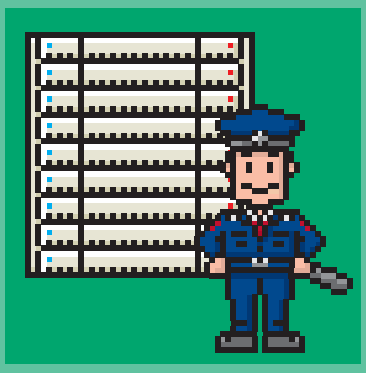
【特集2】



「個人情報保護法」対策の第一歩

セキュリティー機能で選ぶレンタルサーバー

P.102～P.105
株式会社大塚商会 セキュリティコンサルタント
小林 健・長野豊佳
P.106～P.109
大澤文孝

「個人情報の保護に関する法律（保護法）」で処罰される前に、駆け込みで個人情報の流出事件が多発している。特にウェブサイトへの技術的・人為的な不正アクセスで情報を持ち出されるケースが多い。このような事件を防止するために、ウェブサイトを構築する側は何をすればいいのか。本記事では、保護法とは何かを把握するとともに、レンタルサーバーを利用して個人情報を扱う際に配慮すべき点についてまとめた。今一度自身のウェブサイトを確認してみよう。

たび重なる個人情報流出事件で注目されるインターネット利用の盲点

大企業だけの問題ではない！
誰もが保護法を守らなければならない

個人情報保護法が、2005年4月1日に完全施行される。個人情報の流出事故を起こしたり、勝手に収集・利用・提供したりして、個人情報の表す本人から苦情を受けたにもかかわらず適切な対応を怠り、所轄官庁大臣の命令に従わなかった場合などに、担当者や管理者のほか、勤め先の社長や会社にも6か月以下の懲役か30万円以下の罰金が科されることがある。

個人情報保護法は、個人にも適用される。たとえば個人事業でウェブサイトの掲示板を開く、アンケートを採集する、アクセスログを収集するなどの場合は、保護法の要求事項を守らなければならない。現住所などの連絡先やクレジットカード情報にかぎらず、メールアドレス1つでも「個人情報」になる。

保護法で罰せられるのは、過去6か月に5000件以上の個人情報を持っていたことのある事業者となっている（保護法施行令）。ちょっとしたオンラインショップを開設したら、すぐに達成する件数だろう。もっとも、保護法で直接罰せられなくても、流出事故や不適切に取り扱って起訴された場合、保護法を参照して裁判が不利に進むこともありえる。どんな個人情報でも保護法の要求に従って取り扱うべきだ。

■個人情報保護法への対策「10項目」
保護法を守り、罰せられないようにするには、最低限、以下の10項目の対策を行う。
❶個人情報保護に関する方針をわかりやすい文書（プライバシーポリシー）としてウェブサイトなどで公開する（政府の個人情報保護基本方針6項）。
❷個人情報の保護体制を決める（同6項）。
❸誰が何のためにどのように個人情報を使うか（利用目的）を決めて文書にまとめ（保護法15条）、本人に知らせて（同18条）、利用目的どおりに使用する（同16条）。
❹適正に収集、取得する（同17条）。
❺安全に取り扱う（同20条）。
❻従業員を監督する（同21条）。
❼業務委託先を監督する（同22条）。
❽第三者に提供する場合は本人の事前承認を得る（同23条）。
❾持っている個人情報の種類を公表し（同24条）、本人の要請に応じて個人情報の内容を開示（同25条）、訂正・削除（同26条）、利用停止（同27条）をする。
❿本人からの苦情の対応に必要な体制を整備し、対処する（同31条）。

■最近の主な個人情報流出事件

●内部犯行、重過失
パターン：ノートパソコンなどの盗難、廃棄パソコンのデータ消し忘れ、メール／FAXの送信先間違い、名簿業者などへの名簿売却
原因：持ち出し・業務委託先などの管理不十分、遺恨退職者や取引先の放置、データファイルや記録装置の利用制限不足、ID／パスワードの管理不足、システム管理者の恣意、従業員の認識不足、処罰などの抑止不足、個人情報やシステムの放置、モバイル・PDA・携帯電話の管理不足、私有物管理不足、ルールの未整備、教育不足

●外部犯行
パターン：不正アクセス、通信パケット盗聴、なりすまし
原因：アクセス権限の設定ミス、バグの放置、ファイアーウォールや無線LANなどのシステム上のミス、クロスサイトスクリプティング（XSS）やcookie盗聴などのアプリケーション上の問題、システム管理者の管理不足、IDS（不正侵入検知）などの対策不足、ログの管理・分析不足、経営層の理解不足による予算と人員の不足

●その他
パターン：システム障害による個人情報データの消失、パソコンの盗難、苦情対応ミス、不適切な利用
原因：苦情の軽視と放置、障害・危機・被害管理不足、情報価値とリスクの認識や管理・対策不足、営利や利便性への傾注、順法意識の欠落と認識違い、業務統括・統制・牽制・事故発見・報告体制の未整備

Part.1

すべてのウェブマスター必見！ 個人情報保護法で変わるウェブサイト

個人情報保護法の存在は少なからず知っていても、具体的には何を行うべきなのか、イマイチ理解できていない企業や個人事業者は多いだろう。ここでは主に個人情報を扱うサイトを管理・構築するウェブマスターが知っておくべき事項を列挙しよう。

コレで解決！ 一目でわかる個人情報保護法

個人情報を扱う際、利用目的をウェブサイトに掲示して、それに対して本人から同意を得なければならない。さらに問い合わせや苦情の相談方法、安全対策も示して、それらを実施して記録する必要がある。これら具体例をQ＆A式で紹介しよう。

Q「個人情報保護」って何？

A保護法は1条に法の目的として「個人情報の有用性に配慮しつつ、個人の権利利益を保護する」と揚げている。また、政府基本方針によると「(保護)法第3条は(中略)個人が『個人として尊重される』ことを定めた憲法第13条の下、慎重に取り扱われるべきことを示す」としている。
つまり、①利用目的の明示のうえで個人情報を収集し、開示・訂正・削除・利用停止の要求に対応するといった「本人の意思の尊重」が確保されること、および②事件や事故を招かないように「安全性確保」がなされていることの2点を適正に行うのが個人情報保護の施策だ。この個人情報の取り扱いに関する施策によって、個人の尊重を確保することが個人情報保護になる。

Q保護にあたってどのような責任体制が必要か？

A社長などの代表者以下、社内で保護法の認識を維持・向上させるための「維持向上体制」と「監査体制」を構築しておこう。維持向上の体制には、保護法の施策を統括する責任者とライン部門やスタッフ部門の管理体制、教育・システム管理・相談窓口の体制、不測事態が発生したときの危機管理体制が必要だ。保護法の施策の立ち上がり段階では、利用目的の内容や、システムセキュリティーを確保するための確認作業や承認を得るような業務手順を設けるべきだろう。
監査体制は、維持向上体制から独立させて、個人情報を取り扱う業務を行っていない役員クラスの人を監査責任者とする。また、監査に必要な知識と監査技術を持つ人を監査担当者に任命するとよい。監査担当者を社内で用意できない場合は、社外に委託する必要がある。

