5分でわかるモバイルコアのまもりかた

～モバイル特有の攻撃と対策～

NTTドコモ

大宮 直樹

■ 氏名

大宮 直樹（おおみや なおき）

■ 所属

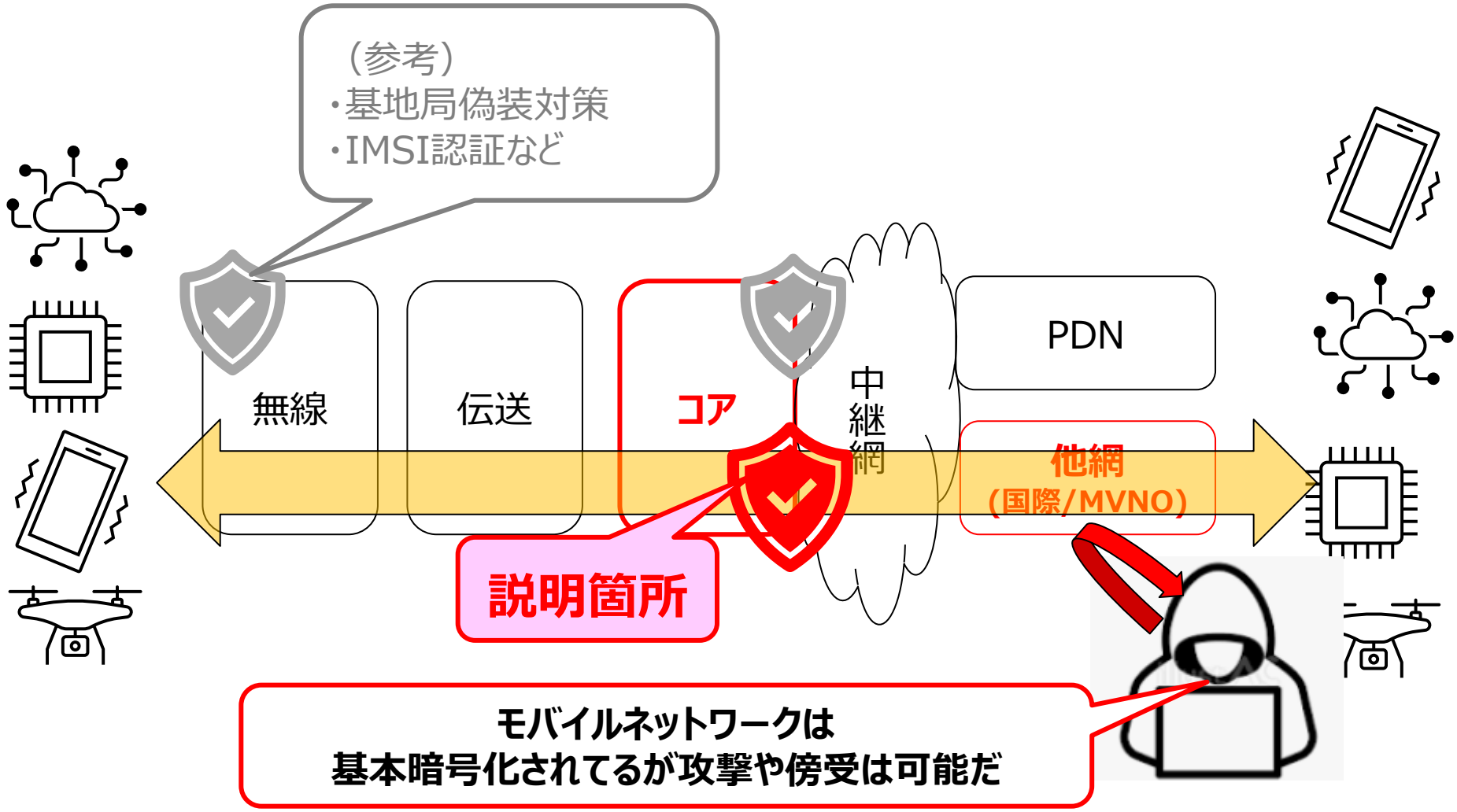
NTTドコモ コアネットワークデザイン部 パケットコア担当

主な業務：コアネットワークにおけるパケット系NW機器の
新規導入～NW設計検証業務

■ 趣味

相撲観戦、オーケストラ鑑賞、レコード収集

- モバイルネットワークを支えるコアネットワークのセキュリティ
- 他網との接続点において近年発生するセキュリティ課題と対策検討



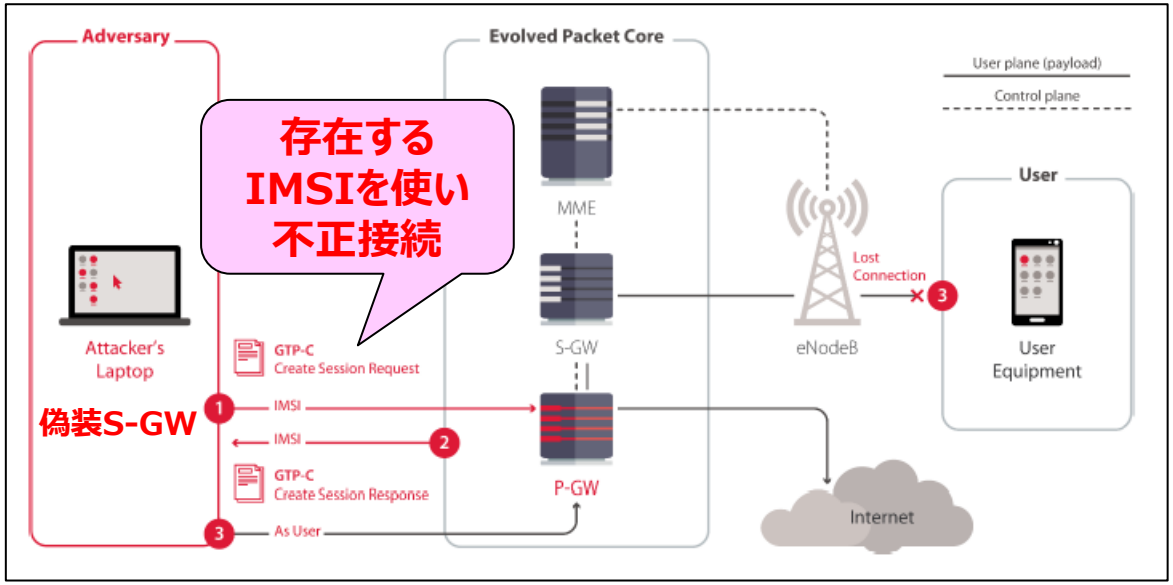
- **モバイルネットワークに求められるセキュリティ要件は、ITネットワークと共通する要素も存在するが、異なる点も多い**

	ITネットワーク	モバイルネットワーク (コア区間)
方式	・LAN/WAN を中心としたIPベースのネットワークにおけるFW/IDS/IPS/VPNなど、**一般的なセキュリティ**	・**左記IPベース＋3GPP標準**に基づく階層構造（RAN/Core/Transport NWなど） ・加入者認証やハンドオーバーなどの移動処理も考慮した作り
プロトコル	・**IETF標準プロトコル群**（IP/TCP/UDP/HTTP/ /DNS/DHCP/SNMPなど）	・**左記IETF標準＋3GPP標準に基づく通信プロトコル**（GTP-C/GTP-U/ Diameter/SIGTRAN） ・5GではSBIにてHTTP/2を採用
脅威	上記プロトコルの脆弱性を突いた ・不正アクセス、フィッシング ・マルウェア、ランサムウェア ・VPN/クラウド経由の侵害	・左記脆弱性＋上記プロトコルの脆弱性を突いた ・不正侵入と破壊 ・**ローミングにおける通信傍受や乗っ取り** ・大量のIoTデバイスによる DDoS

➢ **IPにおける基本的セキュリティを理解した上で、更にモバイル特有の接続処理や各信号パラメータの意味まで理解しなければならない**
・・・広範な知識とモバイルネットワークの深い技術力が必要

