Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

OTサイバーセキュリティの原則

クイックリファレンスガイド

重要インフラは、我々の生活様式を維持し、向上させるために不可欠である。我々の重要インフラ内にあるオペレーショナル・テクノロジー(OT)は、飲料水、エネルギー、交通手段等多くの重要なサービスを制御する。国際的に、OT資産に対する悪意のあるサイバー活動が増加していると報告されている。

OTサイバーセキュリティの原則は、あらゆるレベルの意思決定者がサイバーセキュリティリスクに適切な比重を与え、各国を運営し続けているシステムを最も安全にすることを支援すべく、設計されている。ある提案が、OTサイバーセキュリティの原則の1つ以上に影響を与えるか又はそれを破る可能性が高い場合、その提案は、OT環境に脆弱性をもたらす可能性が高い。

原則1：安全が第一 - システムの安全を確保しよう！
安全性は、物理的環境において非常に重要である。これには人命の安全、プラント、設備、環境の安全、プロセスの信頼性及び稼働時間が含まれる。サイバーセキュリティの管理は安全でなければならず、その安全性はサイバー脅威環境によって十分な情報が与えられなければならない。

原則2：ビジネスの知識が重要 - 重要なシステムを特定し、防御しよう
ビジネスを知り、プロセスがどのように機能しているかを知り、どこに接続があり、どの部分が重要であるかを知ることは、組織が利用可能なリソースに対して最も効果的なサイバーセキュリティの管理と対応能力を設計し、実装することに役立つ。組織は、重要なシステムを特定し、当該システムを防御するアーキテクチャを整備し、求められるビジネス成果を満たす復旧・復元プロセスを含められるようにすべきである。

原則3：OTデータは極めて貴重であり、保護する必要がある - OTデータを保護しよう
悪意のあるサイバー行為者にとって、システムがどのようにセットアップされているか、ネットワークがどのように構築されているか、コントローラーがどのように設定されているか、どのベンダーやデバイスが使用されているか及びどのプロトコルが使用されているかを知ることは、損害を与えるための宝の地図のようなものである。OTデータの完全性を確保しつつ、OTデータへのアクセス及びOTデータの配布を最小限に抑えるためのプロセスを導入すること。

原則4：OTを他の全てのネットワークから分離・隔離する - バックドアを閉めておこう
OTを、同業者、IT、インターネットを含む他の全てのネットワークから分離・隔離する。特に、OT環境においては、管理及び運用の役割の割当てを考慮すること。

原則5：サプライチェーンは安全でなければならない - サイバーサプライチェーンを保護しよう
サプライチェーンのセキュリティは、大手ベンダーのソフトウェアやデバイスにとどまらない。OTに含まれる全てのソフトウェア、デバイス、マネージドサービスプロバイダー(MSP)について、サポート、管理及び維持を含め、購入及び統合から廃止及び廃棄に至るまでを考慮すること。

原則6：OTのサイバーセキュリティには人が重要 - 人が防御の最前線
OTにおけるサイバー関連インシデントは、必要なツールを備え、インシデント検索のための訓練を受けた者なしには、タイムリーに予防し、防御し、特定し、対応し、回復させることはできない。必要なツールを備え訓練を受け、技術を有している者による、成熟し組織全体にわたるサイバーセキュリティ文化に支えられた、協力的なチームを作るための職員に対する投資は、組織のサイバー防御にとって極めて重要である。

Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

National Cyber Security Centre

a part of GCHQ

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

Te Tira Tiaki

Government Communications Security Bureau

National Cyber Security Centre

PART OF THE GCSB

Bundesamt für Sicherheit in der Informationstechnik

National Cyber Security Centre

Ministry of Security and Justice

警察庁

National Police Agency

This publication was developed by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) in collaboration with the U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing and Analysis Center (MS-ISAC), United Kingdom's National Cyber Security Centre (NCSC-UK),Canadian Centre for Cyber Security (Cyber Centre), New Zealand's National Cyber Security Centre (NCSC-NZ), Germany's Federal Office for Information Security (BSI Germany), the Netherlands' National Cyber Security Centre (NCSC-NL), Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and National Police Agency (NPA), and the Republic of Korea's National Intelligence Service (NIS) and NIS' National Cyber Security Center (NCSC).

OTサイバーセキュリティの原則

Australian Government
Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment
Canadian Centre
for Cyber Security

Centre de la sécurité
des télécommunications
Centre canadien
pour la cybersécurité

Te Tira Tiaki
Government Communications
Security Bureau

National Cyber
Security Centre
PART OF THE GCSB

Bundesamt
für Sicherheit in der
Informationstechnik

National Cyber Security Centre
Ministry of Security and Justice

警察庁
National Police Agency

This publication was developed by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) in collaboration with the U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing and Analysis Center (MS-ISAC), United Kingdom's National Cyber Security Centre (NCSC-UK), Canadian Centre for Cyber Security (Cyber Centre), New Zealand's National Cyber Security Centre (NCSC-NZ), Germany's Federal Office for Information Security (BSI Germany), the Netherlands' National Cyber Security Centre (NCSC-NL), Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and National Police Agency (NPA), and the Republic of Korea's National Intelligence Service (NIS) and NIS' National Cyber Security Center (NCSC).

