工場セキュリティガイドライン啓発・連続セミナ

製造業/ 工場サイバーセキュリティの実態および課題と対策

株式会社ＦＦＲＩセキュリティ
東証グロース: 3692
https://www.ffri.jp

自己紹介

株式会社FFRIセキュリティ
技術本部 セキュリティサービス部長

中西 克彦

内閣府大臣官房 情報化参与 最高情報セキュリティアドバイザ
CYDER推進委員
Hardening Project実行委員
Interopプログラム委員

令和4年 サイバーセキュリティに関する総務大臣奨励賞
ISC2 Asia-Pacific Information Security Leadership Awards 2017
CISSP

SI企業にて、Web Application Firewallの開発/サポート、セキュリティ診断を皮切りに、インシデントレスポンス、サイバー演習などのセキュリティ業務に携わる。
2015年より公益財団法人 東京オリンピック・パラリンピック競技大会組織委員会に出向。危機管理（CISO補佐）、CSIRT責任者、脅威情報の分析などを担当。
2022年より、現職。

本日のテーマ

ランサムウェアによる被害で、国内の自動車関連企業等のサプライチェーンが影響を受ける事案が発生したほか、新規患者の受入れ停止、サービス障害、機密情報の流出など、深刻な事案が次々と発生しています。

その被害の実態を、統計情報やセキュリティ事案をもとに紹介し、被害を極小化するために必要な対策を示します。

ランサムウェアによる業務影響

■つるぎ町立半田病院
2021/10/31 院内システム停止
2022/1/4 全13診療科で通常診療再開

■大阪急性期・総合医療センター
2022/10/31 電子カルテ停止
2022/12/12 電子カルテなど基幹システム復旧
2023/1/10 画像診断や生理検査など部門システム復旧

サイバー攻撃で診療停止　電子カルテ、２カ月使えず―病院に「身代金ウイルス」・徳島

2022年01月24日13時30分

「ランサムウエア」に感染して電子カルテが閲覧できなくなり、作成された紙カルテ＝６日、徳島県つるぎ町の半田病院

徳島県つるぎ町にある町立半田病院のサーバーが昨年１０月末、データを暗号化し、解除と引き換えに金銭を要求するコンピューターウイルス「ランサムウエア」に感染した。病院内のプリンターが一斉に作動し、「身代金を支払わなければデータを公開する」という英語の脅迫文が届き、約８万５０００人分の電子カルテが閲覧できなくなった。

ランサムウエア、被害申告６１件　昨年比で急増、検挙はなし―今年上半期・警察庁

2021年10月
サイバー攻撃で診療停止　電子カルテ、２カ月使えず
https://sp.m.jiji.com/article/show/2693470

紙カルテは「汚い文字」厳禁　大阪の病院サイバー攻撃１カ月、システム復旧せず

2022/12/1 19:12　有料プラン記事

社会 | 事件・疑惑　ライフ | からだ　地方 | 近畿　大阪　産経WEST | できごと

集中治療室でカルテなどを手書きする医師ら＝１日午前、大阪市住吉区の大阪急性期・総合医療センター（代表撮影、一部画像処理しています）

大阪急性期・総合医療センター（大阪市住吉区）への身代金要求型ウイルス「ランサムウエア」とみられるサイバー攻撃の発覚から１カ月が経過した。サーバーは依然として復旧せず、診療に欠かせない電子カルテが使えない状態が続く。代わりに使用する紙カルテも作業の煩雑化といった問題に直面しているが、現場は年明けの全面復旧に向け奮闘している。

同センターの入院患者は２９７人（１１月２９日時点）。緊急性が低い患者に退院や転院を勧めたこともあり、昨年度の１日平均５９９人の半分に満たない。１日、記者団の取材に応じた藤見聡(さとし)・高度救命救急センター長は「患者や地域医療機関に負担をかけ申し訳なく思う」と陳謝した。

2022年10月
大阪の病院サイバー攻撃1か月、システム復旧せず
https://www.sankei.com/article/20221201-BCA3QJVW4VLRXG3Z4HQBHLXTLY/

医療機関のランサムウェア感染事例

地域中核病院で医療データ暗号化による脅迫

- 各サーバの格納データが暗号化、サーバの操作履歴やアクセスログも抹消
- プリンターが一斉に英文のメッセージを印刷
- 電子カルテシステムや医事システムなど院内システムの障害が発生
- VPN機器の脆弱性を悪用される。さらにネットワークで繋がっている取引先のシステムから侵入されるケースも

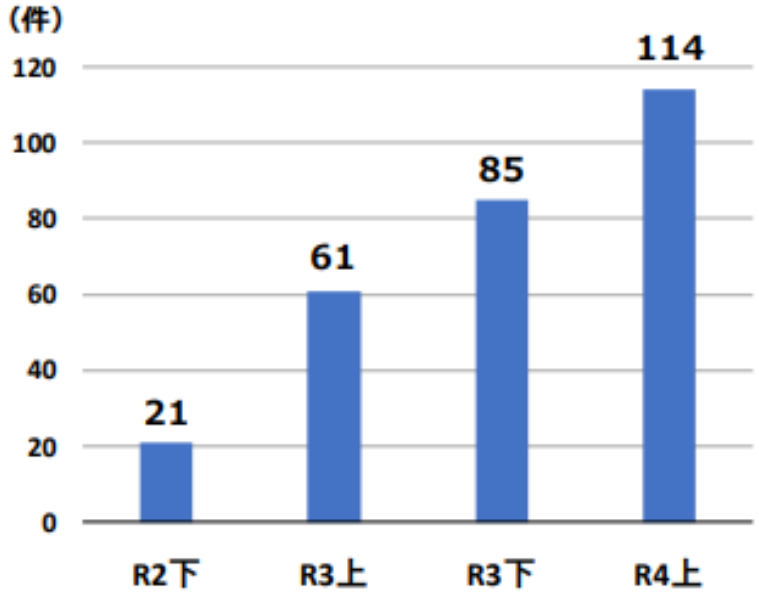
発生した影響

- 救急や新規患者の受入れ停止に伴う地域他病院への負荷増大
- 復旧までシステム停止・手作業による業務を強いられる
- 診療記録が参照できないため、適切な治療ができない
- 個人情報含むデータの流出可能性

