JAEA-Review
2013-038

JAEA-Review

情報セキュリティ教育教材集

Materials for the Information Security Education

矢城 重夫　青木 和久　佐藤 智彦　丹治 和拓

Shigeo YASHIRO, Kazuhisa AOKI, Tomohiko SATO and Kazuhiro TANJI

システム計算科学センター

Center for Computational Science & e-Systems

January 2014

Japan Atomic Energy Agency

日本原子力研究開発機構

本レポートは独立行政法人日本原子力研究開発機構が不定期に発行する成果報告書です。
本レポートの入手並びに著作権利用に関するお問い合わせは、下記あてにお問い合わせ下さい。
なお、本レポートの全文は日本原子力研究開発機構ホームページ（http://www.jaea.go.jp）
より発信されています。

独立行政法人日本原子力研究開発機構　研究技術情報部　研究技術情報課
〒319-1195　茨城県那珂郡東海村白方白根 2 番地 4
電話 029-282-6387, Fax 029-282-5920, E-mail:ird-support@jaea.go.jp

This report is issued irregularly by Japan Atomic Energy Agency.
Inquiries about availability and/or copyright of this report should be addressed to
Intellectual Resources Section, Intellectual Resources Department,
Japan Atomic Energy Agency.
2-4 Shirakata Shirane, Tokai-mura, Naka-gun, Ibaraki-ken 319-1195 Japan
Tel +81-29-282-6387, Fax +81-29-282-5920, E-mail:ird-support@jaea.go.jp

© Japan Atomic Energy Agency, 2014

JAEA-Review 2013-038

情報セキュリティ教育教材集

日本原子力研究開発機構　システム計算科学センター
矢城　重夫、青木　和久、佐藤　智彦、丹治　和拓※

（2013 年 9 月 9 日受理）

業務の IT 化の進展は著しく、IT インフラ（ネットワーク環境や情報システム）は業務推進のライフラインとしてなくてはならないものとなった。一方、IT インフラを取り巻く環境の変化に伴いサイバー攻撃の脅威がグローバル化し、各種情報システムへの不正アクセスやウイルス感染、Web サイトの改ざん等の情報セキュリティインシデントが急増、業務に係わる機微情報の漏えいやシステムの破壊等、情報セキュリティ上のリスクが高まっている。

日本原子力研究開発機構においても情報セキュリティに関する対策は重要課題となっており、システム計算科学センターでは、情報セキュリティ上の脅威から情報資産を守るため、①情報セキュリティ関連規程類の整備、②情報セキュリティ機器の整備・運用、③情報セキュリティ教育の実施、を三位一体として取り組んでいる。

本報告書は、情報セキュリティ対策の取り組みの一つである情報セキュリティ教育について、ｅラーニングにより実施している内容を教材集としてまとめたものである。

原子力科学研究所（駐在）：〒319-1195　茨城県那珂郡東海村白方白根 2-4
※ 技術開発協力員

JAEA-Review 2013-038

Materials for the Information Security Education

Shigeo YASHIRO, Kazuhisa AOKI, Tomohiko SATO and Kazuhiro TANJI※

Center for Computational Science & e-Systems
Japan Atomic Energy Agency
Tokai-mura, Naka-gun, Ibaraki-ken

(Received September 9, 2013)

With the rapid progress of the utilization of Information Technology (IT), IT infrastructure (network environment and information system) became crucial as a lifeline for promoting business. At the same time, changes in the circumstances surrounding the IT infrastructure globalize the threat of cyber attacks and increase the risk of the information security such as unlawful access to an information system, viral infection, an alteration of a website, disclosure of subtlety information, destruction of an information system and so on.

Information security measure is an important issue in Japan Atomic Energy Agency (JAEA). In order to protect the information property of JAEA from the threat, Center for Computational Science & e-Systems (CCSE) has been taking triadic measures for information security: (1) to lay down a set of information security rules, (2) to introduce security equipments to backbone network and (3) to provide information security education.

This report is a summary of the contents of the information security education by e-learning.

Keywords: Information Security, Training, e-Learning

※Collaborating Engineer

目次

Contents

１．はじめに

情報セキュリティ上の脅威は、近年急速に高度化、巧妙化、複雑化してきており、徹底した情報セキュリティ対策への取り組みが欠かせない。特に巧妙化の著しいサイバー攻撃は、ネットワークサイド（IT インフラ）におけるシステム的対策だけで防ぐことは困難であり、ユーザサイド（IT インフラ利用者）の情報セキュリティ対策強化が不可欠である。このため、日本原子力研究開発機構（以下、原子力機構という）システム計算科学センターでは、

①制度：情報セキュリティ関連規程類の整備、

②システム：情報セキュリティ機器の整備・運用、

③教育：情報セキュリティ教育の実施

を三位一体として、情報セキュリティ対策に取り組んでいる。本報告書では、これらの取り組みにおける情報セキュリティ教育について取り上げる。

情報セキュリティ対策においては、小さなセキュリティホールが大きな脅威となり、組織に甚大な被害をもたらすことになる。情報セキュリティ教育においても原子力機構の職員等全員がもれなく受講してこそ意義があり、受講の徹底が不可欠である。このため、情報セキュリティ教育の実施にあたっては、集合教育方式ではなく、受講のしやすいｅラーニングを活用した学習方式を採用した。ｅラーニングを活用することにより、受講者は自身の都合のよい時間帯に自身のパソコン等（以下、PC という）を用いて受講することが可能となり、教育の徹底に効果が見込まれる。

原子力機構における情報セキュリティ教育は、平成 18 年度の開始以来、情報セキュリティに関する規程類の解説などの基本的事項から、世の中の情勢・動向に合わせた個々の対策までを幅広く解説してきた。多くの組織でも情報セキュリティ教育を実施し、また教育教材を必要としている反面、情報セキュリティ教育に関する一貫性のある教育教材としてまとめられた資料は少なく、体系的にとりまとめたハンドブックの有効性は高いと考える。そこで、平成 18 年度以降毎年体系的に実施してきた教育で用いた教材を本報告書にまとめた。

本報告書は、情報セキュリティ情勢や情報セキュリティ対策の確認・点検だけでなく、多くの組織に共通する課題としての情報セキュリティ意識の向上に役立つものと期待する。

２．情報セキュリティ教育の概要

平成 18 年 4 月に制定された「情報セキュリティ管理規程(18(規程)第 26 号)」において、情報セキュリティ教育の実施が盛り込まれ、平成 18 年度より原子力機構の全職員等を対象に情報セキュリティ教育を開始した。情報セキュリティ教育では、

・IT インフラの利用者に対する情報セキュリティ意識の向上

・IT インフラの利用者における効果的かつ確実な対策の実施

を主眼に、情報セキュリティ規程類、情報セキュリティ情勢、インシデント事例、具体的対策方法などを丁寧に解説するとともに、継続的な実施に努めている。本情報セキュリティ教育は、原

子力機構の IT インフラを利用する全ての方を対象としており、原子力機構の役職員の他、人材派遣契約、請負契約等に基づいて原子力機構の電子メールアドレスを付与されている方を含め、約 8,000 名（平成 25 年 7 月現在）が受講対象となっている。

また、全職員等対象の基本教育・一般教育以外にも課室長向けや公開サーバ管理者向け等、職制や立場に応じた教育も実施しており、基本的・一般的な教育だけでなく、専門的な教育との両面から教育に取り組んでいる（図 1）。

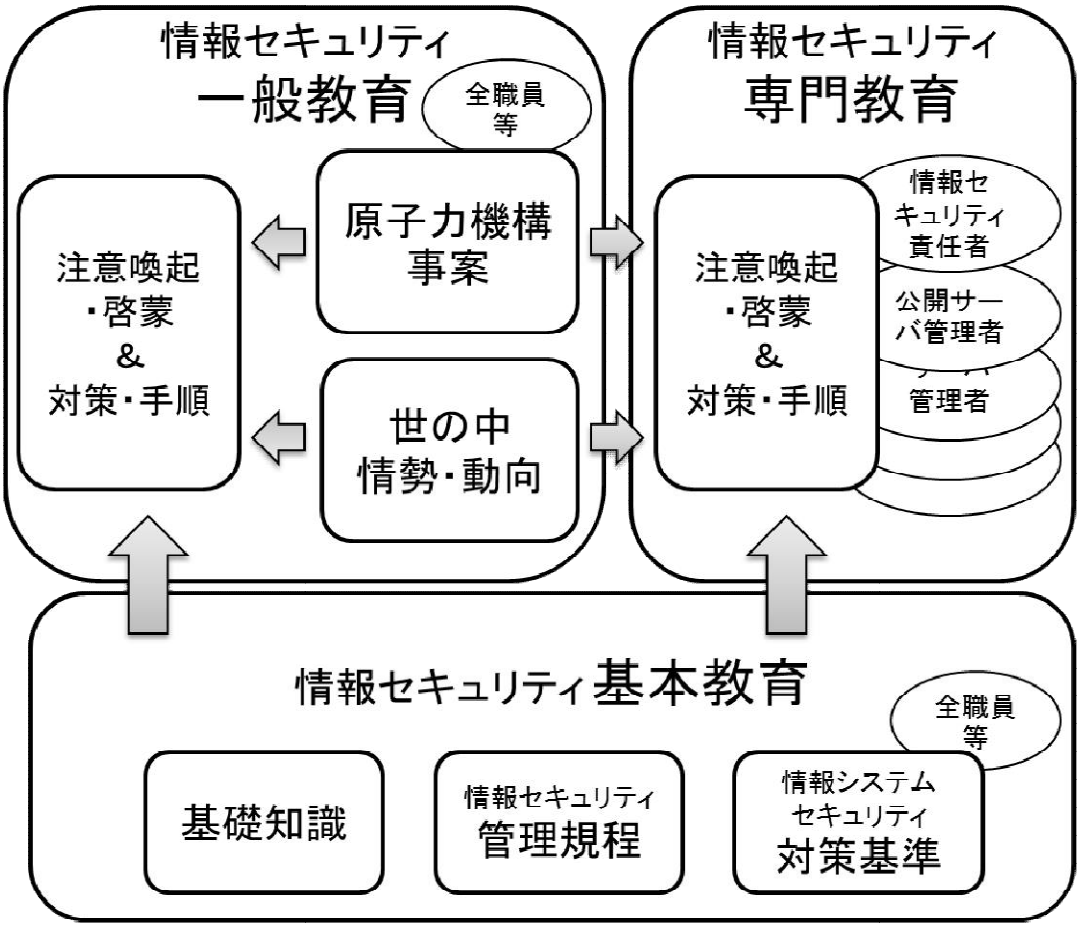


図 1 情報セキュリティ教育体系

本報告書では、3 章に情報セキュリティ教育教材の概要を示し、付録として個々の教材をまとめる。なお、情報セキュリティ教育に使用した教材は、平成 18 年度教育の一部で富士通社製の市販教材を利用したものの、すべてシステム計算科学センターで独自に作成したものである。

3．情報セキュリティ教育教材の内容

情報セキュリティ教育は、図 1 の体系に基づき、基本教育をベースに時勢に沿った世の中や原子力機構の事案・動向などを取り上げ、注意喚起と啓蒙、その対策や手順について毎年度体系的

に解説を行っている（図 2）。

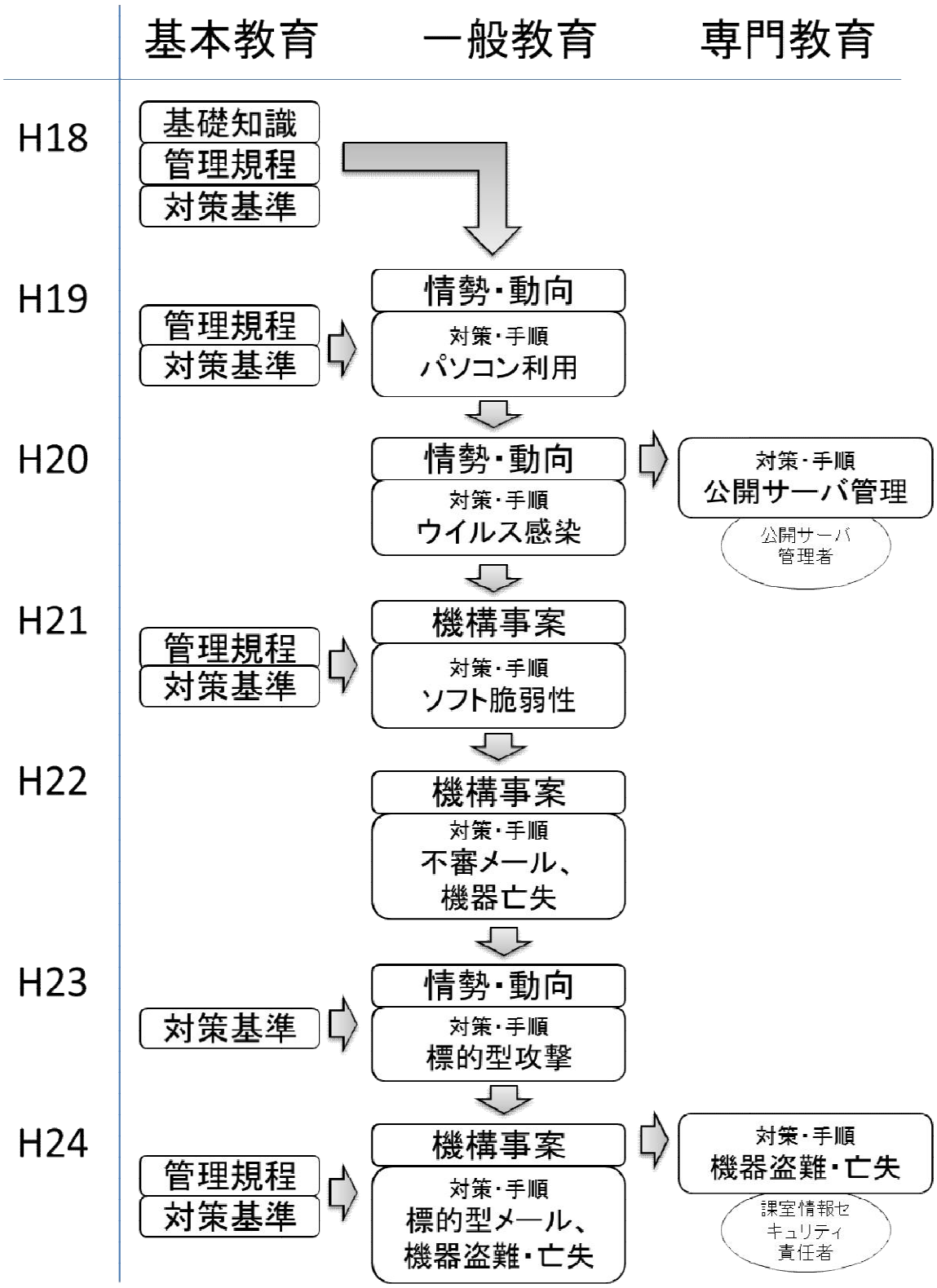


図 2 情報セキュリティ教育の流れ

３.１　情報セキュリティ入門（平成 18 年度教育）

情報セキュリティに関する基礎知識習得を目的とした富士通社製の市販教材「利用部門のための情報セキュリティ入門～現場で役立つ対策～」を利用した。

タイトルのとおり入門向けの教材であるが、脅威の種類とその対策、守るべき情報資産の選定と管理方法、ソフトウェアの導入管理、サーバ等の設置場所に求められる物理セキュリティ等を幅広く解説している。なお、市販教材のため本報告集には収録していない。

３.２　情報セキュリティ規程概要（平成 18 年度教育）

原子力機構の情報セキュリティ関連規程の周知を目的に実施した教育である。

本教育では、以下の事項について解説している。

・情報セキュリティ管理規程について　［p.9］
・情報セキュリティポリシーとその基本的考え方　［pp.9-10］
・原子力機構における情報セキュリティ対策のための体制と責務　［pp.10-12］
・情報セキュリティに関するインシデント連絡体制　［p.13］

３.３　PC および原子力機構外での情報の取り扱いに関する遵守事項（平成 19 年度教育）

情報セキュリティ管理規程、情報システムセキュリティ対策基準に続いて整備された「PC 等情報セキュリティ実施手順書」、「原子力機構外での情報処理に関する実施手順書」の周知を目的に実施した教育である。

本教育では、以下の事項について解説している。

・情報漏えい事例と分析　［pp.15-16］
・情報セキュリティ関連規程と課室情報セキュリティ責任者の役割　［p.17］
・PC の情報システム運用管理者が PC に行なうべき設定　［pp.18-19］
・PC の利用者が PC に行なうべき設定及び PC 利用時の遵守事項　［pp.19-22］
・原子力機構外で情報処理を行う場合の遵守事項　［p.23］
・原子力機構外へ持ち出す情報機器の管理と手続き　［pp.23-24］
・原子力機構支給以外の情報システムを利用する場合の遵守事項　［pp.25-26］
・情報セキュリティインシデント時の対応　［pp.27-28］

３.４　最近の情報セキュリティ事案の傾向と対策（平成 20 年度教育）

過去に発生した情報セキュリティ事案を取り上げ、その概要と対策の周知及び注意喚起を目的に実施した教育である。

本教育では、以下の事項について解説している。

・USB メモリを媒介とするウイルス感染事案と対策　［pp.30-31］
・偽セキュリティソフトによるウイルス感染事案と対策　［pp.31-32］
・改ざんされたウェブサイト閲覧によるウイルス感染事案と対策　［p.33］
・利用禁止ソフトを悪用するウイルスによる情報漏えい事案と対策　［pp.34-35］
・PC 等情報機器の盗難、紛失による情報漏えい事案と対策　［pp.36-38］

・情報セキュリティインシデント発生時の対応 ［p.39］

３.５　公開サーバのセキュリティ対策（平成 20 年度教育）

原子力機構には、外部への情報発信を行なっている公開サーバが約 60 サイトある。これら公開サーバで実施すべき情報セキュリティ対策の周知を目的に、独立行政法人 情報処理推進機構(IPA)が取り纏めている公開資料「安全なウェブサイトの作り方」等を参考に実施した教育である。なお、本教育は、公開サーバの運用管理者を対象とする専門教育として実施した。

本教育では、以下の事項について解説している。

・不要なサービスの停止・無効化 ［pp.42-44］
・OS や各種サーバソフトのセキュリティパッチの適用 ［pp.45-46］
・アクセス権限の適切な管理 ［p.47］
・パスワードの適切な管理 ［pp.48-49］
・不要なファイル、プログラムの削除 ［p.50］
・ログの管理 ［p.51］
・ウェブアプリケーションに対する攻撃の基礎知識 ［pp.52-53］
・ウェブアプリケーションの作成時に考慮すべき事項 ［pp.54-55］

３.６　コンピュータウイルス対策（平成 21 年度教育）

平成 21 年度に入ってからも USB メモリを媒介とするウイルスの検知が頻発していること、アップデート等の実施を怠っている利用者が散見されることから、注意の再喚起と規程等の再周知を目的に実施した教育である。

本教育は、本編と操作手順編の 2 つの教材で構成しており、本編では以下の事項について解説している。

・原子力機構で検知されるウイルスの侵入経路 ［pp.57-58］
・ウイルス対策 7 ヵ条 ［pp.59-60］
・ソフトウェアの脆弱性対策 ［pp.60-61］
・システム計算科学センター配布ウイルス対策ソフトの導入 ［p.62］
・外部から持ち込まれた記憶媒体のウイルス対策 ［p.62］

操作手順編は、OS やアプリケーションソフトの修正パッチ適用、ウイルス対策ソフトによるフルスキャン検査などの情報セキュリティ対策について、その詳しい設定手順をステップ・バイ・ステップ方式で模擬操作しながら習得できるようになっている。なお、操作手順篇は動画コンテンツであるため、操作項目を説明する表示画面のみ収録した。 ［pp.64-67］

３.７　情報セキュリティ事案への対策と自己点検（平成 22 年度教育）

平成 22 年度に発生した情報セキュリティ事案及びトピックスの周知と注意喚起を目的に実施した教育である。

本教育では、以下の事項について解説している。

・原子力機構における盗難被害事例と盗難・亡失対策 ［pp.69-71］

・原子力機構に届いた不審メールの例と不審メールを見分けるポイント ［pp.72-74］
・サポートが終了する OS の対応 ［pp.75-76］
・ウイルス対策 7 ヵ条 ［p.77］
・ソフトウェアの脆弱性対策 ［p.78］
・外部から持ち込まれた記憶媒体のウイルス対策 ［p.79］
・自動実行（Autorun）機能の停止手順 ［pp.79-80］

３.８　情報セキュリティ脅威の動向と対策（平成 23 年度教育）

平成 23 年秋以降、政府関連機関、防衛関連企業等で相次いだ標的型攻撃や、スマートデバイスを取り巻く脅威が増加していることを受 6 けて、注意喚起と情報セキュリティ対策の周知を目的に実施した教育である。

本教育では、以下の事項について解説している。

・防衛関連企業における標的型攻撃の事例 ［pp.83-84］
・標的型攻撃への対策【脆弱性対策編】 ［pp.85-86］
・標的型攻撃への対策【メール編】 ［pp.87-88］
・標的型攻撃への対策【ウイルス対策ソフト編】 ［pp.88-89］
・スマートデバイスを取り巻く脅威と現状 ［pp.90-91］
・日頃取り組むべき情報セキュリティ対策の再徹底 ［pp.92-96］

３.９　原子力機構内における情報セキュリティ事案とその対策（平成 24 年度教育）

平成 24 年度は、標的型攻撃による原子力機構 PC からの情報漏えい事案や、海外出張中の原子力機構職員が PC 盗難被害に遭う事案が発生したことを受けて、標的型攻撃の手口と対策、情報漏えい発生時の連絡方法の周知を目的に実施した教育である。

本教育では、以下の事項について解説している。

・原子力機構に対する標的型攻撃の事例 ［pp.100-102］
・標的型攻撃メールの特徴と対策 ［pp.102-104］
・メールシステムのおける制限事項 ［p.104］
・問い合わせ対応専用 PC の設置 ［p.105］
・原子力機構での盗難事例と問題点、対策、緊急時の対応 ［pp.106-107］
・PC、ネットワークの正しい利用 ［pp.108-109］
・ウイルス検出数の傾向と対策 ［pp.110-111］
・メーカーサポートが終了する OS などの対応 ［pp.111-112］
・電子メールのテキスト設定、パスワードの適正設定 ［p.113］

３.１０　パソコンなどの盗難事案における情報セキュリティ対策と連絡対応（平成 24 年度教育）

海外出張中の原子力機構職員が PC 盗難被害に遭う事案が発生したことを受けて、課室情報セキュリティ責任者（原子力機構外での情報処理の許可者）としての役割と責任を課室長に再認識してもらうことを目的に実施した教育である。なお、本教育は、課室情報セキュリティ責任者（課

室長）を対象とする専門教育として実施した。

本教育では、以下の事項について解説している。

・原子力機構における盗難被害事例と問題点 ［pp.116-117］
・盗難・亡失への対策 ［pp.118-119］
・盗難・亡失へのリスク分析 ［pp.119-120］
・盗難・亡失が発生した場合の連絡 ［pp.120-122］

4．おわりに

情報セキュリティ教育は、平成 18 年度の開始以降、7 年が経過した。「必ず受講する教育」として原子力機構内に浸透し、平成 23 年度以降は受講率 100%を維持している。毎年行なっている情報セキュリティに関するアンケート調査において、各部署の情報セキュリティ意識の向上が確認されており（図 3)、情報セキュリティ教育の効果が現れている。「情報セキュリティ対策を最優先」と考える部署が増大し、「情報セキュリティの確保に努めざるを得ない」と考える部署を合わせて、全体の 97%以上が情報セキュリティを重要視していることが分かる。

今後も情報セキュリティに関する知識の周知や啓蒙を進め、情報セキュリティ意識のさらなる向上を図っていく。

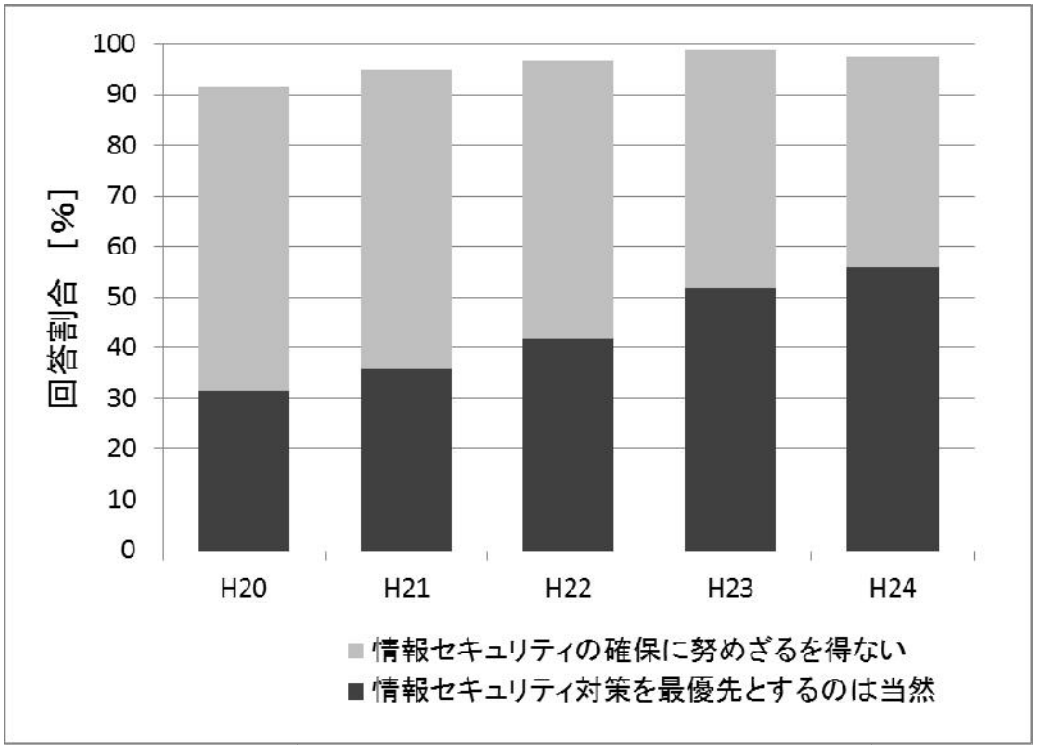


図 3 情報セキュリティ意識調査

謝辞

本報告書をとりまとめるにあたり、ご指導とご助言を頂いたシステム計算科学センターの谷正之センター長、青柳哲雄技術主席、情報システム管理室の久米悦雄室長、清水大志室長代理に深く感謝の意を表します。

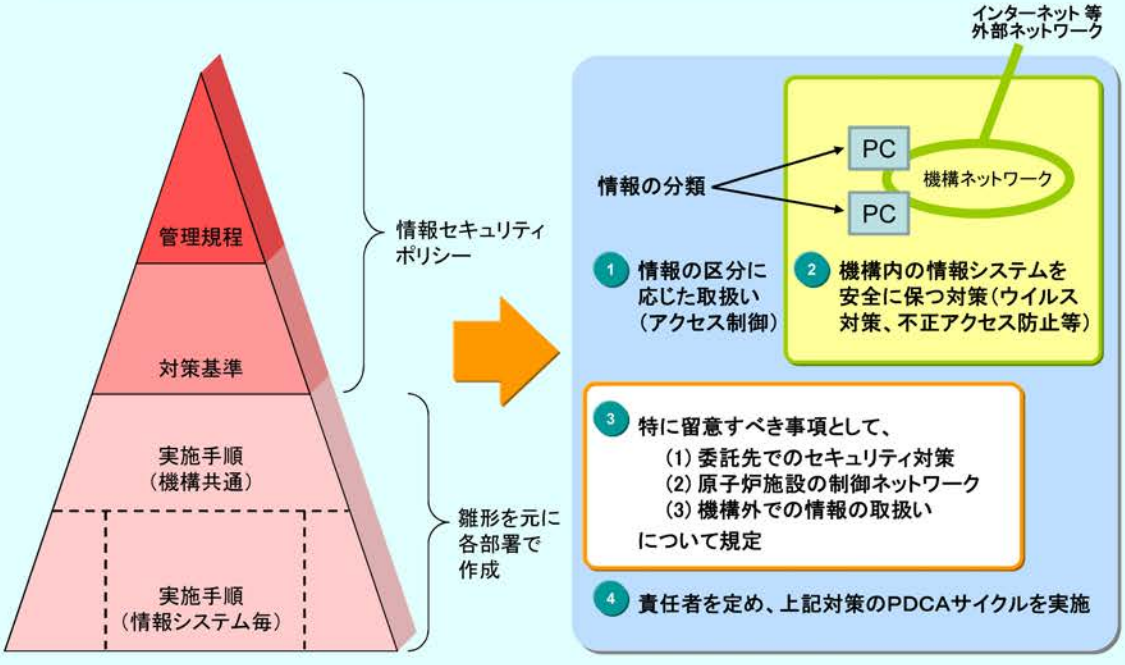
付録１　「情報セキュリティ規程概要」

情報セキュリティ管理規程について

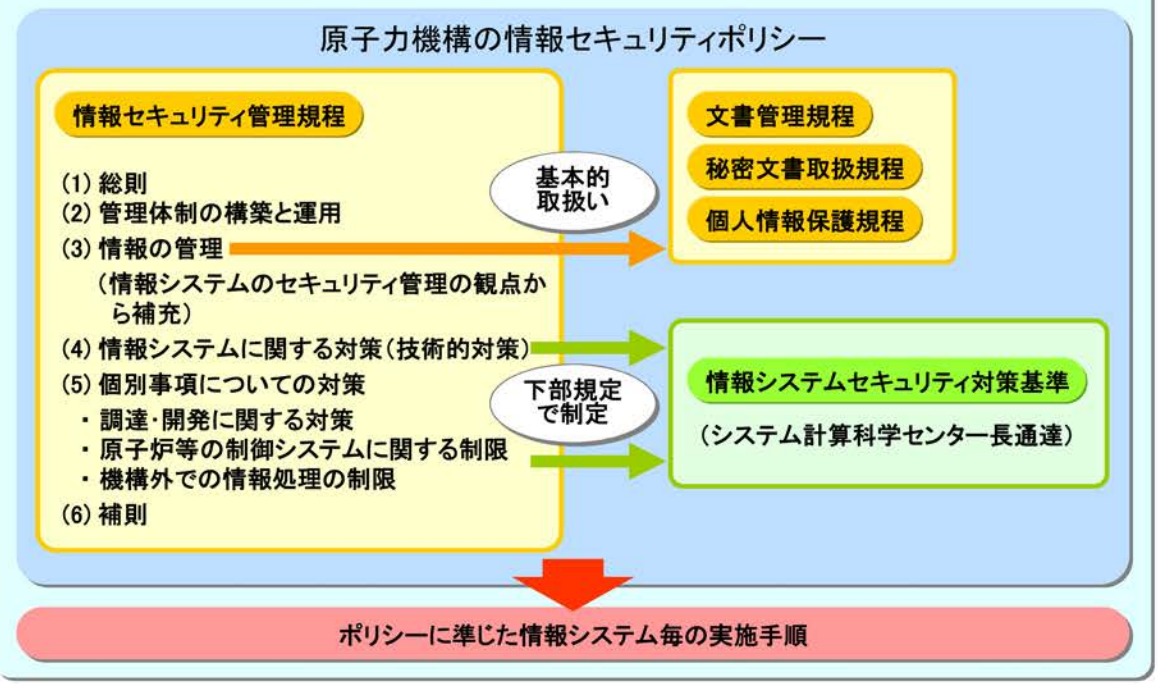
1. **基本方針**
   利便性を確保しつつ、強固な情報セキュリティ対策を実施
2. **管理体制の構築と運用**
   情報セキュリティ責任者、情報セキュリティ委員会、情報セキュリティ監査責任者等を設置
3. **情報についての対策（情報の分類と管理）**
   文書管理規程等の既存規程を適用し、情報システムのセキュリティ管理の観点から補充
4. **情報システムに関する対策（技術的対策）**
   具体的な技術的対策基準は、システム計算科学センター長通達で規定
5. **個別事項についての対策**
   セキュリティの観点から特に留意すべき事項を規定
   - ◆ 外部委託時の対策
   - ◆ 原子炉施設等の制御システムにおける対策
   - ◆ 機構外で情報を取扱う際の対策

   規程URL ： http://intra3.jaea.go.jp/kitei/07vxe_/default.htm

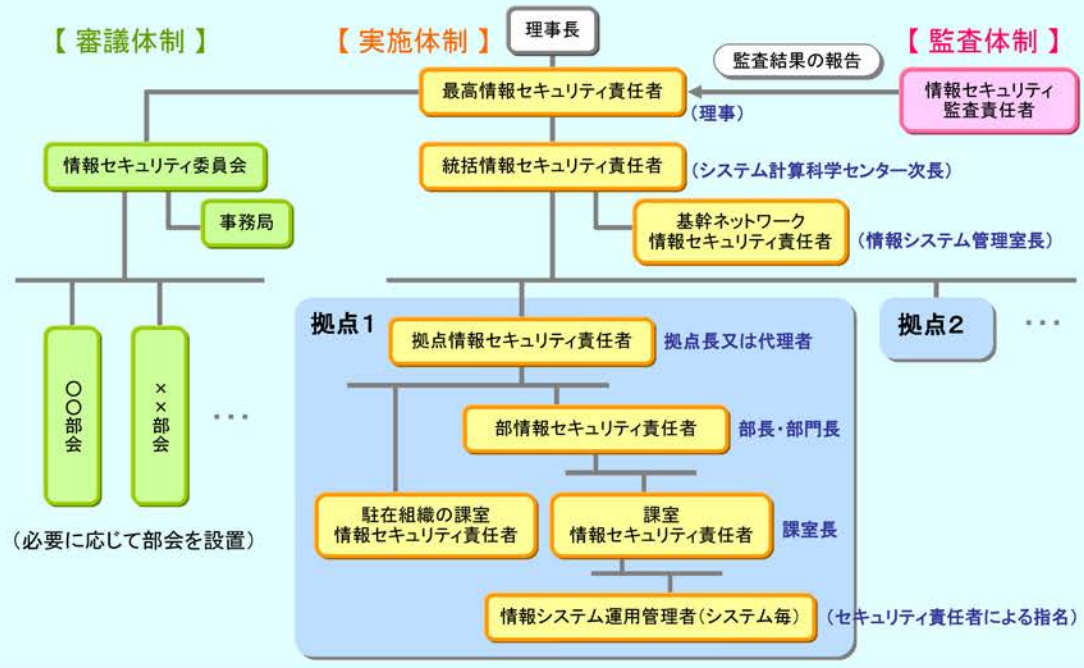
情報セキュリティポリシーとその基本的考え方



原子力機構における情報セキュリティポリシーの概要



原子力機構における情報セキュリティ対策のための体制図



情報セキュリティ意識の共通化と実施

情報セキュリティ対策については、理事長以下機構の情報資産を扱う全ての者が情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行にあたって情報セキュリティに関する法令、規程等を遵守するものとする。

また、職員等は外来者等にこれを遵守させる義務を負うものとする。

課室情報セキュリティ責任者の主な責務

- 課室内の情報システムに対し情報セキュリティ対策を実施する。
- 情報資産を守るため、必要に応じ情報システムの緊急停止措置をとる。
- 情報セキュリティ関連規程等への重大な違反を知った場合、部情報セキュリティ責任者へ報告する。
- 課室内の職員等に情報セキュリティ教育を受講する機会を与える。
- 重要な情報の定期的バックアップを行う。
- 作成または入手した情報の分類を行う。
  (1) 要保全情報(取り扱い制限を実施)
  (2) 要安定情報(取り扱い制限を実施)
  (3) 一般情報
- 情報システムセキュリティ実施手順を策定する。(情報システム毎)

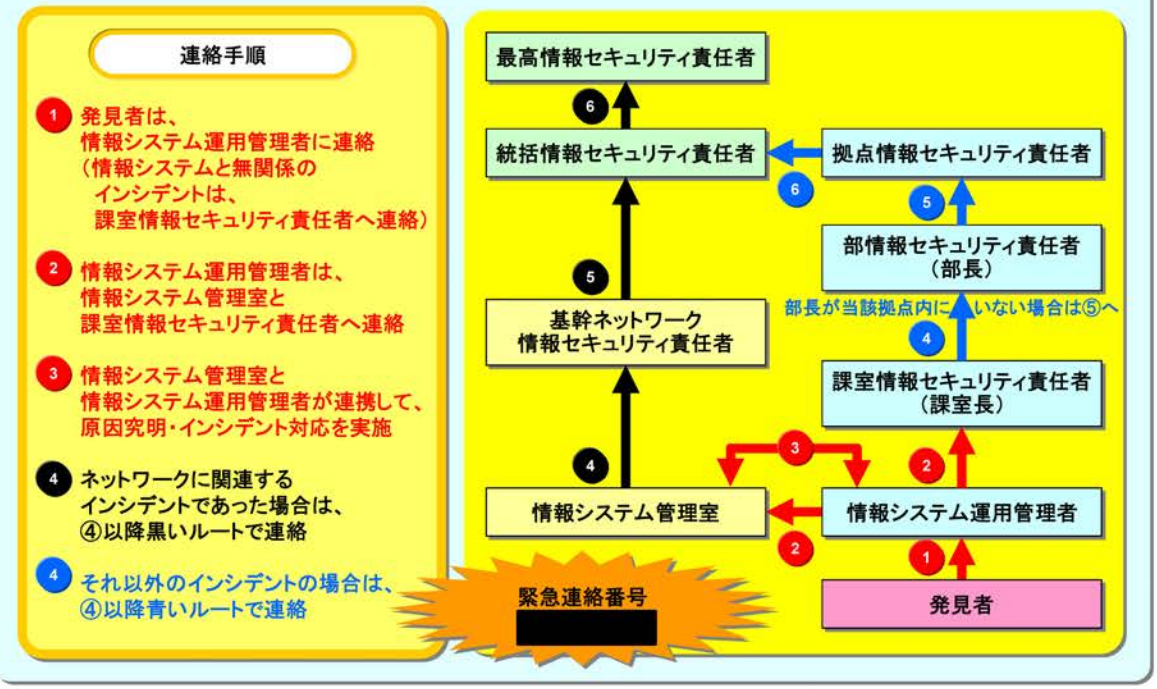
情報システム運用管理者の主な責務

- 課室情報セキュリティ責任者の指示に従い、情報システムの運用、管理等の実作業を行う。
- 情報セキュリティに関する障害等について報告を受けた場合、速やかにその確認を行い、課室情報セキュリティ責任者に報告する。
- 情報セキュリティに関する障害等について、課室情報セキュリティ責任者から指示を受けた際は、その指示に従い、被害の拡大防止対策に努める。