目次

はじめに

重要インフラ組織は、浄水、エネルギー及び輸送の供給等不可欠なサービスを公衆に提供している。当該組織は、それらの重要なサービスを提供する物理的な設備及びプロセスを制御し運用するために、オペレーショナル・テクノロジー(OT)に依存している。そのため、不可欠なサービスの継続性は、OTのサイバーの安全保障及び安全を確保する重要インフラ組織に依存している。

OTは、重要インフラ組織の技術的環境において広く統合されており、当該環境が複雑な構造を有するため、ある決定に起因する特定のリスクを含め、ビジネス上の決定がOTのサイバーセキュリティにどのように影響するかを特定することは困難である可能性がある。決定には、同環境に新しいシステム、プロセス又はサービスを導入すること、技術的環境をサポートするベンダー又は製品を選択すること及びセキュリティ関連の事業継続計画及び実行手順書を作成すること等が含まれ得る。本書は、組織がOT環境の安全で安全が保障されることを確保し、重要なサービスの事業継続を可能にするため、OT 環境の設計、実装及び管理を実施する際の決定を支援することを意図としている。

OTサイバーセキュリティの原則は、豪州通信情報局豪州サイバーセキュリティセンター(ASD's ACSC)によって作成され、米国土安全保障省サイバーセキュリティ・インフラ庁(CISA)、 米国国家安全保障局 (NSA)、米国連邦捜査局 (FBI)、州横断情報共有分析センター(MS-ISAC)、 英国国家サイバーセキュリティセンター(NCSC-UK)、カナダサイバーセキュリティセンター (Cyber Centre)、ニュージーランド国家サイバーセキュリティセンター (NCSC- NZ)、ドイツ連邦情報セキュリティ庁 (BSI Germany)、オランダ国家サイバーセキュリティセンター (NCSC-NL)、内閣サイバーセキュリティセンター (NISC)及び警察庁 (NPA)、並びに韓国国家情報院(NIS)及びNISのサイバーセキュリティセンター(NCSC)によって共同署名されており、安全であり安全が保障される重要インフラのOT環境の創出と維持の指針となる6つの原則について述べている。

1. 安全が第一
2. ビジネスの知識が重要
3. OTデータは、極めて重要であり、保護される必要あり
4. OTを他のネットワークから分離・隔離しよう
5. サプライチェーンは安全でなければならない
6. OTサイバーセキュリティには人材が不可欠

これらの原則は、オーストラリアの重要インフラ事業者と共同で設計された。本書の作成を支援するために時間及び専門知識を提供してくれた全ての方々に感謝する。

本書の使用法

共同執筆機関は、OTについての意思決定者に対し、下されている決定がOT環境のサイバーセキュリティに不利な影響を及ぼす可能性があるかどうかの判断に役立てるために、本書に示されている6つの原則を適用することを推奨する。仮に、ある決定が本書で概説されているOTサイバーセキュリティの原則の1つまたはそれ以上に影響を与える又は反する場合、OT環境に脆弱性をもたらしうるであろう。そのため、そのような決定は、適切なサイバーセキュリティの管理が行われ、管理が実施された後の残存リスクが受容可能であることを確保するよう、また、そうでないのであれば、提案が再検討されるよう、より入念に検討される必要がある。OTのセキュリティに影響を与える決定を特定するために当該決定を迅速にふるいにかけることで、OT環境の設計、実装及び運用の際の安心、安全及び事業継続性を促進する力強く、十分な情報に基づく、包括的な決定の実施が強化される。

共同執筆機関は、OTについての意思決定者が各原則を読み、理解することを推奨する。本書は、組織のリーダー層(戦略的な決定を行う幹部や役員を含む) から戦術的、運用面の意思決定を行う技術担当者に至るまで、OTに影響を与える決定をふるいにかける必要がある全ての者に役立つことを意図としている。

オペレーショナル・テクノロジーサイバーセキュリティの原則

原則１：安全が第一

物理環境では安全が非常に重要である。幹部が生命に対する脅威を心配することなく、イノベーションや迅速な開発を優先するITシステムとは対照的に、サイバーの物理的な運用システムの幹部は、日常の意思決定において、生命への脅威を考慮しなければならない。重要インフラからの第一の危険には、高電圧、圧力放出あるいは可燃性爆発、動的衝撃（例：列車の速度超過）又は水処理におけるような化学的あるいは生物学的な危険等がある。さらに、エネルギー及び飲料水の供給などの不可欠なサービスが劣化又は中断されれば、市民の生活様式に影響が及び得る。連結しているという需要インフラの性質は、人的エラーによるものであれ、サイバー手段を通じた悪意のある破壊によるものであれ、障害が社会の日常的な機能に対して広範かつ予期せぬ影響を及ぼすかもしれないことを意味している

