

# Response to Series of Network Malfunctions



**NTT DOCOMO, INC.**

**January 27, 2012**

# Forward-Looking Statements

This presentation contains forward-looking statements such as forecasts of results of operations, management strategies, objectives and plans, forecasts of operational data such as the expected number of subscriptions, and the expected dividend payments. All forward-looking statements that are not historical facts are based on management's current plans, expectations, assumptions and estimates based on the information currently available. Some of the projected numbers in this presentation were derived using certain assumptions that are indispensable for making such projections in addition to historical facts. These forward-looking statements are subject to various known and unknown risks, uncertainties and other factors that could cause our actual results to differ materially from those contained in or suggested by any forward-looking statement. Potential risks and uncertainties include, without limitation, the following:

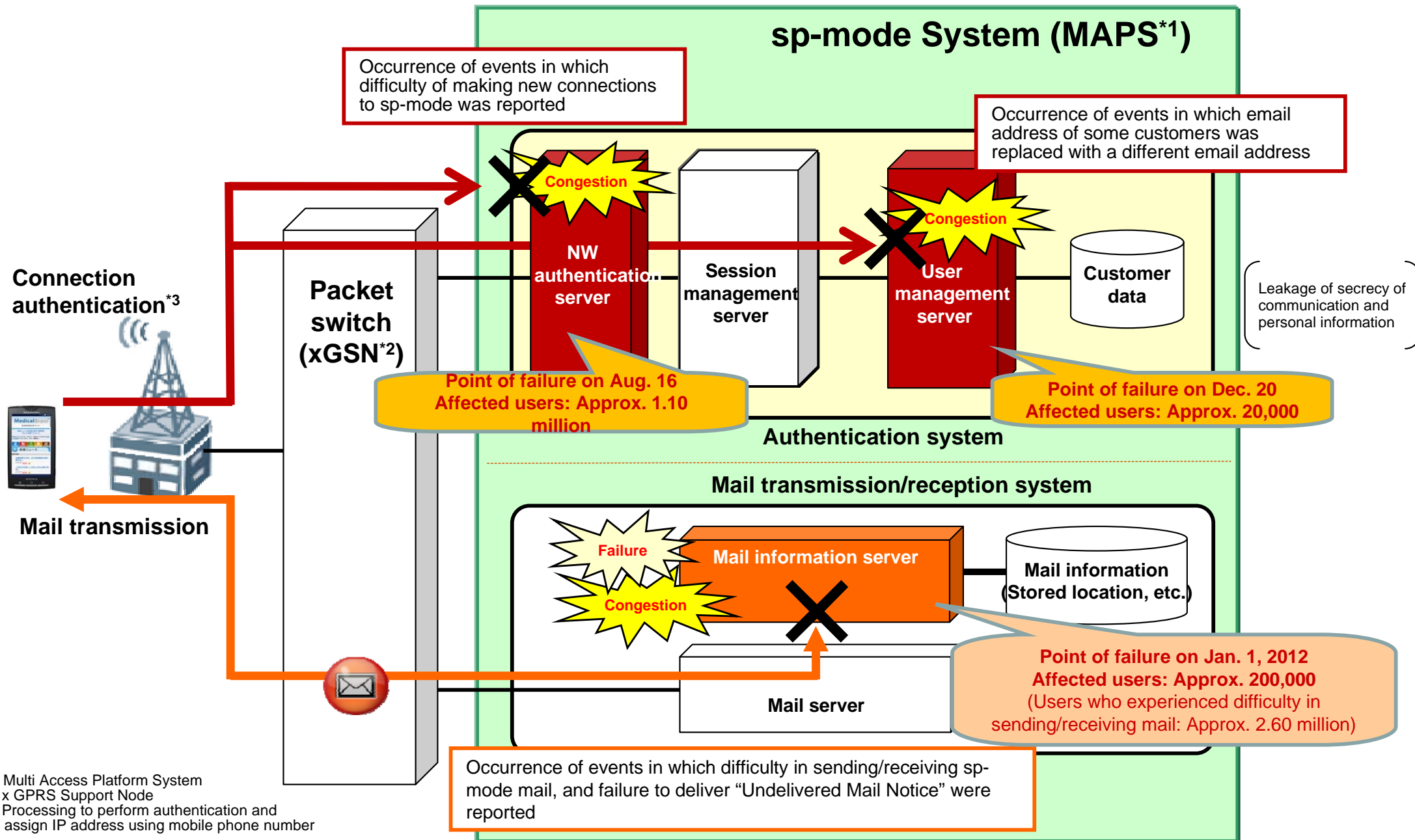
- (1) Changes in the business environment in the telecommunications industry, such as intensifying competition from other service providers, businesses or other technologies caused by Mobile Number Portability, new market entrants and other factors, or the expansion of the areas of competition could limit our acquisition of new subscriptions and retention of existing subscriptions, or may lead to diminishing ARPU or an increase in our costs and expenses.
- (2) Current and new services, usage patterns, and sales schemes introduced by our corporate group may not develop as planned, which could affect our financial condition and limit our growth.
- (3) The introduction or change of various laws or regulations or the application of such laws and regulations to our corporate group could restrict our business operations, which may adversely affect our financial condition and results of operations.
- (4) Limitations in the amount of frequency spectrum or facilities made available to us could negatively affect our ability to maintain and improve our service quality and level of customer satisfaction.
- (5) Other mobile service providers in the world may not adopt the technologies that are compatible with those used by our corporate group's mobile communications system on a continual basis, which could affect our ability to sufficiently offer international services.
