NISC National Information Security Center

政府機関における情報セキュリティ対策に関する取組

平成24年2月

内閣官房情報セキュリティセンター（NISC）

http://www.nisc.go.jp/

なりすまし対策（go.jpドメインの使用／送信側SPF対策）の推進

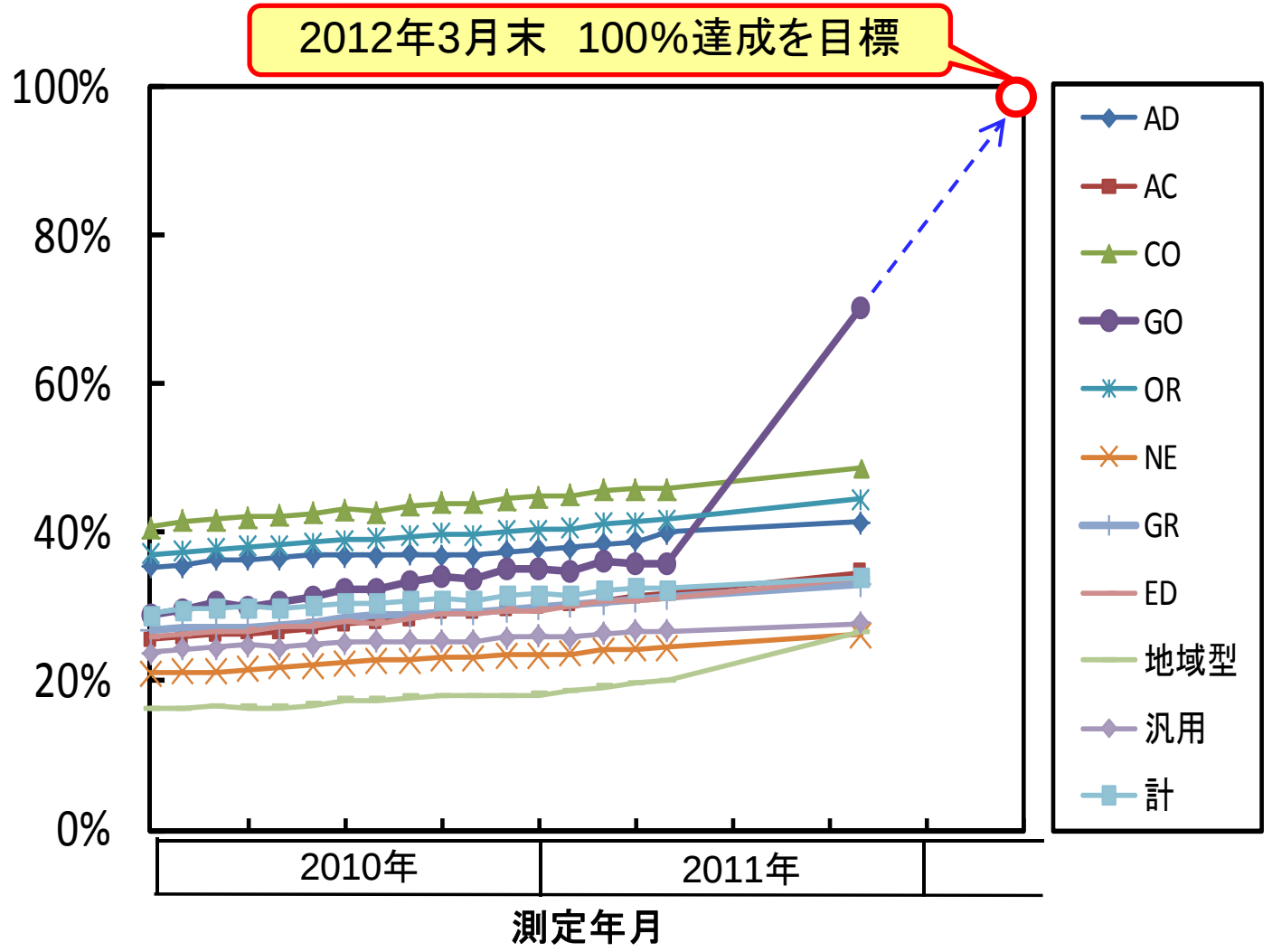
・ 政府機関（go.jp）を騙る**なりすましメール**から、国民や政府機関自身を守るため、go.jpドメインに対し、**送信側SPF対策を推進**しています。＊SPF（Sender Policy Framework）：メールの送信元アドレスの偽装を防止する技術

SPF設定状況

第3レベルのgo.jpドメインの設定率
＊当センターによる調査結果

2011年7月31日	37.4％
2011年10月13日	63.2％
2012年1月16日	85.1％

WIDEプロジェクト調査結果
（http://member.wide.ad.jp/wg/antispam/stats/index.html.ja を基に当センターでグラフを作成）



