1」

陸幕会第５９７号
令和２年４月２４日

各方面総監
中央会計隊長
中央輸送隊長　殿
各機関の長
（自衛隊体育、情報、需品、輸送、化学、高等工科各学校長を除く。）

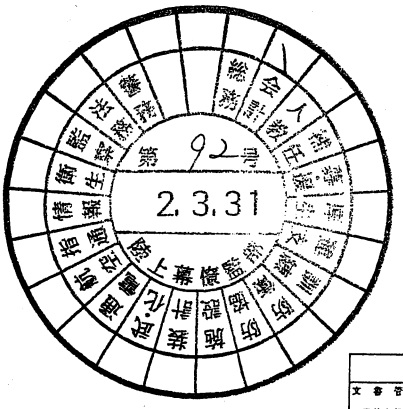
陸上幕僚長
（公印省略）

装備品等及び役務の調達において契約に付したガイドライン又は情報セキュリティ基準に基づき防衛関連企業から報告を受けた場合の速報について（通知）

標記について、別添のとおり通知があったので通知する。

添付書類：装装制第４６０８号（令和２年３月２６日）
配布区分：陸上総隊司令官、会計監査隊長、航空学校宇都宮分校長、小平学校会計科部長

文書管理情報				
文書管理者：陸上幕僚監部監理部会計課長 一元的な管理に責任を有する者：同上 分類：５２－（４）－イ 作成年月日：２．４．８ 取得年月日： 保存期間：１０年 保存期間満了日：１３．３．３１ 本紙含め：１１枚 配布先：以下のとおり２６箇所（うち幕内配布３箇所） 宛先及び配布区分のとおり		開示	部分開示	不開示
	作成時	○		
	区分：１　２　３　４　５　６ 理由：			



装装制第４６０８号
令和２年３月２６日

大臣官房長
各局長
施設等機関の長
各幕僚長殿
情報本部長
防衛監察監
各地方防衛局長

防衛装備庁長官
（公印省略）

文書管理情報			
文書管理者：陸上幕僚監部監理部会計課長 一元的な管理に責任を有する者：同上 分類番号：(52－(4)－イ) 作成年月日： 取得年月日：2.3.31 保存期間：(10年) 保存期間満了日：(13.3.31) 本紙合め：8枚 配布先：以下のとおり　箇所		開示	部分開示	不開示
	作成時	○		
	区分：1 2 3 4 5 6 理由：			

装備品等及び役務の調達において契約に付したガイドライン又は情報セキュリティ基準に基づき防衛関連企業から報告を受けた場合の速報について（通知）

標記について、装備品等の調達に係る秘密等の保全又は保護の確保について（防経装第１９０７２号。２６．１２．２４）（以下「秘密保全通達」という。）第５項並びに装備品等及び役務の調達における情報セキュリティの確保について（防経装第９２４６号。２１．７．３１）（以下「情セキ通達」という。）第１３項の規定に基づき下記のとおり定め、令和２年４月１日から施行することとしたので、通知する。

なお、装備品等及び役務の調達における情報セキュリティの確保に関する特約条項に基づき防衛関連企業から報告を受けた場合の速報について（装装制第６８２号。２７．１０．１）については、令和２年３月３１日付をもって廃止する。

記

１　省内担当部署等（本通知の別図第１、別図第２及び付表に示す部署をいう。以下同じ。）は、装備品等及び役務の調達において、契約に付した秘密保全通達の別添「装備品等の調達に係る秘密保全対策ガイドライン（以下「ガイドライン」という。）」第９(1)又は情セキ通達の別添「調達における情報セキュリティ基準（以下「情報セキュリティ基準」という。）」第１２(1)の規定に基づき、防衛関連企業（秘密（ガイドライン第１に規定する秘密をいう。以下同じ。）又は保護すべき情報（情報セキュリティ基準第２(1)に規定する保護すべき情報をいう。以下同じ。）を取扱う下請負者を含む全ての企業をいう。以下同じ。）から報告を受けた場合には、別図第

１又は別図第２を基準に連絡するものとする。

２　契約担当官等は、ガイドライン第９⑴及び情報セキュリティ基準第１２⑴の報告について、本通知に規定する防衛省における報告先及び防衛関連企業における報告体制を整備することを、平素から防衛関連企業に周知するものとする。特に、下請負者からの報告については、防衛省と直接契約を締結している防衛関連企業を通じて契約担当官等に報告するよう、防衛関連企業に周知しておくものとする。

