Ｖ．基準項目

４．ハードウェア・ソフトウェア供給者基準

(1) 管理体制の整備

・ハードウェア・ソフトウェア供給者の要員の業務範囲を明確にすること。

・不正アクセスを発見したときの連絡体制及び復旧手順を確立し、周知徹底すること。

(2) 設備管理

・開発業務に係る機器は、許可を与えられた者以外立ち入れない場所に設置し、厳重に管理すること。

・開発業務に係るネットワークは、他の業務のネットワークと分離すること。

(3) 開発管理

・製品のセキュリティ機能の実装に関する方針を明確にすること。

・製品は、機密保持機能、認証機能、改ざん検知機能等のセキュリティ機能を設けること。

・製品のネットワークに係る機能は、セキュリティ上の重要な情報の解析を防ぐ機能を組み込むこと。

・製品の保守に係る機能は、利用する者を限定する機能を組み込むこと。

・セキュリティの設定を行わないと製品が利用できない機能を設けること。

・製品の開発に使用したデバッグ機能等は、出荷前に削除しておくこと。

・製品のセキュリティ機能が仕様どおり動作するか検査すること。

(4) 販売管理

・製品は、流通段階における改ざん等を防止するための措置を施すこと。

・製品は、利用上の制限事項及び推奨事項を明示の上、販売等を行うこと。

・製品は、供給者の連絡先を明示しておくこと。

・製品にセキュリティ上の問題が発見された場合は、製品のユーザ及び関係者に情報を通知するとともに、問題を解決するための適切な処置を行うこと。

(5) 事後対応

・製品開発システムにおける異常を発見した場合は、速やかに原因を追究すること。

・不正アクセスであることが判明した場合は、関係者と協調して被害の状況を把握すること。

・関係者と協調して不正アクセス被害の拡大を防止するための処置を行うこと。

・事前に確立した復旧手順を遂行し、関係者と協調して不正アクセス被害の復旧に努めること。

・不正アクセス被害の原因を分析し、関係者と協調して再発防止策を行うこと。

・不正アクセス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。

(6) 情報収集及び教育

・製品のセキュリティ対策に関する情報を随時収集し、その情報を製品の開発に生かすこと。

・製品の販売を通じてセキュリティ対策の情報を提供し、必要に応じて教育を行うこと。

(7) 監査

・ハードウェア・ソフトウェア供給者が行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。