資料2－3

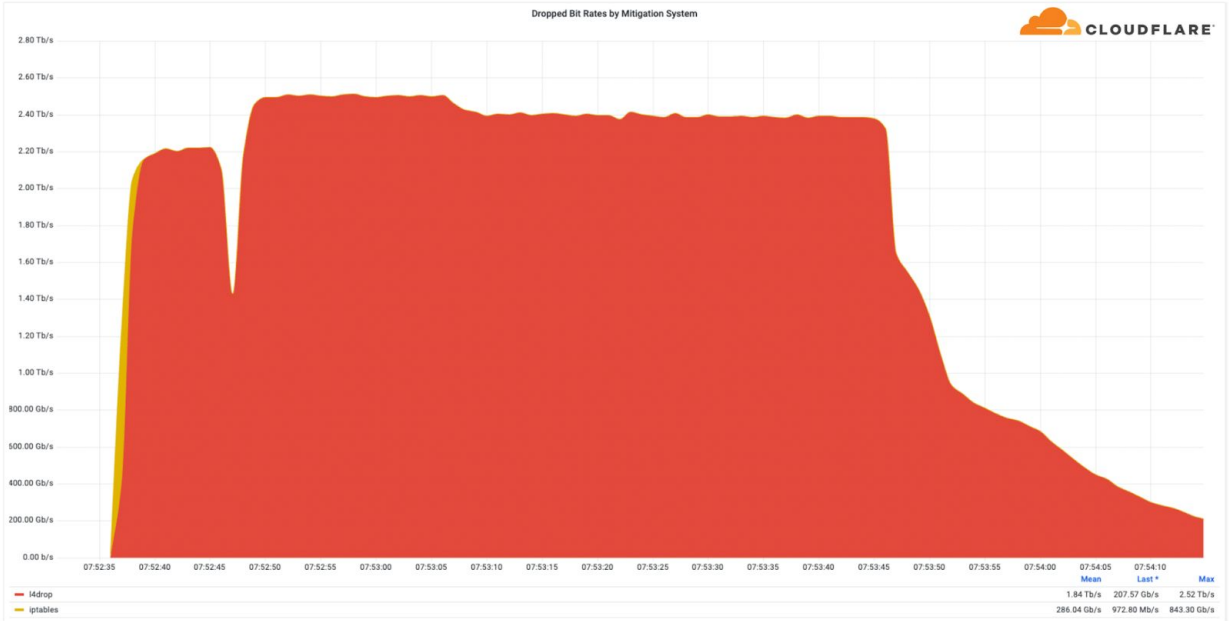
サイバーセキュリティ分科会（第２回）
ネットワークにおけるサイバーセキュリティ対策

ソフトバンク株式会社
2023/02/16

SoftBank

目次

情報通信ネットワークに対するサイバー攻撃についての認識



Miraiが仕掛ける、Wynncraftを標的とした2.5TbpsのDDoS攻撃

Cloudflare DDoS脅威レポート 2022年第3四半期 より
https://blog.cloudflare.com/ja-jp/cloudflare-ddos-threat-report-2022-q3-ja-jp/

レポートで言及されている内容

一般的なDDoS攻撃の傾向
今期全体では、以下のような傾向がありました:

・昨年に比べDDoS攻撃が増加しました。
・長期化する帯域幅消費型攻撃、Miraiボットネットとそのバリアントによって生成された攻撃が急増しました。
・台湾や日本を標的とした攻撃が急増しました

