ランサムウェアとは？
～医療従事者向け～

長崎県警察サイバー犯罪対策課

サイバー犯罪対策課公式キャラクターの私たちが解説していきます。

ランサムウェアとは？

金銭を脅し取ることを目的とした不正プログラム

感染すると・・・

- パソコン内のデータが暗号化されて開けない。
- 画面がロックされて使用不能になる。

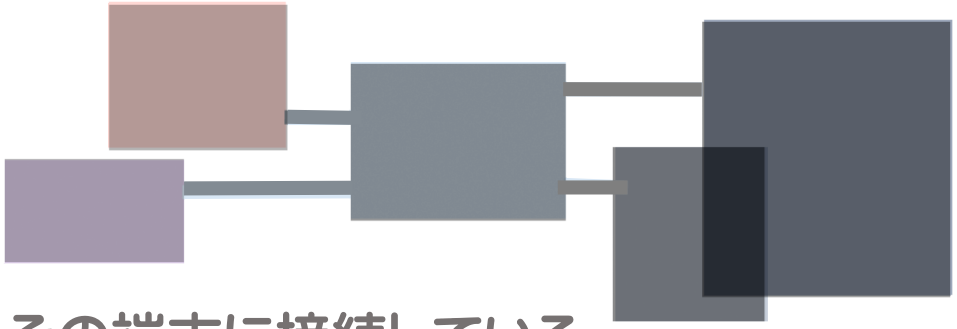
攻撃者からは・・

画面ロックや暗号化の解除と引き換えに

「身代金」を要求される

Ransom（身代金）と
「Software（ソフトウェア）を
組み合わせた造語だよ。

感染は病院全体に影響も・・



○感染した端末（パソコン等）だけではなく、その端末に接続しているハードディスクやUSBメモリー等のファイルも暗号化されます。

○病院内のネットワーク上で共有しているファイル等も暗号化されるおそれがあります。

つまりは・・

業務やサービスの停止による、患者や取引先企業からの

信頼失墜

取引先企業からの信頼失墜・・

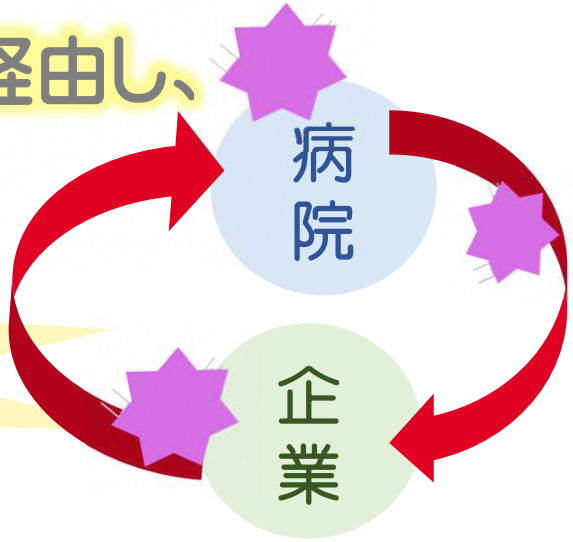
サプライチェーン → 商品の調達から消費に至るまでの<u>一連の流れ</u>

サプライチェーンの流れに病院以外の企業

が関わっている場合・・

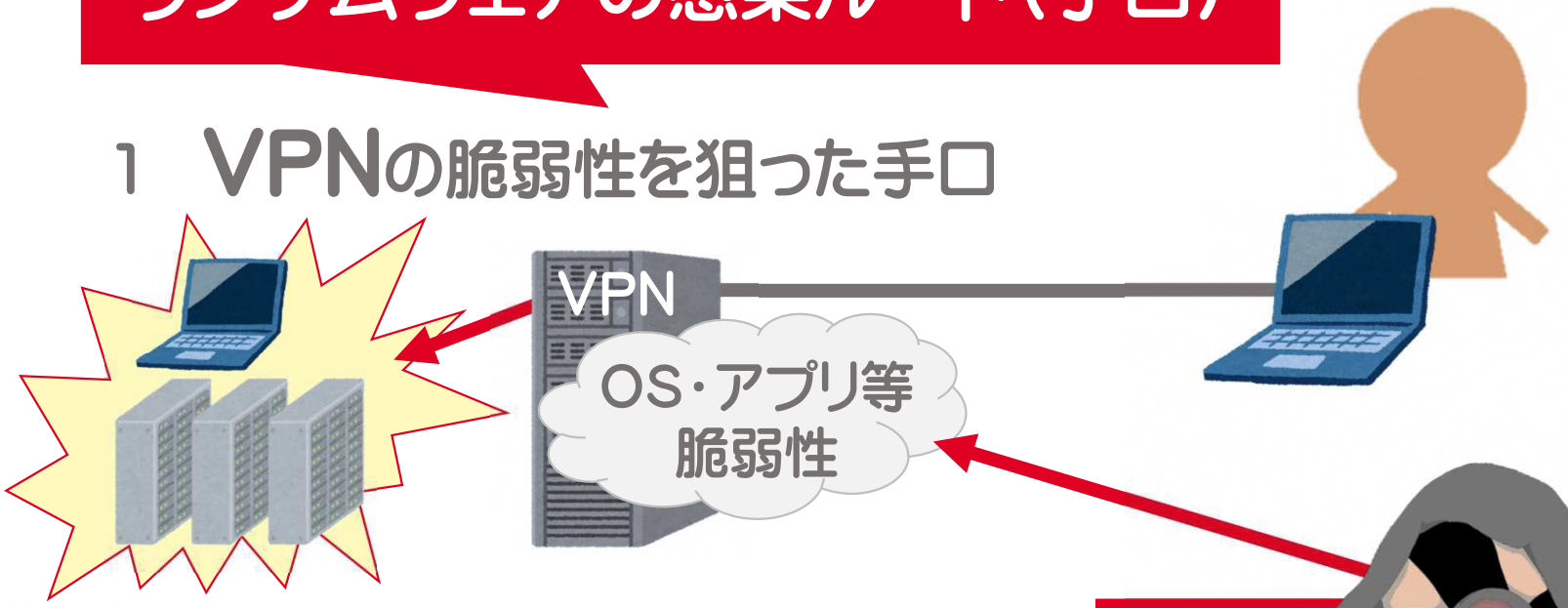
病院がランサムウェアに感染することで、病院を経由し、
取引先企業にも影響を及ぼす。

