資料３－２

総務省
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

フロンティアAI時代の
セキュリティ対策と課題

2026年11月24日
ソフトバンク株式会社

© 2026 SoftBank Corp.

アジェンダ

- フロンティアAIがもたらす脅威と現状認識
- ガバナンス・技術的対策に関する自社の取り組み
- 業界全体として取り組むべき基準やルールのあり方
- 政府への期待

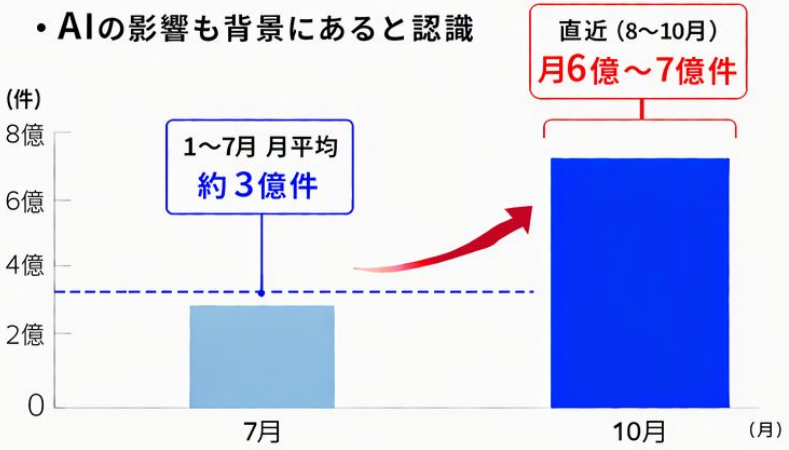
© 2026 SoftBank Corp.

フロンティアAIがもたらす脅威と対応方針

脅威：人が関与できない速さと脆弱性に対する攻撃網羅性
対応方針：①システム再点検と是正、②内容に応じて遮断

偵察行為の件数推移

- 7月までの月平均は約3億件
- 直近は月6億～7億件に増加
- AIの影響も背景にあると認識



- 直近は従来の2倍以上に増加
- 生成AIを含む自動化ツールの拡大が要因の一つと認識

当社の対応方針

AIの脅威に備え、以下を実行

① システム再点検

システム全体を
再点検

- ✓ 脆弱性診断の実施
- ✓ アクセスログの精査
- ✓ 設定・構成の確認
- ✓ 不正侵入の痕跡調査
- ✓ 是正・改善の実施

- ✓ システム全体を再点検
- ✓ 弱点の特定と是正
- ✓ 再発防止策の強化

② 遮断

該当システムへの
外部アクセスを遮断

- ✓ 安全性を確認しながら遮断
- ✓ 影響の拡大を防止

点検と是正のサイクルを継続し、AI時代の脅威に対応

© 2026 SoftBank Corp.

ガバナンス体制

セキュリティが中心となって全社横断で統制

経営層のコミットメント
- 重要方針の決定・監督
- リスク許容度の設定

自社統制の徹底
- 全社共通基準・ポリシー適用
- 継続的な監査・モニタリング

基準と継続評価
- 事業パートナー・委託先にも基準を設定
- 定期評価と改善の徹底

経営層
直接コミットメント／監督

報告・助言
重要事項のエスカレーション

CISO（情報セキュリティ統括責任者）
セキュリティ統制

事業部門	技術・開発部門	セキュリティ部門	法務・コンプライアンス	内部監査部門	その他管理部門
・データ取扱管理 ・業務プロセス管理	・セキュア開発 ・脆弱性管理	・監視 ・インシデント対応	・法令・規制対応 ・契約・統制支援	・統制評価 ・監査・レビュー	・人事・総務・調達 等 ・共通リスク管理

① リスク把握・分類	② 基準適用・契約	③ 評価・モニタリング	④ 改善・是正	⑤ 継続的な見直し
事業・委託先のリスクを特定・分類	セキュリティ・AIガバナンス基準を適用	定期評価・監査・モニタリングを実施	改善計画の実行支援と是正確認	リスク・環境変化に応じ基準を継続的に更新

可視化・標準化・継続評価により、リスクを低減

© 2026 SoftBank Corp.

