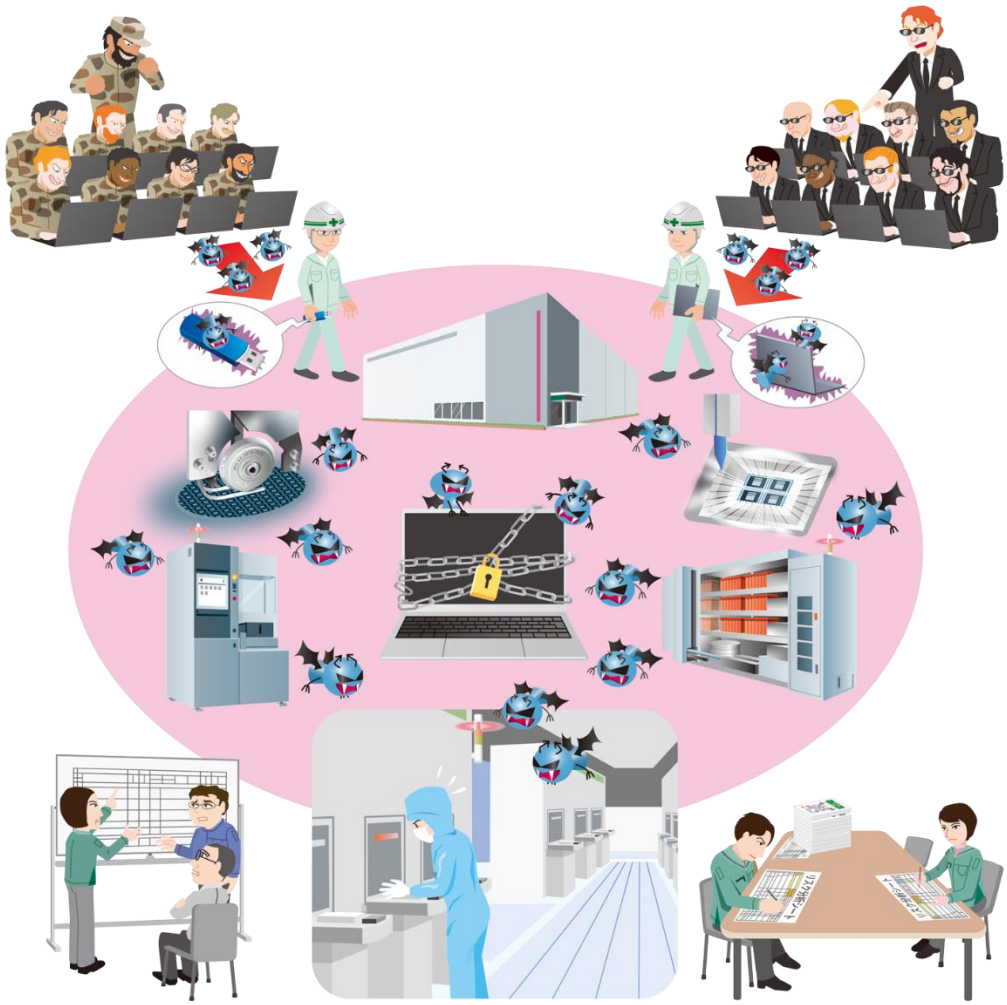
制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例6

～2018 年　半導体製造企業のランサムウェアによる操業停止～



2020 年 9 月

IPA 独立行政法人情報処理推進機構
セキュリティセンター

目 次

はじめに

「セキュリティ対策を推進する上で、過去の事例に学ぶことは有益です。」

制御システムを保有する事業者にとって、国内外で発生したサイバーインシデント事例の情報をもとに、自社の制御システムに対して同様の脅威が発生した場合のリスクアセスメント（リスクの特定・分析・評価）を実施することは、セキュリティリスク管理の強化につながる。

IPA（情報処理推進機構）は、制御システムにおけるリスクアセスメントの具体的な手順を解説した『制御システムのセキュリティリスク分析ガイド』を公開している。このガイドでは、制御システム保有事業者の事業に重大な被害を与えるサイバー攻撃からの回避に重点を置いた「事業被害ベースのリスク分析手法」を紹介している。自社の制御システムに対して、過去の事例と同様の脅威が発生した場合の事業への影響、脅威の発生可能性、発生した脅威の受容可能性／脅威に対するセキュリティ対策の有効性を分析することは、事業者にとって有益であると考えられる。

