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

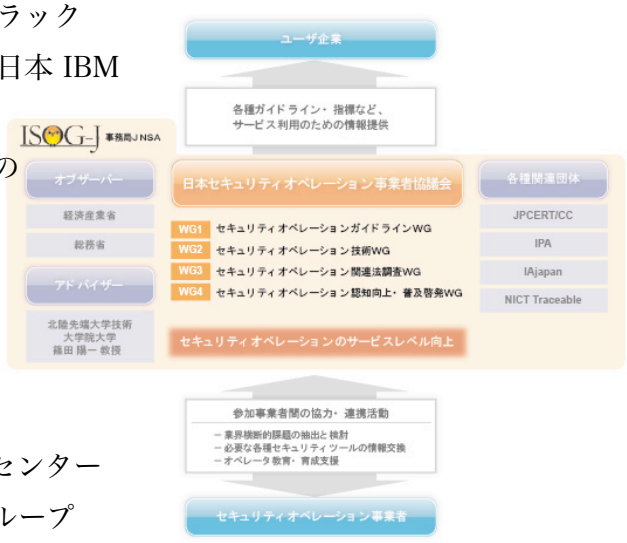
「マネージドセキュリティサービス選定ガイドライン」の活用方法

2011年01月25日

ISOG-J WG1 Chair / 株式会社ラック
許 先明

ISOG-Jとは

- 日本セキュリティオペレーション事業者協議会
  - 代表　：武智　洋　　（株）ラック
  - 副代表：徳田　敏文　（株）日本 IBM
- 目的
  - セキュリティオペレーションのサービスレベル向上
- 関連団体
  - JPCERT/CC
  - IPA
  - IAJapan
  - NICT 情報セキュリティ研究センター トレーサブルネットワークグループ



ISOG-JのWG

- WG1: セキュリティオペレーションガイドラインWG　（許）
  - このWGの成果である「 マネージドセキュリティサービス選定ガイドライン」の活用に関してお話しします
- WG2: セキュリティオペレーション技術WG　（川口）
  - セキュリティオペレーションに関する技術情報交換
- WG3: セキュリティオペレーション関連法調査WG　（出口）
  - 事業者に関連する法律に関する調査
- WG4: セキュリティオペレーション認知向上・普及啓発WG（多田）
  - ISOG-J事務局機能及び広報、セミナー等の取りまとめ
- プロジェクト: 情報共有・連携プロジェクト　（徳田）
  - セキュリティ事業者間での情報共有のための検討

ガイドライン作成の経緯

そもそもは

- ISOG-J発足の理由
  - MSSサービス事業者が増えてきた
  - MSSサービスの認知度が低い
  - MSSサービス毎に定義・品質がバラバラ
  - 利用者が、MSSの比較をするための指針がない
- ISOG-J発足時に、既にガイドラインが必要と云う認識があった

でも、いきなりガイドラインに手を付けるのは重い!!

ISOG-J

WG1活動の経緯

- ＷＧ１本来の活動
  - 「セキュリティサービスの上手な使い方」のガイドライン作成
  - セキュリティオペレーション事業の定義
    - 参加各社の共通理解をまとめる
  - ２００８年度はサービスマップ作成に注力
  - ２００９年度活動の最大目標（最低１本作成）
  - サービスマップを発展・展開させて作成

ISOG-J

ガイドラインとサービスマップ

- いきなりガイドラインを作ることは難しかった
  - というわけで、サービスマップを作って、どこから手を付けるか検討
- ガイドライン作成対象サービスの選定
  - マップ上のカテゴリから選定
    - 候補
      - SOC、脆弱性診断、フォレンジック、認証資格取得支援（コンサル）、その他
  - なるべく多くのWG1参加企業が提供しているカテゴリから着手
    - SOCか脆弱性診断
- 利用者に取って理解しにくいサービスである「セキュリティ機器監視・運用」（SOC/MSS）を選定
  - ***MSS = Managed Security Service***

サービスマップ

セキュリティサービスマップ

		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 経営者啓発	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 認証・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 脆弱性診断	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 脆弱性診断 原因調査 フォレンジック	対応確認検査	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 脆弱性診断	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 脆弱性診断 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 脆弱性診断	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 脆弱性診断 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 脆弱性診断	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 脆弱性診断 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 データ破棄

ISOG-J is a JNSA subsidiary.

