クラウドバックアップ&セキュリティ

株式会社 成文社
https://seibnsha.com
北秋田店 〒018-3331 北秋田市鷹巣字上家下24
大館支店 〒017-0055 大館市字沼館道上102
TEL 0186-62-1231 FAX 0186-63-0092

クラウドバックアップ&セキュリティ

ランサムウェア・BCP対策に クラウドバックアップ

ランサムウエアとは…PCのデータを暗号化し、復元するために代金を要求するマルウエアです。PC内のデータを暗号化します。つまり、使用者はPC内のデータが使えなくなります。暗号化されたデータを戻すためには復元するためのキー（鍵）が必要です。
攻撃者は、キーが欲しければ金をよこせ！と脅してくる訳です。つまりPC内のデータを人質に取り、身代金を要求します。ランサムウエアの「WannaCry」に感染すると、同一ネットワーク機器に感染が広がるため、被害が大きくなります。

BCP（事業継続計画）…企業が自然災害、大火災、テロ攻撃などの緊急事態に遭遇した場合において、事業資産の損害を最小限にとどめつつ、中核となる事業の継続あるいは早期復旧を可能とするために、平常時に行うべき活動や緊急時における事業継続のための方法、手段などを取り決めておく計画のことです。
緊急事態は突然発生します。

クラウドバックアップのご紹介

現在世界で500万人以上の個人ユーザーと、世界のトップ企業100社のうち79社を含む50万社以上の企業に信頼されているアクロニス社のテクノロジーを採用。

イメージバックアップで国内シェアNO1を誇るサービスです。

クラウドバックアップ&セキュリティ Acronis との関係性

アクロニス
CRO　セルゲイ・ベロウゾフ

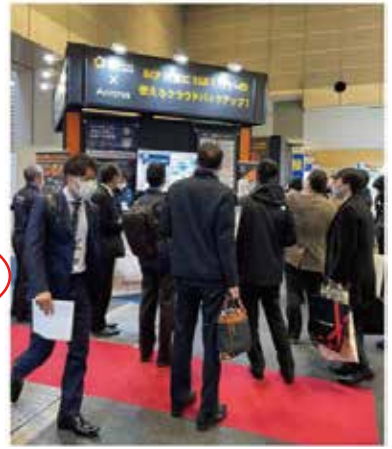
Acronis Cloudデータセンター

アクロニスは、クラウドデータセンターのグローバルネットワークを活かしてさまざまなデータ保護サービスとソリューションを提供しています。Acronisデータセンターは、最高レベルの安全とセキュリティ基準を遵守し、高い信頼性を実現しました。

Acronis　https://www.acronis.com/

クラウドバックアップ&セキュリティ

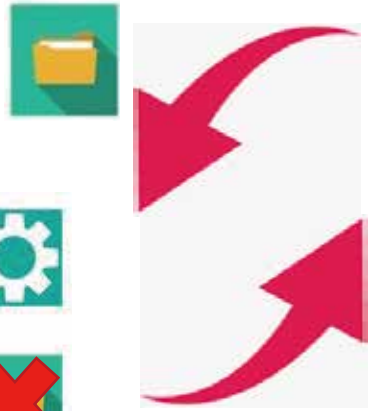
	データセンターのサービスレベル
ティア1	・地震や火災など災害に対して、一般建物レベルの安全性が確保されている。 ・瞬間的な停電に対してコンピューティングサービスを継続して提供できる設備がある。 ・サーバ室へのアクセス管理が実施されている。 ・想定するエンドユーザの稼働信頼性：99.67%以上
ティア2	・地震や火災など災害に対して、一般建物レベルの安全性が確保されている。 ・長時間の停電に対してもコンピューティングサービスを継続して提供できる設備がある。 ・サーバ室へのアクセス管理が実施されている。 ・想定するエンドユーザの稼働信頼性：99.74%以上
ティア3	・地震や火災など災害に対して、一般建物より高いレベルでの安全性が確保されている。 ・機器のメンテナンスなど一部設備の一時停止時においても、コンピューティングサービスを継続して提供できる冗長構成の設備がある。 ・建物およびサーバ室へのアクセス管理が実施されている。 ・想定するエンドユーザの稼働信頼性：99.98%以上
ティア4	・地震や火災など災害に対してデータ保全の安全性を確保、かつ可用性も確保した非常に高いレベルでの耐災害性が確保されている。 ・機器の故障やメンテナンスなど一部設備の一時停止時において、同時に一部機器に障害が発生してもコンピューティングサービスを継続して提供できる、より高いレベルの冗長構成の設備がある。 ・敷地、建物、サーバ室およびラック内のIT機器へのアクセス管理が実施されている。



長野DCは日本データセンター協会認定
（ティア3：富士通・NTTコミュニケーション等）

イメージバックアップとは

ファイル一つからでも復元可能！



株式会社成文社

クラウド上に、今と同じ状態のPCを
1台預けていると想像してください

システムもしくはディスクまるごとのイメージの
スナップショットをバックアップする

データファイルだけでなく**OS・アプリ**や**個人設定**までも
まるまるバックアップ!!