多層防御

攻撃の高速化・攻撃手法網羅性に対し、多層防御を組み合わせ AIを活用して防御層の追加と精度を向上

リスクベースのトリアージ（優先順位付け）

３つの観点でスコアリングし、対応の優先順位を決定

外部公開性	インターネットからの到達可能性、公開範囲の広さ
攻撃転用の可能性	システム破壊、RCE可能等の攻撃手法の確認
事業・社会への影響	業務停止・収益影響、顧客・社会への波及、法規制・信用影響

総合的に優先度を判定

高リスク	中リスク	低リスク
最優先で対応	計画的に対応	標準対応・監視強化

多層防御の適用（リスクに応じた強度で実施）

上流 → 下流

第1層 回避策（出さない）	・攻撃面の削減（公開最小化） ・脆弱性の未然対策（設計・開発・設定管理）
第2層 緩和策（侵入させない）	・境界防御（WAF/IPS、DDoS防御 等） ・ID/アクセス制御・認証強化 ・マイクロセグメンテーション
第3層 検知・監視（早く見つける）	・EDR/NDR、ログ監視、UEBA ・脅威インテリジェンス活用 ・AIによる異常検知・相関分析
第4層 対応・復旧（被害を最小化）	・インシデント対応（封じ込め・根絶） ・BCP/DR（バックアップ・復旧） ・影響評価・ステークホルダー通知

防御強度：強 ↑ 弱

リスクの高い領域ほど、上流・強い対策を優先的に適用

AI活用（防御側の速度と精度を向上）

脅威検知の高度化
大量ログのリアルタイム分析と異常検知の精度向上

トリアージの効率化
アラートの自動分類・重要度判定で対応優先度を最適化

脆弱性・設定の分析支援
脆弱性情報の要約、影響分析、修正提案を自動化

対応ナレッジの活用
過去事例の検索・要約で初動対応を迅速化

継続的なモニタリングと改善

- 対策の有効性を測定（KPI：検知時間、封じ込め時間、再発件数 等）
- 環境変化・新たな脅威を反映し、定期的にリスク評価と防御強度を見直し

© 2026 SoftBank Corp.

脆弱性管理

影響度をフロンティアAIを使って評価し継続的な是正を行う
従来の評価軸に依拠せずAIがトリアージし優先度を決めている

優先順位の評価軸

- **CVSS等の深刻度**
  CVSSスコア・ベンダ評価 等
- **攻撃転用の可能性**
  システム破壊、RCE可能等の攻撃手法の確認 等
- **外部露出**
  インターネット公開・攻撃可能性 等
- **重要サービスへの影響**
  業務重要度・利用者影響・データ重要度 等

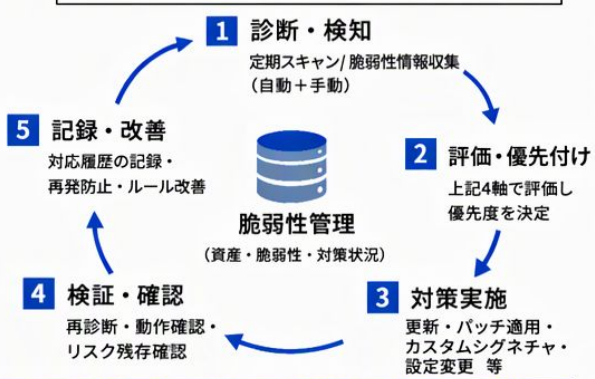
評価の考え方（例）

評価項目	評価基準（例）
深刻度	CVSSスコア High(～) / Medium(～) / Low(～)
攻撃転用の可能性	システム破壊・RCE可能等の攻撃手法の確認 等
外部露出	インターネット公開有無・曝露面の広さ 等
影響度	重要サービス依存度・利用者影響・データ重要度 等

