セキュリティ
ホワイトペーパー

悩む人の明日をひらく。

初版　2023年9月

STYLEEDGE

CONTENT

ホワイトペーパーの対象範囲

このセキュリティホワイトペーパーは、注釈がない限り、当社（株式会社スタイル・エッジ）に関する事項のみを取り扱っています。

スタイル・エッジのビジョン・ミッション

当社は、「悩む人の明日をひらく。」をミッションに掲げ、
弁護士や司法書士といった士業、医師や看護師といった医業の世界に携わる、
いわゆる「プロフェッショナル」の総合支援を事業として展開しています。

クライアントである弁護士や医師の先にいらっしゃる一般消費者の方々は、
士業であれば、借金問題、交通事故被害など、医業であれば美容に関するコンプレックスなど、
何かしらのお悩みを抱えています。

また、プロフェッショナルも同様に事務所経営、たとえば集客や採用などのお悩みを抱えています。

本来、専門家の方々がその専門知識を活かし、目の前のお客様のお悩みを解決することに集中することができれば、より社会的なパフォーマンスを発揮できます。

であれば、当社がプロフェッショナルの経営課題をサポートしお悩みを解決することで、プロフェッショナルのパフォーマンスが上がり、結果としてその先にいらっしゃる一般消費者の方々のお悩みを解決することにつながります。

当社は、人々が抱える様々な悩みを解決し、より良い社会の実現を目指します。

セキュリティに関する考え方

当社は士業・医業に携わるプロフェッショナルの総合支援事業に取り組んでいます。
士業・医業といった業界は機微な個人情報を取り扱うため、万が一、情報漏洩やサイバー攻撃が発生した場合の影響が非常に大きく、セキュリティ対策が特に重要です。

したがって、私たちは、その支援をするに相応しいセキュリティ対策を行う義務があります。つまり、日々変化するセキュリティ情勢を把握し、自らを知り、敵を知り、より最適なセキュリティ対策を実践し続けなければならないと考えています。

私たちは、その過程で得た知見をもとに、自社のセキュリティに留まらず、士業・医業分野におけるセキュリティ体制のベースを構築し、クライアントであるプロフェッショナルに還元します。それにより、士業・医業分野全体のセキュリティレベルが向上すれば、プロフェッショナルだけでなく、その先にいらっしゃる多くの一般消費者の方々を守ることにもつながると考えています。

また、当社は、プロフェッショナルとは単なるクライアントではなく、共に事業を作る「パートナー」という想いで支援しています。だからこそ、プロフェッショナルの事業を他人事ではなく自分事として捉え、主体的に提案や支援ができるのです。この想いは、セキュリティに関しても同様です。個々に抱えるセキュリティの問題にも、共に向き合うパートナーとして、寄り添って支援をしています。

本ホワイトペーパーでは、私たちが上記の考えのもと、どのようなセキュリティ対策に取り組んでいるかを説明します。

当社のセキュリティポリシーについては、下記よりご確認いただけます。
https://styleedge.co.jp/security-policy/

個人情報に関する考え方と扱い方

当社は、お客様の個人情報の重要性を深く認識し、個人情報の適切な保護、取り扱いを行っています。

当社のプライバシーポリシーについては、下記よりご確認いただけます。
https://styleedge.co.jp/privacy-policy/

セキュリティに関する認証

ー ISMS(JIS Q 27001)

ISMSとは、情報セキュリティマネジメントシステムに対する国際的な第三者適合性評価制度です。

当社は、ISMSのISO27001の認証に適合し、国際的にも信頼を得られる情報セキュリティレベルを満たしています。

ー 電子決済等代行業者

電子決済等代行業者とは、財務局により認められた、ITを活用した金融機関の口座情報へのアクセスが可能な事業者のことを指します。

当社は電子決済等代行業者の登録を受けています。

当社の電子決済等代行業についての取り決めは、下記よりご確認いただけます。
https://styleedge.co.jp/collaborative-policy/

