SecuAvail

［セキュアヴェイルニュース］

SECUAVAIL NEWS

セキュリティ運用監視サービスのセキュアヴェイルがお届けする、
情報セキュリティ向上に役立つフリーペーパー

Vol.11
2017.7

導入事例

次世代ファイアウォールの膨大なログを使いこなす！

誌上セキュリティセミナー
セキュリティ啓発 .. ログの「監視」と「管理」を知る

「EternalBlue」、現在もマルウェアの拡散に悪用
米セキュリティ企業が確認

NEWS

セキュリティ情報

「EternalBlue」、現在もマルウェアの拡散に悪用

米セキュリティ企業が確認

世界中に拡散し被害を及ぼしたランサムウェア「WannaCry」の被害拡大の一因となった、WindowsOSの特定バージョンの脆弱性を悪用するツール「EternalBlue」が、現在もマルウェアの拡散に使われていることが、米セキュリティ企業・FireEyeの発表で明らかになりました。

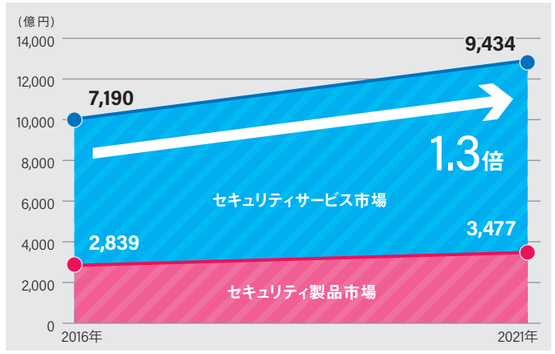
「EternalBlue」は、もともとは米国家安全保障局（NSA）が開発したツールで、何者かが流出させたとみられています。Windowsのファイル共有プロトコルの実装に関する脆弱性を悪用し、標的のコンピュータ上で任意のコードを実行できるようにします。FireEye社のブログによると、コンピュータにバックドアを作成する「トロイの木馬」や、データ窃取やコンピュータ乗っ取りが可能なマルウェアの拡散に、「EternalBlue」とVBスクリプトの組み合わせが使われているのを、それぞれシンガポールと東南アジア地域で確認したとのこと。今後数週間、あるいは数ヶ月にわたり、この脆弱性を悪用したさらなる攻撃や感染拡大が予想されるとしており、マイクロソフト社が配布しているセキュリティパッチの早期適用を呼び掛けています。

セキュリティサービス市場、21年には9,500億円規模に

IT専門の調査会社・IDC Japanはこのほど、国内情報セキュリティ市場に関する2016年から2021年までの予測を発表しました。運用管理をはじめとしたセキュリティサービス市場は、2021年には2016年の約1.3倍の9,434億円に拡大するとしています。

同社によると、国内セキュリティサービス市場の2016年の市場規模は7,190億円（前期比5.1%増）。2021年までの年間平均成長率は5.6%になるとの見通しです。一方、ソフト・ハードを合わせたセキュリティ製品市場は、2016年の2,839億円（前期比5.1%増）から、2021年には3,477億円になると予測しています。

5月に施行された改正個人情報保護法や高度化するサイバー攻撃の影響が2017年の成長の背景となり、2018年以降は、東京オリンピックに向けての社会インフラ防御や個人情報保護対策強化への動きが需要を支えるものと、同社ではみています。特にセキュリティサービス市場では、高度な専門知識を必要とするセキュリティサービスや、クラウド環境へのセキュリティ対策の導入・構築・運用サービスへの需要が拡大するとのことです。



国内情報セキュリティ市場の2021年までの成長予測
（IDC Japan株式会社の発表資料にもとづき当社が作成）

NEWS

セキュアヴェイルからのお知らせ

セキュリティ人材を育成・派遣

新子会社「キャリアヴェイル」を設立

当社は、情報セキュリティに精通した人材の育成・派遣等を行う新会社「株式会社キャリアヴェイル」（本社：東京都中央区、代表取締役社長：神戸仁）を設立しました。労働者派遣事業の許可取得後、9月より事業を開始します。

