政府機関における標的型不審メール訓練について

資料2-1

政府は、本年5月に情報セキュリティ対策推進会議（CISO等連絡会議）において決定した「政府機関における情報セキュリティに係る年次報告」において取り組みを推奨した「標的型不審メール訓練」を以下のとおり実施する。

1．訓練期間　　平成23年10月～12月
2．訓練対象　　内閣官房等12の政府機関約5万名
3．訓練内容

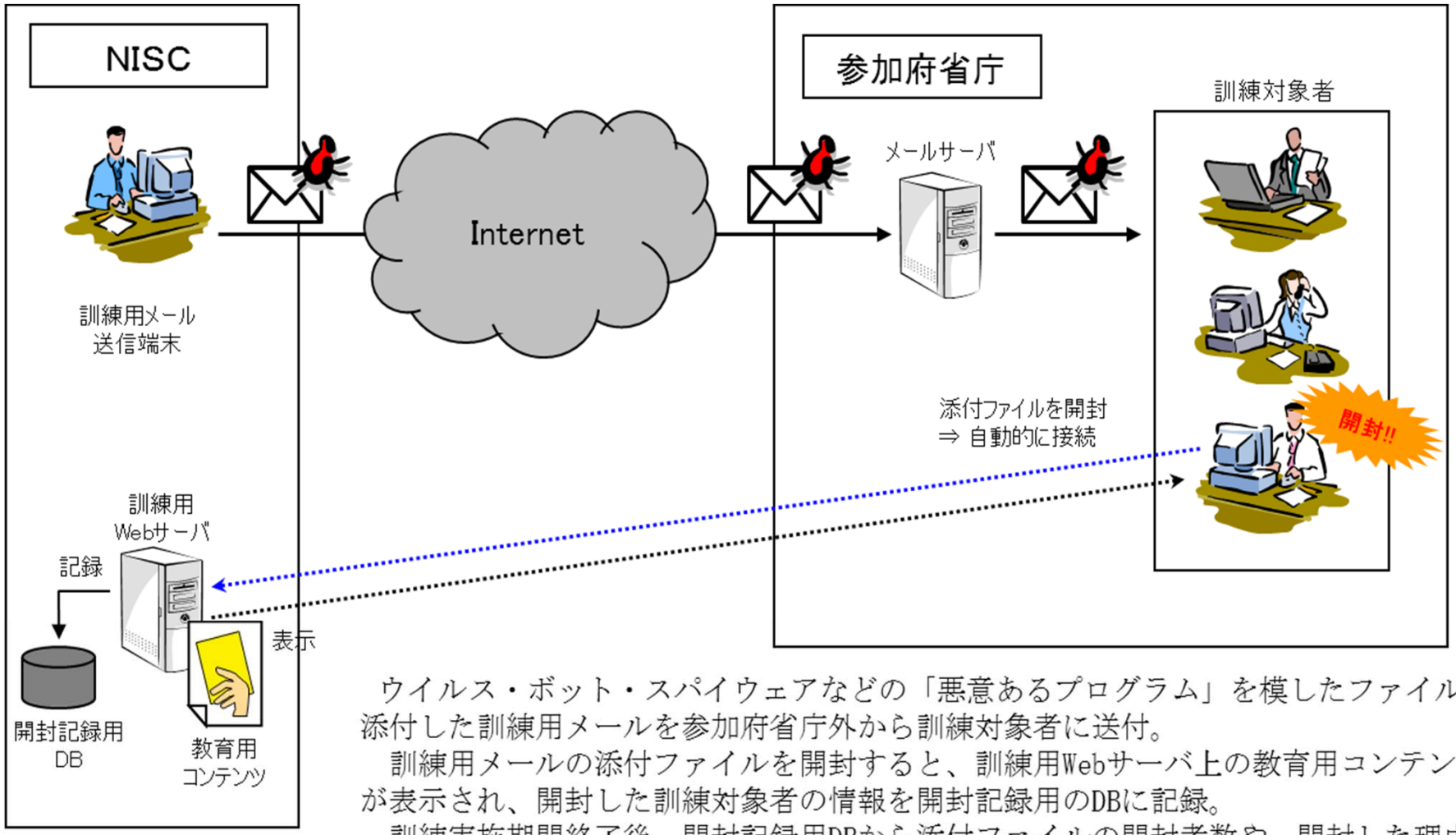
①訓練対象者に対して、標的型不審メールを模擬したメールを送付。

②模擬メール中の添付ファイルを開封するなど不適切な扱いをした場合は、教育コンテンツに誘導。

③参加府省庁のCISOに個別の訓練結果を通知し、府省庁内において適切な教育指導を実施。

④CISO等連絡会議にて訓練結果の総評を報告。

参考 （訓練の実施イメージ図）



ウイルス・ボット・スパイウェアなどの「悪意あるプログラム」を模したファイルを添付した訓練用メールを参加府省庁外から訓練対象者に送付。

訓練用メールの添付ファイルを開封すると、訓練用Webサーバ上の教育用コンテンツが表示され、開封した訓練対象者の情報を開封記録用のDBに記録。

訓練実施期間終了後、開封記録用DBから添付ファイルの開封者数や、開封した理由等の教育結果を集計。

◎　標的型メールを見極めるポイント

1. 差出人欄に注意！！
   （フリーメールアドレスや普段やりとりのない@ドメイン）
2. 件名に注意！！
   （【至急】【重要】は罠キーワード）
3. 本文末の署名に注意！！
   （差出人メールアドレスと署名のメールアドレスが違う）

◎　不審なメールが送られて来た場合の対処方法

ヘルプデスクもしくは、情報システムセキュリティ管理者に連絡する

◎　万が一不審なメールの添付ファイル等を開封してしまった場合の対処方法

1. LANケーブルを抜く
2. ヘルプデスクもしくは、情報システムセキュリティ管理者に連絡する