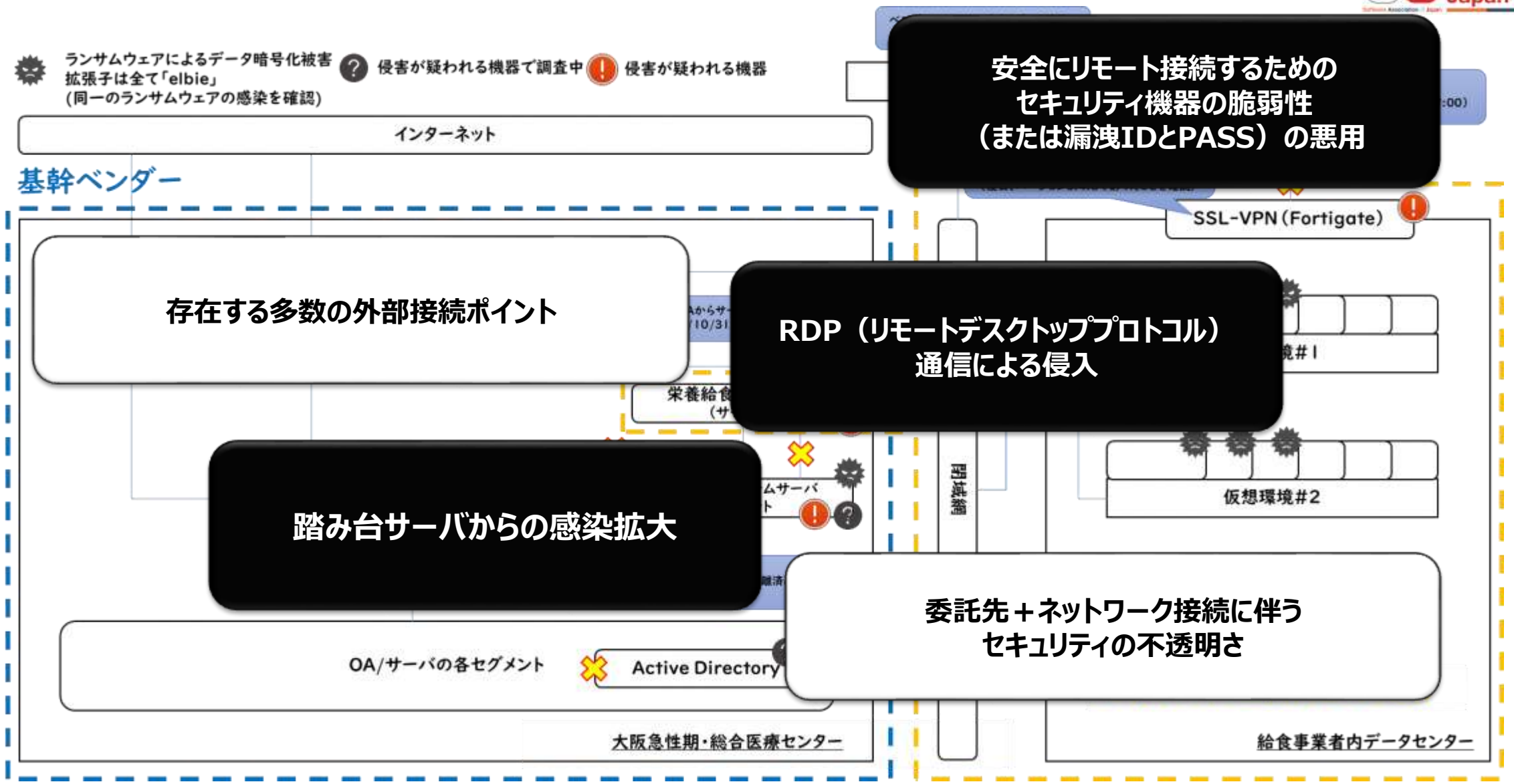
資料４

# インシデント発生時初動対応支援事例及び課題報告
（ソフトウェア協会講演）

2022年12月15日

一般社団法人ソフトウェア協会
理事　萩原　健太

# 大阪急性期Cの攻撃概要と課題



# 大阪急性期Cでの対応

| 日付 | 項目 |
|---|---|
| 22年<br>10月31日<br>(オンライン) | • 厚生労働省より初動対応支援に関する依頼<br>• 大阪急性期・総合医療センター（以下、OGMC）の連絡先情報の入手。<br>• OGMC、電子カルテベンダー等が参加する会議にオンライン参加<br>• OGMC、給食事業者およびOGMCの給食サーバ構築ベンダー等が参加する会議にオンライン参加<br>• 警察庁を経由し、大阪府警察本部（以下、大阪府警）に連絡 |
| 11月1日<br>(現地) | • OGMC、大阪府警、電子カルテベンダー等が出席する会議に参加（定例化）<br>• 給食事業者側の証拠保全のお願い（To 大阪府警）<br>• バックアップ状況の確認のお願い（To 電子カルテベンダー）<br>• Active Directory（AD）のポリシー及び同サーバのログ取得・分析<br>• 復旧対応の優先順位付けと行動の整理<br>• ステークホルダーへの報告のお願い、現状把握、調査方法・方針、復旧に向けた情報整理（To OGMC）など |
| 11月2日 | • 総長、病院長等が参加する幹部会議への参加。状況説明等の実施。<br>• ADサーバや疑わしい端末などの調査継続<br>• フォレンジック端末の選定<br>• 定例会議参加<br>• 関係組織との連携（厚生労働省、警察庁、NISC、大阪府警、電子カルテベンダー（サイバーセキュリティ関連部門（東京）、ネットワーク事業者、セキュリティ事業者）など |
| 11月3日 | • 各種調査を継続（ADサーバや疑わしい端末など）<br>• 給食サーバの調査（検体を含む攻撃ツール等の発見）<br>• 現状整理（現時点での報告書作成）<br>• ローカル端末配布に関する相談対応<br>• 定例会議参加　など |
| 11月4日 | • 電子カルテベンダーとの打ち合わせ<br>• 給食事業者との打ち合わせ<br>• 調査方針の確定会議<br>• 個人情報漏洩調査実施に向けた調整<br>• 大阪府知事向け説明<br>• 定例会議参加　など |

**想定よりも現場が混乱**
**指示者の不在**
**対応できる・経験を**
**有する人材がいない**

初動対応の想定範囲

**遮断**
- ネットワーク、他の端末への感染拡大を防ぐためにすべてを遮断する

**状況確認**
- 状況を把握し、調査や対応方針作成などの初動支援　（→セキュリティベンダーの紹介で本来は終了想定）

**侵入経路の特定**
- 想定される侵入経路はどこか？（ネットワーク機器やプロキシ、ADなどのログを確認する）

**簡易調査**
- ツールを用いた侵害調査や他の不正プログラムなどを探す調査を実施する

**詳細調査**
- 疑わしい端末を選定して、セキュリティ企業に解析やフォレンジック依頼をする

**復旧**
- 基本的には初期化をして再セットアップ／ファイル調査／USBタイプのフルスキャン／複数ベンダーによるフルスキャン）
- 委託先のセキュリティ状況などの確認