彼を知り己を知り“戦う場所を知れば”百戦殆（危）うからず

– イスラエルの最先端セキュリティ戦略、ソリューションからの学び –

2016年11月16日

株式会社 東陽テクニカ
東陽Security & Labカンパニー
バイスプレジデント
北山　正姿

“はかる”技術で未来を創る 東陽テクニカ

本日の内容

- はじめに
- IT成長の歴史とサイバー対策トレンドの変遷
- なぜIsrael ??
- Israelセキュリティ企業の戦略骨子
- Israelセキュリティ企業からのまなび
- 最後に

“はかる”技術で未来を創る 東陽テクニカ

はじめに

東陽セキュリティ & ラボカンパニー ：概要

本社： 東陽テクニカ

- 本社所在地：東京都中央区八重洲1-1-6
- 設立：昭和28年9月4日
- 資本金：41億5800万円
- 従業員数：450名（2014年9月末時点）
- 上場：東京証券取引所　第一部（コード：8151）

Technology Interface Center
製品トレーニング専用設備

東陽セキュリティ & ラボカンパニー（SLC)概要

- 設立： 平成28年11月1日
- 資本金： 3.5億円
- 従業員数： 14名 （発足時点）

端末無線評価ラボ

東陽SLCミッション

「はかる」サービスでセキュアな社会に貢献する

製品トレーニング

東陽テクニカ：事業内容

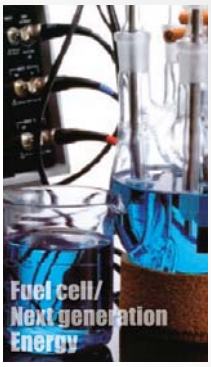
TECHNOLOGY INTERFACE

EMC、アンテナ

情報通信

機械・自動車
計測

理化学計測



ソフトウェア開発

メディカル

TOYO Corporation

技術コンサルティング
統合システム開発
SW 開発
プリ・アフターメンテナンス

マーケティング・情報展開

"はかる"技術で未来を創る 東陽テクニカ

東陽セキュリティ＆ラボカンパニー：Mission

「はかる」サービスでセキュアな社会に貢献する

【人】高度技術と双方向リアルタイムコミュニケーション力を持つ信頼のサービスプロバイダ

【製品】海外最先端パートナと連携し高度ノウハウにより特色あるサービスを提供

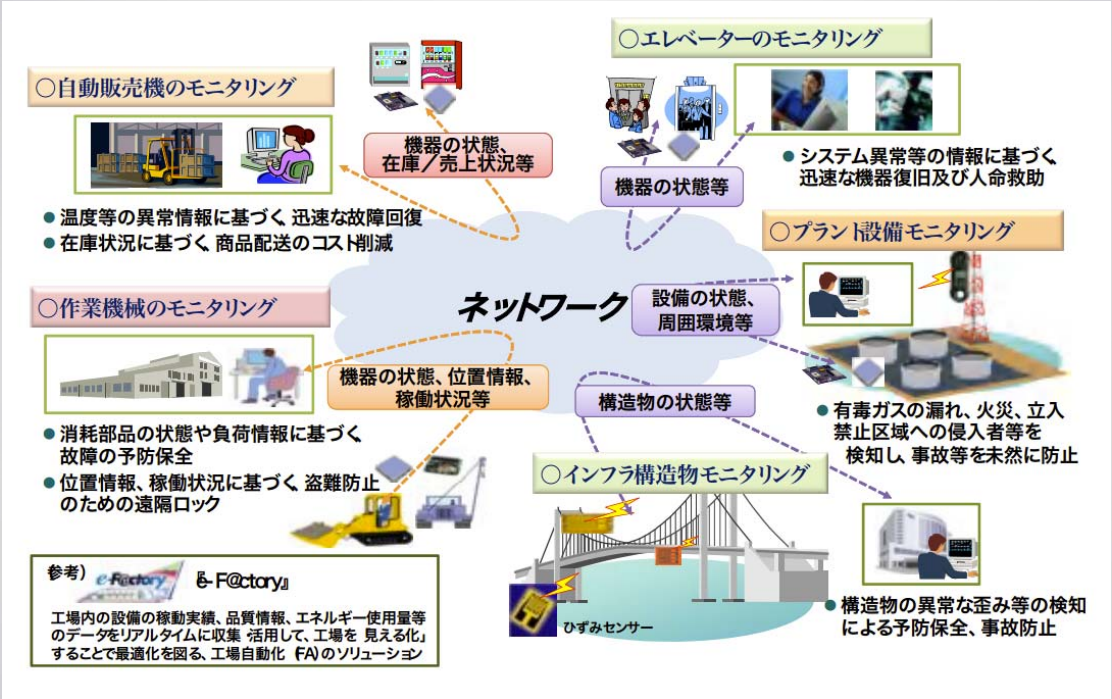
【利益】最先端のクラウドインフラにより高効率・高品質なサービスを提供し規模と利益の最大化を実現する

東陽テクニカの持つ"はかる"企業としての実績
- 第三者 独立かつ公正な評価、監査、相談パートナ
- 広範囲な海外パートナネットワーク
- 真摯に対応する技術者集団

"はかる"技術で未来を創る 東陽テクニカ

東陽セキュリティ＆ラボカンパニー：市場

サイバーセキュリティ、IoT無線通信端末の性能担保が最重要課題



東陽セキュリティ＆ラボカンパニー：事業内容

東陽セキュリティ＆ラボカンパニー

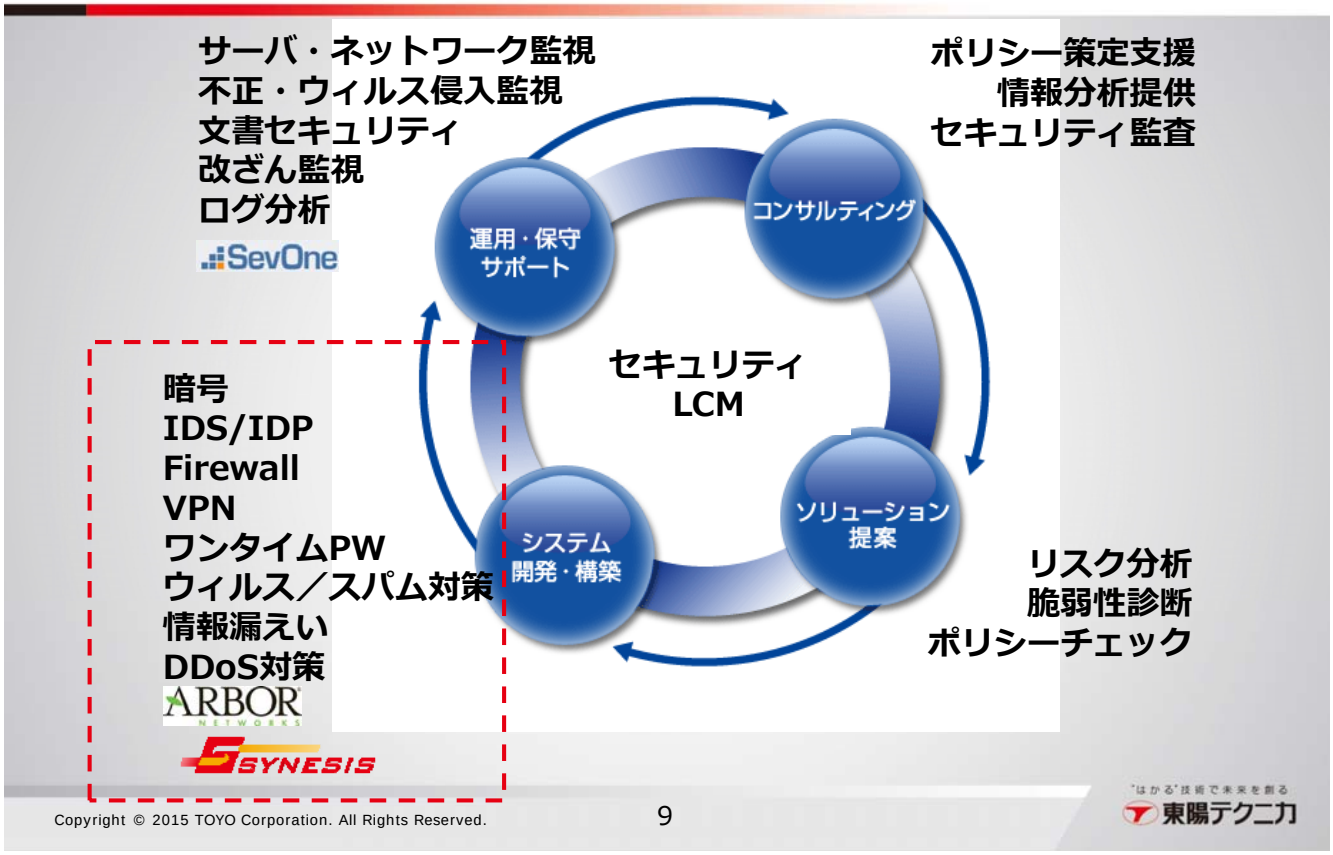
セキュリティ ビジネスユニット

- リスク分析： Penetration Test、リスク査定、脆弱性診断
- 情報インテリジェンス：DarkNET、マルウェア / ブロックlist
- CRAラボ： 分析レポート、SOC as a Service

