OKI

MULTIFUNKTIONALE DIGITALE FARBSYSTEME /
MULTIFUNKTIONALE DIGITALSYSTEME

Sicherheitseinstellungen Management Anleitung

ES9160 MFP/ES9170 MFP
ES9460 MFP/ES9470 MFP
CX3535 MFP/CX4545 MFP

Vorwort

Vielen Dank für den Kauf des digitalen Multifunktionssystems von Oki.
Dieses Handbuch beschreibt die Voraussetzungen und Einstellungen des digitalen Multifunktionssystems für die Kompatibilität mit IEEE Std 2600.1™-2009 *1.
Lesen Sie dieses Handbuch, bevor Sie die Ihr digitales Multifunktionssystem in diesem hohen Sicherheitsmodus benutzen. Lesen Sie die “Sicherheitshinweise” unter “Sicherheitsinformationen”, damit das System in Übereinstimmung mit IEEE Std 2600.1™-2009 betrieben werden kann.
Halten Sie dieses Handbuch griffbereit, damit Sie es jederzeit für die Verwendung des Systems gemäß IEEE Std 2600.1™-2009 benutzen können.

■ Über dieses Handbuch

❑ Symbole in diesem Handbuch

In diesem Handbuch sind wichtige Hinweise durch folgende Symbole gekennzeichnet. Lesen Sie diese Hinweise, bevor Sie das System benutzen.

⚠ **WARNUNG**	Diese Gefahrenstufe weist auf eine potenziell gefährliche Situation hin, die - wenn sie nicht behoben wird - tödliche bzw. ernsthafte Verletzungen, erhebliche Schäden oder Feuer im Gerät oder in seiner Umgebung nach sich ziehen kann.
⚠ **VORSICHT**	Diese Gefahrenstufe weist auf eine potenziell gefährliche Situation hin, die - wenn sie nicht behoben wird - geringfügige bis mittlere Verletzungen, Teilschäden am Gerät oder in seiner Umgebung sowie Datenverlust nach sich ziehen kann.
Hinweis	Kennzeichnet Informationen, die Sie bei der Bedienung des Systems beachten sollten.

Weiterhin sind in diesem Handbuch Informationen enthalten, die die Bedienung des Systems erleichtern:

Tipp	Beschreibt praktische Tips zur Bedienung des Systems.
🕮	Seiten, auf denen Sie weitere Hinweise finden können. Lesen Sie ggf. auch diese Seiten.

❑ Geltende Modelle

ES9160 MFP/ES9170 MFP
ES9460 MFP/ES9470 MFP
CX3535 MFP/CX4545 MFP
Wird eine bestimmte Modellbezeichnung angegeben, gilt der Hinweis nur für das entsprechende Modell. Wird keine Modellbezeichnung angegeben, gilt der Hinweis nur für alle oben genannten Modelle.

❑ Beschreibungen für Bedienfeld und Touch Screen

- Einzelne Menüinhalte können in der Praxis abweichen, da sie von der Systemumgebung, z.B. installierte Optionen, abhängig sind.
- Die Abbildungen der Bildschirme in diesem Handbuch wurden in der Papiereinstellung für A/B-Format erstellt. Wenn Sie als Papiereinstellung das LT-Format verwenden, kann die Anordnung der Tasten von Ihrem System abweichend sein.

❑ Handelsmarken

- Der offizielle Name von Windows XP ist Microsoft Windows XP Operating System.
- Der offizielle Name von Windows Vista ist Microsoft Windows Vista Operating System.
- Der offizielle Name von Windows 7 ist Microsoft Windows 7 Operating System.
- Der offizielle Name für Windows Server 2003 ist Microsoft Windows Server 2003 Operating System.
- Der offizielle Name für Windows Server 2008 ist Microsoft Windows Server 2008 Operating System.
- Microsoft, Windows, Windows NT sowie die Produktnamen anderer Microsoft-Produkte sind Warenzeichen der Microsoft Corporation in den USA und anderen Ländern.
- Apple, AppleTalk, Macintosh, Mac, Mac OS, Safari und TrueType sind Warenzeichen von Apple Inc. in den USA und anderen Ländern.
- Adobe, Acrobat, Reader und PostScript sind Warenzeichen von Adobe Systems Incorporated in den USA und anderen Ländern.
- Mozilla, Firefox und das Firefox Logo sind Warenzeichen oder eingetragene Handelsmarken von Mozilla Foundation in den USA und anderen Ländern.
- IBM, AT und AIX sind Warenzeichen der International Business Machines Corporation.
- NOVELL, NetWare und NDS sind Warenzeichen von Novell, Inc.
- Weitere in diesem Handbuch oder in der Software genannten Firmen- und Produktnamen sind Handelsmarken ihrer jeweiligen Eigentümer.

