

みずほ銀行が、 情報セキュリティプロフェッショナル認定資格 “CISSP”を積極導入

SierやICTソリューションベンダーだけでなく、ユーザー企業においても、積極的に情報セキュリティ資格を所属員に取得させる動きが出てきている。みずほ銀行も、情報セキュリティレベル向上のための重要施策として、取り組みを始めた。



ユーザー企業にも求められる 情報セキュリティ専門家

今日の企業活動において情報セキュリティ対策は必須であり、各企業は経営における情報セキュリティの重要性、社会的要請を認識し、課題解決に向けた努力を日々重ねている。

金融機関も例外ではない。ATMシステムやインターネットバンキングに対する情報セキュリティリスクが

高まる一方の現在、より高度な情報セキュリティ対策を講じていくことが求められている。

このような背景から、みずほ銀行は、銀行の実務に精通する行員に専門知識を身に付けさせることが情報セキュリティレベル向上の鍵だと捉え、情報セキュリティ資格を行員に取得させるという取り組みを始めた。

2006年7月20日付の朝日新聞朝刊記事によれば、情報セキュリティ

などを踏まえ、自らの顧客や業務の特性に応じた必要な検討を行った上で態勢の整備に努めるべきである」としている。さらに、その際に留意すべき点として、「個別の対策を場当たり的に講じるのではなく、セキュリティ全体の向上を目指す」ことを挙げている。

なぜCISSPか？

プロフェッショナル認定資格「CISSP」の取得者を、当面10人をめどに養成するとのことである。

みずほ銀行の取り組みの方向性は、金融機関の監督官庁である金融庁が主催した「情報セキュリティに関する検討会」の検討結果とも合致する。

2006年7月13日に発表された検討結果において金融庁は、「金融機関は、セキュリティ対策を講じるにあたっては、まずは各金融機関がその経営責任において、犯罪の発生状況

情報セキュリティ資格を持つ行員の養成にあたって、数多ある情報セキュリティ関連資格の中から、みずほ銀行がCISSP (Certified Information Systems Security Professional) を選んだ理由はなんだろうか。

「多くの国内外の情報セキュリティ関連資格を調べました。選定の判断基準は、ベンダーフリーであること、包括的であること、ユーザー部門の行員にも有益であること、などでした。

弊行の場合、CISSP取得候補者の行員は、特定の情報システムの管理や運用を担当するだけでなく、銀行業務に相応しい情報セキュリティを実現するために、情報セキュリティ対策全体を、企画・立案・管理・監督する役割を期待されています。ですから、情報セキュリティ全般を

フェーズ	リスク	
	項目	本検討会で検討した主なリスクの例
I 金融機関内のシステム・体制の構築	1 情報セキュリティ問題が重要な問題と位置付けられていないATMシステムのセキュリティ対策の理解・認識が不十分	① ATM周辺のパンフレットを入れる箱などに盗撮カメラ等を設置される
		② 防犯カメラを設置するなどの対応を取らないため、犯行の標的とされる
	2 金融機関内に保管されている口座情報・暗証番号等が流出	① 内部者が口座情報等を故意に流出させる ② 内部者が口座情報等を流出させ、紛失又は窃取される ③ 犯人が利用者を装い、暗証番号を失念したとして金融機関から聴取る
II 口座開設 キャッシュカードの交付	1 類推されやすい暗証番号を顧客が選択	① 顧客が生年月日等を暗証番号に設定する
		② カッシュカードが正当な顧客に交付されない
	2	① 内部者が顧客に無断で違法にキャッシュカードを作成する ② キャッシュカード送付の際、送付物が窃取される
III カード利用時	1 口座番号の漏洩	① ATMコーナーに設置されたゴミ箱から口座番号が記載された利用明細票が窃取される ② キャッシュカード挿入口に隠しカメラが設置され、盗撮される

