CHECK POINT™

https://www.checkpoint.com/jp/

CHECK POINT™

# YOU DESERVE THE BEST SECURITY

## Check Point 導入事例集

# Check Point 導入事例集　目次





## About

**Check Point Software Technologies Ltd.（NASDAQ: CHKP）**
**チェック･ポイント･ソフトウェア･テクノロジーズ株式会社**

| | |
|---|---|
| 設　立 | 1993年(日本法人 1997年) |
| 本　社 | インターナショナル本社: イスラエル テルアビブ |
| 米国本社 | カリフォルニア州 サンカルロス |
| 日本法人 | 東京都港区虎ノ門 |
| 代 表 者 | 創業者 兼 CEO　Gil Shwed（ギル･シュエッド）<br>代表取締役社長　青葉 雅和 |
| 従 業 員 | 約6,000名: R&Dスタッフ 30%以上 |
| 年間売上 | 21億6,700万ドル(FY2021) |

## Solution

Secure the Network　Secure the Cloud　Secure Users & Access

Quantum　CloudGuard　Harmony

Unified Management　Infinity-Vision

THREATCLOUD　Real-time Threat Prevention

## Market Leadership

チェック･ポイント製品は、88カ国、100,000+組織にご利用いただいております。

Gartner
Magic Quadrantにおいて
2度目の“リーダー”に選出

MITRE ENGENUITY
攻撃検知技術で
最高の検出率

Leader WINTER 2022
カスタマーグリッドチョイスで
リーダーとして選出

NSS LABS
侵入防止において、サイバー
被害防止の最高スコアを獲得

IDC
高品質のモバイル
セキュリティサービスを提供

FORRESTER
エンドポイントセキュリティとして
最高スコアを獲得

Quantum Spark™

# 1-400人規模の中小・中堅規模に対応した SMB向けアプライアンス

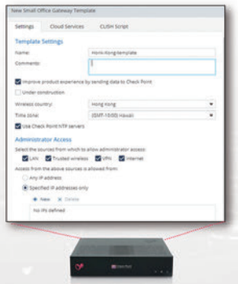
## Quantum Spark シリーズ 特徴

### オールインワンソリューション

- 必要な**セキュリティ機能が1筐体に集約**されています
- 次世代FW ／ IPS ／アンチウイルス／アンチボット／アンチスパム／ URLフィルタリング／ App制御／サンドボックス
- サイト間VPN/リモートアクセスVPN

### 容易な導入管理

- 事前定義された設定ウィザードにより **簡単セットアップ**が可能です
- 洗練されたWebベースのUIから設定、 **集中管理**が可能です
- クラウド管理のため、マネージドサービスを 活用した**運用のアウトソース**が可能です

### 脅威情報を可視化

- 視覚的に見やすい**セキュリティレポート標準搭載**
- セキュリティ機能で検知した脅威の数を明示！
- インターネットのトラフィックとアプリケーションとの利用割合を**グラフ化**！
- **感染の疑いのあるPC**の台数を表示。以降のページで 対象のPCを特定する事が可能！



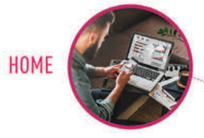


## Secure Users & Access

1 エンドポイント セキュリティ

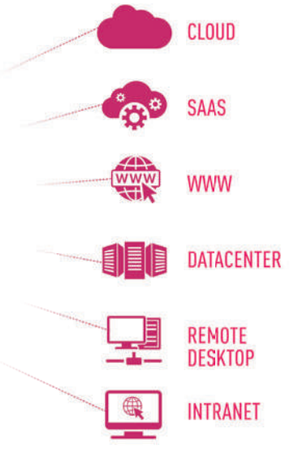
2 クライアントレスの 安全な接続

3 VPN リモートアクセス










4 安全なメール

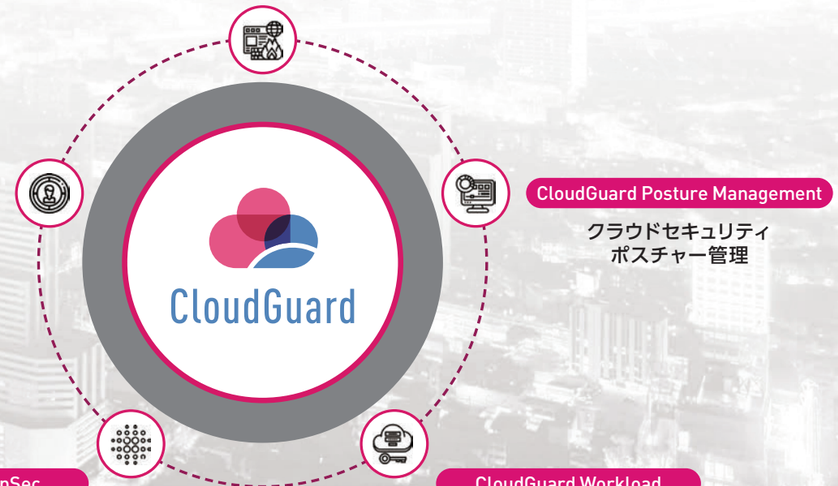
5 安全な ブラウジング

6 安全な モバイルデバイス

## Secure the Cloud

**CloudGuard Network**

プライベート・パブリッククラウド ネットワークセキュリティ




**CloudGuard Intelligence**

クラウドインテリジェンスと 脅威ハンティング

**CloudGuard Posture Management**

クラウドセキュリティ ポスチャー管理

**CloudGuard AppSec**

WebアプリとAPIの保護

**CloudGuard Workload**

ワークロード保護 （コンテナおよびサーバーレス）

# 株式会社 エフオーテクニカ

# 安全な拠点間接続とテレワーク推進に Quantum Spark 1500シリーズを導入

2003年の設立以来、人材派遣サービス・製造請負サービスを通じて顧客企業に貢献してきた株式会社 エフオーテクニカ。同社は“ひと”を大事にする企業として、企業価値の向上と地域経済の発展に貢献している。また、人材派遣に関連する個人情報を大量に保有しているため、高いセキュリティ意識を持ち、日ごろから情報セキュリティ対策にも積極的に取り組んでいる。そして、新規事業所の開設をきっかけに、管理部が中心となって拠点間連携に伴うVPNの導入や、総合的なセキュリティ対策を強化するためにチェック・ポイントの中堅企業向けセキュリティゲートウェイ「Quantum Spark」を導入した。

お客様プロフィール

**株式会社 エフオーテクニカ**

https://fo-technica.com/

所在地　宮崎県宮崎市清武町今泉丙1864番地10号

株式会社 エフオーテクニカは、あらゆる企業にアウトソーシングシステムを提案し、競争力と収益の向上に貢献している。また、労働者派遣事業では、技術派遣から事務派遣に至るまで、すべてのニーズに対応し、企業の採用要件に適した人材も紹介している。そして、設備設計事業では、経験豊かな技術者集団が、顧客の要望に合わせた自動機や治工具などの生産設備を低コストかつ短納期で提供する。

