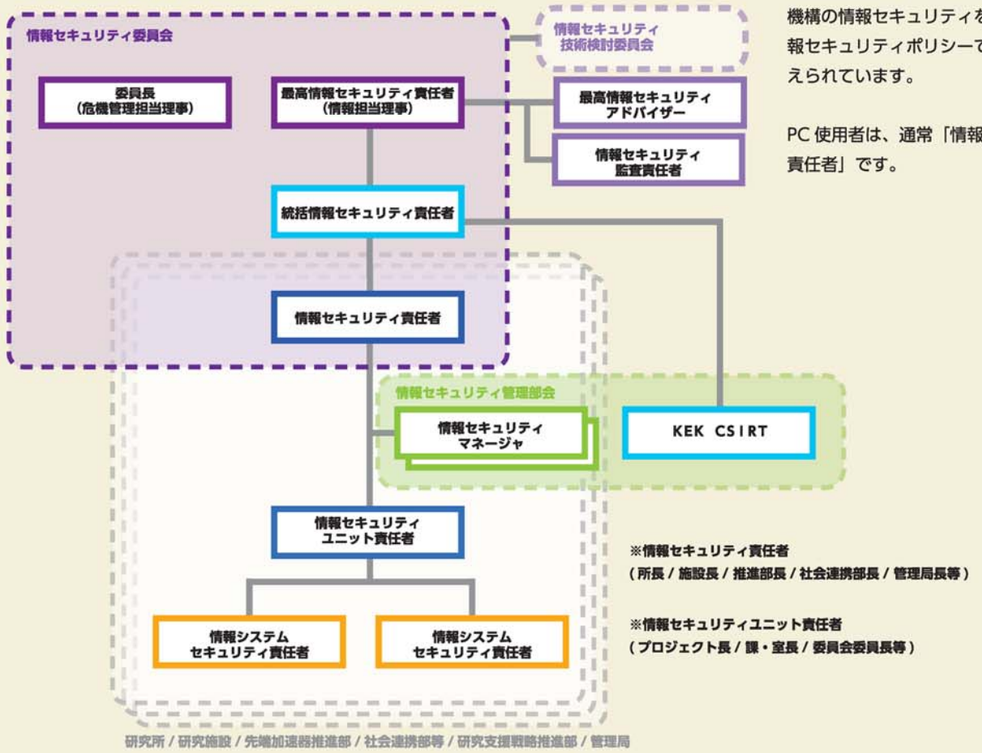
✓ KEK の情報セキュリティの規則等について

機構の情報セキュリティの規則構成は、承認レベルや記述内容の具体性の違いから 4 階層に分かれています。
上位の情報セキュリティ規則で定められた内容が、下位の規則で段階を追って具体化されていきます。

情報セキュリティ規程や情報セキュリティポリシーでは、「なぜ情報セキュリティが必要か」から始まり、何をどこまで守るのか、誰が責任者であるかを明確にしています。情報セキュリティ対策基準では、上位の規程やポリシーで定められた基本方針を受け、「何をしなければならないか」について定められており、様々な情報セキュリティ対策において、適用範囲や対象者、守るための方針が明確にされています。実施手順書では、対策基準の内容を実施する際に「どのように実施するか」が定められ、詳細な手順が記載されています。

✓ KEK の情報セキュリティの管理体制について



機構の情報セキュリティを維持するために、情報セキュリティポリシーで、その管理体制が整えられています。

PC 使用者は、通常「情報システムセキュリティ責任者」です。

※情報セキュリティ責任者
（所長 / 施設長 / 推進部長 / 社会連携部長 / 管理局長等）

※情報セキュリティユニット責任者
（プロジェクト長 / 課・室長 / 委員会委員長等）

✓ KEK の規則等や管理体制について

機構の情報セキュリティに関する規則等や管理体制については、 https://stw.kek.jp/stpg/iso/ をご確認ください。（機構内専用ページです。）

