重要インフラ事業者向けサイバー攻撃関連情報共有システムの提案

平井 達哉[1]　関口 悦博[1]　角田 朋[1]　佐々木 慎一[1]　光武 健二[1]　本川 祐治[1]　丹京 真一[1]

概要：近年，サイバー攻撃が高度化し，人々の生活が脅かされる事態を生じる可能性が高まってきている．このような事態を生じさせないためには，サイバー攻撃やそれらへの対策に関する情報の組織，分野を越えた迅速な共有が必要である．それらの情報を共有する際には，固有情報の秘匿処理，共有範囲の設定，複数の情報の統合や分割，情報の重要度の可視化等を行う必要がある．一方で，従来の情報共有手段では，先に挙げたような処理を人為的に行う必要があるため，迅速に情報を共有することが困難である．そこで我々は，発生したサイバー攻撃やそれらへの対策等に関する情報を，組織の内外で迅速に共有することができる，タイムラインおよびSTIX/TAXIIを利用した情報共有システムを考案し，そのプロトタイプを開発した．

キーワード：サイバー攻撃，情報共有システム，タイムライン，STIX，TAXII

Proposal of a system to share cyberattack-related information for leading infrastructure providers

Tatsuya Hirai[1]　Yoshihiro Sekiguchi[1]　Tomo Kakuta[1]　Shinichi Sasaki[1]　Kenji Mitsutake[1]
Yuji Motokawa[1]　Shinichi Tankyo[1]

Abstract: Recently, cyber-attacks have advanced and the probability that people's life are threatened have increased. To prevent such situations, it is necessary to share information on cyber-attacks and countermeasures to them rapidly. When sharing such information, it is necessary to conceal some elements of the information, set the range to share information, integrate multiple information or divide the information, visualize the importance of the information, and so forth. On the other hand, in conventional measures, it has been difficult to share such information rapidly because it is necessary to do it manually. Therefore, we have devised a system to share information on cyber-attacks, and countermeasures to them, and so forth rapidly using timeline and STIX/TAXII among different organizations, and developed a prototype of the system.

Keywords: cyber-attacks, information sharing system, timeline, STIX, TAXII

1. はじめに

従来，サイバー攻撃は，広範囲にまたがる攻撃であっても，手法は均一ものが主であった．したがって，異なる組織においても同一の対策手法を採用することで，多くの場合被害を抑えることができた．ウイルス対策ベンダが，特定のウイルスへの対策手法をWebサイトに公開し，各組織はそれに沿った行動をするというのは，その一例である．また，対策の実施指示やその結果の管理も，メール等で通知することで時間的に問題は無かった．

一方近年は，標的型攻撃に代表される局所的な攻撃が増えてきた．局所的な攻撃では，組織ごとに攻撃の手法が異なる場合が多い．左記のような攻撃が行われた場合には，複数の組織が特定の対策手法に沿った対策を講じるだけで

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

は，被害を極小化することは多くの場合困難である．特に，左記の攻撃が重要インフラ事業者に対して行われると，それが人々の生活に与える影響は非常に大きいと考えられる．このような観点から，一組織内での情報共有だけでなく，異なる組織間で攻撃や脅威，および被害の情報を迅速に共有し合えるような情報共有プラットフォームを整備することの有用性は，今後より高まってゆくと考えられる．実際，平成 27 年 9 月に閣議決定された「サイバーセキュリティ戦略」においても，重要インフラをサイバー攻撃から守るために「効果的かつ迅速な情報共有の実現」が項目として掲げられている [1].

