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 10

～2022 年　衛星通信網へのサイバー攻撃～

2024 年 03 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

2022 年 2 月 24 日、米 Viasat 社が提供する衛星通信サービスがサイバー攻撃を受け、利用者であるウクライナ、ドイツ、ギリシャ、ハンガリー、ポーランド等で通信ができなくなるインシデントが発生した[1]。

本書では、当局や政府機関、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. 2022 年 衛星通信サービスの機能停止

1.1. インシデント概要

米 Viasat 社は、仏 Eutelsat S.A.が保有する通信衛星 KA-SAT を利用した、衛星ブロードバンド接続サービスを主にヨーロッパと中東の 10 万人を超える顧客に提供している。このサービスの利用者の中には、ウクライナの軍や警察機関も含まれていた。

2022 年 2 月 24 日午前 3 時 2 分頃、ロシアがウクライナへ侵攻を開始する 1 時間前に、突然 KA-SAT ネットワークが利用できなくなった[2][3]。

図1-1 欧州におけるインシデント発生地域

4万から 4 万 5 千台の KA-SAT サービスのためのモデムが機能を停止し、ウクライナの数千の顧客と欧州の顧客がインターネットを利用できなくなり、ドイツの Enercon の 5,800 台の風力タービンの遠隔監視サービスに影響が出て[4]、この障害は 2 週間以上続いた[5]。

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 Viasat 社の資料「SURFBEAM 2 NETWORK DIAGRAM」[6]等をもとに作成した仮想システム構成図（図 1-2）を用いて説明する。

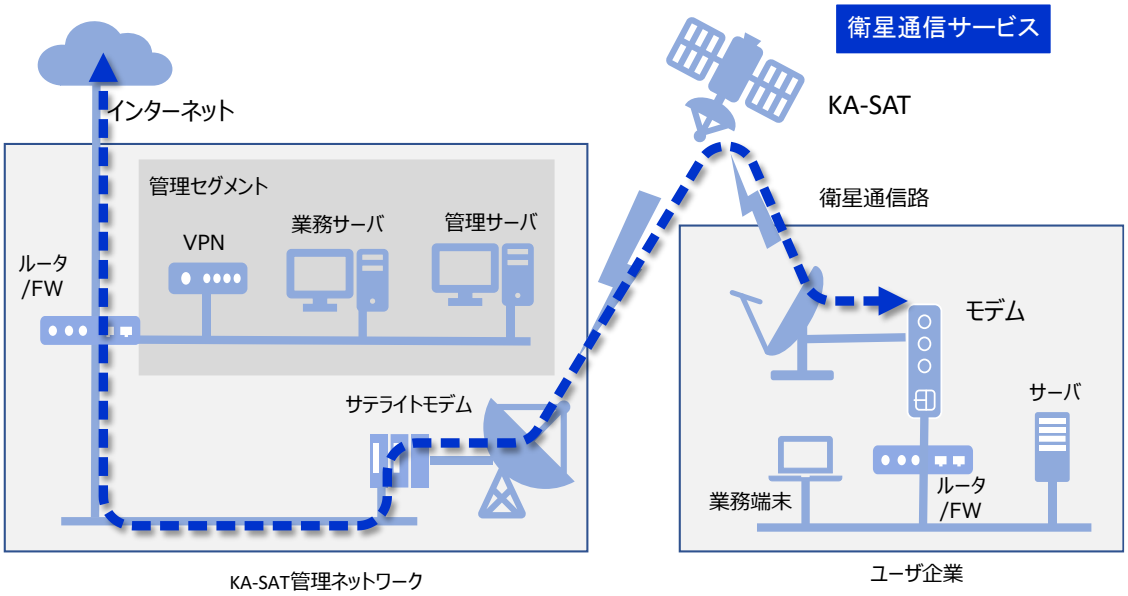


図 1-2　事例理解のための仮想システム構成図（実際のシステム構成とは異なる）[1]

【コラム】ハイブリッド戦争

この衛星通信サービスの停止は、ロシアのウクライナへの軍事侵攻の 1 時間前に発生した。KA-SAT はウクライナ軍等が使用している通信手段であった。このことから、今回のインシデントはハイブリッド戦争（多種多様な手段を使って、政治的な目的を達成するために情報戦、心理戦を強く意識したサイバー戦や情報戦、非正規戦などと正規戦を組み合わせた軍事戦略の手法）の典型例として捉えられている。

