



## AI 搭載のマルウェア対策ソフトウェアで 全国約 800 台の PC セキュリティを守る

婚活サービス業界 No.1 の成婚率を誇るパートナーエージェントは、未知のマルウェアに対する防御を強化すべく、パターンファイルに頼らない次世代セキュリティ製品「Dell Data Protection | Threat Defense」を導入した。



PARTNER AGENT

サービス業

日本

### ビジネス課題

婚活サービスを提供しているパートナーエージェントにとって会員データの保護は最重要・最優先のビジネス課題である。会員データの漏えいを抑止する確実な管理体制が必要であるが、昨今の高度に偽装されたランサムウェアなどによる攻撃に対しては、パターンファイルベースの従来型アンチマルウェアソフトでは防御が難しい状況となってきた。

### ソリューション

- クライアントソリューション
  - Dell Data Protection | Threat Defense
  - Dell ProSupport Plus

### 導入効果

- Dell Data Protection | Threat Defense を導入してから半年以上にわたる実績として、マルウェアの侵入を 100% 防御
- すべての PC の問い合わせ窓口をデル・プロサポートプラスに一元化し、トラブル発生時の問題解決を迅速化
- 導入を検討した従来型マルウェア対策ソフトの場合には、移行作業に 2～3 カ月が必要であったが、Dell Data Protection | Threat Defense では 1 週間で全 PC への導入が完了。

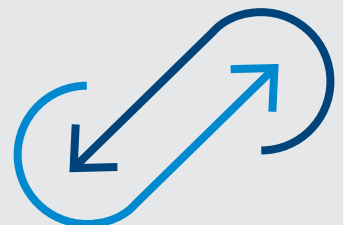
防御率 **100%**

導入してから半年にわたる実績としてマルウェアの侵入をすべて防御



**1/8** 短縮

従来製品では 2 カ月以上かかると思われた移行作業を 1 週間で完了



成婚というゴールに向けて伴走する専任コンシェルジュの存在、豊富な実績データを基にした婚活設計など、「高い成婚率の実現」を婚活サービス企業としての価値と考えるパートナーエージェントにとって、絶対に守らなければならないのが会員データだ。外部から完全に隔離された仮想化環境で厳重な管理を行っているが、一方で懸念されたのが全国各地の店舗で運用している約 800 台の PC である。世の中では標的型攻撃やランサムウェアによる被害が拡大しており、パターンファイルを利用した従来型のマルウェア対策ソフトウェアによる対策はもはや限界と考えられた。

そうした中でデルより提案されたのが、機械学習をベースとした AI を用いた検知手法で未知のマルウェアも防御する Dell Data Protection | Threat Defense (以下、DDP | TD) である。既存のマルウェア対策ソフトウェアからの切り替え時に「空白期間」を生じさせないスムーズかつ短期間の移行をサポートし、これまでの実績として 100%の精度でマルウェアの侵入を防御している。

## 「成婚率」にこだわった 新世代の婚活サービスを提供

結婚は人生の大きなイベントだが、現代社会は結婚しにくい時代と言われている。実際、総務省統計局の調査によると、1970 年をピークに婚姻件数は減少し続けている状況だ。一方で国立社会保障・人口問題研究所が行ったアンケート調査では、独身者の約 90%が「いずれ結婚するつもり」と回答している。要するに結婚したいという望みを持ちながらも、「この人だ」と思えるパートナーとなかなか出会えないという問題が現代社会に顕在化してきている。

そうした中、「プロフェッショナルとしてゴールまで伴走するエージェント（代理人）がいたら状況は大きく変わるはず」という思いを持って、2006 年に創立したのがパートナーエージェントである。もっとも、いわゆる婚活サービスを手がける企業はこれまでも数多くあった。それらの既存の婚活サービスとパートナーエージェントはどこが違うのだろうか。これまでほとんどの婚活サービスは、自社が擁する会員数の多さをアピールしてきた。しかし結婚は、希望条件を満たす人をできるだけ多くの母数から探し出し、マッチングすれば実現するというような単純なものではない。一方で、パートナーエージェントは一貫して「成婚率」にこだわり、その向上こそ企業の真の価値として位置づけ、その実績を数字で公開しているのである。

創立以来 10 年以上にわたって蓄積してきた会員の豊富な実績データを分析・解析し、エリア・年齢別の出会いの人数、交際に至る人数、成婚までの期間などを具体的な数値として抽出。これに個別インタビューから得られた情報を重ねあわせることで、その人だけの活動設計を行っているという。

## マルウェアをエンドポイントで 検知するケースが増加

婚活サービスを展開していくうえで、大前提の条件となるのが厳重なセキュリティ対策である。パートナーエージェントが保持するさまざまな会員データは究極の個人情報といっても過言ではなく、絶対に外部に漏えいさせることがあってはならない。

