サイバー脅威に対する状況認識のために整備すべき態勢と獲得すべき能力

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
NAWA Toshio

Ⅰ　はじめに

世界中でサイバー攻撃の発生に関する報告が急増しており，その被害規模は拡大の一途を辿っている。この背景にはさまざまな要因や事情があると考えられているが，筆者が行っている「攻撃側の主体の特性及びその行動に対する観察（モニター）」及び「サイバー空間の基盤推移と利用変化に注目した遡及的分析」から得られた知見で眺めると，サイバー攻撃の広範化や深刻化が著しくなってきた必然性や因果性を垣間見ることができる。そのような状況認識の努力を重ねていくと，整備すべき態勢のあるべき姿が見えてくる。

Ⅱ　サイバー空間の基盤推移による攻撃メカニズムの劇的変化（図 1）

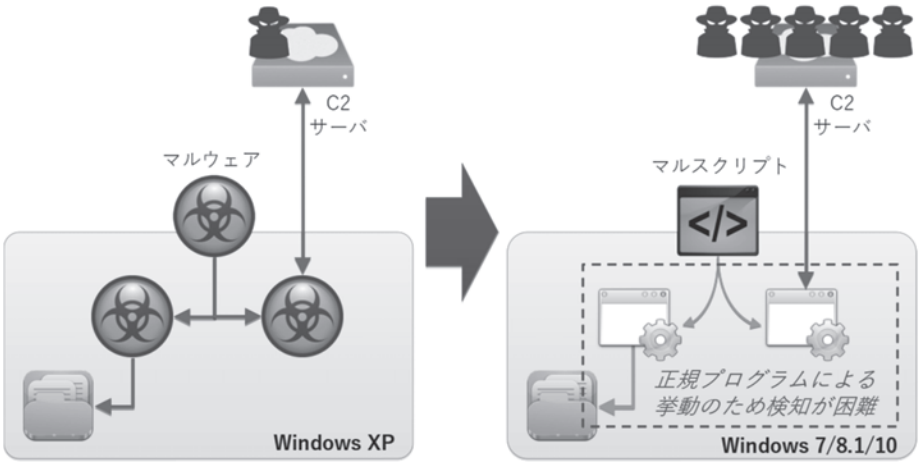
まず，防御側である我々が認識しなければならないのは，Windows XP から Windows Vista/7/8.1/10 への変遷で発生した「攻撃者像と攻撃成功率の上昇」である。長年に渡り PC の基本ソフトとして利用されてきた Windows XP は，一般のオフィスに限らず，鉄道，金融，工場等における機械設備としても利用され，2014 年 4 月にサポートが終了したが，現在（2018 年）でも，いまだにライフサイクルの長い機械設備の一部で利用されている。

攻撃者は，この Windows XP に対して，さまざまな手段（Web サイト，電子メール，USB メモリ等の外部デバイス）でマルウェア（悪意のあるソフトウェア）を感染させようと企てた。一方，ウィルス対策ソフトベンダーはそれを阻止しようと検知率の向上に努めた。つまり，サイバー攻撃とセキュリティ対策の「いたちごっこ」が長らく続いた格好となった。この過程の中で，攻撃者は，ウィルス対策ソフトによる検知を回避するために，マルウェア感染に係る挙動の隠ぺい技術や，外部からの指令伝達や内部データ流出を秘密裏に行う技術を高めていった。さらに，攻撃者は，標的とする PC の内部やセキュリティ対策に関する状況把握，それに基づくマルウェアの設計及び開発に係る能力も格段に向上していった。

ところが，Window XP のアップグレード版である Windows Vista/7 以降，Windows PowerShell と言われる高機能なスクリプト言語が組み込まれたコマンドラインシェル（以下，PowerShell）が実装された。これは，クラウド化により大規模化するサーバの保守管理に対する効率化や集中化，そして組織内における膨大な Windows PC の管理強化等のニーズの高まりを背景として出現したものである。攻撃者は，本来は保守管理やその用途のためのツール開発等のために Windows に実装されたスクリプト言語の悪用を始めている。

ここ数年，特に目立ち始めている攻撃メカニズムは，文書ファイルに悪意のある PowerShell スクリプト（以下，マルスクリプト）を入れ込み[1)]，人間の心理的な隙や行動のミスに付け込む形で，件名や本文が本物と見間違えるような内容にしたメ

