標準から学ぶ **ICS** セキュリティ **#2**

ゾーンとコンジット
（Zone and conduit）

2022 年 10 月 27 日

一般社団法人 JPCERT コーディネーションセンター
制御システムセキュリティ対策グループ

1. はじめに

ICS セキュリティにおける一つの大きな分野が ICS ネットワークのセキュリティです。IEC 62443 では、ICS ネットワークのセキュリティ設計のための基本概念として「ゾーン（zone）」と「コンジット（conduit）」を定義しています。プラントにおいては安全を担保するための区画が設けられ、区画ごとに許される作業や行為が定められています。こうした区画を設定することにより事故を防ぐ考え方を ICS ネットワークに当てはめて作り出された概念が「ゾーン」であると言ってよいかと思います。また、異なるゾーン間を行き来するための通路であって、通路を通ってゾーンをデータや制御が出入りする際の検査プロセスを伴ったものを「コンジット」と呼んでいます。

一般的な情報セキュリティの議論でも類似した概念が存在しますが、システムやネットワークの区画に対して「ゾーン」という用語が使われることはあまりありません。おそらく、標準化に携わった ICS エンジニアが、慣れ親しんでいたプラント安全の方法論を踏まえ、熱い思いを込めて IEC 62443 に「ゾーン」の概念を取り入れたものと推測されます。本稿では、そうした思い入れも想起しつつ、ゾーンとコンジットについ述べてみたいと思います。

2. 一枚岩状のネットワークの危険性

イーサネットやインターネット・プロトコル （Internet Protocol；いわゆる TCP/IP の IP；以下では IP と記します。） 技術を採用することにより、ICS ネットワークでも、比較的廉価で広域にわたる高速の通信ができるようになりました。それ以前の ICS では、ICS のコンポーネントの提供ベンダーごとに、さらにはアプリケーションごとに、別々のネットワークを張りめぐらす必要がありました。インターネット・プロトコル技術の登場により、プラント内のすべての ICS や情報システムなどを一つのネットワークに収容することさえできるようになりました。

ほとんどの ICS 用の通信プロトコルは、IP が採用される以前には、他の通信が存在しない閉じたネットワーク環境を前提に作られてきました。攻撃を受ける可能性が小さく、セキュリティ対策も皆無に近かったのです。そうした ICS 用の通信プロトコルが、特段の対策もないままに IP プロトコル用に改修して利用されるようになったのです。そのために攻撃者に ICS 用の通信プロトコルについて若干の知識があり、アクセスするための開始点さえ得られれば攻撃が極めて容易な、攻撃者にとって天国のようなネットワーク環境になってしまいました。

ここで IP をベースとするネットワークの特性について少しだけ述べておきます。「IP には通信パケットの経路制御技術が組み込まれています。そのために元は 2 つのネットワークであっても相互接続しさえすれば、論理的に一つの縫い目の見えないネットワークとして動作するようになります。これが「ネット間を取り結ぶもの」という意味を込めて Inter-Net の名称が与えられた理由でもあります．さらに、IP レベルでは通信を行うノード

が完全に対等に作られています。そのため、すべてのノードを対象としたネットワーク管理には特別な工夫が必要です。

IP ベースのネットワークは、全体計画なしに逐次に増設されていった結果として、論理的に一枚岩になった巨大なネットワークにすべてのコンピューターが接続されて稼働しているという状況がしばしば見られます。このような一枚岩状のネットワークは、任意のコンピューター対で通信が可能であるなど、正常時には快適に利用できますが、一旦不具合が生じると、原因の解析や不具合の影響を局所化することが極めて難しいという問題を抱えています。さらに、マルウェアやサイバー攻撃者にとって、一旦入り込めれば内部を自在に動き回ることができる一枚岩状のネットワーク環境は攻撃活動のための格好の土俵と言えます。こうした一枚岩状のネットワークに付随する不都合を避けるために一般的な情報処理用ネットワークでは、サブネットあるいはセグメントと呼ばれる小さな複数のネットワークに分割するネットワークの設計（セグメント化；segmentation）が行われてきました。

