令和３年９月 22 日公表
令和５年８月 29 日訂正

令和２年度電気通信事故に関する検証報告

電気通信事故検証会議

目次

はじめに

本報告書は、令和２年度に発生した電気通信事故について、電気通信事故検証会議（以下「本会議」という。）において、電気通信事故の再発防止に寄与することを目的として検証を行った内容等を取りまとめたものである。

令和２年度も本会議では、主に、①電気通信事業法[1]第 28 条に基づく電気通信事業法施行規則[2]第 58 条に定める重大な事故（以下「重大な事故」[3]という。）に係る報告の分析・検証、②電気通信事業報告規則[4]第７条の３に定める四半期ごとに報告を要する事故（以下「四半期報告事故」[5]という。）に係る報告の分析・検証を行った。

①については、原則として重大な事故を発生させた電気通信事業者に対して本会議への出席を要請し、これらの事業者から重大な事故報告書[6]の内容に沿って事故内容等の説明を受け、質疑応答を行った上で、構成員間で事故の検証及び教訓等の整理を行った。

---

[1] 昭和 59 年法律第 86 号

[2] 昭和 60 年郵政省令第 25 号

[3] 重大な事故とは、以下のいずれかの要件に該当する事故をいう。

①電気通信設備の故障により電気通信役務の提供を停止又は品質を低下させた事故で、次の基準に該当するもの

一 緊急通報を取り扱う音声伝送役務：継続時間１時間以上かつ影響利用者数３万以上のもの

二　緊急通報を取り扱わない音声伝送役務：継続時間２時間以上かつ影響利用者数３万以上のもの又は継続時間１時間以上かつ影響利用者数 10 万以上のもの

三　セルラーLPWA（無線設備規則第 49 条の６の９第１項及び第５項又は同条第１項及び第６項で定める条件に適合する無線設備をいう。）を使用する携帯電話（一の項又は二の項に掲げる電気通信役務を除く。）及び電気通信事業報告規則（以下「報告規則」という。）第１条第２項第 18 号に規定するアンライセンス LPWA サービス：継続時間 12 時間以上かつ影響利用者数３万以上のもの又は継続時間２時間以上かつ影響利用者数 100 万以上もの

四　利用者から電気通信役務の提供の対価としての料金の支払を受けないインターネット関連サービス（一の項から三の項までに掲げる電気通信役務を除く）：継続時間 24 時間以上かつ影響利用者数 10 万以上のもの又は継続時間 12 時間以上かつ影響利用者数 100 万以上もの

五　一の項から四の項までに掲げる電気通信役務以外の電気通信役務：継続時間２時間以上かつ影響利用者数３万以上のもの又は継続時間１時間以上かつ影響利用者数 100 万以上

②衛星、海底ケーブルその他これに準ずる重要な電気通信設備の故障の場合は、その設備を利用する全ての通信の疎通が２時間以上不能であるもの

[4] 昭和 63 年郵政省令第 46 号

[5] 四半期報告事故とは、以下のいずれかに該当する事故をいう。

①電気通信設備の故障により電気通信役務の提供を停止又は品質を低下させた事故で、影響利用者数３万以上又は継続時間２時間以上のもの

②電気通信設備以外の設備の故障により電気通信役務の提供に支障を来した事故で、影響利用者数３万以上又は継続時間が２時間以上のもの

③電気通信設備に関する情報であって、電気通信役務の提供に支障を及ぼすおそれのある情報が漏えいした事故

[6] 電気通信事業法施行規則 （以下「施行規則」という。）第 57 条に基づく報告書

②については、総務省より四半期報告事故の集計結果の報告を受けるとともに、総務省が毎年度取りまとめている「電気通信サービスの事故発生状況」について、その公表に先立って説明を受け、電気通信事故の全体的な発生状況の確認等を行った。

本報告書の取りまとめに当たっては、各事業者の機密情報の取扱い等に留意しつつ、本会議の検証結果が事故発生の当事者である事業者のみならず、他の事業者の今後の取組にも反映されるよう、できる限り一般化し、わかりやすい記述に努めた。

なお、本会議による検証は、事故の責任を問うために行うものではないことを付言しておく。

第１章　令和２年度検証案件の概要

１．電気通信事故発生概況

令和２年度においては、重大な事故は４件であり、これは直近約 20 年間において最低であった令和元年度の３件に次いで少ない件数であった。他方で、四半期報告事故（詳細な様式による報告分）の件数は 6,612 件と、前年度から 311 件増加しており、直近３年間では微増傾向となっている。

サービス別で見ると、データ通信サービスの事故が最も多く、全体の 65%を占めており、件数自体も増加傾向にある。

発生要因別に見ると、外的要因が最も多く全体の 62%を占めており、微増傾向にある。中でも他の電気通信事故の割合が最も高く、全体の 55%となっている。

故障設備別で見ると、伝送交換設備に起因する事故が最も多く全体の半数近くを占めており、その内の半数が加入者収容装置の事故である。次いで伝送路設備に起因する事故の割合が高く全体の 39%となっており、その内の６割が加入者ケーブルに起因する事故である。

過去５年間の経年変化で見ると、自然災害を起因として例年第２四半期に件数が多い傾向がある。特に、故障設備別で見ると、電源の故障に起因する事故は多く、継続時間で見ても 24 時間以上継続する事故に繋がっていると考えられる。

また、サービス別でみると、音声サービスについては、アナログ電話サービスの事故が減少する一方で、IP 電話サービスの事故が増加する傾向に変化はない。その他、影響利用者数別、発生要因別の事故発生の傾向については、大きな変化は見られない。

また、異常トラフィックに起因する事故が直近５年間では年に 45～135 件程度報告されており、サイバー攻撃が原因の可能性もあるため今後も注視が必要である。

（１）電気通信事故報告件数

令和２年度に発生した重大な事故については、表１のとおり、４件であり、前年度の３件から１件増加している。また、それらの重大な事故及び四半期報告事故（詳細な様式による報告分）の報告件数は 6,612 件と、前年度の 6,301 件から 311 件増加している。統計的集計が可能となった平成 22 年度[7]以降では、図１のとおり、平成 23 年度から減少していたが、直近３年間は微増している。

（表1）令和2年度に報告された電気通信事故

	報告事業者数	報告件数
重大な事故	4社 （5社※1）	4件 （3件）
四半期報告事故		
詳細な様式による報告[8]	129 社 （111 社）	6,612 件※2 （6,301 件※2）
簡易な様式による報告[9]	33 社 （24 社）	55,001 件 （58,211 件）

（括弧内は令和元年度の数値。）

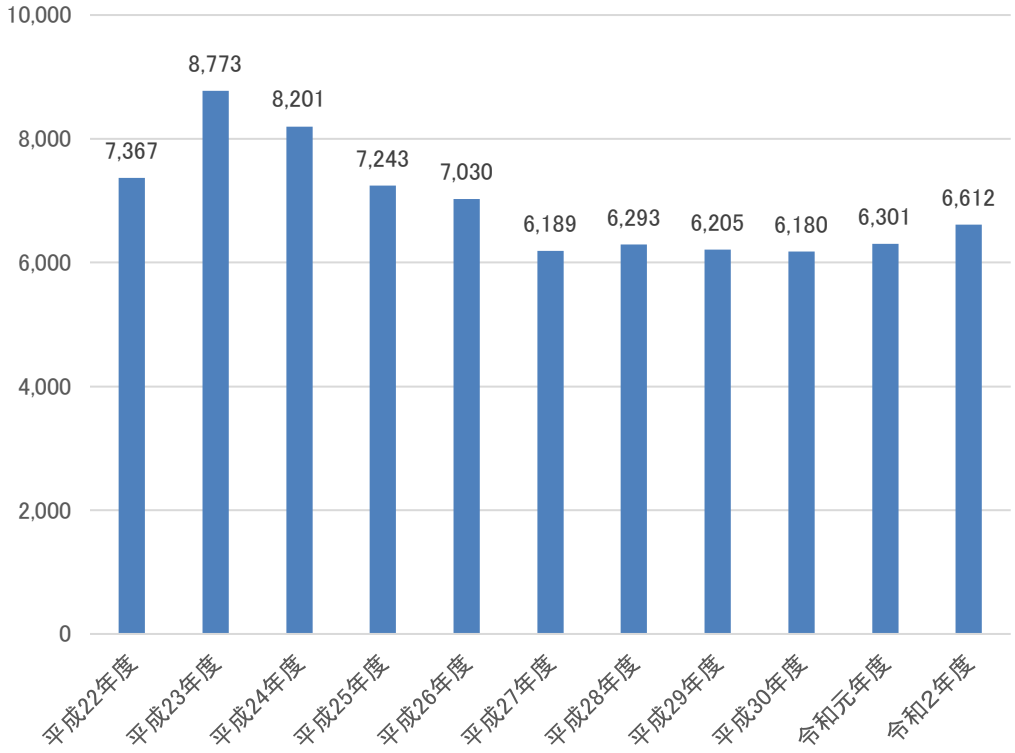
※1 卸役務に関する事故については、報告事業者数として卸提供元事業者及び卸提供先事業者の両方が含まれているため、報告事業者数が報告件数よりも多くなっている。

※2 卸役務に関する事故については、当該事故における卸提供元事業者及び卸提供先事業者の両方からの報告件数が含まれている。

[7] 四半期報告事故は平成 20 年４月から運用が開始されたが、当時における詳細な様式については、内容が自由記述であったため事業者によって記載内容等も異なっており、また、事故の影響規模等の記載が求められていなかったため、統計的な処理が難しく、事故の発生状況について十分に分析を行えなかった。そこで、報告規則が改正され、平成 22 年４月から、報告内容の統一化・明確化等を図るため、詳細な報告について、新たな報告様式への変更が行われている。

[8] 重大な事故については、施行規則様式第 50 の３に加え、報告規則様式第 27 により報告することとされているため、詳細な様式による報告に含めて計上されている。

[9] ①無線基地局、②局設置遠隔収容装置又はき線点遠隔収容装置及び③デジタル加入者回線アクセス多重化装置の故障による事故については、報告規則第７条の３第１項の規定に基づく告示により、簡易な様式による報告が認められている。



（図１）重大な事故及び四半期報告事故（詳細な様式による報告分）件数の推移 [10]

[10] 令和元年度以前の電気通信事故の発生状況は以下の総務省ホームページに掲載。
https://www.soumu.go.jp/menu_seisaku/ictseisaku/net_anzen/jiko/result.html
重大な事故について、電気通信役務の多様化・高度化・複雑化に伴い、それまでのサービス一律の同じ報告基準（影響利用者数３万以上かつ継続時間２時間以上）から見直しが行われ、平成 27 年度からはサービス区分別の基準（脚注３参照）に基づき報告が行われている。

（２）影響利用者数及び継続時間別

重大な事故及び四半期報告事故の件数を影響利用者数で見ると、表２のとおり、総件数 6,612 件のうち、９割強が影響利用者数 500 人未満の事故となっており、これは直近５年間と同様の傾向となっている。

また、継続時間で見ると、継続時間が２時間以上５時間未満の事故については、3,325 件（50.3%）と、直近５年間と同様に半数を占めており、事故収束まで 12 時間以上かかった事故についても、1,728 件（26.2%）と、直近５年間と同様に全体の３割近くを占めている。

なお、４件発生した重大な事故[11]のうち、１件は 10 万人以上 100 万人未満かつ 24 時間以上の事故（※１）、１件は 100 万人以上かつ５時間以上 12 時間未満の事故（※２）、１件は 10 万人以上 100 万人未満かつ２時間以上５時間未満の事故（※３）、１件は 10 万人以上 100 万人未満かつ５時間以上 12 時間未満の事故（※４）となっている。

（表２）影響利用者数及び継続時間別の電気通信事故発生状況（6,612 件）

利用者数 / 継続時間	500人未満	500人以上 5千人未満	5千人以上 3万未満	3万以上 10万未満	10万以上 100万未満	100万以上	計
30分未満	四半期報告対象外			11	10	2	23 (0.3%)
30以上 1時間未満				2	2	2	6 (0.1%)
1時間以上 1時間30分未満				3	4	0	7 (0.1%)
1時間30分以上 2時間未満				0	5	0	5 (0.1%)
2時間以上 5時間未満	2,984	299	36	1	※3 5	0	3,325 (50.3%)
5時間以上 12時間未満	1,458	47	11	0	※4 1	※2 1	1,518 (23%)
12時間以上 24時間未満	965	16	9	0	0	0	990 (15%)
24時間以上	711	16	9	1	※1 1	0	738 (11.2%)
計	6,118 (92.5%)	378 (5.7%)	65 (1%)	18 (0.3%)	28 (0.4%)	5 (0.1%)	6,612 (100.0%)

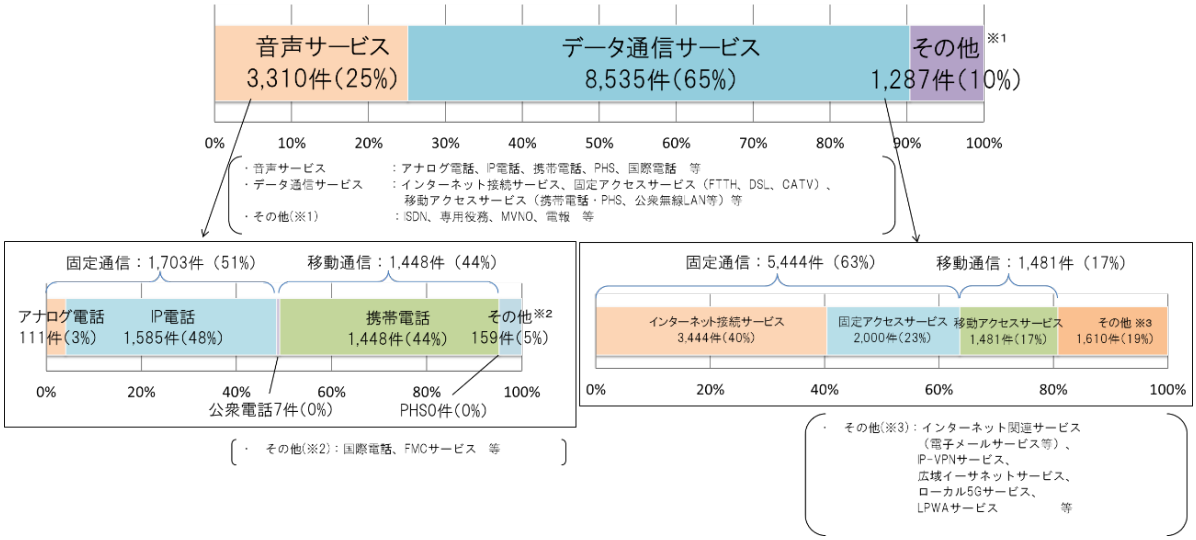
[11] （表２）の※の数字は、（表３）令和２年度に発生した重大な事故の一覧の番号に該当。

（３）サービス別

四半期報告事故をサービス別に見ると、図２のとおり「データ通信サービス」の件数が 8,535 件（65%）と最も多く発生しており、そのうち、「インターネット接続サービス（固定）」が 3,444 件（40%）と最も多く、次いで「固定アクセスサービス」が 2,000 件（23%）、「移動アクセスサービス」が 1,481 件（17%）となっている。

また、音声サービスの事故は 3,310 件（25%）となっており、そのうち、「IP 電話」が 1,585 件（48%）と最も多く、次いで「携帯電話」が 1,448 件（44%）となっており、全体の 92%を占めている。「アナログ電話」は 111 件（3%）であり、事故の割合は非常に低くなっている。[12]

なお、４件発生した重大な事故のうち、１件は主に音声サービス（IP 電話）の事故、３件は主にデータ通信サービス（携帯電話１件、インターネット関連サービス（有料）（電子メールサービス）２件）の事故となっている。



（図２）サービス別電気通信事故発生状況

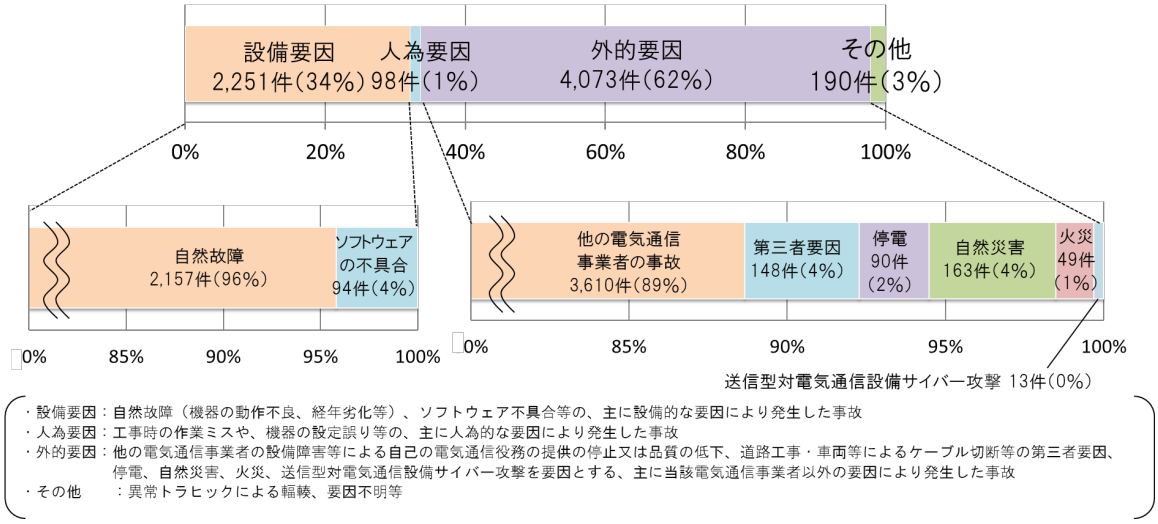
[12] これらの計数は複数サービスへの同時影響があるため、総件数より多くなっている。

（４）発生要因別

四半期報告事故を発生要因[13]別で見ると、図３のとおり他の電気通信事業者の設備障害による事故など、自社以外の要因（外的要因）が 4,073 件（62%）と最も多く、そのうち、他の電気通信事業者の事故によるものが 3,610 件（89%）と外的要因の大半を占めている。

次いで、自然故障等の設備的な要因（設備要因）が 2,251 件（34%）となっており、そのうち、自然故障が 2,157 件と設備要因の 96%を占めている。

なお、４件発生した重大な事故のうち、２件は設備要因（自然故障、ソフトウェアの不具合）、１件は人的要因、１件はその他となっている。



（図３）発生要因別電気通信事故発生状況

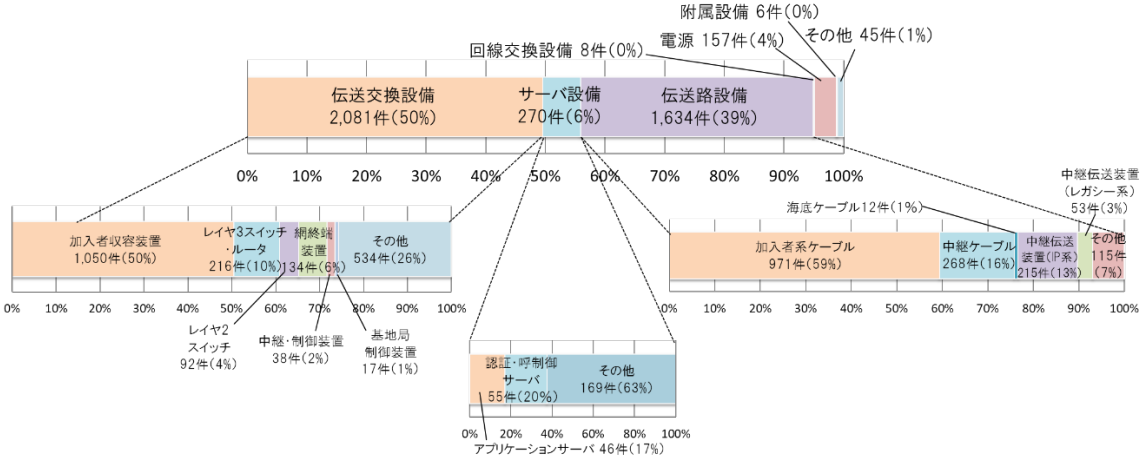
[13] １件の事故で複数の発生要因がある場合であっても、主たる発生要因のみで集計している。

（５）故障設備別

四半期報告事故を故障設備別で見ると、図４のとおり故障設備が明確な 4,201 件のうち、伝送交換設備に起因する事故が 2,081 件（50%）と最も多く、そのうち、加入者収容装置の事故が 1,050 件（50%）と伝送交換設備の半数を占めており、次いで、レイヤ３スイッチ・ルータが 216 件（10%）、レイヤ２スイッチが 92 件（4%）となっている。

次いで、伝送路設備に起因する事故が 1,634 件（39%）となっており、そのうち、加入者系ケーブルが 971 件（59%）、中継ケーブルが 268 件（16%）と、ケーブル支障による事故が伝送路設備の約４分の３占めている。

なお、４件発生した重大な事故のうち、２件はサーバ設備（認証・呼制御サーバ、その他）の事故、１件は伝送交換設備（その他）の事故、１件はその他（ストレージ装置）の事故となっている。



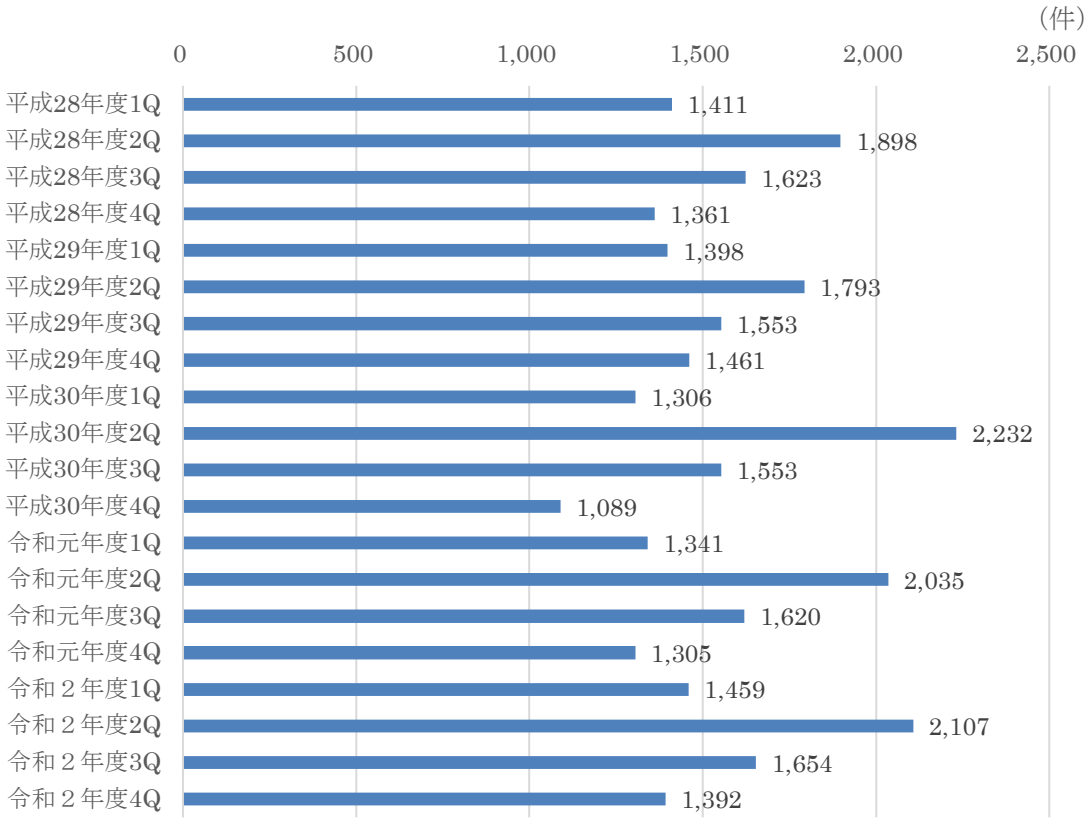
（図４）故障設備別電気通信事故発生状況

２．経年変化の分析（過去５年間の傾向）

四半期報告事故について、過去５年間どのような事故が発生し、傾向があるのかを分析した。

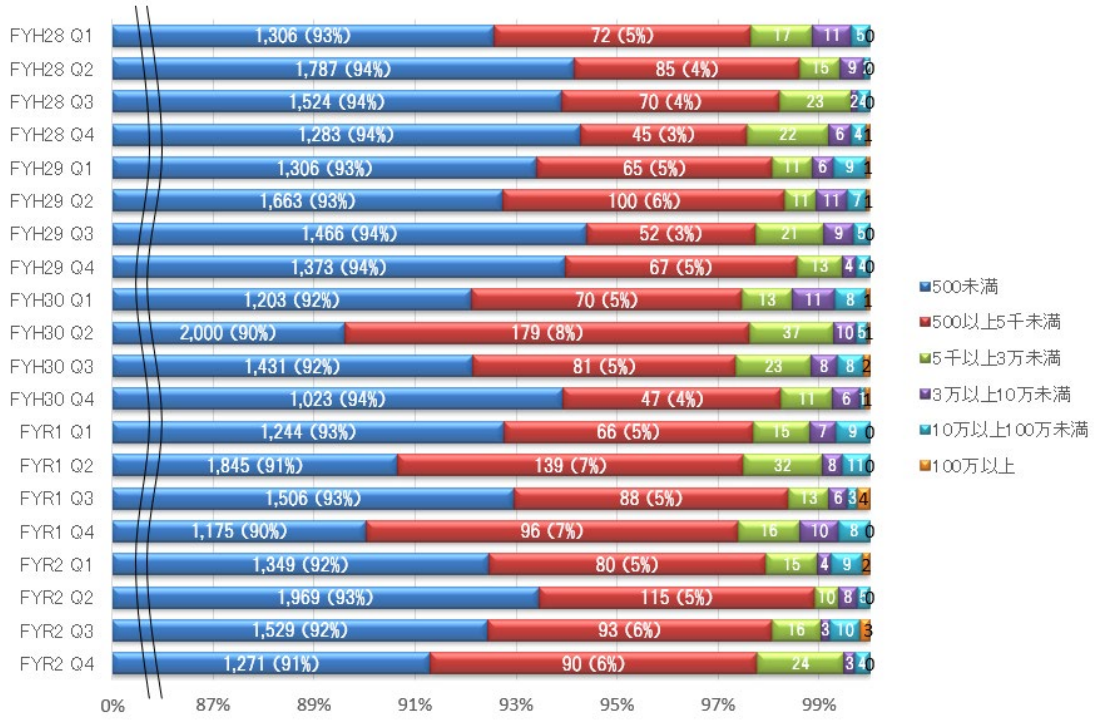
四半期毎の事故件数については、図５のとおり各年度ともに第２四半期（７月～９月）の事故件数がもっとも多くなっている。特に、平成 30 年度第２四半期は事故件数が多かったが、同年７月の西日本を中心とした豪雨など、自然災害による影響が大きかったものと推察される。

また、令和２年７月には、西日本から東日本、東北地方の広い範囲で大雨があり、同年第２四半期は平成 30 年第２四半期に次ぐ事故件数となっている。

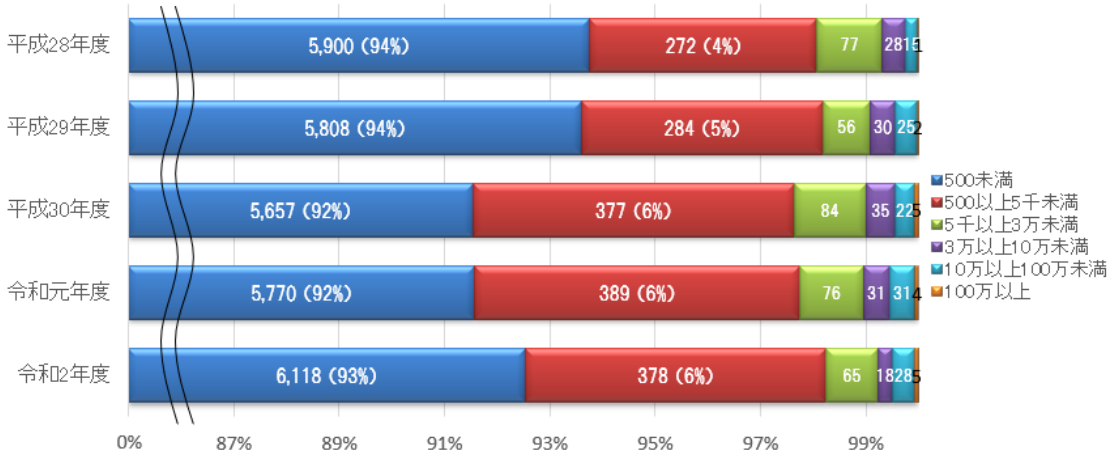


（図５）四半期毎の事故発生件数の推移（平成 28 年度～令和２年度）

影響利用者数別で見ると、図６及び図７のとおり「影響利用者数 500 人未満の事故」が多く、いずれの期においても９割以上を占めている。一方で３万人以上の事故はいずれの期においても１%程度にとどまっている。



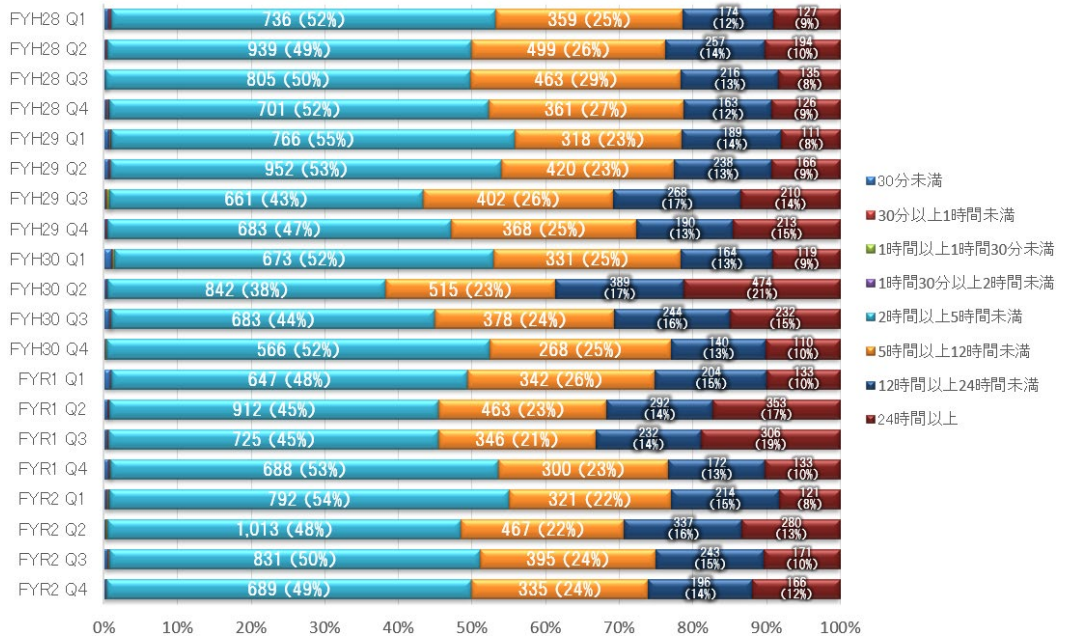
（図６）影響利用者数別　四半期毎の事故発生件数の推移



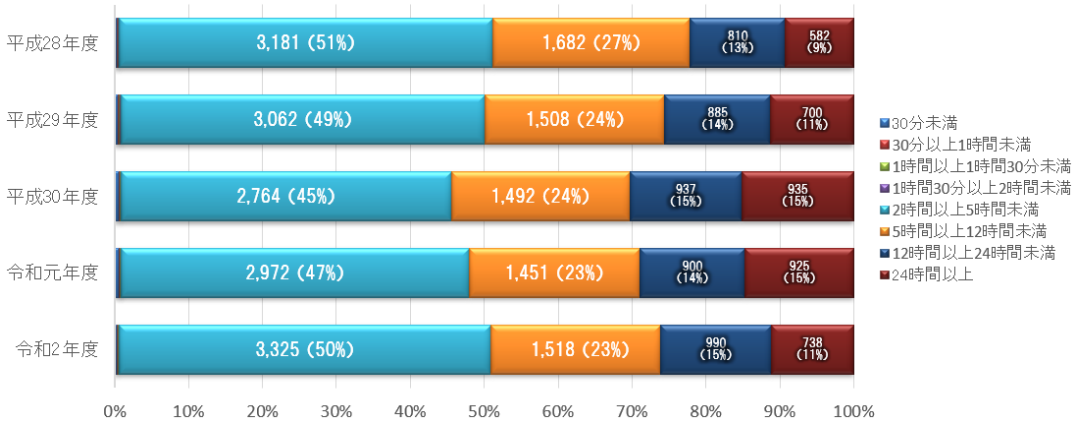
（図７）影響利用者数別　年度毎の事故発生件数の推移

継続時間別で見ると、図８及び図９のとおり事故の半数以上は継続時間５時間未満となっている。一方で、継続時間 24 時間以上の事故は８%～19%の範囲で推移しているが、西日本を中心とした豪雨のあった平成 30 年をピークに減少に転じている。これは、図 10 にあるように第２四半期の事故件数が平成 30 年度以降大きく減少していることが影響しているためである。

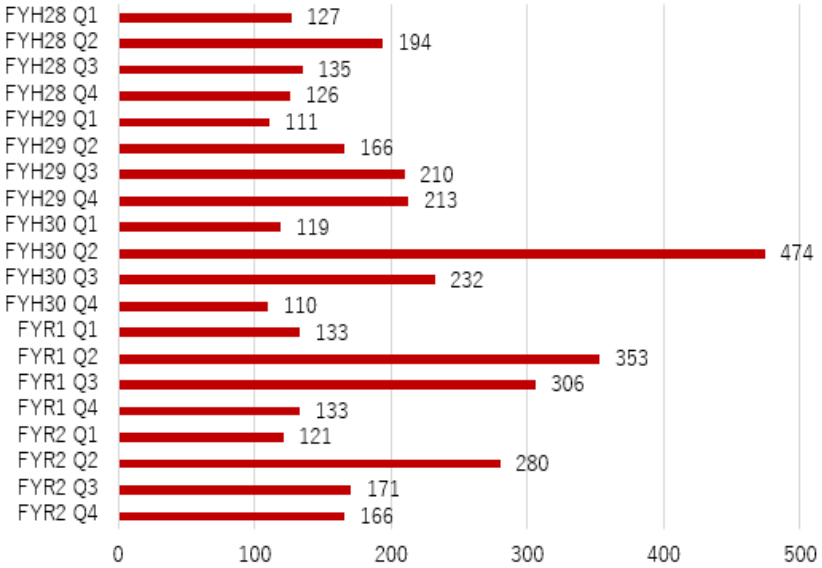
しかしながら、令和元年度は９月、10 月に台風による大雨・暴風等、令和２年度７月の豪雨等の影響を受けて継続時間 24 時間以上の事故発生件数も通常より多くなっている。



