



株式会社アマダ

企業プロフィール

日本を代表する金属加工機械の総合メーカー。海外展開に積極的で、現在、売上げの約5割強は北米、欧州、中国・東南アジアなど海外から。板金加工機械の分野では、売上げ、世界シェアトップクラスを誇る。アマダの連結売上高は163,153百万円、従業員数(連結)は5,899名(2011年3月期時点)



操作パネル(写真左)のコンピューター部分のセキュリティをMESにより強化

※ 本事例の中での「板金加工機械」という用語は、原則として、「Windows搭載型板金加工機械」を指します。また、本事例の中で、「機械のコンピューター活用部分」などの表現があった場合、それは「機械の操作系(Windows)の部分」を指します。「機械の『制御そのもの』を行うコンピューター部分(マイコン等)」は含まれておりません。

※ 本事例の中の「ウイルス」という語は、「ウイルスおよびワーム、トロイの木馬その他の悪質プログラム」を指します。

■ Embedded Security 導入事例 — 株式会社アマダ



「アマダでは、Windows搭載型板金機械のすべてにホワイトリスト方式ウイルス対策 McAfee Embedded Securityを出荷時標準搭載しています」

McAfee Embedded Securityを、自社製品すべてに出荷時標準搭載

— アマダでは、現在McAfee Embedded Securityをどう活用していますか。

アマダでは、自社のWindows搭載型の板金加工機械に、ホワイトリスト方式ウイルス対策ソフトウェアとしてMcAfee Embedded Security(以下MES)を出荷時に標準搭載しています。¹ MES搭載機は、2011年1月からの約半年の間に、約1500台を国内および海外に向けて出荷しました。

また2010年12月以前に出荷したMES未搭載機器に対しても、有償となりますが、後入れ型でのMES導入サービスを提供しています。

アマダでは、「アマダの製品は出荷時点で十分なセキュリティ対策が施されていないと考えるべきであり、「お客様の機械が安定稼働することがアマダにとっての最重要課題」だからです。

MES標準搭載による利用者のベネフィット

— アマダの板金加工機械にMESを標準搭載したことによる効果を教えてください。

MESの標準搭載により、アマダのお客様である工場ユーザーには、「長期間にわたって利用される板金加工機械において、本来は手間の掛かるウイルス対策のことは何も気にしなくていい。手間いらず。忘れて大丈夫」という利便性が確保されます。

※ 1 標準搭載のモデルカバー率ですが、製品のモデル更改のタイミングの兼ね合いから、一部、MESがまだ搭載されていない機器もあります。

「ホワイトリスト方式ウイルス対策」であるMESが、「ブラックリスト方式ウイルス対策」と比較して、どのような点で板金加工機械のウイルス対策に最適なのか、各々の特徴は次の通りとなります。

製品機能の比較軸	ブラックリスト方式	ホワイトリスト方式
組込OS、レガシーOS*の利用が前提となる組込システム	× 最新OSに最新ウイルス対策ソフトを導入する前提。長期利用のレガシーOS、組込OSへのサポート面での制約がある。	○ ウイルス定義ファイルを利用しない保護機能であり、組込OS、レガシーOSへの長期サポートが可能である。
限定的なHWリソースとなる組込システムでの性能影響	× ウイルス定義ファイルの更新とスキャン作業時にシステムに負荷が発生、稼働中のアプリへの性能劣化が懸念される。	○ スキャンは行わず、アプリ起動時にホワイトリスト照合を行い、ウイルス実行を防止する為、オーバーヘッドは少ない。
利用者によるシステム運用面の負担	× 日次での定義ファイル更新とスキャン作業を行う必要があり、これらの確認作業を含めた運用工数がかかる。	○ ホワイトリストの登録作業が完了すると、その後の運用面での利用者負担は発生しない。

※レガシーOSとは、OSベンダーがサポートを終了させたOSを指します。

そもそも、最新のウイルス対策ソフトを導入し、定義ファイルの更新やスキャンに負荷が伴う「ブラックリスト方式ウイルス対策」は、ハードウェアリソースが限定的で、長期利用を前提とする板金加工機械には向きません。

板金加工機械のように、決まったプログラムのみを稼働させる環境では、正しいプログラムのみを稼働させ、ウイルスといった不正なプログラムは稼働させない「ホワイトリスト方式ウイルス対策」が、より向いています。

