記載例

□警報　□注意喚起　■参考情報

（重要インフラ所管省庁→内閣官房）

記載例　：青字
記載上の注意：赤字

情報連絡様式

（第　1　報*）

（*が付与された項目は必須事項）

西暦で記載

24時間表記で記載

識別番号*

情報連絡日時* 2023 年　8 月　19 日　13 時　15 分

（※第1報の識別番号は空欄）

いつ時点での内容かの日付・時間を記載。
（記載するとセルの色は白に変化）

情報連絡元*	省庁名：	XX省	担当者名：	連絡　太郎
	部局名：	YY課		
	電話番号：	03-XXXX-YYYY	FAX番号：	03-XXXX-YYYY
	電子メールアドレス：	renraku.taro@xx.go.jp		

情報共有範囲*

□ RED = 宛先限り
（国家サイバー統括室重要インフラ防護担当(※1)限り）

□ AMBER + STRICT = 特定分野・組織内関係者限り
（国家サイバー統括室重要インフラ防護担当(※1)並びに情報連絡先と直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、組織内関係者限り）

□ AMBER = 特定分野・関係者限り
（国家サイバー統括室重要インフラ防護担当(※1)並びに情報連絡先と直接関係する分野の重要インフラ所管省庁、セプター及び重要インフラ事業者等に属する者のうち、関係者限り）

■ GREEN = 重要インフラ関係主体限り
（国家サイバー統括室、重要インフラ所管省庁、事案対処省庁、サイバーセキュリティ関係省庁、防災関係府省庁、サイバーセキュリティ関係機関、サイバー空間関連事業者、セプター及び重要インフラ事業者等に属する者限り）

□ CLEAR = 公開情報

選択したＴＬＰ（情報共有範囲）に関する補足情報を記載。

特記事項：
企業名・該当サービス等、企業が特定される事項を除いて他分野への情報提供可。

※1：事案対処及び情報の集約・分析のため、必要に応じ、内閣官房（事態対処・危機管理担当）及びあらかじめ連携を要請したサイバーセキュリティ関係機関との間で情報共有を

①発生した事象の類型

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

最初に明らかとなった事象について、１つだけ■を選択する。

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

②上記事象における原因の類型

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

発生原因について■を選択する。複数選択可。

◆情報連絡の内容(※4)　（別紙有無*：☐有　■無）

項　目	リストから選択　情報の内容
③分野名*(※5)	○○分野
④事象が発生した重要インフラ事業者等名	○○株式会社　（西暦で記載）（24時間表記で記載）
⑤概　要	判明日時：　2023 年　8 月　18 日　20 時　0 分 （発生日時：　2023 年　8 月　19 日　2 時　59 分　（サーバログ等より推測）） 事象が発生したシステム・委託先業者等： 会社情報管理サービス（https://example.com/top.php） ・会員がアクセスし、個人情報の変更やサービス申込等を実施。 発生事象の概要： ・○○株式会社の会員情報管理サービスのWEBサイトが改竄された。 ・閲覧したユーザにウイルス感染の恐れがあり、現在、当該サイトを一時閉鎖しサービス停止中。 ・多数の個人情報流出が確認されており、被害の詳細を調査中。 システムの稼働状況：　☐影響なし　■停止中　☐一部稼働中　☐復旧済
⑥重要インフラサービス等への影響	重要インフラサービスのサービス維持レベル(※6)逸脱の有無：　☐有　■無 他の事業者等への波及の可能性：　☐有　■無
⑦当該事象に係る推移等	日時 / 事象・対応状況等 XX/XX 00:00 / 外部より○○株式会社のHPがおかしいと匿名メールを受信。 XX/XX 01:00 / サーバ運用ベンダへ連絡。サーバログ等の調査をし、HPが改ざんされていることを確認。 XX/XX 03:00 / アクセスした利用者にウィルス感染のおそれがあるためサーバを停止。 （必要に応じて行を追加して経緯を記載。） （補足情報） ・XX月XX日現在、○○件の個人情報流出を確認。 （名前、住所、電話番号、メールアドレスが漏えい。） ・コンテンツ管理システムYYYYのv99.99の脆弱性を突かれたものと想定される。
（報道発表等がある場合は、別紙として添付する、あるいは掲載ページのアドレス等を記載。）	対外的な対応状況 報道発表、報道等への掲載：　■済　☐予定有　☐無　（済・予定有では日時・件名を記入） XX/XX 09:00頃　○○株式会社のトップページにニュースリリースを掲載。 （https://example.com/newsXXXX） 個人情報保護委員会への連絡：　☐済　☐予定有　■確認中（済では日時・件名を記入） 現在のところ、個人情報漏洩の事実は確認されていない。 国家サイバー統括室以外に連絡を行った XX/XX 10:00頃　○○県警へ通報
⑧今後の予定	■事象継続中　（続報あり） ☐事後調査実施中　（続報あり） ☐今後の対応策を継続検討　（続報なし） ☐対応完了　（続報なし）
⑨その他 ・得られた教訓等	・現時点での得られた教訓は、経営層への情報のエスカレーション体制を普段から確認し、迅速な判断ができるようにすること。

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