リモナビが導入された背景と貢献

どこからでも、どこへでも接続する
「背景と貢献」編

※この資料は企業セキュリティ水準の技術を必要とします

背景：現在のセキュリティ情勢

コロナウィルス対策でテレワーク導入が増え、それを狙う攻撃が多発

- 情報セキュリティ事故のうち「テレワーク等のニューノーマルな働き方を狙った攻撃」が組織部門の3位にランクイン　（2020年IPA調べ）

個人情報保護による情報漏洩などへの制裁の世界的強化

- 2021年のGDPRによる制裁件数は400件超（セキュリティの取組み不備でもペナルティ）
  - NTTデータ（2022/11）顧客情報漏洩で 940万円の制裁金　：　日本企業初適用
  - Google 個人情報の利用目的のユーザへの提示不備などで 62億円の制裁金
  - 米アマゾン・ドット・コムは、消費者に対する広告表示がGDPR違反で 970億円の制裁金

  その他多数
- 情報漏洩だけでなく、セキュリティへの取り組み不備で制裁金が課されます
- 日本版GDPR/CCPA 個人情報保護法も欧米に倣って厳格化方向

セキュリティへの取り組み強化は社会的義務。企業存続の必須条件に

情報漏洩による損出が、「社会的制裁」に加え「巨額制裁金」まで

背景：リモートワーク社会の新たな脅威

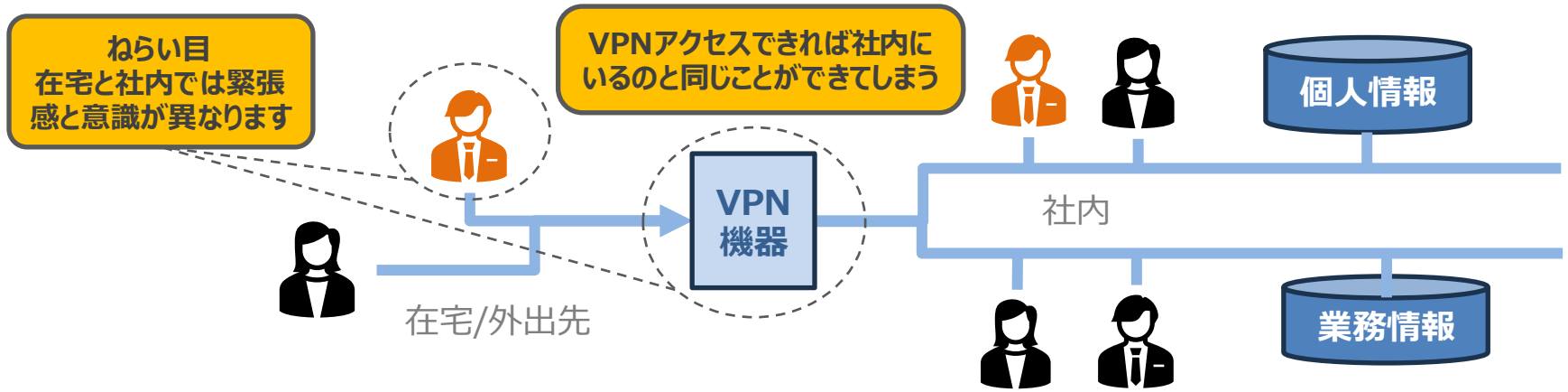
テレワーク環境で利用されるVPNが狙われている

- 2020年8月、米パルスセキュア社製VPN装置の脆弱性を利用した不正アクセスが発生し、国内外900社、国内大手企業38社が被害を受けました。
- 2021年10月、米Fortinet社製VPN装置の脆弱性を利用した不正アクセスが発生し、徳島県のつるぎ町立半田病院で電子カルテ一切が利用できなくなりました。

