新規セキュリティサービス EINS/MSS+、EINS/PKI+の紹介

Introduction of New Security Service 'EINS/MSS+' and 'EINS/PKI+'

庄司　治彦　Haruhiko　Shoji
浜井　章弘　Akihiro　Hamai

概要

昨今、個人情報漏洩、ウィルス感染、情報改竄等にみられるようなセキュリティリスクが増大している。これらのリスクに対応するためには、これまでの対策をより発展させた「次世代のセキュリティ対策」が求められている。当社はRSA Security Inc.（以下、RSA社）、Counterpane Internet Security, Inc.（以下、CIS社）の2社と業務提携し、認証局サービス『EINS/PKI十』（PKI:Public Key Infrastructure）と、リアルタイムで不正監視を行うマネージド・セキュリティ・サービス『EINS/MSS十』（MSS:Managed Security Service）の2つの新しいセキュリティサービスを展開する。これにより、ネットワーク・ソリューション・プロバイダとして総合的なソリューションをお客さまに提供いたします。本稿ではこれら2つの新規セキュリティサービスを紹介する。

1. はじめに

昨今のビジネスにおけるセキュリティリスクの高まりとともに企業等においては、暗号化、ファイアウォール、認証メカニズムといった様々な防止技術が取られている。しかし、これらの防止技術も完璧とはいえないのが実状である。攻撃者はソフトウェアの欠陥に付け込んだり、防止技術を迂回する手段を考え出したり、パスワードの盗み聞きなどのソーシャルエンジニアリングという手法を使って防止技術をすり抜けたりする。セキュリティ問題は防止技術だけでは解決することが困難な状況である。セキュリティ対策には防止技術だけではなく、検出と対応のプロセスが重要であると当社は考えている。

当社は強力な暗号による錠と鍵によりデータを守るサービスとしてEINS/PKI+を提供している。また、コンピュータネットワークを守る検出と対応プロセスのサービスとしてEINS/MSS+も提供している。

2. セキュリティ事業の位置付け

当社は現在までに高度な技術力とノウハウ、万全の設備による、専門・特化したフルスコープのサービスプロバイダFSP（Full Service Provider）として以下のサービスを提供してきた。

- ビル設備＋コロケーションiDC（Internet Data Center）
- インターネット接続サービスISP（Internet Service Provider）
- 企業向けFR/X.25/IPネットワークNSP（Network Service Provider）
- EC(*1)，EDIサービス(*2) ASP（Application Service Provider）
- 運用コンサルから運用管理 MSP（Management Service Provider）
- セキュリティ監視、診断サービス SSP

（*1）EC (Electronic Commerce)：電子商取引、インターネットなどのネットワークを利用して、契約や決済などを行なう取引形態。
（*2）EDI (Electronic Data Interchange)： 商取引に関する情報を標準的な書式に統一し、組織間で電子的に交換する仕組み。

(Security Service Provider)

今回、新しくRSA社とCIS社の2社と業務提携することにより、強力な認証方式による電子認証サービス『EINS/PKI+』及び、より強固なセキュリティ監視・診断サービスである『EINS/MSS+』の2つのサービスを追加し、セキュリティサービスのメニューを拡大する。

3. EINS/MSS+について

3.1 EINS/MSS+とは

CIS社は、世界的に著名な暗号学者Bruce Schneier氏が創設したセキュリティのリアルタイム監視を行っている企業である。マネージドセキュリティモニタリングとして、以下の独自のサービスを提供している。

- 30,000以上のルールとお客さまに特化した優先度付けスキームにより個々のセキュリティ製品ロジックを補完するサービス
- 300データソース(監視対象の機器やアプリケーション)をサポートするリアルタイムログ分析
- 機器とアプリケーションの両方のレベルでカスタマイズできるフレームワーク
- 32ヵ国28キャリアの継続的かつグローバルな監視から得られる攻撃兆候のフィードバック

当社はCIS社と業務提携し、日本においてEINS/MSS+としてサービスを展開する。

3.2 サービスの必要性

近年、種々の攻撃やウィルスによるサービス停止、情報漏洩等、セキュリティ問題で企業イメージが傷つき、対応を誤ったために企業活動そのものに影響を及ぼすことも少なくない。遂には企業経営者が責任を取ることさえ起こりえる。これらの問題を解決する手段としては一般的に、ファイアウォール、IDS(侵入検知システム：Intrusion Detection System)、ウィルス対策ソフト等が存在する。

