

Acronis

New Generation Data Protection

Powered by the Acronis **AnyData** Engine

ランサムウェアとクラウドバックアップ

アクロニス・ジャパン セールスエンジニアマネージャ

佐藤 匡史

目次

- **<ランサムウェア>**
 - ランサムウェアの概要
 - ランサムウェアの動向
 - ランサムウェアが流行る理由
 - 身代金への様々な見解
 - 各ランサムウェアの特徴
 - 実際の被害例
 - 基本的な対策
 - ランサムウェア被害からの復旧
 - バックアップの運用
- **<クラウドバックアップ>**
 - 市場動向
 - クラウドバックアップについて
 - バックアップについて

ランサムウェアとは

- コンピュータ内のファイルを人質にとり身代金を要求するウイルス



感染例

司法省、中央情報局、連邦捜査局
DOJ ! CIA ! ! FBI ! ! !

あなたは414MB(ビデオ)の飛び切り、この上なくやましいファイルをダウンロードした疑いがあります。連邦法にのっとりあなたのコンピュータをロックします。。

罰金を\$300払いなさい ! !



Your computer has been locked due to suspicion of illegal content downloading and distribution.

Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)

18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)

18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to \$250,000.

Technical details:

Involved IP address:

Involved host name: **Note**

Source or intermediary sites: <http://www.pornhub.com>

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unlock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of \$300.

HOW TO UNLOCK YOUR COMPUTER:

- Take your cash to one of this retail locations:
- Get a MoneyPak and purchase it with cash at the register
- Come back and enter your MoneyPak code to unlock your computer (5 attempts available)
Code:

1	2	3
4	5	6
7	8	9
Delete	0	Enter

Permanent lock on 05/04/2013 12:4 p.m. EST

ランサムウェアの動向



ランサムウェア

- ランサムウェアとは
 - コンピュータ内のファイルを人質にとり身代金を要求するウイルス

2016年3月 米国国土安全保障省 ランサムウェアの注意喚起

2016年1月 情報処理推進機構 (IPA) からの呼びかけ

「ランサムウェア感染被害に備えて**定期的なバックアップ**を」
組織における感染は**組織全体に被害を及ぼす**可能性も

2015年6月 IPA パソコン内のファイルを人質にとるランサムウェアに注意

2015年5月 JPCERTCC ランサムウェア感染に関する注意喚起

2015年 警視庁 不測の事態に備え、データのバックアップを！

参照元 US-CERT <https://www.us-cert.gov/ncas/alerts/TA16-091A>

参照元 IPA 2016年1月の呼びかけ、2015年6月の呼びかけ

参照元 JPCERTCC <https://www.jpcert.or.jp/at/2015/at150015.html>

参照元 警視庁 <http://www.keishicho.metro.tokyo.jp/kurashi/cyber/security/cyber503.html>

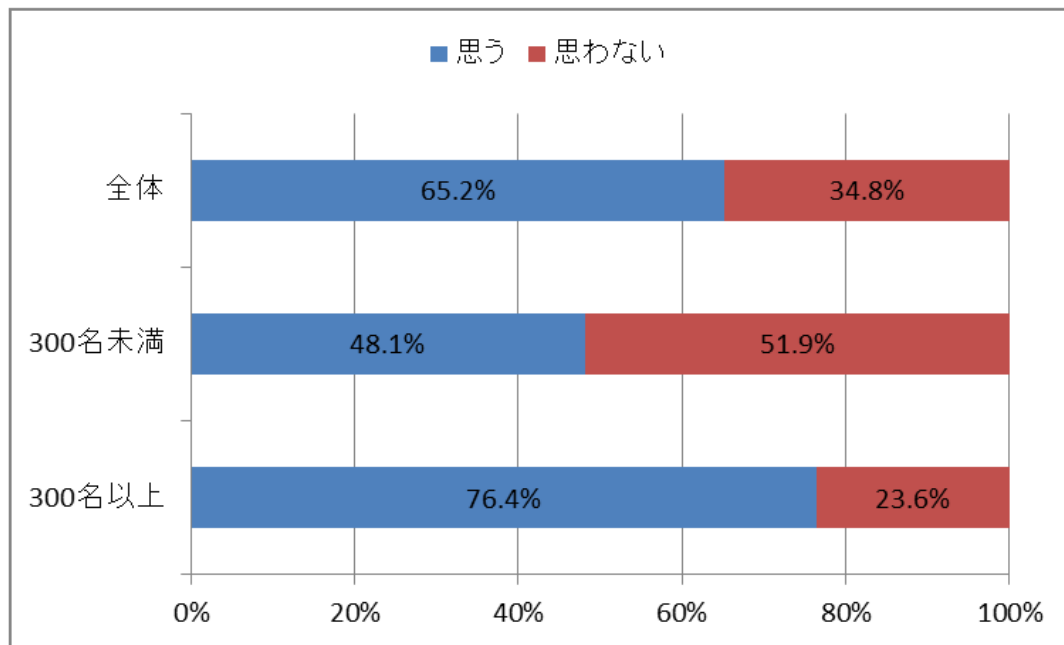
直近の事例

- 米国 ハリウッ드의病院で被害
 - 10日間の一部業務停止、身代金を支払って復旧(40ビットコイン)
- 米国 ケンタッキー州の病院で被害
 - 内部ネットワークから複数台感染、4ビットコイン請求
- カナダ オタワの病院で被害
 - 4台のコンピュータで被害
- 米国 カリフォルニアの2つの病院で被害
- ドイツの病院で被害(ZDNet 3月1日掲載)
 - 復旧には数週間かかる
- 米国ワシントンD.Cの病院で被害(3月25日)
 - 4月1日時点で復旧中

ランサムウェアに関する意識と実態

2016年6月国内534人が対象

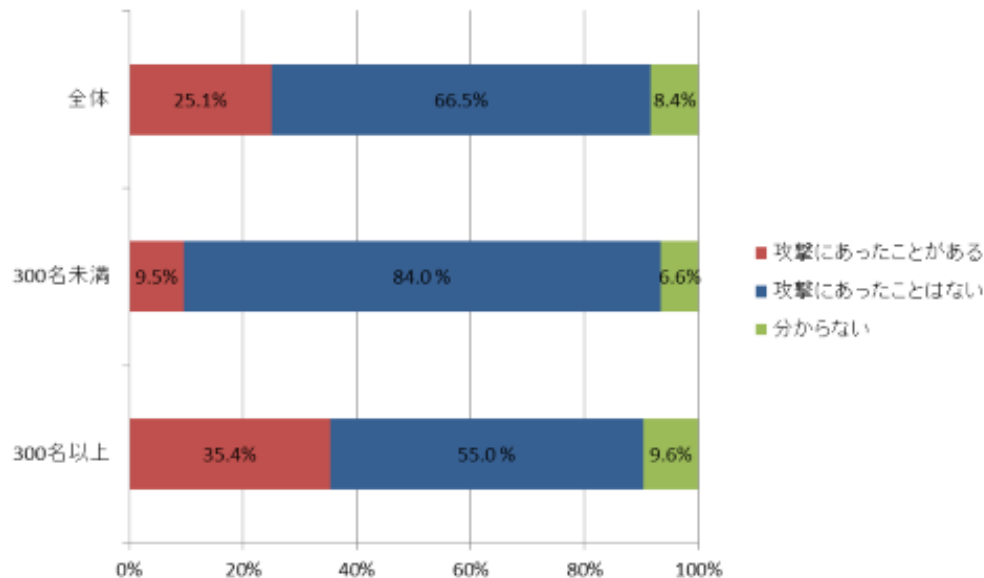
- 自社は大丈夫と思う方が34.8%



参照元: <http://internet.watch.impress.co.jp/docs/news/1013149.html>

ランサムウェアの被害に遭った経験

- 全体の25%が被害に遭っている



参照元: <http://internet.watch.impress.co.jp/docs/news/1013149.html>

2015年の被害報告

- 2015年は法人からのランサムウェア被害報告が2014年の約14倍となった

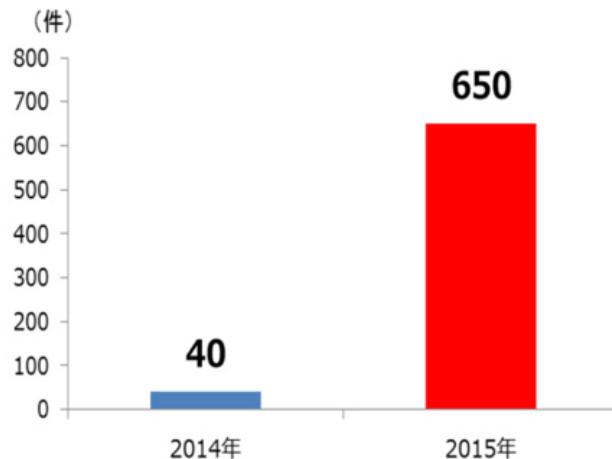


図1: 法人ユーザからのランサムウェア被害報告件数推移(日本)

参照元: <http://blog.trendmicro.co.jp/archives/13175>

2016年の被害報告

- 前年同期で7倍。法人は9倍で全体の87%を占める
- 検出数は16600件、前年比9倍、法人は4500件、前年比35倍の急拡大

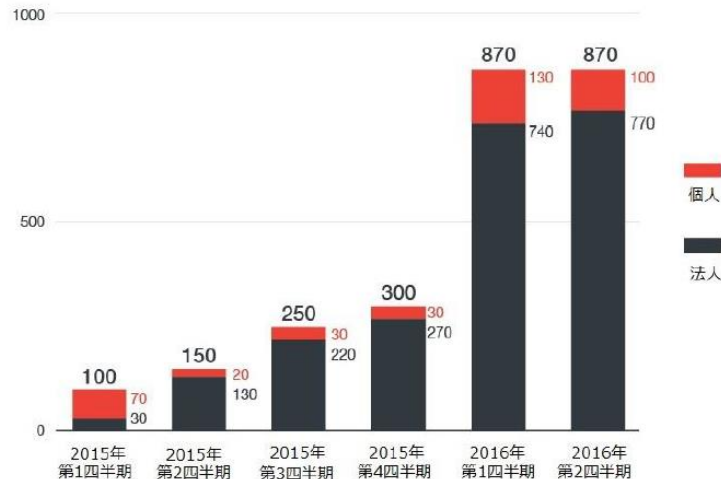


図1：国内法人からのランサムウェア感染被害報告数推移（トレンドマイクロサポートセンター調べ）

参照元:トレンドマイクロ 2016年上半期セキュリティランドアップ

ランサムウェアが流行する理由



RaaS (Ransomware as a service)の存在

- アフィリエイト管理パネル
- 例) 売上の60%はAffiliate、40%はAuthorの配分

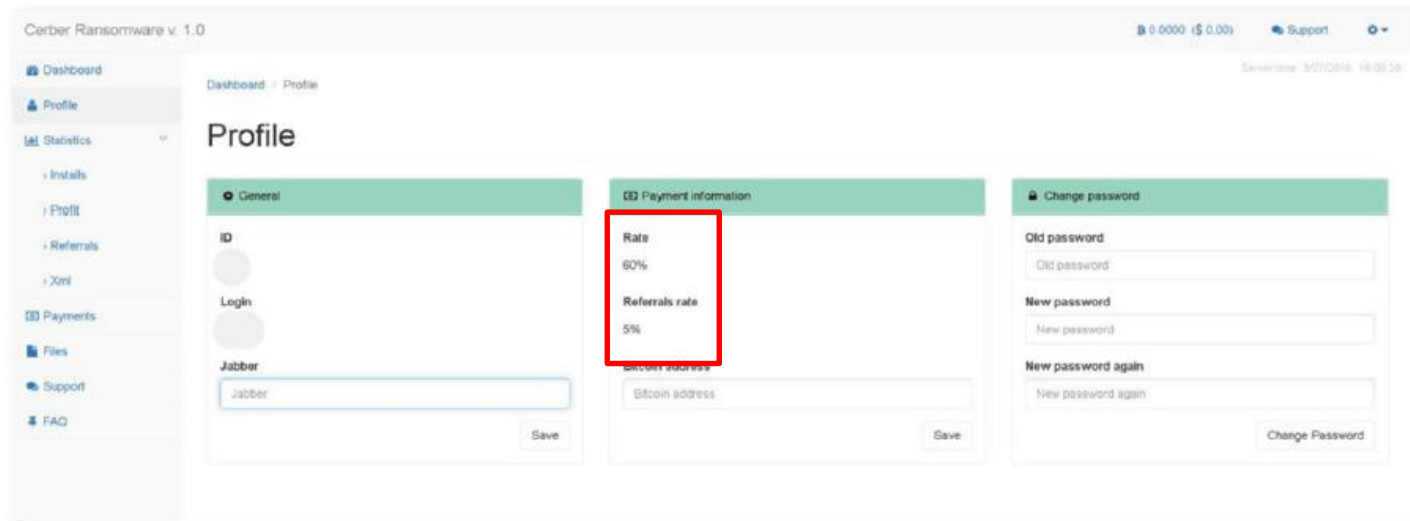
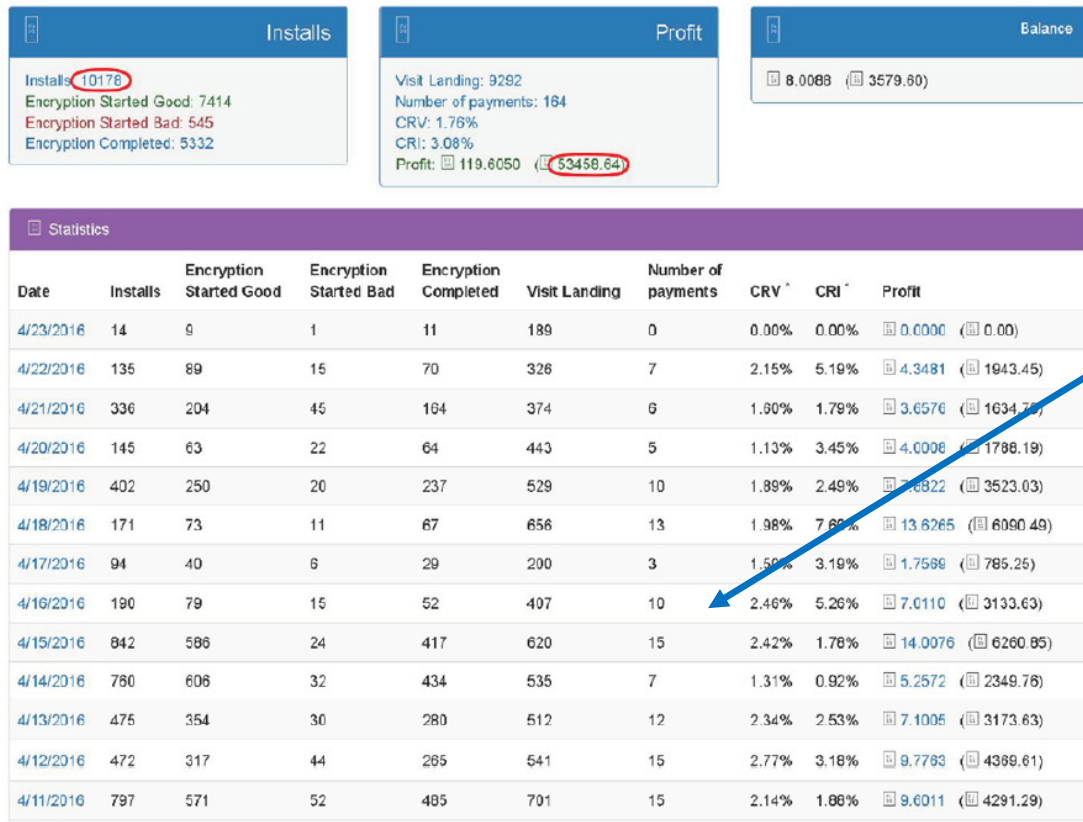


