[From introducer of this article] This article was presented at “Oslo Meeting” on Nov. 16, 2009, which is the reunion meeting of the Japanese delegates to the 11th CCIR General Assembly held in Oslo, Norway in 1966. The author, Dr. Ikegami, had conducted his research work of radio communications a total for 50 years, namely, at Ministry of Telecommunications and Electrical Communication Laboratory of NTT Public Corporation (28 years), Kyoto University (14 years) and Takushoku University(8 years). Now Dr. Ikegami is Professor Emeritus of Kyoto University and Takushoku University (see Fumio Ikegami: “My Researcher’s History”, IEICE Communications Society Magazine, No. 6, pp. 4-10, Autumn, 2008 (in Japanese)). About this article, Dr. Ikegami says, “Since the theme of this article is a special problem in the communication technologies, most of people may wonder if this issue is reasonable, while some people may agree with me. Further, I am not a specialist in this field, so I hope that young researchers are interested in this kind of issue on telecommunication network and correct misunderstandings in my argument”. A discussion of all of you is expected. *(Takashi Iida, JFSC Special Advisor)*

Reconsidering Future of World Communication Network

—The Internet: One Step from Suspicion toward Conviction—

Fumio Ikegami

[Foreword]

It seems strange that the basic risk of the Internet Protocol Network (abbreviated as “IPNet” hereafter), which comes from “Best Effort" of the IPNet, has not been argued. Though I have felt some doubt on this point for these several years, recent move toward NGN [1] and President Obama’s remarks reported in May 2009 [2] pushed my suspicion toward conviction by one step. I tried to reconsider from the beginning. Why did circuit switching network (the old network) turned to the new IPNet with a sudden logical leap? Can the discontinuity of this leap be resolved and then be connected to the future world network? Although there is some move from IPNet to a new network [3], argument on the basic defect of IPNet has been rarely seen. I feel something important is missing. The reconsideration predicts that the IPNet may fail in due time. What should we do now? I am worrying about the future communications network as an old layman, though it’s none of my business now.

1. Proposed Issue

The ARPANet, which began as an anti-nuclear-attack measure network of the US Armed Forces, was used as a computer network between universities and/or research institutes in the US (1969), and as a similar network in Japan (JUNET, 1984), and then it was commercialized as the Internet in US (1988). Since that time, it continues explosive expansion as a part of world public network, and is expected to be a candidate of the final future network. This is because the new network is less expensive and much more convenient particularly for digital communications when compared with the old network. However, IPNet has the grave defect that cannot guarantee Quality, Reliability and Security (QRS) of the network. Now, let us focus our attention on this point.

It is because of the contract of IPNet, that the service provider can be liberated from the duty to guarantee the QRS of services, when the provider made the best effort for the service. This nature of the contract is called by the name of “Best Effort” giving rise to the serious fundamental defect, which cannot guarantee the QRS of IPNet.

One of the problems is ‘security’. Because IPNet cannot guarantee to keep the secret of the information that needs high secrecy, there is apprehension that the IPNet cannot meet the qualifications for a public telecommunication network. Furthermore, there is no guarantee of Q and R also. This means that the performance of the IPNet may not be defined definitely or

quantitatively. In other words, we could say that IPNet is lack of logicality or is of illogicality. As for security, quantitative indication might be difficult. But, as for Q and R, quantification is quite indispensable for a public communication network.

[Security Issue]

The old circuit switching network was designed to keep the communication security first. As an exclusive line is connected between the two terminal points before communication starts, no disturbance from the outside can be made during communication in principle.

On the other hand, an open IPNet does not guarantee security. Although high security can be maintained when used as a closed IPNet, security may be lost again when connected to an open network, even in a case connected via filter or fire wall. The damages due to spam mail and vicious cyber attack occur frequently in the network. Some of these attacks can be evaded by safety measures software, but a new type of attack appears in sequence, falling into a vicious spiral of attack and measure.

Furthermore, free opinions stated in the IPNet can sometimes hurt the human relations. We see many incidents resulted in tragedy due to careless self-disclosure or anonymous slander and so on. Though this is a problem of human ethic, technology must be responsible for the essential risk of the open IPNet. And, perhaps the society must take the responsibility for giving strong warning to the public on this point.

