Vol.2010-CSEC-49 No.4
2010/5/11

クラウドコンピューティングにおけるセキュリティ SaaS の基本検討

小宮康裕[†]　　佐藤直[†]

近年，IP ネットワークは情報セキュリティ上の脅威により安全性が大きく損なわれている．本文では，ユーザの負担を軽減しつつ IP ネットワークの安心・安全な利用のためのセキュリティ対策サービスの提供手段を検討する．具体的には，近年様々な活用がなされているクラウドコンピューティングに注目し，ユーザのネットワークセキュリティ対策のサービスを SaaS で提供しようというものである．特に，ユーザネットワーク内の通信を全てクラウドコンピューティングのネットワークで監視する方法について VLAN を利用する方法を提案し，実現可能性を検討した．

A study of security SaaS on Cloud Computing

Yasuhiro Komiya[†]　and Naoshi Sato[†]

Recently, security of IP networks has been greatly degraded by various threats, and users of network services are forced to implement expensive security countermeasures for themselves. So this paper discusses network security countermeasures from the users' viewpoints and highlights on reduction of user's load on the network security. Assuming that cloud computing would be popular as a new environment for network services in the near future, the paper proposes a method providing security SaaS on the networks. Especially on monitoring overall communication traffic on private networks, the paper suggests a method applying VLAN to the cloud computing and discusses its feasibility.

1. はじめに

急速に発展してきたインターネットは，企業にとってはお客様向け商品の宣伝，販売のメディアとして利用されている．また，インターネットの技術を利用したイントラネットは，ファイル共有やメールで業務に活用されている．このように，IP ネットワークは企業の事業運営には無くてはならない存在となった．一方，「個人情報漏洩」や「機密情報漏洩」など，企業における情報漏洩が重大な問題となっている．個人情報の漏洩は，お客様の名前，住所，電話番号などが悪意ある者の手に渡って悪用されてしまうことがある．また，機密情報の漏洩は，その情報が競争相手の会社に渡ってしまう事態となることもある．企業にとってこのような情報漏洩事件を起こしてしまうと，企業のイメージダウンに繋がるほか，お客様への賠償や機密情報が漏れたことによる競争力低下など，金銭的損害も発生してしまう．IP ネットワークの自由度と利便性は悪意ある利用者にとっても好都合であり，IP ネットワークを介した情報漏洩事件・事故などが絶えない原因となっている．そのため，企業などでは情報漏洩が発生しないよう様々な情報セキュリティ対策の取り組みをおこなっており，IP ネットワークに対しても種々の対策の実施を余儀なくされている．

そこで，筆者らは，安心で安全な IP ネットワーク構築のための研究を行い，いくつかの提案を行ってきた．具体的には，運転免許のように公的なネットワーク利用資格制度を導入し利用を制御する提案[1]や，端末等の安全性を評価してネットワークの利用制御を行う方法の提案[2][3]，私的なあるいは公的なセキュリティポリシを利用し，ネットワークの利用制御を行う方法の提案[4][5]などである．本稿では，さらに，近年注目を集めている，クラウドコンピューティングに着目し，クラウドコンピューティング環境下のセキュリティ対策を，全て SaaS として提供することにより，ユーザの金銭的負担や労力的負担を減らしつつ安心・安全に IP ネットワークが利用できるよう検討を行った．

2. セキュリティ対策の現状

IP ネットワークの利用において，通常の利用者は悪意ある利用から身を守るため，いくつかのセキュリティ対策を行う必要がある．現状のセキュリティ対策は，クライアント側にアンチウィルスソフトをインストールしたり，OS のセキュリティホール対策のためのパッチを導入したり，サーバなどに対し不正な利用が行われないようにアクセス制御を施す．また，検疫ネットワークによりクライアントが安全なものであるかどうか，また，不正な端末が接続されていないかを検証，検疫する仕組みもある．

