国際ボットネット対策ガイド 2018

本ガイド記載の背景や対策は、米国を中心とした幅広い分野のステークホルダーがそれぞれの立場で行う対策の例がまとめてあります。ICT-ISAC Japan の会員のみならず日本の多様な組織においてボットネット対策の参考として役立てていただけるよう、CSDE の会員企業でもある NTT が翻訳を行い、ICT-ISAC Japan が監修しました。

翻訳監修にあたっては、NTT が USTelecom、Information Technology Industry Council (ITI)、Consumer Technology Association (CTA) の承諾を得ており、原本に沿ってできる限り忠実に翻訳していますが、正確性を保証するものではありません。本ガイドをひな形として参照しながら、ステークホルダー同士で議論が進んだり、役割の明確化が進むことで、セキュリティ改善につながる可能性はありますが、本ガイド記載の内容を順守することや参照したことにより生じる損失・損害に対して、ICT-ISAC Japan は一切の責任を負うものではありません。

注意事項

国際ボットネット対策ガイドは、グローバルなインターネットとコミュニケーションのエコシステムを通して、ステークホルダーが自発的に参加し協力することにより、ボットネットや他の自動化された分散型の脅威を軽減するために作成された。このガイドでは、ステークホルダーがお互いに個々の状況と関係を適切に判断しながら、目標に向け積極的に対策を実施するために、情報通信技術（ICT）のステークホルダーに情報を提供し対策の推進を奨励する。

このガイドではICTセクターの各セグメントに対して「ベースライン」から「先進的」な範囲における効果の高い自主的なプラクティスを紹介する。このガイドを作成した業界リーダーたちは、すべての脅威とリスクを排除できる統合した対策は全くないことを認めるが、自動化された分散型の攻撃を軽減するために、ベースラインと先進的なプラクティスは、ICTステークホルダーが自らのプラクティスを特定し選択する際に、参考とする価値あるフレームワークを提供すると考えている。
このガイドではセキュリティ対策を実施するためには、様々なICTステークホルダーが異なる課題に直面し、考慮し優先順位を決定しなければいけないことを理解している。従って、全体としてガイドで示されるプラクティスは、ICTステークホルダーが状況に応じて実施するべきツールであり、プラクティスを実施するかは、要件でも義務でもなく、何ら強制するものではない。

このガイドで議論されているプラクティスと技術のほとんどは、ネットワークサービスプロバイダーによる、ディープ・パケット・インスペクション（DPI）の契約から、セキュリティ対策を十分に備えていないデバイスの使用を禁止することまで、大企業が既にネットワークとシステムの防御に利用しているものである。しかし、幅広い消費者の分野においてこれらの機能を実現するためには、例えば以下のようなより広範囲の政策的な合意が必要である。

- IPトラフィックのDPIのような先進的な機能は、特定の状況で有効であるが、もし公共ネットワークで展開する場合には、個人のプライバシーが関わってくるため慎重に扱わなければならない。

- 政策上の目的のために政府からの要請があった場合、IPアドレスを基に公共のネットワークトラフィックをフィルタリングあるいは他の手段をとることは、個人の情報公開に関して問題となるかもしれない。

- 企業にはサプライヤーと詳細な要件について交渉し、費用便益分析（コストベネフィットアナリシス）を考慮して決定できる有能なITスタッフが存在する。そのような柔軟性は、費用便益分析が大企業とは著しく異なる消費者の分野には存在しない。消費者に対しては、コストと消費者保護の課題は異なるリスク管理の規模で評価する必要があるだろう。

- セキュリティ機能が不十分と思われるデバイスは、国際貿易への影響と地域の規制を考慮せずに、場当たり的に特定の国において、単純に禁止することはできない。

目次

1. 概要

セキュアなデジタル経済に向けた評議会（CSDE）と全米民生技術協会（CTA）のメンバーは、グローバルなデジタル経済、つまり世界中の消費者、中小企業、大手民間企業、政府、非営利団体に利便性を与えるインフラとソフトウェアを提供する複雑なグローバルなインターネットとコミュニケーションのエコシステム全体に渡っている。

このガイド作成に貢献したのは、サイバー脅威からエコシステムを守るために、自主的なプラクティスを先駆的に取り入れた企業である。一方、テクノロジーセクターは、ハードウェア、ソフトウェア、デバイス、システム、そして関連サービスのグローバルなプロバイダーによって供給されるセキュア・バイ・デザイン、マネージド・セキュリティ・サービスそしてライフサイクルサポートから恩恵を受けている。しかし、インフラ提供者、ソフトウェア開発者、デバイスシステム製造業者、システム導入業者、そしてあらゆる種類の企業には課題が山積している。

CTA と密接に協力して作成された CSDE の国際ボットネット対策ガイドでは、グローバルなデジタル経済に絶えず増加する課題、つまりボットネットや自動化された分散型の脅威に対処するために、上述のステークホルダーの多様性あるグローバルな視点、プラクティス、経験を参考にしている。

グローバルなデジタル経済を守るために責任の共有を推進する

デジタル経済は、世界中で商業の発展と生活の質向上における牽引役であり続けている。しかし、官民共に一ステークホルダーだけでは、このシステムを管理することはできない。むしろ、デジタル経済の発展により得られる機会を安全に管理していくことが、情報通信技術（ICT）コミュニティーにおける全てのステークホルダーの課題であり責任である。

しかし、最近では特にボットネットによるデジタル経済への被害が増え損失が増大している。ボットネットは、ウイルスに感染し、インターネットに接続したコンピュータやデバイスの大規模なネットワークのことで、悪意あるアクターは分散型サービス拒否攻撃（DDoS）や、ランサムウェアの増殖、フィッシング攻撃そして、ソーシャルメディアに虚偽の情報を拡散させることができる[1]。残念ながら、インターネットに接続する人々、事業者及びデバイスの数が増加するとともに、これらの悪意ある攻撃を受ける可能性も増えている。2020 年までに接続するデバイスが 200 億個に達すると予想される中、ボットネットが数十億個の IoT デバイスを介して攻撃するにつれ、ボットネットの潜在的な破壊力は現在飛躍的に拡大している。このような実質的な攻撃対象領域の増加と、サイバー犯罪のグローバルでの被害額が数兆ドルに達すると予想されることは偶然の一致ではない。ボットネットの攻撃により、産業規模での損失を引き起こしている。

事実、ボットネットによる脅威は、歴史上過去のいかなる時点よりも現在深刻になっている。小規模で目立たない攻撃は表面に出ず、被害が知られないまま放置されている一方で、大規模で目立った攻撃が大企業を襲っていると最近報告されている。これらの攻撃が増えることで、デジタル経済における、直接的かつ具体的な被害は数十億ドルにのぼっている。これらの脅威により、デジタル経済における根本的な信用と信頼を損なってしまうため、間接的な被害も甚大となる。

このガイドの目的は、こうした傾向を逆転させることにある。このガイドの作者たちは、政府が多様なエコシステムを主導する重要な役割を果たすことを強く支持する一方、規範的な義務やコンプライアンス重視の規制要件では、今日の高度な脅威からエコシステムを守るために、最も重要となるセキュリティの技術革新を妨げてしまう。さらに、かつての政策的取り組みはこれらの脅威に対する非現実的な解決策を前提としており、インターネットサービスプロバイダー（ISP）は、単純にすべてのボットネットを遮断する、あるいは製造業者によってすべてのデバイスを普遍的に安全にするという考えに立っている。代わって、グローバルなデジタル経済を介して、自発的に合意した基準によって周知され、市場の需要により牽引され、ステークホルダーによ

って導入されるダイナミックで柔軟性あるソリューションは、これらの進化しつつある全体的な課題にとってより良い対策となる。

そのようなソリューションを実現し、全ての関係者間で責任の共有を推進するために、このガイドでは、一連のベースラインプラクティス（基準となる慣行レベルの対策）を説明する。さらに、現在利用可能だが十分に活用されていない、付加的かつ先進的な機能も紹介する。このガイドに記載されているセキュリティ対策を広く実行することで、ボットネットを劇的に減らし、グローバルエコノミーの安全確保に役に立つであろう。このガイドは、一ステークホルダーだけまたは一国だけ、あるいは政府の主導権だけで対応することはできないグローバルな課題に対して、現実世界で現在利用できるソリューションを提供する。このガイドは、ボットネットの脅威を劇的に減らすために、多様な産業と国々を超えた企業で進行中のコラボレーションや、急速に拡大するグローバルな脅威・脆弱性と、増加する高度で果敢な攻撃者の分析により提供される。

このガイドでは、以下の核となるセキュリティ原則を前提として前向きに推進を図る:

- セキュリティには、地域や国家の権限によって異なる規制されたコンプライアンスの仕組みではなく、サイバー脅威と同様に機敏かつ適応力の高い、強力なグローバルマーケットの力に牽引され軽減されなければいけないダイナミックで柔軟性のあるソリューションが必要である。

- セキュリティは、インターネットとコミュニケーションのエコシステムにおいて、特定の選ばれた構成要素やステークホルダーで安易なソリューションを求めるのではなく、セキュリティの責任をすべてのステークホルダー間で共有し、政府と業界のステークホルダーは、すべてのステークホルダー間で責任感を高めるソリューションを開発しなければならない。

- セキュリティは、悪意のあるアクターに対する一連の対処や責任あるアクターの貢献に対する報酬を通じて、政府、サプライヤー、プロバイダー、研究者、企業、消費者間で相互に有益なチームワークとパートナーシップを持つことが重要になる。

これらの原則は現状で求められるボットネット対策への新しいアプローチの基礎である。

国際ボットネット対策ガイド：プラクティスと機能に関する要約
インターネット及び関連する通信のエコシステムからなる「システムのシステム」は複雑であるため、全てのステークホルダーに対して均一に適応するまとまったガイダンスを提供することは困難である。このガイドでは、プロバイダー、サプライヤー、ユーザーというステークホルダーを、異なる 5 種類の構成要素に分類する：（1）インフラ（2）ソフトウェア開発（3）デバイスとデバイスシステム（4）家庭と中小企業のシステム導入（5）企業。これらの各構成要素に対して、このガイドでは、そのような全てのステークホルダーの要望に応えるだけでなく、十分に活用されていないかもしれないが、市場において現在入手できる先進的な機能も含めて、ベースラインプラクティスを説明する。以下に簡潔に要約したこれらのプラクティスと機能は、このガイドブックの中核となるものである。

1. **インフラ**： このガイドの目的に対して、「インフラ」は接続性と運用性を可能にするすべてのシステムに言及する。つまり、インターネットサービスプロバイダーの設備、基幹システム、クラウド、ウェブホスティング、コンテンツデリバリー、ドメインネームシステム、そしてサービスだけでなく、形あるものからデジタルコンセプトへのインターネットの進化を反映する Software-Defined Network（SDN）とシステムを含む。インフラに対して下記の点を含むベースラインプラクティスと先進的な機能を推奨する：

    - 悪意あるトラフィックと脆弱性の検知

- 分散型サイバー脅威の緩和
- 顧客やピアとの連携
- ドメイン差し押さえとテイクダウン（停止措置）

2. ソフトウェア開発[2] ソフトウェアは、エコシステムの全ての構成要素の中でユビキタスの要素を増している。ソフトウェア開発には、様々なソフトウェアの革新と改善を牽引する複雑な開発プロセスと相互依存性がある。ソフトウェアが、ベースラインプラクティスと先進的な機能から構成されるよう、下記の点を含めるよう推奨する：

- **セキュア・バイ・デザイン開発の実施**
- **セキュリティ脆弱性の管理**
- **セキュア開発プロセスの透明性確保**

3. デバイスとデバイスシステム[3] 個々の接続されたデバイス（または「エンドポイント・デバイス」）はハードウェアモジュール、チップ、ソフトウェア、センサーやその他の多様な部品で構成される事もある。セキュリティの革新を含む極めてダイナミックで新しい市場を構成するさらなる接続性のレイヤは、個々のデバイスそのものを超えている。IoT のエンドポイントの「モノ」、そしてモノに付帯するアプリケーションとサービスに対して、我々は下記のベースラインプラクティスと先進的な機能を含むことを推奨する:

- **セキュア・バイ・デザイン開発の実施**
- **信頼の基点**
- **生産終了を含む製品ライフサイクル管理**
- **セキュリティ中心のツールチェインの使用**

4. 家庭と中小企業のシステム導入[4]
家庭と中小企業は、いくつかの種類で接続されたデバイスによって利便性を得る。これらのシステムは、家庭では個人が、そして事業主、または専門家が導入できる。専門家とはインテグレーターや警報システム請負業者などである。「コネクテッドホーム用セキュリティシステム」[5]から多くを引用することで、ベースラインプラクティスと先進的機能は下記を含むことを推奨する:

- **認証とクレジデンシャル管理**
- **ネットワーク設定**
- **ネットワーク機器の管理**
- **セキュリティの維持**

5. 企業[6]
急激に増加する IoT デバイスシステムを含む、ネットワークで接続されたデバイスとシステムの主要な所有者、利用者として、すべての種類の企業、すなわち、政府、民間セクター、教育機関、非営利団体などは、デジタルエコシステムの安全性確保において重要な役割を果たす。我々は、企業に対しベースラインプラクティスと先進的な機能として下記を推奨する:

- **確実なアップデート**
- **リアルタイムの情報共有**
- **トラフィックフローをセキュアに管理するネットワークアーキテクチャ**
- **DDoS 攻撃に対する強靭性の強化**
- **ID とアクセス管理**
- **レガシー製品と海賊版製品の課題への対策**

ネクストステップと実現

このガイドの出版は、第一歩にすぎない。次の段階では、ガイドブックのベースラインプラクティスと先進的な機能を推進するために、同じような考えをもつ国々の政府も含み、幅広い分野のステークホルダーに戦略的に関与する予定である。さらに、毎年更新の上出版し、ガイドの改訂版の活用を推進する。

2. 序論

セキュアなデジタル経済に向けた評議会（CSDE）[7]と全米民生技術協会（CTA）[8]のメンバーは、複雑なグローバルなインターネットとコミュニケーションのエコシステム全体に及ぶ。これらの団体には、人材と技術システムを提供し、接続機能、ソフトウェア、デバイスを作り出し導入管理し、世界中の消費者、中小企業、大手民間企業、政府、NPOなど、グローバルなデジタル経済全体に、利便性を与えるメンバー企業が含まれる。CTAと密接に協力して作成されたCSDEの国際ボットネット対策ガイドでは、ボットネットや自動化された分散型の脅威により[9]、絶えず増加するデジタル経済の課題に対処するために、ステークホルダーの多様な国際的視点のみならず、効果の高いプラクティスと現実世界で起こせる行動を描いている。

課題の概要

デジタル経済は、世界中で雇用と機会を生み出し、商業の発展と生活の質向上における牽引役であり続けている。デジタル経済は、すでに世界の経済価値の20%を占めるかもしれないという推計がある[10]。商業取引を含むすべての価値が、デジタル的に提供されるわけではないので、GDPだけで世界の経済価値にどの程度デジタル経済が貢献しているかを完全に把握することはできないが、ウォールストリートジャーナルは、デジタル経済は2016年に11.5兆ドル相当になり、2025 年までには世界のGDPのほぼ4分の1となり23兆ドルまで増加するかもしれない[11]と報じており、デジタル経済の成長はビジネスと消費者によって新しい先端技術が適用されることで加速し続けてきた[12]。著しい成長により得られる機会を安全に管理していくことが、情報通信技術（ICT）コミュニティーにおける全てのステークホルダーの課題であり責任である。

しかし最近では特にボットネットによるデジタル経済への被害が増え損失が増大している。ボットネットは、マルウェアを増殖させ[13]、サービス拒否攻撃をしたり[14]、人為的にソーシャルメディアを混乱させようと虚偽の情報を拡散できる[15]。現在たったひとつのボットネットに3000万個以上の「ゾンビ」のエンドポイントを含むことができ、悪意あるアクターに月10万ドルの利益をもたらすことができる[16]。2020年までにインターネットに接続したデバイスは200億個に達すると予想され、特に何十億個ものIoTデバイスが急速に発展し、デジタル経済そのものの成長が著しくまた前途有望であるため、現在より多くのシステムがかつてないほど脆弱になっている[17]。このインターネット接続による経済面での利便性のために、物に関して商業と消費者活動に変革がおこっており、このガイドを作成した企業はデバイスを展開しながら新しいセキュリティ対策を開発している。そのような状況にもかかわらず、デバイスを防御するよう意図されたシステムがないまま、市場に安全でないデバイスが出回り続けている[18]。さらに現在では比較的未熟な悪意あるアクターは大規模な不正行為をおこすために強力なボットネットを借りることができる[19]。

これらの動きはデジタル経済に直接的かつ具体的な被害をもたらす。例えば2017年以降、マルウェアがヨーロッパ、アジア、アメリカに拡散し100億ドル以上の損害を与えた[20]。今後5年間にサイバー攻撃による犯罪だけで、世界中の事業にもたらす被害累計額は、（罰金、事業の損失、復旧費用など）8兆ドルになると予想される[21]。これらの脅威によりデジタル経済における根本的な信用と信頼を損なってしまうため、間接的な被害も甚大となる。

