我が国政府における ネットワークセキュリティ 確立への取り組み

戸村　哲　産業技術総合研究所情報処理研究部門
s.tomura@aist.go.jp
三輪信介　通信総合研究所情報通信部門
danna@crl.go.jp
大野浩之　通信総合研究所情報通信部門
hohno@ohnolab.org

筆者の大野，戸村は内閣官房情報セキュリティ対策推進室の非常勤職員に併任しており，専門調査チームの一員として勤務している．まず内閣官房情報セキュリティ対策推進室の情報セキュリティ対策への取り組みの経緯と概要を，公開情報に基づいて説明する．続いて筆者らの所属する研究チームにおける，電子政府のための情報セキュリティ対策への取り組みを紹介する．

内閣官房の取り組み

■事の始まり「情報セキュリティ関係省庁局長等会議」

政府機関が情報セキュリティ対策への取り組みを本格化させたのは平成11年である．情報セキュリティ政策について，政府全体として総合的な対策の推進を図るために平成11年9月17日に内閣に情報セキュリティ関係省庁局長等会議（議長：古川官房副長官，内閣官房，関係12省庁の局長級で構成）を設置し，「情報セキュリティ関係省庁局長等会議における課題」[1]の検討を行った．議論の結果として平成12年1月21日に「ハッカー対策等の基盤整備に係る行動計画」[2]を決定した．以降基本的にはこの計画に従って政府の情報セキュリティ対策が進められている．

■事案の発生「情報セキュリティ対策推進室」の設置

この「行動計画」が決定されたわずか3日後の平成12年1月24日に，科学技術庁（当時）のWebページが改竄されたのを皮切りに，いくつかの中央省庁のWebページの改竄事件が発生した．この事件を契機として，政府機関の情報セキュリティ対策の強化の必要性が再認識され，「行動計画」の一部を前倒しで実施することと，そのための体制整備が行われた．関係行政機関相互の緊密な連携の下，官民における情報セキュリティ対策の推進を図るために平成12年2月29日に情報セキュリティ関係省庁局長等会議を廃止し，拡充した情報セキュリティ対策推進会議（議長：古川官房副長官，全省庁の局長がメンバ，衆議院，参議院，人事院，会計検査院，最高裁判所，日本銀行の担当者がオブザーバ）を高度情報通信社会推進本部に設置した[3]．

この高度情報通信社会推進本部（平成6年8月2日閣議決定）は我が国の高度情報通信社会の構築に向けた施策を総合的に推進し，情報通信の高度化に関する国際的な取り組みに我が国として積極的に協力することを目的として，内閣総理大臣を本部長，内閣官房長官，郵政大臣および通商産業大臣を副本部長，その他全閣僚を本部員として設置されている[4]．

また同日，高度情報通信社会推進本部に官民の情報セキュリティ対策の推進を図るために民間の有識者で構成される情報セキュリティ部会を設置した[5]．

さらに同日，内閣官房安全保障・危機管理室に情報セキュリティ対策推進室が誕生する[6] ☆1．

☆1 この時点では，内閣官房内閣安全保障・危機管理室情報セキュリティ対策推進室であったが，平成13年1月6日の省庁再編に伴い，内閣官房の組織再編があり，安全保障・危機管理室が廃止となり，現在は内閣官房情報セキュリティ対策推進室となっている．

■その後の変遷

その後，平成12年7 月7日の閣議決定により高度情報通信社会推進本部が廃止され，情報通信技術（IT）戦略本部が設置され[7]，また同日情報通信技術（IT）戦略本部長決定により民間有識者からなるIT戦略会議が設置された[8]．

さらに平成12年11月29日に高度情報通信ネットワーク社会形成基本法（「IT基本法」）[9] が成立し，同法第3章の規定に従い，高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）が設置される．