Cyber Attack to the government and companies seems to have given considerably serious damage, but the disclosure of the concrete contents to the public has been hesitated, probably because considering the influence to the Internet business and to the USA. Most of communication engineers seem to make a gesture of thinking that "New technology always comes together with the damage of this level. I suppose most users are glad to use it". The actual damage situation seems to get clearer since President Obama disclosed the damage in the USA [2].

[Illogicality Related Problem]

The circuit switching network has reached a stage to be able to calculate, design and realize a communication network that almost satisfies the required international standard characteristics (QRS). It is supported by the studies such as mathematics, physics, statistics, electrical and electronic engineering, communication engineering and so on, which the human beings have accumulated for several centuries. Though not always completed, there are universal proofs confirmed for the physical phenomena of switching, transmitting and receiving in the network. Based on them, the required characteristics can be calculated and designed, and new methods can approach to the various broad applications.

On the other hand, the IPNet is based only on a simple and abstract logic for packet connection. Since there is no universal theory that gives the basis of the packet switching network, the quantitative calculation of physical characteristics QR of network is not possible, including transmission loss, delay characteristics and probability of blocking due to traffic congestion. The network characteristics can be evaluated only by a method to repeat communication experiments many times on a real network. Therefore, it is not possible to make an economical optimum system design.

In other words, all kinds of the network management, such as design･construction･operation, and the progressive studies such as improvement or expansion of the IPNet cannot be done reasonably, due to lack of background theory. Then, we may have a question how the current IPNet was born. The answer is simple. It borrowed the past circuit switching network. It is not a network that was designed especially for the IPNet. The present IPNet is an existence that seems to be so called “Hermit crab”, which cannot be independent by itself. I could say that it is a mysterious technology beyond our common sense.

2. Present and Future of IP Network

Why was the IPNet operated without a fatal difficulty in its early stage? It is because

traffic congestion rarely occurred, as the speed of optical fiber (Gigabps) borrowed from the old network was fast enough for transmission of most traffic of e-mail or file (kByte～MByte) .

However, it is said at present that 90% of e-mails are spam, and traffic increases rapidly year by year due to moving images (GByte) transmitted on YouTube and moreover by use of file exchange software Winny, for example. Thus, the probability that traffic exceeds the ability of optical fiber and router increases nowadays. The Ministry of Internal Affairs and Communications reported that the total traffic of the IPNet reached the order of Terabps in 2007 and is increasing every year nearly with the Moore's Law (principle of increasing rate of transistor number per IC chip: double every 18 to 24 months). Network congestion is apt to occur more frequently in parallel with recent increase of traffic, which forces ISP (Internet Service Provider) to control the traffic by warning a user who sends an extraordinary amount of information to cancel the contract [3].

Now the number of users treating moving images increases, and then the traffic will be increasing also. Assuming that traffic increases with the Moore's Law, the predicted multiple factor required for the IPNet ability is shown in Table 1.

Table 1. Yearly Change of a Multiple Factor Required for IPNet Ability .

						Case A: Double/2 years				
Passed Year	2	4	6	8	10	12	14	16	18	20
Multiple of Ability	2	4	8	16	32	64	128	256	512	1024
						Case B: Double/1.5 years				
Passed Year	1.5	3	4.5	6	7.5	9	10.5	12	13.5	15
Multiple of Ability	2	4	8	16	32	64	128	256	512	1024

From Table 1, the ability of IPNet composed of optical fiber and router must be raised up to around 10 times the present value after 5~7 years from now, and about 100 times after 10~13 years. After 15~20 years, the traffic is estimated to reach the order of Peta (10^{15}) bps, that means about 1,000 times ability is to be required.

Although I am not so familiar with the present status and the provision of optical fiber and router technologies, the IPNet would fail if its ability cannot satisfy the requirements given in Table 1. Moreover, when the present TV broadcast via radio waves is substituted by that via IPNet sooner or later, real time streaming TV broadcast signal may accelerate a collapse of the present IPNet.

