《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（1）

岡　田　好　史

目　次

1　はじめに

コンピュータの出現は，コンピュータ犯罪という新しいタイプの犯罪を生み出し，さらに，コンピュータ・ネットワークやICT（Information and Communication Technology）の進展は，コンピュータ犯罪をサイバー犯

罪へと進化させた。犯罪及び犯罪的な行為の成立についてコンピュータ及びコンピュータ・ネットワークの存在を必要とするコンピュータ犯罪，サイバー犯罪[1]は，伝統的犯罪[2]と比べて，その巧妙さ，狡猾さ，継続性や反復性の点において事件一件当たりの被害額，その範囲は比べ物にならないほど大きく，社会の注目を集めやすくなっている。

社会のコンピュータ化が進み，我々の社会の中にICTが取り入れられ，個々のコンピュータ端末のみならずIoT（Internet of Things）[3]により，あらゆるモノがネットワーク端末の一翼を担うようになったことで，コンピュータやコンピュータ・ネットワークは，もはや社会インフラ化し，ユビキタス・コンピューティング（ubiquitous computing）[4]社会が実現しようとしつつある。我々の社会においてコンピュータ及びコンピュータ・ネットワークが重要な位置を占めるようになったことで，コンピュータ及びコンピュータ・ネットワークを利用した不正加害行為いわゆる「サイバー犯罪」から社会における秩序を維持するための法的対応は，刑事立法及び刑事法学の重要な課題の一つとなってきた。

サイバー犯罪は急速に拡大しており，多くの犯罪者がインターネットのスピード，利便性，匿名性を利用して，物理的または仮想的な境界を越えてさまざまな犯罪行為を行っている。サイバー犯罪は，コンピュータ及びコンピュータ・ネットワークの特性を利用して，数秒で電子メールを送信し，誰にでもWWW（World Wide Web）[5]を介して情報をすばやく公開し，配布することができる。ネットワークへの参入障壁が下がったことで，サイバー犯罪は，地理的位置に関係なく世界のどこからでもなされる可能性がある。また，これらの犯罪行為は，インターネットを使用することによって，より迅速に，より簡単に，より多くの損害を生じさせる可能性もある。

消費者や投資家が損失を被ると，被害を受けた人や組織に対する信頼を大きく損ない，それらへの負のイメージを生み出すことになる。そのため，

多くの国ではサイバー犯罪に関連する脅威を予防，検出，防止するための戦略を策定し，サイバー犯罪対策のさまざまな立法がみられるところである[6]。

アフリカ最大の経済を誇るとされる[7]ナイジェリア連邦共和国は，いわゆる「419詐欺」（419 scam）[8]を中心としたサイバー犯罪の根拠地とされたことから，サイバー犯罪対策の立法について検討を続け[9]，2015年にようやくナイジェリア連邦法「サイバー犯罪防止」（Cybercrimes（Prohibition, Prevention, Etc）Act, 2015）が成立した。本稿では，この新しい立法が我が国におけるサイバー犯罪対策立法を検討する上での示唆ともなりうると考え，紹介するものである。

2　サイバー犯罪防止法の概要

⑴「サイバー犯罪」の内容

サイバー犯罪防止法は，ナイジェリアにおけるサイバー犯罪の禁止，予防，捜査，訴追及び処罰のための効果的かつ統一された法的枠組みを提供し，重要な国家の情報基盤の保護を確保し，サイバーセキュリティ，コンピュータシステム及びネットワーク通信，データ及びコンピュータプログラムの知的財産権及びプライバシー権を含む電気通信の保護を促進することを目的としている（法1条）。

同法に「サイバー犯罪」の定義規定は置かれていないが，次の行為を犯罪とし，罰則を規定している。重要インフラに対する罪，コンピュータへの不正アクセス，インターネットカフェの不正利用，システム妨害，電子メッセージの不正傍受，電子メッセージを用いた誤誘導，コンピュータデータの不正作出，コンピュータ関連の詐欺，電子署名に対する罪，サイバーテロ，個人同定情報の窃用となりすまし，児童ポルノ関連犯罪，ネット上の付きまとい行為（Cyberstalking），ドメイン名等の不正取得行為（Cybersquatting），人種差別及び憎悪犯罪，フィッシング（Phishing）行