ホワイトリスト方式ウイルス対策はどのようにウイルスからシステムを保護するのですか？

— マカフィーに質問です。ホワイトリスト型ウイルス対策の動作原理について簡単に説明してください。

一般的なウイルス対策であるブラックリスト方式は、「悪質なウイルスを見つける(クロを通さない)」という形式です。一方、McAfee Embedded Securityでのホワイトリスト方式ウイルス対策では、「正規なプログラムの動作だけを許可する(シロなら通ってよし)」という形式になります。

ウイルスはシステム環境に混入しただけでは感染しません。ウイルスプログラムを実行されることで初めて感染します。従って、「正規なプログラムの動作だけを許可する」という形式をとると、ウイルスの実行を防止できます。

— 動作するプログラムが正規(シロ)であることを、どうやって判定するのですか。

予め、利用者にとって正規(シロ)なプログラムを登録してもらいます。そして、本番環境では、新たなプログラムが起動される度に、そのプログラムが登録済みの正規(シロ)であるかを判定し、実行の許可・拒否を行っています。より詳細に説明しますと、次の通りです。

1.クリーン・イメージの用意:

はじめに、ウイルスを含まない正規プログラム、すなわち、動作させても良いアプリケーションだけで構成される「クリーンな」マスターディスクを作成・用意する。

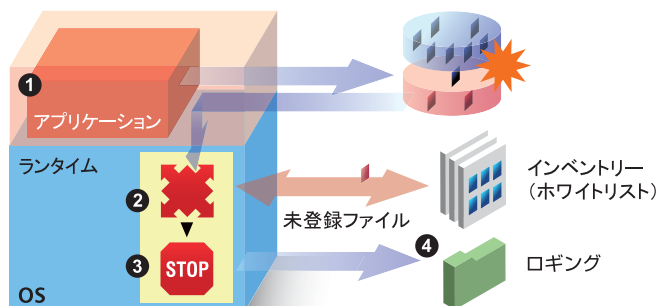
2.ホワイトリストの生成・登録:

次に、このマスターディスクにMESをインストールし、スキャンを行うことで、正規プログラム(シロ)をMES内のホワイトリストに登録する。複雑なプログラミングやパラメーターの設定などは、一切は不要である。

3.ホワイトリスト方式によるウイルス保護実行:

MESを含んだマスターイメージを本番環境に展開し、MESの機能をオンにする。これ以後、新たにプログラムが起動される前に、MESの常駐モジュールがこれをフックし、登録済みのホワイトリストとの照合を行い、正規かどうか(シロかクロか、すなわち、リストに登録されているか、いないか)を判定する。シロなら起動を許可し、クロなら許可しない。

※ 詳細ステップ



- 1 プログラム起動の試み
- 2 ホワイトリスト照合、複数の手法で判断
- 3 ホワイトリストに未登録のプログラムは実行を阻止
- 4 未登録ファイルが起動されようとしたことをリアルタイムに記録

4.ホワイトリストの変更:

アプリケーションの修正・追加といった変更に伴い、ホワイトリストそのものの更新を行う必要が出てくる。このような場合に対して、MESではホワイトリストの変更形式として、セキュリティ署名付きか、Windows Updateなど認定アップデートサービスが配信したもの、管理者・認定ユーザーがインストールする場合に限って変更を認め(MESのロック状態を一時的に解除)、ホワイトリストを自動更新する仕組みを提供している。

このように、ホワイトリスト方式の場合、日々発生する新種のクロを見つけるためのデータベースであるウイルス定義ファイルが不要になります。従って、ウイルス定義ファイルの更新、ウイルススキャン作業といった管理工数が不要です。

「ほったらかしでOK」「古いOSでも使える」「製造業務のジャマにならない」

— アマダの視点から見た「ホワイトリスト方式のメリット」を教えてください。



「ホワイトリスト方式は板金加工機械に向いています」

AMNC自動化ソフト開発部
岡田直人 氏

ホワイトリスト方式の「アマダのお客様(工場ユーザー)にとってのメリット」という視点で説明すると、次のようになると考えます。

メリット1. 余計なウイルス対策管理業務が発生しない ~ ほったらかしでOK

ブラックリスト方式の場合、ウイルス定義ファイル(あるいは対策ソフト本体のバージョン)を常に最新にしないと、最新のウイルスに対応できません。しかし、そのような煩雑なウイルス対策に関連する管理は、工場の生産現場になじみません。一方、ホワイトリスト方式ならば、そうした管理は不要です。工場の皆様は、本来の生産業務に専念できます。

メリット2. ウイルス対策が板金加工機械の動作を阻害することがない

ブラックリスト方式の場合、板金加工機械が高負荷運転をしている真っ最中に、常駐検査や定義ファイルの更新を始めることがあり、そのため機械の運転の支障になることがあります。一方、ホワイトリスト方式の場合、検査はプログラム起動時だけなので、そのような動作障害が起きることがありません。

