

## 「JNSA Press Vol.2」 正誤表

- 1 . 6 ページ 冒頭見出し  
誤：3 . 影響と対策      正：1 . デジタル署名の基本モデル
- 2 . 7 ページ右段 2 - 3 2 行目  
誤： $\mu(M) d$       正： $\mu(M)^d$
- 3 . 8 ページ右段 3 - 2 1 行目  
誤： $\mu(M)=6b\ bb\dots bb\ ba\_Hash(M)\_3x\ cc$   
正： $\mu(M)=6b\ bb\dots bb\ ba\ Hash(M)\ 3x\ cc$
- 4 . 9 ページ左段 3 - 3 9 行目  
誤： $\mu(M)=00\ 01\ ff\dots ff\ 00\_HashAlgID\_Hash(M)$   
正： $\mu(M)=00\ 01\ ff\dots ff\ 00\ HashAlgID\ Hash(M)$
- 5 . 9 ページ左段 3 - 5 1 行目  
誤： $\mu(M)(H\_G(H)\ salt$       正： $\mu(M)\ H\ G(H)\ salt$
- 6 . 9 ページ右段 3 - 6 1 行目  
誤： $\mu(M)= G(H)\ ([00\dots 01\_salt]\_H\_bc$   
正： $\mu(M)= G(H)\ [00\dots 01\ salt]\ H\ bc$
- 7 . 2 8 ページ 社名下 URL  
誤：<http://www.commerce.softbank.co.jp>  
正：<http://www.sb-commerce.co.jp>
- 8 . 2 8 ページ 理事名役職  
誤：戦略本部・技術本部・本部長  
正：執行役員 戦略本部・技術本部・本部長

以上、ご迷惑をおかけいたしました関係者の方々に、深くお詫び申し上げます。

**NPO 日本ネットワークセキュリティ協会**  
〒136 8741 東京都江東区新砂 1 - 6 - 3 5  
Nビル東陽町 (株)ディアイティ内  
【Tel】03-5633-6061 【Fax】03-5633-6062  
【E-mail】[sec@jnsa.org](mailto:sec@jnsa.org)