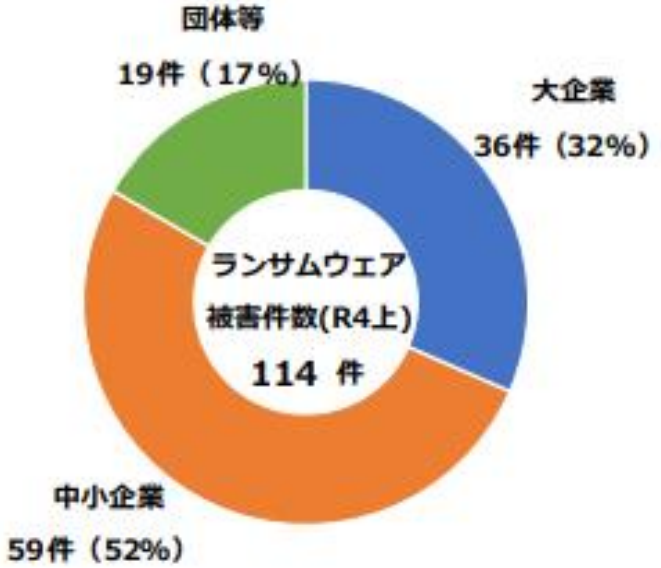
ランサムウェア国内動向

警察庁の調査によると、ランサムウェア被害は右肩上がりに増加。
企業規模によらず被害を受けている。

【図表１：企業・団体等におけるランサムウェア被害の報告件数の推移】



【図表４：ランサムウェア被害の企業・団体等の規模別報告件数】



令和4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
https://www.npa.go.jp/publications/statistics/cybersecurity/

