totalsecurity™

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point Endpoint Securityの導入により、管理担当者の業務負荷が大幅に削減できた上、未知の脅威の防止や不正プログラムの停止など、エンドポイント・セキュリティが強化されました。

業務革新推進室
情報マネジメントシステム課
古賀流石氏

ユーザ

三菱重工業株式会社 高砂製作所

- 本工場所在地：兵庫県高砂市荒井町新浜2-1-1
- 社員数：3,647人
- 生産能力：ガスタービン 600万kW、火力/原子力タービン 240万kW、水車 75万kW他

導入ソリューション

- Check Point Endpoint Security™

ニーズ

- クライアント端末のセキュリティ強化
- Windows Updateとウイルス・チェック・ソフトの定義ファイル更新の徹底
- 不正な通信プログラムの監視・制御

チェック・ポイント選択のポイント

- リアルタイムの通信ログラムの監視・制御において、エージェント常駐型のクライアント・セキュリティが最適であること

チェック・ポイント・エンドポイント・セキュリティで実現した検疫ネットワーク

8,500台のクライアント端末のセキュリティ・レベルを維持・向上

発電用ガスタービンや火力/原子力タービンなどエネルギー・プラントを支える大型回転機械を製造する三菱重工高砂製作所は、エンドポイント・セキュリティの強化をめざし、Check Point Endpoint Security（旧製品名Integrity）による検疫ネットワークを構築している。同ソリューションの導入により、クライアント端末は日々変化する脅威に対して最善のセキュリティ環境が維持され、不正な通信プログラムによる情報流出など脅威の防止に十分な効果を発揮している。

エネルギー・プラントの開発・製造を通して暮らしと産業を支える

高砂製作所は、大型回転機械の専門工場として大きな特長を持ち、暮らしや産業の基盤となる「電気と水」にかかわる製品を製造している。主力製品は、生産高全体の61%を占める発電用のガスタービン（年間生産能力600万kW）をはじめ、火力/原子力タービン、水車、発電所用ポンプなど。高品質の製品を生み出す最先端の技術と生産設備を擁し、発電用ガスタービンは国内シェア40%以上を占めるほか、欧米・アジア・中南米・中近東など40カ国以上に輸出され、海外でも高い評価を得ている。

兵庫県高砂市の瀬戸内海を臨む広大な敷地に本工場や研究所を構え、約3,700人の社員が働く。

OSの脆弱性をつかれた脅威の被害を受け検疫システム導入を検討

高砂製作所管内には、パートナー会社を含め約9,000台のパソコンがある。2003年から2005年にかけて、Windowsの脆弱性に起因するワームやウイルス等の被害が多発し、ネットワークが停止して業務継続が不可能になるような事態が発生していたという。というのも、インターネットなど外部ネットワークへの接続は三菱重工本社のゲートウェイ・シス

テムを経由しているという背景から、セキュリティ・パッチの適用は各ユーザに任せている状態でMicrosoft Software Update Service（SUS）の展開もしていなかったことが要因の1つだった。その後、SUSを所内展開し、各部署のOAサポーター（パソコン関係の管理担当者）がWindows Updateの適用を1台1台確認する体制にしたため、被害は減ったものの依然として脅威にさらされる危険はあった。

「当時はWindows98も残っており、完全にSUSを適用できなかったことに加え、多くの社員が出張等でノートPCを使うことが多く、脆弱性が残るパソコンが外出先でウイルスに感染するケースがなくなりませんでした。エンドユーザにセキュリティ意識を徹底することは難しく、OAサポーターの管理負担も大きいため、Windowsのセキュリティ・パッチやウイルス・チェック・ソフトの定義ファイルの更新を強制化し、外出先から持ち帰ったパソコンが所内ネットワークに及ぼす脅威を防御することが必須でした。当時、ちょうど検疫システムが注目されだしたので、その導入を検討しました」。業務革新推進室情報マネジメントシステム課 古賀流石氏は、当時のクライアント端末のセキュリティ課題とCheck Point Endpoint Securityによる検疫ネットワーク導入の背景をこう述べる。

