事件番号　平成２６年特(わ)第９２７号，刑(わ)第２３７３号，第２５６４号，第２９４２号，第３２６５号，平成２７年刑(わ)第４９０号，第９３４号，特(わ)第１４１１号，第１５５８号，第１６７０号

事　件　名　不正アクセス行為の禁止等に関する法律違反，電子計算機使用詐欺，私電磁的記録不正作出・同供用，不正指令電磁的記録供用，電波法違反被告事件

宣　告　日　平成２９年４月２７日

宣告裁判所　東京地方裁判所刑事第１６部

主　　文

被告人を懲役８年に処する。

未決勾留日数中７００日をその刑に算入する。

押収してある無線接続機器１式（平成２８年押第２５号符号１）を没収する。

本件公訴事実中，平成２７年７月１日付け追起訴状記載の公訴事実第１の電波法違反の点については，被告人は無罪。

理　　由

（罪となるべき事実）

第１（平成２６年１０月２２日付け追起訴状記載の公訴事実第１の関係）

被告人は

１　不正アクセス行為の用に供する目的で，インターネットバンキングサービス「Ａダイレクト」のアクセス管理者である株式会社Ａ銀行（以下「Ａ銀行」という。）になりすまし，同サービスの利用権者に対して同サービスのアクセス制御機能を有する特定電子計算機を特定利用するために付された識別符号の入力を促す「Ａダイレクト」と題するインターネット上のウェブサイトを「(省略)」が管理するサーバコンピュータ内に蔵置させた上，平成２６年２月２０日（以下，本文中の月日の記載は平成２６年のそれを示す。）午前３時２分頃，松山市

ab 丁目 c 番 d 号被告人方（以下「被告人方」という。）において，パーソナルコンピュータを使用して，茨城県つくば市 ef 番地 g 号（省略）ビル２階所在のＢ株式会社（以下「Ｂ」という。）事務所内に設置されたパーソナルコンピュータにＡ銀行からの通知を装って同サイトの閲覧を促す電子メールを送信し，同日午前８時３０分頃，同メールを閲覧したＢ従業員φをして，同メールがＡ銀行からのものであり，かつ，同サイトがＡ銀行の掲載によるものと誤認させ，よって，その頃，同人に同サイトを閲覧させてＡ銀行に開設されたＢ名義の通常貯金口座のお客様番号，ログインパスワード，インターネット用暗証番号等の識別符号を同サイト上に入力させることにより，同識別符号が記録された電子メールを被告人管理のメールアドレス宛に自動送信させ，これをＣ株式会社が管理する東京都千代田区 hi 丁目 j 番 k 号（省略）ビル内設置のメールサーバコンピュータに蔵置させて，これを閲読し得る状態にし，もってアクセス制御機能に係る他人の識別符号を取得し

２　他人の識別符号を使用して不正アクセス行為をしようと考え，法定の除外事由がないのに，別表１記載のとおり（別表１は省略），２月２０日午前１１時３７分頃から同月２１日午前９時２０分頃までの間，３回にわたり，被告人方において，パーソナルコンピュータを使用し，電気通信回線を通じて，Ａ銀行が千葉県印西市内に設置したアクセス制御機能を有する特定電子計算機である認証サーバコンピュータに，第１の１記載のとおり取得したＢを利用権者として付された識別符号を入力し，同サーバコンピュータを作動させて前記アクセス制御機能により制限されている特定利用をし得る状態にさせ，もって不正アクセス行為をした。

第２（訴因変更後の平成２６年１０月２２日付け追起訴状記載の公訴事実第２の関係）

被告人は，別表１の番号３の不正アクセス行為による第１の２の状態を利用し，Ａ銀行の事務処理を誤らせる目的で，２月２１日午前９時２２分頃，被告

人方において，パーソナルコンピュータを使用して，電気通信回線を通じ，Ａ銀行が同市内に設置した前記サーバコンピュータに，Ｂによって登録されていたメールアドレス「k-……@…….co.jp」が「gy……@…….co.jp」に変更された旨の虚偽の情報を送信し，同サーバコンピュータに記憶させ，もって人の事務処理の用に供する事実証明に関する電磁的記録を不正に作出するとともに，Ａ銀行の事務処理の用に供した。

第３（平成２６年１１月２７日付け追起訴状記載の公訴事実の関係）

被告人は，別表１の番号３の不正アクセス行為による第１の２の状態を利用し，前記「Ａダイレクト」に虚偽の情報を与えて，不実の電磁的記録を作り，財産上不法の利益を得ようと考え，別表２記載のとおり（別表２は省略），２月２１日午前９時２３分頃，２回にわたり，被告人方において，パーソナルコンピュータを使用し，電気通信回線を通じて，Ａ銀行が神戸市内に設置し，同銀行の貯金の残高管理，受入れ，払戻し等の事務処理に使用する電子計算機に対し，Ｂ名義の通常貯金口座から，被告人が第三者をして管理させていた同銀行に開設されたＤ名義の通常貯金口座に合計８７万円の振込送金があったという虚偽の情報を与え，同銀行が神戸市内に設置した前記電子計算機に前記Ｄ名義の通常貯金口座の残高を８７万円増加させて財産権の得喪・変更に係る不実の電磁的記録を作り，よって，８７万円相当の財産上不法の利益を得た。

第４（訴因変更後の平成２６年７月２日付け起訴状記載の公訴事実の関係）

被告人は

１　不正アクセス行為の用に供する目的で，第１記載のインターネットバンキングサービス「Ａダイレクト」のアクセス管理者であるＡ銀行になりすまし，第１の１同様に「Ａダイレクト」と題するインターネット上のウェブサイトを「(省略)」が管理するサーバコンピュータ内に蔵置させた上，２月２６日午前１１時５分頃，被告人方において，パーソナルコンピュータを使用して，埼玉県戸田市 lm 丁目 n 番 o 号所在の株式会社Ｅ（以下「Ｅ」という。）事務所内に

設置されたパーソナルコンピュータにＡ銀行からの通知を装って同サイトの閲覧を促す電子メールを送信し，同日午前１１時１１分頃，同メールを閲覧したＥ従業員χをして，同メールがＡ銀行からのものであり，かつ，同サイトがＡ銀行の掲載によるものと誤認させ，よって，その頃，同人に同サイトを閲覧させてＡ銀行に開設されたＥ名義の通常貯金口座のお客様番号，ログインパスワード，インターネット用暗証番号等の識別符号を同サイト上に入力させることにより，同識別符号が記録された電子メールを被告人管理のメールアドレス宛に自動送信させ，これをＣ株式会社が管理する第１の１記載の（省略）ビル内設置のメールサーバコンピュータに蔵置させて，これを閲読し得る状態にし，もってアクセス制御機能に係る他人の識別符号を取得し

２　他人の識別符号を使用して不正アクセス行為をしようと考え，法定の除外事由がないのに，別表３記載のとおり（別表３は省略），２月２６日午前１１時４６分頃から同日午後０時３４分頃までの間，３回にわたり，被告人方において，パーソナルコンピュータを使用し，電気通信回線を通じて，Ａ銀行が千葉県印西市内に設置した第１の２記載のサーバコンピュータに，第４の１記載のとおり取得したＥを利用権者として付された識別符号を入力し，同サーバコンピュータを作動させて前記アクセス制御機能により制限されている特定利用をし得る状態にさせ，もって不正アクセス行為をした。

第５（平成２６年１０月１日付け追起訴状記載の公訴事実の関係）

被告人は，別表３の番号２の不正アクセス行為による第４の２の状態を利用し，第１記載のインターネットバンキングサービス「Ａダイレクト」に虚偽の情報を与えて，不実の電磁的記録を作り，財産上不法の利益を得ようと考え，２月２６日午後０時１４分頃，被告人方において，パーソナルコンピュータを使用し，電気通信回線を通じて，Ａ銀行が神戸市内に設置し，同銀行の貯金の残高管理，受入れ，払戻し等の事務処理に使用する前記電子計算機に対し，Ｅ名義の通常貯金口座から，全国銀行データ通信システムを介して，あらかじめ

Ｆから使用の承諾を得ていた株式会社己銀行庚支店に開設されたＦ名義の普通預金口座に９万６０００円の振込送金があったという虚偽の情報を与え，同銀行が横浜市ｐ区ｑ町ｒ番地ｓｕセンターに設置した電子計算機に前記Ｆ名義の普通預金口座の残高を９万６０００円増加させて財産権の得喪・変更に係る不実の電磁的記録を作り，よって，９万６０００円相当の財産上不法の利益を得た。

第６（平成２７年３月９日付け追起訴状記載の公訴事実第１の関係）

被告人は，他人の識別符号を使用して不正アクセス行為をしようと考え，法定の除外事由がないのに，別表４記載のとおり（別表４は省略），３月２７日午後７時７分頃から同月２８日午前１０時１３分頃までの間，２回にわたり，被告人方において，パーソナルコンピュータを使用し，電気通信回線を通じて，株式会社Ｇ銀行（以下「Ｇ銀行」という。）が東京都港区ｔｕ丁目ｖ番ｗ号（省略）ビルに設置したアクセス制御機能を有する特定電子計算機である認証サーバコンピュータに，有限会社Ｈ（以下「Ｈ」という。）を利用権者として付された識別符号を入力し，同サーバコンピュータを作動させて前記アクセス制御機能により制限されている特定利用をし得る状態にさせ，もって不正アクセス行為をした。

