

# 最近のサイバーセキュリティ事情 とクラウドバックアップについて

## 目次

1. 自己/会社紹介
2. 最近のサイバーセキュリティ事情
3. どう守っていくべきなのか
4. クラウドバックアップのご紹介

INJANET株式会社

---

2024/4/18 たちかわIT交流会

---

INJANET

# 紹介

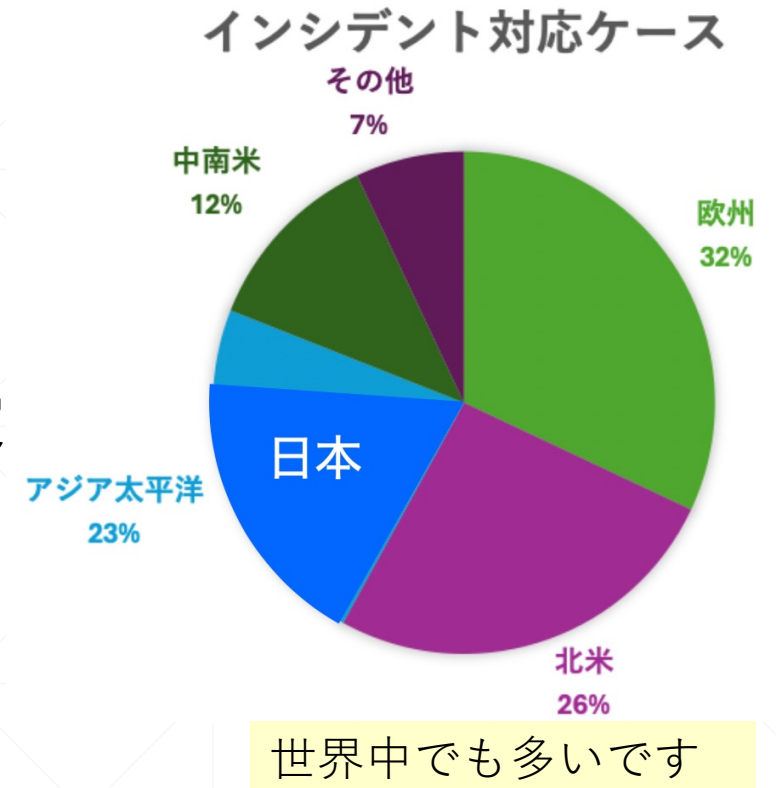
- INJANT(株) 代表取締役：福原聡
  - 立川市錦町在住 約25年
  - 元横河電機（武蔵野市）でエンジニア兼システム管理
  - IT系ライター(雑誌Software Design、Linux/Windows系、単行本など)
  - 現在 技術開発コンサルタント＋サイバーセキュリティ調査  
情報処理推進機構:IPA非常勤としてリスク分析等を担当  
立川市個人情報保護審査会委員
- INJANETのポリシー：すみずみにまでセキュリティ
  - 中小企業を含むすべての組織にセキュリティを