Q安全管理対策は何をどこまでやるのか？

A個人情報の特性と取り扱う業務によって、対策の内容と深さが変わってくる。官公庁や業界団体などのガイドラインや、以下の規範を参考にして事業ごとに決める必要がある。

・個人情報保護に関する認証制度であるプライバシーマーク制度の審査基準(JIS Q 15001)
・情報セキュリティーに関する認証制度であるISMS(情報セキュリティーマネジメント)適合性評価制度の認証基準
・情報セキュリティー管理基準

Q苦情対応は何をすればいい？

A苦情は、クレーム対応に失敗して収拾がつかなくなった状態と考えられる。また、苦情が来てからも適切に対応していないと、官庁に苦情が行って、保護法の罰則を科される恐れがある。
苦情が来てしまった際には、誠意を持って対応し、社内や所轄官公庁などに迅速に報告する必要がある。普段から相談窓口で対処方法のマニュアルを作成し、スタッフに対して対処方法の訓練を行おう。
そもそもクレームや苦情を招かないように、あらかじめ適正な利用目的を的確に定めて本人の同意を得たうえで個人情報を取り扱い、事件が起きないように安全管理や委託先などの監督を適切に行うべきだろう。

Q従業員をどう監督するか？

A社員の採用時、派遣社員の受け入れ時、退職や離職時に、個人情報保護の重要性や施策などに関する説明を行ったうえで誓約書に署名押印してもらう。実際の業務でもOJT教育によって実務的な注意を促す。教育後は、テストや効果測定を行うべきだ。
また、業務作業の内容やアクセスログ、入退室管理などあらゆる場面で「記録」を残しておくようにする。

Q委託先をどう監督するか？

A委託先は委託元の目が行き届かないため、調査して選定するとともに守秘契約を締結する。委託業務を開始したあとも、個人情報の取り扱いに関する査察を定期的に行い、問題があれば指導して改善を依頼し、改善状況を確認する。
プライバシーマークやISMS(情報セキュリティーマネジメント)認証を取得している企業に業務を委託することが望ましい(105ページ参照)。

Qどのログを残すのか？

A収集から利用、提供、業務委託、返却、消去、廃棄にいたるまでの個人情報の取り扱いや承認などの記録と、データベースやファイルサーバー、ファイアーウォールなどのログ、施設やシステムへの出入り記録、ドアの開施錠の記録が必要になる。
レンタルサーバーなどで社外のサービスを利用する場合は、業務委託先でログが保管される。これらのログのうち自社の分を入手できるようにしておく。

アンケート収集も細かな配慮が必須！
個人情報収集の際の注意点

ウェブサイト構築における
一般的な注意事項

ウェブサイトでは、以下のようなさまざまな場面で個人情報を収集している。

・電子商取引での注文
・会員ページなどのログイン・認証
・ページ移動
・パスワードリマインダー
・アンケート入力
・資料・情報請求
・ウェブメール
・掲示板、チャット
・アクセスログ
・cookie　　ほか

これを見ると、ウェブサイトやページの数だけ個人情報を収集する場面があるとも言える。しかし、サイトの訪問者に、個人情報が収集されているということが意識できているとはかぎらない。

オンラインショッピングなどの電子商取引では、入力内容の確認ページで［OK］ボタンがクリックされた時点で注文意思を最終的に確認している。注文内容の送信も、SSLの暗号化などによって機密性を保っている。この暗号化はもはや当たり前だ。

しかし、アンケートや資料請求のページでSSLを実装しているものはまだまだ少ない。まして、あらかじめ断ってからcookieなどを利用して情報の登録を行わせているページは少ない。さらに、ニュースなどの報道でしばしば取り上げられているにもかかわらず、クロスサイトスクリプティング（ウェブサービスなどにアクセスしてきた人に対して意図しないプログラムをダウンロードさせるようなセキュリティーホール）やクエリストリング（URL表記に理解しやすいパラメーターを表示してページ間でやり取りするとページ改ざんの被害に遭いやすい）の対策を行っていないページも多い。

このようなコンテンツ作成上の問題をチェックリストにして管理し、1つ1つ対処して消していくほか、ウェブサーバーのセキュリティー対策を行う。これには、たとえばサーバーOSのバグフィックスパッチの適用、ウイルスチェックツールの運用、セキュリティー侵害の防止や検出ツールの利用などがある。

また、サーバーのセキュリティーが物理的に侵害されないように、サーバーマシンルームの入退室管理を行ったり、盗難に遭わないように夜間を含む警備や従業員の監督を行ったり、ビデオカメラで記録したりする必要もある。さらに、データバックアップテープなどの記録媒体の保管やデータ保全を図ることも重要だ。

ウェブサイトにおける個人情報収集の注意点

その❶ あらかじめ利用目的を明示して本人から同意を得る

・ウェブサイトで個人情報を入力させる際、登録内容の確認ページにある登録ボタンの近くに利用目的を記載し、内容を読んだうえで登録させるようにしよう。利用目的が長文の場合は、登録ボタンの近くに「利用目的に同意したうえで登録してください」と表記して、利用目的へのリンクを張るといい。

・単に目に触れただけでは同意したという確実な証拠が残らない。別途、契約書などの書面や登録内容の確認メールに利用目的を明記するなどして、利用目的が確実に登録者の目に触れるようにする。

・登録後もいつでも利用目的を登録者が確認できるようにウェブサイトに掲示しておく。利用目的の内容を変更した場合は、以前の利用目的も保管して履歴として掲載しておくとベストだ。

その❷ 登録情報の安全性を確保する

・個人情報を収集する際の安全性は、登録情報を覗き見や改ざんがされないようにSSL暗号化などによって確保する必要がある。登録に際して、個人情報を会社内で使うのか、あるいは第三者に提供するのかを利用者にわかるようにする。フレームを使ったページ構成では利用者が登録先を認識しにくいかもしれない。

・アプリケーション上、クエリストリング（URLに表示される“？”以降のパラメーター）に個人情報を含まない、cookieに重要情報を含まない、セッションタイムアウトを短く設定するといったことが必要だ。データベース関連のセキュリティーホールについても、データベース用のアカウントを用意してアクセス制限を管理する、クロスサイトスクリプティング対策を行うほか、一定時間ごとに自動でログオフするような機能などを設けたほうがいい。

・パスワードを外部に漏らさないために定期的に変更するといった、登録者側で行うべきことを登録者に通知しておきたい。

その❸ 委託業者を利用する場合もその旨を明記する

・利用目的に、業務を委託することを明記して登録者が見られるようにする。

・委託業者には、経営状態や個人情報保護、情報セキュリティーの対応状況、サーバーや端末の管理状態、マシンルームを含む施設の管理状況、メインテナンス体制、リモートメインテナンス上のセキュリティー状況などを確認しておこう。また、委託業者がサーバー管理などを再委託していないかを確認し、再委託している場合は再委託先を適切に管理しているか確認する。

・委託業務が行われていたら、個人情報の取り扱い状況を確認するためにできるだけ現地視察を行うようにする。業務委託が1年以上にわたるのならば、取り扱い状況を再確認するべきだろう。

・これらの確認結果は、調査記録として文書化して保管しておこう。

明確なプライバシーポリシーの必要性 レンタルサーバーのあり方も変わる

保護法に対応した
プライバシーポリシーを掲載する

現在、プライバシーポリシーを掲載しているウェブサイトもあるが、技術的な内容のみで、政府基本方針が要求している要件を満たさないものがほとんどだ。

まずは、十分な内容を盛り込んだプライバシーポリシーを策定し、ウェブサイトに掲載する必要がある。

レンタルサーバー選定の評価基準に
情報セキュリティーの観点を盛り込む

レンタルサーバー選定の際、従来は価格や帯域(レスポンス)、ディスク容量、稼働率、障害復旧時間、サポート機能とメニュー、サーバーを置いている場所などを評価して選定していただろう。

