お取引先様向け
情報セキュリティ対応ガイドライン

Ver.　2.2

2022年4月1日

パナソニック オペレーショナルエクセレンス株式会社

グローバル調達本部

パナソニック ホールディングス株式会社

情報戦略部

＜目　次＞

Ⅰ．　パナソニックグループの情報セキュリティ基本方針

パナソニックホールディングス株式会社および関係会社（以下、「当社」という。）は、経営基本方針にのっとり、優れた技術、製品およびサービスによって、お客様の満足と信頼を得ることを目指しています。このためには、お客様の情報、個人情報、財産的情報を始めとする情報の保護が重要であることを認識し、情報セキュリティを経営の重要戦略の一つと位置付け、以下のようにこれに取組み、以って健全なる情報化社会の実現へ向けて尽力します。

１．情報セキュリティ体制

各組織に情報セキュリティの責任体制を敷き、所要の規程の策定と実施により適切な管理に取組みます。

２．情報資産の管理

情報は、そのセキュリティ確保のため、重要性とリスクに応じ取り扱いを明確にし、適切に管理します。

３．教育・訓練

全役員および従業員に対して情報セキュリティについての教育・訓練を継続的に実施し、その意識向上と情報セキュリティに関連する諸規程の徹底を図ります。違反者に対しては、懲戒も含め、厳正に対処します。

４．安心できる製品・サービスの提供

利用されるお客様の情報のセキュリティに配慮し、安心してお使いいただける製品・サービスの提供に努めます。

５．法令順守と継続改善

関連する法令、その他の規範を順守するとともに、環境の変化に合わせ情報セキュリティ確保への継続的な改善・向上に努めます。

Ⅱ.　機密保持契約の締結

当社とお取引先様の間で機密情報を共有する際は、下記の機密保持項目を含んだ取引基本契約または個別契約の締結をお願いいたします。

a) 守秘義務
b) 機密保持の対象となる情報の範囲
c) 守秘義務期限(無期限も含む)
d) 使用目的の制限
e) アクセス者は業務上知る必要のある人に限定
f) 機密情報の管理方法
g) 機密情報の複製・複写の制限
h) 守秘期間満了後の返却または廃棄の規定
i) 当社からの機密保持に関しての確認（ヒアリングや監査等）の措置の規定
j) 契約違反時の措置（損害賠償に加えて市場で差止めができる条項を入れておく等）
k) 無断での再委託の禁止
l) 私用 PC の業務使用の禁止

Ⅲ.　お取引先様情報セキュリティ対応ガイドライン

１.　目的

この基準は、当社が健全なる情報化社会の実現を目指すグローバル企業として、適正な情報セキュリティを推進し、お客様の情報、個人情報、技術・品質・製品・サービス等の情報資産を正しく取り扱い・管理することにより、企業の社会的責任を果たしてゆくために、当社の機密情報を共有するお取引先様に対して、適切な情報セキュリティ対策の実施・要請事項を示したものです。

情報を正しく管理・利用できる環境を構築することで、当社およびお取引先様の安心・安全で効率的な業務遂行を可能とし、安定した事業継続と相互繁栄を実現します。

２.　適用

この基準は、当社が指定した機密情報を共有するお取引先様での該当情報の取り扱い、管理および業務（技術移転・業務委託・資材調達活動等）全般に適用します。

適用の対象となる情報の範囲は、当社と共有している機密情報、およびこれを利用して創出された機密情報（以下、「機密情報」という。）です。

適用の対象となる機密情報の形態は、機密情報が記載された紙（以下、「紙」という。）、電子化情報、機密情報が化体されたもの（以下、「化体物」という。）、ノウハウ等、一切を含みます。

さらに厳重な管理を必要とする厳秘情報や重要情報等に関しては、覚書・機密保持契約等による追加の管理策が適用されます。

３.　お取引先様への情報セキュリティに関する要請事項

お取引先様に要請する事項は、下記の（１）から（５）となります。

なお、本基準の要請事項に関して、お取引先様における情報管理が、当社が定めたレベルに到達しない場合、該当のお取引先様との機密情報の共有を制限させていただくことがあります。下記要請事項の実施をお願いいたします。

