資料３－３

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

2026年11月24日

© NTT, Inc. 2026

本日のご説明

1. 通信事業を取り巻く脅威環境の変化
2. NTTグループのセキュリティ対策の基本的な考え方
3. 脆弱性対応の考え方
4. 通信事業における可用性確保とセキュリティ対応
5. AIを活用した防御能力の高度化
6. 今後の検討に向けた観点

© NTT, Inc. 2026

1. 通信事業を取り巻く脅威環境の変化

脅威環境の変化

フロンティアAIの進展 ▶

基本対策の不備を突く攻撃

- **高速化**：脆弱性探索・分析 攻撃コード生成
- **大規模化**：広範な対象への探索・攻撃
- **複雑化**：複数の脆弱性・設定不備の組合せ

通信事業者の脆弱性対応

多数・多様な通信設備への段階的な対応

影響評価 ▶ 検証 ▶ 緩和策 ▶ 対策適用

攻撃の高速化に伴い、対応までの時間的猶予が縮小

重要な課題

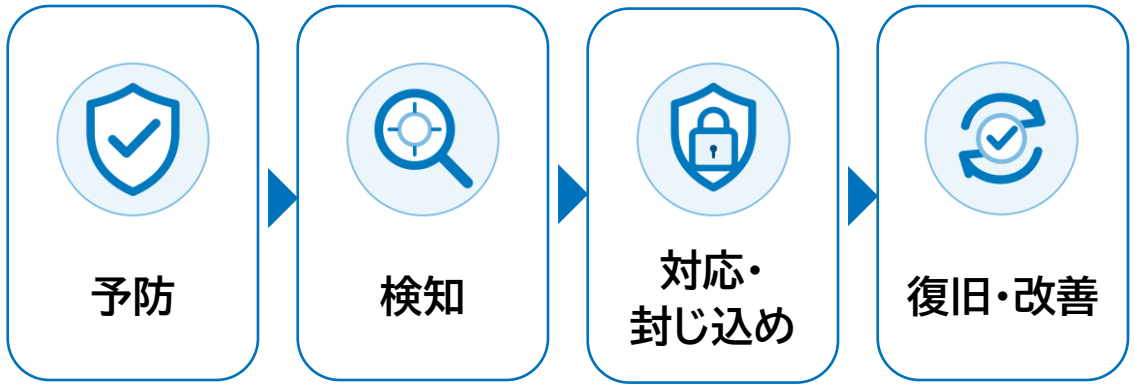
国民生活や他の重要インフラを支える **通信サービスの継続的確保** × 不正アクセスから利用者情報を守る **迅速・大規模なセキュリティ対応** の両立

© NTT, Inc. 2026

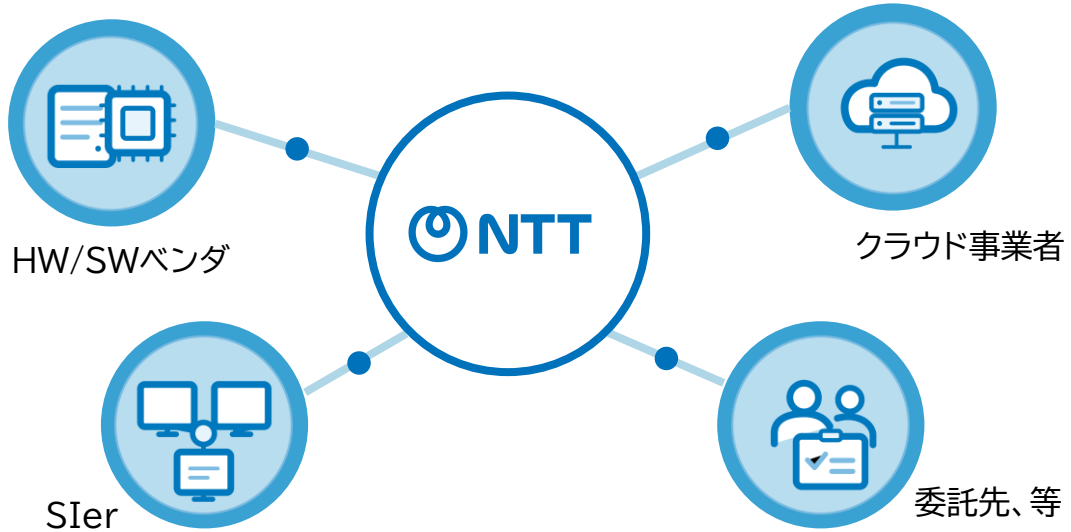
2. NTTグループのセキュリティ対策の基本的な考え方

- 基本的な対策の徹底を土台に、完全な侵入防止は困難との前提で**多層的な対策**を実施
- **サプライチェーンを含めたリスク管理**と**継続的な点検・改善**を推進

