2008 年 5 月 22 日

お客様各位

「Debian GNU/Linux に含まれる OpenSSL/OpenSSH の脆弱性に関する注意喚起」について

拝啓　貴社益々ご清栄のこととお慶び申し上げます。平素は弊社サービスに格別のご高配を賜り、厚く御礼申し上げます。

2008 年 5 月 16 日に JPCERT より行われました
Debian GNU/Linux に含まれる OpenSSL/OpenSSH の脆弱性に関する発表につきまして

<<< JPCERT/CC Alert 2008-05-16 >>>
Debian GNU/Linux に含まれる OpenSSL/OpenSSH の脆弱性に関する注意喚起
OpenSSL packages contain a predictable random number generator
http://www.jpcert.or.jp/at/2008/at080008.txt

その概要及び対応方法を以下に記載いたしますので、お客様の環境をご確認頂きたくよろしくお願いいたします。
尚、弊社システムにおいては該当製品を使用していない事を確認しております。

１．概要

Debian GNU/Linux、Ubuntu などのディストリビューションに含まれる OpenSSL のパッケージには推測可能な乱数を生成する問題があります。
結果として、第三者に暗号化された通信を復号される可能性があります。

２．対象

対象となる製品とバージョンは以下の通りです。

- Debian GNU/Linux 4.0 (etch) 、及び派生バージョン（※）
- Ubuntu 7.04 (Feisty)
- Ubuntu 7.10 (Gutsy)
- Ubuntu 8.04 LTS (Hardy)

※Debian の派生バージョンも対象となる可能性があるため詳しくは配布元にお問い合わせください。

３．対策

該当のディストリビューションを使用して SSH 鍵や SSL 証明書等を作成した場合は OpenSSL

パッケージを最新のバージョンに更新し、SSH 鍵や SSL 証明書等を再作成してください。

1). openssl パッケージを最新に更新してください。
2). 更新した openssl で、鍵ペアの再作成を実施してください。
3). 再作成を行った鍵ペアで、CSR を作成してください。
4). 証明書発行から 30 日以内で再発行前であれば、再発行の手続き (無償) を行ってください。
再発行済または 31 日以上であれば、失効 (無償) と発行の再申請 (有償) を行ってください。

[参考 URL]

http://www.jpcert.or.jp/at/2008/at080008.txt
http://www.debian.org/security/2008/dsa-1571
http://www.ubuntu.com/usn/usn-612-1

今後とも弊社サービスへの変わらぬご愛顧を賜りますよう、重ねてお願い申し上げます。

敬具