DITTA サイバーセキュリティ白書:

医療技術製造環境におけるベストプラクティス

序文

本書の適用範囲に分類される生産およびエンジニアリングプロセスのサイバーセキュリティ管理は、医療技術組織全体にプラスの影響を与えることができます。

DITTA は、医療技術製造施設およびエンジニアリングプロセスにおけるサイバーセキュリティ要件の数は、世界的な規制上の要件が求める製品品質と共に増加するものと見ています。

サイバーセキュリティに関連した以下のような多くのリスクが製造施設で発生する恐れがあります。

- 製造施設の一時閉鎖と生産性の低下
- 製品検査の不履行による品質低下
- 顧客、設計、および生産技術情報の流出
- 生産過程における新製品の悪意のあるソフトウェアへの感染
- 製品ソフトウェア認証の流出

利害関係者が、安全な医療技術の開発プロセスについて話し合い、情報を医療サービス提供者と共有することは、建設的で理にかなったことです。しかし本書では主に、製造業者にとっての新たな重要課題として、製造施設とエンジニアリングプロセスの安全な環境について取り上げます。

本書では、製造施設ネットワークおよびエンジニアリングプロセスに特有のリスクを考慮し、「デバイス」という語を医療技術製品のみに限定せず、製造施設ネットワーク内のあらゆるデバイスを指して用います。

DITTA 医療技術サイバーセキュリティ白書は、NEMA CPSP 2-2018 サイバー衛生ベストプラクティスを基にしています。アメリカ電機工業会の許可により転載されています。

要旨

目的

本白書では、医療技術製造業者が自身の製造施設やエンジニアリングプロセスにおいてサイバーセキュリティのレベルを上げるために実施可能な業界ベストプラクティスおよびガイドライン一式を明らかにします。本書は、人、プロセス、およびシステムに焦点を合わせた事前対応型および事後対応型セキュリティのためのガイドラインを提供します。

本書は、以下の 7 つの基本原則に従って、製造業者のサイバーセキュリティのレベルを上げるための方法を取り上げます。

1. ネットワークのセグメント化
2. データタイプとデータフローの理解
3. デバイスの堅牢化
4. デバイスとシステムのモニタリング
5. ユーザー管理
6. デバイスの更新
7. 復旧プラン/エスカレーションプロセスの提供

本書は、包括的なものではなく、むしろ製造業者が自身の製造施設とエンジニアリングプロセスの両方で実施可能なベストプラクティスの代表例を示すことを目的としています。本書はまた、製造されたデバイスを実装する組織向けのセキュリティベストプラクティスを記載することを目的としたものではありません。最後に、本書が提供するガイドラインの一部は医療 IT サービス提供者に適用可能な場合があるとしても、それらの事業に特有のセキュリティニーズを明確に検討したものではありません。

本書の構成

各基本原則に対して、以下の情報を提供します。

a. 脅威の特定およびそれらの影響の解析
b. 付加的な参考文献
c. 医療技術製造業者が取り入れるべき提案

目次

序文 3

要旨 4

序論 6

本書の適用範囲 6

基本原則 6

定義 22

DITTA について: 24

序論

このサイバーセキュリティに関する文書では、医療技術製造業者が自身の製造施設やエンジニアリングプロセスにおいてサイバーセキュリティ知識のレベルを上げるための業界ベストプラクティスおよびガイドライン一式を明らかにします。本書は、人、プロセス、およびシステムに焦点を合わせた事前対応型および事後対応型セキュリティのためのガイドラインを提供します。

本書に明記された手法は、広範なセキュリティ管理の取り組みの一環として取り入れられるべきです。セキュリティ管理に関する追加の情報は、IEC 62443-4-1、ISO/IEC 27000 シリーズ、および NIST サイバーセキュリティフレームワークなどの標準や枠組から入手可能です。

本書の適用範囲

本ガイドラインは、以下の 7 つの基本原則に従って製造業者のサイバーセキュリティ知識のレベルを上げる方法を述べます。

1. ネットワークのセグメント化
2. データタイプとデータフローの理解
3. デバイスの堅牢化
4. デバイスとシステムのモニタリング
5. ユーザー管理
6. デバイスの更新
7. 復旧プランとエスカレーションプロセスの提供

基本原則

以下の各基本原則に対して、本書の各セクションには、脅威の特定、それらの関連性（適切で参考となる参照規格や適用できる可能性のある他の文献を含む）、影響を見極めるための解析、および DITTA 製造業者が取り入れるべき提案が記載されています。本書に記載されているベストプラクティスは、大半の製造環境に適用可能です。各基本原則は製造業者のサイバーセキュリティ活動に役立ち、1 つの原則だけが実施された場合でも効果的に機能します。

ネットワークのセグメント化

この原則は、製造システムのデータフローをビジネスネットワークや公共のネットワークから論理的あるいは物理的に分離するデータネットワークの設計に焦点を合わせています。この原則はまた、重要な製造サブネットワークを他の製造サブネットワークから分離し、それぞれに異なるセキュリティ要件を持たせる機能を提供します。ネットワークのセグメント化には、ネットワークをゾーンと呼ばれるより小さなネットワークに分けることが含まれます。

個々のデバイスをゾーンに区分することは、必ずしもそれらを孤立させることを意味するわけではありません。セキュリティゾーンはコンジットで接続され、コンジットはセグメント化されたセキュリティゾーン間の必要な通信の伝送を円滑化します。図 1 および 2 に、典型的なセグメント化された製造ネットワーク（OT（Operational Technology：制御運用技術）ネットワークと呼ばれる）、および典型的なセグメント化された複数施設による製造ネットワークを示します。