戦略的な姿勢と目標

私たちの目的はこの傾向を変えることにある。私たちは政府が多様なエコシステム活動において、多様なステークホルダーによる活動の仲介役として貢献し、主要な役割を果たすことを認識し支援するが、コンプライアンス重視の規制要件では、今日の高度な脅威からエコシステムを守るために必要なセキュリティの技術革新を妨げてしまうことを確信している。言い換えれば、規範的規制要件だけではほとんど効果がなく、それらは事実、セキュリティ確保の目的に対して通常逆効果をもたらす[22]。グローバルなデジタル経済を介して、自発的に合意した基準によって周知され、市場の需要により牽引され、ステークホルダーによって実装されるダイナミックで柔軟性あるソリューションは、この複雑なエコシステムの全てのステークホルダーにとって脅威となる、悪意あるボットネットのように、進化しつつある全体的な課題にとってより良い対策となる。

したがってこのガイドでは、将来のデジタル経済を守りその可能性を存分に発揮するために、デジタル経済において責任を持つステークホルダーの能力向上を追求する。積極的に協力して行動することで、長期にわたり、大企業、中小企業全てのステークホルダーにとって商業的に有益なものとなると信じている。そのために、このガイドはインターネットとコミュニケーションのエコシステムの強靭性を高め、基盤となるデジタルインフラのトランザクションの整合性を強化するために活用されるかもしれない。このガイドは、グローバルなデジタル市場における全てのステークホルダーに、一連のベースラインとなるツール、プラクティス、プロセスの実装を促す。さらに、現在利用可能だが十分に活用されていない付加的かつ先進的な機能も紹介する。このガイドに記載されるセキュリティプラクティスを広範囲に実装することは、ボットネットを劇的に減らしグローバルなデジタル経済を守るために役立つであろう。

メソドロジーとネクストステップ

このガイド作成に貢献した企業は、ボットネットのように自動化された分散型の攻撃に対抗するために有効と考えられるプラクティス、テクノロジーとツールを紹介する資料の包括的な見直しに取り組んでいる。また彼らは政府や国際機関の報告書を調査し、外部の専門家や業界、学術、市民社会の情報筋に助言を求めた[23]。しかし明確に言うとこのガイドの出版は最初の一歩に過ぎない。次の段階では、このガイドのベースラインプラクティスと先進的な機能を推進するために、同じような考えをもつ国々の政府も含み、幅広い分野のステークホルダーによって戦略的に関与する予定である。さらに、ガイドを毎年更新の上出版し推進するつもりである。

3. ボットネット：多様化するインターネットのエコシステムにおける自動化された分散型サイバー脅威への対策

グローバルなインターネットとコミュニケーションのエコシステムについて、自動化された分散型の脅威の最も際立つ例は、ボットネットである。ボットネットは、ウイルスに感染したインターネット接続のコンピュータやデバイスの大規模なネットワークのことで、指令を送り制御能力をもつサーバと通信する。

ボットネットは、安全ではないネットワークやコンピュータさらに接続されたデバイスをスキャンするマルウェアを介して自ら感染を世界中に広める。ボットネットが十分な数のデバイスに感染すると、犯罪者である悪意あるアクターは、広範囲の不正な行為を命令できる。例えば、分散型サービス拒否（DDoS）攻撃や、ランサムウェアの増殖、フィッシング攻撃そして、ソーシャルメディアに投稿することで虚偽の情報を拡散させることができる[24]。

ボットネットによる脅威は、歴史上過去のいかなる時点よりも現在深刻になっている。2000 年代初期、犯罪者は主にボットネットを初歩的なサービス拒否（DoS）攻撃に利用し、恣意的にインターネット上にトラフィックを発生させ、標的となる Web サイトやネットワークを溢れさせ負荷をかけた。しかしコンピュータ性能や通信速度の向上など時間の経過とともに、彼らの能力も向上した。マルウェアを大量のデバイスに感染させることで、ハッカーはさらに大規模な不正行為を実施できる事を見つけた。2007 年「Storm Worm」と呼ばれたボットネットは、その集団に 5000 万台近くのコンピュータを集め、それらのコンピュータを使って株価の操作や個人情報を盗むなどの犯罪を犯していたことが判明した。2009 年には、一つのボットネットが驚くことに毎日 740 憶通もの迷惑メールを送付していたことがわかった[25]。そして 2011 年から 2013 年には、攻撃者はボットネットを利用して、世界中のボットネットノードから Web サイトにインターネットのトラフィックの波を送り、北米の銀行に DDoS 攻撃を立て続けに行った[26]。

現在、犯罪者は大規模なボットネットを利用して、DNS プロバイダーの Dyn を攻撃した 2016 年の歴史的な Mirai ボットネットのように、暗号通貨のマイニングから、DDoS 攻撃に至るあらゆる種類のサイバー上の犯罪に関与している。2016 年の Mirai ボットネットのマルウェアは、デフォルトログインでのクレデンシャルリストを使うことで、所有者が気づかずに、またデバイスが感染していることによるいかなる経済的損失を受けることなく、CCTV のビデオカメラやデジタルビデオレコーダーなど 400,000 個近くのエンドポイントのデバイスにアクセスし拡散した[27]。この攻撃により、ボットネットで引き起こされたトラフィック量は、主要な銀行に対する初期の攻撃の ***4 倍***で、利用者は一時的にオンラインの主要なプラットフォームとサービスにアクセスできなくなった。そしていくつか例をあげると、Airbnb、Amazon.com、BBC、CNN や Netflix など、企業のオンラインサービスの利用者に深刻な被害をもたらした[28]。

ほとんどのボットネットは Mirai の規模に達しない[29]が、多くの小規模なボットネットによる攻撃は、Web サイトやサービスを遮断させ、ランサムウェアを拡散し、ソーシャルメディアに虚偽の情報を拡散できる。残念なことに、自分たちでボットネットを構築する技術的な知識がない犯罪者は、小規模の攻撃機能を使ってより犯罪を犯しやすくなっている。オンラインの市場では、初心者のハッカーが「サービスとしてのマルウェア」（MaaS）と呼ばれる個人の要望に合った独自のボットネットを設計するツールキットを購入できるダークウェブが見つかっている。もし犯罪者としての顧客が、ボットネットを開発または購入したくない場合、彼または彼女は、1 日たった 0.66 セントで一つのキットを借りることができる[30]。そして犯罪者は、例えば DDoS 攻撃について、たった 20 ドルで攻撃を実行できる機能を購入できる[31]。それは盛況かつ革新的な市場だ。例えば Mirai 攻撃のすぐ後に、ボットネットの作成者は、Mirai のソースコードをオンライン上で公開し、それ以来、触発された多くのハッカーたちはオリジナルの Mirai コードから亜種を作りだした。

悪意あるアクターは常にボットネットの新しい使い方を模索している。例えば、ハッカーはボットネットを使って、150 以上の国々で 200,000 台以上のコンピュータシステムを機能しないようにさせ、銀行、病院、大学そして他の機関でコンピュータを遮断させるか、犯人に身代金を払わせるようにさせる悪名高き WannaCry ランサムウェアを復活させようとした[32]。マルウェアが未登録のドメインを問い合せていることにセキュリティ

研究者が気付いたことで、WannaCry の拡散は収まった。ドメインを登録することで、ボットネットを遮断する「キルスイッチ」の効果があった[33]。ハッカーは、一時的に抑えこまれたランサムウェアを復活させることを目的として、「Mirai ボットネットのコピー」を使って執拗にこのドメインを攻撃した[34]。その間に、WannaCry より一層高度化したランサムウェアの Petya が表れ、世界中に大混乱をもたらし、Petya を基にしたマルウェア（NotPetya と呼ばれる）はすでに 100 億ドル以上の被害をもたらしている[35]。

残念なことに、インターネットに接続する人々、事業、デバイスの数が増えるほど、ハッカーは力をつけ、より大掛かりな悪意ある攻撃をしかけ、それによって利益を得る可能性が高まっている。上記で述べたように、インターネットに接続して使われるデバイスの合計数が世界で何十億個に達することと、サイバー犯罪のグローバルでの被害額が数兆ドルに達すると予想されることは偶然の一致ではない。ボットネットの攻撃により、産業規模での損失をひきおこしている。明らかに経済的損失をひきおこすことに加えて、悪意あるボットネットの機能によりデジタル経済における根本的な信用と信頼を損なう恐れがある。被害総額を定量化できないが、汚染によって私たちが吸う空気、そして私たちが飲む水の信頼を損なうように、ハッカーの行為による悪影響は、デジタル経済の効果を損なう。

高度な多様性と複雑さをもち、相互に依存するグローバルなインターネットのエコシステムにおいて、ボットネット対処の根本的な課題は、インターネットの本質が非階層で常に接続している状態であることだ。しかし、官民共にーステークホルダーだけでは、このシステムを管理することはできないにも関わらず、私たちはすべてをつなげるインターネットに依存している。悪意あるボットネットに対抗することは、古典の「共有地の悲劇」的な課題である。もし全ての人がインターネットという共有された中で利害関係を持ち必然的に接続されているが、誰も管理できない場合、すべての人が利用する基本的な機能を脅かす悪意あるボットネットを取り除く責任は誰にあるのか。

答えとしては、共有地であるインターネットからボットネットを除去する利他的な目的からだけでなく、全てのステークホルダーが責任を持つべきで事である。エコシステムの全てのステークホルダーには、悪意あるボットネットを軽減する自己本位的な利害関係がある。ボットネットは、全ての ICT の製品やサービスで利用するインターネットを攻撃するために使われ、そして、ボットネット攻撃により企業に被害を与え、企業活動に直接影響が及ぶか、または評判に傷がつくことになる。

このエコシステム対策の過去の取り組み - 広範囲の課題

このガイド作成を担当したのは、サイバー脅威からエコシステムを守るために、自主的なプラクティスを先駆的に取り入れた企業である。例えば、2012 年、米国のコミュニケーションセクターのリーダー達は、啓発、検知、通知、改善そして協力を通して、ボットネット根絶に向け有意義な行動をとるために、ISP に対するボットネット対策の行動規範を作成した。一方、テクノロジーセクターは、グローバルなプロバイダーのハードウェア、ソフトウェア、デバイス、システム、そして関連サービスが提供するセキュア・バイ・デザイン、マネージド・セキュリティ・サービスそしてライフサイクルサポートから利便性を受けている。

しかし、エコシステム全体に課題が山積している：

- 先進的機能を持つ多くの ISP とインフラプロバイダーは、ボットネットの脅威を軽減するためのセキュリティ強化に向け、引き続き市場をけん引し続けている。ボットネットの規模が拡大し複雑さが増すにつれ、インフラネットワークを運営する企業は、増加する大規模な攻撃から顧客を防御することを強化している。しかし、全てのステークホルダーがエコシステムにおいてさらに効率的に運営できるようになるとより小規模のプロバイダーはベースラインに到達するために、通常は技術指導さらに人材が必要になる。

- ソフトウェアは、全てのグローバルの商業と政府のプロセスに不可欠である。デジタル経済における多様なステークホルダーは、安全なソフトウェアにますます頼るようになる。依存度が高まっていることは、さらに高度な手段を開発するよう悪意あるアクターを刺激する。そのような状況に対して、責任ある企業はソフトウェア向けの安全なプラクティスを開発し、プロダクトサイクルの各段階での基本的なセキュリティを設定している。これらのプラクティスは、中小企業の開発者でも見習うことができる。

- 開発、展開における驚異的なイノベーションとインターネットに接続されたデバイスシステムは、両刃の剣である。つまり世界中でインターネットへの接続が可能な何十億個もの新しいデバイスが導入されることで、サイバー上の犯罪者に同じ数の新しいエントリーポイントを利用させることになる。上記に述べたように、これらのデバイスの多くはセキュリティの設計あるいは展開を全く念頭に置いていなかった。そして個々の脆弱性を軽減できるシステム内にセキュリティを展開していない。

- 家庭または企業におけるコンピュータとインターネットに接続されたデバイスは、デバイスの全ライフサイクルを通して安全性を確保しなければいけない。そして恐らく最も重要なことは、デバイスを最初に導入し設定する時である。しかし適切に導入し設定されることはまだとてもまれであるので、製品は最も利用可能なセキュリティを実行できないことが多い。

- 官民セクター共にあらゆる種類の企業は、ボットネットそして自動化した分散型の脅威の被害者でも、ボットネットを拡散させる宿主でもある。これらの企業は市場でさらに利用可能となっているセキュリティソリューションを適用することで、ボットネットから防御できる。

このような状況を背景に、過去の政策的な取り組みでの共通した誤りは、森で手に届く近くの病んだ木々だけを取り除こうとするのと同じように、政策決定は、エコシステムの 1 点または 2 点の構成要素だけに集中してきた。結果として森は病んだ木々で一杯になる可能性が高くなる。同様にボットネットの軽減には、より慎重で包括的なアプローチが要求される。この複雑なエコシステムのそれぞれの部分は、個々にそして協力して、自分たちと他者の責任をもって、自身の責任と他社がどのように協力していくかをよく理解しなければならない。そして、現在の線引きが不明確またはわからない場合、ステークホルダーは協力して明確にしなければいけない。ボットネットと対抗するためにそのような作業をせず戦略をもたないと、パズルのたった 1 つまたは 2 つだけに注目した、非現実的な方針のソリューションの誤った考えに戻ってしまうだろう。例えば、ISP は簡単にすべてのボットネットを遮断する、または何十億個のデバイスは普遍的に安全に製造される、あるいは消費者はあらゆるテクノロジーの知識を持ったユーザーであるべき、などの考えである。

そのような単純なソリューションによってこれまで失敗してきたし、将来これ以上成功することはありえない。代わって、世界中の民間セクターの消費者、企業の市場、学術、市民社会、政府を介して、何十億の人々と自動化された要素で構成されたこの複雑なシステムにおいて、セキュリティを強化するために、各レベルで軽減対策を実装しなければいけない。それは国際ボットネット対策ガイドが意図することである。

現在は何が違うか？

このガイドは、いかなる政府の要件または一国だけでは対応できない今日の市場での課題に対して、現実社会で現在利用できるソリューションを提供する。私たちはボットネットの脅威を劇的に減らすために、多様な産業にわたるグローバルな企業とコラボレーションを進行中である。下記の一致した基本原則を念頭に置き、急速に拡大するグローバルな脅威、エコシステム全体の脆弱性、そして能力を高めている果敢な攻撃者に関する分析によりこのガイドを作成した：

- セキュリティには、地域や国家の権限によって異なる規制されたコンプライアンスの仕組みではなく、強力なグローバルのマーケットの力に牽引され、軽減しなければいけないサイバー脅威と同様に、機敏かつ適応力の高い、ダイナミックで柔軟性のあるソリューションが必要である。

- セキュリティは、インターネットとコミュニケーションのエコシステムにおいて、全てのステークホルダー間で責任を共有する。特定の選ばれた組織やステークホルダー間で、安易なソリューションを求めるのではなく、政府と産業界のステークホルダーは、すべてのプレイヤーが責任感を高めるソリューションを開発しなければいけない。

- 悪意あるアクターとボットネットから得る利益に対して、協力して行動する責任あるアクターが貢献するには、セキュリティは政府、サプライヤー、プロバイダー、研究者、企業、消費者間で相互に有益なチームワークとパートナーシップを持つことが重要になる。

4. グローバルなインターネットとコミュニケーションのエコシステムの概要

上記に述べたように、デジタル経済は複雑なグローバルなインターネットとコミュニケーションのエコシステムによって実現可能となり稼働し続けている。そしてエコシステムは、各システムそれ自体は大変複雑で、全てのシステムに相互依存する数々のシステムで構成されている。これらのさまざまな構成要素はすべて、ボットネットや自動化された分散型の攻撃によってもたらされる脅威に対するエコシステムの脆弱性と、その強靭性の一部を構成している。

インターネット及び関連するコミュニケーションのエコシステムからなる「システムのシステム」によって、全てのステークホルダーに均一に適応する一連のガイダンスを提供することは困難である。政府と民間セクターによる様々な主要な報告書では、各フォーラムの目的と目標に合わせて似ているが異なる分類を用いて、インターネットとコミュニケーションのエコシステムを定義し説明している[36]。エコシステムをどのように理解するべきかの視点を競うことに重点を置くのではなく、これらの定義によってお互いを補完し強化していくことが目的である。

このガイドも例外ではない。私たちはステークホルダーの構成グループ間のボットネット対策プラクティスの認識と実装を容易にする方法でエコシステムの構成要素を分類する。具体的には、このガイドはプロバイダー、サプライヤーそして利用者を下記のように 5 つの種類で構成した：

1. インフラ
2. ソフトウェア開発
3. デバイスとデバイスシステム
4. 家庭と中小企業のシステム導入
5. 企業

確かに、この複雑なエコシステムを定義しようとすると、実際のものであれ、知覚されたものであれ、何らかの方法で過小評価されるリスクを伴う。例えば、上記に記載された 5 つのカテゴリーのいずれも、カテゴリーの組み合わせを必要とするいくつかのユビキタスなプラットフォーム（例えば、大規模なソーシャルメディアのプラットフォーム）に合理的に適応できないことが、経験から明らかになるかもしれない。このような理由のために、システム間の境界は進化し続けているという想定で、柔軟性を持ってこの分類をとらえるべきである。

5. エコシステムの構成要素のプラクティスと機能

A. インフラ

このガイドの目的に対して、「インフラ」は接続性と運用性を可能にするすべてのシステムに言及する。つまり、インターネットサービスプロバイダーの設備、基幹システム、クラウド、ウェブホスティング、コンテンツデリバリー、ドメインネームシステム、そしてサービスだけでなく、形あるものからデジタルコンセプトへのインターネットの進化を反映する Software-Defined Network（SDN）とシステムを含む。私たちは現在のインターネットとコミュニケーションのエコシステムにおける、多様なインフラに対するベースラインプラクティスと先進的な機能を推奨する。