そこでパートナーエージェントでは、Dell EMC PowerEdge サーバなどをホストサーバとして活用し、会員データを外部から完全に隔離された仮想化環境で管理することで安全性を担保している。ただ、懸念されたのは全国各地の店舗でコンシェルジュが利用しているトータル数百台に及ぶ PC のセキュリティだ。同社の情報システム部長のカイン・ミン・スウィ氏は次のように語る。

「会員の皆様をサポートする業務の性質上、それらの PC をインターネットから切り離すことはできません。万が一、不正侵入されたとしても PC のローカルディスクに会員データは一切保存されていないため情報漏えいなどの問題は起こりませんが、とはいえ近年では標的型攻撃やランサムウェア（身代金要求型ウイルス）など、巧妙化する新手のマルウェアをエンドポイントで検知するケースも増えており、安心できる状態ではありません」

一方でパートナーエージェントが直面していたのが、これまで各 PC 上で利用してきたマルウェア対策ソフトウェアのライセンス切れという問題である。これまで利用してきたマルウェア対策ソフトウェアをそのライセンス期

「パターンファイルによるマルウェア対策を  
今後も続けることに疑問を感じる中、  
Dell Data Protection | Threat Defense は  
私たちにとって、まさに待ち望んでいた  
ソリューションでした」

株式会社パートナーエージェント  
情報システム部長  
カイン ミン スウィ 氏

限までに Windows 10 に対応した新しいシステムに切り替えるという課題があった。同社の情報システム部の伊藤聡重氏は次のように話す。

「従来製品のライセンスの期限が迫っており、しかも Windows 10 に対応させるためには後継製品にアップグレードする必要があったのですが、その作業は全国各地の店舗に分散している約 800 台の PC に対して行わなければならない。しかも旧バージョンの製品をいったんアンインストールして再起動した後、あらためて後継製品をインストールするという手順を踏む必要があり、その「空白期間」にサイバー攻撃を受けた場合に無防備になって



「新製品への移行は1週間という短期間で完了しました。もし従来製品の後継版を採用していたら、全国各地の店舗にスタッフが出向かなければならず移行作業に2～3カ月はかかったかもしれません」

株式会社パートナーエージェント  
情報システム部  
伊藤 聡重 氏



しまうリスクもありました」

作業は新旧製品を同時に動作させることができないため、旧製品のアンインストール後に、新製品をインストールする必要がある。この際、セキュリティ上、セキュリティソフトが存在しない空白期間を極力なくすという対応が求められたのである。

## マルウェアの構造や振る舞いから特徴的な「悪意」を瞬時に分析

上述のような背景から2016年6月、パートナーエージェントはPCのセキュリティを強化する新たなソリューションの検討に入った。まさにそのタイミングでデルから紹介されたのが、DDP | TDである。

「どちらかといえばハードウェアベンダーという印象を持っていたデルからの斬新な提案に驚きました」とミン氏は振り返る。どんな点が画期的だったのだろうか。

現在の一般的なマルウェア対策ソフトウェアは、マルウェアの定義（シグネチャ）を利用したパターンマッチングにより検知する。昨今の膨大な量のマルウェアによりシグネチャの作成が追いつかなくなってきており、シグネチャベースの対策は技術的に限界を迎えている。

ある調査によると、2015年に全世界で確認された新種マルウェア（亜種を含む）は約4億3100万種類に上っており、1日あたり118万近い新種が出現していることになる。この膨大なマルウェアを解析してデータベース化するスピードが追いつかなくなってきているのだ。そして当然ながら、このタイプのマルウェア対策ソフトウェアは未知のマルウェアにまったく歯が立たない。

これに対してDDP | TDは機械学習をベースとしたAI（人工知能）を活用したATP（高度脅威防御）機能を搭載し、既知のマルウェアを検知するパターンマッチングではなく、AIエージェントによりマルウェアのプログラム構造を静的に解析し、検知する。これにより既知のマルウェアはもとより未知のマルウェアに対しても99%の検知能力を発揮し、実行を事前に阻止することができるのだ。加えて分析処理も極めて低いCPU使用率（通常3～5%）で軽快に動作するため、エンドユーザの業務を妨げることはない。

「当社としてもパターンファイルによるマルウェア対策を今後も続けることに大きな疑問を感じ始めていました。将来に対する安心・安全を確保できる手段を探していた私たちにとって、DDP | TDはまさに待ち望んでいたソリューションでした」と、ミン氏は導入を決定した背景を語る。