クラウドバックアップ&セキュリティ

バックアップの必要性《データ消失について》

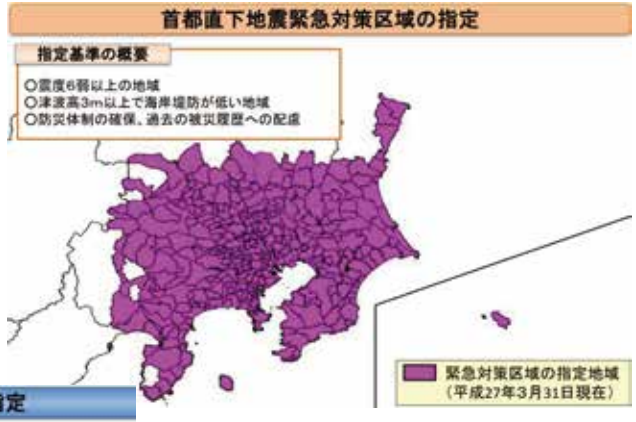
データ消失は誰も予想できない！

- 火災
- 落雷
- 盗難や破損・破壊
- **地震**
  南海トラフM8～9
  首都圏直下型 M7.3
- **大雨による災害**

降水量　世界2位
世界平均の2倍

全ての災害は身近なものとなっている

今後予想される大規模地震【内閣府発表】



熊本地震(M6.5)は
発生確率1%未満だった

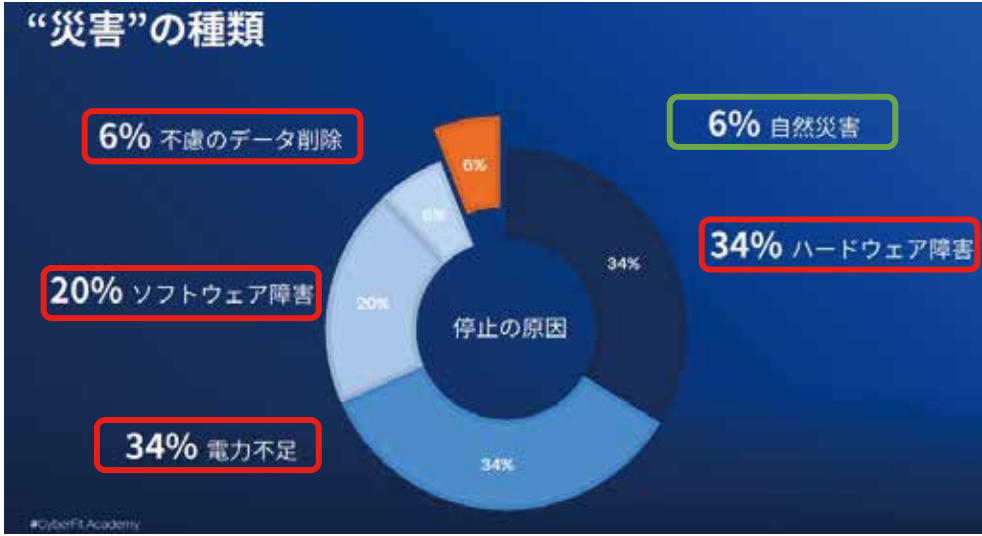
世界で起こる震度6以上の地震の
20%以上が日本で起こっている!!

企業における“災害”リスクとは

企業における**“災害”リスク**とは
自然災害だけではありません。

実は、**自然災害**はリスク全体の**6%**

新規のハードウェアが**1年で5%~10%**、
5年で25~40%が**故障**すると言われてます。

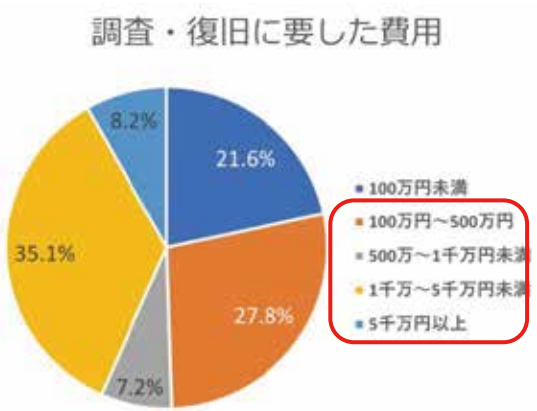


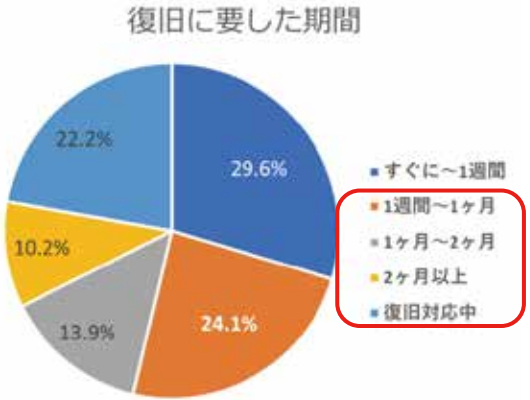
常に最新化されたクラウドバックアップなら、
顧客の**コスト改善**だけでなく**リスクを軽減**することが**可能**です。

ウィルスの脅威は中小企業を狙っている

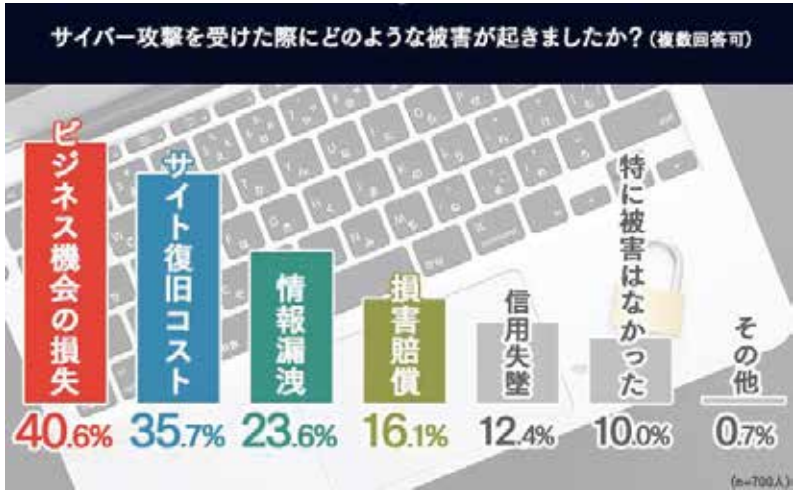
順位	組織	昨年順位
1位	ランサムウェアによる被害	1位
2位	標的型攻撃による機密情報の窃取	2位
3位	サプライチェーンの弱点を悪用した攻撃	4位
4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
5位	内部不正による情報漏えい	6位
6位	脆弱性対策情報の公開に伴う悪用増加	10位
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
8位	ビジネスメール詐欺による金銭被害	5位
9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	不注意による情報漏えい等の被害	9位

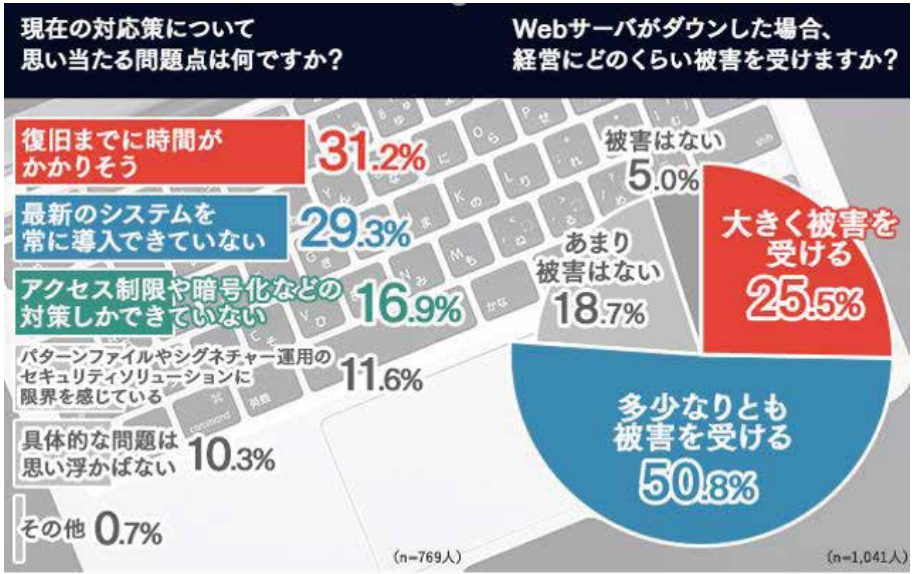
情報処理推進機構(IPA)
『情報セキュリティ10大脅威2022』





≪2021≫最新のバックアップについてのデータ Vol.1





- **機会損失**：復旧までの時間×販管費×人数
- **復旧コスト**：平均50万～300万以上
  《データ復旧・DM・残業代・原因究明・システム導入》
- **情報漏洩**＝**損害賠償**＝信用失墜【取引停止】