Figure 2: Cerber Affiliate Panel – Earn 60% of the Profit, and a 5% Referral Rate

参照元: CheckPoint CerberRing: An In-Depth Expose on Cerber Ransomware-as-a-Service

Dashboard



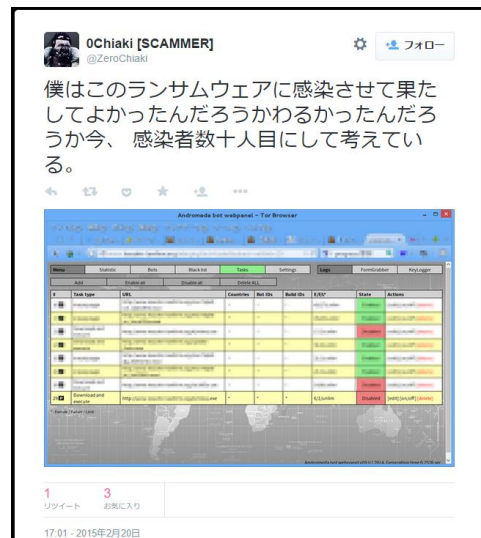
例えば4月16日
訪問者: 407名
インストール: 190台
暗号化開始: 79台
暗号化失敗: 15台
暗号化済み: 52台
CRV: 2.42%
CRI: 5.26%
売上\$3133 (¥313,300)

Figure 6: Second Sample Campaign

参照元: CheckPoint CerberRing: An In-Depth Expose on Cerber Ransomware-as-a-Service

アフィリエイトの影響力

- 2015年7月 17歳少年が不正アクセスで逮捕、余罪でランサムウェア作成
- 2015年11月 14歳少年がランサムウェアを販売逮捕



参照元: <http://d.hatena.ne.jp/Kango/20150701/1435770111>

ハッカーの日々の努力

- ポリモーフィック
 - 感染の度に自身のコードを毎回ランダムに変化させ、セキュリティソフトによる検出を回避する仕組みを持つ性質
 - パターンマッチングで検出できない
- 対多層防御
 - ランサムウェアが多層防御に態勢を持つ
 - ふるまい検知、レピュテーションも十分ではない

身代金への様々な見解



世界での被害

- ビットコインのマスターウォレットを追跡した結果CryptoWall version3の被害額が400億円であった

参照元: <http://blogs.mcafee.jp/mcafeeblog/2015/11/32500400cryptow-a0cb.html>

身代金

- 追跡が難しい(犯人が見つからない)
- ドイツの病院の例 40ビットコイン

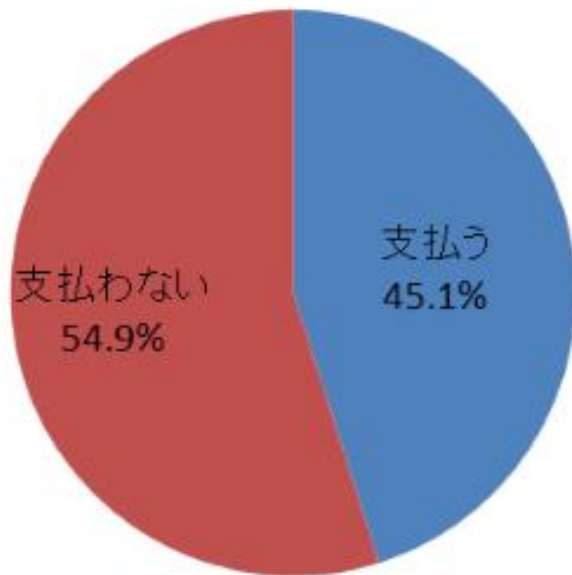


⇒ 約240万円

参照元: <http://jpbitcoin.com/markets>

身代金を払いますか??

- 支払うと答える人の割合が多い！



参照元: <http://internet.watch.impress.co.jp/docs/news/1013149.html>

身代金の払い方

身代金の支払い方法

ほぼビットコイン

bitFlyerで購入



ようこそ！ bitFlyerへ

ご登録のアドレスに確認メールを送りました。
メールに記載されているキーワードを入力してください。
または、メールに記載のリンクからアカウント作成を進めてください。

キーワード

アカウント作成



ようこそ！ bitFlyerへ

個人情報や取引履歴を登録すると、bitFlyerのサービスがもっと便利になります。
もちろん、手数料などは一切発生しない無料のサービスです。
ログインパスワードは初期登録時のメールアドレス、もしくはご登録いただいたメールアドレスに記載されています。

- ☒ ご利用開始とプライバシーポリシーに同意します。
- ☒ ビットコイン取引におけるリスクについて理解しました。
- ☒ 私は未成年の消費者ではありません。

bitFlyerをはじめる

- ・携帯電話認証
- ・Facebook連携が必要
(プロフィール、友達など)



アカウントクラスをアップグレードする

お客様のアカウントは **エコミークラス** です

スタンバイクラス

エコミークラス

プレミアムエコミー

エグゼクティブエコミー

ビジネスクラス

ファーストクラス

アップグレードいただくための要件

Facebook 連携

携帯電話認証

エコミークラスでできること

✓ ビットコイン預入・送付

外部ビットコインウォレットとbitFlyer アカウントの間でビットコインを出し入れします。

✓ ビットコイン購入・売却

日本円によりビットコインを購入・売却します。

✓ bitWire / エコマース

メールアドレスを使用しビットコインを送付します。相手がbitFlyerアカウントを持っていれば、即時に送付が完了します。従来のビットコインウォレットのように、10分以上待たされることはありません。
また、bitFlyer内にお持ちのビットコインを利用して、提携先のネットショップ等でお買い物ができます。

エコミークラスでできないこと

— 円デポジット入金・解約

デポジットをご入金いただくことにより、bitFlyerアカウントでの日本円残高を増やすことができます。また、デポジットをご解約することにより、bitFlyer内にお持ちのデポジットを現金として出金することが可能です。

— Lightning 現物取引

bitFlyer Lightning は、現物取引所です。日本円でビットコインを買うこともできれば、持っているビットコインを売って、円に替えることもできます。

— Lightning FX

Lightning FXでは、5倍のレバレッジを効かせ、値上がり値下がり双方で利益を狙うことができ、多様な戦略での投資が可能です。

— Lightning イーサリアム

Lightning イーサリアムは、イーサリアムの現物取引サービスです。ビットコインでイーサを購入、もしくはイーサを売却しビットコインに替えることができます。

各ランサムウェアの特徴



近年のランサムウェア

- 2012年 Reveton 画面をロックする
- 2013年 CryptoLocker 特定ファイルの暗号化
- 2014年 Cryptwall メール添付ファイルを利用
- 2015年 CrypTesla vvvウィルスとして国内で話題に
- 2016年 Locky メール添付のwordファイルにて感染
- 2016年 SAMAS バックアップ破壊・LAN内拡散
- 2016年 Petya MBR、MFTの暗号化
- 2016年 FairWare Linuxがターゲット
- 2016年 Rex CMSの脆弱性を利用
- 2016年 Rasome32 Javascriptで作られた初めてのモデル
- 2016年 CERBER RaaS型で広く拡散
- 2016年 CryptXXX 現在最も凶悪
- 2016年 JIGSAW 被害者の恐怖を煽る

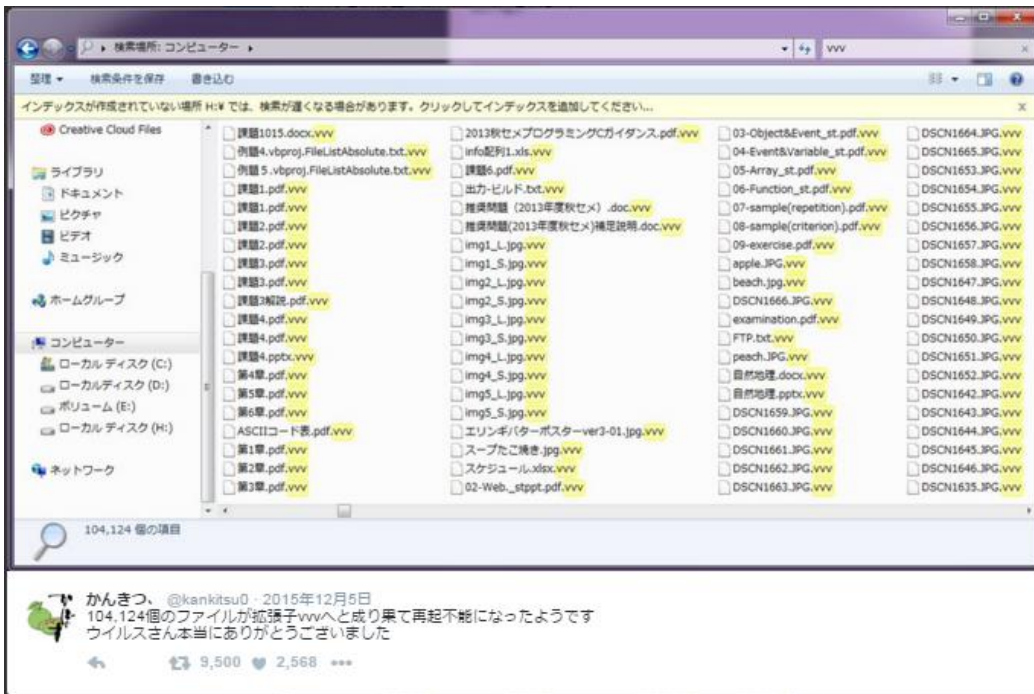
感染経路



CrypTeslaの動作

- 1. 添付ファイル付のメールとして配信
- 2. 不正なJavascriptを実行させる
- 3. 実行ファイルのダウンロード
- 4. 対象ファイルの暗号化
- 5. 請求情報の提示

例 (Cryp Teslaなど)



12月売上.pdf



12月売上.pdf.vww

出典: <https://twitter.com/kankitsu0/status/673057182561112064>

Lockyの動作

- 1. 添付ファイル付のメールとして配信
- 2. Wordファイル内のマクロを実行させる
- 3. 実行ファイルのダウンロード
- 4. 対象ファイルの暗号化
- 5. 請求情報の提示

例(Locky)

名前 ▲	種類
☐ 84E22087FF1A34D1A1D12272246D0D80.locky	LOCKY ファイル
☐ 84E22087FF1A34D1A3B4E976246515DE.locky	LOCKY ファイル
☐ 84E22087FF1A34D1A17C45C51C121FD9.locky	LOCKY ファイル
☐ 84E22087FF1A34D1A1141F470E6AD796.locky	LOCKY ファイル
☐ 84E22087FF1A34D1A5667E288D0F88E8.locky	LOCKY ファイル
☐ 84E22087FF1A34D1AFA06150416535F7.locky	LOCKY ファイル
☐ 84E22087FF1A34D1B1E34408988B188F.locky	LOCKY ファイル
☐ 84E22087FF1A34D1B6A22031A81EFAF6.locky	LOCKY ファイル
☐ 84E22087FF1A34D1B9CB22C3ADCA3952.locky	LOCKY ファイル
☐ 84E22087FF1A34D1B547E25AF5F7ED81.locky	LOCKY ファイル
☐ 84E22087FF1A34D1B5912A6C0C1A2E52.locky	LOCKY ファイル
☐ 84E22087FF1A34D1B005923F4061C37F.locky	LOCKY ファイル
☐ 84E22087FF1A34D1BA6F6ADA8CC3E699.locky	LOCKY ファイル
☐ 84E22087FF1A34D1BAB19C4007A3DBCE.locky	LOCKY ファイル
☐ 84E22087FF1A34D1BB56F8A76CE5337A.locky	LOCKY ファイル
☐ 84E22087FF1A34D1BC9C19175677F2F8.locky	LOCKY ファイル
☐ 84E22087FF1A34D1C00CE0C8BCFF4173.locky	LOCKY ファイル
☐ 84E22087FF1A34D1C1CE108B3EDBA69D.locky	LOCKY ファイル
☐ 84E22087FF1A34D1C8CE4CE1BFFFDFA9.locky	LOCKY ファイル
☐ 84E22087FF1A34D1C42C8A5D9D24ED64.locky	LOCKY ファイル

12月売上.pdf



84E22087FF1A34D1B9CB22C3ADCA3952.locky

参照元: http://image.itmedia.co.jp//im/enterprise/articles/1602/18/l_lcky03.jpg

Crypwallの動作

- 1. 添付ファイル付のメールとして配信
- 2. 不正なJavascriptを実行させる
- 3. 実行ファイルのダウンロード
- 4. シャドウコピー削除、スタートアップ修復無効化
- 5. 対象ファイルの暗号化
- 6. 請求情報の提示

例 (CryptoWall4.0など)

0ulh5uc.m9	4 KB	M9 File	11/5/2015 8:17 AM
1h078xqub.i34eu	16 KB	I34EU File	11/5/2015 8:17 AM
1i0qre6y2v.uq9	6 KB	UQ9 File	11/5/2015 8:17 AM
1o0sbj.2v	12 KB	2V File	11/5/2015 8:17 AM
1pjc9itgoa.9d	106 KB	9D File	11/5/2015 8:17 AM
1t4fyr4h.zc8	19 KB	ZC8 File	11/5/2015 8:17 AM
1v2bb1.e4s	33 KB	E4S File	11/5/2015 8:17 AM
2fq9od.7b	9 KB	7B File	11/5/2015 8:17 AM
2s9zj2jyz.9fn6	10 KB	9FN6 File	11/5/2015 8:17 AM
2ws5t6.4i	223 KB	4I File	11/5/2015 8:17 AM
2ymz2r.d7	8 KB	D7 File	11/5/2015 8:17 AM
03f5mkm5.pqr83	12 KB	PQR83 File	11/5/2015 8:17 AM
3lmpzsbqw.w3	19 KB	W3 File	11/5/2015 8:17 AM
3mukoivy3v.y71p6	3 KB	Y71P6 File	11/5/2015 8:17 AM
3nc9xc.qq3	20 KB	QQ3 File	11/5/2015 8:17 AM
3mfulq.69f	9 KB	69F File	11/5/2015 8:17 AM
3s6kw0msg3.d8	35 KB	D8 File	11/5/2015 8:17 AM
3tzc3ucf.m3wli	5 KB	M3WLI File	11/5/2015 8:17 AM
3u6a0n.cp1k	1 KB	CP1K File	11/5/2015 8:17 AM
3uvn5g64.i00n	6 KB	I00N File	11/5/2015 8:17 AM
3w52d5n.d82	95 KB	D82 File	11/5/2015 8:17 AM

