vmware®

Empowered by Innovation NEC

デスクトップ仮想化　活用ソリューション

マルウェアから情報を守る マイクロセグメンテーションとは

標的型攻撃の防御には、デスクトップ仮想化＋VMware NSX マイクロセグメンテーションでマルウェアの拡散を防止します。

仮想デスクトップ単位の仮想ファイアウォールで、不審な通信を検知・遮断します。

PC環境におけるマルウェア対策の課題

■未知のマルウェアに感染したPCの遮断　という考え方

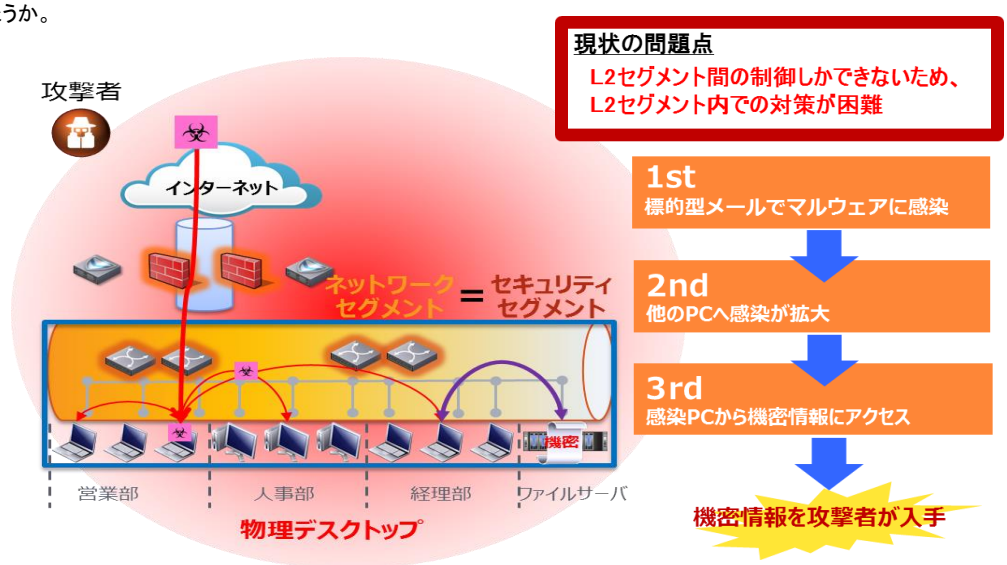
近頃話題の**“職員PCがマルウェアに感染したことにより情報漏えいが発生”**してしまった問題。
セキュリティ体制の強化、対応マニュアル整備、社員・職員の教育など、組織として取り組むべき点はありますが、システムで取り得る対応を考えると**「感染マシンを遮断できていれば被害を最小限に食い止められた」**のではないかと考えられます。マルウェアへの対策としては、一般的に以下が考えられます。

①ウィルス対策ソフトでの検知
ウィルス対策ソフトでマルウェアを検知できれば、感染マシンを自動的に遮断できるのですが、相手が新種のマルウェアの場合などウィルス対策ソフトで検知できないものもあります。

②ネットワーク通信のモニタリング
ネットワーク通信を監視し不審な通信を検知する対策は可能ですが、検知し、アラームを上げるだけでは、マルウェアの感染拡大を防ぎきれません