これらのセキュリティ対策ツールを導入するだけならば比較的簡単であるが、充分なセキュリティを確保するためには、ログの監視、対策ツールのアップデート等の運用・監視を常時行わなければならない。しかし、セキュリティ管理部門は次々に出現するウィルスや新たな手法による攻撃からシステムを守る対策や、一般社員の啓蒙活動に多くの時間を取られる。このため、運用・監視にまわす時間を充分に取れないことが多い。

3.3 サービス概要

EINS/MSS+サービスの概要を図1に示す。EINS/MSS+サービスでは、お客さまのネットワーク内にサーバ、ファイアウォール、IDS等のアラートやログを収集するセントリーと呼ばれる装置を設置する。セントリーは米国の2箇所のSOC(Secure Operation Center)とインターネットを経由しても安全なトンネル接続する。SOCに集まったアラートやログは、CIS社が開発したSOCRATESと呼ばれる相関分析エンジンを用いてフィルタリングすることによりSOCの要員数を削

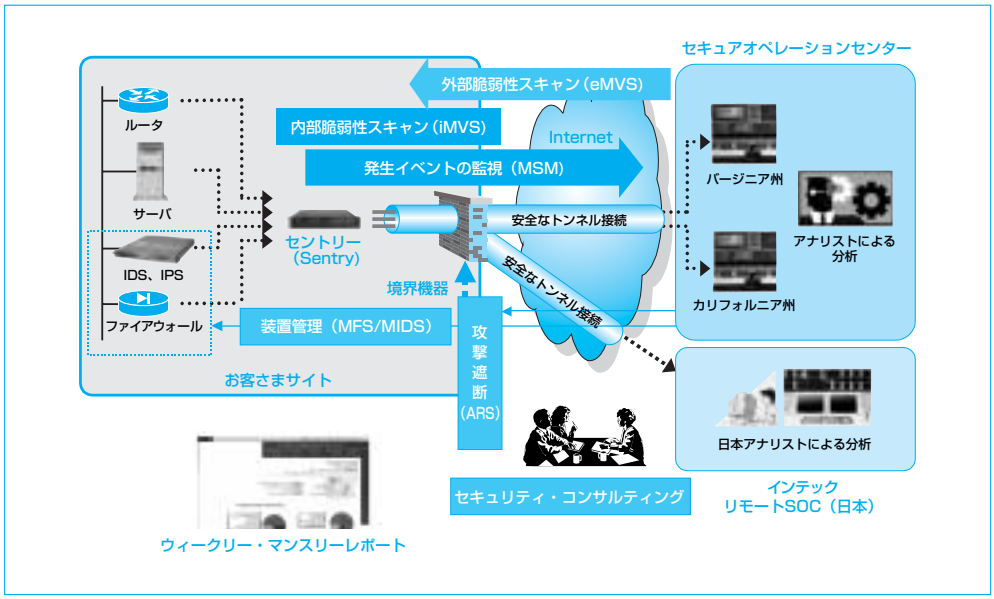


図1 EINS/MSS+サービス概要

減することができる。これにより、お客さまが全ての作業を行った場合に比べて安価にサービスを提供することができる。また、SOCRATESに届いたアラートは、自動でチケットとして生成され、高度なスキルを持った専門の監視要員が24時間365日リアルタイムで処理し、精度の高い監視を行っている。

これらの監視結果は、メール、電話等、お客さまと相談の上、最適な方法で連絡する。また、WEB上で安全な認証を用いて、お客さまに週次、月次の監視レポートを提供する。

その他、オプションとして、外部・内部の脆弱性検査、お客さまが管理しているファイアウォールやIDSを当社が代わりに管理することができる 。

3.4 サービスメニュー

サービスメニューとして、基本サービスとオプションサービスがある。基本サービスには主にログやイベントのリアルタイム監視サービスであるMSM（Managed Security Monitoring）と内部の脆弱性スキャンサービスであるiMVS（Internal Managed Vulnerability Scan）が含まれる。EINS/MSS＋サービス加入のためには基本サービスが必要である。