不足するセキュリティエンジニアを、独自プログラムで育成・派遣

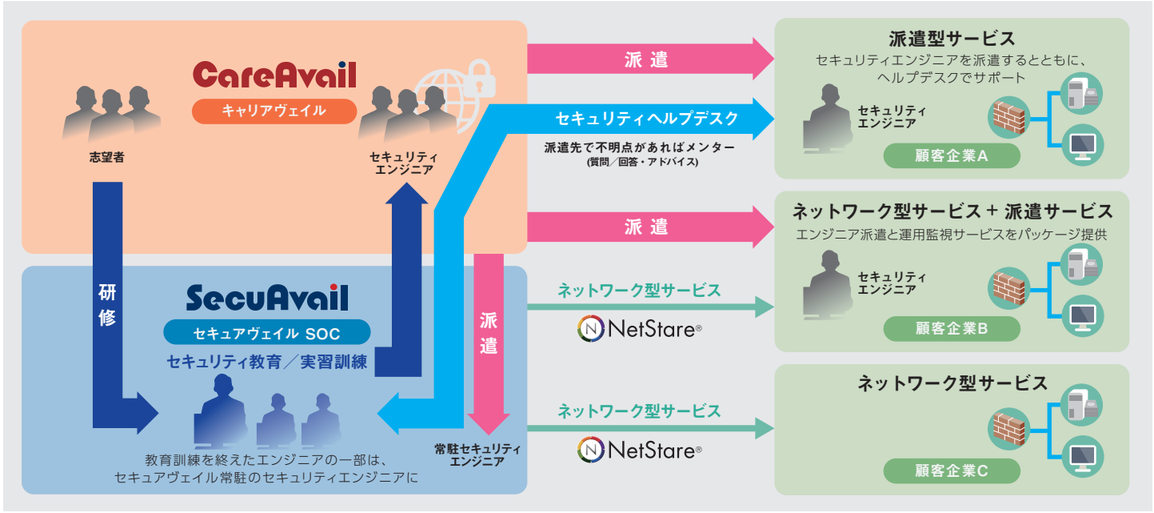
企業などで情報セキュリティに携わるエンジニアの需給は、現時点でも既にかなり逼迫しています。経済産業省の調査によると、2016年時点で既に13万2,000人が不足しており、2020年にはそれが19万3,000人にまで拡大する見通しです（同省「IT人材の最新動向と将来推計に関する調査結果」より）。

一方で当社は2001年の創業以来、SOC（セキュリティ・オペレーション・センター）をはじめとした多様なセキュリティ対策支援サービスを、自社スタッフで運用してお客さまに提供し続けており、その過程でセキュリティ専門エンジニアの育成ノウハウを確立しています。

派遣＋サービス提供の“ハイブリッド”も

そこで、新会社を通じてセキュリティ専門エンジニア志望者を集め、当社で育成プログラムや実習訓練を実施。一定の技術レベルに育てたあと、新会社から当社顧客企業などに派遣し、セキュリティ対策に当たらせます。
当社の運用監視サービスやヘルプデスクサービスと新会社のエンジニア派遣を組み合わせた“ハイブリッドサービス”も、導入を視野に入れています。

このほか、ソフトウェア開発エンジニアの育成・派遣、営業スタッフ、事務スタッフの派遣も手掛けていく方針です。



「キャリアヴェイル」提供サービスのイメージ図
キャリアヴェイルで採用したスタッフをセキュアヴェイルで教育訓練、セキュリティエンジニアに育成

SEMINAR

誌上セキュリティセミナー

セキュリティ啓発..ログの「監視」と「管理」を知る

株式会社セキュアヴェイル 取締役　神戸 仁

グランフロント大阪・コングレコンベンションセンター（大阪市北区）でこのほど開催されたITイベント「セキュリティ関西2017」（日経BP社主催）において、当社の神戸仁取締役が講演を行いました。

テーマは「セキュリティ啓発..ログの「監視」と「管理」を知る」。セキュリティ対策の第一歩目に当たるログ管理で、まず手掛けるべきことは何か。その要諦は、意外なところにありました。
以下の講演録より、ご確認下さい。

約100人の聴衆でにぎわった会場

対策から入らない。現状把握から入る

セキュリティについては、必要かどうかでなく、「何を／どの程度／どの順番で／どのくらいの費用でやるか」だと捉えて下さい。最新のセキュリティ技術と言っても、ベンダーにとって新しいだけ。最新の情報はベンダーが作っているだけなんです。それが役に立つのか、使うべきかどうか、ジャッジするのはあなた方です。