GTPプロトコルにおけるユーザ識別番号(IMSI)を悪用した不正通信

- 攻撃者はユーザパケットを処理するS-GWに成りすまし、存在するIMSI等を使って不正通信を行う
- 存在するIMSIが使われる為、**GTP単独のセキュリティ対策では不正な要求かどうか判別できない**



【攻撃手順】

攻撃準備　：攻撃者は**予め有効なIMSI情報を調査**する（各種方法があります）

攻撃開始　：攻撃者はS-GWに偽装し攻撃対象のP-GWに対して**上記IMSIを使い**
「Create Session Request」などのGTP-Cメッセージを使って**不正にセッション確立**

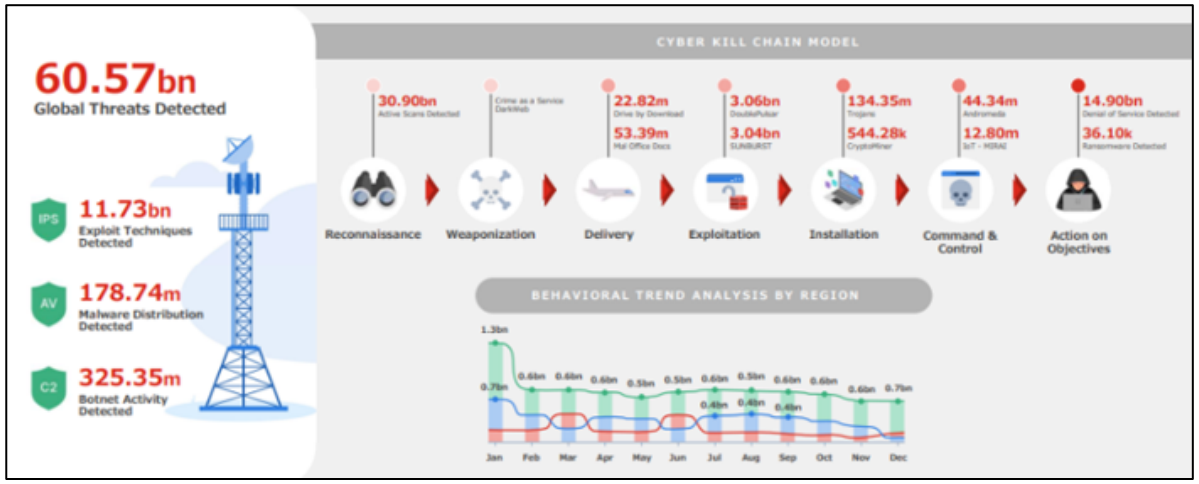
不正通信開始: 上記で**確立されたセッションを利用し**攻撃者はネットワークに**侵入**する

⇒ **本攻撃は正規加入者やオペレーターに経済的損失を与える事が可能**

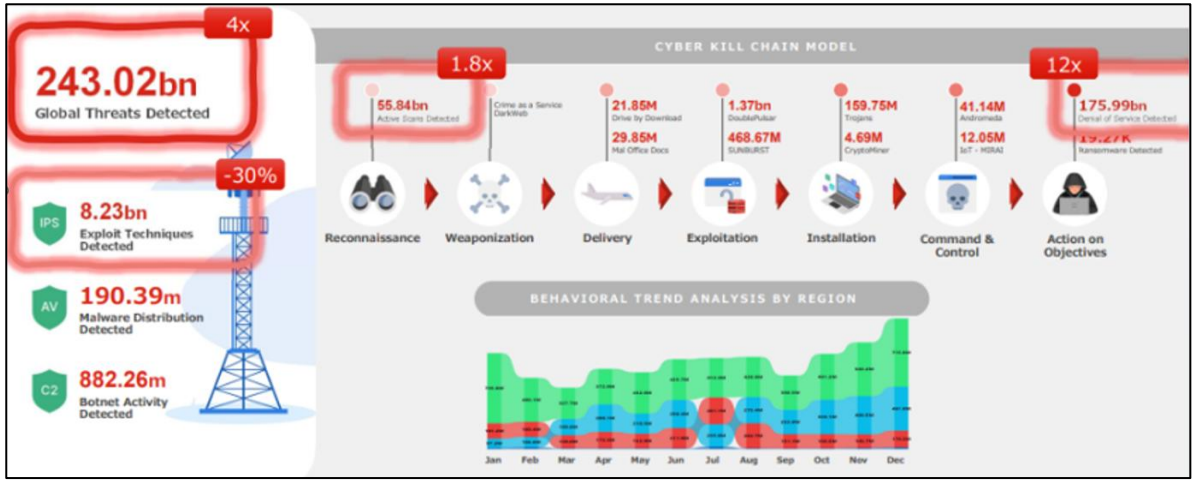
出典：FS.20 GPRS Tunnelling Protocol (GTP) Security
https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-20-gprs-tunnelling-protocol-gtp-security-v3-0/