（図８）継続時間別　四半期毎の事故発生件数の推移

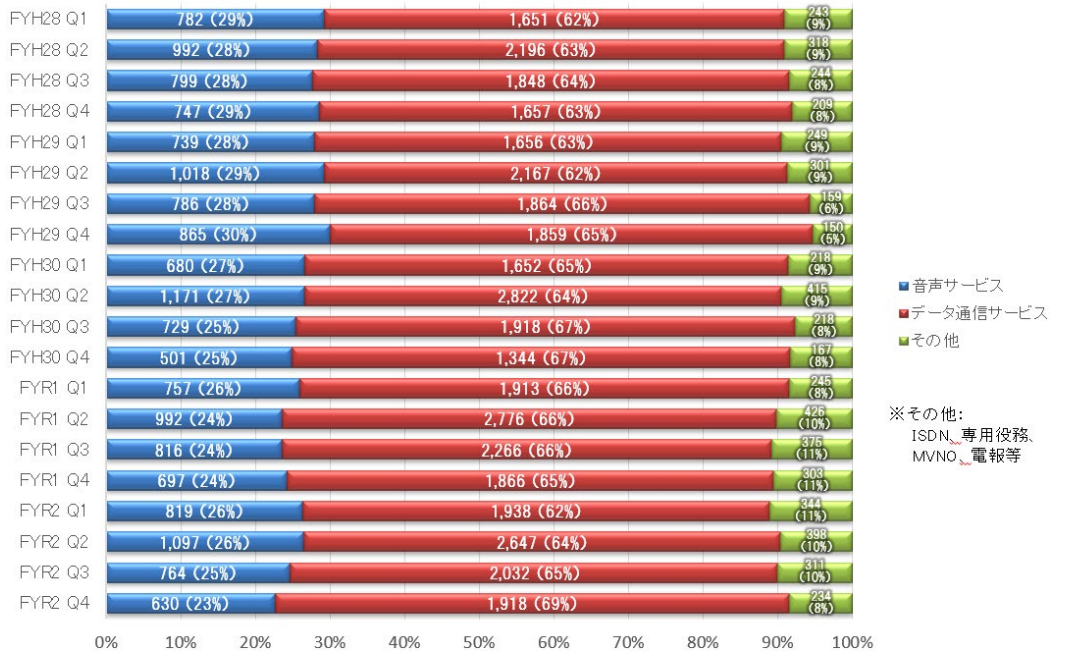


（図９）継続時間別　年度毎の事故発生件数の推移

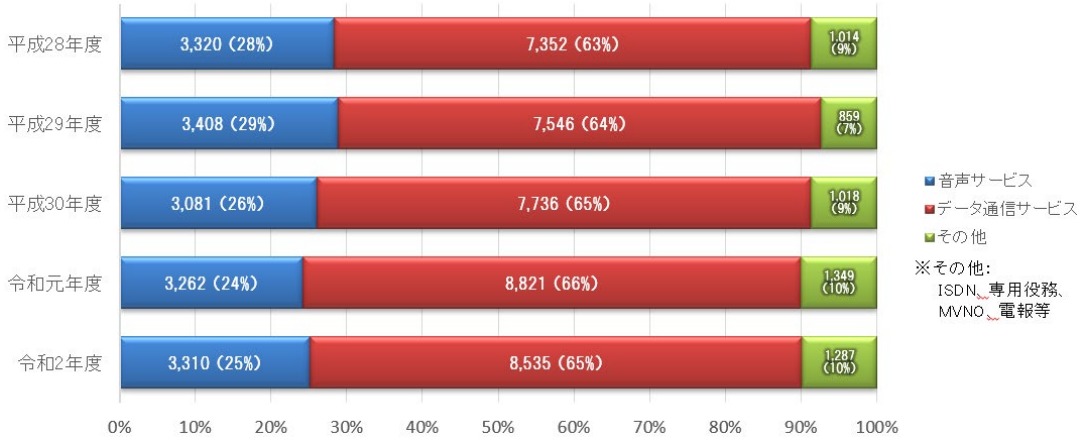


（図 10）継続時間 24 時間以上の事故発生件数の推移

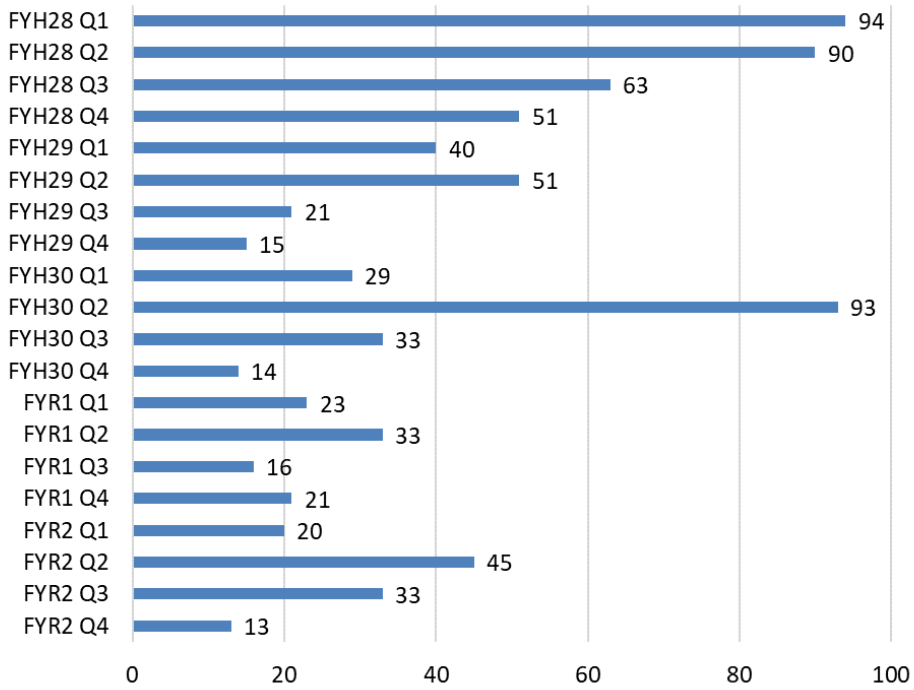
サービス別で見ると、図 11 及び図 12 のとおり「データ通信サービス」の割合が微増し、「音声サービス」の割合が微減傾向にある。また、図 13 及び図 14 のとおり「音声サービス」のうち、「アナログ電話サービス」については件数自身も少なく減少傾向となっている一方、「IP 電話サービス」については音声サービスの事故の半数程度を占めるとともに増加傾向となっている。



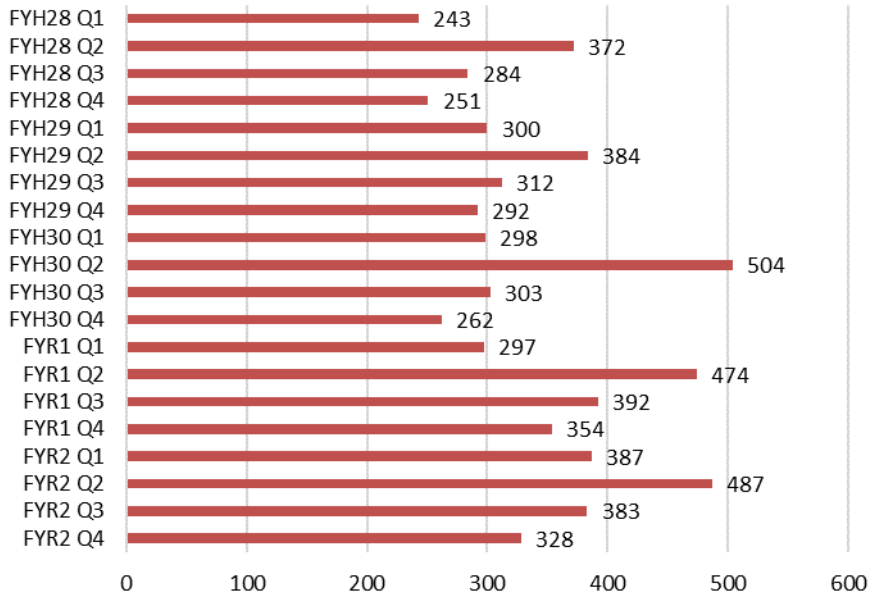
（図 11）サービス別　四半期毎の事故発生件数の推移



（図 12）サービス別　年度毎の事故発生件数の推移

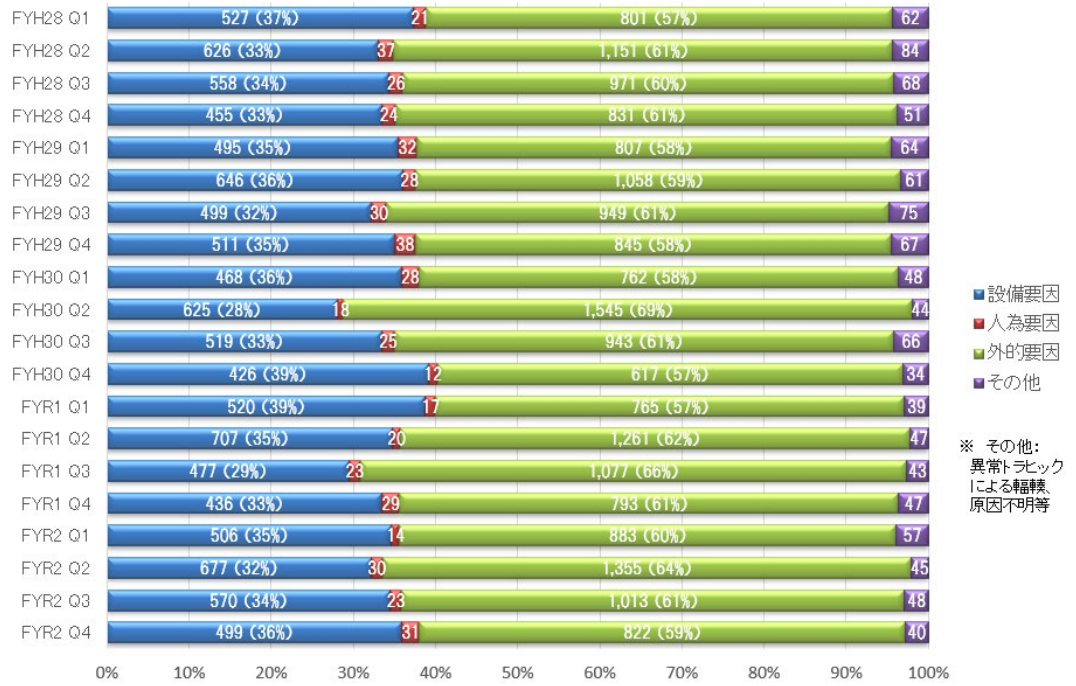


（図 13）アナログ電話サービスの事故発生件数の推移

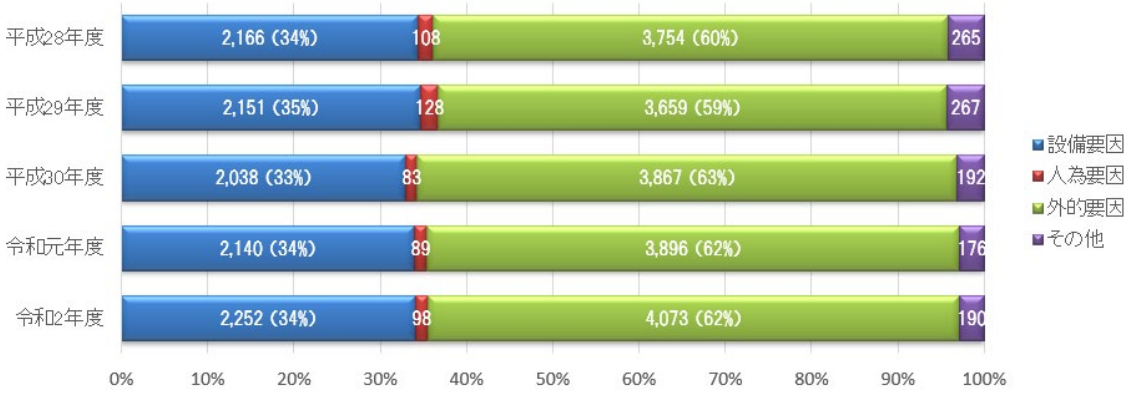


（図 14）IP 電話サービスの事故発生件数の推移

発生要因別で見ると、図 15 及び図 16 のとおり発生要因の構成に大きな変化は見られないが、平成 30 年度第２四半期、令和元年度第３四半期及び令和２年度第２四半期は外的要因による事故の件数が多くなっており、自然災害の影響によるものと考えられる。

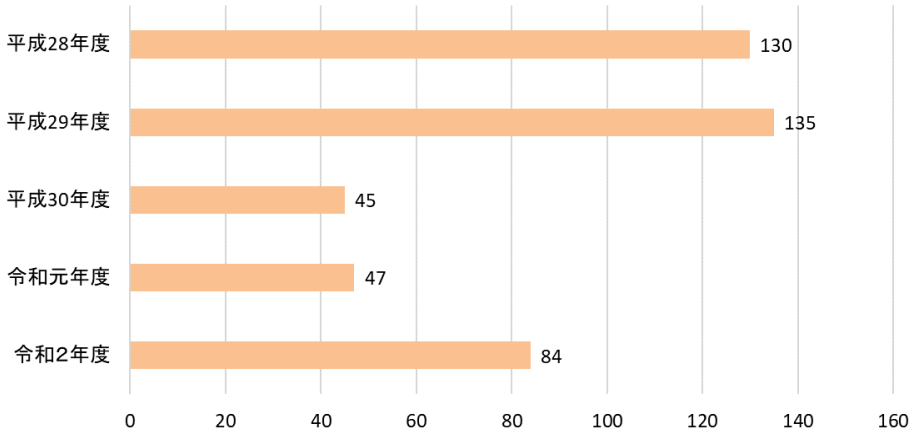


（図 15）発生要因別　四半期毎の事故発生件数の推移



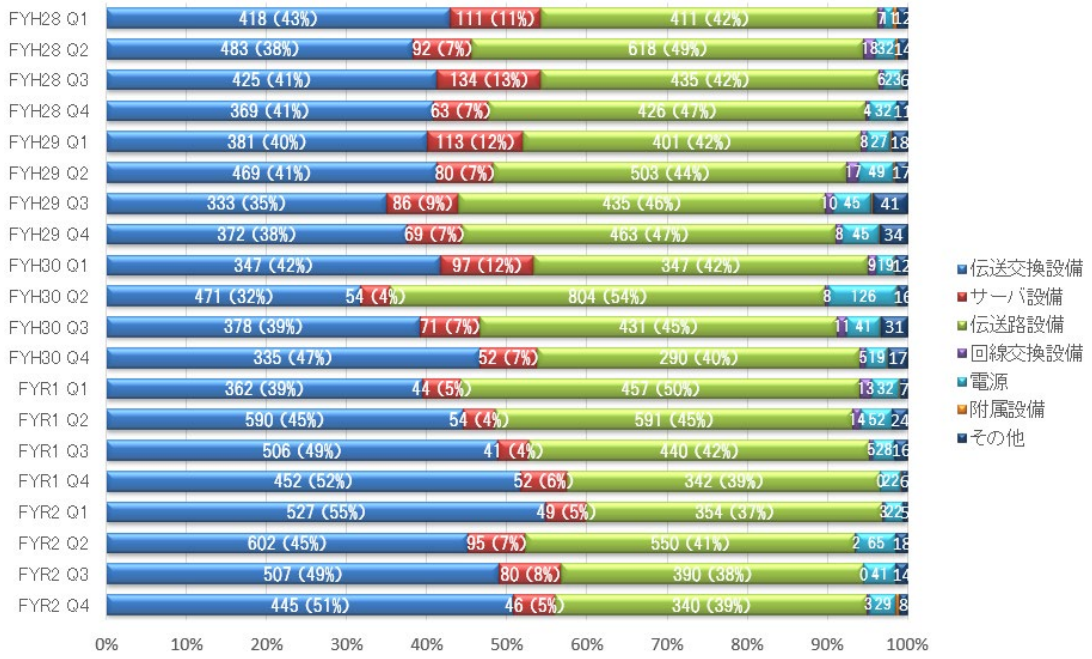
（図 16）発生要因別　年毎の事故発生件数の推移

また、「異常トラヒック」に起因する事故件数の推移について図 17 に示しているが、サイバー攻撃等による通信の急増に起因した障害の可能性も考えられるため、引き続き、異常トラヒックによる電気通信サービスへの支障について注視していく必要がある。

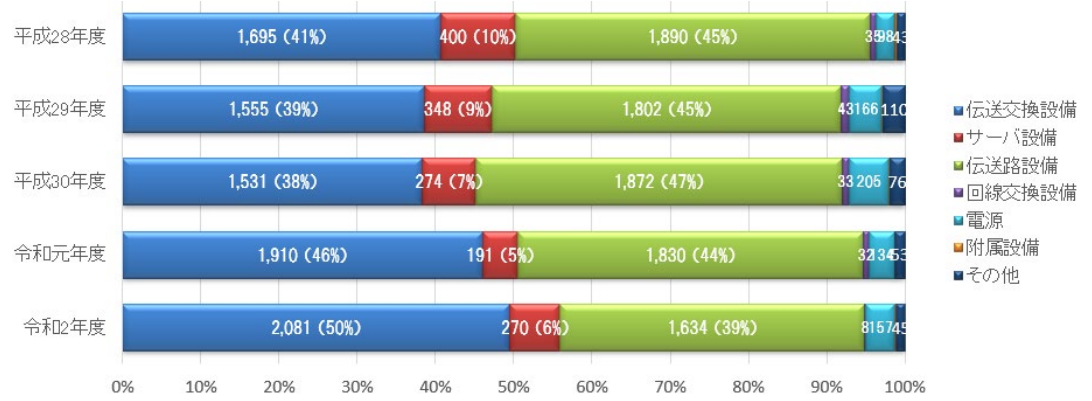


（図 17）異常トラヒックに起因した事故発生件数の推移

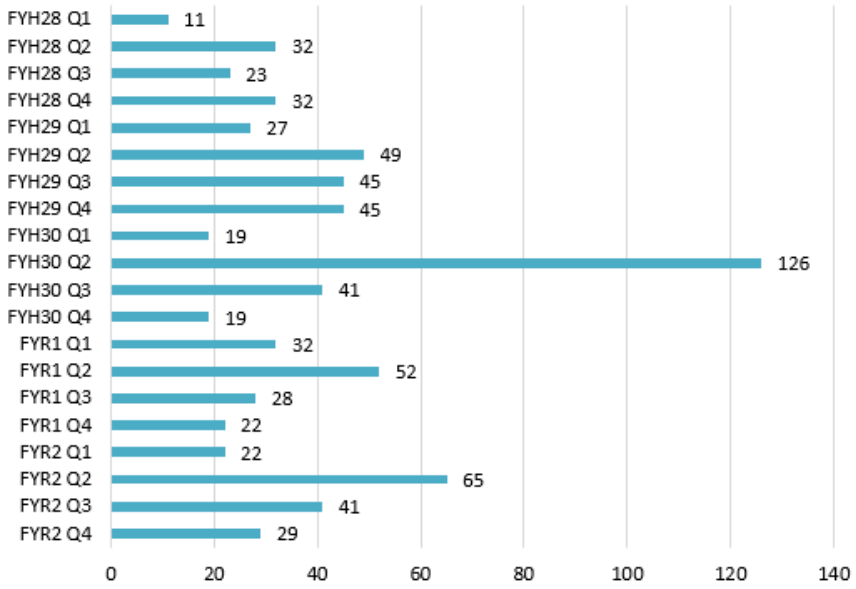
故障設備別で見ると、図 18 及び図 19 のとおり「伝送交換設備」が増加傾向にある。図 20 のとおり、平成 30 年度第２四半期では、「電源の故障」に起因した事故件数が、他の四半期と比較して突出しているが、発生原因が「停電」によるものが３分の２を占めており、自然災害による影響と推察される。同様に、令和２年度第２四半期は自然災害の影響で通常よりも事故件数は多くなっている。



（図 18）故障設備別　四半期毎の事故発生件数の推移



（図 19）故障設備別　年度毎の事故発生件数の推移



（図 20）電源の故障に起因した事故発生件数の推移

３．令和２年度重大な事故等の発生状況

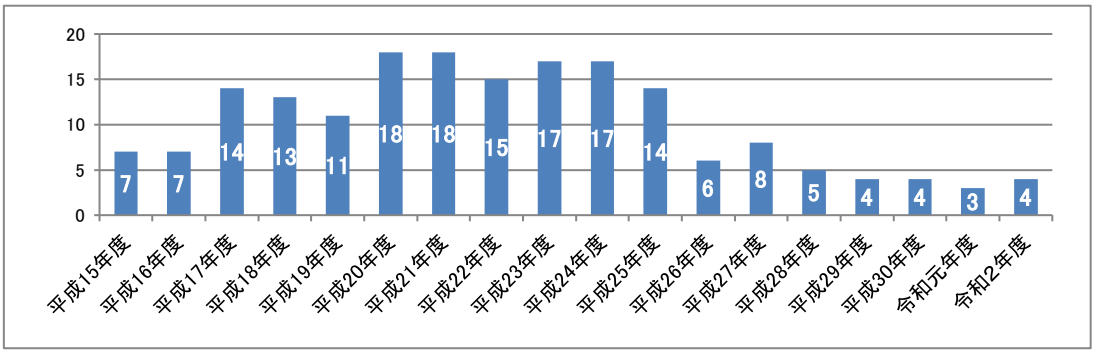
（１）発生件数

令和２年度に発生した重大な事故は表３のとおり４件と、前年度の３件から１件増加している。重大な事故の発生件数は、図 21 のとおり、平成 20 年度及び 21 年度の 18 件をピークに概ね減少傾向にある。

（表３）令和２年度に発生した重大な事故の一覧

No	事業者名	発生 日時	継続 時間	影響 利用者数等	主な 障害内容	重大な事故に該当する電気通信役務の区分　※１
１	キヤノンマーケティングジャパン㈱	R2.4.30 14:07	①2h ②81h32m	166,803 人	①インターネット関連サービス(有料)(電子メール)の提供の停止（利用不可） ②インターネット関連サービス(有料)(電子メール)の品質の低下（遅延）	五：一の項から四の項までに掲げる電気通信役務以外の電気通信役務（インターネット関連サービス（有料）（電子メール））
２	㈱ NTT ドコモ	R2.5.30 12:56	5h36m	最大 220 万人	インターネット接続サービスの提供の停止 （利用不可）	五：一の項から四の項までに掲げる電気通信役務以外の電気通信役務（インターネット接続サービス）
３	西日本電信電話 ㈱	R2.6.29 12:11	①2h36m （石川県） ②4h21m （兵庫県）	①135,000 回線 ②8,000 回線	緊急通報を取り扱う音声伝送サービス（IP 電話）の提供の停止 （着信不可・誤着信）	一：緊急通報を取り扱う音声伝送役務（IP 電話）
４	フリービット㈱	R2.7.31 2:58	8h07m	106,027 人	インターネット関連サービス(有料)(電子メール)の提供の停止 （利用不可）	五：一の項から四の項までに掲げる電気通信役務以外の電気通信役務（インターネット関連サービス（有料）（電子メール））

※１「重大な事故に該当する電気通信役務の区分」については、P.1 脚注３を参照。

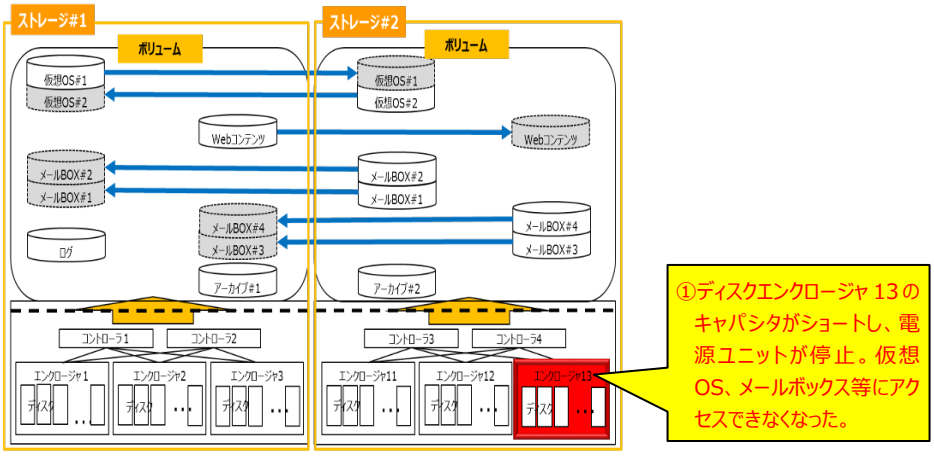
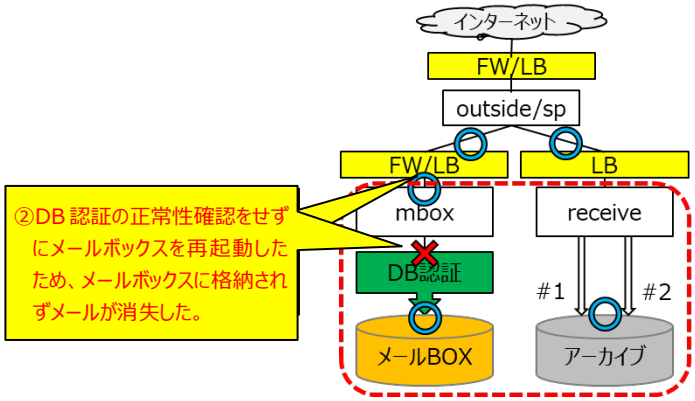


（図 21）重大な事故発生件数の年度ごとの推移

（２）重大な事故の概要

ア　キヤノンマーケティングジャパン（株）の重大な事故

事業者名	キヤノンマーケティングジャパン株式会社	発生日時	令和２年４月 30 日 14 時 07 分
継続時間	①２時間 ②81 時間 32 分	影響利用者数	166,803 人
影響地域	全国	事業者への問合せ件数	電話 192 件、メール 31 件 （令和２年５月 21 日 18 時時点）
障害内容	①ストレージを構成するディスクエンクロージャ（筐体）の一つが停止したことに伴い、同ディスクエンクロージャで稼働していた仮想 OS、メールボックス等の機能が停止した。 ②障害発生中に受信したメールがメールボックスに格納されず消失したため、アーカイブから再配送を実施した。		
重大な事故に該当する電気通信役務の区分	五：一の項から四の項までに掲げる電気通信役務以外の電気通信役務 （インターネット関連サービス(有料)（電子メール)）		
発生原因	①ストレージを構成するディスクエンクロージャのミッドプレーン（基盤）上のキャパシタ（蓄電部品）がショート（短絡）した。電源ラインの異常が発生すると回路保護のために電源ユニットが停止する仕様となっていたため、当該ディスクエンクロージャで稼働していた仮想 OS、メールボックス等にアクセスできなくなった。 ②DB 認証（受信メールとユーザとのひも付け）の正常性確認をせずにメール BOX の復旧を優先させたことにより、DB 認証ができない状態が発生した。その状態のままメールボックスにメールを配送したことにより、メールボックスに格納されず消失した。そのため、アーカイブからメールを復旧し、再配送を実施した。		

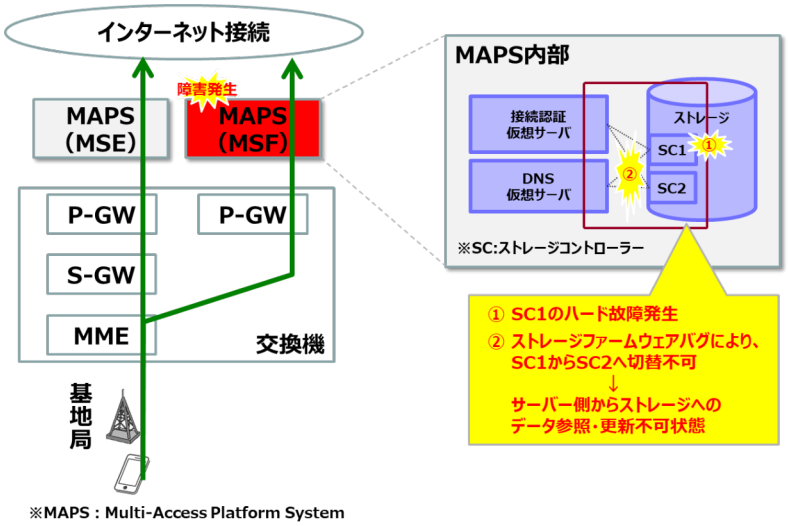
機器構成図	①  ② 
再発防止策	＜対処①　DB 認証の管理機能冗長化＞ DB 認証の管理機能を仮想 OS から切り出して他の物理サーバに配置し、その複製をストレージ#1 及びストレージ#2 に配置した。これにより、同様の障害が発生しても他のサーバにて DB 認証機能が有効であるため、ストレージの復旧作業のみ実施すればよく、早期復旧を可能とした。【令和２年５月 21 日実施済】 ＜対処②　障害時の復旧手順書の見直し＞ 同様の障害発生時に、outside/sp 配下の FW/LB を意図的に切断し、DB 認証機能の復旧及び正常性確認後、メールボックスサーバの復旧を実施する手順を明確化。また、対処①の対策を踏まえた、作業、確認手順を変更した。【令和２年６月 30 日実施済】 ＜対処③　該当ストレージ機器の交換＞ 障害部位の障害発生率が低い水準であるというメーカ回答から、機器の交換を実施した。【令和２年６月 27 日実施済】

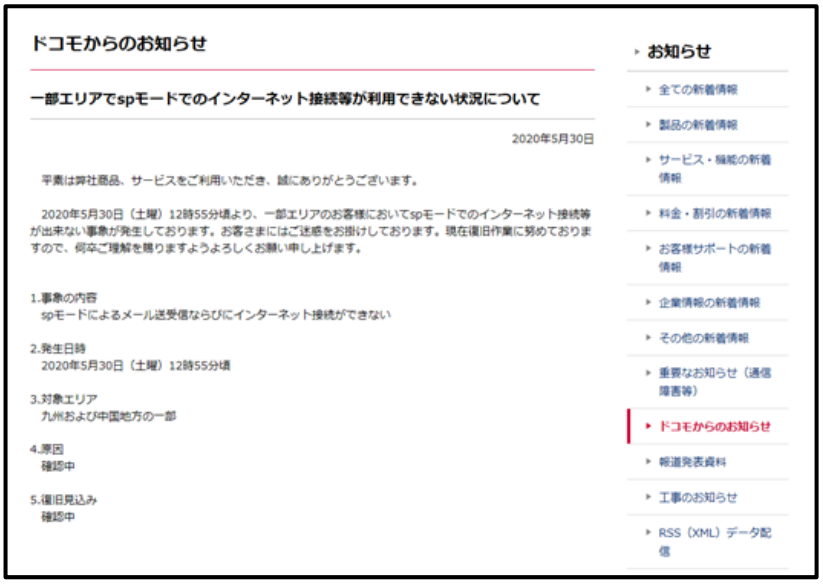
情報周知	自社サイト	【障害情報】 ・令和２年４月 30 日 14 時 45 分、第１報　障害発生のご報告【続報１】  ・令和２年４月 30 日　16 時 00 分、第２報　障害発生のご報告【続報２】 ・令和２年４月 30 日　18 時 10 分、第３報　障害復旧のご報告 ・令和２年５月１日　09 時 00 分、第４報　ホスティング障害（4/30）の影響に関するご報告 ・令和２年５月１日　12 時 30 分、第５報　ホスティング障害（4/30）の影響に関するご報告【続報１】 ・令和２年５月１日　17 時 00 分、第６報　ホスティング障害（4/30）の影響に関するご報告【続報２】 ・令和２年５月１日 20 時 20 分、第７報　ホスティングサービス障害（4/30）の影響の対応完了のご報告 ・令和２年５月３日 17 時 30 分、第８報　ホスティング障害（4 月 30 日）の未受信メール追加対策のご報告 ・令和２年５月４日 00 時 40 分、第９報　ホスティング障害（4 月 30 日）の未受信メール追加対策のご報告【完了】

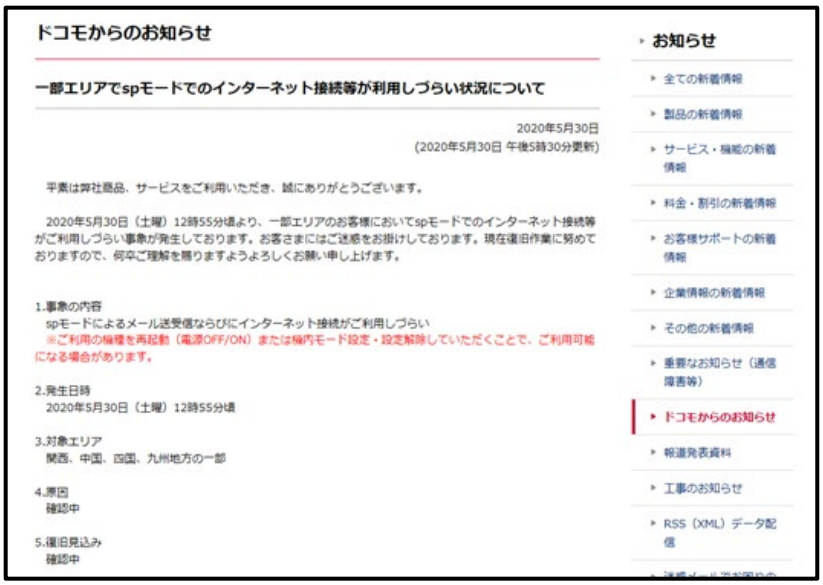
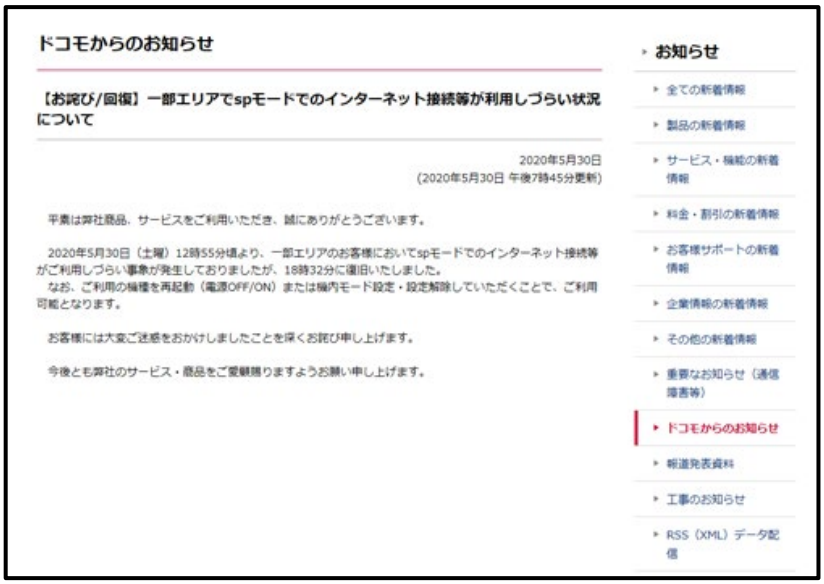
		・令和２年５月５日 08 時 00 分、第 10 報　【重要】ホスティング障害（4 月 30 日）の未受信メール対策に関するご報告【完了】 
	報道発表	なし
	その他	なし

イ　（株）ＮＴＴドコモの重大な事故

事業者名	株式会社ＮＴＴドコモ	発生日時	令和２年５月 30 日 12 時 56 分
継続時間	５時間 36 分	影響利用者数	最大 220 万人
影響地域	西日本の一部（関西、中国、四国、九州地方のそれぞれの一部）	事業者への問合せ件数	885 件（電話窓口への問合せ） （令和２年５月 31 日 17 時時点）
障害内容	sp モードシステム（MAPS）におけるストレージのハードウェア故障発生時に、動作故障を検知するソフトウェアバグにより、ハードウェア故障時の経路切替が正常に行われず、複数の仮想サーバ（DNS、接続認証サーバ等）でストレージへのアクセスができなかったことから、sp モードに接続しづらい事象が発生した。		
重大な事故に該当する電気通信役務の区分	五：一の項から四の項までに掲げる電気通信役務以外の電気通信役務 （インターネット接続サービス）		
発生原因	＜発生原因の概要＞ ストレージのハードウェア故障と同時に、同左故障時に冗長先への迂回措置を行うソフトウェアバグに起因して障害が発生。 当該ソフトウェアバグについては認識しており、本事象との関係性検証と改修版へのアップデートに向けた準備を実施中であった。 ＜大規模化した原因＞ 故障の大規模化を避けるため冗長構成をとっていたが、ストレージのハードウェア故障を検知するソフトウェアバグにより冗長設備への切替が行われず、通信に必要となる複数のサーバ（DNS、接続認証サーバ等）でストレージへのアクセスができなくなったため、当該システム（MAPS_MSF）を利用する全利用者に影響が発生した。 ＜長期化した原因＞ 運用中の正常な sp モードシステム（MAPS_MSB,MSC,MSD）に接続先を拡大するための作業手順書は確立されていたが、拡大対象のシステム数が多かったこと、及び初めての対応となることから正常利用中の利用者への影響回避を前提とした作業の安全性確保等に時間を要し、復旧に時間を要した。		

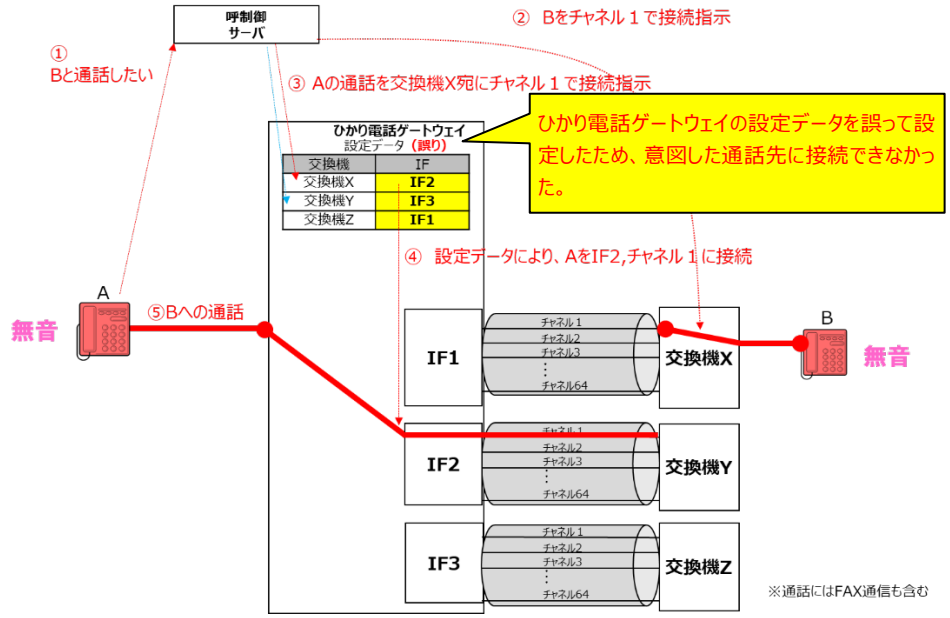
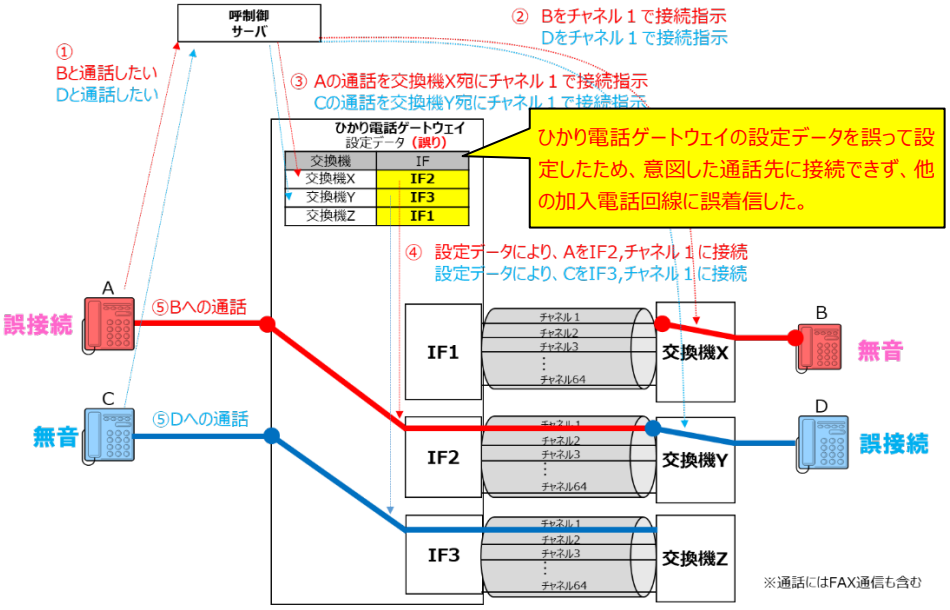
機器構成図	
再発防止策	＜暫定対処＞ 1. ストレージのハードウェア故障を検知した場合に運用者オペレーションで切替を実施する手順を整備【令和２年５月 31 日　適用開始】 ＜恒久対処＞ 1. ストレージのハードウェアを正常な機器に交換【令和２年５月 31 日　実施完了】 2. ストレージのハードウェア故障を検知するソフトウェアのバージョンアップ【令和２年６月 19 日　実施完了】 3. MAPS 接続面追加措置実施時の作業手順書を故障発生時の対応に合わせて整備【令和２年６月 26 日　実施完了】