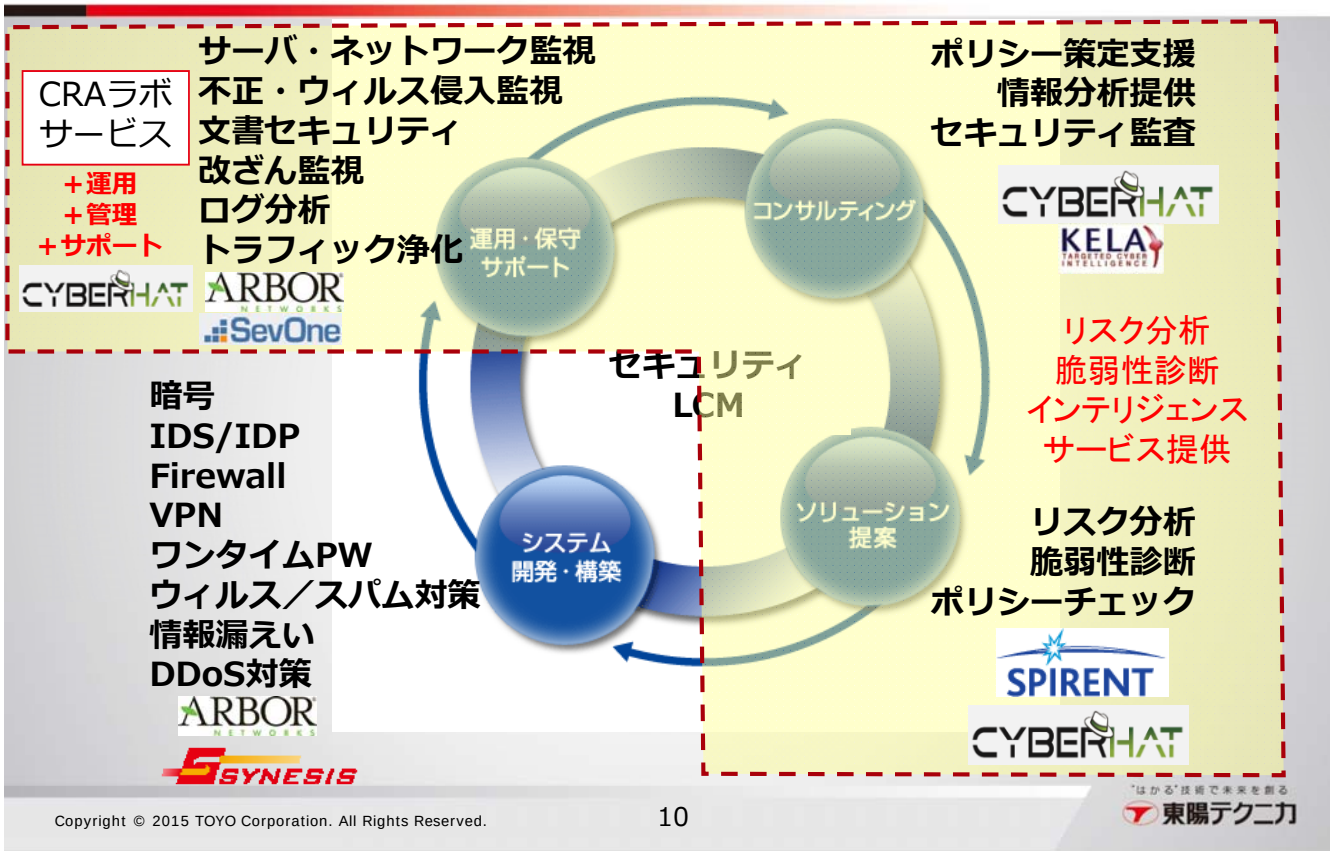
ラボサービス ビジネスユニット

- 無線キャリア：Docomo/AT&T/Telefonica認定ラボサービス
- 国際規格試験：CE、電波法、業界規格（携帯、WiFi、近距離）
- 認定サポート：世界200カ国以上の型式認証、アプリケーション