- モバイルネットワークにおけるセキュリティリスクは、年々増加傾向にあり、2023から1年でグローバルで約4倍にまで攻撃回数が増加
- 攻撃による顧客情報流出や通信不可等の事態に陥るケースもグローバルで発生

【2023年】



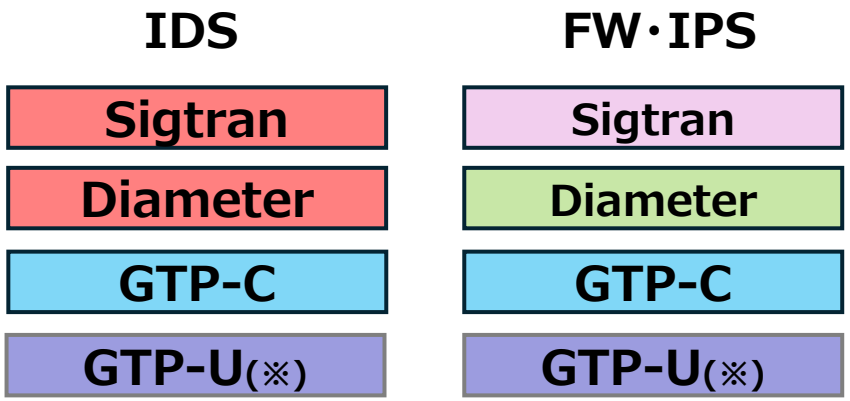
【2024年】



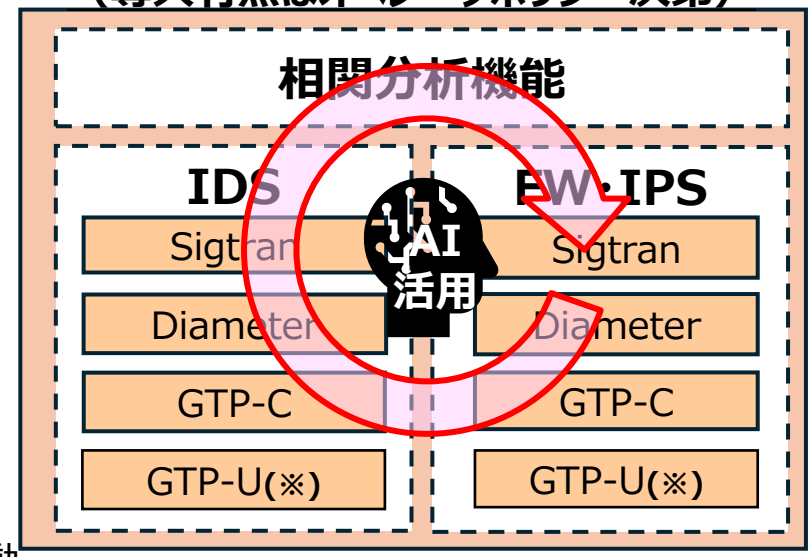
出典：FortiGuard Labs, Spotlight on Telco/Carriers, 2024 Q4

- 近年AIにより攻撃手法が進化しており、**既存機能による単体の対策だけでは、不正アクセスの検知・防御が困難**に
- プロトコル間で状態や順序性を確認するなど、**統合ソリューションによる相関分析**が必要