図1 ATMシステムに対するリスクの例
(金融庁「情報セキュリティに関する検討会」発表資料より抜粋)

網羅した幅広い見識が必要です。

このような観点から検討した結果、CISSPが最も適切な資格であると判断しました。」(みずほ銀行事務統括部 セキュリティ対策室 次長 北山 普弘氏)

CISSPとは？

それでは、みずほ銀行が選択したCISSPとは、どのような資格なのであろうか。みずほ銀行は、CISSPを行員に取得させるにあたって、NTTコミュニケーションズ(NTT Com)に相談した。みずほ銀行は、同社の通信ネットワークを利用しているが、同社が社内にCISSP認定保持者を多数有していることを知り、CISSPの有用性と取得のノウハウを同社の営業担当者を通してヒアリングした。

NTT Comは、情報セキュリティビジネスへの戦略的取り組みとして、専門人材の育成に注力している。IT系資格としては世界で初めてISO17024認証を取得し、全世界で

45,000人以上、日本国内では600人以上(2006年11月現在)の認定保持者がいるCISSPの取得を奨励し、セキュリティを考慮したバランスの良いソリューションをお客様に提供するためのスキルを、社員に修得させている。

CISSPは、現在最も必要とされている情報セキュリティプロフェッショナル認定資格と言われており、そのカバー範囲は幅広く、10のドメインに分類される(図2参照)。

CISSP取得の効果

NTT Comに在籍するCISSP認定保持者の数は、すでに250名を超え、2006年末までには、300名に達するという。

「CISSPの取得を通して、営業、SE、管理職を問わず、それぞれにスキルを高めることができます。現在では、あらゆる通信サービス、ICTソリューションに、情報セキュリティのコンセプトを盛り込むことが必須となっています。このような状況では、職種にか

かわらず、情報セキュリティについての十分な見識を持たなければ、お客様に最適なソリューションを提供することはできません。

CISSP取得奨励でもう一つ成果があったのは、社員に自信がついたことです。各国政府機関をはじめ世界的に認められている資格の



NTTコミュニケーションズ株式会社
プラットフォームサービス部長
CISSP 笠原 久嗣氏

取得は、社員に大きな自信をもたらしています。」(NTTコミュニケーションズ プラットフォームサービス部長 CISSP 笠原 久嗣氏)

CISSPの今後のひろがり

IDCの調査(IDC's Global Information Security Workforce Study, 2005)によると、CISSP認定保持者の所属企業・組織の割合は、プロフェッショナルサービス28%、金融機関22%、政府関係組織14%となっている。

日本においても、みずほ銀行のように、情報システムのユーザー企業が、所属員に取得を奨励する動きが出てきているが、今後さらに、さまざまな業種業界で、CISSP導入の流れが強まっていくと予想される。

◆お問い合わせ先◆

NTTコミュニケーションズ株式会社
プラットフォームサービス部
Email: guardit@ntt.com
TEL: 0120-50-2568
URL: <http://sec.ntt.com/>

◆CISSPに関するお問い合わせ先◆

NTTラーニングシステムズ株式会社
総合研修事業部
Email: cissp-info@hot.nttlls.co.jp
TEL: 03-3440-1983

CISSP®CBK®10ドメイン

- ① Information Security Management
情報セキュリティマネジメント
- ② Enterprise Security Architecture
エンタープライズセキュリティアーキテクチャ
- ③ Access Control Systems&Methodology
アクセス制御のシステムと方法論
- ④ Applications Security
アプリケーションセキュリティ
- ⑤ Operations Security
運用セキュリティ
- ⑥ Cryptography
暗号学
- ⑦ Telecommunications, Network & Internet Security
通信、ネットワーク、インターネットのセキュリティ
- ⑧ Physical Security
物理的セキュリティ
- ⑨ Business Continuity Planning
事業継続計画
- ⑩ Law, Investigation & Ethics
法、捜査、倫理



図2 CISSP®CBK®10ドメイン