

インドネシアにおける
青少年保護のためのインターネット
規制と運用

2012年2月
独立行政法人 日本貿易振興機構

本報告書に関する問い合わせ先：
日本貿易振興機構（ジェトロ）
調査企画課

〒107-6006 東京都港区赤坂 1-12-32
TEL: 03-3582-5544
FAX: 03-3582-5309
email: ORA@jetro.go.jp

【免責条項】

ジェトロは、本書の記載内容に関して生じた直接、間接的若しくは懲罰的損害及び利益の喪失については、一切の責任を負いません。これは、たとえジェトロがかかる損害の可能性を知らされている場合であっても同様とします。

(C) JETRO 2012

本報告書の無断転載を禁ずる。

アンケート返送先 FAX 03-3582-5309
email: ORA@jetro.go.jp

日本貿易振興機構 調査企画課宛

● ジェトロアンケート ●
「インドネシアにおける青少年保護のためのインターネット規制と運用」
に関するアンケート

ジェトロでは将来の市場として、潜在的需要が高い可能性のある国や地域のマーケット情報を日本の中堅中小企業の方々に紹介することを目的に本調査を実施いたしました。報告書をお読みいただいた後、是非アンケートにご協力をお願い致します。

■質問1：「インドネシアにおける青少年保護のためのインターネット規制と運用」について、どのように思われましたでしょうか？（○をひとつ）

4：役に立った 3：まあ役に立った 2：あまり役に立たなかった 1：役に立たなかった

■質問2：上記のように判断された理由、また、その他、本報告書に関するご感想をご記入下さい。

--

■質問3：その他、ジェトロへの今後のご希望等がございましたら、ご記入願います。

--

■お客様の会社名等をご記入ください。(任意記入)

ご所属	□企業・団体	会社・団体名
		部署・部署名

～ご協力有難うございました～

目次

序章 インドネシアのインターネット利用に関する概要.....	2
第一章 情報および電子商取引に関する 2008 年度法令第 11 号	4
I-1 法令制定背景.....	4
I-2 UU ITE の主な内容.....	4
I-3 具体的な規定内容.....	6
I-4 罰則.....	11
I-5 法律違反の決定権限を有する機関、団体.....	11
第二章 インターネットコンテンツ保護における政府の役割	13
II-1 情報通信省の活動 (INSAN).....	13
II-1.1 INSAN 活動その一: 法令違反通報クレームセンター.....	13
II-1.2 INSAN 活動その二: INSAN Goes to Campus.....	13
II-1.3 INSAN 活動その三: テレコミュニケーションボランティアの設立.....	14
II-2 制限ウェブサイトフィルターソフトおよび制限ウェブサイトのアクセス遮断製品.....	14
II-2.1 ソフトウェア	
1:インドネシアの青少年向け、安心・安全なインターネット利用デバイス (PERISAI).....	14
II-2.2 ソフトウェア 2: Trust Positive.....	14
II-2.3 ソフトウェア 3: Nawala プロジェクト.....	14
第三章 インターネットコンテンツ保護に関する民間及び非政府組織の役割	17
III-1 AWARI(インドネシア・インターネットキオスク).....	17
III-2 Information and Communication Technology (ICT) Watch.....	19
III-3 Asosiasi Penyelenggara Jasa Internet Indonesia (APJII).....	20
III-4 Kalam Kata.....	21
参考資料・参考文献.....	22

本報告書で扱う法令「情報および電子商取引に関する 2008 年度法令第 11 号(UU ITE - Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik)」の内容や用語は仮訳・仮名称であり、正確な理解のためには、原文をご参照下さい。

序章 インドネシアのインターネット利用に関する概要

インドネシアのインターネットの歴史は1990年前半に始まり、当初は一定のグループユーザー向けであったが、1994年にはIndonet社がインドネシア初のインターネットサービスプロバイダー(ISP)を設立し、一般向け商用サービスを提供するようになった。それ以来、インドネシアのインターネットユーザー数は著しく増加しており、情報通信省のデータによると、2010年のユーザーは4千5百万人で、人口の約12.3%に上ると発表されている。ユーザー数の増加に伴い、インターネットを利用できる施設も急増しており、インドネシア中のインターネットアクセスの約42%がインターネットキオスクやサイバーカフェ、ホット・スポット・エリアなどから行われていると推測されている。以前は大学や公共図書館、オフィスなどの限られた場所でしかインターネットを利用することはできなかったが、最近では個人用パソコンからのアクセス数も増加しており、またそれを上回る勢いで携帯電話からのインターネット利用が急増している。インドネシアのインターネットユーザーは、今後益々増えることが予想され、人々の生活様式の在り方にも影響を与えている。他の国々同様インドネシアでも、ユーザーが様々な知識や情報に容易にアクセスすることが可能になり、様々な商取引も電子商取引を通して、迅速に確実にこなせるようになってきている。以上のように社会生活に有益な変化をもたらしてはいるが、有害な影響を与える一面も無視できない昨今である。

