エンタープライズセキュリティ設計方法

ブルースター株式会社

ブラックリストの考えでは不可能な時代に

インターネット黎明期においては、悪い使い方をする人は少なく善意で成り立っていました。このためブラックリストにより悪い使われ方を防御すれば安全が担保されました。現在では各国で法整備が進んだため、個人による犯罪は横ばいながら、大規模な犯罪組織や国家諜報機関がクラックを行い、高度化が進んできました。

犯罪組織は既知の脆弱性を突き、国家諜報機関は未知の脆弱性を膨大な予算と専門家を投じて活動を行うように変化をしてきました。このためブラックリストによる防御は意味をなさなくなっています。セキュリティの壁は、１つでは容易に破られたため、複数のセキュリティポイントが標的とされる企業や国家に求められるようになってきています。

セキュリティ商品自身に、国家諜報機関によるバックドアが仕掛けられるなど、以前では考えられない状況になっているため、利用者自身に深い知識によるセキュリティ設計が求められています。

一部を止める、手作業で止めるということはもはや不可能

「必要な人が必要なアプリケーションプロトコルを利用し、必要なサーバのみに接続できる環境」

の構築が急務となってきているのです。この実現には「これのみを許可する」というホワイトリスト的な考え方と、物理的に利用を分割した社内ネットワークの敷設が不可欠です。

時代はホワイトリスト方式へ

バックドアをしかけた犯人は誰？

ポート番号32764へ特殊なパケットを送信することで、管理者権限を取得し設定をすべて変更することができるバックドアが、CISCO、Linksys、Netgear等のベンダー製ルータに仕掛けられていることがスノーデンによって言及され、インドのセキュリティエンジニアがそのソースコード部を発見しました。

2013年頃のファームウェアより装備され、現時点でも仕掛けられたままです。

ウイルス対策ソフトは死んだ

毎日平均25.5万件のウイルスが発見され、そのうち82%は新種。

このため既存のセキュリティ対策ソフトは、現状45%しか検知できないとされています。UTMやファイアウオールも同様です。

2014年5月, PC Worldのコラムへシマンテック社の上級副社長が:

“アンチウイルスはもう製品として死んだ”と言及し話題になりました。

“全マルウェアのうち82 %は 1 時間程しか感染が検知されず、70%は一度しか検知されない。” (=亜種の加速的増加)

http://gigazine.net/news/20140507-antivirus-software-is-dead/
http://www.itmedia.co.jp/enterprise/articles/1405/14/news157.html
http://www.newsweekjapan.jp/stories/business/2014/05/post-3271.php

ウイルス対策ソフトにお墨付きがあるのでは？

ウイルス評価機関はテスト検査を目的にした会社が提供しています。100に満たないサンプルを検査にかけ、パスしなかったウイルスをベンダーに提供し、対応策を促します。こうして数回の検査を行った平均スコアをそのセキュリティソフトウェアの「検知率」として公表しています。

毎日平均25.5万件のウイルスで82%が新種であるいま、意味があることなのかということで、検査会社が提供している「認定」についてはボイコットの動きが2013年から業界団体で活発化しています。

完全な中立団体としてセキュリティ業界発展のために中立的に検査を行い、公表しているのは、「VirusBulletin(vb100)」だけです。

マイクロソフト純正のセキュリティ対策機能よりも性能を向上させることができないベンダーはVirusBulletingの検査に参加しなくなってきています。どこのお墨付きを輝かしく公表しているかで、各ベンダーのセキュリティエンジン実態を一部窺い知ることができます。

検査会社によるAV認定事業

トロイの木馬はさらに高度なものへ

従来のトロイの木馬は、
銃のようにＸ線照射のような
仕組みで簡単に判別可能
でした。

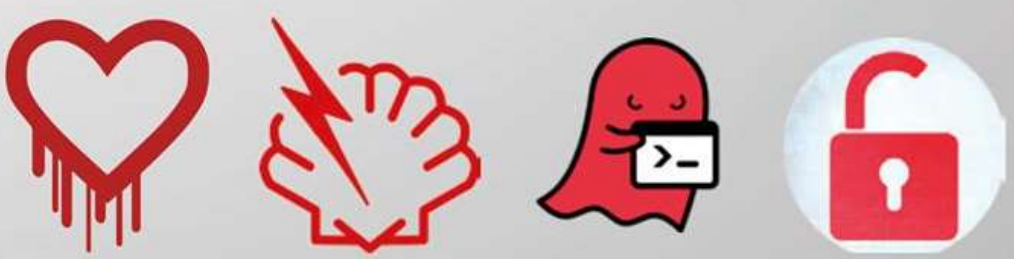
大きな進化

①

現在は、最初に侵入した無害に
見えるアプリケーションが
ある程度の時間経過後に次々に
パーツを自動的にダウンロード。
パーツは、全て無害に見えます。
それらのパーツを統合し、
最終的にスパイウェアになります。