為，コンピュータウイルスの拡散，電子式カードに関連する詐欺，電子メール及びウェブサイトの濫用等である（５条～36条）。

⑵　金融機関及びインターネット接続事業者の責務

金融機関に対しては，氏名・住所及びその他の関連情報を記載した本人確認書類による電子金融取引を行う顧客の身元確認義務が課せられた（40条１項）。さらに，顧客口座に不正請求が行われた際には，顧客の書面による通知を受けて引き落としの許可を与えるか，さもなければ72時間以内に引き落としを取り消さなければならない。72時間以内にその口座の引き落としを止められなかった金融機関は，500万ナイラの罰金に処され，引き落としにより生じた負債を弁済する義務を負う（40条３項）。

インターネット接続事業者には，関係当局が規定するすべてのトラフィック[10]データ[11]及び加入者情報の保管が義務付けられた（41条１項）。また，法執行機関等の要請に応じて，保管するトラフィックデータ，加入者情報若しくは関連コンテンツを公開しなければならず，公開義務を負うとされた（同３項）。

法執行機関の要請を受けて接続事業者が保持，処理または検索したデータは，この法律その他の法律，規則，又は管轄権を有する裁判所の命令に基づいて提供される場合を除き，利用されないものとされ（同４項），法執行の目的のために本条に定められた職務を行う者は，連邦憲法に基づく個人のプライバシー権を尊重し，データの機密性を保護するための適切な措置を講ずるものとされた（同５項）。なお，41条に違反した者又は団体には，３年以上の懲役若しくは700万ナイラ以上の罰金，又はこれを併科される。

⑶　協議機関の設置

41条１項において，国家安全保障顧問事務局（Office of the National

Security Adviser）が，サイバー犯罪対策のために関連するすべてのセキュリティ，情報，法執行機関，軍事サービスを支援するとともに，すべての治安機関及び執行機関の調整機関とされた。同機関ではまた，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土の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ことが求められ，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コーディネーションセンターや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，治安機関及び諜報機関による施設の利用を調整することとされた。さらに，官民パートナーシップのための適切なプラットフォームの確立や国際的なサイバーセキュリティの協力に関与し，サイバーセキュリティに関する世界的枠組みに適合するよう調整することとされた。

そして，すべての法執行機関，治安機関及び諜報機関は，この法律の規定の効果的な実施のために必要な制度面での能力を開発し，国家安全保障顧問事務局と協力して，国内外におけるホワイトハッカーの養成，サイバー犯罪の禁止，予防，検出，捜査及び訴追の責任を負う公務員の養成が求められることとなった。

国家安全保障顧問の下では，知識，経験，情報等を定期的に共有するための環境を作り，サイバー犯罪を防止し，サイバーセキュリティの促進に関する勧告を行う機関として，連邦司法省，連邦財務省，外務省，連邦貿易投資省，ナイジェリア中央銀行，国家安全保障顧問事務局，国務省，ナイジェリア警察，経済犯罪委員会，国家情報機関，防衛諜報局，税関，移民局，通信委員会，インターネット接続事業者協会等からなるサイバー犯罪諮問委員会（Cybercrime Advisory Council）が設置された（42条，43条）。