中小企業の75%以上が実際に感じている課題(問題点)

社内データ全て消えた場合2年以内に

※テキサス州立大学調査レポートより

94%が倒産

- 創業40年の資格者30名在籍の都内の士業法人の例
- データのバックアップは社内のサーバーにすべて集約。
- 2018年頭にランサムウェア（ワイヤー型）に感染。ネットワークを介してバックアップを含めたすべてのデータを破壊される。

黒字倒産

データ消失は企業存続に影響する！

企業が求めるバックアップの3-2-1ルールとは

（ランサムウェア・BCP対策）

旧来のバックアップ認識
2つのデータコピー
＋
1つの異なるストレージメディア

クラウドバックアップ
（遠隔地バックアップ）

マルウェアスキャン
Active Protection
AES256暗号化
パッチ管理
世代管理

外付けHDD（ローカル）　自社サーバ（ローカル）

ローカルではランサムウェア・BCP対策には
不十分!!

3つ以上のデータコピー

2つ以上の異なるストレージメディアの使用

1つ以上のオフサイト保存
（遠隔地クラウドバックアップで単一障害ポイントを排除）
※事業継続の為のDR機能もご用意

クラウドバックアップ&セキュリティ

クラウドバックアップについて《セキュリティ・システム》

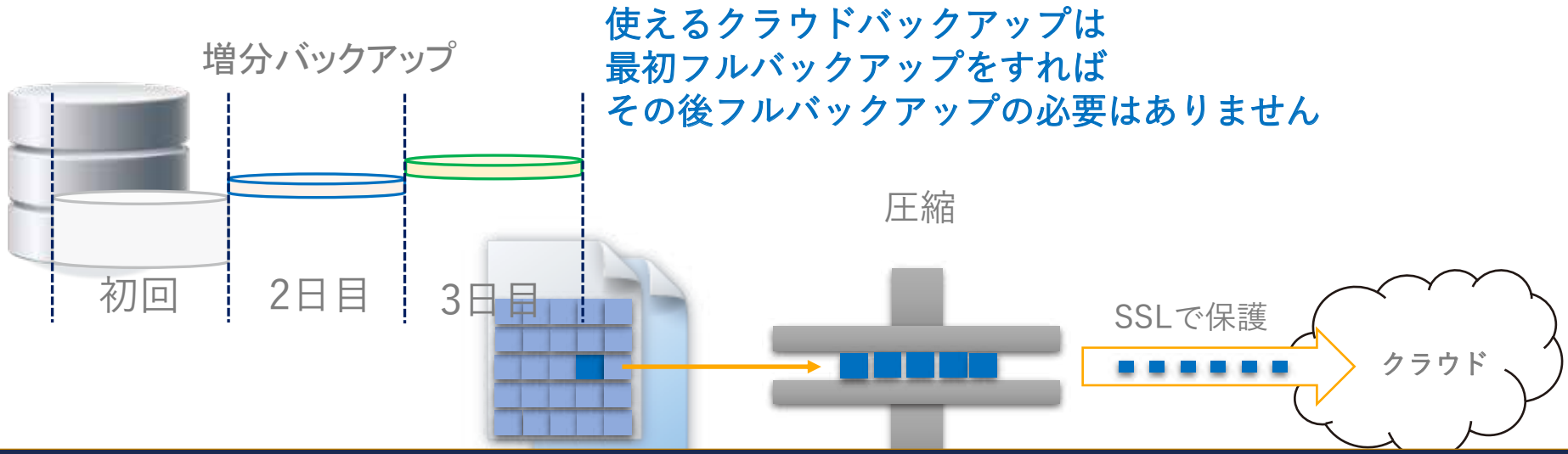
クラウドバックアップセキュリティ

- 米軍採用の世界最高レベルの暗号方式**AES-256**でファイルがアップロードされる前に暗号化
- すべてのファイル転送も**AES-256**で保護され、**SSL通信**にて転送
- DC側でもセキュアに**AES-256**で暗号化された状態で保管
- データの安全な処理・転送・保管に関するあらゆる法律および規制に準拠

（医療データのバックアップ対応：3省2ガイドラインに対応）

データ転送の最適化

- 初回以降は増分のみをバックアップ
- 変更のあったブロックを検出してのバックアップ



ファイルバックアップ　VS　イメージバックアップ

ファイル数が増加するとバックアップ速度が著しく劣化する

ファイル単位のコピー

ファイル数に依存しない高速なバックアップ

ブロック単位のコピー

- イメージバックアップは実際に利用しているブロックのみを高速に転送可能

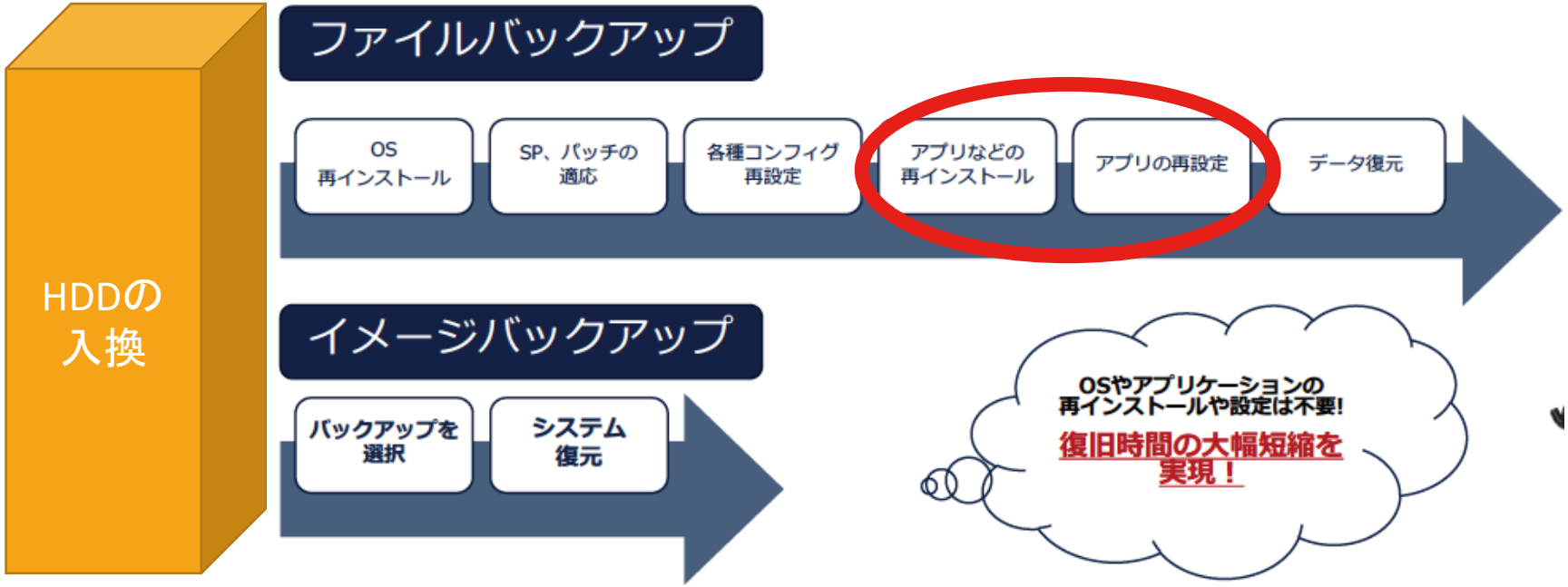
・100万ファイルを配置
Acronis Backup11.5（ブロック）Robocopy（ファイル）で時間を比較

