平成 27 年 9 月 15 日

各位

会 社 名　株　式　会　社　ラ　ッ　ク
代表者名　代表取締役社長　髙　梨　輝　彦
（JASDAQ・コード番号：３８５７）
問合せ先　ＩＲ広報部長　岩　﨑　　勝
電　　話　０３－６７５７－０１０７

ラック、日本全国の自治体の標的型攻撃対策を支援するパートナー制度を開始
～標的型攻撃の脅威からマイナンバーを守る自治体を、地域のプロと協力して支援～

株式会社ラック（本社：東京都千代田区、代表取締役社長：髙梨 輝彦、以下ラック）は、日本全国の自治体の標的型攻撃への対策を支援するため、各地域のシステムインテグレーターやデータセンター事業者と協力し、当社が開発したマニュアルとツール「標的型攻撃対策キット」を用いて、自治体の標的型攻撃対策を支援するパートナー制度「ラック標的型攻撃対策　パートナープログラム」を企画し、パートナー企業の募集を開始しました。

背景

2015年６月１日に公表された、日本年金機構に対する標的型攻撃事件に端を発し、その後多くの企業や公共団体における標的型攻撃事件が相次ぎ報道されました。中でも大きな衝撃を与えたのが、2015年６月17日に長野県上田市がホームページで公表した標的型攻撃による事件です。標的型攻撃による被害が確認されたことにより、安全上の理由から行政ネットワークや住基ネットから遮断されるなど、上田市の行政機能に大きな影響を及ぼしたとされています。

2015年10月より、マイナンバー制度の実施によるマイナンバーの交付が行われます。また、2016年１月からは、実際にマイナンバーを活用した行政サービスもスタートします。マイナンバーには、利用、提供、収集の制限など、特定個人情報の適切な取り扱いが求められており、制度に対応する体制構築やシステム改修、マイナンバーを取り扱う運用ルール策定、情報漏えいリスクなどのセキュリティ対策が必須です。マイナンバーの交付主体は自治体であり、マイナンバーデータベースに保存された特定個人情報や符号の保護は、自治体の義務となっています。そして、2017年に予定されている自治体間の情報連携においては、高度技術を用いたネットワーク接続が必要となります。

このように、高度な情報管理を必要としたマイナンバー制度の実施にともない、今なお攻撃が継続されている標的型攻撃の脅威が、自治体における課題となっています。

当社は、情報セキュリティ対策サービスの提供および、事故発生時の緊急対応に関して、日本の代表的な企業であると自負しております。当社には、自治体がいかにして情報セキュリティ対策を推進し、対策が困難な標的型攻撃に立ち向かうべきかの知見を有しています。しかしながら、1741にも及ぶ自治体全てに当社自らがノウハウを提供し、対策を当社だけで支援することは現実的ではありません。

そこで当社は、当社が開発した標的型攻撃に対抗する運用マニュアルや、標的型攻撃メール訓練のツ

ール、組織への教育コンテンツ、被害発生を発見するためのツール群を、全国の自治体をITで支援する地域のシステムインテグレーターやデータセンター事業者へ提供し、全国の自治体のセキュリティレベルを高めるためのパートナー制度「ラック標的型攻撃対策　パートナープログラム」を企画しました。

「ラック標的型攻撃対策　パートナープログラム」

「ラック標的型攻撃対策　パートナープログラム」は、全国の自治体の標的型攻撃対策を支援するため、各地域のシステムインテグレーターやデータセンター事業者に、当社がこれまでに蓄積した標的型攻撃に対する知見と経験を基に開発したドキュメントやツールである「標的型攻撃対策ツールキット」提供し、全国レベルで対策を推進する取り組みです。

本パートナープログラムにおいては、次のドキュメントやツール、技術者教育やサポートを包含した「標的型攻撃対策ツールキット」が提供されます。

「標的型攻撃対策ツールキット」

＜理解と教育＞

１）　標的型攻撃緊急対応マニュアル

２）　基礎教育（基礎的な知識）用教育コンテンツ

＜演習や訓練＞

１）　基礎訓練（標的型攻撃メール訓練）実施用ツール

２）　基礎訓練（セキュリティ基礎理解用ボードゲーム）実施用ツール

３）　自己点検（遠隔操作ウイルス感染などのチェック）実施マニュアルと、技術者向けトレーニング

＜監督・監査＞

重要情報取り扱いチェックシートによる「割れ窓」チェック用マニュアル

＜気づく・見つける＞

１）攻撃被害発生確認（プロキシサーバーログの確認）の実施マニュアル

２）データセンター様向けソリューション（簡易版セキュリティ監視（SecureNet®））導入支援

パートナープログラムへの参加要件

本パートナープログラムは、2015年６月に発生した日本年金機構への標的型攻撃事件により、急激に危機感を増した自治体を支援するために企画されましたが、標的型攻撃の対策は一朝一夕に行うことはできないため、パートナー企業はある程度の技術的な基盤と企業規模が必要となります。

