SUHO

COMPANY PROFILE

THE BRAND LEADER IN NETWORK SECURITY

Company Review

INTRODUCTION

スホは「Suport User High Quality One Services」の略として、お客様へ高品質のサービスを提供したい意志を持つ者たちが集まった「ITサービス専門会社」です。

スホは、たとえ小規模であっても、すべての産業全般にわたって要求される専門のITサービス分野でトップに立とうと絶えず努力しています。

過去にオンラインゲームチームに所属し、数多くの事例から得た様々な経験と培った高い技術力を基に、確実なプロジェクト遂行を約束いたします。

会社名	株式会スホ	代表取締役	田 昌錫
設立	2010年11月12日		
事業内容	IDC（ラックコロケーション、インターネット回線、Hosting） CDN（Download、Cache、Streaming） Product Sales（Server、Network、Storage、Security） Solution（SBI Payment、nProtect GameGuard、Microsoft SPLA） 運用（構築、運営、監視、保守、障害対応）		
所在地	〒162-0814 東京都新宿区新小川町7-17 飯田橋三幸ビル4F TEL：03-6868-6446　FAX：03-6868-6100		

INTRODUCTION

スホは国内ネットワーク保安市場の問題である「ランサムウェア」のセキュリティを強化するため、独自の様々なセキュリティソリューションを組み合わせることにより、APT(Advanced Persistent Threat) 攻撃に対応できる「悪性ファイル収集 - 分析 - モニタリング - 対応」の総合プロセスを構築しました。

現在ランサムウェアを遮断することができるセキュリティソリューションが開発されていない状況で、攻撃に事前対応するための最適なソリューション技術を保有しているスホは、内部技術者を通して新しいセキュリティハッキング事例が発生した際に、より迅速に対応することができます。

顧客のTCO(Total Cost of Ownership)を劇的に減らし、ROI(Return On Investment)を最大化できる技術力を保有しております。
蓄積された技術力を基に、国内ADN(Application Delivery Network)市場の先頭に位置付けられており、無線及びセキュリティ市場でも圧倒的な成果を出しております。
また、Data center構築及び仮想化の具現する際に必須である高速スイッチング製品を準備し、仮想化市場に先制対応しております。

KEY TECHNIQUE POSSESSION

<スホ次世代セキュリティプラットフォーム技術の核心>

- Networks RNA(Real-time Network Awareness) Solution

：核心技術の一つである内部リソースの分析機能は、リアルタイムでの資産情報を自動的に学習する。自動化された資産分析機能は、スホが保有している次世代の分析システムと連動され、攻撃の影響評価、内部コンプライアンス監査、資産分析などに活用されている。既存のシステムで実装できなかった様々な情報を確認することができる非常に優れた技術である。

- 実際の環境に最適化されたポリシーを自動的に設定

：既存ソリューションの場合、管理者のセキュリティ経験及び技術により、セキュリティの差が生じることがある。
スホの技術を通し、管理者の介入なしでも高レベルのセキュリティを確保することができる。

- イベントの発生時の関連性を分析し迅速に対応

：数々のイベントを正確に分析するためには、次世代の分析システムのようにNext Generation Correlation機能を活用する必要がある。

- この機種間の連動を通した統合イベント分析

- 独自開発された技術を通し、様々なベンダーのセキュリティプラットフォームを一つのConnectorにて統合管理及び連動

SECURITY PARTNERSHIP

お客様に最高の製品とサービスを提供するためにの最高のパートナーシップ

Security Solution

Security Solution：SourceFire

SOURCEfire は、業界最高の性能(NSSLabsテスト結果1位)とAPT攻撃を効果的に遮断するセキュリティ専門企業

- 10年以上の信頼できる企業(NASDAQ上場：FIRE)
- 2001年Snort開発者のMartin Roeshにより設立
- ネットワークよりエンドポイントまでセキュリティソリューション提供
- 180カ国以上へのSourcefireセキュリティソリューション供給
- NSS研究所が実施したNetwork IPS分野でBest検出ソリューションに選定
- Gartner Magic Quadrantリサーチでleader選定
- SCマガジン社が選定した最高のIDS/IPS