こうした脆弱なネットワークのセキュリティ強度を高めるためにネットワークをゾーン（zone）と呼ばれる小さな領域に分割すること（ゾーン化）が考案され、IEC 62443 の重要なセキュリティ概念の一つとして採用されました。

3. ゾーンとは

IEC 62443 では、ゾーンを「リスクやその他の評価基準（重要性や運用上の機能、物理的または論理的な位置、アクセス要件、管理組織）に基づいた、論理的または物理的な資産のグループ分け」と一般的に定義した上で、セキュリティの観点に基づいて分けられたセキュリティ・ゾーンを単にゾーンと呼ぶことにしています。

斜面に開墾された棚田の風景
さまざまな高さに畦で区画された棚田はゾーンと似ています

ネットワーク側から見ると、ゾーン化とは、ネットワーク上に存在してシステムを構成しているコンピューターやコントローラー、データベースなどとともに、ネットワークを重なりのない小さなネットワーク（ゾーン）に分割することです 。各ゾーンは固有のセキュリティ・リスク水準を持ちます。ゾーン化されたネットワークは棚田になぞらえることができます。棚田では、畦で区画して、多数の水面の高さを維持するようにしつらえています。セキュリティのリスク水準の高低をイメージして、水面の高低を見ていただければと思います。

なお、非常に大規模なシステムの場合には、複数の抽象度を導入して、システムが階層的に構成される場合があります。そのような場合には、ある抽象度において一つのゾーンとされたものが、さらに詳細化されたレベルにおいて複数のサブゾーンに分割されることがあります。

どの程度の粒度でゾーンに分けるのか？ICS の各コンポーネントをどのゾーンに含めるのか？各ゾーンのセキュリティ水準をどのように設定するのか？こうした判断がゾーン化に際して必要です。粗すぎるゾーンでは一枚岩状のネットワークの弊害が残り、逆に、ゾーンを細かく分けすぎると各ゾーンのセキュリティ水準を維持するためのオーバーヘッド大きくなる一方で、それに見合った効果が小さくなっていくでしょう。従ってゾーン化はネットワークのセキュリティ設計の重要な要素と言えます。ゾーンのセキュリティ・リスク水準の高低をどのように設計し、どのようにゾーンに分割すべきかについてのガイダンスが欲しいところです。IEC 62443 ではゾーンが一定の特性およびセキュリティ要件を持つとされており、特に注目される特性や要件として、分冊

1-1 では、a） セキュリティ属性（セキュリティ・ポリシーとセキュリティ水準）、b） 資産棚卸、c） アクセス要件とアクセス制御、d） 脅威と脆弱性、e） セキュリティ侵害の影響、f） 技術の成熟是認、g） 変更管理手順、を掲げています。また、分冊 3-2 は、ゾーンとコンジットとリスク評価に対する要件を定義しています。これらの記述をヒントに、ゾーンを設計する手順について考察した概要を次に記しておきたいと思います。

ICS が万一正常に動作しなくなるとプラントの操業が止まったり重大な損害につながったりするようなコンポーネントは、相当のコストをかけてもサイバー攻撃から守りたい資産と言えます。そのコンポーネントが、レガシー製品でサポートが終了しているなどの事情から、脆弱性を持っていて除去が難しいような場合には、さらに手厚い保護が望まれます。こうした資産は高いセキュリティ水準を要求しているわけです。一方、物理的あるいはネットワーク的に多くの人々からアクセスされうる環境や十分な資産管理がなされていない環境に設置された資産はセキュリティ水準が低いと言わざるを得ません。その資産について脆弱性管理が徹底されていないような場合には、さらに低い水準になるでしょう。さまざまなセキュリティ水準の資産をゾーンに区分けし、その間にセキュリティ水準の差を維持するための仕組みを組み込むことによって、システム全体のセキュリティ的な均衡状態を構築することがゾーン化なのです。

