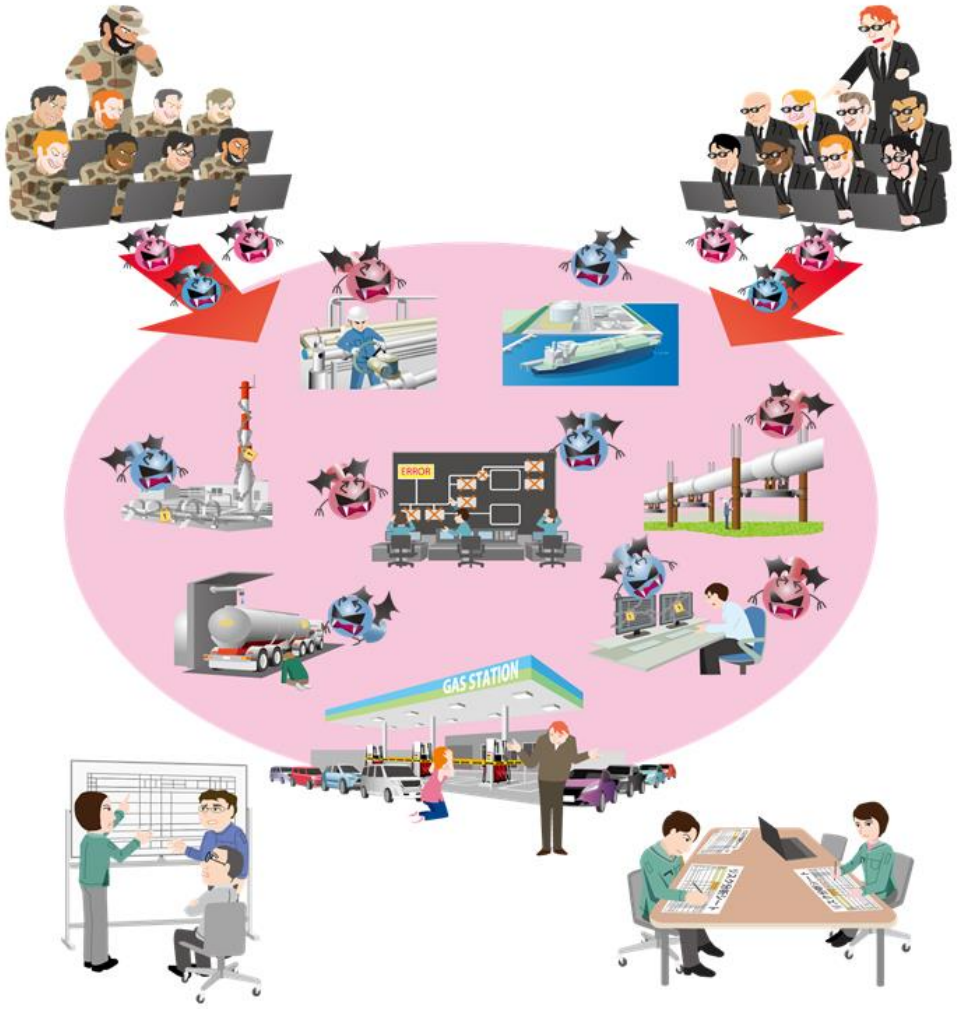
制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例9

～2021 年　米国最大手のパイプラインのランサムウェア被害～



2021 年 10 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

目 次 2
はじめに 3
1. 2021 年 米国最大手のパイプラインのランサムウェア被害 4
1.1. インシデント概要 4
1.2. 被害発生にいたる攻撃の流れ 6
1.2.1【攻撃局面 A1】対象組織への不正侵入 6
1.2.2【攻撃局面 A2】ネットワーク内部の調査 7
1.2.3【攻撃局面 A3】 機密情報の窃取 8
1.2.4【攻撃局面 A4】 コンピュータの暗号化 9
1.2.5【攻撃局面 A5】 制御システムの停止 10
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 11
2.1. 事業被害と攻撃シナリオの検討 11
2.2. 攻撃ツリーの作成 12
2.3. 事業被害ベースのリスク分析の分析要素のまとめ 13
2.4. 対策・緩和策の整理 14
2.5. 攻撃ステップと対策・緩和策の関連付け 17
おわりに 20
参考資料 21