多層的なセキュリティ対策



サプライチェーンを含めたリスク管理



基本的なセキュリティ対策の徹底

既知脆弱性への対応 | 適切な設定・構成 | セキュアな設計・実装

© NTT, Inc. 2026

3. 脆弱性対応の考え方

- 多数の脆弱性に一律の基準・期限で対応するのではなく、深刻度・攻撃可能性・サービスへの影響・代替策を総合的に評価し、**リスクベースで対応の優先順位を判断**
- 脆弱性への対処にあたっては、**NW機器ベンダ等を含め連携した対応が必要**

総合的なリスク評価

脆弱性の深刻度（CVSS等）だけでなく、実際のリスクを総合的に評価

攻撃可能性

- 攻撃手法の実証・公開状況
- 実悪用情報（KEV等）
- 外部からの到達可能性

サービスへの影響

- 対象サービス・システムの重要性
- 扱う情報の重要性
- 侵害時の社会的影響

代替策の有無

- アクセス制御
- 監視強化
- WAF等による攻撃遮断

リスク評価に基づき選択

- 即時対応
- 代替策を講じながら対応
- 計画対応

NTTの取組例　最新の脅威・脆弱性情報の継続的な収集・分析 ｜ 脆弱性診断・攻撃者視点でのセキュリティ検証

© NTT, Inc. 2026

4. 通信事業における可用性確保とセキュリティ対応

- 従来は通信サービスの継続を基本として、サービス影響を抑えながら段階的な脆弱性対応を実施
- フロンティアAI時代には、**面的・質的な縮退や、停止・遮断も選択肢に含めてリスクベースで判断**が必要
- 平時から様々なケースを想定し、技術部門・事業部門・運用部門を含む判断態勢を整備することが重要

従来の脆弱性対応

可用性を確保しながら
段階的に脆弱性対応

- 設備の冗長化・分散化
- 段階的な更新・切替え
- 緩和策・監視強化

ITシステムの場合

重大な脆弱性対応として
予防的なサービス停止の実績あり
（例：PHP脆弱性対応）

フロンティアAIによる変化

・対応までの**時間的猶予縮小**
・従来の運用では対応困難なケースも想定

- 悪用までの時間短縮
- 攻撃経路の複雑化
- 対応件数の増大

リスクベースの対応判断

セキュリティリスクと可用性への影響を総合評価

主な判断要素

- 脅威の切迫性
- サービス・設備の重要性
- 緩和策・代替手段の有無
- 利用者・社会影響

サービス継続	面的・質的縮退	停止*遮断

＊停止・遮断の場合の具体的なケースや、ルール整備、社会の理解などの土壌づくりが前提

© NTT, Inc. 2026

5. AIを活用した防御能力の高度化

- フロンティアAIにより、高度なサイバー攻撃のハードル低下、攻撃能力が急速に向上
- **攻撃者側のAI利用を前提に**、AIを活用したセキュリティ対策の高度化を推進

AIを活用した防御能力の高度化

ホワイトボックス診断とブラックボックス診断を両輪で推進



ホワイトボックス診断

ソースコードを解析
潜在的な脆弱性を発見



ブラックボックス診断

攻撃者視点で検証
実際の攻撃可能性を確認

多面的・継続的な検証による防御能力の高度化

AIの先端性と安全性の両立



高性能なフロンティアAIの活用

高度な脆弱性の発見・分析
攻撃者視点・大量高速な検証



ソブリンなAI環境の活用

重要情報の安全な取扱い
安定的・継続的な利用

高性能なフロンティアAIと
ソブリン環境のAIを適材適所で活用

© NTT, Inc. 2026

6. 今後の検討に向けた観点

既存の官民・業界連携の枠組みを活用した情報共有・連携の強化

エコシステム全体でのセキュリティ対応力の強化

© NTT, Inc. 2026


NTT