サプライチェーンリスク

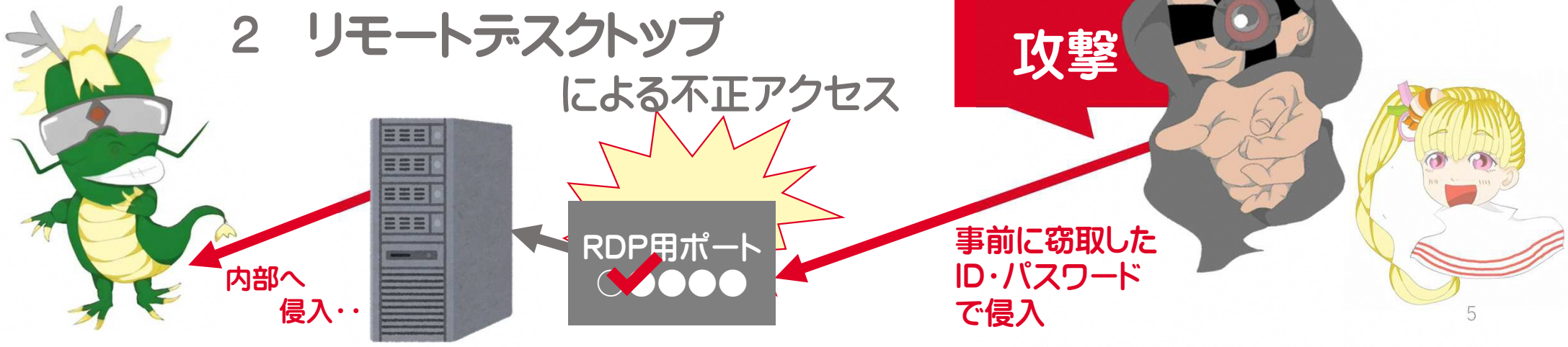


ランサムウェアの感染ルート（手口）

1　VPNの脆弱性を狙った手口

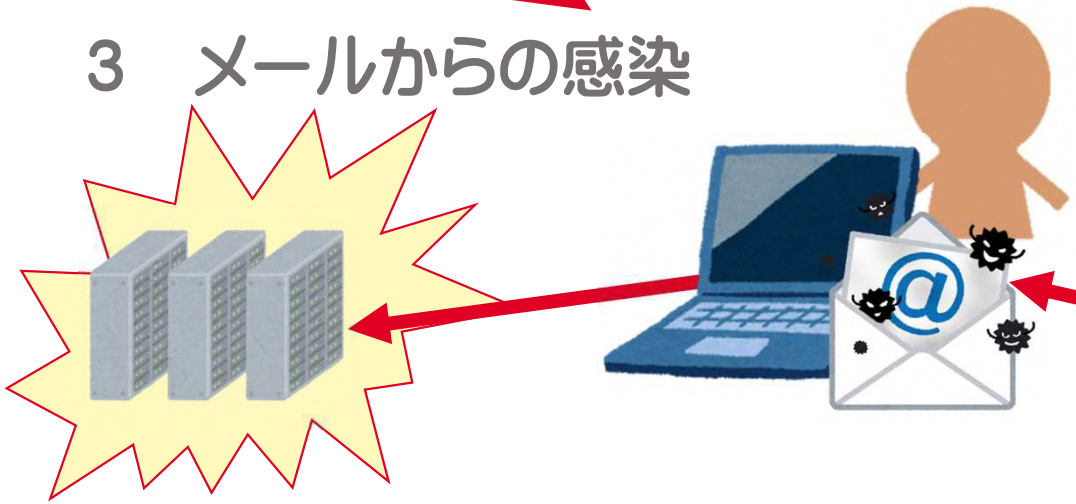


2　リモートデスクトップ
による不正アクセス



ランサムウェアの感染ルート（手口）

3　メールからの感染



4　Webサイトの脆弱性

もし、ランサムウェアに感染したら・・・
皆さんはどうなってしまうと思いますか？

被害に遭ってしまうと・・


システム停止により
業務が停止
診療行為不可
→命の危険性
信用失墜
関係取引先等への影響
者の個人情報など
情報流出の可能性
システムの復旧作業のほか
・問合せ・クレームなどへの対応
・院内の疲弊、不平不満、不安感

