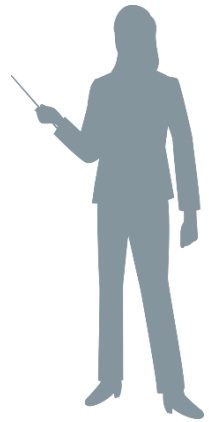
情報セキュリティ教育

2018年度版

目次



1.はじめに

　標的型メール攻撃等の新しい脅威の出現によりKEKを取り巻く情報セキュリティ上の環境は大きく変化しています。しかし、このように環境が変化する状況下にあっても、基本的な情報セキュリティ対策の重要性は失われることはありません。

　今年度は、KEK全体の情報セキュリティ水準の底上げを図ることを目的に、基本的な情報セキュリティ対策である、「コンピューターウィルスの被害を防止するための対策」と「不正ログインを防止するための対策」について改めて学んでいただきます。

2.コンピューターウィルスの被害を防止するための対策について

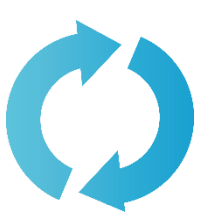
なぜ対策するのか？

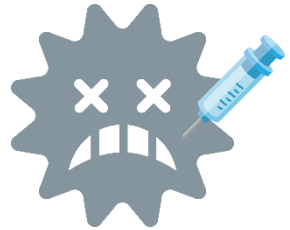
ウィルスに感染すると利用者が意図しない動作*1が引き起こされ、
直接的だけでなく間接的*2にも、
あなた及び機構の業務に大きな影響を及ぼす危険性があります。

実施する基本的対策：

・OSやソフトウェアはできるだけ最新の状態にしてください
・ウィルス対策ソフトウェアを導入してください

*1　ID・パスワードの漏洩を含む情報漏えいや破壊、他者への攻撃など
*2　調査や再発防止のために時間を要することなど

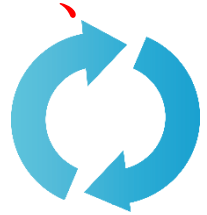




2-1.【基本対策】OSやソフトウェアはできるだけ最新にする

具体策：OSやソフトウェアにセキュリティ修正プログラムを適用してください。
　　修正プログラムの適用方法は各メーカのWebページ等で確認してください。
効　果：OSやソフトウェアのセキュリティ上の問題点を解消し、
　　それを悪用したウィルスに感染する危険性が低減します。

注　意：サポートが終了した古いOSをネットワークに接続することは危険です。
　　特にWindows OSにおいてはWindows XP、Vista、8（8.1は除く）、
　　Windows Server 2003 R2 及びそれ以前のOSはKEK LANに接続できません。
注　意：Internet ExplorerなどのWebブラウザ、Acrobat 等のPDF ビューアー、
　　JAVA、Flash、Microsoft Office には特にご留意ください。



2-2.【基本対策】ウィルス対策ソフトウェアを導入する (1)

具体策：ウィルス対策ソフトウェア（アンチウィルスソフトウェア）を
常時動作させてウィルスを検疫・駆除してください。

効　果：ウィルスに感染する危険性が低減します。

注　意：Windows/ Mac OS(macOSを含む　以下同様）にはウイルス対策ソフトウェアを導入してください。

2-2.【基本対策】ウィルス対策ソフトウェアを導入する (2)

具体策：ウィルス定義ファイルは自動更新するように設定してください。

効　果：日々、作成される新しいウィルスの検知力が向上します。

注　意：ライセンスが期限切れでないことを確認してください。
　　ライセンスが切れているとウィルス定義ファイルが更新されません。

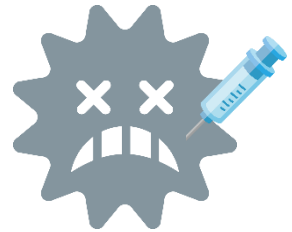
2-2.【基本対策】ウィルス対策ソフトウェアを導入する (3)

