Computer Security Symposium 2017
23 - 25 October 2017

被害の抑制に有効なサイバー攻撃や対策情報の組織間 及び組織内における共有の仕組みの提案

平井 達哉[1]　本川 祐治[1]　佐々木 慎一[1]　丹京 真一[1]

概要：近年，複数の事業者が同時多発的に被害にあうサイバー攻撃が増加している．この種の攻撃による被害を抑制するには，サイバー攻撃，被害状況，対策等の情報を，事業者内・複数の事業者間で迅速に共有できる仕組みが必要である．現在でも複数の人々の間でのサイバー攻撃や対策に関する情報の共有は行われているが，共有範囲が有識者で構成される非公開コミュニティに限定されている場合も多く，広範囲での情報共有は十分には進んでいない．そこで我々は，事業者内，複数事業者間，情報収集・配信組織と事業者の間での情報の共有において想定される特性や，情報を共有するのに有用な仕組み等を提案する．

キーワード：情報共有，サイバー攻撃，被害状況，対策

Proposal of a framework to share information on cyberattack and countermeasures among multiple organizations and within a company effective to reduce damage

Tatsuya Hirai[1]　Yuji Motokawa[1]　Shinichi Sasaki[1]　Shinichi Tankyo[1]

Abstract: Recently, cyberattacks by which multiple companies have suffered simultaneously have increased. To suppress damage due to such attacks, it is necessary to establish mechanisms to share information on cyberattacks, damage situations, and countermeasures in a short period of time. Some of such information have already been shared among multiple persons, but it is limited within private communities, to which only experts on the topics belong and the information has not been shared sufficiently extensively. Therefore, we propose characteristics assumed on the information sharing in a company in various business categories, among the companies, and between the organizations which gather and dispatch such information and the companies, and mechanisms useful to share such information.

Keywords: information sharing, cyberattack, damage situation, countermeasure

1. はじめに

従来，様々な分野の事業者は，以下に挙げるような手段を用いてソフトウェアの脆弱性，サイバー攻撃，攻撃への対策に関する情報を入手してきた．

(1) ソフトウェア開発企業が一般に公開する脆弱性情報，およびその対策手段情報
(2) サイバー攻撃やそれらへの対策に関する情報の収集・展開を専門に行う機関から配信される情報の受信 [1][2][3]
(3) 有識者で構成される非公開コミュニティで交換される情報の受信 [4]

上記のうち，(1) や (2) の形で展開される情報は，大量であったり，誤り，既に無効になったもの，重複するもの等も含んでいたりすることもあった．そのため，情報を受信した事業者は，迅速に対策を実行する必要がある情報を見落としてしまったり，対策の実施を後回しにしたりする事態を生じる懸念があった．これに対し，(3) の形態で展開される情報については，有識者間で交換されていることか

[1] 株式会社 日立システムズ
Hitachi Systems, Ltd.

ら，信頼度や分析結果等に関する情報も含まれている場合もあり，迅速な対策の実施が必要な情報の選別は，(1) や (2) の情報より容易であると考えられる．しかし，有識者がいない事業者は，(1) や (2) の手段でしか情報を入手できない場合もあり，実際に被害を生じる前に対策を完了することができないこともあると考えられる．また，(2) に記載の情報収集機関は，一般的に，情報を配信する前に得た情報の精査，分析等を行うため，実際に情報を配信するまでにも一定の時間を要する．更には，情報の展開自体も，担当者からのメールや電話等で行われることも多く [5]，情報が伝わる速度は担当者が置かれている状況に依存する．一方で情報を受信する側である事業者は，複数の組織から情報を受信することも考えられるため，同一の攻撃に関する最新の状況や対策等を含む情報がどれであるか分析するのに時間を要するといった点も，対策の実施が遅れる要因になっている．

ところで，近年見られるサイバー攻撃の特徴の一つとして，重要インフラ分野の事業者が標的となっている点を挙げることができる [6]．重要インフラの停止は，人々の生活に及ぼす影響が大きいことを鑑みると，サイバー攻撃によってインフラが停止することを防止するための施策を事業者が実施することに関する社会的な要請は，強いと考えられる．実際，国内における ICT システムのサイバーセキュリティ政策を主導する内閣サイバーセキュリティセンター（National center of Incident readiness and Strategy for Cybersecurity; NISC）は，重要インフラ事業者等におけるサイバーセキュリティの確保を促進することを表明している [7]．

