

AhnLab Managed Firewall Service



❖ Service Overview

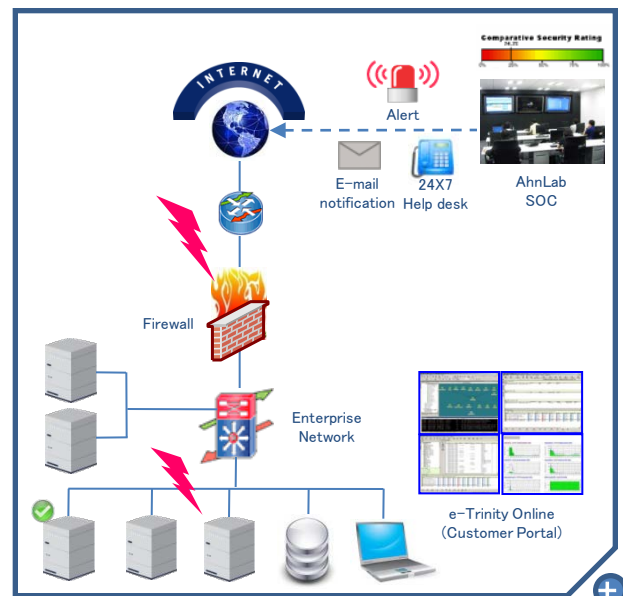
- 今日、高度化されたセキュリティリスクの脅威に対して、セキュリティインフラの基本であるファイアウォールの管理が改めて重要視されてきております。
- ある統計では全企業の70%以上で、セキュリティの専門知識や技術力を持ったIT管理者が不足しております。情報漏洩などの脅威から対策を行うには、セキュリティの専門家による『セキュリティポリシーの作成』や『セキュリティインフラの設計・構築』、『運用・管理』が必要となります。
- 誤った運用・管理、または定期的なメンテナンスを行っていないファイアウォールは、企業の事業継続に係わる深刻なセキュリティインシデントを引き起こす危険性があります。
- セキュリティの専門家に運用・管理をアウトソースを行うことで、ROSI(Return On Security Investment)を最適化する最も現実的な方法であると考えられています。

❖ Service Implementation Flow



❖ Managed Firewall Service Feature

- デバイス運用
 - 既存ポリシーの検証
 - お客様のご要望によりポリシーの変更作業
 - Firewall パフォーマンスおよび可用性管理
- モニタリング
 - 24x7 セキュリティイベント監視(IP基盤)
 - ログ分析
 - Block ログ基準 Report 及びポータル提供
- 運用・障害報告書
 - マンスリーレポートの提供
 - 障害対応レポートの提供
 - セキュリティ脅威関連情報の提供



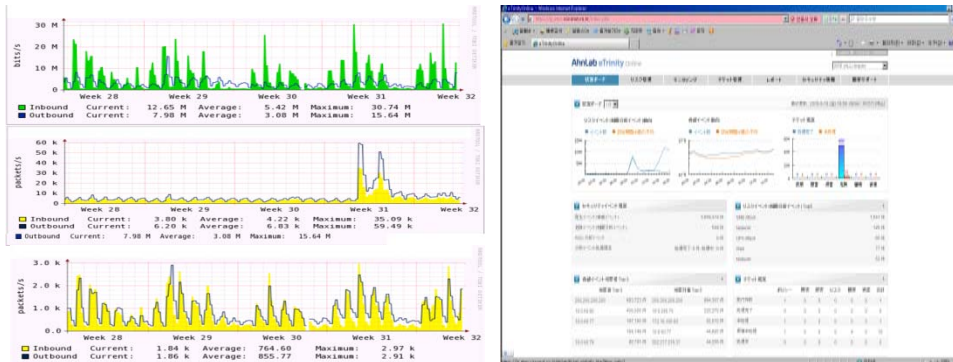
Managed Security Service Architecture

❖ Service Benefits

- 事業継続性の確保
 - 情報漏洩などに繋がる不正アクティビティの早期発見が可能となる
- 教育費用などのコスト削減が可能
 - セキュリティに特化したIT管理者の育成が不要となる
- マルチベンダーサポート
 - Ahnlab, Cisco, Juniper, Fortinet, NetScreen, 他
- 運用・管理体制の強化
 - セキュリティの専門家による監視が可能となる

