ご挨拶

デジタルテクノロジー株式会社

ソリューション営業部 3課　堀口 聖太

2023/6/7

デジタルテクノロジーのソリューション

会社概要

会社概要

■商号　デジタルテクノロジー株式会社
■創業　昭和63(1988)年 8月
■資本金　100百万円(株式会社DTS 100%)
■従業員　105名(2022年4月1日現在)
■拠点　(本社)　東京都荒川区東日暮里5-7-18 コスモパークビル
(営業部門) 東京都中央区八丁堀2-23-1 エンパイヤビル
(大阪支店) 大阪市淀川区西宮原2-7-53 Marutaビル

主なお客様

電気機械系、製薬系、印刷系

従業員1,000名以下の中堅企業
(各種業種)

国立大学法人、独立行政法人

クラウド・データセンター事業者
通信事業者

約2,200法人の口座を保有

当社取扱製品沿革(一部)

基盤関係

1988年8月	Sun Microsystems製品取扱開始	各種UNIX製品取扱
1993年6月	NetApp製品取扱開始(国内第一号)	各種Storage製品取扱
2000年5月	VMware製品取扱開始(国内第一号)	VM社コンサル業務委託
2015年12月	Zerto取扱開始(国内第一号)	現 HPE
2013年11月	Nimble Storage取扱開始(国内第一号)	現 HPE
2016年12月	SimpliVity取扱開始(国内第一号)	現 HPE

バックアップ

1990年10月	Legato Networker取扱開始	現 DELLEMC
2005年1月	BakBone NetVault取扱開始	現 Quest Software
2013年7月	Commvault取扱開始	自営保守指定ベンダー
2016年4月	Veeam取扱開始	国内唯一のテクニカルパートナー
2017年3月	Barracuda製品取扱開始	Microsoft365バックアップ
2020年4月	Druva製品取扱開始	指定ディストリビューター