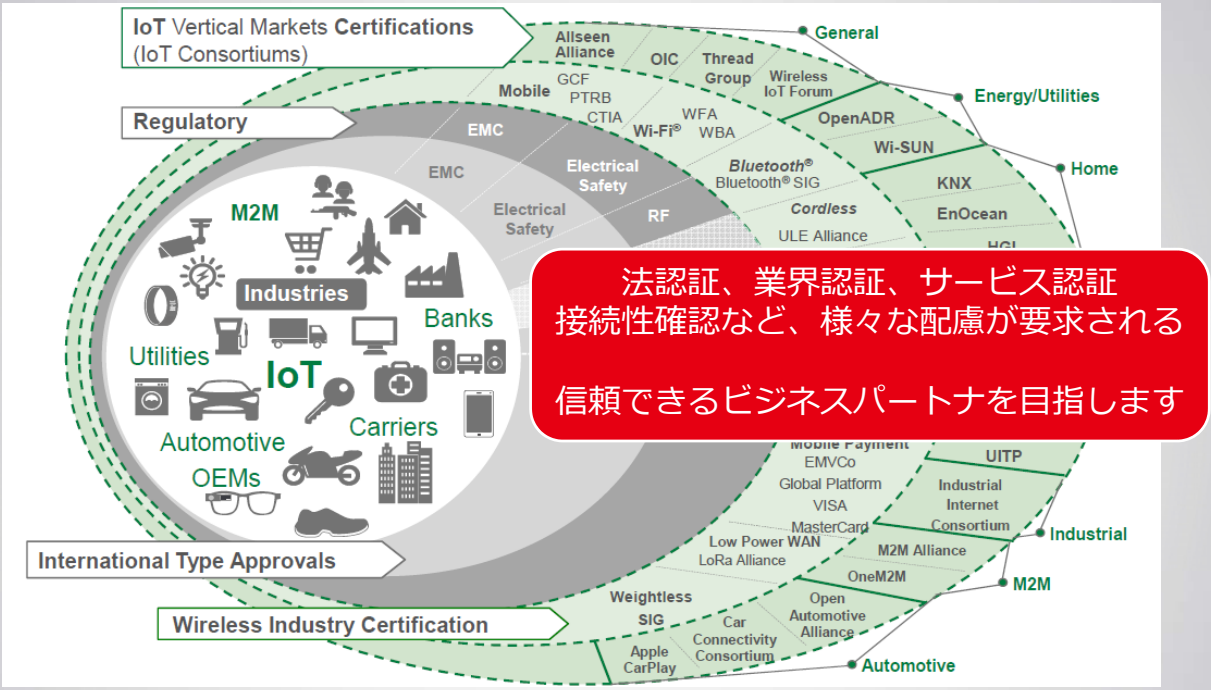
東陽セキュリティ物販事業： 従来



東陽SLC セキュリティBU：
リスク確認試験サービスからオペレーションまで



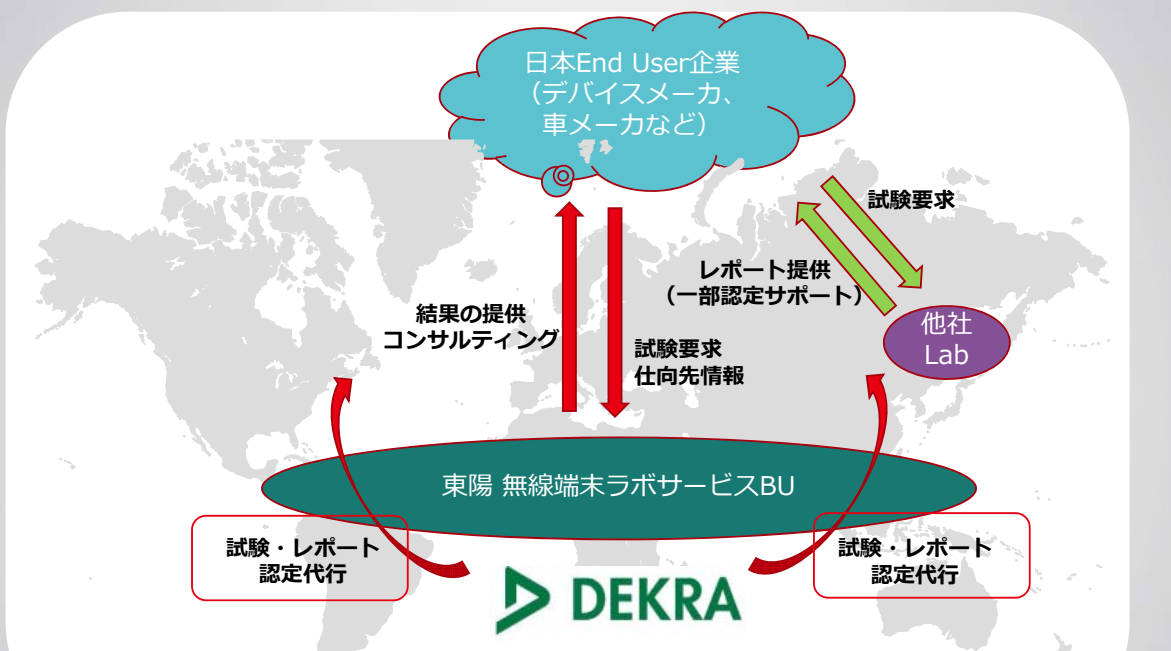
東陽SLC ラボサービスBU：
IoT ／ 無線通信デバイス向け認証サービス



法認証、業界認証、サービス認証
接続性確認など、様々な配慮が要求される

信頼できるビジネスパートナを目指します

東陽SLC ラボサービスBU：
無線規格強制試験から国家強制機関への申請まで



ラボ試験から認定申請までOne Stopでサービス
日々変更される規制・規格に確実に追従できるパートナとして

IT成長の歴史とサイバー対策トレンドの変遷

ITの歴史とサイバー対策トレンドの変遷

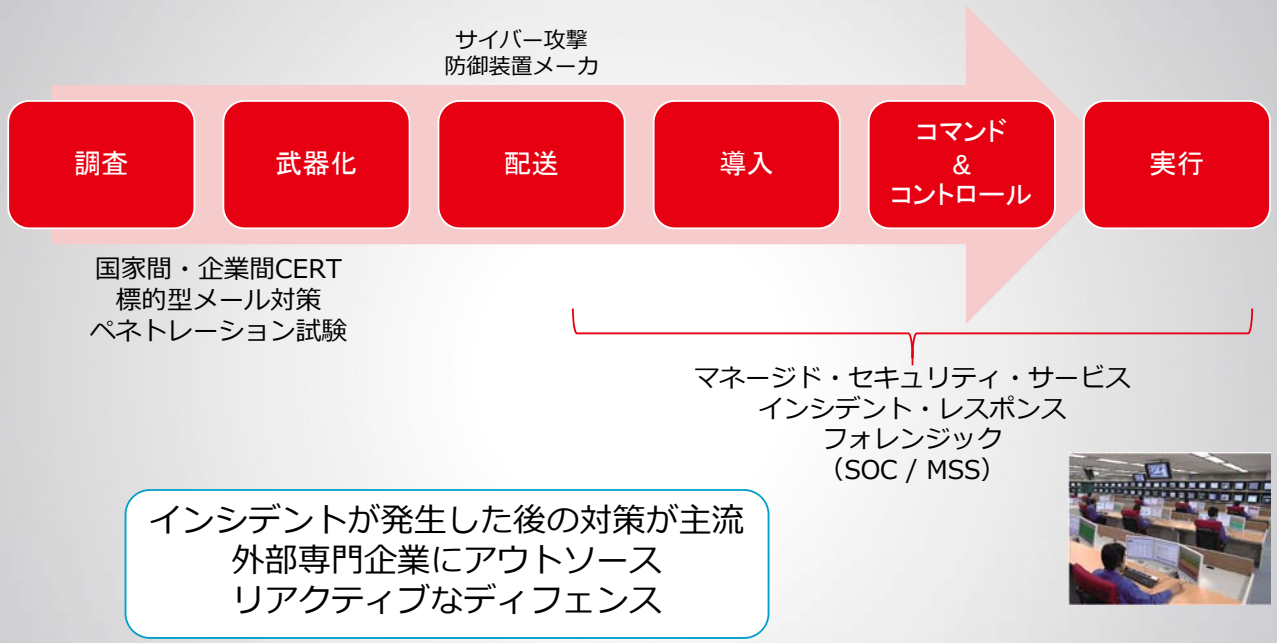
2020年代			
2010年代	すべてがOn-line End to End Encryption スマートフォン	敵対政府 テロリスト ハクティビスト 犯罪組織 自分自身	不正情報搾取対策（UTM、標的型攻撃対策） インシデント情報管理（SIEM） 情報漏えい対策（フォレンジック） 明日はわが身（国家間、企業間CERT活動）
2000年代	携帯データ通信 Webコマース DDoS	敵対政府 テロリスト ハクティビスト 犯罪組織	上位アプリの保護（WAF） マルウェア対策（サンドボックス）
1990年代	Windows 95 NWインフラの脅威認識 コンピュータウイルス	愉快犯 競合企業 （Cyber Criminal）	境界防御（FW、IDS、VPN） PC端末保護（ウイルスSW）
1980年代	TCP/IP標準化 DoD TCSEC	腕試し	正しい設定 パッチ
1970年代	ARPAネット	想定外	ー
	Topics	攻撃者	代表的対策

顕在化したさまざまな悩み

- イタチごっこ
  - 防御にどれだけ努力・費用をかけても、攻撃者の方がすぐに新しい手法を見つけてしまって終わりが見えない。
- セキュリティ人材の不足
  - 機材は揃えても、それを最大限運用し活かすことができない。
- 管理、対応範囲が拡大中
  - 今まで管理していなかった事まで、管理する必要が出てきた。
- 攻撃者の心理
  - 対応をしている事を下手に自慢すると、すぐに攻撃者がやってくる。

攻める側と、守る側の経済的、倫理的
非対称性が問題原因

2016年現在のセキュリティ対策



インシデントが発生した後の対策が主流
外部専門企業にアウトソース
リアクティブなディフェンス

当社SLC セキュリティBU ：重点領域

1) 攻撃予兆監視・インテリジェンス
（イスラエルパートナ連携）

2) 脆弱性診断・侵入試験・リスク査定
（Spirent / CyberHat社連携）

3) トラフィック浄化サービス
（Arbor連携）

4) SOC as a Service
（CyberHat社連携）

攻撃者の狙い（場所、時期、手法）や
攻撃予兆を捕まえ、未然に防ぐ
プロアクティブなディフェンス

当社SLC セキュリティBU ：今後の挑戦

1) サイバーインテリジェンス
（イスラエルパートナ連携）

2) 脆弱性診断・侵入試験・リスク査定
（Spirent / CyberHat社連携）

3)トラフィック浄化サービス
（Arbor連携）

4) SOC as a Service
（CyberHat社連携）

マネージド・セキュリティ・サービス
インシデント・レスポンス
フォレンジック
（SOC / MSS）

拡張・準備中

東陽CRAラボ
（サイバーリスク分析ラボ）

なぜIsrael ???

日経新聞記事より： 2016年9月2日版

真相深層 五輪防衛、イスラエルの傘
サイバーテロ対策で年内にも覚書

2016/9/21付 | 日本経済新聞 朝刊

保存 印刷 その他

日本政府は年内にもサイバーセキュリティー強化のため、イスラエルと技術協力の覚書を交わす。2020年の東京五輪へ向け重要インフラの防御を固める狙いだ。軍事力の強化を図るイスラエルが最近力を入れるのがサイバー分野。五輪などを足場に日本や世界へ売り込む思惑がある。

イスラエル南部のベエルシェバ。旧約聖書ゆかりの地で、数年前まで遊牧民が羊を追う姿が目立ったのどかな町が今、大きく変容し始めている。


画像の拡大
IT特区「サイバースパーク」


画像の拡大
サイバー協力はネタニヤフ首相との14年の首脳会談から始まった＝ロイター

「軍産学が融合」

同国政府は2年前、理工系に強いベングリオン大学の敷地に「サイバースパーク」と名付けたIT特区を設けた。政府や軍、国際企業を集め、サイバー技術開発の戦略拠点にするためだ。近代的なビルにはドイツテレコムなどが入居。軍の技術者部隊もテルアビブ周辺から移動しつつある。

「軍産学が融合し、有能な人材が集まる場になってきた」。イスラエルの元空軍准将で、米防衛関連企業ライドスホールディングスの現法トップ、S・ゴットマン氏は語る。ライドスは8月、イスラエルに調査研究施設を持つロッキード・マーチンの情報システム部門を買収した。狙いはサイバー分野の優秀な人材だ。

長くアラブ諸国との戦闘やテロに直面してきたイスラエルは軍事技術の開発に注力してきた。ただ、主戦場は近年サイバー空間に移っており、1日で万単位の攻撃を受けるという。そのため高校時代の数学の成績優秀者らを登用した「8200」という情報機関を技術開発の母体に、技術力の強化を急いでいる。

日経新聞記事より： 2016年9月2日版 つづき

サイバー関連技術は今や世界の先端を行く。

2010年ごろ、イランの核施設をまひさせるサイバー攻撃が起きた。米国家安全保障局とU8200が共作したとされるウイルスが使われた。あるイスラエル軍OBは「防衛に優れるのは攻撃の経験があるためだ」と打ち明ける。

イスラエルではゴットマン氏のように軍で得た経験や人脈を生かし、産業界に転じる人も多い。それがサイバー防衛産業の躍進を支えている。

その一つ「イリュージブネットワークス」はハッカーを幻惑する対策ソフトを開発した。ニセのサーバーへのログイン情報や閲覧履歴を顧客企業のシステムに埋め込む。戸惑うハッカーの動きを検知・記録し、システム遮断など対策をとる。

同社をつくったのは、U8200出身の3人組。企業を欺くハッカーを逆に欺く――。テロや戦闘に直面する非情な環境で生まれた発想を感じさせる技術だ。

そんなイスラエル企業には世界が注目する。不正ソフトへの対応ソフトを開発した「サイアクティブ」は昨年、米電子決済大手のペイパルが買収し、同社のハッカー対策の司令塔になった。