正しいセキュリティ対策の考え方は、理想があって、現実があって、現実を理想にどう近付けるか。企業経営でも何でも一緒です。

ここで、視点を変えてみましょう。

医療行為では、問診をして検査をして、精密検査からさらに検査入院までします。調べて調べて、こういう症状だから薬か手術か、ということを決める。にも関わらずセキュリティでは、どうも対策から入りがちです。それはおかしい。医療なら、膨大な臨床データベースから数値を比較して、原因や病名を特定してから治療します。

セキュリティも同様です。では、何をもって現状を把握すべきか。

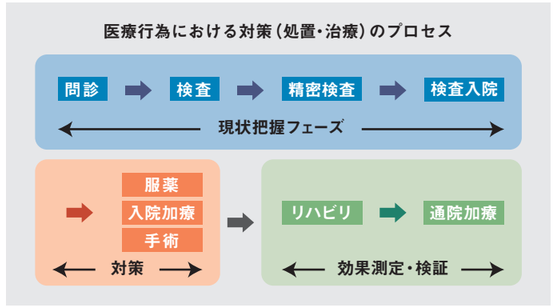


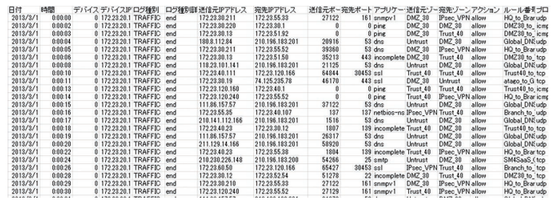
図1　医療もセキュリティも、プロセスは同じ。

それは、ログでしか分かりません。今あるものがちゃんと稼動しているか、脅威を遮断できているか、あるいはオーバースペックではないか。ログ分析・管理なしでは、現実的に判断のしようがないのです。セキュリティ対策のまさに第一歩が、ログ分析・管理です。

数字を見るのではなく、数字の意味を知る

さて、ログ管理の実践です。

ログは見やすくしてもこんな感じ（=**図2**）で、これがまた膨大にあります。一方、レポート（グラフ）にまとめると（=**図3**）、数値が多い所、少ない所に目が行きがちですが、そもそもプリンタ5台を導入するときに月間出力25,000枚を想定していたとしたら、想定外なのは枚数の少ない4台の方になりますね。どこを見るか、何を基点にするかで、ログの見方は全く変わります。



