日本システム監査人協会　第250回月例研究会

「既存対策を凌駕し続けるサイバー脅威と整備すべき態勢（前もっての身構え）」

株式会社サイバーディフェンス研究所
専務理事／上級分析官　名和 利男 氏

2020年9月3日(木)

機械振興会館 ホール

TLP:GREEN
【配布用】

既存対策を凌駕し続けるサイバー脅威と整備すべき態勢(前もっての身構え)

2020年 8月

名和 利男

アジェンダ

1. 2020年1月
   防衛・宇宙関連企業のサイバー事案から「**得るべき教訓**」
2. 2020年1月-4月
   国家支援型サイバー攻撃に利用されている「**ゼロデイ脆弱性**」
3. 2020年7月
   直近の日本組織(企業・団体)における「**セキュリティインシデントの傾向**」
4. 高めるべき「レジリエンス態勢」

TLP:GREEN

既存のセキュリティ対策を台無しにするサイバー攻撃の増加１

2020年1月　防衛・宇宙関連企業のサイバー事案から「得るべき教訓」

2020年1月20日 三菱電機が不正アクセスについて公表

MITSUBISHI ELECTRIC
Changes for the Better

NEWS RELEASE

（経営 No.2005）

2020 年 2 月 12 日
三菱電機株式会社

不正アクセスによる個人情報と企業機密の流出可能性について（第 3 報）

三菱電機株式会社は、1 月 20 日に公表した不正アクセス事案（「不正アクセスによる個人情報と企業機密の流出可能性について」）について、攻撃を受けた可能性のあるすべての端末を精査する中で、流出可能性のあるファイルとして、防衛省の指定した「注意情報」があることを 2 月 7 日に発見し、同日、防衛省に報告の上、2 月 10 日に第 2 報として公表いたしました。当社の調査が完全でなく、国の防衛に関わる情報が流出した可能性があるという事態を引き起こし、深く反省しております。防衛省をはじめ、皆さまにご迷惑とご心配をおかけしていることを、深くお詫び申し上げます。

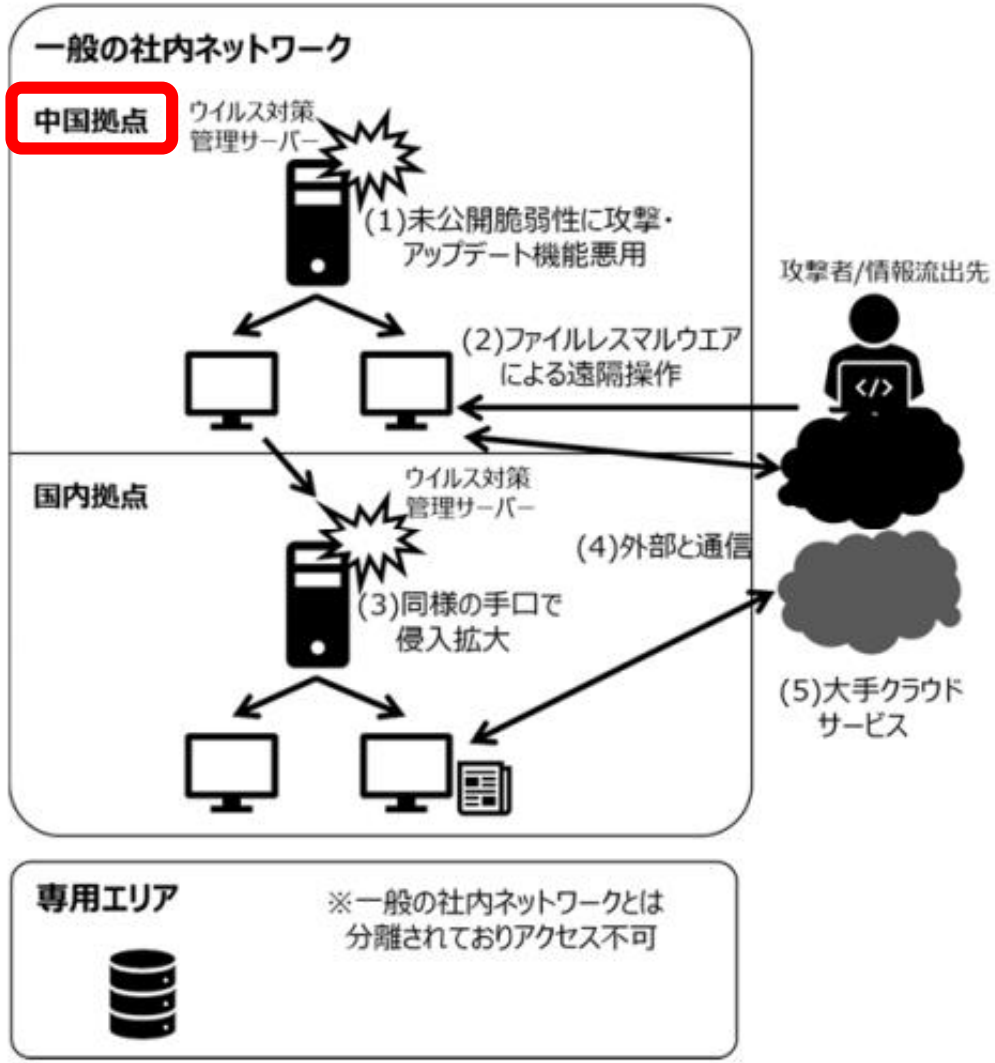
以下に 2 月 10 日に公表した第 2 報についてあらためてご報告するとともに、サイバーセキュリティーに資する情報の共有を図るべく、攻撃手法や当社での検証プロセスなどを、合わせてお知らせします。

電力・鉄道などの社会インフラに関する機微な情報、機密性の高い技術情報や取引先との契約で定められた重要な情報は、攻撃を受けた可能性のあるすべての端末からアクセス可能な範囲に含まれておらず、流出していないことを再確認しました。
現在、1 月 20 日に公表した個人情報が流出した可能性のある方々へのご報告を終え、流出した可能性のある企業機密に関係するお客様への一次報告も終えております。

該当の方々や関係するお客様に多大なるご迷惑とご心配をおかけしていることを、あらためてお詫び申し上げます。また、当社が端末の不審な挙動を認識してから公表に至るまで、半年以上を要したことを反省いたします。

当社グループ全体の情報セキュリティー体制強化に向け、迅速な判断とインシデント発生時のお客様や関係機関との早期情報共有等を目的に、情報セキュリティー全般の企画・構築・運営の機能を一元的に担う社長直轄の統括組織を 2020 年 4 月 1 日付にて新設する予定です。

当社は、今回の事案を教訓として、社会全体のセキュリティーレベル向上に貢献してまいります。



https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf

TLP:GREEN

2020年1月30日 **NEC**が不正アクセスについて公表

NEC \Orchestrating a brighter world

Japan

ホーム > News Room > 当社の社内サーバへの不正アクセスについて

当社の社内サーバへの不正アクセスについて

コンテンツメニュー

2020年1月31日
日本電気株式会社

NECは、当社の防衛事業部門で利用している社内サーバの一部が、第三者による不正アクセスを受けたことを確認しました。当社および外部専門機関による調査の結果、これまで情報流出等の被害は確認されておりません。
関係者の皆様には、多大なご迷惑とご心配をお掛けすることとなり、深くお詫び申し上げます。今回の事態を踏まえて情報管理体制の強化と再発防止に取り組んでまいります。

不正アクセスの概要

NECグループでは、未知のマルウェア検知システムの導入等の対策を実施していますが、2016年12月以降に行われた攻撃の初期侵入および早期の内部感染拡大を検知することができませんでした。
2017年6月、セキュリティ企業の脅威レポートに記載された通信パターンの発生有無を確認した結果、社内のPCから不正通信が行われていることを確認し、感染PCの隔離・調査、不正通信先の検知・遮断を実施しました。2018年7月、感染PCと不正通信をしていた外部サーバとの暗号化通信の解読に成功し、当社の防衛事業部門で利用している他部門との情報共有用の社内サーバに保存された27,445件のファイルに対して不正アクセスが行われていた事実が判明しました。
当社および外部専門機関による調査の結果、これまで情報流出等の被害は確認されておりません。また、これらのファイルには秘密等や個人情報は含まれておりません。なお、不正アクセスを受けたファイルに関連するお客様に対しては、2018年7月以降、個別に状況をご説明しています。

