Cyber Solutions Inc.

NetSkateKoban®

大規模導入事例：東北電力 株式会社　様

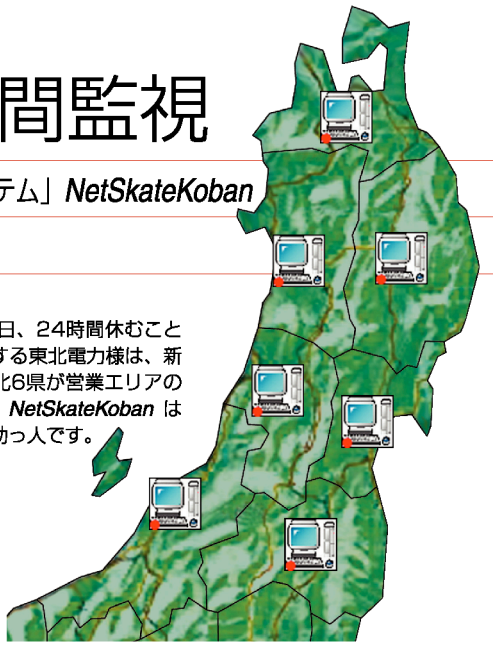
Tohoku Electric Power Co., Inc.

Report

高い安定性で 15,000端末を24時間監視

東北電力株式会社様が導入した製品：「イントラネット監視システム」*NetSkateKoban*

お話：東北電力株式会社情報通信部　滝沢様　石川様



1年365日、24時間休むことなく活動する東北電力様は、新潟県と東北6県が営業エリアの広域企業。*NetSkateKoban* は頼もしい助っ人です。

?御社は2002年ころから、イントラネット不正接続に注目し、社内で調査・検討を開始していたとのこと。なぜそのように早期から注目していたのでしょうか。

!弊社のネットワークは、青森、岩手、秋田、山形、宮城、福島、新潟の7県に約15,000台の端末が稼動しています。このように比較的「大規模」なネットワーク構成のなかで、もしも不正端末がネットワークに接続され、そこからウイルスなど不正プログラムが広まったら大変な事態になり、これを人手で24時間管理するには限界があります。

このため、セキュリティ確保上許可されてない持込み端末（不正接続端末）が万が一接続された場合、どこに接続されたのかがすぐに検出する「しくみ」を作ろうということになったわけです。

NetSkateKoban　採用の決め手

東北電力のアイディアを入れて共同開発 経済的、保守も簡単

?*NetSkateKoban* を採用するまでの経緯は？

!2002年の検討段階では、以下の方針により自社で開発しようと思っていました。

1．東北電力に割り当てられている端末すべてに対してPINGを打つ。
2．応答があった端末については、社内のPC台帳（インベントリ）と照合する。
3．その端末が台帳に載っていれば正規端末、載っていなければ不正端末と見なす。

簡単に言えば、「いるか？」と声をかけて、「いるよ」と返事のあった端末については、それが正しい端末なのかどうか台帳でチェックするというやり方です。

しかし、このやり方は、接続された不正端末にパーソナルファイアウォール等が入っていると、PINGに応答しないため不正接続端末を検知できないという問題があることが分かりました。

次に、LANスイッチから情報が取り出せないかと考えました。それが取り出せれば、そのスイッチに接続している端末が正確に分かります。

そこで色々な製品を調査したところ、*NetSkateKoban* を含めて4～5製品が浮上し、自社開発という選択肢も含めて相互比較しました結果、当社のアイディアを入れて共同開発してくれる*NetSkateKoban* を選び，今回「イントラネット監視システム」を開発しました。

?どのような開発をしたのでしょうか？

!東北電力の既存の端末管理DBと*NetSkateKoban* との連携です。不正接続検出システムの判断基準は、台帳上で管理されている端末かどうかという事です。もしも改良できないパッケージ製品だと15,000台分の端末をDBに登録しなければなりませんからね。

さらに、不正端末検出センサーの配置については、データセンターのサーバで7県と本社の計8つの *NetSkateKoban* を起動し、LANスイッチからの端末接続情報を監視する方式としました。こうすれば、導入はデータセンターのサーバ1台で済むので経済的、しかも、保守も簡単になります。

導入事例：001

NetSkateKoban の活用

ネットワークマップでグラフィカルに管理
トラブル解決支援ツールとしても活用

?「イントラネット監視システム」の使用感はいかがでしょうか？

!現在、7県15,000端末を24時間監視していますが、稼動以来、誤検出で業務に支障をきたすような事は起きていません。細かいバグはあるものの、バグフィックスはその都度誠意をもって対応していただいています。この種のシステムは無事に動いてくれる事が最も重要なので、この高い安定性は評価に値すると思います。