- (6) Our domestic and international investments, alliances and collaborations may not produce the returns or provide the opportunities we expect.
- (7) As electronic payment capability and many other new features are built into our cellular phones/devices, and services of parties other than those belonging to our corporate group are provided through our cellular handsets/devices, potential problems resulting from malfunctions, defects or loss of handsets/devices, or imperfection of services provided by such other parties may arise, which could have an adverse effect on our financial condition and results of operations.
- (8) Social problems that could be caused by misuse of our products and services may adversely affect our credibility or corporate image.
- (9) Inadequate handling of confidential business information including personal information by our corporate group, contractors and others, may adversely affect our credibility or corporate image.
- (10) Owners of intellectual property rights that are essential for our business execution may not grant us the right to license or otherwise use such intellectual property rights on acceptable terms or at all, which may limit our ability to offer certain technologies, products and/or services, and we may also be held liable for damage compensation if we infringe the intellectual property rights of others.
- (11) Events and incidents caused by natural disasters, social infrastructure paralysis such as power shortages, proliferation of harmful substances, terror or other destructive acts, the malfunctioning of equipment or software bugs, deliberate incidents induced by computer viruses, cyber attacks, hacking, unauthorized access and other problems could cause failure in our networks, distribution channels and/or other factors necessary for the provision of service, disrupting our ability to offer services to our subscribers, and may adversely affect our credibility and/or corporate image, or lead to a reduction of revenues and/or increase of costs.
- (12) Concerns about adverse health effects arising from wireless telecommunications may spread and consequently may adversely affect our financial condition and results of operations.
- (13) Our parent company, NIPPON TELEGRAPH AND TELEPHONE CORPORATION (NTT), could exercise influence that may not be in the interests of our other shareholders.

