ハンジャ・タイムズ
Hanja Times

2024
March
3月

Hanja Networks
株式会社ハンジャ・ネットワークス
沖縄県中頭郡北中城村島袋 480 番地
TEL:050-5810-5929 / FAX:098-989-7715

サイバー攻撃にどう対策すべきか？

攻撃者の動向や手口を知ることから未知の攻撃に備えが始まります。
今、企業に求められる新たなセキュリティマネジメント

ランサムウェアとは？感染経路や被害を防ぐ対策方法をチェック

ランサムウェアは、感染すると企業に甚大な被害をもたらすコンピュータウイルスです。企業を狙ったサイバー攻撃の中でも、近年、ランサムウェアによる被害が増加しています。ここでは、ランサムウェアの概要とその被害状況、ランサムウェアに感染したと思われるときの対処法や、被害を防ぐための対策について解説します。

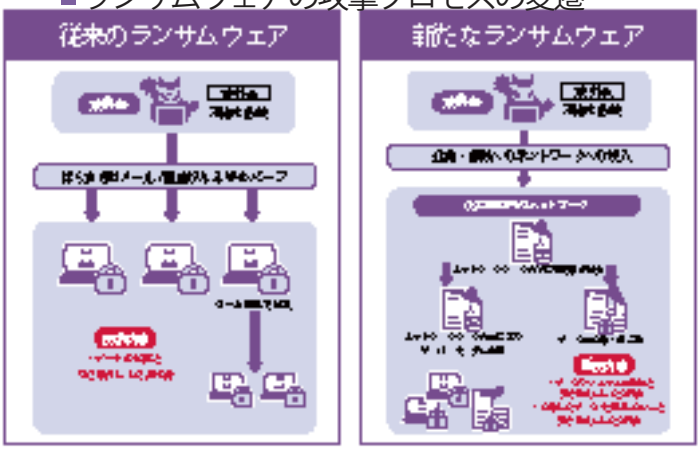
ランサムウェアとは？

ランサムウェアという名称は、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語です。感染したパソコンのファイルを暗号化したり、ロックをかけたりして使用できない状態にした後、元に戻すことと引き換えに金銭を要求するコンピュータウイルスのことで、身代金要求型ウイルスとも呼ばれます。

ランサムウェアの変遷

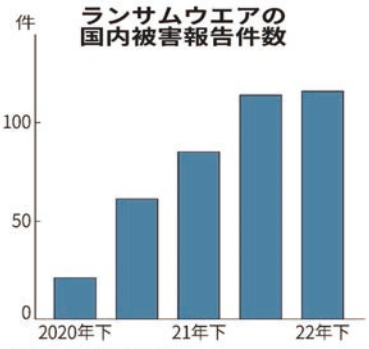
日本でランサムウェアが情報セキュリティ上の脅威と認識され始めたのは、2016 年頃からです。
当初は、不特定多数の利用者に向けてコンピュータウイルスをメールで送信する方法で感染させ、データの復旧と引き換えに身代金を要求するのが一般的でした。しかし、その手口は年々変化しており、テレワークが普及した 2020 年頃からは、VPN 機器をはじめとするネットワーク機器のインフラの脆弱性を狙い、企業のネットワークに侵入する手口が増加しています。また、不特定多数の相手へのメール送信から、標的型攻撃メールも登場しています。標的型攻撃メールとは、対象の組織を狙って、担当者が業務関係のメールだと思い込むように作り込まれたメールのことです。要求の内容も変化が見られ、近年ではネットワーク内のデータを盗み取り、企業に対して「対価を支払わなければデータを公開する」と要求する二重恐喝（ダブルエクストーション）と呼ばれるものが確認されています。