このインシデントに関して、2022 年 5 月 10 日、EU、英国、米国、カナダ、エストニア、オーストラリア、ニュージーランドの政府は、当該攻撃がロシアによるものであると正式に発表し、ロシアの行動を強く非難する声明をそれぞれ発表した[7]。

Viasat 社の報告によるとこのサイバー攻撃の範囲は、KA-SAT ネットワークのユーロブロードバンドインフラストラクチャの消費者に限定され、衛星そのものや政府ユーザーには影響を与えなかったとアナウンスされた[8]一方、ウクライナ政府高官は、KA-SAT ネットワークへの攻撃は「戦争が始まった当初の通信に大損害をもたらした[9]と述べたとの報告もある。

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 5 つの局面に分けて解説する。

1.2.1【攻撃局面 A1】DDoS 攻撃の実行

攻撃者はウクライナで利用されている衛星通信回線用のサテライトモデムに対して、DDoS 攻撃を行った。この回線はウクライナ政府、軍およびセキュリティサービスで利用されていた。この攻撃により、衛星通信回線が一時的に利用不能となった。[8]

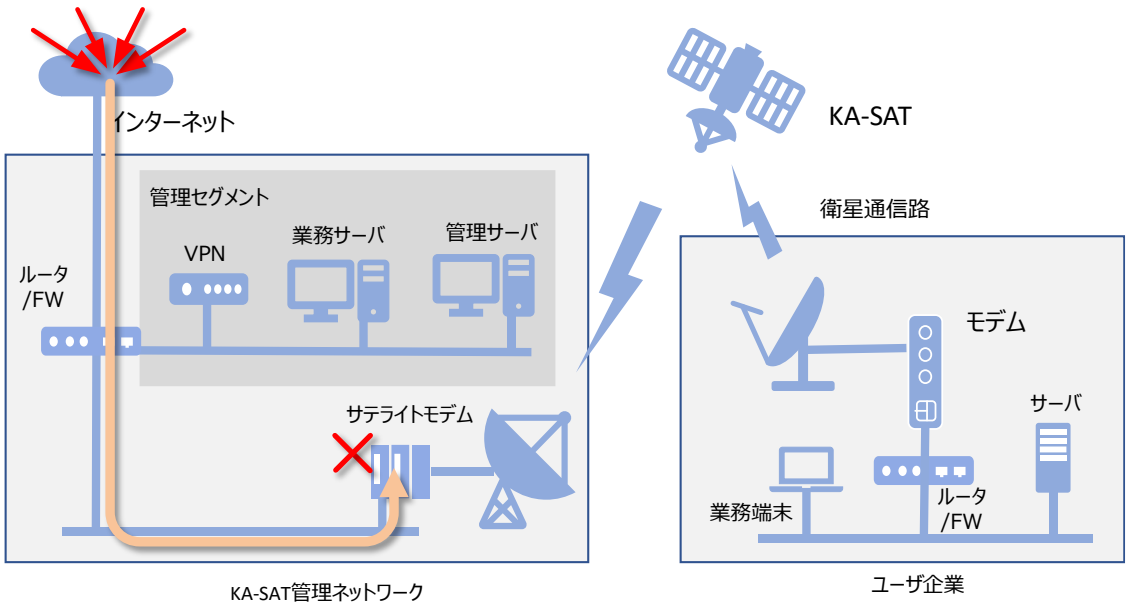


図 1-3 DDoS 攻撃の実行

1.2.2【攻撃局面 A2】対象組織への不正侵入

DDoS 攻撃により通信を混乱させ、攻撃者は VPN への不正アクセスを行う。侵入方法についてはいくつかの報道や発表があるが、以下にまとめておく。

・KA-SAT 管理ネットワーク内の VPN アプライアンスの設定ミスを悪用し侵入したという報告[9]。この設定ミスについての詳細については説明されず、VPN について頻繁に報じられる脆弱性のあるファームウェアを放置したままでその脆弱性を利用されていた可能性が示唆されていた。

・2023 年の Black Hat USA 2023[10]で同社の Viasat 社 副社長兼最高情報セキュリティ責任者 (CISO) が、攻撃者が VPN へのアクセス方法はゼロデイ脆弱性を利用したものでもデフォルトのパスワードを利用したものでもなく不明/内部犯行の可能性についても語っている[11]。(図 1-3)