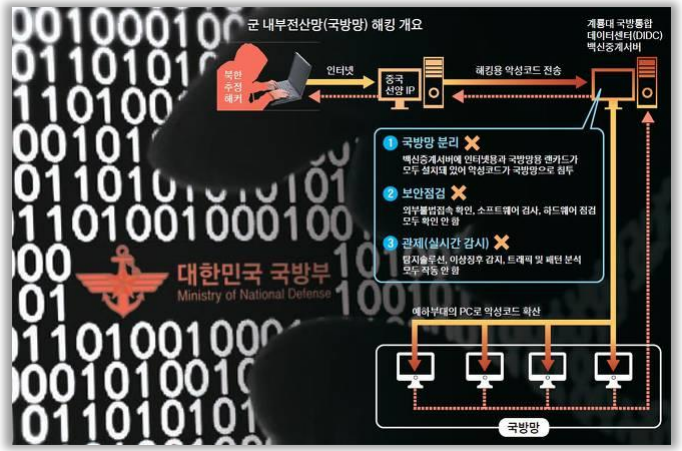
https://jpn.nec.com/press/202001/20200131_01.html

出典元：東京新聞 - NECにサイバー攻撃　中国系集団関与疑い　海自情報流出か
https://www.tokyo-np.co.jp/article/economics/list/202001/CK2020013102000145.html

TLP:GREEN

【参考】2016年10月 韓国軍ネットワークへのサイバー攻撃で情報流出

- 対象：**国防統合データセンター（DIDC）**
  - 各軍のウェブサイトやイントラネットなど軍のすべてのITサービスを統合管理
- 経緯：
  - 8月4日 最初のハッキングの試み、10月6日 データ破壊により検知
- 規模：
  - 3,200台のPC(インターネット接続用PC：2,500台、内部網用PC：700台)
  - 韓民求（ハン・ミング）国防部長官のインターネット用PCも悪性コードに感染したが、「秘密文書は全くなかった」と説明
- 原因：
  - 鶏龍台（ケリョンデ）DIDC内の一部のファイル共有サーバーにLANカード2つ接続されており、外部ネットワークと内部ネットワークが接続されて状態だった。
- マルウェアの特徴：
  - 北朝鮮がこれまでハッキングに使用したものと類似し、C2は北朝鮮が主に利用する中国瀋陽地域
  - 外部ネットワークに置かれている**国軍サイバー司令部のワクチン中継サーバーに感染**し、同サーバーとつながっている複数の端末に汚染させ、秘密資料が流出させたと疑われている。
- 国防関係者による情報：
  - 「悪性コードがDIDCサーバーを通じて軍内部ネットワークに侵入したのは事実だが、DIDC自体が盗まれたことはない。」
- 当初の調査：
  - 韓国軍は2014年に当該サーバーの納入業者に「対共」容疑として重点調査



出典元：[김민석의 Mr. 밀리터리] 국방장관 PC도 해커에 속수무책…'3중 보안' 작동 안 했다 다
https://news.joins.com/article/20994657

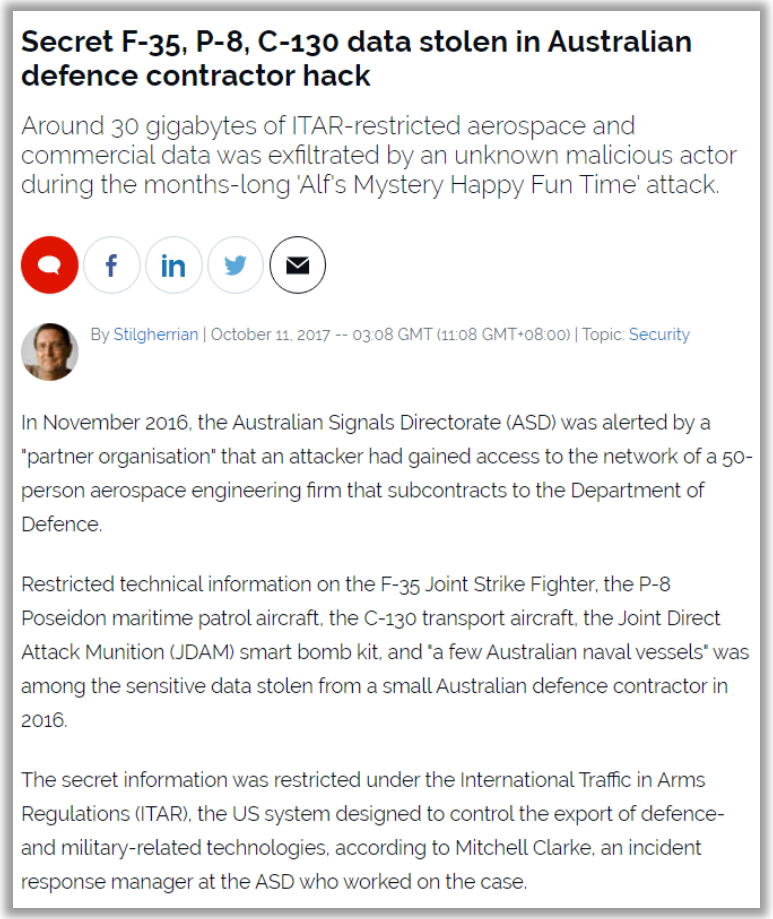
2017年10月、朝鮮日報で次の事実が判明。

- 昨年(2016年)10月に韓国国防統合データセンター（DIDC）が北朝鮮からサイバー攻撃を受けた際、**A4用紙1500万枚相当分の機密情報を盗まれた**。
- 奪われた情報の中には金正恩（キム・ジョンウン）朝鮮労働党委員長を殺害する「斬首作戦」とも言われる「作戦計画5015」など、2－3級の軍事機密が数多く含まれていた。
- 斬首作戦は有事の際、米国の増援部隊が韓半島（朝鮮半島）に到着する前に特殊部隊やミサイルなどを使い、朝鮮人民軍の司令部を攻撃するものだが、その細かい内容である。
- 米軍から提供された機密資料や写真も今回全て流出したと推定されている。

TLP:GREEN

【参考】2016年11月 豪州防衛企業がセキュリティ侵害で情報漏えい

- 2016年7月、オーストラリア国防省と契約する同国の**Tire4レベルの防衛企業が不正アクセス**に遭い、F-35戦闘機、P-8哨戒機、C-130輸送機、JDAM誘導装置及びオーストラリア海軍の艦艇に関する**技術情報が漏洩**した。
  - これらに「極秘」に該当する情報は含まれていないものの、商業上重要な情報であり、国防や軍事に関する米国技術の輸出を管理する「ITAR(International Traffic in Arms Regulations)」によって「取扱注意」に指定されたものだった。
- 不正アクセスを受けた**航空宇宙企業**について
  - 従業員は50名程度
  - 全てのITシステムを経験年数9か月の担当者が一人で管理
  - 同社のネットワークに緩衝領域（DMZ）を設けておらず、定期的にセキュリティパッチを適用する保守体制も未整備
  - 全てのサーバにおいて共通の管理者ID／パスワードが使われ、多くのホストサーバがインターネットに接続



Secret F-35, P-8, C-130 data stolen in Australian defence contractor hack

Around 30 gigabytes of ITAR-restricted aerospace and commercial data was exfiltrated by an unknown malicious actor during the months-long 'Alf's Mystery Happy Fun Time' attack.

By Stilgherrian | October 11, 2017 -- 03:08 GMT (11:08 GMT+08:00) | Topic: Security

In November 2016, the Australian Signals Directorate (ASD) was alerted by a "partner organisation" that an attacker had gained access to the network of a 50-person aerospace engineering firm that subcontracts to the Department of Defence.

Restricted technical information on the F-35 Joint Strike Fighter, the P-8 Poseidon maritime patrol aircraft, the C-130 transport aircraft, the Joint Direct Attack Munition (JDAM) smart bomb kit, and "a few Australian naval vessels" was among the sensitive data stolen from a small Australian defence contractor in 2016.