# Table of Contents

---

<b>1. sp-mode Malfunction: Overview (Aug. 16, Dec. 20, 2011 &amp; Jan. 1, 2012)</b>	<b>...3</b>
<b>2. Packet Switch Malfunction: Overview (Jan. 25, 2012)</b>	<b>...4</b>
<b>3. Advancement of Network Infrastructure</b>	<b>...5</b>
<b>(1) Basic Approach</b>	
<b>(2) Task Force for Improvement of Network Infrastructure:         Current Study Items</b>	
<b>4. sp-mode Malfunction Countermeasures</b>	<b>...7</b>
<b>(1) Implementation Schedule</b>	
<b>(2)-1 Countermeasures Implemented Under STEP I</b>	
<b>(2)-2 STEP I Countermeasures: Points of Implementation</b>	
<b>(3) Countermeasures Implemented Under STEP II</b>	
<b>(4) Countermeasures Implemented Under STEP III</b>	
<b>5. Packet Switch Failure: Countermeasures and Challenges</b>	<b>...12</b>
<b>6. Prompt Information Disclosure to Customers</b>	<b>...13</b>

# 1. sp-mode Malfunctions: Overview (Aug. 16, Dec. 20, 2011 & Jan. 1, 2012)

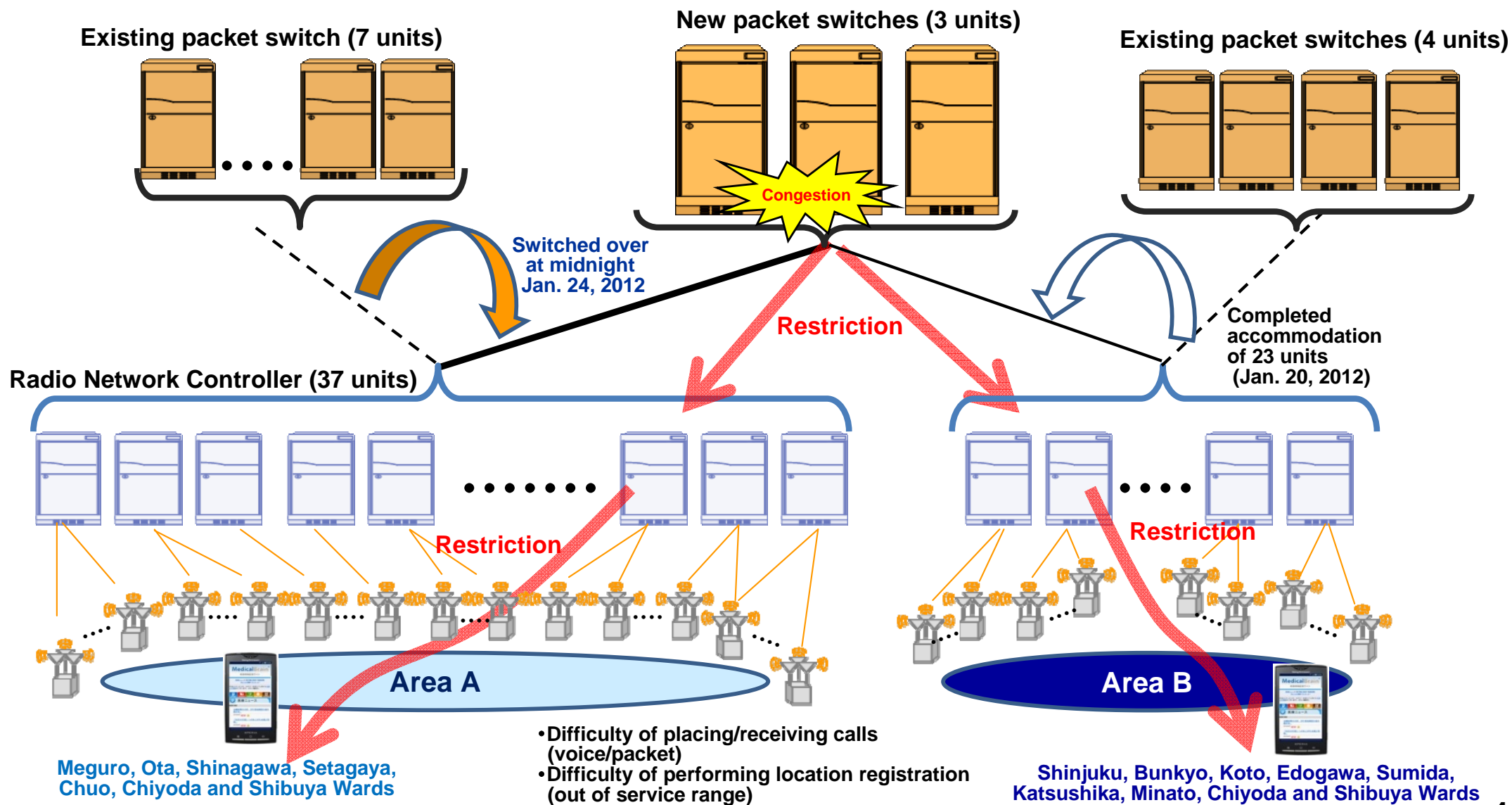


\*1: Multi Access Platform System  
 \*2: x GPRS Support Node  
 \*3: Processing to perform authentication and assign IP address using mobile phone number

\* The malfunctions occurred on Jun. 6, 2011, when congestion in service control equipment (IPSCP) resulted in difficulty of sending/receiving voice calls and packet messages, and were solved in late August 2011 by enhancing the processing capabilities of the service control equipment (IPSCP)

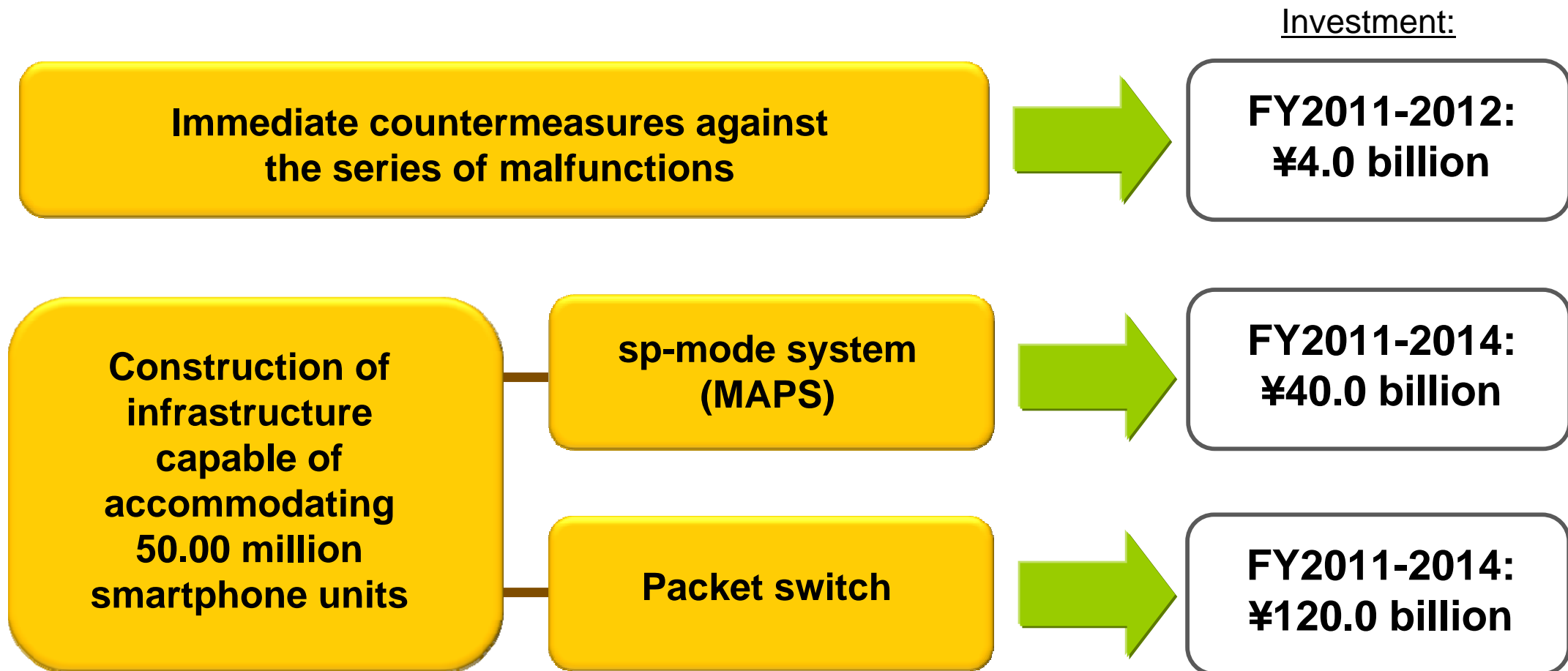
## 2. Packet Switch Malfunction: Overview (Jan. 25, 2012)