・一つの可能性として以下が考察されている。KA-SAT の管理ネットワークでは VPN 装置として Fortinet 社の FortiGate アプライアンスが利用されていた[12]。Fortinet は 2021 年に脆弱性を利用したデータ侵害の被害を受け、約 50 万件の VPN 認証情報が盗まれた[13]。米 NSA,CISA,FBI によるとこの情報はロシアが保有しており[14]、それが今回利用された侵入されたとの考えられる[15]。

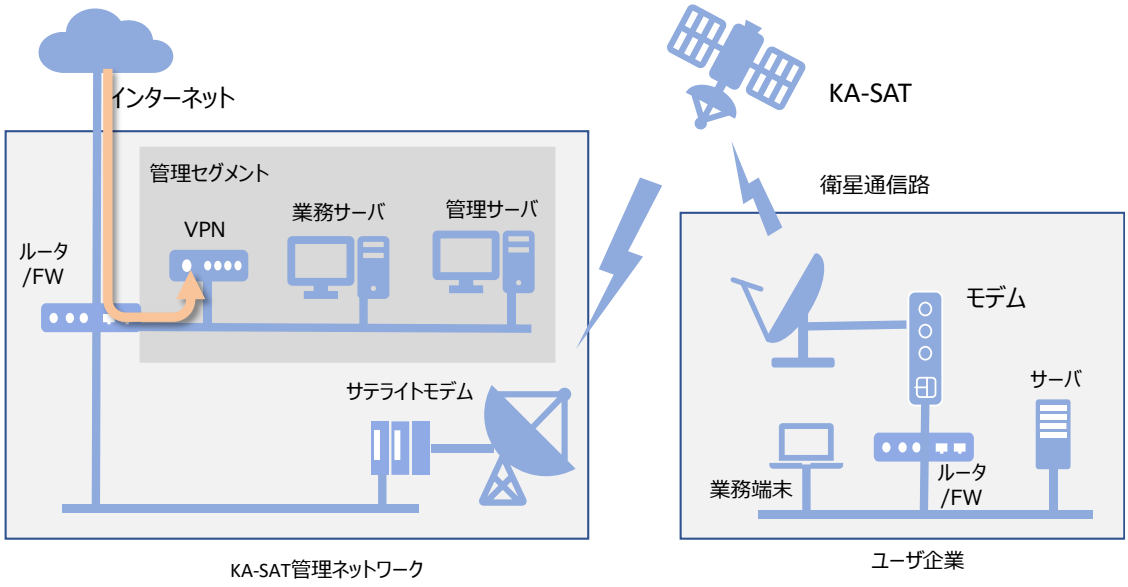


図 1-4　対象組織への侵入

1.2.2【攻撃局面 A3】ネットワーク内部の調査と横展開

攻撃者は内部侵入に成功した後、KA-SAT 管理ネットワークを探索し横展開して、ユーザー企業のモデムの管理セグメントへと侵入し、管理サーバの特権を窃取する。(図 1-4)。