[†]情報セキュリティ大学院大学
INSTITUTE of INFOMATION SECURITY

IP ネットワーク自体を悪意ある利用から守るためには，不正な侵入を防ぐファイアウォールの設置や異常なトラヒックを監視する侵入検出システム IDS や侵入防御システム IPS を設置する．これらの対策は基本的には全て各企業自身による作業で実施されている．すなわち各従業員の端末に関する作業は従業員自ら行なわなくてはならず，それらのソフトウェアの購入や，各システムの構築，運用，保守も，ネットワーク管理者が購入，構築などの作業を行なう．そのため，労力的，金銭的に大きな負担となっている．また，これらの作業をアウトソースしたり委託したりすることで労力は減らせるが，当然費用がかかるため，結局金銭的負担が増えてしまう．また，末端の端末に対する作業が各従業員に委ねられているため，その従業員のセキュリティ対策に対するリテラシーや作業スキルが低いと，そこがウィークポイントになってしまう．企業間で考えた場合も，スキルの高いネットワーク管理者が居る場合はセキュリティレベルも高くすることができるが，そういったスキルを持った者が居ない企業だと，セキュリティレベルは低くなってしまう．

これらのことから，現状のセキュリティ対策の問題点は，

① ユーザ側の作業負担が大きい
② セキュリティ対策にかかる金銭的負担が大きい
③ セキュリティレベルのばらつきが生じやすい
④ セキュリティレベルの低いところを狙って悪意ある利用が可能

と言うことができる．

公衆（あるいは中継）ネットワークとしてのインターネットは，ネットワークは簡単に，端末は高機能に，というコンセプトのもと構築され，誰でも自由に・簡単に使えるという経緯で発展してきた．このため，現在でもユーザの端末は高機能になり，ユーザ端末へのセキュリティ対策が重要になっているのに対し，ネットワークは逆にシンプルに構成されたままである．ネットワーク側で悪意ある利用を制限しようとするなどの機能はほとんどない．このためユーザは自分で自分を守らなくてはならず，この作業が大変な金銭的，労力的負担となっている．この傾向は企業ネットワークにおいても同様である．セキュリティ攻撃手法がますます高度化するにつれて，端末側のみでのセキュリティ対策には限界があると考えられる．この状況でより安心・安全に IP ネットワークを利用するためには，セキュリティ機能をネットワーク側で提供するのが望ましい．ユーザ側の各種負担を少なくし，より安心・安全なネットワーク利用を可能にする IP ネットワークの目標は以下のように考えられる．

① ユーザ側の作業負担が少ない
② セキュリティ対策コストが少ない
③ セキュリティレベルが均一
④ ネットワークの悪意ある利用が不可能

これらの目標を達成するには，ネットワーク側で高性能なセキュリティ対策，又はサービスを実現する必要があると考えている．

3. 関連研究及び既存サービス

3.1 関連研究

近年，IP ネットワークのセキュリティ維持を目的に，IP ネットワークのセキュリティ評価基準，あるいはセキュリティ証明書やネット免許に関する議論が高まっている．

例えば，自動車等で公道を運転するためには運転する自動車の種類に応じた公的な免許が必要であるが，今や情報化社会のインフラとして成長したインターネットは情報通信の公道とみなすことができること，また，この公道を利用したサイバー犯罪が絶えないことから，自動車免許と同様にインターネット利用に関する免許制度導入を検討する時期にいたっている，という提言である [1]．しかし，インターネットは誰でも自由に接続でき，自由に情報発信できるなどの自由度，利便性がメリットであるため，このような免許制度はインターネットの発展の妨げとなるとして反対する声のほうが大きい．

さらに，セキュリティレベルに応じて公的な資格証あるいは検査証を発行し，その管理機関が資格情報やブラックリストの情報を元にセキュリティデータベースを作成・管理し，そのデータベース上のセキュリティレベルによってネットワーク利用を優先させたり，または不正アクセスの排除を行ったりする研究例[2][3]もある．この資格証や検査証の発行や，セキュリティデータベースの維持管理を客観的に行うには，第三者機関が必要で，同機関は公的な位置づけのものが望ましいとされる．従って，この方式はまずそれらを運用するための社会制度の確立が必要であると考えられる．