12月売上.pdf



3s6kw0msg3.i34eu

参照元: <http://researchcenter.paloaltonetworks.com/2015/11/cryptowall-v4-emerges-days-after-cyber-threat-alliance-report/>

SAMSA

- 1. 添付ファイル付のメールとして配信
- 2. 不正なJavascriptを実行させる
- 3. 実行ファイルのダウンロード
- 4. LAN内でJbossなどのAppサーバを探す
- 5. 社内にランサムウェアが拡散していく
- 6. 複数システムのファイルを暗号化
- 7. 請求情報の提示

例 (SAMSA)

- ネットワークに接続するシステムの検索
- ランサムウェア実行ファイルの配置と実行
- 320種類のファイルを暗号化
- ボリュームシャドウコピーの削除

PETYAの動作

- 1. 添付ファイル付のメールとして配信
- 2. ドロップボックス内の自己解凍ファイルに誘導
- 3. 実行ファイルのダウンロード
- 4. MBRの変更
- 5. 再起動
- 6. chkdsk
- 7. MFTの暗号化
- 8. 請求情報の提示

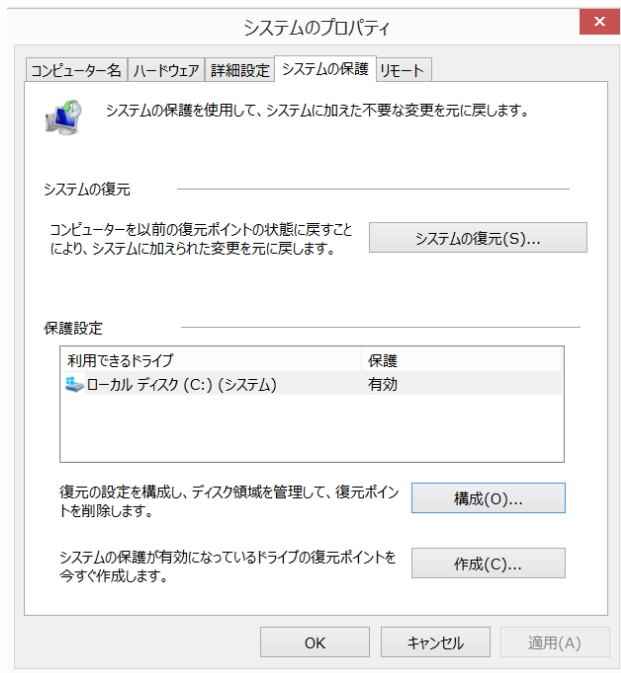
例 (PETYA)

- <https://youtu.be/yfCt35RTR-U>

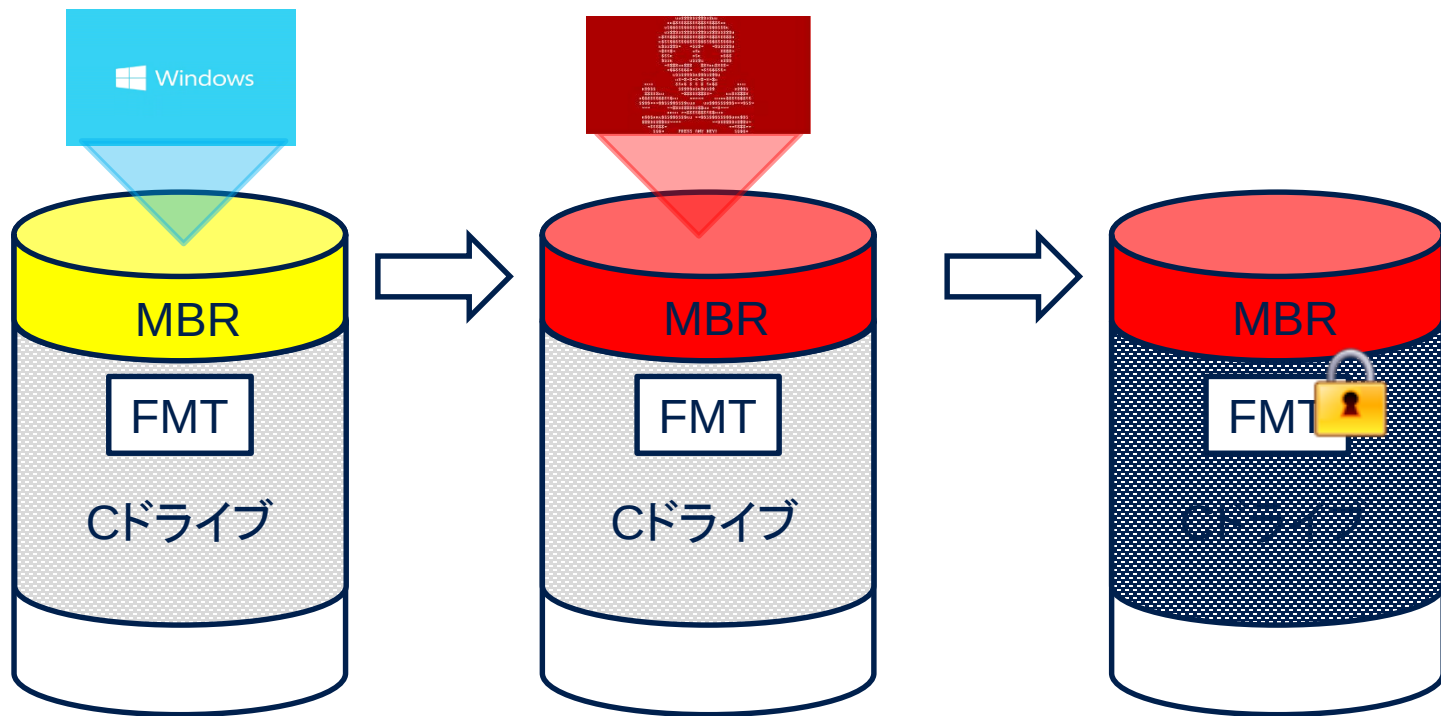


参照元: <http://blog.trendmicro.co.jp/archives/13106>

システムの保護(ボリュームシャドウコピー)



MBRとMFTへの作用



送信されるメールの例

- 取引先のInvoice偽装「Invoice[数字].zip」
- 自分宛ての送信に偽装「Document[数字].zip」
- 自組織内からの差出人偽装 <admin@[組織のドメイン名]>「PDFPart2.pdf」
- 自組織内からの差出人偽装 <nadiam1pa@[組織のドメイン名]>「Document(1).pdf」
- 自組織内からの差出人偽装 <admin@[組織のドメイン名]>「CCE29032016 [数字]」「Sent from my iPhone」
- コピー複合機の受信通知に偽装 <copier@[組織のドメイン名]>「Message from [機種名]」

参照元: <http://www.geocities.co.jp/Playtown-Yoyo/6130/notes/virus-ransomware-locky.htm>

巧妙化するメール

・ 宅配業者を装ったメールの例

例1 件名 出金 本文 ■お届け予定日時 6月30日 時間帯希望なし ※お届け予定日時につきましては、ゴルフスキー・空港宅急便（施設宛）の場合、プレー日（搭乗日）を表示しております。 ■品名：***** ■商品名：宅急便 ■ご依頼主： ■伝票番号：8840-7844-6601 〇〇〇運輸株式会社
例2 件名 商品お届けのご案内 本文 ■お届け予定日時 7月12(水) 時間帯希望なし ※ゴルフスキー・空港宅急便（施設宛）の場合、プレー日（搭乗日）を表示しております。 ■お届け先 （住所）添付ファイルをご確認ください。 ■伝票番号：xxxx-xxxx-xxxx（※12桁の数字がランダムに入ります） 〇〇〇運輸株式会社
例3 件名 宅急便納品完了のお知らせ 本文 ■伝票番号：xxxxxxxxxxxx（※12桁の数字がランダムに入ります） お受け取りの際は、下記のことを必ずご持参ください。 1. 本人確認（運転免許証等） 2. ご印鑑 （お問い合わせ先） 〇〇〇運輸株式会社 お客様サービスセンター *****（※実在する電話番号が入ります）

 ヤマト運輸 [ホームへ](#)

クロネコメンバーズ ログイン [サイトマップ](#)

文字サイズの変更 小 中 大

[商品・サービス](#) [送る](#) [受け取る](#) [ビジネスソリューション](#) [企業情報](#)

[ホーム](#) > [お知らせ](#) > ヤマト運輸の名前を装った添付ファイル付きの不審メールにご注意ください

お知らせ

お客様各位

ヤマト運輸の名前を装った添付ファイル付きの不審メールにご注意ください

ヤマト運輸の名前を装った添付ファイル付きの不審メールが、不特定多数のお客様に断続的に送信されていますが、ヤマト運輸からは添付ファイル付きのメールをお送りすることはありません。

不審メールには、ZIP形式のファイルが添付されており、ファイルを開くとコンピュータウイルスに感染することが想定されます。絶対に添付ファイルを開かず、削除いただきますようお願いいたします。

万が一、添付ファイルを開いてしまった場合は、ウイルス対策ソフトなどでウイルスチェックを行うことをおすすめいたします。

また、不審メールには、ヤマト運輸からお送りしているメールと同じ「件名」や「差出人アドレス」が表示されている場合がありますので、くれぐれもご注意ください。

ご不明な場合は弊社サービスセンターまでご連絡ください。

※本件については、下記の関連サイトもご確認ください。

[警視庁WEB:実在する企業を装ったウイルス付きメールに注意！](#)

[独立行政法人情報処理推進機構\(IPA\) WEB:情報セキュリティ\(ウイルス・不正アクセス\)に関するご相談](#)

以上

http://www.itmedia.co.jp/enterprise/articles/1608/12/news028_2.html

FairWare(2016年8月)

- 1. 改竄されたWebからLinuxに感染
- 2. Web関連フォルダの暗号化
- 3. 暗号化ファイルを外部へコピーと元ファイル削除
- 4. Webサービスが停止
- 5. 脅迫文章を表示

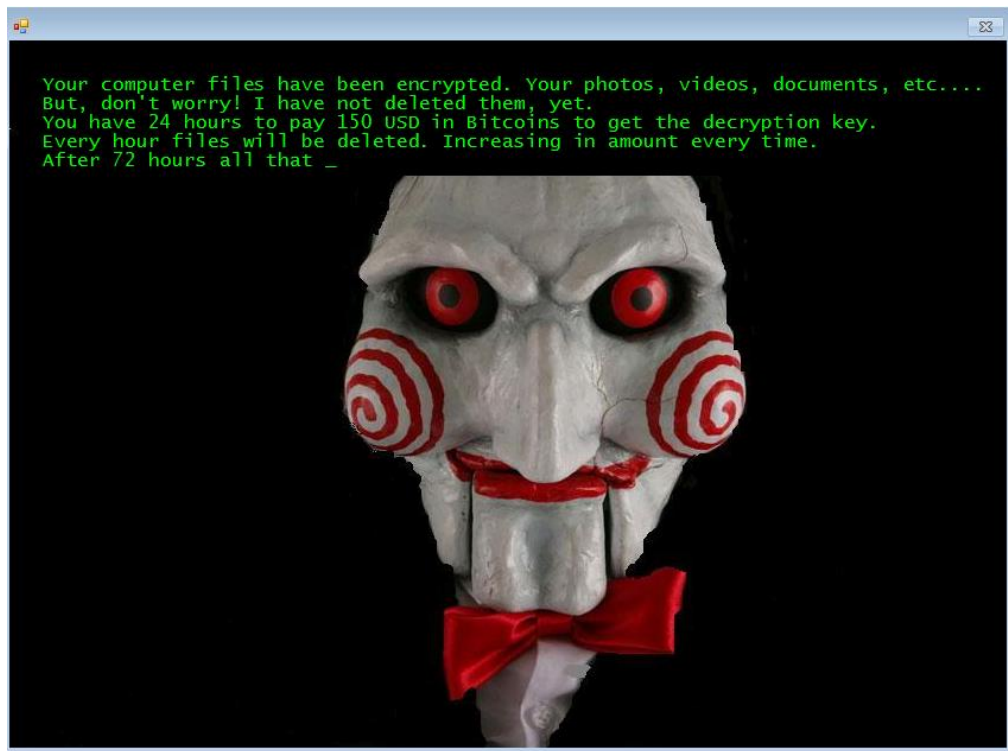
★人質のファイルが漏洩される可能性？

Cerber3(9月)

- 1. Web閲覧 ポップアップ広告から感染
- 2. エクスプロイトキットが組み込まれた別のWebへ誘導
- 3. 環境確認（可能であれば脆弱性を利用し昇格）
- 4. 最適な実行ファイルのダウンロード
- 5. シャドウコピー削除
- 6. ファイル名を.cerberに変更
- 7. 脅迫を文章表示
- Attention,Attention,Attension your documents....



