NISC NEWS

第１７号（２００８年１月２３日発行）
内閣官房情報セキュリティセンター
National Information Security Center (NISC)

★目次

１．情報セキュリティ施策紹介

【 2月2日は情報セキュリティの日 】

今年も2月2日が近づいてきました。2006年のこの日に、内閣官房長官が議長を務める情報セキュリティ政策会議において、我が国の情報セキュリティ問題全般についての中期戦略である「第1次情報セキュリティ基本計画（以下「基本計画」）」が決定されたことにちなみ、毎年2月2日を「情報セキュリティの日」と定めました。

この日の前後の期間において、情報セキュリティの向上への気運を全国的に波及・浸透させるとともに、広く官民における意識と理解を深めることを目的に、政府機関はもとより、広く他の関係機関、団体の協力の下に、国民各層の幅広い参加を得た取組みを集中的に実施することとしています。これにあたっては、内閣官房が警察庁、総務省、文部科学省及び経済産業省の協力を得て推進していきます。

実施概要

（1）「情報セキュリティの日」功労者表彰の実施

情報セキュリティへの取組みに関し、貢献のあった個人又は団体を顕彰するものです。これにより、情報セキュリティに関する優れた取組みを広く普及することを目的としています。

表彰の対象としては、情報セキュリティに関し、

・地方公共団体、企業等の組織における情報セキュリティ対策への先進的な取組み
・情報セキュリティ対策に資する技術等の研究・開発
・情報セキュリティ対策に関する普及啓発、人材育成への貢献

以上3点のいずれかについて特に顕著な功績又は功労があり、省庁横断的な視点から情報セキュリティ政策会議議長が顕彰することがふさわしい個人又は団体としています。その選定にあたっては、民間有識者・学識経験者等からなる「情報セキュリティ啓発推進委員会」において被表彰者の候補案を作成し、政策会議議長に上申することになっています。

本年度は、2月上旬に開催予定の第16回情報セキュリティ政策会議に引き続いて、総理大臣官邸内で表彰等の記念式典を実施し、議長から功労者に表彰状が授与される予定です。

（2）関連行事の開催

情報セキュリティの日の目的にある、「情報セキュリティの向上への気運を全国的に波及・浸透させ、広く官民における意識と理解を深める」ためには、様々な場所で、様々な主催者が、様々な対象に、情報セキュリティ対策の重要性を訴えていくことが必要不可欠です。そこで、2月2日の前後の期間（本年は1月26日（土）から3月2日（日）までの間としています。）に、政府機関はもとより、広く他の関係機関、団体にもご協力いただき、国民各層の幅広い参加を得て、セミナー、講演会、特設ホームページ等などの関連行事を集中的に開催することとしています。

NISCにおいては、情報セキュリティ政策会議による後援や、職員の講師派遣等により、これらの行事を積極的に支援します。関連行事は、全47都道府県で昨年度の300余件を大幅に上回る586件（1月23日現在）が開催される予定になっています。行事一覧はNISCのホームページに掲載されますので、もし読者の皆様のお近くで、ご興味を引く行事がございましたら、是非ご参加いただきたいと思います。

2. 補佐官ノート「情報セキュリティにおける次の一手とは」

【 なぜ管理者はプログラムを書くのか 】

このメールマガジンの読者の方々に、どの程度の割合でプログラミング経験やコンピュータ管理経験があるのかは全く予想がつかないが、今回は情報システムの管理について述べたい。特に、技術者でも無いのに、情報システムの管理運用部門に配置されてしまった方には、是非とも読んでもらいたい。

今や、どんな業種であっても、情報システムが業務の中核を支える基盤機能を提供するようになっている。情報システムは、手間いらずのものではない。日々、何らかの管理業務が発生してしまう、結構手間のかかる奴なのだ。もちろん、10年、20年前から比べれば、最近の情報システムの管理作業は見通しの良い作業に改善されてきているが、それでも手間がかかることには違いない。実際、数多くの方々が、情報システムの運用管理業務に携わる技術者として働いておられる。

運用管理業務に携わる技術者には、私の目からみると三つのタイプに分かれる。一つが、運用管理マニュアルに書かれているままに作業をする技術者。二つめが、運用管理で徹底して書類作成に取り組んだり、システム台帳やデータベースを構築したりする情報管理型技術者。そして最後が、運用管理業務のためにプログラムを作ったり、管理用の小さなプログラムを開発したりする開発型管理者である。この三つのタイプは、経験度に応じて成長する段階と、私は考えている。

最初は誰もが管理業務に右往左往しがちである。そのため、マニュアルどおりの作業をしようとする。これは初心者と言って良いレベル。管理業務に慣れてくると、一つ一つの対応で時間短縮ができるようになり、その効率の良さを極める管理者も出てくる。しかし、この段階ではまだまだ素人のレベルである。というのも単に段取りだけでは作業効率を向上させる限界が見えてきてしまうのだ。各管理者の作業最適化では、そんなに大きな効率化は達成できないのが普通だ。