（１）情報セキュリティの管理体制の確立

情報セキュリティを組織的に進められる体制を構築する。

（1-1）　情報セキュリティ管理の組織体制の構築

（1-2）　情報セキュリティの取り組みに関する基本的な考え方やルールを制定

（２）情報資産の機密管理

機密管理が必要な情報を特定し、機密管理に必要な管理を実施する。

（2-1）　機密情報の明確化

（2-2）　機密情報の交換・返却の管理

（2-3）　物理的管理

（2-4）　情報システムの利用者 ID とパスワードの管理

（2-5）　PC・サーバ等情報システムの設置・運用および廃棄の管理

（2-6）　不正プログラムの対策

(2-7)　バックアップの実施

(2-8)　貴社と機密情報を共有する委託先の管理

（３）人的な対策

機密保持の誓約等、情報漏洩を防止する人的な対策を実施する。

(3-1)　情報セキュリティの啓発、教育および訓練の実施

(3-2)　従業員等からの誓約書の取得

（４）情報セキュリティ事件・事故対応

情報セキュリティ関連の事件・事故が発生した場合の対応を明確化し、実施する。

(4-1)　事故報告・対応体制の確立

(4-2)　事故対応手順の明確化

（５）情報セキュリティマネジメントの実施

継続的な改善活動に向けて、情報セキュリティマネジメントを実施する。

(5-1)　組織的な情報セキュリティ活動が実施されていることの定期的な確認

(5-2)　確認結果に基づく改善活動の実施

４．　詳細要請事項

「３．お取引先様への情報セキュリティに関する要請事項」に記載されている各事項についての詳細を、以下に提示させていただきます。以下、お取引先様を「貴社」と記載させていただきます。

（１）　情報セキュリティの管理体制の確立

1-1	情報セキュリティ管理の組織体制を構築し、その責任と役割を明確にして、文書化してください。
1-2	情報セキュリティの取り組みに関する基本的な考え方（ポリシー）とルールを制定し、文書化してください。

（２）　情報資産の機密管理

(2-1)　機密情報の明確化

2-1-1	機密情報の情報資産リストを作成して資産を特定し、リストを定期的に更新してください。
2-1-2	契約に基づいて機密情報を複製・複写した場合、複製・複写した機密情報も原本と同様の管理をしてください。
2-1-3	機密情報はそれ以外の情報と明確に区分をして管理してください。

(2-2)　機密情報の交換・返却の管理

2-2-1	当社との間で合意したルールに基づいて機密情報の交換を行ってください。
2-2-2	機密情報の持ち出しルールを制定し、下記 a)-d)の該当する項目を全て実施してくだ

	さい。 a) 機密情報を持ち出す場合には、管理責任者の許可を得てください。 b) 持ち出し中は、機密情報を常時携行し、手元から離さないようにしてください。 c) 電子化情報を PC、携帯情報端末、記憶媒体に保管して持ち出す時や、電子メールに添付して送信する場合には、暗号化を実施してください。 d) 化体物（金型・試作品等）を持ち出す場合には、部外者の目に触れないようにしてください。
2-2-3	受託業務の終了後、機密情報を当社と合意した手順で返却してください。貴社で機密情報を廃棄する場合は、当社と合意した内容に基づき、下記 a)-d)の該当する項目を全て実施してください。当社からの要請に応じて、廃棄記録を提出してください。 a) 電子化情報の場合、サーバ、PC、携帯情報端末、記憶媒体に保管されている機密情報を完全に消去してください。 b) 紙（書類・図面等）の場合、シュレッダーによる裁断、溶解または焼却してください。 c) 化体物（金型・試作品等）の場合、破壊して元の情報がわからないようにしてください。 d) 廃棄を産業廃棄物業者等の外部業者に委託する場合、業者とは機密保持契約を締結してください。

(2-3)　物理的管理

2-3-1	機密情報を取り扱う場所（敷地・建物・部屋）へは、関係者以外の立ち入りを制限する物理的な対策を設けてください。
2-3-2	機密情報を取り扱う場所へは、業務上情報を知る必要がある人のみに、管理責任者が立ち入りを許可してください。
2-3-3	社内で従業員と外部からの訪問者を区別できるしくみを設けてください。
2-3-4	機密情報を取り扱う場所への入室・退室の両方または片方の記録（監視カメラ映像を含む）を取得し、記録が正しく取得できていることを定期的に確認してください。
2-3-5	機密情報を取り扱う場所への、私用の PC、携帯電話、携帯情報端末、記憶媒体（SD カード、USB メモリ等）、通信デバイス（無線 LAN 等）などの持ち込みを禁止してください。持ち込みが必要な場合は、下記 a)および b)を実施してください。 a) 持ち込みが必要な場合は、管理責任者の事前許可を得てください。 b) 持ち込みを許可する場合でも、会社の PC や社内ネットワークに接続させないことや、携帯電話・携帯情報端末のカメラ機能を使わせないなどのルールを制定し、管理をしてください。
2-3-6	紙（書類・図面等）・化体物（金型・試作品等）に関して、業務上情報を知る必要がある人のみが取り扱えるようし、盗難防止対策を施してください。