JIGSAW



参照元:トレンドマイクロセキュリティブログ <http://blog.trendmicro.co.jp/archives/13258>

JIGSAW

- 1. クラウドストレージサービス、Webサイトからダウンロード
- 2. ファイルの暗号化と拡張子変更(fun, KKK, BTC,,,))
- 3. 身代金を要求
- 4. JIGSAW2.0では主要プロセスを無効(taskmgr, Regedit, Autoruns, cmd)
- 5. 段階的にファイルを削除する
(最初24時間数個、2日目は数百、3日目は数千)

★PCを再起動すると1000個のファイルが削除される

JIGSAW

- ライブチャットのオペレータによるサポート機能付き

- やり取り

ハッカー) ご要件は

被害者) 本当に復号できるんですか？

ハッカー) はい。振りこみ完了をクリックするだけです

被害者) 高すぎて払えません

ハッカー) 24時間以降は300ドル、72時間で450ドルになります

被害者) 安くする方法はないですか

ハッカー) 24時間以内なら125ドルまで下げられます

Androidデバイス

- 1. システムアップデートを装う
- 2. 各権限を要求(ネットワーク通信、ハードウェア制御など)
- 3. 管理APIの権限要求
- 4. インストール
- 5. 画面のロックと脅迫



アクロニス・ジャパン パートナ様の例



被害に遭った法人

- 従業員20名
- Windowsのラップトップ、デスクトップを利用
- ファイルサーバにてドキュメント管理
- 全PCにはファイルサーバにのみ保存すべき重要な企業データが保存されている

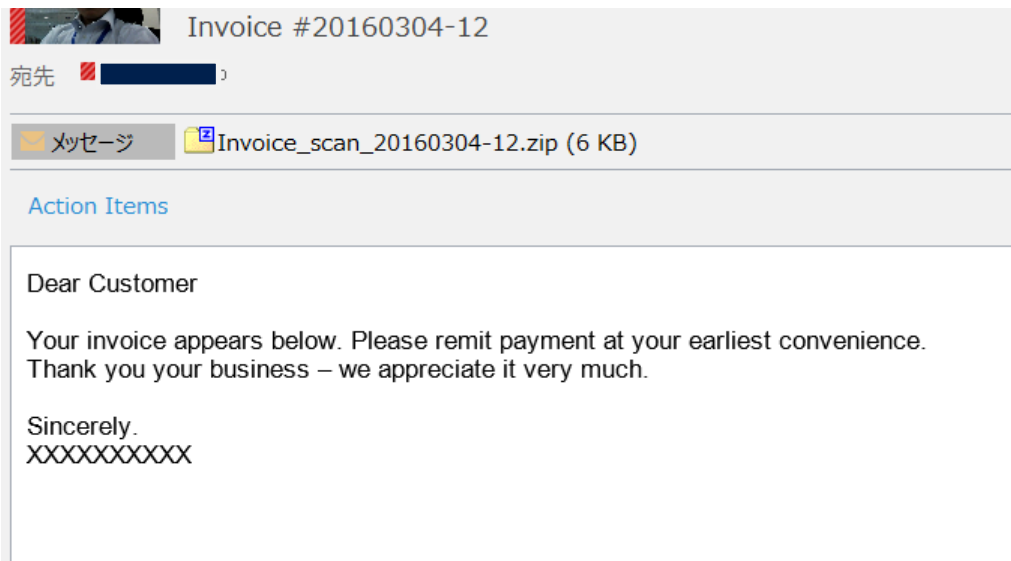
バックアップ

- クラウドへのバックアップを実施
- 日次で永久増分バックアップ
- 日中業務時間帯でバックアップを実施

感染源 メール

件名: Invoice #XXXXXXX

添付ファイル: Invoice_scan_XXXXXXX.zip



感染の詳細

- 感染者: 海外との業務の多い経理部門担当者
 - ①個人宛でInvoiceを装ったメールの受信
 - ②添付ファイル InvoiceXXX.zipの解答
 - ③生成されたファイルの実行
 - ④pdf,xls,docなどの業務利用ファイルが暗号化
 - ⑤ファイルサーバに保存しているファイルも暗号化
 - ⑥ファイルにアクセスすると暗号化されたことを通知するポップアップが表示され感染が発覚

復旧までの道のり

- 1日目：社内IT部門に報告
 - IT部門で調査開始、ランサムウェアの特定
 - 単体のPCとファイルサーバ上のファイルへの感染を確認
 - PCの切り離し
- 2日目：
 - IT部門にて感染ファイルのリストを作成
 - イメージバックアップから感染前の状態に復旧
 - ファイルサーバ側のリスト作成
 - 本番ファイルサーバから感染ファイルの削除
 - バックアップからダミーファイルサーバにバックアップを展開
 - 必要なファイルを本番ファイルサーバにコピー

基本的な対策



3大原則

OS、パッチ最新
セキュリティソフト最新
バックアップ取得

お金があればセキュリティ強化

多層防御

侵入 前

- メールゲートウェイ
 - 悪意のあるメールをブロック
- Webレピュテーション
 - C&C、改竄されたWebサイトへのアクセスをブロック
- サンドボックス
 - 実行ファイル、オフィスファイルを事前確認

侵入 後

- エンドポイント
- アプリケーションコントロール
- 振る舞い検知
 - 未知のプロセス検知
 - ランサムウェアプロセスの制御

見落としがちな

- セキュリティにおける最大の弱点は人
 - 教育（添付ファイル開かないで）
 - 予行演習（たまにダミーメールを送る）
 - ソーシャルエンジニアリング対策

ランサムウェア被害から復旧



ランサムウェアの進化と復旧方法

- CrypTesla(vvv)による被害は拡張子.vvvのファイルをリスト化することで**ファイルバックアップ**からの復元が可能
- CryptoWall4.0ではファイル名、拡張子がランダムに変更される、また暗号化の対象ファイルは200種に及ぶことから被害に遭ったファイルを特定することは不可能。Cドライブ直下、アプリケーションで利用するファイルなども含まれることから、**ファイルバックアップ**からの復元は実質不可能。ディスク全体の**イメージバックアップ**からシステムを含めて復旧することが有効

ランサムウェアの進化と復旧方法

- PETYAではMBRが変更され、MFTが暗号化されることからファイルバックアップから復元する場合にはOSの再インストールが必要。ディスク全体のイメージバックアップからシステムを含めて復旧することが有効

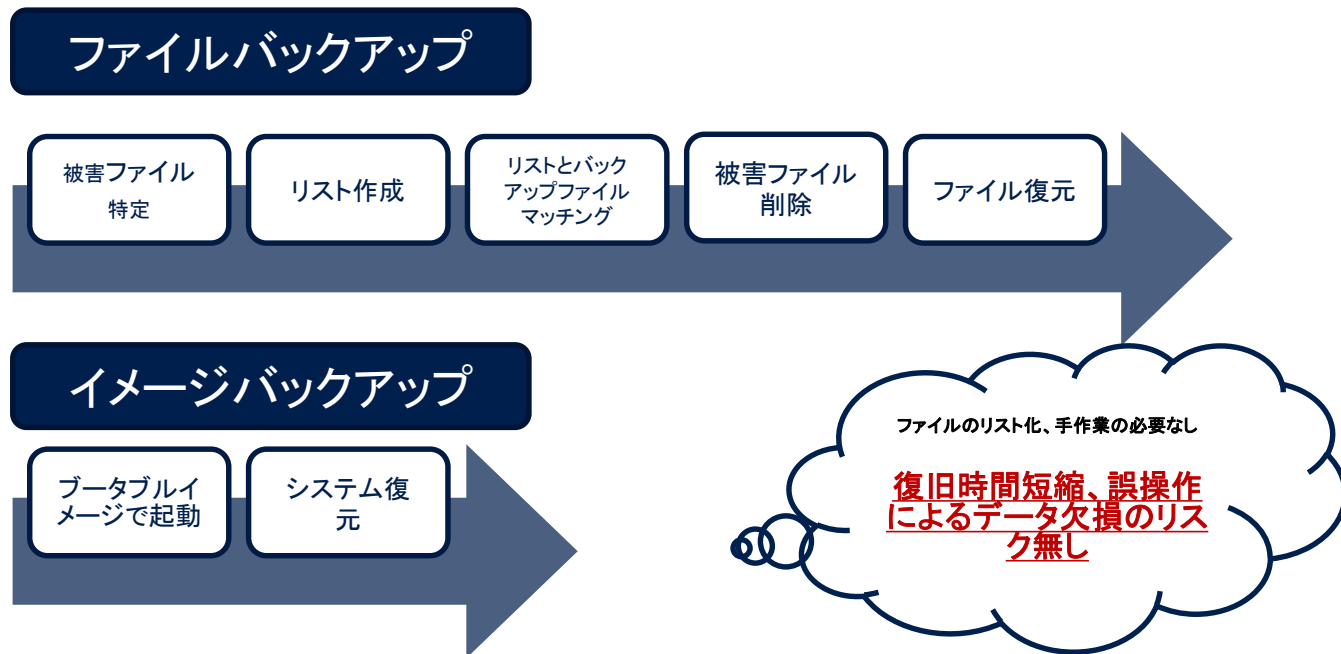
被害と復旧方法



	CrypTesla	CryptoWall	PETYA
被害ファイルの特定	○	×	×
OSの起動	○	○	×
ファイルバックアップによる復旧	○	△	×
イメージバックアップによる復旧	◎	◎	◎

ファイルバックアップ vs イメージバックアップ

- CrypTesla被害からの復旧工程



ファイルバックアップ vs イメージバックアップ

- CryptoWall被害からの復旧工程

ファイルバックアップ



イメージバックアップ



OSやアプリケーションの再インストールや設定は不要!

復旧時間の大幅短縮を実現!

バックアップ運用について



潜在的なリスク

- バックアップの保存先
 - ネットワーク共有
 - OSでマウントしている外付けHDD
- バックアップデータがランサムウェアにより暗号化される



- ランサムウェアにより復元ポイントが失われる可能性がある

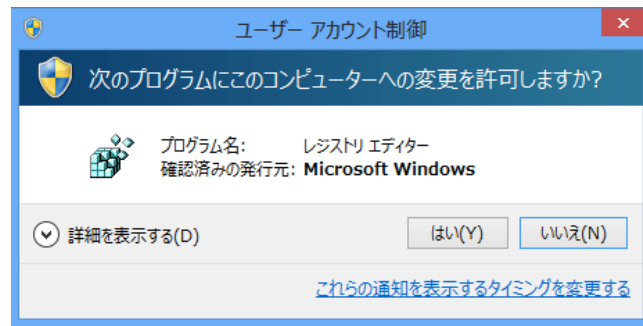
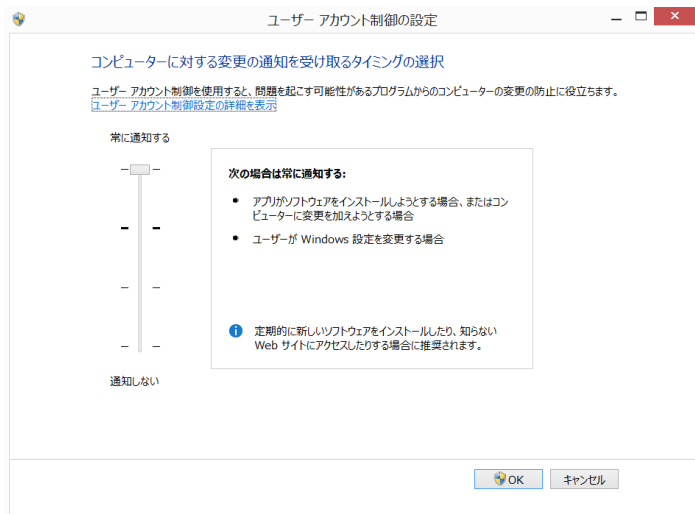
バックアップの留意事項

- 使用する装置・媒体は、バックアップ時のみパソコンと接続する
- 使用する装置・媒体は複数用意し、バックアップする
- 正常に復元できることを定期的に確認する



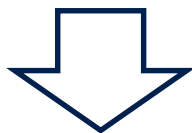
原則

- 通常の業務には権限の弱いユーザを利用する
- UACを必ずオンにする



バックアップ運用のポイント

- バックアップの保存先には適切なアクセス権を付与
- 保存先にアクセスできるユーザを制限
- 複数の世代を保存
- 2つ以上のロケーションにバックアップを保存
- OS標準のバックアップは削除される可能性あり



バックアップ専用ソフトウェアの利用

ネットワーク共有へのアクセス制御

- Acronis Backupの機能
 - バックアップアーカイブの保存先にアクセスするための任意のログイン情報を設定することが可能
 - 上記で指定されたユーザがバックアップアーカイブの所有者となる
- 環境設定
 - バックアップの管理に一般ユーザ(PCのオーナー)ではなく専用のバックアップ管理ユーザを作成する
 - ネットワーク共有側に適切なアクセスコントロールを設定する



- Acronis Backupと適切な環境設定を行うことでランサムウェアによるバックアップアーカイブの改ざんを防ぐことが可能

USB接続のHDDへのアクセス制御

- Acronis Backupの機能
 - バックアップアーカイブの保存先にアクセスするための任意のログイン情報を設定することが可能
 - 上記で指定されたユーザがバックアップアーカイブの所有者となる
- 環境設定
 - バックアップの管理に一般ユーザ(PCのオーナー)ではなく専用のバックアップ管理ユーザを作成する
 - HDDに適切なアクセスコントロールを設定する



- Acronis Backupと適切な環境設定を行うことでランサムウェアによるバックアップアーカイブの改ざんを防ぐことが可能

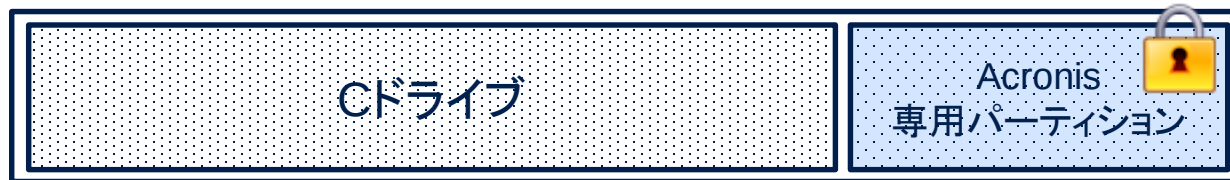
特殊なパーティション



Acronis Secure Zone(ASZ)について

- Acronis Backup/Acronis Backup Advancedが管理する
データ保存領域
 - 特徴
 - セキュアゾーンにアクセスするためにはバックアップエージェントが必要
 - Windows上ではボリュームマウントされない領域として確認される
 - 内部データの管理はエージェント経由でのみ可能
 - 更にセキュアゾーン領域にパスワードを設定することが可能

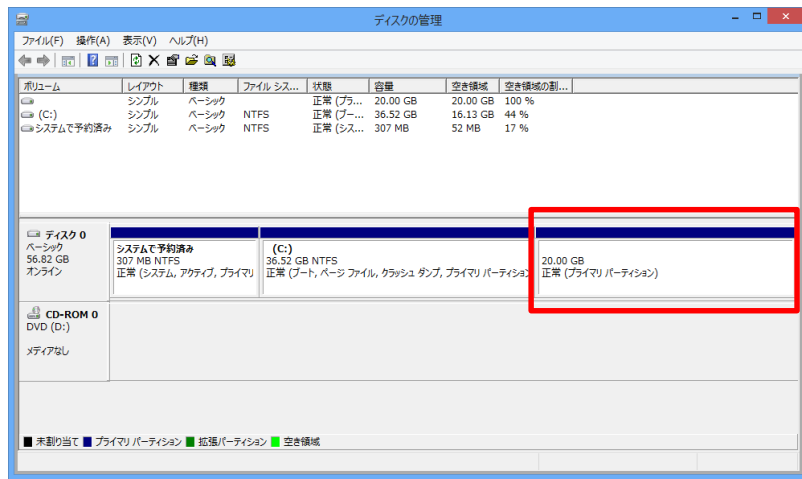
内部/外部
ディスク



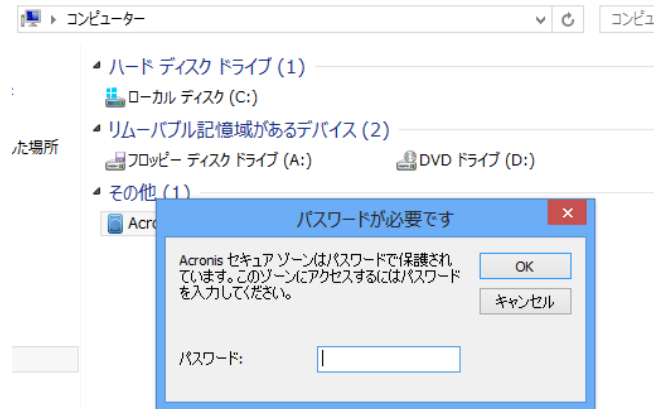
Acronis Secure Zone (ASZ)について

- 表示例 (Windows8)