ツール	所要時間
Acronis Backup11.5	1:20
Robocopy	14:20

イメージバックアップが圧倒的に高速！

※Acronis Japan検証環境での計測結果
※コピー先：Windows2012（4 CPU,4GB Mem仮想サーバ）
※コピー元：Windows2012（物理サーバ）

イメージバックアップは復元も圧倒的に高速



クラウドバックアップ&セキュリティ

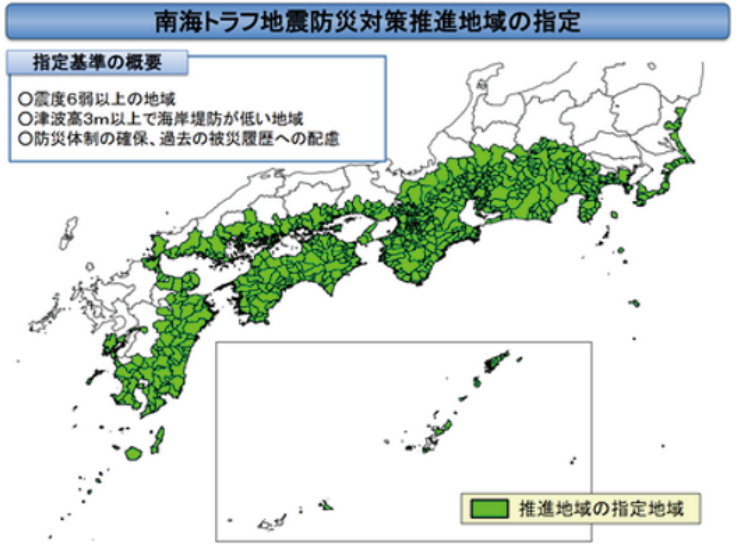
クラウドバックアップDRオプション

台風21号による大型停電

- 関電管内で　２１９万戸
- 発生から５日後　3万1千戸

南海トラフ地震の際の停電

内閣府の予想では　2710万戸



停電、停電って何を言いたいか？

会社のサーバーの

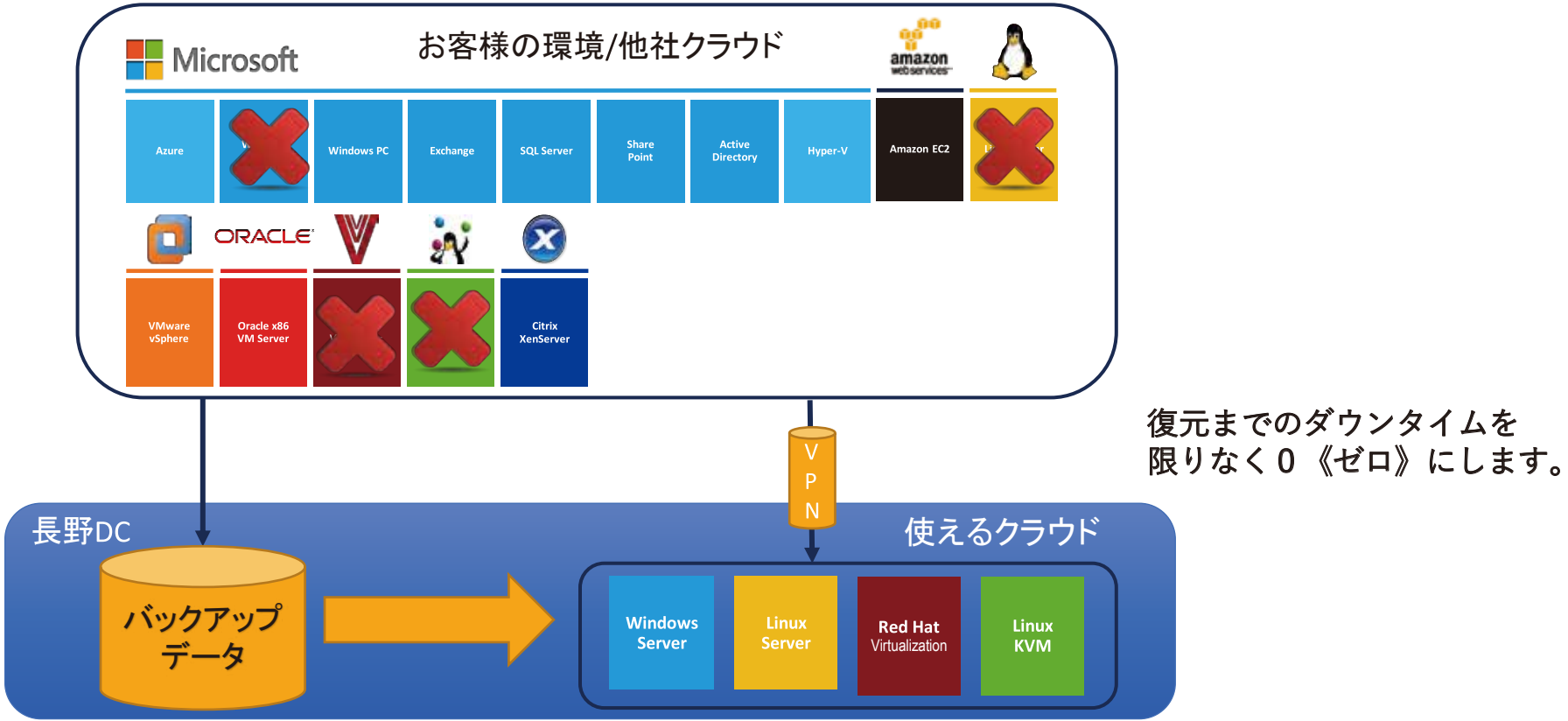
電源が入れられない!!