また、お客さまのネットワーク内に一つ以上のIDSが必要である。お客さまが現在IDSを持たない場合、オプションサービスMIDS（Managed IDS）を契約していただくことで、お客さまにIDSを提供できる。

オプションサービスでは、外部脆弱性スキャンサービスeMVS（External Managed Vulnerability Scan）、前述のIDS、あるいはIPS(Intrusion Prevention System)、ファイアウォールの管理サービス、MIDS、MIPS（Managed IPS）、MFS（Managed Firewall Service）、緊急の攻撃遮断サービスであるARS（Active Response Service）があり、個別に必要に応じて提供できる。

サービスメニューを表1に示す。

3.5 効果

セキュリティ対策は運用・監視という手間がかかり、かつ専門知識が必要な業務である。この業務を EINS/MSS＋ でアウトソーシングしていただくことにより、お客さまの人件費やセキュリティ製品に対する投資を抑制できる。また、セキュリティ専門家が常時監視することで、ビジネスリスクを低減できる。

表1　EINS/MSS＋サービスメニュー

サービス カテゴリ	サービス名	概　　要
基本サービス (MSM&iMVS)	マネージド・セキュリティ・モニタリング (MSM)	SOCサービスの基本となるサービスで、SOCからリモートでのサイト監視を実施
	脆弱性スキャン (iMVS)	内部機器のスキャン：専用機器をサイトに設置し、脆弱性検査をオンデマンド（随時）で実施
オプション サービス	脆弱性スキャン (eMVS)	外部機器のスキャン：SOCセンターよりリモートで脆弱性検査をオンデマンド（随時）で実施
	デバイス・マネジメント (MFS/MIDS /MIPS)	ファイアウォール、IDSおよびIPSをSOCより遠隔管理するサービス
	アクティブ・レスポンス (ARS)	サイトの境界エリアに専用機器を設置し、緊急時にSOCより攻撃を遮断するサービス
	セキュリティ・コンサルティング	ポリシーの作成から構築までのセキュリティ・コンサルティングをおこなうサービス

4. EINS/PKI＋について

4.1EINS/PKI＋とは

RSA社のデジタル証明書管理システム(RSA Keon Certificate Authority) を使用して構築したシステムにより、安全なデータ交換に必要なデジタル証明書を様々なサービス形態でお客さまに提供している。

4.2 サービスの必要性

今までは、専用線やフレームリレー網といった比較的アクセスが制限されていたレガシーなネットワークを利用して情報やデータを交換していた。現在は、誰でも接続できるオープンなインターネットを利用して行われるようになってきている。当社はネットワークサービス事業者として、今後も今までと同等以上のセキュリティを確保したネットワークサービスを提供していくことを使命と考えている。そのため、ファイアウォールやIDSといったシステムへの不正なアクセスを防御するためのソリューションEINS/MSS＋を提供している。また、情報やデータを広く安全にアクセスさせるため、本人性の識別/認証/権限付与/完全性/守秘性/否認防止といった、セキュリティ対策の基本機能を実現するために必要な電子証明書を発行するソリューションEINS/PKI＋を提供している。

4.3 サービス概要

EINS/PKI＋で提供するサービスの特徴は以下の通りである。

- RSA社のルート認証局によるパブリック証明書の発行
- 特定の通信相手との間で利用されるプライベート証明書の発行
- Web Trust for Certification Authorities(*3)監査基準に準拠した設備での発行・管理
- USBトークンやフレキシブルディスクに証明書を格納するサービス
- Webサーバからオンデマンドでリアルタイムに証明書を発行するOneStepサービス
- 強固なセキュリティを確保した設備内にお客さまの認証局をハウジングするサービス

4.4 サービスメニュー

(1) 証明書発行サービス

インターネットを介した企業間の取引などで利用されるパブリック証明書（SSLサーバ証明書、クライアント証明書）や、企業内などのクローズドな環境内での利用が想定されるプライベート証明書を発行するサービスである（図2）。

