2015 年 10 月 30 日
独立行政法人情報処理推進機構（IPA）

WaterISAC／ICS-CERT：10 Basic Cybersecurity Measures 概要

本概要は、米水道業界の情報共有組織 WaterISAC（Water Information Sharing and Analysis Center）と国土安全保障省（DHS）の ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）のパートナーシップによって作成された、“*10 Basic Cybersecurity Measures*”の概訳となります。内容の詳細につきましては、原文をご確認ください。
URL：
https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf

“*10 Basic Cybersecurity Measures*“は、WaterISAC が 2012 年 8 月に発行した“*10 Basic Cybersecurity Measures to Reduce Exploitable Weakness and Attacks*“の改訂版であり、ICS-CERT、IT-ISAC、連邦捜査局（FBI）の協力を得て作成された。ICS-CERT は、1～3 の対策を行っていれば、2014 年度に ICS-CERT に報告されたインシデントを検知し、被害を防止できただろうと述べ、1～3 の対策をできるだけ早く実施するよう勧告している。

※ 原文では、各項目の最後に対策の参考となる ICS-CERT や標準技術研究所（NIST）のガイドラインへのリンクがあります

1. 制御システム機器の正確な棚卸しと管理、およびそれらの機器が外部ネットワークにつながっていないことの確認と徹底

制御システムネットワーク内の機器を、ビジネス（OA）ネットワークやインターネット上の機器と直接通信させないこと。インターネットに直接つながっていなくても、外部ネットワークにつながるビジネス（OA）ネットワーク等につながっている場合、「通信経路」が存在することになる。組織がそうした直接的・間接的通信経路の存在に気づいていないこともあるが、攻撃者はそうした通信経路を見つけ出し、制御システムへの攻撃に利用してくる。

事業者は、ビジネス（OA）ネットワークを含め徹底的な見直しを行い、制御システム機器と外部ネットワーク上の機器との間の通信経路を潰すことが望ましい。

2. ネットワークのセグメント化とファイアウォールの導入

ネットワークを物理的または論理的に分け、アクセス制御を実施することで、侵入を一定範囲内に局地化し、攻撃者が「最もセキュリティが弱い箇所から侵入し、水平移動する」のを防ぐこと。IoT 機器が続々とつながってくる今後、ネットワークのセグメント化はますます重要となる。

セグメント化は、制御システムの場合物理的に分けることができれば最善だが、ファイアウォールを用いることもできる。通信経路を絞り、残った通信経路に適切なセキュリティ対策を実施して、侵入を困難にする。セグメント化により、アクセス制限の実施や監視、通信フローの管理が可能になり、異常や不審な通信に気付く

ことができるようになるなど、検知や防御が可能になる。

3. リモートアクセス時のセキュリティの確保

リモートアクセスは、エンドユーザに多大な利便性を提供するが、その実現には VPN（Virtual Private Network）などセキュアな方法を利用すること。接続可能な IP アドレスの制限や国内からのアクセスに限る等の制約を行うことで、よりセキュアになる。但し、VPN のセキュリティは接続機器のセキュリティに委ねられるため、接続機器がマルウェアに感染している場合などには意味がなくなってしまうことに留意すること。

4. ロールベースのアクセス制御およびログの取得

ロールベースのアクセス制御を行い、業務内容に応じたアクセス制御を実施すること。業務の遂行に最低限必要な権限のみ付与することで、権限の悪用を困難にする。また、ログの取得により、ユーザによるシステム操作を監視できるようになる。これにより、何か起こった場合に問題の原因究明や、問題が顕在化する前に手を打つ機会が得られるようになる。

5. 強固なパスワードの使用、デフォルトパスワードの変更、他の認証方法の利用の検討

デフォルトパスワードは直ぐに変更すること。また、パスワードは最低 8 文字以上とし、大文字小文字、数字、特殊文字など含め、使い回しをしないこと（違うアカウントには違うパスワードを使用すること）。アカウントロックアウト機能などのセキュリティ機能も併せて使うほか、パスワードは定期的に変更すること。生体認証など他の認証方法との組み合わせて使うことを検討するのも良い。