ランサムウェアに効果的な対策とは？

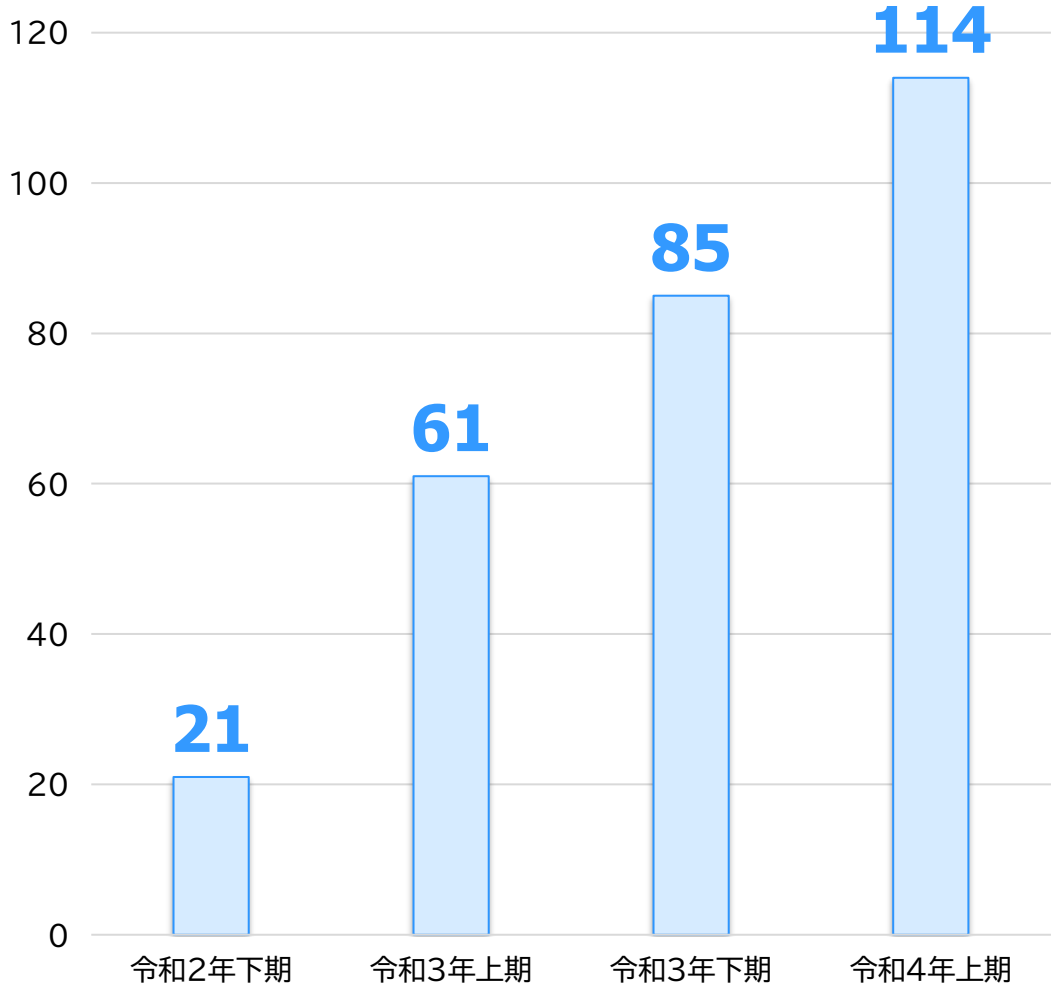
日本情報処理推進機構 情報セキュリティ10大脅威2023

順位	組織	昨年順位
1位	**ランサムウェアによる被害**	**1位**
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位
4位	内部不正による情報漏えい	5位
5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
7位	ビジネスメール詐欺による金銭被害	8位
8位	脆弱性対策情報の公開に伴う悪用増加	6位
9位	不注意による情報漏えい等の被害	10位
10位	**犯罪のビジネス化（アンダーグラウンドサービス）**	**NEW**

引用：**IPA**（日本情報処理推進機構）“情報セキュリティ10大脅威 2023”