外部組織との連携

常に変化するサイバーセキュリティ情勢に対応するため、当社は積極的に外部組織と連携し、最新の情報を把握できるように取り組んでいます。

株式会社 CISO

- 当社セキュリティ外部顧問
- 最新のセキュリティ情勢を共有
- インシデント発生時には協力し対応

日本シーサート協議会

- 協議会に所属
- CSIRT 同士の緊密な連携、情報共有を実施

SGS ジャパン株式会社

- 当社の ISMS 認証機関

LRM 株式会社

- 当社の ISMS 認証取得、運用支援のコンサルタント

株式会社ソフトクリエイト

- 当社のネットワーク構築、保守を支援
- インシデント発生時には協力し対応

社内体制

ー 情報セキュリティ管理者

当社の情報セキュリティマネジメントシステム責任者です。

ー ISMS 事務局

情報セキュリティ管理者を補佐し、情報セキュリティマネジメントシステムの作成および、運用、維持を行います。

ー 情報セキュリティリスク管理委員（以下、リスク管理委員）

当社の各部門に置かれ、情報セキュリティマネジメントシステムが各部署内で適切に実施されているかを確認・啓蒙します。

使用可能なツールの精査や、定期的なセキュリティチェックを実施しています。また、情報セキュリティに関するインシデントが発生した場合は、当事者からの報告を受け、ISMS 事務局に報告し、その再発防止策が有効であるかどうかのチェックを行います。