例示及び含意

安全について議論する際には、人命の安全や、プラント、設備及び環境の安全並びに重要インフラのサービスの信頼性及び稼働時間を考慮することが有用であろう。考慮対象となる環境及びシステムによっては、エンジニアがシステムの弱点を深く理解し、予期・管理が可能な形での障害発生が保障されることを含め、環境に導入された、いかなるサイバーセキュリティのシステム、プロセス及びサービスであっても、必然かつ予測可能であるという要件を意味しうる。同様に、安全のためには、サイバーセキュリティ及び脅威環境の理解によって、情報が与えられる必要がある。サービスの重要度によっては、環境に導入されたサイバーセキュリティシステム、プロセス又はサービスがブラックスタートに準拠することを確保するする必要がある。ブラックスタートに依拠するとは、当該サービス等が完全な電力損失後に遅滞なく再起動を行い、他のシステムへの最小限の依存で運用及び復旧できることを意味する。

「安全が第一」という原則は、以下のインシデント対応に関する質問が重要であることを含意している。

- 作業環境が安全であると見なされるためにはソフトウェアが正しく動作していることが求められる領域(安全及び保護システム)において、サイバーインシデントが発生した場合、組織は、悪意のある行為者がネットワーク上に存在していた又は現在存在していることを知った上で、職員を現場に派遣する準備ができているか？

- 作業環境が安全であると見なされるためにはソフトウェアが正しく動作していることが求められる領域（安全及び保護システム）において、サイバーインシデントが発生した場合、組織は、悪意のある行為者がネットワーク上に存在していた又は現在存在していることを知った上で、職員を現場に派遣する準備ができているか？[1]

- バックアップからの復元は、サイバーインシデントを軽減するための受容可能なアプローチか。つまり、悪意のあるアクターが一定の期間ネットワークに存在していた場合、バックアップは信頼できるか。修復後に重要なOTシステムが安全であることを検証する方法があるか?

人命の安全、プラント設備の安全及び環境の安全、並びに、サービスの信頼性及び稼働時間を維持する必要性は、全てのタスクに浸透する必要がある体系的な考え方である。以下のような、潜在的には関係ないとみなされる、重要かつ共通のサイバー衛生のタスクさえも必要である:

- バックアップをどのように取るか。バックアップを、時間制約が厳しい安全制御メッセージのネットワークと同じ（潜在的には飽和状態に近い）ネットワーク上で実行することにリスクはあるか?

- 資産をどのようにして発見するか？ 主体的な方法は受け入れられるか、又は、受動的な方法が唯一の方法か?

- 一般に、どのようにパッチを適用し、どのように変更管理全般を行うか。頻度、テストの厳密さ、対象範囲、ロールアウト戦略及びロールバック戦略に関するシステム要件は何か。

原則２：ビジネスの知識が重要

ビジネス自体に関する知識が多ければ多いほど、そのビジネスにおいてサイバーインシデントに対して、よりよく保護し、準備し及び対応することが可能となる。組織内のより高い層において、特にOTシステムへのサイバーリスクの理解、可視性及び報告があればあるほど、より良い結果が得られる。

全ての重要インフラ組織は、以下のベースラインを満たしていることを確認すべきである。

- 重要なサービスの継続的な供給に不可欠なシステムを特定する

- OTシステムのプロセス及びプロセスの各部分の重要性を理解する

- 不可欠なシステム及びプロセスを他の内部及び外部のネットワークから保護できる機構を構築する

- OTシステムの設計、運用及び維持の責任者が、OTシステムに接続される物理的なプラント及びプロセスや、利害関係者にサービスを提供する方法を含め、OTシステムが運用する事業の状況を理解していることを確保する

- 不可欠なシステムが動作可能となるのに必要な依存関係、及び、それらシステムがOTシステム外のシステムと接続している場所を理解する

1 ASD's ACSCのアドバイスは、決して身代金を支払わないことである. ランサムウェアの報告および復旧方法に関しては以下のガイダンスを参照のこと - https://www.cyber.gov.au/report-and-recover/recover-from/ransomware

例示及び含意

サイバーセキュリティの緊急課題として広く合意されているのは、守られるべきものを知ることである。この一つ目は、組織が重要なサービスを提供できるようにするために、事業のどの要素が不可欠であるかを理解することである。二つ目は、保護されているシステム及びプロセスを理解することである。これには、システムエンジニアリング図面、資産リスト、ネットワーク構成図、誰が何にどこから接続できるかの把握、復元手順、ソフトウェアベンダー、サービス、並びに、機器及び、可能な限り、ソフトウェア部品表並びに望ましい構成状態が含まれる(ただし、これらに限定されない)。