他国の例に洩れずインドネシアでも、インターネットが社会的に容認できない情報へのアクセスを容易にし、社会モラルを脅かしかねない事態が発生しており、インターネットを通してポルノサイト閲覧(開設)や何らかの不正、偽造、詐欺、中傷等の行為が発生している。特に、若年層への悪影響は深刻化しており、宗教的・社会文化的規範に対する違反行為の多発は、健全な国家の発展に悪影響を及ぼしかねないとも懸念されている。

A.C. ニールセンの2001年サイバー犯罪調査結果によると、インドネシアはサイバー犯罪の発生率・深刻度で、アジアのワースト4位、世界のワースト6位に位置付けられている。また、英国の民間インターネットモニタリング組織であるNS2の調査によると、2006年の時点でネット犯罪行為を行うインドネシアのユーザー年齢層は16歳から25歳の若い年代であるとの結果が発表されている。同時期のコンパス紙(現地主要日刊新聞)によれば、インターネットユーザーの

うち48%が22歳から25歳の年齢層で(大半は大学生)、28%が18歳から21歳であることから、若年層へのインターネット犯罪関与度は深刻に受け止めるべき事実である。¹

インターネットに由来する犯罪の一例として、2011年にジャカルタ東部で起こった9歳の少女強姦事件があり、その容疑者である被害者の友人2人は、インターネットで見たポルノ映画に触発されて事件を起こした。以上のような事件は他にも発生しており、インターネットが若年層の生活に悪影響を与えている事の一部を示している。また、2011年にビバ・ニュース社(インドネシアニュースポータル社)が中学生レベルの子供向けに行ったインターネット調査によると、この調査にアクセスした回答者の約97%が、ポルノサイトにアクセスしたことがあり、92%が何らかの性的行為の経験があるという結果であった。

このような若年層への深刻な悪影響を受け、インドネシア政府は議会を通して、情報および電子商取引に関する2008年度法令第11号を定めた。通称UU ITEと呼ばれる同法令は、後に情報通信省がマルチメディア情報の内容に関する政策や規定を設定する基本の考え方となっている。青少年に限られたインターネット法令ではないが、青少年を含むインドネシア社会全体へのメッセージであり、戒めともなっている。同法令に関する詳細は、次章で詳細に触れる。

¹ コンパス誌(2005年)

第一章、情報および電子商取引に関する 2008 年度法令第 11 号

I-1 法令制定背景

2008年3月25日に発布された「情報および電子商取引に関する2008年度法令第11号(UU ITE)」は、あらゆる電子情報や電子商取引を正しく管理運営する為の内容を盛り込んだ、インドネシア情報技術発展上の基盤構築ともいえる法令である。同法令は14章54条で成り立っており、全関係機関との包括的な協議を経て、様々な局面を想定した上で作成された基準項目が定められている。

UU ITEは、情報技術が急速にインドネシア社会に普及している状況を考慮し制定されている。情報技術が社会生活や国家の経済成長に与える影響は益々大きくなり、関連する社会福祉システムを整備する必要性も生じている事から、特にこのような新しい技術に馴染みやすい若年層を念頭においた内容である。なお、同法令では若年層の定義は述べられていないが、アンチポルノグラフィーにかかる2008年度法令第44号に、若年層は18歳未満の年齢層を指すと定義されており、同定義が当てはまる。

インドネシア政府はインターネット関連法令を制定し基盤を整備することによって、情報技術開発をサポートしている。同法令が安全で正しい情報技術の利用を推進し、インドネシア社会や文化、宗教規範を、有害な影響から守ることが期待されている。

I-2 UU ITE の主な内容

情報および電子商取引法令の各 13 章には、次の内容が述べられている

- I: 共通政策
- II: 目的および原則
- III: 情報、文書、電子署名
- IV: 電子証明および電子システムの取扱
- V: 電子商取引
- VI: ドメインネーム、知的財産権及びプライバシー
- VII: 禁止行為