あらゆるシステムに対応したDR《ディザスタリカバリ》

物理マシンと仮想マシン	▪ Windows	▪ Linux
仮想プラットフォーム	▪ VMware vSphere ▪ Microsoft Hyper-V ▪ Linux KVM	▪ Red Hat Virtualization ▪ Citrix XenServer
アプリケーション認識型バックアップおよびリカバリ	▪ Microsoft Exchange ▪ Microsoft SQL Server	▪ Microsoft SharePoint ▪ Microsoft Active Directory
アプリケーションレベルのレプリケーションをリアルタイムで実現するクラウドサーバー	▪ SQL Server AlwaysOnのようにレプリケーション機能を標準搭載しているアプリケーション向け	

25以上のワークロードを保護、バックアップ業界における最先端のランサムウェア対策テクノロジーを搭載し、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します。**

DR《ディザスタリカバリ》イメージ



復元までのダウンタイムを
限りなく０《ゼロ》にします。

東京本社のサーバーが停電でアクセス不可でも
長野に取ってあるバックアップサーバーで大阪支社の事業継続可能

クラウドバックアップ&セキュリティ

ファイルデータだけでは不完全

クラウドバックアップが守るものは

ファイルデータではなく
現在のお客様の仕事環境!!

災害にあおうと、ランサムウェアの攻撃を受けようと
いつでも最後にバックアップを取った時点の
お客様の仕事環境に戻れます！

クラウドバックアップ&セキュリティ × Acronis を使用したクラウドバックアップなら

- 指定した時間に自動でバックアップ
- バックアップ完了後には自動でレポートメール配信
- システムイメージで取得するので全体を復元できる

クラウドバックアップ&セキュリティ

クラウドバックアップ
その他機能《標準機能》

クラウドバックアップ機能《標準機能：オプション》

機能		クラウドバックアップ
		標準機能 / アドバンスパック
バックアップ	ワークステーション、サーバーのバックアップ（Windows、Linux、Mac）	標準機能
	仮想マシンのバックアップ	標準機能
	ファイル単位のバックアップ	標準機能
	イメージバックアップ	標準機能
	アプリケーションバックアップ：Microsoft 365、G Suite、Microsoft Exchange、 Microsoft SQL、Microsoft SharePoint	標準機能
	Microsoft SQL ServerとMicrosoft Exchangeのクラスター環境のサポート	アドバンスバックアップ
	Oracle DB	アドバンスバックアップ
	SAP HANA	アドバンスバックアップ
	ネットワーク共有のバックアップ	標準機能
	ローカルストレージへのバックアップ	標準機能
	クラウドストレージへのバックアップ	標準機能
	Continuous Data Protection（CDP）：継続的データ保護	アドバンスバックアップ
	データ保護マップ（ファイルの種類別の保護状況の確認）	アドバンスバックアップ
セキュリティ	脆弱性診断	標準機能
	ランサムウェア対策機能 Acronis Active Protection	標準機能
	アンチウイルス＆アンチマルウェア、エクスプロイト防止、URLフィルタリング	標準機能
	フォレンジックモードバックアップ	アドバンスセキュリティ
	バックアップデータのマルウェアスキャン	アドバンスセキュリティ
	セーフリカバリ	アドバンスセキュリティ
	ホワイトリスト	アドバンスセキュリティ
サイバープロテクション管理	デバイスのグループ管理	標準機能
	集中管理	標準機能
	パッチ管理	アドバンスマネージメント
	ダッシュボードとレポート	標準機能
	HDDやSSDのヘルスチェック（故障予測）	アドバンスマネージメント
	リモートデスクトップ＆リモートアシスタンス	標準機能
	ハードウェアのインベントリ	標準機能
	ソフトウェアのインベントリ	アドバンスマネージメント

一つの計画ですべてを保護します

今まで**複数のツール**で管理されていた**バックアップから**
セキュリティまでを管理画面から**すべて管理**できます。

- バックアップ
- マルウェア対策
- URLフィルタリング
- 脆弱性評価
- パッチ管理
- Windows Defender AntivirusとMicrosoft Security Essentialsの管理

マルウェア対策

標準機能

主な機能

- マルウェアからのリアルタイム保護
- 暗号化プロセスの検出
- ランサムウェア検出
- オンデマンドスキャン
- 自己保護
- ネットワークフォルダの保護
- サーバーサイドの保護
- ファイル検疫

WindowsとMacOSのための
完全なアンチマルウェア保護

URLフィルタリングによる悪質なURLへのアクセス制御

標準機能

主な機能

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

悪意のある/ハッキングされたウェブサイトによる攻撃を防止します

デバイスアクセス制御機能

標準機能

PCに接続されるデバイスの認識制御が可能に

クラウドバックアップ&セキュリティ

クラウドバックアップ
その他機能《オプション機能》

ウイルス対策の重要なポイント
パッチ管理とは

アドバンスマネージメント

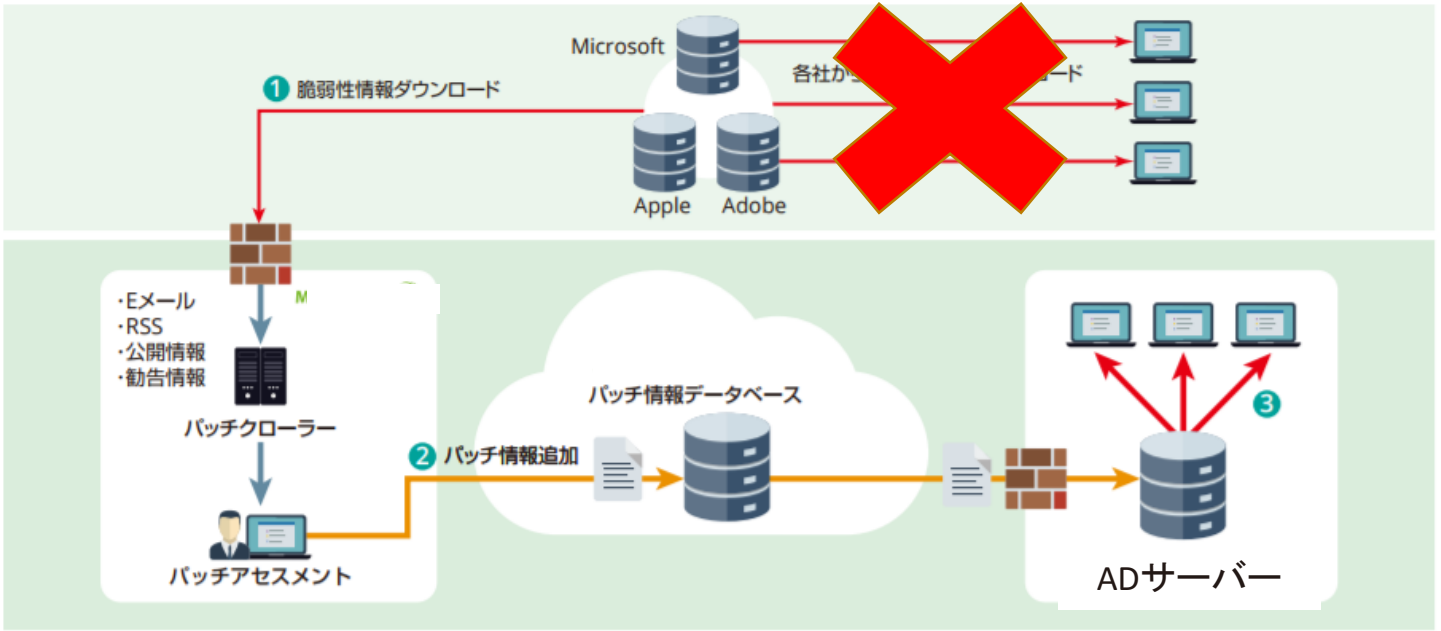
- ソフトやOS等の修正プログラムを言い、衣類の穴を塞ぐための「布当て」が言葉の由来とされてます。文字通り「機能の穴」を「塞ぐ」ために当てられるものとして、各サービスの提供企業から逐一配信されておりその数は1週間に数百と言われております。