■ランサムウェアの攻撃プロセスの変遷



ランサムウェアによる被害

警察庁によると、企業・団体などにおけるランサムウェア被害の件数は、統計を取り始めた 2020 年下半期以降右肩上がりで増加し、2020 年下半期は 21 件だったのが、2023 年上半期では 103 件に増えています。ランサムウェアの被害に遭った企業・団体へのアンケートでは、有効回答数 60 件のうち 17%が復旧までに 1 ヵ月以上を要したと回答しており、また復旧費用についても、有効回答数 53 件のうち半数以上は、500 万円以上が必要だったと回答しています。ランサムウェアによる引き起こされる被害は、要求に従うことによる金銭的損失にとどまりません。ファイルの暗号化や端末のロックによる業務・サービスの停止、窃取された重要な情報の漏洩、そして情報漏洩の結果として、顧客や取引先からの信用が失墜するなど被害は広範囲に及びます。



(注)半期ごとの推移
(出所)警察庁

ランサムウェアの攻撃手順

ランサムウェアの攻撃には 4 段階あります。侵入、端末内部での活動、データ持ち出しやロック、そしてランサムウェア実行の 4 つです。それぞれの段階について解説します。

1 企業内ネットワークへの侵入

まず攻撃者は、VPN 機器などの脆弱性を利用して企業内のネットワークに侵入します。このほか、標的型攻撃メールによるリンクや添付ファイル、外部メモリーなども侵入経路となります。

2 端末内部での探索活動

攻撃者が企業内のネットワークに侵入したら、端末内部での探索活動が始まります。攻撃者は、遠隔操作ツールを使って侵入した端末やネットワークの内部をスキャン。侵入可能なサーバーやアクセス可能な機密情報、管理者のアカウント情報といった、身代金要求に使えそうな情報の探索を行います。

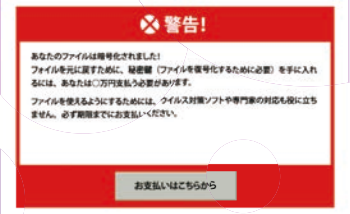
NEXT　PAGE⇨

3 データの窃取やロック

攻撃者が管理者の権限を獲得したら、機密情報や個人情報といった重要情報の窃取を開始。獲得した権限を使って脅迫のための機密情報を窃取、クラウド上か攻撃者のサーバーにアップすることで持ち出します。このほか、データをロックしてサーバーや機密情報にアクセスできないようにします。

4 ランサム（身代金）の要求

最後に、企業のネットワーク内に導入されているセキュリティを停止して不正プログラムを実行し身代金の要求を行います。この段階までに攻撃者による攻撃に気づけなかった場合、ここで初めてランサムウェアによる被害に気づきます。



ランサムウェアに感染したと思われるときの対処法

ここからは、ランサムウェアに感染したと思われるときの対処法について紹介します。
ランサムウェアの感染で恐ろしいのは、攻撃者の要求に応じて対価を支払っても、「データを復旧する」「窃取されたデータは公開しない」といった約束について、守られる保証がない点です。そのため、攻撃者の要求には応じず、被害の最小化を図り、データのバックアップから復旧するのが対処の基本となります。対処の方法は次の３つですできる限り迅速に、人手を分けて同時に行うようにしましょう。

①警察などへ通報・相談する

ランサムウェアに感染したと思われる状況になったら、自社を管轄する警察のサイバー犯罪窓口に相談・通報します。警察から助言を得ることもできますし、サイバー犯罪の実態を明らかにし、被害の拡大を防止するのにも役立ちます。

※県警察本部のサイバー犯罪相談窓口等は下記のとおりです。

沖縄県警察サイバー犯罪対策課・TEL(無料) 098-863-9110　Mail:hitech@police.pref.Okinawa.jp

②感染した端末をネットワークから隔離する

ランサムウェアに感染した場合、感染した端末やシステムをネットワークから隔離します。端末内に復元に必要な情報が残っていることがあるので、切り離した端末の電源は切らないように注意しましょう。

③組織全体で対応する

ランサムウェアはネットワーク上に接続されているほかの端末にも感染を広げるため、組織全体で状況を把握し、対応することが大切です。できるだけ早めに「被害を受けたデータ」「不審な通信を行っている端末」「窃取された情報」の特定を行います。ネットワークからの隔離などの処置により、被害の拡大を防ぎ、迅速な復旧につなげることが可能です。

