平成１８年７月３１日判決言渡　同日原本交付　裁判所書記官

平成１７年(ワ)第８３６２号　不正競争行為差止等請求事件

口頭弁論終結日　平成１８年６月１４日

判　　決

神奈川県川崎市多摩区＜以下略＞

原　　告　　A

同訴訟代理人弁護士　　柳　　原　　敏　　夫

東京都千代田区＜以下略＞

被　　告　　株式会社トリニティーセキュリティーシステムズ

同訴訟代理人弁護士　　古　　谷　　誠

同　　小　野　寺　　良　　文

同　　大　　宮　　立

同　　市　　川　　直　　介

主　　文

１　原告の請求をいずれも棄却する。

２　訴訟費用は原告の負担とする。

事　実　及　び　理　由

第１　請求

１　被告は，別紙営業秘密目録記載の営業秘密を使用して，別紙物件目録記載１の製品を製造，販売してはならない。

２　被告は，別紙営業秘密目録記載の営業秘密を使用して，別紙物件目録記載２の製品を製造，販売してはならない。

３　被告は，原告に対し，金５００万円及びこれに対する平成１７年４月２９日から支払済みまで年５分の割合による金員を支払え。

第２　事案の概要

本件は，原告が，被告に対し，被告において，別紙営業秘密目録記載の原告の営業秘密（以下「本件営業秘密」という。）を，原告との間でネットワーク環境における認証システム等の共同開発事業契約を締結していた会社から，不正開示行為であることを知りながら取得し，同営業秘密を利用して別紙物件目録記載１及び２のコンピュータ機器及びプログラムを製造，販売する不正競争行為（不正競争防止法２条１項８号）を行ったとして，同法３条１項に基づく同営業秘密の使用の差止め，同法４条に基づく損害賠償５００万円（一部請求）及び訴状送達の日の翌日である平成１７年４月２９日から支払済みまで民法所定年５分の割合による遅延損害金の支払を求めた事案である。

１　前提となる事実等（争いがない事実以外は証拠を末尾に記載する。）

(1) 原告が代表取締役を務めるジェーシーエヌ株式会社（以下「JCN」という。）と，日本システムハウス株式会社（以下「NSH」という。）は，平成１４年６月３０日，NSHを甲，JCNを乙とし，「乙の開発したTAO TIME認知システムに係る技術（以下本件技術という）に基づき，甲乙共同でP2Pネットワーク環境の下JAVA仕様の認証モジュール製品（以下対象製品という）の開発を行うに先立ち，乙が甲に本件技術を開示し，対象製品の開発の実現性について協議するのに際し，次のとおり契約を締結する。」として，同技術の開示等に関する契約を締結し（甲７），同契約に基づく協議を行った。

(2) 原告，NSH及びJCNは，平成１４年９月１日，原告を甲，NSHを乙，JCNを丙とし，「甲が考案し，設計し，丙が管理するTAO TIME認知・認証・管理システムに係る技術を基に，乙が有する技術を利用し，甲乙丙共同で本契約に定める対象製品を開発することに関し，次のとおり契約する。」として，これらの技術を利用した製品の共同開発契約を締結し（甲８，以下「第一次共同開発契約」という。），同契約所定の共同開発を行った。

(3) さらに，原告，NSH及び株式会社NAD研究所（以下「NAD」という。）は，平

成１５年７月３０日，原告を甲，NSHを乙，NADを丙とし，「甲が発明し，考案し，設計し，丙がその管理を行うQrAS認知・認証・管理システムに係る技術（以下本件技術という）を基本に，これに乙の有する技術を加え甲乙丙共同で本契約に定める対象製品を開発することに関し，次の通り契約する。」として，これらの技術を利用した製品の共同開発契約（甲９，以下「第二次共同開発契約」という。）及び同契約に基づく覚書を締結し（甲１０），同契約所定の共同開発を行った。

同契約７条には,「甲乙丙は本件技術および本件開発並びに対象製品に関する技術情報，相手方の営業情報などの機密情報について，第１条の目的以外には使用せず，本契約の有効期間中および本契約が終了した後といえどもその秘密を保持しなければならない。」旨の秘密保持義務が定められている。