職員等の主な責務等

- 情報セキュリティ関連規程等への重大な違反を知った場合、課室情報セキュリティ責任者へ報告する。
- 情報セキュリティに関する教育を受講する。
- 情報セキュリティに関する障害等の予防措置を講ずる 。
- 情報セキュリティに関する障害等を発見した場合、ネットワーク接続を解除した後、現状を保持すると共に、速やかに情報システム運用管理者へ連絡する。
- 機構の業務の遂行以外の目的で「情報」を利用しない。
- 機構外で要保全情報又は要安定情報を取扱う場合、課室情報セキュリティ責任者の許可を得る。
- 機構の機器等又は媒体を機構外に持ち出す場合、あるいは機器などを持ち込む場合、課室情報セキュリティ責任者の許可を得る。
- 原則として機構が支給した以外の情報システムで、機構の要機密情報、要保全情報及び要安定情報を取り扱わない。

情報セキュリティに関するインシデント連絡体制



拠点情報セキュリティ責任者等一覧

（平成21年10月現在）

最高情報セキュリティ責任者	理事
統括情報セキュリティ責任者	システム計算科学センター　次長
基幹ネットワーク情報セキュリティ責任者	システム計算科学センター　情報システム管理室長
拠点情報セキュリティ責任者（本部）	総務部　部長
拠点情報セキュリティ責任者（システム計算科学センター）	システム計算科学センター　センター長
拠点情報セキュリティ責任者（東京事務所）	東京事務所　上席参事・副所長
拠点情報セキュリティ責任者（原子力科学研究所）	原子力科学研究所　副所長
拠点情報セキュリティ責任者（原子力科学研究所）	安全研究センター　センター長
拠点情報セキュリティ責任者（原子力科学研究所）	先端基礎研究センター　研究主幹
拠点情報セキュリティ責任者（原子力科学研究所）	原子力基礎工学研究部門　研究副主幹
拠点情報セキュリティ責任者（原子力科学研究所）	量子ビーム応用研究部門　研究主幹
拠点情報セキュリティ責任者（原子力科学研究所）	バックエンド推進部門　副部門長
拠点情報セキュリティ責任者（核燃料サイクル工学研究所）	核燃料サイクル工学研究所　副所長
拠点情報セキュリティ責任者（大洗研究開発センター）	大洗研究開発センター　所長
拠点情報セキュリティ責任者（敦賀本部）	敦賀本部　業務統括部長
拠点情報セキュリティ責任者（高速増殖炉研究開発センター）	高速増殖炉研究開発センター　副所長
拠点情報セキュリティ責任者（原子炉廃止措置研究開発センター）	原子炉廃止措置研究開発センター　研究主席
拠点情報セキュリティ責任者（国際原子力情報・研修センター）	国際原子力情報・研修センター　センター長
拠点情報セキュリティ責任者（那珂核融合研究所）	那珂核融合研究所　所長
拠点情報セキュリティ責任者（高崎量子応用研究所）	高崎量子応用研究所　所長
拠点情報セキュリティ責任者（関西光科学研究所）	関西光科学研究所　所長
拠点情報セキュリティ責任者（幌延深地層研究センター）	幌延深地層研究センター　副所長
拠点情報セキュリティ責任者（東濃地科学センター）	東濃地科学センター　副所長
拠点情報セキュリティ責任者（人形峠環境技術センター）	人形峠環境技術センター　副所長
拠点情報セキュリティ責任者（青森研究開発センター）	青森研究開発センター　所長

[redacted]

◆ 最新版はこちらをご覧ください。

付録２　「PC および原子力機構外での情報の取り扱いに関する遵守事項」

～ 情報セキュリティ教育～

PCおよび機構外での情報の取り扱いに関する遵守事項

本教育の概要

本教育では、機構業務に利用する一般パソコン（以下、「PC」という）および機構外での情報の取り扱いに関する遵守事項について学習します。

不正アクセス等による情報の改ざんや破壊、ウィルス感染、その他の脅威から機構の情報資産を保護するため、本教育の内容を遵守し、情報の管理に十分注意を払いながら業務を行なってください。

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

第１章　最近の情報漏えい事件より

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

１．１　事件例

USBメモリ等の可搬記録媒体やPCを、置き忘れたり盗難されたりすることによる情報漏えいの事例を紹介します。

- 会社員が、業務情報や個人情報を含む**USBメモリをバッグに入れ、通勤電車内にバッグごと置き忘れて**紛失。（駅のベンチや飲食店での置き忘れの同様事例多数。）
- 自治体業務の受託業者が、約1500人のメールアドレスおよびその他の個人情報1900人分を記録した**ノートパソコンの入ったバックを車中に置いたまま車を離れたところ、バッグごと盗難**にあって情報が漏えいした。

個人PCを使用したことによる情報漏えい事件も発生しています。最近では、Winny等の「ファイル共有ソフト」を経由して、情報漏えいが起こるケースが多発しています。

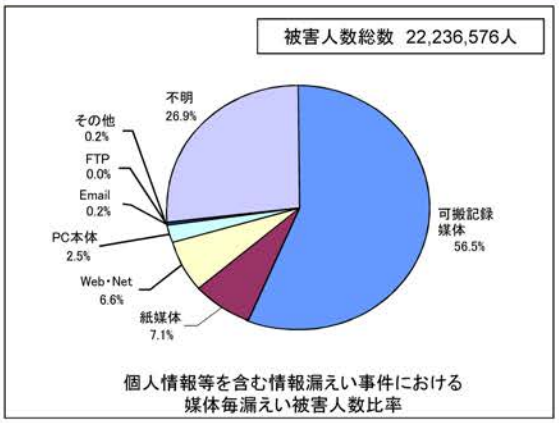
- 某自治体職員が、税の未払い者等、約600人分の**個人情報、住基ネットへの接続パスワード等の業務情報を含むデータを持ち帰り、自宅の私用PCに保存**していた。
  → 私用PCのWinnyを経由して外部に情報が漏えいし、問題となった。

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

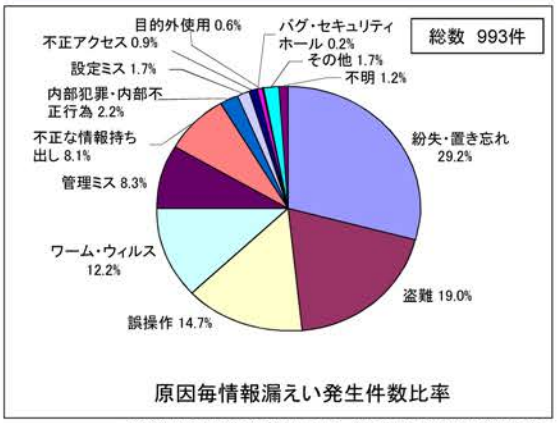
１．２　情報漏えい事件に関する分析結果より

一般に報道された情報漏えい事件の分析結果によると、大規模な漏えいに繋がり易い媒体は、**①可搬記録媒体、②紙媒体、③Web・Net、④PC本体** の順になっています。原因となった事象は、**①紛失・置き忘れ、②盗難、③誤操作** が代表的であり、人為的原因が多いことが判ります。

また、漏えい事件に至る背景に、**許可を得ていない業務情報の持ち出しや私有PCへのコピー**など、ルール違反を伴っているものが約50%を占めているという調査結果もあります。



個人情報等を含む情報漏えい事件における
媒体毎漏えい被害人数比率



原因毎情報漏えい発生件数比率

（参考）JNSA 2006 年 情報セキュリティインシデントに関する調査報告書

機構においては、業務の性格上、適切な管理が必要な情報が多数存在しています。

上記を十分認識して、情報の管理に細心の注意を払ってください。

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

第２章　関連規程・手順書類と責任者・管理者の役割

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

２．１　関連規程・手順書類

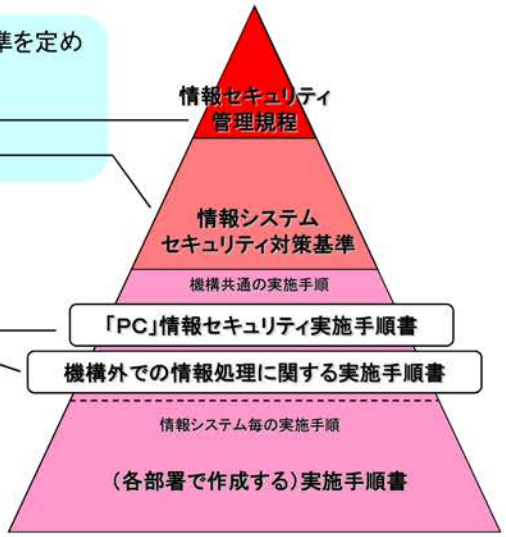
機構では、情報セキュリティポリシーとして以下の規程・基準を定めています。

- 情報セキュリティ管理規程
- 情報システムセキュリティ対策基準

さらに、規程・基準に基づいて情報の管理を適切に行うための手引きとして、二つの実施手順書を整備しています。

- 「PC」情報セキュリティ実施手順書
- 機構外での情報処理に関する実施手順書

本教育の内容は、主としてこの二つの実施手順書に準拠しています。



ＰＣおよび機構外での情報の取り扱いに関する遵守事項

２．２　課室・グループにおける責任者、管理者の役割

課室・グループにおける責任者、管理者の役割は、以下のように規程されています。

情報セキュリティ管理規程（１８規程第２６号）

（課室情報セキュリティ責任者）⇒課室長・GL
第１２条　機構の課（課に相当する組織を含む。以下「課室」という。）毎に課室情報セキュリティ責任者を置く。
２　課室情報セキュリティ責任者は、当該課室組織の長をもって充てる。
３　課室情報セキュリティ責任者は、**当該課室組織の情報システムの情報セキュリティ対策の実施にあたる。**

（情報システム運用管理者）⇒運用管理の実作業を行なう者
第１３条　機構の情報システム毎に情報システム運用管理者を置く。
２　情報システム運用管理者は、拠点情報セキュリティ責任者又は部情報セキュリティ責任者若しくは課室情報セキュリティ責任者が指名し、必要に応じて複数人から構成される。
３　情報システム運用管理者は、**既存の情報システムの運用時又は新規情報システムの導入時において、当該情報セキュリティ責任者の指示に従い、情報システムの運用、管理等の実作業を行う。**

※本教育内における情報システム運用管理者とは、当該課室のPCを所掌する**「PCの情報システム運用管理者」**を指します。なお、**PCの利用者自身が「PCの情報システム運用管理者」を兼ねる場合もあります。**
→【「PC」情報セキュリティ実施手順書　2.1】参照

→ 次頁より、役割毎にPCの導入時や利用時に遵守して頂きたい事項を紹介します。

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

第３章　ＰＣの取り扱いに関する遵守事項

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

３．１．１　ＰＣの情報システム運用管理者が各ＰＣに設定すべき項目（１）

PCの情報システム運用管理者は、各PCに以下の設定を行ってください。

ユーザIDへの管理者権限の付与は必要最低限に限定する

PC利用者のユーザIDには利用者権限のみを付与してください。

→【「PC」情報セキュリティ実施手順書　4.1】参照

特段の理由がない限り、ユーザーIDは個別に発行する

いつ誰がPCを利用していたかを特定できない、離職した人でも知っているといった問題が起こる可能性があるので、ユーザーIDの共用は原則として行なわないでください。

→【「PC」情報セキュリティ実施手順書　4.1】参照

OSのパスワードポリシーを 文字数：8桁以上、有効期間：90日以内 に設定する

PC利用者にパスワード管理を適切に行なってもらうため、OSのパスワードポリシーを設定してください。

→【「PC」情報セキュリティ実施手順書　4.3】参照

詳細な設定方法は、該当する実施手順書を確認してください。（次頁以降も同様）

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

３．１．２　ＰＣの情報システム運用管理者が各ＰＣに設定すべき項目（２）

OSおよびソフトウェアのアップデートは、自動更新機能を活用する

自動更新機能が使えない場合は、月に1回を目途にセキュリティ修正プログラム、パッチ等を確認し、必要な修正を適用してください。
→【「PC」情報セキュリティ実施手順書　5.1】参照

ウィルス対策ソフトウェアを導入する

原則として、システム計算科学センターが整備しているウィルス対策ソフトウェアを使用してください。当該ソフトウェアは、機構イントラネットの「コンピュータ&ネットワーク利用」ページ内から利用申請を行って入手してください。
→【「PC」情報セキュリティ実施手順書　5.2】参照

パーソナルファイアウォール機能を有効にする

ネットワーク経由での攻撃からPCを保護するため、パーソナルファイアウォール機能を有効にしてください。
→【「PC」情報セキュリティ実施手順書　5.3】参照

機構の時刻サーバとPCの時刻を同期させる設定をする

機構内のPCの時刻を統一し、障害時の調査を容易にするため、機構の時刻サーバとPCの時刻を同期させる設定をしてください。
→【「PC」情報セキュリティ実施手順書　10.1】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

３．２．１　ＰＣの利用者が各ＰＣに設定すべき項目（１）

PCの利用者は、各PCに以下の設定を行ってください。

複雑なパスワードを設定する

PCには必ずパスワードを設定してください。その際、容易に他人に推測されないよう、以下を満たした複雑なパスワードを設定してください。

- **文字数：8桁以上**
- **2つ以上のアルファベットと1つ以上のアルファベットでない文字(記号や数字)を含める**
- **4つ以上の異なる文字を含める**
- **辞書にある単語や一般的な言葉を単独で使用しない**

→【「PC」情報セキュリティ実施手順書　4.2】参照

パスワード付きスクリーンセーバを設定する

離席時等に他人に操作されることを防ぐため、パスワード付きスクリーンセーバが自動起動するように設定してください。
→【「PC」情報セキュリティ実施手順書　3.3】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

３．２．２　ＰＣの利用者が各ＰＣに設定すべき項目（２）

HTMLメールを送受信しないように設定する

ウィルス感染等を防ぐため、メール閲覧時にHTMLメールをそのまま表示したり、HTMLメールを作成・送信しないよう、設定してください。

→【「PC」情報セキュリティ実施手順書　8.1】参照

ブラウザのパスワード補完機能を停止する

PCを他人に使用された場合でも、接続先のIDやパスワードを悪用されないために、Internet Explorer等のWebブラウザの「パスワード自動補完機能」を無効にしてください。

→【「PC」情報セキュリティ実施手順書　9.1】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

３．３．１　ＰＣ利用時の遵守事項（１）

PC利用時は、以下の各項目を遵守してください。

利用禁止ソフトウェアをインストールしない

以下の利用禁止ソフトウェアは、情報漏えいにつながる危険性があるため、インストールや利用を行なってはなりません。

（1）P2Pファイル共有ソフトウェア

・Winny　・WinMX　・KaZaa　・Share 等

（2）その他

・SoftEther

※利用禁止ソフトウェアの一覧表（適宜更新されます）は、
http://www2.tokai-sc.jaea.go.jp/kanrika/security/ngsoft.htmlで確認してください。

※PCの情報システム管理者は、インストールしたソフトウェアを管理台帳等を使って管理してください。

→【「PC」情報セキュリティ実施手順書　2.3】参照

離席時はPC画面をロックする

PCを起動したまま席を離れる場合は、PCの画面をロックしてください。

→【「PC」情報セキュリティ実施手順書　3.2】参照

アプリケーションソフトウェアを随時アップデートする

セキュリティホール対策のため、アプリケーションソフトウェアを随時アップデートし、最新の状態にしてください。

→【「PC」情報セキュリティ実施手順書　5.1】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

３．３．２　ＰＣ利用時の遵守事項（２）

不審なメールは開かず削除する

送信元が不明、件名や内容が意味不明、不審なファイルが添付されている等、不審な電子メールを受信した場合には、すぐに削除を行ってください。

→【「PC」情報セキュリティ実施手順書　8.3】参照

実際に機構に届いた不審なメールの例

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

３．３．３　ＰＣ利用時の遵守事項（３）

PCが修理、移行、廃却等により機構の管理下を離れる場合は、ハードディスク内のデータを消去し、消去日および消去方法等を「パソコン等データ消去確認書」に記録する

PCの修理等の場合で、データ消去が不可能な場合には、必ず相手先と守秘義務契約を結ぶ等の措置を行なってください。

→【「PC」情報セキュリティ実施手順書　7.1】参照

必要に応じて電子ファイルにパスワードを設定する

情報の重要性などから判断し、必要に応じて電子ファイルにパスワードを設定してください。

→【「PC」情報セキュリティ実施手順書　6.2】参照

課室情報セキュリティ責任者の指示があった場合は、電子ファイルを暗号化する

課室情報セキュリティ責任者（課室長等）による義務付け・指示があった場合は、取り扱う電子ファイルを必ず暗号化してください。

→【「PC」情報セキュリティ実施手順書　6.3】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

３．３．４　ＰＣ利用時の遵守事項（４）

IDの共有や貸与はしない

IDを共有すると、異動などでIDが不要になった人でも引き続き使用できてしまう等の問題があります。また、IDを他人に利用させると、その後、他人に自分のIDを利用される可能性が高くなります。IDの共有や貸与は、業務上やむを得ず必要な場合以外は、行わないでください。

→【「PC」情報セキュリティ実施手順書　4.1】参照

パスワードは他人の目に触れないように管理する

パスワードをメモした場合は、そのメモが他人の目に触れぬよう、施錠管理等を行ってください。
漏えいした可能性・不正利用される可能性を感じた場合は、遅滞なくパスワードを変更してください。

→【「PC」情報セキュリティ実施手順書　4.3】参照

身分証明書、ハードウェアトークンの貸与はしない

身分証明書は、機構の役職員としての身分を証明するものであり、リモートアクセス等の認証にも使用します。悪用を防ぐため、身分証明書を他人へ貸与しないでください。リモートアクセスの認証に利用するハードウェアトークンも同様です。

→【情報システムセキュリティ対策基準 第28条】参照

重要なデータはバックアップを行なう

ハードディスクの故障やウィルス等により、PCに記録しているデータが破壊されてしまう場合があります。また、不正なアクセスにより内容が改ざんされてしまう恐れもあります。このような場合に業務に支障が出る重要なデータ（要保全情報、要安定情報）は、異なる記録媒体にバックアップを行ってください。

→【情報システムセキュリティ対策基準 別表4】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

第４章　機構外での情報の取り扱いに関する遵守事項

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

４．１　全般事項

機構外で情報処理を行う場合は、以下を遵守してください。

「機構外での情報処理に関する許可申請書 兼 パソコン等物品持出し申請書」による申請をする

機構外で情報処理を行なう場合は、課室情報セキュリティ責任者に申請の上、許可を得ることが必要です。また、機構外での情報処理が終了した際には、速やかに課室情報セキュリティ責任者に報告してください。

→【機構外での情報処理に関する実施手順書　2.1】参照

持ち運ぶ際は手元に置き、交通機関の網棚や車内に放置しない

PCや可搬記録媒体を持ち運ぶ際、置き忘れや盗難に十分注意してください。

→【機構外での情報処理に関する実施手順書　4.1】参照

鍵の掛かる場所に保管するか、目の届くところに置く

PCや可搬記録媒体は、鍵の掛かる場所に施錠保管することが基本です。施錠保管が不可能な場合は常時携帯するか、目の届くところに置いてください。

→【機構外での情報処理に関する実施手順書　4.2】参照

他人へ貸したり預けたりしない

PCや可搬記録媒体は、他人に貸したり預けたりしてはいけません。

→【機構外での情報処理に関する実施手順書　4.3】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

４．２　機構外へＰＣを持ち出す場合の遵守事項

機構外へPCを持ち出す場合は、機構内PCと同様の設定や取り扱いが原則となりますが、さらに以下の措置を行なってください。

PCのBIOSにパスワードを設定する

PCのOSだけでなく、BIOSにも8桁以上の複雑なパスワードを設定してください。BIOSの制約で8桁以上の設定が不可能な場合は、最大の桁数で設定してください。

→【機構外での情報処理に関する実施手順書　5.5】参照

要機密情報を必ず暗号化する

課室情報セキュリティ責任者（課室長等）による義務付け・指示があった場合は、取り扱う電子ファイルを必ず暗号化してください。特に、要機密情報を持ち出す場合は、必ず暗号化してください。

→【機構外での情報処理に関する実施手順書　5.9】参照

機構内への再持ち込み時は、手動でOSやウィルス対策ソフトウェアを最新にする

PCを機構内へ再持ち込みする際は、機構のネットワークに接続されている他のPCを利用してOSのアップデートファイルやウィルス対策ソフトウェアの最新パターンファイルを入手してください。入手したファイルを記録媒体経由で再持ち込みPCに適用した後、ウィルスチェックを行なってから機構のネットワークに接続するようにしてください。

→【機構外での情報処理に関する実施手順書　5.10】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

４．３．１　可搬記録媒体を利用して情報を持ち出す場合の遵守事項（１）

可搬記録媒体を利用して情報を機構外へ持ち出す場合は、以下を遵守してください。

「機構外での情報処理に関する許可申請書 兼 パソコン等物品持出し申請書」を用いて課室情報セキュリティ責任者に申請の上、許可を得る
なお、機構支給以外の可搬記憶媒体を利用する場合は、「機構支給以外情報システムの業務への使用許可申請書 兼 使用終了確認書」による申請も必要となる

→【機構外での情報処理に関する実施手順書　2.2】参照

USBメモリ等、認証機能付媒体がある場合は、認証機能付きのものを使用する

USBメモリは、パスワード機能、指紋認証機能等がついているものがあります。可搬記録媒体を機構外で用いる場合は、これらの認証機能を備えているものを使用してください。

→【機構外での情報処理に関する実施手順書　8.1】参照

格納するデータは必要最小限にする

盗難や紛失に備え、可搬記録媒体に格納するデータは必要最小限にしてください。

→【機構外での情報処理に関する実施手順書　8.2】参照

暗号化を実施する

可搬記録媒体に情報を格納して機構外へ持ち出す場合は、原則としてファイルを暗号化してください。
媒体に暗号化機能がついている場合はそれを用い、機能がない場合には格納するファイルに対して個別に暗号化を行ってください。

→【機構外での情報処理に関する実施手順書　8.3】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

４．３．２　可搬記録媒体を利用して情報を持ち出す場合の遵守事項（２）

作業終了後は、機構の情報（公知は除く）の消去を行い、課室情報セキュリティ責任者に報告する

消去後は、
「機構外での情報処理に関する許可申請書 兼 パソコン等物品持出し申請書」および
「機構支給以外情報システムの業務への使用許可申請書 兼 使用終了確認書」
を用いて課室情報セキュリティ責任者に報告してください。

→【機構外での情報処理に関する実施手順書　2.2、7.9】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

４．４．１　個人ＰＣを業務のために利用する場合の遵守事項（１）

個人PCを業務のために利用する場合は、以下を遵守してください。

個人PCを機構外で使用して業務を行う場合は、
「機構外での情報処理に関する許可申請書 兼 パソコン等物品持出し申請書」および
「機構支給以外情報システムの業務への使用許可申請書 兼 使用終了確認書」
を用いて課室情報セキュリティ責任者に申請の上、許可を得る

→【機構外での情報処理に関する実施手順書　2.2】参照

利用禁止ソフトウェアがインストールされていないことを確認する

家族等と共用している個人PCの場合、自分の知らない間に利用禁止ソフトウェアがインストールされていることも想定されます。念のため、以下の利用禁止ソフトウェアがインストールされていないことを確認してください。

（1）P2Pファイル共有ソフトウェア
　・Winny　・WinMX　・KaZaa　・Share 等
（2）その他
　・SoftEther

※利用禁止ソフトウェアの一覧表（適宜更新されます）は、
http://www2.tokai-sc.jaea.go.jp/kanrika/security/ngsoft.htmlで確認してください。

→【機構外での情報処理に関する実施手順書　7.1】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

４．４．２　個人ＰＣを業務のために利用する場合の遵守事項（２）

以下のセキュリティ対応を行なう

- セキュリティホール対策が実施されていることを確認する
- 不正プログラム等の感染状況を確認する
- BIOSパスワードを設定する
- PCをロックする
- パスワード付きスクリーンセーバを設定する
- パーソナルファイアウォール機能を有効にする
- 要機密情報を暗号化する

作業終了後は、機構の情報（公知は除く）の消去を行い、課室情報セキュリティ責任者に報告する

消去後は、
「機構外での情報処理に関する許可申請書 兼 パソコン等物品持出し申請書」および
「機構支給以外情報システムの業務への使用許可申請書 兼 使用終了確認書」
を用いて課室情報セキュリティ責任者に報告してください。

→【機構外での情報処理に関する実施手順書　2.2、7.9】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

４．５．１　他機関のシステムを利用する場合の遵守事項（１）

他機関のシステムを利用して機構の情報を処理する場合は、以下を遵守してください。

「機構外での情報処理に関する許可申請書 兼 パソコン等物品持出し申請書」および「機構支給以外情報システムの業務への使用許可申請書 兼 使用終了確認書」を用いて課室情報セキュリティ責任者に申請の上、許可を得る

→【機構外での情報処理に関する実施手順書 2.2】参照

利用禁止ソフトウェアがインストールされていないことを確認する

以下の利用禁止ソフトウェアがインストールされていないことを、システムの運用管理者に確認してください。

（1）P2Pファイル共有ソフトウェア

・Winny ・WinMX ・KaZaa ・Share 等

（2）その他

・SoftEther

※利用禁止ソフトウェアの一覧表（適宜更新されます）は、
http://www2.tokai-sc.jaea.go.jp/kanrika/security/ngsoft.html で確認してください。

→【機構外での情報処理に関する実施手順書 6.1】参照

セキュリティホール対策が実施されていることを確認する

OSのアップデート等、セキュリティホール対策が実施されていることを、システムの運用管理者に確認してください。

→【機構外での情報処理に関する実施手順書 6.2】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

４．５．２　他機関のシステムを利用する場合の遵守事項（２）

不正プログラム等の感染状況を確認する

ウィルス対策ソフトの導入と定義ファイル等の更新を実施し、不正プログラムに対する監視を行っていることを、システムの運用管理者に確認してください。

→【機構外での情報処理に関する実施手順書 6.3】参照

離席時の端末放置の禁止

離席時には情報システムからログアウトするか、もしくはシステムの運用管理者と調整の上、PCの画面ロック等の設定を行ってください。

→【機構外での情報処理に関する実施手順書 6.4】参照

要保護情報を暗号化する

課室情報保護セキュリティ責任者の指示がある、もしくは要機密情報・要保全情報等を取り扱う場合は、ファイルの暗号化を実施してください。

→【機構外での情報処理に関する実施手順書 6.5】参照

利用終了時にはデータを消去する

機構外での情報処理終了時には、他機関のシステム上にある機構の情報を消去してください。

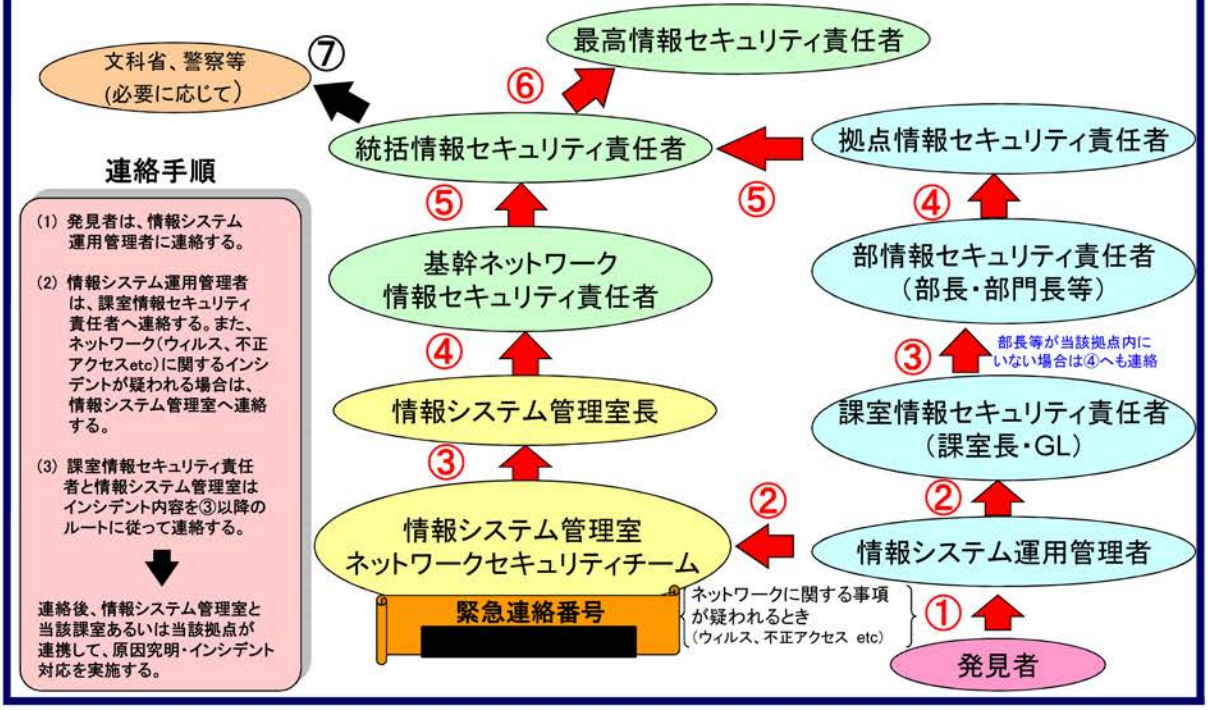
→【機構外での情報処理に関する実施手順書 6.6】参照

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

第５章　情報セキュリティインシデント発生時の対応

ＰＣおよび機構外での情報の取り扱いに関する遵守事項

５．１　情報セキュリティインシデント発生時の連絡手順



ＰＣおよび機構外での情報の取り扱いに関する遵守事項

５．２　セキュリティ緊急Topics（機構イントラページ）

※最新のセキュリティ情報を、機構イントラネットの「**セキュリティ緊急Topics**」にて公開しています。随時ご確認ください。
http://intra.jaea.go.jp/ トップページ参照

以上で学習は終了です。「次へ」のボタンをクリックし、学習を終了してください。
その後、コース一覧画面から「テスト」ボタンをクリックし、クイズに回答してください。
クイズの採点まで行わないと受講完了になりません。

付録３　「最近の情報セキュリティ事案の傾向と対策」

～ 情報セキュリティ教育～

最近の情報セキュリティ事案の傾向と対策

本教育の概要

本教育では、機構内外を問わず、世間一般で多く発生している情報セキュリティ事案に対する注意の喚起と対策の啓蒙を目的として、最近の情報セキュリティ事案について学習して頂きます。

＜ご注意＞

本教育の中で示している対策は、紹介した事案に対する重点対策です。
日頃から行なうべき総合的な対策については、イントラページの「PC等情報機器の情報セキュリティ実施手順書」を参照の上、実施してください。

最近の情報セキュリティ事案の傾向と対策

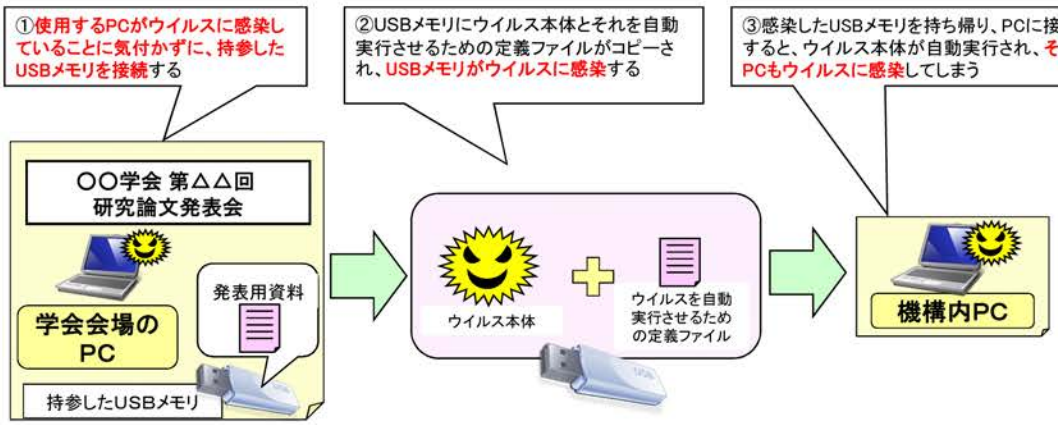
最近の情報セキュリティ事案の傾向と対策

第１章　ウイルス、スパイウェア、フィッシング等の傾向と対策

最近の情報セキュリティ事案の傾向と対策

１．１．１　USBメモリを媒介とするウイルス

USBメモリを介してコンピュータに感染するウイルスの被害が広まっています



感染してしまったPCでの被害の例

- PC内の情報（メールアドレス、アカウント、特定の種類のファイル等）を外部に送信される
- キーボードから入力した情報を外部に送信される
- 別のウイルスをダウンロードし、実行される

最近の情報セキュリティ事案の傾向と対策

１．１．２　USBメモリを媒介とするウイルス（対策）

被害を未然に防ぐための対策

信頼できるUSBメモリを、信頼できるPCのみに接続する

- USBメモリは、ウイルス対策ソフトの利用やセキュリティパッチの適用を適切に行なっている、**信頼できるPCのみに接続**するようにしてください。
- **セキュリティ対策の状態が不明なPCで使用したUSBメモリは、信頼できない**と考えてください。
- 学会の会場で主催者として**PCを提供したところ、そのPCが参加者のUSBメモリを媒介としてウイルスに感染**してしまった事例もあります。他人のPCやUSBメモリを借用する場合、十分な注意が必要です。

ウイルス対策ソフトウェアを導入し、USBメモリ内を検索する

- 原則として、**システム計算科学センターが整備しているウィルス対策ソフトウェアを使用**してください。 当該ソフトウェアを使用していれば、USBメモリ内のファイルにアクセスした時点でリアルタイム検知が行なわれます。 当該ソフトウェアは、機構イントラネットの「コンピュータ&ネットワーク利用」ページ内から入手してください。
- システム計算科学センターが整備しているウイルス対策ソフトウェアを使用できない場合は、**使用しているウイルス対策ソフトウェアでUSBメモリ内を検索するように予め設定しておくか、その都度の手動操作により、USBメモリ内を検索する**ようにしてください。

最近の情報セキュリティ事案の傾向と対策

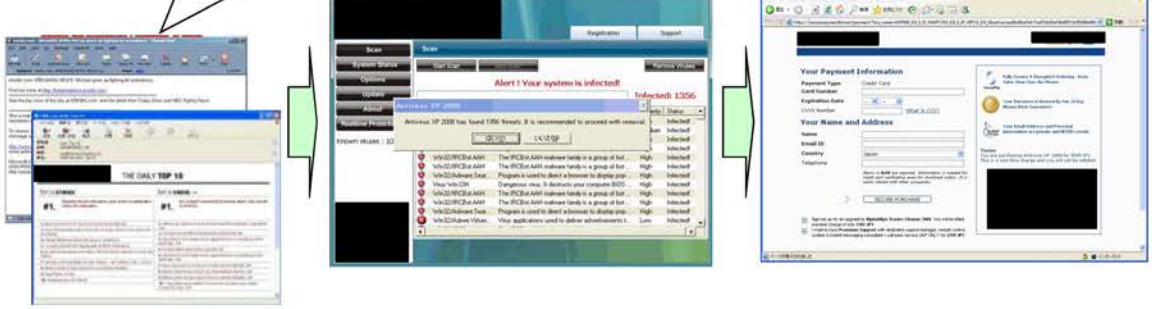
１．２．１　「偽セキュリティ対策ソフト」の押し売り

偽セキュリティ対策ソフトをインストールさせ、氏名やクレジットカード番号をはじめとする個人の機密情報を引き出そうとする被害の報告が寄せられています

①**迷惑メールに添付されたファイル**を不用意に開いてしまったり、**不正なソフトへのリンクが組み込まれたHTML形式のメールを参照**し、不正なソフトを組み込まれてしまう