Even if the capability of IPNet could be upgraded to meet the requirements in Table 1, will the myth "Transmission cost of the Internet can be negligible." be still acceptable? "The IPNet which is not worthy of the name of technology" cannot find logically how to solve the problems caused by rapid increase of traffic. There are measures of next generation networks (NGN and so on), but there is not so much prospect to be a complete solution for the time being. I am afraid that the practice of logical prediction and measures for the future may not be feasible, as far as we use Internet Protocol. For fundamental resolution of the problem, it may be necessary to reexamine the problems much more logically. We should go back to the basics once again, and restart for the fundamental reconsideration of the IPNet.

3. Comparison of Characteristics of Circuit Switching Network and IP Network

The performance of circuit switching network is clear physically and is very easy to understand. On the other hand, it is extremely difficult for a layman to understand the performance of IPNet physically. It is because the IPNet has no basis to stand on physically nor mathematically. For reconsideration, it will be helpful to understand the abstract characteristics of IPNet at least. For easier understanding, the characteristics of IPNet are compared with the well-known properties of circuit switching network, as shown in Table 2, where red parts indicate the deficits of respective network. What we should pay particular

attention to is that important items of both networks are mutually exclusive (antinomy).

Table 2 Comparison of Main Property of Circuit Switching Network and IP Network

	Circuit Switching Network (Old Network)	Internet Protocol Network (IP Network)
Basic Motivation	Basic service: Telephone and telegraph for the public. Security is the first priority.	Computer network: To avoid breakdown of whole network in case of a failure of node switching station.
Operation Structure	Central control system: Node switching station monitors and controls the covering network.	Distributed autonomous control system: Each terminal controls operation of network by itself.
Security of Network	End-to-end exclusive line between the two terminals is connected before communication starts. It assures 100% security in principle.	Logical separation of time-division-multiplex signals in packet switching network may lose security against external disturbance.
Network Performance (Q and R)	Q and R are given theoretically, as signal transmission path is definite and fixed.	Q and R are not well defined, as signal path may vary with time in packet switching network.
Blocking due to Traffic Congestion	Blocking ratio is calculated by Erlang's equation, as transmission path is definite.	No theoretical prediction method is obtained at present for the case of packet switching network.
Flexibility for style of information	Fitted to fundamental end-to-end communication. Flexibility for various digital applications is limited.	Superior in flexibility for large variety of digital information styles, for very wide application fields.
Cost of Network	Transmission cost is high, as transmission efficiency is low. Switching equipment costs high, as the function is more complex.	Transmission cost is low, as transmission efficiency of 100% is mostly available. Functions of router and server are simple and cost low.

4. Looking for Source of IP Network Problem

When the feasibility of a new technology in "research" stage is confirmed to be high sufficiently, its stage is raised up to "development" stage. Since many human resources and expenses are needed for "development", no failure is permitted. So, it is essentially required to confirm not only realization of the required performance but also the mutual influence between the new technology and the society. The rapid progress of communication since the late 20th century has told us useful advices how the new communication technology gave positive and negative influences on the society. Why did the discontinuous leap of the basic logic of communication network from circuit switching network to IPNet occur? Now, I recall the past pioneer's unforgettable words: **"**"Research" and "Development" (in R&D) should be strictly distinguished.**"**

[Mistake in Development of IP Network]

IPNet is one of the examples that new technology was born by a new principle not existed in the past. If a researcher of the communication field develops a new technology essentially different from the past one, he would not suffer from so much difficulty due to technical discontinuity. On the other hand, if a researcher, who used to be engaged in a technical field different from communication, tries to work on "development" of a new communication technology, there would be a considerable risk due to lack of knowledge and/or experience on communication and its environment.

In the case of IPNet, there was a misjudgment in the study program, namely the transition of stage from “research” to “development” was made without confirming the completion of the “research” stage. The causes are the followings.