(2-4～2-7 は、当社との電子化情報を保有する場合のみ対象)

(2-4)　情報システムの利用者 ID とパスワードの管理

2-4-1	情報システムの利用者 ID の管理ルールを制定し、下記 a)-d)の全項目を実施してください。 a) 情報システムの利用者に他の利用者と ID の共有をさせないようにしてください。 b) 情報システムの利用者 ID の発行手順と承認手順を定めてください。 c) 退職者や異動者など関連業務に携わらなくなった者の ID および一時利用者用の ID 等、不要な ID は直ちに削除してください。 d) 管理されていない ID が存在しないことを定期的に確認してください

2-4-2	パスワードの管理ルールを制定し、下記 a)-c)の全項目を実施してください。 a) 他人に容易に推測されないパスワードを設定してください。 b) パスワードは定期的に変更してください。 c) パスワードは他人に知られないように管理してください。
2-4-3	機密情報を保管するサーバへのアクセス制限を実施し、業務上情報を知る必要がある人のみがアクセスできるしくみを設けてください。
2-4-4	機密情報へのアクセス者の記録（ログ）を取得し、当社と合意した期間、適切に保管してください。

(2-5) PC・サーバ等情報システムの設置・運用および廃棄の管理

2-5-1	社内ネットワークは、ルータやファイアーウォールなどにより、社外ネットワーク（インターネット）と分離してください。
2-5-2	PC、携帯情報端末、サーバ等を導入・設置する際の手続きを定め、実施してください。
2-5-3	機密情報は、サーバに保管してください。サーバは適切なセキュリティ管理を実施してください。
2-5-4	私用 PC、私用携帯情報端末、私用記憶媒体は業務で使用させないようにしてください。
2-5-5	PC、携帯情報端末、サーバ、記憶媒体の下記項目を含んだ廃棄・再利用ルールを制定し、実施してください。 ・データが復元できないようにするため、ディスク内の情報を完全に消去または物理的に破壊してください。
2-5-6	機密情報を保管するサーバは、セキュリティを確保できる適切な場所に設置し、下記 a)および b)を実施してください。 a) サーバの設置場所への出入りは業務上必要がある人のみに制限してください。 b) サーバに盗難防止対策を施してください。

(2-6) 不正プログラムの対策

2-6-1	コンピュータウィルス・不正プログラムへの対策ルールを制定し、下記 a)-d)の全項目を実施してください。 a) 情報システムの管理責任者が指定したウイルス対策ソフト（種類・バージョン等）を導入してください。 b) ウイルス対策ソフトを PC に常駐して動作し、ウイルスに対して防御可能な状態にしてください。 c) パターンファイル更新を定期的に実施してください。 d) 保管されているすべてのファイルに対して、ウイルス検索を定期的に実施してください。
2-6-2	ウイルスによる被害を最小限にするための対策手順（ウイルス感染時の物理的対処や報告・通知・対応方法等）を定め、実施してください。
2-6-3	ファイル交換ソフト（Winny・Share 等の情報漏洩のリスクが高いソフト）のインストール・使用を禁止し、定期的な確認を行ってください。
2-6-4	フリーのメール（Yahoo!メール等）やデータ共有サービス（Google docs 等）による機密情報の送信・共有を禁止してください。

(2-7) バックアップの実施

2-7-1	バックアップの必要性・頻度を当社と検討し、バックアップが必要な場合は、電子化

	された機密情報のバックアップのルールを制定し、実施してください。
2-7-2	バックアップデータの保管ルールを制定し、機密区分に応じて適切に管理してください。

(2-8 は、貴社と機密情報を共有する委託先がある場合のみ対象)