被害にあわないための情報セキュリティ 11 の対策

2017 年 3 月 16 日　第 1 版
本リーフレットについての問い合わせ先
kekinfosec@ml.post.kek.jp

情報セキュリティ 11 の対策

被害にあわないために

✓ 異変に気が付いた時の対応

こんなときは、すぐご相談ください。

- 不審なメールの添付ファイルを開いた。
- Web ページが改竄されていたことを発見した。
- クリックしていないのにクリック音が PC から聞こえる。
- ネットワーク接続が突然遅くなった。動作が突然重くなった。

ネットワークから切り離して

すぐに相談

情報セキュリティ緊急対応窓口
Computer Security Incident Response Team

029-879-6285
csirt@kek.jp

ノーサート
KEK CSIRT が対応します。

情報セキュリティ 11の対策

被害にあわないために

01　アップデート

アップデートを頻繁に行ってください。
・パソコンの OS
・OS の上で動作するソフトウェアやアプリ
・その他、ネットワークに接続するような機器
（プリンター、カメラ、スマートフォン、ルーター等）

自動アップデートを設定している場合は、アップデートの履歴情報から、正しくアップデートされているかを定期的に確認してください。また、再起動が必要な場合には、忘れずに再起動してください。

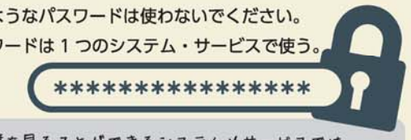
02　ウイルス対策

ウイルス対策ソフトを必ず使用してください。
・有効な状態にしてください。
有効な状態にするためにインストール後にライセンス認証 などの作業が必要な場合があります。
・最新の定義ファイルを使ってください。
・定期的にパソコン全体のスキャンをしてください。
・有償のソフトウェアをご利用ください。

機構の計算科学センターが貸与するウイルス対策ソフト『ESET Endpoint Antivirus』は定期的な自動スキャンを自分で設定する必要があります。詳しくは、http://distavm.kek.jp/ をご確認ください。

03　パスワード

良いパスワードを使ってください。
・十分な長さの文字列
・英大文字小文字と数字、記号を組み合わせる
・類推されるようなパスワードは使わないでください。
・１つのパスワードは１つのシステム・サービスで使う。



ログイン履歴を見ることができるシステムやサービスでは、自分以外の誰かがログインしていないかをこまめに確認することで、被害の早期発見が可能になります。

04　Web サイトの閲覧

近年、Web サイトの閲覧での被害が多発しています。
・業務に関係がない Web サイトは開かない。
・パスワードなどを入力するページでは、
「https」から始まるかどうかを確認する。
・ダウンロードは公式サイトから行ってください。
・無料は危険と疑う。
・画面に表示されたポップアップは、偽警告や、偽表示と疑う。

インターネットからダウンロードしたプログラムをインストールしたり、広告をクリックすることで、意図しないソフトウェアがインストールされることがあります。インストールしたプログラムの一覧を定期的に確認し、自分がインストールした覚えがないプログラムは削除してください。

05　アドオン・プラグイン

ブラウザなどの一部のソフトウェアには、アドオンやプラグインと呼ばれるソフトウェアがあります。よく使われる Adobe Reader や Adobe Flash Player や、Java の脆弱性は攻撃にたびたび悪用されています。
意図せずに導入されている場合もあるので、定期的にブラウザの設定を確認ください。

Adobe Reader や Flash や、Java などのブラウザのプラグインを利用する必要がある場合には、最新の状態で利用してください。また、動作時に確認を求めるような設定にすることで意図しない動作を防げます。

06　メールの取扱

「添付ファイルを開く」、「本文に書かれた URL をクリック」からはじまる被害が多発しています。

・メールを受け取ったら、
「差出人」、「宛先」、「本文」をよく確認してください。
・少しでも不審だと感じたら、安易に添付ファイルを開いたり、
メール内の URL にアクセスしないでください。

