Internet Week ショーケース in 名古屋

昨今の標的型攻撃との向き合い方

伊藤忠商事株式会社　IT企画部 技術統括室
ITCCERT 上級サイバーセキュリティ分析官

国立大学法人　千葉大学　運営基盤機構情報環境部門　准教授

About me

佐藤元彦

- 伊藤忠商事株式会社　IT企画部技術統括室
  ITCCERT 上級サイバーセキュリティ分析官

- Sierで官公庁や大手民間企業に対してセキュリティコンサルティングや、セキュリティ監査、インシデントレスポンスを経験。
- その後、伊藤忠商事にて本社及び、グループ会社へのサイバー攻撃を未然に防ぐ仕事に従事。

もう一つの仕事

国立大学法人千葉大学
　運営基盤機構情報管理部門　准教授

- 伊藤忠商事と千葉大学とでクロスアポイント契約を締結し、一週間に一回国立大学法人千葉大学で勤務しています。
(会社からは、週一の出向扱い)

- 業務は伊藤忠商事と変わらずセキュリティ確保のための仕事をしています

会社概要

伊藤忠商事株式会社は、1858年初代伊藤忠兵衛が麻布の行商で創業したことにはじまり、一世紀半にわたり成長を続けてまいりました。

現在は世界65ヶ国（含日本）に約130の拠点を持つ大手総合商社として、繊維、機械、金属、エネルギー、化学品、食料、住生活、情報、保険、物流、建設、金融の各分野において国内、輸出入及び三国間取引を行うほか、国内外における事業投資など、幅広いビジネスを展開しております。

会社名：　伊藤忠商事株式会社

創業：　1858年

設立　：　1949年12月1日

代表者　：　代表取締役社長　岡藤 正広

本社　：　東京 / 大阪

資本金　：　2,534億円

連結売上高　：　50,835億円（2015年度）

当社株主に帰属する当期純利益　：　2,403億円（2015年度）

連結対象会社　：　326社（2015年度末）

従業員数(単体)　：　4,370名

従業員数(連結)　：　110,487名　*ドール約34,000名含む

ウェブサイト　：　http://www.itochu.co.jp

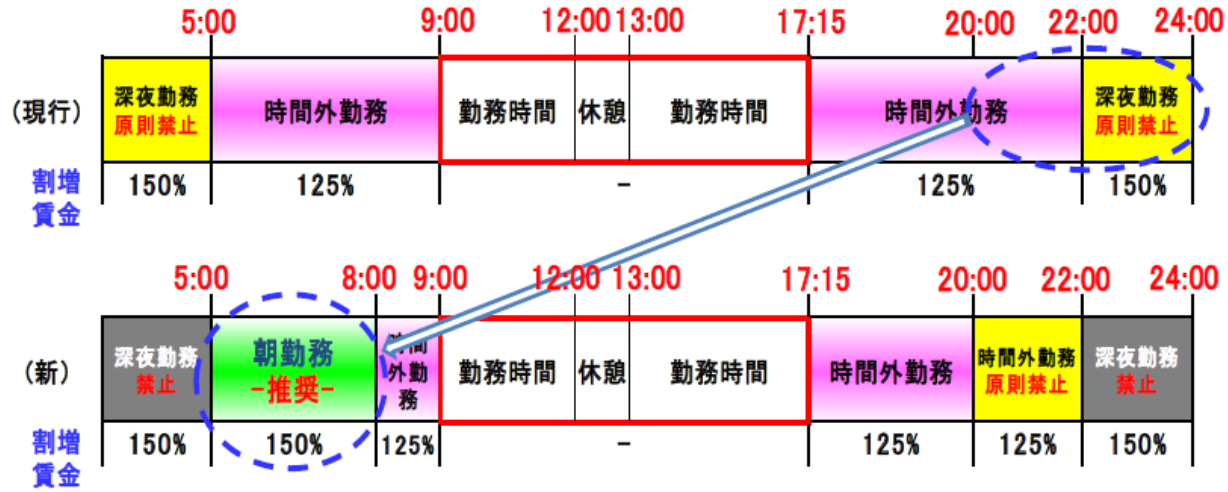
*2016年5月6日現在

＜東京本社＞

＜大阪本社＞

「これ」で知名度

- 20:00-22：00の勤務を**「原則禁止」**
- 深夜勤務（22:00-5:00)を**「禁止」**
- 20:00以降の勤務が必要な場合は、翌営業日の「早朝勤務」へシフト（**早朝割増賃金**支給）