ランサムウェアへの対策

ランサムウェアに感染すると甚大な被害に遭う可能性があります。ランサムウェアの被害を未然に防ぎ万が一感染したとしても被害を最小限にするために、普段から行っておくべき対策は、主に次の６つです。

❶セキュリティを最新にする

ランサムウェアの対策として、セキュリティ対策ソフトを常に最新の状態にしておくことが大切です。OS やソフトウェアは常に更新ファイルやパッチを適用し、常に最新の状態を保つようにします。

❷標的型攻撃メールの検知・ブロック機能を強化する

標的型攻撃メールの検知・ブロック機能を強化することも、ランサムウェア対策のひとつです。メール受信システムのフィルタリング機能や警告機能を利用することで、業務に関するメールを装って届く標的型攻撃メールを検知・ブロックできる可能性が高まります。

❸遠隔操作機能を適切に管理する

ランサムウェア対策として、遠隔操作機能を適切に管理しましょう。例えば、攻撃者に利用されないよう、遠隔操作機能を利用するサーバーを必要最小限にするといった方法があります。また、厳重なセキュリティチェックを行うようにすることも大切です。

❹内部ネットワークや端末の挙動を監視する

内部ネットワークや端末の挙動の監視を自動化することも、ランサムウェア対策のひとつです。組織内の複数の端末を横断するスキャンや不正ログインデータ移動などを素早く検知することで、感染の拡大や侵入範囲の拡大を抑えられます。

❺データのバックアップをとる

被害を受けたときに復旧できるよう、データは定期的にバックアップをとっておきましょう。ランサムウェア対策として、外付けの記録媒体にも保存し、ネットワークと切り離して保管しておく方法もあります。

❻社員のリテラシーを高める

どれだけセキュリティを強化しても、すべてのリスクに対応することは不可能です。システムをすり抜けた標的型攻撃メールへの対処など、人の行動に委ねられる部分も大きいため、研修などを通して社員のセキュリティリテラシーを高めておくことも大切です。

ある日、大切な書類データがランサムウェアの被害で利用できなくなったらどうしますか？

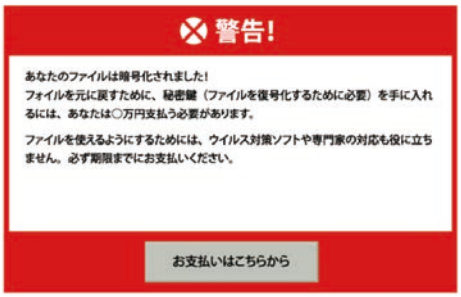
これは、私が聞いたある建設会社に起こった実際の話です・・・

彼（社長）はいつも朝早くに誰よりも先に会社にきてメールや、その日の内容をまとめ仕事に取り掛かるのが日課でありその日は朝から雨で道路は朝の渋滞が激しく出社するのにいつもより時間がかかっていました。
そして誰よりも先に出社して自分のパソコンを開いてみるとすごいことがおきてました。

「おぉーーー、なんじゃこりゃ〜」

それは、彼のパソコンの
すべてのフォルダのファイルがごちゃごちゃな名前になっており、しかもそのデータが開かない。
どんなにやっても開かない（😭）ということがありました。

しかもそれは、そのパソコンだけならまだしも会社の重要なファイル・データ等を保存しているファイルサーバーの中身も同様にすべてのファイルがごちゃごちゃ！
どうあがいてもそれらのファイルらは開かない。「全然開かないっ」



「どうなってるんだっ」

そしてパソコンの画面に見慣れぬ赤いウィンドウがポップアップしてきた！
「あなたの大切なデータはすべて暗号化ロックしたので解除したければビットコインで我々の要求する金額を払え」ってことだった。

「なんやそれっ」
もしかして、最近ニュースなどであがっている病院や図書館のシステムがウィルスによりデータがロックされ使えなくなり使えるようにしたければ身代金を払えって言うやつか？