適切なゾーン化のためには、ICS の各コンポーネントについて、サイバー攻撃で障害を起こした場合に企業が被る損害の大きさと、サイバー攻撃に対する耐性の両面でリスクを正しく評価できていなければなりません。特に ICS では、制御あるいは監視の対象となっている工場の設備や重要インフラ施設の耐用年数が、コンピューターの世代交代周期と比較して非常に長く、そのためにサポート期間を超過したソフトウェアなどを含むレガシー資産を稼働させているケースがあります。また、大型ロボットを含む機械設備などは内部に PLC などのコントローラーを組み込んでいる結果、上流の製品に脆弱性が公表されても、長いサプライチェーンを通じた脆弱性対応に時間を要する可能性、あるいは放置されている可能性さえあります。こうした資産には、いわば無菌室のようなゾーンを用意して収容する対策を検討することが望まれます。

こうした理解を踏まえて、実務的なゾーン設計は次のように進めることになるかと思います。
1) 主要な資産を中核として、それに物理的または論理的に近接した資産を合わせてゾーンを作る。
2) 中核となる資産についてセキュリティ水準を判断し、その水準をゾーンのセキュリティ水準とする。
3) 論理的または物理的に近接したゾーンが同程度のセキュリティ水準の場合には、一つのゾーンに統合する。

異なるゾーンの間におけるデータや制御の受け渡しが行われるポイントでは、低い側のセキュリティ水準が他方に及ばないような対策を組み込む必要があります。そうした検討を行うためには、ICS 内のコンポーネント間でどのようにデータや制御が交換されているのかを網羅的に掌握している必要があります。ICS では、ネットワーク通信のパターン（通信しあうコンポーネント対と通信の形式）が概ねシステム設計時に決まっているはずです。利用者の関心や時々の業務に応じて通信内容が大きく変動する一般のオフィス用ネットワークなどと異なり、ICS では、システムの設計時にネットワークのゾーン化を体系的に行うことができ、ゾーン化の効果も高いことから、IEC 62443 ではゾーンを基本概念の一つとして取り上げたと考えられます。

4. コンジットとは

IEC 62443 では、ゾーンとともにコンジット（conduit）という用語が定義されています。コンジットの定義は、いくらかの揺らぎを含んでいるように思われます。

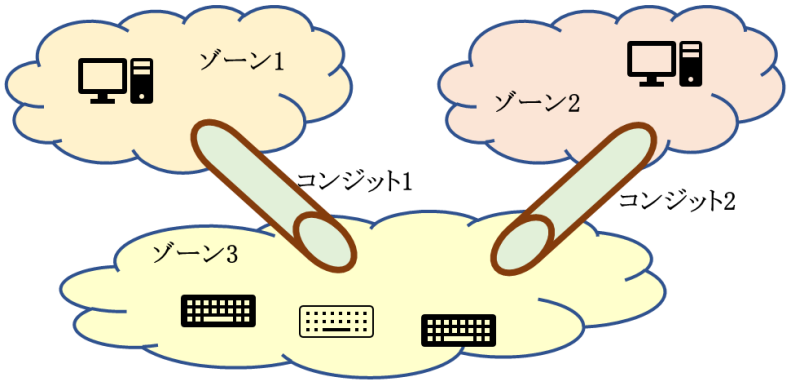


図 ゾーンとコンジット（模式図）

各分冊の用語定義の中では、右図のようにゾーン間を結ぶ通信チャンネル（あるいは複数のチャンネルのグループ）をコンジットとしています。なお、通信チャンネルは、恒久的に設定されているものだけではなく、保守や設定時など特定の時間だけ開かれるような時限的なものも含みます。この定義の下では、ゾーン間で通信が行われる場合には必ずコンジットを経由