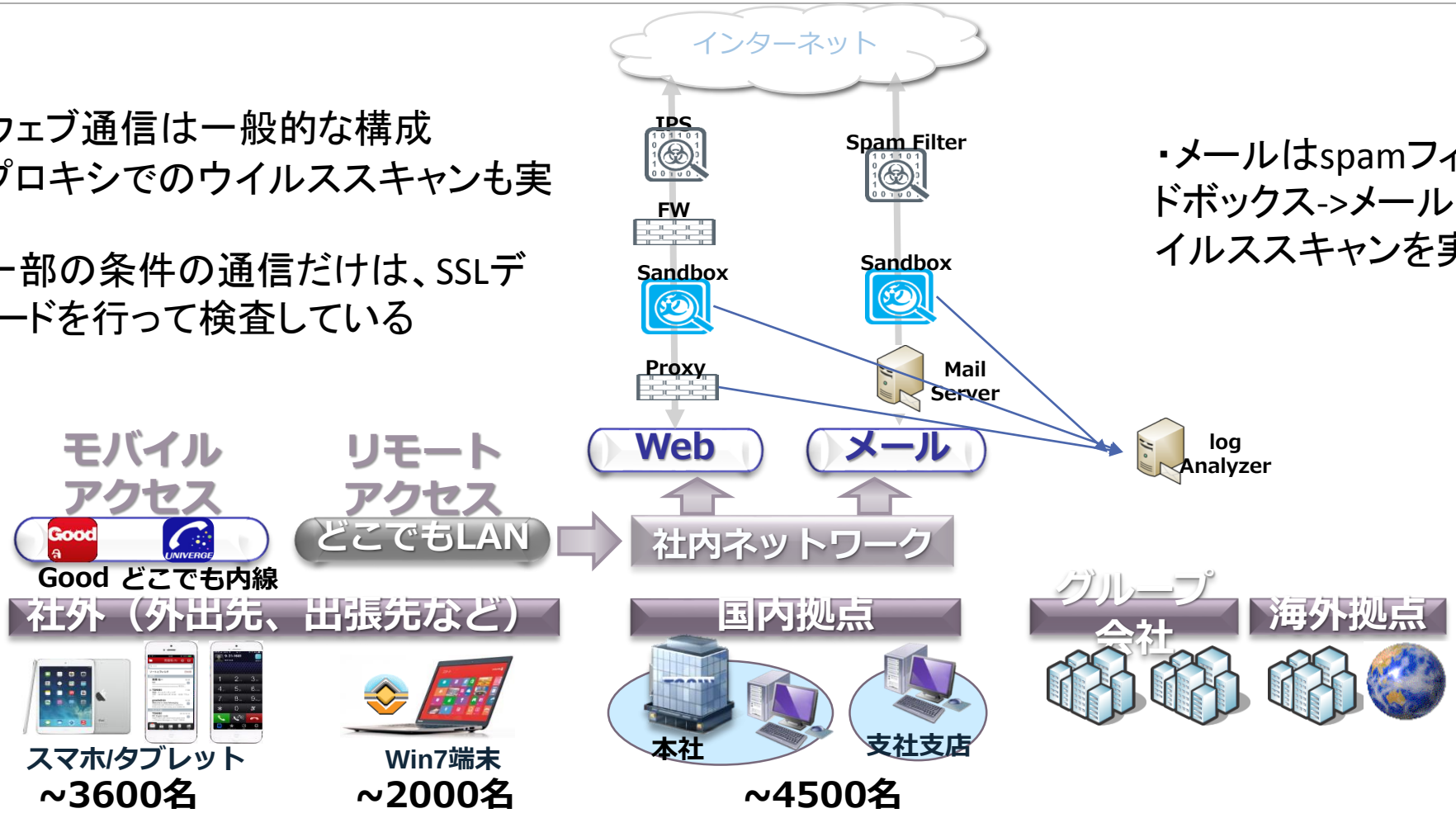


バナナ、ドリンク、パン、おにぎりなどの
各種軽食から無料で1人3品まで選べます

- 健康管理の観点から8時前始業の社員に対し、**無料で軽食を支給**

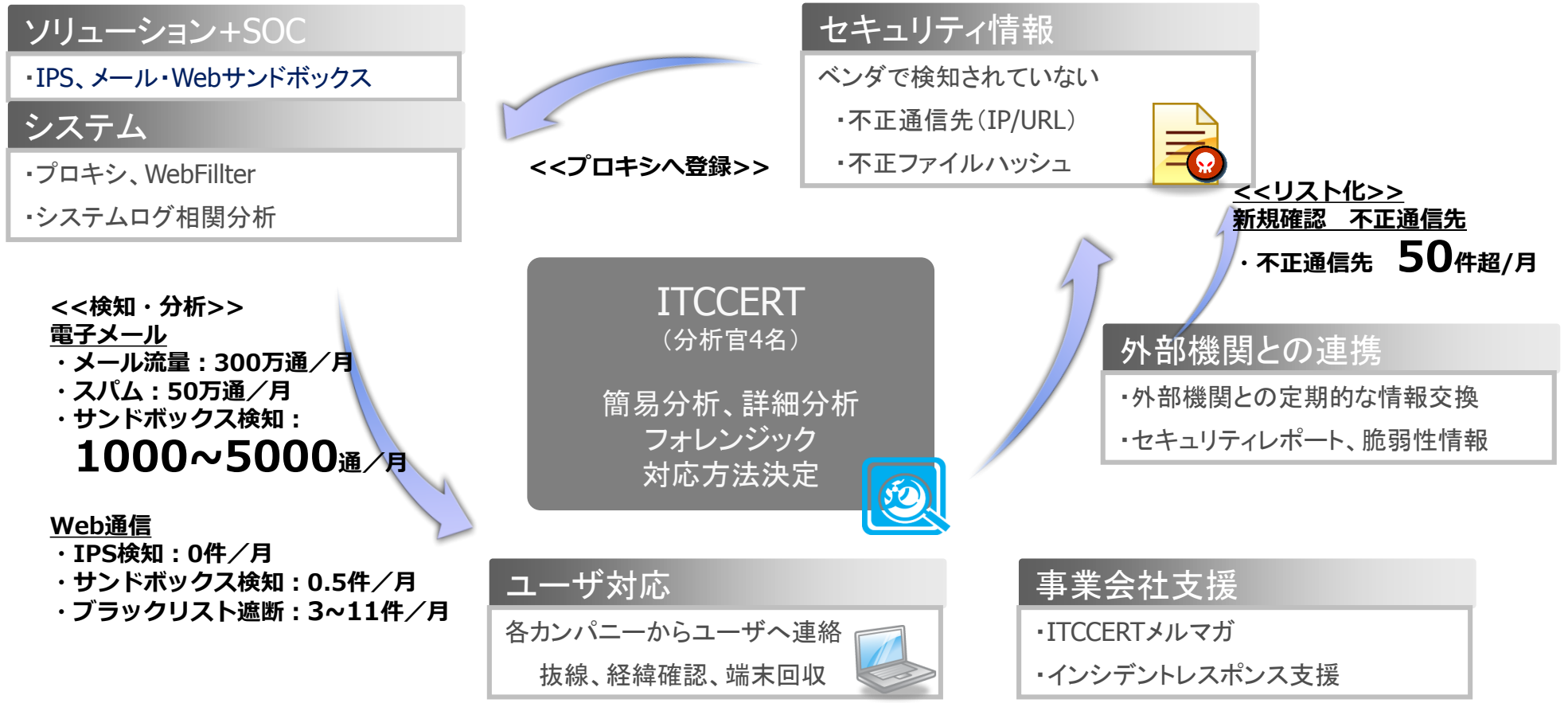
伊藤忠商事のセキュリティの仕組み

・ウェブ通信は一般的な構成
・プロキシでのウイルススキャンも実施
・一部の条件の通信だけは、SSLデコードを行って検査している



・メールはspamフィルタ->サンドボックス->メールサーバのウイルススキャンを実施

ITCCERT取り組み



ITCCERTの仕事

セキュリティアラートを「生」で分析

- SOCより早く、正確に
- イベントとインシデントの切り分け
- 早期警戒情報の入手
- 防衛ルールの策定
- 各機器標準では検知できない攻撃の捕捉と解析
- 各機器への追加セキュリティ設定の設計

ユーザ側にたってわかること

あまりセキュリティの現場は(よい方に)変わっていないように感じます

もちろん、よい機器や製品ができて、特定の組織では先進的な取り組みもしていて、一部はとてもよくなっているのですが、社会全体としてはあまり変わらないような。。。

あまりかわらない
商業セキュリティ業界の風潮

営業や営業推進が、米国から借りてきた事例をもとに、脅威のリスクを煽って、よくわからない製品を勧める講演や営業活動??が継続中

だいたい以下の構成

・当社の米国の誰かの調べとか、他社の調べによると、「とってもヤバいよ!!」(あなた知らないでしょ??)

・で、実際に被害にあうと大変(みたい)

・そんな時。。。(欧米では評判の)製品どうぞ―

なにかに似てる

深夜の健康食品のCFみたい

・「病気になって健康のありがたさを知った」->「そんなときこの商品に出会ったのです!!」

※個人の感想であり、
商品の効能を確約するものではありません

もう聞き飽きた

右肩上がりでサイバー攻撃が増加、とか

より巧妙になった、とか

従来の機器では防げない、とか

未知の脅威が、とか

あと十年後も同じこと言ってそうですね。。。