(4) 被告は，平成１６年１月５日，NSHを吸収合併した。

(5) 被告は，平成１６年３月１８日，別紙物件目録記載１(1)の製品（正式の製品名は「IPNセキュア・プラットフォーム　ゲートウェイタイプ」，製品番号は「IPGWP010」及び「IPGWP020」である。以下，これらを併せて「被告製品１」という。）合計６８台（IPGWP010につき３１台，IPGWP020につき３７台）を，販売総代理店に１台約２０万円で販売した。

(6) さらに，被告は，平成１６年１０月，別紙物件目録記載２(1)の製品（以下「被告製品２」という。）を発表し（甲１７），発売準備を行っている。

また，被告は，被告製品２のソフトウェアタイプとして，別紙物件目録記載２(2)の製品（以下「被告製品３」という。）を開発し（甲５７），販売する予定である。

２　争点

(1) 本件営業秘密が，不正競争防止法２条６項にいう営業秘密に当たるか（争点１）。

(2) 被告が同法２条１項８号の行為を行ったか（争点２）。

(3) 原告の損害はいくらか（争点３）。

３　争点についての当事者の主張

(1) 争点１（本件営業秘密が，不正競争防止法２条６項にいう営業秘密に当たるか）について

（原告の主張）

ア　非公知性

本件営業秘密の内容である認証技術が，原告自らが出願し（特願２００２－１８４７５０号)，公開された特許出願（特開２００３－１０１５３４号）に係る公開特許公報（乙９。以下「本件公知例」という。）にすべて開示されており，公知であるとの被告の主張は，争わない。

イ　秘密管理性

第二次共同開発契約の当事者であったNADは，原告の個人会社であり，本件営業秘密は，原告のみがその情報にアクセスできる体制にあるから，秘密管理性を有する。

ウ　有用性

認証システム製品としては，これまでワンタイムパスワードが主流であったが，これはハードウェア仕様であったためにイニシャルコストが高く，また，認証管理サーバを設置しメンテナンスをしなければならないというランニングコストの問題があったところ，本件営業秘密は，これらの問題を解決するために，ソフトウェア仕様で認証システムを実現し，なおかつクライアントがサーバを認証するという双方向認証を実現することにより，認証管理サーバを不要にした。さらに，ユビキタス社会に不可欠なP2P対応のファイル配信ビジネスにおいて，SOHOユーザ又は個人ユーザにとっても意味があり，有用性を有する。

（被告の反論）

本件営業秘密の内容となる認証技術は，本件公知例（乙９）にすべて開示

されており，公知である。

また，このように公知の技術を秘密として管理することも不可能なので秘密管理性もない。

したがって，本件営業秘密は，不正競争防止法２条６項にいう「営業秘密」に該当しない。

(2) 争点２（被告が不正競争防止法２条１項８号の行為を行ったか）について

（原告の主張）

ア　NSHから被告への不正開示行為

原告開発に係る認証アルゴリズムに関する機密情報は，以下の書面の交付等により，平成１５年５月ないし同年８月ころ，NSHの事業部長石井一夫らから被告の開発責任者へ開示された。

（ア）　QrAS_C言語仕様書（同年５月ころ原告とNSHの共同作成）

（イ）　QrAS_SDK取扱説明書（同上）

（ウ）　QrAS_SDK評価キット一式（同上）

（エ）　QrAS_SDK　Cソースコードプログラム一式（同上）

（オ）　QrAS_SDK　デバッグツール一式（同上）

（カ）　QrAS　自律分散認証アルゴリズムSDK　Ver3.0概要仕様書02版(同年６月１６日原告とNSHの共同作成）

（キ）　説明資料「自律分散認証アルゴリズムQrASとは？」(Ver0.1)（同年２月１９日原告作成）

（ク）　技術解説書「無線LAN企画・n対nバージョン」（平成１４年１１月２１日原告作成）

（ケ）　Pure P2P型自律分散認証アルゴリズム論文（同年７月３０日原告作成）

イ　被告は，ア記載のNSHの行為が第二次共同開発契約７条に定める秘密保持義務に違反する不正開示行為であることを知りながら，NSHから，原告開発

に係る認証アルゴリズムを開示され，平成１６年３月に，被告製品１を少なくとも６８台（IPGWP010を３１台，IPGWP020を３７台）販売した。

このように，被告が，原告開発に係る認証アルゴリズムをNSHから開示され，本件営業秘密を搭載した被告製品１を開発，製造，販売したことは，不正競争防止法２条１項８号の不正競争行為に該当する。

