

## 貴社経営資産である「データ」の 統合型保護ソリューション Acronis Cyber Protect ご紹介

アクロニス・ジャパン

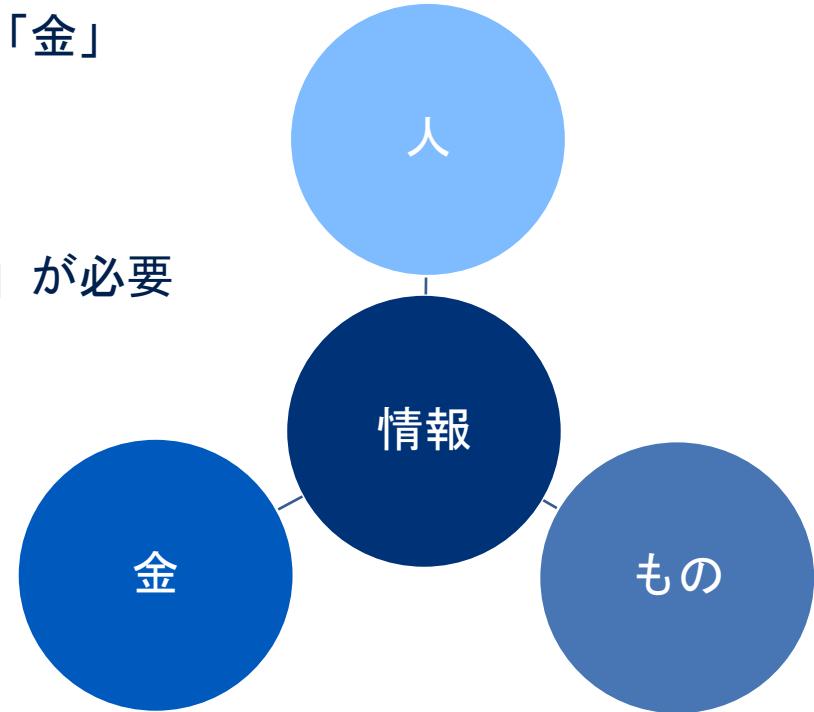
メッセージ：

「貴社ビジネスの「データ」を  
自然災害やランサムウェア攻撃からお守りしたい」

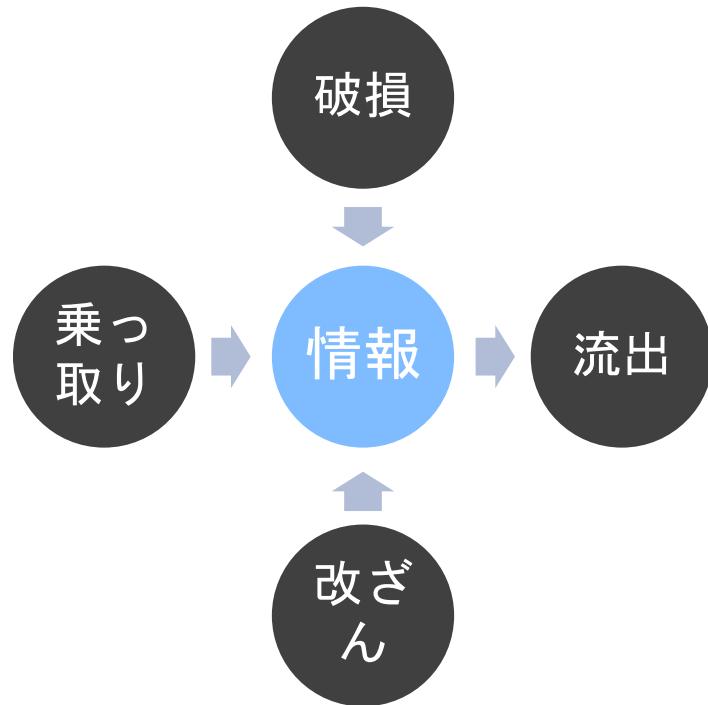
# 経営の安定と拡大

- 経営資産を有効に活用する「人」「もの」「金」
- 「情報」そのものが重要な資産
- 「人」「もの」「金」の可視化には「情報」が必要
- すなわち

情報 を常に安心して活用できる状態  
が重要



# 経営目線で情報をお護りする事：何からお護りするか



# これまで：各対策アプリ=「もの」を導入する

- 「とりあえず」、セキュリティやバックアップ対策アプリ=「もの」を導入すれば大丈夫と思っていませんでしたでしょうか。
- 実際は複数アプリ運用が非常に面倒⇒全く「とりあえず」になっていない

- アプリ設定を各PC・サーバに適用 : 大変
- アプリ管理サーバの管理 : 面倒
- アプリ自身のパッチダウンロード : 大変
- サポート契約、そのコスト : 面倒、高い
- 使い方習熟 : 面倒、人がいない、先々人がいない
- セキュリティアプリの  
バックアップ動作の誤検知 : 業務中断、不便

# これまで：情報を守る複数のアプリ=「もの」を導入

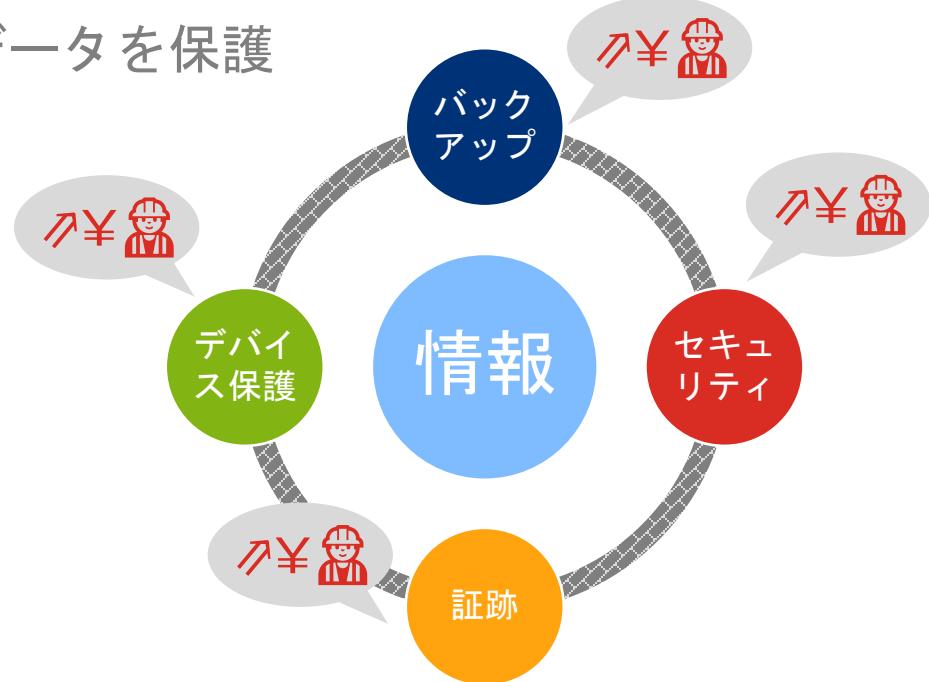
- 従来：複数のアプリケーションでデータを保護

- 管理の複雑化 

- 誤検知による業務停止の頻繁化 

- 維持するための人材不足 

- 複数アプリ契約、高コスト 



# Acronis : 情報をお護りする「こと」をご提供

Acronis Cyber Protect

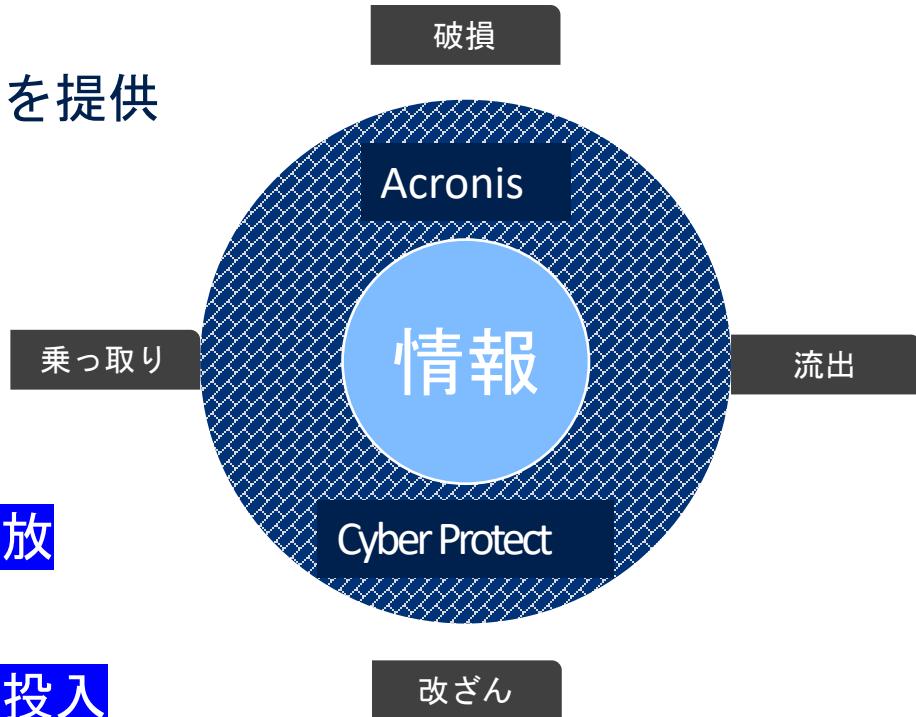
- 情報保護統合ソリューション
- =情報を強固にお護りする「こと」を提供

- ・貴社コンピュータの情報を一括管理
- ・バックアップ+セキュリティ
- ・誤検知の極小化
- ・バックアップを安全に保護
- ・災害時のディザスタリカバリ
- ・強固なランサムウェア対策