②見覚えのないソフトが勝手にウイルスチェックを始め、「ウイルスに感染している」と虚偽の表示をし、対策ソフトの購入を促される

③画面表示に促されるままにクレジットカード番号などを入力して決済すると、**入力した情報を盗み取られ**てしまう



最近の情報セキュリティ事案の傾向と対策

１．２．２　「偽セキュリティ対策ソフト」の押し売り

このような偽セキュリティ対策ソフトが20種類以上出回っています

「偽セキュリティ対策ソフト」の押し売りを行なう主なソフトの名称

AdvancedPrivacyGuard	Alphawipe	AntiSpyware
AntiSpywareExpert	AntiVirus2008	AntiVirusXP2008
Doraibuhogo	DriveCleaner	HadodoraiBugado
NetTurboPro	SpyDajaba	SpywareRemover
SupaShuri	VirusRemover2008	VirusVanguard
WinAntiSpyware	WinAntiVirus	WinAntivirusPro2006
WinAntivirusPro2007	WinFixer	WinXProtector 2.1
XPAntivirus	XPSecurityCenter	

出典：情報処理推進機構(IPA)

最近の情報セキュリティ事案の傾向と対策

１．２．３　「偽セキュリティ対策ソフト」の押し売り（対策）

被害を未然に防ぐための対策

不審なメールは開かず削除する

送信元として、文部科学省や外務省などの政府機関や機構内を詐称している場合もあります

送信元が不明、件名や内容が意味不明、不審なファイルが添付されている、不審なURLがリンクされている等、**不審な電子メールを受信した場合には、すぐに削除**を行ってください。
迷惑メールに添付されてくるファイルを不用意に開かないことがウイルス感染を防ぐ上で最も重要です。

HTMLメールを送受信しないように設定する

ウイルス感染等を防ぐため、メール閲覧時に**HTMLメールをそのまま表示したり、HTMLメールを作成・送信しないよう設定**してください。

→【PC等情報機器の情報セキュリティ実施手順書　9.1】参照

ワンポイントアドバイス

＜HTML形式を使わずに重要な箇所を強調したい場合の記載例＞
HTML形式を使わないプレーンテキストと呼ばれる形式のメールで、強調したいフレーズがある場合の記載例をいくつか紹介します。参考にしてください。

＊参考表示＊	__参考表示__	“参考表示”	参 考 表 示	「参考表示」
『参考表示』	【参考表示】	■参考表示■	参考表示（←重要）	

信頼できるウイルス対策ソフトウェアを導入する

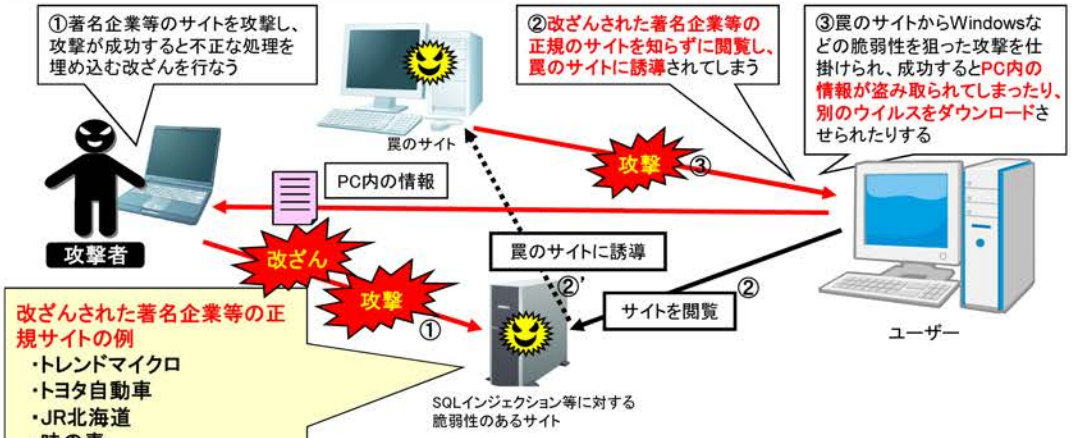
原則として、**システム計算科学センターが整備しているウイルス対策ソフトウェアを使用**してください。当該ソフトウェアは、機構イントラネットの「コンピュータ&ネットワーク利用」ページ内から入手してください。

→【PC等情報機器の情報セキュリティ実施手順書　6.2】参照

最近の情報セキュリティ事案の傾向と対策

1．3．1　改ざんされたサイトを閲覧して情報を盗まれる

著名企業等の正規のサイトが改ざんされ、閲覧しただけで攻撃に晒される場合があります



改ざんされた著名企業等の正規サイトの例

- ・トレンドマイクロ
- ・トヨタ自動車
- ・JR北海道
- ・味の素
- ・ニフティ
- ・サウンドハウス
- ・バンダイビジュアル
- ・クリエイティブメディア
- ・アイドラッグストアー
- ：

ユーザーPCでの被害の例

- ●PC内の情報（メールアドレス、アカウント、特定の種類のファイル等）を外部に送信される
- ●キーボードから入力した情報を外部に送信される
- ●別のウイルスをダウンロードし、実行される

最近の情報セキュリティ事案の傾向と対策

1．3．2　改ざんされたサイトを閲覧して情報を盗まれる（対策）

被害を未然に防ぐための対策

業務に不必要なサイトを閲覧しない

業務に不必要なサイトを閲覧する行為は、コンプライアンス上の問題もさることながら、情報セキュリティ上の脅威に晒される危険性が高いので行なわないこと。

メモ　情報システム管理室では、日頃からセキュリティ情報の収集・分析と対応を行なっており、サイト改ざん等の情報を入手した場合は、業務に必要とされる著名なサイト等であっても、安全が確認されるまで閲覧できないようにアクセス制限等を行う場合があります。

OSおよびソフトウェアのアップデートは、自動更新機能を活用する

自動更新機能が使えない場合は、セキュリティホール情報及びパッチ提供情報を随時確認し、必要な修正プログラムを適用してください。

→【PC等情報機器の情報セキュリティ実施手順書　6.1】参照

ウイルス対策ソフトウェアを導入する

原則として、システム計算科学センターが整備しているウイルス対策ソフトウェアを使用してください。当該ソフトウェアは、機構イントラネットの「コンピュータ&ネットワーク利用」ページ内から入手してください。

→【PC等情報機器の情報セキュリティ実施手順書　6.2】参照

パーソナルファイアウォール機能を有効にする

ネットワーク経由での攻撃からPCを保護するため、パーソナルファイアウォール機能を有効にしてください。

→【PC等情報機器の情報セキュリティ実施手順書　6.3】参照

最近の情報セキュリティ事案の傾向と対策

第２章　情報漏えいの傾向と対策

最近の情報セキュリティ事案の傾向と対策

２．１．１　ファイル共有ソフトとウイルスによる情報漏えい

ファイル共有ソフトをインストールされているPCがウイルスに感染したことに起因する情報漏えいが後を絶ちません

原子力機構の業務情報が流出－Winnyで

独立行政法人日本原子力研究開発機構の業務情報がインターネット上に流出していることが発覚した。

流出した業務情報は、東海研究開発センター核燃料サイクル工学研究所に建設中だった低放射性廃棄物処理技術開発施設(LWTF)に関する業務の電子メール、添付ファイルなどで、配管の材質や設計を検討した資料、施設の一部の図面、品質監査のチェックシートなども含まれていたが、核物質防護にかかわる情報はないという。

流出元となったのは、同機構の施設配管の施工・管理を請け負った契約会社「　　(本社・東京）の社員(51)の自宅個人ＰＣ。社員は、業務情報の一部を自宅に持ち帰って自宅個人ＰＣに保存していたが、そのＰＣにファイル共有ソフト「Winny」がインストールされており、「Winny」を介して業務情報がインターネット上に流出したという。

流出は、同機構への匿名の情報提供によって発覚した。

資料を持ち出す際には同機構の許可が必要だが、許可を得ていなかったという。同機構は「情報管理の一層の徹底を図っていく」とコメントしている。

ファイル共有ソフト

東京消防庁は１日
情報を含む内部文書

病院職員が患者情

医療法人社団 醫光会
ファイル共有ソフト
したことが判明した
流出が確認された個
電話番号、病名など
同病院リハビリ科の
にコピーして自宅に
ルスに感染している
ny」を経由して流出

明治安田生命、就職希望者 9000人の個人情報が流出

明治安田生命（本社・東京都）への就職を希望する大学生の住所や電話番号、一部の顔写真、面接評価、筆記試験の点数などを含む個人情報がファイル共有ソフト「Winny」のネットワークに流出したことが分かった。

個人情報のほかにも経営会議資料など、多数のデータが流出し、これらのファイルは、別のファイル共有ソフト「Share」のネットワークにも流れたり、ネット掲示板「2ちゃんねる」でも一部を紹介されたりしている。

同社によると、採用担当者が社内規則に反して個人情報を入れた会社のパソコンを自宅に持ち帰り、「Winny」の暴露ウイルスに感染したことから流出に至ったものとみられる。

敦賀原発の内部資料が流出 － 原電社員のパソコンから

日本原子力発電は28日、敦賀原子力発電所（福井県敦賀市）に勤務する男性社員(41)の所有するパソコンがウイルスに感染し、ファイル共有ソフト「Share」を介して同原発の内部情報などがインターネット上に流出したと発表した。

流出したのは、低レベル放射性廃棄物を処理するプラズマ溶融炉の温度に関するデータや会議の議事録など約480件のファイル。
核物質防護に関する機密情報は含まれていないという。

原電は、05年にもファイル共有ソフト「Winny」を介して同原発の定期検査工程などの内部資料を流出させている。

ファイルを自宅に持ち帰ることは社内規則で禁止されていた。

※掲載した事例は、マスコミ報道や関係機関等から公表された事実を元に再構成したものです。

最近の情報セキュリティ事案の傾向と対策

2．1．2　ファイル共有ソフトとウイルスによる情報漏えい（対策）

被害を未然に防ぐための対策

利用禁止ソフトウェアをインストールしない

次のページに示す**利用禁止ソフトウェアは、情報漏えいにつながる危険性があるため、インストールや利用を行なってはなりません。**

※PCの情報システム管理者は、インストールしたソフトウェアを管理台帳（インストール管理台帳、ライセンス管理台帳）を使って管理してください。

→【PC等情報機器の情報セキュリティ実施手順書　2.3】参照

最近の情報セキュリティ事案の傾向と対策

2．1．3　利用禁止ソフトウェアリスト

ファイル共有ソフトウェア	
総称名	個別プログラム名
Winny	Winny、Winny2
Gnutella	Limewire、Cabos、Gnutella、Gnutella2、BearShare、LimeWare、Shareaza、Acquisition、Newtella、ToadNode等
WinMX	WinMX
Share	Share、Safe-share
BitTorrent	BitTorrent、ABC、Azureus、BitSpirit、BitTornado、µTorrent、Qtorrent、Mainline、FlashGet(Ver1.8以降)等
eDonkey	eDonkey、eDonkey2000、MLdonkey、eMule、Overnet、OneMX、FlashGet(Ver1.8以降)等
Freenet	Frost、FUQID、FIW等
KaZaA	KaZaA
Kazza	Kazza、Kazza Lite、Grokster、FastTrack
PerfectDark	PerfectDark
Napster	Napster、OpenNap、FileNavigator、Xnap、2get、うたたね、iSwipe、SlavaDev/SlavaNap等
BitComet	BitComet
仮想ネットワーク構築ソフトウェア	
総称名	個別プログラム名
SoftEther	SoftEther、PacketiX VPN等

※利用禁止ソフトウェアには、**上記プログラムの互換ソフトウェア**も含みます。
※利用禁止ソフトウェアの一覧表は随時更新されます。
最新版の内容は、http://cnet-guide.jaea.go.jp/security/ngsoft.html で確認してください。

最近の情報セキュリティ事案の傾向と対策

２．２．１　PC等情報機器の盗難、紛失による情報漏えい

PC等情報機器の盗難、紛失による情報漏えい事案が随所で発生しています

宇宙航空研究開発機構（JAXA）で業務用ノートＰＣ盗難

宇宙航空研究開発機構(JAXA)は、調布航空宇宙センターの執務室から業務用ノートＰＣ１台が盗難に遭ったことを発表した。
盗難に遭ったＰＣには、設計図などの技術的な機密情報は含まれていないが、研究員採用の応募者７０名の個人情報が保存されており、該当者に連絡をとって謝罪するという。
実験施設などを一般公開していた4月20日に公開対象ではない建物に出入りする不審者が目撃されており、届け出を受けた警察と同機構で関連を調べている。

原子力関連工事の現地業務用パソコン盗難

三菱重工業は、原子力関連工事のため出張中の同社の社員が、4月25日に作業用パソコン及び携帯電話の盗難に遭ったと発表した。

盗難に遭ったパソコンには、現地業務に必要なデータを保存していたが、核物質防護に関する情報等の機微情報は含まれていなかったという。
また、盗難・紛失等に備え、データ暗号化の措置を講じていたため、情報漏えいに繋がる可能性は低いとのこと。

同社は、今回の盗難の発生を真摯に受け止め、再発防止対策の徹底に努めていくとコメントしている。

スターバックス、ＪＲ大阪駅でＰＣ置き引き被害 約5700名の個人情報が流出か

スターバックスコーヒージャパンは、同社の従業員が4月16日、JR大阪駅で置き引きの被害に遭い、ノートPC1台を紛失したと発表した。
ノートPCには、採用説明会に応募した4842名の学生と従業員897名の個人情報が記録されているという。
顧客情報は含まれていない。
同社は学生に報告とお詫びを記した文書を郵送した。

出展者各位

【注意】展示会場でのパソコン盗難（置き引き）が多発

平成20年3月以降に開催された4つの展示会において、8件計33台のパソコン盗難が発生しました。
いずれの事案も目を離したわずかな時間に置き引きされており、プロの窃盗団による犯行の可能性が高く、今後の展示会等において十分な警戒が必要です。

800名分の成績と研究データが入ったノートＰＣ盗難（京都大学）

京都大学は、理学研究科のノートPC1台が盗難に遭ったことを明らかにした。PCには延べ800名分の成績および研究データなどが保存されていたという。
6月16日の午前10時から午後5時半のあいだに侵入した何者かによる犯行と思われ、同大学は、警察に被害届を提出した。
学生に事情を説明するとともに、関係者に施錠の徹底を求めるなど、防犯体制の強化と再発防止を目指すという。

※掲載した事例等は、マスコミ報道や関係機関等から公表された事実を元に再構成したものです。

最近の情報セキュリティ事案の傾向と対策

２．２．２　PC等情報機器の盗難、紛失による情報漏えい（対策）

情報漏えいを防ぐための対策

情報機器管理台帳を作成し、PC等情報機器の供用状況と格納された情報を把握する

- 全てのPC等情報機器については、「情報機器管理台帳」を供用課室にて整備・保管し、所在等の供用状況を把握すること。なお、記載方法については、次頁の記載例を参照のこと。
- PC等情報機器は、購入金額や供用状況によらず全て記載すること。CD-R、DVD等については、秘密文書を記録したものについては対象とすること。
- PC等情報機器の供用状況や格納する情報が変更になった場合は、都度更新すること。
- PC等情報機器のうち、未使用・保管中のものはデータを消去又は初期化を行うとともに、消去記録を本台帳に記載し、課室情報セキュリティ責任者の確認を得ること。
- 少なくとも年一回、供用課室にて本台帳に基づき現品を確認し、必要に応じて記載事項を修正すること。

→【PC等情報機器での情報セキュリティ実施手順書　3.1】参照

最近の情報セキュリティ事案の傾向と対策

2．2．3　情報機器管理台帳 記載例

情報機器管理台帳

記載例

機器番号	機種名（製品名、型式等）	機器種別	個体識別番号（MACアドレス等）	購入日	使用者（部外者の場合、所属も明記）	使用又は保管場所	供用状況	情報消去の確認			格納情報	記事（用途等）
								消去方法	日付	確認者		
320501-B-00001	IBM ThinkPad X31	ノート型PC	00.00.00.17.94.47	2003.02.20	外部太郎（X社）	情報交流棟南ウィング 313号室	廃棄済	消去用ソフト	08.03.21	機構太郎	機構外秘	
シ管-0000001	I-O DATA ED-S2/512	USBメモリ	W60628	2008.04.30	機構太郎	情報交流棟南ウィング 313号室	使用中				非公開	出張時用

記載項目について

① 機器番号　：資産物品　：資産管理番号を記載する。
資産物品以外：［部署文字］-［部署内一連番号］を記載する。

② 機種名　：機種名、製品名、型式等を記載する。

③ 機器種別　：記入欄をクリックし、プルダウンメニューから該当する機器種別を選択する。

④ 個体識別番号　：MACアドレス、製造番号等、個体を識別できる番号を記載する。

⑤ 購入日　：取得年月日または納品年月日を YYYY.MM.DD形式で記載する。

⑥ 使用者　：使用者の氏名を記載する。部外者の場合、会社名等の所属も記載する。

⑦ 使用又は保管場所：拠点、建家、部屋番号等、場所がはっきり分かるように具体的に記載する。

⑧ 供用状況　：記入欄をクリックし、プルダウンメニューから該当する供用状況を選択する。

⑨ 情報消去の確認
消去方法　：記入欄をクリックし、プルダウンメニューから該当する消去方法を選択する。
日付　：情報の消去を確認した年月日を YYYY.MM.DD形式で記載する。
確認者　：消去を確認した情報セキュリティ責任者の氏名を記載する。

⑩ 格納情報　：記入欄をクリックし、プルダウンメニューから該当する情報区分を選択する。

⑪ 記事　：使用状況が「使用中」の場合、主な用途を記載する。

最近の情報セキュリティ事案の傾向と対策

2．2．4　PC等情報機器の盗難、紛失による情報漏えい（対策）

職員等が不在となる事務室等は施錠する

PC等情報機器が設置されている事務室等から**職員等が不在となる場合には、短時間であっても施錠する**こと。

→【PC等情報機器での情報セキュリティ実施手順書　3.2】参照

PC等情報機器が持ち出されないようにする

- PC等情報機器は、セキュリティワイヤー、施錠等による**盗難防止策を施す**こと。
- 使用時は、**常に携帯するか、目の届くところに置く**こと。
- **未使用時は、施錠できる棚や引き出しなどに保管する**こと。なお、使用予定が当面ないPC等情報機器は、データ消去又は初期化を行うとともに、その旨を「情報機器管理台帳」に記載して、情報セキュリティ管理者の確認を得ること。なお、データ消去は、「ごみ箱」にドロップして空にしても完全には消去できないことから、専用ソフトウェア等を用いて消去すること。

【製品例】データ消去ソフトウェア
・ターミネータ 8.0 シリーズ（FINAL DATA製）
・完全抹消PRO（Jungle製）

→【PC等情報機器での情報セキュリティ実施手順書　3.3】参照

最近の情報セキュリティ事案の傾向と対策

2．2．5　PC等情報機器の盗難、紛失による情報漏えい（対策）

PC等情報機器は認証機能付きのものを使用する

PC等情報機器は**認証機能（パスワード、指紋認証等）付きのものを選定し、その機能を利用する**こと。

→【PC等情報機器での情報セキュリティ実施手順書　3.4】参照

格納する情報は必要最小限にする

PC等情報機器に**格納する情報は必要最小限にする**こと。

→【PC等情報機器での情報セキュリティ実施手順書　3.5】参照

情報漏えいに備え、格納する情報は暗号化する

課室情報セキュリティ責任者が、**暗号化が必要と判断した情報は必ず暗号化する**こと。

【製品例】暗号化ソフトウェア
- CompuSec（CE-infosys製）
- SecureDoc（WinMagic製）

【製品例】暗号化機能付きのUSBメモリ
- EasyDisk（IO-DATA製）
- RUF-SC（BUFFALO製）
- Container（ed-contrive製）

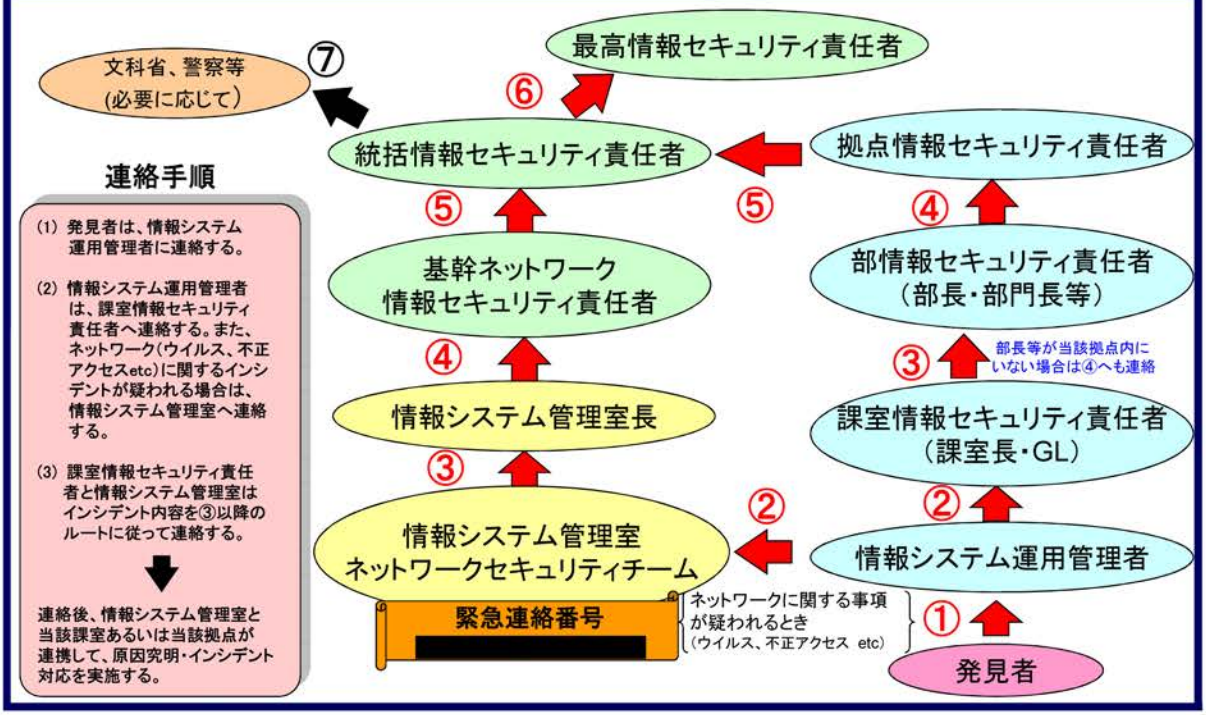
→【PC等情報機器での情報セキュリティ実施手順書　3.6】参照

最近の情報セキュリティ事案の傾向と対策

第３章　情報セキュリティインシデント発生時の対応

最近の情報セキュリティ事案の傾向と対策

3．1　情報セキュリティインシデント発生時の連絡手順



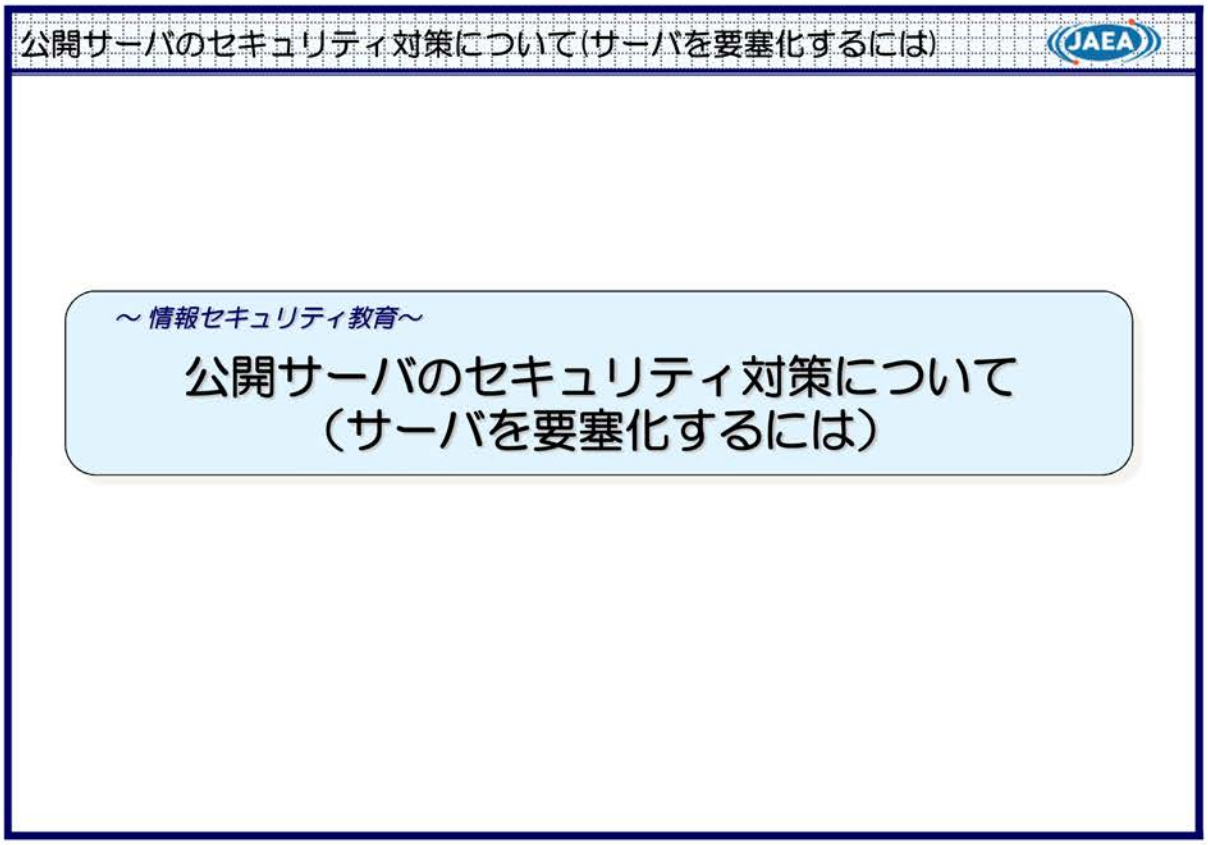
最近の情報セキュリティ事案の傾向と対策

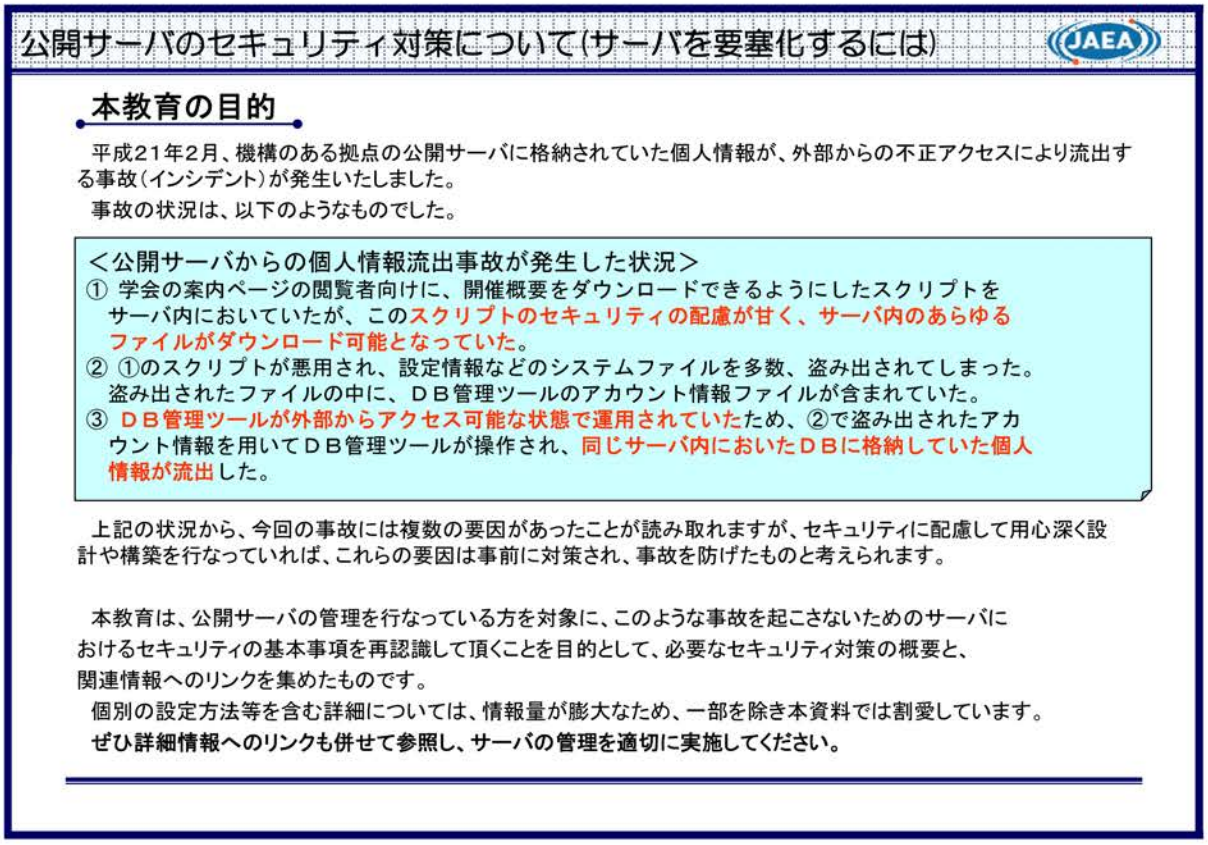
3．2　セキュリティ緊急Topics（機構イントラページ）

※最新のセキュリティ情報を、機構イントラネットの「**セキュリティ緊急Topics**」にて公開しています。随時ご確認ください。
http://intra.jaea.go.jp/ トップページ参照

以上で学習は終了です。
引き続き、問題に対する回答を行ってください。

付録４　「公開サーバのセキュリティ対策について（サーバを要塞化するには）」

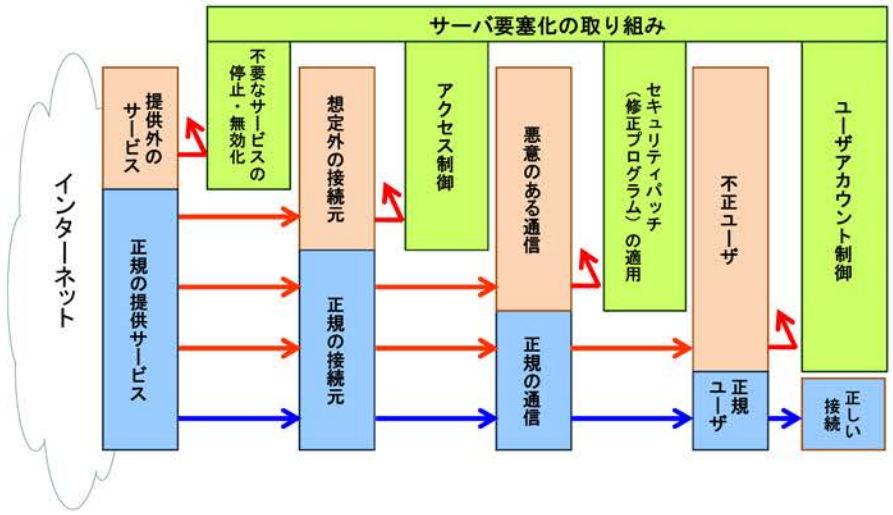




公開サーバのセキュリティ対策について(サーバを要塞化するには)

サーバに必要なセキュリティ対策の全体イメージ

・セキュリティリスクを最小限にする。
・脆弱な部分(または脆弱になる可能性のある部分)を減らす。
・リスクの内容に応じて段階的な要塞化を実施することで、堅牢なサーバ環境を確立する。



公開サーバのセキュリティ対策について(サーバを要塞化するには)

目次

公開サーバのセキュリティ対策について(サーバを要塞化するには)

1．不要なサービスの停止・無効化、アクセスを制御する

公開サーバのセキュリティ対策について(サーバを要塞化するには)

1．不要なサービスの停止・無効化、アクセスを制御する

1.1　状態の確認、不要なサービスの停止・無効化

1)デフォルトの設定でOSをインストールすると、いろいろなサービスが起動するようになっているので、現在の状態を確認する。

・Unix系のOSの場合、「ps」コマンドでサービス、「netstat -a」コマンドでポート状態の確認が可能である。
・Windows系の場合、管理ツールのサービスやタスクマネージャでサービス、「netstat -an」コマンドでポートの状態の確認が可能である。

2)不要なサービスの停止・無効化を行うには、

・現状を確認する
　実行プロセスの確認（psコマンド）
　待機ポートの確認（netstatコマンド）
・不要なサービスを特定する
・不要なサービスを停止する
　Step.1：プロセスの停止
　Step.2：起動スクリプトの無効化
　Step.3：inetd.conf(xinetd.conf)の見直し

3)設定変更後、停止／無効化したサービスが起動されないか、他に不要なポートが開いていないか確認する(自動起動の設定もあわせて確認)。

・Unix系であれば「inetd」「rc.d」の設定、Windowsであれば管理ツールのサービスの設定を確認する。

公開サーバのセキュリティ対策について(サーバを要塞化するには)

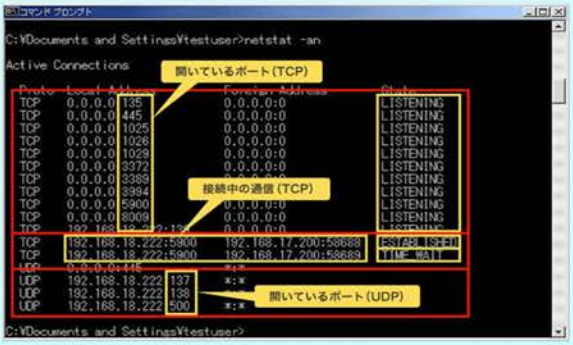
1．不要なサービスの停止・無効化、アクセスを制御する

Linuxサーバでの停止方法例

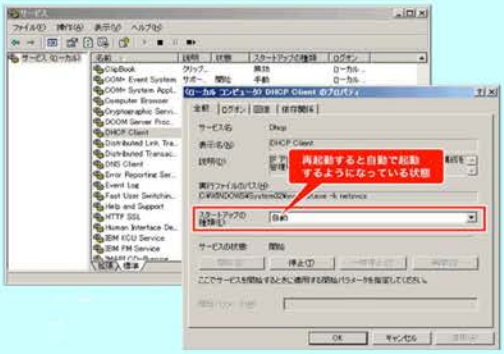
Linuxでのサービス停止は、
- サービスの一覧を表示する。 `# chkconfig --list | less`
- デーモンを停止するにはroot権限でコマンドを実行する。 `# /etc/rc.d/init.d/デーモン名 stop`
- サーバー起動時に自動的に起動しないようにする。 `# chkconfig サービス名 off`

Windowsサーバでの停止方法例

■ netstatコマンドを実行した画面例(Windows)



■ Windows管理ツールのサービス 画面例



公開サーバのセキュリティ対策について(サーバを要塞化するには)

1．不要なサービスの停止・無効化、アクセスを制御する

Linuxサーバの通常の運用では不要と思われるサービス一覧

サービス名	
netfs	/etc/fstabに記述してあるNFS、SMB、NCPなどのネットワークファイルシステムをマウントする
apmd	電源管理を行うAPMデーモン
atd	atコマンドにより、時間を指定してプログラムを実行する
gpm	コンソールでのマウスエミュレータ
autofs	自動でマウントするデーモン
irda	IrDA赤外線通信デバイスの制御サービス(デフォルトoff)
Isdn	ISDN用接続スクリプトサービス。ISDNを使用しているのでなければ停止する。
portmap	リモートプロシージャコールのポートを管理(NFSサーバーで利用)
nfs	ファイル共有を行うNFS(Network File System)サーバー(デフォルトoff)
nfslock	NFSでファイルのロックを行う
sendmail	電子メールサーバー。他メールサーバーを使用しているならば停止させる。
rhnsd	RedHatに接続し、アップデートがないか定期的にチェックする
xfs	XFree86用のフォントサーバー。X-Windowを使用していなければ不要。
canna	カナ漢字変換
FreeWnn	カナ漢字変換
Lpd	ラインプリンタデーモン。プリントサーバーでないのなら不必要。
chargen-udp	デバックなどで利用するキャラクタージェネレーター[UDP](デフォルトoff)
Rsync	ファイルの同期を行う(デフォルトoff)
Chargen	デバックなどで利用するキャラクタージェネレーター[TCP](デフォルトoff)
daytime-udp	日時を通知する[UDP](デフォルトoff)
Daytime	日時を通知する[TCP](デフォルトoff)
echo-udp	pingコマンドへの応答[UDP](デフォルトoff)
Echo	pingコマンドへの応答[TCP](デフォルトoff)
time-udp	timeプロトコル[UDP](デフォルトoff)
Time	timeプロトコル[TCP](デフォルトoff)
dbskkd-cdb	RedHatに接続し、アップデートがないか定期的にチェックする
sgi_fam	ファイルやディレクトリの変更を知らせるサービス。使用していないのであれば停止させておく。デフォルトではon

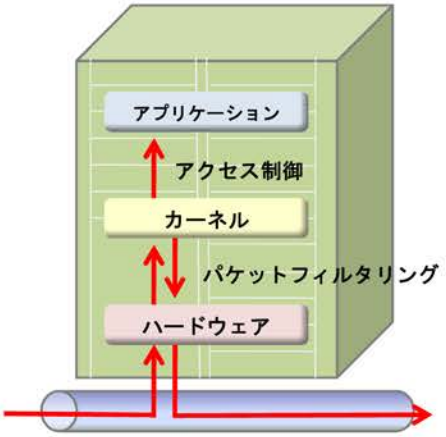
公開サーバのセキュリティ対策について(サーバを要塞化するには)