3　2015年サイバー犯罪防止法　試訳

目　次

59. 引用
別表

１．この法律は，以下のことを目的とする。
(a)　ナイジェリアにおけるサイバー犯罪の禁止，予防，捜査，訴追，処罰のための効果的かつ統一された法的，監督上及び制度上の枠組みを提供すること
(b)　重要な国家情報基盤の保護を確保すること，及び
(c)　サイバーセキュリティ並びにコンピュータシステムコンピュータ・システム及びネットワーク，データ及びコンピュータプログラム，知的財産及びプライバシー権を含む電子通信の保護を促進すること
２．この法律は，ナイジェリア連邦共和国において罪を犯したすべての者に適用する。
３．(1)　大統領は，国家安全保障顧問の勧告に基づき，連邦官報に掲載された命令により，コンピュータプログラム，コンピュータデータないしトラフィックデータを問わず，物理的又は仮想的，ないしわが国にとって不可欠なシステム及び資産の喪失又は破壊または妨害が，治安，国家又は経済の安全保障，国民の健康と安全，又は重要な国家情報基盤を構成するものとしてのそのような事項の任意の組み合わせへの影響を弱めるであろう特定の重要なコンピュータシステムないしネットワークを指定することができる。
(2)　第１項に基づく大統領令は，以下に関連する最低限の基準，指針，規則によりなされうる。
(a)　重要な情報基盤の保護又は維持
(b)　重要な情報基盤の一般的な管理
(c)　重要な情報基盤におけるデータへのアクセス，転送，及び管理
(d)　重要な国家情報基盤に含まれるデータ又は情報の完全性と真正性を

保証するための基盤又は手続きの規則と要件

(e)　重要な国家情報基盤とみなされるデータ又は情報の記憶先又はアーカイブ先

(f)　災害発生時又は重要な国家情報基盤全部又は一部喪失時における復旧計画，及び

(g)　重要な国家情報基盤におけるデータ及びその他の資源の適切な保護，管理，管理に必要なその他の事項

4．前条に定める大統領令は，この法律の規定を遵守するために，あらゆる重要な国家情報基盤の監査と検査を国家安全保障顧問事務局に随時要求することができる。

5．重要な国家情報基盤に対する犯罪

(1)　本法第3条により指定された重要な国家の情報基盤に対して，この法律に定められた罪を犯した者は，懲役10年以上に処する。

(2)　前項に基づく罪を犯し，よって人を傷害した者は，15年以下の懲役に処する。

(3)　本条第1項に基づく罪を犯し，よって人を死亡させた者は，死刑に処する。

6．(1)　権限なく，故意に不正の目的で，コンピュータシステム又はネットワークの全部又は一部にアクセスをし，国家安全保障にとって不可欠なデータを入手した者は，5年以上の懲役若しくは500万ナイラ以上の罰金に処し，又はこれを併科する。

(2)　前項の行為が，コンピュータデータの入手，プログラム又は営業秘密若しくは機密情報へのアクセスの確保を目的として行われたときは，7年以上の懲役若しくは700万ナイラ以上の罰金に処し，又はこれを併科する。

(3)　本条の罪を犯す意図で，機器を使用して検出を回避し，若しくはその他の方法により，作為又は不作為で同定を妨げたときは，7年以上の懲

役若しくは700万ナイラ以上の罰金に処し，又はこれを併科する。

⑷　法律上の権限なく，コンピュータにアクセスすることが可能なパスワード又は同様の情報を故意に不正取引した個人又は組織は，そのような取引がナイジェリア連邦内外の公的，私的，個人的な利益に影響を及ぼした場合，700万ナイラ以下の罰金若しくは３年以下の懲役，又はこれを併科する。

７．インターネットカフェの規制

⑴　本法施行の後，全てのインターネットカフェ運営者は，企業行動委員会への商号登録に加えて，コンピュータ専門家登録審議会に事業を登録するものとする。インターネットカフェはサインイン登録簿を通じてユーザー登録を確保するものとする。この登録簿は，必要なときにいつでも法執行官が利用できるものとする。