2. 関連技術と課題

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プラットフォームは，いくつか存在する．日本においては，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）[2] がある．J-CSIP 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．本仕組みは，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の被害が検知されると，当該組織は IPA にその情報を送信する．IPA は，情報提供元等の情報の匿名化および分析情報の付加後，情報提供元の承認を得た上で，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 に対してフィードバックする．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．この仕組みは，人手による作業も含むため，情報の共有には一定の時間を要する．

他国において実運用されているプラットフォームとしては，Soltra Edge [3]，Threatvine [4] が挙げられる．Soltra Edge は，Structured threat information expression（STIX）[5] で脅威情報を表現し，それをデータベースに格納，また当該情報を Trusted automated exchange of indicator information（TAXII）[6] に従って他の脅威情報共有システムとの間で送受信し合うことができるシステムである．TAXII に従って情報の送受信ができるため，他のシステムとの情報の共有を図りやすいという利点がある．しかし，脅威情報は STIX で記述することを前提としているため，ユーザーによるコメントの追加，およびその脅威情報への迅速な反映という点に関しては，十分なサービスの提供が困難である．一方 Threatvine は，タイムラインをベースとした脅威情報の共有システムである．そのため，システムの利用者によるコメントや情報の追加が容易であるという利点があるが，他のシステムとの間で脅威情報を送受信し合い，これを共有するということはできないという短所がある．

以上に記載したような各システムの長所，短所を鑑み，我々は新たなサイバー攻撃やそれらへの対策方法等の情報を共有するシステムのプロトタイプを開発した．次章以降では，その特性について述べる．

3. 重要インフラ事業者を中心とした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ための仕組み

3.1 共有・連携すべき情報

サイバー攻撃や左記攻撃に対する対策の情報を展開することの目的は，各事業者がそれらの情報を把握し，対策を実際に実行できるようにすることである．そのような観点から考えると，少なくとも以下のような情報を共有できると，被害を抑制に有効であろうと考えられる．

(1) 攻撃（疑義）情報，脅威情報
　重要インフラ事業者に対して現在行われているサイバー攻撃情報．試行中の攻撃も含む．
(2) 緊急対策情報
　重要インフラ事業者に対して現在行われているサイバー攻撃に関する，緊急の対策情報．特定の攻撃元 IP アドレスのブロック要請情報は，その一例である．
(3) 脆弱性情報
　最新の脆弱性に関する情報．
(4) 攻撃予告，早期警戒情報
　サイバー攻撃予告や，サイバー攻撃に関する早期の警戒情報．
(5) ベストプラクティス情報
　各事業者における対策事例情報．特定のサイバー攻撃に対する対策手法だけでなく，攻撃を防ぎつつ実運用にも耐えうるシステムの構成情報や運用方式等も含む．

3.2 情報共有システムが備える機能

本節では，まず，前節に記したような情報を異なる分野に属する複数の重要インフラ事業者間で共有するために必要な組織構成を想定する．各事業者には，事業者内のコンピューターやネットワーク上でセキュリティに関する問題が発生していないか監視すると共に，万が一そのような問題が発生した場合には，その原因の解析，影響範囲の調査，脅威を除去するための対策手段の展開等を行う部門が存在することを想定する．Computer Security Incident Response Team（CSIRT）は，そのような部門の一例である．

重要インフラ関連の事業者に対しては，特定の一つの事業者だけでなく，ある分野に属する複数の事業者に対して，一斉に攻撃が行われることも想定される．このような攻撃やそれらへの対策手段は，同一分野内の他の事業者とだけ