**課題**

旧UTMのセキュリティ性能とVPN対応に限界があった

**ソリューション**

Quantum Spark 1500アプライアンスを本社と営業所に導入しテレワークにも対応


株式会社 エフオーテクニカ
管理部 経理課 係長
安達 孝幸 氏

## 延岡営業所の開設をきっかけにVPN対応を見直す

Quantum Spark 1500アプライアンスを本社と営業所に導入した経緯について、株式会社エフオーテクニカ(以下:エフオーテクニカ)の管理部で経理課の安達孝幸 係長は、次のように切り出す。

「当社は、宮崎市の本社で人材派遣の業務請負とアウトソーシング事業を行っています。事業の拡大に伴って、2021年の6月に宮崎県の延岡市に営業所を開設することになりました。その準備段階で、本社と営業所をインターネット環境で結ぶ計画が検討されました。拠点間接続における重要な課題が、セキュリティ対策でした。人材派遣という業務の関係から、本社のサーバーには多くの個人情報が保管されています。また、業務システムも本社内のイントラネットで利用しています。これらのデータやシステムに延岡営業所からアクセスするためには、VPN(バーチャルプライベートネットワーク)接続が必要だと考えました。そこで、ネットワーク構成や導入機器を含めて、長年にわたり当社の情報システムをサポートしているパートナー企業に相談しました。」

エフオーテクニカから相談を受けた宮崎電子機器株式会社(以下: 宮崎電子機器)は、IT機器の導入からサポートまでワンストップでサービスを提供しているシステムインテグレータ。同社の営業本部で県央営業部 営業Ⅱ課の甲斐時和 主事は、エフオーテクニカとの関係について、次のように説明する。

「当社は、以前からエフオーテクニカのネットワークやIT機器の導入、運用保守を担ってきました。セキュリティ対策においても、以前からUTMを設置して、スパムメールやサイバー攻撃からエフオーテクニカのシステムを保護してきました。延岡営業所の開設に関する相談を受けたときにも、最先端のセキュリティ対策を提案するべきだと検討を開始しました。」

こうして、宮崎電子機器による拠点間VPN接続とセキュリティ対策の強化に向けた取り組みがスタートした。

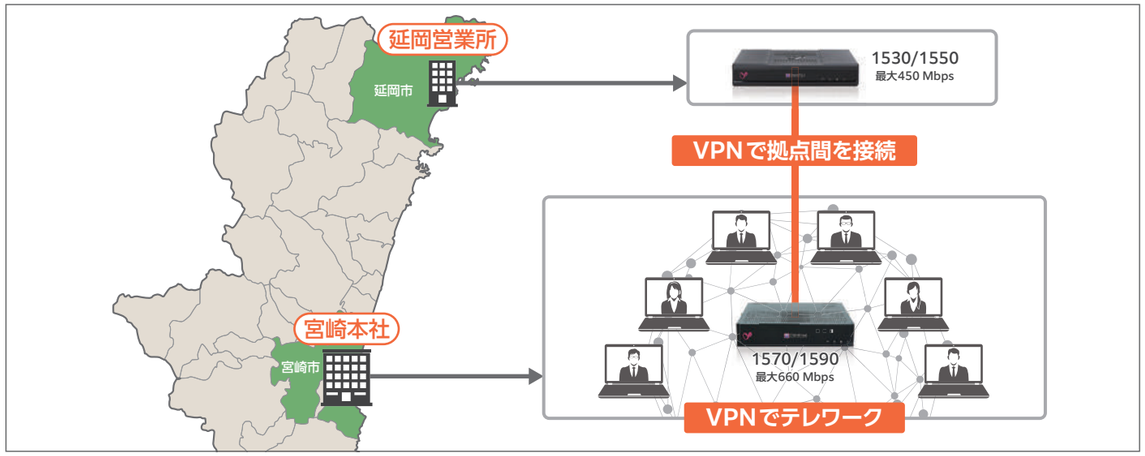
## VPNの性能と価格対性能費でQuantum Spark 1500を選定

宮崎電子機器の営業推進本部 営業推進部ソリューションサポート課の川野祐輔氏は、エフオーテクニカの新たな拠点間接続のためにQuantum Spark 1500アプライアンスを選定した理由について、次のように振り返る。

「3年ほど前に導入したUTMは、時代の変化に伴って、SSLやメールのスパムチェックなどに関して、性能面での限界を感じていました。エフオーテクニカに導入した旧UTMは、セキュリティ性能に加えて、VPN接続のレスポンス低下なども課題となっていました。そのため、延岡営業所への新たなUTM設置にあたっては、VPN性能の高さを中心に、よりセキュリティ性能に優れた製品を検討するべきだと考えました。」

旧UTM製品の課題を解決するために、宮崎電子機器では最新のUTMをリサーチする。その過程で「チェック・ポイント社の勉強会に参加する機会があり、そこでQuantum Sparkを知りました。UTMとしての総合的なセキュリティ性能に優れているだけではなく、我々が求めていたVPN接続においても、優れたスループットとコストパフォーマンスを実現していたのです」と川野氏は話す。

宮崎電子機器からの提案を受けたエフオーテクニカの安達氏は「注目したのは、VPN接続のコストパフォーマンスでした。旧UTMと同じ機器を延岡営業所に設置すると、VPN接続をオプションとして追加購入する必要があるだけではなく、ユーザー数に伴ってライセンス費も増加してしまいます。コロナ禍にあって、テレワークでもVPN接続を使う必要があったので、VPN接続のコストを抑えられるQuantum Spark 1500アプライアンスの提案は、期待に応えてくれるものでした」と評価する。




## チェック・ポイント社のサポートと教育体制を高く評価

エフオーテクニカにQuantum Spark 1500アプライアンスを提案し、安全でコストパフォーマンスに優れたVPN環境の導入に貢献した宮崎電子機器では、チェック・ポイント社のサポートと教育体制を高く評価している。川野氏は「Quantum Spark 1500アプライアンスは、2020年の後半に登場した新しいUTMでしたが、以前からチェック・ポイント社の勉強会を通して、Quantum Sparkシリーズに関しては、機能や性能を理解していました。特に、管理コンソールに関して勉強会で学べたことは、とても有意義でした。その後、社内でも他のUTMと機能や速度などを比較して、製品の優秀さは確認していました。また、当社は二次代理店となりますが、チェック・ポイント社から丁寧なサポートも受けられたので、これならば安心して我々のお客様にも提案できると考えていました」と提案の背景を振り返る。

Quantum Spark 1500アプライアンスは、自動脅威防止機能で最高レベルのセキュリティを実現している。受賞歴のあるチェック・ポイントのSandBlast Zero Day Protectionにより、最大2Gbpsの脅威防止性能と脅威防止に特化した60以上のセキュリティサービスを提供している。また、エフオーテクニカの求めていたリモートワーク向けのセキュリティも標準搭載している。Quantum Sparkゲートウェイでは、一般的なUTMには搭載されることが少ないリモートアクセスVPNを標準で搭載し、テレワーク環境でも社内にあるファイルサーバーやNASなどに、安全にアクセスできる。加えて、二要素認証を活用すれば、アカウントの乗っ取りなども防御できる。こうした性能が総合的に評価され、エフオーテクニカはQuantum Spark 1500アプライアンスを採用した。