今後は、これらを確認するのはもちろん、情報セキュリティーの観点に基づく評価も行おう。1つのサーバーを複数のクライアントが共用している場合、アクセス権限を適切に設定して、他のクライアントが悪さをしないように管理している事業者を選ぶべきだ。

サーバーの管理状況を査察できない場合もあるだろう。この場合は、プライバシーマークやISMS認証などを取得している業者を選定することが望ましい。

個人情報を適切に取り扱っているとして認定を受けた事業者は、プライバシーマークをウェブサイトや印刷物に掲載できる。保護法はプライバシーマークの取得を強制していないが、取引先の安全性の確認や適正な事業を行っているかの判断基準となるため、プライバシーマークを取得していない事業者よりも安心して個人情報の取り扱いを依頼できる。

なお、レンタルサーバーは業務委託に該当するので、これまで述べてきた、委託時に行うべき事項にも留意しておこう。

■プライバシーポリシーとは

自分たちが個人情報をどう使うかを明文化したもので、社長などの代表者が社内・社外に表明する。
内容は、政府基本方針に規定された、目的外での利用禁止や第三者への提供の有無、苦情処理の方針、順法、利用目的の通知・公表・変更の有無、開示・訂正・削除・利用停止の要請先と手順、事故発生時の対応計画などになる。保護法が要求する安全管理対策や従業員・委託先の監督についても書くべきだろう。また、ウェブサイトに掲載する場合はcookie情報やアクセスログ(利用統計など)、子供や未成年者への注意についても記載すべきだ。

■ウェブサイトの個人情報保護として留意すべき主な法令と規範など

【主な法令】
URL http://law.e-gov.go.jp
・個人情報保護法(個人情報の保護に関する法律)
・個人情報保護法施行令(個人情報の保護に関する法律施行令)
・プロバイダー責任法(特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律)
・IT書面一括法(書面の交付等に関する情報通信技術の利用のための関係法律の整備に関する法律)
・電子契約法(電子消費者契約及び電子承諾通知における民法の特例に関する法律)
・電子署名法(電子署名及び認証業務に関する法律)
・特商法(特定商取引に関する法律)
・迷惑メール防止法(特定電子メールの送信の適正化等に関する法律)
・景品表示法(不当景品類及び不当表示防止法)
・不正アクセス禁止法(不正アクセス行為の禁止等に関する法律)
※ほかに対面・訪問販売、通信販売、著作権、営業機密などに関する従来の法令にも留意する。

【主な規範など】
URL http://www.meti.go.jp/kohosys/press/0004141/0/030613denshishotorihiki.pdf
・電子商取引等に関する準則
URL http://privacymark.jp/ref/jisq15001.html
・JIS Q 15001「個人情報保護に関するコンプライアンス・プログラムの要求事項」
URL http://www.jsa.or.jp
・JIS X 5080(ISO/IEC 17799)「情報技術ー情報セキュリティマネジメント実践のための規範」
・JIS Z 9920「苦情対応マネジメントシステムの指針」

■安全性を表現する各種制度

通称	プライバシーマーク制度	ISMS認証	オンライントラストマーク制度
正式名称	プライバシーマーク制度	情報セキュリティマネジメントシステム適合性評価制度	オンラインマーク制度
運営	財団法人日本情報処理開発協会	財団法人日本情報処理開発協会	社団法人日本通信販売協会、日本商工会議所
URL	http://privacymark.jp	http://www.isms.jipdec.jp	http://www.jadma.org/ost/(日本通信販売協会) http://mark.cin.or.jp (日本商工会議所)
対象者	日本国内に事業拠点を持つ民間事業者	すべての業種・業務分野の事業者	インターネットを利用して消費者向けの通信販売を行っている事業拠点を国内に有し、1年程度の活動歴がある事業者
申請範囲	全社的な申請が原則	組織の必要に応じて適用範囲を決定する	消費者向け電子商取引事業
保護対象	組織が取り扱う個人情報	保護すべき情報資産を組織が識別して対策する	消費者の電子商取引に関する取引
管理範囲	社内および委託先の安全管理、提供の管理、個人情報の主体の権利への対応	組織の情報資産の管理	電子商取引に関する取引行為
内容	JIS Q 15001:1999 に基づいて個人情報の取り扱いを適切に行っている民間事業者に、「プライバシーマーク」の使用を認める制度。民間事業者が積極的に推進する自主的な規制、努力にインセンティブを与えるとともに、消費者などの個人が民間事業者の個人情報の取り扱いが適切であることを容易に判断できるようにするもの	英国規格BS 7799-2:2002に基づくISMS認証基準(Ver.2.0)への適合性を評価して認証するもの。技術的なセキュリティー対策と組織全体のマネジメントの両面から情報セキュリティーマネジメントに対する第三者評価を行う	消費者向け電子商取引(BtoC)を行う事業者を審査し、適正な取引を行っていると認めた場合にオンラインマークを付与する制度。ただし、事業者が提供する商品・サービスなどの内容や品質を保証したり、事業者の経営内容を保証したりするものではない

Part.2

個人情報守秘に不可欠 セキュリティー対応で選ぶサーバー

ウェブサイトで集めた個人情報はサーバーに保存される。このためレンタルサーバーを選ぶときには、機能の豊富さだけでなく、セキュリティー機能も重視すべきだ。ここでは、個人情報守秘のために不可欠なレンタルサーバーの機能とサービス内容を見ていこう。

サーバーの規模や種類で異なる 安全性への落とし穴

共用型のレンタルサーバーは 事業者の管理体制が最重要

レンタルサーバーでもっとも手軽な共用サーバーでは、レンタルサーバー業者の管理体制がポイントとなる。たとえばセキュリティーホールが発見されたとき、それを修復するのはレンタルサーバー業者だ。各ユーザーはサーバーの設定権限を持たないため、セキュリティーホールが発見されても修復できず、レンタルサーバー業者に任せることになる。

よって迅速な管理体制がとられていないと、長い間セキュリティーホールが放置されて、そこを狙った不正アクセスによってデータを盗まれてしまう可能性があるし、誤った管理が行われると、他のユーザーに自社のデータが見えてしまうという事故も起こりうる。

専用型のレンタルサーバーは すべて自社で管理するのが基本

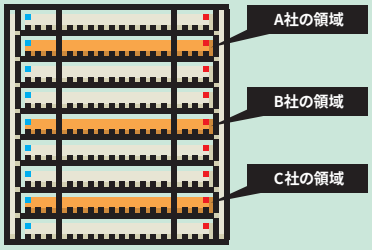
一方で、1台のサーバーを1社で占有する専用型のレンタルサーバーは自社専用であるため、他のユーザーにデータを見られてしまう心配はない。専用サーバーでは、root権限を持ち、構成を自由に変更できるのが一般的だ。

しかしroot権限を持つ専用サーバーでは、サーバーを自社で管理するということを忘れてはならない。セキュリティーホールの修復や攻撃から守るセキュリティーの構成などの管理を怠れば、たちまちデータ流出などの事故が起こりかねない。

