

脱PPAP

パスワード付き ZIP ファイルのメール添付

代替案とは？

株式会社ムービット

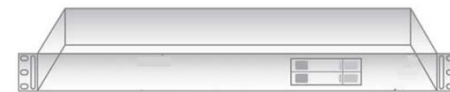
会社概要

社名 株式会社ムービット

設立 1995年12月8日

所在地 東京都北区王子1-28-6

主な製品 Powered BLUE シリーズ
アプライアンスサーバー (Linux)
ソフトウェア開発



ダークWeb



サイバークラッシュの
開市場が拡大して、
身代金目的の暗黒市のデ
ータを暗号化する「ランサ
ムウェア」、標的とする組
織に不正アクセスを強要
し、権利などが売り出られ、
騒がれた「技術を生み出
ていく」商標など、出て
も「武器」の調子が可
能ならば、攻撃者も視野
拡大が懸念されている。
「最も安い検出不能ラン
サムウェア。1カ月
で200万^円、6日で14万
9000^円、12月で900
0^円」¹

サブスク利用も
キヤノンマーケティング
ジャパンが誰にでもラン
サムウェアの販売サイ
トでは、サブスクリプ
ション（定期契約）の利
用が設けられ、最も
高額のプランでは、最も
容易にする追加機能も付
くランサムウェアは今年
だけで既に3回パシ

販売が確認されたサイバー攻撃用のサービスやツール	
医療系大学へのアクセス権	999%
米有力企業へのアクセス権	1万%
ATM用のマルウェア	2000% ～
ランサムウェアのサービス	年間 900%
スパムSMSの送信サービス	25～ 500%
SMS送信用のソフトウェア	499% ～

(出所)トレンドマイクロ

医療系大学へのアクセス権	999 ^円 /年
米有力企業へのアクセス権	1万 ^円 /年
ATM用のマルウェア	2000 ^円 /年 ～
ランサムウェアのサービス	年間 900 ^円 /年
スパムSMSの送信サービス	25～ 500 ^円 /年
SMS送信用のソフトウェア	499 ^円 /年 ～

(出所)トレンドマイクロ

[illegible]

ロシアのウィルヘルム・ドストエフスキの『罪と罰』に「ドクトラ・ラッセル」の博士・シロフ最高経営責任者（CEO）は「死手」が「戦い合うこと」をルウェーなどの攻撃力がなくなる構図になっていると指摘する。ランサウアーで暗号化されたデータの復旧サービスでも「数年前にバー、データを復元できないケースが増えて」いる。（柏木説）

「アックサツされ、使いたるにやある質問」に答へる形で説明、検出を免れるられるウィルス対策ソフトの二覧も掲載されている。同社の西森寛一、セキユリディエバンジリストは「セルスポイントや使い方を丁寧に示する様は一般的なソフトウェアやアプリの悪質なサイトと変わらない」と話す。

群「ダークウェブ」では匿名性の高い闇サイト「ジャクウェーブ」で以前から、流出したクレジットカード情報やSNS（交流サイト）アカウトの書き込みもあった。

セキユリティに関係するところで、国内の強固なネットワークの岡本勝之キムによる「国内の安全が明らかになった疑いが明らかに」なる。これは、V.P.N.（仮想）私網の利用情報について、有料の会員制サービス内でやり取りされていた。サイバー攻撃を仕掛けるマルウェア販売や代行サービスをCaaS（クラウド・サービス・アサイス）とも呼ばれるCaaSを利用することで「高度は技術や専門知識がなくとも攻撃を実行できるものになった」といふ。

機能の劣るマルウェアは市場で淘汰され、攻撃が成功しやすい（低価格）になる。

マルウェアの販売は「匿名内では不正指合電帳簿の記録提供の罪に及ぶ」。だが、「不正なプログラムと見られるかどうかは実質的に使用者によって初めて確定される」と警察関係者は話す。被害が発生した場合も、被害者側はマルウェアの提供者を生かして「闇市場の取引に歯止めをかけるのは難しい」といふ。

「止む難しき」という。

■「ランサムウェア」月120ドルから

真相深層

ランサムウェアのサービス
900ドル

パスワード流出チェックサイト

https://haveibeenpwned.com/



①



password

pwned?

②



Pwned Passwords

Pwned Passwords are 551,509,767 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online system. [Read more about how HIBP protects the privacy of searched passwords.](#)



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

Password reuse and credential stuffing

Password reuse is normal. It's extremely risky, but it's so common because it's easy and people aren't aware of the potential impact. Attacks such as [credential stuffing](#) take advantage of reused credentials by automating login attempts against systems using known emails and password pairs.

