

Network Security Forum 2012

標的型攻撃とセキュリティオペレーション

ISOG-J WG5活動中間報告

2012年1月25日

ISOG-J WG5

齋藤衛 (ISOG-J運営委員、株式会社インターネットイニシアティブ)

ISOG-J WG5のご紹介


- 【WG5】標的型攻撃対策検討WG
 - 2011年7月発足
 - 標的型攻撃の実態調査および、その防衛策について検討、実証実験を行います

 - 成果物(予定)
 - 調査報告書、実証実験報告書
 - 検討テーマ
 - セキュリティオペレーション事業者の協調による標的型攻撃の実態調査および、その防御策について検討を行う
 - 標的型攻撃は古くからある攻撃手法ですが、本年大きく注目を浴びています。このWGにおいては、この対策について実効力のある対策を検討することを目的に活動します。特に、このWGにおける検討、調査、実証実験の結果を元に、実効力のある標的型攻撃への耐性強化の機能の提供を、それぞれの会員のセキュリティオペレーション事業において実現し、顧客に提供できるようにすることがゴールです。

【NEW】【WG5】標的型攻撃対策検討WG (2011年7月発足)

標的型攻撃の実態調査および、その防御策について検討、実証実験を行います。

WGリーダー



齋藤 衛 株式会社インターネットイニシアティブ	
成果物	調査報告書、実証実験報告書
検討テーマ	セキュリティオペレーション事業者の協調による標的型攻撃の実態調査および、その防御策について検討を行う。
WGリーダーの思い	標的型攻撃は古くからある攻撃手法ですが、本年大きく注目を浴びています。このWGにおいては、この対策について実効力のある対策を検討することを目的に活動します。特に、このWGにおける検討、調査、実証実験の結果を元に、実効力のある標的型攻撃への耐性強化の機能の提供を、それぞれの会員のセキュリティオペレーション事業において実現し、顧客に提供できるようにすることがゴールです。

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

WG5活動概要

- 参加メンバー各社
 - 株式会社インターネットイニシアティブ
 - 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
 - NTTデータ先端技術株式会社
 - 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
 - 株式会社日立システムズ
 - 富士通株式会社
 - 株式会社ブロードバンドセキュリティ
 - 三菱電機情報ネットワーク株式会社
 - 株式会社ラック
 - JPCERT/CC
 - IPA(情報処理推進機構)

登録者計 44名

WG5 活動計画と実施状況

• 活動期間・スケジュール

- 平成23年度中
 - キックオフ
 - 定義ブレスト、対象の決定、事前調査、協調スキームの定義 (1～2か月)
 - 協調スキームの実験(3か月～半年)
 - 調査報告、実証実験報告まとめ (1～2か月)
- 平成24年度以後
 - 協調対処、情報共有スキームの運用、もしくは寄与。平成23年度の成果を受けて決定。

• 現在までのWG開催日程

- 第1回 8/2 15:00-17:00 @IJ
- 第2回 8/10 16:00-18:00 @IJ
- 第3回 8/18 16:00-18:00 @IJ
- 第4回 8/26 16:00-18:00 @LAC
- 第5回 9/5 16:00-18:00 @IJ
- 第6回 9/29 16:00-18:00 @IJ
- 第7回 10/27 16:00-18:00 @IJ
- 第8回 11/29 16:00-18:00 @IJ
- 第9回 1/13 16:00-18:00 @IJ

活動経緯と状況の変化

- 活動に向けたブレインストーミングは6月に開始。
- 正式な活動開始は2011年7月から。
- SOC事業者各社のサービスとして、標的型攻撃の対策サービスがなかったため、各社サービス化も視野に対策の検討を開始。
- 9月以降、標的型攻撃に関する複数の事件が報道があり、状況が変わった。

	2011年 6月	7月	8月	9月	10月	11月	12月	2012年 1月
世間の動き				事件報道	各社から サービスリリース 			
WGの活動	WG 検討開始	WG 正式発足	プレスト	活動計画	情報共有トライアル			活動目標 再検討