第７（平成２７年３月９日付け追起訴状記載の公訴事実第２の関係）

被告人は，別表４の番号２の不正アクセス行為による第６の状態を利用し，ＨがＧ銀行と締結していたインターネットバンキングサービスである「Ｇ銀行ビジネスダイレクト」に虚偽の情報を与えて，不実の電磁的記録を作り，財産上不法の利益を得ようと考え，３月２８日午前１０時２３分頃，被告人方において，パーソナルコンピュータを使用し，電気通信回線を通じて，Ｇ銀行が千葉県印西市内に設置し，同銀行の預金の残高管理，受入れ，払戻し等の事務処理に使用する電子計算機に対し，Ｈ名義の普通預金口座から，全国銀行データ通信システムを介して，被告人が第三者をして管理させていた辛信用金庫壬支

店に開設されたＩ名義の普通預金口座に２００万円の振込送金があったという虚偽の情報を与え，同信用金庫が神戸市ｘ区ｙ町ｚ丁目ａ番ｂ号αセンターに設置した電子計算機にＩ名義の普通預金口座の残高を２００万円増加させて財産権の得喪・変更に係る不実の電磁的記録を作り，よって，２００万円相当の財産上不法の利益を得た。

第８（平成２７年７月２２日付け追起訴状記載の公訴事実の関係）

被告人は,法定の除外事由がないのに,別表５記載のとおり(別表５は省略)，５月９日午前３時５９分頃から同月１５日午後２時１６分頃までの間，１８２万１２３３回にわたり，被告人方において，パーソナルコンピュータを使用し，電気通信回線を通じて，東京都豊島区cd丁目ｅ番ｆ号（省略）に設置されたＪ株式会社（以下「Ｊ」という。）が管理するアクセス制御機能を有する特定電子計算機であるサーバコンピュータに，当該アクセス制御機能による特定利用の制限を免れることができる指令を入力し，前記特定電子計算機を作動させて，前記アクセス制御機能により制限されている特定利用をし得る状態にさせ，もって不正アクセス行為をした。

第９（平成２７年４月２４日付け追起訴状記載の公訴事実第１の関係）

被告人は，他人の識別符号を使用して不正アクセス行為をしようと考え，法定の除外事由がないのに，別表６記載のとおり（別表６は省略），５月１５日午前０時３０分頃から同月１９日午後０時４９分頃までの間，７回にわたり，被告人方において，パーソナルコンピュータを使用し，電気通信回線を通じて，株式会社Ｋ銀行（以下「Ｋ銀行」という。）が千葉市ｇ区内に設置したアクセス制御機能を有する特定電子計算機である認証サーバコンピュータに，株式会社Ｌ（以下「Ｌ」という。）を利用権者として付された識別符号を入力し，同サーバコンピュータを作動させて前記アクセス制御機能により制限されている特定利用をし得る状態にさせ，もって不正アクセス行為をした。

第１０（平成２７年４月２４日付け追起訴状記載の公訴事実第２の関係）

被告人は，別表６の番号６及び７の不正アクセス行為による第９の状態を利用し，Ｋ銀行の事務処理を誤らせる目的で，別表７記載のとおり（別表７は省略），５月１９日午後０時４６分頃から同日午後０時５５分頃までの間，３回にわたり，被告人方において，パーソナルコンピュータを使用して，電気通信回線を通じ，Ｋ銀行が千葉市ｇ区内に設置した前記サーバコンピュータに，Ｌが使用する電子メールアドレス等の虚偽の情報を送信し，同サーバコンピュータに記憶させ，もって人の事務処理の用に供する事実証明に関する電磁的記録を不正に作出するとともに，Ｋ銀行の事務処理の用に供した。

第１１（平成２７年４月２４日付け追起訴状記載の公訴事実第３の関係）

被告人は，別表６の番号７の不正アクセス行為による第９の状態を利用し，ＬがＫ銀行と締結していたインターネットバンキングサービスである「(省略)」に虚偽の情報を与えて，不実の電磁的記録を作り，財産上不法の利益を得ようと考え，別表８記載のとおり（別表８は省略），５月１９日午後０時５３分頃から同日午後０時５７分頃までの間，２回にわたり，被告人方において，パーソナルコンピュータを使用し，電気通信回線を通じて，Ｋ銀行が大阪市ｈ区内に設置し，同銀行の預金の残高管理，受入れ，払戻し等の事務処理に使用する電子計算機に対し，Ｌ名義の普通預金口座から，全国銀行データ通信システムを介して，被告人が第三者をして管理させていた辛信用金庫癸支店に開設されたＭ名義の普通預金口座ほか１口座に合計２２２万７０００円の振込送金があったという虚偽の情報を与え，神戸市ｘ区ｙ町ｚ丁目ａ番ｂ号αセンターほか１か所に設置した各金融機関の電子計算機にＭ名義の普通預金口座ほか１口座の残高を合計２２２万７０００円増加させて財産権の得喪・変更に係る不実の電磁的記録を作り，よって，合計２２２万７０００円相当の財産上不法の利益を得た。

第１２（平成２６年１２月２４日付け追起訴状記載の公訴事実の関係）

被告人は，有限会社Ｎ（以下「Ｎ」という。）名義の金融機関口座で使用され

るインターネット用暗証番号等の情報を入手しようと考え，６月３日午後１時２６分頃，被告人方において，パーソナルコンピュータを使用して，電気通信回線に接続されたパーソナルコンピュータ内で起動すると自動的に電気通信回線を介して被告人使用のパーソナルコンピュータとの通信を開始させるとともにＩＰアドレス情報等を同パーソナルコンピュータに通知する機能及び同パーソナルコンピュータでの操作によって起動場所であるパーソナルコンピュータ内の電磁的情報を検索して被告人使用のパーソナルコンピュータに送信させる機能等を有するプログラム「決済情報 8.exe」を添付した「ご注文決済のお知らせ」と題する電子メールを，電気通信回線を介してＮが管理するメールアドレス「re……@…….co.jp」宛てに送信して，これをＣ株式会社が管理する前記（省略）ビル内設置のメールサーバコンピュータに蔵置させ，同日午後１時５０分頃，東京都武蔵野市ij丁目k番l号（省略）所在のＮ事務所内において，事情を知らないφに同所設置のパーソナルコンピュータで同電子メールを受信させて，前記プログラム「決済情報 8.exe」を同パーソナルコンピュータ上で実行可能な状態にし，もって正当な理由がないのに，人が電子計算機を使用するに際してその意図に反する動作をさせるべき不正な指令を与える電磁的記録を人の電子計算機における実行の用に供した。

第１３（平成２７年８月７日付け追起訴状記載の公訴事実の関係）

被告人は，他人の識別符号を使用して不正アクセス行為をしようと考え，法定の除外事由がないのに，６月１０日午後１１時４３分頃，被告人方において，パーソナルコンピュータを使用し，電気通信回線を通じて，Ｐ銀行株式会社が東京都千代田区内に設置したアクセス制御機能を有する特定電子計算機である認証サーバコンピュータに，Ｏ株式会社（以下「Ｏ」という。）を利用権者として付された識別符号を入力し，同サーバコンピュータを作動させて，前記アクセス制御機能により制限されている特定利用をし得る状態にさせ，もって不正アクセス行為をした。

第１４（平成２７年７月１日付け追起訴状記載の公訴事実第２の関係）

被告人は，総務大臣の免許を受けず，かつ，法定の除外事由がないのに，６月１１日午前１１時２８分頃，被告人方において，無線設備（型番「(省略)」。平成２８年押第２５号符号１）を設置して，無線局として運用可能な状態に置き，もって無線局を開設した。

（第１ないし第１４の事実認定の補足説明）

第１　争点

１　第１ないし第３の事実（Ｂ事件という。），第４及び第５の事実（Ｅ事件という。），第６及び第７の事実（Ｈ事件という。），第８の事実（Ｊ事件という。），第９ないし第１１の事実（Ｌ事件という。），第１２の事実（Ｎ事件という。），第１３の事実（Ｏ事件という。）のそれぞれについて，被告人と犯人との同一性が争点である。すなわち，検察官は，各事件は被告人が使用していた押収品番号１番のパーソナルコンピュータ（１号パソコンという。）から行われたものである上，被告人以外の第三者による１号パソコンの操作の可能性はないから，被告人が犯人であると主張する。他方，弁護人は，各事件が１号パソコンから行われたことの立証が不十分である上，１号パソコンは第三者により操作されていた可能性があることなどから，被告人は犯人ではなく，無罪であると主張する。

２　第１４の事実の争点は，被告人の故意の有無である。すなわち，検察官は，被告人がインターネットオークションで無線ＬＡＮアダプタを購入した際に，画面上に，それを国内で使用すれば電波法違反となる旨の記載があったことなどから，被告人は，その無線ＬＡＮアダプタの使用が日本国内では違法とされていることを認識していたと主張する。他方，弁護人は，（省略）という型番のチップセットが使われている無線ＬＡＮアダプタか否かに被告人の関心があったため，被告人は電波法に抵触する性質を備えた機器であるという注意書きを見ることなく，その無線ＬＡＮアダプタを購入して使用するに至ったこと等