ガイドラインの目的

目的

- 作成目的
  - サービス利用者のためのガイドライン
  - 利用すべきサービスを理解する
  - どのようなサービスか理解する
  - RFPを書くときに参考にできる
  - マネージドセキュリティサービス（MSS）の使い方のハウツー集
  - MSS選定／利用における注意点／チェックポイント
  - 各社サービス比較・評価のポイント

我々ベンダの想い

- ベンダの想い
  - ユーザ期待とベンダ提供内容のギャップ解消
- ユーザ幻想の解消
  - MSSを使えばあとはベンダがセキュリティを万全に守ってくれる
- ベンダ任せでなくインタラクティブが必要

➡ **ユーザが賢くなる・・・業者側は苦しくなる？**

作成にあたっての議論

- 議論
  - どの視点で書くか（利用者視点、ベンダ視点）
    - 利用者視点で書く
  - サービスマップとどのようにリンクさせるか
    - セキュリティオペレーションのライフサイクルを意識
  - 構成／目次、読者対象、記載範囲、規模（ページ数）
    - 業務で必要な人、セキュリティオペレーションをある程度わかっている人が対象
    - 本当の初心者には難しいかもしれない

ガイドライン作成方針

- マネージドセキュリティサービス（MSS）選定時のガイドライン
  - ５月から着手、検討開始
  - 月１回会合で宿題持ち寄り、議論
  - 合宿で集中執筆
  - 最後は編集者（エディタ）による全体整合・編集
  - ２０１０年６月完成目標

ISOG-J

ガイドライン内容検討

- ガイドライン内容
  - MSSの上手な使い方、MSSP業者の選定ポイントを書く
  - ベンダの提供内容とユーザの期待のギャップを埋める
  - ベンダに丸投げではない、ユーザがやることもある
  - あくまでもユーザ企業のセキュリティ運用を支援
  - コミュニケーション、相互協力が必要
  - 使い方、良い点、悪い点、注意点をまとめる

ISOG-J

メンバーの執筆範囲・分担

- 目次案作り
  - 各社目次案作成、ディスカッション
- ３パートに分けた内容構成
  - パート１　概要、定義
  - パート２　個別機能の解説
  - パート３　サンプルケース（ケーススタディ）
- パート２はサービスマップの横軸をベースに構成
  - セキュリティオペレーションライフサイクル
    - 導入企画→導入設計・構築→運用（定常、異常）

執筆手段

- パートごとにグループで分担して執筆
- Wordで執筆、Wiki使って共有、バージョン管理
- 書き始めてみて・・・
  - 執筆者により記述のレベル（深さ）が異なる
  - 用語・表記のばらつき
    - 「NW, FW」　←→　「ネットワーク、ファイアウォール」
    - 「ウィルス」　←→　「ウイルス」
    - 「サーバー、センター」　←→　「サーバ、センタ」
    - 「コンサル、ハード　←→　「コンサルティング、ハードウェア」
    - 漢字とひらがなの使い分け
      - 「例えば、たとえば」　「良い、よい」　「更に、さらに」
    - 「・」、「／」使い分け

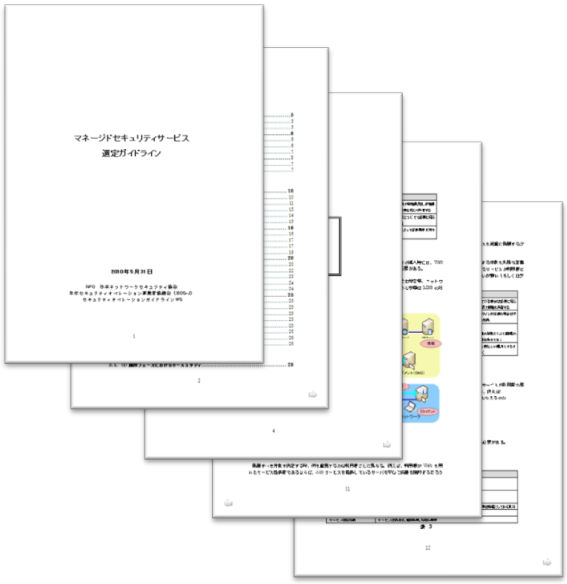
活動履歴

- 2009年5月　議論開始、方針検討
- 2009年6～7月　各社目次案作成・提示、目次検討
- 2009年8月　パート分けしてドラフト執筆開始
- 2009年9月　各パートのレビュー、用語統一
- 2009年10月　マージ版の作成
- 2009年11月　合宿（@石和温泉）
- 2009年12月　章立て編集、図表作成、ケーススタディ修正
- 2010年1～4月　ガリガリ更新
- 2010年5月　α版完成、大幅な加筆訂正
- 2010年6月　ISOG-J内回覧
- 2010年6～8月　関連団体事前回覧・ 最終修正
- 2010年9月　リリース

