これまでに採った措置と今後の対策について

平成２４年２月２日
衆議院事務局庶務部
情報基盤整備室

報告書(H23.12.7)における記載		現在の状況	備考
１　緊急に措置した対策	(1)日常監視強化	・不正サイトへの通信の有無等に対する監視を強化。	実施中
	(2)議員用端末の全台緊急点検	・各議員事務室と会派事務室を対象とした緊急セキュリティ点検を実施。	実施済み
	(3)臨時セキュリティ研修	・議員・秘書等を対象とした臨時セキュリティ研修を実施。	実施済み
２　短期的に実施すべき対策	(1)利用者への周知方法の確立	・不審メール情報等について、イントラ等を活用して周知。	年度内実施予定
	(2)ヘルプデスクによる議員用端末の定期検診	・次年度よりヘルプデスク要員を2名増員し、各議員事務室を定期的に訪問、セキュリティ確認を実施。	
	(3)システムの健全性確認	・すべてのサーバを対象にしたセキュリティチェックと、アカウントサーバに対するデータベース解析・診断によるクリーニングを実施。	実施中
	(4)アカウント管理体制の強化	・システム全体の管理者権限を持つアカウントのパスワードをすべて変更。	実施済み
		・万一の際に被害を限局するため、管理者権限の細分化を実施。	実施中
	(5)不正・不要な通信の排除	・リモートアクセス端末からの接続をより安全に行うための仕組みを導入。	年度内実施予定
	(6)議員用端末の更新及びセキュリティ強化	・全議員事務室の端末更改に伴い、既存の認証証明書の失効をはじめとするセキュリティ対策を実施。	実施中
	(7)標的型不審メール訓練	・政府が行っている標的型不審メール訓練を参考に実施。	年度内実施予定

報告書(H23.12.7)における記載		現在の状況	備考
3　中長期的に検討すべき対策	(1)緊急事態対応訓練	・大規模サイバー攻撃初動対処訓練 ・サイバーインシデント発生時における対応及び連絡体制訓練	実施済み
	(2)定期的なセキュリティ研修	・議員、秘書、会派及び職員に対する定期的なセキュリティ研修を実施していく予定。	
	(3)悪性サイトの通信制限及び監視強化	・不正な通信先の情報等について、衆・参・図で積極的な情報交換を行うこととしたほか、通信制限の自動化については、費用及び効果を踏まえ、導入について検討。	
		・ウィルスの活動に特徴的な通信を自動的に検知する仕組みについて、費用、効果及びそれぞれのサービスによる違い等を踏まえ、導入について検討。	
		・24hの有人監視について、費用、効果及びそれぞれのサービスによる違い等を踏まえ、導入について検討。	