政府機関の局長級会議である情報セキュリティ対策推進会議については省庁再編後の平成13年1月22日にIT戦略本部の下に設置されている[10]．

また情報セキュリティ部会に対応するものとして情報セキュリティ専門調査会が同じく設置されている[11]．

■「情報セキュリティ対策推進室」の取り組み

情報セキュリティ対策推進室では，政府機関の情報セキュリティレベルの向上に資する日常業務を行うとともに，情報セキュリティ対策推進会議の事務局として計画に基づいた施策を行っている．まず平成12年7月14日には，情報セキュリティ部会のセキュリティ対策WGでの検討を経て作成した「情報セキュリティポリシーに関するガイドライン」[12] を情報セキュリティ部会に報告・了承され，7月18日の情報セキュリティ対策推進会議で決定した．この「セキュリティポリシーガイドライン」に基づいて各省庁では，平成12年12月末を目処にそれぞれのセキュリティポリシーを策定している．

次に情報セキュリティ部会にサイバーテロWG を設置し，「重要インフラのサイバーテロ対策に係る特別行動計画」[13] の実務的検討作業を行った．平成12年12月13日の情報セキュリティ部会にこの計画を報告・了承され，12月15日には情報セキュリティ対策推進会議で決定している．

この「特別行動計画」に基づいて平成13年3月16日は，IT戦略本部 情報セキュリティ専門調査会第1回会合を開催し，サイバーテロ対策の今後の進め方の詳細の検討作業を開始した．関係WGを設置し，関係者との協議を経て，平成13年10月2日の情報セキュリティ専門調査会において「サイバーテロ対策に係る官民の連絡・連携体制について」[14] を決定した．

平成13年10月10日の情報セキュリティ対策推進会議にもこの「サイバーテロ対策に係る官民の連絡・連携体制について」を報告するとともに「電子政府の情報セキュリティ確保に係るアクションプラン」[15] を決定した．

産業技術総合研究所 電子政府対応情報セキュリティチームの取り組み

産業技術総合研究所の電子政府対応情報セキュリティチーム（5名）は電子政府の実現と維持に必要なセキュリティ技術の開発を行っている．特に各人の情報セキュリティ技術の専門性を活用した人的貢献を目標としており，現時点では，内閣官房情報セキュリティ対策推進室専門調査チームへの参加，電子政府のための政府調達に係るIT製品等のITセキュリティ評価を行う評価機関の認定を行う情報技術セキュリティ評価機関認定プログラム[16] への参加，電子政府で安心して使用できる暗号の評価を行う暗号技術評価委員会（CRYPTREC）[17] への参加を行っている．

以下にチームメンバの研究を簡単に紹介する．

■インターネットのための資源管理システム

誰でも自由に参加し，全世界と情報交換を行えることがインターネットの特徴であるが，反面，不正侵入，プライバシ侵害，著作権侵害といった問題も顕在化しつつある．この問題を解決するために，インターネット上で取り扱われる多様な情報資源（ディジタルコンテンツから機器類まで）の利用を，その管理者の意図に沿って適切に関する新方式の研究を行っている．意図（ポリシー）の記述方式，利用者の権利や資格の記述方式，それらの安全な伝達方式，さらにこれらに基づく資源管理を安全に行うための「ポリシー実施エンジン」のアーキテクチャの研究が中心である．

■暗号技術評価とセキュリティシステム検証

ディジタル情報のやりとりや取引では，プライバシの保護や偽造防止，相手の認証といった機能を実現する「情報セキュリティ技術」が非常に重要な役割を果たす．情報セキュリティ技術の基礎となる暗号技術の安全性を，理論的に示すための安全性指標として，どのようなものを用いるのが良いのかについて研究する．

■XMLを利用したセキュリティ情報の構造化と利用法に関する研究

セキュリティ対策の実施プロセスを支援するために，セキュリティ情報の表現方法および情報間の関連づけ手法，分析手法の研究を行う．具体的には，情報の表現をXMLで構造化し，個別に作られた情報を相互に関連づける方法，ユーザやアプリケーションプログラムが利用しやすいかたちに加工する方法，定量的な分析方法を研究する．