「制御システム関連のサイバーインシデント事例」シリーズは、『制御システムのセキュリティリスク分析ガイド』の補足資料として作成した。制御システムのサイバーインシデント事例をもとに、その概要と攻撃の流れ（攻撃ツリー）を紹介している。これらの情報をもとに、事業被害ベースのリスク分析を実施する際に、事例に相当する攻撃ツリーの作成、セキュリティ対策の策定に活用することが出来る。

【参考資料】に関しての内容詳細は、リンクから原文を確認いただきたい。本資料では、脚注は上付き番号（例 1）、巻末の参考資料は[ ]付き番号（例 [1]）で表している。

本資料の位置付け

2017 年 5 月ランサムウェア WannaCry(WannaCryptor)[1]が世界各国で猛威を振るい、150 か国 20 万件を超える被害が発生した[2]。被害はその後も続き、特にインターネットから遮断されていたが対策がなされていないコンピュータにも被害が発生した。

本書では、その被害例として、世界的な半導体製造企業の操業停止事象に関する当該企業やセキュリティベンダ等の公開情報（巻末の【参考資料】）をもとに、サイバーインシデントの概要と攻撃の流れを紹介している。後半では、当該インシデントに関係する情報を整理し、本インシデントをモデルとしたリスク分析を行う際の、攻撃シナリオや攻撃ツリー・ステップの作成例、対策・緩和策への活用例など、リスクアセスメントの際にどう活用するのかというアプローチを紹介している。

対象読者

制御システムのリスクアセスメント担当者

1. 2018 年 半導体工場のランサムウェアによる操業停止

1.1. インシデント概要

2018 年 8 月に、台湾の半導体製造企業 TSMC（Taiwan Semiconductor Manufacturing Company Limited）においてランサムウェア WannaCry の被害を受け多くのコンピュータと製造装置に影響を及ぼした[3]。3 日間の生産停止による損害額は、営業利益ベースで最大 190 億円に達するとの事。[4]

このインシデントは、TSMC を狙った標的型攻撃ではなく、WannaCry の亜種に感染した新規追加機器を、必要なウィルスチェックを行わず工場内のネットワークに接続したことにより、連鎖的なネットワーク内感染が発生したと言われている。[3]

今回は、WannaCry に関する分析結果の情報や過去のサイバーインシデントの事例を参考にに補完・推考しながら、被害拡大の状況を IEC 62443 や NIST SP800-82 Rev.2 等をもとに作成した仮想システム構成図（図 1-1）を用いて説明する。