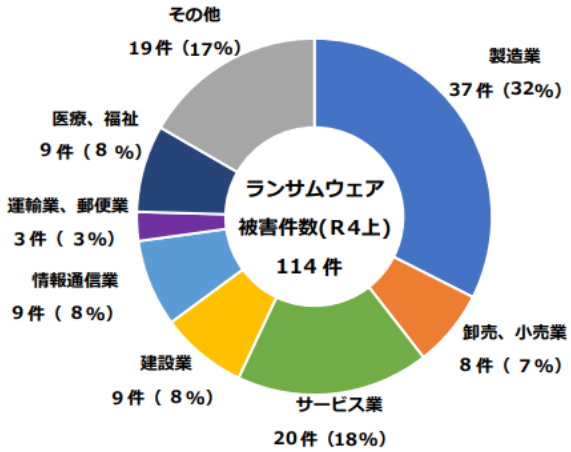
2022年のランサムウェア事例

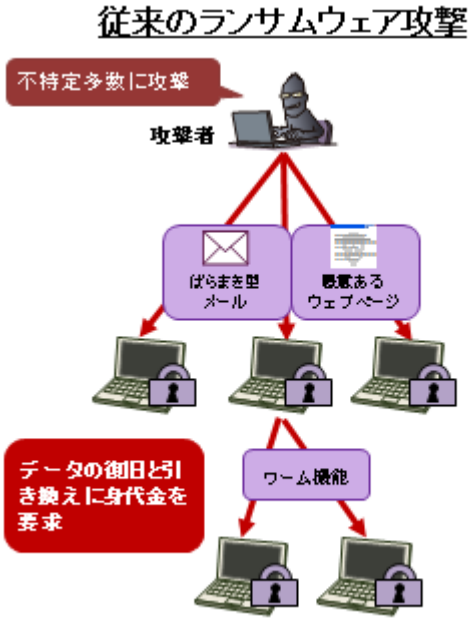
No	被害時期	法人名 団体名	概要
1	2022年2月	小島プレス工業	トヨタ自動車の取引先、樹脂部品を手掛ける小島プレス工業。今回のシステム障害により、トヨタは3月1日に国内全工場の停止に追い込まれた。子会社が独自に特定外部企業との専用通信に利用していたVPN機器に脆弱性あり。
2	2022年2月	GMB	駆動系部品のOEM供給と補修用部品を製造販売する独立系自動車部品メーカー GMB。ネットワークシステムの脆弱性を悪用し、同社サーバに不正侵入した上で、複数のサーバ及びPC端末にアクセスしファイルを暗号化する攻撃を受けた。
3	2022年2月	ブリヂストン	ブリヂストン米子会社がサイバー攻撃を受け、工場の稼働を一時停止していた。身代金要求型ウイルスへの感染で社内システムの総点検に踏み切ったためで、工場は2月下旬から数日程度止めた。LockBitがリークサイトで公表
4	2023年2月	グローバルウエハースジャパン	台湾GlobalWafersの子会社で半導体用シリコンウェーハを製造するグローバルウェーハズ・ジャパン。社内サーバーが不正アクセスを受け、一部工場を除き製造、出荷作業を停止した。
5	2022年2月	エスビー食品	エスビー食品の子会社でコンビニ向け食品の製造を手がけるヒガシヤデリカにおいて、ランサムウェアと見られる被害が発生。生産や供給への影響は出ていない。原因は、従業員のリモートアクセス用に設置した機器の脆弱性。
6	2022年3月	デンソー	トヨタ自動車系部品メーカー、デンソー。ドイツの現地法人がサイバー攻撃を受けたことを明らかにした。身代金を請求するウイルス「ランサムウエア」の感染を確認した。攻撃を仕掛けたとみられる犯罪グループがデンソーを脅迫する声明を出している。デンソーは現時点で事業に影響は出ていないとしており、主要顧客であるトヨタ自動車も「工場稼働など影響はない」としている。
7	2022年3月	東映アニメーション	東映アニメーションは18日、4月22日に予定していた「ドラゴンボール超　スーパーヒーロー」の公開を延期すると発表した。6日に社内システムが不正アクセスを受け、作品製作が難しくなった。ブリヂストンと森永製菓も18日に不正アクセスを受け、生産活動に支障が出ていることを明らかにした。日本企業にサイバー攻撃の影響が広がっている。
8	2022年3月	三桜工業	自動車部品メーカーの三桜工業は24日、米子会社がサイバー攻撃を受けたことを明らかにした。ハッカー組織が身代金要求型ウイルス「ランサムウエア」による攻撃を仕掛け、一部のデータをインターネット上の独自サイトで公開していた。米子会社はネット接続を遮断し、取引先に影響が広がらないようにした。自動車メーカー向けの部品生産に影響はないとしている。
9	2022年3月	森永製菓	大手菓子メーカー「森永製菓」、社内のサーバーへの不正アクセスによって複数のシステムがダウンし、一部の商品の製造に影響が出た。通販事業「森永ダイレクトストア」で商品を購入したことのある顧客合わせて164万人以上の個人情報が流出した可能性がある。システムは、22日の朝に全面復旧したが、在庫の減少などから一部の商品の供給に影響が続く。インターネット回線に設置していたネットワーク機器の脆弱性を悪用され、侵入された可能性が高い。
10	2022年4月	月桂冠	月桂冠は6日、管理するサーバーが第三者による不正アクセスを受け、社内システムに障害が発生したと同社ホームページで発表した。2日に障害を確認した後、拡大を防ぐためサーバーの停止や、外部とのネットワークを遮断するなどの対応を実施した。
11	2022年4月	コニカミノルタ	コニカミノルタのマーケティングなどを担当している英国子会社がサーバーに不正アクセスを受けたことが5日、分かった。現時点で顧客情報や社内情報の流出は確認されていない。外部の専門機関に依頼し、詳細な状況や原因の調査を進めている。身代金要求型ウイルス「ランサムウエア」によるサイバー攻撃を受けたとみられる。ファイルの一部が破損した状態で、パソコンでのメールの送受信ができないなど業務への影響が出ている。
12	2022年4月	パナソニックホールディングス	パナソニックホールディングス（HD）は7日、主に家電の販売を手がけるカナダの子会社がサイバー攻撃を受け、身代金要求型ウイルス「ランサムウエア」に感染したと発表した。「Conti（コンティ）」という攻撃者グループが運営するサイトに、抜き取られたとみられるデータが4月5日に掲載されたことも確認したという。
13	2022年5月	しまむら	しまむらは大型連休中にサイバー攻撃を受けていたことを明らかにした。4日から社内ネットワークへの不正アクセスによるシステム障害が発生し、商品を店舗に取り寄せるサービスが利用できない状況が続いている。個人情報の流出は確認されていないが、小売業界では電子商取引（EC）販売の拡大に伴い顧客情報の取り扱いが増えており、サイバー攻撃への対策強化が急がれる。
14	2022年6月	TBカワシマ	トヨタ紡織子会社で自動車の内装材を手掛けるTBカワシマ（滋賀県愛荘町）に対して、サイバー攻撃をしたと主張する犯行声明が出ていることが21日、わかった。ハッカー集団「ロックビット」が自らのホームページに、攻撃した組織としてTBカワシマの社名を明記した。現時点で生産への影響は確認されていない。
15	2022年7月	安江病院	岐阜市の安江病院は4日、外部から不正アクセスを受け、病院のコンピューターシステムに保管していた患者や職員、計約11万人分の個人情報が流出した可能性があると発表した。病院によると流出した可能性があるのは、患者や新型コロナウイルスワクチン接種者、延べ11万1991人と、職員715人分の名前や住所、電話番号や病歴など。
16	2022年8月	SOMPOホールディングス	SOMPOホールディングスは23日、傘下の台湾保険仲介会社が18日に外部からのサイバー攻撃を受けたと発表した。社内の7台のサーバーでファイルが暗号化され、各種システムが利用できなくなった。
17	2022年9月	大潟村農業協同組合（JA大潟村）	大潟村農業協同組合（JA大潟村）は2022年9月16日、運用するJAシステムにサイバー攻撃が発生し、情報が流出した可能性があると明らかにしました。説明によると、JA大潟村では現在、セキュリティー会社の協力のもと調査・復旧を進めているとのこと。公表時点で詳しい原因や経緯は明らかにされていませんが、判明次第、公表するとしています。
18	2022年10月	大阪急性期・総合医療センター	身代金要求型ウイルス「ランサムウエア」とみられるサイバー攻撃でシステム障害が続く大阪急性期・総合医療センター（大阪市住吉区）は11月7日、完全復旧を2023年1月と見込んでいると明らかにした。給食を委託する業者経由でシステムに侵入された可能性が高いという。障害の発生から7日で1週間が経過。すでに手術は一部再開したが、電子カルテシステムは依然として使えず、一般外来業務も停止したままだ。10月31日に発覚した今回の攻撃では、患者の個人情報や治療内容を記録した電子カルテが使えなくなった。ハッカー側からシステム復旧にあたってビットコインを支払うよう要求されたが、「金銭を支払う考えはない」と拒絶していた。

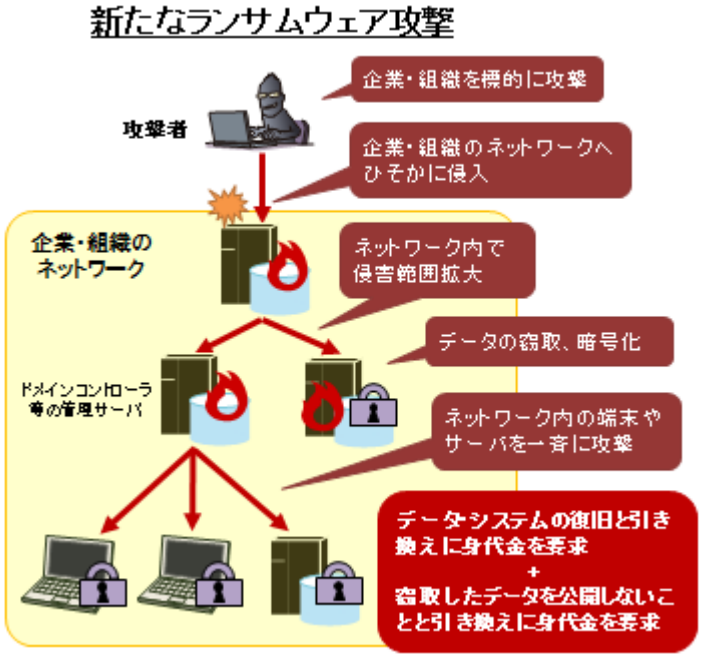
攻撃手法の変化と業種別被害状況

製造業の被害が多いのは、インターネットに直接繋がない対策（クローズドネットワーク）をとっている傾向が高く、また海外子会社など組織的なセキュリティ対策がとれていないといった原因が推測される。