- 万が一ウイルスがUTMなどをすり抜けてきても、日頃からパッチ管理をすることで企業において重要なセキュリティ上のリスクを事前に回避することができます。

- 実態として中小企業では**パッチ管理ができていなところがほぼ！**

一般的なパッチ管理の構図

アドバンスマネージメント



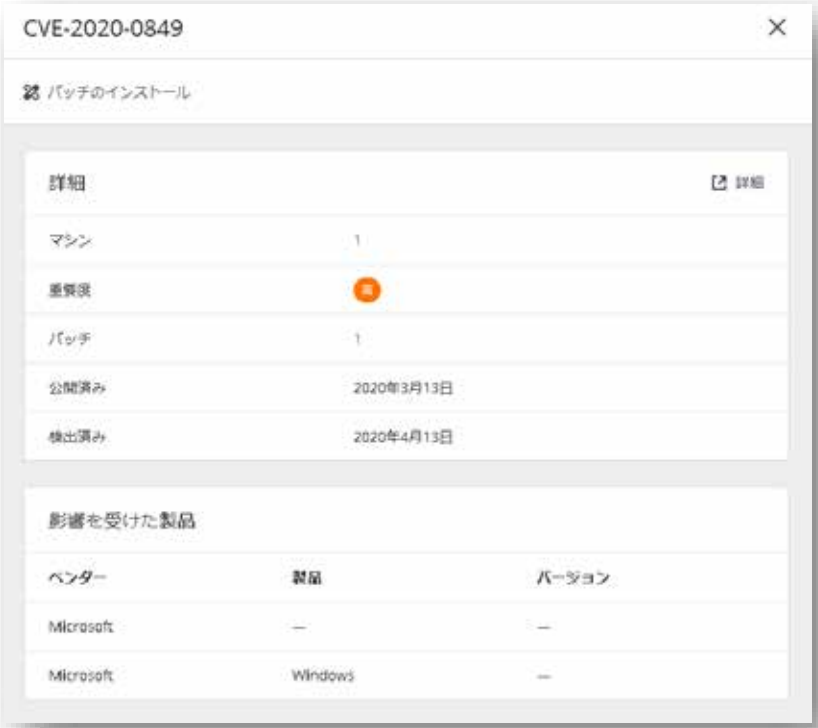
この形だとADサーバー配下のネットワーク上にPCが無いと管理ができず、
テレワーク等で社外にノートPCなどを持ち出した場合管理ができない。

サポート対象

アドバンスマネージメント

問題が発生する前にパッチを速やかに適用することができます

下記をサポートします
ワークステーション - Windows 7 以降
サーバー - Windows Server 2008R2以降
Microsoft Office（2010年以上）と関連コンポーネント
.NET Framework,
Adobe,Oracle, Java, ブラウザーなどのソフト



パッチ管理

アドバンスマネージメント

問題が発生する前に修正。毎週250-300件が報告されるCVEデータベース

- パッチの自動承認
- 展開のスケジュール
- 手動展開 • 再起動の設定、メンテナンスウィンドウのオプション
- ステージング展開
- MSオフィス、Windowsアプリを含めたアップデート • 2020年2月時点で27個のアプリ、1,437バージョン

保護の自動化、潜在的な脅威の軽減、攻撃の防止（WannaCryなど）に役立ちます

ディスク監視

アドバンスマネージメント

機械学習、S.M.A.R.T.レポート、ドライブサイズ、ドライブベンダーなどを組み合わせてHDD/SSDの故障を予測します。
機械学習モデルは98.5%の予測精度を実現しています。
ドライブアラートが表示されたら、障害が発生したドライブから重要なファイルをバックアップするなどの対策を取ることができます。