日付	時間	デバイス	デバイスIF	ログ種別	ログ種別詳細	送信元IPアドレス	宛先IPアドレス	送信元ポート	宛先ポート	アプリケーション	送信元ゾーン	宛先ゾーン	アクション	ルール番号	プロ
2013/3/1	0:00:01	0	172.23.20.1	TRAFFIC	end	172.23.30.211	172.23.55.33	27122	161	snmp-1	DMZ_30	IPsec_VPN	allow	HQ_to_Branch	udp
2013/3/1	0:00:02	0	172.23.20.1	TRAFFIC	end	172.23.30.220	172.23.30.1	0	0	ping	DMZ_30	DMZ_30	allow	DMZ30_to_ic	ms
2013/3/1	0:00:03	0	172.23.20.1	TRAFFIC	end	172.23.30.13	172.23.51.50	0	0	ping	DMZ_30	Trust_40	allow	DMZ30_to_ic	ms
2013/3/1	0:00:04	0	172.23.20.1	TRAFFIC	end	180.8.112.84	210.196.183.201	20916	53	dns	Untrust	DMZ_30	allow	Global_DNS	udp
2013/3/1	0:00:05	0	172.23.20.1	TRAFFIC	end	172.23.30.211	172.23.55.52	39360	53	dns	DMZ_30	IPsec_VPN	allow	HQ_to_Branch	udp
2013/3/1	0:00:06	0	172.23.20.1	TRAFFIC	end	172.23.30.13	172.23.51.50	35213	443	incomplete	DMZ_30	Trust_40	allow	DMZ30_to_ic	tcp
2013/3/1	0:00:08	0	172.23.20.1	TRAFFIC	end	118.23.181.141	210.196.183.201	21125	53	dns	Untrust	DMZ_30	allow	Global_DNS	udp
2013/3/1	0:00:11	0	172.23.20.1	TRAFFIC	end	172.23.40.111	172.23.120.166	64044	38453	ssl	Trust_40	Trust_40	allow	Trust40_to_	tcp
2013/3/1	0:00:11	0	172.23.20.1	TRAFFIC	end	172.23.30.19	74.125.235.78	46170	443	ssl	DMZ_30	Untrust	allow	ataqs_to_G	tcp
2013/3/1	0:00:13	0	172.23.20.1	TRAFFIC	end	172.23.120.160	172.23.40.1	0	0	ping	Trust_40	Trust_40	allow	Trust40_to_ic	ms
2013/3/1	0:00:14	0	172.23.20.1	TRAFFIC	end	172.23.120.240	172.23.55.52	0	0	ping	Trust_40	IPsec_VPN	allow	HQ_to_Branch	ms
2013/3/1	0:00:15	0	172.23.20.1	TRAFFIC	end	111.86.157.57	210.196.183.201	37122	53	dns	Untrust	DMZ_30	allow	Global_DNS	udp
2013/3/1	0:00:16	0	172.23.20.1	TRAFFIC	end	172.23.55.35	172.23.40.107	137	137	netbios-ns	IPsec_VPN	Trust_40	allow	Branch_to_	udp
2013/3/1	0:00:17	0	172.23.20.1	TRAFFIC	end	210.141.112.166	210.196.183.201	1516	53	dns	Untrust	DMZ_30	allow	Global_DNS	udp
2013/3/1	0:00:18	0	172.23.20.1	TRAFFIC	end	172.23.40.23	172.23.30.12	1807	139	incomplete	Trust_40	DMZ_30	allow	Trust40_to_	tcp
2013/3/1	0:00:19	0	172.23.20.1	TRAFFIC	end	111.86.157.57	210.196.183.201	26317	53	dns	Untrust	DMZ_30	allow	Global_DNS	udp
2013/3/1	0:00:20	0	172.23.20.1	TRAFFIC	end	211.129.14.166	210.196.183.201	58920	53	dns	Untrust	DMZ_30	allow	Global_DNS	udp
2013/3/1	0:00:22	0	172.23.20.1	TRAFFIC	end	172.23.40.23	172.23.55.38	1884	139	incomplete	Trust_40	IPsec_VPN	allow	HQ_to_Branch	tcp
2013/3/1	0:00:24	0	172.23.20.1	TRAFFIC	end	218.230.228.148	210.196.183.208	54266	25	smtp	Untrust	DMZ_30	allow	SMRGate5_0	tcp
2013/3/1	0:00:26	0	172.23.20.1	TRAFFIC	end	172.23.60.50	172.23.120.166	65427	38453	ssl	IPsec_VPN	Trust_40	allow	Branch_to_	tcp
2013/3/1	0:00:28	0	172.23.20.1	TRAFFIC	end	172.23.30.12	172.23.53.54	51278	22	incomplete	DMZ_30	Trust_40	allow	DMZ30_to_	tcp
2013/3/1	0:00:29	0	172.23.20.1	TRAFFIC	end	172.23.30.210	172.23.55.33	27122	161	snmp-1	DMZ_30	IPsec_VPN	allow	HQ_to_Branch	udp
2013/3/1	0:00:30	0	172.23.20.1	TRAFFIC	end	172.23.120.240	172.23.55.52	27129	161	snmp-1	Trust_40	IPsec_VPN	allow	HQ_to_Branch	udp

図2　典型的なログの生データ

人間、ログのレポートを見ると、つい隣同士を比較して、平準していないところを異常と見がちです。でもログでは普通、そこまで突出したデータは出ません。余り差のないデータを眺め続けるうちに、飽きてログ自体を見なくなるのも、また人間。

ログは単に見るのではなく、それが表している意味を「知る」ことが大事なんです。具体的には、①「定義」付けをして②良否の「基準」を決め③環境／状況の変化に応じて「定義」を再設定すること、です。