## レポートによる可視化で脅威を未然に防げる

Quantum Spark 1500アプライアンスによって刷新されたUTMによるセキュリティ対策の強化と、拠点間および社員のテレワークで利用するVPN環境の成果について、安達氏は「テレワーク業務を実施している社員からは、『通信速度が速くなった』という声は届いています。また、旧UTMをそのまま利用してVPNを構築した場合と比較して、16%のコスト削減になりました。そして、毎週レポートがメールで届くので、セキュリティの情報を定期的に確認できるようになりました。結果的に、速度も速くなり、経費も節約できて、安全性も増したので、構築された環境には満足しています」と導入の成果を語る。

また、導入後も継続的にQuantum Spark 1500アプライアンスの運用を補佐している川野氏は「レポートによるセキュリティ状況の可視化は、導入を提案した当社としても、大きな成果だと受け止めています。エフオーテクニカから許可をいただいて、レポートの共有や管理コンソールへのリモートアクセスを通して、定期的に状況を確認できるので、サイバー攻撃の兆候などあれば、迅速に対処できるようになりました。また、延岡営業所に設置されているQuantum Spark 1530をリモートで運用監視できる点も、高く評価しています。もしも、リモートアクセスができなければ、宮崎市内から延岡市まで2時間半かけて出向くか、当社の延岡支店からスタッフを派遣しなければなりません。それでは、対応に遅れが出てしまいます。それだけに、リモートで迅速に対応できる環境は、大きな安心につながります」と管理面での利便性を評価する。

## サイバー攻撃の増加にはCheck Point製品で防御

Quantum Sparkシリーズを今後も継続して利用し、より多くの顧客企業に提案していくために、甲斐氏は「当社の中で、Quantum Sparkの勉強会を開いて、より多くの社員が製品を理解する機会を増やしていきたいと考えています。製品に対する理解度が高まれば、エフオーテクニカと同じような課題を抱えるお客様に、提案していけると思います」と話す。

エフオーテクニカの安達氏は「昨今、サイバー攻撃の増加が新聞などでも取り沙汰されています。最近の攻撃のパターンでは、大手企業を直接狙うのではなく、セキュリティ対策の弱い中小企業が攻撃の踏み台にされるケースも増えています。弊社の場合は、取引先に大企業が多いので、サイバー攻撃を受ける危険性も増えています。幸い、これまでにセキュリティ被害は発生していませんが、セキュリティ対策の強化は必須となっています。今回のように、UTMをQuantum Sparkという最新モデルに更新することで、サイバー攻撃を未然に防ぐ強化ができたと思っています」と今回の取り組みを総括し「当社は、宮崎県を中心に営業活動を推進していますが、今後は長崎県や大分県など、九州圏内への進出も計画しています。そのときにも、各拠点に開設する営業所やオフィスへ、Quantum Sparkなどチェック・ポイント社の製品を導入して、VPN接続だけではなく、より強固なセキュリティ対策を実施していこうと思っています」と今後の計画を語る。

Quantum Spark™

# 学校法人札幌国際大学

## 3台のCheck Point 1800で コストパフォーマンスに優れたセキュリティ対策を実現

札幌国際大学は、観光学部、人文学部、スポーツ人間学部からなる大学と、総合生活キャリア学科や幼児教育保育学科がある短期大学、そしてスポーツ健康指導研究科や観光学研究科や心理学研究科のある大学院に、国内外から約1,600名の生徒が在籍している。同大学では、学生の良質な学びの機会を提供するために、2017年から学内でのWiFi環境を整備してきた。一方で、WiFi環境の充実は、利用者の増加に伴うセキュリティ面での課題をもたらした。そこで、同大学のITインフラを整備してきた株式会社近藤商會と株式会社ウチダシステムズは、協力してCheck Point 1800 とBarracuda Load Balancer によるセキュリティ対策の強化を実現した。

お客様プロフィール

**学校法人札幌国際大学**
https://www.siu.ac.jp/
所在地　札幌市清田区清田4条1丁目4-1

1969年(昭和44年)に開学した札幌静修短期大学を前身に、1997年(平成9年)に名称を変更した札幌国際大学。同大学は、学生一人ひとりの確かな自立を目指した良質な学びの機会を提供する「学生ファースト」と、世界とつながる日本語・外国語コミュニケーション能力を育てる「国際化」を教育の柱に、「自立した人間」づくりを実践している。

学校法人札幌国際大学
情報システム課 主査　根津 宗宏 氏

**課題**

学生の学内フリー WiFi利用の増加に伴う
安全なインターネット接続の実現

**ソリューション**

Check Point 1800 アプライアンス×3と
Barracuda Load Balancer x1による
モニタリングと負荷分散

**株式会社ウチダシステムズ**
北海道支社 札幌営業部 公共営業課　大滝 志郎 氏

オフィス空間のデザイン・設計、オフィス家具販売及び内装工事などのオフィス関連事業と、大学市場への備品・情報機器の販売を手がける教育関連事業に、福祉・医療関連事業を推進し、「場」の価値向上を通じて、顧客企業のパフォーマンス向上と目標達成に貢献している。

**株式会社近藤商會**
営業部 営業2課　課長　関根 哲 氏

オフィス・商業施設の空間デザイン・設計・施工・監理や、オフィスネットワークの設計・施工・管理など、「空間コンシェルジュ」を目指して、人の集まる様々な「空間」を「より快適」に「より便利」に「より効率的」なプロデュースを提供している。

### 「学生ファースト」を実践する WiFi環境の整備

Check Point 1800によるセキュリティ対策の強化に取り組んできた経緯について、学校法人札幌国際大学 情報システム課の根津宗宏氏は、次のように振り返る。
「きっかけは、2017年からスタートした学内フリー WiFi環境の整備でした。そこで、当大学のIT基盤を担っている近藤商會に、ネットワークやアンテナなどの施設設備の検討をお願いしました。」
PCや周辺機器の販売からオフィスや学校などのネットワーク環境整備を提供する株式会社近藤商會 営業部 営業2課の関根哲氏は、同大学のWiFi環境の整備について、次のように話す。
「大学からの要望は、敷地内すべてでWiFiが使えるようにしたい、という内容でした。そこで、2017年の夏休みから工事を開始し、そこから毎年少しずつアクセスポイントを追加していきました。そして2019年には、学内全域でWiFiがつながるようになり、学生も教職員も積極的にWiFiを利用する環境が整備されました。」
学生や教職員の利便性を向上させたWiFi環境の整備は、情報システム課にとって新たな課題をもたらした。根津氏は「学生サービスの一環としてのフリー WiFiの提供により、セキュリティ対策の強化という課題が出てきました。学内で学生が授業以外にも利用するフリー Wifi環境において、コンピュータウィルスやマルウェアに感染する危険性のある危険なサイトにアクセスさせないための監視と防御が必要になりました。また、必要最低限の規制を設けなければ、接続回線に対する通信量も膨大になり、サービスの質が低下することも明白だったので、その調整弁となる機能も併せ持った統合脅威管理(UTM)が不可欠となりました」と説明します。