あわせて、防衛関連企業からの報告の速報性を確保するため、形式に捕らわれることなく電話等の手段を積極的に利用するよう指導するものとする。なお、情報の整理に当たっては、別紙様式によるものとする。

３　防衛関連企業に対する次に掲げるサイバー攻撃等（防衛省の情報保証に関する訓令（平成１９年防衛省訓令第１６０号）第２条第５項に規定するサイバー攻撃等をいう。以下同じ。）があった場合には、ガイドライン第９⑴ア又は情報セキュリティ基準第１２⑴ア、イ及びウに規定する事故又は事故の疑い若しくはおそれがある場合として取扱うことを平素から防衛関連企業に連絡するものとする。これらは例示列挙であり、本事例に準じた事態が発生した場合も同様に取扱うものとする。

なお、防衛関連企業の社内規則において、秘密又は保護すべき情報を紙媒体で取扱うことを規定している場合であっても、防衛関連企業における防衛関連部門（防衛省との契約のための情報を取扱う全部門をいう（秘密又は保護すべき情報を取扱う部門に限定されない。）。以下同じ。）の情報システム（以下「防衛部門システム」という。）に当該情報が意図せずに保存されている可能性を否定することができないことから、防衛部門システムにサイバー攻撃等があった場合には、本規定に該当することも併せて連絡するものとする。

⑴　サイバー攻撃（ネットワークを通じた情報システムへの電子的な攻撃）

ア　主として防衛関連部門に属する社員が、不審なメールの添付ファイルを開いたことによるウィルス感染（ただし、防衛部門システムに全く影響が発生していない場合は、この限りではない。）

イ　主として防衛関連部門に属する社員が、不審なメールのリンクをクリックしたことによるウィルス感染（同上）

ウ　主として防衛関連部門に属する社員が、不正なＷｅｂサイトを閲覧したことによるウィルス感染（同上）

エ　自社のＷｅｂサイトを閲覧したことにより、ウィルス感染したとの外部からの連絡

オ　防衛部門システムにおいて、大量のデータや不正なデータを送りつけられたことによるサーバの処理能力の過負荷

カ　防衛部門システムにおいて、大量のデータや不正なデータを送りつけられたことによるネットワーク帯域の圧迫

キ　自社のＷｅｂコンテンツにウィルスを仕込む改ざん

ク　自社のＷｅｂコンテンツの見た目又は内容が変わる改ざん

ケ　防衛部門システムにおいて使用されるセキュリティ器材等（情報システム以外の物理的なセキュリティ器材等を含む。）による外部への不正な通信の検知

コ　防衛部門システムのネットワークを経由した不正な通信の検知

サ　防衛部門システムを送信元とした不正な通信に関する外部組織からの連絡

シ　防衛部門システムにおいて使用されるソフトウェア等の脆弱性を突いた攻撃による不正侵入又は情報窃取

⑵　サイバー攻撃と同様の影響を発生させる情報システムの誤操作

ア 防衛部門システムの誤操作による外部への不正な通信

イ 防衛部門システムの誤設定による閲覧不可情報の開示

ウ 防衛関連部門に属する社員によるメール誤送信による秘密等又は保護すべき情報の漏えい

⑶　サイバー攻撃以外によるウィルスの混入等

ア 可搬記憶媒体経由による防衛部門システムへのウィルス感染

イ 防衛部門システム導入期からのウィルス混入

⑷　その他

経路を問わず、防衛部門システムに対するウィルス感染の拡大が予想される場合のウィルス検知

４　省内担当部署等は、事故等の対処を円滑に進めるため、相互に連携及び協力を図るとともに、被害の状況その他必要な事項を遅滞なくそれぞれの報告先に連絡するものとする。