また，ネットワークに接続する際に認証・検疫を行うシステムとして，企業内のネットワークなどにおける検疫ネットワークがあるが，この検疫機能を公衆系あるいは中継系の IP ネットワークにも拡張し，ネットワークの利用制御を行なう研究[4]もある．この研究は，ユーザの端末の安全性をセキュリティ検証機関で検証し，その結果から，ネットワークの利用制御を行なうものである．ここで制御される対象はネットワーク利用帯域幅であり，安全性の高い端末は多くの帯域を利用でき，安全の低い端末は帯域が抑制されることになる．近年，NGN(Next Generation Network，次世代ネットワーク)が導入されたが，NGN はサービス品質(QoS)の他，回線認証の機能を有し，セキュリティ機能を向上することのできる IP ネットワークとしても期待されている．この NGN を利用し，ネットワーク利用制御によりユーザネットワークを守る研究[5]がある．この研究は，利用者が自ら通信に対する私的なポリシを設定することで，ネットワーク側でその私的なセキュリティポリシに従って，ユーザの意図しない通信トラヒック（DoS 攻撃を想定）を判別し，通信経路を差別化（遅延を発生）して意図し

ない通信を抑制することで，正常な通信の帯域を確保する手法である．

本稿では，新たにクラウドコンピューティングに着目し，SaaS としてセキュリティサービスを提供する方法を検討することとした．

3.2 既存サービス

現在，SaaS として提供しているセキュリティサービスには，スパムメールやウィルス付きのメールからユーザの端末やネットワークを守るサービス[6]や，ファイル，Web，E-Mail などのレピュテーション情報を元にインターネット上にある各脅威から防御するサービス[7]などがある．これらのサービスはクライアント自体をセキュリティの脅威から守るための SaaS として便利なサービスであると考える．しかし，アクセス制御を無視するような通信や DoS 攻撃など，不正あるいは悪意ある IP ネットワーク利用の場合，IP ネットワーク内の通信自体を監視しなくてはならない．

そこで，ネットワーク内を流れる悪意ある通信などを監視するサービスを SaaS として提供する方法について検討，提案する．

4. 提案方式

4.1 提案方式概要

全ての通信はクラウドコンピューティングに用意されたセキュリティ SaaS を利用，もしくはセキュリティ SaaS からの監視を受けることとし，必要なセキュリティチェック，検疫，利用制御，悪意ある通信の監視を受けるような仕組みを提案する．図 1 に概要を示す．