よって社内にサーバーに詳しい人材がいないならば、むしろ共用型のレンタルサーバーやroot権限を持てない専用サーバーを選び、管理をレンタルサーバー業者に任せてしまったほうが安全だ。

近年では、共用サーバーではあるものの仮想的なroot権限を持てるバーチャルサーバーサービスもある。サーバーの管理はしたくないが、root権限は必要という場面では、バーチャルサーバーを使うと管理の手間を軽減できる。

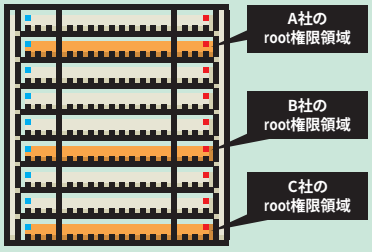
■共用型レンタルサーバーの場合



自社でサーバーを管理しなくてよい
セキュリティーの強度は、レンタルサーバー業者の管理体制次第

自社でサーバーの設定変更はできない
セキュリティーホールが見つかっても、自社では直せず、レンタルサーバー業者が直すのを待つしかない。業者が誤った設定をすると、他のユーザーにデータを参照されてしまう恐れもある

■バーチャルサーバーの場合

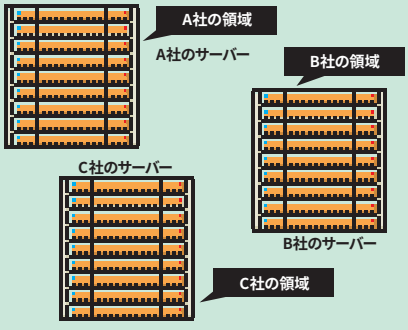


自社でサーバーを管理しなくてよい
セキュリティーの強度は、レンタルサーバー業者の管理体制次第

自社で自分のroot権限領域内の変更はできる
新たなアプリケーションをインストールしたり、設定を変更したりするとセキュリティーホールとなる危険性がある

自社でサーバー全体の設定変更はできない
セキュリティーホールが見つかっても、自社では直せず、レンタルサーバー業者が直すのを待つしかない

■専用型のレンタルサーバーの場合



サーバーは1社占有
同居する他のユーザーは存在せず、それらのユーザーにデータを見られてしまう心配はない

すべての設定を自社で行う
サーバーの運用管理は自社の責任。セキュリティーホールの修正なども含め、すべて自社で対応する。新たなアプリケーションをインストールしたり、設定を変更したりするとセキュリティーホールとなる危険性がある

なりすまし行為からソーシャルクラックまで 不正アクセスを未然に防ぐ

暗号化でパスワード漏洩やデータの盗聴を防止する

サーバーのセキュリティーというと、セキュリティーホールについて語られることが多いが、データ流出という面で考えると、パスワードが漏洩してしまったという事例のほうが多い。サーバーは人ではなくパスワードで認証するため、パスワードが漏洩すると、その人になりすましてどのような操作でもできてしまう。

たとえば、FTPやメールの受信、telnetでのログオンにはパスワードが必要だ。しかし、これらは暗号化されていない通信のため、使用中に盗聴されるとパスワードが漏洩する危険がある。よって、FTPを使わずにSSLとHTTP拡張プロトコルのWebDAVを組み合わせて使う、メールの受信にはAPOPを使う、telnetの代わりにSSHを使うなど暗号化通信が不可欠だ。

またパスワードの漏洩だけでなく、内容(データ)の盗聴に関しても考える必要がある。たとえば入力フォームをSSLで暗号化しているものの、それをメールで担当者に転送するようになっているとメールを盗聴される危険性がある。FTPも暗号化されないので、ファイルをFTPでアップロードやダウンロードするのも厳禁だ。

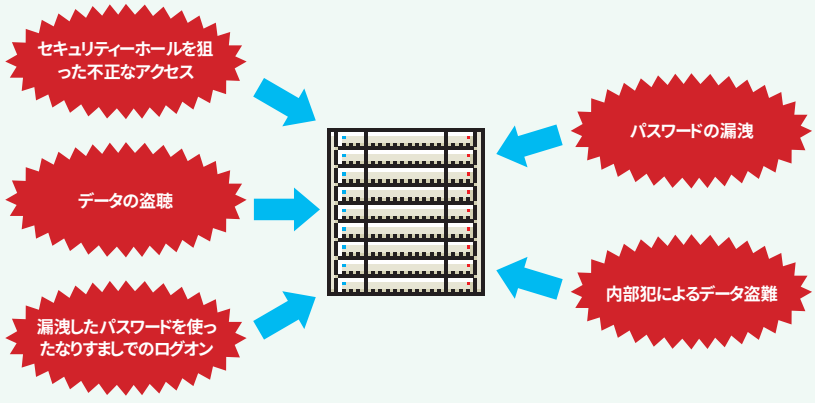
ユーザーごとにアカウントを分けてアクセスログを記録する

パスワードが万一漏洩したときの対策として有効なのが、アクセス元ホストの限定だ。たとえば、ウェブサイトでは.htaccessを使ってアクセス元のホストを制限できる。またいくつかのレンタルサーバーでは管理画面へのログオンを特定のホスト(IPアドレス)だけに制限できる機能を提供するものもある。自社の回線からしかアクセスできないようにしておけばパスワードが漏洩しても安心だ。

しかし、外部から盗聴によってパスワードが漏洩するのではなく、内部の人間からパスワードが漏洩することもある。悪意のある社員がパスワードを漏洩させたりデータを盗み出したりするだけでなく、外部の誘惑などいわゆるソーシャルクラックで、パスワードを口にしてしまう恐れもある。

このような内部からのパスワード漏洩を防ぐ手段は、ユーザーごとにアカウントを作り、最小限のアクセス・設定権限しか与えないようにすることだ。誰がどのファイルにアクセスしたのかはログに記録されるので、個々のユーザーでアカウントを使い分ければ誰がいつどのファイルを参照したのかがわかり、どこから流出したかを知る手がかりになる。

■サーバーを取り巻くセキュリティー関連の危険活動



■不正アクセスへの対処法

不正アクセスの要因	発生理由	対策
セキュリティーホールを悪用したサーバーへの侵入	サーバーOSやアプリケーションのセキュリティーホールを塞がなかったため	・サーバーやアプリケーションの管理を徹底する ・IDSを使い外部からの攻撃を検知する
通信行程での盗聴	メール、FTP、telnetなど暗号化されていない通信を使ったため	・サーバーのファイルを参照したり管理したりするときには、必ず暗号化された通信を使う
パスワードの漏洩	(1)通信行程上でパスワードが漏洩したため (2)社内の誰かがパスワードを流出したため	・通信を暗号化する ・ユーザーごとにアカウントを分けて流出元を明らかにする ・何ごとがあってもパスワードを口にしないように運用を徹底する ・サーバーの管理を行えるアカウントは特に厳格にし、不必要な人にそのパスワードを教えない ・定期的にパスワードを変更する ・万一パスワードが漏洩したときのために、アクセス元ホストを制限しておく
CGIのミスによる、本来は閲覧できてはいけないファイルの閲覧許可	CGIのプログラムや運用上のミス	・CGIプログラムのセキュリティーを見直す ・クロスサイトスクリプティングなどを防止するため、ユーザーが入力したデータは必ず書式チェックするようにする ・CGIが読み書きするファイルやディレクトリーのアクセス権限を念入りに設定する ・CGIが読み書きするファイルはウェブサイトから参照できないところに配置する
アクセスログの流出	ファイルやディレクトリーのアクセス権限の設定ミス	・ログファイルはウェブサイトから参照できないようにアクセス権限を設定する ・ログ管理機能や集計機能のCGIプログラムを使っているのであれば、それらのCGIにパスワードをかけたりアクセス元ホストを制限したりするなどして特定の人しか参照できないようにする