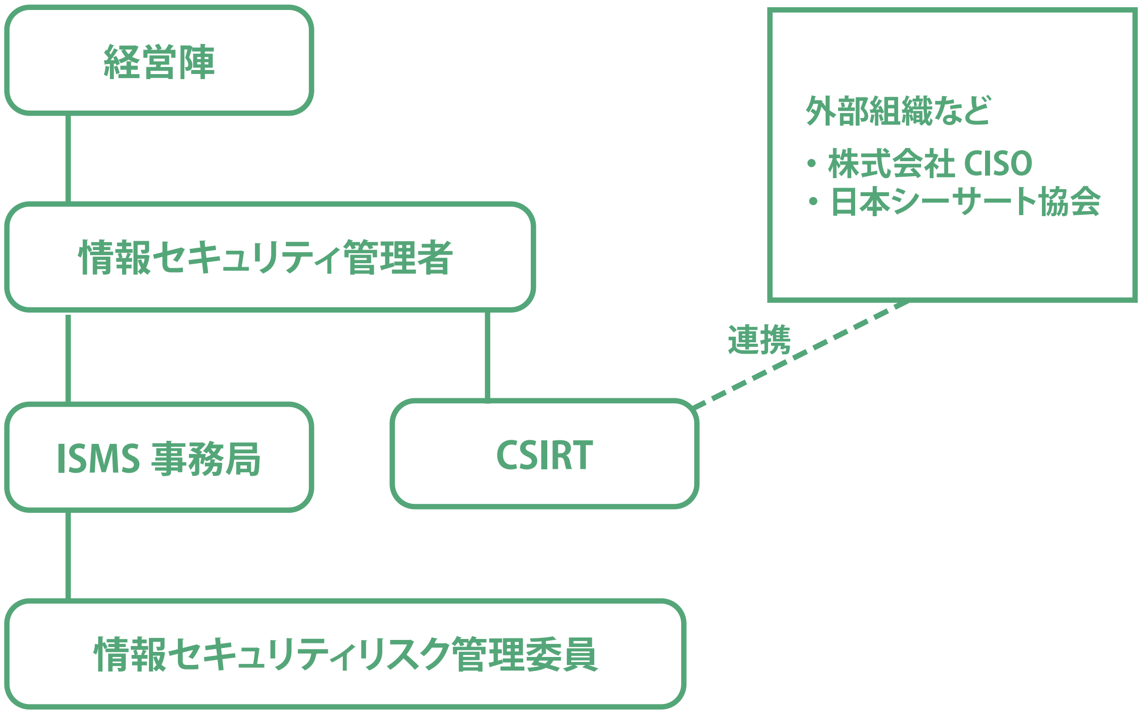
ー CSIRT

当社のサイバーセキュリティ対策チームです。社内外を問わず、セキュリティに関する問合せ対応や、不審な操作、ログの監視・調査を行います。

社外に対してはクライアントのセキュリティ向上のためのサポートを実施しています。

また、サイバーセキュリティに関するインシデントが発生した場合は、社内外に関わらず、率先して対応を行います。詳細は、「インシデント対応」の項目をご覧ください。

組織図



クライアントへのセキュリティサポート

当社は、情報セキュリティ、サイバーセキュリティ双方の観点で、士業・医業分野のクライアント向けにセキュリティ体制構築からその後の運用までを一気通貫で支援しています。
クライアントが抱えているセキュリティ上の問題点を見つけ出し、セキュリティ対策ソフトの見直しの提案や、より効率的で安全な IT 活用方法などを提案しています。

ー セキュリティ教育

セキュリティの必要性は認識しつつも、何から取り組めばよいかわからないというクライアント向けに、情報セキュリティ、サイバーセキュリティ双方の観点で、セキュリティの基礎をお伝えします。クライアントがセキュリティについて正しく理解し、納得感をもってセキュリティ対策に取り組めるよう支援します。

ー セキュリティ体制構築支援（セキュリティブースト）

セキュリティの基礎について正しく理解し、継続した取り組みを表明いただいたクライアント向けに情報セキュリティ、サイバーセキュリティ双方の観点からセキュリティ体制構築や運営を支援しています。
当社では ISMS を取得し、サイバーセキュリティ対策にも取り組んでいるため、それらの知見を活かし、体制構築や運営に関する各種問い合わせにも対応します。

ー EDR 導入 / 運営支援

従来の侵入防御のセキュリティ対策だけでは、すべてのサイバー攻撃を防ぐことが困難になっています。
EDR では、万が一端末へのマルウェアなどの侵入を許してしまった場合でも、
不審な動きを検知し、管理者への通知および端末のネットワークからの強制隔離を行うことができます。

当社では、EDR の導入から効率的に運用できるようになるまでを支援し、最終的には、クライアント自ら対応できるスキル獲得を目指します。

ー セキュリティ診断

セキュリティ体制がある程度整備されたクライアント向けに、弊社がセキュリティ診断を実施し、クライアントの現在のセキュリティ状況を可視化します。そのうえで、今後必要となるセキュリティ対策を実施するための支援を行っていきます。

ー インシデント対応

当社では、セキュリティインシデントが発生したクライアント向けに、インシデント対応の支援をしています。
クライアントの要望に沿って、インシデントの被害拡大防止、原因究明、再発防止策の提案などを行います。