重要なサービスを提供するための事業の不可欠な部分を知るには、トップダウンの思考及びボトムアップの思考双方が必要である。トップダウンの思考は、従来、多くの組織がOTをITから切り離そうとするのを導いてきた。ボトムアップの思考は、組織がさらに前に進み、重要な機能に必要な最小限のOT機器一式を発見する機会を提供する。例えば、電気を発生させるには、発電機にもよるものの、発電機、制御盤のコントローラー及び適切な燃料供給が最低限必要となるだろう。重要インフラ事業者にとって、水を流し続けることや照明を点灯させ続けるといった、絶対的な核となる機能を守るために何が必要かを理解することが、サイバーセキュリティの管理を効果的に積み重ねる指針になるべきである。これは、デバイス及びファイルの機構、保護、検出並びにバックアップに影響を与える。

OT固有のインシデント対応計画及び手順書が、組織のその他の緊急・危機管理計画、事業継続計画、手順書及び必須のサイバーインシデント報告要件と統合されていることは重要である。プロセス・エンジニアの関与は、計画及び手順書を作成する際や調査、抑制又は復旧処理の際の両方で重要である。

また、第三者の関与前又は関与した際に、第三者に対し、情報のパックを提供し、迅速に対応できるようにすることも必要である。この第三者に対する情報のパックには、連絡先、サーバの命名規則、データソース、導入されたツール、どのツールを導入可能か等が含まれているべきである。全ての計画、手順書及び第三者に対する情報のパックは、法務を含む全ての関連当事者によって、定期的に実行され、更新されるべきであり、攻撃者に対する価値ゆえに、保護されなければならない。

職員がOTシステムの知識を得ることを補助する物理的観点も考慮されるべきである。これには、ケーブルを色分けすること、既存のケーブルに色付きのバンドを付けること又はOT環境で許可されているデバイスを視認性の高い方法でマーキングすることが含まれる。OT環境に承認されたコードのみが導入されることを確保すべく、承認されたデバイスのみがOT環境に接続されるべきである。明確な視覚的な手がかりによって、組織が未承認のデバイスを識別することで、環境をより適切に保護することができ、そして、組織がサイバー又はインテリジェンスに基づく事案の対応において、迅速に正しい決定を下すことができる。このようなマーキングは、正確性及び最新性を確保するために、定期的に評価及び検証される必要がある。

OTシステムの事業の状況を理解することは、OTの停止、サイバーセキュリティ侵害の影響及び重要性を評価するために不可欠である。また、重大なインシデント発生時に復旧の優先順位を決定するためにも不可欠である。OTに依存している組織が重要なサービスを提供するため、統合されたOTサイバーセキュリティの機能は事業にとって必要な部分である。OTサイバーセキュリティの職員は、電気、化学又はプロセス・エンジニアが有するであろう物理的なシステムについての深い理解を有することまで期待されないものの、プラント運用の実務知識を有するべきであり、最も重要なのは、物理プラントを担当する組織内の職員との実務的な関係を維持するべきである。そのような関係は、いかなるサイバー強化計画の成功にとっても、サイバー事案に対応する必要がある場合にも、重要である。

原則３：OTデータは極めて貴重であり、保護する必要あり

攻撃者の視点からみれば、使用されるデバイス及びプロトコルを含め、どのようにシステムが構成されているかを知ることは価値がある。これは、OT環境は滅多に変更されないからである。このレベルの情報によって、悪意のある行為者が、標的とされるマルウェアを作成し、テストすることができ、より広範な悪意のある結果を招いてしまう。

特に重要なのは、ネットワーク構成図、動作シーケンスに関する文書、論理図及び回路図等の技術的構成データである(例えば、アドレス1250が回路ブレーカーであるという知識や、特定のタイプのデバイスに関する組織のDNP3（分散ネットワークプロトコル）アドレス規則の理解)。同情報は5年後に変更されることはほぼなく、20年以上継続するかもしれない。そのため、技術的構成データは、長期間継続する価値を持ち、攻撃者にとって非常に有益である。攻撃者が、OTシステムがどのように機能するかについて深い知識を得ることは、特に重要性及び対応の必要性において、企業のIT環境における事前配備の概念に例えられるかもしれない。

また、電圧や圧力レベルといった、より一時的なOTデータは、組織やその顧客が何をしているか、又は制御システムがどのように機能しているかについての洞察を提供し得るため、重要である。OTデータを保護することは、知的財産(IP)や、電気、ガス、水道の計測又は健康に関する患者記録等、個人を特定できる情報(PII)の保護にとっても重要である。当該一時的なOTの値、IP及びPIIなど、その他のタイプのOTデータも保護する必要がある。しかし、OT担当の職員は、運用にとって重要であり悪意のある行為者にとって価値があるにもかかわらず、見過ごされがちな、技術的構成データも保護するべきである。