firePOWER™

NGIPS | NGFW | Virtual | SSL

- ✓ 業界最高の処理性能及び遮断性能(NSSLabs 1位)
- ✓ 45Mbps ~ 80Gbps 様々な製品群
- ✓ NGIPS+NGFW+Anti-Malware 同時提供
- ✓ シングルパスエンジンを搭載した単一プラットフォームとして統合型セキュリティ機能とAgile Securityの利点を提供

fireSIGHT™

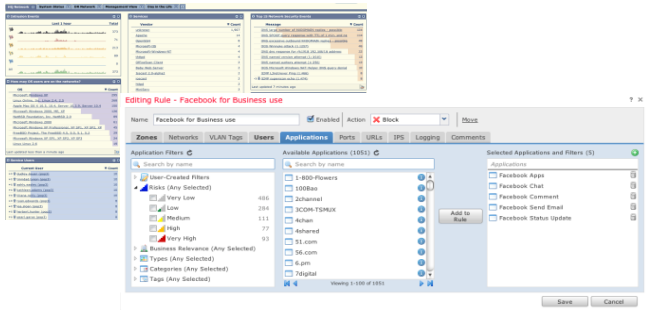
Defense Center

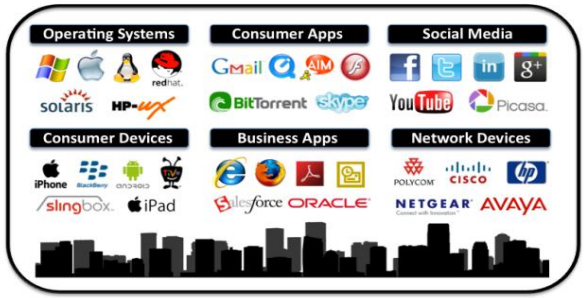
- ✓ ネットワーク点検とエンドポイントの状況認識(Contexture Awareness)を通してリアルタイム IT環境を把握し、自動的に強力な遮断機能提供(2000個のアプリケーション支援)
- ✓ 脅威の相関関係を通し、不必要なセキュリティイベントを最大約99%まで減少
- ✓ リアルタイムのネットワーク及びユーザー認識

fireAMP™

Advenced Malware Protection

- ✓ FireAMPは新たな脅威をリアルタイムで分析しネットワーク内の状況に対し優れた可視性を提供
- ✓ ネットワン上で malwareが広がっていく経路の追跡機能提供
- ✓ 潜在的な脅威を防ぎ、outbreakを迅速に阻止するためのControl機能提供(隔離、治療)



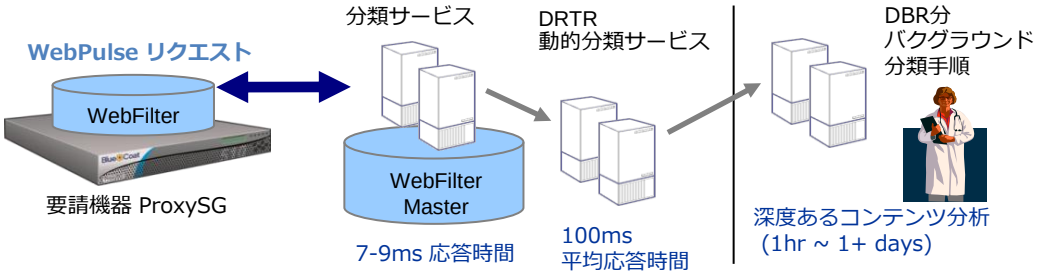


Security Solution : BlueCoat ProxySG

- **Secure Web Gateway 部門で業界1位 Solution**
- **HTTPs Trafficの可視性確保でInternet Trafficに対するセキュリティポリシー付与**
- **Blucoat Web-Filter(BCWF)というDynamic Web-Filter DBでカテゴリー化されたインターネットアクセスポリシー付与**
- **プロトコル規格検査機能でTCP ポートバイパストラフィックを完全遮断**
- **他のセキュリティソリューション連動可能（ICAP標準プロトコルを用いたDLP連動及びネットワークセキュリティソリューション連動）**
- **国内外多数のレファランス確保**

• Blue Coat Web Filter (Dynamic URL DB)

