熊本大学情報セキュリティポリシー実施手順書 (案) 作成について

武藏 泰雄，松葉 龍一，杉谷 賢一

ネットコミュニケーション研究部門

musashi@cc.kumamoto-u.ac.jp

概要

熊本大学における情報セキュリティ実施手順書 (案) を作成致しました。どのようにこの実施手順書解釈すれば良いのかついて実施手順書の基本的考え方を呈示しながらご紹介したいと思います。

1 背景

情報セキュリティポリシーの実施手順書について語る前に，情報セキュリティポリシーについて少し説明致します．情報セキュリティポリシーとは，組織における情報資産を守るためのルールのことです．情報セキュリティポリシーを作成する経緯は，以下の通りです．平成 13 年 6 月 15 日，各機関長に対して丸山剛司文部科学省大臣官房政策課長より “情報セキュリティ対策について (依頼)” の文書があり，それに基づいて情報セキュリティポリシーの策定準備に入りました．平成 13 年 7 月 30 日に情報セキュリティポリシーの策定に関するセミナーが行われました．情報セキュリティポリシーは ISO17799-part 1/2 と呼ばれる国際標準規格が存在し，現時点で ISO17799-part 2 に準拠することが求められます．しかしながら，大学や民間の組織にこれを適用するのは現実的にかなり困難であると考えられたため，ISMS-1.0 と呼ばれる規格が定められました [1] その後 ISMS は 2.0 になっています (ISO17799-part 2 に準拠) またほぼ同時に，国立情報学研究所と一部の大学による大学における情報セキュリティポリシー策定に関する研究会により，策定例と監査・評価例が平成 14 年 4 月 1 日に公表されました．本大学では，これに基づき，総合情報基盤センター内で原案を考案し，その後経理部情報処理課と共同で作業を行ない，平成 14 年 9 月 17 日および 10 月 21 日に情報推進会に提出し，修正を重ね平成 15 年 1 月 23 日の情報委員会で正式に認められました[5]．

さて情報セキュリティポリシー実施手順書 (以下，実施手順書と略す) を策定しないと行けない理由について説明します．

情報セキュリティポリシーを実施する上で必要な手順書と言えば，それまでであるし，また，情報セキュリティポリシー (以下，ポリシーと略す) だけでいいのではと言う気もしますが，ポリシーは ISO17799 拠れば，スタンス+ルールになります．ただ，ルールを頻繁に書き換えるのはあまり嬉しいことではないので，ポリシーとその実施手順書にわけ，ポリシーはできるだけ変更しないため，変化の早い技術面にこだわらず，一般的な方針を記述し，ポリシーを実際に大学のシステムに組み込むために必要最低限の技術を記述したものが実施手順書になります．具体的に言えばマニュアル本です．

実施手順書はいいとして，そもそもポリシーが何故に必要かと言いますと，当大学においても，昨今の情報セキュリティに関する危機を考慮すれば情報資産を何らかの方策で守って行かなければならないからです．

情報資産と言えば，顕著なものとして大学の Web サーバであります．ここで大学の Web サーバとは，大学トップのサーバや学部・学科・研究室単位のサーバ等も含まれると考えてください．仮に当大学のホームページが第三者に書き換えられてしまったらどうでしょう．最悪は，テレビのニュースや新聞記事になることで大学の信頼性は減少し，当大学への受験希望者が減少したりとか，就職先からも見放される等の大学の将来に影を落と可能性が高いような気がして来ます．

[5] 詳細は 2002 年度年報を参照してください．

特に注意しなければならないのは，学外の組織や個人は，大学を大学単位で見ることにあります．また学外組織や個人の Web サーバを故意に攻撃したりあるいはシステムのセキュリティ脆弱性を放置し且つ踏台攻撃基地あるいはウィルスワームの感染経路いや発信源として使われると，やはり最悪の場合，裁判沙汰に発展し，賠償問題にまで発展しかねません．

情報資産に対する認識やインターネット社会における常識を大学を構成員が知らないというのはセキュリティインシデントに巻き込まれた時に弁明しにくくなるし，というか，そんな時代になってしまっているので，文書の形で，組織として情報セキュリティを守る姿勢を学内外に示す必要があるわけです．すなわち情報セキュリティポリシーを策定することが，学外組織への本大学の情報セキュリティ対策を取っている事の意志表示になるということであり，また学内構成員に対する守るべき情報資産の存在と対策を知らしめることになり，極めて有用であると言える訳でもあるのです．