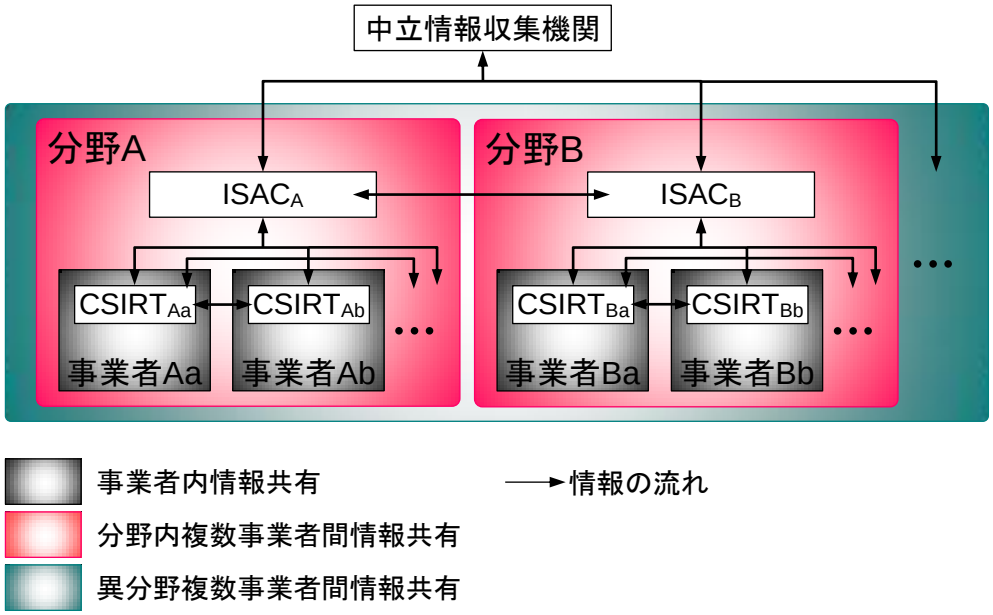

図 1　分野内および異分野の複数事業者間で情報を共有する際の情報の流れ

Fig. 1　Flows of the information when it is shared among providers in a field or some fields.

でなく，他の分野に属する事業者とも迅速に共有できる状態が望ましいと考えられる．また，上記の類の情報を，それらを収集する中立的な組織（国家機関等）から複数の分野に属する事業者に一斉に展開することが求められる場合があると考えられる．このような情報共有を迅速に達成するには，各分野に，共有対象の情報を収集および展開する組織が存在することが望ましい．このような役割を担う組織は，分野によっては既に設立されている．Information Analysis and Sharing Center（ISAC）は，その一例である．

以上に述べたような情報共有の描像を図示すると，**図 1** のようになる．

図 1 に示したような情報の共有を行うために，各事業者や ISAC は，**図 2** に示す処理を実行する．

[事業者 Aa 内で実行される処理]

Step 1: 自社内のシステムについて，サイバー攻撃が行われたかどうかを常時監視する．

Step 2: 監視の結果何らかの異常を検知した場合には，自社内のシステムへの影響を調査し，それへの対応の緊急度を評価する．

Step 3: Step 2 における判断の結果，緊急性が高いと判断されたものから優先的に対応策を講じる．

Step 4: 行われたサイバー攻撃，それへの対応策等の得た知見の中から，分野内の他事業者へ公開する情報を取捨選別する．

Step 5: 分野内他事業者および ISAC へ，情報を展開する．

[$ISAC_A$ 内で実行される処理]

Step 2 における影響調査の対象が分野内であること，Step 3 がないこと，Step 4 および Step 5 における公開先対象に他 ISAC も含まれることを除き，事業者 Aa 内での処理と同じ．

[事業者 Ab 内で実行される処理]

Step 1, 2, 3 については，事業者 Aa 内での Step 1, 2, 3 と同じ．新たに何か知見が得られた場合は，Step 4 において，それらを事業者 Aa や $ISAC_A$ に対して通知する．

以下では，**図 3** に示した情報共有システムの特徴について説明する．

システムは，前節に示したような情報を各事業者内で共有する手段として，以下に挙げる 3 種類の情報の入力，表示，蓄積，送受信機能を備える:

(1) ある事業者に所属する人員間で情報を共用するための情報表示・追加機能

(2) ある事業者に所属する人員が，同一分野の他の事業者や ISAC の人員と情報を共有するための情報表示・追加機能

(3) 中立的な情報収集機関から，ISAC 等の中間的な情報収集機関を介して展開される情報を表示したり，新たに得た情報を中間的な情報収集機関に通知したりする機能

機能 1 は，“タイムライン”によって実現するのが適当である．このタイムラインには，事業者 Aa の $CSIRT_{Aa}$ の他，Aa の運用部門の人員も閲覧およびコメントの書き込みができるようにする．前節に挙げたような情報の展開を E メールや FAX で行う場合には，展開を担当している者が置かれている状況によっては，情報を迅速に展開することが困難な場合もあると考えられる．一方で，タイムラインで情報を提示する形にすれば，情報投稿者と閲覧者は多

