日本国内における
機密情報漏えいの現状と脅威

有限責任中間法人JPCERTコーディネーションセンター
早期警戒グループ
情報セキュリティアナリスト

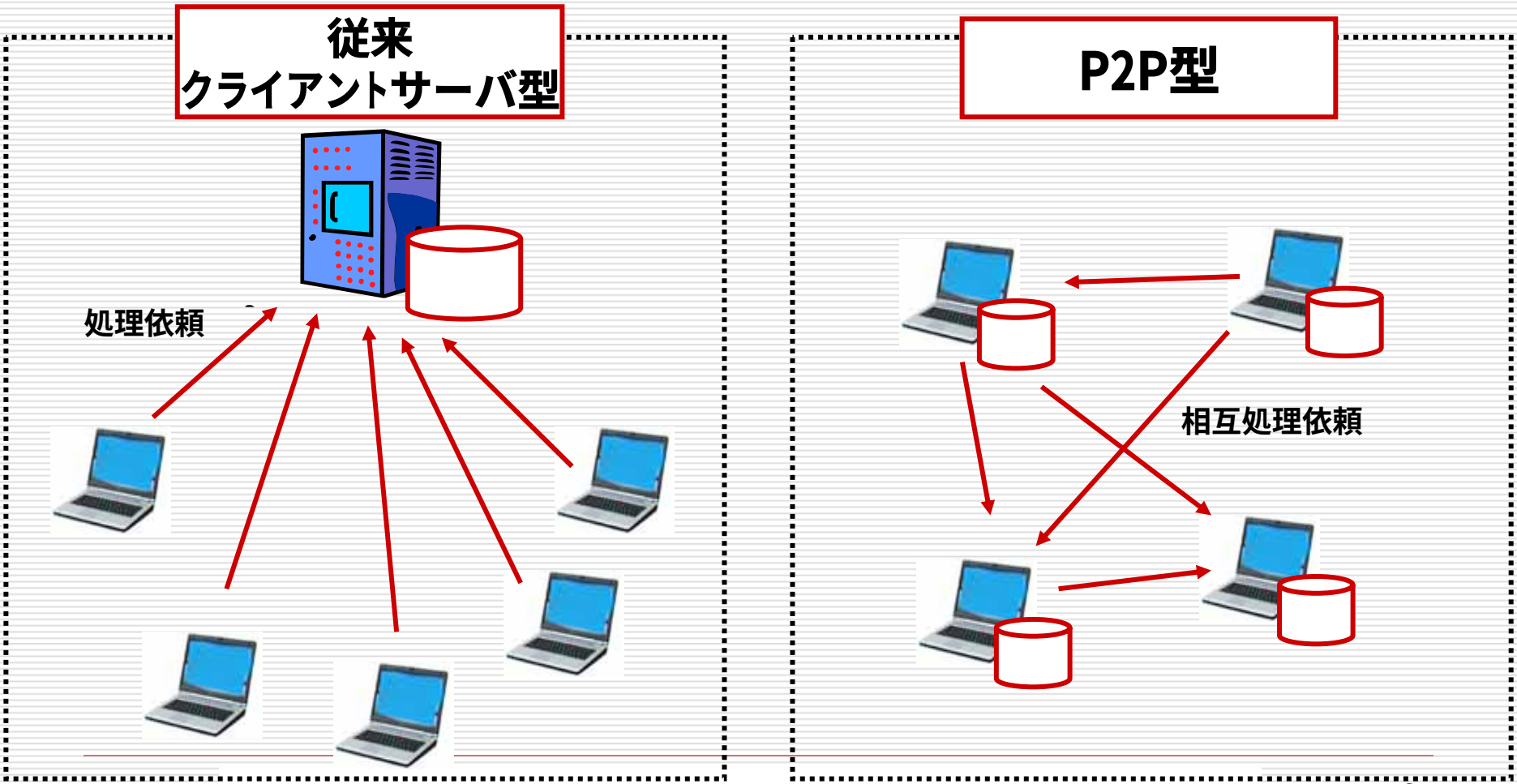
KAMATA Keisuke
鎌田敬介

機密情報漏えいの現状

- P2Pファイル共有ソフトウェアネットワークへの機密情報漏えい事件が後を絶たない
  - 原発情報
  - 中距離地対空誘導弾ミサイルの開発資料
  - 病院の患者情報
  - 取引先企業情報
  - 火力発電所技術資料

多くの場合機密情報を取扱う作業者のPCから流出
データの回収は事実上不可能

P2Pネットワークの構造



中央サーバ非依存の通信、処理分散技術

P2Pファイル共有ソフトウェアとは

- ユーザ同士の「ファイル交換」を目的としたソフトウェアのこと
- 昨今言われているWinny以外にも多数
  - Kazaa, GNUTELLA, etc…
- P2P ネットワークの規模は場合によっては数万台以上
- 流通しているファイルの制御は不可能、または非常に困難

潜在する脅威

1. 悪意のあるプログラムによる情報漏えい
   - 画像や動画を装ったファイル名
   - ダウンロードし、実行することで端末に感染
2. 外部からの攻撃
   - ファイル転送サーバとしても機能する
   - 脆弱性が存在する可能性
   - メンテナンス性の問題
3. 外部への攻撃
   - ボット化することで外部へ攻撃する可能性
4. 通信帯域の圧迫
   - 通信帯域を限界まで利用
   - 組織内・ISPのネットワークを圧迫する

原因と対策

- 主な原因
  - 業務用端末の個人利用
  - 個人端末の業務利用
- 対策
  - 業務利用端末の徹底管理
    - ファイル共有ソフトウェア利用の禁止
    - 機密情報を保存する端末の制限
  - P2Pファイル共有ソフトウェアの通信の禁止
  - 機密情報の暗号化・パスワード
  - 不審なプログラムをダウンロードしない・実行しない

システムでの制御もある程度は可能だが、
業務用データの運用ポリシーやルールなどを
組織として策定し徹底していくことが重要

どのような脅威やリスクがあるのか
潜在している脅威やリスクも含めて
理解した上で運用することが重要

お問い合わせ

- JPCERT/CC
  - 03-3518-4600
  - office@jpcert.or.jp