Japan Computer Emergency
Response Team Coordination Center

電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2014.11.17 10:27:54 +09'00'

サイバーグリーンの背景について

一般社団法人 JPCERT コーディネーションセンター

2014 年 11 月 17 日

「サイバーグリーン」の背景について

１．国際連携によるサイバー空間のクリーンアップのための取組みとしての「サイバーグリーン」

近年蔓延しているサイバー攻撃の攻撃基盤は、次の二つに大きく依存している。まず、マルウエアやボットに感染している PC 群は、サイバー攻撃の踏み台として利用される。また、設定ミスや旧バージョンのソフトウェアの利用などの点で脆弱な端末やサーバーもサイバー攻撃に組み込まれ、攻撃に加担させられていると考えられている。これらの近年の攻撃基盤の特徴としては、

1. ボットネットを構成する端末群に代表されるように量的・速度的な拡大が著しく、
2. インターネットの普及とともに易々と国境を越えて拡大している。

ということがあげられる。このような状況で、各国 CSIRT における現在のサイバーリスクへの対応・調整活動には、次のような課題があると認識されている。

1. インシデントの発生をベースとして対応・調整を開始するインシデント駆動型である場合が多いため、攻撃基盤そのものを制圧することに結び付きにくい。
2. 各国 CSIRT がそれぞれの国内で対応・調整を行う分には相対的に問題が少ないが、各国 CSIRT 間での相互協力・連携が必要な場合には、個人的な信頼関係に頼る場合が少なくなく、組織的・効率的な相互協力・連携が十分にできていない場合がある。それゆえ、国境を越えた攻撃基盤に対する対応・調整活動が有効に結び付かないことがある。
3. 各国 CSIRT ではそれぞれが何らかの測定を行ってサイバーリスクの動向を把握する努力をしているが、その指標に共通の基準がないために相互に比較することができていない。
4. インシデントの数が増大しており各国 CSIRT の対応・調整能力を量的に圧迫しつつある。

加えて、各国 CSIRT からの調整先となる、インターネットサービスプロバイダ、通信事業者などにおいても、技術的または法的にできること、できないことがあるのはもちろん、コスト負担等ビジネス上の観点から効果の判定や実施の可否が問題になる場合など、対応上の検討事項は多いと考えられる。

そこで、「サイバーグリーン」と名付けた取組みとして、このような攻撃基盤に対して、各国 CSIRT や対応する事業者などとの間で連携して適切な対応・調整活動を行い、インターネット及びサイバー空間を妨害行為や犯罪の基盤として悪用しにくくするべく、関係者間でそれぞれの目的に応じた情報を共有し、対応に利用することでインターネットのクリーンアップにつなげるための枠組み検討を行うこととした。

サイバーグリーンにおける課題としては、以下の２点が挙げられる。この課題を克服することにより、各国 CSIRT は、国境を跨ぐ攻撃基盤に対する対応・調整についても、より効率のよい連携ができるようになると考える。

1. グローバルな対応・調整活動を行うための連携メカニズムの構築
2. 相互比較を可能とするために、インターネットエコシステムの健全性を測定する共通の指標の確立

２．サイバーグリーンの取組をグローバルかつ中立的に実現するための調査・研究事業としての「サイバーグリーンプロジェクト」

これらの課題への対応を検討するため、JPCERT/CC では、2014 年度から、経済産業省の委託事業中の調査研究事業として「サイバーグリーンプロジェクト」に取り組んでいる。

