

セキュリティログの集中管理と高度分析サービス 「SecureEagle®/SIM」を SIMに対応した MSSP モデル(国内初)として販売開始

日立電子サービス株式会社（以下「日立電サ」、本社：神奈川県横浜市、社長執行役員：百瀬 次生）は、日々複雑化、巧妙化するサイバー攻撃や、後を絶たない内部情報漏洩などのセキュリティインシデント※¹の未然防止と迅速な検知で、お客様のセキュリティリスクを大幅に低減するセキュリティ統合管理ソリューション「SecureEagle※²/SIM」を7月20日より販売開始しました。

昨今、情報システムを外部からのサイバー攻撃から保護することのみならず、組織内におけるセキュリティポリシーの遵守状況を把握するとともに、日本版 SOX 法に代表されるような内部統制への対応が組織の至上命題となってきました。その為、セキュリティインシデントの原因特定や監査証跡として不可欠となるセキュリティログ管理の重要性はますます高まってきました。しかし、種々の情報システムにはマルチベンダの機器が混在し、様々なセキュリティ装置（ファイアウォール、不正侵入検知装置など）やネットワーク機器、サーバなどが導入されている状況で、日々大量に発生するログを効果的に管理していくことは非常に困難でした。

「SecureEagle/SIM」は、お客様に導入されている様々なシステムのセキュリティログを相関的に分析することで、セキュリティインシデント発生の予防措置や事後対策に係わる時間を大幅に削減するとともに、ITの内部統制をサポートします。

本サービスは、セキュリティ情報マネジメントツールとして世界トップシェアを誇る ArcSight, Inc.（本社：米国カリフォルニア州、CEO:Robert W. Shaw）とセキュリティ管理におけるアライアンスを組み、SIM※³機能を活用したセキュリティログの高度分析サービスを提供します。また、弊社日立ソリューションサポートセンタによる MSSP※⁴型サービスに加え、弊社物理セキュリティマネジメントシステム Webvisor®と連携し、物理/サイバーの両面からお客様をトータルにサポートします。なお、お客様のシステム規模や形態、セキュリティポリシーに応じて SecureEagle/SIM をお客様内に導入し、運用支援を行うオンサイト型のサービスもご提供します。

- ※1 セキュリティインシデントとは、アクセス権を持たない人がコンピュータを不正に利用するようなコンピュータのセキュリティにかかわる事件・出来事のこと。例えば、リソースの不正使用、サービス妨害、データの破壊、情報漏洩など。
- ※2 「SecureEagle®」とは、お客様内で発生するセキュリティインシデントを鳥の王者である鷲（イーグル）のように鋭い視点で、決して見逃さないことで、お客様のセキュリティリスクを低減するという意味を込めて名付けています。「SecureEagle®」は、弊社の登録商標です。
- ※3 SIM : <Security Information Management>多種多様なセキュリティ/ネットワークデバイスならびにサーバ OS、ミドルウェア等のセキュリティに特化したログを相関分析し、それをセキュリティインシデントとして管理する仕組み。
- ※4 MSSP : <Managed Security Service Provider>インターネット等を介してセキュリティ運用・管理業務サービスを提供する事業者。

本サービスは日立グループのトータルセキュリティソリューション「Secureplaza」の一環として位置付け、販売していきます。また、「SecureEagle/SIM」は、7月26日(水)、27日(木)に開催される HITACHI uValue コンベンション2006に出展します。

サービスの特長

「SecureEagle/SIM」は、以下の特長により、お客様のセキュリティインシデント管理や内部統制に対する様々なニーズにお応えします。

(1) ログの集中管理と高度分析によるセキュリティインシデントの管理

複数デバイスのログを収集し、リアルタイムに相関分析することにより、お客様に重大な影響を与えるセキュリティインシデントを抽出し、そのセキュリティインシデントの分析結果と、お客様への影響度、推奨の対策案をご連絡します。

(2) マルチベンダデバイスのサポート

ファイアウォールや不正侵入防御システム等のセキュリティ装置、ルータやスイッチ等のネットワーク機器、サーバ OS、ミドルウェアなど 130 種類以上の様々なデバイスをサポートしており、今まで別々のコンソールで管理・保存していたログを一元管理することで高度な分析を実現しています。

(3) 物理セキュリティ連携

弊社物理セキュリティマネジメントシステム「Webvisor®」との連携によって、サイバーセキュリティのログだけでは判断できない他人のユーザ ID を使用した「なりすまし」による不正アクセスや情報持ち出しなどの追跡調査が可能となります。

(4) 法規制や各業界規制への対応

SecureEagle/SIM は、(財)金融情報システムセンター発行の「金融機関等コンピュータシステムの安全対策基準」や、情報セキュリティ政策会議にて決定された「政府機関の情報セキュリティ対策のための統一基準」などの業界規制にて求められるログ(証跡)管理等のセキュリティ要件をカバーし、それらの規制への対応をサポートします。また、SecureEagle/SIM は、日本版 SOX 法において必要とされるエビデンスレポートにも対応していきます。

提供価格

(1) 外部(公開)ネットワーク監視モデル(MSSP型)

一次導入費用	50万円～ (個別見積もり)
サービス費用(月額)	23万円/月～ (個別見積もり)