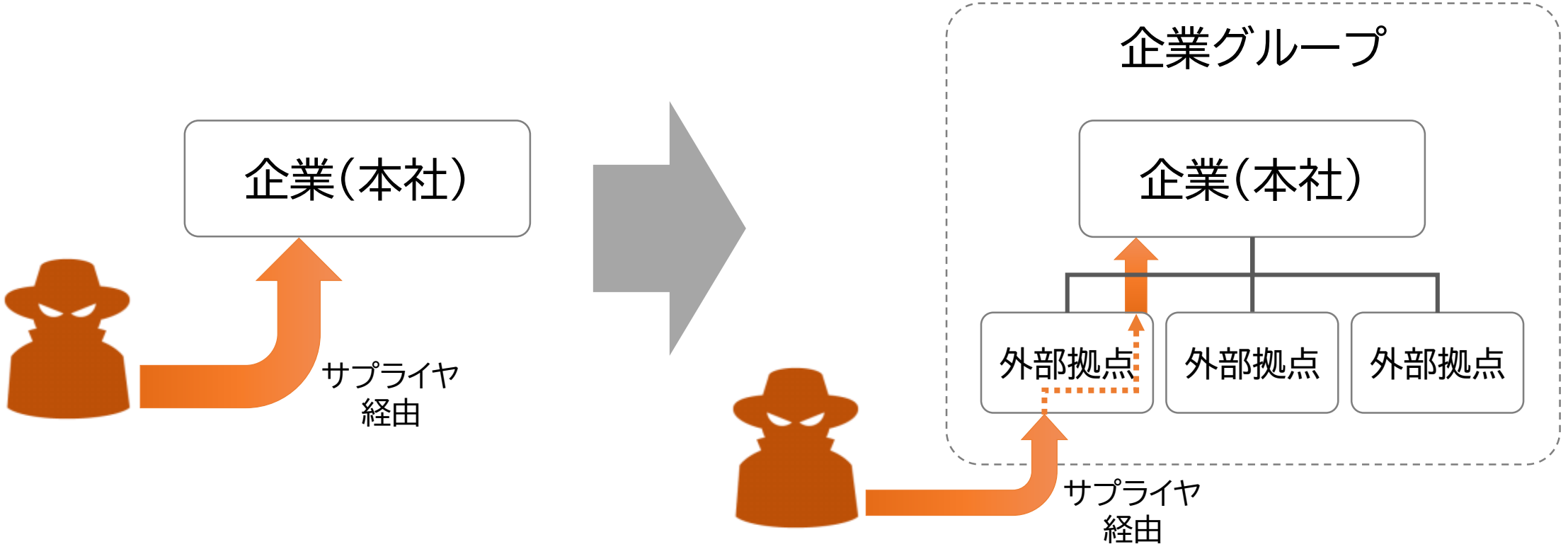
The secret information was restricted under the International Traffic in Arms Regulations (ITAR), the US system designed to control the export of defence- and military-related technologies, according to Mitchell Clarke, an incident response manager at the ASD who worked on the case.

https://www.zdnet.com/article/secret-f-35-p-8-c-130-data-stolen-in-australian-defence-contractor-hack/

TLP:GREEN

【得るべき教訓】脅威主体は、攻撃戦略(Attack Strategy)を進展

- 脅威主体は、企業に対する攻撃戦略(Attack Strategy)を着実に進展させている。
  - 2016年頃：「企業(本社)のサプライヤ」を経由した攻撃
  - 2017年頃：企業グループ内の「脆弱な外部拠点のサプライヤ」を経由した攻撃



  - 2018年頃：企業グループ内の「脆弱な外部拠点」に対する検知困難なゼロデイ攻撃

TLP:GREEN

【得るべき教訓】日本企業は、既存の枠組みで防衛努力を強いられる

- 諸外国の国家サイバーセキュリティ機関及び軍サイバー司令部は、徹底的な状況認識の努力を行い、脅威の認知・分析・共有の能力を構築し、現状に適合した規制・ガイダンス・支援を提供している。一方、日本は既存の（法的）枠組みで防衛努力を継続・・・。

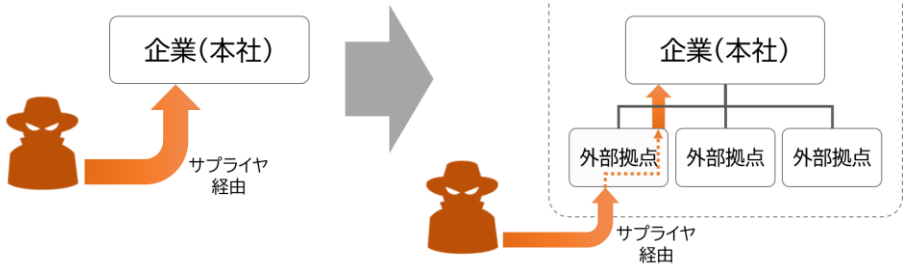
【諸外国のサイバー防衛努力】

国家サイバーセキュリティ庁
／軍サイバー司令部

徹底的な状況認識の努力

サイバー脅威の早期認知・分析・共有

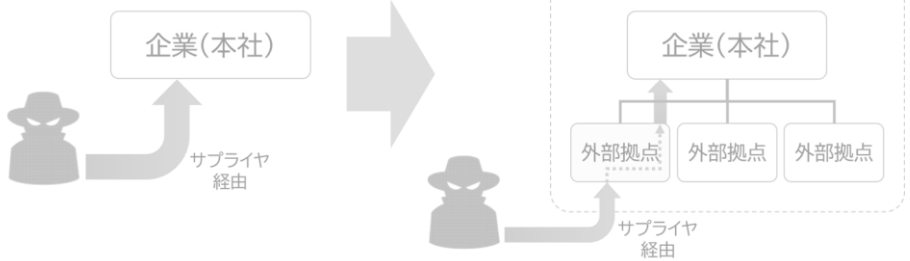
現状に適合した規制・ガイダンス・支援を提供及び継続的な改善努力



【日本のサイバー防衛努力】

国家サイバーセキュリティ庁
／軍サイバー司令部

既存の（法的）枠組みの中で
企業単独で防衛努力を継続・・・



TLP:GREEN

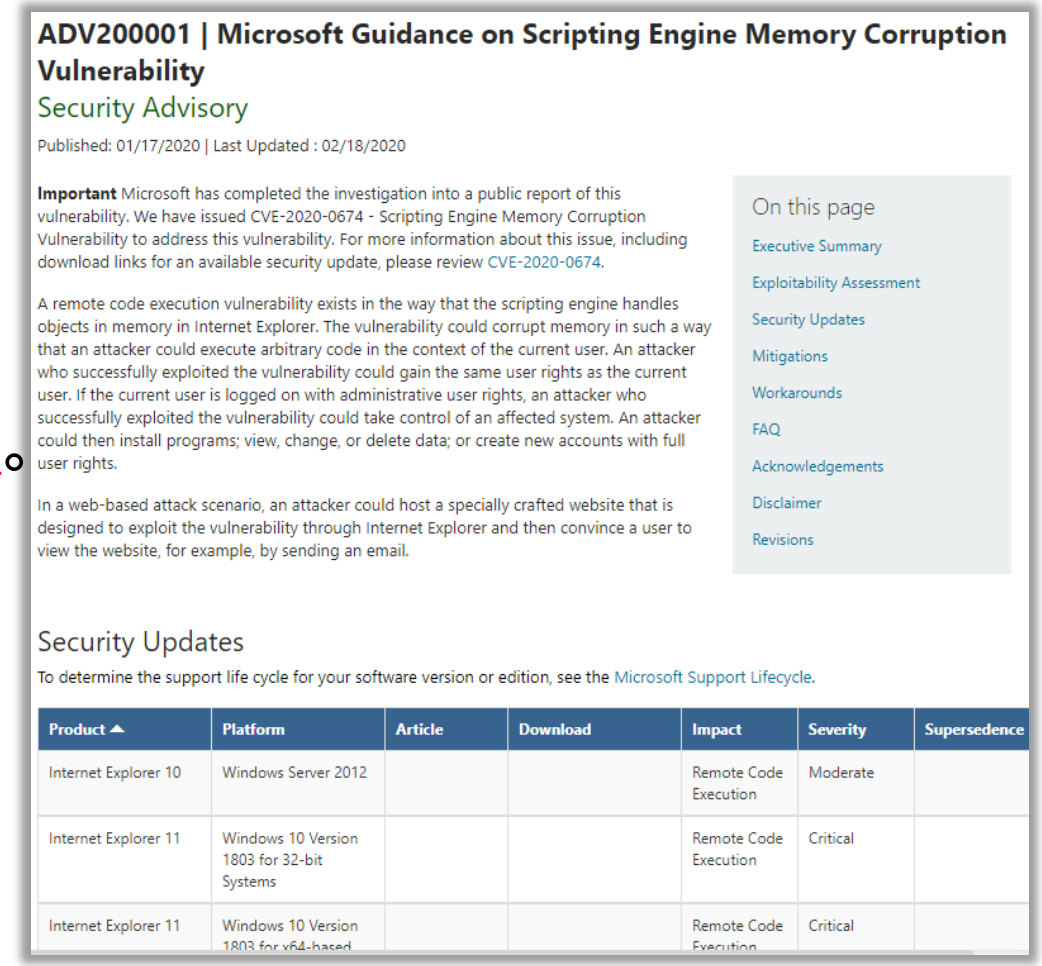
TLP:GREEN

既存の対策・体制では回避不能なサイバー攻撃の現実 2

2020年1月-4月　国家支援型サイバー攻撃に利用されている「ゼロデイ脆弱性」

2020年1月17日 マイクロソフト及び関係機関がIEゼロデイの注意喚起

- 2020年1月17日、マイクロソフトは、IE 9/10/11に**リモートから任意のコードが実行されるゼロデイ脆弱性**が存在することを明らかにした。
  - 脆弱性を悪用した攻撃はすでに確認されており、**米国CISAや日本JPCERT/CCも注意を呼び掛けた**。
  - 細工されたHTMLファイル(ウェブページやメールの添付文書)、PDFファイル、Office文書、IEのスクリプトエンジンで作成された、コンテンツの挿入をサポートする**文書をユーザーが閲覧することで、任意のコードを実行される可能性**がある。



ADV200001 | Microsoft Guidance on Scripting Engine Memory Corruption Vulnerability

Security Advisory

Published: 01/17/2020 | Last Updated : 02/18/2020

Important Microsoft has completed the investigation into a public report of this vulnerability. We have issued CVE-2020-0674 - Scripting Engine Memory Corruption Vulnerability to address this vulnerability. For more information about this issue, including download links for an available security update, please review CVE-2020-0674.