情報周知	自社サイト	【発生情報】 ・令和２年５月 30 日 15 時 30 分、お知らせに「一部エリアで sp モードでのインターネット接続等が利用できない状況について」（初報）を掲載。  ・令和２年５月 30 日 16 時 15 分、お知らせに「一部エリアで sp モードでのインターネット接続等が利用できない状況について」（第２報）を掲載。 

		・令和２年５月 30 日 17 時 30 分、お知らせに「一部エリアで sp モードでのインターネット接続等が利用できない状況について」（第３報）を掲載。  ドコモからのお知らせ 一部エリアでspモードでのインターネット接続等が利用しづらい状況について 2020年5月30日 (2020年5月30日 午後5時30分更新) 平素は弊社商品、サービスをご利用いただき、誠にありがとうございます。 2020年5月30日（土曜）12時55分頃より、一部エリアのお客様においてspモードでのインターネット接続等がご利用しづらい事象が発生しております。お客さまにはご迷惑をお掛けしております。現在復旧作業に努めておりますので、何卒ご理解を賜りますようよろしくお願い申し上げます。 1.事象の内容 spモードによるメール送受信ならびにインターネット接続がご利用しづらい ※ご利用の機種を再起動（電源OFF/ON）または機内モード設定・設定解除していただくことで、ご利用可能になる場合があります。 2.発生日時 2020年5月30日（土曜）12時55分頃 3.対象エリア 関西、中国、四国、九州地方の一部 4.原因 確認中 5.復旧見込み 確認中 お知らせ 全ての新着情報 製品の新着情報 サービス・機能の新着情報 料金・割引の新着情報 お客様サポートの新着情報 企業情報の新着情報 その他の新着情報 重要なお知らせ（通信障害等） ドコモからのお知らせ 報道発表資料 工事のお知らせ RSS（XML）データ配信 ・令和２年５月 30 日 19 時 45 分、お知らせに「一部エリアで sp モードでのインターネット接続等が利用できない状況について」（最終報）を掲載。  ドコモからのお知らせ 【お詫び/回復】一部エリアでspモードでのインターネット接続等が利用しづらい状況について 2020年5月30日 (2020年5月30日 午後7時45分更新) 平素は弊社商品、サービスをご利用いただき、誠にありがとうございます。 2020年5月30日（土曜）12時55分頃より、一部エリアのお客様においてspモードでのインターネット接続等がご利用しづらい事象が発生しておりましたが、18時32分に復旧いたしました。 なお、ご利用の機種を再起動（電源OFF/ON）または機内モード設定・設定解除していただくことで、ご利用可能となります。 お客様には大変ご迷惑をおかけしましたことを深くお詫び申し上げます。 今後とも弊社のサービス・商品をご愛顧賜りますようお願い申し上げます。 お知らせ 全ての新着情報 製品の新着情報 サービス・機能の新着情報 料金・割引の新着情報 お客様サポートの新着情報 企業情報の新着情報 その他の新着情報 重要なお知らせ（通信障害等） ドコモからのお知らせ 報道発表資料 工事のお知らせ RSS（XML）データ配信
	報道発表	なし
	その他	なし

ウ　西日本電信電話(株)の重大な事故

事業者名	西日本電信電話株式会社	発生日時	令和２年６月 29 日 12 時 11 分頃
継続時間	①２時間 36 分 ②４時間 21 分	影響利用者数	①135,000 回線 ②8,000 回線 ※緊急通報を扱う音声伝送役務は、故障中に使用しなかった者も含めた、故障した設備配下の全利用者の数を影響利用者数とする。
影響地域	①石川県（金沢市、かほく市、河北郡の一部エリア） ②兵庫県（丹波市の一部エリア）	事業者への問合せ件数	①発信：43 件、着信：93 件 ②発信：９件、着信：18 件 （令和２年 10 月６日 16 時時点）
障害内容	「ひかり電話」サービス回線から、「ひかり電話ゲートウェイ」に接続する交換機に収容される加入電話回線に対する新規着信が不可となる障害及び当該「ひかり電話ゲートウェイ」に接続する交換機に収容される他の加入電話回線に誤着信する障害が発生した。 着信側の加入電話回線には一部の緊急通報受理機関が含まれており、「ひかり電話」からの緊急通報が着信不可となっていた。		
重大な事故に該当する電気通信役務の区分	ー：緊急通報を取り扱う音声伝送役務（IP 電話）		
発生原因	「ひかり電話ゲートウェイ」の更改工事を委託していた株式会社エヌ・ティ・ティ ネオメイト（以下、ネオ社）の事前作業において、当該「ひかり電話ゲートウェイ」と当該交換機に誤ったデータが設定されていた。 また、データ作成後のデータ確認および試験において、ネオ社作成の業務マニュアルの確認項目に具体的かつ詳細な記載が不足していたため、設計や試験において必要作業の漏れが発生し、データ不一致を発見することができなかった。また、業務マニュアルの具体的な記載内容については、業務を実施するネオ社で作成しており、西日本電信電話株式会社では詳細な記述内容までの確認をしていなかった。		

機器構成図	新規着信が不可となる障害  他の加入電話回線に誤着信する障害 

<table>
<tr><td colspan="2">再発防止策</td><td>【事前作業における対策】
（１）ネオ社工事部門にて、ソフト設計データ作成時は、ソフト設計データを２名の作業者がそれぞれ作成し、それらの差分をプログラムにより自動的にチェックし、データの正常性を確認することを、ネオ社作成の業務マニュアルとして定める。（令和２年７月 22 日実施済）
（２）自動動作確認試験機を西日本電信電話株式会社にて新たに導入し、ネオ社にてそれを用いて動作確認試験を行う。（令和２年７月 22 日実施済）
（３）ソフト設計データの確認を行う作業者に対して、今回の事案の発生原因を改めて示しつつ、新たな業務マニュアルを用いて重点ポイントを解説する研修説明会を実施し、教育を行う。（令和２年７月 27 日実施済）
（４）物理構成が基本方針と異なる場合は、通常の情報伝達とは別に、ネオ社ハード設計者からネオ社ソフト設計者に対して、基本方針と異なる箇所を明示し、情報伝達を実施。（令和２年７月 27 日実施済）

【切替時における対策】
・切替作業直前に、ネオ社にて自動動作確認試験機による最終確認を行い、正常性を再確認した後に切替作業を行う。（令和２年８月６日実施済）</td></tr>
<tr><td>情報周知</td><td>自社サイト</td><td>事故の影響を受けた利用者に対する通信料の取扱いのお知らせ

２０２０年７月３日
西日本電信電話株式会社

6月29日に石川県・兵庫県の一部エリアにおいて発生した電話サービスの故障の影響を受けたお客様に対する通信料の取扱いについて

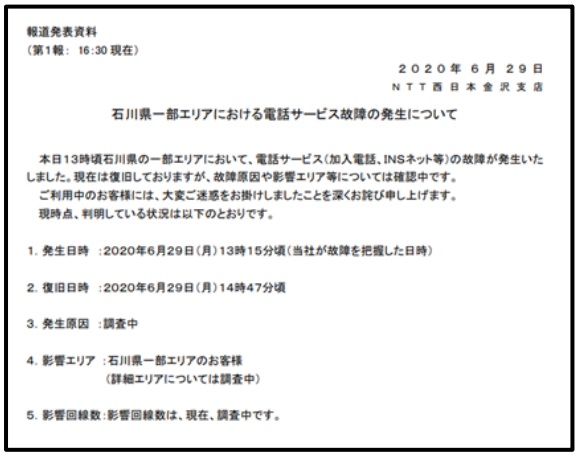
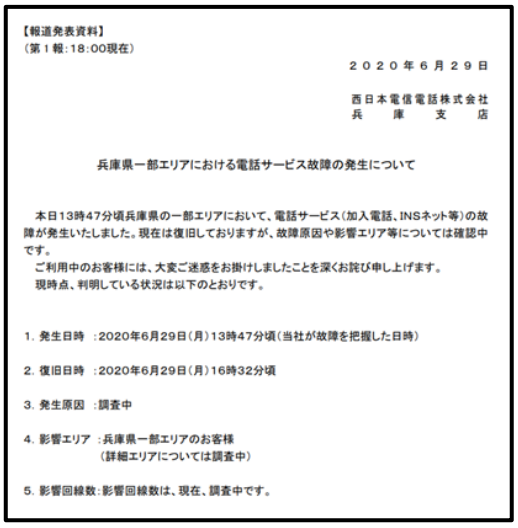
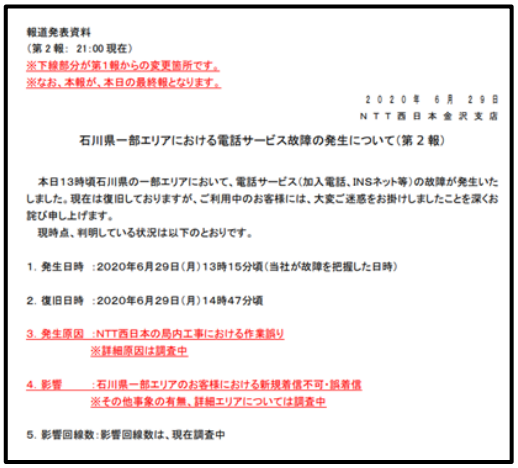
6月29日13時頃に石川県、兵庫県の一部エリアにおいて、電話サービス（加入電話、INSネット等）の故障が発生いたしました。現在は復旧しておりますが、ご利用中のお客様には、大変ご迷惑をお掛けしましたことを深くお詫び申し上げます。
西日本電信電話株式会社（以下、NTT西日本）は、このたびの事象に伴い、影響のあったお客様の対象の通信料につきまして、以下の通りの対応とさせていただくことといたします。

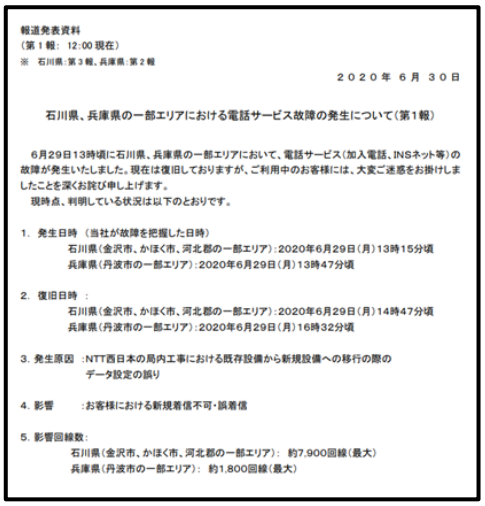
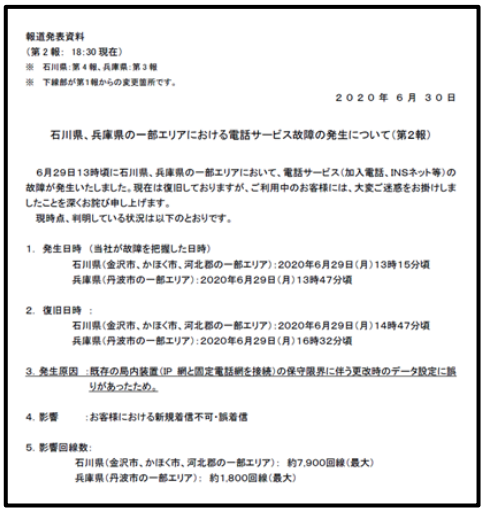
1．発生した事象
既存の局内装置（IP 網と固定電話網を接続）の保守限界に伴う更改時のデータ設定誤りに起因する、電話サービスの故障がございました。その影響により新規着信不可・誤着信が発生したお客様がございました。発生日時および復旧日時は以下のとおりです。

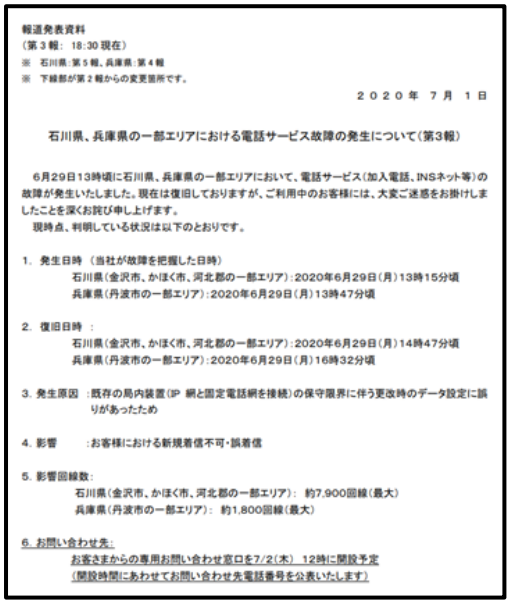
・発生日時 （当社が故障を把握した日時）：
石川県（金沢市、かほく市、河北郡の一部エリア）：2020年6月29日（月）13時15分頃
兵庫県（丹波市の一部エリア）：2020年6月29日（月）13時47分頃
・復旧日時：
石川県（金沢市、かほく市、河北郡の一部エリア）：2020年6月29日（月）14時47分頃
兵庫県（丹波市の一部エリア）：2020年6月29日（月）16時32分頃

2．通信料の取り扱い
事象の起因となる当該作業の開始時刻まで遡り、復旧までの時間帯で対象エリアへ通話・FAX 送信を行った結果、誤着信にもかかわらず通信料が発生したお客様につきまして、当該通信料を、後日の請求にて減算させていただきます。
具体的な実施方法等につきましては、改めてお知らせいたします。

以 上</td></tr>
</table>

	報道 発表	【障害情報】 ・金沢支店 HP 第１報：６月 29 日 16 時 30 分現在の情報を掲載  報道発表資料 （第1報： 16:30 現在） ２０２０年６月２９日 ＮＴＴ西日本金沢支店 石川県一部エリアにおける電話サービス故障の発生について 本日13時頃石川県の一部エリアにおいて、電話サービス（加入電話、INSネット等）の故障が発生いたしました。現在は復旧しておりますが、故障原因や影響エリア等については確認中です。 ご利用中のお客様には、大変ご迷惑をお掛けしましたことを深くお詫び申し上げます。 現時点、判明している状況は以下のとおりです。 1. 発生日時 ：2020年6月29日（月）13時15分頃（当社が故障を把握した日時） 2. 復旧日時 ：2020年6月29日（月）14時47分頃 3. 発生原因 ：調査中 4. 影響エリア ：石川県一部エリアのお客様 （詳細エリアについては調査中） 5. 影響回線数：影響回線数は、現在、調査中です。 ・兵庫支店 HP 第１報：６月 29 日 18 時 00 分現在の情報を掲載  【報道発表資料】 （第１報：18：00現在） ２０２０年６月２９日 西日本電信電話株式会社 兵　庫　支　店 兵庫県一部エリアにおける電話サービス故障の発生について 本日13時47分頃兵庫県の一部エリアにおいて、電話サービス（加入電話、INSネット等）の故障が発生いたしました。現在は復旧しておりますが、故障原因や影響エリア等については確認中です。 ご利用中のお客様には、大変ご迷惑をお掛けしましたことを深くお詫び申し上げます。 現時点、判明している状況は以下のとおりです。 1. 発生日時 ：2020年6月29日（月）13時47分頃（当社が故障を把握した日時） 2. 復旧日時 ：2020年6月29日（月）16時32分頃 3. 発生原因 ：調査中 4. 影響エリア ：兵庫県一部エリアのお客様 （詳細エリアについては調査中） 5. 影響回線数：影響回線数は、現在、調査中です。 ・金沢支店 HP 第２報：障害が復旧した旨を周知  報道発表資料 （第２報： 21:00 現在） ※下線部分が第1報からの変更箇所です。 ※なお、本報が、本日の最終報となります。 ２０２０年 ６月 ２９日 ＮＴＴ西日本金沢支店 石川県一部エリアにおける電話サービス故障の発生について（第２報） 本日13時頃石川県の一部エリアにおいて、電話サービス（加入電話、INSネット等）の故障が発生いたしました。現在は復旧しておりますが、ご利用中のお客様には、大変ご迷惑をお掛けしましたことを深くお詫び申し上げます。 現時点、判明している状況は以下のとおりです。 1. 発生日時 ：2020年6月29日（月）13時15分頃（当社が故障を把握した日時） 2. 復旧日時 ：2020年6月29日（月）14時47分頃 3. 発生原因 ：NTT西日本の局内工事における作業誤り ※詳細原因は調査中 4. 影響 ：石川県一部エリアのお客様における新規着信不可・誤着信 ※その他事象の有無、詳細エリアについては調査中 5. 影響回線数：影響回線数は、現在調査中

	報道 発表	・公式 HP 第１報：障害が発生、復旧した旨を周知  報道発表資料 （第１報：12:00 現在） ※ 石川県：第３報、兵庫県：第２報 ２０２０年６月３０日 石川県、兵庫県の一部エリアにおける電話サービス故障の発生について（第1報） 6月29日13時頃に石川県、兵庫県の一部エリアにおいて、電話サービス（加入電話、INSネット等）の故障が発生いたしました。現在は復旧しておりますが、ご利用中のお客様には、大変ご迷惑をお掛けしましたことを深くお詫び申し上げます。 現時点、判明している状況は以下のとおりです。 1. 発生日時 （当社が故障を把握した日時） 石川県（金沢市、かほく市、河北郡の一部エリア）：2020年6月29日（月）13時15分頃 兵庫県（丹波市の一部エリア）：2020年6月29日（月）13時47分頃 2. 復旧日時 ： 石川県（金沢市、かほく市、河北郡の一部エリア）：2020年6月29日（月）14時47分頃 兵庫県（丹波市の一部エリア）：2020年6月29日（月）16時32分頃 3. 発生原因 ：NTT西日本の局内工事における既存設備から新規設備への移行の際のデータ設定の誤り 4. 影響 ：お客様における新規着信不可・誤着信 5. 影響回線数： 石川県（金沢市、かほく市、河北郡の一部エリア）： 約7,900回線（最大） 兵庫県（丹波市の一部エリア）： 約1,800回線（最大） ・公式 HP 第２報：発生原因を周知  報道発表資料 （第２報：18:30 現在） ※ 石川県：第４報、兵庫県：第３報 ※ 下線部が第1報からの変更箇所です。 ２０２０年６月３０日 石川県、兵庫県の一部エリアにおける電話サービス故障の発生について（第2報） 6月29日13時頃に石川県、兵庫県の一部エリアにおいて、電話サービス（加入電話、INSネット等）の故障が発生いたしました。現在は復旧しておりますが、ご利用中のお客様には、大変ご迷惑をお掛けしましたことを深くお詫び申し上げます。 現時点、判明している状況は以下のとおりです。 1. 発生日時 （当社が故障を把握した日時） 石川県（金沢市、かほく市、河北郡の一部エリア）：2020年6月29日（月）13時15分頃 兵庫県（丹波市の一部エリア）：2020年6月29日（月）13時47分頃 2. 復旧日時 ： 石川県（金沢市、かほく市、河北郡の一部エリア）：2020年6月29日（月）14時47分頃 兵庫県（丹波市の一部エリア）：2020年6月29日（月）16時32分頃 3. 発生原因 ：既存の局内装置（IP 網と固定電話網を接続）の保守限界に伴う更改時のデータ設定に誤りがあったため。 4. 影響 ：お客様における新規着信不可・誤着信 5. 影響回線数： 石川県（金沢市、かほく市、河北郡の一部エリア）： 約7,900回線（最大） 兵庫県（丹波市の一部エリア）： 約1,800回線（最大） ・公式 HP 第３報：お客様問い合わせ窓口開設予定の旨を周知

報道発表資料
（第３報：18:30 現在）
※　石川県：第５報、兵庫県：第４報
※　下線部が第２報からの変更箇所です。

２０２０年　７月　１日

石川県、兵庫県の一部エリアにおける電話サービス故障の発生について（第3報）

6月29日13時頃に石川県、兵庫県の一部エリアにおいて、電話サービス（加入電話、INSネット等）の故障が発生いたしました。現在は復旧しておりますが、ご利用中のお客様には、大変ご迷惑をお掛けしましたことを深くお詫び申し上げます。
現時点、判明している状況は以下のとおりです。

1. 発生日時　（当社が故障を把握した日時）
石川県（金沢市、かほく市、河北郡の一部エリア）：2020年6月29日（月）13時15分頃
兵庫県（丹波市の一部エリア）：2020年6月29日（月）13時47分頃

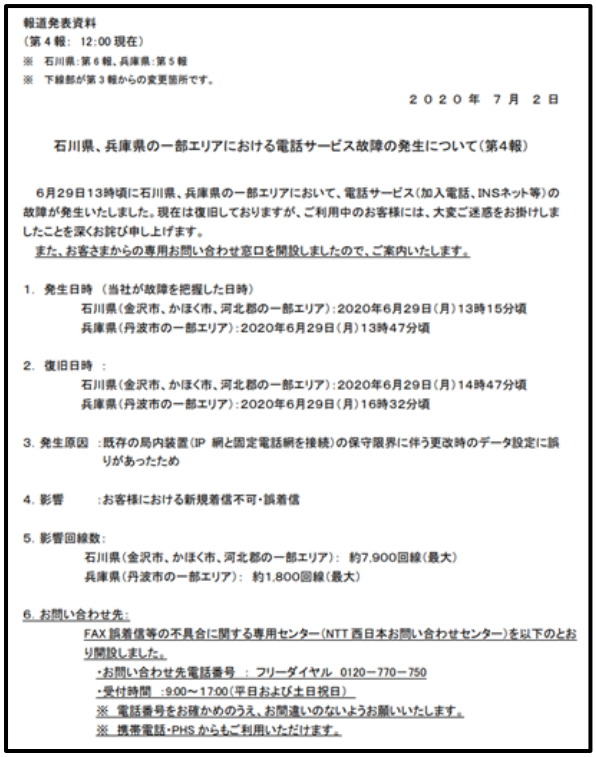
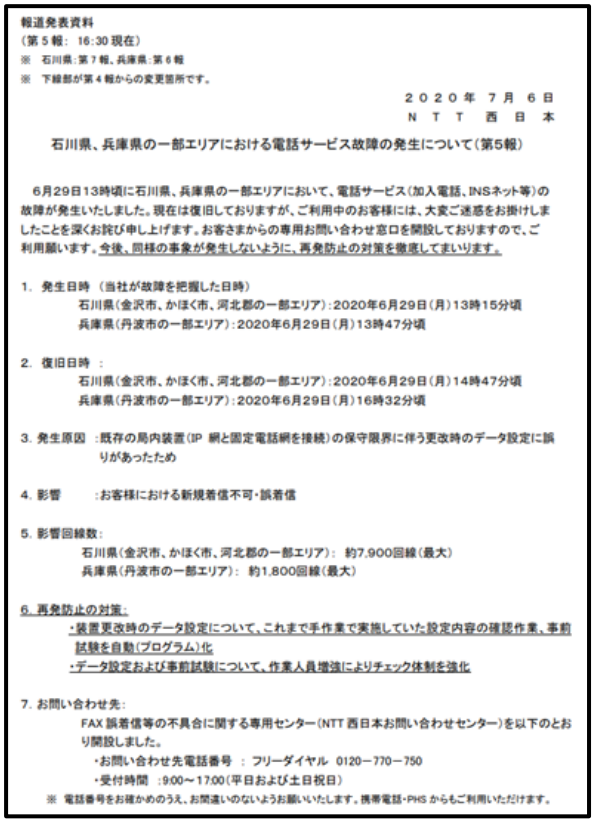
2. 復旧日時　：
石川県（金沢市、かほく市、河北郡の一部エリア）：2020年6月29日（月）14時47分頃
兵庫県（丹波市の一部エリア）：2020年6月29日（月）16時32分頃

3. 発生原因　：既存の局内装置（IP 網と固定電話網を接続）の保守限界に伴う更改時のデータ設定に誤りがあったため

4. 影響　　：お客様における新規着信不可・誤着信

5. 影響回線数：
石川県（金沢市、かほく市、河北郡の一部エリア）：　約7,900回線（最大）
兵庫県（丹波市の一部エリア）：　約1,800回線（最大）

6. お問い合わせ先：
お客さまからの専用お問い合わせ窓口を7/2（木）　12時に開設予定
（開設時間にあわせてお問い合わせ先電話番号を公表いたします）

	報道 発表	・公式 HP 第４報：お客様問い合わせ窓口開設の旨を周知  ・公式 HP 第５報：再発防止策を周知 

報道発表資料
（第４報：12:00 現在）
※　石川県：第６報、兵庫県：第５報
※　下線部が第３報からの変更箇所です。

２０２０年７月２日

石川県、兵庫県の一部エリアにおける電話サービス故障の発生について（第4報）

6月29日13時頃に石川県、兵庫県の一部エリアにおいて、電話サービス（加入電話、INSネット等）の故障が発生いたしました。現在は復旧しておりますが、ご利用中のお客様には、大変ご迷惑をお掛けしましたことを深くお詫び申し上げます。
また、お客さまからの専用お問い合わせ窓口を開設しましたので、ご案内いたします。

1. 発生日時（当社が故障を把握した日時）
石川県（金沢市、かほく市、河北郡の一部エリア）：2020年6月29日（月）13時15分頃
兵庫県（丹波市の一部エリア）：2020年6月29日（月）13時47分頃

2. 復旧日時：
石川県（金沢市、かほく市、河北郡の一部エリア）：2020年6月29日（月）14時47分頃
兵庫県（丹波市の一部エリア）：2020年6月29日（月）16時32分頃

3. 発生原因：既存の局内装置（IP 網と固定電話網を接続）の保守限界に伴う更改時のデータ設定に誤りがあったため

4. 影響：お客様における新規着信不可・誤着信

5. 影響回線数：
石川県（金沢市、かほく市、河北郡の一部エリア）：約7,900回線（最大）
兵庫県（丹波市の一部エリア）：約1,800回線（最大）

6. お問い合わせ先：
FAX 誤着信等の不具合に関する専用センター（NTT 西日本お問い合わせセンター）を以下のとおり開設しました。
・お問い合わせ先電話番号：フリーダイヤル 0120－770－750
・受付時間：9:00～17:00（平日および土日祝日）
※　電話番号をお確かめのうえ、お間違いのないようお願いいたします。
※　携帯電話・PHS からもご利用いただけます。

報道発表資料
（第５報：16:30 現在）
※　石川県：第７報、兵庫県：第６報
※　下線部が第４報からの変更箇所です。

２０２０年７月６日
ＮＴＴ西日本

石川県、兵庫県の一部エリアにおける電話サービス故障の発生について（第5報）

6月29日13時頃に石川県、兵庫県の一部エリアにおいて、電話サービス（加入電話、INSネット等）の故障が発生いたしました。現在は復旧しておりますが、ご利用中のお客様には、大変ご迷惑をお掛けしましたことを深くお詫び申し上げます。お客さまからの専用お問い合わせ窓口を開設しておりますので、ご利用願います。今後、同様の事象が発生しないように、再発防止の対策を徹底してまいります。

1. 発生日時（当社が故障を把握した日時）
石川県（金沢市、かほく市、河北郡の一部エリア）：2020年6月29日（月）13時15分頃
兵庫県（丹波市の一部エリア）：2020年6月29日（月）13時47分頃

2. 復旧日時：
石川県（金沢市、かほく市、河北郡の一部エリア）：2020年6月29日（月）14時47分頃
兵庫県（丹波市の一部エリア）：2020年6月29日（月）16時32分頃

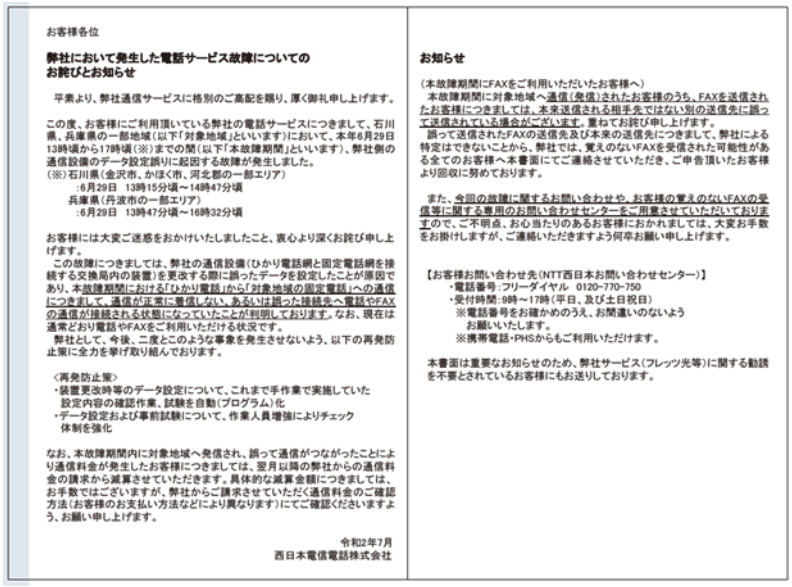
3. 発生原因：既存の局内装置（IP 網と固定電話網を接続）の保守限界に伴う更改時のデータ設定に誤りがあったため

4. 影響：お客様における新規着信不可・誤着信

5. 影響回線数：
石川県（金沢市、かほく市、河北郡の一部エリア）：約7,900回線（最大）
兵庫県（丹波市の一部エリア）：約1,800回線（最大）

6. 再発防止の対策：
・装置更改時のデータ設定について、これまで手作業で実施していた設定内容の確認作業、事前試験を自動（プログラム）化
・データ設定および事前試験について、作業人員増強によりチェック体制を強化

7. お問い合わせ先：
FAX 誤着信等の不具合に関する専用センター（NTT 西日本お問い合わせセンター）を以下のとおり開設しました。
・お問い合わせ先電話番号：フリーダイヤル 0120－770－750
・受付時間：9:00～17:00（平日および土日祝日）
※　電話番号をお確かめのうえ、お間違いのないようお願いいたします。携帯電話・PHS からもご利用いただけます。

		※公式 HP に掲載の④～⑨については、金沢支店 HP・兵庫支店 HP においても掲載
	その他	事故の影響を受けた利用者に対する通信料の取扱いに関するＤＭ 

お客様各位

弊社において発生した電話サービス故障についての
お詫びとお知らせ

平素より、弊社通信サービスに格別のご高配を賜り、厚く御礼申し上げます。

この度、お客様にご利用頂いている弊社の電話サービスにつきまして、石川県、兵庫県の一部地域（以下「対象地域」といいます）において、本年6月29日13時頃から17時頃（※）までの間（以下「本故障期間」といいます）、弊社側の通信設備のデータ設定誤りに起因する故障が発生しました。
（※）石川県（金沢市、かほく市、河北郡の一部エリア）
　　：6月29日　13時15分頃～14時47分頃
　兵庫県（丹波市の一部エリア）
　　：6月29日　13時47分頃～16時32分頃

お客様には大変ご迷惑をおかけいたしましたこと、衷心より深くお詫び申し上げます。
　この故障につきましては、弊社の通信設備（ひかり電話網と固定電話網を接続する交換局内の装置）を更改する際に誤ったデータを設定したことが原因であり、本故障期間における「ひかり電話」から「対象地域の固定電話」への通信につきまして、通信が正常に疎通しない、あるいは誤った接続先へ電話やFAXの通信が接続される状態になっていたことが判明しております。なお、現在は通常どおり電話やFAXをご利用いただける状況です。
　弊社として、今後、二度とこのような事象を発生させないよう、以下の再発防止策に全力を挙げ取り組んでおります。

〈再発防止策〉
・装置更改時等のデータ設定について、これまで手作業で実施していた
　設定内容の確認作業、試験を自動（プログラム）化
・データ設定および事前試験について、作業人員増強によりチェック
　体制を強化

なお、本故障期間内に対象地域へ発信され、誤って通信がつながったことにより通信料金が発生したお客様につきましては、翌月以降の弊社からの通信料金の請求から減算させていただきます。具体的な減算金額につきましては、お手数ではございますが、弊社からご請求させていただく通信料金のご確認方法（お客様のお支払い方法などにより異なります）にてご確認くださいますよう、お願い申し上げます。

令和2年7月
西日本電信電話株式会社

お知らせ

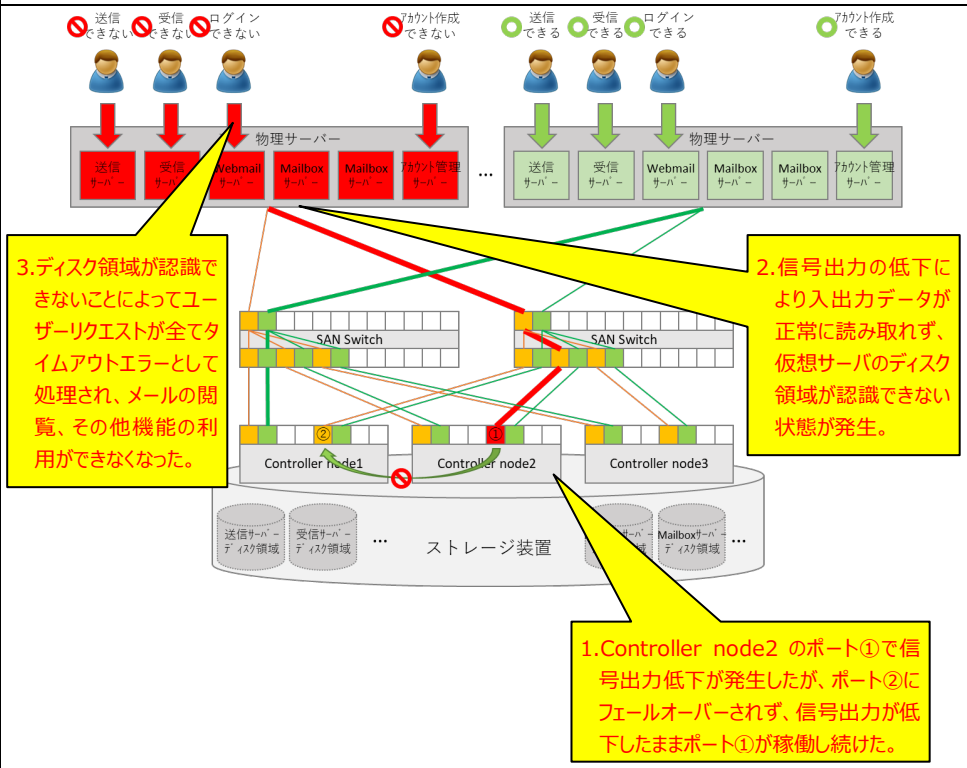
（本故障期間にFAXをご利用いただいたお客様へ）
　本故障期間に対象地域へ通信（発信）されたお客様のうち、FAXを送信されたお客様につきましては、本来送信される相手先ではない別の送信先に誤って送信されている場合がございます。重ねてお詫び申し上げます。
　誤って送信されたFAXの送信先及び本来の送信先につきまして、弊社による特定はできないことから、弊社では、覚えのないFAXを受信された可能性がある全てのお客様へ本書面にてご連絡させていただき、ご申告頂いたお客様より回収に努めております。

　また、今回の故障に関するお問い合わせや、お客様の覚えのないFAXの受信等に関する専用のお問い合わせセンターをご用意させていただいておりますので、ご不明点、お心当たりのあるお客様におかれましては、大変お手数をお掛けしますが、ご連絡いただきますよう何卒お願い申し上げます。

【お客様お問い合わせ先（NTT西日本お問い合わせセンター）】
　・電話番号：フリーダイヤル　0120-770-750
　・受付時間：9時～17時（平日、及び土日祝日）
　　※電話番号をお確かめのうえ、お間違いのないようお願いいたします。
　　※携帯電話・PHSからもご利用いただけます。

本書面は重要なお知らせのため、弊社サービス（フレッツ光等）に関する勧誘を不要とされているお客様にもお送りしております。

エ　フリービット(株)

