TOPICS

学校法人駒澤大学様のOSV-VHD boot導入事例を公開!

当社ホームページに、学校法人駒澤大学様へのネットワークブートPCシステム「OSV-VHD boot」導入事例を公開しました。同大学は別校舎で運用されていたPC教場を新校舎へ移転すると同時に、ネットブートPCシステムのOSをWindows10にアップグレードすることになりました。Windows10では更新ポリシー「Windows as a Service（WaaS）」でどのモデルを選択するかがポイントとなりますが、当社のご提案を採用いただき、安定的に利用できる環境を実現されました。

詳しくは当社HP内の導入事例をご覧ください!
https://is-c.panasonic.co.jp/case/144/

QRコードからもアクセスできます

「ArgosView」がパナソニックの「i-PRO EXTREME」全機種に対応

当社の連結子会社であるヴイ・インターネットオペレーションズ株式会社は、映像監視システム「ArgosView（アルゴスビュー）」を、パナソニック株式会社製カメラ「i-PRO EXTREME」シリーズの全機種に対応しました。高い映像識別性能、データ高圧縮といった特長を有する「i-PRO EXTREME」シリーズに「ArgosView」を組み合わせることで、暗所や遠方の監視精度を高めたり、録画コストや映像データの保管スペースを大幅に抑えることが可能となります。

イベント・セミナー予定

東京地区

経理を驚くほどラクにする!
経費精算から始める
ペーパーレス化推進セミナー

日時｜7月19日（木）15:30～17:30
場所｜東京オフィス　セミナールーム

大阪地区

点検・保守・修理作業員のための超速!
報告書作成セミナー

日時｜7月13日（金）15:00～17:20
場所｜梅田オフィス　セミナールーム

名古屋地区

RPA×EAIで働き方改革

日時｜7月20日（金）14:30～16:30
場所｜中部営業所

詳しくは
https://is-c.panasonic.co.jp/event/
をご覧ください!

あいえす☆プロフェッショナル vol.10

「何が最適かはお客様によって千差万別です」と語るのは、エンタープライズソリューション事業部 クラウド・運用サービス部　ユニットリーダーの上本健太郎。端末展開、ネットワーク運用、サーバ運用など多彩なキャリアを経て、現在はセキュリティのプリセールスを担当しています。これさえしておけば間違いないセキュリティ対策ってありますか?「幾重にも防御壁を設ける『多層防御』が推奨ですが、二重、三重にすれば完璧だとは言い切れません。
お客様の既存の環境を見て、脆弱な部分に対策を施すか、あるいは多層的にプラスするか、予算感も考慮してご提案するのが我々の腕の見せ所だと考えています」。

そう語る彼がお客様との打ち合わせで心掛けているのは「少し突っ込んで聞くこと」。「聞きづらいことも一歩踏み込んでみるようにしています。もしかすると空気を読んでいないかもしれません…（笑）。でも、結果としてお客様のご事情を伺うことができ、その後のコミュニケーションがスムーズに運ぶことが多い気がします」。
自らのお役立ちも、一歩踏み込んでアプローチするのが彼の「現場力」。「幸い色んな分野を経験してきたので、セキュリティの領域だけにとどまらず、例えばネットワーク構成もチェックするなど広い目線で会話するようにしています。そうすることでお客様に対しトータルに貢献できれば」と教えてくれました。

「現場力」とは…

一歩踏み込むこと。
空気を読まず突っ込んで聞いたり、自らの担当領域にこだわらず考えることが、お客様にとってのお役立ちにつながると思っています。

エンタープライズ
ソリューション事業部
クラウド・運用サービス部
ユニットリーダー
上本 健太郎

編集後記

「彼を知り己を知れば百戦殆(あや)うからず」というのは孫子の有名な言葉。
サイバーキルチェーンの「キルチェーン」も元々は軍事で使われる概念だそうです。
敵を知ることの重要性は古代中国から現代に至るまで不変なんですね。
さて、私の目下の敵は衰えることのない食欲です。そろそろビアガーデンの季節、ビールが美味しいと一緒に食べるごはんも美味しいわけで…。攻略法が見当たりません。

発行元
パナソニック インフォメーションシステムズ株式会社
営業統括部 企画管理チーム
〒140-0002 東京都品川区東品川2-3-14 東京フロントテラス18F
TEL:03-5715-5470 FAX:03-5715-5471 https://is-c.panasonic.co.jp/

Panasonic

アイエスクローズ アップ

IS CLOSE UP

パナソニック インフォメーションシステムズ株式会社

2018.6 vol.60

サイバーキルチェーンから学ぶ

標的型攻撃 効果的な備え

TOPICS

学校法人駒澤大学様の
OSV-VHD boot導入事例を公開!

