～二重脅迫型ランサムウェアの予防と対処について～

2019 年頃から、企業のネットワークに侵入し機密情報を窃取したのちに、パソコンやファイルサーバのファイルを暗号化し、暗号化ファイルの復旧と窃取した情報の暴露を止めるための身代金を要求する、二重脅迫型ランサムウェアの被害が発生し始めました。2020 年以降大企業が被害に遭い、高額な身代金を要求されたことが大きく報道されました。

二重脅迫型ランサムウェアの被害は増加の一途をたどっており、2021 年 6 月には、世界で 1 週間あたり 1,210 件の被害が発生しました。（出典：Check Point Software Technologies『Ransomware attacks continue to Surge, hitting a 93% increase year over year』）
また、2021 年の身代金支払い総額は 2 兆円に達するとみられています。

「うちは暴露されて困るような機密情報はないし…」と思われるかもしれませんが、攻撃者は、大企業を直接狙うのではなく、サプライチェーンを構成している、攻撃しやすいセキュリティ対策の甘い中小企業に対象を広げており、日々様々な企業で不正アクセスを受けたとのニュースが報道されています。

外部からの侵入防止に関して、セキュリティ対策を全くとっていない状況も見受けられます。そのような環境では、サイバー攻撃を受けていないのはたまたま攻撃者の網にかかっていないだけなのです。

二重脅迫型ランサムウェアへの最低限の予防と対処について記載しますので、確認・対策を行ってください。

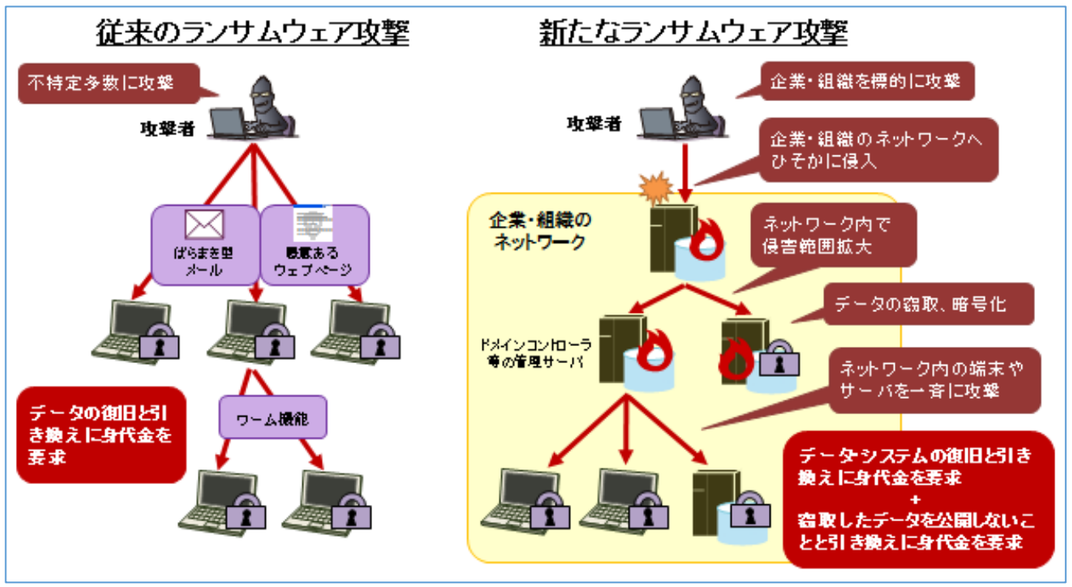


図１　従来の／新たなランサムウェア攻撃の差異

（出典：IPA（独立行政法人情報処理推進機構）　『【注意喚起】事業継続を脅かす新たなランサムウェアについて』）

（１）侵入予防…＞＞＞

・まずは、自社のインターネットの出入口を確認してみましょう。（簡易な調査）

➢ **“SHODAN”で自社のインターネット出入口が外からどう見えているか調べてみる。**
（詳細は「（5）SHODAN サンプル」へ）

- 自社のインターネットグローバル IP アドレスを確認する。
社内の自席から https://www.cman.jp/network/support/go_access.cgi にアクセスし「あなたの利用している IP アドレス」を確認する。
- https://www.shodan.io にアクセスし、「あなたの利用している IP アドレス」に表示されたアドレスを入力し、検索する。
開いているポートや出入口にある機器の脆弱性が表示される。（IP アドレスは住所、ポートは扉に該当する。）

