注目されているセキュリティ事故・事件に関する情報 ＜2021年9月版 (第38号)＞(選り抜き版)

2021年9月28日
ＮＴＴデータ先端技術株式会社
セキュリティ事業本部

今回のサマリー

Colonial Pipelineへのランサムウェア攻撃
2021年5月7日、米国でパイプラインを運営しているColonial Pipelineはランサムウェア攻撃によって全てのパイプラインが停止し、ガソリンが不足するなどの影響が発生しました。本記事ではColonial Pipelineへのランサムウェア攻撃の概要と米国政府の対応、重要インフラのセキュリティ対策について解説します。

Colonial Pipelineへの
ランサムウェア攻撃

1. Colonial Pipelineへのサイバー攻撃事案概要

Colonial Pipelineは、米国の東海岸で空港や軍事施設などのための燃料を輸送する約8,850キロメートルにおよぶ石油パイプラインを運営しています。2021年5月7日、同社は**サイバー攻撃によって全てのパイプラインを一時停止した**と発表しました。パイプラインの一時停止によって、米国の東海岸ではガソリンのパニック買いが発生し、**供給が不足する事態**となりました。

石油パイプラインは重要なインフラであるため、米国政府機関も対応に追われました。同社へのサイバー攻撃はランサムウェア攻撃であり、FBI (連邦捜査局)の捜査によって、**DarkSideランサムウェアが使用された**と特定されました。ホワイトハウスは大統領令14028「Improving the Nation's Cybersecurity」を発令し、連邦政府のシステムのセキュリティ強化や**ソフトウェアサプライチェーンのセキュリティ対策ガイドラインの発行**などが行われました。

