連載企画　新連載

行政における情報セキュリティ対策と人材育成及び活用①

情報セキュリティ対策の必要性

(ISC)² Japan
代表　衣川　俊章（CISSP）

1. はじめに

今回から5回にわたり、地方公共団体を含む行政機関における情報セキュリティ対策についてお話しします。

第1回目では、行政における情報セキュリティ対策の必要性、その中でも、「人」の重要性を説明し、情報セキュリティ対策先進国である米国行政での人材育成・活用の取り組みについて紹介します。第2回目以降は、「人」に焦点を当てて、人材育成及び活用・評価のポイントや、人材に必要と思われる知識、それらの詳細説明という形で進めて行きたいと考えています。

2. なぜ、情報セキュリティ対策は必要なのでしょうか。

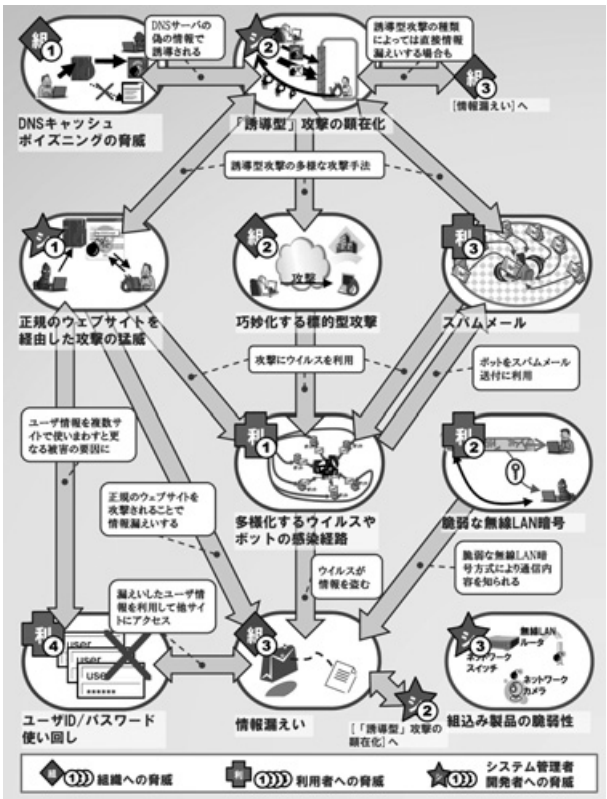
現在、行政機関の基幹業務と呼ばれているものから、市民・企業サービス関連業務にいたるまで、様々な業務においてITシステムが関与していることは疑う余地もありません。このITシステムは、ITに依存する業務の拡大、新規サービス創出の必要性とIT活用や、自治体クラウドなどの新技術などに対応していくために、今後益々、高機能化・複雑化していくことでしょう。

これらのITシステムには、多かれ少なかれ行政機関として保護しなければいけない情報資産が格納されています。またITシステムが止まってしまうことで、日常業務・サービスへの影響も低いものとは言えなくなってきているのではないでしょうか。

情報資産の保護やITシステム常時稼動を可能にするのが、情報セキュリティ対策です。この対策無しでは、行政機関の業務の継続や住民や企業への安心・安全なサービス提供はできません。この重要性を鑑み、情報セキュリティ関連のガイドラインや基準が策定されています。

一方で、情報セキュリティを脅かす脅威は、益々高度化、巧妙化してきています。**図1**の通り、誘導型や標的型攻撃、BOTやウェブアプリの脆弱性を悪用した攻撃を通して、価値のある情報を搾取し、そ

図1　10大脅威　相関図



出典：IPA（独立行政法人 情報処理推進機構）「情報セキュリティ白書 2009 第「 部 10大脅威 攻撃手法の『多様化』が進む」

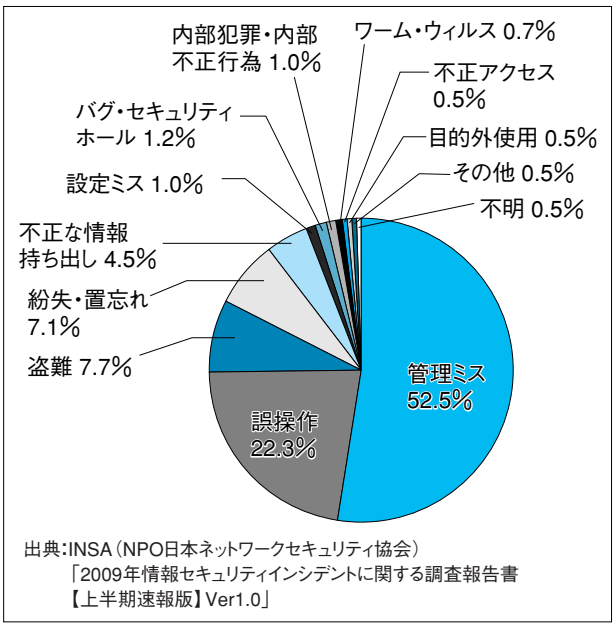
れを経済行為として成立させる攻撃者が多くなってきています。これらの攻撃は、従来のセキュリティ対策だけでは、十分に防ぐことが難しくなってきているのも事実です。