⑵　インターネットカフェを利用して電子詐欺またはオンライン詐欺をした者は，懲役３年若しくは100万ナイラの罰金，又はこれを併科する。

⑶　インターネットカフェの所有者が〔前項の行為を〕黙認したことが明らかになったときは，懲役３年若しくは200万ナイラの罰金に処し，又はこれを併科する。

⑷　前項の黙認の証明の負担は，検察官に課すものとする。

８．法的な権限なく，故意又は不正の目的で，コンピュータデータの入力，送信，毀損，削除，劣化，改変又は隠滅することにより，直接的又は間接的にコンピュータシステムの機能に沿うべき動作をさせず，又は使用目的に反する動作をさせた者は，２年以上の懲役また若しくは500万ナイラ以上の罰金に処し，又はこれを併科する。

９．金銭ないし貴重な情報が伝達されている電子メール又はプロセスを，正当な理由なく破棄若しくは強制中止した者は，懲役７年に処す。ただし再犯の場合には，懲役14年に処す。

10．本法施行後，ナイジェリアの地方政府，民間組織又は金融機関に勤務

している者が，重要基盤ないし電子メールの扱いに関して，権限なく業務契約上行うことが許されていない行為をしたとき，又はそのようにコンピュータを改変したときは，懲役3年若しくは200万ナイラの罰金に処する。

11. 不法の利益を得る意図，若しくは作為又は不作為によりメッセージの重要部分を無効化させるためにメッセージを遅らせるか早める処理を妨害する意図で，電子メッセージを誤った宛先に送った者は，懲役3年若しくは100万ナイラの罰金に処し，又はこれを併科する。

12.（1） 故意に，権限なく，技術的手段により，電磁放射若しくは信号を伝送若しくは送信するコンピュータ，コンピュータシステム又はネットワークからの信号を含む，コンピュータシステム，又は接続されたシステム若しくはネットワークとの間の，非公開のコンピュータデータ，コンテンツ，又はトラフィックデータの通信を傍受した者は，2年以上の懲役若しくは500万ナイラ以上の罰金に処し，又はこれを併科する。

（2） 虚偽の口実を用いて，ナイジェリア連邦，州又は地方政府に勤務している者又はその組織を，明らかに重要ではない電子メール，クレジットカード及びデビットカードの情報，ファクシミリのメッセージを含むがこれに限定されない電子メッセージで誘導した者，又は（組織においてメッセージを受け取る権限を有する）電子機器担当者にメッセージを送信した者は，懲役2年若しくは100万ナイラ以下の罰金に処し，又はこれを併科する。

（3） ナイジェリア連邦，州，地方当局若しくは民間組織に勤務している者が，その者が入手したか，又はその者に誤って届けられ，かつ他の者に届けられるはずであった電子メール，メッセージ，電子決済，クレジットカード及びデビットカードを故意に隠匿し又は引き渡さなかったときは，懲役1年若しくは25万ナイラの罰金に処し，又はこれを併科する。

13. コンピュータ又はネットワークに故意にアクセスし，データが直接読

み書き可能であるかどうかにかかわらず，不正なデータを真正なものであるかのように処理の用に供させる目的で，不正なデータとなるデータを入力し，変更し，削除し，又は隠滅した者は，３年以上の懲役若しくは700万ナイラ以上の罰金に処し，又はこれを併科する。

14.⑴　経済上の利益を得る目的の有無を問わず，故意に，権限なく又は権限を超えて，コンピュータに保持されたデータを変更し，消去し，入力し，若しくは隠滅した者は，３年以上の懲役若しくは700万ナイラ以上の罰金に処し，又はこれを併科する。

⑵　欺く意図で受信者に電子的なメッセージを送信し，その電子的なメッセージが事実又は一連の事実を大きく誤って伝えたことで，受信者又はその他の者に損害又は損失を生じさせた者は，５年以上の懲役若しくは1000万ナイラ以上の罰金に処し，又はこれを併科する。

⑶　詐く意図で，電子的なメッセージや指示を送信し，又は電子的なメッセージや指示を上書きしたは，３年以下の懲役若しくは500万ナイラ以下の罰金に処し，又はこれを併科する。