・他にも出入口がないか確認しましょう。（簡易な調査）

➢ **自社のインターネット出入口の IP アドレス以外で、社外から社内に接続できる環境がないか確認する。**

- 侵入される入口は “RDP（リモートデスクトップ）” や “インターネット VPN” がほとんど。外部から社内に接続できる環境があれば、攻撃者もそこを狙う。
- 他の出入口の IP アドレスが見つかったら、同じように“SHODAN”で検索する。

・対策（簡易な対策）

➢ **出入口のセキュリティ強化：ポートを閉じる／制限する／脆弱性を無くす**

- SHODAN の検索結果画面の「Open Ports（ポート）」と「Vulnerabilities（脆弱性）」を見る。「No results found」または「Open Ports 80 443」しか表示されなければ一安心。
- 危険なポートはできるだけ閉じる：21,23,79,137,138,139,445,512,513,2049,3389 等。
- ポートを閉じられない場合：接続を許可する IP アドレスを制限するなどの対策をとり、第三者が接続できる状態にしない。
- 脆弱性が表示される場合：インターネット出入口にある機器のソフトウェアを最新にする。
- 危険性の判断や対処の方法がわからない場合は、インターネット出入口にある機器の運用を委託している会社に相談する。

・調査（本格調査）

- **セキュリティ専門会社によるペネトレーション（侵入）テスト**
  - 専用のツールや高度な知識を有する専門家により実際に侵入や攻撃を試みる。
  - 費用　数十万円～（自動テストツール）　百万円～（ホワイトハッカーによる実際の攻撃と同様のテスト）

・対策（本格対策）

- **セキュリティ専門会社によるアセスメント・アドバイス**
  - ペネトレーションテストの結果や、ネットワーク環境や機器構成の詳細の確認を行ってセキュリティリスクを見える化し、対策のアドバイスを受ける。
  - 費用　数百万円～

（2）感染予防…＞＞＞

- **中小企業向け「サイバーセキュリティお助け隊」**
  - https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html
- **EDR（ふるまい検知型ウイルス対策ソフトウェア）の導入**
  - ランサムウェアによる暗号化防止
  - 社内に侵入するためのバックアドアを仕掛けるマルウェアの感染防止
- **Windows Active Directory ドメイン管理者の権限管理**
  - ローカル管理者権限を与えている場合は外す。ドメイン管理者権限を乗っ取られたとしても、できることを制限する。

（3）攻撃に備えて実施しておくべきこと…＞＞＞

- **バックアップ取得と復旧訓練**

  ランサムウェアに感染した場合、バックアップもオンラインのものは暗号化されてしまうので、オンラインバックアップ 2 種、オフラインバックアップ 1 種の計 3 種類のバックアップをとることが望ましい。
  また、復旧訓練をおこなっていないと、実際バックアップから戻らない場合があるので、定期的に復旧できることを確認しておく必要がある。

- **サーバー・ネットワーク機器・PC 等の監査ログ取得**

  攻撃を受けたことが判明しセキュリティ専門会社に調査を依頼しても、監査ログを取っていない場合調査をすることができないため、監査ログを取得するよう設定する。

- **サイバー保険加入検討**

  損害賠償・調査や対処の費用・自社の喪失利益、を補償するサイバー保険が数多く提供されているので、加入を検討する。

（4）実際に被害が発生してしまったら…＞＞＞

・ランサムウェアの被害に遭った場合、身代金を支払っても復旧できるとは限りません。まずは信頼できる公的機関に報告・相談してください。

- **通報・相談・アドバイス**

  警察（#9110，https://www.npa.go.jp/cyber/soudan.html）
  IPA　情報処理推進機構　情報セキュリティ安心相談窓口
  （https://www.ipa.go.jp/security/anshin/）
  JPCert　**Jap**an **C**omputer **E**mergency **R**esponse **T**eam Coordination Center
  （info@jpcert.or.jp，https://www.jpcert.or.jp/incidentcall/）