以上の理由により総合情報基盤センターでは，2002 年度には熊本大学情報セキュリティポリシー及び 2003 年度には国立大学法人熊本大学情報セキュリティポリシー実施手順書 (案) につきまして，事務局経理部情報処理課，および情報専門委員会委員の方々の協力の下に策定致しました．

今回は実施手順書について説明いたします．

実施手順書は，本大学における情報の重要性を考慮し，安全性 (セキュリティ) を守る上で必要と思われる項目を定め，実施手順書を示すものです．

ところで情報セキュリティ対する脅威には主として下記の 3 つが考えられます．

(1) 情報資産の機密性に対する脅威
大学における成績や個人情報等が不正に漏洩する等

(2) 情報資産の完全性に対する脅威
情報資産が正確かつ完全に保持されるかどうか，つまり情報改竄等

(3) 情報資産の可用性に対する脅威
公開している Web サーバが利用できない等

情報資産の完全性・機密性・可用性という言葉は情報セキュリティポリシーを形成する重要な言葉です．略して，CIA と呼ぶこともあります．

2 実施手順書用語

実施手順書の説明を行う上で，下記の用語が重要となります．

(1) 最高情報セキュリティ責任者
全学の情報セキュリティに関する総括的な意思決定と，学内および学内組織に対する責任を負う情報担当の理事が相当．

(2) 全学システム管理責任者
情報システムにおけるセキュリティ強化と，情報システム事案発生時の緊急対応，調査，情報収集，及び最高情報セキュリティ責任者の補佐を行う，総合情報基盤センター長が相当．

(3) 部局情報セキュリティ責任者
当該部局長が相当．

(4) 対外接続システム管理責任者
対外接続に関する情報システム管理の実施に関し，全学システム管理責任者との連絡調整を行う総合情報基盤センターの教育職員 (以下「教員」という．) が相当．

(5) 部局システム管理責任者
当該部局内の情報セキュリティに関し，責任を及び権限を有する者が相当．

(6) システム管理者 (1 部局複数名可)
当該部局内の情報システムに関する設定の変更，運用，更新等を行う，管理者権限を有する担当者が相当．

(7) 導入担当者
新規機器を導入する者が相当．

(8) 管理対象
部局システム管理責任者が情報セキュリティに関し，責任及び権限を有する範囲が相当．

(9) 情報
当該部局内で扱う全てのデータ及び管理情報が相当．

(10) データ
情報のうち，当該部局内のコンピュータや記録媒体等に格納されているものが相当．

(11) 管理情報
情報のうち，当該部局内で扱うデータを管理する目的で作成されたものが相当．

(12) 記録媒体
磁気ディスク等情報データを記録する媒体が相当．

(13) 機械室
サーバやネットワーク機器等の重要な情報関連機器が設置してある部屋及びそれに準ずる部屋が相当．[6]

(14) PC
パーソナルコンピューター等の情報機器端末が相当.

(15) 機器使用者
PC の利用者が相当.

(16) 構成員
教職員，学生，非常勤教職員及びこれらに準ずる者，及び契約等により熊本大学の情報データにアクセス可能なものが相当．[7]

(17) 不正アクセス
データ改竄，データ流出，不正侵入等の目的で不正にコンピュータなどにアクセスすること相当.

(18) 個人情報
氏名，性別，年齢，住所，メールアドレス，ホームページアドレス，学籍番号，電話番号，顔写真，学生の身分証明書，パスワード及び SOSEKI 等，学務に関する情報や附属病院，保健センター等の診療に関する情報等の個人を特定可能な情報全てが相当.

3 情報セキュリティポリシー実施手順書の構成

実施手順書は,「データの分類」,「物理的セキュリティ」,「人的セキュリティ」,「技術的セキュリティ」,「連絡体制」から構成されています.「データの分類」は文字どおり重要なデータを分類して厳重に保存し，改竄防止や漏洩防止あるいは漏洩時に暗号化しておけばなんとかなるという様な手順が記述され,「物理的セキュリティ」ではサーバ室や PC 実習室の入退室等について記述され，また,「技術的セキュリティ」についてはウィルス感染時の対処手順や不正アクセス時のログ提出について記述されています．連絡体制は学内外の連絡先等が書かれているため，本文では割愛させていただきます.

ところで実施手順書の評価基準の一つに，セキュリティを破ろうとする者に対してできるだけ手間 (コストあるいは嫌がらせとも言う) を掛けさせるものが，どれくらい含まれているかを数える方法があります.

