Installation example: 001

Cyber Solutions Inc.

NetSkateKoban ®

Large scale installation example : Tohoku Electric Power Co., Inc.

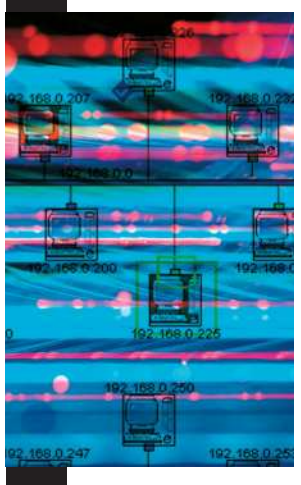
Tohoku Electric Power Co., Inc.

High-stability 24 hour monitoring of 15,000 terminals

Tohoku Electric Power Co., Inc installed the Intranet Monitoring System NetSkateKoban

Interviewees: Mr. Takizawa and Mr. Ishikawa of the Information Communication Department of Tohoku Electric Power Co., Inc.

Report.



Q Your company has been focusing on Fraudulent Intranet Connection since 2002, and carrying out surveys and investigations within the company. Why did you focus on that aspect so early?

A Our company has a comparatively vast network, and it was necessary to detect connections by terminals with no security guarantee (referred to hereon as fraudulent connection terminals) – to have some sort of mechanism to sniff them out.
Currently our company has 15,000 active terminals across the seven prefectures of Aomori, Iwate, Akita, Yamagata, Miyagi, Fukushima, and Niigata.
With a configuration like this, if a fraudulent terminal were to be connected to the network and spread a virus or some other dangerous program, it would be a catastrophe.

There are also limits to how much monitoring can be done manually – it is not feasible to have 24 hour management of these terminals.

Factors which influenced the decision to install NetSkateKoban

Tailor-made development incorporating the ideas of Tohoku Electric Power Co., Inc. – economical and easy to maintain

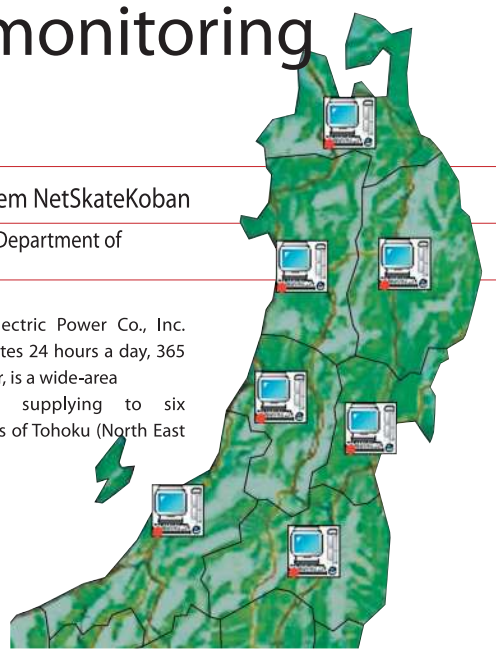
Q How did you go about it before you decided to use NetSkateKoban?

A In the beginning, we thought we would follow the guidelines below and begin development by ourselves.

1. To deliver a PING to all terminals allotted to Tohoku Electric Power Co., Inc.
2. Verify terminals which responded, with our PC inventory
3. If the terminal was listed, it was classified as a legitimate terminal, and if it wasn't, as a fraudulent terminal

Put simply, in response to our call of 'Are you there?', the answer of 'I'm here' was checked with our inventory.

However, there were problems with this method. For example, it wasn't possible to detect those fraudulent terminals with personal firewalls, since they didn't respond to the PING.



Tohoku Electric Power Co., Inc. that operates 24 hours a day, 365 days a year, is a wide-area enterprise supplying to six prefectures of Tohoku (North East

Next, we wondered if it wasn't possible to get information from the LAN switch.
If that was possible, we would know accurately the terminals connected to that switch.
At that point when we surveyed different products, four to five products came up, including NetSkateKoban.

We began a cross comparison of those products, including the option of developing internally. We finally chose NetSkateKoban, which was the only product which was willing to carry out collaborative development with us.

Q What sort of development did you carry out?

A Linking with Tohoku Denryoku's existing terminal management DB.
The fraudulent connection detection system works on the principle of whether the terminal is managed by the inventory or not.
Here, if we got a product package that could not be improved on, we would have to register 15,000 terminals on the DB. With respect to NetSkateKoban, we began joint development to enable linking to our existing DB.
We then shifted to the LAN switch method, activating eight NetSkateKoban (one each for the seven prefectures of Tohoku including Niigata and one for our company).
With a configuration like this, only one server of a data center needed to be installed, and it was economical as well as easy to maintain.