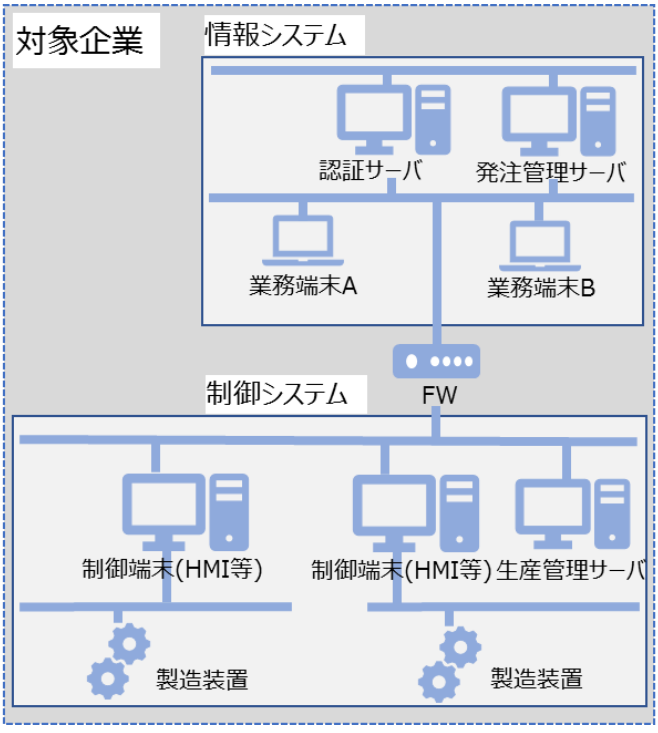


図 1-1 事例理解のための仮想システム構成図（実際のシステム構成とは異なる）

【コラム】WannaCry の特徴

本インシデントの1年 3 カ月前の 2017 年 5 月、WannaCry はわずか数日で 150 か国のコンピュータに影響を与えた。[2]
日本の企業でも、電機、自動車、鉄道など広い分野にわたって被害が報じられた。
WannaCry は特定の標的を選ばない自己拡散型（バラマキ型）のランサムウェアで、ネットワークを介して次々と感染を続ける。感染の手順はまず、ローカルネットワークとグローバル、ローカル含め無作為の IP アドレスに対してスキャンし、対象を絞ると SMB ポート 445 番で接続し、Windows の MS17-010[5] [6] の脆弱性を利用して感染を拡大する。
同時に感染したコンピュータを暗号化し、利用できなくする。[7]
つまり、445 番ポートが開いており、MS17-010 の脆弱性の対策がなされていないコンピュータに感染が広がった[1]。
MS17-010 のセキュリティ更新プログラムは 2017 年の 3 月に公開済みであったため、この爆発的な感染までは2カ月の猶予期間があったにもかかわらず、その対応が出来ていないコンピュータが被害を受けたことになる。

[1] 正確には、WannaCry 感染前にバックドアツールである DoublePulsar がインストールされている場合には、MS17-010 の脆弱性が対策済みでも感染する。

1.2. 被害発生にいたる攻撃の流れ

1.2 節では、参考情報で公開されている内容をもとに、サイバー攻撃から被害発生にいたるまでの流れを次の 2 つの局面に分けて解説する。

1.2.1【攻撃局面 A1（1）】機器の持ち込み

WannaCry の亜種に感染した製造用のツール（コンピュータ）を企業内に持ちこむ（図 1-2）。[3]
実際のところは、過失者が対象企業の職員なのか、ベンダーやサービスといった対象企業の関連会社の人かは定かではないが、ここでは仮に対象企業に入るための制限が無い内部者とする。