会社のみんなが共有するデータはファイルサーバーという機械に全員保存していたのだが、それが全部使えんっ。
オーマイガット！
神様、どうにかならないですか？

しかも問題なのはこれまでのお客様の建築図面データや確認申請書類データ、完成図書、各省庁への申請書類などさまざまなデータが保存されておった。
それが全部開かんのじゃ！

ネットで検索してみると身代金を払ったってデータが回復するとは限らないって書いてある。
まして暗号化を解除する身代金は法外な金額。払えるわけないでしょ！

とりあえず、9時になって直ぐにうちのファイルサーバーを納品・メンテしているシステム会社（弊社ではありません）に電話してみた。

「〇〇さん、今日朝パソコンを開いてみたらエライことになっていた。パソコンのすべてのデータがなんかごちゃごちゃな名前になっていて一切開かない。
データを共有しているファイルサーバーの中身も同じ、すべてのデータがごちゃごちゃになっていて全然開かない。
どうしたらいいかな。
なんかこれって巷で言うウィルス被害なんでしょうか？」
「そうですね。ランサムウェアっていう最近被害が最も多いマルウェア（ウィルス）に感染している可能性がありますね。
とりあえず、そのような症状が出ているパソコンはすべてネットワークから切り離してください。
LAN ケーブルをパソコンから外すなどネットワークに繋がらないようにして隔離してください。」

って、言われるようにそのように処置をした。
そしててっきりその問題を解決してくれるのを期待してそのあとの連絡を待っていた。

だが、その後そのシステム会社からの連絡はなかった・・・

もしもの時に備えて・・・

①無料セキュリティサービスで自社の問題点を把握しよう

自社のセキュリティ状況がハッカー、ビジネスパートナーなど外部からどのように見えているのか
下記のサイトを使ってチェックしてみましょう。（お勧め！）

東京海上日動の Tokio Cyber Portへ会員登録をすると以下の無料サービスが利用できます。

おすすめ！

②ランサムウェア対策にサイバーリスクの補償を利用しよう

「身代金」はサイバー保険で払えるの？

サイバー保険は、サイバー脅威による損害を補償する保険です。このため近年目立つランサムウエア（身代金要求型ウイルス）攻撃を受けて、復旧のために「身代金」を支払った場合も補償されると思われるかもしれません。しかし日本では補償の対象外です。サイバー保険の補償対象は大きく 3 つあります。

1. 事故対応の費用です。原因の調査やデータ復旧の費用などを補償します。
2. 第三者に対する損害賠償責任。取引先の機密情報が流出した際に支払う賠償金や、弁護士費用などが該当します。
3. 機会損失や事業継続の費用です。IT システムが正常に稼働していれば得られたはずの利益などが当てはまります。

事業継続のために身代金を支払ったとしても、それが犯罪を助長するため補償の対象にはしません。そもそも身代金の支払いを保険の補償対象にすること自体、犯罪を助長します。

犯罪者集団の「Conti」から流出した攻撃マニュアルには、被害企業が身代金を支払う保険に加入しているのかを確認するように記載されていました。

一方、欧米諸国の保険会社の多くは身代金の支払いを補償対象にしています。ただ最近はランサムウエアの被害が増えて収支が悪化したなどの理由で、引き受けを大幅に制限しています。一般に身代金よりも、機会損失の損害のほうが高額です。身代金の支払いを補償しなくても、ランサムウエア攻撃への備えとして
サイバー保険は有用です。

イラストレーター 3D機能！！

From：伊禮門

Adobeのイラストレーターで3D機能があるのはご存知ですか？
3Dで商品のイメージなどをする際に
便利な機能をご紹介させていただきます！！

3Dオブジェクトの作成

3D効果を使うと2Dオブジェクトから3Dオブジェクトに作成ができます。
3Dオブジェクトには、ライト・陰影・回転などの細かい調整などが可能です。

3Dオブジェクトは、押し出し・回転方法・膨張・平面の
4種類あります。
既存の3Dオブジェクトをアピランスパネルで修正することもかのうです。
オブジェクトを選択し、効果→3Dとマテリアルを選択すると
3Dオブジェクトを使用することが出来ます。
（※文字・ブラシツールを使用する際はアウトラインを使用してください。）