事業者名	フリービット株式会社	発生日時	令和２年７月 31 日　２時 58 分
継続時間	８時間７分	影響利用者数	106,027 人
影響地域	全国	事業者への問合せ件数	電話 30 件、メール 15 件 （令和２年８月 19 日時点）
障害内容	仮想基盤のストレージ装置の FC ポートの一つで信号出力低下が発生。これにより仮想サーバ群の入出力応答がタイムアウトし、ファイルシステムが OS から認識できない状態になったため、メールの閲覧、その他機能の利用が不可となった。		
重大な事故に該当する電気通信役務の区分	五：一の項から四の項までに掲げる電気通信役務以外の電気通信役務 （インターネット関連サービス（有料）（電子メール））		
発生原因	ストレージ装置の FC ポートの一つで信号出力低下が発生したことにより仮想サーバ群の入出力応答がタイムアウトし、ファイルシステムが OS から認識できない状態になったため、一部仮想サーバでメール送受信及びアカウント管理サービスが停止した。		
機器構成図			

再発防止策	①FC ポートの予防交換が可能なよう、FC ポートの故障予兆サインを監視する。【令和２年８月 11 日に対応済】 ②同様の障害に対し短時間で復旧できるよう、ハードウェアの健全性確認のチェック項目及び冗長系パスの手動切替手順を整備する。【令和２年８月 11 日に対応済】 ③利用者の収容規模に応じて、仮想サーバ別の復旧優先順位を整理し大規模な仮想サーバ再起動を想定した復旧手順書を整備する。また、上記の復旧手順が経年で陳腐化しないよう、定期的な構成変更の復旧手順書への取り込み方法を定め運用を開始する。【令和２年９月９日対応済】 ④FC ポートの信号出力低下時に適切にフェールオーバーするよう、発動条件を整理し適切な閾値設定を行う。【令和２年９月９日対応済】

情報周知	自社サイト	【障害情報】 ＜サービスプロバイダーへの障害周知＞ 第１報 7 月 31 日 03 時 32 分（障害発生の可能性を周知） お客様各位 2020年07月31日 フリービット株式会社 ネットワークオペレーションセンター 【速報】クラウドメールサービス　アラート検知のご報告 平素より弊社サービスをご利用頂き誠にありがとうございます。 障害もしくは障害に発展する可能性のあるアラートを検知致しました。 事象調査中につき、詳細は別途ご案内いたします。 お客様には大変ご迷惑をおかけいたしますことをお詫び申し上げます。 記 ■不具合詳細 1.発生時刻：　2020年07月31日(金)02時59分頃から 2.影響範囲：　クラウドメールサービスをご利用のお客様 以上 第２報 7 月 31 日 06 時 27 分（障害発生を周知） お客様各位 2020年07月31日 フリービット株式会社 ネットワークオペレーションセンター クラウドメールサービス　障害発生のご報告 平素より弊社サービスをご利用頂き誠にありがとうございます。 メールサービスの一部におきまして、サービスをご利用できない障害が発生しております。現在、復旧作業中です。 障害期間中、お客様には、大変ご迷惑お掛けしますことをお詫び申し上げます。 ※同一内容を重複して受信された場合はご容赦ください。 記 ■不具合詳細 1.発生時刻：　2020年07月31日(金)02時59分頃から 2.影響範囲：　クラウドメールサービスをご利用のお客様 3.障害原因：　ネットワーク障害 4.影響内容：　メールサービスの一部が利用できない 以上

第３報 7月31日 11 時 08 分（障害経過を周知）

お客様各位

2020年07月31日

フリービット株式会社
ネットワークオペレーションセンター

【速報】クラウドメールサービス　アラート検知のご報告(経過報告)

平素より弊社サービスをご利用頂き誠にありがとうございます。

ソフトウェア障害に起因するアラートを検知致しました。現在復旧対応中となります。

お客様には大変ご迷惑をおかけいたしますことをお詫び申し上げます。

記

■不具合詳細
1.発生時刻：　2020年07月31日(金) 02時59分頃から
2.影響範囲：　クラウドメールサービスをご利用のお客様
3.障害原因：　ソフトウェア障害
4.影響内容：　メールを送受信できない場合がある
　　Webメールにログインできない場合がある
5.復旧目途：　7月31日12時頃

以上

第４報 7月31日 12 時 09 分（障害が復旧した旨を周知）

お客様各位

2020年 7月31日

フリービット株式会社
ネットワークオペレーションセンター

クラウドメールサービス　障害復旧のご報告

平素より弊社サービスをご利用頂き誠にありがとうございます。

本日 02:59頃より11:50頃にかけまして、クラウドメールサービスにおきまして、メールが送受信できない障害が発生しておりましたが、現在は復旧しております。
障害期間中、お客様には大変ご迷惑をおかけいたしましたことをお詫び申し上げます。

記

■不具合詳細
1.発生時刻：　2020年07月31日(金) 02時59分頃
2.復旧時刻：　2020年07月31日(金) 11時50分頃
3.影響範囲：　クラウドメールサービスをご利用のお客様
4.障害原因：　ソフトウエア障害
5.影響内容：　メールを送受信できない場合がある
　　Webメールにログインできない場合がある

以上

報道発表	なし
その他	なし

（３）その他検証案件

ア　電気通信設備に関する情報の漏えいによる通信サービスの提供に支障を及ぼすおそれに関する事故

ある電気通信事業者において、サイバー攻撃が原因と考えられる電気通信設備に関する情報の漏えい等による通信サービスの提供に支障を及ぼすおそれのある事象が発生した。当該支障が発生した場合には重要インフラ分野事業者にも影響を与えるなど社会的な影響が大きい事故に発展するおそれがあったため、当該電気通信事業者に出席を要請し、本会議において取り上げたところである。

事業者名	―	発生日時	―
継続時間	―	影響利用者数	―
影響地域	全国	事業者への問合せ件数	―
事故の内容	① 不正な局が不正に通信設定することにより、正規局の通信が妨害されるおそれがあった。 ② 不正な局が不正に通信要求を行うことで、不正接続が行われるおそれがあった。		
発生原因	認証機能が十分でなかったこと、通信が暗号化されていなかったことにより、不正に通信設定・通信要求が可能な状態であったため。		
機器構成図	―		
再発防止策	認証機能・通信暗号化機能を追加		
情報周知	ユーザーに個別に連絡		

第２章　令和２年度に発生した事故から得られた教訓等

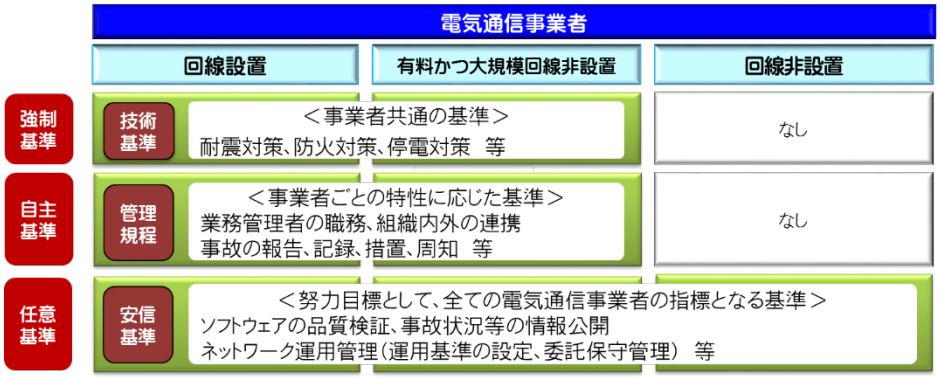
本章では、令和２年度に発生した事故の検証から得られた教訓等を、事故防止の一連の流れに対応して、「事故の事前防止」、「事故発生時」、「事故収束後」といった事故発生に係る段階ごとに整理している。その際、「平成 27 年度電気通信事故に関する検証報告」（以下「平成 27 年度報告」という。）、「平成 28 年度電気通信事故に関する検証報告」（以下「平成 28 年度報告」という。）、「平成 29 年度電気通信事故に関する検証報告」（以下「平成 29 年度報告」という。）、平成 30 年度電気通信事故に関する検証報告（以下「平成 30 年度報告」という。）及び令和元年度電気通信事故に関する検証報告（以下「令和元年度報告」という。）において、各年度に発生した事故の検証から得られた教訓等をまとめてきたところであるが、令和２年度も引続き、それら過去の教訓と類似の事故事案が発生していることから、過去の類似する教訓の内容も取り込みながら、教訓をまとめている。事業者においては、本章を参照し、同様な事故を起こさないよう、自社の取組に反映していくことを期待したい。

教訓等の取りまとめに当たっては、電気通信事業法上の事故防止に関する制度的枠組みを参照する。具体的には、図 22 のとおり

- 強制基準としての技術基準[14]（図 23）
- 事業者毎の特性に応じて定める自主基準としての管理規程[15]（図 24）
- 事業者における総合的な対策項目に関する推奨基準（ガイドライン）としての情報通信ネットワーク安全・信頼性基準[16]（以下「安信基準」という。）（図 25）

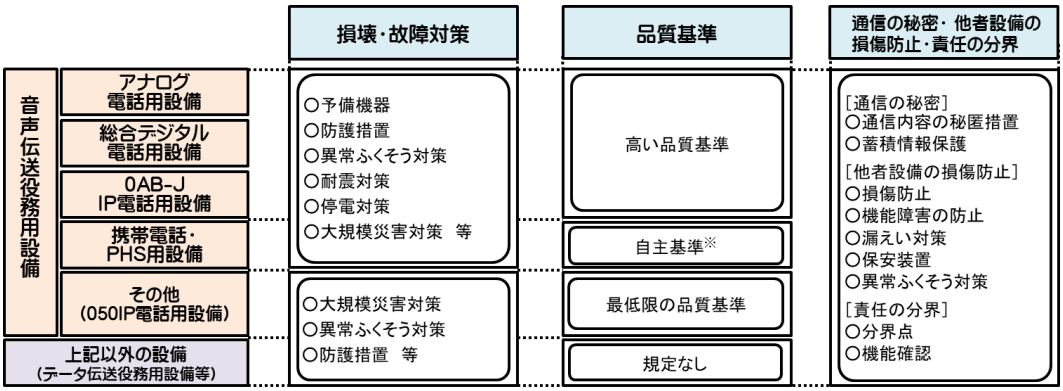
の関係する３つを参照する。

なお、以上の検証報告については、本会議のホームページ（URL：https://www.soumu.go.jp/main_sosiki/kenkyu/tsuushin_jiko_kenshou/index.html）に掲載している。



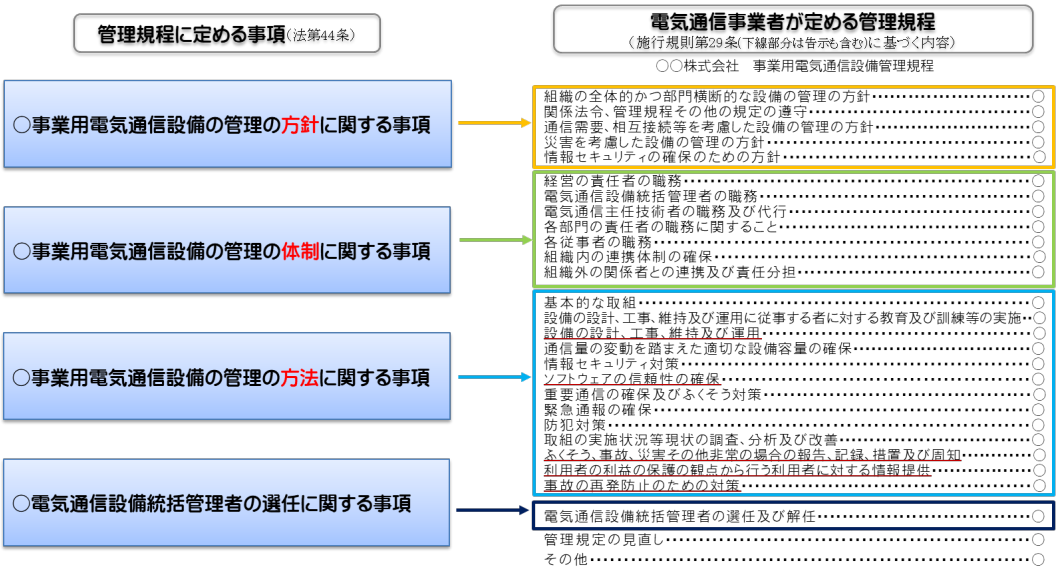
（図 22）安全・信頼性対策に関する制度的枠組み

[14] 事業用電気通信設備規則（昭和 60 年郵政省令第 30 号）
[15] 施行規則第 28 条
[16] 昭和 62 年郵政省告示第 73 号

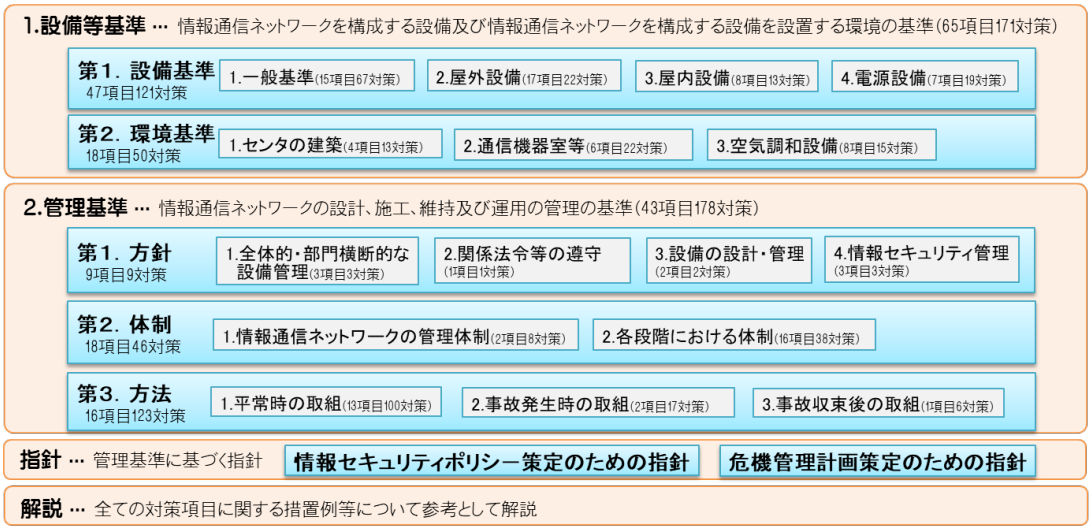


※ 携帯電話の品質基準は、電波の伝搬状態に応じて通話品質が影響を受けることを考慮し、基準を一律に定めるのではなく、自主基準としている。

（図 23）事業用電気通信設備の技術基準



（図 24）事業用電気通信設備の管理規程



（図 25）情報通信ネットワーク安全・信頼性基準

１．事故の事前防止の在り方

（１）手順書の遵守の徹底

障害復旧のための手順書を作成するだけでなく、手順書を遵守させるための取組を実施することが重要である。

＜事故事例＞

障害復旧のための手順書が作られていたにも関わらず、現場の判断によって手順書どおりに復旧作業がなされなかったため、復旧が遅れた事例があった。【新規事例】[17]

＜制度的枠組み＞

管理規程には、関係法令、管理規程その他の規定の遵守に関することを記載することとされ、その細目として、提供する電気通信役務に関する法令等（電気通信事業法等の関係法令、管理規程及び内部規程等）の定期的な確認及び遵守の徹底を盛り込むこととされている。

安全・信頼性基準では、
・保守・運用作業の手順化を行い、手順書の作成を行うこと
・復旧対策の手順化を行うこと
・サービス復旧のための手順及びとるべき措置を講ずること
がそれぞれ定められている。

＜教訓等＞

適切な障害復旧のためには、障害復旧の手順書を作成するだけでなく、障害発生時に手順書の記載内容が確実に実施されるよう、手順書の中でも重要なところは太字や赤字にし、必須の手順を明確にすることや、適切に手順書に従って進んでいるかを確認する進捗管理ツールを利用するなど、現場での作業者に対して手順を分かりやすく示し、手順書通りの作業を実施させるための工夫が重要である。【本年度新規】

---

[17] 以降、本章において用いる用語の説明。
＜事故事例＞
新規事例：過去に類似の事故が発生しておらず、令和元年度に新たに発生した重大な事故の事例。
平成〇年度にも見られた事例：過年度において類似の事故の事例があるもの。
＜教訓等＞
本年度新規：過去に類似の教訓等を挙げておらず、本報告書において新たに提示する教訓等。
平成〇年度報告に挙げた教訓等の再掲：過去の検証報告書において、類似の教訓等を示したもの。

（２）適切な機器の構成の検討

復旧手順の誤りも想定した上で、安全に復旧できるシステムの構成について検討を行うことが重要。

＜事故事例＞

ストレージ機器の故障が原因で、メールサービスの提供に支障が発生し、その際に、復旧の手順を誤り、認証ＤＢの正常性の確認を行わずにメールボックスの復旧を優先させたため、認証ができない状態でメールの配送が行われた結果、多くのメールが消失し、アーカイブから復旧する必要が発生したため、復旧に時間がかかる事例があった。【新規事例】

＜制度的枠組み＞

安信基準には、

・将来の規模の拡大、トラヒック増加（端末の挙動によるものを含む。）、インターネットの経路制御情報等の制御信号の増加及び機能の拡充を考慮した設計とすること。

等を定めている。

＜教訓等＞

今回の場合、認証ＤＢが落ちた場合に、メールボックスがメールを受け付けない仕組みになっていれば、認証ＤＢとメールボックスの復旧の順序を逆にしてもメールの消失が発生することはなかった。このように、復旧手順の誤りも想定した上で、安全に復旧できるシステムの構成について検討を行うことが重要である。【本年度新規】

（３）復旧手順書の作成

冗長化構成をとっていても障害が発生する場合を想定し、復旧の手順書を作成しておくことが重要。

＜事故事例＞

ストレージのハードウェア故障の検知するためのソフトウェアにバグがあったため、冗長化構成をとっていたものの、ハードウェア故障時の経路切替が正常に行われず、ストレージへのアクセスができなかったことから、通信障害が発生する事例があった。この際、ハードウェアとソフトウェアに同時に障害が発生することを想定しておらず、利用者への影響に配慮した復旧手順が確立されていなかったため、復旧に時間を要することになった。【平成 28 年度にも見られた事例】

＜制度的枠組み＞

管理規程では、故障設備に応じた定型的・類型的な応急復旧措置（一次措置）の速やかな実施に関することを記載することとされ、細目として
・事故事象に応じた定型的・類型的な応急復旧措置の内容
・事故事例に応じた項目の類型化を行うこと
・事故の要因分析を踏まえた、一次措置事項への反映に関すること。
と盛り込むこととされている。

安信基準では、
・委託事業者等を含めた関連部門間で工事手順書を作成するとともに、その内容の検証を行うこと。
・保全・運用作業の手順化を行い、手順書の作成を行うこと。
・情報通信ネットワークの維持及び運用に関して、現状の調査・分析結果を、必要に応じ、情報通信ネットワークの維持及び運用体制並びに手順書に反映させること。
等を定めている。

＜教訓等＞

冗長化構成をとっていても、何らかの原因により障害が発生する可能性はあるため、そういった場合も想定し、復旧の手順書を作成しておくことが重要である。【本年度新規】

また、事故の発生時の対応方針が、フェイルソフトの考え方に基づきサービスの継続を重視する方針である場合には、そのための具体的な手法・手順をあらかじめ定めておくことが重要である。【H28 年度報告に挙げた教訓の再掲】

（４）復旧措置の自動化

迅速な復旧のため、手動で行う手順について、自動化できる部分は自動化することが望ましい。

＜事故事例＞

電気通信事業者のシステム上においてストレージ故障が発生し、インターネットに接続しづらい事象が発生した。

故障したシステムとは別の、正常なシステムを接続先として追加するための作業手順書は確立されていたが、初めての対応となることや正常利用中の利用者への影響回避を前提とした作業の安全性確保等に時間を要し、復旧に時間を要した事例があった。【新規事例】

＜制度的枠組み＞

技術基準では、通信路の設定に直接係る交換設備の機器には、その機能を代替することのできる予備の機器を設置すること等、ネットワーク・設備の冗長構成を確保することを求めている。

管理規程には、事業用電気通信設備の設計、工事、維持及び運用に関することを記載することとされ、その細目として以下の項目を盛り込むこととされている。

・ 設備の冗長構成の確保、予備系への切替動作の確認及び予備系への切替不能時における対応に関すること
・ 経年劣化による自然故障等を考慮した、予備系への切替動作の確認も含めた、設備の定期的な点検・検査に関すること

安全・信頼性基準では、
・ 重要な電気通信設備においては冗長構成をとるようにすること
・ 冗長構成をとる電気通信設備においては、予備系への切替動作が確実に行われることを確認すること
・ 冗長構成をとる電気通信設備の予備系への切替えができなくなった場合の復旧手順をあらかじめ準備すること

等を定めている。

＜教訓等＞

本件では、故障が発生したシステムから正常なシステムへ切り替えるための措置が自動化されていれば、復旧に要する時間を半分程度に短縮することが可能であった。

このように、障害発生時に迅速にサービスを復旧させるためには、実際の障害事例を踏まえ、手動で行っている措置について自動化できるところがあるか、検討することが望ましい。【本年度新規】

（５）データ作成時の誤り防止の措置

設備の更改工事においてデータ設定を行う際、ヒューマンエラー防止の観点から、自動でデータを作成する仕組みや自動で入力チェック行う仕組みを検討することが重要。また、自動化が難しい場合には、設定値のダブルチェックを行うことが重要。

＜事故事例＞

設備の更改工事を行う際に、当該設備のハードウェアの設計が通常とは異なる物理構成になっていたところ、ソフトウェアの設計を別のグループ企業に委託していたこともあり、伝達が不十分だったことから、ソフトウェアの設計作業者が物理構成の違いを見落とし、誤ったデータを設定してしまったため、障害が発生する事例があった。【新規事例】

＜制度的枠組み＞

管理規程では、事業用電気通信設備の設計、工事、維持及び運用に関することとして、設備の設定におけるデータの誤設定及び誤入力防止並びに関連する設備間の設定の整合性に関することを記載することとされ、細目として、
・設備のデータ誤設定・誤入力防止のための取組
・設備間の設定値の整合性確保のための取組
を盛り込むこととされており、参考として、以下の項目が具体的な設定方法・確認方法の例として挙げられている。
・パラメータ投入の２人作業を行うこと
・設定値のダブルチェックを行うこと
・ルールに則った設定かどうかをチェックするツールの導入
・データのテンプレート化
・デフォルト値の設定を行う

また、安信基準においては、
・データ投入等における高い信頼性が求められる作業において、容易に誤りが混入しないよう措置を講ずること。
が定められている。

＜教訓等＞

設備の更改工事においてデータ設定を行う際、設計図面から手動で設定データを作成すると、伝達ミス等様々な要因から、誤ったデータを作成してしまう可能性がある。このようなヒューマンエラーの防止のため、作業者が扱いやすいデータフォーマットを用意し、自動的にデータ作成が行える仕組みを検討することが重要である。また、自動化が難しい場合には、設定値のダブルチェックを行う等、誤りが混入しないような措置を講ずることが重要である。【本年度新規】

（６）網羅的な試験の実施

緊急通報を扱う等、重要なサービスに用いる機器の設定変更後には、通話路の整合性の確認等、少なくとも影響が想定される範囲については接続試験を実施することが重要である。

＜事故事例＞

電話設備の更改工事において、切替え作業を実施した際に設定の誤りがあり、無音通話や誤着信が発生する事象があった。【新規事例】

＜制度的枠組み＞

管理規程では、事業用電気通信設備の設計、工事、維持及び運用に関することとして、設備の不具合を事前に発見するための設備の試験に関することを記載することとされ、細目として、
・設備の不具合を事前に発見するための試験
・設備の導入判定の基準
・機器等の製造・販売等を行う者から提供されるシステムの検査手法、品質評価手法の確認
を盛り込むこととされている。

安信基準では、
・設備の設定値の誤設定・誤入力防止のため、設定変更後には、実機に導入する前に確認試験を行うこと。
・設備の不具合を事前に発見するために次の試験を実施すること。
①デグレード試験
②過負荷試験
③商用環境に近い環境での試験
④品質の定量化試験
が定められている。

＜教訓等＞

緊急通報を扱う音声伝送役務等の重要なサービスに用いる機器の設定変更後には、様々なトラブルの発生の可能性を考慮し、各交換機を順番に繋ぐ等、少なくとも影響が想定される範囲について接続試験を行うことが重要である。【本年度新規】

（７）組織外の関係者との連携

ネットワーク・設備の運用維持管理に関しては、自社のみならず組織外の様々な者が関係することが多くなっていることから、これら組織外の関係者と適時適切に情報を共有するとともに、外部委託先を活用する場合には、定期的な業務報告、監査等の業務遂行のための仕組みを構築することが重要である。

＜事故事例＞

設備の更改工事を行う際に作業をグループ企業に外部委託していたが、作業内容について伝達が不十分であったことから電気通信事故が発生した。その際、更改工事を行っていた委託先とユーザー対応を行っていた委託元の連携が上手く取れず、事故の発見や対応が遅れた事例があった。【新規事例】

＜制度的枠組み＞

管理規程には、電気通信役務の確実かつ安定的な提供を確保するための事業用電気通信設備の管理の体制に関する事項として、組織外の関係者との連携及び責任分担に関することを盛り込むこととされている。

安全・信頼性基準では、平時及び事故発生時における社外関係者間の連携方針を策定するとともに、情報通信ネットワークを管理する上で、社外の関係者との連携体制及び責任の範囲を明確にすること、故障等における迅速な原因分析のための事業者と機器等の製造・販売等を行う者や業務委託先との連携体制を確立すること等を定めている。

＜教訓等＞

ソフトウェアのブラックボックス化、マルチベンダー化の進展、運用保守業務の外部委託の増加等、ネットワーク・設備の運用維持管理に当たり、組織外の関係者と密接に連携を図る必要性が増している。事故の発生時に一義的に利用者対応を行うのは電気通信事業者であるから、積極的に情報共有体制を構築する必要がある。ハードウェアやソフトウェアの障害情報について、ベンダー等との定期的な情報交換の場を設定したり、ベンダー等との保守契約をプロアクティブなものに見直すことが考えられる。

また、外部委託を行う場合は、定期的な業務報告、監査等の委託業務の適正性を確保するための仕組みを構築することが望ましい。【平成 27 年度報告に挙げた教訓の再掲】

（８）複数段のフェイルオーバーの仕組みの検討

仮想化システムの利用に当たっては、様々な故障を想定し、複数段のフェイルオーバーの仕組みを検討することが重要。

＜事故事例＞

ストレージ装置のポートの一つで信号出力低下が発生したことにより、仮想サーバの入出力応答がタイムアウトし、ファイルシステムがＯＳから認識できない状態になったことから、障害が発生した事例があった。本来であればストレージ装置からのアラートをきっかけにフェイルオーバーする仕組みであったが、ストレージ装置がアラートを出さなかったため、きっかけがなく、フェイルオーバーが行われなかった。【新規事例】

＜制度的枠組み＞

技術基準では、通信路の設定に直接関係する交換設備の予備機器の設置等を求めている。

管理規程には、事業用電気通信設備の設計、工事、維持及び運用に関することを記載することとされ、その細目として、設備の冗長構成の確保、予備設備への切替動作の確認及び予備設備への切替不能時における対応に関することを盛り込むこととされている。

安信基準では、
・現用及び予備機器の切替えを行うソフトウェアは十分な信頼性を確保すること
・重要な電気通信設備においては、冗長構成をとるようにすること
等を定めている。

＜教訓等＞

仮想化システムの利用に当たっては、装置からのアラートを検出し、フェイルオーバーするだけでなく、例えば、ファイルシステムが応答しなくなった際、別の系に切り替えられるように、ＯＳレベルから冗長化の構成を考えてシステム設計する等、複数段のフェイルオーバーの仕組みを検討することが重要。【本年度新規】

２．事故発生時の対応の在り方

（１）事故発生に関する適時適切な連絡や周知等の徹底

重大な事故の可能性のある事故の発生時における総務省に対する適時適切な報告・連絡や周知が必要。

＜事故事例＞

コロナ禍の中で輪番での勤務を行っており、その中で利用者への対応、パートナーの対応を行っているため、総務省への報告の必要性に思い至らず、報告が 20 日以上遅れる事例があった。【平成 29 年度にも見られた事例】

その後、本件に対する責任者会議の中で、総務省に対する報告が必要かを確認する指示があり、確認の結果、総務省への報告が必要な事案であることが判明したため、総務省への報告を行った。【新規事例】

＜制度的枠組み＞

電波法第 28 条には、重大な事故が発生したときは、その旨をその理由又は原因とともに、遅滞なく、総務大臣に報告することが定められている。

電気通信事業法施行規則第 57 条には、重大な事故が発生した場合に、速やかにその発生日時及び場所、概要、理由又は原因、措置模様その他参考となる事項について適当な方法により報告するとともに、事故発生日から 30 日以内に、その詳細について報告することが定められている。

「電気通信事故に係る電気通信事業法関係法令の適用に関するガイドライン（第５版）」には、重大な事故発生後、第一報として発生日時、発生場所、影響を与えた役務の内容、影響を与えた範囲、影響を与えた利用者数（以下「影響利用者数」という。）、発生原因、措置模様、利用者からの申告状況その他参考となる事項を速やかに総務省へ報告しなければならないことが記載されている。

＜教訓等＞

事故発生時においては　、まずは事故が発生している旨、総務省への報告を速やかに行うことが必要である。【本年度新規】

一方で、責任者会議の中で総務省への報告の必要性について指摘され、確認の結果、報告が必要な事例であることが判明したように、事故発生時の対応について適切な内部統制がとられていることが望ましい。【本年度新規】

また、責任者会議等は事故後速やかに開催し、対応を協議することが重要である。【本年度新規】

（２）障害発生時の責任者等への確認

担当者が、障害等の事象に遭遇した場合は、上長等の有識者・責任者及び関係部署に確認を行い、しかるべき判断を仰ぐことが重要。

＜事故事例＞

データセンターの担当者とコントロールセンターの担当者が別の場所にいたことにより、連携がうまく取れず、急いで復旧作業を行う中で、誤った手順により復旧作業がなされ、障害が長期化した事例があった。【新規事例】

＜制度的枠組み＞

管理規程には、事業用電気通信設備の管理の方法に関する事項として、当該設備の設計、工事、維持及び運用に関することを記載することが義務付けられており、その細目として、

・工事の手順書の適切な作成及び遵守並びに着工前における工事の手順書及び内容の確認に関すること

等を盛り込むこととされている

安信基準には、管理基準として、工事・設備更改における体制について、

・工事及び設備更改の実施に当たっては、作業の分担、連絡体制、責任の範囲等の管理体制を明確にすること（第２．２．（２）ア関係）
・工事及び設備更改の実施に当たっては、委託業者を含む関連部門間での連携を図り、作業手順を明確にするとともに、監督を行うこと（第２．２．（２）ウ関係）

また、平常時における工事の方法について、

・委託事業者等を含めた関連部門間で工事手順書を作成するとともに、その内容の検証を行うこと（第３．１．（４）ア関係）
・工事中に発生する可能性がある事故等に対して、復旧手順をあらかじめ準備すること（第３．１．（４）ウ関係）
・設備更改時に必要となる作業をあらかじめまとめておくこと（第３．１．（４）オ関係）

等を定めている。

＜教訓等＞

障害発生時に担当者同士が離れた場所にいる場合であっても、連携を取りつつ復旧作業を行うことが重要である。【本年度新規】

作業を行っていた担当者が、障害等の事象に遭遇した場合には、上長等の有識者・責任者や関係部署に確認を行い、指示を受けるなど、しかるべき判断を仰ぐことが重要である。【令和元年度報告に挙げた教訓の再掲】

（３）速やかな利用者への情報提供

事故発生時における利用者への情報提供は、速やかに、かつ利用者が状況を正確に理解できるように実施することが重要である。

＜事故事例＞

発生した事象の影響の対象と範囲の確認に時間を要し、第１報の発出に時間がかかる事例があった。【平成 27 年、平成 28 年、平成 29 年、平成 30 年、令和元年にも見られた事例】

また、端末の OFF/ON でサービスが利用可能になる状態になった後、速やかにその旨について利用者に周知を行った事例があった。【新規事例】

＜制度的枠組み＞

管理規程では、利用者の利益の保護の観点から行う利用者に対する情報提供に関することを記載することが義務付けられており、その細目として以下の項目を盛り込むこととされている。

・情報提供の時期に関すること
・情報提供窓口、ホームページ等における情報掲載場所の明確化に関すること
・利用者が理解しやすい情報の提供に関すること
・情報提供手段の多様化に関すること
・速やかな情報提供のための関係者間の連携に関すること

また、安信基準においては、

・平時及び事故発生時における担当部門間の連携方針を策定すること。
・事故・ふくそうが発生した場合には、その状況を速やかに利用者に対して公開すること。
・情報通信ネットワークの事故・障害の状況を適切な方法により速やかに利用者に対して公開すること。
・事故情報の利用者への提供窓口、方法、場所等に関する情報はあらかじめ利用者に周知すること。
・情報の提供方法については利用者が理解しやすいように工夫すること。
・情報提供の手段を多様化すること。

等を定めている。

＜教訓等＞

事故発生時には、利用者に対して速やかな情報提供が求められ、事故原因の特定や被疑箇所の特定ができていない状況においても、不明のため周知を行わないということではなく、まずは事故・障害が発生している旨の第一報を発出すべきである。【平成 27 年度及び平成 28 年度報告に挙げた教訓の再掲】

その後、事故の原因特定や復旧状況に進捗があった場合には、随時情報を更新して途中経過も含めて周知することが好ましい。なお、事故対応においては、状況が判明していくことにより情報が変化して行くことが想定されるが、既報に

誤りが認められるなど、途中で事象の変化が認められた際には、事象の変化の前後を明らかにした情報を提示することが望ましい。【平成 28 年度報告に挙げた教訓の再掲】

また、利用者側の対策によりサービスの利用が可能になる方法が見つかった場合、それを速やかに利用者に周知することが重要である。【本年度新規】

情報提供の方法として、ホームページへの掲載以外に、自社事業の特性を生かしてコミュニティチャンネルや SNS の公式アカウントから情報を発信した事例があった。多様な媒体を用いて事故の発生状況等の情報提供を行うことは、利用者が情報に接することのできる機会を増やし、正確な情報を届ける方法として有益であることから、このような取組を継続していくことが重要である。【平成 28 年度報告に挙げた教訓の再掲】

ある事故事案では、利用者が増加する夕方から夜間にかけて事故が発生し、深夜に復旧したものがある。そのため利用者が障害・復旧状況等の情報を確認できたのは翌朝以降であったと考えられるが、ホームページの障害情報を早期に削除してしまうと、利用者が状況を確認することができなくなってしまうため、障害の状況、経緯については、復旧後２日程度は掲載しておくことが望ましい。また、障害・復旧状況等の情報は、トップページ内にリンクを掲載する等、利用者が容易に確認できるようにしておくことが好ましい。【平成 28 年度報告に挙げた教訓の再掲】

なお、事故の原因が特定され、復旧した段階の情報提供においては、利用者が現状を正確に把握できる情報を発信すべきであり、事故の原因についても正しく伝え、誤解を招くことのない表現とすべきである。【平成 27 年度報告に挙げた教訓の再掲】

３．事故収束後のフォローアップの在り方

（１）教育・訓練の徹底

訓練をしっかりと行うことに加え、訓練が形骸化しないよう、実際の環境を再現しての訓練を行う等の工夫を行うことが重要。

＜事故事例＞

復旧や利用者周知等を含めた障害訓練を毎年行っているが、実際の障害発生時に、個別の判断により手順どおり復旧されず、障害が発生した事例があった。【新規事例】

＜制度的枠組み＞

管理規程には、事業用電気通信設備の設計、工事、維持及び運用に従事する者に対する教育及び訓練等の実施に関することを記載することとされ、その細目として、

・教育・訓練の対象者、内容、実施体制、実施方法、実施頻度、実施計画及びその見直しに関すること
・法令に則った講習を電気通信主任技術者に受講させること

を盛り込むこととされている。

また、商用に近い環境での試験に関することを記載することとされ、その細目として、商用に近い環境や商用のトラヒックパターンを反映した試験の実施等を盛り込むこととされている。

安信基準には、

・情報通信ネットワークの円滑な運用に必要な知識及び判断能力を養うための教育・訓練を行うこと。
・設備の保全に関する知識を養うための教育・訓練を行うこと。
・商用環境に近い環境での試験

等を定めている。

＜教訓等＞

毎年訓練をやっていても、長らく事故がないことによる確認の甘さから、見落としが出てしまう場合がある。そういった見落としがないように訓練をしっかり行うとともに、重大な事故につながる規模の装置を扱う場合には、仮想的な障害復旧対応の訓練だけでなく、可能であれば、模擬環境を作り、そこで実際に模擬故障を起こしての訓練を行う、日常業務の一環として訓練を行う等、訓練が形骸化しないための工夫を行い、ＰＤＣＡサイクルを回すことが重要である。【今年度新規】

第３章　事故防止に向けたその他の取組

１．災害時における通信サービスの確保の在り方について

近年、我が国では、地震、台風、大雨、大雪、洪水、土砂災害、火山噴火等の自然災害が頻発しており、人的・物的に大きな被害を受けている。令和元年度は、９月には令和元年房総半島台風、10 月には令和元年東日本台風等、令和２年度は、令和２年７月豪雨、９月の令和２年台風第 10 号、令和２年 12 月～令和３年１月の大雪、２月の令和３年福島県沖を震源とする地震等によって全国各地で大きな被害が発生した。これら災害時には、停電による影響、通信設備の故障、ケーブル断等により、通信サービスにも大きな支障が生じた。

