文部科学省

A) 情報セキュリティ最高責任者からのメッセージ

文部科学省（以下「当省」という。）は、教育の振興及び生涯学習の推進を中核とした豊かな人間性を備えた創造的な人材の育成、学術、スポーツ及び文化の振興並びに科学技術の総合的な振興を図ることを任務としています。

近年、我が国では、情報通信技術の急速な進歩に伴い、国民生活が飛躍的に向上する一方で、情報セキュリティの脅威についても多様化・高度化・複雑化し、サイバー攻撃の手口もより巧妙化してきております。平成 24 年度においては、中央省庁や裁判所等を標的としたサイバー攻撃により、ウェブサイトの書き換えや情報漏洩等の被害が相次ぎ発生し、社会問題となったのは記憶に新しいところです。

また、昨年 9 月には、外局である文化庁のシステムがサイバー攻撃を受け、ウェブサイトの一部改ざんが発生し、一時当該サイトを閉鎖する事態となりました。このことによって、ご利用者の方々に、大変なご迷惑やご心配をお掛けしましたことを心よりお詫び申し上げます。

当省では、かねてから文部科学省情報セキュリティポリシー（以下「ポリシー」という）を制定し、その運用を通じて情報セキュリティ対策を徹底してきたところでありますが、このことを受けて、以下の点を中心に情報セキュリティ対策のより一層の強化に取り組んでまいりました。

(1) 情報セキュリティ事案に対応する専門チーム（CSIRT）整備による体制強化
(2) 省内職員向けの情報提供及び研修による情報セキュリティの普及啓発
(3) 調達ガイドラインの策定等による情報セキュリティ対策の充実・強化
(4) IT-BCP の整備による情報システム危機管理の強化

本報告書は、これらのことを踏まえ、平成 24 年度に実施した情報セキュリティ対策の取組、監査結果等についてまとめたものです。

情報セキュリティ対策は政府機関にとって重要な課題となっており、今後の情報技術の発達や環境の変化により、新たな情報セキュリティ上の脅威が出現してくることも想定されます。当省としてはそれらに適切に対処し、引き続き、情報セキュリティの維持・向上に努めてまいります。

平成 25 年 6 月 11 日
情報セキュリティ最高責任者
（文部科学省大臣官房長）
前川　喜平

B) 平成 24 年度の総括

ア）平成 24 年度の評価

平成 24 年度は前年度までの取り組みを継承し、「省内 CSIRT の整備等管理体制の拡充」、「関連規程の整備と周知徹底」、「各種技術的対策の実装」等を行うとともに、当省における情報セキュリティ対策の水準を把握し、今後の課題を明らかにするために「自己点検」、「情報セキュリティ監査」を行いました。

自己点検、情報セキュリティ監査の結果、当省においては一定の情報セキュリティレベルを確保できていると思われます。それと同時に、更なる向上のための課題を明らかにすることができました。

また、情報セキュリティ維持に関する訓練として標的型メール攻撃訓練を実施し、標的型メール攻撃に対する職員の意識啓発に一定の効果を上げることができました。

一方で、平成 24 年 9 月、文化庁のウェブサイトが改ざんされるというセキュリティ事案が発生しました。この事案では「国指定文化財等データベース」を停止するに至りました。また、同時期に、当省所管の独立行政法人、国立大学法人等でもハッカー集団によるサイバー攻撃やウイルス感染による情報流出などが発生しました。

当省のみならず政府機関全体へのサイバー攻撃が頻発していることからも、サイバー攻撃とその兆候を見逃さず、すばやく対応する必要があり、そのためには CSIRT を通じて NISC や他府省と問題意識を共有し、緊密な情報連携体制を実現することが重要課題であると認識します。

イ）平成 25 年度の目標

平成 25 年度においても引き続き情報セキュリティ対策に係る自己点検、情報セキュリティ監査等を実施し、情報セキュリティ対策の評価と見直しを行うとともに、平成 25 年度における重点的に取り組む事項を以下のとおり設定します。

