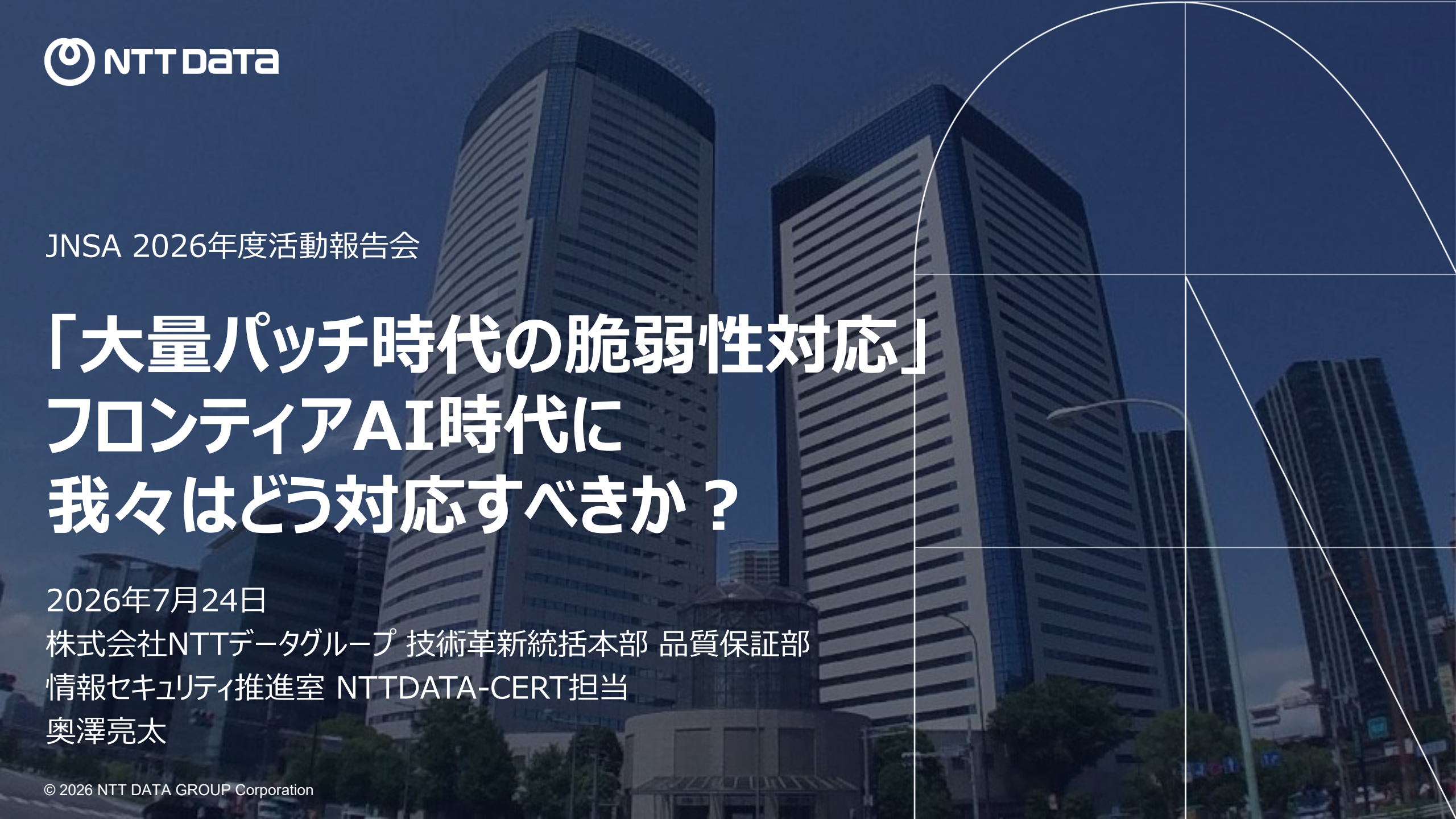


JNSA 2026年度活動報告会

「大量パッチ時代の脆弱性対応」フロンティアAI時代に我々はどう対応すべきか？

2026年7月24日

株式会社NTTデータグループ 技術革新統括本部 品質保証部
情報セキュリティ推進室 NTTDATA-CERT担当
奥澤亮太

1．自己紹介

奥澤亮太（Okuzawa Ryota）

株式会社NTTデータグループ 技術革新統括本部
品質保証部 情報セキュリティ推進室 NTTDATA-CERT

どんな人?