INHALTSVERZEICHNIS

1

HOHER SICHERHEITSMODUS

Sicherheitshinweise

Dieser Modus schützt das System vor unbefugten Zugriffen und Informationsverlust.
Die folgenden Sicherheitsfunktionen entsprechen dem Standard IEEE Std 2600.1™-2009.

- Benutzerverwaltung
- Funktionszuweisungen
- Verschlüsselung der Daten auf der Festplatte
- Protokollierung und Suchfunktion
- Überschreiben der Festplattendaten nach Ausführung eines Jobs oder nach Einschalten des Systems
- Kommunikation mit SSL oder TLS
- Integritätsprüfung
- Managementfunktionen wie:
  Systemprotokolle, Kennwörter, Benutzer, Kennwortrichtlinie, Datum & Uhrzeit, Automatische Rückstellung, Sitzungszeitgeber, Ein-/Ausschalten von SSL/LTS

Zum Betrieb des Systems im hohen Sicherheitsmodus gemäß IEEE Std 2600.1™-2009 ist eine entsprechende Konfiguration der Systemumgebung wie Daten- und Protokollverschlüsselung sowie Authentifizierung von Server und Client PC erforderlich.
Nur wenn die in diesem Handbuch beschriebenen Bedingungen erfüllt sind, kann das System in Übereinstimmung mit IEEE Std 2600.1™-2009 betrieben werden.

Tipp

Einzelheiten zu den jeweiligen Sicherheitsfunktionen siehe TopAccess-Anleitung.

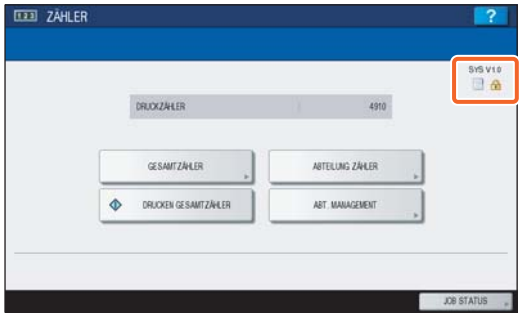
■ Prüfen des Modus

Im hohen Sicherheitsmodus wird  im Touch Screen des Systems angezeigt.

Tipps

- Im hohen Sicherheitsmodus sind die Daten auf der Festplatte des Systems verschlüsselt. Zusätzlich ist in derartigen Systemen der Data Overwrite Kit (GP-1070) installiert.
  Die Prüfung der jeweiligen Funktion kann oben rechts im [Zähler]-Bildschirm des Systems durchgeführt werden.

Die HDD ist verschlüsselt.	wird angezeigt. Auch wenn dies nicht angezeigt wird, ist die Festplatte des Systems verschlüsselt, wenn das System im hohen Sicherheitsmodus betrieben wird.
Der Data Overwrite Enabler ist aktiviert.	zeigt an, dass der Data Overwrite Enabler korrekt funktioniert. Die Systemversion (V1.0) wird angezeigt.



- Wenn der Data Overwrite Enabler installiert ist, werden temporäre Daten während der Job-Verarbeitung überschrieben und können für den nächsten Job verwendet werden.

■ Bedingungen

Wählen Sie [Benutzerauthentifizierung], [Authentifizierungstyp] und [Lokale Authentifizierung]. Wir für die Authentifizierung ein SNTP-, LDAP- oder DNS-Server verwendet, erfüllt das System nicht die Voraussetzungen für IEEE Std 2600.1™-2009.

Für die Verbindungsaufnahme mit den System mittels eFiling BackUp/Restore Dienstprogramm, Datei-Downloader, TWAIN-Treiber oder Adressbuchanzeige müssen Name und Kennwort eingegeben werden. Die Kennworteingabe wird nicht angezeigt. Zusätzlich wird die Systemanmeldung gesperrt, wenn mehrmals ein falsches Kennwort eigegeben wurde.