WG5活動概要

標的型攻撃とその対策に関するブレスト

ブレインストーミング

- 標的型攻撃対策に関するブレインストーミングとして次の4点の議論を行った。
 - 標的型攻撃に対する現在の事業者の立ち位置とあるべき姿
 - 標的型攻撃を行うもののモチベーション
 - 標的型攻撃事例に関する技術的検討
 - 標的型攻撃対策における情報共有のありかたとISOG-Jの役割
 - その他

ブレインストーミング議論から

- 標的型攻撃対策に関するブレインストーミングにより次の意見と問題点がまとめられた(2011年8月時点)
 - この時点でのセキュリティオペレーション事業者のサービスでは標的型攻撃に対応できない場合があるとの認識。
 - そもそも標的型攻撃の定義があいまいで、標的型攻撃の事例も少ない。
 - 標的型攻撃を検出するために必要な情報、手法が不明確である。
 - 標的型攻撃の疑いがある場合の対応(調査、検証、対策)の場がない。
 - 標的型攻撃対策を仕事として既存ビジネスに取り込むことが必要。
- この場で検討した内容を各社に持ち帰り、平成24年度には「標的型攻撃対策の機能」が会員各社のサービス等に実装されることをWG活動のゴールとする。

ブレインストーミング/標的型攻撃とは何か

• 標的型攻撃のモチベーション

– スパイ活動と標的型攻撃

- 対象に**潜入**したスパイ事例
- 中国人収集家の事例

20年以上に
わたる
活動

- 1978年：香港経由で米国に入国。
- 1983年初頭：センシティブなプロジェクトに関する情報を中国へ。
- 1985年：帰化し米国市民となった。
- 1996年：保全適格証を付与。
- 2001年5月：当該エージェントの弟(元解放軍宣伝工作将校)は、妻と息子と共に米国に移住
- 当該エージェントは、米国のセンシティブ情報を可搬式磁気媒体に記録し、それを弟に渡した。
- 2007年：有罪判決

上記事例は米国の国家対情報局 (Office of the National Counterintelligence Executive: ONCIX) が作成した「Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY07」を財団法人防衛調達基盤整備協会が翻訳した「外国の経済情報収集および産業スパイに関する議会への年次報告 (2007会計年度)」より引用したもの

- ネットワーク経由の攻撃においても、攻撃に先だって**標的となる組織の事前情報**(メールアドレス、組織構成、ネットワーク構成/インターネット接続の情報等)を入手して攻撃を組み立てている。また、組織内ネットワークにおいて**潜伏して長期的に活動**する蓋然性が高い。

