平成 24 年 2 月 2 日
参 議 院 事 務 局
情報システム安全管理室

参議院に対するサイバー攻撃への対応状況について

1．組織改編

本年１月１日付けで組織上の体制整備を図るため、これまでの庶務部文書課情報化推進室を事務次長直属の「情報システム安全管理室」に組織改編するとともに、セキュリティ対策の充実を図るため、セキュリティに関する知識、経験を有する者２名を民間から採用・配置いたしました。

新たに採用した職員には、セキュリティを確保する観点から、現行情報システムの運用・管理等の指導や援助、セキュリティ監査やセキュリティ研修の企画・実施或いは、実際にサイバー攻撃等インシデント発生時の適切な対応・連絡調整の実行などを担ってもらうこととしております。

2．これまでに実施した対策

サイバー攻撃前までに実施していたウィルスチェックの二重化や不正侵入監視装置の設置等に加え、以下の対策を実施しました。

1）議員室のパソコンの全台ウィルスチェック

議員室に設置しているパソコンについて、完全スキャンの実施、セキュリティ設定の現状調査を行い、不備が確認されたパソコンについては、対処を行いました。

2）システム監査

ネットワークシステムについて、専門会社が設定内容、運用状況等を調査し、堅牢性の確認、問題点の検出を行いました。

3）抜本的なセキュリティシステムの設計調査

サイバー攻撃による情報流出等の事態を発生させないために、最新の技術動向等を踏まえ、今後のネットワークシステムのあり方について、調査しました。

4）セキュリティ研修、不審メール訓練等の実施

議員、秘書、事務局職員等に対し、昨年１１月と本年２月にセキュリティ研修を、昨年１２月に標的型不審メールの模擬メールを用いた訓練を実施しました。また、本年１月に、関係機関と連携した大規模サイバー攻撃初動対処訓練を実施しました。

5）インターネットとの不正通信の監視

参議院とインターネットとの不正通信の有無について、専門会社による２４時間監視を開始しました。

6）議員室パソコンの運用管理の改善

議員室のパソコンについて、Windows アップデート及びウィルスチェックの自動実行を開始しました。また、参議院のネットワークに接続する私有パソコン向けにウィルス対策ソフトの提供を行いました。

３．今後、実施を検討している対策

昨年１２月１６日の参議院サイバー攻撃対策本部の最終報告（別紙「最終報告書のポイント」参照。）においては、新たに実施すべき「技術的な対策」、「運用的な対策」及び将来的な方策が提示されました。今後、提示された対策については、検討の上、導入の必要性等を勘案しながら、迅速かつ着実に実行してまいります。

また、将来的な方策については、次回のネットワークシステム更改等の際に、最適なシステム構成が選択できるよう、検討を進めてまいります。

○　新たに実施すべき対策

1）Ｗｅｂフィルタリングシステムの導入

不正プログラムを配信するようなＷｅｂサイトの情報を最新に保ち、かつ、当該Ｗｅｂサイトへの接続を自動的に遮断します。

2）検疫ネットワークの導入

ネットワークに接続したパソコンについて、ウィルス対策ソフト、セキュリティパッチの適用状況等を自動的に検出し、不備が確認されたパソコンはネットワークに接続させないようにします。

3）不審な通信の検出

ネットワークの内部において、ウィルスの動作に伴うような異常な通信を、自動的に検出します。

4）アプリケーションの仮想化

ウィルス付きメールの被害を拡大させないよう、サーバで電子メールソフト等が動作するようにし、利用者はパソコン上で、それらの機能を利用するようにします。

5）通信ログの異常検知

ファイアウォール、Ｗｅｂアクセスの履歴等の各種の通信ログを横断的に分析し、異常の有無を検出します。

6）ネットワークトラフィックの監視

ネットワークを流れる全ての通信データを記録し、緊急の事態が発生した際に、原因、影響範囲の分析に利用します。

7）通信のアクセス先の監視

通信の利用実態を記録し、相手先を分析することにより、不審な相手先を検出し、情報漏えい等を回避します。

○将来的な方策

1）ＰＣの接続方式

現在はクライアント・サーバ方式で接続し、セキュリティの設定について、集中管理しています。ＶＰＮ（仮想プライベートネットワーク）方式による接続について、集中管理による安全性とネットワークの利便性の観点から比較、検討してまいります。