(1)　ランサムウェア被害の被害企業・団体等の業種別報告件数







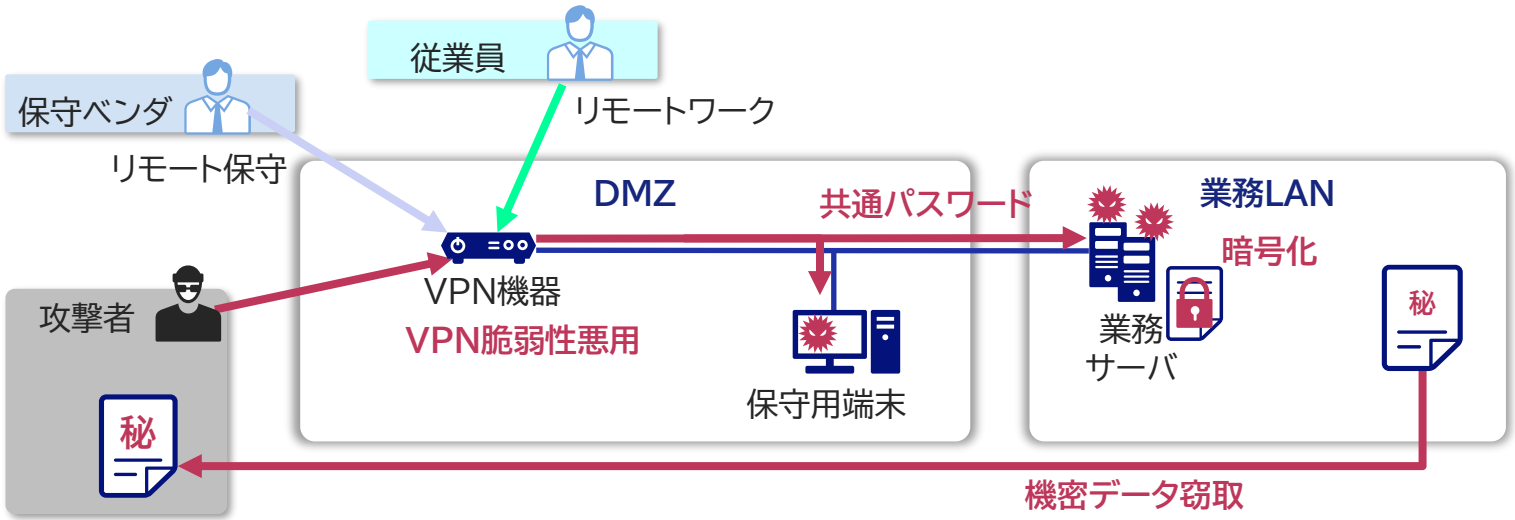
令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/

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

ランサムウェア感染事例

原因

- VPN機器の脆弱性未対策
- リモート保守用PCのアクセス制限不備
- 内部ネットワークがフラットな構成
- 共通のパスワードや弱いパスワードの利用



ランサムウェア感染事例

よくある相談

- とにかく復旧を早くしたいので、データ復元できないか
- 身代金を支払ったらデータ復旧するか
- 漏えいしたデータを特定できないか
- 被害を受けたことや情報はどこまで公開するべきか
- 脆弱性やシステム構成の弱点はどこまで改善したら業務再開していいのか

- NW上のバックアップは、概ね一緒に暗号化される。暗号化されたデータを復号することはほぼ不可能。捜査などにより攻撃者から復号鍵入手できたケースでは、セキュリティベンダ等が復号ツールを作成して公開している。「No More Ransom」 で検索。
- 身代金を払ってもすべてのファイルが復元される保証がない、支払い後に別の攻撃を受ける恐れがある
- イベントログは削除され、流出経路はHTTPSが使われるためデータは通信ログには残らない
- 業務復旧だけではなく、取引先/顧客に関する情報流出など被害状況把握や再発防止のための原因特定も必要