A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website, for example, by sending an email.

On this page
Executive Summary
Exploitability Assessment
Security Updates
Mitigations
Workarounds
FAQ
Acknowledgements
Disclaimer
Revisions

Security Updates

To determine the support life cycle for your software version or edition, see the Microsoft Support Lifecycle.

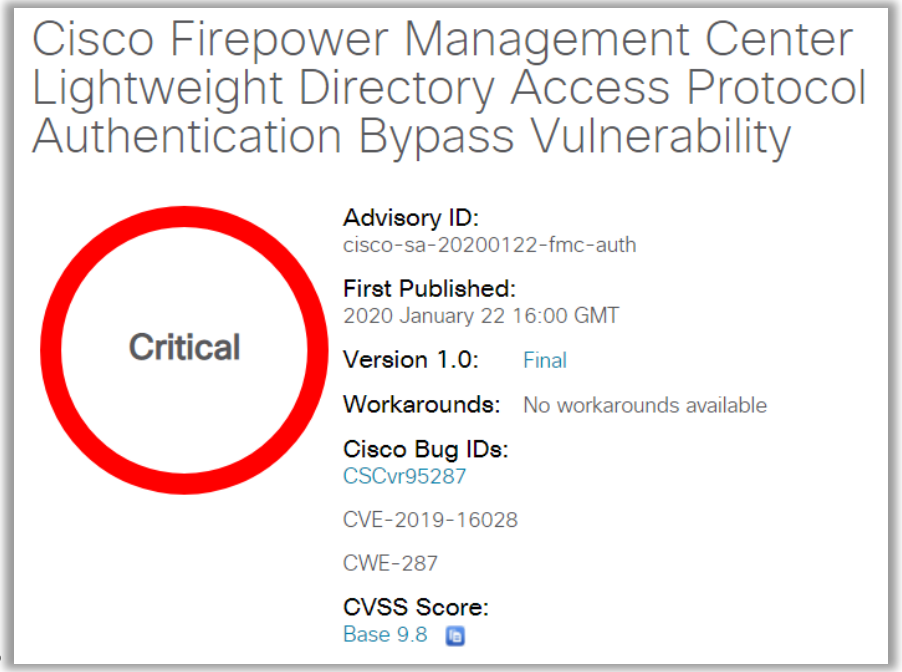
Product	Platform	Article	Download	Impact	Severity	Supersedence
Internet Explorer 10	Windows Server 2012			Remote Code Execution	Moderate	
Internet Explorer 11	Windows 10 Version 1803 for 32-bit Systems			Remote Code Execution	Critical	
Internet Explorer 11	Windows 10 Version 1803 for x64-based			Remote Code Execution	Critical	

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV200001

TLP:GREEN

2020年2月 シスコが複数の脆弱性パッチを公開

- 2020年2月5日、シスコ社は、複数のシスコ製品について、**シスコ検出プロトコルの実装における脆弱性及びソフトウェアの修正情報と対応策**を開示した。
  - しかし、エンタープライズ向けのスイッチやルーターにおいては、**ネットワークが停止しないよう慎重にパッチを適用する必要がある**ため、パッチ適用が困難になる可能性がある。
  - 他に検討可能な対応として、スイッチなどのデバイスでCDPを無効にする方法もあるが、**別の問題（大規模なシスコデバイスの管理能力が低下等）が生じる恐れ**がある。
  - 対処としての**ネットワークのセグメンテーション**は、IoTデバイスのセキュリティを確保するための重要な手段である。



https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200122-fmc-auth

TLP:GREEN

2020年4月 iPhoneの標準メールアプリのゼロデイ脆弱性 (2/5)

- 脆弱性の主な内容
  - 脆弱性は「システムコールの戻り値を正しく処理しない」というバグに起因したもので、「領域外メモリの書き込みでエラーチェックされない」および「ヒープオーバーフロー」の2種類。
  - これら脆弱性を悪用すると、リモートからのコード実行が可能となり、さまざまな攻撃を受ける危険性がある。
  - iOS 13.4.1を含めテストを実施したすべてのiOSに脆弱性が存在。
  - iOSは少なくとも2012年9月のiOS 6以降、この攻撃に対して脆弱な状態だったと考えられる。
  - iOS 13では、**ユーザーが何もしない状態でこの攻撃を受ける可能性**がある。
    iOS 12では、**攻撃を引き起こすには、ユーザーがメールをクリックする必要**がある。
  - 攻撃者は脆弱性が悪用されたあと、それを引き起こしたメールを削除することが可能。

2020年4月 iPhoneの標準メールアプリのゼロデイ脆弱性 (3/5)

- 脆弱性の発見に至るまでの経緯
  - 2019年の夏頃から秋にかけて、顧客のiPhoneで発生した不審なクラッシュ動作を調査の中で、**未知の脆弱性を利用したハッキング被害**を発見。
  - クラッシュを引き起こしたメールはそのiPhoneからは見つけられなかったが、ハッカーが攻撃を実行した後にメールを削除したと推測。
  - ゼロデイ攻撃を再現しそれが機能することを確認した上で、2020年3月にApple社に報告。
- 標的型攻撃が使用された可能性があり、次の人物が狙われた可能性。
  - 北米フォーチューン500にエントリされている個人
  - **日本キャリアの幹部**
  - ドイツの要人
  - サウジアラビアとイスラエルのMSSP(マネージドセキュリティサービスプロバイダ)
  - 欧州のジャーナリスト
  - スイス起業の幹部

TLP:GREEN

2020年4月 iPhoneの**標準メールアプリ**のゼロデイ脆弱性 (4/5)

- 推定される攻撃者像
  - 少なくとも1つの国家支援型サイバー攻撃グループが、第三者のリサーチャーから**概念実証（POC）相当のエクスプロイトを購入**し、「現状のまま」またはわずかに修正して使用したと考えられる。
  - 少なくとも1つの「ハッカー募集(hackers-for-hire)」組織が、メールアドレスを識別子とした**「脆弱性を利用したエクスプロイト」を販売**していたことを確認している。