これまでの様々な煩わしさからの解放

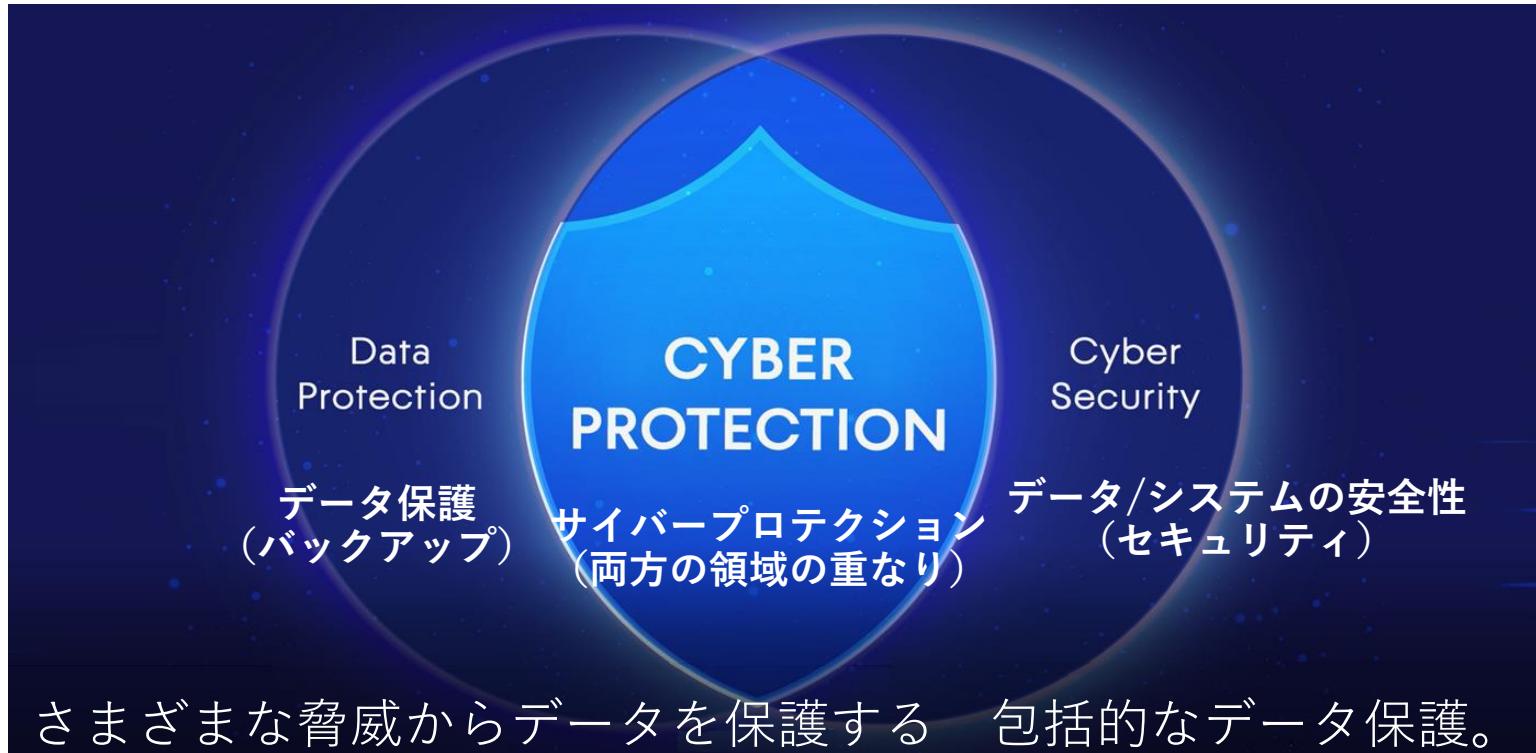
トータルコスト削減

貴重な人材の貴社主力業務への集中投入



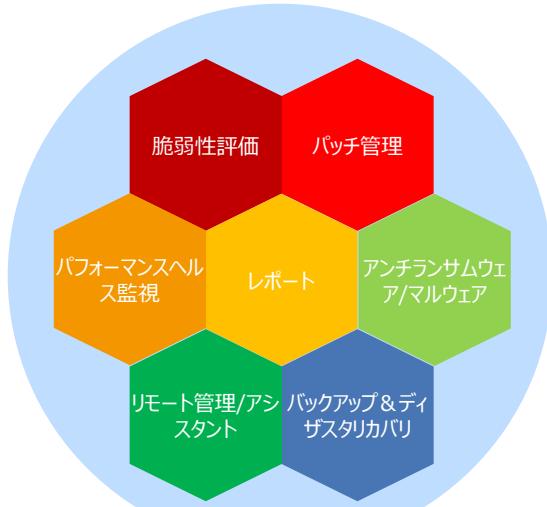
# データ総合保護ソリューション

## - サイバープロテクション -



# Acronis Cyber Protect

## オールインワン型Cyber Protection&管理ソリューション：管理サーバが不要



Acronis

OVERVIEW

Dashboard

Alerts

Activities

Reports

DEVICES

PLANS

BACKUPS

SETTINGS

Powered by Acronis AnyData Engine

Dashboard

PROTECTION STATUS

Group: All

105 Protected

OK: 105  
Warning: 1  
Error: 1  
Critical: 2

STORAGE

Location: test\_storage\_1

454.7 TB Total space

Backups: 181.0 TB  
Other files: 69.8 TB  
Free space: 181.0 TB

ACTIVITIES

Group: All

130 Sat Mon Wed Fri

Successful: 130  
Warning: 0  
Failed: 0

ACTIVE ALERTS (6)

Alerts: All alerts ▾

- Ubuntu 16.04 x64: Validation failed
- Linux Mint: Validation failed
- Windows 10: Backup transaction
- Windows 10 Home: Backup failed
- Ubuntu 16.04 x64: Backup failed

MONTHLY STORAGE USAGE

Location: Total storage usage

Current size: 1.1 PB

17 Apr 24 Apr 1 May 8 May

NOT PROTECTED (4)

Group: All

- Windows 10 Home: Physical machine
- Ubuntu 16.04: Virtual machine
- Linux mint: Virtual machine
- abe-win-inst2: Virtual machine