総合スコアに基づく優先度

- P1（緊急）
- P2（高）
- P3（中）
- P4（低）

継続的な診断・更新・対策サイクル



OSSを含む全ソフトウェアを対象に、継続的に実施

AIによるソースコード全体の確認

- 静的解析＋AIレビューで脆弱性・不具合・設定ミスを検出
- コード全体の依存関係・データフローを可視化し、影響範囲を特定
- AIが過去事例・脆弱パターンと照合し、潜在リスクを早期に検出

継続的に繰り返す

新しいAIモデル登場のたびに診断と対策を再精査

インターネット接続箇所へのブラックボックス侵入テスト

- 外部からの実攻撃を模擬し、侵入可否・影響範囲を検証
- 認証・暗号設定・API・管理画面等の設定不備を網羅的に検出
- 診断結果を可視化し、改善計画に連携

新モデル登場・環境変更 → 情報収集・影響分析 → AIコード診断 → ブラックボックス侵入テスト → 脆弱性評価・優先付け → 対策・パッチ適用 → 再診断・検証 → 完了

© 2026 SoftBank Corp.

業界全体として取り組むべき基準やルールのあり方

リスクに応じて選択できる柔軟な仕組みが望ましい
目的・原則にとどめ、技術・手段は事業者が選択

1. 柔軟で選択可能な枠組み

守るべき水準（目的・原則）

- 安全・信頼性の確保
- 利用者の権利・利益の保護
- 事業の継続性確保／社会への影響の最小化

技術・手段（事業者が選択）

暗号化 / 認証強化 / アクセス制御 / データ分類最小化 / 監視・検知 / バックアップ冗長化 / …

リスクに応じて最適な組合せを選択

リスクレベル	特徴	選択の考え方（例）
高リスク	影響度が大きく脅威が高い	・多層防御の組合せ ・強固な認証・暗号化 ・高頻度の監視・監査
中リスク	影響度・脅威が中程度	・バランスの取れた対策 ・重要データの保護を強化 ・必要に応じて追加対策
低リスク	影響度が小さく脅威が限定的	・シンプルな対策で対応 ・標準的なコントロールを適用 ・コスト効率を重視

2. 既存の仕組みを活用し、継続的に実効性を向上

法令
- 個人情報保護法
- 不正アクセス禁止法
- サイバーセキュリティ基本法 等

＋

ガイドライン
- 政府ガイドライン
- 業界ガイドライン
- 国際標準（ISO等）等

＋

社内規定・基準
- 社内ポリシー
- 運用基準・手順書
- 監査・教育 等

業界団体等を通じたベストプラクティスの継続共有・更新

情報収集（脅威・事例・対策） → 分析・評価（知見の整理） → 共有・展開（会員間で共有） → ルール・対策の見直し・更新

継続的な改善サイクルにより、実効性を高める

© 2026 SoftBank Corp.

政府への期待

サプライチェーン全体の強化と、情報共有基盤の整備・運用強化を期待

政府への期待

1



リアルタイム共有・早期警戒の強化

- 深刻な脆弱性情報の入手と情報の共有
- 脅威情報の早期共有体制の拡充
- 発信情報が活用しやすくなる仕組みづくり（MCP/API等）

2



犯罪インフラの無害化の推進

- マルウェア配布、C2サーバー等の遮断・テイクダウン強化
- 国内外の関係機関との連携強化
- 迅速な執行と技術的対応の両輪による抑止力向上

3



サプライチェーンの責任分担・支援

- 商用ソフトウェア供給者の責任明確化とOSSの修正・検証を支援
- 外部連携先やSaaS等に対する侵害の場合の各種対応の効率化の在り方の検討

新たな脅威に対する迅速な対応力を高め、我が国の通信インフラの安全性・信頼性を向上

© 2026 SoftBank Corp.



© 2026 SoftBank Corp.