例示と含意

組織は、OTデータを管理し保護するために、OTデータを保存できる場所及び方法を定義及び設計するべきである。OTシステムは、多くの場合、企業のITシステムから分離・隔離されているが、攻撃者は、必要な全OTデータにアクセスするために、高度に保護されたOTシステムにアクセスする必要はないことが多い。組織は、職員がOT設定ファイルを企業の文書管理システムに保存することを要求するプロセス等、企業システム内部を含め、OT データの配布及び保存場所を最小限にするために、事業プロセスを変更する必要があるかもしれない。理想的には、重要なOTデータは常にOTシステムのレベルで保護されており、そのようにして、企業環境及びインターネットから分離・隔離されている保護されたリポジトリに保存されるべきである。

OTネットワークでは、外部ネットワークがOTからデータを取り込むのではなく、OTネットワークからデータを送り出すべきである。

重要なOTデータがどこにあるかを特定しようとする場合、以下のような質問が示唆される:

- ベンダー及びサービス技術者は、コピーを持っているか?
- コンサルタントは、コピーを持っているか?
- エンジニアは、OT環境に作業を転送する前に、他の専門家と電子メールで連絡を取ることができる企業のITシステムで作業しているか?
- データは、Eメール、ノートパソコン、企業のバックアップデバイス又はクラウドに保存されているか?
- 情報の破壊及び廃棄のプロセスはどのようなものか(例えば、プログラマブルロジックコントローラー(PLC)が廃棄される場合、ロジックコードは消去されるか)?

- エンドポイントの検知と対応 (EDR) や、ウイルス対策などのテクノロジーが、OTファイルのコピーを組織のネットワーク外に送信することによる不用意なデータ流出を防ぐ方法はあるか、職員によるオンラインのウイルス対策又は保管ストレージサービスへのファイルアップロードを防ぐ方法はあるか?
- 保険企業、人事、調達、ソーシャルメディア等とどの程度の情報が共有されているか?
- OTログファイルはどこに保存され、分析されているか?
- 使用可能なソリューションが整備され、OTに携わる全ての関係者が、潜在的には、作業を完了するためだけに不適切な場所に情報を保存するといった回避策を生み出さなくてもいようになっているか?

組織は、OTデータの機密性、完全性及び可用性を保護する以上のことを行うよう追求すべきである。理想的には、組織が、OTデータが表示又は漏えいした際に警告を受ける、潜在的には、特定のファイルに触れた場合に対応することができる、カナリアトークンを実装することにより、警告を受けるようにすることである。さらに、組織は、攻撃者がどのようなデータに既にアクセスしているか、そのデータが変更可能かどうかを考慮すべきである。これには、デフォルトのパスワードが含まれる。デフォルトのパスワードが変更されている場合、理想的には、失敗したログイン試行をキャプチャする方法があることを確保し、それらを調査しなければならない。

原則４：OTを他のネットワークから分離・隔離する

より重要な機能とネットワークを分離・隔離することは、数十年にわたる、共通のアドバイスとなっている。そのアドバイスは過去多くの出版物で取り上げられている[2]。企業ITネットワークは、通常、インターネット接続や、電子メール、Webブラウジング等のサービスの利用により、侵害のリスクがより高いと評価されることから、組織は、OTネットワークをインターネット及びITネットワークから分離・隔離すべきである。我々は、従前のアドバイスを変更するというよりは、むしろ、2つの主要な分野でアドバイスを追加する。

“他の全てのネットワークから”

最初に追加する分野は、重要インフラ組織のOTネットワーク及び他の組織のOTネットワーク間の接続を保護する必要性に関するものである。他の組織のOTネットワークからの接続は、重要な資産へのバックドアとなるおそれがあり、潜在的には、企業のIT及びインターネットからOTネットワークを保護するセキュリティ水準を迂回してしまう。

重要インフラ組織は、OTを他の全てのネットワークから分離・隔離すべきである。最近では、OTネットワークをベンダーから保護し、制限する必要性がかなりよく理解されている。また、2017年のHatmanマルウェア以来、理解が進んでいるのは、安全にとって必要不可欠なOTネットワークと言った、より重要なOTネットワークを、重要度がより低いOTネットワークから分離する必要性である。一方、あまりよく理解されていないのは、以下の例で定義されているように、上流及び下流の同業者及びサービスからOTネットワークを保護し、制限する必要性である。

2 例えば https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/network-hardening/implementing-network-segmentation-and-segregation, NSAとCISAによる、すべての運用技術及び制御システムにわたる開示を低減するための早急な措置の勧告 https://media.defense.gov/2020/Jul/23/2002462846/-1/-1/0/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF, 接続されたオペレーショナル・テクノロジーに対する悪質なサイバー活動の阻止 https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/0/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF, and https://www.cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-version-20-itsp80022

