CASE STUDY 導入事例

マネージドセキュリティサービスを導入 SOCにより24時間365日のセキュリティを確保

製造

KURIYAMA
クリヤマジャパン株式会社 様

資本金 / 1億円　従業員数 / 約400名(2023年4月現在)
事業内容 / 建機、農機向けゴム・樹脂製品の製造・販売、スポーツ施設や商業施設向け各種床材の製造・販売・施工、スポーツアパレルの販売。
本社 / 〒540-6325 大阪市中央区城見1丁目3番7号 松下IMPビル

多角的な事業を展開されているクリヤマジャパン株式会社様

課題

エンドポイントセキュリティに関する運用負荷軽減とインシデント発生時の迅速かつ適切な対応

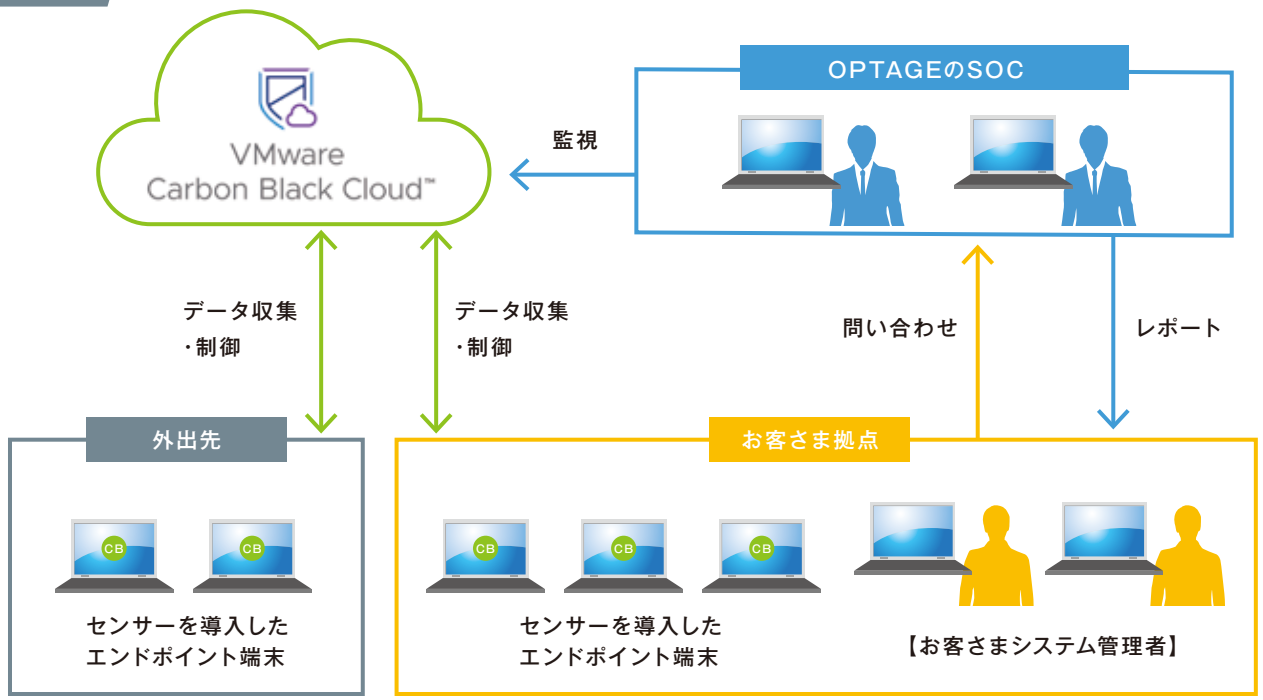
導入サービス

マネージドセキュリティサービス（エンドポイント監視）

導入効果

SOCにより最小限の労力でセキュリティを確保

ネットワーク構成



求められた24時間対応のセキュリティ体制

スタンダード市場に上場しグローバルな事業展開を行うクリヤマホールディングス株式会社、その中核を担う事業会社がクリヤマジャパン株式会社です。同社のIT統括室では少数のスタッフが、システム全般の保守・管理からセキュリティ対応までを引き受けています。

「2020年ぐらいからセキュリティリスクが、世間全般で騒がれ始めるようになり気にはなっていました。もちろん我々もそれなりのエンドポイント対応策は導入していましたが、決して万全とはいえないと自覚してもいました」と、IT統括室室長の吉元良史氏は以前の状況を語ります。

セキュリティ対策ソフトは自社サーバで運用しているため、通知の来ないインシデントを確認するには、自ら毎日ログをチェックしなければならず、仮に深夜に何らかのアタックを受けていたとしても、通知はメールでしか届きません。少人数を言い訳にせず24時間対応できる体制の整備が、セキュリティ対策上の最重要課題となっていたのです。