＜技術知識やお客様環境の把握＞

本パートナープログラムは、ITそのものの技術的知識や情報セキュリティへの知見、提案や対策を行うことから自治体のIT環境を把握していることが条件となります。

＜人員体制＞

標的型攻撃の対策は、継続してルールの徹底や状況確認作業を行う必要があり、それを支援するパートナー企業はある程度の人員体制や、事故が発生した際の緊急対応体制が組める規模を持つ企業が望ましいと考えられます。

＜事業やお取引の実績＞

標的型攻撃への対策は、日本政府や監督官庁からの指導により、徐々に一般的になることが予想されますが、全ての自治体が潤沢な予算を投入し、即時に対策を進められるとは限りません。そのため提案を行えるビジネスの下地をお持ちの企業の皆さまにご参加いただきたいと考えています。

本パートナープログラム参加費用

本パートナープログラムへの参加は、有償となります。パートナーは、本パートナープログラムで提供される「標的型攻撃対策ツールキット」を、標的型攻撃の対策支援サービスをお客様に提供する際に利用することができます。

お支払いいただく参加費は、上記の利用を含め、ドキュメントやツールの新規開発や継続的なメンテナンス、事務局運営などに活用いたします。

初年度は１パートナー様あたり100万円～（税抜）とさせていただきます。また、次年度以降は、ドキュメントの増加、提供されるツールの拡大を予定しており、１パートナー様あたり200万円～（税抜）を予定しています。

なお、パートナープログラムで提供される「標的型攻撃対策ツールキット」は、企業や団体からの要望があれば同額にて販売も可能です。また、ツールキットを活用してサービス提供を行う場合には、パートナープログラムへの参加が必須となります。詳細についてのご質問は、お問い合わせ先までご連絡ください。

最新の情報およびお問い合わせ先

ラック　標的型攻撃対策本部
電子メール：antiapt@lac.co.jp

▼ 標的型攻撃対策パートナープログラム
http://www.lac.co.jp/anti-apt/partner.html

以上

【 株式会社ラックについて 】　（http://www.lac.co.jp/）

ラックは、1986年にシステム開発事業で創業、多くの実績を誇る「金融系の基盤システム開発」「マーケティング・オートメーション支援」「ビッグデータ・アナリティクス」を始め、社会の基盤システムの開発を行っています。1995年にはいち早く情報セキュリティ事業を開始し、現在ではサイバーセキュリティ分野のリーディングカンパニーとして、官公庁・企業・団体等のお客様に業界屈指のセキュリティ技術を駆使した、先端のITトータルソリューションサービスを提供しています。2015年には、米フロスト＆サリバンより、「セキュリティ監視」「脆弱性診断」「セキュリティ事故対応」「セキュリティコンサルティング」などが高く評価され、「日本市場マネージドセキュリティーサービス プロバイダー最優秀賞」を受賞しています。

＊ ラック、LACは、株式会社ラックの国内及びその他の国における登録商標または商標です。
＊ その他、記載されている会社名・団体名、製品名などは、各社の登録商標または商標です。

この件に関するお問い合わせ

■ 一般の方は　※記事掲載時のお問合せ先はこちらをご記載ください

株式会社ラック

Tel： 03-6757-0103（営業）　E-mail： sales@lac.co.jp

■ 報道関係の方は

株式会社ラック　IR広報部　広報担当

Tel： 03-6757-0130　　E-mail： pr@lac.co.jp

Twitter：　@lac_security　Facebook：　https://www.facebook.com/Little.eArth.Corp

住　所：　〒102-0093 東京都千代田区平河町2-16-1 平河町森タワー

※ラックのプレスリリース配信をご希望の報道機関の方は、メールにてお問い合わせください。