1．不要なサービスの停止・無効化、アクセスを制御する

1.2　アクセスの制御

不要なサービスの停止・無効化を行った上で、よりアクセス制御を強化したい場合は、パケットフィルタリング(iptables、tcp-wrapper等)を利用する。
パケットフィルタリングは、「カーネル」と呼ばれるOSの基礎部分でパケットの許可／非許可を決定するので、アクセス制御ソフトを利用するよりも高速に処理でき、細かい制御も可能である。多くのOSでは、カーネルが最初から持っている機能か、専用のソフトウェアをカーネルに組み込むことで、パケットフィルタリングを実現可能である。

サーバ内部にてデータが処理される仕組み



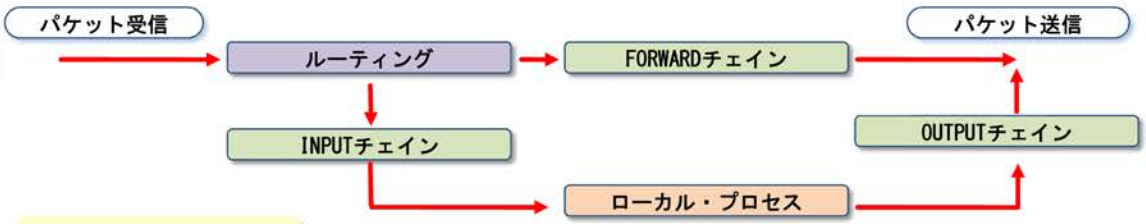
公開サーバのセキュリティ対策について(サーバを要塞化するには)

1．不要なサービスの停止・無効化、アクセスを制御する

iptablesによるパケットフィルタリング

iptablesではIPアドレスやプロトコル、ポート、フラグメントなどで制限をかけることが可能である。さらに、送信先、送信元なのかといった判断もできる。これを行うのが、filterテーブルに含まれるFORWARD、INPUT、OUTPUTという3つのチェインである。

iptablesによるパケットフィルタリングの流れ



詳細情報へのリンク

- iptables
  http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/ja/ref-guide/ch-iptables.html
- tcp_wrapper
  http://www.itmedia.co.jp/help/tips/linux/l0044.html

公開サーバのセキュリティ対策について(サーバを要塞化するには)

2．OSや各種サーバソフトのセキュリティパッチ（修正プログラム）を適用する

公開サーバのセキュリティ対策について(サーバを要塞化するには)

2．OSや各種サーバソフトのセキュリティパッチ（修正プログラム）を適用する

セキュリティパッチの適用の必要性

OSや各種サーバソフトの脆弱性は日々発見されており、それらの脆弱性を狙う攻撃の手法やウイルスが増えている。そのほとんどは、修正プログラムを正しく適用していれば防ぐことが可能である。

セキュリティパッチの適用

OSや各種サーバソフトのインストール後、それらのバージョン確認を行う。
バージョン確認の例として、RedHat Linux等は「rpm」コマンドがあり、rpmコマンドを利用してインストールされているバージョン等の確認が可能である。
また、Windowsであれば、Windows Updateや「プログラムの追加と削除」の画面を利用して確認が可能である。
最新版のインストールパッケージでも修正されていない既知のセキュリティホールを塞ぐために、製品ベンダから提供されている修正プログラムをOSや各種サーバソフトに適用する。

公開サーバのセキュリティ対策について(サーバを要塞化するには)

2．OSや各種サーバソフトのセキュリティパッチ（修正プログラム）を適用する

詳細情報へのリンク

・パッチ管理

[Microsoft Baseline Security Analyzer (HfNetChk)]
http://www.microsoft.com/japan/technet/security/tools/tools/mbsahome.asp

[Microsoft Software Update Services(SUS)]
http://www.microsoft.com/japan/windows2000/windowsupdate/sus/default.asp

・Solaris パッチの管理用ツール

http://docs.sun.com/db/doc/817-2462/6mi4fl28n?l=ja&a=view

公開サーバのセキュリティ対策について(サーバを要塞化するには)

3．ユーザおよびアクセス権を管理する

公開サーバのセキュリティ対策について(サーバを要塞化するには)

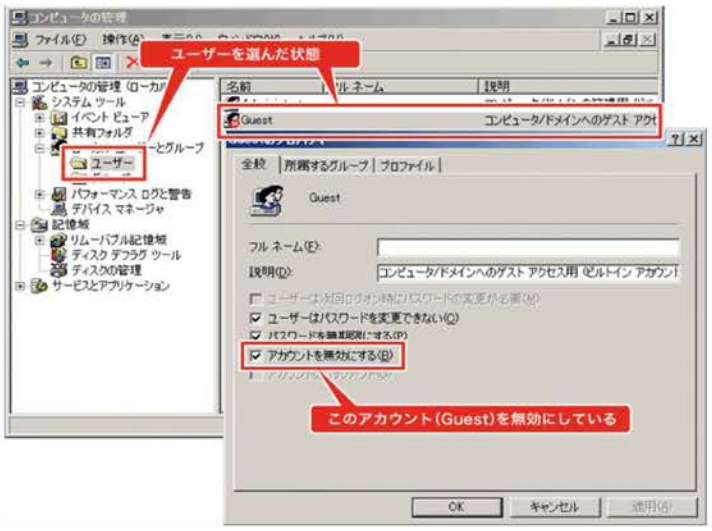
3．ユーザおよびアクセス権を管理する

ユーザ管理

ユーザに応じて適切なアクセス権を設定することで、予想外の動作、人的なミスの発生 を抑えられる。

不要なユーザアカウント等は削除する。また、管理者権限でログインするような運用は避ける。

ユーザ管理の例(Windows)



公開サーバのセキュリティ対策について(サーバを要塞化するには)

3．ユーザおよびアクセス権を管理する

管理者権限を管理する

Unix系のOSであれば「sudo」コマンド等にて管理者権限の一時利用ができる。root のパスワードを共有する必要がなくなり、利用時のログを記録することが可能である。ほかには、PAM(Pluggable Authentication Module)を利用する方法もある。

Windowsであれば、「コンピュータの管理」からユーザの管理を行い、不要なユーザや不要なユーザグループは無効にするか、削除する。一般のユーザが管理者権限を利用する場合は、「runas」コマンドを利用するなどのルール決めも有効な手段である。

ディレクトリやファイルのアクセス権の管理

ディレクトリやファイルのアクセス権において、管理者以外のユーザにも必要以上の権限が与えられていることがあります。各ユーザに対し、必要最小限の権限のみに設定を見直す。また、不要な共有資源については、共有状態を解除する。

詳細情報へのリンク

「runas」コマンド
http://itpro.nikkeibp.co.jp/free/NT/WinKeyWord/20040805/1/runas.shtml

公開サーバのセキュリティ対策について(サーバを要塞化するには)

4．パスワードを管理する

公開サーバのセキュリティ対策について(サーバを要塞化するには)

4．パスワードを管理する

安易なパスワードを設定しない

パスワードに対する攻撃方法で代表的なものは、「辞書攻撃」と「ブルート・フォース攻撃」である。

いずれもパスワード入力を何通りも試して、サービスへのログインを試みるものであるが、安易なパスワードを設定していると短時間で解読されてしまう。

例えば数字4桁のパスワードの種類は1万通り。クラッカがブルート・フォース攻撃で最大1万回試行すれば、パスワードは解読できてしまう。数字や文字などの組み合わせが多くなれば、それだけ解読しにくくなる。また、英大小文字の組み合わせ、桁数を増やすのも効果が大きい。

安易なパスワードは容易に解読されてしまう

公開サーバのセキュリティ対策について(サーバを要塞化するには)

4．パスワードを管理する

パスワードの管理

機構においては、「PC等情報機器の情報セキュリティ実施手順書」にてパスワード管理方法を以下のとおり定めている。最低限これを順守することは当然のこと、可能であれば、パスワードの長さをより長くする等、より強固なパスワードを用いること。

・パスワードの設定
(1) 2つ以上のアルファベットと1つ以上の非アルファベットを含めること。
(2) 4つの異なる文字を含めること。
(3) 辞書にある言葉や一般的な言葉を単独で使用しないこと。

・パスワードの変更管理
(1) パスワードの長さ:8桁以上
(2) パスワードの有効期間:90日以内
(3) 連続して同じパスワードを使用しないこと。

公開サーバのセキュリティ対策について(サーバを要塞化するには)

5．不要なファイル、プログラムを削除する

公開サーバのセキュリティ対策について(サーバを要塞化するには)

5．不要なファイル、プログラムを削除する

不要なファイル、プログラムを削除する

OSや各種サーバソフトをインストールすると、サンプルプログラムも一緒にインストールされることがある。サンプルプログラムの中には脆弱性が存在するものもあるため、攻撃の対象となってしまう可能性がある。テストで使用したファイルやプログラムがアクセスできる状態になっていると、このプログラムの脆弱性を利用した攻撃を受けてしまう可能性がある。このため、不要なファイルやプログラムはサーバ上から削除するか、アクセスできない場所に移動する必要がある。

また、ファイルの改ざんやファイルの追加、削除の部分まで管理する「tripwire」等のツールもあるのでこれを利用するのも一つの方法である。

詳細情報へのリンク

・tripwire
http://www.tripwire.co.jp/

公開サーバのセキュリティ対策について(サーバを要塞化するには)

6．ログを管理する

公開サーバのセキュリティ対策について(サーバを要塞化するには)

6．ログを管理する

ログの管理

重要なファイルへのアクセス履歴やログイン履歴、その他セキュリティに関する警告やエラーメッセージがログとして適切に記録されるように設定します。これらを記録することにより、障害やセキュリティ事案の原因の特定や、攻撃の兆候を把握出来たりする。

ログの管理の留意点
・必要な情報を収集するようにログを設定する
・ログサーバーで集中管理
・ログを安全に保管する
・ツールを利用して分析する
・詳細な監査ログ
・時計の同期(照合のため)
・普段からチェックし正常時を把握しておく

ログを管理するツールとして、「syslog」が代表的である。なお、ログを解析するツールとしては「swatch」「logsurfer」等がある。

詳細情報へのリンク

・syslog
http://www.infoscience.co.jp/technical/press/index.html
・swatch
http://sourceforge.net/project/showfiles.php?group_id=68627
・logsurfer
http://sourceforge.net/projects/logsurfer

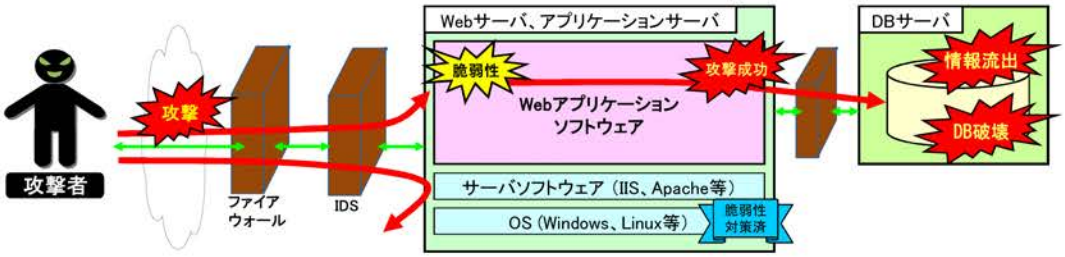
公開サーバのセキュリティ対策について(サーバを要塞化するには)

7．Webアプリケーションに対する攻撃の基礎知識

公開サーバのセキュリティ対策について(サーバを要塞化するには)

7．Webアプリケーションに対する攻撃の基礎知識

Webサーバのセキュリティ対策としては、一般にファイアウォール、IDS(不正侵入検知システム)、ウイルス対策などがある。
一般的に広く使われているWebアプリケーションであれば、IDS等で攻撃パターンの検知・遮断等により、攻撃を防ぐことが可能である。
しかし、**Webアプリケーションのほとんどが独自に開発されたものであるため、一般的なパターンを検知するだけでは不十分**なのが現状である。
従って、**Webサーバの管理者は、Webアプリケーションへの攻撃手法とその対策方法を熟知し、十分な対策を行なうことが重要**である。

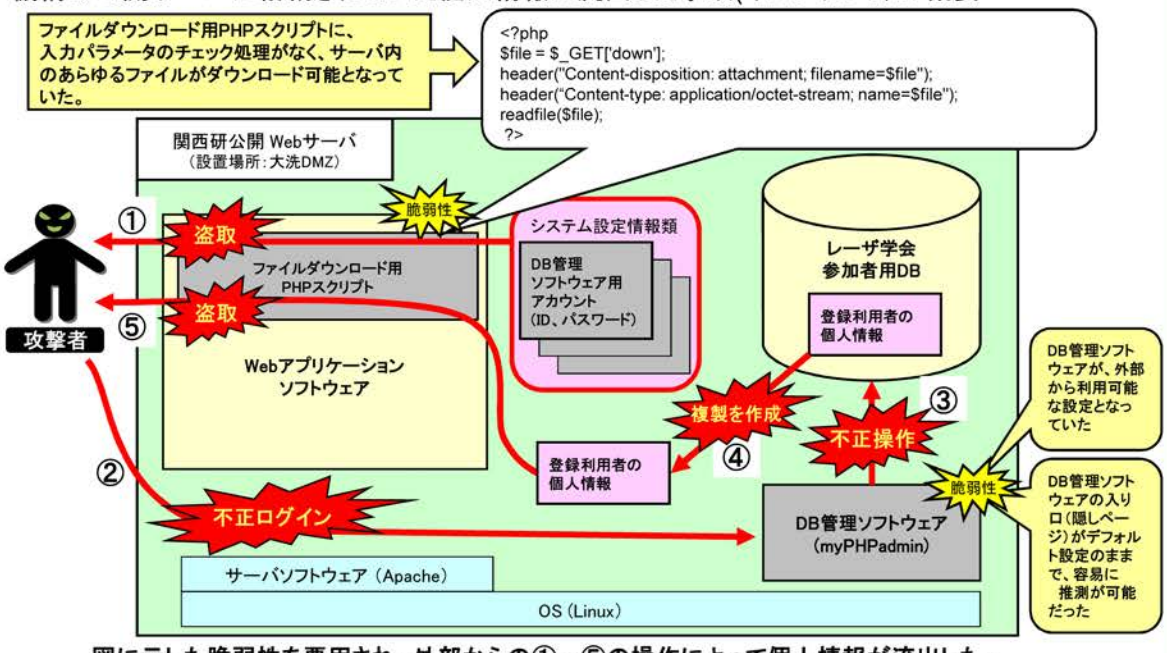


**OSやサーバソフトウェアの脆弱性対策をしていても、
Webアプリケーションソフトウェアに脆弱性があると攻撃を防ぎきれない**

公開サーバのセキュリティ対策について(サーバを要塞化するには)

7．Webアプリケーションに対する攻撃の基礎知識

機構の公開サーバに格納されていた個人情報が流出した事故(インシデント)の概要



図に示した脆弱性を悪用され、外部からの①～⑤の操作によって個人情報が流出した。

公開サーバのセキュリティ対策について(サーバを要塞化するには)

7．Webアプリケーションに対する攻撃の基礎知識

Webサーバに対する代表的な攻撃手法と対策方法

攻撃手法	攻撃内容	対策方法
フォームフィールドの改ざん	①hiddenフィールドに重要な値がある時の改ざん ②Select値の嫌がらせ改ざん ③入力確認フォームの改ざん(の可能性) ④Cookieに重要なデータがあるときの改ざん	①hiddenフィールドには重要な値を載せない ②入力値のサーバ側、JavaScriptチェック ③上記②チェック、改ざんされたときの確認方法の確立 ④Cookieには重要な値を載せない
クロスサイトスクリプティング	①脆弱性を利用した別サイトのCookieの搾取 ②脆弱性を利用した偽ページへの誘導(フィッシング)	①②サニタイジング
セッションハイジャック	①セッションID搾取,盗聴による正規ユーザなりすまし ②セッションフィクセイション(偽IDを使わせる)	①セッションIDを推測されないように作成、盗聴させない
SQLインジェクション	①ユーザ認証の回避(ユーザパスワード無効) ②ユーザ認証テーブルの削除、改ざん	①②サニタイジング、準備済みSQL文の利用、エラーメッセージなどにヒントとなるようなものを含めない
OSコマンドインジェクション	①Webを経由したOSコマンド不正実行	①入力チェック、サニタイジング OSを起動できるような危険な関数は使わない
強制的ブラウズ	①URLを想定したブラウズによる重要コンテンツ搾取 ②ディレクトリ参照可能状態による重要コンテンツ搾取 ③フレームにおけるアクセス制御ミスによるアクセス ④HTML内の不適切(親切過ぎる)なコメントによる情報入手	①重要なデータを公開ディレクトリ上に置いておかない。 ②ディレクトリ参照の不可設定 ③アクセス制御テスト、フレームはなるべく使わない ④HTMLコメントはHTML同様見られることを考慮する
ディレクトリトラバーサル	①相対パス記法による非公開ファイルの搾取 ②動的にファイルを呼び出すサイトでの相対パス記法	①パスやURLに対するパラメータチェック ②ホームディレクトリの隔離、Webサーバでの設定
不適切なエラーハンドリング	①不適切なログインエラー表示による推測 ②HTTPエラー表示によるWebサーバ等の情報収集	①エラーメッセージにヒントとなる情報を与えない ②標準のエラー表示を修正し情報を与えない
バッファオーバーフロー	①C/C++コード時、想定サイズ以上のデータをバッファに送り込み、特別なプログラムを実行	①危険な関数を使わない、既知の脆弱性に対するパッチ、変数のサイズを意識、最小限の特権でプロセスを実行
バックドアとデバッグオプション	①バックドア設置による外部からの不正アクセス ②デバッグ時のオプション設置を見つけ利用	①不正なポートが使われているかの確認 ②デバックモードの除去、認識
Getの不適切なリクエストストリング	①リクエストストリングのURL欄表示やログ(Referrerの記録)による盗み見	①Getは使用しないほうが良い、利用するときは重要なデータをリクエストストリングに出さない

公開サーバのセキュリティ対策について(サーバを要塞化するには)

7．Webアプリケーションに対する攻撃の基礎知識

詳細情報へのリンク

- **Webアプリケーションに起こりうる問題**
  http://www.ipa.go.jp/security/awareness/vendor/programmingv2/web.html
- **セキュアなWebサーバーの構築と運用**
  http://www.ipa.go.jp/security/awareness/administrator/secure-web/index.html
- **Web アプリケーション セキュリティの強化**
  http://msdn.microsoft.com/ja-jp/library/cc785499.aspx

公開サーバのセキュリティ対策について(サーバを要塞化するには)

8．Webアプリケーションの作成時に考慮すべき点

公開サーバのセキュリティ対策について(サーバを要塞化するには)

8．Webアプリケーションの作成時に考慮すべき点

調達を行なう際のセキュリティ要件の提示

情報システムの構築等を調達する場合には、情報セキュリティ対策を委託先に行わせるため、セキュリティ要求仕様を調達仕様書に記載し、委託先からの提案仕様を十分に審査することが、適切な情報セキュリティ対策を実現する上で重要である。

セキュリティ要求仕様の考え方や作成手順については、内閣官房情報セキュリティセンターが作成した以下の資料に記載されています。ダウンロードして参考にしてください。

詳細情報へのリンク

・情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書
（内閣官房情報セキュリティセンター）
http://www.nisc.go.jp/active/general/pdf/dm6-07-071_manual.pdf

公開サーバのセキュリティ対策について(サーバを要塞化するには)

8．Webアプリケーションの作成時に考慮すべき点

Webアプリケーション検査

Webアプリケーションの脆弱性のほとんどは、開発時のささいなミスから生じる。ブラウザから送信されるデータは、基本的にユーザー側で操作することが可能なため、本来、サーバ側ではユーザーのブラウザから送信される入力はすべて疑って処理を行うべきである。しかし、ブラウザから送信される入力のチェックやサニタイジング(無効化)を行わずに処理させてしまうことにより、意図しない動作を行ってしまうことがある。
また、サービスをリリースする前に、脆弱性がないかをチェックする必要がある。検査の手法としては、「BlackBoxテスト」「WhiteBoxテスト」「GlassBoxテスト」の3種類がある。

◆ **BlackBoxテスト**
Webアプリケーションの内部構造がわからない状態で検査を行う方法。用意された機能が仕様を満たしているか、外部からテストパターンを送ることによって調べる。 公開サーバを対象に、情報システム管理室が実施しているテストは、これに相当している。

◆ **WhiteBoxテスト**
Webアプリケーションのソースコードを直接見ることにより、検査を行う方法。inputに対する挙動を確実に追えるので、正確かつ効果的な検査を行うことができる。一般的に開発者(委託した場合は委託先)側が実施する。

◆ **GlassBoxテスト**
WhiteBoxテストとBlackBoxテストの両方の検査を行う方法

詳細情報へのリンク

・**ソフトウェアテスト基本テクニック**
http://gihyo.jp/dev/serial/01/tech_station/0003
・**セキュア・プログラミング講座**
http://www.ipa.go.jp/security/awareness/vendor/programming/index.html

公開サーバのセキュリティ対策について(サーバを要塞化するには)

8．Webアプリケーションの作成時に考慮すべき点

詳細情報へのリンク（セキュリティ対策情報を含む総合サイト）

・**CERT／CC**
http://www.jpcert.or.jp/

・**IPA**
http://www.ipa.go.jp/

・**Microsoft**
http://www.microsoft.com/japan/technet/security/default.mspx

・**Red Hat Linux**
http://www.jp.redhat.com/support/errata/

付録５　「これだけはぜひ！最低限のコンピュータウイルス対策」

～ 情報セキュリティ教育～

これだけはぜひ！

最低限のコンピュータウイルス対策

本教育の概要

パソコンがコンピュータウイルスに感染すると、情報の漏えいや滅失、感染経路や影響範囲の調査及び復旧作業に伴う業務の遅延等、深刻な影響を受けてしまいます。

本教育は、総合的な情報セキュリティ対策の中から、コンピュータウイルスへの感染防止にテーマを絞り、全てのパソコン等で必ず行なうべきコンピュータウイルス対策について再徹底を図ることを目的としています。

目次

これだけはぜひ！
最低限のコンピュータウイルス対策

はじめに

最近のコンピュータウイルス（以下、ウイルス）は、個人情報、インターネット上のサービスを利用するためのアカウント（IDやパスワード）、クレジットカードに関する情報等の盗取を目的としたものが急増しています。

こうしたウイルスは、長期間活動できるようにパソコン内に巧妙に潜伏することが特徴で、感染してもなかなか気づかず、いつの間にか被害に遭うという、悪質なものになっています。

感染経路も変化しており、数年前までは電子メールを介して感染するものがほとんどでしたが、最近では、インターネットのウェブサイトやUSBメモリを介して感染するものが増え、より一層、身近な脅威となっています。

こうしたことから、ウイルス対策の重要性は高まる一方です。

本教育は、本編の他、新たな手法を取り入れた操作手順編を用意し、2本建ての教材構成としています。

これは、機構内のアンケートで多く寄せられた「操作方法等を具体的に分かり易く説明して欲しい」というご要望に応えたものです。

ぜひご活用ください。

これだけはぜひ！
最低限のコンピュータウイルス対策

第１章　当機構で検知が多いコンピュータウイルス

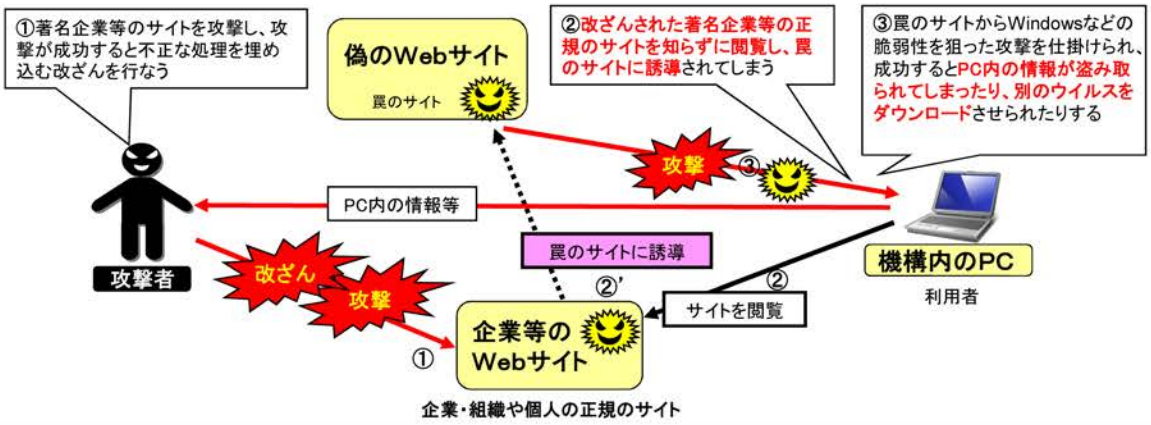
これだけはぜひ！
最低限のコンピュータウイルス対策

1.1 改ざんされたウエブサイトを介して感染するウイルス

著名企業等を含む正規のサイトが多数改ざんされています

企業・組織や個人の正規のサイトが悪意のある者によって改ざんされ、利用者がそのサイトとは別の罠サイトに誘導される事例が相次いでいます。 表面上は本来のサイトの内容が表示されるので、その裏で罠サイトに誘導されていることに気づかないことがほとんどです。

罠サイトではウイルスをダウンロードさせられることが多く、利用者のパソコンのソフトウェアに未対策の脆弱性があると、簡単にウイルスに感染してしまいます。

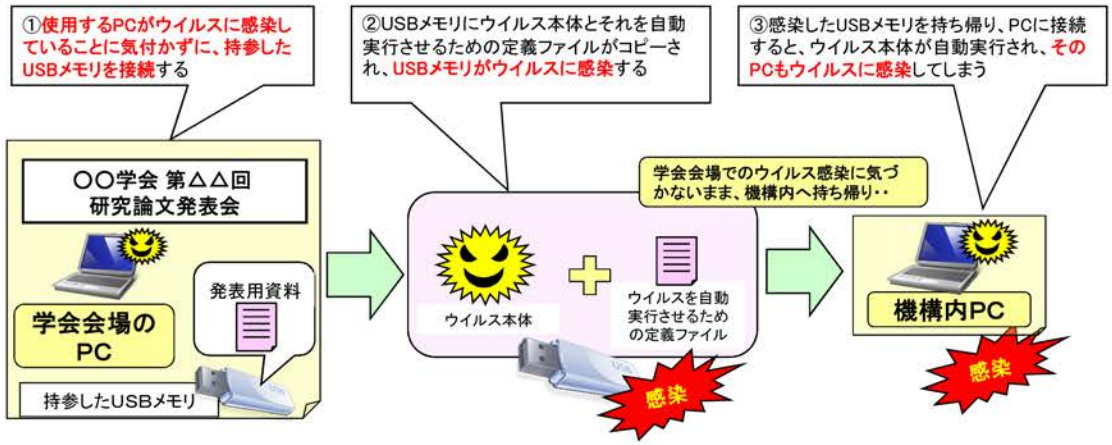


これだけはぜひ！
最低限のコンピュータウイルス対策

1.2 ＵＳＢメモリ等の外部記録媒体を介して感染するウイルス

USBメモリ等を介して感染するウイルスの検知が頻発しています

機構外で使用したUSBメモリやパソコンが、USBメモリ等の外部記録媒体を介して広がるウイルスに感染し、それに気づかずに機構内に持ち込む事例が相次いでいます。 USBメモリだけではなく、外付けハードディスク、デジタルカメラ、音楽プレイヤー、ICレコーダー、SDカード、メモリースティック、コンパクトフラッシュなどもウイルスの感染媒体となることが確認されており、外部記録媒体全般に対する注意が必要です。



第２章　最低限のコンピュータウイルス対策

これだけはぜひ！
最低限のコンピュータウイルス対策

2.1　ウイルス対策７カ条（１／２）

1. ソフトウェアを常に最新の状態にする

操作手順編で手順を解説しています

重点対策項目

ウイルスはソフトウェア（OS及びアプリケーションソフトウェア）の脆弱性を悪用して感染活動を行うことが多い。ソフトウェアのセキュリティ修正プログラムが提供された際には速やかに適用すること。

2. ウイルス対策ソフトウェアを導入する

操作手順編で手順を解説しています

重点対策項目

コンピュータウイルスへの感染を未然に防止するため、ウイルス対策ソフトウェアを導入し、パターンファイルやエンジンを常に最新の状態にすること。

3. 自動実行(Autorun)機能を停止する

操作手順編で手順を解説しています

USBメモリ等をパソコンに接続した際、ウイルスを含む実行ファイルが自動的に実行されてしまうことを防ぐため、自動実行（Autorun）機能を予め停止させておくこと。

4. 不審な電子メールは開かずに削除する

送信元が不明、件名や内容が意味不明、不審なファイルが添付されている、不審なURLがリンクされている等の電子メールは、開かずに削除すること。
添付ファイルには特に注意し、安易にクリックして開かないこと。

これだけはぜひ！
最低限のコンピュータウイルス対策

2.1 ウイルス対策７カ条 （２／２）

5. HTMLメールをそのまま表示したり、作成・送信しない

HTMLメールは、ウイルスに感染したり、行動分析の対象にされたりする等、危険性が高まるので利用しないこと。 受信した場合はそのまま表示せず、テキスト部分のみを表示する等、メールソフトの動作を制限すること。

6. 利用禁止ソフトウェアをインストールしない

利用禁止ソフトウェアは情報漏えいに繋がり易いので、インストールや利用を絶対に行なわないこと。

7. インターネットのサイトへのアクセスは必要最小限に

業務に不必要なサイトへのアクセスは、ウイルスの感染を始め、情報セキュリティ上の脅威に晒される危険性が高まるので行なわないこと。
業務上必要なアクセスであっても、最小限に留めること。

これだけはぜひ！
最低限のコンピュータウイルス対策

2.2 【重点対策１】ソフトウェアを常に最新の状態にする（１／３）

脆弱性（ぜいじゃくせい）

ハードウェアやソフトウェアの欠陥（バグとも呼ばれる）、設計段階での見落とし、開発者が想定していなかった利用形態、などによってシステムに生じるセキュリティ上の弱点のこと。

不正アクセスやウイルスの標的として狙われることが多く、対策をしないと危険です。

脆弱性対策

脆弱性が発見された場合、通常は開発元などからセキュリティ修正プログラム（パッチ、セキュリティパッチ、アップデートプログラム、ホットフィクスなど、呼び方はいろいろある）が提供されます。

修正プログラムの提供が開始されたら、速やかに適用して脆弱性を塞ぐことが大切です。

これだけはぜひ！
最低限のコンピュータウイルス対策

2.2 【重点対策１】ソフトウェアを常に最新の状態にする（２／３）

特段の注意が必要なソフトウェア

脆弱性対策は、パソコンで使用する全てのソフトウェアが対象となりますが、ここに挙げたソフトウェアは利用者数が多い等の理由で狙われ易く、脆弱性に対する特段の注意が必要です。

OS

- Microsoft Windows
- Apple Mac OS

機構イントラ（ http://intra.jaea.go.jp ）内「ｺﾝﾋﾟｭｰﾀ&ﾈｯﾄﾜｰｸ利用」ページにて、随時、脆弱性対策に関する情報を提供しております。

アプリケーションソフトウェア

- Internet Explorer
- Firefox
- Google Chrome
- JAVA
- JRE
- Microsoft Office
- Adobe Reader
- Adobe Acrobat
- Adobe Flash

これらのソフトウェアのセキュリティ修正プログラムは、提供され次第速やかに適用してください。

自動更新の設定が可能なソフトウェアについては、予め自動更新が有効になるように設定しておいてください。

これだけはぜひ！
最低限のコンピュータウイルス対策

2.2 【重点対策１】ソフトウェアを常に最新の状態にする（３／３）

セキュリティ修正プログラムの入手方法

ソフトウェア名	セキュリティ修正プログラムの入手先、確認方法等
Microsoft Windows, Internet Explorer, Microsoft Office	Windows Update (Microsoft Update) を実施するか、下のURLにアクセスする http://www.update.microsoft.com/microsoftupdate/
Adobe Reader, Adobe Acrobat	【バージョン9以降を使用している場合】 ①[スタート]－[すべてのプログラム] から「Adobe Reader」または「Adobe Acrobat」を起動 ②[ヘルプ]－[アップデートの有無をチェック] し、その後は案内に従いバージョンアップ
	【バージョン8以前を使用している場合】 http://get.adobe.com/jp/reader/ から最新版を入手する
Adobe Flash	http://get.adobe.com/jp/flashplayer/ から最新版を入手する
JAVA, JRE	http://www.java.com/ja/download/ から最新版を入手する
Firefox	①[スタート]－[すべてのプログラム] から「Mozilla Firefox」を起動 ②[ヘルプ]－[ソフトウェアの更新を確認] をクリック ③案内に従いバージョンアップ
Google Chrome	①[スタート]－[すべてのプログラム] から「Google Chrome」を起動 ②[Google Chromeの設定] －[Google Chromeについて] を選択し、その後は案内に従いバージョンアップ
QuickTime	http://www.apple.com/jp/quicktime/download/ から最新版を入手する

これだけはぜひ！
最低限のコンピュータウイルス対策

2.3 【重点対策２】ウイルス対策ソフトウェアを導入する

機構ネットワークを利用するパソコン等は、システム計算科学センターが配布するウイルス対策ソフトウェアの導入を義務づけられています

（平成21年12月15日、JAEA情報セキュリティ委員会決定事項）

システム計算科学センターが配布している**McAfee VirusScan以外をご利用の方は、入替え**をお願いいたします。

以下のページで入替えや導入のご案内をしていますので、ご利用ください。
（対象OS：Windows、Mac OS X）
http://cnet-guide.jaea.go.jp/security/virus/

これだけはぜひ！
最低限のコンピュータウイルス対策

2.4 外部記録媒体を利用する際の確認

機構外から持ち込まれた外部記録媒体（USBメモリ、外付けHDD、CD/DVD等）は、コンピュータウイルスに感染していないことを確認してから使用します

＜確認手順＞
① PCのウイルス対策ソフトの定義ファイルおよびOSを最新の状態にする。
② PCからLANケーブルを抜く。
③ 外部記録媒体をPCに挿してウイルススキャンを行う。
④ ウイルス感染していないことを確認してから外部記録媒体を使用する。

これだけはぜひ！
最低限のコンピュータウイルス対策

最後に

本教育の中で示した対策等は、テーマをコンピュータウイルスへの感染の防止に限定したものです。
情報漏えいの防止、情報機器の盗難・紛失防止等を含む総合的な情報セキュリティ対策については、イントラネットの「コンピューター＆ネットワーク利用（機構内限定）」のページから、「PC等情報機器の情報セキュリティ実施手順書」を参照の上実施してください。
コンピューター＆ネットワーク利用（機構内限定）URL: http://cnet-guide.jaea.go.jp/

これだけはぜひ！
最低限のコンピュータウイルス対策

本編はこれで終了です。 お疲れさまでした。
下の手順に従って終了操作をお願いします。

画面左上の「次へ」をクリックします

下の画面が表示されたら、「OK」をクリックします

画面右上の「終了」をクリックします

下の画面が表示されたら、「OK」をクリックします

本教材の実行には、Internet Explorer (IE) 6.0 SP1以降を使用してください。
(FireFox、Google Chrome、Opera等のIE以外のブラウザでは、正常に動作いたしません)
本教材内でオペレーション・レクチャーという手法を用いて具体的な操作方法を説明しており、
その関係でブラウザが限定されております。 ご了承ください。