情報通信ネットワークに対するサイバー攻撃についての認識

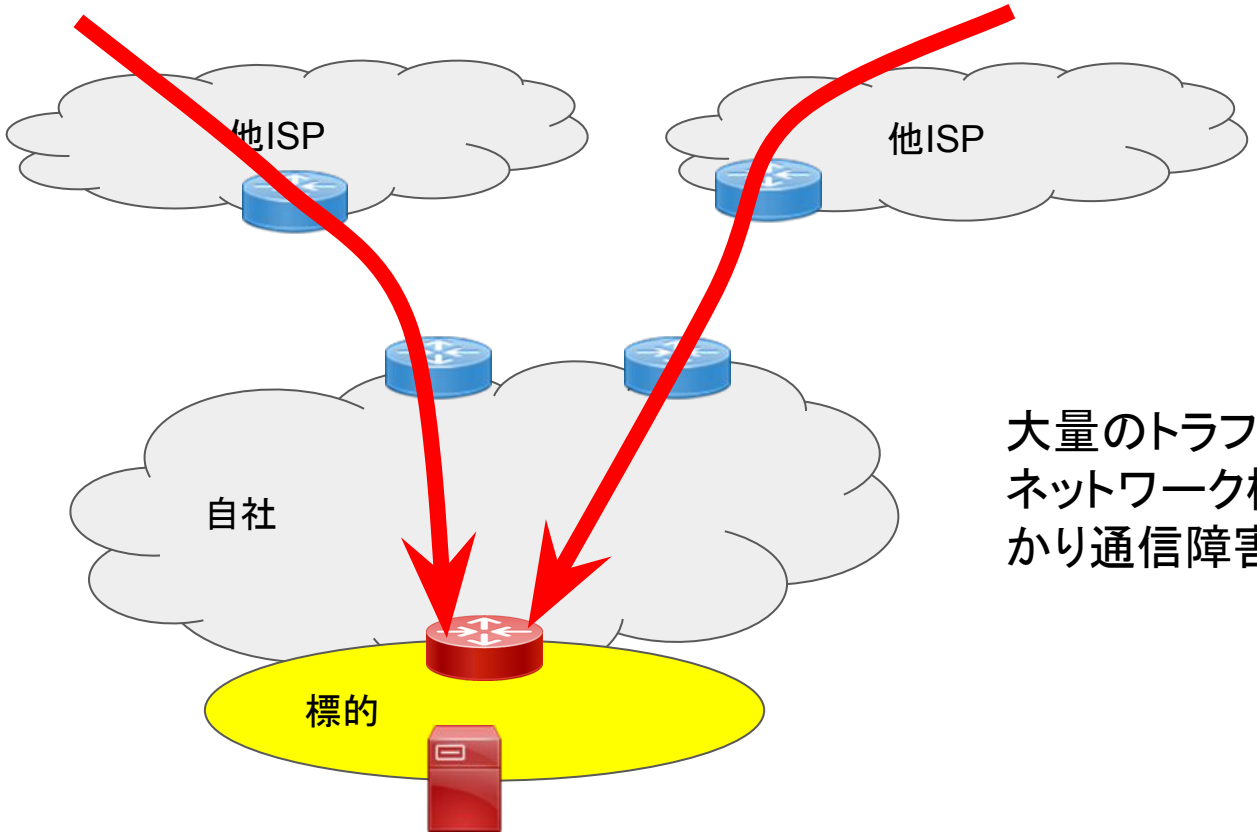
SoftBank

- DDoSの脅威は継続している
  - ソフトバンクとしても日々、異常なトラフィックを観測している
  - 自社が管理するネットワークにおいて受信する異常なトラフィックもあれば、自社が管理するネットワーク（マンションなど）から送信された異常なトラフィックもあった
- 異常なトラフィックの多くは海外から流入している
  - DDoSは国内だけに閉じた話ではない
- KILLNETによるDDoS攻撃は、めずらしくサイバー攻撃予告を伴っていた
  - 多くの異常なトラフィックに予告はない
  - なお、予告があってもその内容が正確であるとは思っていない
- インターネット全体の状況の把握が困難
  - 手元のネットワークしか見えない