このような状況で考え抜いて次のステップに進化する管理者達が出てくる。それが、情報管理型技術者である。情報システム管理者が、管理業務の全体像が理解できるようになると、別のアプローチから効率を上げる可能性に必ず気がつく。それが情報管理の徹底による生産性向上だ。例えば、管理業務の多くに、色々な情報システム運用状況を把握して報告するというのがある。運用状況調査をする度に毎回ログを解析して、指定されたフォーマットに情報を書き入れるという作業だ。

この作業を毎回、毎回ゼロから始めるというやり方もあるだろう。しかし、この手の運用状況調査では、まずどんなシステムがあるかを把握したシステム台帳を作り、さらにログや運用情報を集中的に管理するようにすれば、運用状況報告も簡単に作ることができるようになる。あるいは、システムにおけるハードウェアパーツの台帳と、交換年月日を記録しておけば、次に交換するべき状況も予測できるという利点もある。情報の一元管理を徹底して、事務処理量を減らそうとするようになると、運用管理者も1.0から2.0にバージョンアップされて進化したのだなと感じるものだ。

ところが、管理者の発展もこれが終わりではない。実は、この先にも発展段階がある。それが、開発型管理者である。つまり、自分が行っている作業をできる限りプログラム化して活用しようとする運用管理者である。作るプログラムといっても、スクリプト言語を使った簡単なものから、ちょっとした大きさのプログラムまで千差万別である。しかし、情報管理型技術者とは本質的にレベルが違う。プログラム化された作業とは、自分自身が行っている管理作業を「プログラム」という形で文書化し、さらに再利用可能な形で提供しているのだ。このため、事後の管理作業検証や、機能追加なども明確な形で行うことができる。さらに、プログラム化されていないところが、明確に運用管理者が作業して、判断しなければならないところを示している。

このような開発型管理者は、何を考えてプログラムを作っているのだろうか。多くの場合、3回以上同じ作業をする可能性があるならば、それをプログラムしておこうと思うのは、技術を分かっている人間のすることである、と、私は信じている。そして、一見怠け者のように見えるが、このようなプログラムで書いておこうと思う技術者は、とても良い能力を持った技術者であると言える。そして、その管理者が異動してしまっても、プログラムを見ると、具体的な作業が記述されていることにもなり、引き継ぎでの記憶喪失を減らす効果もあるのだ。

さて、皆さんの組織での情報システム管理者はどうだろうか。どんな管理手法を用いているかを管理者から聞き出すことによって、運用管理者のレベルを推定できると思う。一度、運用管理者に聞いてみて欲しい。「自分の管理作業でプログラム作ったり、スクリプトを書いたりしていますか？」と。「はい」という答えが沢山返ってくるようなら、なかなか大した管理体制を持っていると、私は思っている。

（山口 英 内閣官房情報セキュリティ補佐官）

3. 誰でもわかる情報セキュリティ用語

【 SHA-1 （シャー ワン） 】

SHA-1 は、情報セキュリティの分野では、主にデータが改ざんされていないことを確認するために用いられる、ハッシュ関数の一つです。SHA は Secure Hash Algorithm の略で、米国政府標準のハッシュ関数として採用されています。SHA-1 は SHA の関数群の中で最も良く利用されている関数であり、米国政府のみならず我が国の政府の情報システムのさまざまなアプリケーションやプロトコルにも採用されています。

ハッシュ関数は、任意の長さのデータから固定長の文字列（ハッシュ値）を作り出す一方向関数で、「メッセージダイジェスト」や「要約関数」とも呼ばれます。SHA-1 の場合には、160 ビットのハッシュ値を生成します。一方向関数とは、与えられたデータから容易にハッシュ値を求められても、そのハッシュ値から元のデータを再現することが非常に困難な関数のことです。また、異なるデータが同じハッシュ値を持つことを「衝突」と呼びますが、ハッシュ関数には、同じハッシュ値を持つ別のデータを作り出すのが容易ではないこと（衝突耐性）も求められます。これらの特性を用いることで、通信回線を通じてデータを送受信する際に、経路の両端でデータのハッシュ値を求めて両者を比較すれば、データが通信途中で改ざんされていないかを調べることができます。

ところが、近年 SHA-1 の危殆化の問題が議論されるようになってきました。「危殆化」とは危うくなるという意味で、SHA-1 の衝突耐性が破られる危険性が高まっているということを意味しています。理論的には、どのような暗号でも無限の時間があれば解読が可能です。しかし、高速な計算機を用いても解読するために莫大な時間や費用がかかるのならば、実用上は「破れないのと等価」なことを前提とし、その安全性が保証されています。しかし、暗号研究の進展により、SHA-1 も特定の条件下では、衝突耐性が脆弱であることが報告されました。