事例①

被害企業：　徳島県の病院
発生日　：　2021年10月

発覚した理由

病院内の十数台のプリンタから英文の「犯行声明」が印字された。

被害

電子カルテ利用不可

外来会計、不可

医療サーバダウン

被害額　数億円以上　逸失利益数十億円

通常診療までに掛かった日数　65日間

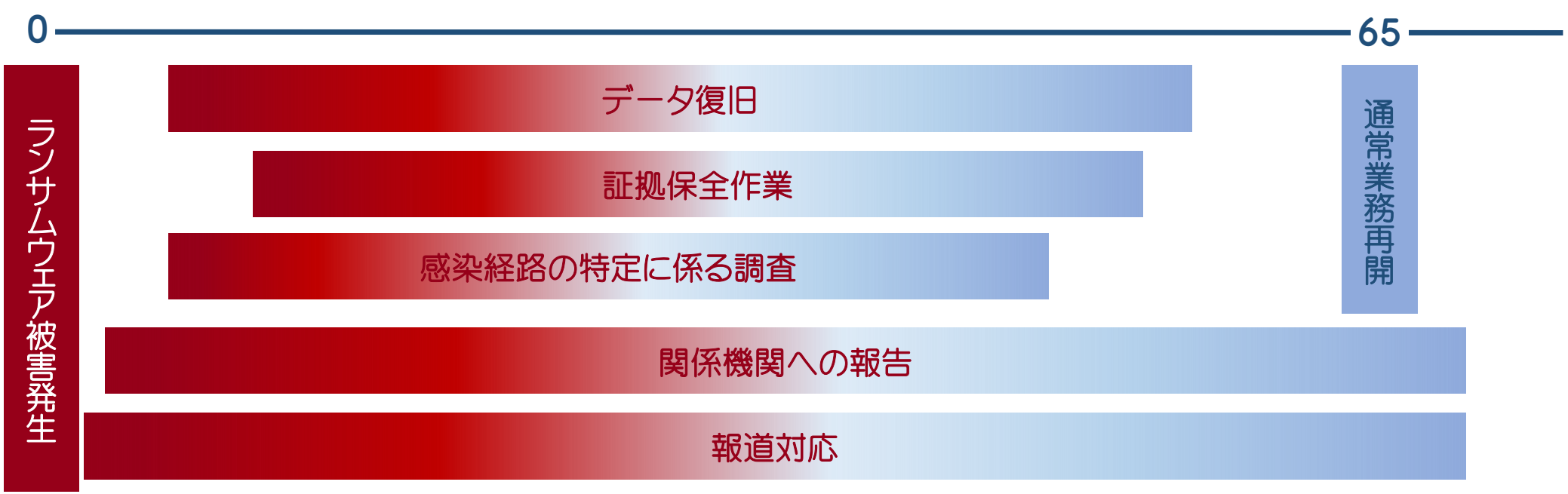
暗号化された電子カルテデータ　約8万5千人

もしも・・

○約8万5千人の個人情報が暗号化

○数億円の損失

○65日間、通常の業務が行えない・・



原因

対策が不十分だった？

▲5桁の短いパスワードで設定できるようにしていた。
⇒　推測されやすい

▲パスワードを何度間違えてもロックしない設定だった。
⇒　何度でもログイン試行できてしまう。

▲誰のパソコンからでも、システム内部を操作できた。
⇒　どのユーザでもアクセスを許可していた。

など、他にもセキュリティ対策が不十分だった。

事例②

被害企業：岡山県の医療センター
発生日　：2024年5月

発覚した理由

「暗号化させている。唯一の方法はここに連絡することだ。」のメッセージを見つけた。

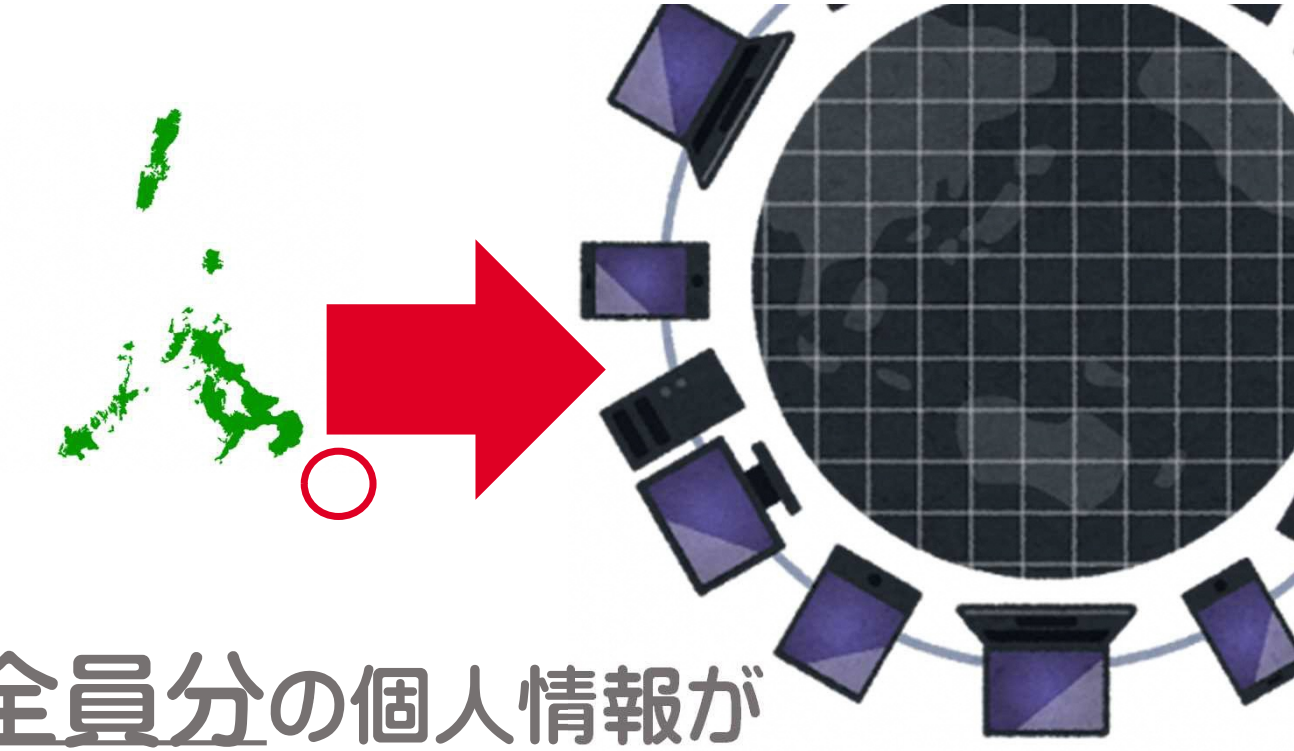
被害

氏名や住所　病棟会議の議事録など、

過去10年分のデータがダークウェブ上に漏えい

漏えいした個人情報　約4万人

もしも・・



4万人って・・

雲仙市民、ほぼ全員分の個人情報が