- VIII: 訴訟行為
- IX: 政府と社会の役割
- X: 検証
- XI: 犯罪行為
- XII: 移行行為
- XIII: 結び

UU ITE が用いる主な7用語について。

- 電子情報および(または)電子文書:

電子情報とは電子データの種類であり、文章、音声、絵画、地図、デザイン、写真、EDI、Eメール、電報、文字多重放送、ファックス、その他事情に通ずる人には理解可能な処理データ等を含む。電子文書は、作成、送信、受信、転送、アナログ保存、デジタル保存、電磁保存、光学保存が可能な電子情報であり、コンピューターやその他電子システムで閲読、閲覧、聞き取りが可能なものである。

- 電子商取引:

コンピューターやコンピューターネットワーク、または他の電子メディアで処理される法的行為

- 電子署名:

特定の電子情報内容につき、同意・提携・遵守を示す電子情報に変換された署名であり、証明や確認用に使用される。

- 電子証明

正式な機関によって認証された、公的な電子証明文書。電子署名を含む

- ドメインネーム:

インターネット上で通信が可能な政府関係者、個人、企業、社会団体のインターネットアドレス。当アドレスはコードや文字で構成され、インターネット上の特定のロケーションを示すものである。

- 知的財産権:

電子情報そして(または)電子文書の形で表わされる知的創造的産物やインターネットサ

イトは、知的財産権によって保護される(情報及び電子商取引法令第 25 条)

- 個人情報:

個人情報を電子メディア上で使用する際には、個人情報の関係者合意を得なければならない。(規定で別途定められた場合を除く)

I-3 具体的な規定内容

同法令の27条から37条には、情報及び電子商取引に関する禁止行為が定められている。下記6点は主要禁止行為であり、若年層を有害サイトから保護する点においては、27条が関連深い。

- a. 猥褻・違法コンテンツ関連行為
- b. 違法アクセス
- c. 違法傍受
- d. データ妨害
- e. 装置の乱用・悪用
- f. コンピューターを使用した詐欺、偽造行為

下記は各禁止行為に関する対象者および対象行為である。

<p>a. Pasal 27: 1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.</p>	<p>a. 第27条: 1) 意図的に特段の権利なく、規範やモラルに反する電子情報や電子文書を配信、送信、アクセス可能にした者</p>
<p>2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.</p>	<p>2) 意図的に特段の権利なく、ギャンブルの要素を含む電子情報や電子文書を配信、送信、アクセス可能にした者</p>
<p>3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat</p>	<p>3) 意図的に特段の権利なく、中傷・名誉棄損内容を含む電子情報や電子文書を配信、送信、アクセス可能にした者</p>

<p>diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.</p>	
<p>4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.</p>	<p>4) 意図的に特段の権利なく、恐喝・脅迫内容を含む電子情報や電子文書を配信、送信、アクセス可能にした者</p>
<p>b. Pasal 28:</p>	<p>b. 第28条</p>
<p>1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.</p>	<p>1) 意図的に特段の権利なく、電子商取引上のでっち上げ、誤解を招くような情報を配信し、消費者の信頼感を損なわせる者</p>
<p>2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).</p>	<p>2) 意図的に特段の権利なく、人種的、宗教的、部族的、またはコミュニティ間など、特定のグループ間の憎悪をかきたてるような情報を配信した者</p>
<p>c. Pasal 29:</p>	<p>c. 第29条</p>
<p>Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakutkan yang ditujukan secara pribadi.</p>	<p>意図的に特段の権利なく、特定の個人に向けて暴力的脅迫や呪詛内容を含んだ電子情報や電子文書を送信した者</p>
<p>d. Pasal 30:</p>	<p>d. 第30条</p>
<p>1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.</p>	<p>1) 意図的に特段の権利なく、違法に、他者が所有するコンピューターや電子システムにアクセスした者</p>
<p>2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.</p>	<p>2) 意図的に特段の権利なく、違法に電子情報や電子文書を手に入れるため、コンピューターや電子システムにアクセスした者</p>
<p>3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses</p>	<p>3) 意図的に特段の権利なく、違法にセキュリティシステムを妨害、故障、すり抜け、</p>