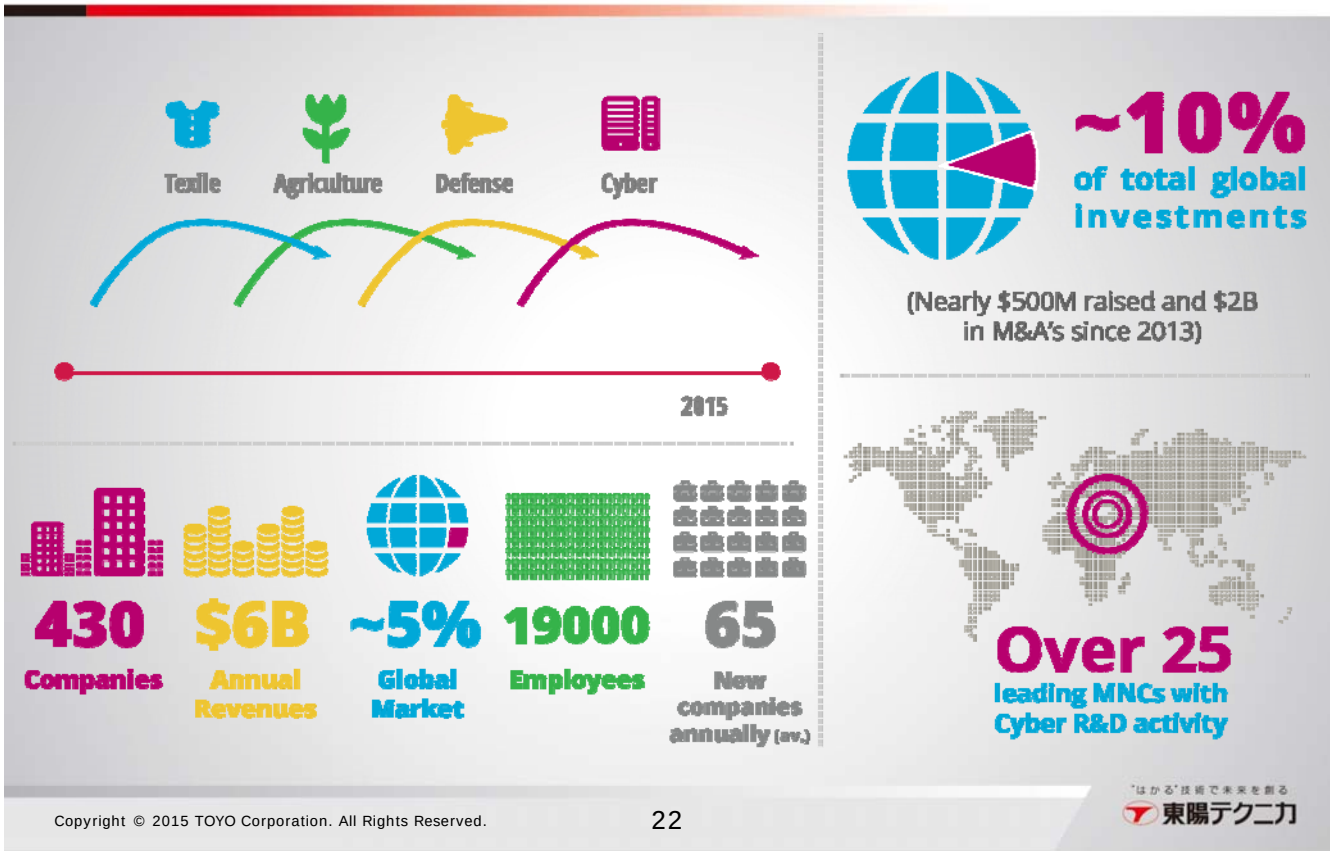
リオでお墨付き

15年にイスラエルの先端技術分野に投資された額は45億ドル。09年から7年連続で増えているが、特に15年は2年前の倍増の勢いだった。サイバー分野が伸びた14、15年は8～9割を外資が占めており、欧米が多いがアジアも増えつつある。

イスラエル政府はサイバー防衛技術の今後の輸出先や投資パートナーを探す地域として、「欧州の割合が減る中、日本やアジアを増やす」（O・コーエン経済省対外貿易局長）と強調する。

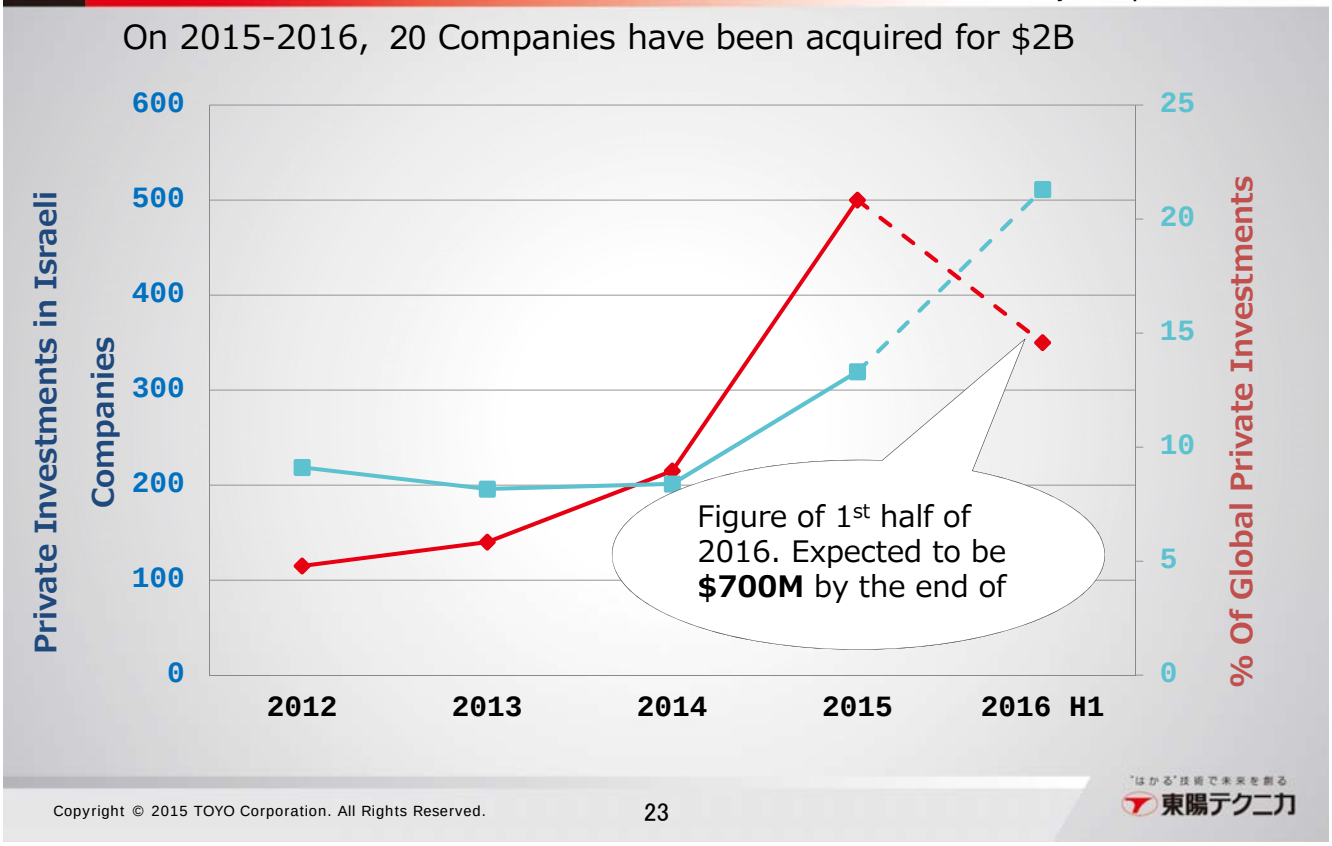
5日来日したIT特区「サイバースパーク」のR・ゼハビ最高経営責任者（CEO）も「イスラエル企業はリオ五輪でサイバー防衛対策を請け負った」と説明。東京五輪へ向けサイバー対策が重要課題の日本を魅力的な市場ととらえ、「喜んで協力したい」と語る。