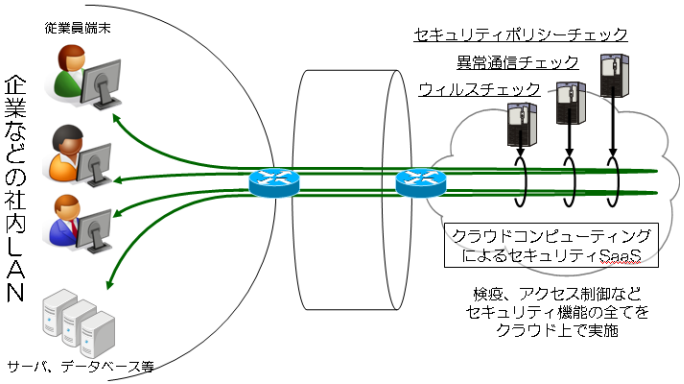

図 1　提案方式の概要

ユーザが IP ネットワーク（インターネットおよびイントラネット）を利用する際，接続される端末は全て，アンチウィルスソフトのインストール状況やパターンファイルの更新状況，OS のパッチなどの状況のチェックを受け，ユーザが設定するセキュリティポリシを満たしているもののみ通信が開始できるものとする．一方，通信の監視については，IP ネットワーク内を流れるパケットを監視し，悪意ある利用など異常が無いか監視を行えるような仕組みとする．イントラネットからインターネットへ，またはその逆など，出入りする通信を全て監視するだけでなく，通常セグメント内で解決してしまうようなユーザ間通信についても，必ずクラウド上の SaaS から監視できる仕組みとする．これらの機能のうち，「アンチウィルスソフト」「OS のパッチ」「検疫」に関しては，既存の技術やサービスをそのまま利用，あるいは SaaS への応用をすることにより実現可能であると考える．「IP ネットワーク内の通信の監視」については，クラウドコンピューティングによって，ネットワークを通過するパケットを監視，又は対象のネットワークを監視し，異常なパケットを検知し，管理者への通知などを行う．具体的には，IDS を用いてネットワーク内のパケットを監視し，異常なものを検知，管理者に通知する，または IPS で自動的に排除する．通常の IDS は外部ネットワークとの出入り口にあたる部分で利用される．また，特定のセグメントを監視したい場合は，該当するセグメント内に IDS を設置して監視をするのが普通である．ただし，提案方式ではクラウドネットワークから監視を行う．企業などのイントラネットからアクセス回線を通ってクラウドネットワークに接続される過程には，様々なネットワーク機器がある．代表的なものでは，ルータ，L2-SW などがある．これらの機器がネットワークを分割したり，他のネットワークとの中継を行うことで，現在のインターネット，イントラネットが成り立っている．ところが，一般に，IDS は一つのセグメント内しか監視できない，ネットワークの途中に L2-SW があると全ポート分の監視ができない（ミラーポートを装備している L2-SW であれば，その L2-SW に接続されたネットワークであれば監視は可能）．つまり，クラウドコンピューティング上のネットワークから監視しようとしても，先述の理由により配下のネットワークを監視することは不可能である．そこで，次節では IDS の監視機能を複数セグメントに共通的に適用可能とする方法を検討する．

4.2 提案方式の実現方法

前述の通り，クラウドコンピューティングからイントラネット内の通信の監視は，従来の IDS であると 1 セグメント内しか監視できず，また，ルータや L2-SW などがあると，それを越えた先のネットワークや別のポートに接続されているネットワークへは監視を行うことができない．また，ユーザ同士の通信も，従来の IP ネットワークでは，同セグメント内での通信はそのセグメントのルータ（デフォルトゲートウェイ）で解決できる場合はそこで折り返し，上位のセグメントへ通信は転送しない．本提案

を実現させるためには，どのような通信もクラウド上の IDS（以下，クラウド IDS とで監視する必要がある．このクラウド IDS を実現するため下記の案 1 から案 3 を検討する．

（案 1）VLAN タグを利用する方法

IEEE802.1Q に定められている，タグ VLAN の MAC フレーム内の VLAN グループ情報（VLAN-ID）フィールドを利用する．端末側直近の L2-SW は，ポート毎に違う VLAN ID を付与する．そのままルータを使わず，アクセス回線を経由してクラウドへ接続する．この間，VLAN 間では通信ができない．クラウド内でルータに接続するが，その手間の部分にクラウド IDS の設置ポイントを設け，ここでネットワーク内を監視する．概要を図 2 に示す．これにより，LAN 内での端末間通信を全面的に禁止しつつ，クラウド上の IDS で通信内容の監視を行なうことができる．