<p>Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.</p>	<p>破壊して、コンピューターや電子システムにアクセスした者</p>
<p>e. Pasal 31: 1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.</p>	<p>e. 第31条 1) 意図的に特段の権利なく、違法に、他者が所有するコンピューターや電子システムにアクセスし、電子情報や電子文書の妨害や盗用行為を犯した者</p>
<p>2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.</p>	<p>2) 意図的に特段の権利なく、違法に、他者が所有するコンピューターや電子システム内の電子情報や電子文書の送受信妨害を行った者。情報内容の変更や削除、抹消行為が発生しなかった場合にも該当する</p>
<p>3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.</p>	<p>3) 警察、検事、その他規定で定められた法的機関の要請によって法的行為の範囲内で行われる妨害行為は、(1)項及び(2)項で述べられた妨害行為から除かれる</p>
<p>4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.</p>	<p>4) (3)項で述べられた妨害行為プロセスの詳細規定については、別途政府規定によって定められる</p>
<p>f. Pasal 32: 1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak,</p>	<p>f. 第32条 1) 意図的に特段の権利なく、違法に、他者または公的電子情報や電子文書を、変更、追加、切り取り、送信、妨害、削除、移動、隠す等の行為を犯した者</p>

<p>menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik.</p>	
<p>2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.</p>	<p>2) 意図的に特段の権利なく、違法に、電子情報や電子文書を、認可されていない第三者の電子システムに移動、送信した者</p>
<p>3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.</p>	<p>3) 一般にはアクセス不可であるべき電子情報や電子文書が、非アクセス対象者に放出されるなど、(1)項で述べられる行為に関与した者</p>
<p>g. Pasal 33: Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.</p>	<p>g. 第33条 意図的に特段の権利なく、違法に、電子システムに妨害行為を働き、電子システムの本来の作業を妨げるような行為を犯した者</p>
<p>h. Pasal 34: 1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33; b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27</p>	<p>h. 第34条 1) 意図的に特段の権利なく、違法に、第27条から第33章までに触れる行為を行い、助長させるようにデザインされたコンピュータハードウェアやソフトウェアを生産、販売、使用、輸入、流通、提供、所有している者 また、第27条から第33章までに触れた行為を実現させる為に、電子システムへのアクセスを助長させるコンピュータコード、アクセスコード、類似のものを含む</p>

<p>sampai dengan Pasal 33.</p>	
<p>2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.</p>	<p>2) (1)項で述べられた行為は、研究活動や電子システムを法的に守る新たな電子システムの開発テストに該当する場合、犯罪行為とみなされず、違法にはならない</p>
<p>i. Pasal 35: Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.</p>	<p>i. 第35条 意図的に特段の権利なく、違法に、ある電子情報や電子文書が純正物に見えるように、操作、介入、変更、削除、破壊行為を行う者</p>
<p>j. Pasal 36: Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.</p>	<p>j. 第36条 意図的に特段の権利なく、違法に、第27条から第34条までの行為を行い、第三者に損失を招いた者</p>
<p>k. Pasal 37: Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.</p>	<p>k. 第37条 インドネシア域外の電子情報に、第27条から第34条までに述べられた禁止行為を意図的に行い、インドネシアの司法権下にある者</p>

I-4 罰則

UU ITEのXI章は第45条から第52条を含み、UU ITEへの違反行為に対する罰則について述べている。対象罰則行為とその罰則内容は、次の7項目である。

- a. 猥褻文書/違法コンテンツ関連行為について
罰則:6-12年間の収監、そして(または)10億ルピアから20億ルピアの罰金刑。(第45条)
- b. 違法アクセスについて
罰則: 6-8年間の収監、そして(または)6億ルピアから7億ルピアの罰金刑。(第46条)
- c. 違法傍受について
罰則:10年年間の収監、そして(または)最高8億ルピアの罰金刑。(第47条)
- d. データ妨害について
罰則: 8-10年間の収監、そして(または)10億ルピアから50億ルピアの罰金刑。(第48条)
- e. システム妨害について
罰則: 10年間の収監、そして(または)最高100億ルピアの罰金刑。(第49条)
- f. 装置の乱用・悪用について
罰則: 10年間の収監、そして(または)最高100億ルピアの罰金刑。(第50条)
- g. コンピューターをしいした詐欺、偽造行為について
罰則: 12年間の収監、そして(または)最高120億ルピアの罰金刑。(第51条)

I-5 法律違反の決定権限を有する機関、団体

UU ITE X章の第42条と第43条では、インドネシア国家警察および情報通信省の2機関が、UU ITEの定める違反行為の判断をする権限機関、団体として挙げられている。法令違反の審査・認定を実施する上で、警察や情報通信省は次のような行動を取ることが認められている。