危険を回避する
レンタルサーバー10の機能＆サービス

レンタルサーバー業者は、それぞれが特色ある機能を提供している。ここではサーバーの機能やサービスのうち、特にセキュリティーを高めるのに有用なものを紹介する。今後、サーバーを選定する際にはぜひ参考にしてほしい。

暗号化通信でのサーバー管理

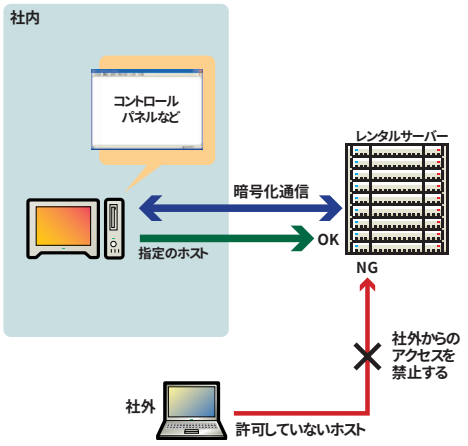
共用 専用

レンタルサーバーの設定変更は、通常、コントロールパネルと呼ばれるウェブページから行う。コントロールパネルが暗号化されていないと、パスワードが盗聴され、誰でもサーバーの設定変更ができてしまうので極めて危険だ。

さらに安全性を高める機能として、IPアドレスフィルタリングなど、コントロールパネルへのログオンを特定のホストからでしか許可しない機能を備えているものもある。社内からしかログオンできないようにすれば、インターネット経由で不正な第三者によってサーバーの設定を変更されてしまう心配がない。

またコンテンツのアップロードにはFTPを使うことも多いが、パスワードの漏洩やデータ転送時の盗聴を考えると、この部分も暗号化されていると安心だ。レンタルサーバーの中には、暗号化したFTPである「SFTP」を提供したり、前述のようにSSLで暗号化されたコントロールパネルを使ってファイルのアップロードやダウンロードができたり、そしてSSL＋WebDAVのファイル共有がサポートされていたりするものもあるので、盗聴を防止するためにそれらの機能を用意するレンタルサーバーを使うとよい。

またメールも暗号化されていないので、最低限パスワードを暗号化するAPOPに対応しているサーバーを選ぶべきだろう。



複数アカウントの対応

共用 専用

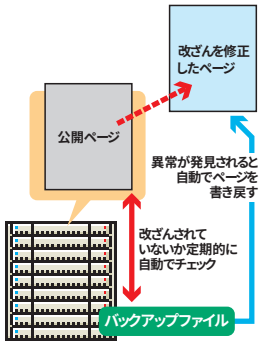
1つのアカウントを数人で共有して使うとセキュリティーに対する意識が低くなる。パスワードの漏洩を最小限に抑えるためには、複数アカウントの対応は必須だ。複数アカウントの対応状況は、「メールだけ」「メールとFTPだけ」「管理者権限の有無まで」などレンタルサーバーによって差がある。管理者が複数いるならば、管理者権限においても複数アカウントを設定できるものを選ぶとよい。

自動監視と改ざん防止（24時間365日対応）

共用 専用

レンタルサーバーは管理体制が行き届いているものを選びたい。24時間の電話対応だけでなく、障害を24時間監視し、即座に復旧対応するところがよい。多くの事業者は障害の発生や復旧の履歴をウェブサイトで公開している。管理体制は見えにくいものだが、それらを参照すれば目安がわかるだろう。

また、ディレクトリーを監視して、不正なファイルの書き換えを発見するとバックアップされているファイルから自動的に内容を書き戻す「改ざん防止機能」を備えるレンタルサーバーもある。この機能があれば、セキュリティーホールやCGIプログラムの不具合などを利用されてファイルが書き換えられても安心だ。



CGIプログラムのセキュリティー対応

共用

CGIはサーバー上でプログラムを動かすものなので、セキュリティー上の問題がよく発生しがちだ。そこで多くの共用サーバーではsuExecなどでCGIをサーバーの所有者権限でしか動作しないように制限し、サーバーの破壊行為や他のユーザーのファイルを読み書きできないように保護している。

また、さらに安全性を高めるため、CGIを設置するサーバーとコンテンツを設置するサーバーとを分けて構成しているレンタルサーバーもある。分離して構成されていると、万一CGIが不具合を起こしてもコンテンツの書き換えが起こらないので安心だ。

CGIを使わないなら、あえてCGIを許可しないサーバーを使うという手もある。そうすれば共用サーバーでも、他のユーザーが作成したCGIのセキュリティーホールの巻き添えを食う恐れがない。

セキュリティーホールへの対応やアドバイス

専用

ユーザーにroot権限を渡す専用サーバーの場合には、自社で責任を持ってセキュリティーホールに対応するのが基本だ。

しかし専用サーバーであっても、セキュリティーホールが発見されたときに、それをレンタルサーバー業者側で修復してくれるサービスもある。ただし、セキュリティーホールを正す際には、サーバーを再起動する必要があったり、サーバー上で一部のアプリケーションが動作しなくなったりする危険性もあるので、すべてを任せっきりにはできない。そこでレンタルサーバー業者からセキュリティーホールを正すためのアドバイスを受けて自社で直すという選択肢もあるのが一般的だ。

社内にサーバーに詳しい人材がいない場合には、ある程度の管理を担い、運用面の相談を受けてくれる事業者を選ぶのが賢明だ。

ファイアーウォールとIDS機能

共用 専用

共用サーバーの多くは、明示されていなくても、ファイアーウォールまたはIDS（不正侵入検知）の設備の下に配置されていて、何らかの保護を受けているのが一般的だ。しかしごく一部のレンタルサーバーでは、セキュリティー対策がとられていないこともある。

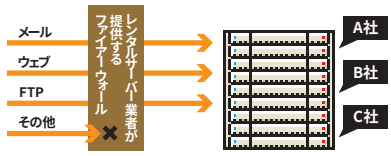
共用サーバーでは、基本的にメールやウェブ機能だけが使えればよいというスタンスなので、通常はメールやウェブに利用するポートしか開けていないはずだ。もし共用サーバーをすでに契約しているのであれば、使用中の共用サーバーに対してポートスキャンをかけてみれば、どの程度保護されているのかがわかるはずだ（契約前にレンタルサーバーにポートスキャンをかけると攻撃とみなされるので避けること）。

ただしシェルを利用できるサーバーでは、同じサーバーを利用する他のユーザーが、メールとウェブ以外のアプリケーションを実行し、インターネットからの通信をすべて受け付けるようにしていることも考えられる。このように、インターネットからの通信を受け付けるアプリケーションを利用しているユーザーがいると、サーバー全体のセキュリティーが弱まる。

専用サーバーの場合には、各社が自由にサーバーを構成することになるので、レンタルサーバー業者がファイアーウォールを共通で設けていないことが多い。よって専用サーバーに自社でファイアーウォールを構成することになる。