メリット3. 同じソフトを長期間で継続使用できる

私見ですが、ソフトウェアの世界は、製品寿命が2年~3年程度であるように見えます。「常に最新技術を」「常に最新の状態にバージョンアップを」「足りない点にはパッチ(つぎはぎ)を当てて応急対応」というサイクルで動いているようです。一方、板金加工機械の場合、一度買うと、長年にわたって使い続けます。「安定第一」「枯れた技術がよい」「動く限りは使い続ける」という考え方をとります。

ホワイトリスト方式ならば、先ほどのマカフィーの説明にもあった通り、レガシーOSでも継続的、安定的に使い続けられます。ホワイトリスト方式のウイルス対策ソフトは、製造業の価値観に向いています。

— ほったらかしといっても、板金加工機械を5年、10年と使い続ける中で、アマダ製の機械操作プログラムがバージョンアップされることもありうるかと思うのですが、その場合のホワイトリストの変更作業はどのように実施されているのですか。

MESでは、幾つかのホワイトリスト更新方法を提供していますが、アマダでは、セキュリティ署名の方式を採用しています。

アマダの機器に搭載されるアプリケーションプログラムはすべて当社

が用意するわけですから、これらの一連のプログラムに当社固有のセキュリティ署名を付与しています。また、当社の署名付きプログラムは予めホワイトリストに更新できるポリシーを組み込んでいます。

これにより、サービスマンは、これまでと同じやり方でプログラムの変更を行いつつも、実はその裏では、MESがセキュリティ署名の照合を行い、不正なプログラムは混入しないように、当社のプログラムのみの更新が行われます。要するに、MES搭載による、一切の追加作業をサービスマンに強いることなく、かつ、プログラム更新作業中にセキュリティが低下するかもしれないという不安をお客様に与えることがないわけです。

アマダが板金加工機械のセキュリティ強化に取り組むようになった理由

— アマダが板金加工機械のセキュリティ強化に本格的に取り組むようになった経緯をお聞かせください。

「板金加工機械のネットワーク化に伴い、セキュリティ強化の必要が生じました」

AMNC自動化ソフト開発部
岩野剛 氏



大きくは、「1995年頃を境に、板金加工機械のコンピューター化、ネットワーク化が進み、利便性、生産性が向上しました。その後、2004年ぐらいからでしょうか、その副作用としてウイルス脅威が顕在化してきたので、アマダとして自社製品のセキュリティ強化に注力するようになった」ということとなります。

かつては板金加工機械の操作は、ボタンやレバーで行うものであり、そこにコンピューターは介在していませんでした(この時代には、板金加工機械におけるコンピューターセキュリティは気にする必要がありませんでした)。

しかし、1990年代から、「やがて退職する熟練技術者のノウハウを工場内で継承する必要」が課題として顕在化し、その課題を解決する手段として、「熟練技術者の暗黙知のデータベース化」「そのデータベース(プログラム)を使って、高度な製造を容易に行う」などの手法が注目されるようになりました。

IT化は、まず開発・設計部門で先行し、設計図面はCADにより「データ化」されるようになりました。そうすると、板金加工機械の方にも、そのデータを受け付けるインターフェースが必要になります。こうして板金加工機械の操作部分にもコンピューター(Windows)が搭載されるようになりました。

その後も、製造業のIT化は進展し続け、やがて板金加工機械同士を相互接続する「ネットワーク化」も一般的になり、工場内部の生産性や利便性は大きく向上していきました。

しかし、工場内のネットワーク化の進展は、同時に、インターネットやUSBメモリー経由でのデータ共有を通じて、ウイルスなどのセキュリティ脅威が工場内に侵入する可能性が高まったことをも意味します。こうして、工場内でのセキュリティ強化の必要が顕在化してきました。

工場内でのウイルス被害の例としては、「USB経由でウイルスが工場に侵入すると、ウイルス自身が感染拡大のために攻撃パケットをネットワーク上に流し続けるために、ネットワーク性能が劣化し、システム性能に影響が出た」という事例もあったと聞きます。

ブラックリスト方式の対策に限界を感じた

— 当初、アマダでは、そうしたセキュリティ問題にどのように対処していたのですか。

当初は、「ブラックリスト方式のウイルス対策ソフトウェアによる対策」をお客様に推奨していました。具体的な方法は次の通りです。

1. アマダ側で、市販のブラックリスト型のウイルス対策ソフトが、アマダの板金加工機械で安定動作するかを検証する。
2. 検証済みのソフトウェアを、「アマダ推奨のウイルス対策ソフトウェア」としてお客様に通知する。
3. お客様がその対策ソフトを購入、インストールし、運用する。