上記以外の近年のサイバー攻撃の特性として，攻撃者が戦術的かつ組織的に攻撃を行うようになっていることやゼロデイ攻撃が増加していることが挙げられる [8][9][10]．そのような攻撃には，事業者内の情報システムだけでなく制御システムを対象としていたり，ある分野の複数事業者を同時多発的に狙うものであったりという特徴がある [10][11]．従って，サイバー攻撃，攻撃への対策等の情報を，事業者内及び異なる組織や事業者の間で迅速に共有できる仕組みが確立されていれば，上記のような攻撃によって引き起こされる被害を，より小さく抑えることを期待できる [12]．尚，上記における「情報の共有」は，明らかにある者から他者への単なる「情報の送信」を意味するものではない．同句は，サイバー攻撃に関する情報の共有であれば，例えば，受信した複数の情報の中から最新のものや重要度の高いものを判別し，その内容を受信者が理解することを，対策の情報の共有であれは，受信した複数の情報の中から優先的に実施すべき施策を判別及び理解すること等を意味する．そこで以下では，「情報の共有」を，上記のような意味を持つ語句として用いる．

本論文の構成は以下の通りである．2 章において，既存の情報共有の仕組みと課題を紹介する．続いて 3 章において，我々が提案する事業者内，異なる組織や事業者の間で情報を交換・共有するのに想定される特性や仕組み，また情報共有を達成するのに有用なシステムの機能について述べる．4 章では，情報を共有することによって得られると推測される定性的効果について述べる．そして 5 章で本論文の内容をまとめる．

2. 既存の仕組みと課題

実際に運用されているサイバー攻撃に関する脅威，侵害，および被害の情報を共有するための仕組みは，いくつか存在する．

日本においては，公的機関である独立行政法人 情報処理推進機構（Information-technology Promotion Agency; IPA）を情報の集約点として，参加組織間で標的型攻撃メールに関する情報共有を行うための仕組みであるサイバー情報共有イニシアティブ（Initiative for Cyber Security Information sharing Partnership of Japan; J-CSIP）[3] がある．J-CSIP は，IPA と各参加組織，あるいは参加組織を束ねる業界団体の間で秘密保持契約を締結することを前提とする．ある参加組織において標的型攻撃メールによる攻撃が検知されると，当該組織は IPA にその情報を送信する．IPA は，情報の提供元を匿名化したり分析情報を付加したりした後，情報提供者の承認を得た上で，電子メール等を用いて参加組織に情報を展開する．展開された情報を受け取った他の組織は，それに基づいた施策を実施した結果を IPA に対して通知する．IPA は，受信したその情報を，内容に応じて他組織に再展開する．この仕組みには，標的型メール以外の手段で実際にサイバー攻撃が行われている場合に，その情報が随時交換されない可能性がある点や，人手を介さない情報の伝達に不向きな方法を用いているために情報を活用しにくいといった点，また事業者内での情報を共有するための仕組みの提供は企図されていないといった点に課題がある．

英国では，政府と企業の間や信頼関係がある組織の間でサイバー攻撃や脆弱性情報を共有することを目的とした仕組みである Cyber Security Information Sharing Partnership（CiSP）[13] が，サイバー犯罪に対抗するための国営のセンターである National Cyber Security Centre（NCSC）によって運用されている．CiSP には，英国に本社がある企業や英国における電気通信事業者，政府組織により設立された組織等のみ参加が可能である．一方，参加する組織や個人は，無料で利用することができる．

CiSP では，情報の交換は SNS のような形で情報を登録するシステムを用いて行われる [14]．本システムに対しては，個々の参加者の他，参加者が業界や立場を超えて情報を交換するようにする部門（Fusion Cell）も登録できる．Fusion Cell にはモデレータおよびアナリストと呼ばれる

者が存在する．モデレータは，投稿されたある情報の内容が不十分であった場合に不足している情報を参加者から引き出したり，システム上のあるグループで登録された情報を，情報提供者を匿名化して他のグループに展開したりする．アナリストは，登録されたマルウェア等の調査，分析，評価等を行う．

上記の通り，CiSP で用いられている情報交換用システムでは，参加者が非定型な情報を登録することができる．その一方で，情報の交換は，当該仕組みへの参加者（当該システムの利用者）に限定されていて，別のシステムとの間で情報を交換することはできないという短所がある．

米国では，契約した事業者等に対し，Structured threat information expression（STIX）[15] と呼ばれる形式で表現された指標 （インディケータ）[*1] を，Trusted automated exchange of indicator information（TAXII）[16] と呼ばれるプロトコルで送信する AIS[17] と呼ばれる指標配信システムが，The Department of Homeland Security（DHS）によって運用されている．ここで STIX は，サイバー攻撃や脆弱性の情報を XML や json を用いて記述する標準化された表現法であり，TAXII は同様の情報を交換するための標準化されたプロトコルである．

STIX 形式の情報を，TAXII プロトコルを使って送受信する AIS を通じた情報交換の仕組みは，特定の情報交換システムの利用を強制しないという利点がある．ただし，J-SCIP の仕組みと同様に，本仕組みは情報の最終受信者である各事業者での情報の共有を支援することを企図してはいないという点で，課題がある．

3. サイバー攻撃および対策方法に関連した情報を共有するのに有用な仕組みとその特性

1 章に述べたように，サイバー攻撃によってもたらされる被害を小さく抑えるには，ソフトウェアの脆弱性，サイバー攻撃，左記攻撃への対策の情報を，事業者内及び異なる組織や事業者の間で迅速に共有できるようにすることが重要である．これを実現する組織としては，サイバー攻撃等に関する情報の収集・分析・展開などを専門に行う機関が想定される．情報を交換，あるいは共有する対象が異なると，そこで想定される特性も異なると考えられる．以下では，それらについて分析した結果を述べる．

3.1 一事業者内における情報共有において想定される特性

事業者がサイバー攻撃を受ける場合の対象は，事業者が保有する情報システムや制御システムである．これらのシステムのセキュリティ的観点における管理は，一般的に以下に挙げる部門によってなされると考えられる．

- 現場部門
  システムの管理，保守・運用（サイバー攻撃による被害の発生を抑制したり，ソフトウェアの脆弱性を除去したりするための対策の実施），監視を行う．システム運用者，業務運用管理者等が想定される者である．業務運用管理者とは，業務の運用状況を管理する者で，システム自体の運用をする者とは別である．
- Computer Security Incident Response Team（CSIRT[*2]）
  サイバー攻撃に関する情報の収集，分析，知見化，攻撃への対策方法の確定，収集した情報や確定した対策の関係部門や他事業者への展開などを行う．
- 経営層
  下位層からセキュリティ上の問題に関する報告を受け，事業継続計画（Business Continuity Plan; BCP）の観点から各システムの稼働継続や停止を決定し，下位層に指示する．

現場部門がサイバー攻撃を検知した場合，自身で対策方法や対策を実施する場合に生じる影響が小さいことなどが自身で把握できれば，現場部門が独自で対策を実施する．しかし，現場部門だけでは対策方法を確定できない場合は，CSIRT に攻撃の内容を報告し，対策方法の提示を依頼する．CSIRT は，報告を受けたサイバー攻撃を分析の上，対策方法を現場部門へ提示する．また，当該攻撃がシステムに及ぼす影響が甚大で，システムの稼働継続／停止の判断等を経営層に仰ぐ必要がある場合は，サイバー攻撃による被害状況や課題，経営上のリスク等を経営層に報告する．経営層は，上述の通り，BCP の観点からサイバー攻撃を受けたシステムの稼働継続や停止を決定し，情報システムの運用者や制御システムの運用者に，結果を指示する．以上に述べた処理の流れは，**図 1** のようにまとめられる．

図 1 に示したように，上述の 3 つの部門で行われる処理や部門間で行われる情報の伝達について，これらを支援する仕組みを事業者が導入できれば，当該処理や情報の伝達をより迅速に達成することができると考えられる．また，その結果として，サイバー攻撃の検知から対策の実施までに要する時間の短縮化，更にはシステムの停止が必要な事態に陥る可能性を低く抑えられるようになることを期待できる．上記目的に対しては，既存の SNS サービス [19][20] でも見られるような，特定のメンバーからなるグループを作成できること，そのグループ用のタイムラインが構成され，そのグループのメンバーが自由にそこに情報を登録できることといった特性を備えるシステムが有効であると考えられる．上記特性に加えて，以下に挙げる機能を備えていると，本システムは経営層，CSIRT，現場部門間のより円滑な情報共有を実現できると考えられる．

- 先に述べた通り，現場部門の者は，検知したサイバー

[*1] サイバー攻撃を特徴付ける特定の情報．IP アドレスや URL の値などがその例である．

[*2] 日本国政府は各事業者に対して CSIRT の設立を推奨している．実際，CSIRT を設立する事業者の数は増加している [18]

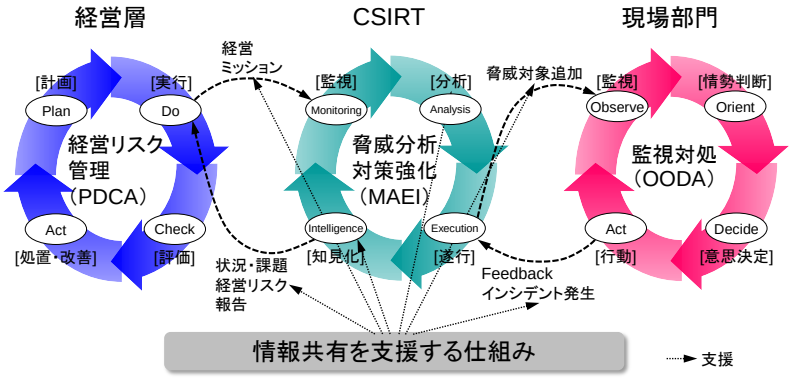

図 1　事業者内で求められる情報の伝達と情報共有を支援する仕組み

Fig. 1　Propagation of the information and mechanism supporting information sharing required in a company

攻撃への対策手段を自身で確定できない場合，CSIRT に攻撃内容の分析を依頼する．また，CSIRT は，分析を行う際に，所属する分野の Information Sharing and Analysis Center（ISAC）のアナリスト等に，技術的な支援を依頼することがある．最終的に CSIRT が対策方法を確定すると，それを現場部門に通知し，同部門の者が対策を実施する．これらの情報伝達や処理を迅速に行えるようにするためには，以下の機能が有効である．

- 新しく登録された情報を，蓄積されている情報の中で関連があるものと関連付けたり，統合したりする（あるいはそれを支援する）機能
- 分析に必要な情報（有害サイトの URL，マルウェア，システムのログに関する情報等）に触れた場合でも，攻撃用のコードが実行されたりすることのないようにする機能
- 蓄積されている情報から，サイバー攻撃への対策方法を迅速に検索できる機能

- CSIRT は，必要に応じて分析結果をまとめて経営層に報告するため，この作業を効率的に行えるようにする機能（例: 報告をまとめる作業を支援する機能）
- CSIRT は，現場部門に対して対策の指示，対策の実施状況の把握，およびフォローアップを実施するため，これを迅速に行えるようにするための以下の機能
  - 大量の情報から，必要な情報を絞り込んで表示する機能
  - 各組織や対象システムへの対策の実施状況を可視化する機能

3.2　情報を収集・中継する組織と事業者間における情報共有において想定される特性

1 章に述べたように，ある分野に属する複数の事業者が同時並列的にサイバー攻撃を受ける事態は実際に発生している．従って，分野内の多くの事業者が，サイバー攻撃やその対策方法を早期かつ同時期に入手できれば，被害の抑制に有効であろうと考えられる．

一方で，異分野の事業者間での情報が共有できることには，上記とは異なる利点があると考えられる．その一つは，供給連鎖管理（Supply Chain Management）上の利点である．例えば，情報通信分野に属する複数のプロバイダ事業者（A とする）がサイバー攻撃を受け，情報の送受信が滞る事態を生じたとする．その場合，他の分野の攻撃を受けていない事業者（B とする）のシステム も，必要な処理を十分に実行できなくなる可能性がある．この時，事業者 A と事業者 B の間で当該攻撃に関する情報が共有されていれば，事業者 B は早期に対策を講じることができるため，上記のような事態を生じる可能性を低く抑えることができる．このような推察から，異分野に属する事業者間でも迅速に情報を共有できる仕組みを整備することは，有用であると考えられる．

ところで，ある事業者が検知したり分析の結果得たりしたサイバー攻撃等情報の他の分野の事業者への展開が，情報を得た事業者から相手事業者への直接発信のみしか存在しない場合，情報が十分広範囲には広がらないことが懸念される．そこで，ある事業者から他の多くの分野の事業者への情報の展開がより円滑に進むようにするために，以下のような，情報の収集および展開を行う組織を設けることが有用であると考えられる．

- 各分野内に各々の事業者とは独立した組織を設け，そこに情報送受信・蓄積システムを設置する．当該組織は，本システムを用いて，分野内の各々の事業者に，収集・知見化・体系化された情報を一斉に展開する．ISAC[21][22] は，このような役割を果たす組織の実例である．以下でも，このような役割を果たす組織を ISAC と呼ぶ．
- 特定の分野に属さない組織を設け，そこに上記機能を備えた情報送受信・蓄積システムを設置する．当該組織はある ISAC が把握した情報を各分野の ISAC や事

業者に展開する役割を担う．このような役割を果たす組織を，以下では分野横断情報共有支援機関と呼ぶ．分野横断情報共有支援機関から各事業者への情報の展開は，各分野の ISAC を経由して行われる場合だけでなく，ISAC が設立されていない分野があることも考慮し，ISAC を経由せずに事業者に対して直接行われる場合も想定する．

以上に述べたことをまとめると，我々が提案する組織と事業者の間での情報交換は，**図 2** のようになる．

ところで，分野横断情報共有支援機関，ISAC，各々の事業者が導入する情報送受信・蓄積システムは，狙いや準備できる資金量に応じて決定されると考えられる．つまり，全てが同じシステムを導入しているとは限らないと考えるのが自然である．このような状況でも情報を交換できるようにするために，異なる事業者や組織の間で交換される情報の形式とそのプロトコルの一つを，規定しておくことは有用である．2 章に挙げた STIX および TAXII は，このようなことを目指して規定されたものの一つである．そこで，各事業者や組織における外部との間で情報を送受信するシステムに対しては，STIX 形式の情報を TAXII プロトコルに沿って送受信できる機能を備えていることを要請する．

ところで，分野横断情報共有支援機関や ISAC が収集する情報には，重複するものが含まれたり，全ての情報を人が確認しきれないほどの数の情報を受信したりすることが考えられる．このような情報がそのまま事業者に送信されると，早急な対策の実施が必要な内容を含む情報を，事業者の CSIRT や現場部門の者が見落とす可能性がある．このような事態を生じないようにするために，情報送受信・蓄積システムが以下のような機能を備えていると有益である．

- 蓄積済みの情報と同じ情報を新たに受信した場合には，それを破棄する機能
- 蓄積済みの情報と関連する情報を新たに受信した場合には，関連する蓄積済み情報を提示する機能
- 各々の情報に優先度や識別子を付与することができ，優先度の高いものを優先的に表示したり，同一の識別子のものをまとめて表示したりする機能
- ある事象に関する最新の状況や対策方法を表示する機能

上記機能が存在すれば，事業者が情報を受信してから対策を実施するまでの時間の短縮や，より有効性の高い対策を早期に実施できるようになること，その結果として，サイバー攻撃による被害を抑制できることが期待できる．

3.3 情報共有上有用な CSIRT，ISAC，横断的情報共有組織における役割

3.1，3.2 節における考察から，正しい情報が適切に整理された状態でかつ活発に交換されるためには，情報を中継，分析，整理する役割を負う CSIRT，ISAC，横断的情報共有組織が，そのような状態を実現するべく活動することが必要であると考えられる．そこで本節では，これらの部門及び組織が担うべき役割について，より詳細に述べる．

- CSIRT

  3.1 節に述べように，CSIRT は，異なる組織や事業者から展開されたり現場部門が検知したりしたソフトウェアの脆弱性情報やサイバー攻撃情報等の恒常的な収集と分析，対策方法の確定と現場部門への対策実施の指示，経営層への報告，社外の組織への情報の発信などを行う．これらを適切に行えるようにするには，CSIRT には以下に挙げる役割を設けることが有用である [*3]．

  [モデレータ]
  - 現場部門，他の事業者，他の組織等から送信された情報の受信
  - 入手した情報の現場部門，他の事業者，他の組織への送信
  - 上記情報の送信前における送信すべき情報の取捨選択（情報の一部秘匿化，情報の提供者に関する部分の匿名化等）
  - 誤っていることが確実な情報の削除
  - 情報の発信が活発かつ適切に行われるようにするための意見の発信（対他組織，事業者，自社内現場部門）
  - 情報交換の場に加えることが望ましいと考えられる有識者の提案

  [アナリスト]

  サイバー攻撃情報の分析; 但し，アナリストは，分析を行うサービスを提供する事業者外の組織を利用することも想定する．

  [スーパーバイザー]

  CSIRT 全体の統括; アナリストやモデレータへの実行すべき作業の指示は，スーパーバイザーが担う役割の一例．

- ISAC

  3.2 節に述べたように，ISAC は各分野に置かれ，ソフトウェアの脆弱性情報，サイバー攻撃情報の収集・分析や，それらの情報の分野内の事業者への展開を行う組織である．文献 [21][22] にあるように，既に ISAC が設立されている分野がある一方で，未だ ISAC が設立されていない分野も多数ある．このような分野においては，分野内の業界団体などを活用する形で情報の展開を行うことも考えられる．上記職務を適切に行えるようにするには，ISAC には以下に挙げる役割を設けることが有用である．

  [モデレータ]

[*3] 実際の運用においては，1 人の者が複数の役割を担う場合もありうる．

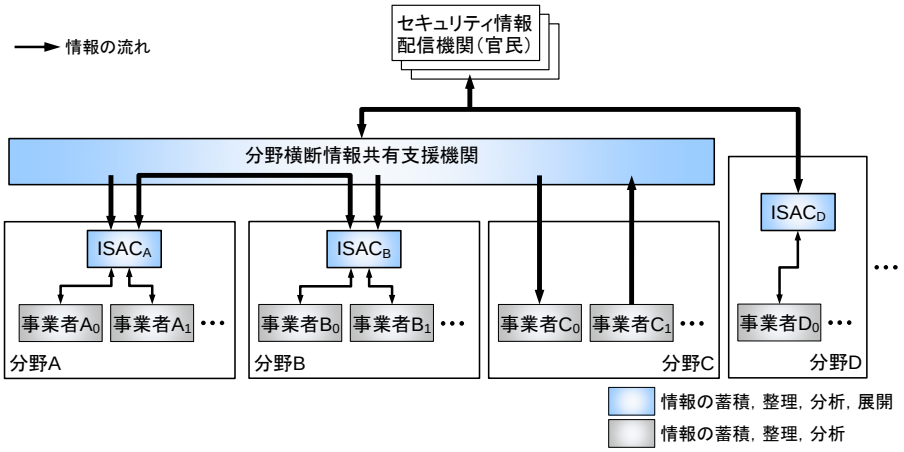

図 2　組織と事業者の間で行われる情報交換

Fig. 2　Exchange of the information executed among the organizations and companies

当該組織が担っている役割，責任の範囲を把握した上で，CSIRT のモデレータに挙げた職務のうち，左記に適合するものを遂行．

[アナリスト]

CSIRT におけるアナリストと同様．

- 分野横断情報共有支援機関

分野横断情報共有支援機関は，複数の分野に属する事業者や組織の間の情報交換を支援する，特定の分野に属さない組織である．インテリジェンスサービスが展開するグローバルレベルの情報や官民のセキュリティに関連する組織が展開する情報を各 ISAC や事業者に展開したり，ある ISAC が把握した情報を他の分野の ISAC や事業者に展開したりする役割を担う．分野横断情報共有支援機関から各事業者への情報の展開は，各 ISAC を経由して行われる場合に限らない [*4]．上記職務を適切に行えるようにするには，分野横断情報共有支援機関には以下に挙げる役割を設けることが有用である．

[モデレータ]

ISAC のモデレータと同様．

[アドバイザ]

サイバー攻撃や対策方法の提供を含め，様々な時事に対する助言を実施．

4. 情報の共有と得られた情報に基づいた対策の実行により事業者が得る効果

3 章に述べたような仕組みを基礎とした組織や事業者の間での情報の共有は，以下のような効果の連鎖を生むと考えられる．ある事業者や組織が，得たサイバー攻撃やその分析結果，対策等に関する情報を他の事業者や組織に対して発信するようになると，その情報を得られる事業者や組織は，高度な知見を獲得できるようになると考えられる．ある事業者や組織が高度な知見を獲得できると，それは自他の事業者や組織に，以下のような利点をもたらすことを期待できる．

(1a) 知見を利用することにより，同種や類似の他のサイバー攻撃に関する情報をより早期に把握できる

(1b) 自事業者内にアナリストの役割を果たす者を準備することが困難な事業者 [*5] にとっては，より少ない労力で分析結果を得ることができ、その帰結としてセキュリティ対策のベースライン向上が期待できる

入手した情報を利用して実際に対策に取り組むと，それらの情報を得ずに対策に取り組む場合に比べて，事業者は別の利点を得られるようになると考えられる．高度な知見の獲得から直接得られる利点は (1.1)，早期の情報の入手 (1a) から得られる利点は (1a.1) である．

(1a.1) 予防対策をより早期に実施できるようになる

(1.1) より高度な対策を実施できるようになる

利点 (1a.1) に沿って対策を実施できると，事業者は更に以下 2 つの効果を得られる可能性がある．

(1a.1.1) 他の事業者へ被害が拡大することの防止

(1a.1.2) 知見を得た事業者内での更なる被害の発生の未然防止

同様に，利点 (1.1) に沿って対策を実施できると，事業者は更に以下 5 つの効果を得られる可能性がある．

(1.1.1) 高度な対策を実施した事業者での被害発生の未然防止

(1.1.2) 高度な対策を実施した事業者内で被害が拡大することの防止

(1.1.3) 高度な対策を実施した事業者において被害が発生した場合に，その状態からの早期の復旧

(1.1.4) 高度な対策を実施した事業者での被害の再発の防止

(1.1.5) サイバー攻撃が困難化することによる攻撃頻度の

[*4] ISAC が設立されていない分野も存在するため．

[*5] CSIRT を設置していてもアナリストを確保できない事業者は，その一例である．

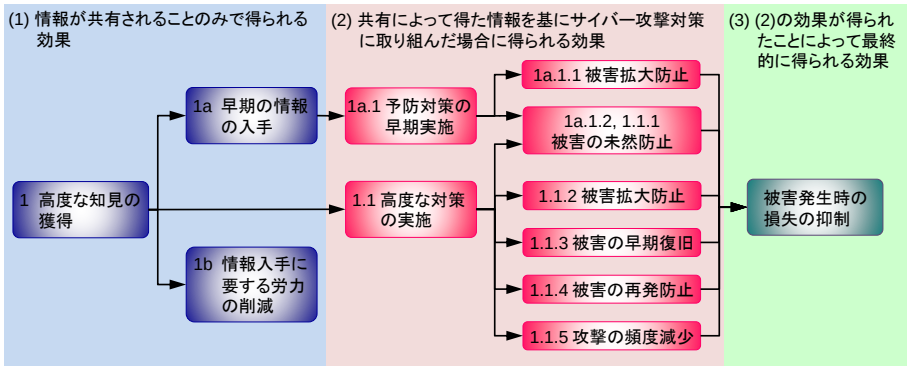

図 3 情報共有及び対策に取り組むことより事業者が得られると考えられる効果

Fig. 3 Presumed effect which companies obtain by sharing the information and implementing countermeasures

減少

上記 7 つの効果は，最終的にはいずれも被害が実際に生じた場合の損失の抑制をもたらすと考えられる．以上の関係を図示すると，**図 3** のようになる．

5. まとめと今後の課題

近年，複数の事業者が同時多発的に被害にあうサイバー攻撃が増加しており，この種の攻撃による被害を抑制するには，サイバー攻撃，被害状況，対策等の情報を，事業者内・複数の事業者間で迅速に共有できる仕組みが必要である．そこで本論文では，事業者内および異なる事業者の間で情報を交換するのに有用な特性，また情報を共有するのに有用なシステムの特性とその機能について述べた．左記の中で，事業者内での情報共有においては，現場部門，CSIRT，経営層の間での双方向の情報発信を支援するシステムが有用であることや，有効な情報の活発な交換を達成するには CSIRT におけるモデレータが情報の発信を適切に誘導することが重要であることなどを述べた．異なる事業者間での情報交換に関しては，流される情報の形式とプロトコルを規定の上，各事業者や組織が設置する情報送受信システムが左記形式及びプロトコルに沿って情報を送受信できることの他，情報の収集，冗長化排除，分析等を行う独立した機関の設置が有効であることなどを述べた．情報の共有と，得られた情報に基づいて対策を実行することによって，事業者は，高度な知見の獲得等を通して，生じる被害の抑制が期待できることを述べた．

今後は，本論文で述べた組織体制を各事業者や政府等へ提案すると共に，提案した仕組み，情報送受信・蓄積システムの開発，それらの広範な事業者や政府への導入，実運用時に生じる問題点の明確化，および提案した効果の検証に取り組むことが重要である．

謝辞 本研究は，総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人: NEDO）によって実施された．

参考文献

[1] JPCERT/CC. 情報提供 “注意喚起”, https://www.jpcert.or.jp/at/2016.html
[2] JPCERT/CC. 情報提供“早期警戒情報の提供について”, https://www.jpcert.or.jp/wwinfo/
[3] 情報処理推進機構. “サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））”, https://www.ipa.go.jp/security/J-CSIP/
[4] “攻めの防御 サイバーインテリジェンス”, 日経コンピュータ, pp. 20 - 37, 2016 年 6 月 9 日
[5] 内閣サイバーセキュリティセンター. 「セプターカウンシル」の活動 “重要インフラ セプター一覧表”, http://www.nisc.go.jp/active/infra/pdf/cc_ceptoar.pdf
[6] 内閣サイバーセキュリティセンター. 主要公表資料 “サイバーセキュリティ政策に係る年次報告（2015 年度）”, http://www.nisc.go.jp/active/kihon/pdf/jseval_2015.pdf
[7] 経済産業省. 産業構造審議会 商務流通情報分科会 割賦販売小委員会（第 14 回） - 配布資料 “資料 4 重要インフラ等に係るサイバーセキュリティ政策の概要”, http://www.meti.go.jp/committee/sankoushin/shojo/kappuhanbai/pdf/014_04_00.pdf
[8] JPCERT/CC. “高度サイバー攻撃（APT）への備えと対応ガイド”, https://www.jpcert.or.jp/research/20160331-APTguide.pdf
[9] ビジネス + IT. “門林雄基氏県談 - 攻撃側や利用者側の変化に伴い、新局面へ突入した IT セキュリティ対策”, 2012 年 9 月 10 日, http://www.sbbit.jp/article/cont1/25361
[10] Symantec. インターネットセキュリティ脅威レポート 第 22 号, 2016 年 4 月, https://www.symantec.com/ja/jp/security_response/publications/threatreport.jsp
[11] ITPro. “韓国激震、サイバー攻撃が同時多発”, http://itpro.nikkeibp.co.jp/article/COLUMN/20130328/466648/?rt=nocnt
[12] ダイヤモンド社. “情報セキュリティの方程式 第 2 回 攻撃者はエキスパート。守る側は英知を結集し連携せねば勝ち目はない”, 2015 年 3 月 6 日, DIAMOND online, http://diamond.jp/articles/-/67624
[13] National Cyber Security Center; Cyber Security Information Sharing Partnership, https://www.ncsc.gov.uk/cisp
[14] Surevine, https://www.surevine.com/threatvine/
[15] Structured Threat Information eXpression,

https://stixproject.github.io/
[16] Trusted Automated eXchange of Indicator Information, https://taxiiproject.github.io/
[17] Department of Homeland Security; Automated Indicator Sharing. https://www.dhs.gov/ais
[18] 独立行政法人 情報処理推進機構. “企業の CISO や CSIRT に関する実態調査 2016 -調査報告書-“, https://www.ipa.go.jp/files/000052362.pdf
[19] Facebook. https://www.facebook.com/
[20] Line. https://line.me/ja/
[21] 一般社団法人 金融 ISAC. http://www.f-isac.jp/
[22] 一般社団法人 ICT-ISAC. https://www.ict-isac.jp/