2）仮想化技術の活用

情報漏えい等を回避するために、パソコンからインターネットに直接接続しないよう、全てのソフトウェアの動作をサーバで行い、利用者は、それがあたかもパソコンで操作しているかのように見せる技術について、今後の動向を踏まえ、採用を検討してまいります。

別　紙

平成23年12月16日
情報化推進室

最終報告書のポイント

本日、今般の参議院に対するサイバー攻撃に関する感染事象の事実解明、システム監査及び抜本的なセキュリティシステムの設計調査について、参議院サイバー攻撃対策本部から最終報告があった。

各報告のポイントは以下のとおりであるが、共通する主要課題は、運用面も含めたシステム全体のセキュリティ水準の向上、セキュリティ体制の見直し、サイバー攻撃を前提としたシステムの在り方であった。

これらの実効的な対応策は、各報告の中で具体的な対策として掲げられており、今後第２、第３のサイバー攻撃が想定される中、迅速、かつ、着実に実行することが求められている。

１．参議院におけるサーバ等のウイルス感染事象について

１）概要

感染した機器は、サーバ２台、パソコン２９台。

２）感染原因

ウイルスは、衆議院へのサイバー攻撃で確認されたものとは異なる、トロイの木馬型ウイルスの亜種「Trojan.Mdropper」。

３）流出の可能性がある情報

感染したパソコンが受信したメールのヘッダ情報、当該パソコンの設定情報・動作情報・ファイルリスト、ネットワーク情報、アカウント認証サーバ内のアカウント及び暗号化されたパスワードデータ等が想定される。

４）感染経路

［一次感染］８月５日、悪意のあるメールの添付ファイルを開封した３台のパソコンが感染。
［二次感染］同月８日、既に感染したパソコンから同じ議員室内のパソコン１台に感染。
［三次感染］同月８～９日、当初感染した２台のパソコンからアカウント認証サーバ１台、監視サーバ１台の計２台に感染。
［四次感染］同月２２日、同認証サーバを踏み台として、議員室１０室のＰＣ２５台に感染。

２．システム監査状況

システム監査から、次のような指摘があった。

・ウィルス対策ソフトの定期スキャンやWindowsアップデートが強制実行されていない。

→現在は、ウィルス対策ソフトの定期スキャンやWindowsアップデートの強制実行がなされている。

・不正な通信の分析・評価などを行っていない。

→現在は、不正通信に対する異常検知システムとして、外向けの２４時間監視システムがが導入され、分析・評価も行っている。

・ウィルス対策が実施されていない私有パソコンの利用がある。

→現在は、私有パソコンについて、定期スキャンを組み込んだウイルス対策ソフトの提供等をしている。

・利用者の利便性・自由度を重視し、重要なセキュリティ対策が十分ではない。

→現在は、セキュリティ専門家の任用等による体制整備のほか、議員事務室のセキュリティポリシーの策定作業等を行っている。

３．抜本的なセキュリティシステムの設計調査

１）技術的なセキュリティシステムの設計調査

技術的な対策と運用的な対策との組み合わせによる対応の検討。

[技術的な対策]

・ウェブフィルタリングシステム（危険なサイトへのアクセス拒否）

・検疫ネットワークシステム（検疫を経ない私有パソコンの使用禁止）

・不審な動作の検出システム（正常な通信内の不審な動作の検出）

・アプリケーションの仮想化（メール等アプリケーションの仮想環境での実行）

[運用的な対策]

・通信ログ異常検知システム（通信ログの横断的な異常検知）

・ネットワークトラフィック監視システム（全てのパケット情報の記録・監視）

・通信のアクセス先監視システム（不適切な通信の監視）

２）情報セキュリティ体制の抜本的見直し

情報セキュリティに関する人的物的体制の抜本的見直し（人的体制や責任の明確化。セキュリティポリシーやマニュアルの詳細化。利用者がセキュリティを遵守するためのルール整備等）。

→来年１月の情報化推進室の組織改編、セキュリティ研修の実施。

３）将来的な方策

将来的なセキュリティシステムの方策として、「仮想化技術活用方式」（シンクライアント（ソフトは全てサーバ上で動作する仕組み）を活用するシステム方式）と「新LAN方式」（現行ＬＡＮに検疫ネットワークシステム等の機能拡張を施したシステム方式）の提案。