経営陣からも求められたセキュリティ強化

「2022年ぐらいからでしょうか、ロシアによるウクライナ侵攻のあたりからさまざまなサイバー攻撃が急激に増えてきました。ちょうどその頃に、当社で社外監査役を務めている方の関わっている会社がランサムウェアに感染したのです。これで経営陣の危機感が一気に高まり、直ちにできる限りの対策を取るようにとの指示が出ました」と、吉元氏。

当時オンプレミスで導入していたソフトも、もちろん自動更新は続けていましたが、どうしても最新の攻撃に対して即応しきれない部分が出てきます。世間では新たな攻撃が相次いで発生していたため、危機感を募らせた吉元氏は数社に提案を求めました。

「オプテージさんに声をかけたのは、実は最後でした。当時同社のインターネットオフィスを導入してはいましたが、セキュリティ関連のサービスを取り扱っているとは知らなかったのです」と、吉元氏は当時を振り返ります。

決定的にした1営業日以内の復旧保証

オプテージが提案したのはVMwareの「Carbon Black」を活用したマネージドセキュリティサービス。アンチウイルスはもちろん、EDR（Endpoint Detection and Response）に加えてSOC（Security Operation Center）のサービスも標準パッケージとなっています。仮に何らかの攻撃を受けてエンドポイントが再起不能となった場合でも、1営業日以内の復旧が保証される。復旧には遠隔操作で対応するので、IT統括室のメンバーには何の作業負担も生じません。

「EDRに関しては、各社でそれほど違いは感じなかったのですが、SOCの安心感には強いインパクトがありました。しかもたまたまですが、Carbon Blackはアメリカのグループ会社がすでに採用済みで、運用負荷などについては、まったく気にする必要のないレベルだと聞かされたのも大きな安心感につながりました」と、吉元氏は語る。

そして発注が決まってから約1カ月でのスピード導入となりました。

24時間365日対応が与える絶大な安心感

導入後には1カ月かけた検証と、さらに社内説明のための資料作りなどにもう1カ月が費やされました。

「インシデント発生時には自動的にネットワークから切り離され、SOCでリカバリー対応してくれる。つまりインシデント発生時の対応が、これまでとはまったく異なります。新しい体制を理解してもらうため説明資料をつくり、国内の各拠点を回って説明会を開催しました。これは改めてセキュリティ意識を高めるためのイベントとしても効果的でした」と、吉元氏。

同社では、従来から社内でメールセキュリティについての教育と訓練を実施しています。教育の過程で理解度チェックも行っていて、元々セキュリティリテラシーは高いのです。

「その上でSOCが与えてくれる安心感はとても大きい。幸いEDRに関しても、今のところ何もインシデントは起きていません。IT統括室のメンバーの負荷を大きく軽減しながら、セキュリティを確保できた。コストパフォーマンスはかなり高い」と、吉元氏は導入成果を評価してくれました。

次はオンプレミスからの移行に関するサポートを

サイバーアタックの被害が頻繁に報道されるようになり、気が気でないというのが正直なところでした。攻撃する側が狙うとしたら、おそらくは深夜帯です。けれども以前のシステムではメールアラートしか届かない。朝になってから気づいたのでは手遅れになります。だから24時間365日対応のSOCは非常に心強い。Carbon Black導入でセキュリティ関連の対策は一通り整えることができたので、次の課題は基幹システムを含むより包括的な対策です。自社サーバでの管理はBCP対応を考えても、この先難しくなると考えています。一気にオンプレミスからクラウドへ全面移行するのは考えにくいとしても、部分的なアウトソーシングとしてデータセンターの活用などは視野に入れています。その際にはネットワーク周りの提案も含めてオプテージさんにはいろいろ期待しています。

IT統括室 室長 **吉元 良史**氏

（2024年2月取材）

株式会社オプテージ　関西電力グループ power with heart

本　　社　〒540-8622 大阪市中央区城見2丁目1番5号 オプテージビル
東京支社　〒100-0013 東京都千代田区霞が関1丁目4番2号 大同生命霞が関ビル

https://optage.co.jp/business/

ビジネスインフォメーションデスク
通話料無料 0120-944-345
biz-support@optage.co.jp
受付時間/9:00~17:00（土・日・祝・12/29~1/3・5/1を除く）