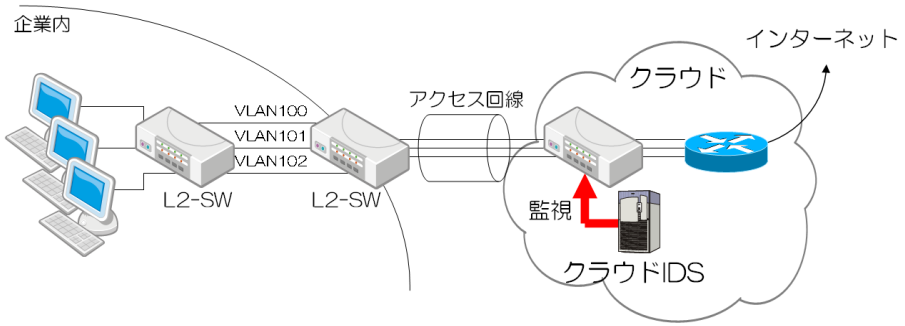

図 2　提案方式（案 1）の概要

（案 2）トラヒック（アクセス）制御を LAN 側で分担する方法

ダイナミック VLAN の機能を利用し，クラウド上の認証・検疫サーバにて認証・検疫を受けた端末（又はサーバ）については，それら同士で随時 VLAN を構成する．すなわち，認証・検疫を受けている端末（又はサーバ）は同一の VLAN 内で通信が許可されるものとする．概要を図 3 に示す ． この方法では，（案 1）のように全トラヒックをクラウド IDS で監視する必要がなくなるが，逆に通信開始後は監視できない．このため，通信中の悪意ある攻撃などは監視できない．

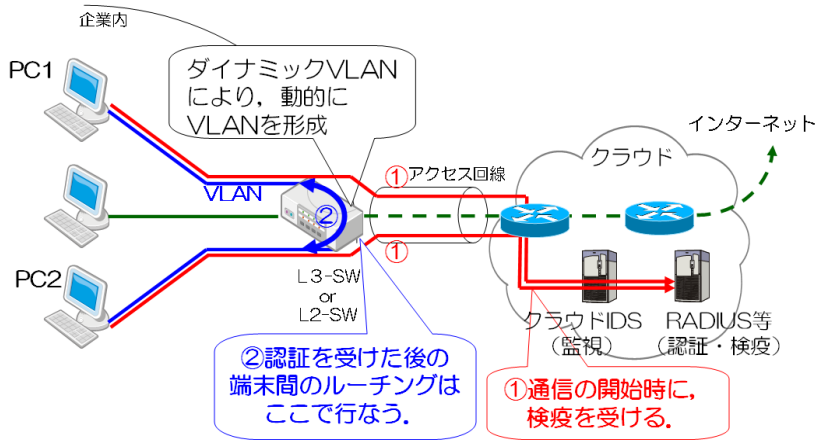

図 3　提案方式（案 2）の概要

（案 3）IDS 機能をユーザネットワークに張り出す方法

（案 1）におけるクラウド IDS の機能を，ユーザネットワークに張り出すことで，ユーザネットワーククラウド間のトラヒック（アクセス回線の負荷）を減らす．クラウド上にはユーザネットワーク内の IDS を制御する機能（IDS 制御サーバ）だけを持たせ，シグネチャの更新等が発生した場合など必要に応じ，クラウドからユーザネットワーク内の IDS を制御する．概要を図 4 に示す．

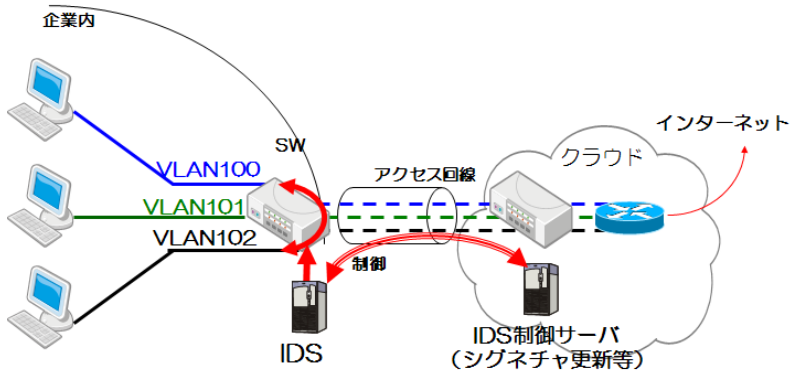

図 4　提案方式（案 3）の概要

本案は，ユーザ側で IDS 機能を果たす機器を用意する必要があり，また，クラウド上に設置した IDS がそれを制御するなど新しい技術が必要となる．

5. 考察

5.1 効果

本提案による効果は以下のように想定される．

(1)ユーザ側作業負担の軽減

SaaS 上でまとめてセキュリティ対策を管理することで，ユーザ側の作業が軽減される．アンチウィルスソフトの導入，OS のパッチ当てなど，現在ユーザが行っている作業は，全て SaaS 上のソフトウェアをアップデートさせるだけになる．また，ネットワーク管理者も，個々人の作業が無くなることで指導や作業説明をする必要が無く，SaaS 上のソフトウェアの設定を変更するだけで新しいセキュリティポリシーを全てのユーザに適用させることができる．