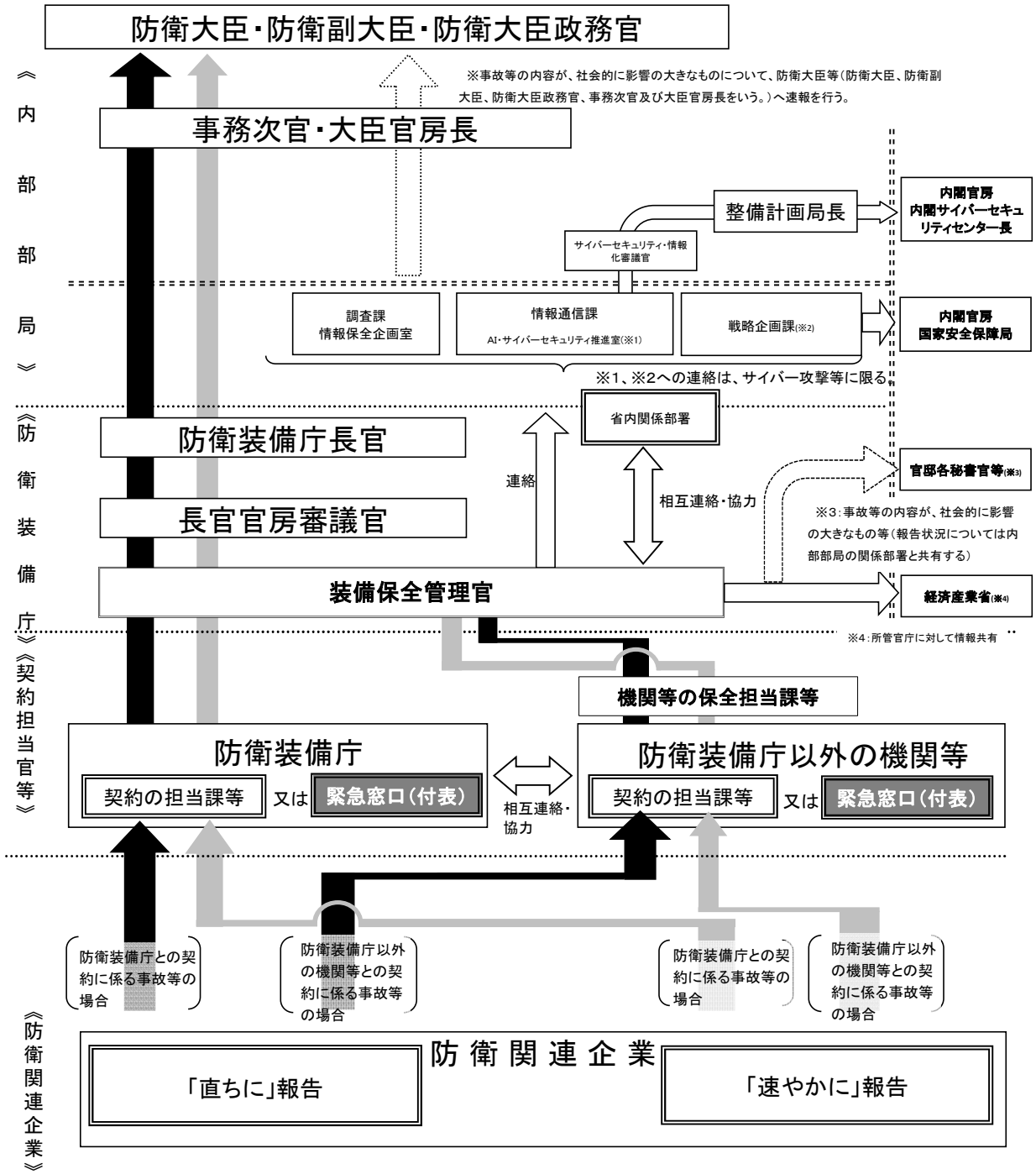
添付書類：１　別図第１及び別図第２

２　別紙様式

配布区分：長官官房会計官、長官官房監察監査・評価官、長官官房各装備開発官、長官官房艦船設計官、各部長、施設等機関の長

別図第１

ガイドラインに基づき防衛関連企業から報告を受けた場合の速報

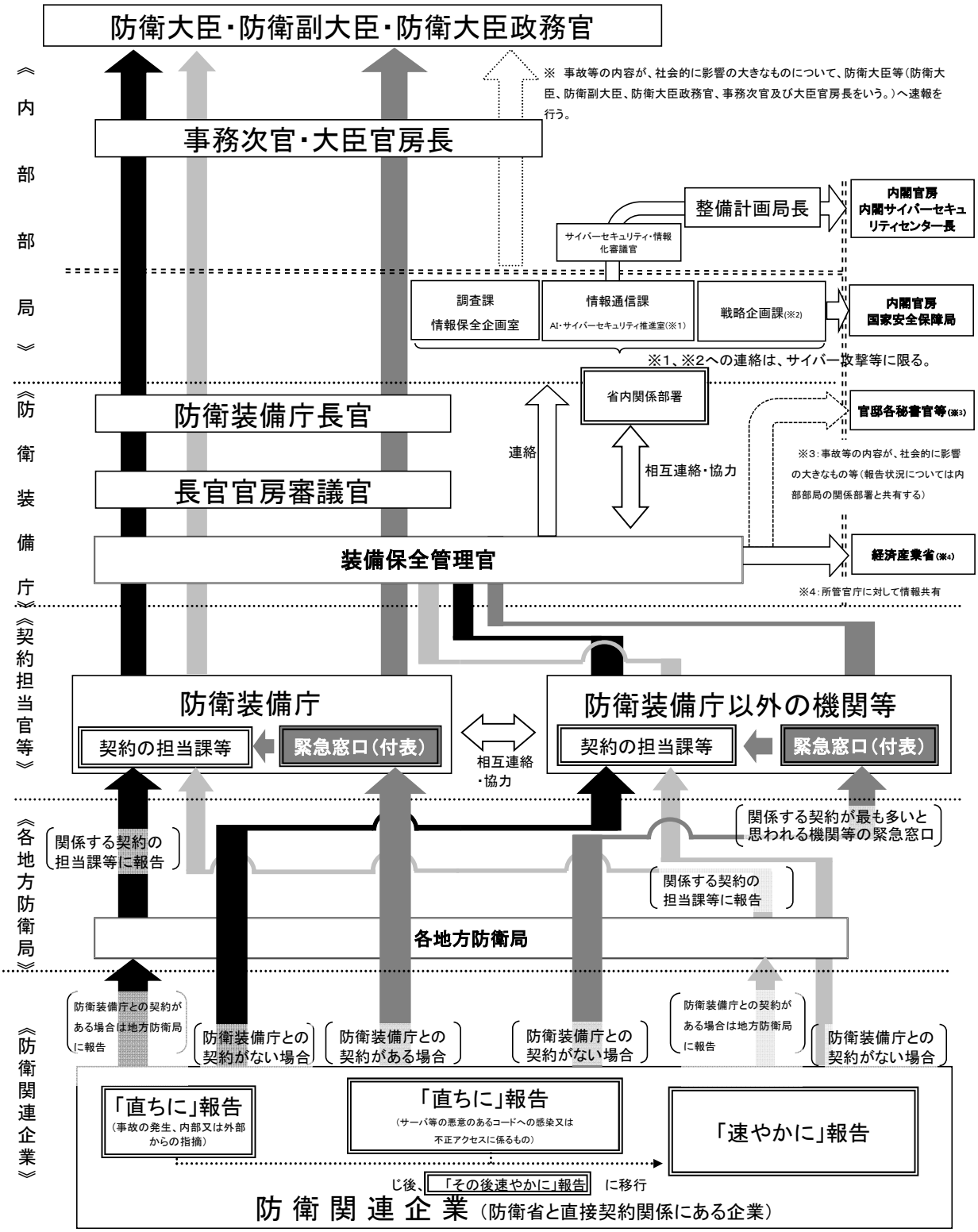


■ 凡例

報告の内容	区分	「直ちに」報告		「速やかに」報告		根拠条文
秘密の漏えい、紛失、破壊（それらの疑い又はおそれがあるときを含む。）に係るもの	事故の発生		把握し得る限りの全ての内容		詳細	ガイドライン第9(1)ア
事故が発生した可能性又は将来発生する懸念についての内部又は外部からの指摘	秘密の漏えい、紛失、破壊等の事故が発生した可能性又は将来発生する懸念について防衛関連企業の内部又は外部から指摘があった場合		当該可能性又は懸念の真偽を含む把握し得る限りの全ての背景及び事実関係の詳細		－	ガイドライン第9(1)イ