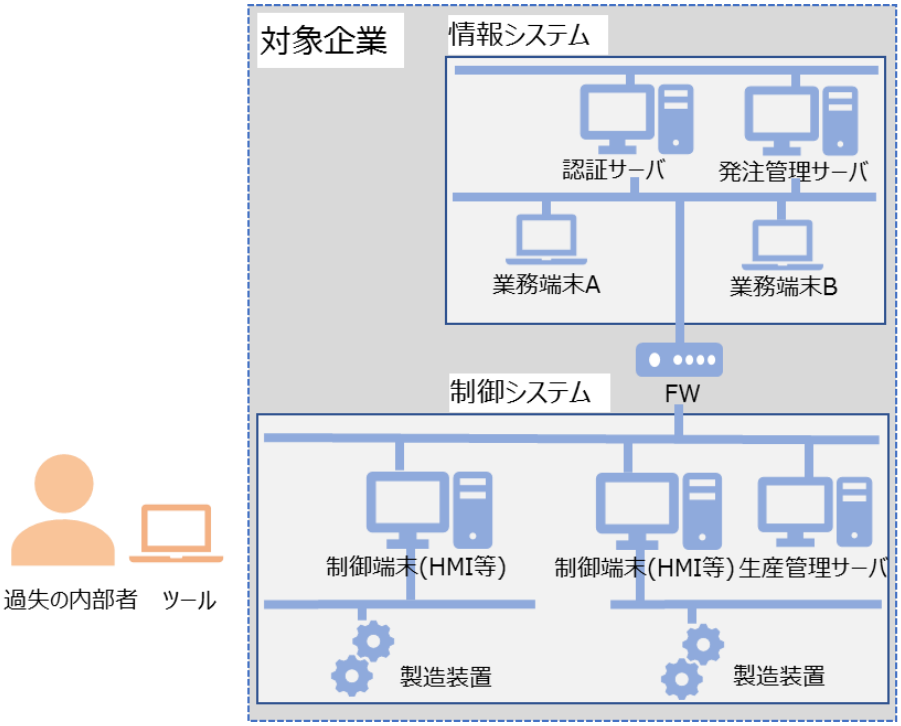


図 1-2 対象企業への侵入

1.2.2【攻撃局面 A1 （2）】製造用ツール（コンピュータ）のネットワーク接続

過失の内部者が、製造用のツールを導入するためにランサムウェアに感染したコンピュータを制御系ネットワークに接続する（図 1-3）。

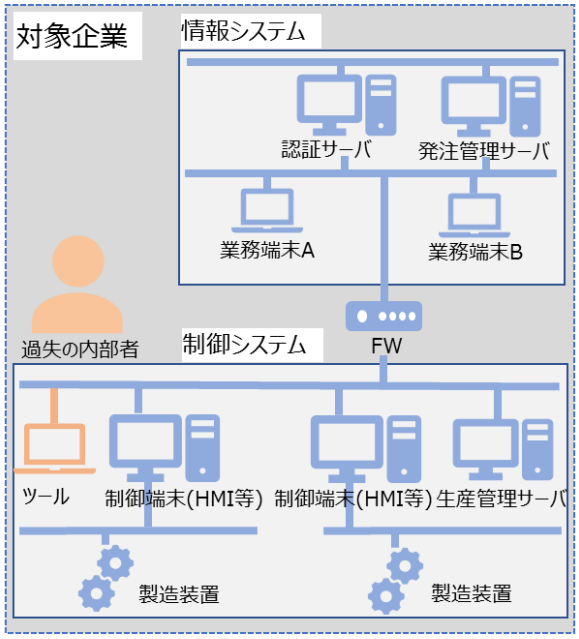


図 1-3 機器のネットワーク接続

1.2.3【攻撃局面 A2 （1）】製造用ツールから制御系ネットワークのスキャンと感染

持ち込んだ製造用ツール（コンピュータ）に感染したランサムウェアが、ネットワーク内の別のコンピュータをスキャンし、感染可能なコンピュータに自分自身をコピーしていく（図 1-4）。[6]

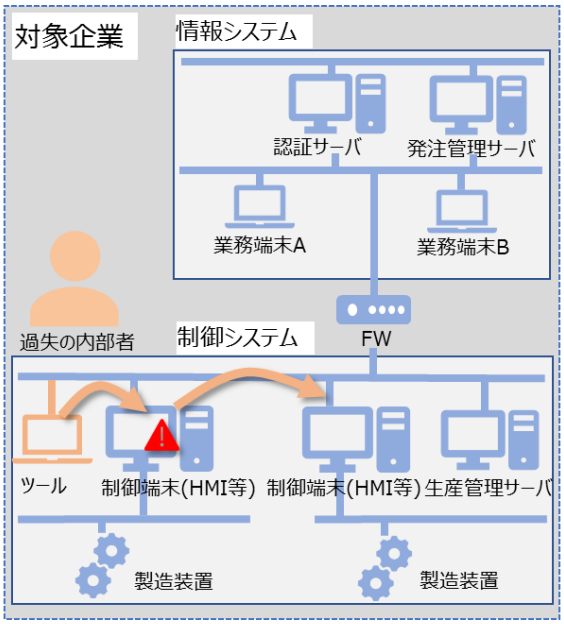


図 1-4 制御系ネットワークのスキャンと感染

1.2.4【攻撃局面 A2（2）】ネットワーク内での感染拡大と暗号化

ランサムウェアはネットワーク内のコンピュータに次々とスキャン―感染を続け、同時に感染したコンピュータのデータを暗号化していき（図 1-5）[7]、制御システムの機能が停止する（図 1-6）。

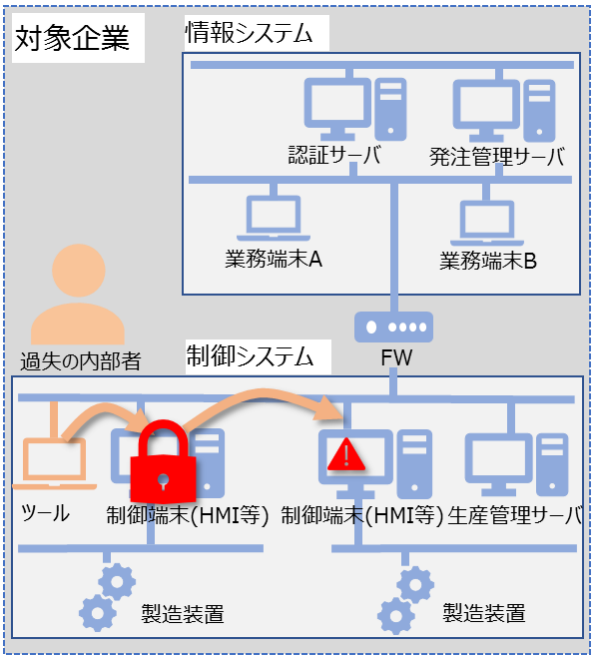


図 1-5 コンピュータのデータ暗号化(1)