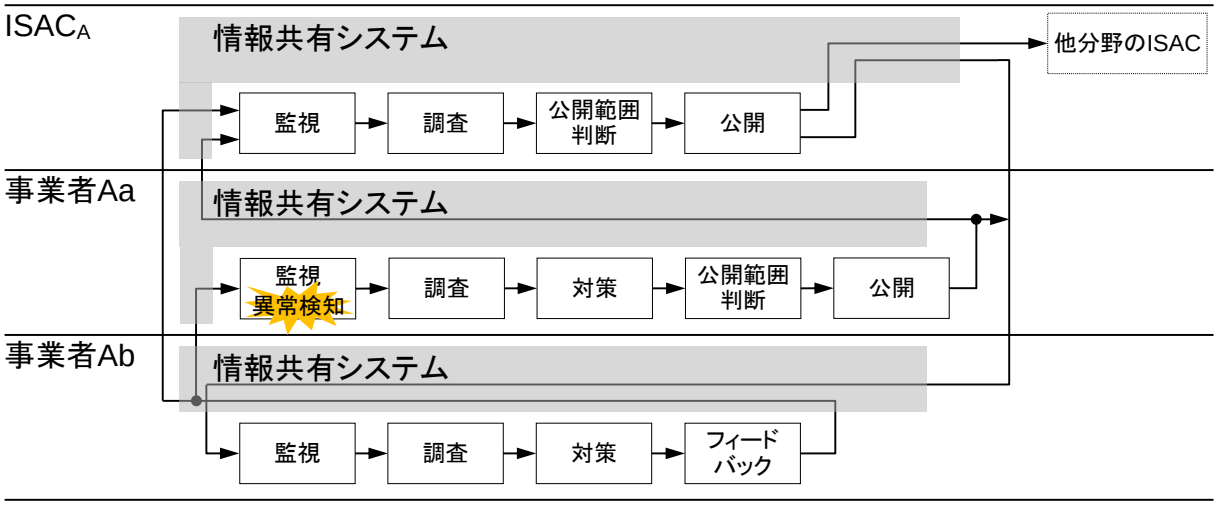

図 2　情報共有システムを用いて複数の事業者間で情報を共有する際に各組織で実行される処理

Fig. 2　Processes executed in providers when the information is shared among them using the system

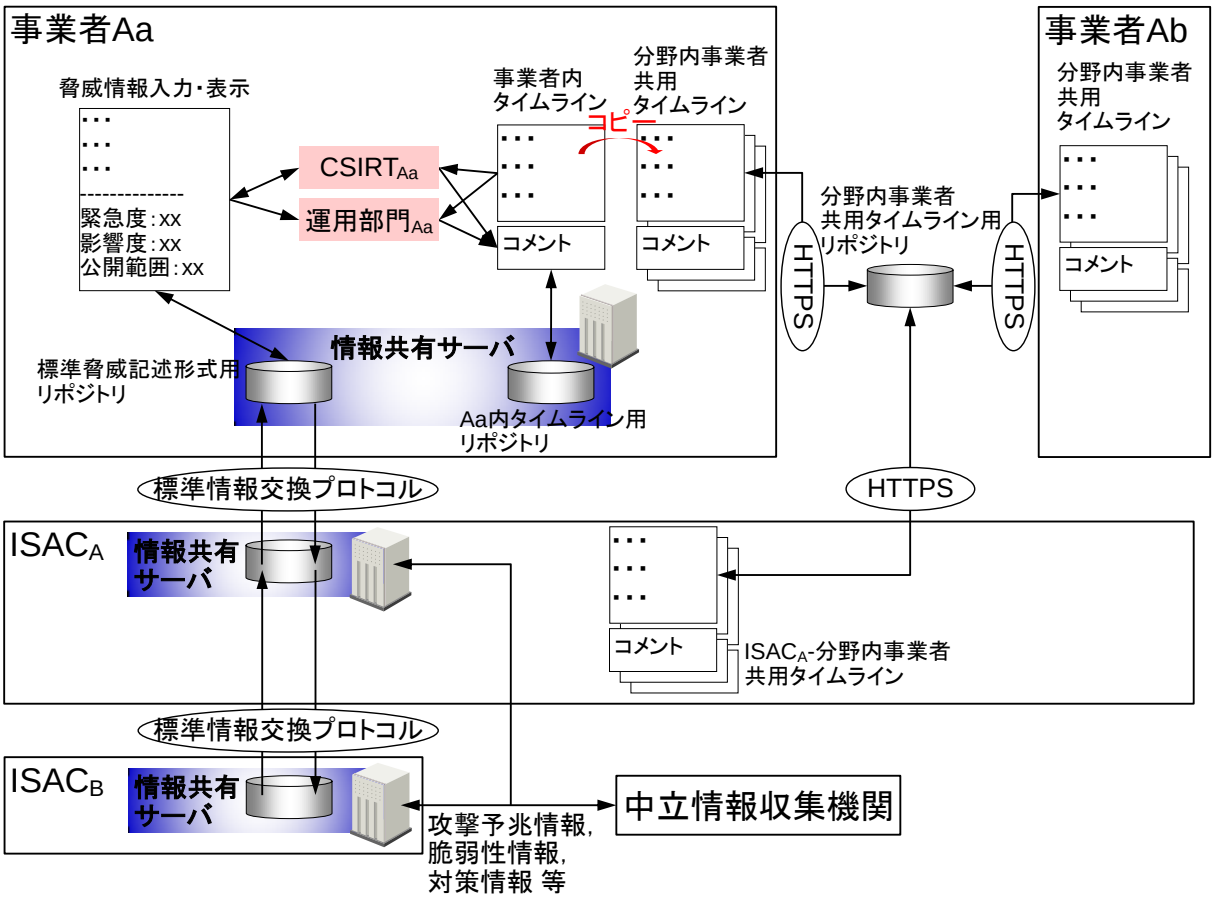

図 3　システムが備える情報の入力，表示，蓄積，送受信機能

Fig. 3　Functions to input, indicate, store, and transmit/receive the information which the system has

対多の関係となることから，そのような事態を回避できる可能性がより高くなると考えられる．

機能 2 も，機能 1 同様に“タイムライン”によって実現するのが適当である．E メール等ではなくタイムラインによって情報を共有する場合の利点は，機能 1 の場合と同じである．情報を他事業者等と共有する場合，共有対象者および共有する情報のいずれも，ターゲットとする情報によって異なると考えられる．そこで，タイムラインを作成した事業者 Aa 内の人員は，初めにこのタイムラインを共有する対象を設定することができるようにする．分野 A 内

の事業者の場合，共有対象者として選択できるのは，分野 A 内の他事業者および $ISAC_A$ とする．事業者 Aa の人員は，Aa 内共有用タイムラインに投稿された情報を，このタイムラインにコピーできるようにする．この時，作業者は，情報を共有する相手事業者に公開する情報を，コピー元の情報から適宜取捨選択できる．また，共有する情報の保存先は，全ての事業者から中立な場所に配置し，蓄積先に保存された情報へのアクセス権は，全ての事業者に対等であるようにする．

機能 3 は，国家機関等の中立的な情報収集機関から展開された情報を各事業者内の人員が閲覧したり，各事業者において得られた知見を当該機関に対して通知したりするためのものである．このような情報は，多くの事業者が等しく解釈できる形態であることが望ましいことから，脅威・対策手段等を表現するための標準化された記述形式で表現されていることが想定される．STIX は，そのようなものの代表例である．各事業者には，機能 1 で共有される情報の蓄積先とは別に，左記のような形式で表現された情報の蓄積先を設けられる．また，上記と同様の理由により，このような情報は，標準化されたプロトコルに沿って事業者-ISAC 間等を転送されると考えられる．TAXII は，そのような目的で開発された情報交換手順の代表例である．以上のような理由から，情報共有サーバーは，標準化された記述形式で表現された情報を標準化されたプロトコルに沿って情報を送受信する機能も備えることとする．

4. 分野内複数事業者間での情報共有の例と本システムの有用性の確認

本章では，事業者 Aa でサイバー攻撃を検知した後，3.2 節に述べた特徴を備えたシステムを用いて左記の情報を他事業者 Ab と共有するまでのシーンを想定する．

- 想定シーン
  - 分野 A: 電力業界
  - 電力会社 Aa がサイバー攻撃を受ける．その結果，Aa 社が保有・管理する太陽光発電システムに異常が発生する．
  - 電力会社 Aa は，上記情報を検知，当該情報を別の電力会社 Ab および $ISAC_A$ と共有する．
  - $ISAC_A$ から同分野内の各事業者に対し，本攻撃情報を展開，対応を依頼する．
- シーンの推移

  第 1 段階（**図 4**）: 情報を共有するグループの選択

  第 2 段階（**図 5**）: 事業者 Aa が把握したサイバー攻撃情報を事業者 Ab と共有

  第 3 段階（**図 6**）: 入手したサイバー攻撃情報の事業者 Ab 内での展開

  第 4 段階（**図 7**）: 分野 A 内 $ISAC_A$ から同分野内各事業者への状況確認依頼

以上の考察から，開発したシステムは，上記のようなシーンにおいて複数事業者間で迅速な情報共有を図るのに，有効であると考えられる．

5. まとめと今後の課題

分野内外を問わず，複数の事業者間でサイバー攻撃やそれらへの対策方法等を迅速に共有するためのシステムを開発し，同システムが備える情報の入力，表示，蓄積，送受信機能の特性について述べた．続いて，同一分野内の 2 つの事業者が本システムを用いて情報を共有するシーンを想定し，両者が迅速に情報を共有するのに本システムが有効であると考えられることを示した．今後取り組むべき事項は，できるだけ広範な分野の事業者が本システムを用いて実際に情報を共有する場合に生じる問題点を明らかにすること，それらの解決方法を考案しシステムを開発すること，およびその有効性を定量的に提示することである。

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] 内閣サイバーセキュリティセンター, “サイバーセキュリティ戦略”, http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf（参照 2016 年 8 月）
[2] 情報処理推進機構 サイバー情報共有イニシアティブ, https://www.ipa.go.jp/security/J-CSIP/（参照 2016 年 8 月）
[3] Soltra, https://soltra.com/（参照 2016 年 8 月）
[4] Surevine, https://www.surevine.com/threatvine/（参照 2016 年 8 月）
[5] Structured Threat Information eXpression, https://stixproject.github.io/（参照 2016 年 8 月）
[6] Trusted Automated eXchange of Indicator Information, https://taxiiproject.github.io/（参照 2016 年 8 月）

図 4　情報共有システムを用いて同一分野内の 2 つの事業者間で情報を共有する際の処理：第 1 段階

Fig. 4　Processes executed to share the information using the system among two providers in a field: Phase 1

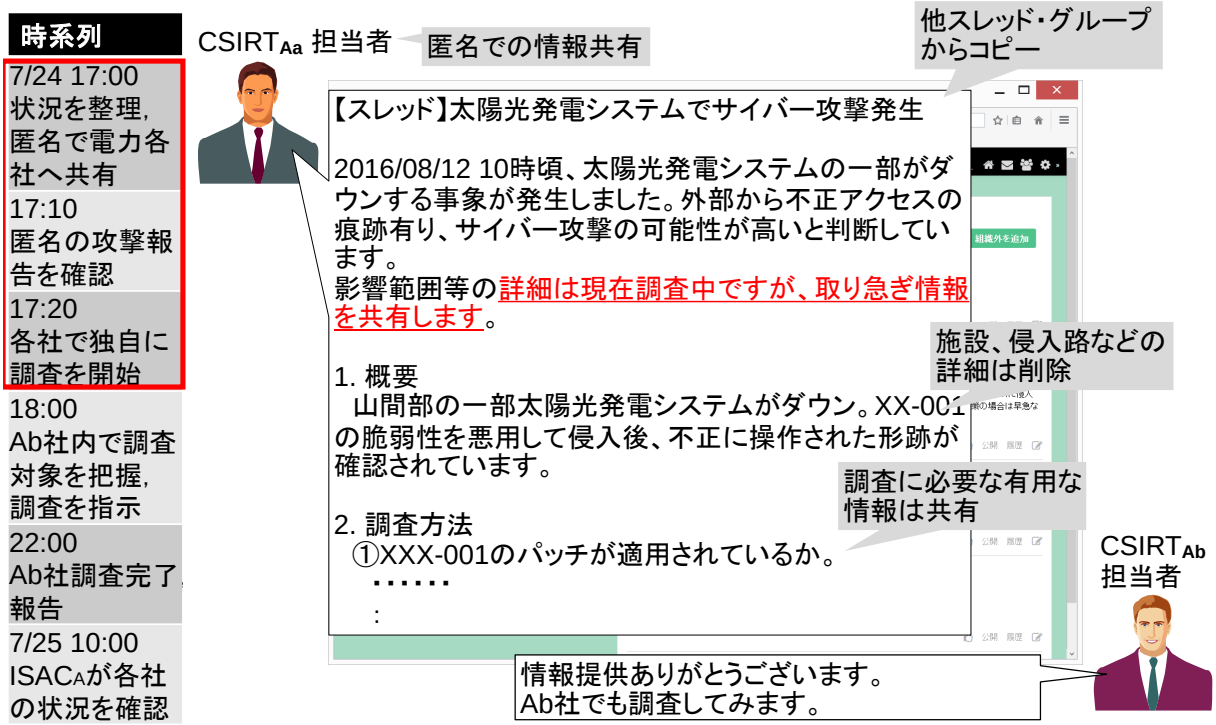

図 5　情報共有システムを用いて同一分野内の 2 つの事業者間で情報を共有する際の処理：第 2 段階

Fig. 5　Processes executed to share the information using the system among two providers in a field: Phase 2

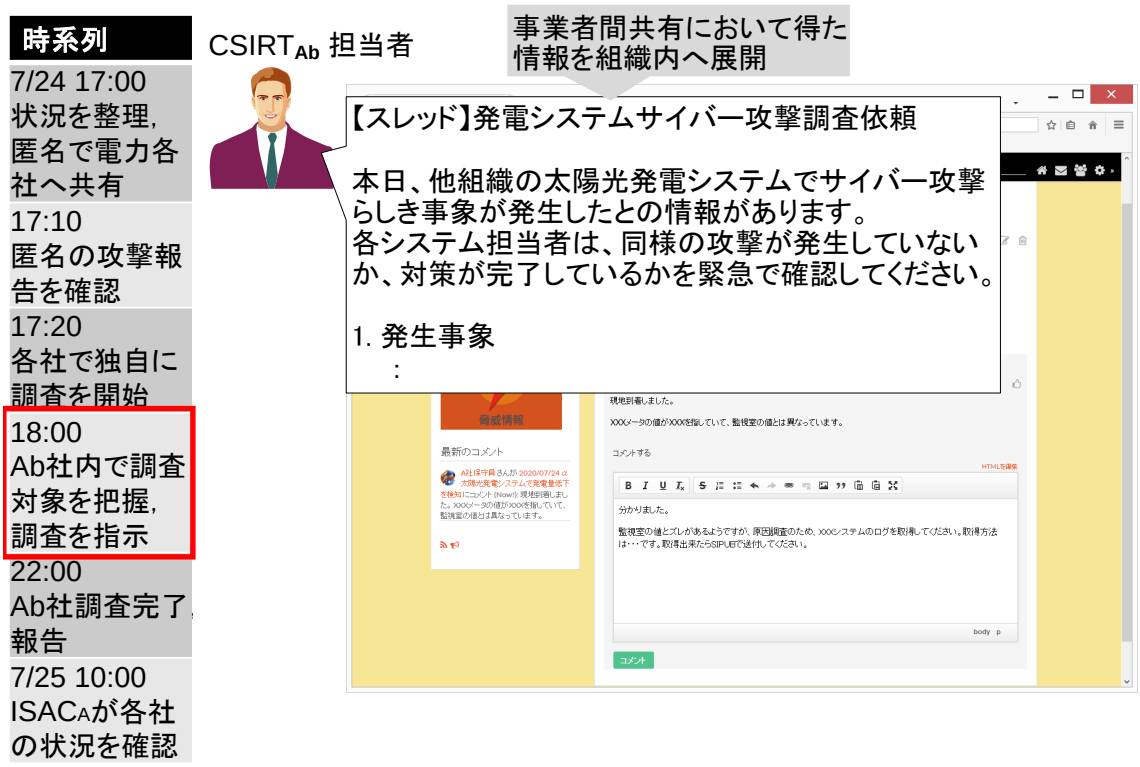

図 6　情報共有システムを用いて同一分野内の 2 つの事業者間で情報を共有する際の処理：第 3 段階

Fig. 6　Processes executed to share the information using the system among two providers in a field: Phase 3

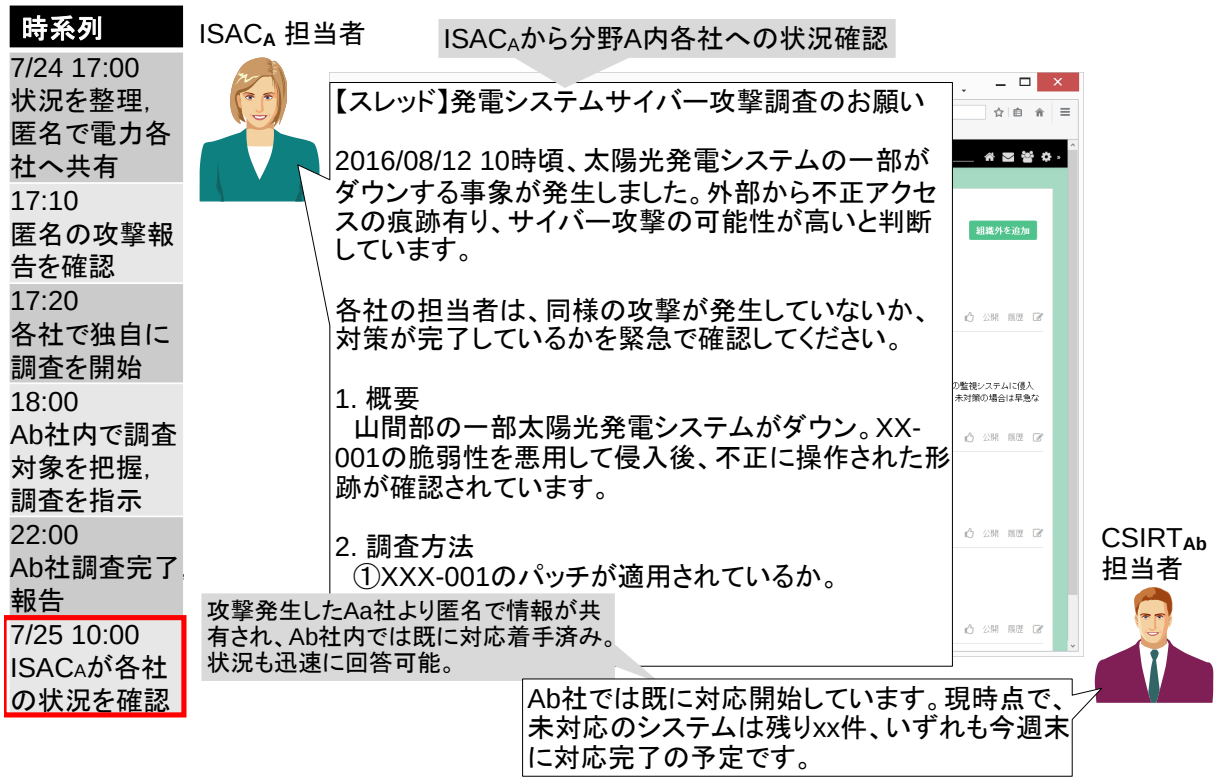

図 7　情報共有システムを用いて同一分野内の 2 つの事業者間で情報を共有する際の処理：第 4 段階

Fig. 7　Processes executed to share the information using the system among two providers in a field: Phase 4