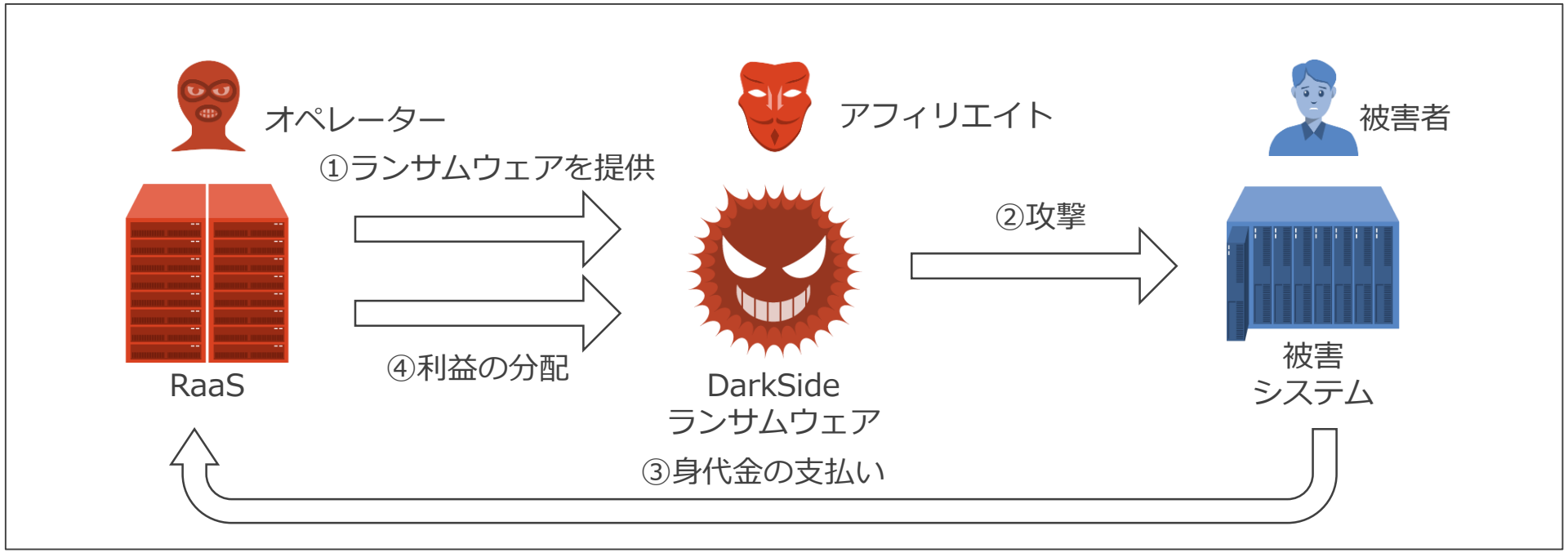
2. タイムライン

日時	出来事
2021/05/06	Colonial Pipelineがランサムウェア攻撃を受ける
2021/05/07	Colonial Pipelineが東欧の攻撃者に身代金約500万ドルを支払う
2021/05/08	Colonial Pipelineが攻撃を受け、パイプラインの操業を一時停止したと公表
2021/05/10	FBIは本件を「DarkSideランサムウェア」による攻撃と特定
2021/05/11	CISA(※1)とFBIが共同で、DarkSideランサムウェアのサイバーセキュリティアドバイザリ「Alert AA21-131A」を公開
2021/05/12	Colonial Pipelineがパイプラインの操業を再開
2021/05/12	本件を受けて米国が大統領令14028「Improving the Nation's Cybersecurity」を発令
2021/06/07	司法省はColonial Pipelineが支払った身代金のうちの約230万ドル分のビットコインを押収したと発表
2021/06/26	NIST(※2)が大統領令14028に従い「重要なソフトウェア」の定義を発表
2021/07/11	NISTが大統領令14028に従い、重要なソフトウェアのセキュリティ対策ガイダンスを発表

※1 Cybersecurity and Infrastructure Security Agency サイバーセキュリティ・インフラストラクチャセキュリティ庁。
米国土安全保障省(DHS)配下の組織
※2 National Institute of Standards and Technologyアメリカ国立標準技術研究所。
米国商務省(DoC)配下の組織。

3. DarkSideランサムウェア

本件の攻撃で使用されたDarkSideランサムウェアは「RaaS(Ransomware as a Service)」と呼ばれ、クラウドサービスのようにランサムウェアの機能を提供する「オペレーター」と、それを利用して標的を攻撃する「アフィリエイト」が存在する攻撃の形態です。RaaSによる被害者から支払われた身代金は、オペレーターとアフィリエイトで利益を分配する課金形態を採用しています。



4. 米国政府機関の対応 (1/3)

本事案を受けて、米国ホワイトハウスは2021年5月12日に**大統領令14028**を発令しました。大統領令14028では**サイバーセキュリティに関す各省庁の下部組織(CISA、FBI、NIST)に対して連携した対応**を指示しています。

大統領令14028「Improving the Nation's Cybersecurity」

1. 国家のサイバーセキュリティの改善に関する方針
2. 脅威情報の共有 (CISAとFBIへ指示)
   - 連邦政府システムのインシデント対応を実施するITおよびOTのサービスプロバイダとの契約
   - サービスプロバイダとCISAおよびFBIとの脅威情報の共有
3. 連邦政府のサイバーセキュリティの近代化 (CISAとNISTへ指示)
   - クラウドテクノロジーの採用と使用
   - ゼロトラストアーキテクチャの実装計画の作成
4. ソフトウェアサプライチェーンのセキュリティの強化 (NISTへ指示)
   - ※次スライドで解説
5. サイバー安全審査委員会の設置(国土安全保障省へ指示)
   - 委員会のメンバーはCISA、NSA、FBIの代表者および国土安全保障省長官によって決定された民間のサイバーセキュリティの代表者で構成
6. 脆弱性とインシデントに対応するための連邦政府のプレイブックの標準化 (CISAとNISTへ指示)
7. 連邦政府ネットワークにおけるサイバーセキュリティの脆弱性とインシデントの検出の改善 (CISAへ指示)
8. 連邦政府システムの調査および修復機能の改善 (CISAとFBIへ指示)
9. 国家安全保障システム
10. 定義

参考：Executive Order on Improving the Nation's Cybersecurity
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

4. 米国政府機関の対応 (2/3)

大統領令14028の4章では、NISTに対して産学官民からから意見を募り、**ソフトウェアのサプライチェーンのセキュリティを強化するための基準やツール、ベストプラクティスなどを整理・開発する**ことを指示しています。

NISTは大統領令14028の専用サイトを公開し、2021年6月26日に「**重要なソフトウェア**」を定義するホワイトペーパーを公開しました。ホワイトペーパーには重要なソフトウェアの定義だけでなく、重要なソフトウェアに該当する具体的な製品分類のリストが含まれています。

「重要なソフトウェア」の定義

- 権限を昇格させるか管理権限で動作するように設計されているもの
- ネットワークや計算機資源に直接または特権でアクセス可能なもの
- データや運用技術へのアクセスを制御するように設計されているもの
- 信頼に不可欠な機能を実行しているもの
- 通常の信頼の境界外で特権アクセスで動作するもの

参考：Critical Software - Definition & Explanatory Material
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory

4. 米国政府機関の対応 (3/3)

2021年5月11日にCISAとFBIは共同で、サイバーセキュリティアドバイザリ「Alert AA21-131A」を公開しました。AA21-131Aには、**DarkSideランサムウェア攻撃からビジネスを守るための対策**が記載されています。

