別紙

＜チェックリスト＞

昨今の標的型攻撃や新しいタイプの攻撃[1)]などに、それぞれの関門における多段の防御が有効となります[2)]。それぞれの組織におけるシステムやネットワークにおいて、下記の対策状況をチェックし、不足している部分を改善してください。

1. ネットワークの入口と経路での防御

- □ ファイアウォール
- □ 最新のウイルス対策ソフト　（ネットワーク、サーバ、クライアント）[3)]
- □ 侵入検知システム／防止システム
- □ 通信路の暗号化（Virtual Private Network などの利用）
- □ ネットワーク構造／設計　（重要なサーバに対するルート制御）

2. 脆弱性対策

2.1 サーバソフトウェアの脆弱性対策

- □ OS やサーバソフトウェアの定期的な脆弱性診断
- □ ウェブサイトで使用している OS やサーバソフトウェアに関する脆弱性情報の、時期を逸しない収集とパッチの反映[4)]

2.2 ウェブアプリケーションの脆弱性対策

- □ ウェブアプリケーションへの脆弱性の作り込みの回避[5)]
- □ ウェブアプリケーションの定期的な脆弱性診断
- □ ウェブアプリケーションファイアウォール（WAF）[6)]

3. アクセス制御

- □ ユーザ認証
- □ アクセスするプログラムの特定（ホワイトリスト化）

4. 情報の暗号化

- □ 暗号
- □ 暗号鍵管理

5. システム監視、ログ分析

- □ ネットワークログ取得・分析
- □ サーバログ取得・分析
- □ アクセスログの監査（DB 監査ツールなど含む）

6. 管理統制およびコンテンジェンシープラン

- □ セキュリティポリシー
- □ 海外を含むグループ会社間でのセキュリティガバナンス
- □ 危機対応体制の整備

上記のチェックリストは、下記 URL にて最新版を公開していますので、ご参照ください。
URL：http://www.ipa.go.jp/security/topics/alert230527.html

【参考資料】

1). IPA テクニカルウォッチ「新しいタイプの攻撃」に関するレポート
http://www.ipa.go.jp/about/technicalwatch/20101217.html
2). 2011年版 10大脅威　http://www.ipa.go.jp/security/vuln/10threats2011.html
3). コンピュータウイルス対策基準　http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm
4). 脆弱性対策情報データベースJVN iPedia　http://jvndb.jvn.jp/
5). 安全なウェブサイトの作り方 / 安全なSQLの呼び出し方
http://www.ipa.go.jp/security/vuln/websecurity.html
6). Web Application Firewall（WAF）読本　http://www.ipa.go.jp/security/vuln/waf.html
ウェブサイト攻撃の検出ツール iLogScanner　http://www.ipa.go.jp/security/vuln/iLogScanner/