問題が起こる前にディスクの問題を知ることができます

クラウドでのバックアップのマルウェアスキャン

ディスクのフル バックアップをスキャンすることで、潜在的な脆弱性やマルウェア感染を発見し、マルウェアのないバックアップを確実に復元することができます。

感染したファイルのバックアップからの復元を防止

セーフリカバリー機能

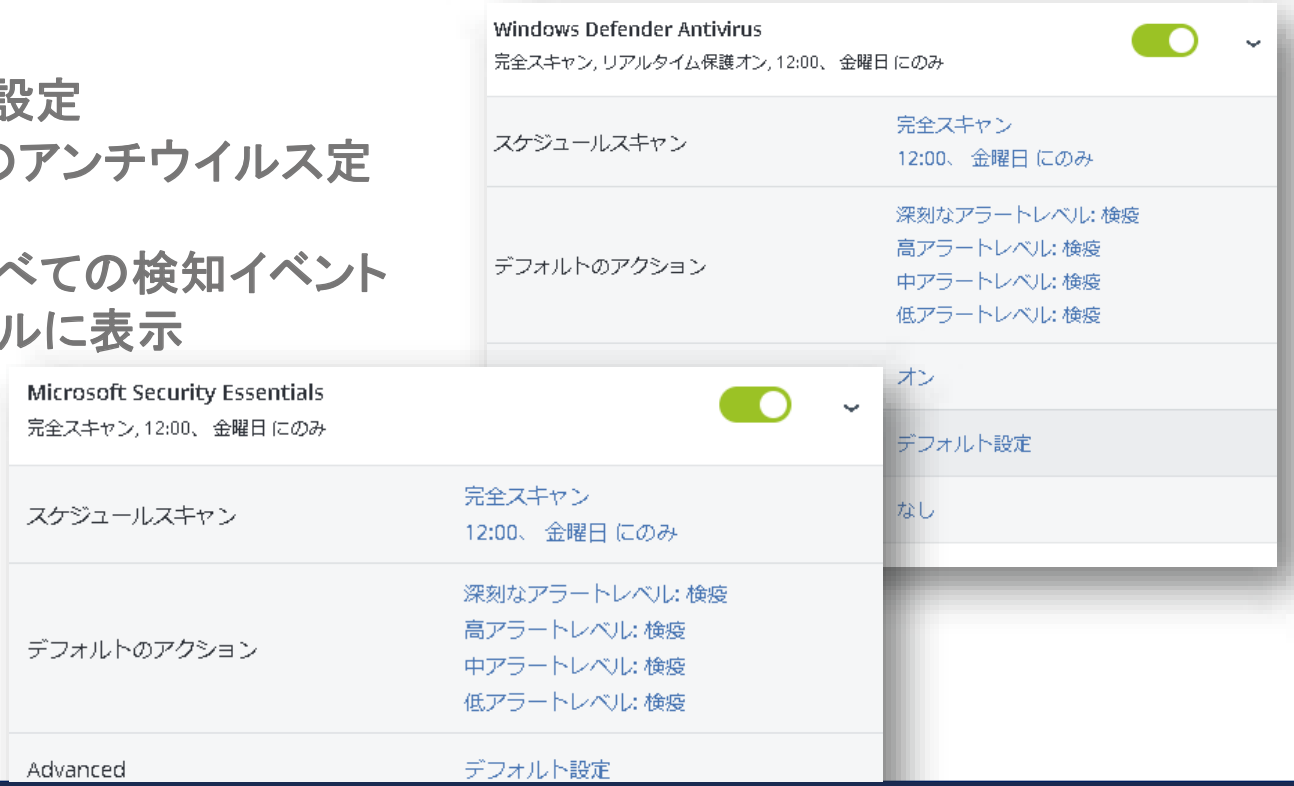
アドバンスセキュリティ

バックアップされたOSイメージには、復旧後にマシンを再感染させるマルウェアが含まれている可能性があります。
マシンにパッチを当て、最新のマルウェア対策定義を適用することで、ユーザーは最新のパッチでOSイメージを復元することができ、再感染の可能性を減らすことができます。

Windows Defenderまたは Microsoft Security Essentials管理

アドバンスセキュリティ

- 複数マシンに強制的に設定
- すべてのマシンで最新のアンチウイルス定義に更新
- Windows Defenderのすべての検知イベントを収集し、管理コンソールに表示



クラウドバックアップ
&セキュリティ

メールバスター

AI学習でスパムメール99.98%撃退

メールバスター

完全クラウドメールセキュリティサービス
個々のPCへのソフトウェアインストール　最新版更新が不要
ウイルス撃退率 /スパム撃退率 99.98%！
ランサムウェア対策やOffice365にも対応

安心・ストレスフリーな受信トレイを今すぐ実現

メールセキュリティサービスの重要性

順位	組織
1位	ランサムウェアによる被害
2位	標的型攻撃による機密情報の窃取
3位	サプライチェーンの弱点を悪用した攻撃
4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
5位	内部不正による情報漏えい
6位	脆弱性対策情報の公開に伴う悪用増加
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
8位	ビジネスメール詐欺による金銭被害
9位	予期せぬIT基盤の障害に伴う業務停止
10位	不注意による情報漏えい等の被害

スパムメール

→ウイルス配布や個人情報の流出などが目的

ウイルスメール

→添付ファイルやURLから悪質なウイルスを感染させる目的
（Emotet など）

標準型メール

→機密情報や顧客情報を盗む目的
(主に金融機関や官公庁などが標的)