(1) Since IPNet was originally devised (it is told) as a computer network for the US anti-nuclear-weapon measures, most of the researchers in the early stage are supposed to be the experts in the IT field, who had not enough knowledge and experience to practice the management of public communication network. For example, they might have misunderstood simply that a computer network could be used just same as a communication network in practice.
(2) Since the future of IPNet cannot be predicted theoretically due to its illogicality, there was no way to confirm its feasibility besides the experiments on ARPANet. As the results of the experiments were quite satisfactory, the IPNet project went up to “development” stage without proper criticism.
(3) AT&T, that had the highest technology at the time, was prohibited a study of data communication by FCC according to the Anti-trust Laws, and was excluded from this study project. If the Bell Laboratory, mother of the philosophical concept of “R&D”, joined this project, the mistake could have been avoided.
(4) Probably there was critical trend against IPNet among communication network researchers at that time, but on the other hand, the US FCC gave strong support of economy and policy for the new fields of Information Technology.
(5) In addition, there was a tendency to have got tired of the “de jure” standards by ITU since the late 20th century, and to turn toward the “de facto” standards particularly in the field of Information Technology. It is felt that the discontinuous change of network occurred in relation with the tendency to “de facto” and perhaps partly concerned with the attitude of US government overlooking the UN.

In this way, IPNet started as a public communication network in an immature form, but almost no traffic congestion occurred in the early time, because the traffic was small compared with the network capability as mentioned above. The preferable test results in the earlier stage gave an optimistic prospect, quite free from the necessary care about the risks of future failures as shown in Table 1.

ISPs try to regulate the users who send extraordinary amount of information, as a measure to reduce rapid increase of traffic for the moment [3]. However, a measure of this level is not effective enough, because of the following reason. Our “virtual world" is an ideal society of the ethical doctrine that human nature is fundamentally good. But it is nothing but a vacant wish. As a matter of fact, it means that we live in this “real world” without law and police. We must face the reality that there is no effective way to protect various kinds of malicious actions in the real world. As a member of the researchers in the communication field, I am deeply ashamed of the current situation that the surging waves of risky IPNet are covering the whole world, because of improper management of “R&D” in communication network technology.

[Lessons from World Financial Collapse]

We are now just in the midst of a big economic depression once in 100 years. In order to find the origin of the collapse, it is said that we must go back to the Nobel Prize winners’ stochastic achievements of financial engineering to isolate and evade the risks in financing activities. In this case, there was the fine backbone theory, but probably someone in charge of handling the project could not understand a technical skill of the theory correctly. Originally, finance business is called “the world without logic” and “a fight between human desire and risk”. In this situation, we could say that even the persuasive power based on the logic worthy of Novel Prize could not work well to show its expected results.

On the contrary, there is no backbone theory for the current IPNet, and moreover the risks of “Best Effort" are well-known. When a thing without the logic continues swelling out, it explodes by all means. I cannot help worrying that IPNet may repeat an incident similar to the

case of the financial failure, when the whole communication networks in the world are composed of IPNet. When a communication failure occurs, the influence to the society might be more serious than that of financial collapse, with much more widespread reactions to the human living.

Every time I think of the future of communication, I regret that the structure of IPNet would have been quite different from the present one, if engineers of AT&T had participated in the development of IPNet from the earliest stage, though I know it's of no use now. But we should never give up.

5. A Desirable Way of Thinking for Future Communication Network

What is a desirable future communication network? The old (conventional) network and the IPNet have opposite characteristics and have both advantages and disadvantages, as shown in Table 2. I am afraid that no desirable result will be obtained with a method which combines two opposing networks into one network, for example, by putting together both advantages or by adding them and dividing by two. Therefore, necessity of a completely new "third system" such as a system drawn on "Clean Slate" is fully agreeable, if possible.

Then, what will be a "Clean Slate" system? Now, let me try to continue my consideration, faintly hoping that a hint to the solution might be found at least.

[Relationship between Structures and Characteristics of Both Networks]

The opposite structure of both networks is seen in the item of "Operation structure" in Table 2. The old network is a centralized system in which a central switch monitors and controls the network, while IPNet is a distributed autonomous system of terminals.

