BLUE TERMITE（ブルー ターマイト）
～日本を標的にするAPT攻撃～

Save the World from IT Threats

※ 本資料は、6月4日のプレスカンファレンス発表時に使用した
オリジナル版を、一般公開向けに加工・編集したものです。

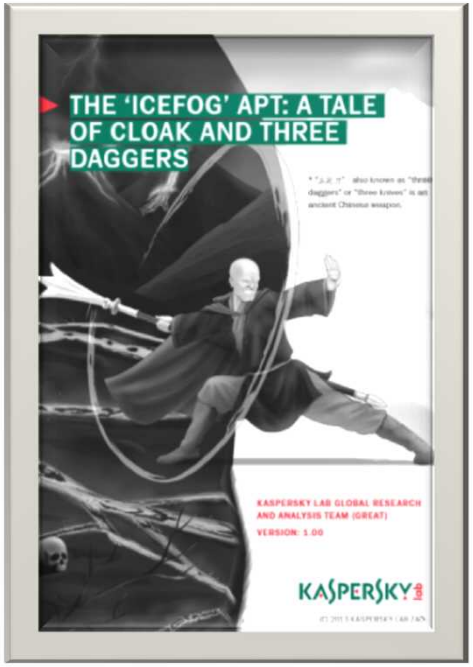
2015年6月4日（木）

株式会社カスペルスキー

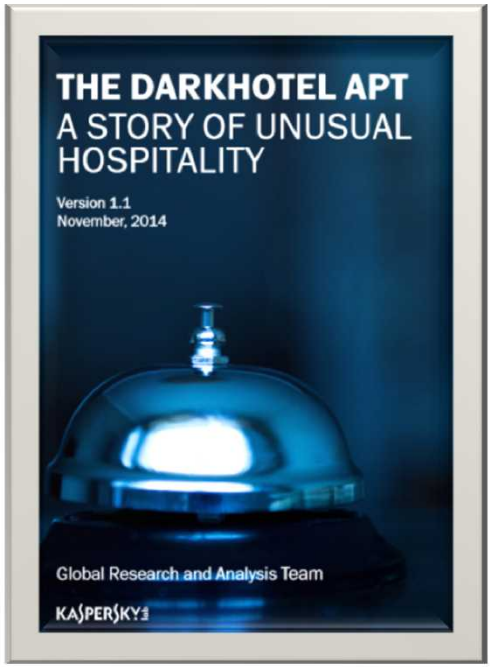
本カンファレンスの目的

- 「Blue Termite」（ブルー ターマイト）と名付けた、
  日本を標的とした新たなAPT攻撃の紹介。
- この攻撃にさらされている日本の被害状況の解説。
- 本格的な攻撃に直面した日本が、マイナンバーの導入や
  オリンピックの開催を控え、現状を再認識しセキュリティを高めるための提言。