⑷　公共又は民間部門に勤務している者が，詐く意図で，コンピュータシステム又はその他の電子決済機器を操作して，給与支払を短縮させ又は過払いさせようとし，若しくは実際に短縮させ又は過払いさせたときは，７年以下の懲役に処し，銀行，金融機関又は顧客に対し，領得された金銭又は財産の所有権を喪失するものとする。

⒜　銀行その他の金融機関に勤務している者が，直接的又は間接的に電子メールを流用したときは，懲役５年若しくは700万ナイラ以下の罰金に処し，又はこれを併科する。

⒝　４項に定める罪を犯し，銀行，金融機関ないし顧客に重大ないし財政上の損失をもたらした者は，懲役７年に処すのに加え，領得した金銭若しくは銀行，金融機関又は顧客に転換された財産は没収されるものとする。

⑸　金融機関の従業員が，コンピュータシステム又はネットワークを使

用して詐欺行為を行うために他の者又は集団と共謀したときは，7年以下の懲役に処し，領得した金銭を返還させるか，又は銀行，金融機関，若しくは顧客に転換された財産を没収しなければならない。

15.（a） 金融機関または公的基盤の端末を窃取した者は，懲役3年若しくは100万ナイラの罰金に処し，又はこれを併科する。

（b） ATM（現金自動預け払い機）を窃取した者は，7年以下の懲役若しくは1,000万ナイラ以下の罰金に処し，これを併科する。窃取された収益は，ATMの正当な所有者のために没収されるものとする。

（c） ATMの窃盗の未遂は，1年以下の懲役若しくは100万ナイラ以下の罰金に処し，又はこれを併科する。

16.（1） 権限なく直接的又は間接的にコンピュータシステムに保持されているデータを不正に改変した者は，3年以上の懲役または700万ナイラ以上の罰金に処し，又はこれを併科する。

（2） 本条において，コンピュータシステム又はネットワークに保持されているデータの改変とは，コンピュータ，コンピュータシステム，又はネットワークに関するあらゆる機能の動作により，以下のことが生ずる場合をいう。

（a） そこに保持されているプログラム又はデータを変更又は消去すること。

（b） そこに保持されているプログラム又はデータに，プログラム又はデータを追加又は削除すること。

（c） 権限あるユーザーのデータ又は機能の可用性を妨げ若しくは終わらせるためにプログラム又はデータを隠匿すること。若しくは

（d） 関係するコンピュータ，コンピュータシステム又はネットワークの正常な動作を損なう行為を生じさせること。

（3） 正当な権限なく，故意に，コンピュータデータの入力，送信，損壊，削除，劣化，改変，隠匿，又はその他の方法で，直接的又は間接的にコン

ピュータシステムの機能に沿うべき動作をさせず，又は使用目的に反する動作をさせた者は，２年以上の懲役若しくは500万ナイラ以上の罰金に処し，又はこれを併科する。

17.（1）(a)　商品の購入その他の取引に関する電子署名は拘束力を有するものとする。

（b）　署名に疑義があるときは，署名の真正性の証明は，相手側が負担するものとする。

（c）　不正使用又は作出の意図で，電子機器を通じて人の署名又は会社の委任状を不正に作り出した者は７年以下の懲役若しくは1000万ナイラ以下の罰金に処し，又はこれを併科する。

（2）　以下は，電子署名により有効である契約又は告知の類型から除外されるものとする。

（a）　遺言，遺言補足書ないしその他の遺言証書の作成及び執行

（b）　死亡診断書

（c）　出生証明書

（d）　結婚，離婚，養子縁組などの家族法に関する書類

（e）　裁判所命令，告知書，宣誓供述書，嘆願書，召喚状及びその他の関連する司法文書並びに証書などの公式の裁判所の書類の発行

（f）　公益事業の取り消しまたは終了

（g）　自然状態で固体または液体の危険物の運搬または取扱いに伴い必要な証書

（h）　偽造品ないし人や環境に危険なものであることを理由として，薬物，化学物質，その他の物の使用中止命令を発する権限を与えられた当局により使用中止を命ぜられた文書，又は失効させられた文書