Israelサイバーセキュリティ市場環境



イスラエル サイバーセキュリティ産業に対する投資額

CyberSpark,Roniより



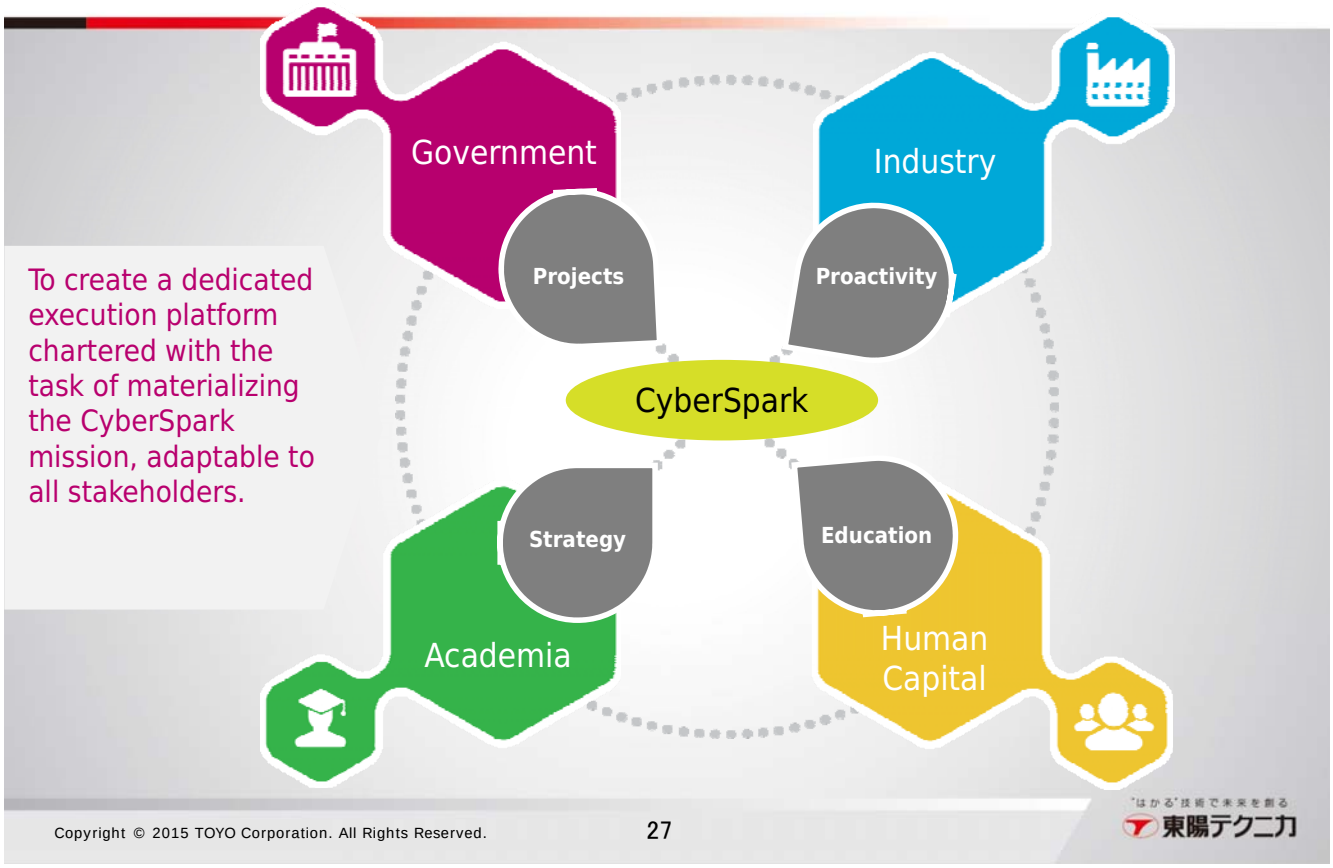
Be'er Sheva

cyberspark
ISRAELI CYBER INNOVATION ARENA

Cyber Security Park

ちなみに： Roni Zahavi

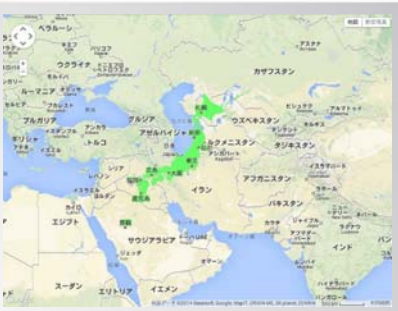
CyberSpark設立＆存在理由



To create a dedicated execution platform chartered with the task of materializing the CyberSpark mission, adaptable to all stakeholders.

なぜIsrael ???

- 常に戦時中 （残念ながら）
- 国土が小さい （日本の四国程度）
- 徴兵制
- セキュリティ教育（U8200）
- SERT-IL
- ベンチャ



Israelセキュリティ企業の戦略骨子
プロアクティブなDefense

Cyber Kill Chain：“防衛”コンセプト

彼を知り[1] 己を知れ[2]ば　　孫子：謀攻
百戦殆(危)うからず

- 彼：　Attacker / Hacker / 受益者
- 知る[1]：　心理、ふるまい、プロセス、目的
- 己：　自社、情報、従業員、名声（ブランド）
- 知る[2]：　リソース、価値、守るべきもの

Cyber Kill Chainは占領のStrategy !!
Processの1か所を止める事で、被害の拡大、浸透を止める事ができる

サイバー攻撃対策コンセプト：Cyber Kill Chain

Reconnaissance（偵察）	ターゲット、ターゲットの環境、ソフトウェアミックス、慣習およびソフトウェアのLoadoutなどについて公開情報から研究
Weaponization（兵器化）	攻撃が成功させる為に、バックドアと制圧計画を準備
Delivery（配信）	攻撃を開始し、バックドアを注入
Exploitation（悪用）	バックドアに攻撃開始命令を発行
Installation（インストール、浸透）	ブートストラップとしてのバックドア、およびとりうる限りの追加のリモートアクセスツールを混入
Command and Control（コマンドおよび制御）	リモートアクセスを確立ツールを利用
Actions on Objectives（目的行動）	情報を収集し、必要な情報を抜き取るもしくはターゲットに対して更なるアクションをこうじる

Kill Chainの“どこか”のプロセスを切り取る事で、被害の拡大を防ぐ!!

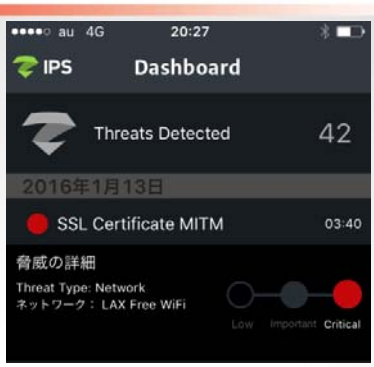
Cyber Kill Chain： 代表的攻撃プロセス

Cyber Kill Chain 実例： モバイルアタック

Reconnaissance(調査)

ARPプロトコルを用いた
IPサーチと空きポートのサーチ

Terranera Resort HotelのWiFi



Delivery (配信)
偽のSSL認証を用いた中間者攻撃
Lax Free WiFi

Exploitation (悪用)
外部C&Cとの設立を確立
Kernel ExploitからOS Exploit

Action on Target (目的行動)
個人データ搾取
盗聴、写真の流出、不正サイトへの接続

Delivery (配信)
不正APRを使った中間者攻撃
（デモンストレーション）

Zimperium
zIPS参照

Israel 最先端セキュリティ企業からのまなび 1
– 敵の視点・インテリジェンス –

Threat Intelligenceとは

- Stop attacks before they knocking on your door
- Proactive approach
- Managed costs – smart perimeter defense
- Brand protection
- Remediate corporate vulnerabilities
- ...

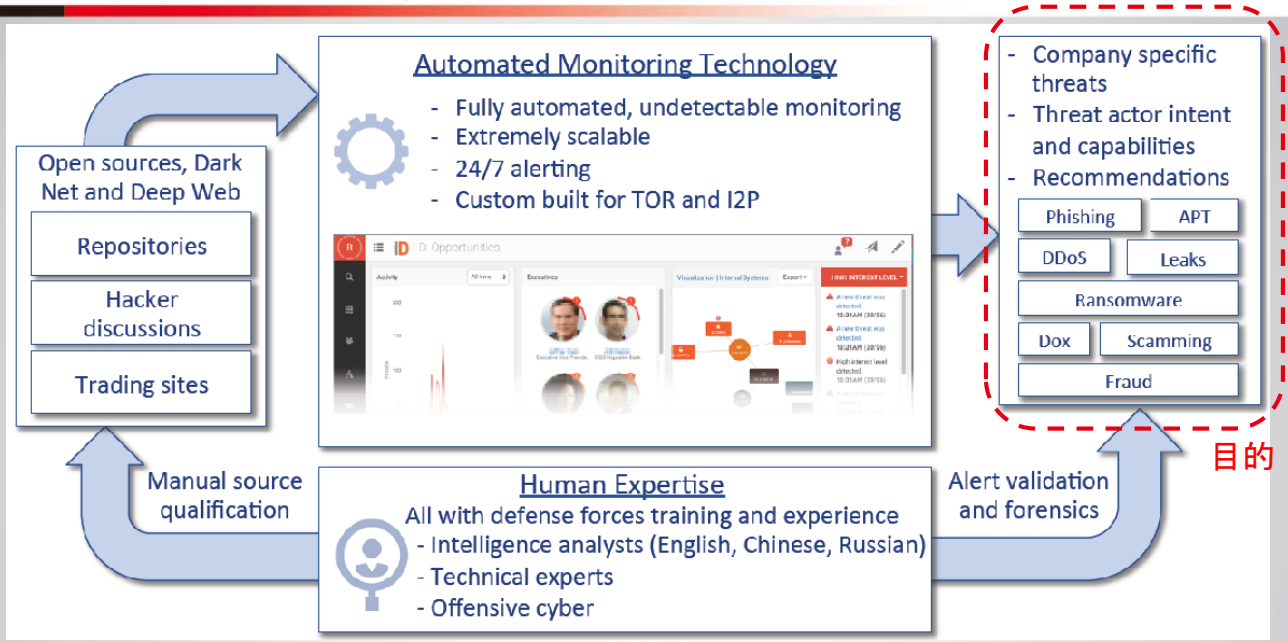
By 2018, 60% of large enterprises globally will utilize commercial threat intelligence services (Gartner - "Security and Risk Management Scenario Planning, 2020")

インテリジェンスの必要性

"外部から（サイバー攻撃者）の視点"で、攻撃者の思考、手口、攻撃（調査フェーズで）を理解する

- What：従業員、資格情報、企業情報、個人情報、クレジットカード、銀行口座…
- Who： ブランド、Cレベル、クライアント、IP
- When： 日時 （厳密なスレッシュホルドを設定する事で事前に）
- How: 脆弱性、攻撃ベクトル

Israelセキュリティ企業からのまなび 1
Threat Intelligence



【 まなび 】

- 実践での情報分析能力が必要
- クラッカーの会話を収集しても不審に思われないデコイ能力

Israel 最先端セキュリティ企業からのまなび 2
– オフェンシブ / プロアクティブ –

セキュリティリスク査定＋Gap分析

- 攻撃者視点での侵入検査
  - ソーシャルエンジニアリング（Email、なりすまし）
  - マルウェア挿入
  - 最新手法のフィッシング攻撃 (インターネット or 無線網経由)
  - 防御装置の出し抜き、侵入
  - 分離されたネットワークを不正に結合
  - インフラ構造、設置の論理的弱点＆問題点を洗い出す
  - 外部 Dark web情報からの抽出、デコード、バイパス、“暗号解読"

- 現行のNW装置の設定および、セキュリティオペレーションの強度を診断
- 脆弱性だけでなく、緊急度・重要度の査定
- 解決法の提案

ネットワークのセキュリティ強度のチェックだけでなく
クライアントの“企業活動”のコアとなる情報＆アセット自体の
セキュリティ強度を監査

CDOC:
Cyber Defense Operation Center

Hacking and Forensics | Intelligence | Professional Service | Monitoring

- サイバーインテリジェンス
- ペネトレーション試験
- 標的型攻撃シミュレーション
- データフォレンジックス
- インシデントレスポンス
- セキュリティ監査・リスク査定
- 教育