※　既出の情報の掘り下げや報道の加熱、ならびに被害者を槍玉に上げることは、本カンファレンスの目的にはありません。



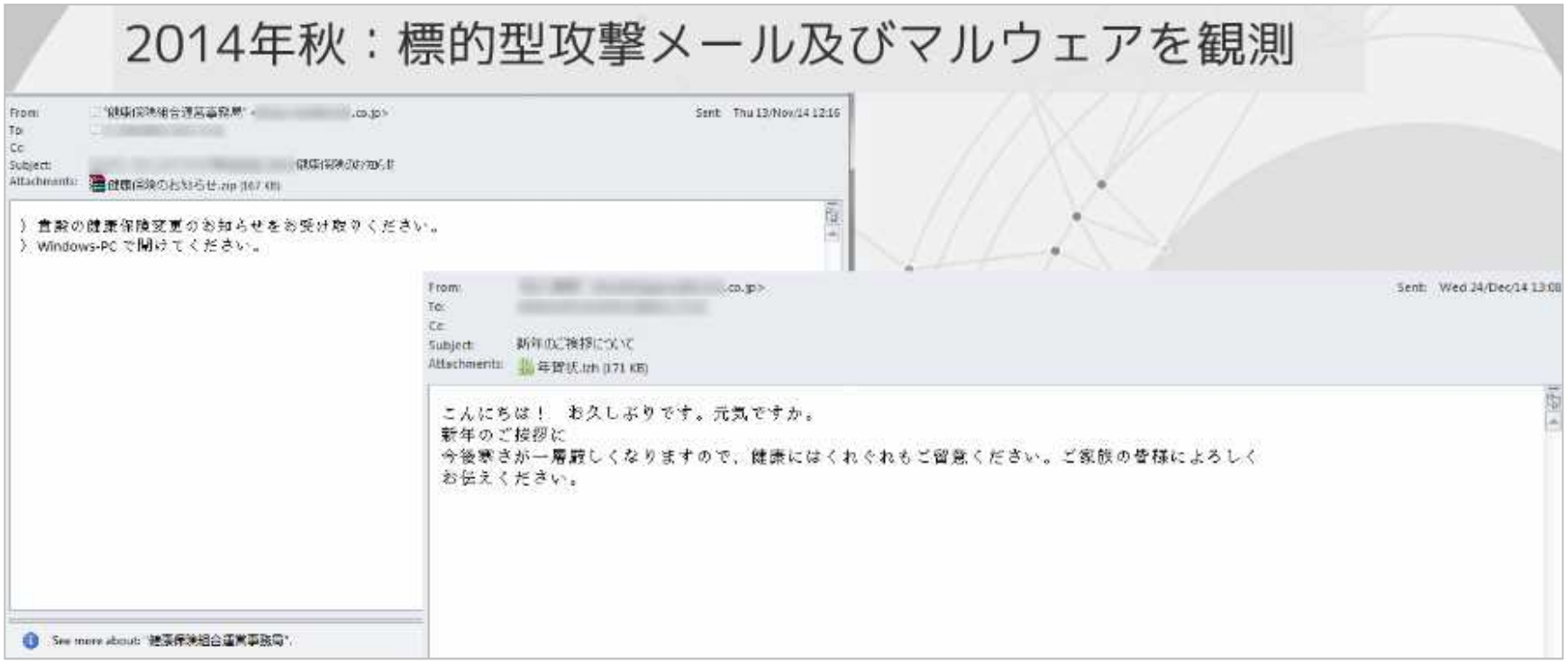
2013年
日本を標的にした初の大規模APT「ICEFOG」（アイス フォグ）を確認



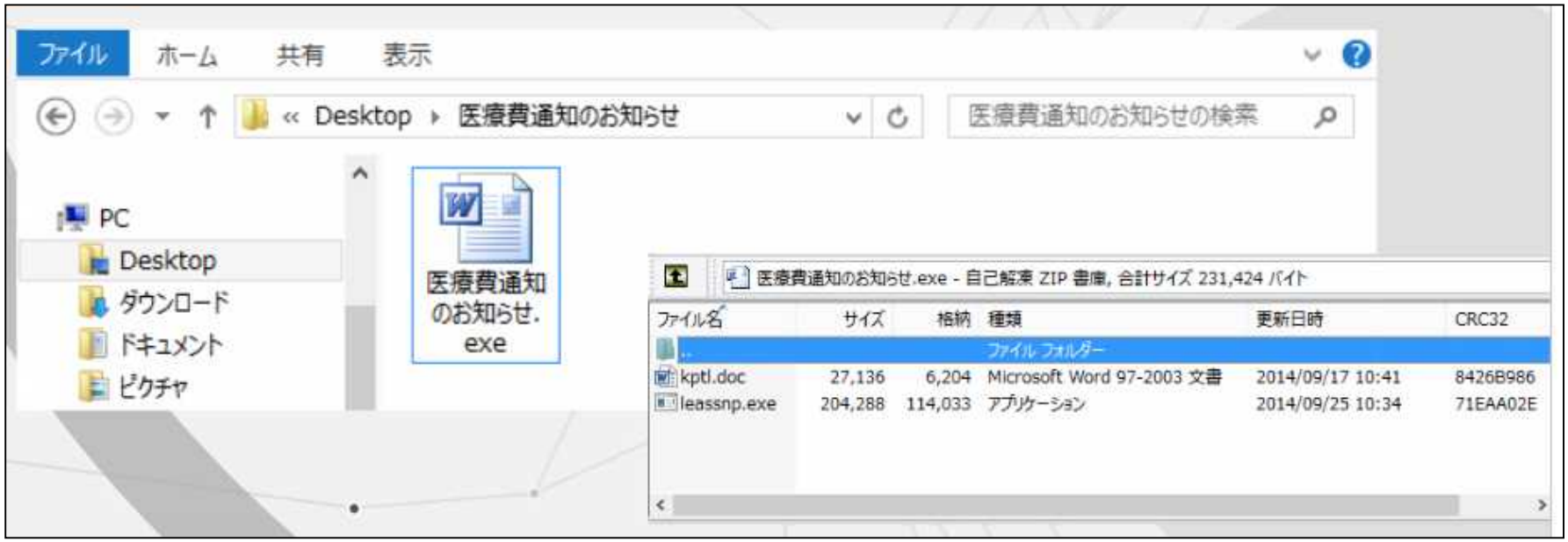
2014年
日本を含むアジア地域のホテル滞在者を標的にした「DARKHOTEL」（ダークホテル）を確認