①情報セキュリティに関する普及啓発

・最近の手口も考慮した標的型メール訓練の継続的な実施及び標的型メールへの対応に係る教育の充実

・政府全体で推進することとされているリスク評価の取組及び継続的な教育を通じた情報の格付及び取扱制限の理解促進

・情報セキュリティの障害・事故等を踏まえた情報システム管理者向けの教育の見直し

②情報セキュリティに関する自己点検

・自己点検の円滑な実施のための対策立案と実行

・自己点検結果を改善活動につなぐための仕組みの確立

③情報セキュリティ監査

・情報セキュリティの障害・事故等を踏まえた監査内容の見直し

C) 情報セキュリティ対策の実施状況

ア）省庁対策基準に関する自己点検

①把握率

当省における全報告対象者のうち、実際に自己点検結果を報告した者の割合が把握率です。平成 24 年度の把握率は 100%でした。過去 2 年間、報告対象者が増加している中で、平成 23 年度に引き続き、徹底した状況把握ができました。

②実施率

各点検項目について、「情報セキュリティ対策が実施できている」と自己評価した割合が実施率です。平成 24 年度における主体（※）別の実施率は、主体により若干の差はありますが、いずれも高い水準（95%以上）でした。

（※）ここでいう主体とは、情報セキュリティ管理体制上の役割です。

責任者等：　統括情報セキュリティ責任者、情報セキュリティ責任者、課室情報セキュリティ責任者等

システム担当：　情報システム責任者、情報システム管理者

行政事務従事者：全職員（行政事務従事者）

イ）情報システムごとの状況

①内容及び手法

統一管理基準及び統一技術基準の遵守事項についての具体的な対策実施状況を確認するため、NISC が作成及び配布する調査票に基づき、公開ウェブ、電子メール、ドメイン、DNS、ネットワーク等に対して行いました。調査結果は、統一管理基準及び統一技術基準における各遵守事項の実施率によって評価されます。

②情報システムの対策状況

以下の項目について対策状況を調査し、NISC に報告しました。

・当省が管理する全ての公開ウェブサーバ
・当省が管理する全ての電子メールサーバ
・当省が管理する全てのドメイン
・当省がインターネットに接続して運用しているネットワーク

ウ）監査の状況

①情報セキュリティ監査の概要

情報セキュリティ監査は、当省における情報セキュリティ対策の状況を客観的に評価し、今後取り組むべき課題を明らかにするために実施しました。

②情報セキュリティ監査の内容

・ポリシーの準拠性監査（ポリシーが統一管理基準及び統一技術基準に準拠した内容となっているか）
・情報セキュリティ関係規程の準拠性監査（ポリシー実施手順がポリシーに準拠した内容となっているか）
・運用の準拠性監査（実際の運用がポリシー及び情報セキュリティ関係規程に準拠して

いるか）
・自己点検の適正性監査（自己点検の実施内容が適正か）
・脆弱性診断（個別の情報システムの脆弱性に対する技術的対策が妥当か）
③監査結果の総括
ネットワーク、サーバ、ウェブアプリケーションにおいて発見された脆弱性については、修正プログラムの適用を行い、再診断により正しく対処されていることを確認しました。
ポリシー等関係規程類の準拠性や、運用の準拠性、自己点検の適正性において検出された問題点については、原因を分析し、今後継続して改善への取り組みを行う予定です。

エ）教育・啓発

当省における情報セキュリティ普及啓発のため、以下の各施策に取り組みました。
①平成 25 年 2 月の情報セキュリティ月間に併せて、文部科学省関係機関の情報セキュリティ対策担当者等を対象とした情報セキュリティセミナーを開催し、情報セキュリティ意識の向上に努めました。
②当省が策定した新たな情報セキュリティ関係規程「情報システムに係る調達ガイドライン」の利用を促進するため、各部署のシステム管理者に対し集合研修を企画、実施しました。
③NISC 等から提供される注意喚起情報を省内電子掲示板に掲載するとともに、緊急性の高い情報については全職員向けにメールで発信しました。
④標的型メール攻撃に関する教育・意識啓発のため、「平成 24 年度標的型メール攻撃に対する教育訓練」（NISC 主管）を実施しました。