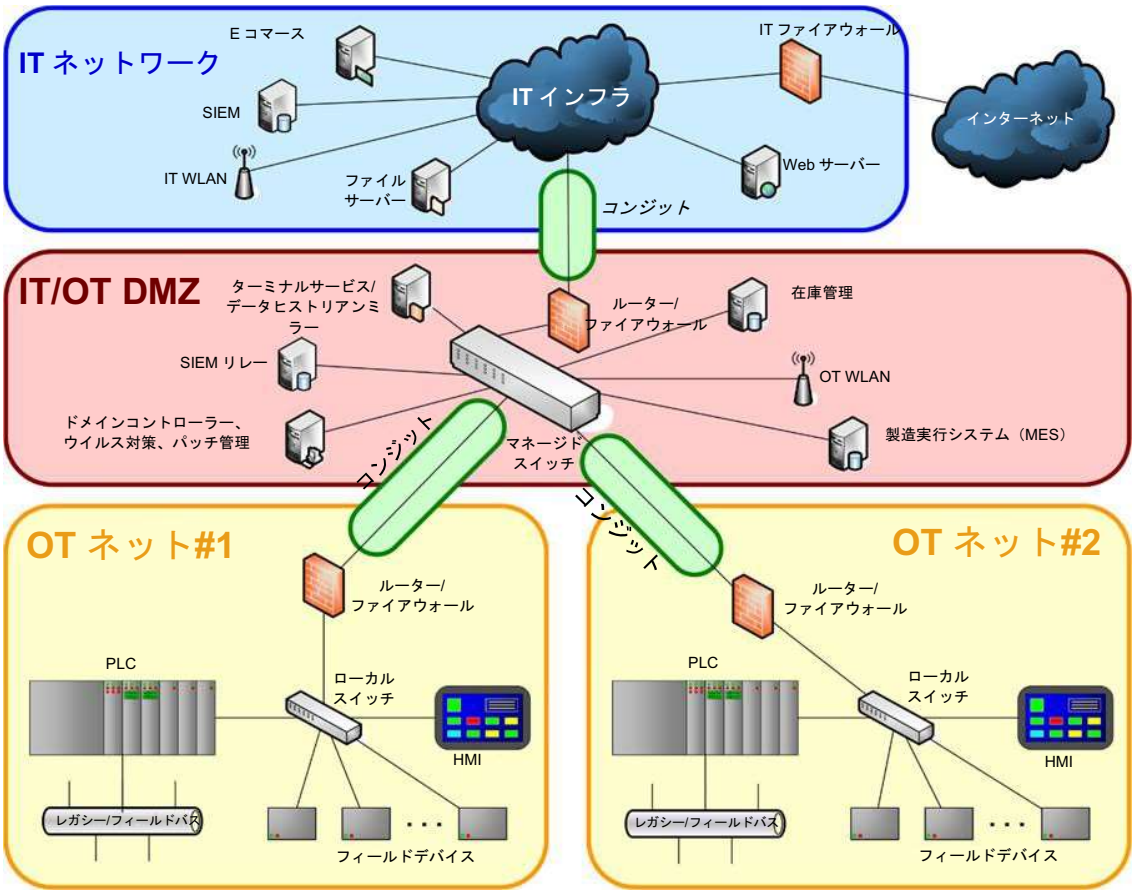

図 1.　　典型的なセグメント化された製造ネットワーク

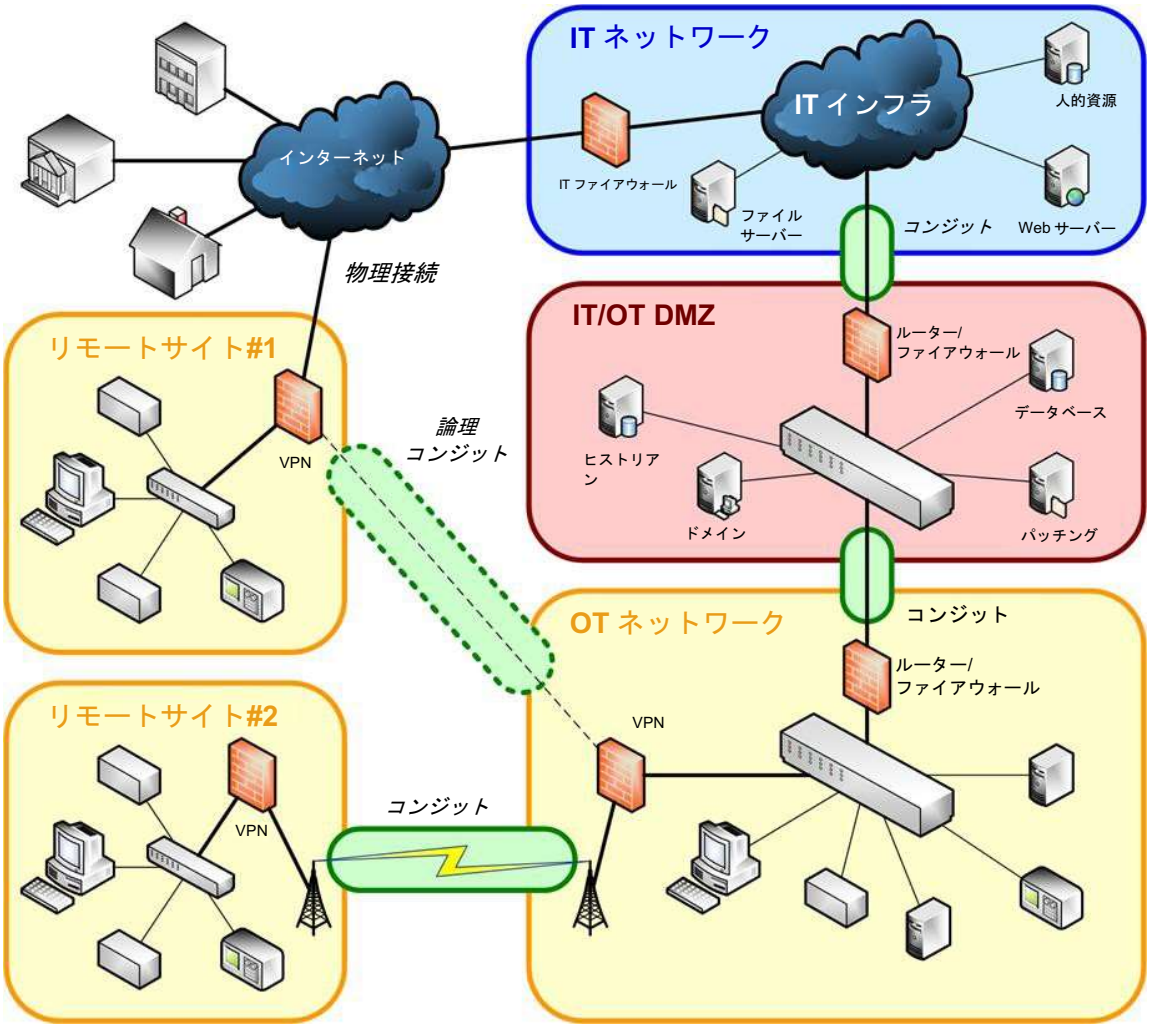

図 **2.** 典型的なセグメント化された複数施設による製造ネットワーク

脅威の特定およびそれらの影響の解析

包括的リスク評価を使用することで、製造業者は自社のデバイスへの脅威を特定し、解決策を見出すことができます。製造業者が利用可能な多くのリスク評価方法があります。ネットワークのセグメント化の目的の 1 つは、不必要なネットワークトラフィック、更には悪意のあるネットワークトラフィックがオペレーショナルテクノロジー（OT）ネットワークに進入するのを防ぐことです。この種のトラフィックは、OT トラフィックや OT デバイス機能の邪魔をしたり、場合によっては改変することがあります。そのため、有効で認証された OT ネットワークトラフィックのみが、OT ネットワークゾーンへの進入を許可されるべきです。