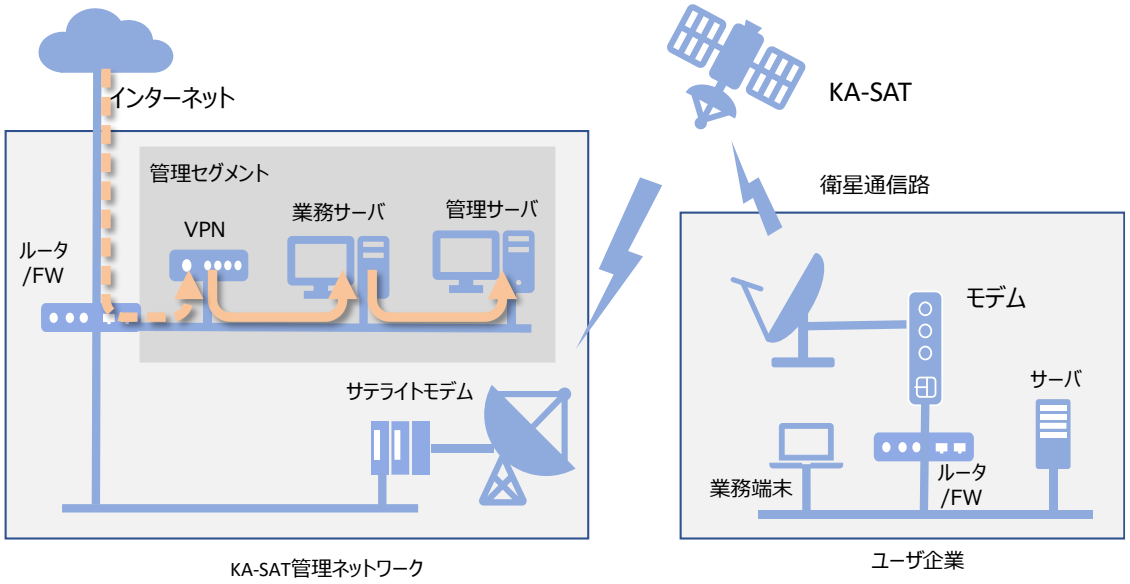


図 1-5 ネットワーク内部の調査と横展開

1.2.3【攻撃局面 A4】AcidRain の配布

攻撃者は管理サーバから正規の管理用コマンドを利用して、利用者のモデムへマルウェア AcidRain を送付する。この AcidRain はワイパーと呼ばれるプログラムで、モデム内部のフラッシュメモリや外部記憶として利用される SD カード、マルチメディアカード(MMC)等に存在するファイルを上書きし削除する。

さらにセキュリティ機能を担う可能性のあるジョブやサービスの停止、証明書の削除等も行うことができる[16]。

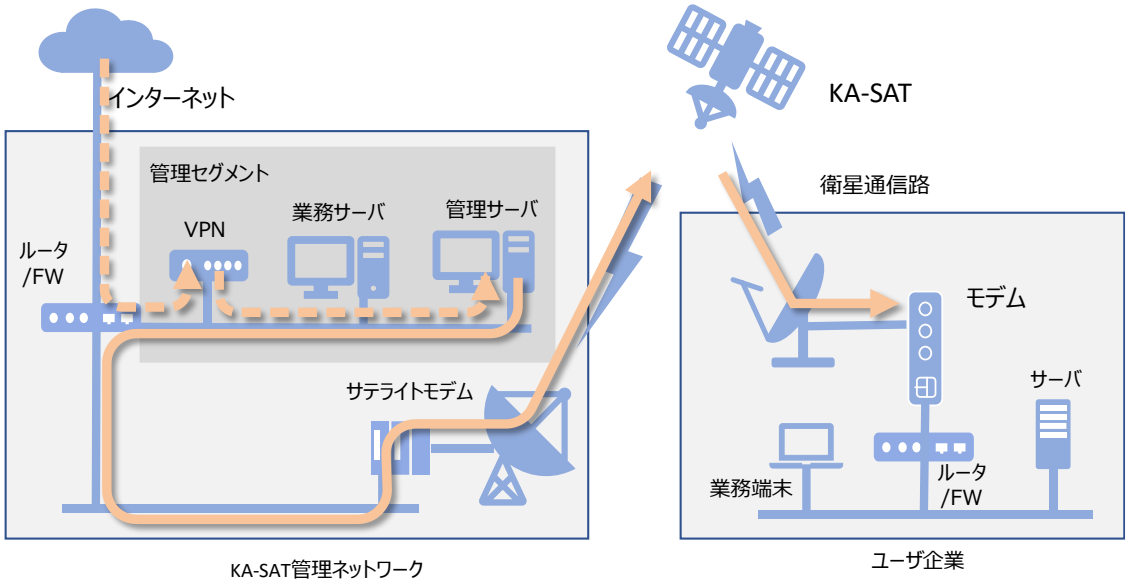


図 1-6　AcidRain の配布

1.2.4【攻撃局面 A5】 データの削除とモデムの再起動

KA-SAT ネットワーク利用者のモデムに配布された AcidRain は起動しモデム内のプログラムの停止とデータの削除を実行する。削除が完了したのち、モデムを再起動させモデムを動作不能とした[17]。