To cope with the rapid increase of smartphones, a new packet switching system was introduced to replace the existing system. After the switch-over, however, the new system failed to complete the processing of control signals that have increased due to rapid proliferation of applications (VoIP, etc.), which caused congestion and resulted in connection difficulty for FOMA voice/packet services



### 3. Advancement of Network Infrastructure (1) Basic Approach

Determine the causes of events that have occurred in line with the rapid increase in the number of smartphone users, so that immediate countermeasures against the causes of problems can be developed and implemented without delay. At the same time, perform company-wide, cross-sectional studies for stable network operations and further enhancement of processing capabilities for the future, etc., and construct network infrastructure capable of accommodating 50.00 million smartphone units by implementing drastic measures for reliability improvement





### 3. (2) Task Force for Improvement of Network Infrastructure: Current Study Items

Meeting dates		Items studied
Meeting #1	<b>Dec. 25, 2011 (Sun)</b>	<ul style="list-style-type: none"> <li>▪ Determined scope of malfunction (of Dec. 20), identified cause of problem and developed immediate countermeasures</li> <li>▪ Decided on policy and organizational structure for customer response</li> </ul>
Meeting #2	<b>Jan. 3, 2012 (Tue)</b>	<ul style="list-style-type: none"> <li>▪ Identified cause of problem (of Jan. 1) and developed immediate countermeasures</li> <li>▪ Decided on policy and organizational structure for customer response</li> <li>▪ Confirmed effects of countermeasures implemented before Jan. 3</li> </ul>
Meeting #3	<b>Jan. 12, 2012 (Thurs)</b>	<ul style="list-style-type: none"> <li>▪ Confirmed effects of countermeasures implemented and performed studies on drastic measures for further reliability enhancement</li> <li>▪ Confirmed status of customer response</li> </ul>
Meeting #4	<b>Jan. 19, 2012 (Thurs)</b>	<ul style="list-style-type: none"> <li>▪ Performed studies on concrete measures for network infrastructure advancement</li> </ul>
Meeting #5	<b>Jan. 24, 2012 (Tue)</b>	<ul style="list-style-type: none"> <li>▪ Decided on comprehensive action plan for sp-mode system (MAPS)</li> </ul>
Meeting #6	<b>Jan. 25, 2012 (Wed)</b>	<ul style="list-style-type: none"> <li>▪ Confirmed effects of measures implemented on Jan. 25</li> <li>▪ Identified cause of problem (of Jan. 25) and studied drastic countermeasures</li> </ul>
Meeting #7	<b>Jan. 26, 2012 (Thurs)</b>	<ul style="list-style-type: none"> <li>• Performed studies on methods of prompt information disclosure to customers in the event of a failure</li> <li>▪ Decided on comprehensive action plan for packet switches</li> </ul>