から，被告人に日本国内での使用が違法であるとの認識はなかったと主張する。

3　当裁判所は，第１ないし第１３の事実について，被告人が犯人であり，第１４の事実について，被告人に故意があったと認定したので，その理由について説明する。

第２　前提となる事実

1　１号パソコンの使用

１号パソコンは，被告人が１月３０日に購入したものである。被告人方では，被告人以外の家族が１号パソコンを使用することはなかった。

2　ウイルスに感染した会社のメールアドレス等が保存されていたこと

押収品番号５番のパソコン（５号パソコンという。）の「ζ.csv」内と，押収品番号６番の外付けハードディスク（６号外付けハードディスクという。）内の「η.csv」のファイル内に，Ｂ，Ｅ，Ｈ，Ｌ，β（Ｏ）のメールアドレス等の情報が保存されていた。

3　被告人が１号パソコンからＱ方無線ＬＡＮのＷＥＰ鍵を取得したこと

(1)　認定できる事実

警察官は，６月１１日午前１１時２８分から被告人方の捜索を実施した。押収された１号パソコンのデスクトップ上にあった暗号化ファイル「メモ.atc」を復号すると作成される「メモ.txt」内に，被告人方の真向かいにあるＱ方の無線ＬＡＮに接続するためのＷＥＰ鍵が保存されていた。

「メモ.atc」の復号パスワードは，「ma……」であった。

その取得経緯は，次のとおりと認められる。すなわち，被告人は，１号パソコンを購入した１月３０日午後２時３９分頃，１号パソコンにＲというＯＳをインストールした。同日午後３時２０分頃，そのＲ上でＷＥＰ鍵情報の解析を行うことができるソフトウェアＳにより，被告人方の真向かいにあるＱ方の無線ＬＡＮアクセスポイント（以下「Ｑ方無線ＬＡＮ」という。）に対して攻撃がなされて，ＷＥＰ鍵が取得され，同日午後５時２６分頃から同日

午後６時２７分頃までの間，１号パソコンからＱ方無線ＬＡＮに接続した。

そして，後述するとおり，被告人は，６月１１日午前１１時２６分頃，１号パソコンを操作して，Ｑ方無線ＬＡＮに接続したと認められる。

なお，１号パソコンのほか，被告人方から押収された押収品番号１８号のパソコン（１８号パソコンという。）と６号外付けハードディスクから，暗号化ファイル「cra.atc」が発見され，それを復号すると作成される「cra.txt」に，Ｑ方無線ＬＡＮのＷＥＰ鍵情報などが記録されていた。

⑵　検討

被告人が，１号パソコンを購入し，Ｒをインストールした当日に，第三者が１号パソコンに対する遠隔操作の準備を済ませ，Ｒのインストールからわずか４０分程度で，Ｓを実行し，不正アクセスの準備行為であるＷＥＰ鍵の取得をした可能性は現実的には極めて低いと考えられる。そして，後述のとおり，６月１１日に，被告人がＱ方無線ＬＡＮに接続したということは，１号パソコンを購入し使用した被告人がＱ方無線ＬＡＮのＷＥＰ鍵情報を取得したと合理的に推認することができる。このことは，被告人所有の他の機器から発見された暗号化ファイルの中にもＱ方無線ＬＡＮのＷＥＰ鍵情報が保存されていたことにより裏付けられている。

第３　Ｏ事件（第１３の事実）について

１　Ｏ事件の事実経過

θが取締役を務めていたＯは，Ｐ銀行のインターネットバンキングに登録していた。６月頃，Ｏのコンピュータは，コンピュータウィルス「Ｘfile.exe」に感染した。このウィルスの元のファイル名は，「syouhingazou7.exe」であった。「syouhingazou7.exe」を実行すると，感染した旨，犯人側のコンピュータに送信される。

犯人は，６月１０日午後１１時４３分頃，Ｐ銀行のサーバコンピュータに，Ｏのログイン１Ｄとログインパスワードからなる識別符号を入力して，不正に

ログインした。この不正ログインの接続元のＩＰアドレスは，Ｑ方無線ＬＡＮに割り当てられていたものであった。

２　被告人が犯人であることを基礎づける事実

⑴　本件不正ログインは，１号パソコンによって取得保存されたＯの識別符号を用いて行われたこと

ア　認定できる事実

㋐　６月２日，１号パソコンからリンク先に「syouhingazou7.exe」が蔵置されたＵＲＬが記載されているメールがＯのメールアドレス等に一括送信された。

㋑　１号パソコンには，遠隔操作ウィルスを作成し，操作できるソフトウェアＴがインストールされている。Ｔで作成されたウィルスを実行すると，自動的にファイル名が変更される機能がある。また，その機能の一つとしてファイルの取得がある。

㋒　１号パソコンのＴのフォルダ内にあった「θ+++」のフォルダに，「法人 No.docx」というファイルが保存されており（更新日時は６月１０日午後６時２０分），その中に，ＯのＰ銀行に関するログインＩＤ（省略）とログインパスワード（省略）が記録されていた。そのほか，Ｕという文字列や別の識別符号なども記録されていた。

㋓　Ｏのパソコンが感染した「Ｘfile.exe」のファイルと，１号パソコンから発見された「syouhingazou7.exe」のファイルのハッシュ値（ファイルを識別するための文字列情報であり，ファイルの内容が少しでも異なれば全く違う文字列が生成される）が，SHA-1 と MD5 という２種類の計算方法で一致した。ハッシュ値が同一であるのにファイルが異なる確率は，比較的重複する可能性がある MD5 という計算方法でも，約１８００京分の１の確率である。そうすると，１号パソコンから発見されたファイルとＯに送信されたファイルは,同一のファイルであると認められる。

㈠　上記「Ｘfile.exe」の通信先と１号パソコンのＴの通信先は，いずれも「ma…….me」に設定されており，１号パソコンでは，この文字列とＱ方無線ＬＡＮのＩＰアドレスがダイナミックＤＮＳ（一般家庭のインターネット回線のＩＰアドレスは変化するところ，ＩＰアドレスが変化しても，必ず同一のコンピュータと接続できるようにする仕組み）により対応付けられていた。

㈡　１号パソコンは，本件不正ログインの時刻を含む６月９日午前１０時６分５７秒から６月１１日午前３時４８分２０秒までの間，無線ＬＡＮで，Ｑ方無線ＬＡＮに接続されていた。

イ　検討

識別符号は，その性質上，これを登録した者やその関係者以外の第三者が知りえない情報である。そして，識別符号を取得するためのコンピュータウィルスの通信先は，犯人が使用している端末が設定している通信先とするのが通常と考えられる。

上記アの事実によれば，１号パソコン内から発見されたＯの識別符号等が記録されたファイルは，１号パソコンのＴを用いて，Ｑ方無線ＬＡＮを通じて取得され保存されたこと，犯人は，１号パソコンに取得保存されたこの識別符号を用いて，１号パソコンから本件不正ログインをしたことを推認できる。

そして，１号パソコンは，被告人方居室において，被告人が専属で使用していたのであるから，この事実は，被告人が犯人であることを強く指し示している。

(2)　本件不正ログインの翌日，被告人が，上記「法人No.docx」や「メモ.txt」のファイルを開いて，Ｑ方無線ＬＡＮに接続したこと

ア　認定できる事実

㈠　被告人方居室の捜索差押が開始された６月１１日午前１１時２８分，

１号パソコンのデスクトップ画面上では，ＯのＰ銀行に関する識別符号が記録されたファイル「法人 No.docx」が開かれていた上，インターネットエクスプローラーで，Ｕ銀行のホームページが開かれていた。捜索開始時，被告人の顔面から５０ないし６０センチメートルの位置に１号パソコンのデスクトップ画面が置かれていた。

㈠ その直前の１号パソコンのインターネット接続状況は，概ね次のとおりである。すなわち，１号パソコンは，６月１１日午前３時４８分２０秒以降，インターネットから切断された状態にあった。ユーザーの直接操作により，同日午前１１時２５分５４秒から午前１１時２６分０４秒までの間に，「メモ.atc」が復号され，「メモ.txt」がデスクトップ上に作成されて，これが開かれた。この「メモ.txt」には，Ｑ方無線ＬＡＮに接続するためのＷＥＰ鍵情報が保存されていた。同日午前１１時２６分から午前１１時２８分までの間，１号パソコンのクリップボードに，Ｑ方無線ＬＡＮのＷＥＰ鍵の文字列が保持された。

そして，午前１１時２６分３５秒，１号パソコンはＱ方無線ＬＡＮに接続され，午前１１時２７分４秒に「法人 No.docx」のファイルが開かれた後，午前１１時２７分２１秒，インターネットエクスプローラーが開かれた。

イ 検討

１号パソコンがインターネットに接続される前の時点で，１号パソコンが遠隔操作されていた可能性はない。また，その当時，被告人方居室内にいたのは被告人だけである。したがって，Ｑ方無線ＬＡＮ接続に必要なＷＥＰ鍵情報が保存された暗号化ファイル「メモ.txt」を開いて，Ｑ方無線ＬＡＮに接続し，かつ「法人 No.docx」のファイルを開いた人物は，被告人であると認められる（このことから，被告人は，「メモ.atc」の復号パスワード「ma……」を認識していたと認められ，１月３０日にＱ方無線ＬＡＮ

を攻撃し，そのＷＥＰ鍵情報を入手して，「メモ.txt」に保存し，それを暗号化したファイルである「メモ.atc」を作成した人物は被告人であると合理的に推認できる。)。