しかし、ブラックリスト方式のウイルス対策ソフトを使うこのやり方には、これまで述べた通り、「お客様(工場ユーザー)にとって管理工数がかかる」という問題がありました。また、アマダ側の問題として、ブラックリスト方式のウイルス対策の場合、1、2年で新バージョンがリリースされますので、新バージョンが出る度に、アマダ側で検証を行っていたため、相当な手間がかかっていた。

このような問題を回避するため、アマダでは、ブラックリスト方式に代わる、良い方法を模索していました。そんな折に、取引先を通じて知ったのが、McAfee Embedded Securityでした。説明を通じて、ホワイトリスト方式が、板金加工機械のウイルス対策に非常に向いていることが理解できたので、積極的に検討を開始しました。

OSの基本機能を使っているが…

— ホワイトリスト方式以外に、他の方式を検討したことはありますか。

Windows Embeddedを搭載した機械では従来よりEnhanced Write Filter を使って、ウイルス対策を行っています。このフィルター機能とは、「ウイルスによるディスク書き込みがあったとしても、電源を入れ直せば、ディスクが元の状態に回復する(毎回、まっさらになる)」という方法でした。

この方式の場合、「電源を入れ直せば元に戻るといっても、逆に言えば、電源を入れている間はウイルスが活動し続けることになる。そ

から他のマシンに感染することがありうる」「そもそも板金加工機械は長期間運転で半年間電源を入れっぱなしであることも珍しくない。その場合はウイルスが半年間、活動し続けることになる」などの問題があったため、更なる対策を模索していました。そこでホワイトリスト方式の検討を始めました。

ホワイトリスト方式の製品は、当時、MESともう一社の製品しかありませんでした。二製品を比較検討したところ、MESの方が仕様、機能、実績いずれも優っていたので、これを採用することで、基本方針を決定しました。その後、アマダのWindows搭載型製品の全てで動作検証を実施しました。検証の過程で判明した問題については、都度、メーカーに調整して修正させました。

約1年間の検証の後、「MESがアマダの品質基準を満たしていること」が確認できたので、2010年10月にアマダの製品への標準搭載を会社として決定しました。

その後、2011年1月の初出荷以来、半年後の今に至っており、冒頭でも申し上げた通りの、「お客様にとって手間いらずのセキュリティの確保」を実現するに至っている次第です。

今後の期待

— マカフィーへの今後の期待をお聞かせください。



「マカフィーの今後の支援に期待します」

AMNC自動化ソフト開発部
グループリーダー
成田真庸氏

今回、MESをアマダ製品に標準搭載したことで、板金加工機械のIT化の「影の部分」であるセキュリティ脅威への対処を、お客様に負担をかけない形で、実現することができました。アマダでは、今後とも「お客様にとっての利便性とセキュリティ」を両立した製品を開発していく所存です。マカフィーには、今後とも優れた製品力と技術サポートを通じて、アマダの板金加工機械のセキュリティ向上を支援していただくことを希望します。今後とも宜しくお願いします。

取材日時 2011年6月

 **McAfee** マカフィー株式会社
www.mcafee.com/jp

東京本社 〒150-0043 東京都渋谷区道玄坂1-12-1 渋谷マークシティウエスト20F
TEL: 03-5428-1100(代) FAX: 03-5428-1480

西日本支店 〒530-0003 大阪府大阪市北区堂島2-2-2 近鉄堂島ビル18F
TEL: 06-6344-1511(代) FAX: 06-6344-1517

名古屋営業所 〒460-0002 愛知県名古屋市中区丸の内3-20-17 中外東京海上ビルディング3F
TEL: 052-954-9551(代) FAX: 052-954-9552

福岡営業所 〒810-0801 福岡県福岡市博多区中洲5-3-8 アクア博多5F
TEL: 092-287-9674(代) FAX: 092-287-9675

●製品、サービスに関するお問い合わせは下記へ

McAfeeの英文/和文社名、各商品名、ロゴはMcAfee, Inc.またはその関連会社の商標または登録商標です。本書中のその他の登録商標および商標はそれぞれその所有者に帰属します。©2011 McAfee, Inc. All Rights Reserved. ●製品、サービス、サポート内容の詳細は、最寄りの代理店または弊社事業部までお問合せください。●製品の仕様、機能は予告なく変更する場合がありますので、ご了承ください。

MCACS-ESAM-1107-MC