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

2021 年 5 月 7 日、米国の燃料パイプライン最大手の Colonial Pipeline が、サイバー攻撃によりランサムウェアに感染し業務を停止した[1]。この停止は 6 日間続き、米国東部南部でガソリンスタンドの休止や油価の上昇を招いた。

本書では、当該企業や政府機関、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. 2021 年 米国最大手のパイプラインのランサムウェア被害

1.1. インシデント概要

2021 年 5 月 7 日米国最大手のパイプライン企業 Colonial Pipeline がランサムウェアによるサイバー攻撃を受けた。被害は情報系であり、パイプライン制御システムそのものは直接の影響を受けていなかったが、予め決められていた全社的なインシデント対応プロセスに則って、パイプラインは予防保全的に停止された。[1]

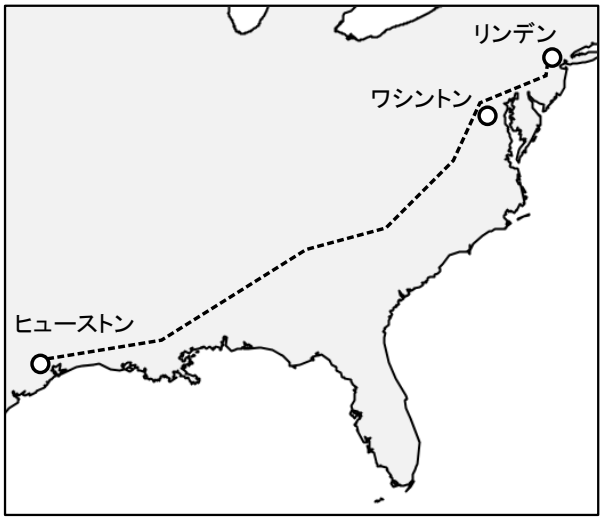


図1 Colonial Pipeline 社の主要なパイプライン

このパイプラインは米国東海岸で消費される燃料の約 45%を扱っており、6 日間続いたパイプラインの停止により、例えば首都ワシントンのガソリンスタンドのうち約 81%でガソリンが売り切れ状態となったなど市民生活に大きな影響を与えた[2]。また、ランサムウェアを使用する近年のサイバー攻撃は、二重の脅迫[3]と呼ばれる手口が併用され、データの暗号化のみならずデータの窃取が行われ脅迫される。本ケースでは 100GB 近いデータが窃取されたと報道されている。[4]
当該インシデントについて FBI[1]は DarkSide ランサムウェアが関与していると声明を出している[5]。DarkSide はランサムウェアの呼称でもあり、攻撃グループの名前でもあり、ランサムウェアによるサイバー攻撃のクラウドサービスの呼称でもある[6]。

今回は報道やセキュリティ企業の情報を参考に補完・推考しながら、サイバー攻撃の状況を 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。[2]

---

1 Federal Bureau of Investigation 連邦捜査局）

2 本インシデントは、サイバー攻撃が制御システム自体に被害を与えたのではないが[1]、情報システムへのサイバー攻撃によってもこのようなインシデントが起こりうるとして紹介している。