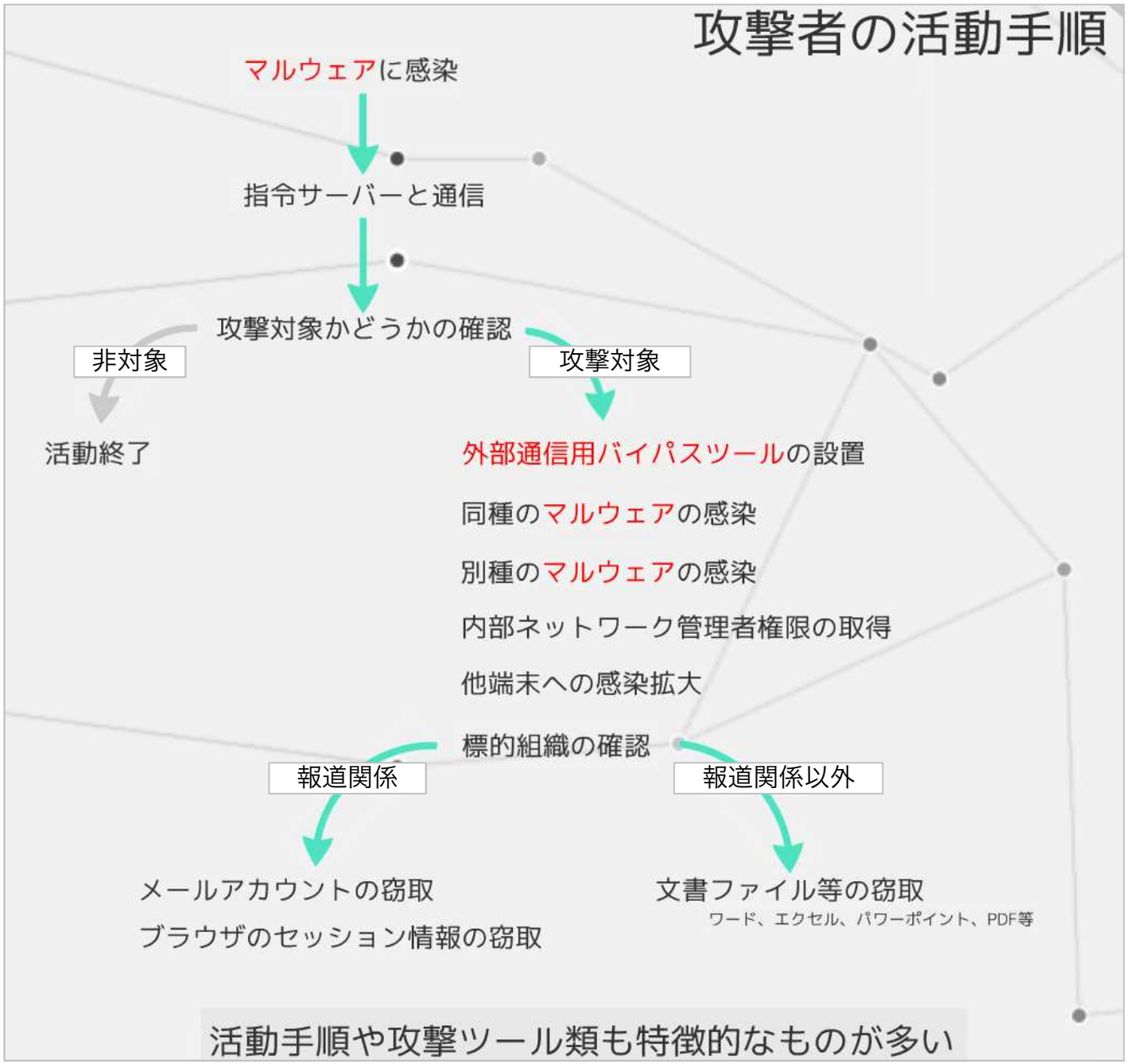
2015年
遂に日本をメインターゲットにしたAPT「BLUE TERMITE」を確認。
本格的な自衛が求められる時代に突入