(1) まず、「インターネットエコシステムの健全性を測定する共通の指標」を確立するために、以下の検討を進めている。

1. 先行事例を調査して既存の指標に関連するベストプラクティスを特定する。
2. そのために、CSIRT や研究機関、あるいは主要企業における事例や、優れた研究者の業績を調査する。
3. 同様に、指標を計算する元になるリスク環境要因の収集方法、計測手法について、既存のベストプラクティスを調査する。
4. リスク環境要因の収集に協力を仰ぐ組織などとの関係を確立してデータを継続的に入手する方法を検討する。
5. そのようにして得たデータを格納するデータベースもしくはストレージについて検討する。
6. これらのデータを入力として、比較可能で堅牢な定量的評価のための指標を策定する。さまざまな側面を持つセキュリティの実態を反映して、複数の指標が必要となる。既存の指標の活用と同時に、必要に応じて独自の指標を開発していく。

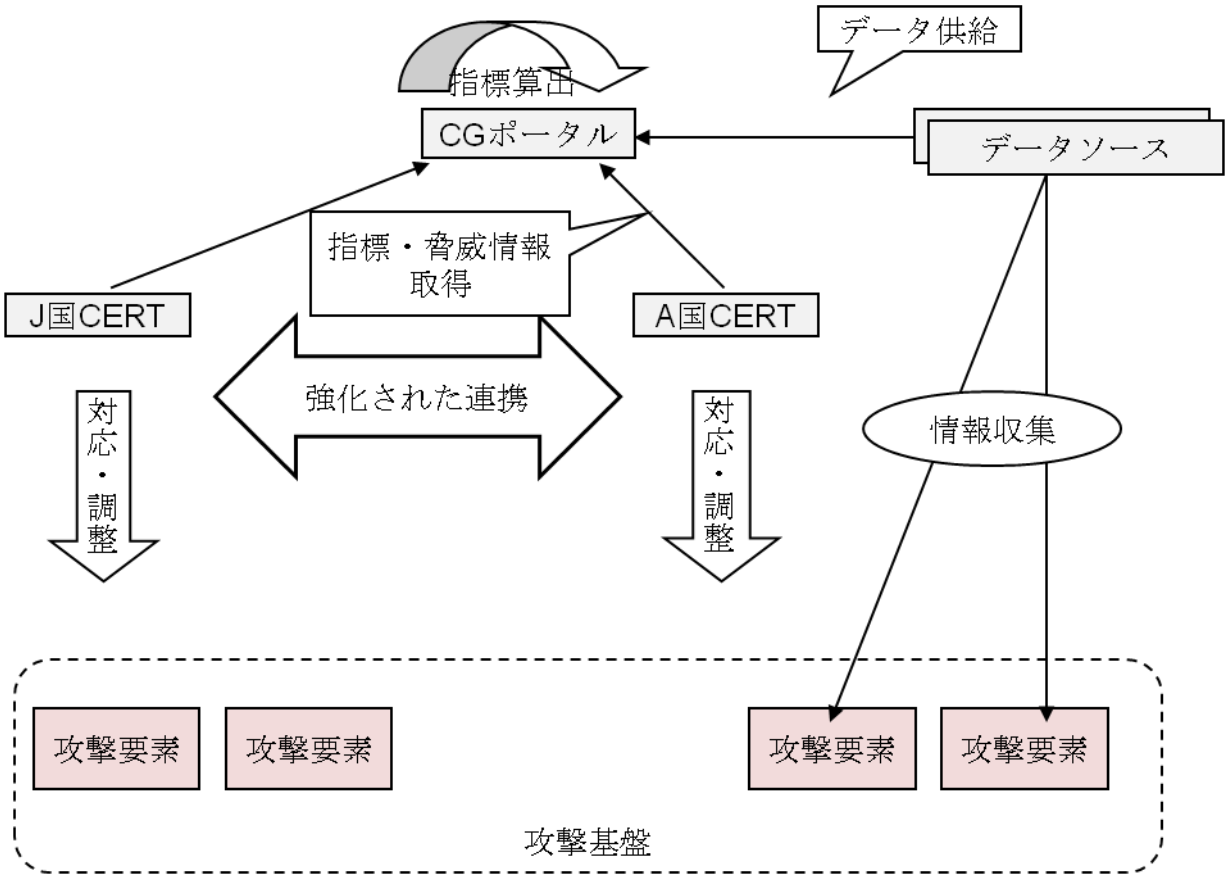
(2) さらに、これらの指標を各国 CSIRT の間で共有するために、情報共有メカニズム（ポータル）を構築する必要がある。このポータルは、