- ▷ 80+分類、50言語、2000万個に分類されたドメイン
- ▷ 許可/遮断の他、ユーザー定義の例外処理を支援
- ▷ リクエストURLの95%を7-9msに分類結果をすぐに提供(on-proxy)
- ▷ ～5%の未分類リクエストをWeb Pulseに要求リクエスト
- ▷ 国内URLリスト及びユーザー定義分類DB支援



• HTTPs トラフィック可視性確保及びヘッダーコントロール

- ▷ Man-In-Middle方式でHTTPs トラフィックセッション処理
- ▷ 自体認証書インポート/エクスポート機能具現
- ▷ 可視性が確保されたトラフィックに対し、一般HTTP トラフィックと同じレベルのポリシーを具現可能
- ▷ HTTP/HTTPs トラフィックのヘッダー制御可能
- ▷ HTTP/HTTPs ヘッダー全体の中、メソッド部分(Get、Put、Postなど)を制御しウェブメール発信及び遮断可能でファイルサイズなどの制限ポリシーを適用可能

•プロトコル規格検査及び他Solution連動

- ▷ 非規格トラフィックを源泉封鎖し、TCPバイパスプログラム(ex、NateOn Messengerなど)の使用を遮断可能
- ▷ TCP443を用いたリモートコントロール(リモートコントロールを通した内部資料の流出危険)などの遮断可能
- ▷ その他のインターネット TCP ポートを用いた非正規/非業務/内部情報流出(Online-Storageなど)を遮断可能
- ▷ 標準プロトコルのICAPを用いて、Symantec DLPなどとネットワークで連動可能

Security Solution：FireEye, Anti-APT

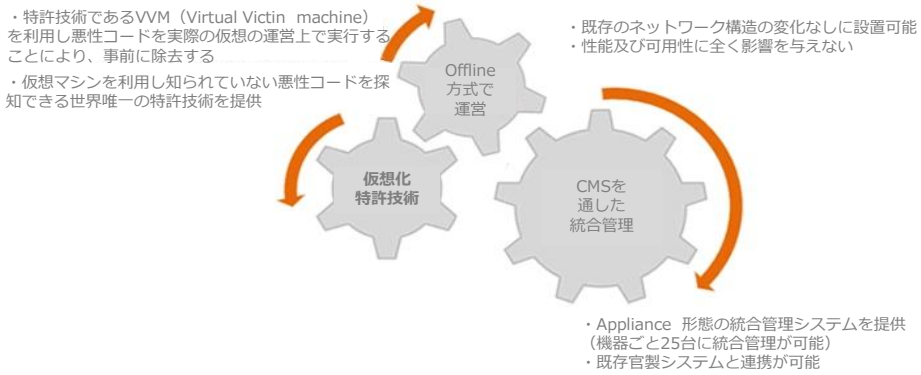
- ローカルネットワーク上に知られているmalwareに感染したPCを探知(Sand-Box+ Signature基盤)
- ネットワークトラフィックの分析及びHoneypot技術を応用した新型または変種Botに対する探知機能
- ネットワーク機器と連動し、C&Cサーバーとのトラフィックを遮断
- Botnetに感染した情報をGlobalに配置されたBotwall機器間の自動配布機能を通し共有
- 全世界悪性コード分析分野の占有率1位

● BOTとは?

ユーザーの知らない間に一般のPCにインストールされたバックドアプログラムで発展した悪性ボットは、Agobot、IRCBot、rBotなどの名前からも分かるようにBotという接尾語が付くすべての種類の悪性コードです。既存のウイルスやワームなどの用語と区別されている「BOT」は、ロボット(Robot)から始まったもので、ハッカーや流布者が遠隔地からボットに感染したシステムを調整することができるという意味を持っています。つまり、ボットは一般のPCをハッカーが勝手に調整できるように作ったロボットプログラムだと考えられます。

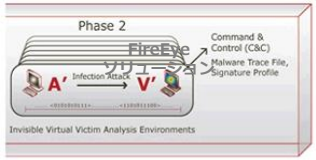
●FireEye社の製品と競合製品の比較

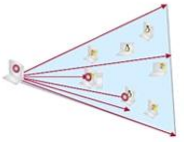
- ▷ 仮想化技術を通し、知られていない悪性コードをネットワーク上で探知可能な世界で唯一のセキュリティソリューション
- ▷ オンラインモードで動作し、既存ネットワークの構造変化なしに設置及び運営が可能
- ▷ 性能低下及びサービスの可用性に全く影響を与えないCMS(Central Management System)を通した統合管理の提供