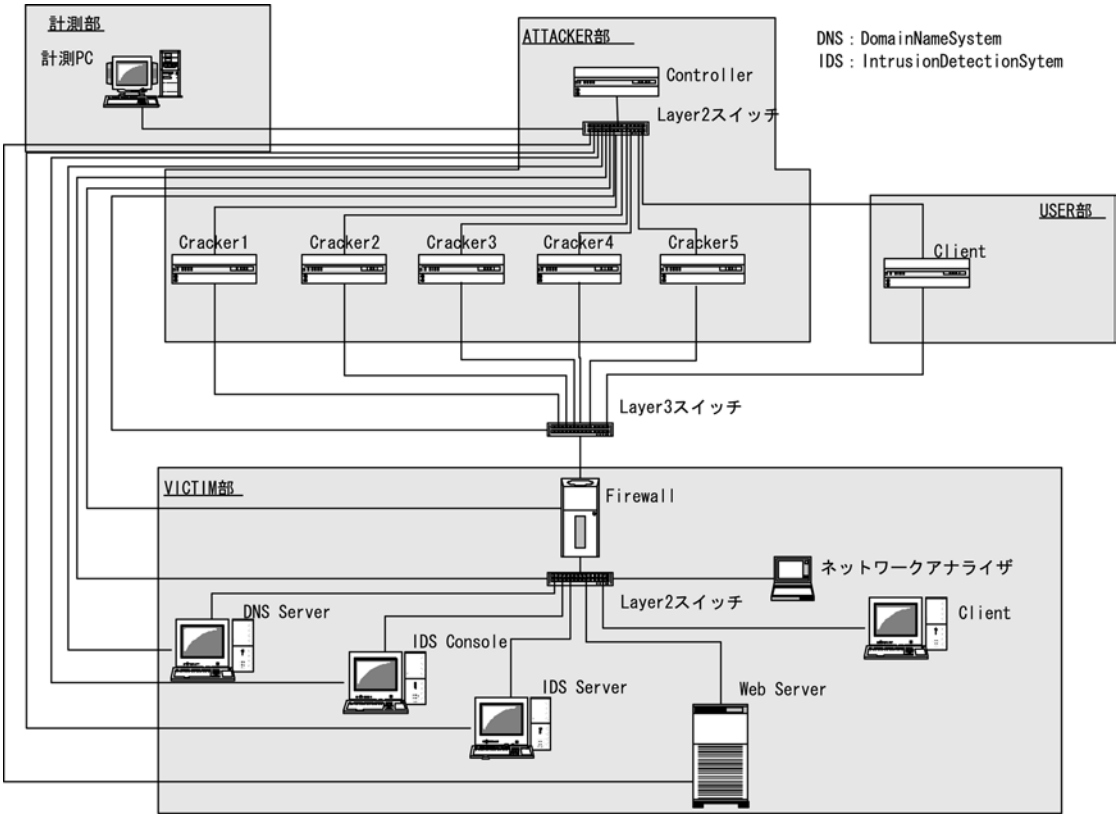

図-1　不正アクセス再現実験装置の概要

■セキュリティ管理の実践的研究

効果的なセキュリティ対策を行うには，暗号やファイアウォールなどといった個別技術面での対策ばかりでなく，運用管理面での対策が必要となる．セキュリティにおいては，たとえ個別的に強化されたとしても，最も脆弱な部分がインシデントの原因となるため，網羅的でバランスの取れた対策が必要である．また日常いかなる運用管理を行っているか，ということはセキュリティレベルを大きく左右する．政府機関を念頭においてこれらのセキュリティ管理の運用管理をいかにすれば実効あるものにできるのかを実践的方法論に基づいて進めている．

通信総合研究所非常時通信グループの取り組み

独立行政法人通信総合研究所情報通信部門非常時通信グループ（以下，非常時通信グループ）では，「インターネット」と「危機管理」を2大研究テーマとして研究活動を進めており，ネットワークセキュリティに対しても，「インターネットの危機管理」という視点に基づいて取り組んでいる．

