資料３－１

フロンティアAI時代の通信事業におけるデータの保護・セキュリティの在り方に関する検討会

データ保護・セキュリティ対策の高度化に向けて

KDDI株式会社

2026年11月24日

Spark Your Journey

ISP事業者向けメールシステムへの不正アクセス事案

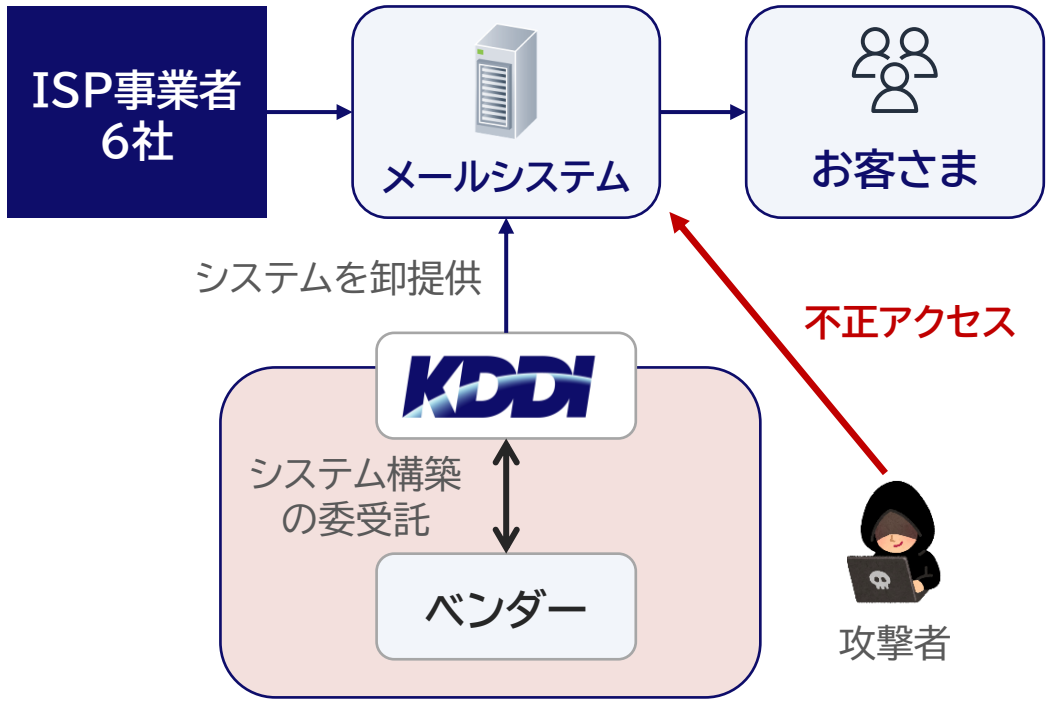
第三者製ソフトの“未知の脆弱性”を突かれ 約1,223万名分のメールアドレス、約762万名分のパスワードが漏えい

第三者製ソフトの“未知の脆弱性”を悪用した不正アクセス

約1,223万名分
個人情報の漏えい
メールアドレス

約762万名分
通信の秘密の漏えい
IDやパスワード等（内数）

- **5/16** 不正アクセス発生
- **6/17** 当社確認・システム改修
- **6/21** 全サーバーへEDR(*)導入
- **6/23** 公表・フォレンジック完了



(*)EDR：Endpoint Detection and Response
エンドポイント（ユーザーのデバイスやサーバーなど）に対するセキュリティ脅威を検出し、分析し、対応するためのセキュリティ技術

本事案で顕在化した課題

“未知の脆弱性”や巧妙化する攻撃に対し、
既知の脅威を前提とした検知、多層防御、旧来の通信規格の3点に課題が顕在化

① 検知・監視	② 多層防御	③ 旧来の通信規格
“未知の脆弱性”を突かれ、 既知の脅威に基づく 監視では検知困難	侵入を前提とした多層防御 （マイクロセグメンテーション）が できていなかった	従来型メールソフト利用者への 影響を踏まえ、 ISP事業者と協議のうえ 旧来の通信規格を継続使用

再発防止に向けた取組み

AIによる網羅的なソフトウェア点検と通信規格の強化により、“未知の脆弱性”に先回りして備える体制へ転換

抜本的な再発防止策

AIを活用した網羅的なソフトウェア点検	• 設計書・プログラムをAIも活用し、潜在的な問題を網羅的に分析 • 外部ベンダーと当社の多段階で不具合を確認 • 本事案以外のシステムに対しても全社展開
高強度な通信規格への移行	• 従来型メールソフト利用のお客さまへの影響に配慮しつつ、ISP事業者と共に高強度な通信規格への移行を早期推進 • ICT-ISAC・JAIPA・日本ケーブルテレビ連盟を通じ業界全体へ注意喚起し、安全性向上に貢献
監視・ガバナンス強化	• 外部通信を制御する全サーバーにEDRを導入し、不審な挙動を常時監視 • SOC(*)にログ分析内容の強化とアクティブユーザー数監視を追加 • 「漏えいのおそれ」段階で経営層へ原則24時間以内の報告体制化 • 外部ベンダーと月次で脆弱性情報を確認