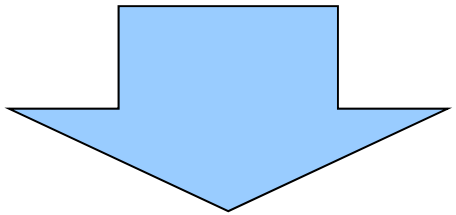
政府機関における情報セキュリティ対策の向上のための訓練・検査の実施

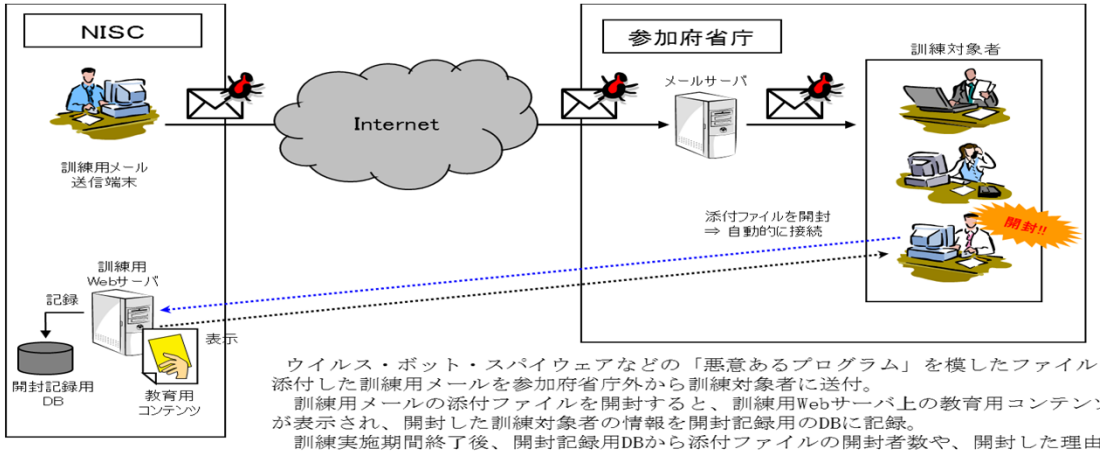
標的型不審メール攻撃訓練結果の概要（中間報告）

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。

訓練の目的・効果

標的型メール攻撃に対する職員の意識向上と注意喚起を促すとともに、適切に対応するための対処手順の確認を目的として実施。また、得られた課題については、今後の職員教育等に反映。

「標的型不審メール攻撃訓練」実施結果の概要（中間報告）

●訓練結果（中間報告）：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。
- ◆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%）

●結果分析（中間報告）：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。

●課　　題（中間報告）：不審メールを開封した事例のほか、
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。

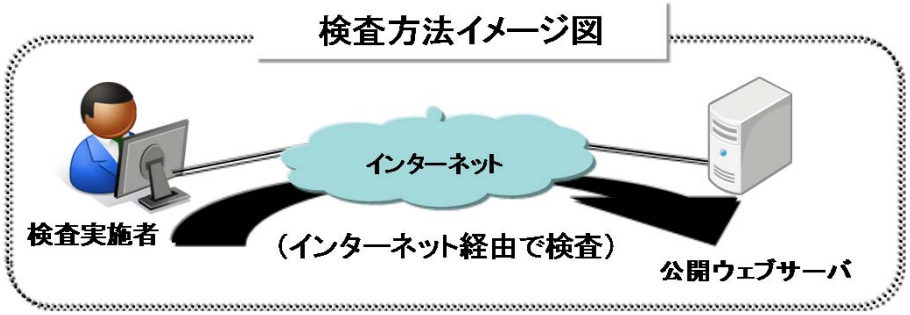
※　各府省庁からのリクエストにより、訓練方法をカスタマイズしているケースがある。

脆弱性検査の実施による政府機関のセキュリティ対策の向上

脆弱性検査実施内容

1. 検査期間：平成23年9月～12月
2. 検査対象：政府機関における公開ウェブサーバ（検査希望のあった11省庁、約330画面）
3. 検査方法：対象とする公開ウェブサーバにインターネット経由でアクセスし、ツール及び手動により検査を実施
4. 検査内容：プラットフォームに関する検査
   ウェブアプリケーションに関する検査
5. 検査結果：検出された脆弱性のうち緊急性の高いもの（別紙参照）については、当該府省庁に対し速報を発出し、対策を実施