In a centralized system, a switchboard monitors and controls the network automatically or artificially when needed, so that the network keeps proper performance. On the other hand, IPNet is devised so as to maintain the network function when a switching station is destroyed. As functions for monitoring and controlling are unnecessary, routers and servers are simple and the cost of switching device can be cheaper compared with a centralized system. In other words, both networks have their own story of structure and characteristics aimed to meet the opposite objectives of network, respectively.

In the history of ARPANet, a computer network was found to be cheap and convenient, when used as a general digital communication network. IPNet was put into development stage, working smoothly in the early days. But various inconvenient phenomena occurred one after another, as the usage spreads wider. Measures have been tried in each occasion, but the final solution has not been obtained yet. We are still looking for the way to go.

If each of the above mentioned two types of network is used separately for each purpose as designed originally, then there would be no problem at all. This might be one of the hints to a desirable way of thinking.

[Meaning of "Best Effort"]

The "Best Effort" problem of IPNet is caused by packet switching, in the process that each router selects a vacant path on the route between the two terminals. This makes the signal route to vary with time depending on the contingency determined by network structure and information packet group. Even if a transmission loss of optical fiber is assumed to be zero regardless of path length, a delay time of signal varying with time may not be determined definitely. Even if information path can be predicted statistically, prediction of blocking probability due to traffic congestion would be supposed considerably difficult.

At the same time, evaluation of QR of switching and transmission is necessary for designing and operating any type of network. To answer this question, it is essentially required to develop a new basic theory of packet switching network. We should wait for a young genius to solve this question nicely.

Otherwise, there would be no way other than to remove the successive problems one by one, or to give up the packet switching that is the cause of "Best Effort". In such a way, it is

not easy to completely remove the influence of “Best Effort”, but there may be a method to minimize the influence. For example, just like a case of ARPANet, security problem can be evaded in case of communication in a perfectly closed society. Or, it may be also possible to make the best use of the characteristics of low cost and/or flexibility in digital communication of IPNet. It reminds me of a Japan’s saying that means “When illogicality comes in, logicality fades away.” To make the best use of a sole merit might be a hint to the solution also.

Here, you may have some unnecessary words by an old layman, again. When a fault of IPNet is criticized, an engineer who did not make his "Best Effort" should not say the following haughty prevarication. "It could not be helped, because that was 'Best Effort'". The words like this should be talked more modestly, being ashamed of lacking in technological power.

[Problem on Cost]

The circuit switching network guarantees 100% of security in principle, while IPNet enables cheap communication for various kinds of digital information. If so, it is the most rational and simplest method that the circuit switching network is used for the aim of severe security and IPNet is used for the cases particularly requiring cheapness and/or easiness. Then, we can have more choices, not the IPNet only.

For a criticism that a circuit switching costs very high in comparison with IPNet, we can answer that it is quite natural to pay more for higher security. Today, there may be methods to lower the cost of circuit switching equipment by making use of the latest technology. If it is still too expensive, it might be necessary to reconsider more seriously the cost of security. How much money did you pay for the security? And now do you feel really safe enough? Everyday, we hear about the incidents on lost security. How much do you want to pay more for security in the future?

It is certain that a cost is a very important factor, but it is not easy to simply evaluate the cost of security. For example, the world is struggling now for the security measures of IPNet, but how much is the total amount of loss (study cost / measures cost / personnel expenses / time) for the whole world? If it continues for longer time, the cost will be countless. In such a case, we could see that Security can be superior to cost.

[Problem on Assignment of Cost and Responsibility]

There is one more thought about a cost. That is “assignment of the cost of whole communication system”. In a circuit switching system, a communication operator owns nearly all the system except the terminal unit, and is responsible for the services in general. On the other hand, a user owns a terminal unit only, and can enjoy all provided services, by operating the terminal and paying for the services.

The present IPNet system is same as the centralized system in that a carrier owns all facilities except users’ terminals. However, there is a big difference from the case of centralized system, in the point that QRS of the total network service depends largely on the user’s terminal unit. This may be the main reason of that the operator’s responsibility for the service is limited to “Best Effort” (that means almost irresponsible) and the remaining almost all responsibility for QRS is taken by the users who take care of their terminal units.