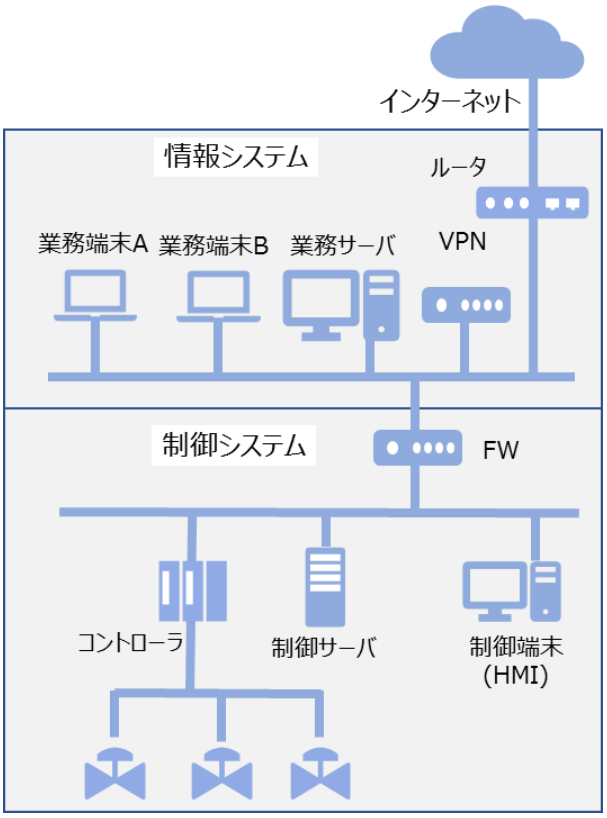


図 1-1　事例理解のための仮想システム構成図（実際のシステム構成とは異なる）

【コラム】 Ransomware as a Service

このインシデントで用いられた DarkSide ランサムウェアは、クラウドでランサムウェアの攻撃サービスを提供する RaaS(Ransomware as a Service)という形態で提供されている。このサービスは、攻撃ツールの開発者が攻撃を行う RaaS 利用者を募集して、利用者が攻撃により得た身代金の一部を開発者が手数料として徴収するという仕組みとなっている。

RaaS では、ランサムウェア本体の作成とカスタマイズや、被害者からの身代金の集金、被害者から受け取ったビットコインのマネーロンダリングと思われる機能などが提供される。

DarkSide のクラウドサービスに関しては、パートナーに対しクラウド上で被害者とのコミュニケーションを管理するための管理パネルや、テスト用の自動復号化の機能、標的に対する DDoS 攻撃[3]を行う機能なども提供されていたとのことである[7]。

[3] Distributed Denial of Service attack（分散型サービス拒否攻撃）

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】対象組織への不正侵入

本稿執筆時点ではまだ調査が続いているが、攻撃者はインターネット上から VPN の正規のアカウントを使って侵入してきたと考えられている。この VPN 装置は当該企業の情報システム管理部門では把握していなかった。また、パスワードは十分に複雑なものではあったが、多要素認証は構成されていなかった[8]。このパスワードについては、以前に漏えいしていたもので、今回のインシデントは漏えいしたものとは異なるアカウントであり、このパスワードを使い回ししていたと考えられている[9]。(図 1-2)