ブレインストーミング/標的型攻撃とは何か

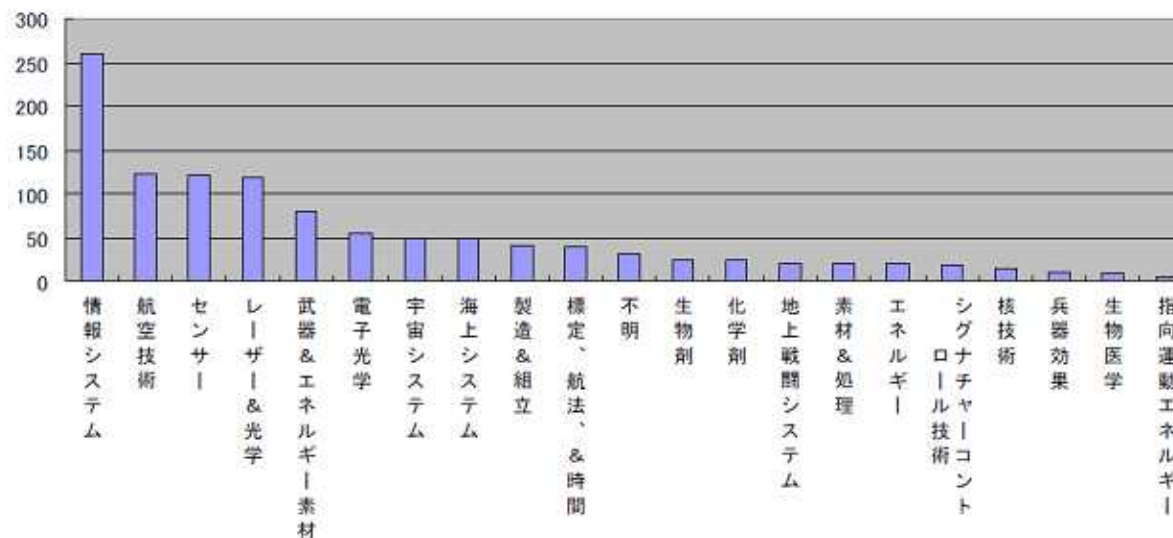
- 標的型攻撃のモチベーション

- 行為者の姿

- 産業スパイにおける攻撃者の姿と標的型攻撃

- 攻撃者の目的意思と技術力は高い。もともと国家間の情報エスピオナージなどを発端にしており、そこではふんだんに技術開発資金と攻撃ソフト開発者が育成されていた。
 - その裾野が広がり、攻撃側で技術、開発したソフト、ノウハウが共有されているという歴史と経緯をたどっており、防御側も特定企業の努力で守り抜くことは困難、協調による対策が必要となる。

07会計年度に標的となった米国の防衛技術、国防保全局



10 上記の図は米国の国家対情報局 (Office of the National Counterintelligence Executive: ONCIX) が作成した「Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY07」を財団法人防衛調達基盤整備協会が翻訳した「外国の経済情報収集および産業スパイに関する議会への年次報告 (2007会計年度)」より引用したもの © 2012 ISOG-J

ブレインストーミング/標的型攻撃事例

- 個別事例研究 (事例詳細はこの場では非公開)
 - メンバ間でいくつかの事例についてメールヘッダを含む詳細を共有。
 - メールヘッダ、マルウェア等から**検出と情報共有のやり方に関する議論**のたたき台とした。
- 標的型攻撃メールの検出状況を共有 (詳細この場では非公開)
 - 特定組織に少数を短時間に送付する事例から、複数組織である程度時間をおいて検出している事例まで多様。
 - 事例の一部(時間間隔のみ紹介)
 - 検知期間約43時間、全6組織、最初の10分で4組織、残りは約40時間後
 - 検知期間約76時間、全6組織、初検知から約10時間後、約24時間後、約27時間後2組織、約34時間後
 - 検知期間約9時間、全4組織、1時間以内に3組織、最後は約2時間後
 - 検知期間約10分、全3組織、最初の10分以内に全組織に送付
 - 他の攻撃発生情報を**情報共有によって知ること**で防げる場合がある。