また，被告は，同年６月から，第二次共同開発契約７条の秘密保持義務に違反し，原告開発に係る認証アルゴリズムを，同契約１条に定める共同開発等以外の目的に使用して，本件営業秘密を搭載した被告製品２及び３を開発し，製造する不正競争行為を行った。

（被告の反論）

ア　原告は，第一次及び第二次共同開発契約に基づき，平成１４年６月ころから平成１５年１２月まではNSHに，NSHと被告が合併した平成１６年１月以降同年４月までは被告に，それぞれ常駐あるいはこれと同視できる状況で，NSH又は被告と共同開発を行っていたのであり，本件紛争に至る以前に，被告製品１の開発，製造，販売について異議を申し述べたことは一度もなかった。

そして，NSH及び被告は，原告に対し，平成１６年４月３０日までに，第一次及び第二次共同開発契約に定める対価として，合計３５５０万円を支払済みである。

被告は，第一次及び第二次共同開発契約に従って，原告から適法に原告開発に係る認証アルゴリズムの開示を受けてこれを被告製品１に搭載したものである。また，被告は，第一次及び第二次共同開発契約の契約上の地位をNSHから承継しているので，同契約に基づいて平成２０年７月２９日まで被告製品１を単独で販売できる権限を有している（甲９，１２条１項，１３条）。

このように，被告による被告製品１の開発，製造，販売は，適法な許諾

に基づくものであって，当該行為が不正競争防止法２条１項８号に定める不正競争行為に該当することなどあり得ない。

イ　被告製品２及び３においては，認証アルゴリズムとして原告開発に係る認証アルゴリズムではなく，別途開発された動的パスワード認証方式が使用されている。

原告は，本件営業秘密が被告製品２及び３のどこに搭載されているのか具体的に主張していない。

ウ　原告は，不正競争防止法２条１項８号にいう，被告の悪意・重過失も主張していない。

エ　さらに，被告は，別紙物件目録記載１(2)ないし(7)の製品については，製造も販売も行っていないし，将来これを製造・販売する予定もない。原告も，これらの製品に対する差止請求権の根拠について，何ら主張をしていない。

(3) 争点３（原告の損害はいくらか）について

（原告の主張）

ア　被告製品１の開発，製造，販売

被告は，平成１６年３月に，被告製品１を少なくとも６８台（IPGWP010を３１台，IPGWP020を３７台）販売した。

上記販売後，本件訴訟提起までの約１年以上の期間の経過を考えれば，被告製品１の販売台数が合計で３００台を下ることはない。また，その価格は約２０万円である。

他方，第一次共同開発契約９条には実施料の基本が定めてあり，これを参考にして計算すれば，本件営業秘密の無断使用に基づく被告製品１の開発，製造，販売による原告の損害は，

２０万円×３００台×（７＋３．５）％＝６３０万円

を下らない。

イ　被告製品２及び３の開発，製造，販売

被告製品２及び３が前記被告製品１と同等の性能であり，にもかかわらず，販売価格が約５倍することを考えると，平成１６年１２月の発売より約５か月間で，販売台数が３０台を下ることはない。

前記被告製品１と同様の計算方法により計算すれば，本件営業秘密の無断使用に基づく被告製品２及び３の開発，製造，販売による原告の損害は，

９８万円×３０台×１０．５％＝３０８万円（万未満切り捨て）

を下らない。

ウ　慰謝料

原告は，NSH及び被告を，最も信頼する共同事業のパートナーとして，原告が手塩に掛けて発明してきた本件営業秘密を開示し，その事業化の成功のために運命を共にしてきたにもかかわらず，一方的に裏切られるという結果となり，なおかつ，本件訴訟提起前の１年にわたる交渉においても，被告の態度によって原告の被った精神的苦痛は測り難い。それゆえ，原告の被った精神的苦痛を慰謝するための慰謝料の金額は，少なくとも１０００万円を下らない。

エ　弁護士費用

原告は，上記の経緯からやむなく本件訴訟を提起したものであり，前記賠償金額や本件訴訟遂行の難易度等に照らし，弁護士費用は少なくとも５００万円を下らない。

オ　原告は，被告に対し，これら損害合計２４３８万円のうち，一部請求として，５００万円及びこれに対する訴状送達の日の翌日である平成１７年４月２９日から支払済みまで民法所定年５分の割合による遅延損害金の支払を求める。