インフラの種類

インターネットサービスプロバイダー
インターネットサービスプロバイダー（ISP）はケーブル、DSL(デジタル・サブスクライバー・ライン)、ダイアルアップ、ワイヤレスなどを使って、顧客にインターネットにアクセスする手段を提供する組織である。ISP は、インターネットの基幹システムとなる、ネットワークのアクセスポイント、公共のネットワーク施設を通してお互いに接続される。ISP は、遠く離れたところでも数秒で情報を伝達するために、相互に接続された基幹システムの構成要素として膨大なシステムを使う。ISP は、Web サイトホスティング、ドメイン名登録、バーチャルホスティング、ソフトウェアパッケージ、そして E メールアドレスなど、インターネットへのアクセスだけではないサービスを提供するかもしれない。多くの ISP は、マネージド・セキュリティ・サービスを含む、ボットネット攻撃を減らすために設計されたサービスを提供する。それによってプロバイダーは、顧客の脅威を軽減する積極的な役割を果たす。ほとんどのブロードバンド ISP は、サービスの一部としてアンチウイルスを提供し、多くが追加料金なしで顧客に感染を知らせる。

インターネットバックボーンプロバイダー
インターネットバックボーンは、広範囲に接続されたコンピュータネットワークの集まりであり、通常は商業、政府、学術、その他のネットワークのアクセスポイントによって接続される。これらの組織は、通常、通信能力を高めるために基本的に束ねられた光ファイバーを集めた大型の高速ネットワークと光ファイバー幹線を制御する、それらは遠く離れたところでもより速いデータスピードと広い帯域を可能にし、電磁妨害に対して免疫性がある。バックボーンプロバイダーは、高速インターネットアクセスを顧客に提供しながら、インターネットへのアクセスと相互に ISP を接続させる ISP を提供する。最も規模の大きいバックボーンプロバイダーは「Tier 1」プロバイダーと呼ばれる。これらのプロバイダーは、国や地域に限らず、世界中の国々をつなげる広大なネットワークを持つ。いくつかの「Tier 1」プロバイダーは、ISP そのものでもあり、そして規模が大きいため、小規模の ISP に彼らのサービスを販売している。

DNS プロバイダー
ドメインネームシステム（DNS）は、基本的に世界中にある何百万のサーバにコピーし保存された IP アドレスに関連するドメイン名の住所録である。ユーザーが Web サイトを訪れるために検索バーにドメイン名をタイプすると、コンピュータが DNS サーバに情報を送付する。このサーバ（リゾルバとも呼ばれる）は、通常ユーザーの ISP により運用される。するとリゾルバは、IP アドレスとドメイン名を一致させ、一致する IP アドレスをユーザーのブラウザに送り返すことで、Web サーバにつなぐことができる。

DNS プロバイダーは、そのような DNS 解決サービスを提供する組織である。彼らはドメイン変換、ドメイン検索、そして DNS 転送など、最も一般的な DNS 機能を提供する。DNS プロバイダーは、また最新の情報を提供するために、定期的に彼らのネームサーバを更新している。

コンテンツデリバリネットワーク

コンテンツデリバリ（またはディストリビューション）ネットワーク（CDN）は、地理的に分散したデータセンターとのプロキシサーバのネットワークである。CDN とは、ソフトウェアのダウンロード、Web とモバイルコンテンツのアクセラレーション、そしてビデオストリーミングなど、コンテンツデリバリサービスの様々な種類を表現するときに使われる名称である。CDN ベンダーは、DDoS 攻撃の防御そして Web アプリケーションファイアウォール（WAF）のようなサイバーセキュリティ業界にも及ぶ。CDN はユーザーが Web ページをリクエストし、コンテンツがスクリーンに表れるまでの間に起こるレイテンシと呼ばれる遅延の問題を解決するよう設計された。遅延の時間は通常エンドユーザーとホスティングサーバの距離によって異なる。この待機時間を短くするために、数か所にあるコンテンツのキャッシュバージョンを保存することで物理的距離を短くし、サイトレンダリングの速さと性能を高める。そしてそれはポイントオブプレゼンスまたは PoP として知られ、各 PoP は、コンテンツ配信を担当するキャッシュサーバの近くにエンドユーザーを接続しする。Web サイトのコンテンツを一度に多くの場所に保存することで、企業は遠く離れたエンドユーザーでもより多くのコンテンツを利用できるようにする。

クラウドとホスティングプロバイダー

インターネットホスティングサービスは、顧客が世界中の人々と組織に対してインターネット上のコンテンツにアクセスできるようにする。近年、ローカルサービスまたは個人のデバイスに代わって、オンラインで提供されるリモートサーバを使うクラウドホスティングサービスの採用が増加することで顧客に拡張性があり、より安全なホスティングサービスへのアクセスを提供している。クラウドで提供されるソフトウェア、インフラ、そしてプラットフォームは、定期的に使用料を払うことでアクセスすることができ、顧客は幅広い範囲のコンピュータ機能を実行できる。クラウドネットワークが分散化しているために、それらは通常多数のネットワークの構成要素の障害に耐えることができる。この設計機能によって、クラウドは幅広く分散されたボットネットに対して強靭性があり、さらに軽減機能を提供する。本質的に、クラウドサービスは ISP が提供するインフラの外側にセキュリティの追加層を提供する。ボットネット攻撃の範囲が拡大するにつれ、この防御レイヤーはますます有効になる。なぜならクラウドは攻撃対象からの ISP に対して上流にあり、攻撃元により近い問題を緩和できる。クラウドセキュリティサービスは補完機能となり、ボットネット軽減における ISP の役割が減ることはない。

インフラのベースラインプラクティスと先進的な機能

CSDE のメンバーは、ボットネットに対して、自身のネットワーク、顧客のネットワーク、グローバルなエコシステムの強靭性を強化するために重要なステップをとる。政府と業界の専門家たちは、エコシステムの複雑さからたったひとつのツールでは脅威を軽減する効果はなく[37]業界が新たな脅威、新しい技術とツールに適応する十分な柔軟性を持ち続けることが重要であることを認識した。しかし、いくつかのベースラインプラクティスは、すでに DDoS 攻撃のようなボットネットによる攻撃の影響を軽減することが証明されており、それらのプラクティスはエコシステムを介して実装されるべきである[38]。下記に、分散型の脅威からエコシステムを防御するために業界リーダーが利用できるベースラインプラクティスのみならずより先進的な機能を示す。

1. 悪意あるトラフィックと脆弱性の検知

ボットネットのような分散したサーバ脅威を軽減する最初のステップは、攻撃から守るべき資産と、これらの資産を攻撃にさらす可能性がある潜在的な脆弱性（例えば、攻撃対象領域）を確認することである。さらに企業は各々の確認された脆弱性に対して最新の突破口（例えば、攻撃ベクトル）に関する情報を常に取得するようにしなければいけない。

プロバイダーは、業界内とセクターにわたって信頼できる第三者機関のデータフィードと情報共有の仕組みを活用できる。さらに、多くの国において政府が情報を共有する仕組みによって、機械的な速さで官民セクター間で瞬時に情報を共有できる[39]。

ベースラインプラクティス：プロバイダーは、定期的に更新されるデータベースで既知のマルウェアの種類をチェックする。責任ある企業は、新しいマルウェアの情報をセキュリティベンダーと研究者と適時に共有することで、検知する取り組みに貢献するかもしれない。

先進的な機能:豊富な人材を採用できる企業は、マルウェアを検知するためにヒューリスティックスと特異な行動を分析するセキュリティ専任の研究者を採用できるかもしれない。そして研究者が発見した内容はステークホルダーと共有できる。

a) シグネチャ分析

セキュリティの専門家がマルウェアに遭遇すると、彼らは固有のパターンまたは「シグネチャ」（例えばマルウェアのコードやエクスプロイトコードの一部）を探す。シグネチャを基にした分析については、どこに脅威があったとしても脅威を特定できるように、更新したマルウェアシグネチャのデータベースに誰でもアクセスして使えるようにする。これはアンチウイルスソフトウェアと侵入検知システムの一般的な分析の種類で、ネットワークで最も悪意ある脅威を検知するために使われる。シグネチャ分析は一般に使われるとはいえ、より巧妙な手口を使う悪意あるアクターは拡散するたびにマルウェアの特質を変えるので、この技術を使っても脅威を検知できなくなる。本物のウイルスのように、マルウェアはホストからホストに移動しながら順応し進化する[40]。シグネャ分析に明らかに限界があるのは、マルウェアに対して予備知識が必要なためである。その分析が効果的であるかは、エコシステムを通してシグネチャ分析が随時更新されその情報が共有されるかに左右される。理想的には、シグネチャ分析はこの技術固有の限界を克服するために、下記に述べるヒューリスティック分析あるいは挙動分析などの種類の分析と組み合わせるべきである[41]。

ベースラインプラクティス：プロバイダーは、シグネチャデータベースの更新を確認し、マルウェアの情報共有に貢献すべきである。

先進的な機能：プロバイダーは、より良い結果を得るためにコードヒューリスティック（下記に述べる）とネットワークとトラフィック挙動（この点も下記に述べる）の分析と組み合わせることができる。

b) ヒューリスティック分析

ヒューリスティック分析は既知の問題の兆候をコードで調べることでマルウェアを検知する。コードが既知のマルウェアと完全に一致していなくても、潜在的に悪意のあるものとしてフラグを立てることができる。ヒューリスティック分析では、コードが疑わしいかどうかを決定する多くの異なる手がかりを検索する。静的ヒューリスティック分析では、潜在的に悪意のあるコードがデータベース内のマルウェアのコードと比較され、十分な類似性があれば、コードにフラグが付けられる。誤検知の可能性があるとはいえ、進化する未知の脅威と対抗するためにはヒューリスティック分析は、シグネチャ分析よりはるかに効果的である。時としてコードを安全に解体するために、科学者はマルウェアと思われる疑わしいコードを「サンドボックス」と呼ばれる仮想マシンの中に格納し、他のホストへの拡散を防ぐこともある。これは動的ヒューリスティック分析として知られている[42]。

先進的な機能：プロバイダーは静的と動的ヒューリスティック分析の両方を組み合わせて使うことで、未知の脅威を検知できる。プロバイダーは研究者チームとともに、脅威を軽減する効果的戦略を決定するために、サンドボックスの中で疑わしいコードを分析し、エコシステムにおけるステークホルダーと共有できる。

c) 挙動分析

シグネチャ分析とヒューリスティック分析ともマルウェアコードに注目する一方、挙動分析はマルウェア感染の「症状」に注目する。ネットワークトラフィックが予想外の挙動を見せる時、最初は挙動の変化がどうして起こったか明確ではない。しかし、例えば権限の昇格を得ようとする、またはソフトウェアあるいはシステムのファイルと変則的な方法で相互作用する時、ソフトウェアの一部がマルウェアかもしれない既知の指標がある。しばしば挙動分析は医療の専門家に類似している。医者は問題が何であるか理解する前であってもその人が病気である事がわかる。挙動分析は、まだ特定できておらずシグネチャもわかっていない未知の脅威を発見することで、別の種類の分析を補足し完全なものにする[43]。

先進的な機能：プロバイダーは異常なトラフィックパターンを検知し組織に蓄積された知識を活用するためにアルゴリズムを利用できる。あるいは必要であれば、異常なトラフィックの根本的な原因を診断するために、外部のセキュリティ専門家を雇うことができる。

d) パケットサンプリング

ネットワークを介する膨大な量のデータの流れを解明するために、多くの大手プロバイダーはパケットサンプリングと呼ばれる技術を利用する。この技術はルータで捉えたネットワークトラフィックのサンプルから、トラフィックの流れを解明する熟練した技術が必要である。検査するデータ量を減らすことで、規模が大きくスピードが速い現在のネットワークでも、大規模なネットワークのオペレーターは、パケットサンプリングによってトラフィックを分析できる。

ベースラインプラクティス：プロバイダーは少なくとも検査用のパケットを選択する類似乱数でパケットを選ばなければいけない。このサンプリングは、内容に依存しない方法で実行できる。

先進的な機能：プロバイダーは確率に重点を置きトラフィックの変化に適応するより複雑なサンプリング技術を活用できる。プロバイダーは、マルウェア脅威に関連する特定のコンテンツを検査するかもしれない。

e) ハニーポットとデータレベルのデコイ

上記に述べたネットワークレベルのソリューションに加えて、プロバイダーは攻撃者をおびきよせるデータレベルのデコイ、例えばハニーポットのような「罠」を利用するかもしれない。ハニーポットは悪意あるアクターにとって価値があるように見せる、ネットワーク内にある典型的なデータやシステムのことで、彼らがアクセスしようとするとブロックするか監視する。注目すべき事はハニーポットそしてデコイはサードパーティーによって展開される点で、プロバイダーは潜在的な犯罪行為またはサイバー攻撃を見つけるためにそのようなサードパーティーと連携するかもしれない。犯罪行為を見つけるのに有効なために、ハニーポットは法執行機関のおとり捜査に使われる。

ベースラインプラクティス：ハニーポットは限られた機能と情報収集機能を持つが、実際に侵入がおこるリスクが低いので、プロバイダーは低対話型のハニーポットを展開できる。ハニーポットは攻撃者をだまし彼らに関する情報を収集するために、侵入が成功したように見せかける。

先進的な機能：プロバイダーは高対話型のハニーポットを展開することで攻撃者についてより多くを知ることができる。このシナリオでは、攻撃者は模倣ではなくプロバイダーの実際のシステムと対話し、しばしば未知だった攻撃ベクタを明らかにする。攻撃者に多くをさらすために、高対話型のハニーポットは本質的にリスクがより高いが、攻撃者の手法をさらに明らかにできる。

2. 分散型の脅威の軽減

悪意あるトラフィックや潜在的脅威を検知することを考慮すると、インフラのプロバイダーはまた、これらの課題に対処するために下記に述べるように多様な軽減方法を適用できる。

ベースラインプラクティス：プロバイダーはイングレスフィルタリングを用いるべきである。すなわちインバウンドのトラフィックのレートを制限できるフィルターを適用する。プロバイダーはまた彼らのネットワークのトラフィックをシェーピングし、ネットワーク管理ツールとしてブラックホールそしてシンクホールを用いて適切な対応するべきである。

先進的な機能：より多くの情報にアクセスできる企業は、イングレスフィルタリングに加えてイグレスフィルタリングを使うかもしれない。そしてそれによってアウトバウンドとインバウンドのトラフィックの両方のレートを制限する。彼らは攻撃ベクタを減らすためにアクセスコントロールリスト（ACL）を使用するかもしれない。企業はトラフィックをシェーピングする際、例えば Selective Black Hole を配備して、サービスの混乱を最小限にする手段をとるかもしれない。トラフィック管理オプションを増やすために、BGP Flowspec のような技術を用いるかもしれない。彼らは悪意あるボットネットの停止措置をとるために官民と連携できる。また彼らはトラフィックのスクラビングや DDoS 攻撃の防御などの商用サービスを提供するかもしれない。

a) フィルタリング

ボットネットを軽減する際に複雑化させる要因の一つは、悪意あるアクターが IP スプーフィングを使って、悪いトラフィックを実際の発信元ではなく、どこか他から来ているように見せかけることだ[44]。プロバイダーのネットワークに侵入した時（例えばイングレスフィルタリング、BCP38 と BCP84）[45]、悪いトラフィックを取り除くことによって、プロバイダーはスプーフィングの影響を減らすことができる。従って DDoS 攻撃の実行をより困難にする。このプラクティスの実施で即座に効果が表れるので、Internet Engineering Task Force（IETF）はイングレスフィルタリングをベストプラクティスとして認識している[46]。イングレスフィルタリングは、例えば顧客の構内設備など、ネットワークのイングレスポイントでより効果がある点は注目すべきである。が、ネットワークエクスチェンジポイントではより困難になる。

さらにプロバイダーは通常悪意あるトラフィックを識別することはできるが、BCP38 のような技術は、企業を含めて自身の IP アドレス空間を運営するあらゆる組織で使用されるべきである。ISP のようなプロバイダーは、多くの IP アドレスを顧客に割り当てる。そして顧客は順番に自身のフィルタリング機能を操作し、また BCP38 に従う必要がある。

さらに、彼らのネットワークの境界にフィルタリングを展開することで、エコシステムの端から出てくるトラフィック、あるいは端から入ってくるトラフィックを監視し、ステークホルダーへの被害を減らすことができる。イグレスフィルタリングは、イングレスフィルタリングに置き換えることはできないが、補完的な解決策である。イグレスとイングレスの組み合わせは、プロバイダーのレジリエンスを強化させるために最も良い方法である[47]。

最後にネットワーク設定の際、その送信元と送信先、IP プロトコル、ポート、EtherType や他の特徴などのパラメータをもとに、トラフィックフローを識別するために ACL が使われる。一般的な例では、安全性が低いインターフェースからのトラフィックは、安全性が高いインターフェースへのアクセスができない[48]。ある状況では、マルウェアがネットワーク侵入を可能にする攻撃ベクターをさらに制限するために、ACL はアクセス権限のあるアカウントを個々のユーザーに設定するかもしれない。

ベースラインプラクティス：プロバイダーは、ネットワークに入ってくる悪意あるトラフィックの量を減らすために、ネットワークイングレスポイントで、インバウンドトラフィックをフィルタ（イングレスフィルタリング）するべきである。フィルターは、ネットワークリソースを圧倒する攻撃がおきた場合、インバウンドトラフィックの量を制限する事ができなければいけない。