当社のパブリック認証局はRSA社のルート認証局によって承認されているため、一般的なブラウザからは警告なしでSSL通信を行うことができる。

(2) 証明書格納サービス

お客さまからのユーザ情報を元にプライベート証明書を一括発行し、USBトークンやフレキシブルディスクに格納するサービスである（図3）。

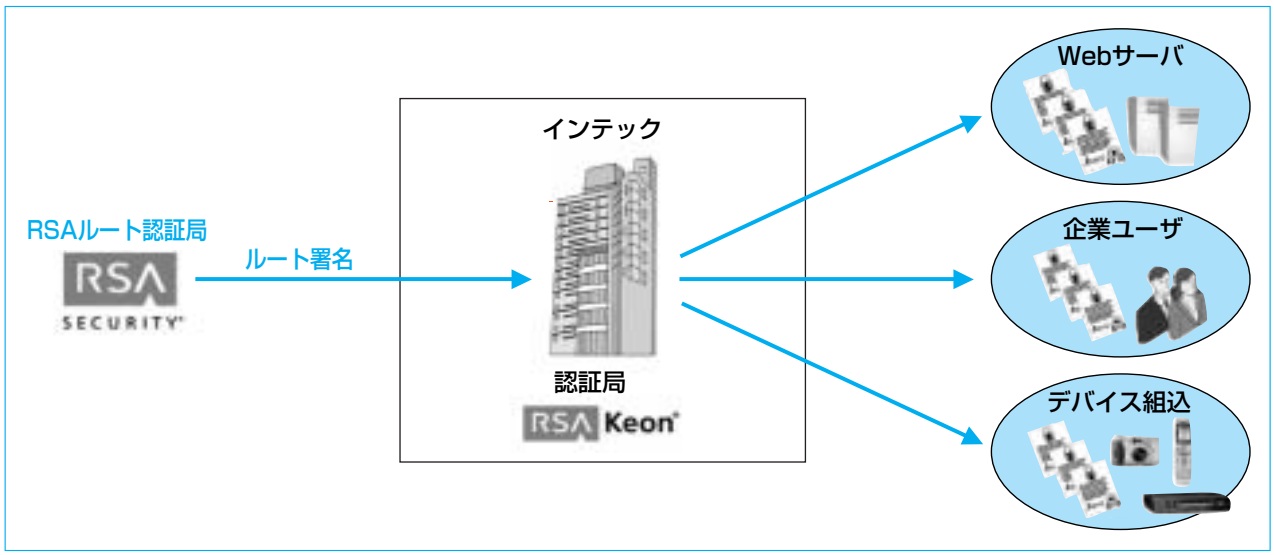


図2　証明書発行サービス

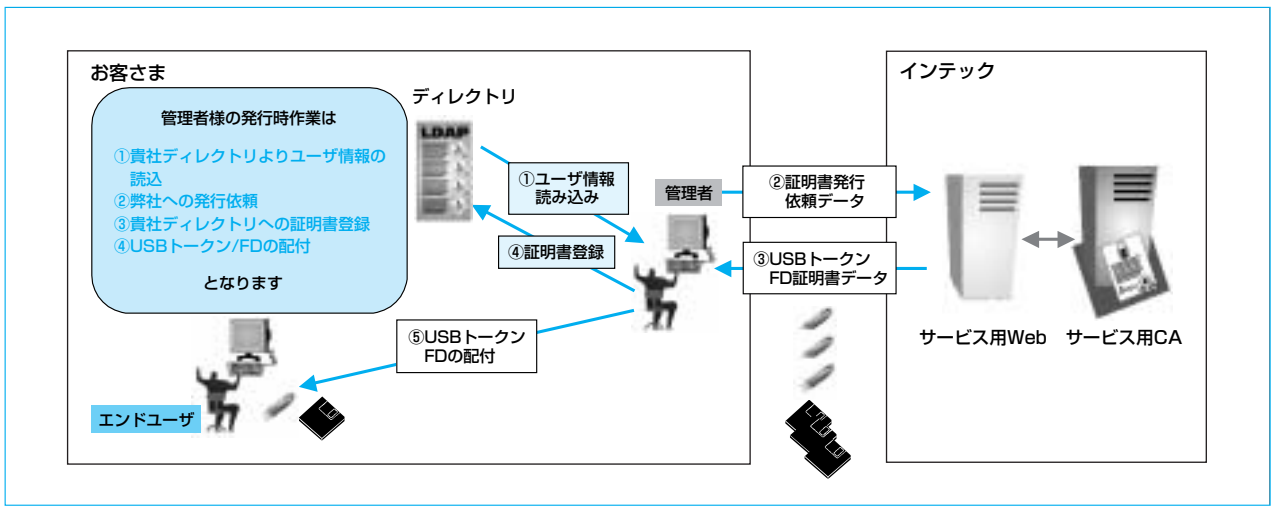


図3　証明書格納サービス

(*3) WebTrust for Certification Authorities：電子認証局の信頼性や安全性を審査する基準、米国公認会計士協会（AICPA）および、カナダ公認会計士協会（CICA）が確立。