ドライブレターを持たないパーティションとして
OS上は認識されている



エージェントがインストールされている場合、エクスプローラから表示は可能。※操作一切不可



USB接続HDDにおけるASZ利用

- Acronis Secure Zoneの利点
 - 安価なUSB接続HDDにバックアップが可能
 - 通常の利用領域とは別にパーティショニングが可能のため既存のHDD空き領域を活用できる
 - OSからの操作はできないことから誤操作によるデータ損失も防止可能



- ランサムウェアによるバックアップアーカイブの改ざんを現在の環境で簡単設定で防ぐことが可能

ローカルディスクにおけるASZ利用

- Acronis Secure Zoneの利点
 - 外付けのHDDなどの購入ができないユーザでも導入が可能
 - 外付けHDDの持ち運びなどによるディスクの破損がない
 - 通常の利用領域とは別にパーティショニングが可能のため既存のHDD空き領域を活用できる
 - OSからの操作はできないことから誤操作によるデータ損失も防止可能



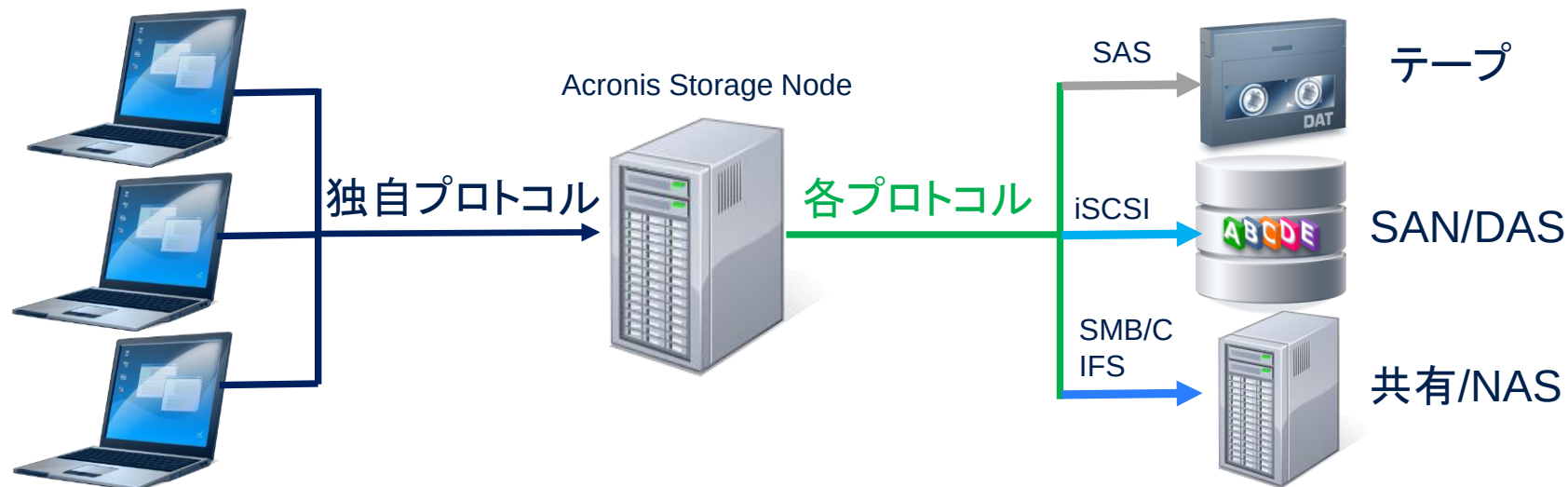
- ランサムウェアによるバックアップアーカイブの改ざんを現在の環境で簡単設定で防ぐことが可能

中継サーバの利用



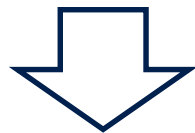
Acronis Storage Node

- Acronis Storage NodeはWindows上で動作するアプリケーション。
- 仮想マシンの構成も可能



Acronis Storage Nodeによる運用

- Acronis Storage Nodeの利点
 - 重複除外により保存するデータ量を削減することが可能
 - バックアップアーカイブの処理を代行することによりバックアップエージェント側の負荷を軽減
 - Windows上で動作するアプリケーションとして実装可能なことから、仮想、クラウドなどでも利用が可能



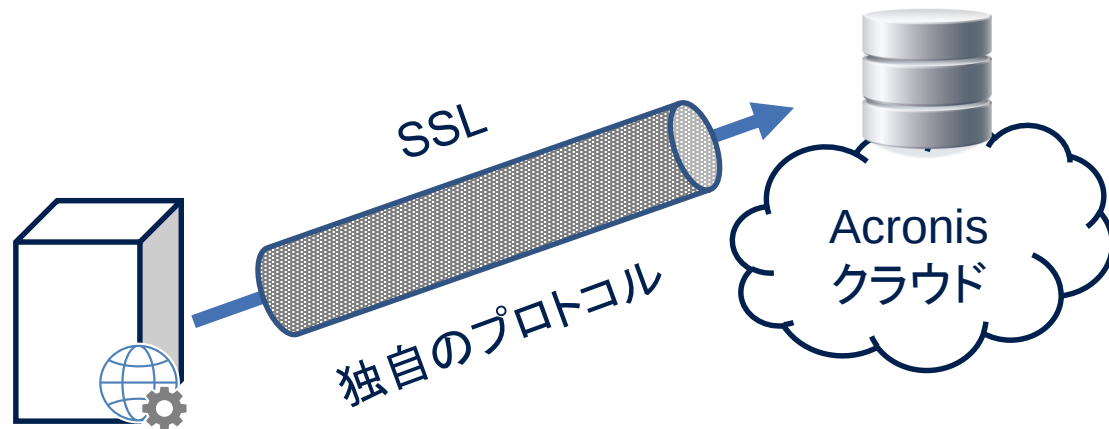
- クライアントからバックアップ保存領域を直接参照しない。また、ASNへの接続は独自のプロトコルを用いることからバックアップアーカイブのランサムウェア被害を完全に防ぐことが可能

クラウドの利用



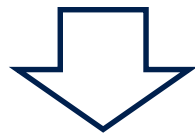
Acronisクラウドの利用

- 独自のプロトコルでクラウド領域にデータを転送
- 転送、バックアップアーカイブは暗号化



Acronis クラウドによる運用

- Acronis クラウドの利点
 - オンプレミスにストレージを構築する必要がない
 - 急激なデータ増加があってもスケールアウトが可能
 - 転送・バックアップアーカイブの暗号化



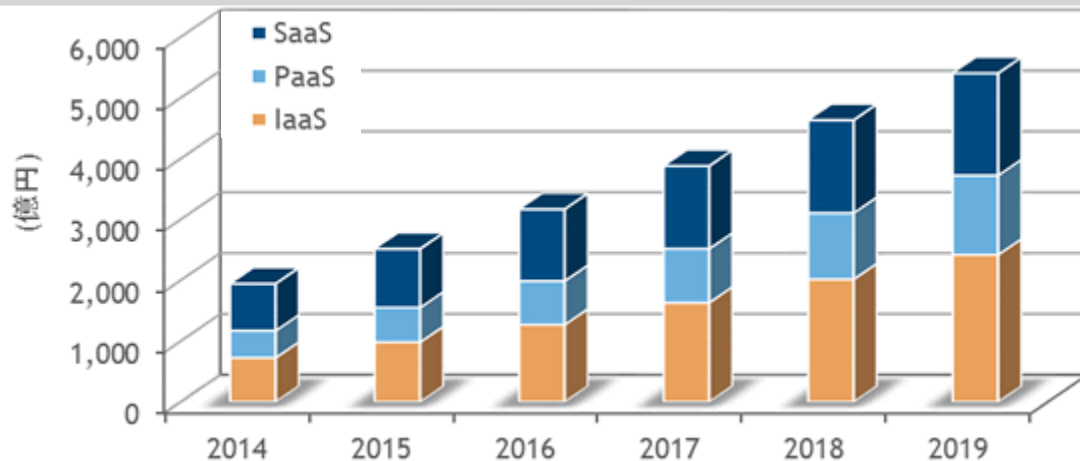
- クライアントからバックアップ保存領域を直接参照しない。また、Acronis クラウドへの接続は独自のプロトコルを用いることからバックアップアーカイブのランサムウェア被害を完全に防ぐことが可能

クラウドバックアップ 市場動向



パブリッククラウドサービス市場

- 2019年には2.8倍の市場になる
- クラウドの発展が新しいIT需要を喚起する鍵



Note: Intelligent Industry SolutionはICTを使った「業務プロセス、コンテンツ、マーケットプレイス/コミュニティ環境」のサービスであり、IT機能を有償で提供することを目的としていないため国内パブリッククラウドサービス市場には含まれていない。

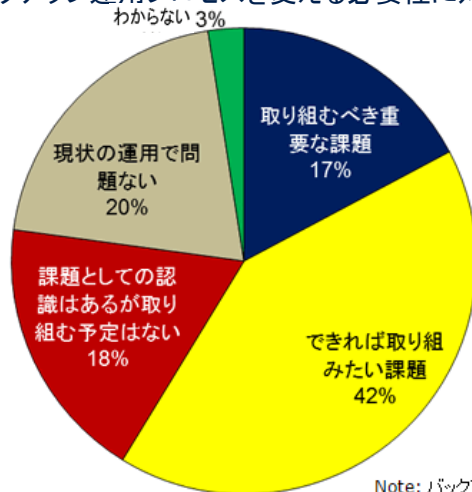
Source: IDC Japan, 8/2015

出典: IDC Japanプレスリリース「国内パブリッククラウドサービス市場予測を発表」(2015年8月6日)

バックアップ運用

- 全体の約60%が運用を変える必要性を認識している
- クラウドサービスの浸透も影響を与えている

現在のバックアップ運用プロセスを変える必要性に対する認識



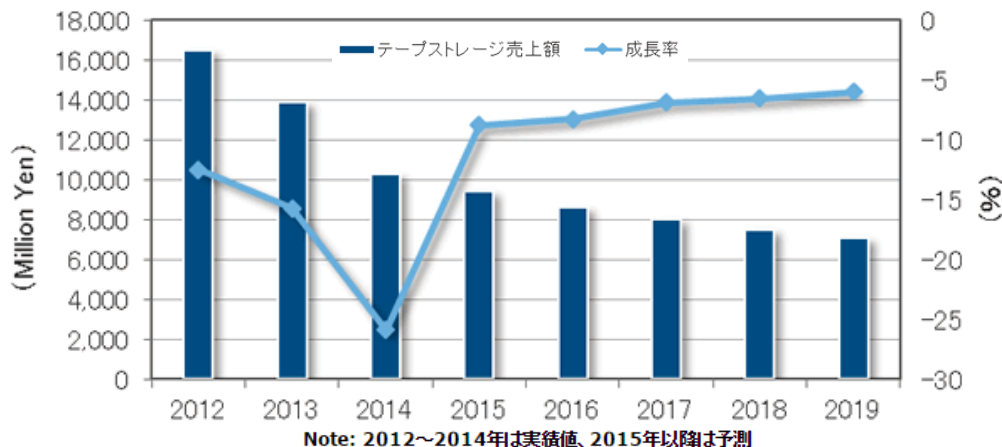
Note: バックアップ業務に関わっている回答者(n = 766)が対象

出典: IDC Japanプレスリリース「国内データ保護の実態と将来展望を発表」(2015年1月30日)

テープストレージ市場

- サーバへの装着率が低下している
- 従来環境におけるバックアップ用途の需要は減少

国内テープストレージ市場 売上額実績および予測：2012年～2019年

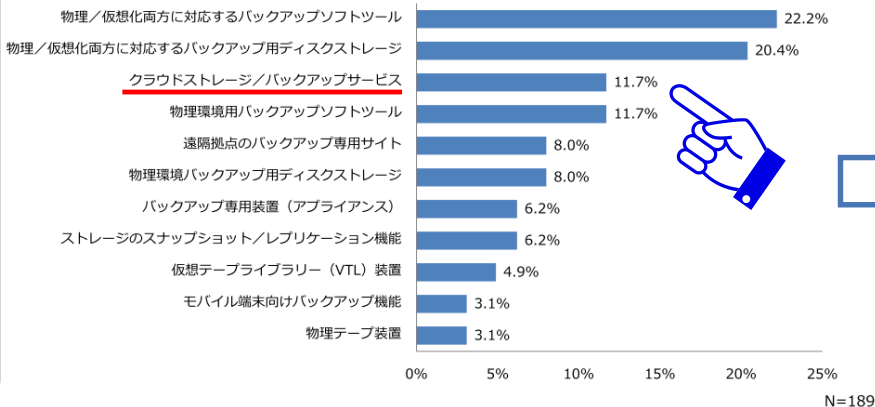


出典：IDC Japanプレスリリース「国内テープストレージ市場予測を発表」(2015年7月6日)

現在検討中、導入予定のバックアップ

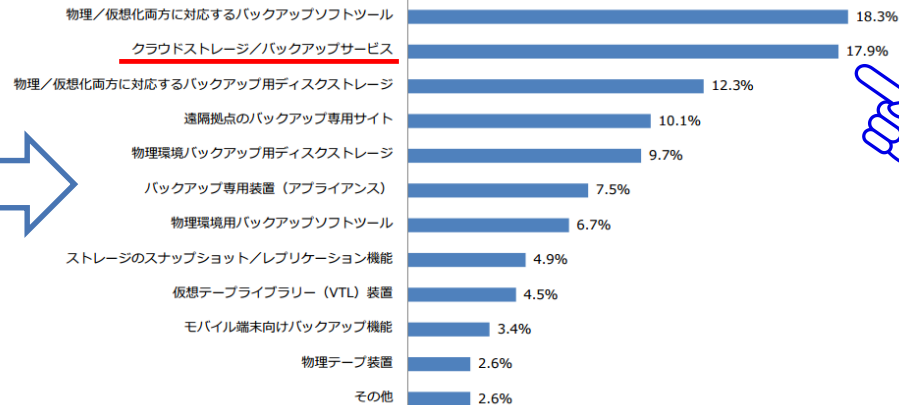
- クラウドバックアップサービスは**6.7ポイント**の急上昇
- その他ストレージ、テープなどは明らかな**下降**トレンド

2014年の調査結果



本調査結果は TechTargetジャパン会員調査レポートバックアップ/リカバリ環境に関するアンケート調査
～(2014年4月2日～4月30実施) から一部を抜粋したものです。