KA-SAT ネットワークの利用者はモデムが機能を停止したため、インターネットを利用できなくなった。

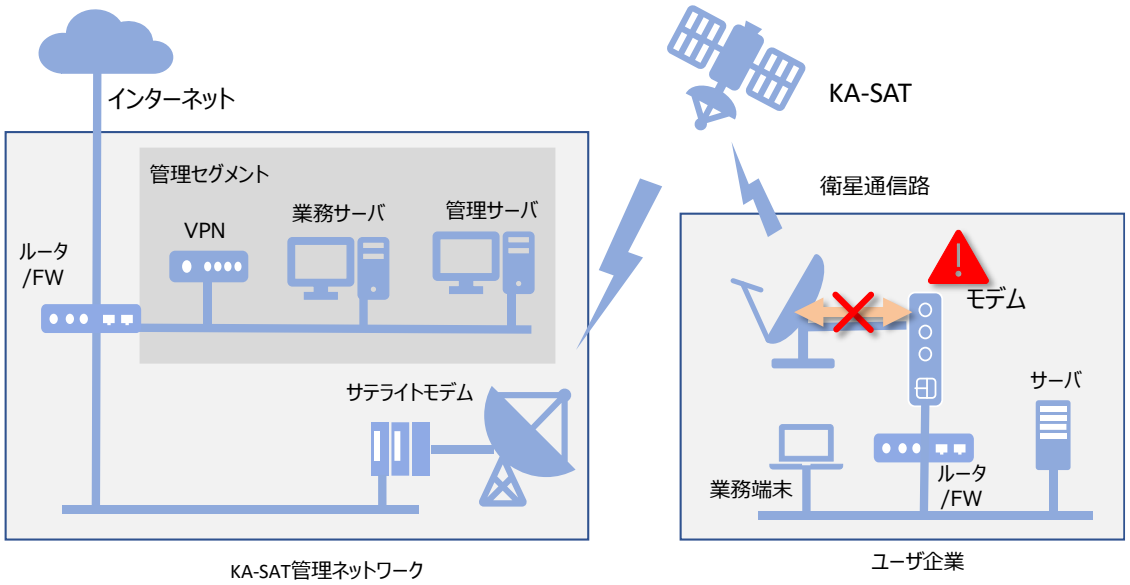


図 1-7 データの削除とモデムの再起動

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	インターネット接続サービスの停止			
	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃
	モデムの機能を損ない、インターネット接続を不能にする	管理サーバ	モデム	ファイルの削除

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*	インターネット	VPN アプライアンスからの侵入	管理サーバ	モデム	ファイルの削除

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:インターネット接続停止の例

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 ＜モデムの機能を損ない、インターネット接続を不能にする＞
【A1】	S1	サテライトモデムに対し DDoS 攻撃を行い、衛星通信回線を一時的に利用不能とする
【A2】	S2	侵入口= インターネット*1 から VPN アプライアンスを経て内部ネットワークへ侵入する
【A3】	S3	管理サーバへのアクセス権を窃取する
【A4】	S4	管理サーバから AcidRain をモデムに送付し動作させる
【A5】	S5	AcidRain がモデムのデータを削除し動作不能にする

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	インターネット
	攻撃対象	モデム
	攻撃拠点	管理サーバ
	経由	VPN アプライアンス
攻撃者		悪意ある外部者
事業被害		インターネット接続が不能
攻撃シナリオ		モデムのファイルを削除することで機能しなくする
最終攻撃（目的）		モデムの機能停止
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 管理サーバの特権窃取 管理サーバの操作

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 CISA(Cybersecurity & Infrastructure Security Agency：サイバーセキュリティー・インフラセキュリティー庁)から公表された、『Strengthening Cybersecurity of SATCOM Network Providers and Customers[18]』、NSA(National Security Agency：米国家安全保障局)が公開している『Protecting VSAT Communications [19]』、さらに、DDoS 攻撃に関しては、CISA から公表された『DDoS QUICK GUIDE[20]』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。表 2-5 は、当事例に参考となる代表的な対策・緩和策をまとめたものとなる。なお DDoS 攻撃に関しては非常に多くの手法が存在しそれぞれの手法についての対策・緩和策が存在することから、本書ですべてを取り扱うと本書の主旨が不明確となりかねないため、単に「DDoS 対策を行う」とし、詳細は参考文献を参照のこと。