そして運用を考えられる人が少ない

新規の機器導入。アラート発生。該当の端末を特定して調査してください。<- こういう運用文書を作る人が多い!!

現場が一番最初に行うのは、「アラート」の正誤。(よく誤検知があるわけで、まずは、そのアラートの正当性を確認するために実施する作業が多い)

そして、端末の調査の際には、どういうアラートだからどこを見る、ということが決まっていないと何もできない。

->使えない運用図書が出てきたときには、”優しく”この文書に基づいて、我々の隣に座って運用してみてください、と言うことが効果的

本当に必要なのは。。。

道具と情報を組み合わせてつかいこなす「**現場力**」ではないかと感じてきました

本日の主題:現場

様々な被害に遭った組織では。。。

セキュリティ運用がなされていなかったことが多い

今回は、機器はいれたけれど、不安が、という方向けに、日々、CERTチームが何をしているか、をお伝えします

さて質問!!

この一年間、サンドボックスで検知できなかったマルウェアメールを自組織では受信したことがある？

ポイント:

サンドボックスを
「すり抜けた」
とわかる運用が
できているか？

サンドボックスは簡単に越えられる？

サンドボックスを各種のマルウェアは簡単に検知して、無害なアプリを装うようになりました。

例えば。。。

- 仮想環境とわかるファイルの存在を確認する
- 疑似通信型の機器の場合は、ダウンロードするファイルのハッシュを整合する
- OSの起動時間を確認する
- マウスの位置を確認する。。。など

大事なことは、サンドボックスが「万能ではないこと」を知って管理策を立てることです。

サンドボックスは有能だけど。。。

サンドボックスで検知できる程度のマルウェアを本気の犯人が送ってくると思いますか？

セキュリティ運用者が本当に注目すべきは、サンドボックス越えを果たしたマルウェア

でも、どうやって？

1.ウイルス対策製品を使い込もう

ウイルス対策ソフトで、定期スキャン、常時スキャンしていますよね？

結果、確認していますか？

いらないもの

検知数

(増加数等の指標以外には特に。。。)

