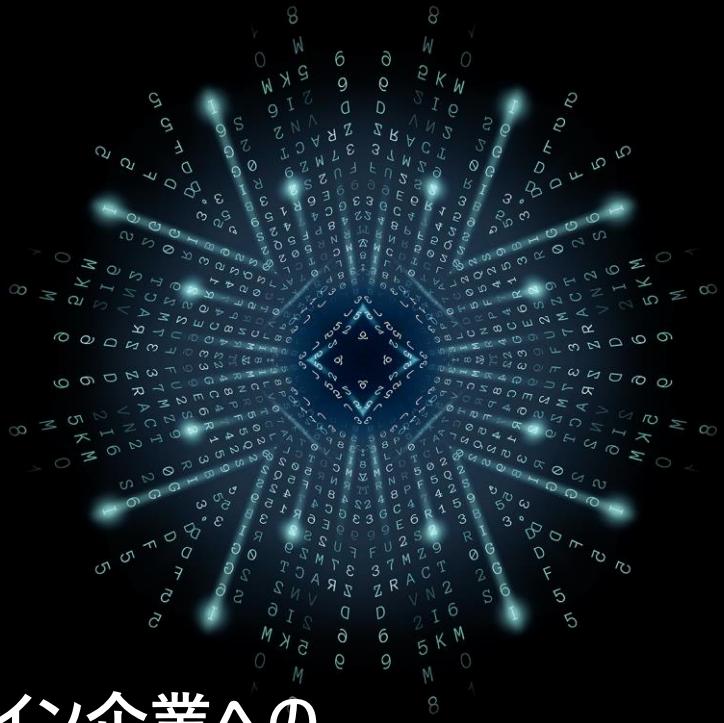
Deloitte.
デロイト トーマツ



米国大手石油パイプライン企業へのサイバー攻撃まとめ

デロイト トーマツ グループ

2021年5月31日作成
2021年6月17日改定

目次

改定履歴

2021年5月31日	初版作成
2021年6月17日	米国大手石油パイプライン企業の公表情報以外の情報、および本資料作成後の情報を追加

インシデントの概要

2021年5月7日（金）、米国大手石油パイプライン企業は、ランサムウェア攻撃の被害に遭い、脅威を抑えるために特定のシステムをオフラインにし、すべてのパイプラインの操業を予防措置として停止した。

パイプラインの操業停止は、アラバマ州、アーカンソー州、コロンビア特別区、デラウェア州、フロリダ州、ジョージア州、ケンタッキー州、ルイジアナ州、メリーランド州、ミシシッピ州、ニュージャージー州、ニューヨーク州、ノースカロライナ州、ペンシルバニア州、サウスカロライナ州、テネシー州、テキサス州、バージニア州など、米国東海岸の複数の州に影響を与えた。