D）情報セキュリティに関する障害・事故報告

ア）情報セキュリティに関する障害・事故等の把握

文部科学省においては、今年度１件の情報セキュリティに関する事故を把握しています。

イ）公表した障害・事故等の概要、それに対する対応等

◆文化庁・「国指定文化財等データベース」ウェブサイトの改ざん
〇発生日時
平成 24 年 9 月 24 日（月）朝、当該ページが改ざんされていることが発覚しました。
〇概要
文化庁が運営する「国指定文化財等データベース」のウェブサイトがサイバー攻撃により改ざんを受け、トップページが「尖閣諸島（沖縄県）と中国国旗の合成画像」に書き換えられました。
文化庁では、改ざんを発見した直後に当該ウェブサイトの公開を停止し、被害状況の調査、原因究明と再発防止策の検討を開始しました。再発防止策を講じた上で平成 25 年 3 月 28 日にサービスを復旧しました。
〇障害・事故の原因

「国指定文化財等データベース」のプログラムの一部に不備があり、そこに不正なアクセスがなされた結果、トップページが書き換えられました。

〇対応

（暫定措置）

更なる攻撃と被害の拡大を防止するため、事象の発覚直後に委託事業者に連絡し、当該ウェブサイトの公開を停止しました。

これに伴い「国指定文化財等データベース」を休止し、文化財に関する情報を検索する場合は、「文化遺産オンライン（http://bunka.nii.ac.jp/）」を利用するよう、ウェブサイト上でアナウンスしました。

（恒久措置）

今回の事象の再発を防止するため、プログラムの修正を行い、システムの再構築を行いました。

〇再発防止策

情報システム管理者向けの教育について見直しを図るとともに、脆弱性診断を強化して、再発防止に努めます。

E）最高情報セキュリティアドバイザーからのメッセージ

文部科学省では、この報告書に示した情報セキュリティ対策を、計画的に実施してきました。この結果、職員の情報セキュリティに関する意識の維持向上が図られ、省内の情報セキュリティも一定の水準を保っていると考えています。しかし、一方で標的型攻撃に代表されるインシデントが毎日のように報道されており、文部科学省を含む行政機関においても、新たな脅威への対応を含む一層の情報セキュリティ対策が重要な課題となっています。

この報告書本文では触れられていませんが、文部科学省の IT システムが更新され、本年 1 月より順次運用が開始されています。新システムにおいては、職員の利便性向上と情報セキュリティ強化の両面からいくつかの新しい仕組みが導入されています。今後は、これらの仕組みを利用シーンに合わせてきめ細かくチューニングすることにより、業務効率の改善と同時に、情報セキュリティの一層の向上が実現できるものと確信しています。

とはいえ、情報セキュリティ対策には完璧な対策は存在しません。情報セキュリティ確保の根幹は職員一人一人の意識と行動です。情報セキュリティ責任部門だけでなく、職員全員の防衛意識の維持と向上が不可欠です。しかし、現状ではセキュリティに対する職員の意識やスキルにはバラつきがあると判断せざるを得ず、継続した教育・訓練が必要です。また、職員が発注する情報システムについて、そのライフサイクルを通じ、要件定義、設計・開発、運用の各段階において、適切なセキュリティ要件を策定できるスキルを身につけてゆく必要があります。本年度はこのためのガイドラインを作成しましたが、今後はそれらのより広範な活用促進と効果のアセスメントが期待されます。

文部科学省では、本年度の反省を踏まえ、NISC など政府内外の関連部門と密接に連携を取りながら、情報セキュリティに関する各種情報や技術動向を注視しつつ、この報告書に示された計画・施策を着実に推進してまいります。

平成 25 年 6 月 11 日
情報セキュリティアドバイザー
（文部科学省 CIO 補佐官）
岩崎　進