表 2-5 代表的な対策・緩和策の例

項番	対策・緩和策
D1	DDoS 対策を行う「[20]
D2	セキュアな認証方式を使用する [18]
D3	強力で複雑なパスワードの使用[18]
D4	アカウントと資格情報の監査 [18]
D5	最小特権の原則の実施[18]
D6	トラフィックの監視[18][19]
D7	デフォルトの認証情報の変更[18][19]
D8	ソフトウェアやファームウェアのアップデート[19]
D9	伝送経路での通信を保護する[19]

「D1. DDoS 対策をおこなう」 各種の DDoS 攻撃手法に対する対策・緩和策を講じる。各種手法と対策・緩和策は参考資料を参照。

「D2.セキュアな認証方式を使用する」衛星通信ネットワークのアクセス、管理に使用するすべてのアカウントに、可能であれば多要素認証などのセキュアな認証方式を使用する。

「D3. 強力で複雑なパスワードの使用」 長く複雑なパスワードを利用する。

「D4. アカウントと資格情報の監査」 終了したアカウントや不要なアカウントを削除し、期限切れの認証情報を変更する。

「**D5. 最小特権の原則の実施**」 特権を必要最小限にする。個々の担当者アカウントに割り当てる特権だけでなく、担当者以外のアカウントに割り当てる特権（ソフトウェアやシステムに割り当てる特権など）も考慮する。アカウント特権を明確に定義し、範囲を絞り、使用パターンに照らし合わせて定期的に監査することが望ましい。

「**D6. トラフィックの監視**」通信機器への出入口に監視機能を追加し、予期しない通信やアクセスを監視する。

「**D7. デフォルトの認証情報の変更**」デフォルトの認証情は利用せずに変更しておく。

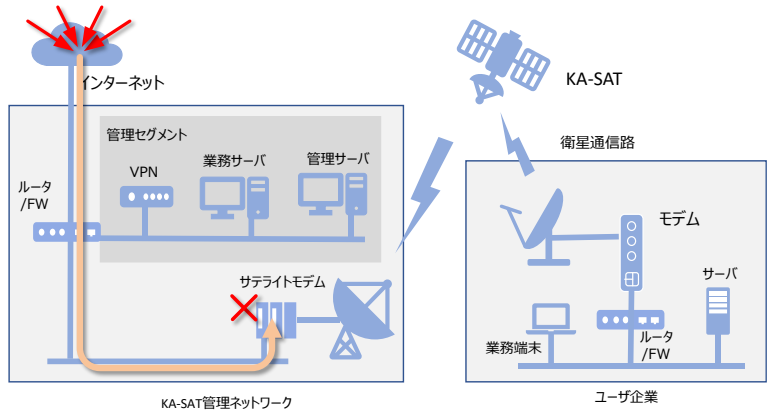
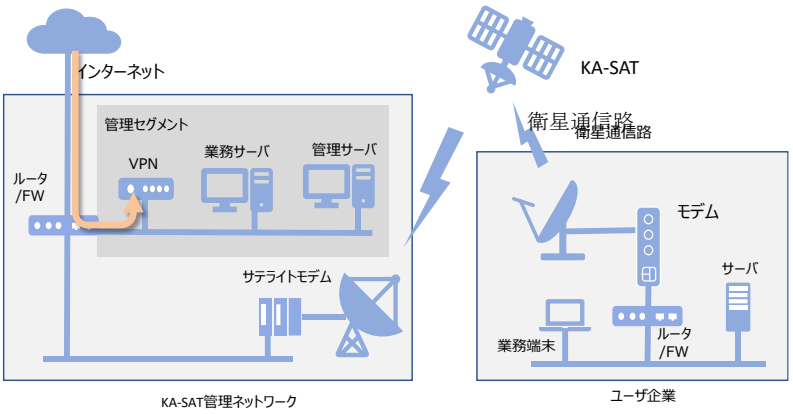
「**D8. ソフトウェアやファームウェアのアップデート**」 脆弱性の発見されたソフトウェアやファームウェアに対し、すぐにアップデートを行えるようにし、常にシステムを最新の状態を保つ。

「**D9. 伝送経路での通信を保護する**」 通信の伝送経路を、セグメント化し通信時のデータのみの暗号化ではなくヘッダを含む暗号化を行う事、スペクトラム拡散や周波数ホッピング等の技術を用いて通信の傍受の可能性を低減させる TRANSEC を実現する。

