【別紙1】お客さま企業のCSIRTによるセキュリティ管理体制（参考モデル）

◆ インシデント発生を前提としたセキュリティ管理体制

情報収集

- 自社システムの構成情報(インターネット接続の有無など)をデータベース化
- セキュリティインシデント、脆弱性情報やその影響範囲などを情報収集

脆弱性管理などの事前対策

- 自社システムの防御機能や、監視強化すべきポイントの確認
- 自社システムに対して、定期・随時で脆弱性診断を行い、脆弱性を発見した場合は、マルウェア感染の調査や、システム改修を実施

インシデント発生

事実の把握と迅速対応

- 事実に基づく正確な情報を再調査し、経営層に状況報告
- 自社システムへの影響有無を判断し、迅速に対策を講じる
- 自社システムの構成情報に基づき、再点検の実施

CSIRT運用支援ソリューション

WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

アドバイザリーサポート

脆弱性診断

インシデント
レスポンス

脆弱性マネジメントプラットフォーム(仮称)