- **調査・対処の依頼**

  「サイバーセキュリティ事故　緊急対応」で検索し、対応できるセキュリティ専門会社に依頼する。

- **被害に遭った場合の対応と再発防止対策（例）**

  1.セキュリティ専門会社による侵入の疑いのある機器の完全初期化、または機器の入れ替え。

  2.必要なファイルをバックアップから復旧する。

  3.インターネット出入口にある Firewall 及び VPN 装置は再構築し最新バージョンへアップデートする。最新のセキュリティ対策ができているかを定常的に確認する。

  4.外部からのリモートデスクトップ接続は禁止としポートを閉鎖する。

  5.暗号化を免れた PC、外部記憶媒体（USB メモリ／外付 HDD）の安全性を確認する。

  6.ウイルス対策ソフトを刷新する。

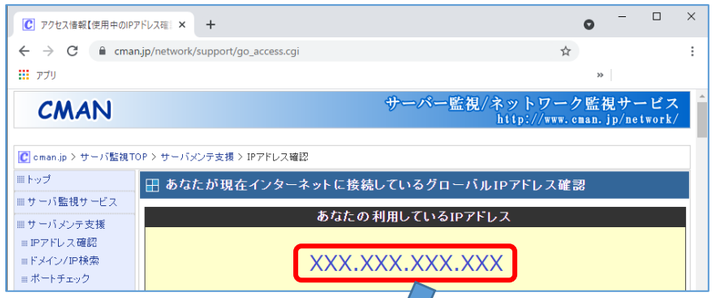
  7.特権アカウントや業務用のアカウントを見直す。

  8.不審な挙動を検知するための EDR（ふるまい検知型ウイルス対策ソフトウェア）を導入する。

（5）SHODAN サンプル…＞＞＞

SHODAN の利用にあたっては、IPA（情報処理推進機構）発行の「増加するインターネット接続機器の不適切な情報公開とその対策」を必ず参照してから実施してください。
https://www.ipa.go.jp/about/technicalwatch/20140227.html
また、社内ネットワークから SHODAN へのアクセスを禁止している企業もあるので、アクセスできない場合は自社のセキュリティ担当部署に相談してください。

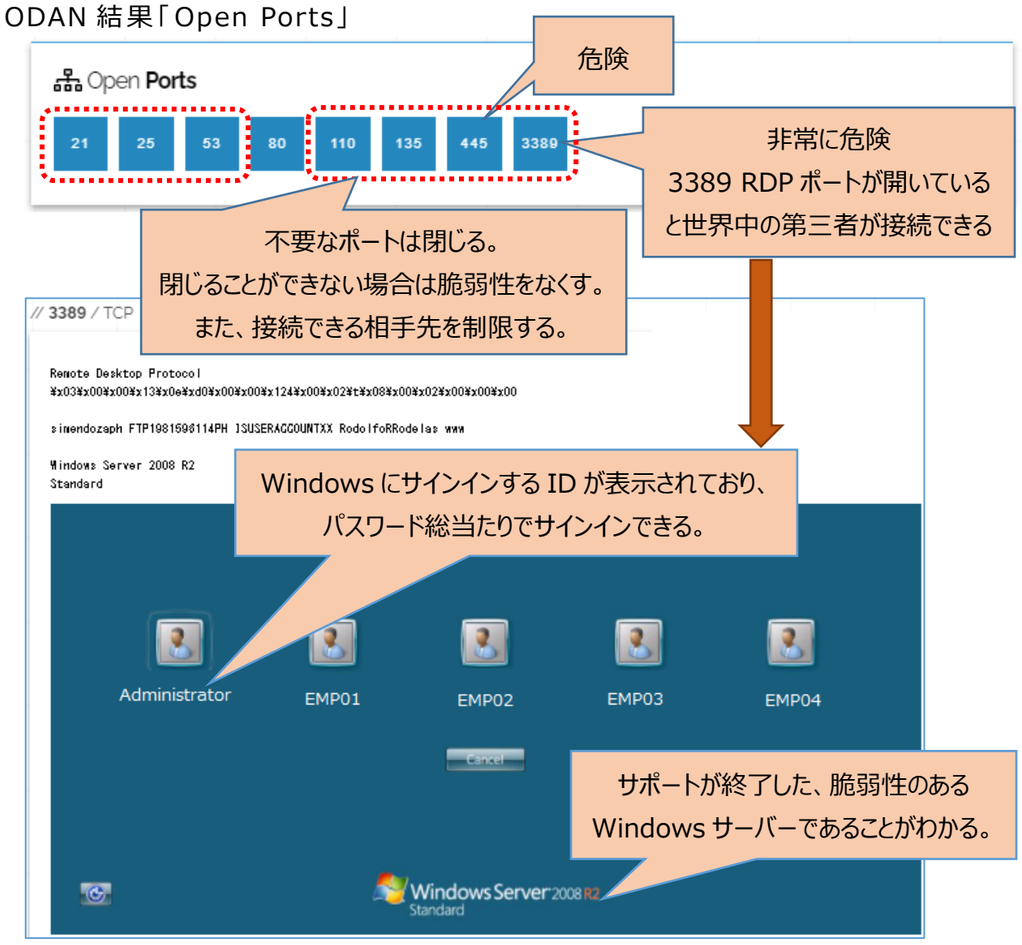
・自社のグローバル IP アドレスの確認　https://www.cman.jp/network/support/go_access.cgi