「ArgosView」がパナソニックの
「i-PRO EXTREME」全機種に対応

あいえす☆プロフェッショナル

エンタープライズソリューション事業部
クラウド・運用サービス部
ユニットリーダー
上本 健太郎

Close Up NOW

サイバーキルチェーンから学ぶ

標的型攻撃 効果的な備え

攻撃者の視点に立てば 対策のヒントが見えてくる!

特定の団体や人物をターゲットとして仕掛けられる「標的型攻撃」。
年々巧妙化、複雑化が進み、守る側の対策が追いつかないほどですが、
一度攻撃者の視点に立ってみませんか?
攻撃者の一連の活動をモデル化した「サイバーキルチェーン」を
知ることで、対策のヒントが見えてくるはずです。

まずは敵を知ろう。標的型攻撃のフロー「サイバーキルチェーン」

サイバーキルチェーンは上の図にあるように「偵察」「武器化」「配送」「攻撃」「インストール」「遠隔制御」「目的達成」の7段階であり、具体的には「事前調査」「標的型攻撃メールの送付」「C&Cサーバ※による遠隔制御」「情報の盗み出し」として考えることができます。一昔前は「侵入させない」セキュリティ対策が主流でしたが、サイバー攻撃の高度化、巧妙化が進むにつれて、それだけでは防御しきれなくなってきました。そのため、現在では「侵入前提」の考え方が主流となっています。

サイバーキルチェーンを意識した標的型攻撃対策では、網羅的な防御がポイントとなります。まず侵入を防ぐ入口対策として、不審なファイルからマルウェアを検知する機能。次に、感染拡大を防ぐ内部対策としてアクティビティログの監視、分析機能。そして外部流出を防ぐための出口対策には、マルウェアのC&C通信をブロックする機能が有効です。

標的型攻撃対策のポイント

- ☑ **入口対策** …侵入を防ぐ
- ☑ **内部対策** …感染拡大を防ぐ
- ☑ **出口対策** …外部流出を防ぐ

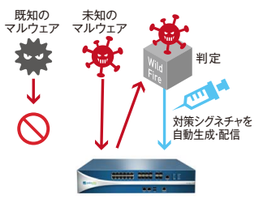
網羅的に対策することが重要です!

パナソニックISのご提案する標的型攻撃対策

入口対策 マルウェアの侵入を防ぐ

新種のマルウェアも防げる 次世代ファイアウォール「Palo Alto」

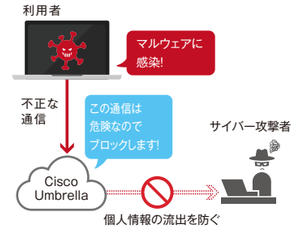
不審なファイルをクラウド上の仮想環境で実行しマルウェアかどうかの判定を行います。マルウェアだった場合、検知後約30分以内に対策シグネチャを自動生成するため、未知のマルウェアに迅速に対応することができます。導入後のレポーティングサービスもパナソニックISが行います。



出口対策 マルウェアのC&C通信をブロック

万一マルウェアに侵入されても セキュアDNS「Cisco Umbrella」で動作をブロック

マルウェアの侵入に成功した攻撃者は、C&C通信でマルウェアを遠隔操作しようとします。万一マルウェアに感染したとしても、「Cisco Umbrella」がこのC&C通信を停止し、マルウェアの動作を途中でブロックします。



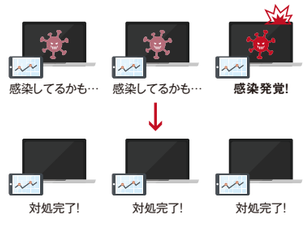
内部対策 侵入を迅速に察知し感染拡大を防ぐ

潜入するマルウェアの 不審な動きを「Splunk」が察知

マルウェアはウィルス対策ソフトに痕跡を残さず侵入・攻撃することも少なくありません。「Splunk」は大量のデータをマシンラーニングで解析し「正常値」を学習するので、異変の発生を容易に検出できます。

エンドポイントの感染経路と観戦範囲を特定する 「Trend Micro Endpoint Sensor」

エンドポイント(サーバ・PC・スマートフォンなどの端末)のアクティビティログを記録し、ネットワークセキュリティ側の情報と組み合わせて感染経路と感染範囲を特定します。感染が顕在化した端末以外にもマルウェアが潜んでいないか確かめることができます。



※C&C(Command and Control)サーバ:マルウェアに感染したコンピュータに対し指示・制御を行うサーバ。