ネットワークのセグメント化のもう 1 つの目的は、極秘データがセキュリティゾーンの中から出て行くのを防ぐことです。最近注目を集めている攻撃の中には「実家への電話」とよばれる機能が含まれているものがあり、その攻撃には被害者のネットワークにあるデータを、コマンドやコントロールホストに

送信することができる引き出しエージェントが含まれていました。重ねて述べますが、有効で認証されたネットワークトラフィックのみが、セキュリティゾーンから出ることを許可されるべきです。

製造業者への提案

ネットワークは、通過するものをコントロールできるバリアデバイスを使用してセグメント化します。伝送制御プロトコル/インターネットプロトコル（TCP/IP）を実装しているイーサネットベースのネットワークにおいて最も一般的に使用されているバリアデバイスは、ファイアウォール、ルーター、データダイオード、およびレイヤ 3 スイッチです。

一般的に取り入れられている優良な手法は、OT ゾーンを情報技術（IT）ゾーンにリンクするコンジットを介して行われる通信を、バリアデバイスを使用して管理する方法です。バリアデバイスは、インターネットへのまたはインターネットから入ってくる電子メールや通信を許可しないなど、セキュリティ対策が OT ゾーンで実施される事を確実にする有効な自動化ツールとしての役割を果たすことができます。

高いリスクを伴う産業用制御システム（ICS）の場合、OT ゾーンと併せて非武装地帯（DMZ）を使用することで、セキュリティレベルの低い IT ゾーンとセキュリティレベルの高い OT ゾーンの間でリスクをさらに低下させる機会を得ることができます。DMZ のセキュリティレベルは IT ゾーンより高いですが、OT ゾーンよりは低くなります。このゾーンには、OT ソーンと IT ゾーンの間の直接的な通信をすべて排除する、または大幅に少なくするという機能があります。製造業者が、無線 LAN（WLAN）による OT ネットワークへのアクセスを必要とする場合、OT WLAN ネットワークには個別の SSID を付与することを推奨します。その WLAN から接続できるのは、可能な限り小さな OT ゾーンのみに限定されるべきです。

セグメント化でさらに考慮するべきなのは、リモートアクセスのセグメント化です。OT ゾーンへのリモートアクセスは、必要性があり認証された場合にのみ有効にされるべきです。OT ゾーンへのリモートユーザーアクセスには、セキュリティレベルの要件に応じて、多元的な認証が必要になる場合があります。

ICS に関連したリスクが大きく、外部エージェントによる悪影響を排除できない可能性がある。施設によっては、OT ゾーンと他のすべてのゾーンの間にあるすべてのコンジットを切断することを選択するかもしれません。これは考慮すべき非常に有効な、ネットワークセグメント化戦略です。この分離型アプローチを施設に取り入れても、すべてのリスクを自動的に排除できるわけではありません。依然として、ローカルで悪用される可能性のある多くの脆弱性があります。OT ゾーンを IT ゾーンから分離した後に残るリスクに対応するために、サイバー保護および物理的防護のための適切なレイヤを取り入れるべきです。

ネットワークのセグメント化 参考文献

a. IEC 62443-2-1:2010 産業用通信ネットワーク — ネットワーク及びシステムセキュリティ —第 2-1 部: 産業用オートメーション及び制御システムセキュリティプログラムの確立
    1. A.3.3.4 ネットワークのセグメント化
b. IEC 62443-3-3:2013 産業用通信ネットワーク — ネットワーク及びシステムセキュリティ — 第 3-3 部: システムセキュリティ要件及びセキュリティレベル
    1. SR 5.1 ネットワークのセグメント化

c. NIST SP 800-53 Rev 5（原案）情報システムと組織のためのセキュリティとプライバシーの管理（2017 年 8 月）

    1. AC-4 情報フローの実施
    2. SC-7 境界の保護

d. NIST SP 800-82 Rev 2 産業用制御システム（ICS）セキュリティガイド（2015 年 5 月）

e. ISO/IEC 27001: 2013 情報技術 — セキュリティ技術 — 情報セキュリティマネジメントシステム — 要件

    1. A.13.1.3 ネットワークにおけるセグメント化

[参考文献に関する注釈]

- IEC 62443 シリーズ

IEC 62443 シリーズは、産業自動化制御システム（IACS）セキュリティ向けの標準ではありますが、医療技術の分野で多くの注目を集めています。これらの標準が医療技術に適用されている理由の 1 つは、セキュリティに関しては IACS が最も先進的で確立された分野の 1 つだからです。本書の適用範囲は製造施設とエンジニアリングプロセスにあるため、本書においては、それらの要件や技術を一切言い換えることなく直接適用することができます。

- NIST SP 標準

アメリカ国立標準技術研究所（NIST）は米国商務省の傘下にある組織であるにも関わらず、その標準化活動は広範囲に及ぶ包括的なもので、グローバルな観点から参照するに値します。NIST は、国際的なサイバーセキュリティ構想や規格と協調するよう継続的な努力を払っています。例えば、NIST は多くの国々や地域と定期的な討議を行っており、国際化において注目に値する進展を遂げました。NIST SP 800-53 は、セキュリティ制御とプライバシー制御のカタログを提供します。そのカタログは、2019 年 3 月に発行される予定です。NIST SP 800-82 は、ICS の概要と典型的なシステムトポロジーを提供し、それらのシステムに対する典型的な脅威と脆弱性を明らかにし、関連するリスクを軽減するための推奨セキュリティ対策を提供します。以下のリンクを参照してください。

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft
https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

- ISO/IEC 27001

これは、情報セキュリティマネジメントシステム（ISMS）規格と見なされる ISO/IEC 27000 ファミリー規格の 1 つで、医療技術分野で広く認められています。この規格を適用するのは適切なことです。なぜなら、この国際規格に定められている要件は包括的なものであり、種別や、規模、性質に関わらず、すべての組織に適用できるように意図されているからです。またこの規格は、IEC 62443-2-1 および NIST SP 800-82 によって参照されています。