例示及び含意

例えば、送電企業は、自身のOTネットワークと他の送電企業(同業者)のOTネットワークとの間に接続を有する可能性がある。また、自身のOTネットワークと発電装置企業のOTネットワーク(上流)との間に接続を有する可能性がある。送電企業は、自身のOTネットワークと配電企業及び大口顧客(下流)のOTネットワークとの間に接続を有する可能性がある。

長年にわたり異なる組織間のOTの相互接続に関する問題をさらに深刻にしているのが、多くの重要インフラの下位部門で発生している混乱である。例えば、発電セクターでは、大型の画一的な発電機が多くのより小型発電機及び蓄電デバイスに置き換えられつつある。当該小型発電機及び蓄電デバイスを運用する組織は、海外に制御室を有し、OTネットワークから海外のベンダーへの恒久的な接続を有する可能性がある。

工学技術への信頼からサイバーセキュリティへの、重要な発想転換は、接続が存在する場合、接続されている組織の規模にかかわらず、その接続は安全でなければならないという概念である。すなわち、工学技術への信頼の観点からは、5 MWの太陽光発電所への接続よりも2 GWの発電所への接続の方が重要である。しかし、送電組織のOTネットワークへの攻撃ベクトルというサイバーセキュリティの観点からは、5MWの太陽光発電所の制御システムへのネットワーク接続は、2GWの発電所の制御システムへのネットワーク接続と同じ重要度を持つ。

組織は、他の組織が自身と同じサイバーリスク選好度、サイバー衛生及びサイバーセキュリティ基準を有していると推測することはできない。組織のOTネットワークが、ログ取得及びアラートなどの通常の考慮事項を含め、他の組織のOTネットワークから十分に保護されていないのであれば、OTネットワークのセキュリティ境界には他の組織が含まれていることになる。第三者のリスクを理解することは非常に重要である。

資産及びプロセスの重要度が異なる場合や、環境の信頼度が異なる場所では、OTネットワーク内の分離が用いられなければならない。例えば、配電網の柱上インフラは、南京錠でしか保護されておらず、信頼されていない携帯電話ネットワークを使用している可能性がある。このインフラは、より低い信頼レベルを持つべきであり、強固なセキュリティ措置及び完全に暗号化された通信経路により保護されたゾーン制の変電所のインフラから分離されるべきである。

管理と運用

また、本原則は、OTシステム及びサービスの管理・運用をめぐるアドバイスにも基づいている。典型的なアドバイスは、OTネットワークをITネットワークから論理的及び物理的に分離・隔離することを含んでいる。これに加え、組織は、明確に、システムの管理・運用サービスがどこに配置されているかを検討し、管理・運用のインターフェイスをIT環境のカウンターパートから適切に分離することを確保すべきである。運用・管理アカウント又はシステムの侵害により、それらが管理するシステムも侵害される。重要なOTシステムは、ITシステムに運用を依存すべきではない。

例示及び含意

企業のITネットワークは、通常、侵害されるリスクが高いと見られていることから、企業のITネットワークとOTネットワークとの間にファイアウォールがしばしば設置される。しかし、悪意のあるサイバーアクターの共通の目標は、一旦ネットワークに接続した後における特権昇格の追求である。悪意のあるサイバーアクターが企業のITネットワークを侵害し、特権昇格を果たし、ファイアウォールが特権ITアカウントを介してIT側から管理された場合、ITとOTの間のファイアウォールは、もはやOT環境に対して望ましいレベルの保護を提供できない可能性がある。このアーキテクチャは、信頼及びセキュリティレベルが異なる2つの環境がある場合に常に必要とされる。つまり、重要度の高い環境は、重要度の低い環境から管理されるべきではなく、常に同じ又はより高いセキュリティ体制を持つネットワークから運用されるべきである。

その他にも、管理・運営システムが重要であり、そのため適切な分離が必要な場合が数多くある。たとえば、Microsoftが指摘しているように、アクティブ・ディレクトリ (AD)ドメインは、ADフォレスト内のセキュリティゾーン境界としては機能しない。OT環境がIT環境と同じADフォレスト内にある場合又は信頼関係が存在する場合、OT環境に対して望ましいレベルの保護及び運用の分離は提供されない可能性がある。

同様に、仮想化は多くのOT環境で一般的になりつつある。OTインフラ又はコンポーネントの仮想化が、企業ドメインの特権アカウントによって管理されている場合を考えてみる。ランサムウェアやその他のメカニズムによって企業環境が侵害されると、仮想化されたOT環境が直接影響を受けていなくても、OT環境の管理に必要な特権ITアカウントにはもはやアクセスできなくなる。

重要なもう1つの例は、バックアップである。OT環境のバックアップ又はバックアップインフラが企業ITの特権アカウントによって管理されている場合、サイバーインシデントに対して望ましいレベルのリスク軽減が提供されない可能性がある。

