インシデント対応項目(案) ～初動･影響範囲の確認～

Rev.20160517

①実施した内容については、実施日時、範囲、設定内容の記録を行ってください。
②感染端末や痕跡が発見された場合には、時系列に状況を整理してください。

	対象		APT	不正送金	ランサム	内部不正	項目	内容
1	PROXYサーバ/コンテンツフィルタ	初動	○	○	○	○	現在のログを確保	①ログがローテーションにより削除されないよう、ログを退避します。 （ログが長期間保持できる仕組みになっており、必要なログをすぐに参照できる場合は、この対応は不要となります）
2			○	○	○	○	DHCPログの確保（IPアドレスと機器の特定）	①DHCPを利用している環境では、IPアドレスだけでは機器が特定できないケースがあります。 ②機器を特定できるよう、DHCPのログを確保すると共に調査用に準備しておきます。 （機器の隔離を行うのに必要な情報となります）
3			○	○	○	○	標準時とのズレを確認	①機器がNTP等により標準時同期されているか確認します。同期されていない場合には、標準時とのズレを記録します。 ②標準時と時刻にズレがある場合は、秒単位でのズレを記録します。 ③今後の為、NTPなどを使い標準時と時刻同期するように設定してください。
4			○	○	△		C2サーバへの通信をブロック （C2＝command and control）	①C2サーバのアドレスが判明している場合は、該当アドレス宛の通信をブロックするように設定します。 (C2サーバへの通信が、HTTP/HTTPSだけでなくDNSを利用しているケースもあります) ②C2サーバへの通信をフィルタする際は、IPアドレスベースの指定だけでなく、ドメイン名による指定も行います。 （C2サーバのIPアドレスが変化した時に対応できる様にします） ③既知のC2サーバへの通信を遮断する事で、マルウェアが異なるC2サーバとの通信を開始する可能性があります。新たなC2サーバとの通信が確認された場合は、適宜C2サーバとの通信をブロックするように設定を追加します。
5			△				内部サーバからの外部への通信をブロック	①APTケースにおいて、サーバ機器が侵害されている可能性がある場合、サーバ機器からのデータ流出等を防ぐため下記対策の実施を検討します。 ②サーバ機器が侵害されている可能性がある場合、PROXY経由で行う通信をブロックしホワイトリストによる通信に制限します。 ③サーバ機器がPROXYを経由せずに通信可能な場合は、FireWall にて通信を制限します。
6			○	○	○	○	迂回路の確認	①PROXYサーバを経由せずにインターネットと接続できる経路が無いか確認します。PROXYサーバを経由せずに通信できる経路が存在する場合、問題の通信がPROXYログに記録されていない可能性がある為、PROXYログ調査の意味があるかを検討します。 ②特にサーバ類は、PROXYを経由せずにインターネットとの接続が許可されているケースがある為、例外が無いか確認します。
7		影響範囲	○	○	○		ブラックリストの適用 （既知 C2 サーバとの通信検出）	①PROXYログに対して、すでに判明しているC2サーバ、公開情報やJPCERT/CCから連絡を受けたC2サーバとの通信が記録されていないか確認します。 ②C2サーバと通信を行っている機器を発見した場合は、該当機器の隔離など初動対応を行います。
8			○	○			PROXYログ内容の精査	①一定の時間間隔でインターネット上のサイトと通信を行っている端末が無いかを確認します。 （就業時間外など、利用者による通信でないと考えられる時間帯で通信の発生状況を確認） ②一定間隔で不審な通信が存在する場合、文字列パターンの特徴などで参考情報がないかを検索、VirusTotalなどを使い該当サイトの安全性などを確認すると共に、機器の利用者による通信か確認します。 ③C2サーバとの通信である可能性がある場合は、通信元の機器を特定し初動対応を行います。
9			○					①HTTP の CONNECT 通信において非常に長い時間セッションが張られている通信が無いか確認します。 （C2サーバとの通信にCONNECTが利用され、セッションを長時間維持して通信している場合は、通信開始時のログだけでは、頻繁に通信が発生いている事を把握しにくい可能性があります。）