Wählen Sie [VOLLSTÄNDIG] für die Durchführung der Integritätsprüfung.

* Einzelheiten siehe MFP Management-Anleitung.

Ändern Sie nicht die Kommunikations-Voreinstellungen des Systems. Die Netzwerk-Kommunikation kann geschützt über SSL durchgeführt werden, sofern dies nicht geändert wird.

Stellen Sie unter [USER FUNCTIONS] - [ADMIN] - [LISTEN/BERICHTE] - [BERICHTEINSTELLUNG] - [KOMM. BERICHT] die Position [SPEICHER SE] auf AUS.

Im Modus für hohe Sicherheit können folgende Funktionen nicht benutzt werden.

- Unterbrechungskopie
- Netzwerk Fax
- Zeitversetzter Druck
- Speichern in e-Filing über den Druckertreiber*
  * Die Funktion kann zwar ausgewählt werden; aber ein Fehler tritt auf und der Job wird gelöscht. Daher wird der Druck nicht ausgeführt. Gelöschte Jobs werden im Fehlerprotokoll aufgezeichnet. Prüfen Sie dies in TopAccess unter [Protokolle] oder am System unter [JOB STATUS] - [PROTOKOLLE] - [DRUCK].
- Deaktivieren der Benutzeranmeldung

Die automatische Benutzeranmeldung der mit dem System ausgelieferten Clientsoftware steht nicht zur Verfügung. Zur Benutzung der Clientsoftware müssen Sie immer Benutzernamen und Kennwort eingeben.

An das System gesendete Daten wie Fax und Internet Fax oder vom Druckertreiber* empfangene Druckdaten können nur gedruckt werden, wenn ein Anwender mit entsprechenden Benutzerrechten am System angemeldet ist.

* Verwenden Sie IPP SSL oder SSL unter WS-Druck für die Kommunikation mit dem System.

Verwenden Sie für den IPP-Druck den, durch Eingabe von “https://[IP-Adresse]:[SSL Portnummer]/Print” in das URL-Feld, erzeugten Port.

(Z.B.: https://192.168.1.2:443/Print)

* Einzelheiten siehe [IPP-Druck] unter [Druckertreiber installieren] - [Weitere Installationen] in der Software Installationsanleitung.

Verwenden Sie keine Anwendungen, die eine Änderung im Untermenü [ODCA] von [Setup] im Register [Verwaltung] von TopAccess erfordert.

Zur sicheren Benutzung des Systems sind folgende Punkte empfehlenswert.

- Verwenden Sie zum Speichern oder Senden von Dateien das verschlüsselte PDF Format mit der Verschlüsselungsstufe 128 bit AES.
- Definieren Sie einen zuverlässigen PC als Speicherziel für Scandaten.
- Verwenden Sie als Speicherziel nicht die ÖFFENTLICHE BOX in e-Filing, da hierfür kein Kennwortschutz möglich ist.
- Verwenden Sie als Speicherziel nicht MFP LOKAL, da hierfür kein Kennwortschutz möglich ist.
- Verwenden Sie für Berichtdrucke von InternetFax nicht “Druck mit Bild erste Seite”, damit die Kopie des Originals nicht angehängt wird.
- Verwenden Sie SMP Übergabe unter [Druckfreigabe].
- Deaktivieren Sie [Raw TCP] und [LPD] in den Druckdiensten.
- Administratoren sollten die Systemprotokolle regelmäßig exportieren und speichern.
- Wählen Sie [Deaktivieren] für [Twain Scan].

2

BESONDERE FUNKTIONEN

Temporäres Kennwort

Im hohen Sicherheitsmodus wird ein vom Administrator vergebenes, vorläufiges Kennwort als temporäres Kennwort angesehen. Zur weiteren Verwendung des Systems müssen Sie das temporäre Kennwort nach dem ersten Zugriff auf das System durch ein eigenes Kennwort ersetzen.

Hinweis

Wenn Sie das temporäre Kennwort weiter verwenden, ist die Sicherheitsstufe unzureichend. Speichern Sie so bald wie möglich ein eigenes Kennwort.