CDOC
SOC as a Service

CDOC:
Cyber Defense Operation Center

CYBERHAT

Hacking and Forensics | Intelligence | Professional Service | Monitoring

- セキュリティオペレーション
  - SEIM等経由でのリモートモニタリング
- NW機器の設定変更アドバイス
- サーバ、PCなどのアクセスポリシー
- Operatorの教育、OJT
- インシデント発生時の対策アドバイス

Call centerから真のSOC as a Serviceへ

Israelセキュリティ企業からのまなび 2
プロアクティブな防衛

CYBERHAT

- 防衛すべきものをしっかり定義
  - 企業活動をささえる/ゆるがすコアな“アセット”
- 最適な運用をする事で、リスクを軽減
  - ネットワーク装置、アーキテクチュア、分離
  - セキュリティ装置、SEIMなどのDashboard
  - ポリシー設定、Privileges
  - リテラシー＆意識向上のための教育
- 最適化する事で、セキュリティAlertの無限地獄からの開放
  - クライアントの組織、NW、運用、運営

セキュリティアラートの洪水は、真に深刻な問題・攻撃を隠す
Noiseを軽減する事は、セキュアな環境を守るための一歩

Israel 最先端セキュリティ企業からのまなび 3
– ルートの可視化 –

中間者攻撃

ルートハイジャック

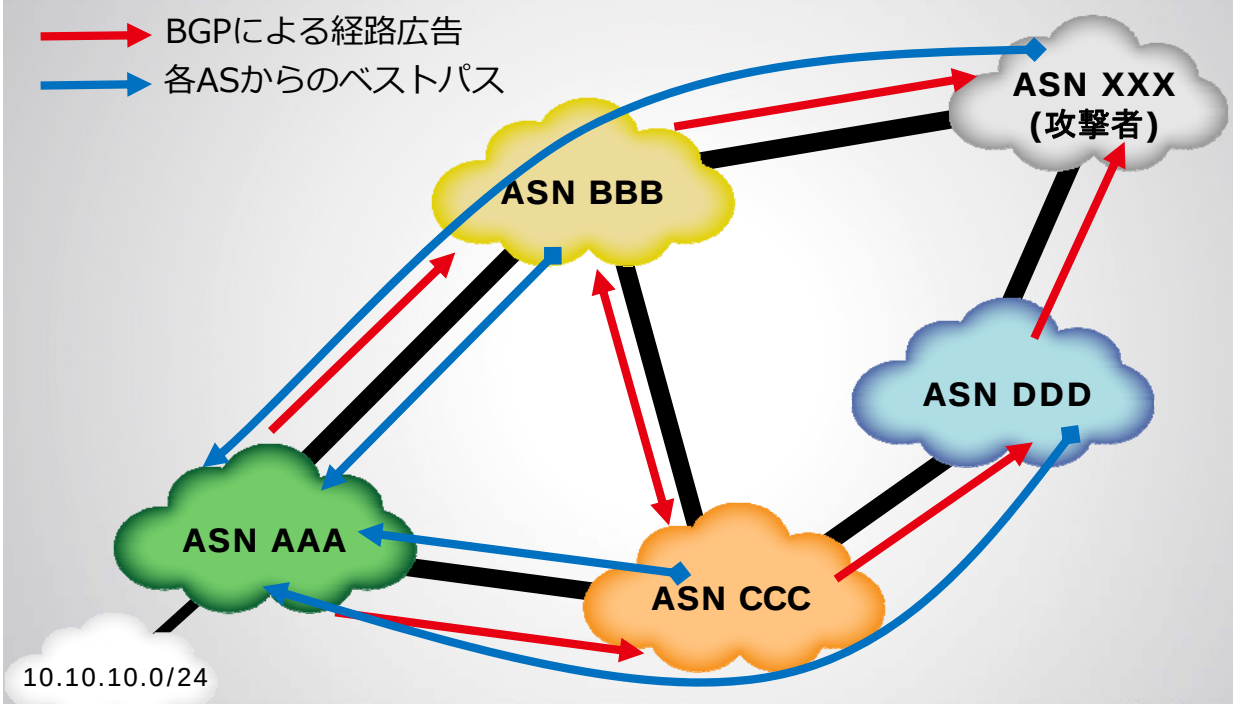
- BGPのプロトコル上の特性を利用
  - 最長一致（Longest Match）の法則
    - 宛先経路をより特定できるパスを選択（手紙と同じ）
  - ASループ回避(AS Loop　Prevention)
    - ASパス属性に自身のASが含まれる経路は破棄
- ハイジャッカー(攻撃者)は証拠を隠蔽
  - 攻撃者のルータを隠蔽
    - TTLの調整(Traceroute対策)