図 1：攻撃メカニズムの劇的変化



出典：筆者作成

ールを送りつけて，PC ユーザーに添付された文書ファイルを開封させてマルスクリプトを動作させる，或いは本文中のリンクから特定の Web サイトを閲覧させることでマルスクリプトをダウンロードさせて動作させる等の手段で，標的の PC 内情報を操作及び窃取する。

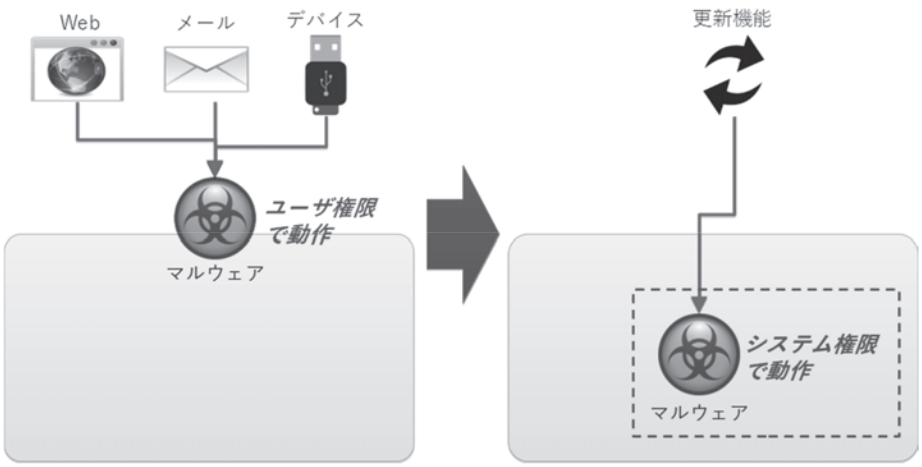
このような悪意のあるメールを送りつける手法は，以前から存在していたが，PC ユーザーに開封させる文書ファイルや Web サイトは，それらの設計上，スクリプトを埋め込みやすいため，瞬時に正規であるのか或いは悪意あるスクリプトを含んでいるのかを見極めることは非常に難しい。以前のように悪意のある挙動（攻撃活動）に特化した形で独立した機能で成り立つマルウェアは，機械的に識別しやすかったが，マルスクリプトは旧来の検知技術では識別することが難しく，動作して他のプログラムが実行してからでないと検知することが難しい。さらに，このような類のマルスクリプトは，インターネット上で広く共有され，特定の活動をさせるためのサンプルスクリプトやそれらを解説した記事が豊富に存在するようになったため，時間の経過とともに容易に入手できるようになり，ソフトウェア開発技術が十分でなくても意図通りに改変できるようになっていった。

そして，自らが攻撃挙動の実行主体となるマルウェアと異なり，マルスクリプトにおいては，Windows 内部に予め実装されている正規プログラムを実行させるため，以前のマルウェアの挙動に着目したウィルス対策ソフトでは検知することが困難になった。Windows 内部の正規プログラムは検知対象外となっているためである。

このような大きな IT の歴史的変遷の中で，観察できた限りの攻撃側の行動変化として注目すべき点は，主要な攻撃者像が「（高度で特殊なマルウェアを作成することにより）高いレベルのソフトウェア開発能力を有した者達」から，ここ数年「（汎用的なマルスクリプトを再利用するだけの）低いレベルのソフトウェア開発能力しか有していない者達」に変化したことである。一般的にソフトウェア開発者の能力分布を見ると，前者は少数で，後者は多数と捉えるのが自然である。そして，以前までの主要な攻撃者像の認識として，スクリプトキディと言われる「他人が作成したプログラムやスクリプトを悪用し，興味本位で第三者に被害を与える攻撃者」による攻撃の成功率は低いとみなされていたが，後者の主要な攻撃者像は，PowerShell 等のスクリプト実行環境の恩恵を受ける形で攻撃の成功率を飛躍的に向上させ，その規模を

1） What is a fileless attack? How hackers invade systems without installing software (https://www.csoonline.com/article/3227046/malware/what-is-a-fileless-attack-how-hackers-invade-systems-without-installing-software.html).

