

Nikkan Kogyo Shimbun
Ensure Card Security with Global Standards
Utilize the timing of IC device adoption

August 12, 2014, Midori Yuhara

With the expansion of the card users, importance of the card security will increase and the global standard for secure network development and maintenance, and data protection are becoming absolutely necessary. We have conducted an interview with Bob Russo, General Manager at PCI SSC.

- What is the importance for security enhancement?
 - The most important thing is education. To publicize the PCI standards and let people know how they can protect data through them. When we see the case, major breaches are simple to prevent with our standards. Japan is under the process of making credit cards integrated circuit-compatible and it's good timing to also adopt other technologies to enhance security.
- What is the feature of the "version 3"?
 - There are some cases recently that merchants leak data by the fault of their outsourcing company. Given that, the new version clarifies the responsibility of the service providers and other third parties on their keeping and sending data. In addition, it has an expanded flexibility for the merchants to select the way to comply with the standards at their own discretion.
- What do you think about the Benesse case in Japan?
 - It is covered by overseas media. Talking about a merchant, consumers may think it's risky to purchase things if their data is not being protected. The shop should recognize that it is the most important issue to protect the brand. The case may be one of the motivations of how necessary they should enhance security.
- You will hold an international conference "PCI Community Meeting" in 2015 in Japan.
 - This is annual event with approximately 600 people. We introduce global trend, future security standards and others. Then, we let people to know about PCI further deeply, and let them consider how to protect data in an optimal way.

■ Journalist's eye

Mr. Russo appealed about the repeated third-party-related data leak recently as "companies involved may take joint responsibility." In addition, he continued to emphasize the importance of education and showed PCI's focus on enhancing the quality of the education. People may think that information leak can be easily avoided with some technologies, but making steady efforts in terms of people education and technology improvement may be truly required.

カードの安全性 国際標準で担保

カード利用の拡大に伴い、セキュリティの重要性が増し、安全なネットワークの構築と維持、カード会員のデータ保護などを目的とした国際標準が必要不可欠となる。世界40カ国・地域以上で採用されている国際標準を策定するPCIセキュリティ標準協議会(PCI SSC)のジェネラルマネージャーのボブ・ルツン氏に安全性への取り組みについて聞いた。

「セキュリティを高めるために大切なことは、まず啓発活動だ。PCIの基準を周知し、この取り組みによりいかに情報を守れるか広く知らしめることが大切だ。データ侵害の手口をみると、我々の基準でセキュリティ性を担保し、簡

単に防げることがある。また暗号化など、仮に情報が盗まれても使い物にならないようにすれば安心だ。カードのIC化を進める日本は良い時期にいる。加盟店がIC対応端末に変える際に、他の



PCI SSC ジェネラルマネージャー ボブ・ルツン氏

IC 端末導入 機に周知

技術も導入してセキュリティ性を高められる」
「2013年にセキュリティ基準の「バージョン3」を策定した狙いは、

「最近では委託先など第三者が原因で、加盟店から情報漏えいすることが多い。そこで第三者や会員データの保管や送信を

「海外メディアも取り上げている。もし店舗ならば、消費者は自分の情報が守られている保証がなく、その店で買うのは危険だと考える。最も大切なブランドに関わる問題と認識すべきだ。今回の事件によって、いかにセキュリティ性を向上させないといけないか、

「海外メディアも取り上げている。もし店舗ならば、消費者は自分の情報が守られている保証がなく、その店で買うのは危険だと考える。最も大切なブランドに関わる問題と認識すべきだ。今回の事件によって、いかにセキュリティ性を向上させないといけないか、

「毎年開催し、約600人が集まる。国際的な動きや今後のセキュリティ基準の方向性などを説明する。そしてPCIをより深く理解し、どうすれば最適に情報を守れるか考えてもらう」

金
融

情報漏洩対策 まず教育から

「まず啓発活動だ。PCIの基準を周知し、この取り組みによりいかに情報を守れるか広く知らしめることが大切だ。データ侵害の手口をみると、我々の基準でセキュリティ性を担保し、簡

「最近では第三者の関与によるデータ侵害が多くなると考え、ルツン氏は「関係各社の連携責任として追求していかないと」

記者の目

「最近では第三者の関与によるデータ侵害が多くなると考え、ルツン氏は「関係各社の連携責任として追求していかないと」

ITpro by Nikkei Computer

[Data Utilization Case Study in Overseas]

What are the card industry-recommended security measures “to avoid second Benesse case”

<http://itpro.nikkeibp.co.jp/atcl/column/14/080600034/080700005/?ST=security&P=1>

August 21, 2014, Naoki Asakawa

Enterprises can utilize personal data thanks to the reliable security. However, the confidence for the security is shaken by continuous data leaks including Benesse case.