データタイプとデータフローの理解

この原則は、ネットワークに接続されたデバイスが展開されている製造環境の理解に焦点を合わせています。製造業者とエンドユーザーにとって、どんなデータがネットワーク内を流れているべきなのか、そのデータは通常はどこへ行くのか、そして誰または何がそのデータにアクセスできるのかを知るのは重要なことです。

脅威の特定およびそれらの影響の解析

包括的リスク評価を使用することで、製造業者は自社のデバイスへの脅威を特定し、解決策を見出すことができます。製造業者が利用可能な多くのリスク評価方法があります。モノのインターネット（IoT）、ICS、また、監視制御およびデータ収集システム（SCADA）ネットワーク内では、それらの機器が送受信するデータの量や種類は比較的静的です。通常の典型的なデータフローパターンを越えた新たな通信経路の出現は悪意ある活動を表している場合があり、それによって個別のネットワークが危険にさらされたり停止したりする恐れがあります。

製造業者への提案

ネットワークに新たな通信経路が出現したり、既存の通信経路に変更が加えられたりした場合、何かがおかしい可能性があることを示すアラームを発するべきです。それらのアラームは、製造業者のモニタリングデバイスやシステムにフィードされます。

データタイプとデータフローの理解 参考文献

NIST SP 800-53、Rev 5（原案）: 情報システムと組織のためのセキュリティとプライバシーの管理（2017 年 8 月）

AC-4 情報フローの実施

CA-9 内部システム接続

NIST SP 800-82 Rev 2 産業用制御システム（ICS）セキュリティガイド（2015 年 5 月）

NEMA/MITA CSP 1-2016 医用画像サイバーセキュリティ

DITTA 医用画像機器サイバーセキュリティ白書（2016 年 11 月）

ISO/IEC 27001: 2013 情報技術 — セキュリティ技術 — 情報セキュリティマネジメントシステム — 要件

A.13.2.1 情報転送の方針と手順

[参考文献に関する注釈]

DITTA 医療技術サイバーセキュリティ白書

この DITTA 白書には、製造業者や納入業者向けの現在のベストプラクティスの原則が示されています。

サイバーセキュリティは単一の利害関係者だけの役割ではないため、この白書ではその責任について記述しています。製造業者や病院の IT 部門は、それらのアプローチを実施するために協力する必要があります。以下のリンクを参照してください。

https://www.globalditta.org/media-centre/press-releases/article/new-report-from-ditta-underlines-its-commitment-to-cybersecurity.html

デバイスの堅牢化

この原則では、製品の設計や生産に使用するデバイスを堅牢化させる（より安全にする）ために製造業者が使うべき技法について述べます。ベストプラクティスは、製造業者の業種によって異なる場合があります。

製造業者への提案

製品の設計や生産に使用するデバイスを堅牢化させるために製造業者が利用できる技法は多数あります。製造業者は、不必要または特有のセキュリティリスクが存在し得るデバイスのいくつかの機能をオフにするか無効にすることを検討すべきです。例として、ジョイントテストアクショングループ（JTAG）、Telnet、SNMP Ver. 1、2、および無線通信が挙げられます。

製造業者は、ゲームや Java 等のブラウザーのプラグインといった不必要なプログラムの削除を検討してもよいでしょう。製造業者はさらに、印刷スプーラーやリモートデスクトップなどの不必要なサービスの削除も検討してもよいでしょう。さらに、製造業者はクッキーを無効にすることも検討してもよいでしょう。

イーサネットやユニバーサルシリアルバス（USB）のポートブロッカーは、製造されたデバイスに出入りするネットワークトラフィックをブロックするのに効果的な場合があります。

エラー処理や入力検証機能についても検討すべきです。例として、入力のサニタイズ、静的コードテスト、およびソフトウェア部品表（SBOM）解析が挙げられます。

部品やサプライチェーンの安全に関しては、製造業者は、納入業者をモニタリングしたり、製造された製品に含まれている部品のバージョンを容易に特定したりできるプロセスを作成しておくべきです。加えて、製造業者は、各部品やそれらの部品の新たに公開されたバージョンを製品に実装する前に、それらの徹底的な評価を可能にする適切なテストプランを作成しておくべきです。それらの評価には、標準部品品質チェックに加えて、マルウェア検出解析が含まれているべきです。NEMA が発行する白書であるサプライチェーンベストプラクティスは、サプライチェーンの安全に関して付加的な詳細を提供しており、本セクションの最後のリストに参考文献として掲載されています。

情報が機密で慎重に扱われるべきものであれば、データ暗号化を使用するべきです。製造業者は、デバイス内に保存されているデータを暗号化する必要があるか、伝送中のデータを暗号化する必要があるか、あるいはそれらを組み合わせて行う必要があるかを考慮する必要があります。この決定は関係するデー

タによって異なります。そしてデータが、保護されるべき医療情報（PHI）などの特に慎重に扱われるべきものであれば、保存時および伝送時に暗号化を実施するべきです。情報転送が確実でエラーのないものでなければならない場合、完全な保護を使用するべきです。

DDOS（分散型サービス妨害）攻撃は頻繁に発生します。一部の防御では主として、攻撃検知、トラフィック分類、そしてレスポンスツールの組み合わせが使用されています。これら目的は、違法であると特定されたトラフィックをブロックし、合法であると特定されたトラフィックを許可することです。大抵のファイアウォールやルーターには外部の攻撃者から送られてくるトラフィックを拒否する機能がありますが、それらは攻撃がより巧妙になると簡単に突破されてしまいます。他の利用可能な選択肢には、侵入防止システムや、アプリケーションフロントエンドハードウェアを使用してデータパケットがシステムに入ってくる際にそれらを解析し、優先、普通、または悪質に分類することが含まれます。

最後に、製造業者は、自身が使用するすべての製品に対してセキュリティベースラインを作成する *デフォルトでのセキュリティ強化*方式を検討してもよいでしょう。この方式では、最も安全になるように構成が設定されます。欠点は、それらの設定は後方互換性があまりない場合があり、より複雑な初期構成が必要となるため、製品があまりユーザーフレンドリーではなくなるということです。

デバイスの堅牢化 参考文献

NEMA CPSP 1-2015 サプライチェーンベストプラクティス

NEMA/MITA CSP 1-2016 医用画像サイバーセキュリティ

IEC 62443-3-3:2013 産業用通信ネットワーク — ネットワーク及びシステムセキュリティ — 第 3-3 部: システムセキュリティ要件及びセキュリティレベル