（被告の反論）

争う。

第３　当裁判所の判断

１　争点１（本件営業秘密が，不正競争防止法２条６項にいう営業秘密に当たるか）について

(1) 本件訴訟は，平成１７年４月２６日に提起され，同年６月２０日に第１回口頭弁論期日が開かれた後，弁論準備手続に付され，主に原告が主張する営業秘密の特定をめぐって双方の主張が行われた。そして，原告は，平成１８年６月１４日の第８回弁論準備手続期日において，被告の不正競争行為の対象となる営業秘密について，本件営業秘密のとおり特定した。

上記期日において，被告から，本件営業秘密の内容である認証技術は，本件公知例にすべて開示され，公知である旨主張されたのに対し，原告は，これを争わないと陳述した。

(2) 不正競争防止法における「営業秘密」は,「秘密として管理されている生産方法,販売方法その他の事業活動に有用な技術上又は営業上の情報であって,公然と知られていないものをいう」とされており（同法２条６項),「公然と知られていない」ものであることが要件とされる。

しかし，本件営業秘密の内容である認証技術が，原告自らが出願した本件公知例にすべて開示されている公知のものであるとの被告の主張に対し，原告は，上記のとおり，これを争わないとし，そのほか，本件営業秘密が「公然と知られていない」ものであることについて何ら主張，立証を行わない。

そうすると，本件営業秘密は,「公然と知られていない」ものであるとは認められず，不正競争防止法２条６項にいう営業秘密には当たらないというべきである。

(3) よって，その余の点について検討するまでもなく，原告の主張はいずれも理由がない。

２　以上のとおりであるから，その余の争点について判断するまでもなく，原告の請求は，いずれも理由がないから，これらを棄却することとして，主文のと

おり判決する。

東京地方裁判所民事第２９部

裁判長裁判官　　清　　水　　節

裁判官　　山　　田　　真　　紀

裁判官　　片　　山　　信

（別紙）

営業秘密目録

「１対nによる」接続形態における「P to P」機能を実現するための，下記「独自のタイムスタンプ値生成技術」及び「タイムスタンプを元にした認証データ生成／認証技術」

第１　独自のタイムスタンプ値生成技術

１　クライアントからの要求送信

①　クライアントは，サーバに対して要求を送信する。クライアントは，同時に，

（ｉ）　前回の「クライアント要求送信タイムスタンプ値」

（ii）　前回の「クライアント応答受信タイムスタンプ値の隠蔽値」

（iii）　前々回の「クライアント応答受信タイムスタンプ値の隠蔽値の復号値」の３つの値をサーバに対して送信する。ただし，クライアントとサーバが初めて送受信を行う場合などは，前回あるいは前々回といった過去の通信履歴を持たないため，値は「０」を送信する。

２　サーバの要求受信

②　サーバは，クライアントからの要求を受信する。同時にクライアントから送信された，

（ｉ）　前回の「クライアント要求送信タイムスタンプ値」

（ii）　前回の「クライアント応答受信タイムスタンプ値の隠蔽値」

（iii）　前々回の「クライアント応答受信タイムスタンプ値の隠蔽値の復号値」の３つの値をサーバが保有するデータベースに格納する。

③　サーバは，任意の乱数Ｓを生成する（又は，コンピュータの現在時刻を示すシリアル値Ｓを取得する。）。

④　サーバは,③で生成したＳと前回クライアントとの通信の際に生成した「共有値」とを比較し,

・　（前回生成した「共有値」＋３）≦Ｓであれば，Ｓを今回の「共有値」とする

・　（前回生成した「共有値」＋３）＞Ｓであれば,（前回生成した「共有値」＋３）を今回の「共有値」とする

・　クライアントと初めて通信する場合などは，前回生成した「共有値」が存在しないため，Ｓを今回の「共有値」とする

⑤　サーバは，④で得られた「共有値」をサーバが保有するデータベースに格納する。

⑥　サーバは，前々回までのクライアントとの通信における,「クライアント応答受信タイムスタンプ値」と「クライアント要求送信タイムスタンプ値」の差の合計値である「累積差分」を算出する。ただし，クライアントと初めて通信を行う場合や，２回目の通信の場合は，前々回までのクライアントとの通信が存在しないため,「累積差分」は０とする。そうでない場合,「累積差分」は以下の手順で算出する。

（ⅰ）　②で受信した前々回の「クライアント応答受信タイムスタンプ値の隠蔽値の復号値」を利用して，前々回の「クライアント応答受信タイムスタンプ値の隠蔽値」を生成する際にデータベースから任意に抽出した値Ｘを算出する。