(2)端末（ユーザ）毎セキュリティレベルの均一化

セキュリティ機能が SaaS 上にまとまっているため，SaaS 上でアンチウィルスソフトや OS のパッチの設定に関するセキュリティポリシなどを設定，変更すれば，配下の端末全てに適用されることになる．SaaS 側だけしっかり設定を行なえば，全ての端末は同じセキュリティレベルになる．

(3)端末動作の軽減

セキュリティ対策の関連ソフトを端末にインストールする必要がなくなり，端末動作が軽くなる．例えば，アンチウィルスの機能を SaaS で利用することにより，アンチウィルスソフトなどを端末に入れる必要が無くなるため，端末の動作が軽くなる．

(4)費用の低廉化

SaaS の利用料金等のランニングコストは発生するがシステムの初期構築や更改費用がかからず，総合的に安く安全なセキュリティ機能が利用できる．

5.2 課題と対策

提案方式の課題と対策を以下にまとめる．

5.2.1 課題

(1)利用料金

本提案方式のサービスを提供する場合，システムを利用する費用や管理のための稼動等は既存のクラウドコンピューティング同様概ね低減されると考えられる．しかし，企業のイントラネットとクラウドコンピューティング間で大容量のアクセス回線を必要とする（案 1）では，その回線使用料が膨大になると予想される．そのため，本提案のようなサービスが増えてくることにより，アクセス回線利用料を低廉化することと，セキュリティ SaaS とセットで導入することにより割引を行う，など，大容量の帯域利用に対して割安に提供する仕組みが必要である．

(2)SaaS 化することによる新たなセキュリティ脅威

クラウドコンピューティングにすると新たな脅威が発生する場合がある．クラウドの課題については，Cloud Security Alliance が 2009 年 4 月に発表したガイダンス「Security Guidance for Critical Areas of Focus in Cloud Computing」などで記述されている．実際には主に以下のような問題が考えられる．

(i)ネットワーク上のどこにデータがあるか分からないことによる情報漏えい

クラウドコンピューティングの利用者は自身のデータがどこにあるか一切分からないため，物理的にはユーザの意思で保護することができない．物理的にハードウェアが盗まれ，そこから情報が漏洩してしまう可能性がある．

(ii)ネットワーク機器サーバ機器の構成による情報漏えい

クラウドコンピューティングでは，そのネットワーク機器の構成やサーバ機器の構成がどうなっているのか一切分からない．サーバなどは仮想技術を使ったものもあるが，サーバ機器などへの攻撃により，他者のメモリ空間やディスク領域が読み出されてしまう危険性もある．

(iii) SaaS のサービスが停止することによる事業継続不可

SaaS を利用すると，サーバなどの保守の必要が無いが，その反面，自社の意思でサーバなどのハードウェアを操作することもできない．そのため，機器のメンテナンスを行いたくても行なえない．何らかの要因で故障等が発生しても，ユーザは自身では何も対処できないため，自社が提供するサービスが停止してしまうことも考えられる ．

5.2.2 対策

(1)プライベートクラウドの利用

5.2.1 の(2)の解決方法の一つとして，プライベートクラウドを利用する方法が考えられる．例えばパブリッククラウドであると企業のデータが格納されているサーバの物理的位置が全く不明なのに対し，プライベートクラウドでは構築場所をある程度限定（日本国内だけに設置，等）できるなど，パブリッククラウドよりは安心できる構築方法をとることができる．ユーザは，自社の要件に合った選択をすれば良い．