通信プログラムの監視・制御要件を満たすCheck Point Endpoint Security

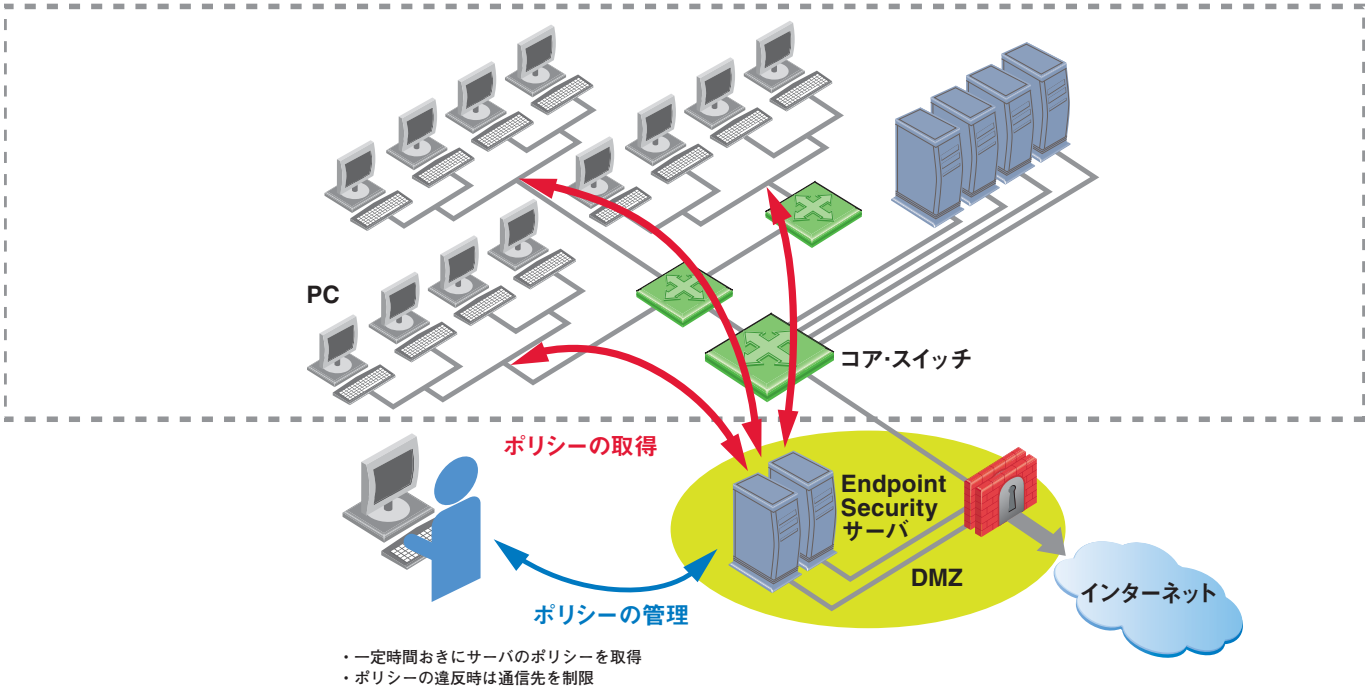
古賀氏は2004年後半に一度、出そろってきた検疫システムの方式であるネットワーク・スイッチ認証方式、セキュリティ・ゲートウェイ方式、DHCP方式について、どの方式が適切かそれぞれ検討をした。しかし、当時は検疫システム自体が登場したばかりで、各社とも頻繁にバージョンアップを繰り返し、必要とする機能を問い合わせると次期バージョンで対応という回答が多く、仕様が固まっていないために導入を見送った経緯がある。

「そうこうしているうちに、ファイル共有ソフトによる機密情報の流出事故などもあり、セキュリティ・パッチや定義ファイルの更新徹底させる機能だけでなく、危険なソフトの使用を検知する通信プログラムの監視と制御が必須になり、検疫システムの導入が火急の課題になりました」（古賀氏）という。

古賀氏がクライアント端末の検疫機能に求めた要件は、①Windows Updateとウイルス・チェック・ソフトの定義ファイルの精査、②セキュリティ・ポリシーにかかわるレジストリの精査、③通信プログラムの監視と制御を強制的に実行できる環境だった。