(*)SOC：Security Operations Center
情報セキュリティを監視し、異常を検知した際に迅速に対応するための組織や施設

本事案から得られた教訓

本事案の教訓は当社固有ではなく通信業界共通の課題
「監視の高度化」「多層防御」「業界全体での旧規格廃止」が不可欠

① 監視の高度化

未知の脆弱性は、
社内監視だけでは検知困難

▼

**振る舞い監視・AI分析で
監視の高度化が必要**

② 多層防御

多層防御ができておらず、
侵入後の被害拡大を防げなかった

▼

**侵入される前提で、
マイクロセグメンテーションに
よる多層防御が必要**

③ 業界全体での旧規格廃止

旧来の通信規格は
利用者のメールソフト設定変更を伴い、
個社では移行が進みにくい

▼

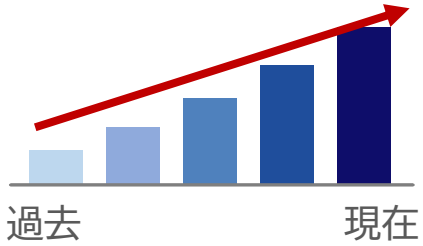
**業界全体で旧規格の廃止の
働きかけが必要**

**通信は365日止められない社会インフラ
“止められない通信”を守るには、セキュリティ監視の高度化が不可欠**

フロンティアAI時代に高まるサイバー攻撃の脅威

通信事業者を狙う大規模な漏えいが相次ぎ、攻撃はAIでマシンスピード化
通信業界全体を守るには、事業者単独・人手依存の監視では対応困難

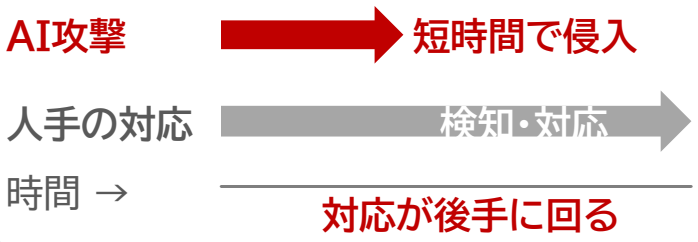
漏えい事案の増加・大規模化



漏えい報告
増加
大規模化

通信事業者を標的とした
不正アクセスが国内外で相次ぐ

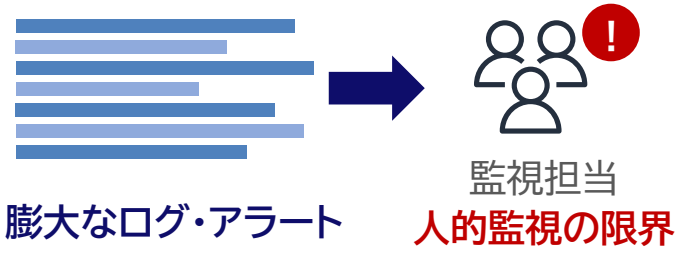
攻撃のAI化・高速化



生成AI・フロンティアAIの悪用や
攻撃ツールのサービス化が進行

防御側にもマシンスピードでの
検知・遮断が必要

従来型監視の限界



膨大なログ・通信を
人の目で監視・分析しきれない

ウイルス対策やIDS(＊)等の従来
型の不正侵入検知だけでは不十分、
外部基盤でのAI分析も不可欠

(＊)IDS:Intrusion Detection System
ネットワークやサーバーへの不正な侵入・攻撃の兆候を検知し、管理者に通知するシステム

環境変化を踏まえたセキュリティ監視のあり方

エコシステムの複雑化と攻撃の高度化により、自社だけで守り切ることは困難
外部クラウド・SaaS・AIと連携した常時監視の体制が必要

従来：自社内で完結する監視

自社

自社設備にセキュリティ製品を直接導入

社内に閉じてアラート・ログを分析



高度・高速化する未知の攻撃に
自社のみでは追随困難

これから：外部と連携した常時監視

通信事業者
自社設備・SOC

クラウド型基盤
（EDR/SIEM(*)等）

外部AIによる
高度な分析

外部専門家
（マネージドSOC）

データ連携

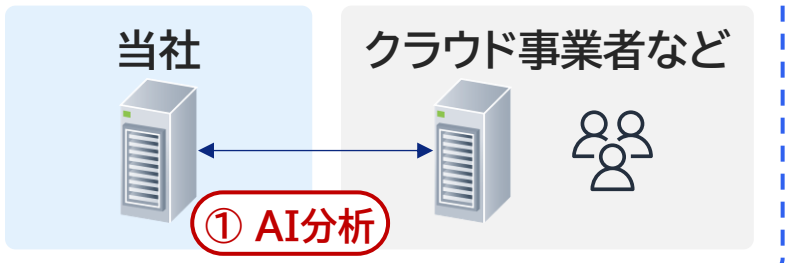
環境変化　クラウド・複数ベンダー連携のサービス構造へ移行　／　生成AIの悪用等で攻撃が巧妙化・高度化