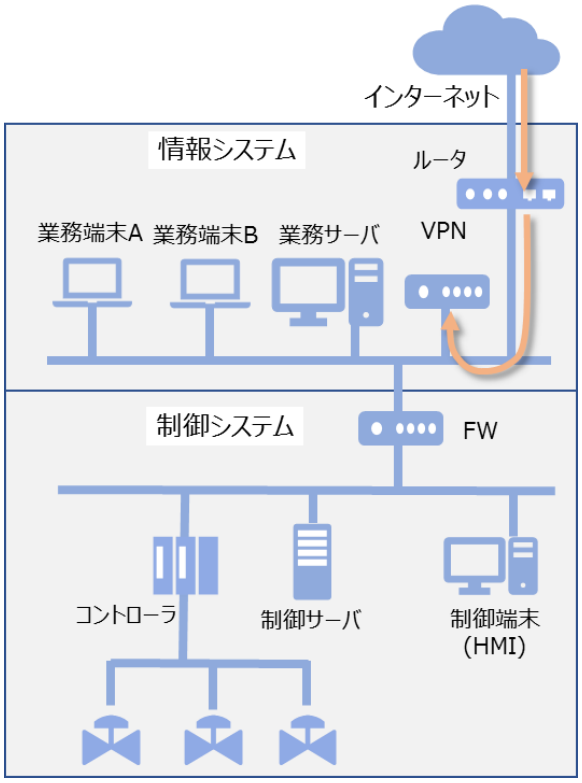


図 1-2 対象組織への侵入

1.2.2【攻撃局面 A2】ネットワーク内部の調査

攻撃者は、窃取して脅迫に利用できうる機密情報の所在についての調査を行う。

更に、サイバー攻撃の対象を増やし効果が最大となるように、当該組織内のネットワークを調査し、攻撃可能な機器に対しランサムウェアを配布する。(図 1-3)。

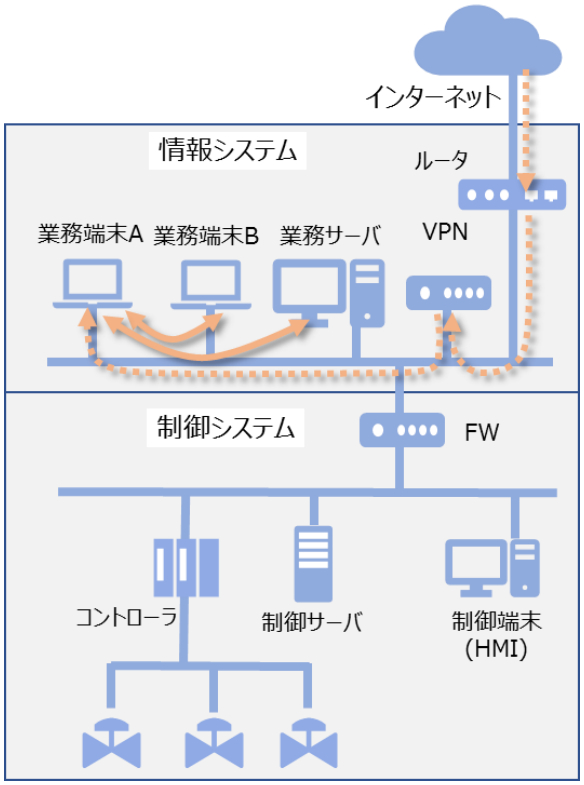


図 1-3 ネットワーク内部の調査

1.2.3【攻撃局面 A3】 機密情報の窃取

ネットワーク内部の調査により判明した機密情報を組織内部から外部へと運び出す（図 1-5）。

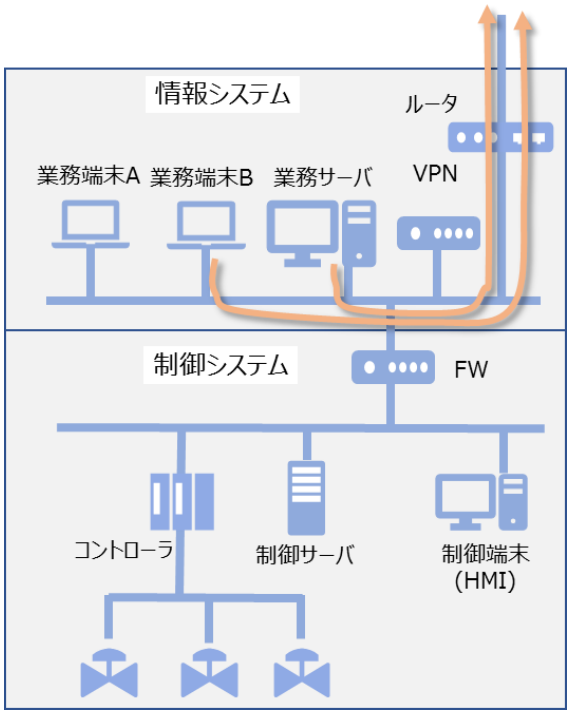


図 1-4 機密情報の窃取

1.2.4【攻撃局面 A4】コンピュータの暗号化

機密情報を窃取後、配布したランサムウェアによりコンピュータを暗号化し情報ネットワークを機能不全に陥れる(図 1-5)。

本インシデントでは、ランサムウェアの制御系への侵入は無かったという調査結果が出ている[9]。

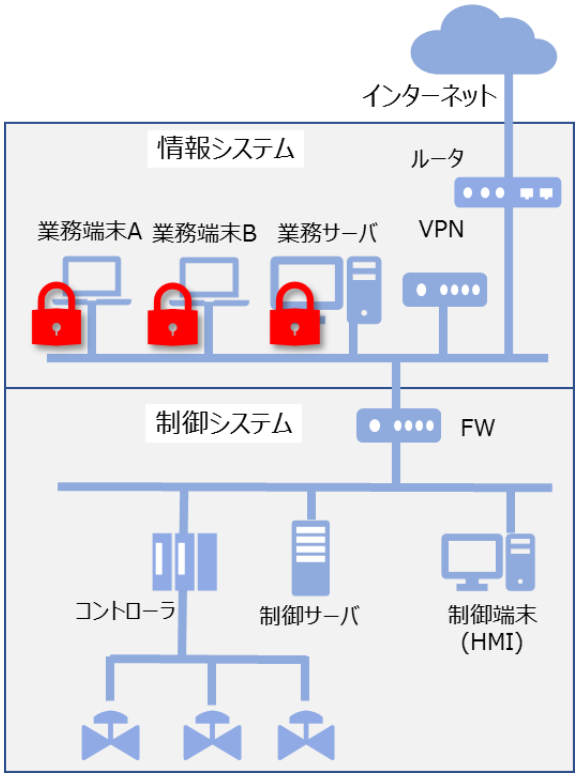


図 1-5 機密情報の窃取

1.2.5【攻撃局面 A5】 制御システムの停止

情報ネットワークがサイバー攻撃を受けたことが判明した時点で、現場担当者が制御システムへのランサムウェアによる被害拡大を懸念して制御システムを停止する。
この判断は、全社的なインシデント対応プロセスに沿った手順だったと上院公聴会資料【1】に記録されている。

この制御システムの稼働停止により、顧客への燃料の供給がストップし、最終的に市場に燃料が枯渇することになった。(図 1-6)

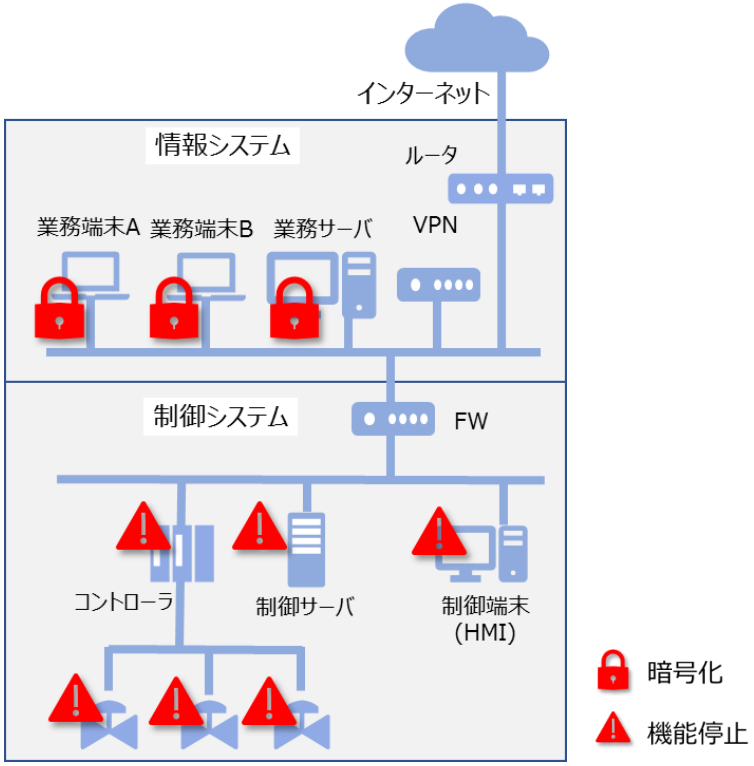


図 1-6 制御システムの停止

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	燃料の供給停止			