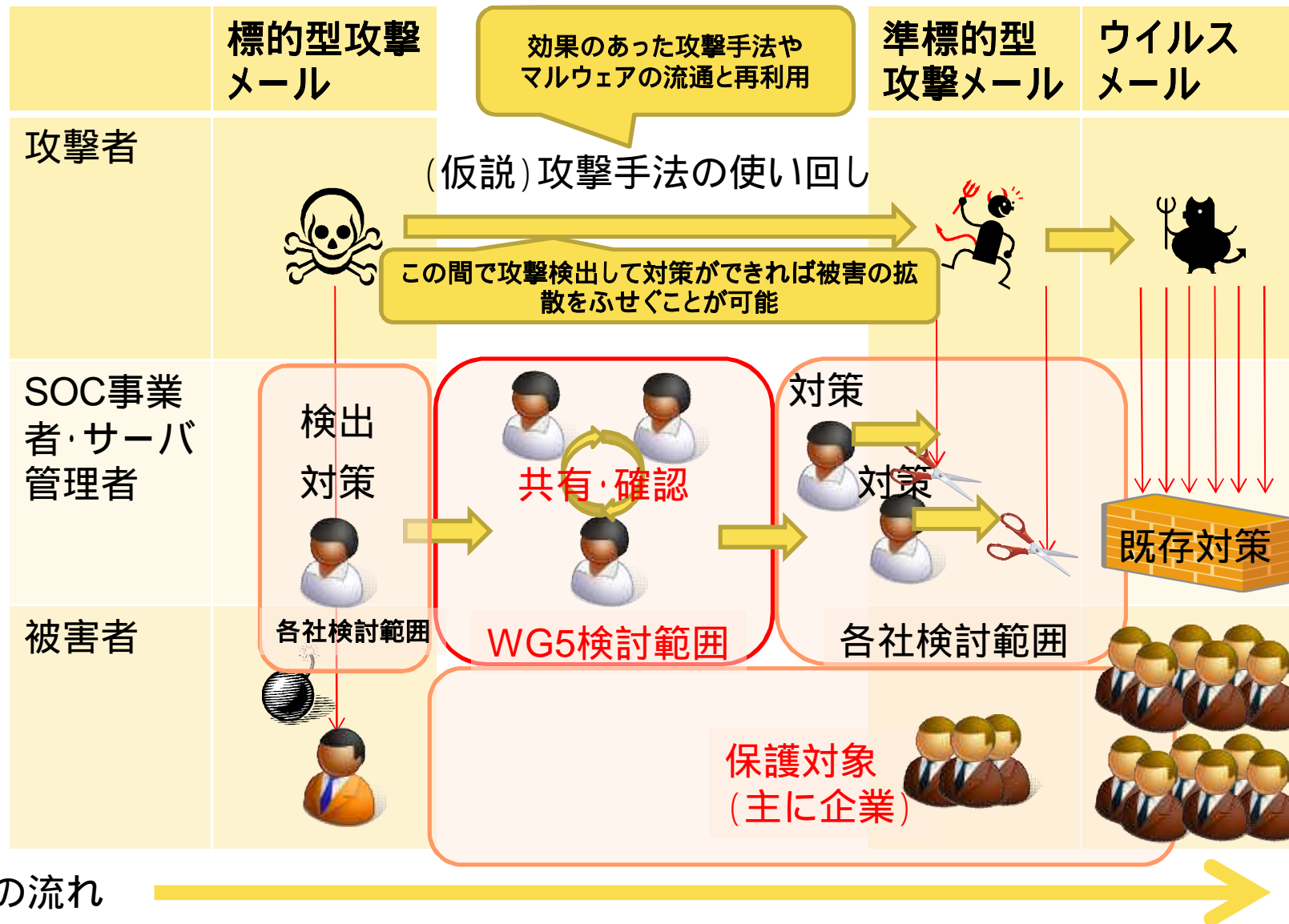
ブレインストーミング/標的型攻撃事例

- 標的型攻撃対策の検討範囲
 - 広くとらえると内部犯行やソーシャルエンジニアリング等も含まれる。
 - WG5はSOC事業者の集まりで、IT技術で対応可能な事象を対象とする。
 - 今回は入口としてメールを利用した標的型攻撃への対策を検討することとした。
- 再利用の仮説に基づきWG5で標的型攻撃を分類し、検出、対策のスコープを定める
 - 標的型攻撃
 - ある特定の組織や集団を標的とした攻撃
 - 準標的型攻撃
 - 標的型攻撃よりも広く、ある属性をもった組織や集団を対象とした攻撃
 - 一般のメールウイルス
 - 不特定多数に対する感染行為

今回検討の対象となる範囲

各社の既存サービスで対応

ブレインストーミング/標的型攻撃とその対策イメージ



ブレインストーミング/情報共有のありかた

- 参加事業者の立ち位置

- WG参加メンバー各社はそれぞれがSOC事業者としての背景や事業内容が異なり、扱う情報や対象顧客や契約等の活動条件が異なることに配慮しなければならない。
 - セキュリティ専門事業者
 - FWやIPSなどの情報を主に保有
 - ISP
 - 通信サービスに関する情報を保有(メールサービス、フィルタリングサービス等)
 - Sler
 - 企業ユーザにインテグレーションしたシステムの運用情報を保有
 - アンチウイルスベンダ
 - マルウェアに関する情報を保有
 - ユーザ企業
 - 自社のメールやWebアクセスに関する情報を保有
 - 関連団体

