CYBER GRID JOURNAL

サイバー・グリッド・ジャーナル

VOL.4

特集

サイバー戦から読み解くサイバーセキュリティ

日本のサイバー防衛が備えるべき要件

CYBER GRID JOURNAL VOL.4

TABLE OF CONTENTS

巻頭言

脅威情報を活用して先進的で実効性のあるセキュリティ対策の支援を目指します

小笠原 恒雄
次世代技術開発センター長

サイバー攻撃の脅威が社会的な課題となっています。そこで今回のサイバー・グリッド・ジャーナルでは、「脅威情報」に焦点を当てました。

「脅威情報」に注目が集まる背景

サイバー・グリッド・ジャーナルの読者の中にも、「脅威情報」に関してご存じない方がいらっしゃることでしょう。脅威情報とは、Cyber Threat Intelligence（サイバー・スレット・インテリジェンス、サイバー脅威インテリジェンスなど表記はさまざま）の和訳で、サイバー攻撃という脅威に関する情報を集約・蓄積し、分析することでセキュリティ対策に活かす取り組みのことを指します。

ラックは日本におけるセキュリティサービスの先駆者として、日本最大級のセキュリティ監視センターや、サイバー救急センターを運営しています。間断無くセキュリティ対策を支援するこれらのサービスにおいては、サイバー攻撃に関係するさまざまな情報が収集され、その情報量は膨大なものとなります。そこでラックは、脅威情報の実現に向け、収集した情報を活用するための研究を行っています。

脅威情報の研究を進めるに当たり、収集した情報をいかにしてセキュリティ対策に活かすかを考え始めたとき、まずは情報から得られる攻撃者の意図や、攻撃の手口をお客さまにお伝えし、被害を最小限に食い止める取り組みが重要だという結論に達しました。そこで実施しているのが、CYBER GRID VIEWの発行や注意喚起情報の発信といった情報提供です。

続いてラックは、2016年8月に次世代技術開発センターを設置し、さらなる情報提供の拡充と対策手段の提言を行う取り組みを開始しました。

ラックは、日本でセキュリティサービスを生み出し、お客さまのご支援の下で成長してきた企業です。膨大に得られる国内の脅威情報を、未だ見ぬ脅威に対する「新たな気付き」につなげてお客さまを守るための、研究開発や業界連携を推進します。

今回のサイバー・グリッド・ジャーナルから、脅威情報とはいかなるもので、どのように活用されるべきかを知っていただき、そして読まれた皆さまが自分事として活用に目を向けてくださることを期待しております。

特集

サイバー戦から読み解くサイバーセキュリティ

日本のサイバー防衛が備えるべき要件

佐藤 雅俊

サイバー・グリッド・ジャパン
ナショナルセキュリティ研究所長
CISA（公認情報システム監査人）

1984年防衛省航空自衛隊入隊。第3高射隊長兼ねて霞ヶ浦分屯基地司令、第23警戒管制群司令兼ねて輪島分屯基地司令、航空システム通信隊システム管理群司令等の職を経て、2014年サイバー戦を行う部隊として創設されたサイバー防衛隊の初代隊長として自衛隊のサイバー部隊の育成に尽力した。2017年航空自衛隊を退官（一等空佐）、同年ラックに入社し、現在はナショナルセキュリティの観点から各種研究を行っている。セキュリティに関する啓蒙活動として、メディアにおいてサイバー戦に関するコメンテーター対応を行う傍ら、多くの組織においてサイバーセキュリティに関する啓蒙活動を展開。また週末は、趣味のヨットを通じてセーリングの楽しさを普及するための活動を実施している。

はじめに

今年の1月に自衛隊を退官し、ナショナルセキュリティ研究所長に就任した佐藤と申します。自衛隊では初代のサイバー防衛隊長を拝命し、多くの経験を積みました。本日はその経験を踏まえて、私個人の見解をお話ししたいと思います。

皆さまは、サイバー戦が遠い世界の出来事だと思っていませんか？ サイバー空間は、陸・海・空・宇宙に続く第5の戦場（図1参照）ともいわれており、今もまさにそこで戦いが行われています。サイバー戦は他の領域での物理的な戦いと異なり、イメージしにくいかもしれません。エストニアとロシアの例を挙げてみると、エストニアがNATOに加盟したことによって両国の関係が悪化し、2007年にエストニアの首都タリンに設置されていた解放者の像を撤去したことを機にロシア系住民の暴動が発生し、ロシアからのサイバー攻撃を受けたといわれています。この際には、エストニアの政府Webサイトが利用できない状態が3週間以上続いたと報道されました。IT立国を標榜してインターネットの活用を推進してきたエストニアでは、銀行や図書館、病院等の多くのサービスがインターネットに依存していましたが、攻撃のターゲットが公共機関や企業等にも拡大したことから、サービス停止により市民生活に多大な影響が出たといわれています。また、ウクライナとロシアとの関係では、2014年にロシアがウクライナのクリミアを分離独立させ編入したことから、両国は事実上戦闘状況に陥りました。2015年及び2016年にウクライナ西部で発生した大規模な停電はロシアからのサイバー攻撃によるものと報道されており、この攻撃ではインターネットを利用しない市民の活動にも深刻な影響が発生したことになります。

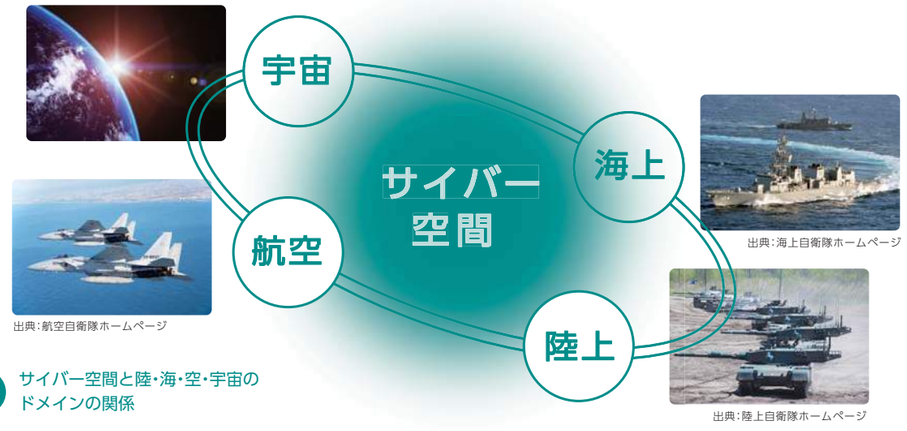


図1 サイバー空間と陸・海・空・宇宙のドメインの関係

このような国家が関与したと疑われる攻撃では、攻撃者は相手の力の中心である重心[1]を狙い周到に準備し、ここぞというタイミングで攻撃を発動します。偵察活動や工作活動等には時間がかかることから、攻撃のための活動はこれから行われるのではなく、すでに行われていると考えるべきです。

このように、サイバー空間における戦いでは緊張感が高まっている状況にあるにもかかわらず、日本では攻撃を受けるとシステムやそれを管理している人に落ち度があるように見られがちです。情報漏えい事案が発生するたびに開かれる謝罪会見を目にすると、第5の戦場を知る者としてはやるせない気持ちになります。もちろん、「妥当な注意」を払わない経営者は誇りを免れないでしょうが、本来断罪されるべきは加害者であると思います。

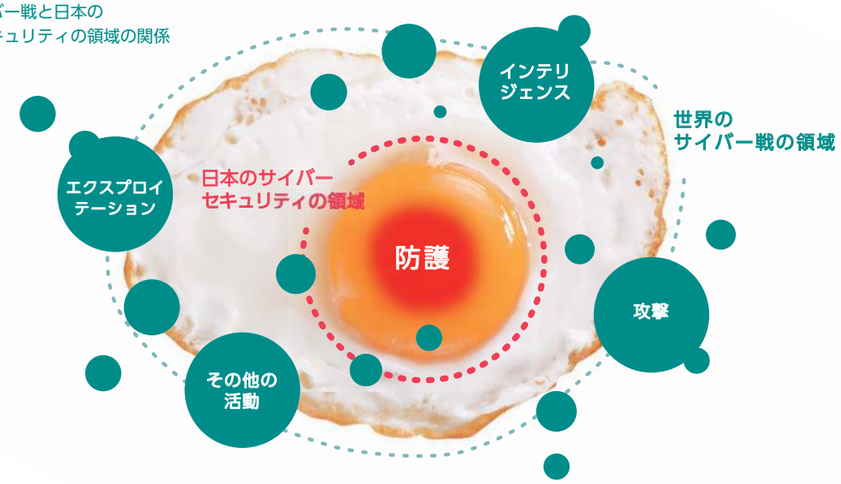
何故このような対応になるのでしょうか？ 本稿においては、世界で行われているサイバー戦の中で日本のサイバー防衛がどのような特性を有しているのか、また、戦いの原則という観点でサイバー戦を考察した場合、日本のサイバー防衛が備えるべき要件は何なのか所見を述べたいと思います。

1 クラウゼヴィッツ「戦争論」参照、重心とは敵の力の中心であり、弱点でもある。この重心を攻撃することによって敵の撃破、すなわち戦争の目標が達成される。

サイバー戦と日本のサイバー防衛

外国の方と話をすると、「日本のサイバー防衛には常識が通じない」などと言われることがあります。「あんたには言われたくないよ」と思いながら話を聞くと、それは、世界で行われているサイバー戦と日本のサイバー防衛の活動範囲の違いに起因していることに気が付きます。ご承知のとおり日本のサイバー防衛はサイバーセキュリティ基本法とサイバーセキュリティ戦略の上に成り立っています。基本法の目的はインターネットの効果的かつ安定的な利用ですので、いかに安全にインターネットを活用するかにフォーカスしたものとなっています。一方、世界で行われているサイバー戦は、防護だけではなく、相手を特定する活動や、攻撃もその領域に含まれています。米国の軍事ドクトリン[2]では、サイバー戦はそれらの活動に加え、インテリジェンスを含むものとして定義されています。また、中国においては、中国の戦略である三戦[3]「心理戦」「法律戦」「世論戦」の中で、外交・安全保障だけではなく経済面を含む全ての活動の中で戦略的に運用されていると考えられます。世界のサイバー戦と日本のサイバー防衛との関係は、いわば、卵と黄身の関係 図2参照 にあるといえます。日本が行っている活動はサイバー戦の核心ではありますが、全てではないのです。この活動領域の違いに対する認識のずれが、日本のサイバー防衛に常識が通じないといわれるゆえんであると感じています。

図2 世界のサイバー戦と日本のサイバーセキュリティの領域の関係



日本のサイバー防衛に潜む慢性的なセキュリティホール

日本の多くの経営者の方々は、日本のサイバーセキュリティ戦略に沿って活動していることと推察しますが、それだけでセキュリティが十分に守られているとはいえません。政府が示しているのは最低限のガイドラインや基準に過ぎないからです。例えると、ドアに最低限のロックを掛けている状態の企業に対し、攻撃者はロックを破るための手法を次々と考案し、さらには、ドア以外の窓や煙突からの侵入の可否をも探っている状況です。とても十分な備えとはいえません。

攻撃者の特定についても、現行の日本の法律の枠組みでは、ドアをノックされても相手の名前を尋ねることはできません。ノックの音や足音に耳を澄ませ、不穏な行動に気付いた場合には、警察に通報して捜査を依頼しなければならないのです。警察側も具体的な被害が確認できないと動けないのが現状ですので、さながらストーカー対処のような様相となります。この、自らを守りにくい環境が、日本の慢性的なセキュリティホールであると感じています。

2 CYBER OPERATIONS（J-pub3.12）　3 中国人民解放軍政治工作条例2003年

戦いの原則から見たサイバーセキュリティ

ビジネスにおいて、事業をいかに運用するかは事業戦略上の重要な考慮事項になると思いますが、軍事作戦を考える上では、運用のベースとなる考え方として「戦いの原則」があります。孫子の兵法やクラウゼヴィッツの戦争論等がそれに当たり、長い年月を伴う実戦を経て原理原則として昇華するに至っています。私が所属していた航空自衛隊でも、幹部の必須教育としてこれらの原則を学びました。

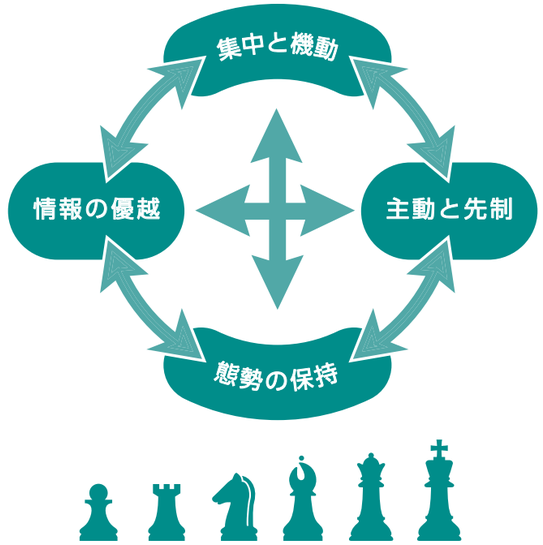
戦いの原則を構成する主要な項目は4つあります。

1つ目の原則は「態勢の保持」で、部隊が常にその精強を維持して不敗の態勢を確立し、侵略を未然に抑止するとともに即応の態勢を堅持することです。2つ目の原則は「情報の優越」で、機を制して主動に立ち、戦勝を獲得するためには不可欠の要件です。平時から一貫した組織の下に継続的に情報を収集し、敵の動きを未然に察知し敵に先んじて準備し、初動において勝機を捕捉することを指します。3つ目の原則は「主動と先制」で、機を制し主動の地位に立つことで戦勝獲得のための要道となすものです。4つ目の原則は「集中と機動」で、戦闘力を適時要点に集中発揮し戦勝を獲得することをいいます。戦いの状況により、適応する原則の重み（重心）は変わりますが、それぞれの原則は相互に作用する関係 図3参照 にあります。防御が主体となる日本のサイバー防衛では、敵からの攻撃に対していかに迅速、的確に対応できるかが活動の重心で、「態勢の保持」が主要な原則になります。しかしながら、即応の態勢を維持するためには、最新の攻撃に対応できる技術的スキルに加え、決して負けないというモチベーションが必要です。また、たとえ十分な態勢を取ったとしても、システムの欠陥や人為的な失敗による固有リスクは残りますので、システムを完璧に防御することはできません。相手が見えない暗闇で、いつ辻斬りに襲われるかと怯えながら夜道を歩いているような状況が続くことになります。この暗闇に灯火をつけるのが、戦いの原則における「情報の優越」だと考えます。孫子の兵法にいう「敵を知り己を知れば百戦危うからず」に当たります。

防戦における「情報の優越」の必要性を示す戦例を見てみましょう。第二次世界大戦において、日本はミッドウェー海戦で敗北しましたが、この際は敵空母の位置情報を入手できず、敵航空機からの奇襲攻撃を受けて多くの艦船を失い、その後の戦いで劣勢が決定的になったといわれています。

サイバー攻撃には、多様性、匿名性、隠密性、攻撃側の優位性、抑止の困難性、相手を特定する困難性等の特性[4]があるといわれ、常に新しい攻撃手法が考案され、テストされています。さらにサイバー攻撃は弱者の兵器ともいわれ、資金の少ない国、場合によっては個人すらも戦いの主体となり得ます。多様な攻撃に加えて不特定の相手にも対応する必要があるのがサイバー戦です。攻撃側が圧倒的に優位な状況下において、少しでも早く、相手の攻撃手法や使用するマルウエアについての情報を得て、対策を取ることは防護の劣勢を改善する必須の要件であると思います。

図3 適応する作戦の原則の関係



4 防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて（平成24年9月防衛省策定公表）

「情報の優越」とサイバー・スレット・インテリジェンスの活用

最近、カンファレンス等ではサイバー・スレット・インテリジェンス（CTI）[5]という言葉をよく耳にします。この言葉は、2014年ごろからFIRST[6]等の国際的なカンファレンスで使われるようになってきていますが、もともとは米軍において、サイバー戦の領域でインテリジェンスとの融合が必要であるとの議論が行われるようになり、サイバー戦における「情報の優越」を獲得するための手法として使われるようになったものと認識しています。CTIとは、一言でいうと敵をプロファイリングすることで、オープンソース等から情報を集めて攻撃手法や使われているマルウエア等の種類をマッピングし、類似性や関連性を分析して軍やその他が保有する一次情報（直接入手した情報）と相関を取ることにより、情報の精度や粒度を高めサイバー防衛に役立てようとするものです。

敵の行動や攻撃手法等が可視化できれば、全く予測できない暗闇のような状況に、ようやく足元を照らす薄明かりの灯火を点灯することができます。つまり、「情報の優越」を獲得するための現時点で考えられる有効な手段がCTIなのです。

もしもあの時CTIがあったなら

やられてボコボコになった話をするのも癪なので、希望を持って過去に発生したサイバーインシデントに対して、「もしもあの時CTIがあったなら」という、タラレバの話をしてみましょう。

2011年に防衛関連企業がサイバー攻撃を受けて個人情報等が漏えいしたとされる事案を例にしてみます。この事案は一企業の情報漏えい事案と捉えられがちですが、サイバー戦という視点で考えると思考の幅が広がり、別の見方ができます。NISC[7]が公表した資料に基づき、日本以外の関係国の状況も考慮してインシデントを時系列で並べてみます。

① 2011年3月：複数の米国企業が中国からハッキングを受け、防衛関連情報が漏えいしたとの報道。
② 2011年4月：複数の日本の防衛関連企業（A社、B社）がサーバーへの不正アクセスを受けた。
③ 2011年8月：日本の防衛関連企業C社のサーバーが攻撃を受け、情報が漏えいした可能性がある。
④ 2011年9月：日本の防衛関連企業C社へのサイバー攻撃が確認されたと報道。
⑤ 2011年10月：中国の関与が疑われるとの報道。
⑥ 2011年12月：中国はこれらの報道を否定。

次にこれらのインシデントについて、中国の関与の可能性について背景を分析してみましょう。

① 中国は、経済の競争力を強化して西側諸国との科学及び技術ギャップを埋めることを目的として、1863年に863計画を策定し経済・技術情報を収集していた。
② 軍事的には、2009年以降に空母の活動を本格化するため、空母の最大の脅威である潜水艦の能力等に関心を持っていたと推察される。
③ 折しも日本では、2010年武器輸出等3原則の見直しの議論が開始され、輸出する武器の候補として救難機や潜水艦を検討していたことから、通常型潜水艦では世界でもトップクラスの性能を持つといわれる日本の潜水艦技術情報に対して、中国が強い関心を寄せ、情報を搾取しようとしていたと推察される。

以上が中国からのサイバー攻撃を想定した場合の背景です。

これらの背景を踏まえて、改めて発生したインシデントを分析してみると、2011年8月にC社から情報が漏洩したとされる以前に対策が取れた可能性が幾つか見つかります。

1回目のチャンスは、2011年3月頃に中国が米国の防衛関連企業に対するハッキングに成功したと報道された時点にあります。改定された日米防衛協力の指針の枠組みでサイバー攻撃に関する情報を日米間で共有[8]し、米国で発生した事案をもとに日本の防衛関連企業の情報搾取に利用される可能性を予見して、攻撃で使用されたマルウェア等の情報を入手できていれば、日本の防衛関連企業に対して警報を発令することが可能であったと考えられます。次の機会は、2011年4月に防衛関連企業のA社、B社がサーバーへの不正アクセスを受けた時点です。企業がこれらのアクセスを検知し、国に対して迅速に報告できていれば、国は関連する企業に対し、システムの異常の有無について調査を要請することが可能であったと考えられます。最後の機会は、2011年8月にC社が自社内のサーバーへ不正なアクセスを受け始めた時点です。不正なアクセスを検知できれば、セキュリティ装置のパラメータの変更等により情報漏えいを防げたかもしれません。さらに攻撃相手側の特定に至れば、外交的な対応も可能となります（図4参照）。つまり、あの時CTIがあったなら、被害を極限まで抑えることができた可能性があったといえるでしょう。

図4　発生事象とベストプラティクス

日 時	発生事象	ベストプラティクス
2011年3月	複数の米国企業が中国からハッキングを受け、防衛関連情報が漏えいしたとの報道	日本の防衛産業に対する警報
2011年4月	複数の日本の防衛関連企業（A社、B社）がサーバーへの不正アクセスを受けた	・攻撃発見 ・防護対策の実施
2011年8月	日本の防衛関連企業C社のサーバーが攻撃を受け、情報が漏えいした可能性がある	・攻撃発見 ・防護対策の実施
2011年9月	日本の防衛関連企業C社へのサイバー攻撃が確認されたと報道	報道対応
2011年10月	中国の関与が疑われるとの報道	・攻撃者特定 ・外交的対応
2011年12月	中国はこれらの報道を否定	外交的対応

5 日本においては「脅威情報」という言葉が一般的に使われていますが、米国由来の言葉であること及び情報がinformationを意味するのかintelligenceを意味するのか曖昧であることから、ここではサイバー・スレット・インテリジェンスという言葉を使用しています。
6 Forum of Incident Response and Security Teams
7 National center of Incident readiness and Strategy for Cybersecurity／内閣サイバーセキュリティセンター
8 新日米防衛協力のための指針（H27.4.27）により、日米両政府は、サイバー空間の安全かつ安定的な利用の確保に資するため、適切な場合に、サイバー空間における脅威及び脆弱性に関する情報を適時かつ適切な方法で共有する。また、日米両政府は、適切な場合に、訓練及び教育に関するベストプラクティスの交換を含め、サイバー空間における各種能力の向上に関する情報を共有する。日米両政府は、適切な場合に、民間との情報共有によるものを含め、自衛隊及び米軍が任務を達成する上で依拠する重要インフラ及びサービスを防護するために協力する。

点の防御から面の防御へ

2014年に米国のソニーピクチャーズが北朝鮮の金正恩総書記のパロディ映画を公開しようとして、北朝鮮からのサイバー攻撃を受けたといわれる事例は、サイバー戦の特徴である防御の困難性を示す適例であると思います。この際、北朝鮮は米国に対し公開を中止するように警告し、米国としても相当程度に警戒していたと思われますので、北朝鮮VS米国という明確な構図の中で繰り広げられたサイバー戦であったと捉えることができます。結果として、ソニーピクチャーズのシステムが停止し、情報が漏えいしたことから120億円程度の損害が発生したと報道されています。日本の数十倍のリソースをサイバー関連分野に割いている米国ですら攻撃を防ぐことができなかったことから、セキュリティに携わる者だけでなく、多くの方へ衝撃を与えた事件であったと思います。

それでは、日本はいかにして防衛していけばよいのでしょうか？その成否を握るのは「情報の優越」であり、そのためのCTIの活用であると考えます。先述のとおり、日本のサイバー防衛は専守防衛という国の方針に従い、相手側の特定、攻撃、諜報活動等について制限を受けています。その中でCTIを真に機能させるためには、現行のJ-CSIP[9]等の情報共有の枠組みを発展させ、重要インフラに関する情報だけではなく、軍事面を含めた全ての分野において官・民が一体となって情報を収集し、分析する情報プラットフォーム（図5参照）のような態勢が必要であると考えます。津波警報は、津波の発生を探知し、到達時間や到達地点を予測することにより、津波の被害を少なくする可能性を高めますが、これらの警報を適時適切に発令するためには、予報の精度を検証するための現場のAs Is情報が必要になります。サイバー戦においても、国が攻撃予兆等を分析するためには、民間で起きている事象を正確に把握する必要があります。それらの情報を多角的に分析することで、攻撃傾向や予兆を掴むことが可能になるからです。

これまで企業は、保有する情報を守るためにシステムを要塞化して、攻撃を受けないシステムの構築にリソースを投入してきました。いわば点の防御です。しかしながらこの守り方は、入手できる情報のソースが限られ、分析できる幅が狭いことから、結果的に攻撃を防ぐ機会を逃すことになります。発生するインシデントの影響を最小限に抑え、攻撃者を特定するためには、点の情報をつなぎ合わせて面にする工夫が必要になります。面で防御することにより、攻撃兆候を予見できれば、インシデントに対処する機会が増えると考えます。

図5 脅威情報プラットフォームのイメージ

おわりに

世界のサイバー攻撃の状況を観測していると、2015年以降はオープン系システムへの攻撃に加え、クローズした環境の制御系システムへの攻撃も多数検知されるようになってきています。制御系への攻撃は市民生活にも多大な影響を及ぼしますし、場合によっては死傷者が出る懸念もあります。また、本年5月に拡散した「WannaCry」という身代金要求型のランサムウエアでは、全世界150カ国30万件以上のシステムに影響が出たと[10]報じられています。この攻撃は、金銭搾取の脅迫の手段としてコンピューターのデータを暗号化してしまうので、金銭搾取による被害に加えて、システム停止によって業務継続にも影響が出ました。被害を受けた企業は、身代金の支払いに応じるまでデータが使えない、また、払ってもデータが復元されない、まさに「泣きたい（WannaCry）」状態に追いやられてしまいました。

さらにこの攻撃では、システムの脆弱性を突いて組織内のパソコン間でも感染するような挙動が確認されていますので、対策を行っていなかった組織では、被害端末が一気に拡大したと見られます。攻撃手法は日々進化し常態化していることを認識しなければなりません。

2020年には待望の東京オリンピック・パラリンピックが開催されますが、平和の祭典に向けて我が国もIT化がさらに進み、某国からのサイバー攻撃の対象になることは想定しておかねばなりません。今年5月の報道では、政府が電力や鉄道等の重要インフラが攻撃を受けた際に、サイバー手段による対抗措置を取れるよう検討に入ったと[11]されています。一刻も早い法制化が待たれるところです。法制化が整うまでどのくらい時間がかかるかわかりませんが、それまで座しているわけにはいきません。国と民間が今まで以上に協力・連携してオールジャパンで対応するアクティブな防御が、日本のサイバー防衛に求められています。粛々と攻撃を迎え撃つなどという幻想は通じないことを肝に銘じなければなりません。

9 IPAは、サイバー攻撃による被害拡大防止のため、2011年10月25日、経済産業省の協力のもと、重工、重電等、重要インフラで利用される機器の製造業者を中心に、情報共有と早期対応の場として、サイバー情報共有イニシアティブ（J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan ）を発足させました。

10 米高官サイバー攻撃の被害は世界150カ国で30万件以上（NHK5月16日）
11 サイバー攻撃に対抗措置（日経5月17日）

リサーチャーの眼

研究・開発の最前線からお届けする技術情報

第4回

攻撃者の先を行く！ 進化するサイバー攻撃から 日本を守る脅威情報の取り組み

仲上 竜太　次世代技術開発センター チーフリサーチャー

進化し続けるサイバー攻撃！我々が取り得る策は？

テクノロジーの発展とともに進化し続けるサイバー攻撃は、攻撃の回数とともに複雑さを増し、身近な脅威として日常生活の中に迫っています。

今年5月に発生したランサムウエア(*1)「WannaCry」は、普段使われているパソコンの弱点を突く攻撃によって、世界中の組織で混乱を引き起こしました。

*1 ランサムウエア：コンピューターウイルスの一種。感染したパソコンのファイルを暗号化し、ファイルを復元するための身代金を要求する。身代金を払ってもファイルが復元される保証はない

また、一つの組織に標的を定め、組織や人間関係、ネットワークシステムを調べ上げた上でサイバー攻撃が行われる「標的型攻撃」では、被害の発見が難しく、人知れず大量の個人情報や重要機密が攻撃者に窃取されている事例も数多く存在します。

日々進化し、増え続け、悪質化するサイバー攻撃に対処するためには、攻撃の背後にいる攻撃者の次の一手を推測して、あらかじめガードを行っておく「先回り防御」の実現が効果的であると考えます。

先回り防御の実現に有効な知見＝インテリジェンスとは？

サイバー攻撃が行われた際には、攻撃者が残したサイバー攻撃の痕跡を丹念に読み解くことで、その背景や目的をある程度把握することが可能です。

通常、インターネット経由で行われるサイバー攻撃では、

- マルウエア（ネットワークに裏口を作ったり、遠隔操作や破壊を行ったりする不正プログラム）
- IPアドレス
- ドメイン名
- URL
- ファイル操作履歴

など、極めて少量ではありますが、不正行為にたどり着くことができるいくつかの痕跡が残ります。現在の防御体制は、このような痕跡の情報をもとに整備されており、過去発生した事案によって得られた「知見(＝インテリジェンス)」を活用する仕組みで基本的には構成されています。現在リリースされている最先端のセキュリティ対策ツールや先回り防御で未来や未知の脅威に対抗するといっても、この知見をもとに検知・防御を実現しているに過ぎず、今後も知見を活用したセキュリティ対策が基本になることに変わりはないと考えます。

このため、大量のデータが存在する社会における今後のセキュリティ対策としては、この知見をさまざまな角度から分析し、いかに有効活用していくのかが極めて重要です。このように、サイバー攻撃の痕跡から情報を組み合わせて攻撃者の姿を導き出す手法を「脅威情報（スレットインテリジェンス）」と呼び、サイバー攻撃へ対抗するための有効な手法として、ここ数年大きく注目を集めています。

サイバー攻撃には世界的な流行がある反面、国や地域によって特徴があります。

ラックは、日本のお客さまを中心に、重要な情報資産へのサイバー攻撃の監視やサイバー攻撃の被害に遭った際の救急処置、セキュリティに強い組織を作るコンサルティングなど、さまざまなセキュリティサービスを提供しています。そして、これらのサービスの提供を通じて蓄積した膨大な情報を分析し、サイバー攻撃の実態の解明を進めています。この調査の過程で、過去のサイバー攻撃との関連性を導き出し、これを「脅威情報」として対策に役立てるための研究開発を行っています。

脅威情報を創出するために

先回り防御を実現する「脅威情報」を創出するには、何が必要になるのでしょうか。

私たちは、脅威情報創出のためには、

■ 情報　■ 人材　■ 道具

の3つが必要になると考えます。

脅威情報の入手先：情報源

脅威情報を活用するためには、過去から現在までに行われたサイバー攻撃の情報を、大量に、しかも整理された状態で入手する必要があります。

脅威情報がセキュリティにおいて重要視されるようになった昨今では、情報源として活用可能な脅威情報サービスが存在します。

例えば、全世界で発生しているサイバー攻撃で利用されたマルウエアの情報を蓄積・提供するサービスや、過去に利用されたドメイン名とIPアドレスの紐付けを時系列順に記録し続けているPassiveDNSサービスなど、海外ではさまざまな企業や組織から特色ある脅威情報サービスが提供されています。

また、世界各国のセキュリティリサーチャーやセキュリティベンダーによって一般に公開されているブログやレポート、有志によって収集・蓄積されているサイバー攻撃に関するデータ集も、無料で手に入る情報ながらOSINT（Open Source INTelligence：公開情報をもとにした情報収集を行う専門領域）として、重要視されています。

これらは、自組織内で入手可能な情報とあわせて、脅威情報による対策を進める上で重要な情報源となります。

情報を活用する人材：脅威情報アナリスト

脅威情報を有効に活用するためには、サイバー攻撃の痕跡をいち早く見つけ出し、膨大な情報から攻撃者を推定する「脅威情報アナリスト」の育成が不可欠です。脅威情報アナリストには、ネットワークやソフトウエアの複合的な知識や、過去に行われたサイバー攻撃に対する知識、多様なサイバー攻撃のパターンから推測し検証する仮説検証能力など、高度な分析能力が要求されます。

セキュリティ先進国のアメリカでは、脅威情報アナリストの定義として、経営層に対する事業へのリスクとアクションプラン提示が業務領域に含まれているなど、幅広い役割が期待されている職種となります。

脅威情報を分析する道具：TIP（脅威情報プラットフォーム）

組織内でも数少ない脅威情報アナリストを支援するのが、TIP(Threat Intelligence Platform=脅威情報プラットフォーム)と呼ばれる分析システムです。

まずTIPは、組織内で独自に収集した情報や、外部の脅威情報をデータベースに蓄積し続けます。さらに、蓄積した膨大な情報に対して、半自動的に分析を行うことで情報の関連付けや選別を可視化し、脅威情報アナリストによる分析活動を支援します。

これらの人材やシステムを活用することで、脅威情報による防御を実現することが可能になります。

ラックが目指す脅威情報を活用したセキュリティコンセプト

サイバー・グリッド・ジャパン次世代技術開発センターでは、ラックならではの脅威情報を実現するべく、セキュリティサービスの現場と連携し、脅威情報の蓄積や分析、システムの開発を行っています。

その先には、脅威情報を中心として先回り防御を実現する、新たなセキュリティコンセプトである「SecureGRID構想」の実現を目指しています。

SecureGRID構想は、契約組織をグリッド状に結合することによって、わずかな攻撃兆候をリアルタイムに感知し、脅威情報プラットフォームとアナリストによる即応分析を通して、集団的に先回り防御を行うコンセプトです（**図1**）。

図1:「SecureGRID」コンセプト図

サイバー攻撃を集団で見張ることにより、日本を対象とした攻撃の兆候を早期段階で検知し、全体で防護を行うこのコンセプトは、組織ごとに行われている単体のセキュリティと組み合わせることで、より高度な防御を提供することが可能です。

SecureGRIDの実現により、日本の特定産業領域を狙った同一犯による標的型攻撃などの被害も、効果的に抑制することが可能になると考えています。

SecureGRID実現に向けた脅威情報の取り組み

ここでは、現在行っている脅威情報を推進する取り組みの一例を紹介します。

マルウエア自動収集分析システム（Malware Automated Hunting System/MAHS）

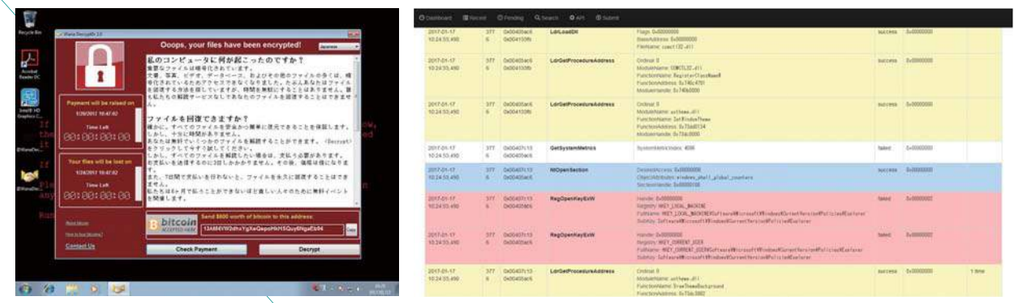


図2.先日発生したWannaCryのスクリーンショットと分析例

サイバー攻撃では、さまざまな種類の不正プログラムが利用されます。一例を挙げると、

- コンピューターに自由に侵入するためのネットワークの裏口（バックドア）を仕掛けるプログラム
- コンピューターを遠隔で自由に操って情報を収集するプログラム
- 業務を妨害するためにコンピューターを破壊するプログラム
- ファイルを暗号化して回復に身代金を要求するプログラム
- 他のコンピューターに勝手に大量アクセス攻撃を仕掛けるプログラム
- 銀行の口座へのアクセスを検出して送金先を書き換えたりパスワードを盗んだりするプログラム

等が存在します。

マルウエアと呼ばれるこれらの不正プログラムは、主にメールの添付ファイルや改ざんされたウエブサイトの閲覧を通じてコンピューターに侵入します。

マルウエア自動収集分析システムは、サイバー攻撃で利用される多種多様なマルウエアをインターネット上の情報源から自動的に収集し、解析用の仮想環境で実行することによってその振る舞いを記録するシステムです（**図2**）。

このシステムでは、収集したマルウエアに対して、以下のようなデータを記録します。

- 実行時に外部のサーバーからダウンロードされるファイル
- WindowsプログラムのAPI呼び出し情報
- アクセスするファイルやレジストリ
- 通信先や情報

これらの情報を分析することによって、攻撃者が利用するネットワークの情報や被害の検知に役立てることが可能になります。

TIP/脅威情報プラットフォーム

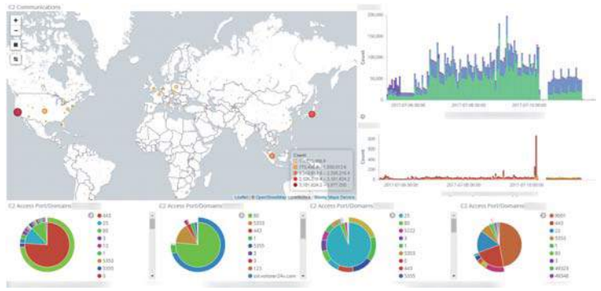


図3：脅威情報プラットフォームの一部

SecureGRIDの中核となるシステムが、TIPです。

TIPは、社内外から収集した脅威情報を蓄積し、アナリストが分析に必要な情報を効率的に検索・可視化するためのシステムです（**図3**）。

アナリストは、TIPを通して複数の情報源を横断的に検索することで、比較的短時間でサイバー攻撃の痕跡から攻撃者を推定し、次に行われる攻撃パターンを予測したり、攻撃に使用するネットワークや攻撃ツールから先回り防御用のデータを導き出し、作成したりすることが可能になります。

脅威情報連携プライベートSOCモデル

TIPはラック社内のアナリストがSecureGRID全体を防御するために利用する分析ツールですが、このシステムの一部をお客さまの側でも活用いただけるようにするのが、脅威情報連携プライベートSOC（Security Operation Center）モデルです。

このモデルは、お客さまの組織内で、ネットワーク機器やサーバー、端末から情報ログを収集、分析・可視化するシステムであるSIEM（Security Information Event Management）と、ラックの脅威情報プラットフォームを連携することによって、アラートとして検出された脅威の分析の自動化を可能にします。

脅威情報を活用するためには、システムの開発や人材育成など多くの投資と時間が必要となりますが、このモデルを利用することにより、お客さまの組織内でもスムーズに脅威情報を活用できる環境を整えることが可能になります。

脅威情報の活用が拓く、安全・安心なサイバー空間の実現に向けて

サイバー攻撃の被害に遭う可能性は、多くの場合、

- 利用しているOSやソフトウエアのアップデートを欠かさない
- サーバーやネットワーク機器などの情報資産を適切に運用する

といった、日々の基本的なセキュリティ対策によって低減することが可能です。

それでも防ぎきれない高度なサイバー攻撃から組織を守るためには、組織的なセキュリティ対策とともに、脅威情報を活用した先回り防御が効果を発揮すると考えています。

先回り防御を実現するためには、脅威情報にまつわるシステムの開発と並行して、日々発生するサイバー攻撃の痕跡を丁寧に観察し、分析の精度を高めていく地道な活動が何よりも重要です。

日本のお客さまとともに歩んできたラックならではの脅威情報を活用し、より安全・安心なサイバー空間の実現を目指してまいりたいと思います。

ラックの顔

第4回

マルチな能力を駆使して インターネットの健全化に立ち向かう

技術的な立場における国内CSIRTの窓口、JPCERTコーディネーションセンター（JPCERT/CC）。そこで国内外のインターネット健全化を目指す実証実験「サイバーグリーンプロジェクト」に従事する川崎基夫は、要件定義からコーディングにいたるまで、システム構築を一人でこなす多彩な能力を持つ。幅広い見識を有する川崎に、自らが手がけるプロジェクトの野望を聞いた。

川崎基夫
moto kawasaki

常に「時代を先取りする」サービスを立ち上げてきた

「過去、公称150万ユーザーを抱えるインターネットサービスプロバイダ（ISP）で働いていたときに20ラック分ほどのサーバーを自分ともう一人の人間で管理していまして。激務でどんどん体重が落ち、今より5、6 kgは痩せていましたね」。今でも十分にすらりとした体躯の川崎は、そんな過去のハードな経験を「面白かった」と語る、屈託のない空気感が印象的な人物だ。しかし、人当たりのよい笑顔の裏には、非常に多彩な見識が潜んでいる。それゆえ彼は、ラックの社内から「早く戻ってきてほしい」と声が上がる傍ら、現在籍を置くJPCERT/CCからは「ずっといてほしい」と請われる、引く手あまたの人材だ。

川崎とJPCERT/CCとの関わりは、ラック入社前の2007年にさかのぼる。ITセキュリティ予防接種のプロジェクトを実施するために、JPCERT/CCが協力企業を公募した際に、エンジニアとして手を挙げたことがそのきっかけだ。

メールの添付ファイルによるサイバー攻撃の危険性は今でこそ広く知られているが、当時はそういった危機意識が社会的にまだ希薄だった。それゆえ、立ち上げ当時のITセキュリティ予防接種サービスは鳴かず飛ばずの状態であったという。

2010年、川崎はラックへと籍を移して同サービスの立ち上げに関わる。その翌年、国内の大手企業がサイバー攻撃を受けたことを機に、同サービスの価値は一気に社会的認知を得ることとなった。次に川崎が取り組んだのが、サイバービジネスセンター（CBC）の開発だ。現在ラックの社長である西本の発案によるこのプロジェクトは、いわばデスクトップのクラウド化を実現するものであった。しかし、ITセキュリティ予防接種と同様、CBCのようなサービスも当時はまだ非常に先端的で、販路の開拓には苦労したという。

真に信頼できる客観的な指標づくりに挑む

2014年、サイバーグリーンプロジェクトのスタートに伴い、川崎は再びJPCERT/CCへと迎え入れられる。同プロジェクトでは、インターネット上のリスク要因を世界規模で縮小させることを目的として通信データのスキャンと解析を行い、国や地域間でインターネットのリスクを比較できる指標を立てている。この指標をもとに、リスクの高い国のナショナルCSIRTと連携し、セキュリティ対策をサポートしていくほか、将来的には、インターネット環境の構築にかけるリソースが不足している国などに対して、支援や指導を行うことも視野に入れているという。

しかし、現状の指標は通信やリスクの数をベースにした定量的なものであることから、通信規模とリスクの高さにどうしても比例関係が生じてしまう。そこで川崎が取り組んでいるのが、通信規模に左右されない、統計処理を施したスコアリングのシステム開発だ。ここで、先に述べた川崎の「多彩な見識」が大いに発揮される。川崎は、要件定義からアルゴリズムの設計、データ分析、コーディング、システムの実装と、開発フェーズのすべての工程に深くコミットしている。課題を俯瞰で捉え、改善策を洗い出すというマクロな視点と、実践的な技術力の双方を持つ川崎ならではのビジネススタイルだといえるだろう。

現在、開発は最終段階に入っているというが、データ解析によって明らかになったリスクに対しては同時進行で対応を進めている。特有のリスク要因が見られた国に対してアラートを出したほか、特定のオープン系サーバーを多数有する国内のISPに情報提供を行い、設定変更による改善へと導くなど、すでに成果は出始めているという。

川崎 基夫（51）

2010年入社。ITセキュリティ予防接種サービスの立ち上げや、クラウドサービスであるサイバービジネスセンターの開発、運用を担当。2014年4月、JPCERTコーディネーションセンター（JPCERT/CC）の国際部に情報セキュリティアナリストとして着任し、サイバーグリーンプロジェクトにおいて、インターネットの健全性とリスクを国別に比較するシステムの構築に従事。

視点はすでに、システムの「今後」に向いている

システムのリリース後には、弾き出された指標を持って世界中を飛び回る生活が始まるのでは？ と尋ねると、川崎は「その前に、まずはデータをしっかりと読み込むことが大切です」と答えた。「指標ももちろんですが、環境改善に結び付けるには、わずかなデータの変化を捉え、その意味を理解できる能力が必要です。そのためには、どれだけ地道に、自分の体を通してデータを読んでいるかが問われてくるでしょう」

そういった実直な一面を持つ川崎の視点はすでに、「顕著になったリスクに対応する」というシステム本来の目的の先に向いている。「データを解析してみると、大規模なDDoS攻撃などの前には不穏な動きや前兆現象のようなものがどこかにあります。天気予報ではないですが、そういうものを見つけ、事故を未然に防ぐシステムができればいいなと思います」

最後に、川崎はインターネット分野における日本の今後について語った。「欧米にはすでにいくつかありますが、インターネット上に公開されているさまざまな情報をデータベース化する組織、日本国内にもそれが必要でしょう。そしてそういった組織とJPCERT/CCが協力してインターネットを観測し、抽出した公共的なデータの上に立って議論をしていくような研究コミュニティ、「国際インターネット観測年」のようなものを日本発の施策としてぜひやってみたいですね」

インタビュー後に2人の愛娘について尋ねると、相好を崩した川崎。娘たちの喜ぶ顔見たさに、オフィス近くの老舗和菓子店で最中を買って帰るというエピソードに、家族を思うやさしさが垣間見えた。

活動のご紹介

近年、AIやIoTに代表される新たなテクノロジーの潮流が、ビジネス構造を変革しようとしています。企業がビジネスにおける優位性を維持するためには、新たなテクノロジーを自社の経営に戦略的に活用する必要があります。

テクノロジーが企業の経営を左右する社会においては、皮肉にもテクノロジーが悪意ある者にとっても有用な武器にもなり得ます。企業が安全で公正に取引を行い、社会が健全な発展を遂げるためには、悪意ある者から企業、ひいては社会を守るために最新のテクノロジーに裏打ちされた、セキュリティ対策が不可欠です。

サイバー・グリッド・ジャパンは、高度に巧妙化するサイバー攻撃とそれによる被害発生を防ぐため、2014年に発足しました。サイバー・グリッド・ジャパンの主な活動は、以下のとおりです。

情報分析・動向調査

高度な知見を有するリサーチャーが、サイバー攻撃の動向や各種公開情報などを集積・分析して防御に資する知見を見出し、積極的に活用・発信していきます。また、国レベルのセキュリティ対策を支援すべく、サイバー戦・国際情勢・法制度の動向などの調査・研究を行います。

注意喚起情報 脆弱性情報の発信

ラックは、コンピューターのOSやソフトウェアにおいて、不正アクセスやコンピューターウイルスなどのサイバー攻撃を受けやすくなるセキュリティ上の欠陥(脆弱性)の発見を全社的に推進しています。サイバー・グリッド・ジャパンでは、その取りまとめを行うほか、JSOCやサイバー救急センターと攻撃情報を連携し、広く一般に周知を図るべき攻撃や脆弱性などを把握したときには、注意喚起情報や脆弱性情報を発信して確認・対策を呼び掛けます。

研究開発

急速に進化するICT(情報通信技術)や関連業界の動向を踏まえ、攻撃検知／防御技術、インシデント対応技術、IoT セキュリティ技術、脅威情報など、変革を続ける社会に求められる技術の研究開発を行います。

啓発活動

各種団体での活動や講演を通して、専門家や技術者以外の方々に対しても、セキュリティをはじめとしたICTの適切な利用を促します。また、若年層や地域住民へも積極的な啓発活動を行い、日本全体での安心・安全なICT利用を推進します。

若手技術者支援

次世代を担うICT人材の育成と裾野拡大のために、ITスーパーエンジニア・サポートプログラム「すごうで」を主催し、卓越した技術力を持つ若者の才能の芽を発掘・支援します。また、若年層の高度IT人材育成を目的として2004年からスタートし、現在はIPA(独立行政法人情報処理推進機構)とセキュリティ・キャンプ実施協議会が共同で開催する合宿形式のイベント「セキュリティ・キャンプ」の支援など、次世代を担う若手IT人材の発掘、育成に積極的に取り組みます。

2017年度は、2016年度に引き続き「サイバー・グリッド研究所」「ナショナルセキュリティ研究所」「次世代技術開発センター」「ICT利用環境啓発支援室」の4部門体制で活動を推進していきます。また、研究開発体制を強化するため、ラックの100%子会社であり高度なハッキング技術を有するネットエージェント株式会社との共同研究を開始しました。

サイバー・グリッド・ジャパンの活動はラック単独の取り組みにとどまらず、他企業・機関と連携して推進いたします。各種業界団体・コミュニティにおける活動や、研究開発におけるオープンイノベーションを通して、技術と情報のシナジーを生み出し、日本のセキュリティレベルを向上させます。

サイバー・グリッド・ジャパンは、ラックの長年の経験・技術力を結集し、産官学連携を通して、ICT環境を強く、安全に進化させ、日本の発展に寄与すべく邁進いたします。

CYBER GRID JOURNAL VOL.4

サイバー・グリッド・ジャパンは株式会社ラックの研究開発部門です。
サイバー攻撃や各国のセキュリティ事情、セキュリティ防御技術などに関する最先端の研究のほか、
複数のセキュリティ企業との連携や新たな製品・サービスの開発、各種啓発活動などにより
日本のセキュリティレベルと情報モラルの向上に貢献しています。

株式会社ラック
〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
TEL：03-6757-0113(営業)　E-MAIL：sales@lac.co.jp　https://www.lac.co.jp/

株式会社ラック
サイバー・グリッド・ジャパン