WebSAM IncidentGuardと認証スイッチによるサイバーアタック対策

江幡 和雅・渡邉 洋子
根津 雄一郎・谷村 聡

要　旨

近年のウイルス/ワームの特徴として、感染力が非常に強く短時間で感染被害が拡大する傾向にあることが挙げられます。そのためウイルス感染拡大への対策のニーズが高まっています。これまで、ネットワークセキュリティ製品WebSAM IncidentGuardはNECのサイバーアタック対策の枠組みの中で、セキュリティ機器と連携したウイルス拡散防止策を提供してきました。そして今回の機能強化により、IEEE802.1X対応認証スイッチとの連携を可能とし、接続時の不正接続防止を認証スイッチで行い、運用中のウイルス拡散防止をIncidentGuardで行うことで、より強固な二重のサイバーアタック対策の提案を可能としましたので、その概要と改善効果について説明します。

キーワード

●サイバーアタック対策　● IEEE802.1X 認証機能

1. まえがき

近年ウイルス/ワーム感染により、企業内ネットワークがダウンし、基幹業務などの各種システムが停止するというような、ビジネス活動停止につながる被害が増加しています。企業にとって利益の損失を防ぐためには十分なサイバーアタック対策を講じることが急務となっています。

従来のサイバーアタック対策としては、検疫ネットワークに代表されるように、端末の接続時に不正な端末やセキュリティレベルの低い端末は一旦隔離し、セキュリティパッチを適用するなど安全な状態にしてから、業務ネットワークへの接続を許可するというソリューションが主流でした。

しかし近年のウイルス/ワームの特徴であるメール感染型ウイルスなどは感染力が非常に強く、セキュリティパッチが提供されるまでの期間より短い時間で一気にネットワーク全体に感染してしまいます。このためネットワークへの接続時の対策だけでなく、接続後の運用中のサイバーアタック対策も併せて重要となってきています。

2. 従来機能の説明

2.1 接続ポート検索・遮断機能

WebSAM IncidentGuard(以下、IncidentGuardと略す)は、NECのサイバーアタック対策製品の一部であり、ウイルス感染端末をネットワークから隔離する製品です。セキュリティ機器と連携させてIncidentGuardを導入することにより、ウイルス拡散防止対策が可能となります。

IncidentGuardの従来機能としては、セキュリティ機器からのイベントに含まれるウイルス感染被疑PCのIPアドレスをもとに、接続されているスイッチのポートを検索する機能、および当該ポートを遮断する機能を提供しています。この検索・遮断処理は、セキュリティ機器からのイベント受信などを契機にオペレータの手動操作によって行います。

具体的な処理の流れを**図1**と合わせて説明します。

① セキュリティ機器からイベントを受信し、検索対象ホストのIPアドレスを抽出する

② ネットワーク内の各L3スイッチのIPアドレステーブルから、検索対象ホストのIPアドレスと同一ネットワークのL3スイッチを求め、そのスイッチのARPテーブルから、検索対象ホストのMACアドレスを求める

③ 各スイッチのMACアドレステーブルに相当するMIB(BRIDGE-MIB)から求めた接続ポート情報、およびディスカバリプロトコルから求めた隣接情報をもとに各スイッチの位置関係を求め、検索対象ホストが直接接続されているスイッチとポートを絞り込む