Antivirus

Full scan, on Mondays

Severity: Remove

High: Remove

Medium: Skip

Low: Skip

Real-time protection

Advanced

Any Antivirus Engine

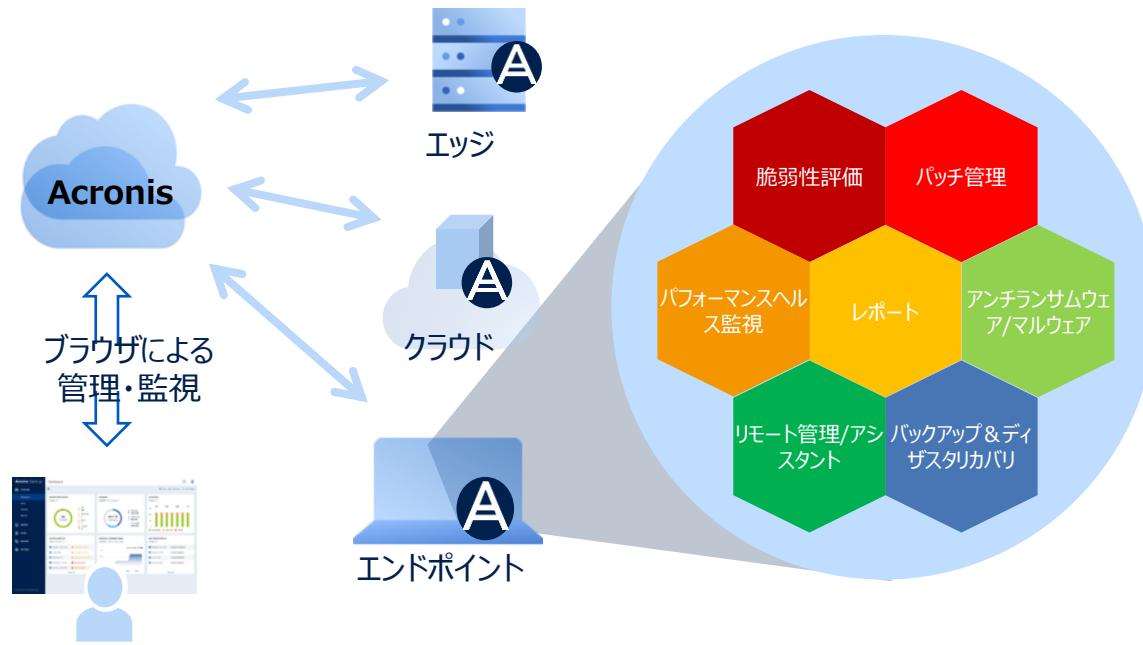
Windows Firewall

Exclusions

Vulnerability assessment

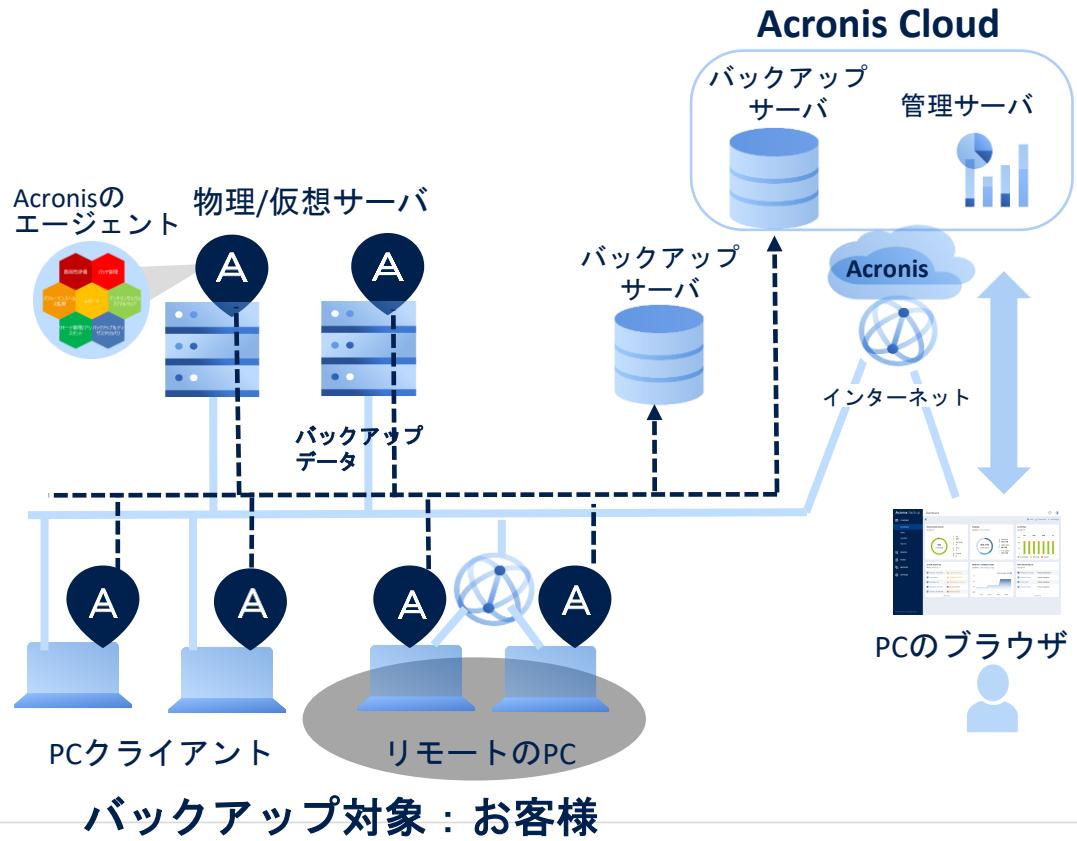
バックアップとディザスター回復にセキュリティを加え強化し、管理サーバ不要、ブラウザによる管理で管理とリモート操作によりIT管理者の労力を最小化し、貴社システムの可用性を最大化する

# オールインワン型 バックアップ+セキュリティ+IT管理 統合ソリューション



-  **単一ライセンス**
-  **単一ユーザインターフェース**
-  **単一管理コンソール**
-  **単一エージェント**

# Acronis Cyber Protect の構成



- ・ハイブリッドなバックアップ
- ・NAS
- ・バックアップに最適化されたクラウドストレージ提供
- ・管理サーバ不要
  - ・管理機能をクラウドから提供
  - ・ブラウザベースのシンプルな管理画面
- ・リモートデスクトップ機能でリモートワーカーの業務を支援

# Acronis Cyber Protectが実現する強固なデータ保護

バックアップ+AIセキュリティ+IT管理  
統合ソリューションです。

通常のAIセキュリティ保護に加え  
バックアップ/レストア時に  
セキュリティチェックする保護計画を簡単  
に設定でき、

更にCloud上へもバックアップ保護  
そのアーカイブをセキュリティスキャンし、  
更なるシステム保護を提供する、  
唯一のサービスです。

	Acronis Cyber Protect	他社 バックアップ サービス	他社 セキュリティ サービス
セキュリティ チェック機能	○		○
バックアップ 機能	○	○	
バックアップ/ セキュリティ 統合コンソール	○		
バックアップ& セキュリティ チェック	○ 自動や同時設定 単一コンソール		
レストア& セキュリティ チェック	○ 人気 機能		マルチベンダーで オペレーションが大変

# 1つの保護計画でトータル管理

機能のオン/オフ含めて  
クラウド上で統合管理：

- バックアップ
- マルウェア対策
- URLフィルタリング
- 脆弱性診断
- パッチ管理
- データ復旧（データプロテクションマップ経由）
- Windows Defender AntivirusとMicrosoft Security Essentialsの管理

The screenshot displays the Acronis Cyber Cloud web interface. On the left, a sidebar menu includes 'アカウントの管理', 'タッシュボード' (with a red notification dot), 'デバイス', 'すべてのデバイス' (selected), 'エージェントがインストールされているマシン', 'Mobile devices', 'エンドカスタマー - 日本', 'Microsoft Office 365', 'G Suite', '非監理マシン', 'データ保護マップ', '計画', and 'ディザスタリカバリ'. The main content area is divided into three sections: '保護計画' (Protection Plans) showing a list of plans with names like 'ファイル& ローカル', 'Mobile backup', 'Acronis Cyber Protect保護計画-WIN2016', and 'Acronis Cyber Protect 保護計画'; 'すべてのデバイス' (All Devices) showing a list of devices including 'WIN2016-1.jpdemo.local', 'Sato\_Photo', 'EC2-WIN2012R2-1', 'WIN2019-1', 'Azure-WIN2012R2-3', and 'WIN10-1'; and a detailed view for 'WIN2016-1.jpdemo.local' showing various protection settings like 'バックアップ' (Backup), 'マルウェアからの保護' (Protection from Malware), 'URL フィルタリング' (URL Filtering), 'Windows Defender Antivirus' (Windows Defender Antivirus), '脆弱性診断' (Vulnerability Scan), and 'データ保護マップ' (Data Protection Map). The right sidebar contains 'アクション' (Actions) with options like '新規の作成' (Create New), 'インポート' (Import), '詳細' (Details), '編集' (Edit), 'アラート' (Alerts), 'クローンを作成' (Create Clone), 'エクスポート' (Export), '無効化' (Disable), and '削除' (Delete).

統合管理により効率的な自動保護を実現

# パワフルかつ様々な機能群 = 貴社サービスの拡充

1つのエージェント、1つの管理コンソールで  
ライセンスでバックアップとAI型セキュリティ + 多彩な機能を提供（更に拡張予定）

✓ バックアップ	✓ パッチ管理	✓ Remoteデスクトップ <sup>°</sup>
✓ バックアップの保護	✓ URLフィルタリング	✓ ファイル同期・共有
✓ ディザスタリカバリ	✓ 脅威アラート	✓ ファイルノータリゼーション
✓ AI型ランサムウェア対策	✓ Web会議保護	✓ 電子署名
✓ マルウェア対策	✓ デバイス制御	
✓ 脆弱性診断	✓ レポート機能	✓ +新機能 (本年,次年と次々リリース)

# バックアップ

# Acronisのバックアップ<sup>®</sup>

簡単、効率的、さらにセキュアなバックアップ機能を提供

## 簡単

### ロスタイム無く復旧

- 問題発生があったことを気付かれないほど迅速に、VM としてバックアップを開始し迅速に復旧可能
- サーバやPCをペアメタルまたは異種ハードウェアに柔軟に復元することで、半分の速度で復旧完了
- **変更された情報ブロックのみを抽出しバックアップに保存することで、VMの復旧時間を最大百分の一に短縮**

## 効率的

### 生産性維持

- **オンプレミスまたはクラウド上の管理サーバーのデプロイを活用し、インフラの負荷を軽減**
- 管理作業の簡素化によりIT担当者の作業時間は20%増加。最小限の作業量でバックアップ業務の完遂を実現
- データ/デバイスの増強に伴うクラウドストレージの導入により、作業量を最大10分の1に低減