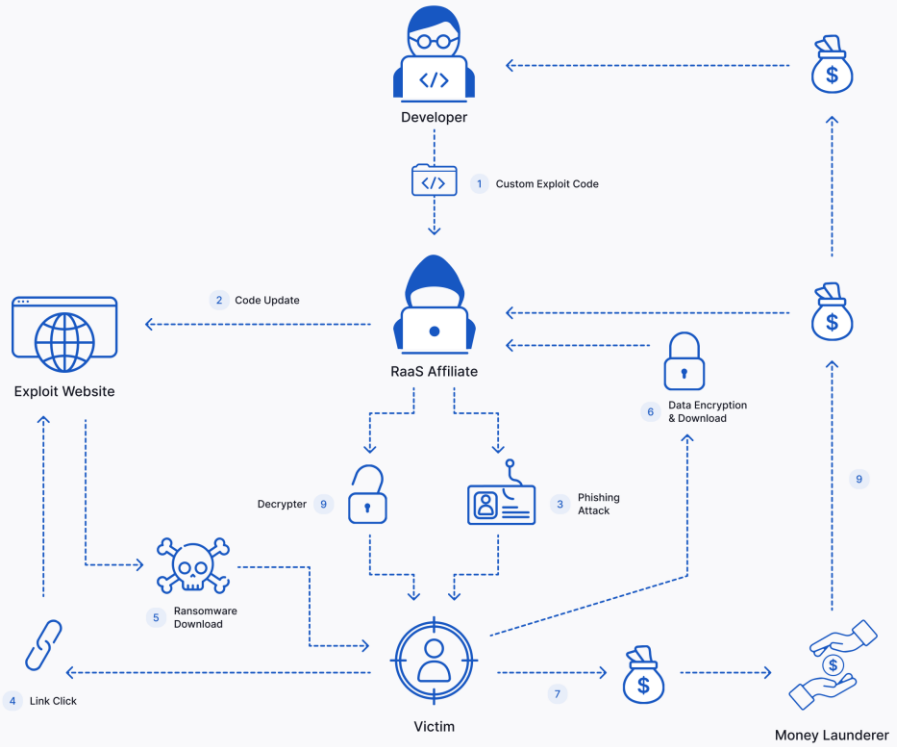
RaaSとは

Ransomware as a Serviceの略。

ランサムウェア開発者がランサムウェアとコントロールパネル、攻撃マニュアルをサービスとして提供。

アフィリエイトが、それらのサービスを利用して実際に攻撃・脅迫を行う。

獲得した身代金のうち、7～8割をアフィリエイトが入手し、残りをRaaS提供者であるランサムウェア開発者が得る。



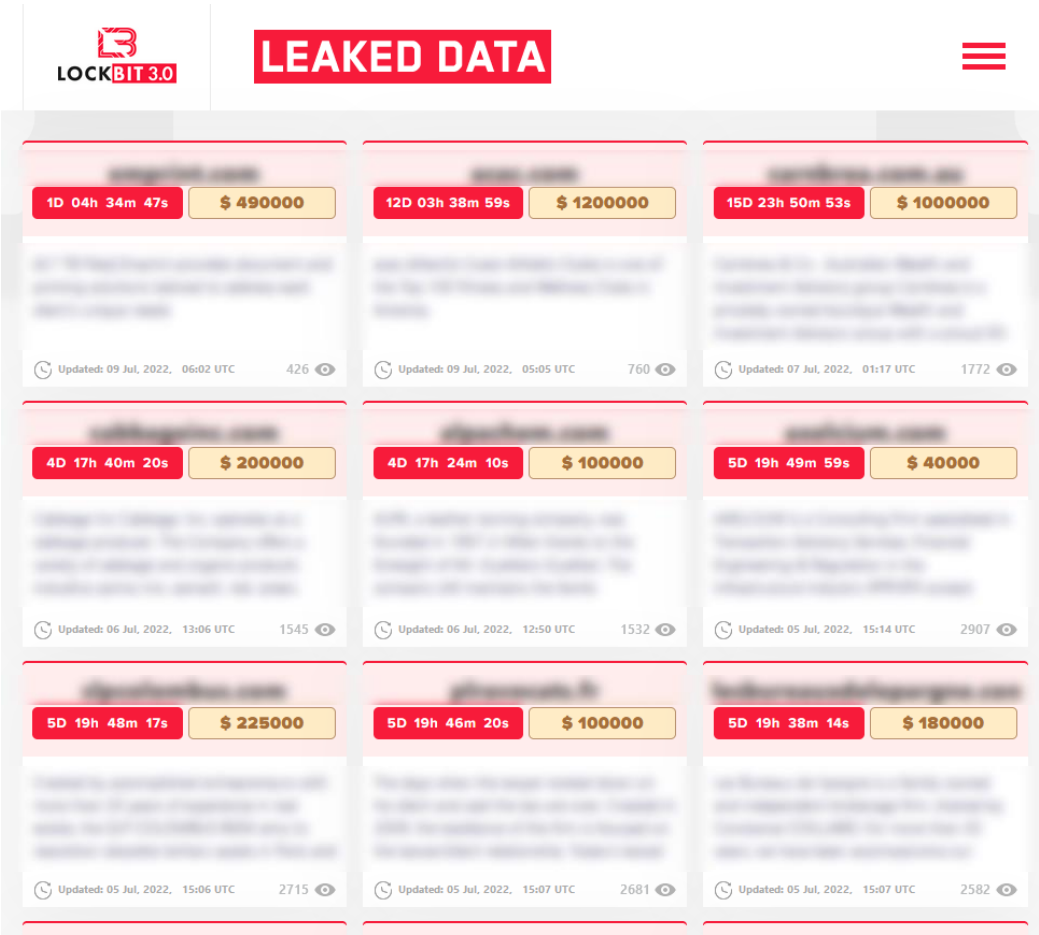
What is Ransomware as a Service (RaaS)? The Dangerous Threat to World Security
https://www.upguard.com/blog/what-is-ransomware-as-a-service

ダークウェブ上で公開される被害組織

半田病院を襲ったLOCKBIT2.0が3.0にアップデート

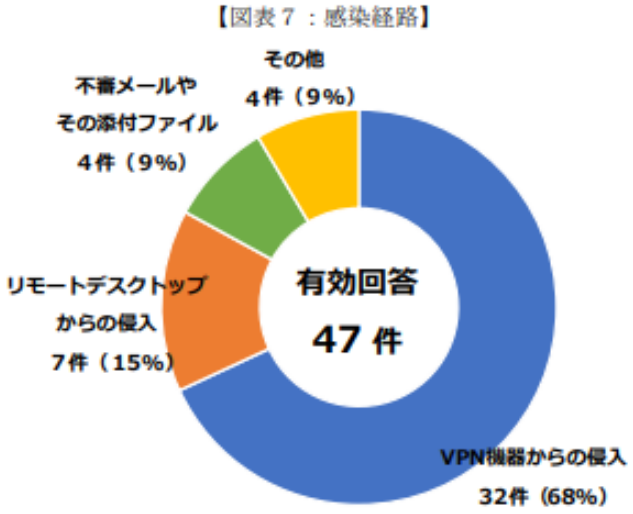
1. バグバウンティ※を開始
2. MoneroとBitcoinとともにZcashの支払いを受け入れ
3. 盗んだデータを別の犯行グループに販売