④ ③で求めたスイッチのポートに対して、ポートの設定状態を操作するMIB(ifAdminStatus)の値を書き換えてリンク

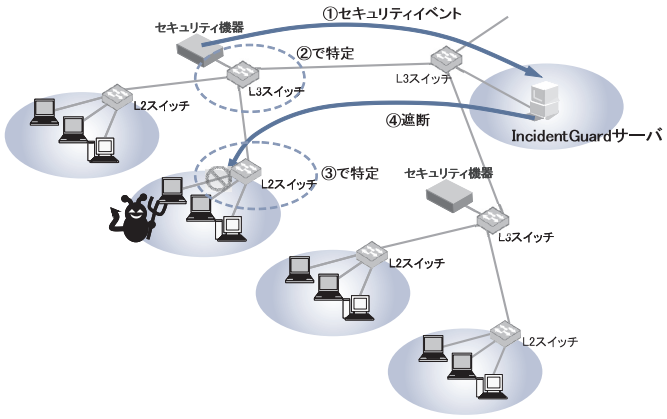

図 1　IncidentGuard の動作イメージ

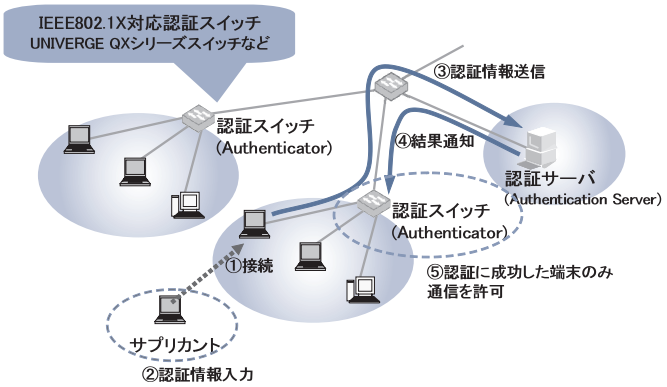

図 2　IEEE802.1X 認証処理の流れ

ダウン状態にする

この処理方式では、ポートを求める際にBRIDGE-MIBを参照していることからBRIDGE-MIB検索方式と呼んでいます。

2.2 IEEE802.1X認証機能

IEEE802.1X認証機能はネットワークへの端末接続時に認証チェックを行う機能です。UNIVERGE QXシリーズスイッチなどのIEEE802.1X対応認証スイッチ(以下、認証スイッチ)を使用することによって、あらかじめ登録されたユーザのみをアクセス許可することが可能になります。

認証処理の流れを**図2**と合わせて説明します。

① 端末を認証スイッチ(Authenticator)に接続する
② 端末上のサプリカントにユーザ認証情報を入力
③ ユーザ認証情報が認証サーバ(Authentication Server)に送信される
④ 認証サーバによる認証結果が認証スイッチに通知される
⑤ 認証スイッチは認証結果に応じてネットワークへのアクセスを制御する

3. 本開発における機能強化

3.1 検索方式の拡大

認証スイッチはIEEE802.1X認証MIBを保持しています。このIEEE802.1X認証MIBには**表**に示す情報などが含まれています。

本開発において、IncidentGuardの検索機能で、従来のBRIDGE-MIB検索方式に加えて、検索精度の向上を目的としてIEEE802.1X認証MIBをもとにした検索も行えるように機能強化を行いました。この新方式をIEEE802.1X認証MIB検索方式と呼んでいます。

IEEE802.1X認証MIB検索方式では、検索対象のIPアドレスからMACアドレスを求める処理は従来と同じですが、検索対象のMACアドレスを持つ端末が接続されたスイッチのポートを求める処理(2.1の③)が以下の③’のように変更になります。

まずIncidentGuardが各認証スイッチから事前に収集しておいたIEEE802.1X認証MIB情報をもとに、検索対象ホストが接続されているスイッチのポートを求めて検索結果の候補とします。その後、求めたスイッチからIEEE802.1X認証MIBを再取得し、検索対象ホストが現時点でも接続されていた場合、当該ポートが正しい検索結果であると判断します。

表　IEEE802.1X 認証 MIB(一部)

項目		詳細
1	名称	dot1xPaeSystem.dot1xPaeSystemAuthControl
	説明	装置全体のIEEE802.1Xポートアクセス制御機能の使用状態 enable(1), disable(2)
2	名称	dot1xPaeAuthenticator.dot1xAuthConfigTable.dot1xAuthConfigEntry. dot1xAuthAuthControlledPortStatus
	説明	当該ポートの現在のIEEE802.1X認証状態 authorized(1), unauthorized(2)
3	名称	dot1xPaeAuthenticator.dot1xAuthStatsTable.dot1xAuthStatsEntry. dot1xAuthLastEapolFrameSource
	説明	該当ポートで最後にIEEE802.1X認証された端末のMACアドレス

*ただし表中のMIB名称は、以下を起点として記載しています。
iso.std.iso8802.ieee802dot1.ieee802dot1mibs.ieee8021paeMIB.paeMIBObjects.