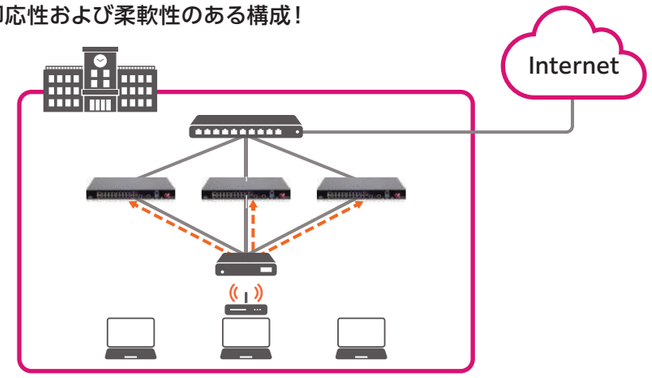
### WiFi利用の安全性を守るために チェック・ポイントのUTMを導入

情報システム課からWiFi環境におけるセキュリティ対策の強化を依頼された近藤商會では、ウチダシステムズと連携して、提案する機器の選定を開始した。その経緯について、株式会社ウチダシステムズ北海道支社 札幌営業部 公共営業課の大滝志郎氏は、次のように説明する。
「札幌国際大学からの相談を受けて、高性能なUTMによる監視と制御が必要だと考えました。そこで、当社で取り扱う製品の中でも、数多くの導入実績があり、セキュリティ性能についても信頼の高いチェック・ポイントのUTMが最適だと判断して、提案することにしました。」
提案を受けた大学では「様々な業者のサービスからの案内が、日々紹介される中において、チェック・ポイントの提案がダントツに費用対効果、費用対機能面で優れていることがわかったため、一も二もなくチェック・ポイントを指名買いさせてもらいました」と根津氏が選定の理由に触れる。
2019年から導入を開始したチェック・ポイントのUTMの効果について、関根氏は「導入して間もなく、UTMからのアラートがありました。そのアラートについて、根津氏から相談を受けてレポートを調べたところ、動画投稿サイトを長時間閲覧している学生の存在や、データ量の多いファイルをダウンロードするサイトへのアクセスなどが確認されました。チェック・ポイントのUTMを導入していなければ、こうした行為は見過ごされていました。このエピソードのおかげで、チェック・ポイントのUTMに対する大学からの信頼も高まりました」と話す。
根津氏も「チェック・ポイントのUTMは、レポートが見やすいので、学生のWiFi利用の傾向を的確に把握しやすく、危険性の兆候も事前に察知しやすいと感じています。2019年の導入から、トラブルもなく円滑に利用していましたが、年々 WiFi環境を利用する生徒が増えてきました。授業のない時間帯に学生が自分のスマートフォンやPCなどを接続する程度でしたが、BYODを活用した授業が増えてきたことに加えて、コロナ禍により教員がオンライン授業でWiFi環境を利用する頻度も増え、2020年になると以前に比べて利用数もトラフィック量も増大してきました。そこで、UTMの増強も検討することになりました」と導入の成果とさらなる取り組みについて振り返る。

### Check Point 1800と Load Balancerの組み合わせで 価格対性能比も向上

大学構内におけるWiFi利用の増加に伴い、セキュリティ対策の強化とトラフィック増大に対応する処理能力の向上を求められた近藤商會とウチダシステムズでは、チェック・ポイントのシステムエンジニアと連携して、機器の選定を行った。その結果「3台のCheck Point 1800 とロードバランサーの組み合わせを提案しました。チェック・ポイントのUTMには、1台で大学のトラフィックをすべて処理できる高性能な上位モデルもあります。しかし、大学側の求めるコストパフォーマンスと、今後のトラフィック増加を見据えた拡張性を考えると、1台で対応するよりも、3台で負荷分散するシステムを構築した方が、価格対性能比も向上すると判断しました」と大滝氏は説明する。
Check Point 1800は、ファイアウォール、VPN、アンチウイルス、アプリケーション可視化およびコントロール、URLフィルタリング、メール セキュリティ、SandBlastゼロデイ保護など、「オールインワン」のセキュリティソリューションを提供する中規模ビジネスに適したUTMアプライアンス。Webインタフェースを使ったローカル管理や、クラウドベースのQuantum Spark SMP (Security Management ポータル) を使った一元管理が可能になる。
根津氏は「チェック・ポイントのUTMの性能については、これまでの運用実績で信頼していました。そこで、チェック・ポイントを基本とした増強案を求めました。その期待に、近藤商會とウチダシステムズの提案は十分に応えてくれました。特に、ロードバランサーにより3台のCheck Point 1800を組み合わせた構成は、今後の拡張も可能にする柔軟な提案だったので満足しています」と評価する。






### 新入生等のBYOD環境にも 対応していく

今後に向けた取り組みについて、根津氏は「2022年度からは、新入生に一人一台のPCを利用してもらう計画です。そのため、学内のWiFi利用もさらにトラフィックが増加すると予想しています。現在は、まだ余裕がありますが、来年度の利用状況を見て、夏ごろにはCheck Point 1800の増強を検討するかもしれません」と話す。
また、大滝氏は「情報セキュリティ対策という観点では、Check Point 1800による監視や防御も重要ですが、それに加えて学生たちの利用するPCのエンドポイントセキュリティ対策も求められると思います。Check Point 1800で学内の安全性は担保できても、自宅に持ち帰るPCには学外での感染リスクもあります。そこで、チェック・ポイントのエンドポイントセキュリティ製品を提案したいと考えています」と今後に向けた考えを示す。
そして、関根氏も「すでに、2022年の夏には、WiFi環境の増設も計画されています。これからも、学生や教職員の安全で快適なネットワーク基盤の構築やサポートで、札幌国際大学の『学生ファースト』を支えていけたらと願っています」と語る。
根津氏は「情報セキュリティ対策にゴールはありません。これからも、学生や教職員のネットワーク環境には、さらなる利便性の提供と情報セキュリティ対策の強化を継続していきます。そのためにも、近藤商會とウチダシステムズからの提案には、これからも期待しています」と抱負を述べる。

Quantum Spark™

# 学校法人吉田学園

## Check Point 1800が学生や教職員の安全なインターネット利用に貢献

学生の満足、保護者の満足、高校の先生方の満足、採用した企業の満足、教職員自身の満足という「5つの満足」を使命に、北海道で専門性に優れた人財の育成に努めている学校法人吉田学園。同学園は、保健医療の専門職業人を育成する札幌保健医療大学を筆頭に、自動車整備やスポーツ専門など8つの大学校・専門学校、さらに3つの保育園を運営している。また、同学園のコンピュータシステム部では、各校のITシステムを整備している。その一環として、2019年に学生が利用するWiFi環境を構築するにあたり、安全なインターネット接続のためにCheck Point 1800を導入しセキュリティ対策に取り組んでいる。

お客様プロフィール

**学校法人吉田学園**

https://yoshida-g.ac.jp/

所在地　札幌市中央区南3条西1丁目15

1956年、遠別町に開校した「北海珠算専修学院」から始まった学校法人吉田学園。同学園は、札幌保健医療大学を始め、専門学校グループとスポーツ施設、また姉妹法人として保育園グループを有する一大教育ネットワークを形成し、スペシャリストな人財を輩出するために、より良い教育環境の提供に取り組んでいる。