18.（1）　テロ行為の目的でコンピュータ若しくはコンピュータシステム又はネットワークにアクセスし，若しくはアクセスさせた者は，終身刑に処する。

（2）　本条における「テロ行為」とは，改正2011年テロ（防止）法における意味と同一のものとする[12]。

19.（1）　この法律の施行後，金融機関は，従業員1人のみを〔コンピュータに〕アクセスするために配置し，アクセスを許可してはならない。

（2）　従業員にコンピュータへのアクセスを許可した者及び複数のアクセス権を付与した者は，懲役7年若しくは100万ナイラの罰金，又はこれを併科する。

（3）　金融機関は，顧客に対し，保護必要情報を保護するための効果的な不正行為対策を講じる義務を負うものとする。ただし，セキュリティ上の違反が生じた場合，問題の金融機関がその情報の完全性を保護するためにさらに多くのことができたという過失の証明は顧客側が負うものとする。

20.　金融機関の許可を得て，貸借の転記，電子貸借メッセージの送信に関連する電子命令の発行又は電子資金送金の確認義務を負うような電子命令の発行等の金融取引のためにコンピュータその他の電子機器を使用する責任を負う者が，違法に，人を欺く意図で真正ではない電子メールや口頭のメッセージを発したときは，懲役7年に処する。

注

1　サイバー犯罪の定義については，拙稿「サイバー刑法の概念と展望」専修大学法学論集118号（2013年）63頁以下参照。

2　犯罪ではない行為とははっきり識別できる行為としての犯罪，「それが悪であるということに特別の説明」を要しない，「しかも，その悪の範囲がどのようなものであるかについても，厳密な定義づけを必要としない」行為とされる（藤木英雄「現代型犯罪と刑事政策」犯罪と非行20号（1974年）138頁）。

3　1999年に無線 ID タグの専門家であるケビン・アシュトンが初めてこの語を使ったとされる。情報通信機器に限らず，あらゆるモノに通信機能を持たせることにより，インターネットに接続することで，経由で情報のやりとりを行うことをいう。

IoT については，さしあたり，坂村健『IoT とは何か　技術革新から社会革新へ』角川学芸出版（2016年），畠中信敏編著『IoT 時代のセキュリティと品質―ダークネットの脅威と脆弱性』日科技連出版（2017年）等参照のこと。

4　生活や社会の至る所にコンピュータが存在し，コンピュータ同士が自律的に連

携して動作することにより，人間の生活を強力にバックアップする情報環境をいう。1989年にXerox社のパロアルト研究所が提唱した概念であるが，携帯電話などを中心とした小型情報端末の進化に代表されるコンピュータの小型化や，インターネットの爆発的な普及などの通信技術の発展・浸透に伴って，再び注目が集まりつつある。ユビキタス・コンピューティングにおいては，コンピュータはその存在を意識させることなく，必要に応じてネットワークに蓄積された個人情報などを参照しながら，自動的に他のコンピュータと連携して処理を行う。ユビキタス・コンピューティングの研究から生まれた技術としては，VICS（Vehicle Information and Communication System）情報やGPS（Global Positioning System）と連動した経路探索・周辺情報探索を行うカーナビゲーションシステムや，衣服と一体化することにより「身にまとう」ことができるウェアラブルコンピュータなどがある。

なお，ユビキタス・コンピューティングについては，さしあたり，Simone Rescio & Roberto Maieli, Ubiquitous Computing（2011），Paul Dourish & Genevieve Bell, Divining a Digital Future: Mess and Mythology in Ubiquitous Computing（2011），Fabian K. Ppen, Ubiquitous Computing（2007），坂村健『ユビキタスとは何か―情報・技術・人間』岩波書店（2007年）等参照のこと。