先進的な機能：理想的には、プロバイダーはインバウンドトラフィックに加えて、アウトバウンドトラフィックをフィルタ（イグレスフィルタリング）すべきである。そしてアウトバウンドかインバウンドに関わらず、トラフィックの量を制限することができなければいけない。このハイブリッドソリューションはより多くの量のトラフィックを守ることができ、それによって同業他社に対してエコシステムにおいてプロバイダーが責任を果たすことができる。さらにプロバイダーは攻撃ベクターを減らすために ACL を使うことができる。

b) トラフィックシェーピング

潜在的に悪性のあるトラフィックを特定した時、プロバイダーは結果として通常トラフィックをドロップするか、データ率が異常に高くなった時、遅延させる技術を使うことで、トラフィックを安全に管理できる。これら両方の技術は特定な状況で有効で、おそらく包括的トラフィック管理の戦略の一部となるかもしれない[49]。

ベースラインプラクティス：プロバイダーはネットワークでトラフィックをシェーピングする適切な対応をしなければいけない。最低でも、プロバイダーは攻撃者による目標の到達からトラフィックを守る「ブラックホール」を展開できるはずだ。正当なサービスの混乱を防ぐために、規定の地理的領域内のみでトラフィックのリダイレクトまたはドロップによる努力をするべきである。

先進的な機能：より多くの人材をもつプロバイダーは、正当なトラフィックに多くの混乱を起こすことなくトラフィックをシェーピングできる。例えば、商用のスクラビングセンターでは、悪意ある成分を選別して取り除き正当なトラフィックを送信先まで送ることで、トラフィックを清浄する。小規模なプロバイダーは大手のプロバイダーと提携し、これらのサービスを顧客に提供するかもしれない。

c) ブラックホール

ブラックホールは、特定のオンライン上の送信先に向かっている全てのトラフィックをドロップする技術である。この技術の一般的な方法は Remote Triggered Black Hole（RTDBH）であり、通常攻撃元に最も近い上流ネットワークにおいて、被害にあうかもしれない対象のネットワークに到達する前に悪意あるトラフィックをドロップする。

ブラックホールは、悪意あるトラフィックが送信先に到達するのを防ぐのに有効であるとはいえ、明らかな欠点は、正当なトラフィックが送信先に到達することができない事で、それは悪意あるアクターの明らかな目的であるかもしれない。この問題を最小限にするために、プロバイダーは他の地域からのトラフィックが目的地に到達するのを許可するが、特定の地理的地域（国または大陸など）からのトラフィックをドロップする Selective Black Hole として知られる技術を使用できる。

ベースラインンプラクティス：プロバイダーは彼らのネットワークを防御するためにブラックホールを活用するべきである。理想的にはプロバイダーが正当なトラフィックへの混乱を最小限にするべきであるが、より粒度の細かいツールが利用できないまたはうまく機能しない場合、少なくとも基本的な RTDBH を使用するべきである。

先進的な機能：プロバイダーは他のプロバイダーと協力することで、監視とフィルタリングの PoP の両方について、ブラックホールの効果を高めることができる。さらに、プロバイダーは特定の地理的地域を対象とした正当なトラフィックの混乱を最小限にするために Selective Black Hole を使用できる。

d) シンクホール

シンクホールは、特定の IP 範囲のトラフィックを指定のサーバ（「シンクホール」）に送信するのに対して、特定の IP 範囲以外のトラフィックは通常通り送信する技術である。シンクホールの目的は、調査と軽減を目的としたボットネットの捕獲である [50]。シンクホールは、ボットネットを構成するマルウェアに罠をしかけて、ポリシールーティングまたは他のルーティング手法を用いてしばしば達成できる。そして法執行機関または研究者がシンクホールを調査する。シンクホールで捕らえられたマルウェアが、コマンド&コントロールサーバと通信しようとする時、セキュリティ専門家はマルウェアが情報を配信するマシンの IP アドレスを追跡できる。その結果として犯罪行為を見抜くことができる。プロバイダーは、またマルウェアとコマンド&コントロールサーバ間の通信を完全に断ち切る事ができる。世界中の多くの国で何十万ものインターネットに接続が可能なシステムを利用するボットネット攻撃に対して、シンクホールはボットネットの大規模な停止措置を行うために不可欠である。

ベースラインプラクティス：インバウンドの悪意あるトラフィックをリダイレクトし、分析と情報共有を目的として、プロバイダーのネットワークへの脅威に関する情報を集めるために、プロバイダーはシンクホールをネットワーク管理ツールとして使うべきである。

先進的な機能：業界のリーダーたちは、プロバイダーや法執行機関と協力して、エコシステム全体への脅威を破壊し情報を収集するために、シンクホールを利用できる。プロバイダーはまた、多くの管轄を越えて関係当局やステークホルダーと効率的に連携することで、国際的な法執行機関の活動を支援できる。

c) スクラビング

スクラビングソリューションは、通常ネットワークトラフィックを分析し、DDoS 攻撃を含めて悪意あるトラフィックを取り除く専用のスクラビングセンターによって実装される。他のソリューションと比較してスクラビングはリソース集約型なので、いくつかの大手プロバイダーは商用サービスとしてスクラビングを提供している。トラフィックをドロップする代わりにセンターにリダイレクトすることによって、スクラビングは正当なトラフィックを目的地へ送付することに成功する確率が高い。このことは、多くの企業にとってブラックホールやシンクホールに代わり、スクラビングはより望ましい選択肢となる。

先進的な機能：スクラビングセンターは、単に大量のフラッド攻撃を制限するだけでなく多くの種類の攻撃をフィルターすることで、プロバイダーまたは顧客の防御のために、重要な防御層を強化できる。例えば、センターは SSL（暗号化された通信路）を基にした攻撃を防御する技術を統合するかもしれない。

f) BGP flowspec

BGP flowspec は、動的な技術で、プロバイダーは多様で異なる軽減オプションを即座に展開でき、それによって専門家が状況に応じて判断できる。ブラックホールのみをサポートするルータと異なり、flowspec はトラフィックのシンクホールなどのオプションを追加することができ、それによって専門家が確認できる、言い換えるとシェーピングしたトラフィックを定義した割合で進めさせることができる [51]。

先進的な機能：プロバイダーは BGP flowspec を使うことで、従来の画一的なソリューションに代わって、境界ルータに個別に指示できるようにする。BGP flowspec では、flowspec のオリジネーターの適切な検証のもと、ルータはトラフィックをドロップするか、トラフィックをリルートする、あるいはトラフィックのレートを制限するよう指示できる。

3. 顧客とピアとの連携

ボットネットや分散型の脅威から復旧するには、プロバイダは顧客やピアとの連携を確保するために進捗を知らせることが必要かもしれない。ユーザー通知の有効性は、明らかにユーザーに大きく左右される。 M3AAWG に委託された調査によれば、ユーザーと連絡をとるために最も効果的な方法は、電話と郵便である事がわかった[52]。他に利用可能なそして利用すべき方法は、E メールと Web サイトでの通知だ。利用者に連絡をとる別の方法は「Walled Gardens」で、このアプローチではプロバイダーが決定した具体的な手順を踏むまで、利用者にオンラインサービスへのアクセスを制限する。いくつかの国では、このような新しい種類のアプローチは、法的あるいは公共の政策上の懸念を提起した[53]。ピアは顧客と同じ多くの方法で通知を受ける。プロバイダーとピア間の関係が確立していれば、通知はより効果がある。業界の主要なステークホルダーと親近感をもつことは、プロバイダーにとって有益だ。そして緊急の場合、最初に儀礼的な挨拶をする必要がない。

ベースラインプラクティス：承諾した使用方針に違反したり、不正な行為に関わった顧客やピアに、プロバイダーは通知すべきである。もし顧客またはピアのトラフィックをブロックする場合、（1）文書または電話でメッセージを送りかつ（2）E メールもしくはユーザーアカウントの Web ページで通知する。顧客またはピアにブロックされていないコミュニケーションチャネルを介して、どのようにプロバイダーに連絡をとるか明確な指示が提供されるべきである。

先進的な機能：訓練を受けたスタッフと専門の人材を持つプロバイダーは、消費者が公正な手段でサービスを利用する時にめったにサービス利用を中断されないよう誤検知率を減らす事ができる。

4. ドメイン差し押さえと停止措置の対処

法執行機関には、悪意のあるボットネットや犯罪行為者を効果的に緩和するために近年使用されている特定のツールがあり、ある程度の成功を収めている。 犯罪者が不正な目的（例えばボットネット攻撃）を実行するために、特定のドメインを使う明らかな証拠がある時、関連する法律に沿って、プロバイダーは法執行機関の強制命令に従いドメインの停止措置をとる。悪意あるアクターに対して、現実的な結果をもたらす法執行機関の活動が、対処療法ではなく、ボットネットや DDoS 攻撃の根本原因に対処する唯一の解決策だ。法執行機関のこの種の活動では多くの人材が必要で、しばしば広範囲のフォレンジックが必要である。また大規模なドメイン差し押さえには国際的に連携した取り組みが必要かもしれない[54]。 例えば 2016 年、Avalanche ボットネットに対して停止措置をとり、世界中のインターネットとコミュニケーションのエコシステムに散在する 800,000 個以上のドメインの制御を差し押さえるために、プロバイダーは 30 か国以上の政府関係者と協力した[55]。

ベースラインプラクティス：プロバイダーは、法執行機関やセキュリティ研究者のために、連絡先のリストを容易に入手できるようにしておくべきである。また、プロバイダーは法執行活動をどのように支援できるか、支援できないかについて、明確な方針を持つべきである。

先進的な機能：通常、業界リーダーは法執行機関を支援するためのより多くの手続きと技術を持つことになる。彼らはまた、特定の法執行機関の戦略について方針と法的立場を明確にするだろう。彼らはグローバルな法的要件を説明するために、グローバルなリスク評価を実施するかもしれない。例外

的なイベントが起こった場合、プロバイダーは法執行機関との協力に加えて、競合他社とも協力するプロセスを持つかもしれない。

B. ソフトウェア開発

ソフトウェアは、このガイドで言及する全てのエコシステムの構成要素に対して普遍的な要素を増している。このガイド全体で議論されるように、このガイドで紹介するソフトウェアの主要なシステミックなユーザーの中には、ソフトウェア革新と改善を牽引する多種多様の複雑な開発プロセスと相互依存性がある。例えば、インフラ、デバイス、デバイスシステム、システム導入業者、企業などである。従って、このセクションではエコシステムの各部分において特化したソフトウェア開発に関連する、多様なセキュリティのベースラインプラクティスと先進的な機能の獲得には言及しない。そのかわりに、このガイドではエコシステム全体でソフトウェアの安全性確保が極めて重要であることを強調することを目的とする。このガイドの別の個所で紹介されていない場合、ソフトウェア開発は通常下記のプラクティスから構成すべきである。

ソフトウェアのベースラインプラクティスと先進的な機能：

1. セキュア・バイ・デザイン開発プラクティス

ソフトウェアとアプリケーションは、効率を高めるためにますます商用とインフラプロセスと製品に統合されている。しかしこのことによって、ソフトウェアとアプリケーションがハッカーの主要なターゲットとなる。グローバルな経済、重要インフラと政府の運営は、ソフトウェアへの依存度がますます高まっている。

ベストプラクティスを追及する組織は、リスク管理を基に開発ライフサイクル全般において、開発者の研修、静的なアプリケーションセキュリティスキャン、脅威のモデル化、動的なアプリケーションセキュリティテスト、そして手動の侵入テストなど、セキュリティを品質の要素とし安全な開発プラクティス範囲内で実施する。開発者がこれらのベストプラクティスを導入する際に有用な資料は、一般に公開されている。例えば、ソフトウェアアシュアランス推進に特化した主要組織、SAFECode（the Software Assurance Forum for Excellence in Code）は、安全なソフトウェア開発トレーニング資料を出版し、「ソフトウェア開発の基本的なプラクティス」（*Fundamental Practices for Secure Software Development*）を含めて、無料で一般に公開している[56]。

ベースラインプラクティス：開発設計によるセキュリティは、少なくとも下記の点を含めるべきである。

- ✓ **保存または送信データの強力な暗号化**：盗難または不正アクセスが起きた場合、暗号化によりデータの可視化を阻止する。データを保存中または送信中であっても、暗号化は情報を保護するための必須のツールである。特定の組織や製品のニーズに合った異なる暗号のオプションがあるが、特定の使用例の内容が、簡単に見破られないように暗号化は通常強力なアルゴリズムを使用すべきである。アルゴリズムの強さは前後関係によって、未解決の攻撃の種類、そして適切に機能するある種のサービスへのニーズなど、要素によって異なるかもしれない。例えば、暗号化が強すぎると、ほとんどのファイアウォールとセキュリティパケットインスペクションサービスが機能しなくなるかもしれない。

- ✓ **デフォルトによるセキュリティ**：ソフトウェアのデフォルト設定はセキュリティの点に最も重点をおかなければいけない。この設定は、防御力を低くくしソフトウェアがより多くのオプションを許可するよう慎重に変更しなければいけない。この原則によって、悪意あるアクターが重大な被害をもたらす攻撃ベクトルを減らすことができる。

- ✓ **パッチ容易性と更新設計**：悪意あるアクターによる常に進化し精巧な手口を使う攻撃から防御するために、パッチと更新が必要であるという予想のもとに、ソフトウェアは設計されなければな

らない。パッチと更新は、ソフトウェアを設定する際、素早くそして安全な方法で最小限手動によって実行しなければいけない。

- ✓ **最低限の権限の原則**：必要なタスクを実行するために基本的な権限のみを、ユーザーに与えアプリケーションアクセスを制限することで、ソフトウェア開発者は製品への攻撃対象領域を減らすことができる。設計フェーズで最低限の権限の原則を適応することで、悪意あるアクターまたはウイルスに感染したサービスが管理アクセス権を取得してシステム全体を管理する可能性が低くなる。

- ✓ **ソフトウェアの構成要素分析**：この分析の目的は製品におけるオープンソースとサードパーティーの一覧表を作ること。そのためには、たとえサードパーティーのセキュリティとオープンソースの構成要素の保証はできないとはいえ、問題が起きた場合、ソフトウェア開発者自らが開発していなかった構成要素を認識し続けることができる。どの構成要素が製品やアプリに使われたかについて一覧表を持つことによって、開発組織が関連する既知の脆弱性を追跡し特定するのに役立つ。

- ✓ **ソフトウェアセキュリティの認識と啓発**： ソフトウェアセキュリティに対する意識の向上を、開発者、プロジェクトマネジャも含めてソフトウェア開発プロセスにかかわった全社員に広めるべきである。費用対効果の高い教育または研修を受けられるよう体制を整えるべきである。

先進的な機能：設計プラクティスによる主要なセキュリティは以下を含む：

- ✓ **動的アプリケーションセキュリティテスト（DAST）**：この先進的な技術では、アプリケーションを稼働している間、脆弱性をみつけるために侵入テスト（攻撃を模倣する）を用いる。この種のテストは IoT コンテキストで特に有効だ。しかし管理可能な設定オプションと高い能力をもつ専門家を雇用する能力が必要となる。

- ✓ **静的アプリケーションセキュリティテスト（SAST）**：この先進的な技術とともに、開発者はソースコードあるいはバイナリデータを検査し脆弱性を特定できる。その技術は使用できる言語とプラットフォームが限られている。IoT 空間における多くの製品は、この技術はオプションではないかもしれない。しかし特に重要な構成要素の慎重なコードレビューは、セキュリティ強化に有効かもしれない。

- ✓ **アーキテクチャに対する脅威モデルとリスク分析**：政府と協働するまたは運営上非常に重要なデータを取り扱う企業は、不正行為を実行しようと悪意のあるアクターが、仮設上、どのようにシステムに脆弱性を作り出すか、あるいは脆弱性を攻撃するかを特定するために、専門家のチームを採用するかもしれない。脅威モデルは、自動化され分散型の攻撃を含む、多くの種類のリスクを考慮するかもしれない。

- ✓ **セキュリティに特化したツールチェーン**：開発者は新しいソフトウェアを開発するために、セキュリティに特化したツールチェインを利用するかもしれない。ツールチェーンは、ソフトウェア開発を容易にするソフトウェアまたはハードウェアツールの集合体である。ツールチェーンがセキュリティを優先する場合、コーディングエラーはあまり発生することなく、プロバイダーは品質管理を強化できる。企業は新たな脆弱性と得られた教訓を開発ツールに組み入れるかもしれない。

- ✓ **セキュアなサードパーティーとオープンソースの構成要素**：主要企業は使用するサードパーティーの構成要素とオープンソースライブラリーに既知の脆弱性がないことを確認するだろう。

- ✓ さらに、企業は顧客に対して、ソフトウェアは安全な開発プロセスを経ているという証明を提供し、国際基準と整合する認証を求めることがある。

2. セキュリティとしての脆弱性の管理

世界中の様々な企業は、新たに発見した脆弱性を修正するために、製品を出荷後、顧客に対してどのくらいの期間、セキュリティパッチを提供できるかに関して異なる方針を持つ。大手の製品製造業者は、製品のパッチをより定期的にリリースする傾向があるが、中小の製品製造業者は、セキュリティパッチを開発し提供可能にする専任の人材が通常あまり多くない[57]。