# 最近のサイバーセキュリティ事情ーインシデント

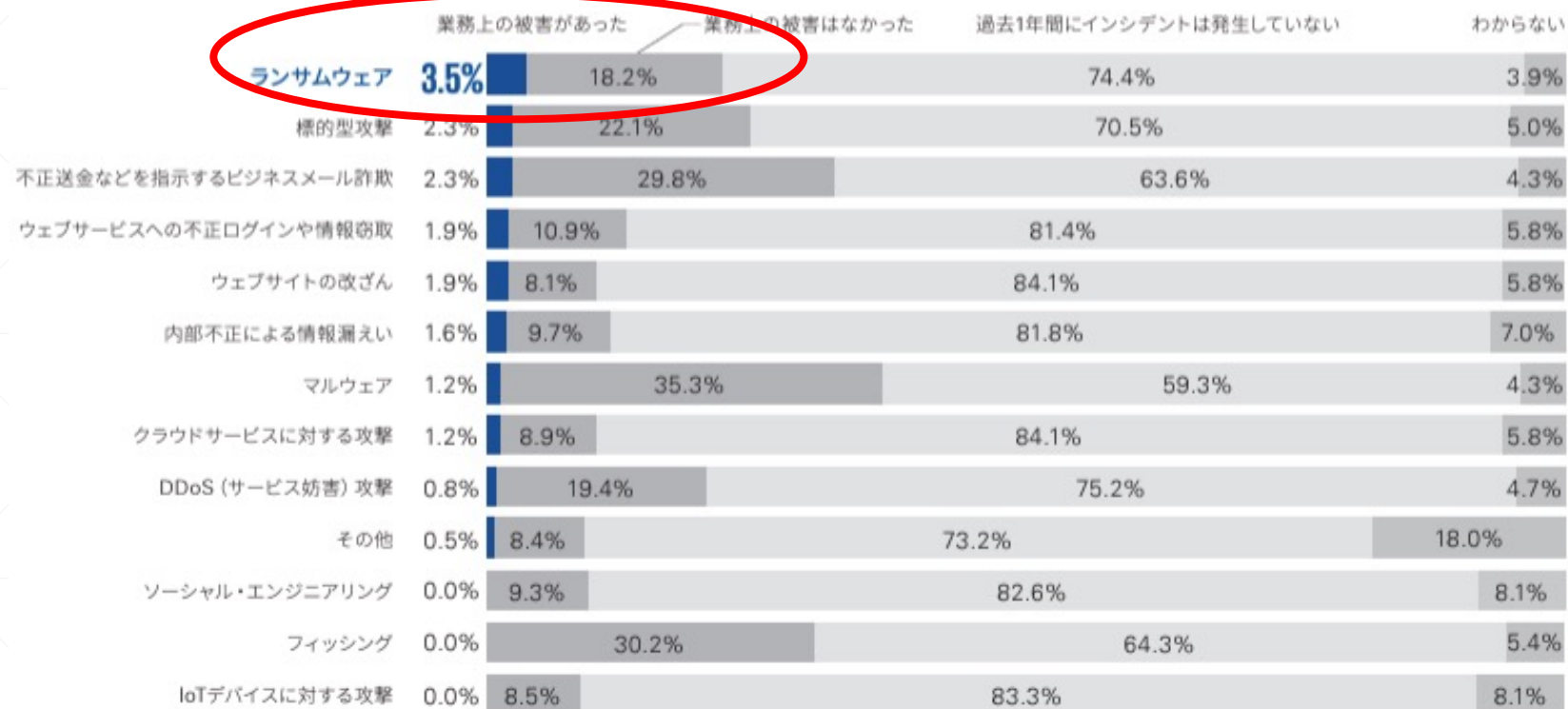
## • 事件

- 大阪急性期・総合医療センター
  - 復旧まで2ヶ月 + 損失数十億円
  - 出入りの業者（給食業者）から感染
- 名古屋港
  - 3日間業務停止（輸出入が止まる）



# 最近のサイバーセキュリティの実態－大企業

- KPMG 国内大企業（上場企業）4000社へのアンケート

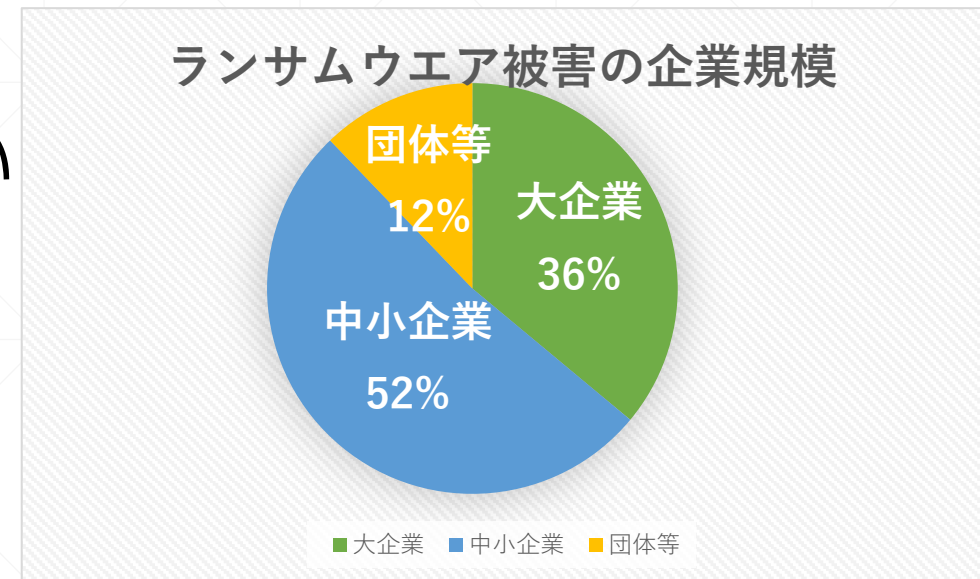


大企業だから  
この程度で済  
んでいる

<https://kpmg.com/jp/ja/home/media/press-releases/2024/02/kc-cs-survey2023.html> n=258