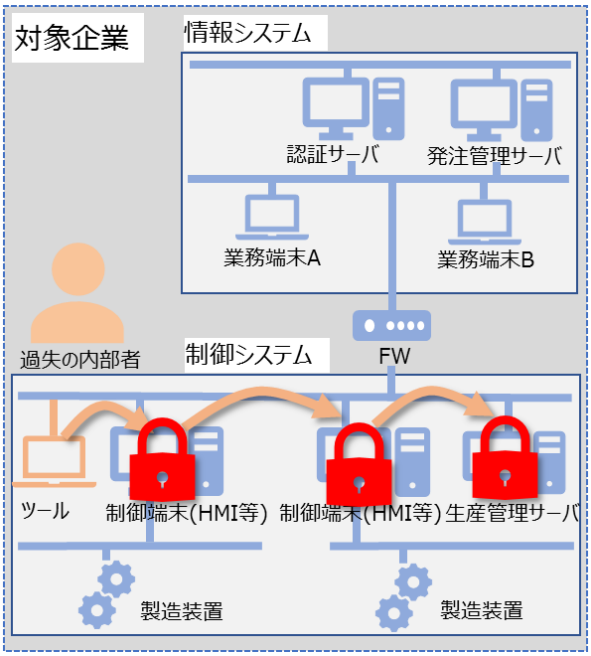


図 1-6 コンピュータのデータ暗号化(2)

2. リスク分析（事業被害ベース）の素材としてのインシデント情報の整理

2.1. 事業被害と攻撃シナリオの検討

本インシデントを参考に、検討した事業被害の例を表 2-1 に示す。
2.2 節では、この事業被害と攻撃シナリオに至る攻撃ツリーを検討する。

表 2-1 事業被害の例

項番	事業被害			
1	製造システムの操業停止			
	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
	工場の操業を制御する役割のコンピュータが暗号化され操業停止となる。	感染したすべてのコンピュータ	感染したすべてのコンピュータ	感染したコンピュータの暗号化

また、事業被害に至る攻撃ルートの例を表 2-2 に示す。

表 2-2 攻撃ルートの例（下線はリスク分析をする上での IPA による想定）

項番	誰が	どこから	どうやって	どこで		何をする
	攻撃者	侵入口	経由	攻撃拠点	攻撃対象	最終攻撃
1	*過失の内部者*	*制御システムエリア入り口*	*ランサムウェアに感染した新規導入機器*	全ての感染端末	全ての感染端末	暗号化

類似の経路として、ランサムウェアが混入された USB 外部記憶媒体を制御ネットワーク上の機器に接続して感染するケースもあり、同様に考えられる。

2.2. 攻撃ツリーの作成

今回のインシデント事例をリスク分析における攻撃ツリー・ステップの枠組みにあてはめ整理した内容が表 2-3 となる。分析対象の範囲などによっては切り出し方のパターンは考えられるが、一例として参照いただきたい。

表 2-3 事業被害:製造システムの操業停止の例

攻撃局面	攻撃ステップ項番	攻撃シナリオ 攻撃ツリー・ステップ ＜持ち込みの機器がランサムウェアに感染しており、当該機器を制御ネットワーク上の機器に感染。感染したコンピュータが暗号化され機能停止＞
【A1】	S1	侵入口= 制御システムエリア入り口 ランサムウェアに感染した製造用ツール(コンピュータ)を制御システムエリアに持ち込む
【A1】	S2	製造用ツール(コンピュータ)を制御ネットワークに接続する。
【A2】	S3	ランサムウェアが、接続されたネットワークをスキャンし、通信可能なコンピュータにランサムウェアをコピーする。
【A2】	S4	感染したコンピュータは、ランサムウェアによるコンピュータ内のデータの暗号化により機能停止する

【コラム】もう一つの事業被害

今回、半導体製造システムが停止することを事業被害としたが、半導体製造業において考慮すべき事業被害の一つに、製造した半導体素子に知らないうちにバックドアが組み込まれてしまうというものもある。これは、素子設計から製造に図面が渡される途中に図面内にバックドア回路が付加されて、それを知らずに製造し、その素子を購入し組み込んだ機器にバックドアが仕込まれてしまうというものである。

この場合、製造チップ内に証明書を入れ正真性を保つなど、製品自体のセキュリティへの配慮も必要となる。

2.3. 事業被害ベースのリスク分析の分析要素のまとめ

本インシデントをリスク分析の際の素材として活用するために、1.2 節で紹介した攻撃局面を分析ガイドで説明している事業被害ベースの分析要素毎にまとめた結果が表 2-4 となる。

