# 大規模システムにおけるセキュリティコンサルティング

## Security Consulting in Large Scale Systems

吉田篤正*
Atsumasa Yoshida


### 要　旨

サーバ台数が100台以上の高トラヒックな大規模システムに対するセキュリティSIでは，対象システムで想定されるセキュリティ脅威を洗い出し，その脅威に対抗する必要最低限の重過ぎないセキュリティ対策を実施することが肝要です。

大規模システムのセキュリティSIを実現する上で，セキュリティ対策と性能，運用性，および可用性とのトレードオフをいかに解決していけばよいか，その概要を説明します。

Large scale systems, which consist of several hundreds servers and handle large amount of traffic, need specific security objectives. In security SI for such systems, it is important to dig up threats against the system, and to take necessary and minimum security measures against those threats.

This paper explains how to resolve tradeoff among security measures, performance, applicability, and availability.


### 1．まえがき

NECが実施しているセキュリティコンサルティングの対象システムは，小規模システムから大規模システムまで多岐にわたります。特に，サーバ台数が100台以上で，トランザクション量が数百メガ～数ギガbpsの高トラヒックな大規模システムを対象としたセキュリティコンサルティングでは，セキュリティ対策実施による性能影響あるいは運用への影響を十分に考慮したご提案が必要となります。一般的にセキュリティ対策の実施は性能あるいは円滑な運用とトレードオフであり，このギャップを埋め，お客様のシステム要件を満たすような最適なセキュリティシステムをNECは提案します。

本稿では，このような大規模システムに対していかにセキュリティSIを実現するのか，その手法について具体的に説明します。

### 2．NECのセキュリティコンサルティングメニュー

NECが提供するセキュリティコンサルティングメニューは以下のとおりです。

① セキュリティマネジメントコンサルティング
ISMSに基づいた組織のセキュリティマネジメント確立に向けたコンサルティング

② セキュリティ認証取得コンサルティング
製品やシステムに対するISO15408認証取得のためのコンサルティング，あるいは組織に対するISMS（Information Security Management System）認証取得のためのコンサルティング

③ セキュリティ監査
システムのセキュリティ脆弱性の診断と改善案提示

④ 情報漏えい対策コンサルティング
システムが保有する個人情報の外部への漏えいを防止するためのセキュリティ対策提案

⑤ システムセキュリティコンサルティング
小規模から大規模までのシステムに対するセキュリティ対策の提案およびSI

本稿のテーマである，大規模システムにおけるセキュリティコンサルティングは，項番⑤に相当します。

### 3．セキュリティSIの内容

本章では，大規模システムに対して実施するNECのセキュリティSIの具体的内容について述べます。

#### 3.1　全体方針

高トラヒック，大規模システムに対するセキュリティ対策は，一般的な対策を万遍なく実施するだけでは，かえってシステムに悪影響（性能劣化，運用性悪化，あるいは可用性低下）を与えてしまう可能性があります。これを回避するためには，対象システムで想定されるセキュリティ脅威を洗い出し，その脅威に対抗する必要最低限の重過ぎな

＊ IT基盤システム開発事業部
IT Platform Systems Development Division.

いセキュリティ対策を実施することが肝要です。

本章では，大規模システムのセキュリティSIの具体的内容として，セキュリティ対策と性能，運用性，および可用性とのトレードオフをいかに解決するかについて，概要を紹介します。

① 高トラヒックインターネット口での不正侵入防止対策
② 大規模サーバ群，高トラヒック条件下での円滑な監視運用の実現
③ HA（High Availability）サービス維持のための製品選定

### 3.2 高トラヒックインターネット口での不正侵入防止対策

たとえば，大規模システムがインターネットから大量のトラヒック（数百メガ～数ギガbps）を受けるような場合を想定します。このような場合，ポートスキャン，IPスプーフィング（ソースIPアドレス詐称），smurf攻撃（攻撃対象システムのIPアドレスをソースIPアドレスに詐称設定したping要求パケットをブロードキャストする攻撃），あるいはSynFlood攻撃などのいわゆる不正アクセス/DoS（Denial of Service）攻撃のパケットを含めると，最大Gbpsレベルにも及ぶ超高トラヒックをインターネット口で処理しなければならないケースもあります。

一般的にはインターネットからの不正侵入を防御するためには，Firewallの設置を行いますが，トラヒック要件が非常に厳しいため，処理性能がFirewallよりも優れたIPルータあるいはL3スイッチによるIPパケットフィルタリングもソリューションの一選択肢として想定し，以下の4つの観点で比較検討を行う必要があります。

① セキュリティ強度
② 高速性
③ スケーラビリティ
④ 経済性

比較検討例を**表**に示します。表には，IPルータ，L3スイッチ，およびFirewallについて，上記の4つの観点での特性を記載し，その特性が要件を満たすか3段階評価しました（○：満足，△：難点あり，×：満足しない）。その結果，Firewallの高機能なセキュリティ対策を実現せずとも，サーバ特性や通信形態を考慮すれば，IPパケットフィルタリングのみでセキュリティの確保は可能であるという結論となり，高トラヒック要件を満足するL3スイッチによるセキュリティ対策を提案することになります。