NIST's guidance: check passwords against those obtained from previous data breaches

The Pwned Passwords service was created in August 2017 after NIST released guidance specifically recommending that user-provided passwords be checked against existing data breaches. The rationale for this advice and suggestions for how applications may leverage this data is described in detail in the blog post titled [Introducing 306 Million Freely Downloadable Pwned Passwords](#). In February 2018, version 2 of the service was released with more than half a billion passwords, each now also with a count of how many times they'd

- ① パスワードを入力
- ② pwned? を押す

Oh no --- pwned !

残念でした

Good news — no pwnage found!

大丈夫

PPAPとは ？

P assword 付きzip暗号化ファイルを送ります

P assword を送ります

A ん号化

P rotocol

命名 大泰司 章 おおたいし あきら

パスワード付き～ZIP暗号化 平井 デジタル大臣



日立製作所 秘文でのZIP暗号化 禁止



PPAPのメリット

- ZIP 盗聴防止
パスワードも、同一経路の場合には効果半減
- 複数ファイルの1ファイル化
- 誤送信対策
パスワードの遅延配送 & 送信キャンセル
- Pマーク対策
個人情報保護
- ISO27001 (ISMS認証)
情報管理

PPAPのデメリット

- ウイルスチェックができない
Emotetなどの
攻撃者のパスワードZipの悪用
- 業務の遅延
パスワードの遅延配送のためすぐに
受信ファイルが展開できない

パスワードが来ません….
- ZIPファイルを受信しない企業など
クラウド会計ソフトを提供するfreee
(2020・12から実施)

海外企業

■ PPAPの廃止は困る

どうやってファイルを送るか

現在の業務ルーチンを変更したくない

■ 社内の情報管理

■ Pマーク対策

■ ISO27001（ISMS認証）

対策－1 現状のルティーンはなるべく踏襲

■ ZIPパスワード

●2経路で送信

ZIPパスワードはSMS送信

口頭やFAXでZIPのパスワード通知

●固定パスワード

相手先ごとに固定パスワード

パスワードは都度、通知はしない

ZIPファイル拒否・外部ストレージ禁止の相手先

返信 全員に返信 転送 アーカイブ 迷惑マークを付ける 削除 その他

差出人 サポートチーム ★

件名 Re: カタログお待ちしております 10:09

宛先 mubit.co.jp ★

Cc mubit.co.jp ★

株式会社ムービット
〇〇〇 様

お世話になっております。
〇〇〇 サポートチームでございます。

弊社 〇〇 宛てにご連絡をいただき誠にありがとうございます。

誠に恐れ入りますが、
弊社のセキュリティの都合上 パスワード付きZIPファイル・外部ストレージでの
ファイルのお受け取りができかねるため、

パスワード設定なしの状態での再送付か、
もしくは 下記専用ストレージサーバーへカタログをアップロードをお願い申し上げます。

https://upload.〇〇〇〇.com/ui/_〇〇〇/guest/b2thbml3YS15QGJwcm9zLmpwIjE2MTM0Mzc3MzUgMTYxNDY0NzZmNQ%3D%3D