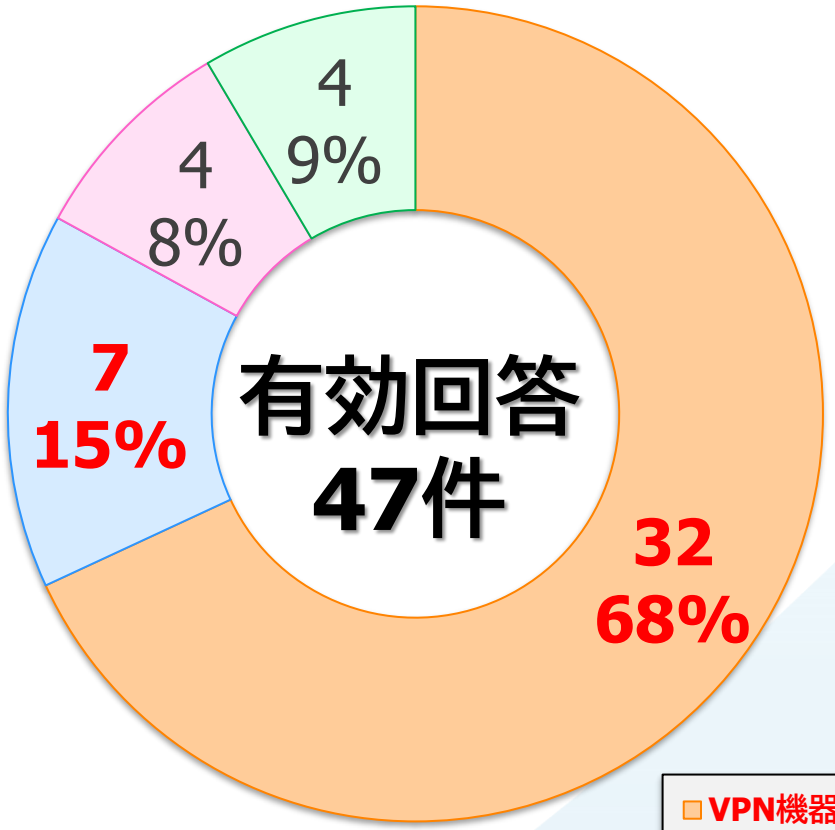
ランサムウェアの被害の状況

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



単位:件

感染経路

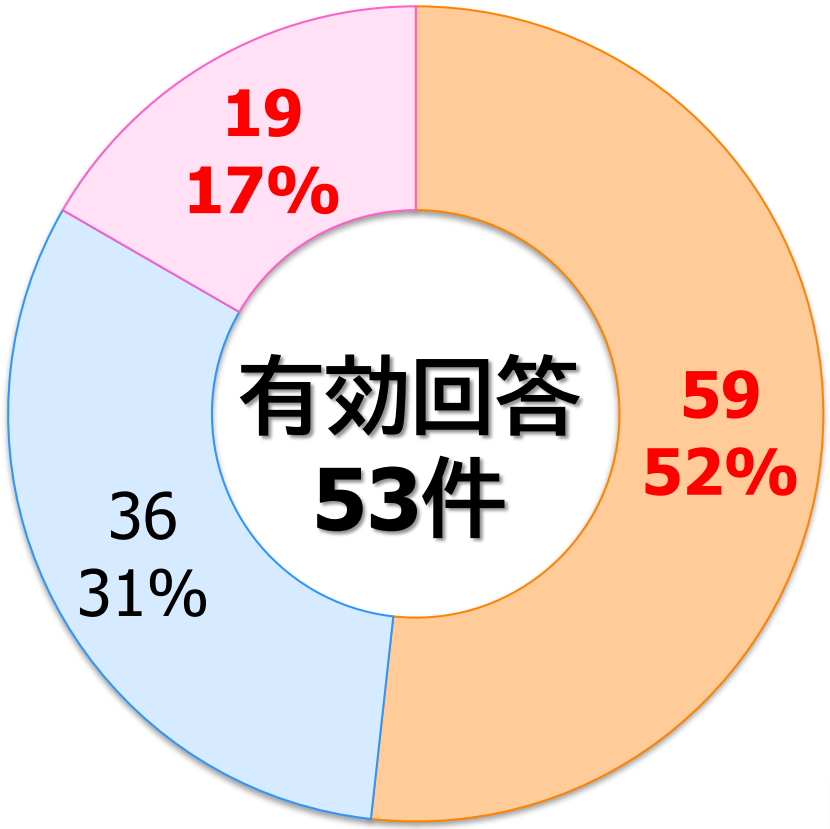


引用:警察庁「令和3年におけるサイバー空間をめぐる驚異の情勢等について」

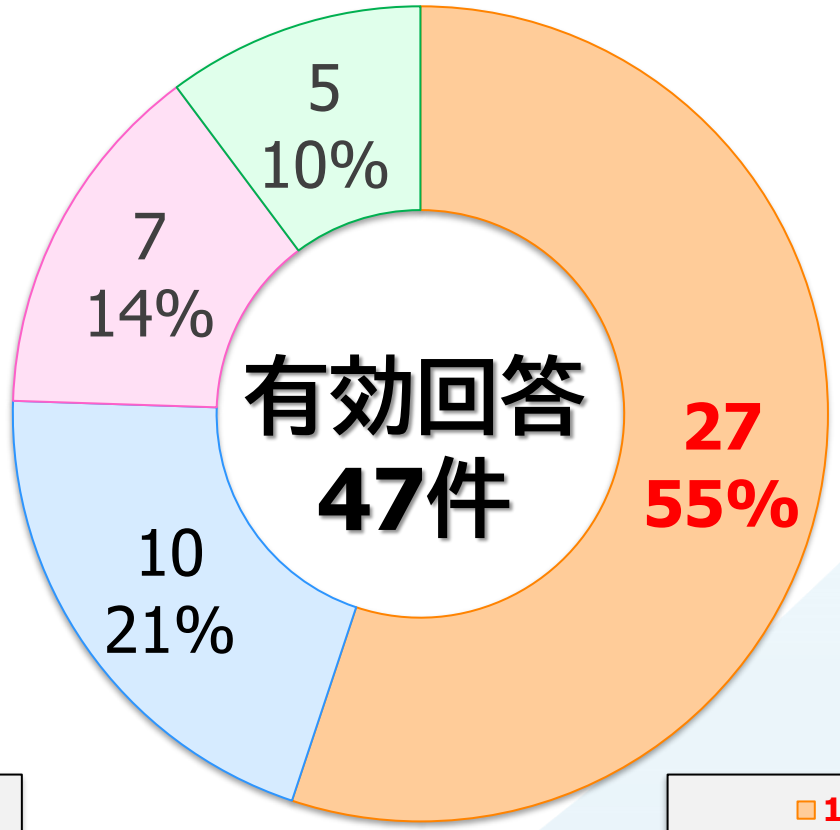
ランサムウェアの被害の状況

単位:件

被害団体の規模別報告



調査復旧費用の総額



引用:警察庁「令和4年におけるサイバー空間をめぐる驚異の情勢等について」

犯罪のビジネス化(アンダーグラウンドサービス)とは？

RaaS　Ransomware as a service

サイバー攻撃を目的としたサービスやツールが、
アンダーグラウンドで取引されているサービス名

**IT技術に精通していない反社会的勢力
がランサムウェア攻撃に参画**

ランサムウェアが狙って来るところとは？

主に**Windowsファイル共有のプロトコル（CIFS）**でつながるところが狙われます

Active Directory
ファイルの管理権限を乗っ取る目的

File Server
ファイル自体を攻撃

Backup Server
データ復旧を阻止し身代金を確実に取る目的

ランサムウェアが狙って来るところとは？

主に**Windowsファイル共有のプロトコル（CIFS）**でつながるところが狙われます

Active Directory
ファイルの管理権限を乗っ取る目的

File Server
ファイル自体を攻撃

重要：特にWindows OSベースのバックアップソフトは危険です

