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

ISOG-J WG1における活動のご紹介

マネージドセキュリティサービス（MSS）
選定ガイドライン
2010年06月11日

ISOG-J WG1 Chair / 株式会社ブロードバンドセキュリティ
許 先明

経緯

ガイドライン作成に至るまでの経緯

- 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

サービスマップとの関係

- 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、ペネトレーションテスト、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WG1参加会社が提供しているカテゴリから着手
    - SOCかペネトレーションテスト
- 第１弾として、サービスマップにおける「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

JNSA

ISOG-J

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

ISOG-J is a JNSA subsidiary.

目的

2-1. 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

作成方針と手順

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

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

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）

3-4. 執筆手段

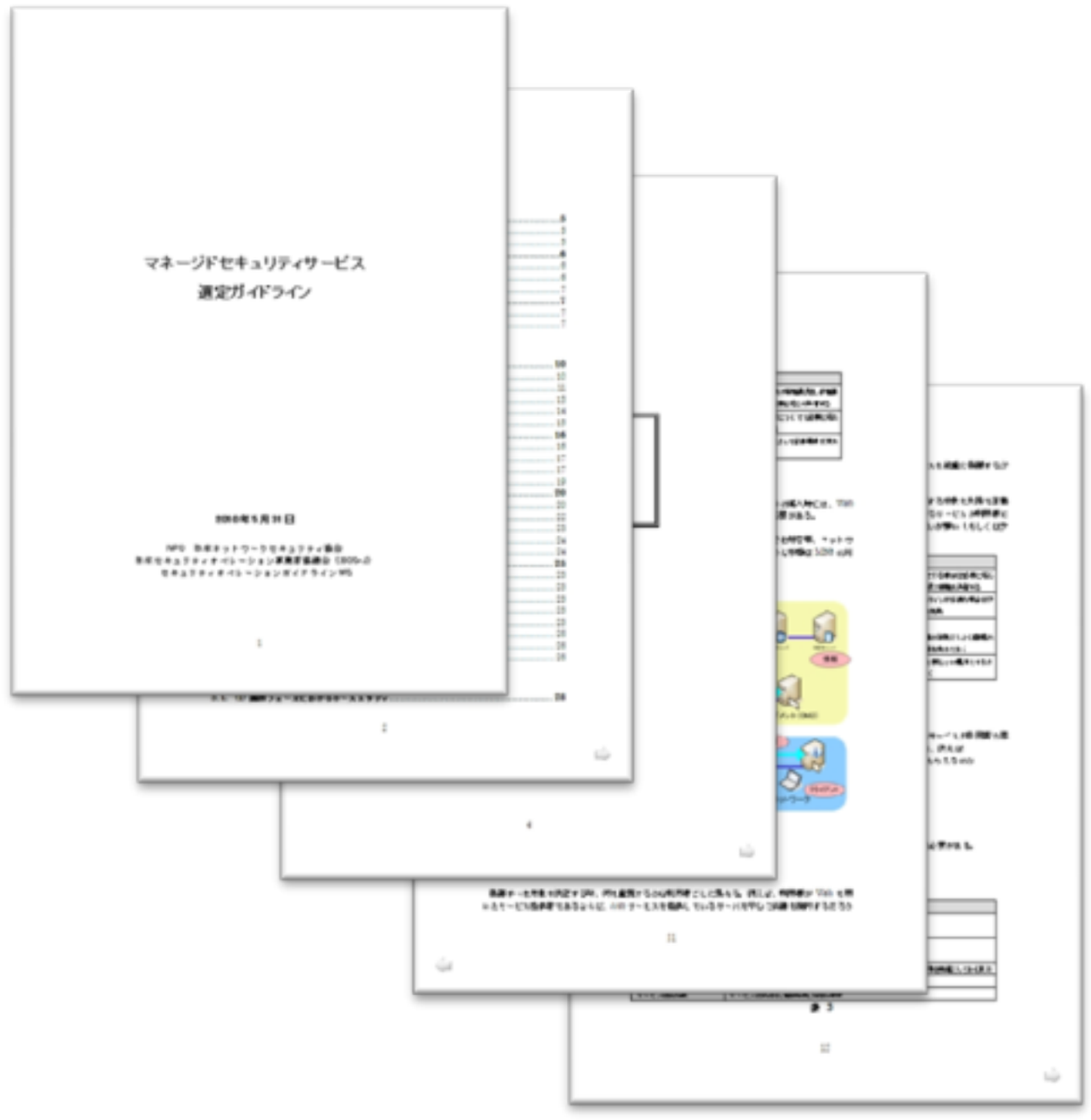
- パートごとにグループで分担して執筆
- Wordで執筆、Wiki使って共有、バージョン管理
- 書き始めてみて・・・
  - 執筆者により記述のレベル（深さ）が異なる
  - 用語・表記のばらつき
    - 「NW, FW」　←→　「ネットワーク、ファイアウォール」
    - 「ウィルス」　←→　「ウイルス」
    - 「サーバー、センター」　←→　「サーバ、センタ」
    - 「コンサル、ハード　←→　「コンサルティング、ハードウェア」
  - 漢字とひらがなの使い分け
    - 「例えば、たとえば」　「良い、よい」　「更に、さらに」
  - 「・」、「／」使い分け

活動履歴

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

ガイドラインの内容

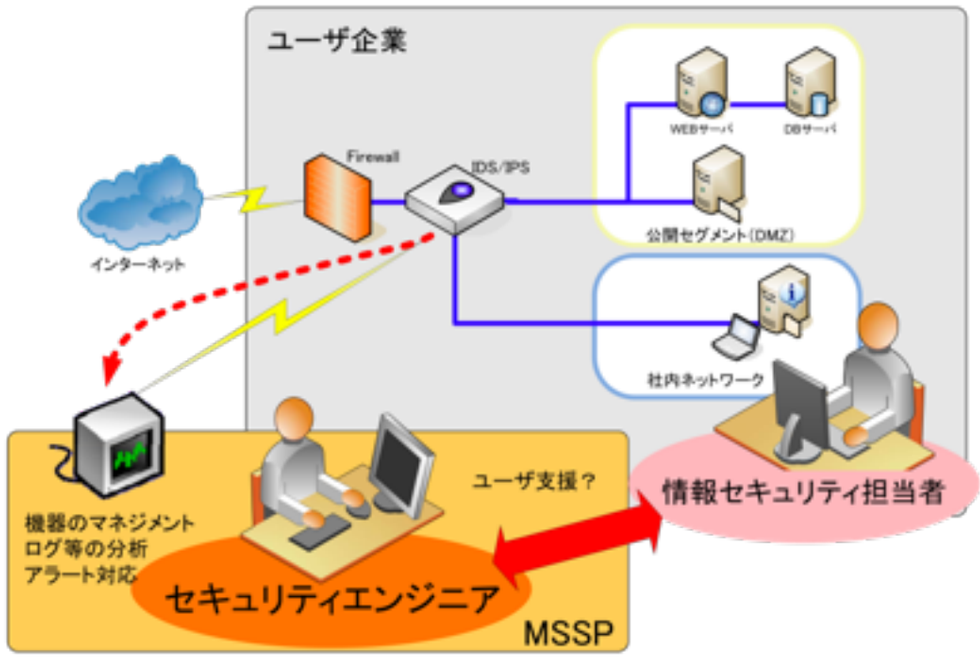
4-1. ガイドライン目次



「1章 はじめに」概要

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。

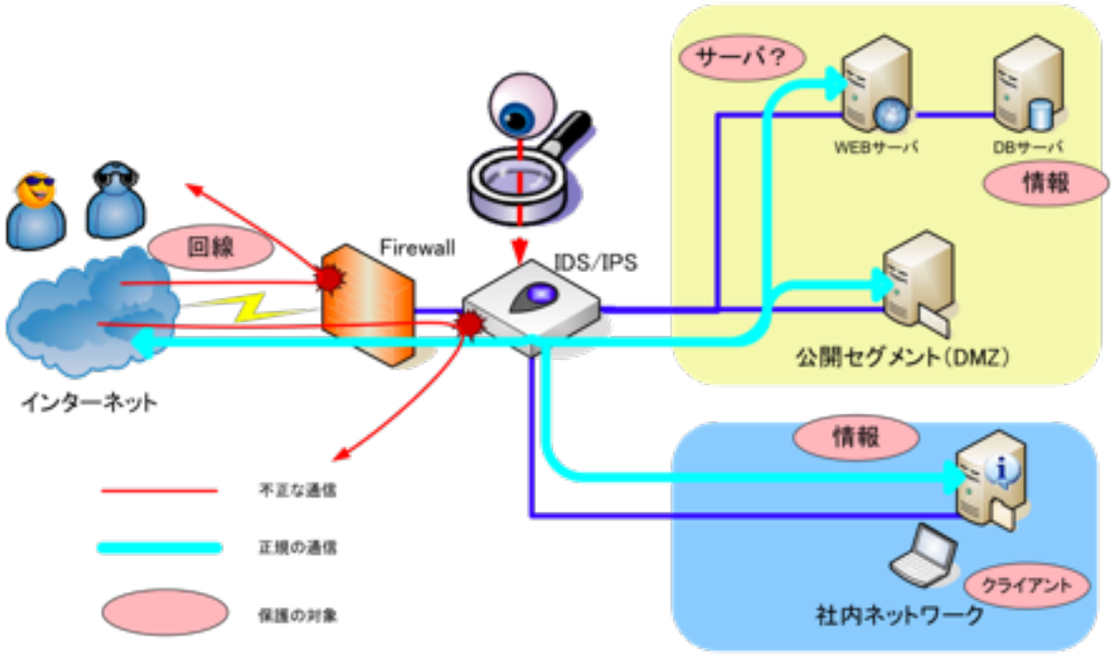
- ガイドライン提供の背景
- MSS等の定義
- MSSの目的
- MSS概要



「2章 個別機能についての説

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

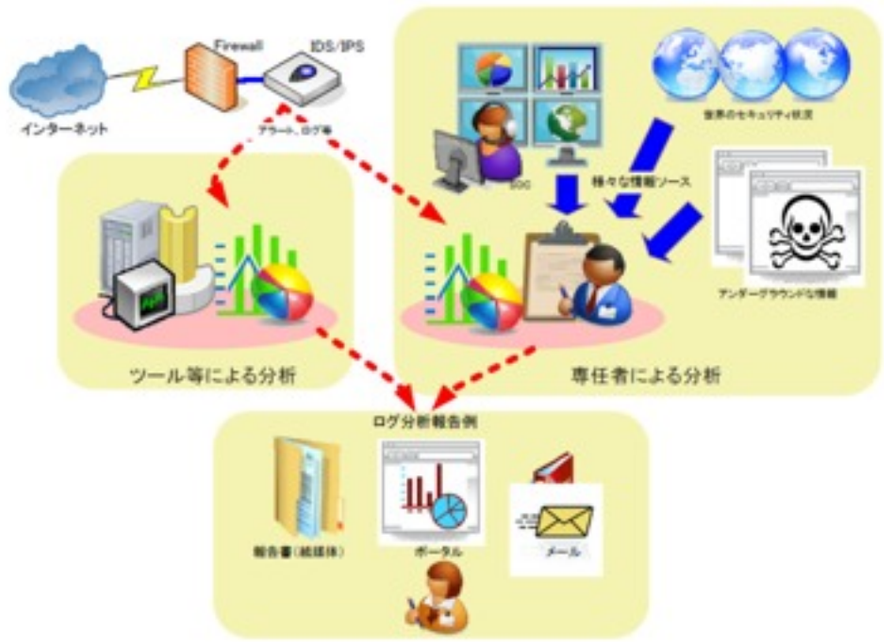


導入企画

- 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

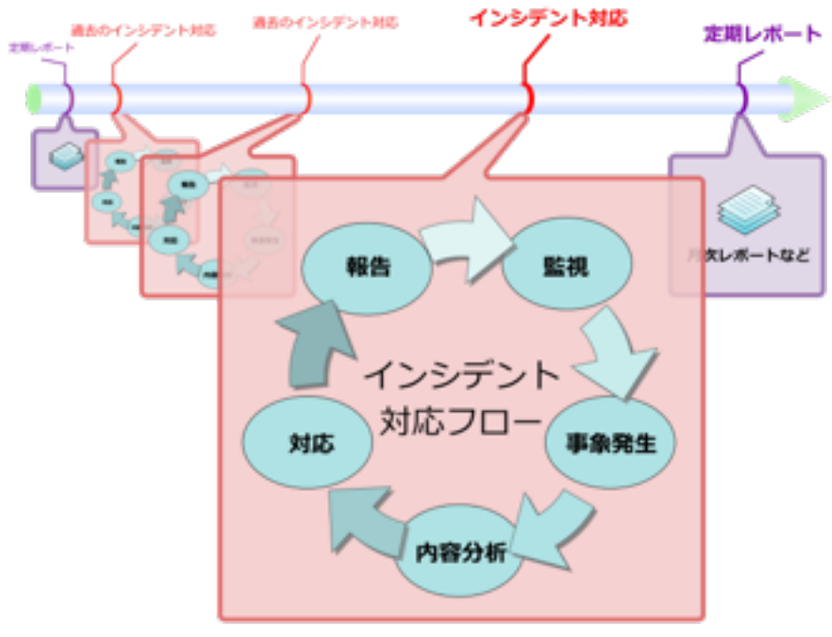
導入設計・構築

- 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

「3章 ケーススタディ」概要

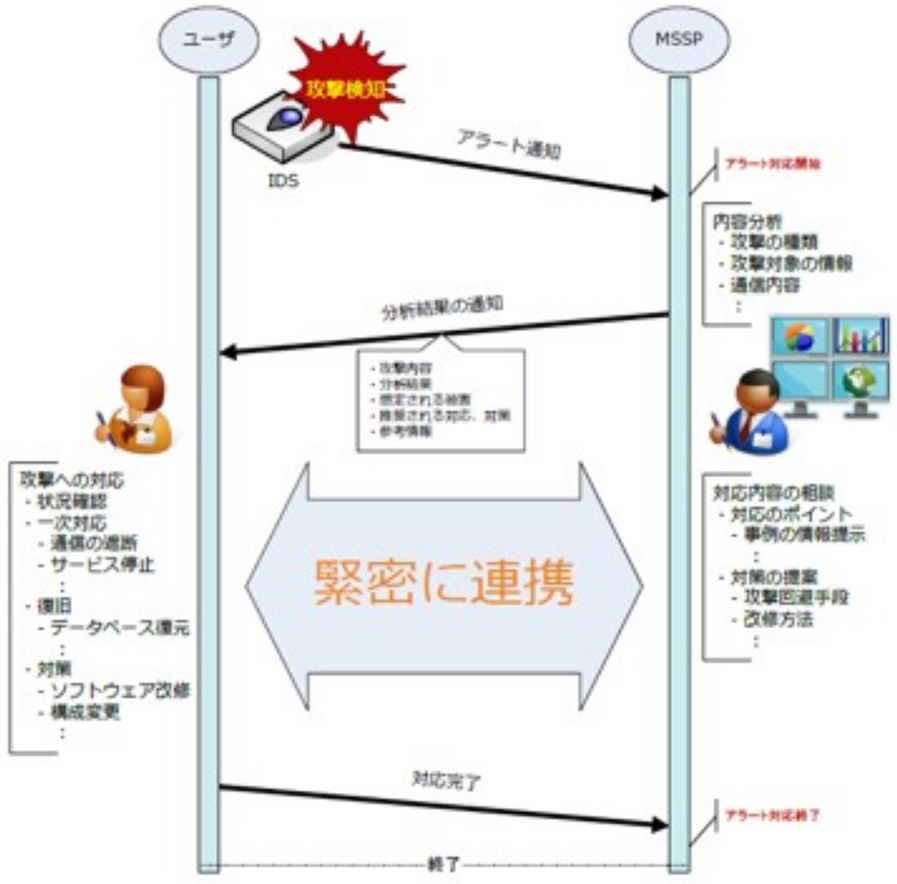
１～２章で説明した、MSSやMSSとの連携方法について、最近の事例より例示し、具体的にユーザがイメージしやすくすることによって、より相互のオペレーションについて理解を深めることを目的として作成。

- 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

「4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

まとめ

まとめ

- まとめ
  - ガイドライン作成の経緯、手順、内容等について説明した
- わかったこと、苦労したこと
  - 書き始めまでの敷居が高い
    - 一度書き始めればエンジンがかかる
  - Wordでのマージ／編集は煩雑
    - オートナンバリング、インデントが崩れる、Mac使いが多い。。
  - ユーザにわかる用語、表記も一議論
  - 日本語は難しい
  - SOC事業（オペレーション）は大変だということ
  - 会社毎に対応方針やオペレーションの内容が違うところもある
    - 平準化はなかなか難しい

ご清聴

ありがとうございました

ISOG-J

JNSA