# 最近のサイバーセキュリティの実態－企業規模

- R5、ランサムウェア被害報告は197件\*1
- 年間で推計
  - 中小企業の件数は大企業より多い  
しかも対策が弱いので割合はさらに多いと思われる



\*1 警察庁：サイバー空間をめぐる脅威の情勢等 R5上期

\*2 IPA 2021年度中小企業における情報セキュリティ対策に関する実態調査

ランサムウェア以外にもサイバー攻撃はあります

# 最近のサイバーセキュリティの実態ーランサム攻撃

- ランサムウェアは現在、クラウドファンディング的
- 攻撃者と出資者がいる  
RaaS (Ransomware as a Service)

ランサムウェアでみんなで稼ごう！  
キャンペーン

The screenshot shows a crowdfunding campaign on the CAMPFIRE platform. The campaign title is "【募集！】日本の株式会社のランサムウェア攻撃ターゲット 株式会社XXX 株式会社YYY ZZZ合同会社". The campaign description includes "あくまでイメージです" (Just an image). The campaign goal is "予想成功時リターンxxx%" (Expected return xxx% at success). The campaign has received 28 supporters and has 17 days remaining. The current amount raised is 337,500 yen.

CAMPFIRE キーワード検索

プロジェクトを掲載するには

あくまでイメージです

【募集！】  
日本の株式会社のランサム  
ウェア攻撃  
ターゲット  
株式会社XXX  
株式会社YYY  
ZZZ合同会社 . .

