CrowdStrike 導入事例

CROWDSTRIKE

# 株式会社竹中工務店様

偽装ウイルス見抜けず、水際対策の限界を痛感
国内外20,000台のPCを守る方法とは

## 偽装ウイルス見抜けず、水際対策の限界を痛感

竹中工務店グループは国内外で事業を展開する大手建設会社として、以前から真摯（しんし）な姿勢でセキュリティ対策に取り組んできた。

しかし、同社が「水際のウイルス対策だけでは防ぎきれない」と認識し始めたのは2016~2017年ごろだ。偽装ウイルスを用いた診断サービスでテストを実施したところ、当時のセキュリティ体制では見逃したという。これを契機に、同社は、侵入を前提にした検知への注力と侵入後の対応の体制を整え、被害を最小化する対策を検討することにした。候補として挙がったのは、エンドポイント系とネットワーク系のセキュリティ製品・サービスだが、同社は前者を選択した。

そして2018年からエンドポイントで侵入を検知し、脅威に対応するためのEndpoint Detection and Response（以下、EDR）製品を探すことになった。

## ワンパッケージで全セキュリティ機能を提供するCrowdStrike Falconを採用

EDRの導入に当たって、竹中工務店はセキュリティ専門ベンダーによる運用アウトソーシングを前提にした。その理由を株式会社 竹中工務店 グループICT推進室 ICT企画グループ 副部長 髙橋均氏は次のように語る。

「外部脅威の巧妙化スピードは、もはや一企業で追いつけません。サイバー攻撃の高度化に対応する専門性が必要なため、セキュリティの専門企業に協力を仰ぎました」

製品として最終的に選ばれたのはCrowdStrikeの次世代エンドポイントセキュリティソリューション「CrowdStrike Falcon」だ。

髙橋氏は選択理由について次のように語る。

「CrowdStrikeは、主要調査機関でリーダーのポジションに位置付けられ、高く評価されています。クラウドネイティブのアーキテクチャで、海外拠点に適用しやすい点も高く評価しました。」

さらに、株式会社竹中工務店のグループICT推進室 ICT企画グループの三宅宗俊氏は、選定理由を次のように付け加える。

「CrowdStrikeは『ワンパッケージですべてのセキュリティ機能を提供する』というコンセプトが印象的でした。セキュリティ分野は次々と脅威が出現するため、対抗策がどうしても“継ぎはぎ”になり、システムが複雑化して運用負荷が高まることを懸念していました。この製品はカーネルレベルでログを一括収集しており、このプラットフォームを活用すれば、資産管理やデバイス制御もやりたい時にすぐ始められる拡張性の高さも評価しました」（三宅氏）

そして2018年後半には、同社全PCを対象にEDR「Falcon Insight」、次世代アンチウイルス「Falcon Prevent」、セキュリティプロフェッショナルによるプロアクティブな脅威ハンティングサービス「Falcon OverWatch」の導入を正式に決定した。

## 後手に回りがちだった対応が、未然防止へと大きく変化

導入決定後、セキュリティの専門企業の支援を受けて国内の環境分析を開始し、2019年1月から順次エージェントをインス トールした。

現在は、同社1万3500台、海外8カ国の拠点、約2000台への導入が完了しており、引き続きその他の海外拠点、グループ会社にも展開を予定している。

「運用がきちんと回っていることが何よりです。上がってくるアラートの切り分けをセキュリティ専門企業にしてもらい、直ちに対応が必要なものは連絡をもらって、こちらから利用者に知らせるなど迅速にアクションできています。今までは脅威が顕在化しないと対処で

## 導入製品

**CrowdStrike Falcon Insight**
EDR

**CrowdStrike Falcon Prevent**
次世代アンチウイルス

**CrowdStrike Falcon OverWatch**
驚異のハンティング

## 株式会社竹中工務店

所在地：大阪市中央区本町4丁目1-13

導入時期：2019年1月

URL：https://www.takenaka.co.jp/

2019年に創立120周年を迎えた竹中工務店は、大手建設会社としてこれまでオフィスビルや商業施設、ドーム球場などのランドマークとなる数多くの建築物を手掛け、社会発展の一翼を担ってきた。現在では、建築の枠を超え「まちづくり」にも貢献している。
時代の変化を読み、企業活動に取り組んできた同社は、グローバル化やIT化も積極的に進める。