ルートハイジャックの例①

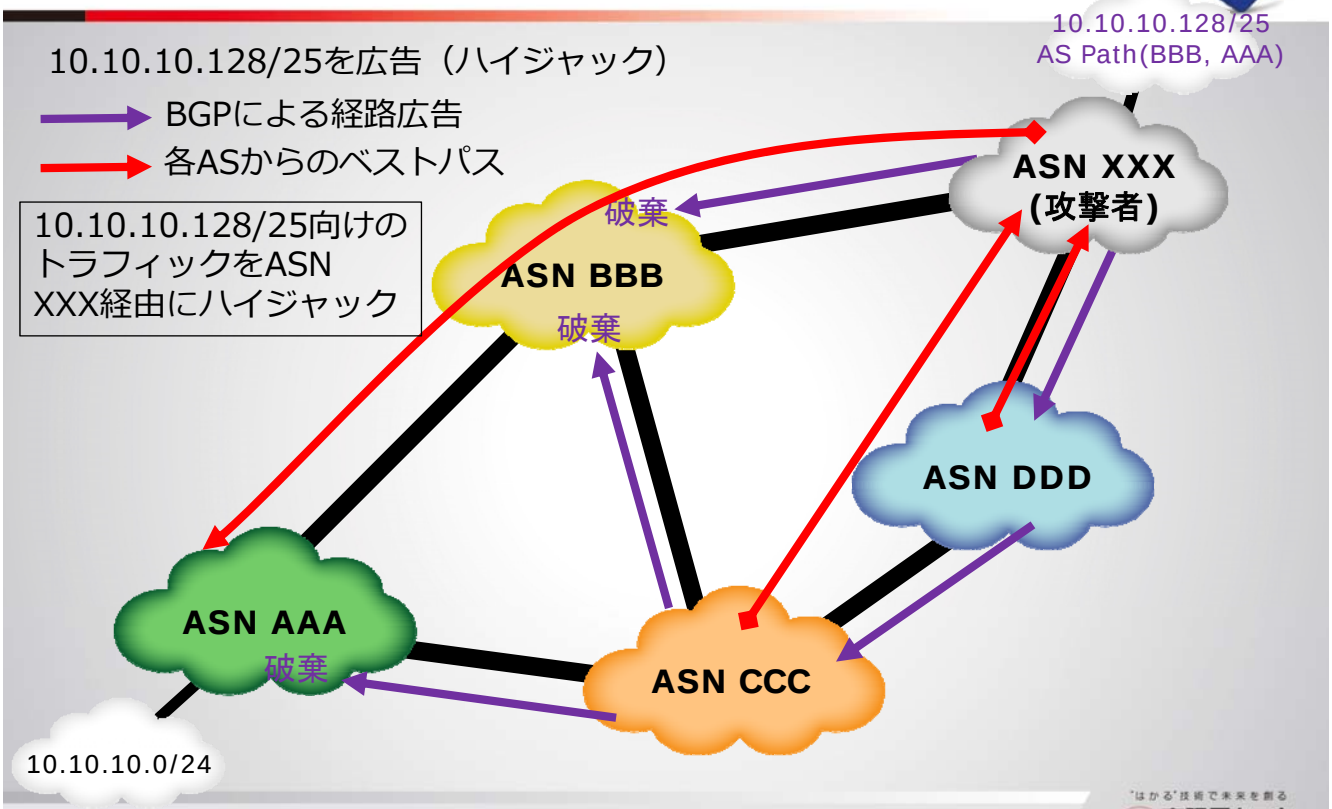
10.10.10.0/24への通信

BGPによる経路広告

各ASからのベストパス



ルートハイジャックの例②



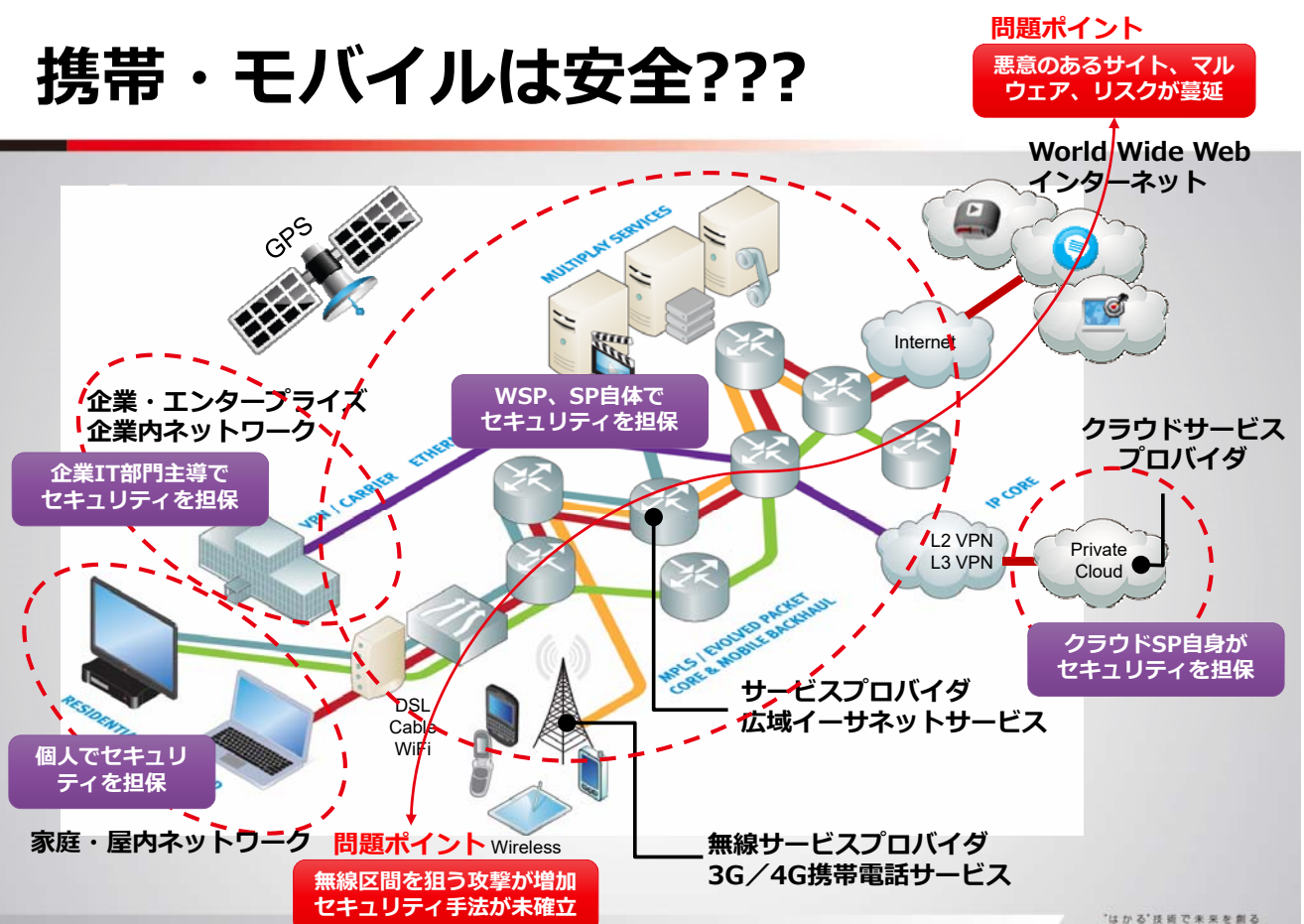
Israel 最先端セキュリティ企業からのまなび 3
– ルートの可視化 –

- ルートが捻じ曲げられた時とその期間
  - どのセッションが盗聴された可能性があるかを特定
- 曲げられた場所
  - 各種ASの物理的な場所データを保有
  - ロケーションを知る事でPoliticalな攻撃の可能性を示唆
- 対策方法を検討できる
  - ASを管理しているキャリアに連絡
  - 重要な情報であるならば、別のルートでのやりとりを検討する

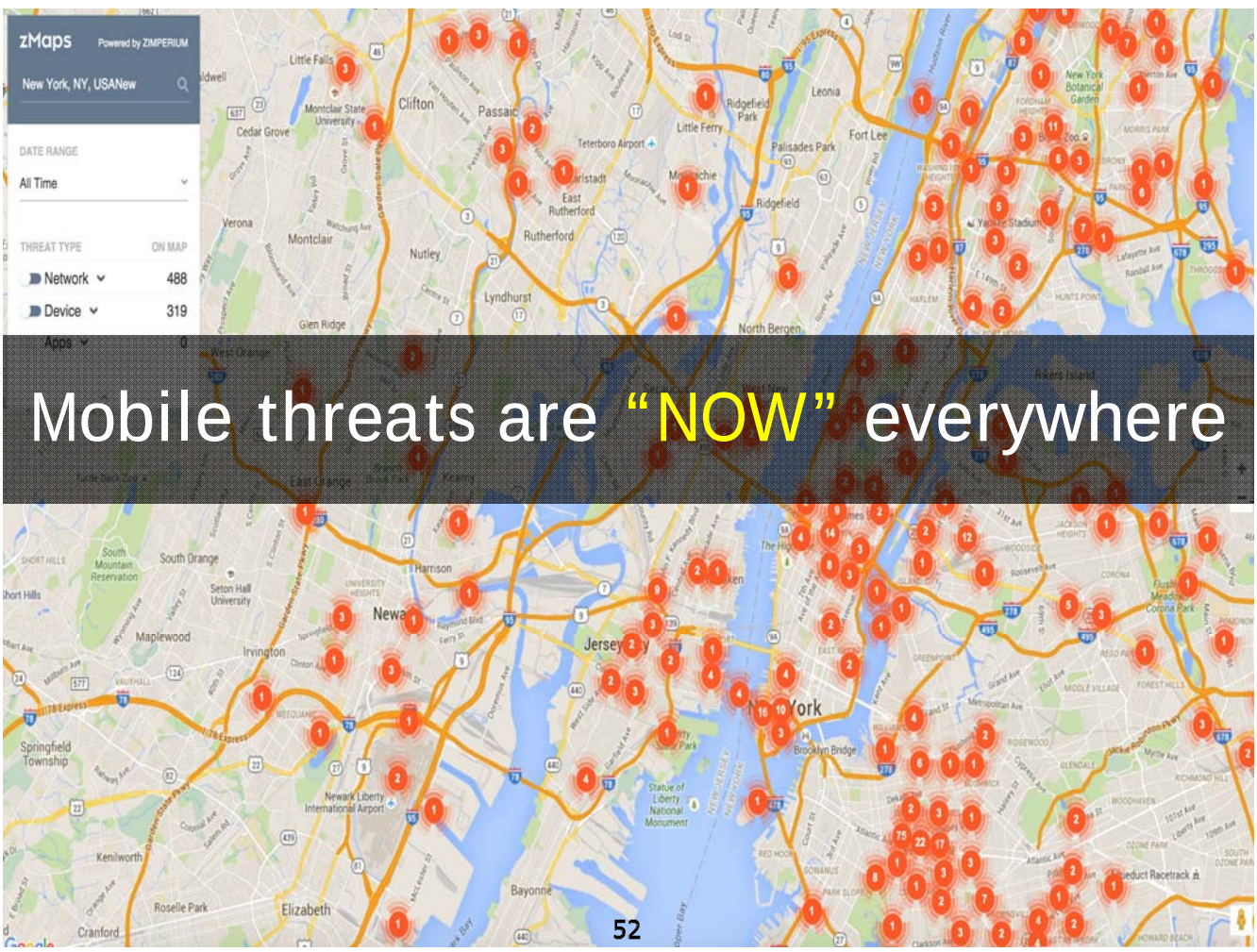
知らずに行われていた攻撃を可視化する事で
セキュリティ担保に対する意識の向上、およびリスクを認識

Israel 最先端セキュリティ企業からのまなび 4
– モバイルに迫る脅威 –

携帯・モバイルは安全???