● Malware判定

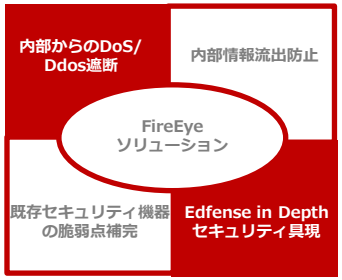
- ▷ VM(Virtual Machine)を通し疑わしいC&Cサーバーと通信の試み
- ▷ Malware rowパケットを保存及び分析(pcap)
- ▷ 新種及び変種Malwareに対するシグニチャーを自動で生成し、Botwall Networkを通し情報共有





● FireEye Botwall設置により期待される効果

- ▷ FireEyeは、既存のセキュリティソリューションでは、防御が難しいBot&Botnet探知及び遮断、C&Cサーバーへの接続遮断、知られていないBot遮断機能を利用し、更に強化された安全なネットワーク具現
- ▷ BotはDoS/DDoS攻撃及び情報流出に最も多く利用されており、これらのDoS/DDoS及び情報流出を根本的に予防するためにはFireEyeのソリューションが必要



Security Solution：BlueCoat, SSL VA 外

SSL Visibility Appliance は 2013年 BlueCoat社が NETRONOME より買収した SSL トラフィック専用可視性確保ソリューション

- 動作原理は、BlueCoat ProxySGと同一であり、In-Line及びMirror Modeで構成可能
- HTTPs トラフィックを復号化し、既存のセキュリティソリューションの限界を克服
- クライアント前段のForward Mode及びサーバー前段のReverse Modeの全て支援

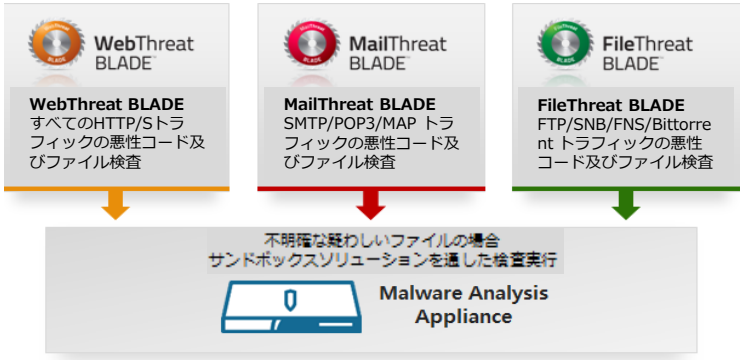
SOLERA NETWORKS / RSA / FireEye / AhnLab / ArcSight / splunk> / Symantec. / McAfee

DeepSee VIRTUAL APPLIANCE は 2013年 BlueCoat社が SOLERA NETWORKS より買収したNetwork Forensicソリューション

- SPAN/TAPを利用し、伝達されたトラフィックに対するフォレンジック機能提供(事後監査証跡及びエビデンス提供)
- FireEyeまたはBlueCoat製品と連動し、PCAP形式のLog提供可能
- 特定デスティネーションまたは特定パターンのファイルなどヘッダー及びペイロードに存在する情報に対するフィルタリングが可能

MAA (Malware Analysis Appliance) は 2013年 BlueCoat社が norman SHARK より買収した悪性コード分析 ソリューション

- CAS(Contents Analysis System)より伝達されたトラフィックで悪性コード分析
- Sand-Box技術を利用し、実際のユーザー環境と同一環境でFileを実行した後の結果転送



* CAS(Contents Analysis System)とは?