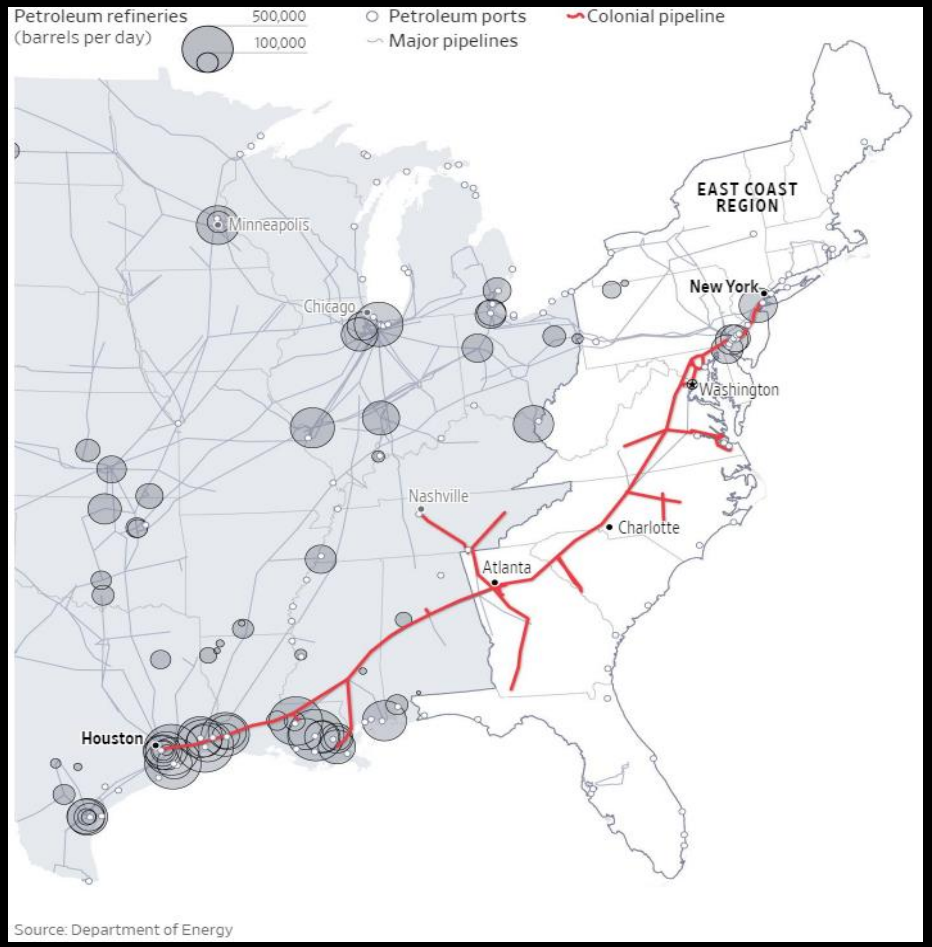
米国大手石油パイプライン企業は、米国東部から南部にかけて燃料輸送を行う大規模なパイプラインを運営している企業です

米国大手石油パイプライン企業の概要

Pipeline Company

- メキシコ湾岸の製油所から米国南部および東部の顧客に燃料を運ぶ5,500マイルのパイプラインを運営
- 東海岸の軽油、ガソリン、ジェット燃料の供給量の45％に相当する日量250万バレルを輸送
  - 輸送量：250万バレル／日
  - パイプラインの延長距離：5,500マイル
  - 接続される石油精製施設：29施設
  - 接続される顧客のターミナル：267ターミナル
  - パイプラインの移動速度：5マイル／時
  - 供給する大きな都市： 8 都市
  - 供給する主要空港： 7 空港
  - 供給する軍施設： 5 施設

米国大手石油パイプライン企業のパイプライン



https://www.wsj.com/articles/why-the-colonial-pipeline-shutdown-is-causing-gasoline-shortages-11620898203?mod=searchresults_pos6&page=1

米国大手石油パイプライン企業は、5月8日から継続的にインシデントを公表しており、ランサムウェアに対する身代金を支払っています

米国大手石油パイプライン企業等の事故経緯（1/2）

※は米国大手石油石油パイプライン企業の公表以外の情報

4月29日※	攻撃者は**多要素認証がない当該企業のVPNにログイン**し、企業ネットワークに従業員のアカウントを使って侵入。アカウントの認証情報の入手については不明。（Mandiant社調査）
5月7日5時前※	攻撃者からの身代金請求書を発見。CEOはパイプラインを停止する全社的な事故対応プロセスを指示し、同日6時10分にパイプライン全体が停止（6月8日公聴会）
5月7日※	5月7日以降、攻撃者が侵入して、ネットワークの探索活動や攻撃活動を行った形跡はなかった。また、**パイプラインを制御するコンピュータシステムに侵入した形跡はなかった**（Mandiant社調査）
5月8日※	身代金の支払い（6月8日公聴会）
5月8日12:30	ランサムウェア攻撃により**ITシステムに影響が出ており、パイプラインの操業を停止**したとの最初の報道発表。法執行機関や連邦機関へ連絡。第三者のサイバーセキュリティ企業に依頼し、調査
5月9日17:10	ランサムウェア攻撃に関する2回目の報道発表。継続調査中。パイプラインの安全性の維持、安全なシステム復旧が最優先。**メインラインは停止中であるが、ターミナルと配送地点にある小規模なラテラルラインは稼働中**
5月9日 ※	米国政府が地域緊急事態宣言2021-002-05-09-2021を発出。影響を受けた18州にガソリン、ディーゼル、ジェット燃料、その他の石油精製品を輸送者に対して、一時的に時間外労働を認める
5月10日12:25	復旧のために膨大なリソースを投入。**エネルギー省と協議し、段階的に復旧。今週末までに操業を再開することを目標。すべてのシステムをスキャンして、マルウェアの可能性や侵害の兆候がないことを調査**
5月10日※	米国FBIはDarkSideと呼称されるランサムウェアが今回の犯行に使われたと公表

