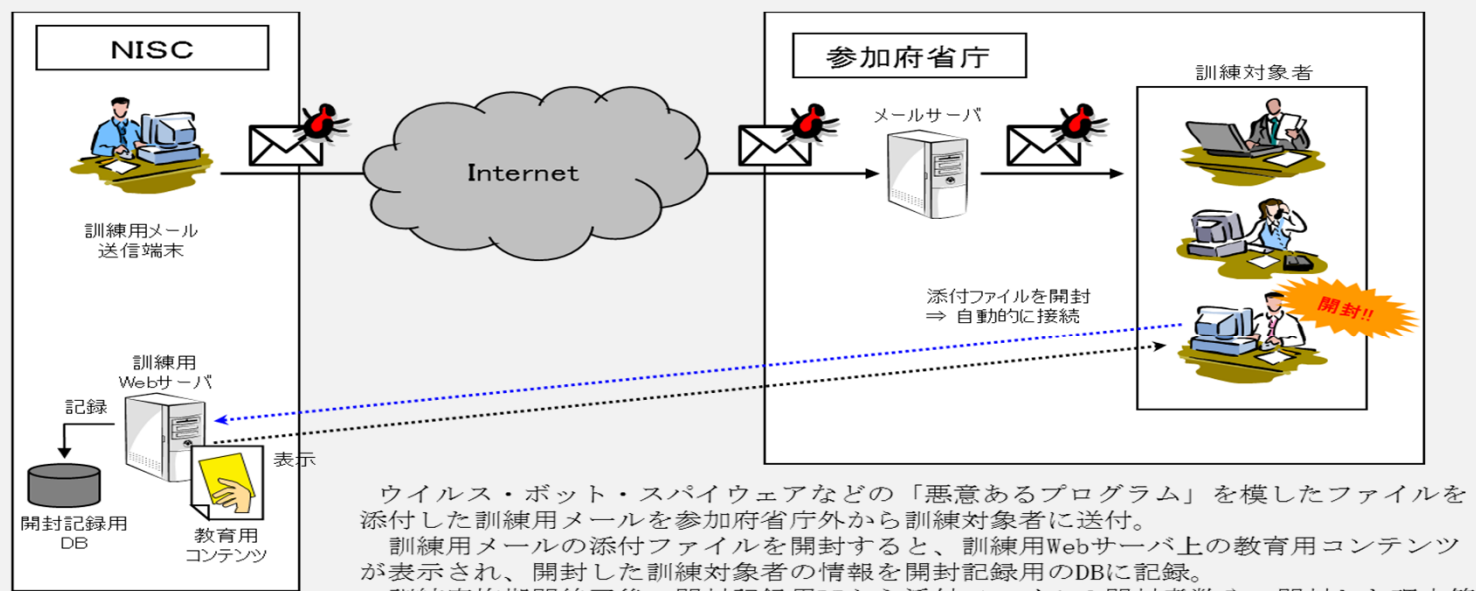


平成23年度 標的型不審メール攻撃訓練結果の概要(中間報告)

標的型不審メール攻撃訓練結果の概要(中間報告)

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6万名
3. 訓練内容：
 - ①訓練対象者に対して事前教育の実施。
 - ②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2回送付。
 - ③模擬メール中の添付ファイルを開封もしくは、URLをクリック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。
 - ④参加府省庁に個別の訓練結果を通知し、各府省庁内において適切な事後教育指導を実施。



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。

平成23年度 標的型不審メール攻撃訓練結果の概要(中間報告)

4. 訓練結果：今回の訓練における不審メールの開封率は以下のとおり。
(中間報告) ◆1回目(添付メール) 10.1% (1.1%~23.8%)
◆2回目(リンクメール) 3.1% (0.4%~6.1%)
5. 結果分析：①1回目の結果と比べ2回目の結果が良くなっていることから、標的型不審メール
(中間報告) に対するセキュリティ意識は向上したものと想定される。
②ただし、この効果は一時的なものであり、時間の経過とともに意識レベルは低下するものと想定されるため、今後も訓練を継続していくことが重要である。
6. 課題：不審メールを開封した事例のほか、
(中間報告) ①不審メールの送信元に対し、メールを返信する方法で差出人の確認をしているケース
②メールの自動返信機能を設定することにより、攻撃者に対し、不在通知が自動発信されたケース
がみられた。
これらの事例では、組織で使用している有効なアドレスを攻撃者に通知してしまうことになり、攻撃者に次の攻撃に資する組織内の情報を提供したことになる。
したがって、これらについても対策が必要となる。
対策としては、
①差出人の確認については、電話等により行うこと
②自動返信の範囲を組織内に限定すること
などが考えられる。

※ 各府省庁からのリクエストにより、訓練方法をカスタマイズしているケースがある。