DarkSideランサムウェア攻撃からビジネスを守るための対策

- OTおよびITネットワークへのリモートアクセスに多要素認証の使用
- フィッシングメールや実行ファイルを含むメールのフィルタリング
- ユーザに対するフィッシング攻撃の訓練の実施
- ブラックリストに対するネットワークトラフィックのフィルタリング
- ソフトウェアやファームウェアの迅速なアップデート
- RDPによるネットワーク経由のシステムへのアクセス制限
- マルウェア対策プログラムによる定期的なスキャン
- 不正実行の防止
  - メールに添付されたMicrosoft Officeのマクロの無効化
  - アプリケーションの許可リストの実装
  - Torなどの匿名化サービスから、外部からの接続を想定していない内部ネットワークへの接続の監視およびブロック

参考：Alert (AA21-131A)
DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks
https://us-cert.cisa.gov/ncas/alerts/aa21-131a

5. 参考：日本における重要インフラのセキュリティ対策の取り組み

日本では、NISCの重要インフラグループによる「サイバーセキュリティ戦略」と「重要インフラの情報セキュリティ対策に係る第4次行動計画(改定)」に基づいて、重要インフラの各分野はセキュリティガイドラインを策定しています。また、IPAは「制御システムのセキュリティリスク分析ガイド 第2版」をリスク分析シートとチェックリストと共に公開しています。

調査対象一覧（全14分野26件）

NISC

分野		安全基準等の名称
情報通信	電気通信	・事業用電気通信設備規則 ・情報通信ネットワーク安全・信頼性基準 ・電気通信分野における情報セキュリティ確保に係る安全基準（第4.1版）
	放送	・放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン ・放送設備サイバー攻撃対策ガイドライン
	ケーブルテレビ	・ケーブルテレビの情報セキュリティ確保に係る「安全基準等」策定ガイドライン ・電気通信分野における情報セキュリティ確保に係る安全基準（第4.1版） ※再掲 ・放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン ※再掲
金融	銀行等 生命保険 損害保険 証券	・金融機関等におけるセキュリティポリシー策定のための手引書 ・金融機関等コンピュータシステムの安全対策基準・解説書 ・金融機関等におけるコンティンジェンシープラン策定のための手引書
航空		・航空分野における情報セキュリティ確保に係る安全ガイドライン（第５版）
空港		・空港分野における情報セキュリティ確保に係る安全ガイドライン（第２版）
鉄道		・鉄道分野における情報セキュリティ確保に係る安全ガイドライン（第４版）
電力		・電気事業法施行規則第50条第２項の解釈適用に当たっての考え方 ・電気設備の技術基準の解釈 ・電力制御システムセキュリティガイドライン ・スマートメーターシステムセキュリティガイドライン
ガス		・都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説
政府・行政サービス		・地方公共団体における情報セキュリティポリシーに関するガイドライン
医療		・医療情報システムの安全管理に関するガイドライン（第5.1版）
水道		・水道分野における情報セキュリティガイドライン（第４版）
物流		・物流分野における情報セキュリティ確保に係る安全ガイドライン（第４版）
化学		・石油化学分野における情報セキュリティ確保に係る安全基準
クレジット		・クレジットCEPTOARにおける情報セキュリティガイドライン
石油		・石油分野における情報セキュリティ確保に係る安全ガイドライン

2

NISC 重要インフラにおける安全基準等の継続的改善状況等に関する調査について
https://www.nisc.go.jp/active/infra/pdf/keizoku20.pdf

IPA 制御システムのセキュリティリスク分析ガイド 第2版
https://www.ipa.go.jp/files/000080712.pdf

6. まとめ

米国の石油パイプラインへのサイバー攻撃が発生しました。攻撃はランサムウェアであり、パイプラインが停止することでガソリンの不足が発生しました。
米国ホワイトハウスは大統領令の発令に基づき、連邦政府のシステムのセキュリティ強化や、ソフトウェアサプライチェーンのセキュリティ対策ガイドラインの発行などの対応が行われました。
日本においても重要インフラに対するセキュリティ対策の取り組みがされており、セキュリティ対策の指針の策定や、具体的な対策を実施するためのガイドが公開されています。

重要インフラへのサイバー攻撃はITに限らず広い範囲の経済活動に影響します。そのため、高いレベルのセキュリティ対策を継続することが重要です。重要インフラ企業には、これら日米のガイドラインを活用し対策を強化することが望まれます。また、重要インフラ以外の分野の企業においても、可能な範囲でガイド記載の対策の導入を検討することをお勧めします。

7. 参考URL

- Executive Order on Improving the Nation's Cybersecurity
  https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- US-CERT Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks
  https://us-cert.cisa.gov/ncas/alerts/aa21-131a
- NISC 重要インフラの情報セキュリティ対策に係る第4次行動計画
  https://www.nisc.go.jp/active/infra/outline.html
- 制御システムのセキュリティリスク分析ガイド 第2版
  https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

NTT DATA

Trusted Global Innovator