(2)サーバの設置場所（サーバセグメント）の適正化

サーバは企業情報等が多数格納されており，その設置場所をどこにするかは重要な問題である．パブリッククラウドの場合，前述したような，預けたデータがどこの物理的なサーバ内に格納されているのか明確ではない．そのため，サーバをどこに設置するかは重要な問題である．設置場所を，「パブリッククラウド上」，「プライベートクラウド上」，「自社内」と箇所とした場合，その設置場所の選択にはユーザのセキュリティポリシーによって以下のような(i)～(iii)を選択すればよいと考える．

(i)パブリッククラウドの利用とした場合，ユーザがパブリッククラウドを信用できるならクラウド上，安全のために自社内に置いておくなら自社内，とする．

(ii)パブリッククラウドは信用できないが，プライベートクラウドの利用なら信用できる場合はプライベートクラウドを利用の上，そのクラウド上に置く．

(iii)どちらも信用できないなら自社内に置く．

5.3 個人向けサービスへの展開

本提案は企業向けを想定して検討してきたが，個人向けにサービスを展開しようとした場合について考察する．例えば，現在，インターネットマンション（集合住宅向けブロードバンド接続サービス）においては，マンション内の各戸ごとにインターネットに接続するための設備が備えられており，各戸の設備はマンションに 1 台，または複数台設置されているスイッチに接続され，そこから ISP と接続されている例がある．マンション内のスイッチでは，各戸同士が通信できないように VLAN が構成されている．そこで，マンションに設置されているスイッチ毎にクラウド IDS へ接続する構成とすれば，本提案による SaaS サービスが提供可能であると考える．

6. おわりに

本研究では，まず IP ネットワークのセキュリティ対策は全てクラウドコンピューティングで行うという観点にたち，セキュリティ SaaS の検討を行った．セキュリティ SaaS として既に実現されているサービスや，ASP などネットワーク上で実現されている機能に関してはそのまま適用すればよいが，現状では困難と思われるネットワークの共通的監視機能の実現方法，すなわち， IDS と同様の監視機能をクラウドからの SaaS として実現する方法を提案した．この提案により，ユーザのネットワーク監視に関する負荷が軽減できることを明らかにした．

一方，上記提案については新たな課題もあることも示した．本提案の提供形態によってはアクセス回線の帯域が太いものが必要となり通信コストが嵩んでしまうことが想定されること，また，逆に，アクセス回線の帯域を小さいままで提供しようとすると，ユーザ側のネットワーク機器に新たな監視機能を追加する必要のあることも分った．また，本提案のセキュリティ SaaS に関連する利用料金や新たなセキュリティ脅威，といった課題について対策を考察した．セキュリティサービスをクラウドコンピューティングを用いて実施し，ユーザがより安心安全なネットワークを手軽に安価に利用できる，という目標を達成するため，検討を継続する．

参考文献

[1] 佐藤直，岡田康義，"情報セキュリティレベルに応じたネットワーク利用資格制度導入の提言"，2007 年日本社会情報学会(JSIS&JASI) 合同研究大会研究発表論文集 pp160-163，日本社会情報学会，2007.9
[2] 岡田康義, 佐藤直, "情報セキュリティデータベースを用いたインターネット優先転送方式", 信学技報 ISEC2007-17，2007.7
[3] 佐藤直，岡田康義，"情報セキュリティのための IP ネットワーク利用制御"，情報処理学会第 70 回全国大会，5E-6，2008.3
[4] 堀琢磨，岡田康義，佐藤直，"ユーザの安全性評価に基づいたネットワーク利用制御"，電気情報通信学会，2009,3
[5] 西川康宏，岡田康義，佐藤直，"私的セキュリティポリシを利用した NGN における DoS 対策の考察"SCIS2009，2E3，2009,1
[6] Trendmicro 社,InterScan Messaging Hosted Security, http://jp.trendmicro.com/jp/products/enterprise/imhs/index.html
[7] Trendmicro 社,SMART PROTECTION NETWORK,http://www.trendmicro.co.jp/spn/