いるもの

検知場所・検知名

スキャンの結果確認の重要性

リアルタイムスキャン -> パターン対応できている既知のマルウェア -> 発見された場所や、マルウェア名に注目する

・多くはメールの添付や、ウェブサイト内のスクリプト検知

・動作しているもののトラップ -> 動作している(なにが？どうして感染？)

・メールの添付検知でも。。。危険なタイプのマルウェアが着信していることを知ることが重要

確認ポイント (1)

以下のような検出名のマルウェアには注意

- Downloader -> 他のマルウェアを呼び込む
- Backdoor -> 外部から通信可能にする
- PlugX, PoisonIvy, emdivi, **RAT ->
  有名なマルウェア名のもの・遠隔操作
- Infostealer -> 認証情報などを外部送信する
- Keylogger -> タイプした内容を外部送信する
- pwdump -> パスワードを解析する
- ELIRKS と asurex …

確認ポイント (2)

以下のパスからの検出にも注意

- C:¥Windows の中　(動いているかも)
- C:¥Program Files の中　(動いているかも)
- D:¥の中　外部記憶媒体？　持ち込まれた元が感染しているかも？

- また、ソフトウェアによってレジストリやプロセスで検出することも。これらは特に注意!!

消えたから安心ではない

ウイルス対策ソフトで消されたから安心、といえるのは「リアルタイム検索の結果だけ」です。(それすら不安なAVも)

定期スキャンで検知されたマルウェアは、**過去には未知だった、侵入した、動いていた危険なマルウェア**かもしれません。

追跡が必要です!!

当社では全アラートがリアルタイムで
CERTに届くようになっています

そして

エンドポイントは多層防御をした先のはずなのにどうしてここにマルウェアがいる？ということに疑問を持つべきです

端末にマルウェアが届く前に「いろいろ」しているはずなのに。。。

見直しのチャンスです。

2.スパムフィルタを使い込もう

カスタムルールいれていま
すよね？

サンドボックスに届くそもそ
もの不審メールを減らす

特定条件の添付メールの複
写を残す

標的型攻撃メールで
最も有効な管理策は。。。

実は、サンドボックス製品ではなく、従来型のスパムフィルタ製品の活用が標的型攻撃メールに効く最高の管理策だと考えています。

単にスパムフィルタ製品をいれればよい？

そんなことはありません。

スパムフィルタの機能を使い切ることが、標的型攻撃メール(ばらまき型攻撃も含む)の最大の防御策になっています。

設定ポイント　不審ファイル対応-1

スパムフィルタで、「特定の拡張子」に対して件名に警告を表示するなど、利用者に注意喚起する。

特定の拡張子: .exe .lnk .js .docm .xlsm .pptm .potm .ppsm .ppam

.exe : 実行ファイル。本当は遮断したいところですが、セキュリティソフトが暗号化のために「実行ファイル形式」にしてくることがあり、残念ながらビジネス上、拒否しきれません。

.lnk : ショートカットファイル。任意のスクリプトを動作させられる可能性があり危険ですが、ブックマークを共有するために添付されることもあり、ビジネス上で制限をかけることは微妙。

.js : JavaScriptファイルそのもの。プログラムとして動作しますが、例えば、ウェブサイトを保存して一括して送ってきた場合に含まれてしまうなど、ビジネス上制限をかけるのは困難。

.docm等 : マクロが含まれるMS Officeファイル。マクロを含むファイルは多くビジネスでやり取りされており制限できません。

サンドボックスで検知できない形式の拡張子を加える!!

設定ポイント　不審ファイル対応-1

危険度の高いメールは、”abnormal file attached”や、そのもの”危険な形式の添付ファイル”というようにスパムフィルタで件名付与して、利用者に注意を促すことが、リスクの低減に繋がる。

もちろん、開かせなくすることが目的ではなく、利用者に注意喚起をすることが目標。

設定ポイント　不審ファイル対応-2

危険度の高い拡張子の添付ファイルは、そもそもビジネス上、受信する必要がないため受信拒否する。

.scr : スクリーンセイバーファイル
.com :実行ファイル
.hta : HTML Applications
.cpl :コントロール パネル ファイル
.wsh .wsf :ウインドウズ・スクリプト
.jar : Java Archive

設定ポイント　不審ファイル対応-2

拡張子を表示する設定にしていない環境を狙って、exeを隠す形になる、いわゆる二重拡張子のファイル送信されてくることがありますが、こちらも基本的にビジネス上では発生しません

.doc.exe .pdf.exe jpeg.exe など。。。

拡張子を表示しない設定にした環境では、.doc .pdf .jpegに見えてしまいます

設定ポイント　フリーメール対応

フリーメールから標的型攻撃メールを受信しているケースはかなり多くあるため、フリーメールから受信したメールには、スパムフィルタでフリーメールからの着信であることを明記する。

フリーメールの例　@yahoo.com, @yahoo.co.jp, @gmail.com, @excite.co.jp, @hotmail.co.jp, @goo.ne.jp, @live.jp, @infoseek.jp

設定ポイント　フリーメール対応

利用者に注意を促すことが、リスクの低減に繋がります。例としては、”from freemail”や”フリーメールからの受信”などという件名を付加することが考えられる。