Blue Termiteで使用されたメールのサンプル



標的型メールに添付された実行形式のファイルと、そこに含まれるマルウェア



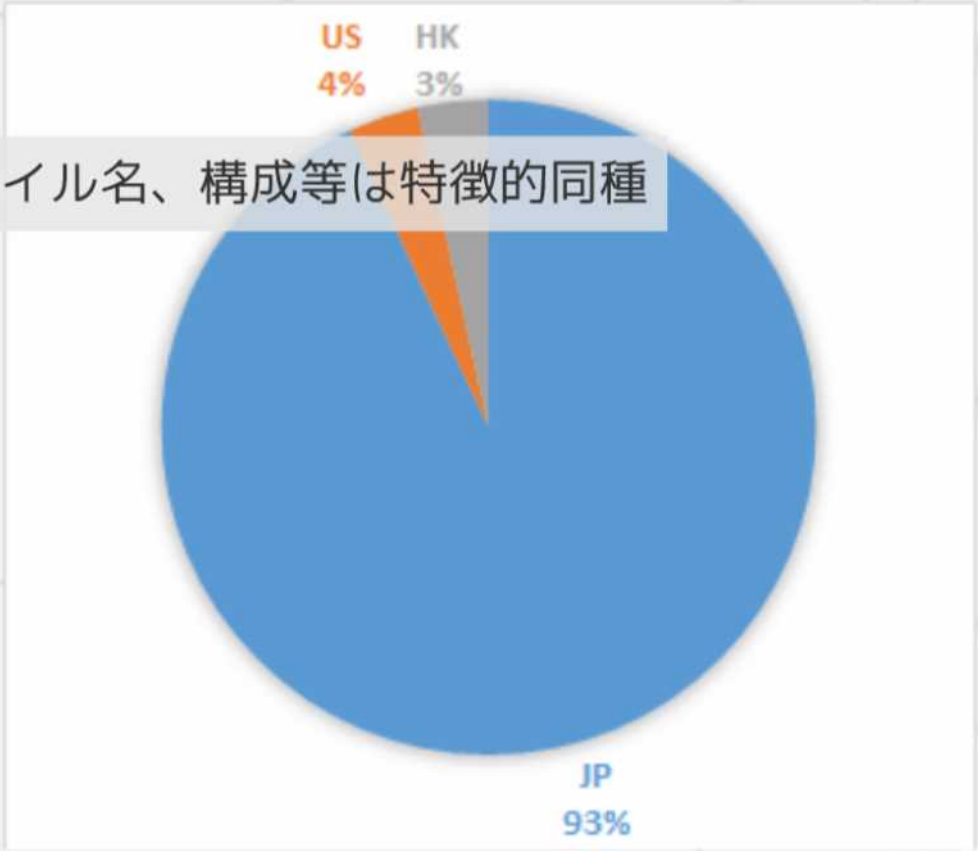


確認されたC2サーバーの実に93%が国内に存在

1 l**********9
2 ha**********i.jp
3 hi**********a.com
4 www.a******c.jp
5 www.a
6 www.a*********n.jp
7 www.a********l.jp

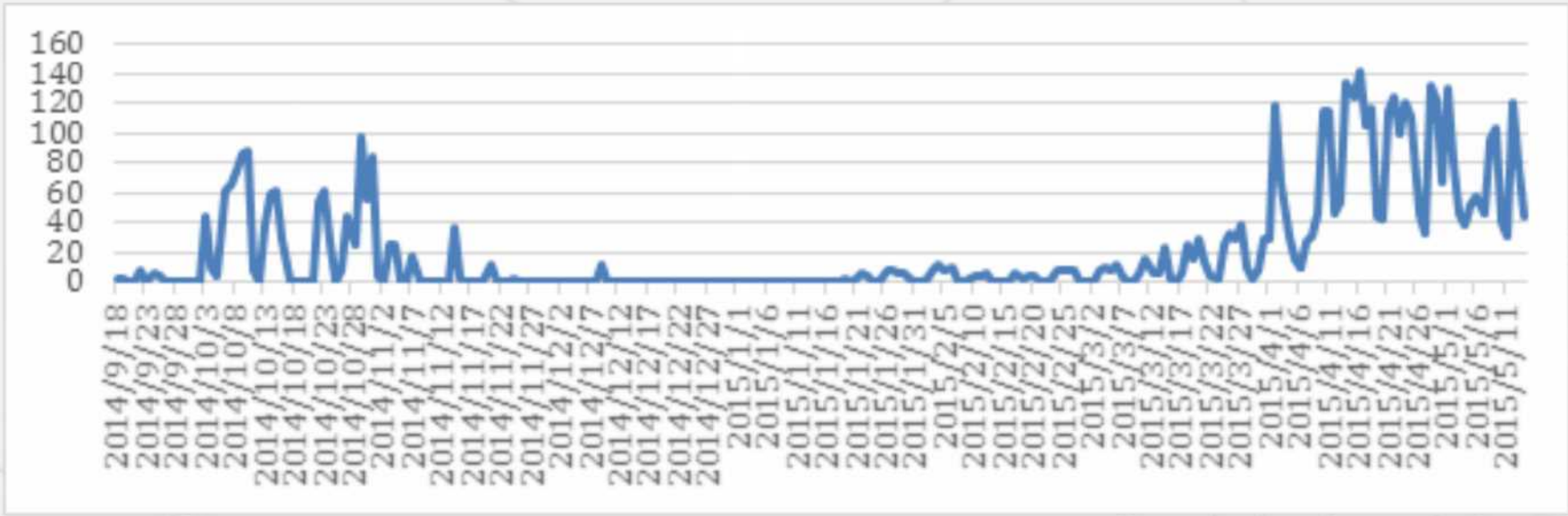
73 www.s********e.jp
74 www.s**********o.jp
75 www.t******n.com
76 www.t*******u.jp
77 www.w********e.jp
78 www.w**********r.jp
79 www.y******o.jp
80 www.y**********t.jp