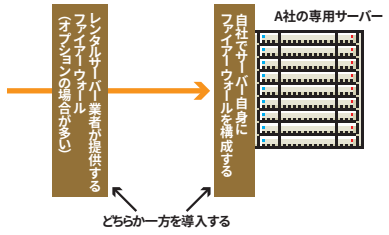
しかし一部のレンタルサーバーでは、オプションとして汎用的なファイアーウォールやIDS機能を適用したり、自社専用のファイアーウォールを構成してくれたりするサービスもある。専用サーバーのセキュリティーを高めたい場合には、それらのオプションを活用するとよい。

■共用型のレンタルサーバーの場合



メール、ウェブ、FTPなど、共用サーバーが提供するサービスだけ通すファイアーウォールが構成されるのが一般的

■専用型のレンタルサーバーの場合



デフォルトではファイアーウォールは用意されない

バックアップ機能と保管体制

共用 専用

レンタルサーバーの中には、万が一サーバーが壊れたときに備え、バックアップだけでなくRAID構成（複数のハードディスク領域を1台のハードディスクにまとめて構成）でミラーリングし、ハードディスクが故障してもサーバーを止めず、そのまま継続して運営できるようにしているものも多い。また地震などの天災に備え、日本と海外など異なる拠点でバックアップ設備を用意するサービスもある。バックアップは、「データの複製」であるため、バックアップから個人情報が流出する懸念もある。すなわち、バックアップしたデータの保全管理も重要だ。

流出が許されない重要な情報を扱うときには、レンタルサーバー業者によってバックアップデータがどのように保管されているのか、どのような人物が触れることができるのか、そして、どの程度の期間でどのように破棄されるのかなども調べる必要があるだろう。

サーバールームの立地条件と入退室管理

共用 専用

レンタルサーバーに物理的に近づいて直接サーバーを操作すれば、レンタルサーバー内のデータを根こそぎ持って行くことができる。よって、レンタルサーバーのサーバールームの入退室管理は厳しければ厳しいほどよい。このため、レンタルサーバーのユーザーであっても入室を禁止したり、サーバールームの所在地すら明らかにしていなかったりすることが多い。所在地を明らかにしないのはセキュリティー面で優れるが、サーバールームの環境が整備されているかどうかの情報は必要だ。

ちなみにレンタルサーバーの管理は、レンタルサーバー業者が行うことになるので、事業者はレンタルサーバー内のデータを参照できる。つまり信用できる事業者でなければならない。前述したように、信頼できるかどうかの目安として、プライバシーマークを取得しているかどうかなどを参考にするといいだろう（105ページ参照）。

サーバーウイルススキャン機能

共用 専用

レンタルサーバーにウェブサーバーだけでなくメールサーバーも任せるならば、ウイルススキャン機能があると安心だ。ウイルススキャン機能は、プロバイダーのメールサービスでは提供されていることが多いが、近年になって、レンタルサーバーでも対応してきている。

ウイルススキャン機能がレンタルサーバー側にあれば、最新のウイルス定義のパターンファイルもレンタルサーバー業者によって適用されるので、管理の手間も省ける。また、受信にかぎらず、送信メールも保護されるため、ウイルス付きメールの送信を事前に防ぐ効果もある。

シェル／telnetの不許可

共用

自由度を高めるため、シェルアカウントをユーザーに与えているレンタルサーバーもある。telnetでログインでき、コマンドラインからサーバーを操作できて便利だ。

しかしtelnetは暗号化されていないので、代わりに、暗号化されたSSH（Secure SHell）を使うようにしよう。

とはいえ、telnetが本当に必要かどうかは疑問だ。特に共用サーバーの場合には、シェルによって他のユーザーに不正に操作されてしまう可能性もある。telnetを必要としないならば、telnetをサポートしないレンタルサーバーを選んだほうがセキュリティー的には優れる。

■書籍紹介

本記事では、個人情報保護法について、要点をまとめて紹介したが、より詳しく知りたい情報システム担当者や企業の管理部門の担当者には、インプレス発行の『個人情報保護法対策 セキュリティ実践マニュアル』がおすすめだ。プライバシーポリシーの文例や保護法対策のチェックリストなども掲載している。

『個人情報保護法対策
セキュリティ実践マニュアル』

著者：特定非営利活動法人日本ネットワークセキュリティ協会（NPO JNSA）、個人情報保護ガイドライン作成ワーキンググループ
価格：3,675円（税込み）
ISBNコード：
4-8443-1858-6
サイズ・判型：B5正寸
ページ数：224P
URL http://internet.impress.co.jp/books/

PR

事故に遭ってからでは遅い

セキュリティー対策を積極的に提案するレンタルサーバーガイド

一般的にレンタルサーバーが用意するセキュリティー対策の機能は、オプションとして提供されていることが多い。そうすると、せっかく安価に提供しているレンタルサーバーも、追加料金が発生すると一見割高に見えてしまう。結果、企業は、毎月かかるコストと機能を天秤にかけた場合、オプションならばすぐには必要ないだろうと判断しかねない。

レンタルサーバー業者に話を聞いたところ、企業であってもセキュリティー対策の重要性に対する意識がまだまだ低く、レンタルサーバーのスペックや動作するアプリケーション、ソフト周りにばかり目が行きがちだという。そして、セキュリティー対策はこの次になってしまう。

とはいえ、ここ最近はウイルスの流行や不正アクセスによる被害がニュースで頻繁に取り上げられるようになり、若干意識が向上している。このような被害に遭った経験のある企業なら、レンタルサーバーを選ぶ際にもセキュリティー対策や運営体制が選択基準の筆頭に挙がるが、経験がないとそうもいかない。しかし、セキュリティー対策は被害に遭ってから導入したのではまったくもって遅いのだ。被害に遭うことで社会的な評価が下がる可能性も大きく、損害も計り知れない。

セキュリティー対策は、できるかぎり導入すべきだ。レンタルサーバー業者にまずは相談し、適切に構成することで、自ら利用するサーバーを危険から守ろう。

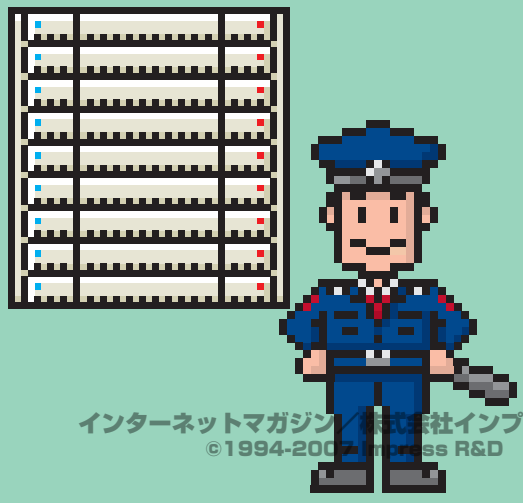
セキュリティー対策機能

- サーバーウイルスチェック
- サーバーOS／アプリケーションソフトのアップデート
- ファイル改ざん対応
- ファイアーウォール
- 不正侵入検知（IDS）
- アクセスログ記録
- アクセス制限
- SSL証明書発行サービス
- サーバールーム入退室管理

