NX-C6000

【ユーザー事例】株式会社エヌ・ティ・ティ エムイー様

近年企業電話のIP化が進んでいるが、SIP/VoIPネットワークには、国際呼不正発信、不正ユーザー発信（なりすまし）、DoS攻撃といった脅威が潜んでおり、通信事業者、ユーザー企業それぞれにおいて対策が急務になっている。通信事業者のひとつである株式会社エヌ・ティ・ティ エムイー（以下、NTT-ME）では、2012年12月、ネクストジェンのVoIP/IDSネットワークフォレンジックシステム「NX-C6000」を導入し、これらの脅威に対応した。

導入の経緯について、NTT-MEネットワークソリューション事業部ネットワークシステム部門石川担当課長、松野尾主査に話を伺った。

課題と効果

課題・脅威	効果
DoS攻撃	DoS攻撃の早期検知および迅速な詳細把握
海外不正発信	不正ユーザーからの発信検知および迅速な詳細把握
故障端末、解約顧客端末からの不正メッセージ受信	故障端末、解約済端末の特定
サイレント故障	メッセージ流量変化からサイレント故障を早期に検知

導入の経緯

― 何故「NX-C6000」のようなVoIP/IDSフォレンジックシステムが必要だと判断されたのですか？

NTT-MEのVoIPサービスで使用しているSIPというプロトコルは近年世の中での使用範囲が広がっており脆弱性等の報告も増加していることから、セキュリティ問題について能動的／即時検知できることが重要であると考えたためです。(石川氏)

― 御社のVoIPサービスについて教えていただけますか？

NTT-MEは「ネットワーク総合エンジニアリング企業」としてネットワークサービスやアプリケーションサービス、カスタマサービス、エンジニアリングサービスを提供しています。NTT-MEがVoIP草創期よりネットワークサービスとして全国展開している企業向けVoIPサービスでは、多くの場合、ISPネットワークを介して加入者契約端末との通信を行います。(石川氏)

ネットワークソリューション事業部
ネットワークシステム部門
担当課長 石川氏

― ISPネットワークを介してしているということですが、ISPネットワークはインターネットにもつながっていますよね。そのために、様々な問題が生じる可能性があるのではないでしょうか？

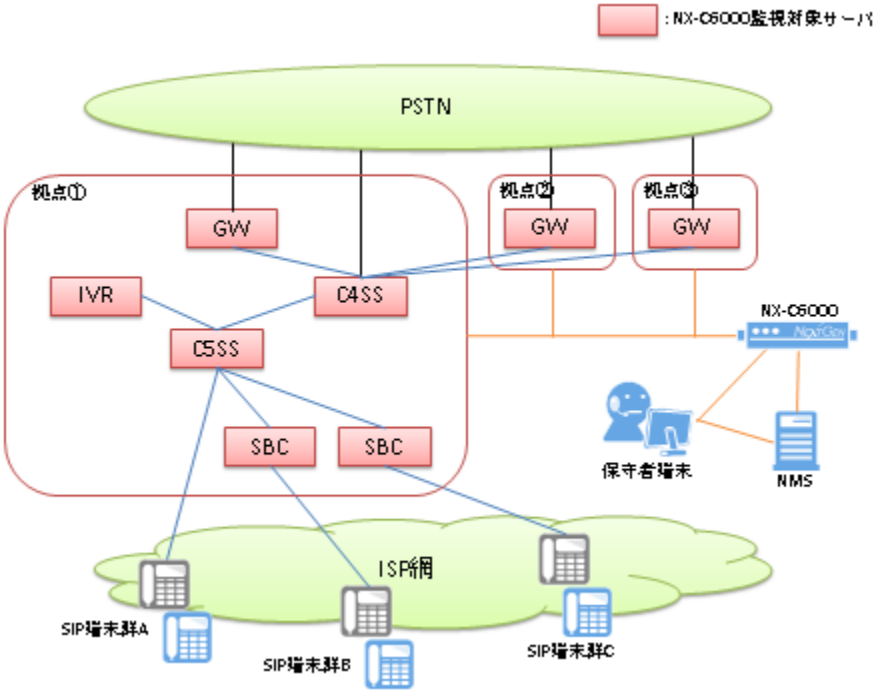
そうですね。問題発生を防ぐためにファイアウォール設置などの対策を行っていますが、通信を許可しているIPアドレスが踏み台となってしまったりする可能性はゼロとはいえません。その場合には、DoS攻撃によりSIPサーバーの処理負荷が上昇したり、SIPサーバーに不正なSIPメッセージを送信されることによりサービスに影響を及ぼすようなことになったりという状態が起こらないとも限りません。