**課題**

学生や教職員が利用する校内WiFiの安全なインターネット接続

**ソリューション**

Check Point 1800によるモニタリングとレポート

学校法人吉田学園
法人本部 法人経営企画局
コンピュータシステム部
管財部 部長
千葉 一俊 氏

学校法人吉田学園
法人本部 法人経営企画局
コンピュータシステム部
久保 嘉 氏

**大丸株式会社**

http://www.daimaru-inc.com

本社所在地　札幌市白石区菊水3条1-8-20

大丸株式会社は、1892年に創業し、和紙の販売から始まった事業は、文具、印刷、雑貨へと発展。IT化が進むなかでお客様のニーズの変化を敏感にとらえ、OA機器、情報システム分野など取扱商品と商領域を広げてきた。常に変化するお客様の要望に応え続けるため、総合力だけでなく、専門性を高める努力と新たな取り組みを続けている。

### 校内のWiFi環境の整備に伴うセキュリティ対策

Check Point 1800を導入した背景について、学校法人 吉田学園 法人本部 法人経営企画局コンピュータシステム部の久保 嘉 氏は、次のように振り返る。

「きっかけは、校内で学生が利用するWiFi環境の整備でした。当学園では、一部の学校でWiFiは施設していましたが、学生が自由に接続できるアクセスポイントは整備していませんでした。その整備に伴って、セキュリティ対策も強化しなければならないと考えて、複数のシステムインテグレーターにネットワーク施設とセキュリティ対策を含めた提案を依頼しました」

コンピュータシステム部から提示された要件は、学生が快適に利用できるWiFiアクセスポイントとネットワーク環境の構築に加えて、学生が学園に持ち込むPCなどのデバイスから、ウイルスやマルウェアなどが侵入する危険性を排除するセキュリティ対策だった。生徒が持ち込むデバイスを制限することは難しく、セキュリティ対策を個々に確認するのも困難だったので、WiFiアクセスも含めたネットワーク全体を安全に監視して制御する仕組みが求められた。

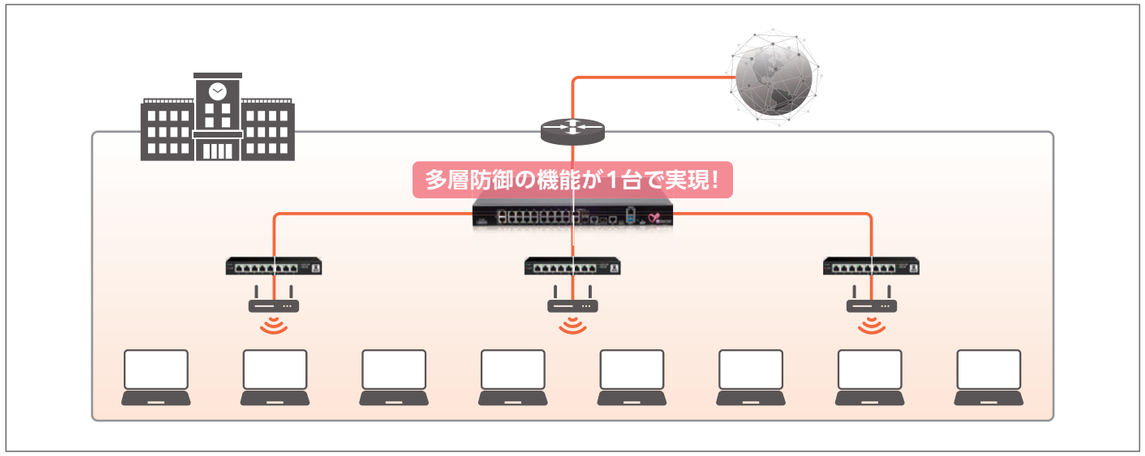
WiFi環境の整備とセキュリティ対策は、複数の業者から提案が提供されたが、コンピュータシステム部では、北海道の地場企業として長い歴史と実績のある大丸株式会社からの提案を採用した。その理由について、久保氏は「大丸からの提案の中にあったCheck Point 1800のレポート機能に注目しました。当学園では、以前から他社のアプライアンスUTM（統合脅威管理）を利用している学校がありました。しかし、そのUTMでは、ネットワークの遅延が発生する可能性がありました。他社からの提案では、そのUTMが含まれているケースもあり、WiFi環境構築における総合的な技術力と、Check Point 1800によるセキュリティ対策を評価して、大丸からの提案を採用しました」と説明する。

### 最初は1校からスタートし3年後に全校で導入

学内のWiFi環境は2019年から整備を開始し、「2020年8月にセキュリティ対策としてチェック・ポイント製品の利用を始め、現在は5校舎8校のWiFi環境でCheck Point 1800が稼働しています。」と久保氏は現状の対応に触れ、「Check Point 1800を全校で利用しようと判断した大きな理由は、レポート機能の見やすさとチェック・ポイント社のサポート対応の良さにありました」と理由を語る。

Check Point 1800は、ファイアウォールに侵入防止システム（IPS）やアンチウイルスとアンチスパムといった基本的なセキュリティ対策に加えて、VPNやURLフィルタリングにアプリケーション制御やアンチボットとサンドボックスなどのセキュリティ対策を一台のアプライアンスで提供する。さらに、Check Point 1800のレポートは、トップページに脅威の有無やアプリケーション別の帯域消費などのデータが、見やすいグラフやアイコンで表示されるので、学生がインターネットをどのように利用しているのかを的確に把握できる。例えば、最初の行にアンチボット機能、アンチウイルス機能、IPS機能、Threat Emulation（サンドボックス）機能（オプション）など、検知された脅威の数が表示される。その下には、円グラフでインターネットトラフィックの合計とアプリケーションごとの利用割合が表示される。さらに、もしもウイルスに感染したPCが発見されると、感染したPCの台数を表示し、以降のページで感染したPCのIPアドレスも確認できる。他ベンダーの場合はこのようなセキュリティレポート機能が別途有償オプションになる事もあり、標準搭載されている場合は言語が英語やテンプレートが見にくいこともあるが、チェック・ポイントの場合はこうした見やすいレポートにより、セキュリティ対策の専門家ではなくても、トップページをチェックするだけで、校内のネットワークに脅威があるかないかを的確に把握できるようになる。






### レポートの見やすさからウイルスの脅威も未然に防ぐ

Check Point 1800を提案し、現在も吉田学園のネットワーク環境やセキュリティ対策をサポートしている大丸株式会社 システム販売推進部の桜岡峰生 主幹は、その利便性について、次のように説明する。

「用語や挙動など、セキュリティ イベントの把握対応は難しいものですが、チェック・ポイントSMB製品のレポートは利用者視点で見やすいです。レポートで通常の通信状況を把握して、差異があれば調査し、状況に応じてサポートへ問い合わせする。こんな対応フローをお客さま自身でも行える製品なので、お勧めしています。レポートのチェックは、お客さまの運用となりますが、当社にも共有していただいて、ダブルチェックすることも可能です。」

大丸の対応とチェック・ポイントのサポート体制について、久保氏は過去のエピソードに触れる。運用開始後に「Check Point 1800の定時レポートで、前回より脅威の検知数が増えている。」という報告が大丸からありました。そのときに、教職員のPCに影響が出ているかどうか調査するために、チェック・ポイント社のサポートに連絡をしたことがあります。すると、サポートセンターからリモートでCheck Point 1800に接続してもらい、学園内のネットワークをチェックして、被害が教職員のPCには及んでいないと確認してもらいました。サポートセンターの的確な対応には感謝しています」と久保氏は評価する。