予想成功時リターンxxx%

プロジェクト

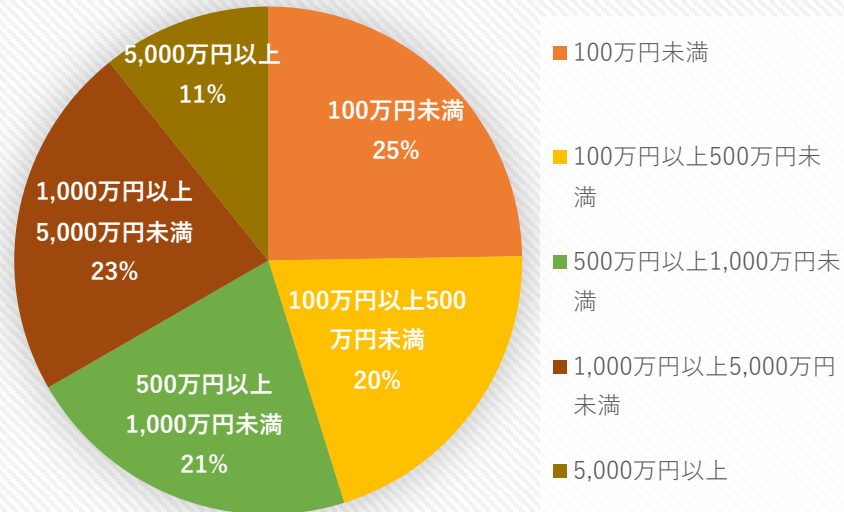
24時間で6人が支援

支援 28人 残り 17日

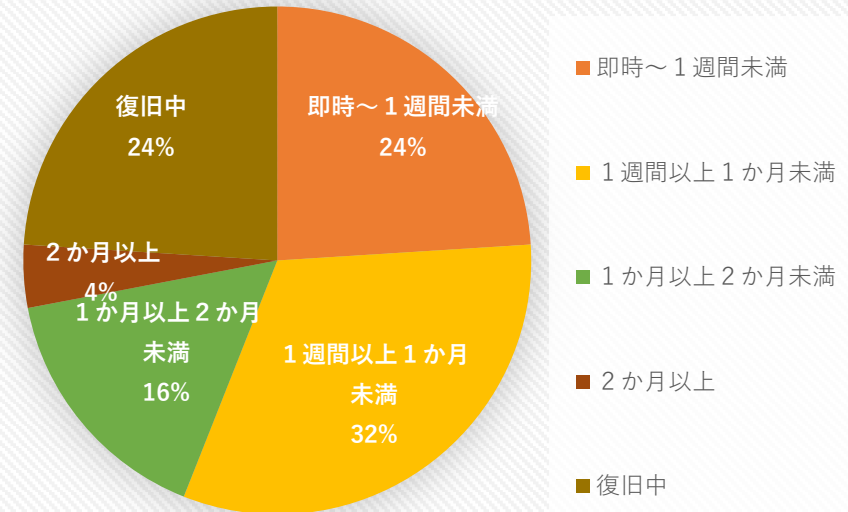
337,500 円

# 最近のサイバーセキュリティの実態ーランサム被害

## 調査・復旧費用の総額



## 復旧に要した時間



**調査、復旧に数百万円**

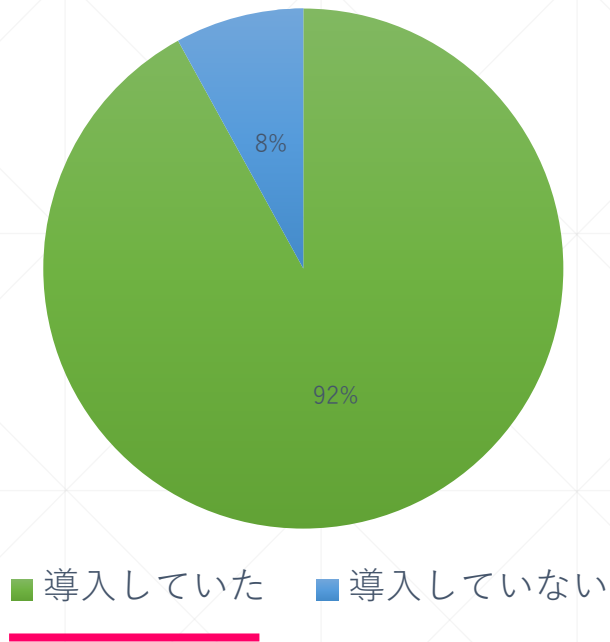
**半数が復旧まで1ヶ月程度**

\*1 警察庁：R5 サイバー空間をめぐる脅威の情勢等