今までのプロトコル別対策
（サイロ化されたセキュリティ対策）



近年のプロトコル横断の統合対策
（導入有無はオペレータポリシー次第）



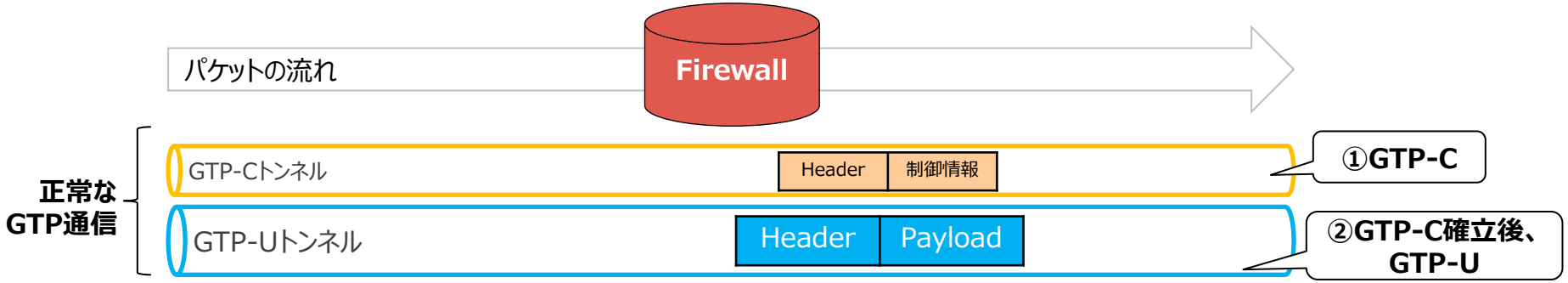
※実際は通秘などの制度と契約上の合意状況に応じて確認範囲が変動

◇機能及びプロトコル毎の検知・防御
◇監視・保守運用の複雑化

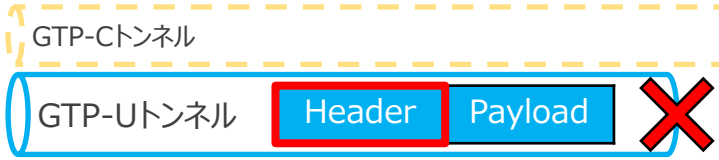
◇検知・防御の高度化
◇監視・保守運用体制の一元化

➢ **高度なセキュリティ機能の有効性を検証するためPoCしてみた**

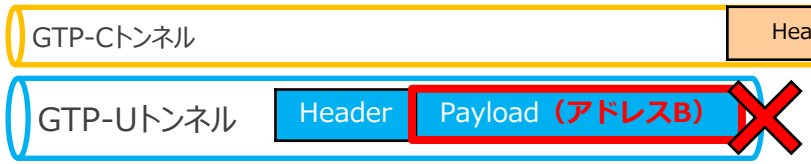
- ユーザデータを運ぶためのGTP-CとGTP-Uを使った相関分析により不正な攻撃を検知する。
- GTP-Uペイロードまで検査する場合、より多くの検知が可能。



