別紙

セキュリティ対応状況チェックリスト

本チェックリストを用いて、自組織のセキュリティに対する攻撃や事象、マネジメントの確立、システムの構成状況、および技術的対策事項に対して現状把握と確認を行い、不足している部分を改善して下さい。　＜　　＞は具体的な内容記載に利用下さい。

１．これまでの攻撃、セキュリティ事象の有無

(1) サイバー攻撃の有無

□　不正アクセス　（頻度：これまで　（　　）度；　具体的な攻撃　＜　　＞）
□　DDoS 攻撃　（頻度：これまで　（　　）度；　具体的被害　＜　　＞）

(2) ウイルス感染の有無

□　あり　（感染経路：□外部メディア　□メール　□Web 閲覧　□その他）
（感染対象：□PC 感染　　□サーバー感染　　□重要サーバー感染）
（被害状況：□感染のみ　□業務停止　□情報漏えい　□その他）

(3) 標的型攻撃の有無

□　あり　（攻撃経路：□メール　□メディア　□電話　□その他）
（被害有無：□なし　　□あり　＜　　＞　）

(4) その他：　(1)~(3)以外で、セキュリティ脅威となった事項があれば
□　内部犯行　　□その他　＜　　＞

２．セキュリティマネジメント体制

(1) セキュリティ管理の専門部署、体制の有無

□　あり　＜体制のレベル：　　＞

(2) セキュリティポリシー

□　あり　（ベースとしている基準：　□ISMS　□P マーク　□その他＜　　＞）
□　機密レベルに応じた実施基準の有無
□　セキュリティでの認証の取得　（　□ISMS　□P マーク　□その他＜　　＞）
□　インシデント、事故発生時の行動規範記載有無
□　届出先機関　＜　　＞　　□事故対応体制　＜　　＞

(3) グループ会社、海外に対するガバナンス

□　海外含むグループ統一ポリシー　　□国内のグル―プ会社統一ポリシー
□　各グループ会社、海外子会社毎の個別ポリシー

(4) 御社のセキュリティマネジメントで不足しているものがあれば教えて下さい：

□ベースとなる基準の不足　＜　　＞
□その他　＜　　＞

３．システムの構成状況

(1) 情報系インフラと基幹系（製造/勘定/研究など）インフラは、分離されていますか？

□　物理的に完全に分離している
□情報のやり取りの有無　（ルート：□メディア　□その他＜　　＞）
□　論理的に分離している　（　□FW　　□VLAN　　□その他＜　　＞）
□情報のやり取りの有無　（ルート：□メディア　□その他＜　　＞）

(2) 基幹系インフラへのウイルス感染や不正アクセスの可能性を診断していますか？

□　している　　（診断：□机上　　□擬似アタック　□その他＜　　＞）

(3) 基幹系インフラへの脅威として認識していることがあれば教えて下さい。

□ウイルス感染　　□脆弱性　　□可用性　　□その他：下記へ記載下さい：
＜　　＞

４．技術的 対策事項

(1) システムへ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、サーバー、クライアント）[2)]
- □ 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 （重要なサーバーに対するルート制御やネットからの隔離）

(2) 脆弱性対策

- □ OS やサーバー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 やサーバー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 [3)]
- □ ウェブアプリケーションへの脆弱性の作り込みの回避 [4)]
- □ ウェブアプリケーションファイアウォール（WAF）[5)]

(3) 標的型攻撃ルート対策

- □ スパムフィルター
- □ URL フィルター
- □ 外部メディア利用規則、強制利用抑止

(4) ウイルス活動の阻害および抑止 (出口対策) [6)]

- □ 端末間、他部署間のネットワーク通信の制限（ウイルスの組織内蔓延抑止）
- □ 組織の端末からの外部通信はプロキシを経由させる等の経路制御
- □ 組織内ネットワーク量の監視（異常さを早期に検知しウイルスの蔓延を早期に発見）
- □ 知財等のある重要なサーバーはインターネットから隔離

(5) 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）

(6) 情報の暗号化

- □ 暗号
- □ 暗号鍵管理

(7) 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）

(8) 管理統制およびコンテンジェンシープラン (事前準備・事後対応)

- □ 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

【参考資料】

1). 2011年版 10大脅威 http://www.ipa.go.jp/security/vuln/10threats2011.html
2). コンピュータウイルス対策基準 http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm
3). 脆弱性対策情報データベースJVN iPedia http://jvndb.jvn.jp/
4). 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
5). 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/
6). 「新しいタイプの攻撃」の対策に向けた設計・運用ガイド
http://www.ipa.go.jp/security/vuln/newattack.html