（ⅱ）　前々回の「クライアント応答受信タイムスタンプ値」＝前々回の「クライアント応答受信タイムスタンプ値の隠蔽値」－（ⅰ）で算出した値Ｘの式により，前々回の「クライアント応答受信タイムスタンプ値」を求める。

（ⅲ）　（ⅱ）で求めた前々回の「クライアント応答受信タイムスタンプ値」から，前回通信時にクライアントからサーバへ送信された前々回の「クラ

イアント要求送信タイムスタンプ値」の差を求める。

（ⅳ）「累積差分」＝前回算出した「累積差分」＋（ⅲ）で求めた差

の式により「累積差分」を求める。

⑦ サーバは，前回の「サーバ要求受信タイムスタンプ値」を，次の式により生成する。

前回の「サーバ要求受信タイムスタンプ値」＝前回の「共有値」＋「累積差分」

次に，この式により生成した「サーバ要求受信タイムスタンプ値」を，サーバが保有するデータベースに格納する。

⑧ サーバは，今回の「共有値」をクライアントに送信する。

3 クライアントの応答受信

⑨ クライアントは，サーバから応答を受信する。同時にサーバから送信された「共有値」を受信して，クライアントが保有するデータベースに格納する。

⑩ クライアントは，過去にサーバと行った送受信の際の「クライアント応答受信タイムスタンプ値」と「クライアント要求送信タイムスタンプ値」の差の合計値である「累積差分」を算出する。ただし，過去に送受信を行った履歴が存在しない場合は，「累積差分」を０とし，そうでない場合は，前回クライアント内で算出した「累積差分」に前回通信の際の「クライアント応答受信タイムスタンプ値」と「クライアント要求送信タイムスタンプ値」の差を加算して，「累積差分」を算出する。

⑪ クライアントは，①で行った今回の「クライアント要求送信タイムスタンプ値」を，次の式により生成する。

今回の「クライアント要求送信タイムスタンプ値」＝（⑨で受信した「共有値」－１）＋⑩で算出した「累積差分」

⑫ クライアントは，今回の「クライアント要求送信タイムスタンプ値」をクライアントが保有するデータベースに格納する。

⑬　クライアントは，任意の乱数αを生成する。

⑭　クライアントは，クライアントが保有するデータベースに格納されている値からランダムに値を抽出する。

⑮　クライアントは，ランダムに抽出した値の位置を示す値βを確定する。

⑯　クライアントは，⑨でサーバからの応答を受信した際のタイムスタンプ値である今回の「クライアント応答受信タイムスタンプ値」を次の式により生成する。

今回の「クライアント応答受信タイムスタンプ値」＝⑫で生成した「クライアント要求送信タイムスタンプ値」＋⑬で生成した乱数α

⑰　クライアントは，今回の「クライアント応答受信タイムスタンプ値」をクライアントが保有するデータベースに格納する。

⑱　クライアントは，次の式により，今回の「クライアント応答受信タイムスタンプ値の隠蔽値」を生成する。

今回の「クライアント応答受信タイムスタンプ値の隠蔽値」＝⑯で生成した今回の「クライアント応答受信タイムスタンプ値」＋⑭でランダムに抽出した値

⑲　クライアントは，⑱で生成した今回の「クライアント応答受信タイムスタンプ値の隠蔽値」と，⑮で確定したランダムに抽出した値の位置を示す値βをデータベースに格納する。

第２　タイムスタンプを元にした認証データ生成／認証技術

１　「クライアント識別子」の生成

①　クライアントは，前回の「クライアント要求送信タイムスタンプ値」と前々回の「クライアント応答受信タイムスタンプ値」の差分を求める。もしクライアントに前回の「クライアント要求送信タイムスタンプ値」が存在しない場合，値は０とする。同様に，前々回の「クライアント応答受信タイムスタンプ値」が存在しない場合，値は０とする。

② クライアントは，次の式により，「クライアント識別子」を生成する。

「クライアント識別子」＝前回サーバから送信された「サーバ識別子」－①で求めた差分

の式によって求める。前回サーバから送信された「サーバ識別子」が存在しない場合は，値は０として計算する。

次に，クライアントは，生成した「クライアント識別子」をクライアントが保有するデータベースに格納する。

③ クライアントは，②で生成・格納した「クライアント識別子」をサーバに送信する。ただし，「第１　独自のタイムスタンプ値生成技術」で述べたタイムスタンプ値生成手順（アルゴリズム）と併せて行われるため，クライアントからサーバへ送信されるデータは，