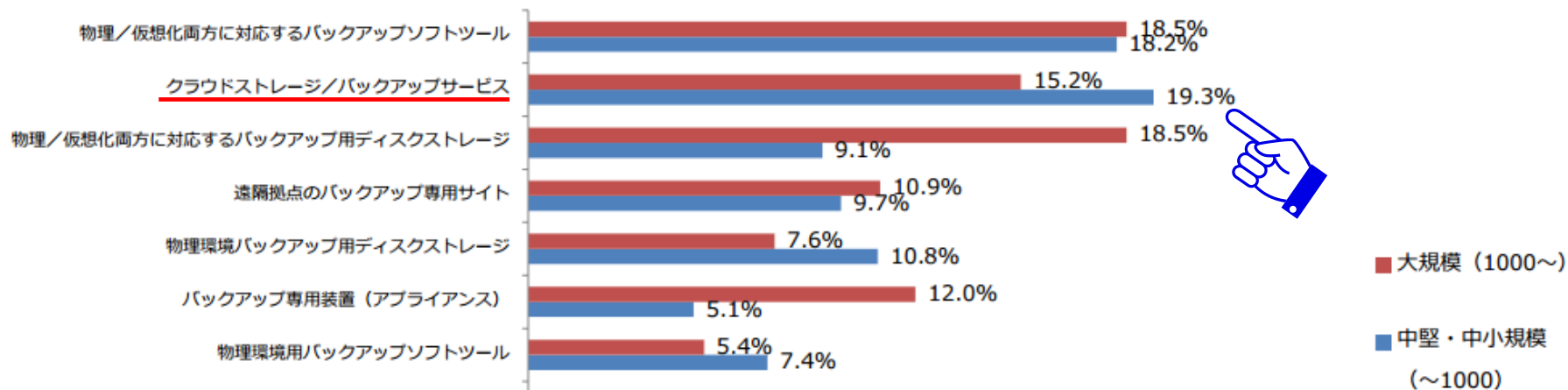
2015年の調査結果



TechTargetジャパン: バックアップ・リカバリ環境に関する読者調査 (2015年4月)
<http://techtarget.itmedia.co.jp/it/news/1504/27/news04.html>

検討中、導入予定のバックアップ(企業別)

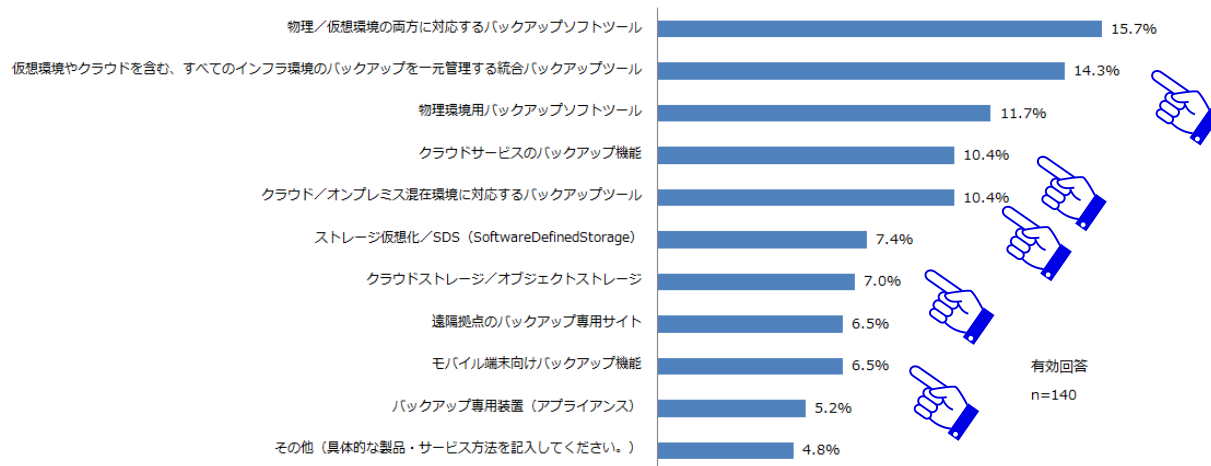
- 中堅・中小企業ではクラウドバックアップサービスへの注目度が圧倒的に高い



TechTargetジャパン: バックアップ・リカバリ環境に関する読者調査(2015年4月)
<http://techtarget.itmedia.co.jp/it/news/1504/27/news04.html>

2016年今度導入予定のバックアップ関連の技術や製品、サービス

- 2016年ついにクラウド一辺倒となった
- バックアップ＝クラウドはついにブレイクする



TechTargetジャパン: 解消されない“バックアップの避けられない課題”にどう立ち向かう？
<http://techtarget.itmedia.co.jp/it/news/1606/08/news01.html>

今後の予測

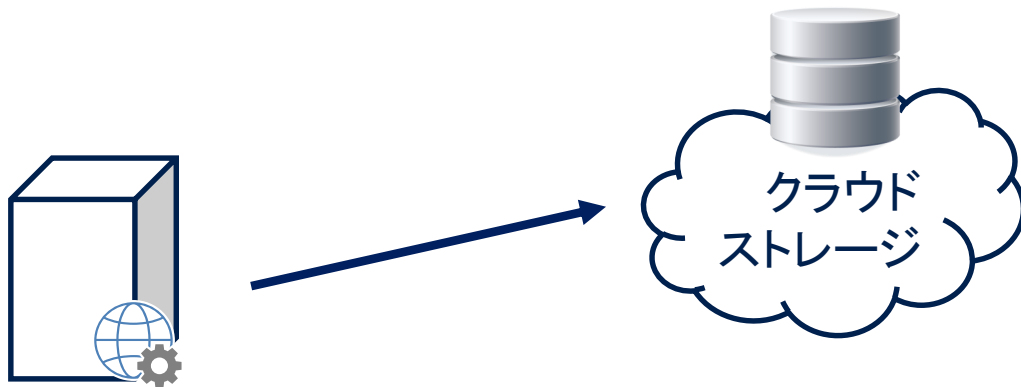
- 世界でのBackup as a Serviceの推進には4つの要素が必要
- ①SMACへの適応 (Social, Mobile, Analytics, Cloud)
 - ②仮想マシンのクラウドバックアップ
 - ③クラウドへの集約
 - ④バックアップと復元の自動化

クラウドバックアップについて



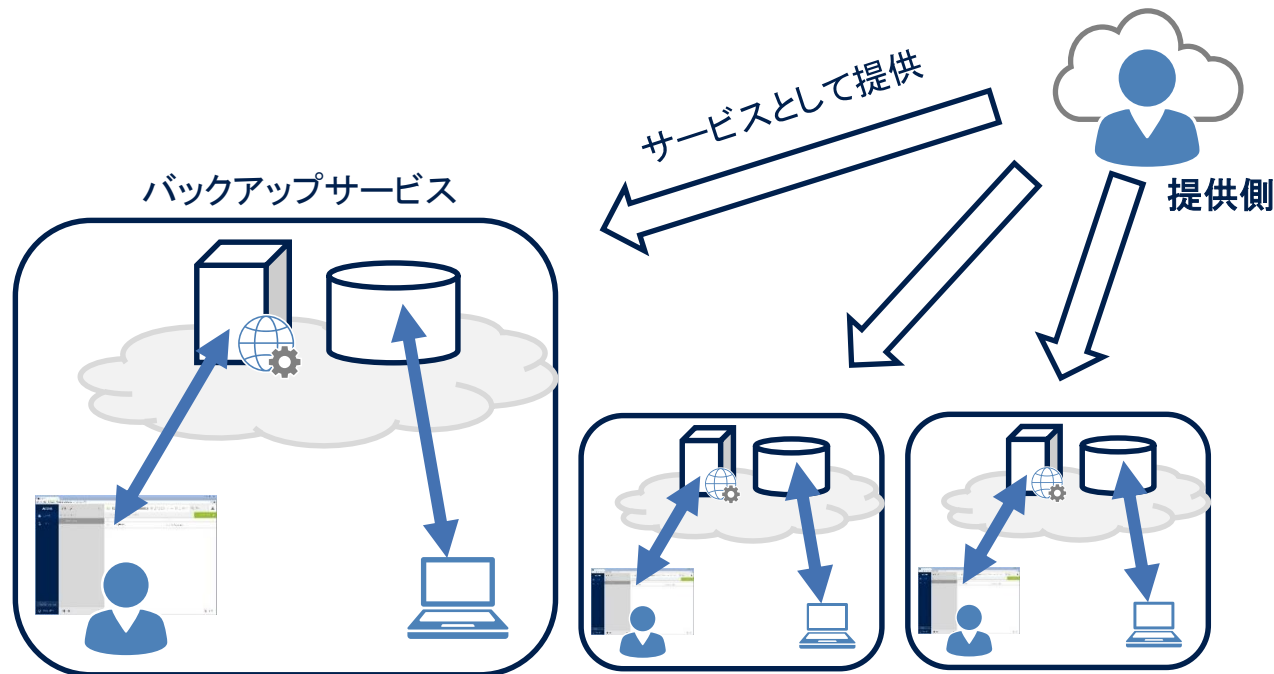
クラウドストレージへのデータ転送

- バックアップツールを利用したクラウドストレージへのデータのコピー、転送。



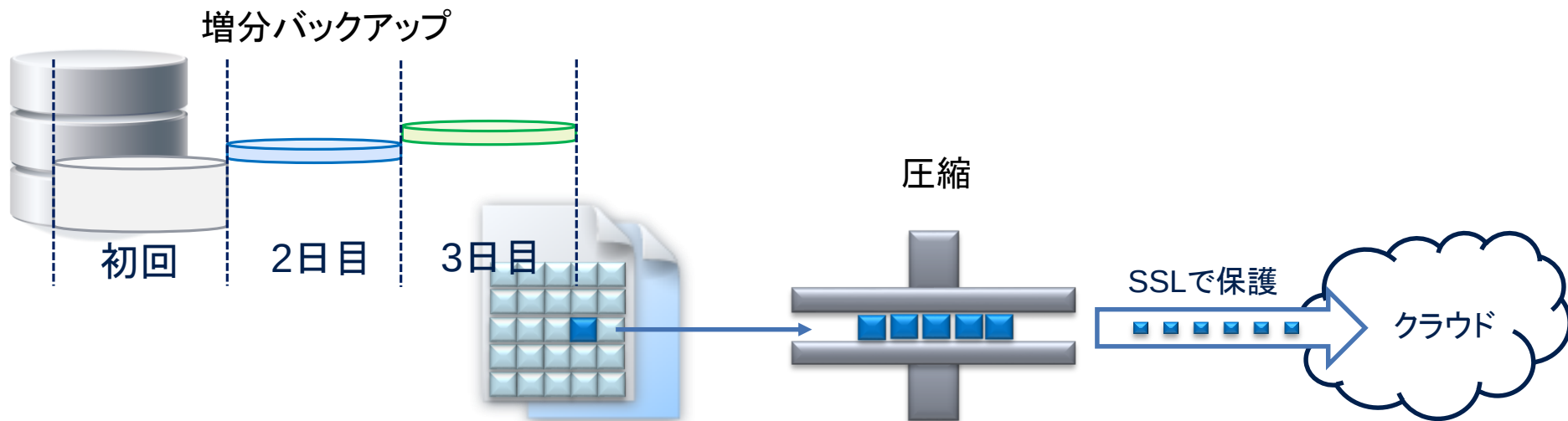
SaaSとして提供が可能

- SaaS型のバックアップを提供



データ転送の最適化

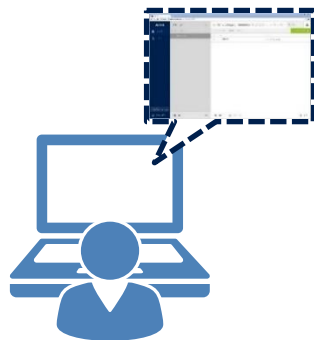
- 初回以降は増分のみをバックアップ
- 変更のあったブロックを検出してのバックアップ



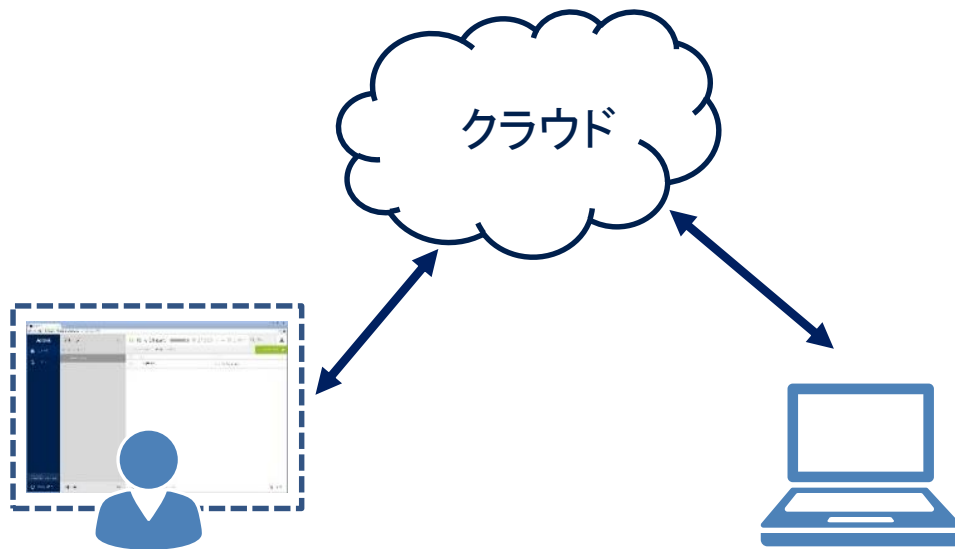
クラウドベースのバックアップ管理

- クラウドからのコンソール操作の提供
- クラウド経由の運用管理

オンプレ



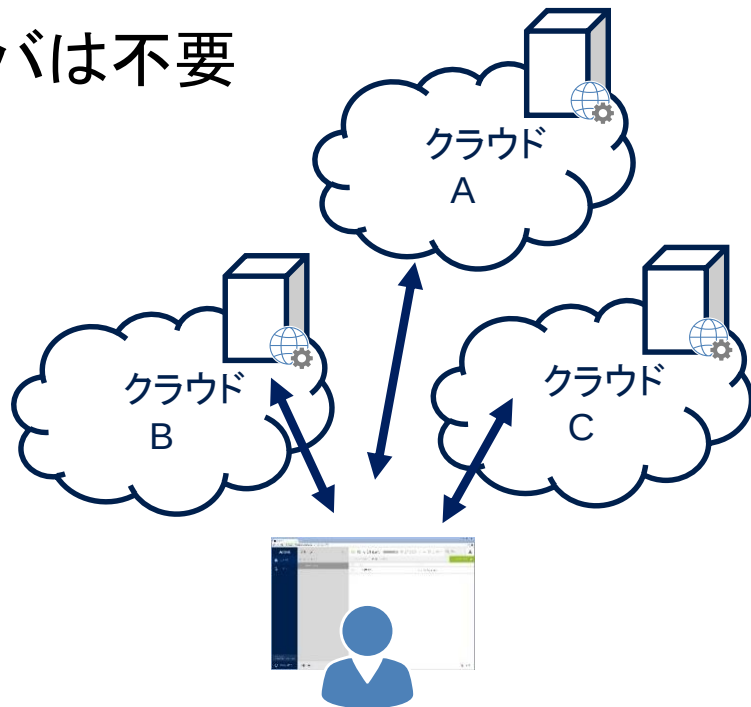
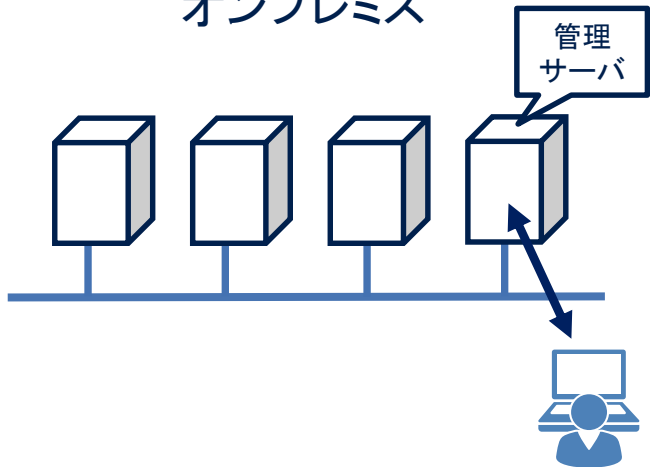
クラウド