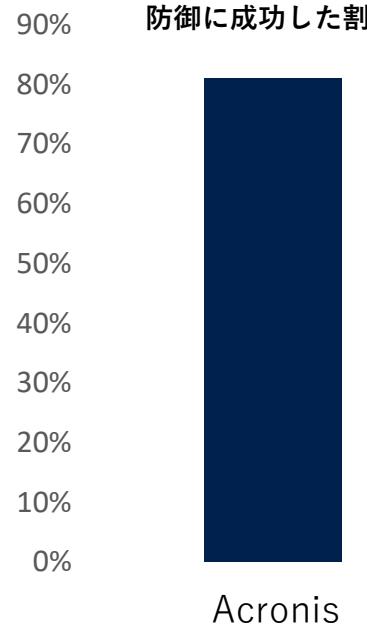
## セキュア

### データを安心・安全に保護

- 20種以上のプラットフォームに対応可能な単一のソリューション(物理および仮想、クラウド、アプリ、モバイル等)
- **組み込み式のサイバー脅威保護機能**に付帯するランサムウェア攻撃を排除 – 従来にない200,000件もの攻撃を防御
- アーカイブファイルを標的とした攻撃を防御する革新的なブロックチェーンベースの技術により、データの整合性を確保

# バックアップソフトを自身で守るAcronis 第3者機関によるソフトウェア攻撃

31項目の試験シナリオ



ファイルの保護	バックアップファイルの保護
	プログラムの保護
	プロセス、サービスの停止
	コード注入
プロセス、サービスの保護	プロセスメモリの変更
	プロセスオブジェクトの変更
クラウドバックアップの保護	クラウドバックアップデータの変更
	DNSポイズニング

# 幅広いサポートプラットフォーム

- **Acronis Cyber Protectは20以上のプラットフォームを保護**
  - ✓ 物理、仮想、オンプレミス、クラウドを問わずあらゆる環境のシステムとデータを保護
- **ベンダーサポートが終了しているOSもバックアップ対象としてサポート**
  - ✓ Windows XP Professional, Windows Server 2003 SP1など



Azure	Windows Server	Windows PC	Exchange	SQL Server	Share Point	Active Directory	Hyper-V	Office 365	G Suite	Linux サーバー	SAP HANA
-------	----------------	------------	----------	------------	-------------	------------------	---------	------------	---------	------------	----------



ORACLE®



Amazon EC2
------------

Mac
-----

iPhone
--------

iPad
------

Android
---------

VMware vSphere
----------------

Oracle x86 VM Server
----------------------

Oracle Database
-----------------

Red Hat Virtualization
------------------------

Linux KVM
-----------

Citrix XenServer
------------------

Virtuozzo
-----------

Nutanix
---------

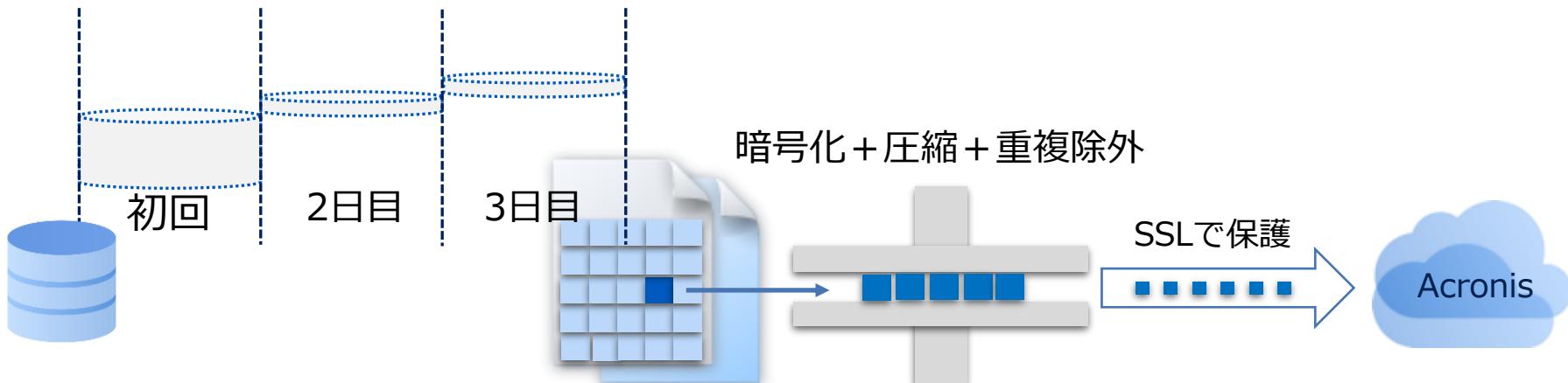
サポートされるバックアップ対象

[https://www.acronis.com/en-us/support/documentation/CyberProtectionService/index.html#supported-operating-systems-and-environments.html?TocPath=Software%2520requirements%257C\\_\\_\\_\\_\\_3](https://www.acronis.com/en-us/support/documentation/CyberProtectionService/index.html#supported-operating-systems-and-environments.html?TocPath=Software%2520requirements%257C_____3)

# 超効率、安全なバックアップ

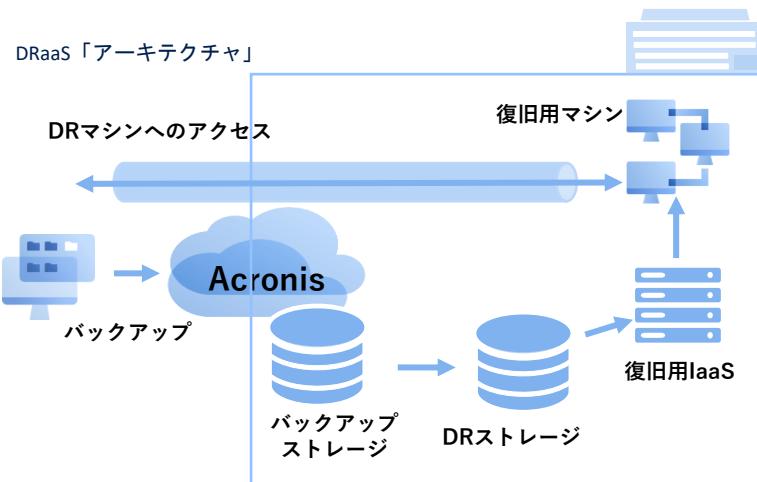
- ◆クラウドへのバックアップに備えた効率性と安全性
- ◆増分（ブロック）データを高度に検出
- ◆転送前に圧縮、暗号化、重複データ除外
- ◆世代管理のための超高速バックアップマージ

## 永久増分バックアップ

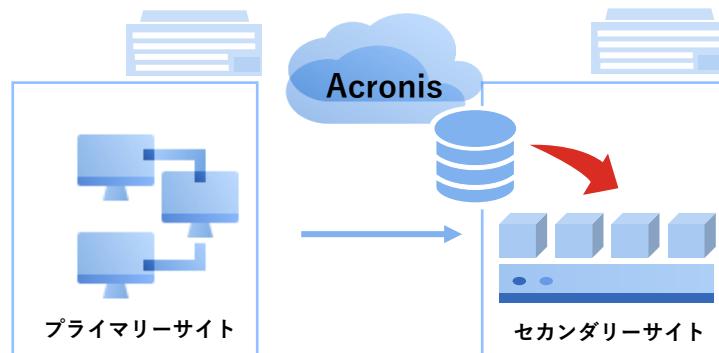


# 災害時のバックアップ、DR

- Disaster Recovery as a Service (DRaaS)
  - 災害が発生したときにフェールオーバーを実行するため、サーバーのレプリケーションおよびホスティングサービス
  - ミッションクリティカルなアプリケーションとデータを保護
  - 自前のDRサイトを事前に準備せずに環境構築
  - 簡単、迅速にデプロイ
  - セキュアなインフラ
  - 従量課金の料金設定
- インスタントリストア
  - 仮想マシン起動までの自動化
  - 簡単な手順での復元のリハーサル（スケジュール可）
  - 遠隔データセンタを利用した高速ディザスタリカバリ
  - VMの動作に必要なデータのみを展開することからRTOを数分にすることが可能
  - バックアップアーカイブから直接VMを起動



遠隔地への復旧「Instant Restore」



# 継続的データ保護

## 重要なデータの変更を継続的に保護することでRPOを削減

- 指定した領域に変更が加わると自動でバックアップ
- 作業工程を失いたくない状況で有効



### 利点

変更を常に監視し、変更があったファイルを即時バックアップ

- ◆ ファイル/フォルダ指定  
選択したフォルダ配下、または選択したファイル自体が更新されるごとにバックアップします。
- ◆ アプリケーション指定  
選択したアプリケーションによって変更された全てのファイルを更新ごとにバックアップします。

重要なファイルをリアルタイムで保護することが可能

新しい保護計画

キャンセル 作成

バックアップ  
マシン全体 クラウドストレージ、月曜日から金曜日 11:15 に行う + CDP

バックアップの対象 マシン全体

継続的データ保護 (CDP)