	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
	パイプラインの制御システムがランサムウェアの被害を受け、あるいは被害を受ける可能性が高くなり制御システムをシャットダウンし、石油の供給が停止される。	制御サーバ	コントローラ	コントローラの制御停止

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	*悪意ある外部者*	VPN 装置		制御サーバ	コントローラ	コントローラの制御停止

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 ＜情報システムをランサムウェアにより暗号化することにより、制御システムの稼働を停止する。＞
【A1】	S1	侵入口= VPN 装置 VPN の正規のパスワードを利用し、組織内へ侵入する
【A2】	S2	業務端末 A から組織内ネットワークを探索し、機密情報を探し出すと同時に、攻撃範囲を広げる調査をおこなう
【A3】	S3	探し出した機密情報を、組織外部へと運び出す
【A4】	S4	攻撃対象とした組織内の情報ネットワークのコンピュータにランサムウェアを送り暗号化する
【A5】	S5	制御システムへのランサムウェアの被害拡大を防ぐため、現場担当者が制御システムをシャットダウンする

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	VPN 装置
	攻撃対象	コントローラ
	攻撃拠点	制御サーバ
	経由	
攻撃者		悪意ある外部者
事業被害		燃料の供給停止
攻撃シナリオ		ランサムウェアによる情報システムの稼働停止
最終攻撃（目的）		制御システムの停止
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		不正アクセス ネットワーク上のコンピュータのスキャン ランサムウェアの配布と暗号化