https://www.otisac.org/ot-isac-resources
https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption

米国大手石油パイプライン企業は、法執行機関へ早期に通知し、対応を行い、盗取情報の国外持出しの未然防止、身代金の回収が行われました

米国大手石油パイプライン企業等の事故経緯（2/2）

※は米国大手石油石油パイプライン企業の公表以外の情報

5月10日19:55	第三者サイバーセキュリティ専門家、法執行機関、連邦機関と連携して復旧の作業を実施中。**ノースカロライナ州からミズーリ州までのパイプラインは在庫に限って、手動で稼働中**
5月11日17:15	パイプラインを再稼働に向けて人手により点検中
5月12日17:10	17時ころ、**パイプラインの操業を再開。通常業務に戻るまで数日を要する**見込み
5月13日09:00	**サービス提供先への供給が再開**。13日正午ころに各供給先で製品が受領できる見込み
5月13日16:40	**パイプラインシステム全体で再開**。輸送に関わるサプライチェーン全体が正常に戻るまで数日かかる見込み
5月13日※	DarkSideが米国からの圧力を理由に、RaaSプログラムの活動を停止したことをセキュリティ研究者らが報告
5月19日※	WSJ誌に米国大手石油パイプライン企業CEOが**ハッカーに身代金を支払った**理由を語る
6月7日※	身代金として支払われたデジタル通貨75ビットコイン（約440万ドル）のうち、約64ビットコイン（約230万ドル）を司法省が回収したことを公表
6月8日※	CEOが米国上院国土安全保障委員会の公聴会に出席。現在も一部のシステムの復旧および調査を継続 重要インフラ・OTセキュリティの専門家であるDragos社およびBlack Hills Information Security社を起用し、サイバー防御の強化
6月9日※	CEOが米国下院国土安全保障委員会の公聴会に出席

https://www.otisac.org/ot-isac-resources
https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption

米国大手石油パイプライン企業は、停止によるリスクと復旧にかかる時間を考慮し、身代金を支払いましたが、司法省により一部回収されました

パイプライン停止の影響、身代金支払い判断と身代金の追跡

パイプラインの停止による影響

- 米国大手石油パイプライン企業は、アトランタ空港、テネシー州ナッシュビル、ボルチモア・ワシントン、ノースカロライナ州シャーロット、ローリー・ダーハムなどの空港を含む複数の州の重要な産業やサービスに供給されており、**閉鎖期間によっては、一部の小規模空港でジェット燃料が不足**する可能性がある
- 主要パイプラインの閉鎖により、ガソリンの価格が上昇
- 東海岸の一部において、ガソリン不足が生じ、ガソリンスタンドの燃料が枯渇

身代金(440万ドル)支払いの経営判断理由

（米国大手石油パイプライン企業はサイバー保険に加入しているが、詳細は言及なし）

- サイバー攻撃によるシステム侵害の程度が不明であったため、**パイプラインの復旧にどれくらい時間がかかるかわからない**
- **重要なエネルギーインフラ停止に伴うリスクの評価**をした結果
- 政府からの勧告によるものではない

身代金の追跡

- 攻撃者が侵入し、ランサムウェアを展開し、企業のデータをロックし、システムを麻痺させる
- 被害者はデータロックを解除するためのツールの代金を要求するメッセージを受け取る
  攻撃者は、被害者が**暗号通貨を預けられるデジタルウォレットのアドレスを共有**する
- 被害者は、サイバーセキュリティ企業に電話して、ハッカーとの交渉などを行う。ブローカーは**現金を暗号通貨に換金し、送金**をする
- 攻撃者は活動を偽装、またはハッキングに参加した仲間への支払いのため、**ウォレット間で資金を移動**させる。攻撃者は、海外の**暗号通貨取引所で、暗号通貨を米ドルなどの現金に換金**する