機密情報流出や金銭問題など、さまざまな被害に。

Emotet

Emotet とは？？？

→ロシアを拠点とする、マルウェア亜種およびサイバー犯罪活動。
他のマルウェアやスパイウェアもセットで感染させる機能がある。

企業がEmotetに感染した場合の最大の問題点は？？

「 盗まれた個人情報が第三者に悪用される 」

「 周囲の関係者に感染を広げる 」

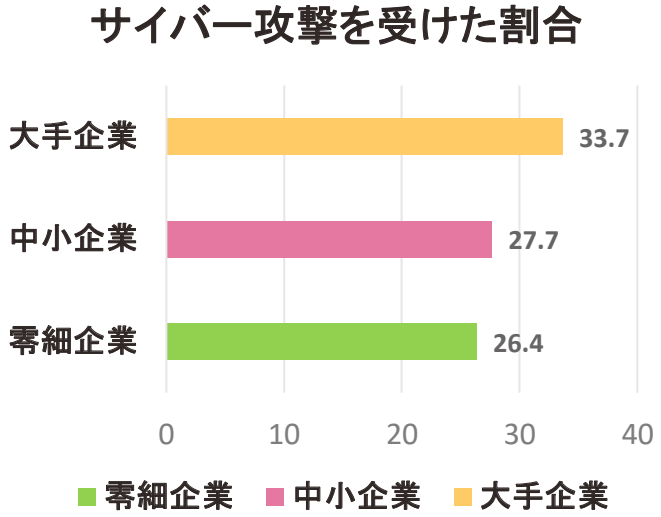
他のウイルスを呼びこみ、さらなる被害を。

中小、零細企業の現状

中小、零細企業におけるセキュリティ対策の優先度は最下位。

- 小規模な企業には関係がない。
- セキュリティ強化のための予算が割きづらい。
- 専門の人材がいない。

中小、零細企業の”約8割”がセキュリティ対策が十分ではない。



“堅牢な対策の大手企業“から、”対策が十分ではない中小、零細企業“へ。

標的の事業規模による差がなくなってきている。

被害を受けた際の中小、零細企業に与える影響

・損害賠償

個人情報や機密情報などの情報漏洩で、取引先や顧客から**損害賠償**を受けることに。

さらに原因調査と復旧にもコストがかかる。

・信用の低下、失墜

社会的信用の低下により、競合他社に顧客が流出してしまう。

情報漏洩で顧客データなどを流出してしまう事により、**取引停止**に。

・業務の停滞

被害の調査、復旧には大幅に時間がかかる。その間、業務が停止し、**機会損失**につながる。

対策にかかるコスト　＜　被害を受けた際にかかるコスト

ランサムウェア被害　事例

日本年金機構

2015.5/8　から　18日間
社内用メールアドレスと社員個人の業務メールアドレス宛に“標準型攻撃メール”が124通送られる。

そのうち5通の添付ファイルを開いたり、URLリンクをクリックしファイルをダウンロード。

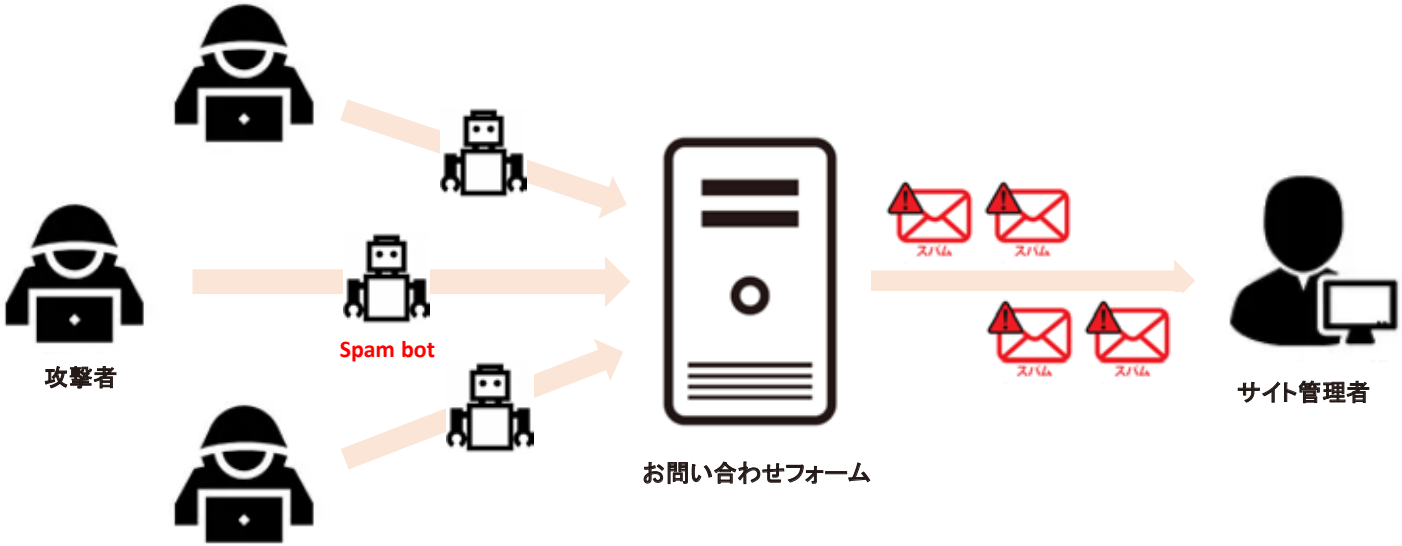
結果、125万人の個人情報の流出に。

日本年金機構の受けた“標準型メール攻撃”の手口

特定の拠点の社員を狙い、実在の社員の名前や業務に関する内容を記載する巧妙な手口。

ランサムウェア被害の“約6割”はメールからの被害となっている

スパムメール投稿のしくみ



攻撃をプログラムされたspambotが、インターネット上の問い合わせフォームから機械的にスパムを送信してくる。

マルウェアを含むURLを勝手にダウンロードするサイトに誘導するため、警戒が必要。

スパムメール対策の基本

- 不審なメールは削除する
- 信頼できない添付ファイルを開かない
- 知っている送信元でも怪しい内容は開かない
- 不要なファイルを添付しない
- セキュリティソフトを使用する

Q. 基本を抑えただけで、標的型攻撃メールの被害は防げるのか？？

A. いいえ。防げません。

標準型攻撃メールを受信した時点で、

社内情報流出の危機に立たされています。

メールボックスに受信しない仕組みが必要！！！

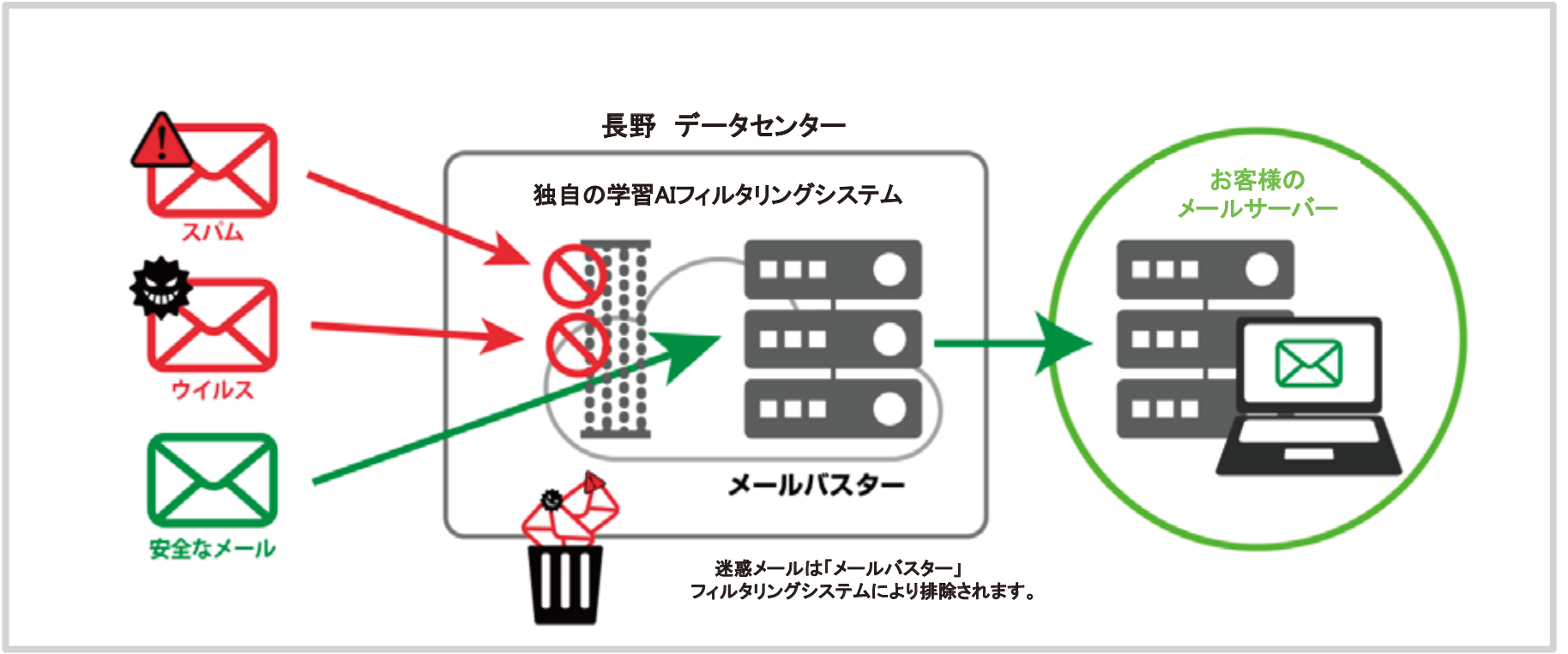
メールバスターとは　？？

日々進化する

完全クラウド型メールセキュリティサービス

- 使いやすい管理画面　Web完結型
- AI学習型のメールフィルタリング
- スパム撃退率　99.98%
- ウイルス対策
- ランサムウェア対策

受信メールに届く様々な攻撃から、ネットワークを守ります。



参考資料

クラウドバックアップ&セキュリティ

上場企業を含む4,000社以上のサービス導入実績

主な企業