User’s terminal unit includes various kinds of hardware and software, such as computer and its various peripheral devices, various software, Internet fee, disturbance measures software, etc. A big burden, not only economic but also mental, is required for a user to keep proper maintenance of the whole network performance. Thus, a user must bear almost all responsibility for QRS of the whole network system as his own “self-responsibility”.

This situation is also just opposite to the old network. People always say ‘IPNet is cheap’, but it is quite natural for QRS without guarantee. Even if we take into consideration of the terminal units commonly used for other purposes, user’s burden would be still severe.

It must be a peculiar spectacle that professional engineers with extremely high techniques take just a little responsibility, while many users of “Layman” (billions in the whole world?) must pour huge expenses and energy (perhaps with a lot of loss) into maintenance of QRS. The responsibility assignment like this would not stimulate the motivation of engineers,

resulting in an extreme inefficiency. Moreover, it would be one of the causes of the digital dilemma of CO_2.

[Charging System of IP Network]

A wonder of IPNet emerges right in the charging system. It must be the usual social financial principle that the communication fee is charged for the communication cost, which depends on amount of information, distance, frequency bandwidth, utilization time, and so on. The present flat fee system is completely against this principle. How much is it against? The fee for an e-mail (kiloByte) is same as for a moving image (GigaByte), the ratio of amount of information being a million. Also, e-mail to a next door and that to the backside of the earth are charged the same, the distance ratio being a million too. This surprising unfairness continues from the beginning to the present. We should recognize that this is one of the reasons to allow huge number of scoundrels such as spam e-mails to rush over the IPNet.

The above phenomenon also came from “Best Effort”. It is because the cost of IPNet communication cannot be counted, as there is no logical method to evaluate the QRS of IPNet. This is not a hint for more desirable way of thinking, but is a necessary condition for a desirable future network.

6. Exercise to Desirable Communication Network

Reconsideration on the future communication network has been made above. In order to realize it, we should consider what to do now, as an exercise to give a hint.

(1) We have not enough time to discuss on the existing IPNet, as there is a risk of collapse coming soon. We need to stop or delay the failure. (Postpone the failure.)
[Practice plan]: To regulate the sender who transmits extraordinary large amount of information. (Laws and organization for regulation)

(2) Since it will take more than ten years to complete a desirable ultimate network, provisional network is needed before the failure of the present IPNet. (Immediate realization of a provisional network)
[Practice plan]: To build up a provisional network that is easily carried out and effective. (The following combination method, for example)

(3) Early realization of desirable ultimate communication network.
[Practice plan]: Completely innovative new generation network, for example.

[Example of Provisional Network by Combined System] (Your good ideas are expected)

[[Plan One]] Make a combined use of circuit switching network, closed IPNet and open IPNet, depending on the required grade of security.
Circuit switching network: Super important duties to need 100% of security.
(Diplomacy, military and police, for example)
Closed IPNet: Important duties to need high security
(Lifeline, special business and others, for example)
Open IPNet: General communication of “Best Effort".

[[Plan Two]] Make a combined use of closed IPNet and open IPNet.
This can be used when the security needed for super important duties is confirmed with closed IPNet. Super important and important duties use two closed IPNet independent from each other. Open IPNet is used for general communication.

[[Additional condition]] When a user uses two or three physically (never logically) separated networks, he must have completely separated two or three full sets of terminal units on his desk, in order to keep the required security. This system would be named “2 (or 3) terminals per table system”.

7. Conclusions: Research for Ultimate Communications Network

It is the first conclusion of this reconsideration that both old network and present IPNet are not fit for our ultimate target. Our second conclusion is that combination of the two types of network can be a provisional network until the ultimate target is realized, by making the best use of the respective merits of each network. In addition to the above, it is essential to enact the necessary laws for protection against the risks of IPNet by all means.

A target of the study that we aim at as an ultimate network should be a network that can guarantee the required security together with logical design and operation. For further research, we must deny the present state first, and then pay much more attention and power to the research of provisional system and ultimate system with international cooperation. I think that this will be the most important conclusion of this reconsideration.

[Other Related Problem]

In Japan, there is no organization to study a strategy for future communication network. For this purpose, FCC of Japan should be newly established immediately. The most important purpose of FCC Japan for the time being is to study and decide the world standards for the provisional network, in tight cooperation with the international organizations.