攻撃者グループDarkSideはロシア系のRaaSグループとされており、窃取したデータを自組織の脅迫用Webサイトで公開するとして身代金を要求します

攻撃者グループDarkSideとは

DarkSideは、独自ブランドの不正プログラムをサブスクリプションベースで提供する「Ransomeware-as-a-Service(RaaS)」グループ

- ✓ ロシア語を話すチームとみられる
- ✓ 調査を進めるセキュリティ企業は、現在RaaSプラットフォームを活用する他のアフィリエイト5組織を特定済み

DarkSideは二重脅迫キャンペーン用のWebサイトであるエクストーションサイト「DarkSide Leaks」も運用

- ✓ 被害企業が支払いを拒絶した場合は窃取したデータが公開される仕組みを採用
- ✓ 交渉相手は被害企業だけでなく、状況に応じてその競合他社やステークホルダーにも交渉の手を伸ばす

同グループは今回のインシデントに対し、「目的は金銭であり、政治に関心はない」とする声明も発表

DarkSideの一般的な侵入手段

- フィッシングにより、企業のネットワークにアクセス
- リモートでアクセス可能なアカウントやシステム、VDI (Virtual Desktop Infrastructure)を悪用
- リモート・デスクトップ・プロトコル(RDP)を使用し、コマンド&コントロールにThe Onion Router(TOR)を使用してアクセスを維持、有効な認証情報を窃取して横展開や追加攻撃に悪用
- アクセス権を獲得したのち、ITネットワークに対してDarkSideランサムウェアを展開
  - ✓ 機密データを窃取し、システムを「Salsa20」および「RSA-1024」プロトコルで暗号化
  - ✓ エンコードされPowerShellコマンドでボリュームシャドウコピー（ある時点でのWindows内のデータのコピー）を削除
- 身代金を要求

DarkSideのような攻撃に備え、FBI等が公表した緩和策がとられているか、今一度確認が求められます

FBI等が公表した緩和策

不正侵入の予防

- ✓ OTおよびITネットワークへのリモートアクセスには多要素認証を必須とする
- ✓ フィッシングメールおよび実行可能ファイルを含む電子メールがエンドユーザに届かないようにする
- ✓ ユーザーが悪意のあるウェブサイトにアクセスしたり、悪意のある添付ファイルを開いたりしないようにするため、ユーザートレーニングプログラムやスピアフィッシングの模擬攻撃を実施し、ユーザーの適切な対応を再徹底させる
- ✓ ネットワークトラフィックをフィルタリングして、既知の悪意のあるIPアドレスとの通信を禁止する。URLブロックリストや許可リストを導入し、ユーザーが悪意のあるウェブサイトにアクセスできないようにする

パッチ、アンチウィルスプログラム等の適用と最新化

- ✓ ITネットワーク資産のOS、アプリケーション、ファームウェアなどのソフトウェアをタイムリーに更新する。パッチマネジメントプログラムに参加すべきOTネットワーク資産とゾーンを決定する。ネットワーク上のリソースへのアクセス、特に RDP を制限する
- ✓ アンチウイルス／アンチマルウェアプログラムを設定し、最新のシグネチャを使用してITネットワーク資産の定期的なスキャンを行う。マルウェアの存在についてOTネットワーク資産をどのように特定し評価するかを決定する

不正実行防止策の実施

- ✓ 電子メールで送信される Microsoft Office ファイルのマクロスクリプトを無効にする
- ✓ 外部からの接続が想定されていないIPアドレスやポート（VPNゲートウェイ、メールポート、Webポート以外）へのインバウンド接続を監視・遮断する