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、本資料でも参照している ICS-CERT から公表された、Alert AA21-131A[4]『DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks』[10]、CIS から公表されている『Security Primer – Ransomware』[11]、IPA から公開されている『事業継続を脅かす新たなランサムウェア攻撃について』[12]を例に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。
特に、標的型ランサムウェア攻撃（二重の脅迫）の対策・緩和策は大きく以下の 3 種類に分類できる。

① 入口対策（防御と検知）[13]
② 内部対策（防御と検知、出口対策を含む）[13]
③ 対応・復旧

表 2-5 に、代表的な対策・緩和策をまとめる。

表 2-5 代表的な対策・緩和策の例

項番	対策・緩和策	分類
D1	多要素認証の使用[10][12]	①②
D2	リモートデスクトッププロトコルの制限[10][11]	①
D3	フィッシングメール、標的型メールへの対策[10][11][12]	①
D4	制御ネットワークや情報系重要資産のネットワーク分離・防御強化 [10]	②
D5	プログラムの不正実行の防止[10][11]	②
D6	定期的なバックアップと確実なリストアの確認[10][11][12]	③
D7	ユーザアカウントとプロセスアカウントの制限[10]	①②
D8	感染したシステムの分離[10]	③
D9	攻撃対象領域(attack surface)の最小化[12]	②
D10	脆弱性対策[11][12]	①②
D11	エンドポイント・内部ネットワーク監視[11][12]	②
D12	強力なパスワードを使用し更新をおこなう[11]	①②

[4] 本件に対する Alert ではないが US-CERT では 2020 年にパイプラインのランサムウェア対応に関しての文書、AA20-049A ” Ransomware Impacting Pipeline Operations”という Alert も公開している。関連企業ではこちらも参照することを勧める。

「D1. **多要素認証の使用**」 OS や VPN、リモートソフトのログイン方法として多要素認証を使うことで安全性を高める。

「D2. **リモートデスクトッププロトコルの制限**」 RDP[5]が必要な場合は、IP アドレスのホワイトリストなどの通信制限をおこなう。

「D3. **フィッシングメールへの対策**」 電子メールゲートウェイにフィルタを設け、同時にユーザが不審なメールの添付ファイルの開封やリンクへのアクセスをしないように教育をおこなう。

「D4. **制御ネットワークや情報系重要資産のネットワーク分離・防御強化**」 インターネットや情報システムと制御ネットワークや制御システムの稼働に大きな影響を与える資産の境界にはルータやファイアウォールの設置、IPA,IDS の設置、通信プロトコルや通信相手の制限などをおこない外部との通信を遮断するなど保護する。

「D5. **プログラムの不正実行の防止**」 メール添付されたドキュメントのマクロの実行の禁止、管理ツールとして一般的に利用されている PowerShell の実行を署名付きスクリプトや信頼できるスクリプトに制限する。

「D6. **定期的なバックアップと確実なリストアの確認**」 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。DarkSide ランサムウェアの様にネットワーク共有されているデータも暗号化するものもあるため[7]、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 。

「D7. **ユーザアカウントとプロセスアカウントの制限**」 アカウント使用ポリシー、ユーザアカウントを管理してアクセス権の制限を設定する。

「D8 **感染したシステムの分離**」 感染したシステムをすべてのネットワークから削除し、WiFi、Bluetooth といった無線接続についても分離されている事を確認する。

「D9 **攻撃対象領域(attack surface)の最小化**」 インターネットからアクセス可能な、あるいは意図的に公開するサーバやネットワーク機器を最小限にするとともに、アクセス可能なプロトコルやサービスも最低限にする。また、本件では、情報システム管理部門で把握されていない VPN 装置が発端となったとされている。このような機器の適切な管理も必要となる。

---

[5] Remote Desktop Protocol:サーバ側コンピュータの画面をクライアントに転送して表示や操作を行うリモートデスクトップのためのプロトコル

「D10 脆弱性対策」 OS、利用するソフトウェア、VPN 装置を含むネットワーク機器のファームウェアを最新の状態に保つ。

「D11 エンドポイント・内部ネットワーク監視」 攻撃者による侵害範囲拡大を検知・防御するため統合ログ管理、ネットワーク監視、エンドポイント監視といった仕組みを取り入れる事を検討する。