指令サーバーの機能、ファイル名、構成等は特徴的同種

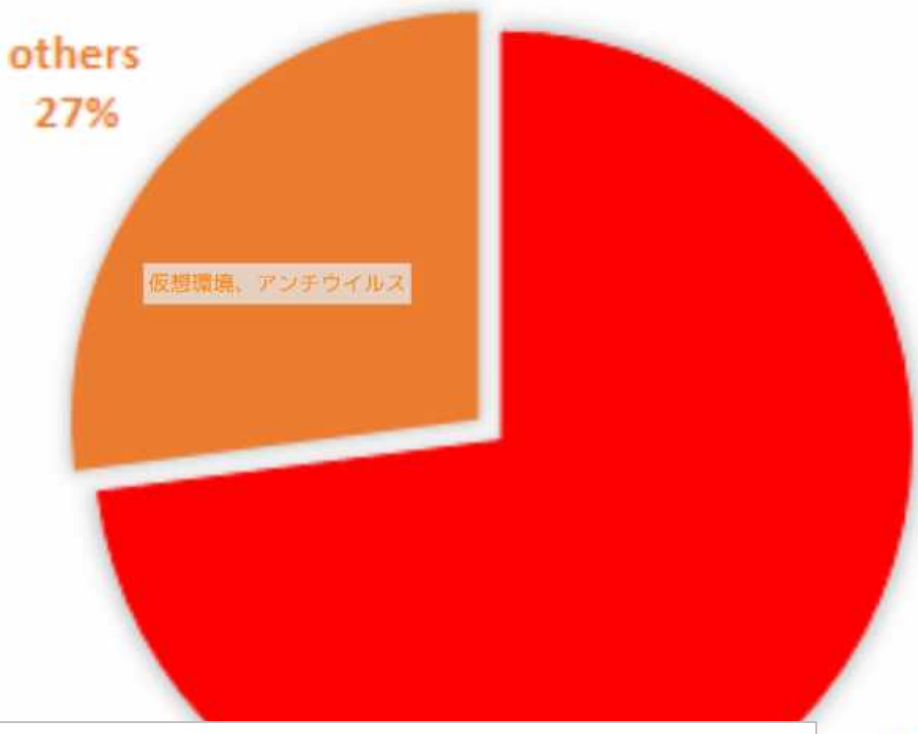


Targets

指令サーバーへの通信数

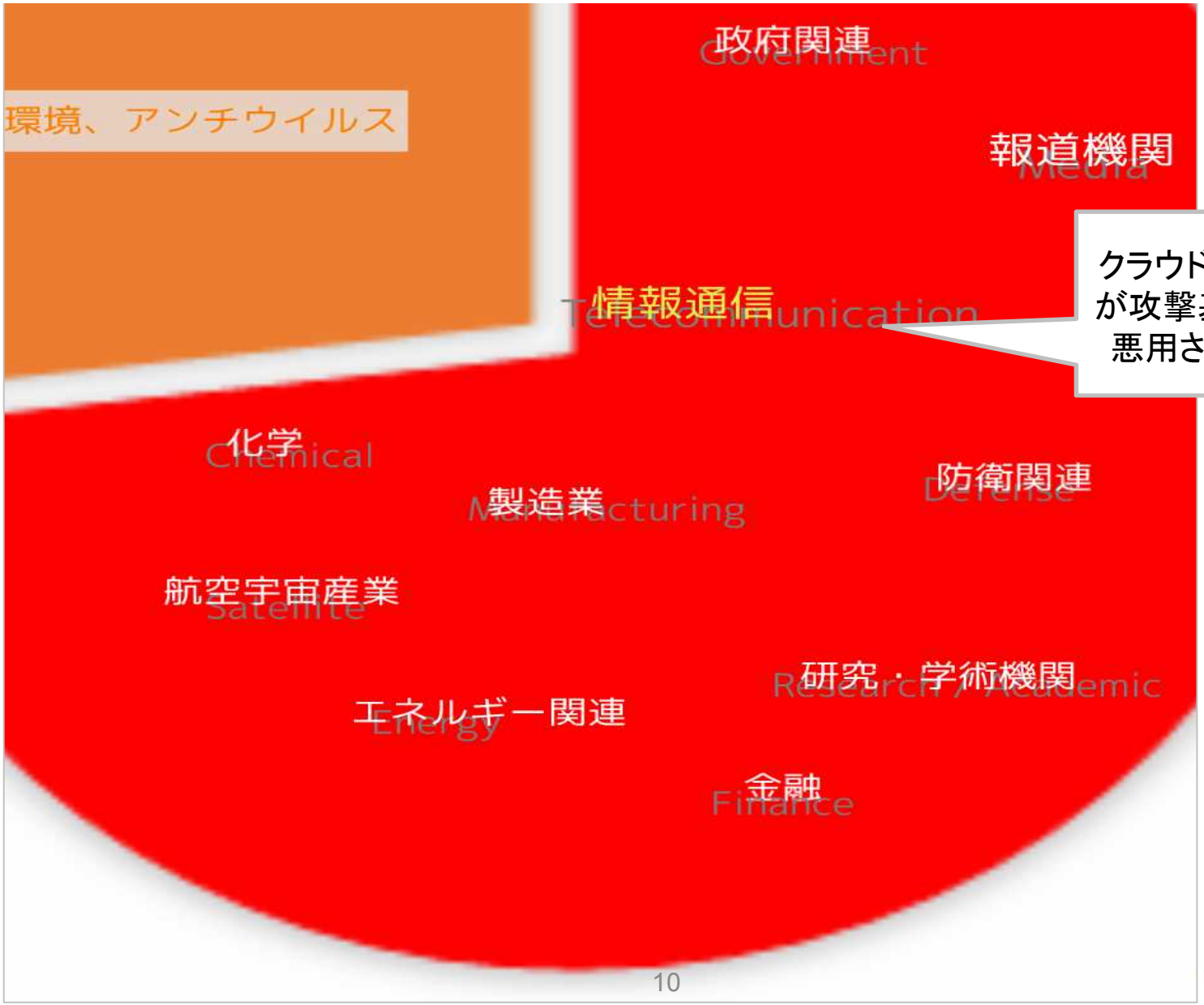


国別IPアドレスの集計



指令サーバーとの通信が確認されたIPアドレスの73%が日本国内に存在。
リサーチ会社やクローラーなどの非感染者を除くとその割合はさらに増大する。

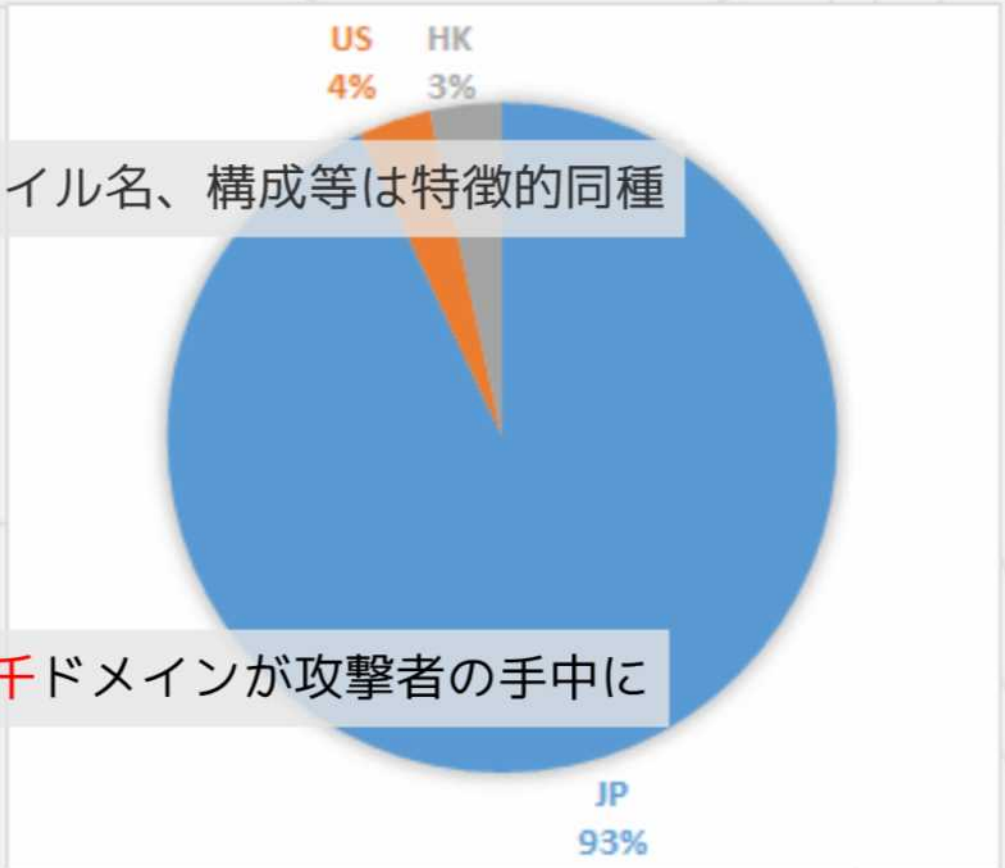
被害は多岐にわたる業種・団体に広がっている



1 l**********9
2 ha**********i.jp
3 hi**********a.com
4 www.a******c.jp
5 www.a
6 www.a*********n.jp
7 www.a********l.jp

73 www.s********e.jp
74 www.s**********o.jp
75 www.t******n.com
76 www.t*******u.jp
77 www.w
78 www.w
79 www.y******o.jp
80 www.y**********t.jp