### 教職員のWiFi活用も増えCheck Point 1800の重要性が増す

今後の取組について、コンピュータシステム部 管財部の千葉一俊 部長は、次のように語る。

「コロナ禍の影響で、教職員も校内の各教室や離れた場所からリモート授業やWeb会議を行う機会が増えています。そのため、今後も校内のWiFiを含めたネットワーク環境の利用は増えていくでしょう。将来的には、学生と教職員の利用するネットワークは、完全に分離する計画もあります。ネットワークの構成は変わっても、Check Point 1800によるセキュリティ対策は、継続して利用していきます。」

また、大丸の桜岡氏は、Check Point 1800によるセキュリティ対策について「学校だけではなく、行政が提供するWiFiスポットなど、不特定多数の利用者が接続するネットワークでは、Check Point 1800によるセキュリティ対策は必要になると思います。当社もCheck Point 1800で得られた知見を活かして、より多くのお客様にセキュリティ対策を提案していきたいと考えています」と話す。

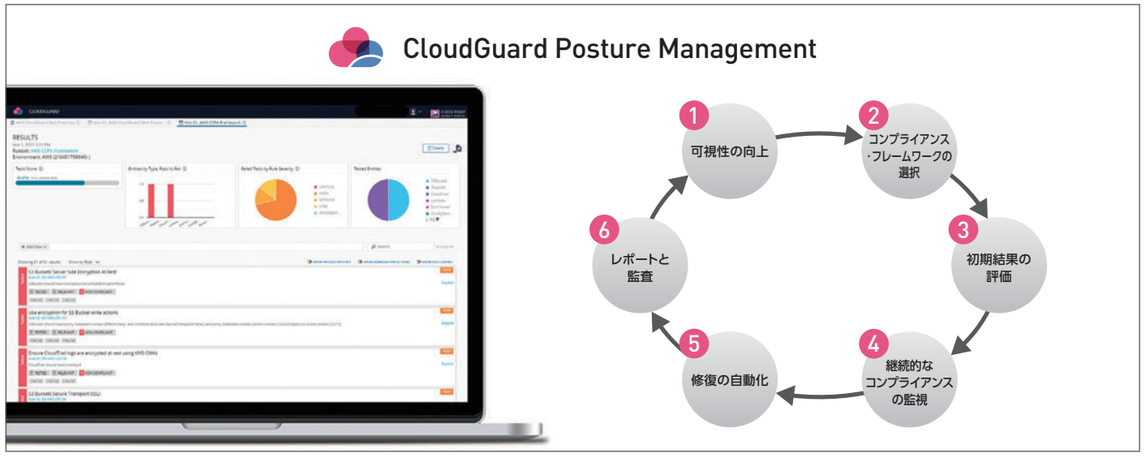
そして、久保氏は「運用に特別な負担は感じておらず、現状、安全に使えているので、通信に何らかのトラブルがなければ、このままCheck Point 1800を継続して使っていきたいと考えています。将来的に、何かしらの新たな脅威が発生したときには、その対策を相談して、必要があれば新しい機種でサポートするなど検討していきます。そうした対策についても、大丸やチェック・ポイントのサポートに相談できればと願っています」と期待を語る。

CloudGuard Posture Management

# 株式会社BeeX

# パブリッククラウドの安全・安心を強化するために BeeXがCloudGuard Posture Managementを採用

SAPなど基幹システムを中心としたエンタープライズシステムのクラウドインテグレーションを専業に2016年3月に設立されたBeeX。同社は、「Be Excited」(わくわくする)と、受粉を助けるBee(蜂)に社名の由来があり、企業活動を通して世の中にポジティブなエネルギーを与えている。オンプレミスからパブリッククラウドへの移行を推進する企業にとって、同社の提供する先進テクノロジーは、成長と変革にも貢献してきた。そして、BeeXではクラウドに移行したエンタープライズシステムを、より安全に効率よく効果的に運用するために、CloudGuard Posture Managementを採用し、新たなサービスの提供に取り組んでいる。




お客様プロフィール

**株式会社BeeX**

https://www.beex-inc.com/

所在地　東京都中央区銀座7-14-13
日土地銀座ビル10F

クラウドの黎明期からSAP基幹システムのクラウド移行を手掛ける敏腕コンサルタントが一同に集結し、数多くのSAP基幹システムのAWS移行を実施してきた。また、レガシー体質になりがちな基幹システムの運用業務を改革するために、「わくわくする」サービスを提供している。

**課題**

マネジメントサービスのセキュリティ対策と運用効率の改善

**ソリューション**

CloudGuard Posture Managementを採用し運用管理の改善

株式会社BeeX
デジタルプラットフォーム本部
マネージドサービス部
部長
石井 博和 氏

株式会社BeeX
デジタルプラットフォーム本部
マネージドサービス部 第2グループ
小野内 貴啓 氏

## マルチクラウド対応とクラウドサービス管理の強化

BeeXのマネージドサービス部が、CloudGuard Posture Managementを採用した背景について、デジタルプラットフォーム本部 マネージドサービス部の石井博和部長は次のように説明する。

「当社は、エンタープライズシステムやSAPシステムのクラウド移行・環境構築に秀でたスペシャリストが数多く在籍するSIerです。中でも我々マネージドサービス部は、創業時より数多くのお客様の基幹システムをAWSを中心としたパブリッククラウドに移行させた後の運用保守をMSP(マネージドサービスプロバイダ)という形で提供しております。そうした取り組みの中で、2つの課題がありました。ひとつは、マルチクラウドの広がりです。我々が創業した当初は、AWSへの移行が中心でしたが、最近ではMicrosoft AzureやGoogle Cloud といったパブリッククラウドを利用されるお客様も増えてきました。加えて、単一のパブリッククラウドではなく、複数を組み合わせて利用するマルチクラウド化も進んでいます。もうひとつは、運用管理に携わる人的なリソースの課題でした。」

2つの課題のうち、マルチクラウド化における顧客企業の変化について、プロフェッショナルサービス本部 マネージドサービス部 第2グループの小野内 貴啓氏はパブリッククラウドの違いを次のように解説する。

「例えば、Windowsのライセンスを多く利用されているお客様であれば、Microsoft Azureを利用した方が、コストを削減できます。また、大容量のデータ分析を必要とするお客様は、Google CloudのBigQueryの活用などを検討されます。こうした理由から、複数のパブリッククラウドを効果的に組み合わせて利用するお客様のご要望も高まっています。」

そして、人的な課題について石井氏は「当マネジメントサービス部では、お客様ごとに専任の担当者がいて、パブリッククラウドの運用管理を担うだけではなく、お客様の利用状況などを定期的にモニタリングして、プロアクティブな改善提案を行ってきました。そのメンバーが、より効率よく的確に改善提案をするためには、各パブリッククラウドベンダーが提供している監視ツールだけでは、業務効率を改善できないと考えたのです」と補足する。

## MSP事業の競争力を高めるために採用

マルチクラウドの運用と監視を効率よく推進し、運用管理にかかる人的な負担を軽減するために、マネージドサービス部では、いくつかの観点から製品の選定を開始した。その一つについて、石井氏は「マルチクラウドに対応した運用監視ツールの選定においては、機能に加えて我々のMSP事業に貢献できるかどうかも判断しました」と選定の理由を振り返り、「CloudGuard Posture Managementに関しては、AWS、Azure、Google Cloudのコンポーネントにフル対応し、クラウドネイティブのAPIと連携して、パブリッククラウドの設定状況を可視化する、といった機能に注目しました。加えて、ライセンスをリセールするだけではなく、サービスプロバイダのツールとして、CloudGuard Posture Management機能を我々のお客様に対して様々な形で提供できるよう、柔軟に対応頂けた点も評価しました」と説明する。