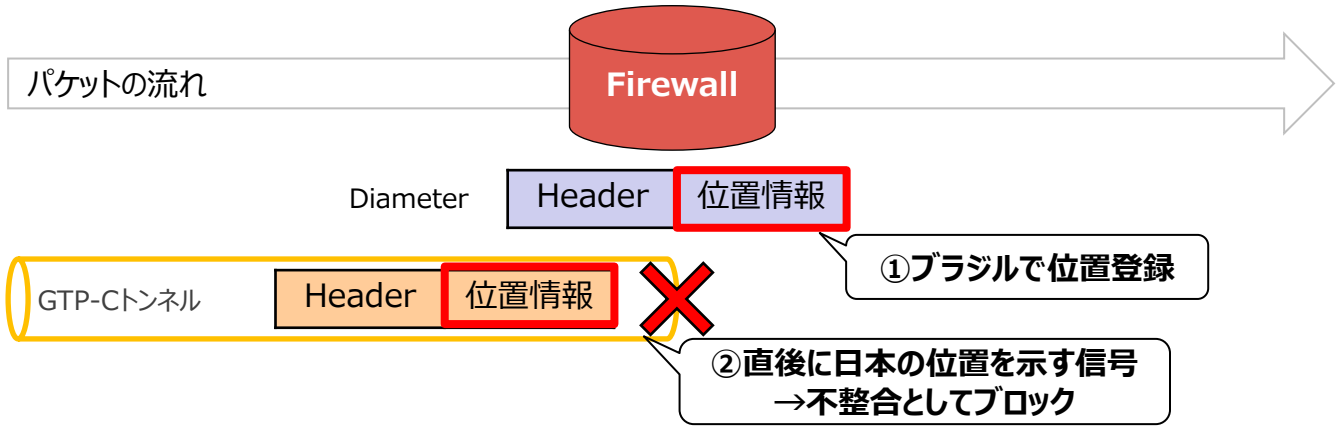
攻撃ケース1：GTP-C情報が存在しない状況で流れてくるGTP-Uはブロック



攻撃ケース2： GTP-Cで割り当てたGTP通信用IPアドレスと、GTP-Uペイロードの送信元IPアドレスを比較し、異なる場合はブロック

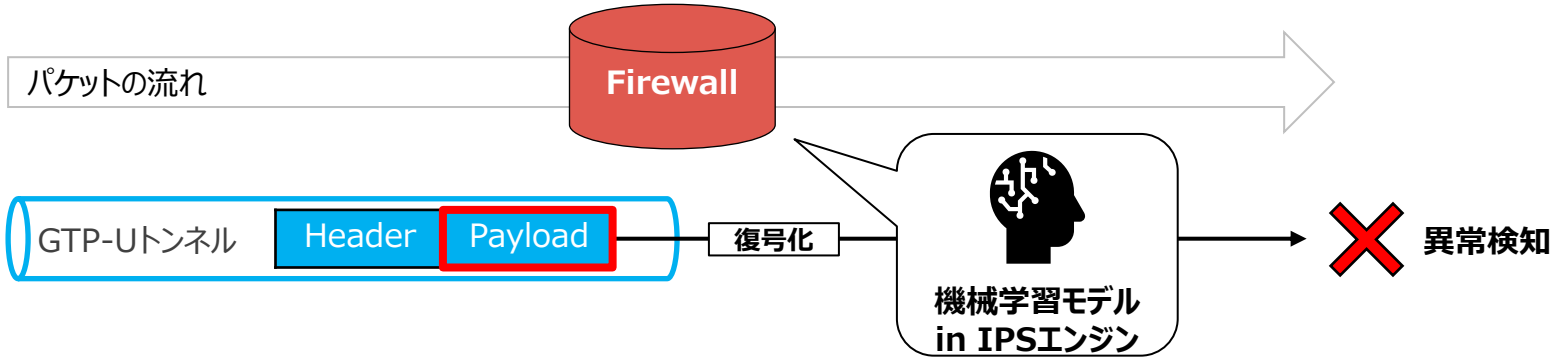


- **位置情報を処理するDiameterで流れてきた位置情報と、GTP-Cで流れてきた位置情報を比較し、地理的な不自然を検知したらブロック**



- **モバイル網はプロトコル単体では守れない。複数プロトコルを相関分析した検知が重要**

- 復号化したGTP-Uペイロードに対し、機械学習によるIPSでの検査を実施し、悪意あるパケットをブロック



- ペイロード検査は制度上のハードルが高いため、商用実装が難しい。
- モバイルプロトコルはフォーマットやシーケンスが固定なので、検知精度向上のためのAI利用は限定的。運用支援補助としての利用が想定される。
（障害切り分け、対策提示等）

- **モバイルコア特有の攻撃に対し、複数プロトコルを利用したセキュリティ対策が有効。必要性と費用対効果を見極めてセキュリティ対策を検討する。**

会場にお越しの通信キャリア、セキュリティベンダ、興味ある方へ

Day3まで本会場におりますので、気軽にお声がけ下さい
どこまで対策を行うべきなのか、ご意見頂けると嬉しいです

- AIをどの程度利用しているか（検査・分析？運用アシストまで？）
- GTP-U検査の有無（ヘッダまで？ペイロードも？）
- MNO~MVNO間POIのセキュリティレベル