別図第２

情報セキュリティ基準に基づき防衛関連企業から報告を受けた場合の速報



■ 凡例

報告の内容	区分	「直ちに」報告		「速やかに」報告		根拠条文
保護すべき情報の漏えい、紛失、破壊等に係るもの	事故の発生	⬆	把握し得る限りの全ての内容	⬆	詳細	情報セキュリティ基準第12(1)ア
	事故の疑い又は事故につながるおそれ					情報セキュリティ基準第12(1)ウ
事故が発生した可能性又は将来発生する懸念についての内部又は外部からの指摘	保護すべき情報の漏えい、紛失、破壊等の事故が発生した可能性又は将来発生する懸念について防衛関連企業の内部又は外部から指摘があった場合	⬆	当該可能性又は懸念の真偽を含む把握し得る限りの全ての背景			情報セキュリティ基準第12(1)エ
サーバ等（サーバ又はパソコンをいう。の悪意のあるコードへの感染又は不正アクセスに係るもの	保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染又は不正アクセスが認められた場合	⬆	把握し得る限りの全ての内容			情報セキュリティ基準第12(1)イ(ア)
	保護すべき情報が保存されているサーバ等と同一のイントラネットに接続されているサーバ等に悪意のあるコードへの感染が認められた場合					情報セキュリティ基準第12(1)イ(イ)

付　表

ガイドライン又は情報セキュリティ基準第12(1)イに基づき
防衛関連企業が防衛省に対して「直ちに」報告を行う場合の緊急窓口

	機関等	緊急窓口	電話番号
防衛装備庁による契約	防衛装備庁	装備政策部 装備保全管理官	03-3268-3111 （内線21040、21043） （夜間・休日等） 080-8420-0628
防衛装備庁以外の機関等による契約	内部部局	大臣官房 会計課管理班契約係	03-3268-3111 （内線20813、20814）
	防衛大学校	総務部 会計課調達係	046-841-3810 （内線2054、2055）
	防衛医科大学校	事務局経理部 経理課調達係	04-2995-1211 （内線2142、2145）
	防衛研究所	企画部 総務課会計室会計第3係	03-3268-3111 （内線29126）
	統合幕僚監部 及び自衛隊指揮通信システム隊	指揮通信システム部 指揮通信システム企画課 指揮通信システム企画班調達係	03-3268-3111 （内線30628）
	陸上自衛隊 （自衛隊情報保全隊、自衛隊体育学校、自衛隊中央病院、陸上幕僚長の監督を受ける自衛隊地区病院及び地方協力本部を含む）	陸上幕僚監部 装備計画部装備計画課 補給管理班	03-3268-3111 （内線40752～40754）
	海上自衛隊 （海上幕僚長の監督を受ける自衛隊地区病院を含む）	海上幕僚監部 装備計画部装備需品課 補給管理室	03-3268-3111 （内線50746・50747）
	航空自衛隊 （航空幕僚長の監督を受ける自衛隊地区病院を含む）	航空幕僚監部 装備計画部整備・補給課 総括班	03-3268-3111 （内線60836）
	情報本部	情報本部総務部 総務課管理班調達係	03-3268-3111 （内線31712）
	防衛監察本部	総務課企画室	03-3268-3111 （内線33062）
	北海道防衛局	総務部会計課総務係	011-272-7560 （直通）
	東北防衛局	総務部会計課会計係	022-297-8210 （直通）
	北関東防衛局	総務部総務課企画係	048-600-1805 （直通）
	南関東防衛局	総務部会計課会計係	045-211-7101 （直通）
	近畿中部防衛局	総務部総務課企画係	06-6945-4951 （直通）
	中国四国防衛局	総務部総務課企画係長	082-223-8284 （内線225）
	九州防衛局	総務部総務課企画係	092-483-8811 （直通）
	沖縄防衛局	総務部総務課企画係	098-921-8131 （内線108）

上記の緊急窓口に連絡がつかない場合
防衛装備庁装備政策部装備保全管理官　　電話　03-3268-3111　（内線35258、35242）
（夜間・休日等）　　電話　080-8420-0628