(3) OneStepサービス

エンドユーザがOneStep用のWEBサーバにアクセスし、必要なときにリアルタイムでクライアント証明書を発行するサービスである。管理者の登録・管理業務の負荷を大幅に軽減することができる。

当社認証局内のOneStepサーバを利用するシェアード型（図４）と、OneStep用WEBサーバをお客さま設備内に設置するお客さま設置型（図５)のサービス形態がある。

シェアード型サービスでは、OneStepサーバを当社が運用・管理する。このため、ユーザの登録・管理業務の負荷が大幅に軽減でき、小規模なプライベート証明書の発行に適している。また、お客さま設置型サービスは、当社への発行依頼の作業が必要なく、タイムリーに発行できるため、比較的大規模な発行業務に適している。

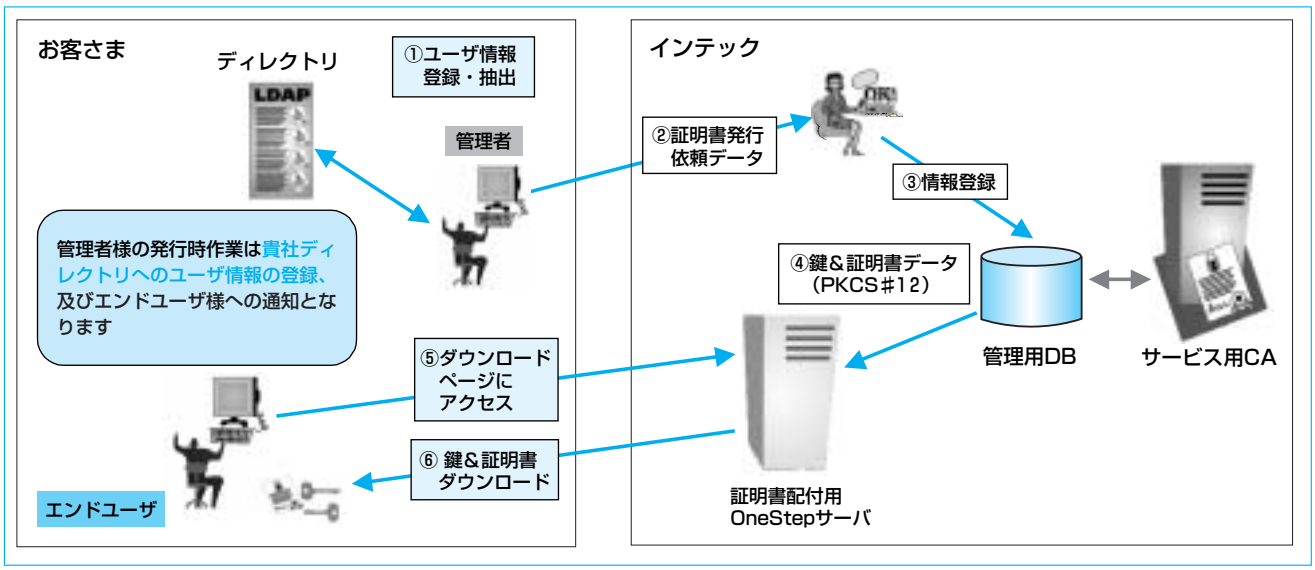


図４　シェアード型サービス

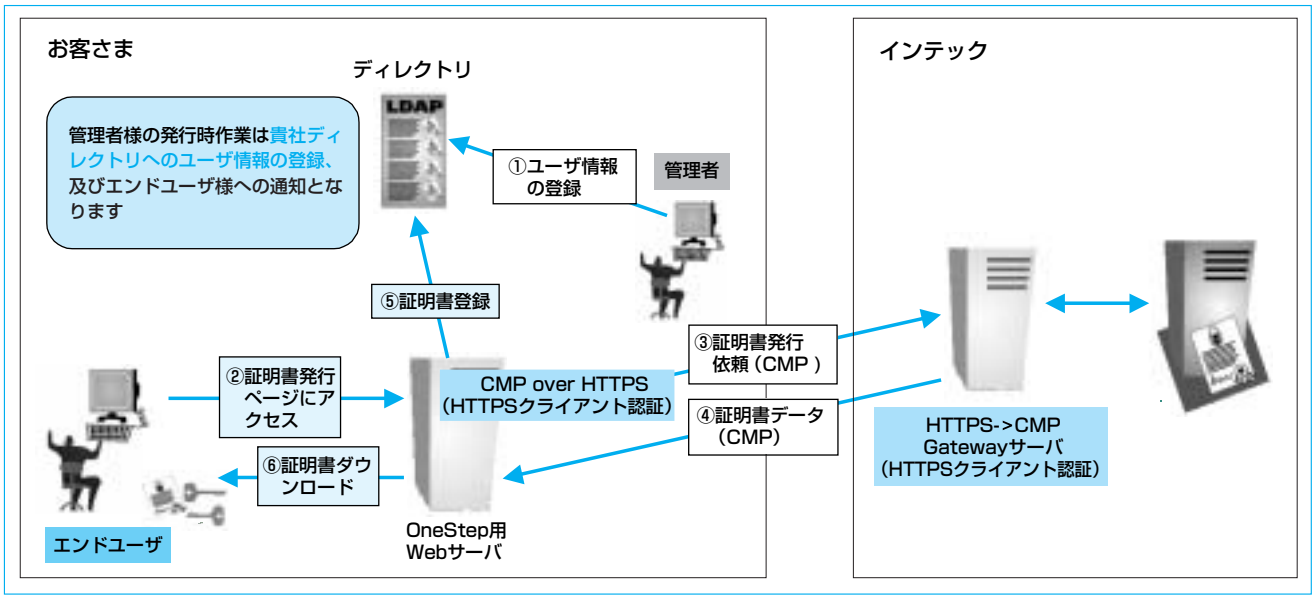


図５　お客さま設置型サービス

（4）認証局ハウジングサービス

当社の証明書発行サービスは、WebTrust for Certification Authorities監査基準に準拠（2005年3月取得予定）した設備と運用により強固なセキュリティを確保した状態で運営している。これとほぼ同等な設備をハウジングスペースとして提供するサービスが認証局ハウジングサービスである。

4.5 効果