ですが過去に使用していたSIPキャプチャツールでは問題発生後に収集データの参照により調査は行えるものの、収集したデータの解析に時間を要しますし、なにより問題の能動的／即時検知ができるような機能がありませんでした。

こうした課題の解決のソリューションとして、ネクストジェンの「NX-C6000」を採用しました。これにより、DoS攻撃等の即時検知や、ネットワークトレンド情報による異常発生有無の能動的かつ容易な確認が可能になりました。(石川氏)

― ISPネットワークを介した通信がもたらす様々な脅威に対して、よりプロアクティブな対応が可能である「NX-C6000」を導入いただいたのですね。

― 導入前には、試用版をご利用いただきました。
2011年10月から12月にかけて、「NX-C6000」を使ったVoIPサービス網内のSIPメッセージ調査を実施していただきました。その際に、弊社でも把握できていなかった問題点が明らかになり、こういったツールの必要性をより強く感じました。(石川氏)



【NX-C6000】 構成イメージ

ネクストジェンのVoIP/IDSネットワークフォレンジックシステム「NX-C6000」は、NTT-MEのVoIPネットワークに対する脅威となる可能性のある事象の早期発見やその事象の調査の迅速化に役立っている。

選定理由

― SIPメッセージをキャプチャし、シーケンスを可視化する製品は他にもありますが、その中で「NX-C6000」を選ばれた決め手は何だったのでしょうか？
「NX-C6000」を選定したのには、大きく5つの理由がありますが、決め手となったのはやはりセキュリティ機能です。(石川氏)

■セキュリティ
セキュリティ機能について大きな決め手となったのは、検討したツールの中で最も優れたIDS機能を持っていたのが「NX-C6000」だったことです。「NX-C6000」が持つ、SIPメッセージヘッダーなどキャプチャしたメッセージの中身をリアルタイムに解析できるという特長が弊社の要望にマッチしていたのです。 (石川氏)
― キャプチャしたメッセージのリアルタイム解析に基づくIDS機能があれば、不正なSIPメッセージが送信された場合や、DoS攻撃があった場合の即時検知が可能になりますね。
また、特定国への発信をチェックする設定を行っておけば、近年発生しているユーザー端末を踏み台とすることなどによる海外不正発信(※1)も早期に防ぐことが可能になります。
(※1：通信端末やアカウントを乗っ取られた加入者が高額な請求を支払えず、裁判で争うことを避けるため通信事業者が請求を取りやめるケースがある。)

― 疑わしい通信を直ちに遮断するIPS機能ではなく、不正侵入を検知するIDS機能が重要であった理由は何でしょうか。

IPSでは正規ユーザーの正規通信を誤って遮断してしまう可能性があり、これはVoIPサービスを運営している通信事業者としては許されないことです。弊社としては、IDSで問題を検知させ、機械的にではなく人間の判断のもとにアクションを起こす、ということが非常に重要でした。(石川氏)

■網監視

2つめは、網内のネットワークトレンド監視機能です。

SIPサーバーは、故障時にアラートを発報するよう設計されていますが、過去にSIPサーバーの監視装置にはアラートが発報されていないがサービスに影響が出ているというような故障が発生したケースがあります。(石川氏)

― いわゆる"サイレント故障"と言われるものですね。故障検知の遅れが、サービス影響の長時間化を招く恐れがあります。

そうです。「NX-C6000」を使ってSIPエンティティ間のメッセージ送受信流量を監視することで、メッセージ流量の急減や急増を検知して即時に監視部門に通知し、お客様からの申告が来る前にNTT-ME側で故障の早期発見ができるようになります。

同時に、通常時のメッセージ流量を正確に把握し傾向を知ることで、設備設計の目安にもなっています。(石川氏)

