# 次世代ネットワークのセキュリティソリューション

岡部 稔哉・中井 正一郎・世良 孝文
河津 正人・伊東 一博・河内 康郎

**要　旨**

キャリア網を取り巻く環境は変化しています。通信主体や通信内容が変化し、ネットワークや端末の能力は飛躍的に向上しました。またオープン化された技術によって構成されるとともに、様々なアプリケーションを取り込んだプラットフォームへとその役割も移り変わります。本稿では、変化する環境のなかでキャリア網としての要件を満たすために取るべき対策として攻撃防御、激甚対策、トラフィック制御、運用管理の4つのソリューションを紹介します。

キーワード
●次世代ネットワーク　●セキュリティ　●攻撃防御　●激甚対策　●トラフィック制御　●運用管理

## 1. はじめに

キャリアの提供するサービスのめざすべき姿は次世代ネットワークになっても変わることなく、最重要項目として、悪意のあるユーザ（意図的な脅威）に対する堅牢性(要件1)、過失や災害(偶発的脅威)に対する堅牢性(要件2)、サービス提供の公平性の維持(要件3)、セキュリティシステムの効率的な構築、運用(要件4)が挙げられます。

今後キャリア網は他網との相互接続や、異なるアクセス網の収容、サードパーティによるコンテンツ配信など、外部依存度が増加します。また、ビジネスモデルも多様化していくでしょう。すなわち次世代ネットワークは事業構造の複雑さが増加していくと予想されます。事業構造上の複雑さの増加は脆弱性の増加を意味します。一方で今まで同様の高水準のセキュリティレベルが期待されます。

変化する環境のなかでこれらの4つの要件を満たすために取るべき対策として攻撃防御、激甚対策、トラフィック制御、運用管理の4つのソリューションを紹介します(図)。

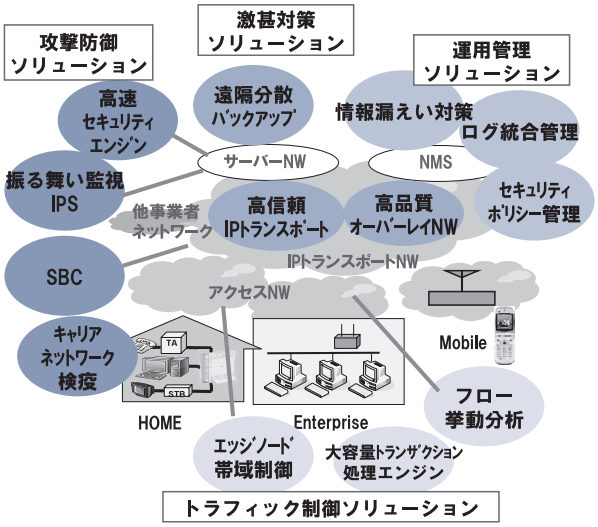


**図　次世代ネットワークセキュリティを実現する要素技術**

## 2. 攻撃防御ソリューション

不正な外部端末からのアクセスに対しては、ファイアウォールに代表される境界防御が有効です。境界防御は不正なパケットがネットワークに侵入することを防ぎます。一方OSやアプリケーションの脆弱性を狙う攻撃の多くは、境界での検出が困難です。これらはサーバ内で防御します。サーバや端末内での防御を単点防御と呼びます。

ここで、相互補完防御という考え方を導入することが効果的です。端点で検知した予兆情報をリアルタイムに、網の要所に設置するすべての境界防御装置に一斉通知することで、後続の不正アクセスを自動的に遮断します。即時に防御守備範囲を拡大し、被害を局所化します。

以下に、利便性や性能を犠牲にすることなく不正な行為を検知することでディペンダビリティを向上する相互補完防御

の要素技術について紹介します。

**(1) 振る舞い監視型IPS**

振る舞い監視型IPS(Intrusion Prevention System)は、サーバで動作するプログラムの「振る舞い」に着目して不正行為を検知､防御します[1)]。たとえば､正規の保守者が設定ファイルを更新する場合、認証手順を経ますが、バッファオーバーフローに代表されるOSの脆弱性を悪用したプログラムの場合認証手順がありません。この振る舞いの差に注目して、不正な行為を検知し、未然に防御します。

