NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

ISOG-J年間活動報告
「セキュリティオペレーション事業の現状問題点と改善課題について」

日本セキュリティオペレーション事業者協議会
ISOG-J
2009年6月3日

発表内容

- 1年間の活動
- セキュリティオペレーションガイドラインWG
- セキュリティオペレーション技術WG
- セキュリティオペレーション関連法調査WG
- セキュリティオペレーション認知向上・普及啓発
- 今後の活動

JNSA

設立のきっかけ

- 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）がどのようなものか、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

JNSA

課題

- セキュリティオペレーションとは何か
- セキュリティオペレーションに関してユーザに必要な情報は何か
- セキュリティオペレータが持つべきスキルとは？
- 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

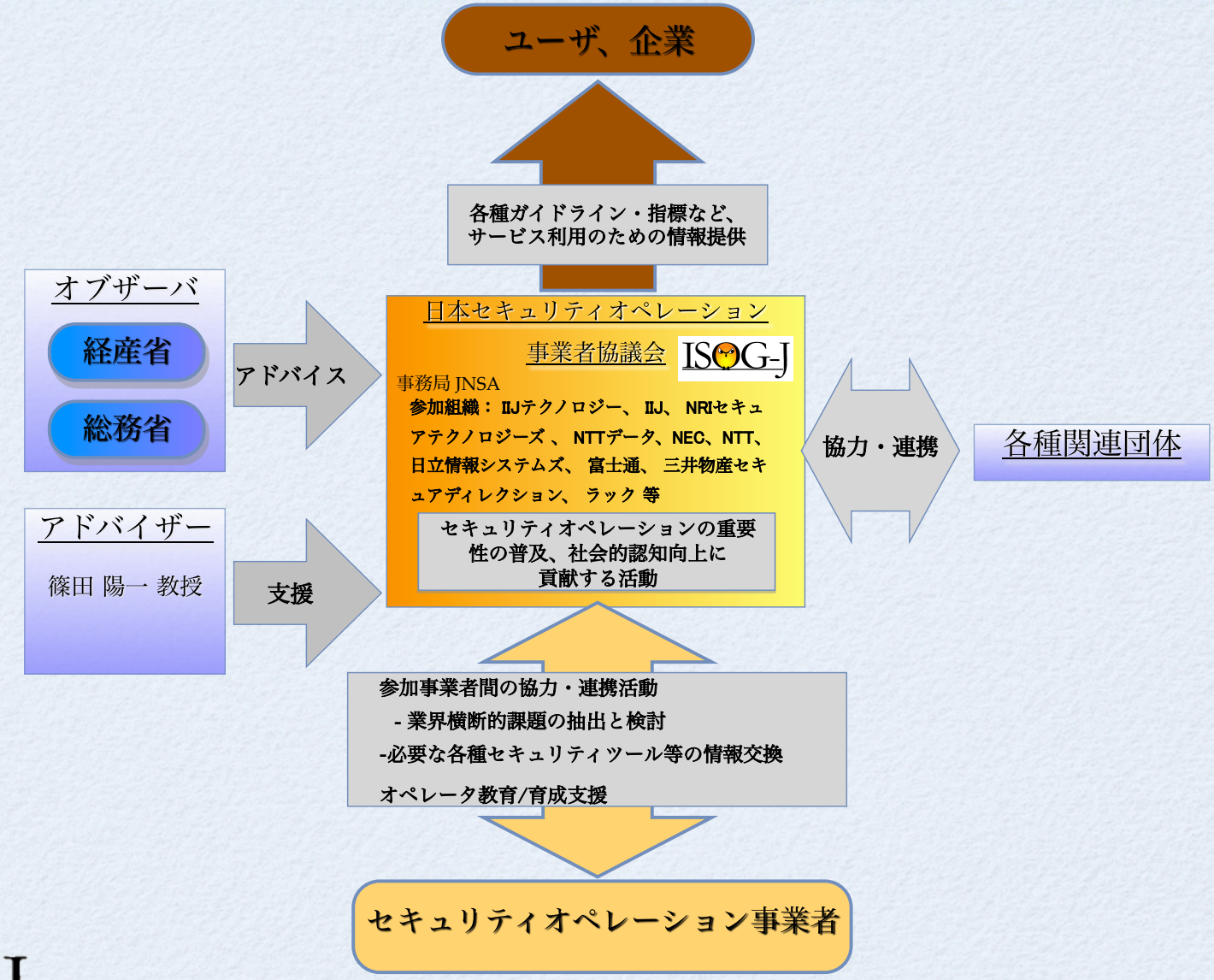
JNSA

ISOG-J設立の目的

- ユーザへの各種情報提供
  - セキュリティオペレーションサービスの各種ガイドライン・指標の作成
- 参加事業者間の協力・連携
  - セキュリティオペレーションに関する業界横断的な課題の抽出と検討
  - セキュリティオペレーションに必要な各種セキュリティツール等に関する情報交換
  - 横断的なオペレータ教育/育成支援活動
- 他の関連団体との協力・連携
- セキュリティオペレーションの重要性の普及・社会的認知向上への貢献
- セキュリティオペレータ間の交流の促進

JNSA

ISOG-J の概要



ISOG-J

JNSA

この一年で…

- 2008年6月13日 発足
  - 約一年たちました
- 会員
  - 発足時10社、現在、17社
- オブザーバー・アドバイザリー・関連団体
  - 情報処理推進機構(IPA) 様が活動へ参加
- 活動メンバー数
  - 登録メンバー数 約80名
- 運営委員会とWGの設立と活動
  - 原則それぞれ月1回開催（今までで合計約40回の会合開催）

JNSA

会員企業

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
NECネクサソリューションズ株式会社
株式会社エヌ・ティ・ティ・データ
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
株式会社 Kaspersky Labs Japan
日本アイ・ビー・エム株式会社
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
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
