

青 警 本 情 第 7 8 号

平 成 2 2 年 3 月 3 0 日

各 所 属 長 殿

青 森 県 警 察 本 部 長

青森県警察インターネットシステム運用要領の制定について

この度、「青森県警察インターネットシステム運用要領」を別添のとおり制定し、平成22年4月1日から実施することとしたので、所属職員に周知徹底し、その運用に誤りのないようにされたい。

なお、「青森県警察インターネットシステム運用要領の制定について」（平成14年12月26日付け青警本情第202号）は廃止する。

記

1 制定の趣旨

平成22年度の組織改編により、青森県警察本部組織条例（平成6年10月青森県条例第41号）及び青森県警察組織規則（昭和36年11月青森県公安委員会規則第15号）の一部が改正されたことに伴い、システム総括責任者を総務室長とし、整合性を図ったものである。

2 制定に伴う改正要点

(1) システム総括責任者（3の(1)関係）

システム総括責任者を「警務部長」から「総務室長」に改めた。

別添

青森県警察インターネットシステム運用要領

1 趣旨

この要領は、総務室情報管理課に設置されたサーバと各所属にインターネット接続のために設置されたパソコン（以下「ＩＴ端末」という。）を通信回線等を介して接続することに関し、その安全性及び有効性を確保するため、必要な事項を定めるものとする。

2 適用範囲

この要領は、警察本部内各所属にあつては知事部局の全庁ＬＡＮを経由してインターネットに接続するＩＴ端末、各警察署にあつては総務室情報管理課を経由してインターネットに接続するＩＴ端末に適用する。

3 運用管理体制

(1) システム総括責任者

インターネットシステムの適正かつ効果的な運用を図るため、システム総括責任者を置き、総務室長をもって充てる。

(2) システム管理者

インターネットシステムを適正に運用管理し、安全性及び有効性を確保するため、システム管理者を置き、情報管理課長をもって充てる。

(3) 運用管理者

ア 所属に運用管理者を置き、所属長をもって充てる。

イ 運用管理者は、所属におけるインターネットシステムの適正な運用及び管理に努めるものとする。

(4) 運用管理補助者

ア 所属に運用管理補助者を置き、次長等をもって充てる。

イ 運用管理補助者は、運用管理者の事務を補佐するものとする。

(5) 取扱責任者

ア 所属に取扱責任者を置き、警察本部にあつては運用管理者が指定する課長補佐等、警察署にあつてはＩＴ端末を設置する課の課長をもって充てる。

イ 取扱責任者は、ＩＴ端末の利用状況を把握するなど、運用管理者及び運用管理補助者の事務を補佐するものとする。

(6) I T指導員

「I T指導員制度の運用要領の改正について」（平成18年3月24日付け青警本情第47号）に基づくI T指導員は、所属職員の指導、セキュリティ措置及びその他運用管理者が命じる事項を行うものとする。

4 コンピュータウイルス対策

- (1) システム管理者は、インターネットシステムについて、コンピュータウイルス等不正なプログラム（以下「ウイルス」という。）の侵入防止及び発見のための必要な措置を講じなければならない。
- (2) 運用管理者は、ウイルスを発見したときは、その利用を中止するとともに、直ちにシステム管理者に報告するものとする。
- (3) 前記(2)の報告を受けたシステム管理者は、ウイルスの駆除及び復旧方法について運用管理者に指示するものとする。

5 不正アクセス防止等

- (1) 職員は、インターネット接続に必要な情報を、第三者に漏らしてはならない。
- (2) 運用管理者は、インターネットシステムを定められた接続方法以外の方法で他の通信回線と接続してはならない。

6 インターネット利用に関し職員が守るべき事項

職員は、インターネット利用に関し、別紙「I T端末でのインターネット利用に関し職員が守るべき事項」を守らなければならない。

7 利用記録

職員は、インターネットシステムを利用する場合は、インターネット利用記録簿（別途指示）に所要事項を記録しなければならない。

8 障害等発生時の措置

職員は、インターネットシステム利用中に障害等が発生した場合には、システム管理者及び運用管理者に報告するとともに、その状況を把握し、システム管理者の指示により、障害等の復旧措置を講じなければならない。