検討段階で検証した具体的な機能について、小野内氏は「CloudGuard Posture Managementを利用すると、単一のコンソールから、AWSやAzureなど複数のパブリッククラウドの設定を変えられるのは、とても便利だと実感しています」と評価する。

CloudGuard Posture Managementは、マルチクラウドに対応した設定・運用の可視化ツールとして、Security Groupをグラフィカルに表示し、コンプライアンスのチェックや自動修正を行う。また、IAM Safetyによるアカウントの保護も可能になる。そして、ログやイベント解析によるセキュリティ・インテリジェンスで、侵入検知や構成変更などのアラートも受信できる。石井氏は「マルチクラウド環境に対応した可視化とカスタマイズ可能なダッシュボードによって、これまで以上に各担当者は的確にお客様の運用状況を一元的に把握できるようになります。MSP事業にとっては、お客様へのサービス品質を向上し、社内業務の効率化も図れる優れたツールとなります」と指摘する。


## 顧客企業も高い興味を示す

CloudGuard Posture Managementによる新たなマネージドサービスの提供について、BeeXの顧客企業からも、すでに問い合わせが寄せられているという。その一例について、石井氏は「人事業務のアウトソーシングサービスをMicrosoft Azureで提供しているお客様が、CloudGuard Posture Managementによるセキュリティ対策を検討されています。そのお客様は、給与計算などのWebアプリケーションをサービスとして公開しているので、どのように自分たちのセキュリティポリシーに合わせて運用していくかが、課題となっていました。こうしたお客様にとって、CloudGuard Posture Managementは、とても効果的なサービスになると思います」と説明する。

パブリッククラウドの利用では、セキュリティ対策において「責任共有モデル」が適応される。クラウドプロバイダーは、クラウドベースのインフラ部分に対する基本的なセキュリティ対策は提供するが、それだけではパブリッククラウド上に構築したシステムの安全性は確保されない。仮想マシン(ヴァーチャルマシン)の運用状況においては、ルートテーブルやネットワークACLにセキュリティグループなど、各種の設定が適切に行われているかを定期的に確認する必要がある。もちろん、設定に加えて不正な侵入や意図しない構成変更などが行われないように、常に監視しなければならない。こうした業務を人手だけで対応するのは限界がある。CloudGuard Posture ManagementをBeeXがマネージドサービスの一環として顧客企業に提供することにより、利用者はより安全な運用が可能になる。

CloudGuard Posture Managementによるコンプライアンスの改善により、図のように継続的なコンプライアンスの監視と自動修正によりコンプライアンスが維持される。

## 中小企業へのサービス提供を計画

今後の取り組みに向けて、石井氏は「現在は、我々のクラウドマネジメントサービスに、どのようにCloudGuard Posture Managementを組み入れていくか、そのサービスメニューを編成している段階です。CloudGuard Posture Managementには、豊富なマネジメント機能が備わっているので、お客様によってどの範囲までを求められるのか、ご要望に合わせて提供できるメニューを整備していきます。そうすることで、我々のMSP事業の強みにつながると考えています」と話し、さらに「将来的には、CloudGuard Posture Managementによるパブリッククラウドのセキュリティマネジメントを中堅中小のお客様も手軽に利用できるサービスへと発展させていきたいと計画しています」と展望を語った。

# 株式会社フーバーブレイン

# スマートフォンの安全を確保するために Harmony Mobileを全社導入

未来の価値を創造する情報セキュリティ対策を提供している株式会社フーバーブレイン。同社は、2001年の創業から情報トラッキング技術によるセキュリティ対策を提供してきた。現在は、第４次産業革命という社会モデルの変革を見据えて、「セキュリティ+α」を意識したビジネスを推進している。同社の情報システム部では、2019年から社員が業務で利用するスマートフォンのセキュリティ対策を強化するために、チェック・ポイントのHarmony Mobileを全社員に導入した。

お客様プロフィール

**株式会社フーバーブレイン**

https://www.fuva-brain.co.jp/

所在地　東京都千代田区紀尾井町4-1
ニューオータニガーデンコート22F

マルウェア対策のEye 247 AntiMalwareをはじめとして、サイバーセキュリティソリューションの提供や、テレワーク環境の構築、そして生産性およびクオリティオブライフの向上支援を事業として展開。Check Point UTMと自社開発のソフトウェアを組み合わせたソリューションも提供している。

**課題**

全社員が利用するスマートフォンの
情報セキュリティ対策の強化

**ソリューション**

Check Point Harmony Mobileを導入し
会社支給と個人利用の端末（BYOD）にも対応

株式会社フーバーブレイン
カスタマーサポート部 部長
韓 富根 氏

株式会社フーバーブレイン
情報システム部
塚本 真誠 氏

## 全社員に貸与したスマートフォンのセキュリティ対策が課題

株式会社フーバーブレインがスマートフォンのセキュリティ対策を必要としていた背景について、同社のカスタマーサポート部の韓富根部長は次のように振り返る。

「約3年前に、全社員に会社からスマートフォンを貸与することになりました。スマートデバイスの業務活用は時間や場所に縛られない多様な働き方を可能にします。その一方で、企業の重要なデータや個人の行動履歴などを簡単に社外に持ち出せるようになります。そのため、情報漏えいや第三者による不正アクセスなどのリスクが増大します。しかし、当初は社員の情報セキュリティに対するリテラシーの高さに頼って、貸与した端末の管理については各自に任せていました。」

情報セキュリティ対策に関するソフトウェアやソリューションを提供している同社では、社員のセキュリティに対する意識も高く、これまでにもセキュリティ被害が発生したケースはなかった。スマートフォンの導入と管理を担当していた情報システム部の塚本真誠氏は、運用面での課題について次のように話す。

「社員には、ゲームなどのアプリをインストールしないように、フィッシング詐欺やマルウェアなどに注意するように、といった通達はしていました。しかし、導入当初から数ヶ月が経過したころに、スマートフォンなどのモバイルデバイスを標的にしたサイバー攻撃が急増していたので、何らかの技術的な対策を施すべきだと考えました。」