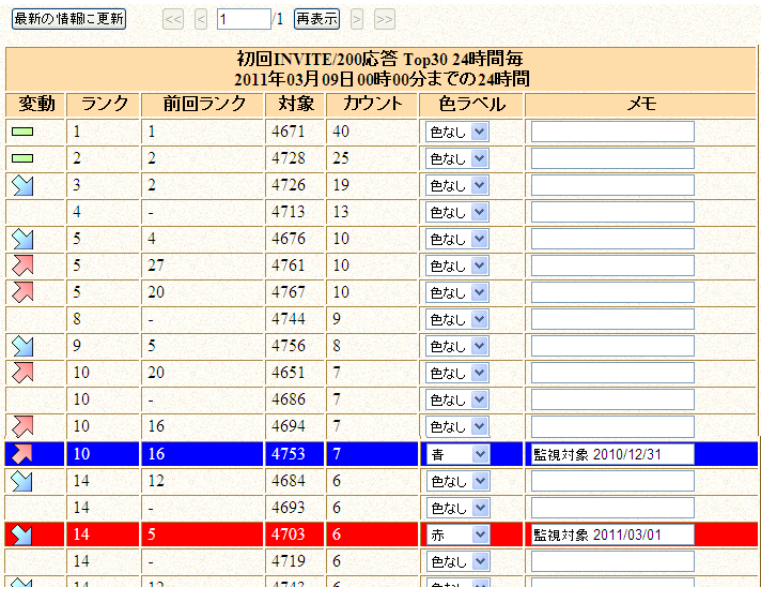
■直観性

3つめは、攻撃や異常の「見える化」ができることです。

これは試用導入時にも感じたことですが、「NX-C6000」で収集したメッセージ流量やメッセージ解析結果の情報等はグラフ形式や、ランキング形式での表示が可能なので、SIP/VoIPに精通していなくても情報を分かり易く知ることができるようになりました。(石川氏)

― ランキング表示では、監視対象がランキング入りした場合にアラームを上げる機能も備えています。

ランキング表示機能は、監視対象端末や電話番号、発信元の長期的な動向チェックに非常に役立っています。(石川氏)


最新の情報に更新 << < 1 /1 再表示 > >>

初回INVITE/200応答 Top30 24時間毎
2011年03月09日00時00分までの24時間

変動	ランク	前回ランク	対象	カウント	色ラベル	メモ
	1	1	4671	40	色なし	
	2	2	4728	25	色なし	
↘	3	2	4726	19	色なし	
	4	-	4713	13	色なし	
↘	5	4	4676	10	色なし	
↗	5	27	4761	10	色なし	
↗	5	20	4767	10	色なし	
	8	-	4744	9	色なし	
↘	9	5	4756	8	色なし	
↗	10	20	4651	7	色なし	
	10	-	4686	7	色なし	
↗	10	16	4694	7	色なし	
↗	10	16	4753	7	青	監視対象 2010/12/31
↘	14	12	4684	6	色なし	
	14	-	4693	6	色なし	
↘	14	5	4703	6	赤	監視対象 2011/03/01
	14	-	4719	6	色なし	

【ランキング表示イメージ】
電話番号に「色」をつけることでランキング検知

■パフォーマンス

4つめの評価ポイントは、1システムで網全体を一元監視できる強力なパフォーマンスでした。今回導入したエントリークラスのサーバー1システムで、VoIPサービス網内の60以上のSIPエンティティ間通信を監視できています。(石川氏)

■ネクストジェンの技術力

最後の1つですが、これはネクストジェンの技術力、サポート力がありますね。ネクストジェンはVoIPエンジニアリング企業としてSIPはもちろん、SIP/VoIPセキュリティに対する知識も深く、また常に最新情報の収集に努めていることは知っていました。

この知識、情報量により「NX-C6000」で様々な脅威を検知する仕組みを導入することが可能でした。これは我々だけでは追い切れない部分もあり、ネクストジェンの情報収集力にかなり貢献いただいた部分です。(石川氏)

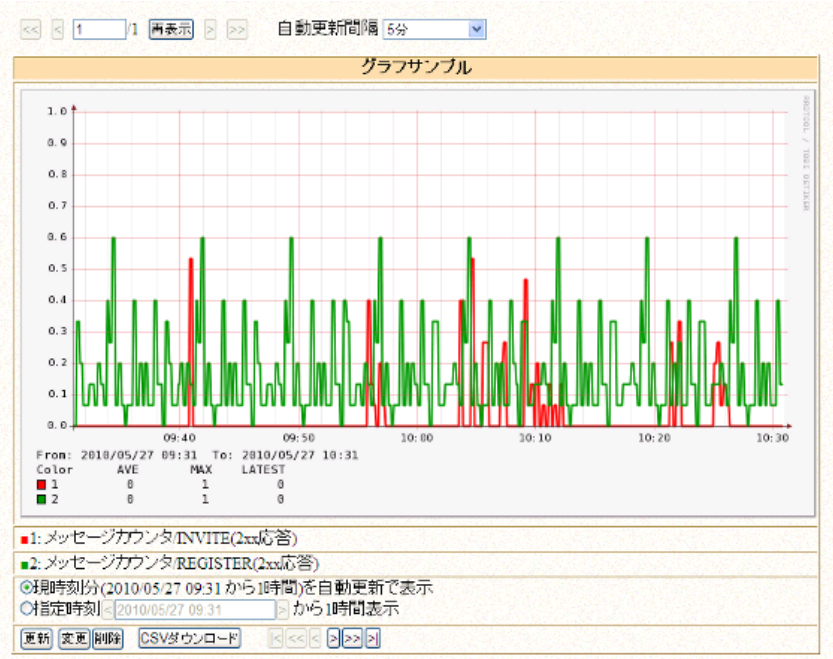
数あるSIPメッセージキャプチャツールの中で唯一DPI（Deep Packet Inspection：ペイロード部分の解析によるフィルタリング）が可能であること、セキュリティ機能だけでなく網監視にも有用であること、表示がユーザーフレンドリーであること、エントリークラスのIAサーバーでも十分なパフォーマンスを発揮すること、さらに弊社の技術力を高く評価いただいた。