それから、不正端末検出という非常時の機能のほかに、日常のネットワーク管理の支援ツールとしても活用しています。

?日常のネットワーク管理の支援ツール、と言いますと？

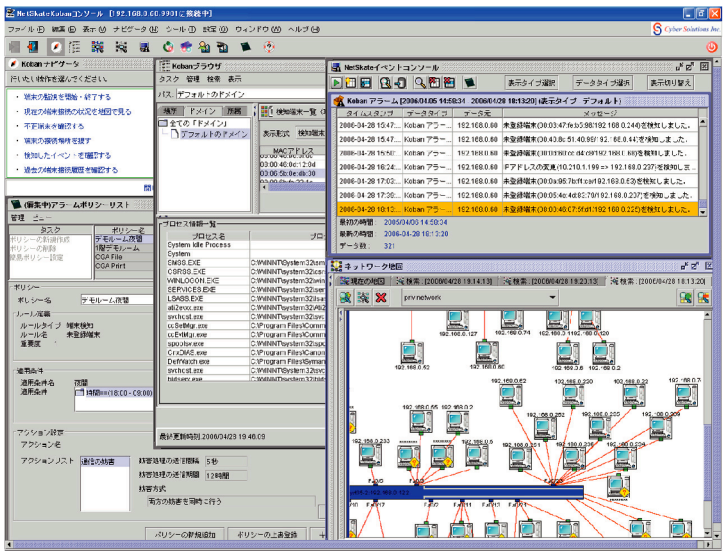
!ネットワークマップを使えば、各事業所の端末接続状況が、グラフィカルに把握できます。端末とLANスイッチの接続構成が配置表のように表示されるので端末状態を管理する立場にある我々としては重宝しています。

NetSkateKoban の運用形態

当面は手動遮断
将来的には自動遮断へ

?現在は、不正端末の接続が判明した場合、まず不正接続をネットワーク管理者に通知し、それから管理者の判断によって手動で遮断するという方式を取っていますね。これだと不正接続から接続遮断までの間に若干のタイムラグが発生します。なぜ自動遮断しないのですか？

!不正端末を見つけたら、自動遮断すべきだと考えています。しかし、誤遮断するようなことがあれば、正しい端末が不正と見なされて遮断されてしまいます。正しい端末が遮断されれば業務が混乱するので、端末の導入、移設、撤去といった作業との連携も含め全体として運用していけるか検討中です。



ワンクリックでネットワーク地図を自動生成。目に見える確かさで24時間監視。

?NetSkateKoban によって、誤検出が起きる可能性があるということでしょうか?

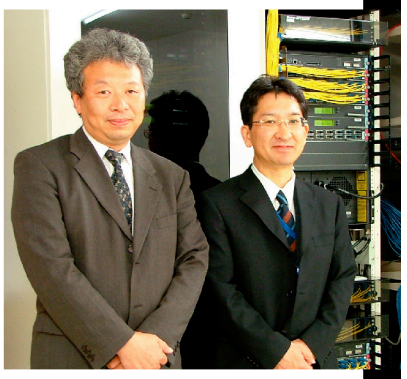
!いいえ、そういう事ではありません。例えば、次の場合にそういう事が生じえます。

1．正規調達したPCが、端末台帳DBに登録される前に現場に届けられ、ネットワーク接続された場合。
2．大規模な移動や配置換えが起こる時は、端末台帳DBもそれに合わせて更新しなければならない。この更新が滞ったり更新ミスがあると、大量の端末が不正とみなされることになる。
3．ハードウエア修理などでネットワークカードを交換した場合、台帳DBに速やかに反映させないと修理後の端末は、不正マシンとして見なされる。

将来的には、『疑わしきは遮断する』という原則で自動遮断によって臨む他ないと考えていますが、不正端末に対する自動遮断を行う前に、こうした日常的に起こりうる事態にどう対処するかを充分に練りこんでおかないと、かえって業務を混乱させてしまいます。

セキュリティは確かに重要ですが、それを追求するあまり、日常業務を止めてしまったのでは本末転倒になるので安全性と利便性の両立が大切です。

起こりうる運用トラブルの洗い出しがある程度終わったら、本格的に自動遮断に向けて検討を開始する事になると思います。



NetSkateKoban は、ネットワーク接続の現況を把握するツールとして、日常的に使っています。（東北電力株式会社 情報通信部 滝沢様 石川様）

※この記事は，2005年6月に取材したもので滝沢様，石川様の所属もこの時点のものです。

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

NetSkateKoban®

株式会社 サイバー・ソリューションズ　NetSkate 事業部
Cyber Solutions Inc.
〒989-3204　仙台市青葉区南吉成6-6-3 ICRビル 3F
TEL 022-303-4012　FAX 022-303-4015　e-mail netskate-sales@cysol.co.jp
http://www.cysol.co.jp/