サイバーセキュリティ通信 Vol.11

令和４年３月

長崎県内でランサムウェア被害が発生！

長崎県内の介護施設で、ランサムウェア被害が発生し、サーバ内のデータが暗号化されてしまいました。

このほかにも、ランサムウェアの前兆にもなり得るEmotetの被害も散見されています。

世界情勢が不安定なことと直接的な因果関係があるかどうかは不明ですが、長崎県内でもこのような被害が発生していますので、自社のシステムのセキュリティ対策を今一度見直すと共に、従業員へのセキュリティ教育の再徹底をお願いします。

１　どのような被害だった？

介護施設で運用しているサーバ内のデータが暗号化され使用できなくなりました。

サーバの管理会社が、リモートデスクトップを利用して当該サーバをメンテナンスしていましたが、このリモートデスクトップに対し、攻撃者は総当たり攻撃を仕掛け、介護会社のサーバに侵入したと思われます。

２　リモートデスクトップとは？

離れた場所にあるパソコンの遠隔操作ができる機能のことで、テレワークなどでもよく利用されています。

３　どんな点に注意したらいい？

①　リモートデスクトップの管理強化

- 多要素認証を活用しましょう。
- 総当たり攻撃の被害に遭わないよう、パスワード入力上限回数を設定しましょう。

②　アクセス権限の最小化

- システムにアクセスできる人を限定しましょう。
- ユーザーごとに、アクセスできる範囲を必要最小限にしましょう。

③　バックアップの取得

- 定期的にバックアップを取っておきましょう。
- バックアップは適切に保管しましょう。せっかくバックアップを取っても、ネットワークからアクセスできる状態のままだと、バックアップも暗号化されて使用できない状態になってしまうおそれがあります。

  バックアップ取得後は、バックアップ媒体はネットワークから切り離しましょう。

これらの点について、自組織のシステムを確認してください。システム構築を他社と契約している場合は、契約先に確認してください。

４　その他注意点は？

ランサムウェアは、リモートデスクトップ以外にも、VPNの脆弱性やメールからも感染する可能性があります。次のことにも注意してください。

①　インターネット接続制御装置の脆弱性の確認

- VPNやゲートウェイなどのインターネットとの接続を制御する装置に脆弱性がないか確認しましょう。
- 脆弱性がある場合は、セキュリティパッチを迅速に適用しましょう。

②　組織内への周知

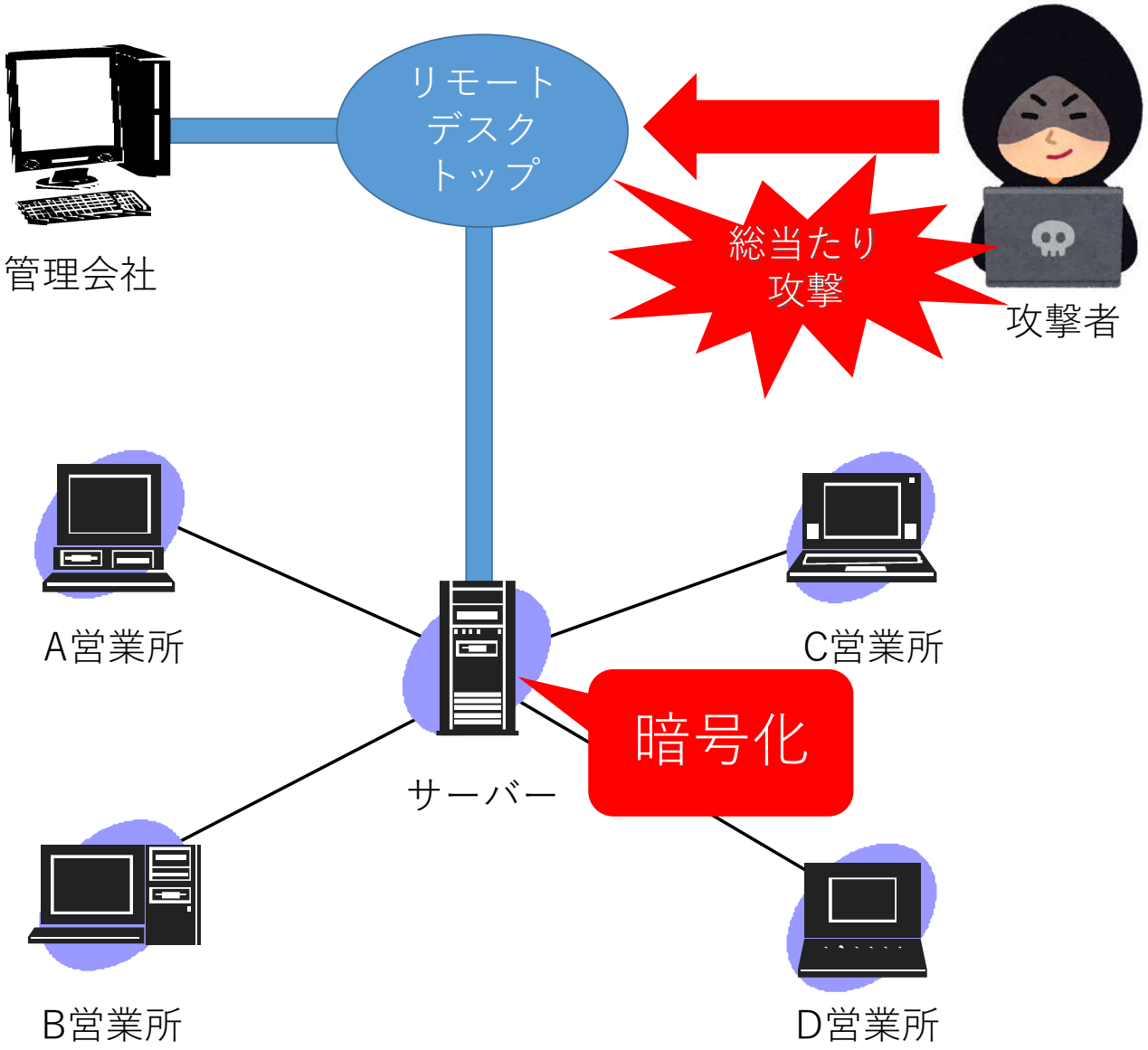
- メールの添付ファイルを不用意に開かない、URLを不用意にクリックしない、ということを周知しましょう。
- 不審なファイルを開いてしまった場合等には、セキュリティ担当部門に即座に連絡・相談することを周知しましょう。

