平成 28 年度 技術士第二次試験 模擬答案用紙

受験番号	
問題番号	Ⅱ－２－１

技術部門	情報工学　部門
選択科目	情報システム・データ工学
専門とする事項	

※

○受験番号，問題番号，技術部門，選択科目及び専門とする事項の欄は必ず記入すること。
○解答欄の記入は，１マスにつき１文字とすること。（英数字及び図表を除く。）

（１）仮想通貨を扱う際のリスク

仮想通貨で利用されるブロックチェーンは、データ改ざんに強く、一般的にセキュリティに強い技術である。しかし、仮想通貨を扱う取引所のセキュリティが脆弱である場合、以下のリスクが想定される。

①秘密鍵の漏えい

仮想通貨では、公開鍵と秘密鍵を利用した「公開鍵暗号」の技術が利用されている。一般的に、秘密鍵は、取引所で管理されているが、これらの管理がずさんである場合、秘密鍵がハッキングされ、仮想通貨が不正に送金される等のリスクが想定される。

②内部犯行による不正操作

企業が外部からのセキュリティ対策を行った場合でも、自社の従業員が職務上与えられた権限を使って送金などが行われる場合がある。このような、内部犯行による、不正操作のリスクが想定される。

（２）リスクに対する技術対策

①秘密鍵の漏えい対策

秘密鍵を保管する場合、ウォレットという銀行の預金口座のようなものを利用する。ウォレットには、ホットウォレットとコールドウォレットがある。ホットウォレットは、インターネットに接続された、オンライン上のウォレットで、ハッキングによる盗難の危険性が高いウォレットである。一方、コールドウォレットは、インターネットから隔離されたオフライン上の

●裏面は使用しないで下さい。　●裏面に記載された解答は無効とします。　24 字×25 字

平成 28 年度 技術士第二次試験 模擬答案用紙

受験番号	
問題番号	Ⅱ－２－１

技術部門	部門
選択科目	
専門とする事項	

※

○受験番号，問題番号，技術部門，選択科目及び専門とする事項の欄は必ず記入すること。
○解答欄の記入は，１マスにつき１文字とすること。（英数字及び図表を除く。）

ウォレットで、盗難の危険性の低いウォレットである。当然取引所では、より安全性の高い、コールドウォレットで管理すべきである。

②内部犯行の対策

内部犯行の対策においては、マルチシグを採用する。マルチシグとは、仮想通貨の出金に、複数のシグネチャ（秘密鍵）を必要とする方式で、一般的にセキュリティレベルが高い技術である。マルチシグでは、単独の担当者では、仮想通貨の出金ができないため、内部犯行による不正のリスクが低くなる。

（３）各技術対策における留意点

①コールドウォレットにおける留意点

コールドウォレットを利用する場合は、外部犯行による情報漏えいのリスクは低くなるが、コールドウォレットにアクセスできる担当者は容易に、不正送金が可能である。そのため、コールドウォレットを採用する場合等においても、マルチシグなどの技術を組み合わせて、分散保管することが必要である。

②マルチシグにおける留意点

マルチシグにおいては、同一サーバーにM個の秘密鍵を保管し、サーバーが侵略されれば秘密鍵が全て、盗まれる場合がある。また、適切に分散管理しても、担当者がM個の秘密鍵全てにアクセス可能であれば、対策にならない。そのため、マルチシグを使用した場合でも、適切な運用管理が必要になる。

●裏面は使用しないで下さい。　●裏面に記載された解答は無効とします。　24 字×25 字