# 4. (1) sp-mode Malfunction Countermeasures: Implementation Schedule

		FY2011				FY2012			FY 2013	FY 2014	Cost		
		Dec	Jan	Feb	Mar	Apr	May	Jun					
<b>STEP I</b>	<b>Immediate measures against causes of problem</b>	<div style="display: flex; align-items: center;"> <div> <p><b>&lt;Response to Dec. 20 malfunction&gt;</b>                      (1) Modified internal processing of user management server (thru Dec. 22)                      (2) Controlled volume of signals fed to sp-mode system (thru Dec. 30)                      (3) Reduced load by changing signal processing sequence (thru Jan. 6)                      (4) Expanded buffer size of NW authentication server (thru Jan. 12)</p> <p><b>&lt;Response to Jan. 1 malfunction&gt;</b>                      (5) Modified internal processing of mail information server (thru Jan. 3)</p> </div> </div>											¥2.0 billion
<b>STEP II</b>	<b>Drastic measures for reliability improvement</b>	<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="display: flex; align-items: center;"> <span>(6) Change of connection sequence (thru Feb. 20)</span> </div> <div style="display: flex; align-items: center;"> <span>(7)-1 Measures against burst traffic (thru late April)</span> </div> <div style="display: flex; align-items: center;"> <span>(7)-2 Measures against burst traffic (thru early August)</span> </div> <div style="display: flex; align-items: center;"> <span>(8) Migration to new mail information server (thru Feb 20)</span> </div> </div>											
<b>STEP III</b>	<b>Scalability capable of accommodating 50.00 million smartphones</b>	<div style="display: flex; flex-direction: column; gap: 10px;"> <div style="display: flex; align-items: center;"> <span>(9) Reexamination of processing capability/scheme of each equipment (¥10.0 billion)</span> </div> <div style="display: flex; align-items: center;"> <span>(10) Measures for enhanced scalability</span> </div> <div style="display: flex; align-items: center;"> <span>(11) Facility build-up in response to increase of smartphones (¥30.0 billion)</span> </div> </div>											¥40.0 billion

\* Completed measures against malfunction on Aug. 16, 2011:

•NW authentication server processing speed enhancement (thru Aug. 22) •NW authentication server facility build-up (thru Nov. 30)



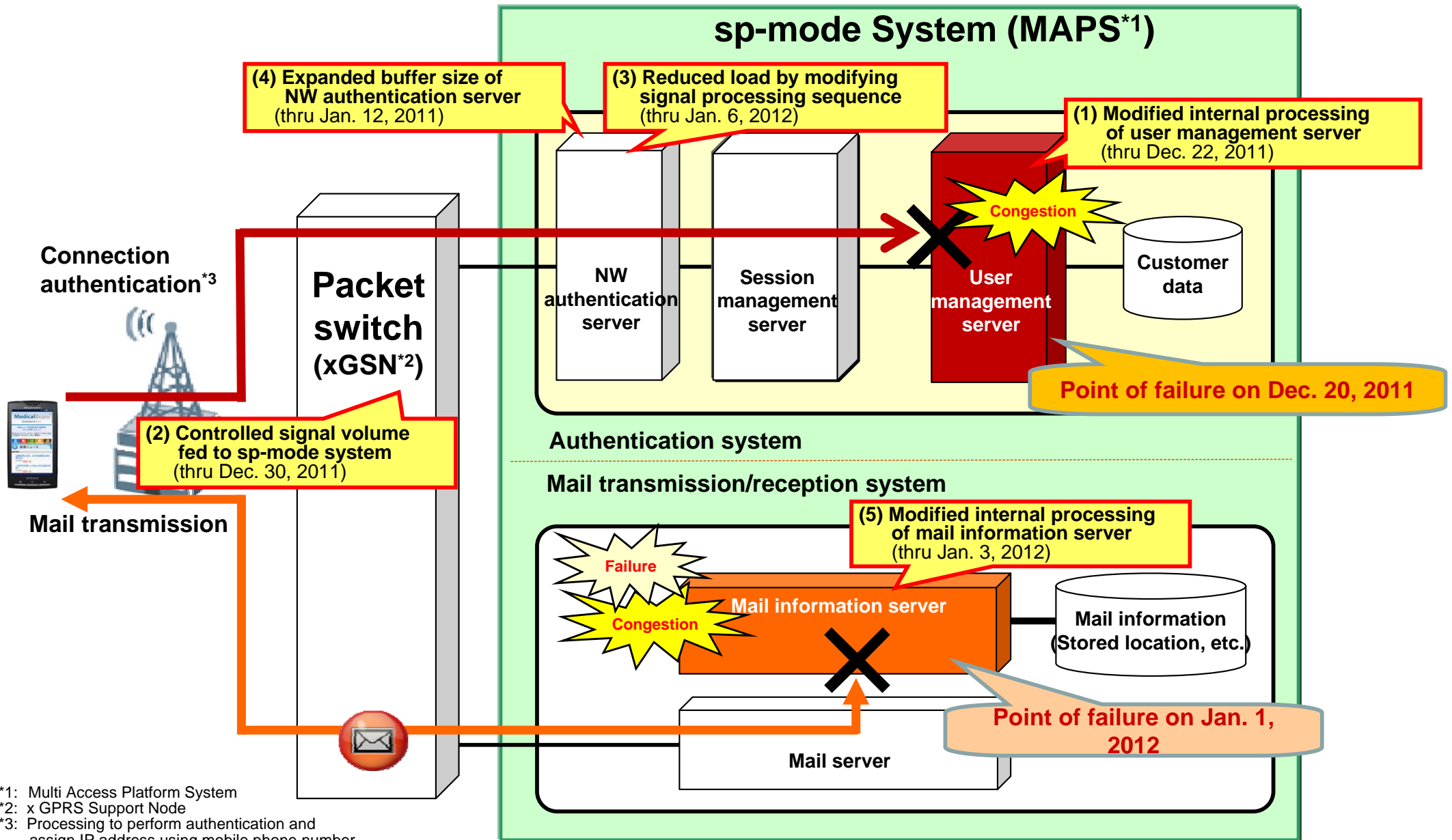
## 4. (2)-1 Countermeasures Implemented Under STEP I