ブレインストーミング/情報共有のありかた

- 標的型攻撃に対する協調活動、情報共有のあり方について次の認識を得た(2011年8月時点)
 - － 標的型攻撃は特定組織の少数に対する攻撃であり、攻撃に関する情報には、**攻撃先となった組織の情報が含まれる**場合がある。
 - － そもそも顧客との契約等の理由により**情報の提供が困難な場合**がある。
 - 自社の調査等、事業とは別の何らかの形での参加しても構わない。
 - － メンバー各社においてこの活動のための**NDA締結も困難**である。
 - 会員規約範囲の守秘義務と情報の任意提供の範囲での活動とする。
- 標的型攻撃対策のゴールの設定の困難さ
 - － 検出技術は個別事業者依存。
 - － 情報共有だけでは未然に防げるか不安。
 - － 一方で標的型攻撃に関する情報が極端に少ない状況であり、事例研究や情報共有に意味は見出せる。

ブレインストーミング/奇策の検討

- 攻撃している人の気持ち、調査能力、目的を想定して対策できるか。
- 攻撃される側はインターネットに開示している情報は対策に利用できるか(もしくは、標的型攻撃を受けやすい人はいるか)。
- レディ・ガガさま事例は対応可能か？
- 迷惑メール対策で標的型攻撃対応可能か？(通信経路、署名付きメール(SMIME)等)
- 標的型攻撃の外延情報というものはあるか(標的型攻撃の被害とは何か？)。
- 標的型攻撃を受ける組織が他のソーシャルエンジニアリング(電話とか)で攻撃されているか。
- どこかで伝手を手繰って標的型攻撃を体験してみるか？