CASE STUDY 導入事例

マネージドセキュリティサービスを導入し マンパワー不足をカバーしてセキュリティを確保

卸売・小売

SHINEI
伸栄商事株式会社 様

資本金 / 8,000万円　従業員数 / 103名(2020年4月現在)
事業内容 / 全国の生活協同組合および事業連合会を取引先とする、化粧品、健康食品、日用品雑貨の卸商社。
新大阪本部 / 〒532-0003 大阪市淀川区宮原3-4-30 ニッセイ新大阪ビル

左から　●伸栄商事株式会社 情報システム課 係長 山本崇大氏　●髙田美菜子氏

課題

業務負荷を
増やさずにエンドポイントの
セキュリティ確保

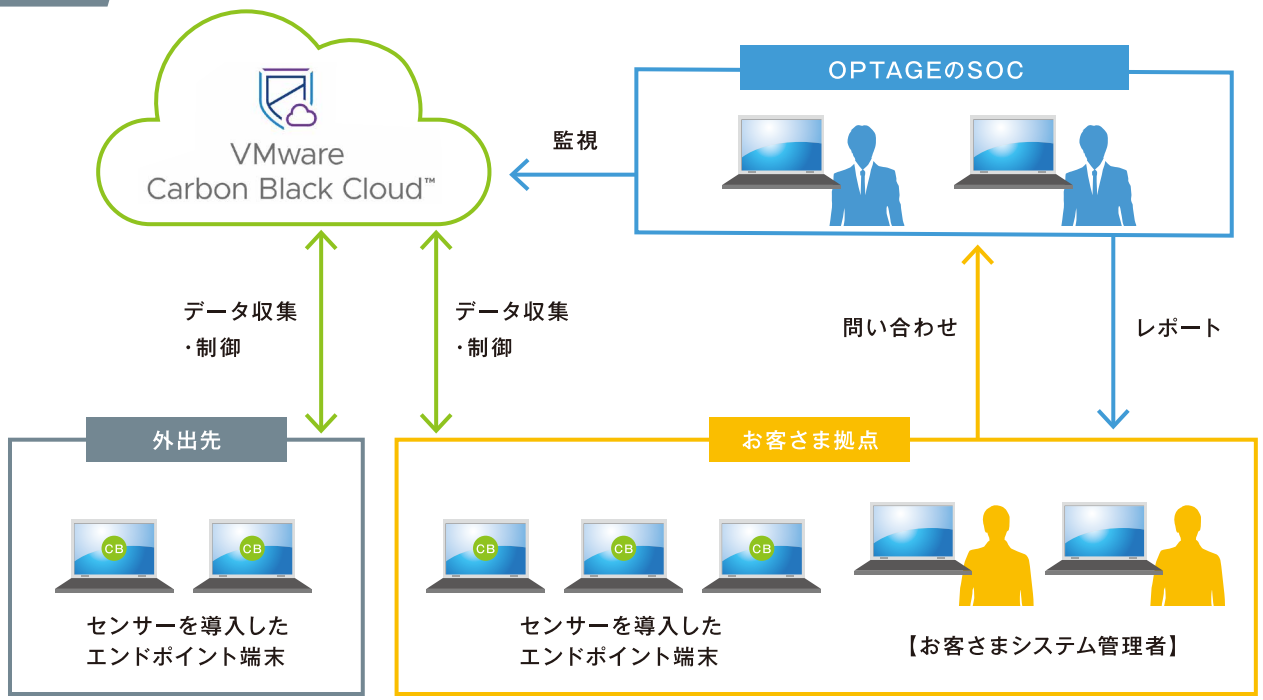
導入サービス

マネージド
セキュリティ
サービス
（エンドポイント監視）

導入効果

最小限の労力で
セキュリティの基盤を確立

ネットワーク構成



人員不足の中、迫るマルウェア感染の危機

伸栄商事株式会社は、化粧品や健康食品、日用品雑貨などを全国の生活協同組合に卸しています。同社では以前から情報システム課員が2人体制で、約170台に及ぶ社内のパソコンはもとより、システム全般の保守や管理まで全業務を担当していました。

「正直なところマンパワーが絶対的に不足していますから、可能な限り業務をアウトソーシングしたいと考えていました」と、情報システム課の山本崇大氏は厳しい状況を振り返ります。

同社ではこれまでも社内端末に次世代型のアンチウイルスソフト（NGAV）を導入するなどのセキュリティ対策をとっていました。そんな中、同様のNGAV製品を利用している企業でマルウェア被害が発生しているとの情報を受け、「自社の状況を直ちに確認し、比較的早い段階でパスワード変更やアカウントの再作成等の対策を実施しましたが、それだけでは不十分だと思っていました」と、山本氏。「人員も少なく、セキュリティ対策はベンダーに任せきりでしたが、エンドポイントのセキュリティについてさらなる強化が急務と考えたのです」と、山本氏は振り返ります。