※バグバウンティ：社内のリソースのみでは発見することが難しいセキュリティの脆弱性を発見するための制度。GoogleやMicrosoft, Facebook, LINE, 任天堂など多くの企業が取り組んでおり、脆弱性もしくはバグを発見したホワイトハッカーに報奨金を支払う。



ランサムウェア事例：感染経路

保守用あるいはリモートワーク対策として導入したＶＰＮ，ＲＤＰが、インターネットから直接アクセス可能な脆弱点として残存している。



令和4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
https://www.npa.go.jp/publications/statistics/cybersecurity/

システム管理者の対策

- 特にVPNなどのネットワーク境界における脆弱性を放置しない。パッチマネジメントのサイクルをルール化する。「常に最新にする」は不可能、要件定義していないのと同じ。60日以内など具体的な数値を設定する。
- 認証を強化する。強いパスワード、多要素認証の導入。MFA未導入で脆弱性を放置していた期間の調査を実施できないなら、全パスワード変更する。
- アクセスコントロールの強化。内部ネットワークの分離など、機密サーバや情報には必要な人・端末だけがアクセスできるように制御する。踏み台マシン、RDPゲートウェイなど。

攻撃手法

1．脆弱なVPNルータ、リモートデスクトップを探索する
2．あらかじめ入手したアカウントを使ってログインする。または脆弱性を悪用して認証を突破する
3．攻撃者はネットワークに侵入し、ランサムウェアを実行する

侵入型ランサムウェア被害の実態

- 可用性・・・業務停止
- 機密性・・・機密/個人情報の暴露
- 完全性・・・データの真正性が毀損される
- 脅迫/身代金・・・サービスに対するDDoS、窃取した情報を使って被害組織の顧客や取引先への脅迫/嫌がらせ
- 調査/復旧コスト・・・顧客対応、データ復旧サービス、フォレンジック、暫定対応と恒久対応、脆弱性対策、復旧後のデータの真正性確認

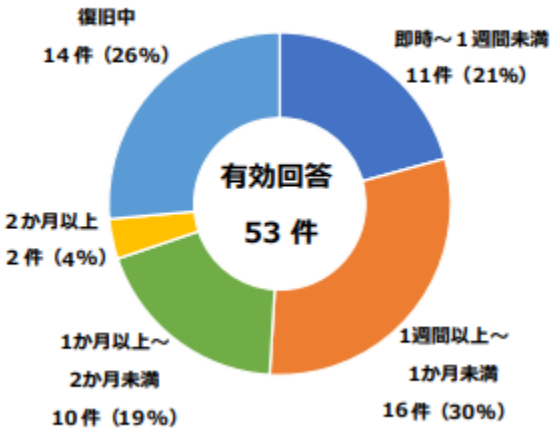
学ぶべきポイント

- すべての侵入経路を完全に塞ぐことはできない。という前提にたって備える
- バックアップサーバから先に暗号化される
- 原則、暗号化されたデータは戻せない。法執行機関により秘密鍵が押収されるケースがあるため、念のためバックアップをとっておく

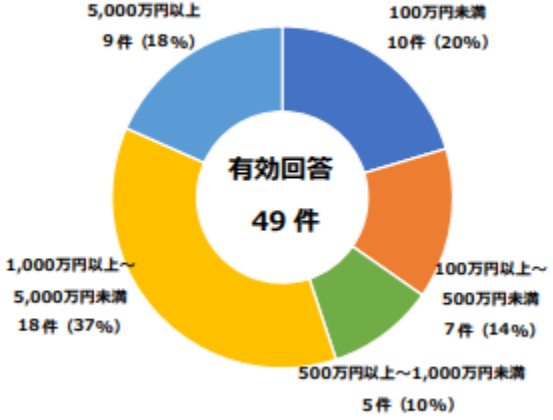
調査・復旧コストについて

復旧までに１か月以上を要したものが12件
1,000万円 以上の費用を要したものが27件で55％を占めている。

【図表５：復旧に要した期間】



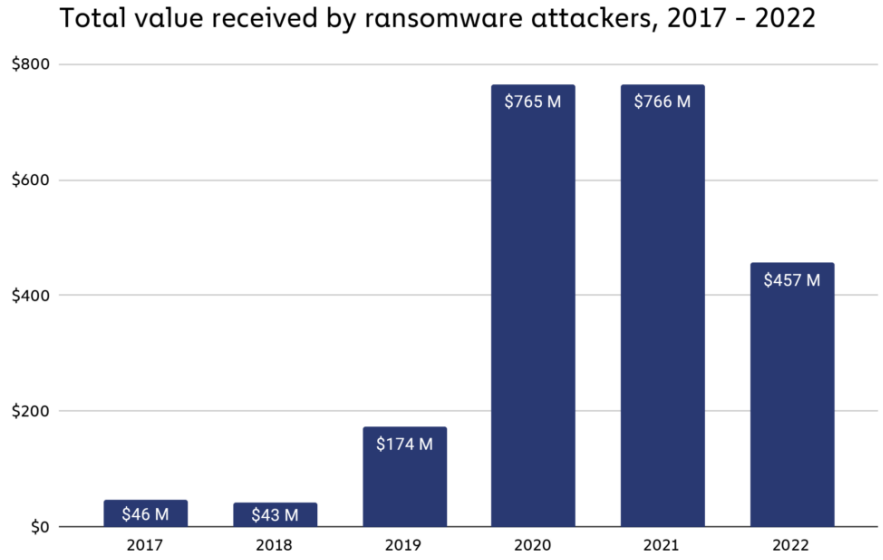
【図表６：調査・復旧費用の総額】



注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

身代金について

2022年第3四半期の平均値で258,143ドル（3,500万円相当）



Coveware社顧客 ランサムウェア被害時 身代金支払い割合©Chainalysis

	2019	2020	2021	2022
Paid	76%	70%	50%	41%
Did Not Pay	24%	30%	50%	59%

Chainalysisの分析

- 22年度の身代金総額の減少傾向は、攻撃が減少したことを意味するのではなく、身代金の支払いを拒否する被害組織が増えたということ
- 身代金の支払いが制裁の対象になる可能性が出てきたこと。OFACの勧告
- サイバー保険会社が保険適用範囲を変更したこと。身代金を支払うために保険金を使用することを許可しない。厳格なサイバーセキュリティやバックアップ対策を満たさなければ保険金を支払わない
- このような背景から、企業のサイバーセキュリティ対策が促進され、結果的にインシデントコストが削減された

