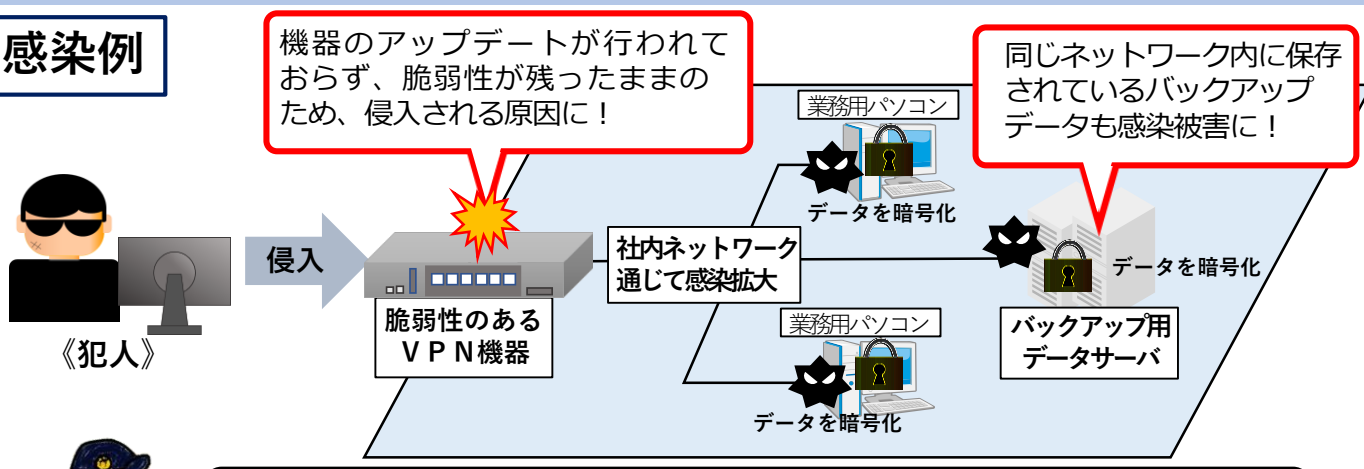
サイバーセキュリティ対策通信

大阪府警察本部サイバーセキュリティ対策課

ランサムウエア に感染！どうする?

脆弱性のあるＶＰＮ機器等から感染！！

感染例



VPN等のネットワーク機器は常に最新の状態を保ちましょう！
バックアップデータはネットワークから切り離して保管を！

データを暗号化されたら？

- 感染端末をネットワークから隔離
- 至急セキュリティ担当者に報告
- 速やかに警察に通報・相談

復号に必要な情報が残っている場合があるので電源は切らない！

有事に備えて予め担当者を決め、連絡体制を確立しておく！

被害の拡大を防ぐためにも、被害を隠して潜在化させない！

暗号化されたデータが復元できることも！？

一部のランサムウェアについては、復号ツールが「No More Ransom(※)」のウェブサイトに公開されており、暗号化されたデータを復号できる場合があります。

https://www.nomoreransom.org/ja/index.html

※　「No More Ransom」は、ランサムウェアの被害低減を目指す国際的なプロジェクトです。

その他サイバー犯罪対策に関する事は
大阪府警ホームページをご確認ください。

※　企業・組織に向けたサイバーセキュリティ講演も実施中！

警察庁 National Police Agency