニング（ブルートフォースアタックを用いて、制御システムのウェブインターフェース（HMI）のログイン情報を入手するための、戦術や手法、手順について解説）

以上