国家諜報機関が当初利用していた技術ですが、大規模犯罪組織にもその技術が知れ渡り、いまや普及してきています。この手法をブラックリストで見破ることは不可能です。
このため、社内には悪意のあるアプリケーションが入り込んだ場合を想定したセキュリティシステムの設計が重要になっているのです。

Linuxベースのファイアウォールは脆弱性リスクが



	Heartbleed	Shellshock/Bash	Ghost	FREAK
Barracuda				
Checkpoint				
Cisco				
Clavister				
Cyberroam		*		
Fortinet				
gateProtect				
GeNUA				
Juniper				
Palo Alto Networks				
Securepoint				
SonicWALL				
Sophos		*		
Watchguard				

LEGEND

- All firewall products affected
- Some firewall products affected
- No firewall products affected
- No information available

Source: Manufactures Web sites

* Products contained or contains the vulnerability but, according to the manufacturer, can not be attacked.

複数のセキュリティ・ポイントで安全性を担保

国家組織によるサイバー戦争に民間企業が巻き込まれています。相手政府は、敵国を混乱させるため、政府機関・電力会社・メディア会社を始め、社会的インパクトが大きくなる企業を既にターゲットにしています。

軍隊と同様に、いくつかのセキュリティポイントを設けて、侵入を防ぎ、侵入されても逃げ出さない仕組みを採用することで始めて安全性が担保されます。

万全を尽くしていたのに漏洩してしまってからでは、会社の信頼・存亡が脅かされます。最終的に破られるか・破られないかの二択しかないのです。

Point 1: 電子メールで標的型を防御

標的型のスパイウェアを完全に防御するのは困難ではありますが、一般的なウイルスは防御することは容易です。狙われやすく情報漏洩されやすい、電子メールクライアントソフトを利用することは大変危険です。特にWindows Liveメールは狙われやすいソフトです。

手法１：クラウドサービスを利用

Google Apps for work, Office 365による法人向け電子メールサービスは、セキュリティ保護機能、迷惑メール対策、オフィス文章のオンライン表示などを持ち、企業内コラボレーションもしやすく、システム管理も不要かつ安価。

Google Apps for Work　Office 365

手法２：ファイアウォールのAV機能を利用

自社サーバやセキュリティ機能のないプロバイダのメール機能に有効。
UTM、NGFWがもつSMTPリレーサーバやPOP3時のAV監査機能を利用し、ウイルスを除去する。除去能力は一般的なレベル。

例：Clavister 次世代ファイアウォール

clavister

手法３：複数のAVエンジンで100%近く脅威を除去

米国州政府、連邦政府、米国発電施設など、高い脅威排除能力を必要とされる施設で利用されているのが複数のAVエンジンを併用し、脅威除去能力を高めたOPSWAT社製MetaScanエンジンを利用する。

OPSWAT.

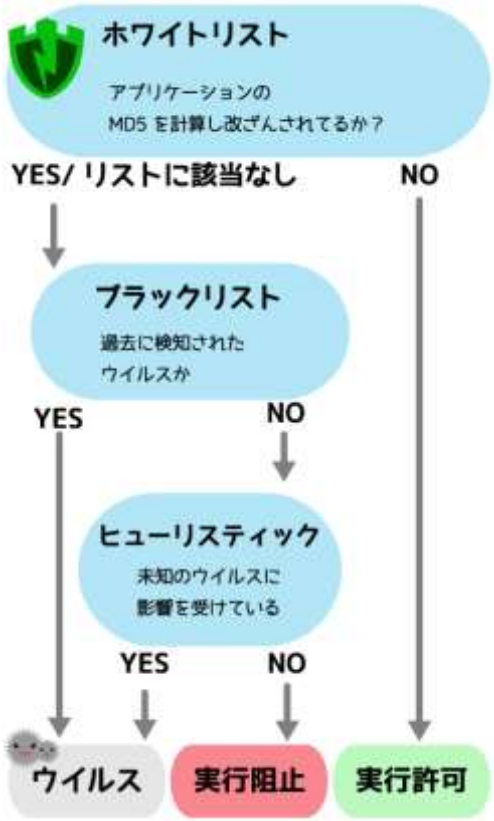
Point 2:未知のウイルスを高く防御するエンドポイント

毎日25.5万件のウイルスが発見され、そのうち82%は新種です。ブラックリスト方式では検知できません。挙動をみるヒューリスティックも、時限型や標的型をうまく発見できません。PC Matic なら、信頼のおける世界中のアプリケーションをホワイトリスト化し、それのみ起動を許可します。このため未知のウイルスやスパイウェアも含めて高い防御能力を実現出来ているのです。他のセキュリティ対策ソフトにはない安心をもたらす３つめのエンジンです。