令和２年度は、平成 23 年３月に発生した東日本大震災の発災から 10 年となることから、東日本大震災以降の災害時における通信サービスの確保の在り方について、総務省及び電気通信事業者等による主な取組を紹介する。

（１）東日本大震災を踏まえた通信障害への対応等

東日本大震災では東日本全域に甚大な被害をもたらした。通信サービスでは、固定通信網は 385 の通信ビルの機能停止等により約 190 万回線が途絶し、携帯電話・PHS 基地局については、長時間停電等により合計約２万９千局が停波した。

この震災では、災害時に重要な役割を担う通信インフラに広範囲にわたる輻輳や通信途絶等の状態が生じたこと等を踏まえ、今後の大規模災害に対応するため、総務省では平成 23 年 12 月に「大規模災害等緊急事態における通信確保の在り方に関する検討会」において、「緊急事態における通信手段の確保の在り方」をとりまとめた。この最終とりまとめでは「アクションプラン」として、国・電気通信事業者等の各主体が今後取り組むべき事項として、

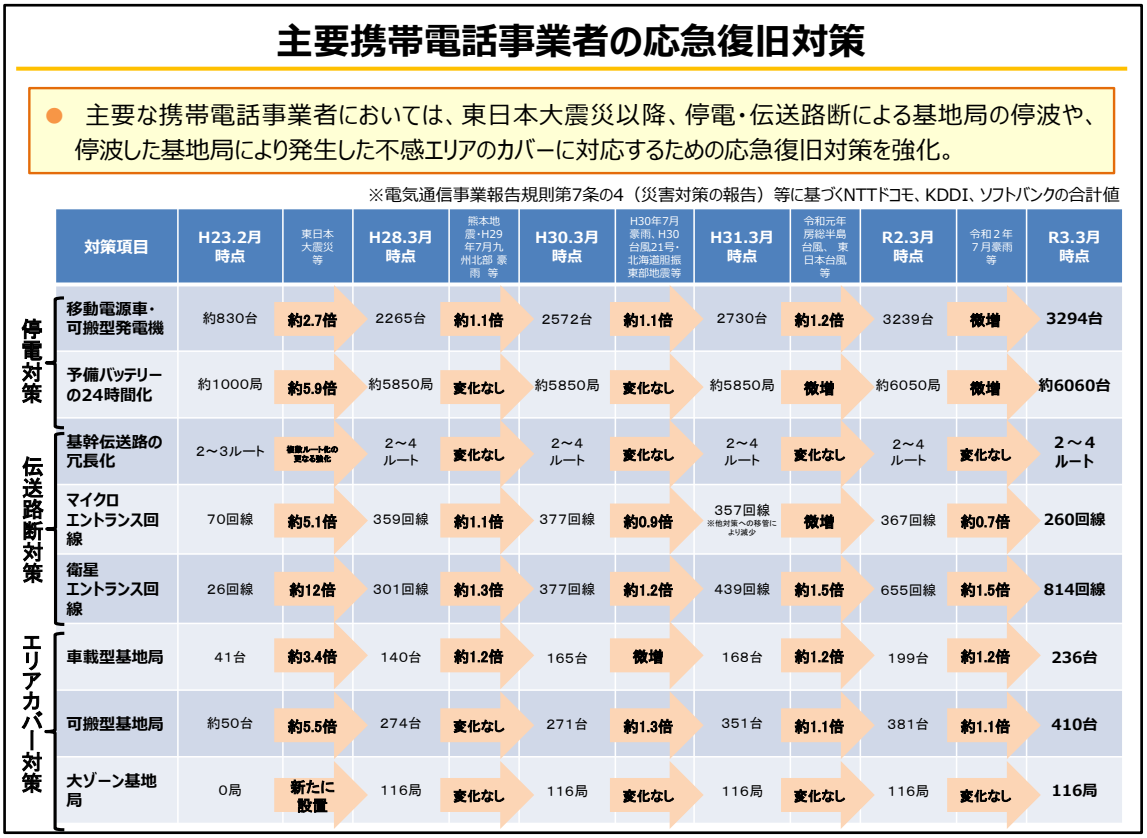
・災害時優先電話の安定的な利用確保
・災害用伝言サービスの高度化
・避難場所等における有効な通信手段の事前配備
・通信設備の種類・規模に応じた非常用電源確保（燃料確保を含む）の在り方
・ネットワークの安全・信頼性確保の在り方
・関係事業者における災害対応体制の検証・見直し
・インターネットのネットワークの構築の在り方

等が整理された。これらを踏まえ、総務省では平成 24 年７月に事業用電気通信設備規則等を改正し、

・自家用発電機や蓄電池の持続時間の長時間化
・交換設備相互間の複数経路化の徹底
・災害対策の実施状況等の報告制度

等を規定した。また、平成 24 年８月から、電気通信事業者が提供する災害用伝言板サービスの相互連携が開始され、各社利用者間での安否確認が可能となった。

なお、東日本大震災以降、携帯電話事業者においては応急復旧対策の強化が図られており、災害対策用通信機材の配備状況は図 26 のとおりである。



（図 26）携帯電話事業者における東日本大震災以降の災害対策の強化の状況

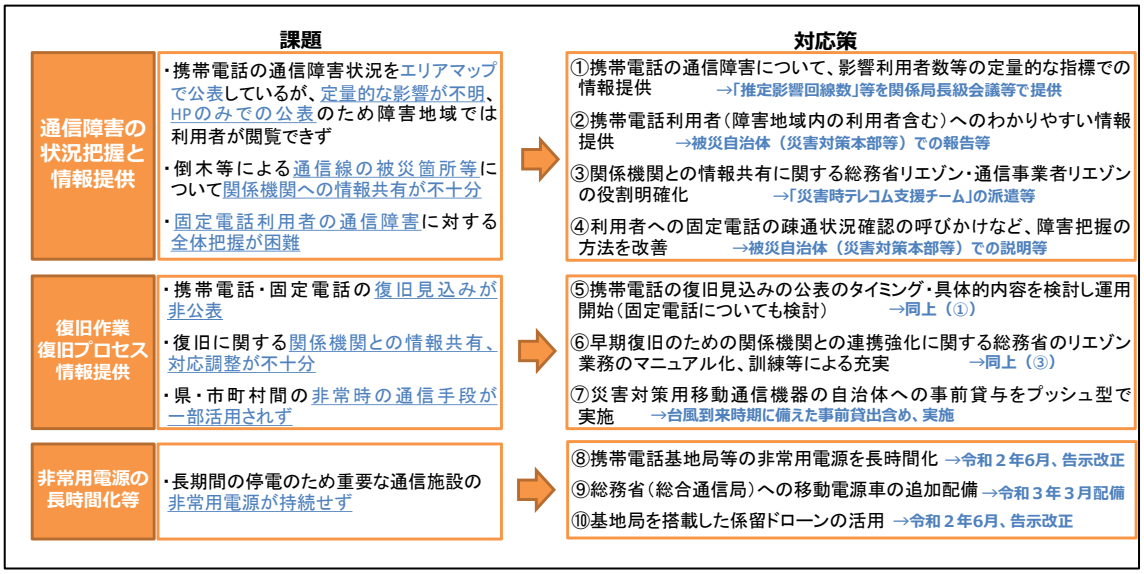
平成 30 年度は、平成 30 年７月豪雨、台風第 21 号、北海道胆振東部地震等の様々なタイプの災害が発生し、重要インフラに支障を来したことを踏まえ、政府において「重要インフラの緊急点検」や、緊急に実施すべきハード・ソフト対策を３年間で集中的に実施する「防災・減災、国土強靱化のための３か年緊急対策」が 12 月に取りまとめられたところであり、同年の検証報告ではこの点等が取り上げられたところである。

令和２年度の検証報告では平成 31 年（令和元年）度以降に発生した災害への対応を紹介する。

（２）令和元年房総半島台風等を踏まえた通信障害への対応等

令和元年９月に発生した房総半島台風では、強風による倒木等の影響により電柱の倒壊や通信ケーブルの断線等、甚大な被害が発生した。また、広域かつ長期間にわたる停電等によって、携帯電話基地局等における非常用電源が枯渇・機能停止し、台風通過後の約１日後となる９月 10 日にエリア支障が最大となる等、千葉県の約 40 の市町村の広範囲で長期間にわたる通信障害が発生した。

この房総半島台風やその後に発生した東日本台風等の一連の災害において課題となった長期停電及びその復旧プロセス、通信障害等その他の課題について検証を行うため、令和元年 10 月、政府において「令和元年台風第 15 号・第 19 号をはじめとした一連の災害に係る検証チーム」が設置され、有識者等による議論を経て、令和２年３月に最終とりまとめが行われ、通信障害関係における課題と対応策について、図 27 のとおり整理された。



（図 27）「令和元年台風第 15 号・第 19 号をはじめとした一連の災害に係る検証チーム」最終とりまとめ（令和２年３月）概要（通信障害関係）

他方、総務省においては、房総半島台風等における甚大な通信障害が発生したことを教訓に、通信インフラの耐災害性を強化するため、令和２年６月に「情報通信ネットワーク安全・信頼性基準」を改正し、都道府県庁、市役所及び町村役場の災害における重要な拠点をカバーする通信設備の予備電源について、少なくとも 24 時間にわたる停電対策に取り組むこと等を新たに規定するとともに、令和元年度補正予算により各総合通信局に災害対策用移動電源車等を追加配備した。

また、災害時における被災者等への情報提供を推進するため、通信がつながらなくなる場合に想定される故障等、通信事業者による早期復旧の取組み、電話がつながらなくなる場合に想定される原因とそれに対する一般利用者による対応策、通信事業者が提供する被災者向けサービス等に関するリーフレット「通信確保のための対応ガイド」を作成した。（図 28）

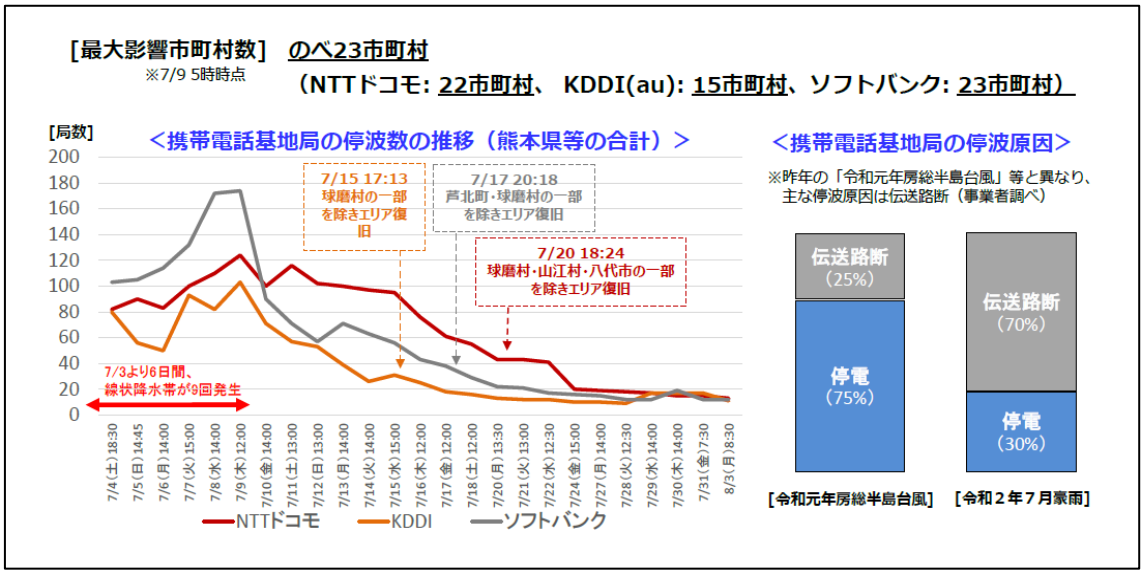
なお、令和２年６月には情報通信手段の確保に向けた災害対応支援を行うため、「総務省・災害時テレコム支援チーム（MIC-TEAM）」を立ち上げ、以降の災害時において順次派遣した。

（図 28）「通信確保のための対応ガイド」

（３）令和２年７月豪雨等を踏まえた通信障害への対応等

令和２年７月豪雨においては、携帯電話では、球磨川等の決壊や土砂崩れ等による道路崩壊や橋梁落下等により、携帯電話基地局同士をつなぐ基幹的な中継系伝送路の断線等による基地局の停波、固定電話では、多ルート化している両系の中継ケーブルの断線や水没等による通信ビルの機能停止が発生した。

７月３日以降の６日間、線状降水帯が９回発生したことに伴い、発災後６日後の７月９日に携帯基地局の停波局数が最大となる等、熊本県等の約 20 の市町村の広範囲で通信障害が発生するとともに、固定電話においても７月５日に最大 24 の通信ビルが機能停止した。



（図 29）「令和２年７月豪雨」による影響（携帯電話）

この７月豪雨等の総務省及び電気通信事業者における対応等を検証するため、総務省において「災害時における通信サービスの確保に関する連絡会」を開催した。本連絡会では、被災地域における情報提供、携帯基地局の停波原因の切り分け、伝送路故障による携帯基地局への被害等の把握等について、現状把握、今後の対応の方向性、具体的な対応策等を主要な通信事業者と議論した上で、令和３年４月、次の点を総務省リエゾン活動マニュアルに反映させること等として整理した。

・通信障害の状況及びその復旧見込みに関する住民への情報提供について、自治体と協議・調整しつつ広報車や防災行政無線の活用を検討すること
・被害を受けた通信設備が公設公営の場合、当該設備が迅速に復旧できるよう自治体の意向を確認すること
・電力を優先復旧させるための基地局の位置情報の提供方法について電柱番号もしくは契約番号とすること

なお、総務省では、大規模自然災害時において、被災した市町村役場における通信サービスを迅速に応急復旧させるとともに、通信の復旧における電力供給、燃料供給及び倒木処理等に関する課題に対応するため、地方自治体及び電気通信事業者等との間で、初動対応に関する連携訓練を令和２年度に実施し、これらの成果についても、今後の初動対応やリエゾン活動マニュアルへの反映させたところである。

近年、自然災害が激甚化・頻発化する中で、発災による通信サービスへの支障を完全に無くすことは現実的には困難である。しかしながら、被害の最小化、復旧の迅速化・効率化により、影響を最小限に留める取組を今後も継続して取り組んでいくことが重要であり、関係者における不断の取組に期待したい。

２．昨今の重要インフラ事業者に対するサイバー攻撃の事例について

通信事故の報告制度において、サイバー攻撃を原因とする通信事故については、平成 30 年度までは、四半期報告事故として報告される「外的要因」のうち「異常トラヒック」や「第三者要因」、「その他」等として報告されてきており、明確に把握できていなかったところである。そこで、サイバー攻撃のうち、特に通信事業者が設置する通信設備の機能に障害を与えるものについては、一定規模以上の通信サービスの停止や品質の低下による事故を引き起こす恐れがあることから、総務省が発生状況を把握した上で、政策等に的確に反映するため、令和元年度から、四半期報告事故における発生原因の分類として、新たに「送信型対電気通信設備サイバー攻撃」が追加されたところである。

以上の結果、令和元年度においては、送信型対電気通信設備サイバー攻撃を発生要因とする四半期報告事故が 8 件、また、令和２年度においては、同様に 13 件の報告があり、通信設備に対するサイバー攻撃が確認されたところである。また、令和２年度においては、第１章３．令和２年度重大な事故等の発生状況（３）で取り上げたとおり、サイバー攻撃が原因と考えられる電気通信設備に関する情報の漏えいによる通信サービスの提供に支障を及ぼすおそれに関する四半期報告事故のうち、当該支障が発生した場合には重要インフラ事業者にも影響を与えるなど重大な事故に該当する可能性のある事故も発生している。

以上の電気通信事業者を取巻くサイバー攻撃のリスクの深刻化等を踏まえ、通信設備へのサイバー攻撃に対する事前又は事後の対応を強化していく必要がある。電気通信事業者におけるサイバー攻撃に対する対応の参考として、内閣サイバーセキュリティセンターが事務局となっている「サイバーセキュリティ本部　重要インフラ調査会」が行った重要インフラにおける補完調査の資料[18]を、「参考３　重要インフラ事業者に対するサイバー攻撃の事例」として添付している。

参考３に挙げられているサイバー攻撃の事例の中でも、DDoS 攻撃については、電気通信事業者が被害にあった場合、当該攻撃に起因する異常トラヒックにより電気通信役務に使用するサーバがダウンし、電気通信サービスの提供に支障を来たす事態につながる可能性がある。
また、重要インフラ事業者の管理サーバへの不正アクセスについては、電気通信設備に関する情報が漏洩した場合、四半期報告事故の基準の１つである、「電気通信設備に関する情報であつて、電気通信役務の提供に支障を及ぼすおそれのある情報が漏えいした事故」に該当する可能性があるものである。

---

18 サイバーセキュリティ対策本部　重要インフラ専門調査会
https://www.nisc.go.jp/conference/cs/ciip/index.html

また、マルウェア感染についても同様に、電気通信設備に関する情報漏洩が発生した場合、四半期報告事故に該当する可能性がある。
また、本年５月には、ランサムウェアによる被害の結果米国のパイプラインが操業停止に追い込まれる事態が発生しており[19]、同様の被害が電気通信事業者において発生した場合、電気通信サービスが停止に追い込まれる事態が想定されるため、注意が必要な事例だと考えられる。

電気通信事故検証会議においても、これらサイバー攻撃による電気通信事故が発生した場合に検証を行っていくことが必要であり、今後もサイバー攻撃の事例について注視していく必要がある。

なお、これらのリスクの深刻化を踏まえ、「情報通信審議会 情報通信技術分科会 IP ネットワーク設備委員会 事故検証・報告制度等タスクフォース」において、サイバー攻撃を原因とする通信事故の報告制度等の在り方について検討が行われたところであり、検討結果について、次節で紹介を行っている。

表４　電気通信事業において発生した場合に電気通信サービスに影響を及ぼす可能性があると思われるサイバー攻撃の事例

類型	事例
DoS 攻撃・DDoS 攻撃	平成 27 年 ア DDoS 攻撃によるサービス障害
	平成 29 年 キ DDoS 攻撃
	平成 30 年 オ 脆弱性を悪用した攻撃
	平成 30 年 カ 広域 DoS 攻撃による Web サイト閲覧攻撃
	平成 30 年 キ 商用ネットワークの高負荷による通信障害
ランサムウェア	平成 28 年 ウ ランサムウェア被害
	平成 29 年 ア WannaCry によるサイバー攻撃
	令和２年 オ 重要インフラ事業者における２度のランサムウェア被害
	令和２年 カ 重要インフラ事業者における「WannaCry」の感染
マルウェア感染	平成 26 年 ウ 端末へのマルウェア感染
	平成 27 年 ウ USB メモリを介したマルウェア感染
	令和元年 オ 不審メールによるマルウェア「Emotet」への感染
不正アクセス	平成 28 年 エ 管理サーバへの不正アクセス
	平成 29 年 イ 認証の脆弱な IoT 機器への第三者アクセス
	平成 30 年 エ IoT デバイスへの不正侵入及び改ざん
	平成 30 年 ク 他人の認証情報の悪用による情報の不正取得
	令和元年 カ 重要インフラ事業者が利用するサーバへの不正アクセス
	令和元年 キ クラウド型メールサービスへの不正ログイン

[19] 米最大のパイプライン、操業停止　ランサムウェア攻撃で
https://www.asahi.com/articles/ASP592PNYP58ULFA008.html

３．令和時代における事故報告・検証等の在り方について

「令和元年度電気通信事故に関する検証報告」においては、電気通信事故検証会議の設置以降５年間における平成時代の総括とともに、令和時代における新たな動向を踏まえ、今後の電気通信事故の報告及び検証の在り方について検討が行われた。その結果、ニュー・ノーマルに対応したデジタル強靱化社会には、より安心・安全で信頼できる情報通信ネットワークの確保が必要不可欠とされ、電気通信事故の報告及び原因究明等の検証等を通じたPDCAによるリスクマネジメント等、マルチステークホルダー連携によるガバナンスの在り方に関する議論を深める必要性が提言されている。

これらの提言を踏まえ、安心・安全で信頼できる情報通信サービス・ネットワークの確保を図るため、令和３年３月から、「情報通信審議会　情報通信技術分科会　IP ネットワーク設備委員会」に設置された「事故報告・検証制度等タスクフォース（以下「ＴＦ」という。）」において、2020 年代半ばに向け、事故報告・検証制度等の在り方に関する検討が行われており、その主な概要を紹介する。

なお、本検討において、通信事故の検証制度の見直しの在り方として、検証会議の機能強化の必要性が挙げられており、検討結果を踏まえ、電気通信事故検証会議においても検討を行っていく必要がある。

（１）検討の経緯・進め方

ア　検討の背景・目的

通信サービス・ネットワークを取り巻く環境について、近年、①自然災害やサイバー攻撃等の発生自体が不可避なグローバルリスクの深刻化、②外国企業、スタートアップ等を含む多様な者による通信事業者やサービスの多様化、③with/after コロナに伴い益々浸透している遠隔・非接触サービスに不可欠なブロードバンドサービスやインターネット関連サービス等の通信サービスのユニバーサル化、④5G 本格展開等による他の重要インフラとの相互依存の深まり等の情報通信ネットワークの産業・社会基盤化、そして、⑤仮想化・ソフトウェア化等による情報通信ネットワークの構築・管理運用の高度化・マルチステークホルダー化等の変化が発生している。

新たな環境変化に伴い、通信事故の発生により生命・身体・財産に直接的な影響を与えるリスクも増大するなど、通信分野における安全・信頼性対策が取組むリスクが多様化・複雑化している。これらのリスクに適切に対応するためには、通信事業者による自主的な取組のみならず、関係する他の事業者、個人や法人等の利用者等のマルチステークホルダー間の連携・協力によるガバナンスを通じて、通信事故の防止や被害の拡大防止等に社会全体で取組むことが必要となっている。

そこで、国民生活、社会経済活動や危機管理等のために不可欠なインフラとして、安心・安全で信頼できる情報通信ネットワークが確保されるよう、2020 年代半ば頃に向けた、①事故報告・検証制度、②情報通信ネットワーク安全・信頼性基準等の在り方について検討を行うための作業班として、「事故報告・検証制度等タスクフォース」が開催されることとなった。

イ　現状・課題

通信事故の報告・検証制度については、全ての通信事業者（2021 年 4 月現在、約 2 万 2 千者）が対象になっている。そして、実際に発生した通信事故の報告・分析・評価等を通じ、通信サービス・ネットワークの安全・信頼性対策について、総務省が改めて検証し、再発防止等に向けた関係者の取組を継続的に充実・強化するために不可欠な PDCA サイクルの要となっている。

そこで、上記 PDCA サイクルを取り巻く環境として、近年、次の変化が進展することに伴い、当該サイクルが取組むリスクが多様化・複雑化しており、2020 年代半ば頃に向けた通信事故の報告・検証制度の在り方について、検討が必要となっている。

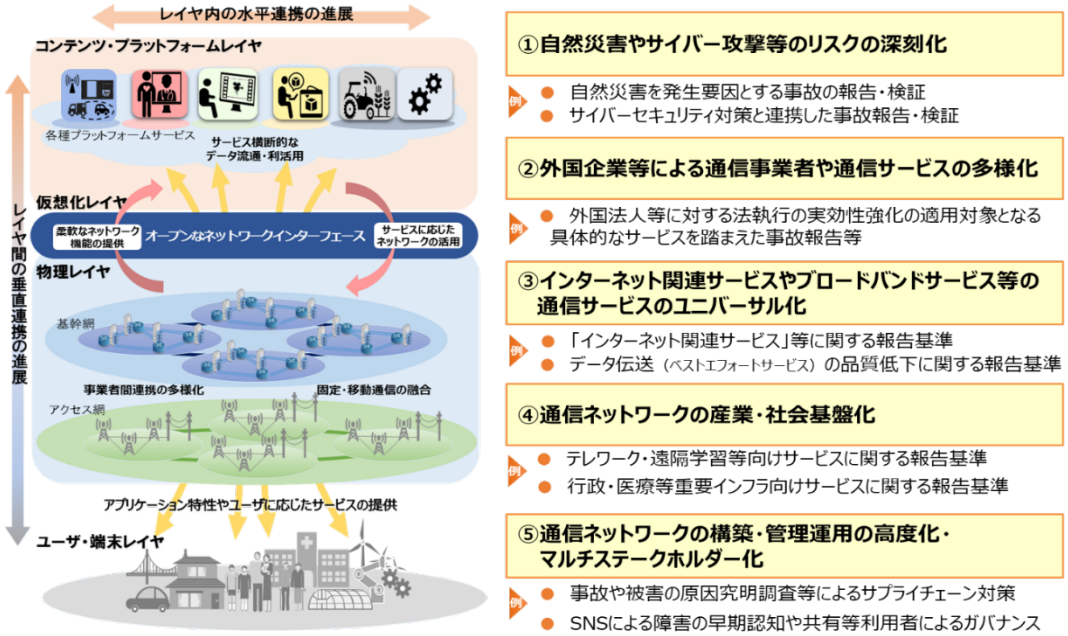
１）　自然災害やサイバー攻撃等の発生自体が不可避なグローバルリスクの深刻化

２）　外国企業、スタートアップ等を含む多様な者による通信事業者やサービスの多様化

３）　with/after コロナに伴い益々浸透している遠隔・非接触サービスに不可欠なブロードバンドサービスやインターネット関連サービス等の通信サービスのユニバーサル化

４）　5G 本格展開等による他の重要インフラとの相互依存の深まり等の情報通信ネットワークの産業・社会基盤化

５）　仮想化・ソフトウェア化等による情報通信ネットワークの構築・管理運用の高度化・マルチステークホルダー化



（図 30）通信事故の報告・検証制度を取巻く環境・リスクの変化と検討事項

ウ　通信事故の報告・検証制度の見直しに関する基本的な考え方

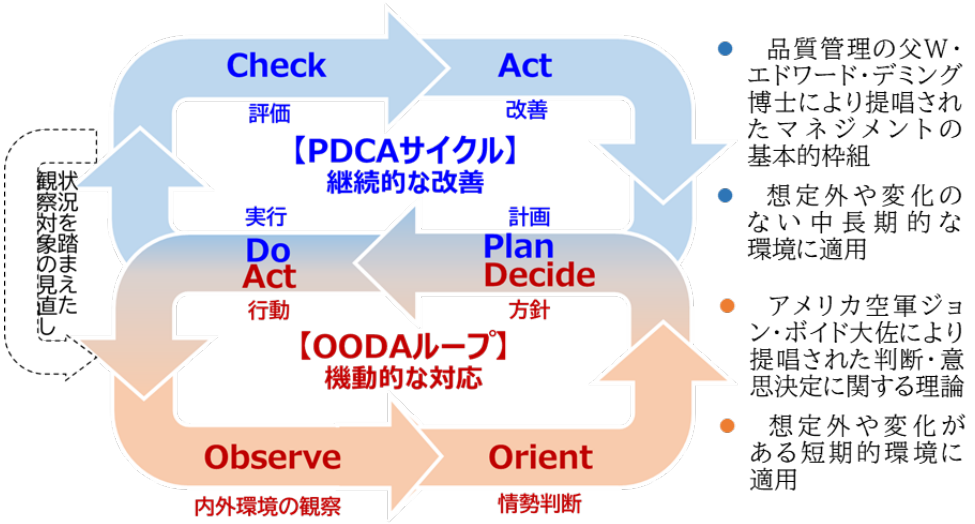
デジタル社会の実現のためには、その中枢基盤として、サイバー空間とフィジカル空間を繋ぐ神経網である通信サービス・ネットワークが安心・安全で信

頼され、円滑に（安定的かつ確実に）提供されることが不可欠である。そのため、通信サービス・ネットワークの安全・信頼性対策が極めて重要になると考えられる。

この点、本年 5 月に成立したデジタル社会形成基本法においては、基本理念として「国民が安全で安心して暮らせる社会の実現」（第 7 条）が規定されるとともに、デジタル社会の形成は民間が主導的役割を担うという原則の下、国等は民間の知見を積極的に活用して、環境整備を中心とした施策を行うとされ、例えば、サイバーセキュリティの確保や通信ネットワークの災害対策など国民が安心して高度情報通信ネットワークを利用できるようにするために必要な措置を講じる旨が規定されている。

以上を踏まえると、デジタル社会を支える中枢基盤である通信分野においては、イノベーションの進展が著しい中、通信事業者間のサービス競争も激しく、市場環境変化のスピードが速いこと等から、引続き、民間である通信事業者が主導的役割を担うことが必要と考えられる。

通信サービス・ネットワークの安全・信頼性対策の継続的な改善を図る PDCA サイクルは、車の両輪として、①OODA[20]ループ的な対応に関する重大事故の報告制度、②検証会議による重大事故等の検証制度かる構築されている。



【出典】㈱日本総合研究所・経営コラム「“VUCAの時代”のビジョンデザインと未来年表」（2018年09月14日 粟田恵吾）やチェット・リチャーズ著等「OODA LOOP」（東洋経済新報社）等を参考として事務局作成

（図 31）OODA ループによる PDCA サイクルの補強

これらのことから、VUCA[21]といわれる環境変化に伴うリスクの量的・質的な変化及び通信事業者以外も含むマルチステークホルダーへの拡散に対応するため、OODA ループ及びリスクマネジメントの考え方を踏まえ、2020 年代半ば頃に向け、

[20] OODA：Observe（内外環境の変化）、Orient（方向付け・情勢判断）、Decide（方針・意思決定）、Act（行動）の略であり、判断・意思決定に関する理論として、想定外や変化がある短期的環境に適用される考え方

[21] VUCA：Volatility（変動性）、Uncertainty（不確実性）、Complexity（複雑性）、Ambiguity（曖昧性）の略。

通信事業者が主導的役割を担うことができる環境整備が必要である。

エ　検討の方向性

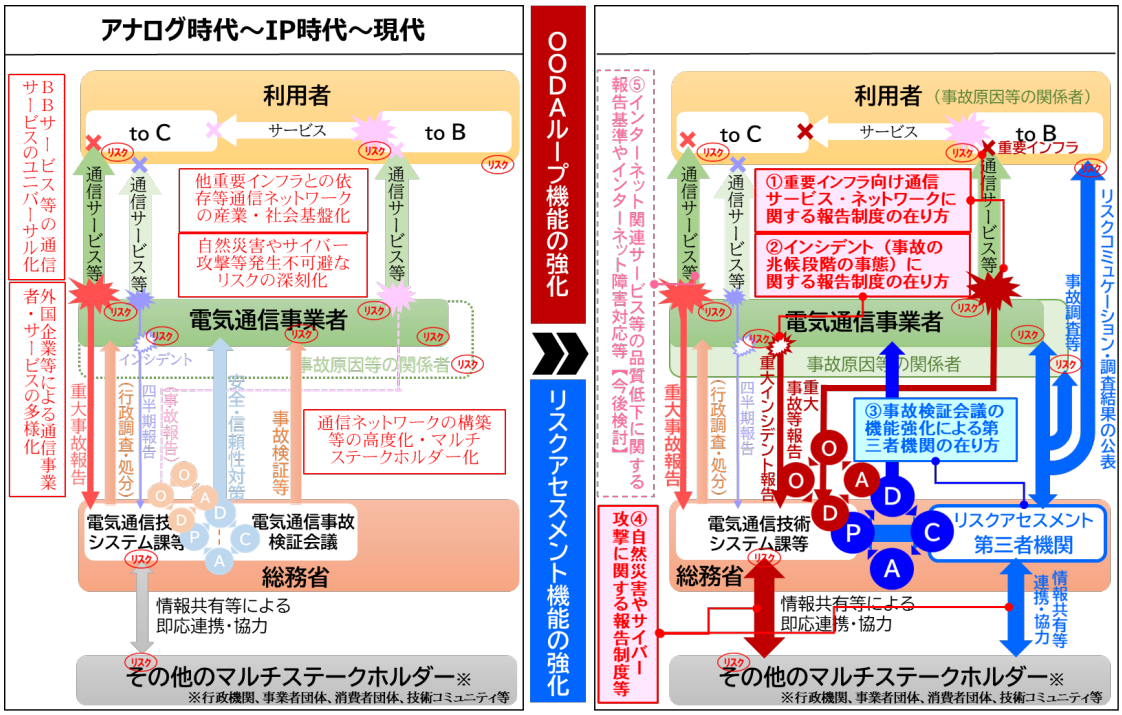
2020 年代半ば頃に向けて、デジタル社会における通信事故の防止や被害の拡大防止等という目的を達成するため、総務省においては、そのリーダーシップにより、マルチステークホルダーとの連携・協力を通じた統合を推進し、通信事業者が引続き主導的な役割を担うことができる環境を整備することが必要である。

具体的には、①重大なリスクの Observe（内外環境の観察）及び Orient（方向付け・情勢判断）による OODA ループ機能の強化、②重大なリスクに関するリスクアセスメント機能の強化の観点から、次の点を検討することが必要である。

１）　BtoB/GtoX（通信事業者ｔｏ法人利用者/行政機関ｔｏ一般利用者等。以下同じ。）型の通信サービス・ネットワークのうち、通信分野との相互依存が深まりつつある重要インフラ分野に提供される場合等の通信事故に関する報告制度の在り方

２）　リスクが顕在化したアクシデントではなく、その兆候段階の事態であるインシデントに関する報告制度の在り方

３）　事故調査を通じた演繹的なアプローチ等の電気通信事故検証会議の機能強化による第三者機関の在り方



（図 32）通信事故の報告・検証制度の見直しに関する基本的な方向性

（２）通信事故報告制度の見直しの在り方

ア　報告制度の概要

通信事故の報告制度においては、重大事故等の報告を契機として、総務省と

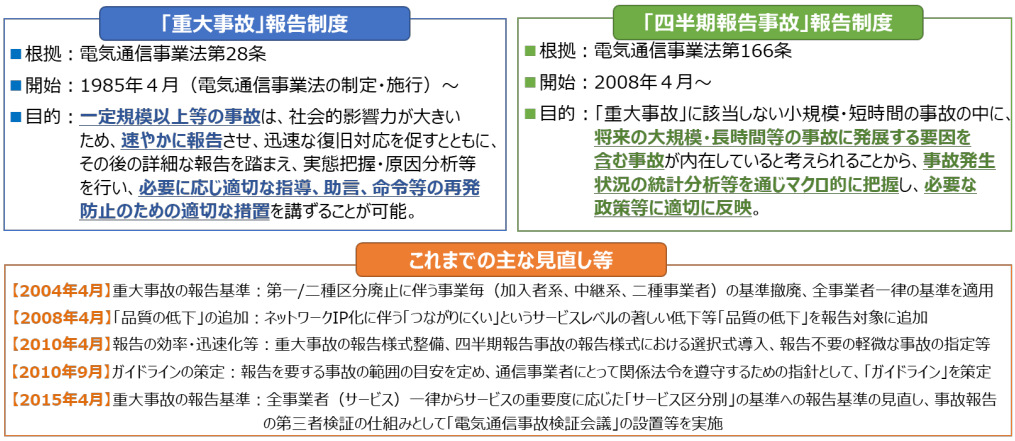
通信事業者等との即応連携等の OODA ループ的な対応により、通信サービス・ネットワークの円滑な（確実かつ安定的な）提供の確保と利用者利益の保護を図っている。また、検証会議と相俟って、重大事故等の分析・評価等を通じ、通信事故の事前防止や応急対応等の対策を検証し、再発防止や被害軽減等に向けた施策を充実・改善するために不可欠な安全・信頼性対策に関する PDCA サイクルの要となっている。

そして、回線設備設置事業者や有料で利用者 100 万以上のサービスを提供する回線設備非設置事業者等のみならず、無料サービス等を提供する海外事業者等の回線設備非設置事業者も含めた全ての通信事業者（2021 年 4 月現在、約 2 万 2 千者）が対象となっている。

この点、現行の報告制度においては、通信設備の故障による通信サービス・ネットワークの提供停止又は品質低下を対象として、リスクによる影響が顕在化した「アクシデント」、そして、アクシデントの兆候段階の事態である「インシデント」について、同じ「通信事故」として定義し、それらの報告を通信事業者に求めている。

以上のうち、重大なリスクによる影響が顕在化したアクシデントのみが「重大事故」と定義され、総務省と通信事業者等による即応連携等の OODA ループ的な対応の対象となっている。

従って、リスクの量的・質的な変化及びマルチステークホルダーへの拡散に対応するため、OODA ループ機能を強化する観点から、その対象となる重大事故の範囲やインシデントに関する報告の在り方等、報告制度について量的・質的にも見直すことが必要である。



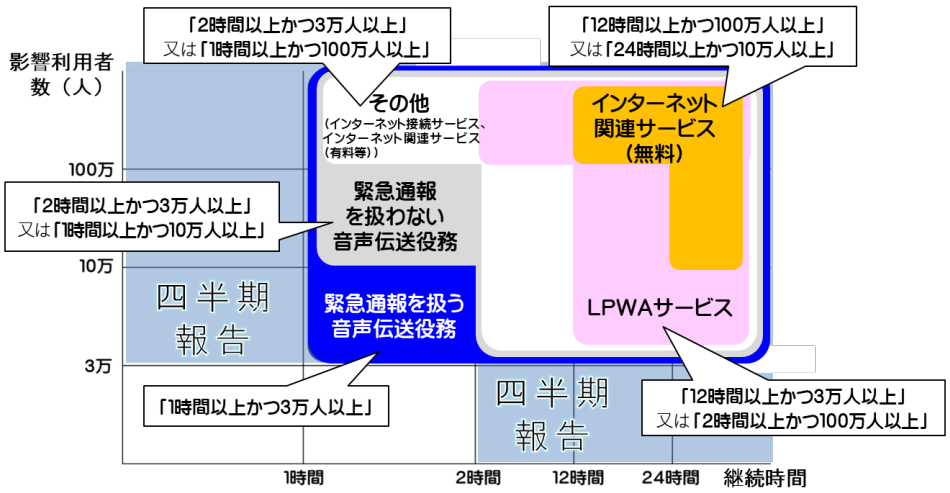
（図 33）事故報告制度のこれまでの主な見直し等について

● 通信事業者において、電気通信事業法※に基づき、総務大臣に対する報告を要する電気通信事故（電気通信設備の故障による電気通信役務の提供の停止又は品質の低下等）は、次の２つに大別。