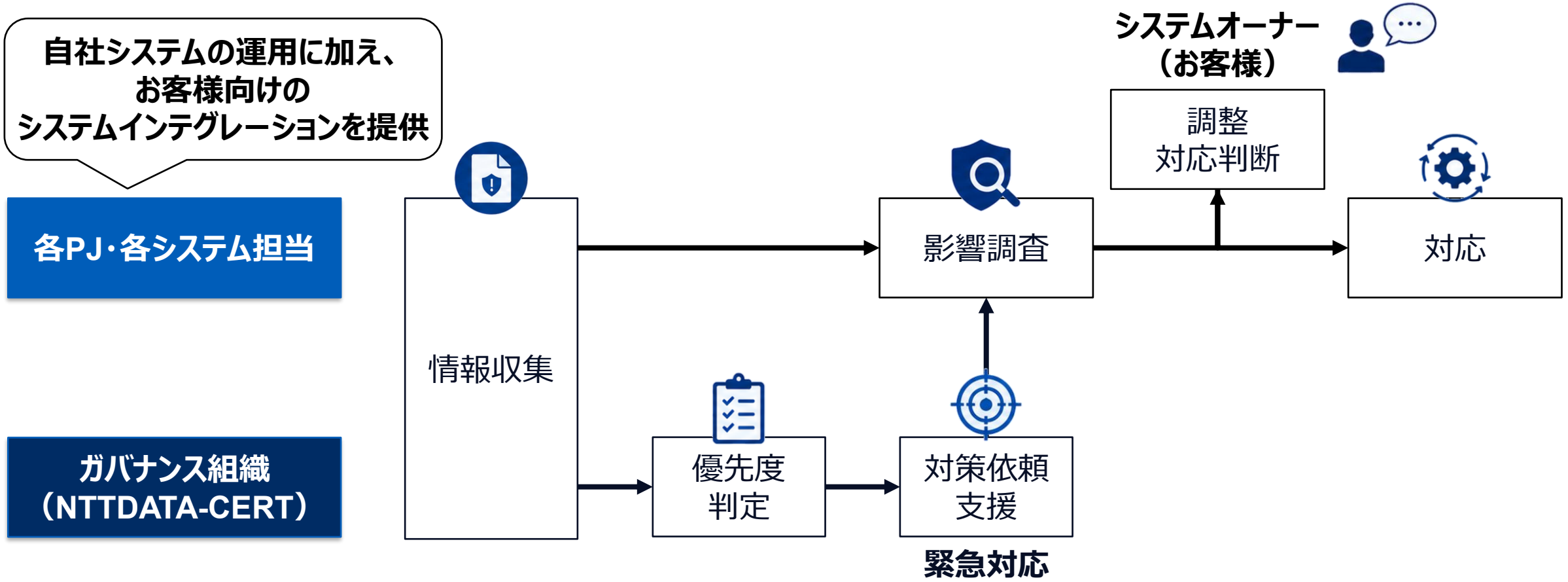
- もともと　官公庁やベンダーで勤務
- 2021年　中途社員としてNTTデータへ入社
  NTTDATA-CERTへ配属
  入社後間もなくLog4Shell公表、
  慣れない環境で右往左往した思い出
- 2023年　組織再編により
  NTTデータグループ（持株会社）配下へ
- 現在、主に日本地域におけるグループ会社全体を支援

何をやっている?

- 主に脆弱性対応管理
  - 脆弱性情報を収集・評価し、緊急対応
  - ここ数年は、VPN・境界装置の対応が多かった
    - Fortinet FortiOS (CVE-2023-27997)
    - Ivanti Connect Secure / Policy Secure
      (CVE-2023-46805 / CVE-2024-21887)
    - Palo Alto PAN-OS (CVE-2024-3400)
  - だんだん忙しくなってきたので、つらいですね
- その他、社内インシデント対応等も担当

2．当社の緊急対応体制

基本的に各プロジェクト（PJ）・各システム担当が脆弱性対応を実施
ガバナンス組織（NTTDATA-CERT）は、緊急対応を要する深刻な脆弱性について、調査・判定・対策依頼・支援する



3．当社の進化：大量の脆弱性をどう捌いてきたか

属人対応から、標準化・自動化・対象特定型対応へ進化

判定基準の設定と自動化により、大量の脆弱性情報の処理が可能になった

属人対応

個別判断
個別調整

基準化

周知・実行管理の
基準を整備

- 社内ルールを通して
  社内の実行体制を確立
- システム台帳も整備

自動化

情報収集、一次判定、低緊急度の
フィルター処理を自動化

- 大量情報処理のターニングポイント
- 脆弱性集約、判定、通知の基盤を整備
  (Vulnerability Handling System : VHS)

体制整備

緊急対応時の
役割・担当者割当、
対応ガイドラインを整備

対象特定型対応

影響可能性のある
対象を早期特定、
個別に対応管理

従来からの積み重ねの上に、優先度判断と対象特定の自動化・省力化を進める

４．具体的なリスクを評価し、優先度に傾斜をつけた対応

優先度を付けてリスクを最大効率で下げる方向性は、合理的かつ依然として有効

- システム側の属性・リスク特性も踏まえて評価するなどが望まれる

対応件数が人的リソースを上回りうる前提で、対応スピードにメリハリをつける

優先度判断の軸

脆弱性情報

- 想定される被害内容
- インターネットからの攻撃可否
- 権限・操作・前提条件の要否

攻撃者にとっての利益

- 攻撃可能なシステムの多さ（普及率）
- 技術的難易度、悪用状況、概念実証コード（PoC）公開状況
- 攻撃で得られる価値の大きさ

資産側・システム側の属性

- システム・情報の重要度、事業影響
- 公開状況・アクセス制限
- 自社の責任範囲・責任の性質

5．システムインテグレーター（SIer）としての悩み：一律統制できない構造

環境・契約・責任分界・変更判断が案件ごとに異なり、
お客様・PJ・ガバナンス組織の役割分担の中で対応を進める必要がある

ガバナンス組織の論点

一律の全社対応指示は現実的ではない
各PJの環境を細部まで把握できない
それでも、各PJで実行可能な対応設計が必要

これまでの進化の方向性で正しいのか？

パッチ適用以外の支援強化が必要か？
遮断・検知・侵害調査など
・環境差の大きな支援は限界あり

各PJ（具体策の実行側）の論点

契約、可用性、費用、停止判断などが
対応上の制約となる
・システム責任者・お客様を巻き込んだ意思決定が必要

優先度判断から対処実行までをどう高速化するか
・根本的な仕組みや役割分担を見直さざるを得ない
可能性

SIerはどこまで踏み込み、ガバナンス組織はどこまで支援すべきか？


NTT DATA