5　1989年に欧州核物理学研究所（CERN）のティム・バーナーズ・リーが所内の論文公開・閲覧システムとして考案したものが基礎となっている。インターネットが一般に開放され普及していく過程で，インターネット上で標準的に用いられている，文書の公開・閲覧システムとなり，電子メールなどと共にネットの中心的な応用システムとして広く利用されるようになった。文書内に別の文書への参照を埋め込むことができる「ハイパーテキスト」と呼ばれるシステムにより，文字や画像，動画などを一体化した文書をネット上で公開・配布したり，また，それを入手・閲覧することができたりする。大規模なハイパーテキストの文書間の繋がりを図示すると複雑な蜘蛛の巣のように見えることからWorld Wide Webと呼ばれる。

6　我が国では，サイバー犯罪に対処するための規定形式としては，1987（昭和62）年6及び2001（平成13）年，2011（平成23）年に追加・改正された刑法各条のほか，個別的な特別刑法によってきた。たとえば，「不正アクセス行為の禁止等に関する法律」，「電子署名及び認証業務に関する法律」，「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律」，「児童買春，児童ポルノに係る行為等の処罰及び児童の保護等に関する法律」，「特定電子メールの送信の適正化等に関する法律」が制定され，「電波法」，「電気通信事業法」，「不正競争防止法」，「著作権法」等において，コンピュータ及びコンピュータ・ネットワークの普及に伴う新たな刑事規制を導入している。

7　*See,"Nigeria becomes Africa's largest economy"*〈http://www.aljazeera.com/news

/africa/2014/04/nigeria-becomes-africa-largest-economy-20144618190520102. html〉, *"Nigerian Economy Overtakes South Africa's on Rebased GDP"*〈https://www.bloomberg. com/news/articles/2014-04-06/nigerian-economy-overtakes-south-africa-s-on-rebased-gdp〉（2017年5月1日確認）

8　原型は，裕福な囚人を監獄から釈放するには金が要るが，その金がないので貸してくれれば後日返済すると持ちかけて金品を騙し取る「スペインの囚人」と呼ばれる詐欺の手法である。1980年代半ばから，ナイジェリアから先進国を狙った手紙やファックスを使い「スペインの囚人」の手口を応用した国際的な詐欺事件がおこったことから「ナイジェリアからの手紙」（Nigerian money transfer fraud, Nigerian scam）とも呼ばれるようになった。「419詐欺」と呼ばれるのは，この種の手口がマネーロンダリングを規制するナイジェリア連邦刑法419条に抵触することに由来している。現在では電子メールの発達にともない，もっぱら電子メールを悪用したものが主流となっており，詐欺の実行者側も組織化され，汎用マルウェアを使って企業を狙った攻撃を行っているといわれる。

なお，手口については，日本貿易振興機構のウェブサイトの紹介に詳しい（「419詐欺について」〈https://www.jetro.go.jp/contact/faq/419case.html〉（2017年5月1日確認））。

9　2004年にはサイバー犯罪ワーキンググループによるサイバー犯罪法案が，2006年にはコンピュータセキュリティ法案が提出された。2009年から2010年には，ネット詐欺防止法案を含む10種類以上の法案が提出されたがいずれも成立をみなかった。

10　通信回線やネットワーク上で送受信される信号やデータのことや，通信回線上で一定時間内に転送されるその量や密度のことをいう。デジタルデータを細かい単位に分割して送受信する回線や機器では，ある期間に流入・処理するデータ量や，それを単位時間あたりに換算したものをトラフィックとすることが多い。また，Web サーバや Web サイトへの外部からの接続要求数，アクセス数，送信データ量などのことや，サイトやページの間を行き来する閲覧者の流れのことをトラフィックということもある。

11　サイバー犯罪防止法は，58条においてトラフィックデータを定義している。そこでは，「トラフィックデータ」を，「通信の発信元，宛先，経路，時間，日付，サイズ，継続時間，または基本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る，コンピュータシステムまたはネットワークを用いた通信に関連するコンピュータデータを意味する」ものとしている。

12　2011年テロ（防止）法（Terrorism（Prevention）Act. 2011）1条2項参照。