Provisional measures which are common throughout the world such as [[Plan One]] must be realized before the existing IP network fails. Realization of International regulation laws and police activity for this purpose is necessary in time for the practical use of the provisional measures.

[Acknowledgment]

I would like to express my thanks to Dr. Takashi Iida, who invited me to the Space Japan Review and kindly took care of the laborious translation of this article. I also thank Dr. Hiromitsu Wakana for his cooperation to Dr. Iida in the translation work. Owing to the two gentlemen, my job was just to make final confirmation with some changes and additions in small parts. I must thank Mr. Kozo Iwaso, who has encouraged me for several years with the hottest articles of the Financial Times.

[Reference]

[1] Tomonori Aoyama, et al., ”Prospect and Problem of a new generation network for 2020’s”. IEICE Tokyo Section Symposium, Oct.9, 2008.
Research plan and related technologies on a new generation network NWGN (NeW Generation Network) in Japan.

[2] “Obama responds to cyber threat”
(The Financial Times, May 30, 2009) (presented by Mr. Kozo Iwaso)
The President Obama emphasizes the importance of measures for the Internet, and Obama Administration raises the importance order of related Agenda. Damage of US industrial world reached $1,000 Billion. Important information of armed forces and government leaked out by Cyber Attack.

[3] “Guideline for regulating network ‘occupation’”
(The Asahi, May 23, 2008)
Internet Service Providers try to reduce traffic congestion of the Internet by regulating the users who sends extraordinary amount of information.

POSTSCRIPT

[Now Considering ・・・・]

The above article was written more than one year ago. Since that time, the world and IPNet itself have made a big change. Firstly, the flat charge system of IPNet which I pointed out in the above article is criticized by European telecoms. Secondly, cyber attacks are grown up to “Cyber war”, that is a ghastly war with invisible enemies in the dark battlefield of IPNet. However, I felt with the shocking news as if I saw a small light of ‘Hope’ in a dark, because the world noticed the real risk of “Best Effort” of IPNet.

In spite of this event, the world seems still to persist in IPNet, probably because most

people do not quite understand the risk of IPNet yet. The research of the ultimate network must be the most important work of the communication engineers, but we have another important job beforehand for this purpose. It is to get the world's agreement to avoid the risk of IPNet, through a series of hard discussions on logical basis. When the first door is opened, the second door to the ultimate network will be opened easily. I believe that the human intellect can open the two doors to the ultimate network.

[Reference Data]

The material below shows the reality of the world reported by the Financial Times, but the "headline" and 「keyword」of the article only, because of shortage of time and space. I hope your imagination will catch what are going on and what will be the future.

List of the Financial Times article headlines related to the Internet

(Presented by Mr. Kozo Iwaso)

May 30, 2009 "Obama responds to cyber threat"
「see the [Reference」in the above main article」
Jan. 27, 2010 "US urges shared cyber attack defense"
「Cross-border collaboration needed for cyber attack defense」
Feb. 22, 2010 "US experts close in on Google hackers"
「Harder for China to deny involvement」
Apr. 10, 2010 "Google accused of YouTube 'free ride'"
「European telecoms groups vent angry」「Bandwidth used for little or no fee」
Jun. 11, 2010 "O_2 axe to fall on 'all you can eat' plan"
「Charges to be levied by data usage」
Jul. 6, 2010 "France Telecom hints at web fees"
「Heavy internet users face higher charges」
Sep. 24, 2010 "Malicious computer worm launched at industrial targets"
「Stuxnet」「Attack may be aimed at Iran's nuclear plant」
Sep. 24, 2010 "Computer worm triggers worldwide alarm"
「How the Stuxnet virus works」「Computers infected by Stuxnet virus worldwide」
Oct. 2/3, 2010 "A code explodes"
「We are in a dangerous new era of cyberwarfare」
Oct. 5, 2010 "The undeclared war in cyberspace"
「no explanation needed」
Oct. 9, 2010 "Who controls the internet?"
「States are investing serious resources into developing next-generation viruses」