■ Fälle, in denen ein temporäres Kennwort verwendet wird

Ein temporäres Kennwort wird in folgenden Fällen verwendet:
- Für die erste Systemanmeldung nach der Registrierung durch den Administrator.
- Wenn ein Administrator das Benutzerkennwort zurückgesetzt hat.
- Wenn das Kennwort als Klartext vom Administrator importiert wurde.

Hinweis

Wenn ein Administrator das Benutzerkennwort zurückgesetzt hat, muss der Anwender darüber informiert werden, sein Kennwort durch ein eigenes zu ersetzen.

Tipp

Um zu verhindern, dass exportierte Benutzerinformationen verändert werden, sind diese mit Hash versehen. Zum Ändern des Kennworts für die exportierten Benutzerinformationen, wird Klartext für das Kennwort verwendet.

■ Benutzerhinweise für die Verwendung eines temporären Kennworts

Wenn das Kennwort bei einem Zugriff auf das System registriert werden kann.

Sobald Sie über das Bedienfeld oder die folgenden Dienstprogramme auf das System zugreifen, können Sie Ihr neues Kennwort registrieren. Nach der Registrierung können Sie die Funktionen benutzen, für die Ihnen die entsprechenden Berechtigungen erteilt wurden.
- Bedienfeld
- TopAccess

Wenn Sie mit temporärem Kennwort über das Bedienfeld oder TopAccess auf das System zugreifen, erscheint die Hinweismeldung, dass Sie ein temporäres Kennwort verwenden. Nach der Bestätigung erscheint ein Fenster zur Registrierung Ihres neuen Kennworts. Geben Sie ein neues Kennwort ein, bestätigen Sie es und drücken Sie [OK] (Bedienfeld) oder [Speichern] (TopAccess), um es zu registrieren. Das neue Kennwort können Sie direkt für die nächste Systemanmeldung benutzen.

Wenn das Kennwort bei einem Zugriff auf das System nicht registriert werden kann.

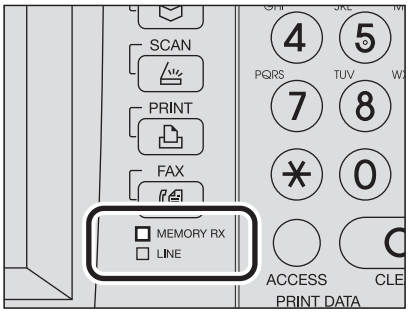
Mit folgenden Dienstprogrammen können Sie nicht mit temporärem Kennwort auf das System zugreifen. Daher kann auch kein neues Kennwort registriert werden. Registrieren Sie ein neues Kennwort über das Bedienfeld oder in TopAccess, bevor Sie diese Dienstprogramme verwenden.
- Remote Scan Treiber
- e-Filing Web Dienstprogramm
- Back Up/Restore Dienstprogramm
- Datei-Downloader
- TWAIN-Treiber
- Adressbuchanzeige

HALTEN (FAX)

Im Modus für hohe Sicherheit werden empfangene Emails, die FAX, Internet FAX oder Bilddaten enthalten, nicht automatisch ausgedruckt. Diese Jobs werden in der Warteschlange [GEHALTEN(FAX)] gespeichert und können nur von Anwendern gedruckt werden, die über die Berechtigung [Faxempfang drucken] verfügen.

Tipp

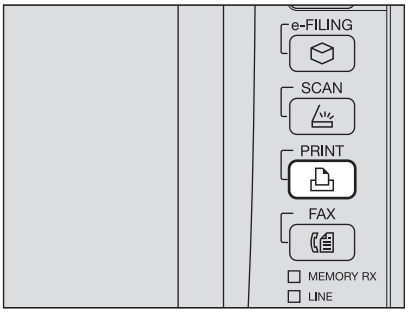
Wenn sich in der Warteschlange [GEHALTEN(FAX)] Jobs befinden, blinkt die Anzeige MEMORY RX / LINE.