Backup Server
データ復旧を阻止し身代金を確実に取る目的

万が一のランサムウェア被害を想定して

経営者・自治体首長
絶対に身代金は払わないと決意する（相手は反社会的勢力）

情報セキュリティ部門
復旧手順と被害想定の洗い出しを事前に実施しておく

情報システム部門
エンドポイントセキュリティの見直しを行う

情報システム部門
「しかるべきシステム」でバックアップを取る

「しかるべきシステム」でバックアップを取る とは？

必須：バックアップデータ部分の隔離

必須：WORM(Write Once Read Many)機能の保有

推奨：振る舞い検知機能を保有

withランサムウェア時代に必要な対策(業種・従業員規模 問わず)

予防

被害者とならないための対策

教育・訓練
従業員のセキュリティリテラシー向上(セキュリティ研修、メール攻撃訓練etc)

認証
本人確認、個人権限の認可、常時確認、認証基盤(ADなど)の保護

脆弱性対策
パッチ適用、OS・ファームウェアの定期的なバージョンアップ

マイクロセグメンテーション
ワークロード単位の区画細分化、常時監視、感染時の隔離

Backup
バックアップデータの隔離、バックアップサーバの保護

EDR
異常監視と早期対策、被害の発生防止・抑制、アクセスログの保存・解析

ログ管理
各デバイスのログ管理、別拠点へのログ保管

監視

加害者とならないための対策

自社のWebサイト改ざん防止
自社サイトがウイルス被害拡散の踏み台となることを防ぐ。訴訟リスクの低減。

Restore
ランサムウェア感染後に正しくデータ復元

Recovery
代替環境の準備、緊急時のフェイルオーバー

復旧

withランサムウェア時代に必要な対策(業種・従業員規模 問わず)