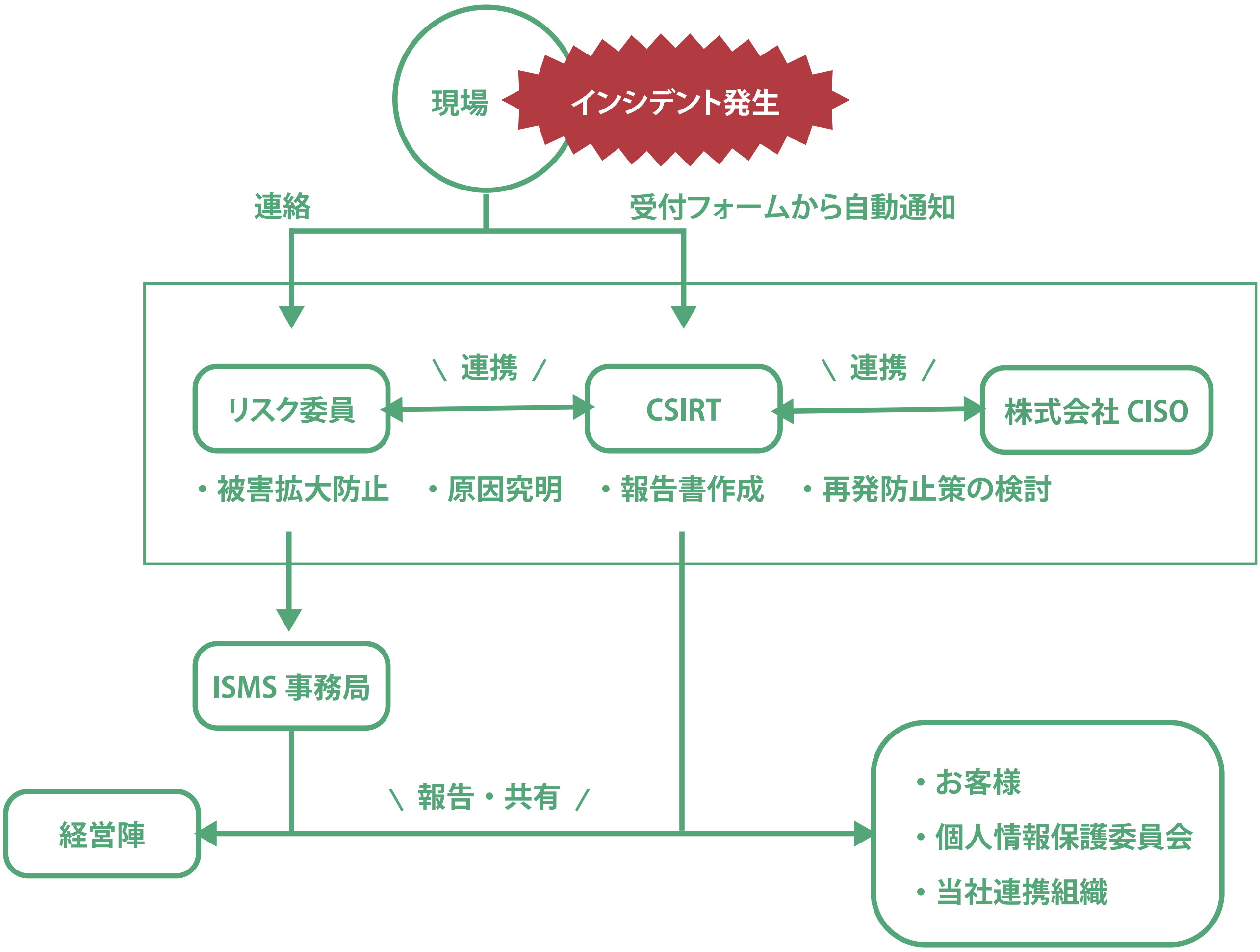
インシデント対応

当社では、インシデント発生時に、当社およびクライアントの大切な情報を守るために、事前に定めたインシデント発生時のフローに則って対応を行います。

インシデントには、端末の紛失などの情報セキュリティインシデントおよびマルウェア感染などのサイバーセキュリティインシデントを含みます。

インシデントが発生した場合は、当事者より各部門のリスク管理委員へ連絡、および受付フォームからCSIRT へ問合せを行います。リスク管理委員・ISMS 事務局と CSIRT が連携し、関係各所へ連絡・対処を行います。インシデントの深刻度、クライアント・当社のビジネスへの影響を鑑みて、外部組織と連携し、被害拡大防止、原因究明、インシデント報告書作成、再発防止策の検討を行います。