対策－2 共有ディスク

■ Webダウンロード方式

添付ファイルを共有ディスクに保存

受信者に添付ファイルをダウンロードさせる

■ 共有ディスクの運用先

1) クラウド 2) SaaS 3) 自社管轄下での運用

■ 共有ディスクへのアクセス

ユーザー認証

A) 添付ファイル処理機能



【1】共有ディスク機能

メール添付ファイルのWebダウンロード機能
ダウンロード時のWeb認証

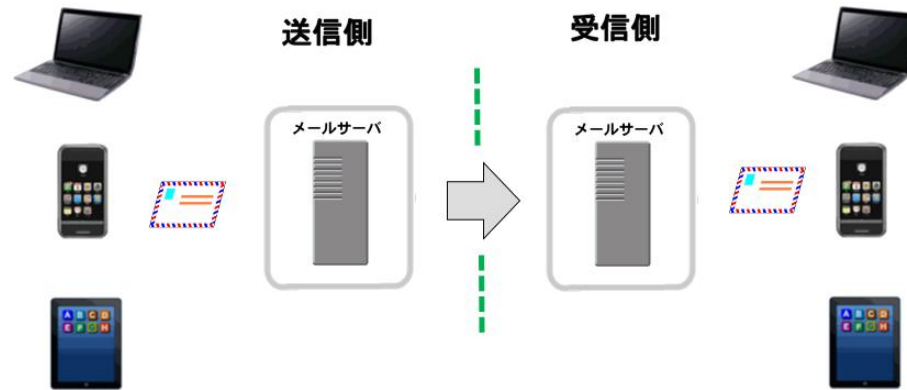
【2】ZIP暗号化機能

B) 大容量ファイル送受信機能

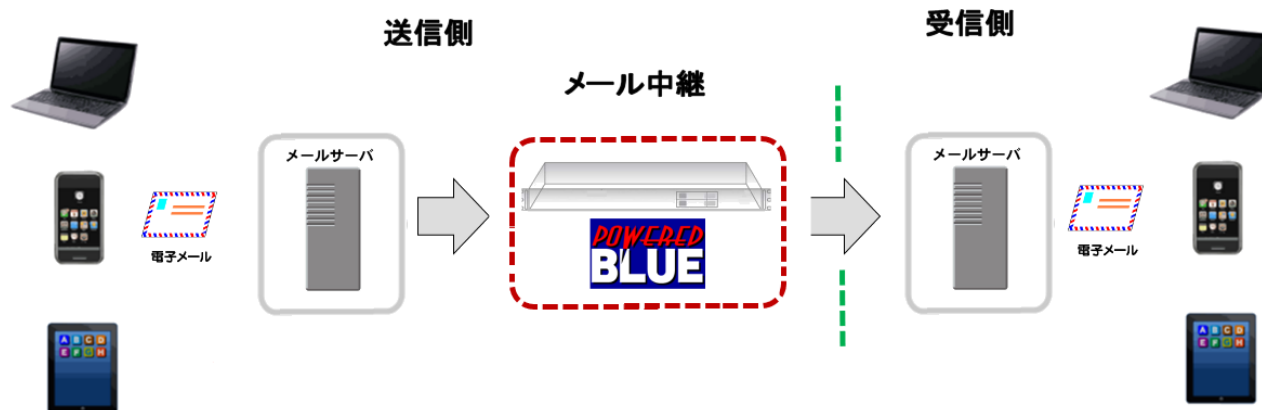
双方向での大容量ファイル送受信
アカウント無しでも認証に対応

設置構成-1

■ 現状



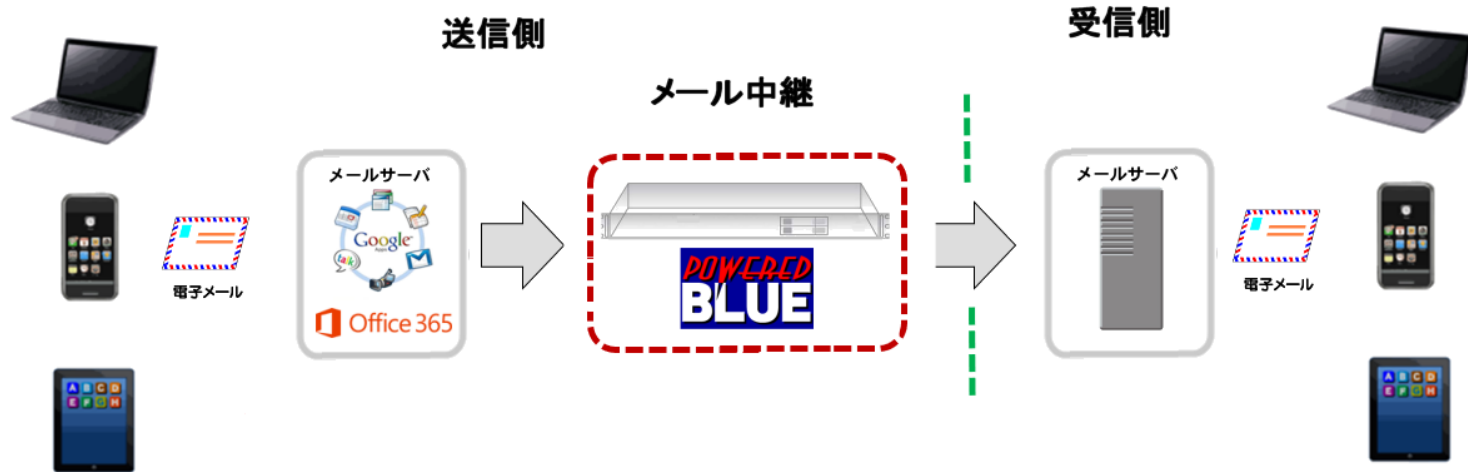
■ Powered BLUE MailPlus アプライアンス



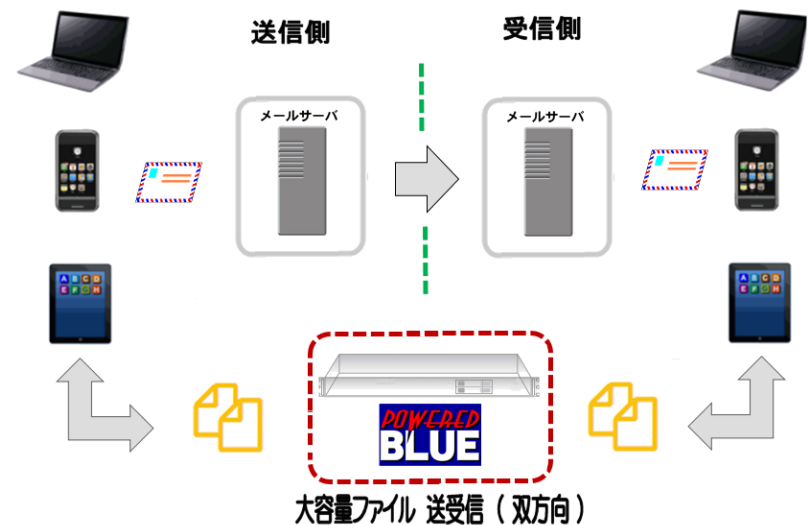
共有ディスク機能 & 大容量ファイル送受信機能

設置構成-2

Gsuite / Office 365との連携



メールは既存環境を利用



大容量ファイル送受信機能

運用時の動作やWeb認証

■ 添付ファイルのダウンロード

送信者は従来同様、メールを送信操作

URLの自動通知 キャンセル操作に対応



Webダウンロード時の認証

- 1) 認証なし (アカウント不要)