SR 3.5 入力の検証

SR 3.6 決定性出力

SR 3.7 エラー処理

NIST SP 800-53 Rev 5（原案）情報システムと組織のためのセキュリティとプライバシーの管理（2017 年 8 月）

SC-27 プラットフォームに依存しないアプリケーション

SC-41 ポートおよび I/O デバイスへのアクセス

NIST SP 800-82 Rev 2 産業用制御システム（ICS）セキュリティガイド（2015 年 5 月）

DITTA 医用画像機器サイバーセキュリティ白書（2016 年 11 月

デバイスとシステムのモニタリング

この原則では、製造業者が自身の環境内のデバイスやシステムの健全性やセキュリティをモニタリングする機能を提供する方法について述べます。モニタリング機能は、特定の処理パラメータに影響を及ぼさない、既存のよく知られた標準ソフトウェアメカニズム（つまり、簡易 ネットワーク管理 プロトコル [SNMP]、Syslog）を通して提供されるべきです。

脅威の特定およびそれらの影響の解析

包括的リスク評価を使用することで、製造業者は自社のデバイスへの脅威を特定し、解決策を見出すことができます。効果的なモニタリングシステムは、対応するデバイスやシステムに組み込まれたセキュリティを強化することに役立ちます。

製造業者への提案

製造業者は、パフォーマンス、ネットワーク統計、コア機能、およびセキュリティ機能の集中モニタリングができるように設計されたデバイスを所有するべきです。

SNMP は管理データを、管理情報ベース（MIB）に編成された管理対象システム上で変数の形で明らかにし、システムのステータスと構成を表示するため、幅広く使用されています。それらの変数は、管理する側のアプリケーションからリモートで照会することができます（操作できる場合もあります）。SNMP には主要な 3 つのバージョンが開発されていますが、バージョン 3 ではパフォーマンス、柔軟性、およびセキュリティにおいて改善が施されています。従って、バージョン 3 を使用またはサポートするべきです。一般に、SNMP をサポートするデバイスには、ケーブルモデム、ルーター、スイッチ、サーバー、ワークステーション、およびプリンターが含まれます。

Syslog は、メッセージロギングの規格です。これにより、メッセージを生成するソフトウェア、それらのメッセージを格納するシステム、そしてそれらのメッセージについて報告し解析するソフトウェアを分割することができます。プリンターやルーターなどの幅広い種類のデバイスが、Syslog 規格を使用しています。これを、システム管理やセキュリティ監査だけでなく、一般的な情報、解析、およびデバッギングにも使用できます。Syslog 内には利用可能なオプションもあり、製造業者の環境がサポートできる場合は TCP およびトランスポート層セキュリティ（TLS）を使用して、セキュリティイベントを確実かつ安全に伝達させることができます。

Windows、Linux、および他のオペレーティングシステムでは、イベントログをコンピュータアラートや通知の記録として使用することができます。Microsoft はイベントを「ユーザーに通知する必要のある、またはログに記録を追加する必要のある、システムまたはプログラムにおけるすべての重大な出来事」と定義しています。

セキュリティ情報およびイベント管理（SIEM）ソリューションを実施する製造業者は、SIEM を使ってサーバー、ルーター、スイッチなどのデバイスから情報を収集したり、侵入検知システム/侵入防止システム（IDS/IPS）機器やファイアウォールを使って、その業者のネットワーク全体からセキュリティに関する全体像を収集することができます。SIEM には大抵、イベント解析機能が含まれており、その機能は、製造業者のネットワーク内の複数のソースからの情報を相互に関連づけ、それらをより状況把握しやすい表示書式で製造業者の IT/OT ネットワークセキュリティエンジニアリング担当者に提示して、アクティブなセキュリティイベントを特定することができます。

デバイスとシステムのモニタリング 参考文献

IEC 62443-3-3:2013 産業用通信ネットワーク — ネットワーク及びシステムセキュリティ — 第 3-3 部: システムセキュリティ要件及びセキュリティレベル

FR 6 イベントへのタイムリーな対応

NIST SP 800-53 Rev 5（原案）情報システムと組織のためのセキュリティとプライバシーの管理（2017 年 8 月）

AU-2 監査イベント

AU-3 監査記録の内容

AU-7 監査量の低減と報告書作成 AU-8 タイムスタンプ

CA-7 継続的モニタリング

SI-4 システムのモニタリング

NIST SP 800-82 Rev 2 産業用制御システム（ICS）セキュリティガイド（2015 年 5 月）

IETF RFC 5424: Syslog プロトコル

ユーザー管理

基本的なサイバーセキュリティの実施は、組織内のエンドユーザー、特に開発や製造環境にいるエンドユーザーの適切なトレーニングから始まります。最も技術的に高性能なサイバー防御システムであっても、スタッフに自分のパスワードを付箋紙に書いてモニターに貼り付けることを止めることはできません。トレーニング以外に、他のエンドユーザー管理機能も、コンピュータネットワークへのアクセスを制御し、更なるセキュリティを提供するのに役立ちます。

エンドユーザートレーニング – 既存のエンドユーザーに義務づけられる再教育コースに加えて、すべての新規エンドユーザーにセキュリティトレーニングを受けることを義務づけるべきです。容易に習得できる基本的なセキュリティ原則があり、必須のトレーニングはベストプラクティスを強化するの役立ちます。

管理 — 製造業者は、システムのアカウントを作成、変更、および削除する機能を有しているべきです。アカウントは、集中管理またはローカル管理できます。

認証 — 製造業者はエンドユーザーの身元を確認するプロセスを有しているべきです。許容可能なリスクの程度に基づいて、この認証は多元的であるべきです。

権限付与 — 製造業者は、エンドユーザーの権限を管理する機能を提供するべきです。例えば、役割に基づいたのアクセス制御です。

監査 — 製造業者は、エンドユーザーやプロセスによって実行されたアクションや消費されたリソースをモニタリングし、そのデータを監査ログに保存する方法を有しているべきです。監査ログは定期的に精査するべきであり、関係するアクセス権に応じて、精査する頻度を変更することもできます。