ネットワークの分離・隔離は、OT環境におけるサイバーリスクを軽減する主要な方法の1つとして、長い間推奨されてきた。より従来からの物理的及び論理的な分離の問題に加えて、管理・運営システムも注目されている。ネットワークセキュリティ、認証及びアクセスコントロール、仮想化及びバックアップを含む、非常に重要な管理領域における、上述の非網羅的なリストで示されているように、組織は、OT環境における管理・運営システム及びサービスの分離が不十分であることのリスクを定期的に評価する必要がある。

原則５：サプライチェーンは安全でなければならない

サプライチェーンをより安全にすることは、かねてから、アドバイスの焦点となっている。当該アドバイスは、多くの過去及び現在の出版物で取り上げられている。例えば、機器及びソフトウェアのサプライヤー、ベンダー、管理サービスプロバイダー（MSP）が特にOTにアクセスし、サポートを提供する場合のサプライチェーン保証プログラムの導入の必要性等のアドバイスである。サプライチェーンをより安全にするという要件により、多くの場合、組織のOT環境における主要なベンダーの厳格な評価のレベルがもたらされている。組織は、既存のアドバイスに従うべきである一方で、我々はさらに、OT環境にとって特に懸念されるいくつかの追加的な分野を呼びかける。

例示及び含意

ベンダーが提示する重要度及びリスク開示に関し、考え方の転換が必要である。組織は、従来、大規模ベンダー又は工学技術の観点から最重要なベンダーのみが精査されることが多かったことから、監視が求められるシステムの範囲を再評価すべきである。サイバーセキュリティにとって、多くの場合、規模及び工学技術上の重要性は関係ない。

OT環境では、通例、ネットワークは極めてオープンなものとなっている。重要な制御メッセージは、一般的に、暗号化されない等、保護がほぼない又は全くされていない状態で送信される。一部の制御システムのプロトコルでは、ネットワーク上の全てのデバイスに送信されるマルチキャスト又はブロードキャストメッセージにて通信される。そのため、ネットワーク上のほぼ全てのデバイスは、重要な制御メッセージを見ることができる可能性があり、また望ましくないアクションを引き起こすためのメッセージを作成及び挿入できてしまうかもしれない。こうした要因により、全てのデバイスのサプライチェーンが重要となる。

「あらゆるデバイス」には、プリンター、ネットワーク機器通信機器等の周辺機器のほか、より一般的に考えつく、リモートターミナルユニット（RTU）、ヒューマンマシンインターフェイス（HMI）、エンジニアリングワークステーション、ヒストリアン、リレー（継電器）、インテリジェント電子デバイス（IED）及びコントローラーが含まれる。また、OTが正しく機能するために相互接続の観点や、他のシステムの正常機能の必要性の観点等に応じ、他のシステムについても考慮されなければならないだろう。これらには、ビル管理システム、空調(HVAC)、消火システム、エレベーター、カメラ及び物理的出入管理システムが含まれうる。

OT環境内の全てのデバイスのソース及び出所を把握する必要がある。これには、OTネットワークに接続するベンダー又はコンサルタントのノートパソコンが含まれる。当該ノートパソコンは、電子メールやウェブ閲覧等の明示的に禁止されているコンテンツにアクセスするために使用される可能性がある。デバイスが接続されていた、ベンダーの代わりの顧客等の他のネットワークはどのようなものか、また、当該ネットワークがOTネットワークと同じ信頼レベルにあるかどうかにも、考慮を払う必要がある。それには、信頼性の低い企業ITネットワークのネットワークやその他デバイスが、信頼性の高いOTネットワークで使用するために再利用される場合も含む。

ほぼ全ての組織がデバイスの評価中に行うことができる、小さい技術的なチェックとしては、トラフィックをキャプチャしているパケットアナライザーにデバイスを接続してみて、デバイスが予期せず遠隔アドレスとの通信を行おうとするかどうかのチェックがある。

もう一つ必要な考え方の転換は、テスト可能なデバイスが現在どのように構成されているかを考えるだけでなく、ファームウェアや設定が変更された場合デバイスは何をしうるかを検討することである。同検討は、デバイスが常時又は時折、ファームウェアのアップデートが可能なベンダーに接続されている場合、特に重要である。第三者の干渉から保護するため、組織は、ファームウェアが信頼できる場所から受信されていること、暗号をかけて署名されていること及び署名がチェックされていることを確保すべきである。

ベンダーは、OTシステムに対するリスクを増大させる可能性がある。組織にOTサイバーセキュリティの原則の1つ以上破ることを要求するベンダーの要求、習慣又はアーキテクチャは、OTシステムのサイバー攻撃に対する脆弱性を高めるおそれがある。ベンダーの製品又はサービスの適合性を評価する際、かかる活動は、ベンダーのサイバーセキュリティの成熟度につき、否定的な評価をすべきである。一般的な例としては、ライセンスの更新プロセスがある。このプロセスでは、OTネットワークの重要な部分から外部のインターネットへの接続が必要となる。その他の例としては、ベンダーがデータを収集し、ファームウェアを更新し、設定を変更し、又はその他の形態のリモートサービスやサポートの実行を可能にする手段として、リモートアクセスのセキュリティのアーキテクチャを迂回して、OTとインターネットを直接接続すること等が含まれる。