最近では，多くの組織が，不正アクセスを防止する目的で，組織内のネットワークと外部のネットワークとの間にファイアウォールを設置してアクセス制限をしたり，メールサーバやWebプロキシサーバでウィルスチェックを自動的に行うようになってきている．これは良い傾向であるが，あくまで，不正アクセスを抑止することしかできないため，実際に不正アクセスが発生した場合の対応や，復旧方法などを念頭に置いた対策が重要である．しかし，危機管理の「準備」「対応」「復旧」「防止」という4つの視点から言えば，現状では不正アクセスに対する備えを「準備」してはいても，発生時の「対応」や被害が生じた場合の「復旧」を考えた対策を立て，「防止」を目的とした普及啓蒙を行っている組織はほとんどない．

このような状況を打破するためには，情報通信システムの危機管理の重要性を強く意識した研究者集団が，日頃から最新の情報の蓄積と分析を行い，万が一の事態に際しては，さまざまな対応策の中から最適なものをすばやく選び出し，平常時には教育・普及啓蒙活動，基礎理論の研究などをしっかり行う必要がある．

そこで，通信総合研究所では平成12年度公共事業等予備費などを得て，非常時通信グループが中心となって「情報通信危機管理研究施設」の整備に着手し，「脆弱性情報データベース」と「不正アクセス再現実験装置」を設置して研究開発を開始した（**図-1**）．このうち前者は，近年の不正アクセスの主要な手段として利用される情報通信システムの脆弱性に関する情報を蓄積・分析するためのデータベースであり，後者は，DDoS攻撃（Distributed Denial of Service，分散サービス不能攻撃）などに代表される大規模な不正アクセス手法を模擬実験することで，実際の攻撃の影響や対策につい

て，分析・実験する装置である.

■脆弱性情報データベース

過去の不正アクセスは，アカウントの不正取得によるシステムへの不正侵入が主であった．それに対し，近年の不正アクセスでは，システムの脆弱性を利用した権限の不正取得によるシステムの乗っ取りやサービスの不能化が行われている．各種のシステムに対して，さまざまな脆弱性が日々発見されており，それを利用した不正アクセス手法が次々に編み出されている．そのため，不正アクセスを防止するためには，いち早くシステムの脆弱性に関する情報を把握し，脆弱性を取り除くことが重要である.

しかし，脆弱性に関する情報を十分に収集し，対策を採るためにはいくつかの困難がある.

・全情報を網羅することが困難

脆弱性に関する情報は，CERT/CCによるアドバイザリや，OSやソフトウェアベンダが提供するセキュリティ情報などによって提供されているが，1つの情報ソースだけですべてのセキュリティ対策をカバーできるわけではなく，十分なセキュリティ対策を施すためには多くの情報ソースから情報を収集する必要があり，非常に困難である.

・非公開の情報の多さと重要性

これらの情報には，その性格上，非公開とされている情報が多く，対策手法を検討するには不十分である．特に，脆弱性を引き起こしている部分のソースコードや実際にその脆弱性を利用する攻撃手法などはクラッカーの間では流通しても，セキュリティ情報としては流通しないため，対策を採る側が情報量の点で不利を強いられている.

・情報のローカライズ

多くの情報は英語で記述されており，日本語で記述されたものが少ないために，日本人が緊急対応を行う場合には，障害になる．これは，日本に限らず，非英語圏のすべての国に当てはまることである.

こういった問題に対し，非常時通信グループでは脆弱性に関する情報を蓄積・整理し，新規の攻撃が発生した場合，既知の脆弱性データに類似情報がないかを検索可能とする「脆弱性情報データベース」を研究開発している.

脆弱性情報データベースでは，以下を実施し，脆弱性に関する情報を整理して蓄積する.

・脆弱性データごとにさまざまな情報ソースから情報を登録．脆弱性データベースから一度に多くのセキュリティ情報を取得可能.
・脆弱性を引き起こしているソースコードや攻撃手法および攻撃ソフトウェアのソースコードなども同時に登録.
・情報は，日本語にローカライズする.

