デジタルプラクティス　Vol.9 No.3 (July 2018)

特集招待論文

企業におけるCSIRTの活動とそれを支援する情報共有システム

平井 達哉[1]　本川 祐治[1]　佐々木 慎一[1]　丹京 真一[1]

[1]（株）日立システムズ

近年，ソフトウェアの脆弱性が明らかになってから，その点を突くサイバー攻撃が行われるまでの時間が短くなり，実被害を生じる例が増大している．生じる被害を抑えるために，各事業者では，セキュリティインシデントを未然に防止すること，セキュリティインシデントを生じた場合には迅速に対応することが，急務になってきている．それらを達成できるようにするには，各企業内に設置されているCSIRTが，各地で発生しているサイバー攻撃の動向やソフトウェアの脆弱性の情報，それらへの対策の方法を早期に入手できること，情報システム・機器の管理者や利用者に迅速に対策情報を通知できること，通知を受けた管理者や利用者が各機器に対して迅速に対策を実行できること等が必要である．そのためには，CSIRTがソフトウェア開発企業や国内外の情報収集機関等が発信するソフトウェアの脆弱性やサイバー攻撃，およびそれらへの対策に関する情報を入手し，情報を整理した上で，必要なものを，自事業者内や下位の組織・事業者等に展開できる必要がある．このような背景から，関連する組織，事業者，および人員の間で，情報を共有することを適切に支援するICTシステムが存在することが望まれる．上記観点から，我々はまず，被害を抑制するためにCSIRTが遂行する必要がある作業を分析し，その上でそれらをより迅速にCSIRTが遂行できるようにするためのICTシステムを開発・構築した．現在その有用性について検証を進めている．

1. はじめに

近年，ソフトウェアの脆弱性が明らかになってから，その点を突くサイバー攻撃が行われるまでの時間が短くなり，実被害を生じる例が増えつつある．そのため各事業者においては，生じたセキュリティインシデントに対応したり，それらを未然に防止する施策を実施したりすることが，急務になってきている．このような作業を中心になって推進する組織として，Computer Security Incident Response Team（CSIRT）と呼ばれる部署の設置が，多くの事業者で進んでいる ☆1．

上述の施策を各事業者が実行するには，平時，インシデント発生時の双方において，CSIRT，情報システム・機器管理者，情報システムの利用者が，以下に挙げることを達成できることが有用である．

（1）ソフトウェア開発企業や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が展開する脆弱性情報，その対策方法に関する情報，サイバー攻撃やそれらへ

の対処法に関する情報[1], [2], [3]を，各事業者のCSIRTが早期に入手できる．
（2）CSIRTから情報システム・機器の管理者や利用者へ，脆弱性や攻撃への対策の情報を迅速に通知できる．
（3）通知を受けた情報システム・機器管理者や利用者が，指示された対策を各機器に対して迅速に実施できる．

上記に対し，情報が流通し始めたばかりのものであったり，攻撃の分析結果が加えられたりしたものであったりするほど，有識者で構成されるコミュニティ内において，非公開で交換されているのが実態である[4]．その背景には，ある事業者がサイバー攻撃を受けたという情報が広まって，風評がその事業者の業績に影響を及ぼしたり，不特定の者によって虚偽の情報を流されたりすることを防ぐという意図があると考えられる．しかしながら，項目（1）を実現するには，日本国内にとどまらず，世界中の組織，事業者間で，ソフトウェアの脆弱性，サイバー攻撃，攻撃への対策等に関する情報を迅速に伝達する統一的な仕組みが存在することが望ましいのは明らかである．

その一方で，情報の入手先が増大すると，収集する情報の総数自体が増えることや，収集した情報の中に，重複，誤り，あるいはすでに無効化されていたりするものが含まれる可能性が高くなる．このような状態になると，結局CSIRTは，本当に必要であったり迅速な実行が必要であったりする情報や対策を，見落とす，把握するのに時間を要する，さらには誤配信するといった可能性が高くなる．その結果，情報システム・機器の管理者や利用者へ適切に通知すること，すなわち項目（2）の達成に支障をきたすようになる．