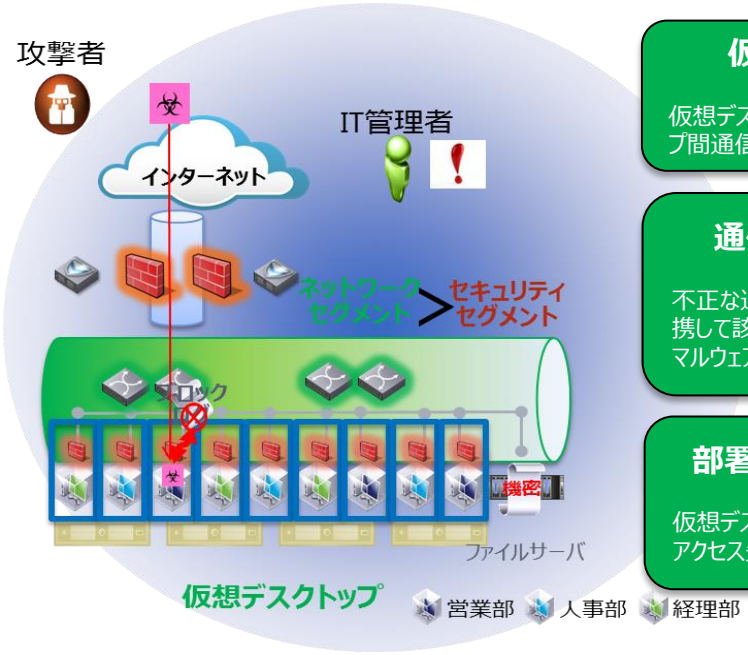
③ネットワークファイアウォールでの通信遮断
②に加えて、ネットワーク上でファイアウォールを設定し、不審な通信を遮断するという対策が必要です。

①②は導入済みだが③は全てのPCに対して適用するには運用が煩雑で対応が難しいため、基幹ネットワークへの接続口や、サーバへのアクセスルート上のファイアウォールのみに設定しているというケースが多く、この場合、今回の様なPCからPCへの感染拡大を防げないのではないでしょうか。



マルウェアから情報を守る マイクロセグメンテーション とは

標的型攻撃への防御
マイクロセグメンテーション ＝ デスクトップ仮想化 ＋ VMware NSX



仮想デスクトップ同士の通信をブロック

仮想デスクトップ単位の仮想ファイアウォールにより、仮想デスクトップ間通信を拒否設定。マルウェア感染拡大を防ぎます。

通信のブロックが発生すると、ログを発行

不正な通信を検知し、管理者への通知やウィルス対策ソフトと連携して該当する仮想デスクトップの隔離を自動的に実行。
マルウェア感染時の被害を最小限に食い止めます。

部署ごとのセキュリティセグメントが分割可能

仮想デスクトップへのログインユーザレベル（ロールベース）で
アクセス先を制御可能です。

感染PCからのマルウェア感染拡大対策として**「マイクロセグメンテーション」**という方法を紹介します。
従来のネットワークセグメントはルータ（とファイアウォール）で区切られており、ネットワーク上のファイアウォールで末端PCの通信まで制御するには限界がありました。
そこで、**「マイクロセグメンテーション」**の出番です。
セキュリティセグメントを従来のネットワークセグメントに依存させずデスクトップ単位まで最小化、デスクトップ単位で仮想ファイアウォール設置することで不審な通信を検知、遮断する解決策です。１台のデスクトップがマルウェア感染した場合でも、デスクトップ毎に仮想で設置したファイアウォールが通信を監視しますので、感染後もデスクトップ間の不審な通信を検知・遮断できるのです。

！ ネットワークセグメントでのファイアウォールでもできる！

いいえ。できません。
アプライアンス型ファイアウォールはネットワークセグメント間でしか機能しません。ネットワークレベルで実装する場合は、すべてのスイッチのポートで、MACアドレスベースのアクセス制御設定が必要で、日々の運用を考慮すると非現実的です。

！ Windows標準のファイアウォールを使えばいい！

ダメです。
OS上で動作するファイアウォール機能では、マルウェアに感染するとOS設定を変更される、または、設定情報を認識してリモートから動作をコントロールされてしまい、不正な通信を遮断できません。

お問い合わせは、下記へ

NEC　プラットフォームソリューション推進本部
E-Mail: contact@pfsl.jp.nec.com

日本電気株式会社　〒108-8001　東京都港区芝五丁目7-1（NEC本社ビル）　2015070301