アプリケーション: Acrobat Distiller, Adobe Acrobat DC+ 39 その他

継続的な保護対象のアイテム

バックアップ先 クラウドストレージ

スケジュール 月曜日から金曜日 11:15 に行う

保持する期間 月単位: 6 月  
週単位: 4 週  
日単位: 7 日

暗号化

アプリケーションバックアップ 無効

バックアップオプション 変更

# セキュリティ

バックアップソフト会社のセキュリティ機能って、  
おまけ的な程度でしょ？

いいえ。このサービスは違います。

他社が実現できていない仕組みで、  
強固な「データ保護」を実現しています。

## ■ ICSA Lab. (認定 ※3)



テストの種類 ※2	Real Time Protection	On Demand Scanning	ICSA Labs	False Positive Testing (誤検知テスト)
結果	98.23%	99.89%	99.98%	0

Endpoint Anti-Malware Certification Testing Report. July 24, 2020

Test Version: 12.5.23094 ※4

[https://www.icsalabs.com/sites/default/files/FINAL\\_Acronis\\_Endpt\\_Anti-Malware\\_Report\\_20200724.pdf](https://www.icsalabs.com/sites/default/files/FINAL_Acronis_Endpt_Anti-Malware_Report_20200724.pdf)

## ■ Virus Bulletin (認定 ※3)



テストの種類 ※2	Wild List	False Positive (誤検知テスト)	Diversity Test Rate
結果	100.00%	0.00%	99.90%

2020-12 (latest) on Windows 7 Professional, Windows 10 Professional

<https://www.virusbulletin.com/testing/results/latest/vb100-antimalware>

## ■ AV-Comparatives



テストの種類 ※2	Real-World Protection Test	Malware Protection Tests	Performance Tests
結果	97.60%	99.40%	Fast, Very Fast

Business Security Test 2020 (August – November)

<https://www.av-comparatives.org/vendors/acronis/>

※1 全プロダクトが共通で参加している評価機関は今のところありません。

※2 テストセットはそれぞれの評価機関が定めた内容になります。

※3 評価機関が定めた認定基準によります。認定基準はテスト機関ごとに異なります。

※4 レポート形式なっていませんが、公開されているmonthly Testでは10月以降v15を使用し、パスしています。

# アナリストの所感

- IDC Phil Goodwin

- [https://dl.acronis.com/u/rc/WP\\_IDC\\_Acronis\\_Cyber\\_Protect\\_and\\_Acronis\\_Cyber\\_Protect\\_Cloud\\_EN-US\\_200428.pdf](https://dl.acronis.com/u/rc/WP_IDC_Acronis_Cyber_Protect_and_Acronis_Cyber_Protect_Cloud_EN-US_200428.pdf)
- *We believe that Acronis Cyber Protect is among the most comprehensive attempts to provide data protection and cyber security to date....Acronis shows potential to disrupt traditional IT security vendors by delivering integrated components for backup/recovery and malware detection and protection.*



Phil Goodwin

Research Director – Cloud Data Management and Protection, IDC

セキュリティだけを提供するトラディショナルな  
ITセキュリティを変えるポテンシャル

# Acronisセキュリティ製品としてのポジション

 <p>Microsoft</p>	MVI member	 <p>VIRUSTOTAL member</p>	 <p>Cloud Security Alliance member</p>
 <p>AMTSO Anti-Malware Testing Standard Organization</p>	Anti-Malware Testing Standard Organization member	 <p>Anti-Phishing Working Group member</p>	 <p>MRG-Effitas participant and test winner</p>
 <p>Anti-Malware</p>	Anti-Malware Test Lab participant and test winner	 <p>ICSA Labs certified</p>	 <p>NioGuard Security Lab participant and test winner</p>
 <p>comparatives APPROVED Business Security JUL 2020</p>	AV-Comparatives approved business security product	 <p>Passed VIRUS 100</p>	 <p>AV-TEST participant and test winner</p>
		VB100 certified	

# Acronisが取得しているセキュリティ認定

## FIPS 140-2

Acronis AnyData Cryptographic Library has been [successfully verified by NIST](#)



## GDPR

Acronis is GDPR compliant through self-assessment as of May 25, 2018.



## GLBA (Gramm-Leach-Bliley Act)

GLBA is applicable to financial institutions, compliant to Title V, Subtitle A, Section 501.(b)



## HIPAA

An independent third party gap analysis, showing that Acronis is compliant with HIPAA rules



## ISO 27001

Acronis has Information Security Management System in accordance with standard ISO 27001:2013.



## ISO 9001

Compliant with ISO 9001:2015



## TAA

Acronis products are "TAA compliant" as manufactured or "substantially transformed" in Switzerland

## Privacy Shield

Acronis is EU-US and Swiss-US Privacy Shield certified

# 2021年10月 徳島の病院でランサムウェア被害

日本経済新聞 Pro

朝刊・夕刊  
LIVE  
Myニュース

トップ 速報 オピオン 経済 政治 ビジネス 金融 マーケット マネーのまなび テック 國際 スポーツ 社会・調査

## ランサム攻撃でカルテ暗号化 徳島の病院、インフラ打撃

事件・司法

2021年11月12日 11:30

保存 



サイバーアクセスで電子カルテによる診療が中断されている半田病院(2日、徳島県つるぎ町)=共同

引用：<https://www.nikkei.com/article/DGXZQOUE071OK0X01C21A1000000/>

## 時系列

- 院内の複数のプリンターから突如、英語で書かれた書類が大量に印刷される
- 英語で「あなたのデータは盗まれた。そして暗号化された」などと書かれ、記載されたウェブサイトへのアクセスを求められる
- 電子カルテのシステムに不具合が発生
- 患者8万5千人分のカルテ情報にアクセスできない
- ランサムウェアに感染したと判断し、警察に被害届を提出
- 電子カルテが使えなくなつたため救急患者と新規患者の受け入れを余儀なく停止
- ウイルスに感染したサーバー本体を専門のセキュリティー会社が修復を試みるが、復旧の見通しあたっていない
- 職員は毎日病院内のコンピュータ130台全てをウイルスがいないか何度もチェック
- 再発防止策については絶対安全と言い切れる方策が見当たらない
- LockBit(ロックビット)2.0\*に感染したものとみられている

大企業でなくても感染被害が  
身近なところに感染リスク

# Acronis Cyber Protectは 該当の最新ランサムウェアを以前より検知・防御

 Suspicious activity is detected Aug 16, 2021, 02:07 PM

On machine 'Thor', process 'C:\Users\Sif\AppData\Local\Temp\3582-490\lockbit22.exe' modified file 'C:\php\license.txt'. The process has been stopped, and the file changes have been reverted.

Device	Thor
Process	C:\Users\Sif\AppData\Local\Temp\3582-490\lockbit22.exe
Monitored because	Process certificate is not valid
Suspicious because	Binary format has been changed for several files.
Action	Revert using cache
Affected files	C:\php\license.txt C:\php\news.txt C:\php\readme-redist-bins.txt C:\php\snapshot.txt C:\Program Files\7-Zip\History.txt C:\Program Files\7-Zip\Lang\af.txt C:\php\extras\ssl\openssl.cnf
Support	Clear

# 「ランサムウェアからデータを守るには」 すなわち総合データ保護のアプローチ

侵入を防ぐ

感染を防ぐ

復旧できる環境を準備



- 常に最新のソフトウェアを使用
- IDaaSなどを使用した多要素認証
- ゼロトラスト

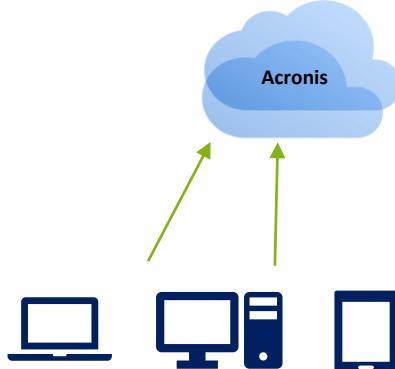
- 最新のエンドポイントセキュリティを使用
- 特権管理ソリューションによる権限管理
- 脆弱性を排除