[6]PC 実習室もここに準ずる
[7]データにアクセス可能なものの範疇は結構広い.

実施手順書を入手されましたら，その点について留意して頂ければ理解しやすいと思われます.

3.1 データの分類

守るべき情報資産はどのようなものがあるのか，それを知っておくのは非常に重要なことです．ただ，むやみやたらと分類すると，それだけで書類作成やら表計算作成が豊富に発生しますので，本大学では公開用データと非公開用データに分類する方法を採用することにしました．また諸々の理由で個人情報の取り扱いが非常に重要なので，個人情報を含むデータは原則としては非公開データへ分類し，それ以外のデータは公開データと非公開データへ分類することにしました．時節柄個人情報漏洩等を防止しなければいけないという理由もあります.

公開データを，データ漏洩 (流出) により該当データの作成者 (管理者) データの利用者及び大学に不利益が生じないものであり，公開可能なものと定義します．理想的には個人情報をまったく含まないデータのことですが，現実的には多少の個人情報を含んでいても公開しないといけないデータも含まれています.

非公開データを，個人情報や大学の運営に関る重要な機密情報を含むものと定義します．具体的に言えば，SOSEKI 等の学務情報や附属病院，保健センター等の診療に関する情報，大学の財務，経理，ネットワーク IP アドレスや全学向けサーバ，メールサーバ，研究目的で知り得るところの企業秘密やログ情報，情報の非公開契約をした情報が含まれているデータということになります.

さて，非公開データの管理責任については，当該部局の部局情報セキュリティ責任者が負うことになっていますが，実際に管理するのはシステム管理者ということになります．ほとんどの構成員は PC に関っていますのでなんらかのシステム管理者というわけです．そこで非公開データの管理方法について構成員全員が知る必要があります.

3.2 非公開データの管理方法

システム管理者は (PC 利用者含まれる)，非公開データを管理するため，非公開データへのアクセス年月日時分秒を自動的に記録するシステムを構築するのが望ましいとされます．最近のサーバプログラムはほとんど言ってよいほど標準でこのログを採る設定になっており，何もしなくても良くなりました．非公開データの格納，消去，

複製及びバックアップについては，以下のとおりする．

非公開データは暗号化して保存することをお薦めします．最近の PC の Windows や MacOS X はファイルやフォルダ自体にパスワードロックを付加したり，ファイル自体を暗号化する機能がついています．Linux 等 UNIX-like な OS では，アクセス制御および暗号化ツールを使用して簡単に中を見えないようにします．どうしても心配な人は，極端な例ですが，金庫等人目に付かない場所へ保管することが望ましいと言えます．[8]

3.3 非公開データの消去/複製

書き換え不可能な記録媒体に書き込んである媒体をそのまま捨てると，ソーシャルエンジニアリングの一手法である，ゴミ箱漁りによる情報漏洩というセキュリティ脆弱性が自然と発生します．探偵等のセキュリティ関連の仕事をされた方は判りますが，とある家庭や組織から出されるごみから，内部事情を伺う手係が得られることがあります．重要な機密情報を入れた CD-R やノート PC を捨てて，情報漏洩事件に巻き込まれたケースはここ最近非常に多くなっています．

そこで，CD-R や DVD-R などを捨てる場合は，破砕してください．そして万一，第三者の手に渡ってもそう簡単には中を閲覧できないように，暗号化して書き込んでください．ノート PC 内の書き換え可能な磁気ディスクメディアに書き込む場合も暗号化して，更にそのままデータ破壊プログラムで破壊消去することが望ましくなっています．[9]更に，磁気ディスクが不要の場合は磁気ディスク装置を分解し，中のディスク盤を物理的に破壊することも可能です．

個人的には暗号化はかなり現状では，非常に困難だと認識しています．元来インターネット技術ができるだけ開放的に作られて来た経緯があり，今更暗号化等言ってもどうするという事情はあります．かと言って流石に，非公開データが簡単に中が見れる状態で流出した場合の言い訳は無理なので，パスワードロックが掛けられる圧縮方式にすれば，悪用する際コストが発生しますから，より暗号化と同等まではいかないが，流出して問題になった時,「可能なセキュリティ対策はやっておりました」と言えると思います．

更に，パスワードロックが掛けられないような圧縮方式の場合でもこれは個人的にですが，圧縮を伸張 (展開ともいう) してと，悪用するためのコストが掛かるため，圧縮を掛けていないものよりも多少はセキュリティが高いと言えると思います[10]．