表 2-4 各種情報をもとにした分析要素のまとめ

分析要素		内容
攻撃用途		
	侵入口	制御システムエリア入り口
	攻撃対象	制御用のコンピュータ
	攻撃拠点	制御用のコンピュータ
	経由	新規導入されたツール
攻撃者		過失の内部者
事業被害		製造システムの操業停止
攻撃シナリオ		持ち込みの機器がランサムウェアに感染しており、当該機器を発端に制御ネットワーク上の他のコンピュータがランサムウェアに感染。感染したコンピュータが暗号化され機能停止
最終攻撃（目的）		コンピュータの暗号化
攻撃ルート		表 2-2 を参照
攻撃ツリー		表 2-3 を参照
攻撃手法		ネットワーク上のコンピュータのスキャン ランサムウェアのコピー ランサムウェアによる暗号化

リスク分析を進める上では、日々の活動を通じて実際のインシデント事例などの情報収集を行い、最新動向をキャッチアップし、事例毎に表 2-4 のように整理した情報を蓄積していくことが肝要となる。

2.4. 対策・緩和策の整理

対策・緩和策の検討を進める上で、一般的なランサムウェアの観点からは、CIS[2]から公開された Security Primer – Ransomware[8]、マイクロソフトの「Petya や WannaCrypt などのラピッド サイバー攻撃を緩和する方法」[9]、また、サプライチェーン管理の観点から NIST[3] Best Practices in Cyber Supply Chain Risk Management[10]、NCSC[4]の Supply chain security guidance[11]等を参考にして、リスク分析作業に活用するための制御システムに対する緩和策を整理した。表 2-5 は、代表的な対策・緩和策をまとめたものとなる。

表 2-5 代表的な対策・緩和策の例

項番	対策・緩和策
D1	システムのバックアップを作成し、リストアの確認を行う[8][9]
D2	システムが最新のパッチで更新されていることを確認する[9]
D3	アンチウィルスなどのマルウェア対策を行う[9]
D4	ファイル共有やリモートデスクトップのポートが不要であれば塞ぐ[8]
D5	不要なレガシィプロトコルの無効化[8][9]
D6	ネットワークのセグメンテーションを行い、アクセス制御を適用する[8]
D7	物理的な入退管理
D8	機器持ち込み時のウィルスチェック[10]
D9	サプライヤーのセキュリティ要件を設定し、サプライチェーン内のセキュリティに対する意識を高める[10][11]
D10	自動的な検疫システムの利用[10]

「D1. システムのバックアップを作成し、リストアの確認を行う」は、ランサムウェアによって暗号化された場合は、あらかじめバックアップしたデータからリストアするしか確実な対応策が無い。ランサムウェアによっては、共有フォルダや接続された外部記憶媒体のバックアップやボリュームシャドウコピー[5]を削除するものもあるため、バックアップデータをオフラインで保管するのが望ましい。また、定期的にバックアップが取得できているか、スムースにリストアできるかの確認も定期的に行う必要がある。

「D2. システムが最新のパッチで更新されていることを確認する」は、特に WannaCry のような脆弱性を利用したランサムウェアに対する一般的な対応策となる。

---

2 Center for Internet Security https://www.cisecurity.org/

3 National Institute of Standards and Technology

4 National Cyber Security Centre

5 アプリケーションやシステムを稼働したままバックアップできる Windows の機能

「**D3. アンチウィルスなどのマルウェア対策を行う**」は、既知のマルウェアを検出可能なシグネチャ型のアンチウィルスだけではなく、ふるまい検知型の導入など未知のマルウェアに対しても対策を講じることが望ましい。

「**D4. ファイル共有やリモートデスクトップのポートが不要であれば塞ぐ**」は、リモートデスクトッププロトコル port3389、ファイル共有（SMB） port445 などのサービスを利用していないのであれば、ファイアウォールなどでマルウェアが利用できないように設定をしておく。

「**D5. 不要なレガシィプロトコルの無効化**」は、具体的にはマイクロソフトの SMB v1 を可能であれば無効にするという事である。SMB v1 に対するセキュリティパッチは既に提供されてはいるが、SMBv1 の機器が上位バージョンとの通信時に、上位バージョンの持つより高度なセキュリティ機能を無効としてしまう（セキュリティダウングレード攻撃）。[11]。

「**D6. ネットワークのセグメンテーションを行い、アクセス制御を適用する**」は、ネットワークの適切なセグメンテーション（VLAN 等）を行い、セグメント間に境界 FW を設置して必要最小限の通信のみ許可する事を意味する。

「**D7. 物理的な入退管理**」は、基本的には非関係者の侵入を防ぐためや、関係者の行動監視として活用されるものであるが、今回の事例では、入室時に所持している機器のウィルスチェックを行うといったルール作りを含んでいる。