- 定期的なバックアップを取得
- 確実に復元できるバックアップを準備

# 「皆様への 3つのお願い」 すなわち総合データ保護のアプローチ

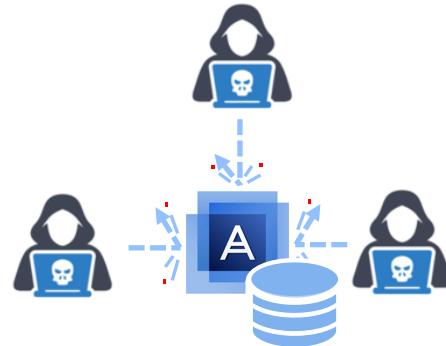
## 遠隔地バックアップ

感染端末と距離をとり有事の際にも復旧可能のように備える



## バックアップデータの保護

万が一サイバー攻撃を仕掛けられてもバックアップデータを保護し、  
**確実に復旧**できるように備える



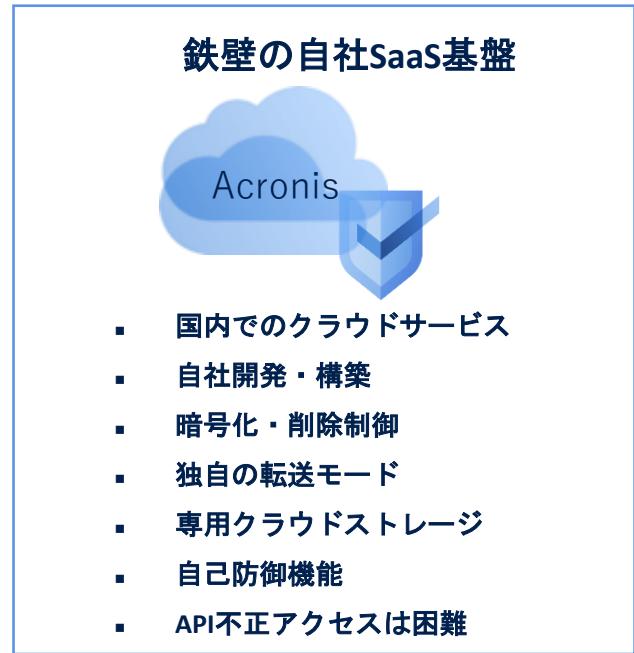
## 最新のエンドポイントセキュリティ

「感染しない」ために最新型の対策をとり、被害にあわないように備える。



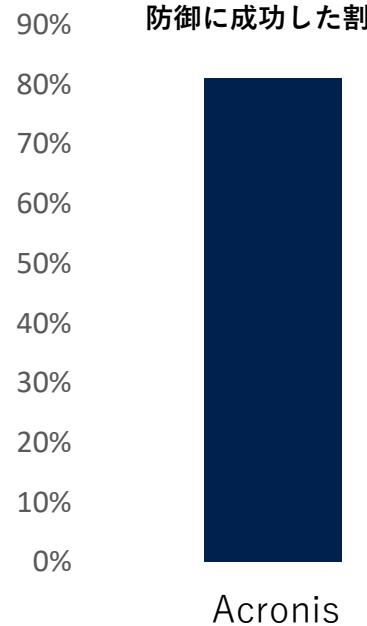
# Acronis独自のアプローチ

世界でも類を見ないデータ・システムを守る特殊なSaaS



# バックアップソフトを自身で守るAcronis 第3者機関によるソフトウェア攻撃

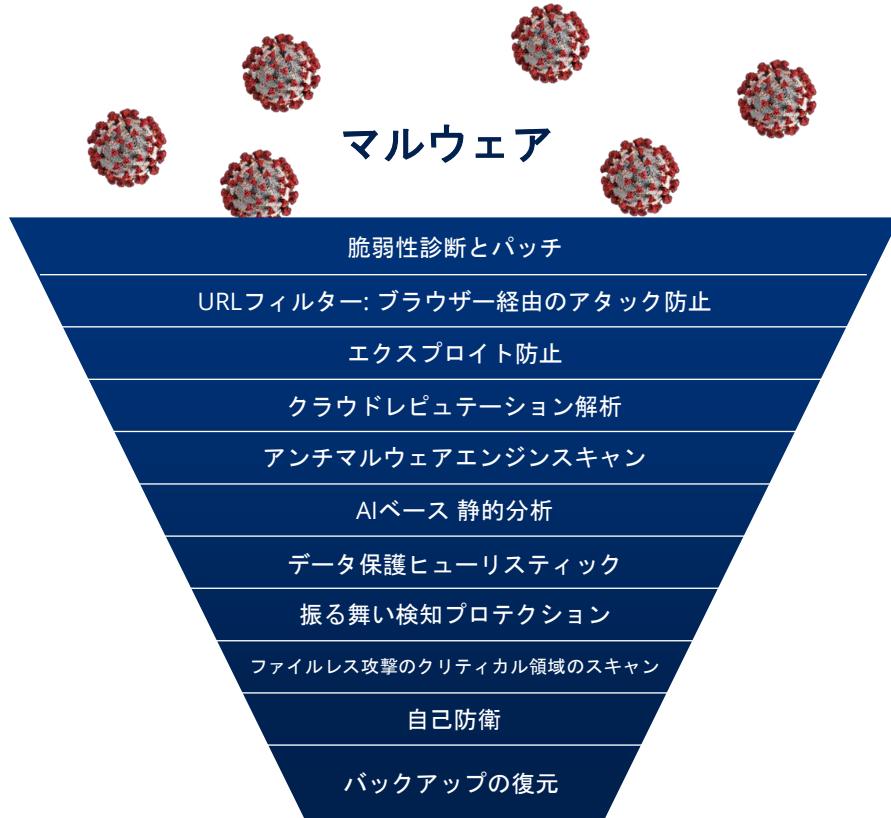
31項目の試験シナリオ



ファイルの保護	バックアップファイルの保護
	プログラムの保護
プロセス、サービスの保護	プロセス、サービスの停止
	コード注入
プロセス、サービスの保護	プロセスメモリの変更
	プロセスオブジェクトの変更
クラウドバックアップの保護	クラウドバックアップデータの変更
	DNSポイズニング

# Acronisが実現するエンドポイントの多層防御

- 企業イントラネットの外に出たデバイスを自立型で高度に多層防御
- あらゆるユーザに有効な要素を積み上げ一つのサービスとして提供
- 全てが干渉せずに共同でマルウェアを防御する
- ソフトウェア自身の安全性が担保されている
- 最後の砦となるバックアップ