イラストだけでなく、アウトラインやシェイプ形成を使用することで、
文字やブラシツールなども3Dとして作成することが可能です。

3Dオブジェクトをうまく使用する際には、陰影や奥行きや細かい
調整も大切なのですが、アウトライン・シェイプ形成・ブレンド
グループ化の機能をうまく扱うことも大切です！

このこの4つの使いこなす事で自分のイメージ通りのイラストを
作成することが出来ます！！

※3Dオブジェクトの回転体を使用


※3Dオブジェクトの押し出しを使用
※3Dオブジェクトの平面・膨張を使用

シールの貼り付け

3Dオブジェクトに対して、文字やイラストを貼り付けたい時は、
シンボル♣（クローバーマーク）をクリックします。
（上のメニューバーのウィンドウにシンボルがあります）

貼り付けたいイラストや文字を選択し、ステッカーとして
シンボル♣に追加します。
（※追加ボタンはシンボルのパレットの右下にあります）

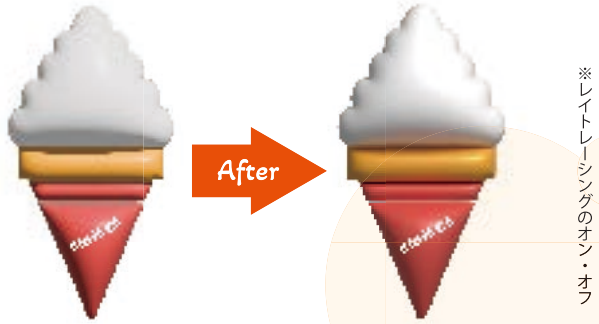
次に、3Dとマテリアル→マテリアル→グラフィックで進んで行き
グラフィックに先ほどシンボルに追加した物があるので、
これをクリックするとプロパプロパティのレイヤーの中に
ご自身で追加した物をくりっくし、調整をしたら完了です！！
(※イラストをつける場合は、グループ化をするのをおすすめします)

レンダリング

3Dオブジェクト設定ができたら、3Dとマテリアルのパネルの右上の
「レイトレーシング」のアイコンがあります。
これをクリックすると、レンタリングが処理されます。

※レイトレーシングをオンにした状態で作業をすると、環境やパソコンの
スペックによって、表示や動作が重くなります。

オンとオフを切り替えて結果えを確認しながら作業に取り掛かることが
おすすめです！！



※レイトレーシングのオン・オフ

←詳しいことは
Adobe　マニュアル
3Dオブジェクト作成

https://helpx.adobe.com/jp/illustrator/using/creating-3d-objects.html

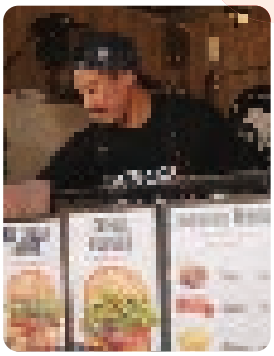
AI 3D オブジェクト

オススメ ハンバーガー屋さん

From：伊禮門

今月はぜひ食べてほしいハンバーガー屋さんをセレクトさせていただきました！
どこも美味しかったのですが
個人的に行って欲しい３軒を紹介させていただきます！

Barger&Bar Sunny

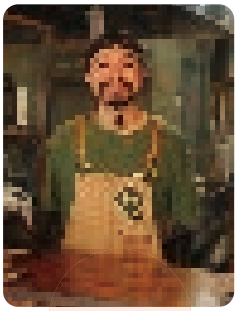


「バーガー&バーサニー」は約4年前に創業されたハンバーガーとお酒のフードトラックです。

沖縄の様々なイベントに積極的に参加しておりそのトラックには提供されるハンバーガーは野菜が多くてボリュームもあり、さっぱりとした味わいが特徴です。使用される野菜は新鮮であり、生ビールや、オリジナルドリンクがあり、ハンバーガーを包む箱のデザインも可愛らしいものとなっています。