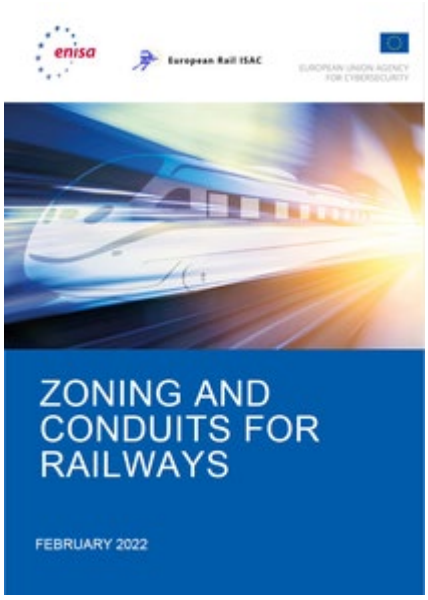
して行われるとも解されます。

一方で、ゾーンのうち他のゾーンとの通信を守るセキュリティ機能に特化したものをコンジットと呼んでいる記述もあります（分冊 1-1）。例えばファイアウォール機能や DMZ（非武装ゾーン）のような部分がこれに相当するものと考えられます。この定義の下では、ゾーン間の通信はコンジット経由で行われる場合も、単なる通信チャンネルを経由して行われる場合もあり得ることになります。

いずれにせよ、コンジットは単なる通信路ではなく、ゾーン間のセキュリティ水準の違いを維持するための「セキュリティ機能」に注目した概念であることが重要です。

5. ゾーン化とコンジットの設計例

ここまで抽象的概念的にゾーン化とコンジットについて述べてきましたが、もう少し具体的な設計例を見てみたいという読者のために、EU のサイバーセキュリティ機関 ENISA （European Union Agency for Cybersecurity）が 2022 年 2 月に公表した報告書「鉄道のためのゾーン化とコンジット」[1]について簡単に紹介しておきます。この報告書は、欧州の鉄道事業者からなるセキュリティ情報の共有分析センター（ER-ISAC： European Rail ISAC）と ENISA が共同で作成したもので、鉄道用システムにおけるゾーン化の手順を詳しく述べています。59 ページとやや大きな文書ですが、図を多用して分かりやすく書かれており、鉄道以外の ICS 関係者にも大いに参考になると思います。



鉄道システムのためのゾーン化とコンジットに関する ENISA の報告書

この報告書では、ゾーン化のための設計プロセスを 9 段階に分け、各段階の入力情報と作業内容と手順、成果物を明示的に説明しています。

第1段階： ゾーン化する資産とシステムを特定する.
第2段階： リスクの一次評価を行う.
第3段階： ゾーンとコンジットに分割する.
第4段階： 高いレベルのリスク評価を行う.
第5段階： 詳細なリスク評価を行う.
第6段階： サイバーセキュリティ要件を文書化する.
第7段階： 設計結果について承認を得る.
第8段階： ゾーン化した構成にシステムを移行する.
第9段階： ゾーン化されたシステムを運用する

また、ゾーン化設計の中核とも言うべき第 1～5 段階について、報告書ではさらに細かく段階に分けた手順を述べています。本稿では紹介を割愛しますが、ゾーン化設計をする際の参考文書として是非ともご一読ください。

6. まとめ

ゾーンとコンジットは、多層的に防護層を設置して重要資産を脅威から守るための「深層防御」をネットワーク構造の中に組み込むことを意図して導入された考え方です。セキュリティへの配慮なしに構築された ICS ネットワークは、ともすると一枚岩ネットワークになりがちです。一枚岩ネットワーク上に構築された ICS では、その一部が一旦侵害を受けると、時を置かずに侵害が重要資産にまで拡大し、大きな被害を生じる可能性が高まります。また、侵害を受けた後の復旧を進めるにあたっても、ゾーンを単位として進めることにより、体系的に見通し良くできるようになるはずです。

参考資料

[1] European Union Agency for Cybersecurity （ENISA）： Zoning and Conduits for Railways、2022 年 2 月 28 日
https://www.enisa.europa.eu/publications/zoning-and-conduits-for-railways/