(*)SIEM：Security Information and Event Management
リアルタイム監視やアラート機能により、ネットワーク上の脅威や異常を検出・対応するための統合管理ツール

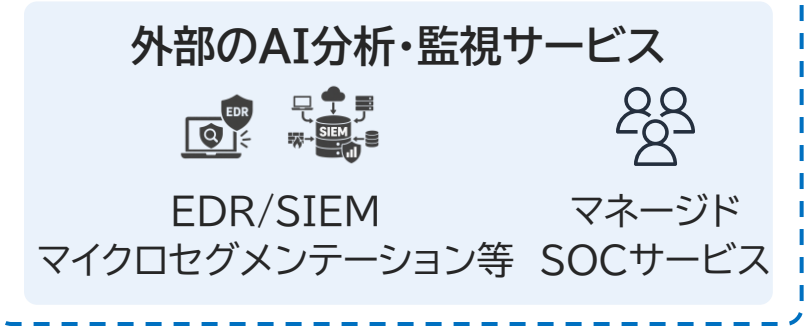
AI分析・外部連携における「通信の秘密」の制約

お客さまの通信を守るための**平時のAI分析・外部連携**であっても
現行解釈では位置づけが明確でなく、**制度上の整理が必要**

通信エコシステムの変化



対策の高度化



AI分析・外部連携に必要なデータ例

項目	必要な理由
ヘッダ情報	攻撃元・宛先の特定、通信の相関分析
データ部	マルウェア・攻撃コードの検知、手法分析
プロセス情報	端末上の不審な実行、侵害範囲の特定
設定情報	設定不備・脆弱性の把握、影響度評価
認証・アクセスログ	不正ログイン・なりすましの検知
…	…

① 通信のAI分析・監視
未知の攻撃を早期検知するため、
平時から通信ログ等をAIで常時分析

② 外部へのデータ連携
EDR/SIEM・マネージドSOCにて
高度な分析のためログ等を外部送信

「個別具体的かつ明確な同意」なく
通信内容等の分析や外部提供することは
「通信の秘密」の侵害（知得・窃用）に該当

既存手段ではAI分析・外部連携を実現できない理由

「通信の秘密」は厳格な運用が求められる中、**平時の常時監視に必要なAI分析・外部連携は**
個別同意・緊急避難等のいずれの手段においても実現が困難

手段	想定される整理	課題	
個別同意	全利用者から 個別具体的かつ明確な同意を取得	全利用者から同意を取るのは困難 同意者／未同意者を分けた監視は不可能	×
緊急避難	攻撃発生時の緊急対応として整理	平時から常時行う予防的な対策であり、 緊急避難の要件に当たらない	×
自社・内製	データを外部に出さず、 自社設備で完結して分析	高度なAI分析や迅速な機能更新が困難で、 防御が攻撃のスピードに劣後	×

AI分析や外部監視基盤等へのデータ連携について、
例えば、通信事業の本来業務として「正当業務行為」と整理することが現実的

AI分析・外部連携の想定と安全確保の考え方

外部事業者の役割に応じたリスクベースの安全措置を取ることで、
段階的にAI分析・外部連携を進める必要がある

外部活用の想定ステップ

STEP 1

クラウド型セキュリティ基盤の活用
クラウド型EDR・SIEM等に
ログ・通信情報を連携し、検知・分析を高度化

STEP 2

AIによる高度な分析
マルウェアの性質、不正プロセス起動、
外部通信を試みるソフトの有無など、
サーバー内部まで把握

安全確保の考え方

調達	懸念国の製品・サービスを除外
データ最小化	分析に必要なデータのみ提供
担保措置	目的限定・二次利用禁止を契約で担保 第三者認証、暗号化等の 技術的措置で担保
接続形態	閉域接続や分析結果のみの受領により、 安全性を確保

本検討会でお願いしたい「通信の秘密」の整理

安定的な通信提供のためのAI分析・外部監視基盤等へのデータ連携については
適切な安全措置を講じることを前提に**平時から実施可能となるよう整理**いただきたい

① 目的の正当性

通信役務の円滑・安定提供の確保

設備維持・障害予兆検知等、
セキュリティ確保を中心とする
本来業務に限定

② 行為の必要性

AI分析・外部基盤の活用が不可欠

人手や内製のみでは、
フロンティアAI時代の
攻撃スピードに対応が困難

③ 手段の相当性

通信の秘密への影響を最小化する措置

下記のような措置を講じることで、
通信の秘密への影響を必要最小限に抑制

③ 手段の相当性に係る主な考慮事項

考慮事項 1

自動処理を基本とした人の関与の最小化

処理は自動化を基本とし、
人による閲覧等は
必要な範囲に限定

考慮事項 2

データの最小化・保存期間管理

最小限のデータ項目・
保存期間に限定
不要となった時点で
速やかに自動消去

考慮事項 3

目的外利用の禁止

汎用AI学習や他社流用を
契約・技術の両面で禁止

考慮事項 4

安全管理・越境リスク対策

守秘義務、権限・操作監査、
暗号化等を徹底

Spark Your Journey

KDDI

「つなぐチカラ」を進化させ、
誰もが思いを実現できる社会をつくる。

KDDI VISION 2030