マルチクラウド

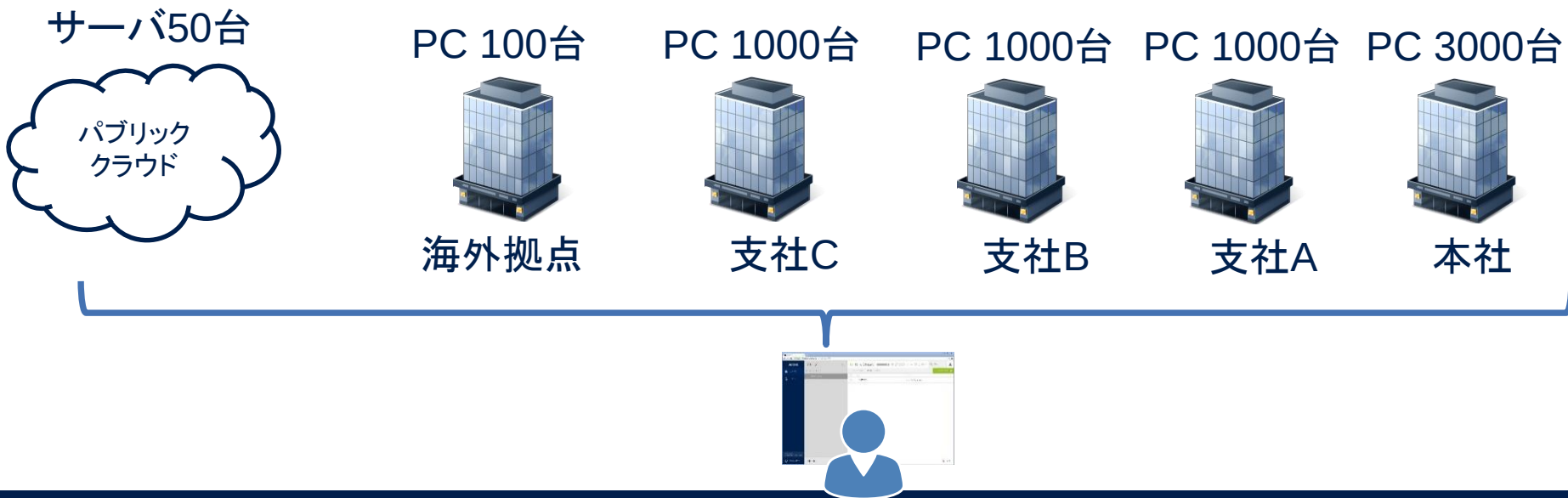
- 異なるクラウド間で一元的管理
- オンプレミスで鉄板だった管理サーバは不要

オンプレミス



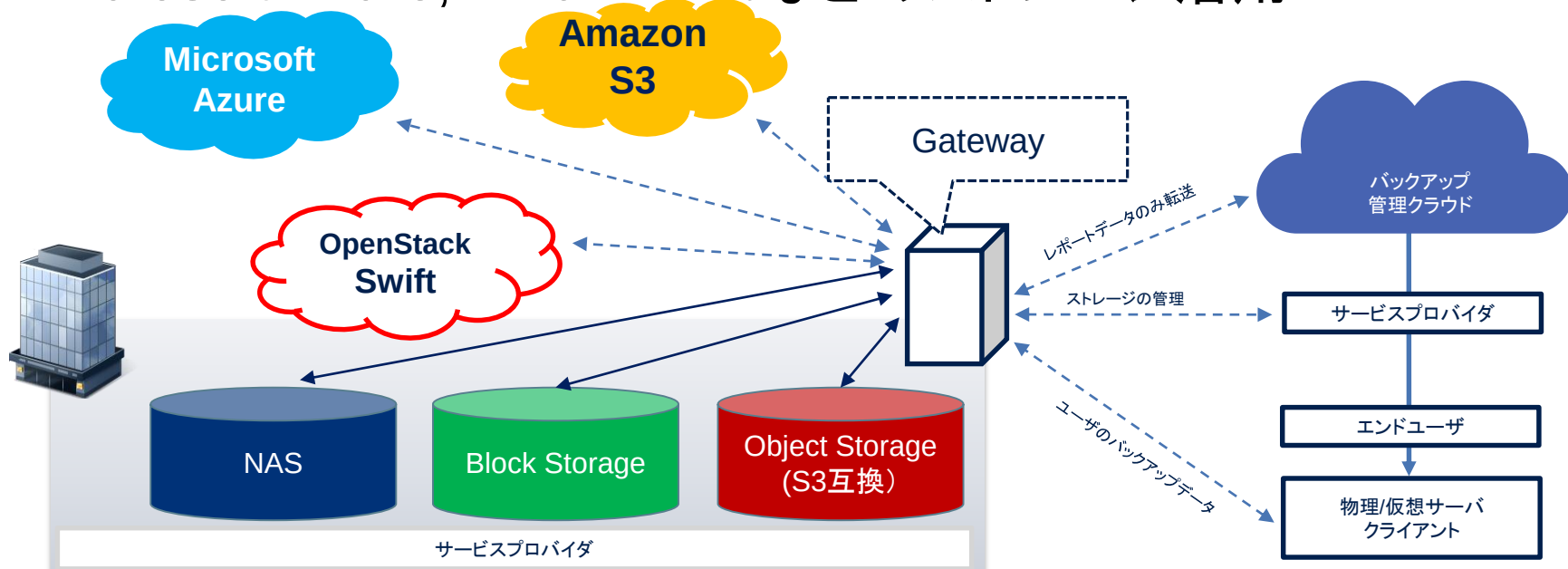
スケールアウト

- 管理台数の制約なし
- インフラ設計、投資不要のオンデマンドなスケールアウト



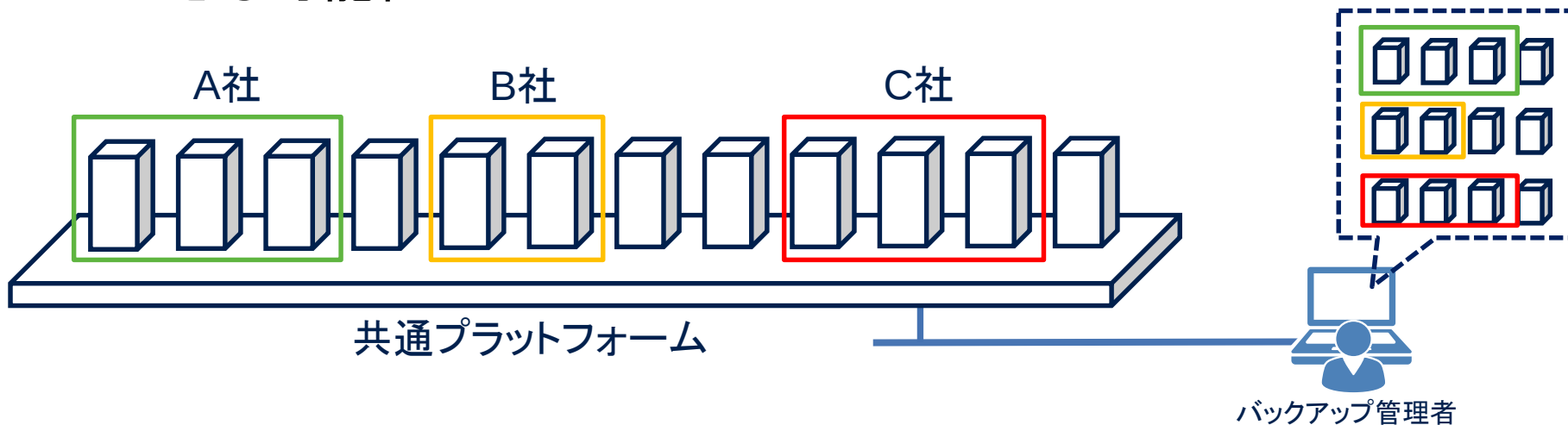
各種ストレージの活用

- 様々なストレージをクラウドに接続
- Microsoft Azure, Amazon S3などのストレージ活用



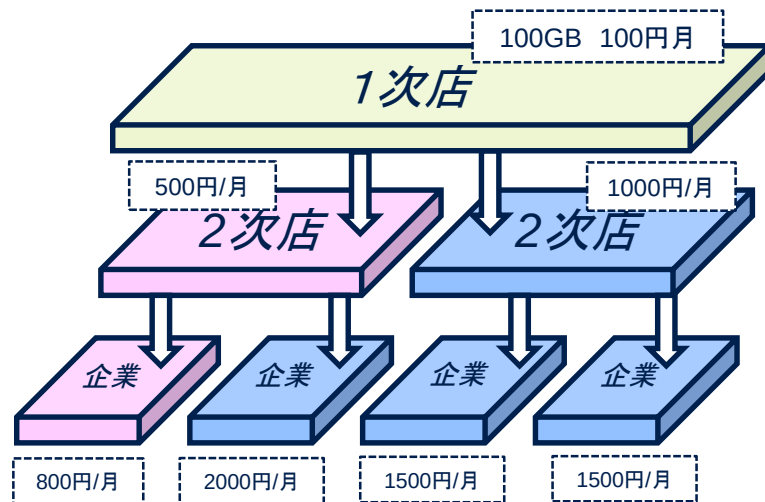
マルチテナント

- クラウド基盤上に複数の企業が相乗り
- バックアップ管理者がすべてのバックアップにアクセスできる可能性



マルチティア

- 商流に応じた階層構造のデザイン、請求情報生成
- 単価、台数、容量パラメータの設定、台数、容量制限



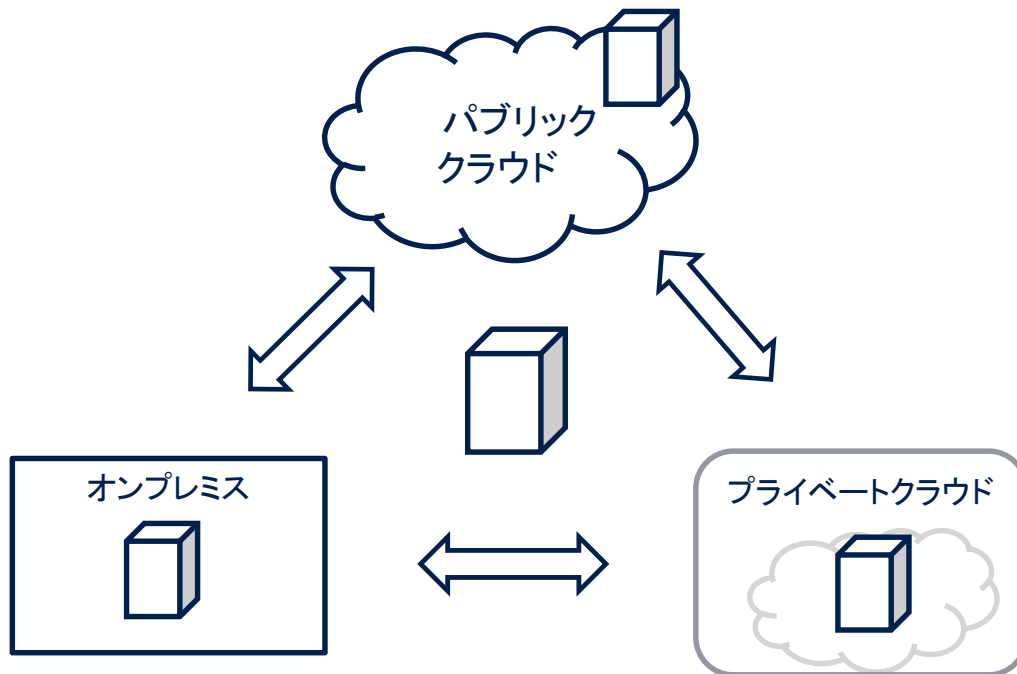
リモートからのシステム復元が可能

- クラウドベースのコンソールからシステム全体の復元可能
- レスキューメディア不要、異なる環境へも復元可能



マイグレーション

- P2C、V2Cなど環境に依存しないマイグレーション

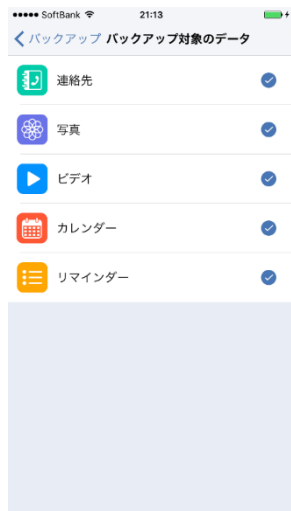


DR/BCP

- 利用方法: DR対策として2次バックアップ、BCP対策としてクラウドへ復元を実施する
- メリット: バックアップ+DR/BCPの付加価値のあるクラウドサービスを実現する