10			○	○				①PROXY認証を利用している場合、一定間隔で認証に失敗しているアカウントが無いかログを確認します。 ②一定間隔で認証に失敗し、マルウェアによる通信失敗の可能性がある場合は、通信元の機器を特定し初動対応を行います。
11			○	○				①GETメソッドを利用し、不審な実行形式ファイル（EXE)をダウンロードしているレコードが無いか確認します。

	対象		APT	不正送金	ランサム	内部不正	項目	内容
12			○	○		○		①通常利用が無い海外サイトへの通信が発生していないか確認します。 ②通常利用がないWebストレージ（DropBox等）への通信が発生していないか確認します。 ②不明な海外サイトへの通信が確認された場合は、VirusTotalなどを使い該当サイトの安全性などを確認すると共に、機器の利用者による通信か確認します。
13			○					高度サイバー攻撃への対処におけるログの活用と分析方法 https://www.jpcert.or.jp/research/apt-loganalysis.html ①CONNECTメソッドを利用した 80/tcp への通信、443/tcp 以外のポートへの CONNECT 通信 ②標準利用以外のUser-Agentの検出 ③大量のHTTP通信
14	FireWall	初動	○	○	○	○	現在のログを確保	①ログがローテーションにより削除されないよう、ログを退避します。 （ログが長期間保持できる仕組みになっており、必要なログをすぐに参照できる場合は、この対応は不要となります）
15			○	○			C2サーバへの通信をブロック	①C2サーバのアドレスが判明している場合は、該当アドレス宛の通信をブロックするように設定します。 ②C2サーバへの通信をフィルタする際は、IPアドレスベースの指定だけでなく、ドメイン名による指定も行います。 （C2サーバのIPアドレスが変化した時に対応できる様にします）
16			○				外向き通信の制限	①インターネットに向けた通信を必要な通信だけに制限します。 ②特にサーバ機器からのインターネットに向けた通信は遮断処理を行い、ホワイトリストに従い許可します。 例）プロトコル毎に通信を制限します HTTP/HTTPS通信はPROXYサーバ経由のみ許可。DNSはDNSサーバからのみ許可。メールはメールサーバからのみ許可。
17		影響範囲	○	△	△		ブラックリストの適用 （既知 C2 サーバとの通信検出）	①FireWallログに対して、すでに判明しているC2サーバ、公開情報やJPCERT/CCから連絡を受けたC2サーバとの通信が記録されていないか確認します。 ②C2サーバのアドレスとIPアドレスの紐付けは別途行う必要があります。DNSサーバで名前解決のログを取得している場合は、DNSサーバのログを利用します。または、PassiveDNS などの情報・サービスを利用する方法もあります。 ③C2サーバと通信を行っている機器を発見した場合は、該当機器の隔離など初動対応を行います。
18			○	△	△	○	FireWallログ内容の精査	①FireWallのログにて、インターネット向けの通信でブロックされている（通常利用が無いポートでの）不審な通信が無いか確認します。 ②ブロックされている不審な通信を発見した場合は、機器の利用者による通信か確認します。マルウェアによる通信失敗の可能性がある場合は、通信元機器を特定し初動対応を行います。
19			○					高度サイバー攻撃への対処におけるログの活用と分析方法 https://www.jpcert.or.jp/research/apt-loganalysis.html
20	DNS	初動	○				現在のログを確保	①DNSサーバにおいて、名前解決のログを記録している場合のみ該当 ②ログがローテーションにより削除されないよう、ログを退避します。 （ログが長期間保持できる仕組みになっており、必要なログをすぐに参照できる場合は、この対応は不要となります） ※PassiveDNS などの情報・サービスを利用する方法もあります。