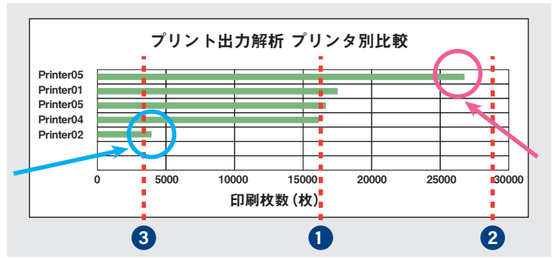


図3　プリンタの月間出力枚数を比較したグラフ

結果を見てジャッジし、次の「PLAN」に繋げる

ログマネジメントサイクル。こういう考え方があるということを、今日は持って帰っていただきたい。いわゆる「PDCA」を、ログに応用したものです。

「P」ではどこを見るのかを決め、「D」ではログレポートを実装、「C」ではアラート基準を定めて、「A」で結果をちゃんとジャッジする。

「A」は一般には「Action」ですが、今回は「ジャッジ」です。そこから次の「P」に繋げないと、サイクルは回りません。

ここで大切なのは、どのログを捨てるのかということ。不要なデータを捨てないと、見つけたいものが見つかりません。

九州のある市役所では、「1セッションで10GB以上の通信を異常とする」と定義したところ、9割は不要なログとなりました。

データの要・不要を判断するには、まず仮説を立てることです。例えば、標的型メール攻撃を検知するのにはどうすべきか。深夜にどこかにアクセスしている、起動アプリがそれまでと変わる、同一サーバ（C&Cサーバ）にずっとアクセスしている、など、兆候は色々あります。まず、どの兆候でアラートを鳴らすべきか仮説を立ててやってみて、駄目なら指標を変えていく。これがログマネジメントサイクルを回すための、基本的な姿勢です。

このような取り組みを進めていくと、最終的には、理想的なログレポートは「白紙」となります。

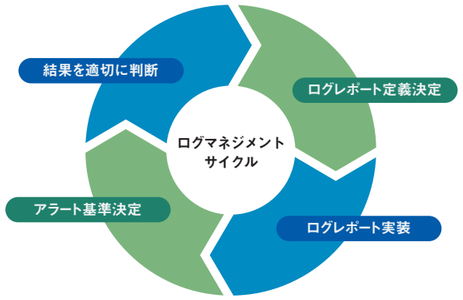


図4　ログマネジメントサイクル

シンプルなログマネジメントは、不要なログを捨てることから

最後にまとめます。

- 「ログ」で正しく現状把握をして、するべき対策を導く。
- ログは見ない。知ること。理解することが重要。視点を思考を変えて…。
- ログマネジメントサイクルを運営する。定義付けと適切な判断。
- 定義は環境／状況に応じて変えること。これがログ管理をする本質的な意味。
- 不要なログは何か..という視点がシンプルなログマネジメントになる。

神戸 仁 取締役

ご清聴ありがとうございました。

CASE

導入事例

次世代ファイアウォールの膨大なログにも対応、セキュリティのレベルアップサイクルの構築へ

株式会社大阪チタニウムテクノロジーズ さま

日本で初めてスポンジチタンの工業化に成功した、株式会社大阪チタニウムテクノロジーズさま（以下、同社）。高純度・高品質の素材供給を通じ、世界の航空宇宙産業やエレクトロニクス産業などを支えています。それだけに、同社の業務を支えるネットワークシステムに万一の事態が起これば影響は広範囲に及びかねず、セキュリティの維持強化は”永遠の課題”。そこで選ばれたのが、セキュアヴェイルのネットワーク運用監視サービス「NetStare®」でした。

課 題

- ☑ 次世代型ファイアウォールで質・量ともに増えるログに対処し切れるか？
- ☑ 機器の設定を適切なタイミングで変えていけるか？

成 果

- ☑ 定期的なログ解析レポートで、多忙なご担当さまをサポート。
- ☑ 脆弱性検査や設定変更提案を通じ、セキュリティのレベルアップサイクルを構築。

海外ハッキンググループの脅威を受け、侵入防御から通信検知へ

同社で動いているサーバは、インフラ、業務系を含め約130台。その多くが兵庫県尼崎市の本社にあり、ファイアウォール経由でインターネットに接続されています。

「以前はセキュリティについては、侵入防御を基本とする考え方でした」と語るのは、同社システム部長の三角龍平さん。

「考え方が変わったのは、2015年の日本年金機構の情報漏えい事件から。危機感を抱いて調べているうちに、海外には強力な（ハッキング）グループがいることが分かってきました」（三角さん）。

海外のハッキンググループの中には、企業の先端技術情報などを集中的に狙うグループがあり、素材系ハイテク企業として国内外から知られる同社も標的とされる恐れがあります。

「巧妙化する昨今の標的型メール攻撃を見ていると、攻撃を100%防ぐのは困難ではないか、と思えてきました。そこで侵入防御に加え、（侵入したマルウェアなどが社内から発する）不正通信検知に重きを置かねば、と思うようになったんです」（三角さん）。

