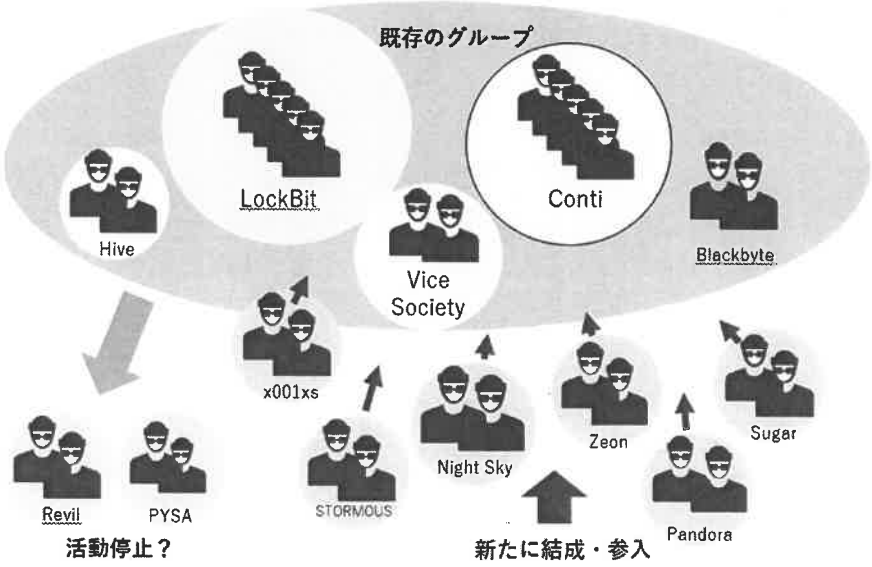
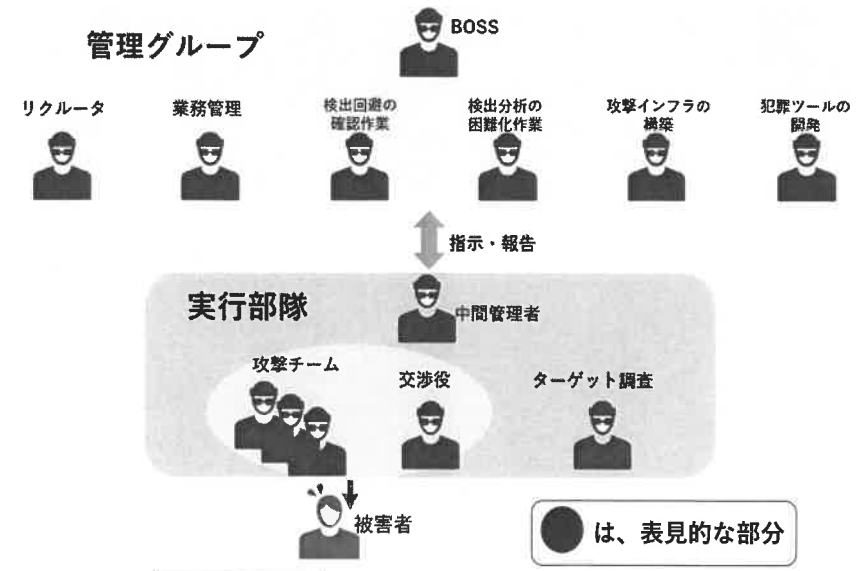
世界的なランサムグループの盛衰興亡