そして，本件不正アクセスの翌日に，被告人がＯの識別符号が記録されたファイルを開き，上記操作を行っていたということは，本件不正アクセスの犯人が被告人であることを強く指し示している。

(3) 被告人が１号パソコンから無線ＬＡＮアダプタを引き抜いたこと

ア　認定できる事実

証人γ及び証人Δの証言によれば，６月１１日午前１１時２８分頃，警察官が被告人に対し，捜索差押の開始を告げたこと，γ警察官が寝そべっていた被告人と１号パソコンとの間に手を差し入れたが，被告人は，その下をかいくぐり無線ＬＡＮアダプタのＵＳＢコードを引き抜いたことが認められる。

イ　証言の信用性

証人γ及び証人Δの証言は，主要な点において概ね一致しており，不自然不合理な点はない上，捜索に入った警察官としては被疑者の行動を意識的に観察しているものであり,両名ともに見間違いがあるとは考えられないから，両名の証言は十分信用できる。

ウ　被告人の弁解

被告人は，他人の無線ＬＡＮに接続していたことはない，無線ＬＡＮアダプタのコードに指を巻き付けて遊んでいたところ，警察官が突然入ってきたため驚き，無線ＬＡＮアダプタが抜けてしまったと供述している。

被告人の供述は，直前にＱ方無線ＬＡＮに接続したことに反するし，内容自体不自然であるから信用することができない。

エ　検討

警察官による捜索開始に当たり，被告人が無線ＬＡＮアダプタを引き抜いたということは，少なくとも被告人に，直前の自分の不正な行為を隠匿する

意図があったと考えられる。

3　小括

以上の事実を合わせると，特段の事情のない限り，被告人がO事件の犯人であると推認することができる。

第４　Ｂ事件（第１ないし第３の事実）について

１　Ｂ事件の事実経過

Ｂは，Ａ銀行のインターネットバンキングを利用していた。

犯人は，２月２０日午前３時３分頃，Ａ銀行になりすましてＡダイレクトを装い，ログイン画面をリニューアルしたなどと偽ってフィッシングサイトのＵＲＬを記載し，同サイトへのアクセスを促すメール（フィッシングメールという。）をＢに送信した。同日午前８時３０分頃に上記メールを確認したＢの従業員は，フィッシングサイトにアクセスし，Ｂが開設したＡ銀行の貯金口座にかかるインターネットバンキングのお客様番号，ログインパスワード，インターネット用暗証番号等の識別符号を入力した。同日午前９時３０分頃，その識別符号がメールアドレス「ft……@…….co.jp」に自動的に送信された。

犯人は，同日午前１１時３７分頃，同月２１日午前０時２３分頃，同日午前９時２０分頃の３回にわたり，Ａ銀行のサーバコンピュータに，Ｂに付された識別符号を入力し，不正にログインした。そして，同日午前９時２０分頃に行われた不正ログインによる状態を利用して，同日午前９時２２分頃にはＡダイレクトの連絡用メールアドレスを「k-……@…….co.jp」から「gy……@…….co.jp」に変更し，同日午前９時２３分頃，Ｄ名義の銀行口座に２回にわたり合計８７万円を送金した。

２　被告人が犯人であることを基礎づける事実

⑴　不正ログインの接続元が１号パソコンであること

ア　認定できる事実

㋐　１回目（２月２０日午前１１時３７分頃）の不正ログインは，Ｑ方無

線ＬＡＮを接続元とし，Ｖ株式会社が管理するWの中継サーバを経由してなされたものであった。

その中継サーバの接続履歴に記録されたクライアントＩＤ（Ｖ社がWの利用者を識別するために，Wのソフトウェアダウンロード時に割り当てる一意の文字列で，ダウンロード時に重複して割り当てられることはないもの）が１号パソコンにインストールされたWのクライアントＩＤと一致した。

１号パソコンは，１回目の不正ログイン時にWに接続しており，中継サーバ側の接続履歴に記録されていたセッションＩＤ（Wの中継サーバを利用する各端末の通信を識別するために割り当てる一意の文字列であり，同一接続時に同一のセッションＩＤが重複することはないもの）と，１号パソコンに記録されていたセッションＩＤが一致した。

したがって，この不正ログインが１号パソコンからなされたことは明らかである。

㈠　２回目（同月２１日午前０時２３分頃）の不正ログインの接続元は，Ｑ方無線ＬＡＮであり，中継サーバを経由せずに，直接不正アクセスされたものであった。

㈡　３回目（同月２１日午前９時２０分頃）の不正ログインは，Ｑ方無線ＬＡＮのＩＰアドレスを接続元とし，Wの中継サーバの一つであるボランティアサーバを経由してなされたものであった。また，ボランティアサーバへの接続元のクライアントＩＤが１号パソコンに割り当てられたものであった。

㈢　なお，被告人は，２月６日の時点で，１号パソコンにWをインストールしていた。

イ　検討

１回目の不正ログインが，１号パソコンからＱ方無線ＬＡＮを通じて行

われたことは明らかに認められる。そして，１回目の不正ログインから約１３時間後に，同一の接続先に，同様にＱ方無線ＬＡＮからなされた２回目の不正ログインと，さらに，その約９時間後に，同一の接続先に，同じＱ方無線ＬＡＮを通じてＷのボランティアサーバを経由してなされた３回目の不正ログインについても，その接続元の同一性やログイン間隔の近接性等に照らせば，１回目の不正ログインと同様に１号パソコンからなされたものであることが合理的に推認できる。

⑵　Ｂが受信したフィッシングメールが１号パソコンから送信されたこと

ア　認定できる事実

㋐　１号パソコン内の３つのテキストファイル，Ｘによる自動保存ファイル，削除データ領域内のファイルから，それぞれ，Ｂのメールアドレス「ko……@…….co.jp」の文字列が発見された。最も更新日時が古いものは「ι.txt」であり，その日時は２月１６日午後３時３分４３秒であった。

㋑　フィッシングサイトに入力されていた識別情報の送信先メールアドレス「ft……@…….co.jp」に対応するＣ株式会社ＩＤ「ft……」と，不正ログイン状態を利用してＡ銀行に虚偽情報として送信された連絡用メールアドレス「gy……@…….co.jp」に対応するＣ株式会社ＩＤ「gy……」は，同じ日（２月２７日）に，同一のＹが付与されたブラウザからログインされたことがある。Ｙは，Ｃ株式会社が，Ｃ株式会社会員の使用するコンピュータ内のブラウザに対して発行する個別の文字列であり，一度発行された値と同じものは二度と発行されないものである。

イ　検討

このようにフィッシングメールが送信された２月２０日よりも前の時点で，既に１号パソコン内にＢのメールアドレスが保存されていた上，Ｂの識別符号等が「ft……@…….co.jp」に送信された約２時間後には１号パソ

コンから１回目の不正ログインが行われていること，１号パソコンから不正ログイン状態を利用して変更された連絡用メールアドレスとフィッシングサイトの情報送信先メールアドレスが同一端末で利用されていると考えられることからすると，Ｂが受信したフィッシングメールは，不正ログインの準備行為として１号パソコンから送信されたことが合理的に推認できる。

３　小括

このように不正ログイン及びフィッシングメールの送信元がいずれも１号パソコンであると認められる。そして，１号パソコンは，被告人が専属で使用しており，かつ，被告人がＱ方無線ＬＡＮのＷＥＰ鍵情報を入手していたことを併せ考慮すると，特段の事情のない限り，被告人がＢ事件の犯人であると推認することができる。

第５　Ｅ事件（第４及び第５の各事実）について

１　Ｅ事件の事実経過

Ｅは，２月２６日当時，Ａ銀行のインターネットバンキングを利用していた。

犯人は，２月２６日午前１１時５分頃，Ａ銀行になりすましてＡダイレクトを装い，メッセージが届いたなどと偽ってフィッシングサイトのＵＲＬを記載し，同サイトへのアクセスを促すメールをＥに送信した。その頃，同メールを確認したＥの従業員は，フィッシングサイトにアクセスし，Ｅが開設したＡ銀行の貯金口座にかかるインターネットバンキングのお客様番号，ログインパスワード，インターネット用暗証番号等の識別符号を入力した。同日午前１１時１１分頃，その識別符号が「da……@…….co.jp」に自動的に送信された。

犯人は，同日午前１１時４６分頃，同日午後０時１１分頃，同日午後０時３４分頃の３回にわたり，Ａ銀行のサーバコンピュータに，Ｅに付された識別符号を入力した。そして，犯人は，同日午後０時１１分頃に行われた不正ログイン状態を利用して，同日午後０時１４分頃，Ｅ名義の貯金口座からＦ名義の銀

行預金口座に９万６０００円を送金した。

２　被告人が犯人であることを基礎づける事実

⑴　不正ログインの接続元が１号パソコンであること

ア　認定できる事実

㋐　Ｅの識別符号を用いてなされた３回の不正ログインの接続元のＩＰアドレスはいずれもＷの中継サーバのものであった。この中継サーバの通信履歴と接続履歴から，中継サーバがその接続元の端末に割り当てたクライアントＩＤ及びセッションＩＤが１号パソコンのものと一致した。また，中継サーバへの接続元のＩＰアドレスは，当時Ｑ方無線ＬＡＮに割り当てられていたものであった。