「D12 強力なパスワードを使用し更新をおこなう」 簡単に推測できないパスワードを利用し、ユーザやコンピュータ毎に異なるパスワードを利用する。本インシデントでは、パスワード自体は簡単に推測できない複雑なものだったものの、過去に漏えいしていたパスワードを再利用していたと報告されている【9】。

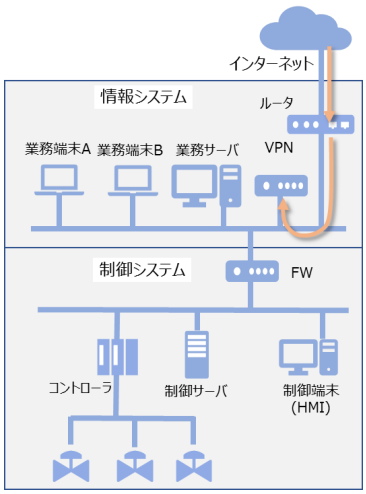
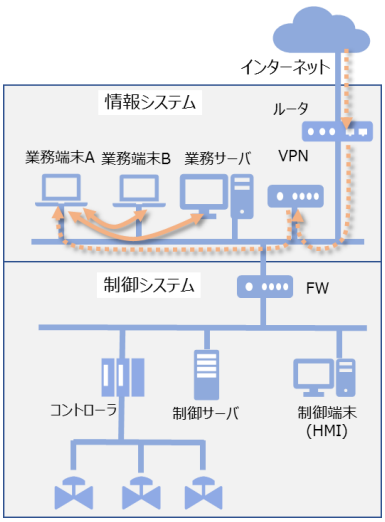
【コラム】DarkSide だけではないパイプライン関連のサイバー攻撃

攻撃グループ DarkSide が 2021 年 5 月に Colonial Pipeline へのサイバー攻撃を行ったのちに活動を停止したと報じられているが[14]、パイプラインに関連するサイバー攻撃は DarkSide 以外にも行われている。2021 年 4 月の下旬には、が Xing Team と呼ばれる集団が LineStarIntegrity Services 社に対してランサムウェアによるサイバー攻撃を行い、70GB の電子メールやプログラム、人材情報等の機密情報が窃取され公開された。同社はパイプラインを中心とした産業用制御システムのサービス会社で、窃取された情報の精査はされていないものの、パイプラインに関する顧客の情報技術や産業用システムを構成するソフトウェアも含まれていて、次のターゲットのための資料となるのではと懸念されている。[15]

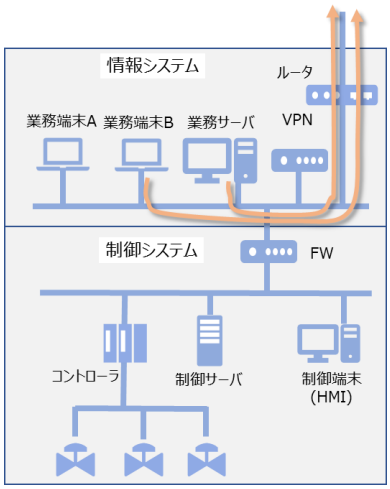
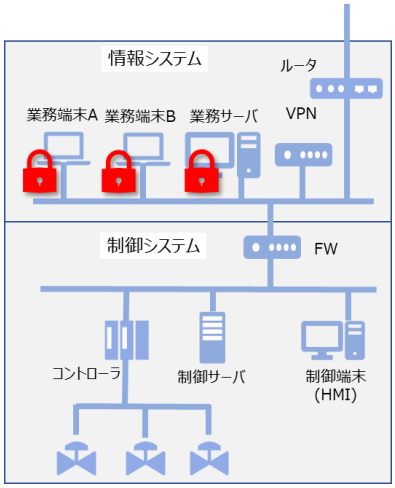
2.5. 攻撃ステップと対策・緩和策の関連付け

2.3 節までの情報をもとに、【攻撃局面 A1～A5】の代表的な対策・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。