セキュリティ対策を評価する時には，セキュリティを破ろうとする相手に如何にコスト (嫌がらせ) を与えるかが重要なポイントになります．

3.4 非公開データのバックアップ (複製)

不測の事態等によるデータ損失を防止するため，定期的にバックアップ (複製) をしてください．新規バックアップ (複製) をする場合は，暗号化して記録媒体に記録し，更に，記録する前に暗号化を兼ねて圧縮を掛けてください．[11]．またバックアップは可能限り定期的に行ないましょう．

4 物理的セキュリティ

PC 実習室やサーバ室の入退室管理は学内外の者を問わず，情報セキュリティを守る上で大変重要な要素の一つです．サーバ室や PC 実習室の情報セキュリティを守るため，身分証明書 (ID) カードを使用して自動的に入退室の記録が残る管理システムが導入されていることが望ましくなっています．また，非常にローテクですが，ノート等の入退室の記録を採ることでもかなりの効果があると言えます．入退室管理システムは非常に有効ですが，なかなか導入できないなど理由がある場合はノート記録等も OK です．

教職員の部屋にも PC がありますので，外出時はスクリーンセーバなどでロックしたり，部屋を施錠するなど普段より心掛けて置けば，いろいろなセキュリティ面で効果があります．

5 人的セキュリティ

5.1 PC 使用時の構成員の責任

構成員は，自分の使用する PC 第三者により無断使用，及び許可なく非公開データ又は管理情報を閲覧されることがないようにすることが大事です..

PC の不正利用を避けるため，構成員は，ログインのパスワード設定を行いましょう．パスワードを掛けられない場合は，物理的セキュリティで述べた，部屋に鍵を掛けるなどの対策をするのが良いと思います．またでき

[8]机の上等に放置しない．
[9]まったく別の OS 等を複数回インストールしてアンインストールするなどがある．
[10]かなりグレーですが
[11]ファイル圧縮ツールにはパスワードロックできるものがある

れば，PC の不正利用を避けるため，PC を第三者に利用可能な状態で放置しないようにしましょう．

5.2 不正アクセス被害状況報告

構成員は，データの改竄，非公開データの流出，不正侵入等，情報セキュリティに関する事故を発見した場合は，システム管理者及び部局システム管理責任者へ緊急扱いとして連絡し，不正アクセス抑止に関する指示を仰いでください．そして，緊急連絡後，部局システム管理責任者，部局情報セキュリティ管理者とともに全学システム管理責任者に被害上京をできるだけ速やかに報告してください．報告手順は以下の通りです．

プロセス	手続きを行う者	手続き
(I) 連絡	構成員	• 不正アクセスを発見した場合、緊急連絡として部局システム管理責任者へ連絡し、指示を仰ぐ。 注1) システム管理者または部局システム管理責任者による連絡は、6.1.1「事案発生時の連絡」に従う。
(II) 報告	構成員	• 「不正アクセス被害状況報告書」に必要事項を記入する。 • 記入済の報告書をシステム管理者、部局システム管理責任者及び部局情報セキュリティ責任者が確認後、全学システム管理責任者に提出する。
(III) 確認	全学システム管理責任者	• 提出された報告書の記入内容を確認する。

6 技術的セキュリティ

6.1 サーバ等アクセス記録の取得及び分析

システム管理者は，各サーバ及びネットワークのアクセスログを採取しておいてください．と言われると難しいことを強要された気がするのですが，実は，新規サーバやネットワークをいれた場合は，通常システムログと言うものが自動的に採取される設定になっていますので，これも，大抵のシステムで何もする必要がほとんどありません．それと一般的にアクセス記録はプロバイダ等の大規模なネットワークを扱う組織では，不正アクセス防止法等で，通常三ヶ月間保存することが求められておりますので，それ従う事になります．

ところで，アクセス記録は何のために必要かと言いますと，実は，全学システム管理責任者は，警察からの捜査依頼等でサーバおよびネットワーク上の通信ログの提出を部局情報セキュリティ責任者に請求することができます．システム管理者は，部局情報セキュリティ責任者によるログの提出を請求された場合は，保存されているサーバ及びネットワークのアクセスに関するログを依頼書に沿った提出形式で部局情報セキュリティ責任者にできるだけ速やかに提出しなければなりません．手続き手順は下記の様な手順になります．