### 3.3 大規模サーバ群，高トラヒック条件下での円滑な監視運用の実現

通常，セキュリティ監視機能として，以下の3種類のセキュリティ監視システムのいずれかあるいはすべてが組み込まれている場合が多々あります。

① 不正侵入検知（Intrusion Detection System：IDS）
システムへの不正侵入パケットをリアルタイムに検知し，監視センターに通報
② ファイル改ざん検知
システムのサーバ群への不正アクセス＆ファイル改ざんを検知し，監視センターに通報
③ ウイルス検知
パターンファイル/検索エンジンのサーバ/端末への定時配信＆定時ウイルス検索

上記の各監視システム導入において，特に超大規模/高トラヒック条件下での特徴的な導入方法について，以下に説明します。

**表　不正侵入防御ソリューションの比較検討**
**Table　Solutions against unauthorized intrusion.**

| 項　目 | IPルータ | L3スイッチ | Firewall |
|---|---|---|---|
| セキュリティ強度 | ○<br>IPパケットフィルタリングにより，ポートスキャン/DoS攻撃/IPスプーフィング等の不正アクセスパケットを遮断，特定ポート/サーバ宛てのパケットのみ通過許可 | ○<br>IPパケットフィルタリングにより，ポートスキャン/DoS攻撃/IPスプーフィング等の不正アクセスパケットを遮断，特定ポート/サーバ宛てのパケットのみ通過許可 | ○<br>IPパケットフィルタリングに加え，ステートフルインスペクションによる動的アクセス制御や，Web脆弱性を狙った攻撃に対する防御可能<br>→サーバが脆弱性対策を実施している場合，あるいはトランザクションが1コネクション上で1対のHTTP Request/Responseが流れる通信形態である場合，Firewallの効用は薄い |
| 高速性 | △<br>レイヤ3/4でのソフトウェア処理によるIPパケットフィルタリング(数百kpps)<br>*pps:PacketPerSecond | ○<br>同一セッションの2番目以降のパケットをハードウェア･スイッチングするため，ワイアスピードMppsの高速IPパケットフィルタリングを実現 | ×<br>レイヤ3以上でのソフトウェア処理，IPパケットフィルタリング性能は数十Mbps<br>→Gbpsの最大トラヒックを処理するためには100台以上のFirewallが必要 |
| 高スケーラビリティ | △<br>アクセスリスト数に応じた性能劣化発生 | ○<br>処理性能はアクセスリスト数に依存しない | △<br>アクセスリスト数に応じた性能劣化発生 |
| 経済性 | ○<br>経路上のネットワーク装置でパケットフィルタリングを実現するため，セキュリティ対策用に専用装置不要 | ○<br>経路上のネットワーク装置でパケットフィルタリングを実現するため，セキュリティ対策用に専用装置不要 | ×<br>Firewall専用装置が必要（数百万） |

(1) 不正侵入検知

IDSは監視対象とする不正侵入パケットタイプを監視ポリシーとして定義し，同一タイプのパケットを検知した場合，監視センターにソースIPとその検知パケット情報を通報するシステムです。一般的には，CVE/CAN（Common Vulnerabilities and Exposures /CANdidates）などの脆弱性情報データベースに基づき，通常セキュリティ観点で危険とみなされるパケットタイプをIDS監視ポリシーに設定します。しかし，これらのパケットタイプのなかには，通常のシステムへのメールトラヒックとして日常的に発生するもの(メールアカウント検索，DNSゾーン転送等）も含まれており，高トラヒックが故にIDS検知メッセージが日常的に大量に発生する可能性があります。このメッセージラッシュにより，監視システムに負荷がかかり，監視センターへの通報が遅延したり，あるいはより重要なメッセージがラッシュメッセージに埋もれてしまう可能性もあり，円滑な運用を妨げる結果となります。

このため，IDS監視ポリシーの各パケットタイプについて，システムのサービスへの影響度を検討し，影響がないものについては，たとえ一般的に危険度が高いパケットタイプであっても，監視センターにリアルタイムに通報はしない設定とすることを提案することも可能です。

たとえば，メールアカウント検索，あるいはバッファオーバーフローの脆弱性を狙ったパケットに対しては，システムのメールサーバがパケット無視，あるいはレングスチェックなどの対策を実施済みのため，メールサービスへの影響はないと判断し，監視センターにリアルタイムに通報しない設定としました。

(2) ファイル改ざん検知

ファイル改ざん検知システムは，監視対象ディレクトリ/ファイル，および監視対象のファイル属性を「監視ポリシー」としてあらかじめ定義し，監視ポリシーに記述された監視対象ファイルの監視対象属性が変更されると，それを検知し，監視システムに通報します。