証明書格納サービスやOneStepサービスなどの提供により、お客さま管理者の作業負荷を劇的に減らすことができる。さらに、証明書の管理・運用までを当社が代行する運用代行サービスを提供することができる。また、様々な使用用途に合わせた証明書を発行できるため、EDIなど特定企業間のデータ交換サービスの実現、IP-VPNネットワークおよびECサイトの構築・運用など、様々な場面で柔軟で安全性の高いサービスを提供することができる。

5. おわりに

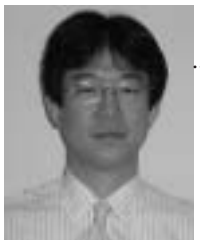
景気低迷が続く中、ＩＴサービスにおけるセキュリティ面への投資に関しては、大企業を中心に底堅く、またセキュリティへの関心度も年々高まりつつある。昨今、顧客情報流出を始め、類似の事件が頻発し、情報漏洩対策を中心とした内部セキュリティへの関心も高まっている。

今後、当社ではトータルなセキュリティソリューションを提供できる企業として認知度を高めてゆきたいと考えている。

参考文献

（1）Bruce　Schneier（山形浩生訳）：“暗号の秘密とウソ”翔泳社,（2001）

（2）Andrew Nash、William Duane、Celia Joseph、Derek Brink（スリー・エー・システムズ訳　RSAセキュリティ監修）：“PKI e セキュリティの実装と管理”，翔泳社,（2002）



庄司　治彦
Haruhiko Shoji
・ネットワークソリューション事業本部
ネットワークサービス事業部
ネットワークテクニカルセンター
グループリーダー
・iDC構築・運用に従事

浜井 章弘
Akihiro Hamai
・ネットワークソリューション事業本部
ネットワークサービス事業部
ネットワーク技術部
グループリーダー
・WEBサイト設計・構築・運用に従事