Countermeasure	Overview	Completion date
Measures against sp-mode malfunction reported on Dec. 20, 2011		
<b>(1) Modification of internal processing of user management server</b>	Enhanced processing capability by modifying data processing method of user management server	<b>Completed Dec. 22</b>
<b>(2) Control of signal volume fed to sp-mode system</b>	Improved method of controlling the signal volume fed from packet switch to sp-mode system in the event of failure, to provide for generation of burst traffic	<b>Completed Dec. 30</b>
<b>(3) Load reduction through modification of signal processing sequence</b>	Reduced the signal processing load of user management server by changing the internal processing sequence of sp-mode system	<b>Completed Jan. 6</b>
<b>(4) Expansion of network authentication server buffer size</b>	Expanded receiving buffer size of network authentication server to ensure proper processing by the user management server, so that signals can be processed normally even in the event of burst traffic generation	<b>Completed Jan. 12</b>
Measures against sp-mode malfunction reported on Jan. 1, 2012		
<b>(5) Modification of internal processing of mail information server</b>	Enhanced processing capability by optimizing the value settings for signal processing by the mail information server	<b>Completed Jan. 3</b>

# 4. (2)-2 STEP I Countermeasures: Points of Implementation

Implemented immediate measures to cope with the causes of problems

(All completed by Jan. 12, 2012)