WG5活動概要

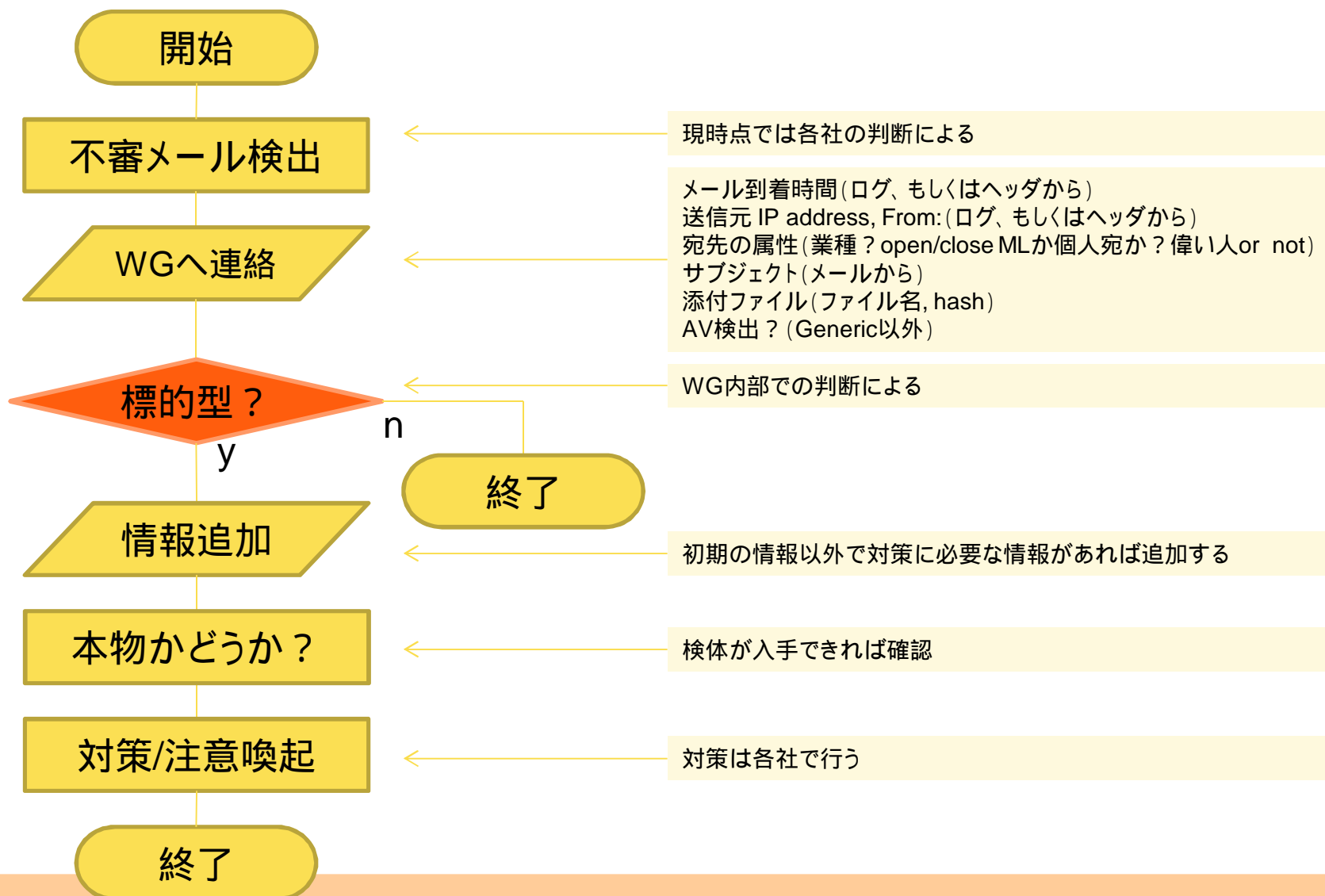
情報共有トライアル

実証実験トライアル

- テーマ
 - メンバー各社の持つデータの突き合わせは可能か
 - 付き合わせのキーとなる情報は何か
 - 実効力のある時間で共有は可能か
- トライアル1
 - 広く検出されているメールウイルス事例について各社での検出状況を比較し、早期の対策、攻撃者側のプロファイリング等を検討を行う。
- トライアル2
 - 標的型攻撃に利用されたマルウェアの情報をもとに情報共有が可能か検証する。
- トライアル3
 - 標的型攻撃に利用されたメールの送信元、マルウェアの通信先のIPアドレスに関する情報共有が可能か検証する。

以下、トライアルへの参加は任意(母集団はWG5参加メンバーの一部)であり、検出数等から意味を見出すことはできない点に留意してください。

実証実験/業界団体として想定する標的型攻撃協調対応の流れ



実証実験トライアル1

- メールヘッダ、本文の情報共有による攻撃検出(2事例でテスト)
 - Invoice.zip事例
 - 4社で攻撃を検出
 - xerox workcentre事例
 - 3社で攻撃を検出
 - どちらも内容的には**広範囲事例と考えられたため技術的には深追いせず**
(ただしAntiVirusは初期の段階では抜けてきている)
- 結果
 - 多数メンバーで検出。各メンバーの情報の突合せは可能であることを確認。
 - 一方で日常業務の範囲の違いや、組織的に確認できるデータ範囲の違いにより、確認速度や内容はメンバー各社でばらばらであった。
- 課題
 - 突き合わせる情報の粒度や内容の精査が必要となる。
 - リアルタイム性の担保方法の検討が必要。
 - 検証結果として共有できる情報にもかなり差がでてしまった。

実証実験トライアル2

- 標的型メールに使用されたマルウェア関連情報より流通状況を確認しての攻撃検出(2データセットをもとにトライアル)
 - WG5メンバーから提供された**検体名のリスト**を元に各社で過去ログ調査
 - 1社で1検体24通のみ発見
 - WG5メンバーから提供された**マルウェアリストのサブジェクト、添付ファイル名**でマッチング
 - 未検出
- 結果
 - マルウェア名称でのマッチングは困難であった。
 - AntiVirusごとに検体の収取時期が異なる。名称がつかないうちに攻撃される、また、名称が途中から変わることもある。
 - AntiVirusで検出されなければメールは素通りする。
 - 現在一般的にログとして記録されている情報には添付ファイル名やサブジェクトなどは入らず、これらの情報をキーにしてのマッチングも困難という結果に。