# Acronisのデータ・システムセキュリティ

- AIベースのセキュリティ機能でゼロデイ攻撃も防ぎます

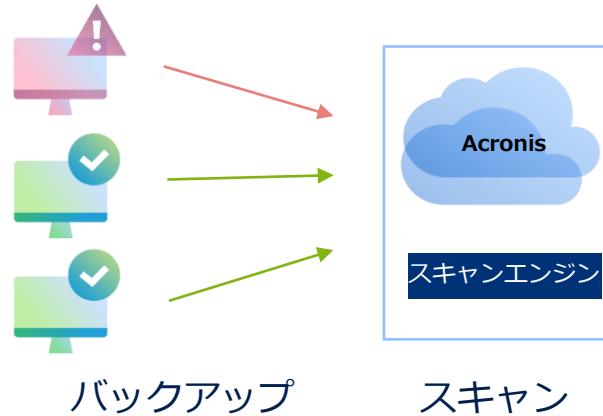
## フルスタックEPP

システムを常に安全な状態に

アンチランサムウェア
スタティックAIアナライザ
アンチマルウェアエンジン
ビヘイビアエンジン

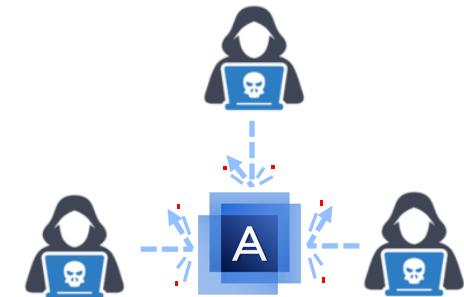
## バックアップスキャン

バックアップ内部の脅威をチェック



## 自己防御

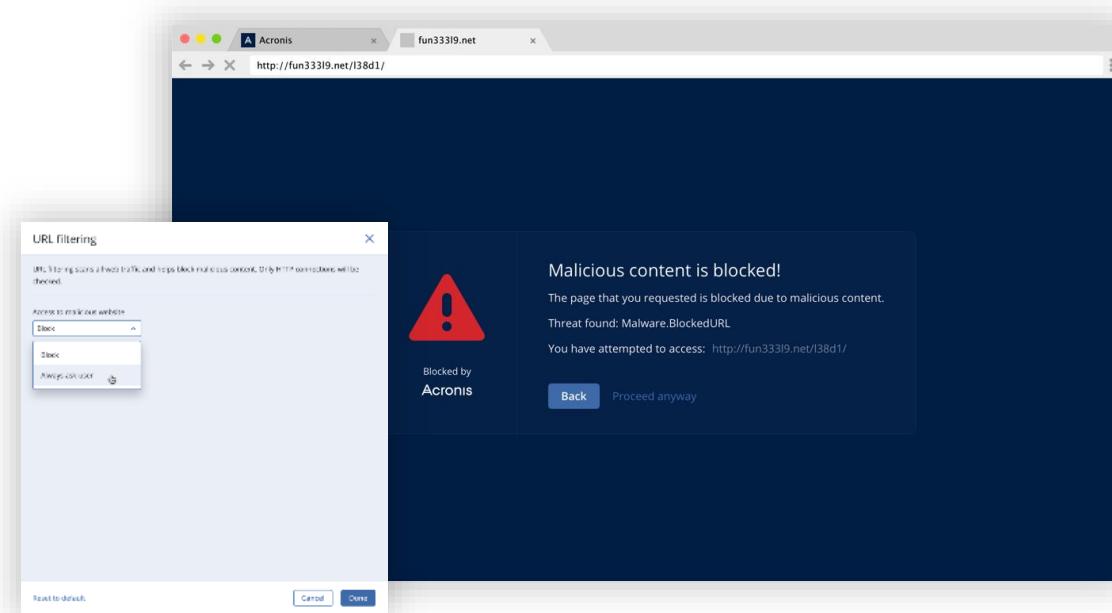
Acronisプロセス、アーカイブを  
マルウェアから守っています



# URLフィルタリングによる悪意のあるサイトへのアクセス制御

URLフィルタリングにより、Webサイトへのアクセス許可/拒否をリストベースで実施

- HTTP/HTTPS インターセプト
- URLのブラックリスト/ホワイトリスト
- 悪意のあるURLのペイロード分析



---

悪意のある/ハッキングされたWebサイトによる攻撃を防ぎ、コンプライアンスを維持

# 情報漏えい対策(Data Loss Prevention機能)

コピー&ペーストや周辺デバイスの制御により、情報の入出力を制御します。

## 1. デバイスやクリップボードを制御

- ・ [デバイス]  
リムーバブルメディア、プリンター、クリップボード、モバイルデバイス、Bluetooth、光学ドライブ、フロッピーディスク
- ・ [ポート]  
USB、FireWire
- ・ [リダイレクトされたデバイス]  
マッピングされたドライブ、クリップボード受信/送信、USBポート

## 2. 通知とアラート

- ・ 「許可」以外のデバイスにアクセスがあると、アラートを発生可能
- ・ ユーザへの通知も可能

## 3. サポートOS

1. Microsoft Windows 7 Service Pack1以降
2. Microsoft Windows Server 2008R2以降

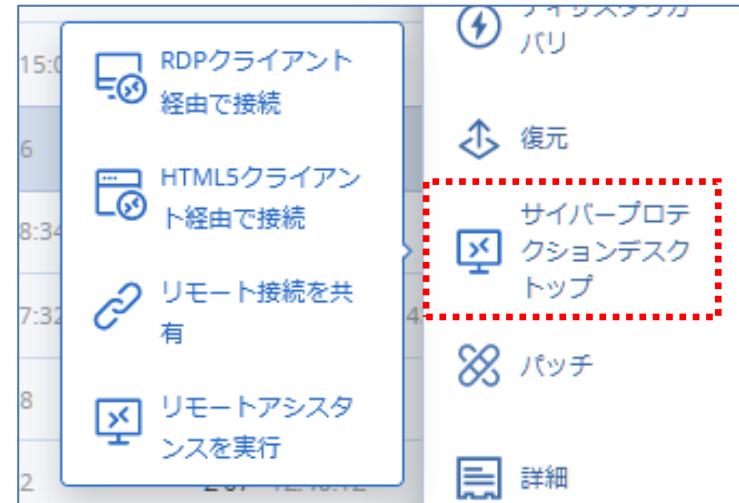
デバイス	アクセス	アラートを送信
リムーバブル	読み取り専用	<input type="checkbox"/>
プリンター	許可済み	<input type="checkbox"/>
クリップボード	許可済み	<input type="checkbox"/>
モバイルデバイス	拒否済み	<input checked="" type="checkbox"/>
Bluetooth	許可済み	<input type="checkbox"/>
光学ドライブ	読み取り専用	<input checked="" type="checkbox"/>
フロッピードライブ	読み取り専用	<input checked="" type="checkbox"/>

# 資產管理

# リモート接続機能: サイバー・プロテクション・デスクトップ

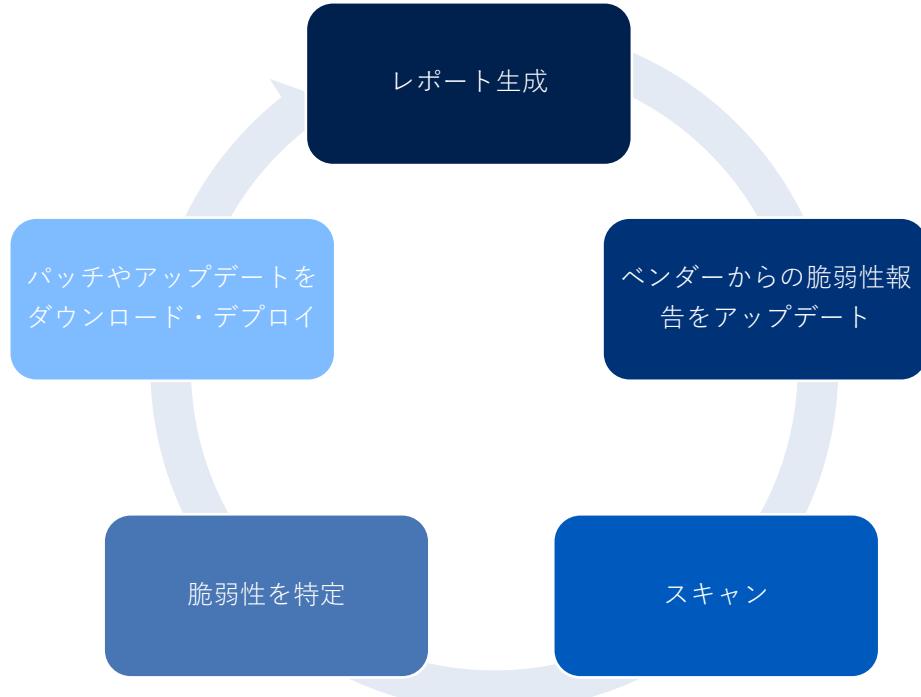
## Windowsクライアントを遠隔で操作

- リモートユーザーを支援して膨大な時間を節約
- ファイアウォールの設定変更や追加のVPNトンネル確立は不要で、プライベートネットワーク内のシステムにアクセス（外向けの443番ポートで通信）
- RDPのほか、HTML5をサポート
- リモート接続共有機能  
任意のユーザが対象マシンにリモートでアクセスするためのリンクを生成して共有します。
- リモートアシスタンス(操作画面共有)機能



# 脆弱性診断とパッチ管理

1. 脆弱性スキャン
2. 重大度に応じた脆弱性の優先順位付け
3. ソフトウェアのリリースやアップデートに沿ったパッチ適用サイクル
4. 脆弱性が見つかった場合、対応と修復を実施（パッチやアップデートをインストール）



脅威のリスクを低減し、自動プロテクションにより攻撃を防御

# ソフトウェアインベントリ

## クライアントにインストールされているソフトウェアの一覧を表示

### ◆クライアントデバイス別の表示

- ✓ バージョン
- ✓ ステータス
- ✓ ベンダー
- ✓ インストールされた日付(実装中)
- ✓ 前回の実行(実装中)
- ✓ ロケーション(実装中)
- ✓ システムの種類
- ✓ ユーザ

Software Inventory

名前	バージョン	ベンダー	システムの種類	ユーザー
秀丸エディタ	8.91	有限会社サイト一企画	X86	System
Zoom	5.0	Zoom Video Communi	X86	System
Wireshark	3.2.7	The Wireshark develop	X86	System
VMware vSphere Client	6.0.0.5505	VMware, Inc.	X86	System
VMware Client Integration Plug-in	6.0.0.4222	VMware, Inc.	X86	System
TAP-Windows	9.24.2	OpenVSwitch	X86	System
OpenVPN	2.4.9-i601-Win10	OpenVPN	X86	System
Office 16 Click-to-Run Localization Component	16.0.13530.20440	Microsoft	X86	System

前回のスキャン: 2021年2月3日 01:14

デバイス名  
選択

アプリケーション  
選択

ベンダー  
選択

ステータス  
選択

インストールされた日付  
Select

スキャン日  
Select

キャンセル

適用

### ◆特定のアプリケーションがインストールされているデバイス

- ✓ フィルタや検索(デバイス/アプリケーション)が可能

# ドライブヘルスマニタリング

## 問題が発生する前に予測

- ◆ 機械学習、S.M.A.R.T.レポート、ドライブ容量、ドライブベンダーなどを組み合わせて HDD、SSD の障害を予測
- ◆ 機械学習モデル
  - ✓ すべての障害の80%以上を予測可能
  - ✓ 98.5%の予測確度（継続的に向上）
- ◆ アラート発生後に重要なファイルをバックアップするなどの迅速な対応が可能