① 重大な事故：１）サービス毎の影響利用者数・継続時間の基準（下図参照）に該当するもの、又は、
２）重要電気通信設備（衛星・海底ケーブル等）の故障により、全ての通信の疎通が２時間以上不能のもの
（→ 事故後、速やかに一報、30日以内に報告書を提出）

② 四半期報告事故：１）影響利用者数3万人以上又は継続時間2時間以上（電気通信設備以外の設備の故障により電気通信役務の提供に支障を来した事故を含む）、又は、
２）電気通信役務の提供に支障を及ぼす恐れのある電気通信設備に関する情報の漏えい（インシデント）
（→ 四半期ごとに報告）

※電気通信事業法28条・166条、同法施行規則58条、電気通信事業報告規則7条の3



（図 34）通信事故の報告制度の概要

イ　重要インフラ向け通信サービス・ネットワークに関する報告制度の在り方

昨今、通信事故から波及する金融分野等の重要インフラサービスの障害やクラウドサービス障害を原因とする通信事故が発生している。このような重大リスクが顕在化したアクシデントを定義する重大事故について、BtoB/GtoX型の通信サービス・ネットワークのうち、通信分野と相互依存が深まる重要インフラに提供されるものの通信事故に関する考え方等が不明確となっている。同様に、クラウドサービスが通信サービスに該当する場合、重要インフラである通信分野に提供される際のクラウドサービス障害に関する通信事故としての考え方等も不明確である。

これらのことから、重大なリスクに関する OODA ループ機能やリスクアセスメント機能の強化のため、報告制度を量的・質的に見直すことが必要である。また、重要インフラに提供される通信サービス等の通信事故について、総務省への速やかな報告に関する考え方の明確化や四半期報告事故にかかる報告事項の追加等、所要の制度整備が適当である。更に、通信サービス等に提供されるクラウドサービスの障害について、上記重要インフラに関する考え方、現行のガイドラインにおける通信事業者間に関する判断や外国法人等に関する適用の考え方を踏まえ、通信事故への該当性に関す考え方の現行ガイドラインによる明確化等が適当である。

ウ　インシデント（通信事故の兆候）に関する報告制度の在り方

令和２年度において、通信設備に関する情報が、サイバー攻撃により漏洩し、当該通信サービス等の利用者である重要インフラ事業者において、緊急時のための当該通信サービスが利用不可となるおそれのある事態等の重大なインシデントが発生した。

このインシデントについては、一部のみが四半期報告事故として対象となるが、通信事故として報告しない場合等が罰則規定の適用対象となる現行報告制度の対象とされている。他方で、重大事故と同様に社会的な影響が大きい重大なリスクとなるインシデント（重大インシデント）については、重大事故としての速やか報告の対象外となっている。

これらのことから、重大なリスクに関する OODA ループ機能やリスクアセスメント機能の強化のため、報告制度を量的・質的に見直すことが必要である。また、アクシデントを対象とする通信事故の報告制度とは別に、インシデント（通信事故の兆候段階である事態）について、重大インシデントの速やかな報告等、所要の制度整備が適当である。

エ　通信事故の検証制度の見直しの在り方

2015 年度から開催されている検証会議により、通信サービス・ネットワークの安全・信頼性対策に関する PDCA サイクルについては、一定の意義や成果が現れている。この検証会議における検証の対象については、通信事故に該当しない障害や重大インシデント等の重大事故以外の重大なリスクにも拡大しているところ。他方で、事故原因の関係者による参加や情報提供等が得られず、原因究明やリスクアセスメントにおける公正性や実効性の確保が困難となっている。

これらのことから、重大事故等の事故調査を通じたリスクアセスメント機能の強化によるリスクマネジメントに関する PDCA サイクルの強靭性・実効性を確保するため、検証会議の機能強化が必要である。また、重大事故・インシデントの原因に関係するマルチステークホルダーからの報告徴収等を通じた原因の究明等によるリスクアセスメント等、第三者機関に関する所要の制度整備が必要である。

なお、この第三者機関は、科学的・公正な判断が可能な者等から構成され、産学の専門機関等と連携・協力し、中立・公正で、行政処分等からの一定の独立性や十分な体制の確保等を行うことが適当である。

オ　自然災害・サイバー攻撃を原因とする通信事故の報告制度等の在り方

近年、豪雨、台風、地震等による大規模自然災害が頻発化・激甚化しており、これらの災害により通信障害における広域化・長期化が進展している。そのため、災害対策基本法に基づく被害状況等の報告や報告制度に基づく四半期報告事故等による OODA ループ的な対応の強化や総合的な検証等が可能な PDCA サイクルの構築が必要である。

また、サイバー攻撃の巧妙化・悪質化等により、通信サービスの提供停止に至る通信事故や通信設備に関する情報の漏えい等による重大なインシデントが発生している。そのため、報告制度等とサイバーセキュリティ対策における

一層の連携・協力の推進による OODA ループ的な対応や PDCA サイクルの強化が必要であり、サイバー攻撃を原因とする重大インシデントの速やかな報告やサイバー攻撃による重大事故等に関する詳細報告期限の柔軟化等、所要の制度整備等が適当である。

（３）今後の対応

今後は、残された次の検討課題等について、関係事業者からヒアリングしつつ、引続き検討を行う。

① 外国企業等による提供も含めた、テレワーク・遠隔学習等向けのインターネット関連サービス等の通信事故に関する報告基準の在り方
② データ伝送サービス（ベストエフォートサービス）の品質低下に関する報告基準の在り方
③ 通信事故に該当しない、インターネットにつながりづらい障害に対するＳＮＳの活用等による対応の在り方

なお、以上の検討にあたっては、以下の状況等を踏まえつつ、検討することとする。

① 改正電気通信事業法（2021 年 4 月施行）に基づく外国企業等からの通信事業者等に関する届出等の状況
② 「ブロードバンド基盤の在り方に関する研究会」（総務省において 2020 年 4 月より開催）によるブロードバンドサービスのユニバーサルサービス化の検討状況
③ 「固定ブロードバンドサービスの品質測定手法の確立に関するサブワーキンググループ」（総務省において 2020 年 12 月より開催）による同サービスの品質計測手法の検討状況

おわりに

本報告書では、令和２年度に発生した重大な事故を中心に取りまとめを行った。令和２年度においては、重大な事故は４件であり、これは直近約 20 年間において最低であった令和元年度の３件に次いで少ない件数であった。他方で、四半期報告事故の件数は 6,610 件と、前年度から 309 件増加しており、直近３年で増加傾向となっている。

本年は平成 23 年３月に発生した東日本大震災の発災から 10 年となることから、東日本大震災以降の災害時における通信サービスの確保の在り方について、総務省及び電気通信事業者等による主な取組の紹介をしている。

また、昨今の電気通信事業者を取巻くサイバー攻撃のリスクの深刻化等を踏まえ、内閣サイバーセキュリティセンターの資料に基づき、重要インフラ事業者へのサイバー攻撃の事例の紹介をしている。四半期報告事故として、送信型対電気通信設備サイバー攻撃の事例が、令和元年度は８件、令和２年度は 13 件報告されている。また、異常トラフィックに起因する事故は直近５年間で年に 45～135 件程度報告されており、サイバー攻撃が原因の可能性もある。電気通信事故検証会議においても、これらサイバー攻撃による電気通信事故が発生した場合に検証を行っていくことが必要であり、今後もサイバー攻撃の事例について注視していく必要がある。

さらに、自然災害やサイバー攻撃を原因とする事故報告制度の在り方を含め、2020 年度半ばに向けた電気通信事故の報告制度及び検証制度の検討が「情報通信審議会 情報通信技術分科会 IP ネットワーク設備委員会 事故検証・報告制度等タスクフォース」において行われ、その検討結果についての紹介もしている。本検討においては、電気通信事故の検証制度の見直しの在り方として、検証会議の機能強化の必要性が挙げられており、検討結果を踏まえ、本会議においても検討を行っていく必要がある。

本報告書の検証結果を踏まえ、事業者団体や総務省においては、これまでの教訓等を踏まえた対策のうちベストプラクティスと考えられるものや、自然災害やサイバー攻撃等、その発生自体を避けることができず、接続等を通じて相互に依存している電気通信事業者に共通するリスクに対する被害の最小化や応急復旧の迅速化等の取組等については、関係事業者間における一層の情報共有を図るなどにより、引き続き、電気通信事故の再発防止に向けた取組を図ることが期待される。

ニュー・ノーマルに対応したデジタル強靱化社会を構築するためには、より安心・安全で信頼できる情報通信ネットワークの構築・管理運用等を確保することが必要不可欠となっている。今後、総務省をはじめとする関係者においては、電気通信事故の報告及び原因究明等の検証等を通じたＰＤＣＡによるリスク

マネジメント等、マルチステークホルダーの連携によるガバナンスの在り方について議論を深めていくことが必要である。

本会議としては、以上の議論も踏まえつつ、電気通信サービス及びその基盤となる情報通信ネットワークが安心・安全で信頼できるものとなるよう、電気通信事業者において事故の再発防止等に自主的に取り組むことを基本とし、重大な事故の検証等を通じて電気通信事業者が取るべき対策を提言すること等により、電気通信事故の発生や再発防止に引き続き貢献していきたいと考えている。

最後に、電気通信事故の検証を行うにあたり、電気通信事故検証会議への出席を含め協力していただいた電気通信事業者の皆様に、この場を借りて御礼を申し上げる。

参考１

（改正　令和３年５月 21 日）

「電気通信事故検証会議」開催要綱

１．目的

電気通信は、我が国の基幹的な社会インフラであり、電気通信事故は、国民生活や企業の経済活動に多大な支障を招来するものであるため、その防止は喫緊の課題である。近年の電気通信事故の大規模化・長時間化やその内容・原因等の多様化・複雑化を踏まえ、電気通信事故の報告について、外部の専門的知見を活用しつつ検証を行う観点から、「電気通信事故検証会議」を開催する。

本会議は、「①重大な事故に係る報告の分析・検証」、「②四半期ごとに報告を要する事故に係る報告の分析・検証」等を行うことにより、電気通信事故の発生に係る各段階で必要な措置が適切に確保される環境を整備し、電気通信事故の防止を図ることを目的とする。

２．名称

本会議の名称は、「電気通信事故検証会議」と称する。

３．主な取扱事項

(1)　重大な事故に係る報告の分析・検証
(2)　四半期ごとに報告を要する事故に係る報告の分析・検証
(3)　その他

４．構成及び運営

(1)　本会議は総合通信基盤局電気通信事業部長の会議とする。
(2)　本会議の構成員は、別添のとおりとする。
(3)　本会議に座長及び座長代理を置く。
(4)　座長は構成員の互選により定め、座長代理は構成員の中から座長が指名する。
(5)　本会議は、座長が運営する。
(6)　座長代理は、座長を補佐し、座長不在のときは、その職務を代行す

る。

(7)　本会議は、必要があると認めるときは、構成員以外の者の出席を求め、意見を聞くことができる。
(8)　構成員は、議事に対して利害関係を持つ場合には、その旨を事務局に申告し、当該会議への出席を見送る。
(9)　構成員は、本会議における情報の取り扱いに関して、別紙の事項を遵守する。
(10)　構成員の任期は１年とする。ただし、再任を妨げない。
(11)　その他、本会議の運営に必要な事項は座長が定めるところによる。

５．会議等の公開

(1)　本会議においては、電気通信事業者の経営上の機密情報や通信ネットワークの構成等の機微な情報を取り扱うため、会議及び議事録は非公開とする。
(2)　本会議の議事要旨、配布資料等は原則公開とする。ただし、座長が、当事者又は第三者の権利、利益や公共の利益を害するおそれがあると認める場合は議事要旨、配布資料等の全部又は一部を非公開とすることができる。

６．開催期間

本会議は、令和３年５月から令和４年３月まで、原則毎月定例日に開催する。ただし、議事がない場合には、休会とする。

７．庶務

本会議の庶務は、総合通信基盤局電気通信事業部電気通信技術システム課安全・信頼性対策室が行う。

別紙

本会議における情報の取扱いについて

本会議においては、電気通信事業者の経営上の機密情報や通信ネットワークの構成等の機微な情報を取り扱うため、中立かつ公正な検証を確保する観点から、構成員は下記の事項を遵守するものとする。

記

１．　構成員は、本会議で知り得た非公開情報について、厳に秘密を保持するものとし、総務省の書面による承諾なくして、第三者に開示しないこと。また、構成員を辞した後も同様とすること。

２．　構成員は、本会議で知り得た非公開情報に基づく活動を行わないこと。

以上

別添

電気通信事故検証会議　構成員一覧

（五十音順、敬称略）
※所属・役職は令和３年７月現在

相田（あいだ）　仁（ひとし）	東京大学大学院工学系研究科 教授
阿部（あべ）　俊二（しゅんじ）	国立情報学研究所 アーキテクチャ科学研究系 准教授
内田（うちだ）　真人（まさと）	早稲田大学　理工学術院　教授
加藤（かとう）　玲子（れいこ）	独立行政法人国民生活センター 相談情報部 相談第２課 課長
森島（もりしま）　直人（なおと）	EY ストラテジー・アンド・コンサルティング株式会社 ディレクター
矢入（やいり）　郁子（いくこ）	上智大学 理工学部 情報理工学科 准教授

参考２

電気通信事故検証会議　開催状況

〔令和２年度〕

① 第１回（令和２年４月 14 日～22 日（メール審議））
- 令和２年２月に発生した株式会社オプテージの重大な事故について
- 令和元年度第３四半期に発生した電気通信事故の集計結果について
- 令和元年度電気通信事故に関する検証報告の骨子（案）について
- その他

② 第２回（令和２年６月１日）
- 令和２年２月に発生した株式会社オプテージの重大な事故について
- インターネット障害の把握の在り方に係る調査研究結果について
- 「令和元年台風第 15 号・第 19 号をはじめとした一連の災害に係る検証レポート（最終とりまとめ）」等について
- 令和元年度電気通信事故に関する検証報告（素案）について

③ 第３回（令和２年７月２日）
- 令和元年度第４四半期に発生した電気通信事故の集計結果について
- 過年度検証報告のフォローアップアンケートの集計結果（暫定版）について
- 令和元年度電気通信事故に関する検証報告（素案）について
- その他

④ 第４回（令和２年７月 30 日）
- 令和２年２月及び３月に発生した株式会社グッド・ラック等の障害について
- 令和元年度に発生した電気通信事故の集計結果等について
- 過年度検証報告のフォローアップアンケートの集計結果について
- 令和元年度電気通信事故に関する検証報告（案）について
- その他

⑤ 第５回（令和２年９月 29 日）
- 令和２年４月に発生したキヤノンマーケティングジャパン株式会社の重大な事故について
- 令和２年５月に発生した株式会社 NTT ドコモの重大な事故について

・　その他

⑥　第６回（令和２年 11 月 10 日）

・　令和２年６月に発生した西日本電信電話株式会社の重大な事故について

・　令和２年７月に発生したフリービット株式会社の重大な事故について

・ 令和２年度第１四半期に発生した電気通信事故の集計結果について

・ その他

参考３　重要インフラ事業者に対するサイバー攻撃の事例

（１）平成 26 年の事例[22]

ア　Web サイト（トップページ）の改ざん

概要	・Web サイトに対する不正アクセスにより、トップページが改ざんされた。 ・閲覧すると、攻撃者の主義主張を表す画像が表示され、更に別の Web サイトに誘導される。 ・Web サイトを一時閉鎖後、改ざん箇所の修正と他への影響有無確認を実施して復旧。
背景	・ Web サーバは外部の共用サーバ（ホスティングサービス）を利用。 ・ Web サイト自体の運用は事業者の広報担当者（IT 担当部署ではない）が実施。 （Web サイトの構築は外部委託したが、日々の運用・保守は外部委託せずに広報担当者が実施。）
検知	NISC からの所管省庁を通じた情報提供により、IT 担当部署の担当者が Web サイトの改ざんを認知。
対処	・ 検知が深夜であり、また、ホスティングサービスの業者の応対時間外だったため、IT 担当部署の担当者判断により、翌朝から対処を行った。 ・ 広報担当者が Web サイトの一時閉鎖作業に着手したが、トップページのみではなく、Web サイト全体を閉鎖する方法が容易に判明せず、作業に時間を要した（約半日）。 ・ 危機管理の責任者の指示により、Web サイトの一時閉鎖について報道発表を閉鎖当日中に実施。 ・ 危機管理の責任者の指示により、費用発生の如何に関わらず早期復旧すべき方針が示され、Web サイト構築時の業者と協力して復旧作業（作業用に一時閉鎖を部分解除／改ざん箇所を修正）を実施。 ・ その後、トップページ以外の全ページを目視により検査・確認し、Web サイトを再公開。
原因	・ホスティングサービスの契約内容にログ採取が含まれておらず、改ざん原因は特定できなかった。 ・ なお、状況から推測される原因は次のとおり。 ✓ 使用していた CMS※について、数年間更新しておらず、脆弱性があるバージョンを使用していた。

[22] サイバーセキュリティ本部 重要インフラ専門調査会 第 1 回会合 「資料 10 2014 年度重要インフラにおける補完調査結果について」を基に作成。
https://www.nisc.go.jp/conference/cs/ciip/index.html

	※ Content Management System：Web サイト上のコンテンツを管理・編集するためのソフトウェア。 ✓ Web サイトを更新するためのソフトウェア（FTP クライアント）に脆弱性があるバージョンを使用していた。（パスワードを保持する設定としていたが、パスワード漏えいの脆弱性があった。） ✓ パスワード（FTP パスワード）を運用開始以来、一度も変更していなかった。
再発防止策	・FTP パスワードを変更（推測されにくいようランダムな文字列を使用。）。 ・使用しているソフトウェアについては、パッチ適用等の脆弱性対策を実施。 ・専門知識を持った外部業者への運用委託を含めた、Web サイトの全面更改を検討・計画。 ・Web サイト更改に当たり、情報セキュリティ対策の検討などに外部専門家（コンサルティング会社）を活用。

イ　会員制サービスの不正ログイン

概要	・複数の会員制サービスのサーバに対し、大量のログイン試行が行われた。 ・一部のログイン試行が成功し、個人情報を含む会員情報が閲覧された。 ・サービスを一時停止し、不正ログインされたアカウントの凍結や監視強化等を措置。
背景	・攻撃を受けた事業者は会員制サービスを複数運用。 ・各会員制サービスは、各担当部署（IT 担当部署ではない）が原則として管理。 ・会員制サービスのログイン状況の監視は、一定時間ごとのログ監視により実施。
検知	・短時間に大量のログイン試行が行われたことが、ログ監視により検出され、担当部署へ通知。 ・その後も、大量のログイン試行が、同一サービスだけでなく、他のサービスにおいても行われたことを確認。 （管理状況の異なる他のサービスの監視体制を強化する前にログイン試行を受けた。）
対処	・会員制サービスを一時停止。深夜であり担当者が駆けつけるまでに数時間を要した。 （その後、24 時間対応を実施している別の部署に停止作業を移管することで改善。） ・一時停止中に、不審な IP アドレスを特定。通信の遮断（フィルタリング）等を実施後、サービス再開。

	・不正ログインされたアカウントを凍結し、電子メールにて連絡。再開手続きはコールセンターにより実施。 ・サービスの会員全員に対して、電子メールでパスワード管理に関する注意喚起を行った。
原因	・第三者によるアカウントリスト攻撃※と推定される ※アカウントリスト攻撃･･･ID とパスワードがセットになった「アカウントリスト」を元に不正ログインを試行する攻撃。アカウントリストは、何らかの方法（例：他のオンラインサービスへの不正アクセス）により事前に入手しておく。利用者が ID とパスワードをオンラインサービス間で使い回していると、攻撃が成功してしまう。
再発防止策	＜早期対策＞ ・大量アクセスに対する監視間隔の短縮による早期検知。（例：日時→毎時、毎時→15 分ごと） ・大量ログイン試行の検知後、通信を遮断するまでのプロセスを自動化。 ＜中長期対策＞ ・ログイン画面に画像認証（CAPTCHA※）を追加。 ※歪んだり崩れた文字列を表示させ、それを利用者に入力させることで、機械的な自動アクセスを防ぐ方法。 ・ログイン後の画面や会員情報照会画面に個人情報を表示させず、閲覧・変更時は二重認証※を実施。 ※本事例の場合においては、ID・パスワード以外に、個人情報の一部を認証項目として入力させることとしている。 ・リスクベース認証※を実施。 ※利用者のログイン環境（IP アドレス、使用パソコン、使用ブラウザ等）を総合的に分析し、普段と異なる環境からのアクセスと判断した場合に、追加的な認証を要求する方式。

ウ　端末へのマルウェア感染

概要	・マルウェア感染によるものと疑われる通信について、NISC から該当事業者へ情報提供を行った。 ・情報提供した内容を元に、事業者の IT 管理部署が調査を実施。 ・感染の疑いがある端末を特定し、端末の初期化を行うとともに、部署内で情報共有を行った。
背景	・部署ごとに別の業務システムを有しており、それぞれ別のファイヤーウォールを通してインターネットに接続。 ・マルウェア感染が疑われた業務システムは、複数の下部組織が使用。下部組織ごとに管理者がおり、独立した管理が行われている。また、外部から下部組織内への接続は行えない設定※となっている。

	※NAT 変換（ネットワークアドレス変換）を行い下部組織内のネットワークが当該下部組織の外からは隠蔽されている。
検知	・ NISC からの所管省庁を通じた情報提供により、IT 担当部署の担当者がマルウェア感染の疑いを認知。
対処	・ 情報提供の内容（IP アドレス）から、該当のファイヤーウォールを特定し、該当部署に連絡を実施。 ・ IT 担当部署でファイアウォールのログを調査し、マルウェア感染の疑いのある複数の下部組織を特定した。 ・ 該当の下部組織に対してそれぞれ連絡を行い、現地にて端末の調査を実施。 ・ マルウェア駆除ツールを使用し、マルウェアによるものと疑われる通信の停止を確認。端末の初期化も実施。 ・ 各部署の責任者間、各下部組織の責任者間、及び各下部組織の管理者間において、情報を共有した。
原因	・ ウィルス対策ソフトの設定について、調達時の仕様書に十分な内容が記載されていない等の理由により、定義ファイルの更新や定期的なスキャンが行われていない端末が存在した。 ・ マルウェア感染が疑われた業務システムは、下部組織ごとの管理者が管理しているものの、業務システム全体としての管理状況の把握が十分に行われていなかった。 ・ 端末利用者に対して情報セキュリティ研修を行っていないなど、情報セキュリティ意識が不十分であった。
再発防止策	＜早期対策＞ ・ 該当業務システム配下の全端末について、定義ファイルの更新と定期的なスキャンの設定※を実施。 ※定期スキャンの設定時刻経過後に電源を入れた場合には、電源投入時に定期スキャンを実施するよう確実な設定を実施。 ・ ウィルス対策ソフトがマルウェアを検知した場合、IT 担当部署の管理者に、電子メールで通知するよう設定。 ＜中長期対策＞ ・ 業務システム内のネットワーク管理については、下部組織ごとではなく、部署として統一的な管理を実施。 ・ 調達仕様書のひな形の作成や運用手順等の明確化を行い、部署内での調達・運用管理を統一化。 ・ 情報セキュリティに関する従業員・職員研修を定期的に実施。 ・ IT 担当部署（情報セキュリティ担当）の増強を実施。

（２）平成 27 年の事例[23]

ア　DDoS 攻撃によるサービス障害

概要	・サービス提供 Web サイトが DDoS 攻撃を受け利用者がアクセスできない状態となった。 ・データセンター事業者にてトラフィック制限を行う等の対応を実施した。 ・分野内での情報共有を行うとともに、利用者への周知を実施した。
背景	・サービス提供 Web サイトを外部のクラウドサービスを利用して構築。 ・告知用 Web サイトは災害対応等を考慮し、別のデータセンターでも運用していた。
検知	・監視担当部署でサービス提供 Web サイトの異常を検知し DDoS 攻撃と判断。 ・同時にインターネット上に公開されているメールアドレス宛に金銭を要求する脅迫メールが届き、その情報が事業者内で共有された。
対処	・データセンター事業者側にてアクセス制限を実施した。 ・告知用 Web サイトには影響がなかったため、そちらを通じて利用者にサービス利用不可の状況と代替サービスの提供方法の案内を実施した。 ・分野内での情報共有を実施。同じような攻撃を受けたケースを参考に対応を検討した。
原因	・国際的な犯罪組織による DDoS 攻撃により、平時の 1000 倍以上もの通信がありデータセンターの回線がパンクした。 （DDoS 攻撃解除のために金銭を要求※。） ※要求通り金銭を支払っても攻撃がやまない場合が多い。
再発防止策	＜短期的対策＞ ・データセンター事業者にてサービス提供に用いていない通信を遮断※した。 ※攻撃に利用された通信が UDP パケットのみだったため、UDP パケットがサービス提供に利用されていないことを確認の上、データセンター事業者側で UDP パケットをカットすることにより通信を維持させた。 ＜中長期的対策＞ ・CDN※サービスを利用することにより大量の通信を処理できる環境を検討。

[23] サイバーセキュリティ本部 重要インフラ専門調査会 第 5 回会合 「資料 7 2015 年度重要インフラにおける補完調査」を基に作成。
https://www.nisc.go.jp/conference/cs/ciip/index.html

	※ Contents Delivery Network:ウェブコンテンツの大量配信に最適化されたネットワーク。負荷分散以外にも不要な通信を遮断し、必要な通信のみを正規サイトに流すオプションメニューもある。 ・ DDoS 攻撃対策を含むセキュリティに関する社内規程を追加準備中。 ・ 今後不審な通信を遮断できるよう、送信元の国単位や IP アドレスの範囲を指定した遮断など柔軟な通信遮断手順を検討。

イ　改ざんされた Web サイトの閲覧によるマルウェア感染の疑い

概要	・ 改ざんされた Web サイトにアクセスした事業者に対して、NISC から注意喚起を実施。 ・ 端末を特定し隔離するとともに、事業者全体のインターネット接続を遮断。 ・ 事業者の IT 担当部署が調べたところ、Adobe Flash Player が最新だったため感染はなかった。
背景	・ 事業者内 LAN 及びインターネット接続の管理を IT 担当部署が実施。 ・ 職員が業務上よく利用する Web サイトが改ざんされた。
検知	・ NISC からの所管省庁を通じた情報提供により、IT 担当部署がマルウェア感染の疑いを認知。
対処	・ 保守ベンダー※と連携し、情報提供の内容を元にプロキシログから感染の疑いがある端末を特定。 ※事業者内 LAN 管理業務の委託先。契約時間外であったが、緊急時対応として対処。 ・ 該当端末を隔離するとともに、プロキシの停止によりインターネット接続を遮断※。 ※インターネット接続の遮断についての権限は IT 担当部署にあることが、規程に定められていた。 ・ プロキシログから該当端末が外部へ不審な通信をしていないことを確認。 ・ 改ざんされた Web サイトの管理者からマルウェアに関する情報※を入手し、マルウェア感染がないことを確認。 ※マルウェアのファイル名、保存先、通信先情報等
原因	・ 事業者内 LAN に接続された端末が、改ざん※された Web サイトにアクセスした。 ※ブラウザのプラグイン（Adobe Flash Player）の脆弱性を利用しマルウェアに感染させる仕掛けが埋め込まれた。 ・ 端末のブラウザのプラグインは更新済みであったため、マルウェア感染はなかった。

再発防止策	＜短期的対策＞ ・ 業務上必要な場合を除き、該当のプラグインを原則使用禁止とした。 ・ やむを得ず使用する場合は常に最新版にアップデートするよう注意喚起を実施。 ＜中長期的対策＞ ・ ネットワーク機器のログ監視・分析能力の強化策を検討。

ウ　USB メモリを介したマルウェア感染

概要	・ スタンドアローン※で運用中の PC におけるマルウェア感染が発覚。 ・ PC 間のデータ交換のために、USB メモリを日常的に使用しており、それを介して感染が拡大した。 ・ USB メモリを使用した全 PC を特定し、ウイルス対策ソフトを用いて駆除。 ※LAN 等のネットワークに接続していない状態をいう。
背景	・ 事業所内のほとんどの PC がスタンドアローンによる運用で、外部の事業者とのデータ交換、PC 間のデータ交換、PC のソフトウェア更新に、それぞれ特定の USB メモリを使用。 ・ USB メモリの使用は管理され、許可されていない USB メモリの使用は許されていない。 ・ 業務要件によりウイルス対策ソフト等が導入できない PC も存在。
検知	・ ソフトウェアの更新に用いていた USB メモリをネットワーク運用されている PC に挿入した際、マルウェアを検知。
対処	・ PC 間のデータ交換用 USB メモリを使用した全ての PC を特定。 ・ ウイルス対策ソフトが導入できる PC は、ウイルス対策ソフトを最新の状態にし、ウイルス駆除を実施。 ・ ウイルス対策ソフトが導入できない PC は、USB メモリ型のウイルス対策ソフトでウイルス駆除を実施。
原因	・ 過去に外部の事業者と USB メモリを用いてデータ交換していたことから、その USB メモリを介して PC がマルウェア感染していたものと思われる。 ・ 上記 PC から、組織内 PC 間のデータ交換に用いる USB メモリを介して、他の PC へ更に感染が拡大したものと考えられる。
再発防止策	＜短期的対策＞ ・ ウイルス対策ソフトを導入できる PC USB メモリ等を用いて、定期的にウイルス定義ファイル等の更新を実施する。 ・ ウイルス対策ソフトを導入できない PC

	USB メモリ型のウイルス対策ソフトを用いて、定期的にウイルスチェックを実施する。 USB メモリを用いて外部とデータ交換をする際は、事前に別の PC でウイルスチェックを実施する。 ＜中長期的対策＞ ・ PC のネットワーク化及び管理サーバーの導入による手動更新の負担軽減などを検討している。

エ　Web サイトへの不正アクセス

概要	・ Web サイトへの不正アクセスにより、Web 管理者情報の窃取や Web サイトの改ざんが発生。 ・ 事案の発生が NISC 等から事業者に対して速やかに伝達され、被害を最小限に。 ・ Web サイトを一時閉鎖後、CMS※やレンタルサーバの脆弱性対策等を実施。 ※Content Management System：Web サイト上のコンテンツを管理・編集するためのソフトウェア。
背景	・ Web サイトのコンテンツ制作は外部業者に委託。 ・ Web サーバは外部のレンタルサーバを利用するが、日々の保守・運用は事業者自らが対応。
検知	（事案２は事案１から約半年後に発生） ・ 【事案１】NISC 等からの情報提供により、IT 担当部署の担当者が Web 管理者情報の窃取を認知。 ・ 【事案２】NISC 等からの情報提供により、IT 担当部署の担当者が Web サイトの改ざんを認知。
対処	・ 【事案１/２】不正アクセスを認知後、事業者内セキュリティポリシーを踏まえ速やかに責任者に報告し、当日中に Web サイトを閉鎖。 ・ 【事案１】Web 管理者情報を変更した上で、CMS やレンタルサーバの脆弱性対策を実施。 ・ 【事案２】Web 管理者情報を変更した上で、セキュリティ向上を図るため別会社のレンタルサーバに移転。 ・ 【事案１/２】事案発生１週間以内に Web サイトを再開。
原因	・ 【事案１】使用していた CMS が汎用的なものでなく独自仕様なので安全といった誤解もあり、脆弱性対策が不十分であった。 ・ 【事案２】CMS 管理外の Web サイトが改ざんされており、レンタルサーバのセキュリティに問題ありと推定。 ・ 【事案１/２】IT 担当部署の職員数の不足もあり事案対応に追われ、対外機関との間での情報共有が必ずしも十分でなかった。
再発防止策	＜短期的対策＞

	・【事案１】CMS やレンタルサーバの脆弱性情報を常に把握し、速やかに更新。 ・【事案１】レンタルサーバのアクセスログを定期的に確認し、不正アクセスを速やかに検知。 ※（独）情報処理推進機構が提供する Web サイトの攻撃兆候検出ツール”iLogScanner”を使用。 ・【事案２】Web サイトの更新作業に際して、送信元を特定の IP アドレスに限定するなどセキュリティ対策を柔軟に適用できるレンタルサーバを利用。 ＜中長期的対策＞ ・【事案１/２】事業者単独では対応できない事案も想定して、事案発生時におけるグループ会社のセキュリティ担当者間での連携を強化。 ・【事案１/２】平時から対外機関との間のセキュリティ情報に係る共有体制を把握。

（３）平成 28 年の事例[24]

ア　メールフォームへの攻撃

概要	・Web サイトに設置した複数のメールフォームに、脆弱性を狙った大量のリクエストがあった。 ・メールフォームに脆弱性はなく、メールフォームや Web サイトに影響はなかった。 ・メールフォームから大量のメールが事業者内に送信され、事業者内のメールが約 1 日受信できない状態になった。 ・メールを利用した一部の業務について、手順を変更して実施した。
背景	・アンケートや各種イベントの申込受付のために、Web サイトに 20 か所程度メールフォームを設置していた。 ・メールフォームに入力されたメッセージは、事業者内の特定のメールアドレス宛に送信される仕組みだった。 ・メールフォームは定期的にメンテナンスされており、未対応の脆弱性などはなかった。
検知	・他事業部の担当者からシステム担当者へメールが届いていないとの連絡があった。
対処	・攻撃元 IP アドレスを特定し、該当 IP アドレスからの接続を拒否した。 ・現在使用されていないメールフォームを閉鎖した。 ・メールフォームに CAPTCHA を設定した。
原因	・攻撃者が、複数のメールフォームに対して Web サイトの脆弱性を探る多数の攻撃リクエストを送信したため。 ※Web サイトに XSS や SQL インジェクションなどの脆弱性はなく、攻撃者の意図は失敗に終わったと思われる。
再発防止策	＜システム面＞ ・特定の送信元 IP アドレスを FW で接続拒否する設定を追加。 ・特定の送信元 IP アドレスをメールフォームのプログラムで拒否する設定を追加。 ・すべてのメールフォームに CAPTCHA を設定し、自動化された大量アクセスへの対策を実施。 ＜運用面＞ ・大量アクセスがあった場合に、送信元 IP アドレスを特定する方法の共有。 ・特定の送信元 IP アドレスを拒否する設定方法の共有。 ・利用していないメールフォームの閉鎖。

[24] サイバーセキュリティ本部 重要インフラ専門調査会 第 10 回会合 「資料３ 2016 年度 重要インフラにおける「補完調査」について」を基に作成。
https://www.nisc.go.jp/conference/cs/ciip/index.html

	※今回は単一 IP アドレスからの大量アクセスだったが、今後、不特定多数の IP アドレスからアクセスされた場合の対応体制については。継続して検討を進めている。

イ　アクセス制限の不備

概要	・主要装置へのアクセス制限には対応していたものの、監視装置へのアクセス制限に不備があった。 ・監視装置への不正アクセスにより、機能が停止された。なお、主要装置の基本的な動作には影響はなく、重要インフラサービス自体への影響はなかった。 ・監視装置を切り離し、主要装置の機能を維持した。
背景	・インターネットを経由して、アクセス制限をしていないゲートウェイルータを介して、監視装置をつないでいた。 ・地方施設のシステムの保守・点検については、保守ベンダーに委託していた。
検知	・本社では、毎日定時に監視装置の管理画面にアクセスし、機器が正常に動作しているか確認していたが、その日は監視ができなかった。また同日、システムの保守ベンダーから、当該施設で使用していたものと同型の機器で構成されている他の施設で、監視装置に不具合が発生しているとの連絡があり、発覚した。
対処	・現地でサービス提供が維持できているかを現地業者に確認。 ・保守ベンダーに施設の対応を依頼。 ・監視装置へのアクセスに問題があることが分かったため、同装置をシステムから切り離した。 ・所管省庁等へ連絡。
原因	・ゲートウェイルーターの設定で、ポートにアクセス制限がかけられておらず、また、監視装置で不要なポートが開いていたため、悪意を持った第三者から送信されたコマンドが送られてしまったもの
再発防止策	・ゲートウェイルーターのポート制限を実施（通常操作は可能） ・悪意あるコマンドを受け付けないよう、プログラムを改修

ウ　ランサムウェア被害

概要	・Web サイトの閲覧中に、ウイルス対策ソフトからアラートが表示された。 ・システム担当に連絡し、早急に PC をネットワーク（インターネットに接続）から切り離した。 ・ランサムウェアに感染したものであり、インシデント対応中も PC 内で次々にファイルが暗号化され、最終的には数百のファイルが暗号化されていた。