指令サーバーの機能、ファイル名、構成等は特徴的同種



2015年5月時点で,国内数千ドメインが攻撃者の手中に

THE BLUE TERMITE APT

THIRD TIME ISN'T THE CHARM

マルウェア、指令サーバー、感染後の手順等一連の攻撃である

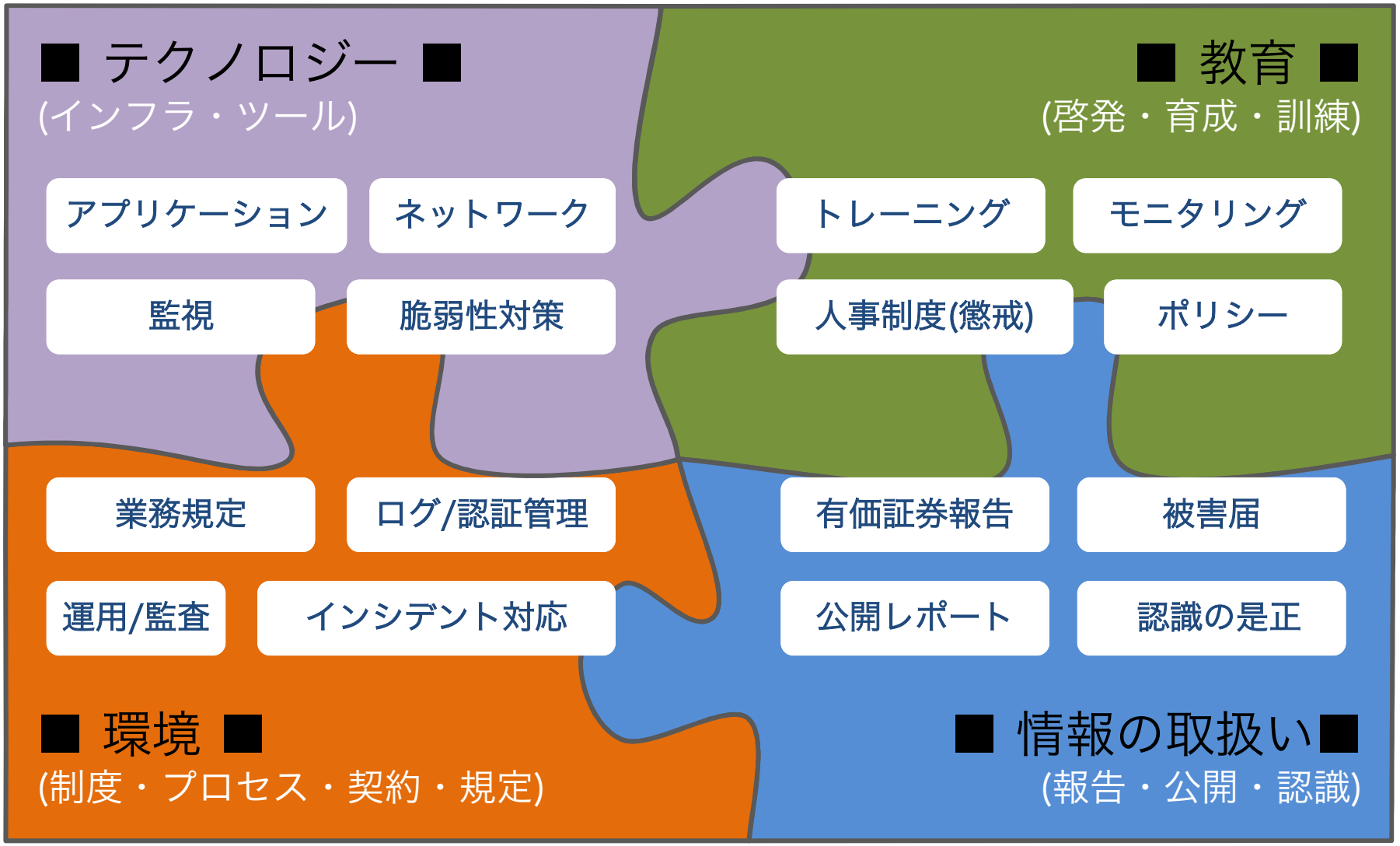
日本国内で様々な組織が標的となり実被害が出ている

日本国内に多数の指令サーバーが設置

二つの疑問

- ウチは大丈夫か？
- どのように立ち向かえばいいのか？

よりよいサイバー対策を実現するために



現状の再確認と認識の是正

- ウチは大丈夫といった、根拠の無い自信を捨てる
- 誰もが標的になる可能性がある事を認識する
- 攻撃を受ける・被害に遭うことは恥では無い
- 攻撃に遭った事実は、次の対策への財産として共有する
- 良かった点は吸収し、非難や揶揄は行わない

テクノロジーの観点からの提言

- 最後の砦であるエンドポイント対策を見直す
- 脆弱性対策を導入する
- メールの設定を見直す
  （.exeはデフォルトで削除ないし隔離）
- セキュリティコンサルティングを実施し、現状の設計/環境/運用の確認と評価

1件のインシデントで発生するコストは
中小企業の平均で $56,000
大企業では $649,000

ウチは大丈夫？ と思ったら

Malware:
leassnp.exe、vmwere.exe、nvsvcv.exe、vmmat.exe、vmat.exe、mdm.exe、vmatap.exe、vmater.exe、upsl.dll、userControl-v80.exe、userControl-v90.exe、userControl-v100.exe

Tools:
ct.exe、yrar.exe、csvde.exe、GetPassword.exe、mimikatz.exe、mimikatzx64.exe

※上記MalwareおよびToolsのプロセス名がタスクリスト上に存在する場合、もしくはMalwareがスタートアップに登録されている場合も感染の可能性がある。

カスペルスキー製品での検知名

Backdoor.Win32.Agent
Backdoor.Win32.Emdivi