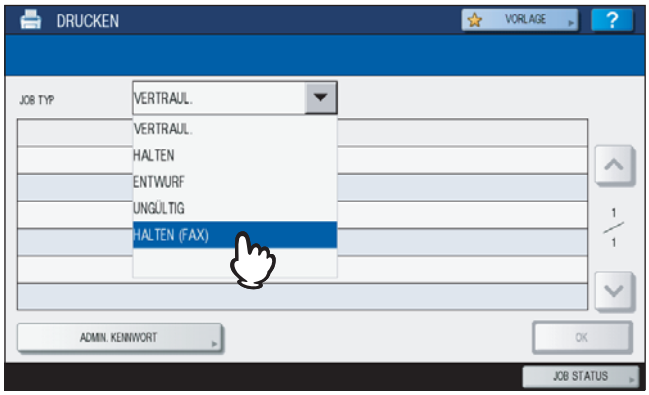
Jobs in der Warteschlange HALTEN (FAX) drucken

1 **Melden Sie sich mit Benutzerrechten für [Faxempfang drucken] am System an.**

2 **Drücken Sie die Taste [PRINT] am Bedienfeld.**

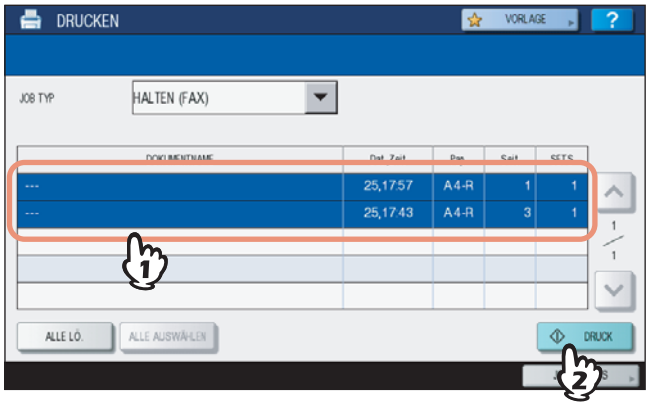


3 **Wählen Sie [HALTEN (FAX)].**



- Alle Jobs in der Warteschlange [HALTEN (FAX)] werden angezeigt.

4 Wählen Sie den gewünschten Job oder drücken Sie [ALLES AUSWÄHLEN] und drücken Sie anschließend [DRUCK].



- Die Jobs werden ausgegeben und anschließend aus der Warteschlange [HALTEN (FAX)] gelöscht.

3

DIE VOREINSTELLUNGEN

Sicherheitshinweise zu den Voreinstellungen

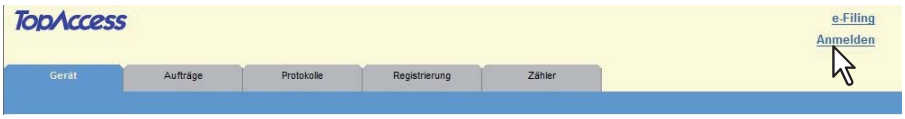
Die Voreinstellungen und die einstellbaren Positionen unterscheiden sich im Modus mit hoher Sicherheit vom normalen Sicherheitsmodus. Diese Unterschiede sind nachfolgend beschrieben.
Damit das System in Übereinstimmung mit IEEE Std 2600.1™-2009 betrieben werden kann, dürfen die nachfolgend beschriebenen Voreinstellungen nicht geändert werden.

Hinweise

- Zu den Voreinstellungen und die einstellbaren Positionen im normalen Sicherheitsmodus siehe TopAccess-Anleitung und MFP Management-Anleitung.
- Sichern Sie alle Systemeinstellungen und Benutzerdaten, bevor Sie eine “Initialisierung” des Systems durchführen und dadurch alle Einstellungen zurücksetzen. Einzelheiten siehe TopAccess-Anleitung und MFP Management-Anleitung.

■ Systemanmeldung

- Die Register [Benutzerverwaltung] und [Administrator] werden in TopAccess nur angezeigt, wenn die Systemanmeldung mit Administratorrechten erfolgt. Öffnen Sie TopAccess, klicken Sie oben rechts auf “Anmelden” und geben Sie Benutzername und Kennwort ein.



- Achten Sie darauf, die Anmeldung am System mit [USER FUNCTIONS] als [ADMIN] durchzuführen.

■ Tabelle der Voreinstellungen

Register [Verwaltung]
Menü [Setup]
Untermenü [Allgemein]

Funktionen		
Speichern an FTP	Deaktiviert	
Netzwerk iFax	Deaktiviert	
Netzwerk Fax	Deaktiviert	
Web Services Scan	Deaktiviert	
Twain Scan	Aktiviert	Diese Voreinstellung entspricht dem normalen Sicherheitsmodus; sie sollte auf AUS geändert werden.
Adressbuchgebrauch einschränken durch Administrator		
Benutzung nur durch Administrator		
Energie sparen		
Autom. Löschen *	45 Sek.	Diese Voreinstellung entspricht dem normalen Sicherheitsmodus; sie kann nicht auf AUS geändert werden.