～情報セキュリティ教育～

これだけはぜひ！

最低限のコンピュータウイルス対策

＜操作手順編＞

本教育の概要

パソコンがコンピュータウイルスに感染すると、情報の漏洩や滅失、感染経路や影響範囲の調査及び復旧作業に伴う業務の遅延等、深刻な影響を受けてしまいます。

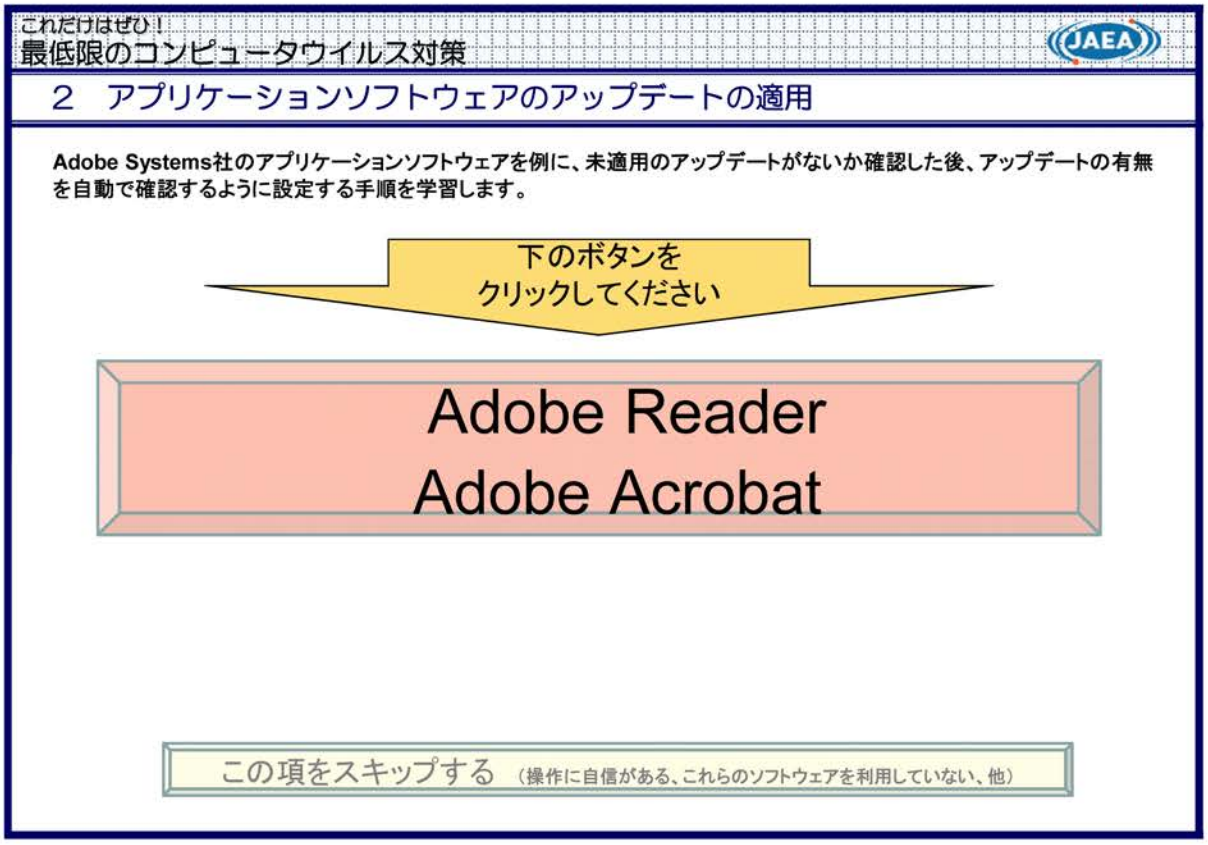
本操作手順編は、コンピュータウイルスへの感染を未然に防止するため、パソコンで必ず行なうべきウイルス対策の具体的な手順を示し、点検・再確認を通じて確実にウイルス対策を実施して頂くことを目的としています。

教材を見ながら実際に操作することにより、設定や確認を容易に行なうことができますので、ぜひご活用ください。

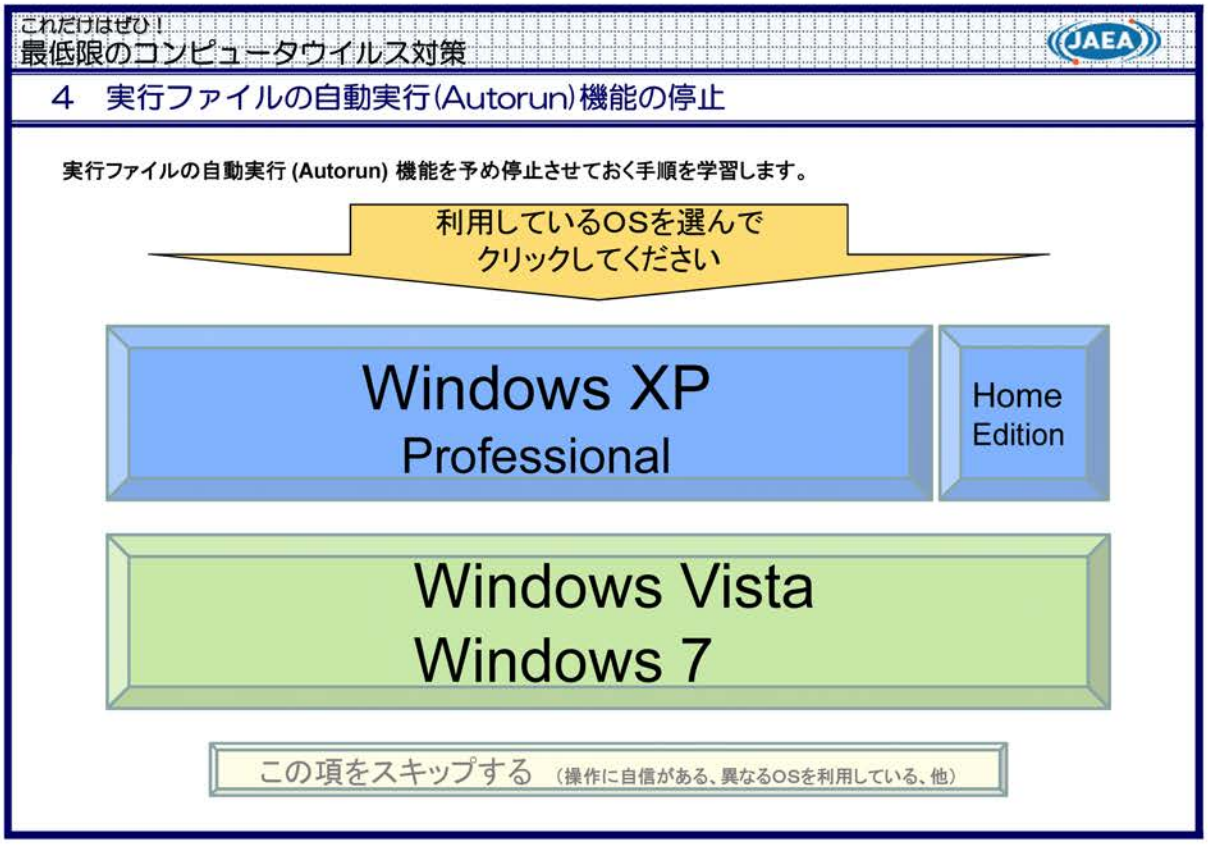
マウスクリックで次のページに進みます

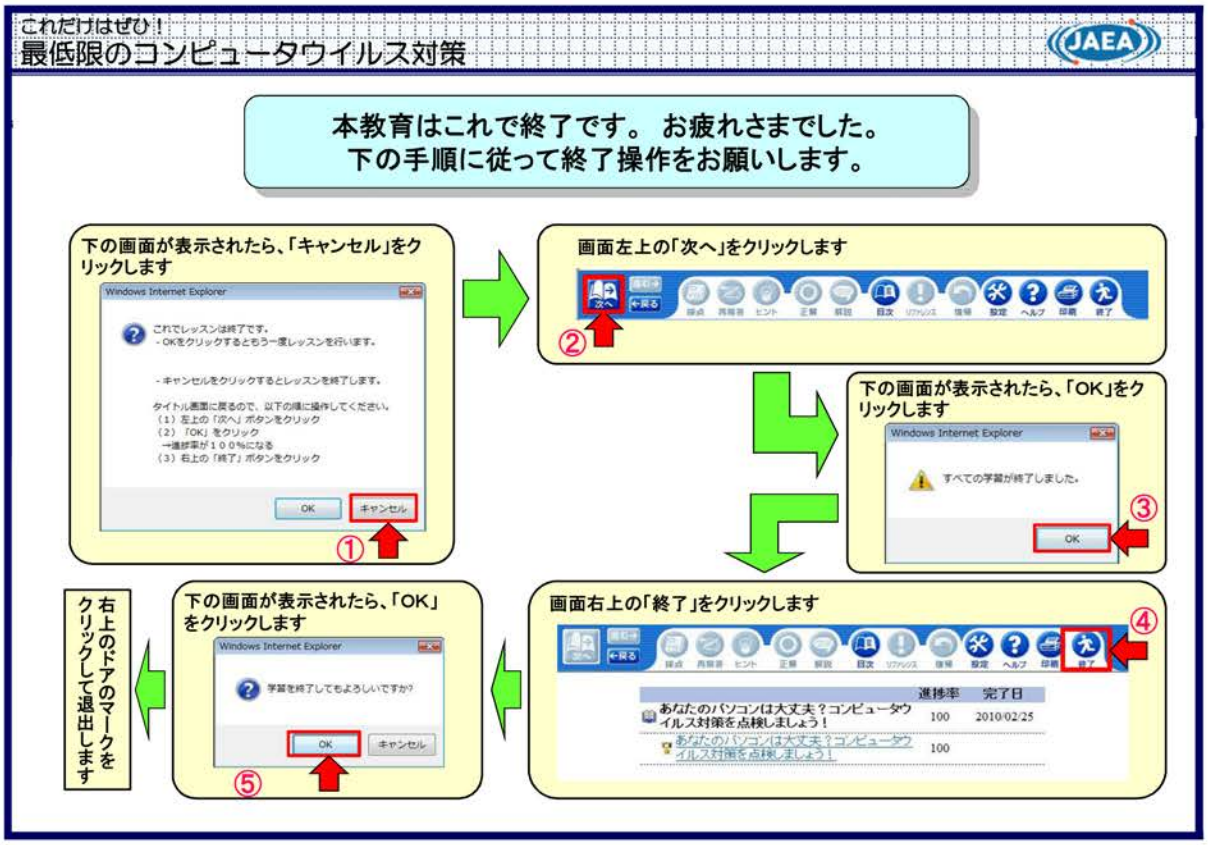
目次


これだけはぜひ！
最低限のコンピュータウイルス対策
JAEA
1　OSのアップデートの適用
機構で利用されている代表的なOSを例に、アップデートが提供された際に自動で適用を行うように設定した後、未適用のアップデートがないか確認するまでの手順を学習します。
利用しているOSを選んで
クリックしてください
Windows XP
Windows Vista
Windows 7
この項をスキップする （操作に自信がある、異なるOSを利用している、他）


これだけはぜひ！
最低限のコンピュータウイルス対策
JAEA
2　アプリケーションソフトウェアのアップデートの適用
Adobe Systems社のアプリケーションソフトウェアを例に、未適用のアップデートがないか確認した後、アップデートの有無を自動で確認するように設定する手順を学習します。
下のボタンを
クリックしてください
Adobe Reader
Adobe Acrobat
この項をスキップする （操作に自信がある、これらのソフトウェアを利用していない、他）


これだけはぜひ！
最低限のコンピュータウイルス対策
JAEA
3　ウイルス対策ソフトウェアでの検査（フルスキャン）
システム計算科学センターで配布しているウイルス対策ソフトウェアを最新の状態にした後、パソコンを検査（フルスキャン）する手順を学習します。
下のボタンを
クリックしてください
McAfee VirusScan
この項をスキップする （操作に自信がある、他のソフトウェアを利用している、他）


これだけはぜひ！
最低限のコンピュータウイルス対策
JAEA
4　実行ファイルの自動実行(Autorun)機能の停止
実行ファイルの自動実行 (Autorun) 機能を予め停止させておく手順を学習します。
利用しているOSを選んで
クリックしてください
Windows XP
Professional
Home
Edition
Windows Vista
Windows 7
この項をスキップする （操作に自信がある、異なるOSを利用している、他）


これだけはぜひ！
最低限のコンピュータウイルス対策
本教育はこれで終了です。 お疲れさまでした。
下の手順に従って終了操作をお願いします。
下の画面が表示されたら、「キャンセル」をクリックします
Windows Internet Explorer
これでレッスンは終了です。
- OKをクリックするともう一度レッスンを行います。
- キャンセルをクリックするとレッスンを終了します。
タイトル画面に戻るので、以下の順に操作してください。
（1）左上の「次へ」ボタンをクリック
（2）「OK」をクリック
→進捗率が１００％になる
（3）右上の「終了」ボタンをクリック
OK
キャンセル
①
画面左上の「次へ」をクリックします
次へ
戻る
②
下の画面が表示されたら、「OK」をクリックします
Windows Internet Explorer
すべての学習が終了しました。
OK
③
画面右上の「終了」をクリックします
終了
④
進捗率
完了日
あなたのパソコンは大丈夫？コンピュータウイルス対策を点検しましょう！
100
2010/02/25
あなたのパソコンは大丈夫？コンピュータウイルス対策を点検しましょう！
100
下の画面が表示されたら、「OK」をクリックします
Windows Internet Explorer
学習を終了してもよろしいですか?
OK
キャンセル
⑤
右上のドアのマークをクリックして退出します

付録６　「平成 22 年度情報セキュリティ教育」

～ 情報セキュリティ教育～

平成22年度情報セキュリティ教育

本教育の概要

本教育は、最近の情報セキュリティ上の脅威に対する注意喚起と対策の啓蒙を目的とし、機構で実際に発生した情報セキュリティ事案を取り上げています。
教材の内容を身近な脅威として認識し、対策の着実な実施をお願いします。

教材を用いての学習の後、情報セキュリティ対策のセルフチェックを実施していただきます。両方を終了しないと受講完了となりませんので、ご注意ください。

※本教育内で使用しているソフトウェアの名称、アイコン等は、各販売元等の登録商標です。

平成２２年度情報セキュリティ教育

目次

平成２２年度情報セキュリティ教育

１．情報機器の盗難・亡失に対する備え

１．１ 盗難被害事例
１．２ 盗難・亡失に備える
１．３ クイズ

平成２２年度情報セキュリティ教育

１．１　盗難被害事例

海外出張中の機構職員が列車内で盗難被害に遭っています。

事例1：フランス、シャルル・ド・ゴール空港からパリ市内へ向かう列車にて

途中駅に停車中、男がコインを床に落とし、それに気を取られた隙に、横に置いていたバッグを別の男に盗まれてしまった。すぐには気づかず、周囲の人が騒ぎ出したことで犯行に気づいた。追いかけようとしたが、扉が閉まり発車してしまったため、緊急ボタンを押して列車を停車させた。車掌が来たが、犯人達は既に駅から逃亡した後であった。

盗難被害品（情報機器関連のみ抜粋）：　PC、USBメモリ、外付けハードディスク

事例2：スイス、チューリヒ空港へ向かう列車にて

途中駅に停車中、通路に置いていたトランク（スーツケース）を「移動した方がいい」と男に助言された。座席から立ち上がり、トランクを1m程度移動した。振り向くと男の姿は無く、座席に置いていたリュックを持ち去られていることに気づいた。慌てて車外へ出たが男は見あたらなかった。発車間際だったので再び乗車し、下車駅で警察に届け出た。

盗難被害品（情報機器関連のみ抜粋）：　PC、USBメモリ



平成２２年度情報セキュリティ教育

１．２　盗難・亡失に備える(１/３)

２つの事例は、「列車内」「途中駅での停車中」「気を取られるような出来事が発生する」「発車間際であり、追いかけることを諦めざるを得ない」といった共通点があり、プロに狙われて盗難被害に遭ってしまったものと考えられます。
荷物をできるだけ少なくし常に目を離さないようにする等の注意を払っていても、プロに狙われてしまうと盗難被害を防ぐことは難しいのが現実です。
情報漏えいによる2次被害を発生させないため、以下に示す対策を事前に実施してください。

１．情報機器をまるごと暗号化する　(H22年度情報セキュリティ委員会)

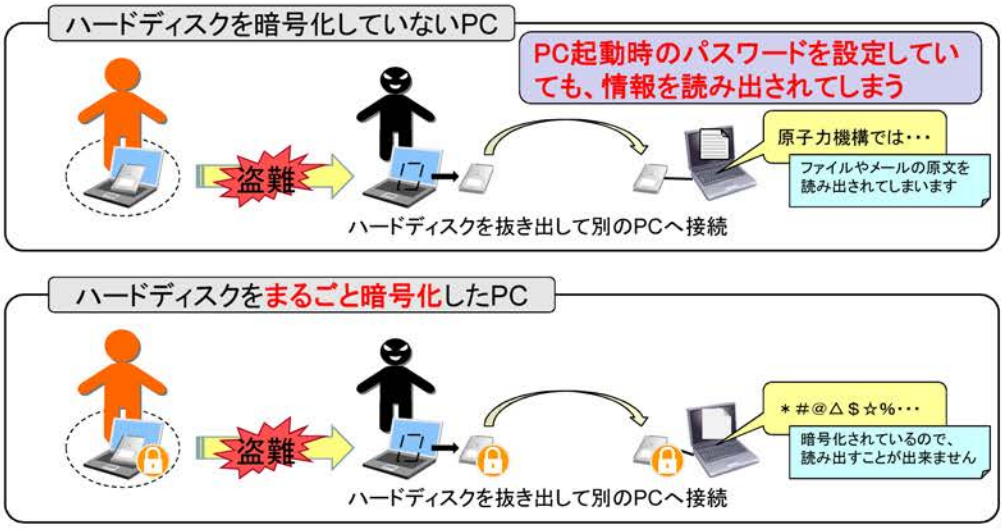
万一の際でも情報を読み出されないようにするため、持ち出しの際は、格納する情報の機密性に関係なく、情報機器をまるごと暗号化してください。

PCだけでなく、外部記録媒体も暗号化が必要です。

平成２２年度情報セキュリティ教育

１．２　盗難・亡失に備える(２/３)

まるごと暗号化とは？



ハードディスクをまるごと暗号化しておけば、万一の盗難・亡失の際も第三者に情報を読み出されることがありません。

平成２２年度情報セキュリティ教育

１．２　盗難・亡失に備える(3/3)

２．情報機器を持ち出す際は、必ず手続きを行う

格納されている情報の内容、情報機器の暗号化の状態を十分に確認し、
申請書を用いて課室情報セキュリティ責任者に申請、許可を得る必要があります。
PC本体だけではなく、USBメモリや外付けハードディスクについても漏れなく手続きを
行なってください。なお、私物の情報機器へは機構の業務情報を格納しないでください。

３．持ち出す情報の記録を残す　(H22年度情報セキュリティ委員会)

盗難・亡失の際には、格納していた情報の正確な特定を求められます。
これに備え、バックアップの取得等により、持ち出す情報の記録を機構内に残してください。

平成２２年度情報セキュリティ教育

１．３　クイズ

問1 情報機器(PC、記録媒体等)を持ち出す際の対策について、正しい方を選択してください。

- A　携行品の盗難・亡失には十分注意しているので、対策は特に必要ない。
- B　持ち出す情報機器を、不測の事態に備えて暗号化する。

問2 情報機器を持ち出す手続きについて、正しい方を選択してください。

- A　持ち出す情報機器に格納している情報の内容や暗号化の状態を十分に確認していれば、手続きを行わずに持ち出しても問題ない。
- B　USBメモリや外付けハードディスクを持ち出す際についても、情報セキュリティ責任者へ申請を行わなければならない。

平成２２年度情報セキュリティ教育

2．不審メールへの対応

2．1　機構に届いた不審メールの例
2．2　不審メールを見分けるポイント
2．3　クイズ

平成２２年度情報セキュリティ教育

2．1　機構に届いた不審メールの例（2/2）

3つのメールの例から、不審な点を探してみてください。

不審メール例　1

Subject: 竹島の近況
From:[redacted]海外安全[redacted]@mofa.go.jp>
Date: Fri, 12 Oct 2007 09:05:17 +0900
Reply-To:[redacted]@mofa.go.jp
To:[redacted]@jaea.go.jp

外務省海外危険情報：竹島の近況

=-=
[redacted]海外安全
FAX :0570[redacted]（日本国内から）
0422-42-[redacted]（日本国外から）
web:[redacted]
=-=

添付ファイル

［添付ファイル名］ﾌﾟｵ.zip

不審メール例　2

Subject: Fw:【機2】所信案文（外交）
From:[redacted]
Sent: Friday, June 25, 2010 5:28 PM
To:[redacted]@jaea.go.jp

[redacted]外務大臣
[redacted]防衛大臣
[redacted]国務長官
[redacted]国防長官

横島様　よろしくご査収ください。 前段部分は[redacted]先生のどこを気に入られているのかわかりませんが、とりあえず、書いてみました。国際社会で尊敬される云々は、夢見がちな話なので削除して様子を見たいと思います。 返事等は、お手数ですがこのアドレスおよびCCのアドレスにお送りください。
[redacted](See attachedfile: 20100625.doc)

添付ファイル

［添付ファイル名］
20100625_cod.zip

不審メール例　3

Subject:核不拡散と原子力の平和利用
From:[redacted]@jaea.go.jp>
Date:Tue, 9 Oct 2007 07:36:08 +0900
To:[redacted]@jaea.go.jp

?j?s?g?U?????q???????a???p?????????????A?]????
?l?????????o?????W?A?G?l???M?[?E?Z
?L?????e?B?[???m???????_?????A???????????C???
??A?C???????k???N?????????j?J???ANPT?i?j?????s
?g?U?????j???????????C???h???????q?
???????A???X?????????????A???????????????????
?A?v???[?`?????????????????????B

?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?
¥?¥?¥?¥?¥?¥?¥?¥?¥?¥
??319-1195
???????????S???C??????????2-4
?j?s?g?U???w?Z?p?Z???^?[?@
TEL: 029-[redacted]
FAX: 029-[redacted]
E-mail:[redacted]@jaea.go.jp

添付ファイル

［添付ファイル名］jsgUqap.zip

平成２２年度情報セキュリティ教育

2．1　機構に届いた不審メールの例（2/2）

貴方の業務はこのような件名、送信元と関連がありますか？

Subject: 竹島の近況
From: [redacted]海外安全[redacted]@mofa.go.jp>
Date: Fri, 12 Oct 2007 09:05:17 +0900
Reply-To: [redacted]@mofa.go.jp
To: [redacted]@jaea.go.jp

外務省海外危険情報：竹島の近況

本文がない

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[redacted]海外安全
FAX：0570[redacted]（日本国内から）
0422-42-[redacted]（日本国外から）
web：[redacted]
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

ファイル名が不自然

添付ファイル

[添付ファイル名] ﾌﾟｵ.zip

Subject: Fw:【機2】所信案文（外交）
From: [redacted]
Sent: Friday, June 25, 2010 5:28 PM
To: [redacted]@jaea.go.jp

[redacted]外務大臣
[redacted]防衛大臣
[redacted]国務長官
[redacted]国防長官

不自然な宛て名

不一致

横島様　よろしくご査収ください。 前段部分は[redacted]先生のどこを気に入られているのかわかりませんが、とりあえず、書いてみました。国際社会で尊敬される云々は、夢見がちな話なので削除して様子を見たいと思います。 返事等は、お手数ですがこのアドレスおよびCCのアドレスにお送りください。
[redacted](See attachedfile: 20100625.doc)

メールをもらう覚えのある相手ですか？

添付ファイル

[添付ファイル名]
20100625_cod.zip

Subject: 核不拡散と原子力の平和利用
From: [redacted]@jaea.go.jp>
Date: Tue, 9 Oct 2007 07:36:08 +0900
To: [redacted]@jaea.go.jp

```
?j?s?g?U?????q???????a???p?????????????A?]????
?l?????????o?????W?A?G?l???M?[?E?Z
?L?????e?B?[???m???????_?????A???????????C???
??A?C???????k???N?????????j?J???ANPT?i?j?????s
?g?U?????j???????????C???h???????q?
???????A???X?????????????A????????????????????
?A?v???[?`?????????????????????B

?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?¥?
¥?¥?¥?¥?¥?¥?¥?¥?¥?¥
??319-1195
???????????S???C??????????2-4
?j?s?g?U???w?Z?p?Z???^?[?@
```

TEL: 029-[redacted]
FAX: 029-[redacted]
E-mail: [redacted]@jaea.go.jp

極端な文字化け

添付ファイル

[添付ファイル名] jsgUqap.zip

平成２２年度情報セキュリティ教育

2．2　不審メールを見分けるポイント

不審メールは以下のような点に違和感のあることがほとんどです。

① 送信元のメールアドレスが信頼できそうな組織のアドレスであるが、業務上の関連が思い当たらない

② 興味を引くような件名であるが、業務上の関連が思い当たらない

③ 本文の内容が不自然であったり文字化けしたりしている

④ 添付ファイルのファイル名が不自然

不審メールは、速やかに削除する

違和感を感じるメールは、速やかに削除してください。
添付ファイルやURLには特に注意し、安易にクリックして開かないでください。

平成２２年度情報セキュリティ教育

２．３　クイズ

問1　メールの利用方法として正しい方を選択してください。

- A　宛先を確認してから送信し、誤送信を防いでいる。
- B　メールに記載されているURLや添付ファイルは、全て開いて確認している。

問2　メールを受信した際の行動として正しい方を選択してください。

- A　同僚から怪しい添付ファイルが付いたメールを受信したが、確認のため添付ファイルを開いた。
- B　官公庁をかたる署名・ドメイン名、違和感のある件名、違和感のある宛名、件名と結びつかない本文、名前が不自然な添付ファイルのメールを受信したため、速やかに削除した。

平成２２年度情報セキュリティ教育

３．OS(※)のサポート終了への対応

３．１　Windowsのサポート期限
３．２　後継OSへの移行
３．３　クイズ

※OS（Operating System）とは
コンピュータのハードウェアと連携しながら動作する基本ソフトウェアのことで、代表的なものとして、Microsoft社のWindowsシリーズ、Apple社のMac OSシリーズが普及しています。

平成２２年度情報セキュリティ教育

３．１　Windowsのサポート期限

Microsoft社によるサポート期限を過ぎると、セキュリティパッチ等が提供されません。

OS名	Microsoft社による サポート期限
Windows 2000（Serverを含む）	2010年7月13日 終了
Windows XP（SP2以前）	2010年7月14日 終了
Windows XP（SP3）	2014年4月8日
Windows Vista（Home Basic/Home Premium）	2012年4月10日
Windows Vista（Business/Enterprise/Ultimate）	2017年4月11日
Windows 7（Starter/Home Basic/Home Premium）	2015年1月13日
Windows 7（Professional/Enterprise/Ultimate）	2020年1月14日

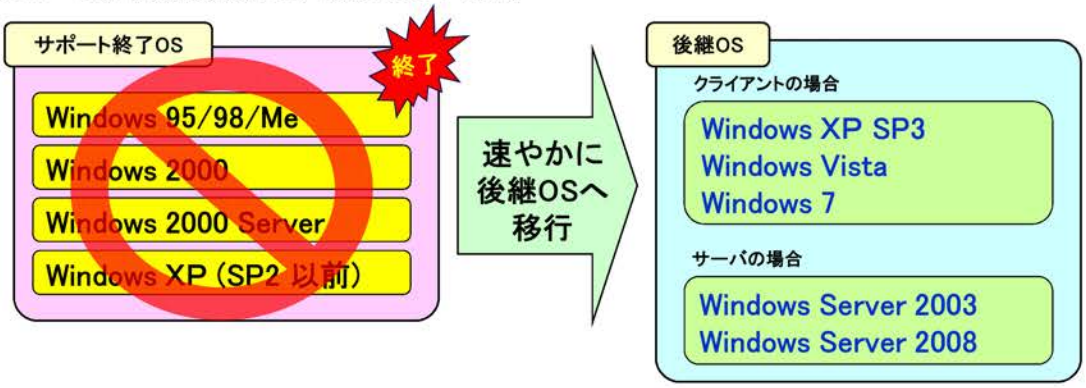
Windows 2000、Windows XP(SP2以前)は、既に脆弱性が放置されたままの危険な状態になっています。

Windows 2000は、システム計算科学センターが配布しているウイルス対策ソフトウェア(McAfee VirusScan)によるサポートも2011年３月３１日で終了します。
※Windows 2000については、2011年4月1日以降、ネットワークへの接続を制限します。

平成２２年度情報セキュリティ教育

３．２　後継OSへの移行

Microsoft社によるサポートが終了したWindowsは、脆弱性が放置されたままの危険な状態になっています。
該当OSを使用している場合は、速やかに、メーカのサポート及びウイルス対策ソフトウェアのサポートが有効な後継OSへ移行して下さい。



※Mac OSについて※
Apple社はOSのサポート期限を公表しておらず、旧OSのセキュリティ状態が不明確です。
セキュリティを維持するため、できるだけ最新のMac OSを使用するようにして下さい。

平成２２年度情報セキュリティ教育

３．３　クイズ

問1メーカによるサポートが終了しているOSの使用について正しい方を選んでください。

- A　メーカから修正プログラムが配布されないということは、修正を必要とするような問題は無いということなので、安心して継続使用することができる。
- B　メーカによるサポートが終了しているOSを使用している場合は、サポートが有効な後継OSへ移行し、システム計算科学センターが配布しているウイルス対策ソフトを導入する。

問2　メーカによるサポートが終了しているOSを選択して下さい。

- A　Windows 2000、Windows XP（SP2以前）
- B　Windows XP(SP3)、Windows Vista、Windows 7

平成２２年度情報セキュリティ教育

４．ウイルス対策

平成２２年度情報セキュリティ教育

４．１　ウイルス対策７カ条（１／２）

「これだけはぜひ！最低限のコンピュータウイルス対策　操作手順編」（平成21年度教育）で実際の手順を確認することができます。

１．ソフトウェアを常に最新の状態にする

４．２項で解説します

ウイルスはソフトウェア（OS及びアプリケーションソフトウェア）の脆弱性を悪用して感染活動を行うことが多い。このため、ソフトウェアのセキュリティ修正プログラムが提供された際には速やかに適用すること。

２．ウイルス対策ソフトウェアを導入する

４．３項で関連解説をします

コンピュータウイルスへの感染を未然に防止するため、システム計算科学センターが配布しているウイルス対策ソフトウェアを導入すること。
また、全ての電子ファイルを定期的にスキャンすること。
（推奨頻度：月１回以上）

３．自動実行（Autorun）機能を停止する

４．４項で解説します

USBメモリ等をパソコンに接続した際、ウイルスを含む実行ファイルが自動的に実行されてしまうことを防ぐため、自動実行（Autorun）機能を予め停止させておくこと。

平成２２年度情報セキュリティ教育

４．１　ウイルス対策７カ条（２／２）

４．不審メールは速やかに削除する

送信元が不明、件名や内容が意味不明、不審なファイルが添付されている、不審なURLがリンクされている等のメールは、速やかに削除すること。
添付ファイルには特に注意し、安易にクリックして開かないこと。

５．HTMLメールをそのまま表示したり、作成・送信しない

HTMLメールは、ウイルスに感染したり、行動分析の対象にされたりする等、危険性が高まるので利用しないこと。 受信した場合はそのまま表示せず、テキスト部分のみを表示する等、メールソフトの動作を制限すること。

６．利用禁止ソフトウェアをインストールしない

利用禁止ソフトウェアは情報漏えいに繋がり易いので、インストールや利用を絶対に行なわないこと。

利用禁止ソフトウェアリスト：　http://cnet-guide.jaea.go.jp/security/ngsoft.html/

７．インターネットのサイトへのアクセスは必要最小限に

業務に不必要なサイトへのアクセスは、ウイルスの感染を始め、情報セキュリティ上の脅威に晒される危険性が高まるので行なわないこと。
業務上必要なアクセスであっても、最小限に留めること。

平成２２年度情報セキュリティ教育

４．２　ソフトウェアを常に最新の状態にする（１／２）

特段の注意が必要なソフトウェア

脆弱性対策は、パソコンで使用する全てのソフトウェアが対象となりますが、ここに挙げたソフトウェアは利用者数が多い等の理由で狙われ易く、脆弱性に対する特段の注意が必要です。

OS

- Microsoft Windows
- Apple Mac OS

機構イントラ（ http://intra.jaea.go.jp ）内「ｺﾝﾋﾟｭｰﾀ&ﾈｯﾄﾜｰｸ利用」ページにて、随時、脆弱性対策に関する情報を提供しております。

アプリケーションソフトウェア

- Internet Explorer
- Firefox
- Google Chrome
- JAVA
- JRE
- Microsoft Office
- Adobe Reader
- Adobe Acrobat
- Adobe Flash

これらのソフトウェアのセキュリティ修正プログラムは、提供され次第速やかに適用してください。

自動更新の設定が可能なソフトウェアについては、予め自動更新が有効になるように設定しておいてください。

平成２２年度情報セキュリティ教育

４．２　ソフトウェアを常に最新の状態にする（２／２）

セキュリティ修正プログラムの入手方法

ソフトウェア名	セキュリティ修正プログラムの入手先、確認方法等
Microsoft Windows, Internet Explorer, Microsoft Office	Windows Update (Microsoft Update) を実施するか、下のURLにアクセスする http://www.update.microsoft.com/microsoftupdate/
Adobe Reader, Adobe Acrobat	【バージョン10以降を使用している場合】 ①[スタート]－[すべてのプログラム] から「Adobe Reader」または「Adobe Acrobat」を起動 ②[ヘルプ]－[アップデートの有無をチェック] し、その後は案内に従いバージョンアップ
	【バージョン9以前を使用している場合】 http://get.adobe.com/jp/reader/ から最新版を入手する
Adobe Flash	http://get.adobe.com/jp/flashplayer/ から最新版を入手する
JAVA, JRE	http://www.java.com/ja/download/ から最新版を入手する
Firefox	①[スタート]－[すべてのプログラム] から「Mozilla Firefox」を起動 ②[ヘルプ]－[ソフトウェアの更新を確認] をクリック ③案内に従いバージョンアップ
Google Chrome	①[スタート]－[すべてのプログラム] から「Google Chrome」を起動 ②[Google Chromeの設定] －[Google Chromeについて] を選択し、その後は案内に従いバージョンアップ
QuickTime	http://www.apple.com/jp/quicktime/download/ から最新版を入手する

平成２２年度情報セキュリティ教育

４．３　外部記録媒体を利用する際の確認

外部記録媒体（USBメモリ、外付けHDD、CD/DVD等）は、
コンピュータウイルスに感染していないことを確認してから使用します

＜確認手順＞
① PCのウイルス対策ソフトの定義ファイルおよびOSを最新の状態にする。
② PCからLANケーブルを抜く。
③ 外部記録媒体をPCに挿してウイルススキャンを行う。
④ ウイルス感染していないことを確認してから外部記録媒体を使用する。

平成２２年度情報セキュリティ教育

４．４　自動実行(Autorun)機能の停止手順（１／２）

USBメモリ等をパソコンに接続した際、ウイルスを含む実行ファイルが自動的に
実行されてしまうことを防ぐため、自動実行（Autorun）機能を停止します

Windows XPの場合

＜停止手順＞
①「スタート」―「ファイル名を指定して実行」から
「gpedit.msc」と入力する

②「コンピュータの構成」―「管理用テンプレート」―
「システム」を選択する

③「自動実行機能をオフにする」をダブルクリックする

④「有効」―「全てのドライブ」を指定し、OKをクリックする

平成２２年度情報セキュリティ教育

４．４　自動実行(Autorun)機能の停止手順（２／２）

Windows Vistaの場合

＜停止手順＞

①画面左下の「Windowsボタン」―「コントロールパネル」をクリックする

②「CDまたはその他のメディアの自動再生」をクリックする。

③「全てのメディアで自動再生を使う」のチェックを外す。

④「保存」をクリックする

詳細は機構イントラ内「コンピュータ＆ネットワーク利用」を参照願います。
・PC等情報機器の情報セキュリティ実施手順書
http://cnet-guide.jaea.go.jp/index.php/ja/security/security-tejun

平成２２年度情報セキュリティ教育

４．５　クイズ

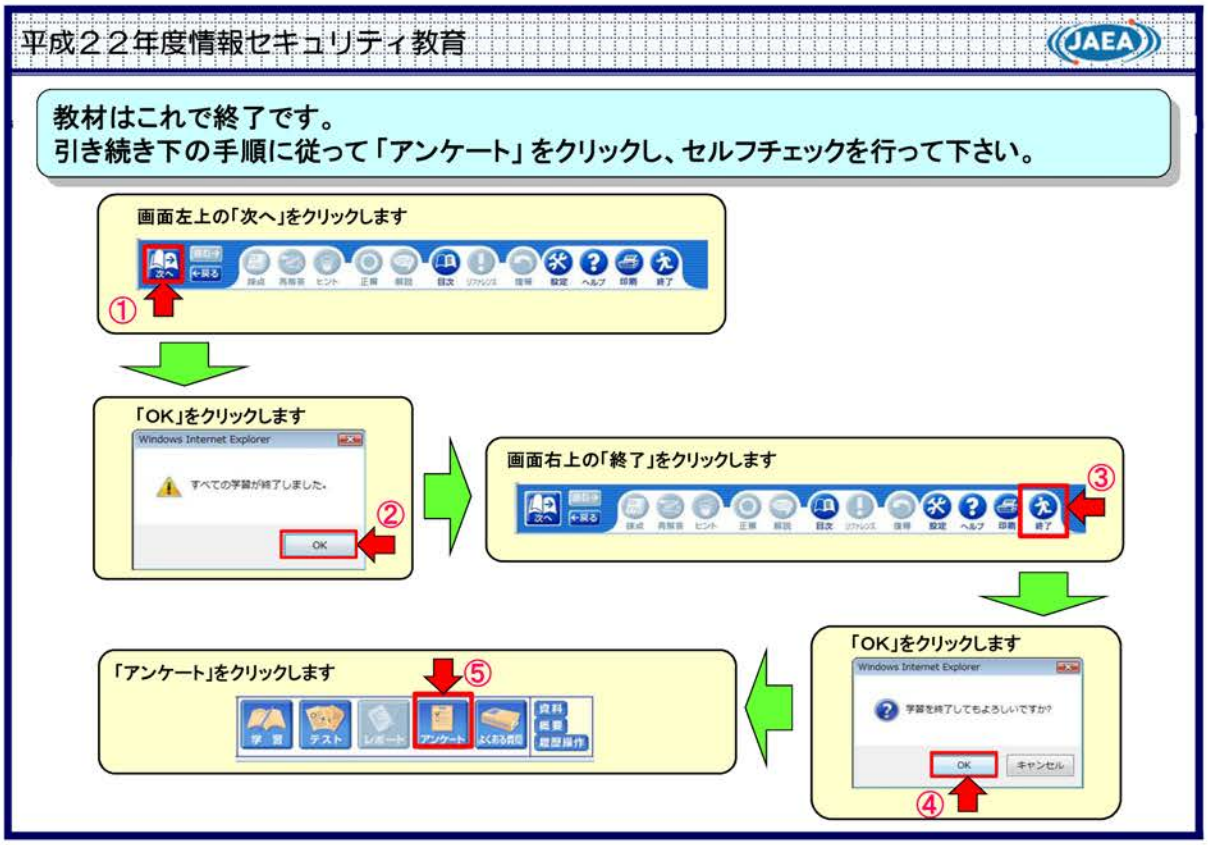
問1　ウイルス対策に関して正しい方を選択してください。

- A　自動実行（Autorun）機能は便利なので、有効活用している
- B　新種のウイルスに対応する為に、ウイルス対策ソフトウェアを最新の状態にしている

問2　外部記録媒体を利用する際の確認手順について正しい方を選択してください。

①PCからLANケーブルを抜く。
②ウイルス感染していないことを確認してから外部記録媒体を使用する。
③PCのウイルス対策をふとの定義ファイルおよびOSを最新の状態にする。
④外部記録媒体をPCに挿してウイルススキャンを行う。