## 従来型のマルウェア対策ソフトウェアと共存させたインストールも可能

パートナーエージェントがDDP | TDを高く評価したもう1つのポイントが、そのスムーズな移行手順である。

パターンファイルを利用する一般的なマルウェア対策ソフトウェアはWindowsの特殊なAPIを利用するため、2つの製品を同居させることができない。先に述べた「旧製品のアンインストール、再起動、後継製品のインストール」という面倒な手順を踏まなければならなかったのはこのためだ。



その点、異なるアーキテクチャで作られた DDP | TD ならば、従来型のマルウェア対策ソフトウェアと同居させたとしてもまったく問題はない。DDP | TD をインストールして正常に動作していることを確認した後、ライセンス切れなどの任意のタイミングで旧製品をアンインストールすればいい。これによりセキュリティの“空白期間”が生じるのを避けることができる。

さらに DDP | TD はサイレントインストールもサポートしており、全国各地の店舗に分散する PC に対してリモートからバックグラウンドでインストールを実行することができる。実際、この機能は移行に際して絶大な効果を発揮したようだ。仮に既存のマルウェア対策ソフトウェアの後継製品を選択していた場合、まず環境構築およびホワイトリスト設定などの準備作業に1週間程度を要する。繰り返しになるが、そのうえで「旧製品のアンインストール、再起動、後継製品のインストール」という作業を数百台の PC に対して個別に実施しなければならないのだ。

「運用ポリシーでエンドユーザがソフトウェアのインストールを行うことは許可しておらず、この作業は情報システム部のスタッフが各地の店舗に出向いて実施する必要があります。こうしたことからすべての PC の移行を完了するまでは、2～3カ月を費やしたかもしれません」と伊藤氏は語る。

一方、DDP | TD は、クラウド環境から提供するサービスであるためサーバ設定などの準備作業は不要だ。「各 PC へのインストールもスタートアップスクリプトを使ってコマンドを実行するという方法をとったことで、短時間で作業を実施することができ、1週間後にはすべての PC の移行を完了しました」と伊藤氏は語る。

なお話は前後するが、パートナーエージェントでは数年前からライフサイクルに応じて段階的に各店舗の PC を、Dell Latitude や Dell OptiPlex を中心としたデル製品へとリプレースを進めてきた。これによるエンドユーザ環境の統一も、今回の DDP | TD のスムーズな移行に貢献したようだ。

「それ以前はさまざまなベンダーの製品が混在した環境で、PC ごとに問い合わせ窓口が違えば、サポート内容も異なっているという状況でした。仮にその環境下でセキュリティ対策の移行を行っていた場合、エラーが発生した際の対処にもかなりの混乱が生じていたと予想されます。シンプルなデザインや堅牢性が気に入って新しく導入する PC はすべてデル製品にすると基本方針のもと、問い合わせ窓口も Dell ProSupport Plus に一元化された体制だったからこそ、私たちは安心して DDP | TD への移行に踏み切ることができました」と伊藤氏は語る。

## マルウェアの侵入を完全に防御し エンドユーザにも快適な操作を提供

2016年9月に全社的な運用を開始して以来、DDP | TD はパートナーエージェントの PC に高い安心・安全を提供している。これについてミン氏は、「導入からすでに半年以上が経ちましたが、現在までセキュリティインシデントはまったく起こっておらず、マルウェアの侵入は完全に防御されています。エンドユーザからも PC が遅くなったといったクレームは入っていません。こうした当たり前のことを着実に実現してくれたことが、DDP | TD の最大の成果と考えています」と評価する。

もっとも、セキュリティ対策にここまでやれば安心といったゴールはなく、今後も悪質化・巧妙化の一途をたどるサイバー攻撃の動向やビジネスの変化を見据えながら、タイムリーな施策を打っていく必要がある。

パートナーエージェントでは、会員の成婚率をより一層高めるべく、今後新しいサービスの展開を見据えている。そうした中でも依然とセキュリティの重要性は変わらず、これまでとは観点の違った対策が求められることになるだろう。ミン氏は、「デルには今後も単なるハードウェアベンダーとしてではなく、私たちのビジネスのパートナーとしての立ち位置から、より広範かつ効果的なソリューションを提案していただけたらと思います」と語り、デルのさらなるサポートに期待を寄せている。

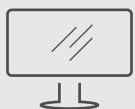


株式会社パートナーエージェント  
情報システム部長  
カイン ミンスウイ 氏



株式会社パートナーエージェント  
情報システム部  
伊藤 聡重 氏

ユーザ導入事例ウェブサイトにて、他にも多くの事例をご覧ください。 [www.dell.co.jp/casestudy](http://www.dell.co.jp/casestudy)



Dell EMC の  
ワークステーションの  
詳細は [こちらから](#)



専門スタッフへの  
お問い合わせ



お客様導入事例の一覧は  
[こちらから](#)



この記事を共有する