- a. 法令違反に関する報告またはクレームを第三者から受領すること
- b. 法令違反の関係者から聞き取りを行うこと
- c. 法令違反についての報告や説明に関しての事実確認作業
- d. 法令違反の容疑者または容疑の掛けられた企業の取り調べを行うこと

- e. 法令違反が疑われる情報技術関連の対象ツールや設備、ロケーションの調査
- g. 法令違反が疑われる情報技術活動のツールや設備の封鎖、排除(有害ウェブサイトの封鎖、排除を含む)

所有するウェブサイトが封鎖、排除対象となった第三者は、異議申し立てを裁判所に訴える事が可能である。裁判所で、異議申し立ての内容について審査の上、法令に違反していないとの判決が出た場合、情報通信省は該当ウェブサイトの封鎖を解く事になる。

第二章 インターネットコンテンツ保護における政府の役割

II-1 情報通信省の活動 (INSAN)

INSAN (Internet Sehat dan Aman)とは、インドネシア語で「健全で安全なインターネット」の略称で、有害なインターネットコンテンツから社会を守る事を目的にした、情報通信省の国家的プログラムの一つである。同プログラムでは、インターネットの有効・有益利用に関する意識普及活動を実施している。インドネシアは、ポルノグラフィーのダウンロード率が世界で 10 位以内に入る国であるが、安心、安全なインターネット利用を社会に促すためにインドネシア政府が推進している活動である。また、INSAN は、法令違反の報告を受理するクレームセンターとしての役割も担っており、主な活動は次の通りである。

II-1.1 INSAN 活動その一：法令違反通報クレームセンター

マルチメディアの内容に関して一般人が違反行為を通報する場合、情報通信省では下記の専門の部署で通報を受理している。

部署名	Ditjen Aplikasi Telematika
住所	2 Gedung depan, kantor Kementerian Kominfo, Jakarta Indonesia
電話番号	62 -21- 3899 - 7800
電子メール	aduankonten@depkominfo.go.id

II-1.2 INSAN 活動その二：INSAN Goes to Campus

「INSAN Goes to Campus」は、全 4 学期中を通して行われる、大学キャンパスでの周知活動である。大学側は場所と設備を提供し、インターネット産業関連業者や情報通信省の担当者を招待して、安心・安全なインターネット利用に関する説明会を定期的で開催する。運営メンバーの参加者は高校生や大学生であり、熱心なインターネットユーザーである他の学生や学校スタッフに対して、インターネット利用に関する普及活動を行っている。また大学は同プログラムに参加するよう積極的に高校生に働きかけている。活動に参加しているインターネット業界の有名人も多く、Andrew Darwis 氏 (Kaskus-インドネシアの SNS 創始者) や、情報通信省テレコミュニケーション・アプリケーション総局局長 Ashwin Asongko 氏、インドネシア人有名ブ

ロガーの Enda Nasution 氏などが挙げられる。

全学生メンバーは、安心、安全なインターネット利用の必要性を理解した事を証明する証明ホルダーを得て、引き続き普及活動を行う事を義務付けられる。また、彼らの活動は全国的なメディアで紹介され、INSAN 殿堂サイトに参加者の名前が記録される。

II-1.3 INSAN 活動その三: テレコミュニケーションボランティアの設立

同ボランティアの設立背景には、安全なインターネット利用とインターネットの有効性を社会に周知する事にあるが、具体的にはインターネットの技術的問題を解決することで、安心・安全なインターネット利用を実現させるものである。テレコミュニケーションボランティアは、インターネット接続問題の修復法や、有効・有益なインターネット利用に関する教育法などの研修を受けて、ボランティアとしての活動を行う事ができる。また、テレコミュニケーションボランティアは黄色、緑、赤の 3 カテゴリーに分類され、緑ラベルは普及教育活動、黄色ラベルはインターネットコネクションデバイスのテクニカルサポート、赤ラベルはネットワークとデバイスサポートを通じての災害管理など、色によってサポート業務レベルが分けられている。

II-2 制限ウェブサイトフィルターソフトおよび制限ウェブサイトのアクセス遮断製品

インドネシア情報通信省コミュニケーション・アプリケーション総局では、未成年者をポルノグラフィックコンテンツが含まれるサイトから守る為に、次のような保護ソフトウェアや商品を開発している。