(2-8)　貴社と機密情報を共有する委託先の管理

2-8-1	貴社が委託先と機密情報を共有する場合、その旨を当社に事前に文書で伝えてください。
2-8-2	貴社と機密情報を共有する委託先とは、下記 a)-l)の条項を含む機密保持契約（または機密保持の項目を含む契約）を取り交わし、機密情報の取り扱いや交換に関するルールを制定し、管理をしてください。 a)　守秘義務 b)　機密保持の対象となる情報の範囲 c)　守秘義務期限（無期限も含む） d)　使用目的の制限 e)　アクセス者は業務上情報を知る必要のある人に限定 f)　機密情報の管理方法 g)　機密情報の複製・複写の制限 h)　守秘期間満了後の返却または廃棄の規定 i)　機密保持に関しての確認（ヒアリングや監査等）の措置の規定 j)　契約違反時の措置（損害賠償に加えて市場で差止めができる条項を入れておく等） k)　無断での再委託の禁止 l)　私用 PC の業務使用禁止
2-8-3	貴社と機密情報を共有する委託先に電子化された機密情報を送付する場合、該当ファイルを暗号化してください。
2-8-4	貴社と機密情報を共有する委託先との間の機密情報の受け渡しを記録し、管理してください。
2-8-5	貴社と機密情報を共有する委託先に対して、貴社従業員と同等の機密保持の誓約書を社員から取得することを要請してください。
2-8-6	貴社と機密情報を共有する委託先に対して、貴社と同等レベルの情報セキュリティ管理を要請し、実態確認を定期的に実施してください。
2-8-7	貴社と機密情報を共有する委託先に対して、委託先社員への情報セキュリティ教育の実施を要請してください。

（３）　人的な対策

(3-1)　情報セキュリティの啓発、教育および訓練

3-1-1	全従業員に対して定期的に情報セキュリティ教育を実施してください。
3-1-2	管理責任者に定期的に情報セキュリティ教育を実施してください。
3-1-3	全従業員に対して、自己点検チェックの実施等により、情報セキュリティに関するルールの順守実態を定期的に確認してください。管理責任者は、不適合事項がある場合は、改善を指示してください。
3-1-4	全従業員に対して標的型攻撃の教育または訓練を実施してください。

(3-2)　従業員等からの誓約書の取得

3-2-1	就業規則等に機密保持の項目を設け、従業員から機密保持の誓約書を取得してください。
3-2-2	派遣社員を受け入れる場合、派遣社員から機密保持の誓約書を取得してください。

（４）　情報セキュリティ事件・事故対応

(4-1)　事故報告・対応体制の確立

4-1	事故発生時の連絡・対応の責任者を選任し、下記 a)～c)の項目を含む事故報告体制を構築してください。 a)　情報セキュリティ上の問題を発見したり、発生の恐れがある場合、または事件・事故を目撃したり、その痕跡を発見した場合には、管理責任者に速やかに報告してください。 b)　当社の情報について、上記の問題が発生した場合には、当社と合意した時間内に当社に報告してください。 c)　標的型攻撃によって当社の情報に関連する機器がウイルス感染した場合には、当社と合意した時間内に当社に報告してください。

(4-2)　事故対応手順の明確化

4-2	下記 a)-f)の全項目を含む事故対応の手順を明確にし、組織内に徹底してください。 a)　被害の把握とその影響を最少にするための緊急対応 b)　原因究明と暫定措置 c)　情報の漏洩時には、当該第三者への報告等、関係者の自衛や対応を可能にする措置 d)　必要な場合、広報対応、関係官庁への報告 e)　事故の経緯、対応経過の記録 f)　再発防止対策の実施と周知徹底できるような体制構築

※　情報セキュリティ事故の例：情報（書類、PC、記憶媒体、化体物等）の盗難・紛失、情報の漏洩、電子メール・FAX 誤送信、情報への不正アクセス、不正入手、可用性の喪失（システムダウン、データ破壊等）、完全性の喪失（データの改竄、消去）など

（５）　情報セキュリティマネジメントの実施

(5-1) 組織的な情報セキュリティ活動が実施されていることの定期的な確認

5-1	組織的な情報セキュリティ活動が実施されていることを定期的に確認してください。

(5-2)　確認結果に基づく改善活動の実施

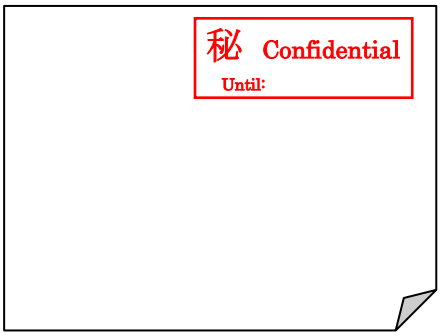
5-2	確認の結果、明確になった不適合事項に対して、改善計画を立て、改善を実施してください。

附則

１．　施行日　　2022 年 4 月 1 日

２．　本基準が適用される機密情報の当社からの指定方法

＜表示例＞



下記 1.－3.のいずれかの方法で指定します。

1.書類、図面、ファイル、電子データ等に
　「秘 Confidential」と記載された情報

2.　電子データのファイル名が「秘―ファイル名」
　または「C－ファイル名」となっている情報

3.　別途当社が機密情報と指定した情報

３．　チェックシート

「お取引先様向け情報セキュリティ基準チェックシート」を用いて定期的に自主チェックを実施し、当社からの要請に応じて、報告してください。