* Die Einstellung kann am Bedienfeld des Systems unter [USER FUNCTIONS] im Register [ADMIN] geändert werden.

Untermenü [Netzwerk]

HTTP-Netzwerkdienst		
SSL aktivieren	Aktiviert	
SMTP Client		
SSL aktivieren	Mit importierten CA Zertifikat(en) prüfen	Die Sicherheitseinstellung ist "Mit importierten CA Zertifikat(en) prüfen" oder "Alle Zertifikate ohne CA akzeptieren".
Authentifizierung	AUTO	Achten Sie darauf, dass in Ihrer Systemumgebung entweder "CRAM-MD5", "Digest-MD5", "Kerberos" oder "NTLM (IWA)" angewendet wird.
SMTP Server		
SMTP-Server aktivieren	Deaktiviert	
POP3-Netzwerkdienst		
SSL aktivieren	Mit importierten CA Zertifikat(en) prüfen	
FTP Client		
SSL aktivieren	Mit importierten CA Zertifikat(en) prüfen	
FTP Server		
SSL aktivieren	Aktiviert	
SNMP-Netzwerkdienst		
SNMP V1/V2 aktivieren	Deaktiviert	
SNMP V3 aktivieren	Aktiviert	
Web Services Einstellung		
SSL aktivieren	Aktiviert	
Web Services Scan	Deaktiviert	

* Die Einstellung kann am Bedienfeld des Systems unter [USER FUNCTIONS] im Register [ADMIN] geändert werden.

Untermenü [Drucker]

Allgemeine Einstellung		
Einschränkung für Druckjobs	Nur Halten	

Untermenü [Druckdienst]

IPP Druck		
SSL aktivieren	Aktiviert	

FTP Druck		
FTP-Druck aktivieren	Deaktiviert	

Menü [Sicherheit]

Untermenü [Authentifizierung]

Benutzerauthentifizierung Einstellung		
Benutzer Authentifizierung	Aktiviert	Kann nicht auf "Deaktiviert" geändert werden.
Authentifizierung Typ	Lokale MFP-Authentifizierung	
Gastbenutzer aktivieren	Nicht markiert (Deaktiviert)	Diese Voreinstellung entspricht dem normalen Sicherheitsmodus; sie kann nicht auf "Aktiviert" geändert werden.

Untermenü [ODCA]

Netzwerk		
Port aktiviert	Deaktiviert	

Untermenü [Kennwortrichtlinie]

Richtlinie für Benutzer		
Minimale Kennwortlänge	8 (Stellen)	
Zu erfüllende Anforderungen	Aktiviert	
Sperreinstellung	Aktiviert	(Identisch mit normalem Sicherheitsmodus)
Anzahl Wiederholungen	3 (mal)	
Sperrzeit	2 (Minuten)	
Verfügbarer Zeitraum	Deaktiviert	(Identisch mit normalem Sicherheitsmodus)
Ablauftag(e)	90 (Tage)	
Richtlinie für Administrator, Auditor		
Minimale Kennwortlänge	8 (Stellen)	
Zu erfüllende Anforderungen	Aktiviert	
Sperreinstellung	Aktiviert	(Identisch mit normalem Sicherheitsmodus)
Anzahl Wiederholungen	3 (mal)	
Sperrzeit	2 (Minuten)	
Verfügbarer Zeitraum	Deaktiviert	(Identisch mit normalem Sicherheitsmodus)
Ablauftag(e)	90 (Tage)	
Richtlinie für e-Filing Boxen, Vorlagengruppen, Vorlagen, SicherePDF, SNMPv3 und Klonen		
Minimale Kennwortlänge	8 (Stellen)	
Zu erfüllende Anforderungen	Aktiviert	
Sperreinstellung	Aktiviert	(Identisch mit normalem Sicherheitsmodus)
Anzahl Wiederholungen	3 (mal)	
Sperrzeit	2 (Minuten)	

Oki Data Corporation
4-11-22 Shibaura, Minato-ku,Tokyo
108-8551, Japan

www.okiprintingsolutions.com

45117404EE