㋑　１号パソコンは，上記３回の不正ログインがあった時間帯に，いずれも無線ＬＡＮに接続しており，Ｗにも接続していた。

イ　検討

以上によれば，本件不正ログインは，１号パソコンからＱ方無線ＬＡＮに接続し，Ｗの中継サーバを経由して行われたと認められる。

１号パソコンは，被告人が専属で使用していたものであるし，被告人は，Ｑ方無線ＬＡＮに接続するためのＷＥＰ鍵情報を入手していたから，本件不正ログインが１号パソコンからなされたということは，被告人が犯人であることを強く指し示している。

⑵　フィッシングサイトに入力された識別符号の送信先メールアドレスのＣ株式会社ＩＤと被告人使用のＣ株式会社ＩＤのＹが一致したこと

ア　認定できる事実

㋐　Ｅが受信したフィッシングメールには，フィッシングサイトのＵＲＬ「http://……」が記載されていたところ，１号パソコン内の仮想メモリである「κ.sys」にも，このＵＲＬと同じ文字列が保存されていた。

㋑　このフィッシングサイトに入力されていた識別符号の送信先メールア

ドレス「da……@…….co.jp」に対応するＣ株式会社ＩＤは「da……」である。被告人の使用するＣ株式会社ＩＤは「hi……」であった。

㋒　同じ２月２６日のうちに,同一のＹが付与された端末から,「hi……」,「as……」,「da……」の３つのＣ株式会社ＩＤを利用して合計４回のログインがあった（うち「as……」は２回)。前述したとおり，Ｙが一致するログは同一端末からログインされたことを意味する。

これら４回のログインのそれぞれのＩＰアドレスは，被告人の自宅に割り当てられたＩＰアドレス，被告人方に隣接するε方に割り当てられたＩＰアドレス，被告人方向いのＱ方に割り当てられたＩＰアドレス，被告人利用と認められる中継サーバのＩＰアドレスであった。

イ　検討

このように，Ｃ株式会社ＩＤ「da……」と「hi……」を利用して，同一のＹの付与された端末からログインがなされているということからすると，２月２６日頃，被告人が「da……」及びこれに対応するメールアドレス「da……@…….co.jp」を使用していたと認められる。そして，犯人がフィッシングサイトに入力した識別符号の送信先は，犯人が使用可能な端末のメールアドレスであると考えるのが合理的である。したがって，そのメールアドレスを使用していた被告人が犯人であることを強く指し示すものである。

フィッシングメールに記載されたＵＲＬの文字列が，１号パソコン内に残っていたことは，これを裏付ける。

⑶　不正送金先に宛てたメールの送信元メールアドレスと被告人のメールアドレスのＹが一致したこと

ア　認定できる事実

㋐　２月２６日午後０時５０分，メールアドレス「as……@…….co.jp」から，「ar……@…….co.jp」に対し，「こちらにメールを変更します。送り先ですが，〒（省略）　愛媛県松山市ｋ町ｌ－ｍ－ｎ（省略）留め（被告

人名）宛までお願いします。（省略）の追跡番号をお知らせください。今後の警察のこともありますので，あとでまた連絡をしてください。」という内容の電子メールが送信された。

㈠　「ar……@…….co.jp」は，Ｅの貯金口座からの不正送金先であるＦ名義の普通預金口座の顧客情報として登録されたメールアドレスである。

㈡　Ｃ株式会社ＩＤ「as……」は，被告人使用の「hi……」及び「da……」と同一のＹが付与された端末からログインがなされている。

イ　検討

したがって,「as……」に対応するメールアドレスを，２月２６日当時，被告人が使用していたものであり，さらに，メールの内容や送信時期に照らせば，被告人が，Ｅの不正送金先の人物に宛てて，送り先を指示する内容のメールを送信したことを合理的に推認させる。

この事実は，被告人が犯人であることを強く指し示すものである。

３　小括

以上の事実を総合すれば，特段の事情のない限り，被告人がＥ事件の犯人であることは，合理的に推認することができる。

第６　Ｈ事件（第６及び第７の事実）について

１　Ｈ事件の事実経過

Ｈは，３月当時，Ｇ銀行のインターネットバンキングを利用していた。

３月２７日，Ｈの経営者は，同社のパーソナルコンピュータに送信されたコンピュータウィルス「卸価格 5.exe」を実行した。「卸価格 5.exe」は，これを実行すると，コンピュータのＩＰアドレスが犯人側のコンピュータと同期した特定の通信先に送信され，犯人側のコンピュータで遠隔操作ソフトウェアを使用すると,「卸価格 5.exe」を実行したコンピュータを遠隔操作することができるウイルスである。「卸価格 5.exe」の通信先は,「ma…….biz」であり，この通信先は，平成２６年３月及び４月の一時期，ダイナミック DNS によりＱ方Ｉ

Ｐアドレスに対応付けられていた。

犯人は，３月２７日午後７時７分頃，同月２８日午前１０時１３分頃の２回にわたり，Ｇ銀行のサーバコンピュータに，Ｈに付された識別符号を入力するなどして不正ログインした。そして，犯人は，同日午前１０時１３分頃に行われた不正ログインの状態を利用して，同日午前１０時２３分頃，Ｈの預金口座からＩ名義の銀行口座に２００万円を送金した。

２　被告人が犯人であることを基礎づける事実

⑴　不正ログインの接続元が１号パソコンであること

ア　認定できる事実

㋐　１回目の不正ログインの接続元のＩＰアドレスは，当時Ｑ方無線ＬＡＮに割り当てられていたものであった。この不正ログインが行われた際，１号パソコンはＱ方の無線ＬＡＮに接続していた。

㋑　２回目の不正ログインの接続元のＩＰアドレスは，Ｗの中継サーバのものであり，中継サーバの接続履歴に記録されたクライアントＩＤは，１号パソコンのＷのクライアントＩＤと一致した。この２回目の不正ログイン時，１号パソコンは，Ｗに接続しており，中継サーバに記録されたセッションＩＤと，接続時の１号パソコンのセッションＩＤが一致した。

また，２回目の不正ログイン時の中継サーバの接続元のＩＰアドレスは，Ｑ方無線ＬＡＮに割り当てられたものであり，当時，１号パソコンはＱ方無線ＬＡＮに接続していた。

イ　検討

２回目の不正ログインは，１号パソコンのクライアントＩＤ及びセッションＩＤと中継サーバ側のクライアントＩＤ及びセッションＩＤがそれぞれ一致しているから，１号パソコンから行われたことが認められる。そして，不正送金が行われた２回目の不正ログインは，Ｑ方無線ＬＡＮからＷ

の中継サーバを経由してなされたものであり，その約１５時間前という近接した日時においてなされた１回目の不正ログインが２回目と同様にＱ方無線ＬＡＮから接続されたものであることにかんがみると，各不正ログインは，一連の行為として，１号パソコンからＱ方無線ＬＡＮを接続元として行われたことが合理的に推認される。

そして，１号パソコンは，被告人が専属で使用していたものであり，被告人は，Ｑ方無線ＬＡＮに接続するためのＷＥＰ鍵情報を入手していたから，本件不正ログインが１号パソコンからなされたということは，被告人が犯人であることを強く指し示している。

⑵　１号パソコンにＨの識別符号が保存されていたこと

ア　認定できる事実

㋐　１号パソコンのデスクトップ上に「λ.atc」という暗号化ファイルがあり，その中にある「μ」というフォルダに，Ｈの識別符号（ログインＩＤは（省略），パスワードは（省略））が記載されていた。

㋑　Ｈの識別符号が保存されていた「λ.atc」を復号するためのパスワードは，「ma……」であった。

㋒　１号パソコンの「ν.txt」内に，Ｈのメールアドレスが保存されていた。

イ　検討

１号パソコンに通常他人に知られることのないＨの識別符号が保存されていたところ，前述したとおり，１号パソコンには，遠隔操作ウイルスを作成し，ファイルを取得することができるＴがインストールされていた。また，「卸価格 5.exe」の通信先は，一時期Ｑ方無線ＬＡＮのＩＰアドレスに対応づけられていた。したがって，不正ログインの準備行為であるＨの識別符号の取得は，１号パソコンから行われたことを合理的に推認することができる。

そして，Ｈの識別符号が保存されている暗号化ファイルの復号パスワードが「ma……」であり，Ｑ方無線ＬＡＮのＷＥＰ鍵情報等が保存されていて被告人が捜索差押の開始直前に開いた暗号化ファイル「メモ.atc」の復号パスワードと同一であるということは，被告人自らがＨの識別符号の保存された暗号化ファイルを作成し保存したものと推認することができる。

したがって，１号パソコンにＨの識別符号が保存されていた事実は，被告人が犯人であることを強く指し示すものである。

３　小括

以上の事実によれば，特段の事情のない限り，Ｈ事件の犯人が被告人であることを推認することができる。

第７　Ｊ事件（第８の事実）について

１　Ｊ事件の事実経過

犯人は，５月９日午前３時５９分頃から同月１５日午後２時１６分頃までの間，１８２万１２３３回にわたり，脆弱性検査ツールとして海外で配布されているソフトウェアＺによりＪが管理するサーバコンピュータに SQLinjection（SQL というデータベースを検索するための命令文に，不正な SQL を挿入することで本来表示すべきでないデータを表示させるという攻撃手法）を行った。