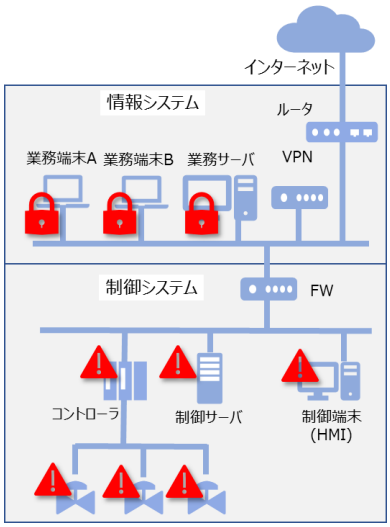
表 2-6 制御システムにおける攻撃ステップと対策・緩和策の紐づけ例

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]対象組織への不正侵入	・フィッシングメール、標的型メールへの対策[D3] ・多要素認証の使用{D1} ・リモートデスクトッププロトコルの制限[D2] ・攻撃対象領域(attack surface)の最小化「D9」 ・脆弱性対策[D10] ・強力なパスワードを使用し更新をおこなう[D12]	・ファイアウォール
【攻撃局面 A2】  	[S2] ネットワーク内部の調査	・プログラムの不正実行の防止[D5] ・ユーザアカウントとプロセスアカウントの制限[D7] ・脆弱性対策[D10] ・エンドポイント・内部ネットワーク監視[D11]	・事務用 PC

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 A3】  	[S3] 機密情報の窃取	•多要素認証の使用[D1] •プログラムの不正実行の防止[D5] •ユーザアカウントとプロセスアカウントの制限[D7] •エンドポイント・内部ネットワーク監視[D11]	•操作端末 •データサーバ •SCADA
【攻撃局面 A4】  	[S4] コンピュータの暗号化	•定期的なバックアップと確実なリストアの確認[D6] •感染したシステムの分離[D8] •エンドポイント・内部ネットワーク監視[D11]	・操作端末

[7] [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[8]	・対策・緩和策	対象システム・資産
【攻撃局面 A5】  	[S4] 制御システムの停止	•制御ネットワークや情報系重要資産のネットワーク分離・防御強化[D4] •感染したシステムの分離[D8]	・SCADA

8 [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] [上院公聴会資料]: Hearing before the United States Senate Committee on Homeland Security & Governmental Affairs: 2021/06/08
https://www.hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf

[2] [CNN]: 米首都のガソリンスタンド、8割が売り切れ パイプライン停止の影響続く
https://www.cnn.co.jp/business/35170841.html

[3] [情報処理推進機構]:【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について
https://www.ipa.go.jp/security/announce/2020-ransom.html

[4] [BBC]: 米石油パイプラインにサイバー攻撃、燃料不足の懸念 データ「人質」の犯罪集団
https://www.bbc.com/japanese/57052827

[5] [FBI]: Statement on Compromise of Colonial Pipeline Networks
https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks

[6] [日本経済新聞]: 「ダークサイド」の正体 3 つの意味と 4 重の脅迫
https://www.nikkei.com/article/DGXZQOUC203IC0Q1A520C2000000/

[7] [FireEye ブログ]: DARKSIDE ランサムウェア・オペレーションのヒント
https://www.fireeye.com/blog/jp-threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

[8] [Bank info security]: Colonial CEO at Senate Hearing Details Ransomware Attack
https://www.bankinfosecurity.com/colonial-ceo-at-senate-hearing-details-ransomware-attack-a-16836

[9] [Bloomberg]: Hackers Breached Colonial Pipeline Using Compromised Password
https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[10] [ICS-CERT]: Alert AA21-131A “DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks”

https://us-cert.cisa.gov/ncas/alerts/aa21-131a

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

[12] [情報処理推進機構]:【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について
https://www.ipa.go.jp/security/announce/2020-ransom.html

[13] [情報処理推進機構]:「高度標的型攻撃」対策に向けたシステム設計ガイド
https://www.ipa.go.jp/files/000046236.pdf

[14] [Wall Street Journal] Colonial Pipeline Hacker DarkSide Says It Will Shut Operations
https://www.wsj.com/articles/web-site-of-darkside-hacking-group-linked-to-colonial-pipeline-attack-is-down-11621001688

[15] [Pipeline Technology Journal] Yet Another Pipeline Company Targeted By Cyber Criminals
https://www.pipeline-journal.net/news/yet-another-pipeline-company-targeted-cyber-criminals

更 新 履 歴

2021 年 10 月 18 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 9

～2021 年　米国最大手のパイプラインのランサムウェア被害～

[発　　行]　2021 年 10 月 18 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