インシデント発生時のフロー



社員教育

ー e ラーニングによる情報セキュリティ教育

ISMS 事務局より、社内の情報セキュリティリテラシー向上のため、年 1 回以上定期的に e ラーニングを活用した学習を実施しています。

ー 月次セキュリティチェック

リスク管理委員より、社内の各部門に対し、当社が定めるセキュリティルールが守られているかを確認します。

ー CSIRT 通信

CSIRT より、サイバーセキュリティに関する最新情報を社内外に発信し、セキュリティに関する啓蒙を実施しています。

ー リスク管理通信

ISMS 事務局より、情報セキュリティに関する情報を社内に発信し、従業員のセキュリティに対する意識向上を促しています。

ー エンジニア向けセキュリティチャレンジ

当社のエンジニアを対象に、システム上の脆弱性を発見し、修正するための実践的な演習を実施しています。演習を通して、セキュリティ対策の重要性やシステムを開発するうえで注意すべき点を学ぶことができます。

ー エンジニアによる CYDER/ 各種セミナー参加

当社のエンジニアを対象に、技術力向上のため、積極的に外部のイベントやセミナーに参加しています。

入退室管理

ー 本社執務エリア

従業員は社員証を兼ねたセキュリティカードで執務エリアへ入室できます。オートロックドアを設置し、従業員以外の入室を制限しています。

ロックを解除すると、セキュリティカードに紐づいたログが管理システムに保存されます。また、入退室は監視カメラで記録しクラウド上に保存しています。

ー 本社サーバールーム

サーバールームには、オートロックドアを設置し、ネットワーク管理関連チームのみがセキュリティカードで入室できます。ロックを解除すると、セキュリティカードに紐づいたログが管理システムに保存されます。

また、ネットワーク機器が設置されているラックは常に施錠し、ネットワーク管理者のみが開閉できます。入退出は監視カメラで記録しクラウド上に保存しています。

ー 本社応接エリア

社外のお客様とのミーティングを実施するエリアが用意されています。入退出は監視カメラで記録しクラウド上に保存しています。

なお、当社（本社）が置かれているビルのセキュリティ対策により、オフィスエリアへ移動するには、セキュリティカードまたはゲスト用入館カードが必要になります。

※支社においても、執務エリア、サーバールームへの入室制限、監視を実施しています。

端末管理とエンドポイントセキュリティ

当社では、すべての端末で資産管理ソフト、EDR 製品を導入しエンドポイントでのセキュリティ対策を行っています。

- 許可していないサービスの利用や望ましくない操作を制限し、社内規定を遵守した端末利用を実現しています。また、端末の操作ログをクラウド上に保存し管理しています。
- 端末などの資産を利用者、保管場所と紐づけて管理することで資産の所在を明確にします。また、紛失・盗難が発生した場合はリモートロック・ワイプを実施できます。
- 万が一、攻撃者やマルウェアが端末内部へ侵入した場合でも、すぐに EDR が不審な挙動を検知し、管理者へ通知、場合によっては自動でネットワークから隔離することができます。また、当社では個人の USB ストレージの利用を原則禁止していますが、万が一接続された場合でも、セキュリティ対策ソフトにより USB ストレージ接続時に不審なファイルが保管されていないかを確認しています。
- EDR が検知した不審な挙動は CSIRT が監視し、インシデントと思われる事象が発生した場合は速やかに対応します。また、CSIRT では EDR の検知内容について定期的に議論する機会を設け、より適切なインシデント対応を行えるよう、日々知識と技術を磨いています。

アカウント・パスワード管理 / 認証

ー アカウントの認証

当社では、従業員使用端末のアカウントをクラウド上で管理し、アカウント管理担当メンバーのみがアクセスできるようになっています。アカウントの認証はクラウド上で行われ、端末にログインした際に、アカウント情報や位置情報のログを保存しているため、いつでも端末の使用状況を確認できます。