安心を提供するサービス

- 24時間365日監視
- RAID、二重化
- 自動バックアップ
- データ復旧

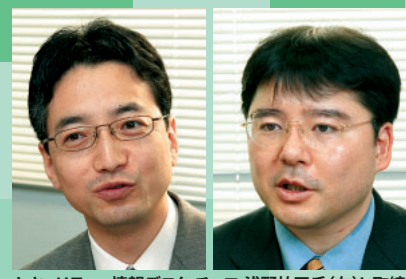
■協賛企業
- AT-LINK専用サーバ・サービス
- シーサイドネット
- ドリーム・トレイン・インターネット（DTI）



PR

多彩なメニューでセキュリティーレベルが細かく設定できる

AT-LINK専用サーバ・サービス



セキュリティー情報デスク チーフ 浅野祐司氏(左)と取締役営業本部長 永井浩和氏

“OSを最新の状態に保つことがセキュリティー対策の根幹”という考え方で、Red Hat 7.3/8.0/9.0の無償サポートを継続して行うAT-LINK専用サーバ・サービス(at+link)。それに加えてファイアーウォールほか多彩な対策メニューも用意された同サービスのセキュリティー事情に迫る。

2006年末までRed Hatのセキュリティーパッチを無償で提供

AT-LINK専用サーバ・サービスは、その名が示すとおり専用レンタルサーバーに特化したサービスだ。提供開始から7年半、この事業での経験が深いだけに、セキュリティー関連サービスの提供に対する考え方にも特徴と真摯な姿勢が伺える。

同サービスの技術責任者である株式会社エーティー・ワークス 取締役営業本部長の永井浩和氏は「弊社のユーザーは、Red Hatの無償サポートが継続して受けられる。実はこれがセキュリティー的に最大の強み」と胸を張る。理由はこうだ。Red Hat 7.3/8.0/9.0に関するパッチ提供は昨年末から今年4月末にかけて打ち切られ、テンアートニ社が年額6万円の有償サービスとして引き継いでいるが、at+linkは同社との一括契約に基づいて、2006年末までユーザーへの無償サポートを継続する。このためセキュリティーホールが見つかってもユーザーは無償でパッチ当てサービスが受けられる。つまり、サーバーOSの環境は常に最新の状態を保ち、必然的に高度なセキュリティーが維持できるという考え方だ。営業窓口であるリンク「セキュリティー情報デスク」チーフの浅野祐司氏も「さまざまなセキュリティー対策を講じることも大切だが、サーバーのセキュリティーホールをなくすことが先決」と付け加える。5月にはRed Hatのパッチモジュールの最新版が自動アップデートできる仕組みもリリースするという。

運営形態により最適なものが選べるセキュリティーメニューの数々

at+linkのサーバーメニューは、あらゆる要求に応えるべく多様なサービスで彩られており、そうした特徴はセキュリティー関連のメニューにも受け継がれる。

まず、サーバーへのアクセス手段を規定した「セキュリティーレベル」では、標準で提供される「TCP Wrapper」によるアクセス制御から最高レベルの「専用ファイアーウォール」まで運用形態により4段階の対策を選べる。また、すべての送受信メールにウイルスチェックを実施する「ウイルスチェッカー」も提供され、共用ゲートウェイを使うものから専用のものまで、ユーザーのメールアカウント数などに応じて複数のコースがある。このほかにも「ファイル改ざん通知サービス」「不正侵入検知サービス」など、さまざまなセキュリティー対策用のメニューが用意されている。

セキュリティーとは異なるが、「安心」のサーバー環境にも触れておきたい。最近、人為的要因による個人情報流出事件のニュースを耳にするが、「サーバーはすべてケーブル＆ワイヤレスIDCの専用フロアに設置されており、厳格な入出管理が行われているため、当サービス以外の人間がサーバーを操作することはありえない」(永井氏)と語る。また、「サービスの開始から7年、情報流出事故は一件も起きていない。多発する事故を契機に制度の強化も行っている」(浅野氏)とも。その言葉の節々からは、専用サーバーサービスで業界をリードする自信が垣間見える。

AT-LINK専用サーバ・サービスのセキュリティー対策

AT-LINK専用サーバ・サービスには、ユーザーのコスト、ニーズ、技術レベルなどに応じ、以下のような複数のセキュリティー対策メニュー(オプション)が用意されている。あまりにも多彩で選択肢が多いため、契約時に何を申し込み、導入すべきか迷うほどだ。だが、セキュリティー対策とコストの両方をバランスよく調和した「オススメ」メニューもあるので、契約時に迷うようであれば、これを参考にするといいだろう。

Red Hat無償サポート	Red Hat 7.3/8.0/9.0においてセキュリティーホールが見つかった場合は、同サービスのユーザーは無償でパッチ当てサービスを受けられる(2006年末まで)。
セキュリティーレベル	「TCP Wrapper」から「専用ファイアーウォール」まで、ユーザーは運用形態、技術スキル、コストなどを見ながら4段階のアクセス制御レベルを選ぶことができる。TCP Wrapperによるアクセス制御は無償。
ウイルスチェッカー	共用ゲートウェイを使うものから専用のものまで、ユーザーのメールアカウント数やコストなどに応じて複数のコースが用意されている。アカウント無制限のアプライアンス提供も開始した。
ファイル改ざん通知	「Tripwire」を導入し、コンテンツの改ざんが行われた場合にメールで通知するサービス。コンテンツの自動復元機能もある。
不正侵入検知	サーバーに到達するパケットを監視するサービス。あらかじめ登録されている侵入パターンに基づいて不正パケットを検知した場合にアラートメールが送信される。

PR

http://www.cssv.jp

SSL証明書や不正検知機能を標準搭載した共用型サーバー

C'S SERVER Professional

株式会社シーサイドネット
代表取締役 小尾英樹氏

シーサイドネットとセコムトラストネットの業務提携で実現した高セキュリティーレンタルサーバー「C'S SERVER Professional」は、SSL証明書（セコムパスポート for Web）やセキュリティー診断、不正侵入検知、ウイルス検知機能などを標準搭載した、セキュリティーを重視するサイト運営にジャストフィットするサービスだ。

SSL証明書を標準で搭載して高いセキュリティーを確保

シーサイドネットが4月から新設した事業者向けのレンタルサーバーメニュー「C'S SERVER Professional」では、セコムトラストネットが提供するSSL認証サービス「セコムパスポート for Web」が標準で提供されている。これにより、ユーザー企業は、高額な費用や手間をかけることなく、SSL暗号化通信を使って自社サイトを運営できる。また、セコムトラストネットが発行するSSL証明書の搭載およびウェブサイトの実在証明を表現するWebステッカーをサイトに貼り付けられるため、自社サイトへの訪問者に“ セキュリティーに気を遣っている企業 ”というイメージをアピールできる。

このようにSSL証明書を標準提供としたわけを、株式会社シーサイドネット 代表取締役の小尾英樹氏は「これからは企業の大小にかかわらずインターネットに情報を出す場合、セキュリティーを意識せずにはいられない。特に個人情報を扱うなら、SSL証明書は企業にとって必要最低限の備えだ」と語る。

これまでもシーサイドネットは、Cside2NDという独自ドメイン型のレンタルサーバーメニューでSSL証明書には対応していたが、ユーザーが別途証明書を取得する必要があり、コスト面を考えると「決しておすすめできるものではなかった」（同氏）という。だが、今回のC'S SERVER Professionalによって中小企業には敷居の高かったSSL証明書がぐんと身近なものになったと言える。また、このサービスでは「不正侵入検知サービス」「セキュリティー診断サービス」「ウイルス検知機能」も月額8,800円の料金内で提供される。セキュリティー重視のサイトをリーズナブルに構築したい企業にはうってつけのメニューだろう。