日本向けの攻撃では、日本のフリーメールが使われることが多いです。

ばらまき型のメールでは、騙りメールが多いですが、使われる場合は海外のフリーメールが使われることが多いようです。

運用ポイント　スパムフィルタ監視

スパムフィルタでブロックされたり、特定の拡張子やフリーメールから受信したメールを確認し、自組織への攻撃の検知や、誤検知によるビジネスへの影響を測る。

監視の観点は、フリーメールからの警戒・拒絶ファイルが添付されたメールの接到や、Header Fromとsmtpサーバが不一致になるメール、そして日本語で書かれたメールなどです。

回数は、組織への攻撃の認知のために、一日に一回は行うべきです。(当社では朝夕二回)

不審メールを減らせれば

ノイズが減って、より担当者は、
少数のポイントに力を絞ることが
できます。

セキュリティ機器は、こういった使
い方をするもの、と割り切って考
えると、運用がしやすくなります。

日々やってほしいこと

サンドボックスの検知結果と、ウイルス対策ソフトの結果と、スパムフィルタの結果の比較

例えば、exeなどは流量が少なく
マッチングが簡単です

->冒頭の質問
　サンドボックスをすり抜ける
マルウェアをキャッチする仕組みの一つ

でも。。。

最近の悩みは、PDFにJSが埋め込まれたファイル

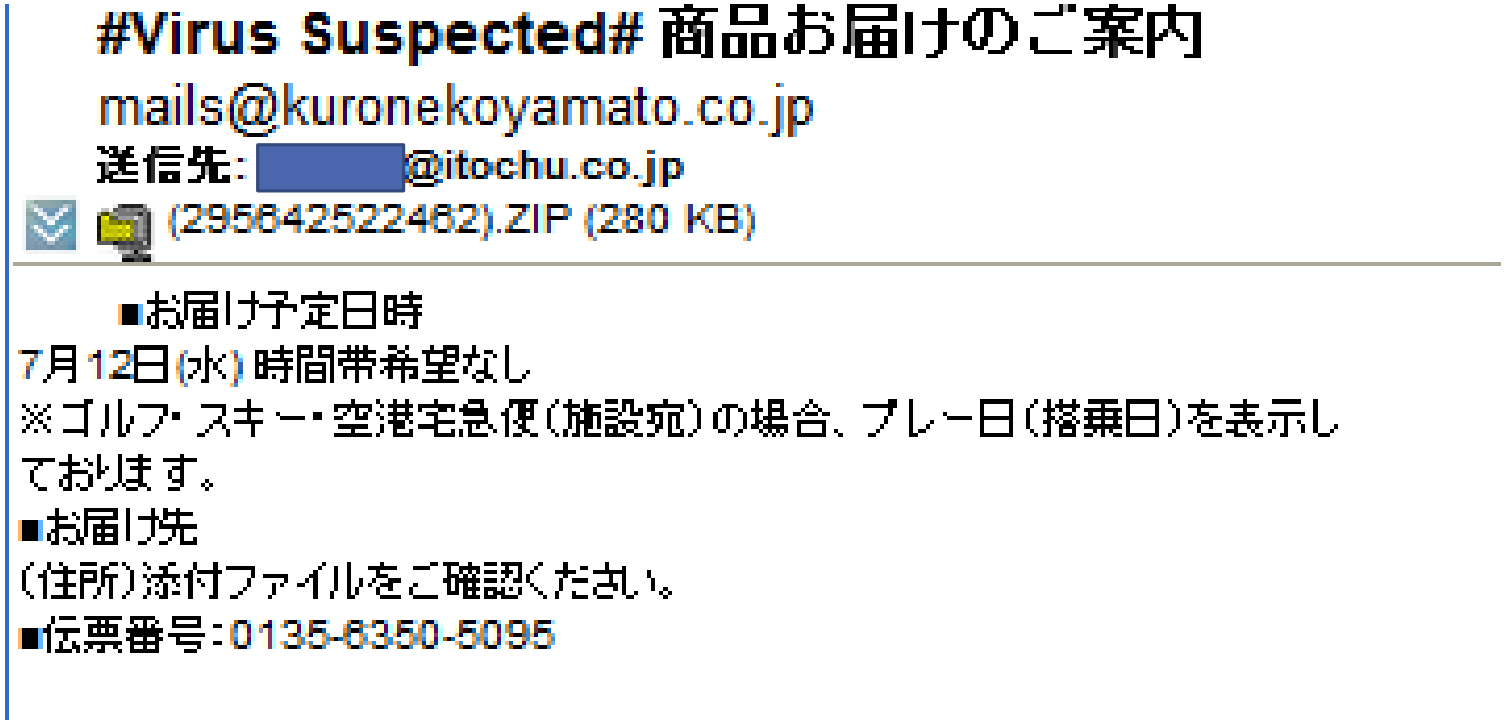
PDFの中をクリックしないと発動しないことから、被害に至ることは少ないですが、そもそもマルウェアを流入させたくないという方針に大きく影響しています
(対策検討中)

3.プロキシログを分析しまくろう

当社ではsplunkを使ってログの分析をしていますが、レポートとアラート機能を駆使して、省力化をはかっています。

分析ポイント　特徴に注目

日本語マルウェアメールのマルウェアには通信に特徴があります。



バンキングマルウェアの特徴

POST /images/_2Fk_2Fj0/ECYTSwCu_2FGwAgAbDN6/kbztlKYJiApNknHwNWL/wxmqY6l0lpIpybgbceSgkg/2JM6iNgruYTXK/a1DfuhoW/9a4wJ4V_2BrKLzmzQTUKBxE/1w_2FM6EvO/z7qIZ21J_2FDFwm7i/OZhUABPkV_2B/YjM8362k79K/CbBW_2F0mniqY8/aca_2FSRDg/6.bmp

-> bmpのパス に “POST” <- 異常な通信

ずっと変わらない普遍の通信形式!!