２　被告人が犯人であることを基礎づける事実

⑴　Ｊへの SQLinjection 攻撃にかかる通信の接続元が１号パソコンであること

ア　認定できる事実

SQLinjection 攻撃の通信の接続元ＩＰアドレスは，Ｑ方無線ＬＡＮのものと，Ｗの中継サーバのものとがあり，Ｗの中継サーバの通信履歴によれば，SQLinjection 攻撃時の各通信に割り当てられていたセッションＩＤは，同じ時刻に割り当てられていた１号パソコンのセッションＩＤと一致した。また，１号パソコンは，本件 SQLinjection 攻撃が行われた当時，Ｑ方の無

線ＬＡＮに接続していた。

イ　検討

Ｗの中継サーバを経由して行われた SQLinjection 攻撃は，１号パソコンに割り当てられたセッションＩＤにかかる通信により行われていたのであるから，１号パソコンから行われたものと認められる。そして，Ｑ方無線ＬＡＮを接続元としてなされた SQLinjection 攻撃についてみても，１号パソコンがＱ方無線ＬＡＮに接続していた上，Ｗの中継サーバを経由して行われた SQLinjection 攻撃と近接した日時に行われていることからすれば，一連の SQLinjection として１号パソコンから行われたことが推認される。

そして，１号パソコンは，被告人が専属で使用していたものであるし，被告人は，Ｑ方無線ＬＡＮに接続するためのＷＥＰ鍵情報を入手していたから，本件攻撃が１号パソコンからなされたということは，被告人が犯人であることを強く指し示している。

⑵　１号パソコン等から SQLinjection 攻撃の痕跡が発見されたこと

ア　認定できる事実

㋐　１号パソコンから，Ｚが発見された。それは，被告人がインストールしたものである。

㋑　１号パソコンから，８０００件弱のメールアドレス一覧が保存されたファイルが発見された。後日，調査した結果，そのメールアドレスのうち５８件を除いて，Ｊが保有しているメールアドレスと一致した。

㋒　ＪのウェブサイトのＵＲＬ情報が，１号パソコンのバックアップデータの領域内のデスクトップに相当する部分に保存されたテキストファイル中に記録されていた。

㋓　被告人の居室内から押収された書籍「(省略)」には，Ｚが，SQLinjection という形でハッキング等の脆弱性検査のツールとなる旨の記載があり，

書籍中の「SQL サーバーの脆弱性検出から攻撃まで簡単に　Ｚ」との記載部分がマーカーで着色されていた。

イ　検討

これらの事実によれば，１号パソコンからＺを用いて SQLinjection 攻撃が行われ，その結果としてＪが保有するメールアドレスが取得されたと考えられる。なお，メールアドレス５８件につき不一致であったが，その理由としては，Ｚでは対応していない文字が含まれたメールアドレスについて一部欠損したものがあったこと，また，メールアドレスが漏えいした可能性があるとの情報を受けて，メールアドレスを変更した者がいたことが挙げられる。

１号パソコンは，被告人が専属で使用していたものであるから，本件攻撃が１号パソコンからなされたということは，被告人が犯人であることを強く指し示している。Ｚにより SQLinjection 攻撃が可能である旨の記載がある書籍を被告人が読み，かつ，関心を持っていることは，上記推認を更に強めるものである。

３　小括

以上によれば，特段の事情のない限り，被告人がＪ事件の犯人であると推認できる。

第８　Ｌ事件（第９ないし第１１の各事実）について

１　Ｌ事件の経過

Ｌは，５月当時，Ｋ銀行のインターネットバンキングを利用していた。

５月１３日頃，Ｌの代表者が，同社のパーソナルコンピュータに送信されたコンピュータウィルス「screenshot2.exe」を実行した。「screenshot2.exe」は，これを実行したコンピュータのＩＰアドレスが，犯人側コンピュータと同期した通信先に送信され，犯人側のコンピュータから遠隔操作ソフトウエアを使用して，「screenshot2.exe」を実行したコンピュータを遠隔操作することができ

るウイルスである。

犯人は，５月１５日午前０時３０分頃から同月１９日午後０時４９分頃までの間，７回にわたり，Ｋ銀行のサーバコンピュータに，Ｌに付された識別符号を入力し，不正ログインを行った。そして，同日午後０時３９分頃及び同日午後０時４９分頃に行われた不正ログインの状態を利用して，同日午後０時４６分頃から同日午後０時５５分頃までの間，登録電子メールアドレスや振込先口座２件の登録が行われた。また，同日午後０時５３分頃から同日午後０時５７分頃までの間，登録された振込先口座であるM名義の銀行口座に２回にわたり合計２２２万７０００円が送金された。

２　被告人が犯人であることを基礎づける事実

⑴　「screenshot2.exe」と１号パソコンの結びつきについて

ア　認定できる事実

㋐　１号パソコンには，遠隔操作ウィルスを作成し，操作できるソフトウェアＴがインストールされている。その機能の一つとしてファイルの取得がある。

㋑　Ｌに送信された「screenshot2.exe」の Mutex 値が１号パソコンのＴの設定ファイルに記載された Mutex 値と一致した。Mutex 値は，プログラムが重複して起動しないようにするために用いられる識別情報であり，遠隔操作ウイルス作成ソフトＴにおいては，英数字を組み合わせた４０ケタの文字列で乱数が自動的に生成される仕組みになっているから，同じ Mutex 値が生成されることはまずないと考えられる。

㋒　「screenshot2.exe」の通信先は，「ma…….me」に設定されていた。前記第３の２⑴ア㋔のとおり，この文字列は，１号パソコンにインストールされたＴの通信先と同一であり，また，１号パソコンでは，この文字列とＱ方無線ＬＡＮのＩＰアドレスが，ダイナミックＤＮＳにより対応付けられていた。

イ　検討

以上の事実によれば,不正ログインの準備行為である「screenshot2.exe」の作成及び送信は，１号パソコンにより行われたことを合理的に推認することができる。

そして，当時被告人が１号パソコンを専属的に使用しており，Ｑ方無線ＬＡＮのＷＥＰ鍵情報を入手していたのであるから，上記の事実は，被告人が犯人であることを強く指し示すものである。

⑵　１号パソコンからＬの識別符号が発見されたこと

ア　認定できる事実

㋐　１号パソコンから，暗号化ファイル「ξ.atc」が発見された。その中にある「ｏ」というフォルダ内の「Ｋ銀行.rtf」というフォルダに，Ｌの識別符号（ＩＤは（省略），パスワードは（省略））が記録されていた。

㋑　Ｌの識別符号が保存されていた「ξ.atc」を復号するためのパスワードは，「ma……」であった。

イ　検討

Ｌの識別符号が保存されている暗号化ファイルの復号パスワードが「ma……」であり，これがＱ方無線ＬＡＮのＷＥＰ鍵情報等が保存され，かつ被告人が捜索差押の開始直前に開いた暗号化ファイル「メモ.atc」の復号パスワードと同一であるということは，被告人自らがＬの識別符号の保存された暗号化ファイルを作成し保存したものと推認することができる。

したがって，１号パソコンにＬの識別符号が保存されていた事実は，被告人が犯人であることを強く指し示すものである。

⑶　本件不正ログインの接続元がＱ方無線ＬＡＮであったこと

ア　認定できる事実

㋐　７回の本件不正ログインの接続元のＩＰアドレスは，いずれも当時Ｑ方無線ＬＡＮに割り当てられていたものであった。

(イ) この７回の不正ログインの各当時，１号パソコンはＱ方の無線ＬＡＮに接続されていた。

イ　検討

被告人は，１号パソコンを専属的に使用しており，Ｑ方無線ＬＡＮのＷＥＰ鍵情報を入手していたから，この事実は，被告人が犯人であることを指し示すものである。

３　小括

これらの事実によれば，特段の事情のない限り，被告人がＬ事件の犯人であることを推認することができる。

第９　Ｎ事件（第１２の事実）について

１　Ｎ事件の事実経過

犯人は，６月３日午後１時２６分頃，コンピュータウィルス「決済情報 8.exe」が添付されたメールをＮに送信した。

同日午後１時５０分頃，Ｎの経営者がそのメールを受信し，「決済情報 8.exe」を実行した。「決済情報 8.exe」は，これを実行したコンピュータのＩＰアドレスが，犯人側コンピュータと同期した通信先に送信され，犯人側のコンピュータから遠隔操作ソフトウェアを使用して，「決済情報 8.exe」を実行したコンピュータを遠隔操作することができる。

２　被告人が犯人であることを基礎づける事実

(1)　１号パソコンで「決済情報 8.exe」が作成されたこと

ア　認定できる事実

(ア)　１号パソコンから「決済情報 8.exe」というファイルが発見された。

(イ)　１号パソコンから発見された「決済情報 8.exe」とＮに送信された「決済情報 8.exe」のハッシュ値が，SHA-1 と MD5 という２種類の計算方法で値が一致した。そうすると，１号パソコンから発見されたファイルとＮに送信されたファイルは，同一のファイルであると認められる。

㈢　また，Ｎに送信された「決済情報 8.exe」の Mutex 値が，１号パソコンから発見されたＴの設定ファイル内に記録されていた「決済情報 8.exe」の Mutex 値と一致した。

イ　検討

Ｎに送信された「決済情報 8.exe」と，１号パソコン内に記録された「決済情報 8.exe」のハッシュ値と Mutex 値とが一致したことから，Ｎに送信された「決済情報 8.exe」は，１号パソコンにインストールされたＴで作成されたことが明らかである。