The latest version of PCI DSS shows specific measures to prevent leaks such as “refocused requirement on assignment of access based on individual’s job classification and function.” Bob Russo, Troy Leach and Ella Nevill talked about the successful data security measures.

- Internal engineer was the criminal of the Benesse’s case. What kind of measures does the card industry have to avoid leaks by employees?
 - The new PCI DSS Ver3.0 adds some clarifications considering the internal threats. There are two things that are inevitable toward internal threats. First one is access authority abridgment and the second one is log data monitoring. Adding firewall and other prevention systems to them and make the measure multiple may be important for data security.
- How to judge the return on investment of the security measures including PCI DSS?
 - The biggest incentive for the enterprises may be “not to be a second Benesse.”
- What do you think about the several new card payment technologies such as Square?
 - New payment technologies focus on convenience, and there are some cases that security receives a low priority. We would recommend to adopt security requirements of the PCI DSS such as tokenization at the system design phase.

Tsuhun Shimbun
PCI SSC General Manager Bob Russo
Launched “PCI DSS” / Understanding of the standard is steadily growing
 August 14, 2014, Tomoyuki Kawanishi

Summary

He is a general manager of PCI SSC, which standardizes the security of credit card. One of his objectives to visit Japan was to confirm the progress of the PCI DSS adoption in Japan. Another one is to invite people to the community meeting, which is scheduled to be held in Japan in 2015. Meeting will be held across two days and multiple sessions are planned.

He told that “the understanding of the standard is not enough (in Japan)” when he visited Japan four years ago, but this time “the situation is increasingly shifting to the good direction,” he commented. He also said that the question at the speech is shifting from “why the standard is necessary?” to “how we can meet the standard.”

Recently the number of devices that can use credit card is growing. “It is good for card industry, but hard situation for security,” he said.

PCI SSC has two actions to protect card data. The first one is to limit the number of servers and the second one is tokenisation. The latter one is effective in terms of security and cost. There are so many companies adopting tokenization of card numbers with plenty of solutions.

談話室



PCI SSC
ゼネラルマネージャー
ボブ・ルッソ氏

クレジットカードのセキュリティ基準「PCI DSS」を策定する団体、PCI・セキュリティ・スタンダード・カウンシル（PCI SSC）のゼネラルマネージャーを務める。

今回の来日目的の一つは、PCI DSSの日本における進捗状況の確認。もう一つは2015年に日本での開催を予定するコミュニティミーティングへの参加呼びかけだ。ミーティングは2日間

にわたり、PCI DSS基準の詳細な説明のセッション、不正アクセスや情報漏えい起きた際のデータ分析から防御手段を探る「フォレンジック」に関するセッションなど、多数のセッションを開催する。

4年前に来日した際は「（日本では）基準への理解がまだ進んでいない」と話していた同氏だが、「状況は大きく変化しており、良い方向に進んでいる」。講演で受ける質問も「なぜ基準が必要なのか」という内容から

「基準への理解、順調に進む」「PCI DSS」を策定

「基準を満たすためにどうしたらいいのか」といったものに変わってきているという。近年はスマートフォンやタブレットの普及が進んでおり、クレジットカードが利用できる端末も増えている。「カード業界にとってはいいいことだが、セキュリティの担当者にあっては大変な状況

後者はカード番号の「トークン化」と呼ばれるものだ。これは、カード番号を乱数で生成した別の文字列に置き換えるという技術。実データとの対照が必要となるが、元の文字列とはまったく違うものに置き換わっているため、犯罪者にとっては無意味なデータとなる。さらにはカード番号ではないため、PCI DSSの対象範囲から外れることから、結果的にコスト削減につながるというメリットもある。欧米ではカード番号のトークン化を採用する企業が増えており、そのためのソリューションも多々あるという。