※対象デバイス: 3デバイス(ファイアウォール1台、侵入検知装置1台、Webサーバ1台)

(2) 内部ネットワーク監視モデル(MSSP型)

一次導入費用	100万円～ (個別見積もり)
サービス費用(月額)	140万円/月～ (個別見積もり)

※対象デバイス: 1,030デバイス(サーバ30台、クライアント1,000台)

販売開始

2006年7月20日より。

販売目標

2008年まで3年間で10億円。

《添付資料》 セキュリティ統合管理ソリューション「SecureEagle/SIM」の概要

■日立電子サービス株式会社について

日立電子サービスは、「お客様の飛躍を支えるベスト・ソリューション・パートナーになる」を経営ビジョンに、情報システムにおける企画・調達、設計、構築、導入、運用、保守のライフサイクル全体を手掛ける「統合サポートサービス」で、ハードウェア／ソフトウェアが一体となった、より進化したトータルなソリューションを提供。全国320ヵ所のサービス拠点網と日立ソリューションサポートセンターを中心に、24時間365日万全の体制で、安心と信頼の情報システムを実現します。

■報道機関問い合わせ先

日立電子サービス株式会社 社長室広報グループ【担当：矢野、阿久澤】

〒244-0801 横浜市戸塚区品濃町 504-2

TEL：045-824-1071（ダイヤルイン）

※本リリースに記載の会社名および製品・サービス名は各社の商標または登録商標です。

以 上

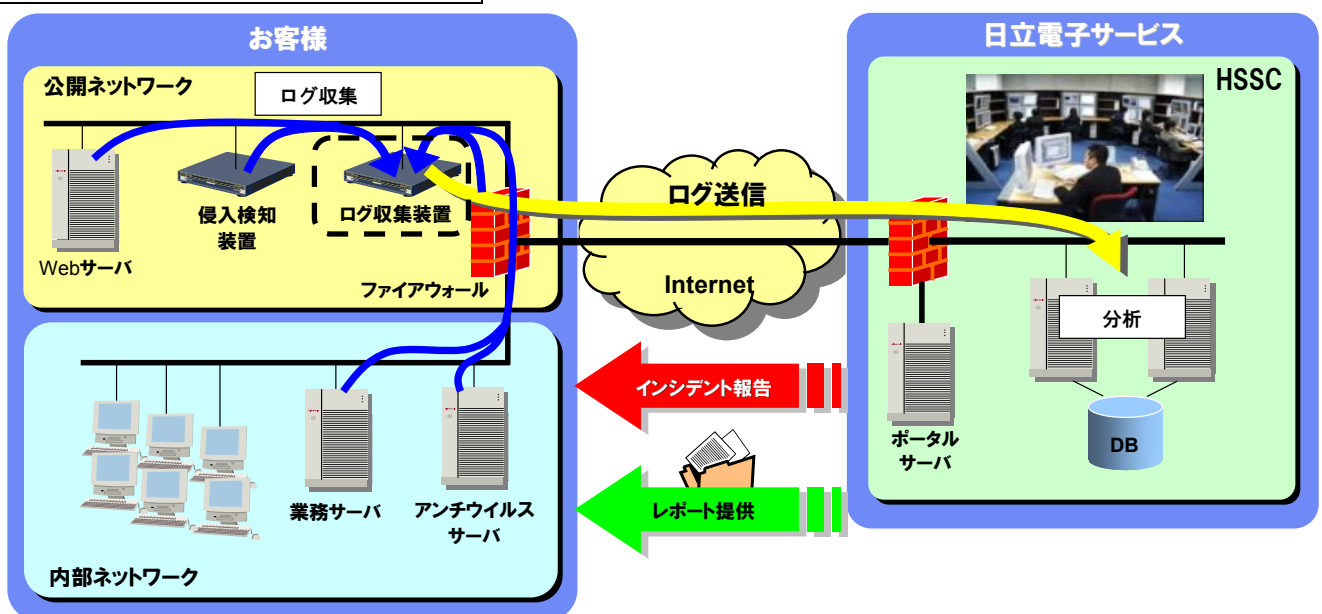
【添付資料】

セキュリティ統合管理ソリューション「SecureEagle/SIM」の概要

サービス概要

サービス名	サービス項目	サービス内容
SecureEagle/SIM (基本サービス)	インシデント監視	お客様システム内のセキュリティログやイベントを相関分析し、単なるアラートではなくお客様へ重大な影響を与える可能性の高いセキュリティインシデントの発生を監視します。インシデントを検知した場合、お客様へその分析結果と影響度、推奨の対策案をご連絡します。これにより、お客様は緊急に対応が必要なインシデントを早期に把握することが可能となります。
	インシデント情報照会	お客様専用のポータルサイトにて、インシデントの詳細情報やレポート、収集した正規化ログを参照することができますので、お客様はいつでも自組織のセキュリティ状態を把握することが可能となります。
	インシデントレポート	お客様システムで発生したインシデント情報を纏めたセキュリティ・インシデントレポートを定期的にご提供します。
SecureEagle/SIM/DRP (オプションサービス)	デバイス詳細レポート	セキュリティ装置毎の詳細レポートを月次または週次で提供し、お客様の幅広いレポートニングニーズに応えることが可能です。

サービス構成 (MSSP 型)



[]: 日立電子サービスが設置するログ収集装置