9 システム管理者のW e b サイト閲覧状況の記録

システム管理者は、職員のW e b サイトへのアクセス状況について、警察本部情報管理課設置のサーバに記録しておかなければならない。

10 電子メールの存在場所についての職員の自覚

職員は、当該電子メールは、原則として、I S P等本県警察が管理しない部外のメールサーバに受信するまで存在することを自覚しておかなければならない。

11 その他

運用管理者は、I T端末の設置場所の変更、業務上必要なソフトウェアの追加及びその他インターネットシステムの利用に関する事項について疑義が生じた場合は、システム管理者と事前に協議して措置するものとする。

別 紙

「ＩＴ端末によるインターネット利用に関し職員が守るべき事項」

職員は、ＩＴ端末でインターネットを利用する場合、次の事項を理解し、遵守しなければならない。

1 ＩＴ端末を取り扱う上で基本的に守るべき事項

(1) 規定以外のソフトウェア、ハードウェアの導入制限

ＩＴ端末には、システム総括責任者が承認した場合を除き、規定以外のソフトウェア、ハードウェアを導入してはならない。

(2) ＩＴ端末のパスワード管理の徹底

運用管理者は、ＩＴ端末の起動パスワードをＩＴ指導員等をして適正に管理しなければならない。

(3) ＩＴ端末での業務文書の作成、保存の禁止

ＩＴ端末では、業務文書を作成し又は保存してはならない。

(4) 基本ソフトウェア等のセキュリティの確保

運用管理者は、ＩＴ端末の規定の基本ソフトウェア(ＯＳ)、Ｗｅｂブラウザソフトウェア、電子メール送信・受信ソフトウェア等について、ＩＴ指導員等をして、当該ソフトウェアのバージョンアップ及びセキュリティパッチの適用を確実にを行い、常に安全性を確保しておかなければならない。

(5) ＩＴ端末の持出し、移動の禁止

ＩＴ端末は、システム総括責任者の承認を得た場合を除き、部外に持ち出すなど所定の場所から移動してはならない。

(6) ＩＴ端末以外の接続の禁止

ＩＴ端末が接続されている通信回線及び通信機器に、当該ＩＴ端末以外のパソコンや通信機器を接続してはならない。

2 インターネット利用に際しての基本

(1) インターネットの業務目的以外の利用禁止

ア 電子メール、Ｗｅｂサイトについては、業務目的以外に利用してはならない。

イ インターネット上のオンライン・ストレージは、これを利用してはならない。

(2) インターネットを利用した業務情報の送信・受信

ア 職員及び警察機関相互で業務情報の送信・受信を行ってはならない。

イ 業務上やむを得ず業務情報を送信もしくは受信する場合は、システム管理者の

指示のもと暗号化の処置を施すこと。

(3) インターネットの利用

ア インターネットの利用は、電子メール及びW e b 閲覧以外で使用しないこと。

イ I T 端末では、規定の電子メールサービス以外の電子メールサービスを利用しないこと(フリーメール、W e b メール)。ただし、これによりがたい場合は、事前にシステム管理者の承認を得ること。

ウ 送信及び受信した電子メールのバックアップを作成すること(当該主管課保管)。

エ インターネット利用者は、接続中の I T 端末を当該接続以外の電話回線、携帯電話、P H S、無線L A N、専用線等を利用して規定外のネットワークに接続しないこと。

オ 出所不明のファイルや、内容に確証のもてないファイルをダウンロードや実行してはならない。

3 ウイルス対策のために守るべき事項

(1) ウイルス感染防止対策の基本

ア アンチウイルスソフトの利用義務

I T 指導員は、I T 端末起動中は、アンチウイルスソフトを常駐設定にし、ファイルへのアクセス及び電子メールの受信時には、常時スキャンできるように設定しなければならない。

イ I T 指導員は、常時スキャン設定の外、概ね1週間に一度は、ファイル全体に対するスキャンを実施しなければならない。

ウ I T 指導員又はI T 端末利用者は、毎日一回定義ファイルを更新するように設定すること。

エ I T 端末で、外部媒体を使用する時は、最新のウィルス定義ファイルが適用されているパソコン(I T 端末を含む。)で、当該媒体をスキャンし、ウイルスに感染していないことを確認しなければならない。

(2) 電子メールからのウイルス感染被害の防止

ア メール受信にあたっては、電子メール保護機能(オートプロテクト)を有効にしなければならない。

イ 送信元が不明のメールに添付されたファイルや実行形式のまま添付されたファイルなど不審な添付ファイルに対しては、「開く」「保存する」等の操作を加えてはならない。

ウ ファイルを添付してメールを送信する場合は、当該ファイルがウイルスに感染

していないことを必ず確認しなければならない。

エ 電子メールサービス利用中に、ウイルスを発見したり、ウイルス感染を疑わせる症状を発見した場合は、(利用者又はI T指導員は) システム管理者に報告し、その指示に従うこと。