プロセス	手続きを行う者	手続き
(I) システムログ提出の依頼	全学システム管理責任者	• 「サーバ及びネットワークのアクセスに関するシステムログ提出依頼書」に必要事項を記入する。 • 記入済みの依頼書を部局情報セキュリティ責任者に依頼する。
(II) ログ採取依頼	部局情報セキュリティ責任者	• 依頼書に基づき該当するシステムを管理するシステム管理者へログの採取を依頼する。
(III) ログの採取	システム管理者	• ログを提出形式の媒体等に採取、部局情報セキュリティ責任者に提出する。
(IV) ログの提出	部局情報セキュリティ責任者	• ログの記録された媒体等と依頼書を全学システム管理責任者に提出する。
(V) 確認	全学システム管理責任者	• 提出されたログの解析を行う。

6.2 アクセス制御

非公開データ及び管理情報に対する権限外者からのアクセスを防止するため，システムの管理者はできるだけ利用者 ID を設定するなど制限してください．それと必要でなくなった利用者 ID はできるだけ速やかに削除しましょう．他人 ID を使ってその人に成りすます行為を防ぐためです．

6.3 ウィルス対策

ウィルスから情報を守るため，構成員は，次の手順に従ってウィルス対策を実施してください．

ネットワークに接続する前にシステムのセキュリティホール (脆弱性) を修正ソフト等で修正すること．可能であればシステム管理者の立ち会いの下で行うのが望ましい．特に，新規サーバ/PC 機器に，ウィルス対策を施すこと．また，ウィルス対策を施す前にウィルスに感染した場合は，ネットワークケーブルを抜き直ちにシステム管理責任者の指示を仰いでください．

去年大流行した Blaster の亜種である Welchia(Nachi) と呼ばれるウィルスはシステムが起動し，ネットワーク接続するだけで感染するという極めて高い感染力を誇り，特に新規購入した PC や持ち込みの PC で感染が拡大した経緯がありまして，ウィルス対策もこの様な手順となっております．

6.4 既存サーバ/PC のウィルス対処

OS(オペレーティングシステム) 等のシステム自体にセキュリティホールを有する場合は，可能な限りこれを修

正するのが望ましい．現行システムに多大な影響を及ぼす等の理由で修正が困難である場合は，使用断念するとか，アクセス制御などを導入する等，他システムや PC 等に影響を及ぼさない独立したシステムとしなければなりません．[12]

6.5 新種のウィルス感染発見時の処理

新種と思われるウィルス感染が発見された場合は，早急に新種ウィルス感染発見時の処理を実施しましょう．

新種ウィルス感染発見時の処理手順は，次の通りです．

プロセス	手続きを行う者	手続き
(I) 緊急連絡	感染した機器使用者	• ネットワーク環境(LAN)から使用機器を取り外す。 • 使用機器は電源ONの状態を継続する。 • システム管理者に状況を報告する。
(II) 指示	システム管理者	• 報告を受けたシステム管理者は、6.1.1『事案発生時の連絡』に従い、早急に事象の連絡を部局システム管理責任者に行う。又、ウィルス対処方法が全学システム管理責任者等から通達されている場合は、その指示に従う。 • ウィルスの駆除方法を確認後、機器使用者に適切な指示を与える。
(III) 対処	機器使用者及びシステム管理者	• 全学システム管理責任者等の指示に従い、ウィルス対策を行う。
(IV) 復旧	機器使用者及びシステム管理者	• ウィルス対策完了後、全学システム管理責任者等の指示に従い、使用機器を復旧する。
(V) 報告書の作成	機器使用者	• 「新種ウィルス感染報告書」に必要事項を記入し、システム管理者に提出する。
(VI) 報告書の確認	システム管理者	• 提出された報告書の記入内容を確認後、部局システム管理責任者及び部局情報セキュリティ責任者の確認を経て、全学システム管理責任者に提出する。
(VII) 再発防止対策	全学システム管理責任者	• 提出された報告書の記入内容を確認する。 • 再発防止策を検討し、職員に再発防止策を周知徹底する。

ところでふと疑問に思うのは，既知のウィルスはどうすればいいのでしょうか．既知のウィルスの感染例はすべて報告すると，大変な量になる可能性があり，セキュリティインシデントの把握にマイナスになる可能性があると思われます情報セキュリティ研究を行っていると，良くセキュリティインシデントという言葉を聞きますが，ウィルス流行とかセキュリティ攻撃などをセキュリティインシデントと呼びます．

