サイバー攻撃（標的型攻撃）対策防御モデルの解説

1.防御モデルの解説概要

○本解説は、巧妙化・複雑化し続けるサイバー攻撃（特に標的型攻撃）への対策として、官公庁・民間企業が具備することが推奨される機能群(以下「防御モデル」という。)を解説するものです。本解説内容の公開・普及により、サイバー攻撃への対応能力が向上することを目的としています。

○防御モデルは、人・組織対策と技術的対策から構成されており、前者ではインシデントレスポンスの計画と実行について、後者では事前対策・検知・事後対策について解説しています。

○本解説書は、情報システム等の安全性を確保する立場から、標的型攻撃に対応する担当者及び関係者を想定読者としております。

＜本解説の読者について＞

想定読者		説明
自組織	情報セキュリティ責任者	自組織の情報セキュリティ責任者（CISO等も含む）
	設計・開発担当者	自組織の情報システムに関する設計・開発の担当者
	LAN管理者	自組織のLAN管理者
	LAN運用者	自組織のLAN運用者
外部専門組織	設計・開発者	自組織の設計・開発者からの依頼に基づき一部の設計・開発を行う外部専門組織の設計・開発者
	運用者	自組織のLAN管理者又はLAN運用者からの依頼に基づきLANの運用を行う外部専門組織の運用者

サイバー攻撃（標的型攻撃）対策防御モデルの解説

2.防御モデルが対応するサイバー攻撃について

○防御モデルは、「標的型メール」、「Drive-by-Download等のWebサイト」、「不正コードを流入させたソフトウェア」、「USBメモリ」、「保守業者の持ち込んだ機器」、「クラウドサービス」を攻撃経路とするサイバー攻撃（標的型攻撃）を想定しています。