ベースラインプラクティス：プロバイダーはミッションクリティカルアプリケーションで、重大な脆弱性に優先順位をつけるべきである。

先進的な機能：より先進的なプロバイダーは、リスク評価中に特に優先順位付けにより、ほぼ全ての既知の脆弱性を修正できる。彼らは、企業からソフトウェアを購入する、またはアプリケーションを介した企業とのやりとりに対してセキュリティを保証する能力を持っている。

3. 開発プロセスにおける安全性の透明化

上記の各プラクティスは安全なソフトウェアとハードウェア開発において、重要な役割を果たす。ソフトウェアの開発組織と民間セクターは、セキュアな開発プロセスに関して市場に基づく評価の開発を開始した[58]。また一方、政府機関と産業界のステークホルダーの連携によって開発されたフレームワークは、用語とプロセスの標準化と、市場での強い信頼を築くことに役立った。アメリカの国立標準技術研究所（National Institute of Standards and Technology（NIST））は、現在、SAFECode（the Software Assurance Forum for Excellence in Code）とステークホルダーと連携し、安全なソフトウェア開発プロセスとプラクティスに関するSpecial Publicationの出版を進めている。NTIAは組織が、どのようにサードパーティー製ソフトウェアの構成要素に関する情報を伝達し、どのようにより透明性を提供できるかを検討するため、多数のステークホルダーを主導しながらプロセスの検討を進めている[59]。

ベースラインプラクティス：ソフトウェアを購入する企業に、セキュリティに対する姿勢を証明する。

先進的な機能： 企業からソフトウェアを購入したり、またはアプリケーションを介してその企業と関係する人たちにセキュリティを保証する。

C. デバイスとデバイスシステム

個々にインターネットに接続したデバイス（または「エンドポイントデバイス」）は、ハードウェアモジュール、チップ、ソフトウェア、センサーまたは部品を含み、それ自身多数の構成要素からなるかもしれない。数十万の企業と何百万の開発者が、世界中に展開されている何十億個の個々のデバイス（開発に）貢献するかもしれない。セキュリティの革新を含む極めてダイナミックで新しい市場を構成するさらなる接続層は、個々のデバイスそのものを超えている。つまり、インターネットと接続したデバイスはもはや単なる個々のデバイスではない。そうではなくて、この複雑さを念頭に置いて、このガイドではデバイスシステムを以下のように説明する。接続したエンドポイントデバイスの共有体、つまり、モノのインターネットのひとつで、アプリケーションとクラウドサービスを含めて、インターネットのどこかに関連したサポート要素がある[60]。

デバイスとデバイスシステムに対するベースラインプラクティスと先進的な機能：

1. セキュア・バイ・デザイン開発のプラクティス

セキュリティがもし初期の開発プロセスの一部で、プロセス全体を通して重要な要素として含まれるのならそれが最善で効果的である。ベストプラクティスの特定の範疇において、エンドプロダクトは基本的な機密性、完全性そして可用性をもつことを確保する必須のツールとして一般的に受け入れられてきた[61]。ボットネットはデバイスとシステム実装の弱点をたくみに利用するので、そのような弱点を防ぐためにセキュリティ計画を製品開発の早い段階でそして全段階で含めることが適切である。

a) セキュアな開発ライフサイクルのプロセス

ベストプラクティス：セキュアな開発ライフサイクルのプロセス（SDL）は整っていなければいけない。SDLプロセスにおいて、各開発フェーズには手動または自動でおこなわれるセキュリティ活動がある[62]。

先進的な機能：安全な開発ライフサイクルプロセスを確立してから、先進企業はプロセスの能力を測り高めている。 SDL 能力を測ることは、BSIMM プロジェクト（セキュリティの設定 - 成熟度モデル[63]）の一部である。そして BSIMM に関する資料は無料で公開されており、能力を測る際の参考資料となる。

b) セキュアデザインの要素

このセクションでは、プロダクトデザインにおける開発レベルのプラクティスを記載する。

(1) 保存中と送信中のデータを保護する手段

ここでは、主にデバイスに保存されたデータの保護とデータ通信の暗号化について述べる。このような保護を実装する際には、例えばセキュアなハードウェアの要素、セキュアなブートプロセスなどについて決定しなければいけない事がある。先進的な機能の信頼の基点参照のこと。

ベースラインプラクティス：データ通信は暗号化されなければならない。 機密データは暗号化して保存しなければならない。どんな手順を使用するかにかかわらず、認証が可能であればそれを使うべきである。通常、どのようなシステムを使っていても利用できるセキュリティ対策を採用すべきである。非推奨の 暗号化技術方法の使用は避けるべきである。

先進的な機能：最新のプロトコルとセキュリティ機構を使うべきである。情報を保存するために暗号化の代わりに安全なメモリーを使用できる。暗号化は主にNIST FIPS 140-2またはISOあるいはIEC 24759と適合する方法を使用すべきである[64]。

(2) 不正アクセスを制限する手段

ベースラインプラクティス：IoT製品は通常ローカルまたはリモートで管理サービスが必要である。製品開発と製造工程で、デバイスのエンドユーザーには必要がないまたは利用できないメモリー、プロセッサ、周辺機器、または制御構造に対して低レベル層へのアクセスが必要になるかもしれない。これらの追加機能は慎重に保護しなければいけない。

このレベルでの典型的なステップには以下が含まれる：デバイスごとに固有の「admin」クレデンシャル、初回起動時のパスワード変更要件、ブルートフォースによるパスワード推測防止のための速度制限技術、製品出荷前の開発レベルのポートとサービスのセキュア化または停止、telnetのような未使用または安全でないローカルとリモートの管理サービスの除去などである。

先進的な機能：多要素認証のユーザーのアクセス管理をサポートすべきである。

さらに、エンドポイントデバイスとルータの開発者は、ボットネットによる不正アクセスと利用の防御に特に役立つ最新の規格を考慮すべきである。例えば、IETF Manufacturer Usage Descriptorまたは「MUD」[65]が多くの使用例で適切かもしれない。MUDはIETFにより定義された組み込みソフトウェア基準で、インターネットに接続する際、デバイスの意図するコミュニケーションパターンを含むデバイス仕様の公表をIoTデバイスメーカーに許可している[66]。デバイスとルータ両方がMUD要件を遵守する場合、ルータは、製造業者が意図する目的だけに、デバイスを制限する仕組みがある。それらの目的以外の行為、例えば大規模なDDoS攻撃に加担するなどは、ローカルルータが特定しブロックする。IEEE 802.1AR[67] と Device Identifier Composition Engine (DICE)[68]アーキテクチャのような追加基準は、IoTデバイスとそのMUDの構成要素のセキュリティを高めることができる。

(3) 難読化の使用

ベースラインプラクティス：デバイス製造業者は、機密情報（例えばデバイスキー、極秘データ）を保護するために、難読化の使用のみに頼ってはいけないが、難読化は攻撃者が機密情報を見つけにくくするために有効かもしれない。それでも機密情報はアクセス管理と暗号化のような手段で保護されるべきである。

先進的な機能：ベースラインと同様の実装。

(4) 利用者入力の検証とシステム出力の符号化

ベースラインプラクティス：
外部システムから受信したいかなる入力は、外部の敵による侵入や攻撃を受けないように管理しなくてはいけない。入力によって、長さ、文字型、受諾可能な価または範囲を許可しなければいけない。この点はまたホワイトリスト方式フィルタリングを参照のこと。ひとつのサブシステムから別のサブシステム、あるいは別のサイトへの出力はまた、フィルタされなければならない。この点は「文字の正規化」を参照のこと。

先進的な機能：ベースラインと同様の実装。

(5) 製品のニーズに応じた暗号化

ベースラインプラクティス：暗号化の方法では、データの完全性と機密性、クリデンシャリティ、権限の認証そしてリクエストの否認付加性の確保が必要である。この暗号化は評価されたリスクと適合するものを選択しなければいけないが、公開され相互評価を受けた方法のアルゴリズムを使用しなければいけない。可能であれば、暗号化の手段は更新可能とする。

先進的な機能：オープンで相互評価された手段とアルゴリズムを使用した強力で証明された更新可能な暗号化を行う。暗号化が、対称暗号化に対して、ポスト量子耐性鍵長を支援する能力をもつ事を確認する。

2. 信頼の基点

様々な種類の攻撃は、別の組織を模倣することで発生する。例えば、デバイスに対する新しいソフトウェアの信頼できるソースは、通常、ハードウェアのオリジナルの製造業者だ。マルウェアに汚染されたソフトウェアを導入することは明らかに防がなければいけない。これは本物と偽物の区別することが問題になってくる。

この解決策は信頼のシステムを持つことだ。信頼できるチェーンとは、各要素がチェーンに追加されるときに認証されるハードウェアとソフトウェアの要素のつながりである。チェーンの始まりは信頼の基礎であり、信頼できる組織によって提供される。認証はデジタル署名により暗号学的に処理される。最初の要素が信頼ある機関に再びつながるので、チェーンによって暗号学的に認証された各要素もまた信頼できる。

システムが符号のついたソフトウェア更新を受け取る時、システムはデジタル署名をチェックできる。システムそのものが元の信頼すべき組織の信頼に根付いているので、ソフトウェア更新が認証されると、ソフトウェアは信頼性を持つ。

a) ハードウェア機器を基にしたセキュリティ

ベースラインプラクティス：ハードウェア機器を基にしたセキュリティが、現在そして将来の製品の安全な開発ライフサイクルに適合するか検討する。

先進的な機能：ハードウェアを基にしたセキュリティは技術的に可能なところで活用される。

3. 生産終了を含めたプロダクトライフサイクル管理

プロダクトライフサイクル管理とは、デザイン、製造、サポート、生産終了にいたる概念から製品管理を積極的に行うことを意味する。生産終了管理とは、製品が定められた終末点に達した時にすべきことを定義し方針をもつことであり、決められたサポート期間の終了、あるいは機能の終了、または年月日による終了を含む。

ベースラインプラクティス：デバイス製造業者は、セキュリティサポート方針と保証期間中デバイスがどのようにサポートされるか、そしてサポート終了後に予想される状況について消費者に通知するかもしれない。可能であれば、適切なアクセス管理でデバイスを、ソフトとハード両面で監視する能力を持つことで、デバイスはネットワーク資産管理をサポートすべきである。

サポート期間終了後、消費者はデバイスの「廃棄」方法に関する能力をもちその方法を知らされなければならない。製品を廃棄する際、消費者は工場出荷時のデフォルト状態にもどし、いかなる個人情報（PII＝ Personally Identifiable Information）も削除しなければいけない。廃棄に関する知識には、売却、廃棄、または製品のリサイクル、IoTデバイスを設定した部分を売却するなど、様々なシナリオがある。

プロバイダーはセキュリティ脆弱性に関する方針と特定、軽減するプロセスを策定し、必要であれば製品について既知のセキュリティ脆弱性を開示しなければいけない。

先進的な機能：技術的に可能な場合、セキュリティサポート保証期間中における、アンチロールバック保護を伴った確実なアップデートと適切なアクセス管理を計画する[69]。

4. セキュリティ重視のツールチェインの使用

セキュリティ重視のツールチェインはソフトウェアとハードウェアの集まりで、製品を展開し、生産、管理を可能にするだけでなく、エンドプロダクトのセキュリティを強化するよう設計されている。

ベースラインプラクティス：ツールを使って、実装が安全なコーディングガイドラインに沿っているかどうか確認することができ、オープンソースのソフトウェアに記載されている共通脆弱性識別子（CVE)のサブセットを検索できる。

先進的な機能：ファジング、シンボリック実行、サンドボックス、静的および動的解析、そして安全なメモリーを使った言語などのツールは、脆弱性を発見し軽減するために使われる。

D. 家庭と中小企業でのシステム導入

家庭と中小企業では多くの分野で接続されたデバイスによって利便性を受けている。暖房、換気、エアコン（HVAC）などのシステムは住人が高性能な機能を利用して遠隔でアクセスすることで接続できる。セキュリティシステムには、インターネットを介して全てを管理できるカメラ、ロックシステム、警報システムがある。娯楽関連機器のシステムは、中央制御のおかげで、音声とビデオの複雑な設定が簡単にできる。これらの分野には驚くほど多様な製造業者とシステムがある。これらのシステムは家庭では個人が、そして事業主、または専門家が導入できる。専門家とはインテグレーターや、警報システム請負業者、である。

理想としては、家庭、オフィス、小売り、医療または産業環境で用いる各デバイスとシステムは、デバイスの全体のライフサイクルでベースラインプラクティスによって守られることである。このライフサイクルとは、デバイスの導入と設定を含む。正しく導入することで、製造品で「利用可能な最善のセキュリティ」を実行できるだろう。このセクションでは、最も一般的な種類のデバイスで、ベースラインプラクティスと先進的な機能により利用可能な最善のセキュリティを実行できることを説明する。

以下に記事*「接続される家庭のセキュリティシステム」*[70]から多くを引用する。

家庭と中小企業でのベースラインプラクティスと先進的な機能の導入：

1. 認証とクレジデンシャルの管理

機能の導入によって、暗号化された外部記憶装置のパスワード管理システムを利用できる。これらのシステムは、ユーザーがパスワードを覚え管理し、安全な場所にパスワード保管する手間を省く。

ベースラインプラクティス：パスワードがデバイスにとって特有でない場合、インストーラーでは、セキュリティ度が高いパスワードに変更しなければいけない。異なるパスワードを全てのデバイスとシステムで使用しなければいけない。導入には信頼できるパスワード管理を使用すべきである。

先進的な機能：多要素認証による利用者クセス管理を使用する。

2. ネットワーク設定

ネットワーク設定とは、ハードおよびソフトの配置、ネットワーク構成要素の接続、設定を意味する。

a) 概要

ベースラインプラクティス：システム（デスクトップ、ラップトップなど）は、最新のウイルス対策とマルウェア対策ツールを設定し稼働しなければいけない。特定の要請がない限り、管理者権限のあるシステムはどれも稼働してはいけない。

b) ファイアウォール、アクセスポイント、ルータの設定

ベースラインプラクティス：WAN側（インターネット接続側）のUPnPは、正当な目的が要求されない限り（例えばピアツーピアのゲーム）、無効にすべきである。適切なDHCPスペースには、推定される使用量を割り当てるべきであり、推定される使用量を超えてはいけない。

ファイアウォールは必要なポートのみを使用できるようにする。ポートフォワーディングは、それを必要とする特定のアプリケーションを除いて無効にすべきである。

先進的な機能：ネットワークは監視すべき、アプリケーションは非標準ポート値を使用すべき、ファイアウォール防御機能と連動させて、特定のアプリケーションのポートフォワーディングのみを有効にすべきである。巧妙な手口を使う攻撃者は打破できるが、MACアドレスフィルタリングは使用すべきである。

c) ハードとソフトの構造

ベースラインプラクティス：ワイヤレス環境と物理的な配線配置に関して、クライアント拠点の建物の外からのネットワークアクセスは制限されなければならない。セグメントは目的に応じて分割すべきであり、各無線チャネル、ケーブル布線、各アクセスポイントまたはゲートウェイなどのオプションを利用して、物理的に、あるいは論理的に分割されたネットワークを使用すべきである。

先進的な機能：セグメントはVLANsまたはVPNs使って目的によってさらに分割しなければいけない。ポートスキャンツールは、プライベートネットワークを監視するために使われる。

3. ネットワーク機器の管理

ネットワーク機器の管理は、ネットワークデバイスを正しく識別し設定するための進行プロセスの事である。

a) モデムとルータ、ネットワーク管理デバイス

ベースラインプラクティス：ネットワークデバイスは、定期的にファームウエアを更新するプロセスまたは手段をもつべきである。

先進的な機能：ISPが提供するモデム／ルータ／APシステム、別売りのルータ／APには、ソフトウェア更新のためにローカルで管理するLANトラフィックを処理する機能を加えるべきである。

b) ネットワークプロトコル

ネットワークプロトコルとは、TCP、UDP、IP、RTP など、デバイスがネットワーク通信に使う多層の言語である。

ベースラインプラクティス：非推奨のプロトコルは使用してはいけない。特にネゴシエーションされたSSL（どのバージョンでも）、TLS 1.0、または1.1の使用は不可であり許可もしてはいけない。

先進的な機能：必要であれば最新のプロトコルを設定する。

c) ワイヤレスリンク

ワイヤレスリンクはデバイス間の無線式のネットワーク接続である。これらのリンクは多様なデバイス間で、一方向、双方向あるいはネットワークトポロジーを使うかもしれない。

(1) Bluetooth

ベースラインプラクティス：利用可能なセキュリティ機能を有効にすべきである。利用可能であれば「検知されないオプション」を使用すべきである。機密情報はBluetooth low energy（BLE）ビーコンにさらしてはいけない。

(2) NFC

ベースラインプラクティス：NFC リーダーは、簡単な「スニッフィング」または簡単に改ざんを許可する状況に置いたり、マウントしたりすべきではない。

(3) Wi-Fi

ベースラインプラクティス：他のセクションで述べたベースラインネットワーク設定に加えて、WPA2パーソナルAES（推奨）またはWPA2パーソナルTKIPなどの、最新のWi-Fi暗号化オプションを使用すべきである。WPSは無効にすべきである。デフォルトまたはSSIDブロードキャストは使うべきではない。