AhnLab Managed Firewall Services

❖ Reporting & Customer Portal (Sample report および e-Trinity 画面提示)



❖ Support Device

- Cisco ASA Series, Catalyst Firewall Services Module (FWSM)
- Fortinet FortiGate Series
- AhnLab TrusGuard UTM Series 他

❖ AhnLab Security Operation Center の差別化ポイント

- ◆ 10年以上の Managed Security Service 提供経験
 - 韓国 No.1 セキュリティ監視企業 (1998年サービス開始, 現在およそ 500 社)
 - 国際的なインシデント対応に対するフォーラムであるFIRST に加盟 (<http://www.first.org/members/teams/asec/>)
- ◆ 脅威情報分析センターを自社にて保有
 - ASEC (AhnLab Security E-Response Center)
 - 悪性コードの専門分析およびシグネチャ提供
- ◆ 業界専門家で人材構成 (資格多数保有)
 - セキュリティー一般および管理: CISSP, CISA
 - ネットワークデザインおよび管理: CCNP, CCIE
 - システムおよびアプリケーション管理: SCNA, SCJP
 - 脆弱性分析および模擬ハッキング: CEH, セキュリティフォレンジック

❖ Service Level Information (サービスレベル詳細は SLA 参考)

サービス区分	サービスメニュー	デバイス種類	サービスレベル
基本サービス	デバイス運用	ASA/FWSM/Fortigate/TrusGuard	<ul style="list-style-type: none"> • ACL 設定 • Config 設定 • パフォーマンス管理
	モニタリング	ASA/FWSM/Fortigate/TrusGuard	<ul style="list-style-type: none"> • 24 時間365日監視(ログ管理) • 障害発生時 メール又は電話にて通報 • マンスリーレポート
オプションサービス	デバイス管理	ASA/FWSM/Fortigate/TrusGuard	<ul style="list-style-type: none"> • デバイス構築/交換 • 現地サポート • ライセンス管理
	リソース管理	グローバル IP を保有するサーバ	<ul style="list-style-type: none"> • ICMP/Service 監視 • URL 監視

AhnLab Managed IDS/IPS Service



❖ Service Overview

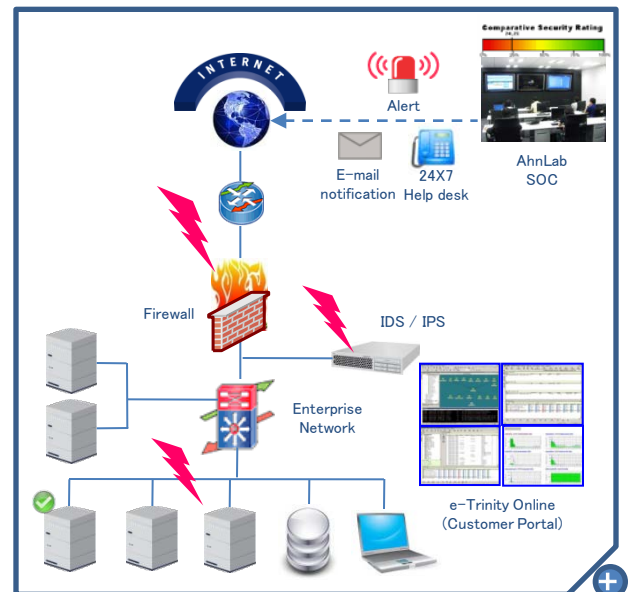
- 今日、情報漏洩などの脅威からシステムチックに防御するには、不正侵入検知／遮断装置(IDP/IPS)の導入が一般化しております。
- しかし、企業内における不正侵入検知／遮断装置(IDP/IPS)の管理では、最適なシグネチャ管理が出来ていない事が多く、セキュリティ専門家の知識が必要とされています。
- 不正侵入検知／遮断装置(IDP/IPS)が導入されていない企業では、事前に不正アクティビティ(不正侵入、不正操作、情報漏洩)の検知ができず、企業の事業継続に係わる深刻なセキュリティインシデントを引き起こす危険性があります。
- セキュリティの専門家に運用・管理をアウトソースを行うことで、ROSI(Return On Security Investment)を最適化する最も現実的な方法であると考えられています。