ネットワークにおける対策

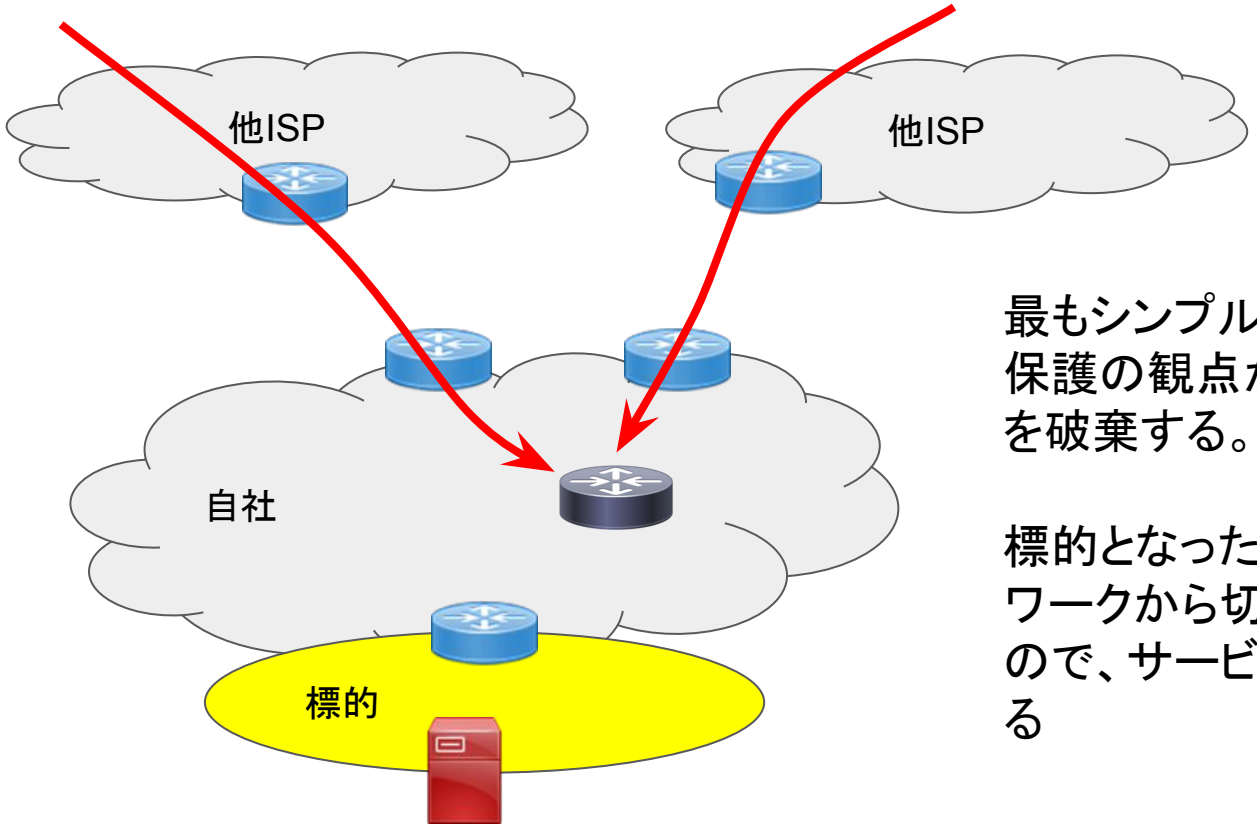
区分	実施項目（例）
DDoS発生時	・設備保護のために異常なトラフィックを破棄する ・関連するサイバー攻撃の情報収集 ・他社と情報交換 ・申告に基づくお客様対応
平時	・ネットワークのトラフィック量をモニタリング ・サイバー攻撃の情報収集、動向把握 ・他社と情報交換 ・NOTICE/NICTERへの参画（DDoS発生源を減らす取り組み）

ネットワークにおける対策



大量のトラフィックを受けた場合、
ネットワーク機器に過剰な負荷がか
かり通信障害となる

ネットワークにおける対策



最もシンプルな対策としては、設備保護の観点から、異常なトラフィックを破棄する。

標的となったシステムは半ばネットワークから切り離された状態になるので、サービスの提供に支障が出る

NOTICE/NICTERの対応状況

SoftBank

IoT機器調査及び利用者への注意喚起の実施状況（2022年12月度）

- 参加手続きが完了しているISP（インターネット・サービス・プロバイダ）は74社。
  当該ISPの約1.12億IPアドレスに対して調査を実施。
- NOTICEによる注意喚起は、4,416件の対象を検知しISPへ通知。
- NICTERによる注意喚起は、1日平均670件の対象を検知しISPへ通知。