Installation example: 001

Applying NetSkateKoban

NetSkateKoban can be alternately used as a network trouble shooting support tool

? How does it feel to use this Intranet Monitoring System?

! Currently 15,000 terminals in seven prefectures are being monitored twenty four hours a day, and since the day of inception there have been no incidents of incorrect detection causing interference to business.

Small bugs do exist, but there is a sincere response for the bug fix every time.
It is of utmost importance that a system like this works safely, and therefore a degree of stability of this high order is worth mentioning in the appraisal.

? When you say 'support tool for daily network management' you mean…?

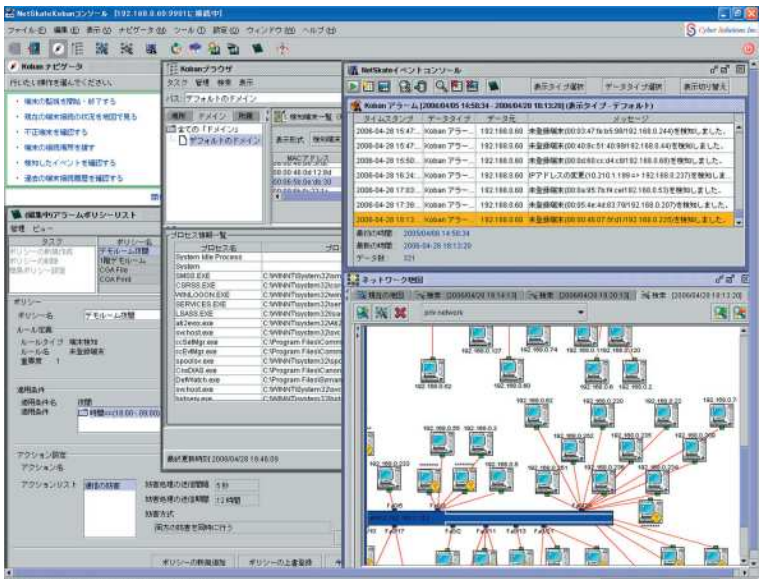
! If you use a network map, you can graphically grasp the terminal connection status at each business point.
The connection configuration of the terminals and the LAN switches are displayed like a layout, and so from our point of view as terminal status management, it is indispensable.

Application Configuration of NetSkateKoban

From manual shutoff to automatic shutoff in the future

? Currently, even when it is clear that a fraudulent terminal is connected, you don't use the automatic shut-off, but first report the fraudulent connection to the network manager, and then manually terminate the connection based on the manager's decision.
In situations like this, isn't there a time lag between the fraudulent connection and termination of the connection? Why isn't automatic shutoff used?

! When a fraudulent terminal is found, we think automatic termination must be initiated. However, if there is an incorrect termination, it would have a huge impact on business, and so we are investigating whether it would be possible to link the installation, relocation, and removal of the terminal and treat all this as one function.



One-click for network map auto-generation! Sturdy and Obvious Around-the-clock monitoring.

? Is that because NetSkateKoban is not fully capable and there is a possibility of incorrect detection?

! No, there is no such problem.
They could occur in the following situations -

1. A legitimate PC connected to the network before it is registered in the inventory DB.
2. When a large scale transfer or arrangement-change occurs, it is necessary to update the terminal inventory DB. If the update is late, or there is an error, a huge number of terminals will be deemed fraudulent.
3. If a network card is exchanged for hardware servicing, if the changes aren't reflected quickly in the inventory DB, the serviced terminals will be deemed fraudulent machines

In future, we need to approach all situations with the principle 'if in doubt, terminate'.
Security is certainly important, but to allow everyday work to come to a standstill in its pursuit would be like putting the cart before the horse. It is important to balance safety and convenience.
At present we are ironing out all the application troubles, and once that is largely over we plan to really get down to investigating the automatic termination issue.

NetSkateKoban is routinely used as a tool for understanding the network connection status. (By Mr. Takizawa and Mr. Ishikawa of the Information Communication Department of Tohoku Electric Power Co., Inc.)

Tohoku Electric Power Co., Inc. & Cyber Solutions Inc.

NetSkateKoban ®

Cyber Solutions Inc.
Cyber Solutions Inc.
ICR Bldg, 6-6-3, Minami Yoshinari, Aoba-ku Sendai-shi, Miyagi, 989-3204 JAPAN
TEL 022-303-4012 022-303-4015 e-mail netskate-sales@cysol.co.jp
http://www.cysol.co.jp/