**(2) 高速セキュリティエンジン**

次世代ネットワークはユニバーサルサービスプラットフォームとして莫大な数の端末を収容しなければなりません。IMS(IP Multimedia Subsystem)に代表されるサーバ群とともに侵入検知システムにも高性能化が要求されます。一方で、常に進化する外部システムや既存オープンシステムとの連携も重要です。

そこで、システム内部に閉じた､Virus/Worm検知機能、プロトコル異常検知機能､トラフィック計測機能をハード化し、大量のパケットを効率よく処理します。外部との連携部分は柔軟性を残すためソフトウェアとして実現します。

ハードとソフトの適切な機能分割によって、高速化と柔軟性を両立させる技術が高速セキュリティエンジンです[3)]。

**(3) キャリアネットワーク検疫**

ウイルスやボットと呼ばれる攻撃プログラムによる攻撃は、大半が端末に実装したソフトウェアの脆弱性を狙ったものです。脆弱性を抱えたままネットワークに接続すると、自らが感染するだけでなく、さらなる感染源となって被害を拡大します。この問題には、ネットワークに接続する前に端末の安全性を診断し、適切な対処を行うといった一連の手続きが有効です。

アクセス網に接続した端末は、最初に検疫サーバと呼ばれる特定のサーバに対してだけアクセスを許可され、診断を受けます。問題があれば事業者ごとに定めたセキュリティポリシーに従い対処し、解決したことを確認した後にはじめてネットワーク接続を許可します。

端末数の増大がもたらすセキュリティ脅威への対策を、一般利用者のスキルに依存することなく実現します。

**(4) SBC境界防御**

VoIPサービスプロバイダが直面する、大量呼接続要求による処理負荷の増大、トラフィック集中による緊急呼の不通、そして悪意あるユーザによるSIPサーバへの不正アクセスなどの脅威をSBC(Session Border Controller)は解決します。SBCはSIPの呼接続状態を監視し、必要な音声トラフィックのみをVoIP網に通過させます。また、一次的な大量接続要求によるSIPサーバへの負荷の抑制や緊急呼の優先処理、SIPサーバへの不正アクセス排除を行います。

さらに、災害などにより特定地域への呼接続が集中した場合にはSIPサーバとSBCが連携し、対地規制を実施し、ネットワーク全体の負荷を軽減します。

## 3. 激甚対策ソリューション

過失や災害などの偶発的脅威が発生しても、ネットワークの到達性と蓄積したデータの完全性を守らなければなりません。そこでまず高信頼かつ高品質なIP網を構築し、さらにその上位レイヤで、分散配置したサーバ群がIP網とは独立した高信頼オーバーレイネットワークを構成することによってサービスごとの到達性を高めます。そして分散データバックアップがデータ完全性を確保します。

**(1) 高信頼IPトランスポート**

社会インフラであるキャリア網は短時間であってもサービス停止が深刻な影響を与えます。障害が発生してもサービスを継続できる高信頼IPトランスポートが必要です。IPとの親和性が高く、経路制御やQoS管理に適したMPLSを活用して信頼性を高めます。

QoSサーバ[3)]はあらかじめ設定した条件をもとにQoS保証可能な最適経路のパス設計を行います。同時に迂回パスを設定し、万一の障害に備えます。迂回パスは、帯域専有型、帯域共有型、非保証型の3つから選択でき、保証性と経済性の要求に応じたパス設計を実施します。障害発生に備えて迂回パスを含めた最適な経路を設計することで、高信頼なIPネットワークを構築します。

**(2) 高品質オーバーレイネットワーク**

既存IP網に手を加えることは容易ではないため、網の特定部分のみを高信頼化、高速化できるオーバーレイネットワークが注目されています。

物理網(特にIP網) 上に設置したTCPセッション処理ノードがサービスごとの論理網(オーバーレイ網)を構築します。物理網とは独立した上位サービスに特化した専用の経路制御を行い、物理網の輻輳や障害に影響を受けない、高品質な接続性を提供します。