21			○				C2サーバへの通信をブロック	①DNSサーバのログにて、ホスト名 やTXTレコードを利用しエンコード（例：BBY4HvMtGqIINDTHZHVlSdvqu9Jb47xp.mail.example.com）された不審な名前解決が発生していないかを確認します。 ②マルウェアがDNSの通信を通じてC2サーバとの通信を行っている場合は、該当DNSサーバとの通信をFireWall等でブロックします。
22	VPN / RAS	初動	○			○	正規のリモート接続手段の悪用	①ログがローテーションにより削除されないよう、ログを退避します。 （ログが長期間保持できる仕組みになっており、必要なログをすぐに参照できる場合は、この対応は不要となります）
23		影響範囲	○			○		①アカウント ログオン履歴を確認し、VPN/RAS アカウント情報が搾取され、利用されていないか確認します。 （事象発生の日時が判明している場合は、該当時間帯を中心に確認します） ②VPN/RAS 経由での侵害が疑われるケースでは、VPN システムの管理者アカウントのパスワードも変更します。

	対象		APT	不正送金	ランサム	内部不正	項目	内容
24	ネットワーク	初動	△	△		△	パケットキャプチャ	①PROXYなどが無い環境で、通信状況を確認する必要がある場合は、インターネットとの接続ポイントで（一時的に）パケットの取得を行う事を検討します。 ②一定サイズでパケットファイルを分割して取得する設定としておきます。 ③パケットの取りこぼしについては許容します。 ④キャプチャデータから通信元機器の特定が可能かを確認します。
25	通信の制限（遮断）	初動	△				ホワイトリストの作成	①インターネットへの接続をホワイトリストで運用できるように、通信を許可するサイトを整理します。 ホワイトリストにて通信を許可するサイトの例： (1)Microsoft（Windows Update） 注意：過去にTechnetのフォーラムがC2通信に利用されたケースがあります。 (2)Adobe（Flash Player、Acrobat Reader） (3)各種ブラウザのアップデートサイト (4)Javaのアップデートサイト (5)ウイルス対策ソフトのアップデートサイト (6)MyJVNバージョンチェッカのアップデートサイト ※APTケースにおいては、水のみ場攻撃（業務で利用しているサイトの改ざん）、アプリケーションの更新を通じたマルウェアダウンロードなどが想定されます。通信を許可するサイトは事前に安全性を確認した上でホワイトリストへ登録します。
26		被害防止	△				ホワイトリストによる通信制限の実施 （または通信の遮断）	①組織内に侵入したマルウェア等により、インターネットを通じた情報漏えいが発生している可能性がある場合、一時的にインターネットとの通信を遮断するか、ホワイトリストを利用した通信の制限を検討します。
27			△				メールの制限	①電子メールを利用して、キーロガーの内容が外部に送信されるケースがあります。 ②電子メールサーバ（例：Exchangeサーバ）が侵害されている可能性がある場合は、電子メールの送受信ログを退避します。
28	マルウェア対応	初動	○	○	○		マルウェアは削除せず隔離	①マルウェアを発見した際は、削除せず安全な状態でファイルの確保を行います。（メタ情報が維持される方法を推奨） ②マルウェアを削除した場合、パターンファイルの作成や、マルウェアの動作（通信先）確認が出来なくなります。 ③マルウェアのファイル名変更、隔離を行った場合、タイムスタンプが変化する可能性があります。可能であれば、検知のみとして隔離などの操作も行わないようにします。
29		初動	○	○	○		ウイルス対策ソフトによるスキャン	①マルウェア感染がPROXYログなどから明確な場合は、ウイルス対策ソフトによるスキャンを行う前に、メモリ・ディスクイメージの取得を行ってください。 ②マルウェアと考えられるファイルを発見した場合、専用の環境にて複数のウイルス対策ソフトを利用してスキャンを行い、マルウェアとして検出されるか確認します。（被害環境でのスキャンは推奨されません） ③ウイルス対策ソフトのスキャンでは判別が行えない場合は、ファイルのMD5またはSHA1ハッシュ値を計算し、VirusTotalでハッシュ値の検索を行い検知が無いかを確認します。