世界中に流出するようなものです。

※2024年4月調査（公益財団法人国土地理協会）　4万935人

原因

何で侵入された？

▲VPN機器の脆弱性から侵入された。

⇒脆弱性があることを認知していたにも関わらず、
1年間対応していなかった。

VPN機器とは？

他者で共用しているインターネット回線内に仮想的に専用回線を設け、
オンラインデータを第三者から保護するサービス

事例③

被害企業：　出版会社とIT関連企業
発生日：令和6年6月

発覚した理由

複数のサーバにアクセスできない障害が発生

被害

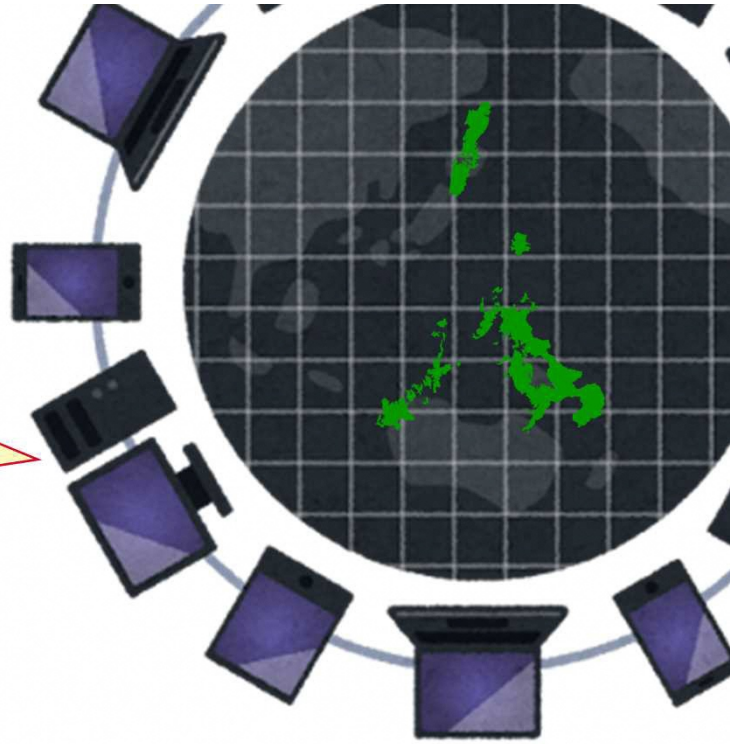
出版事業の流通が減少　動画配信の停止　情報流出

調査、復旧費用等で30億円を超える損失

1.5テラバイトのデータ（うち個人情報　約25万4千人）

もしも・・

○ 30億円の損失



○ 25万人分って・・

佐世保市民の全員分を上回る個人情報が
世界中に流出してしまったようなものです。

※2024年4月調査（公益財団法人国土地理協会）　23万4,504人

原因

なぜ情報漏えいした？

フィッシングなどの攻撃により従業員のアカウント情報が窃取されたことにより、社内ネットワークに侵入された。

⇒　ランサムウェアの実行、個人情報の漏えいにつながった。

ランサムウェアへの対策

○経営者

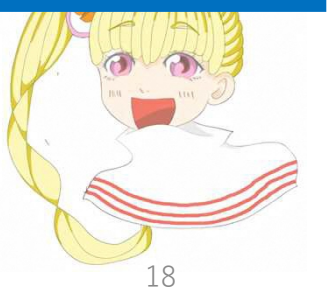