Ransomware Revenue Down As More Victims Refuse to Pay
https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/

警察庁が復号ツールを作成

身代金ウイルス、警察庁が暗号解除成功　支払い未然防止

事件・司法　＋フォローする

2022年12月28日 19:00 [有料会員限定]

保存

データを暗号化して金銭を要求するランサムウエア（身代金要求型ウイルス）の一種に対し、警察庁が新たな対抗策に乗り出した。ウイルスの暗号を強制解除し、国内企業3社でデータの復元に成功。従来の予防と摘発で被害の拡大を防げないなか、身代金支払いの未然防止につなげた。日本のサイバー当局の技術力の高さを示したといえ、欧州の複数の捜査当局とも連携し、国際的な包囲網の形成を急ぐ。

身代金ウイルス、警察庁が暗号解除成功　支払い未然防止
https://www.nikkei.com/article/DGXZQOUE062930W2A201C2000000/

Part 2: LockBit 2.0 ransomware bugs and database recovery attempts

By Danielle Veluz

Published Mar 11 2022 10:02 AM　10.5K Views

In Part 1 of this series (which you can find here), we provided background about our analysis of the LockBit 2.0 ransomware and described our suspicions that "faulty crypto" was at play. In this post, we will outline the issues that the decryptor poses and how we simply cannot trust it and must remove it from any equation we intend on using to successfully decrypt these database files.

***Disclaimer**: The technical information contained in this article is provided for general informational and educational purposes only and is not a substitute for professional advice. Accordingly, before taking any action based upon such information, we encourage you to consult with the appropriate professionals. We do not provide any kind of guarantee of a certain outcome or result based on the information provided. Therefore, the use or reliance of any information contained in this article is solely at your own risk.*

If only it were so easy...

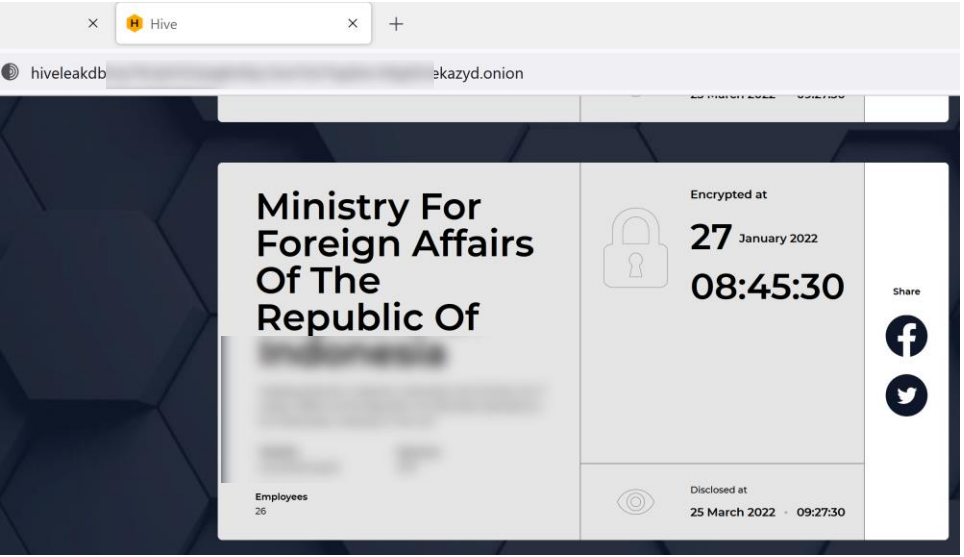
Our earlier Procmon observations identified the encryptor randomly encrypting 65k bytes *after* it was only supposed to encrypt the first 4k. So, while we do successfully decrypt the *intended* encrypted region of the encrypted file, which is the first 0x1000 bytes, we fail to identify and decrypt the *unintended* regions which are splattered throughout the now-decrypted file due to the bug we've outlined in the encryptor.

LockBit 2.0 ransomware bugs and database recovery attempts
https://techcommunity.microsoft.com/t5/microsoft-security-experts-blog/part-1-lockbit-2-0-ransomware-bugs-and-database-recovery/ba-p/3254354

FBIによるHiveランサムウェア ネットワーク解体

米司法省発表：2021年6月以降、病院/学校/金融機関/重要インフラなど、世界80か国以上で1,500以上の被害組織を標的にし、1億ドル以上の身代金を受け取った Hive ランサムウェアネットワークを解体した。