30		初動	○	○	○		パターンファイル作成の依頼	①マルウェアと考えられるファイルを発見した後、自組織で利用しているウイルス対策ソフトで検知出来ない場合は、ウイルス対策ソフトベンダに検体として提供し、パターンファイルの作成を依頼します。
31		影響範囲	○	○	△		通信先の確認	①マルウェアの通信先（C2）サーバを確認します。 ②通信先のIPアドレス、ドメイン名などが判明した場合には、該当通信先との通信をPROXYやFireWallで遮断します。 ③判明したC2サーバのアドレス情報を元に、PROXYログなどを調査し、他に同じアドレスと通信を行っている機器が無いかかを確認します。（通信している機器を発見した場合には、初動対応を取ります）
32		影響範囲	○	○	○		タイムスタンプの確認	①マルウェアと考えられるファイルを発見した場合には、ファイルの作成日時を確認します。 ②ファイルの作成日時は改ざんされている可能性がある為、専用ツールにて $FILE_NAME のタイムスタンプも確認します。 ③マルウェアと考えられるファイルの作成日時の近辺で、他に作成・更新されたファイルが無いかを確認します。
33		影響範囲	○	△	△		ハッシュ値によるスキャン	①マルウェアを特定できている場合、マルウェアファイルのハッシュ値を計算し、他の機器に同一ハッシュ値を持つファイルが無いか確認します。

	対象		APT	不正送金	ランサム	内部不正	項目	内容
34	Active Directory（ドメインコントローラ）	初動	○			○	現在のログを確保	①Windows イベントログ（システム・セキュリティ・アプリケーション・タスクスケジューラ）が、ローテーションにより削除されないよう、ログを退避します。
35			○	○		○	ログイン履歴の確認	①アカウントの不正な利用がないか、セキュリティログを確認します。
36			○				アカウントパスワード変更	①ドメイン管理者アカウント不正に利用されている場合は、パスワードを変更します。 ②一般ユーザーについては、マルウェア感染した端末を利用していたアカウントについてはパスワードの変更を行います。 ③ドメイン全体のアカウント・パスワード情報が漏洩している可能性がある場合は、全てのアカウントについてパスワード変更を行います。 ④パスワード変更は、必ず汚染されていない環境で行います。 （キーロガーが設置されている場合、変更したパスワードが漏洩する危険性があります） ⑤アカウントのパスワード変更後、ログオン失敗を監視し、不正なログイン試行が発生していないかを確認します。
37			○	○	○		自動起動プログラムの確認	①Autorunsツールを使い、自動起動に不審なプログラム（マルウェア）が登録されていないか確認します。 ②マルウェアの種類によっては、Autorunsツールでは検出できない場合があります。
38			○				タスクスケジューラのログ確認	①タスクスケジューラを通じてバックドアプログラムの登録が行われていないかを確認してください。 （タスクスケジューラのログは事前に取得するように設定が必要です） ②タスクスケジューラのログから、不審なジョブの登録・実行が確認できた場合は、アカウントの確認、該当機器の隔離など初動対応を行います。
39		影響範囲	○				管理者用PCの安全性確認	①ドメインの管理者権限を持つユーザーが利用している機器が、マルウェアに感染していないか安全性を確認します。 ②ドメインの管理を行う専用の機器を準備し、専用の機器からドメインの管理を行います。
40			○				ログオン・ログオフ スクリプト	①ログオン、ログオフスクリプトに、攻撃者がマルウェア配布を行う設定などを行っていないか、スクリプトファイルの改ざんが無いかを確認します。
41			○			○	KRBTGT アカウントのリセット	①KRBTGT アカウントのパスワードを2回リセットし、攻撃者によるKerberos Golden Ticketの利用を防ぎます。 http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_07_PassTheGolden_Ticket_v1_1.pdf http://blogs.technet.com/b/jpsecurity/archive/2015/07/30/kerberos-krbtgt-account-password-reset-scripts.aspx