こうした背景から、同社の情報システム部が中心となり、スマートフォンのセキュリティ対策の強化が検討された。

## Check Point Harmony Mobileを導入しアプリ、ネットワーク、OSを保護

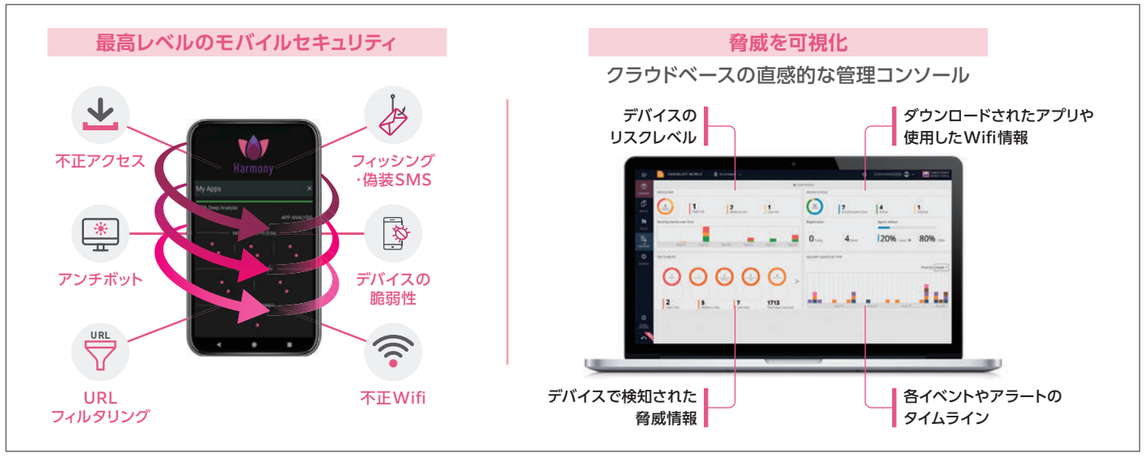
スマートフォンのセキュリティ対策の検討において「当初は、セキュリティ対策と並行して、MDM（モバイルデバイス管理）で対応できないか検討しました。ただ、MDMでは端末の管理はできても、セキュリティ対策までは強化できないので、最終的には当社で導入したiPhoneに対応しているセキュリティ対策を探すことにしました」と塚本氏は経緯を説明する。

セキュリティ対策の選定にあたって、情報システム部ではモバイルデバイスに対する3つの防御ポイントに注目した。それは「アプリケーションとネットワークにOSです」と塚本氏は指摘する。スマートフォン用のアプリケーションの中には、個人情報を盗み出したりデバイスを不正に利用するマルウェアが含まれている危険性が潜んでいる。社員のITリテラシーに頼った運用だけでは、悪意のあるアプリケーションからの保護は万全とはいえない。また、街中や商業施設などで利用できるフリー WiFiスポットの中に、不正なアクセスポイントを立てて個人情報を盗むケースも増えている。そして、OSの脆弱性を狙った攻撃や意図しない構成変更など、デバイスそのものへの攻撃への対策も強化が求められている。こうした課題に対して「Check Point Harmony Mobileは、脅威検知と脅威防御を両立していたので、導入を決めました」と塚本氏は評価する。

## スマートフォンに必要とされるすべての脅威対策を実現し強固な運用管理を実現

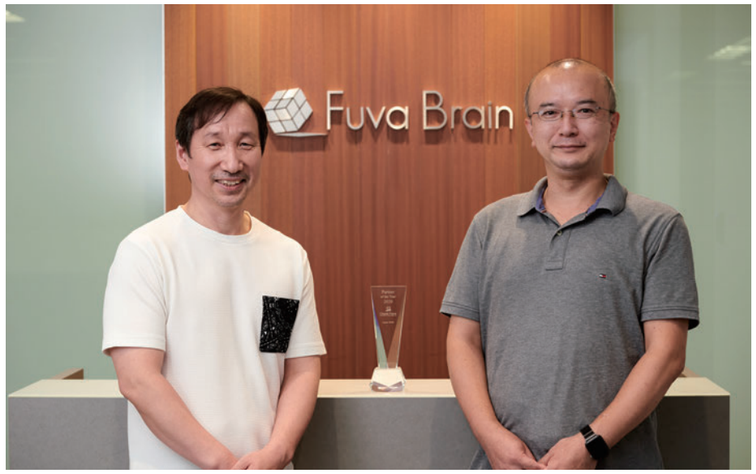
同社の情報システム部が求めていたスマートフォンのセキュリティ対策において、Check Point Harmony Mobileは必要とされるすべての脅威対策を実現していた。具体的には、不正アプリの検知や不正WiFiによる攻撃の検知に、Webフィルタリングとセーフ･ブラウジング、そして危険なコンテンツのダウンロード防止などになる。韓氏は「セキュリティ対策における機能面で注目したのは、AIを用いたリスク評価や専任チームでの分析により、未知（ゼロデイ）の不正アプリを検知できる点でした。また、専用のブラウザなどが不要で、アプリに依存しない設計も、利用者の利便性に配慮していると感じています。それと、社員の中には個人の所有するスマートフォンを業務に利用するBYOD希望者もいたので、そうした利用方法にも柔軟に対応している点も評価しました」と選定の背景を語る。

さらに、日々の運用管理を行っている塚本氏も「管理者としては、ブラウザベースで利用できる直感的な操作画面は、使いやすいと思います。また、何か問題が発生すれば、すぐに登録しているメールアドレスに通知が届くので、定期的に管理画面をチェックする必要もなく、運用管理も容易です。実際に、Check Point Harmony Mobileを導入してからは、管理者に届くメールも、月に1～2通ほどで、セキュリティ被害も発生することなく、安全な保護を継続しています」と導入の成果を話す。




## ITの専任者がいない中小企業にも適したスマートフォン向けのセキュリティ対策

2019年に全社員のスマートフォンへ導入し、約2年を経過した現在もセキュリティ被害はゼロを継続している。塚本氏は「Check Point Harmony Mobileは、導入から日々の監視まで操作も運用管理も容易なので、当社のようなセキュリティ対策のスペシャリスト集団に限らず、ITの専任者がいない中小企業にも、安心して導入できるスマートフォン向けのセキュリティ対策だと思います。セキュリティ対策にはゴールがないので、毎日70万件以上も発生する新たな脅威に対して、いかに安全に守るかが問われています。そうした脅威に対して、Check Point Harmony Mobileはスマートフォンの安全な業務利用に貢献するソリューションです」と評する。




さらに韓氏は「当社では、社内でCheck Point Harmony Mobileを利用しているだけではなく、我々のお客様にもCheck Point UTMのようなセキュリティ製品を提供しています。Check Point UTMは、セットアップが簡単で事前にキッティングしておくと、客先でのセットアップを数分で完了できます。このCheck Point UTMを導入されているお客様からも、スマートフォンを含めたモバイルデバイスのセキュリティ対策を強化したい、という要望が数多く寄せられています。こうしたお客様にも、Check Point Harmony Mobileを推奨しています」と話す。

Check Point Harmony Mobileを2年以上にわたって利用してきた実績から、フーバーブレイン社としても、安心して自社の顧客に紹介できる自信があるという。それに加えて「Check Point Harmony Mobileの管理画面は、SaaS型のクラウドサービスなので、お客様から許可をいただければ、当社のサポートチームが遠隔で運用管理を担うことも可能です。そのため、IT専任者がいない中小企業でも、スマートフォンにCheck Point Harmony Mobileをインストールしてもらうだけで、その後の運用監視は専門家である当社に任せていただけます」と塚本氏は補足する。

今後に向けて韓氏は「現在のところ、スマートフォンなどのモバイルデバイスに関しては、Check Point Harmony Mobileで 十分に守られているので、これ以上に強化する計画はありません。ただ、コロナ禍の影響で在宅勤務が増えているので、社員が自宅から安全にネットワークを利用する対策を強化していきたいと考えています。Check Point Harmony Mobileの他にも、優れたセキュリティ対策があれば、積極的に検討していきます」と取り組みを話す。