	・重要業務ネットワークは、事務用ネットワークとは切り離されていたため、重要業務ネットワークへの感染はなかった。
背景	・重要業務ネットワーク(クローズドなネットワーク)と事務用ネットワーク(インターネットに接続されているネットワーク）を分けて構築していた。 ・事務用 PC の管理は利用者各自に任せられており、セキュリティアップデートがなされていないものもあった。
検知	・Web サイトの閲覧中にウイルス対策ソフトのアラートが表示され、利用者がシステム担当へ連絡した。
対処	・システム担当が現場に急行し、ネットワークケーブルを抜線した。 ・当該 PC がランサムウェアに感染していること、及び重要業務ネットワークへの影響がないことを確認した。 ・全従業員にウイルスチェックを依頼し、報告させた。 ・状況を上司に報告し、関係省庁等と連携をとった。 ・関係省庁等から助言をもらい、復号ツール(ウイルス対策ベンダー提供)を試した。
原因	・Web ブラウザやソフトウェアの脆弱性を悪用したドライブバイダウンロード攻撃によるランサムウェア感染
再発防止策	・OS のセキュリティパッチやソフトウェアのバージョンを管理する仕組みの検討を始めた。 ・ウイルス対策ソフトの管理サーバを導入し、定期的なパターンファイルの更新管理を検討した。 ・個人が作成したデータを保存するファイルサーバの導入を進めていたが、ランサムウェア対策として、 ・世代管理できること ・PC から書込みができないドライブにバックアップが取れること をファイルサーバーの要件に加えた。

エ　管理サーバへの不正アクセス

概要	・攻撃者は、管理者 ID/PW を取得し（経緯不明)、当該 ID/PW で管理サーバへ不正アクセスを行った。 ・事業者は、管理サーバへの不正アクセスを定期メンテナンスで発見、顧客情報漏えいが判明。 ・委託先でログを取得する契約となっていないものの、委託先へ開示請求を行い、アクセスログを入手。 ・アクセスログを基に、セキュリティベンダーに調査を依頼し、HP で顧客へお詫びと注意喚起。 ・継続的な評価・改善、ID/PW の管理徹底、アクセスの制限、ログによる早期検知などの対策を講じた。

背景	・委託先のサーバを利用し、顧客情報のやり取りを行っており、外部の IP アドレスからのアクセスが可能。 更に、アクセスログを取得する契約となっていない。 ・管理者 ID/PW を定期的に変更していない。
検知	・管理サーバへの不正アクセスを定期メンテナンスで発見し、委託先へログの開示請求を行った。 ・セキュリティベンダーによる調査を行ったものの、管理者 ID/PW 漏えいの原因特定に至らず。
対処	・管理者 ID/PW を変更。 ・HP で顧客情報漏えいについてお詫びと注意喚起。
原因	① 導入時からセキュリティ対策等の評価や見直しを行っていない。 ② 管理者 ID/PW の管理が徹底されていない。 ③ 外部の IP アドレスからのアクセスを制限していない。 ④ ログを適切に取得していない。
再発防止策	① 定期的にシステムの安全性を評価・改善するため、情報セキュリティ委員会（社長が委員長）を設置。 ② 社内システム全ての ID/PW を変更し、ID 管理規程を整備し、PW 変更管理を徹底。 ③ 管理サーバへのアクセスを事業者の IP アドレスに制限。 ④ ログ管理に関する規程を定め、ログを適切に取得。

オ　ソフトウェアの継続的なセキュリティ対策

概要	・WordPress に XSS(クロスサイトスクリプティング)の脆弱性が発見され、セキュリティアップデートが公式 HP において公開された。 ・該当 Web サイトはメンテナンス契約などを結んでおらず、担当者が脆弱性に気づかないままだった。 ・情報セキュリティ関係機関から、XSS の脆弱性に関する連絡を受け、委託先事業者に調査・対応を依頼した。
背景	・自部門のプロジェクトに関する Web サイトの構築を外部に委託し、システム部門が運用する共用サーバに配置した。 ・共用サーバにおける OS のセキュリティ対策は、自社のシステム部門で一括して行われるが、CMS(コンテンツマネジメントシステム)等のセキュリティ対策は、各部門において管理する運用となっている。 ・該当 Web サイトは CMS(コンテンツマネジメントシステム)の WordPress を用いて構築している。
検知	・情報セキュリティ関係機関から Web サイトに XSS の脆弱性がある旨、システム部門に情報連絡があった。

	・WordPress に関する脆弱性であり、セキュリティアップデートが 10 カ月前にリリースされていた。 ・調査の結果、脆弱性を利用したサイバー攻撃を受けた形跡はなかった。
対処	・委託先事業者に連絡し、調査・対応を依頼した。 ・一次対応：脆弱性のあるファイルは、当該 Web サイトでは使用していなかったため、削除した。 ・本対応：サーバ移行にあわせて、WordPress を最新のセキュリティアップデートにバージョンアップした。
原因	・継続的に脆弱性情報をチェックする体制が定められておらず、該当 Web サイトが脆弱性のある状態で放置されてしまった。 当時の体制 委託先事業者・・・Web サイト構築までの契約 （保守契約等なし） 自社システム部門・・・共用サーバの OS のセキュリティ対策 各部門・・・CMS 等のセキュリティ対策 ※各部門は当時セキュリティアップデートを確認しなければいけない認識がなかった
再発防止策	＜短期的対策＞ ・担当部門が Web サイトに関する定期的な脆弱性に関する情報を収集することとした。 ・保守契約があり、保守期間が残っている Web サイトについて、委託先事業者と脆弱性対応に関する取決めの確認を実施した。 ＜中長期的対策＞ ・システム部門にて、運用保守契約の中に、定型的に盛り込むべき継続的な脆弱性対応に関する項目を検討している。

カ　システムの不具合によるサービス障害

概要	・顧客が、端末にデータに異常があるカードを挿して操作を行ったところ、全グループ会社において、端末で他社との取引ができなくなった（複数の外部センタ間の接続も不可）。 ・過去に例のない障害のため、障害範囲の切り分けに手間取り、原因究明や復旧に時間を要した。 ・障害原因となったプログラムを改修。他の類似ロジックの総点検を実施した。 ・システム監視設計強化、組織間情報共有の円滑化、想定外事態への対処を迅速化する対策を講じた。
背景	・グループ会社とともにシステム運用を外部委託（システムは複数の外部センタと接続してサービスを提供）。 ・機器の切り替えなどのシステム障害対応訓練を、外部委託ベンダやグループ会社と定期的に実施。

	・カードの不良によって、偶発的に、端末から規定外コードがシステムに送信。
検知	・システムと外部センタとの連携を要する特定の処理でタイムアウトを検知。 ・外部委託先から全グループ会社に自動通報。
対処	・店舗や外部委託先のサービス影響情報では原因特定に至らず、タイムアウト多発したことを受け、過去障害事例を参考にネットワークの障害状況を確認・解析。 ・機器の切り替えや外部センタとの接続規制を実施するも同事象が再発。 ・共通バッファ領域※が枯渇していることを究明し、該当機器の再立ち上げ（バッファクリア）を実施し、復旧。 ※バッファ領域は、外部センタとの共通バッファ領域であったため、関連する全ての外部センタで障害が発生。
原因	・特定業務においてカードの事前チェック処理が一部漏れており、規定外コードがシステムに送信され、特定の処理が異常終了。 ・規定外コードのエラー処理がループ化されており、共通バッファ領域が枯渇し、当該領域を使用する処理にも影響が波及。 ・バッファ領域の異常をリアルタイムに検知する仕組の不備。
再発防止策	・エラー処理ロジックの適正化（事前チェック処理の実装、リトライ処理の上限設定など） ・その他の業務に関連する類似ロジックの総点検を実施 ・現状把握・対処の迅速化に向けた手順の見直し及びマニュアル・ツール類の整備。 ・早期検知を可能とする監視設計の見直し（バッファ領域の状態の常時監視など）

（４）平成 29 年の事例[25]

ア　WannaCry によるサイバー攻撃

概要	・シンクライアント端末からファイルサーバにアクセスした際、「.WCRY」拡張子のファイルがあることに気づいたが、該当するファイルは開くことができなかった。 ・保守ベンダにて、ファイルサーバの LAN ケーブルを抜線してネットワークから隔離し、ファイルサーバがランサムウェアに感染していることをウイルス対策ソフトにて確認した。 ・ランサムウェア感染していると考えられるファイルをすべて消去し、バックアップデータから復元した。 ・再度、感染がないことを確認した上で、ファイルサーバをネットワークに接続し、元の状態に戻した。
背景	・業務都合上、シンクライアント端末上で USB メモリを利用していたが、許可された USB メモリのみ使用可としていた。 ・インターネットからダウンロードするものは全てウイルスチェックを徹底していた。 ・シンクライアント端末は環境復元ソフトが入っており、再起動の度に設定された状態に復元される仕様になっていた。
検知	・シンクライアント端末からファイルサーバにアクセスした際、「.WCRY」拡張子のファイルがあることに気づいた。 ・関係省庁から、WannaCry に関する注意喚起があり、内容が酷似していることを確認した。
対処	・ファイルが開けない状態であったため、上司に報告し、システム担当が保守ベンダに対処を依頼した。 ・保守ベンダがランサムウェアの感染を確認し、インターネット接続用の LAN ケーブルを抜線した。さらにファイルサーバ内の感染していると考えられるファイルを削除した。 ・保守ベンダにより、システム担当が事前に取得し、ローカルに保存していたバックアップデータから、ファイルを復元した。 ・再度感染がないか確認した上で、ファイルサーバをネットワークに接続し、元の状態に戻した。 ・状況を上司に報告し、関係省庁等と連携をとった。
原因	・感染原因は特定できておらず、おそらく USB メモリ経由ではないかと思われる。
再発防止策	・シンクライアント端末は、環境復元ソフトにより、セキュリティアップデートも無効化されてしまうため、セキュリティアップデートが有効化されるよう検討した。

[25] サイバーセキュリティ本部 重要インフラ専門調査会 第 14 回会合 「資料６ 2017 年度 重要インフラにおける補完調査」を基に作成。
https://www.nisc.go.jp/conference/cs/ciip/index.html

	・USB メモリの使用方法に関しては、再度周知徹底を行った。 ・ローカルへのバックアップの定期的な取得を検討した。 ・システム担当の一時対応強化のため、外部のセキュリティ研修に参加した。

イ　認証の脆弱な IoT 機器への第三者アクセス

概要	・水圧監視用の IoT 機器（以下、水圧センサ）数十台が、インターネット経由で第三者が容易にログインでき、監視情報を閲覧できる状態になっていることが、外部からの指摘により発覚した。 ・水圧センサに内蔵された監視用 Web の認証が不要又はマニュアルから入手できる ID/初期パスワードが使われており、接続可能な IP アドレスや端末も制限されていなかった。 ・情報セキュリティ担当と IoT 機器所管の事業部門（水道設備部門）で連携して設置場所を特定し、機器設置業者の協力の下、対象の全ての IoT 機器のパスワードを複雑なものに変更した。
背景	・水道施設の水圧監視のため、水圧データを閲覧できる簡易 Web サーバ機能（パスワード認証）を持つ IoT 機器（水圧センサ）を水道施設約 20 か所に設置した。 ・導入は、各種設定の検討も含め、機器設置業者に委託していた。 ・当該 IoT 機器以外にも水圧監視の手段を有していた。
検知	・　事業者の情報セキュリティ担当が、第三者から、「脆弱な IoT 機器を発見した」との連絡があり、対象の機器の IP アドレス、大まかな地理情報、問題点等を受領した。
対処	・情報セキュリティ担当にて、受領した IP アドレスが割り当てられた機器の所管の事業部門を特定するため、調査を開始した。IoT デバイスは資産管理台帳の対象に含めていなかったため難航したが、最終的に水圧センサであることを特定し、事業部門（水道設備部門）に連絡した。 ・水道設備部門から機器設置業者に対して、該当機器のパスワードを複雑なものに変更するよう指示した。 ・機器設置業者にて、全ての水圧センサのパスワードを複雑なものに変更した。また、水圧センサの不正操作の痕跡、機微情報の漏えい、他の設定不備及び水圧の制御システムへの影響がないことも確認した。 ・情報セキュリティ担当にて、他の事業部門に対して、IoT 機器が脆弱な状態で運用されていないか、確認を依頼した。結果、他に問題のある機器は発見されなかった。

原因	・事業部門及び機器設置業者において、IoT 機器のセキュリティ対策の必要性の認識が浅く、認証の設定についても導入時の検討事項に挙がらず、初期パスワードのまま導入されていた。 ・業務上、モバイル端末でのアクセスが必要であるため、インターネット経由でアクセスできる環境に水圧センサを接続していたが、水圧センサ及びルータへのアクセス元の IP アドレスや端末の制限は行っておらず、誰でもアクセス可能な状態で稼働していた。
再発防止策	・IoT 機器の設置に関して、資産管理やセキュリティ対策のルールを策定し、事業部門及び機器設置業者に展開した。

ウ　コインマイナー

概要	・攻撃者は、アプリケーションサーバ（AP サーバ）の脆弱性をつき、仮想通貨をマイニングする不正なプログラムを埋め込み、マイニングさせた（結果は通信遮断により、攻撃者に届かず）。 ・大量のトラフィック（UDP パケット）の発生により、利用者がサービスにアクセスしづらいなどの影響が発生した。 ・大量のトラフィックの発生をネットワーク監視により検知し、調査後、本事案が発覚した。 ・AP サーバの脆弱性対応を行った上で、不正プログラムを削除し、検知する仕組みを導入した。
背景	・CSIRT 部門は、関係機関等を通じて、日々脆弱性情報等を収集し、サーバに保有する情報の重要度に応じて対策を行っていた。 ・CSIRT 部門からシステム部門に対して脆弱性対策を指示していたが、長期間対応を行っていなかった。
検知	・ネットワーク監視により、海外の IP アドレスへの大量トラフィック（UDP パケット）を検知（通常の３倍程度まで徐々に増大。CPU 負荷も上昇）。
対処	・システム部門は、脆弱性対応を行った上、不正プログラムを削除した（任意のコード実行が可能な状態であり、他のサイバー攻撃を受けるおそれがあったが、コインマイニング以外の形跡がないことを確認した）。 ・不正プログラム（cron の改ざん）を検知する仕組みを導入した。 ・インシデント内容について、関係機関と情報共有を行った。
原因	・任意のコード実行が可能な緊急度の高い脆弱性を突かれ、不正プログラムを埋め込まれた。 ・過度に CPU 負荷を与えないようなマイニングにより、検知するまでに時間を要した。

再発防止策	・事業者内で、脆弱性情報の重要度・緊急度の認識を統一し、CSIRT 部門は、システム部門から定期的に対応状況の報告を受けることとした。 ・任意のコード実行が可能な脆弱性等が、マイニングに利用されたため、脆弱性対応に漏れがないよう、情報システムの構成管理方法を検討した。

エ　SNS アカウント乗っ取り

概要	・海外への PR のため、５年以上前から海外の短文投稿サイトを使用して情報発信を実施していた。 ・短文投稿サイト(SNS)のアカウントが乗っ取られ、パスワードが変更されるとともに、過去の投稿がほとんど削除され、政治的な発言が投稿された。 ・SNS 運営会社を通じてパスワードをリセットするとともに、SNS アカウント管理について見直し、周知を行った。
背景	・事業者は、海外への PR を積極的に行うために、海外の短文投稿サイト(SNS)にアカウントを作成し、定期的に情報を発信していた。 ・事業者は、SNS 担当者として現地出身の人を１年ごとに雇用し、現地文化を踏まえた表現を用いて、現地の言葉で発信していた。フォロワー数は順調に伸びており、クレーム等は発生していなかった。
検知	・SNS 担当者が情報発信しようとしたところ、短文投稿サイトのログインができないことから本事案が判明した。 ・攻撃者にパスワードが変更されていたこと、及び本人認証コードの送信先が退職した前任者の携帯電話となっていたことから、パスワードリセットも不可であった。 ・投稿内容を見ると、ほとんどの投稿が削除されており、政治的な発言が投稿されていた。
対処	・短文投稿サイトの SNS 運営会社に連絡し、本人確認後、パスワードリセットが認められた。しかし、これ以上の対応(過去の投稿の復元、ログの解析や提供) はできないとの回答があった。 ※やり取りはすべて現地の言葉で行われた ・短文投稿サイトは、アカウントを退会(削除)できない仕様となっていたため、投稿内容及び登録していた画像をすべて削除した。 ・警察とも相談して対応したが、過去の投稿が削除されているため、被害を証明することが難しいことに加え、SNS 運営会社が日本にはないため、対応が難しい案件となった。

	・SNS 運営会社の日本の代理店を通じて、有料の公式アカウントを申請した。新しいアカウントができ次第、新アカウントへ旧ユーザーを誘導する予定。
原因	・攻撃者が ID/パスワードの認証を突破し、短文投稿サイトのアカウントを乗っ取ったものと思われる。
再発防止策	・２段階認証を有効化し、不審なログイン試行(通常と異なる環境からのログインや連続パスワード試行等)が発生した際に、認証コードを入力させるようにする。 ・担当者の異動等によりアカウントを引き継ぐ際には、 ・ログインパスワードの変更 ・2 段階認証に用いるメールアドレス(携帯電話番号等)の変更を確実に実施する。

オ　世界中で広く利用されているフリーソフトウェアに由来したサプライチェーン攻撃

概要	・保守ベンダから、マルウェアに感染したフリーソフトウェアに由来する不正通信が検出されたとの報告があった。 ・システム担当が導入していた端末運用管理ソフトウェアにより、フリーソフトウェアをインストールした端末を特定し、早急に端末をネットワーク（インターネットに接続）から切り離した。 ・不正通信は、正規のフリーソフトウェアに埋め込まれたマルウェアによるものであり、フリーソフトウェアを利用していた感染端末以外からの不正通信等はないことを確認した。
背景	・インターネット接続用にファイアウォールを構築していた。 ・端末へのソフトウェアのインストールは許可制(要申請)になっており、その旨は定期的な研修等で伝えていた。
検知	・所管省庁から、広く利用されているフリーソフトウェアのマルウェア感染の可能性について注意喚起があった。 ・保守ベンダからシステム担当に対して、不正通信を行っている端末があることが報告された。
対処	・システム担当が端末運用管理ソフトウェアを利用し、当該ソフトウェアを使用している端末を探り当て、当該端末がマルウェアに感染して不正通信が行われていたことを確認した。 ・ネットワークケーブルの抜線により、不正通信が停止したことを確認した。 ・保守ベンダに調査を依頼し、感染端末以外から不正通信が行われていないことを確認した。 ・状況を上司に報告し、関係省庁等と連携をとった。 ・保守ベンダの調査報告後に、該当端末の OS の再インストールを実施した。

原因	・信頼できると考えられるフリーソフトウェアの正規インストーラにマルウェアが埋め込まれていた。 ・許可を取らずにフリーソフトウェアをインストールした。 ※ただし、今回の場合は申請しても許可されていた可能性あり
再発防止策	サプライチェーン攻撃に対して、決定的な対策を取ることは困難ではあるが、効果があるものと考え、以下の対策を実施した。 ・インストールするソフトウェアの管理・把握を強化した。 ・マルウェア感染事例として注意喚起を実施した。 ・全従業員向けに研修を実施し、セキュリティ意識の高揚を図った。 ・サイバー攻撃に起因した事業継続計画（ICT-BCP）が策定されていないため、策定を検討した。

カ　送信元詐称メールに対する備え

概要	・近年、知名度の高い事業者名を使用した不審メールが出回る事例が多く、送信元を詐称された事業者はどのような対応を行っているのか好事例を調査した。 ・送信元詐称メールの情報は、複数のチャネルから寄せられていた。 ・情報はインシデント対応部門に集約され、迅速な対応がなされていた。
背景	・知名度の高い金融機関や物流事業者、テーマパーク等の事業者名を送信元に詐称する不審メールが増えている。 ・特に、重要インフラ事業者は、顧客からの信頼も厚いため、攻撃者に社名が利用されやすいと考えられる。 ・利用者からの信頼を維持するために、どのような対応が望ましいのか好事例を調査した。
検知	・送信元詐称メールを認知する経路は、複数のチャネルにわたっていた。具体的には、利用者からの問合せ(コールセンター)、SNS による投稿、セキュリティ関係機関やセキュリティベンダーからの報告、同業他社からの連絡等により、本事案を把握した。 ・大規模なものだと、コールセンターへの問合せ量が通常時の 15 倍近くになることもあった。
対処	・複数の検知経路から受領した情報について、最終的にはインシデント対応部門に集約していた。 ・インシデント対応部門は、HP に迷惑メールの文面等を掲載して注意喚起を行い、さらにコールセンターへの情報提供及び対応の指示を行うなど、対応を迅速に行うための連絡ルートを確立していた。

キ　DDoS 攻撃

概要	・DDoS 攻撃の数日前から、HP への軽微な DoS 攻撃が行われていた（攻撃者による偵察の可能性あり）。 ・その後、匿名の脅迫メールを受信し、ほぼ同時に海外からの DDoS 攻撃が発生し、HP にアクセスしづらくなった。 （同日中に複数回（グループ会社にも攻撃）、数日後にも DDoS 攻撃が発生した） ・当該 HP の代替用サイトを開設するとともに、Web サーバの移設等を行い、影響を緩和した。 ・HP にアクセスしづらくなっている事象について、メールや SNS により顧客に周知した。
背景	・事業者は、メインとなるサービスを HP で提供しており、当該サービスを継続的に提供することが最も重要であると位置づけていた。 ・DDoS 攻撃が発生する数日前から、HP への軽微な DoS 攻撃が行われていた(攻撃者による偵察の可能性あり)。また、関係機関からも同様の情報を得ていた。
検知	・匿名の脅迫メールを受信し(DDoS 攻撃解除のためにビットコインを要求するもの)、ほぼ同時に、海外からの DDoS 攻撃が発生し、HP へアクセスがしづらくなった。 ※同日中に複数回（グループ会社にも攻撃）、数日後にも DDoS 攻撃が発生した。 ・脅迫メールの受信とほぼ同時に DDoS 攻撃が行われたため、攻撃を事前に気づくことはできなかった。
対処	・代替用サイトを開設するとともに、攻撃対象となったグループの Web サイトのサーバー分離等の対応を行った。 ・顧客対応については、HP で対応することができなかったため、メール及び SNS により顧客に周知した。
原因	・事業者は、これまで DDoS 攻撃を受けたことがなく、特段の技術的対策や対応マニュアル等が整備されていなかった。
再発防止策	・早期検知や未然防止の観点から、クラウド型の DDoS 攻撃対策サービスを速やかに導入した。 ・不審メールの受信時やサイバー攻撃を受けた際における情報連絡体制を整備した。 ・DDoS 攻撃等のサイバー攻撃を踏まえた BCP を策定し、業務継続体制を構築することを検討した。

ク　リスト型の不正ログイン攻撃

概要	・事業者が運営している会員サイトに、ログインエラーが急増した。

	・保守ベンダがWAFを用いて、攻撃元のIPアドレスからの通信を遮断した。 ・攻撃者が別のIPアドレスから攻撃を行うことによって、サービスへの影響が出ることを懸念し、会員サイトを一時閉鎖した。 ・攻撃があった時間帯にログインのあったユーザに対して、パスワードを強制変更した。
背景	・会員サイトのセキュリティ対策として、WAF（Web Application Firewall)を構築していた。 ・会員サイトへのログインにはID/パスワードが必要であり、同一IDによるログイン試行が複数回失敗した場合、一定時間アクセスができなくなる設定としていた。
検知	・WAFにより、会員サイトへのログイン試行が増えていることを検知し、保守ベンダが攻撃元IPアドレスからの通信を遮断した後、事業者に報告した。 ・ログの状況から、第三者によるリスト型攻撃と判断した。(数件の不正ログインが成功した形跡があり、氏名やメールアドレス等の情報が盗み見られた可能性がある)
対処	・保守ベンダが、大量のログイン試行を行ったIPアドレスを特定し、WAFにて当該IPアドレスからの通信を遮断した。 ・上司に相談し、攻撃者が別のIPアドレスから攻撃するおそれがあったため、会員サイトを一時閉鎖した。 ・攻撃時間帯にログインのあったユーザのパスワードを強制変更した。 ・パスワードを強制変更したIDのユーザに対して、メールや電話等により、パスワードの変更を通知した上で、会員サイトを再開した。
原因	・WAFによる不正ログインの検知は行っていたが、自動遮断機能は設定していなかった。 ・ユーザが他サイトと同じパスワードを利用していた。
再発防止策	・大量のログイン試行による攻撃を検知した際、WAFにて自動的にアクセスを遮断する設定を行った。 ・他サイトと同じパスワードを利用しないこと、パスワードを定期的に変更することをユーザに周知（メール、ログイン画面）した。

ケ　SQLインジェクションによる個人情報流出

概要	・業務部門は、個人情報を含むHPのコンテンツのサービス終了に伴い、管理しなくなった。 ・攻撃者は、SQLインジェクションにより、サービス終了済みで管理していないHPから顧客情報を取得した。

	・HP の高負荷状態の検知により、本事案が発覚した。さらにセキュリティベンダーの調査により、過去の類似の事案も発覚した。 ・攻撃対象となった不要な HP を削除し、不正アクセスの検知機能を強化した。
背景	・業務部門は、個人情報を含む HP のコンテンツを管理していたが、システム部門で一括管理することとなった。 ・一部のサービス終了済み HP のコンテンツは、業務部門からシステム部門に引き継がれないまま、管理されない状態となっていた。 ・システム部門で管理している HP 等については、脆弱性アセスメントやペネトレ―ションテスト等を実施し、適切に対応していた。
検知	・HP の高負荷状態を検知し、SQL インジェクションによる顧客情報の漏えいが発覚した。 ・セキュリティベンダーの調査により、過去にも SQL インジェクションによって顧客情報が漏えいしていたことも発覚した。
対処	・攻撃対象となった、管理していない不要な HP を削除した。 ・SQL インジェクション等の不正アクセスの検知機能を強化した。
原因	・攻撃対象となった HP は、既に存在自体が認識されておらず、管理や対策が行われていなかった。 ・資産管理台帳が整備されていないことから、担当者がコンテンツを作成・削除・更新した場合に、管理者が認識できる仕組みになっておらず、オリジナルデータのコピー等も複数箇所に散在していた。
再発防止策	・業務部門の情報資産管理が不十分であったため、システム部門は、必要な情報資産以外を削除し、Web サーバを再構築した。 ・検知機能の強化の観点から、導入が容易な WAF のクラウドサービスの利用を開始した。 ・情報共有強化の観点から、経営層が関与するリスク管理委員会を設置した。 ・対策の実効性の観点から、各種関連規程・マニュアルを策定した。

（５）平成 30 年の事例[26]

ア　インターネットサービス利用時の認証の障害

概要	・インターネットを通じて提供される重要インフラサービスにおいて、利用時に認証が必要な一部のサービスが利用できなくなる事象が発生。 ・原因は、利用者の認証に使用している外部事業者のクラウド型認証サービスの障害。当該外部事業者では、データセンターの移行のために新旧データセンターを暫定のネットワークで接続しており、そのセキュリティ強化のためにネットワーク認証を導入していたが、認証情報の有効期限が切れたことにより、通信断が発生。 ・恒久対策として、特定の外部事業者１社のサービスに依存しないよう、複数の認証方法の導入を検討。
背景	・インターネットを通じて提供される重要インフラサービスにおいて、利用者の認証に外部事業者（海外）のクラウド型認証サービスを採用していた。 ・外部事業者では、クラウド認証サービスの基盤があるデータセンターの移行を進めており、新旧データセンター間を暫定ネットワークで接続し、セキュリティ強化の為にネットワーク認証を導入していた。
検知	・監視システムにてクラウド型認証サービスの異常を検知。 ・障害発生直後からコールセンターに多数の問い合わせ。
対処	・重要インフラシステム側のログのエラー情報から、クラウド型認証サービスでの障害であることを特定。 ・システムベンダ経由で、外部事業者から障害に関する調査・対応状況を収集し、テレビ会議で利用者対応部門（広報、コールセンター等）にリアルタイムに共有。 ・外部事業者による復旧までの間、ホームページとコールセンターを通じて、復旧状況を利用者に逐一提供。
原因	・ネットワーク認証の認証情報の有効期限切れにより、新旧データセンター間の接続に障害が発生した結果、旧データセンター側のシステムに登録されていた利用者情報との照合ができなくなった。 ・ネットワーク認証の認証情報は自動で更新される仕組みであったがプログラムの不具合により更新されなかった。
再発防止策	・重要インフラサービス側の認証機能の多様化や代替手段の導入を検討し、特定１社への依存を解消。

[26] サイバーセキュリティ本部 重要インフラ専門調査会 第 18 回会合 「資料６ 重要インフラにおける補完調査について(2018 年度)」を基に作成。
https://www.nisc.go.jp/conference/cs/ciip/index.html

	・外部事業者の現地の運用者とのホットラインを構築し、日本法人を経由する連絡体制で生じる時間ロスを解消。

イ　重要インフラ事業者間での映像データ送受信の中断

概要	・重要インフラ事業者間で映像データの送受信に使用している回線が、予約日時に切り替わらず、接続障害が発生し、受信側の重要インフラ事業者では予定の映像を利用者に提供できなくなった。 ・回線が切り替わらなかった原因は、回線を提供している通信事業者の回線制御システムの不具合。 ・通信事業者の回線網は冗長化されているため、回線起因の障害は当該重要インフラ事業者では前例が無かったが、「サービス（映像の提供）の継続を最優先に行動」という共通の対応方針の下、衛星回線経由のルートに切り替え、迅速に復旧。
背景	・重要インフラ事業者間で、サービスに使用する映像データを送受信する際、通信事業者の回線を利用している。 ・回線は、通信事業者の回線制御システムに使用時間帯を予約設定することで時間帯毎に切り替わる仕組み。
検知	・受信側の重要インフラ事業者のオペレーターが、映像提供予定時刻に映像データが届いていないことを発見。同時に、受信側の重要インフラ事業者では利用者に提供する映像に異常が発生。 ・送信側の重要インフラ事業者は、受信側からの連絡により、映像データが正常に届いていないことを認識。
対処	・回線制御システムの予約含め、重要インフラ事業者側の操作ミスや設備不具合を調査したが、該当無し。 ・重要インフラ事業者から通信事業者に問い合わせたが、原因・復旧共に不明との回答。 ・送信側で、別の通信事業者が提供するバックアップ用の衛星回線への切り替えを決定し、送信のタイミング等を連絡。 ・受信側は、通信事業者の回線の復旧までの約 30 分間、手動操作によりサービスを継続。
原因	・通信事業者の回線制御システムのソフトウェア不具合。（通信事業者内でも回線は冗長化されていたが、制御するソフトウェア側の不具合のため機能せず）
再発防止策	・回線制御システムの不具合の解消（通信事業者にて実施）。 ・通信事業者に対する、異常発生時の迅速な情報提供の依頼。 ・緊急時対応プロセスの更なる効率化による有事の切り替え時間短縮、及びオペレーター全員への定期訓練等による手順の浸透。

	・自組織全体、及び同じ分野の重要インフラ事業者への事例共有による、分野内での類似事案への対処能力の強化。

ウ　重要インフラサービスの受付業務の遅延

概要	・複数の事業者が利用する顧客受付システムを接続する共通ネットワークにおいて、ある事業者の設定ミスによりループが発生。ネットワーク全体が輻輳し、複数の事業者が当該システムを利用できなくなった。 ・現場担当者は、別の経路を利用して顧客受付システムに接続し、業務を継続。 ・恒久対策として、システムベンダでネットワーク機器の交換および障害検知のためのログ監視ツールを導入。
背景	・複数事業者が利用する顧客受付システムのネットワークに、個々の重要インフラ事業者が管理する部分と、複数事業者が利用する部分（共通ネットワーク）がある。 ・共通ネットワークについては、システムベンダに保守を委託している。
検知	・重要インフラ事業者の現場担当者が、当該システムが利用できなくなっている状態を検知した。
対処	・現場担当者は、まずシステムベンダに連絡し、ネットワークベンダにて原因の切り分け作業を行った。 ・切り分け作業の結果を元に、システムベンダにて調査を開始した。 ・経路のループの箇所を特定し、設定を修正することでネットワークを正常化した。 ・顧客受付システムは別のネットワーク上に設置されていたため、現場担当者はインターネット経由、もしくはバックオフィスの専用端末で当該システムに接続することで顧客の受付業務を継続した。
原因	・共通ネットワークに接続する他事業者の作業ミスで、当該事業者と共通ネットワークとの間でループが発生した。 ・共通ネットワークが輻輳し、接続された複数の事業者において、顧客受付システムが利用不可となった。
再発防止策	・システムベンダにおいてループが発生しないネットワーク機器および障害検知のためのログ監視ツールを導入。 ・対処に時間がかかったことへの対策として、委託先のシステムベンダの保守体制（緊急時の情報伝達経路等）の見直しを依頼。 ・顧客受付システムを利用する事業者間で事例を共有。

エ　IoT デバイスへの不正侵入及び改ざん

概要	・重要インフラ事業者が管理する施設情報の監視に使用していたネットワークカメラが外部から侵入され、管理ログインができなくなる、映像が改ざんされる、などの被害が複数の分野で発生した。 ・侵入された原因は、第三者が容易に類推できるパスワードや、アクセス制御の不備。 ・今回の件を受け、ネットワークに接続する IoT 機器のパスワード設定やファイヤーウォール等でのアクセス制御の総点検を行ったほか、導入時のセキュリティ上の考慮事項を内規に盛り込んだ。
背景	・重要インフラ事業者の施設情報の監視・公開を目的として、ネットワークカメラを設置し、映像を Web サイトで公開。
検知	・施設の映像を確認するためにアクセスした従業員が、複数のカメラの映像内に不審なメッセージを発見。 ・ネットワークカメラのパスワードが侵入者により変更され、管理画面にログインできなくなっていた。 ・他の事業者でもネットワークカメラに対し、同様の不正侵入が確認され、メーカーから注意喚起が発出された。
対処	・Web サイトでの監視映像の公開を停止し、当該カメラに対する外部からの直接アクセスも制限。 ・当該重要インフラ事業者が保有している全ての IoT 機器の状況を調査。念のためパスワードを全て変更。 ・対応方針について、同時期に同様の攻撃を受けた同じ分野の事業者と情報交換、外部の調査機関にも相談。 ・侵入された機器をネットワークから切り離したうえで、ログ等の痕跡を保全するため電源は維持し、外部の調査機関立ち合いのもと、調査。１日分のログしか残らない設定となっていたため、侵入元特定には至らず。 ・Web サイト閉鎖中の代替措置として、従業員による目視で施設の監視を行い、状況を Web サイトや Twitter を通じて利用者に逐一伝達。 ・代替機器を手配し、監視映像の公開を再開。
原因	・ネットワークカメラのパスワード設定は、導入時、事業者と機器設置業者のいずれでも検討されず、初期設定のまま運用されていた。 ・ネットワークカメラへの直接アクセスによる閲覧は許可する予定はなかったが、特にアクセス制限を行っていなかった。
再発防止策	・IoT 機器のセキュリティ設定やログの取得・保存期間に関して、導入時および運用時の手順を見直し、利用部門への研修も企画。

	・IoT 機器を調達する際の検討事項として、認証やアクセス制御等のセキュリティ機能の観点を追加。 ・ネットワークカメラへのアクセスは VPN 経由のもののみ許可するようにし、外部からアクセスできないようにネットワークを構成変更。

オ　脆弱性を悪用した攻撃

概要	・ネットワーク機器の脆弱性をついた DoS 攻撃により、複数の Web 上のサービスが停止した。 ・当初はシステム障害として対応したが、ベンダに調査を依頼したところ、ネットワーク機器の特定の機能に含まれる脆弱性をついたサイバー攻撃が原因だと判明し、社内 CSIRT 部門に報告した。 ・脆弱性を含む機能の停止、及びファームウェアのバージョンアップを実施した。
背景	・事案発生の数日前、当該脆弱性を利用した攻撃があったという情報をつかんだ。 ・該当機器には、情報をつかんだ 10 日後の、月次メンテナンスの日にパッチを適用する予定であった。
検知	・システム監視にて検知し、保守担当にて確認した。 ・ネットワーク機器のステータスランプが点滅状態（正常時は点灯）になっていたため、ハード故障と判断し対応した。
対処	・ネットワークから該当機器を切り離しバックアップ用の機器で運用し、翌日には該当機器を交換した。 ・ベンダーにて該当機器のログ等を調査したところ、ネットワーク機器の特定の機能の脆弱性をついたサイバー攻撃が原因と報告があり、社内 CSIRT に報告した。 ・　脆弱性を含む機能を停止し、ファームウェアをバージョンアップした。
原因	・ネットワーク機器の特定の機能の脆弱性をついた攻撃が原因であった。 ・該当機器では、アクセス制限を使用機能に応じたプロトコルと IP アドレスで実施していたが、本脆弱性がある機能に気がつかず、アクセスが可能な状態になっていた。
再発防止策	・本内容を社内、グループ会社で共有した。 ・普段使用しない機能の脆弱性をついた攻撃であったことから、他にも各ネットワーク機器で動作中の機能を確認し、不要な機能を停止した。 ・ネットワーク機器への脆弱性が出た場合は、検証環境にて対象かどうかの確認を行う、診断ツールが利用できる場合は使用する等、社内ルールを変更した。