予防

被害者とならないための対策

認証
本人確認、個人権限の認可、常時確認、認証基盤(ADなど)の保護

脆弱性対策
パッチ適用、OS・ファームウェアの定期的なバージョンアップ

Backup
バックアップデータの隔離、バックアップサーバの保護

EDR
異常監視と早期対策、被害の発生防止・抑制、アクセスログの保存・解析

監視

加害者とならないための対策

Restore
ランサムウェア感染後に正しくデータ復元

Recovery
代替環境の準備、緊急時のフェイルオーバー

復旧

実現できるサービス(SaaS)のご紹介

druva

AWS基盤上に作っているクラウドのバックアップサービス

inSync

エンドポイントバックアップ

PC/スマホ/タブレット/Microsoft365

Phoenix

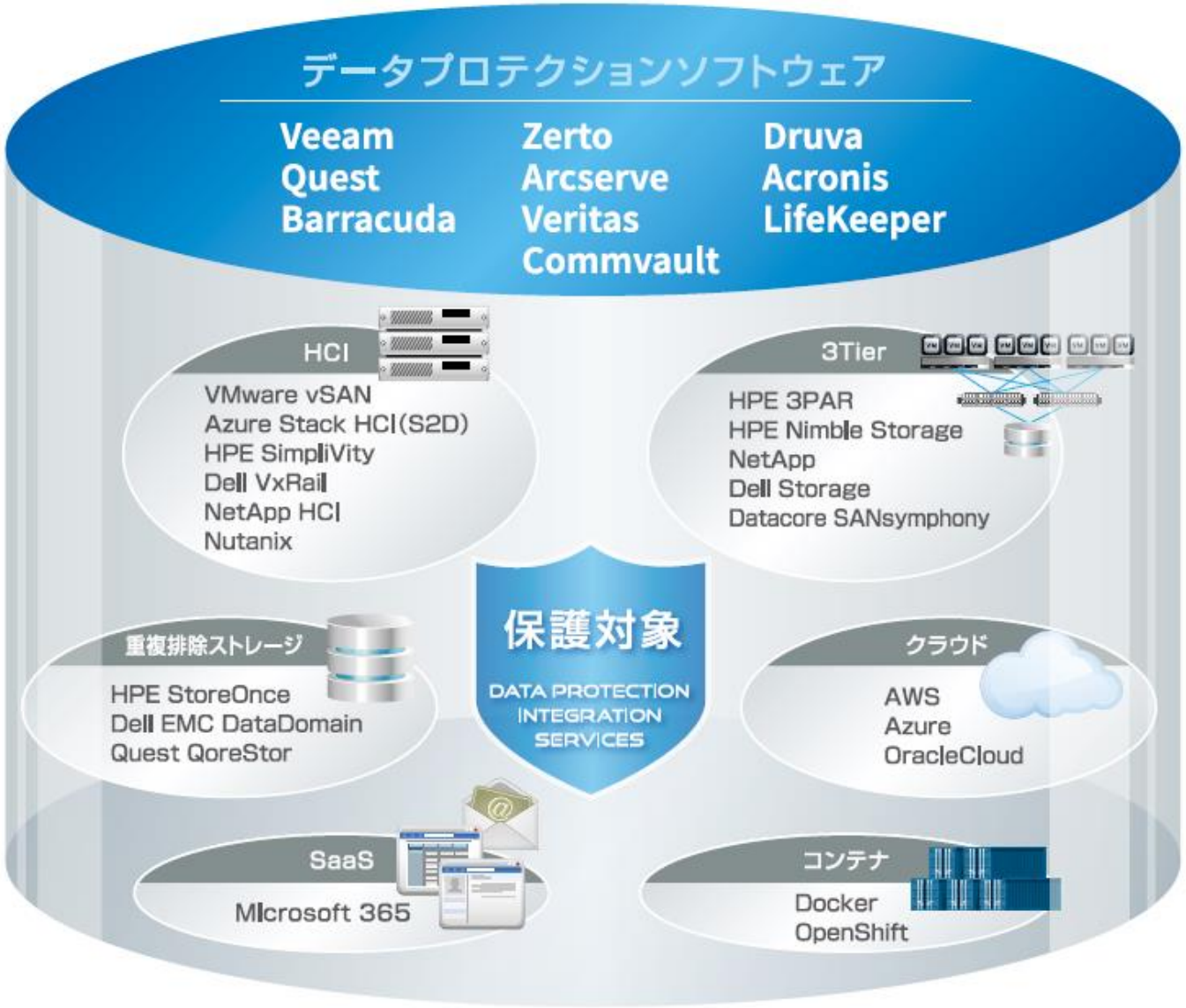
サーババックアップ

物理基盤/仮想基盤/各種クラウド

［事例］トレンドマイクロ社におけるエンドポイントバックアップ

某省庁でも本サービスをご採用戴いております

当社の強み



国内に流通するほぼ全ての
バックアップソフトウェアにおいて
構築運用の実績があります

バックアップで連携が必須である
各種ストレージ機器においても
構築運用の実績があります

**既存のストレージと
バックアップ環境の
コンサルが出来る
国内有数のSIerです！**

お問い合わせ

デジタルテクノロジー株式会社

URL https://www.dtc.co.jp/ransomware

東京本社	〒116-0014 東京都荒川区東日暮里5-7-18 コスモパークビル TEL:03-5604-7565
東京セールスオフィス	〒104-0032 東京都中央区八丁堀2-23-1 エンパイヤビル TEL:03-6914-5499
大阪支店	〒532-0004 大阪市淀川区西宮原2-7-53 Marutaビル TEL:06-6393-1301