別紙様式

情報セキュリティ基準第12(1)イの速報
（サーバ又はパソコンの悪意のあるコードへの感染又は不正アクセスに係るもの）

（宛先）

① 会社名 （事業所名を含む）		
② 連絡先部署、担当者名 ③ 電話番号		（内線　　）
④ 速報の内容	第12(1)イ(ア)に規定する速報	□ ア　保護すべき情報が保存されたサーバ等（サーバ又はパソコンをいう。）に悪意のあるコードへの感染が認められた。 □ イ　保護すべき情報が保存されたサーバ等に不正アクセスが認められた。
	第12(1)イ(イ)に規定する速報	□ ウ　保護すべき情報が保存されているサーバ等と同一のイントラネットに接続されているサーバ等に悪意のあるコードへの感染が認められた。
⑤ 現時点でわかっていることの詳細		
⑥ これまでにとった対応		□ ア 悪意のあるコードへの感染又は不正アクセスのあったサーバ等をネットワークから物理的に切断 □ イ 下記の公的関係機関に通報 □ 警察庁サイバーインテリジェンス情報共有ネットワーク □ 独立行政法人 情報処理推進機構 J-CSIP □ その他の機関 〔　　〕 □ ウ その他 （　　）
⑦ 影響のある主な契約 ※個別の契約件名でなくともよい。 (例) 〇〇式〇〇に関する契約		□ ア 防衛装備庁 （担当課等を合わせて明記） （　　） □ イ その他の契約機関 （担当部署を合わせて明記） （　　）

※1　省内関係各署への伝達を迅速に行うため、防衛関連企業から緊急窓口への第一報については、この様式を用いて行うことを基準とする。（作成に当たっては、付紙の記入要領を参照のこと。）

※2　防衛関連企業から緊急窓口への本報告書の送信は、当該緊急窓口に対して必ず電話連絡を行ったのちに、FAX又は電子メールにより行うものとする。また、本報告書を省内関係各署間で送信する場合についても、送信に先立ち、当該送信先に対して必ず電話連絡を行うこと。

※3　防衛関連企業からFAX又は電子メールの送信が不可能な場合は、緊急窓口の担当者が上記を聴取し、以降、本様式により省内関係各署へ伝達する。

付　紙

（記入要領）

情報セキュリティ基準第12(1)イの速報
（サーバ又はパソコンの悪意のあるコードへの感染又は不正アクセスに係るもの）

（宛先）　*防衛装備庁　○○部　○○官　○○　宛*

① 会社名 （事業所名を含む）	*○○(株)　○○事業所*　　チェックは、■、レのいずれでもよい。
② 連絡先部署、担当者名	*○○課　○○*
③ 電話番号	*03-○○○○-○○○○*　　（内線　*○○○○○*　）
④ 速報の内容	第12(1)イ(ア)に規定する速報 ■ ア　保護すべき情報が保存されたサーバ等（サーバ又はパソコンをいう。）に悪意のあるコードへの感染が認められた。 □ イ　保護すべき情報が保存されたサーバ等に不正アクセスが認められた。
	第12(1)イ(イ)に規定する速報 □ ウ　保護すべき情報が保存されているサーバ等と同一のイントラネットに接続されているサーバ等に悪意のあるコードへの感染が認められた。
⑤ 現時点でわかっていることの詳細	*○○に関するデータの流出の可能性あり*
⑥ これまでにとった対応	■ ア　悪意のあるコードへの感染又は不正アクセスのあったサーバ等をネットワークから物理的に切断 ■ イ　下記の公的関係機関に通報 ■ 警察庁サイバーインテリジェンス情報共有ネットワーク □ 経済産業省J－CSIP □ その他の機関　〔　〕 ■ ウ　その他 〔 *社内対策会議を緊急召集* 〕
⑦ 影響のある主な契約 ※個別の契約件名でなくともよい。 (例) ○○式○○に関する契約	□ ア　防衛装備庁　（担当課等を合わせて明記） 〔 *○○式○○に関する契約(装備庁○○官)* 〕 □ イ　その他の契約機関　（担当部署を合わせて明記） 〔 *○○の補用品(陸自○○補給処)* 〕

※　テキスト形式による送信の場合は、下記の略記例を参照

（テキスト形式による送信の場合の略記の例）　※テキスト文中の①～⑦の番号は、上記様式中の番号に対応。

情報セキュリティ特約条項第6条第2項の速報

①　○○(株)　○○事業所
②　○○課　○○
③　03－○○○○－○○○○　(内線○○○○)
④　6-2-1　ア　悪意のあるコードへの感染
⑤　○○に関するデータの流出の可能性あり
⑥　ア　サーバ等をネットワークから物理的に切断
*　　イ　警察庁サイバーインテリジェンス情報共有ネットワークに通報*
*　　ウ　社内対策会議を緊急召集*
⑦　ア　○○式○○に関する契約　(装備庁○○官)
*　　イ　○○の補用品　(陸自○○補給処)*