❖ Service Implementation Flow



❖ Managed IDS/IPS Service Feature

- デバイス運用
 - シグネチャアップデートおよびシグネチャ最適化
 - お客様のご要望によりポリシー適用
 - IDS/IPS パフォーマンスおよび可用性管理
- モニタリング
 - 24x7 内部・外部セキュリティイベント監視
 - IDSイベントによりFirewall遮断設定
 - ログレビュー
- リソース管理
 - 主要サービス状態チェック (MRTG, AliveCheck, Service Check など)
 - 主要サービス障害発生時メールまたは電話通報
- レポート
 - マンスリーレポートの提供
 - 攻撃ログレポートの提供
 - 障害対応レポートの提供
 - セキュリティ脅威関連情報の提供



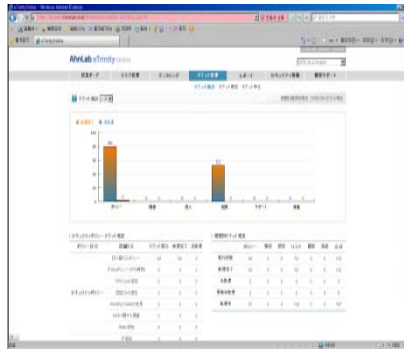
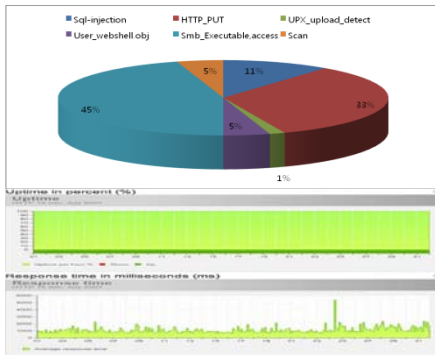
Managed Security Service Architecture

❖ Service Benefits

- 事業継続性の確保
 - 情報漏洩などに繋がる不正アクティビティ(不正侵入、操作)の早期発見が可能となる
- 教育費用などのコスト削減が可能
 - セキュリティに特化したIT管理者の育成が不要となる
- マルチベンダーサポート
 - IBM Proventia Network IPS、IBM Real Secure、他
- 運用・管理体制の強化
 - セキュリティの専門家による監視が可能となる

AhnLab Managed IDS/IPS Service

❖ Reporting & Customer Portal (Sample report および e-Trinity 画面提示)



❖ Support Device

- IBM / ISS Proventia Network Intrusion Prevention System
- IBM / ISS RealSecure(Software) 他

❖ AhnLab Security Operation Center の差別化ポイント

- ◆ 10年以上の Managed Security Service 提供経験
 - 韓国 No.1 セキュリティ監視企業(1998年サービス開始, 現在およそ 500 社)
 - 国際的なインシデント対応に対するフォーラムであるFIRST に加盟 (<http://www.first.org/members/teams/asec/>)
- ◆ 脅威情報分析センターを自社にて保有
 - ASEC (AhnLab Security E-Response Center)
 - 悪性コードの専門分析およびシグネチャ提供
- ◆ 業界専門家で人材構成(資格多数保有)
 - セキュリティー 般および管理: CISSP, CISA
 - ネットワークデザインおよび管理: CCNP, CCIE
 - システムおよびアプリケーション管理: SCNA, SCJP
 - 脆弱性分析および模擬ハッキング: CEH, セキュリティフォレンジック

❖ Service Level and Price Information (サービスレベル詳細は SLA 参考)

サービス区分	サービスメニュー	デバイス種類	サービスレベル
基本サービス	デバイス運用	Proventia/RealSecure	・パフォーマンス管理 ・ポリシーチューニング ・シグネチャアップデート
	モニタリング	Proventia/RealSecure	・24 時間365日監視(ログ管理) ・障害発生時 メール又は電話にて通報 ・マンスリーレポート
	リソース管理	グローバル IP を保有するサーバ	・ICMP/Service 監視 ・URL 監視
オプションサービス	デバイス管理	Proventia/RealSecure	・デバイス構築/交換 ・現地サポート ・License 管理
	脆弱性診断	Web/Network/Linux /Windows	・Network脆弱性スキャン ・ウェブ脆弱性スキャン ・顧客要請によるシステム診断
	インシデント対応	インシデント発生時	・現地対応 ・セキュリティフォレンジック