「D8,D9」はサプライチェーンセキュリティマネジメントの観点からの対策として、機器の持ち込み前にウィルスチェックを確実に行うことや、サプライヤーを含む意識を高めることでチェックのし忘れを防ぐ。

「**D10. 自動的な検疫システムの利用**」は、自動的な検疫システムを利用する事で、人手の介入によるリスクを低減させる事を意味する。

【コラム】サプライチェーンのリスクマネジメント

新たに機器やソフトウエアなどを導入する場合、それらのベンダーやサプライヤーのセキュリティ対策の影響を直接被ることになる。IPA が毎年報告する「情報セキュリティ 10 大脅威」[12]でも 2019,2020 年と 4 位と高い順位となっている。

サプライチェーンにおけるセキュリティマネジメントに関しては、本文で参照した NIST や NCSC の資料によると、導入する機材のセキュリティチェックだけでなく、ベンダーやサプライヤーのセキュリティ管理やセキュアな開発体制の確立と維持向上が重要である。

例えば、

・サプライヤーの実施している脆弱性対応、マルウェア保護、アクセス制御の確認、物理的なセキュリティ対策状況の把握

・セキュリティに関する考慮事項を契約プロセスに組み込むこと

・流通プロセスの安全性の確認

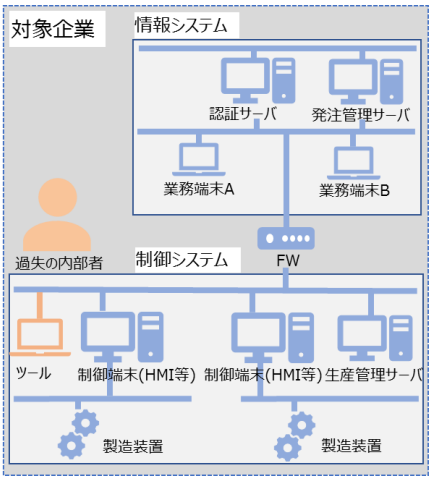
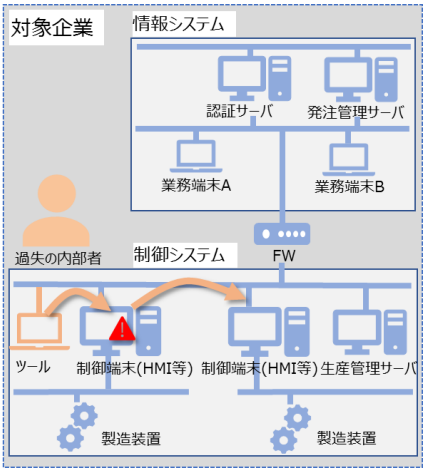
・契約解消時の守秘情報の扱いを明確にすること

リスク分析でいうところの侵入口となるため、確実な対策と運用が必要となる。

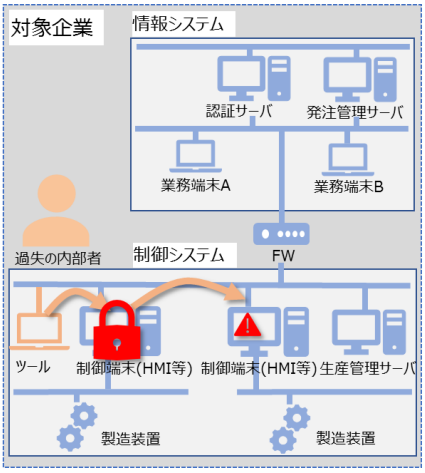
2.5. 攻撃ステップと対策・緩和策の関連付け

2.3 節までの情報をもとに、【攻撃局面 A1】や【攻撃局面 A2】と代表的な対策・緩和策を紐づけた例が表 2-6 となる。セキュリティ対策の基本である「多層防御」を考慮し、緩和策を立案することがポイントとなる。

表 2-6 制御システムにおける攻撃ステップと対策・緩和策の紐づけ例

攻撃局面	攻撃ステップ[6]	対策・緩和策	対象システム・資産
【攻撃局面 A1】  	[S1][S2] 制御システムエリアへの感染機器の持ち込みと接続	•システムが最新のパッチで更新されていることを確認する[D2] •アンチウィルスなどのマルウェア対策を行う[D3] •物理的な入退管理 [D6] ・持ち込み品のウィルスチェック[D8]	•持ち込みのツール
【攻撃局面 A2】  	[S3] マルウェアによるネットワークのスキャンと感染	•システムが最新のパッチで更新されていることを確認する[D2] •アンチウィルスなどのマルウェア対策を行う[D3] •ファイル共有やリモートデスクトップのポートが不要であれば塞ぐ[D4] ・ネットワークのセグメンテーションと境界 FW の設置[D6]	•制御端末、生産管理サーバ、製造装置など