**(3) 遠隔分散バックアップ**

WANを介したファイルアクセスを高速化する手段としてWAFS (Wide Area File Services) が注目されています。遠隔地に分散配置するストレージの近傍に設置する中継バックアップ装置は、高速回線を活かしたデータ同期を行います。伝送遅延やパケットロスを考慮したマルチパス転送とマルチパス上のトラフィック平滑化によって低速回線経由で接続する遠隔地との間でもデータ複製を行い、データ完全性を確保します。

## 4. トラフィック制御ソリューション

他網からの過剰なトラフィックの流入、DoS(Denial of Service)攻撃、スパム、SPIT(spam over IP Telephony)などのサイバーアタックによるネットワークリソースの占有を防止する取り組みが必要です。

キャリア網の目的は個人のプライバシーを守った上で安定したサービスを万人に公平に提供することです。企業網のように、教育や社内規定、パケットをモニタし業務と関係のないトラフィックを排除するといった手法をとることができません。

パケットの中身をのぞき見ることなくトラフィックを識別し、不正なトラフィックは廃棄、緊急通信や有料放送などは確実な品質保証、そしてベストエフォート部分についても適切にリソースを割り当てることによってサービス提供の公平性を実現するトラフィック制御ソリューションの要素技術について紹介します。

**(1) 大容量トランザクションエンジン**

大容量トランザクション処理エンジンとは、大量発信される迷惑メールやWebアクセスからサーバを守るハードウェアエンジンです。アプリケーションのトランザクションをフィルタリング、もしくはレート調整を行います。特にメールシステムに適用した商品がSLIMIT-Lです[4]。秒間1,000通以上のメール処理性能を有します。

さらに今後、高度なWebサービスやシングルサインオンなどの普及に伴い、記述言語であるXMLがより多くの場面で利用されるようになります。トランザクション処理エンジンは、サーバのXML処理負荷を軽減し、より多くのユーザに快適なWebサービスを提供します。

**(2) フロー挙動分析**

フロー挙動分析技術とは、パケットサイズや到着時間間隔など、パケットの中身をのぞき見ることなく得られる情報からアプリケーションを推定する技術です[5]。一定時間観測することによって得た統計的情報や、パケットごとの特徴の遷移パタンからアプリケーションを推定します。

この技術によって、キャリア網において重要なユーザトラフィックの秘匿性を維持した上で、暗号化したトラフィックやヘッダ情報を偽装したトラフィックのアプリケーションを識別します。P2Pトラフィックの検出やVoIPなどの優先トラフィック成りすまし防止、品質劣化検出にも有用です。

**(3) エッジノード帯域制御**

多くのサービスを安定に提供するため、一部のユーザや一部のサービスのトラフィックが互いに干渉しあうことを防止する仕組みが従来以上に重要になります。そこで、光化し大容量化するアクセス網を集約するエッジノードが、高速処理を実現する専用チップによって、サービスごとユーザごとにトラフィックの流量をきめ細かく管理し、決まった量以上のトラフィックが流入した場合には制限します。

サービスを管理するサーバや網管理装置からの動的な制御と併せて、災害輻輳時のトラフィック規制を、サービスやユーザの優先度を考慮した上で実施します。

## 5. 運用管理ソリューション

より高度なセキュリティを確保するためには今以上に多くのそして様々なセキュリティ機器を管理しなければなりません。セキュリティ運用管理のPlan-Do-Check-Actionサイクル(セキュリティ設計、ルール設定、インシデント監視、インシデント分析)には、予防措置や対策の遅れ、様々な攻撃を検出するための高度な専門知識不足、サービスの多様化や管理対象の増加、頻繁な変更の結果生じる管理負荷増大などの新たな課題が現れます。さらに、運用管理ステムは個人情報などの重要な情報を保持するため、情報漏えい対策も不可欠です。

