日本セキュリティオペレーション事業者協議会の活動報告

株式会社ラック
武智　洋

1. はじめに

2008年6月13日 JNSA総会にて日本セキュリティオペレーション事業者協議会(Information Security Operation providers Group Japan, 略称名：ISOG-J)が発足いたしました。発起人10社からスタートし約10ヶ月が過ぎ、2009年2月時点で会員団体は17社となり、活発な活動が行われています。今回はこのISOG-J について、発足経緯および現在までの活動についてご紹介したいと思います。

●発足にいたるまで

一般的な意味でセキュリティが重要だと言うことに異論を挟む人はいないと思います。また、セキュリティのレベルを維持していくための日々の運用に関しても、多くの人が重要だと言ってくれるのではないでしょうか。 以前、研究としてセキュリティ監視システム運用に関係する仕事をしており、日々、セキュリティに関わるシステムの運用ってどうしたらよいのだろうと悩んでおりました。同僚と雑談する中で確認したのは、

- そのセキュリティに関わる運用(セキュリティオペレーション)がどんなものなのか、明確な定義がない
- セキュリティオペレーションに携わる人たちがどのように働いているのか明確なイメージがない
- 何より、いろいろ相談したくても、セキュリティオペレーションに関わっている人たちのコミュニティがない

ということでした。で、ある日、ISOG-Jのきっかけになることを思いついたのです。

「セキュリティオペレーションに携わっている人たちと意見交換をしてみよう！」

仕事柄、この分野の知り合いは多かったので、その中から、問題意識が高く、社外活動も活発な人たちに2007年秋に相談をしました。順次、人が加わり、様々な話をするうちにセキュリティオペレーションに関係する事業を行っている人たちが集い、問題解決を行えるような場が必要という結論に達しました。そして、最終的に10社から発起人が集まり、ISOG-Jを設立することになったのでした。

●設立に当たっての問題意識

設立に向け発起人の間でセキュリティオペレーションに関して話をしました。

例えば、これは私自身の話ですが、ある仕事でセキュリティオペレーションセンター（SOC）構築の RFPを書こうとしたときに困ったのは、SOCの機器やシステムの要件はある程度書くことができるが、運用の部分の要件が上手く書けないというものでした。

SOCの運用ですので、24時間365日稼働というのはわかるのですが、それ以外SOCの運用に関して基準が明確でない。

また、運用に携わる人材の要件を考えたときに、単にオペレータあるいは、アナリストと呼んだとしても、それらの人材がどのようなスキルセットを持つべきか、どのようなレベルの人が必要であるのかなど、基準となるものが無いということでした。

SOC構築のRFPを書くというのは、あまりないことと思いますが、一般に企業の情報システム担当がセキュリティに関する運用をアウトソースしようとした場合にも、同じようなことが起こるのではないかと思います。

また、ユーザが様々な事業者から出ているサービスを比較することが出来るようなセキュリティオペレーションサービスマップも必要ではないかということになりました。

こういった話し合いをする中で、セキュリティオペレーション事業者の各社もさまざまな問題意識や解決案を持っていることや、セキュリティ情報を扱う性格上、情報共有が難しいジレンマなどが見えてきました。

このような議論の中、ISOG-Jの活動で扱うべき課題として次のようなものが挙がってきました。

1)セキュリティオペレーションとは何なのか
2)ユーザにセキュリティオペレーションを使ってもらうために必要な情報は何なのか
3)セキュリティオペレータが持つべきスキルとは?
4)セキュリティオペレーションの重要性をもっと世の中の人に知ってもらうにはどうしたらよいか

これらの問題意識を元にいくつかのワーキンググループを作り活動を始めました。

2. ISOG-J 設立経緯と目的

設立経緯

電子メールの普及、インターネットバンキング、電子商取引など、我々を取り巻くIT環境は人々の生活、企業活動、各種社会活動に無くてはならない基盤となっています。基盤化したIT環境が停止することは許されず、“止まらないサービス”を実現することへの要求がますます高まっています。また、不正アクセスやサイバー攻撃は多様化し、その手口もますます巧妙になりつつあります。