- A　③→①→④→②
- B　①→③→④→②


平成２２年度情報セキュリティ教育
JAEA
教材はこれで終了です。
引き続き下の手順に従って「アンケート」をクリックし、セルフチェックを行って下さい。
画面左上の「次へ」をクリックします
①
「OK」をクリックします
Windows Internet Explorer
すべての学習が終了しました。
OK
②
画面右上の「終了」をクリックします
③
「OK」をクリックします
Windows Internet Explorer
学習を終了してもよろしいですか?
OK
キャンセル
④
「アンケート」をクリックします
⑤
学習
テスト
レポート
アンケート
よくある質問
資料
板書
意思操作

付録７　「情報セキュリティ脅威の動向と対策」

情報セキュリティ教育

情報セキュリティ 脅威の動向と対策

本教育の概要

2011年秋以降、政府関連機関、防衛関連企業、独立行政法人等で、「標的型攻撃」と呼ばれる高度なサイバー攻撃の被害が次々に発覚し、マスコミ等を賑わせています。

原子力機構もいつ標的にされるか予断を許さない状況であり、パソコン等の利用者一人一人が、日頃からしっかりと情報セキュリティ対策を行なっていないと、ある日突然、大きな被害を被る可能性があります。

また、パソコンのみならず、スマートデバイス（スマートフォン、タブレット端末等）を狙う不正プログラムや不正サイトも急速に増えており、アドレス帳や電話の発着信記録（本人および他人の個人情報）、ネットサービスのアカウント、文書、画像や動画、音声情報、位置情報、等々の漏えいのリスクが盛んに報道されています。

本教育は、こうした身近な脅威をしっかりと認識し、情報セキュリティ対策を着実に実施していただくことを 目的としています。

※本教育内で使用しているソフトウェアの名称、アイコン等は、各販売元等の登録商標です。

情報セキュリティ脅威の動向と対策

目次

情報セキュリティ脅威の動向と対策

1．標的型攻撃について

情報セキュリティ脅威の動向と対策

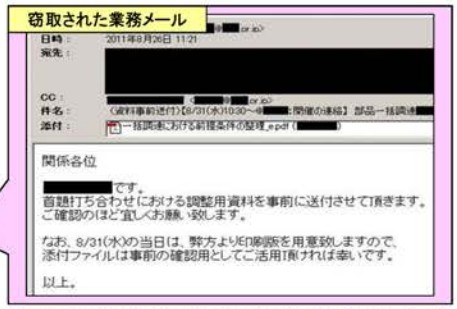
1．1 三菱重工への標的型攻撃の事例（1/2）

三菱重工が被害に遭った標的型攻撃の事例を紹介します。

日本航空宇宙工業会（SJAC）職員が、攻撃者から送られてきたメールの添付ファイルを開き、PCがウイルスに感染した。

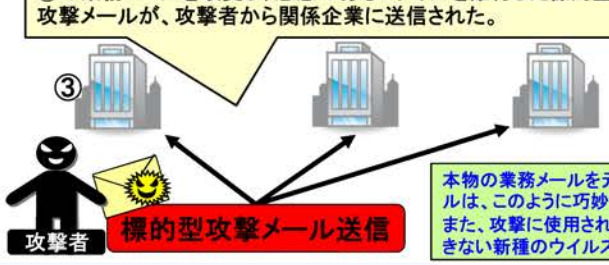
ウイルスの動作により、職員が関係企業とやり取りしていた業務メールを攻撃者に窃取されてしまった。

窃取された業務メール

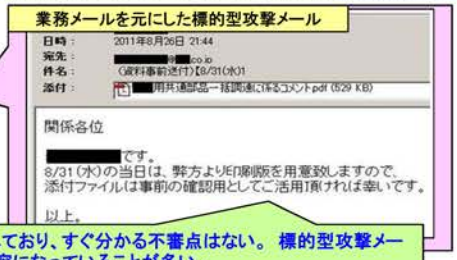


約10時間後

②の業務メールを改変し、悪意のあるファイルを添付した標的型攻撃メールが、攻撃者から関係企業に送信された。



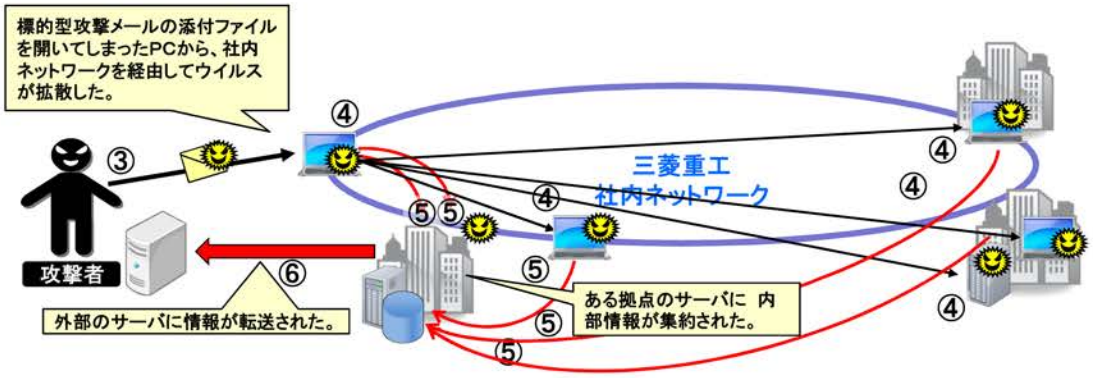
業務メールを元にした標的型攻撃メール



本物の業務メールを元にしており、すぐ分かる不審点はない。 標的型攻撃メールは、このように巧妙な内容になっていることが多い。
また、攻撃に使用されたウイルスは、その時点のウイルス対策ソフトでは検知できない新種のウイルスだった。

情報セキュリティ脅威の動向と対策

１．１　三菱重工への標的型攻撃の事例（２/２）



＜被害＞
ウイルス感染が確認されたPC等：１１拠点にまたがる計83台（サーバ 45台、一般PC 38台）
漏えいの疑いが報じられた情報　：
- 防衛省の装備品に関する受注情報
- ８０式空対艦誘導弾等の性能データ他、管理情報の一部
- 原子力発電所の設計や設備、耐震性などに関する情報
- 社員約2000人の個人情報
- IPアドレス他、社内システム情報の一部

Copyright © 2011 独立行政法人 情報処理推進機構
紹介した内容は、独立行政法人 情報処理推進機構(IPA)が複数の報道から導き出したシナリオに基づいています。

情報セキュリティ脅威の動向と対策

１．２　標的型攻撃への対策

標的型攻撃への対策は、以下の3項目がポイントになります。

標的型攻撃への対策

- 脆弱性対策をしっかりと行なう
  - １．３ 標的型攻撃への対策 【脆弱性対策編】 で解説します。
- 標的型攻撃メールに注意する
  - １．４ 標的型攻撃への対策 【メール編】 で解説します。
- ウイルス対策ソフトを活用する
  - １．５ 標的型攻撃への対策 【ウイルス対策ソフト編】 で解説します。

情報セキュリティ脅威の動向と対策

１．３　標的型攻撃への対策 【脆弱性対策編】（１/４）

情報機器に搭載されている各ソフトウェアの脆弱性対策が極めて重要です。
ソフトウェアを常に最新の状態にするよう心掛けてください。
特に、セキュリティパッチが提供されない「サポート期限切れのソフトウェア」は、脆弱性が放置されたままとなり、非常に危険です。

＜Microsoft Windowsシリーズのサポート期限＞

シリーズ名	Microsoftによるサポート期限
Windows 95, 98, Me, 2000, XP SP2(32bit版)	既に終了
Windows XP SP3（32bit版）、Windows XP SP2(64bit版)	2014年4月　8日
Windows Vista	2017年4月11日
Windows 7	2020年1月14日

脆弱性が放置されたままの危険な状態になっています。

＜Microsoft Officeシリーズ（Word、Excel、Power Point、Outlook他）のサポート期限＞

シリーズ名	Microsoftによるサポート期限
Office XP（Office 2002）以前	既に終了
Office 2003 SP3	2014年　4月　8日
Office 2007 SP3	2017年10月10日
Office 2010 SP1	2020年10月13日

脆弱性が放置されたままの危険な状態になっています。

以下のサイトにMicrosoft社製品のサポート期限に関する情報があります。
Microsoft プロダクトサポートライフサイクル：http://support.microsoft.com/gp/lifeselect

既に業連等で周知しておりますとおり、メーカによるサポートが終了した古いOS等を利用しているPCは、機構ネットワークの利用を制限させていただきます。

情報セキュリティ脅威の動向と対策

１．３　標的型攻撃への対策 【脆弱性対策編】（２/４）

特段の注意が必要なソフトウェア

脆弱性対策は、インストールされている全てのソフトウェアが対象となりますが、ここに挙げたソフトウェアは利用者数が多い等の理由で狙われ易く、脆弱性に対する特段の注意が必要です。

OS
- Microsoft　Windows
- Apple Mac OS

機構イントラ（http://intra.jaea.go.jp）内「ｺﾝﾋﾟｭｰﾀ&ﾈｯﾄﾜｰｸ利用」ページにて、随時、脆弱性対策に関する情報を提供しております。

アプリケーションソフトウェア
- Internet Explorer
- Firefox
- Google Chrome
- JAVA
- JRE
- Microsoft Office
- Adobe Reader
- Adobe Acrobat
- Adobe Flash

これらのソフトウェアのセキュリティ修正プログラムは、提供され次第速やかに適用してください。
自動更新の設定が可能なソフトウェアについては、予め自動更新が有効になるように設定しておいてください。

情報セキュリティ脅威の動向と対策

１．３　標的型攻撃への対策 【脆弱性対策編】（３/４）

独立行政法人 情報処理推進機構(IPA)が公開しているソフトウェアバージョン確認ツール「MyJVN バージョンチェッカ」により、PCにインストールされているチェック対象ソフトウェア(※)のバージョンが最新かどうかを確認することができますので、ご活用ください。

※チェック対象ソフトウェアの一覧：http://jvndb.jvn.jp/apis/myjvn/vccheck.html#myjvnapp04

MyJVNバージョンチェッカ： http://jvndb.jvn.jp/apis/myjvn/vccheck.html

**最新のバージョンではないと判定されたソフトウェアは、
表示される案内や次ページの情報を参考に、最新版に更新してください。**

情報セキュリティ脅威の動向と対策

１．３　標的型攻撃への対策 【脆弱性対策編】（４/４）

（参考）セキュリティ修正プログラムの入手方法について

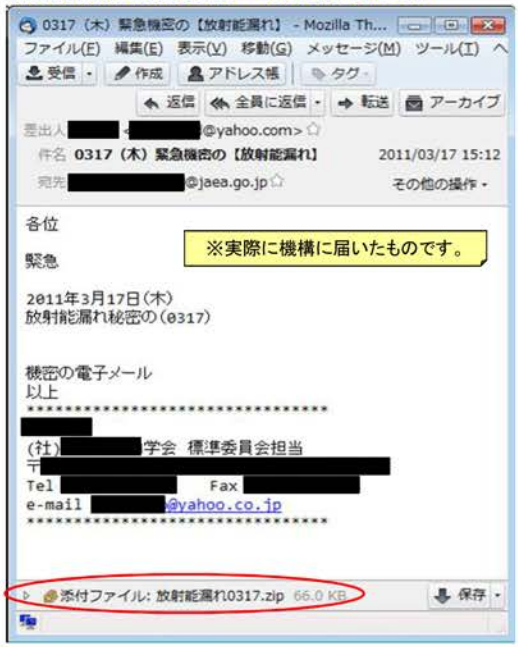
ソフトウェア名	セキュリティ修正プログラムの入手先、確認方法等
Microsoft Windows, Internet Explorer, Microsoft Office	Windows Update (Microsoft Update) を実施するか、以下のURLにアクセスする http://www.update.microsoft.com/microsoftupdate/
Adobe Reader, Adobe Acrobat	【バージョン10以降を使用している場合】 ①[スタート]－[すべてのプログラム] から「Adobe Reader」または「Adobe Acrobat」を起動 ②[ヘルプ]－[アップデートの有無をチェック] し、その後は案内に従いバージョンアップ
	【バージョン9以前を使用している場合】 http://get.adobe.com/jp/reader/ から最新版を入手する
Adobe Flash	http://get.adobe.com/jp/flashplayer/ から最新版を入手する
JAVA, JRE	http://www.java.com/ja/download/ から最新版を入手する
Firefox	①[スタート]－[すべてのプログラム] から「Mozilla Firefox」を起動 ②[ヘルプ]－[ソフトウェアの更新を確認] をクリック ③案内に従いバージョンアップ
Google Chrome	①[スタート]－[すべてのプログラム] から「Google Chrome」を起動 ②[Google Chromeの設定] －[Google Chromeについて] を選択し、その後は案内に従いバージョンアップ
QuickTime	http://www.apple.com/jp/quicktime/download/ から最新版を入手する

このページの情報を以下のイントラページにも掲載しております。
http://cnet-guide.jaea.go.jp/security/vercheck.html

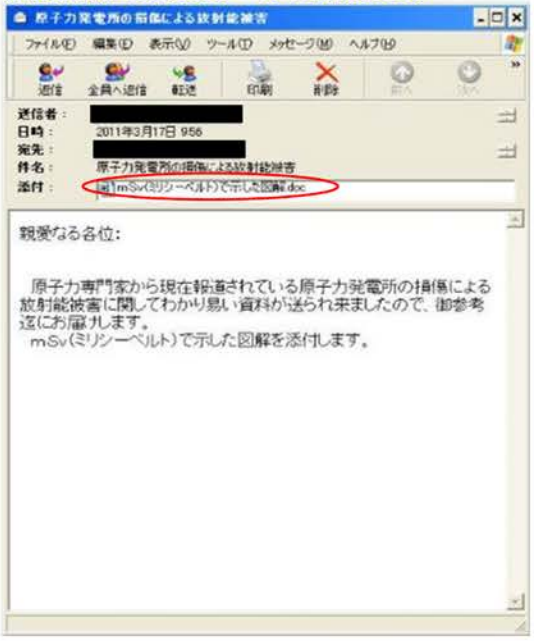
情報セキュリティ脅威の動向と対策

１．４　標的型攻撃への対策 【メール編】（１/３）

原発事故に便乗したメールの例（その１）



原発事故に便乗したメールの例（その２）



情報セキュリティ脅威の動向と対策

１．４　標的型攻撃への対策 【メール編】（２/３）

標的型攻撃メールは、以下に示すような「騙しのテクニック」を駆使しており、不審な点に気づくことが困難になっています。ご注意ください。

件名や内容が不自然にならないよう、かつ、受信者の関心をひくように工夫している。

守秘情報であることを強調したり、タイムリーなテーマで受信者の関心をひくように工夫しています。
2011年は、東日本大震災や原発事故に便乗した標的型攻撃メールの事例が多数報道されました。

信頼できそうな組織のメールアドレスを詐称している。

従来に比べ、官公庁や独立行政法人、関連団体等のメールアドレスを詐称するものが増えています。

Microsoft Officeの文書ファイルやPDFファイルを添付したものが増えている。

不信感を持たれ易い実行形式（.exe、.scr、.bat、.pif等）のファイルではなく、Microsoft Office の文書ファイル（.doc、.xls等）やPDFファイル（.pdf）を添付したものが増えています。

実行形式のファイルを他の形式に偽装している場合もある。

ファイル名の途中にRLOと呼ばれる右から左へ文字列を反転して読ませる制御文字を加え、添付ファイルが実行形式（.exe、.scr、.bat、.pif等）のファイルであることが容易に分からないように偽装している場合もあります。

例

表示上のファイル名	：サンプル_rcs.doc	見ると文書ファイルのように見えます。
PCに認識されるファイル名	：サンプル‮cod.scr	実際は、文書ファイルを装った実行形式のファイルです。

ここにRLO制御文字を挿入し、実際と表示の左右を反転させる偽装が施されています。

情報セキュリティ脅威の動向と対策

１．４　標的型攻撃への対策 【メール編】（3/3）

次のようなメールは安易に開かないよう、ご注意ください。

- 日頃やりとりすることがない相手から届いた。
- 何故自分に送られてきたのか、心当たりがない。
- 日頃やりとりすることがない種類のファイルが添付されている。
- いつもはパスワード付きの圧縮ファイルを添付してくるのに、パスワードなしの圧縮ファイルが添付されている。
- 実行形式(.exe、.scr、.bat、.pif等)のファイルが添付されている。(偽装にも注意)
- 無料メールサービス(Gmail、Yahooメール等)のアドレスを利用している。
- 何となく違和感を感じる。

そのメールに記載されている連絡先ではなく、電話番号案内(104)、Web等から送信者の連絡先を調べ、そのメールを送ったか直接確認する。

送信者への確認の結果、不審メールであると判明した場合は、以下に連絡してください。

情報システム管理室　ネットワークセキュリティ管理チーム
内線:[redacted]　メールアドレス:[redacted]

情報セキュリティ脅威の動向と対策

１．５　標的型攻撃への対策 【ウイルス対策ソフト編】（1/2）

システム計算科学センターが配布しているウイルス対策ソフトを導入してください。

システム計算科学センターが配布しているウイルス対策ソフトは、機構に適した設定を施しています。PCの適正な管理のため、必ず導入してください。

≪システム計算科学センターが配布しているウイルス対策ソフト≫

Microsoft Windows用　：McAfee VirusScan for Windows
Apple Mac OS用　　：McAfee VirusScan for Mac
Linux、UNIX系OS用　：Sophos Anti-Virus for Linux/UNIX

導入はこちらのページから ⇒ http://cnet-guide.jaea.go.jp/virus/

関連規程

情報システムセキュリティ対策基準：第１８条
　課室情報セキュリティ責任者は、電子計算機（当該電子計算機で動作可能なウイルス対策ソフトウェア等が存在しない場合を除く。）にウイルス対策ソフトウェアを導入するものとする。システム計算科学センターが当該計算機で動作可能なウイルス対策ソフトを配布していない場合は、同等の機能を有するウイルス対策ソフトウェアを導入するものとする。ただし、実験や計測のための情報システム等において、所期の性能を維持するためにウイルス対策ソフトウェア等を導入できない場合は、この限りではない。

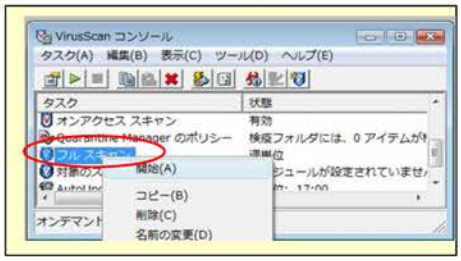
２　課室情報セキュリティ責任者は、想定される不正プログラムの感染経路のすべてにおいてウイルス対策ソフトウェア等により不正プログラム対策を実施するものとする。また、前項によりウイルス対策ソフトウェア等を導入できない場合には、当該電子計算機ではメール及びWebを利用しない、未検疫の可搬型記憶媒体を接続しない、他の情報システムと分離する等の不正プログラム感染防止措置を講ずるものとする。

情報セキュリティ脅威の動向と対策

１．５　標的型攻撃への対策 【ウイルス対策ソフト編】（2/2）

最低でも月に１回はすべての電子ファイルのウイルス検査（フルスキャン）を実施してください。

侵入時にウイルス対策ソフトで検知できなかった新種のウイルスを、その後のパターンファイルの更新によって検知出来るようになる場合があります。
定期的にフルスキャンを行なうことで、そのようなウイルスの早期発見が期待できます。



関連規程

情報システムセキュリティ対策基準：第３４条
　不正プログラムの感染を未然に防止するため、ウイルス対策ソフトウェアの使用に当たっては、次の各号に定める事項を遵守するものとする。
(1) ウイルス対策ソフトウェアを常時動作させて使用すること。
(2) 不正プログラムの検疫は、最新の不正プログラム検疫エンジン及び不正プログラム定義ファイルにて実施すること。
(3) 定期的にすべての電子ファイルについて不正プログラムチェックを行うこと。

情報セキュリティ脅威の動向と対策

１．６　確認テスト

問1不審なメールへの対応に関して、正しい方を選択してください。

A　差出人は業務でやり取りをしている人だが、本文に違和感があった為、メールに記載されている電話番号ではなく、自分で調べた電話番号に電話して、本人にそのメールを送信したか確認した。

B　同じ差出人から、2日前と同じ文面のメールが届いた。添付ファイル名が前回のメールと異なっていたので、確認の為に開いてみた。

問2 脆弱性に対する対応について、正しい方を選択してください。

A　OSのアップデート情報が出ていたが、ウイルス対策ソフトを導入している為、しばらくは大丈夫だろうと思い、その場で更新 しなかった。

B　OSの状態を常に最新にする為、アップデートを自動実行するように設定している。

情報セキュリティ脅威の動向と対策

2．スマートデバイスを取り巻く脅威

2．1 スマートデバイスを取り巻く脅威の現状
2．2 確認テスト

情報セキュリティ脅威の動向と対策

2．1　スマートデバイスを取り巻く脅威の現状（1／2）

現在、スマートフォン、タブレット端末等を取り巻く脅威が深刻な状況のため、これらの機構業務での利用はご遠慮ください。

Android OSを搭載したスマートデバイスを例に、情報漏えいに繋がり易い脅威の現況を示します。

脅威	脅威の説明	脅威を軽減する対策	備考（注意点等）
セキュリティパッチの提供が必ずしも迅速に行なわれない	Google社のAndroid OSに端末メーカが独自の機能追加等を行なって製品化しているため、脆弱性発見後の対応がメーカや機種によって異なる。最悪、対応されない場合もある。	サービス事業者や端末メーカのサポート情報に注意する。	常に情報収集を怠らないようにすること。
		新バージョンのAndroid OSを導入できない旧機種は、できるだけ速やかに新機種に移行する。	Android OSのバージョン更新頻度は比較的高いので、新機種等の発売情報に注意すること。
信頼できるとされるマーケット内にも、不正アプリケーションが混在している	アプリケーションの流通が統制されておらず、不正アプリケーションが出回り易い。ウイルス等を混入した不正アプリケーションが正規アプリケーションと同名で流通している場合もある。	信頼できるとされるマーケットでも用心する。	常に情報収集を怠らないようにすること。
		インストール時、不用意にアクセス許可をしない。	疑問を感じるアクセス許可を求められた場合は、インストールを中止すること。
		端末に対応するセキュリティソフトを導入する。	PCのウイルス対策ソフトほど有効性が高くないので、過信しないこと。
QRコードや短縮URLを用いた不正サイトへの誘導が起き易く、気づきにくい	QRコードや短縮URLを用いてURL偽装された不正サイトにアクセスしてしまい、入力情報や端末内の情報を窃取される場合がある。	Webフィルタリングを利用する。	有効性が高いとは言い難い状況なので、過信しないこと。
		端末に対応するセキュリティソフトを導入する。	PCのウイルス対策ソフトほど有効性が高くないので、過信しないこと。

（1/2）

情報セキュリティ脅威の動向と対策

2．1　スマートデバイスを取り巻く脅威の現状（2／2）

脅威	脅威の説明	脅威を軽減する対策	備考（注意点等）
不正なWiFiアクセスポイントが存在している	WiFiアクセスポイントの中には、通信の傍受を目的とした不正なものが存在しており、各種サービスのIDやパスワードを窃取される等の被害に遭う場合がある。	信頼できるサービス事業者が設置しているアクセスポイントを利用する。	設置者が不明なアクセスポイントを利用しないこと。
近距離無線通信機能を悪用した目的外の読み取り（スキミング）が可能	電子決済等のための近距離無線通信機能を搭載する端末では、機能を悪用され、電子マネー等を窃取される可能性がある。	利用しない場合は機能をロックする。	サービス利用後のロック忘れに注意すること。
		機能部分に通信を遮蔽するカバーをつける。	商品の一例： エレコム社「スキムバリア」
メモリーカードの抜き取りが容易に可能	端末からメモリーカードを抜き取られ、保存したデータを窃取される。	データをできるだけ暗号化する。	暗号化の抜け・漏れがないように注意する。
		メモリーカード装着部にセキュリティシールを貼付する。	商品の一例： サンワサプライ社「セキュリティシール」
盗難や置き忘れによる紛失が起き易い	端末に保存したデータを窃取される。	端末のロック機能やデータ消去機能を利用する。	ロック解除用パスワードをできるだけ複雑にすること。
	端末に保存した各種サービス（バンキング、ショッピング、写真・データ保存、Web Mail等）のIDやパスワードを用いて、なりすまし利用される恐れがある。	ユーザIDやパスワードを非保存設定にする。	面倒でも毎回入力すること。

（2/2）

情報セキュリティ脅威の動向と対策

2．2　確認テスト

問1スマートフォンやタブレット端末の利用に関して、正しい方を選択してください。

A　スマートフォンやタブレット端末は、携帯性や操作性に優れていて便利なので、積極的に業務に取り入れて活用すべきである。

B　スマートフォンやタブレット端末を情報セキュリティの観点から評価すると、現状では情報漏えい等のリスクが高いと考えられ、機構の業務での利用は推奨できない。

情報セキュリティ脅威の動向と対策

3．情報セキュリティに関する再周知

3．1 持ち出しに関する遵守事項
3．2 外部記録媒体がウイルスに感染していないことを確認する
3．3 自動実行(Autorun)機能を停止する
3．4 機構メールアドレスで受信したメールを自動転送しない
3．5 情報機器の移行・廃棄に関する対策
3．6 パスワードを適切に設定・管理する
3．7 各種申請および変更手続きを正しく行う
3．8 確認テスト

情報セキュリティ脅威の動向と対策

3．1 持ち出しに関する遵守事項（1／2）

2010年度、出張中に機構の情報を格納した情報機器を盗難される事例が立て続けに発生しました。
盗難・亡失への備えとして、持ち出し時には、以下の4つの事項をすべて厳守してください。
なお、詳細は「*機構外での情報処理に関する実施手順書*」を参照してください。

1．持ち出しは、必要最小限にする

持ち出す情報、情報機器、記録媒体等を精選し、持ち出しは必要最小限にしてください。
万一の際の被害を少なく抑えられ、情報の管理も容易になります。
なお、機構の拠点間の移動も持ち出しに当たりますので、ご注意ください。

2．持ち出す場合は、必ず申請して許可を得る

持ち出しに際しては、格納している情報および暗号化の状態を確認の上、課室情報セキュリティ責任者に申請し、許可を得る必要があります。
PC本体だけではなく、USBメモリや外付けハードディスクについても漏れなく手続きを行なってください。
なお、機構支給以外の情報機器へ格納できる情報は一般情報（公知情報、公開しても機構の業務の遂行に支障を及ぼす恐れのない情報）のみとなっておりますので、ご注意ください。

「機構外での情報処理に関する許可申請書・誓約書 兼 パソコン等物品持出し申請書」
http://intra3.jaea.go.jp/kitei/19ethbg_/06vxevzwz_/172dopro/172dopro.xls

情報セキュリティ脅威の動向と対策

３．１　持ち出しに関する遵守事項（２／２）

３．持ち出す情報を暗号化する

万一の際に情報を読み取られないようにするため、メールの保存領域等を含め、持ち出す情報を漏れなく暗号化してください。

【推奨】「まるごと暗号化」に対応した持ち出し専用のPCや外部記録媒体を利用する

※「*機構外での情報処理に関する実施手順書*」に暗号化ソフトを例示しています。

関連規程

情報システムセキュリティ対策基準：第４９条２項７号
機器等及び記録媒体を機構外に持ち出す場合には、暗号化の措置を行うこと。

４．持ち出す情報の記録を残す

盗難・亡失の際には、格納していた情報の正確な特定を求められます。
持ち出す情報のファイル名のリストを作成し、機構内に保存してください。

【推奨】持ち出す情報のバックアップを取得し、機構内に保存する

【ファイル名のリストを作成するツール】
get filelist.bat （機構イントラネットより入手可能）
http://cnet-guide.jaea.go.jp/security/johotejun/johotejun.html#08_02

関連規程

情報システムセキュリティ対策基準：第４９条２項８号
機器等及び記録媒体を機構外に持ち出す場合には、持ち出した情報を特定するために必要な情報を記録に残すこと。

情報セキュリティ脅威の動向と対策

３．２　外部記録媒体がウイルスに感染していないことを確認する

機構内で「USBメモリを媒介とするウイルス」の検知が頻発しております。

外部記録媒体（USBメモリ、外付けHDD、CD/DVD等）は、ウイルスに感染していないことを確認してから使用してください。

＜確認手順＞
① PCのウイルス対策ソフトの定義ファイルおよびOSを最新の状態にする。
② PCからLANケーブルを抜く。
③ 外部記録媒体をPCに挿してウイルススキャンを行う。
④ ウイルス感染していないことを確認してから外部記録媒体を使用する。

情報セキュリティ脅威の動向と対策

３．３　自動実行(Autorun)機能を停止する

USBメモリ等をパソコンに接続した際、ウイルスを含むファイルが自動的に実行されてしまうことを防ぐため、自動実行（Autorun）機能を停止してください。

Windows 7 での設定方法

①「スタート」―「コントロールパネル」をクリックする。

②「ハードウェアとサウンド」をクリックする。

③「CDまたは他のメディアの自動再生」をクリックする。

④「全てのメディアで自動再生を使う」のチェックを外す。

⑤「保存」をクリックする。

Windows 7 以外での設定方法は、以下を参照願います。
PC等情報機器の情報セキュリティ実施手順書
http://cnet-guide.jaea.go.jp/security/tejun/tejun.html#06_04

情報セキュリティ脅威の動向と対策

３．４　機構メールアドレスで受信したメールを自動転送しない

機構メールアドレスで受信した電子メールには、非公開情報や個人情報等、機構外に不用意に持ち出すことが不適切な情報が含まれる可能性があります。
自動転送は、こうした情報を適正な管理をすることなく、サービス事業者のサーバ、個人の携帯やパソコン等、機構外の情報機器に蓄積することになり、情報漏えいの危険性が著しく高まりますので、行なわないでください。

関連規程

文書管理規程：第５条２項
文書は、必要ある場合を除き、みだりに機構外への持ち出し、又は機構外部ネットワークへの発信等をしてはならない。

秘密文書取扱規程：第１３条２項
秘文書及び機構外秘文書をＦＡＸ、電子メールその他の電子的手段により送付する場合には、宛先を十分に確認し、送信直前に受信者に連絡の上、送信直後にその受信を確認しなければならない。

情報システムセキュリティ対策基準：第４９条２項
職員等及び外来者等は、規程第28条に定める機構外での情報処理に関する許可を得る場合には、次の各号に定める事項について措置を講ずるものとする。
(1) 情報及び機器等又は記録媒体に要機密情報が含まれていないことを事前に確認すること。要機密情報を機構外へ持ち出すことが機構の業務遂行上不可避である場合には、秘密文書取扱規程に定める管理責任者の許可を得ること。

情報セキュリティ脅威の動向と対策

３．５　情報機器の移行・廃棄に関する対策

修理や廃棄、リース満了後の返却等により、情報機器が機構の管理下を離れる場合は、以下に例示する方法等により、情報の読み取りが不可能になるように措置してください。データ消去等が不可能な場合、契約先と守秘義務契約を結ぶ等の措置を講じてください。

・廃棄時　：ハードディスク等の記録部分を物理的に破壊するか、
　データ消去ツールでデータを消去する。
・修理時　：ハードディスク等の取り外しが可能であれば取り外して一時保管するか、
　データ消去ツールでデータを消去する。
・リース返却時：データ消去ツールでデータを消去する。

廃棄するPC内のデータは、フォーマットやリカバリをしても、復元ツール等で情報の読み取りが可能な場合があります。

ツールを使い、確実にデータ消去します。

データ消去ツールの一例

Darik's Boot and Nuke（DBAN）
→ 配布元　：http://www.dban.org/
→ 操作方法：http://www.atmarkit.co.jp/fsecurity/rensai/securitytips/024dban.html

関連規程

情報システムセキュリティ対策基準：第３９条
　記録装置の含まれる機器等について機構外へ移行する場合（機器等が機構の管理下になくなる場合）又は廃棄する場合は、ハードディスクや記録媒体内のデータの消去、初期化、破砕等、情報の復元が不可能となるような措置を講じた後、移行又は廃棄するものとする。
２　リース満了等により記録装置の含まれる機器等を返却する場合は、ハードディスクや記録媒体内のデータをデータ消去ツールにて消去した後、返却するものとする。

情報セキュリティ脅威の動向と対策

３．６　パスワードを適切に設定・管理する

ユーザアカウント（ユーザID、パスワード）は機構の情報資産を守るうえで重要な役割を果たしています。
多くの場合、ユーザIDは管理者より発行されたものを使用しますが、パスワードは、利用者自らが設定・管理する必要があります。他人に不正に利用されることがないよう、パスワードを適切に設定・管理しましょう。

安全性の高いパスワード

- 長さ　：８文字以上にする。文字数が多いほど安全性が高まる。
- 文字種：アルファベット、句読点、記号および数字を含めるなど、使用する文字種が多いほど安全性が高まる。
- 更新　：最低でも3ヵ月に一度は更新する。その際、連続して同じパスワードを使い回さない。
- 多様性：複数のサービスで同じパスワードを使い回さない。

安全性の低いパスワードの例

- 辞書に載っているような単語。
- 逆スペリングの単語、よくあるミススペル、略語。
- 連続した文字。　例：12345678、777777、abcdefg、qwerty（キーボード上で連続している）
- 自分の名前、生年月日、電話番号などを元にした簡単なもの。

情報セキュリティ脅威の動向と対策

3．7　各種申請および変更手続きを正しく行う

機構ネットワークに関連するサービスは、システム計算科学センターにて、皆さまからの申請に基づいて登録や管理を行なっております。
申請に抜けや誤りがあると、インシデント時の対応に支障が生じ、障害が長時間・広範囲に渡る等、機構ネットワークの運用に深刻な影響を及ぼす場合があります。機構ネットワークの健全性を維持するため、申請はもとより、変更等が生じた際の手続きを確実かつ速やかに行っていただきたく、よろしくお願いいたします。

各種申請へのクイックリンク		問い合わせ先
・IPアドレスの交付 ・利用者や機器の変更 ・廃棄等に伴う返却	IPアドレス交付申請 http://cnet-guide.jaea.go.jp/network/ipinfo.html ※未申請の機器の利用は厳禁です。	
・メールアドレスの交付 ・所属や氏名の変更 ・退職等に伴う返却	メールアドレス交付申請 http://cnet-guide.jaea.go.jp/network/mailinfo.html	
・機構外から機構内の情報システムを利用する ・機構内から機構外の情報システムを利用する	アクセス許可申請 http://cnet-guide.jaea.go.jp/access/index.html	
・機構外で機構の情報処理を行なう ・持ち出しを行なう ・機構支給以外の情報機器を利用する	機構外での情報処理に関する実施手順書　※申請様式へのリンクがあります http://cnet-guide.jaea.go.jp/security/johotejun/index.html	