3.2 検索・遮断処理の自動化

従来、IncidentGuardでの検索・遮断処理はオペレータの手動操作によって行っていましたが、今回の開発において、従来の手動操作に加えて、あらかじめ動作ルールを設定しておくことによって、セキュリティ機器からのイベント受信を契機に自動処理することも可能としました。

この機能強化によって、セキュリティ機器からのイベントの中でも特に重要でウイルス感染の可能性が高いイベントをあらかじめルール設定しておくことで、オペレータによる操作を必要とせずにウイルス感染拡大を防止することができます。

4. 本開発による改善効果

今回の開発によって、まずIEEE802.1X認証スイッチにより接続時の不正接続防止を行い、さらにIncidentGuardにより、仮に運用中にメールの添付ファイルなどからウイルス感染が発生しても迅速に感染端末をネットワークから切り離すことでウイルス拡散防止を行うという、二重のサイバーアタック対策の提供が可能となりました。このソリューションによって、持ち込みPCによるウイルス感染だけでなく、接続が許可された後の運用中のウイルス感染拡大という問題点が解決できるようになります。接続時の不正接続防止と運用中のウイルス拡散防止の動作イメージを図3に示します。

通常のネットワーク構成ではディスカバリプロトコルに対応したスイッチを末端に配置することはまれで、通常はノンインテリジェントハブを介して端末を接続しています。そのためスイッチのポートを遮断する場合、同一ハブに接続された複数端末をまとめて遮断せざるを得ないケースが多くありました。この問題点に対して、今回の機能強化により、末端に配置される認証スイッチに対して検索・遮断が行えるように改善したため、ウイルス感染PCのみをピンポイントで遮断することが可能となりました。

またこのように、ネットワークの末端での遮断機能を、センターに配置した運用管理マネージャから一括して行うことが可能になると、セグメントごとにIDPなどの防御装置を配置する必要がなくなるため、安価にサイバーアタック対策を構築することが可能となります。

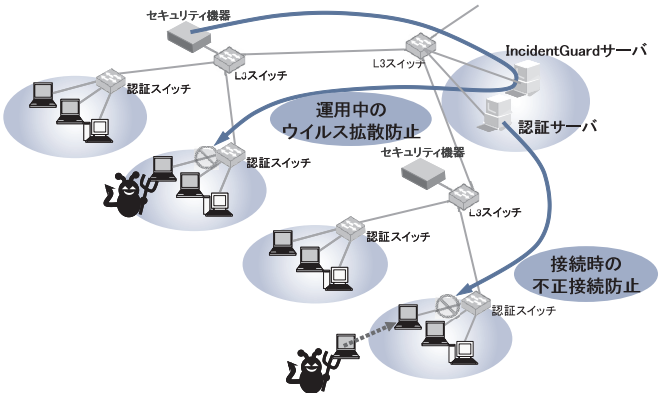

図3 接続時の不正接続防止と運用中のウイルス拡散防止の動作イメージ

5. むすび

以上、「WebSAM IncidentGuardと認証スイッチによるサイバーアタック対策」について概要と改善効果を紹介しました。

本ソリューションにおいて、現状は有線LAN環境に対応していますが、今後無線LAN環境でのウイルス拡散防止策への対応も検討中であり、より幅広いユーザニーズに対応できる製品にするための検討を継続していきます。

不正接続対策、ウイルス拡散防止に対するニーズはますます高まっているため、お客様環境に導入しやすいセキュリティ対策ソリューションを今後も提供していきたいと考えています。

執筆者プロフィール

江幡 和雅
コンピュータソフトウェア事業本部
第一コンピュータソフトウェア事業部主任

渡邉 洋子
NECシステムテクノロジー
プラットフォーム事業本部
ネットワークソフトウェア事業部

根津 雄一郎
NECソフト
プラットフォームシステム事業部

谷村 聡
コンピュータソフトウェア事業本部
第一コンピュータソフトウェア事業部

●本論文に関する詳細は下記をご覧ください。

関連URL:http://www.sw.nec.co.jp/middle/WebSAM/products/IncidentGuard/