「ゲストネットワーク」オプションは、多くのアクセスポイントで利用できる。そしてこのネットワークは来訪者または一時滞在者、派遣社員など、リスクの高い利用者に利用可能にすべきである。利用可能な場合、802.1 管理フレーム保護規格を有効にすべきである。
このガイドの別のセクションで述べるベストプラクティスに沿って、アクセスポイント設定へのアクセスが強力なパスワードで保護されていることを確認する。必要に応じてポートフィルタリングを有効にする。更新可能なファームウェアのアクセスポイントまたはルータを選択する。

(4) Z-WAVE

ベースラインプラクティス：基本的なセキュリティには、ユニークなHome ID、パスワードで保護された管理機能、必要に応じてデバイスのAES-128使用を有効にすることが含まれる。

先進的な機能：セキュリティを強化することとして、RFパワーによる距離の要件を満たすこと、特にAES-128対応デバイスを使用することがある。

(5) Zigbee

ベースラインプラクティス：インターネットに接続できる唯一のデバイスはZigbeeゲートウエイで、それをファイアウォールで保護すべきである。

先進的な機能：インターネットトラフィックは、Zigbeeネットワークに入るときと出るときにアドレス（送信元と送信先）とポートナンバーによってフィルターできる。802.15.4レベルとネットワークとアプリケーションレベルが利用可能な場合、オプショナルの802.15.4のセキュリティ機能を有効にできる。

(6) リモートアクセスコントロール

この分野には、通常のデバイス機能の全種類のリモートアクセスコントロール、例えば、セキュリティカメラビデオ、HVAC温度調節、遠隔始動やドアのロック解除などの自動車のサブシステムなどを含む。

ベースラインプラクティス：デバイスに故障または改ざんがなされた場合の警告を利用可能な場合、有効にする。全てのリモートアクセスは、IPの制限されたファイアウォールで防御されるべきで、ポートにかかわらず、ホワイトリストに記載のあるIPアドレスとサブネットのみデバイスにアクセスできるようにする。もしファイアウォールの外側からのリモートアクセスに機能が必要な場合には、リモートアクセス用にVPNと非標準のインターネットポートを使うべきである。

4. セキュリティ管理

ベースラインプラクティス：利用可能であれば、ネットワーク上での違反未遂またはインストールに対する攻撃未遂が見つかった場合、行動を追跡し対策を検討すべきである。違反未遂行為は、ネットワーク内で頻繁に攻撃を受ける個人や対象を特定するために関連付けるべきである。ネットワーク設定を文書化し接続したデバイスを列挙しセキュリティ管理計画を明確に定義すべきである。

E. 企業

飛躍的に増えている IoT デバイスシステムを含むネットワークデバイスとシステムの主な所有者、ユーザーとして、全ての種類の企業、例えば政府、民間セクター、教育、非営利団体などは、デジタルエコシステムを守るために重要な役割を果たす[71]。企業はしばしばデータを不正に取得されそうになったり、自動化された分散型の攻撃の犠牲となるが、その一方で、DDoS 攻撃とその他の分散型の攻撃による影響を拡大するために、企業の大規模なシステムが乗っ取られることもある。したがって、企業は、より広範囲のデジタルエコシステムを保護するために、自社のネットワークとシステムを適切に保護する責任を共有する重要なステークホルダーである。

世界中の何百万にも及ぶ民間セクターと政府機関による技術に関する知識と能力、各種資源へのアクセス、ベースラインセキュリティプラクティスを適応するきっかけは、組織、機関によって大きく異なる。例えば、大企業にはしばしば最高情報責任者と最高情報セキュリティ責任者がおり、各責任者はあらゆる IoT システムを含むネットワーク化された組織のシステムとデバイスを守る責任の一端を担う。中小企業では IT 専門の情報セキュリティ担当の人材はいないかもしれないが、かわりに既成のソリューションを利用する。

企業は、中小と大手企業両方のネットワークとシステム防御に役立つように、さらにツールを開発し提供している。おそらくボットネット対策ガイドに最も関連するのは、Cybersecurity Framework を基にした DDoS とボットネットの防御、軽減のためのプロファイルを作成し推進する Cybersecurity Coalition の取り組み[72]である。そしてそれは DDoS 攻撃やその他の自動化された分散型の攻撃への対策と軽減に取り組む企業と組織を支援することを意図している。
あらゆる規模の企業はまた、エコシステムのリスクを軽減するために、例えば、適切な ID とアクセス管理技術を実装し、特に更新ができないレガシー製品や海賊版製品、ソフトウェアの使用を停止することで、自ら積極的な手段をとることができる。企業がこのようなステップをとることで、ネットワークにおける機密データと知的所有権を保護し、さらに、DDoS 攻撃とその他の分散型の攻撃の対象領域になることが少なくなるので、全体としてエコシステムを守るために役立てることが出来る。

もちろん、このガイドを作成したサプライヤーとプロバイダーは、自身がグローバルな大企業である。
さらに、私たちは DDoS 攻撃とその他の自動化された分散型の脅威に対して、企業のネットワークを守り、脅威を軽減するために、ハイエンド仕様のソリューションを提供する。その市場での「供給」面は、堅実に成長している。そしてサイバーセキュリティサービスを求めるあらゆる規模の企業に対する、この市場での「需要面」がさらに拡大することで、革新と高度化、費用効率化がもたらされるだろう。

企業にとってのベースラインプラクティスと先進的な機能：

1. 確実なアップデート

製品製造業者には確実なアップデートを作り出す責任があるが、通常は利用者による許可または行為なしでアップデートは実行されない。組織のどのレベルでアップデートを管理することが必要かは、顧客の種類によって大きく異なる。例えば大企業または政府機関は有能なスタッフをもち、彼らはどのような種類のセキュリティアップデートが適切か、いつアップデートを実施したらよいか合理的に決定できる。一方通常家庭のユーザーはほとんどの場合、自動アップデートを利用する[73]。

> ベースラインプラクティス：企業は入手次第すぐにアップデートを実施すべきである。通常自動アップデートが望ましい。
>
> 先進的な機能：有能な技術スタッフを持つ企業は、セキュリティアップデートの実装を情報に基づいて決定できる。

2. リアルタイムの情報共有

大規模なネットワークまたは重要なネットワークを持つ企業は（例えば、大企業や政府機関）あらゆるステークホルダーとエコシステム参加者と脅威に関する重要な情報を共有できる。近年、情報共有の取り組みは著しく向上し、ボットネットの脅威や自動化された分散型の脅威との対抗に向け、大きな前進をとげている[74]。

ベースラインプラクティス：企業はまだ情報共有を積極的に行っていない場合でも、情報共有活動によりサイバー脅威の情報を受け取ったら責任をもって行動できるよう準備しておくべきである。例えば、政府や法執行機関との情報共有活動、様々なコンピュータ緊急対応チーム（Computer Emergency Response Team （CERT））、業界グループ、ネットワークプロバイダー、RFC2142で規定されたアドレス、そしてベンダーや他の情報源からの情報の更新や警告の情報を含む。

企業はセキュリティ情報とイベントマネジメント（SIEM）を相関しまたは自動化した取り組みと連動させて活用し、複数の脅威インテリジェンスの配信またはサービスの提供を受けるべきである。企業は内部または外部から入手した脅威情報を、その場で迅速に実行できる方法で内部のステークホルダーと共有するプロセスをもつべきである。企業は情報を共有したコミュニティーと連絡を保ち、彼らの地域と業界内でサイバーセキュリティのインシデントを適切に報告する、あるいは情報を共有するプロセスと防御手段に対する認識をもつべきである。企業は内部で脅威インテリジェンスを共有することを継続的に行うべきである。攻撃されたことを示す痕跡（Indicator of compromise（IOC））と明らかな脅威に関する情報は定期的に共有されるべきである。

先進的な機能：先進企業は、反応の薄いサイバー脅威情報を共有する多様なコミュニティー（政府、業界など）に責任をもって適切に共有することで、サイバー脅威情報を共有するコミュニティーの強化に努めるべきである。先進企業は共有活動に貢献する形で、サイバー脅威の情報を検知し、分析し、サイバー脅威の情報を捉える十分な能力を確保すべきである。先進企業は、地域、業界に適したサイバー攻撃脅威の情報共有コミュニティーの管理と強化に積極的に参加すべきである。先進企業は検知、分析、対応に関する能力を継続して高めるようにすべきである。

3. トラフィックフローを安全に管理するネットワークアーキテクチャ

企業はボットネットまたは他の手段を使ったDDoS攻撃に際し、悪意のあるトラフィックのフローを制限するために、ネットワークアーキテクチャを設計することで、制御できる[75]。インフラプロバイダーそしてエコシステムのステークホルダーが提供するDDoS対策サービスなど、明確な目標としてセキュリティを含んで設計したネットワークアーキテクチャは、防御策の補完手段となる。アプリケーションプログラミングインターフェース（API）は、アプリケーション、デバイス、バックエンドのデータシステム間の接続を管理する。一般に、APIによって企業が彼らのバックエンドのデータと新しいアプリケーションサービスの再利用のために機能の公開ができる。APIゲートウェイを通って周辺で展開するセキュリティは、強いセキュリティを維持しながら、アプリケーション開発者による企業データへのアクセス提供を許可し、企業のネットワークに侵入される前に脅威をくい止めることに役立つ。

ベースラインプラクティス：企業はDDoS攻撃に対して、ネットワークプロバイダーが提供する機能とサービスを大いに活用して、イントラネットを防御しなければいけない。企業はインターネットとイントラネットの相互接続アーキテクチャ、運用方針とプロセス、アクセス、パケットフ

ロー制御設定を標準化すべきである。企業はこのアーキテクチャが正しく展開し運営されているか確認する体制を実施しなければいけない。さらに企業は全てのインバウンドとアウトバウンドのデータフローとEメール、ブロックパケットまたはマルウェアを含むEメールをすべて検査しなければいけない。つまり、イントラネットで無許可のネットワークトラフィックをブロックし、業界標準のDMZアーキテクチャと運営プラクティスを活用する。

先進的な機能：先進企業はボットネットのC&Cフロー、Fast Flux DNS、疑わしいURLへのアクセスなど、ボットネットフローを示す観測可能な挙動を特定するかもしれない。先進企業はボットネットフローを自動的にブロックし、フローの送信元を修正する、受け取るメールからインターネットにアクセス可能なURLリンクを削除する、ボットネットアクターを特定するために使用する情報を共有および受信する、DNS要求者とDNSサーバ両方で、不適切なDNS動作を防ぐかもしれない。

分散型の攻撃に対する強靭性を強化するために、先進企業はアプリケーション・プログラミング・インタフェースゲートウェイを利用するかもしれない。アプリケーション・プログラミング・インタフェース（API）は、アプリケーション、デバイスと、バックエンドデータシステム間の接続を管理する。API ゲートウェイを通じて集中型アーキテクチャにセキュリティを展開することで、組織は強力なセキュリティを維持しながら、アプリケーション開発者に対して企業データへのアクセスを提供することに役立つ。

4. DDoS 攻撃に対する強靭性の強化

顧客としての意識がとても高く啓発活動に熱心であっても、多くの顧客は自身のネットワークの防御に必要な技術的な専門知識に欠けているであろう。ボットネットと分散型の攻撃が引き起こすかもしれない脅威を無視するのではなくて、企業はリスクプロファイルに適した業務用の DDoS 攻撃防御を購入すべきである[76]。商用サービスは、分散型の攻撃に対してより確実に企業を守るオフプレミスでの防御、またはオフプレミスとオンプレミスを合わせた防御を含むかもしれない。顧客が市販品を購入しサービスを利用することで、ボットネットとその他の分散型の攻撃からの脅威を受ける可能性が実質的に低くなる。

CSDE のメンバーは、ハイエンドの商用 DDoS 対策ソリューションを市場に提供する。例えば、統合セキュリティを持つ家庭用ゲートウェイ、エニーキャストサービスそして様々なマネージドセキュリティサービスが含まれる。エニーキャストサービスはコンテンツデリバリーの複数のルートを提供し、世界中に広がるかもしれない複数のネットワーク構成要素を介して負荷のバランスをとることで、DDoS 攻撃からの強靭性を強化する。もし DDoS 攻撃によってネットワークの一部が侵害された場合、トラフィックは別のルートへ自動的に切り替えられる。マネージドセキュリティサービスは、商用のスクラビングサービスを含む[77]。他の商用サービスは、ネットワーク型ファイアウオール、モバイルデバイスマネジメントシステム、脅威分析、そしてイベント検知、クラウドに対する安全な VPN 接続、Web とアプリケーションのセキュリティ、E メールのセキュリティを含む。

プロバイダーは、顧客の独自のニーズやリスクプロファイルに合わせたフィルタリングソリューションを提供するかもしれない。理想的には、これらのソリューションによって、オフプレミス防御とオンプレミス保防御の両方を統合するだろう。商用サービスは顧客に対してセキュリティの追加レイヤを作成することで、悪意あるトラフィックを攻撃元の近くでブロックする事が可能になる。

ベースラインプラクティス：企業はサイバーセキュリティインシデントに効率的に対処し、妥当な水準のセキュリティを維持するために、有効な緊急対策法をもつべきである。企業は製品とサービスについて適切なセキュリティ機能を持つ商用プロバイダーを選ぶべきである。（すなわちDDoS攻撃に対する防御能力とソフトウェア自動更新の技術があるISPとクラウドまたはホスティン

グプロバイダー）。企業はDDoS攻撃とボットネット攻撃の対応を含んで、インシデント発生時の対応について、文書化しテスト済みの計画を持つべきである。企業は自動化またはデフォルトで有効になっている対応を提供できる商用プロバイダーを選択すべきである。企業は選択した商用プロバイダーが有効かどうか定期的に再評価すべきである。

先進的な機能：先進企業は、オンプレミスとオフプレミス防御機能への十分なサポートを含めて、DDoS攻撃とボットネットへの防御に対して多層化したアプローチをとるべきである。先進企業は、スタッフの技術的な専門知識を高め、知識に差があればそれを特定し適切なトレーニングを実施し、緊急時のサポートで活用できるよう能力を維持し、そしてスタッフを増加しこれらのギャップに対処する。先進企業は、より質の高い結果を得られるよう機械学習やパターン分析などの先進的な機能を提供する商用サービスとソフトウェアの活用を検討すべきである。先進企業は市場で入手できる機能を定期的に再評価することで、継続して能力向上に努めるべきである。

5. IDとアクセス管理

IDはアプリケーション、デバイス、データそしてユーザー全般について制御点の一元化を成す。IDとアクセス管理ツールは、個人とサービスを認証し許可を得た行為を管理する。ITリスクがある最も重要な部分の一つは、IT管理者、最高情報セキュリティ管理責任者、システム全体へのアクセス権を持つ個人などの特権ユーザー関連である。特権ユーザーによる不注意な行為であろうと、悪意ある不適切な行為であろうと、それらの行為は、IT 運営とセキュリティ全体、そして組織の資産と情報のプライバシーに壊滅的な影響をもたらす。システムは管理者が彼らの役割に必要な行為を行うためだけに設定されるべきである。つまりリスクを少なくするために、「最小権限のアクセス」のみを可能にすることだ。脅威分析によって、挙動に関する洞察を提供でき、セキュリティリスクを示す何か異常なことが起きた場合、防御するまたは警告できる[78]。

最近の特筆すべき進歩は、パスワードまたはワンタイムコードに代わって用いられる物理的なセキュリティキーである。2017年はじめにグーグルが全社員に合計85,000個以上の物理的なセキュリティキーの使用義務を開始して以来、従業員関連のアカウントはひとつもフィッシングされていない[79]。

ベースラインプラクティス：組織のIDとアクセス管理プラクティスでは少なくとも下記の点を含まなければいけない：

- ✓ **認証**（多元的でリスクに基づく認証を含む） - アクセスを実施する際、対象者が事実上本人で、他人になりすましていないことを確認する。
- ✓ **認可** - オペレーションにアクセスする際、現状に基づいてアクセスを許可するか決定する。
- ✓ **アクセス管理** - ビジネスリーダーが、適切なアクセス決定をする際の方針を定義し明確にするプロセスに役立つ。
- ✓ **アカウンティング** - 傾向を分析し不審な行動を特定するために、システムリソースにアクセスする個別のユーザーの行動に関して、データをロギングするプロセス。
- ✓ **プロビジョニング/オーケストレーション** – 追加・移動・削除のプロセスを容易に行ったり、異なる接続リソース間でのイベント変更を調整する操作。
- ✓ **IDレポジトリ** – 対象者のプロファイルの現状と属性を維持するために長期間保管する。

企業はまた企業名簿からIDを適時削除し、IDと関連するアクセス権を削除し、特権的アクセス権とクラウドソースのアクセス権を24時間以内に取り消す、退職時の運営方針を適用すべきである。

企業は認証を促進するために、構文規則を基にしたパスワードの代わりに、より強固で覚えやすいパスフレーズを使用すべき、パスワード用辞書に照らしあわせたチェックをすべき、パスワード強度メーターを使用すべきである。さらに企業は、例えばシステム管理者などに対する特権的アクセス権には二要素または多要素認証(2FAあるいはMFA)を使用するべきである。企業は、段階的認証の2FAを要するシングルサインオンを使ってWeb、そしてSaaSアプリケーションにアクセスすべきであり、前もって検査、信任されていないデバイスへアクセスする際にも使うべきである。加えて、企業はフィッシング攻撃を阻止し、フィッシング攻撃によっておこるリスクを軽減する妥当な予防措置をとるために、FIDO U2Fトークンを使うべきである。

企業は最小権限アクセスの原則を忠実に守るべきである。その原則とは、ロールベースアクセス制御(Role-Based Access Control= RBAC)による役割に基づくアクセスリクエスト、さらに承認、検知、アウトプロセスの修正、異常値、休止、不正アクセスを防ぐための職掌分散（Separation of Duties = SoD）、アクセスの定期的な再検証によるアクセス管理（継続するビジネスニーズまたはCBN）などである。

企業は特権ユーザーの監視および監査そしてSecurity Information and Event Management（SIEM）を実行すべきである。彼らはまたサービスやアプリケーションIDについてクレジデンシャルあるいは機密情報の金庫を持つべきで、IDはプレインテキストで設定ファイルに保管してはいけない。

先進的な機能：先進企業はIDとアクセス管理のより優れた手段をもつかもしれない。

- ✓ **継続に認証**する方式では、利用者がログインからログオフをする間、操作によって危険にさらされているかどうか判断するために行動と生体情報の監視を利用する

- ✓ **リスクベース認証**は、位置情報や購入履歴などから、企業がIDに関してさらに理解できるようにする。このシステムではIDを認識し、従来の認証が不要であると判定しアクセスを許すかもしれない。反対に、もしシステムが真夜中にパスワード入力に何度か失敗したあとに、外国からログインするなどの異常を検知すると、これはリスクの高い操作であり、2段階の認証手順がないためにアクセスは拒否されるだろう。

- ✓ **特権アクセス管理**ソリューションは、特権を持つそれらのユーザーとアカウント（「王国への鍵」）にとって必要な透明性、監視、制御を提供する。管理者が彼らの役割にとって必要な行為の実施のみを許可すること、つまりリスクを少なくするために「最小限のアクセス」を有効にすることは重要である。この透明性によって、セキュリティリスクを示す何か異常なことが起こるあるいは警告を発することを防ぐので、行動と作業に関して判断できる。

- ✓ **適用型の認証**では、デバイスフィンガープリンティング、イントラネットやインターネットのような要因、複数の場所または地域からの同時アクセス、異常な時間帯のログインなどより、はるかに完璧で高度なリスク計算を用いた2FAまたはMFAを使用する

- ✓ **無限のループのアイデンティティ**ガバナンスによって、アクセス管理ツールを使って、サーバとアプリケーション内で、ユーザーのアクティビティ監視と分析を統合する。例えば、もし彼または彼女が保護されたデータにアクセスする、あるいは不正な方法によりアプリケーション内でアクセスすることを検知した場合、特権ユーザーのアクセスを無効にする。

- ✓ **賢いアクセス**管理は、分析論とAIによって実施できる。例えば休止しているアクセスを検知し無効にする。休止しているアクセスとは所有者によって長期間アクセスされておらず、アクセス管理上無効になっているまたは離職した可能性を示す。

- ✓ **ハッキングに対する検知と安全防御対策**は、特権アクセス管理とユーザーやシステムの振る舞いの分析（User and Entity Behavior Analytics（UEBA））を統合して向上させることができる。ソーシャルネットワークの情報とEメールを使ったスピアフィッシングにより、ワークステーションに入り込んだマルウェアは異常な行動を見せ、ワークステーションと特権のクレデンシャルが感染したことを示す。

6. 期限切れ製品と海賊版製品の課題への対策

企業は製造業者のサポート期限が切れたレガシー製品の使用を中止すべきである[80]。技術サポート面でより関連する問題となるのは海賊版のソフトウェアである。米国では5台のPCの内ほぼ1台が海賊版ソフトウェアを使っている。一方中国では、海賊版のソフトを使った個人用PCはしばしば70%を超える[81]。もちろん、メーカーは既知の不正行為に対して脆弱なままの海賊版ソフトウェアを通常はパッチ適用しない[82]。企業は海賊版のソフトウェア使用を避け、グローバルなインターネットとコミュニケーションのエコシステムにおける全体の脆弱性を減らすべきである。

ベースラインプラクティス：企業はメーカーのサポート期限が切れる前に正式にサポートされている製品に置き換えるべきである。企業は海賊版の使用を常に避けるべきである。そのような製品の使用はほとんどの国で違法でありそれはまたエコシステム全体のセキュリティに脆弱性をもたらす主な原因となる[83]。

先進的な機能：先進企業は最新のセキュリティ仕様と機能を持つ入手可能なサポート期限内の最新の製品をもつかもしれない。

6. ネクストステップと結論

このガイドの初版（1.0 版）の発行は、ボットネットと自動化された分散脅威に対する前例のない業界主導の戦略的キャンペーンの第一歩となる。CSDE、USTelecom、ITI そして CTA は、共通の課題に対処し悪意あるアクターによる攻撃を受ける傾向を逆転するために、ステークホルダーに推奨するプラクティスの実現を促す。

このガイドの序論で述べたように、デジタル経済は世界中で商業の成長と生活の質向上における牽引役であり続けている。しかし官民共にーステークホルダーだけでは、このシステムを管理することはできない。そこでデジタル経済の発展により得られる機会を安全に管理していくことが、情報通信技術（ICT）コミュニティーにおける全てのステークホルダーの重要な責任である。

私たちは目標に向けて、全てのステークホルダーが検討できるようこれらのベースラインプラクティスと先進的な機能を設定した。これらはダイナミックで柔軟性あるソリューションで、自主的に合意した基準で周知し、力強い市場の自由競争によって牽引され、世界中のデジタル経済を通してステークホルダーによって実装される。これは現在直面するシステミックなサイバーセキュリティの課題に対する最も適切な答えである。

この使命を心にとどめ、私たちはこのガイドに最新の開発と技術革新の内容を反映させ、毎年更新の上出版し、ガイドの改訂版の活用を推進する。そしてそのことによって、自身のネットワークとシステムだけでなく、幅広いエコシステムを通じて観測と測定可能なセキュリティの推進を牽引する世界中のメンバー企業とその他の企業を支援していくでしょう。

今後数か月、ただちに行う次のステップは、インターネットとコミュニケーションのエコシステムにおける、推奨するプラクティスの促進、またプラクティスへの積極的な関与に最も適した幅広い国内外のステークホルダーとともにこのガイドの活用を推進していくことである。こられの幅広いステークホルダーによって責任が共有されることは、私たちのデジタル経済の将来を守る重要な鍵となる。

7. ガイド作成に貢献した組織

CSDE について
セキュアなデジタル経済に向けた評議会（CSDE）は、情報通信技術（ICT）セクターの企業を結集して、ますます高度化し台頭しつつあるサイバー脅威に協力して対処している。設立パートナーは、Akamai、AT&T、CA Technologies、CenturyLink、Cisco、Ericsson、IBM、 Intel、NTT、Oracle、Samsung、SAP、Telefonica、Verizon である。CSDE は USTelecom と米国情報技術工業協議会（The Information Technology Industry Council（ITI））によってとりまとめられている。

USTelecom について
USTelecom は通信業界のサービスプロバイダーとサプライヤーを代表する主要な業界団体である。その多様な会員基盤は、上場する大手通信企業から、中小企業、そして協同組合まで多岐にわたっており、いずれも都市部そして郊外の両方に先進的な通信サービスを提供している。

ITI について
米国情報技術工業協議会（The Information Technology Industry Council（ITI））は、テクノロジーセクターについて、世界中からの意見をとりまとめる機関である。ITI は、世界の主要な革新的企業のための政策提言機関として、政策立案者、企業、非政府組織の関係を調整し、世界中で技術の開発と利用を促進する創造的なソリューションを提供する。

全米民生技術協会（CTA）について
全米民生技術協会（The Consumer Technology Association（CTA）™）は 3,770 億ドルに及ぶ米国の民生技術業界を代表する業界団体であり、1,500 万人以上の米国での雇用を支援する。80%が中小とスタートアップ企業で、他は世界的に有名なブランド企業である 2,200 社以上の企業は、政策提言、市場調査、技術指導、業界振興、規格開発、事業の戦略的関係の促進など、CTA 会員のメリットを享受している。CTA はまた、民生技術の事業で繁栄している全ての人々が集まる見本市 CES®の主催者である。CES で得た利益は CTA の業界サービスに再投資される。

8. 巻末注

[1] 全てのハッカーが悪意があるわけではないが、悪意あるアクターもまた通常ハッカーと呼ばれる。一般にこのガイドでは用語の言い換えが可能で、文脈から言及される個人が悪意あるアクターかそうでないかを判断する。このガイドはまた悪意あるアクターに着目しているので、概してこのガイドでの「ハッカー」は悪意あるアクターである事に留意するべきである。

[2] IoT エコシステムにおいて同時に全種類のソフトウエア要件を設定するのは実用的ではない。デバイスとデバイスシステム、企業とインフラでは特定の要件がある。このセクションでは、ガイドの別の箇所で対象とならない分野を網羅する。

[3] 個々に接続されたデバイス（あるいは「エンドポイントデバイス」）はハードウエア、モジュール、チップ、ソフトウエア、センサー、あるいは他の稼働している構成要素を含めて、多数の構成要素からなるかもしれない。何十万もの企業と何百万もの開発者は、世界中で展開する何十億個ものデバイス開発に貢献している。セキュリティ革新を含む極めてダイナミックで新しい市場を構成するさらなる接続性のレイヤは、個々のデバイスそのものを超えている。つまり接続されたデバイスはもはや単なる個々のデバイスではない。この複雑さに留意して、このガイドではデバイスシステムを以下のように説明する：接続されたエンドポイントデバイスの結合、つまり IoT の中でひとつの「モノ」、そしてアプリケーションとクラウドサービスを含むインターネットでの関連サポートの要素である。

[4] 暖房、換気および空調(HVAC）システムは、居住者が自動化された仕様とリモートアクセスを使って接続する。カメラ、ロックシステム、警報システムを含めたセキュリティシステムは、インターネットを介して管理する。娯楽関連機器のシステムは、中央制御のおかげで、音声とビデオの複雑な設定が簡単にできる。これらの分野には驚くほど多様な製造業者がある。これらのシステムは、家庭では個人がそして事業主または専門家が導入できる。専門家とはインテグレーターや、警報システム請負業者である。理想としては、家庭、オフィス、小売り、医療または産業環境で用いられる全てのデバイスとシステムは、デバイスのライフサイクル全体でベースラインプラクティスによって保護される。そしてそれは、製品で「利用可能な最善のセキュリティ」を実行するデバイスの導入と設定を含む。

[5] Consumer Tech. Ass'n, *The Connected Home Security System*, https://cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security-Checklist.aspx (last visited Oct. 10, 2018).

[6] 急激に増加する IoT デバイスシステムを含む、ネットワークで接続されたデバイスとシステムの主要な所有者、利用者として、すべての種類の企業、すなわち、政府、民間セクター、教育機関、非営利団体などは、デジタルエコシステムの安全性確保において重要な役割を果たす。企業がしばしばデータを不正に取得されそうになったり、自動化された分散型の攻撃の犠牲となるが、企業の大規模なシステムが DDoS 攻撃とその他の分散型の攻撃の影響を受けることが増え、乗っ取られることもある。その結果、幅広い範囲のデジタルエコシステム防御に役立つように、ネットワークとシステムを十分に守り、企業は協力して主要なステークホルダー間で責任を共有する。技術的な知識とスキル、リソースへのアクセス、ベースラインセキュリティプラクティスを適応するインセンティブは、世界中の何百万にも及ぶ民間セクターと政府機関で大きく異なる。あらゆる規模の企業はまた、エコシステムのリスクを軽減するために、自ら積極的な手段をとることができる。企業がそのような手段をとることによって、ボットネットの攻撃対象領域になることが少なくなり、エコシステム全体の防御に役立つので、ネットワークにおける機密データと知的所有権を保護できる。このガイドを作成したサプライヤーとプロバイダーはグローバルな大企業であり、そして私たちは DDoS 攻撃やその他の自動化された分散型の脅威に対して、企業のネットワークを守り、脅威を軽減するために、ハイエンドのソリューションを提供する。「供給」面は、堅実に成長しており、あらゆる規模の企業におけるそのようなサービスの「需要面」がさらに拡大することで、革新と高度化、費用効率化がもたらされるであろう。

[7] CSDE, ITI, and USTelecom descriptions *infra* p. 39.

[8] CTA description *infra* p. 39.

[9] 簡潔にするために、以下「ボットネットとその他の自動化された分散化脅威」を「ボットネット」として言及する。

[10] Andrew Sheehy, *GDP Cannot Explain The Digital Economy*, Forbes (June 6, 2016), https://www.forbes.com/sites/andrewsheehy/2016/06/06/gdp-cannot-explain-the-digital-economy/#47c4db1218db.

[11] Irving Wladawsky-Berger, GDP Doesn't Work in a Digital Economy, *The Wall Street Journal* (Nov. 3, 2017) https://blogs.wsj.com/cio/2017/11/03/gdp-doesnt-work-in-a-digital-economy.

[12] Paul Tentena, *Artificial Intelligence to Double Digital Economy to 23 Trillion by 2025*, East African Business Week (May 30, 2018), http://www.busiweek.com/artificial-intelligence-to-double-digital-economy-to-23-trillion-by-2025.

[13] *See, e.g.*, Catalin Cimpanu, *Sly Malware Author Hides Cryptomining Botnet Behind Ever-shifting Proxy Service*, ZDNet (Sept. 13, 2018), https://www.zdnet.com/article/sly-malware-author-hides-cryptomining-botnet-behind-ever-shifting-proxy-service（「暗号通貨マイニング作業に特化したボットネットは、2018 年のマルウェア感染の最も活発な形の一つ」）

[14] Sam Thielman and Chris Johnston, *Major Cyber Attack Disrupts Internet Service Across Europe and US*, The Guardian, (Oct. 21, 2016), https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service.

[15] Michael Newberg, *As Many as 48 Million Twitter Accounts Aren't People, Says Study*, CNBC (Mar. 10, 2017), https://www.cnbc.com/2017/03/10/nearly-48-million-twitter-accounts-could-be-bots-says-study.html.

[16] JP Buntinx, *Top 4 Largest Botnets to Date*, Null TX (Jan. 7, 2017).

[17] Daniel Newman, *The Top 8 IoT Trends for 2018*, Forbes (Dec. 19, 2017), https://www.forbes.com/sites/danielnewman/2017/12/19/the-top-8-iot-trends-for-2018/#2523096867f7 (citing HIS Markit IoT Trend Watch 2018, *available at* https://ihsmarkit.com/industry/telecommunications.html); *see also* Gartner, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016* (Feb. 7, 2017), https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.

[18] Jan-Peter Kleinhans, *Internet of Insecure Things: Can Security Assessment Cure Market Failures?*, Stiftung Neue Verantwortung (Dec. 2017), https://www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf.

[19] Bill Connor, *Ransomware-As-A-Service: The Next Great Cyber Threat?*, Forbes (Mar. 17, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/#14a38e5b4123.

[20] Andy Greenberg, *The White House Blames Russia for NoPetya, the 'Most Costly Cyber Attack in History'*, Wired (Feb. 15, 2018) https://www.wired.com/story/white-house-russia-notpetya-attribution; Damien Sharkov, *Russia Accused of 1.2 Billion NoPetya Cyberattack*, Newsweek (Feb. 15, 2018) https://www.newsweek.com/russia-accused-massive-12-billion-cyber-attack-807867; CBS News, *What Can We Learn from the Most Devastating Cyber Attack in History?* (Aug. 22, 2018), https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation（NotPetya マルウェアがいかに 100 億ドル以上の被害をもたらしたかを説明する）

[21] Alex Zaharov-Reutt, *Cyber Crime, Data Breaches to Cost Businesses US $8 Trillion Thru 2022*, ITWire (April 25, 2017), https://www.itwire.com/security/77782-$8-trillion-business-cost-from-cybercrime-and-data-breaches-thru-2022.html.

[22] Commc'n Sec., Reliability and Interoperability Council IV Working Group 4, *Final Report on Cybersecurity Risk Management and Best Practices* 4 (Mar. 2015), *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (「規範的で静的なコンプライアンス体制に対する非規制アプローチの利点」を認識している)

[23] *See supra* notes 1–26 and *infra* notes 28–80.

[24] Daniel Palmer, *Researchers Discover Huge Crypto Scam Botnet on Twitter*, Coindesk (Aug. 7, 2018), https://www.coindesk.com/researchers-discover-huge-crypto-scam-botnet-on-twitter （「研究者は、ツイッターで合法なアカウントをまねて暗号通貨の「ギブアウェイ」詐欺を拡散するための大規模なボットネットを発見した。」）

[25] Tobias Knecht, *A Brief History of Bots and How They've Shaped the Internet Today*, Abusix (Aug. 23, 2017), https://www.abusix.com/blog/a-brief-history-of-bots-and-how-theyve-shaped-the-internet-today.

[26] Dustin Volz and Jim Finkle, *U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam*, Reuters (Mar. 2016), https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF.

[27] Lee Matthews, *World's Biggest Mirai Botnet Is Being Rented Out for DDoS Attacks*, Forbes (Nov. 29, 2016), https://www.forbes.com/sites/leemathews/2016/11/29/worlds-biggest-mirai-botnet-is-being-rented-out-for-ddos-attacks/#6bdec4cb58ad.

[28] *Compare* Elie Bursztein, I*nside the Infamous Mirai IoT Botnet: A Retrospective Analysis*, Cloudflare (Dec. 14, 2017), https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis.（2016 年 3 月 24 日の ArsTechnica によると「Mirai による攻撃は、群をぬいて大きく毎秒 623Gbps に達していた」と「サイバー攻撃のキャンペーン」に対して、7 人のイラン人を告訴した連邦大陪審 Sean Gallagher 氏は述べた。（「ピーク時には、DDoS 攻撃は毎秒 140 ギガビットに達した」）

[29] 2018 年 3 月、Mirai のボットネットトラフィックは攻撃者が GitHub を標的として、DDoS 攻撃が毎秒 1.35 テラバイト（bps）に達した点を留意してください。See Lily Hay Newman, GitHub Survived the Biggest DDoS Attack Ever Recorded, Wired (Mar. 1, 2018) https://www.wired.com/story/github-ddos-memcached.
Notably, the attack did not use a botnet. Instead, the attackers spoofed requests to vulnerable "memcached" servers used to speed up websites, causing victims to be flooded with about 50 times the normal amount of internet traffic.
とりわけ、攻撃はボットネットを使用しなかった。代わりに攻撃者はスプーフィングされたリクエストを Web サイトを高速化するために使用する、脆弱性がある「Memcached」サーバーに送った。そして通常のインターネットトラフィックの約 50 倍の量で被害者のコンピュータに氾濫を起こさせた（「Memcached」は分散したメモリーキャッシュシステムを指し、外部のデータソースに依存せずに、ランダムアクセスメモリーの「キャッシング」データによって、Web サイトを高速化するためによく使われる）。Memcached サーバーは、悪意あるアクターを含めて、誰にでも応答するであろう。そしてそれらは公共のインターネットにさらしてはいけない。しかし、これらのサーバーの約 100,000 台は危険にさらされ脆弱性を持つ。多くはセキュリティに関わる人材に限りがある中小企業と組織が持つサーバーである。 See Liam Tung, New World Record DDoS Attack Hits 1.7Tbps Days after Landmark GitHub Outage, ZDNet (Mar. 6, 2018), https://www.zdnet.com/article/new-world-record-ddos-attack-hits-1-7tbps-days-after-landmark-github-outage. サーバーの脆弱性を利用したこの種のフラッド攻撃手法は、悪意あるアクターの間でますます広まっている。「これまでに記録された中で最大規模の DDoS 攻撃」でも GitHub が生き残ったほんの数日後、記録は再び破られた。Arbor Networks の顧客が、1.7Tbps に達する同じような攻撃の標的になった。

[30] Cyren, Cyren Cyber Threat Report 8 (Jan. 2017), http://www.vcwsecurity.com/wp-content/uploads/2017/01/Cyren_2017Q1_Botnet_Threat_Report.pdf.

[31] Denis Makrushin, *The Cost of Launching a DDoS Attack*, Kaspersky (Mar. 23, 2017), https://securelist.com/the-cost-of-launching-a-ddos-attack/77784.

[32] Alfred Ng, *WannaCry Ransomware Loses Its Kill Switch, So Watch Out*, CNET (May 15, 2017), https://www.cnet.com/news/wannacry-ransomware-patched-updated-virus-kill-switch.

[33] Ellen Nakashima, *Russian Military was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes*, Washington Post (Jan. 12, 2018), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.bc4ce7d72018.

[34] Andy Greenberg, *Hackers Are Trying to Reignite WannaCry with Nonstop Botnet Attacks*, Wired (May 19, 2017), https://www.wired.com/2017/05/wannacry-ransomware-ddos-attack.

[35] CBS News, *What Can We Learn from the Most Devastating Cyber Attack in History?* (Aug. 22, 2018), https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation.

[36] U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (May 22, 2018), *available at* https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf; Commc'n Sec., Reliability and Interoperability Council IV Working Group 4, *Final Report on Cybersecurity Risk Management and Best Practices* (Mar. 2015), *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf; ENISA, Botnet Measurement, Detection, Disinfection and Defence (Mar. 7, 2011), https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-

defence; Int'l Telecomm.Union, ITU Botnet Mitigation Toolkit (Jan. 2008), https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf.

[37] U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* 10 (May 22, 2018), *available at* https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

[38] Tim Polk, *Enhancing Resilience of the Internet and Communications Ecosystem*, Nat'l Inst. of Standards and Tech. 7–9 (Sept. 2017) （DDoS攻撃の防御として、イングレスまたはイグレスフィルタリングを含むツールと技術を論ずる。つまりオンプレミスとオフプレミスによるDDoS攻撃の防御である）*available at* https://doi.org/10.6028/NIST.IR.8192. *See also*, Ctr. for Democracy and Tech, Comments to the NTIA on Promoting Stakeholder Action Against Botnets and Other Automated Threats 2 (Feb. 12, 2018) （「ボットネット軽減のための一般的な技術は、イングレスまたはイグレスフィルタリング、リルーティング、インターネットトラフィックのシェーピング、デバイスの分離、その他のエンティティを含む」というNTIAの報告草案に同意する）*available at* https://cdt.org/files/2018/02/CDT-NTIA-Botnet-Comments-Feb-2018.pdf; Commc'n Sec., Reliability and Interoperability Council IV Working Group 4, *Final Report on Cybersecurity Risk Management and Best Practices* (Mar. 2015), *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[39] *See, .e.g.*, United States, DHS Automated Indicator Sharing (AIS) System, https://www.us-cert.gov/ais (last accessed Oct. 17, 2018); United Kingdom, Cyber Security Information Sharing Partnership (CiSP), https://www.ncsc.gov.uk/cisp (last accessed Oct. 17, 2018); Japan, Cyber Clean Center, https://www.telecom-isac.jp/ccc/en_index.html (last accessed Oct. 17, 2018); New Zealand, CORTEX, https://www.gcsb.govt.nz/our-work/information-assurance/cortex-faqs (last accessed Oct. 17, 2018).

[40] *See* David Strom, *What Is Polymorphic Malware and Why Should I Care?* (Oct. 16, 2015), https://securityintelligence.com/what-is-polymorphic-malware-and-why-should-i-care.

[41] Verizon, 2012 Data Breach Investigations Report 71 (2012), https://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf.

[42] *See* Stephen Sladaritz, *About Heuristics*, SANS Institute 4 (Mar. 23, 2002), *available at* https://www.sans.org/reading-room/whitepapers/malicious/about-heuristics-141（2 種類の異なるヒューリスティック分析を比較している）; *see also* John Aycock, Computer Viruses and Malware 74 (2006) （静的と動的ヒューリスティックの唯一の違いは、「データがどのように集められるか」の点で、その違いがなければデータは同一であることを説明している）

[43] *See, e.g.*, Cisco, Cisco Cognitive Threat Analytics v1 (Feb. 2016), https://dcloud-cms.cisco.com/demo_news/cisco-cognitive-threat-analytics-v1.

[44] Nat'l Inst. of Standards and Tech., *Advanced DDoS Mitigation Techniques* (Oct. 18, 2017) （10 年以上にわたり、業界は偽装された送信元アドレスのネットワークトラフィックをブロックするために、IP レベルのフィルタリング技術について、技術仕様と展開のガイダンスを開発してきた）*available at* https://www.nist.gov/programs-projects/advanced-ddos-mitigation-techniques.

[45] P. Ferguson & D. Senie, *Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing*, Internet Engineering Task Force (IETF) Network Working Group (May 2000), *available at* https://tools.ietf.org/html/bcp38; F. Baker & P. Savola, *Ingress Filtering for Multihomed Networks*, Internet Engineering Task Force (IETF) Network Working Group (Mar. 2004), *available a*t https://tools.ietf.org/html/bcp84.

[46] *Id*.

[47] *See generally, e.g.*, Chris Benton, *Egress Filtering FAQ*, SANS Institute (Apr. 19, 2006), *available at* https://www.sans.org/readingroom/whitepapers/firewalls/egress-filtering-faq-1059.

[48] *See* Cisco, *Access Control Lists* (last updated July 17, 2018), https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/asdm79/firewall/asdm-79-firewall-config/access-acls.html.

[49] *See* Cisco, *Policing and Shaping Overview* (last updated Nov. 23, 2017), https://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfpolsh.html.

[50] *See generally, e.g.*, Guy Bruneau, *DNS Sinkhole*, SANS Institute (Aug. 7, 2010), https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523.

[51] *See* Cisco, *Implementing BGP Flowspec* (last updated Jan. 31, 2018), https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-2/routing/configuration/guide/b_routing_cg52xasr9k/b_routing_cg52xasr9k_chapter_011.html.

[52] *See* Georgia Tech Researchers, *DNS Changer Remediation Study, Presentation to M3AAWG 27th General Meeting, San Francisco, CA* (Feb. 19, 2013), *available at* https://www.m3aawg.org/sites/default/files/document/GeorgiaTech_DNSChanger_Study-2013-02-19.pdf (last accessed Oct. 17, 2018); *see also* Commc'n Sector Coordinating Council, Botnet Whitepaper 24–25 (July 17, 2017) （Eメール、電話、郵便、テキストメッセージ、Web ブラウザで知らせる、Walled Garden、ソーシャルメディアの方法など、インフラプロバイダーが利用者に知らせる多様な手段を記載している）available at https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

[53] *See* Ctr. for Democracy and Tech, Comments to the NIST Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malwares (Nov. 14, 2011) （「ボットネットの攻撃を受け回復せざるをえない時、「切断またはさもなくば顧客のインターネット接続を中断する」プラクティスに関する懸念を示す）*available at* https://www.nist.gov/sites/default/files/documents/itl/CDT-Comments-on-BotNet-FRN-11-14-11.pdf; Elec. Frontier Found., Comments to the NIST Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malwares 5 (Nov. 4, 2011) (explaining how uninfected parties could have their internet access affected by quarantine), *available at* https://www.nist.gov/sites/default/files/documents/itl/EFF-Comments-to-BotNet-RFI_11-4-11.pdf.
（感染していない関係者が、どのように検疫の影響を受けてインターネットにアクセスする事ができたかを説明している）

[54] *See* Commc'n Sector Coordinating Council, Botnet Whitepaper 21 (July 17, 2017), （「犯人の逮捕につながる法執行以外より効果的な手段はない。これは症状に対してだけではなく、問題の根本原因に対処する唯一の解決策だ。ボットネットの停止措置はしばしば国際的国境を越えて、慎重なフォレンジックと多くのステークホルダー間での慎重な調整が必要となる。ほとんどのボットネットは国家間の協力のもと多くの人材と多くの時間が必要となり、事実上国際的な事件となる。」）*available at* https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf.

[55] *See* Robert Wainright and Frank J. Cilluffo, Responding to Cyber Crime at Scale: A Case Study, Europol & the George Washington Univ. Ctr. for Cyber and Homeland Sec. (March 2017), *available at* https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/Responding%20to%20Cybercrime%20at%20Scale%20FINAL.pdf.

[56] See SAFECode, Fundamental Practices for Secure Software Development (2018), https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf

[57] A. Arora et al., Carnegie Mellon University, An Empirical Analysis of Software Vendors' Patching Behavior: Impact of Vulnerability Disclosure (Jan. 2006) （他のベンダーと比較して規模の大きいベンダーの動機について分析している）*available at* https://www.heinz.cmu.edu/~rtelang/disclosure_jan_06.pdf.

[58] *See* SAFECode, Principles for Software Assurance Assessment (2015), *available at* https://safecode.org/publication/SAFECode_Principles_for_Software_Assurance_Assessment.pdf; CA Tech., Veracode, https://www.veracode.com/verified (last accessed June 18, 2018).

[59] Nat'l Inst. of Standards and Tech., NTIA Software Component Transparency, https://www.ntia.doc.gov/SoftwareTransparency (last accessed Nov. 6, 2018).

[60] This section on Devices and Systems draws on Consumer Tech. Ass'n, *Securing Connected Devices for Consumers in the Home – A Manufacturer's Guide (CTA-CEB33)*, https://members.cta.tech/ctaPublicationDetails/?id=c12ebabe-84cd-e811-b96f-0003ff52809d (last accessed Oct. 15, 2018).

[61] このプロセスには、早期の要件計画と最終的な認定が不可欠である。例えば、CTIA はワイヤレスネットワーク上のデバイスセキュリティに関する業界要件を確立し、認定プログラムを提供している。必要条件やデバイスの認証方法など、プログラムの詳細はこちら：https://www.ctia.org/about-ctia/programs/certification-resources.

[62] *See* Microsoft, What is the Security Development Lifecycle?, https://www.microsoft.com/en-us/sdl/default.aspx (last accessed Oct. 19, 2018).

[63] *See* BSIMM, https://bsimm.com (last accessed Nov. 6, 2018).

[64] For more international standards, *see* Nat'l Inst. of Standards and Tech., *Cryptographic Module Validation Program*, https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards. In addition, NIST has a draft summary of international standards: Nat'l Inst. of Standards and Tech., *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*, https://csrc.nist.gov/publications/detail/nistir/8200/draft (last accessed Oct. 10, 2018).

[65] For the current Proposed Recommendation, *see* IETF, Manufacturer Usage Description Specification, https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/ (la6st accessed Oct. 19, 2018).

[66] Cisco, What is Manufacturer Usage Description? (MUD) https://developer.cisco.com/docs/mud/#!what-is-mud (last accessed Oct. 19, 2018).

[67] IEEE, 802.1AR: Secure Device Identity, https://1.ieee802.org/security/802-1ar/ (last accessed Oct. 19, 2018).

[68] Trusted Computing Group, Device Identifier Composition Engine (DICE) Architectures, https://trustedcomputinggroup.org/work-groups/dice-architectures (last accessed Oct. 19, 2018).

[69] For a discussion on updates, *see* Nat'l Inst. of Standards and Tech., *Stakeholder-Drafted Documents on IoT Security*, https://www.ntia.doc.gov/IoTSecurity (last accessed Oct. 10, 2018).

[70] Consumer Tech. Ass'n, *The Connected Home Security System*, https://cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security-Checklist.aspx (last visited Oct. 10, 2018).

[71] U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* 12–15 (May 22, 2018), *available at* https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

[72] Cybersecurity Coalition, DDoS Threat Mitigation Profile, https://www.cybersecuritycoalition.org/ddos-framework (last accessed Nov. 14, 2018), and Cybersecurity Coalition, Botnet Threat Mitigation Profile, https://www.cybersecuritycoalition.org/botnet-framework (last accessed Nov. 14, 2018).

[73] *See* Commc'n Sec., Reliability and Interoperability Council II Working Group 8, *Final Report on ISP Network Protection* 16（利用者は「オペレーティングシステムと自動的にインストールされるアプリケーション両方に対して、重要な更新をダウンロードをするためにコンピュータを設定する事」を特に推奨する）(Nov. 2011), *available at* https://www.atis.org/01_legal/docs/CSRICII/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

[74] Tim Polk, *Enhancing Resilience of the Internet and Communications Ecosystem*, Nat'l Inst. of Standards and Tech. 13 (Sept. 2017) (citing opinions of participants in the NIST Enhancing Resilience of the Internet and Communications Ecosystem workshop on July 11-12, 2017), *available at* https://doi.org/10.6028/NIST.IR.8192.

[75] Scott Bowen, *Akamai, Defense By Design: How To Dampen DDoS Attacks With A Resilient Network*, Forbes (Sept. 14, 2017) https://www.forbes.com/sites/akamai/2017/09/14/defense-by-design-how-to-dampen-ddos-attacks-with-a-resilient-network/#79144da56f8a.

[76] *See, e.g.*, AT&T, Distributed Denial of Service (DDoS) Defense (2014), *available at* https://www.business.att.com/content/productbrochures/ddos_prodbrief.pdf; Verizon, DDoS Shield Solutions Brief (2016), *available at* http://www.verizonenterprise.com/resources/ddos_shield_solutions_brief_en_xg.pdf; CenturyLink, DDoS Mitigation (2014), *available at* http://www.centurylink.com/asset/business/enterprise/brochure/ddos-mitigation.pdf; Telefonica, Anti-DDoS, https://www.cloud.telefonica.com/en/open-cloud/products/security/anti-ddos (last visited May 14, 2018); NTT, DDoS Protection Service, https://www.ntt.com/en/services/network/gin/transit/ddos.html (last visited May 14, 2018).

[77] *See* discussion *supra* Part V.A.b(5) （ボットネット軽減に向けたスクラビングセンターの役割を説明）

[78] Nat'l Inst. of Standards and Tech., *Digital Identity Guidelines* (June 2017), *available at* https://doi.org/10.6028/NIST.SP.800-63-3.

[79] Brian Krebs, *Google: Security Keys Neutralized Employee Phishing*, Krebs on Security (July 23, 2018) https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing.

[80] *See* Microsoft, *Windows XP Support has ended*, https://support.microsoft.com/en-us/help/14223/windows-xp-end-of-support (last visited May 15, 2018).

[81] *See* BSA The Software Alliance, *Seizing Opportunity Through License Compliance: BSA Global Software Survey* 6–7 (2016), http://www.bsa.org/~/media/Files/StudiesDownload/BSA_GSS_US.pdf.

[82] *Id.* at 4（マルウェアと無許可のソフトウエアの「強い相関関係」を議論する）

[83] National University of Singapore, *Cybersecurity Risks from Non-Genuine Software, The Link Between Pirated Software Sources and Cybercrime Attacks in Asia Pacific* 6 (Nov. 1, 2017), https://news.microsoft.com/uploads/2017/10/Whitepaper-Cybersecurity-Risks-from-Non-Genuine-Software.pdf
（「世界の多くの地域において、海賊版、偽造または非正規のソフトウエアを使用する事は、サイーバリスクを高める重大な要因となり、経済への被害拡大と生産性低下の原因となる。またサイバー犯罪攻撃が増え関連した損失も増える」）