こういった通信は「すべて」自動アラート

こんな感じでデータを抽出し、踏んだ人情報を含めて、メールがCERTに届くようにしています -> 省力化

```
sourcetype=bluecoat cs_User_Agent_="Microsoft-CryptoAPI/6.1" cs_uri_port="443"  | iplocation r_ip |
lookup itochu_users cn as cs_username OUTPUT displayName, department, mail | table _time cs_categories
s_action c_ip cs_username displayName department mail cs_host r_ip Country cs_uri_port cs_uri_path
cs_uri_query cs_Referer_ cs_User_Agent_
```

他にも

ELIRKSのymailer miniのリファラ

```
sourcetype=bluecoat cs_Referer_"XXX" | iplocation r_ip | lookup itochu_users cn as cs_username
OUTPUT displayName, department, mail | table _time cs_categories s_action c_ip cs_username
displayName department mail cs_host r_ip Country cs_uri_port cs_uri_path cs_uri_query cs_Referer_
cs_User_Agent_
```

DaserfやELIRKSのUA

```
suorcetype="bluecoat" cs_User_Agent_="*SV1)"
```

などマルウェアの特徴ドリブンの警告や。。。

動作に着目

いくつかのマルウェアが、グローバルIPを取得に行く行為をトラップするなど、動作に着目したりしています

```
sourcetype=bluecoat cs_host="icanhazip.com" OR cs_host="myexternalip.com"| iplocation r_ip |
lookup itochu_users cn as cs_username OUTPUT displayName, department, mail | table _time cs_host
r_ip cs_uri_port Country cs_categories c_ip cs_username displayName department mail cs_Referer_
sc_filter_result x_exception_id
```

更には広いチェックも

.exeのダウンロード

200MBを超える外部へのファイル送信

短いUserAgentの通信

DynamicDNSへの通信

をリスト化し、定期的に確認することで
「異常」を見つけ出すようにしています

毎日のルーチン

大量マルウェアメールの受信や、日本語のマルウェアメールの受信があった場合は、通信先の制限だけでなく、特徴的なパスや、ファイル名を警告対象に投入し、もしもに備えています。

本日受信した日本語マルウェアメールについて、共有致します。

●件名：{LET:Fwd:,Fw:,FW:}
添付ファイル名：01458255282853.zip
添付ファイルハッシュ(MD5)：ec4d9c93ca99033cd793061e3d0732eb
展開後ファイル名：order_sent_92037847882911.pdf.exe
展開後ハッシュ(MD5)：9f013cbeee67113c2ccfc5d4e421ad56
⇒荷物の発送完了通知を装う日本語マルウェアメールでした。
検疫フォルダにて5件受信しています。

【一次通信先】
ssl.pathwaystopromise[.]com/setup32s.bin　⇒Malnets
【二次通信先】
ping.cloudchai[.]net/images/　⇒Malnets

●件名：05.17
添付ファイル名：00164.29.05.17.zip
添付ファイルハッシュ(MD5)：96117f899b1fa1312202f3086a52feee
展開後ファイル名：00178.29.05.17.doc.exe
展開後ハッシュ(MD5)：9f013cbeee67113c2ccfc5d4e421ad56
⇒入金依頼を装う日本語マルウェアメールでした。
検疫フォルダにて2件受信しています。
展開後ハッシュは「{LET:Fwd:,Fw:,FW:}」と同様のため、
詳細は割愛致します。

メールサンドボックスの結果も条件によりリアルタイムアラート

たとえば、

・一定時間で大量にマルウェアメール検知があった場合アラート発報 -> 必要に応じて対応

・当社やグループ会社のドメインのメールアドレスでマルウェアメールを受信した場合にアラート発報 -> メールボックス乗っ取りのリスクも含めメールヘッダ確認

これで大きなポイントの二か所

内部に入り込むメールと、外との通信経路、あと一つは。。。

ADです

4.ADを見張ろう

管理者OUにあるアカウントに対して、ログイン失敗があるとすぐにアラートメールがCERTに飛んできます。

->たいてい、システム管理者のミス

->システム管理者のMLにも、失敗通知メールが飛ぶ

->失敗を自己申告してもらう

->結果、省力化して対応可能

(報告のないものの多くは複合機のメンテナンス)

