

2005年5月24日

報道関係各位

株式会社ラック

## ラック、「ホームページ情報漏えい診断サービス」に新メニューを緊急リリース ～セキュリティ専門スタッフによる診断サービスを、より安価な価格帯で提供開始～

ネットワークセキュリティ分野でのリーディングカンパニー、株式会社ラック(本社:東京都港区、代表取締役:三輪信雄、以下ラック)は、昨今多発している企業へのホームページを狙った相次ぐ不正アクセス被害を重くみて、この度セキュリティ専門スタッフによる『ホームページ情報漏えい診断サービス』の新メニューを、2005年5月24日より、緊急に提供を開始します。

インターネット環境がビジネス基盤として定着し、ネットショッピング、ネットバンキングだけでなく、ホームページ上でのアンケートやメールマガジンの登録、リクルート問い合わせなどホームページを活用した様々なサービスを展開するビジネスが急拡大しており、ホームページ上で扱われる個人情報も増加の一途を辿っています。一方で、個人情報保護法の施行を受け、個人情報を扱うホームページプログラムの安全性確保について企業の責任はますます大きくなっているにもかかわらず、対策が徹底されていないのが現状です。しかも情報漏えいだけでなく業務停止も企業にとっては大きなリスクとなってきました。

当社コンピュータセキュリティ研究所では、昨年度当社がホームページ情報漏えい診断を行った企業ホームページのうち、成りすましの可能性のある欠陥が67%、情報漏えいの可能性のある欠陥が37%も見つかったという調査結果が出ており、企業、官公庁においては、自サイトの緊急の点検確認と対策の必要性を求めています。

これらの状況を踏まえ、この度、ラックではより幅広いお客様へホームページの安全をご提供するため、従来の診断メニューに加え、緊急的に新たな2つのメニューをリリースします。

本サービスは、実際の攻撃を想定した擬似攻撃を行うことによりホームページの欠陥を検出し、発見された欠陥修復への対策・アドバイスを行うサービスです。一般的に行われているツールによる画一的な診断とは異なり、セキュリティ専門スタッフのハンド・オペレーションによる診断を行うことで、よりきめ細やかな情報漏えい対策を提供することができます。

### ホームページ情報漏えい診断サービスメニュー

ホームページ安全点検パック(新メニュー):39万円:1日間

ホームページに対してスピーディーに網羅的な診断を行い、安全性をチェックします。

ホームページ情報漏えい診断スピードパック(新メニュー):78万円:3日間

オーダー画面やアンケート画面など情報漏えいの恐れのある画面に対して集中的に診断を行い、安全性をチェックします。

ホームページ情報漏えい診断トータルパック:個別お見積り

ホームページ全ての画面に対して、お客様とのヒアリングを交えながら、ご要望に応じた詳細な診断を行い、安全性をチェックします。

### サービス提供開始

2005年5月24日

### 参考資料

別紙添付資料、弊社 CSL(コンピュータセキュリティ研究所)レポート・ダイジェスト資料

詳細は、弊社 HP (<http://www.lac.co.jp>) 掲載の CSL レポート「ホームページからの情報漏洩に対する脅威の現状」～WEB アプリケーションの脆弱性と脅威発生の実態をベースに～を、ご参照ください。

#### 株式会社ラックについて

株式会社ラックは、いち早くネットワーク社会の到来を予測して 1986 年 9 月 3 日に設立されました。ネットワークセキュリティソリューション分野でのリーディングカンパニーとして、「CSL」(コンピュータセキュリティ研究所)にてセキュリティに関する情報を日々、蓄積・分析・検証を行い、JSOC にて顧客システムの 24 時間 365 日のセキュリティ監視・分析を行っています。また、先進のセキュリティテクノロジーを、セキュアネットサービス事業とシステムインテグレーション事業が提供するサービスに付加して、官公庁・企業・団体等の顧客にセキュリティソリューションサービスを提供しています。

#### 本件に関する報道関係お問合せ

株式会社ラック

SNS 営業本部 マーケティング部 大塚 英恵

TEL: 03-5537-2610 FAX: 03 -5537-2619

E-Mail: [mktpr@lac.co.jp](mailto:mktpr@lac.co.jp)

URL: <http://www.lac.co.jp/>

## 参考資料

### 株式会社ラック、CSL(コンピュータセキュリティ研究所)レポート・ダイジェスト資料

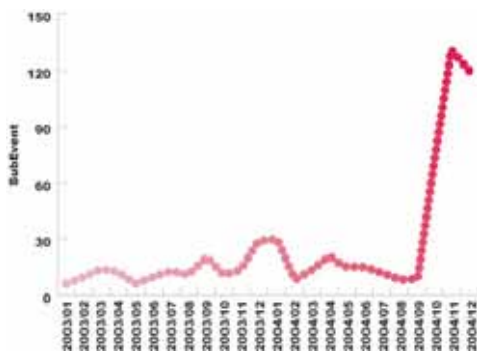
## 「ホームページの7割に欠陥」

### 個人情報入力ホームページで7割の成りすまし、4割で個人情報漏えいの欠陥

ショッピング、資料請求やセミナー申し込みページなどの個人情報を入力するホームページの約7割で他人に成りすますことができ、約4割で個人情報が格納されているデータベースに侵入(データベース侵入)されてしまう欠陥があることが、弊社コンピュータセキュリティ研究所の調べでわかった。

### 欠陥を悪用した個人情報の抜き取りも急増、実害も発生

一方、昨年10月頃からこのデータベース侵入の試みも急増しており、この手法による個人情報漏えい事件も最近になり実際に発生している。同研究所では、昨年10月ごろ中国のホームページにて個人情報を自動的に取得するコンピュータプログラムが公開されたことも、抜き取り急増の原因ではないかと睨んでいる。



[急増しているデータベース侵入の試み]

### 企業の対策は内部の管理強化が優先、ホームページの対策はこれから

4月1日から個人情報保護法が施行になり大手企業などを中心に保護対策は進んでいる。これまでは、個人情報漏えい事件の約80%は内部の関係者によるものと言われており、各企業での対策も書類の管理やパソコンの持ち出しを禁止するなどの、内部の管理強化が主体で、ホームページからの個人情報漏えい対策が徹底されていない実態が、今回の調査で判明したこととなる。

### 大規模な被害発生の危険性も、ホームページ管理者は利用者の保護を優先した対策を！

最近、電子メールを悪用した架空請求詐欺やワンクリック詐欺等の脅迫まがいの行為やフィッシング詐欺と呼ばれる本物そっくりな偽のホームページに誘導してインターネットバンキングのアクセスコードを不正に騙し取ろうとする行為も急増しているが、同研究所は、欠陥の放置が、こういった犯罪をさらに助長させてしまう危険性が高いことを指摘している。今後、国際的犯罪組織やテロリストがこういった手法を悪用し個人情報を大規模に入手、彼らの資金源確保の為に悪用される危険性もあるとして、同研究所は個人情報を取り扱っているホームページの管理者に対して、個人情報の保護だけでなく、利用者の保護も考慮した対策を行うように注意を呼びかけている。銀行キャッシュカードのスキミング問題では当初、被害に関して利用者の責任とされていたが、その後、銀行側で被害補償を含め責任を負うように変わった。今後はインターネットでも利用者の保護対策の実施が求められるようになると思われる。

調査は、同社が2004年に東証一部上場企業などの大手企業約120社に対して実施したホームページ情報漏えい診断結果と約200社へのセキュリティ監視結果ならびに手がけた個人情報漏えい事件の原因調査など元に、同研究所が分析した。