II-2.1 ソフトウェア 1:

インドネシアの青少年向け、安心・安全なインターネット利用デバイス (PERISAI)

情報通信省は前述の INSAN プロジェクトの支援の一貫として、有害なインターネットから子供たちを守り、同時に教育を提供する PERISAI という名称のオープンソース・ソフトウェアを、技術研究省と Linux の IGOS センターと共同で開発した。このソフトウェアは、特にインドネシアの子供たち向けに作成された地場のソフトウェアで、幼稚園から中学生までの幅広いレベルの数学や言語、コンピューター、地理、化学、物理学などの教育コンテンツを含んでいる。教

育コンテンツに加えて、同ソフトウェアは有害なウェブサイトへのアクセスを遮断する機能を備えており、<http://www.perisaianak.com>（インドネシア語）で詳細閲覧可能である。

PERISAI は次の 7 点から有益と考えられている。

1. 有害インターネットから青少年を守ることができる。
2. 幼稚園、小学校、中学校、高等学校および大学教育プログラムを提供できる。
3. 教育ゲームを提供できる。
4. インドネシア中の都市に展開する PERISAI 支部から無料で入手可能である。
5. 合法的なソフトウェアで、海賊版ソフトウェアを排除できる。
6. 地場の開発チームによって作成されたため、インドネシアのコンピューターユーザーのニーズに通じている。
7. 政府プログラム、特に INSAN プログラムに沿っている。

II.-2.2 ソフトウェア 2: Trust Positive

Trust Positive は情報通信省によって開発されたインターネットコンテンツ保護支援システムで、健全で信頼性の高いウェブサイト情報に従い、インターネットアクセス保護サービスを提供するものである。TRUST はインドネシア語の Terpercaya(信頼)、Referensi Utama(主要リファレンス)、Sehat(健康)、Teramankan(安全)の各用語の頭文字を取って名付けられたもので、政府機関内では情報通信省から導入され始めた。同システムは、次のような機能を持っている。

- ドメイン保護
- トップ・レベル・ドメインのフィルタリング
- URL(リンク)保護
- URL のフィルタリング
- 情報コンテンツ保護

TRUST システムは、全公的情報アクセスサービスを参照できる中央サーバーとしてのメカニズムを持っており、インドネシアのインターネットユーザー像の分析を行う事も可能である。同システムは情報通信省のウェブサイトから詳細を閲覧することが可能である。

<http://trustpositif.depkominform.go.id> (インドネシア語)

II-2.3 ソフトウェア 3: Nawala プロジェクト

Nawala プロジェクトはDNSで構成され、有害なインターネットコンテンツをフィルタリングできる無料システムである。同システムは、インドネシアの法令や社会的規範、モラルに反するポルノグラフィやギャンブルなどの有害コンテンツをブロックすることが可能であり、また、ウイルスやマルウェアのような有害なプログラムを含んでいるインターネットウェブサイトを遮断する事もできる。

2009 年末に、情報通信省と AWARI 社によって開発・公開された同システムは、このシステムの将来的なユーザーとなり得るインターネットコミュニティや一般人の意見を取り入れてデザインされている。システムを通して得られた意見は、Nawala プロジェクトチームによって精査され、該当ウェブサイトをフィルタリングにかけるかどうか判断される。同プロジェクトの詳細は www.nawala.org (インドネシア語)を通じて閲覧することが可能である。

第三章 インターネットコンテンツ保護に関する民間及び非政府組織の役割

前章で詳細に触れた INSAN プログラムは、政府支援に加えて非政府組織の支援も受けており、プログラム実施に関する監視作業が行われている。INSAN プログラムを確実に実行していくためには、プログラム監視能力を備えた独立系非政府組織が、政府やその他民間組織と協力し、支援を行っていくことが重要である。

III-1 AWARI(インドネシア・インターネットキオスク)

2000年5月25日に設立した AWARI は、インターネットキオスク(インターネットサービスを提供する小規模な店舗)オーナーを中心とする協会である。AWARI は政府の INSAN プログラムを支援し、「健全なインターネットキオスクプログラム」でインターネットキオスクからポルノグラフィやギャンブル、中傷行為やウィルス等の有害なサイトアプリケーションを排除することを宣言している。「健全なインターネットキオスクプログラム」のミッションは次の 2 項目から成り立っている。