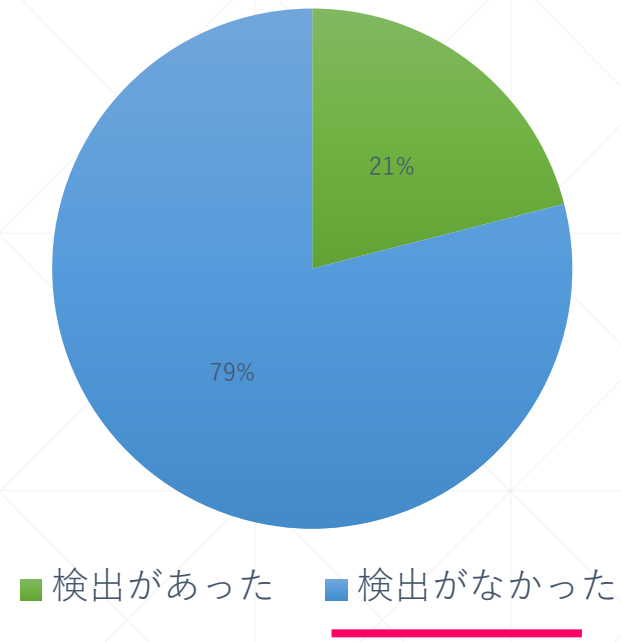
# 最近のサイバーセキュリティの実態－アンチウィルス

## ・アンチウィルスの効果

被害企業でアンチウィルスの導入



被害企業で検出があったか



\*1 警察庁：サイバー空間をめぐる脅威の情勢等 R5上期

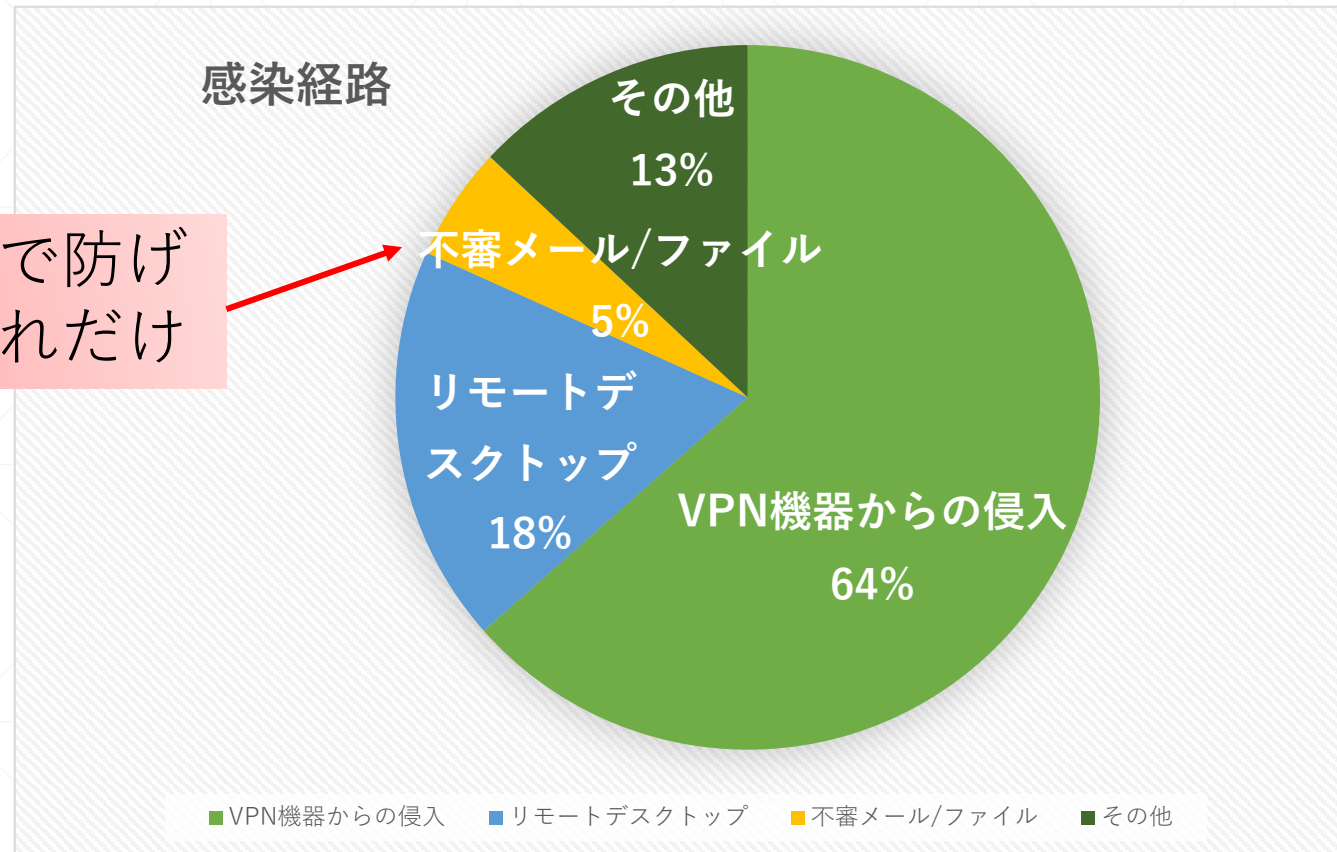


# どう守っていくべきなのかー感染経路

## ・感染経路

アンチウイルスで防げるのはたったこれだけ

\*一般的なアンチウイルスは  
ファイルを検査  
します



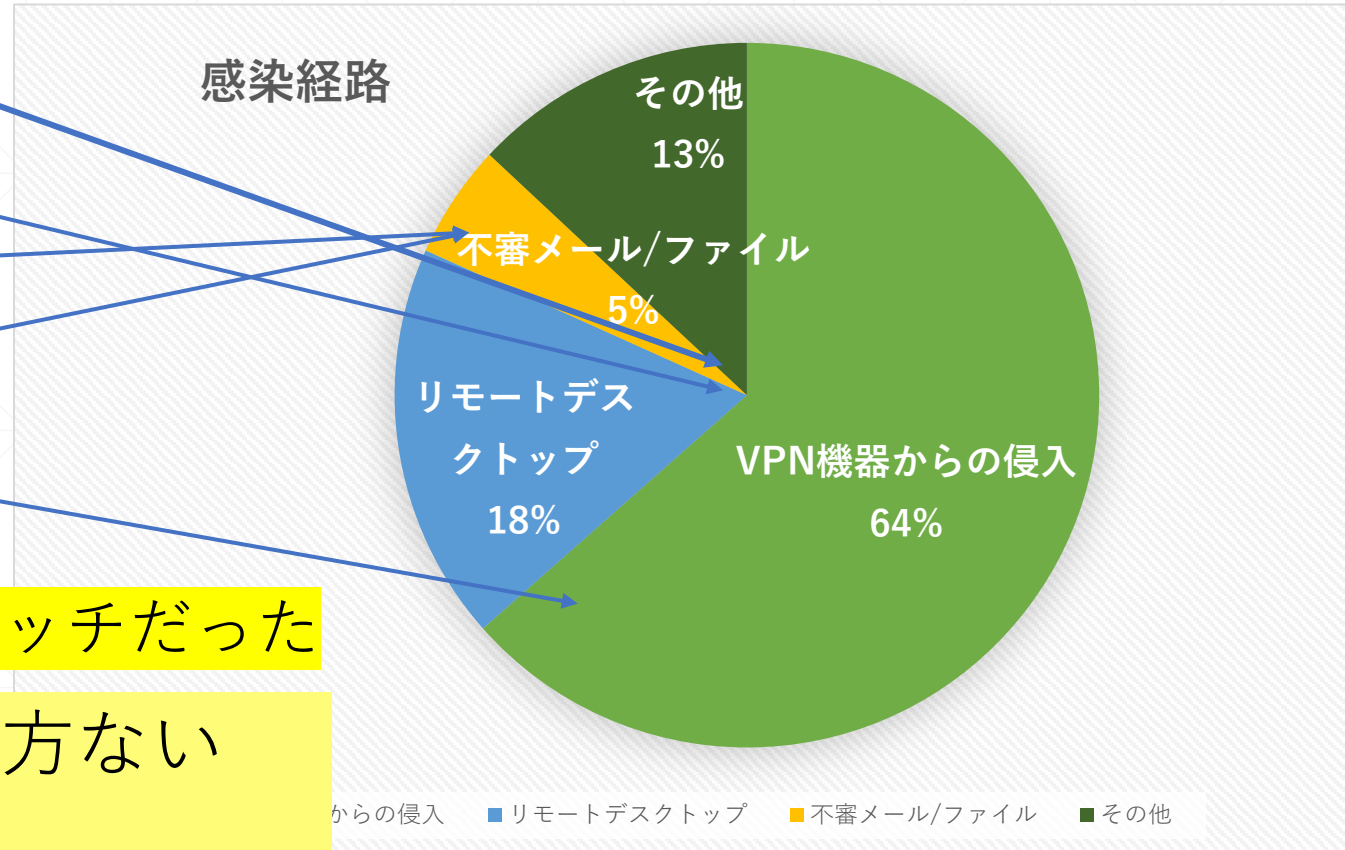
\*1 警察庁：サイバー空間をめぐる脅威の情勢等 R5上期

# どう守っていくべきなのかー対策

- ふるまい検知
- EDR
- URLフィルタ
- メール保護
- 日頃のアップデート

40%の企業では最新のパッチだった

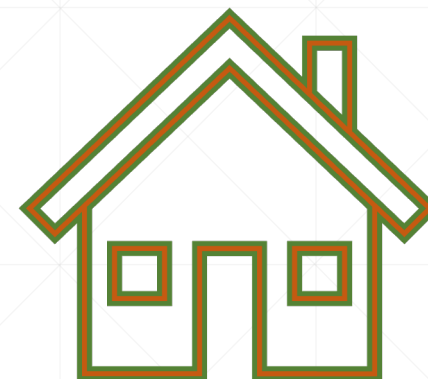
攻撃を受けるのは仕方ない  
バックアップが重要



# ここまでまとめると

- アンチウィルスを使っても被害の数%程度しか減らない
- 普段の管理（脆弱性管理、ID/パスワード管理等）がとても重要→  
毎日鍵をかけて、鍵が古くなったらすぐ交換する
- といってもサイバー攻撃の過半数は防げない