脅威の特定およびそれらの影響の解析

包括的リスク評価を使用することで、製造業者は自社のデバイスへの脅威を特定し、解決策を見出すことができます。製造業者が利用可能な多くのリスク評価方法があります。例えば、アメリカ国立標準技術研究所（NIST）は、以下に言及するサイバーセキュリティフレームワークを提供しています。リスク評価は、実施するのに複雑なものである必要はありません。しっかりしたパスワード方針の欠如が、特定される最も一般的な脅威の 1 つかもしれません。例えば、最初に使用する際に必ず行うべきデフォルトパスワード変更を、製造業者が有効にしていない場合があります。デフォルトパスワードは製造業者やエンドユーザーにとって、箱から取り出したばかりのデバイスを素早く構成するのにとても便利な一方で、エンドユーザーがデフォルトパスワードを変更しない、製造業者がデフォルトパスワードを容易に変更するメカニズムを提供しない、あるいはハードコードされたパスワードがデバイスに含まれている場合、問題が発生します。

最近の事例が示すように、壊滅的ダメージを与える分散型サービス妨害（DDoS）攻撃を実行できる大規模なボットネットを作り上げるために、モノのインターネット（IoT）デバイスが使用されています。Mirai ボットネットは、デフォルトパスワードまたは簡単に破られるパスワード使って 300,000 を超える IoT デバイスに影響を与え、被害に遭ったすべてのサイトにほぼ 600 Mbps の破裂的なインターネットトラフィックを生成しました。

製造業者への提案

エンドユーザーのトレーニング

すべての新規エンドユーザーにセキュリティトレーニングを修了することを義務づけ、無事修了したことをエンドユーザーの人事ファイルに記録します。

すべての既存エンドユーザーに定期的なセキュリティ再教育トレーニングを修了することを義務づけ（大抵の場合、年１回）、無事修了したことをエンドユーザーの人事ファイルに記録します。

管理:

システム内の任意のユーザーおよび対応する認証情報を追加、変更、および削除する機能。

認証:

最初のログインでデフォルトパスワードを変更するという要件。

固定/ハードコードされた認証情報（ユーザー名やパスワードなど、自分で変更することのできない認証情報）をデバイスに設定しない。

アカウント情報の保存

アカウントをローカルに保存する機能。

中央に保存されたアカウントシステムにアクセスする機能。例えば、アクティブディレクトリやライトウェイトディレクトリアクセスプロトコル（LDAP）など。

多元的認証を使用する機能。

公開鍵基盤の使用。特にリモートログインの場合。

権限付与:

役割に基づいたアクセスの実施。

事前定義の役割。

ユーザー定義の役割を作成する機能。

役割に基づいたアカウント管理の実施。

一般ユーザーと管理的ユーザーで、それぞれ異なる役割を付与。

役割に任意の権限を割り当てる機能。

任意のユーザーアカウントを任意の役割に割り当てる機能。

監査:

ユーザーログイン/ログアウトをタイムスタンプと共に記録する機能。

ログイン中にアクセスしたファイルや実行したアプリケーションを記録する機能。

ユーザーが作成したタスクをモニタリングする機能。アクティブなログインセッションを必要としないスケジュールされたタスクも含みます。

失敗したログイン試行をタイムスタンプと共に記録する機能。

システム構成の変更を記録する機能。

ユーザー管理 参考文献

IEC 62443-2-1:2010 産業用通信ネットワーク — ネットワーク及びシステムセキュリティ —第 2-1 部: 産業用オートメーション及び制御システムセキュリティプログラムの確立

A.3.3.5 – 要素: アクセス制御: アカウント管理

A.3.3.6 – 要素: アクセス制御: 認証

A.3.3.7 – 要素: アクセス制御: 権限付与

IEC 62443-3-3:2013 産業用通信ネットワーク — ネットワーク及びシステムセキュリティ — 第 3-3 部: システムセキュリティ要件及びセキュリティレベル

必須機能のサポート

FR 1 本人確認と認証の制御

FR 2 使用制御

NIST SP 800-53 Rev 5（原案）情報システムと組織のためのセキュリティとプライバシーの管理

AC アクセス制御ファミリー

AU-14 セッション監査

IA 本人確認および認証ファミリー

NIST SP 800-82 Rev 2 産業用制御システム（ICS）セキュリティガイド（2015 年 5 月）

NIST サイバーセキュリティフレームワーク V1.1

KrebsOnSecurity が記録的な DDoS 攻撃を受ける、https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with- record-ddos

国際標準化機構（ISO）27002:2013、*情報技術 -- セキュリティ技術 -- 情報セキュリティマネジメントの実践のための規範*

現場デバイスのモニタリングと更新

このセクションでは、最新の影響の大きな脆弱性をモニタリングし、現場デバイスを更新してそれらの脆弱性を緩和するために製造業者が取り入れるべき手順について取り上げます。

脅威の特定およびそれらの影響の解析

脅威の特定は、NIST サイバーセキュリティフレームワーク V1.1 の最初のカテゴリーで、製造業者はそれを進行中のプロセスと見なすべきです。脅威状況は絶えず変化しており、新たな脅威が連続的に登場しています。製造業者は、この脅威活動をモニタリングして、自身の組織への潜在的なリスクを解析するプロセスを作成しておくべきです。この解析を行うためのさまざまなツールが利用可能で、その最終目標は、他の組織機能と共有できるレポートを作成して、対策を講じることができるようにすることです。モニタリングを通して得られた知識を活用するための次の重要なステップは、可能な範囲でデバイスやシステムを更新することです。残念なことに、さまざまな理由でこの段階を踏むのが遅れる場合がよくあります。例えば、製造業者でのリソース不足、また機器やソフトウェアの提供者からの更新の欠如などです。加えて、パッチ配信に固有の性質から、ユーザーが自分で無効なパッチや更新をインストールしてしまうというリスクもあります。

製造業者への提案

パッチは、プログラムを更新する方法として、また特にオンライン環境でたびたび発生する新たなシステムセキュリティ脅威を更新する方法として、その重要性がますます高まっています。一般的にソフトウェアおよびハードウェアの提供者は、展開された自社の製品やシステム向けに何らかの形のパッチングシステムを提供しています。大抵の場合、そのパッチングシステムは自動化されていません。なぜならそれらの提供者には、パッチの信頼性を検証し、パッチをテストし、システムの再起動が必要な場合はガイダンスを提供し、パッチを有効にするのに適切な時間帯をエンドユーザーに通知する際に従ういくつかの推奨された手順があるためです。

時には、ソフトウェアおよびハードウェアの提供者は、パッチが利用可能になり、十分にテストされ、有効化されるまで、制限を緩和するよう推奨する場合があります（補償対策としても知られています）。例えば、脆弱なサービスを無効にしたり、ポートを無効にしたりすることがあります（これは、境界またはデバイスレベルで行うことができます）。