大阪チタニウムテクノロジーズ
兵庫県尼崎市／チタン・シリコン素材の製造


システム部長　三角龍平さん


システム部システムグループ
若林健太郎さん

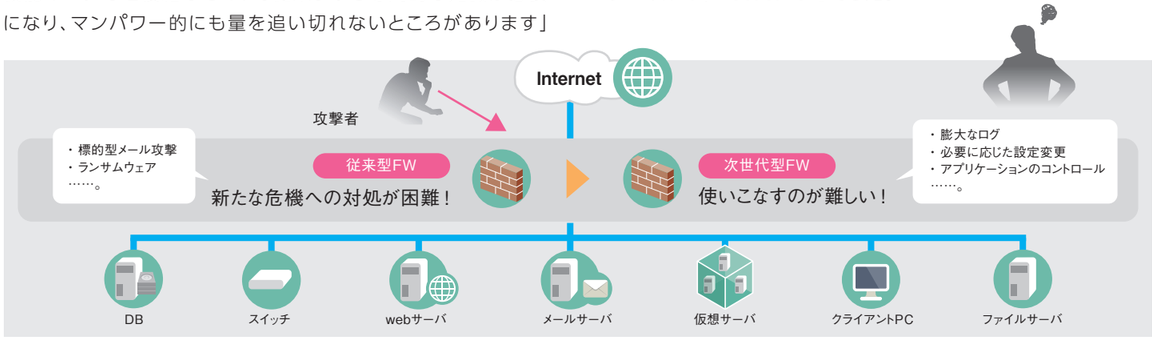
複雑化するログ解析や設定変更をどうする？

部内での協議の結果、「新しいタイプのファイアウォール装置を使い、通信の中身を分析し、攻撃の兆候を捉えよう」（三角さん）という方針が決まりましたが、そこには問題が。アプリケーション制御機能などを搭載した次世代型ファイアウォールは、ログが量・質ともに複雑化するのです。

「一日のログの量は、次世代型は旧型の3～5倍。1日100MB級だったのが、1GB以上になります。質的にも、従来のIPアドレスやポート番号でのブロックログからIPS（侵入防止システム）機能のログなど複雑なものに。従来よりも専門的な知識が必要になり、マンパワー的にも量を追い切れないところがあります」（同社システム部システムグループ　若林健太郎さん）。

加えて「機器の設定も、一度やれば終わりではありません。その時々の攻撃側に合わせて設定を変えねばならず、現場にとってはかなりの負荷です。一方で設定変更のタイミングを間違えれば、脅威に対し後手に回りかねない」（三角さん）。

このほか、技術レベル、サービス内容、緊急時の即応性、将来的なサービス拡張性、価格と、検討すべきポイントは多岐に亘ります。悩んだ末、三角さんや若林さんが最後に選んだのが、セキュアヴェイルの「NetStare®」でした。



ログ解析で見つかったリスクが、新たな議論のきっかけにも

「『NetStare®』を選んだ理由のうち大きかったのは、ログ解析のレポートを適宜出してもらえること。的を射た内容で分かりやすく、社内の報告資料としても役立っています」と若林さん。三角さんは「ログ解析に加え、24時間365日の保守。さらに、何かあった時の緊急電話連絡。当社の今の体制では出来ないので、これがマストでした。全体的な総合力と、価格のリーズナブルさが最終的に決め手となりました」と語ります。

導入後の感想については、「次世代ファイアウォールに対する問い合わせ対応や、当社が実現したいことを踏まえての設定提案などのサービスには満足しています。ログ解析についても、『NetStare®』導入前の過去ログまで解析してしっかりしたレポートを出してくれた※。その結論が『特に問題なし、安心です』ということでホッとしました。今後も、定期的なレポートに期待しています」（若林さん）。

また、「脆弱性検査をやって頂き、設定も変更対応してもらい、ブラックリストの追加も。タイムリーなレベルアップサイクルが非常に良いですね。また、過去ログの解析でいくつかの脆弱性が見つかり『こういう攻撃リスクがあります』というコメントを頂いたことが、それを放っておいて良いのか、部内で議論するきっかけとなりました。その後のレポートも、部下に対策を考えさせる良い契機になっています」（三角さん）。

※有償サービス

CSIRTとSOC、二段構えの体制へ

しかしセキュリティは、次世代機器を使いこなして終わり、ではありません。

同社のセキュリティの将来像について三角さんは「我々も経済産業省の『サイバーセキュリティ経営ガイドライン』に沿って社内に『CSIRT※1』を置くとともに、『SOC※2』によるログ分析や対応を実施したいと思っています。ただ、SOCは高度な技術を持っていないとなかなか難しい。優れた外部組織に委託したいと考えています」と語ります。