ガイドラインの内容

ガイドライン目次

JNSA



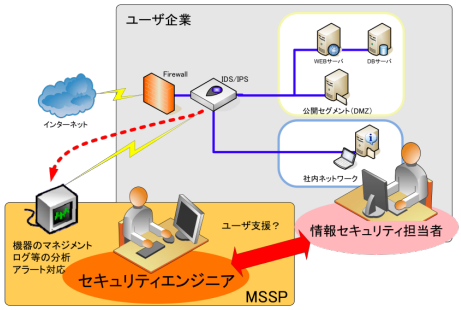
ISOG-J

「1章 はじめに」概要

JNSA

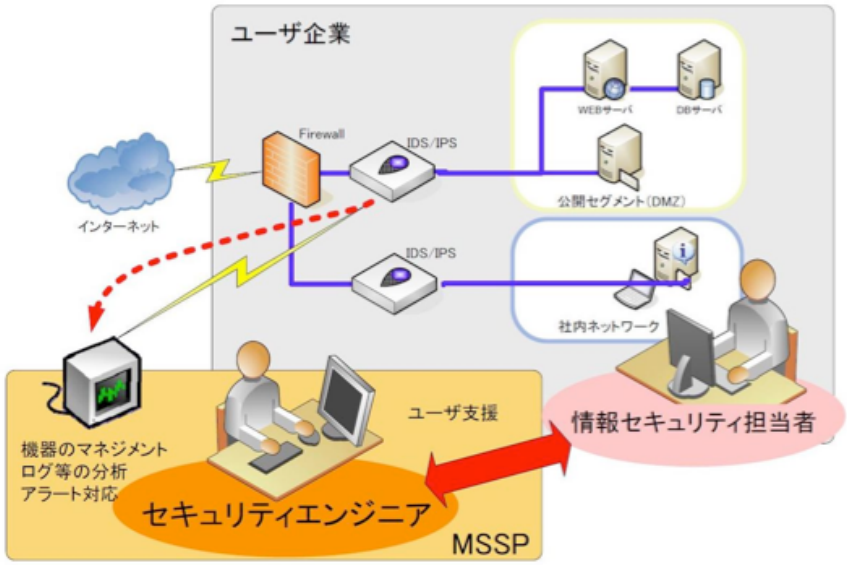
導入部分。MSS利用に際して検討のスタートとなる章として作成。MSSとは何かを定義し、MSSを受ける利点やMSSの限界、利用者の責務などの理解を通じ、責任分界点を明らかにすることで、相互に行うべきオペレーションの必要性を定義する。

- ガイドライン提供の背景
- MSS等の定義
- MSSの目的
- MSS概要



ISOG-J

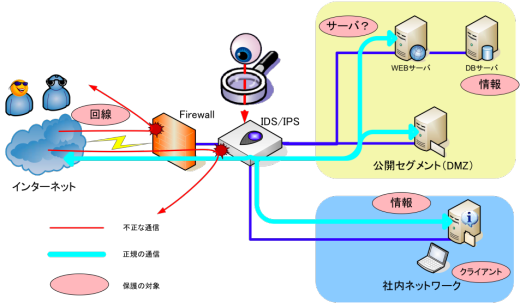
MSSとは



「2章 個別機能についての説明」概要

マネージドセキュリティサービス（MSS）を受けるにあたり、導入企画～運用までの一連の流れや個別機能について、利用者が把握し、最終的に十分な要件定義やRFPの作成ができるようにするため、内容的にも一歩踏み込んで作成。
利用者がよりよいサービスをよりよいMSSPから受けて欲しいとの思い。

- 個別機能についての説明
  - 導入企画
  - 導入設計・構築
  - 定常運用
  - 異常時運用

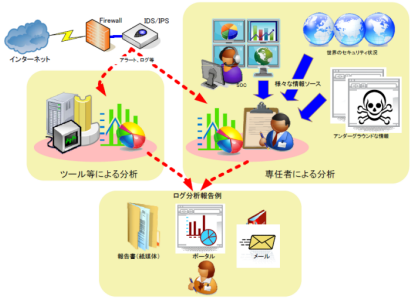


導入企画

- MSSP選定時における事前確認事項や選定方法、契約締結等、サービス導入に至るまでの事前作業について解説
  - 導入企画時に検討すべき内容
    - サービス利用者側での導入ポリシーの決定 等
  - 何を保護するのか
    - 保護ポリシーの決定、NWの把握、保護対象の決定 等
  - MSSPが提供するサービスの選定
    - 適合要件、サービス内容、RFP 等
  - サービス提供事業者の選定
    - 選定のポイント 等
  - 契約・SLA
    - 契約・SLA締結時に確認すべき事項 等

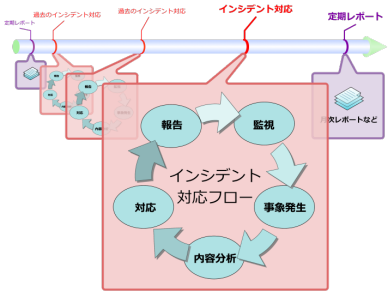
導入設計・構築

- セキュリティ対策装置の導入、保守等、対策装置にかかわる確認事項
  - セキュリティ対策装置の選定
    - 提供・設置形態、新規/既存機器利用時のポイント
  - 監視設計・導入
    - 監視設計時の注意事項、MSSPとの連携 等
  - サービス開始まで
    - 開通試験 等
  - 分析とレポート
    - 定型分析、非定型分析 等
  - 保守
    - ハードウェア保守、ソフトウェア保守 等



定常運用

- MSS利用における定常時の運用の解説
  - サービス
    - 定常運用機能、コミュニケーション 等
  - 監視
    - リモート監視、稼働監視、異常検知 等
  - 監査
    - ログ保存、提供 等
  - 報告
    - 報告方法、情報提供 等



異常時運用

- 何らかの対応作業が必要となる異常時の運用に関して解説
  - 異常の定義
    - 定常状態からの遷移、内部状態
  - 異常時の状態
    - 異常の検知
    - 原因の追及
    - 対応策の検討
    - 利用者側との調整
    - 対策の実施
    - 定常運用への復帰

チェック項目 -1-

確認項目	ポイント	備考
ネットワーク構成	回線種別、IP アドレス体系、NAT/NAPT 設定、DMZ 配置、物理構成等	IP アドレス表や論理構成図、物理構成図等を必要に応じて共有する
ネットワーク帯域	LAN、WAN	現利用帯域についても必要に応じて確認する
リモートメンテナンス回線	WAN、ダイアルアップ、VPN	サービスによって必要帯域が異なる

確認項目	ポイント	備考
対象マシン	対象システムの用途(Web サーバ、Mail サーバ、DNS サーバ、ファイルサーバ、クライアント等)と台数	仮想化している場合は必要に応じて物理構成の情報も共有する
対象マシン詳細	IPアドレス、OS、ミドルウェア、アプリケーション、バージョン等	リモートログインが必要な場合はアカウントを提供
対象通信、アプリケーション	各サーバで利用するプロトコル(HTTP、FTP、SMTP 等)	
監視目的	インターネットからの不正アクセス、ウイルス感染、イントラネットでのワーム拡散、外部からのコンテンツ改ざん等	監視、防御の対象にしたい脅威の向きと内容を決めておく
委託範囲	サービス委託範囲	どこまでを自社での運用とするか決めておく

確認項目	ポイント	備考
サービス導入に必要な機材	セキュリティ対策装置は購入が必要か、リースが可能か等	
緊急時対応	緊急時の対応内容、オンサイト対応の要否、追加費用の有無等	
セキュリティインシデント判断基準	セキュリティインシデント判断の基準が明確か、現在の運用体制に照らして妥当か等	
サービス品質	SLA、サービス内容、利用システム、保険、保証等	事前に対象を明確にしておく(表 2)
サービス価格	値段、バンドル提供されるサービスの範囲	
サービス提供体制	サービス提供地域、連絡体制、対応体制等	

ISOG-J

チェック項目 -2-

確認項目	ポイント	備考
サービスに対する要求事項	24 時間 365 日監視なのか、対応の早さは充分か等	機器提供を受ける場合、障害等に対する対応上の SLA の有無、その内容を確認すること
サービスの技術的要求	監視だけなのか、防御するのか、検知精度をどうするか等	
契約形態	契約年数、更新方法等	1年ごとに更新なのか、5年契約なのか、自動更新なのか協議によるのか等
契約範囲	監視時間帯、対応時間帯、問合せ方法等	機器提供を受ける場合には機器障害への対策方法を確認すること
制限事項の確認	サービスメンテナンス、回線断時の対応等	機能の停止またはアップデートの停止等
解約	解約時の制限、途中解約時の違約金等	ログおよびレポートの保存、設定変更、アカウント削除等

確認項目		ポイント	備考
サービス仕様		実施内容、報告形態、SLA、対応プラットフォーム等	
体制、実績		監視体制、監視実績、導入実績、サービス提供期間等	
技術背景		研究・調査機関の有無と実績	
資格の有無	組織の資格	組織として、高い品質でセキュリティ運用や情報の保護が可能である等を確認できることが望ましい。	ISO/IEC 27000 シリーズ、ISO 9000 シリーズ、ISO 14000 シリーズ、プライバシーマーク等
	個人の資格	個人として、情報セキュリティに精通し、技術スキルを有している等を確認できることが望ましい。	CISSP、CISA、CISM、情報セキュリティスペシャリスト、GIAC 等

ISOG-J

チェック項目 -3-

確認項目	ポイント	備考
セキュリティ対策装置の設定	基本設定（NW 設定、管理設定等）、監視設定（シグネチャ毎の脅威レベル、ブロック要否等）	
関連機器の設定	MSSP との通信経路に位置するアクセス制御機器のポート解放等	
導入場所	ラックマウント、電源、温度、騒音等	

確認項目	ポイント	備考
MSSP への接続	管理通信、監視通信の接続確認	
運用試験	連絡フローの確認、動作テスト、障害テスト	

これらの項目を確認

重要!!!!!

利用者の状況に合わせて重みを付ける

やって欲しいことをできるだけ明確化する

わからなければ遠慮せずに相談する

「3章 終わりに」概要

- 終わりに
  - まとめ
  - 謝辞
  - 作成メンバーリスト

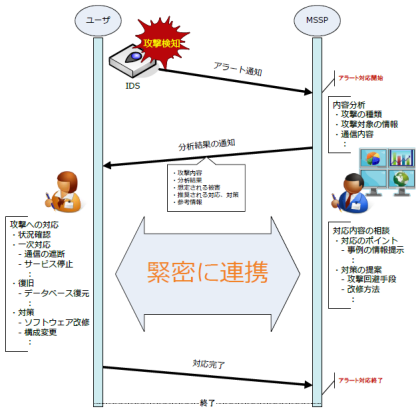
「Appendix.A ケーススタディ」概要

１～２章で説明した、MSSやMSSとの連携方法について、最近の事例より例示し、具体的にユーザがイメージしやすくすることによって、より相互のオペレーションについて理解を深めることを目的として作成。

- ケーススタディ
  - 運用フェーズにおけるケーススタディ
  - 導入フェーズにおけるケーススタディ

運用フェーズにおけるケーススタディ

- SQLインジェクション攻撃でサーバのコンテンツが改ざんされたケース
- 社内でウイルス（conficker）感染ホストを検知したケース
- Gumblarの感染を確認したケース
  - 攻撃概要
  - 検知情報
  - 分析例
  - 推奨される対応例



導入フェーズにおけるケーススタディ

- 公開ネットワーク（DMZ）の監視
  - 設置構成の検討
  - 監視対象NW情報の共有
  - 監視機器と監視センタとの接続
  - サービス開始

「Appendix.B 用語説明」概要

本ガイドラインでは様々な用語を利用しているため、言葉の定義を必要とした。そのため、本ガイドラインで利用した用語の説明を記載した

- 用語説明
  - 本ガイドラインで利用した用語に関して、用語、詠み方、内容の説明を記載。

「Appendix.C リファレンス」概要

本ガイドラインでは、サービス利用者が接する可能性の高い様々な規格を取り上げている。その各種規格に関する参照先を記載した。

- リファレンス
  - ITU-TやIEEE、JIS等で規定されている様々な規格に関するリファレンス、リンクなどを記載

まとめ

まとめ

- Internetでサービス提供している企業等が、サービスのセキュリティ面を向上するためにMSSを利用する場合に参照する資料として作成
- MSS利用者がMSSを選定するにあたって検討、比較する際の指針として利用して頂ければありがたい
- ISOG-J URL: http://www.jnsa.org/isog-j/
- 活動成果URL: http://www.jnsa.org/isog-j/activities/result.html

ご清聴
ありがとうございました