検査方法イメージ図

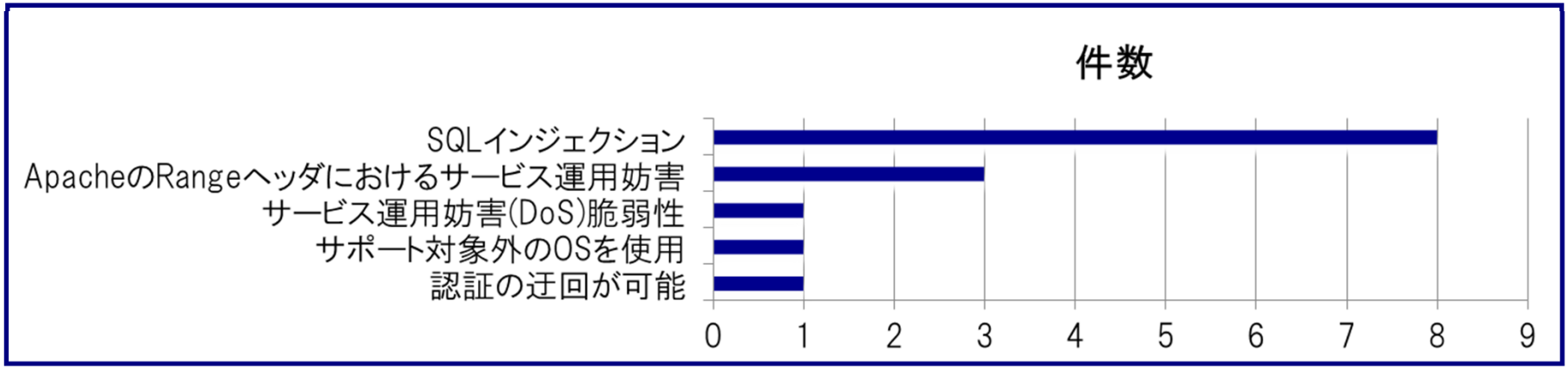


検査結果の活用

検査結果については、全府省庁に対して情報共有を行い、政府機関全体の情報セキュリティ対策の向上（情報流出の防止、ウェブサイト閲覧等の持続性維持）に活用

「公開ウェブサーバの脆弱性検査」実施結果の概要

危険度「高」の検出結果（延べ14件）



	脆弱性内容	原　因	想定される被害
1	SQLインジェクション	ウェブアプリケーションにおいて、入力値チェックやエスケープ処理が徹底されていない	データベースに格納されている情報の漏えい、改ざん、破壊等の可能性
2	ApacheのRangeヘッダにおけるサービス運用妨害	パッチ未適用	サービス運用妨害(DoS)により、サーバが停止する可能性
3	サービス運用妨害	ハードスペックやソフトウェア設定において、システム導入時に見積もった内容が実運用時のデータ送信量に対し過少である可能性	サービス運用妨害(DoS)により、サーバが停止する可能性
4	サポート対象外のOSを使用	ー	パッチ適用による対策が行えず、セキュリティ侵害が発生する可能性
5	認証の迂回が可能	ウェブアプリケーションにおいて、ログイン処理の成功、不成功にかかわらずアクセス可能なプログラムになっていた可能性	IDとパスワードを入力せずにログイン後のページにアクセスでき、情報漏えい等の可能性

東日本大震災を踏まえた政府機関のIT-BCP策定に向けた取組

平成23年3月11日に発生した東日本大震災おいて、政府機関で実施していた情報システムに関する対策とその被害状況について調査を行い、得られた知見や教訓を政府機関のIT-BCP策定に反映していきます。

取組の概要

調　査

- 政府機関の情報システムに関して、東日本大震災時の対策実施状況とその被害状況について調査
- 調査方法：主にアンケートとヒアリングによる調査を実施

＊アンケート有効回答数
　延べ 約250件
＊調査対象
　本府省庁、東北3県（岩手、宮城、福島）と首都圏の一部の省庁の地方支分部局及び施設等機関
＊調査時期
　平成23年9月～12月

分　析

- IT資源（建屋、ハードウェア、データ等）毎に、地震・津波・計画停電の各脅威に対し有効であった対策と有効ではなかった対策を整理
- 事前に実施していた対策と、その有効性との相関関係から、その対策の効果の有無を分析

成果の反映

- 分析によって得られた知見から、優先的に取り組むべき対策を整理
- 効果の高い対策について政府機関のIT-BCPガイドラインや統一基準群への反映について検討

- **検討結果を踏まえ、政府機関のIT-BCP策定に反映**

注意喚起等による各府省庁のセキュリティ対策の促進・支援

情報セキュリティセンターでは、日々のセキュリティ動向を踏まえ、適宜、各府省庁向けの注意喚起等の文書を発出し、各府省庁のセキュリティ対策の促進・支援を行っています。

最近発出した注意喚起等

年　月	概　要
2011年12月	ネットワーク利用者を管理するサーバのセキュリティ対策の徹底について ⇒ネットワーク利用者を管理するサーバ（Active Directoryサーバ、Notesサーバ等）の適切な設定を推奨
2011年12月	システム管理権限を狙った辞書攻撃、ブルートフォース攻撃への対処について ⇒辞書攻撃及びブルートフォース攻撃への対処として、サーバの運用管理に当たってとるべき対策を推奨
2012年 1月	公開ウェブサーバ脆弱性検査において複数の省庁で確認された脆弱性について ⇒SQLインジェクション及びサービス運用妨害（DoS）の脆弱性の確認、対応を推奨
2012年 2月	情報セキュリティポリシーに基づき職員が遵守すべき事項の周知徹底について （「情報セキュリティ月間」における取組） ⇒情報漏えいを防ぐため、職員が特に留意すべきポイントなどについて周知徹底