BlueCoat社の既存の製品群の中、ネットワーク Anti-Visur ソリューションであるAV製品の新しい名称でProsySGと連動されたCASにInbound/Outbound リアルトラフィックが伝達され、リアルタイムでTV accineの機能をネットワーク上で実行可能なソリューション
McAfee、KASPERSKY、Sophos、PANDAなど4台 Major Vaccine Engineが搭載可能で、最大2つのEngineを同時に使用可能

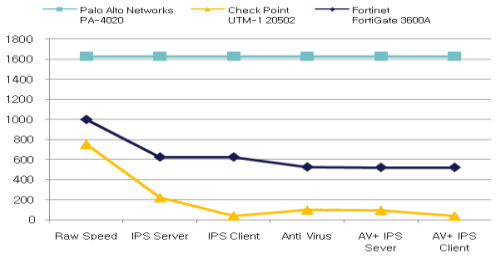
Security Solution：Palo-Alto NG Firewall

- Applicationを区分し、制御する機能を提供(1000個以上)
- ユーザー区分(ユーザーアイデンティフィケーション)が可能(IP アドレス≠ユーザー)
- 送受信DataのContents(Application Data)部分を分析し、制御することができるファイアウォール
  (内部ユーザートラフィック現況把握及び業務分析機能を提供 - 管理者の満足度は非常に高い)
- ファイアウォール+IPS+URL フィルタリング機能はもちろん、強力なレポート報告書機能を提供する次世代ファイアウォール

- **Palo Alto 次世代ファイアウォールは?**

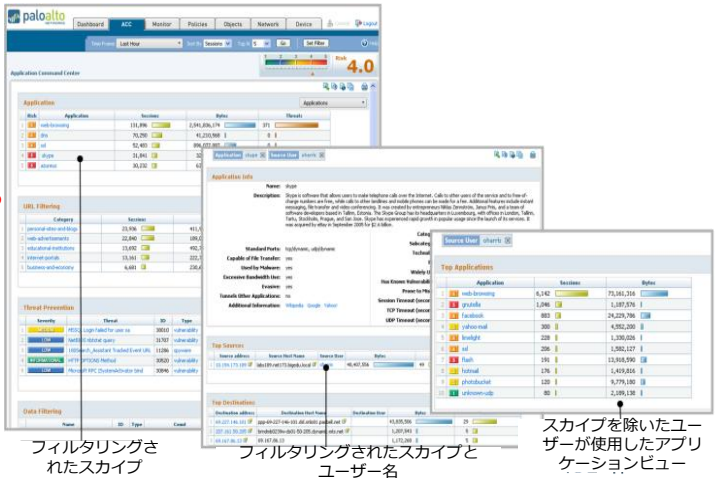
単純ポート基準ではなく、1,000個以上のアプリケーションとコンテンツ、ユーザー別のセキュリティポリシーを樹立することができるので、既存のポート基盤の限界を克服することができ、IPSなどでは探索及び遮断できないスカイプとP2Pなど、暗号化された内容のアプリケーションに対してもセキュリティが可能。Palo Alto Next Generation FireWallはファイル基盤ではなく、ストリーム基盤のスキャン技術を提供し、性能の低下なしにコンテンツを分析、制御することができ、主要資産や個人情報などのようなデータ流出防止も可能。

< 既存UTMと差別化された安定的性能>



- **既存のセキュリティ機器は忘れて！Palo Altoだけの差別化**

1. Applicationを区分し制御
   - シグネチャ、プロトコルデコーディング、ヒューリスティック技法を通し、アプリケーションを認知してアプリケーションDBを作成
   - アプリケーション DBを通し、ファイアウォールポリシー、QoS、Routing、Logging及びReportingを単位Objectに使用
   - ユーザー定義アプリケーション登録も可能
2. 既存のUTMを越えた本当の意味でのファイアウォール
   - ファイアウォールの「Helper」である専用の機器を増やすことは、ネットワークをより複雑にするだけで、実質的な解決は不可能
   - Palo Alto機器はアプリケーションDBに基づき、様々なアプリケーションの制御を通し、ネットワークの帯域幅管理とコンテンツフィルタリングエンジンを通したりアルタイムコンテンツスキャニングで攻撃及び脅威遮断、内部情報流出遮断とURL フィルタリングなどの機能を遂行することで、専用機器の統合と既存のUTMを凌ぐ本当の意味でのファイアウォールである
3. 最高のパフォーマンス保障
   - 目的基盤のハードウェア構造とユニバーサルシグニチャーDBを基盤にシングルパス探索技術を提供し、性能の低下がなく正確なアプリケーション探索が可能(IPS、Anti-Virusなど)
   - 既存のUTMで提供するアプリケーション探索は、異なるベンダーの技術及び製品を基にモジュール化されており、機能の実行時にそれぞれのモジュール別機能を別途に実行しなければならないので、深刻な性能の低下を招く
4. 強力なレポーティング機能提供