Trojan-Downloader.Win32.Agent
Trojan.Win32.Agent
HEUR:Backdoor.Win32.Generic
HEUR:Trojan.Win32.Generic
HackTool.Win32.Agent
HackTool.Win32.Mimikatz.gen
HackTool.Win32.WinCred
HackTool.Win64.Agent
HackTool.Win64.Mimikatz.gen
not-a-virus:PSWTool.Win32.Messen
not-a-virus:PSWTool.Win32.NetPass
not-a-virus:RiskTool.Win32.PwDump
UDS:DangerousObject.Multi.Generic

ホワイトペーパー

APT: 今そこにある脅威
～効果的なAPT対策を実現するために～
www.kaspersky.co.jp

Blue Termite に関するお問い合わせ先（対策・調査）

APT_taisaku@kaspersky.com

ホワイトペーパー

APT: 今そこにある脅威
～効果的なAPT対策を実現するために～

用語解説

- APT ： 明確なターゲットと目的を持った高度で執拗なサイバー攻撃の事であり、ソーシャルエンジニアリングや標的型メール、中間者攻撃、水飲み場攻撃といった技術を駆使し、ターゲットの情報の窃取や妨害、破壊を行う活動を言う。
- Blue Termite ： APT攻撃の名称であり、個別の被害者やマルウェア、事件に限定されるものでは無い。
- C2サーバー ： Command & Control サーバーの略で指令サーバーと訳されることもある。攻撃者が感染者の端末とやりとりをしたり、攻撃用のツール・マルウェア等を配したり、窃取した情報を保管する目的で利用される。
- 標的型メール ： 攻撃者がターゲットへの侵入を目的にマルウェアに感染させるためのメールで、受信者が開封しやすい情報を用いたり、実際にやりとりしている人になりすましたりといった工夫が盛り込まれている。
- エクスプロイト ： サイバー攻撃に多用されるマルウェアの一種でシステムやソフトウェア等の脆弱性を突いてターゲットの端末に攻撃を仕掛ける。