## 4. (3) Countermeasures Implemented Under STEP II

Countermeasure	Overview	Planned completion date
<p><b>(6) Modification of connection sequence</b> (Countermeasure against malfunction reported on Dec. 20, 2011)</p>	<p>Change the connection sequence so that IP address notification from packet switch to devices will be performed after completion of IP address registration in sp-mode system, to prevent mismatch of IP address</p>	<p><b>Feb 20 2012</b></p>
<p><b>(7) Countermeasure against burst traffic</b> (Countermeasure against malfunction reported on Dec. 20, 2011)</p>	<p><u>In case of failure in connection route</u> (1) Curb burst generation of re-connection signals to sp-mode system by changing the reconnection procedures in the event of a failure in the route connecting the packet switch and sp-mode system, so that only the users who are currently in session can perform re-connection</p>	<p><b>Late April 2012</b></p>
	<p><u>In case of switchover of service control equipment</u> (2) Curb burst generation of re-connection signals to sp-mode system by changing the location information update procedures when the service control equipment (IP Service Control Point: IPSCP) switches over to standby system due to failure, etc.</p>	<p><b>Early August 2012</b></p>
<p><b>(8) Migration to new mail information server</b> (Countermeasure against malfunction reported on Jan. 1, 2012)</p>	<p>Realize more stable operations by replacing the existing mail information server, where congestion was triggered by a glitch, with a new mail information server that offers superior reliability and maintainability</p>	<p><b>Feb 20 2012</b></p>

## 4. (4) Countermeasures Implemented Under STEP III

Countermeasure	Overview	Planned completion date
<b>(9) Reexamination of processing capability/scheme of each equipment</b>	<ul style="list-style-type: none"> <li>▪ Reexamine processing capability/scheme of each platform &amp; network equipment, taking into consideration possible generation of burst traffic (scale of 50 million smartphone units) or a surge of control signals resulting from diversification of applications, etc.</li> <li>▪ Reexamine conditions for occurrence of mismatch of states in user ID information management between different network components and fail/safe functions.</li> </ul>	<b>FY2012/End</b>
<b>(10) Measures for enhanced scalability</b>	<ul style="list-style-type: none"> <li>▪ For construction of a system capable of accommodating 50.00 million units of smartphones, the processing schemes of sp-mode system will be reviewed based on re-analysis of commercial and verification data, to improve the ease of facility build-up to be made in response to the growth of smartphone traffic</li> <li>▪ Secure reliability of overall system by reviewing the redundancy configuration of each equipment comprising sp-mode system</li> <li>▪ Strengthen capability of verifying marginal performance, e.g., burst traffic, etc., by reinforcing verification facilities</li> </ul>	<b>FY2012/End</b>
<b>(11) Facility build-up in response to increase of smartphones</b>	Carry out facility build-up of platform/network equipment on a continual basis in response to the increase in number of smartphones	<b>FY2014/End</b>

# 5. Packet Switch Failure: Countermeasures and Challenges

Countermeasure	Overview	Planned completion date	Investment
Comprehensive inspection on processing capability of packet switches across Japan	Carry out a comprehensive inspection on the processing capability of all packet switching systems across Japan (approx. 200 units) using the signal volume measurement function to be newly introduced in the switches.	Mid February 2012	—
Further processing capability enhancement of packet switches	Optimize resource allocation of packet switches, to expand the number of signals that can be processed	Mid August 2012	¥2.0 billion
Facility build-up to cope with the increase in control signals	Swiftly expand the capacity of packet switches as required based on the outcome of general inspection, and secure sufficient capacity by using the new switches in parallel with the existing switches	To be implemented swiftly in or after mid-February or later	¥120.0 billion
	Increase installation of packet switching system capable of accommodating 50.00 million smartphones	FY2014/end	

## Challenges

Tackle the challenge of suppressing the volume of control signals transmitted by applications in cooperation with carriers around the world (GSMA\* is also discussing countermeasures recognizing the importance of this issue)

\* GSMA (GSM Association) :  
An industry association of mobile operators. established in 1995 for the purpose of proliferating the GSM mobile telephone system. Today, the largest association in the wireless industry with membership of more than 1,000 companies representing 219 countries, including over 800 mobile operators.

# 6. Prompt Information Disclosure to Customers

In the event of a failure, ensure prompt information disclosure (within approximately 30 minutes after failure detection) to various customer contact points (home page, docomo Shops, information centers, Corporate Marketing teams, etc.) and relevant institutions (Ministry of Internal Affairs and Communications, mass media, etc.), so that customers can be kept aware of the conditions of service