国土安全保障省はパイプライン分野の企業に対する脅威を適切に特定・防御・対応できるようにするためにセキュリティ指令を発表しました。

パイプラインの所有者・運営者に対するサイバーセキュリティ指令

対象

- ✓ 重要なパイプラインの所有者および運営者

セキュリティ要件

- ✓ 確認されたサイバーインシデントおよび潜在的なサイバーインシデントをCISAに報告すること
- ✓ 24時間365日対応可能なサイバーセキュリティコーディネータを任命すること
- ✓ サイバー関連のリスクを評価し、ギャップを特定し、関連する改善策を策定し、その結果をTSAおよびCISAに報告すること

今後の方針

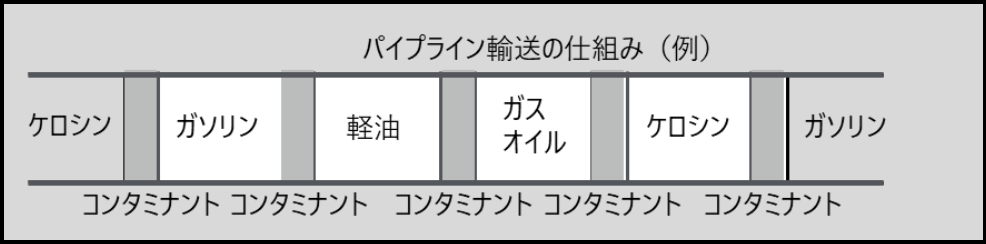
- ✓ 運輸安全局（TSA）はパイプライン業界のサイバーセキュリティ強化をさらに支援する
- ✓ 官民のパートナーシップを強化する

重要インフラ企業への攻撃に備えて：
考察とディスカッション

米国大手石油パイプライン企業のインシデントを考察するため、まずパイプライン事業の特徴とシステムに求められる要件を確認します

パイプライン事業の特徴

- 大規模なパイプラインでは、1本のパイプラインで数種類の油を輸送するのが普通であり、そのため、製品（油）の品質管理が重要になる。輸送する油種ごとに貯油タンクが必要となる
- 数油種をある定められた順序で連続的に1本のラインで輸送する方式では異種油境界面に隣接油の混合部分が生じ、これをコンタミナントと称している。このコンタミナントの処理（計測／操作）が重要となる
- 送油側よりポンプで油に圧力を加え、パイプの中に圧送すれば、パイプ内の圧力損失により、距離に比例して圧力が下がり、受油側のタンクに注入される。圧力は流速、パイプの直径、パイプの延長や標高差などによって決まる



システムに求められる要件

- 長距離に直列的な制御点
  - ✓ 製油所、ポンプステーション、着ターミナルがつながり、大きな時間遅れを持ちながら密着
- 保安管理
  - ✓ 異常予知、異常の早期検出と安全処理がパイプライン運転の前提
- 品質管理と計量管理
  - ✓ 一本のパイプでいくつかの石油会社の油を数種類ずつ輸送するため、混合物の適正処理が必要
- 情報量と遠隔伝送
  - ✓ 長距離、複雑な輸送経路のため、制御・監視点が多く、制御には密接な関連を持つため、情報量が膨大となり、なおかつ遠隔からの伝送が必要
- プラントの有効利用（スケジューリング）
  - ✓ 需要予測から綿密に長期の運転計画を立て、送油側から受油側までの到着に数日を要する
  - ✓ パイプライン中、貯油タンクの油量の制御にはスケジュール管理が重要