長崎県警察本部サイバー犯罪対策課
095-820-0110（3451・3452）
ﾒｰﾙｱﾄﾞﾚｽ e103107@police.pref.nagasaki.jp

サイバー犯罪対策課
公式LINEアカウントで
情報配信中！
友だち登録お願いします！

@387ojopi

＜今回の事件の手口は？＞



介護施設が運用していたシステムのメンテナンスを行っていた管理会社は、当該システム内のサーバをリモートデスクトップを利用してメンテナンスしていました。

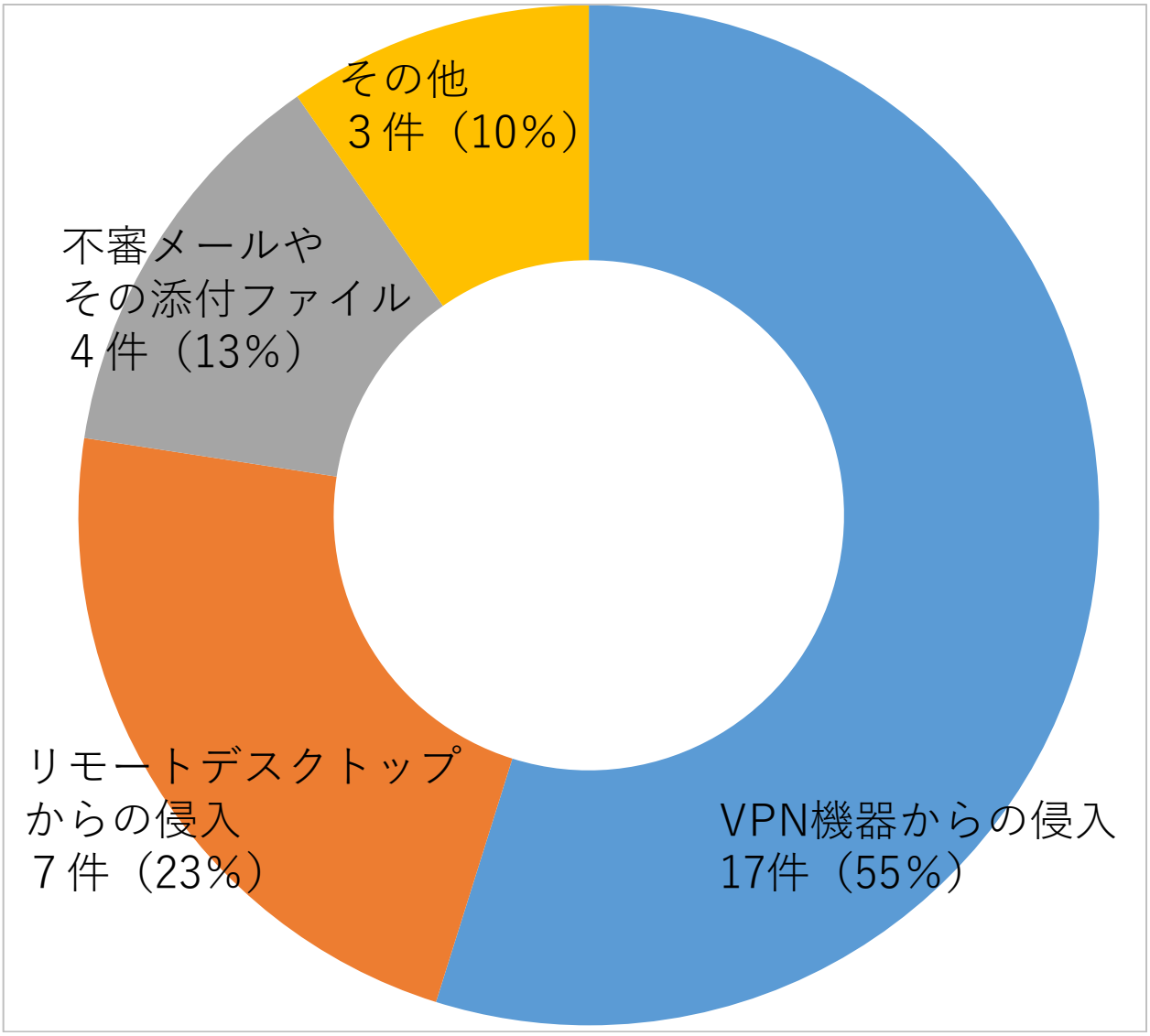
そのリモートデスクトップに対し、攻撃者は総当たり攻撃を仕掛け、介護施設のサーバー内に侵入し、サーバー内のデータを暗号化したものと思われます。

※　総当たり攻撃（ブルートフォースアタック）とは

パスワードや暗証番号などの秘密情報に対して考えられる全ての組合せを試行することによって、システムに侵入する攻撃です。

キャッシュカードやマイナンバーカードの４桁のパスワードを３回連続で間違えるとロックされるのは、この総当たり攻撃対策のためです。

＜ランサムウェア感染の経路は？＞



警察庁の「令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について」によると、有効回答31件のうち、VPN機器からの侵入が17件で全体の55%を占め、次いでリモートデスクトップからの侵入が７件で全体の23%を占めており、テレワーク等の普及を利用して侵入したと考えられるものが全体の８割近くを占めています。

＜被害に遭わないためには？＞