この事実は，当時１号パソコンを専属で使用していた被告人が犯人であることを強く指し示すものである。

⑵　「決済情報 8.exe」の通信先と１号パソコンとのつながり

ア　認定できる事実

㈠　「決済情報 8.exe」が添付されたメールの送信元のＩＰアドレスは，Ｑ方無線ＬＡＮアクセスポイントに割り当てられていたものであった。

㈡　１号パソコンは，「決済情報 8.exe」がＮに送信された日時頃，Ｑ方無線ＬＡＮアクセスポイントに接続していた。

㈢　「決済情報 8.exe」の通信先は，「ma…….me」であった。

㈣　前記第３の２⑴ア㈣のとおり，１号パソコンのＴの通信先も，「ma…….me」であり，この文字列は，ダイナミックＤＮＳという仕組みにより，１号パソコン内でＱ方無線ＬＡＮのＩＰアドレスに対応付けられていた。

イ　検討

識別符号を取得するためのコンピュータウィルスの通信先は，犯人が使用している端末が設定している通信先とするのが通常と考えられる。したがって，Ｎに送信された「決済情報 8.exe」の送信元がＱ方無線ＬＡＮであり，かつ「決済情報 8.exe」の通信先が，１号パソコン内でＱ方無線ＬＡＮに対応付けられた通信先と同一であるということは，当時１号パソコン

を専属で使用し，かつ，Ｑ方無線ＬＡＮに接続するためのＷＥＰ鍵情報を入手していた被告人が犯人であることを強く指し示すものである。

⑶　１号パソコン内からＮの識別符号が発見されたこと

ア　認定できる事実

㋐　１号パソコン内のＴフォルダの下層に「π」というフォルダがあり，その中に，Ｎのパソコンで作成されたものと同一内容のＮの識別符号情報が記録されたファイルがあった。

㋑　Ｔを起動して，「決済情報 8.exe」を操作する実験をしたところ，被害者側のパソコンのファイルを犯人側のパソコンで取得することができた。

イ　検討

識別符号は，その性質上，これを登録した者やその関係者以外の第三者が知りえない情報である。それにもかかわらず，被告人が専属で使用していた１号パソコン内に識別情報が保存されていたということは，被告人が犯人であることを強く指し示すものである。

３　小括

このように，ウイルスの作成及び送信元，識別符号の取得及び保存の点からいずれも被告人が犯人であることを強く指し示しているから，特段の事情のない限り，Ｎ事件の犯人が被告人であることを推認することができる。

第１０　上記各事件（第１ないし第１３の事実）について，１号パソコンが遠隔操作されたり，被告人以外の第三者によってなされた可能性がないこと

１　１号パソコンには，遠隔操作ウイルスによる感染及び遠隔操作された痕跡がなかったこと

１号パソコンから検出されたウイルスは，いずれも１号パソコンで作成されたものであり，少なくとも１号パソコンの押収時点においては，遠隔操作ウイルスに感染していなかった。

そして，少なくとも１号パソコンを解析した時点では，遠隔操作を受けるこ

とが可能となるツールであるρの設定は，接続許可を禁止する値となっていた。また，同様のツールであるσが使用された履歴が存在しなかった。さらに，１号パソコンは，４つの正規のプログラム以外には自動起動プログラム（登録すると，パソコンをシャットダウンして再び電源を入れた時に自動で動くようになる）の設定がなされていなかった。

２　Ｑ方無線ＬＡＮの電波を受信できる範囲

一連の犯行に用いられたＱ方無線ＬＡＮの電波の受信状況についてみると，建物等がなく見通しが良い場合には約５８メートル離れていても受信できたが，そうでない場合には約３０ないし４０メートルの範囲でしか電波を受信できず，この範囲には被告人方やＱ方を含む２０世帯程度しか建物がなかった（なお，被告人が犯人の可能性として指摘する甲方はその範囲にはない。）。

このようにＱ方無線ＬＡＮの電波を受信できるのは，数十メートルという限られた範囲であったのであり，本件各犯行は１号パソコンが上記の限定された範囲に存在していたときのみ可能であったことから，第三者による直接操作の可能性は特に小さいということができる。

３　一連の犯行が，被告人以外の第三者による直接操作又は遠隔操作により行われたとすると，合理的な説明ができない事実が存在する。

⑴　上記一連の犯行は，いずれも，１号パソコンからＱ方無線ＬＡＮを通じて行われたものであるところ，ＷＥＰ鍵情報は，その接続に不可欠であり，かつ，他人には基本的に知られることのないものである。被告人が１号パソコンを購入し，自らＲをインストールした約４０分後に，このことを知った第三者が１号パソコンに遠隔操作又は直接操作によりＲでＳを実行し，ＷＥＰ鍵を取得し，Ｑ方無線ＬＡＮへ接続した可能性は現実的には考えられない。

⑵　Ｑ方無線ＬＡＮのＷＥＰ鍵情報は，１号パソコン内の「メモ.txt」のみならず，被告人方居室内の１８号パソコンと６号外付けハードディスクにも，暗号化ファイル「cra.atc」を復号すると作成される「cra.txt」に保存され

ていた。各犯行が第三者による１号パソコンの遠隔操作により行われたものであるとすれば，被告人が「メモ.txt」を作成したと認められることや，ＷＥＰ鍵情報が１号パソコン以外の機器の暗号化ファイルに保存されていたことについて，合理的な説明がつかない。

(3) 本件各犯行は，いずれもＱ方無線ＬＡＮ及びWの中継サーバの双方又は一つを経由することで通信元を匿名化する手法で行われている。仮に，被告人以外の第三者が，１号パソコンを遠隔操作して犯行に及んだというのであれば，このような匿名化工作を更に施す必要性は乏しいと考えられる。

４　証人τは，１号パソコンが遠隔操作された可能性がある旨証言するものの，その理由として，捜査報告書の内容だけでは判断できない，作成過程が不明であるなどと証言するだけで，具体的に遠隔操作がなされた痕跡を指摘しておらず，その可能性は抽象的なものにとどまるから，第三者による遠隔操作が行われていないことにつき合理的な疑いを生じさせることにはならない。

５　被告人の弁解について

(1) 被告人は，①１号パソコンを甲に何度も貸しており，甲又はその関係者が犯行を行った可能性がある，②被告人の外出中に第三者が１号パソコンにアクセスしたことをうかがわせる痕跡がある旨供述している。

(2) ①の点に関して，甲は，被告人の依頼を受けて，１月頃から４月か５月頃までの間，被告人と不正送金先口座からの現金引き出し役である乙や丙との間の仲介をしていた，被告人からの指示を乙や丙に伝え，その後，同人らから受け取った現金を被告人に渡し，被告人から報酬をもらっていた，４月９日に骨折により入院するまでの間，被告人方を数回訪れ，被告人の部屋でパソコンを短時間操作したことはあるものの，パソコンを借り出したことはなく，４月９日から６月１４日までは骨折により整形外科に入院していた旨証言している。

甲の証言は，その内容自体に特段不自然不合理な点は見当たらないし，Ｂ

事件，Ｈ事件，Ｌ事件が行われた前後において，被告人と甲との間，甲と乙及び丙との間，乙と丙との間で電話による通話があったこととともよく合っている。さらに，被告人とは面識がなく，殊更被告人に不利な供述をする理由のない乙も，甲から「先の人間」がパソコンで現金を振り込むので，それを引き出してほしい旨頼まれたと証言しており，甲の上記証言を裏付けている。

したがって，上記の甲証言は基本的に信用できる。

⑶ 他方，①に関する被告人の供述について，既に検討したとおり，Ｑ方無線ＬＡＮのＷＥＰ鍵情報が，１号パソコンだけでなく，１８号パソコンや６号外付けハードディスクにも保存されていたことや，被告人自身，６月１１日に，ＷＥＰ鍵情報を使用してＱ方無線ＬＡＮに接続した事実と符合しない。

また，被告人は，自分以外にパソコンを使ったことがあるのは，友人の甲と丁の２人であり，自宅に遊びに来た時にインターネット検索や音楽を聞くために使わせたくらいである旨供述していたのであり，不自然に変遷している。

さらに，甲は，４月９日以降入院していたというのであるから，少なくとも，甲自身が，Ｊ事件，Ｌ事件，Ｎ事件については，１号パソコンを直接操作してＱ方無線ＬＡＮを通じて犯行に及ぶことは不可能である（一時外出や一時外泊の時期とも合っていない。）。そして，甲の関係者による犯行の可能性も主張するものの，極めて抽象的な可能性にとどまるものである。

そもそも，被告人は，甲が暴力団関係者とつながりがあり，他人名義の携帯電話機や保険証の調達を依頼したり，詐欺を持ちかけてくる人物であると認識しており，携帯電話機や保険証を貸すことは躊躇して断っていたというのに，１号パソコンを何度も甲に貸し続け，内容不明の暗号化ファイルが作成されていたことにも，疑いを持たなかったというのは不自然である。

⑷ 被告人の②の弁解については，検察官が論告で的確に指摘するように，そもそも被告人が不在であったという前提を欠いていたり，被告人が不在であ

った場合についても，パソコンによる自動更新等によるものであり，人為的な操作がなされたものではないことが明らかである。

被告人の弁解は信用することができない。

6　以上によれば，第三者が１号パソコンを遠隔操作又は直接操作して上記一連の犯行に及んだことを疑わせる事情は認められず，被告人が上記一連の犯行の犯人であることにつき合理的な疑いを入れる余地はない。