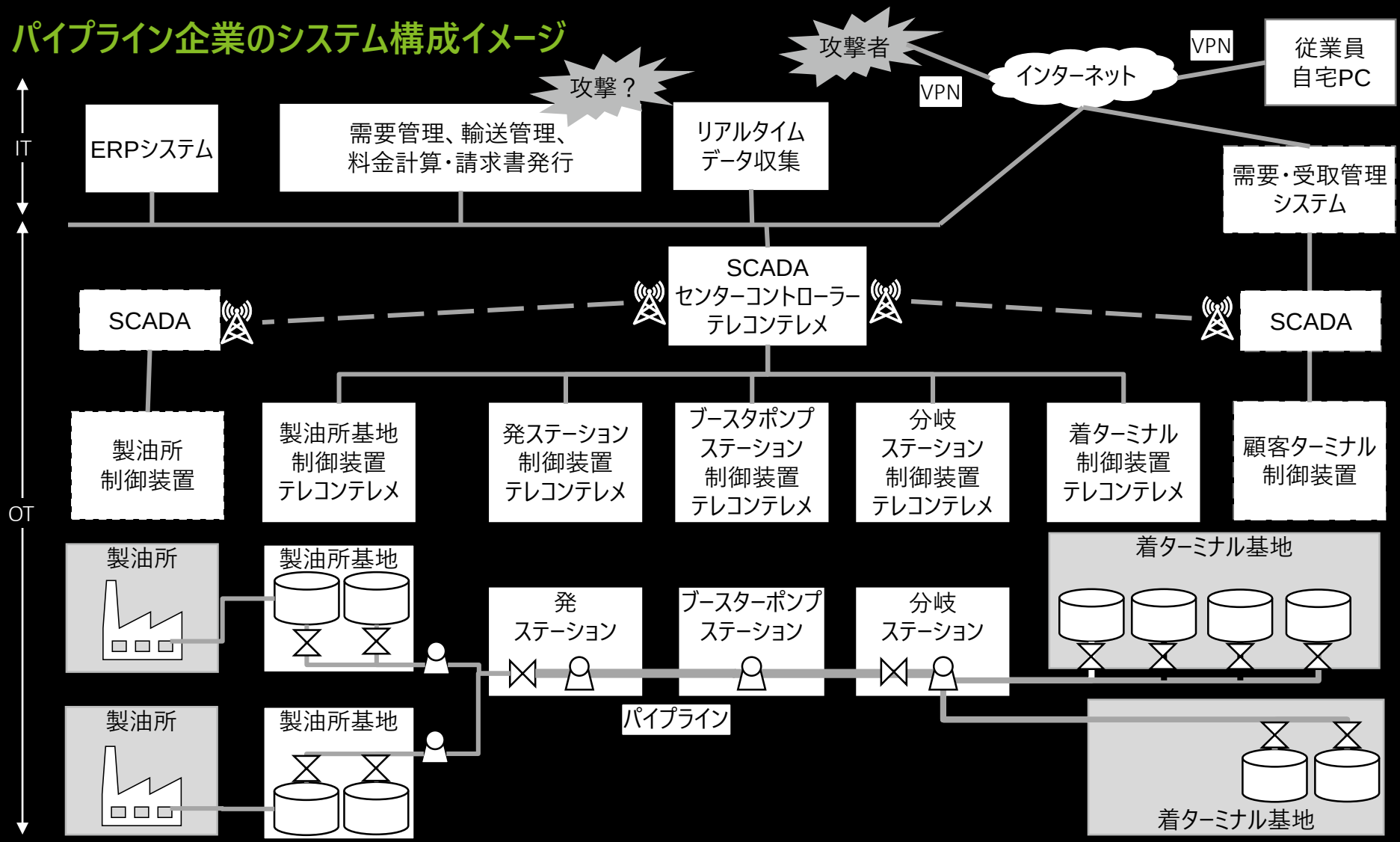
パイプラインは遠隔監視・制御がベース、かつオペレーションがITに依存しており、ITシステムの停止が設備稼働に影響してしまう結果となりました

パイプライン企業のシステム構成

- **パイプラインシステムはポンプステーション、貯蔵施設、供給・配送ステーションそして相互に接続された膨大なパイプラインで構成**
  - ✓ 上記システムは広大な地域にまたがるため、ポンプステーションや分岐ステーションでのローカル制御や部分的な自立制御に加え、パイプラインネットワーク全体をSCADA（Supervisory Control and Data Acquisition）システムおよびテレコン／テレメトリーで遠隔監視・制御
  - ✓ パイプラインは内部の操作とは別に、製油所の制御システムや顧客の貯蔵施設の制御システムと相互接続
- **パイプラインのオペレーションは製品の移動注文、測定値の補正、請求書の発行など、ITシステムに依存**
  - ✓ ERPなどのビジネスシステムは、パイプライン業務の間で統合されていることが多く、ビジネスと財務の部分に対応
  - ✓ 製品の注文データは、ITシステムからSCADAシステムへ、移動やバッチ操作等で連携
  - ✓ データはITシステムに戻され、製品の測定値の補正、在庫管理、請求書の発行、履歴管理などを実施
- **ITシステムとOTシステムは、システム的には独立しているが、ビジネス全体としては協調。OTのデジタルトランスフォーメーションの進展により、パイプライン企業にとって、ITからOTへの接続は一般的**
  - ⇒ パイプラインそのものはITシステムがなくても操業することができるが、米国大手石油パイプライン企業で起こったランサムウェアのインシデントの例の通り、ITシステムが停止した場合にはオペレーションが行えなくなり、深刻な影響を受ける