HTML（リッチテキスト）形式のメールは、プレビューで感染するため、テキスト形式での受信を推奨します。

07　バックアップ

バックアップは被害にあったときの早期復旧や被害の軽減に有効です。定期的にデータやシステムをバックアップし、きちんと管理する事が必須です。

重要な情報は、自分だけしかアクセスできないところにバックアップしてください。クラウドへのバックアップは規約をよく読んで自分のデータがどのように扱われるかをご確認ください。

08　USB 機器

USB の機器をパソコンに挿した途端、ウイルスに感染することがあります。Windows では、USB を接続したときの自動実行を切ってください。USB メモリだけでなく、スマホ、デジタルカメラ等など USB で接続できるものにマルウェアが潜んでいることがあります。

データの移動や持ち運び、データの提供などで USB メモリを使う場合は、使用する USB メモリを限定し、使用前後にウイルスチェックをしてください。使用後にフォーマットをするのもよい方法です。

09　使わないときの対策

自分のパソコンが簡単に他人に操作されないように責任ある管理をお願いします。
- パソコンの前から離れるときは、スクリーンロックを必ずかけてください。
- 長時間使用しないときは、電源を切ってください。
- 使わないパソコンは、ネットワークの廃止申請を行ってください。

しばらく使っていなかったパソコンを使用する場合には、OS・ソフトウェアをアップデートし、ウイルス対策ソフトを最新の状態にしてパソコン全体のスキャンを行った後にご使用ください。

10　使い分け

非常に重要な情報を扱うパソコンと、通常の研究業務を行うパソコンとを使い分けてください。
使い分けが難しい場合には、重要な情報は外付メディアに保存し、必要な時だけ接続して利用することで重要データが被害にあう確率を減らします。

個人情報などの重要情報を扱うパソコンを web サイトの閲覧やメールの送受信に利用するパソコンと分離して使用する『インターネット分離』が一般的に広がっています。

11　情報収集

危険は突然やってきます。メール攻撃や偽警告など人間の心の隙をついて騙す攻撃もどんどん進化しています。

情報セキュリティ対策で最も大切なことは、「知識をもつこと」と「自分で考えること」です。

情報収集については、
下の情報源を参考にしてください。

✓ NISC のハンドブック

内閣官房内閣サイバーセキュリティセンター (NISC) から、「ネットワークビギナーのための情報セキュリティハンドブック」が公開されています。このハンドブックは、家庭で使用するパソコンやスマートフォンなど、身近なものを題材に、セキュリティの基本や、安全に使用するための方法などを解説されたものです。

NISC 情報セキュリティハンドブック
http://www.nisc.go.jp/security-site/handbook/

✓ 安全に Web サイトを閲覧する

aguse Gateway
https://gw.aguse.jp/

aguse Gateway は URL を入力すると、aguse のサーバが対象のウェブサイトから受け取った情報をもとに、サイトを画像に変換して表示してくれます。表示されたページにあるリンク先も同様に画像で表示されるので、怪しいサイトでもある程度安全にアクセスすることができます。

※URL に個人を識別するような情報が入っている場合には使用をお控えください。

✓ 情報セキュリティに関するリンク集

公的機関である NISC や IPA、JPCERT/CC から情報セキュリティに関する最新情報が発信されています。また、セキュリティに関する情報を扱う民間の web サイトも数多くあります。多くの場合、ひとりひとりが状況を認識し、正しい情報に基づいて判断することで危険を回避することができます。情報セキュリティに関する信頼性の高い情報源を用意しましたので、情報収集に活用いただければ幸いです。

JPCERT/CC
- https://www.jpcert.or.jp/

IPA 情報処理推進機構　～情報セキュリティ～
- https://www.ipa.go.jp/security/index.html

内閣サイバーセキュリティセンター（NISC）
- http://www.nisc.go.jp/

Security NEXT
- http://www.security-next.com/

ITpro ～セキュリティ～
- http://itpro.nikkeibp.co.jp/security/

マイナビニュース ～セキュリティ～
- http://news.mynavi.jp/enterprise/security/

フィッシング対策協議会
～フィッシングに関するニュース～
- https://www.antiphishing.jp/news/alert/

SecurityFocus
- http://www.securityfocus.com/