ー パスワード管理

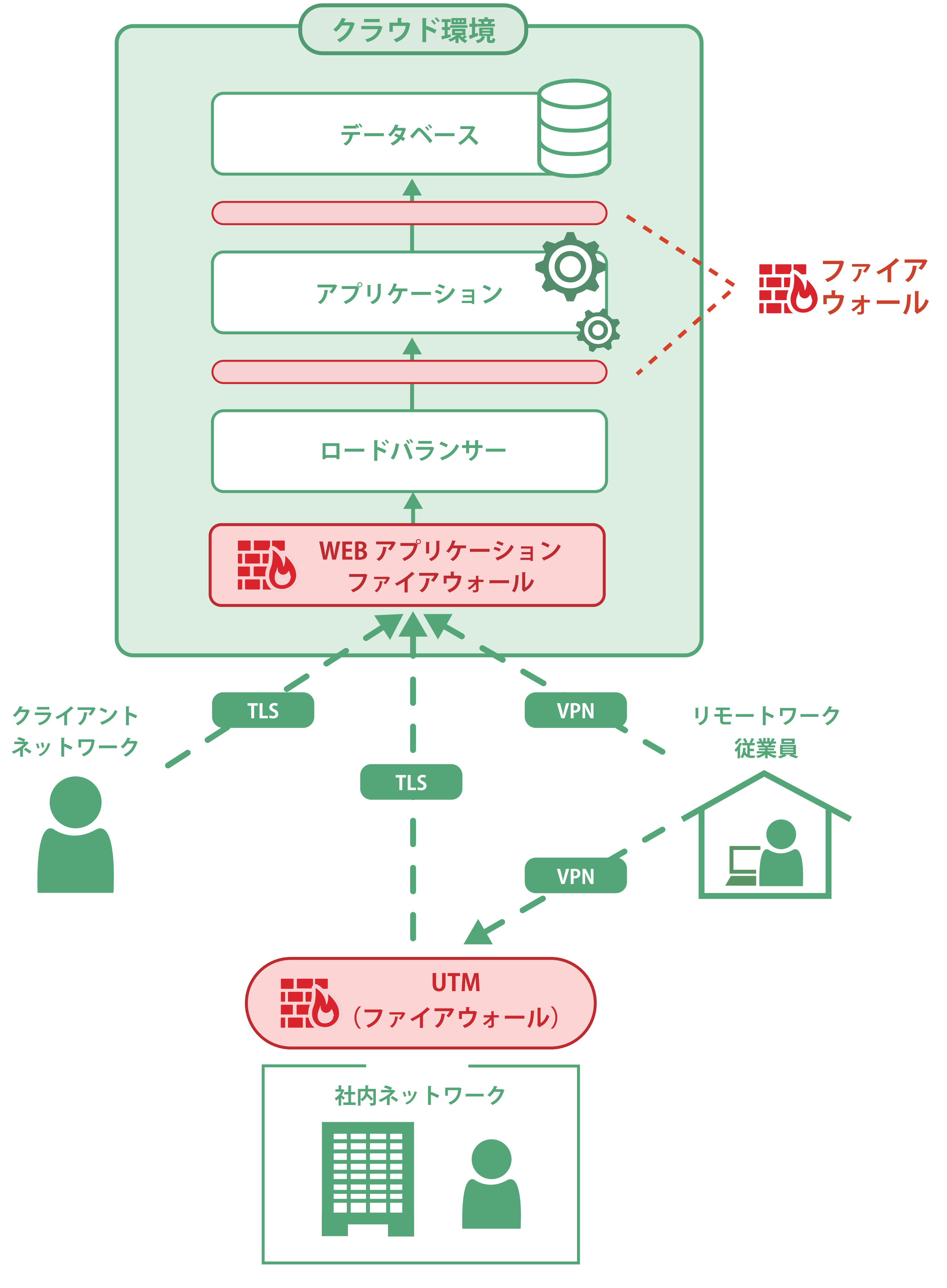
当社では業務で使用するシステムにアカウントを登録する場合、パスワードマネージャーを使用し、当社パスワードポリシーに則った高強度のパスワードを設定しています。また、登録したアカウントに関する ID やパスワードは、システム上で一括管理し、パスワードの流出が起きないよう対策しています。