ア　前回の「クライアント要求送信タイムスタンプ値」

イ　前回の「クライアント応答受信タイムスタンプ値の隠蔽値」

ウ　前々回の「クライアント応答受信タイムスタンプ値の隠蔽値の復号値」

エ　「クライアント識別子」

となる。

２　サーバ内部での「クライアント判断子」の生成

④ サーバは，前回の「サーバ要求受信タイムスタンプ値」と前々回の「サーバ要求受信タイムスタンプ値」の差分を算出する（以下「差分Ａ」という。）。

⑤ サーバは，「第１　独自のタイムスタンプ値生成技術」で述べたタイムスタンプ値生成手順（アルゴリズム）に基づいて，③でクライアントから送信された前々回の「クライアント応答受信タイムスタンプ値の隠蔽値の復号値」から，前々回の「クライアント応答受信タイムスタンプ値」を算出する。

⑥ サーバは，③でクライアントから送信された前回の「クライアント要求送信タイムスタンプ値」と⑤で算出した前々回の「クライアント応答受信タイムスタンプ値」の差分を算出する（以下「差分Ｂ」という。）。

⑦　サーバは，次の式により，「クライアント判断子」を生成する。

「クライアント判断子」＝前回の「クライアント識別子」＋（差分Ａ－差分Ｂ）

の式によって求める。

⑧　サーバは，次の方法により，認証を行う。認証は，③にてクライアントから送信された「クライアント識別子」と⑦において生成した「クライアント判断子」の比較によって行う。

・「クライアント識別子」＝「クライアント判断子」であれば認証OK

・「クライアント識別子」＜＞「クライアント判断子」であれば認証NG

・　認証OKであれば，引き続き，以下の手順を実施する。

３　「サーバ識別子」の生成

⑨　サーバは，前回の「サーバ要求受信タイムスタンプ値」と前々回の「サーバ要求受信タイムスタンプ値」の差分を算出する。

⑩　サーバは，次の式により，「サーバ識別子」を生成する。

「サーバ識別子」＝前回の「クライアント識別子」＋①で算出した差分

次に，サーバは，生成した「サーバ識別子」をサーバが保有するデータベースに格納する。

⑪　サーバは，「サーバ識別子」をクライアントに送信する。

ただし，「第１　独自のタイムスタンプ値生成技術」で述べたタイムスタンプ値生成手順（アルゴリズム）と併せて行われるため，サーバからクライアントへ送信されるデータは，

ア　「共有値」

イ　⑩で生成した「サーバ識別子」

となる。

４　クライアント内部での「サーバ判断子」の生成

⑫　クライアントは，前回の「クライアント要求送信タイムスタンプ値」と前

々回の「クライアント応答受信タイムスタンプ値」の差分を算出する。

⑬　クライアントは，次の式により，「サーバ判断子」を生成する。

「サーバ判断子」＝②で生成した「クライアント識別子」＋⑫で算出した差分

⑭　クライアントは，次の方法により，認証を行う。認証は，⑪にてサーバから送信された「サーバ識別子」と⑬において生成した「サーバ判断子」の比較によって行う。

- 「サーバ識別子」＝「サーバ判断子」であれば認証OK
- 「サーバ識別子」＜＞「サーバ判断子」であれば認証NG

（別紙）

物件目録

1　次のコンピュータ機器又はコンピュータプログラム

(1) 製品名を「IPN Gateway（製品番号：IPNGWP010, IPNGWP020)」とするコンピュータ機器

(2) 製品名を「IPN Gateway　ソフトウェアタイプ」，又は「ソフト　IPN」とするコンピュータプログラム

(3) 製品名を「IPN-NIC」とするコンピュータ機器

(4) 製品名を「IPN-Chip」とするコンピュータ機器

(5) 製品名を「IPN-Box」とするコンピュータ機器

(6) 製品名を「IPNポリシーサーバLight」とするコンピュータ機器

(7) 製品名を「IPNポリシーサーバStandard」とするコンピュータ機器

2　次のコンピュータ機器又はコンピュータプログラム

(1) 製品名を「IPNTK」とするコンピュータ機器

(2) 製品名を「IPN-WIN」とするコンピュータプログラム