運用状況

― 「NX-C6000」導入後のメリットをお聞かせください。

「NX-C6000」の導入により、今までは特定のSIPエンティティに蓄積された過去の情報を参照するしかなかった網内のネットワークトレンドを、リ アルタイムで目視することができています。その結果、異常が発生した場合の発生箇所や影響範囲を速やかに特定することができるようになりました。

また、SIP信号のリアルタイムの解析により不正な国際発信が発生している可能性がないか、DoS攻撃を受けている可能性がないかなどを常時監視するとともに具体的な情報を数値やデータで見ることができるようになりました。（松野尾氏）



【グラフ表示イメージ】
任意のメッセージのグラフ表示が可能

これらの脅威が発生した場合、サービスへの影響を及ぼす危険性もあり速やかな対応が必要ですが、その際に的確な対応を実施することが可能になったと考えています。

また、故障端末や解約済端末からのSIPメッセージの受信量を把握できるようになったことから、お客様に端末の故障等をお知らせし、再起動や交換いただくことで無用なトラフィック負荷削減を実現することも可能になったという認識です。(松野尾氏)

― そのようにしてトラフィック負荷が削減できれば、長期的に見て「NX-C6000」がコスト削減に貢献できるということでしょうか？

はい、SIPメッセージ流量の正確な把握に加え、無駄なトラフィックを削減できれば無用な設備増設をしなくてすむと考えます。
また、問題の能動的／即時検知ができるようになったことや、容易に各種条件でのSIP信号検索ができるようになったことでお客様の申告があった場合の対応の迅速化にもつながっていることから、保守運用コスト削減に加え、お客様の信頼確保にも繋がっています。(松野尾氏)


ネットワークソリューション事業部
ネットワークシステム部門
松野尾氏

― 「NX-C6000」に対する要望等はございますか？

「NX-C6000」を利用することでより一層のVoIPサービスの運用品質の向上が図れればと思っています。
例えば、SIPエンティティ間での同時接続呼数などのセッション状況を把握できるようになるとか、RTPなどSIP以外のプロトコルにも対応していただけると嬉しいですね。RTPに関しては、音声通話品質も監視できるようになるといいと思います。(松野尾氏)

― 今後はどのように運用されていかれる予定でしょうか？

SIP/VoIPに対する脅威は日々進化していて、常に動向をチェックしていくことが必要だと思っています。今後はネクストジェンの「NX-C6000運用サポートメニュー」(※2)を活用し、都度最新の脅威に対応した設定の導入をお願いしていきたいと考えています。(石川氏)
(※2：SIP/VoIPセキュリティのエキスパートによるデータ分析をもとにしたコンサルティング。「NX-C6000」に蓄積されたデータを元に、より効果的な監視方法やアラーム設定を提案、導入する。)

― ありがとうございます。ネクストジェンでは「NX-C6000トレーニングメニュー」もご用意しています。「NX-C6000」の特徴や使い方をレクチャーさせていただきますので、新入社員の方や、新たに配属された方などがいらした際にはご用命ください。

なるほど、せっかく導入したツールですから、有効活用していくためにもそういったメニューも積極的に利用させていただきたいですね。(石川氏)

取材日：2013年3月
取材協力：株式会社エヌ・ティ・ティ エムイー（略称NTT-ME）
所在地：東京都豊島区東池袋三丁目21番14号
設立：1999年(平成11年)4月1日
代表者：岡　政秀
ホームページ：http://www.ntt-me.co.jp/