6. 脆弱性に対する意識向上、および必要なパッチやアップデートの適用

多くのベンダは脆弱性が見つかった場合、パッチやアップデートを提供する。しかし、パッチやアップデートがリリースされても、事業者が脆弱性やパッチやアップデートの存在を知らなかったり、知っていても適用しないことを選択し、多くのシステムが脆弱なまま放置されているのが実状である。シスコ社の 2015 Annual Security Report によれば、最高情報セキュリティ責任者（CISO）の 40%が脆弱性対策をしていないと回答しており、放置された脆弱性が攻撃者にとって格好の標的となっている。

組織を守るために脆弱性対策は必須である。漏れのないよう自動アップデート機能なども活用し、脆弱性対策を行うことが望ましい。

7. モバイル機器向けのセキュリティポリシーの策定と実施

会社支給・私用を問わず、気軽に持ち歩かれ、外部ネットワークに日常的に接続するノート型 PC、タブレット、スマートフォンなどのモバイル機器は、業務での利活用が増えるにつれ、組織にとってセキュリティ上の大きな課題となっている。

事業者は、モバイル機器のオフィスでの使用やネットワークへの接続に関するポリシーを定め、従業員だけでなく請負契約者を含め、関係者全員に厳格に守らせることが重要となる。

8. 従業員向けのサイバーセキュリティ教育プログラムの実施

サイバーセキュリティはチームワークと認識し、組織の全員がそれぞれの役目を果たすこと。関係者一人一人がセキュリティ対策に参画していないと、脅威に気付かず見逃してしまったり、関係者が攻撃の媒体として利用される可能性があるため、関係者が定期的にセキュリティ教育を受け、組織全体のセキュリティの維持に一助を担うことが重要となる。

中でも、あの手この手で関係者に認証情報等の漏洩や添付ファイルの開封等をさせようとするソーシャルエンジニアリングの手法や、ウェブサイトにアクセスしただけでマルウェアに感染させられるドライブ・バイ・ダウンロード攻撃、よく行くウェブサイトを介してマルウェアに感染させられる水飲み場攻撃など、ウェブサイトの閲覧に関する教育が必須となる。

9. 経営陣のサイバーセキュリティ対策への参画

Ponemon Institute の調査によれば、経営陣と日頃からサイバーセキュリティに関してやり取りをしていると回答したセキュリティ担当者は 20%であったほか、インシデント発生の際に経営陣も関与すると回答したのは僅か 14%であった。経営陣のサイバーセキュリティに対する意識や関与は未だに低く、予算の確保や対策の実行力にも影響を与えていると想像される。ThreatTrack Security による別の調査では、経営陣の 44%が CISO がセキュリティインシデントに関する最終的な責任を負うべきと回答したのに対し、セキュリティ対策の予算や調達に関しては 54%が CISO を責任者にするべきでないと回答するなど、CISO が必要な支持と権限を得られていない状況が浮き彫りになっている。

Mandiant は、インシデントが起こった場合、メディア、取引先、投資家、顧客らがインシデントに係る情報をより詳しく要求してくる傾向にあり、情報を提供しない場合勝手な憶測が広まる可能性があることからも、タイムリーに情報を提供するため、社内における密接なコミュニケーションと情報共有が重要になると指摘している。

10. 侵入を検知するための対策とインシデント対応計画の策定

サイバー攻撃はあれこれと対策をしていても完全には防げない。従って、如何に早く侵入を検知し、対応できるかが重要であり、そのための対策・準備を行っておくこと。検知にはウィルス対策ソフト、侵入検知システム（IDS）、侵入防止システム（IPS）が広く使われているが、これらに頼り切るのではなく、ファイアウォール、IDS/IPS センサ、サーバ等のログを活用し、侵入の兆候を見逃さないよう努めることが望まれる。また、対応計画には、制御システムに破壊的マルウェアが侵入し、自動処理やネットワークが使用できなくなった場合に備え、手動での運用を想定しておくことが望ましい。

対応計画は一部署が策定するのではなく、全関係部署を巻き込み策定することで、必要関係者の協力と理解を得ることが期待できる。策定した計画は定期的に見直し、必要に応じて更新するほか、定期的に訓練を行うことが重要である。

以上