「特にWinnyのようなレジストリを精査しても検知できないタイプのソフトウェアの使用をコントロールするためには通信プログラムの監視・制御は必須であり、当時のDHCPサーバ方式やアプライアンスによるセキュリティ・ゲートウェイ方式では難しく、クライアント端末にエージェントをインストールしてチェックする方式、あるいはネットワーク内部のパケットを随時キャプチャする方式でないと駄目だろうという結論に至りました。また、ネットワーク・スイッチによる方法ではネットワーク機器をすべて同じベンダーに統一する必要があるため、導入コストが膨らみ、現実的ではありませんでした。そうした検討を経て、Check Point Endpoint Securityに代表されるようなエージェント常駐型（パーソナル・ファイアウォール型）の検疫システムが最適だと判断しました」（古賀氏）。リアルタイムに発生する通信プログラムを収集し、その通信プログラムが何なのかを調査して、危険な通信プログラムである場合は停止するという通信プログラムの監視と制御を実行するには、Check Point Endpoint Securityが最適なソリューションだったと選定の動機を語る。

ネットワーク構成



totalsecurity™

Check Point SOFTWARE TECHNOLOGIES LTD.

約8,500台のクライアント端末に展開 その効果

情報マネジメントシステム課
古賀流石氏

Check Point Endpoint Securityは、9か月のテスト運用を経て2006年12月に社内の約3,000台に展開、翌年1月にはパートナー会社も含めた約8,500台のクライアント端末に展開された。また、検出された通信プログラムの検証作業にアイ・オー・エス（東京・港区）の不正通信監視サービス（NRMS）を採用して運用している。本格導入後2年を経て、これまでに約3万件の通信プログラムを検出し、NRMSで精査してもらった結果、250件の不正プログラムが発見され排除できた。また、定義ファイルが配布される前に感染が確認された端末があったときは、被害は数台に限定され感染拡大を阻止できたという。

「未知の脅威に対してもネットワーク接続を阻止できるなど、十分に導入の効果は出ています。何よりも、Windows Updateや定義ファイルの更新が徹底され、約100人の部門OAサポーターが1か月に361.5時間かけて、1台1台確認していた作業が不要になったことが大きな成果です。自分の業務を持つOAサポーターにとって、そうした端末管理は多大な業務負荷だったわけですから」（古賀氏）と、Check Point Endpoint Security導入の効果を強調する。

Active Directoryと連携したきめ細かなポリシー設定へ

現在、パートナー会社を含む高砂製作所管内のクライアント端末は、検疫機能においては同一の基本的なポリシーで運用されている。同社ではすべてのユーザがActive Directory（AD）で管理されているため、今後はこれと連携させることにより、パートナー会社の社員や自社の社員のグループ管理によってポリシー設定を細かくしていきたいと考えている。「インベントリ収集ツールや暗号化ソフトなどパートナー会社と違いがあり、クライアントの統一環境を作るのは難しい状況。ADと連携させれば、それぞれの社員のユーザ環境に適したポリシー設定ができ、端末の制御環境をより詳細にすることができるでしょう」（古賀氏）。

また、現在通信プログラム制御をブラックリスト方式で運用しているため、一度不正なプログラムが検出されない限り通信を止めることはできない。古賀氏は、導入検討当初より許可された通信プログラムのみを利用できるホワイトリスト方式の方が安全との考えを持っており、今後はホワイトリスト方式へ変更していこうと計画している。

チェック・ポイント製品導入のポイント

検疫機能に求めた要件

以下にあげた要件を強制的に実行できる環境であること

1.Windows Updateとウイルス・チェック・プログラムの精査

2.セキュリティ・ポリシーの精査

3.通信プログラムの監視と制御

Check Point Endpoint Securityに代表される常駐型（パーソナル・ファイアウォール型）の検疫システムが最適であると判断

ソリューション

Check Point Endpoint Security

社内、およびパートナー会社も含め、約8,500台のクライアントPCへインストール

サービス

NRMS

Check Point Endpoint Securityによって検出された通信プログラムの検証作業サービス

導入の効果

1.コストの削減

管理者が1台1台行っていたWindows Updateの適用確認作業が不要になり、管理者は本来の業務に専念できるようになった。

2.ウイルスの拡散を未然に防止（2回）

ウイルスに感染したPCが確認されたが、検疫システムによるプログラム停止と感染PCの隔離による拡大防止が実施され、大きな混乱が避けられた。

3.不正プログラムの検出（2年間で約250件）

その他、業務に無関係なプログラムを約100件検出した。

製品に関するお問い合わせ

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
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F
http://www.checkpoint.co.jp/ E-mail : info_jp@checkpoint.com Tel : 03(5367)2500

P/N 950010-J 2010.03 ※記載された製品仕様は予告無く変更される場合があります。