想いをかたちに 未来へつなぐ
TAKENAKA

きなかったために、対応が後手に回りがちでした。どういった動きをしているのか、大きな脅威になる前に分かることが大きな成果です。海外に関してはログを見るすべもありませんでした。今では未然防止へと大きくかじを切れました。非常に満足しています」（三宅氏）

CrowdStrike Falconの導入は、2019年末、Emotetウイルス流行時にも効果を発揮した。

「当社も既存アンチウイルスソフトウェアでは検知できなかったのですが、CrowdStrike Falcon側で止めていました。入れていたことで大事に至らずに済んだため、導入による効果を大きく実感した1件でした」（三宅氏）

## セキュリティ対策で費用削減、従業員の利便性向上を実現 在宅勤務にも CrowdStrike Falconが安心材料に

今回の導入により、サンドボックスソリューションを停止したり海外拠点のアンチウイルスソフトウェアを切り替えたりでき、セキュリティ対策の費用削減効果も出ているという。

さらに、エンドポイントセキュリティの強化は在宅勤務など“どこからでも”アクセスできる環境を実現した。

「当社は情報漏えい対策にも力を入れています。PCでのデータ暗号化やリモート消去に加えて、最近まで公衆無線LANや自宅LANからの接続も許可していませんでした。最近、感染症対策で在宅勤務がクローズアップされています。CrowdStrike Falconの次世代アンチウイルスとEDRを導入しているので、常に何が起きているか可視化、検知できています。自宅でのPC利用においてもセキュリティを確保できていると判断し、『事業部門がゴーサインを出せば在宅勤務可能』とルール変更に踏み切りました。どんな環境でも不正通信を検知できることに安心感があります」（髙橋氏）

## 今後はCrowdStrike Falconとサードパーティー製品との連携に期待

三宅氏はCrowdStrike Falconが「CrowdStrike Store」でサードパーティー製品との連携を強化していることもメリットと感じているという。クラウドで一括管理されているログが更に活用されることになり、例えば機械学習を用いた行動分析により不正な行動とリスクを検知するUEBA（User and Entity Behavior Analytics）サービスとクラウドで連携することにも期待しているという。

「当社には図面など重要なデータ資産がたくさんあります。従来はセキュリティ上の観点からアクセス権を厳格に設定し、必要なデータが迅速に利用できないケースが少なくありませんでした。UEBAを用いた行動分析が実現すれば、新たな仕組みで情報漏えいを監視しながらのデータの利活用を促進できると考えています」（三宅氏）

髙橋氏は今後期待することを次のように話す。「あらゆるデータを蓄積し、建設プロセスで活用することで、抜本的な生産性向上を実現したいと考えています。情報端末やクラウドサービスなど、あらゆる環境でのセキュリティ確保の重要性がさらに増すでしょう。クラウドサービスの進化とともに、クラウドサービス側の連携も加速してもらえればと思います。OSの最新機能なども活用して一層シンプルなセキュリティソリューションを提供してくれることを願っています」

国内外全2万台のPCへの次世代アンチウイルスとEDR展開を完遂しつつある竹中工務店は、どこまでも先進セキュリティの導入に前向きなようだ。

## POINT

- クラウドネイティブのアーキテクチャで、国内のみならず海外拠点にも容易に適用
- ワンパッケージのセキュリティプラットフォームを今後活用できる拡張性を評価
- セキュリティ専門ベンダーによる運用アウトソーシングで専門性をカバー
- どんな環境でも不正通信を検知できる、在宅勤務にも安心材料となるセキュリティ確保

株式会社 竹中工務店
グループICT推進室
ICT企画グループ 副部長
髙橋 均氏

株式会社 竹中工務店
グループICT推進室
ICT企画グループ
三宅 宗俊氏

クラウドストライク 株式会社
〒104-0031 東京都中央区京橋2丁目2-1 | crowdstrike.jp