-
- | | |
|---------|--|
| 1. クリーン | <ul style="list-style-type: none"> - 海賊版ソフトウェアを持たない - 有害サイトコンテンツを持たない - オープンスペースインテリア |
|---------|--|
-
- | | |
|--------|---|
| 2. 安全性 | <ul style="list-style-type: none"> - 青少年の為の安全性 - 社会と環境の安全性 - インターネットキオスクオーナーの安全性 |
|--------|---|
-

「健全なインターネットキオスクプログラム」は、情報通信省を初めとする政府関係者やその他の AWARI 関係者から様々な支援を受けているが、マイクロソフトもその支援者の一員である。マイクロソフトの支援の中には、AWARI メンバーにソフトウェアを割引して販売するものがある。

AWARI は、インターネットキオスクの機能を社会に有効的に生かしていく為には、青少年や女性を有害コンテンツから守る責務があると考えている。そこで、インターネットキオスクオーナーである全メンバーに、政府プログラムへの支援を義務付けており、ポルノグラフィコンテンツフィルターを各インターネットキオスクで設置する事等が求められている。具体的には

INSAN プログラムと連携をとり、次の 3 通りの有害コンテンツフィルタリング方法を推奨している。

1. パソコン上のフィルタリング
2. プロキシまたはサーバーのキャッシュ情報を通してのフィルタリング
3. AWARI が開発した DNS Nawala を通してのフィルタリング（「DNS poisoning」と呼ばれる技術で、誰かがポルノグラフィックサイトを開こうとした場合、該当ユーザーを他の有益サイトに飛ばしてしまうもの）

また INSAN プログラムを支援するために、AWARI は「情報及び電子商取引にかかる法令」に関し声明を発表しており、下記に一部引用する。²

1. AWARI は、インドネシアの情報技術業界の発展と合法性のために、「情報及び電子商取引にかかる法令」の正当性を全面的に支援する。
2. ポルノグラフィックサイトに関し、各インターネットキオスクは次のフィルタリング行為を実施する。
 - a. インターネットカフェ・ユーザーガイドライン、マニュアルの整備
 - b. ポルノグラフィックサイトにアクセスするユーザーへの直接的警告
 - c. ルーターまたはプロキシにポルノグラフィック・フィルターをインストール
 - d. インターネットカフェに設置してある全コンピューターにポルノグラフィック・フィルターをインストール
 - e. 最も有効なソリューションの一つである DNS フィルターを使用（しかし、ポルノグラフィックであるとの解釈は、DNS フィルターのサービスプロバイダーが同様の解釈をした時に限る為、限界性もある。）
3. インターネットキオスクにとってポルノグラフィックコンテンツは有害である。なぜなら、
 - a. そのような制限回線は負荷が高く、高価であるため

² 同声明の内容や用語は仮訳であり、正確な理解のためには、インドネシア語の原文参照が薦められる。

- b. ポルノサイトやギャンブルサイトからは、ウイルス、スパイウェアおよびマルウェアに侵入されやすく、感染しやすいため
- c. インターネットキオスクにネガティブイメージを植えつけるため

更に、AWARI は Yayasan Keluarga Kreatif Indonesia (インドネシアクリエイティブ家族協会) と協力してフリーホットラインを開設し、社会に対してネガティブ影響をもたらしかねないインターネット行為の通報を推奨している。(電話番号 0800-1000147)

AWARI	
住 所	: Jl. Hang Lekir Raya No. 2, Kebayoran Baru Jakarta Selatan DKI Jakarta 12120

Yayasan Keluarga Kreatif Indonesia(インドネシアクリエイティブ家族協会)	
住 所	: Komplek Pondok Mandala II, Cimanggis, Depok

III.-2 Information and Communication Technology (ICT) Watch

インドネシア ICT パートナーシップ (ICTWatch)は、2002 年に設立されたインドネシアの非営利組織(市民団体)である。情報通信技術の発展に懸念を抱く若い世代によってジャカルタに設立されたものであり、インドネシア法務人権省の決定書に基づきパートナーシップが認められた法的機関である。同組織のビジョンは「全ての人は、懸念や不安感を抱くことなく、安全で確実な情報メディアを介して、有益な情報にアクセス、生産、配信、利用する権利がある。」ものである。

同組織の重要なプログラムである Internet Sehat (健全なインターネット)は、インターネットを賢く安全に、責任をもって利用する活動として全国に広まっており、「賢く安全なインターネット利用で、表現の自由をもたらす」事を、下記アプローチで実現させようとしている。