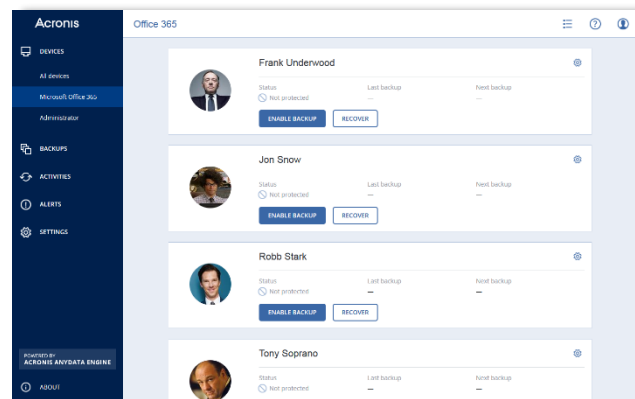


モバイルデバイスバックアップ



クラウドサービスのバックアップ

- メールボックスのバックアップと復元
- ローカルへのバックアップも可能



エージェントの一括リモートアップデート

- ロケーションに依存せず一括でリモートからアップデートが可能（再起動不要）

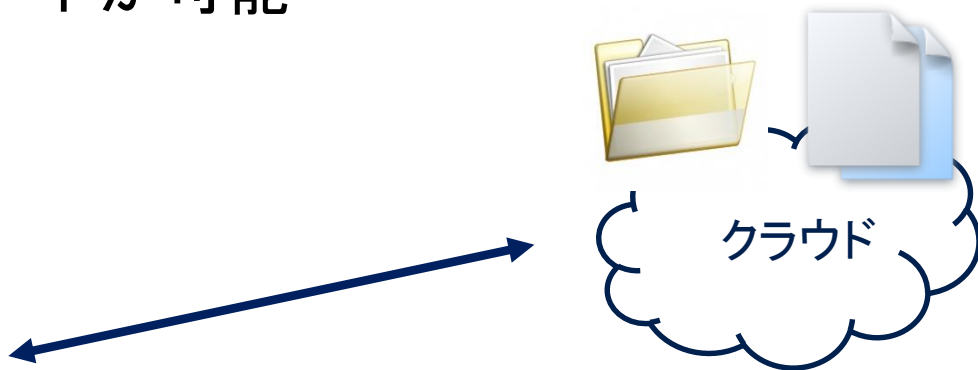
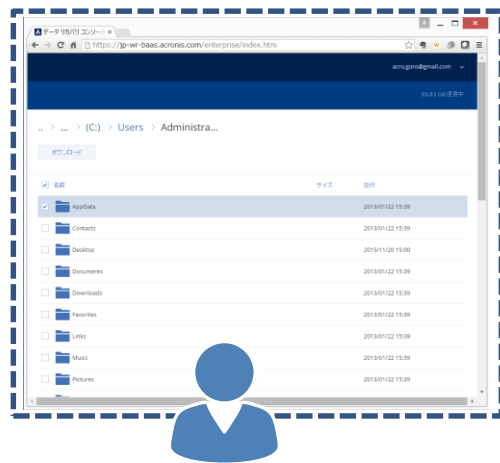
チェックボックスで一括選択が可能

ホスト名	インストールされているエージェント	エージェントのバージョン
ABC-B-WIN2K8-1		12.0 1588 ⚠
Azure-WIN2012-1		12.0 1299 ⚠
Hyperv-W2012-2		12.0 1299 ⚠
Hyperv-W2012-3		12.0 1299 ⚠
ONPRE-RHEL64-1		12.0 1299 ⚠
ONPRE-WIN2K8-2		12.0 1299 ⚠
vCloudAir-WIN2012-1		12.0 1299 ⚠

現在のバージョン、アップデートの必要性確認可能

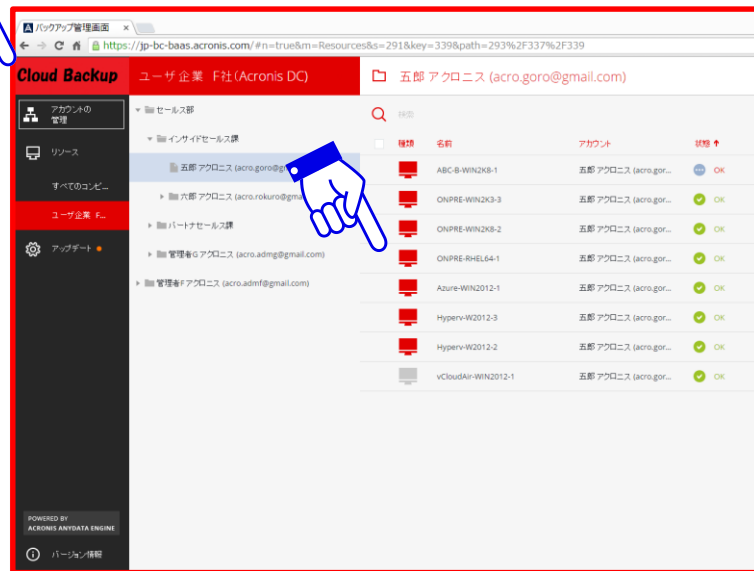
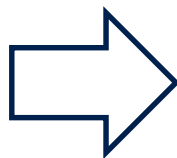
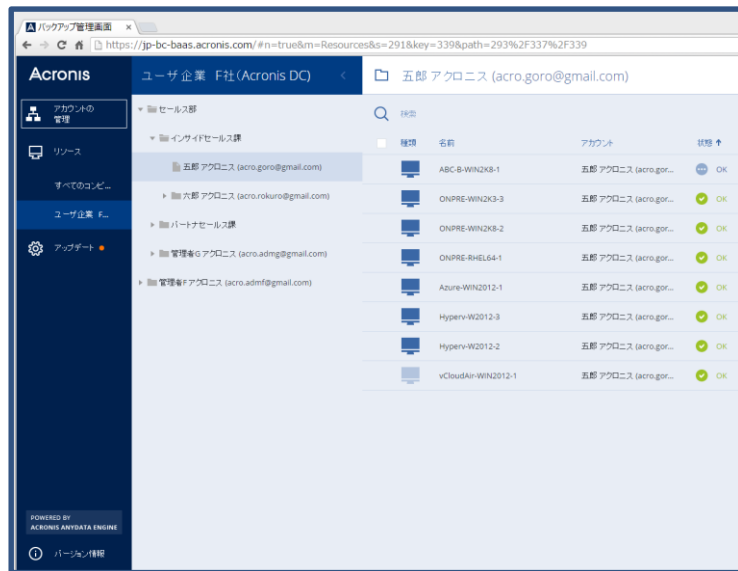
クラウドデータリカバリコンソール

- ロケーション、マシンに依存しないデータの取り出し
- イメージバックアップアーカイブ内の任意のファイル・フォルダ参照とダウンロードが可能



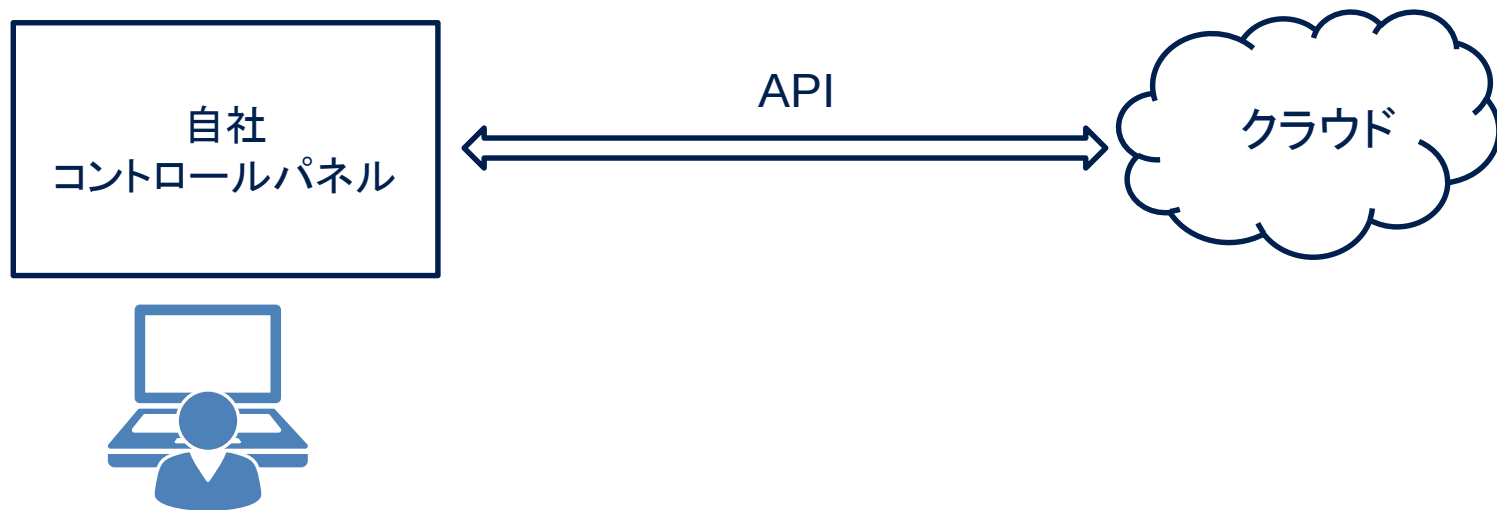
ホワイトレーベル化

- イメージカラー、ロゴの変更が可能



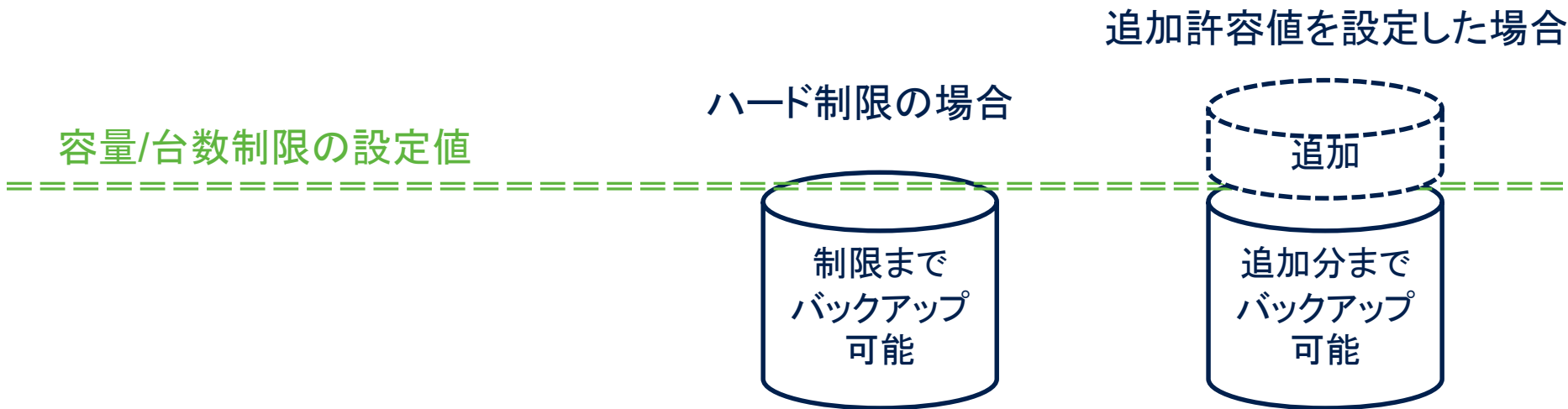
APIによる既存環境への統合

- APIによる外部からのコントロール



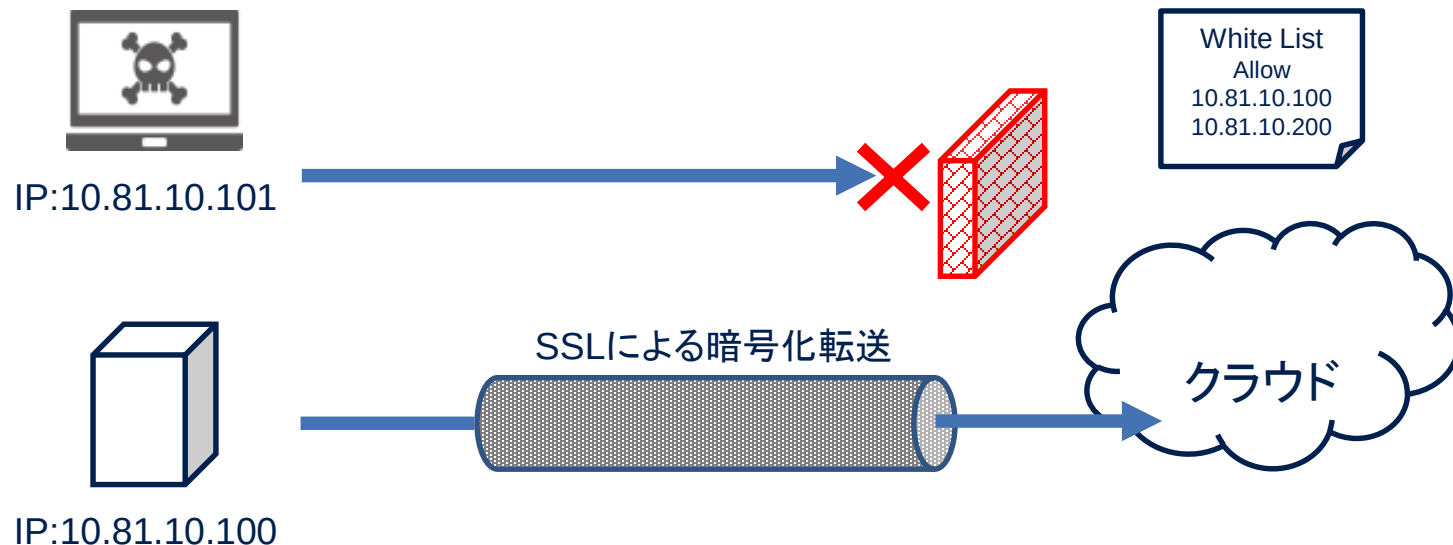
容量/台数の柔軟な制限値設定

- 容量/台数の制限が可能
- ハード制限/追加許容値の設定が可能
- 制限を超えた場合の自動通知



ログオンコントロール

- アクセスするIPをホワイトリストにより制限することが可能



主要なサービス

Feature	MozyPro	CrashPlan	Asigra	Carbonite
File backup	●	●	●	●
Image backup				
NAS backup	●		●	●
Office 365			●	●
Agent-less backup of virtual machines			●	?
Backup to vendor cloud	●	●		●
Backup to storage on SP premises		●	●	
Backup to a public cloud (Azure,Amazon S3 etc.)				
Application granular backup	●		●	●
Initial seeding	●			
Bare Metal Recovery (BMR)			△	
BMR to dissimilar hardware			△	
Web-restore	●			
File search	●		●	△
Portal branding	●			
Agent branding	●	●		
Emails branding (customization)		●		
Usage reporting	△	△	△	△
Vendor hosted	●	●		●
Storage on SP premises (Hybrid)		●	●	
Full on-premise deployment		●	●	
Form factor	Software	Software	Appliance/Software	Appliance/Software
Partner management	●	●		
RPO (Min schedule)	not defined	15min	CDP	1day
Soft quotas				
Hard quotas	●	●		●
vSphere (agentless)			●	
Hyper-V (agentless)	△		●	●

Acronis

New Generation Data Protection

Powered by the Acronis **AnyData** Engine

www.acronis.com



twitter.com/Acronis_Japan



blog.acronis.co.jp



facebook.com/acronisjapan