3. 情報セキュリティ対策における「人」の重要性

情報セキュリティ対策を考える上で、当然何かしらの「技術」要素の対策を導入することで解決しようというのは、自然なことです。ただそれだけ十分でしょうか。

情報漏えい事件として届出があったものの中で、誤操作、紛失・置忘れ、内部犯罪など「人」が原因になっている事故の割合が40%を超えています（**図2参照**）。一番多い原因の管理ミスを含めて考えてみると、決して技術要素だけで事故が防げないことが分かります。いくら完璧と思われる技術要素やプロセス（そもそも「完璧」といえるものはないのですが）を導入しても、それを管理、利活用する人間が、ある一定のレベルになっていないと、事故は起こってしまうのです。当然、一定レベルになっていても、「人」がやることですから、事故が起きない保証はありませんが、少なくともそのリスクを軽減することはできますし、今より有効な対策の導入をすることが可能になります。

図2　情報漏えい事件で届出があったものの割合



出典：INSA（NPO日本ネットワークセキュリティ協会）
「2009年情報セキュリティインシデントに関する調査報告書【上半期速報版】Ver1.0」

当然、一定レベルは、組織の規模、業務内容、ITシステムや情報資産との関わり方によって、個々人によって違ってきます。ここでは、どの職員、契約社員やベンダ社員に、どのレベルを求めるかをきちんと決めて、明文化し、それに対しての雇用・研修・評価に対してのポリシーや制度を導入することが最も重要なポイントになります。

2009年、オープンソフトウェア利用促進事業の一環として、独立行政法人・情報処理推進機構（IPA）が行った「自治体における情報システム基盤の現状と方向性の調査」では、各自治体におけるIT情報化組織の存在率が90%に上っている反面、ITに対する担当職員の知識・スキル不足が指摘されており、情報セキュリティへの知見に至っては、推して図るべきではないでしょうか。総務省が行った「地方公共団体　情報化推進調査」では、各自治体のCIO、CIO補佐官の設置は、それぞれ82.1%、62.3%と比較的高い数字になっています。ただ、これらの方々が専任なのは2%未満にとどまっています。また情報化についての研修計画を策定していると回答したのは、わずか3.8%となっています。

結果として、地方自治体の職員の多くは、ベンダから提案される技術仕様や、費用見積りの的確性、妥当性を判断することが難しい状況になってきており、一方で出入りのベンダの人員の知識・スキルレベルを図るすべがないもの事実である、との指摘も

されています。システムの品質や費用について、相互に齟齬なく的確に把握できるための仕組みや共通言語の確立と共に、前述した「人」の質を担保出来る仕組みの導入が必要となってきているのではないでしょうか。特に、今後クラウドやSaaSなどの活用が活発になっていくと、サービス提供者側のセキュリティレベルを確認し、保証する仕組みの導入は必須になっていくと考えます。

4. 米国政府での人材育成・活用の取組み

オバマ大統領は、大統領として初めて、サイバーセキュリティの重要性と情報資産保護が米国にとって最重要課題であると宣言しました。その結果、様々な取組み、法案が成立、または審議されています。当然、その中にはセキュリティ人材に関連したものがいくつか存在しています。

一番顕著なものとして、Cyber Security Act of 2010が上げられます。この法案は現在審議中のものですが、米国政府の情報セキュリティ人材に対しての姿勢と真剣さが十分に把握できるものになっています。

・政府機関の情報セキュリティ人材確保のための奨学金制度の導入
・情報セキュリティ技術コンテスト開催
・政府機関の情報セキュリティ人材の採用、トレーニング計画の提出とその年次レビューの提出

採用、昇進に関しては、職種毎に必要なスキル・知識レベルの特定、またその証明となる資格保有が義務付けられる形になっています。これらは、政府職員だけではなく、契約事業者にも適用されることになっています。

本法案は、まだ実施されていませんが、既に実施されている例として米国・国防省（DoD）のDirective 8570があります。**図3**では、DoDの情報セキュリティの業務に携わる為に、必要なスキルとそれを証明する為の取得必須資格名が記載されています。

このように米国政府では、政府機関の情報資産保護を最重要課題と位置づける中で、人材育成や評価の取組みが既に施行されています。日本においても、国としての取組みに期待すると共に、各行政機関としても、安心・安全な行政サービスの提供を継続していく上で、出来ることから始めていっていただきたいものです。特に人材育成・評価は、成果が出るまで時間のかかる施策ですので、早めの対策をお勧めしたいです。

次回は、人材育成及び活用・評価のポイント、と行政機関の情報セキュリティ人材に必要と思われる知識について、ご紹介します。

図3　DoDの情報セキュリティ業務に必要なスキルおよび取得必須資格

Table AP3.T1. DoD Approved Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+ Network+ SSCP	GSEC Security+ SCNP SSCP	CISA CISSP (or Associate) GSE SCNA
IAM Level I	**IAM Level II**	**IAM Level III**
GISF GSLC Security+	GSLC CISM CISSP (or Associate)	GSLC CISM CISSP (or Associate)

CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CND-SP Manager
GCIA	SSCP	GCIH CSIH	CISA GSNA	CISSP-ISSMP CISM

IASAE I	IASAE II	IASAE III
CISSP (or Associate)	CISSP (or Associate)	ISSEP ISSAP