OT側が適切にセグメンテーションされていても、IT側の複数システムが停止したことにより、全体のオペレーションが不能になった可能性があります

パイプライン企業のシステム構成イメージ



ディスカッション①：設備自体の制御システムは独立していても、その業務オペレーションの根幹をIT側のシステムが担っている可能性はないでしょうか

設備・システム構成に関するディスカッション

- ✓ ITシステムによって需要家からの注文により発電/ガス製造計画を立案し、SCADA側に計画情報を流し、メータの実績値を送配電会社/導管部門経由で収集し、需要家に請求するような仕組みはありますか？
- ✓ 将来的に、蓄電池への電力提供のための需給計画管理などをITシステムで行う可能性はあるでしょうか？
- ✓ 現状、OT側のシステムはセグメンテーション化した上で階層防御（縦階層に区切った対策）がとられていると思いますが、IT側のレイヤーにおいても、FWやIPS/IDSを入れる、DMZを設ける等、セグメンテーション化した上での対策（横に区切った対策）を取る必要はないでしょうか？

デロイトの考察：

電力・ガスの場合、系統運用・中央制御/給電指令所が機能していれば、社内ITシステムが一部停止したとしても、電力やガスの供給停止には至らない

また、パイプライン企業と同様にLNG等のエネルギー輸送はあるものの、1本のパイプラインで複数種類の油を輸送するパイプラインとはコントロールレベルが異なるため、万が一システムによる制御が十分機能しなくなった場合においても、手動対応がある程度可能なものと思料

但し、将来的なITシステムによる需給計画管理の可能性等を考慮した場合、ITシステム側のセグメンテーション化による対策も必要になる可能性

ディスカッション②：今回のインシデントに対し、FBI等が提示している緩和策が貴社内においても徹底されているでしょうか

FBI等が提示している緩和策(抜粋)実施状況に関するディスカッション

- **リモートアクセス**
  - ⇒ OT環境においてはリモートアクセス環境は取られていないものと思いますが、唯一あり得るものとして「ベンダーのリモートメンテナンス」があります。こちらは多要素認証の仕組みが取られているでしょうか？
- **トレーニングプログラムやスピアフィッシングの模擬攻撃を通じたユーザーへの対応再徹底**
  - ⇒ OTに関わる担当者にトレーニングや演習は徹底されているでしょうか？
- **アンチウィルスプログラム・パッチの適用と最新化**
  - ⇒ OT環境について、パッチ適用対象が明確になっているでしょうか？（資産管理・構成管理・ゾーニング）
- **ITネットワーク資産の定期的なスキャン、OTネットワーク資産のマルウェア確認**
  - ⇒ OT環境について、定検などの機会でマルウェア混入有無のチェックを実施しているでしょうか？また、実施するルールとしてベンダー等に指示しているでしょうか？（現場の規程類へのセキュリティ対策の埋め込み、重要資産に対するインシデント対応手順書：PlayBook（いつ、だれが、どのように対応すべきかを定めた文書）の策定）

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市以上に1万名を超える専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務およびこれらに関連するプロフェッショナルサービスの分野で世界最大級の規模を有し、150を超える国・地域にわたるメンバーファームや関係法人のグローバルネットワーク（総称して“デロイトネットワーク”）を通じFortune Global 500®の8割の企業に対してサービスを提供しています。“Making an impact that matters”を自らの使命とするデロイトの約312,000名の専門家については、（www.deloitte.com）をご覧ください。

IS 669126 / ISO 27001