6 [S]は表 2-3 の項番と対応。 [D]は表 2-5 の項番と対応。

攻撃局面	攻撃ステップ[7]	対策・緩和策	対象システム・資産
【攻撃局面 A2】  	[S4] 感染したコンピュータの暗号化	•システムのバックアップを作成し、リストアの確認を行う[D1]	制御端末、生産管理サーバ、製造装置など

【補足説明】

すでに暗号化されてしまったケースへの対応は、一部のランサムウェアに対してではあるが、ID Ransomware[14]、No More Ransom Project[15] 等のランサムウェアデータベースサイトでランサムウェアの特定や暗号化の解除キー（復号キー）を提供しており、本解除キーが使えるケースもあり得る。

7 [S]は表 2-3 の項番と対応。 [D]は表 2-5 の項番と対応。

おわりに

本資料では、制御システムにおけるインシデント事例を紹介すると共に、セキュリティリスクアセスメントへの活用方法について一つのアプローチを紹介した。

事業被害ベースのリスク分析においては、自社の制御システムにとって回避すべき事業被害を明確化し、被害に至る攻撃シナリオと攻撃ルートを漏れなく洗い出すことが重要である。攻撃シナリオは、過去に発生した制御システムのインシデント事例を含む各種の公開情報を参考にしつつ、自社の制御システムに生じ得る脅威とその影響を検討するが、具体的な攻撃ルート・攻撃手順を想定することで、セキュリティ対策を効率的に進めることが可能となる。

本資料が各社の制御システムのセキュリティ向上に活用されることを期待する。

参考資料

[1] [IPA] 世界中で感染が拡大中のランサムウェアに悪用されている Microsoft 製品の脆弱性対策について
https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html

[2] [REUTERS] Cyber attack hits 200,000 in at least 150 countries: Europol
https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX

[3] [TSMC] TSMC Details Impact of Computer Virus Incident
https://www.tsmc.com/tsmcdotcom/PRListingNewsArchivesAction.do?action=detail&newsid=THHIANTHTH

[4] [経済産業省] 電力分野を巡るサイバーセキュリティ政策の動き
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/003_07_00.pdf

[5] [マイクロソフト]マイクロソフト セキュリティ情報 MS17-010 - 緊急
https://docs.microsoft.com/ja-jp/security-updates/securitybulletins/2017/ms17-010

[6] [トレンドマイクロ] ランサムウェア「WannaCry／Wcry」のワーム活動を解析：侵入／拡散手法に迫る
https://blog.trendmicro.co.jp/archives/14920

[7] [三井物産セキュアディレクション] 「WannaCry 2.0」の内部構造を紐解く
https://www.mbsd.jp/blog/20170518.html

[8] [CIS] Security Primer – Ransomware
https://www.cisecurity.org/white-papers/security-primer-ransomware/

[9] [マイクロソフト]「Petya や WannaCrypt などのラピッド サイバー攻撃を緩和する方法」
https://msrc-blog.microsoft.com/2018/03/06/how-to-mitigate-rapid-cyberattacks-such-as-petya-and-wannacrypt/

[10] [NIST] Best Practices in Cyber Supply Chain Risk Management
https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

[11] [NCSC] Supply chain security guidance
https://www.ncsc.gov.uk/collection/supply-chain-security

[12] [IPA]情報セキュリティ 10 大脅威 2020
https://www.ipa.go.jp/security/vuln/10threats2020.html

[13] [Microsoft] Stop using SMB1
https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858

[14] ID Ransomware
https://id-ransomware.malwarehunterteam.com/

[15] No More Ransom Project
https://www.nomoreransom.org/ja/index.html

更 新 履 歴

2020 年 9 月 8 日	初版	ー

制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例 4

～2018 年 半導体製造企業のランサムウェアによる操業停止～

[発　　行]　2020 年 9 月 8 日　第 1 版

[著作・制作]　独立行政法人情報処理推進機構　セキュリティセンター

編集責任　辻　宏郷

執筆者　福原　聡

協力者　桑名　利幸　木下　仁　高見　穣　小助川　重仁