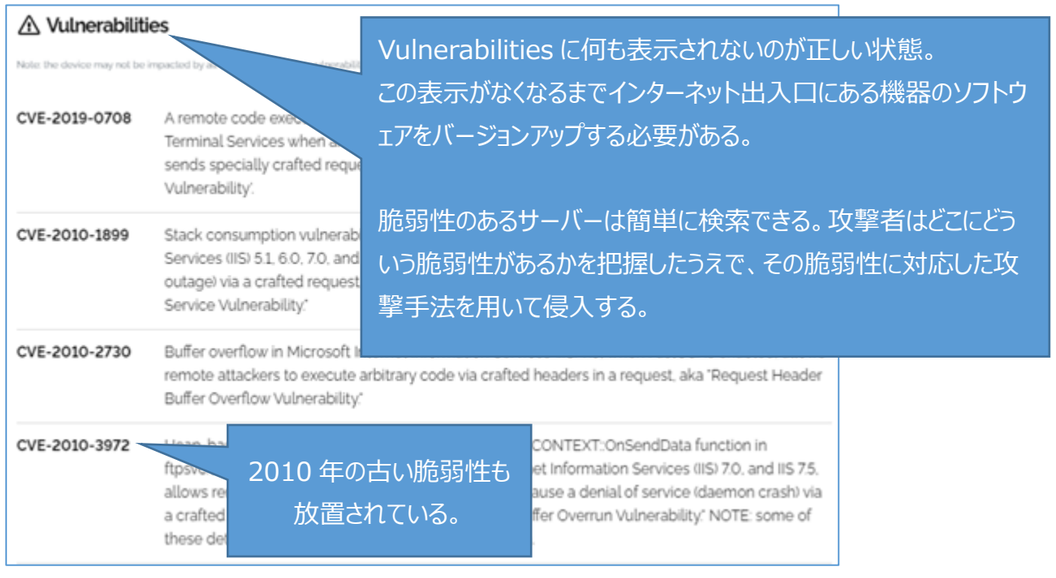
・SHODAN　https://www.shodan.io

・SHODAN 結果表示

・SHODAN 結果「Open Ports」



・SHODAN 結果「Vulnerabilities（脆弱性）」



※参考資料

＊NISC（内閣サイバーセキュリティセンター）

『ランサムウェアによるサイバー攻撃に関する注意喚起について』（2021 年 4 月 30 日）

https://www.nisc.go.jp/active/infra/pdf/ransomware20210430.pdf

＊IPA（情報処理推進機構）

『増加するインターネット機器の不適切な情報公開とその対策』（2017 年 4 月 17 日）

https://www.ipa.go.jp/security/technicalwatch/20160531.html

『【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について』（2020 年 8 月 20 日））

https://www.ipa.go.jp/security/announce/2020-ransom.html

一般社団法人 日本建設業連合会　ＩＣＴ推進部会 情報セキュリティ専門部会（2021 年 8 月発行）