したがって，第１ないし第１３の事実は，合理的な疑いを超えて証明十分である。

第１１　無線局開設の認識について（第１４の事実）

1　弁護人は，被告人が１号パソコンに接続して使用していた無線ＬＡＮ接続機器（３号物件）につき，被告人には，３号物件が日本で定められている出力制限値を超える出力が可能なものであったという認識がなかったから，無線局開設の故意がなく，無罪である旨主張し，被告人もこれに沿う供述をしている。

2　証拠によれば，次の事実が認められる。

⑴　被告人方には，日本で定められている出力制限値を超える出力が可能な同種の「戊」という名称の無線ＬＡＮ接続機器が３つあった（３号物件，１７号物件，１９号物件)。なお，３号物件と１７号物件は品番（省略）も同じであった。

⑵　被告人は，平成２５年１２月２８日，Ｃオークションにより，３号物件又は１９号物件のいずれかの戊を購入した。その際のウェブページの「商品説明欄」直下には,「実験用・研究用・海外向け製品です　国内の使用は電波法違反になります」との記載があり，さらにその下方の「注意事項」欄には,「日本（11ｎ　150Mbps）出力制限値５mWをはるかに超えております　国内でのご使用はお控えください　海外でのご利用は使用する国の電波法を必ずご確認お願い致します」との記載があり，その最終行には「こちらも必ずご確認御願い致します」との文字が紫色で着色され，かつ，アンダーライン

が引かれて記載されていた。

その後，被告人は，再度戊２台を購入した。

３　上記認定のとおり，被告人が使用していた３号物件は，客観的には日本で定められている出力制限値を超える出力が可能な無線ＬＡＮ接続機器であり，被告人自ら３号物件を含む戊を，２回にわたりインターネットオークションで購入したこと，１回目に戊を購入した際のオークションのウェブページの商品説明欄には，戊を国内で使用すると電波法違反になる旨の記載，注意事項欄には出力制限値を超える出力が可能であることの記載があり，ウェブページの中央に配置され，必ず確認するよう注意喚起する文まで付され，強調されていたことが認められる。商品の購入にあたっては，その商品の性質や利用方法，使用上の注意点等について一応の関心を持つのが通常である上，本件の注意文言は，特に注意が向けられるように工夫されてウェブページに配置されており，通常人であれば，このウェブページを見て上記注意文言が目に入らないとは到底考え難い。従って，被告人が，１回目に戊を購入した平成２５年１２月２８日の時点では，少なくとも，３号物件と同種の戊が，国内で定められている出力制限値を超える出力が可能な機器であり，国内での使用が電波法違反になる旨の注意事項を閲読し，これを認識したことが推認される。そうすると，少なくとも，被告人は，同日以降，３号物件を含む戊の使用が無線設備の設置により無線局の開設に当たり，電波法違反になることを認識していたものと認められる。

なお，被告人は，チップセットの型番しか見ずに買ったので，違法なものであるとの認識はなかった旨も供述するが，他方，１号パソコンで戊を使用した際，戊が認識しなかった，システムの不具合なのか，無線ＬＡＮアダプタ自体の問題なのかわからなかったが，色違いの戊をもう一度購入し直したなどと供述しているのであり，２回の購入時のいずれについても，商品説明や注意事項を確認することなく再度同様の無線ＬＡＮアダプタを購入したなどという供述は不自然であり，到底信用できない。

４　よって，被告人には，出力制限値を超える出力が可能な無線ＬＡＮ接続機器を使用して無線局を開設したことの認識があったと認められる。

（量刑の理由）

被告人は，フィッシングメールや遠隔操作ウイルス等を利用して複数企業のインターネットバンキングの識別符号を不正に取得し，不正ログインやそれに引き続く不正送金を行っている。その他にも，データベースへの攻撃によりメールアドレスを取得したり,遠隔操作ウイルスを送信して実行可能な状態にさせたりもしている。このように被告人は様々な手法を用いてサイバー攻撃を行っている。その上，犯行の発覚を免れるため，あらかじめ不正に取得した暗号化鍵を用いて他人の無線ＬＡＮアクセスポイントへ接続し，ときには中継サーバも経由させて接続元を隠し，また，不正送金の前には連絡用メールアドレスを変更するなどしており，本件犯行の態様は巧妙で悪質である。不正送金による財産的被害は合計５１９万円余りと高額に上っており，その被害結果は大きい。

被告人は，同種前科による前刑の仮釈放後間もなく本件各犯行に及んでいることからすれば，常習性は顕著であり，強い非難に値する。サイバー犯罪が増加し，ネットワーク秩序や電子金融取引の安全を保護する必要が高まっている今日においては，この種事犯には厳正な態度で臨む必要がある。

また，高出力の無線ＬＡＮアダプタを違法に使用した点も軽視はできない。

以上からすれば，被告人の刑事責任は重大であり，被告人が不合理な弁解に終始しており，反省の態度が見られないことなども考慮した上，主文のとおりの刑に処するのが相当であると判断した。

（一部無罪の理由）

第１　無線通信の秘密の窃用の公訴事実等

平成２７年７月１日付け追起訴状記載の公訴事実第１は,「被告人は，Ｑ方に設置して運用する小電力データ通信システムの無線局である無線ＬＡＮルータのアクセスポイントと同人方に設置の通信端末機器で送受信される無線局

の取扱中に係る無線通信を傍受することで，同アクセスポイント接続に必要なパスワードであるＷＥＰ鍵をあらかじめ取得し，平成２６年６月１１日午前１１時２６分頃，松山市 ab 丁目 c 番 d 号被告人方において，同所に設置のパーソナルコンピュータを使用し，前記ＷＥＰ鍵を利用して前記アクセスポイントに認証させて接続し，もって無線局の取扱中に係る無線通信の秘密を窃用したものである。」というものである。

被告人が，同日時頃，Ｑ方無線ＬＡＮアクセスポイントにかかるＷＥＰ鍵を利用して，同アクセスポイントに接続していたことは，証拠上認められるものの，当裁判所は，ＷＥＰ鍵は電波法１０９条１項にいう「無線通信の秘密」にはあたらず，それを利用することが同項違反にはならないと判断したので，以下補足して説明する。

第２　ＷＥＰ等

１　ＷＥＰは，無線通信を暗号化する国際的な標準形式である。その際に用いられる暗号化鍵がＷＥＰ鍵である。

暗号化の過程は概ね以下のとおりである。平文（暗号化したい情報）に，１０４ビットのＷＥＰ鍵と２４ビットのＩＶ（誰にでもわかるようになっている数字）を組み合わせた１２８ビットの鍵をＷＥＰというシステムに入れることでできる乱数列を足し込んで暗号文を作成する。復号するためには，平文に足し込まれた乱数を引く必要があるが，その乱数を知るためには，ＷＥＰ鍵が必要になる。

ＷＥＰ方式の無線ＬＡＮ通信において，ＷＥＰ鍵自体は無線通信の内容そのものとして送受信されることはない。

２　前記（事実認定の補足説明）第２の３に認定のとおり，被告人は，１号パソコンからＲに収録されているＳを用いて，Ｑ方無線ＬＡＮのＷＥＰ鍵情報を取得している。Ｓの攻撃手法はＡＲＰリプライ攻撃と言われるものであり，ＷＥＰ鍵を計算で求める前提として，通信している者が出しているパケットが少な

い場合に，大量のパケットを発生させることで大量の乱数を収集するというものである。

第３　検討

１　電波法１０９条１項の「無線通信の秘密」とは，当該無線通信の存在及び内容が一般に知られていないもので，一般に知られないことについて合理的な理由ないし必要性のあるものをいうと解される。

２　前記のとおり，ＷＥＰ鍵は，それ自体無線通信の内容として送受信されるものではなく，あくまで暗号文を解いて平文を知るための情報であり，その利用は平文を知るための手段・方法に過ぎない。

ＷＥＰ鍵は，大量のパケットを発生させて乱数を得ることにより計算で求めることができるという点では，無線通信から割り出せる情報ではあるものの，ＷＥＰ鍵が無線通信の内容を構成するものとは評価できない。このことは，ＷＥＰ鍵を計算によって求めるためには，必ずしも無線ＬＡＮルータと端末機器との間で送受信されるパケットを取得する必要はなく，ＡＲＰリプライ攻撃によってパケットを発生させることでも足りることからもいえる。すなわち，ＷＥＰ鍵は，無線ＬＡＮルータと端末機器との間で送受信される通信内容の如何にかかわらず，取得することができるのであり，無線通信の内容であるとはいえない。

３　そうすると，ＷＥＰ鍵は，無線通信の内容として送受信されるものではなく，無線通信の秘密にあたる余地はない。

したがって，ＷＥＰ鍵の利用は犯罪を構成せず，結局前記公訴事実については罪とならないから，刑訴法３３６条により，被告人には無罪の言渡しをする。

（求刑　懲役１２年，主文同旨の没収）

平成２９年５月２３日

東京地方裁判所刑事第１６部

裁判長裁判官　　島　　田　　一

裁判官　　島　　田　　環

裁判官　　髙　　野　　将　　人