(3) ウイルスに感染した場合の措置

ア I T端末がウイルスに感染した場合は、直ちにL A NケーブルをI T端末から抜き、駆除等の措置操作を行わず、ウイルスチェックソフトのメッセージが表示されている状態で、I T指導員を介し(I T指導員不在の場合はこの限りではない。以下同じ。)、システム管理者に報告し、対応方法の教示を受けること。

イ I T端末利用者は、以下のウイルス感染を疑わせる症状等が発生した場合には、I T指導員を介し、システム管理者に報告し、対応方法の教示を受けること。

(例示)

P Cの動作が重くなった

画面の動作がおかしい

ドライブへ勝手な書き込みや意図しないアクセスをする

ウイルス付のメールが送られたとの連絡があった

突然、音が鳴る、勝手に音楽を演奏する

突然、異常なエラーやメッセージがでる

プログラムのサイズが勝手に変化する

ファイルが破壊・削除される

ファイルの属性が勝手に変更されている

ファイルを開こうとしたら、マクロの警告メッセージが出た(メッセージの意味していることを理解しているなら報告の必要なし)

4 電子メールサービス利用時に守るべき事項

(1) 電子メールの送信・受信は規定のメールソフトウェアで行うこと。

(2) 業務上必要な場合以外、メールアカウント(アドレス)を外部へ公開しないこと。

(3) 電子メールを送信する場合は、送信先のメールアドレスに間違いがないか、確認の上送信すること。

(4) 個人のプライベートアドレスへの電子メールの自動転送は、禁止する。

(5) チェーンメール等を受信した場合は、これを転送せず、システム管理者に報告すること。

(6) メーリングリストへの登録は、原則としてしてはならない。

- (7) 電子メールの送信に当たっては、送信メールのサイズ(容量)を考慮し、一定のサイズを超える場合は、分割送信を考慮すること。
- (8) 無用な電子メールの送信・受信をしないこと。
- (9) 電子メールの送信は、HTMLメールで行わないこと。

5 Webサービス利用時に守るべき事項

- (1) インターネット利用者は、信頼できないWebサーバにアクセスしてはならない。
- (2) インターネット利用者は、インターネット掲示板などへの書き込みはしてはならない。
- (3) 次に該当する情報の発信をしてはならない。また、情報の閲覧についても、業務上必要な場合以外はしてはならない。

ア 著作権、商標、肖像権を侵害するおそれのあるもの

イ 他人のプライバシーを侵害するおそれのあるもの

ウ 他人の社会的評価にかかわる問題に関するもの

エ 他人の名誉・信用を傷つけるおそれのあるもの

オ 警察組織の信頼・品位を傷つけるおそれのあるもの

カ 性的な画像や文章に該当するおそれのあるもの

キ 不正アクセス等を助長するおそれのあるもの

ク 差別的なもの

ケ 虚偽のもの

コ 警察組織の内部情報

サ その他公序良俗に反するおそれのあるもの

- (4) インターネット利用者は、いかなるWebサーバに対しても、攻撃等不正なアクセスを行ってはならず、また、攻撃、不正なアクセスを目的として部内のシステムを利用してはならない。
- (5) インターネット利用者は、部内外のWebサーバに対して、他人のIDやパスワードなどを利用してアクセスしてはならない。
- (6) アクセス制限されたWebサイトの閲覧
インターネット利用者は、パスワードをWebブラウザに記憶させるような行為をしてはならない。

6 IT端末のセキュリティ確保のために守るべき事項

- (1) インターネット上のWebサーバへのアクセス制限

ア インターネット利用者は、業務上必要な場合において、利用者の個人情報又は

利用警察組織の情報を入力して認証登録を受ける必要のあるWebサイトへ、アクセスしようとする時は、事前にシステム総括責任者の承認を受けなければならない。

インターネット利用者は、署名の無いActiveX、Java、JavaScript、VBScriptなどのコードを実行してはならない。

(2) ファイル等のダウンロード制限

インターネット利用者は、業務上必要のないファイルやソフトウェア、セキュリティ上問題があると疑われる不審なファイルなどは、ダウンロードしてはならない。

業務上必要なファイルやソフトウェアであっても、ダウンロード後、確実にウイルスチェックを実施してから操作すること。

IT端末を利用して、ホームページの開設運用をしてはならない。