それが直ちに SHA-1 を用いているアプリケーションが、現実的な時間で突破されてしまうことを意味する訳ではありません。仮に同じハッシュ値を持つ別のデータを生成できたとしても、それが犯罪者の望む形にデータを偽造できることとは別です。また、現実のシステムでは、SHA-1 は他の多くの暗号や認証の機能と相互に連携して、アプリケーションのセキュリティを担保しています。しかし、将来的な計算能力や更なる攻撃手法の進化に備えておく必要はあります。SHA-1 が容易に突破される事案が出始めてから対策を練っても手遅れだからです。

すでに米国では、2010 年までに SHA-1 の運用を終了し、SHA-2（SHA-224、SHA-256、SHA-384、SHA-512 の総称）に移行する計画を公表しています。加えて、SHA-1 を用いている既存のアプリケーションをどう新しい規格に移行させていくかなどが、現在、世界的に議論されています。

4. NISCOLUMN（ニスコラム）

【 文系出身者は情報セキュリティの夢を見るか？ 】

新年明けましておめでとうございます。

新しい年を迎え、今年新たな仕事や業務に取り組まれる予定の方や新しく社会人になられる学生の方も多いことと思います。

さて、胴回りのお肉が少々気になり始めた筆者としては、既に大学で勉強していた時間より社会に出てからの時間の方が遙かに長くなりつつありますが、この仕事をやっていまして人とお会いしたとき、学生時代に何を勉強していたのかを尋ねられた際に、大学は文系でした、とお答えすると驚かれることがしばしばあります。これはむしろこの業界の方々とお会いした時より、あまりシステムや情報セキュリティと縁の無い方とお話している場合が多いように感じられます。一般の人々には、情報セキュリティ＝とっつきにくい＆難しそう＝理系出身者が従事する仕事、という推測が成り立つのかも知れません。

ところが、情報セキュリティの業界で活躍されている方には実に色々な畑のご出身の方がいらっしゃいます。ＯＳ やネットワーク系のエンジニアの方やコードをバリバリ書くプログラマ等の技術系ご出身の方ばかりではなく、経営コンサルタントの方から弁護士や会計士の先生まで。昨今の社会的な要請を受け、いかに多様な人材が要求され、急速に立ち上がってきた分野かがわかります。その中には、必ずしも大学では情報工学等を専門に学んでこなかった人々も相当数いらっしゃる訳です。筆者も上述の通り、大学時代は完全な文系で社会人として初めて配属された部署は情報セキュリティとは何の関係もない仕事でしたが、何故か様々な紆余曲折を経て、現在この業務にどっぷりつかってしまった次第です。

このように情報セキュリティというのは、非常に幅広い領域だと改めて感じます。そこで必要とされるのは単純に技術のみとは言えません。勿論、技術を正確に理解しておくことは極めて重要な要素ですが、それだけではなく、技術の使い方やそれを運用する人とのバランス、それらのフレームワークを考えていくことも重要な課題です。また、情報セキュリティは、広い視野で社会全体を相手としていく仕事でもあります。情報化が極度に進んだ現代では、情報やコンピュータを利用するのは、一部の専門家や社会的な訓練を受けたビジネスマンだけとは限りません。例えば、インフルエンザを予防するために手洗いとうがいを欠かさないことが常識になっているのと同様に、子供やご年配の方々にも情報セキュリティの必要性やその対策をすることが常識になるよう、正しく分かりやすい形で広く啓発していく必要があります。その意味で、プレゼンテーションやコミュニケーション等のヒューマン的なスキルも重要になってくるでしょう。こうした複雑化したニーズが、情報セキュリティを携わる人材を理系・文系という分け方で一概にくくることを、難しくしているのかも知れません。

さらに情報技術全般においてですが、昨今ダブルメジャー的な人材の活躍の場も増えています。法律に詳しいセキュリティ屋さん、経営学を学んだセキュリティ屋さん、社会学や教育学を修めたセキュリティ屋さん、そんな様々な分野から様々な知見をもった人達が集まって情報セキュリティという困難な問題を解決していければいいですね。

（T）

【編集後記】

日頃から、情報セキュリティ関連施策やNISCの活動にご関心を持っていただき有難うございます。

本年１月16日、情報セキュリティ政策会議の下に設置された、基本計画検討委員会の第１回会合が開催されました。本委員会の任務は、平成21年度以降の情報セキュリティ政策の中長期的な戦略である「第２次情報セキュリティ基本計画」（仮称）の策定に係る事項について調査検討を行うことです。NISC においては、本委員会での検討の参考となるよう、国民の皆様から広く情報セキュリティ政策に関するご意見を伺うこととしており、ご要望や課題などを募集しています。下記ページの要綱にて、ご応募いただければ幸いです。

http://www.nisc.go.jp/active/kihon/keikaku-iken.html

＜バックナンバー・配信先変更・配信中止＞

本メールマガジンにおけるバックナンバーの取得及び配信先の変更、配信の中止等は下記の URL から可能です。

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

＜御意見、御感想＞

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