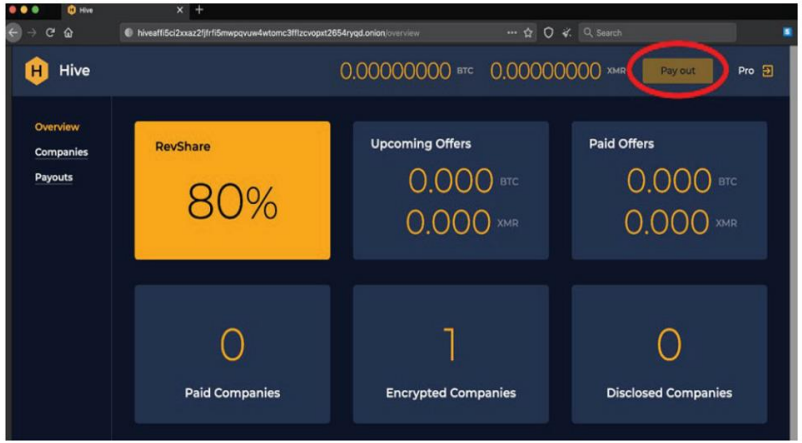
Hiveのデータリークサイト

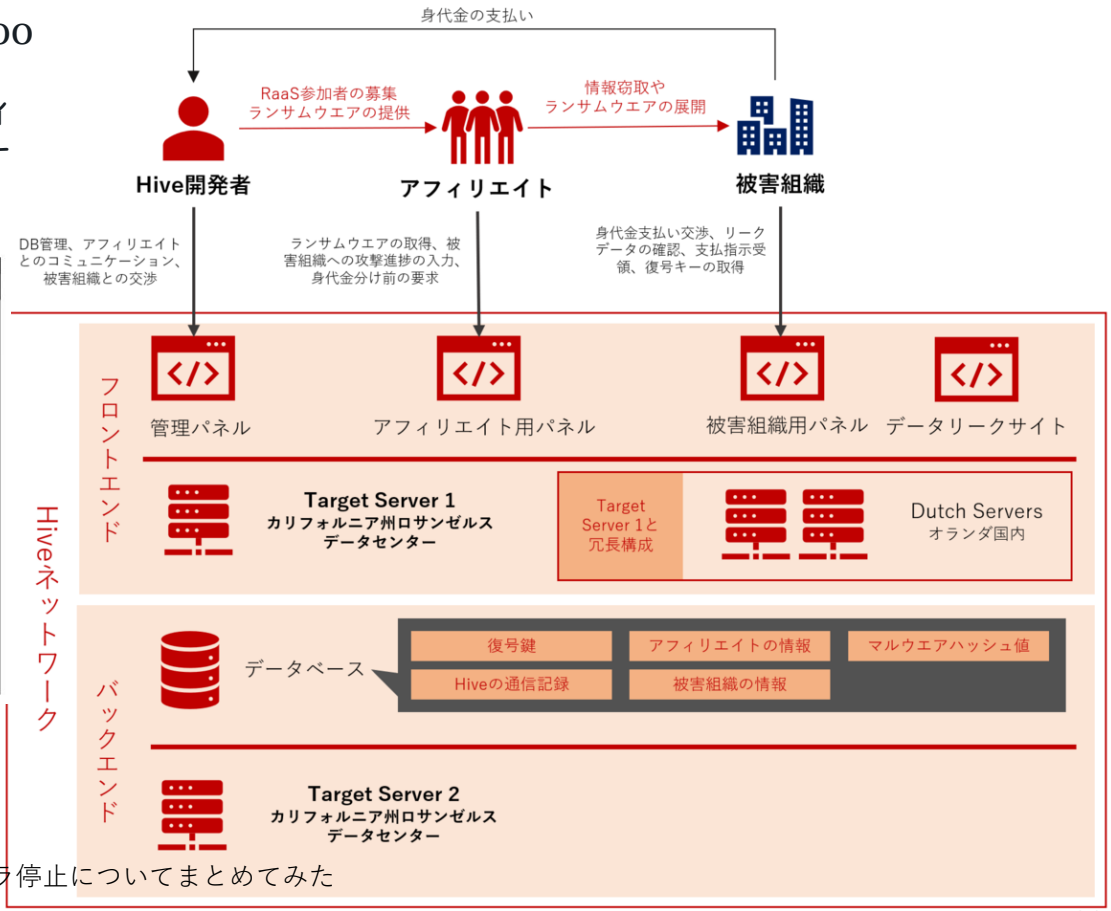


差し押さえられた Hiveのデータリークサイト

336の被害組織に復号キーを提供

復号キーのおかで、要求された身代金1億3000万ドルの支払いを回避できた。
また、捜査の過程で、Hiveのインフラやアフィリエイトの情報を入手することで、他のグループの逮捕や対策の促進に繋がる





司法機関によるHiveランサムウエアのネットワーク潜入とインフラ停止についてまとめてみた
https://piyolog.hatenadiary.jp/entry/2023/01/28/015633

ランサムウェア感染事例から見る対策の考え方

- 主要な侵入経路は脆弱性悪用（VPN, RDPなど）とID/PW認証突破

要因	対策
• ネットワークアクセス制御不備	• アクセス制御（ポート開閉、IPフィルタ） • 要塞化（サービス停止） • 内部ネットワークセグメント分割
• 認証突破	• 複雑なパスワードへの見直し • 多要素認証（MFA）の実装
• セキュリティパッチの未適用	• 定期的な脆弱性診断や脆弱性収集 • 定期的なアップデートと切り戻し訓練
• ランサムウェア感染予防・検知	• アンチウイルス対策、シグネチャー最新化 • EDR/XDR導入やSOC（監視）
• データ窃取	• ファイル暗号化（IRM）
• 事業復旧(システム復旧)の遅れ	• 定期的なオフラインバックアップとリストア訓練 • 情報収集と教育、ISACなどへの積極的な参画 • IT-BCPの策定と見直し

平時のパッチマネージメントサイクルと緊急時のサイクル

1. CISA-KEV

サイバーセキュリティ・インフラセキュリティ庁(CISA)
「Binding Operational Directive 22-01」(米国政府系システム向けの運用指令)
「攻撃コードが公開されており野生のインターネットで攻撃に悪用された事例が数多くある極めて重大なリスクのある脆弱性リスト(Known Exploited Vulnerabilities (KEV) catalog)」

2. JPCERT/CC Alert

深刻且つ影響範囲の広い脆弱性などに関する情報。メーリングリストで受け取れる

3. 特にインターネットに接点を持つ機器ベンダの情報

メーリングリストやRSS配信をチェック

平時のパッチ適用は、月やクォータ毎の定期パッチ。**適用間隔を数値で決めることが重要**。
緊急時は注意喚起が届いたら影響を確認し、即時適用するか定期パッチに入れるか管理者が判断

KNOWN EXPLOITED VULNERABILITIES CATALOG
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

JPCERT/CC 注意喚起
https://www.jpcert.or.jp/at/2022.html