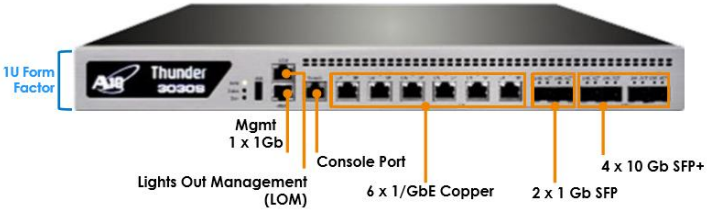


Security Solution :

- RSA及び Diffie-Hellman Key Exchange 技法支援
- ECDHE Ciper及び様々な Ciphper 支援
- SSL暗号化トラフィック増加によるシステム性能拡張支援
- 多数のセキュリティ機器の構成時、ロードバランシング支援
- TLS暗号化適用時、TCP 443ポート以外のポートまたは ダイナミックポートを使用支援

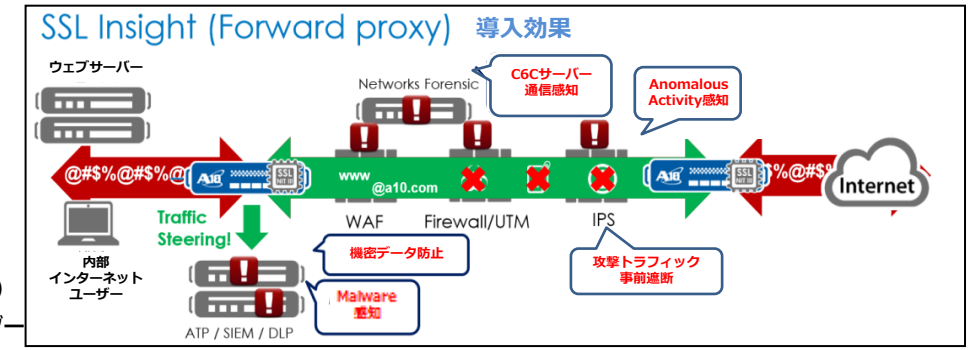
• SSL Insight とは?

SSL traffic Inbound/Outbound SSLトラフィック内に隠れている脅威に対する可視性を提供し、セキュリティゲートウェイ機器とサーバーのSSL負担を大幅に削減することができる専用の機器です。
SSL traffic は、既存のセキュリティ機器をバイパスすることができ、暗号化されたSSL trafficの可視性がなく追跡ができません。
SSL traffic inspectionを支援するセキュリティ機器であっても、セキュリティ機器性能の問題を引き起こす可能性があり、全体的なソリューションの拡張に制限をかけます。
SSL Insightは、これらの問題点を補完することができる最適のソリューションです。



• SSL Insightは、暗号化されたネットワークトラフィックに対する高性能の可視性と拡張性を提供するソリューション

▷ ICAP(Internet Content Adaptation Protocol)支援
▷ URL Classification Service - Webroot BrightCloud 連動
▷ 高性能 SSL 処理能力、SSL Traffic Steering、ロードバランシング提供
▷ 完璧な SSL 可視性(ECDHE ciphers 支援)
- SSLi により復号化されたトラフィックは、セキュリティ検査後、再暗号化され目的地(サーバー/内部ユーザ/インターネット)に送られる



• グロバール技術支援

▷ グローバル27個の支社及び4箇所の「24x7x365」グローバル技術支援(TAC)センター運営 - 迅速な技術支援
▷ 韓国を含むグローバルRMA Depotセンター51個所支援 - 迅速なRMA代替品の需給(GoldレベルSupport)
▷ MQガートナーMQレポート基準に「ニッチベンダ」から「リーダーグループ」に成長している唯一のベンダー

Thank you

営業　：林　裕錫 090-8171-8676 ｜ youlim@suhojapan.com

：宮田 杏奈 090-5172-7117 ｜ miyata@suhojapan.com