かつ、ADをどんどん要塞化

RDPのポート番号を変える -> 検知

ADの前にFireWallをいれて、通信をトラップ

AD-IDSを導入して特定の攻撃をトラップ

ハニートラップアカウントを設定してログイン試行即攻撃と判断

本丸のADを触ろうとする不届きものを検知する仕組み

5.インテリジェンスを磨こう

不審通信先の情報は様々な形で共有されています。

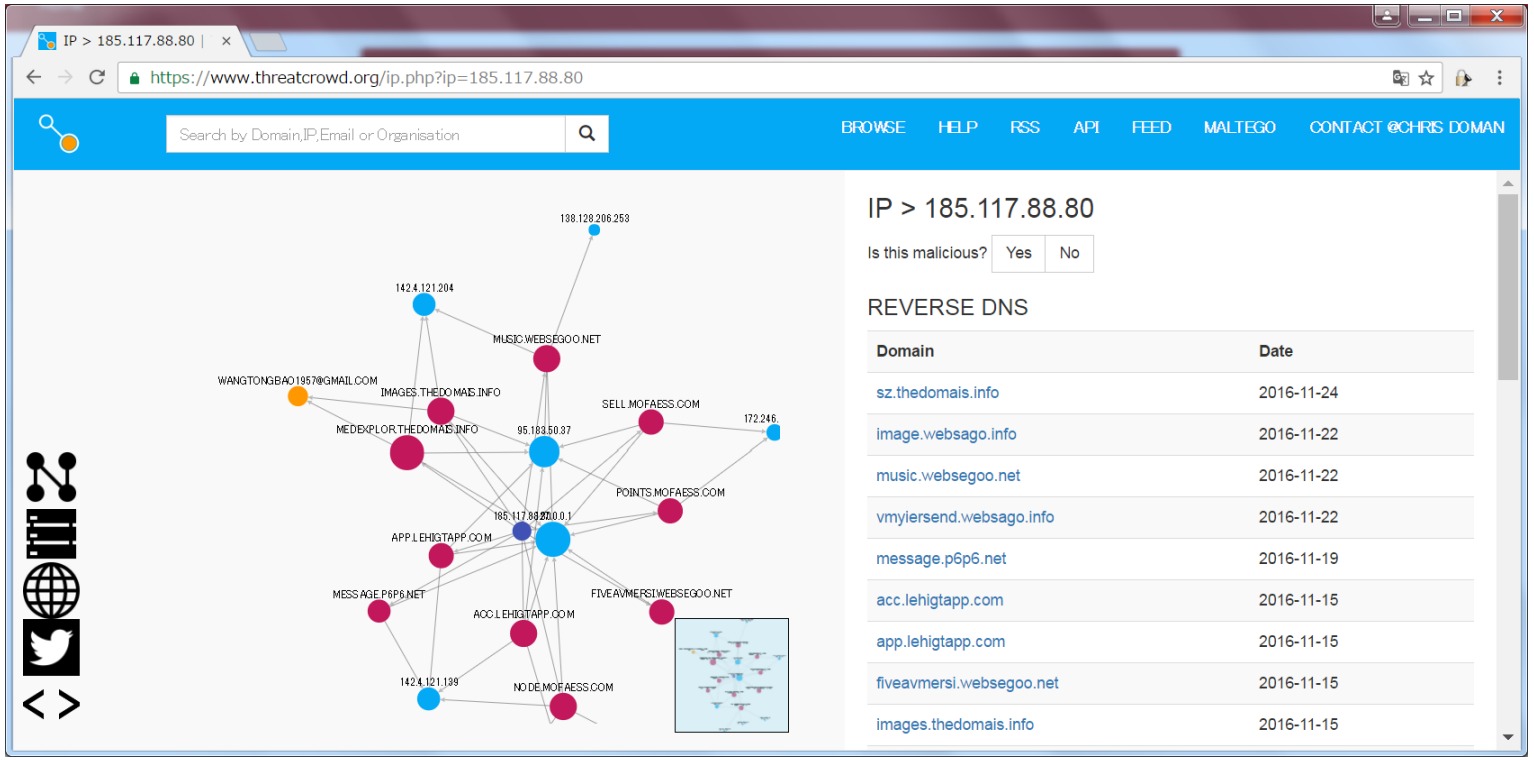
それをそのまま不審通信先として制限するだけ。。。

それではあまりにもったいない!!