42		被害防止	○	○	○	○	グループポリシーの変更	①監査設定において、プロセス追跡の監査を行うようにドメインのポリシーを設定することで、クライアントPC上でのプログラム実行の履歴を記録する事で、セキュリティログでマルウェア実行を追跡できるようにします。 ※セキュリティログのサイズをデフォルト値より大きくする事が推奨されます。
43			○	○	△	○	揮発性情報の取得	①ネットワークから隔離する前に、netstat -naob、ipconfig /displaydns などOS標準コマンドを実行し、通信先の確認、通信元プロセスを確認してからネットワークから隔離します。 ②メモリイメージを取得します。 ③内部不正のケースにおいては、手続きに従った証拠保全を実施します。
44			○	○	△	○	イメージの取得	①マルウェア感染、侵害が疑われる機器をネットワークから隔離します。 ②メモリ、ディスクイメージを取得します。 ③内部不正のケースにおいては、手続きに従った証拠保全を実施します。
45			○	△	△	○	現在のログを確保	①Windows イベントログ（システム・セキュリティ・アプリケーション・タスクスケジューラ）が、ローテーションにより削除されないよう、ログを退避します。 ※感染が疑われる端末の場合
46			○	○	○		自動起動プログラムの確認	①Autorunsツールを使い、自動起動に不審なプログラム（マルウェア）が登録されていないか確認します。 ②マルウェアの種類（（例：Autorunsが確認しない登録項目の利用や、Rootkit、MBR/VBRの利用など）によっては、実機上でAutoruns ツールを利用してもマルウェアを検出できない場合があります。 イメージファイルを利用しオフラインでAutorunsによるチェックを行う、Rootkit検出専用ツール（例：GMER）を使うなど、マルウェアの影響を受けない状況で確認を行います。

	対象		APT	不正送金	ランサム	内部不正	項目	内容
47	クライアント機器	初動	○				資格情報マネージャに保存していたパスワードの変更	①「資格情報マネージャ」にてアカウント・パスワード情報を感染機器に保存していた場合は、それらのアカウント情報の漏洩・悪用を防ぐ為、安全が確認できている環境にてパスワードを変更します。 ②Windowsに保存されている資格情報を確認するには、下記2つの方法で結果を確認します。（両方を実施し確認） ・コントロールパネル⇒資格情報マネージャ、を起動して確認 ・vaultcmd /listcreds:"Windows 資格情報コンテナー"
48			○	○	○	△	ブラウザ等に保存していたパスワードの変更	①マルウェアへの感染が確認された場合、Webブラウザや電子メールアプリケーション、SNS、クラウド・サービス、Webサーバの管理画面等のアカウント・パスワード情報を感染機器に保存していた場合は、それらのアカウント情報の漏洩・悪用を防ぐ為、安全が確認できている環境にてパスワードを変更します。（共通のアカウント名・パスワード文字列を利用しているサービス等がある場合、二次被害を防ぐ為、パスワード変更を検討してください） ②パスワード情報が漏洩している場合、新たなパスワードを設定しても、古いパスワードを利用する事でパスワードを再設定出来る仕組みを持つサービスも存在する為、2要素認証などを有効にし古いパスワードを悪用出来ないようにします。 ③パスワード設定に関連した、秘密の質問などが漏洩している可能性がある場合、パスワードの再設定に必要となる情報などについても変更します。 ④保存していたアカウント情報が悪用されてないかを確認します。Webサーバ等の管理パスワードが漏洩した可能性がある場合、コンテンツが改ざんされていないかを確認します。
49				○			オンラインバンキング等のパスワードの変更	①マルウェアへ感染した機器において、オンラインバンキング等（カード会社や証券会社を含む）を利用している場合、関連するアカウント情報の漏洩・悪用を防ぐ為、安全が確認できている環境にてパスワードを変更します。 ②オンラインバンキング等で利用する証明書が盗まれた可能性がある場合、証明書の悪用を防ぐためオンラインバンキングの会社と連携して対応を取ります。 ③オンラインバンキング等のアカウント情報が悪用されてないかを確認します。