1. 各国 CERT の対応・調整活動の連携を図るための基盤として
2. WebGUI を備えたポータルサイトの形式で
3. このポータルを介してリスク環境要因データの提供、指標の閲覧を可能にし
4. また、このポータルを介して各国 CERT 間の連携のための対話の少なくとも一部を可能にする

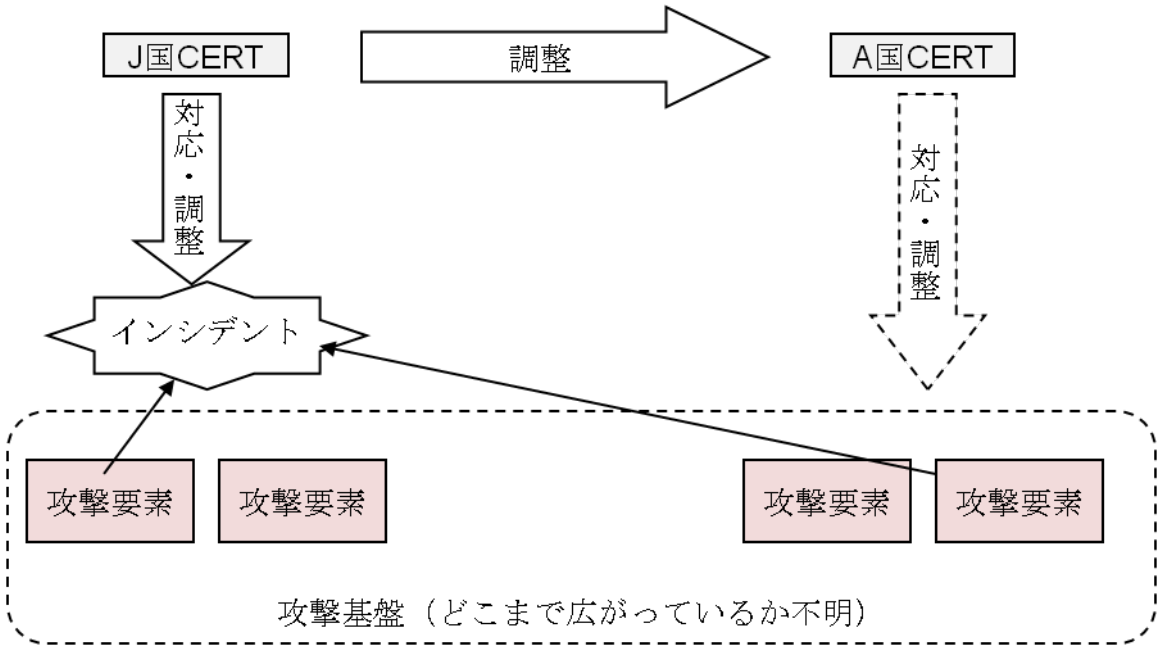
このような指標とポータルを構築することで、サイバーグリーンプロジェクトは、サイバーグリーンの基盤を以下のように提供することを期待している。

1. 国境を跨ぐような攻撃基盤に関する各国 CERT の状況認識を統一することができる。
2. また、各国 CERT から見てそれぞれの国内に存在する攻撃基盤が、実は国境を跨ぐ攻撃基盤の一部であることを確認することができる。
3. これによって、各国 CERT がその対応・調整活動を連携して行うことが可能となる。
4. 相互比較可能な指標により、リスク要因の優先順位付けから、リソース配分にいたる、様々なレベルの意思決定を支援する。

参考１：サイバーグリーンプロジェクトにおける情報共有経路

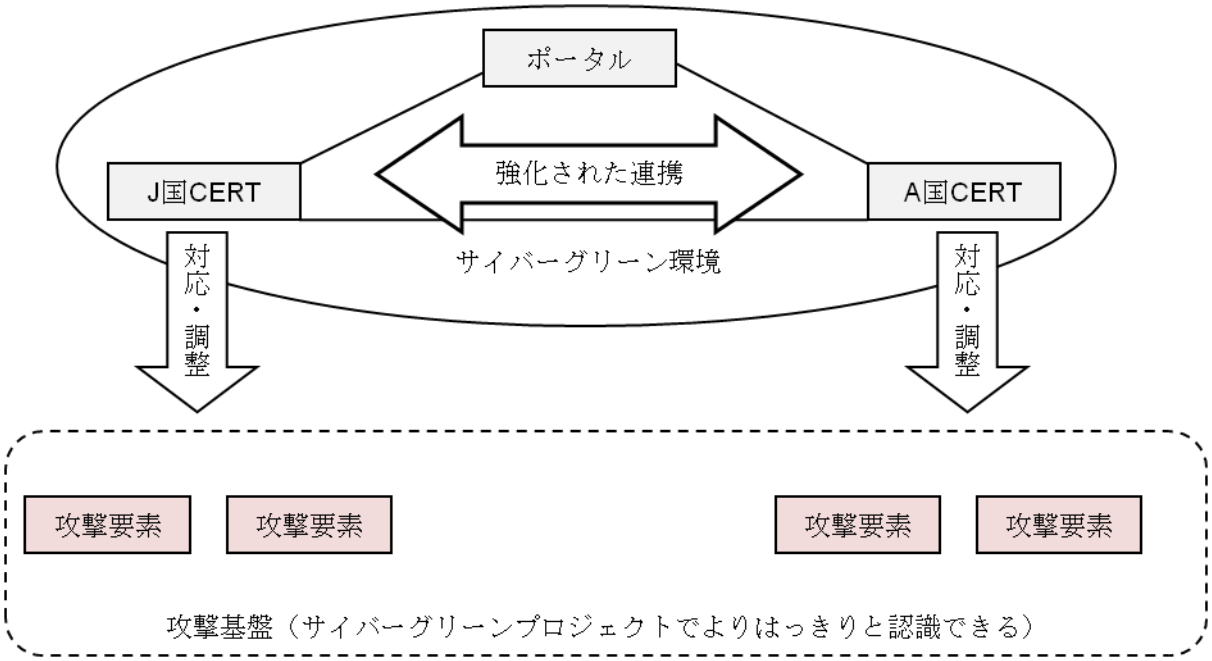


参考２：現状のインシデント対応模式図



1. J 国でインシデントが起きると、J 国 CERT がインシデント対応・調整を開始する。
2. インシデントの構成要素の一部が A 国にも存在することが判明すると、J 国 CERT は A 国 CERT に連絡して協力を要請する。
3. A 国 CERT による A 国内の攻撃要素への対応・調整は、現状では人的つながりに頼るなど必ずしも常にうまくいく状態ではない。
4. インシデントへの対応はある程度成功するものと思われるが、その原因となった攻撃要素への対応については、インシデント件数増加に追われて手が回らない状態である。
5. 攻撃要素の集合体である攻撃基盤がどのようなものかという認識も、把握しきれていないのが現状である。
6. 今後は、インシデント対応に終始するだけでなく、共通の指標を用いて各国 CERT 相互が連携し、攻撃基盤への対応を進めていく必要がある。

参考３：サイバーグリーンプロジェクトが目指す対応模式図（案）



1. 各国 CERT はサイバーグリーンプロジェクトが提供する共通の指標とポータルによって平時から連携を強化している。
2. 指標計算を目的とした計測を平時から行っているため、攻撃基盤に対する認識がより正確なものになる。
3. これによって、インシデント対応においても攻撃基盤への対応においても、各国 CERT がより強く連携して対応することができる。