なぜVPNが狙われるのか？

VPNを日本語にすれば仮想私設網。つまりこの網に侵入できてしまえば、あとは**社内で作業しているのと同じことが全て、無制限にできてしまう**からです。

侵入による犯罪リスクに対して、リターンが極めて大きいからなのです



目的：狙われるVPNからの脱却

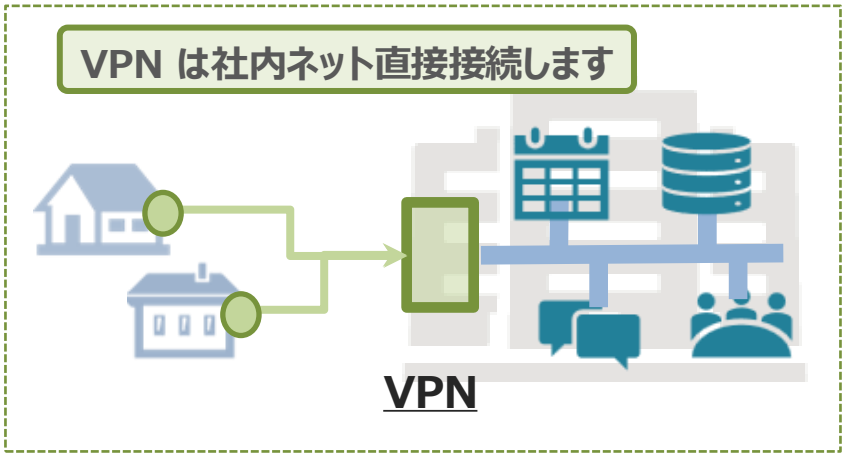
社内と同じネット環境が得られるVPNの生産性・効率は無視できません

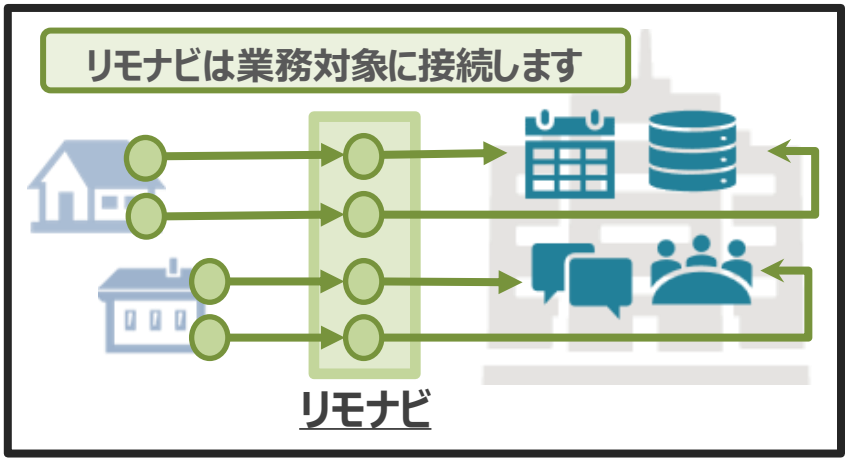
同じネット環境は提供せずとも、同じ業務環境をするならどうか？

ネット環境を提供するのではなく　攻撃対象のVPNはありません

必要なシステムのみの接続を提供　ML感染でも影響範囲を限定

侵入によるリターンを縮小　**必要な業務操作は確保**





VPNでないと困難な作業も Raw TCP|UDP通信をサポートしているため、ほぼ全てのシステム管理が可能です

◆SSHのターミナル接続、リモートデスクトップ接続で問題なし　◆クラサバ・システムも TCP|UDP通信提供で問題なし

貢献：リモナビの社会貢献

ロ VPNとは異なるリモート接続環境の社会提供

- VPNは有益なリモート接続であり、リモナビはそれを否定しません。
- **VPNとは異なるリモート接続を提供しているのです。**
  - **保守・運用会社が、お客様環境の調査・操作・保守をする場合、リモナビは最適です。**
  - **会社ではなく、保全業務など外出先で利用する端末への接続もできるのです。**
  - **IoTなどのデータをプライベート環境に収容する場合、リモナビは最適です。**
  - **※ リモナビは、限定された接続先、業務対象に接続するのに最適なのです。**

ロ 実用性とセキュリティを両立した経済化

- 知識も導入機器も必要とせず、**リモナビ**だけで実現できるリモート接続
  - VPN導入には敷居が高い「小企業」「フリーランス」などでも利用できるリモート接続
  - 容易には実現できない「家の端末」や「外出先での端末」にリモート接続できるのです
- **「個人｜小企業向け」では月額数千円で利用可能**
- 「エンタープライズ向け」では高度なACLの他、**セキュリティ・インシデント管理**や**セキュリティ検査機能**など総合的なセキュリティ機能が提供されます。