2012 年 9 月 13 日
独立行政法人情報処理推進機構（IPA）

制御システムセキュリティプログラム（CSSP）
ICS-CERT 脆弱性公開方針

本ドキュメントは、米国土安全保障省の制御システムセキュリティプログラム（CSSP：Control Systems Security Program）における、ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）の制御システムに関する脆弱性の公開方針“ICS-CERT Vulnerability Disclosure Policy”の日本語訳となります。
原文 URL： http://www.us-cert.gov/control_systems/ics-cert/disclosure.html

---

制御システムセキュリティプログラム（CSSP）
ICS-CERT 脆弱性公開方針
ICS-CERT では、届出を受けた全ての脆弱性について、関係ベンダとの調整に努めています。

セキュリティパッチの準備および脆弱性情報の公開方法・公開時期に関するタイムスケジュールは、関連する要因に応じて決定します。考慮すべき状況、例えば、攻撃が活発に行われている場合、脅威が特に深刻である場合、現状確立されている決まりごとを変更する必要性がある場合などには、公開が早まったり、遅れたりすることが考えられます。その他の要因には、以下のようなものがあります。

- 既に一般に公表されている脆弱性か
- 脆弱性の深刻度
- 重要インフラへの潜在的な影響
- 国民の健康と安全に対して脅威となる可能性
- 直ぐに対策が可能か
- ベンダの対応（積極性）、バージョンアップやパッチ準備の実現性
- エンドユーザがパッチを入手し、テストし、適用するのに必要だと、ベンダが想定する時間

脆弱性届出者の氏名と連絡先は、本人からの異議がない限り、関係ベンダにお伝えさせて頂きます。ICS-CERT では、届出を受けた脆弱性の対策状況に進展があった場合、ベンダより内密に提供を受けた情報を漏らさない範囲で、届出者に状況をお知らせします。

ICS-CERT による情報公開に関する予定は、全て関係ベンダに通知されます。スケジュールの変

更については、必要に応じて関係ベンダと交渉を行います。

【今回更新】ベンダの対応が鈍い場合、または、ベンダが提示するパッチの準備に必要なタイムスケジュールが妥当ではないと思われる場合、ICS-CERT はベンダに脆弱性発見の通知をした日から 45 日後以降に、パッチや回避策の在る無しに関わらず、脆弱性情報を公開することがあります。

本情報公開方針の目的は、セキュリティ上の脆弱性について知っておかなければならないという制御システム・コミュニティのニーズと、効果的に対応するためには時間が必要だとするベンダのニーズのバランスを取ることにあります。最終的な脆弱性の公開方法・公開時期は、全体の利益を最優先に考えて決定されます。

ICS-CERT の脆弱性対策プロセスは、5 つの基本的段階によって行われます。

1. 検知／情報収集 ― ICS-CERT では、次の 3 つの方法で脆弱性情報を収集しています:
   - ICS-CERT による脆弱性分析
   - 公開されている脆弱性情報の監視
   - ICS-CERT への直接の届出

   脆弱性の届出を受けると、重複や誤報告を排除するため、先ず一次分析を行います。その後、その時点でわかっているあらゆる情報（公開・非公開）を含め、脆弱性の分類を行います。

2. 分析 ― 分類が終了すると、ベンダおよび ICS-CERT のアナリストが脆弱性の分析を行い、問題および潜在的な脅威の特定と検証を行います。ICS-CERT の分析には、Advanced Analysis Lab による脆弱性のテスト、必要な調査研究の実施、関係ベンダと直接やり取りしての協同作業などを含みます。

3. 対策の調整 ― 脆弱性の分析後も引き続きベンダと協力し、パッチや回避策の準備を行います。ICS-CERT では、脆弱性の公開、全体的な技術評価およびテストに関して、安全で信頼性の高いパートナーシップを制御システムベンダと確立しています。ベンダが不具合を効果的に解決し、リグレッションテストを行う十分な時間が取れるよう取り組みます。また、ICS-CERT では、複数ベンダの製品に影響を与える脆弱性についても、調整を行った経験があります。

4. 対策の適用 ― 情報公開の前にベンダと共に、エンドユーザが対策情報を入手し、テストを行い、対策を実施するのに十分な時間が取れるよう取り組みます。

5. 公開 ― ベンダとの調整および技術情報・脅威情報の収集後、適切な手順に基づき、エンド

ユーザに脆弱性を公開します。ICS-CERT では、事業者や運用者のため、技術的な修正やリスクの軽減に重きを置いた、正確で、中立的、客観的な情報の提供に努めています。また、可能な限り、他にも情報がある場合には参考情報として提供しているほか、誤情報の際には訂正を行っています。

ICS-CERT に脆弱性を届け出る場合は、ics-cert@dhs.gov にメールを送るか、1-877-776-7585 に電話をください。機微な情報をメールで送る場合には、暗号化することを奨励しています。

ICS-CERT PGP 公開鍵のダウンロード

【IPA 補足】
今回 ICS-CERT の脆弱性公開方針で更新された【45 日】は、情報セキュリティ早期警戒パートナーシップガイドライン(3.(2) 3))に規定された、製品の脆弱性の公開目安と同じになります。

「情報セキュリティ早期警戒パートナーシップガイドライン」
http://www.ipa.go.jp/security/ciadr/partnership_guide.pdf