一部の環境に対しては、ソフトウェアおよびハードウェアの提供者は、推奨されるウイルス対策ソフトウェアパッケージを提供したり、ホワイトリストアクセス制御法を実施したりして、セキュリティ脅威を緩和するかもしれません。

現場デバイスのモニタリングと更新 参考文献

NEMA CPSP 1-2015 サプライチェーンベストプラクティス

NEMA/MITA CSP 1-2016 医用画像サイバーセキュリティ

NIST サイバーセキュリティフレームワーク V1.1

IEC 62443-2-1:2010 産業用通信ネットワーク — ネットワーク及びシステムセキュリティ —第 2-1 部: 産業用オートメーション及び制御システムセキュリティプログラムの確立

A.3.4.2.5.1 IACS デバイスのパッチング

A.3.4.3 要素: システム開発とメンテナンス

IEC TR 62443-2-3:2015 産業自動化制御システムセキュリティ —第 2-3 部: IACS 環境におけるパッチ管理

DITTA 医用画像機器サイバーセキュリティ白書（2016 年 11 月)ISO/TR 11633-1:2009 医療情報学 – 医療デバイスおよび医療情報システムのリモートメンテナンス用情報セキュリティ管理

復旧プランとエスカレーションプロセスの提供

この原則は、製品の設計や製造に使用されるデバイスに脆弱性が見つかった際に製造業者が使用すべき復旧プラン/エスカレーションプロセスの提供に焦点を合わせています。この原則ではさらに、デバイスに対するアクティブな攻撃の可能性についても取り上げます。製造業者にとって、脆弱性が発見された前の時点の状態に復旧させることは非常に重要です。そうしなければ、復旧しても製造業者はその脆弱性をすべて再び経験することになります。例えば、埋め込まれた部品により違反が発生した場合、影響を受けたデバイスを復旧させる前に、製造業者はその埋め込まれた部品を安全なバージョンにアップグレードしてその脆弱性を除去するプランを有しているべきです。

脅威の特定およびそれらの影響の解析

IT 環境において障害復旧（DR）プランを作成しておくのは一般的なことであるように、製造業者はサイバーセキュリティ問題に対するインシデント対応プランを作成しておく必要があります。復旧プランやエスカレーションプロセスがない場合、事業活動、情報セキュリティ、IT システム、従業員、顧客、上流納入業者、および他の不可欠な機能がたちまち混乱する恐れがあります。プランを作成しておくことで、製造業者は事前にチームの役割や責任を定義しておくことができ、効率な対応の手順を定めておくことができます。NIST サイバーセキュリティフレームワーク V1.1 の保護セクションでは、このプランについて詳述しています。

製造業者への提案

製造業者は、インシデントや脆弱性を管理するプロセスを作成するべきです。理想的には、そのプロセスに、インシデントの検出と記録、分類と初期サポート、調査と診断、解決と復旧、インシデントの終結、インシデント解決の進捗モニタリング、および影響を受けた当事者に解決状況について連絡するための伝達プランが含まれているべきです。この協調的な脆弱性の公開（CVD）プロセスは、発見された脆弱性が適切に緩和され、当該の利害関係者に情報が伝えられることを徹底するのに役立ちます。詳細

については、NIST サイバーセキュリティフレームワーク V1.1 を参照してください。

製造業者はさらに、すべての脆弱性に関する問題やその問題を緩和するための段階について常に把握しておくため、エンドユーザーや上流納入業者との通信経路を維持するべきです。また、継続的なデータフィードを提供する多数のソースも存在し、申し込むだけで最新の更新を電子メールやテキストメッセージで受信することができます。簡単なインターネット検索で、利用可能なさまざまなソースを見つけることができます。

最近、一部のソフトウェアおよびハードウェア製造業者は「バグバウンティ」と呼ばれるものを使用して、セキュリティ調査員が脆弱性を特定し、その情報を製造業者に提供できるようにしています。製造業者は「バグバウンティ」プログラムの実装に着手する前に、脆弱性の発見そのものに対する反応の仕方、セキュリティ調査員に対する反応の仕方、および自身の顧客に情報を知らせる方法について注意深く考慮するべきです。会社はまず、信頼できる開示メカニズムを通してセキュリティ調査員がバグについて報告できるコンピュータセキュリティインシデント対応チーム（CSIRT）を社内に設置することを検討したいと思うかもしれません。これにより会社は、セキュリティ調査員に脆弱性の発見に対する報酬を支払うことを検討する前に、それらの脆弱性を緩和する方法を確実に見つけることができます。

復旧プラン/エスカレーションプロセスの提供 参考文献

NEMA CPSP 1-2015 サプライチェーンベストプラクティス

IEC 62443-2-1:2010 産業用通信ネットワーク — ネットワーク及びシステムセキュリティ —第 2-1 部: 産業用オートメーション及び制御システムセキュリティプログラムの確立

A.3.4.5 要素: インシデントプランニングと対応

NIST SP 800-53 Rev 5（原案）情報システムと組織のためのセキュリティとプライバシーの管理（2017 年 8 月）

IR インシデント対応ファミリー

NIST SP 800-82 Rev 2 産業用制御システム（ICS）セキュリティガイド（2015 年 5 月）

ISO/IEC 29147:2014: 情報技術 — セキュリティ技術 — 脆弱性の開示

ISO/IEC 30111:2013: 情報技術 — セキュリティ技術 — 脆弱性情報取扱手順

NIST サイバーセキュリティフレームワーク V1.1

定義

アクティブディレクトリ: Microsoft の商標が付されたディレクトリサービス。集中型の標準化されたシステムで、ユーザーデータ、セキュリティ、および分散リソースのネットワーク管理を自動化し、他のディレクトリとの相互運用を可能にします。

部品表（**BOM**）: 原材料、小組立部品、中間組立部品、従属部品、と部品のリスト、および最終製品を製造するのに必要なそれぞれの数量のリストです。

ボットネット: インターネットで接続された一群のデバイス。各デバイスは自動化タスクを使ってインターネット上で 1 つまたは複数のソフトウェアアプリケーションを実行しています。

コンピュータセキュリティインシデント対応チーム（**CSIRT**）: 現実の組織的なエンティティ。コンピュータセキュリティイベントやインシデントへの対応の調整やサポートの責任を割り当てられています。CSIRT の目的は、インシデントによって受ける損害を最小限に抑えて制御し、対応や復旧活動に対して効果的なガイダンスを提供し、今後のインシデントの発生を防ぐよう勤めることです。