ランサムグループの分裂から見えるもの

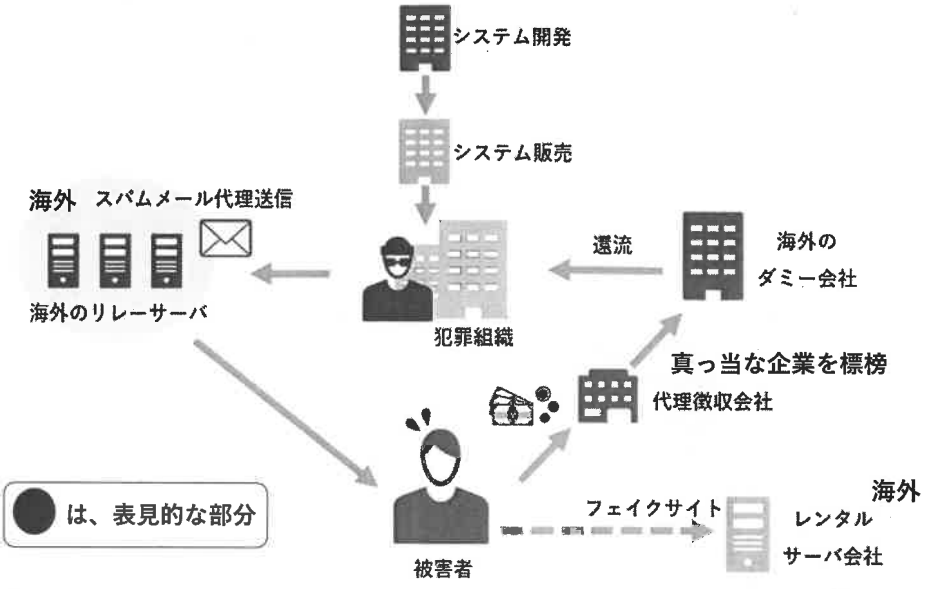
- **エピソード　～　東欧周辺のC2サーバ**
  - 通信系プログラムとしてのウイルスの動向
- **CONTIランサムグループの動向**
  - ２年前に確認されたランサムウェア
  - 現在、全世界で多くの被害を出している標的型ランサムウェア
  - 二重脅迫（暗号化、公開）を行う悪質なグループ
- **ウクライナ侵攻をめぐり内部分裂**
  - 特別軍事侵攻賛成派と戦争反対派が対立
  - 業務で使用していた6万件のチャットデータを公開、流出
  - グループはロシアが中心、反乱側は少数派と思われる
- **ランサムグループの高度な組織化と分業が判明**
  - 組織は、管理グループと実行部隊に分かれている
  - 日本の犯罪組織、犯罪インフラ企業の構造に酷似

ランサムウェアを収益ツールとする犯罪グループ



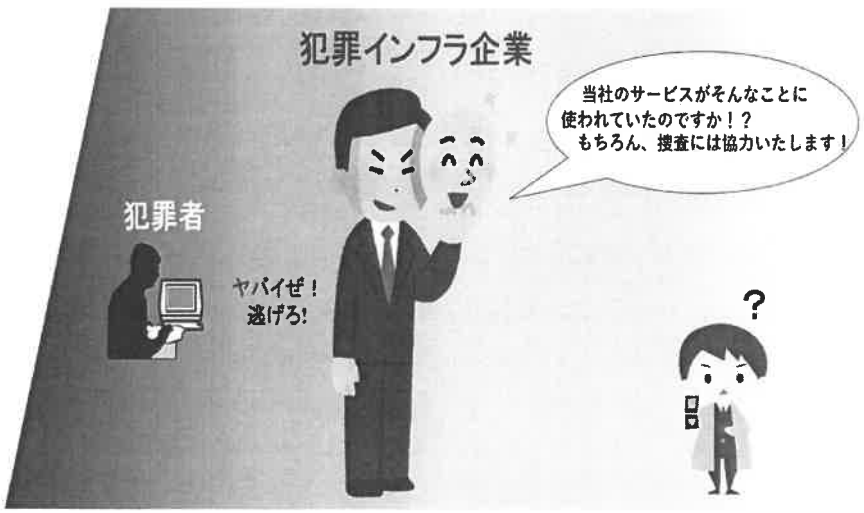
ランサムグループと酷似している日本の犯罪組織
～　通称パクラレ屋（求人名目は社長業）

犯罪の分業化から生まれた日本の犯罪インフラ企業



11 © NEC Corporation 2022

真っ当な一般企業を装う犯罪インフラ企業！



捜査協力要請の境界線に気を付ける必要性！

12 © NEC Corporation 2022