24時間体制で監視、サイバー攻撃から保護

EDR（Endpoint Detection and Response）サービス導入の必要性を痛感した山本氏は、“セキュリティ・一括対応”をテーマに数社に提案を求めました。

「他社からはネットワーク監視型のUTM（統合型脅威管理）の提案もありましたが、オプテージさんが提案したマネージドセキュリティサービスならEDRと専門アナリストによる支援が組み合わされているため、当社には最適なサービスだと感じました。全端末のログをリアルタイムで収集・分析し、セキュリティインシデントが発生した場合直ちに適切に対処してもらえる。24時間365日体制での対応ですから、まさに理想のアウトソーシングです」と、山本氏。

採用されたオプテージのマネージドセキュリティサービスはVMwareの「Carbon Black Cloud Endpoint」を組み合わせており、その高度なマルウェア検知能力には定評があります。ポリシーチューニングの柔軟性が高いので、要望をきめ細かく反映しながらもエンドポイントの脅威にフレキシブルに対応します。山本氏は「信頼できる外部のエキスパートに対応を任せられる。これほど安心感のあるソリューションは他にはないなというのが、正直な感想です」と、語ります。

信頼感を高めた、丁寧な導入プロセス

以前はベンダーに任せきりだった山本氏、今回は要望をしっかり伝えなければと意気込んでいると「こちらから話を切り出すまでもなく、オプテージさんの方からわかりやすい説明を徹底してもらった上で、じっくりとこちらの要望を聴いてもらえました。SEの方のサポートも受けながら、ヒアリングシートの項目に答えていき、わからないところがあれば納得行くまで質問できました」と、当時を振り返ります。

写真左から、伸栄商事株式会社の山本崇大氏、髙田美菜子氏と打ち合わせをするオプテージ大石康介

ヒアリングした内容に基づいてオプテージが管理サーバを設定。いったん設定が終了した段階でテストを実施し、問題がなければ全端末に展開します。「完全にブロックすると業務上支障をきたすアプリケーションがありましたので、一部は除外する必要があります。当社からのさまざまな要望にもSEの方が的確に対応してくれました」と、山本氏。テストは問題なく終了し、山本氏が用意したインストーラーを使って社員各自によるインストール作業も無事終了。2022年8月に申し込みを受け、10月から本格運用を開始するスピーディな導入となりました。

多層防御の基盤を確立、次のレベルのセキュリティ確保へ

新しいシステムの運用を開始した直後に、取引先がランサムウエア攻撃の被害を受けたと報道されました。そこで社員のセキュリティ意識をより高める必要があると考え、同社では標的型メール対応などのセキュリティ講習を実施しています。「幸い、これまでのところ導入後はインシデントは発生しておらず、Carbon Blackからのアラート通知も上がってきていません。導入時に全メールを自動スキャンした際には、過去メールの感染を検知してくれたので、その精度には信頼感をもっています。ただ、現状で安心してはいけないと気を引き締めています」と、山本氏。

次の課題と考えているのが、ネットワーク全般のセキュリティ強化です。取引先のトラブルを目の当たりにした経営層もセキュリティの重要性は理解しています。「今後もこういったサービスを利用することで社内のセキュリティ対策に取り組みたい。仮に感染したとしても、端末1台だけで直ちに封じ込められるような体制づくりを急ぎたい」と、山本氏は次の課題を語ってくれました。

全体的なセキュリティサポートを期待

とにかく人手が足りない、これが現状です。だからSEの人件費にかけるコストをシステム投資に回してでも、セキュリティを確保する必要があります。ランサムウエアの被害事例は、マスコミでも大きく取り上げられましたから、上層部でもセキュリティに対する関心は高まり、費用対効果を考えた安全確保のための投資に前向きになってもいます。旧式となっている基幹システムの問題に加えてBCP対策も充実を図る必要があります。私は開発担当ですから、セキュリティ関連はできる限りアウトソーシングしたい。ぜひオプテージさんにはネットワーク全般も含めて、安心して任せられるセキュリティ提案を期待しています。

情報システム課
係長
山本 崇大氏

（2024年2月取材）

株式会社オプテージ　関西電力グループ power with heart

本　　社　〒540-8622　大阪市中央区城見2丁目1番5号 オプテージビル
東京支社　〒100-0013　東京都千代田区霞が関1丁目4番2号 大同生命霞が関ビル

https://optage.co.jp/business/

ビジネスインフォメーションデスク
通話料無料 0120-944-345
biz-support@optage.co.jp
受付時間/9:00~17:00（土・日・祝・12/29~1/3・5/1を除く）