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

JNSA

協力組織等

- オブザーバー
  - 経済産業省
  - 総務省
- アドバイザリー
  - 北陸先端科学技術大学院大学 篠田陽一教授
- 関連団体
  - JPCERT/CC（有限責任中間法人JPCERTコーディネーションセンター）
  - IPA（独立行政法人　情報処理推進機構）

JNSA

ISOG-JのWG

1. セキュリティオペレーションガイドラインWG
2. セキュリティオペレーション技術WG
3. セキュリティオペレーション関連法調査WG
4. セキュリティオペレーション認知向上・普及啓発WG

JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

セキュリティオペレーション ガイドラインWG

(株)ブロードバンドセキュリティ
許 先明

ISOG-J

What is WG1

- 「セキュリティオペレーションガイドライン」WG
  - 現在、様々なSecurity Serviceが提供されている
    - 利用者から見てどんなサービスか判らない
      - 何をしてくれるのか、どのような効果があるのか
  - どのようなサービスがあるのか？
    - 今の段階でどんなサービスが利用できるの？
    - 将来どんなサービスを利用すればよいの？
    - Alternativeはあるの？
  - どのようにサービスを利用すればよいのか？
    - 出来ることは何？出来ないことは何？

JNSA

WG1 Goal

- Security Serviceを分類する
  - Service MAPを作成する
  - Service MAPを保守する
- サービス利用者のためのガイドラインを作成する
  - 利用すべきサービスを理解するためのガイドライン
  - どんなサービスであるのかを理解するためのガイドライン
  - RFPを書くときに参考にできるガイドライン

JNSA

Output of year 2008

- 2008年度は、Service MAPの作成を実施
  - サービスのライフサイクルを元にマップを作成
    - 横軸にサービスのフェーズ、縦軸に保護対象
    - 様々な軸の取り方が考えられるが…
  - ISOG-J参加組織のサービスを基にしてマップを作成
    - 「Security Consultingというだけで大部分が含まれてしまう」
      - できるだけ判りやすいように分類した
    - 「名前は似たようなサービスだけど、微妙に違う」
      - サービスをジャンル分けしてなるべく判りやすくする

2008年夏時点のサービスは概ね盛り込めた（と思いたい）

JNSA

Why Service MAP

- Security Serviceを体系的に分類した物が無い
  - Security Serviceを理解するための基礎資料がなかった
  - サービス提供者毎に異なる「サービス名称」
  - どんなサービスが利用できるのかも判らない