サーバ群が大規模である場合，保守作業の頻度が高く，サーバのOSリブート，failover（クラスタ構成において，アクティブ側サーバをリブートし，スタンバイ側サーバをアクティブ側に組み込むこと），あるいはハードウェア障害によるサーバOSリブートなどが頻発します。このような事象発生時に，OSの挙動として監視対象ファイルが動的に更新されることにより，改ざんではないにもかかわらず，改ざん検知通報が監視センターにあがってしまい，いわゆる誤検知が大量に発生してしまう可能性があります。

これを回避するために，OSリブート時やハードウェア障害発生時などでのOSファイルシステムの挙動を，監視ポリシー設計時によく調査分析し，誤検知が発生しないポリシーを設定することが必要となります。

(3) ウイルス検知

監視対象サーバ数および端末数が大規模である場合，パターンファイルダウンロード，あるいはウイルス検索は，センター集中型で端末側操作が一切発生しない自動化運用でなければ，監視対象サーバ群および端末群を同一のセキュリティレベルに保つことは不可能です。

このような場合，パターンファイル/検索エンジンの定時ダウンロード＆配信，定時ウイルス検索，ウイルス検知時通報を1サーバで統合管理できる製品を含めたシステム提案が有効です。

### 3.4 HAサービス維持のための製品選定

Webを使った決済システム，あるいはネットオークションシステムでは，HTTPコンテンツに住所，電話番号，あるいはクレジットカード番号などの個人情報が含まれます。このため，クライアント詐称を防止すること，さらに通信路上を流れる個人情報の漏えいを防止することが必要であり，そのためのセキュリティ対策としてSSL（Secure Socket Layer: Webサーバとブラウザ間の暗号化と認証）アクセラレータを適用することをご提案することがあります。SSLアクセラレータは，ハードウェア専用装置が一般的でありますが，このようなシステムにはサービス特性上，24時間365日ノンストップ稼働を求められるシステムもあり，このため，装置故障時に24時間365日直ちに故障対応を行うことのできるHAサービスが製品事業部/ベンダにより提供される必要があります。このため，SSLアクセラレータ選定の際には，機能面，性能面だけでなく，保守サポートレベルも選定条件に加え，ハードウェア製品だけでなく，ソフトウェア製品も候補製品に加えて，製品比較検討を行う必要があります。

1つの例として，以下の3製品を，機能面，性能面，および保守サポートレベルで比較検討すると，下記のような結果となります。

- F5社（F5ネットワーク社）製SSLアクセラレータ（ハードウェア専用装置）
- SonicWall社製SSLアクセラレータ（ハードウェア専用装置）
- HP社（ヒューレット・パッカード社）製SSLProxyサーバ（NX7700/i4410アプライアンスソフトウェア製品）

(1) 機　能

3製品とも，SSLハンドシェイク（クライアントからのHTTPSリクエストを受信し，SSLサーバ証明書によるサーバ認証，およびクライアント証明書によるクライアント認証を行うための通信シーケンス）を行った後，クライアント証明書のDN（Distinguished Name：クライアント識別子）情報をWebサーバに転送する機能は同様です。また，1＋1の冗長構成もいずれの製品も可能であり，機能面では差異はありませんでした。

(2) 性　能

同一のクライアントからWebサーバへの一トランザクションの間には，複数のHTTPコネクションの接続/切断が含まれます。HTTPコネクション確立時のSSLハンドシェ

イクは，新規接続時のみ鍵交換のため処理が重たくなるため（ヘビーハンドシェイク），同時新規接続時のHTTPSコネクト要求処理性能がSSLアクセラレータの性能指標となります。この処理性能は，3製品ともトラヒック要件を満たすため，性能面でも差異はありません。

(3) 保守サポートレベル

F5社およびSonicWall社とも，原則，9時から17時の対応のみであり，ソフトウェア障害発生時には，基本的に再現する場合のみ対応可能とのことであり，一方，HP社は，ソフトウェア障害発生時には，24時間365日，直ちに故障対応を行うことのできるHAサポートが可能とのことです。

以上の比較検討結果より，保守サポートレベルが決め手となり，HP社製アプライアンスソフトウェア製品を，SSLアクセラレータとして提案することも，1つのソリューションとなります。

## 4. むすび

今回紹介した，大規模システムに対するセキュリティSIの手法の根底には，「対象システムで想定されるセキュリティ脅威を洗い出し，その脅威に対抗する必要最低限の重過ぎないセキュリティ対策を実施する」という基本的考え方があります。これは，対大規模システムに限らず，あらゆるシステムに対して適用できる，否，適用しなければならない手法であると考えます。

今後，性能，運用性，および可用性とのバランスのとれたセキュリティコンサルティングを実施していきますので，関係各部門のご協力をよろしくお願いいたします。

＊本稿に記載している社名，商品名は，各社の商標または登録商標です。

### 筆者紹介

Atsumasa Yoshida
吉田（よしだ） 篤正（あつまさ） 1983年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センターコンサルティングマネージャー。