項目（3）に関しては，当該項目に記載の通りである．すなわち，各事業者において情報の収集を中心になって行うCSIRTにとってみれば，入手する情報が自然言語等で詳細に説明されていると，背景等を含めた内容を把握できるという利点がある．一方で，そのような形式で情報が表現されていると，情報システム・機器の管理者や利用者は，各機器に対してどのような対策を実行すべきか把握するのに時間を要する上，必要な対策を手動で実行することが必要となる．

以上に述べたことは，（株）日立システムズのCSIRTがソフトウェアの脆弱性，サイバー攻撃，およびそれらへの対策に関する情報を実際に収集し，関連する情報システム・機器管理者に対策を指示する局面においても，実際に直面している事項である．以下に，その一例，および感じている問題点について述べる．

- 情報の入手

[社外からの入手法]

CSIRTのメンバが，IntelGraph[5]☆2を中心に，サイバーセキュリティ情報を掲載しているさまざまな社外Webサイト（IPA[6]やJPCERT/CC4[2], [3]等の機関，セキュリティホールmemo[7]），Twitter，メールマガジン等を目視で確認．

[社内からの入手法]

情報システム・機器の管理者や利用者からの電子メールや電話等．

- 社内への情報の配信
  電子メールによる配信，社内ポータルへの掲示．

- 実感している問題点

[社外からの情報入手]

- 複数の情報源から情報を収集するため，その作業に要する工数が大きい
- 複数の情報源から情報収集をしているため，情報の関連性を人手で行わなければならない．
- 人手で情報を収集するため，収集される情報のレベルを一定に保てない（見逃し，出遅れを生じる）．

[社内からの情報入手]

- 電子メールや電話で情報を取得する形では，過去の経緯の追跡が困難，あるいは大きな工数を要する．
- 情報に触れる人間が限定的．多くの知見を結集することで，最適な対策法を決定するというアプローチが取れない．

[社内への情報の配信]

- 電子メールや電話を用いて，情報ごとに伝達する相手を変えて情報を伝えることが求められる場合があるのに対し，これを人手で行わなければならない．結果的に，配信が遅延する．
- 特に電子メールによって情報を伝達する場合，宛先誤りを犯す危険性がある．セキュリティに関する情報は機微情報も含む場合があるため，誤送信を行ってしまうと，大きな経営的問題となる場合がある．

以上に述べたような現場における経験も鑑みた上で，以下の章では，ソフトウェアの脆弱性，サイバー攻撃，および攻撃への対策に関する情報をCSIRTが適切に収集し，また各関係者と迅速に共有でき，その結果として被害を抑制できるようなICTシステム（以下ではシステムと略す）の特長について述べる．なお，上記における「情報の共有」とは，明らかに該当者間での情報を授受することだけを意味するものではない．同句は，ソフトウェアの脆弱性やサイバー攻撃に関する情報の共有であれば，たとえば，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までを，対策の情報の共有であれば，受信した複数の情報の中から優先的に実施すべき項目を，受信者が理解することまでを意味する．したがって，本システムの役割の正確な表現は，情報の共有を支援することである．

2. 情報共有を支援する既存のICTシステムとその課題

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）[8]が，サイバー犯罪に対抗するための国営のセンタである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することができる．一方，参加する組織や個人は，この仕組みを無料で利用することができる．

CiSPでは，SNSのような形で参加者が情報を登録・閲覧できるICTシステムが用いられている[9]．本システムに対しては，個々の参加者のほか，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．

CiSPで用いられているICTシステムでは，参加者は非定型な情報を登録することができる一方で，情報の共有を支援する目的で開発された他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）[10]形式で表現された指標[☆3]（インディケータ）を，Trusted Automated Exchange of Indicator Information（TAXII）[11]プロトコルで送信するAIS[12]と呼ばれる脅威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．STIXは，MITRE[13]が中心となり，サイバー攻撃の分析，サイバー攻撃を特徴づけるインディケータの特定，サイバー攻撃への対応の管理，サイバー攻撃に関する情報の共有等を，人手を介さずとも達成できるようにすることを企図して規定された仕様である．現在は，OASIS[14]によって管理されている．Version 1ではXML形式，Version 2ではjson形式で，サイバー攻撃活動，サイバー攻撃に関与している人・組織，インディケータ，脆弱性等を記述するよう規定されている．TAXIIはSTIX形式で記述された情報を交換することを1つの目的として規定された，標準化された通信プロトコルである．

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，特定のシステムの利用を強制しないという利点がある．一方で，一まとまりの情報だけから，その情報の背景や過去の経緯等を把握することはできない．また，あるIPアドレスやURLが割り当てられた機器との通信を遮断させるための設定をFirewallや制御機器にバッチ処理的に行うには，現状では設定する内容をXMLやjsonではなく，特定の形式（Yara Rule[15]はその一例）で与える必要があるものがほとんどである．したがって，STIX形式で記述された情報を各機器に対してそのまま送り込むことでは，対象の機器に対して上述のような設定変更は実現できないのが実情である．

3. サイバー攻撃に関連した情報を共有するのに有用なICTシステムの特性

第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，サイバー攻撃の特性，攻撃への対策の情報を，事業者内およ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．このような，規模や習熟度も多様あるいは不特定な者の間でこれを実現するには，情報の共有を支援する適切なシステムが存在することが望まれる．上記の類の情報は，自社で監視を行う中で把握する場合と，外部のセキュリティ関連情報収集機関やソフトウェア開発企業が発信する情報を受信することで把握する場合とがある．そこで以下では，まずこの2つの経路で情報を入手する場合の各々について，各機器に迅速に対策を行うまでに，上記システムに求められる特性について述べる．

3.1 自組織内で検出されたサイバー攻撃およびそれらへの対策に関する情報の共有

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，以下に挙げる部門によってなされているのが一般的である．

- 現場部門

  システムの管理，サイバー攻撃の監視，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）を行う．想定される者は，システム運用者，業務運用管理者等である．ここで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異なる．

- CSIRT
  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．ただし，実態としては，部署としてのCSIRTは設立されていても，十分な分析能力のある人員がいない事業者や組織も存在する．そのため，高い分析能力を持つ外部の機関やコミュニティと情報を交換するための仕組みが存在することが求められる．

- 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，事業継続管理（Business Continuity Management; BCM）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，攻撃が自社内の多くのシステムに影響を及ぼし，経営的観点からシステムの稼働継続あるいは停止を決定する必要がある場合は，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まとめて，経営層に報告する．経営層は，BCMの観点からサイバー攻撃を受けたシステムを稼働させ続けるか，あるいは停止させるかを決定し，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．以上に述べたことは、**図1**のように表現できる．

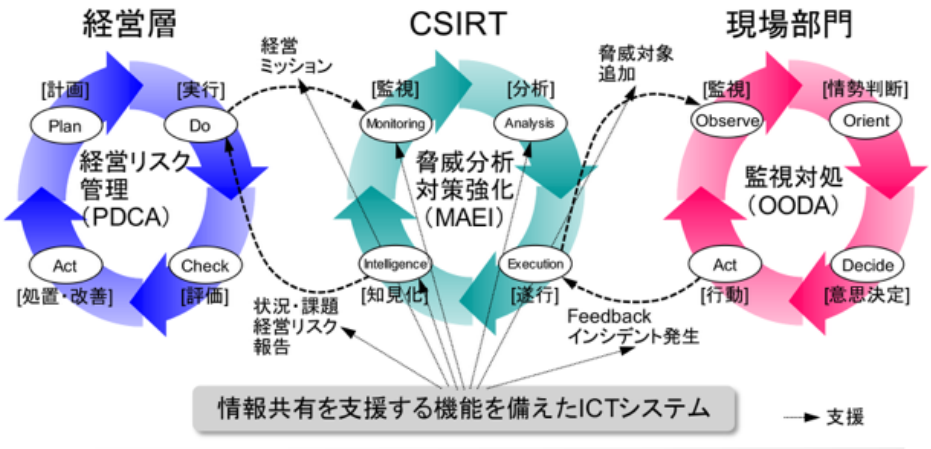

図1　事業者内で求められる作業および情報の共有とそれを支援するシステムの関係

図1に示した3つの部門間で行われる情報の伝達や，CSIRTが担う分析や知見化といった作業について，これらを支援する機能を備えたシステムが事業者内に存在すれば，サイバー攻撃の検知から対策の実施までに要する時間を短縮化することができ，その結果として事業者内で利用されていたり顧客へ提供したりしているさまざまなシステムを停止しなければならない事態に陥る可能性を低く抑えることが期待できる．

3.2　他組織から入手したサイバー攻撃，対策，ソフトウェア脆弱性等に関する情報の共有

ところで，第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が、近年は実際に発生している．したがって，自社内で検出した攻撃やそれらへの対策を自社内で共有する仕組みだけでなく，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る仕組みが整備されていれば，被害の抑制に有効であろうと考えられる．

一方で，同一分野内の事業者間だけでなく，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1つは，供給連鎖管理（Supply Chain Management）上の利点である．たとえば，情報通信分野に属する複数のプロバイダ事業者（An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，業務上必要な情報の送受信を行えなくなる状況も想定される．このとき，事業者An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は早期に対策を実行することができ，その結果上記のような事態に陥る可能性を低く抑えることができる．このような点から，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の情報のほか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，以下に述べるような組織の体系を整備した上で，各組織・事業者の間で，システムを利用して情報の収集および展開を行えるようにすることが望ましい．

- 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．この組織は，本システムを用いて，分野内の各々の事業者に，収集された（可能であれば分析や知見化も実行する）情報を展開する．ISAC[16], [17]は，このような役割を果たす組織の実例である．

- 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．この組織はある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は，各分野のISACに情報を展開するだけでなく，ISACが設立されていない分野については，直接事業者に対して情報を展開する．

ここで，情報を送受信・蓄積するために各組織や各事業者が導入するシステムは，目的や投じることができる費用に応じて決定されると考えるべきである．つまり，すべてが同じシステムを導入することを想定するのは非現実的である．このような状況においても情報を交換できるようにするためには，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，規定しておくことが必要である．第2章に挙げたSTIXおよびTAXIIは，このようなものの中で，すでに実際に利用されているものである．以上に述べたことをまとめると，**図2**のようになる．

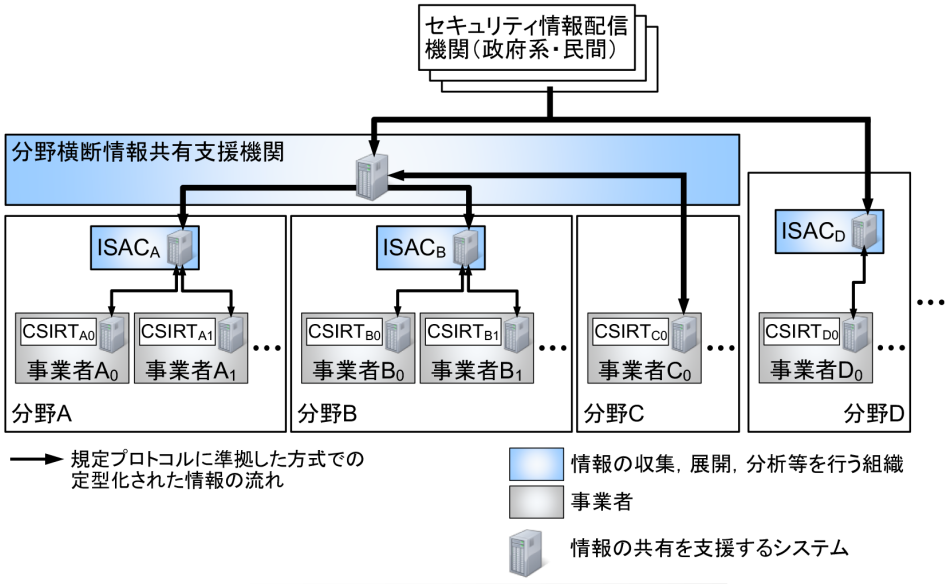

図2　組織と事業者の間で行われる情報交換

3.3　開発したシステムの特性と機能

第3.1節および第3.2節に述べた特性を鑑み，我々は**図3**，**表1**，**表2**に述べるような特性および機能を備えるシステムを開発，構築した．

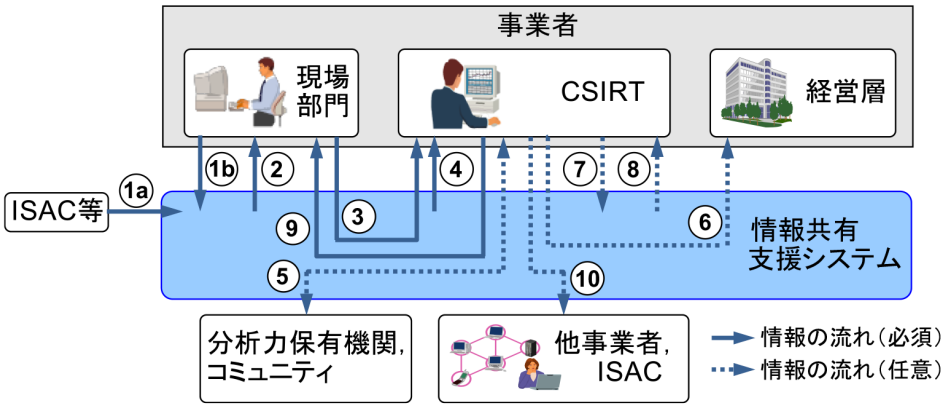

図3　情報の共有を支援するシステムを用いて交換される情報の流れ

表1　システムに対して入力，あるいはシステムから出力される情報と作業

役割	作業 No	作業の内容
ISAC 等	1a	収集したサイバー攻撃に関する情報の配信
現場部門	1b	検出したサイバー攻撃に関する情報の登録
	2	本システムに蓄積されている情報を調査し，対策の方法を検討
	3	2 において対策の方法を確定できなかった場合，検知した情報を CSIRT に通知し，対策方法の指示を依頼
CSIRT	4	現場部門から通知されたサイバー攻撃に関する情報を，本システムに蓄積されている情報等を用いて分析し，対策の方法を確定
	5	必要に応じて，他の分析力保有機関やコミュニティに分析を依頼，結果を受領
	6	経営への影響が懸念される場合等，必要に応じた経営層へ報告
	7	本システムに登録されている情報との関連付け，統合，重要度や ID の付与
	8	対策の実施状況の把握
	9	対策の方法の登録，現場部門への周知
	10	他の事業者や ISAC へのサイバー攻撃，対策の方法の展開

表2　情報の共有を支援するシステムが備えるべき機能☆4☆5☆6☆7☆8☆9

No	本システムが備えるべき機能	機能が有用な作業
1	迅速かつ正確に情報を登録できるようにする機能（例: 定型のフォーマットの表示）	1, 7
2	規定のプロトコルに沿って送信された定型形式の情報を受信し，解釈できる機能	1
3	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ようにする機能	2, 4
4	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）を安全に伝える機能 ☆4	3, 8, 10
5	報告をまとめる作業を支援する機能	6
6	新しい情報を，本システムに登録されている情報と関連付ける，同一の情報を統合する，各情報に重要度や識別子を付与する（あるいはそれを支援する）機能（例: 続報管理，重複情報排除)☆5	7
7	現場部門に指示を出すに当たり，登録されている情報から，重要度が高い順に，続報がある情報については最新のものを表示する機能	8
8	各機器への対策の実施状況を表示する機能☆6	8
9	機器への対策の実行を支援する機能 ☆7	9
10	情報の一部を秘匿する機能 ☆8	10
11	情報の送信先を限定する機能☆9	10

図3および表1は，システムに対して情報を入力あるいはシステムから情報を取得する者と，それらの者とシステムの間で交換される情報の流れ，および各者が行う作業の内容をまとめたものである．表2は，表1に記した作業を迅速に行えるようにするために，システムに搭載することが望ましい機能である．我々が開発したシステムも，機能項目5（報告をまとめる作業を支援する機能）が未完，機能項目6，7（情報の関連付け，統合，重要度付与とそれに基づく表示）が部分的である点を除き，本表にある機能を実際に実装した．2018年現在実際に検証に取り組んでいるところである．

図2のように事業者が外部の組織等から情報を入手する場合，自社内で検知したサイバー攻撃に関する情報の数と比べ，蓄積する情報の総量は，経験的には数倍から時には100倍を超える程度に達することが判明している．このような状況では，表2に挙げた機能のうち，機能項目3（目

的の情報の迅速な検索性），6（情報の関連付け，統合，重要度や識別子の付与），7（高重要度情報の優先表示），9（機器への対策の実行の支援）の重要性は，事業者内で検出されたサイバー攻撃に対応する場合と比較し，より高いといえる．

そこで，表2に挙げた機能の中で，我々が実装した関連情報表示機能の画面の一例を，**図4**に示す．上側がターゲットのある1つの情報を，下側が上側にある情報と関連する情報の一覧である．我々が実装したシステムでは，STIX形式で蓄積されている情報に関しては，ある1つの情報を選択した後，関連情報を表示するためのボタンを押すことによって，同図の下側にあるような形式で，当該情報と関連する情報の一覧を表示することができる．関連した情報には，図の左端にあるように，重複，関連度高，関連度低のいずれかの関連度が表示される．関連度は，定期的に以下の観点で分析を行うことにより，決定される．

図4　ある情報と関連する情報の表示実装例

[重複] 2つの情報が，以下2種のいずれかを満たす場合

- メッセージ同士のSTIX IDの値が一致する

- STIX IDの値以外の項目がすべて一致する

[関連度高] メッセージに含まれるSTIX ID以外のID値が，関連する情報のID値と一致する場合

[関連度低] IPアドレス，Hash値などのうちのいずれかが一致する場合

先に述べた通り，いまだ検証を実施している最中ではあるが，対策方法を迅速に検索できる機能，新たな情報をシステムにすでに登録されている情報と関連付けたり同一の情報を統合したりする機能，および各情報に重要度や識別子を付与する（あるいはそれを支援する）機能などは，情報の提供元が増え，システムに登録される情報の総数が増えた場合には，必須性が高いという意見，異なる組織・事業者の間で情報の拡散が進むためには，情報の一部を秘匿する機能や，情報の展開先を限定できる機能が必要であるという意見を検証実施者からいただいている．

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

第3章に述べたようなシステムを利用することによって，事業者内，および組織と事業者の間での情報の伝達や共有に要する時間の短縮化が図れるようになると，**図5**に示すような効果の連鎖を生み，最終的には発生する被害を抑制できると考えられる．

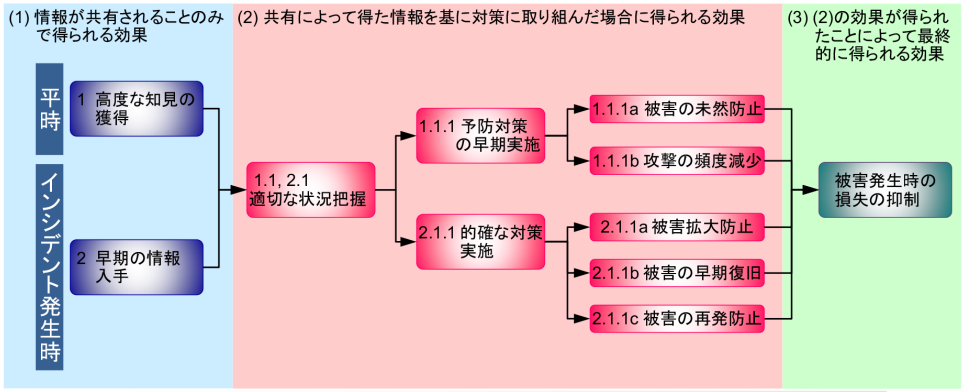

図5　情報共有および対策に取り組むことより事業者が得られると考えられる効果

すでに公知となっている通り，（株）日立システムズでは，2017年5月中旬に，ランサムウェアWannaCryによる被害を生じた[18]．一方，WannaCryが突くソフトウェアの脆弱性については，2016年後半から，関連する情報が徐々に公開されていた．このことから，本稿で提案したシステムを用いて事前に適切に情報が共有されていたと仮定すると，実際に生じた被害より被害を抑制できたと考えられる．左記のような観点から，**表3**では，本システムを用いて情報を適切に共有していた場合に推測される状況の変遷とそこで得られる効果について述べる．同表における括弧内の数字は，図5に示した効果の項目の番号を示している．

表3　本システムを利用してWannaCryに早期対処した場合の対応の流れと被害（推測）

時期	検知事象 及び 公的機関，ソフトウェア開発企業等が発した情報	システムを用いて行われる情報の共有，左記を受けての対応，及びその結果推測される効果
2016後半	Microsoft 社: SMBv1 の利用停止の推奨	CSIRT は，社内の現場部門に注意喚起（図 5 の(2)参照）
2017/3	Microsoft 社: セキュリティ情報 MS17-010 発行 IPA: Microsoft 製品の脆弱性対策について発信 JPCERT/CC: Microsoft セキュリティ情報に関する注意喚起	CSIRT は，SMBv1 の脆弱性は，早期の対応が必要であることを現場部門に通知すると共に，状況の把握に着手（図 5 の(2.1)参照）
2017/4/14	SMBv1 の脆弱性を突くエクスプロイト（EternalBlue）が公開	SMBv1 の脆弱性を突くエクスプロイトが発見されたことをCSIRT，現場部門間で共有した上で，本脆弱性についての感度を更に上げ，状況の完全な把握に努める（図 5 の(2.1) 参照）
2017/4/20頃	SMBv1 で利用されるポート(445)の悪用例が観測される（以後増加）	SMBv1 の脆弱性を狙う事例が観測されていることを CSIRT，現場部門間で共有し，機器への対策の実施を徹底 （図 5 の（1.1.1，1.1.1a）参照）
2017/4 末頃		CSIRT，現場部門の間で，機器への対策の実施状況を共有.
2017/5/12	WannaCry によるキャンペーン攻撃が開始されたことが検知される	対策が大部分の機器に対して実施されていることにより，生じる被害の極小化に成功.

前述の通り，表3に述べた状況の変遷は推測であるが，本システムを導入することによって，WannaCryによる攻撃が行われた日時より2週間程度前までに，事業者内に存在する各機器への対策の実施を完了できた可能性があると考えられる．その結果として，公表されているほどの被害を生じることはなかったであろうと推測できる．

5. まとめと今後の課題

サイバー攻撃による被害を抑制するには，サイバー攻撃，被害状況，攻撃への対策，ソフトウェアの脆弱性等の情報を，CSIRTを中心として事業者内で迅速に共有できることが求められる．また，これを実現するためには，ソフトウェア開発企業や国内外の情報収集機関等が発信するソフトウェアの脆弱性やサイバー攻撃，およびそれらへの対策に関する情報をCSIRTが入手し，情報を整理した上で，必要なものを，自事業者内や下位の組織・事業者等に展開できる必要がある．

このような観点から，本稿では，上記作業をCSIRTがより迅速に遂行できるようにするのに有効なICTシステムの特性，機能を実際の経験を基に検討し，実装した．本システムの有用性についてはいまだ検証中ではあるが，搭載した機能の中でも，対策方法を迅速に検索できる機能や，新たな情報をシステムにすでに登録されている情報と関連付けたり同一の情報を統合したりする機能，および各情報に重要度や識別子を付与する（あるいはそれを支援する）機能などは，情報の提供元が増え，システムに登録される情報の総数が多い場合には必須性が高いこと，また，異なる組織・事業者の間で情報の拡散が進むためには，情報の一部を秘匿する機能や，情報の展開先を限定できる機能は必要であるとの意見をいただいている．

上記について述べた後，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もたらされる効果の連鎖と，最終的な効果として被害の抑制が期待できることを述べた．

今後は，本稿で提案したシステムをより広範な情報配信機関や事業者でさらに運用していただき，改善点の明確化や推測した効果の検証に取り組む予定である．

謝辞　本研究の一部は，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）Microsoft：セキュリティ TechCenter,
https://technet.microsoft.com/ja-jp/security/bulletins.aspx
2）JPCERT/CC：注意喚起,
https://www.jpcert.or.jp/at/2017.html
3) JPCERT/CC： 早期警戒情報,
https://www.jpcert.or.jp/wwinfo/
4）日経コンピュータ：攻めの防御 サイバーインテリジェンス，pp.20-37（2016年6月9日号）
5）Accenture Security：iDefence IntelGraph,
https://intelgraph.idefense.com/#/login
6）独立行政法人 情報処理推進機構：重要なセキュリティ情報一覧,
https://www.ipa.go.jp/security/announce/alert.html
7）セキュリティホールmemo，https://www.st.ryukoku.ac.jp/~kjm/security/memo/
8）National Cyber Security Center：Cyber Security Information Sharing Partnership，https://www.ncsc.gov.uk/cisp
9）Surevine，https://www.surevine.com/threatvine/
10) Structured Threat Information eXpression，https://stixproject.github.io/
11) Trusted Automated eXchange of Indicator Information，https://taxiiproject.github.io/
12) Department of Homeland Security; Automated Indicator Sharing，https://www.dhs.gov/ais
13）MITRE，https://www.mitre.org

14）OASIS，https://www.oasis-open.org/
15）YaraRules Project，http://yararules.com/
16）一般社団法人 金融ISAC，http://www.f-isac.jp/
17）一般社団法人 ICT-ISAC，https://www.ict-isac.jp/
18）日経XTECH：日立のセキュリティ担当、WannaCry感染の反省を語る，http://tech.nikkeibp.co.jp/it/atcl/news/17/112102710/
19）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2017」報告書について，https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html

脚注

☆1　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[19]．
☆2　脆弱性，マルウェア等のファイル，攻撃に利用されるURLを中心に，契約締結者に対して，ブラウザで閲覧できる形で，サイバー攻撃に関連する多種の情報を提供するサービス．契約の内容によっては，APIを利用して，プログラムを用いてデータを取得することもできる．
☆3　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．
☆4　情報の閲覧者が分析に必要な情報に触れた場合でも，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ため．
☆5　ここに記載した処理をシステムが自動的に実行できれば理想的であるが，最終的な判断をCSIRTが下すのが現時点では実際的である．
☆6　本情報に基づいて，対策が未完の機器への対策の実施を，CSIRTが現場部門に要請できるようにするため．
☆7　ある特定のIPアドレスからのアクセスをブロックするような対策を各機器に対して行う場合，その規則を記述したコードを生成する機能はその一例である（第2章に述べたYara Rule は，そのような記述形式の一例）．
☆8　自社において攻撃が検出されたことについては他組織へ公開することを望まない場合等は，本機能が求められる．
☆9　情報の内容により，特定の組織にのみ提供することを希望する場合は，本機能が求められる．

平井 達哉（非会員）tatsuya.hirai.cf@hitachi-systems.com
1992年早稲田大学理工学部物理学科卒業，1994年同大学院理工学研究科修士課程修了．1994年（株）日立製作所 システム開発研究所入社．以後，同研究所，同社中央研究所等において，磁気記録用低誤り率ブロック符号化・復号化，コンテンツ保護を目的とした公開鍵暗号基盤，鍵交換プロトコル，ファイル管理方法，コールドストレージシステム向け分散ファイルシステム等の研究開発，規格化等に従事．2008年京都大学大学院情報学研究科単位認定退学．2016年（株）日立システムズ入社．現在，本稿に記載した情報共有支援システムの開発プロジェクトのリーダーを担当．IEEE，電子情報通信学会各会員．京都大学博士（情報学）．

本川 祐治（非会員）yuji.motokawa.qz@ hitachi-systems.com

1985年（株）日立情報ネットワーク（現（株）日立システムズ）入社．メインフレームのシステム運用の開発，社内SOC立ち上げ（SOC長），緊急即応（CSIRT長），セキュリティリサーチセンタ（センタ長）等の業務に従事．本稿の内容に関しては，情報共有支援システムの開発プロジェクト統括責任者として，開発の方向性，システムの基本構成等の決定に寄与．ISACA東京支部理事・副会長，JNSA幹事，NISC・PA等の委員会委員．CISA，CISSP，RMCA（非会員）．

佐々木 慎一（非会員）shinichi.sasaki.qh@ hitachi-systems.com
1997年東京理科大学理工学部情報科学科卒業．同年（株）日立情報ネットワーク（現（株）日立システムズ）入社．以後，（株）日立製作所 システム開発研究所等において，リスク分析，アクセス制御方式の研究，およびセキュリティ診断，コンサルティング等の業務に従事した後，現在はCSIRT業務に従事．本稿の内容に関しては，CSIRTの観点から，情報共有支援システムに望まれる機能，および情報共有支援システムがあった場合に実行できると推測される事前対処施策の明確化に寄与．技術士（情報工学）．

丹京 真一（非会員）shinichi.tankyo.xh@ hitachi-systems.com
1997年京都大学工学部電子工学科卒業．同年（株）日立情報ネットワーク（現（株）日立システムズ）入社．以後，同社において，脆弱性情報やマルウェア情報の分析，セキュリティインシデント対応等の業務に従事．本稿の内容に関しては，セキュリティインシデント対応によって得た知見，および近年のマルウェアの特性の傾向等の観点から，情報共有支援システムに望まれる機能の明確化に寄与．フィッシング対策協議会運営委員．APWG（Anti-Phishing Working Group）日本代表．

投稿受付：2018年2月15日
採録決定：2018年3月22日
編集担当：平林元明（（株）日立製作所）