S1864-10

正　誤　表

下記の部分に誤り，および記述の不足部分がありましたので訂正いたします。
ご迷惑をおかけし大変申し訳ございません。

2005 秋　基本情報技術者 徹底解説本試験問題

<table>
<tr><th>No</th><th>訂正箇所</th><th>誤</th><th>正</th></tr>
<tr><td>1</td><td>H16 秋-126
問 65 の解説
上から 6 行目</td><td>……。(イ)が適切な記述である。</td><td>……。(エ)が適切な記述である。</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">H17 春-127
問 64 の解説</td><td colspan="2">解説に誤りがありました。大変申し訳ございません。次の解説に差替えをお願いします。</td></tr>
<tr><td colspan="2">（正しい解説）
公開かぎ暗号方式は，公開かぎと秘密かぎをペアで使用する暗号方式である。公開かぎで暗号化したものは，公開かぎに対応する秘密かぎでしか復号できず，逆に秘密かぎで暗号化したときには，秘密かぎに対応する公開かぎでしか復号できないという性質を持つ。さらに，秘密かぎを保有していることは，その所有者の身元を保証することになる。したがって，送信者が間違いなく本人であることを受信者が確認できるのは，送信者は自分の秘密かぎで暗号化する必要があるので，(イ)の記述が正しい。
なお，公開かぎ暗号化方式を使って，不特定多数の人から，暗号化メッセージを送信してもらうケースでは，不特定多数の人に事前に公開かぎを配っておく(公開かぎは，そもそも一般に公開するので，インターネットを介して配ることができる)。公開かぎで暗号化したメッセージは，公開かぎに対応する秘密かぎでしか復号できないので，たとえネットワーク上で盗聴されたとしても，秘密かぎがない限り復号できないので，メッセージの機密性が確保できる。</td></tr>
</table>

（株）アイテック　教育開発部