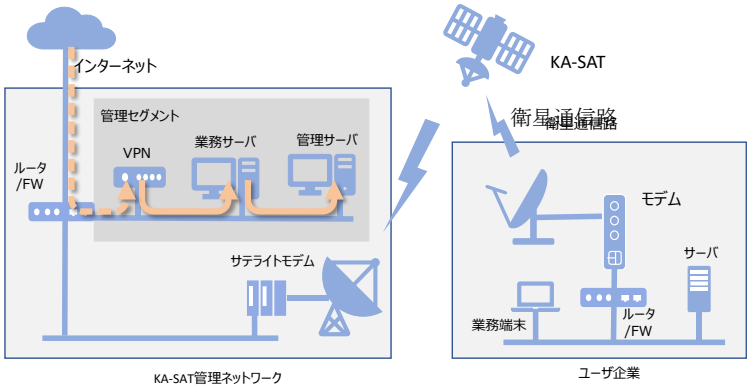
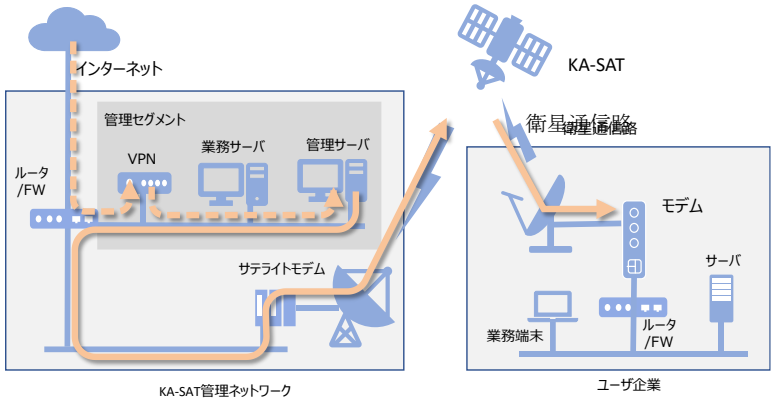
2.5. 攻撃ステップと対策・緩和策の関連付け

2.3 節までの情報をもとに、【攻撃局面 A1～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

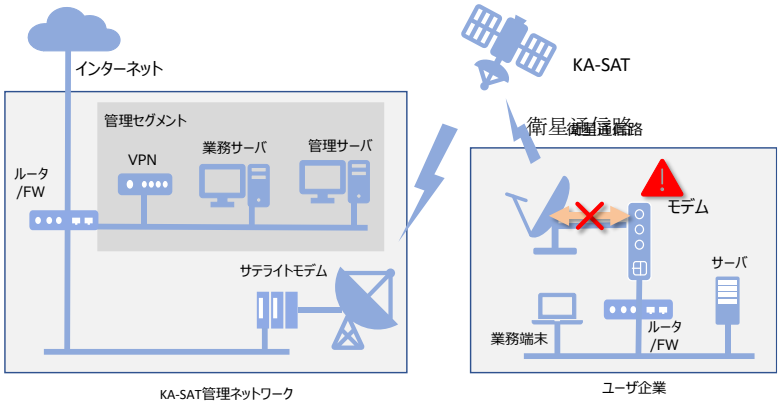
攻撃局面	攻撃ステップ[2]	対策・緩和策	対象システム・資産
【攻撃局面 A1】  	[S1] DDoS 攻撃の実行	•DDoS 対策を行う[D1]	・ネットワーク ・サテライトモデム
【攻撃局面 A2】  	[S2]対象組織への不正侵入	•セキュアな認証方式を使用する[D2] •強力で複雑なパスワードの使用[D3] •アカウントと資格情報の監査[D4] •トラフィックの監視[D6] •デフォルトの認証情報の変更[D7] •ソフトウェアやファームウェアのアップデート[D8]	•KA-SAT 管理ネットワークのルータ/FW、VPN •

[2] [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[3]	対策・緩和策	対象システム・資産
【攻撃局面 A3】  	[S3] ネットワーク内部の調査	•セキュアな認証方式を使用する[D2] •強力で複雑なパスワードの使用[D3] •アカウントと資格情報の監査[D4] •デフォルトの認証情報の変更[D7] •ソフトウェアやファームウェアのアップデート[D8]	•業務サーバ
【攻撃局面 A4】  	[S4] AcidRain の配布	•なし[4]	•モデム