ITシステム運用においても、ITシステムのセキュリティを確保するためのオペレーションは各組織の業務として必須となっています。

各企業等においては、セキュリティポリシー策定など制度面の対策の整備が進んでおり、そのなかで、セキュリティに関するオペレーションも対象となっています。しかし、実際のセキュリティオペレーションを各組織でしっかりと行うことは容易ではない状況といえます。

原因としては、人材確保が難しいこと、セキュリティオペレーションをどのようにやればよいのか、どこまでやるべきなのかについての具体的な指針がないことなどがあります。

また、セキュリティオペレーションのアウトソースに関しても、セキュリティオペレーションアウトソースサービスに関しての情報がサービス事業者毎に表現が異なっており、一様に比較検討しにくいこと、また、事業者側としても、サービスの内容と品質を規定する基準が整備されていないことなどの問題点があります。

このようなセキュリティオペレーションに関する現状と課題を改善するためには、セキュリティオペレーションとはどういうものか、あるいは、どうあるべきかについてユーザおよびセキュリティオペレーション事業者に共通の理解を持てるようにしなければなりません。

また、利用にあたっての様々なガイドラインや指標を策定していくことも必要と考えます。

しかしながら、これらのことを議論し、具体的に問題解決を行う場がない状況です。このような状況を鑑み、現在、セキュリティオペレーションサービスを提供している事業者が結集して、セキュリティオペレーションの必要性を社会にアピールし、かつ、諸問題を解決していく場として、本組織の設立を行います。

目的

日本セキュリティオペレーション事業者協議会は、セキュリティオペレーション技術向上、オペレータ人材育成、および関係する組織・団体間の連携を推進する事業を実施することによって、セキュリティオペレーションサービスの普及とサービスレベルの向上を促し、安全で安心して利用できるIT環境実現に向けて寄与することを目的としています。

3. 参加組織

会員(発起人)
株式会社アイアイジェイテクノロジー
株式会社インターネットイニシアティブ
エヌ・アール・アイ・セキュアテクノロジーズ株式会社
株式会社エヌ・ティ・ティ・データ
日本電気株式会社
日本電信電話株式会社
株式会社日立情報システムズ

富士通株式会社
三井物産セキュアディレクション株式会社
株式会社ラック
会員
NECネクサソリューションズ株式会社
エヌ･ティ･ティ･コミュニケーションズ株式会社
NTT コムテクノロジー株式会社
日本アイ･ビー･エム株式会社
株式会社富士通ソーシアルサイエンスラボラトリ
株式会社ブロードバンドセキュリティ
株式会社Kaspersky Labs Japan
オブザーバー
総務省
経済産業省
アドバイザー
北陸先端科学技術大学院大学　篠田陽一教授

4. WGの紹介

セキュリティオペレーションガイドラインWG

リーダー：ブロードバンドセキュリティ　許　先明
サブリーダー：
　　IIJ　齋藤　衛
　　三井物産セキュアディレクション　青木　歩

セキュリティオペレーションサービスの利用に関するガイドラインの作成を目標とするWGです。

一般に、セキュリティオペレーションに関するサービスは、ネットワークサービスやサーバーサービスなどと異なり、どのようなサービスが提供され、どのような機能があるのか等の情報が少なく、サービス導入に当たってアウトソースする場合、RFPを書くことが難しいという現状があります。本WGではこの問題を改善し、サービス導入やRFP作成の際などに利用するための指標となるようなガイドラインを作成することが目標です。

当WGでは、まずセキュリティオペレーションサービスに関するサービスマップの作成をすべく活動を行っており、今年度の成果として提出する予定です。来年度より、サービスマップを基にガイドラインに関する検討を始める予定となっております。

セキュリティオペレーション技術WG

リーダー：ラック　川口　洋
サブリーダー：
　　NECネクサソリューションズ　中西　克彦
　　日立情報システムズ　浅野　豊

セキュリティオペレーションに関わるエンジニアの技術力向上、エンジニア同士の交流を目的としたWGです。

セキュリティオペレーションといってもかかわっている人の仕事の内容はさまざまであり、抱えている課題も違います。

それぞれのセキュリティオペレーションの現場で奮闘している技術者の課題を解決し、技術力を向上していくことが目的です。

これまでにWGの会合を4回行いました。会社見学、セキュリティ製品の製品説明会などと行いました。

また、WGの会合の後には必ず懇親会を行っています。参加者同士の交流を重ねるうちに、お互いの課題や業界の課題についての認識を共有することができればと思っています。

今ではこの懇親会自体がWGのメインであると言われているくらいに恒例となっています。

セキュリティオペレーションに関わる方のご参加をお待ちしています。

セキュリティオペレーション関連法調査WG

リーダー：富士通　出口　幹雄
サブリーダー：NTT　雨宮　俊一

ユーザ･セキュリティオペレーション事業者がそれぞれの立場で遵守すべき関連法規について整理･情報発信することを目的としたWGです。

セキュリティオペレーションといっても不正アクセス対策･ウィルス対策･情報漏洩対策･迷惑メール対策等さまざま種類があり、サービス実施する内容によって意識しなくてはならない法律が変わってきます。

また、ユーザ・セキュリティオペレーション事業者の業種・業態によって監督官庁が違ったり、業界固有ガイドラインがあったりと遵守すべきものが異なるといった点もあります。

このような環境下でセキュリティオペレーションの関連法規をユーザ、事業者が共通の認識を持ちそれぞれが遵守すべき事を相互に理解しあうことでセキュリティオペレーションの認知度向上にもつながることを目指しております。

興味のある方の参加をお待ちしております。

セキュリティオペレーション認知向上・普及啓発WG

リーダー：ラック　武智　洋

サブリーダー：

NTT　渡瀬　順平

日立情報システムズ　多田　昭仁

セキュリティオペレーション事業をより皆さんに知っていただくことと、この業界に関わる人財の地位向上を目指した様々な活動を企画することを目標としたWGです。

ISOG-Jには、セキュリティオペレーション事業を通して、ユーザ組織のセキュリティレベルを向上することを目標としている事業者が集っています。セキュリティオペレーションへの我々の熱い思いを知っていただくには、まずは、ユーザにセキュリティオペレーション事業という業界そのものについて知っていただく必要があると考えています。また、セキュリティオペレーション事業の核となるのは、オペレータやアナリストなどの人財です。現在、日々セキュリティレベル向上のために頑張っているオペレータがいることを世の中の多くの方に知ってもらうことも重要なISOG-Jの役割だと考えています。

こういったことを目的に、今年度は、まずはISOG-J 内での活動を中心として行ってまいりましたが、来年度からは外部に向けての積極的な活動を行っていく予定です。

5. イベント報告

■JNSA 2007年度活動報告会（2008年6月13日）

「日本セキュリティオペレーション事業者協議会（ISOG-J）発足について」報告。

■JNSA主催「Network Security Forum 2008」

（2008年12月17日）パネルディスカッションを実施。

「最新セキュリティ事情とセキュリティ運用の勘所～セキュリティオペレーションの現場から～」

■ラックJSOC見学

■富士通館林センタ見学

■NTT武蔵野研究所見学

6. 今後の展開

今後もWG主体による活動を継続していくと共に会員団体、オブザーバー、アドバイザー、外部専門家を招いてセキュリティオペレーションに関する講演会も計画しています。

7. 連絡先

JNSA事務局（E-Mail）：isogj-info@jnsa.org

8. まとめ

本協議会の設立に関しては、関係各位の協力を頂き、活動を開始することができました。

各WGの活動も活発に行われ、活動初年度の成果物としていくつかのアウトプットも報告できる見込みです。

今後ともセキュリティオペレーション事業者がISOG-Jとして一丸となり、安全で安心して利用できるIT環境実現に向けて努力していく所存です。

引き続きの関係各位のご支援、セキュリティオペレーション事業者の参加をお願い致します。