	･サイバー攻撃に関する勉強会を定期的に実施することとした。

カ　広域 DoS 攻撃による Web サイト閲覧障害

概要	・ ある分野の広範囲の重要インフラ事業者に DoS 攻撃があり、運営している Web サイトが閲覧できなくなった。 ・ 異常を察知した重要インフラ事業者が、当該分野の全体調整を行っている分野 CSIRT に報告した。 ・ 報告により得られた内容から原因を特定し、被害を受けている事業者に攻撃元等の情報を展開することで、事態の収束を図った。また、被害を受けていなかった同一分野の重要インフラ事業者にも攻撃元等の情報を共有し、セキュリティインシデントの抑止に繋げた。
背景	・ 複数の重要インフラ事業者において、Web サイトの運用を同一の事業者に委託していた。
検知	・ Web サイト運用担当者が、Web サイトの表示が不安定であることに気づいた。 ・ 外部機関からも「攻撃を受けているのではないか」、という指摘があった。
対処	・ インシデントハンドリングを実施することとなっている事業者に状況を報告し、関係する事業者全体の被害状況を把握した。 ・ 取りまとめられた状況から、攻撃元 IP アドレス等の詳細な攻撃情報を関係事業者全体に周知した。 ・ 委託事業者に Web サイト運用サーバへの攻撃を遮断するよう指示した。
原因	・ 委託先運用のサーバへの DoS 攻撃
再発防止策	・ 委託先事業者に指示し、関係事業者を防護しているファイアウォールに攻撃元と考えられる IP アドレスをリスト登録した。 ・ 早期に情報共有できる体制を構築し、サイバー攻撃があった際、関係する事業者に素早く展開できるよう、共有体制の見直しを行った。

キ　商用ネットワークの高負荷による通信障害

概要	・ DNS サーバに通常の数十倍以上の大量のアクセスがあり、DNS サーバからの応答ができなくなったことで、利用者がインターネットに接続できなくなった。DNS サーバへの DoS 攻撃の可能性も視野に入れ、調査を実施。 ・ 原因は、経路上のネットワーク機器と DNS サーバ間で大量のトラフィックが発生し、DNS サーバにアクセスしづらいなどの影響が発生したことによるもの。当該 DNS サーバと同一セグメントにあるメールサーバ等への接続にも影響が出たほか、機器監視

	も同一セグメントで行っていたため、ログが追えない状態となった。 ・ 今後に備えた対策として、監視用の専用ネットワークの整備や帯域制御などの設計の見直しを行った。
背景	・ 利用者にインターネット接続サービスを提供していた。 ・ 機器の監視は、商用ネットワークで実施していた。 ・ 商用ネットワークは帯域制御しておらず、異常トラフィックを考慮した設計となっていなかった。
検知	・ 利用者から、「インターネットに接続できない」という問い合わせがあった。 ・ 商用ネットワークの状況を確認するために、機器にアクセスしたが、輻輳が発生しており、確認できなかった。
対処	・ 現地で直接各ネットワーク機器の通信状況を確認した。 ・ 通信内容から、特定の機器間で通信が再送され続けていることを確認。サイバー攻撃の可能性も考慮し、対応を実施した。 ・ 当該機器を再起動し、輻輳が正常化したことを確認後、機器を交換した。
原因	・ 当該機器の一部ポートにおけるソフトウェアエラーにより、再帰的にリクエストが発生した。
再発防止策	・ 輻輳によるネットワーク機器のリソース逼迫も誘発していたため、帯域制御を実施した。 ・ 商用ネットワークの障害時にも状態把握が可能となるよう、監視専用のネットワークを別途構築し、監視方法を変更した。 ・ 利用者への周知方法として、自組織の Web サイトを利用する以外に、SNS の公式アカウントを取得し、周知方法を増やした。

ク　他人の認証情報の悪用による情報の不正取得

概要	・ ある重要インフラ事業者では、業務用データは部署ごとにアクセスを制限しており、他部署の従業員の ID によるアクセスは、通常であれば利用できない状態であった。 ・ 不正を行った従業員は、他部署の従業員（被害者）の ID からパスワードを類推し、本来アクセス権の無い他部署の業務用データにアクセスし、機密情報を印刷した上、私的利用していた。 ・ 複合機の印刷ログから不正を行った従業員を特定するとともに、全システムのパスワードを、より複雑性を高めた上で変更を行った。また、全従業員向けに研修を行うことで内部不正の抑止に関する意識向上を図った。
背景	・ 重要データ（顧客の個人情報等）と業務用データ（その他の情報）が別のシステムで管理されていた。

	・業務用データを取り扱うシステムへのログインは、部署ごとにアクセス制御を実施しており、関係する従業員のみ利用可能となっていた。
検知	・該当部署で閲覧不可能な業務用データの資料が印刷され、プリンターに放置されていた。
対処	・プリンターのログを確認し、印刷した端末を特定した。 ・該当する端末を利用している職員に聞き込みを実施し、職員の特定に至った。 ・サーバのアクセスログから、業務用データへの不正なアクセスを開始した時期を特定した。
原因	・業務用データへのアクセスに使用するID・パスワードは、使用頻度が高いことから、類推しやすい平易なものになっていた。
再発防止策	・パスワードの桁数を増やし、ランダムなものに設定しなおした。また、類推しやすい平易なものを設定不可とした。 ・アクセスログを取得していることを含めて、全従業員向けに研修を実施し、内部不正の抑止に関して意識向上を図った。

（６）令和元年の事例[27]

ア　改元に伴うシステム変更トラブルへの対応

概要	・利用者が、2019 年 5 月（改元後）に処理されるサービス（重要インフラサービスに該当）の予約手続きを同年 4 月（改元前）に行ったところ、サービスの提供日が「1989 年 5 月〇日」と表示されるトラブルが発生 ・重要インフラ事業者は、当該トラブルが予約に影響しないことを特定し、サービスを継続する対応を意思決定 ・システムベンダや他の重要インフラ事業者と連携し、利用者への対応を統一して迅速に HP 等で周知し、問い合わせ対応を行ったことで、分野全体で大きな混乱なく事態を収拾
背景	・共同利用型の基幹システムは、店舗端末接続ネットワークを通じて、重要インフラサービスを店舗に提供する。 ・改元対応に向け、約２年前から、システムベンダとも連携し、影響調査や改修等を進めてきた。 ・処理が 5 月以降となるサービス予約の日付の形式（和暦）を、連休前の 2019 年（平成 31 年）4 月 26 日に切り替え、令和の年号に対応した。
検知	・4 月 26 日、店舗端末の利用者から、サービス予約日の日付表示が 1989 年（平成１年）となる旨の問い合わせが、システムベンダ B のコールセンター経由で重要インフラ事業者のシステム部門に寄せられた。 ・システム部門の職員が店舗に出向き再現性を確認
対処	・基幹システムでのサービス予約のステータス確認により、影響はサービス予約の日付表示のみのトラブルであることを特定すると共に、該当する利用者数を正確に把握 ・システムベンダ及び共同利用の重要インフラ事業者と連携して、影響範囲と対応の選択肢を精査し、当該トラブルへの対応方針を統一 ・調査結果と対応方針を顧客対応部門に展開し、顧客からの問い合わせへの態勢を用意 ・トラブル認識から 3 時間後に、ホームページ等を通じて、サービス予約に影響がないことを利用者に提供し、混乱が大きくなる前に事態を収拾
原因	・日付形式の切り替え日に関する認識が、店舗端末接続ネットワーク側との間で異なっていたため。（２つのシステムの切り替えタイミングに関する試験項目の不足）

[27] サイバーセキュリティ本部 重要インフラ専門調査会 第 22 回会合 「資料８ 重要インフラにおける補完調査について（2019 年度）」を基に作成。
https://www.nisc.go.jp/conference/cs/ciip/index.html

再発防止策	・システムの移行計画に関するプロジェクト管理方法（要件定義、試験観点抽出、コミュニケーションプロセス等）の見直し

イ　重要インフラサービスの一部業務の停止

概要	・重要インフラサービスで利用するデータベースのシステムファイルが破損したことにより、顧客がサービスを利用できなくなった。 ・データベースサーバとデータベース間の通信が不安定になった際に発生するデータベースソフトの不具合により、データベースのシステムファイルが破損したことが原因。 ・恒久対策として、データベースソフトの不具合を解消するパッチを適用。
背景	・複数の業務において利用する、認証、印刷等の複数の機能を統合した、共通基盤システムを運用している。 ・システムは、各機能が利用するデータを格納したデータベースサーバと接続している。 ・システムにおいて、インシデント発生の１週間前から、業務に支障がないレベルの通信エラーが頻発していた。
検知	・システムを監視するシステム担当者がアラートの発生を確認し、障害を覚知した。 ・システムを利用する複数の拠点から、印刷処理ができない旨の連絡が寄せられた。
対処	・インシデント発生前から通信エラーが頻発していたため、ハードウェア故障を疑い、ファイバーチャネルを交換した。 ・機器交換後、システムを再起動するも障害が復旧せず、データベースのシステムファイルの破損が判明した。 ・サービスの優先度が高い業務から再開すべく、対応方針を決めた。また、バックアップファイルからシステムファイルを復元することで復旧し、業務を再開した。
原因	・データベースサーバのハードウェア不調により、サーバとデータベース間の通信が不安定になった。 ・サーバとデータベース間の通信が不安定になった場合に発生するデータベースソフトの不具合により、データベースのシステムファイルが破損した。 ・不具合を改修する修正パッチを未適用であった。
再発防止策	・データベース管理システムの修正パッチを適用した。 ・データベースのシステムファイルを三重化した。 ・ハードウェアが不調の場合に速やかに交換できるよう、システムの監視体制を強化した。

ウ　委託先のシステムトラブルに伴うサービス障害

概要	・複数の重要インフラ事業者が共同利用する業務システムにおいて障害が発生し、利用する複数の事業者において同時にサービス障害が発生。 ・重要インフラ事業者は、テレビ会議によりシステムベンダからの報告及び他事業者からの情報共有を受け、状況を把握。早期に代替手段での対応を店舗に指示、ホームページにお詫びを掲載するなどして、混乱を回避。 ・再発に備えた対策として、通信制御ソフトウェアのリソース監視強化、リソース枯渇時の対応マニュアルの策定、共同利用事業者の処理方法変更、他に同様の不備がないかを確認。
背景	・業務システムの開発・運用・保守は、システムベンダに委託していた。 ・当該システムは、汎用機ホストコンピュータ 2 台の 2 系統によるロードシェア構成としており、複数の事業者で共同利用していた。
検知	・システムベンダのオペレーターがシステム障害発生を検知。 ・職員が障害の再現性を確認。
対処	・ホームページ上へのお詫びの掲載、他事業者の店舗への誘導、当該システムを利用しない代替手段での顧客対応等を実施。 ・システムを共同利用する複数の事業者間で、テレビ会議システムを利用して情報共有。 ・2 系統のうち、障害が発生していないホストコンピュータへ片寄せ。 ・ホストコンピュータ、通信制御ソフトウェアを再起動。
原因	・大量データの処理が一時的に集中し、ホストコンピュータ上の通信制御ソフトウェアのリソースが枯渇。
再発防止策	・通信制御ソフトウェアのリソース監視強化。使用率がしきい値を超えた場合に警告メッセージを通知するようプログラムを変更。 ・リソース枯渇時の対応マニュアルを策定。 ・データ処理が集中しないよう、共同利用の事業者を順番に処理するように変更。 ・障害発生時、システムベンダから重要インフラ事業者の担当者への第一報がより迅速に伝えられるよう、初動対応を見直し。 ・業務システムの再点検(本件同様の不備の有無等)。

エ　重要インフラサービスの業務遅延

概要	・重要インフラサービスに遅延が生じたことから、業務スケジュール管理システム経由で業務スケジュールの組み換え処理を試みたが、システムが正常に動作せず、重要インフラサービスの業務遅延が拡大。

	・業務スケジュール管理システムにおいて、排他制御の誤りが発生し、データの不整合が生じたことが原因。 ・再発防止として、データベースから取得したデータが最新であるか否か確認する等、排他制御が確実に実施されるようにシステムを改修。
背景	・重要インフラ事業者では、事象発生当日、重要インフラサービスの一部業務に遅延が生じていた。 ・本重要インフラサービスでは、業務に遅延が生じた場合、業務スケジュール管理システムを操作することで、業務スケジュールの組み換えが自動で実施されるようになっていた。 ・業務スケジュール管理システムでは、複数の運用担当者からの業務スケジュール組み換え操作を誤りなく処理するため、排他制御処理（データベースへの同時アクセスによりデータの不整合が生じないよう、データの読み書きを一時的に制限する処理）を行っていた。
検知	・運用担当者が業務スケジュール管理システムで、業務スケジュールの組み換え処理を実行したが、変更が反映されなかったことで、事象を把握。
対処	・システムベンダに原因の調査を指示 ・業務スケジュール管理システムの再起動。 ・重要インフラサービスの進行状況の更なる遅延を防止するため、業務スケジュールの組み換えを手動で実施。
原因	・関連システムの一部更改や通信回線速度の高速化の影響で業務スケジュールの組み換え処理の実行速度が向上し、一部処理のタイミングずれが生じたため、排他制御が適切に実施されなくなった。 ・排他制御の誤りにより、古いデータを基に業務スケジュールの組み換えが実施され、業務スケジュールデータに不整合が発生。
再発防止策	・排他制御の誤りを防止するため、業務スケジュール管理システムにデータを取得、反映する際に、取得したデータが最新か否か確認する処理をシステムに追加。 ・排他制御の誤りを防止するため、業務スケジュールデータの参照時や更新時に同データにアクセスしている端末が存在するか否か迅速に確認できるよう、システムを改修。

オ　不審メールによるマルウェア「Emotet」への感染

概要	・実在の組織や人物になりすます手口で、マルウェア「Emotet」に感染させる不審メールが流行。 ・重要インフラ事業者の職員が不審メールの添付ファイルを開封し、マクロを有効化したことで、端末がマルウェア「Emotet」

	に感染。感染後、感染端末を使用していた職員を騙るメールが、外部組織に送信。 ・再発防止策として、クラウド型メールサンドボックスの導入や職員に対する継続的なセキュリティ教育を実施。
背景	・実在の組織や人物になりすます手口で、マルウェア「Emotet」に感染させる不審メールが流行していた。添付ファイル(Word 形式)を開き、マクロを有効化することで、端末がマルウェア「Emotet」に感染した。 ・重要インフラ事業者では、スパムメールフィルタを導入済。 ・重要インフラ事業者は、CSIRT 間の情報共有コミュニティに参加しており、他の CSIRT に相談しやすい状況にあった。
検知	・重要インフラ事業者（発生組織）の職員になりすましたメールを別部署の職員が受信、発生組織へ連絡したことで、担当者が事象を把握。
対処	・マルウェア感染が疑われる端末について、フォレンジック事業者にフォレンジック調査を依頼。 ・重要インフラ事業者が管理する全ての端末に対して、ウイルス対策ソフトのフルスキャンを一斉に実施。 ・迅速に第一報を公表した後、詳細な調査結果が判明する度に、続報を公表。
原因	・重要インフラ事業者の職員が、外部から送信された不審メールの添付ファイルを開封してしまった。
再発防止策	・組織内のメールセキュリティ対策を強化し、比較的導入が容易なクラウド型のメールサンドボックスソリューションを導入。 ・攻撃の特徴や対策をまとめたリーフレットを全職員に配布。さらに、職員のセキュリティ知識の定着状況を確認するテストを実施。

カ　重要インフラ事業者が利用するサーバへの不正アクセス

概要	・重要インフラ事業者が利用するサーバが不正アクセスされ、同サーバから外部に不審なメールが送信。 ・サーバに導入していたコンテンツ管理システム(CMS)のプラグインの脆弱性を悪用し、攻撃者がサーバに不正アクセスした可能性が高いと考えられる。 ・重要インフラ事業者は、新たにサーバの運用契約をベンダと締結し、サーバのパッチ適用やインシデント発生時のログ調査をベンダに迅速に依頼できるようにした。
背景	・重要インフラ事業者のシステム部門がレンタルサーバを契約し、複数部署でサーバを共同利用していた。 ・重要インフラ事業者自身がサーバへのパッチ適用を実施していた。

	・インシデント発生以前から、同レンタルサーバ上で構築された Web サイトのレイアウトが崩れるといった事象が発生していた。
検知	・レンタルサーバの提供事業者が「当該重要インフラ事業者が利用するサーバから不審なメールが送信されている」と連絡したことで重要インフラ事業者は事象を把握。
対処	・レンタルサーバの提供事業者が、当該サーバを迅速に停止。 ・バックアップ取得後、サーバの全データを削除し、別環境にて代替サイトを構築。 ・システム部門が、レンタルサーバの利用者に対し、パッチ適用の最新化等を求める注意喚起を発出。 ・警察に本事案の届出を実施。
原因	・コンテンツ管理システム(CMS)のプラグインの脆弱性を悪用され、サーバが不正アクセスされた可能性が高い。
再発防止策	・新たにベンダとサーバの運用契約を締結し、パッチ適用やインシデント発生時のログ調査をベンダに迅速に依頼できるようにした。

キ　クラウド型メールサービスに対する不正ログイン

概要	・重要インフラ事業者が利用するクラウド型メールサービスに対し、攻撃者が不正アクセスを実行し、重要インフラ事業者のメールアカウント経由で、当該事業者とは無関係なメールが大量に外部へ送信。 ・重要インフラ事業者の職員が受信メールボックスを確認した際、身に覚えのない配信エラーメールが複数存在していることに気付き、本事象を把握。 ・再発防止として、クラウド型メールサービスのログイン画面へのアクセス制限や取得可能なログの整理と設定の見直しを実施。
背景	・重要インフラ事業者では、クラウド型メールサービスを利用しており、同サービス上に、重要インフラ事業者配下の各組織の代表メールアカウントを作成していた。 ・ログイン画面で、ID(メールアドレス)とパスワードを入力することで、メールサービスを利用可能であった。
検知	・職員が自組織の代表メールアドレスを確認した際、身に覚えのない配信エラーメールが受信メールボックス内に複数存在していることに気付き、事象を把握。
対処	・不正アクセスされたメールアカウントのロックを実施。 ・同メールアカウントを使用していた職員の端末全てに対し、ウイルス対策ソフトのフルスキャンを実施。 ・重要インフラ事業者配下の全ての組織のメールアカウントに対して、ログインパスワードを変更。

	・クラウド型メールサービスのログ等をもとに、攻撃者が不正ログインしたアカウント経由で外部に送信したメールの件数や不正ログインの痕跡を特定。
原因	・クラウド型メールサービスのログイン画面について、どこからでもアクセスできるようになっていた。 ・クラウド型メールサービスに対して、ID とパスワードのみでログインできるようになっていた。
再発防止策	・クラウド型メールサービスのログイン画面にアクセス可能な IP アドレスを制限。 ・クラウド型メールサービスのアクセスログ保存期間を見直し。 ・Web フィルタリングソフトを用いて、過去に職員がアクセスしたフィッシングサイトをブロック。 ・職員に対する e ラーニングやセキュリティ勉強会を実施。

（７）令和２年の事例[28]

ア　ハードウエア故障に伴う重要インフラサービスの停止

概要	・重要インフラ事業者の基幹システムで使用しているNAS(ネットワークストレージ)に障害が発生、当該システムは冗長化していたが、設定値の誤りにより、予備系への自動切り替えに失敗、NAS上のデータにアクセスできなくなり、事業者のルールに基づき、重要インフラサービス(以下「サービス」という)の停止を決定した。 ・システムの再立ち上げによる当日中のサービス再開も検討したが、事前にサービスに関わる関係者との取り決めなく、再開することが混乱を招くと重要インフラ事業者が判断、当日中のサービス再開を断念した。
背景	・重要インフラ事業者では、従前からシステム障害発生時にサービスを停止する条件を定めていた。
検知	・システム監視のアラート通知により、障害発生を検知。
対処	・システム障害の対策本部を迅速に設置、あわせて、経営層が参加するリスク管理にかかる会議体を開催。 ・事業者のルールに基づき、サービスの停止を決定、迅速に公表。 ・事前にサービスに関わる関係者との取り決めなく、障害発生当日中にサービスを再開することが、サービスの混乱を招くと判断し、当日中のサービス再開を断念。 ・サービス停止の謝罪及び停止に至った経緯等を説明する記者会見を開催。 ・NAS(ネットワークストレージ)のマザーボード交換を実施、翌日には、サービスを再開できるようにした。
原因	・本番系システムで利用していたNASが故障、それに伴い、システム障害が発生。 ・本来、予備系システムに自動で切り替わる設計だったが、NASの設置値の誤りにより、自動切り替えに失敗。 ・NASの設定値は、システム構築時は正しいもの(自動切り替えされるもの)だったが、NASの製品仕様の変更により、誤ったもの(自動切り替えされないもの)に変わってしまった。
再発防止策	・システム障害時の予備系システムへの自動切り替えにかかる設定値の総点検を実施、自動切り替えが成功するかを確認。

[28] サイバーセキュリティ本部 重要インフラ専門調査会 第25回会合 「資料４ 重要インフラにおける補完調査について（2020年度)」を基に作成。
https://www.nisc.go.jp/conference/cs/ciip/index.html

	・障害発生当日にサービスを再開するための手続き、手順を関係者と検討し、今後は、サービスを迅速に再開できるようにした。

イ　クラウドでのシステム障害に伴うサービスの停止

概要	・クラウド事業者のクラウドサービス基盤でシステム障害が発生し、重要インフラ事業者のクラウドサービス基盤上に構築した複数の顧客向け重要インフラサービス(以下「サービス」という)が一時停止した。 ・重要インフラ事業者では、複数のサービスへの影響が想定されたことから、迅速にCIOに状況を報告し判断を仰ぎ、さらに、事前に定めていた各サービスの復旧優先順位に基づき、クラウド事業者と連携して、各サービスの復旧を進め、重要インフラサービスの障害による影響を最小限に抑えた。
背景	・重要インフラ事業者とクラウド事業者は、クラウドサービス基盤の利用契約を締結、各部署は、クラウド基盤上に構築した重要インフラサービス(以下「サービス」という)を提供している。 ・重要インフラ事業者は、過去にも本事案と同一のクラウドサービス基盤でのシステム障害を経験していた。 ・上記事案対応時の反省から、重要インフラ事業者は、クラウド上のサービス一覧、各部署の緊急連絡先を事前に収集、サービスの復旧優先順位を定めていた。
検知	・クラウド事業者から、重要インフラ事業者のクラウド契約窓口に、クラウドサービス基盤のシステム障害発生にかかる連絡があり、本事象を認識。
対処	・CIO(最高情報責任者)に、システム障害発生を連絡、クラウド上の複数サービスへの影響が想定されたことから、状況を報告し、指示を仰いだ。 ・クラウド契約窓口から該当する部署に、システム障害発生を通知、サービス影響の確認及び報告を指示。 ・クラウド契約窓口から、クラウド事業者に対して、クラウド上の各サービスの復旧優先順位を通知、優先順位を考慮し、対応を進めるよう連絡。 ・クラウドサービス基盤のバックアップから各サービスを復旧。
原因	・クラウド事業者が、クラウドサービスのストレージのファームウエアをアップデートした際、クラウドサービス基盤の障害が発生。
再発防止策	・重要インフラ事業者とクラウド事業者でサービスレベルの合意(SLA(Service Level Agreement)の締結)を実施。

ウ　システム障害に伴う重要インフラサービスの業務遅延

概要	・業務システム(以下「システム」)で、ハードウエア障害が発生したと誤認識した結果、ストレージがロックされ、データが閲覧できなくなり、重要インフラサービスの業務が一時的に遅延、サービス利用者がサービスを受けられない等の事象が発生 ・事業継続計画に基づき、システム担当部署の職員がシステム上の情報を紙に印刷し、各部署の職員に配布。職員は、紙による事務処理等を行うことで、業務を継続。
背景	・重要インフラ事業者では、業務システム(以下「システム」)上で表示される情報をもとに、サービス利用者にサービス提供や受付業務等を実施していた。 ・システムは、2系統(本番系と予備系)にしており、ハードウエア故障時には、予備系に自動切替されるようになっていた。
検知	・重要インフラ事業者の各部署の職員が、業務システムがフリーズし、情報が閲覧できない旨、システム担当部署に報告したことで、事象が判明。
対処	・施設内にいるサービス利用者に対して、サービスを提供できないこと等を連絡し、代替手段の実施にかかる協力を要請。 ・事業継続計画に基づき、システムの情報を紙に印刷し、各部署に配布し、重要インフラサービスが継続できるようにした。 ・故障の原因が、ハードウエア故障でなかったことから、予備系に自動切替しなかったため、手動切替を実施。 ・別途、本番系を起動し、完全に復旧。
原因	・SAN(Storage Area Network)インターフェースの障害により、ハードウエア障害が発生したと誤認識し、ストレージがロックされ、データを読み取ることができなくなった。
再発防止策	・システム(本番系と予備系)の独立性が担保されているか確認した。 ・本番系と予備系で同じストレージを参照していた部分は、障害時に当該ストレージを参照しない形で運用できるよう変更した。 ・ストレージのロックを検知するプログラムを作成、当該プログラムを用いた定期的な監視により、障害を早期に検知できるようにした。 ・紙による業務継続手段は、緊急マニュアルに記載し、周知していたが、職員の定期的な異動等の理由により、運用が浸透せず、事象発生当日、職員に混乱が生じ、業務が遅延したことから、緊急時はシステム担当部署の職員を派遣する形に変更。

エ　連携サービス間の脆弱性を突いたサービスの不正利用

概要	・重要インフラ事業者は、他事業者が提供するサービスと連携するサービスを提供していたが、利用者から身に覚えのないサービスの利用履歴があるとの問合せを短期間に複数受領。 ・システム担当部署は、問合せが短期間に相次いだことを不審に思い、役員まで報告、該当サービスを一時停止。原因は、サービスを連携する他事業者の仕様変更により生じた連携サービス間の脆弱性の悪用と判明。 ・再発防止策として、他事業者と連携する際のリスク評価に関する規定・要領を見直し、契約も変更。
背景	・重要インフラ事業者では、他事業者が提供するサービスと連携するサービス(以下「連携サービス」という)を提供していた。 ・連携サービス開始後、連携する他事業者が仕様を変更したが、重要インフラ事業者では把握していなかった。 ・利用者から、身に覚えのないサービス利用履歴があるという問合せを受領することは平時からあったが、そのほとんどは利用者の勘違いによるものであった。 ・利用者から、自身のサービス利用履歴を確認したところ、身に覚えのないサービスの利用履歴があるとの問合せを短期間に複数受領した。
検知	・システム担当部署は、同様の問合せが短期間に相次いだことを不審に思い、該当サービスの一時停止を視野に入れて、役員まで報告した。
対処	・同日中にサービスを一時停止した。 ・同日中に事業者内及び関係機関等へ情報を共有し、Web サイトで利用者に対して情報を公開した。 ・同じ連携サービスを提供する他の重要インフラ事業者とも情報交換した。
原因	・サービスを連携する他事業者の仕様変更により生じた連携サービス間の脆弱性が悪用された。
再発防止策	・他事業者の仕様変更により生じた脆弱性を塞ぐよう、連携サービスを修正した。合わせて、他事業者でも、連携するサービスを修正した。 ・他事業者と連携する際のリスク評価に関する事業者内の規定・要領を見直し、これに合わせ、他事業者との契約を変更した。

オ　重要インフラ事業者における 2 度のランサムウエア感染

概要	・重要インフラ事業者の職員が、サーバーのデスクトップ上のファイルが暗号化されていることを認識。原因は、ランサムウエアの感染で、当該ランサムウエアは機密情報の窃取を伴うものではなかった。

	・重要インフラ事業者は、本事案の半年前にも、サーバーがランサムウエアに感染。その対策で、ファイアウォールを導入予定だったが、新型コロナ禍に伴い調達できず、2 度目のランサムウエア感染が発生。
背景	・重要インフラ事業者では、本事案の半年前に、サーバー等がランサムウエアに感染(1 回目)。 ・その対策で、ファイアウォールを導入予定だったが、新型コロナ禍に伴い調達できず未設置。 ・事案 1 回目では、端末やログの保全が遅れたため、調査に必要な情報が揃っておらず、不正アクセスの原因を特定できなかった。
検知	・重要インフラ事業者の職員が、サーバーのデスクトップ上のファイルの暗号化に気づき、事象を把握。
対処	・システム担当部署が、端末・サーバーを、ネットワークから切り離し、保全、使用禁止を迅速に指示。 ・システム担当部署が、システム保守事業者、セキュリティベンダー、警察に連絡、当該事案の調査にかかる協力を依頼。 ・サーバーやネットワーク機器のログ等から、侵入経路を特定。 ・全ての端末・サーバーの ID・パスワードの変更。 ・サーバーのフルクリーンアップにより復旧。
原因	・サーバーがリモートメンテナンスのため、インターネット経由でリモートデスクトップ(RDP)接続可能であり、ID・パスワードも推測可能なものであったため、総当たり攻撃により、RDP 経由で組織内に侵入された。
再発防止策	・ファイアウォールの設置、適切な通信制御の実施。 ・リモートメンテナンスの廃止。 ・全ての端末・サーバーの ID・パスワードを推測が困難なものに変更。

カ　重要インフラ事業者における「WannaCry」の感染

概要	・重要インフラ事業者のネットワークに、マルウエア「WannaCry」に感染した端末が接続、各ネットワークに設置しているパッチ未適用のシステム監視用サーバーを経由して、「WannaCry」の感染が拡大 ・本事案においては、すべての端末において、「WannaCry」によるファイルの暗号化は発生しなかった ・重要インフラ事業者のシステム担当部署の職員が、感染端末のイベントログや端末上に攻撃者が作成したファイルの特徴等から、本事象は「WannaCry」の感染によるものと判断、ネットワークからの切り離しを実施

背景	・2017 年に登場したマルウエア「WannaCry」は、ファイル共有等で利用されるプロトコル SMB に関する脆弱性(MS17-010)を悪用し、感染を拡大する。 ・「WannaCry」には、感染端末上のファイルを暗号化するもの(ランサムウエア)と、暗号化を伴わないものが存在。
検知	・重要インフラサービスに直接影響するネットワークで使用している複数の端末が、再起動を繰り返したことで、異常を把握。
対処	・システム保守事業者に端末再起動の原因調査を依頼。 ・システム担当部署の職員が、端末のイベントログや端末上に攻撃者が作成したファイルの特徴等から、本事象は「WannaCry」の感染によるものと判断。 ・感染端末を特定し、ネットワークからの切り離しを実施。 ・感染端末は、クリーンインストール後にセキュリティアップデートを実施したうえでネットワークに再接続。
原因	・グローバル IP アドレスを割り当てた端末をインターネットに接続した際、適切な対策を講じていなかったことから、脆弱性を悪用され、「WannaCry」に感染。 ・「WannaCry」に感染した端末を、重要インフラ事業者のネットワークに接続、同ネットワーク内のパッチ未適用のシステム監視用サーバーを経由して、別のネットワークの端末に「WannaCry」の感染が拡大した。
再発防止策	・各ネットワークの境界点にファイアウォールを設置し、必要最小限の通信のみ通過させるように設定。 ・利用が終了した端末はクリーンインストールを必ず実施し、端末をネットワークに再接続する際には、ウイルス対策ソフトによるスキャンを必須とするように組織内のルールを変更。

キ　重要インフラ事業者の偽サイトの確認

概要	・重要インフラ事業者の Web サイトをコピーしたサイトが確認された可能性がある旨、警察から連絡があり、調査したところ、偽サイトであることが判明したため、Web サイト、SNS 等で利用者に注意喚起を実施。 ・後日、上記の件が影響し、重要インフラ事業者の Web サイトがスパム対策組織により有害サイトと判定されたことから、重要インフラ事業者は、同組織が管理する拒否リストの解除申請を実施。
背景	・本事案発生当時、国内外の事業者等の Web サイトをコピーした偽サイトが相次いで発見される事象が発生。
検知	【事象①：偽サイトが作成された事案】 ・重要インフラ事業者が、同事業者の偽サイトが確認された可能性があると警察から連絡を受け、事案が判明。

	【事象②：Web サイトが有害サイトと判定された事案】 ・ 重要インフラ事業者の職員が、同事業者の Twitter を確認した際、ツイート内の同事業者の Web サイトへのリンクが有害サイトに判定されていたことで、事案が判明。
対処	【事象①：偽サイトが作成された事案】 ・ Web サイトの保守事業者に原因調査を依頼。 ・ 事業者の Web サイト、SNS 等を通じて、偽サイトの確認に関する注意喚起を実施。 【事象②：Web サイトが有害サイトと判定された事案】 ・ 過去の他事業者の類似事案をインターネットで調査。 ・ スパム対策組織に対し、拒否リストの解除申請を実施。
原因	【事象①：偽サイトが作成された事案】 ・ 攻撃者が、自身で取得したドメインに、重要インフラ事業者の Web サイトの IP アドレスを紐付け、外部 DNS 上で公開したことにより、偽サイトが作成された。 【事象②：Web サイトが有害サイトと判定された事案】 ・ 重要インフラ事業者のドメインが、スパム対策組織が管理する拒否リストに登録されたことで、そのリストを参照していると思われる Twitter が、同ドメインを有害サイトに判定した。
再発防止策	・ 重要インフラ事業者の正規の URL 以外からは、同事業者の Web サイトにアクセスできないように設定を実施した。

ク　問合せシステムを悪用した不正なメールの送信

概要	・ 重要インフラ事業者の Web サイトに設置していた問合せフォームが踏み台として利用され、同事業者のメールアドレスから、不特定多数の第三者に不正なメール(フィッシングメール)が送信された。 ・ 後日、同事業者のドメインがスパム対策組織の拒否リストに追加されたことを契機に、同事業者が送信したメールが迷惑メールに振り分けられ、重要インフラ事業者の顧客に正しく届かない事象が発生。
背景	・ 重要インフラ事業者では、同事業者の Web サイト上に、顧客からの問合せを受け付ける問合せフォームを設置。 ・ 重要インフラ事業者では、システム監視の一環で、メール送信ログを監視していた。
検知	【事象①：不正なメールが多数送信された事象】 ・ メール送信ログの監視により、同事業者のメールアドレスから、大量のメールが送信される事象を検知。 【事象②：同事業者のメールが正しく届かない事象】 ・ 職員が作業中に、同事業者のドメインから送信したメールが、迷惑メールフォルダに振り分けられることを確認。

対処	【事象①：不正なメールが多数送信された事象】 ・攻撃元 IP アドレスをブロックした。 ・事業者の Web サイト、Twitter、アプリ等を通じて、本事象に関する注意喚起を実施。 【事象②：同事業者のメールが正しく届かない事象】 ・スパム対策組織に対し、拒否リストの解除申請を実施。
原因	【事象①：不正なメールが多数送信された事象】 ・攻撃者が、問合せフォームの氏名入力欄に「フィッシングサイトの URL」を、問合せ者のメールアドレス入力欄に「不正なメールの送信先メールアドレス」を入力したため、問合せ受付メール(不正なメール)が第三者に届いた。 【事象②：同事業者のメールが正しく届かない事象】 ・重要インフラ事業者のドメインが、スパム対策組織が管理する拒否リストに登録されたことで、同事業者が外部に送信した一部のメールが正しく届かない等の事象が発生した。
再発防止策	・問合せフォームへの投稿が人間によるものか機械によるものかを判定する技術(CAPCHA)の導入。 ・連続投稿を防止する機能の追加等、一部プログラムを改修。

ケ　業務用 PC におけるサポート詐欺

概要	・被害組織の職員が、夜間、業務用 PC で Web 閲覧した際、警告音が鳴り、ウイルス感染の警告と指定の電話番号へ連絡するよう案内が画面表示された。表示の電話番号へ連絡し、電話先の指示に従い PC 操作を行うと、有償のサービス契約の情報が画面表示。 ・職員が不審に思い、同僚に相談、電話番号を検索したところ、サポート詐欺と判明。 ・再発防止として業務用 PC を使う全職員に対し、最新の攻撃事例を交えたセキュリティ教育を定期的に実施。
背景	・Web 閲覧時、偽のセキュリティ警告を画面表示等し、電話をかけさせ、PC 遠隔操作等のソフトウエアのインストールを促し、対応費用としてプリペイドカード等を搾取する事案(サポート詐欺)が相次ぎ発生している。 ・被害組織の職員が、夜間、業務用 PC で Web 閲覧した際、ウイルス感染の警告画面が表示され、警告音が鳴り、指定の電話番号へ連絡するよう画面表示された。 ・指定の電話番号へ連絡し、電話先の指示に従い PC 操作を行うと、有償サービス契約が画面表示された。
検知	・職員が不審に思い、同僚に相談し、指定の電話番号を検索したところ、サポート詐欺であることが判明した。

対処	・職員は緊急時の連絡体制の連絡順位に従い、緊急連絡先に架電し、その後、システム担当部署の指示に従い、職員らは該当PCを含む被害組織内の全業務用PCをネットワークから切断、同PCを使用中止にした。 ・システム担当部署は、委託先のシステム管理会社に、全業務用PCについて、ウィルスチェック、各種ログ調査等を依頼し、影響範囲を特定した。 ・業務用PCが使用中止になり、職員らは業務影響を抑えるべく、代替手段として別の事業所のPCを使用した。
原因	・職員がWeb閲覧の際、画面表示に従いサポート詐欺の電話番号に連絡した。
再発防止策	・業務用PCを使う全職員に対し、最新のサイバー攻撃事例を交えたセキュリティ教育を月1回程度、実施することとした。 ・夜間や休日でも緊急時に対応できるように、連絡体制を見直し、委託先のシステム管理会社を含む緊急時の連絡体制を再確認し、事業者内でも全職員に再周知した。