・インシデント対応体制の整備
　CISO等、専門知識を持つ責任者を配置
・CSIRTの構築

・複雑なパスワード
・多要素認証
　を活用しましょう！

○システム管理者・従業員

・認証情報（ログインするための情報）の適切な管理
・オフラインバックアップの作成
　⇒ネットに繋がっていない場所へのデータ保存
・VPN機器の更新等
　⇒機器の提供元から新しいバージョンを取得
・OSを最新の状態に保つ
　⇒OSとは、Windows、MacOS等のことです。

所有している機器の
最新情報は常に確認を！



ランサムウェアに感染してしまったら・・【対応】

・感染した端末をネットワークから隔離

・セキュリティ担当者への迅速な報告

・感染した端末の
電源を落とさない！再起動は行わない！

・適切な報告・連絡・相談
各都道府県警察への相談

警察では、サイバー事案に関する通報・相談等を
受付けています！↓
【警察庁ホームページ】
https://www.npa.go.jp/bureau/cyber/soudan.html

一度ご覧に

もしかした

警察では、サイバー事案に関する通報・相談等を
受付けています！↓
【警察庁ホームページ】
https://www.npa.go.jp/bureau/cyber/soudan.html

ランサムウェアに感染してしまっても・・

身代金を支払わないで下さい！

・身代金を支払ってもデータの復元や情報流出を防げるとは 限らない。

END

皆様おつかれさまでした！