50					○		ランサムウェア：タイプの確認	①ランサムウェアの被害が発生している場合、暗号化されたファイルの拡張子、脅迫文の内容から感染したランサムウェアの種類が判明する場合があります。ウイルス対策ソフトなどによっては脅迫文などを削除するケースがあるため、必要に応じてそれらのファイルを退避しておきます。
51					○		ランサムウェア：感染端末の確認	①ランサムウェアに感染した機器を特定する方法の一つとして、ランサムウェアにより作成される脅迫文がクライアント機器内に作成されていないかを確認する方法があります。 ②ファイル共有上のファイルが暗号化されている場合は、該当ファイルの所有者情報などを確認し、感染元となっているアカウント・機器を特定します。 ③ランサムウェアに感染した機器を特定できた場合は、被害拡大を防止するため該当機器をネットワークから隔離します。 ④感染機器の特定に時間を要する場合で、ファイルサーバ等の被害を防ぎたい場合は、共有を一時的に読み取り専用などにアクセス権を変更します。
52		影響範囲	○				タスクスケジューラのログ確認	①タスクスケジューラを通じてバックドアプログラムの登録が行われていないかを確認してください。 （タスクスケジューラのログは事前に取得するように設定が必要です） ②タスクスケジューラのログから、不審なジョブの登録・実行が確認できた場合は、アカウントの確認、該当機器の隔離など初動対応を行います。
53			○	△		○	イベントログ内容の精査	①セキュリティログを確認し、ドメイン管理者権限を持つユーザーからのログオン履歴がないかを確認します。 ②接続元のコンピュータ、IPアドレスを確認し、接続元コンピュータ側でマルウェア感染が無いかチェックを行います。
54			○				USB機器の汚染（データ移動）	①分離・隔離されたネットワーク間におけるデータのやり取りに、USB機器などを利用している場合は、利用しているUSB機器がマルウェアに汚染されていないかを確認します。 ②分離・隔離されたネットワーク側の機器でマルウェア感染による問題が発生していない事を確認します。
55			○			○	Administratorアカウントの利用確認	① ローカル Administrator アカウントを通常の管理で利用していない場合、ローカル Administrator アカウントによるログオンがないかセキュリティログを確認します。
56		被害防止	○				Administratorアカウントのパスワード	①ローカル Administrator のパスワードを共通で利用している場合、悪用される危険性があります。 ②ローカル Administrator のパスワードを共通でなくすと共に、パスワードは長く複雑なものを設定します。
57			○				管理共有の無効化	①攻撃者が端末間での横展開を行っている状況が確認された場合は、Windows FireWall などで端末間の通信を制限する、管理共有の無効化を検討・実施します。

	対象		APT	不正送金	ランサム	内部不正	項目	内容
58	その他	初動	○				Webサーバの完全性確認	①Webサーバなどを管理している機器やアカウントが侵害された場合は、管理対象となっているWebサーバ等の管理パスワードを変更します。 ②Webコンテンツに改ざんが発生していないかを確認します。
59		影響範囲	○	○		○	資産管理ツールのログ確保	①資産管理ツールを導入している場合、資産管理ツールの取得ログから攻撃の追跡が可能になる場合があります。 ②古いログが、ローテーションにより削除されないようログを退避します。
60			○	△			攻撃痕跡の確認	①不正なプログラムの実行に伴う痕跡、タスクスケジューラによりマルウェアの実行などが行われた痕跡がないか、悪性ファイルの文字列パターンが無いか確認します。 ②マルウェアに感染した端末が特定できた場合、攻撃痕跡の特徴を確認し、同一のフォルダ名（攻撃者の作業フォルダ）が無いかを他の機器についても確認します。 例）ログオンスクリプトでフォルダやファイルの有無を確認するコマンドを実行するなど