加えて，項目ごとのキーワードによる検索や全文検索により，蓄積されている情報から必要となる既知の脆弱性に関する情報を，すばやく検索できる.

また，データの入出力をXML化することで，他のアプリケーションとの連携や独自の検索手法の提供，組織間での情報共有を可能としている.

■不正アクセス再現実験装置

DDoS攻撃に代表される多数の踏み台ホストを利用した大規模な攻撃は，その対策の困難さから，大きな脅威となっている．そのため，こういった攻撃の仕組みや影響，対策の効果などを十分に計り，根本的な対策を見出すことは非常に重要な研究課題となっている.
そこで，非常時通信グループでは閉じたネットワーク実験環境において実際にDDoS攻撃などを実行し，その仕組みや影響の分析，対策の研究を行うための基盤として，「不正アクセス再現実験装置」を研究開発した（**図-2**）.

不正アクセス再現実験装置は，模擬攻撃部，ネットワーク部，攻撃対象部，計測・管理部から構成されている.

・模擬攻撃部

DDoS攻撃などの多数の踏み台ホストを介した大規模な攻撃を模擬実行するために，模擬攻撃部は100台のPCによって構成されている．普通のPCで構成されているため，一般に利用されている攻撃ツールをそのまま利用することが可能であり，新たな攻撃ツールの追加も容易である．攻撃ツールの管理は，OS非依存とするためJavaで記述されている専用のコントロールデーモンによって行われる．コントロールデーモンは，管理部から攻撃のスケジュールなどを読み込み，設定し，その

図-2　不正アクセス再現実験装置

実行を管理する．模擬攻撃部のネットワーク構成は，VLANを利用して柔軟に組み替えられるように設計されており，さまざまな形態の攻撃を模擬実行することが可能である．

・ネットワーク部

模擬攻撃部と攻撃対象部の間は，ネットワーク部によって接続されている．ネットワーク部には，帯域制御可能なVLAN対応のLayer 3スイッチが導入されており，実際の攻撃時に想定される攻撃者と攻撃対象の間のさまざまなネットワーク状態を模倣することが可能である．

・攻撃対象部

攻撃対象部は，一般的なサイトを模倣するように設計されており，サイトの外部，公開サーバ領域（DMZ），内部の3つの領域から構成されている．それぞれに，ファイアウォールやIDSとSMTP・DNS・Webサーバが配され，一般的なサイトに攻撃が行われた場合の影響を分析することを可能とする．攻撃対象部の状態は，計測部に基本的にはSNMPで送られる．

・管理部

模擬攻撃部のアドレス・ネットワーク構成，攻撃のスケジュール，攻撃対象までのネットワーク帯域，計測項目などはすべて管理部で集中管理され，管理部から設定を行うことができるよう設計されている．100台に及ぶ模擬攻撃部のPCとそれにかかわるネットワーク構成などを集中管理，自動設定できるようにすることで，円滑に実験を行うことが可能となっている．

・計測部

データ収集は，SNMPを基本として行い，SNMP MIBだけで対応できない部分は専用agentによって収集している．収集したデータはリアルタイムに表示し，実験成否の判断を即座に行えるようにした．また，同時に攻撃パケットをキャプチャし，MACアドレスとIPアドレスの対応表示を行うことで，IPスプーフィングの状況をリアルタイムで観測できるようになっている．収集したデータは実験終了時にファイルに保存することで，実験後に詳細な解析を行うことを可能としている．

■展望

非常時通信グループの，「インターネットの危機管理」への取り組みはその端緒についたところである．インターネットの現状を鑑みるに研究は速やかに進める必要があり，以下の課題に取り組んでいる．

- 脆弱性情報データベースのコンテンツ充実
- 不正アクセス再現実験装置によるソフトウェア・セキュリティ機器の耐久性測定方法の確立
- 脆弱性情報データベースと不正アクセス再現実験装置の連携機構の整備
- 不正アクセス検出環境の高性能化と実際の広域ネットワークでの評価
- タイガーチーム養成を含む，教育・啓蒙施設としての機能の整備
- 公共的研究実験基盤としての意義の明確化