情報セキュリティ脅威の動向と対策

3．8　確認テスト

問1 持ち出しに関して、正しい方を選択してください。

A　持ち出す情報機器に格納している情報の内容や暗号化の状態を十分に確認していれば、手続きを行わずに持ち出しても問題ない。

B　USBメモリや外付けハードディスクを持ち出す場合も、課室情報セキュリティ責任者へ申請し、許可を得る必要がある。

問2 持ち出しに関して、正しい方を選択してください。

A　本人しか利用出来ないようにOSのパスワードを設定している為、暗号化をせずにPCを持ち出した。

B　万一の際でも情報を読み取られない様、PCをまるごと暗号化してから持ち出した。

情報セキュリティ脅威の動向と対策

3．8　確認テスト

問3 PCを廃棄する際のデータ消去に関し、正しい方を選択してください。

A ハードディスクのフォーマットやリカバリを行なえば、情報を読み取られる恐れはない。

B ハードディスクのディスク部分を物理的に破壊するか、データ消去ツールで確実に消去しない限り、情報を読み取られる恐れがある。

問4 パスワード管理について、正しい方を選択してください。

A 忘れると大変なので、同じパスワードを使いまわしている。

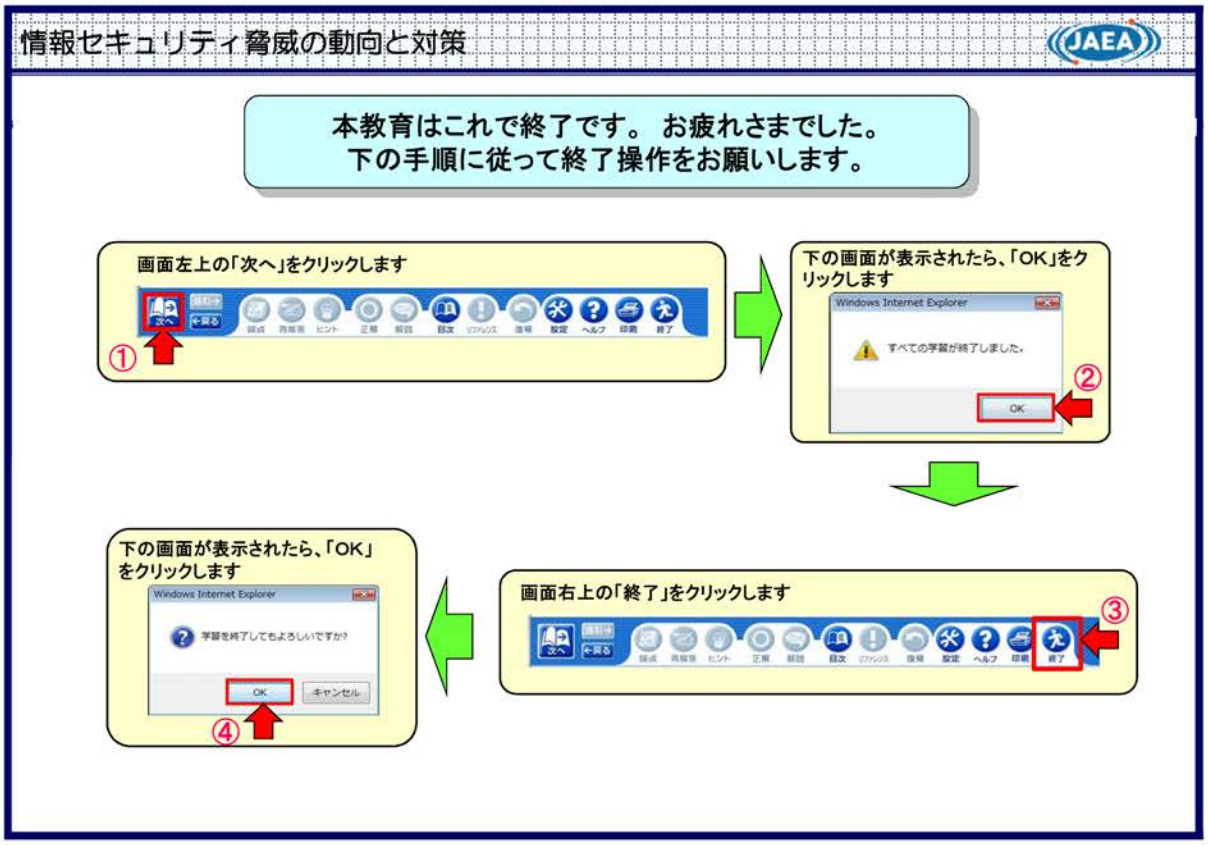
B パスワードを定期的に変更している。

情報セキュリティ脅威の動向と対策

出典元・関連リンク

出典元	
IPA 独立行政法人 情報処理推進機構	http://www.ipa.go.jp/
IIJ Internet Initiative Japan	http://www.iij.ad.jp/
JAPAN SMARTPHONE SECURITY FORUM	http://www.jssec.org/

関連リンク	
標的型攻撃対策レポート	http://www.ipa.go.jp/security/fy23/reports/measures/index.html
『新しいタイプの攻撃』への対策	http://www.ipa.go.jp/security/vuln/newattack.html
不正アクセス届出情報	http://www.ipa.go.jp/security/txt/2012/02outline.html#5
脆弱性に関する届出情報	http://www.ipa.go.jp/security/vuln/report/vuln2011q4.html
スマートフォンへの脅威と対策	http://www.ipa.go.jp/about/technicalwatch/20110622.html


情報セキュリティ脅威の動向と対策
JAEA
本教育はこれで終了です。 お疲れさまでした。
下の手順に従って終了操作をお願いします。
画面左上の「次へ」をクリックします
次へ
戻る
①
下の画面が表示されたら、「OK」をクリックします
Windows Internet Explorer
すべての学習が終了しました。
OK
②
画面右上の「終了」をクリックします
終了
③
下の画面が表示されたら、「OK」をクリックします
Windows Internet Explorer
学習を終了してもよろしいですか?
OK
キャンセル
④

付録８　「原子力機構内における情報セキュリティ事案とその対策」

～ 情報セキュリティ教育～

機構内における情報セキュリティ事案とその対策

本教育の概要

平成24年度は機構に対しても「標的型攻撃」があり、コンピュータウイルスの感染により情報が漏えいする事案が発生しました。また、海外出張中の職員が、海外の空港においてパソコン盗難被害に遭う事案が発生しました。

本教育では、今回発生した「標的型攻撃」の手口とその対策方法、パソコンの盗難・亡失に備えた情報漏えい対策や発生時の連絡方法などを主要な内容としております。

本教材では、マルウェア、悪性プログラム、コンピュータウイルスを総称し「ウイルス」と呼びます。

※本教育内で使用しているソフトウェアの名称、アイコンなどは、各販売元などの登録商標です。

機構内における情報セキュリティ事案とその対策

目次

機構内における情報セキュリティ事案とその対策

１．標的型攻撃について

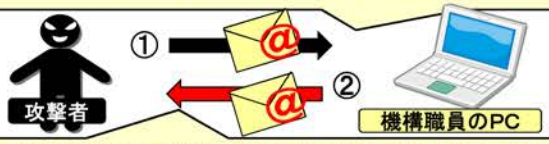
標的型攻撃とは、特定の企業または組織が標的にされる攻撃のことです。

機構内における情報セキュリティ事案とその対策

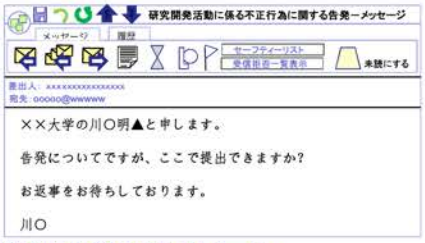
１．１ 機構に対する標的型攻撃の事例（その１）

大学関係者になりすました攻撃者は、機構職員とメールで何回か連絡を取り合った後、ウイルス付きメールを送りつけてきました。事前にやり取りしたことで、職員は、送られてきたメールを不審に思わず開封してしまい、ウイルスに感染しました。

①告発の受付窓口を確認するメールが、大学関係者になりすました攻撃者から機構に送られてきました。



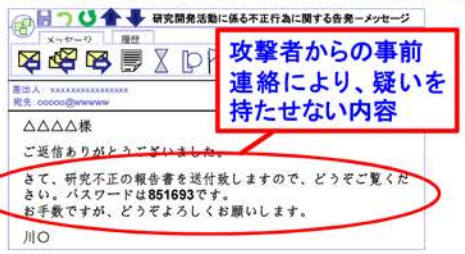
②機構職員は攻撃者に、この窓口で間違いありませんという内容で返答しました。



攻撃者から送付されたメール

③返答したメールアドレスに対し、攻撃者から、「告発書.zip」というファイルが添付されたメールが送られてきました。

④告発書.zipを開いた機構職員のPCがウイルスに感染しました。



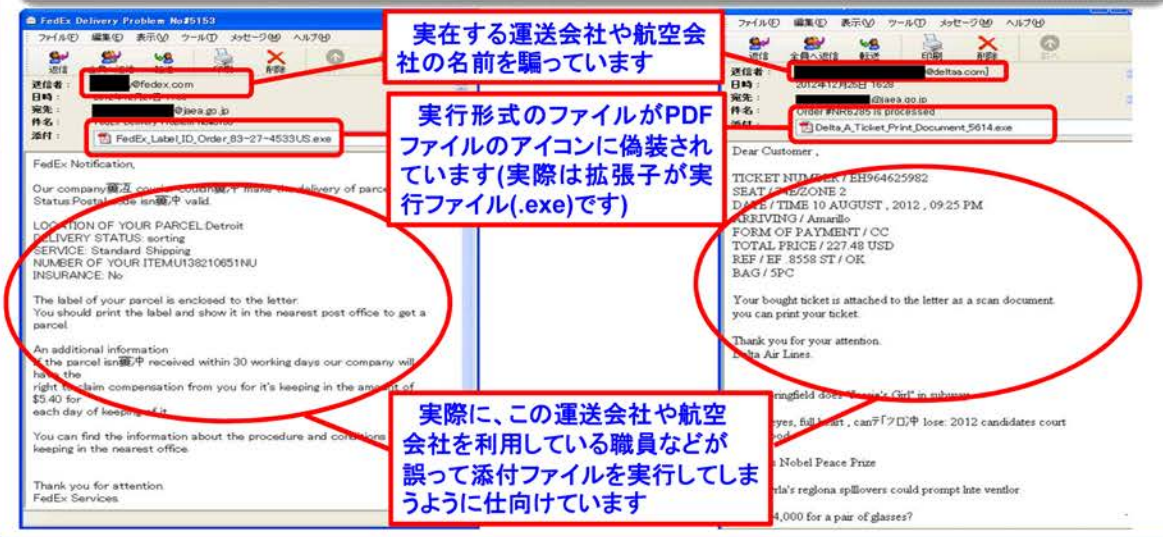
攻撃者からの事前連絡により、疑いを持たせない内容

攻撃者から送付されたメール

機構内における情報セキュリティ事案とその対策

1．1　機構に対する標的型攻撃の事例（その2）

実在する運送会社や航空会社の名前を騙り、メールアドレスを詐称したウイルス付きメールが、機構の不特定の職員に送りつけられました。メール送信者が実在する企業だったことで不審感を抱かず、また、添付ファイルのアイコンが偽装されていたことに気づかなかったため、何人かの職員はついメールを開封してしまい、ウイルスに感染しました。



機構内における情報セキュリティ事案とその対策

1．2　標的型攻撃メールの特徴

機構に送られてきた標的型攻撃メールは、以下に示す「騙しのテクニック」が駆使されているのが特徴であり、不審な点に気づくことが困難でした。

特定の部署を狙い、件名や内容が不自然にならないように工夫されている

公開ホームページに掲載されている問い合わせ窓口など、面識のない人からのメールも読まれる部署に送付してきました。
また、各窓口の要件に合うようメールの件名や内容を工夫もされていました。

差出人とメールアドレスを詐称し疑われない工夫されている

受信者が疑わないように実在する組織名を騙ったり、メールアドレスを詐称していました。

実行形式のファイルを他の形式のファイルに偽装されている

Microsoft Officeの文書ファイル(Word・Excel)やPDFのアイコンに偽装されていました。また、右書き制御文字を利用し、実行ファイルと分からないようにファイル名を偽装していました。

機構内における情報セキュリティ事案とその対策

１．３　標的型攻撃への対策

標的型攻撃への対策は、以下の3項目がポイントになります。

不審と感じないよう工夫したメールがあることに注意する

メールの添付ファイルの取り扱いに注意する

１．４ 標的型攻撃への対策 【標的型攻撃メールへの対策】で解説します。

なお、メールシステムで行っている対策は、１．５ 標的型攻撃への対策 【メールシステムにおける制限事項について】で説明します。

問い合わせ対応専用PCを設置する

１．６ 標的型攻撃への対策 【問い合わせ対応専用PCの設置】で解説します。

機構内における情報セキュリティ事案とその対策

１．４　標的型攻撃メールへの対策（１/４）

実在する大学の関係者や会社名などを騙って、相手を油断させる手法をソーシャルエンジニアリングと言います。「人」を対象にして心の隙やミスから入り込み、不正アクセスや機密情報を入手する心理的な攻撃手法です。
ソーシャルエンジニアリングの悪用を防ぐには、相手の手口を知り、常に「疑う」という心構えを持つことが重要です。

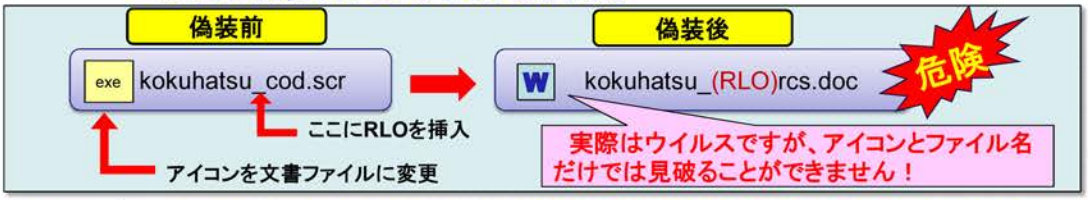
ソーシャルエンジニアリングを利用した標的型攻撃の手口(一例)

- ホームページに記載されている職員の名前を騙たり、相手を油断させます。
- 付き合いのある業者や関係者から情報を入手し、悪用します。
- ホームページからダウンロード出来る様式(例えば、人事採用に係る書類)にウイルスを埋め込んで送りつけます。
- SNS（Facebookなど）を利用して関係者になりすまして近づき、ウイルスを仕掛けたサイトへ誘導したり、直接ウイルスを送りつけます。

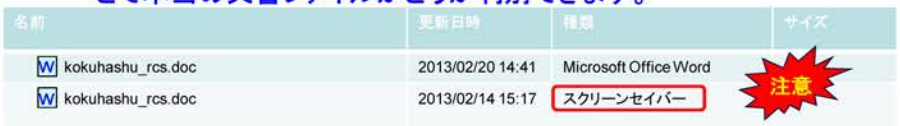
機構内における情報セキュリティ事案とその対策

1．4　標的型攻撃メールへの対策（2/4）

解説　標的型攻撃メールで送付される添付ファイル（ウイルス）には、RLOと呼ばれる右から左へ文字を読む言語に対応する機能を悪用して、普通の文書ファイルのように偽装されているものがあります。



対策　フォルダの「詳細表示の設定」で「種類」、または「並べて表示」を 選択することで本当の文書ファイルかどうか判別できます。



また、RLOを利用したファイルの実行を禁止するPCの設定をしてください。

詳細は、以下を参照願います。
ファイル名にRLOを使用したファイルの実行禁止設定
http://cnet-guide.jaea.go.jp/index.php/ja/security/security-setup

機構内における情報セキュリティ事案とその対策

1．4　標的型攻撃メールへの対策（3/4）

解説　標的型攻撃メールで送付される添付ファイル（ウイルス）は、アイコンを偽装して普通の文書ファイルに見せかけ、実行形式のプログラム（拡張子がexeやscr）であることを隠します。

拡張子：そのファイルの種類を示す3～4の文字列

ファイルの内容	拡張子の表示設定	
	表示しない設定	表示する設定
通常の文書ファイル	文書	文書.doc
ウイルスの疑いがあるファイル	文書	文書.exe
ウイルスの疑いがあるファイル	文書.doc	文書.doc.exe

アイコンが偽装されています！

拡張子が”exe”の為、文書ファイルではありません！

通常のファイルと見分けがつきません！(二重拡張子)

対策　Windows標準の設定では、拡張子が表示されずファイルの種類をアイコンにより判別する設定となっていますので、拡張子を表示する設定を行なってください。

詳細は、以下を参照願います。
Windows のファイル表示設定（拡張子、隠しファイル）
http://cnet-guide.jaea.go.jp/index.php/ja/security/security-setup

機構内における情報セキュリティ事案とその対策

1．4　標的型攻撃メールへの対策　-まとめ-（4/4）

次のようなメールは安易に開かないよう、ご注意ください。

- 日頃やりとりすることがない相手から届いた。
- 何故自分に送られてきたのか、心当たりがない。
- 日頃やりとりすることがない種類のファイルが添付されている。
- いつもはパスワード付きの圧縮ファイルを添付してくるのに、パスワードなしの圧縮ファイルが添付されている。
- 圧縮ファイルの中に実行形式(.exe、.bat、.pifなど）のファイルが入っている。（偽装にも注意）
- 無料メールサービス（Gmail、Yahooメールなど）のアドレスを利用している。
- 何となく違和感を感じる。

そのメールに記載されている連絡先ではなく、電話番号案内（104）、Webなどから送信者の連絡先を調べ、そのメールを送ったか直接確認してください。

送信者への確認の結果、不審メールであると判明した場合や、添付ファイルを開いた時に不審な動きや白紙（中身が無い）などの期待していた動作ではない場合は、PCからネットワークケーブルを抜き、そのままの状態を維持して、速やかに以下に連絡してください。

情報システム管理室　ネットワークセキュリティ管理チーム
内線：[redacted]　メールアドレス：[redacted]

機構内における情報セキュリティ事案とその対策

1．5　メールシステムにおける制限事項について

情報セキュリティ対策強化のため、以下のようにメールシステムで添付ファイルの取扱いを制限しております（平成24年度情報セキュリティ委員会決定事項）。

1．ウイルス感染のリスクが高い、次の形式のファイルを添付したメールの送受信を原則禁止
1)実行ファイル形式及びそれに類するファイル形式：exe、scrなど
2)zipを除く圧縮形式：rar、lzh、7-zipなど

メール送受信において制限される添付ファイルのリストを掲載しています。（随時更新）http://cnet-guide.jaea.go.jp/index.php/ja/security/security-security/92-japanese-category/security-ja/1093-ngappend

2．禁止対象ファイルを添付したメールを機構の外から受信した場合の処置
禁止対象ファイルが添付されているメールは、メールシステム側で当該ファイルを削除し、本文のみを利用者に配信しています。

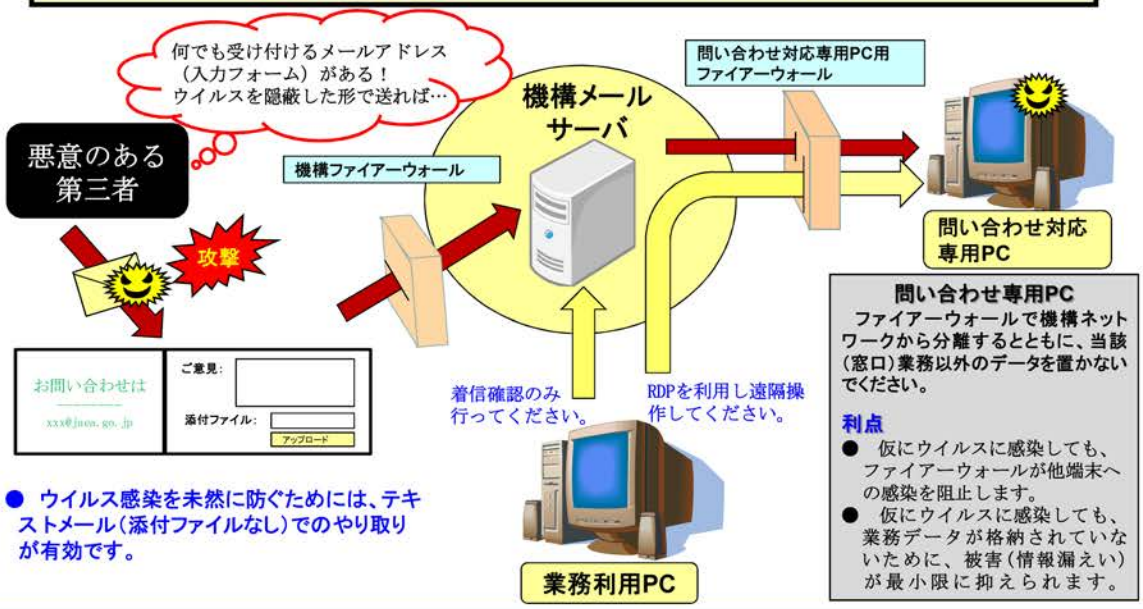
3．業務上、禁止対象ファイルのメールでの送受信が不可欠な場合の対処
実行ファイル形式及びそれに類するファイル形式の拡張子を変更するなどしてそのままでは開けないようにしてください。

禁止対象ファイルを格納したzipファイルや禁止対象ファイル以外（Microsoft Officeの文書ファイル(Word・Excel)やPDFファイルなど）の添付ファイルを受け取った場合、信頼できる人からのメールを除き、ウイルスの可能性を必ず疑ってください。

機構内における情報セキュリティ事案とその対策

1．6　問い合わせ対応専用PCの設置（機構公開サーバ管理者対象）

公開しているホームページに問い合わせ窓口などを設置している管理者は、ウイルスが送りつけられることを前提に、問い合わせ対応専用PCを設置してください。



● ウイルス感染を未然に防ぐためには、テキストメール（添付ファイルなし）でのやり取りが有効です。

問い合わせ専用PC

ファイアーウォールで機構ネットワークから分離するとともに、当該（窓口）業務以外のデータを置かないでください。

利点

- 仮にウイルスに感染しても、ファイアーウォールが他端末への感染を阻止します。
- 仮にウイルスに感染しても、業務データが格納されていないために、被害（情報漏えい）が最小限に抑えられます。

機構内における情報セキュリティ事案とその対策

2．パソコン盗難・亡失における情報セキュリティ対策

機構内における情報セキュリティ事案とその対策

2．1　機構での盗難被害事例と問題点（ケース1）

被害内容

平成24年6月、フランスから国内へ帰路において、機構支給のノートPCをスーツケースに入れ航空会社に預けたところ、成田空港到着時にスーツケースの鍵が壊されており、荷物を確認したところノートPCが無くなっていました。

問題点

1) 常に携行しなくてはならないノートPCをスーツケースに入れ、航空会社に預けてしまいました。
2) 航空会社に預けた荷物は、紛失または盗まれる可能性があるという認識に欠けていました。

対策

1) 機構外での情報処理に関する許可申請書※の誓約を遵守してください。
2) ノートPCなどの情報機器は、航空会社に預けず、肌身離さず機内に持ち込んでください。

※機構外での情報処理に関する許可申請書・誓約書　兼　パソコン物品持出し申請書（様式 - 1）
http://intra3.jaea.go.jp/kitei/19ethbg_/06vxevzwz_/172dopro/172dopro.xls

機構内における情報セキュリティ事案とその対策

2．1　機構での盗難被害事例と問題点（ケース2）

被害内容

平成24年6月、外国出張中の空港の公衆トイレにて、一人が機構職員に肩を接触させて注意を逸らせている隙に、もう一人が足元へ置いてあった機構職員のバッグを盗みました。バッグには、業務に使用する個人のノートPC、機構外から機構ネットワークにアクセスする際に使用する認証機器(ハードウェアトークン)などが入っていました。

問題点

1) 機構外で個人のノートPCを業務に使用するための手続き（機構外での情報処理申請※1、機構支給以外情報機器の使用許可申請※2）の認識がなく、情報セキュリティ責任者の許可なしに個人のノートPCを業務に使用していました。
2) 使用予定が無いハードウェアトークンを持ち出していました。
3) 空港内の公衆トイレで足元にバックを置いてしまいました。

※1機構外での情報処理に関する許可申請書・誓約書　兼　パソコン物品持出し申請書（様式 - 1）
http://intra3.jaea.go.jp/kitei/19ethbg_/06vxevzwz_/172dopro/172dopro.xls
※2機構支給以外情報機器の業務への使用許可申請書　兼　使用終了確認書（様式 - 2）
http://cnet-guide.jaea.go.jp/images/security/yoshiki2.xls

対策

1) 機構外への情報機器などの持出しは、必要最小限にしてください。
2) 機構外で情報機器などを使用する場合は、必ず許可手続きをしてください。
3) 申請書の誓約を遵守して、ノートPCなどの情報機器は、公衆の場では肌身離さずに携行してください。

機構内における情報セキュリティ事案とその対策

2．2　盗難・亡失に備える

持ち出す 情報、情報機器、記録媒体などを精選し、必要最小限に 止める

管理を容易にするとともに、万一の場合に被害を少なくします。

必要最小限（例）
発表用資料のみを保存した記憶媒体1つだけ持ち出す

ノートPCと、USBメモリと、資料のデーター式と、あとこの資料も…
とりあえず全部持っていこう…

情報機器、記録媒体などをまるごと暗号化する

万一の場合に備え、情報機器、記録媒体などを丸ごと、AES 256ビットなどの十分な強度を持つ方式で暗号化します。

HDD → まるごと暗号化 → PC
＊＃＠△＄☆％･･･
暗号化されているので、読み出すことが出来ません

外部記録媒体の認証機能を利用する

パスワードロック、指紋認証などのセキュリティ機能が付いた外部記録媒体を使用し、第三者による情報へのアクセスを防止します。
また、ウイルス検知機能付きの製品を使用することが望ましい。

HDD

持ち出す情報のバックアップを機構内に保管し、万一の場合に全情報を復元できるようにする

情報機器を亡失した場合、メールの1通に至るまで、格納されている全ての情報内容を確認、報告する必要が生じます。
また、事業継続の観点からもバックアップは必須です。

機構PC → HDD 機構内に保管
持ち出す情報のバックアップ

持ち出す際には必ず申請する

PC本体だけではなく、USBメモリや外付けハードディスクについても漏れなく情報機器持ち出しの手続きが必要です。私物の情報機器へは機構の業務情報を格納しないでください。

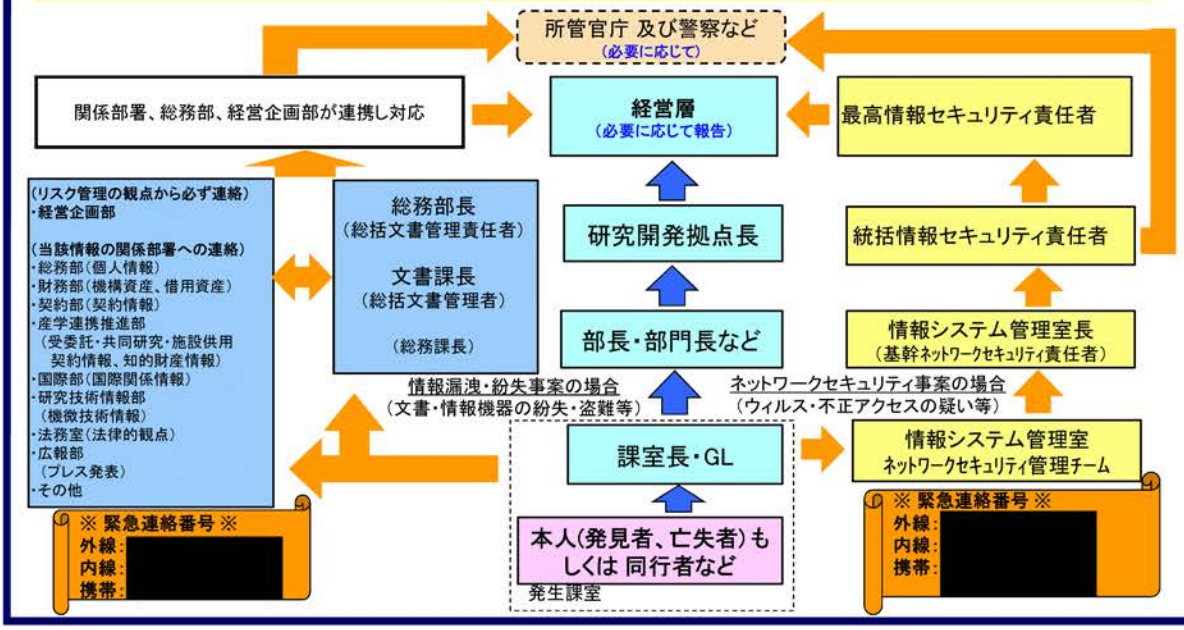
速やかに連絡出来るよう準備する

万一盗難・亡失した場合、速やかに連絡できるように、課室長・GLの連絡先を確認し、手帳などに控えてください。

機構内における情報セキュリティ事案とその対策

2．3　緊急時の対応

情報機器の盗難・亡失が発生(発見)した場合には、直ちに課室情報セキュリティ責任者(課室長・GL)に連絡し、指示を受けてください。



機構内における情報セキュリティ事案とその対策

3．普段から取り組むべき情報セキュリティ対策

3．1 パソコン、ネットワークの正しい利用
3．2 ウイルス対策
3．3 メーカサポートが終了するOSなどの対応
3．4 電子メールのテキスト形式の設定
3．5 パスワードの適正な設定

機構内における情報セキュリティ事案とその対策

3．1 パソコン、ネットワークの正しい利用

外部のWeb管理者から誤解を受けた事例

機構のPCからインターネットを用いて、右に示すようなキーワードを入力して検索したところ、外部のWebサイト管理者から著作権侵害と誤解されました。

誤解され易い検索キーワード（例）
- アプリ 広告解除
- 有料アプリ 無料化
- アプリ ライセンス認証 解除
- 有料アドオン 不正利用

対策

- 業務に必要であっても、キーワードによっては誤解を招く可能性があるため、検索する際には配慮が必要です。インターネット利用においても社会から信頼される良識ある行動を心がけてください。
- 業務に不必要なサイトを閲覧する行為は、コンプライアンス上の問題もさることながら、情報セキュリティ上の脅威に晒される危険性が高いので行なわないでください。

機構内から外部へのアクセス状況は、機構のセキュリティシステムにより全て記録されています。

機構内における情報セキュリティ事案とその対策

3．1　パソコン、ネットワークの正しい利用

フリーソフトからのウイルス感染事例

ダウンロードしたフリーソフト（例：freepdfunlocksetup）に、ウイルスが埋め込まれており、フリーソフトをインストールした時にウイルスが活動し、外部のサーバへ通信を行っていました（ただし、情報漏えいはありませんでした）。

対策

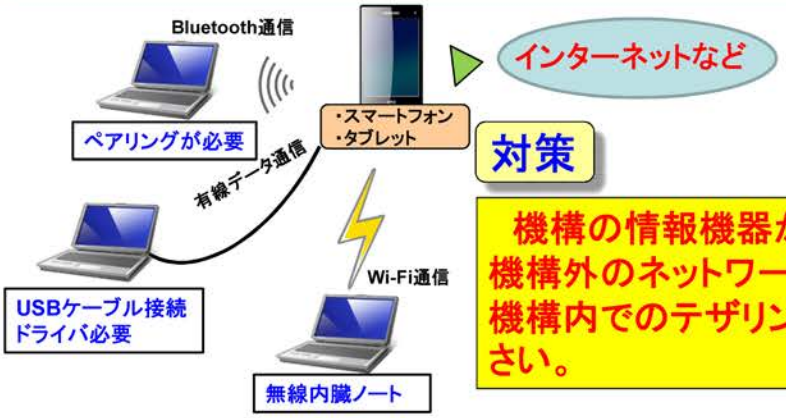
- 事例に示すように、フリーソフトの中にはウイルスが仕込まれた危険なものがあることを認識し、安易にインストールはしないでください。
- 業務利用の必要性を勘案してソフトウェアライセンス管理規定に従い、ソフトウェア管理責任者の許可を得てからPCへインストールを行なってください。

機構内における情報セキュリティ事案とその対策

3．1　パソコン、ネットワークの正しい利用

テザリングの危険性について

最近のスマートフォンには、スマートフォンをアクセスポイント（親機）として、PCなどの機器（子機）を接続して外部ネットワークへつなぐテザリング機能が備わっています。
テザリング機能が有効になっていた場合、機構の情報機器がスマートフォンを介して機構外のネットワークに直接接続されてしまう可能性があります。



対策

機構の情報機器が意図しないところで機構外のネットワークに接続しないよう、機構内でのテザリング利用は控えてください。

機構内における情報セキュリティ事案とその対策

３．２　ウイルス対策 - 検出数と増加原因 -

下のグラフに示すように、機構内でのウイルスの検出数は、毎月200件以上あり、システム計算科学センターから配布しているウイルス対策ソフトにより、ウイルス感染を未然に防いでいます。

ウイルスの検出数が、特に多かった原因として挙げられるのが、

① ウイルス対策ソフトを導入していないPCがウイルス感染していました。ウイルスがネットワークを介して感染を拡げようとしたことを、ウイルス対策ソフトが導入されている他のPCにより検出されました。

②・④ 機構内外で「標的型攻撃」が発生したことを受けて、全PCのフルスキャンを実施、侵入時に未検出だったウイルスが最新の定義ファイルにより検出されました。

③ 外来者が持ち込んだ外部記憶媒体(USBメモリ)からウイルスが検出されました。

機構内でのウイルス検出数

機構内における情報セキュリティ事案とその対策

３．２　ウイルス対策

1．ソフトウェアを常に最新の状態にする

ウイルスはソフトウェア（OS及びアプリケーションソフトウェア）の脆弱性を悪用して感染活動を行うことが多いです。このため、ソフトウェアのセキュリティ更新プログラム(セキュリティパッチなど)が提供された際には速やかに適用してください。

2．ウイルス対策ソフトウェアを必ず導入する

システム計算科学センターが配布しているウイルス対策ソフトの導入が、情報システムセキュリティ対策基準第18条により義務付けられています。機構に適した設定が施されている計算センター配布のウイルス対策ソフトを必ず導入してください。

なお、ウイルス対策ソフトが導入されていないPCについては、機構ネットワークの利用を制限させていただく場合があります。

3．全ての電子ファイルを定期的にスキャンをする

侵入時にウイルス対策ソフトで検出できなかった新種のウイルスを、その後の定義ファイルの更新によって、検出できることがあります。定期的にフルスキャンを実施してください。

4．外部記憶媒体について確実にスキャンを行う

外部記憶媒体(USBメモリなど)を利用する際は、ウイルスに感染していないことを決められた手順で確認してから使用してください。

個人所有のUSBメモリなどは、職場で使用しないでください。

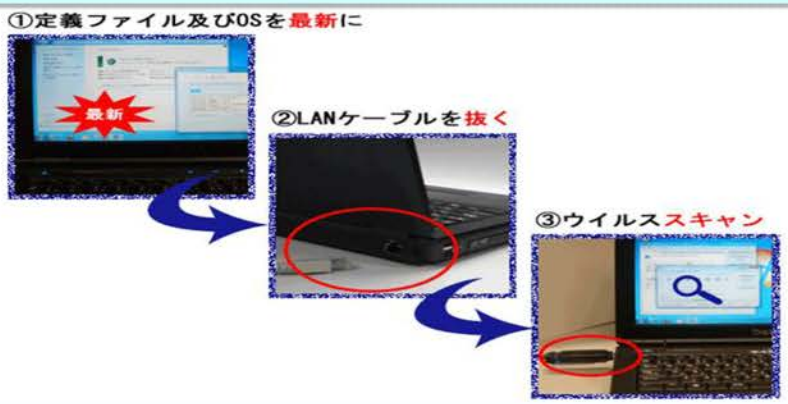
USBメモリなどの外部記録媒体を利用する際の確認ついては次ページで説明します。

機構内における情報セキュリティ事案とその対策

3．2　ウイルス対策　-外部記録媒体を利用する際の確認-

**外部記録媒体（USBメモリ、外付けHDD、CD/DVDなど）は、
ウイルスに感染していないことを確認してから使用してください。**

＜確認手順＞
① PCのウイルス対策ソフトの定義ファイルおよびOSを最新の状態にする。
② PCからLANケーブルを抜く。
③ 外部記録媒体をPCに挿してウイルススキャンを行う。
④ ウイルス感染していないことを確認してから外部記録媒体を使用する。



機構内における情報セキュリティ事案とその対策

3．3　メーカサポートが終了するOSなどの対応　-Windowsのサポート期限-

サポート期限切れのOSを使い続けると
主に次のことが問題となります。

1．セキュリティの問題が修正されない

セキュリティの問題(脆弱性)が発見された時に、メーカから提供されるセキュリティ更新プログラム(セキュリティパッチなど)により脆弱性を塞ぐことができます。サポート期限が切れると更新プログラムの提供が終了し、脆弱性が放置され、ウイルス感染の危険性が高まります。

2．最新版のウイルス対策ソフトが導入できない

ウイルスの感染を防ぐ為には最新版のウイルス対策ソフトの導入が欠かせませんが、古いOSのフォローを続けることは難しく、OSのサポート期限を目安に対応を終了し、導入できなくなるソフトウェアが多くあります。サポート終了したOSへ導入できる古いウイルス対策ソフトを導入しても、日々進化するウイルスの感染を防ぐ手立てとはなり得ません。

機構内における情報セキュリティ事案とその対策

3．3　メーカサポートが終了するOSなどの対応　-Windowsのサポート期限-

Microsoft社によるサポート期限を過ぎると、セキュリティパッチなどが提供されません。

OS名	Microsoft社による サポート期限
Windows XP	2014年4月8日
Windows Vista（全エディション）	2017年4月11日
Windows 7（全エディション）	2020年1月14日
Windows Server 2003（全エディション）	2015年7月14日
Windows Server 2008（全エディション）	2020年1月14日

期限まで約1年

Microsoft社によるサポートが終了したWindowsは、脆弱性が放置されたままの危険な状態になります。

Windows XPを使用中のPCにおいては、上の示した期限までにメーカサポートが有効な後継OSへ移行するようにしてください。

※Mac OSについて※
Apple社はMacOSは、最新バージョンより二世代前のOSについては、セキュリティアップデートが無くなり、事実上のサポート終了と言えます。
情報セキュリティを維持するため、最新のMac OSに移行してください。

機構内における情報セキュリティ事案とその対策

3．3　メーカサポートが終了するOSなどの対応　-Javaのサポート期限-

JavaSE 6 のサポート期限の終了について

Java SE 6は、2013年2月末日をもってサポートが終了しています。
Java SE 6がインストールされているままのPCは、速やかにJava 7にバージョンアップしてください。

● Oracle Java SE サポート・ロードマップ
http://www.oracle.com/technetwork/jp/java/eol-135779-ja.html