ネットワーク管理

当社では、社内ネットワークおよび当社運営システムにおいて、侵入防御、多層防御や通信の暗号化を実現しています。

- 当社では本社においてUTMを導入し、第三者からの不正侵入防止、アンチウィルスや Web フィルタリングなどの複合的なセキュリティ対策を行っています。また、UTM を通過するすべての通信のログを取得し、クラウドシステム上に保管しています。
- 当社では、リモートワーク時の社内ネットワークへの通信や当社サービスへ接続する通信を暗号化し、第三者に通信内容を改ざん、傍受されても、情報漏洩を防止します。また、従業員の自宅 Wi-Fi の暗号化規格が当社の定める基準（WPA2 以上）を満たしているか毎月確認しています。
- 当社では、社内ネットワークを業務セグメントと管理セグメントに分離しています。管理セグメントには、重要なネットワーク機器が置かれ、ネットワーク管理者のみがアクセスできます。これにより、管理者のみがネットワーク機器を操作できるよう制限しています。
- 当社運営システムでは特定のIPアドレスからのみアクセスできるようロードバランサーの設定を行い、外部からの不正なアクセスなどを防止しています。また、当社運営システムへの通信はすべて暗号化されています。

ネットワーク構成



※この図は当社のネットワーク構成を簡易的に表した図です。侵入防御、多層防御、通信の暗号化についてご理解いただきやすいよう一部省略しています。

ログ管理

当社では、従業員へ貸与した端末、ネットワーク機器、当社提供サービスなどのログを専用のログ管理システム もしくは 利用サービス内のログ管理機能で保管 / 管理しています。
万が一インシデントが発生した場合も、速やかに原因や情報漏洩の発生有無などを調査できる体制を整えています。

端末ログ	・端末の操作ログ ・EDR 製品のログ	・資産管理ソフトのログ
ネットワークログ	・社内ネットワークの通信ログ	・セキュリティイベントログ
サービスログ	・当社管理システムの操作ログ ・当社管理サーバーのアクセスログ	・当社管理メールサーバーのメールログ ・当社標準利用サービスの操作ログ
入室ログ	・執務エリアへの入室ログ ・サーバールームへの入室ログ	・監視カメラのログ

当社運営システムの
セキュリティに関する取り組み

当社では、クライアントに安心してシステムをご利用いただくために、様々なセキュリティに関する取り組みを行っています。代表的なものは以下の通りです。

アクセスの制限	特定の IP アドレスからのアクセスのみを許可することで、不正アクセスを防止します。
通信の暗号化	通信を暗号化することで、第三者に通信内容を改ざん、傍受されても、情報漏洩を防止します。
不審な通信の検知・遮断	不審な通信が行われた場合はファイアウォールによって、検知・遮断されます。
パスワードの暗号化	アカウントのパスワードを暗号化して保存することで、情報漏洩を防止します。
ログイン試行回数の制限	アカウント認証時には、ログイン試行回数を制限し、ブルートフォース攻撃の対策を行っています。
強度の高いパスワードの設定	第三者に推測されにくいパスワードでなければ、システムに登録できないよう制限しています。
ログイン履歴・操作ログ確認	管理者権限のあるクライアントがログイン履歴、操作ログをシステム上で確認できます。
定期的なバックアップ	全てのシステムで日々、ログやデータのバックアップを取得しています。 また、バックアップについては、クライアントの案件の要件に合わせて保存期間を定めています。

終わりに

最後までお読みいただき、ありがとうございました。本セキュリティホワイトペーパーが、当社のセキュリティに対する想いや取り組みについて、理解の一助となれば幸いです。

本セキュリティホワイトペーパーについてのお問い合わせは、当社ホームページの CONTACT（お問い合わせ）までお願いいたします。
https://styleedge.co.jp/

当社は個人情報の保護に取り組んでいます。お問い合わせの際は、必ず当社のプライバシーポリシーをご一読いただき、同意のうえお問い合わせフォームをご利用ください。
https://styleedge.co.jp/privacy-policy/

改訂履歴

版数	発行日	改訂内容
第 1 版	2023 年 9 月	初版発行