今後の展望

以上のように，我が国政府においては，内閣官房情報セキュリティ対策推進室を中心とした政府機関の情報セキュリティ対策の推進活動と，筆者らの所属する産業技術総合研究所・通信総合研究所におけるセキュリティに関する研究など，ネットワークセキュリティ確立に向けた取り組みが行われている．

これらの取り組みが，国内における他のさまざまな取り組みと相互に結びつき，我が国全体でのネットワークセキュリティ確立のための活動となっていくことが重要である．

参考文献

1）「情報セキュリティ関係省庁局長等会議の設置について」（平成11年9月17日内閣官房長官決裁）．
http://www.kantei.go.jp/jp/it/security/taisaku/0917kyokutyou.html

2）「ハッカー対策等の基盤整備に係る行動計画」（平成12年1月21日情報セキュリティ関係省庁局長等会議決定）．
http://www.kantei.go.jp/jp/it/security/taisaku/0121actionplan.html

3）「情報セキュリティ対策推進会議の設置について」（平成12年2月29日高度情報通信社会推進本部長決定）．
http://www.kantei.go.jp/jp/it/security/suisinkaigi/0229suisinkaigi.html

4）1 高度情報通信社会推進本部の動き，本編 第3章情報通信政策の動向，第1節 高度情報通信社会実現に向けた政府の主な取組，平成12年度通信白書，総務省． http://www.soumu.go.jp/joho_tsusin/policyreports/japanese/papers/h12/html/C3110000.html

5）「情報セキュリティ部会の設置について」（平成12年2月29日高度情報通信社会推進本部長決定）．
http://www.kantei.go.jp/jp/it/security/bukai/0229bukai.html

6）「情報セキュリティ対策推進室の設置に関する規則」（平成12年2月29日内閣総理大臣決定）．
http://www.kantei.go.jp/jp/it/security/suisinsitu/0229kisoku.html

7）「情報通信技術（IT）戦略本部の設置について」（平成12年7月7日閣議決定）． http://www.kantei.go.jp/jp/it/000707/setti/1honbusetti.html

8）「IT戦略会議について」（平成12年7月7日情報通信技術（IT）戦略本部長決定）． http://www.kantei.go.jp/jp/it/000707/setti/2kaigisetti.html

9）「高度情報通信ネットワーク社会形成基本法」
http://www.kantei.go.jp/jp/it/kihonhou/honbun.html

10）「情報セキュリティ対策推進会議について」（平成13年1月22日高度情報通信ネットワーク社会推進戦略本部決定）．
http://www.kantei.go.jp/jp/it/network/dai1/1siryou04.html

11）「情報セキュリティ専門調査会について」（平成13年1月22日高度情報通信ネットワーク社会推進戦略本部決定）．
http://www.kantei.go.jp/jp/it/network/dai1/1siryou03.html

12）「情報セキュリティポリシーに関するガイドライン」（平成12年7月18日情報セキュリティ対策推進会議決定）．
http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html

13）「重要インフラのサイバーテロ対策に係る特別行動計画」（平成12年12月15日情報セキュリティ対策推進会議）．
http://www.kantei.go.jp/jp/it/security/taisaku/2000_1215/1215actionplan.html

14）「サイバーテロ対策に係る官民の連絡・連携体制について」（平成13年10月10日）．
http://www.kantei.go.jp/jp/it/security/suisinkaigi/dai4/terotaisaku.html

15）「電子政府の情報セキュリティ確保のためのアクションプラン」（平成13年10月10日情報セキュリティ対策推進会議）．
http://www.kantei.go.jp/jp/it/security/suisinkaigi/dai4/actionplan.html

16）情報技術セキュリティ評価機関認定プログラム（JITAP）．
http://www.tech.nite.go.jp/its/its-index.htm

17）暗号技術評価委員会（CRYPTREC），
http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index.html
http://www.ipa.go.jp/security/enc/CRYPTREC/index.html

（平成13年11月12日受付）