「製造業においては、セキュリティの専門家は育てるのに時間も掛かります。外部との協業を上手に活用していきたいですね」（三角さん）。そして、セキュアヴェイルに今後期待することを伺うと、「SOCの知見を持った方による監視やインシデント対応をやって頂ければ」と、嬉しいお言葉を頂きました。

※1　CSIRT：セキュリティ事故の発生を前提として企業内に設置される対応チーム。発生時には“消防団”として事故対応に当たる。

※2　SOC：「セキュリティオペレーションセンター」の略称。24時間体制でネットワークインフラを監視し、サイバー攻撃の発見や分析、対応策の立案を担う。

なるほど～ NetStare®

何でセキュアヴェイルには営業部門がないの？

お客様：セキュアヴェイルには営業部門が無いって聞いたけどなんで？

SA：営業部はありませんが、カスタマーサービス部という部署が顧客との窓口を担っています。

お客様：営業部とは何が違うの？

SA：機器やサービスを売るだけではなく、お客様の要望を実現するために、何をしたらよいかを提案しています。

お客様：モノを売らないってどんなことをしているの？

SA：例えば既にNetStareを契約いただいているお客様には「運用状況報告書」として機器の稼動状況やログを分析し定期的に報告会を実施しています。

お客様：サービスって契約したら全て任せておいたらいいんじゃないの？

SA：もちろん危険度が高い通信や怪しい通信があればサービスの中で対応しているため任せていただいて問題はありません。
しかし実際運用をしていくとセキュリティポリシーや脅威は日々変化していくため、変化に応じて設定が合致しているのか見直す必要があります。

SA：ポイントになるのが現状把握です。日々の運用を「見える化」して把握することで、改善点を見つけていきます。

お客様：ふーん、なんだか面倒そうだな。

SA：そこでカスタマーサービス部のメンバーがお客様毎の環境や利用方法を踏まえ現状分析を行い、必要に応じて機器のリプレイスや構成の見直し等を提案しています。

お客様：なるほど！カスタマーサービス部がいることで日々の運用をサポートしてもらえるんだね。

コラム 「わ・か・る」と「き・く」

4月に17名の新たな仲間を迎えた。1ヶ月の集合研修後、職場に仮配属されて毎日様々なことを学んでいる。普通なら社会人、セキュリティエンジニアとしての常識や知識を覚える時期だが、弊社ではそれは許されない。覚えることを原則禁止しているからだ。あくまでも考え方だが、覚えるはNGで、理解することが大事だと徹底指導する。覚えたことはいつか忘れるし、応用が利かない。状況を理解してこそ適切な判断ができる。これがプロの仕事と、説く。つまり、先ずは「分かる」ことからスタートするのだが、よく聞いて考えることで「解る」ようになり、どのように対応すべきか「判る」ようになる。自らの判断で提供した成果物が価値となり顧客満足を高める。サービス事業であるからには顧客の環境、状況、目的を理解せねば有益な提案はできない。そのためには「顧客を知る」必要がある。知る手段として有効なのは聞くことだが、これも聞くだけではダメ。「聞く」ことから始めて、詳細を「聴く」、それ故「訊く」必要がある。訊くことで得た情報が提案のスパイスとして「利く」ようになり、それを実行することでセキュリティ対策が「効く」。そういう論法で顧客と向き合う姿勢を教育する。言葉遊びのようではあるが、本質的な理解へ導くには有効だ。弊社開催のセミナー「セキュリティ講座」でも、日常的なセキュリティ用語からその本質的な意味と実効性のある対策を導く…というテーマで講義をしている。「おもしろそうだな…」と、思われた方は是非「セキュリティ講座」にお越しいただきたい。「わかる」と「きく」が体験できます。

SecuAvail

株式会社セキュアヴェイル（SecuAvail Inc.）
www.secuavail.com

大阪本社
〒530-0044　大阪府大阪市北区東天満1-1-19
アーバンエース東天満ビル
TEL:06-6136-0020　FAX：06-6136-0018

東京本部
〒104-0044　東京都中央区明石町8−1
聖路加タワー40階
TEL:03-6264-7180　FAX：03-6264-7181

発行 2017.7