- 1) 家族および学校レベルでの自己検閲
- 2) 面白く、有益な現地コンテンツの充実
- 3) 情報通信技術に関する市民の自発的行動促進

同プログラムを推進していくために、ICT Watch では、外部のテレコミュニケーション・プロバ

イダーPT XL Axiata から支援を得ており、共同でガイドライン本を出版している。このガイドライン本は図書館や大学キャンパス、その他教育機関、教育コミュニティに無料で配布され、次のURLから自由にダウンロードすることも可能である。特に、青少年がガイドライン本の内容について学べるように、配慮されている。 <http://www.internetsehat.org> (インドネシア語)

Information and Communication Technology (ICT) Watch	
住 所	: Perumahan Rawa Bambu I, No.B/10, Pasar Minggu, Jakarta12520, Indonesia
電話番号	: 62-21-98495770
電子メール	: info@ictwatch.com

III.-3 Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)

APJII は、1996 年 5 月 15 日に設立されたインドネシアインターネットサービスプロバイダー協会である。同協会では、インドネシアネットワークインフォメーションセンター(ID-NIC)を形成し、国内のインターネットネットワーク開発に役立っている。なお、同協会は前述の INSAN プログラムを支援しており、「潜在力を導き出すための健全なインターネット」というテーマ会議を開催している。会議の参加者には AJI(独立系ジャーナリスト団体)、APJII、Cipta Media Bersama、ウィキ・メディア・インドネシア、フォード財団、Detikcom、ICT Watch などがあげられる。

APJII	
住 所	: Cyber Building 11 th floor, Jl. Kuningan Brat No.8, Jakarta Selatan 12710, Indonesia
電話番号	: 62-21- 5296-0634
電子メール	: info@apjii.or.id

III.-4 Kalam Kata

Kalam kata は様々な関係者が集うプログラムであり、IDC Indonesia(データセンター)やAP JII、サーバー技術に関して Rainer、技術管理に関して Gunadarma 大学および ICT Watch、その他 Hivos やフォード財団の協力を得ている。

同プログラムの目的は、インドネシアの人々(非個人)が、有用・有益で面白いコンテンツを自発的に開発できる機会を提供することにある。その際、外部からの干渉をできるだけ抑えられるように、それぞれが表現の自由に責任をもつことを課している。

Kalam Kata のサーバー運用管理は、ICT Watch チームによって行われ、下記アドレスにコンタクト可能である。

support@ictwatch.com

参考資料・参考文献

- 1、Lawangpost 誌
- 2、Catatan-sakti ウェブサイト
- 3、Edmon Makarim., S.Kom., S.H., LL.M, Rancangan Undang-Undang Informasi dan Transaksi Elektronik (RUU-ITE), Depkominfo, 2008
- 4、Cahyana Ahmadjayadi, Peran e-Government Untuk Pelayanan Publik yang Lebih Baik, Depkominfo, 2003
- 5、I Wayan “Gendo” Suardana, UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dan Ancaman Terhadap Kebebasan Berekspresi, 2008
- 6、M Jafar Elly, Mengoptimalkan UU ITE, Republika 17 April 2008
- 7、Tempo 誌
- 8、法令:Undang Undang Nomor 11 Tahun 2008, tentang Informasi dan Transaksi Elektronik.
- 9、Cahyana Ahmadjayadi, Dirjen Aplikasi Telematika Depkominfo. Regulasi Konten dan kaitannya dengan UU ITE. Jakarta 11 Juni 2008.
- 10、 <http://insan.or.id>
- 11、 <http://www.apatika.kominfo.go.id>
- 12、 <http://www.nawala.org/>
- 13、 <http://www.ictwatch.com>
- 14、Politikindonesia 誌
- 15、 <http://www.awari.or.id>
- 16、 www.internetsehat.org
- 17、 <http://www.trustpositif.depkominfo.go.id/>
- 18、 <http://kalamkata.org/tentang-kalamkata/>
- 19、Detik.com
- 20、 <http://www.awari.or.id>
- 21、Republika 誌
- 22、Tekno Kompas 誌
- 23、Teknologi.vivanews 誌

インドネシアにおける青少年保護のためのインターネット規制と運用

2012年2月発行

著作・発行 日本貿易振興機構(ジェトロ) 海外調査部

〒107-6006 東京都港赤坂 1-12-32 アーク森ビル 6階

Copyright © 2012 JETRO. All rights reserved. 禁無断掲載