ただし、従来の個人向けサービスC'S SERVER Personal（Cside2ND改め）においても「第三者の監視こそ入らないが、Professional版と同等のセキュリティーレベルは維持している」（同氏）。ただ「SSL証明書抜きで、個人情報を扱うのはおすすめできない」と付け加える。

厳格な情報管理体制を導入するため今夏にオフィスを移転

シーサイドネットはこの夏、東京池袋にある高層ビルのサンシャイン60にオフィスを移す予定だ。小尾氏はその理由を「最近ニュースで個人情報の持ち出しという人為的なセキュリティーホールが話題になっているが、同ビル内のサーバールームまで構内LANを使って弊社のLANを結び、生体認証による入退室管理システムを導入するなど、厳格な情報管理体制を構築するため」と説明する。また、それにより個人情報の取り扱いを適切に行っている民間事業者に対して認定される「プライバシーマーク」を取得する予定でもある。

このようにシーサイドネットでは、ネット上のセキュリティー機能を提供するだけでなく、同社自身の情報管理・運営面を強化することで、ユーザーに安心のサービスを提供していく。

C'S SERVER Professionalのサービス概要

「セコムパスポート for Web」によるSSL認証サービスを標準装備した事業者向けの独自ドメイン型レンタルサーバー。これにより低コストでセキュアーなサイトを構築できる。また、レンタルサーバーでメールを利用する場合、通常は“ ハガキ ”程度のセキュリティーレベルでしか提供されていない。しかしC'S SERVER Professionalでは、メールの送受信を暗号化するため、この問題を解消。社内メールの安全が確保される。

初期費用	12,000円
月額利用料金	6か月契約8,800円／12か月契約8,000円
ウェブスペースのディスク容量	1GB
メール容量	500MB
メールアドレス	100個
転送量	3GB／日
ウェブサーバー定員	40契約／サーバー
SSL証明書	標準添付（セコムパスポート for Web）
主な機能	サブドメイン4個まで設定可能、PHP/Perl対応、アクセス解析、アクセス制限、アクセスカウンター、アクセスログ（生ログ）、ウェブメール、メーリングリスト、メールマガジン、メール転送（転送機能）、メールセキュリティー対策

問い合わせ先
株式会社シーサイドネット
TEL 03-5960-2282
info@cssv.jp

PR

標準でファイアーウォールとIPフィルタリングサービスを提供

DTI-Magic 1U Server

株式会社ドリーム・トレイン・インターネット セールス本部 ビジネスセールスグループマネージャ 小山幸春氏(左)と同 エキスパート 藤巻弘章氏

DTI-Magic 1U Serverは、標準でファイアーウォールとIPフィルタリングサービスが提供される信頼性重視の専用サーバーサービスだ。2種類の管理者権限を用意しており、あらゆるアプリケーションを取り込んでヘビーに使いたい企業だけでなく、ウェブサイトやメールだけで十分な企業にも最適な環境を提供する。

IPフィルタリングと暗号化で堅固な運用体制を実現

DTI-Magic 1U Serverは、1Uラックマウント型のハードウェアを使用したドリーム・トレイン・インターネット(DTI)が提供する専用サーバーサービスだ。サーバーはIX(Internet eXchange)と同一のデータセンター内に設置することで14Gbps超のバックボーンに直結している。帯域は最低でも2Mbps(最大10Mbps)を確保し、転送量は無制限で利用できるといった安定と信頼の環境を用意する。

セキュリティー機能を随時拡張しており、現在は標準でファイアーウォールを提供している。このほか、上流でIPアドレスによるフィルタリングを行い、SSHやSSLによる通信の暗号化と組み合わせることで、堅固な運用体制を実現できる。ウイルス対策はメールアカウントのライセンス数に応じてオプションで対応している。

近年、専用サーバーサービスでは、サーバーの管理者権限(root権限)をユーザーに与えるところが増えている。DTI-Magic 1U Serverでは、root権限を与えるコースのほか、root権限をDTIが預かり、セキュリティーパッチの適用や標準ソフトウェアのインストールをDTIが代行する準root権限コースも用意する。準root権限は、ウェブサイトやメール、メーリングリストといった標準的な機能だけで十分なユーザーに適した管理者権限で、root権限のようにユーザー側でアプリケーションを自由にインストールできるわけではないため、システム破壊を含む管理リスクを軽減できるメリットもある。

要望に合わせて短期間に対応できる専用サーバーならではの柔軟さが鍵

DTI-Magic 1U Serverのセキュリティー面のメリットについて、株式会社ドリーム・トレイン・インターネット セールス本部 ビジネスセールスグループ エキスパートの藤巻弘章氏は「専用サーバーならではの自由度の高さでセキュリティーを追求していけること」を挙げる。

専用型サーバーを自社で構築するためには、導入までにある程度の検証期間が必要になる。DTI-Magic 1U Serverにはそうした制約がなく、ユーザーの要望に合わせて比較的短い期間で導入できる。このため、ファイル改ざん対策などの、なかにはオプションでも対応していない機能まで、ユーザーの裁量で対応が可能になる。特に商用サイトを運営するような企業にとって、すぐに対応してほしい状況が生じた場合を考えても、この自由度の高さは重要なポイントだ。

同グループ マネージャの小山幸春氏が指摘するように「プロバイダー、ユーザー、サイトの運営を行うSI(システムインテグレーター)の間で役割分担が明確にならない部分が増えてきている」こともあり、柔軟に対応できるサーバー環境が望まれている。DTIとしては「標準化できるものは順次サービスに追加するなど、プロバイダーの立場でできることについてはそのつど対応していく」(小山氏)とのことだ。

DTI-Magic 1U Serverのサービス概要

DTIでは、以前より「Magic 1U Server RaQ4/RaQ550」の名前でサン・マイクロシステムズ(Sun)のCobalt RaQ4/RaQ550を使ったサービスを提供してきたが、SunによるCobaltの提供終了に合わせて、新規ハードウェアを導入。同時に、ポートフィルタリングサービスと24時間365日体制のサポート対応を開始する。コントロールパネルはHDE Controller 3.0を採用し、IPアドレス数に応じて2種類のプランが用意される。

プラン名	Magic 1U Server ES3.0/32	Magic 1U Server ES3.0/29
初期費用	105,000円	
IPアドレス取得代行費用(初回のみ)	なし	10,500円
月額費用	73,290円	78,540円
通信帯域	最大10Mbps(2Mbpsを確保)	
CPU	Intel Pentium4 2.4GHz	
メモリー	512MB	
ハードディスク容量	80GB×2(RAID1)	
OS	Red Hat Enterprise Linux ES3.0	
管理ツール	HDE Controller 3.0 ISP Edition	
IPアドレス名義	DTI	ユーザー
IPアドレス数	1個(最大2個)	5個
ファイアーウォール	標準サービスで提供	
ポート監視	標準サービスで提供	
管理者権限	lcadmin(準root権限)もしくはroot権限	
ソフトウェアアップデートパッチ	lcadmin(準root権限)時のみDTIで対応	

問い合わせ先
株式会社ドリーム・トレイン・インターネット
TEL 03-3505-3647
(月〜金9:00〜18:00・祝祭日除く)
corp@dti.ad.jp

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp