日本セキュリティオペレーション事業者協議会

ISOG-J セミナー
「ISOG-Jの情報共有WG活動 ISOG-Jでの情報交換の試み」
～情報の共有と発信を目指して～

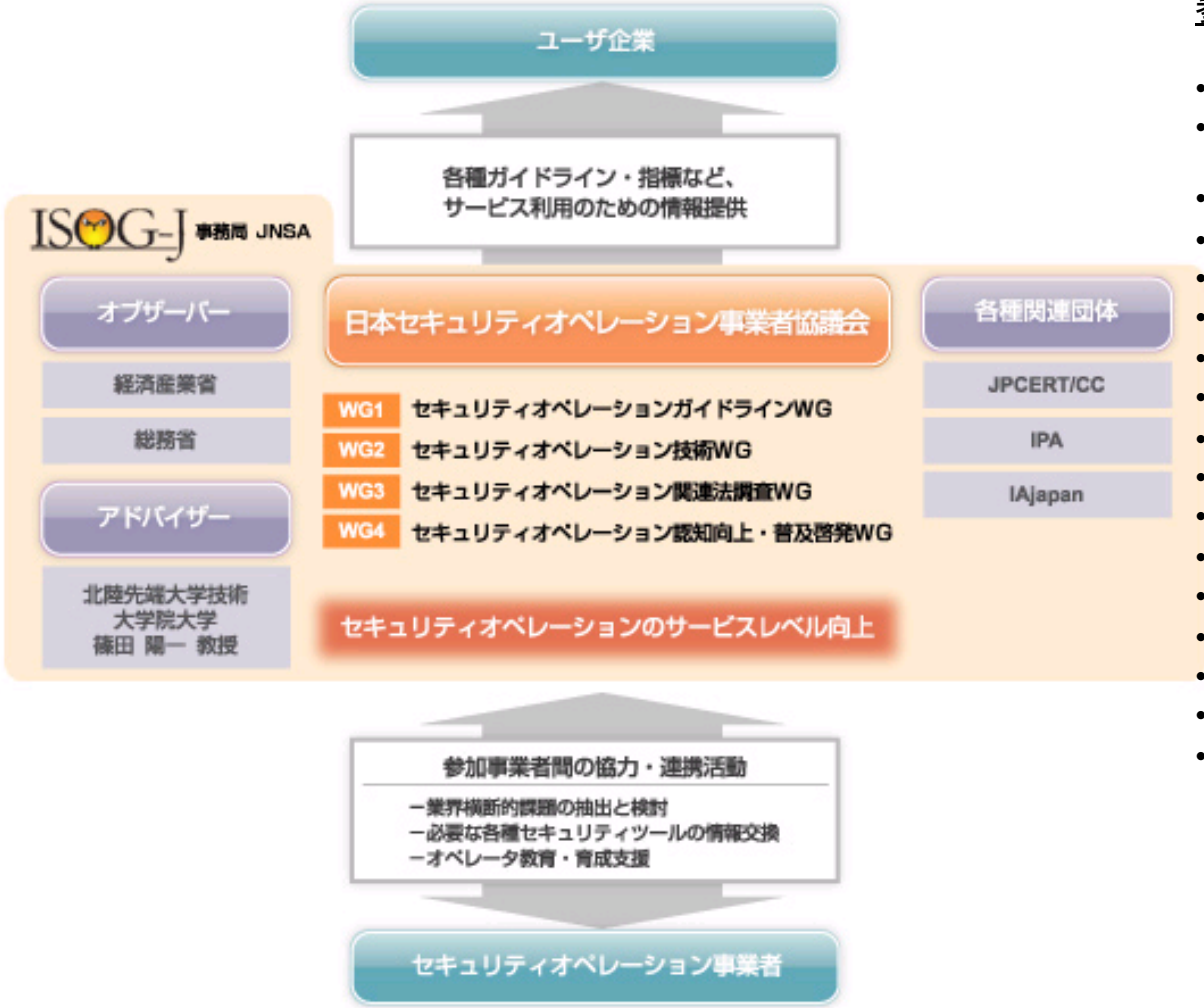
2010年10月13日
ISOG-J 情報共有 Project Leader
徳田　敏文 (Tokuda, Toshifumi)

はじめに
日本セキュリティ・オペレーション事業者協議会のご紹介

- 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：ISOG-J）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。

- http://www.jnsa.org/isog-j/index.html

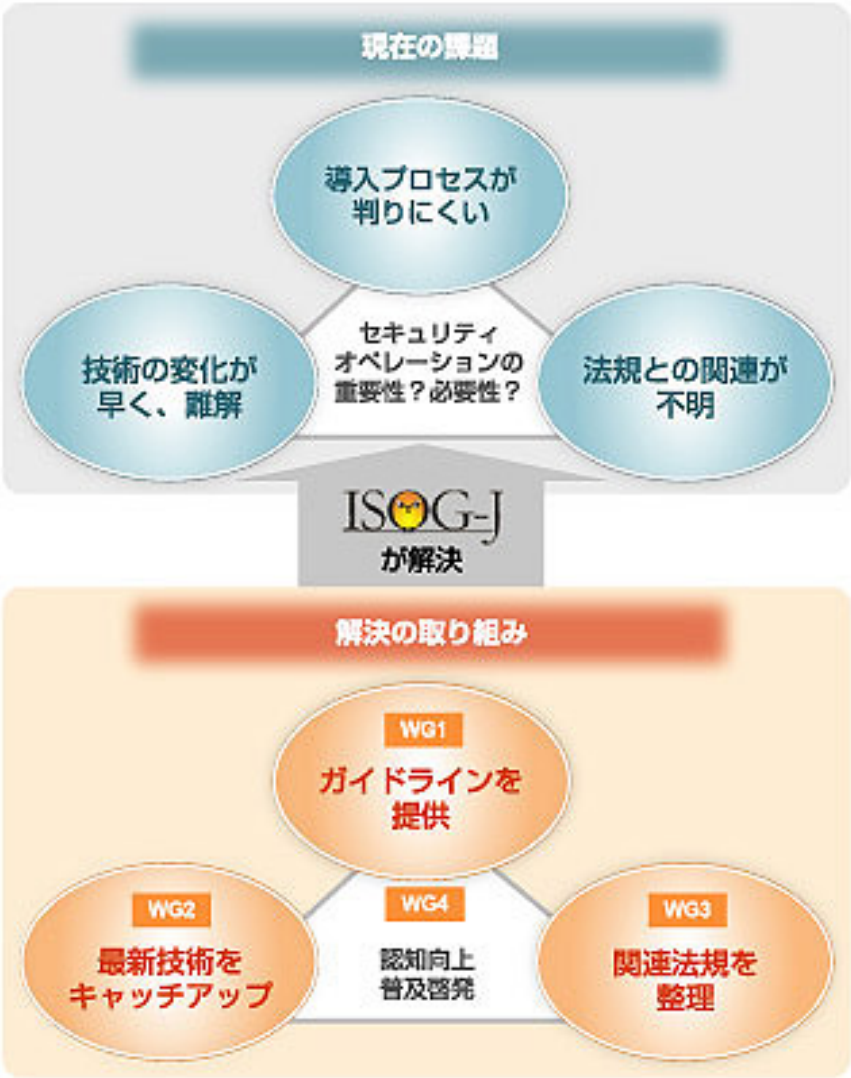
ISOG-J組織と参加企業



参加企業

- 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
- 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
- 株式会社エヌ・ティ・ティ・データ
- エヌ・ティ・ティ・データ・セキュリティ株式会社
- 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

ワーキンググループの活動内容



- 【WG1】セキュリティオペレーションガイドラインWG（2008年6月発足）
- セキュリティオペレーション事業者(MSSP)の提供するサービスを選別する際に利用できるガイドラインを策定します。

- 【WG2】セキュリティオペレーション技術WG（2008年6月発足）
- 最新の技術動向を調査し、最適なセキュリティオペレーション技術を探究し、技術者の交流を図ります。

- 【WG3】セキュリティオペレーション関連法調査WG（2008年7月発足）
- 数多くの関連法規が散在する中、利用組織および事業者が特に認識すべき項目を分かり易く整理します。

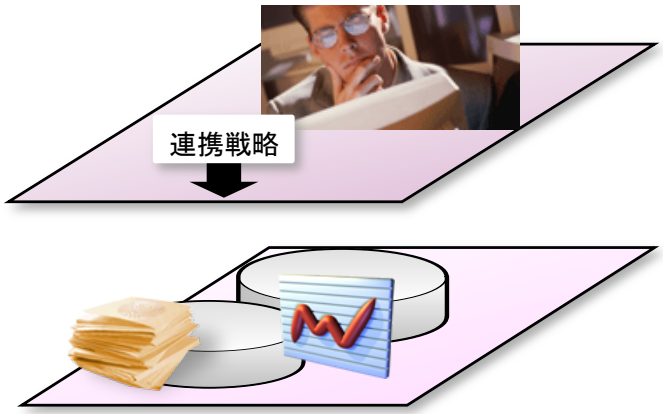
- 【WG4】セキュリティオペレーション認知向上・普及啓発WG（2008年6月発足）
- セキュリティオペレーションの必要性についての認知度向上を目的とし、普及啓発活動を行います。

- **【NEW】セキュリティオペレーション情報共有・連携プロジェクト（2010年4月発足）**
- セキュリティオペレーション事業者間の情報共有・連携のあり方について検討し、情報発信に向けて活動を行います。

セキュリティオペレーション情報共有・連携プロジェクト

（2010年4月発足）

- 情報共有WG活動 ISOG-Jでの情報交換の試み
- SOC事業が本格的に芽吹いた2000年頃から、マーケット拡大やSOC事業の認知、お客様の安全を目的に多くの共有・連携が試みられました。
- なぜ連携は難しいのか。
- ISOG-Jでは、過去の失敗した場合の原因（阻害要因）を見つけ、解決策を探りながら、情報の連携を試行しています。

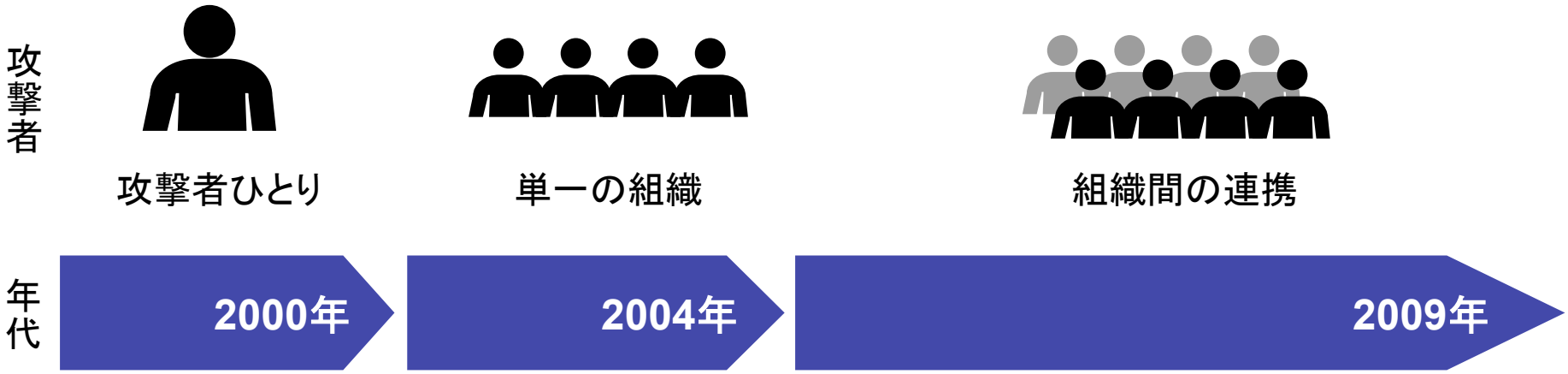


プロジェクトの参加メンバー

- 様々な視点や技術を持つメンバーでプロジェクトを構成し、情報の共有や連携が役に立つ、効果のある連携を目指しています。
  - 情報の提供
  - 分析の実施
  - 経営者視点で活動をレビュー
  - 研究者視点で活動を支援
  - SOCの運用者・アナリスト
  - アウトプットデザイン、プロセス管理の専門家等

攻撃者は、過去10年間にどのように変化したか？

攻撃の目的の変化により、単独犯から専門性を高める為、機能別組織へと変化しました。



攻撃組織間の連携

人材採用・育成
・優秀な学生を金銭面で支援
・ハッキング学校 http://hscool.net

ツール作成
・ツールの作成・脆弱性の調査

ツール販売
・掲示板を使用して販売
Neosploit：マルウェア販売業者

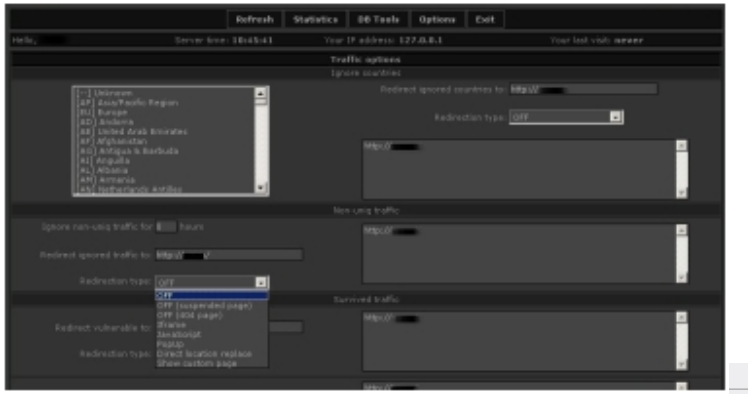
インフラ基盤
・Botnet(500万台)
AS-Troyak(カザフスタン), Real Host , Rustock, Grum, Mega-D

不正アクセス
・Rock Phish 団：オンライン犯罪者集団
・Russian Business Network：ロシア犯罪グループ

情報売買
・掲示板を使用して販売
カーダー(カードデータの売買)
Carder.cc(ドイツ),CallService.biz(ベラルーシ)
DumpsMarket、CarderPortal、Shadowcrew

情報の悪用
・詐欺し(カーディング)
不正に入手したクレジットカード情報を使って商品を購入する詐欺行為

換金・ロンダリング
・運び屋(ミュール)
盗品の受領や詐取した現金の振込み
・リシッピング
商品を他国へ転送して換金



・SaaS型の攻撃ツール

The pack contains following exploits:

- FLASH 9;
- FLASH 10;
- HCP;
- JAVA GSB;
- JAVA DESERIALIZE;
- JAVA SMB;
- IEPEERS;
- MDAC;
- PDF COLLAB;
- PDF PRINTF;
- PDF GETICON;
- PDF NEWPLAYER;
- PDF LIBTIFF.

ATTENTION! Builder will be sold just for one person. Price is 1350 USD including technical support and free updates. Escrow service is welcome. New javarox-sploit coming soon ;-) (+3-5%).

Mirrow: Exploits pack (builder)

ICQ: 562-one-583-58
JID: nextunit[dog]thesecure.biz
MSN: nextunit[dog]live.com

Last edited by NextUnit; 08-13-2010 at 09:27 AM.

・攻撃ツールの販売

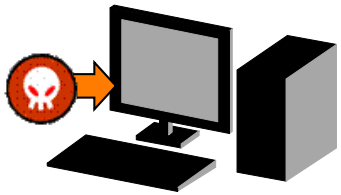
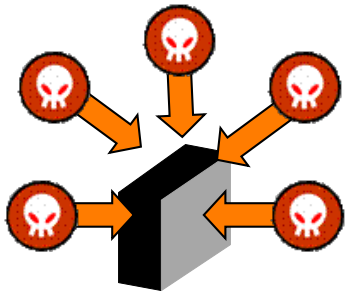
ランク 2009年	ランク 2008年	商品	割合(%) 2009年	割合(%) 2008年	価格帯
1	1	クレジットカード情報	19%	32%	$0.85-$30
2	2	銀行口座認証情報	19%	19%	$15-$850
3	3	電子メールアカウント	7%	5%	$1-$20
4	4	電子メールアドレス	7%	5%	$1.70/MB-$15/MB
5	9	シェルスクリプト	6%	3%	$2-$5
6	6	完全な個人識別情報	5%	4%	$0.70-$20
7	13	クレジットカードのダンプ	5%	2%	$4-$150
8	7	メーラー	4%	3%	$4-$10
9	8	キャッシュアウトサービス	4%	3%	$0-$600 プラス 50%-60%
10	12	Web サイトの管理認証情報	4%	3%	$2-$30

表 21. アンダーグラウンドエコノミーサーバーで販売が宣伝された商品とサービス
資料作成：シマンテックコーポレーション

・情報の販売

攻撃手法は、過去10年間にどのように変化したか？

組織に優秀な人材を採用し、技術開発の強化が図られています。結果、攻撃の高度化・巧妙化が進んでいます。

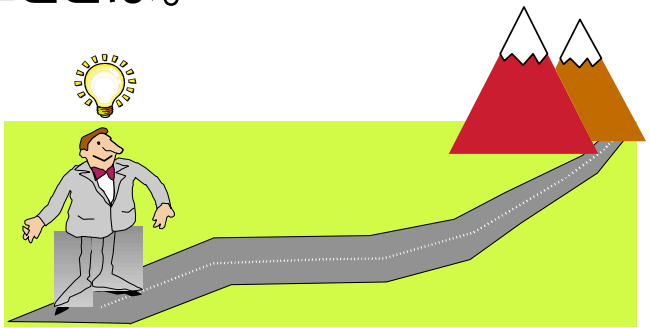
2000年	2004年	2006年	2009年
•Web改ざん •DDoS攻撃 •ワームによる攻撃 •Antinnyによる情報漏えい	•ボットネット(オープンソース) •フィッシング詐欺 •SQLインジェクション攻撃 •辞書攻撃(ブルトフォース)	•ボットネット(高度化・基盤利用) •リモートファイルインクルード •スパムメール風説の流布 •偽りのセキュリティソフトの販売 •エストニアへのDDoS攻撃	•Operation Aurora •Conficker ワーム •Gumblarウイルス •Stuxnetウイルス
手法			
			
不正侵入・改ざん	攻撃の自動化と管理 (Botnet)	検出回避・障害対策 (Botnet技術基盤利用)	advanced persistent threat (APT)
年代			

プロジェクトの2つの大きな目的

- ISOG-Jという中立的な立場を利用した情報発信
  - ISOG-Jメンバー企業の連携による情報の共有
  - 情報共有・分析手法の共有による情報の分析
  - ISOG-Jとして情報の発信

※情報とは、情報セキュリティ関連情報を指す。

- 企業間連携の必要要素の考察（副次的に導き出される結果）
  - 連携を阻害する要因は何か。
  - できる・できない、出せる・出せない、の基準や判断の根拠はどこに？
  - 阻害要因を克服するために協議会がなせることとは。
  - 協議会の存在意義



連携を阻害する要因は何か

- 最初に連携阻害要因を洗い出し振り返ってみた

- 例えば、
  - 無料の情報提供と有料の差は何？
  - 契約ユーザと一般の差は？
  - 情報を先に出したほうが不利？
  - 情報は欲しいけど出すことはできない？
  - 運用の組織が別になっているので情報の取得が自組織内でも難しい？

阻害要因の事例 1

- ある連携の事例では、情報を収集した後にそれを活用することができなかった。
  - 意味が見出せず、尻すぼみになっていった。
  - 継続する目的意識が必要。
  - 金銭をモチベーションにすると、金の切れ目が縁の切れ目になってしまう。
  - 気付きや事象を共有し、何らかの結論（起こっていること）がわかれば報告できたはず。

- 他社のログから情報を得ても、そこから有意なアクションを起こすことはできなかった。
  - 一過性の情報（脅威動向の速報）にどれだけ価値があるのか？その価値は一過性のものでしかないのでは？

阻害要因の事例２

- 人と人との信頼関係に基づいた連携は、人が変わる（異動する）と消滅してしまう。
  - 上司が連携活動に積極的でないとむずかしい。
  - 自社の顧客に役立つフィードバックを得られないと連携を積極的に進めることが難しい
  - 担当者が変わったときに適切に引き継がれない（自社内に説明できなくなってしまう）
  - 共有すること自体が目的になってしまうと、現場のモチベーションが落ちてしまう。

その他の阻害要因

- これまで連携を試みてきた内容とは何か整理する必要がある。
  - 情報共有、連携、オペレーションフローなど
- 各社ともに視点、技術が異なるため、情報共有からスタートするのが好ましい。
  - 連携は当初は難しい。
- そもそも社内でも情報共有が難しいのに社外と共有していけるのか疑問である。
- セキュリティ業界の人は、情報を出したがらない傾向にあると思う。
  - 出してはいけない情報：顧客情報（IPアドレス、ホスト名）などがある。
  - 慎重な取り扱いや規定が必要。
- 共有する、と一口に言っても何を共有するのかわからなくなってしまう。
  - アウトプットを先に定義すると、頓挫しやすい
- 経営者や部門責任者の理解が得られていれば、情報を出しやすい。
  - 共有･連携を進めて利益につながるか？この活動の各社へのメリットが必要。

ISOG-Jにおける情報の共有・連携の利点

- 個社で発生したインシデントについて、他での発生状況をISOG-Jという名前で出すことができる。
  - 情報提供会社は自社の調べた情報をISOG-Jの看板をつけることで、客観情報として提供することができる。また、他の会社は情報提供会社が調査した情報を自社を含むISOG-Jの調査した情報として顧客に提供することができる。
- 情報を発表するとき個社で発表するのとISOG-Jから発表するのを使い分けることができる。
- 定期的に情報公開することで、他の協議会活動と同様に各種メディアや各社の文書等に引用が可能になる。
- 何か起こったときに、他社ではどうやって対処したのかを共有できる。
  - 調査結果などコンテンツを共有する。
  - チャットなどで緊急時に事態・状況を共有する。
- 「教育目的」で特定ネットワークの検知情報を相互に分析しあうというのは最初のステップとして良い。

- 日本のアドレス空間は膨大なので、その端っこに対する検知情報を提供するだけでも他のアドレスを保持している業者の役に立つ場合がある。具体的なアドレス情報の含まれないイベント情報（●のイベントを●時●分に検知した！など）を共有するだけでも、意義があるのではないか。

- ちょっと気づいた傾向を共有する。
  - データそのものではなく人の意見を共有する（ここから始める）
  - 生ログは、必要に応じてマスクして一部共有するなど
  - どうやったら出しやすいか

参加メンバーからの提案例 1

- 経営者向け脅威分析ドキュメントを発行してはどうか。
  - セキュリティ専門各社が出す注意喚起は技術的な内容で、経営者が見る内容とは言えない部分がある。
  - 経営者がこのドキュメントを読むことで情報システムを脅かす脅威がどんなもので事業継続にどんなリスクがあるのかをタイムリーに把握できるようにしてはどうか。
    セキュリティの重要性を経営陣に理解させるには、どのような問題に立ち向かっているのかを継続的にインプットすることが肝要と思う。

参加メンバーからの提案例 2

- 情報の共有・連携を行っていく上で、一番基本的なデータとなるのは、IDS/IPSやその他NW機器やサーバのログではないか。

- ログを共有する際に、以下のようなルールというか注意点が挙げられる
  - 共有・連携する目的
  - ポリシー（ログの保管期間など）を決める
  - ログの内容からユーザや組織などが特定できないように加工等する
  - ログの共有方法の確立
  - ログフォーマットの共通化

  初めは統計情報のみで始めてみる。しかし、情報を丸めてしまうため各社のログとの突き合わせをどう解決するかが課題。

参加メンバーからの提案例 3

- 日本で検知される定量的なインシデント状況が知りたい

- 各SOCで検知したインシデント情報(※)を ISOG-J に集め、加入者で参照可能とする
  - 日本で検知できる情報が網羅できれば、先日の中国からのサイバー攻撃の影響がどの程度あったのか？とか、新たなインシデント発生時における定常状態との比較が可能となる。
  - 顧客や社内経営層に対して、「どの程度発生した/するのか？」がSOCに関連するビジネスに取って必要。
  - 全体の分析、統計データを外部に公開することで、ISOG-Jの存在意義アピールにも繋がるのでは？

※インシデント情報・・・当面IDSの検知ログ、FW のdrop/accept ログを想定

参加メンバーからの提案例 4

- メタ情報(「気付き」)を共有する

- 一般公開しづらい脅威動向に関する情報共有が可能になる。
  - 先日の「中国からのサイバー攻撃」のように一般公開はされていないが、各社が動向を注視しているような場合。個社での情報収集には限界があるが、お客様はセキュリティベンダに多くの情報を期待する
  - 各社で観測している状況を取りまとめて、自社の顧客へ提供することができる。(例:「現在のところ、中国からの大規模な攻撃は確認されておりません」)
  - まだ自社顧客には到達していない脅威に対して、事前に備えておくことができる(自社だけ何も知らないという状況は回避できる)

ISOG-J はこれらの提案を実現するために活動していきます。

- セキュリティオペレーション情報共有・連携プロジェクト
  - メタ情報(「気付き」)を共有する。
  - ISOG-J より引用として、WEB記事などメディアに引用されるような情報の発信をする。
  - 提案書などに張る図式やデータ、表などをISOG-Jより引用として使える素材の作成と共有をする。
  - 広域インシデント発生時などに他社の対応状況について確認しあえる環境を整備する。
  - 情報共有のためのバックエンド(インフラ)の技術を考える
    - 参加者で意見を出し合い運用してあるべき姿のシステムを構築してみる