エンドポイントの感染はシンクライアントでも防御できません。

方法：未知のアプリケーションの起動を全て阻止するエンドポイントセキュリティ

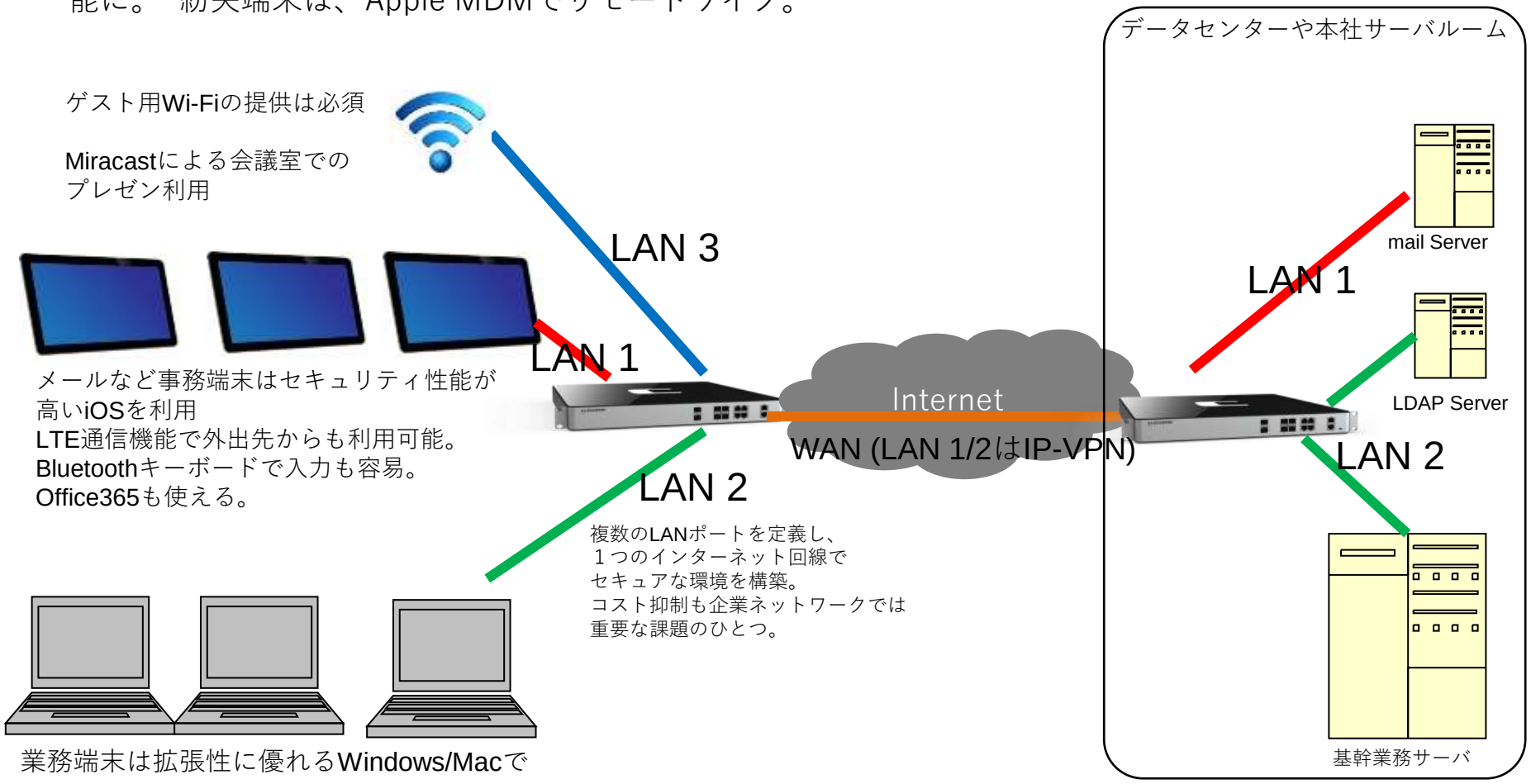
PC Pitstop ピーシーピットストップ ピーシーマチック
PC Matic