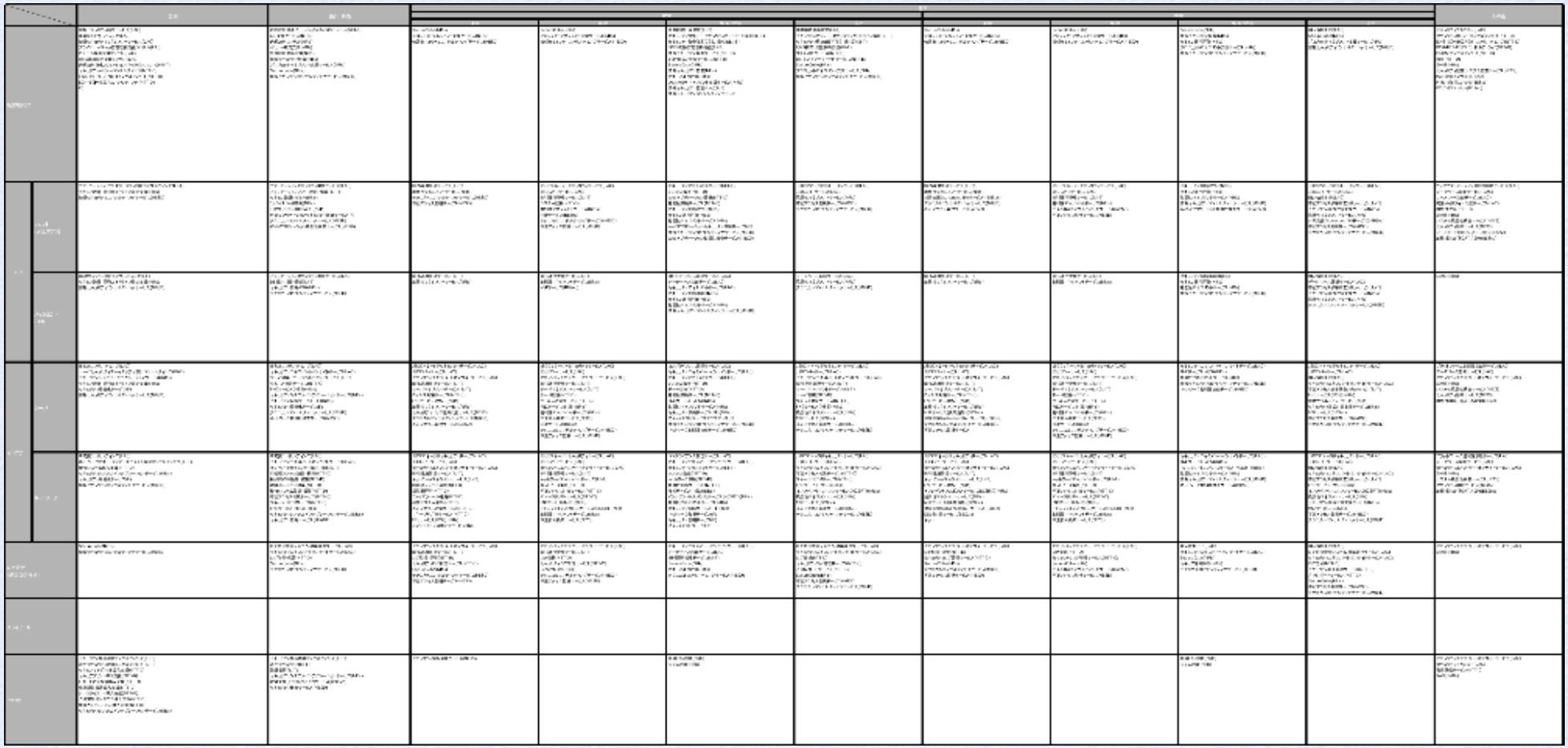
ここを解決しなければガイドラインも書けない

- その為にService MAPを作成する
- いつ、どのようなサービスを検討すればよいのか？
- どんなサービスがあるのか

参加各社の協力を得てサービスマップを作成する

JNSA

サービス分類表



はっきり言って、読めません!!
目がちかちかします

Creating Service MAP

- 分類表の作成
  - 作成に4ヶ月を費やす
- サービス分類表を基に、サービス分類の検討を行った
  - 様々な問題発生
    - 一般的なサービス名称が未定義のサービスが多い
    - 同じような名称でも対象範囲が微妙に異なる
  - 大量の議論
    - 分類方法の議論、MAPの範囲や作り方、情報収集
    - 内容に関わる物や全体のまとめ方、公開方法など

JNSA

最終Service MAP

		企画	設計・構築	運用						その他
				定常			異常			
				運用・監視	分析	監査/評価	運用・監視	調査	対応	
組織		認証・資格取得支援 ポリシー・ガイドライン作成支援 啓発普及等	認証・資格取得支援 ポリシー・ガイドライン作成支援 プロジェクト管理支援	セキュリティ管理運用支援	セキュリティ管理運用支援	認証・資格審査 監査・資格監査支援 セキュリティ監査	セキュリティ管理運用支援 緊急対応	緊急対応 影響度分析 フォレンジック	対応支援	セキュリティ情報提供 セキュリティ教育・研修
アプリ	フロント (Webアプリ等)	要件定義支援	設計支援 レビュー支援 脆弱性検査	システム監視・運用 セキュリティ機器監視・運用	脆弱性診断 ログ分析	脆弱性診断	システム監視・運用 セキュリティ機器監視・運用 事後対応	対応策策定 脆弱性検査 原因調査 フォレンジック	対応確認検査	セキュリティ情報提供 セキュリティ教育・研修
	バックエンド (DB等)	要件定義支援	設計支援 レビュー支援 脆弱性検査	システム監視・運用 セキュリティ機器監視・運用	脆弱性診断 ログ分析	脆弱性診断	システム監視・運用 セキュリティ機器監視・運用 事後対応	対応策策定 脆弱性検査 原因調査 フォレンジック	対応確認検査	セキュリティ情報提供 セキュリティ教育・研修
インフラ	サーバ	要件定義支援	設計支援 レビュー支援 脆弱性検査	システム監視・運用 セキュリティ機器監視・運用	脆弱性診断 ログ分析	脆弱性診断	システム監視・運用 セキュリティ機器監視・運用 事後対応	対応策策定 脆弱性検査 原因調査 フォレンジック	対応確認検査	セキュリティ情報提供 セキュリティ教育・研修
	ネットワーク	要件定義支援	設計支援 レビュー支援 脆弱性検査	システム監視・運用 セキュリティ機器監視・運用	脆弱性診断 ログ分析	脆弱性診断	システム監視・運用 セキュリティ機器監視・運用 事後対応	対応策策定 脆弱性検査 原因調査 フォレンジック	対応確認検査	セキュリティ情報提供 セキュリティ教育・研修
クライアント		要件定義支援	シンクライアント パッチ管理 検疫ネットワーク	シンクライアント パッチ管理 検疫ネットワーク	端末挙動分析	端末検査	シンクライアント パッチ管理 検疫ネットワーク 端末検査 事後対応	対応策策定 端末検査 原因調査 フォレンジック	対応確認検査	セキュリティ情報提供 セキュリティ教育・研修
その他		物理セキュリティ関連	物理セキュリティ関連	物理セキュリティ関連 ログ保全			物理セキュリティ関連 ログ保全			セキュアメール セキュアファイル交換 PKIソリューション データ暗号

本年度の成果を、一般公開する予定です
ISOG-JのWeb Page等をご参照下さい
(http://www.jnsa.org/isog-j/index.html)

Goal of year 2009

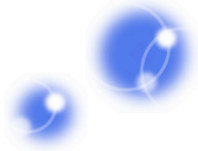
- Service MAPの保守
  - 内容の見直しや追加・削除
- ガイドラインの作成
  - 各サービス毎にガイドラインを作成する
    - 今年度は恐らく１つ
      - うまく行って２つ？
    - 運用サービスか脆弱性診断か、…

頑張ります

としか言えません

JNSA

ありがとうございました



NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

セキュリティオペレーション
技術WG

(株)ラック 川口 洋

ISOG-J

技術ワーキンググループ

- 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、情報交換、交流を目的とするWG。
- 基本的に月に1回開催
- 各企業さんの訪問、見学、サービス説明、製品説明、技術情報交換などを実施（実績は次ページ）

- リーダ：川口（ラック）
- サブリーダ：中西（NECネクサソリューションズ）、浅野（日立情報システムズ）

- 大きな目的は”交流”です。

JNSA

会合状況

- 2008/9/30：第1回目
  - ラック。キックオフ。顔合わせ。
- 2008/10/23：第2回目
  - ラック。Fortify様製品紹介。
- 2008/11/26：第3回目
  - 富士通センター見学。SecureSoft様製品紹介。
- 2009/1/27：第4回目
  - NTT武蔵野研究開発センタ見学。
- 2009/2/25：第5回目
  - NECネクサソリューションズ。住商情報システム様製品紹介。
- 2009/3/19：第6回目
  - IBMセンター見学。製品紹介。
- 2009/4/22：第7回目
  - NTTコミュニケーションズ。IDS/IPS/UTMの検知回避の実験
- 2009/5/27：第8回目
  - NEC。

JNSA

セキュリティオペレーション
関連法調査WG

富士通株式会社
出口 幹雄

ＷＧ３の目的

- セキュリティオペレーション定義の明確化
- 意識するべき関連法規
- 各種遵守事項(監督官庁, 業界固有ガイドラインなど)

整理・情報発信

セキュリティオペレーションの認知度向上
ユーザ・SOC事業者間での遵守すべき法規 相互理解

JNSA

活動状況

日程		場所	活動内容
第1回	08.09.09	富士通	・キックオフ、会社の状況紹介 ・関連法規の情報ソース洗い出し。
第2回	08.10.20	BBSec	・法律一覧たたき台レビュー ・法規のカテゴリー検討
第3回	08.11.26	富士通	・法律一覧たたき台二次レビュー ・ユーザと事業者との契約形態、契約のあり方検討
第4回	09.01.23	日立情報	・法律一覧カテゴライズ実施。 ・法律要求事項の解説、意見交換
第5回	09.02.27	ラック	・法律要求事項に対するSOCで関連する事例、事象（案） 意見交換
第6回	09.04.16	富士通	・法律一覧及び法律要求事項に対するSOCで関連する事 例、事象のレビュー（1回目）
第7回	09.05.19	ラック	・法律一覧及び法律要求事項に対するSOCで関連する事 例、事象のレビュー（2回目）

＊会社名は、敬省略

JNSA

関連法規一覧（サンプル）

個人情報保護法　:個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号）　最終改正:平成一五年七月

法律	条番	項番	題名	条文	違反時の措置	概要	SOC事業における想定シーン
個人情報保護法	第15条		利用目的の特定	個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。		取り扱う個人情報に関して、利用目的を特定しなければならない	→条文の通り
		2		個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。		利用目的変更の場合、変更前との関連性が合理的に認められる範囲である必要がある	設定シートで集めた情報を、SOCサービスの変更(サービスエンハンス)にあわせて使用していくことは許される。
個人情報保護法	第16条		利用目的による制限	個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。	主務大臣による監督指示に従わない場合、六月以下の懲役又は三十万円以下の罰金	（条文の通り）	設定シートで集めた情報を、本人の同意なく他の目的で使用してはならない。

消防法　:消防法(平成21・5・1・法律　34号 改正)

法律	条番	項番	題名	条文	違反時の措置	概要	SOC事業における想定シーン
消防法	第5条		火災の予防	消防長又は消防署長は、防火対象物の位置、構造、設備又は管理の状況について、火災の予防に危険であると認める場合、消火、避難その他の消防の活動に支障になると認める場合、火災が発生したならば人命に危険であると認める場合その他火災の予防上必要があると認める場合には、権原を有する関係者（特に緊急の必要があると認める場合においては、関係者及び工事の請負人又は現場管理者）に対し、当該防火対象物の改修、移転、除去、工事の停止又は中止その他の必要な措置をなすべきことを命ずることができる。ただし、建築物その他の工作物で、それが他の法令による建築、増築、改築又は移築の許可又は認可を受け、その後事情の変更していないものについては、この限りでない。 ○2　第三条第四項の規定は、前項の規定により必要な措置を命じた場合について準用する。	第五条第一項の命令違反者に対して、二年以下の懲役又は二百万円以下の罰金（§ 39の3の2）	消防長又は消防署長からの防火対象物の位置、構造、設備又は管理の状況についての改善命令には従うこと。	SOCセンターに対する、消防に関する改善命令には従い、必要な改善を実施しなくてはならない。

下請法:下請代金支払い遅延等防止法

法律	条番	項番	題名	条文	違反時の措置	概要	SOC事業における想定シーン
下請法	第2条の2		下請代金の支払期日	下請代金の支払期日は，親事業者が下請事業者の給付の内容について検査をするかどうかを問わず，親事業者が下請事業者の給付を受領した日（役務提供委託の場合は，下請事業者がその委託を受けた役務の提供をした日。次項において同じ。）から起算して，60日の期間内において，かつ，できる限り短い期間内において，定められなければならない。		下請代金の支払期日が定められなければならない。	・契約時に、支払期日を明記した文書が含まれなければならない。
		2		(省略)			
下請法	第3条		書面の交付等	親事業者は，下請事業者に対し製造委託等をした場合は，直ちに，公正取引委員会規則で定めるところにより下請事業者の給付の内容，下請代金の額，支払期日及び支払方法その他の事項を記載した書面を下請事業者に交付しなければならない。ただし，これらの事項のうちその内容が定められないことにつき正当な理由があるものについては，その記載を要しないものとし，この場合には，親事業者は，当該事項の内容が定められた後直ちに，当該事項を記載した書面を下請事業者に交付しなければならない。	50万円以下の罰金（親事業者の代表者、代理人、使用人その他の従業員）	親事業者は、必定事項を記載した書面を下請業者に交付しなければならない。	SOCにおける委託の例 (1) 情報成果物作成委託がよく起こりうると考えられる。典型的な例としては、自社のシステム開発の一部（プログラム開発等）を外部に委託するパターンが考えられる。 (2) 役務提供委託の例としては、客先への機器設置作業を下請事業者に委託するパターンが考えられる。 (3) 修理委託の例としては、客先の設置機器の修理を下請事業者に委託するパターンが考えられる。

今後の計画

- 法令一覧（第1.0版）完成に向けて継続レビュー（2009年9月末）
- 法律関連の有識者との意見交換
- 一般向け小冊子の作成（2010年3月末目標）
- 業界ガイドラインの要求事項とＳＯＣ事業の想定シーンの検討
- 契約とリスクに関する意見交換

JNSA

セキュリティオペレーション
認知向上・普及啓発WG

(株)ラック 武智 洋

活動内容

- セキュリティオペレーション事業の認知度を向上したい！をかなえるべく、まずは、ISOG-Jを活性化させるため、裏方に徹するWGとして設立
  - 運営委員会の支援
  - 内部中間報告会
  - 内部セミナー開催
  - 外部発表支援
    - NSF2008 パネルディスカッション
      「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～」
  - 関連団体との調整

JNSA

総括　1年間の成果

- ユーザへの各種情報提供活動
  - セキュリティオペレーションサービスの各種ガイドライン・指標の作成
- 参加事業者間の協力・連携活動
  - セキュリティオペレーションに関する業界横断的な課題の抽出と検討
  - セキュリティオペレーションに必要な各種セキュリティツール等に関する情報交換
  - 横断的なオペレータ教育/育成支援活動
- 他の関連団体との協力・連携活動
- セキュリティオペレーションの重要性の普及・社会的認知向上に貢献する活動
- セキュリティオペレータ間の交流を促進する活動

ガイドラインWG

関連法調査WG

今後

技術WG

継続中

認知向上・普及啓発WG

技術WG

JNSA

今後の改善課題について

- 事業形態の変化に合わせたセキュリティオペレーションのあり方
  - アウトソース需要の増大に応じたサービス品質の向上
  - 新しい技術への対応 (IPv6 等)
- 社会的認知向上(ユーザへの働きかけ)
  - ユーザ団体とのコラボレーション
  - ガイドラインなど各種情報の提供
- 他の関連団体との協力・連携活動
  - 共同での外部セミナーなど

JNSA

今年度の予定

	全体（WG4）	WG1	WG2	WG3
4	20:#1内部セミナー			
5				
6	3:JNSA総会（発表）	成果中間発表	成果中間発表	成果中間発表
7				
8	初旬：#2 内部セミナー 懇親会(1)		上旬:セミナー準備	
9		合宿		末:メンバー向け一覧公開
10	（外部向けセミナー：未定）			
11				上旬:合宿
12	中旬：NSF（発表）		パネルディスカッション等	
1	上旬：懇親会(2)			
2	（外部向けセミナー：未定）			
3				末:一般向け一覧公開

JNSA

ご清聴ありがとうございました。
今後とも、ISOG-Jをよろしくお願いします

E-Mail : isogj-info@jnsa.org

JNSA