61		被害防止	○	○	○		Windows Updateの実施	①Windows機器についてはWindows Updateを実施し、OSを最新の状態にします。（IEを含む）
62			○	○	○		Flash Playerの更新	①必要が無い場合は、アンインストールします。 ②必要な場合は最新版へアップデートを行います。 ※通信先を制限している場合、アップデートに必要となる通信をホワイトリストへ追加し許可する必要があります。
63			○	○	○		Javaの更新	
64			○	○	○		Microsoft Silverlightの更新	
65			○	○	○		利用ブラウザのアップデート	
66	営業秘密等	初動				○	情報の管理、社内記録	①営業秘密の要件該当性（特に秘密管理性）の証明に有効な資料の収集 「秘密情報の保護ハンドブック　～企業価値向上に向けて～（案）」P93 http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595215025&Mode=0
67						○	私物機器の持ち込み利用	①私物のパソコン、スマートフォン、USBメモリや記録媒体の無許可での接続、カメラなど撮影機能を持つ機器を許可なく持ち込みしていないか確認します。 ②USBメモリなどの記録媒体の接続記録を確認します。
68						○	営業秘密を含む機密情報へのアクセス履歴	①営業秘密など機密情報を取り扱う機器におけるファイルへのアクセス・コピーの履歴を確認します。 ②サーバ側でアクセスログを取得している場合は、サーバ側のアクセス履歴を確認します。
69						○	監視カメラ、入退出記録	①営業秘密など機密情報を取り扱う機器、区画における監視カメラ、入退出記録を確認します。
70		被害防止	○				営業秘密等を扱うシステムの隔離	①営業秘密、個人情報など機密情報を取り扱う機器、区画（ネットワークセグメント）において、インターネットとの接続を遮断または内部ネットワークからの隔離が必要と判断される場合は、対象データを取り扱うシステムへのアクセス制限や隔離を行います。

	対象		APT	不正送金	ランサム	内部不正	項目	内容
71	対外（報告）	初動	○			○	事故報告(主務大臣への報告）	①個人情報・マイナンバーの漏洩 「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」への対応 http://www.meti.go.jp/policy/it_policy/privacy/kojin_gadelane.html 「特定個人情報の漏えい事案等が発生した場合の対応について」 http://www.ppc.go.jp/legal/policy/rouei/ ②企業・組織がプライバシーマークを取得している場合 「個人情報の取り扱いに関する事故の報告について」 http://privacymark.jp/privacy_mark/about/accident.html
72			○			○	事故報告(契約企業・組織）	①守秘義務契約などおいて、事故発生時には報告を行うように取り決めがある場合、契約企業・組織に対して事故報告を行います。
73						○	IR情報の開示（適時開示）	①上場会社における「重要な会社情報の開示」が必要となる場合は、開示対応について検討します。
74			○	○	△	○	警察への相談、被害届け	①事案の状況に応じて、最寄のサイバー犯罪相談窓口に連絡を取ります。 「都道府県警察本部のサイバー犯罪相談窓口等一覧」 https://www.npa.go.jp/cyber/soudan.htm
75	情報共有	被害防止	○	○	○		JPCERT/CC、IPA 等への情報共有	①経済産業省の告示に基づく IPA への届出 https://www.ipa.go.jp/security/todoke/ ②JPCERT/CC へ情報提供を行い、C2サーバの停止などの調整を依頼 ③サイバーセキュリティ経営ガイドライン P25の項目(8)を参照 http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf