

《研究ノート》

ナイジェリア 2015年サイバー犯罪 防止法の概要(3)

岡田好史

目次

- 1 はじめに
- 2 2015年サイバー犯罪防止法の概要
- 3 2015年サイバー犯罪防止法 試訳
 - 第1章 目的と適用地
 - 第2章 国家情報基盤の保護
 - 第3章 違反行為と刑罰
 - 5条~20条(以上, 専修法学論集130号)
 - 21条~36条
 - 第4章 金融機関等の義務(以上, 専修法学論集131号)
 - 第5章 運用体制と執行
 - 第6章 逮捕, 搜索, 押収及び訴追
 - 第7章 管轄及び国際協力
 - 第8章 雑則別表
- 4 おわりに

3 2015年サイバー犯罪防止法 試訳

第5章 運用体制と執行

41. (1) 国家安全保障顧問事務局は、この法律に基づくすべての治安機関及び執行機関の調整機関とする。

- (a) ナイジェリアのサイバー犯罪を予防し対抗するために関連するすべての治安、情報、法執行機関、軍を支援する。
 - (b) 包括的なサイバーセキュリティ戦略とナイジェリアの全国サイバーセキュリティポリシーの策定と効果的な実施を確保する。
 - (c) ナイジェリアにおけるサイバーインシデントの管理を担当する国家コンピュータ緊急対応チーム（CERT）コーディネーションセンターを設置し、維持する。
 - (d) 国立コンピュータフォレンジック研究所を設立及び維持し、すべての法執行機関、治安機関及び情報機関による施設の利用を調整する。
 - (e) ナイジェリアのこの法律又はその他のサイバー犯罪に関する法律に基づき、関連するすべての治安、情報、法執行及び軍の機能の効果的な遂行能力を構築する。
 - (f) 官民パートナーシップ（PPP）のための適切なプラットフォームを確立する。
 - (g) ナイジェリアがサイバーセキュリティの国際連携に関与し、サイバーセキュリティに関する世界的枠組みに確実に統合されるよう調整する。及び
 - (h) この法律に基づき、関連する治安機関及び執行機関の機能の効果的な実施に必要なその他の行為又は事柄を行うこと。
- (2) 連邦法務長官は、次のことを確保するために既存の法的枠組みを強化し向上しなければならない。
- (a) ナイジェリアのサイバー犯罪及びサイバーセキュリティの法律及び政策が地域及び国際基準に適合していること
 - (b) サイバー犯罪の予防及び対抗並びにサイバーセキュリティの促進に必要な国際協力の維持、及び
 - (c) サイバー犯罪及びサイバーセキュリティ事案の効果的な訴追
- すべての法執行機関、治安機関及び情報機関は、この法律の規定の効果

的な実施のために必要な制度上の能力を開発し、国家安全保障顧問事務局と協力して、サイバー犯罪の禁止、予防、取調べ、捜査及び訴追の責任を負う役人ために国内的又は国際的にプログラマーの研修を開始、開発又は組織しなければならない。

42. (1) この法律の別表1に記載されている省庁の代理人からなるサイバー犯罪諮問会議（この法律では、以下「会議」と称する。）が設立される。

(2) 本条第1項により任命された代表者は、行政府の幹部職員又はそれと同等の者であってはならない。

(3) 会議の構成員は、

(a) その者が会議の構成員になったことにより役職が停止され、又

(b) 議長は、その者が会議の構成員として公職を継続することが公益にならないと確信している。

(4) 会議は、国家安全保障顧問によって主宰されるものとする。

(5) 会議は、1年に少なくとも4回、国家安全保障顧問により招集されるたびに行われるものとする。

43. (1) 会議は、次の事項を行わなければならない。

(a) 構成員が知識、経験、機密情報及び情報を定期的に共有するための環境を作り、サイバー犯罪を予防し、対抗し、サイバーセキュリティの促進に関する問題に関する勧告をナイジェリアで提供すること。

(b) この法律の規定の実施に関する一般的な政策指針を策定し提供すること。

(c) コンピュータ関連の犯罪、サイバー犯罪、国家的なサイバー空間への脅威、及びその他のサイバーセキュリティ関連の問題の予防及び対抗策に関して助言すること。

(d) 現実世界の環境において新しいサイバーセキュリティの防衛、技術、プロセスの開発を支援するサイバーセキュリティリサーチセンターを設立するための高等教育機関への助成金プログラムを創設すること。及び

(e) サイバーセキュリティ及びコンピュータセキュリティ並びにネットワークセキュリティの研究開発における大学卒業生の訓練手当を奨励すること。

(2) 会議は、会議の開催、通知、議事録の保管その他委員会が定める他の事項について随時決定する権限を有する。

44. (1) 国家サイバーセキュリティ基金（本法では「基金」と呼ぶ）と称する基金を設立する。

(2) 次のものは、ナイジェリア中央銀行に所在する本条第1項に基づいて設立された基金に拠出され、入金されるものとする。

(a) この法律の別表2において指定された事業によるすべての電子取引の0.005を徴収したもの。

(b) 寄贈者、二国間及び多国間機関からの援助及び無償資金援助。

(c) 寄贈品、寄付金、遺贈、個人や組織によるその他の募金により基金に発生したその他すべての金銭。ただし、これらの寄贈品、寄付金、遺贈又は寄付に付随する条件が、基金の機能を害することがない場合に限る。

(d) 国会が基金に充当することができる資金。及び

(e) 随時、基金に拠出する可能性があるその他すべての金銭又は資産。

(3) 基金に発生したすべての資金は所得税を免除され、基金へのすべての拠出は税額控除可能となる。

(4) 第2項a号に基づき課される徴収金額は、30日以内に、影響を受けた事業者又は組織により中央銀行に所在する基金に直接送金されるものとする。

(5) 基金の40%を超えない額は、暴力的過激主義に対抗するためのプログラムに配分することができる。

(6) ファンドの勘定及び記録について、

(a) 国家安全保障顧問事務局は、勘定の適切な記録を保持しなければならない。

(b) 基金の口座は、連邦政府の監査役が提供するガイドラインに従って監査されるものとする。

第6章 逮捕、搜索、押収及び訴追

45. (1) 法執行官は、関連する犯罪捜査において電子的証拠を得る目的で、令状を発行することを裁判所に一方的に申請できる。

(2) 裁判官は、法執行官に対し、次の権限を与える令状を発することができる。

(a) 敷地内に立入り、土地、建物又は乗物を搜索する

(i) この法律に基づく犯罪が行われている。又は

(ii) この法律に基づく犯罪が行われている証拠がある。又は

(iii) この法律に基づく犯罪がなされるのを防止することが緊急に必要である。

(b) 本条 a 号に基づき立入り、搜索の権限を与えられた権限のある公務員が、土地又は建物にある人又は乗物を搜索する。

(c) この法律に基づいて犯罪を行った証拠がある場合は、乗物を停止し、乗り込み、搜索する。

この法律に基づく犯罪を行った証拠を含む、又はそれを含むものを差し押さえ、押収し、拘留する。

(e) コンピュータシステム又はコンピュータネットワークに含まれる、若しくは利用可能なデータを検索するために、コンピュータ又はデバイスを使用又は使用させる。

(f) コンピュータに含まれるコード化されたデータ又は暗号化されたデータを解読又は解読する技術を使用して、判読可能なテキスト又は理解可能な形式にする。

(g) 本法に基づく違法行為に関して、コンピュータ又は電子機器を製造するために、コンピュータ又は電子機器の操作を担当し又は関係のある者を

必要とする。

(3) 裁判所は、本条第2項の下で令状を発するものとし、

(a) この法律に基づく犯罪を防止するため、又はこの法律に基づく捜査手続の妨害を防止するために、令状が求められている。又は

(b) 令状は、サイバー犯罪、サイバーセキュリティ違反、コンピュータ関連犯罪の捜査、又は電子的証拠の入手を目的としたものである。又は

(c) 調査中のサイバー犯罪又はコンピュータ関連の犯罪に関連している可能性があると信ずる合理的な根拠がある。又は

(d) 令状に記載された者が、この法律に基づく犯罪を行う準備をしている。

46. ナイジェリア連邦共和国憲法の規定に従うことを条件として、次の行為をした者は、2年間の懲役若しくは50万ナイラ以下の罰金又はその双方を併科する。

(a) この法律により与えられた権限の行使において、法執行官を故意に妨害する。又は

(b) 本法の規定に従い、法執行機関によって行われた合法的な照会又は要求に従わない。

47. 法務執行機関は、法務長官の権限に従うことを条件として、この法律に基づく犯罪を起訴する権限を有するものとする。この法律第19条及び第21条に基づく犯罪の場合、法務長官の承認は、起訴前に取得されなければならない。

48. (1) 裁判所は、この法律に基づく犯罪で有罪判決を受けた者に刑を科す場合、有罪判決を受けた者の次の物をナイジェリア連邦政府に没収するよう命令することができる。

(a) 有形又は無形の資産、金銭又は財産、そのような犯罪の追跡可能な収益、及び

(b) コンピュータ、設備、ソフトウェア、電子機器、又はそのような犯罪を遂行するため又は遂行を容易にするために使用又は使用される他の機器

(2) 有罪判決を受けた者が、外国において資産又は財産を有している場合、そのような資産又は財産がこの法律に挙げられた犯罪行為の結果として取得されたときは、外国との条約又は手続きを経て、ナイジェリア連邦政府に没収されなければならない。

(3) 連邦法務長官事務局は、没収された資産又は財産がナイジェリア連邦政府に有効に移転され帰属されることを確保しなければならない。

(4) 本法に基づく犯罪で有罪判決を受けた者は、国際旅券を取り消すものとする。外国人の場合、旅券は保留され、刑を執行した後、又はその者に課された罰金を支払った後にのみ返還される。

49. 裁判所は、この法律に基づいて科される罰金に加えて、本法に基づく犯罪で有罪判決を受けた者に、虚偽表示又は詐欺の被害者に対して、直接的に損害賠償を命じなければならない。

(a) 財産が金銭である場合、被害者が被った損害額に相当する金額を被害者に支払うこと。その他の場合には、

(i) 犠牲者又はその者が指名した人物に財産を返却する。又は

(ii) 財産の返還が不可能又は実行不可能な場合には、財産の価値に等しい金額を支払うこと。

(b) 民事訴訟における判決と同様の方法で、被害者又は被害者のために検察官によって賠償命令が実施されうる。

第7章 管轄及び国際協力

50. (1) 次の場合には、犯罪が行われた場所にかかわらずナイジェリアの連邦高等裁判所は、この法律に基づく犯罪についての管轄権を有するものとする。

(a) ナイジェリア国内において罪を犯した場合、又は

(b) ナイジェリアに登録された船舶又は航空機内において罪を犯した場合、又は

(c) ナイジェリアの市民又は居住者によるその行為が、行われた国の法律に基づいて犯罪を構成する場合、又は

(d) ナイジェリア国外において、

(i) 犯罪の被害者がナイジェリアの市民又は居住者である場合、又は

(ii) 被疑者はナイジェリア国内にいて、他の国から起訴されていない場合

(2) この法律に基づく犯罪の裁判において、被告人が次のものを所持していたならば、裁判所は審判において証人の証言を裏付ける証拠として検討することができる。

(a) 金銭的に十分に説明できない金融資産又は財産、又は

(b) その者の知られている収入源と不均衡な金融資産又は財産、又は

(c) 被疑犯罪の時又はその頃にその者が金融資産又は財産に接することがあったことを十分に説明できない金融資産又は財産

(3) 裁判所は、委員会がこれに先立って人、身体又は権限に対して提起したすべての事項を迅速に処理し、速やかな聴聞が行われることを確実にしなければならない。

(4) ナイジェリア連邦憲法の規定に従い、この法律に基づいて提起された刑事事件に関する手続の申し立ては、判決が下されるまで受け入れられないものとする。

51. この法律に基づく犯罪は、2004年ナイジェリア連邦法 CAP E25 身柄引渡し法に基づき身柄を引き渡されるものとする。

52. (1) 連邦法務長官は、この法律に基づく犯罪の捜査又は訴追において、外国当局に援助を要請し又は外国当局の援助を受けることができ、かつこの法律に基づく犯罪を検出し、防止し、対応し、訴追する目的で行われた共同捜査又は協力を認可又は参加することができる。

(2) ナイジェリアと要請国又は被要請国との間に二国間又は多国間の合意が存在するか否かにかかわらず、第1項にいう共同捜査又は協力を行う

ことができる。

(3) 連邦法務長官は、事前の要請がなくても、捜査中に得た情報が犯罪捜査又はこの法律に基づく犯人の逮捕に役立つ場合には、外国の管轄機関に送付することができる。

53. (1) この法律による請求に基づき、収集された証拠が、外国の裁判所における捜査又は手続において立証された場合には、この法律が適用される手続においても明白に認容されるものとする。

(2) 本条第1項の目的のために、次の場合に証拠は認容される。

- (a) 外国の裁判官、治安判事又は公証人により認定された、又は
- (b) 証人の誓約又は宣誓による誓約、次の公式の印又は公印によって封印されている

(i) 外国政府の省庁又は部局

(ii) 外国領土、保護領若しくは植民地及び外国領土、保護領若しくは植民地の政府を管轄する者又はその領土、保護領若しくは植民地の部局

54. (1) この法律に基づく請求は、その請求をした者により又はその者の代理人により書面で、日付が記され、かつ署名されているものとする。

(2) 請求は、ファクシミリ若しくはその他の電子機器又は方法により送信することができ、かつ以下を含むものとする。

- (a) 捜査、訴追又は手続を行う当局の名称
- (b) 事件に関連する特定の犯罪、訴訟で到達した段階、及び更なる訴訟の日程を含む、捜査、訴追又は訴訟の主題、争点及び種類の記述
- (c) 求められる証拠、情報その他の援助の記述、及び
- (d) 証拠、情報その他の援助が求められている目的の陳述

(3) 必要かつ可能な範囲で、請求には次のものも含まれなければならない。

- (a) 証拠を求める者の身元及び所在地に関する情報
- (b) 提供される者の身元及び所在地、捜査、訴追又は手続に対するその者

との関係、及び提供方法に関する情報

- (c) 居場所を見つげられた者の身元と所在に関する情報
- (d) 搜索される場所又は人物及び押収される物品の正確な記述
- (e) その国の認容性に関する証拠の採取方法についての要請国法の特別の要件を含む証言又は供述の録取方法の記述
- (f) 証人になされた質問のリスト
- (g) 要求を実行する際に従わなければならない特定の手順の記述
- (h) その請求に関連して請求国において請求された者に権利が与えられる手当及び経費に関する情報
- (i) 裁判所からの命令又はもしあれば、その命令が最終的に実行されたという認証謄本及び陳述書
- (j) 請求された国の要請に応じることができるその他の情報

(4) 連邦法務長官が請求を実行するのに十分な法令順守があることを確認した場合、この法律の目的上、請求又は訴訟手続は本条第2項の規定の遵守を怠ったことにより無効とされてはならない。

(5) 連邦法務長官は、国際的な協定が必要とするか又は公益上の理由により、適切であると判断した場合、この法律に基づいて没収された財産の全部又は一部を請求国に返還又は送金することができる。

55. (1) ナイジェリアは、コンピュータシステム又はネットワークに格納された電子機器又はデータの保存を、本法又はその他の法律に記載されている犯罪について、これらのデータの搜索、差押え、開示のための援助要請の提出に応じて速やかに行うよう要請することができる。

(2) 本条第1項に基づく請求は、次の事項を明記しなければならない。

- (a) 保存又は開示を請求する当局
- (b) 犯罪が捜査され又は起訴されたこと、及びそれらに関する事実の簡単な説明
- (c) 保持される電子機器又はコンピュータデータと犯罪との関係

(d) 電子機器又はデータの責任者若しくはコンピュータシステムの所在地を特定するために利用可能なすべての情報

(e) 保存措置の必要性, 及び

(f) データの検索, 押収及び開示のための援助要請を提出する意思

(3) 連邦法務長官は, 前項の規定に基づいて外国当局の請求を行うにあたり, サービス提供者を含むそのようなデータの管理又は入手可能な者に対し, それらを保存し又は適切な機関又は人に適切な保存をさせることを命ずることができる。

(4) 本条第3項の規定を害することなく, 保存は, この法律の規定を実行する責任がある法執行機関によっても要求され, 緊急性があるか又は遅延のおそれがある場合には, 裁判所の命令に従い, 一方的にその命令を得ることができる。

(5) 裁判所が本条第4項の規定に従って命令を認める場合, その命令は, 以下の事項を示すものとする。

(a) 証拠の性質

(b) 既知の場合には, その起源と目的地及び

(c) データを保存しなければならない期間として90日以内の範囲の期間

(6) 保存命令に従い, サービス提供者を含むそのようなデータの管理又は入手可能な者は, 指定された期間のデータを直ちに保存し, その完全性を保護し維持するものとする。

(7) 電子的な証拠又はデータの迅速な保存の請求は, その後の検索, 差押え, 及び公開のための法的援助の請求の執行が拒否されると信ずる合理的な理由がある場合, 拒否されることがある。

56. (1) 国家安全保障顧問事務局は, この法律に基づく国際協力の目的で直ちに援助を提供するために, 24時間365日間有効な連絡先を指定し維持するものとする。

(2) この連絡先は, ナイジェリアが拘束されている協定, 契約, 条約又

は国際司法機関若しくは法執行機関との協力手続に従い、他の連絡先から到達することができるものとする。

- (3) 連絡先が提供する即時援助には、以下を含めるものとする。
- (a) 他の連絡先への技術的助言
 - (b) 緊急性があるか又は遅延のおそれがある場合の証拠の迅速な保存
 - (c) 緊急性があるか又は遅延のおそれがある場合に法的権限を有する証拠の収集
 - (d) 緊急性があるか又は遅延のおそれがある場合に被疑者の捜査及び法的情報の提供
 - (e) 本条第3項b号及びd号で示された措置に関する要請の速やかな伝達

第8章 雑則

57. (1) 連邦法務長官は、この法律の規定の効率的な実施に必要な命令、規則、ガイドライン又は規則を発することができる。

(2) 本条第1項に基づく命令、規則、ガイドライン又は規定は、以下のために定めることができる。

- (a) この法律により逮捕された被疑者のビデオ及びその他の電子記録の保管方法
- (b) サイバーセキュリティ及びサイバー犯罪に関する国際機関によって発行された規則又は慣行の遵守方法
- (c) 凍結、凍結解除、凍結した資金その他の資産へのアクセス手続き
- (d) 資産の差押え、没収及び処分の手続き
- (e) 司法共助
- (f) 国内及び国際人権基準に沿ったすべてのサイバー犯罪事件の訴追手続き
- (g) 刑罰及び訴追を含む、本法案に規定される徴収の迅速な支払いを確保

するための手続き、及び

(h) 法務長官がこの法律の実施のために必要又は適切とみなすその他の事項

58. この法律において

「アクセス」とは、コンピュータシステム又はネットワークの論理演算又はメモリ機能のリソースへのエントリ、命令又は通信を得ることを意味する。

「アクセス機器」とは、電子カードを含む以下のものを意味する。

- (a) デビットカード
- (b) クレジットカード
- (c) 掛売りカード
- (d) ポイントカード
- (e) 磁気ストライプカード
- (f) IC カード
- (g) EMV 方式 IC カード
- (h) パスワード
- (i) 個人識別番号 (PIN)
 - (i) 電子基板
 - (ii) 電子シリアル番号
 - (iii) コード番号
 - (iv) モバイル識別番号
 - (v) アカウント番号、その他の電気通信サービス、機器、機器識別子又は電話、携帯情報端末〔PDA〕等を含むその他アカウントへのアクセス手段
 - (vi) 現金自動預払機
 - (vii) 販売時点情報管理端末
 - (viii) その他の自動販売機

「ATM」とは、現金自動預払機を意味する。

「権限あるアクセス」とは、次の場合に、ある者にコンピュータに保持されているプログラム又はデータへのアクセス権限があることをいうものとする。

- (a) その者に、問題のプログラム又はデータへのアクセスを制御する権利がある。又は
- (b) 承諾を与えることができる者が、そのプログラム又はデータにアクセスすることをその者に承諾している。

「権限ある製造業者」とは、制定法に基づきカードを作成する権限を与えられた金融機関又はその他の人を意味する。

「権限ある公務員又は権限ある人」とは、コンピュータ犯罪及びサイバーセキュリティ上の脅威の禁止、予防、排除又は対抗に関与する法執行機関の構成員又はその委託を受けた者を意味する。

「銀行カード」とは、銀行サービスカード、キャッシュカード、小切手保証カード若しくはデビットカード、又は商品、役務、その他価値のあるものを得るためにカード名義人が使用するための発行者から手数料の有無にかかわらず発行される若しくは機器を介して提供される金銭又は役務を得るために自動預払い装置で使用される類似の名称で知られている文書、トークン、機器又はカードを意味する。

「カード」とは、キャッシュカード、クレジットカード、又は支払機能付きカードを意味する。

「カード名義人」とは、カード発行者によって発行され、キャッシュカード、クレジットカード又は支払機能付きカードにより利益を得るそのようなカードの表面に記載されている者をいう。

「カード製造装置」とは、カード、偽造カード又はカードの外観若しくは構成要素を製造するために設計、使用、又は使用することができるあらゆる装置、機械、基板、機構、刻印又はその他の装置を意味する。

「コンピュータ」とは、論理演算処理又は記憶機能を実行する電子的、磁氣的、光学的、電氣化学的又はその他の高速データ処理機器及びデータ記憶機能を含む機器を意味し、通信プロトコルを介してコンピュータと直接インターフェースすることができるすべての通信機器は、この定義の一部を形成するものとする。なお、この定義には、携帯型手持ち式電卓、タイプライター及び植字機又はその他同様の機器類を含むものとする。

「コンピュータデータ」は、コンピュータユーザが実行しているプログラムに関連付けられたテキストファイル又はその他のファイルのような、コンピュータユーザが必要とする情報を格納し、プログラムを実行し、実行するためにコンピュータが必要とする情報を含むあらゆる情報を含むものとする。

「コンピュータプログラム」又は「プログラム」とは、コンピュータで特定のタスクを実行又は実行するために書かれた一連の命令を意味する。「コンピュータシステム」とは、プログラムに従って、データの自動化又は対話型処理を実行する1つ又は複数の、相互接続された、又は関連する機器若しくは機器のグループを指すものとし、コンピュータや携帯電話等のデータ処理機能を備えたあらゆる種類の機器が含まれるが、これらに限定されるものではない。ハードウェア及びソフトウェアとからなる機器は、独立していても、ネットワーク又はその他同様の機器に接続されている入力、出力及び記憶コンポーネントを含んでいてもよく、また、コンピュータのデータ記憶装置又はメディアも含まれる。

「消費者」とは、コンピュータサービス事業者並びに顧客及び消費者の代理人とコンピュータベースの購入、リース移管、保守及びコンサルタントサービス契約を締結するすべての人又は組織を意味し、金融カードを持っている銀行口座の名義人も含むものとする。

「コンテンツデータ」とは、通信セッション中に送信された実際の情報又はメッセージを意味する。

「偽造カード」とは、架空の若しくは変造又は偽造されたキャッシュカード、クレジットカード又は支払用カードを意味し、そのようなカードの複製又は虚偽表示、偽装又は構成要素又は盗難カード、不正使用のスキームの一部として入手されたカード又は違法に取得されたカードを含み、口座情報又は発行者情報がエンボス加工されているものとされていない場合もあるものを含むものとする。

「暴力的過激主義（CVE）対策」には、暴力行為の発生率を減らし、暴力的過激主義者の行動を変えるために、暴力的先鋭化に固執することに対抗し、中核的な国家価値を奨励しつつ、否定的な極端な集団に対抗するための介入、すなわち、先鋭化の根本原因（社会的、文化的、宗教的、経済的）を特定し、解決策を提供する戦略を開発するプログラム及び潜在的な新兵の態度や認識を変える措置を導入し、受刑者の職業訓練や持続可能な生計手段の提供、改心した過激派の家族や地域社会への再統合を含むものである。

「クレジット」には、現金貸付又はその他の財務情報を含むものとする。

「クレジットカード」とは、買掛側から商品、役務、その他の価値あるものをクレジットで取得する際にカード名義人が使用するために発行者による手数料の有無にかかわらず発行され、又は自動バンキング機器で使用して、機器を介して提供される金銭又は任意の役務を取得する、掛け売りカード又はその他同様の名前で知られているかどうかにかかわらず、あらゆる文書、トークン、機器又はカードを意味するものとする。

「買掛側」とは、商品、役務、その他価値のあるものを提供することに同意するか、カード発行者が承認し、商品、役務、又は価値のあるものをカード名義人に供給するためのキャッシュカード、クレジットカード、支払用カードの使用による支払いを受け入れる個人又は企業を意味するものとする。

「重要基盤」とは、そのシステムや資産の破壊が国の安全保障、国家経

済安全保障、国家公衆衛生安全に影響を及ぼす国にとって非常に重要なシステムと資産を意味するものとする。

「偽造アクセス機器」とは、模造の、架空の、変造の若しくは偽造のアクセス機器又は偽造されたアクセス機器の特定可能な構成要素を意味するものとする。

「ネットワーク上の付きまとい行為」とは、合理的に人に恐怖を感じさせる特定の人に向けられた行為をいうものとする。

「ドメイン名等不正取得行為」とは、利益を得る、誤解を招く、評判を害する、他人の登録を拒絶させる不正の意図で、インターネット上で次のような場合にドメイン名を取得することをいう。

- (i) ドメイン名登録時に、適切な政府機関に登録されている既存の商標と類似、同一又は混同を惹起する
- (ii) 個人名の場合には、登録者以外の者の名前と同一又は混同惹起する、及び
- (iii) 権利又は知的財産権を持たずに取得しようとする

「損害」とは、コンピュータ又はデータ、プログラム、システムの完全性若しくは可用性又は以下の情報の障害を意味するものとする。

- (i) 財政的損失を引き起こすこと、又は
- (ii) 1人又は複数人の健康診断、診断、治療又はケアを変更又は損害するか、又は潜在的に変更又は損害すること、又は
- (iii) 人に身体的傷害又は死亡を引き起こすこと又は脅かすこと、又は
- (iv) 公衆衛生又は公衆の安全を脅かすこと

「データ」とは、コンピュータで使用するのに適した形式で準備されている又は準備されてきた情報若しくは概念の表現を意味するものとする。

「データベース」とは、データへの簡単なアクセス、管理、更新を可能にする1つ又は複数の目的のために、デジタルで組織されたデータの収集を意味するものとする。

「機器」とは、特定の仕事をを行うように設計されたか、又は機械的若しくは電氣的動作がマイクロプロセッサによって制御又は監視されるように設計された物又は装置を意味するものとする。

「電子コミュニケーション」とは、電子的形式、インスタントメッセージ、ショートメッセージサービス (SMS)、電子メール、ビデオ、ボイスメール、マルチメディアメッセージサービス (MMS)、ファクシミリ、及びポケットベルによる通信を含むものとする。

「電子機器」とは、その目的を電子的に達成する機器を意味し、コンピュータシステム、電気通信機器、スマートフォン、アクセスカード、クレジットカード、デビットカード、ポイントカードなどを含むものとする。

「電子的記録」とは、情報システムにおいて電子的、磁氣的、光学的又はその他の手段によって生成、伝達、受信、又は保存された記録又はある情報システムから別の情報システムへ伝送するための記録をいうものとする。

「資金の電子的移転」とは、指示、承認又は命令により、銀行が電子的手段を用いてその銀行で維持されている口座から借方記入又は借方記入するために、人によって開始された資金の移転を意味し、販売時点の移動、現金自動預払機による取引、直接預金又は資金の引き出し、電話、インターネット及びカード決済による振替を含むものとする。

「期限切れのカード」とは、表示された期限が切れたために有効ではなくなったカードを意味するものとする。

「金融機関」には、ファクタリングプロジェクト、ファイナンス設備リース、債務管理、ファンドマネジメント、プライベート帳簿サービス、投資管理、現地購入注文資金調達、輸出金融、プロジェクトコンサルタント、金融コンサルタント、年金基金管理、保険機関、負債の差押え、ディーラー、決算及び清算会社、法律実務家、ホテル、カジノ、外貨両替所、スーパーマーケット及び中央銀行又は適切な監督当局が適宜指定するその他の

事業を含む法人であれ非法人であれ、個人、団体、組合又は個人の集団を含むものとする。

「金融取引」とは、(a)いかなる形であれ、電信又はその他の電子的手段による資金の移動を伴う取引であり、(b)1つ以上の貨幣調達手段を含み、(c)不動産又は動産への小所有権の移転を伴う。取引を意味するものとする。「機能」には、コンピュータに対する論理、制御、演算、削除、記憶、検索、通信又は電気通信を含むものとする。

「個人同定情報の窃用」とは、電子的な取引を介して商品や役務を入手するために、他人の個人情報を盗むことを意味するものとする。

「基盤端末」には、銀行その他の機微情報にアクセスするために使用することができる携帯電話、POS 端末、及び現在使用されているか将来導入される可能性のある他のすべてのカードアクセプタ機器を含むものとする。

「通信傍受」には、コンピュータシステム又は通信ネットワークの機能に関連して、コンピュータの通信データを聴取又は記録すること、又はこれらの機能のいずれかを遮断又は防止することができるそのような行為の実態、意味又は目的を取得することを含むものとする。

「発行者」には、中央銀行により承認された支払い用カードを発行する権限を有する金融機関又はその他の事業体を含むものとする。

「法執行機関」には、この法律の規定の実施及び執行を担当する機関を含むものとする。

「長官」とは、連邦法務長官をいうものとする。

「変更」とは、コンピュータシステム又はネットワーク内のデータの削除、劣化、改変、制限又は隠滅を意味し、コンピュータシステムからのデータ転送を含むものとする。

「ネットワーク」とは、リソース及び情報の共有を可能にする通信チャネルによって相互接続されたハードウェアコンポーネント及びコンピュー

タの集合を意味するものとする。

「支払い用カード」とは、商品、役務又はその他の価値のあるものを取得する際にカード名義人の使用に当たり、定められた金銭的価値をエンコードし、発行者が手数料の有無にかかわらず発行する文書、トークン、機器又はカードを意味するものとする。

「人」には、個人、団体、企業又は人の集団を含むものとする。

「大統領」とは、ナイジェリア連邦共和国軍司令官であるナイジェリア連邦共和国大統領を意味するものとする。

「フィッシング」とは、ユーザーの銀行から送られた電子メールの形で、電子メール又はインスタントメッセージによる電子通信における信頼を偽装することによって、ユーザーに自分のパスワードを変更させたり、その情報を後でユーザーに不正をしったりするために使用される、ユーザー名、パスワード、クレジットカードの詳細などの機微情報を取得しようとする犯罪及び詐欺行為を意味するものとする。

「不正作出された電子的手段による購入」とは、クレジットカード、デビットカード、ICカード、ATM又はその他の関連電子決済システム用機器などのようなクレジット／デビットの移し替え手段によるものをいう。

「交付」とは、信頼の裏付けとしてカードの占有権、所有権、支配権を取得し又はカードを受け取ることを意味するものとする。

「失効カード」とは、カード発行者又はカード名義人の請求にかかわらず、それを使用する許可が発行者によって中断又は中止されたためにもはや有効ではないカードを意味するものとする。

「サービス事業者」とは、次のものを意味するものとする。

(i) コンピュータシステム、電子通信機器、モバイルネットワークを使用して通信する能力を、そのサービスの利用者に提供する公共又は民間企業、及び

(ii) 通信サービス又はそのようなサービスの利用者に代わってコンピュ

ータデータを処理又は保存する組織体

「性的に露骨な行為」には、少なくとも以下の实在又は模擬的の行為を含むものとする。

- (a) 性器同士、口腔性交、肛門性交（肛門と性器又は口腔による性交）、児童間又は成人と児童の間、同性又は異性間での性交
- (b) 猥姦
- (c) 自慰行為
- (d) 性的状況におけるサディズム又はマゾヒズムの濫用又は
- (e) 实在のものであるか否かを問わず、児童の性器又は陰部の煽情的な展示すること

「迷惑メール送信行為」とは、個人及び法人に無差別に大量のメッセージを送信する電子メッセージシステムの濫用をいうものとする。

「取引」とは、財産の販売、譲渡、頒布、分配、又はその他の方法で処分すること又は財産の購入、受領、所有、支配権の獲得又は財産の売却、譲渡、頒布、分配その他の処分を目的として、又は使用することを意味するものとする。

「トラフィックデータ」とは、送信元、宛先、経路、時間、日付、サイズ、継続時間、又は基礎となるサービスのタイプを示す一連の通信の一部を形成するコンピュータシステムによって生成された、コンピュータシステム又はネットワークによる通信に関する任意のコンピュータデータを意味するものとする。

59. この法律は、2015年のサイバー犯罪（禁止、防止等）法として引用することができる。

別表 1

[42条関係]

サイバー犯罪諮問会議の構成員

(1) サイバー犯罪諮問会議は、次の各省庁、部局、機関の代表者により構成されるものとする。

- (a) 連邦司法省
- (b) 連邦財務省
- (c) 外務省
- (d) 連邦貿易投資省
- (e) ナイジェリア中央銀行
- (f) 国家安全保障顧問事務局
- (g) 国務省
- (h) ナイジェリア警察
- (i) 経済及び金融犯罪委員会¹
- (j) 独立汚職防止委員会²
- (k) 国家情報機関
- (l) ナイジェリアの安全保障及び民間防衛隊³
- (m) 国防諜報局
- (n) 国防司令部
- (o) 人身取引防止庁
- (p) ナイジェリア税関
- (q) ナイジェリア入国管理局
- (r) 国立宇宙管理局
- (s) ナイジェリア情報通信技術開発庁
- (t) ナイジェリア通信委員会
- (u) ギャラクシーバックボーン社⁴
- (v) 個人番号管理委員会⁵

- (w) ナイジェリア矯正局
- (x) 以下の代表者
 - (i) ナイジェリア電気通信事業者協会
 - (ii) ナイジェリアインターネットサービスプロバイダー協会
 - (iii) ナイジェリア銀行委員会
 - (iv) ナイジェリア保険協会
 - (v) ナイジェリア証券取引所
 - (vi) サイバーセキュリティに重点を置く非政府組織
- (2) サイバー犯罪諮問評議会は、長官が連邦官報の公告による通知により本別表第1条の表に追加することができるその他の省庁、機関、機関の代表者を含むものとする。

別表2

第44条第2項a号にいう事業は次のとおりとする。

- (a) 携帯電話事業者及びすべての電気通信事業者
- (b) インターネット接続事業者
- (c) 銀行その他の金融機関
- (d) 保険会社
- (e) ナイジェリア証券取引所

4 おわりに

情報通信技術の進展と共に、サイバー空間では次々と新たなサービスや技術が現れており、その利便性が向上している反面、これらを悪用したサイバー犯罪・サイバー攻撃の手口も日々新たなものが現れている。

サイバー犯罪をめぐる問題は、コンピュータ及びコンピュータネットワークに関わる問題だけに、技術に対する依存度が極めて高いため、必然的

に技術的対応を検討し、進めていく必要がある。また、技術の進展の早さゆえに行政上の対応は遅れがちであることから、法的手段を講じるよりも技術的対応による解決が可能かつ適切な場合も少なくない。

その一方で、情報化社会を主体的に生きていくために、情報倫理の視点をもって克服していくことが大事なものとなる。すなわち、我々自身が生活者としての立場で、セキュリティの問題に対し関心を持ち、利用者に対する教育、啓発による人的対策も進めて行く必要がある。

さらに、発生した場合の損害や影響の大きさなどから、近年社会問題化し、時には国際的な時事問題にまで発展するものであるから、単純な技術的対策以上に、より広い立場からの対応として、その法的対応、とりわけ加害行為に対する刑事法的対応を検討する必要がある。

サイバー空間の脅威に対処するためには、総合的な対策が求められている。とりわけ、法執行機関の対処能力の強化だけでは限界があり、行政機関と民間事業者との連携が不可欠なものとなる。

サイバー犯罪として何を扱うか、手続きをどうするか、官民連携のあり方、被害者の救済のあり方等、諸外国の取り組みが参考になることもあろうかと思う。今後も引き続き検討を続けていきたい。

注

- 1 2004年経済及び金融犯罪委員会（EFCC）制定法により設立された法執行機関である。詐欺や資金洗浄等の金融犯罪、経済犯罪等の捜査を行い、適切な場合には経済犯罪をした者を起訴する。資金洗浄とテロリストの資金調達に対する世界的な取り組みを国内において調整し、国際基準に対応させる機関でもある。
- 2 2000年汚職及び関連犯罪法に基づき発足した法執行機関である。汚職の報告を受けて捜査し、適切な場合には汚職をした者を起訴し、汚職をなくすために、汚職の起きやすいシステムや公共機関の手続の是正を検討し、実施すること、汚職の排除について国民の支持を得、醸成するために、汚職や関連する犯罪について市民を教育し、啓発することにある。
- 3 内戦時に爆弾を避ける方法等を住民に指導すること等を目的として1967年5月に設立されたラゴス民間防衛委員会を母体として、2003年ナイジェリアの安全保障及び民間防衛隊（NSCDC）法により設立された準軍組織である。NSCDCの主

な任務は、ナイジェリア警察と協力して人命と財産を保護すること等であり、2007年改正法により権限が強化され、民間警備会社の活動の監督及び監視、自然災害や人的緊急事態時の被災者の救助及び避難活動等を行っている。

- 4 2006年に設立された公開有限責任会社であり、ナイジェリアにおいて公共及び民間部門向けの統一された情報通信技術基盤プラットフォームを構築し、運用している。
- 5 2007年個人番号管理委員会(NIMC)法により制定された、国の個人番号管理システムを運用する組織である。個人番号カード・データベースの作成、運用及び管理、既存の個人番号データベースの政府機関への統合、個人及び法人の登録、固有の識別番号の割り当て、多目的カードの発行等を行っている。