実証実験トライアル3

- 過去に標的型メールが送信されたIPアドレスもしくは検体が動いたときに通信しようとするIPアドレス情報の共有による攻撃検出。
 - WG5メンバーから提供された情報で検証
 - 4社で攻撃を検出。
 - 時系列で複数社にまたがって行われている通信や、ある特定のタイミングでピンポイントに発生している通信が観測された。
- 結果
 - WG参加メンバー4社で検出報告がなされており、情報共有による攻撃の検出として価値があった。
 - 情報共有してみても大量配信型メールウイルスであることがわかった事例も見つかった。
 - オペレーションとしてはログからIPアドレスを検索するだけであり、トリガーとしては比較的扱いやすい。
- 課題
 - ログデータが膨大なため、検索そのものに時間がかかりすぎる。特に、時間をどこまでさかのぼって調べるかによってデータ量は大きく異なる。
 - 同じIPアドレスでもメール送信元と検体動作後の接続先では検出後のアクションが異なる。実際の防御にどうつなげるかはもう少し議論が必要。

各トライアル比較

- 3つのトライアルを行うことで、情報共有による攻撃検出の可能性および、共有する情報の内容によって作業負荷や結果の精度が異なること等に関する知見が得られた。

	共有内容	今回の情報共有Trialで何か見つかったか	トリガーとなる情報の精度	調査対象ログのデータ量	調査にかかる時間	調査のしやすさ
トライアル1	メールヘッダ、本文、添付ファイル (メールそのもの)	見つかった	細かい (メールに関する複数の情報共有)	多い (特に全文保管している場合)	長い (データ量が多い、確認内容が多い)	たいへん (日本語エンコード等も考慮が必要)
トライアル2	攻撃に使用されたウイルス検体名称 (メール周辺情報)	見つかっていない	荒い (AV名称のブレ、未知検体はログに出ない)	少ない (AV検知ログのみ)	短い (AV検知ログから名称を検索するのみ)	やさしい (単純なパターンマッチ)
トライアル3	攻撃に関連するIPアドレス (ネットワーク関連情報)	見つかった	荒い (アドレス情報のみで内容は関係ない)	多い(FWのAccept logも対象とした場合)	長い (検索は単純だがデータ量が多くなる)	やさしい (単純なパターンマッチ)

これまでの活動のまとめ

- いままでの活動を通じて参加メンバーが得られた知見
 - 標的型攻撃対策に必要な情報共有のスキームの在り方に関する知見。
 - 標的型攻撃対策に必要な情報の内容に関する知見。
- 結論
 - 標的型攻撃に関する情報共有により、**複数事業者で検出した事例**が存在する。
 - この情報交換の方法によっては**未然防止につながる可能性**がでてきた。
- 一方で見えてきた課題
 - 検出のトリガーとなる情報を誰がどう見つけるか
 - 現在はWG5メンバーによる人的な作業である。
 - 情報を確認するスピードをどう担保するか
 - ログ形式やデータ格納場所、格納方法、日常的な取り扱いの有無の違いにより情報の確認にかかる時間に、メンバー間でかなりのばらつきがある。

今後の活動

- 状況の変化によって、WG5当初の設立目的である、「メンバー各社の標的型攻撃対策サービス」の実現は各社がすでに行っている状況となった。
- そこで、活動趣旨を「各社サービスの対応品質を上げる」に変更。
- 「対応品質を上げる」ために
 - 検出技術の共有
 - 情報共有のスキームを実務としてまわす
 - 情報共有の結果を効果測定
- 今までは情報共有にフォーカスしたが、攻撃そのものの検出技術確立、事後の対応まで含めて検討する。

ご清聴ありがとうございました。