Java 7 は最新版にアップデートしてください

「Java 7 Update 15」およびそれ以前のすべての バージョンで、深刻な脆弱性が発見されています（2013/03/05時点）。
Oracle社のサイトにて java（JREなど）を最新バージョンにアップデートしてください。

【関連サイト】
Oracle Security Alert for CVE-2013-1493（英語）

http://www.oracle.com/technetwork/topics/security/alert-cve-2013-1493-1915081.html

機構内における情報セキュリティ事案とその対策

３．４　電子メールのテキスト形式の設定

HTML形式のメール表示機能やメールソフトのプレビュー機能が悪用され、不正なスクリプト（プログラム）が実行される危険性があります。
スクリプトが実行されると悪意あるホームページに誘導され、ウイルスに感染する恐れがあります。

●受信した電子メールを**テキストとして表示**するようにしてください。
●HTML形式の電子メールを送信しないでください。
●メールソフトのプレビュー機能をオフにしてください。

設定手順について詳細は、以下を参照願います。
PC等情報機器の情報セキュリティ実施手順書
http://cnet-guide.jaea.go.jp/index.php/ja/security/security-tejun
パソコンのセキュリティ確保のための設定手順
http://cnet-guide.jaea.go.jp/index.php/ja/security/security-setup

機構内における情報セキュリティ事案とその対策

３．５　パスワードの適正な設定

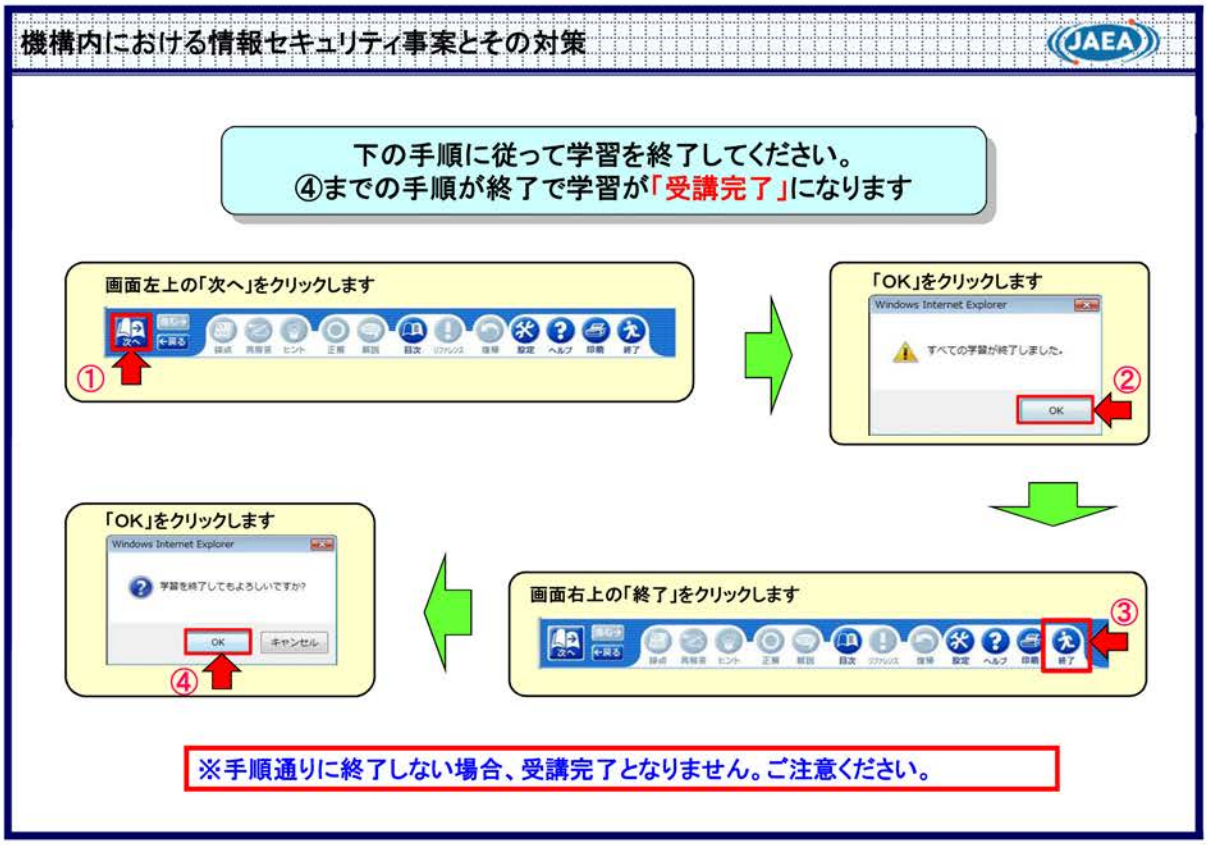
パスワードは、機構の情報資産を守るうえで重要な役割を果たしています。
多くの場合、パスワードは、利用者自らが設定・管理する必要があります。
他人に情報機器が不正に利用されることがないよう、パスワードを適切に設定・管理してください。

安全性の高いパスワード

- 長さ　：**８文字以上にする。**文字数が多いほど安全性が高まる。
- 文字種：アルファベット、句読点、記号および数字を含めるなど、使用する文字種が多いほど安全性が高まる。
- 更新　：最低でも3ヵ月に一度は更新する。その際、連続して同じパスワードを使い回さない。
- 多様性：複数のサービスで同じパスワードを使い回さない。

安全性の低いパスワードの例

- 辞書に載っているような単語。
- 逆スペリングの単語、よくあるミススペル、略語。例：pass→ssap、word→ward
- 連続した文字。　例：12345678、777777、abcdefg、qwerty（キーボード上で連続している）
- 自分の名前、生年月日、電話番号などを元にした簡単なもの。


機構内における情報セキュリティ事案とその対策
JAEA
下の手順に従って学習を終了してください。
④までの手順が終了で学習が「受講完了」になります
画面左上の「次へ」をクリックします
①
「OK」をクリックします
Windows Internet Explorer
すべての学習が終了しました。
OK
②
画面右上の「終了」をクリックします
③
「OK」をクリックします
Windows Internet Explorer
学習を終了してもよろしいですか?
OK
キャンセル
④
※手順通りに終了しない場合、受講完了となりません。ご注意ください。

付録９　「パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について」

～課室情報セキュリティ責任者向け教育～

パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

目次

パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

はじめに

平成22年度、平成24年度と続けて海外出張中の機構職員が、パソコン（以下、PCといいます）の盗難被害に遭っています。

盗難・亡失は、「いつ」「どこ」で発生するか分からないものです。

機構の情報が格納されたPCなどの盗難・亡失は、情報漏えい事案となりえます。情報が漏えいした場合、機構内、取引先、関連研究機関などの様々な関係者に被害が波及することになります。また、機構支給品の盗難・亡失や情報漏えい事案は、文部科学省や経済産業省及び会計検査院などの関連省庁への報告も必要になります。

本教育は、課室情報セキュリティ責任者である、課室長の方々に、その役割と責任を再認識して頂くためのものであり、

1)機構外での盗難・亡失による情報漏えいを防ぐために、
機構外での情報処理を許可する場合のポイントと対策、

2)盗難・亡失が発生してしまった場合の連絡体制

について解説します。

パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

1　機構における盗難被害事例（平成２２年度盗難事案）

事例1：シャルル・ド・ゴール空港からパリ市内へ向かう列車にて

途中駅に停車中、男がコインを床に落とし、機構職員の注意を逸らしている隙に、横に置いてあった機構職員のバッグを別の男が持ち去った。
バックの中には、機構支給のノートPC、USBメモリ、外付けハードディスクが入っていた。

事例2：チューリッヒ空港へ向かう列車にて

途中駅に停車中、通路に置いていたスーツケースを「移動した方がいい」と男に助言され、機構職員が座席から立ち上がり、スーツケースを移動している隙に、座席に置いてあった機構職員のリュックをその男が持ち去った。
リュックの中には、機構支給のノートPC、個人所有のUSBメモリが入っていた。

パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

1　機構における盗難被害事例(平成２４年度盗難事案)

事例1:マルセーユ空港にて

空港の公衆トイレで、男が機構職員の肩に接触し注意を逸らせている隙に、足元に置いてあった機構職員のバッグを別の男が持ち去った。
バッグには、個人所有のノートPC、機構支給のハードウェアトークン(認証機器)が入っていた。

事例2:フランスから国内への帰路にて

機構支給のノートPCをスーツケースに入れ航空会社に預けたところ、成田空港到着時にスーツケースの鍵が壊されており、荷物を確認したところノートPCが無くなっていた。

パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

2　盗難被害における問題点

機構で発生した盗難事案は、盗難のプロと思われる仕業であり、これを防ぐことは困難でした。
一方で、機構職員がノートPCなどを肌身離さずに携行するなど、機構の情報セキュリティポリシー※1、※2を遵守していれば、被害は最小限に防げたかもしれません。

※1:情報セキュリティ管理規程【22(規程)第35号】
※2:情報システムセキュリティ対策基準について【23シ(通達)第3号】

具体的な問題点を以下に示します。

問題点1　機構外での情報処理申請※3、機構支給以外情報機器の使用許可申請※4の手続きをせずに、機構外へノートPCなどを持ち出していた。

※3:機構外での情報処理に関する許可申請書・誓約書　兼　パソコン物品持出し申請書(様式 - 1)
※4:機構支給以外情報機器の業務への使用許可申請書　兼　使用終了確認書(様式 - 2)

問題点2　必要以上にノートPCやUSBメモリなどを持ち出していた。

問題点3　ノートPCを航空会社に預けたり、ノートPCなどが入ったカバンやリックから目を離してしまった。

パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

3　盗難・亡失への対策（その1）

課室情報セキュリティ責任者は、機構から支給されている情報機器などを機構外で利用させる場合、盗難・亡失に備えて以降の1～5に示す対策を徹底させてください。

1．機構外で情報処理をする場合は、必ず手続きをさせる

課室情報セキュリティ責任者は、課室・グループ員が機構外で機構から支給されている情報機器や記録媒体（これらに格納される情報を含む）を利用する場合は、

①機構外での情報処理申請（様式 - 1）、

②機構支給以外情報機器の使用許可申請（様式 - 2）

の**手続きを必ず実施**させるようにしてください（②は必要に応じて）。

また、課室情報セキュリティ責任者は、申請手続きを通して、課室・グループ員の**機構外での情報処理の内容を把握**するとともに、情報機器などの持ち出しにおける**リスク分析を実施**してください。

リスク分析については、「4　盗難・亡失へのリスク分析について」にて説明します。

パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

3　盗難・亡失への対策（その2）

2．情報機器や記録媒体に格納された情報を全て暗号化させる

平成22年度の盗難事案を受けて機構外に情報機器や記録媒体を持ち出す場合、情報機器や記録媒体に格納された情報を**全て暗号化することが義務化**※1されています。

格納された情報を全て暗号化することにより、盗難・亡失時の情報漏えいのリスクが大きく低減されます。

※1：情報システムセキュリティ対策基準について第49条2項7号

3．持ち出す情報機器や記憶媒体、及びこれらに格納する情報は、必要最小限にさせる

持ち出す情報機器などを**必要最小限**※2にすることで管理が容易になり、盗難・亡失時の被害の最小化や情報漏えいリスクの低減につながります。

※2：情報セキュリティ管理規定第28条5項、第28条6項

パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

３　盗難・亡失への対策（その３）

4．漏えいした情報を特定するため、機構内に持ち出した情報のバックアップを保管させる

情報機器や記録媒体を盗難・亡失し、情報漏えい事案が発生した場合には、メールの１通、1通に至るまで、格納されている全ての情報内容を確認して報告する必要が生じます。

課室・グループ員に被害品（情報を含む）の特定が容易になるよう、**持ち出し品リストやバックアップ**の作成※1を徹底させてください。

※1：情報システムセキュリティ対策基準について第49条2項8号

5．持ち出す情報機器などは、肌身離さず携行させる

持ち出し中は情報機器などから**目を離したり**、**安易に預けたり**せず、**常に携行**させるように指導してください。盗難・亡失に遭うリスクの低減につながります。

また、盗難・亡失が発生した場合、課室・グループ員が直ちに対応できるよう、「**緊急時における連絡先**」の再確認をしてください。

パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

４　盗難･亡失へのリスク分析について

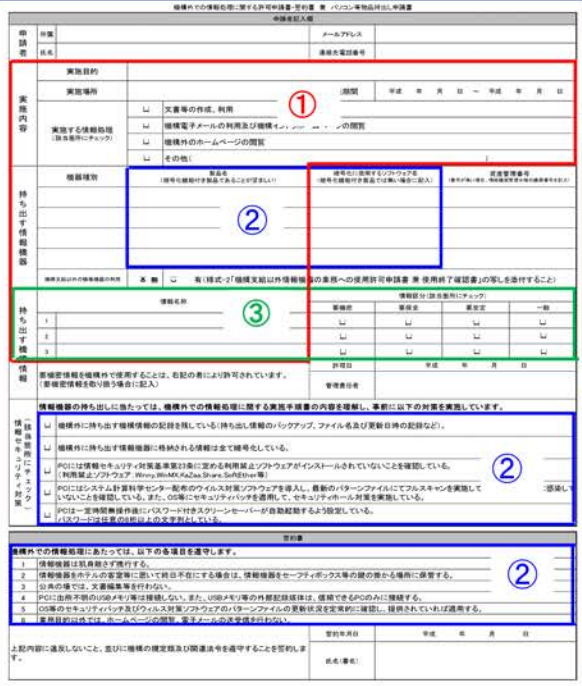
課室情報セキュリティ責任者は、機構外における情報処理を許可するにあたり、様式−1「許可書」における以下の項目について、**リスク分析(検討)を確実に実施**する必要があります。

①情報資産の持ち出しの必要性
②情報資産の持ち出しによる情報漏洩の危険性
③情報資産の持ち出しによる情報漏洩の影響度

次ページでは、検討結果(所見)を記載するにあたって、課室・グループ員から提出された様式−1「申請書」の記載内容に対する確認ポイントを説明します。

パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

4　盗難･亡失へのリスク分析について（記載内容に対する確認ポイント）



① 情報資産の持ち出しの必要性

申請者の実施目的や実施内容に鑑みて、「持ち出す情報機器」（記録媒体含む）や「持ち出す機構情報」が本当に必要なのかを確認してください。

② 情報資産の持ち出しによる情報漏洩の危険性

「持ち出す機構情報」が全て暗号化されていることを確認してください。

また、「持ち出す情報機器」には、情報システムセキュリティ対策基準などで定めている対策が実施されていること、及び課室･グループ員が誓約事項をきちんと理解していること、を確認してください。

③ 情報資産の持ち出しによる情報漏洩の影響度

「持ち出す機構情報」に持ち出し禁止の情報※が含まれていないことを確認してください。「一般」情報以外の場合は、万一その情報が漏えいした時を想定し、影響度を十分に検討してください。情報が漏えいした場合、機構内外の関係者へ被害が波及する恐れがあります。

また、文部科学省や総務省など関連省庁への報告が必要になります。

「持ち出す機構情報」が必要最小限にしてあるかを再度確認してください。

※ 秘密文書管理規定第12条

パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

5　盗難・亡失が発生した場合の連絡

課室情報セキュリティ責任者は、盗難･亡失の連絡が入ったら、課室･グループ員をしっかりとサポートし被害状況などの把握に努めてください。

右の確認項目にて被害状況などを把握し、被害品(情報も含む)を特定してください。

確認項目

1. 氏名
2. 日時
3. 場所
4. 被害品名
5. 被害状況
6. 初動対応

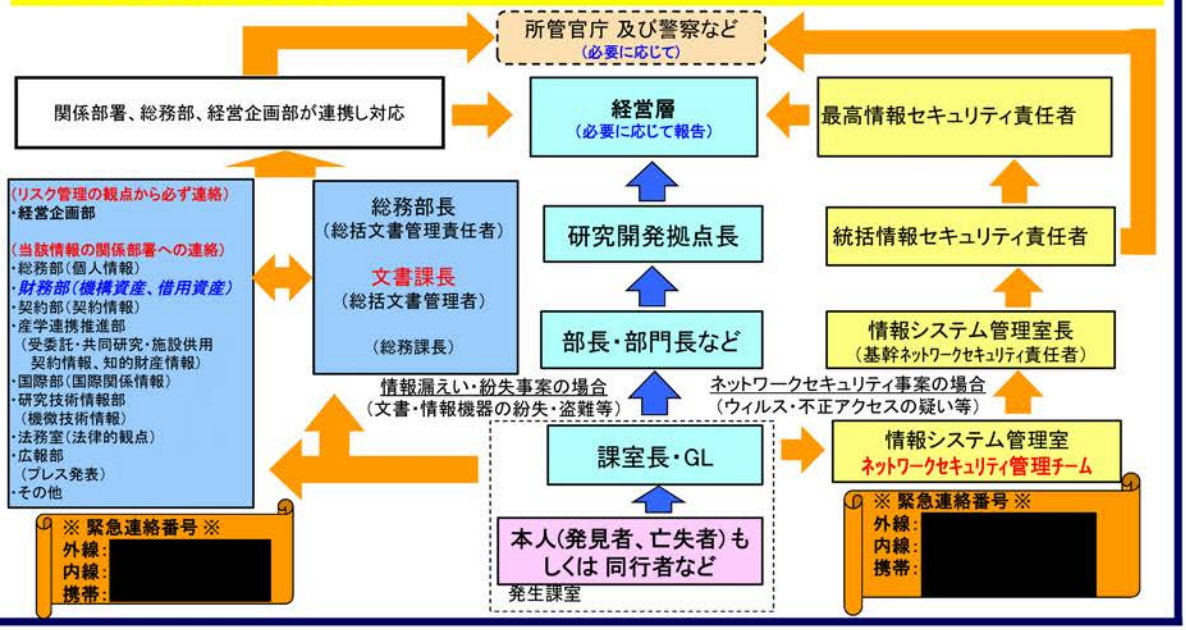
以下の手順に従い連絡してください。

- **手順1：情報漏えい、ネットワークセキュリティの観点からの連絡手順**
  「5　盗難･亡失が発生した場合の連絡（緊急連絡手順）」を参照してください。
- **手順2：物品管理規定における連絡手順**
  「5　盗難･亡失が発生した場合の連絡（機構資産の盗難･亡失した場合）」を参照してください。

パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

5　盗難・亡失が発生した場合の連絡（緊急連絡手順）

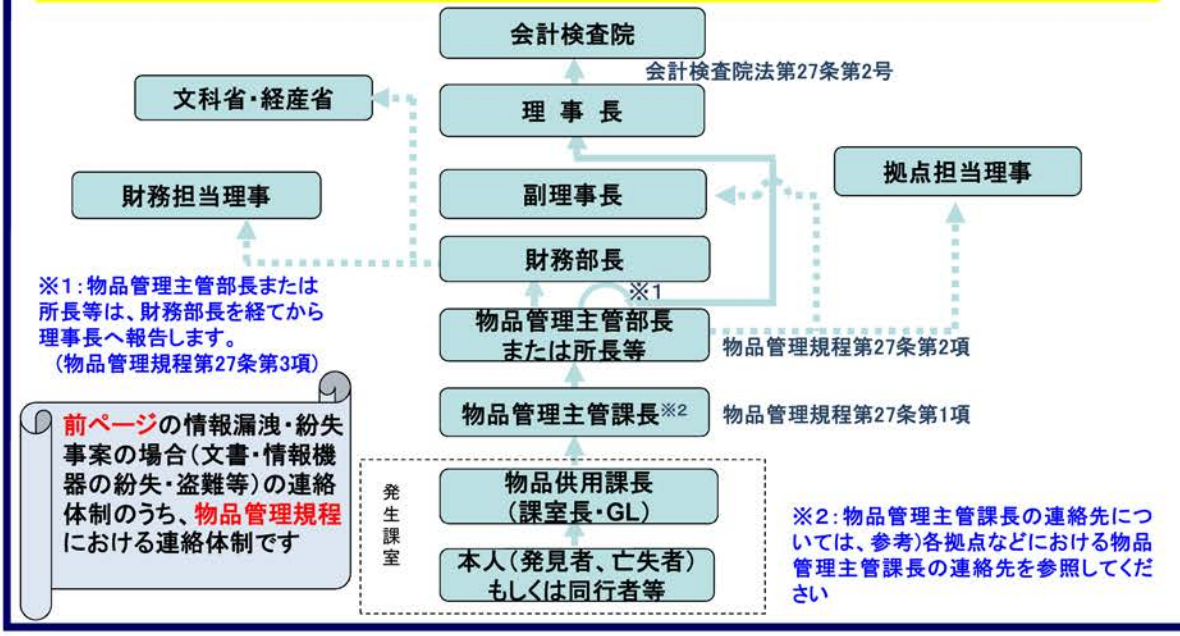
直属の上司（部長・部門長）だけなく、以下に示す緊急連絡手順に従って、関係各所へ直ちに連絡してください。



パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

5　盗難・亡失が発生した場合の連絡（機構資産の盗難・亡失した場合）

機構資産の盗難・亡失が判明したら、直ちに物品管理主管課（管財課など）に連絡をしてください。



パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

参考)　各拠点などにおける物品管理主管課長の連絡先

物品供用課長(課室長等)は、物品を管理している拠点の物品管理主管課長へ連絡します。

物品を管理している拠点	物品管理主管課長
本部	財務部　管財課長[redacted]
東海	管理部　管財課長[redacted]
大洗	管理部　経理課長[redacted]
敦賀	業務統括部　経理課長[redacted]
那珂	管理部　経理課長[redacted]
高崎	管理部　経理課長[redacted]
関西	管理部　経理課長[redacted]
幌延	経理課長[redacted]
東濃	経理課長[redacted]
人形峠	経理課長[redacted]
青森	管理部　経理課長[redacted]

パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について

おわりに

課室情報セキュリティ責任者の役割は、

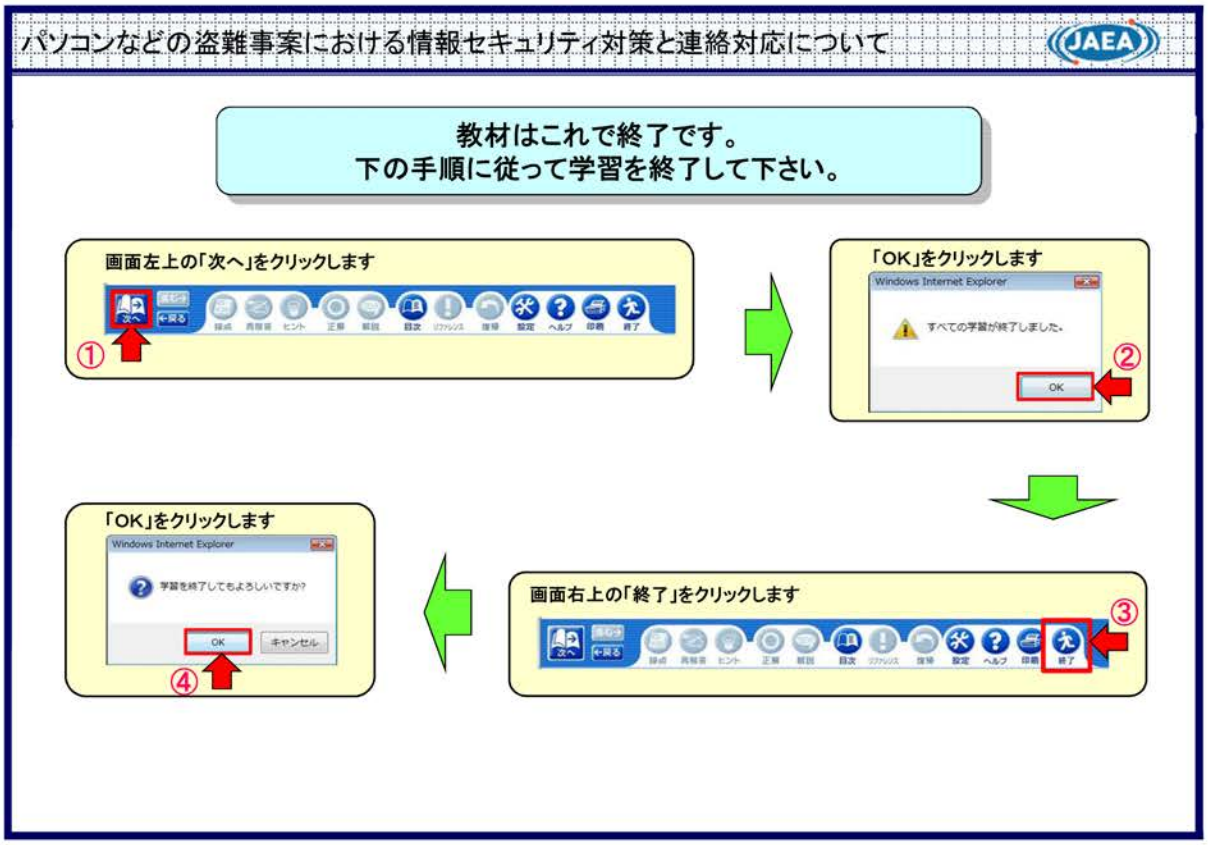
現場における**最初の堤防**であり**最後の砦**となります。

最初の堤防

課室・グループ員に機構の情報セキュリティポリシーを遵守させ、情報機器などの盗難・亡失、情報漏えいを起こさないよう、事前の対策を責任もって実施して(させて)ください。

最後の砦

万一、情報機器などの盗難・亡失、情報漏えいが発生してしまった場合には、連絡手順に従い速やかに関係部署に連絡するとともに、原因究明と再発防止策の検討を行い、その対策を関係部署と協力して最後まで責任もって実施してください。


パソコンなどの盗難事案における情報セキュリティ対策と連絡対応について
JAEA
教材はこれで終了です。
下の手順に従って学習を終了して下さい。
画面左上の「次へ」をクリックします
①
「OK」をクリックします
Windows Internet Explorer
すべての学習が終了しました。
OK
②
「OK」をクリックします
Windows Internet Explorer
学習を終了してもよろしいですか?
OK
キャンセル
④
画面右上の「終了」をクリックします
③

This is a blank page.

国際単位系（SI）

表１．SI 基本単位

基本量	SI 基本単位	
	名称	記号
長さ	メートル	m
質量	キログラム	kg
時間	秒	s
電流	アンペア	A
熱力学温度	ケルビン	K
物質量	モル	mol
光度	カンデラ	cd

表２．基本単位を用いて表されるSI組立単位の例

組立量	SI 基本単位	
	名称	記号
面積	平方メートル	m^2
体積	立法メートル	m^3
速さ，速度	メートル毎秒	m/s
加速度	メートル毎秒毎秒	m/s^2
波数	毎メートル	m^{-1}
密度，質量密度	キログラム毎立方メートル	kg/m^3
面積密度	キログラム毎平方メートル	kg/m^2
比体積	立方メートル毎キログラム	m^3/kg
電流密度	アンペア毎平方メートル	A/m^2
磁界の強さ	アンペア毎メートル	A/m
量濃度(a)，濃度	モル毎立方メートル	mol/m^3
質量濃度	キログラム毎立法メートル	kg/m^3
輝度	カンデラ毎平方メートル	cd/m^2
屈折率(b)	（数字の） 1	1
比透磁率(b)	（数字の） 1	1

(a) 量濃度（amount concentration）は臨床化学の分野では物質濃度（substance concentration）ともよばれる。
(b) これらは無次元量あるいは次元１をもつ量であるが、そのことを表す単位記号である数字の１は通常は表記しない。

表３．固有の名称と記号で表されるSI組立単位

組立量	SI 組立単位			
	名称	記号	他のSI単位による表し方	SI基本単位による表し方
平面角	ラジアン(b)	rad	1 (b)	m/m
立体角	ステラジアン(b)	sr(c)	1 (b)	m^2/m^2
周波数	ヘルツ(d)	Hz		s^{-1}
力	ニュートン	N		m kg s^{-2}
圧力，応力	パスカル	Pa	N/m^2	m^{-1} kg s^{-2}
エネルギー，仕事，熱量	ジュール	J	N m	m^2 kg s^{-2}
仕事率，工率，放射束	ワット	W	J/s	m^2 kg s^{-3}
電荷，電気量	クーロン	C		s A
電位差（電圧），起電力	ボルト	V	W/A	m^2 kg s^{-3} A^{-1}
静電容量	ファラド	F	C/V	m^{-2} kg^{-1} s^4 A^2
電気抵抗	オーム	Ω	V/A	m^2 kg s^{-3} A^{-2}
コンダクタンス	ジーメンス	S	A/V	m^{-2} kg^{-1} s^3 A^2
磁束	ウエーバ	Wb	Vs	m^2 kg s^{-2} A^{-1}
磁束密度	テスラ	T	Wb/m^2	kg s^{-2} A^{-1}
インダクタンス	ヘンリー	H	Wb/A	m^2 kg s^{-2} A^{-2}
セルシウス温度	セルシウス度(e)	℃		K
光束	ルーメン	lm	cd sr(c)	cd
照度	ルクス	lx	lm/m^2	m^{-2} cd
放射性核種の放射能(f)	ベクレル(d)	Bq		s^{-1}
吸収線量, 比エネルギー分与, カーマ	グレイ	Gy	J/kg	m^2 s^{-2}
線量当量, 周辺線量当量, 方向性線量当量, 個人線量当量	シーベルト(g)	Sv	J/kg	m^2 s^{-2}
酸素活性	カタール	kat		s^{-1} mol

(a)SI接頭語は固有の名称と記号を持つ組立単位と組み合わせても使用できる。しかし接頭語を付した単位はもはやコヒーレントではない。
(b)ラジアンとステラジアンは数字の１に対する単位の特別な名称で、量についての情報をつたえるために使われる。実際には、使用する時には記号radおよびsrが用いられるが、習慣として組立単位としての記号である数字の１は明示されない。
(c)測光学ではステラジアンという名称と記号srを単位の表し方の中に、そのまま維持している。
(d)ヘルツは周期現象についてのみ、ベクレルは放射性核種の統計的過程についてのみ使用される。
(e)セルシウス度はケルビンの特別な名称で、セルシウス温度を表すために使用される。セルシウス度とケルビンの単位の大きさは同一である。したがって、温度差や温度間隔を表す数値はどちらの単位で表しても同じである。
(f)放射性核種の放射能（activity referred to a radionuclide）は、しばしば誤った用語で"radioactivity"と記される。
(g)単位シーベルト（PV,2002,70,205）についてはCIPM勧告2（CI-2002）を参照。

表４．単位の中に固有の名称と記号を含むSI組立単位の例

組立量	SI 組立単位		
	名称	記号	SI 基本単位による表し方
粘度	パスカル秒	Pa s	m^{-1} kg s^{-1}
力のモーメント	ニュートンメートル	N m	m^2 kg s^{-2}
表面張力	ニュートン毎メートル	N/m	kg s^{-2}
角速度	ラジアン毎秒	rad/s	m m^{-1} s^{-1}=s^{-1}
角加速度	ラジアン毎秒毎秒	rad/s^2	m m^{-1} s^{-2}=s^{-2}
熱流密度，放射照度	ワット毎平方メートル	W/m^2	kg s^{-3}
熱容量，エントロピー	ジュール毎ケルビン	J/K	m^2 kg s^{-2} K^{-1}
比熱容量，比エントロピー	ジュール毎キログラム毎ケルビン	J/(kg K)	m^2 s^{-2} K^{-1}
比エネルギー	ジュール毎キログラム	J/kg	m^2 s^{-2}
熱伝導率	ワット毎メートル毎ケルビン	W/(m K)	m kg s^{-3} K^{-1}
体積エネルギー	ジュール毎立方メートル	J/m^3	m^{-1} kg s^{-2}
電界の強さ	ボルト毎メートル	V/m	m kg s^{-3} A^{-1}
電荷密度	クーロン毎立方メートル	C/m^3	m^{-3} sA
表面電荷	クーロン毎平方メートル	C/m^2	m^{-2} sA
電束密度，電気変位	クーロン毎平方メートル	C/m^2	m^{-2} sA
誘電率	ファラド毎メートル	F/m	m^{-3} kg^{-1} s^4 A^2
透磁率	ヘンリー毎メートル	H/m	m kg s^{-2} A^{-2}
モルエネルギー	ジュール毎モル	J/mol	m^2 kg s^{-2} mol^{-1}
モルエントロピー, モル熱容量	ジュール毎モル毎ケルビン	J/(mol K)	m^2 kg s^{-2} K^{-1} mol^{-1}
照射線量（X線及びγ線）	クーロン毎キログラム	C/kg	kg^{-1} sA
吸収線量率	グレイ毎秒	Gy/s	m^2 s^{-3}
放射強度	ワット毎ステラジアン	W/sr	m^4 m^{-2} kg s^{-3}=m^2 kg s^{-3}
放射輝度	ワット毎平方メートル毎ステラジアン	$W/(m^2$ sr)	m^2 m^{-2} kg s^{-3}=kg s^{-3}
酵素活性濃度	カタール毎立方メートル	kat/m^3	m^{-3} s^{-1} mol

表５．SI 接頭語

乗数	接頭語	記号	乗数	接頭語	記号
10^{24}	ヨタ	Y	10^{-1}	デシ	d
10^{21}	ゼタ	Z	10^{-2}	センチ	c
10^{18}	エクサ	E	10^{-3}	ミリ	m
10^{15}	ペタ	P	10^{-6}	マイクロ	μ
10^{12}	テラ	T	10^{-9}	ナノ	n
10^9	ギガ	G	10^{-12}	ピコ	p
10^6	メガ	M	10^{-15}	フェムト	f
10^3	キロ	k	10^{-18}	アト	a
10^2	ヘクト	h	10^{-21}	ゼプト	z
10^1	デカ	da	10^{-24}	ヨクト	y

表６．SIに属さないが、SIと併用される単位

名称	記号	SI 単位による値
分	min	1 min=60s
時	h	1h =60 min=3600 s
日	d	1 d=24 h=86 400 s
度	°	1°=(π/180) rad
分	’	1’=(1/60)°=(π/10800) rad
秒	”	1”=(1/60)’=(π/648000) rad
ヘクタール	ha	$1ha=1hm^2=10^4m^2$
リットル	L, l	$1L=11=1dm^3=10^3cm^3=10^{-3}m^3$
トン	t	$1t=10^3$ kg

表７．SIに属さないが、SIと併用される単位で、SI単位で表される数値が実験的に得られるもの

名称	記号	SI 単位で表される数値
電子ボルト	eV	$1eV=1.602\ 176\ 53(14)\times10^{-19}J$
ダルトン	Da	$1Da=1.660\ 538\ 86(28)\times10^{-27}kg$
統一原子質量単位	u	1u=1 Da
天文単位	ua	$1ua=1.495\ 978\ 706\ 91(6)\times10^{11}m$

表８．SIに属さないが、SIと併用されるその他の単位

名称	記号	SI 単位で表される数値
バール	bar	1 bar=0.1MPa=100kPa=10^5Pa
水銀柱ミリメートル	mmHg	1mmHg=133.322Pa
オングストローム	Å	1 Å=0.1nm=100pm=10^{-10}m
海里	M	1 M=1852m
バーン	b	$1\ b=100fm^2=(10^{-12}cm)2=10^{-28}m^2$
ノット	kn	1 kn=(1852/3600)m/s
ネーパ	Np	SI単位との数値的な関係は、対数量の定義に依存。
ベル	B	
デジベル	dB	

表９．固有の名称をもつCGS組立単位

名称	記号	SI 単位で表される数値
エルグ	erg	$1\ erg=10^{-7}$ J
ダイン	dyn	$1\ dyn=10^{-5}$N
ポアズ	P	1 P=1 dyn s cm^{-2}=0.1Pa s
ストークス	St	1 St =$1cm^2$ s^{-1}=$10^{-4}m^2$ s^{-1}
スチルブ	sb	1 sb =1cd cm^{-2}=10^4cd m^{-2}
フォト	ph	1 ph=1cd sr cm^{-2} 10^4lx
ガル	Gal	1 Gal =1cm s^{-2}=$10^{-2}ms^{-2}$
マクスウェル	Mx	1 Mx = 1G cm^2=10^{-8}Wb
ガウス	G	1 G =1Mx cm^{-2} =10^{-4}T
エルステッド(c)	Oe	1 Oe≙ $(10^3/4\pi)$A m^{-1}

(c) ３元系のCGS単位系とSIでは直接比較できないため、等号「 ≙ 」は対応関係を示すものである。

表10．SIに属さないその他の単位の例

名称	記号	SI 単位で表される数値
キュリー	Ci	$1\ Ci=3.7\times10^{10}Bq$
レントゲン	R	$1\ R = 2.58\times10^{-4}C/kg$
ラド	rad	$1\ rad=1cGy=10^{-2}Gy$
レム	rem	$1\ rem=1\ cSv=10^{-2}Sv$
ガンマ	γ	1γ=1 nT=10-9T
フェルミ		1フェルミ=1 fm=10-15m
メートル系カラット		1メートル系カラット = 200 mg = 2×10-4kg
トル	Torr	1 Torr = (101 325/760) Pa
標準大気圧	atm	1 atm = 101 325 Pa
カロリー	cal	1cal=4.1858J（「15℃」カロリー），4.1868J（「IT」カロリー）4.184J（「熱化学」カロリー）
ミクロン	μ	1 μ =1μm=10^{-6}m

（第8版，2006年改訂）

この印刷物は再生紙を使用しています