原則６：OTのサイバーセキュリティには人材が不可欠

OTにおけるサイバー関連のインシデントは、必要なツールを備え、防御の構築及びインシデントの探索訓練を受けた者なしには、防止又は特定することはできない。OTでサイバー関連のインシデントが特定された場合、訓練を受け、能力のある者が対応を求められる。

安全性に基づく強力なサイバーセキュリティ文化は、現在進行中のOTシステムのサイバー強靭性にとって重要である。各組織は、当該原則に基づく要件を、サイバーセキュリティ要件とは対照的に、職場の安全要件として捉え直す必要がある。

特に現場の技術者及びその他全ての運営担当の職員は、組織にとって、防御及び検知の最前線となることが多い。

例示及び含意

効果的なOTサイバーセキュリティの実行を支えるためには、様々なスキル、知識、経験及びセキュリティ文化を備えた、異なる背景を持つ者の組み合わせが必要である。同組み合わせには、インフラストラクチャー及びサイバーセキュリティチーム(一般的にITでみられる)のメンバーとともに、制御システムのエンジニア、現場の運営担当の職員及び資産管理者 (一般的にOTでみられる) を含む。

しっかりとまとまったOTサイバーセキュリティ文化を発展させるためには、組織全体でOT原則に沿った全般調整が求められる。異なる背景を持つメンバーによって持ち込まれる、異なる固有の価値観及び優先順位があることを考慮すること。例えば、OTサイバーセキュリティの第1の原則である「安全が第一」は、非エンジニアリングではない、又は、重要インフラではない背景を持つ人々にとっては、考え方の根本的な転換が必要になることが多い。エンジニアリングではない背景を持つチームメンバーがOTの課題を理解することは、チームがOTにおいてまとまって働くために重要である。

発電から水処理施設まで、ほぼ全ての重要インフラのOTの現場では、職員が防御の最前線に立っている。彼らはほぼ確実に、OTサイバーセキュリティの専門家でもなければ、企業のIT部門で働く者でもない。現地の作業員が、正式な情報技術（IT）や、サイバーセキュリティの訓練及び資格を受けることはめったにない。多くの場合、産業制御システム（ICS）のITコンポーネントを用いた経験は、ICTインフラ及びIPベースの通信への現場運営の依存度が高まってきているため、必要に迫られて勤務中に培われている。

そのため、作業員が嘲笑や評価を恐れることなく、潜在的なサイバー上の懸念を提起することについて、自信を持ち、権限が与えられていると感じられるようにするために、サイバーセキュリティ意識の発展を現場の安全文化の中核的要素とすることに大きく焦点を当てることが求められる。さらに、サイバーの安全性に関連する観察力が評価される文化を備え、当該観察力を急速に高めることができるプロセスを整備する必要がある。

職員のセキュリティ意識及びサイバーの安全性の文化を向上させるための潜在性のある戦略には、以下が含まれる:

- 安全性評価、工場受入試験（FAT）、サイト受入試験（SAT）及びエンジニアリング変更管理プロセスにサイバーセキュリティを組み込むこと。確立された手法としては、サイバーインフォームドエンジニアリング、サイバーPHA、HAZCADS等が含まれる。
- 現場の職員が不審な行動を特定及び報告することを奨励する環境及びプロセスを構築すること。一般的な悪い例は、エンジニアが現場にいる職員に知らせずにリモートでのメンテナンスを実施するものである。現場の作業員は、エンジニアの活動を、現地の端末上でのマウスの移動又はヒューマンマシンインターフェイス（HMI）との目視可能な相互作用として見ている。現地の職員は、このような行動を正常及び正当であるとして無視するようになっていく。
- 運用上の障害が特定された場合、現地の作業員に対し、サイバー侵害の可能性を考慮するように条件付けること。従来、エンジニアが対処する障害は、誤った設定、デバイスの故障、データの破損や許容範囲外でのデバイスの稼働等の工学技術上の問題によるものである。典型的な対処としては、プログラムの再起動、デバイスの再起動又はリセット、正常な設定の再読み込み及び書き込み、デバイスの交換等がある。従来、悪意のあるサイバー行為は考慮されてこなかった。すなわち、サイバーインシデントは、運用上の障害として誤って特定される又は退けられるか、完全に見落とされてきた可能性がある。障害がサイバー関連の原因を有する可能性も考慮すべきである。全てではなくとも、リスト化された従来の修復手順のほぼ全ては、サイバーセキュリティの調査に役立った可能性がある通信のリンクをリセットし、揮発性メモリを消去するというものである。OTにおけるサイバー事案の特定、分類及び調査には、特定の追加プロセス及び既存のプロセスの変更が求められる。

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre