資料 12-２

平成 31 年４月 18 日

内閣サイバーセキュリティセンター

重要インフラ事業者等との情報共有に関する手引書（骨子案）

「資料 12　情報共有体制の改善の具体策について（案）」において、重要インフラ事業者等が情報連絡の具体的な手順や解説についてしっかりと把握できていない現状を解決するため、情報連絡を行うに当たっての解説書として「重要インフラ行動計画に基づく情報共有の手引き試行版（仮称）」（以下、「情報共有の手引き」という。）を作成することとした。

情報共有の手引きにはサイバーセキュリティ基本法をはじめとした根拠、記載すべき内容の解説、具体的な内容、様式等を掲載し、重要インフラ事業者等及び重要インフラ所管省庁が情報連絡を行う際に必要な情報を網羅したものとする。

また、併せて情報提供に関しての解説等も掲載することにより、情報共有全体についてまとめた一冊とする。

具体的な記載事項は次ページのとおり。

情報共有の手引き構成（案）

Ⅰ　まえがき

サイバーセキュリティ基本法、重要インフラの情報セキュリティ対策に係る第４次行動計画等に触れつつ、情報共有の目的等を記載。

Ⅱ　情報共有体制の全体像

①対象とする情報の範囲と原因

情報共有を行う対象範囲の説明：重要インフラサービス障害等を含むシステムの不具合や予兆・ヒヤリハットに関する情報（以下「システムの不具合等に関する情報」という。）すなわち「重要インフラサービス障害」、「システムの不具合」、及び「予兆・ヒヤリハット」

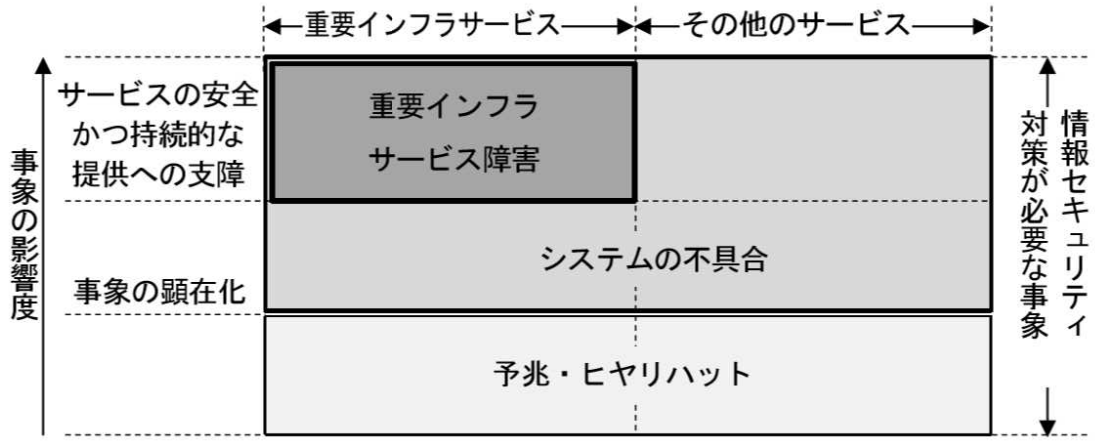

図　情報共有の対象範囲

②共有された情報の活用

・セプター、重要インフラ事業者等への参考情報の提供

重要インフラ事業者等のサービスの維持・復旧に資するための参考情報として統計化する等し、セプターや重要インフラ事業者等に対して提供。

・行動計画の検証・確認における活用

NISC は、行動計画で示されている重要インフラ事業者等の対策及び行動計画の施策の確認・検証において活用

③情報共有体制

・秘匿性の確保

共有する情報は、機微情報を含むことから、情報共有に際して秘匿性を確保する。共有された情報は、付番、公開範囲等に基づき体系的に管理・保存し、必要な時にいつでも参照できるようにする。

・情報共有の方法

情報共有の方法は、電子メールを基本とする。FAX 及び電話も使用可。

④情報連絡

情報連絡の記載内容、流れを記載

⑤情報提供

情報共有の記載内容、流れを記載

Ⅲ　インシデント対応に資する情報等

①参考事項

平素から確認すべき事項（ベンダーのアップデート情報等）を紹介

②情報連絡の際に注意すべき事項

検体の送付方法等を記載

□警報　□注意喚起　□参考情報

（重要インフラ所管省庁→内閣官房）

情報連絡様式

（第　　報*）

（*が付与された項目は必須事項）

識別番号* （※第1報の識別番号は空欄）

情報連絡日時* 平成　　年　　月　　日

情報連絡元*	省庁名：		担当者名：	
	部局名：			
	電話番号：		FAX番号：	
	電子メールアドレス：			
情報共有範囲*	□Red = 宛先限り （NISC重要インフラ防護担当(※1)限り） □Amber=特定分野・関係者限り （NISC重要インフラ防護担当(※1)並びに直接関係する分野の重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者のうち、関係者限り） □Green=重要インフラ関係主体限り （NISC、重要インフラ所管省庁、事案対処省庁、情報セキュリティ関係省庁、防災関係府省庁、情報セキュリティ関係機関、オリパラ関係組織、サイバー空間関連事業者及び各分野のセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者限り） □White=公開情報			
	特記事項：			

※1：情報の集約・分析のため、必要に応じ、あらかじめ連携を要請した情報セキュリティ関係機関との間で情報共有を行う。

①発生した事象の分類 （別紙2参照）

事象の類型		事象の例	チェック（1つのみ選択(※2)）
未発生の事象		予兆・ヒヤリハット	□
発生した事象	機密性を脅かす事象	情報の漏えい （組織の機密情報等の流出など）	□
	完全性を脅かす事象	情報の破壊 （Webサイト等の改ざんや組織の機密情報等の破壊など）	□
	可用性を脅かす事象	システム等の利用困難 （制御システムの継続稼働が不能やWebサイトの閲覧が不可能など）	□
	上記につながる事象(※3)	マルウェア等の感染 （マルウェア等によるシステム等への感染）	□
		不正コード等の実行 （システム脆弱性等をついた不正コード等の実行）	□
		システム等への侵入 （外部からのサイバー攻撃等によるシステム等への侵入）	□
		その他	□

※2：最初に検知した事象を1つのみ選択する。
※3：機密性・完全性・可用性を脅かす事象までには至らないものの同事象につながり得る事象。

②上記事象における原因の分類 （別紙2参照）

原因の類型	原因	チェック（複数選択可）
意図的な原因	不審メール等の受信	□
	ユーザID等の誤り	□
	DoS攻撃等の大量アクセス	□
	情報の不正取得	□
	内部不正	□
	適切なシステム運用等の未実施	□
偶発的な原因	ユーザの操作ミス	□
	ユーザの管理ミス	□
	不審なファイルの実行	□
	不審なサイトの閲覧	□
	外部委託先の管理ミス	□
	機器等の故障	□
	システムの脆弱性	□
	他分野の障害からの波及	□
環境的な原因	災害や疾病等	□
その他の原因	その他	□
	不明	□

◆情報連絡の内容(※4) （別紙有無*: ☐ 有　☐ 無 ）

<table>
<tr><th>項　目</th><th>情報の内容</th></tr>
<tr><td>③分野名*(※5)</td><td>リストから選択</td></tr>
<tr><td>④事象が発生した重要インフラ事業者等名</td><td></td></tr>
<tr><td>⑤概　要</td><td>判明日時 :　平成　年　月　日　時　分
（発生日時 :　平成　年　月　日　時　分 ）
事象が発生したシステム・委託先業者等 :
発生事象の概要 :
システムの稼働状況 :　☐ 影響なし　☐ 停止中　☐ 一部稼働中　☐ 復旧済</td></tr>
<tr><td>⑥重要インフラサービス等への影響</td><td>重要インフラサービスのサービス維持レベル(※5)逸脱の有無 :　☐ 有　☐ 無
他の事業者等への波及の可能性 :　☐ 有　☐ 無</td></tr>
<tr><td>⑦当該事象に係る推移等</td><td>
<table>
<tr><th>日時</th><th>事象・対応状況等</th></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>
（補足情報）

対外的な対応状況
報道発表、報道等への掲載 :　☐ 済　☐ 予定有　☐ 無　（済・予定有では日時・件名を記入）

NISC以外に連絡を行った先 :</td></tr>
<tr><td>⑧今後の予定</td><td>☐ 事象継続中 （続報あり）
☐ 事後調査実施中 （続報あり）
☐ 今後の対応策を継続検討 （続報なし）
☐ 対応完了 （続報なし）</td></tr>
<tr><td>⑨その他
・得られた教訓等</td><td></td></tr>
</table>

※4：情報連絡の迅速性を優先するため、必ずしも全ての項目を記載する必要はない。
※5：「重要インフラの情報セキュリティ対策に係る第4次行動計画」に定める「分野名」、「サービス維持レベル」を指す。

様式2

□警報　□注意喚起　□参考情報

（内閣官房→重要インフラ所管省庁）

情報提供様式

（第　　報*）

（*が付与された項目は必須事項）

識別番号*	
情報提供日時*	平成　　年　　月　　日

情報提供先* （所管省庁名及び分野名）	
情報共有範囲*	□Red = 宛先限り （情報提供先の重要インフラ所管省庁限り） □Amber=特定分野・関係者限り （情報提供先の重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者のうち、関係者限り） □Green=重要インフラ関係主体限り （重要インフラ所管省庁及びセプター（セプターを構成する重要インフラ事業者等を含む。）に属する者限り） □White=公開情報
	特記事項：

◆情報提供の内容　　**（別紙有無*：□有　□無 ）**

項　目		情報の内容
脅威等の内容	①概　要	
	②対　象	
③対処方針		
④その他		

本件問い合わせ先（情報共有範囲からの問い合わせに限る。）
内閣サイバーセキュリティセンター
重要インフラ防護担当：
電話番号：
FAX番号：
電子メールアドレス：