具体策：定期的(週１回程度以上)にフルスキャンを実行するよう設定し、
フルスキャンを実行するよう努めてください。

効　果：過去に検知不能でメールやWebから意図せずに取り込んでしまったウィルスを駆除できる場合があります。

要　請：業務に若干の支障をきたす場合であっても、可能な限り定期的にフルスキャンを実行してください。

注　意：多くのウィルス対策ソフトウェアでは、定期的にフルスキャンが行われる設定になっていません。ウィルス対策ソフトウェアの設定を確認してください。



3.不正ログインを防止するための対策

なぜ対策するのか？

・安易なパスワードを設定するとパスワードを推測（解析）され、
　不正ログインされる危険性が増大するためです。
・パスワードを使い回すと一か所でパスワードが漏洩した場合に、
　他のシステムに不正ログインされる危険性があるためです。

実施する基本的対策：

・安全なパスワードを設定してください。
・パスワードはできるだけ複数のシステムで使い回さないでください。

3-1.【基本対策】安全なパスワードを設定する

具体策：パスワードは、長く複雑なものを設定してください。

効　果：第三者にパスワードを推測や解析をされる危険性が低減します。

安全なパスワード（例）：下記の条件をすべて満たすもの
・十分長い文字数（注1）
・数字や記号（@ % $ など）を含めている
・アルファベットの大文字と小文字の両方を含めている

危険なパスワード（例）：下記の条件のいずれかを満たすもの
・キーボード上の配列をなぞったもの「qwertyui」、「zxcvbnm,」等）
・IDと同一の文字列
・利用者の氏名、電話番号、誕生日をそのまま使用
・単純な文字数字の羅列（「123456…」や「abcd…」など）
・辞書にある単語をそのまま使用

注1：文字数や文字種とパスワード解読に必要な速度に関しての例　http://www.dit.co.jp/report/security_report/forensic_center/20141001.html

3-2.【基本対策】パスワードは複数のシステムで使い回さない（1）

具体策：別のシステムでは別のパスワードを使用して、1つのパスワードを使いまわさないようにしてください。

効　果：パスワードが漏洩した場合に、
一度に複数のサービスに不正アクセスされる危険性が低減します。

3-2.【基本対策】パスワードは複数のシステムで使い回さない (2)

要　請：機構内のシステムと機構外のシステムで、同じパスワードを使用しないでください。

インターネットから利用できる機構内のサービスのパスワードは特に注意してください。

（例：post/mail.kek.jp Webメールや VPNサービス）

要　請：**過去のログイン記録を閲覧できる場合は、ログイン元に不審なものがないか確認するようにしてください。**

post/mail.kek.jp Webメールでは、「メールホーム」ページでログイン元IPアドレス/日時を確認できます。

4. ネットワークの監視について

- 機構は、外部機関 *1 が提供しているセキュリティ監視サービスを利用し、KEK LANと外部インターネット間の通信に不審な通信 *2 がないかモニターしています。

- 最近、業務に無関係と考えられるアプリケーションが行う通信が、不審な通信としてこのモニターにキャッチされ、機器管理者に調査を依頼することが増えています。特にスマートフォン*3をKEK LANに接続して利用する場合は、これにご留意ください。

*1 民間のセキュリティ事業者及び国立情報学研究所
*2 通信相手先が不正アクセスに関与した疑いがあるIPアドレスやホスト名であるなどの特徴がある通信
*3 スマートフォンには業務に無関係な多くのアプリケーションがインストールされている場合があるため

5. 異常を感じたときの対応 (1)

情報セキュリティ緊急対応窓口：

KEK CSIRT
029-879-6285
csirt@kek.jp

できれば異常が発見された機器をネットワークから切り離して
すみやかに KEK CSIRT に連絡してください。

異常(例)
・身に覚えのないログイン履歴がある
・不審メールの添付ファイルを開いた
・クリックすることなくPCからクリック音が聴こえる
・改ざんされているWebページを発見した

参考資料

安全なパスワードの作り方などを知りたい方向け

情報処理推進機構：チョコっとプラスパスワード

https://www.ipa.go.jp/chocotto/pw.html

パスワード使い回しの危険性などを知りたい方向け

JPCERT コーディネーションセンター：STOP! パスワード使い回し!キャンペーン2018

https://www.jpcert.or.jp/pr/2018/stop-password2018.html