図２：ソフトウェアの更新機能を利用したマルウェア感染



出典：筆者作成

急拡大させている。

Ⅲ　民間組織が検知或いは識別することが困難なサイバー攻撃

国を挙げてIT技術の発展とインターネットの利活用の拡大を進めてきたことにより，労働生産性の向上や効率性の改善がみられ，企業経営に大きな恩恵をもたらす一方で，現場のIT環境の変化によりサイバー攻撃を受けやすい状況になってきたことが十分に認識されていないところがある。

そこで，民間組織が検知或いは識別することが困難なサイバー攻撃の手口・手法として，代表的な２つを説明する。

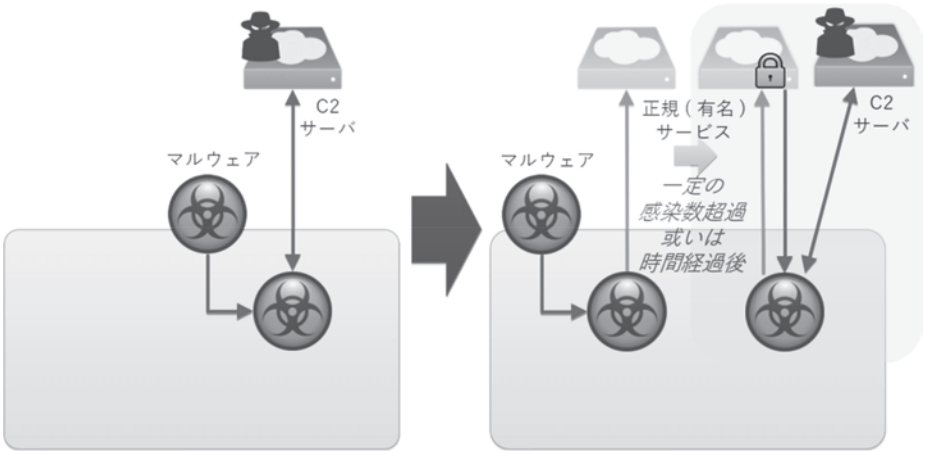
１　ソフトウェアの更新機能を利用したマルウェア感染（図２）

代表的なマルウェア感染の経路は，スピアフィッシングメール，悪意のあるサイトの閲覧，外部記憶デバイス（USBメモリ，DVD-R/CD-R等）である。これまで政府機関やセキュリティ企業が，このような代表的な感染経路を想定した啓発や取り組み等を行ってきたことで，その影響を受けやすい主要な民間組織における対策は進んでいる。そのため，攻撃側が，このような主要な民間組織を標的とした場合，マルウェア感染の難度が高くなっており，概ね成功率も低くなってきている。執拗に攻撃対象へのマルウェア感染をさせようと考えている攻撃側は，他の感染経路として「ソフトウェアの更新機能」を利用するようになってきた。

この背景には，主要な民間組織における基幹業務（生産管理，販売管理，購買管理，在庫管理，会計，人事給与等）のIT基盤への依存性が高まり，一部では自社運用コストやセキュリティコストの肥大化の解決策としてクラウドに移行する民間組織も目立ってきているため，利用するソフトウェアの数や種類が増加していることにある。一般的に，ソフトウェアは，利便性，操作性，セキュリティの向上のために更新（アップデート）を行う保守管理のプロセスを伴う。攻撃者は，このような攻撃対象の状況変化をよく観察し，その変化から発生する新たな脆弱な箇所を見出しているのである。

特に，「更新サーバを乗っ取った」場合，マルウェア感染させる機能を組み込んだ更新モジュールが，配信対象のPCに対して一斉にインストールされるため，同時多発的な被害が発生する。さらに，このようなマルウェアは，PCをコントロールするための権限が一部制限されている「ユーザ権限」ではなく，PC全体をコントロールすることが可能な「システム権限」で動作するため，PCユーザが騙されて実行させてしまうマルウェアとは異なり，PCに与える被害規模は大きい。

図３：正規サービスを（時間差で）踏み台にするC2通信



出典：筆者作成

２　正規サービスを（時間差で）踏み台にするC2通信（図３）

攻撃側は，攻撃対象のPCに対するマルウェア感染に成功すると，攻撃者が意図した挙動をさせるためのマルウェアに対する指令や，感染PC内部のデータをマルウェアから受信するための指令（Command and Control）サーバ（以下，C2サーバ）とのやり取りのための通信（以下，C2通信）を確立する。これに対するセキュリティ技術として，URLブラックリスト（既知のC2サーバリストによるURLフィルター）があり，早期検知による被害抑制のために適用するところが多い。

攻撃側は，このような対策を無能化するために，初度の通信先を「正規サービス」にすることで，攻撃側はC2サーバの機能停止や通信検知によるマルウェア感染の拡大阻止を回避しようとする。また，利用されている「正規サービス」の多くは，有名なブログサイトであるため，攻撃対象がアクセスしても不自然でないサイトを選んでいる様子が窺える。

攻撃者は，マルウェア感染が一定数を超える，或いは感染活動が一定期間を超えた時点で，「正規サービス」上に，「マルウェアのみが解釈できる文字列」を書き込み，それにアクセスしたマルウェアが当該文字列を解釈（多くの場合，復号化）し，C2サーバのドメイン或いはIPアドレスを入手する。その直後，マルウェア感染したPCが一斉或いは段階的にC2サーバにアクセスし，本格的な攻撃が行われる。つまり，「正規サービス」を時間差で踏み台にしたC2通信を確立する手段である。さらに，攻撃側にとっては，本格攻撃を仕掛ける段階までC2サーバを隠すことができるため，攻撃者にとって手間とコストのかかるC2サーバの費用対効果が向上する。

特別な検知システムを導入していない限り，C2通信が確立した直後に検知することは難しく，他のケースより感染規模が大きいため，マルウェアの挙動による被害が甚大化しやすい。

Ⅳ　日本特有のサイバー攻撃対処における厳しい環境

以前のサイバー脅威への対策のキーワードとして「情報セキュリティ」が長らく叫ばれていた。これは，情報資産を機密性（権限を与えられた者のみが利用可能な状態）・完全性（権限を与えられてない者が変更できない状態）・可用性（権限を与えられた者が必要なときに利用できる状態）の確保を行い，正常に維持することである。この概念は，英国の規格協会（BSI）が1995年に規定したBS7799で示された，情報セキュリティマネジメントシステム（ISMS）の構築手順が標準化したものである。（民間の経済活力の向上等を任務とする）経済産業省は，このISMSを認証制度として，広く民間組織等にこの認証制度を取得させる施策を展開した。例えば，契約先業者に求める要件としてISMS認証取

表1：ISMS（ISO27001）の上位10の国別取得数

Top 10 countries for ISO/IEC 27001 certificates - 2016		
1	Japan	8945
2	United Kingdom	3367
3	India	2902
4	China	2618
5	Germany	1338
6	Italy	1220
7	United States of Amerdica	1115
8	Taipei, Chinese	1087
9	Spain	752
10	Netherlands	670

出典：ISO（国際標準化機構）中央事務局[2)]

得を前提とする商慣習の構築などである。これは，経済活動の阻害要因となる可能性のあるセキュリティインシデント（事業運営に悪影響を与える情報セキュリティを脅かす事件や事故のこと）の発生回避或いは被害抑制を狙ったものである。2016年におけるISMS（ISO27001）の取得企業・団体数は，ISO（国際標準化機構）中央事務局による発表によると，日本は8,945社で世界1位である。2位の英国（3,367社）を大きく引き離す数である（表1）。

数字の上では，日本は高い水準の情報セキュリティの確保が実現した形となっているが，運用が定着しない，リスクアセスメントが有効に行われない，インシデントが減らない等の理由で，取得したISMS認証が形骸化している状況[3)]が見られている。

また，民間組織が個人情報の漏洩を公表するという義務的行動が当たり前のようになっているのは，経産省が2004年に公表した「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」において，“二次被害の防止，類似事案の発生回避等の観点から，個人データの漏えい等の事案が発生した場合は，可能な限り事実関係，再発防止策等を公表することが重要である”と示されたためである。なお，このガイドラインは，2017年5月30日をもって廃止され，同種のものは，2016年に内閣府の外局として設置された個人情報保護委員会が「個人データの漏えい等の事案が発生した場合等の対応について（平成29年個人情報保護委員会告示第1号）[4)]」として公表している。

1　動的に変化するサイバー脅威に対する認識

情報セキュリティは，あらゆる脅威から情報資産を守るための施策であるため，サイバー脅威への対策として特化したものではない。他の脅威への対策もしなければならないため，常に新しい脅威が発生し，かつさまざまな事業領域に関係するサイバー空間を積極的に観察及び認識することは難しい。特に，ISMS認証は，サイバー脅威が高頻度かつ広範囲に変化することを前提して設計されたものではない。例えば，閑散とした地域に建てた住宅に住み始めた頃は，周囲にセキュリティ上の脅威が少なく，リスクは低いため，施錠のみのセキュリティ対策で十分と考える。しかし，その地域の開発が進み近隣に風俗店やギャンブル店が乱立すると，セキュリティ上の脅威が発生し，空き巣や泥棒のリスクが高まるため，施錠に加えて防犯カメラや金網の設置などの追加的なセキュリティ対策を考えることになる。ところが，サイバー空間における脅威の変化は，直感的に認識することが難しいものである。特に，セキュリティ対策に係る予算割当を決定する経営層にとっては，脅威の高まりを理解するための必要な専門的な概念や技術用語に馴染みが少ないため，実際の被害事例や自社に対する影響などの具体的なシナリオを求める傾向にある。しかし，情報セキュリティを担当する部門は，他社から具体的事例を入手することや，自社内の事業部門からネガティブな話となる被害想定を得ることは非常に難しい。実際には，特定の情報セキュリティ担当者が，経営層に対して献身的な説得を続けることで，ある程度

2）https://isotc.iso.org/livelink/livelink?func=ll&objId=18808885&objAction=Open&nexturl=%2Flivelink%2Flivelink%3Ffunc%3Dll%26objId%3D18808772%26objAction%3Dbrowse%26viewType%3D1

3）情報セキュリティマネジメントシステムの形骸化に関する考察（https://www.jstage.jst.go.jp/article/jasmin/2015s/0/2015s_121/_article/-char/ja/）。

4）https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf

の予算を獲得するという努力が行われている。

2　セキュリティ対策に係る役割・責任に基づく行動の実効性

情報セキュリティ対策に係る体制の構築においては，関係者の役割・責任を明確化するという作業が重要になる。ところが，サイバー攻撃対処の観点で，策定された「役割・責任に基づく行動」を眺めていくと，担当者の実務能力をほぼ無視したものが散見される。例えば，ISMS 認証取得企業における情報セキュリティの取り組みの中で「情報セキュリティに関する事故（セキュリティ・インシデント）を発見した者は，その起こる可能性を含めた事象の段階から速やかな報告を義務付ける」というものがある。この行動を実現するためには，" 認知した事象に対して，情報セキュリティに関する事故につながる可能性の有無が判断できる或いはその能力を有する " ことが暗黙的に求められる。ところが，最近のサイバー攻撃は検知回避の技術が飛躍的に向上しているため，専門家ですら発生した事象に対する判断を間違えるようになってきている。したがって，管理者は，この行動だけで情報セキュリティに関する事故の可能性を察知できる割合が相対的に減少していることを認識しなければならない。しかしながら，実際には，ISMS において強く求められる PDCA の Check（点検・監査）において，サイバー脅威に対する認識の変更管理がほとんど行われていないため，実情に即した方針変更をすることができていない。逆に，サイバー脅威に対する認識の変更を試みようとすると，広範囲かつ専門的な技術領域に及ぶサイバー攻撃に関連した情報の収集と分析，そして自組織に対する影響評価を仔細に行わなければならないため，ISMS 認証の維持管理を遥かに超える労力に加え，サイバー攻撃に関する専門的知識や組織内部の業務知識・慣習などの深い知識や豊富な経験を必要とする。

3　サイバー攻撃発生時における対処時に発生する想定外のコスト

最近のサイバー攻撃は，事象発生時から管理者が気づくまでに数十日から数百日かかるケースが散見され，一様に被害が大規模化している。しかし，各方面においてサイバー攻撃に関するリサーチが積極的に行われているため，自らの力で，組織内で発生している攻撃に気づく前に，行政機関からの情報提供やマスコミからの取材などがきっかけで気づくケースが増えてきている。この背景には，行政機関が取り組んでいるサイバーセキュリティの強化の一環として，民間企業において発生したサイバー攻撃を把握する仕組みを整備しつつある。ところが，物理世界において消防や救急などの公共サービスを求めるための緊急通報（119 番等）に相当する仕組みが，サイバー空間には存在していないため，民間企業のサイバー攻撃に係る財務的負担や被害による経済損失は拡大の一途を辿っているところである。残念ながら，行政機関は，サイバー攻撃が発生した民間企業が行う対処行動に対して十分な支援を提供しないどころか，複数の行政機関からほぼ同時に情報提供依頼をかけることで，サイバー攻撃を受けた企業に相当な負担をかけているという自覚が見られない。筆者は，これを行政機関が行う施策の限界であると見ている。先進的な取り組みを実現している他国は，国民の生命・身体・財産を守る任務を持つ公的機関が主導している。日本は，「国民生活の基盤に関わる行政を所管する行政機関」や「民間の経済活力の向上等を所管する行政機関」及びそれらに由来する役人がサイバーセキュテリィ対策の主導的立場を取っているため，国民の生命・身体・財産を守るためのより踏み込んだ施策を作り出すことは難しいようである。

Ⅴ　サイバー脅威への状況認識と対処を可能とする態勢整備と能力獲得

以上のように，サイバー脅威の変化と，それに立ち向かっていかなければならない我々の（少々残念な）実情について言及した。筆者は，国民の生命・身体・財産を守る任務を持つ公的機関が，より広範囲かつ体系的にサイバー脅威の認識を徹底的に行い，我々のサイバー攻撃対処における客観的な問題分析と必然的に導かれる解決策，及び（言いっ放しではない）確実な実現に向けた取り組みとプロセス管理を厳格に行っていくことで，今後のサイバー防衛を高めていくことは可能であると

考えている。

現時点で，筆者における活動経験の限りで必然的に見出された「サイバー攻撃への状況認識と対処を可能にする態勢整備と能力確保」を紹介する。

1　対処行動の実効性の確保

まず，情報資産の保護に偏重した情報セキュリティの概念や慣習から脱却することである。そして，実際の現場で誰がどのような対処行動をするかに着目し，その実務能力の見極めと実効性を確保した上で，インシデントレスポンスを設計する必要がある。現場の実情や当事者の人物像を把握していない者が設計することは避けるべきである。

2　徹底かつ包括的な状況認識

脅威として認識すべき攻撃者像とその行動特性に着目した積極的な対処姿勢を取らない限り，防衛活動を実現することは非常に難しい。愚策のみを繰り返すことになる。常に，サイバー空間の脅威動向の変化を徹底的かつ包括的に認識していくことが必須である。これにより，潜在化している可能性のある事象を見つける手がかりの獲得につながり，サイバー攻撃の早期検知につなげることが期待できる。さらに，新しいサイバー攻撃には，これまで着目していなかった技術領域を伴うことが多いため，それらを積極的に理解しようとする行動の中で，自身の教養不足を補い，新しい概念や技術を獲得することができる。

3　権限を有する者が積極的（強制的）に関与

サイバー攻撃による被害が組織に重大な被害を与えることになった場合，組織の上層部が適切な意思決定や指揮を執らなければならない。その際，上層部が，現場から報告されたインシデントの概要や現場への影響が発生する仕組みを理解しなければ，的を外した状況認識とそれに基づく意思決定をしてしまう可能性がある。また，現場から組織の上層部までの報告ラインにある各部門長も同様である。そのため，現場の業務活動に対して強い権限を持つ各部門長が緊急時に参集する場を整備するなどして，適切な状況認識と意思決定ができる環境を確保し，権限を有する者に（やや）強制的に関与していただく仕組みを作る必要がある。

4　メンバー間の定例会の開催

もはや組織の業務は，ITやインターネットに大きく依存しているため，そこで発生したインシデントは，少なからず業務に係る情報を含むことになる。そして，インシデントの報告先は，CSIRTやSOC等の他の部門であることが多いため，業務情報を含むインシデント報告をすることに抵抗感を感じ，上長の承諾を得ようとする傾向にある。これを厳格な内部規則の徹底と運用で報告を徹底しようとする動きもあるが，インシデント報告をすることに対するデメリットを与えるだけの結果になりやすく，逆効果となる。したがって，やや不都合な情報或いは適用すべきルールが不明な事象の情報でも，インシデント報告先に伝達しやすい雰囲気を形成するために，関係者間の対面による定例会を開催することが必要である。他の分野と同様に，連携強化を図る上で，やり取りする相手の顔が見えることが最も重要である。この定例会により，各部門の考え方やインシデントハンドリングの円滑な流れを構築するにあたり必要な改善点を得ることも期待できる。ただし，定例会は単なる勉強会や伝達のみにするだけでは効果は低くなるため，双方向の討議を伴うものにする必要がある。

5　初動対処に係る行動を伴う訓練の実施

情報セキュリティ対策と異なり，サイバー攻撃対処は，想定外の事象を扱うことが多い。この理由は，大きな被害につながる可能性のある事象は，事前に想定可能なものとして抑止策や回避策を実施しておくためである。想定外の多くは，サイバー空間における脅威動向の変化に追随することでできなかった領域であり，想定内であっても被害が発生するのは，自組織内の初動対処に係る行動が，迅速かつ円滑に実行されていなかったためである。このため，相互の関係性強化を図る目的で，対処行動に係る行動を伴う訓練を実施する必要がある。