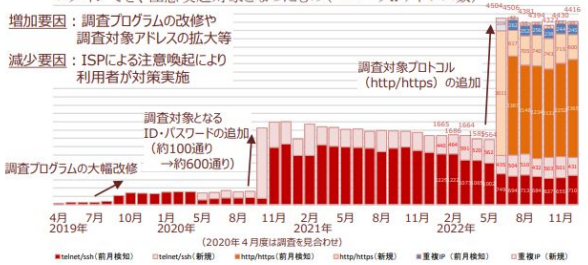
NOTICE注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

4,416件（11月度:4,430件）

（参考）2019年度からの累積件数：70,184件
ID・パスワードが入力可能だったもの：19.2万件

*) 特定のID・パスワードによりログインできるかという調査をおおむね月に1回実施し、ログインでき、注意喚起対象となったもの（ユニークIPアドレス数）



NICTER注意喚起※の取組結果

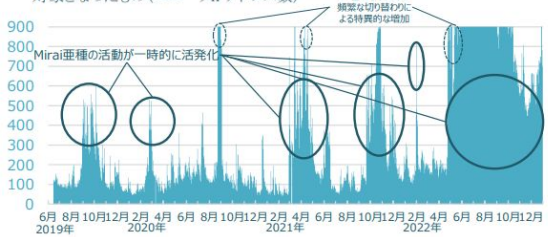
※マルウェアに感染しているIoT機器の利用者への注意喚起

注意喚起対象としてISPへ通知したもの**

1日平均670件（11月度:560件）

（参考）期間全体での値：1日平均427件
最小：40件(2021/2/10)／最大：3,288件(2022/6/6)

**) NICTERプロジェクトによりマルウェアに感染していることが検知され、注意喚起対象となったもの（ユニークIPアドレス数）



https://notice.go.jp/docs/status202212.pdf

- NOTICE
パスワード設定等に不備がある端末の特定と注意喚起

- NICTER
Mirai系マルウェアに既に感染している端末の特定と注意喚起

全体での対応状況はホームページにて公開されている

ここで掲載されているのは「ISPへ通知した件数」

NOTICEの対応状況

非公開

SoftBank

NICTERの対応状況

非公開

SoftBank

NICTERの対応状況

非公開

SoftBank

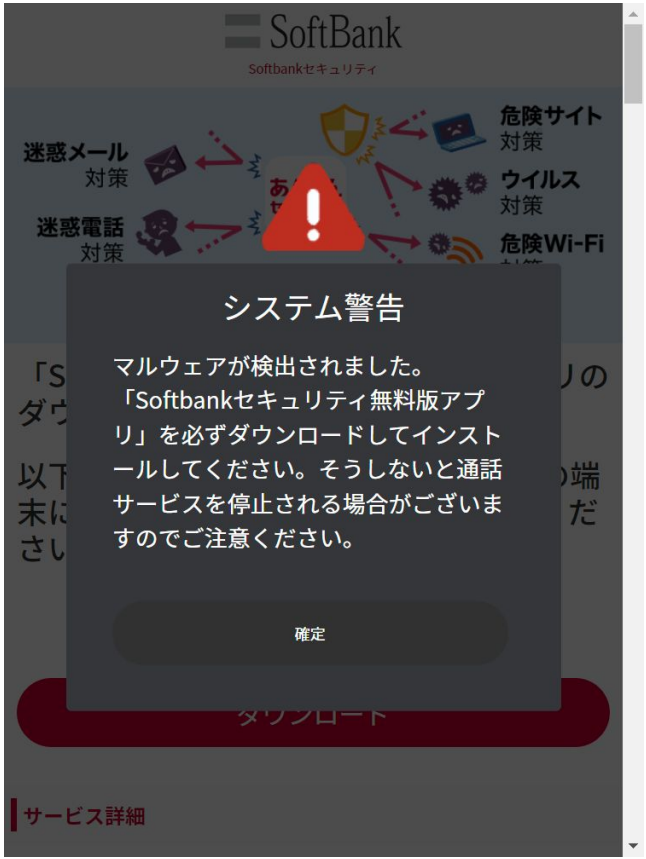
NOTICE/NICTERの課題

No	項目
①	対応の負担と効率
②	費用対効果が不明確
③	海外からのDDoS
④	他のDDoS発生源

課題① 対応の負担と効率

- ISPに通知されてから、対処完了に至るまでの作業負担は大きい
  - お客様の特定作業
  - 注意喚起レターの発送手続き、架電
  - 何回も対応する必要がある
    - 対応しない／できないお客様も多い（お客様は困っていない可能性あり）
    - 数か月後に再発するお客様もいた（原因は不明）
  - 対応状況を取りまとめて報告
- お客様に到達できない場合がそれなりにある
  - お客様特定できず、注意喚起が実施できない
- 効率よく、該当する全てのお客様に対応してもらうスキームにはなっていない

課題① 対応の負担と効率



- DDoS対策だけを実施すればいいわけではなく、通信事業者を取り巻くセキュリティ環境は厳しい

- フィッシングサイト、メールの増加
- 発信者情報開示の件数の増加による、お客様対応工数上昇
- サプライチェーンの問題
- 地政学的な問題
- 内部不正への対策

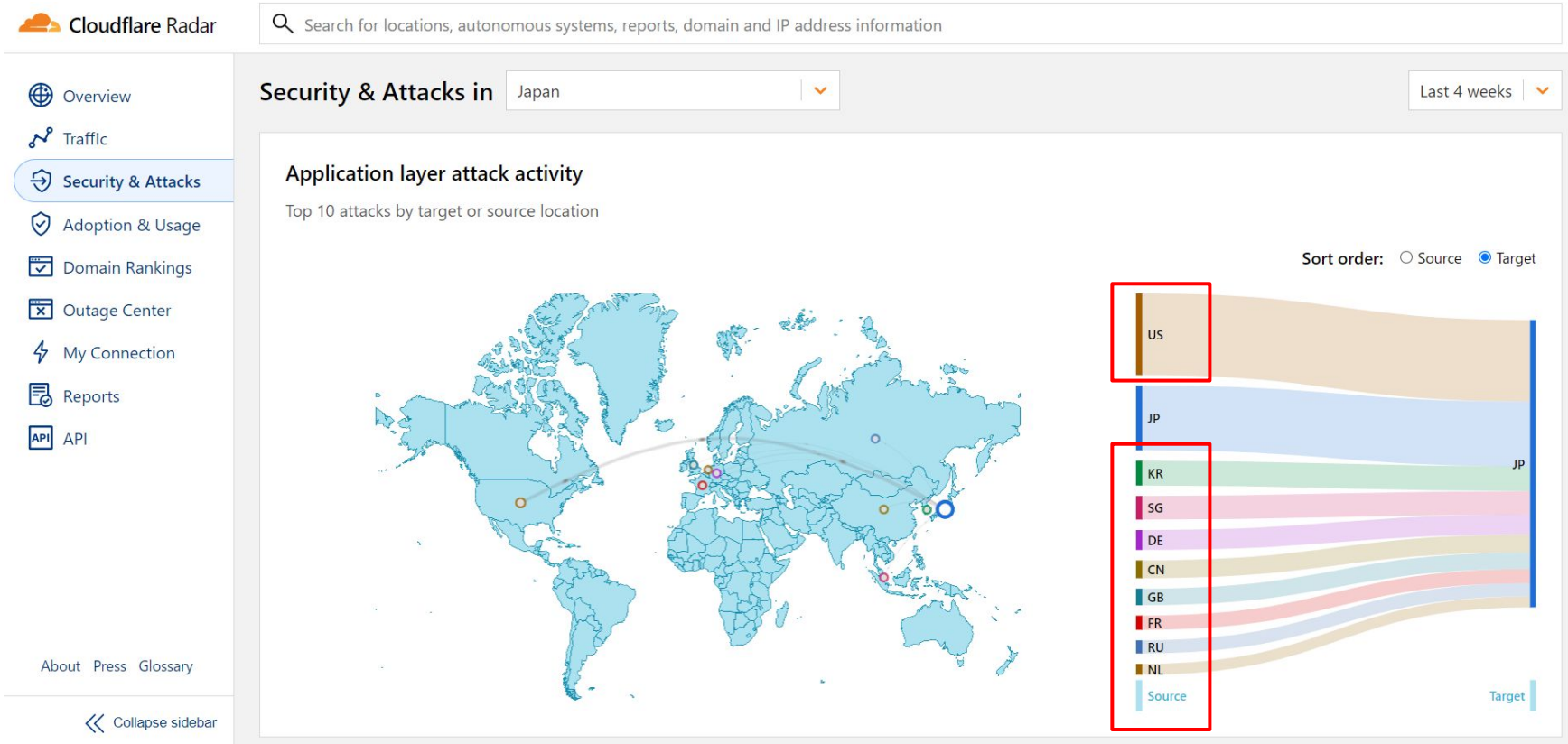
課題② 費用対効果が不明確

非公開

SoftBank

課題③ 海外からのDDoS

SoftBank



https://radar.cloudflare.com/security-and-attacks/jp?range=28d

課題④ 他のDDoS発生源

SoftBank

NOTICE/NICTERでカバーしていないDDoS発生源がある

- ファームウェアに脆弱性があるIoT機器
- マルウェアに感染したPC、サーバー
- 悪用されている、乗っ取られているホスティングサービスのサーバー
- （ひょっとすると）スマートフォンの不審なアプリ

今後の取り組みについて

SoftBank

No	項目
①	全体像の把握
②	より上流工程での対策
③	ボットネット単位での対策

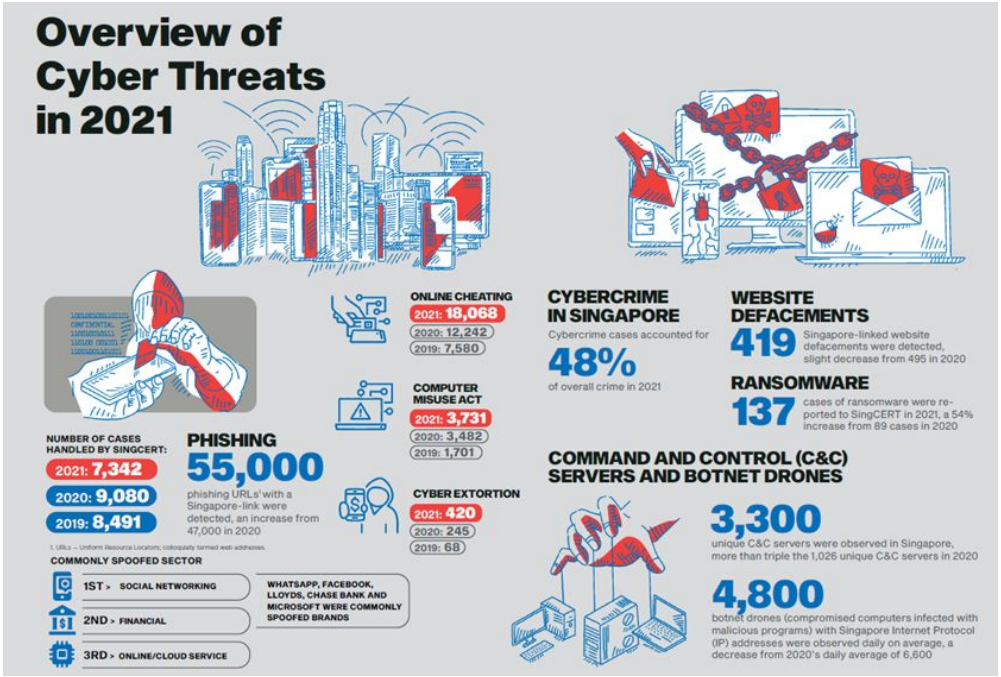
取り組み① 全体像の把握

SoftBank

まずは全体像を十分に把握する必要があるのではないか。
現在は、下記が十分に把握されてないのではないか。

- 日本の中に対応が必要な機器は何台あるのか？
- どの程度まで脆弱な機器を減らせば、安全になったといえるのか？
- 脆弱な機器を悪用しようとしている攻撃者（グループ）は誰か？
- ボットネットと国内のマルウェア感染した機器の紐づけはできているか？
- ボットネットのうち、現在DDoS攻撃に活用されているものはどれか？