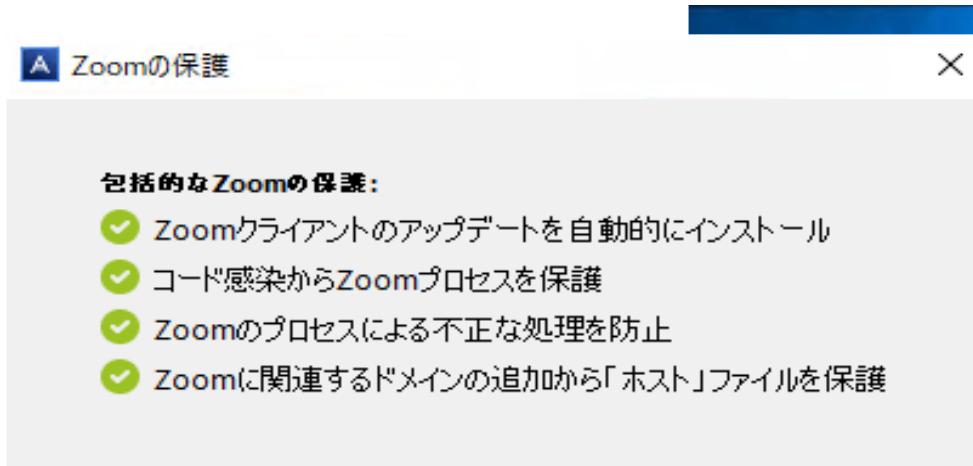


**利点** 予測不能なデータ損失を防ぎ、プロアクティブにアップタイムを改善

# リモートワークツール対応

## Zoom、WebEx、Microsoft Teamsの保護

1. Acronisの自己防御技術によるインジェクション防止やhostsファイル保護など
2. 脆弱性診断とパッチ管理
3. Acronis Cyber Protectionモニターで保護状態を確認



リモート会議ツールを保護し、安全に業務を行う

貴社主力業務への集中、  
生産性向上

# 2030問題 -IT人材不足-

- IT人材 :

2030年には約50万から80万人の  
IT人材が不足する。 (経産省/みずほ情報総研2019)

- 日本のセキュリティ人材

2019年で19万人不足の状態。 (経産省2016)

生産性上昇率 (年率)	IT 需要の伸び		
	低位 : 1% (経済成長準拠)	中位 : 2~5% (低位と高位の中間)	高位 : 3~9% (IPA 企業アンケート)
0.7%	16.4 万人	44.9 万人	78.7 万人
2.4%	△7.2 万人	16.1 万人	43.8 万人
需給ギャップゼロ	1.84%	3.54%	5.23%

無印 : 需要数 > 供給数、△ : 供給数 > 需要数

(出所) 試算結果をもとにみずほ情報総研作成

IT人材需給に関する調査  
(みずほ情報総研2019)



# 2030問題 -IT人材不足-

- ・ 2030年には約50から80万人のIT人材が不足する。 (みずほ情報総研2019)
- ・ 既存システムの運用保守に割かれている人材

(経産省2018)

## • 一つのアプローチ

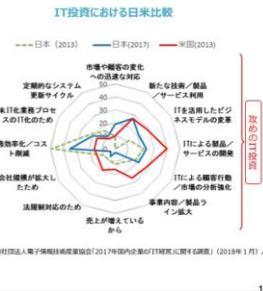
- セキュリティ対策を強固にしつつ生産性を高める  
すなわち、既存システムにおいて、  
マルチベンダーなデータ保護を集約



## すなわち、Acronis Cyber Protect

## 2.2.5 既存システムの運用・保守に割かれてしまう資金・人材（1／2）

- 我が国企業のIT関連費用の80%は現行ビジネスの維持・運営（ラン・ザ・ビジネス）に割り当てられている。
- この結果、戦略的なIT投資に資金・人材を振り向けていない。



## DXレポート (経産省2018)

## 集中の阻害要因： マルチベンダーでのセキュリティ対策

- バックアップとセキュリティアプリは相性が悪い
- マルチベンダーではチューニングが必要
- 多様なサイバー攻撃への対策として、複数のアプリ、アプライアンス、エージェント、管理サーバーの導入する、、、

**These 5 Vectors  
of Cyber Protection**  
are all critical, but they often  
work against each other



# 集中の阻害要因： マルチベンダーでのセキュリティ対策

- マルチベンダー環境の  
バックアップとセキュリティアプリは相性が悪い
- マルチベンダーではチューニングが必要
- 多様なサイバー攻撃への対策として、  
複数のアプリ、アライアンス、エージェント、  
管理サーバの導入すると、、、、、、

## ⇒管理煩雑、競合の調整

- ⇒複数ある対策アプリ自身の脆弱性リスク
- ⇒コンピュータの不安定化、誤検知
- ⇒ITサポートサービス企業の負荷増大

## These 5 Vectors

Safety, Accessibility, Privacy, Authenticity, Security

## of Cyber Protection

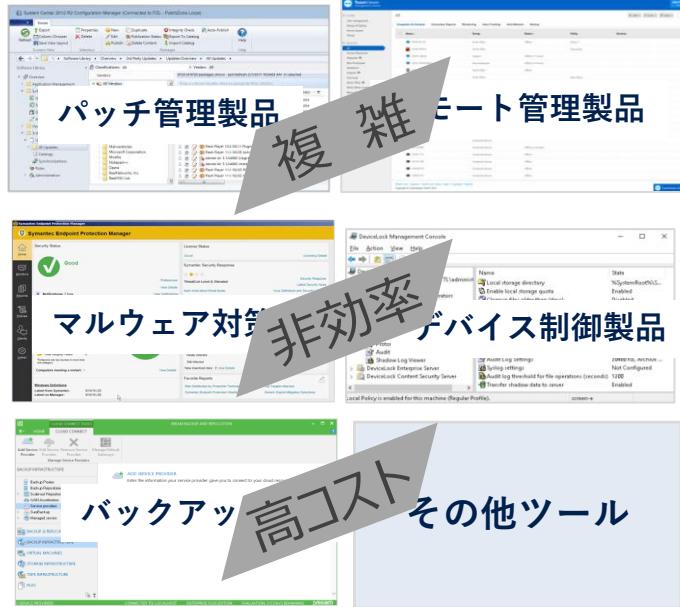
are all critical, but they often  
work against each other



# プラットフォームサービスの統合：管理

## 従来型

複数のツールを併用してエンドポイントを管理



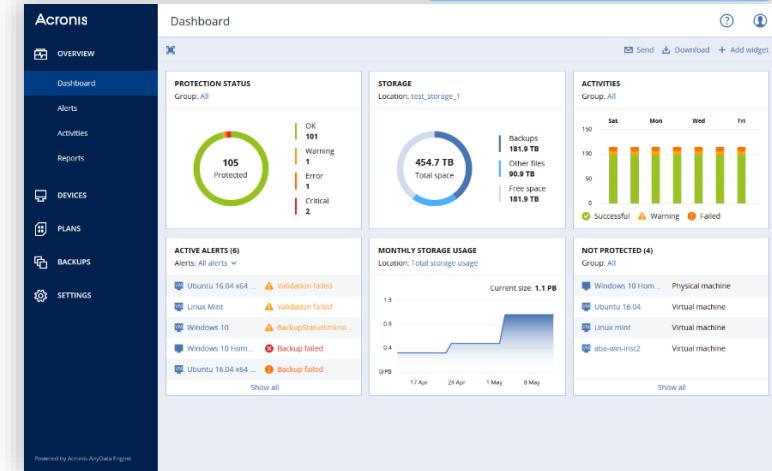
VS

## 次世代型

ブラウザでのログインから、エンドポイントを一元管理

一元管理  
直感的

統一感  
操作性



# プラットフォームサービスの統合:機能実装

バックアップ、DR、セキュリティ、資産管理を一つのエージェントに統合

従来型



VS

次世代型



# 一つの管理コンソール：「技術習得面」からの生産性向上

1つの管理コンソールで様々なサービスを管理 = サポート環境の理想形

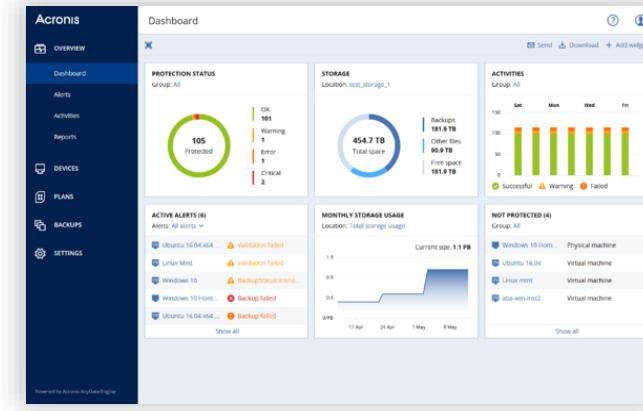
⇒様々な機能の習得に向けて、異なるマルチベンダーでトレーニングを受けるオーバヘッドの排除



## 1つのエージェント

各種機能を提供

マルチエージェントの競合、調整からの解放



## 1つの管理コンソール

複数の機能・顧客を一元管理、管理サーバ不要

複数の管理サーバ・ソフトからの解放

# Acronis Cyber Foundation

知識に富む未来を築くアクロニスサイバー基金

知識を創造し、広げ、保護する  
活動へのご支援をお願いします。

- ・新たな学校の建設
- ・教育プログラムの提供
- ・書籍の出版

[www.acronis.org](http://www.acronis.org)

#CyberFit