繰り返しになりますが、被害に遭わないために、次のことに注意しましょう。

【今回の被害のようなケースを防ぎたい】

① リモートデスクトップの管理強化
- 多要素認証を活用しましょう。
- 総当たり攻撃の被害に遭わないよう、パスワード入力上限回数を設定しましょう。

② アクセス権限の最小化
- システムにアクセスできる人を限定しましょう。
- ユーザーごとに、アクセスできる範囲を必要最小限にしましょう。

【代表的な手口から被害を防ぎたい】

① インターネット接続制御装置の脆弱性の確認
- VPNやゲートウェイなどのインターネットとの接続を制御する装置に脆弱性がないか確認しましょう。
- 脆弱性がある場合は、セキュリティパッチを迅速に適用しましょう。

② 組織内への周知
- メールの添付ファイルを不用意に開かない、URLを不用意にクリックしない、ということを周知しましょう。
- 不審なファイルを開いてしまった場合等には、セキュリティ担当部門に即座に連絡・相談することを周知しましょう。

しかし、どんなに万全な対策を施しても、被害に遭ってしまうこともあります。
必ず、バックアップを取得しましょう。

※ バックアップの取得
- 定期的にバックアップを取っておきましょう。
- バックアップは適切に保管しましょう。せっかくバックアップを取っても、ネットワークからアクセスできる状態だと、バックアップごと使用できない状態になってしまう可能性が高くなります。

これらの点について、自組織のシステムを確認してください。システム構築を他社と契約している場合は、契約先に確認してください。