取り組み① 全体像の把握



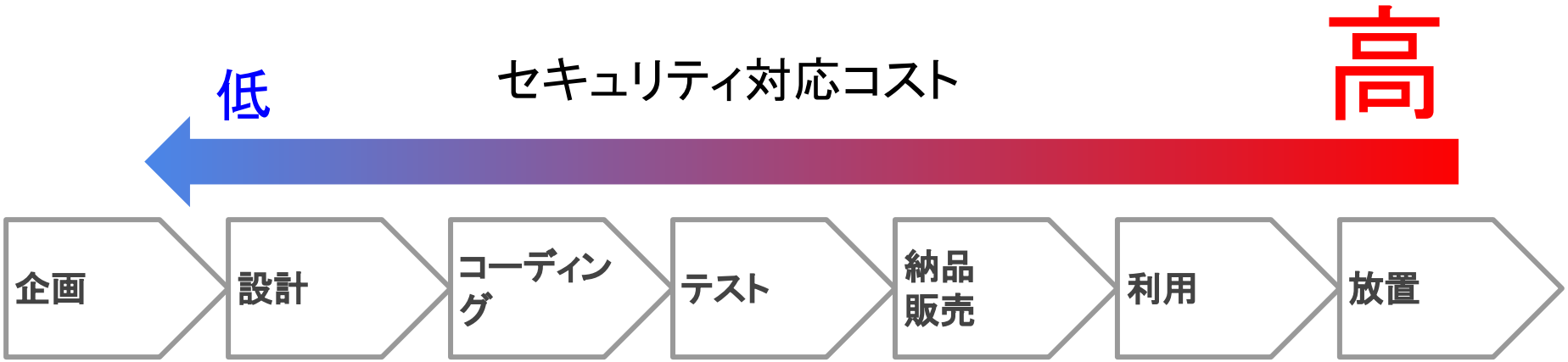
シンガポール
Cyber Security Agency（サイバーセキュリティ庁）

iii. Malicious Command and Control (C&C) Servers & Botnet Drones. In 2021, CSA observed 3,300 malicious C&C servers hosted in Singapore, more than triple the 1,026 C&C servers observed in 2020. This was the largest number recorded since 2017. This spike was driven by a large increase in servers distributing CobaltStrike malware, which made up nearly 30 per cent of all C&C servers observed.

In 2021, CSA detected about 4,800 botnet drones with Singapore IP addresses daily, a 27 per cent decrease from 2020's daily average of 6,600. Malware strains for the infected drones varied greatly, with no single strain accounting for a clear majority among compromised devices. This trend could have been caused by threat actors diversifying away from 'old' malware strains and exploring new infection methods, as system owners cleaned up infected computers and devices progressively.

https://www.csa.gov.sg/News/Press-Releases/ransomware-and-phishing-attacks-continued-to-threaten-singapore-organisations-and-individuals-in-2021

取り組み② より上流工程での対策



こちらにもっと力を入れるべき

NOTICEの対応

取り組み③ ボットネット単位での対策

SoftBank

- ボットネットのテイクダウンによるボリューム感のある対策が必要ではないか
  - ボットネットを構成する末端の脆弱なIoT機器群に対して、注意喚起で数十台に対応しても、攻撃者に与える影響は小さい（DDoS攻撃の低減に至らない）と危惧する
- 現在進められている、C2サーバーの検知の取り組みについて、最終的にボットネットのテイクダウンにつながることに期待したい
  - 検知できるようになっただけでは、DDoS攻撃は止まらない
  - なお、将来的な対応として、単純に、C2サーバーへの通信をしらみつぶしに通信事業者が止めるのは、運用負担の面や誤遮断のリスクから難しいのではないか

まとめ

SoftBank

1. 情報通信ネットワークに対するサイバー攻撃の脅威は続いている
2. NOTICE/NICTERの取り組みは現時点でいくつか課題がある
3. 今後の取り組みとして、特にボットネットのテイクダウンにつながる活動が必要ではないか

EOF