※オープン時間や場所は
Instagram に
記載されています
TELL：080-2581-4420

BargerCafe GNOTI（ノティ）



「バーガーカフェ ノティ」は、地元では非常に評判の高い名店として知られています。去年、アゲアゲめしという番組でも取り上げられていましたね！

提供されるハンバーガーはボリュームたっぷりで、肉肉しい味わいが凄かったです。ハンバーガー以外の料理も非常に美味しく多彩なメニューが楽しめます。店内は落ち着いた雰囲気で、暖かいオレンジの照明が心地よい空間を演出しています。また、ステッカーのデザインも可愛らしく、お客様に楽しい印象を与えています。イベント出典、様々な活動に積極的に参加しています。

場所：沖縄県 宜野湾市
普天間 2-35-2
TELL:080-4280-2352
駐車場：有り

GORDIES

「ゴーディーズ」は北谷の砂辺と嘉手納にも店舗を構えています。砂辺の店舗をご紹介する理由は嘉手納とは異なる独自のメニューが提供されているためです。

砂辺の「ゴーディーズ」では、ハンバーガーの種類が驚くべき16種類も用意されています。食事を楽しむ際には、炭の香りが漂います。シンプルなものからボリュームのあるものまで、単品で注文してもポテトやピクルスがついてきます！店内は独自の雰囲気で、飽きることなく楽しめます。広々としたホールには多くの席が配置されており、外にも座席が用意されています。

場所：沖縄県 中頭郡
北谷町 砂辺 2-35-2
TELL:098-926-0234
駐車場：有り

沖縄 開催中 イベント

第 42 回東村つつじ祭り

開催日時：2024 年 3 月 20 日（水）
開催場所：東村村民つつじ園

やんばる風景花街道
第 10 回名護東海岸フラワーフェスティバル

開催日時：2024 年 3 月 9 日（土）～2024 年 3 月 24 日（日）
開催場所：名護市東海岸・久志地域 13 区全域

第 8 回弥生闘牛ダービー

開催日時：2024 年 3 月 10 日（日）
開催場所：うるま市石川多目的ドーム

オクマかりゆし海開き開催！

開催日時：開催日時：2024 年 3 月 17 日（日）
開催場所：オクマ プライベートビーチ
リゾートオクマ ビーチ

第 3 回風と緑のちいさなクラフトフェア

開催日時：2024 年 3 月 30 日（土）・31 日（日）
開催場所：名護市三原区公民館

沖縄南国イルミネーション

開催日時：2024 年 5 月 26 日（日）まで
開催場所：東南植物楽園

ボクネン展 Vol,35「ひねもす」
～朝、昼、夕、夜～

開催日時：2024 年 3 月 31 日（日）まで
開催場所：ボクネン美術館

美浜アメリカンビレッジ
2023 クリスマスイルミネーション

開催日時：2024 年 3 月 15 日（金）まで
開催場所：美浜アメリカンビレッジ

琉球ランタンフェスティバル

開催日時：2024 年 3 月 31 日（日）まで
開催場所：

海を眺めながらチルアウト
のんびり鯨をまつ

開催日時：2024 年 3 月 10 日（日）まで
開催場所：星野リゾート　バンタカフェ

花庭（ハナナ）フェア

開催日時：2024 年 3 月 31 日（日）まで
開催場所：カヌチャーリゾート
カヌチャベイホテル＆ヴィラズ

第 19 回美ら海花まつり

開催日時：2024 年 3 月 31 日（日）まで
開催場所：海洋博公園　沖縄美ら海水族館周辺
～中央ゲート

マヤ先住民の日常着
星野利枝コレクション展

開催日時：2024 年 3 月 31 日（日）まで
開催場所：おきなわ工芸の杜　企画展示室