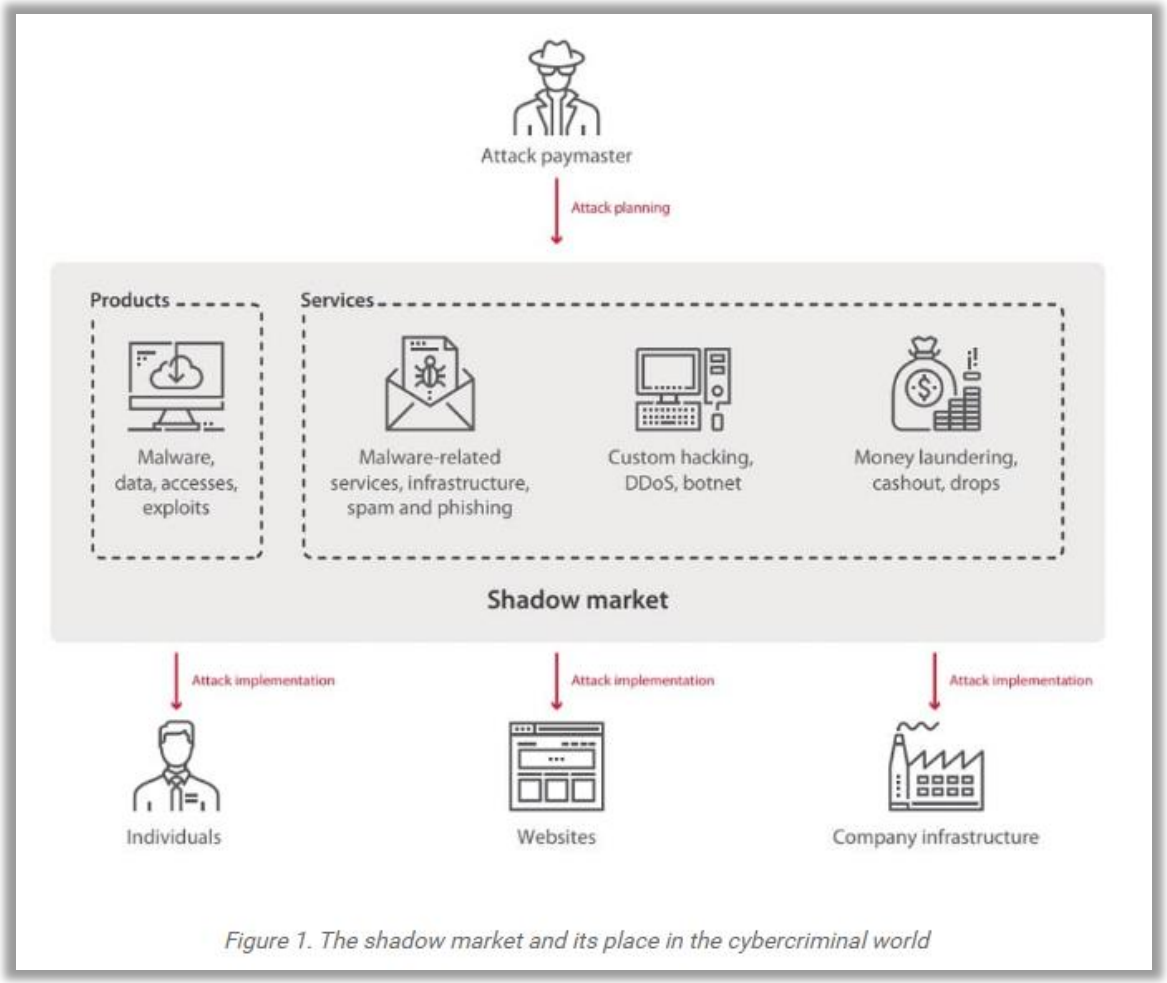


Figure 1. The shadow market and its place in the cybercriminal world

2018年 Positive Technologies社によるサイバー犯罪マーケットの分析
https://www.ptsecurity.com/ww-en/analytics/darkweb-2018/

TLP:GREEN

2020年4月 iPhoneの標準メールアプリのゼロデイ脆弱性 (5/5)

- Apple社の反論
  - 「徹底調査した結果、**ユーザーが差し迫った危険に晒されることはない**と結論。」
  - 「メールにおいて3件の問題が特定されたが、それだけでiPhoneやiPadのセキュリティ対策をかわすことはできず、それが顧客に対して使われたという証拠は見つからなかった。」
- ZecOpsの主張
  - 「この**2件の脆弱性だけではiOSユーザーに危害を加えることはできない**。攻撃者が標的とするデバイスを完全に制御するためには、別の情報流出のバグとカーネルのバグが必要。」
  - 「どちらのバグも、**公開されたベータアップデートで把握可能となった**。攻撃者はすでにこの脆弱性の絶好の機会が終わりを迎えていることを認識しており、パッチが利用可能になるまでの時間を使用して、できるだけ多くのデバイスを攻撃する可能性がある。」
  - 「我々が確認したデータは限られているが、**少なくとも6つの主体がこの脆弱性の影響を受けているため、悪用の可能性は計り知れない**。このようなベータアップデートで脆弱性が公知になった場合、できるだけ早くパッチを提供する必要がある。」

2020年4月 ウィルス対策ソフトに破壊可能な脆弱性 (1/3)

- 2020年4月20日、米国サイバーセキュリティ会社RACK911 Labs が、**ウイルス対策ソフトの挙動とディレクトリ操作を併用した脆弱性**について公表した。
- WindowsのディレクトリジャンクションやmacOS/Linuxのシンボリックリンクといったディレクトリ間やファイル間を結ぶ機能を悪用し、**ウイルス対策ソフトが自身やOSを破壊可能**であった。
  - 同社は、2018年の秋頃からソフトウェアベンダーに通知を開始し、現在はいくつかのソフトを除き修正が施されている。


RACK911 Labs

Home Services Security Advisories Security Research About Us Contact Us

Security Research

Exploiting (Almost) Every Antivirus Software

April 20, 2020 - By RACK911 Labs

Summary

Antivirus software is supposed to protect you from malicious threats, but what if that protection could be silently disabled before a threat can even be neutralized? What if that protection could be manipulated to perform certain file operations that would allow the operating system to be compromised or simply rendered unusable by an attacker?

RACK911 Labs has come up with a unique but simple method of using directory junctions (Windows) and symlinks (macOS & Linux) to turn almost every antivirus software into self-destructive tools.

https://www.rack911labs.com/research/exploiting-almost-every-antivirus-software/

TLP:GREEN

2020年4月 ウィルス対策ソフトに破壊可能な脆弱性 (2/3)

- 脆弱性の本質は、「**Symlink race (シンボリックリンクの競合)**」である。
  - プログラムが安全でない方法でファイルを作成することで生じる、ソフトウェアのセキュリティ脆弱性の一種。
  - 悪意のあるユーザは、他の方法でアクセスできないファイルにシンボリックリンクを作成する。
  - 特権プログラムがシンボリックリンクと同じ名前のファイルを作成すると、「リンク先のファイルが作成される」ため、悪意のあるユーザが望むコンテンツの挿入や、悪意のあるユーザが(プログラムへの入力として)送り付けたコンテンツを挿入したりすることができる。
  - 「リンク先のファイルか作成される」は、プログラムがその名前のファイルがすでに存在するかどうかをチェックし、存在しない場合には、プログラムがそのファイルを作成するためである。これを「race(競合)」と呼んでいる。
  - ウィルス対策ソフトは、スキャン等により「疑わしいファイル」を隔離または削除することを判断して、それを実行する。その**決定と実行の僅かな間で、悪意のあるソフトウェアが、その「疑わしいファイル」を「消えて欲しいシステムファイルやAVファイル」に置き換えることができる**。

TLP:GREEN

出典：Symlink race https://en.wikipedia.org/wiki/Symlink_race

【参考】Window におけるリンク機能

機能名	ジャンクション	シンボリック・リンク	ハードリンク
サポートOS	Windows 2000以降	Windows Vista／Server 2008以降	Windows 2000以降
必要なファイル・システム	NTFS	NTFS	NTFS
利用している機能	NTFSのリパース・ポイント	NTFSのリパース・ポイント	NTFSのファイル・オブジェクトのリファレンス・カウント
リンクの作成に必要な権限	一般ユーザー権限でよい	管理者権限が必要(シンボリック・リンクの作成権SeCreateSymbolicLinkPrivilegeが必要)	一般ユーザー権限でよい
ファイルへのリンクとdirコマンド出力での表記	×	○ <SYMLINK>	○
フォルダへのリンクとdirコマンド出力での表記	○ <JUNCTION>	○ <SYMLINKD>	×
絶対パス指定	○	○	−
相対パス指定	×(リンク先表記は絶対パスに変換されて保存される)	○	−
同一ボリューム内のオブジェクトへのリンク	○	○	○
同一PC内のほかのボリューム内オブジェクトへのリンク	○	○	×
ネットワーク共有フォルダへのリンク	×(リンク先はローカルのみ)	○	×(リンク先はローカルのみ)
リンクを作成するためのコマンド	「mklink /j ～」	「mklink ～」「mklink /d ～」	「mklink /h ～」「fsutil hardlink create ～」
リンクを削除するためのコマンド	「rmdir ～」	リンク先がファイルなら「del ～」、フォルダなら「rmdir ～」	「del ～」
存在しないオブジェクトへのリンク	作成できる	作成できる	作成できない
エクスプローラで見ると……	ショートカットを表す矢印が付く	ショートカットを表す矢印が付く	通常のファイルと同じように見える

TLP:GREEN

出典：Windowsのシンボリックリンクとジャンクションとハードリンクの違い
https://www.atmarkit.co.jp/ait/articles/1306/07/news111.html

2020年4月 ウィルス対策ソフトに破壊可能な脆弱性 (3/3)

- 2020年4月24日、RACK911 Labs は、この脆弱性情報の開示に対する思い（メッセージ）を伝えた。
  - ほとんどのウイルス対策ベンダーは、すでにパッチを適用している。
  - 開示の目的は、ベンダーを名指しして恥をかかせることではなく、**ウイルス対策ソフトを破壊的なツールにすることがいかに簡単であるかを知っていただき**、関心を持ってもらうためである。
  - 我々の目標は、ウイルス対策ベンダーだけでなく、すべてのソフトウェアベンダーが潜在的なディレクトリジャンクションおよびシンボリックリンク攻撃について**コードチェックの重要性を高める**ことである。これらの実行はとても簡単であり、この開示情報で説明したとおり、非常に危険な場合がある。

※今回の RACK911 Labs のリサーチ・分析の対象に日本企業のウィルス対策ソフトは確認されていない。**リストにないから安全であるとは言えない**ことを留意する必要がある。

TLP:GREEN

既存の対策・体制では回避不能なサイバー攻撃の現実 3

2020年7月　直近の日本組織(企業・団体)における「セキュリティインシデントの傾向」

2020年7月における日本の組織(企業・団体)のインシデント傾向 (1/2)

- **「ヒューマンエラー(人的ミス・人為的過誤)」(14件)**が最も多い。
  - メールやFAXの誤送信(9件)が突出しており、デバイス紛失(3件)とWebサイトへの掲載ミス(2件)は以前と変わらず発生している。
  - これは、業務におけるメール利用の安全性確保が、「職員・社員に対する啓発や教育訓練」などの人的な措置に依存していることが影響を与えていると考えることができる。
    - 一部の被害組織は、改善策として「セキュリティ教育の徹底」としていることから、技術的な措置を並行することの必要性や重要性に対する理解が十分に浸透していない可能性がある。
  - コロナ禍において、急ごしらえのIT環境構築により馴れないデジタル業務をする職員・社員が、ヒューマンエラーの発生確率が必然的に高くなると考える必要があるため、その発生を抑止するための仕組みを作る必要がある。
    - 技術的措置を伴う仕組みを作ることなく、職員・社員に対して「セキュリティ教育の徹底」などの短絡的な対策は、現状から乖離したものとなる。

2020年7月における日本の組織(企業・団体)のインシデント傾向 (2/2)

- **「脆弱性を悪用した不正アクセス」(12件)**は依然として多い。
  - 不正アクセスにより窃取される情報が「経済的価値に直結するもの」である場合、早期の検知や周囲からの通知などによる迅速対処が図られている。
  - しかし、個人情報などのような「経済的価値に置換するためにプロセスを要するもの」である場合は、検知や認知するまでにかなりの時間がかかることがある。
- **「メールのサーバやアカウントの不正利用」(5件)**が目立つ。
  - 現在、日本国内で猛威を振るっているEmotet(単体で動作するのではなく、あらゆるマルウェアを感染させる“プラットフォーム”としての役割を持つ)の影響も見られるが、メールアカウントの認証情報が窃取された可能性を示唆する事案が目立ってきている。
  - 認証セキュリティの確保のために2段階認証の利用が強く推奨されているが、古い設計のアプリ(ケーション)の中には2段階認証をサポートしていないものがある。そのため、代替手段として、サーバサイドにおいてアプリパスワード(サインイン時に通常のパスワードの代わりに 1 回だけ入力する、ランダムに生成された長いパスワード)の実装がある。

TLP:GREEN

変革すべき意識・姿勢

高めるべき「レジリエンス態勢」

サイバーレジリエンスについて

- サイバー空間に依存している事業におけるレジリエンス(Resilience)とは
  - 悪意のあるサイバーイベント（セキュリティ侵害等）が発生しても、**意図した結果（Intended outcome）を継続的に提供する企業・組織の能力**のこと
- レジリエンスを高めることで、事業の継続性を脅かすサイバー脅威を受けたとしても、**早期の正常な事業環境を復元し、通常の事業を再開できる**ようにする。

「レジリエンス（Resilience）」は、**対象に圧力がかかった状態**に対する「復元力」や「回復力」「弾力性」などと意訳され、物理学、生態学、心理学などで使用されている。

TLP:GREEN

サイバーレジリエンスの技術と実装のためのアプローチ (1/2)

テクニック	実装のためのアプローチ
適応的対応 （Adaptive Response）	・動的な再構成（ルーターのルール、ACL、IDSのパラメータなど） ・動的なリソース割り当て（動的プロビジョニング、負荷分散、緊急遮断など） ・適応的管理（動的アクセス無効化、システムの自動無効化など）
分析的監視 （Analytic Monitoring）	・監視とダメージ評価（HW障害検出の利用、CDMの利用、IDSの利用など） ・センサーの融合と分析（組織全体の状況認識、組織間の監査、異なるツールからのデータの関連づけ） ・フォレンジックおよび行動分析（アナリスト・開発者・運用者の統合チーム、リバースエンジニアリングやマルウェア分析ツール）
協調的な保護 （Coordinated Protection）	・調整された多層防御（複数の異なるチャレンジを使用したID確認、ネットワークベースとホストベースのIDSの組み合わせなど） ・一貫性の分析（統合IDAM管理ツールの使用、特権分析ツールを利用したレビューなど） ・オーケストレーション（オペレーションおよび組織プロセスのミッションの継続性とともにインシデントハンドリングを調整） ・セルフチャレンジ（電源投入テスト、役割ベースの演習、侵入テストやレッドチーム演習など）
状況認識 （Contextual Awareness）	・動的なリソース認識（リアルタイムの統合された状況認識） ・動的な脅威認識（自然災害の追跡、インシデントおよび脅威データの動的な取り込みなど） ・ミッションの依存関係とステータス（広範な（ミッション/ビジネス機能全体、組織全体）視点の構築）
欺瞞 （Deception） **敵対的な脅威に対処する場合に使用*	・難読化（暗号化、通信パターンを隠蔽またはランダム化、オニオンルーティングなど） ・偽情報（誤った情報に基づく公開フォーラムへの質問の投稿、偽の資格情報とトークン） ・誤った方向づけ（ハニーポット、ハニーネット、おとりファイルなど） ・汚染（ビーコントラップ、内部ネットワークテーブルへのキャッシュポイズニング（DNS、ARPなど））
多様性 （Diversity）	・アーキテクチャの多様性（異なるOSでのログの取得・保存、複数のプロトコルのサポートなど） ・設計の多様性（多くのバージョンのプログラミング、アナログ通信とデジタル通信の使用、など） ・総合的な多様性（アドレス空間レイアウトのランダム化、ランダム化コンパイラの使用） ・パスの多様性（代替の電気通信サービス（例：地上回線、衛星通信）の確立、代替通信プロトコルなど） ・サプライチェーンの多様性（多様なサプライヤのセット）
動的ポジショニング （Dynamic Positioning）	・センサーの機能的再配置（IDSまたはIDSセンサーの再配置（仮想化）または再構成） ・サイバーリソースの機能移転（処理場所の変更（例：異なる物理コンポーネント上の仮想マシン）、ストレージサイトの変更） ・アセットモビリティ（監視しながら機器を施設内の別の部屋に移動など） ・フラグメンテーション（分散データベースの断片化およびパーティション分割） ・機能の分散（構成機能を異なるシステムコンポーネントに配置できるようにアプリケーションを設計）

TLP:GREEN

出典：NIST SP 800-160 Volume 2 [Final Draft, November 27, 2019]
Developing Cyber Resilient Systems: A Systems Security Engineering Approach

サイバーレジリエンスの技術と実装のためのアプローチ (2/2)

テクニック	アプローチ
非永続性の生成と保持 (Non-Persistence Generate and retain)	・非永続情報(価値のある情報の処理後削除、監査レコードのオフラインストレージへのオフロードなど) ・非永続サービス(時間ベースまたは非アクティビティベースのセッション終了、コンポーネントのイメージ再作成など) ・非永続的な接続(SDN(ソフトウェア定義ネットワーク)の実装、時間ベースまたは非アクティビティベースのネットワーク切断)
特権の制限 (Privilege Restriction)	・信頼ベースの権限管理(最小限の特権、時間ベースのアカウント制限) ・属性ベースの使用制限(ロールベースのアクセス制御(RBAC)、属性ベースのアクセス制御(ABAC)など) ・動的な特権(ミッションまたはビジネスタスクのステータスに応じた権限に対する時間ベースの調整、動的なアカウントプロビジョニングなど)
再調整 (Realignment)	・目的化(ホワイトリストによる未承認アプリケーションのインストール防止、ホワイトリストによる指定されたアドレスセットへの通信の制限) ・オフロード(必須ではないサービスのマネージドサービスプロバイダーへのアウトソース) ・制限(必須の機能のみを提供するようシステムを構成など) ・置換え(サポートされていないシステムコンポーネントを削除または置換え) ・専門化(重要コンポーネントを再実装またはカスタム開発、カスタマイズされた構成の定義および適用)
冗長性 (Redundancy)	・保護されたバックアップとリストア(以前のベースライン構成の保持、システムレベルのバックアップ情報の維持と保護) ・余剰能力(予備部品の維持、外部システムとのサービスレベル契約) ・複製(代替の監査機能の提供、シャドーデータベース、1つ以上の代替ストレージサイトの維持など)
セグメンテーション (Segmentation)	・定義済みのセグメンテーション(仮想化を使用した個別の処理ドメインの維持、システム機能からのアプリケーション分割など) ・動的なセグメンテーションと隔離(コンポーネントの動的な分離、SDNとVPNの実装など)
実証済みの整合性 (Substantiated Integrity)	・整合性チェック(改ざん防止用シールと改ざん防止コーティング、データ品質チェック用の自動化ツールなど) ・出所追跡(SCRM(サプライチェーンリスクマネジメント)の一部としてのコンポーネントのトレーサビリティ、偽造防止対策など) ・動作検証(機能検証の実装、ブートプロセスの整合性の確認など)
予測不能性 (Unpredictability) **敵対的な脅威に対処する場合に使用*	・一時的な予測不能性(ランダムな間隔で再認証の要求、1日の異なる時間のルーチンアクションの実行) ・状況の予測不能性(役割と責任の交代、ランダムチャネルホッピングの実装)

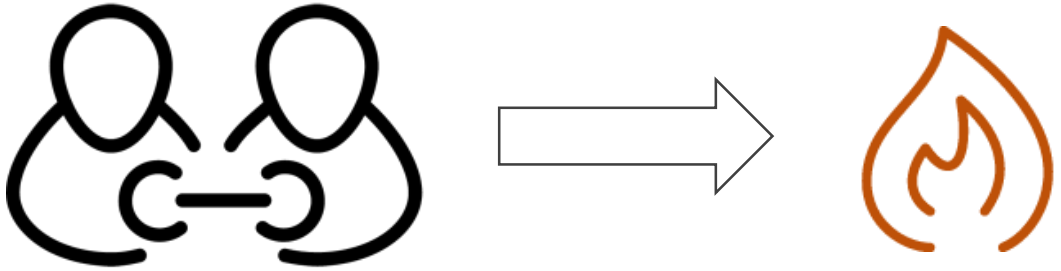
TLP:GREEN

出典: NIST SP 800-160 Volume 2 [Final Draft, November 27, 2019]
Developing Cyber Resilient Systems: A Systems Security Engineering Approach

【参考】「態勢」と「体制」は、取るべき準備行動 が大きく異なる。

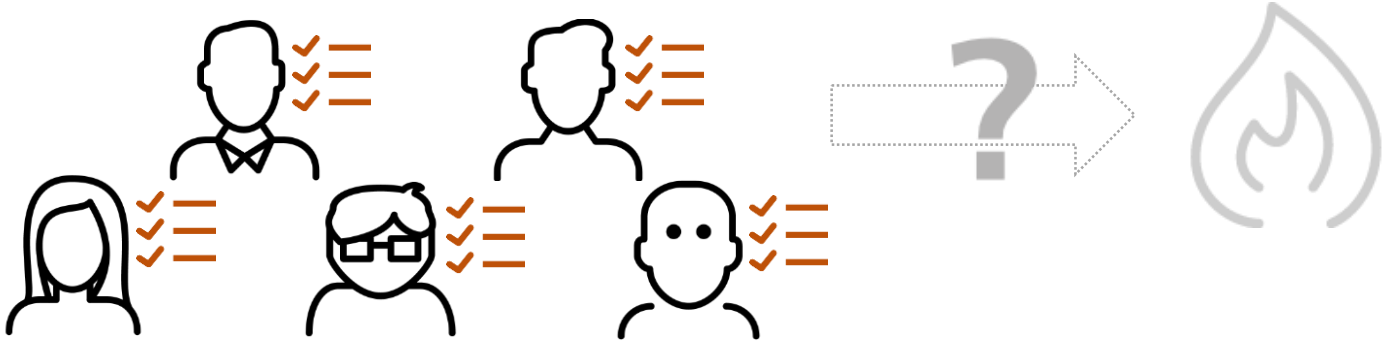
- 態勢: 事態に対処するための準備ができている状態のこと。(前もっての身構え)

実際に事態対処できるかどうかが重要



- 体制: 基本原理・方針によって秩序づけられている組織のこと。(政治支配の様式)

組織内の役割分担(責任所在)が重要



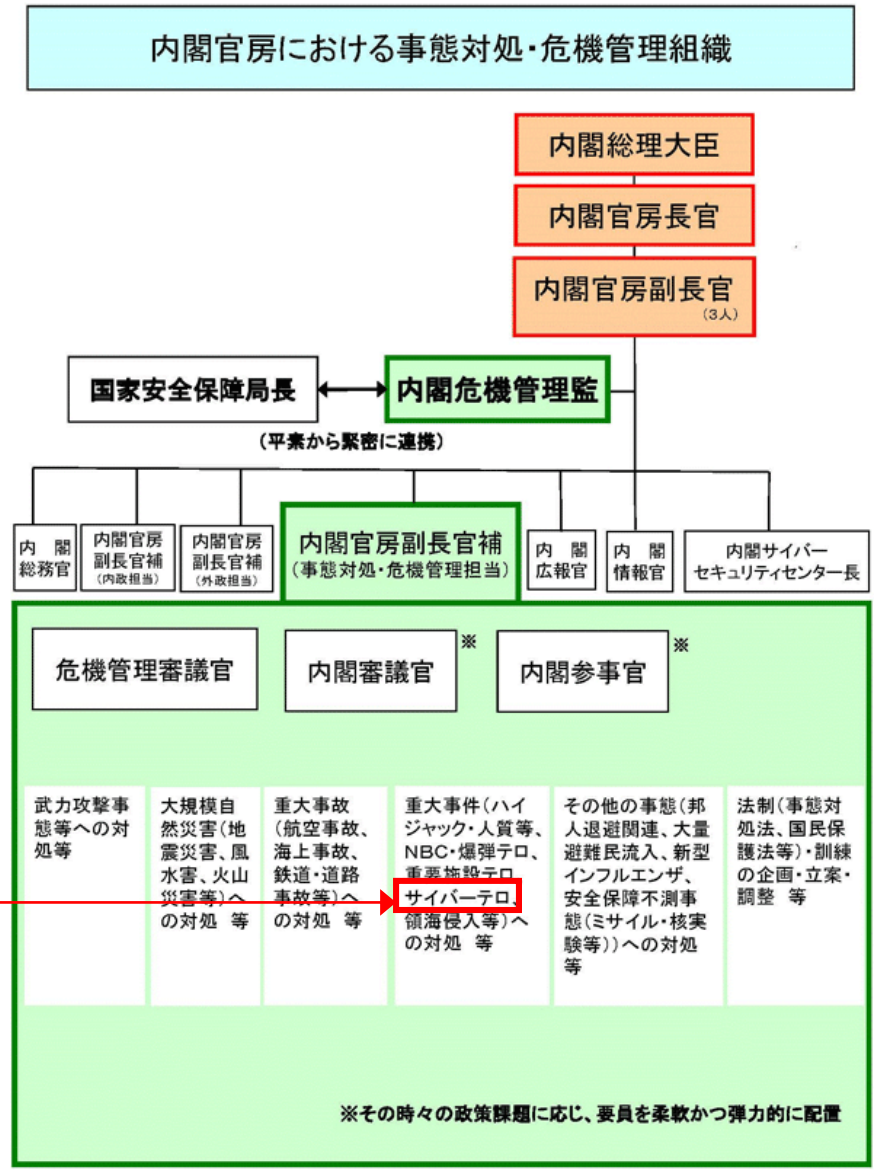
TLP:GREEN

事業を停滞させる「サイバーテロ(大規模サイバー攻撃)」

- サイバーテロ(大規模サイバー攻撃)は、我が国における緊急事態の一つ。

【判断の観点による緊急事態の特性】

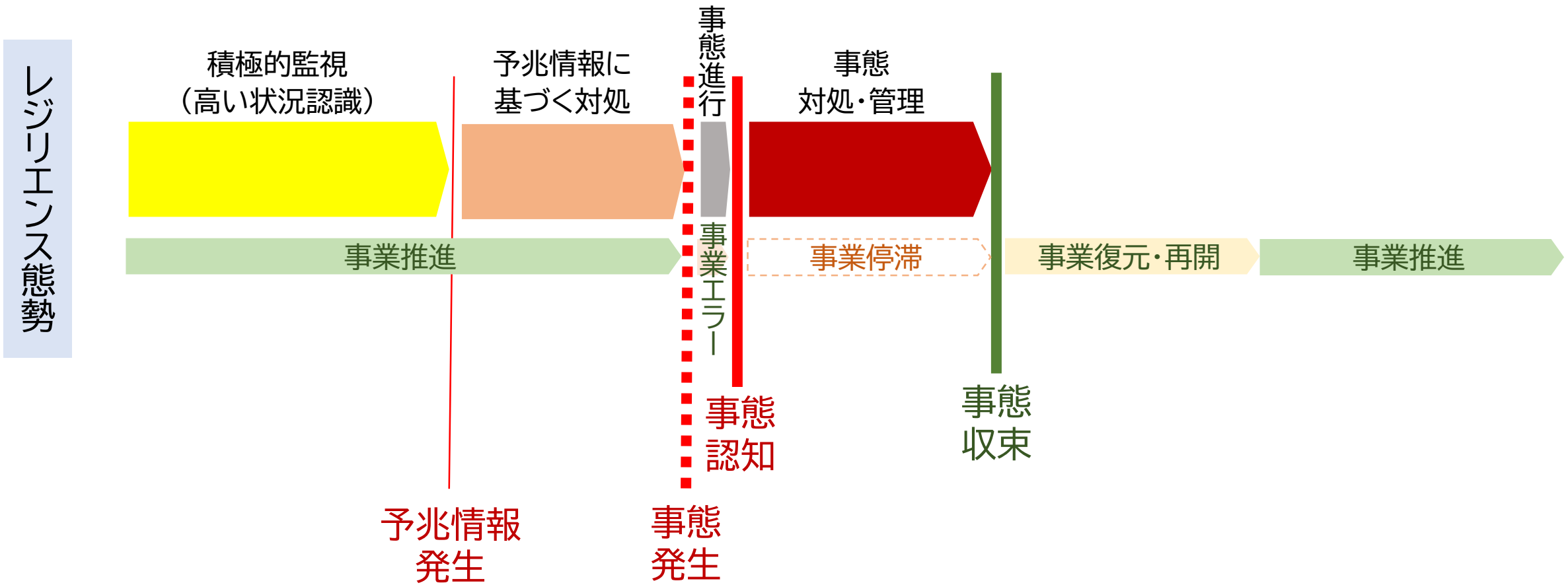
- 「自然災害のような明らかに多くの生命が脅かされる事態」は、**あらゆる主体者が迅速に判断**する。
- 「サイバーテロのような緊急性の有無を判断するために必要な事態」は、**観察者(あるいは当事者)による主観的な評価を必要**とする。



出典:内閣官房副長官補｜内閣官房ホームページ
https://www.cas.go.jp/jp/gaiyou/jimu/fukutyoukanho.html

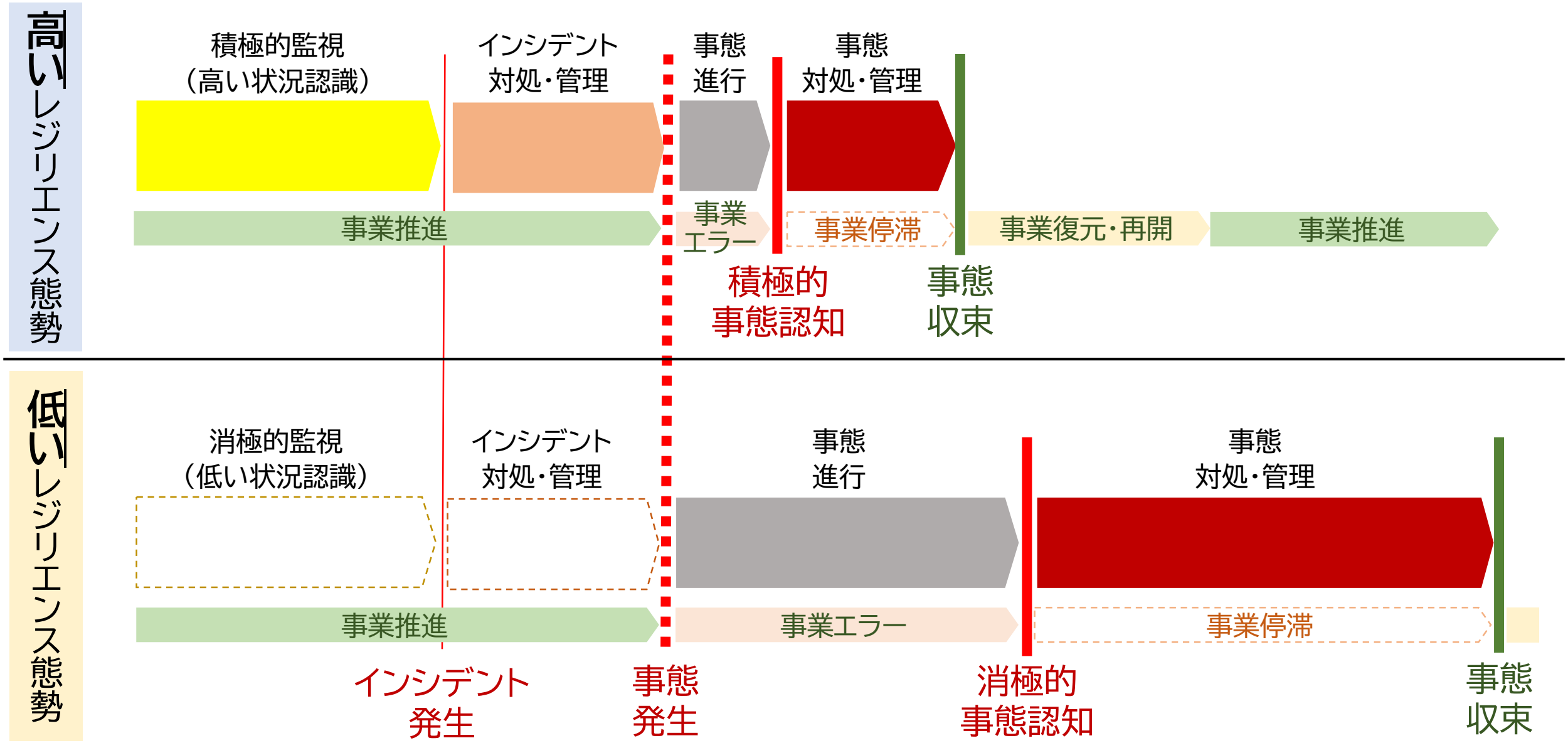
TLP:GREEN

自然災害のような「明らかに多くの生命が脅かされる緊急事態」



TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

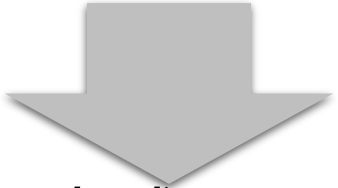


TLP:GREEN

【参考】「リスク管理」の限界

*リスク管理とは、**潜在的な脅威**を評価し、それらの脅威を**回避する最良の方法**を見つけるための手続き的管理のこと。*

- サイバー攻撃の態様が急激に変化している。
  - サイバー攻撃が、極めて**複雑化(sophisticated)**・**大規模化(large-scaled)**
  - **攻撃対象領域(Attack Surface)**が、拡大・深化
  - **攻撃戦略(Attack Strategies)**が、多様化・重層化・個別化・高度化・弾力化



- 旧来の体制と能力では、「潜在的な脅威」の**見出し・識別・特定・評価は困難**になってきた。
- 「回避する最良の方法」の適用可能な範囲は、**急速に縮小**する。（すぐに最良の方法でなくなる）

TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

- サイバー脅威の**動向変化に適合(Adapt)**したセキュリティ監視を実施・強化（対象増強、選択と集中）していない。
- 初期段階のセキュリティ事象の**検知あるいは識別ができない**。
- 潜在化した**攻撃挙動を見逃す**。

TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

- 「サイバー攻撃の挙動痕跡を積極的に残す設計思想」が適切に組み込まれていない。
- 発生したセキュリティ事象を検知あるいは識別ができない。
- （インシデント対処の対象にならない）セキュリティ事象が潜在的に活動する。
- 事前に規定・プロセス化したインシデント管理が機能しない。

TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

- 発生判断のために、当事者や観察者による**評価(事象の識別、今後の被害推定等)に一定時間を要する**。
- 監視やインシデント管理の不足が多いほど、発生判断に長期間かかり、**推定に頼る領域が発生**する。

TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

- 事実解明のために、当事者や観察者(専門家)による**対処（調査、識別・特定、分析、報告・説明）に一定時間を要する**。
- 監視やインシデント管理の不足が多いほど、事実解明に長期間かかり、**未対処の領域（被害）が拡大**する。

低いレジリエンス態勢

TLP:GREEN

本資料に関する連絡先

名和 利男（NAWA Toshio）

SITE: https://www.nawa.to

PGP: 0xE38B4E01