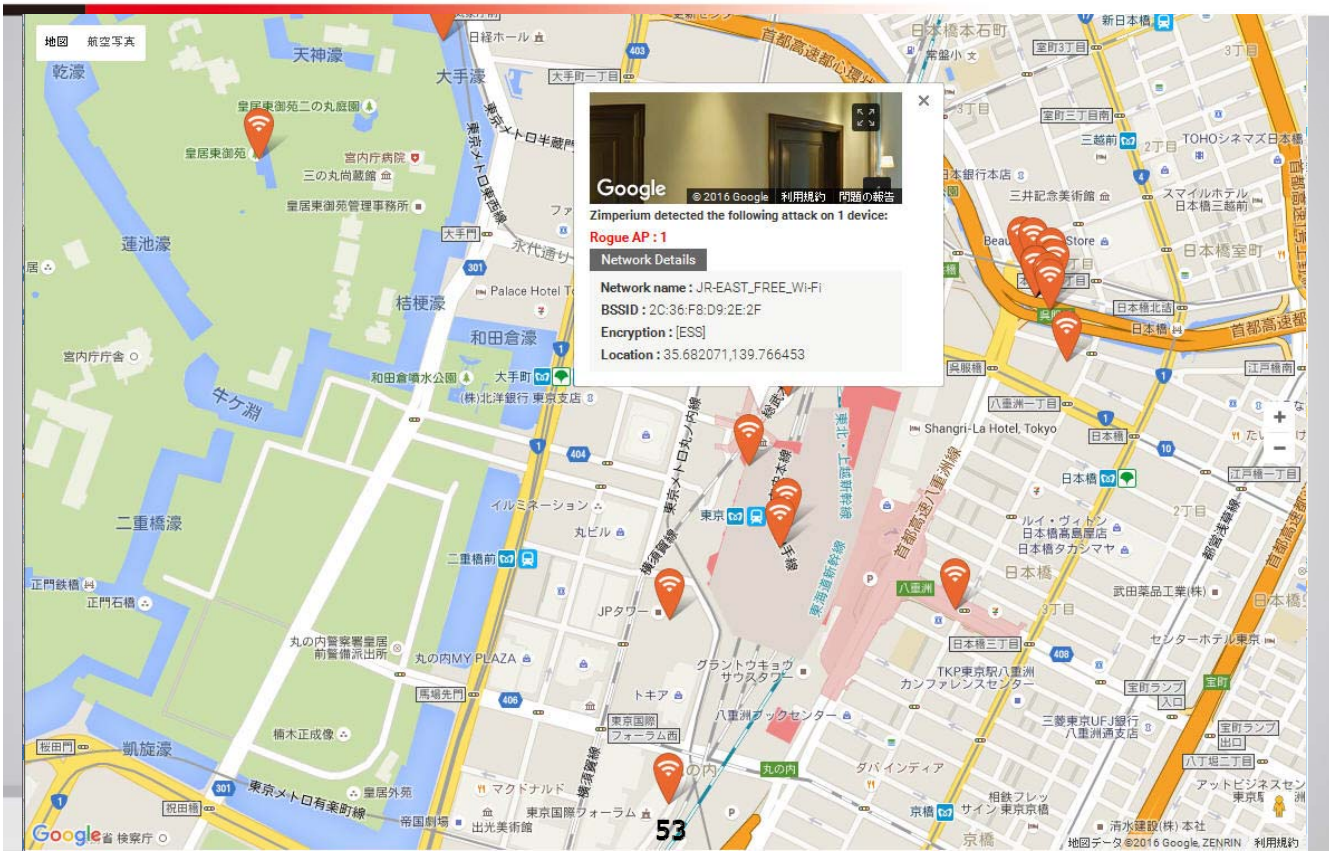


モバイル攻撃： 巧妙化かつ強毒化が進む



モバイルをターゲットにした攻撃 現状

Source：zlab AttackMap



Israelセキュリティ企業からのまなび 4
モバイルに迫る脅威

CYBERHAT

- End PointデバイスはPCからモバイル (Tablet) に
  - 重要企業機密のみならず、プライバシーの塊
- モバイルを狙う攻撃が拡大しはじめている
  - Malwareだけではない
  - コードをクリックするだけで、C&Cサーバとの接続を完了
  - 無線LAN区間のハイジャック（中間者攻撃）
  - ニセのSSIDをもつAPが増加
- モバイルとPCのOSアーキテクチュアの違い
  - モバイル特有の対処が必要 → PCと同様の防衛では無意味

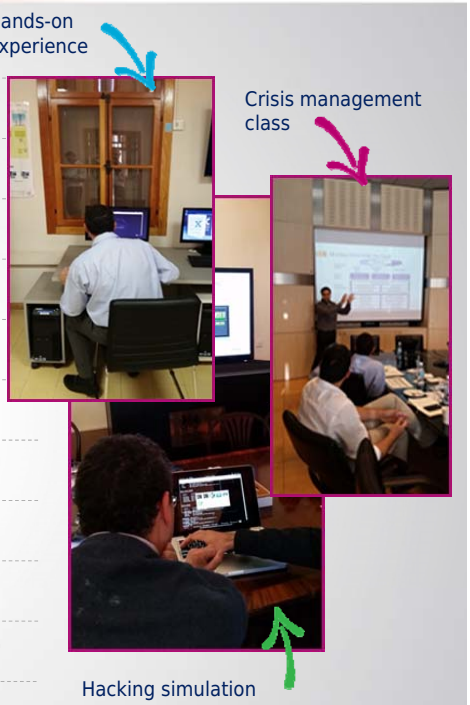
Israel 最先端セキュリティ企業からのまなび 5
– 次々うまれるセキュリティベンチャを育む土壌 –

次々うまれるベンチャーを支える土壌
Cyber Security Park

cyberspark
ISRAELI CYBER INNOVATION ARENA

セキュリティ“マネージャ”向け教育プログラム

- 3-5日間のフルカバレッジのセミナ
- “C”クラスの皆様に特化、最適化したメニュー
- 以下の5つのトレーニングモジュール:
  - 一般的なセキュリティ知識
  - ハッカー（攻撃者）との対話
  - 経営検討課題 – Risk, ROI, フレームワーク
  - 多国間の法律および規制
  - 攻撃実演と、ロールプレイング
- BG大学との連携プログラム
- 高度セキュリティ技術者および経験豊富なトレーナ



自動運転 サイバー攻撃防衛強度を「はかる」

リアルな攻撃シナリオ

360° 完全に制御された環境とモニタリング

コンセプトおよびソリューションの査定

セキュリティ認定プロセス

スタンダードおよび法および業界規制

3つのレイヤに対する攻撃からの防衛が重要
1) 車両内制御NWレイヤ
2) センシングレイヤ
3) アプリケーションレイヤ

Cyber Science Parkにいるハッカー軍団が
あらゆる方向から自動運転車に侵入、妨害攻撃を加える

Israel 最先端セキュリティ企業からのまなび 5
– 次々うまれるベンチャ土壌 –

- 軍・官・学・民のタイトな連携
  - 人の移動、協調
  - 攻撃、リスク情報の共有
- CERT-ILをはじめとした広範囲な情報共有
- 年数100人もの退役セキュリティエンジニアが市場に投入
  - 5年近いSOC，NOCエンジニア経験
  - 国、風土もベンチャー企業、産業振興をサポート

安心・安全はタダではえられない事
国土の小ささ、人口の少なさをカバーする施策
国民としての特異性を活かす事から、様々な先端技術が登場

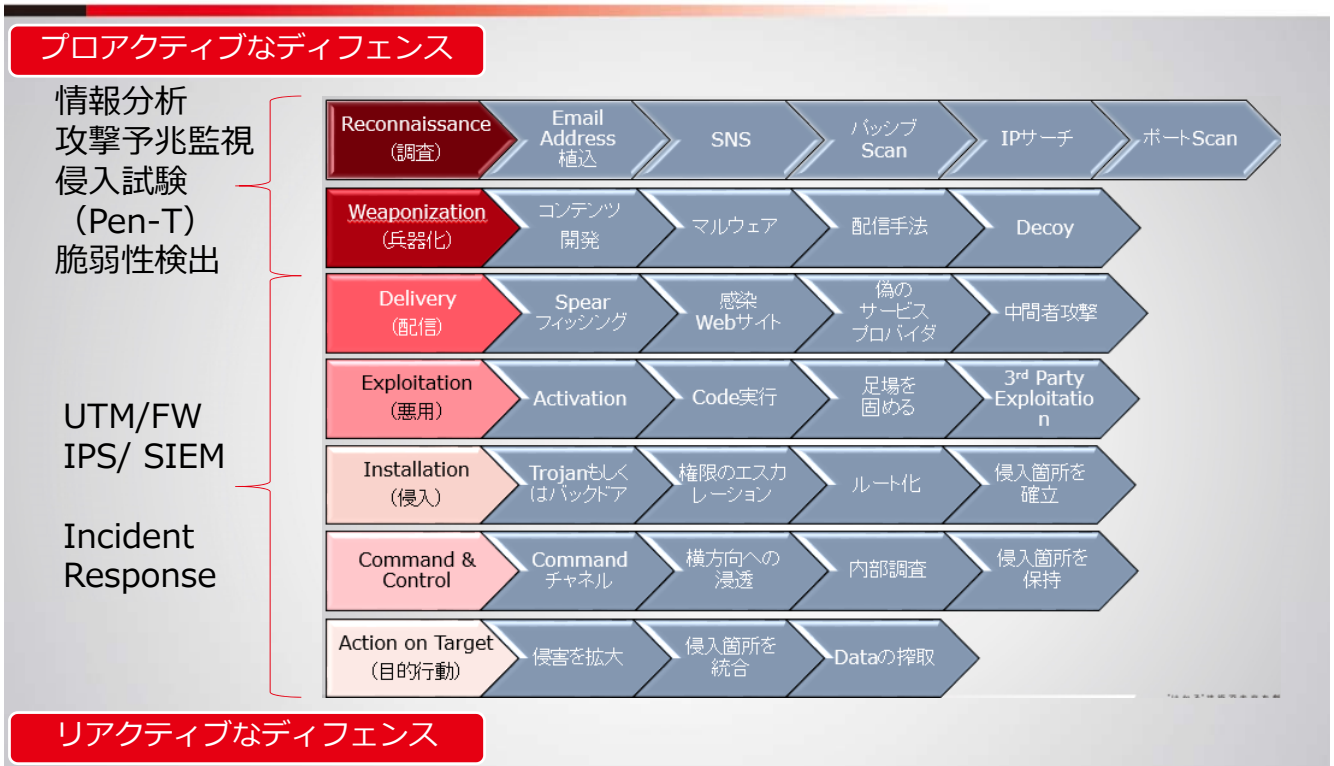
最後に

“防衛”戦略 コンセプト

彼を知り[1] 己を知り[2]
戦う場所を知れば[3]
百戦殆（危）うからず

- 彼： Attacker / Hacker / 受益者
- 知る[1]： 心理、ふるまい、プロセス、目的
- 己： 自社、情報、従業員、名声（ブランド）
- 知る[2]： リソース、価値、守るべきもの
- 戦う場所： Cyber空間、ハッカーのNW（DarkNET）
- 知る[3]： 流出情報、キッカケ、ネガティブキャンペーン

Cyber Kill Chainコンセプトの補完



Israelセキュリティ企業から学んだこと

- 内側からではなく、外側から
  - 自社視点ではなく、攻撃者視点での効果的ディフェンス
- クラッカー（攻撃者）の心理、手段を厳密に再現
  - 何を、どこから狙ってくるのかの視点
- インテリジェンスの重要性
  - 未然的防衛
  - もちは餅屋
- 盾矛
  - 最強の矛を持つ人材が、最高の盾を開発
- CERTの重要性
  - 医療同様に、サイバー攻撃をうけた情報共有が次のInnovationにつながる

ご清聴ありがとうございました

ご質問等 遠慮なくお問い合わせください。

連絡先： 株式会社 東陽テクニカ
セキュリティ＆ラボカンパニー
セキュリティ ビジネスユニット
Email: SLC_Security@toyo.co.jp
電話：03-3279-0771 （直通 03-3245-1245）