[3] [S]は表 2-3 の項番と対応。[D]は表 2-5 の項番と対応。

[4] ファームウェアのアップデート機能は必要かつ正規の手続きとなるため利用者側での対策は困難。起動時の完全性のチェックなど機器側での対応が必要となる。

攻撃局面	攻撃ステップ[5]	対策・緩和策	対象システム・資産
【攻撃局面 A5】  	[S5] データの削除とモデムの再起動	•セキュアな認証方式を使用する[D2] •デフォルトの認証情報の変更[D7]	•モデム

【コラム】: 衛星の乗っ取り

本書のインシデントでは、生成通信網を構成する地上の顧客のモデムへのサイバー攻撃の事例だったが、2007 年,2008 年米国では衛星制御が乗っ取られるインシデントがあった。

NASA の地球観測衛星 Landsat-7 と Terra AM-1 が計 4 回以上のサイバー攻撃を受け、数分間操作が妨害された事がある*。この時はノルウェーにある地上局経由衛星へと侵入された。

衛星にはこのように、インフラ自体を脅かす脅威も考慮する必要がある。

参考 URL:
https://www.satellitetoday.com/uncategorized/2011/10/31/report-hackers-interfered-with-landsat-7-terra-am-1-in-2007-and-2008/

[5] [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] Satellite outage knocks out thousands of Enercon's wind turbines
https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/

[2] AcidRain | A Modem Wiper Rains Down on Europe
https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

[3] Internet disruptions registered as Russia moves in on Ukraine
https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K

[4] NSA, Viasat say 2022 hack was two incidents; Russian sanctions resulted from investigation
https://therecord.media/viasat-hack-was-two-incidents-and-resulted-in-sanctions

[5] Viasat's KA-SAT network still disrupted by suspected cyberattack more than two weeks later
https://www.datacenterdynamics.com/en/news/viasats-ka-sat-network-still-disrupted-by-suspected-cyberattack-more-than-two-weeks-later/

[6] SURFBEAM 2 SYSTEM ADVANTA/SURFBEAM 2 NETWORK DIAGRAM
https://silo.tips/download/surfbeam-2-high-performance-high-capacity-broadband-satellite-system

[7] Press release: Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion
https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion

[8] SentinelLabs: AcidRain | A Modem Wiper Rains Down on Europe
https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

[9] Viasat: KA-SAT Network cyber attack overview
https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

[10] Lessons Learned from the KA-SAT Cyberattack: Response, Mitigation and Information Sharing
https://www.blackhat.com/us-23/briefings/schedule/#lessons-learned-from-the-ka-sat-cyberattack-response-mitigation-and--information-sharing-34478

[11] The Record: NSA, Viasat say 2022 hack was two incidents; Russian sanctions resulted from investigation
https://therecord.media/viasat-hack-was-two-incidents-and-resulted-in-sanctions

[12] VIASAT incident: from speculation to technical details.
https://www.reversemode.com/2022/03/viasat-incident-from-speculation-to.html

[13] Bleeping Computer: Hackers leak passwords for 500,000 Fortinet VPN accounts
https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/

[14] Degital Garden: NSA Urges Organizations to Patch Five Vulnerabilities Exploited by Russia
https://www.digitalguardian.com/blog/nsa-urges-organizations-patch-five-vulnerabilities-exploited-russia

[15] ESPI: The War in Ukraine from a Space Cybersecurity Perspective
https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Report-84.pdf

[16] Threat Update: AcidRain Wiper
https://www.splunk.com/en_us/blog/security/threat-update-acidrain-wiper.html

[17] MIT Technology Review: Russia hacked an American satellite company one hour before the Ukraine invasion
https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/

[18] Strengthening Cybersecurity of SATCOM Network Providers and Customers
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-076a

[19] Protecting VSAT Communications
https://media.defense.gov/2022/May/10/2002993519/-1/-1/0/CSA_PROTECTING_VSAT_COMMUNICATIONS_05102022.PDF

[20] CISA: DDoS QUICK GUIDE
https://www.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf

更 新 履 歴

2024 年 3 月 4 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 10

～2022 年 衛星通信網へのサイバー攻撃～

[発　行]2024 年 3 月 4 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　木下　仁　木下　弦　小助川 重仁　高見　穣