ここでは我々が良く直面するウィルスについて新種と既知と分類してその扱い方を考えてみましょう．

6.5.1 新種と既知のウィルスの違い

新種のウィルスに感染する場合と古いウィルスに感染する場合は状況が少し違ってきます．新種のウィルスは主としてワーム活動を行ない感染能力が高いのが普通です．ですので，緊急で対処する必要があります．ワーム活動を行うウィルスはメールを介するものとシステム脆弱性を利用するものとの 2 種類に大別できます．

メールを介するメール型ワームはウィルス駆除ソフトのパターンや駆除方法が行き渡るまでは腰すえて対処する必要がありますが，メール型のワーム活動は，メールワームはウィルスパターンをアップデートすることで，また駆除方法が行き渡るとネット上にある種のフィルタが形成されるため次第に感染が減少します．その為既知ウィルスとなってしまえば，これらのフィルタで感染はある程度防げることになります．従って新種だけ報告した頂ければ，良いと言うことになります．

6.5.2 システム脆弱性悪用型ワーム

しかし，システム脆弱性利用型のワームは，ウィルス駆除ソフトで対処しきれない問題がある場合があり，その様なウィルスは，システム脆弱性を修正しない限り感染拡大は終わらない可能性があります (例えば，W32/Welchia.A)．更にこの種類ワームは利用者やウィルス駆除ソフトから見えないところで活動しますので，特殊な検知システムが必要になる場合もあります．簡単に言えば，システム脆弱性利用型ワームはいつまでたっても上記で述べた所の新種でありつづけるわけです．この様な場合は，システム脆弱性悪用型のワームにつきましては，完全なシステム脆弱性が修正されるまで新種と同じ扱いにしていただければと思います．そしてシステム脆弱性がネット上に存在しなくなればワーム活動は事実上できなくなるため，やはり新種のウィルスの報告だけしていただけ良いということになります．

7 今後の展開

前回情報セキュリティポリシーが策定されたのに引き続き，今回は情報セキュリティポリシー実施手順書が策定されました．以後セキュリティ対策の評価や監査をどの様にすすめていけば良いか議論する段階になったと思

[12] 具体的に当センターの事例を紹介致しますと，センターがメンテしている，本大学の重要なサーバ (DNS やメール等) も大部分が Linux で動作させています．ただ Windows 同様にしばしば OS(カーネル) の脆弱性がが見つかるため，脆弱性の報告がある都度その修正を行っております．しかし IPv6 等に対応させているため通常の Update が行えず，OS の修正が半月遅れになるなどあまり嬉しい状態ではありません．そこでセキュリティ攻撃を掛けてくる IP アドレスをあらかじめ Linux に元々備わっているフィルタを使って制限を掛けたり，ローカル利用者を一時的に使えなくしたりとか，不要な，サーバ等はできるだけ切ってセキュリティ対策とします．この様なセキュリティ対策を講じておけば，やはりセキュリティ攻撃的にコスト高なりますので，自然とセキュリティが高くなります．

われます．今後はセキュリティ対策評価を行いながら実施手順書を改訂して行くことになると思います．構成員全員皆様のご協力をお願い申し上げます．

8 情報セキュリティ関係法令

(1) 主な情報セキュリティ関係法令

- 不正アクセス行為の禁止等に関する法律
- 行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律
- 行政機関の保有する情報の公開に関する法律
- 電子署名および認証業務に関する法律
- 著作権法
- 不正競争防止法
- 犯罪捜査のための通信傍受に関する法律
- 刑法
  - 第 7 条の 2(定義)
  - 第 157 条第 1 項 (公正証書原本不実記載等)
  - 第 158 条第 1 項 (偽造公文書行使等)
  - 第 161 条の 2(電磁的記録不正作出および供用)
  - 第 234 条の 2(電子計算機損壊等業務妨害)
  - 第 246 条の 2(電子計算機使用詐欺)
  - 第 258 条 (公文書等毀損)
  - 第 258 条 (私用書等毀損)

注) 下記 URL を参照すること．

http://law.e-gov.go.jp/cgi-bin/idxsearch.cgi

(2) 施行が予定されている法律

- 特定電気通信役務提供者の損害賠償責任の制限および発信者情報の開示に関する法律

注) 下記 URL を参照すること．

http://www.soumu.go.jp/joho_tsusin/top/-denki_h.html

(3) 成立が予想される法律案

- 個人情報の保護に関する法律案

注) 下記 URL を参照すること．

http://www.kantei.go.jp/jp/it/index.html

[1] http://www.isms.jipdec.or.jp/