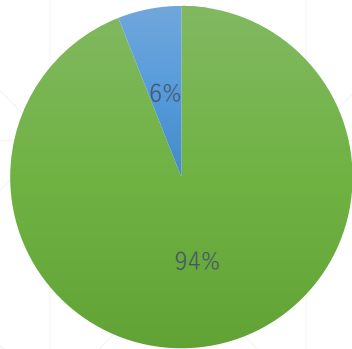
→大切なものは金庫（バックアップ）へ



# どう守っていくべきなのかーバックアップの現状

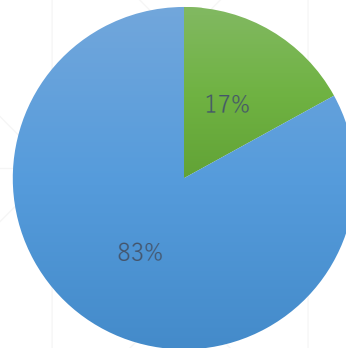
- バックアップも暗号化されます

バックアップの取得



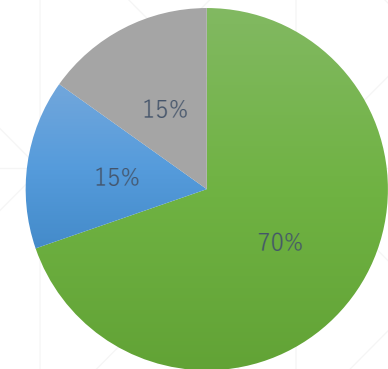
■ 取得していた ■ 取得していなかった

バックアップからの復元



■ 復元出来た ■ 復元出来なかった

復元できなかった理由



■ バックアップも暗号化  
■ 運用の不備  
■ その他

\*1 警察庁：サイバー空間をめぐる脅威の情勢等 R5上期

# どう守っていきべきなのかー推奨のバックアップ

- 共有フォルダ（サーバ）のデータは暗号化される
- クラウド上のデータも暗号化される
- 同期を取っているクラウドデータは暗号化されたファイルで上書き



対策方法は、

- **オフラインバックアップ（バックアップ後断線する）**
- **マルウェア/ランサム対応クラウドバックアップ**

# Acronis Cyber Protect

## 中小を悩ませるサイバーセキュリティ対策

- 全部の対策は困難で、高価
- そもそもシステム管理者がいない
- 問題発生時、別々のベンダーだと何が原因かわからない

オールインワンのセキュリティ管理ソリューション

(必要部分のみも可能)

Acronis Cyber Protect

The Acronis logo is displayed in white text on a dark blue rectangular background.

# Acronis社とは

- 本社がスイスとシンガポール
- 取り扱い高 3億ドル
- 150カ国以上で販売、11カ国にデータセンター

Acronis

AI搭載のサイバープロテクション, Cyber Cloud, Cyber Platform

## スイス

2008年にスイスの  
シャフハウゼンに  
コーポレート本部を  
設立

二重保護のため2拠点に本社を設置



## シンガポール

2003年シンガポールに  
国際統括本部を設立



## 拡大 & 急成長

取扱高3億ドル超  
企業成長率50%達成  
クラウドビジネス成  
長率100%達成



## 国際的な存在感

1,500名以上の従業員  
33か所を超える拠点  
150か国以上で販売実  
績  
33言語に対応  
11か国にデータセン  
ター, 2年以内に200か  
国以上に拡大計画