本当に正しい情報？

特にIP情報は、制限してよいか悩みます。そんな時。。。

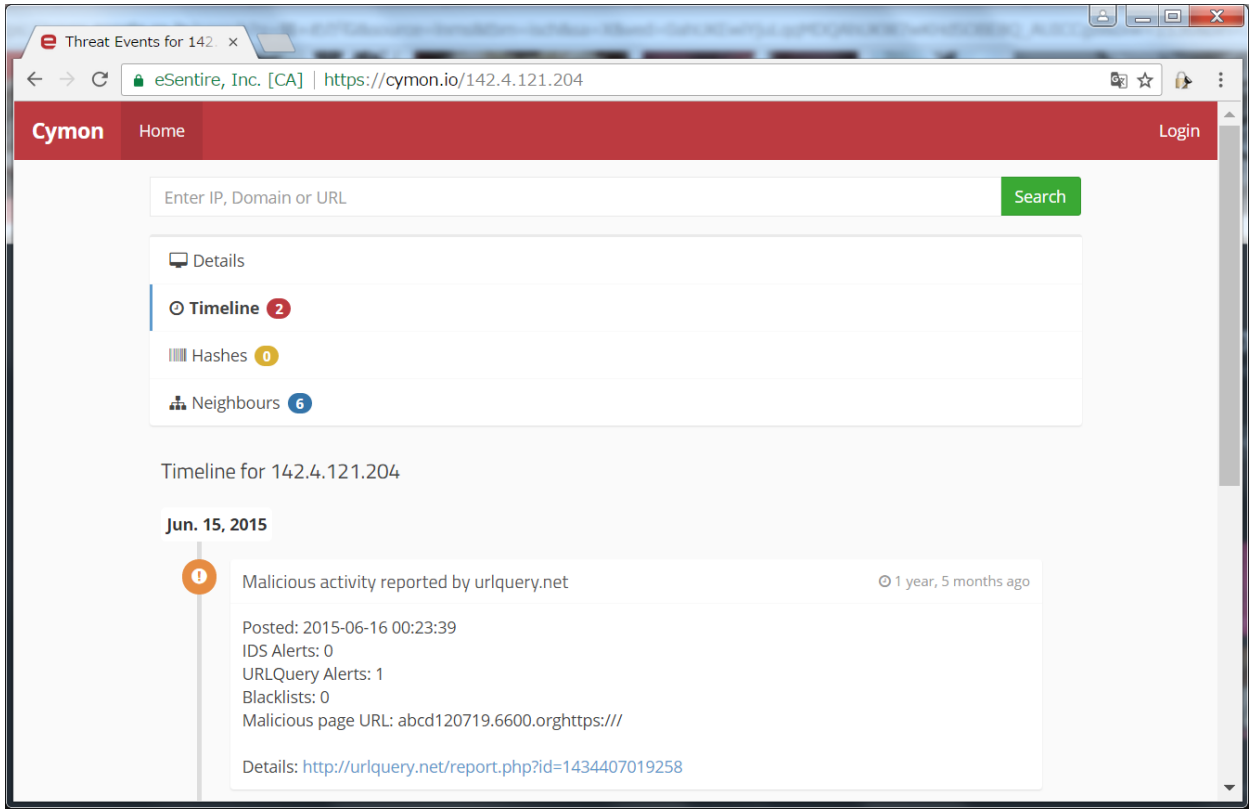
調べましょう!!



https://www.threatcrowd.org/

様々なOSINTツール

調べましょう!!



https://cymon.io/

調べれば。。。

関連情報など、怪しい痕跡がうかびあがってきます。

同じ登録者に登録されたドメイン

同じIPに紐づけられたドメイン

関連性のある名前のドメイン　など。。。

調べることで、オリジナルの「鑑識眼」が養えます!!

	First Seen	2014-03-24T22:44:32Z	Ended	Name	Org.	Street
j.com	4-Nov-16	2016-11-03T20:48:30Z	2017-11-04T01:55:32Z	Juanita Dunham	Wild Oats Markets	745 Melody Lane Richmond, VA 23219
maste.com	4-Nov-16	2016-11-04T01:55:32Z	2017-11-04T02:19:40Z	Megan Delgado	Newhair	3328 Sigley Road Burlingame, KS 66413
kingl.com	4-Nov-16	2016-11-04T02:19:40Z	2017-11-04T02:45:18Z	Elisabeth Green	Consumers Food and Drug	2679 Zappia Drive Lexington, KY 40507
-go.com	4-Nov-16	2016-11-04T02:45:18Z	2017-11-04T03:27:44Z	Rufina Webb	William Wanamaker & Sons	4120 Alpaca Way Anaheim, CA 92801
-obert.com	4-Nov-16	2016-11-04T03:27:44Z	2017-11-04T03:43:38Z	Robert Butler	Sammy's Record Shack	383 Howard Street Grand Rapids, MI 49503

運用ポイント　情報の再分析

ホワイトペーパや、インジケータで入手した情報をもう一度自分なりに解釈してみましょう。

マルウェア、ドメイン、IPを再度自分の目で見直すスキルをつけることで、普段や有事の際の調査スキルが身に付きます!!

と、こんな感じで「運用」しています

その他、例えばHDDの間に挟んでおいて、いつもOSを初期化できる機器を活用して、マルウェアは「走らせて」解析したり、特定カテゴリのSSLをデコードしてサンドボックスを通したり、もっとやっていることもありますが。。。

今回は時間もないのでここまでとさせていただきます。

この運用は四名体制

09:00～17:30で、実務は実質運用担当一名と、修行中二名で対応。

(佐藤は実務もしますが、インシデントに近いアラート対応の切り分けに注力し、普段は検知ルール作りやグループ会社向けのセキュリティ施策の立案推進などを行っています)

より効果が高くより手抜きできる方策を考えて日々仕組みを改善実施。

フィードバックの実施

検知されなかったマルウェアは、経路上の機器ベンダーに提供しています。

新たな悪性の通信先についても、検体の分析結果とともに、プロキシのベンダーに提供しています。

また、当社に接到するマルウェアについては、Virustotal等で分析履歴がない検体だった場合は、ポストするようにしています。こういった取り組みが回りまわって、我々に返ってくることを願って。。。

今日のまとめ

建物にいくら鍵をかけていても、警報がついていたり、警備員が見回っていないと、被害に気付けないように、日々の運用が大事です

ところが、見まわるポイントはあまりにおおく、効率的に行うための知恵が必要です。

そこで

現場どうしで仲良くなりましょう。

実現不可能な上から智識や、高くて知覚過敏の機器(誤検知だらけ)や、ゆっくり告知のSOCなど、もう飽き飽きじゃないですか？

これからのセキュリティの仕組みと改善はユーザサイドで作っていきたい、ということをお伝えしてこの時間を終えさせていただきます。

ご清聴ありがとうございました