セキュリティポリシーの運用、ログ情報の活用と情報漏えい対策の自動・統合・連携によってセキュリティ運用管理システムを効率化します。

**(1) セキュリティポリシー管理技術**

ネットワーク管理者の負荷を軽減するために、作業工程ごとに改善に向けた取り組みが必要です。

セキュリティ設計工程では、アクセスポリシーや監視ポリシーなどを特定の機種に依存しない形式で策定します。

ルール設定工程では、策定したポリシーから個々の機器に特化した形式のルール(設定値)を自動導出します。人手でルールを変更した場合でも、適用済みルールとポリシーが

一貫性を維持することを検証します[6]。
これらの工程を自動化することで、管理負荷を削減、設定不備などの事故防止、またインシデント発生時の対応迅速化が図れます。

**(2) ログ統合監視・一元化技術**

インシデント監視、インシデント分析工程において、セキュリティ機器が生成する大量のログを一元管理して、攻撃や侵入などインシデントを検出します。
振る舞い分析技術は、ログから特定パタンを抽出し、ネットワークへの侵入や攻撃をリアルタイムに検出します。傾向分析技術はログの比較的長期間かつ広範囲の傾向を分析し、ネットワーク全体での異常行動や未知の脅威を検出します。

**(3) 情報漏えい対策**

情報漏えいを防ぐには、機密データの持ち出し制御と秘密分散法による暗号鍵分割手法が有効です。
持ち出し制御技術を応用した製品InfoCage[7]は、サーバ上にあるデータの閲覧、編集を行っても、端末のローカルディスクにデータを残しません。また外部メディアへの保存や印刷、画面キャプチャ、メール送信を制限します。利用者の故意、過失による情報漏えいを防止します。
一方、持ち出しを許可したデータは暗号化し、その鍵を秘密分散法で分割することで、単独犯や一部結託による漏えいを防止します。秘密分散法とは、秘密情報を任意の複数個に分割する技術です。個々の分割情報からは元の情報を一切類推することはできず、あらかじめ定めた個数が揃わないと復元できません[8]。
持ち出し制御と秘密分散法を組み合わせることで、キャリア網の運用管理業務において、利便性を損なわずに高いレベルの情報漏えい対策を実現します。

## 6. おわりに

次世代ネットワークを取り巻く環境変化に対応した高水準なセキュリティレベルを維持するためにはセキュリティに対する戦略的な投資が必要です。事業者ごとに網構成や事業構造、想定するリスクやセキュリティへの投資バランスなど、要件が異なります。個々のソリューションのなかでも各防御手段をどこまで適用するかは事業者ごとの要件に合わせて最適な組合せを見つけ出さなければなりません。NECは幅広い保有技術をもとに、次世代ネットワークのセキュリティ対策の最適ソリューションを提供します。

**参考文献**

1) 中江ほか、「ふるまいに基づくサーバ侵入防御方式」、FIT2004講演論文集(第4分冊)、pp. 275-276、2004.9
2) 神谷ほか、「10Gbps 高性能セキュリティエンジンプラットフォームの開発」、信学総大BS-5-13、2006.3
3) QoSサーバ CX6800-QS http://www.sw.nec.co.jp/netsoft/cx6800-qs/
4) SLIMIT http://www.nec-mobilesolutions.com/application/jcontents/slimit/
5) 北村ほか、「フロー挙動分析技術に基づくアプリケーション識別手法」、信学技報Vol.105 No.470, NS2005-136、2005.12
6) 岡城ほか、「セキュリティ運用管理における機器設定統合分析システム」、情報処理学会研究報告CSEC-28, Vol.2005, No.33、pp.303-308、2005.3
7) InfoCage http://www.sw.nec.co.jp/cced/infocage/
8) Furukawa, et al., "Group Signatures with Separate and Distributed Authorities," Proc. SCN2004, Lecture Notes in Computer Science, vol. 3352, Springer Verlag, pp.77-90, 2004

## 執筆者プロフィール

**岡部 稔哉**
中央研究所
システムプラットフォーム研究所
主任

**中井 正一郎**
ネットワークソフトウェア事業本部
第一ネットワークソフトウェア事業部
統括マネージャー

**世良 孝文**
キャリアソリューション事業本部
マネージャー

**河津 正人**
ソリューション開発研究本部
システム基盤ソフトウェア開発本部
マネージャー

**伊東 一博**
ネットワークソフトウェア事業本部
第二ネットワークソフトウェア事業部
マネージャー

**河内 康郎**
ブロードバンドネットワーク事業本部
ネットワークプラットフォーム開発本部
グループマネージャー