- 2) Basic 認証
- 3) SSLクライアント認証 (アカウント不要)
- 4) ワンタイムパスワード認証
- 5) AD認証
- 6) SAML認証 (idP)

■ 大容量ファイル送受信

送信者は従来同様、メールを送信操作

対策-3 自社に共有ディスクがある場合

- NAS Webベースでの動作に対応
共有フォルダー



認証が脆弱

ID / パスワード

リバースプロキシ経由でアクセス

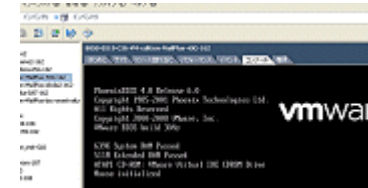
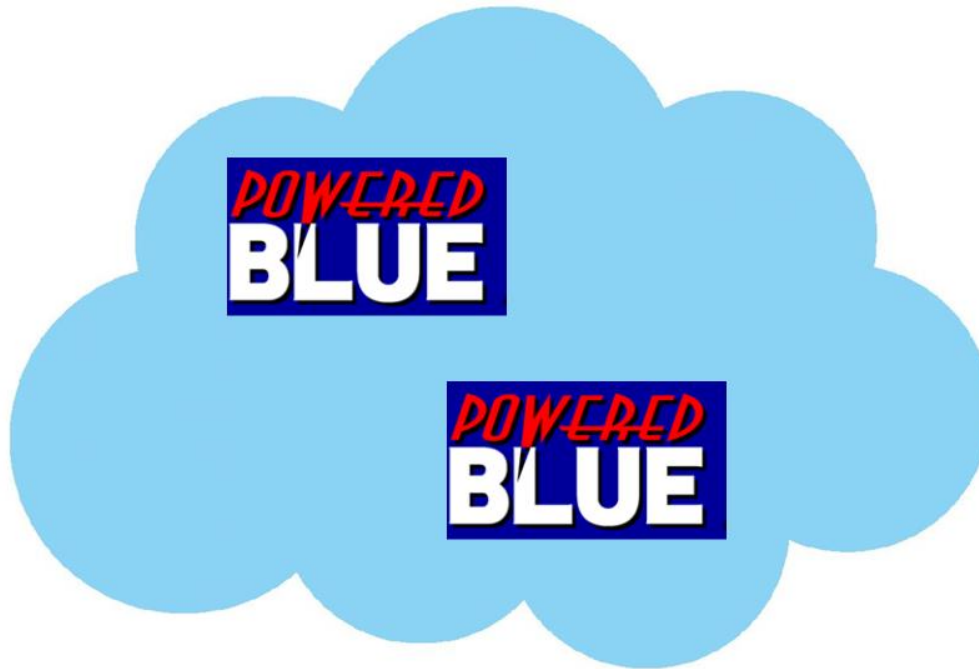
■ 認証対応のリバース・プロキシ



Powered BLUE Reverse-Proxy

SSLクライアント認証・OTP認証・AD認証・SAML認証

アプライアンスでの提供・動作環境



■ 自社管理で運用できるアプライアンス

■ ZIPを利用の場合

2経路でのパスワード通知
固定パスワード

■ 共有ディスク その1

添付ファイル自動ストリップ
Web認証
大容量ファイル送受信



➡ <https://www.mubit.co.jp/sub/products/mp/pb-mailplus-cloud.html>

■ 共有ディスク その2

NAS + 認証対応リバースプロキシ



➡ <https://www.mubit.co.jp/sub/products/cloud/pb-auth-rev-cloud.html>