クッキー: コンピュータに保存される小さなファイルで、過去のブラウズ情報を収容しています。

サイバーセキュリティ: 使用するすべてのデータやソフトウェアの機密性、保全性、および可用性が保護されている状態です。

非武装地帯（**DMZ**）: 物理的または論理的なサブネットワーク。組織の外部向けのサービスを収容し、それを信頼できないネットワーク（通常はインターネットなどのより大きなネットワーク）に公開します。

分散型サービス妨害（**DDoS**）: 複数のソースからのトラフィックで圧倒することによって、オンラインサービスを利用できなくする攻撃です。

堅牢化: 脆弱な面を減らすことでシステムを安全にするプロセスです。

産業用制御システム（**ICS**）: 一般的な用語で、産業用プロセス制御に使用されるいくつかのタイプの制御システムと関連装置を包含しています。

国際電気標準会議（**IEC**）: 国際標準化機構であり、すべての電気技術、電子技術、および関連技術に対して国際標準を作成し、発行します。

インターネットエンジニアリングタスクフォース（**IETF**）: 任意のインターネット標準、特にインターネットプロトコル群を構成する標準を開発し、促進する団体です。

情報技術（**IT**）: データの処理や配信に使用するコンピュータシステム、ソフトウェア、およびネットワークの開発、メンテナンス、使用に関係する技術です。

モノのインターネット（**IoT**）: インターネットに接続された物理オブジェクトで構成される拡大し続けるネットワーク、およびそれらのオブジェクトや他のインターネット接続が可能なデバイスやシステムの間で発生する通信です。

侵入検知システム/侵入防止システム（**IDS/IPS**）: ネットワーク内の予期しない、または悪意のある活動を特定するために使用する技術手段です。一般に、IDS はセキュリティ管理アプリケーション（SIEM な

ど）に潜在的な侵入について通知し、IPS は検出した侵入を自動的にブロックします。

Joint Test Action Group（**JTAG**）**:** IEEE 1149.1 標準テストアクセスポートおよびバウンダリスキャンアーキテクチャの一般名です。これは、プリント基板上の相互接続や集積回路のサブブロックをテストするための手法です。

ライトウェイトディレクトリアクセスプロトコル（**LDAP**）**:** アクティブディレクトリなどのディレクトリサービスプロバイダに保存されているアイテムを照会したり、変更したりするためのアプリケーションプロトコルです。

管理情報ベース（**MIB**）**:** SNMP を通して管理可能なネットワークオブジェクトのセットについての形式的記述です。

アメリカ国立標準技術研究所（**NIST**）**:** 計測標準研究所で、米国商務省の非規制機関です。

オペレーショナルテクノロジー（**OT**）**:** システムの物理的状態の変化を検出する、または変化を生じさせるために指定されたハードウェアおよびソフトウェアです。

パッチ**:** オペレーティングシステムやソフトウェアプログラムの問題を修復するために使用する一編のソフトウェアです。

印刷スプーラー**:** Microsoft の Windows オペレーティングシステムのシステムサービスで、プリンターやネットワーク内のプリントサーバーに送られたジョブを管理する役割を担っています。

リモートアクセス**:** 他の場所から制御システムに行われるアクセスです。

リモートデスクトップ**:** 大抵のオペレーティングシステムに備わっている独立したプログラムまたは機能で、ユーザーはこれを使用して、稼働中のコンピュータシステムのデスクトップにアクセスし、やり取りをすることができます。このアクセスは、インターネットを介して、または地理的に異なる位置にある別のネットワークを通して行われます。

リスク許容度**:** リスク許容度とは、製造業者が戦略的目的を達成するために許容するリスクの量のことです。注釈: 組織にはそれぞれの分野や経営に応じて、それぞれ異なるリスク許容度があります。許容可能なリスクレベルを理解し、文書化しておくことは、それらのリスクに取り組むための正しいプロセスを確立するのに不可欠です。

簡易ネットワーク管理プロトコル（**SNMP**）**:** IP ネットワーク上の管理対象デバイスについての情報を収集し、編成するためのインターネット標準プロトコルです。

セキュリティ情報およびイベント管理（**SIEM**）**:** 収集され、相互に関係づけられ、解析されたセキュリティ関連情報の全体像を提供するためのセキュリティ管理手法です。

監視制御データ収集システム（**SCADA**）**:** コンピュータ、ネットワークデータ通信、およびグラフィカルユーザーインターフェースを高レベルのプロセス監視管理に使用し、プログラマブル論理制御装置などの他の周辺デバイスを加工プラントや加工機械へのインターフェースとして使用する制御システムアーキテクチャです。

伝送制御プロトコル**/**インターネットプロトコル（**TCP/IP**）**:** インターネット上のネットワークデバイスを相互接続するために使用する通信プロトコル一式です。

トランスポート層セキュリティ（**TLS**）：コンピュータネットワークにおいて通信セキュリティを提供する暗号プロトコルです。

テルネット: インターネットやローカルネットワークで、仮想端末接続を使用して双方向対話式テキスト指向通信機能を提供するために使用するプロトコルです。

ユニバーサルシリアルバス（**USB**）：コンピュータとデバイスの間の接続、通信、および電力供給のためにケーブル、コネクター、通信プロトコルを定義する業界標準です。

ホワイトリスト: システムやネットワークへのアクセスを許可された受入可能エンティティのリストに基づいたアクセス制御手法で、リストにないものはすべて遮断します。

無線 LAN（**WLAN**）：家、学校、コンピュータ実験室、あるいはオフィスビルといった限定された領域内で、無線通信を使って 2 台以上のデバイスを接続する無線コンピュータネットワークです。

DITTA について**:**

DITTA は、画像診断、放射線治療、ヘルスケア ICT、医療用電気装置、および放射性医薬品のために団結したグローバルな業界の代弁者で、600 を超える医療技術製造業者を代表し、ヘルスケアと患者予後の改善に尽力しています。DITTA は 2001 年に創設され、2012 年には、成長を可能にしグローバルな組織と提携しやすくするために、非営利事業者団体として法人化されました。発足以来、会員数は大きく増加し、今日ではその会員の間で世界中に 10 の地域団体が存在しています。2015 年に、DITTA は世界保健機関との公式な関係にある NGO 資格を授与され、2016 年には世界銀行との覚書に署名しました。DITTA のウェブサイト http://www.globalditta.org を参照してください。