Tya-net Newsletter
富山大学
総合情報基盤センター
No.53

連休明けのセキュリティ対策について

世界各国で長期休暇を狙ったサイバー攻撃が多発しています。特に休暇明け直後の機器は，セキュリティレベルが低い状態であるため，各々が適切に対策を実施しなければ甚大な被害が発生します。

以下にセキュリティ対策方法等を簡潔にまとめましたので，必ずご確認願います。

ウイルス対策ソフト

ウイルス対策ソフトを導入し，常に最新の状態にする。

OS・ソフトウェア

OSやソフトウェアは最新の修正プログラムを適用する。

不審なサイト・メール

ウェブサイトへのアクセスは慎重に。不審なメールは開かない。

アクセスログの確認

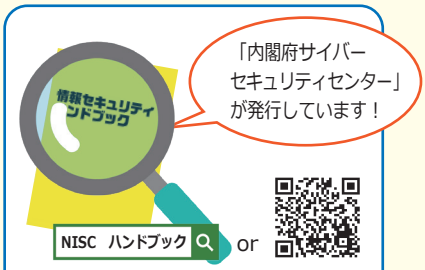
ネットワークに接続する機器は，定期的に通信記録を確認する。

ID・パスワードの管理

パスワードは他人に教えない，共有しない，適切な文字列を設定する。

安全なソフトウェア利用

ソフトウェアは正規の方法で入手し，正規ライセンスを適正に利用する。



セキュリティハンドブックを確認

情報セキュリティの「いろは」が記載してあります。
https://www.nisc.go.jp/security-site/handbook/index.html

不審なことや情報セキュリティ事案が発生した場合は・・・

- **総合情報基盤センターへ連絡（TEL:076-445-6946）**

【 総合情報基盤センター情報セキュリティに関する連絡窓口 】
security@itc.u-toyama.ac.jp
http://www.itc.u-toyama.ac.jp/inquiry/index.html

- **情報政策課へ連絡（TEL:076-445-6058）**

※　記載事項は一般的な必要最低限の対策事項です。管理状況に合わせて適切に対応してください。

富山大学 総合情報基盤センター
2019年8月20日
http://www.itc.u-toyama.ac.jp/
内線：6946（五福）
▶ バックナンバー ： http://www.itc.u-toyama.ac.jp/cn/