## Acronis Cyber Protect

1,600,000+ のコン  
ピュータ保護  
1,000,000+ の攻撃防御  
実績  
18,000+ のパートナー、  
サービスプロバイダー

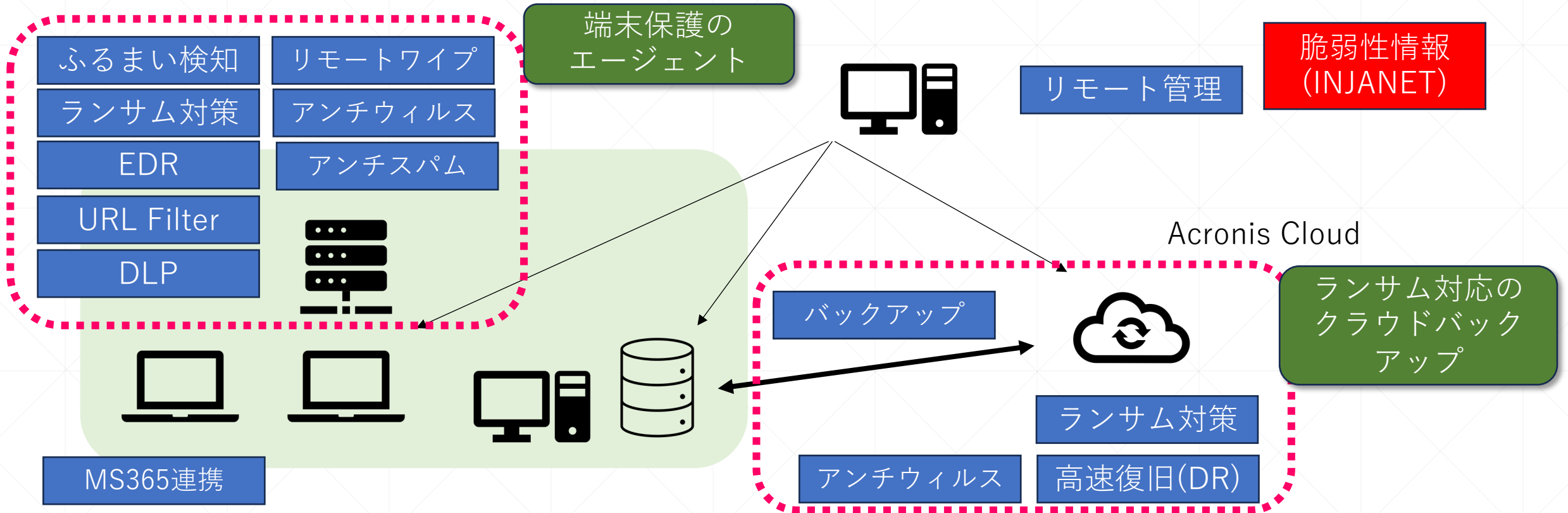


中小企業をメイン  
ターゲットにした低  
料金のソリューション(300円台/1台/月  
~)

INJANET

# Cyber Protect Cloudの全体像

- 主に中小を顧客としたセキュリティ管理のワンストップ統合ソリューション





# Cyber Protect Cloud セキュリティ機能

## ワンストップ統合ソリューション

- オンラインバンキングを安心に行いたい →
- データを確実に保護したい →
- EDRを導入したい →
- ソフトウェアアップデートの管理コストを下げたい
- 情報漏えいを防ぎたい（内部不正対策） →
- 災害復旧を迅速に →
- Etc.

E-mail Security

Protect Cloud

Advance Security EDR

Advance Management

Data Loss Prevention

Disaster Recovery

# Cyber Protect Cloud バックアップ機能

- クラウドバックアップは、**アンチウイルス、アンチランサムウェア**搭載
- クラウドバックアップが 99世代まで保存可能
- MS Office、Google Cloud等にも対応
- オンプレミスバックアップにも対応
- Disaster Recovery（災害復旧）オプションあり

# Cyber Protect Cloud コンソール機能

- リモート管理（アップデート、再起動など）可能
- ステータスマニタ
- コンソールはユーザ様が利用、または弊社で管理も可能

The screenshot displays the Acronis Cyber Protect Cloud management console. The interface is divided into several sections:

- 概要 (Summary):** Overview of system protection status, active alerts, and activity. It includes circular gauges for protection status (3 machines), alerts (5 total), and device status (2 machines).
- アラート (Alerts):** A table listing alerts with columns for time, type, severity, device name, plan name, and message.
- デバイス (Devices):** A list of managed devices including INJANET\_test, Microsoft 365, and PC-YFINJ.
- バックアップ (Backup):** Detailed view of backup operations for LAPTOP-OFBKPUV7 and PC-YFINJ, showing backup status, schedule, and file details.

アラート時刻	アラートタイプ	アラート重要度	デバイス名	計画名	アラートメッセージ
01:59	Microsoft Defenderファイアウォール...	警告	PC-YFINJ	新しい保護計画	内部エラーにより、Mig
13:45	Microsoft Defenderファイアウォール...	警告	PC-YFINJ	新しい保護計画	内部エラーにより、Mig
14:18	マルウェアが検出され、隔離されま...	警告	PC-YFINJ	新しい保護計画	オンデマンドスキャン
14:10	マルウェアが検出され、隔離されま...	警告	PC-YFINJ	新しい保護計画	オンデマンドスキャン

ありがとうございました。

気になる点があればまずはこちらご連絡ください。

今後ともよろしくご依頼申し上げます。

---

**INJANET**