Point 3:メール端末(事務)と業務端末のネットを分離

ウェブサービスや電子メールを閲覧する事務端末と機密情報を扱う業務端末のネットワークを物理的に分割。
LAN1とLAN 2 は、どちらへも接続ができない仕様。LAN1/2はインターネットVPNであり、LDAP連携により利用認証を行う。LAN2は限定されたMACアドレスの端末のみ利用可能とし、よりセキュアな運用環境に。

LAN1は、外出先からVPNで社内ネットワークへも入ることが可能で社内メールも出張先から利用可能に。 紛失端末は、Apple MDMでリモートワイプ。



Point 4:社内LANのOSI7層をフル制御

社内LANでは従業員に必要なアプリケーションプロトコルや通信先を限定し、全社員が全プロトコル、到達可能LAN内サーバを利用不可に。

- 従業員毎にアプリケーションプロトコル(http, Mail, SAP会計, SIPプロトコル等)を必要なものに限定し、他のOSI7層の通信利用を禁止。
- 従業員毎にアクセス可能なLANセグメント内のサーバを限定。
- 従業員毎に利用可能な時間帯を限定。
- 従業員毎にVPN利用の可否、利用可能時間帯を制限。

スパイウェアの多くが通常ではない通信を行うため、制限することで多くのスパイウェアの行動を阻止することができます。ただし、ブラウザと詐称し、http通信を行うものも多くありますので注意が必要です。

方法：次世代ファイアウォールを利用する

Point 5:業務端末の脆弱性対策

業務端末の脆弱性対策として、利用アプリケーション、ドライバなど脆弱性を抱えやすいものを強制的にアップデートする機能の実装が必要です。シンクライアントでもこの問題は解決できません。

特にAdobe ReaderやFLASHは脆弱性を抱えやすく狙われています。Word, Excelのスクリプトも脆弱性を抱えやすいものです。

手法　1: Kaseyaを利用する

米国の金融機関の多くで採用されているWSUS機能+アプリケーションアップデート機能をもつKaseyaを利用する。Kaseyaはパソコンの運用保守を自動化する強力なツールでセキュリティに対する自動運転が可能。人的対処では数分から数日間の対処時間を要するが、機械的に行うと瞬間的な対処が可能。

手法　2:PC Matic Pro/MSPを利用する

脆弱性を抱えやすいアプリケーションやドライバの自動更新機能をもつエンドポイントセキュリティ　PC Maticを利用して対処する。

Point 6:脆弱性検査を定期的に行う

脆弱性は毎月500件以上報告されています。これら全てに目を通すのは困難です。このため、これらの情報をもとに脆弱性検査を行う「ペネトレーションツール」の定期的な自社運用が欠かせません。社内ネットワークへビル外から侵入可能とするWi-Fiの脆弱性検査も必須です。

手法　1:安価な自社運用型ペネトレーションツールを利用

日本国内で出回っているペネトレーションツールは、顧客企業がコンサルティングを無償で要求することが多いためか、国際標準価格よりもかなり高額になっています。このため自社運用にはむいていませんでしたが、ブルースター株式会社は、欧州で広く利用されているペネトレーションツールである「Penetrator」を年間使いたい放題で6万円強から提供しています。

【資料】

- PC Matic Pro:ホワイトリスト方式によるエンドポイントセキュリティ

  未知のウイルス防御能力が高く、著名アプリ・ドライバの自動更新機能を装備

  http://www.blue.co.jp/products/pcmaticmsp/PCMatic_Pro.pdf
- Clavister:次世代ファイアーウォール

  アプリケーション層を用いて利用可能アプリを制限可能。LANセグメントを複数持つことができセキュリティ性能を格段に高めることができる。

  http://clavister.blue.co.jp/resources/pdf/clavister.pdf
- Penetrator:脆弱性検査ツール（ペネトレーションツール）

  6万件を越す脆弱性情報と毎月500件の新規脆弱性情報を検査することができるツール。ビル侵入なしにネットワークに入ることができるWi-Fi脆弱性検査も可能。

  http://www.blue.co.jp/products/secpoint/SecPoint.pdf
- Kaseya:パソコン自動運用ツール

  世界中の金融機関にて活用されているパソコン自動運用ツール。IBM Tivoli, 日立JP1に相当する製品だが、Lua Scriptによりパソコンに異常が発生した場合の対処を記述することができ運用の自動化と迅速化が可能。

  http://kaseya.blue.co.jp/kaseya.pdf
- OPSWAT Metascan:複数アンチマルウェアによる高防御能力アプライアンス

  複数社製のアンチマルウェアエンジンを搭載し、検知率を極限にまで高めた国家間サイバー戦争時に狙われやすい政府機関、発電施設向けの攻撃型メール対策のメールゲートウェイ向けセキュリティエンジン。

  https://www.opswat.com/products/metascan/explore